Herramientas de Transición

IPv6 Workshop

La Habana 15 Octubre 2008

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

Mecanismos de Transición

1. Conceptos de Transición
2. Doble Pila
3. Túneles
4. Tunnel Broker
5. 6to4
6. Teredo
7. Softwires
8. Traducción
9. MPLS
10. Seguridad

1. Conceptos de Transición

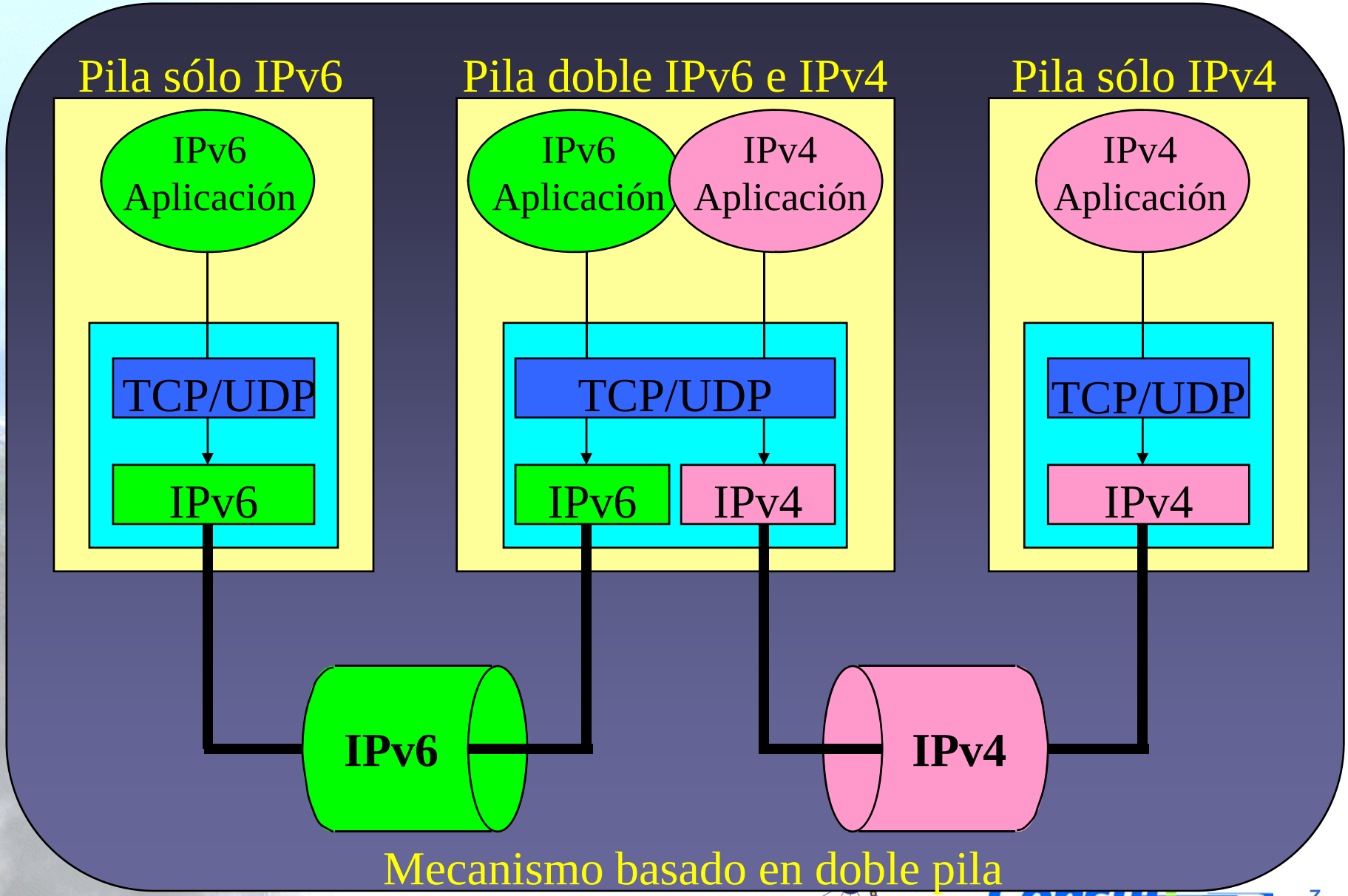
Técnicas de Transición / Coexistencia

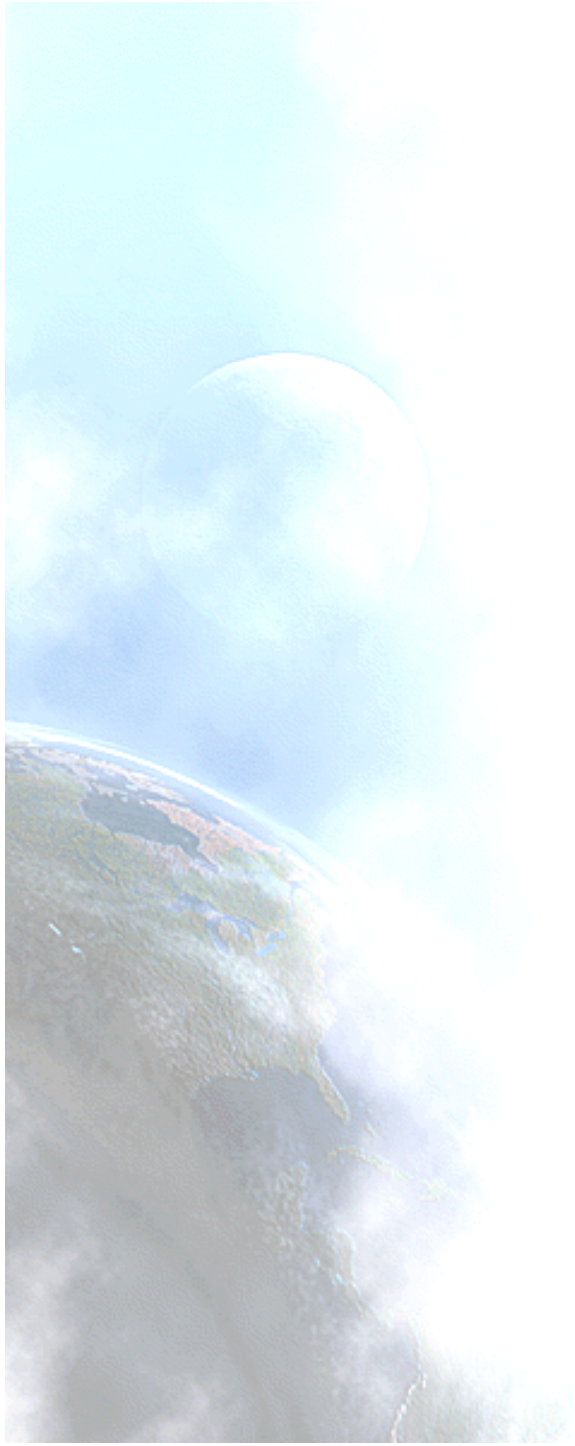
- IPv6 se ha diseñado para facilitar la transición y la coexistencia con IPv4.
- Coexistirán durante décadas -> No hay un “día D”
- Se han identificado e implementado un amplio abanico de técnicas, agrupadas básicamente dentro de tres categorías:
  1) **Doble-pila**, para permitir la coexistencia de 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.

2. Doble Pila

Doble Pila

- 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.


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

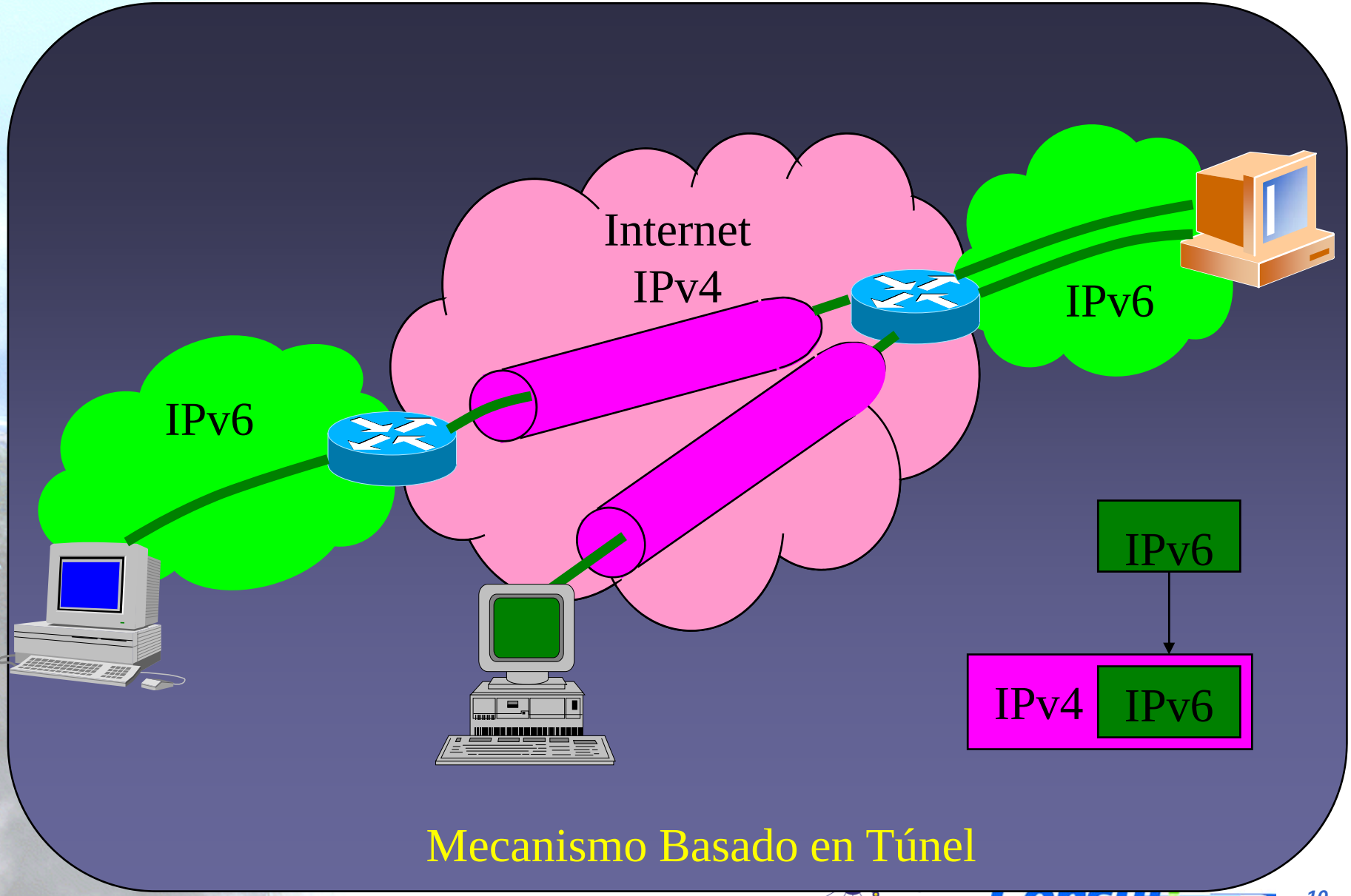


3. Túneles

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 (link-layer) virtual, o
  - una VPN IPv6 sobre la Internet IPv4

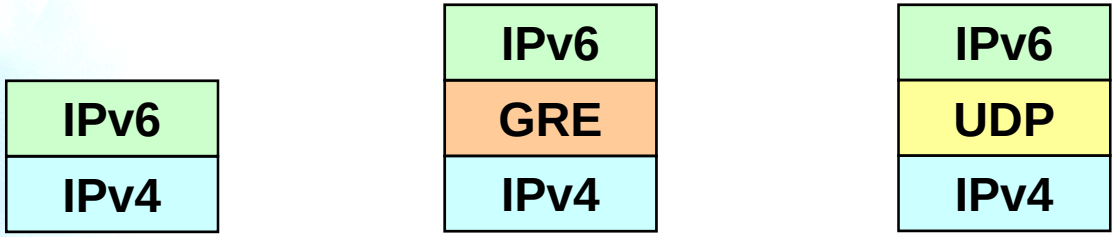
Túneles 6in4 (1)



Mecanismo Basado en Túnel

Túneles 6in4 (2)

- Existen diversas formas de encapsular los paquetes IPv6:



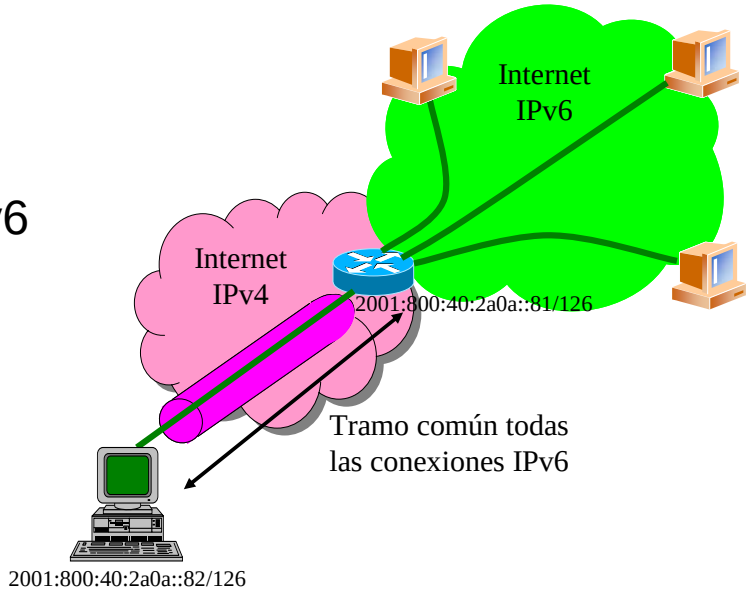
- Lo mismo se aplica para IPv4 usado en redes solo IPv6.

Túneles 6in4 (3)

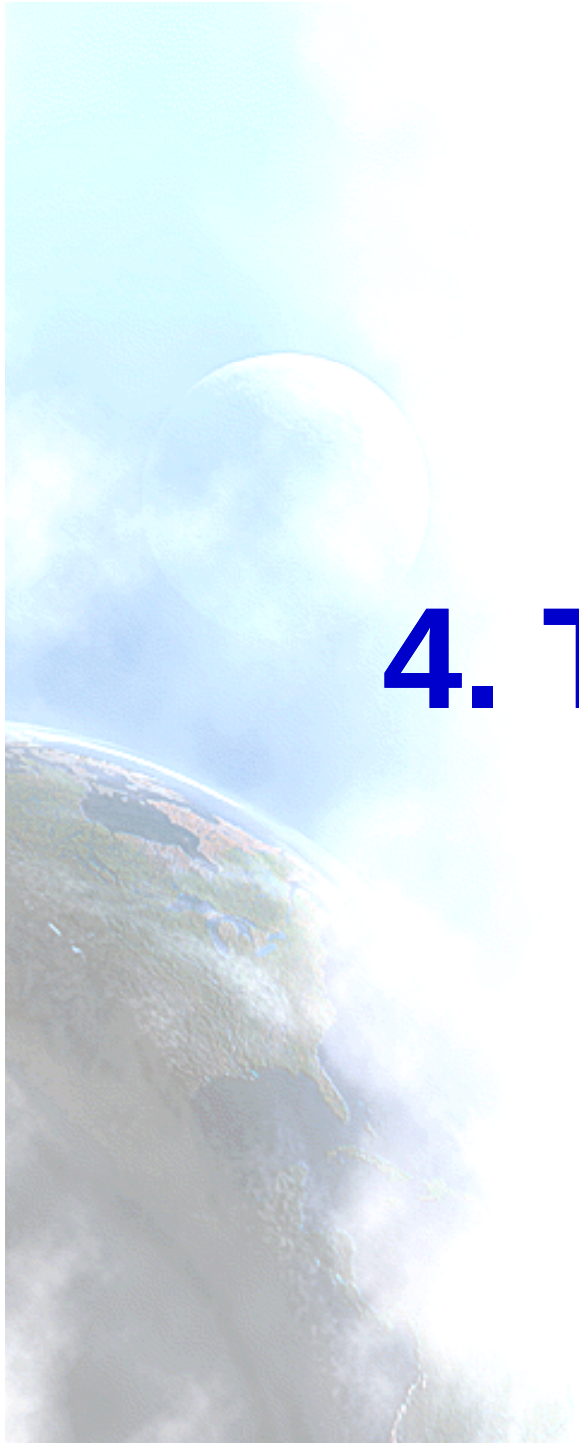
- Algunos mecanismos de transición basados en túneles
  - 6in4 (*) [6in4]
  - TB (*) [TB]
  - TSP [TSP]
  - 6to4 (*) [6to4]
  - Teredo (*) [TEREDO], [TEREDOC]
  - Túneles automáticos [TunAut]
  - ISATAP [ISATAP]
  - 6over4 [6over4]
  - AYIYA [AYIYA]
  - Silkroad [SILKROAD]
  - DSTM [DSTM]
  - Softwires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

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

Detalles Túneles 6in4 (RFC4213)

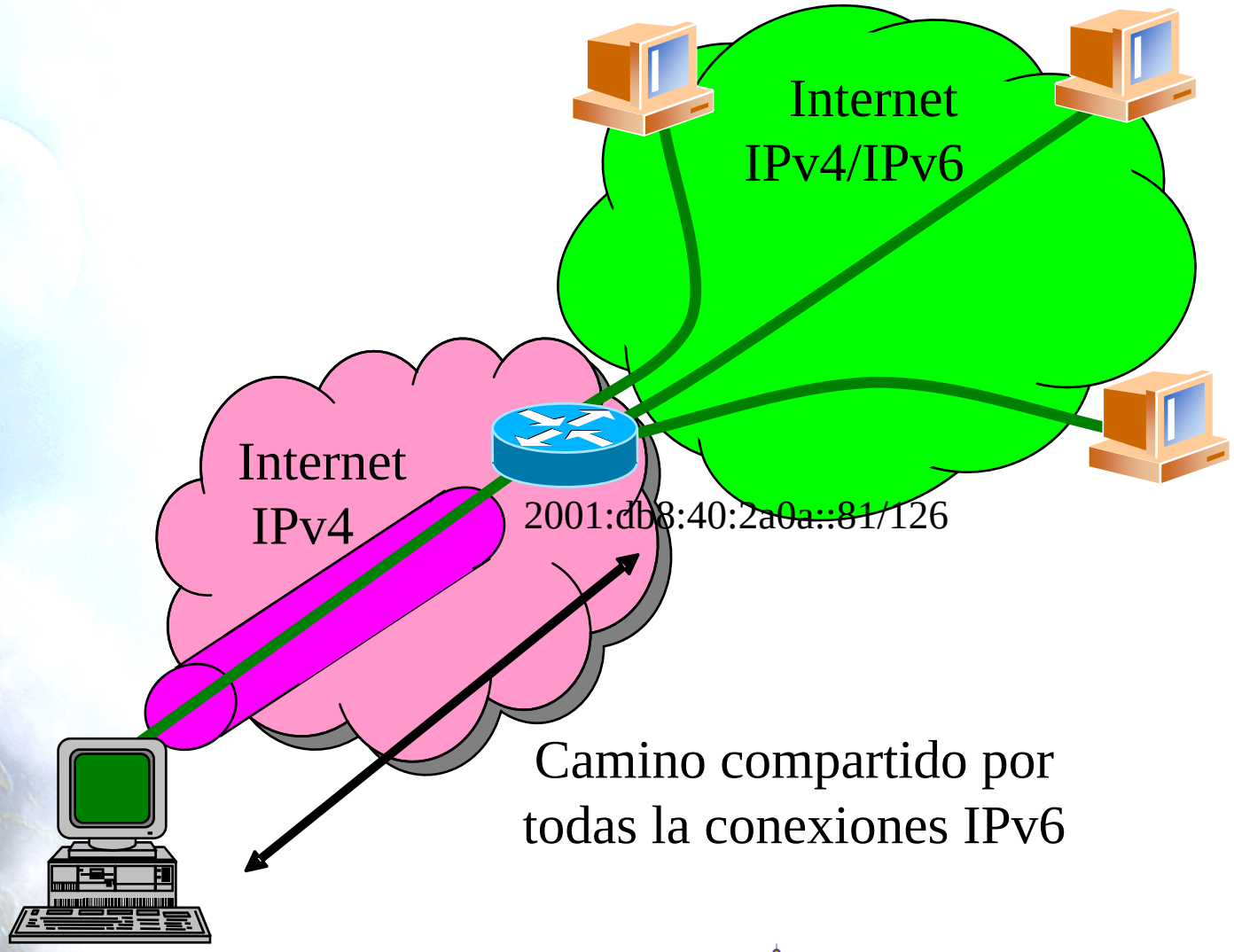


- Encapsula directamente el paquete IPv6 dentro de un paquete IPv4.
- Se suele hacer entre
  - nodo final ==> router
  - router ==> router
- Aunque también es posible para
  - nodo final ==> nodo final
- El túnel se considera como un enlace punto-a-punto desde el punto de vista de IPv6.
  - Solo un salto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



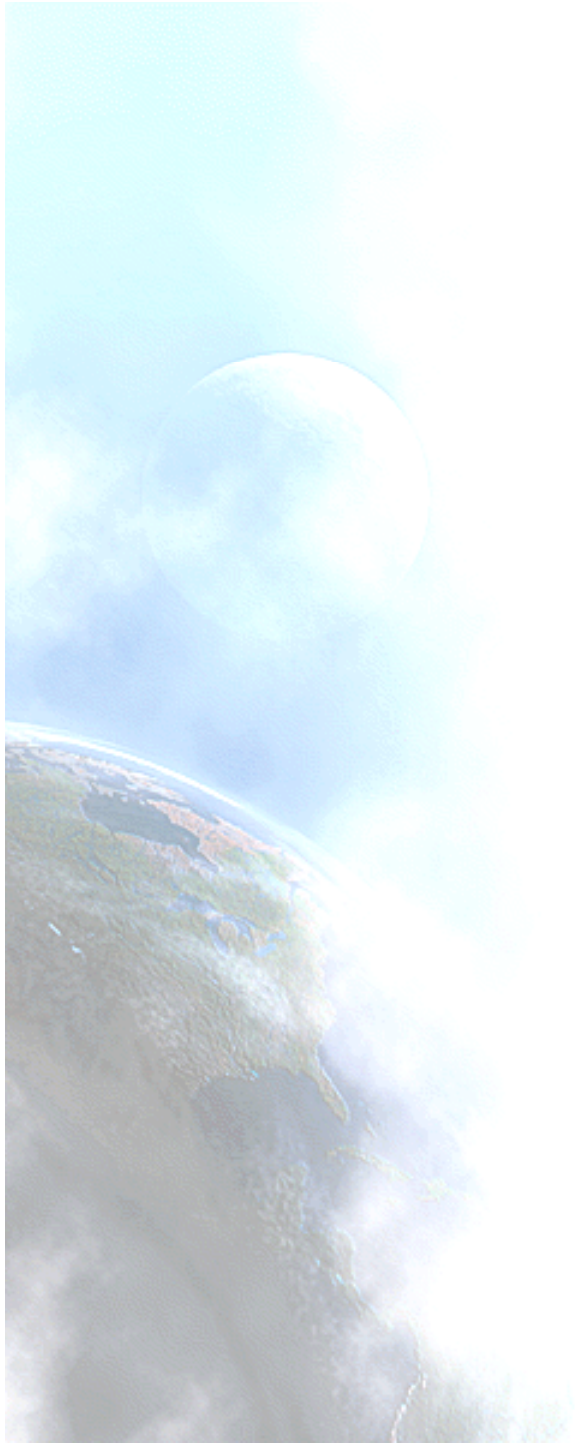
4. Tunnel Broker

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.

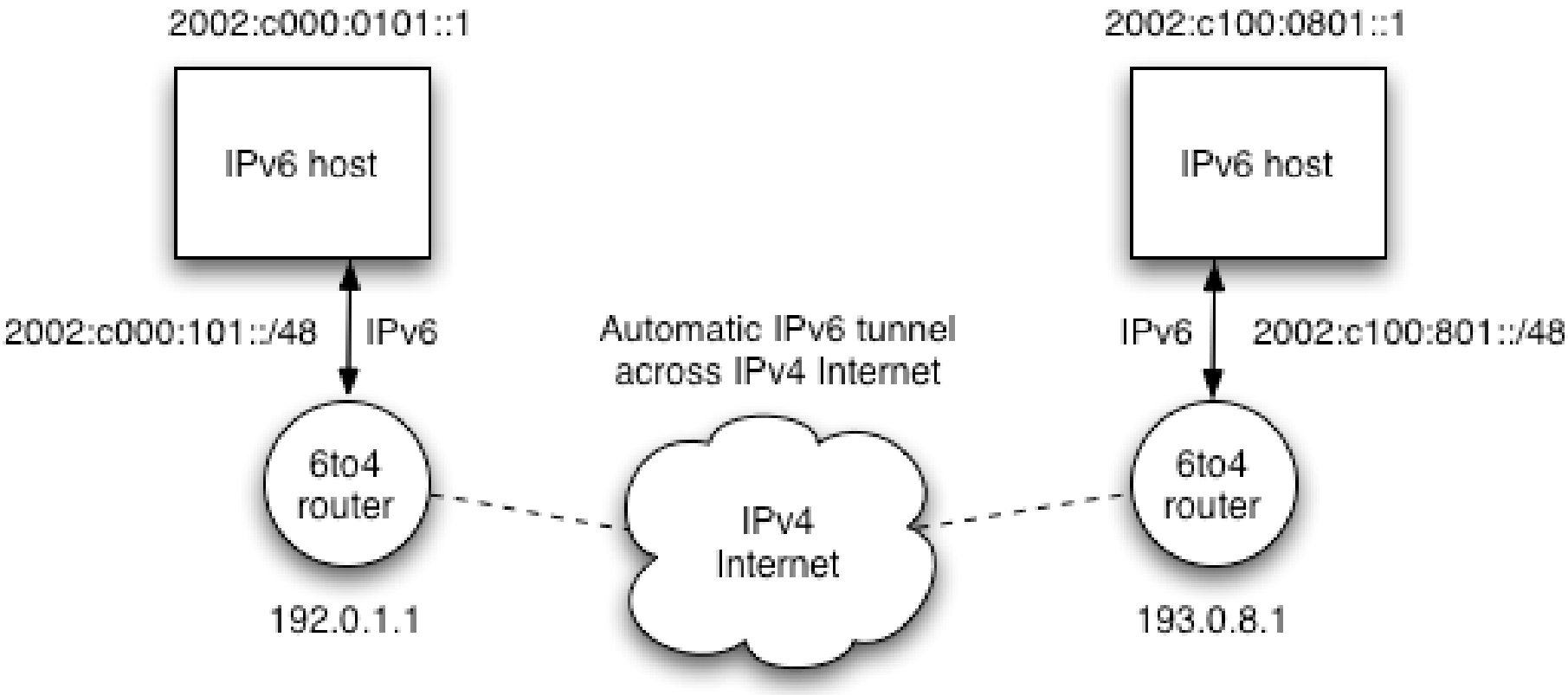


5. 6to4

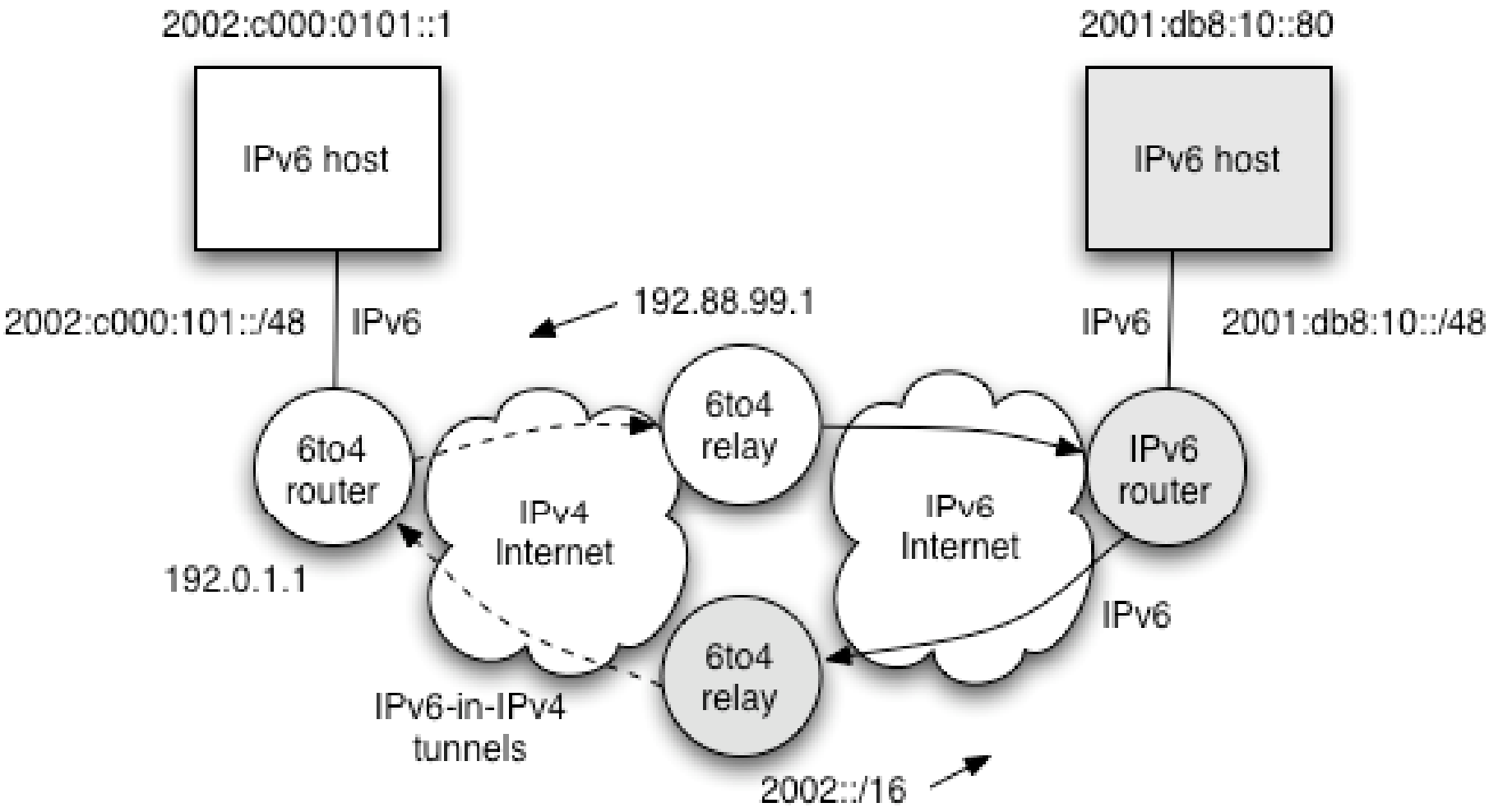
Túneles 6to4 (1)

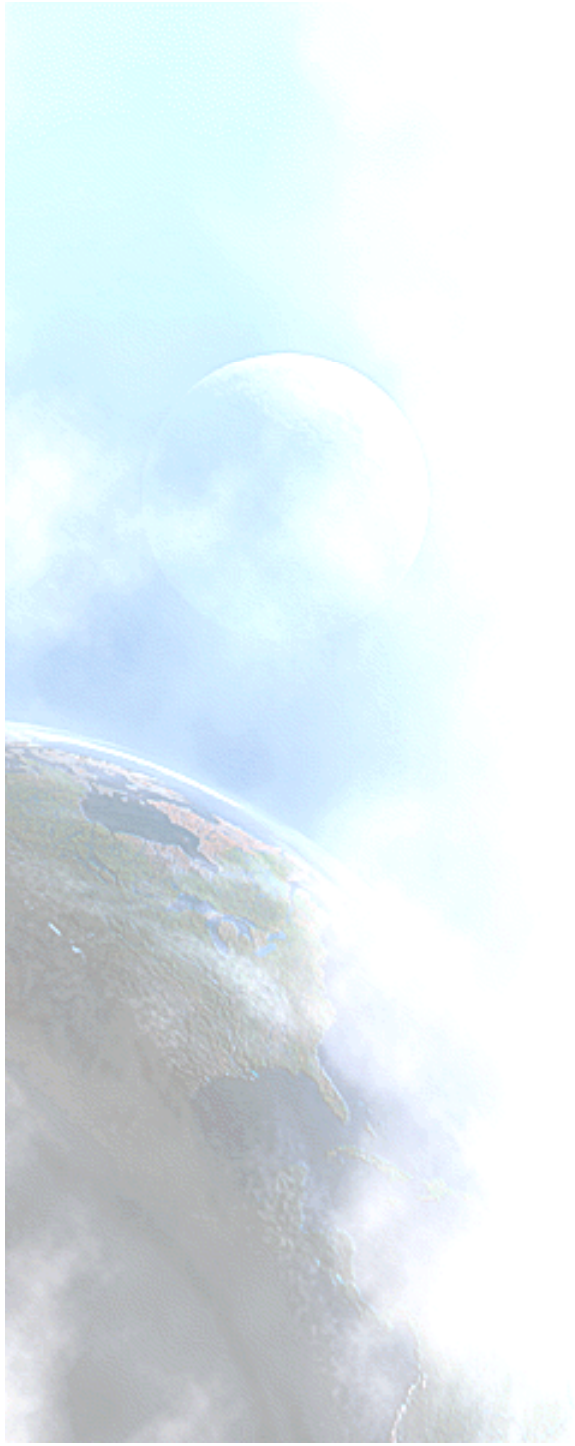
- Definido en RFC3056
- Se utiliza un “truco” para proporcionar direcciones 6to4.
  - Prefijo 6to4: 2002::/16
  - Se usa la IPv4 pública (p.e. 192.0.1.1) para siguientes 32 bits
  - Se obtiene así un prefijo /48 (p.e. 2002:C000:0101::/48)
- Cuando un router 6to4 ve un paquete hacia el prefijo **2002::/16**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



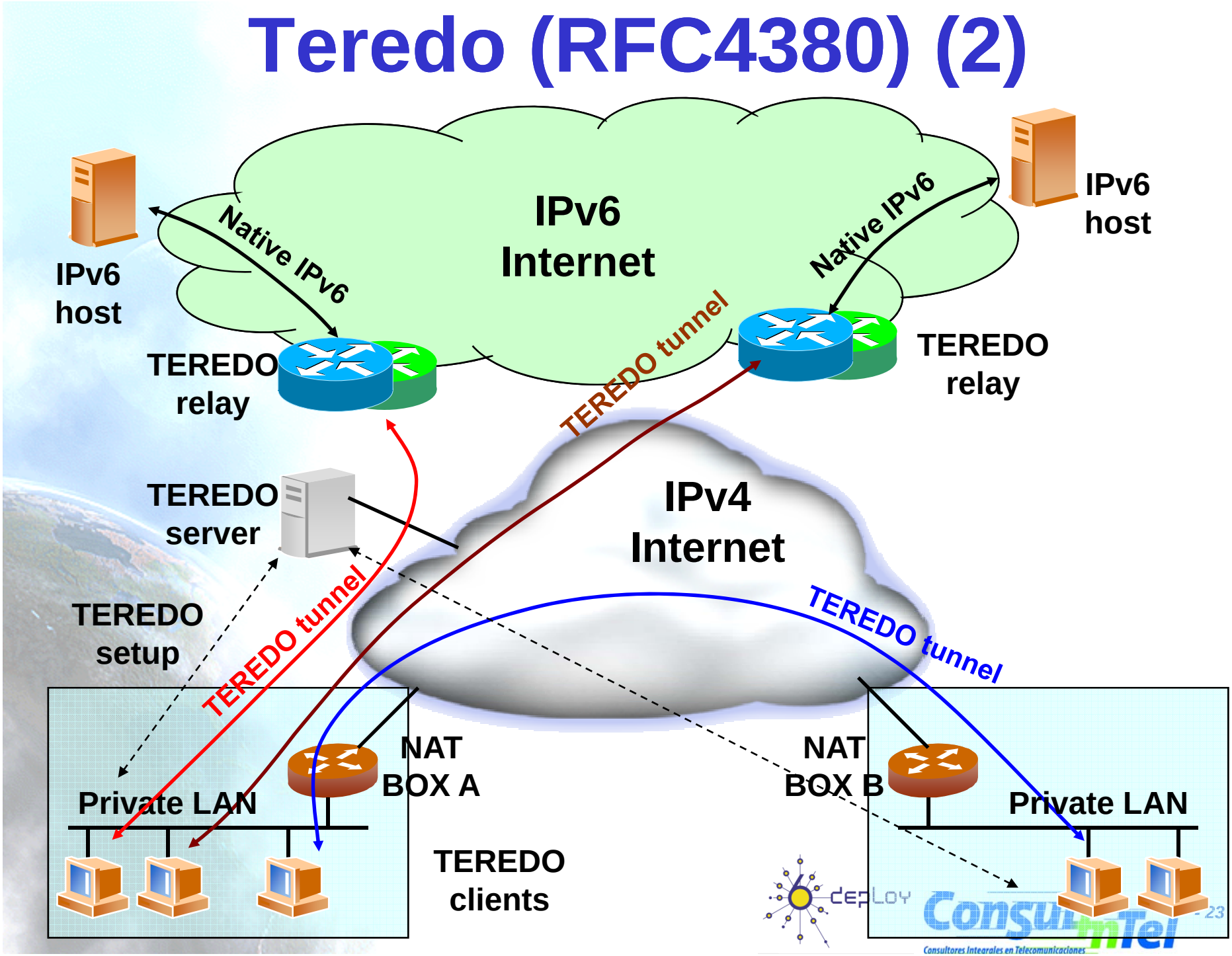


6. Teredo

Teredo (RFC4380) (1)

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

Teredo (RFC4380) (2)



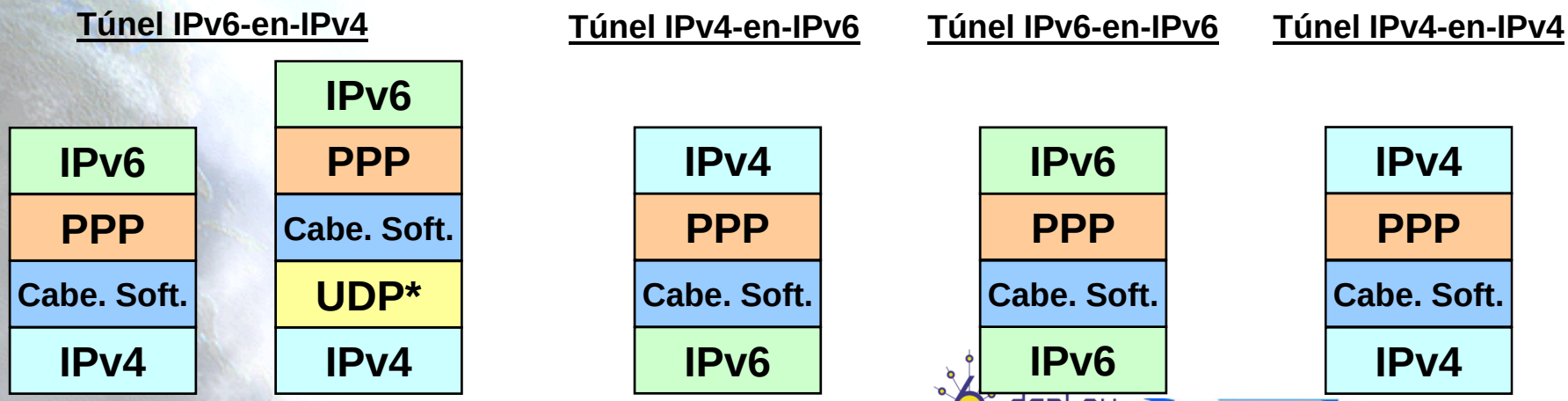
7. Softwires

Softwires

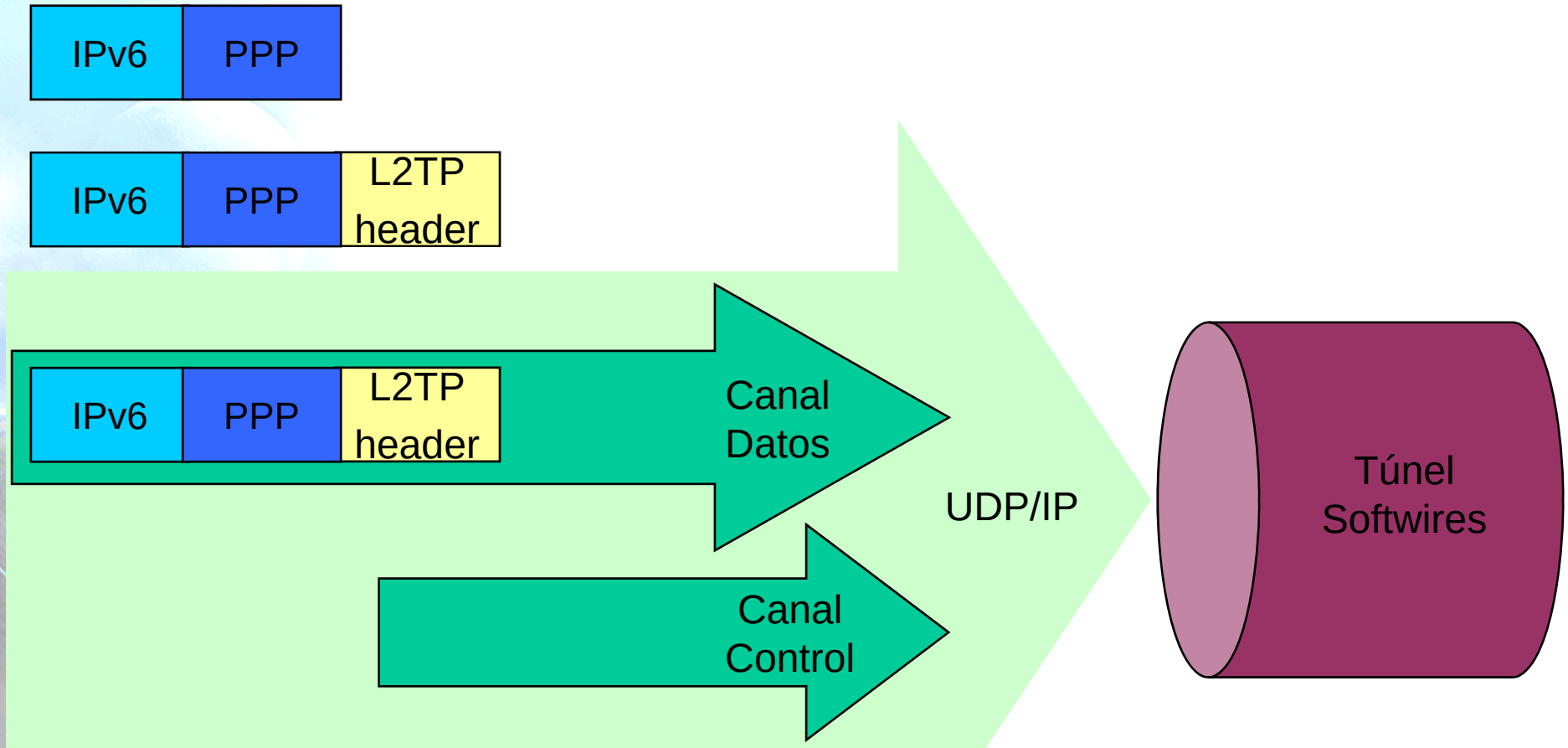
- Protocolo que esta siendo discutido en el grupo de trabajo Softwire del IETF. Presenta las siguientes características:
  - Mecanismo de transición “universal” basado en la creación de túneles
    - IPv6-en-IPv4, IPv6-en-IPv6, IPv4-en-IPv6, IPv4-en-IPv4
    - Permite atravesar NATs en las redes de acceso
    - 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
  - Posibilitará la provisión de conectividad IPv6 en dispositivos como routers ADSL, teléfonos móviles, PDAs, etc. cuando no exista conectividad IPv6 nativa en el acceso
  - También posibilita la provisión de conectividad IPv4 en dispositivos que solo tienen conectividad IPv6 nativa
- En realidad Softwires no es un nuevo protocolo, sino la definición de cómo usar de una forma diferente protocolos ya existentes con el fin de proporcionar conectividad IPv6 en redes IPv4 y viceversa
- Sofwires se basa en **L2TPv2** (RFC2661) y **L2TPv3** (RFC3991)

Encapsulamiento de Softwires basado en L2TPv2

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



Softwires basado en L2TPv2

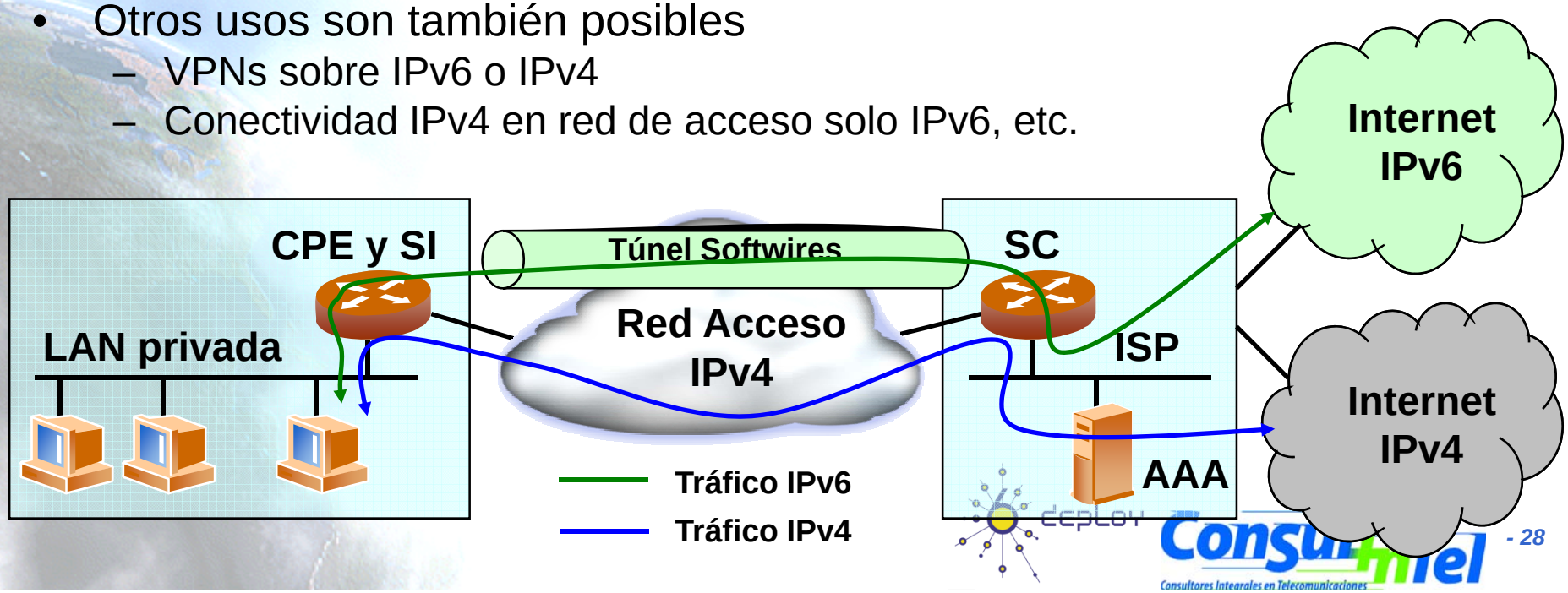


- Existe un plano de control y otro de datos
- Se usa PPP como protocolo de encapsulamiento

Ejemplo de uso de Softwires

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

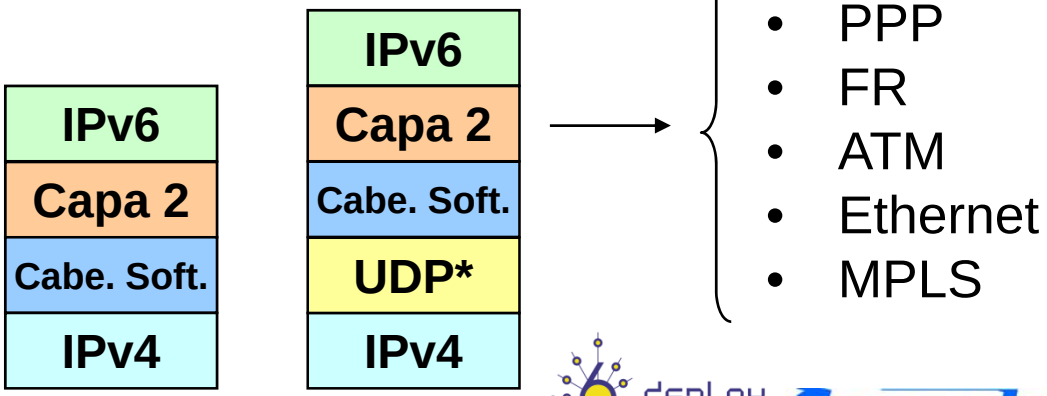
- Otros usos son también posibles
  - VPNs sobre IPv6 o IPv4
  - Conectividad IPv4 en red de acceso solo IPv6, etc.



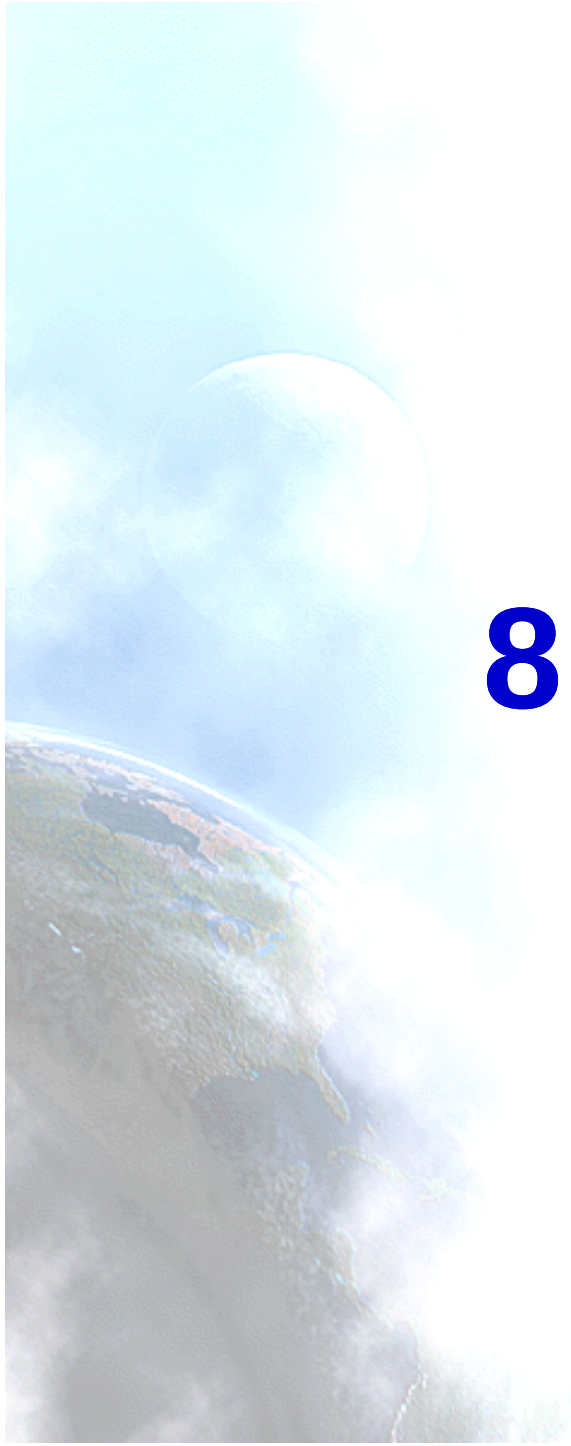
Encapsulamiento de Softwires basado en L2TPv3

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

Túnel IPv6-en-IPv4



*** Opcional**



8. Traducción

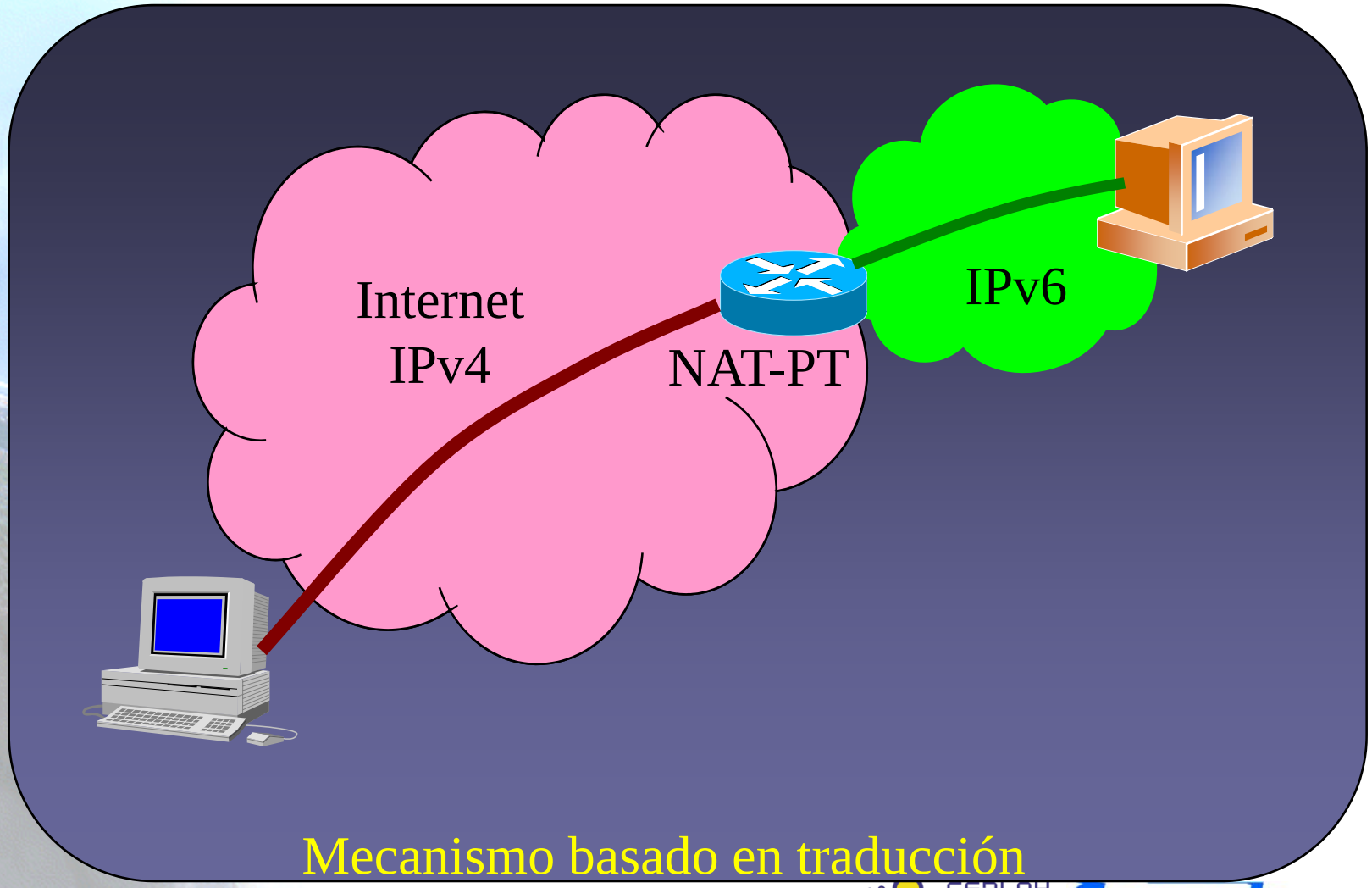
Traducción

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

Traducción IPv4/IPv6 (obsoleto) (1)

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

Traducción IPv4/IPv6 (obsoleto) (2)



Mecanismo basado en traducción

9. IPv6 sobre MPLS

IPv6 sobre MPLS (1)

- Cuando ya existe una red MPLS/IPv4 desplegada las siguientes estrategias son posibles:

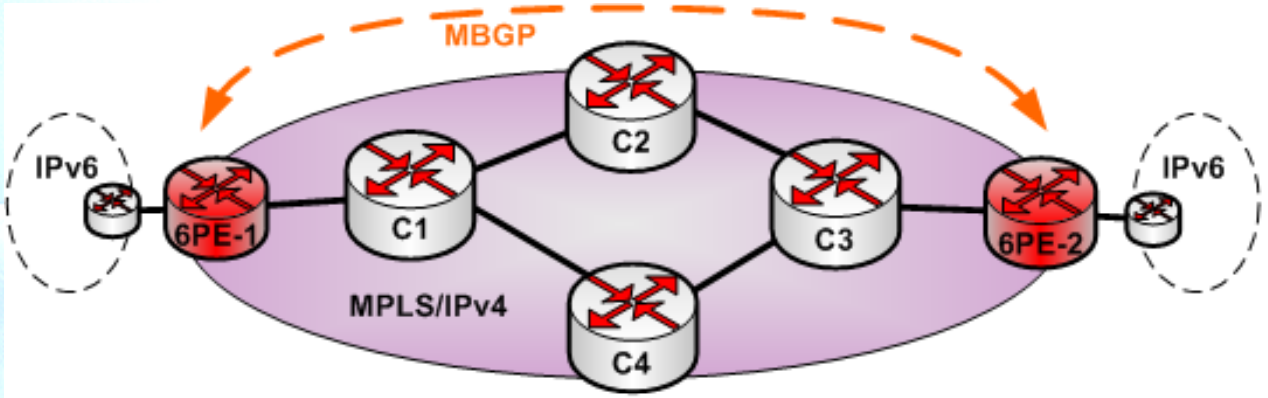
1. **Encaminamiento IPv6 nativo**: Sin hacer uso de MPLS. Está sujeto al soporte IPv6 disponible en todos los dispositivos de la red y requiere configuración de toda la red. No aprovecha las ventajas de MPLS.
2. **Encaminamiento IPv6 nativo y MPLS para IPv6**: Replicar el esquema existente MPLS/IPv4 para el tráfico IPv6. Está sujeto al soporte IPv6 y MPLS disponible en todos los dispositivos de la red y requiere configuración de toda la red.
3. **Aprovechar la infraestructura MPLS/IPv4** para el reenvío de tráfico IPv6: Bajo este esquema se pueden diferenciar varios métodos:

   3.1 IPv6 Provider Edge Routers (6PE): Los 6PE o encaminadores del borde de la nube MPLS/IPv4 deben ser de doble-pila y soportar Multiprotocol-BGP

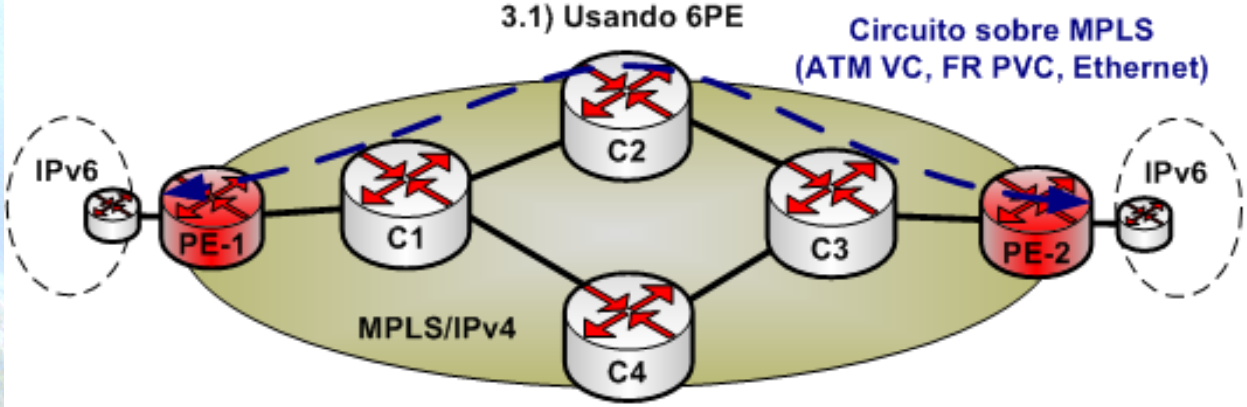
   3.2 Circuitos de Transporte sobre MPLS: Se crean interfaces dedicadas mediante circuitos estáticos configurados sobre MPLS (AToM – Any Transport over MPLS o EoMPLS – Ethernet over MPLS). No requiere cambios de configuración en los encaminadores de la nube MPLS/IPv4. Este es un mecanismo estático y no escalable.

   3.3 Túneles en los Encaminadores del Usuario: Los encaminadores de los usuarios son los encargados de establecer túneles IPv6-en-IPv4 entre las redes IPv6, de forma totalmente transparente a la red MPLS/IPv4. Este es un mecanismo estático y no escalable.

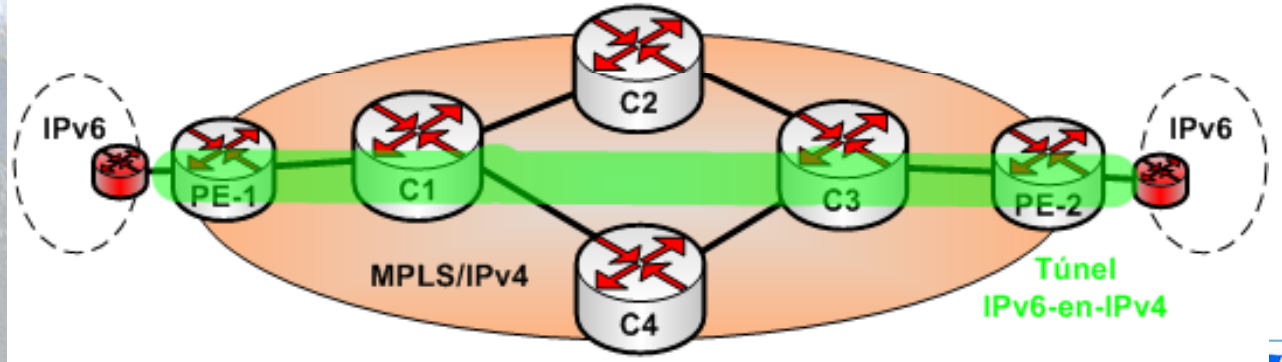
IPv6 sobre MPLS (2)



3.1) Usando 6PE



3.2) Usando Circuitos sobre MPLS

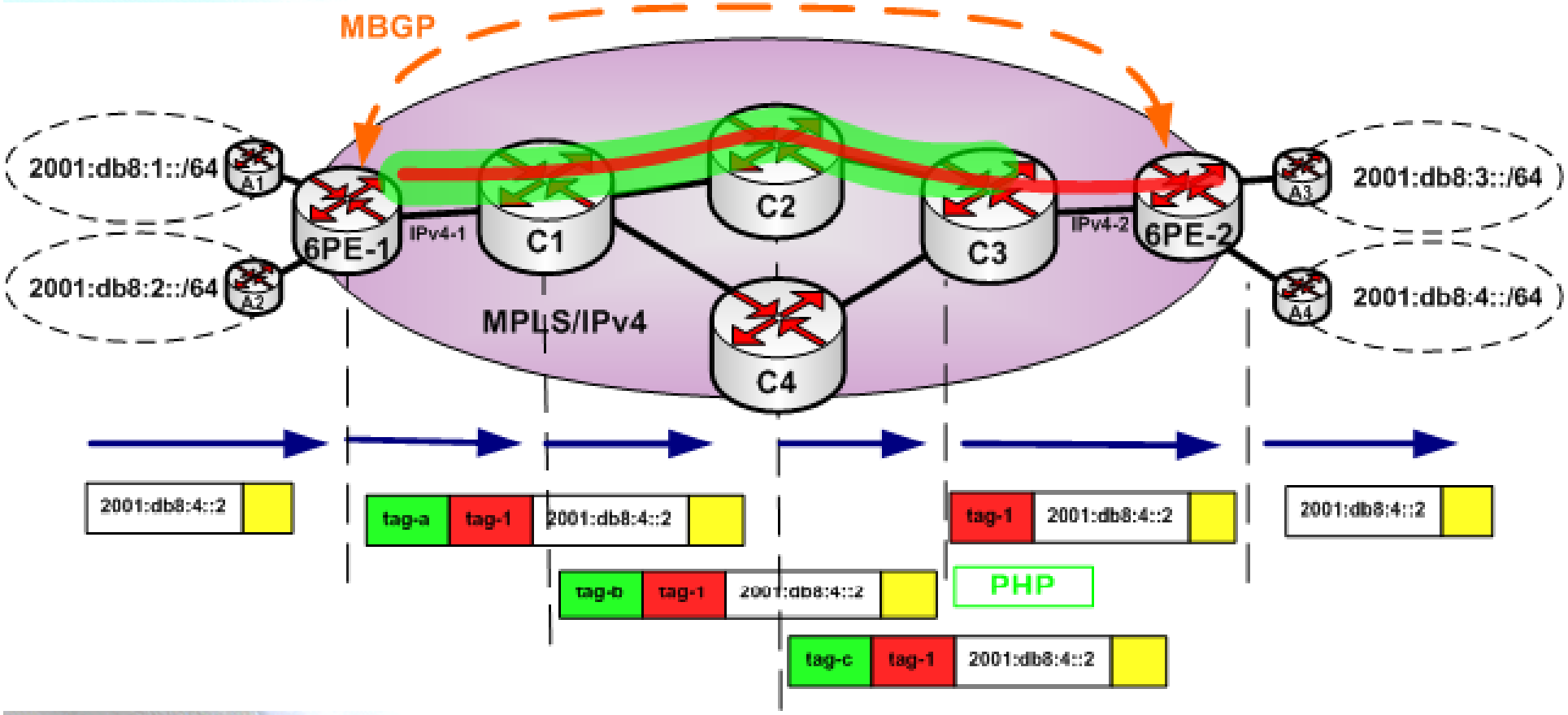


3.3) Usando Túneles desde los Usuarios

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

10. 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

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

Seguridad en túneles 6to4

- 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 TEREDO

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

Referencias Transición (1)

- [6in4] RFC1933, RFC4213
- [6to4] RFC3056
- [6over4] RFC2529
- [AYIYA] draft-massar-v6ops-ayiya-02
- [BIS] RFC2767
- [DSTM] draft-ietf-ngtrans-dstm-10
- [ISATAP] draft-ietf-ngtrans-isatap-24
- [NATPT] RFC2767
- [NATPTIMPL]
  - http://www.ipv6.or.kr/english/download.htm ==> Linux 2.4.0
  - http://www.ispras.ru/~ipv6/index_en.html ==> Linux y FreeBSD
  - http://research.microsoft.com/msripv6/napt.htm Microsoft
  - ftp://ftp.kame.net/pub/kame/snap/kame-20020722-freebsd46-snap.tgz ==> KAME snapshot (22.7.2002)
  - http://ultima.ipv6.bt.com/
- [PRIVACY] RFC3041
- [PROTO41] draft-palet-v6ops-proto41-nat
- [SIIT] RFC2765
- [SILKROAD] draft-liumin-v6ops-silkroad-02

Referencias Transición (2)

- [SOCKSv64] RFC3089
- [SOFTWIRES] draft-ietf-softwire-hs-framework-l2tpv2
- [STATELESS] RFC2462
- [STATEFUL] RFC3315
- [STUN] RFC3489
- [TB] RFC3053
- [TEREDO] RFC4380
- [TEREDOC] http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx
- [TRT] RFC3142
- [TSP] draft-vg-ngtrans-tsp-01, http://www.hexago.com/index.php?pgID=step1
- [TunAut] RFC1933
- Windows IPv6
  - http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_ip_v6_add_utils.mspx
  - http://www.microsoft.com/technet/community/columns/cableguy/cg0902.mspx

Gracias !

Contacto:

- Jordi Palet Martínez (Consulintel): jordi.palet@consulintel.es
- Alvaro Vives Martínez (Consulintel): alvaro.vives@consulintel.es

6DEPLOY Project

http://www.6deploy.org

The IPv6 Portal:

http://www.ipv6tf.org