alice2
América Latina Inter Conectada con Europa

Taller: Mecanismos de Transición IPv6

Alvaro Vives, Consulintel
alvaro.vives@consulintel.es

This project is funded by the European Union
A project implemented by CLARA

Agenda

1. Formatos de cabeceras y tamaño de paquetes
2. Direccionamiento IPv6
3. ICMPv6, Neighbor Discovery y DHCPv6
4. Mecanismos de Transición

1. Formatos de cabeceras y tamaño de paquetes

1.1 Terminología

1.2 Formato cabecera IPv6

1.3 Cabeceras de Extensión

1.1 Terminología

IPv6 (RFC2460)

- Especificación básica del Protocolo de Internet versión 6
- Cambios de IPv4 a IPv6:
  - Capacidades expandidas de direccionamiento
  - Simplificación del formato de la cabecera
  - Soporte mejorado de extensiones y opciones
  - Capacidad de etiquetado de flujos
  - Capacidades de autenticación y encriptación

Terminología

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

1.2 Formato cabecera IPv6

Formato de la Cabecera IPv4

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

bits: 4	8	16	20	32
Version	H. Length	TOS	Total Length	
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
32 bits Source Address				
32 bits Destination Address				
Options				

Campo Modificado
Campo Eliminado

Formato de la Cabecera IPv6

- Reducción de 12 a 8 campos (40 bytes)

bits: 4	12	16	24	32
Version	Class of Traffic	Flow Label		
Payload Length		Next Header		Hop Limit
128 bits Source Address				
128 bits Destination Address				

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

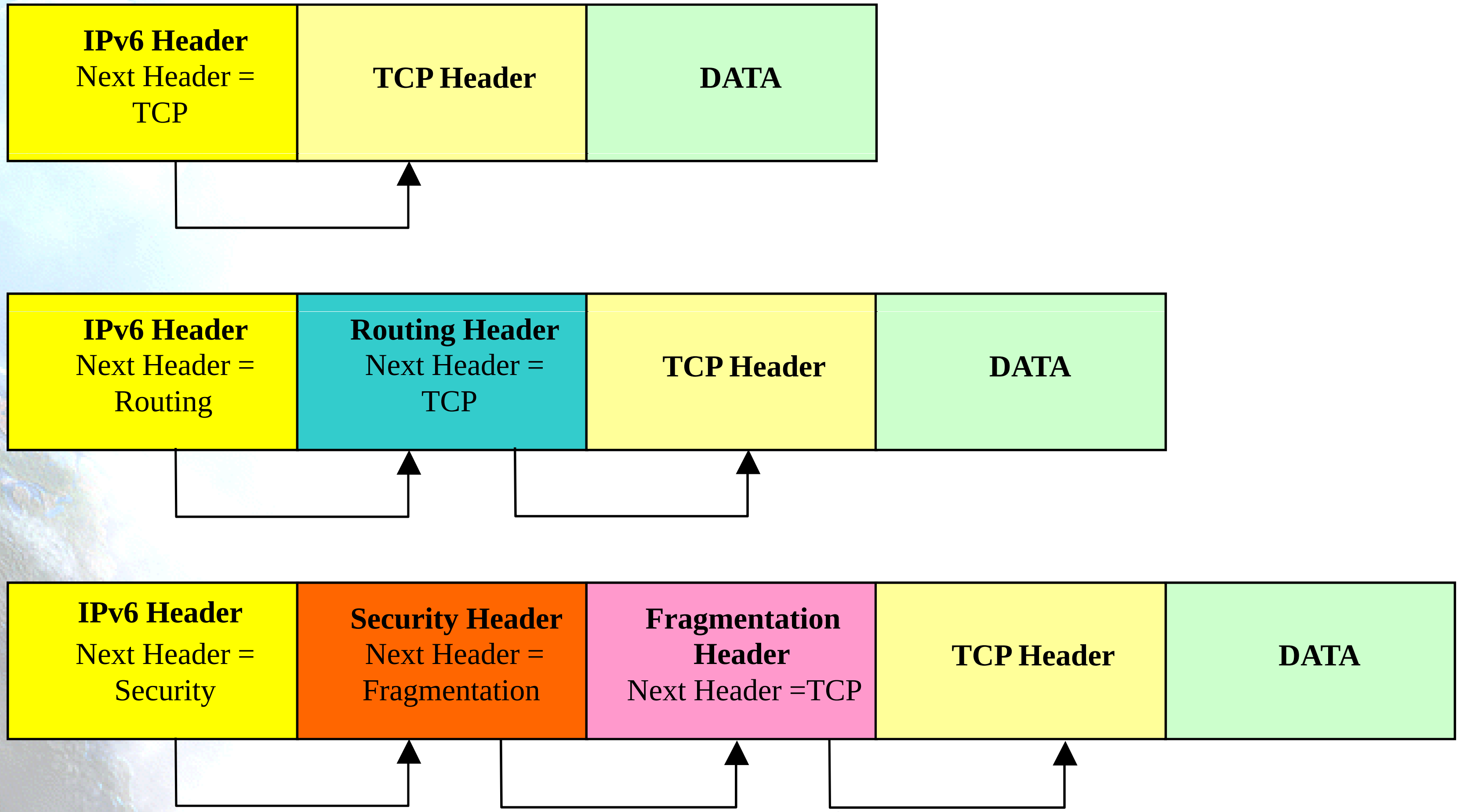
Resumen de los cambios de la Cabecera

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

1.3 Cabeceras de Extensión

Cabeceras de Extensión

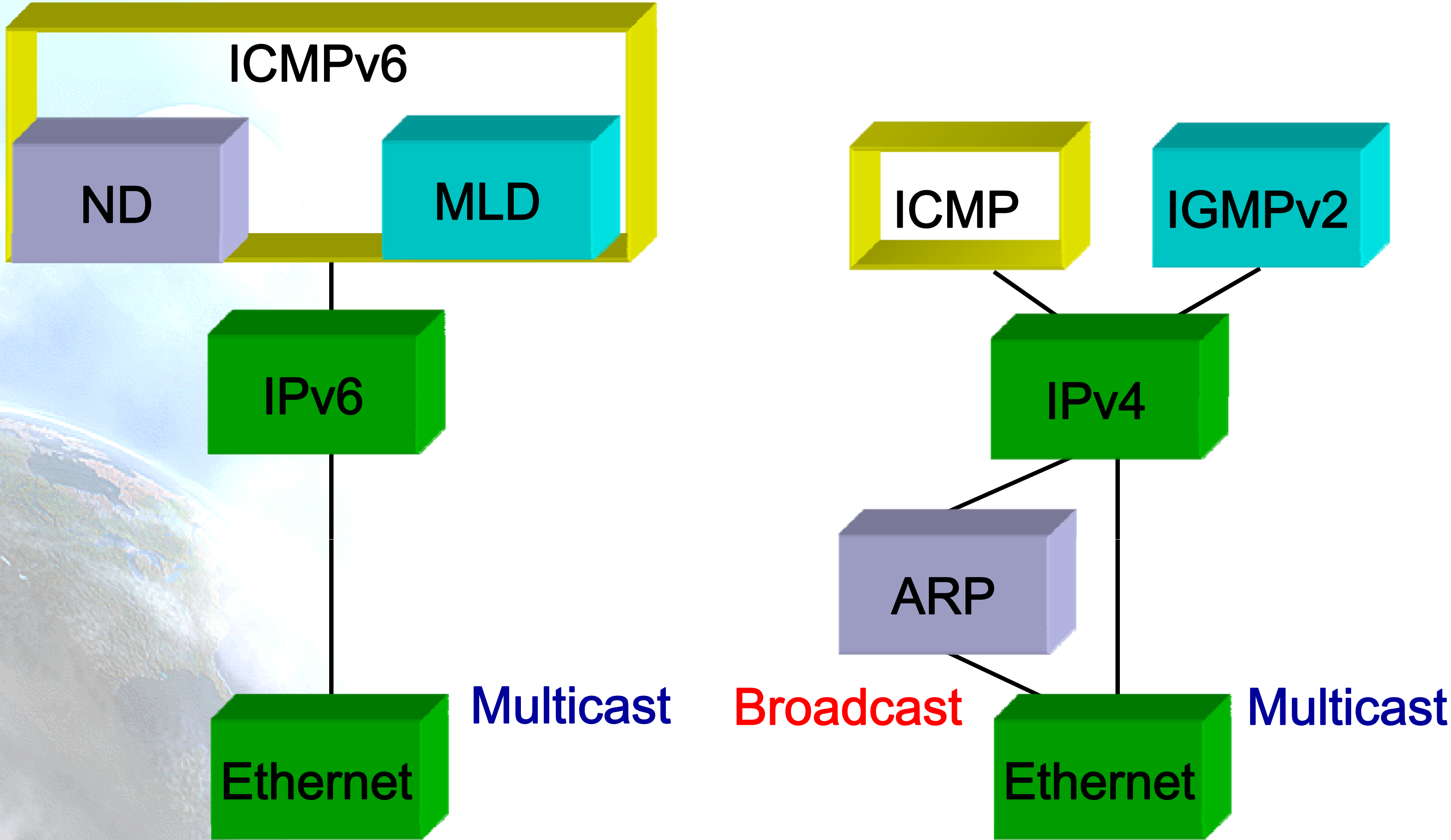
- Campo "Next Header"



Ventajas de las Cabeceras de Extensión

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

Plano de Control IPv4 vs. IPv6



2. Direccionamiento IPv6

2.1 Tipos de Direcciones

2.2 Prefijo y representación

2.3 Direcciones IPv6 Unique Local

2.4 Identificadores de interfaz

2.5 Direcciones Multicast

2.6 Gestión de direcciones

2.1 Tipos de Direcciones

Tipos de Direcciones (RFC4291)

Unicast (uno-a-uno)
- globales
- enlace-local
- local-de-sitio (desaprobada)
- Unique Local (ULA)
- Compatible-IPv4 (desaprobada)
- Mapeada-IPv4

Multicast (uno-a-muchas)

Anycast (uno-a-la-mas-cercana)

Reservado

Algunas Direcciones Unicast Especiales

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

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

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

2.2 Prefijo y representación

Representación Textual de las Direcciones (1)

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

Formato comprimido: 2001:DB8::43

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

IPv4-mapped: ::FFFF:13.1.68.3

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

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

2001:DB8:3003::/48

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

Representación Textual de las Direcciones (2)

Normas:

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

Ejemplos:

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

   Queda: 2001:db8:3003:1::6543:ffe

2. (Alumnos) 2001:0db8:0000:0000:0300:0000:0000:0abc

Prefijos de los Tipos de Direcciones

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

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

Dirección Global Unicast (RFC3587)

001	Glob. Rout. prefix	subnet ID	interface ID
	Prefijo global de encaminamiento (45 bits)	Identificador de sub-red (16 bits)	Identificador de interfaz (64 bits)

- 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

Direcciones Link-Local y Site-Local

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

1111111010	0	interface ID

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

1111111011	0	SLA*	interface ID

Dirección Anycast

- Es un identificador de un conjunto de interfaces (normalmente en diferentes nodos).
- Un paquete enviado a una dirección anycast se entregará a una de las interfaces identificadas por esa dirección (la más cercana desde el punto de vista de los protocolos de encaminamiento)
- Se obtienen del espacio de direcciones unicast (de cualquier ámbito) y son **sintacticamente indistiguinguibles de las direcciones unicast.**
- Las direcciones anycast reservadas se definen en el RFC2526

2.3 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:

Prefix	L	global ID	subnet ID	interface ID
7 bits	1	40 bits	16 bits	64 bits

- 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

2.4 Identificadores de interfaz

Identificadores de Interfaz

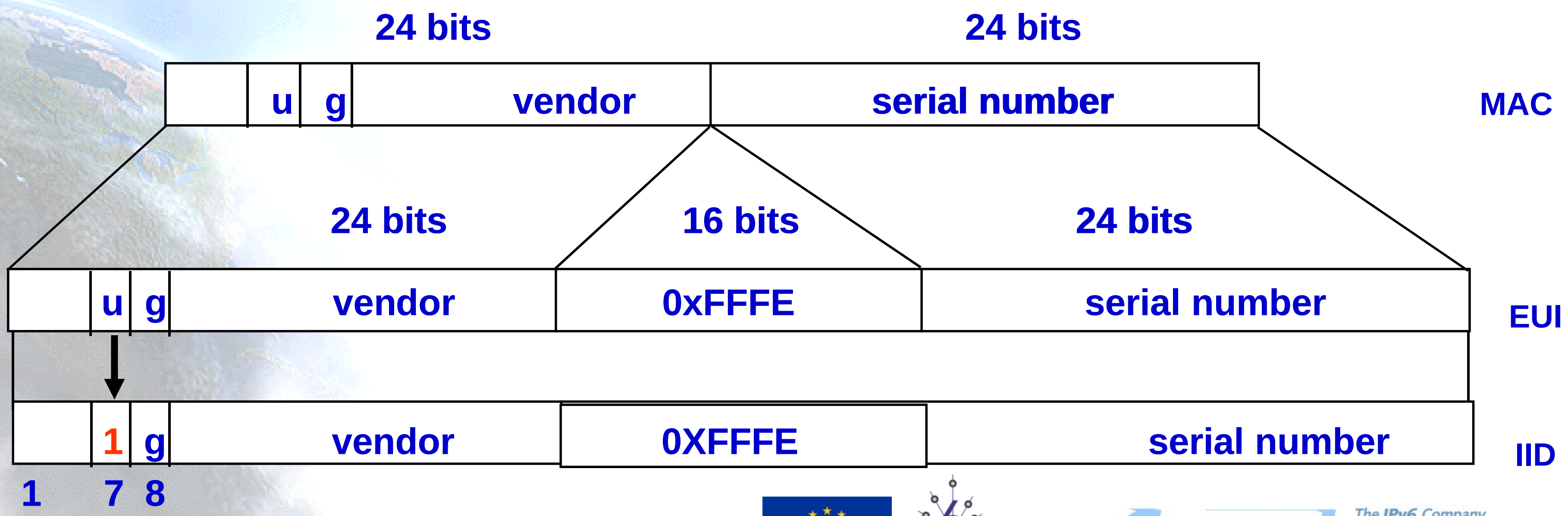
Los 64-bits de menor peso de las direcciones Unicast pueden ser asignados mediante diversos métodos:

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

Network ID	Interface ID
64 bits	64 bits

EUI-64

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



2.5 Direcciones Multicast

Direcciones Multicast

11111111	flags	scope	group ID
8	4	4	112 bits

- 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)

2.6 Gestión de direcciones

Gestión Direcciones

- Una vez que se tiene el plan de direccionamiento, en el día a día se deben gestionar las direcciones y prefijos
- Recomendable usar alguna herramienta de gestión de direcciones, comercial o de elaboración propia
- Se pretende que se puedan aumentar las asignaciones hechas, si fuese necesario en el futuro
- Dos formas de hacer esto: **método flexible de asignación de bits** [RFC3531] y **prefijos separados por distancia potencia de dos**

Método Flexible (1)

- Se especifica en el RFC3531 como una manera flexible de asignar los bits de un prefijo que permite posponer al máximo la decisión del número de bits a asignar
- Si dividimos una dirección IPv6 en N partes (p1, p2,…, pN), la asignación de direcciones de p1 se hará usando los bits más a la izquierda, la de pN usando los bits más a la derecha y para el resto (p2, …, pN) se fijará un límite arbitrario y se usarán los bits centrales de cada parte
- El algoritmo viene descrito en el RFC3531, haría falta una herramienta que calcule los prefijos adecuadamente
- Se crea un *pool* de direcciones con el orden en que se irán asignando

Método Flexible (2)

Prefijo Inicial	Asignación (binario)	Asignación (hexadecimal)	Prefijo Asignar	Orden
2001:db8::/32	0000 0000 1000 0000	0080	2001:db8:0080::/48	1
	0000 0001 0000 0000	0100	2001: db8:0100::/48	2
	0000 0001 1000 0000	0180	2001: db8:0180::/48	3
	0000 0000 0100 0000	0040	2001: db8:0040::/48	4
	0000 0000 1100 0000	00C0	2001: db8:00C0::/48	5
	0000 0001 0100 0000	0140	2001: db8:0140::/48	6
	0000 0001 1100 0000	01C0	2001: db8:01C0::/48	7
	0000 0010 0000 0000	0200	2001: db8:0200::/48	8
	0000 0010 0100 0000	0240	2001: db8;0240::/48	9
	0000 0010 1000 0000	0280	2001: db8:0280::/48	10
	0000 0010 1100 0000	02C0	2001: db8:02C0::/48	11
	0000 0011 0000 0000	0300	2001: db8:0300::/48	12
	0000 0011 0100 0000	0340	2001: db8:0340::/48	13
	0000 0011 1000 0000	0380	2001: db8:0380::/48	14
	0000 0011 1100 0000	03C0	2001: db8:03C0::/48	15
	0000 0000 0010 0000	0020	2001: db8:0020::/48	16

Distancia Potencia de Dos (1)

- En la práctica lo que se suele hacer es simplificar el método flexible haciendo asignaciones de prefijos con cierta “distancia”
- En el futuro se podrán asignar prefijos contiguos a los ya previamente asignados, éstos se agregarán para formar un prefijo mayor
- A mayor “distancia” mayor flexibilidad futura, pero también mayor “desperdicio” de direcciones (siempre se podrán asignar a otro usuario pero perdiendo flexibilidad)

Distancia Potencia de Dos (2)

Prefijo Inicial	Asignación (binario)	Asignación (hexadecimal)	Prefijo Asignar	Orden
2001:db8::/32	0000 0000 0000 0000	0000	2001:db8:0000::/48	1
	0000 0000 0000 0100	0004	2001:db8:0040::/48	2
	0000 0000 0000 1000	0008	2001:db8:0008::/48	3
	0000 0000 0000 1100	000C	2001:db8:000C::/48	4
	0000 0000 0001 0000	0010	2001:db8:0010::/48	5
	0000 0000 0001 0100	0014	2001:db8:0014::/48	6
	0000 0000 0001 1000	0018	2001:db8:0018::/48	7
	0000 0000 0001 1100	001C	2001:db8:001C::/48	8
	0000 0000 0010 0000	0020	2001:db8;0020::/48	9

3. ICMPv6, Neighbor Discovery y DHCPv6

3.1 ICMPv6

3.2 Neighbor Discovery

3.3 Autoconfiguración

3.4 DHCPv6

3.5 Secure Neighbor Discovery

3.1 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.

Mensaje ICMP de Error

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

Tipos de mensajes de error ICMPv6

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

Mensajes ICMP Informativos

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

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

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

3.2 Neighbor Discovery

ND (RFC4861)

- 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).

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.

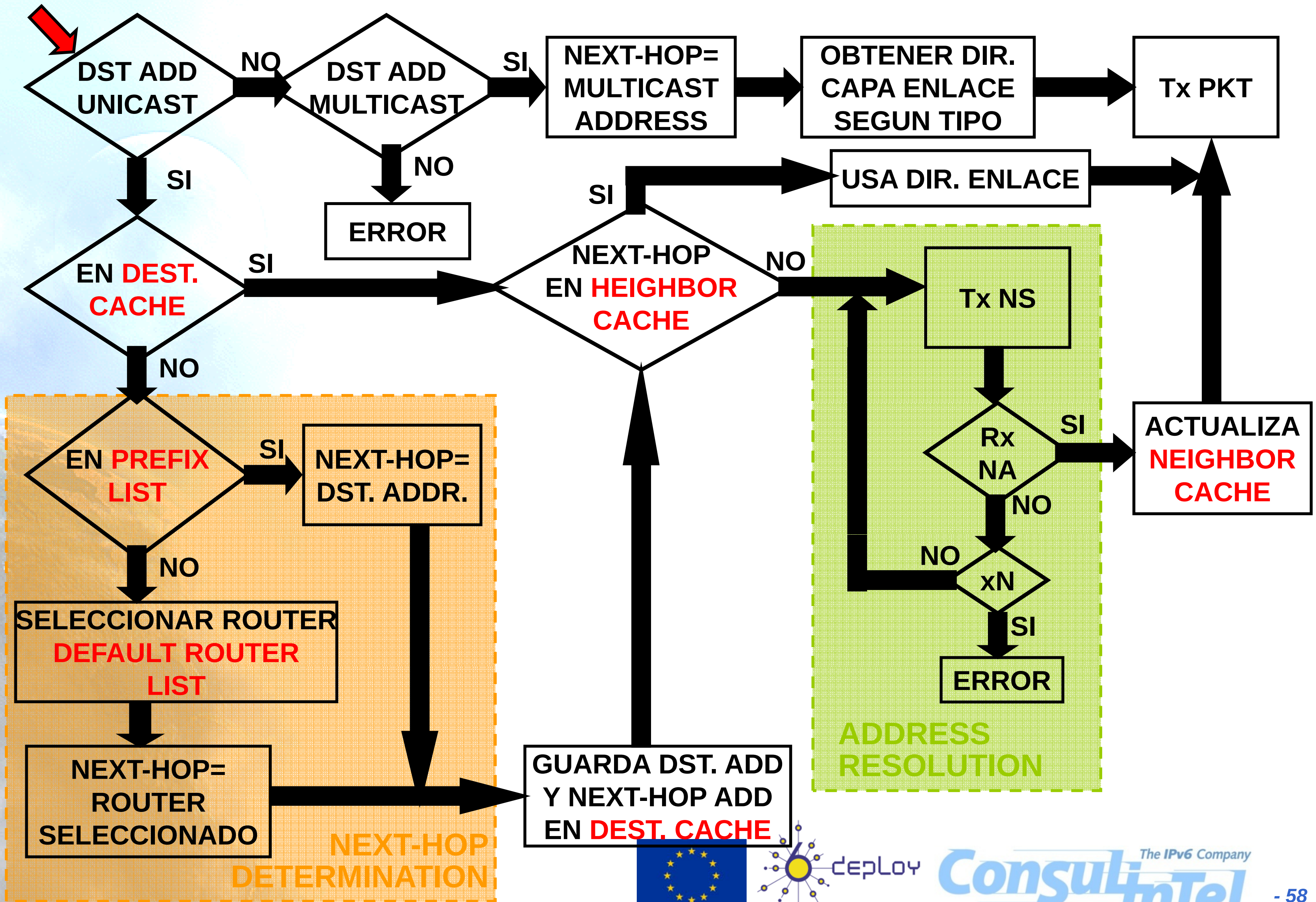
Bits 8	16	32
Type = 137	**Code = 0**	**Checksum**
Reserved = 0		
Target Address		
Destination Address		
Options …		

- 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



3.3 Autoconfiguración

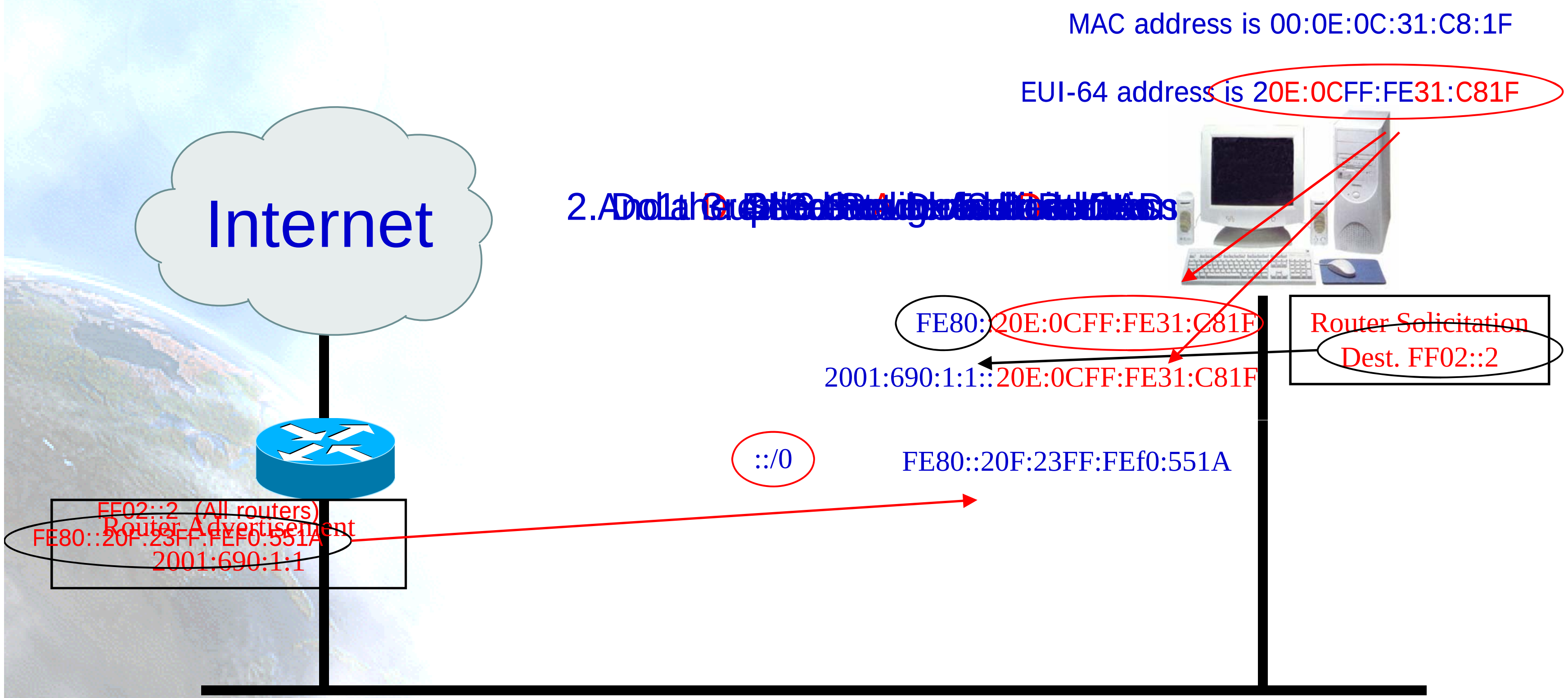
Autoconfiguración

- El estándar especifica los pasos que un host debe seguir para decidir cómo auto-configurar sus interfaces de red en IPv6
- El proceso de auto-configuración incluye la creación de una dirección IPv6 de ámbito local (link-local) y la verificación de que no está duplicada en el mismo segmento de red, determinando qué información debería ser auto-configurada y en el caso de direcciones, si estas deberían obtenerse mediante “stateful”, “stateless” o ambos
- IPv6 define tanto un mecanismo de auto-configuración de direcciones de tipo “stateful” como “stateless”
- La auto-configuración “stateless” (SLAAC) 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 (64 bits)
- 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 (64 bits)
- 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

Autoconfiguración Stateless



Configurar el Servidor DNS con Autoconfiguración Stateless (1)

- Hay dos maneras de configurar el servidor DNS en un nodo:
  - Manualmente
  - Con DHCPv6 o DHCPv4 (en caso de nodos dual-stack)
- Puede ser un problema en algunos entornos:
  - Necesidad de usar dos protocolos en IPv6 (Stateless Autoconfguration y DHCPv6)
  - Retardo al obtener el servidor DNS cuando se usa DHCP
  - En entornos wireless, donde el nodo cambia de red frecuentemente, no es posible usar configuración manual o el retardo del DHCP puede ser demasiado
- Una nueva forma de configurar servidores DNS sedefine en el RFC6106, la opción Recursive DNS Server (RDNSS) para los RA
  - Se puede usar conjuntamente con DHCPv6

Configurar el Servidor DNS con Autoconfiguración Stateless (2)

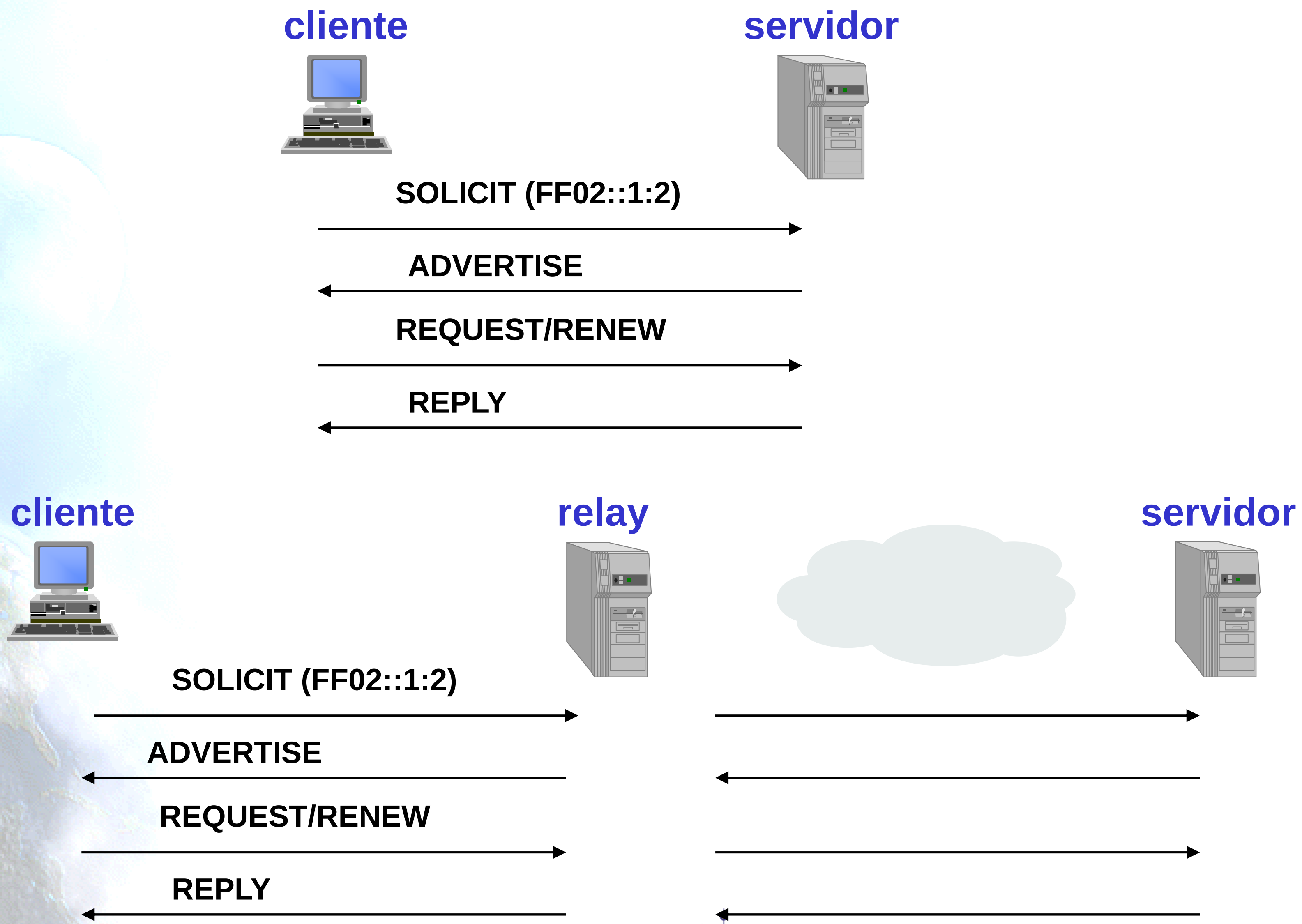
- Funciona de la misma manera en que se aprenden los prefijos y routers usando ND: IPv6 Sateless Address Autoconfiguration [RFC4862]
- Con la opción RDNSS el nodo aprende, con solo un mensaje:
  - Prefjo para usar en la autoconfiguración
  - Gateway IP
  - Servidores DNS Recursivos
- Si, además de la opción RDNSS, se usa DHCPv6, se debe activar el flag "O" en el RA
- Dos opciones para configurar la opción RDNSS en los routers:
  - Manualmente
  - Automaticamente, siendo un cliente DHCPv6

3.4 DHCPv6

DHCPv6

- DHCPv6 [RFC3315] se usa cuando:
  - No hay router
  - Lo indica el RA (ManagedFlag y OtherConfigFlag)
- Modelo cliente servidor sobre UDP, que proporciona al cliente una dirección IPv6 y otros parámetros (Servidor DNS, etc.)
- No proporciona Puerta de enlace (Default Gateway)
- Utiliza direcciones multicast conocidas: All_DHCP_Relay_Agents_and_Servers (FF02::1:2), All_DHCP_Servers (FF05::1:3)
- También hay un DHCPv6 stateless, definido en [RFC3736]

Ejemplo Básico de DHCPv6



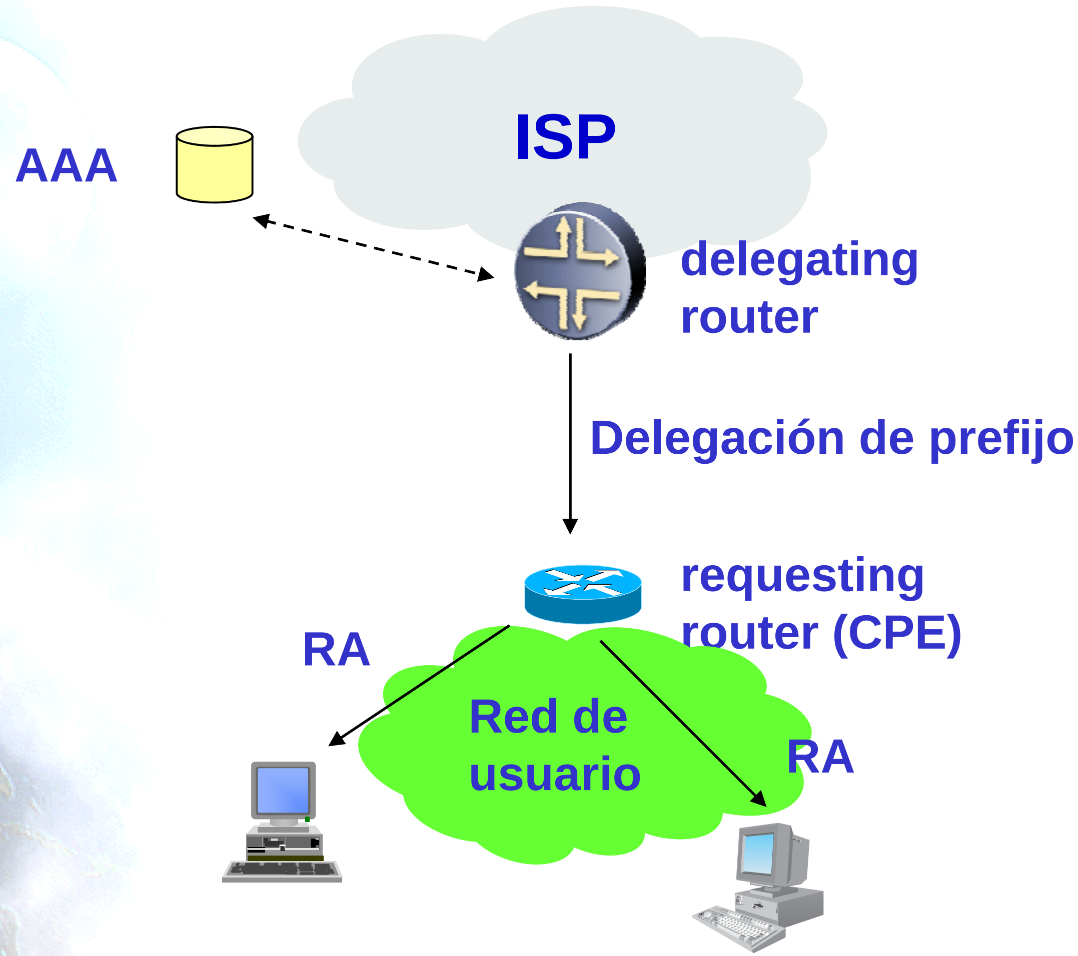
DHCPv6-PD (RFC3633)

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

Detalles de DHCPv6-PD

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

Arquitectura de Red para DHCPv6-PD



4. Mecanismos de Transición

4.1 Estrategias coexistencia IPv4-IPv6

4.2 Doble Pila

4.x Túneles

4.12 Traducción

4.13 NAT64

4.1 Conceptos de Transición

Técnicas de Transición / Coexistencia

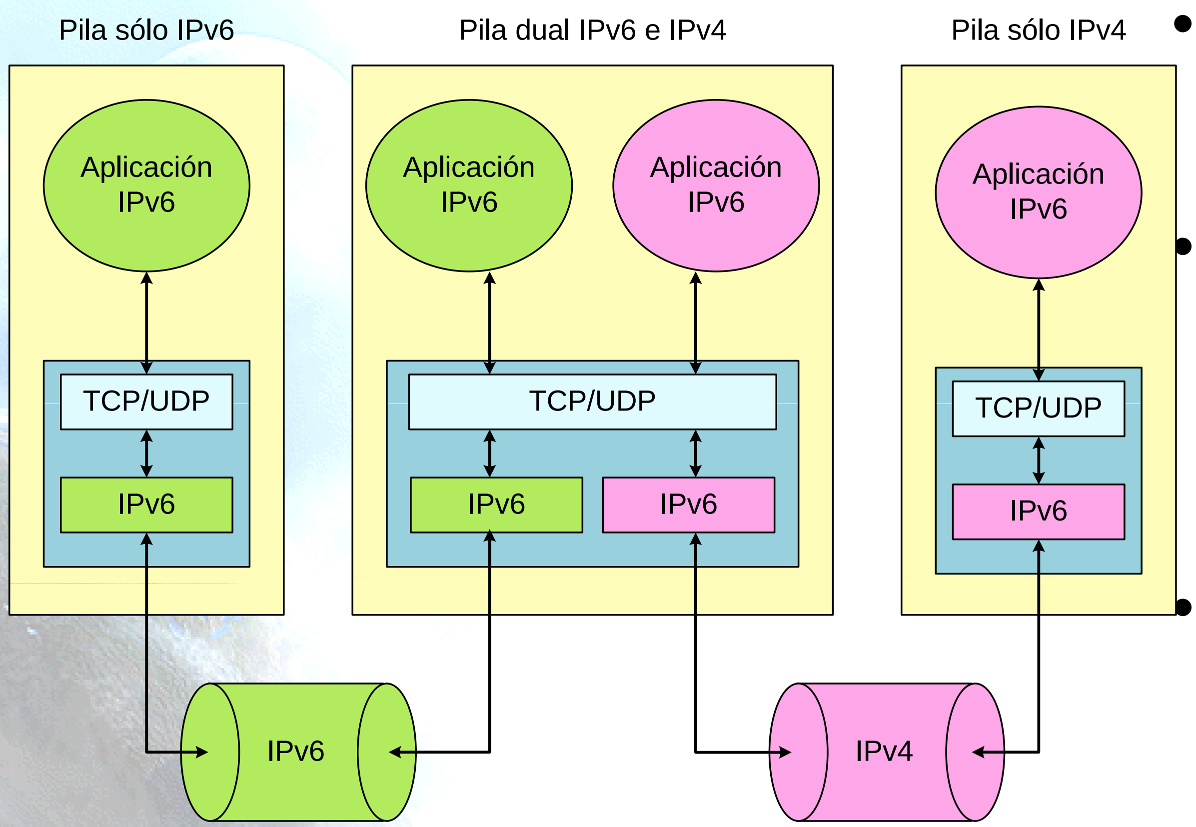
- IPv6 se ha diseñado para facilitar la transición y la coexistencia con IPv4.
- Coexistirán durante décadas -> No hay un “día D”
- Se han identificado e implementado un amplio abanico de técnicas, agrupadas básicamente dentro de tres categorías:
  1) **Doble-pila**, para permitir la coexistencia de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

4.2 Doble Pila

Doble Pila (1)

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

Doble pila (2)



Mécanismo basado en doble pila

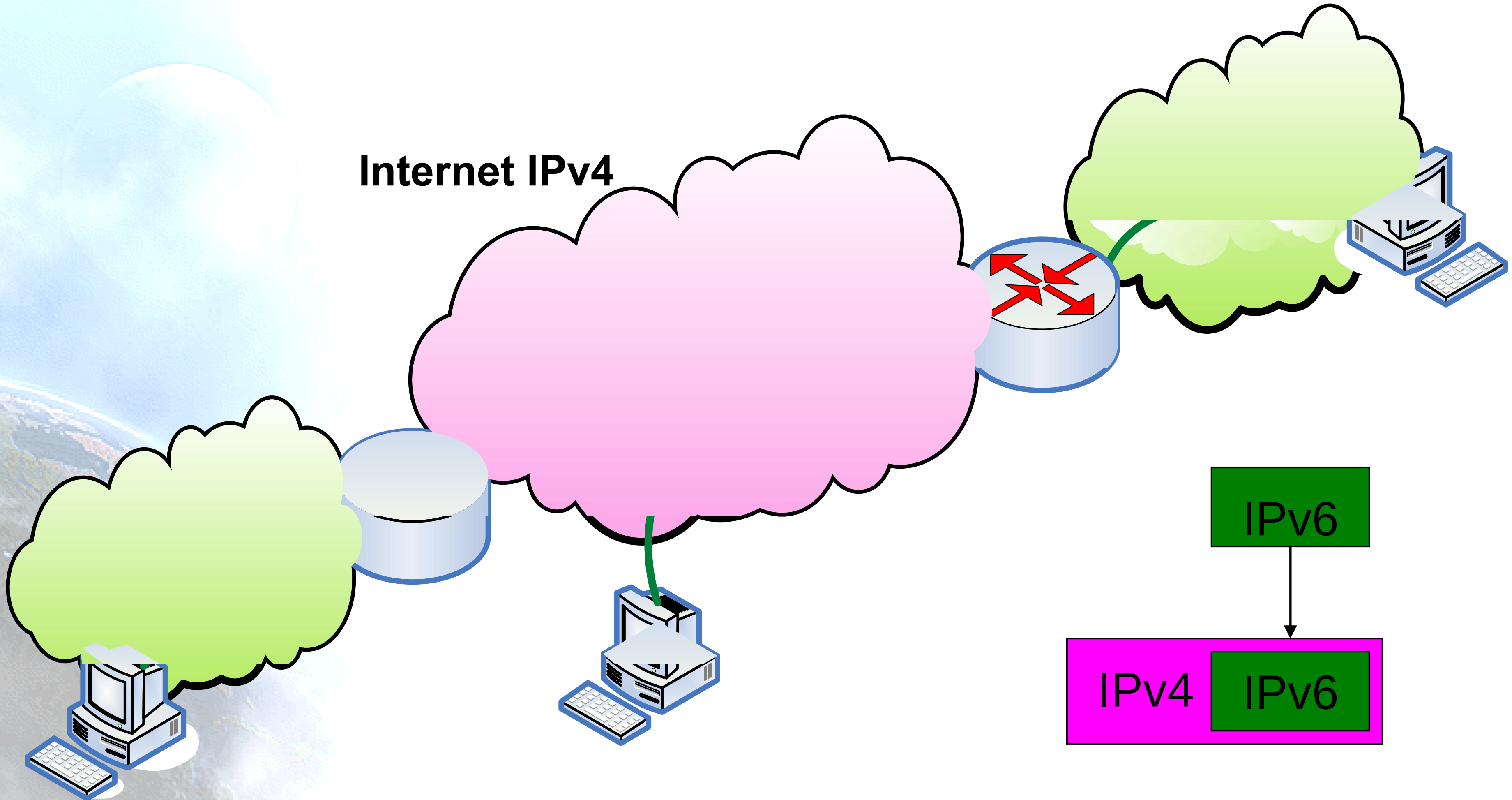
- Los nodos tienen implementadas las pilas IPv4 e IPv6
- Comunicaciones con nodos solo IPv6 ==> Pila IPv6, asumiendo soporte IPv6 en la red
- Comunicaciones con nodos solo IPv4 ==> Pila IPv4

4.3 Túneles

Túneles para Atravesar Routers que no Reenvían IPv6

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

Túneles IPv6 en IPv4 (6in4) (1)



Mécanismo basado en túneles

Túneles 6in4 (2)

- Existen diversas formas de encapsular los paquetes IPv6:

	IPv6	IPv6
IPv6	GRE	UDP
IPv4	IPv4	IPv4

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

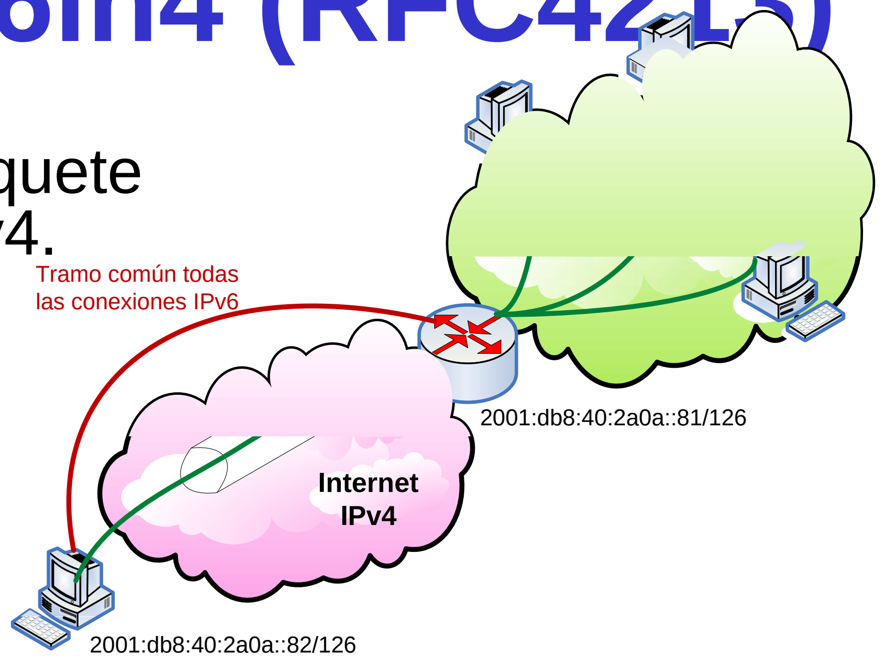
Túneles 6in4 (3)

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

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

Detalles Túneles 6in4 (RFC4213)

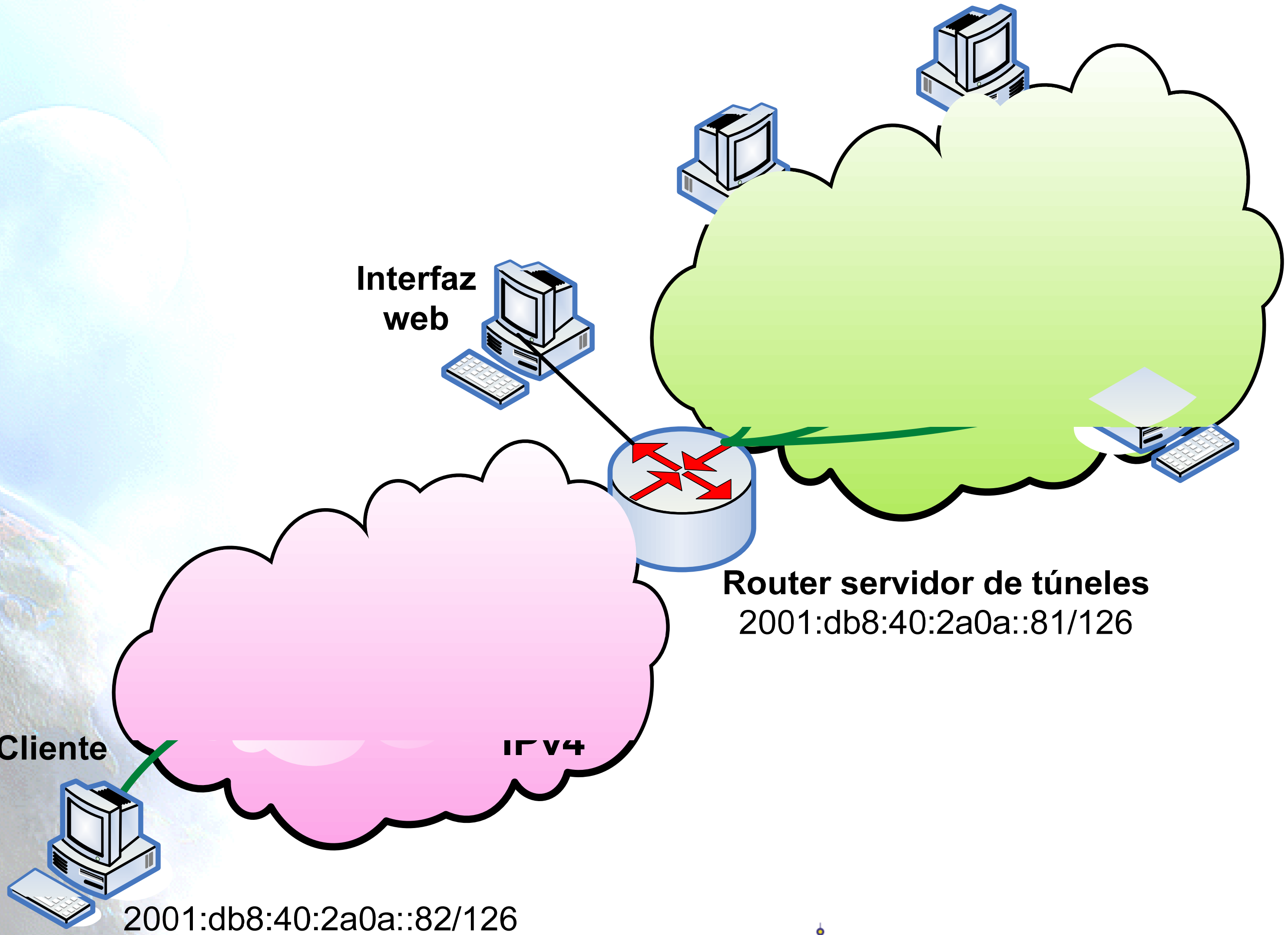
- Encapsula directamente el paquete IPv6 dentro de un paquete IPv4.
- Se suele hacer entre
  - nodo final ==> router
  - router ==> router



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

4.4 Tunnel Broker

Tunnel Broker (RFC3053) (1)



Tunnel Broker (RFC3053) (2)

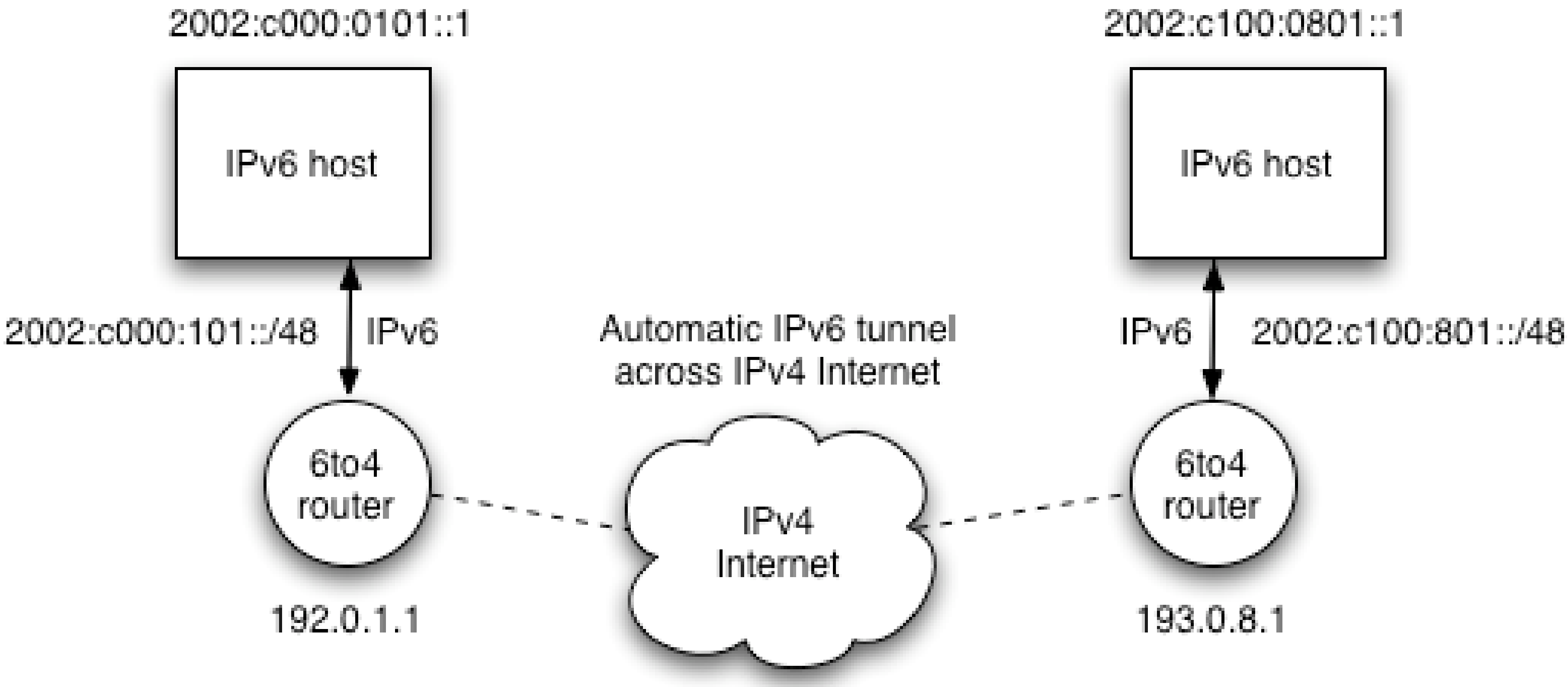
- Los túneles 6in4 requieren la configuración manual de los equipos involucrados en el túnel
- Para facilitar la asignación de direcciones y creación de túneles IPv6, se ha desarrollado el concepto de Tunnel Broker (TB).
  - Es un intermediario al que el usuario final se conecta, normalmente con un interfaz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

4.5 6to4

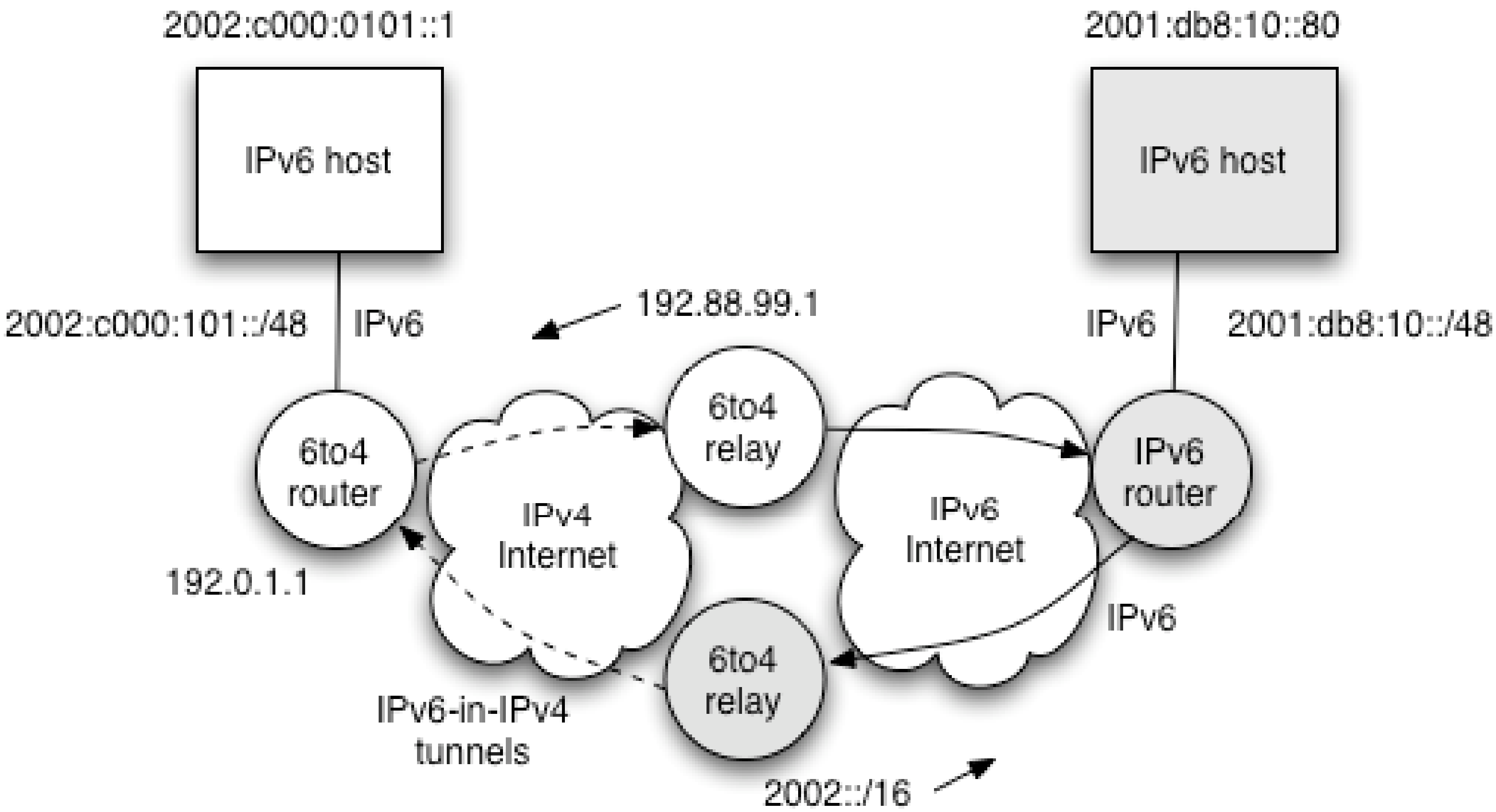
Túneles 6to4 (1)

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

Túneles 6to4 (2)



Túneles 6to4 (3)



4.6 6RD

6RD: Un refinamiento de 6to4

- RFC 5969: IPv6 Rapid Deployment on IPv4 infrastructures (August 2010)
  - 6RD utiliza IPv4 para proporcionar acceso a Internet IPv6 e IPv4 con calidad de producción a los sitios de los usuarios
- Implementado por FREE (ISP Frances)
  - En un plazo de 5 semanas el servicio estaba disponible
- Cambios a 6to4:
  - Formato dirección (de nuevo) => esfuerzo implementación
  - Usa prefijo IPv6 “normal” (2000::/3), en vez de 2002::/16
  - Desde el punto de vista del usuario y de la Internet IPv6: se percibe como IPv6 nativo
  - Relay (o gateway) se encuentra solamente dentro del backbone del ISP, en el borde de la Internet IPv6
  - Múltiples instancias son posibles: anunciadas mediante una dirección anycast
  - Bajo estricto control del ISP

6RD: Formato direcciones

ISP IPv6 relay prefix	Site IPv4 address	Interface ID
32	*32*	*64*

ISP IPv6 relay prefix	Site IPv4 address	SN	Interface ID
32-n	*32*	*n*	*64*

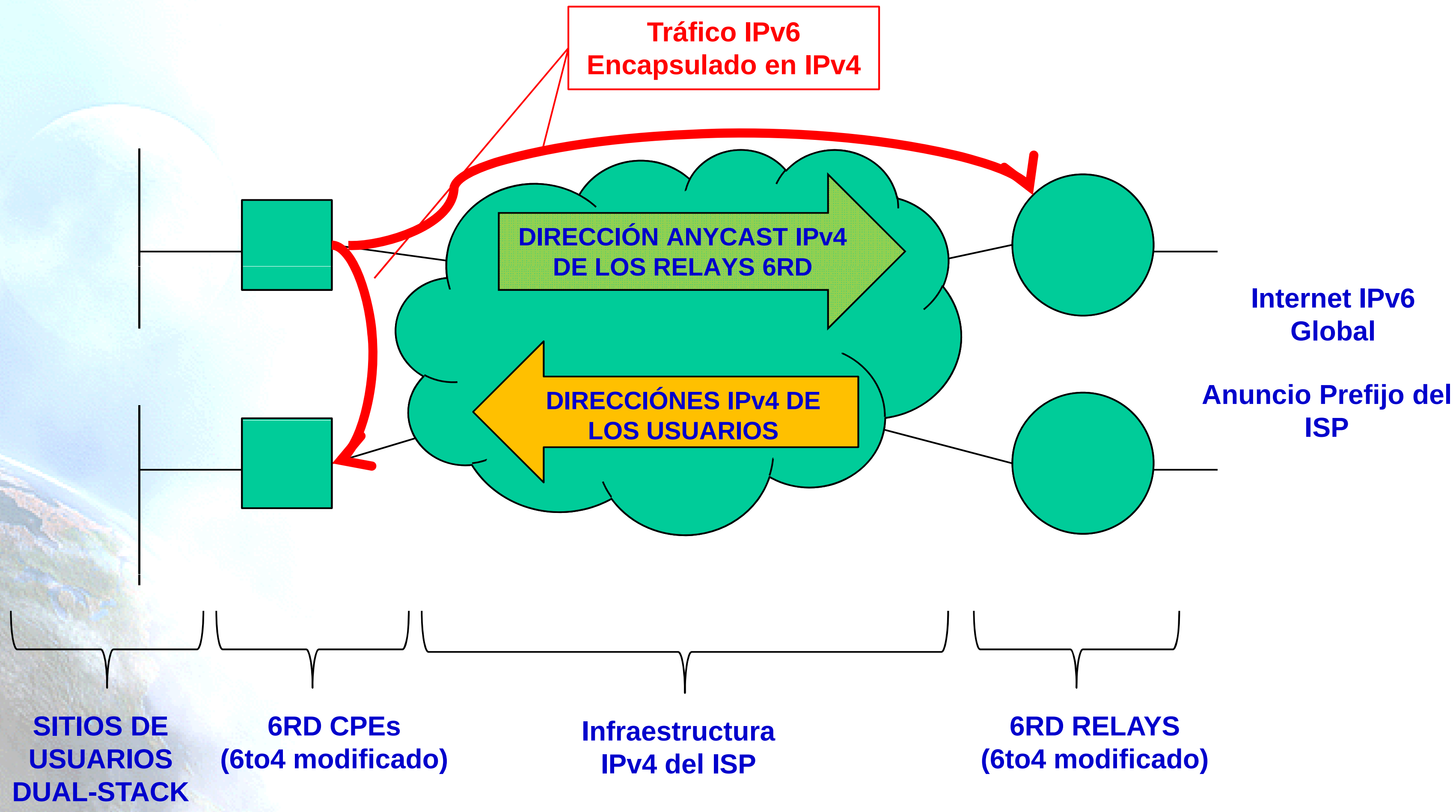
6RD: Pros & Cons

- Pros
  - Parece fácil de implementar y desplegar si los dispositivos de red están "bajo control" (CPEs, …)
  - Soluciona todos (?) los problemas de 6to4
    - seguridad, routing asimétrico, …
    - Relay (o gateway) en la red del ISP bajo su control
  - Transparente para el cliente
    - Configuración automática del CPE
  - Funciona con direcciones IPv4 públicas y privadas
    - Asignadas al cliente
- Cons
  - Necesario cambiar software de todos los CPEs
    - Actualmente solo hay un par de ellos
  - Añade una nueva "caja": 6RD relay/gateway
    - Hasta que otros fabricantes de routers soporten 6RD (Cisco ya lo hace)

6RD: Arquitectura

- **Sitios de Usuario (Dual-Stack):**
  – Asignado prefijo RD IPv6 => LAN(s) IPv6 Nativo
  – (+IPv4)
- **CPE (= 6RD CE = 6RD router):**
  – Proporciona conectividad IPv6 nativo (lado cliente)
  – Ejecuta código 6RD (6to4 modificado) y
  – Tiene una interfaz multipunto virtual 6RD para soportar en en/desencapsulado de IPv6 en IPv4
  – Recibe un prefijo IPv6 6RD de un dispositivo del SP
  – y una dirección IPv4 (lado WAN = red del ISP)
- **6RD relay (= border relay)**
  – Gateway entre infraestructura IPv4 del ISP e Internet IPv6
  – Anuncia una dirección IPv4 a los CPEs
    - Dirección anycast puede ser usada para redundancia

6RD: Escenario de Implementación

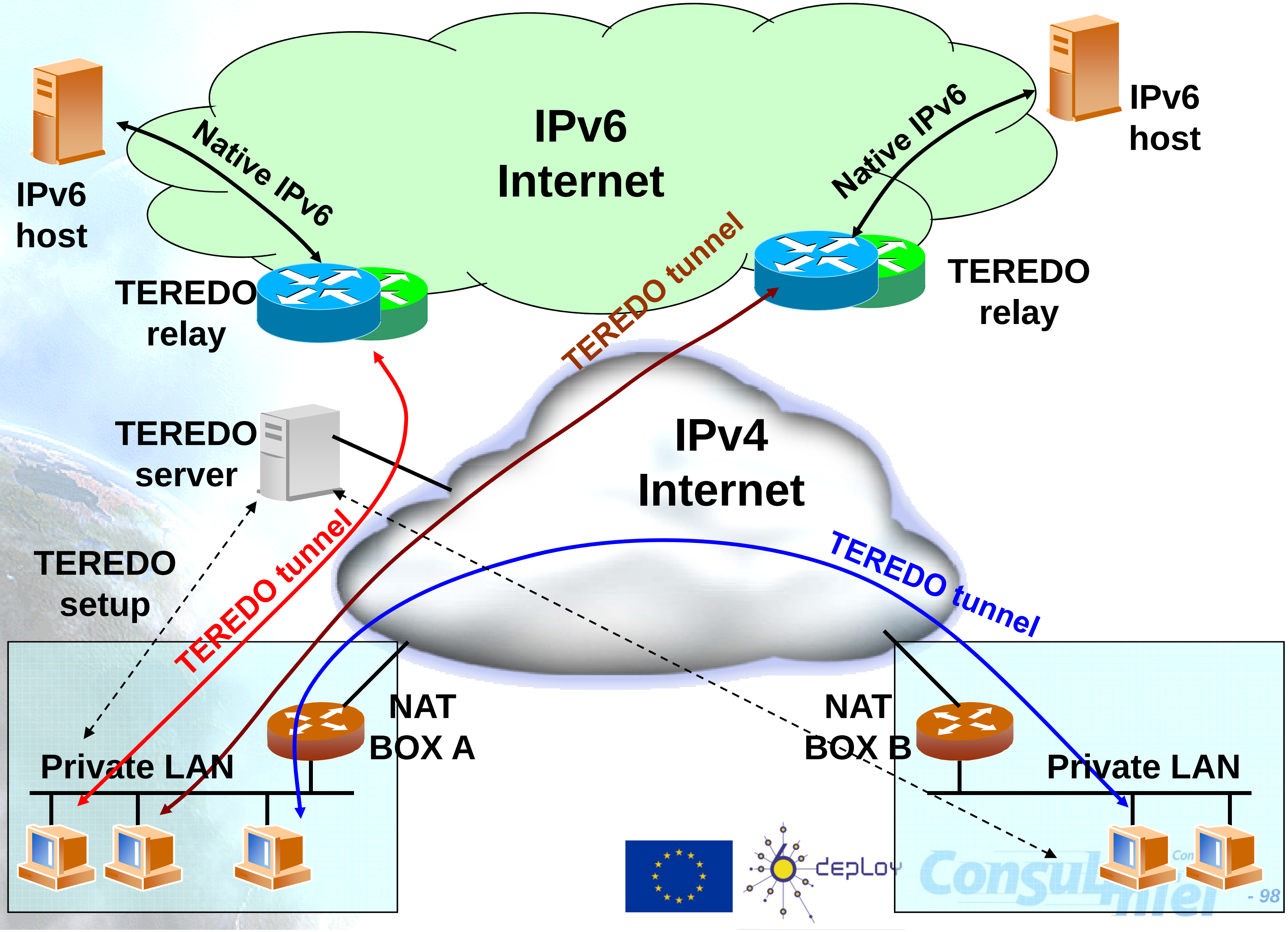


4.7 Teredo

Teredo (RFC4380) (1)

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

Teredo (RFC4380) (2)



4.8 Softwires

Softwires

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

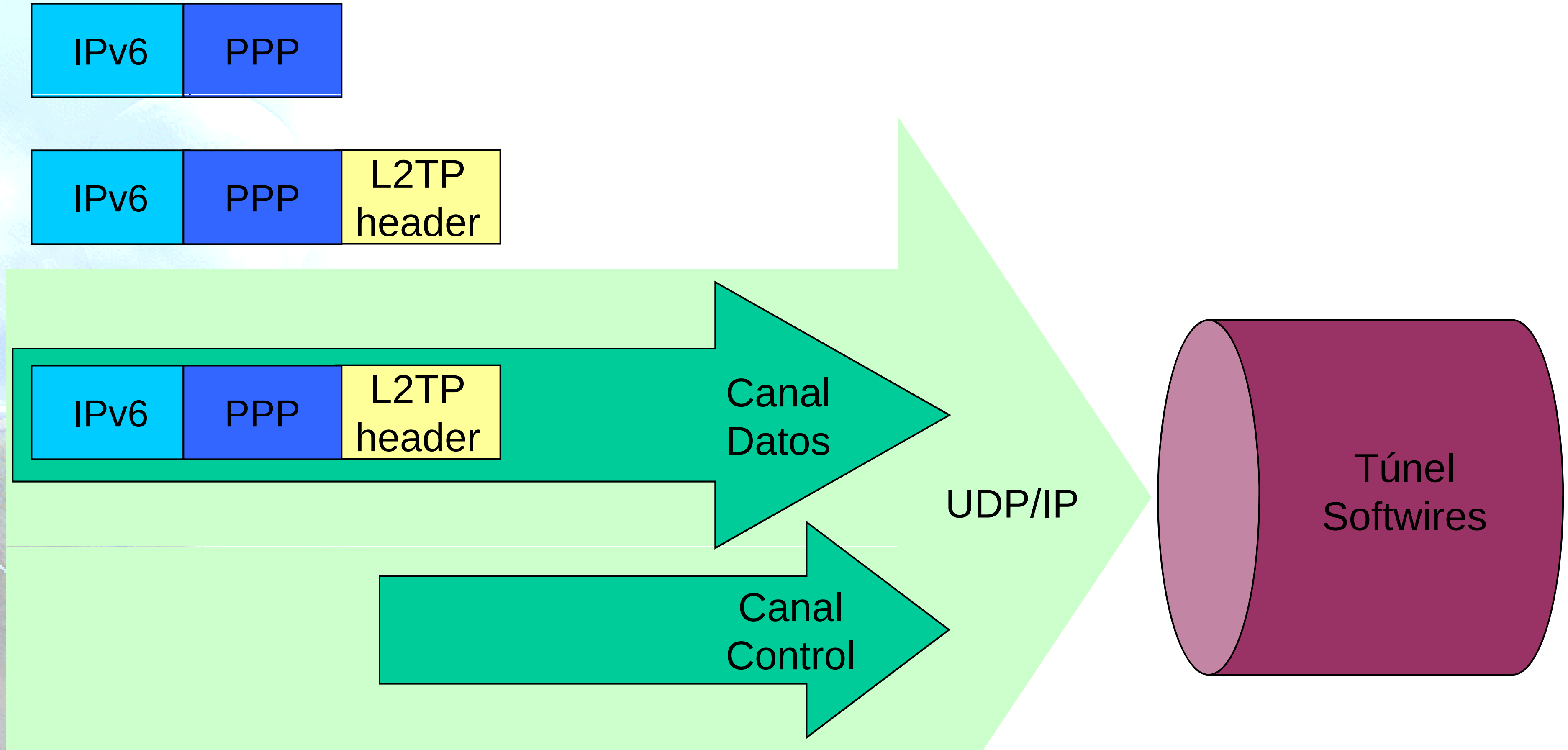
Encapsulamiento de Softwires basado en L2TPv2

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

Túnel IPv6-en-IPv4		**Túnel IPv4-en-IPv6**	**Túnel IPv6-en-IPv6**	**Túnel IPv4-en-IPv4**
	IPv6			
IPv6	PPP	IPv4	IPv6	IPv4
PPP	Cabe. Soft.	PPP	PPP	PPP
Cabe. Soft.	UDP*	Cabe. Soft.	Cabe. Soft.	Cabe. Soft.
IPv4	IPv4	IPv6	IPv6	IPv4

*** Opcional**

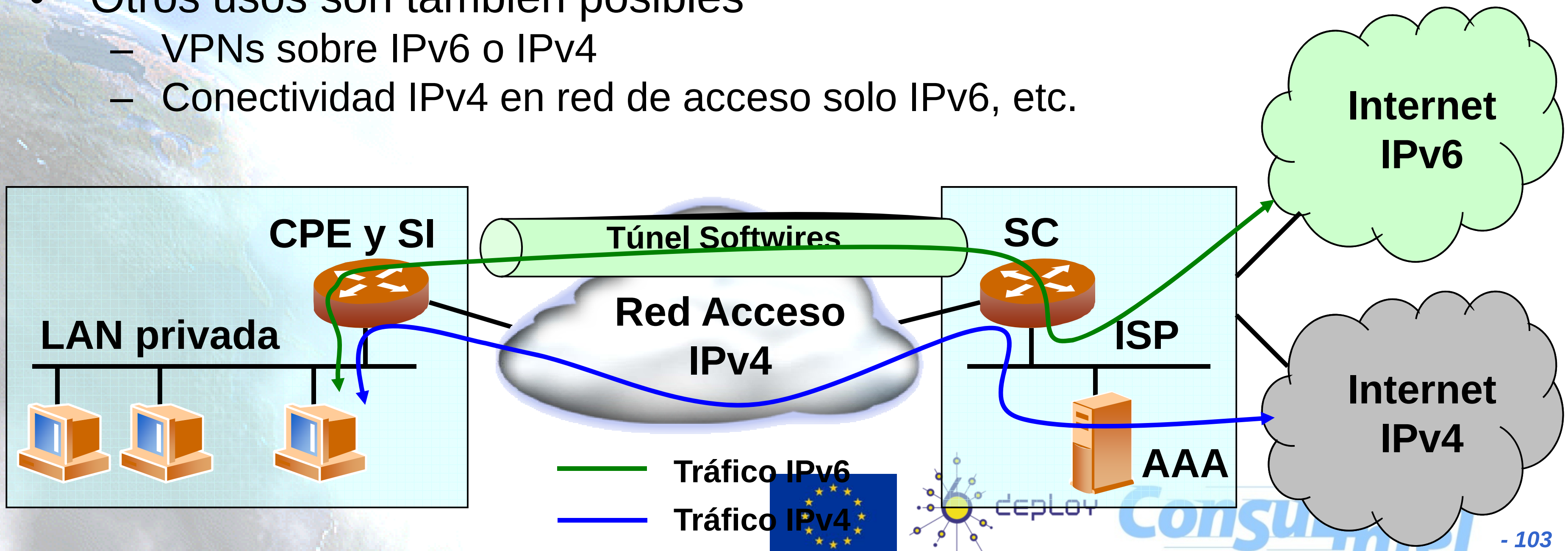
Softwires basado en L2TPv2



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

Ejemplo de uso de Softwires

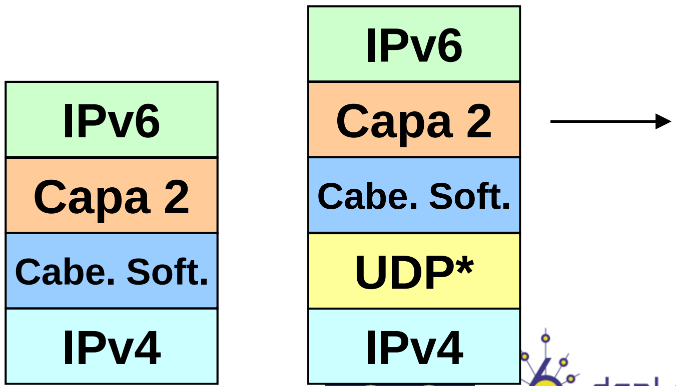
- Un uso típico previsible de Softwires es la provisión de conectividad IPv6 a usuarios domésticos a través de una red de acceso solo-IPv4
  - El SC está instalado en la red del ISP (DSLAM, Router de agregación u otro dispositivo)
  - El SI está instalado en la red del usuario
    - CPE típicamente.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



- HDLC
- PPP
- FR
- ATM
- Ethernet
- MPLS

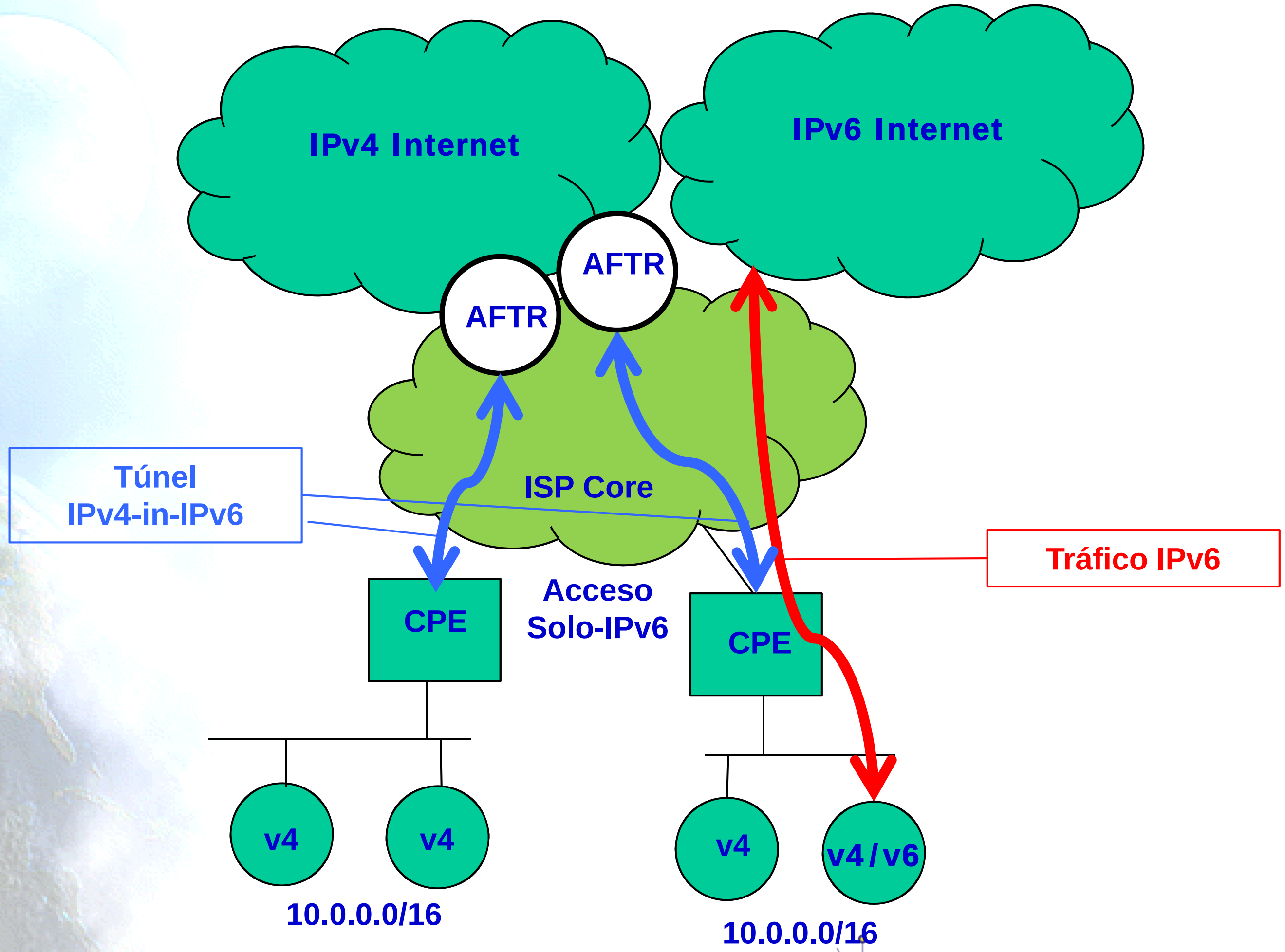
* Opcional

4.9 DS-Lite

Dual Stack Lite (1)

- Trata de solucionar le problema del agotamiento de IPv4
- Comparte (las mismas) direcciones IPv4 entre usuarios combinando:
  - Tuneling
  - NAT
- No hay necesidad de varios niveles de NAT.
- Dos elementos:
  - DS-Lite Basic Bridging BroadBand (B4)
  - DS-Lite Address Family Transition Router (AFTR) (También llamado CGN (Carrier Grade NAT) o LSN (Large Scale NAT))

Dual Stack Lite (2)

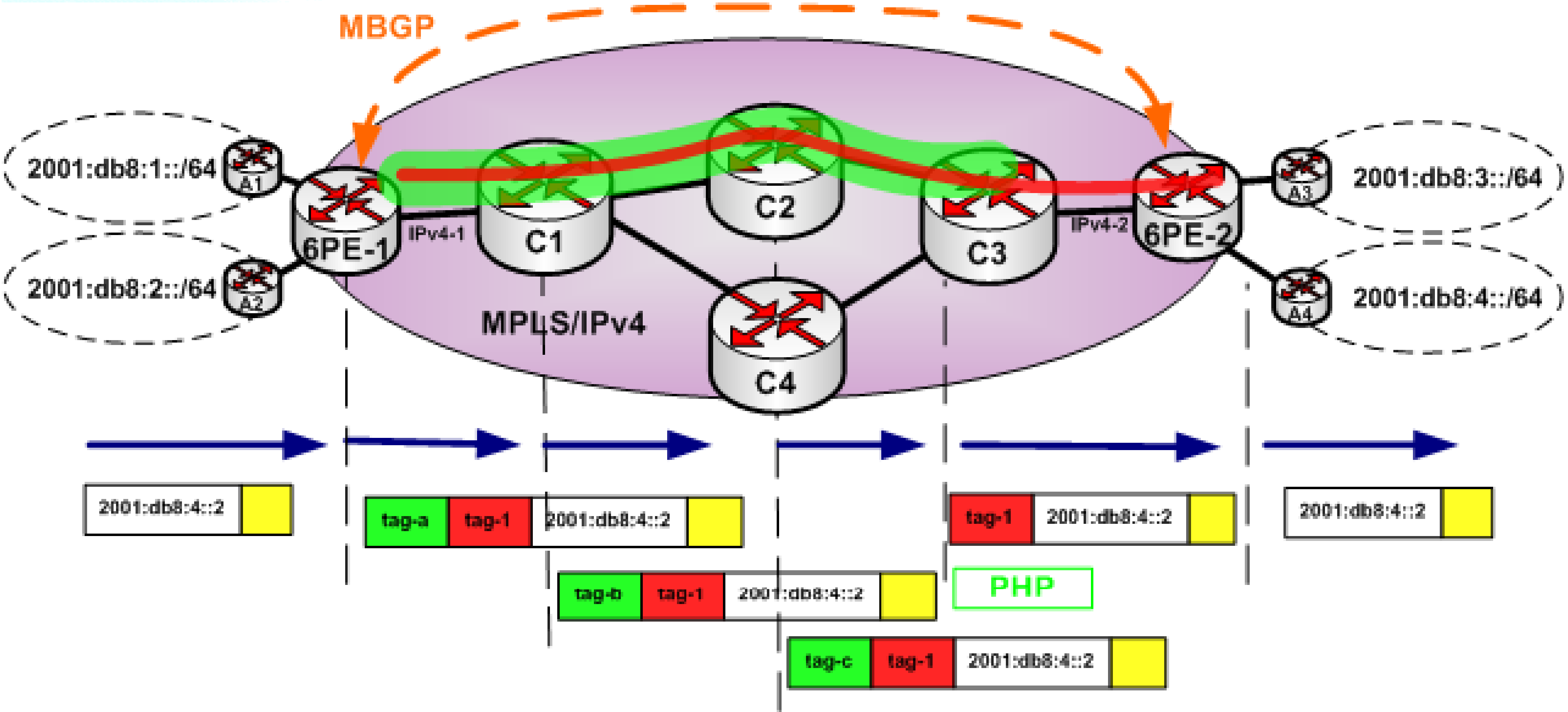


4.10 6PE

IPv6 con 6PE (1)

- Los dominios IPv6 remotos se comunican a través de un Core de MPLS IPv4
  - Usando MPLS label switched paths (LSPs)
  - Aprovechando en el PE las extensiones Multiprotocol Border Gateway Protocol (MBGP) sobre IPv4 para intercambiar información de ruteo IPv6
- Los PEs tienen pila doble IPv4/IPv6
  - Usan direcciones IPv6 mapeadas a IPv4 para el conocer la "alcanzabilidad" de los prefijos IPv6

IPv6 con 6PE (2)



6PE-1 aprende de 6PE-2 a través de MBGP lo siguiente:

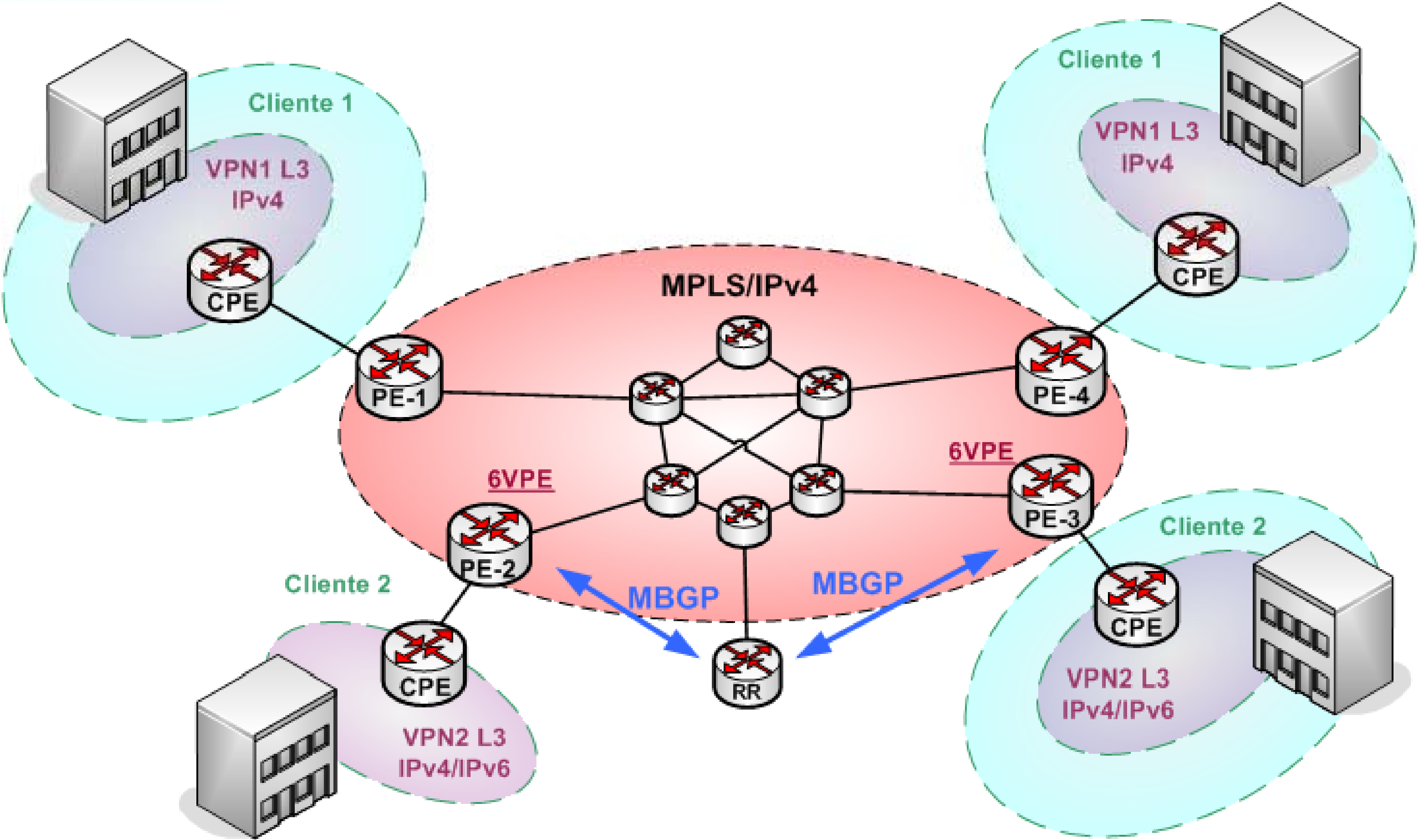
Prefijo	Next-Hop	Tag-IPv6
2001:db8:3::/64	::FFFF:IPv4-2	tag-2
2001:db8:4::/64	::FFFF:IPv4-2	tag-1

4.11 6VPE

IPv6 con 6VPE (1)

- 6PE permite una única tabla de routing para todos los dispositivos
- IPv4: VPN de Nivel 3 -> Aplicación muy usada en redes MPLS
- 6VPE: IPv6 VPN Provider Edge Router -> Equivalente a IPv4 VPN Provide Edge Router añadiendo soporte IPv4
- 6VPE: Una tabla de routing separada para todos los routers pertenecientes a la VPN IPv6
- 6VPE: Soporta fácilmente IPv4 y/o IPv6
- MBGP VPN IPv6 Address Family

IPv6 con 6VPE (2)

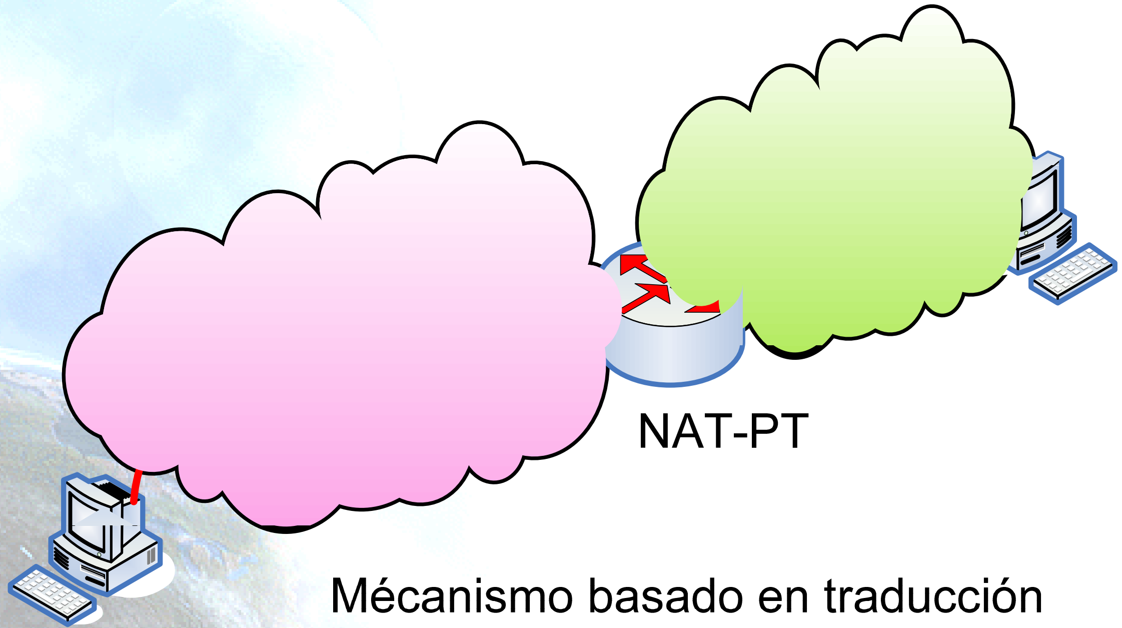


4.12 Traducción

Traducción

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

Traducción IPv4/IPv6 (obsoleto)



Mécanismo basado en traducción

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

4.13 NAT64

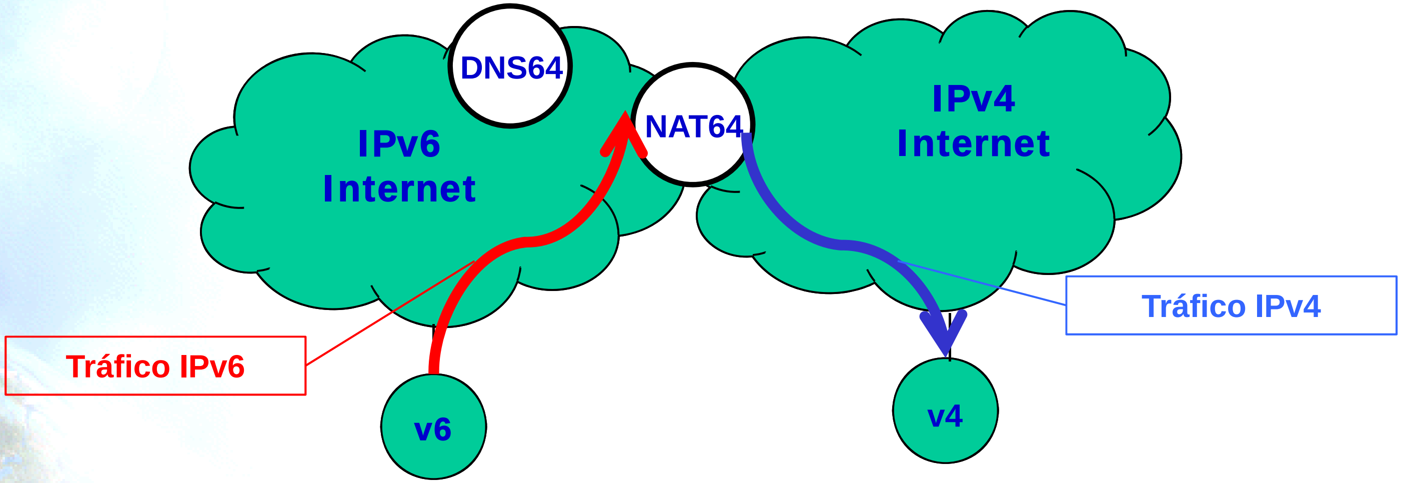
NAT64 (1)

- Cuando los ISPs solo proporcionen conectividad IPv6 o los dispositivos sean solo-IPv6 (celulares)
- Pero, siga habiendo algunos dispositivos solo-IPv4 en Internet
- La idea es similar al NAT-PT, pero funcionando mejor
- Elemento opcional, pero desacoplado, DNS64

NAT64 (2)

- Stateful NAT64 es un mecanismo para traducir paquetes IPv6 a IPv4 y vice-versa
  - La traducción se lleva a cabo en las cabeceras de los paquetes siguiendo el Algoritomo de Traducción IP/ICMP
  - La dirección IPv4 de los hosts IPv4 se traducen algorítmicamente a/desde direcciones IPv6usando un algoritmo específico
  - La especificación actual sólo define como NAT64 traduce paquetes unicast con tráfico TCP, UDP e ICMP.
  - DNS64 es un mecanismo para sintetizar RRs tipo AAAA a partir de RRs tipo A. Las direcciones IPv6 contenidas en el AAAA sintetizado se genera mediante un algoritmo a partir de la dirección IPv4 y el prefijo IPv6 asignado al dispositivo NAT64
- NAT64 permite a múltiples nodos solo-IPv6 compartir una dirección IPv4para acceder a Internet.

NAT64 (3)


DNS64
IPv6
Internet
NAT64
IPv4
Internet
Tráfico IPv4
Tráfico IPv6
v6
v4

Preguntas?

Gracias!

ALICE2: http://alice2.redclara.net/

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

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