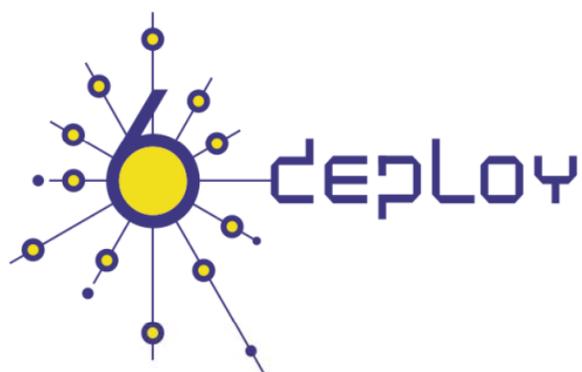


# Curso IPv6

WALC 2009

Bogotá – Colombia

21 al 25 Septiembre 2009



César Olvera ([cesar.olvera@consulintel.es](mailto:cesar.olvera@consulintel.es))

Alvaro Vives ([alvaro.vives@consulintel.es](mailto:alvaro.vives@consulintel.es))



# Contenido del curso (1)

- **Bloque 1. Tutorial IPv6**

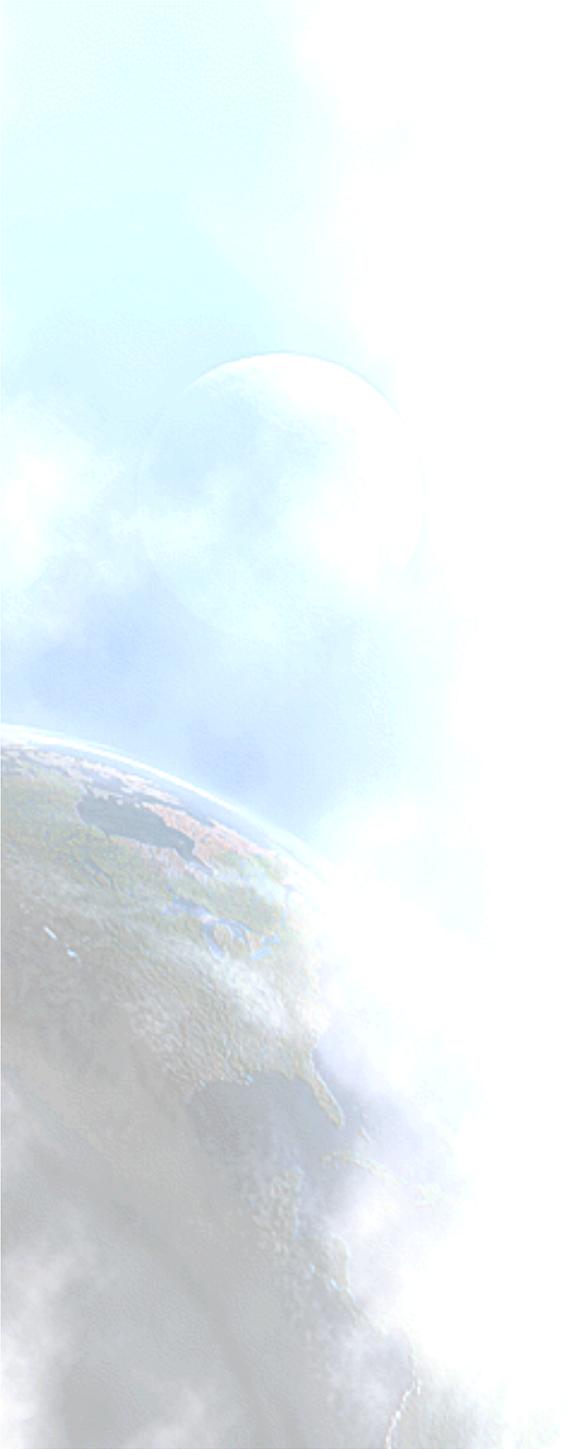
1. Introducción a IPv6
2. Formatos de cabeceras y tamaño de paquetes
3. Direccionamiento IPv6
4. ICMPv6, Neighbor Discovery y DHCPv6
5. Seguridad IPv6
6. Encaminamiento con IPv6
7. Mecanismos de Transición
8. Movilidad IPv6



# Contenido del curso (2)

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





# Bloque 1

# Tutorial IPv6



# 7. Mecanismos de Transición

7.1 Conceptos de Transición

7.2 Doble Pila

7.3 Túneles

7.4 Tunnel Broker

7.5 6to4

7.6 Teredo

7.7 Softwires

7.8 Traducción

7.9 Seguridad





# 7.1 Conceptos de Transición



# Técnicas de Transición / Coexistencia

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





## 7.2 Doble Pila

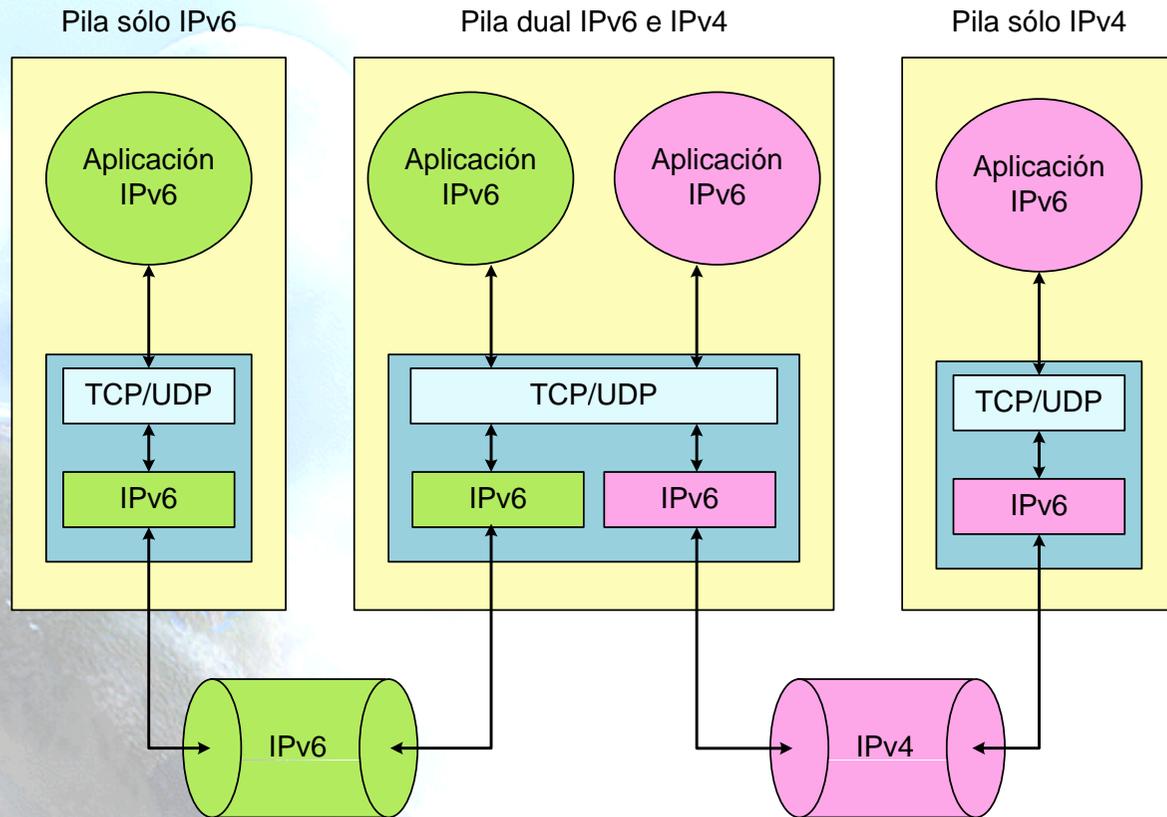


# Doble Pila (1)

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

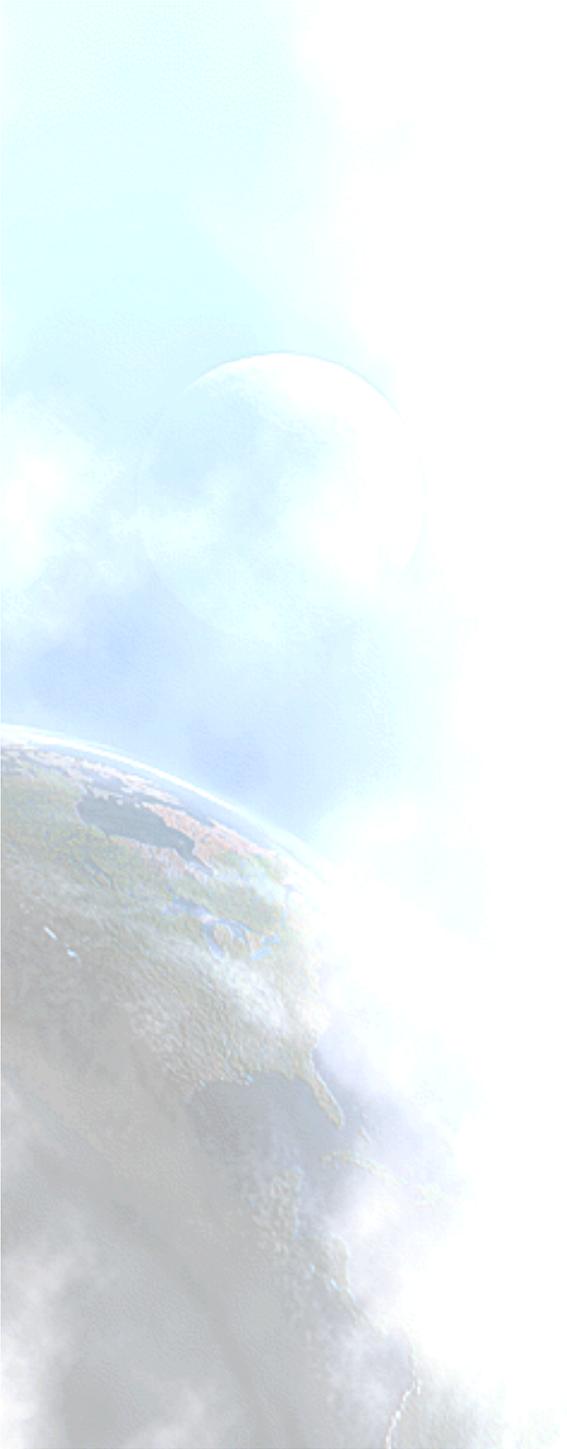


# Doble pila (2)



Mécanismo basado en doble pila

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



## 7.3 Túneles

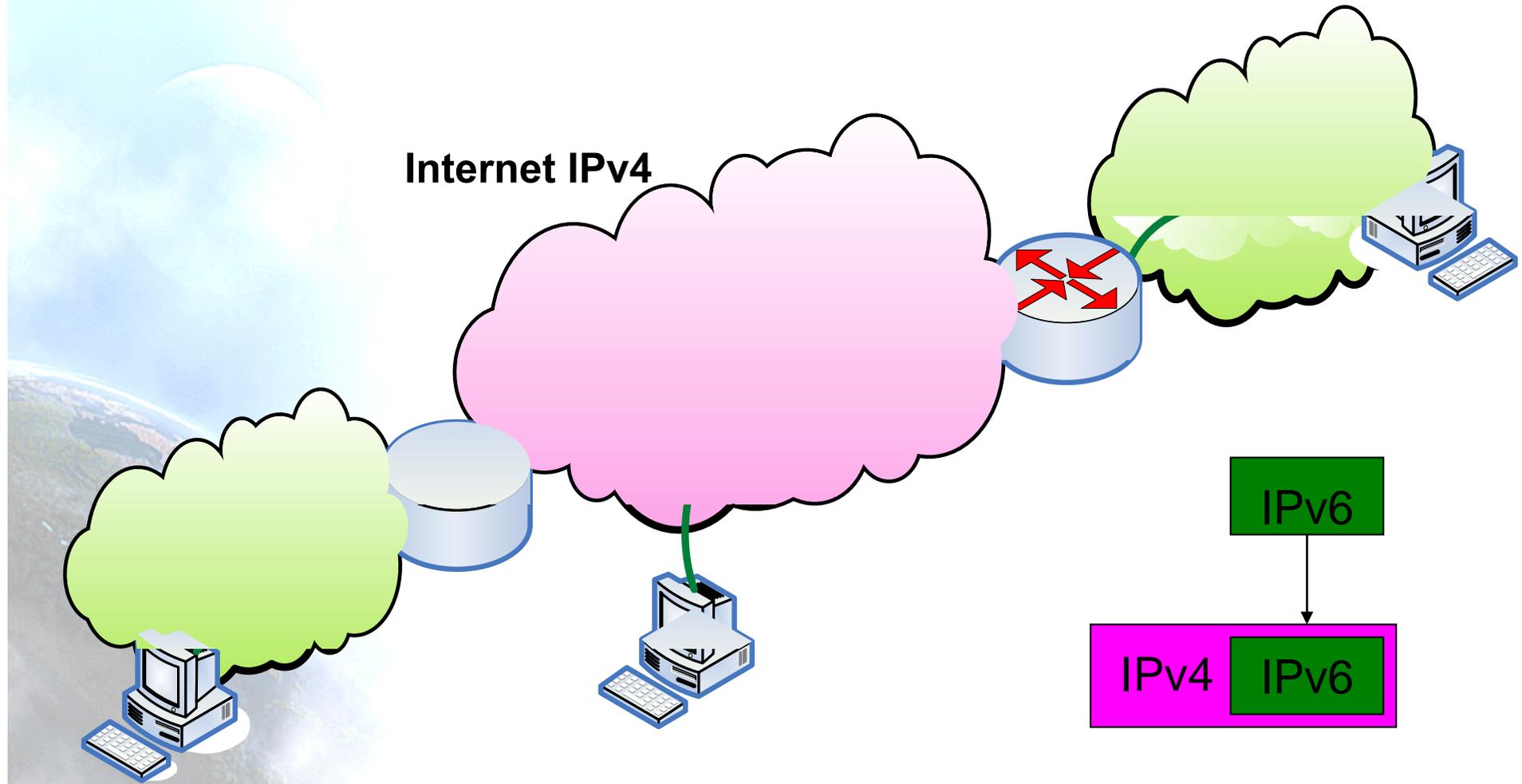


# Túneles para Atravesar Routers que no Reenvían IPv6

- Encapsulamos paquetes IPv6 en paquetes IPv4 para proporcionar conectividad IPv6 en redes que solo tiene soporte IPv4
- Muchos métodos para establecer dichos túneles:
  - configuración manual -> 6in4
  - “tunnel brokers” (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



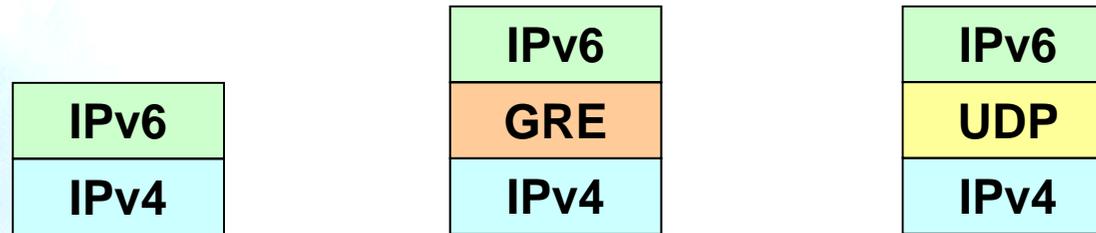
# Túneles IPv6 en IPv4 (6in4) (1)



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.

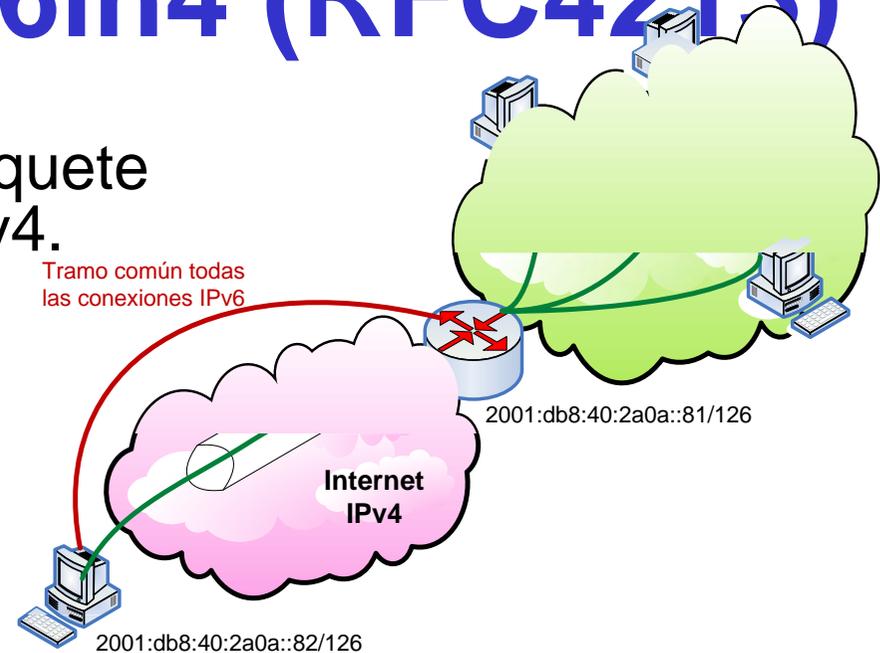
# Túneles 6in4 (3)

- 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.

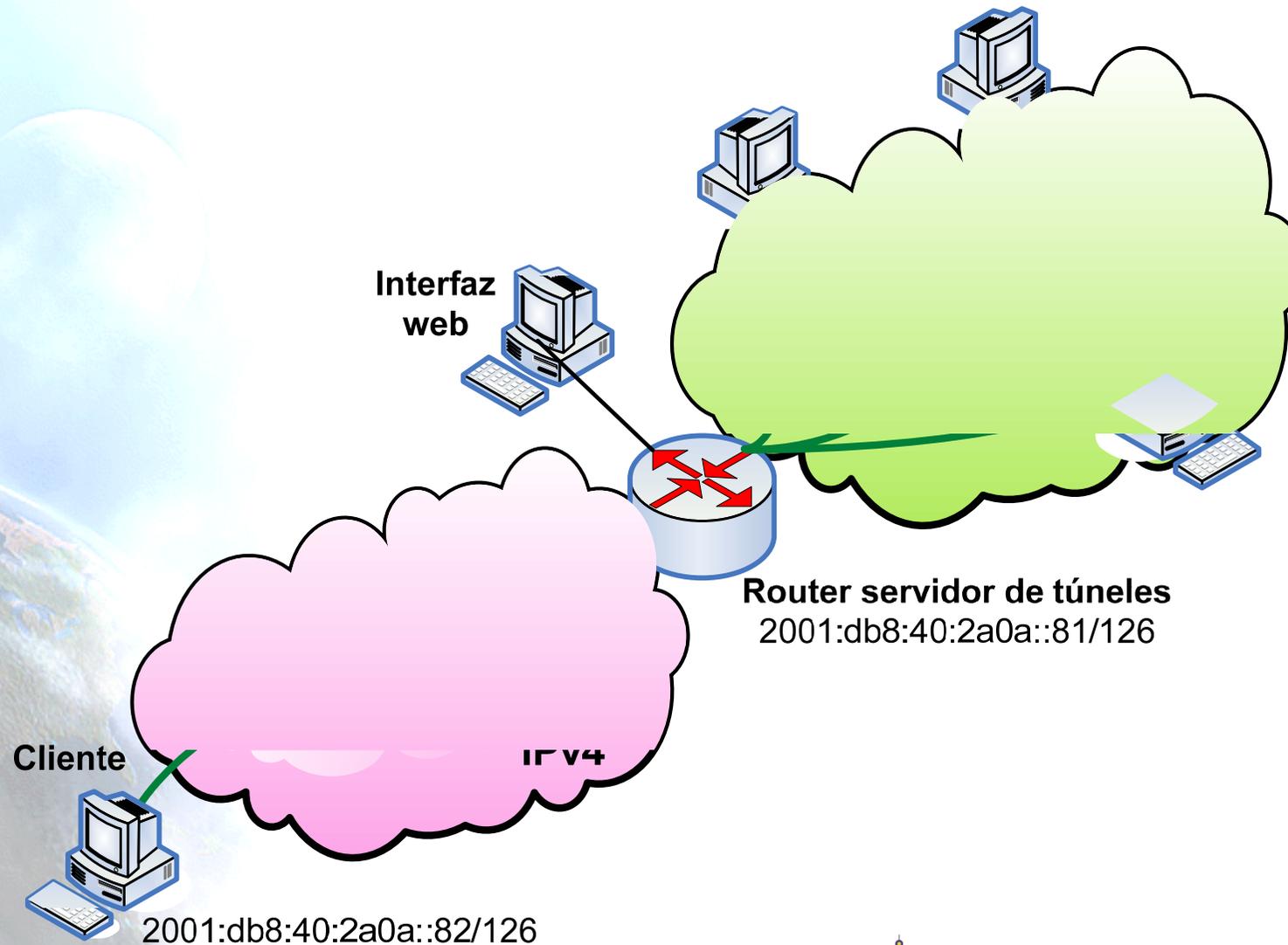




## 7.4 Tunnel Broker



# Tunnel Broker (RFC3053) (1)



# Tunnel Broker (RFC3053) (2)

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



# 7.5 6to4

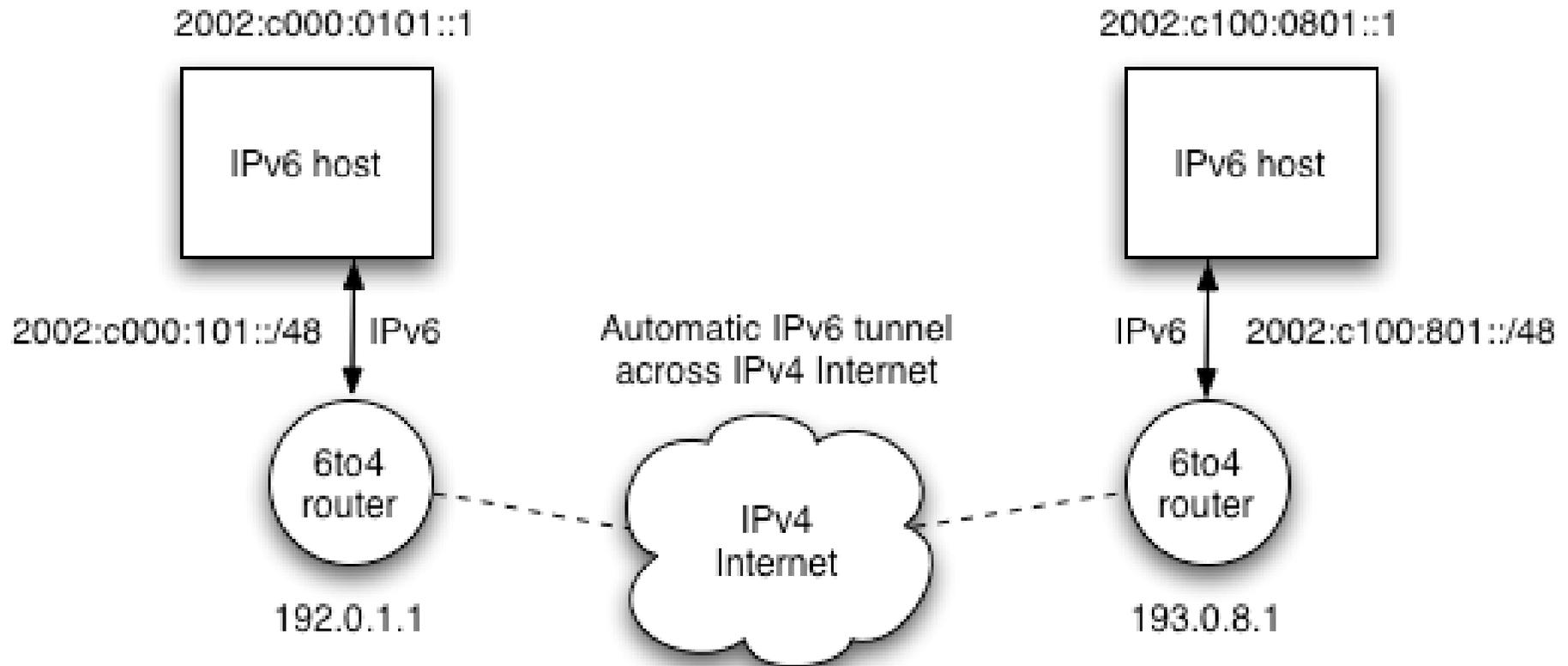


# Túneles 6to4 (1)

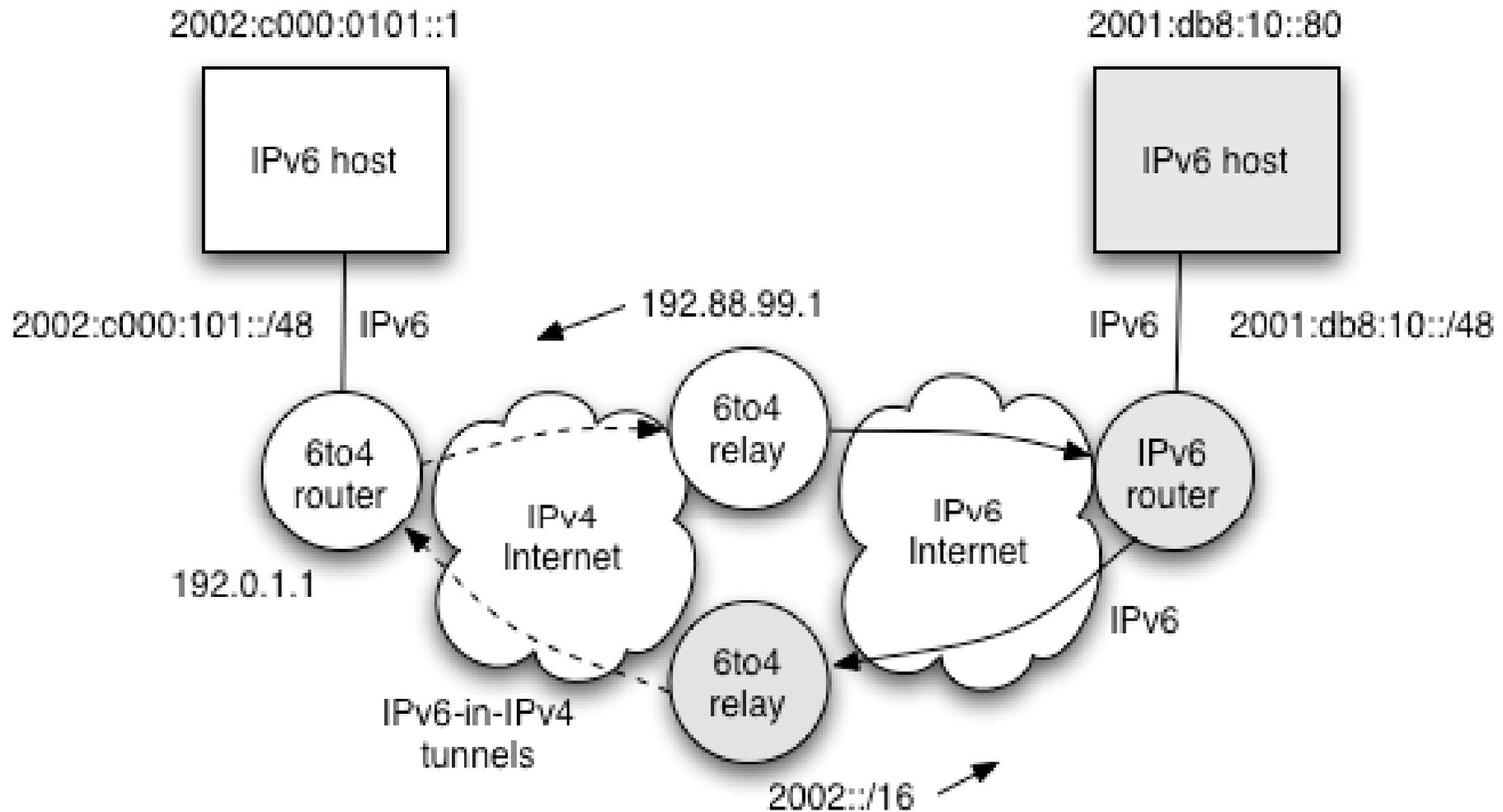
- Definido en RFC3056
- Se utiliza un “truco” para proporcionar direcciones 6to4.
  - Prefijo 6to4: 2002::/16
  - Se usa la IPv4 pública (p.e. 192.0.1.1) para siguientes 32 bits
  - Se obtiene así un prefijo /48 (p.e. 2002:C000:0101::/48)
- Cuando un router 6to4 ve un paquete hacia el prefijo **2002::/16**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

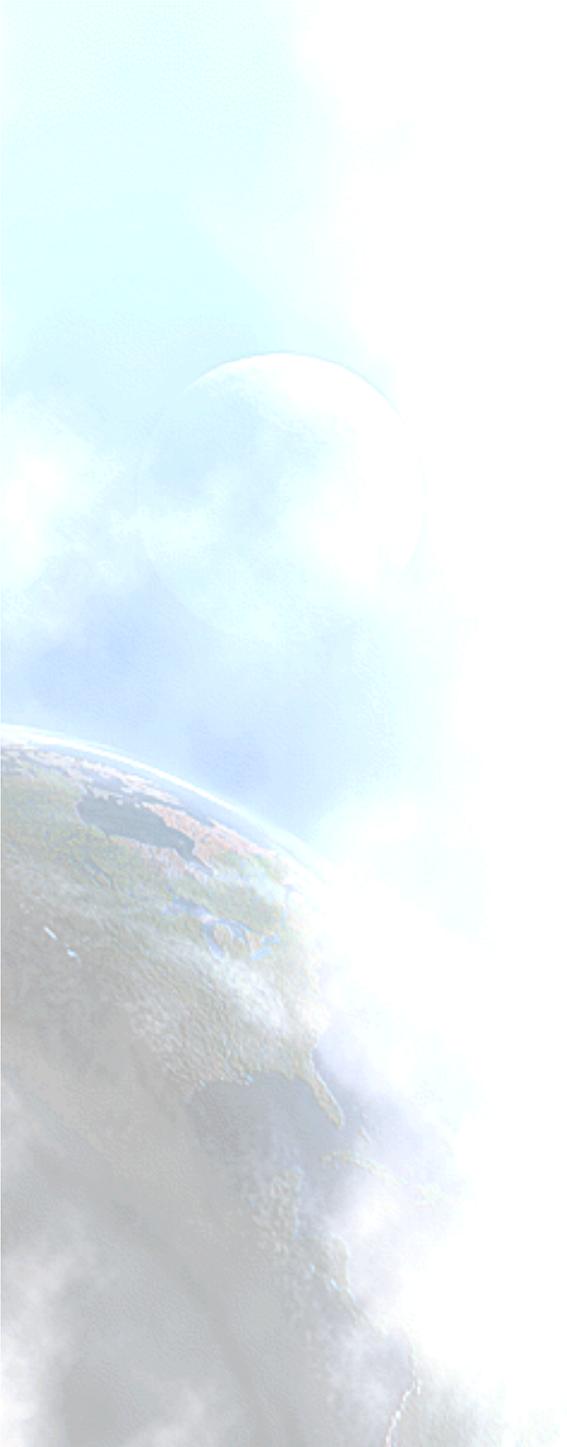


# Túneles 6to4 (2)



# Túneles 6to4 (3)





# 7.6 Teredo

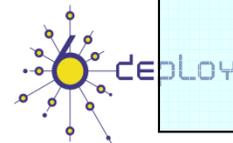
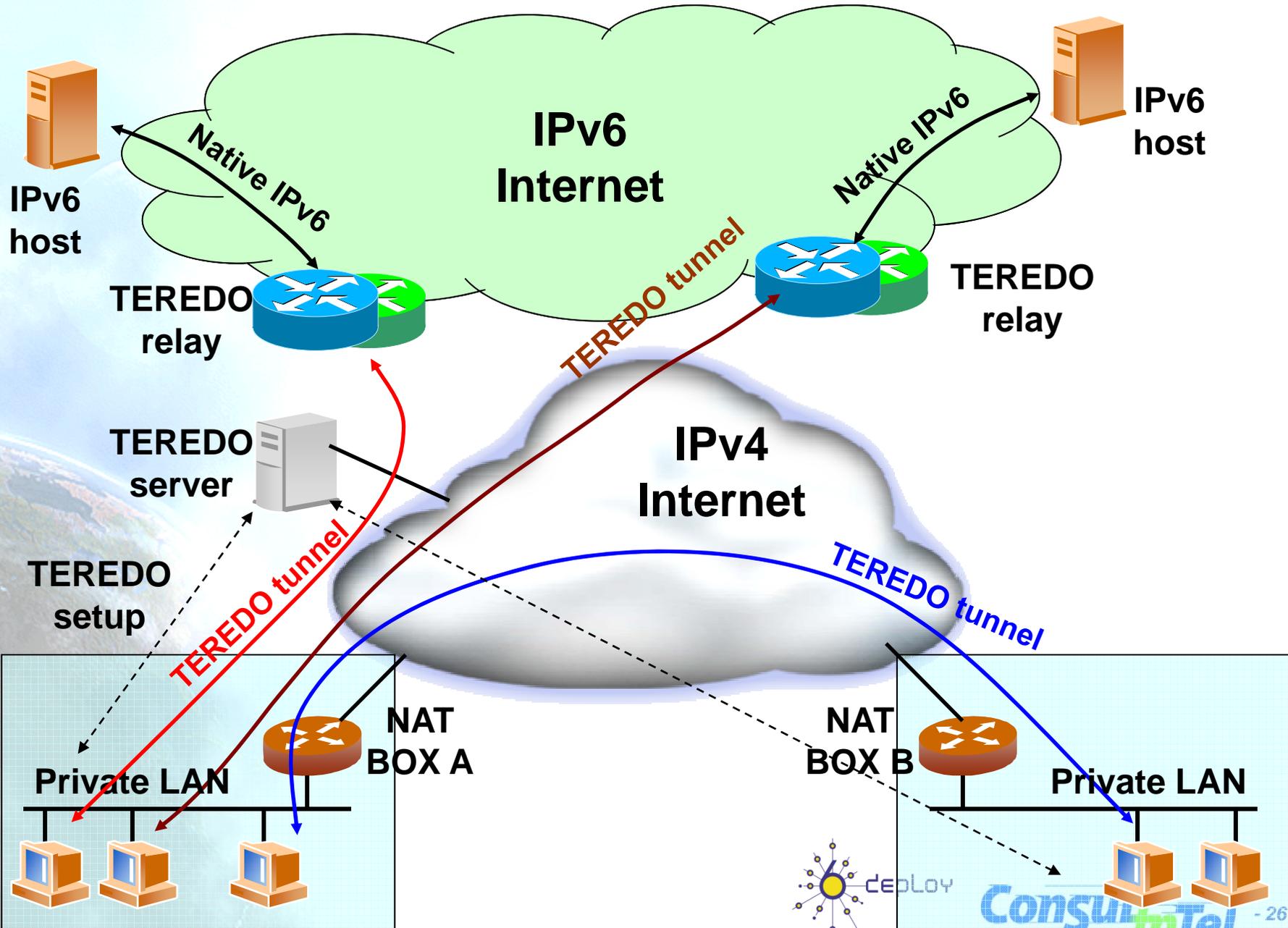


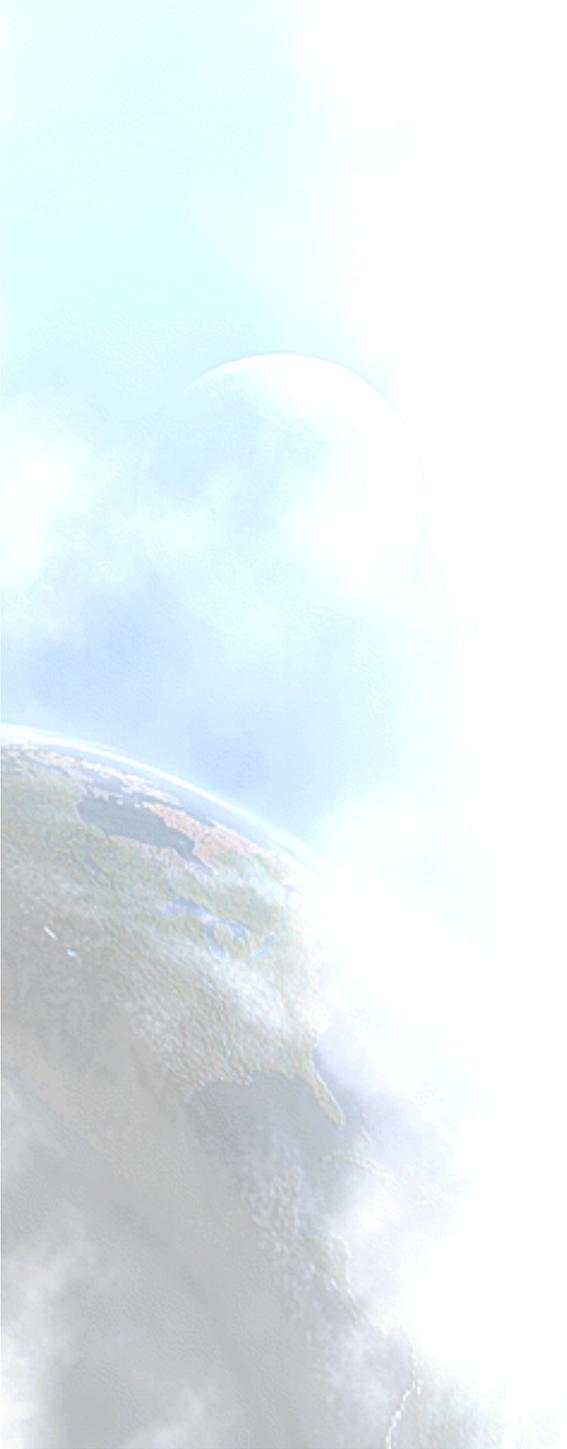
# Teredo (RFC4380) (1)

- Teredo [TEREDO] [TEREDOC] está pensado para proporcionar IPv6 a nodos que están ubicados detrás de NAT que no son “proto-41 forwarding”.
  - Encapsulado de paquetes IPv6 en paquetes UDP/IPv4
- Funciona en NAT de tipo:
  - Full Cone
  - Restricted Cone
- No funciona en NATs de tipo
  - Symmetric (Solventado en Windows Vista)
- Intervienen diversos agentes:
  - Teredo Server
  - Teredo Relay
  - Teredo Client
- El cliente configura un Teredo Server que le proporciona una dirección IPv6 del rango 2001:0000::/32 basada en la dirección IPv4 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)





# 7.7 Softwires



# Softwires

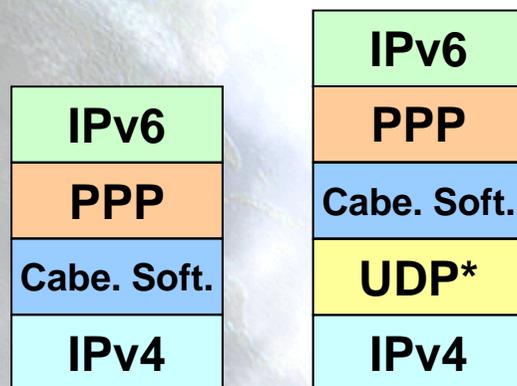
- Protocolo que esta siendo discutido en el grupo de trabajo Softwire del IETF. Presenta las siguientes características:
  - Mecanismo de transición “universal” basado en la creación de túneles
    - IPv6-en-IPv4, IPv6-en-IPv6, IPv4-en-IPv6, IPv4-en-IPv4
    - Permite atravesar NATs en las redes de acceso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



# Encapsulamiento de Softwires basado en L2TPv2

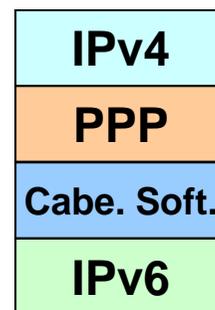
- El funcionamiento se especifica en draft-ietf-softwire-hs-framework-l2tpv2
- Existen dos entidades:
  - Softwires Initiator (SI): agente encargado de solicitar el túnel
  - Softwires Concentrator (SC): agente encargado de crear el túnel (tunnel end point)
- Se utiliza PPP para transportar paquetes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

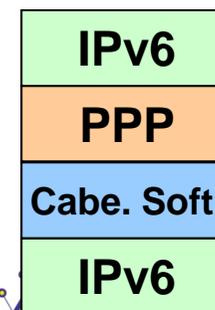


\* Opcional

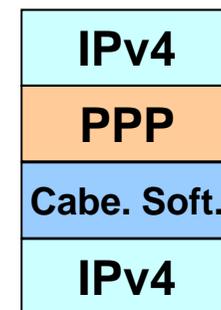
Túnel IPv4-en-IPv6



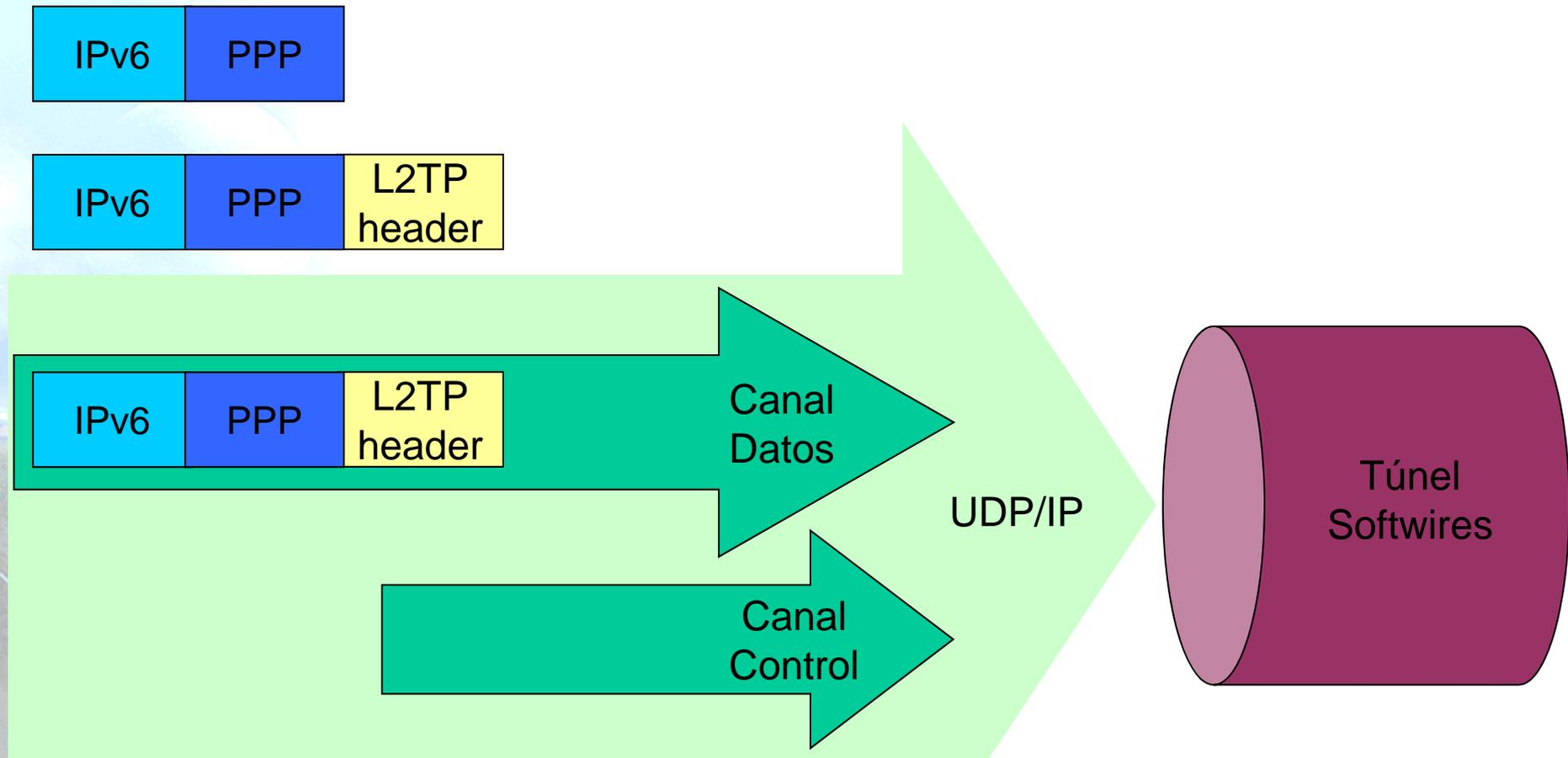
Túnel IPv6-en-IPv6



Túnel IPv4-en-IPv4



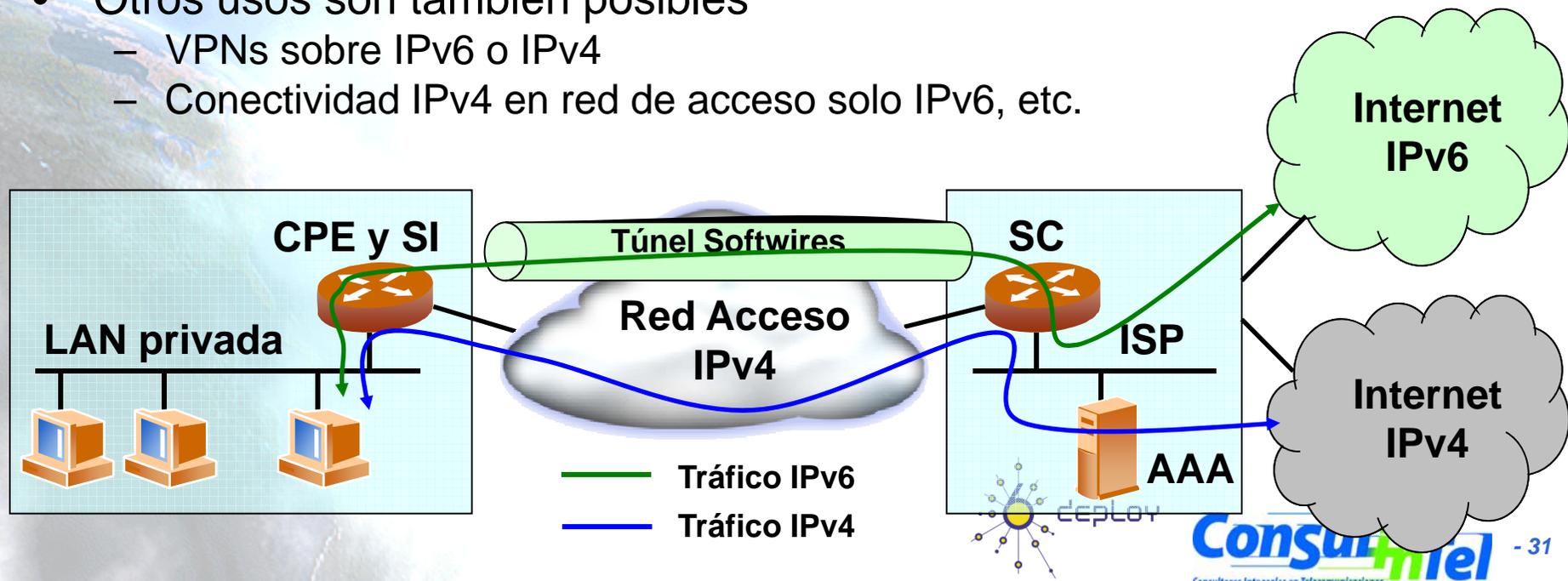
# Softwires basado en L2TPv2



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

# Ejemplo de uso de Softwires

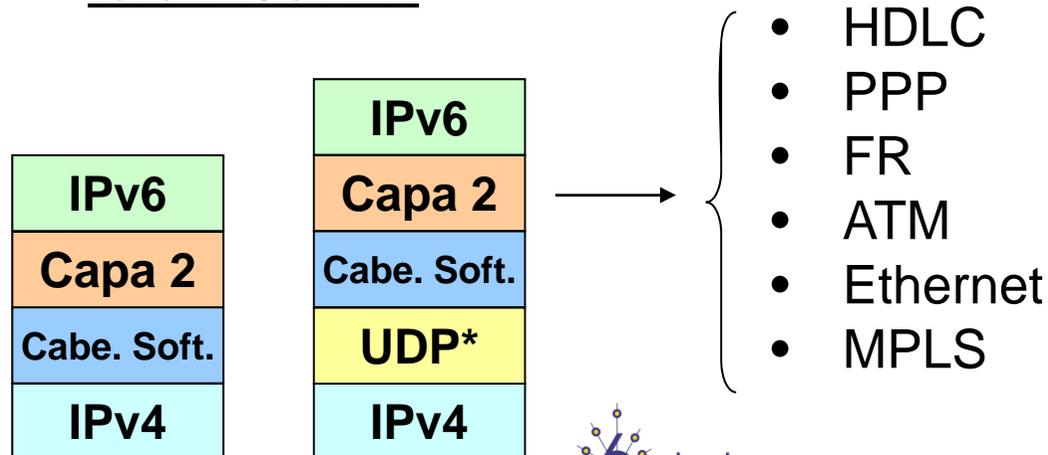
- Un uso típico previsible de Softwires es la provisión de conectividad IPv6 a usuarios domésticos a través de una red de acceso solo-IPv4
  - El SC está instalado en la red del ISP (DSLAM, Router de agregación u otro dispositivo)
  - El SI está instalado en la red del usuario
    - CPE típicamente.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

## Túnel IPv6-en-IPv4



\* Opcional





## 7.8 Traducción

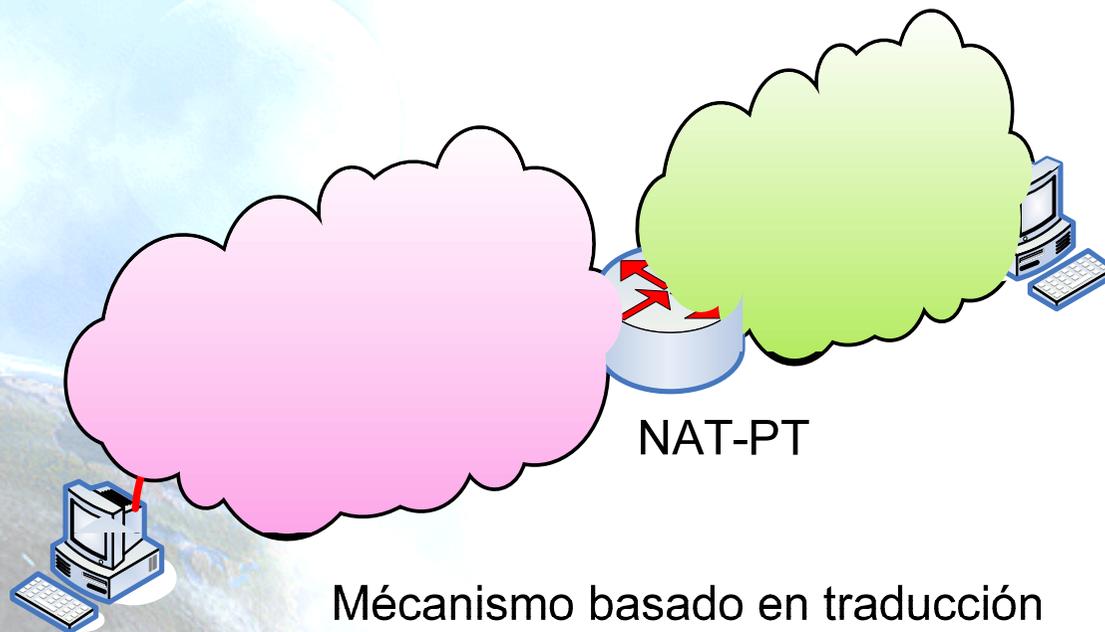


# Traducción

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



# Traducción IPv4/IPv6 (obsoleto)



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



# 7.9 Seguridad



# Seguridad en los mecanismos de transición

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



# Seguridad en túneles 6in4 (RFC4891) (1)

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



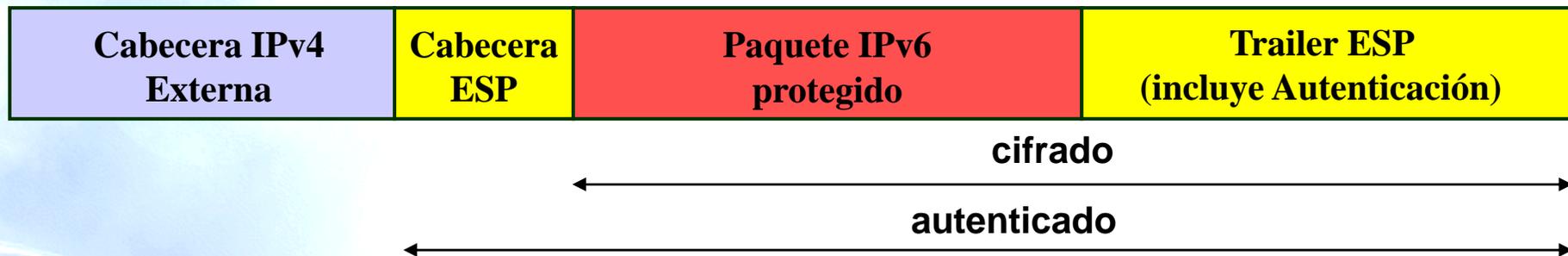
# Seguridad en túneles 6in4 (RFC4891) (2)

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



# IPsec con modo transporte en túneles 6in4

## Ejemplo del Modo Transporte con ESP

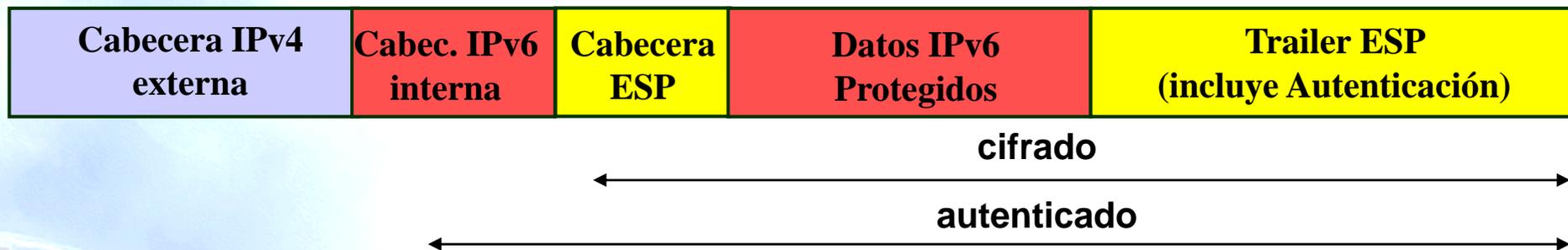


- Modo transporte
  - Se emplea ESP o AH dependiendo del grado de seguridad deseado
  - La SA se define mediante (entre otros):
    - IPv4 origen
    - IPv4 destino
    - Tipo de tráfico: IPv6, (protocolo 41)
  - En el receptor, cuando un paquete IPsec se acepta se garantiza que viene de la dirección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



# IPsec con modo túnel en túneles 6in4

## Ejemplo del Modo Túnel con ESP



- Modo túnel
  - Se emplea ESP o AH dependiendo del grado de seguridad deseado
  - La SA se define mediante (entre otros):
    - IPv6 origen
    - IPv6 destino
  - En el receptor, cuando un paquete IPsec se acepta se garantiza que viene de la dirección IPv6 adecuada
  - Con IPsec en modo túnel 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 tráfico
  - Tráfico IPv6 benigno
  - Tráfico IPv6 maligno con deseo de vulnerar nodos/servicios
- De este modo cierto tipo de tráfico pasa por los sistemas perimetrales sin ningún tipo de control, sin que el administrador de la red/seguridad pueda saber qué tipo de tráfico IPv6 atraviesa su red
  - Hasta la fecha no existen dispositivos capaces de inspeccionar el tráfico TEREDO, de manera que no es posible aplicar políticas de seguridad al tráfico IPv6 encapsulado con ese método
- Por este motivo, en caso de permitir el uso TEREDO en los nodos finales dentro de una red, es altamente recomendable:
  - El nodo final esté adecuadamente protegido
    - Puesta al día de actualizaciones de software, sistema operativo, etc.
    - Instalación de mecanismos de protección adecuados (anti-virus, etc.)
  - El administrador de red/seguridad debe estar al corriente de las posibles vulnerabilidades introducidas por TEREDO
    - [draft-ietf-v6ops-teredo-security-concerns](#)



# Referencias Transición (1)

- [6in4] RFC1933, RFC4213
- [6to4] RFC3056
- [6over4] RFC2529
- [AYIYA ] draft-massar-v6ops-ayiya-02
- [BIS] RFC2767
- [DSTM] draft-ietf-ngtrans-dstm-10
- [ISATAP] RFC5214
- [NATPT] RFC2766, RFC4966
- [NATPTIMPL]
  - <http://www.ipv6.or.kr/english/download.htm> ==> Linux 2.4.0
  - [http://www.ispras.ru/~ipv6/index\\_en.html](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)

- [SOCKSv6 ] RFC3089
- [SOFTWIRES] RFC5571
- [STATELESS] RFC4862
- [STATEFUL] RFC3315
- [STUN] RFC3489
- [TB] RFC3053
- [TEREDO] RFC4380
- [TEREDOC] <http://technet.microsoft.com/es-es/library/cc722030%28WS.10%29.aspx>
- [TRT] RFC3142
- [TSP] draft-vg-ngtrans-tsp-01,  
<http://www.hexago.com/index.php?pgID=step1>
- [TunAut] RFC1933
- Windows IPv6
  - [http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag\\_ip\\_v6\\_add\\_utils.mspx](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_ip_v6_add_utils.mspx)
  - <http://www.microsoft.com/technet/community/columns/cableguy/cg0902.mspx>



# Gracias !!

## Contacto:

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

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

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

