

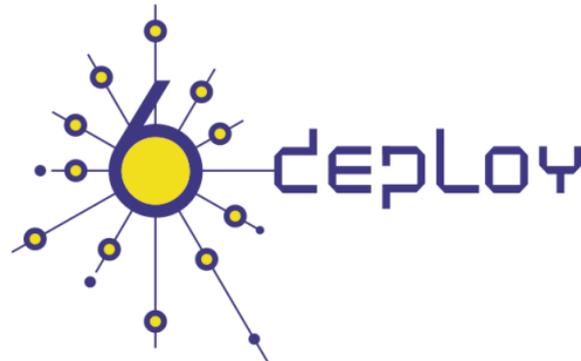
WALC2012

Track 2: Despliegue de IPv6

Día - 3

Panamá

15 -19 Octubre 2012



Alvaro Vives (alvaro.vives@consulintel.es)



8. Mecanismos de Transición

8.1 Estrategias coexistencia IPv4-IPv6

8.2 Doble Pila

8.x Túneles

8.10 Traducción

8.11 NAT64

8.12 Seguridad



8.1 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.



Técnicas Transición/Coexistencia (2)

- La situación actual es que hay un peligro **real** de agotamiento de direcciones IPv4.
- Esto, añade un nuevo problema al que ya existía (implementar IPv6): pocas o nulas direcciones IPv4 públicas
- Hay que tener en cuenta que las herramientas utilizadas necesitan IPv4 públicas: NAT44, NAT444, etc.
- Los nuevos mecanismos de transición:
 1. Intentan solucionar el problema del agotamiento de direcciones IPv4
 2. Tienen en cuenta que cada ve habrá más redes **solo-IPv6**



8.2 Doble Pila

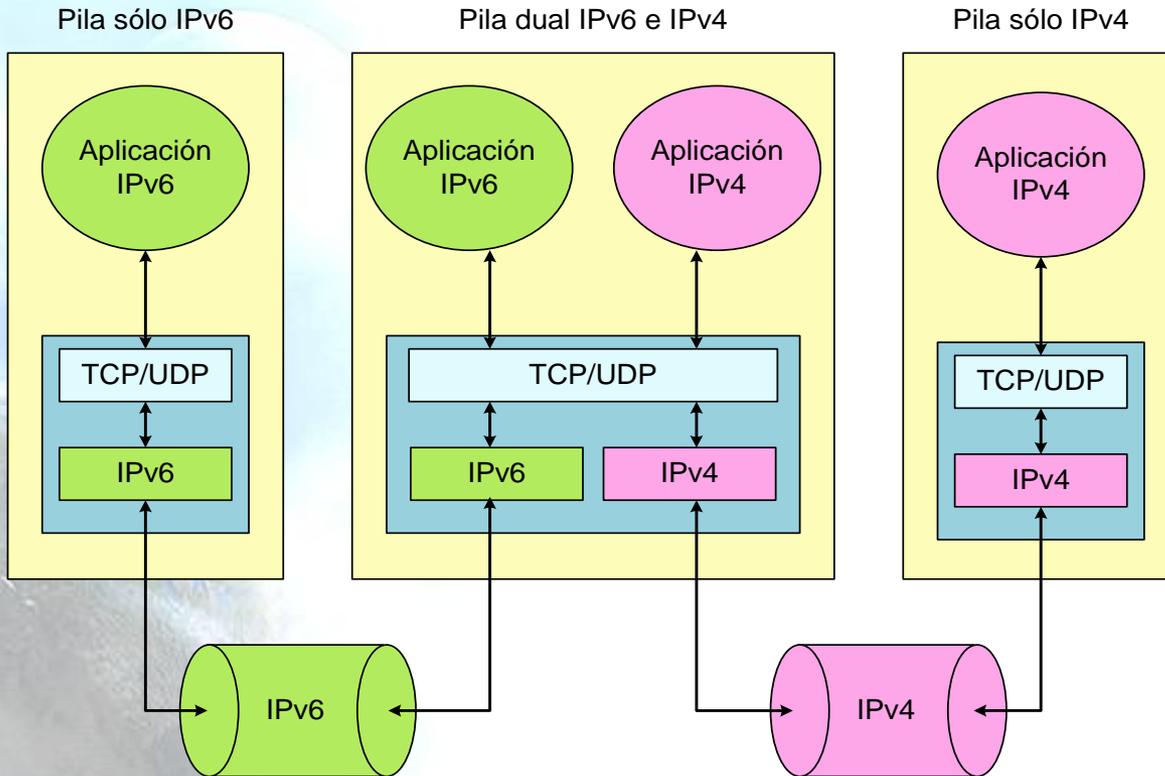


Doble Pila (1)

- 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



Happy-eyeballs (1)

- El ofrecer un servicio con doble pila puede traer problemas, mala experiencia del usuario
- A + AAAA -> el cliente elige cual usar, por defecto, se suele usar IPv6 primero
- Existen varios “tipos de IPv6”: nativo, encapsulado, traducido
- Se pueden dar escenarios en los que el usuario sufre mucho retardo al usar un “mal IPv6” o tener que pasar de IPv6 por defecto a IPv4
- Solución: aproximación **Happy-eyeballs** [RFC6555]
- Implementaciones: Google Chrome, Firefox 7, Mac OS Lion X



Happy-eyeballs (2)

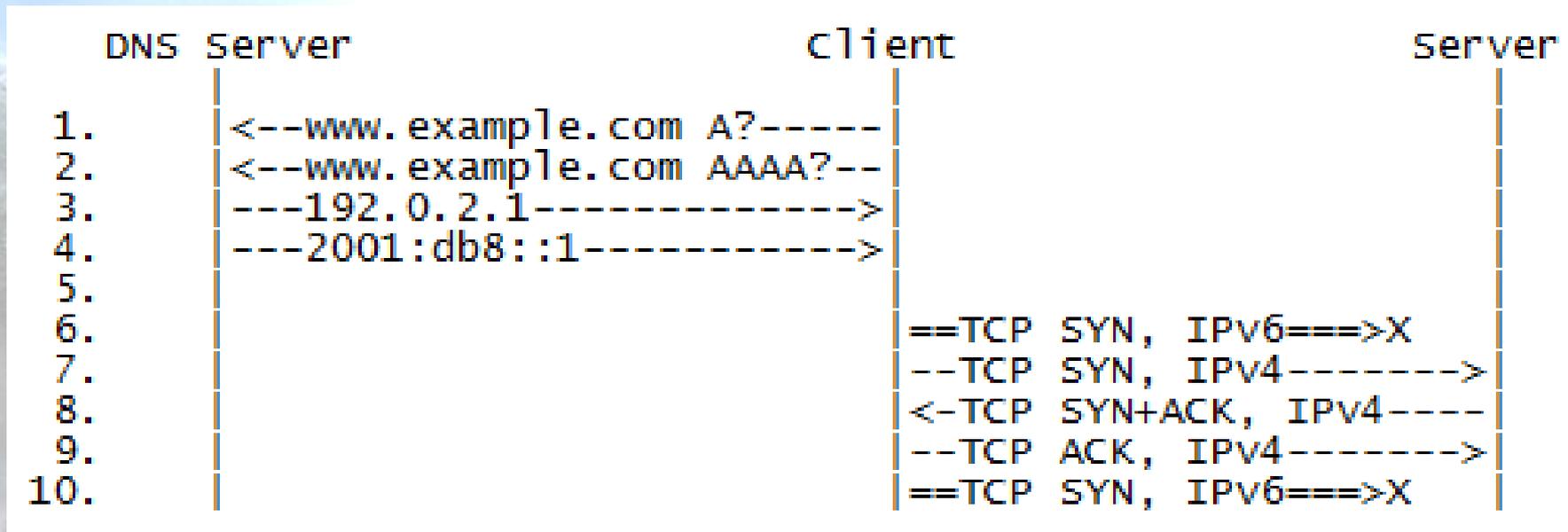
- Funcionamiento habitual:

	DNS Server	Client	Server
1.		<--www.example.com A?-----	
2.		<--www.example.com AAAA?--	
3.		---192.0.2.1----->	
4.		---2001:db8::1----->	
5.			
6.		==TCP SYN, IPV6===>X	
7.		==TCP SYN, IPV6===>X	
8.		==TCP SYN, IPV6===>X	
9.			
10.		--TCP SYN, IPV4----->	
11.		<-TCP SYN+ACK, IPV4----	
12.		--TCP ACK, IPV4----->	



Happy-eyeballs (3)

- Dos objetivos básicos: hacer que las conexiones de los usuarios sean más rápidas y no generar demasiada “basura” en la red
- Se “memoriza info sobre conexiones



8.3 Túneles

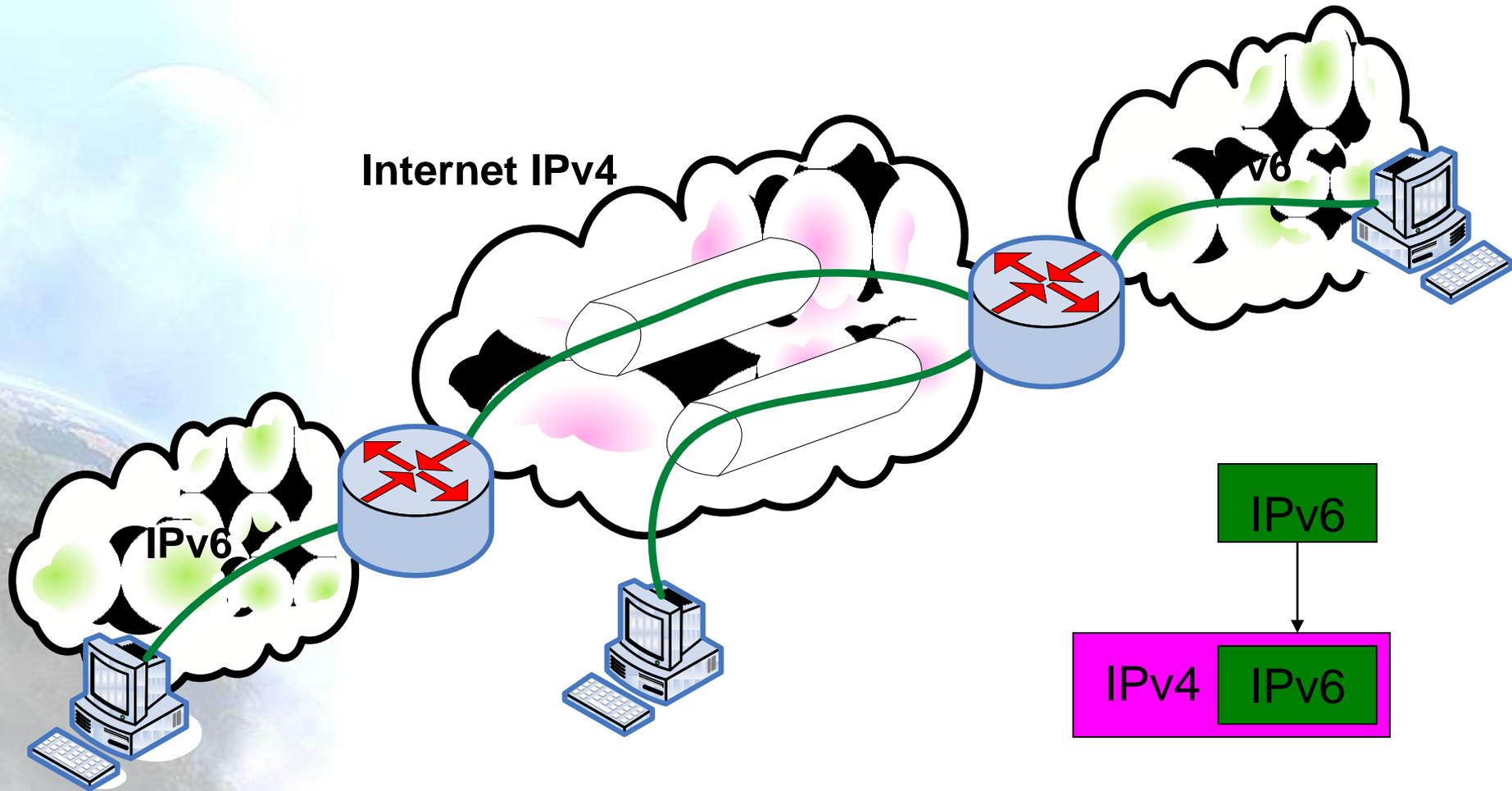


Túneles para Atravesar Routers que no Reenvían IPv6

- 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” (típicamente con interfaces web) -> 6in4
 - “6-over-4” (intra-domain, usando IPv4 multicast como LAN virtual)
 - “6-to-4” (inter-domain, usando la dirección IPv4 como el prefijo del sitio IPv6)
- Puede ser visto como:
 - IPv6 utilizando IPv4 como capa de enlace virtual link-layer, o
 - una VPN IPv6 sobre la Internet IPv4



Túneles IPv6 en IPv4 (6in4) (1)

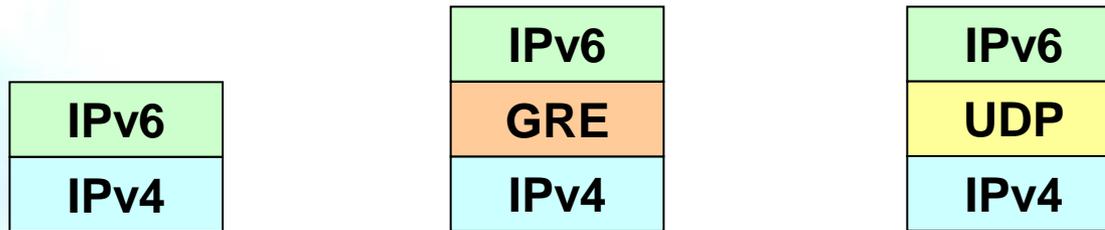


Mécanismo basado en túneles



Túneles 6in4 (2)

- Existen diversas formas de encapsular los paquetes IPv6:



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



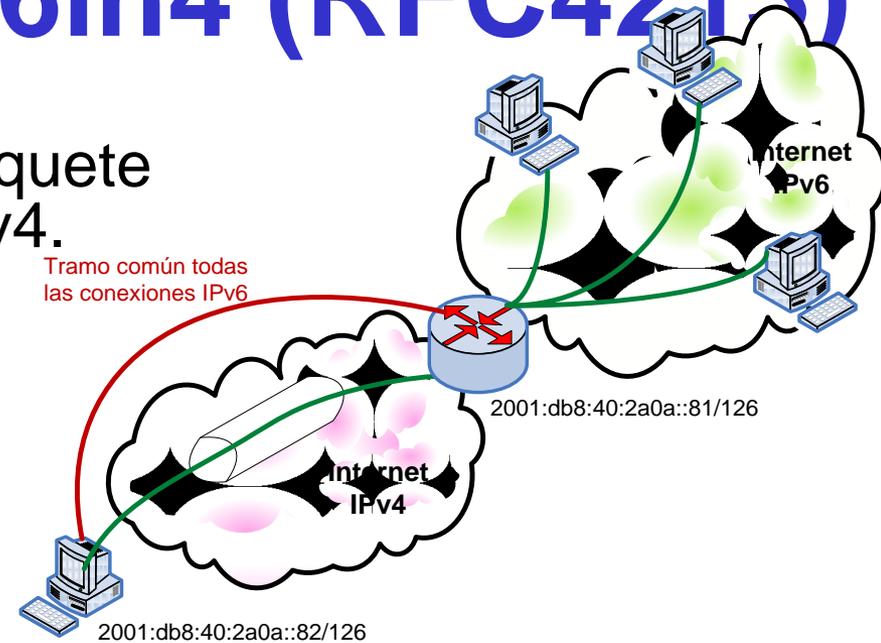
Túneles 6in4 (3)

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



Detalles Túneles 6in4 (RFC4213)

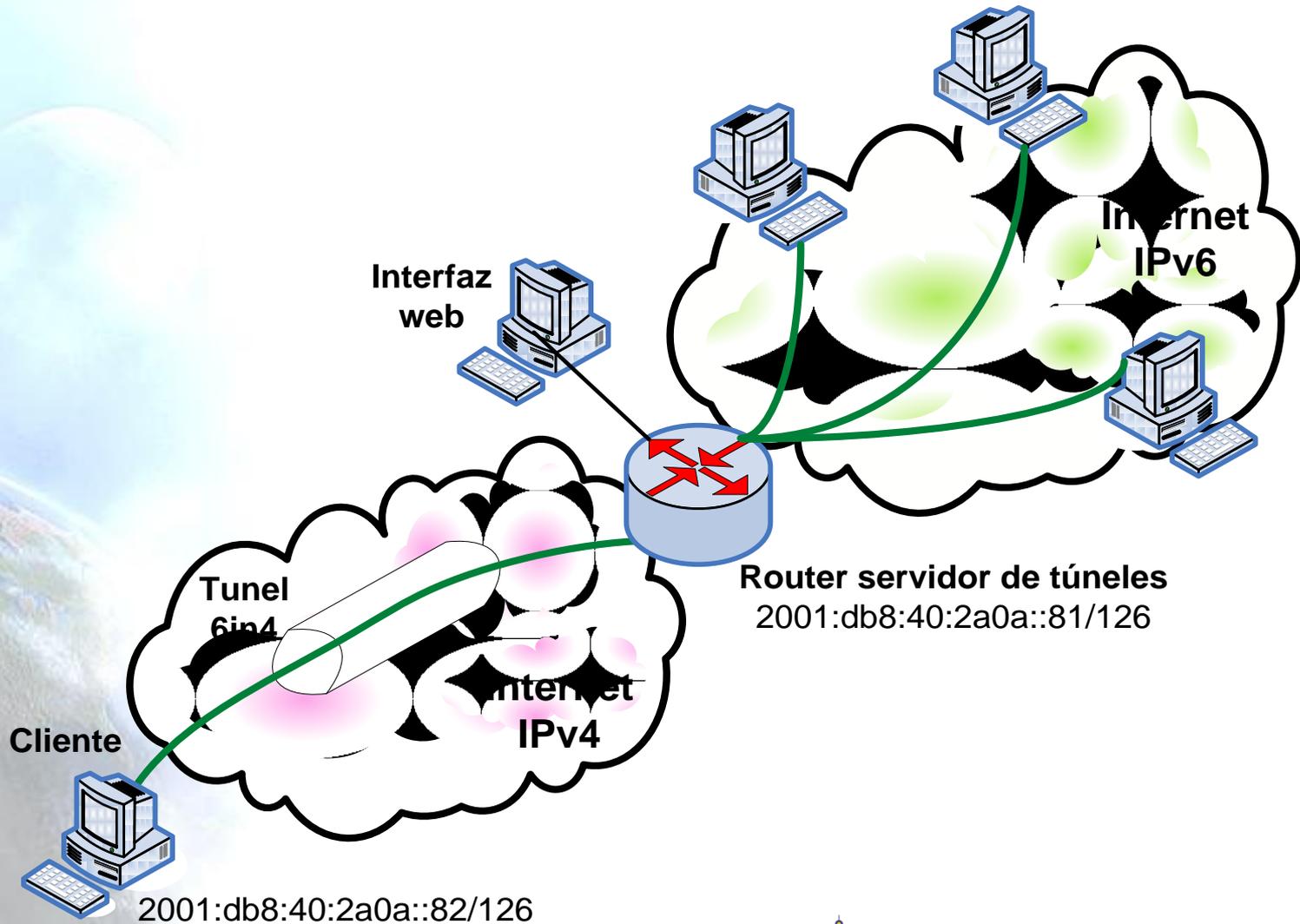
- Encapsula directamente el paquete IPv6 dentro de un paquete IPv4.
- Se suele hacer entre
 - nodo final ==> router
 - router ==> router
- Aunque también es posible para
 - nodo final ==> nodo final
- El túnel se considera como un enlace punto-a-punto desde el punto de vista de IPv6.
 - Solo un salto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



8.4 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 está 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.



8.5 6to4

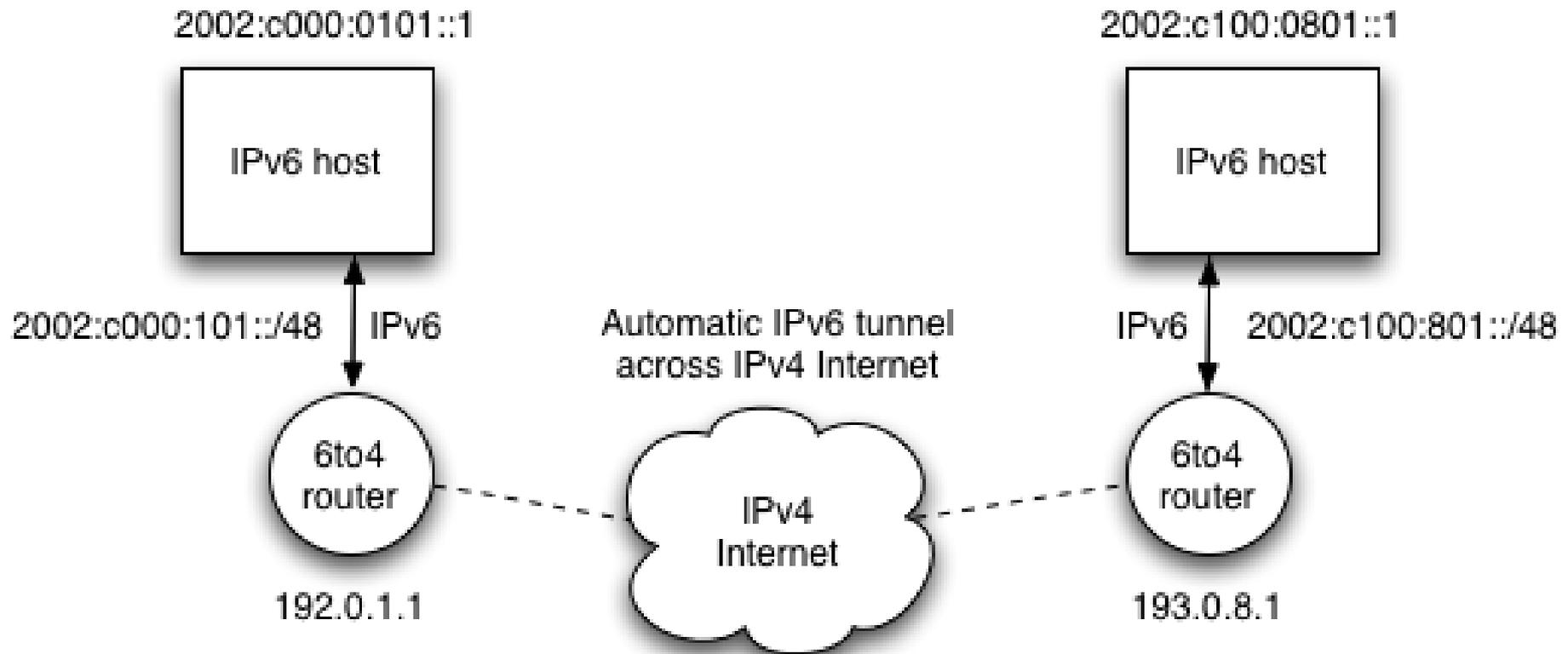


Túneles 6to4 (1)

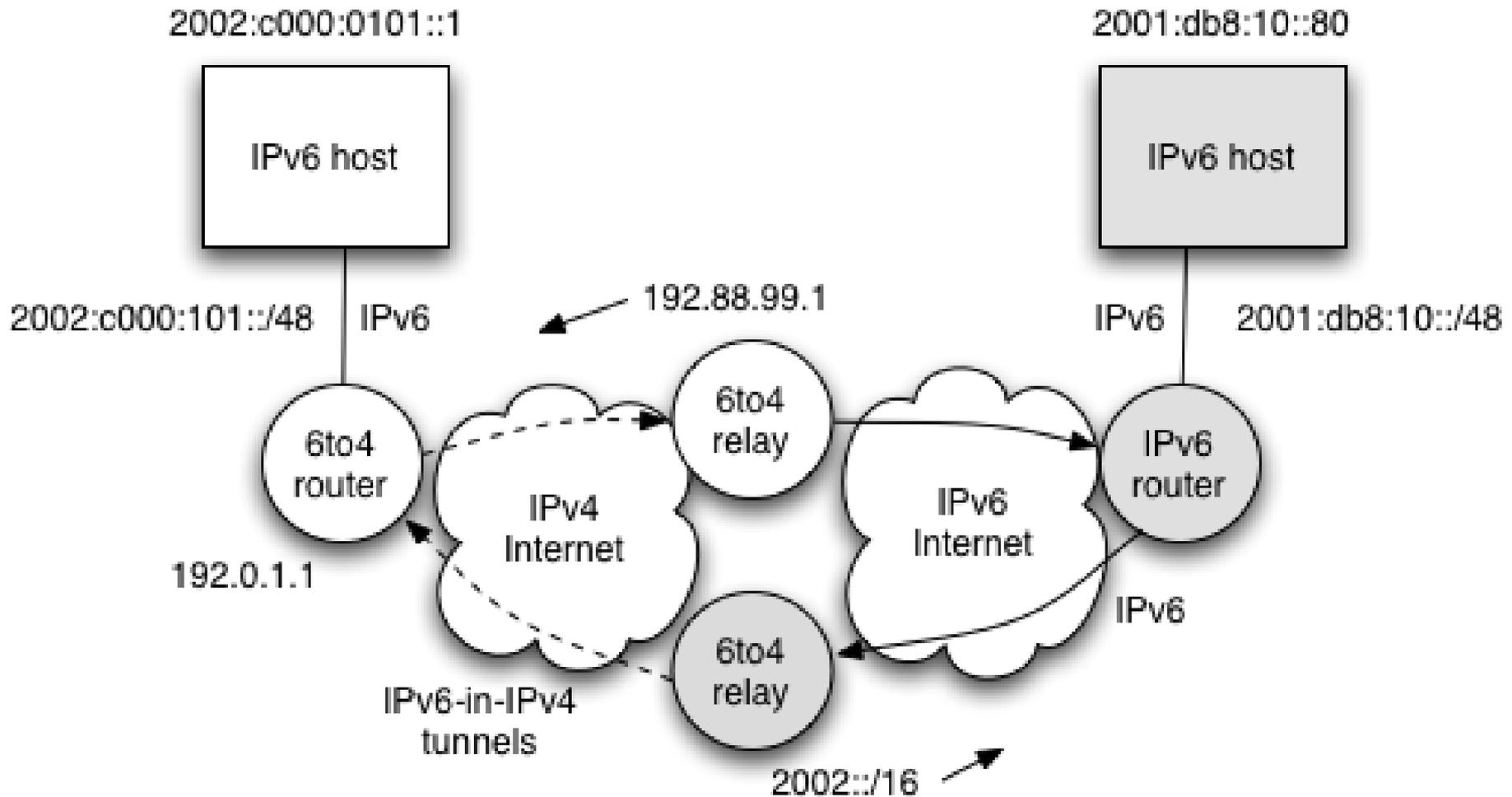
- Definido en RFC3056
- Se utiliza un “truco” para proporcionar direcciones 6to4.
 - Prefijo 6to4: 2002::/16
 - Se usa la IPv4 pública (p.e. 192.0.1.1) para siguientes 32 bits
 - Se obtiene así un prefijo /48 (p.e. 2002:C000:0101::/48)
- Cuando un router 6to4 ve un paquete hacia el prefijo **2002::/16** 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)



8.6 6RD

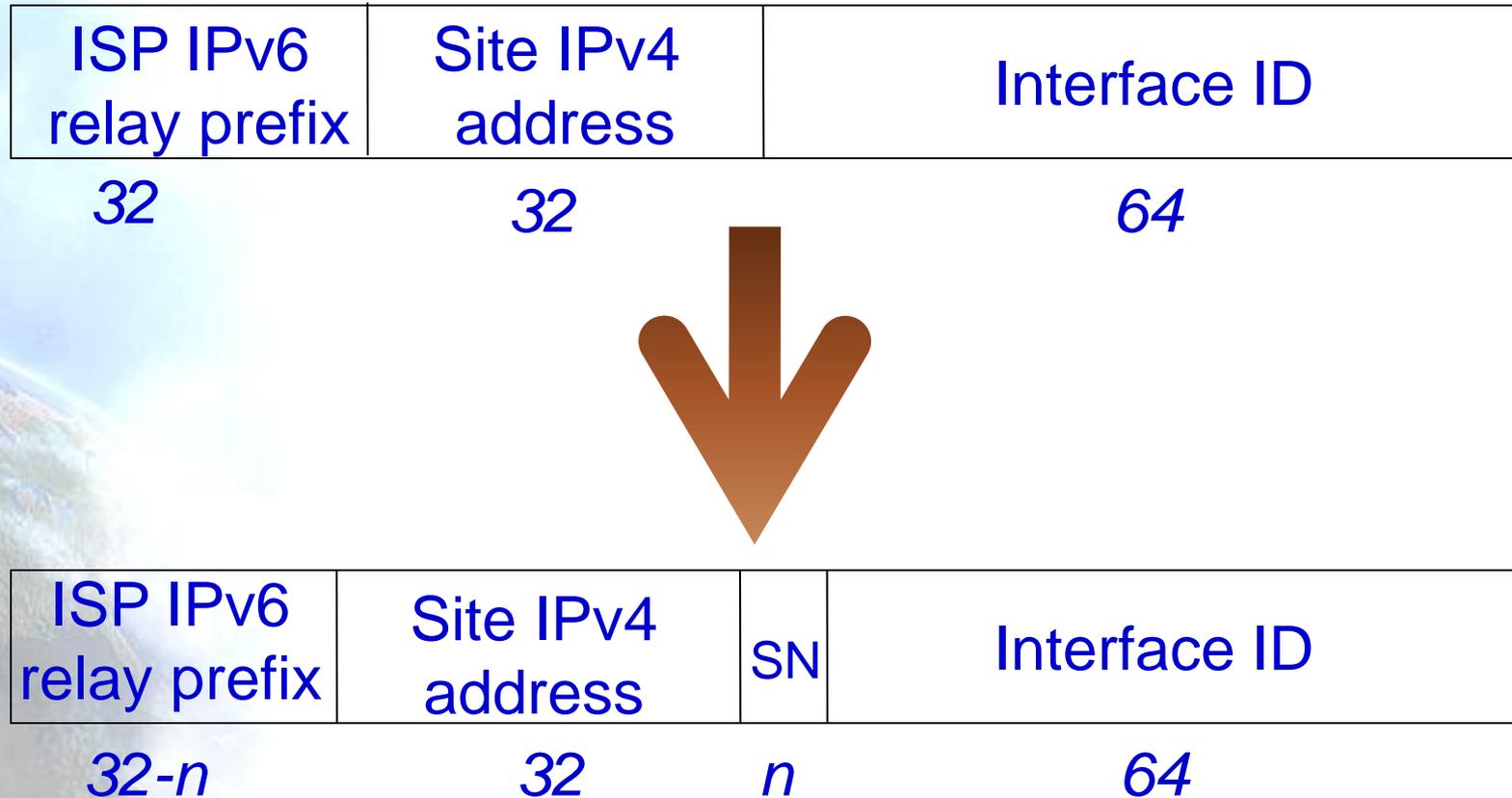


6RD: Un refinamiento de 6to4

- 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



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)

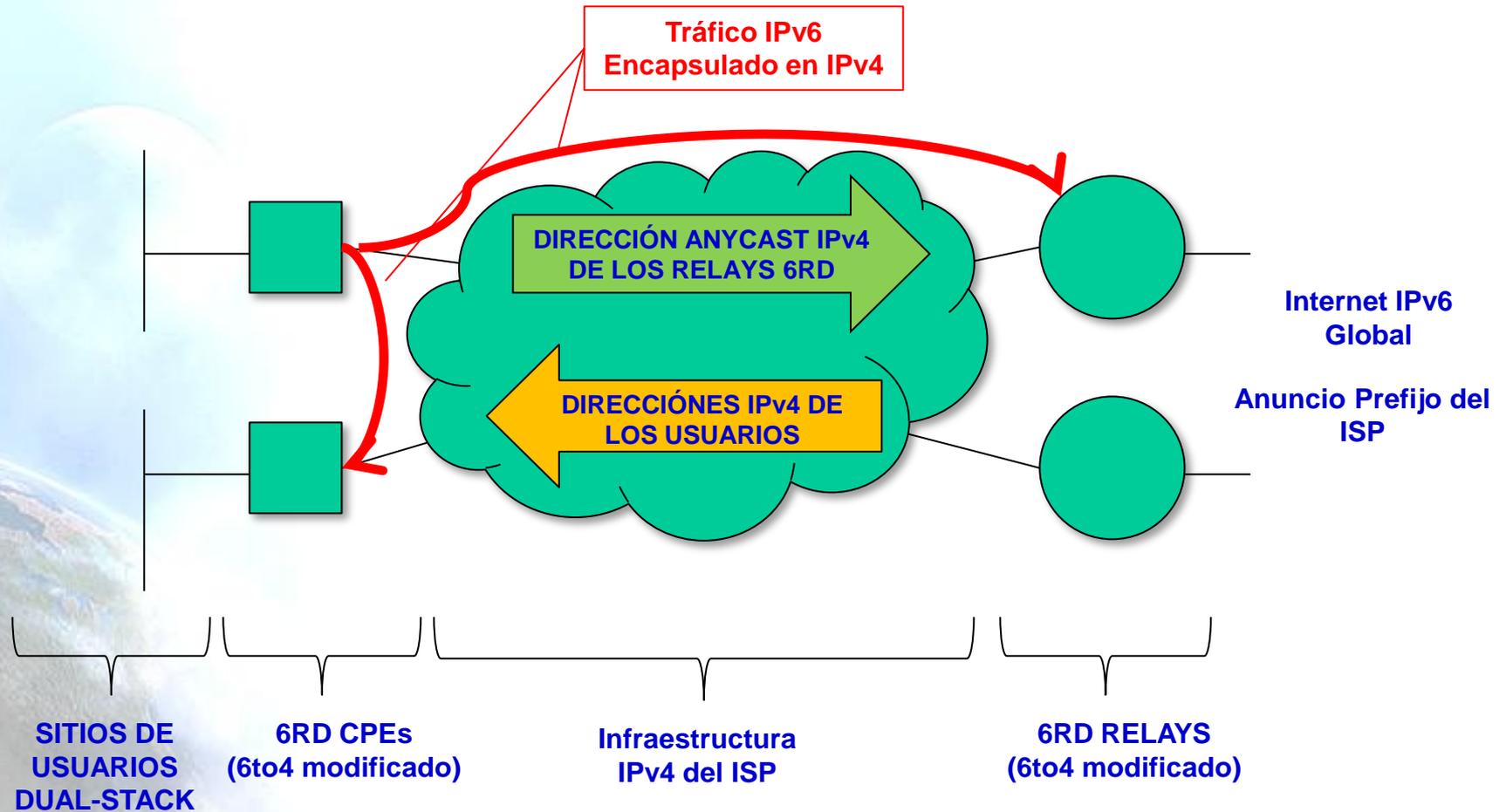


6RD: Arquitectura

- **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



8.7 Teredo

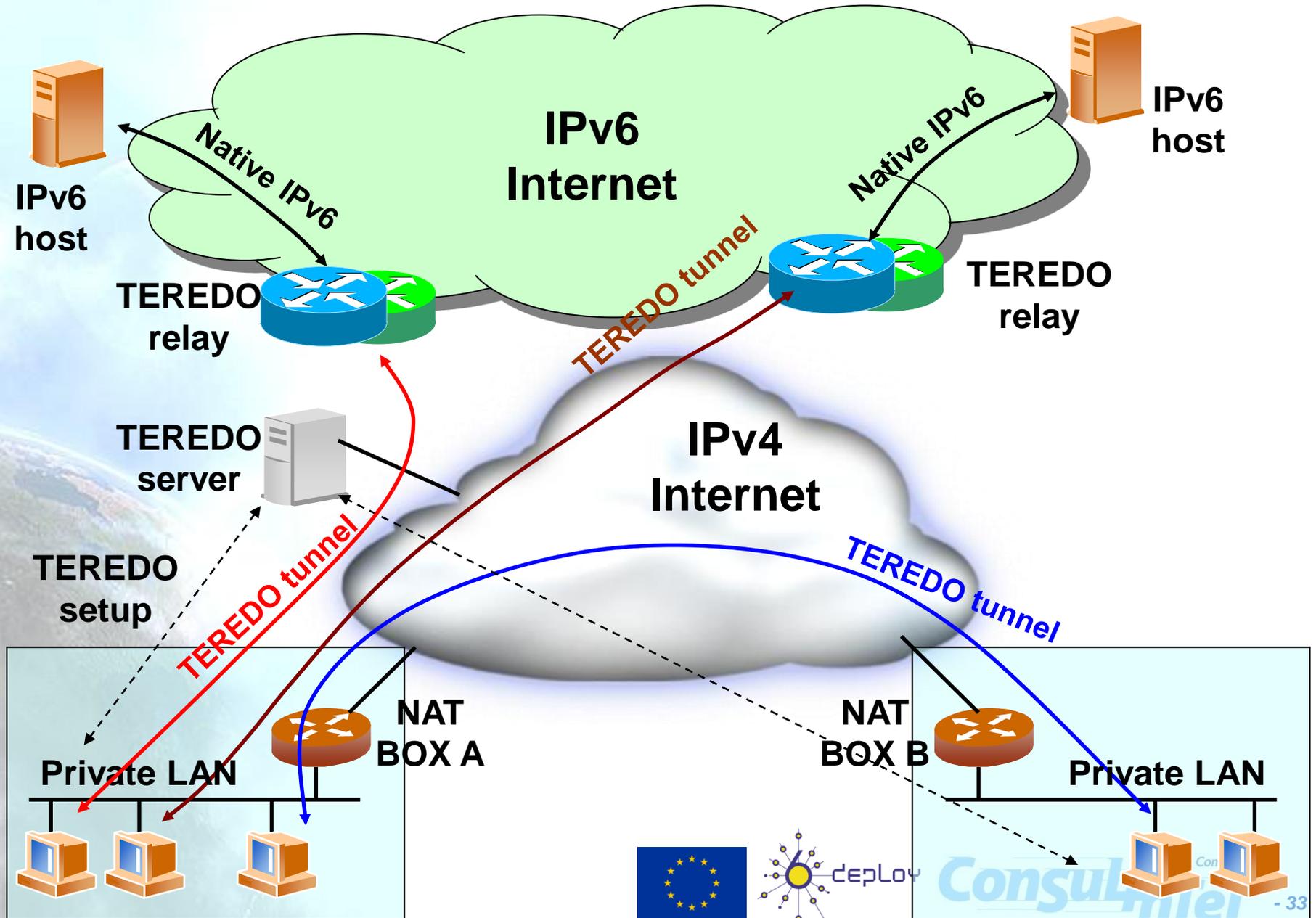


Teredo (RFC4380) (1)

- 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 pública 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)



8.8 Softwires



Softwires

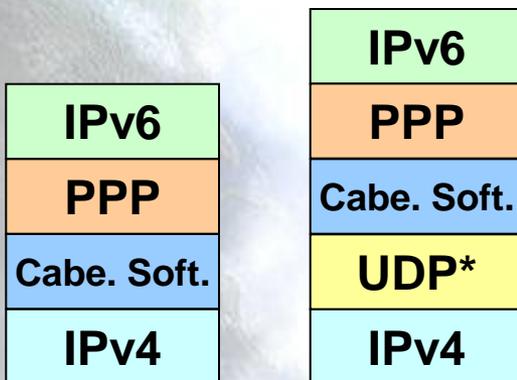
- Protocolo que esta siendo discutido en el grupo de trabajo Softwire del IETF. Presenta las siguientes características:
 - Mecanismo de transición “universal” basado en la creación de túneles
 - IPv6-en-IPv4, IPv6-en-IPv6, IPv4-en-IPv6, IPv4-en-IPv4
 - Permite atravesar NATs en las redes de acceso
 - 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
- Softwires se basa en **L2TPv2** (RFC2661) y **L2TPv3** (RFC3991)



Encapsulamiento de Softwires basado en L2TPv2

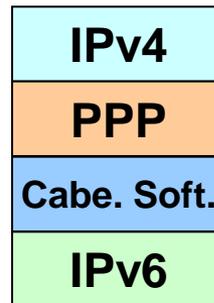
- El funcionamiento se especifica en draft-ietf-softwire-hs-framework-l2tpv2
- Existen dos entidades:
 - Softwires Initiator (SI): agente encargado de solicitar el túnel
 - Softwires Concentrator (SC): agente encargado de crear el túnel (tunnel end point)
- Se utiliza PPP para transportar paquetes IPx (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

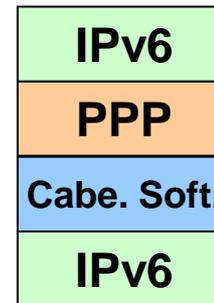


* Opcional

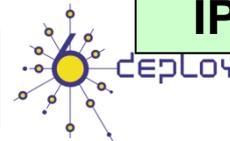
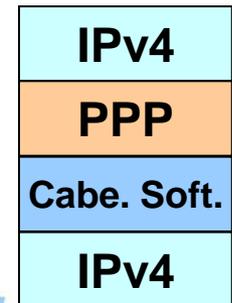
Túnel IPv4-en-IPv6



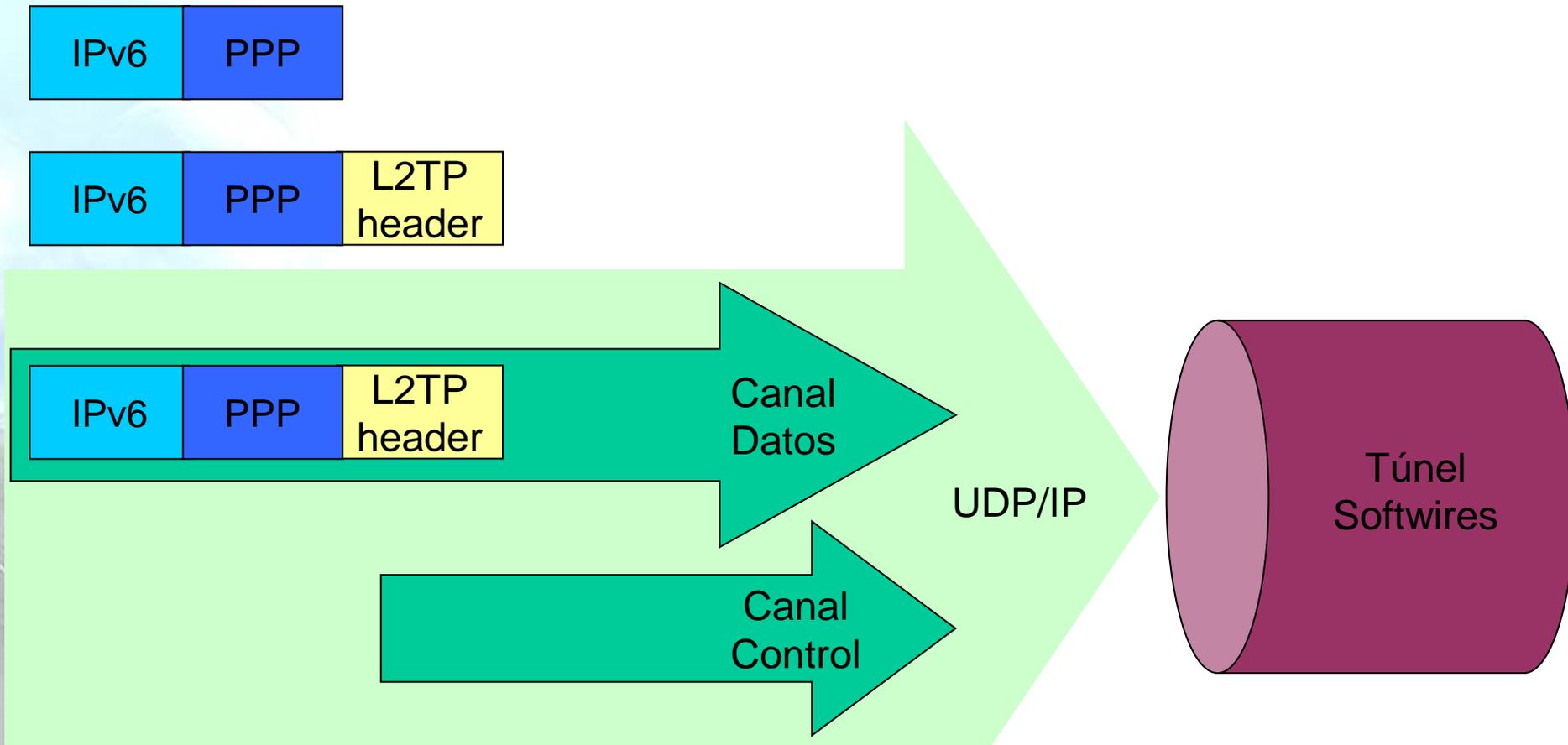
Túnel IPv6-en-IPv6



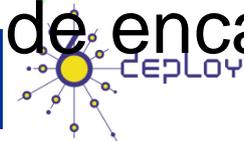
Túnel IPv4-en-IPv4



Softwires basado en L2TPv2

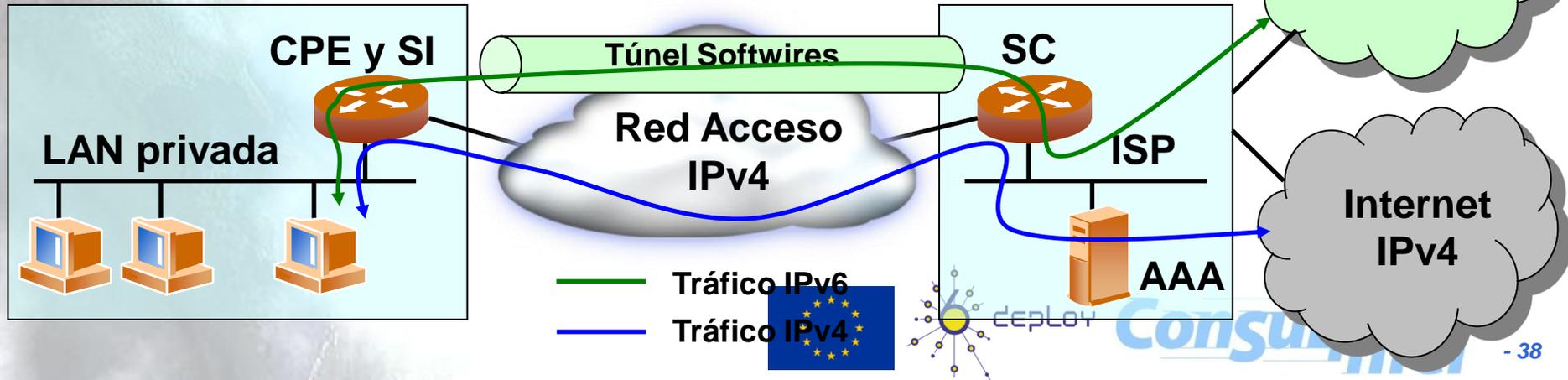


- Existe un plano de control y otro de datos
- Se usa PPP como protocolo de encapsulamiento



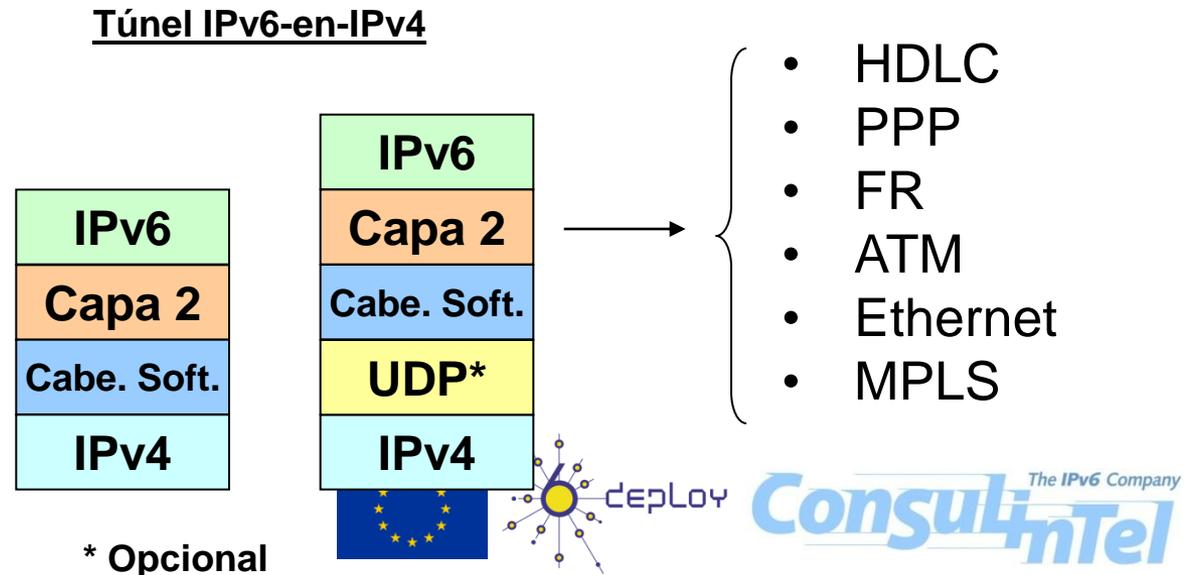
Ejemplo de uso de Softwires

- 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



8.9 DS-Lite

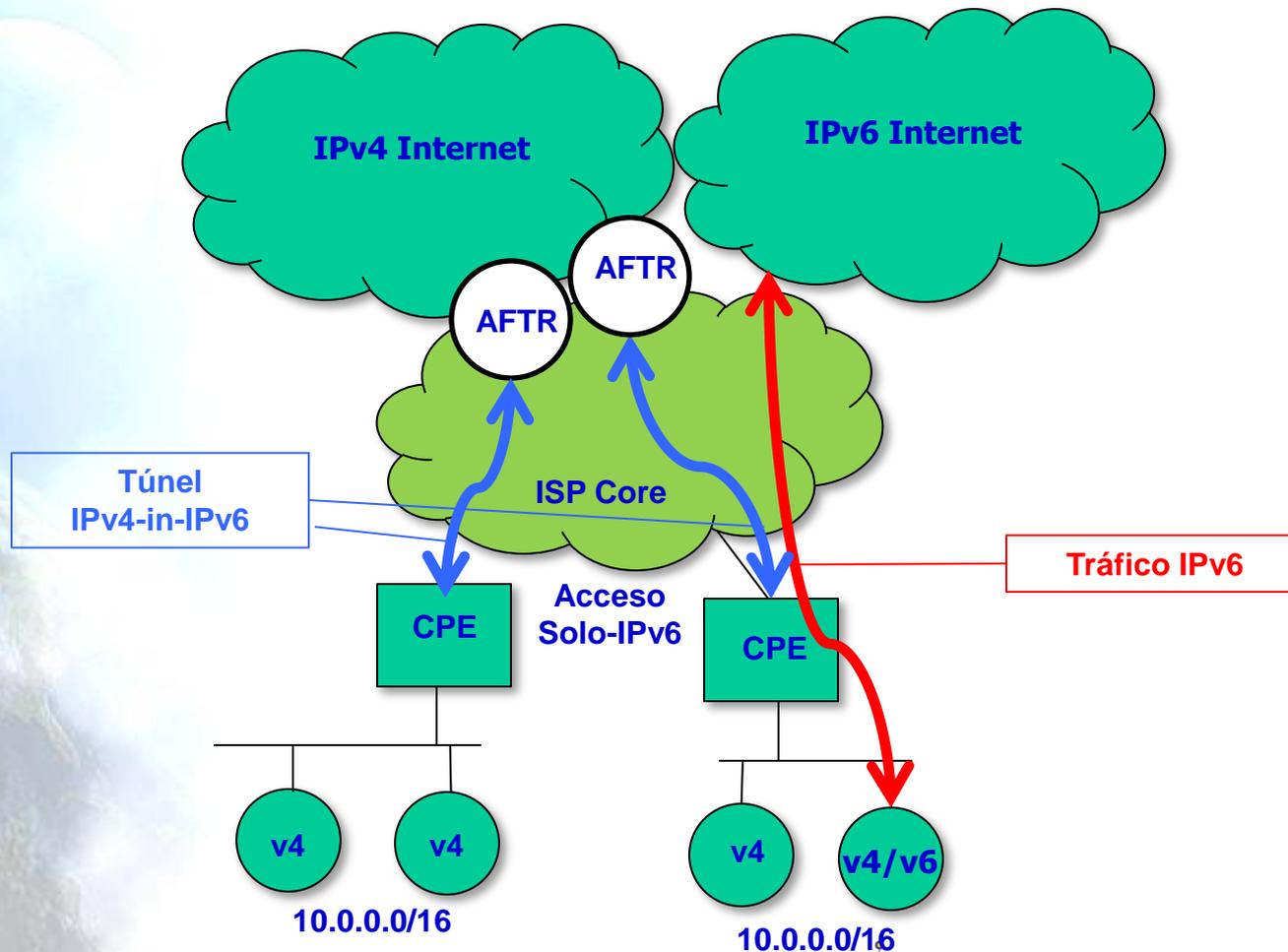


Dual Stack Lite (1)

- Trata de solucionar el problema del agotamiento de IPv4
- Comparte (las mismas) direcciones IPv4 entre usuarios combinando:
 - Tunneling
 - 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)



8.10 Traducción

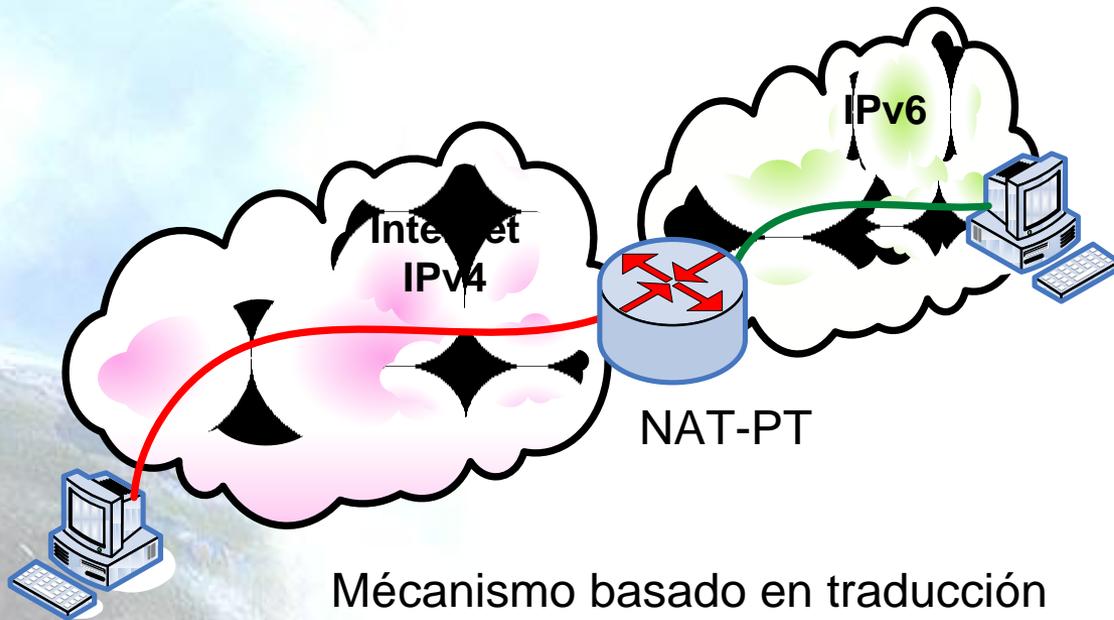


Traducción

- 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)



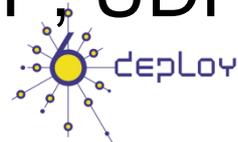
- Diferentes soluciones, pero tiene en común que tratan de traducir paquetes IPv4 a IPv6 y viceversa
 - [SIT], [BIS], [TRT], [SOCKSv64]
- La más conocida es NAT-PT [NATPT], [NATPTIMPL]
 - Un nodo intermedio (router) modifica las cabeceras IPv4 a cabeceras IPv6
 - El tratamiento de paquetes es complejo
- 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.

8.11 NAT64



NAT64 (1)

- Problema: 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
- Múltiples nodos solo-IPv6 comparten una dirección IPv4 para acceder a Internet IPv4
- 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 Algoritmo de Traducción IP/ICMP [RFC6145] [RFC6146]
- La especificación actual sólo define como NAT64 traduce paquetes unicast TCP, UDP e ICMP



NAT64 (2)

- La dirección de los hosts IPv4 se traduce algorítmicamente a/desde direcciones IPv6 usando un algoritmo específico [RFC6052]
- Se basa en información configurada estáticamente, incluido un prefijo conocido
- Se define prefijo “bien conocido” (64:ff9b::/96), se puede usar otro

PL	0	32	40	48	56	64	72	80	88	96	104
32	prefix	v4(32)				u		suffix			
40	prefix	v4(24)				u	(8)	suffix			
48	prefix	v4(16)				u	(16)	suffix			
56	prefix				(8)	u	v4(24)	suffix			
64	prefix					u	v4(32)	suffix			
96	prefix							v4(32)			



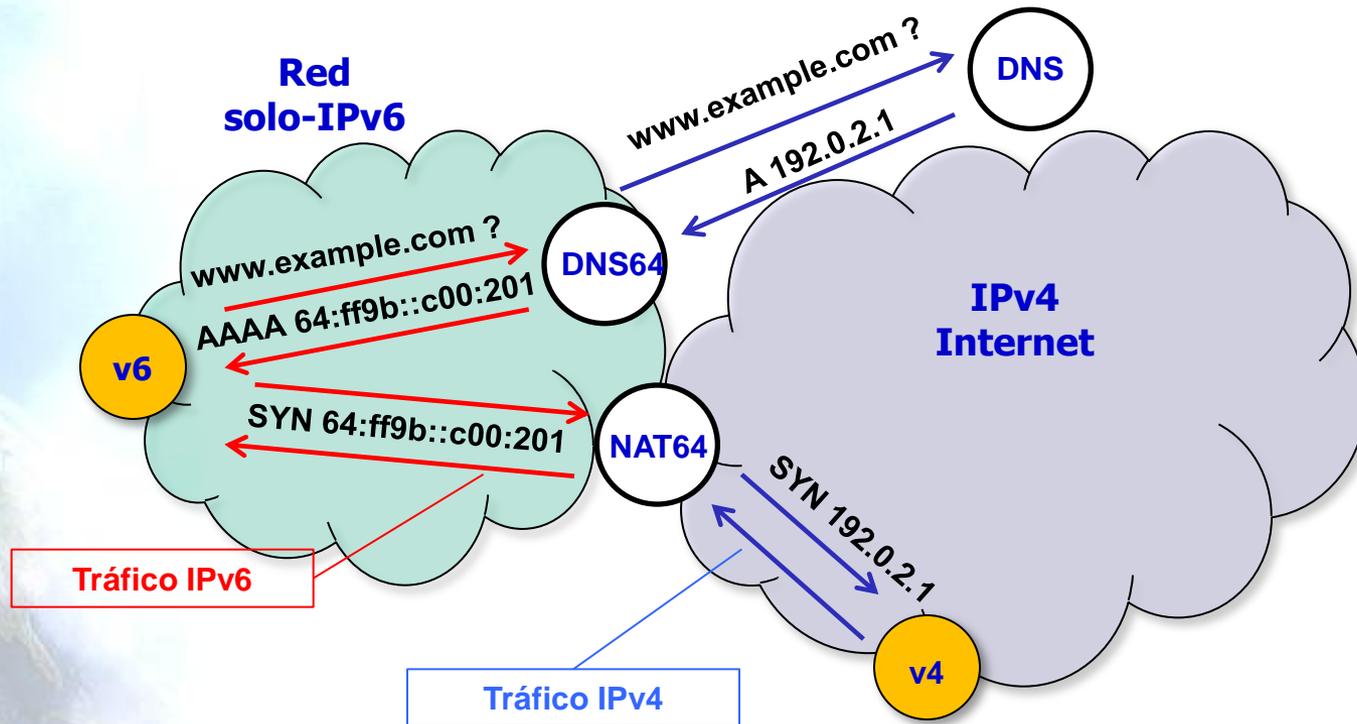
DNS64

- DNS64 es un mecanismo para sintetizar RRs tipo AAAA a partir de RRs tipo A [RFC6147]
- 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
- Cuando recibe una pregunta por un AAAA, pregunta hacia afuera por A y AAAA. Si recibe solo un A, lo convierte en AAAA
- Los host piensan que acceden a un nodo IPv6, con una dirección IPv6



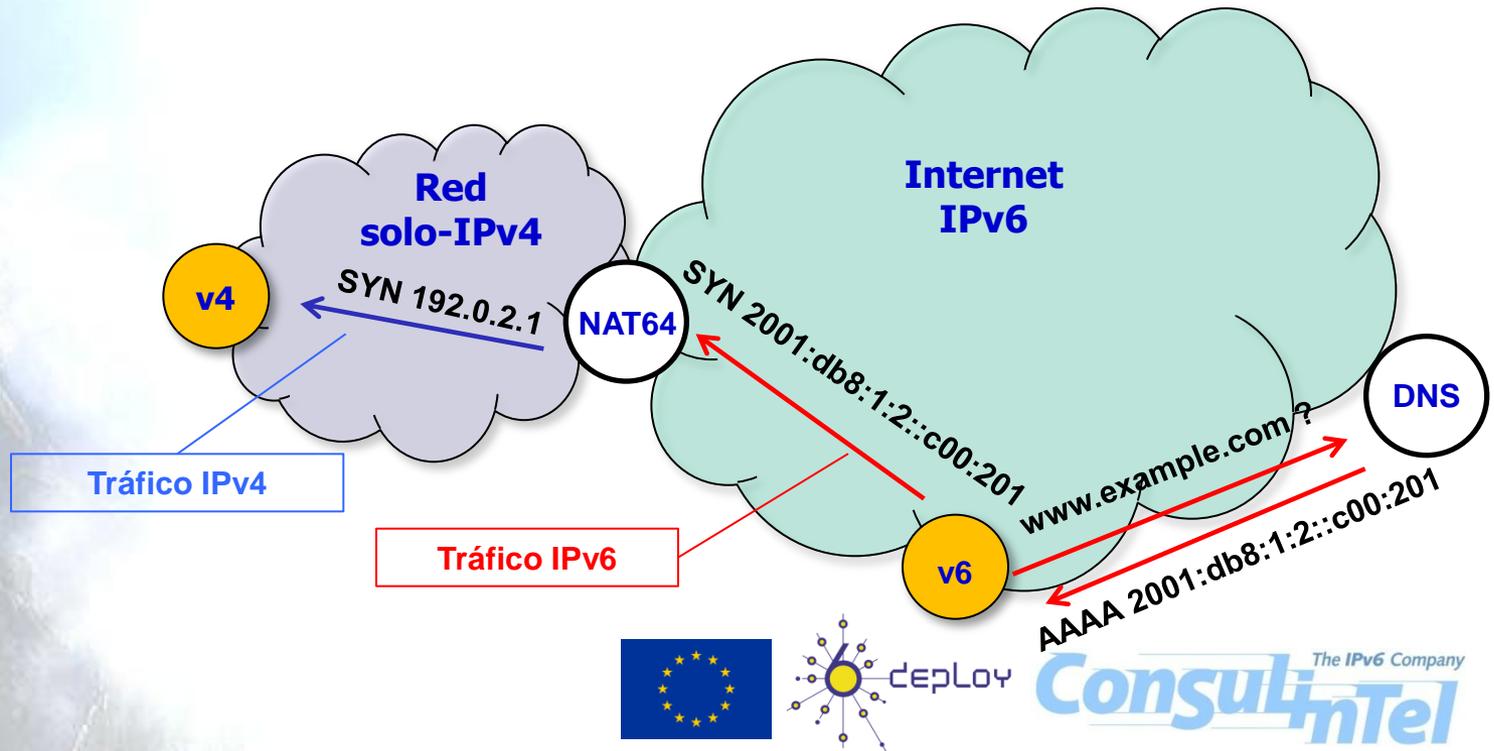
Stateful NAT64

- Permite a una red IPv6-solo conectarse a la Internet IPv4



Stateless NAT64

- También se puede usar para que la Internet IPv6 acceda a un nodo IPv4.
- Traducción 1-a-1: Dirección IPv6 fija para cada nodo IPv4, formada usando un prefijo global IPv6 incrustándole la dir. IPv4



NAT64 (3)

- Se sabe que hay cosas que no funcionan:
 - Todo lo que no sea TCP,UDP o ICMP: Multicast, Stream Control Transmission Protocol (SCTP), the Datagram Congestion Control Protocol (DCCP), e IPsec
 - Aplicaciones que llevan info de capa 3 en capa aplicación: FTP [RFC6384], SIP/H323
 - Algunas aplicaciones: juegos en línea, skype, etc.



Gracias !!

Contacto:

– Alvaro Vives (Consulintel):

alvaro.vives@consulintel.es



The IPv6 Company
Consulintel