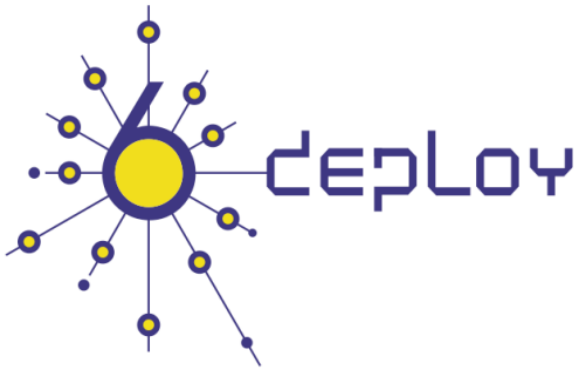
IPv6 Básico
Introducción
LACNIC XVIII / LACNOG 2012
Montevideo
28 Octubre 2012



Alvaro Vives (alvaro.vives@consulintel.es)

Agenda

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

1. Introducción a IPv6

¿Porque un Nuevo Protocolo de Internet?

Un único motivo lo impulsó: Más direcciones!

- Para miles de millones de nuevos dispositivos, como teléfonos celulares, PDAs, dispositivos de consumo, coches, etc.
- Para miles de millones de nuevos usuarios, como China, India, etc.
- Para tecnologías de acceso “always-on”, como xDSL, cable, PLC, fibra, ethernet, etc.

Hechos Históricos

- **1983** : Red investigación con ~100 computadoras
- **1991 Nov.**: IETF crea un working group para evaluar y buscar soluciones al agotamiento de direcciones
- **1992**: Actividad Comercial, crecimiento exponencial
- **1992 Julio** : IETF determina que era esencial comenzar a crear el next-generation Internet Protocol (IPng)
- **1993** : Agotamiento de direcciones clase B. Previsión de colapso de la red para 1994!
- **1993 Sept.**: RFC 1519, “Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy”
- **1994 Mayo**: RFC 1631, “The IP Network Address Translator (NAT)”
- **1995 Dic.**: Primer RFC de IPv6: “Internet Protocol, Version 6 (IPv6) Specification”, RFC 1883
- **1996 Feb.**: RFC 1918, “Address Allocation for Private Internets”
- **1998 Dic.**: RFC 2460 Obsoleted RFC1883. Especificación IPv6 actual

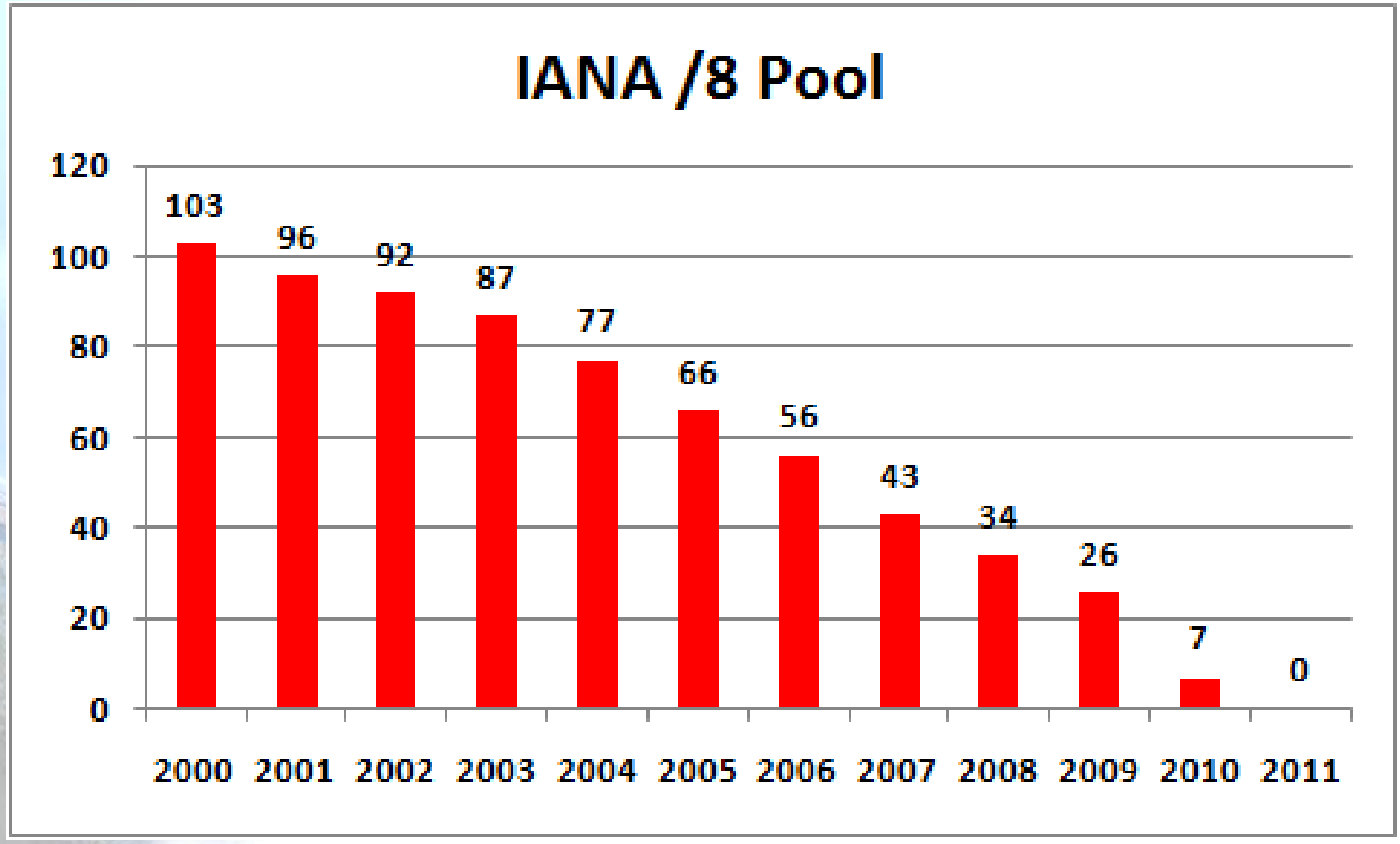
Agotamiento Direcciones IPv4 (1)

- Opinión extendida: quedan pocos años de direcciones IPv4 públicas -> Debate: Cuando se agotarán?
- Tres estrategias a seguir:
  - Aumentar el uso de NAT -> **introduce problemas técnicos y costes**
  - Tratar de obtener direcciones IPv4 libres o liberadas
  - Implementar IPv6 -> **válida a largo plazo**
- Existen múltiples comunicados de los actores de Internet recomendando la implementación de IPv6 debido al agotamiento de direcciones IPv4:
- The IPv6 Portal: Policy Recommendations: http://www.ipv6tf.org/index.php?page=meet/policy_recommendations

Agotamiento Direcciones IPv4 (2)

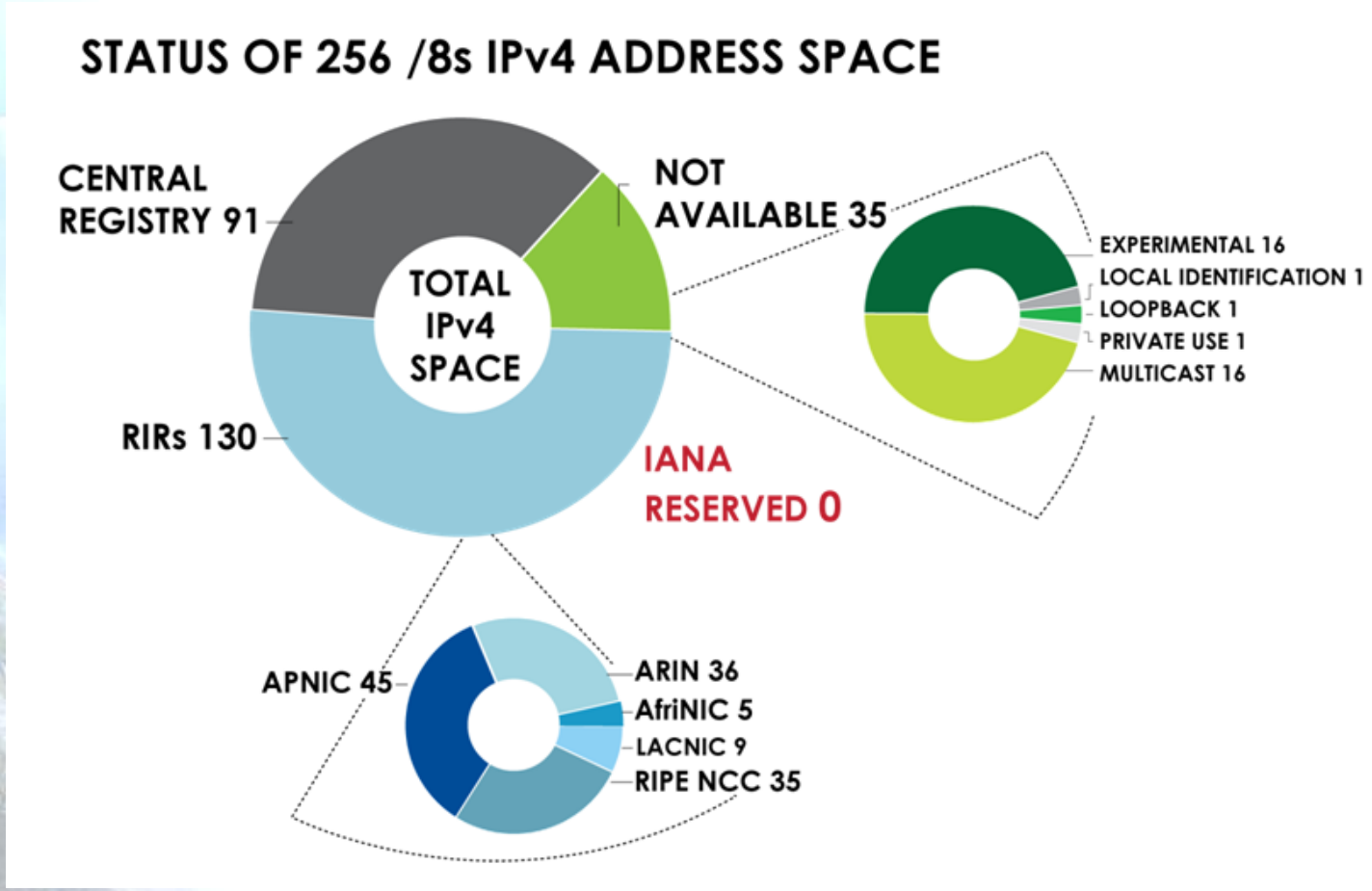
- RIRs: Registros regionales reciben de IANA y dan a ISPs

Agotamiento Direcciones IPv4 (3)



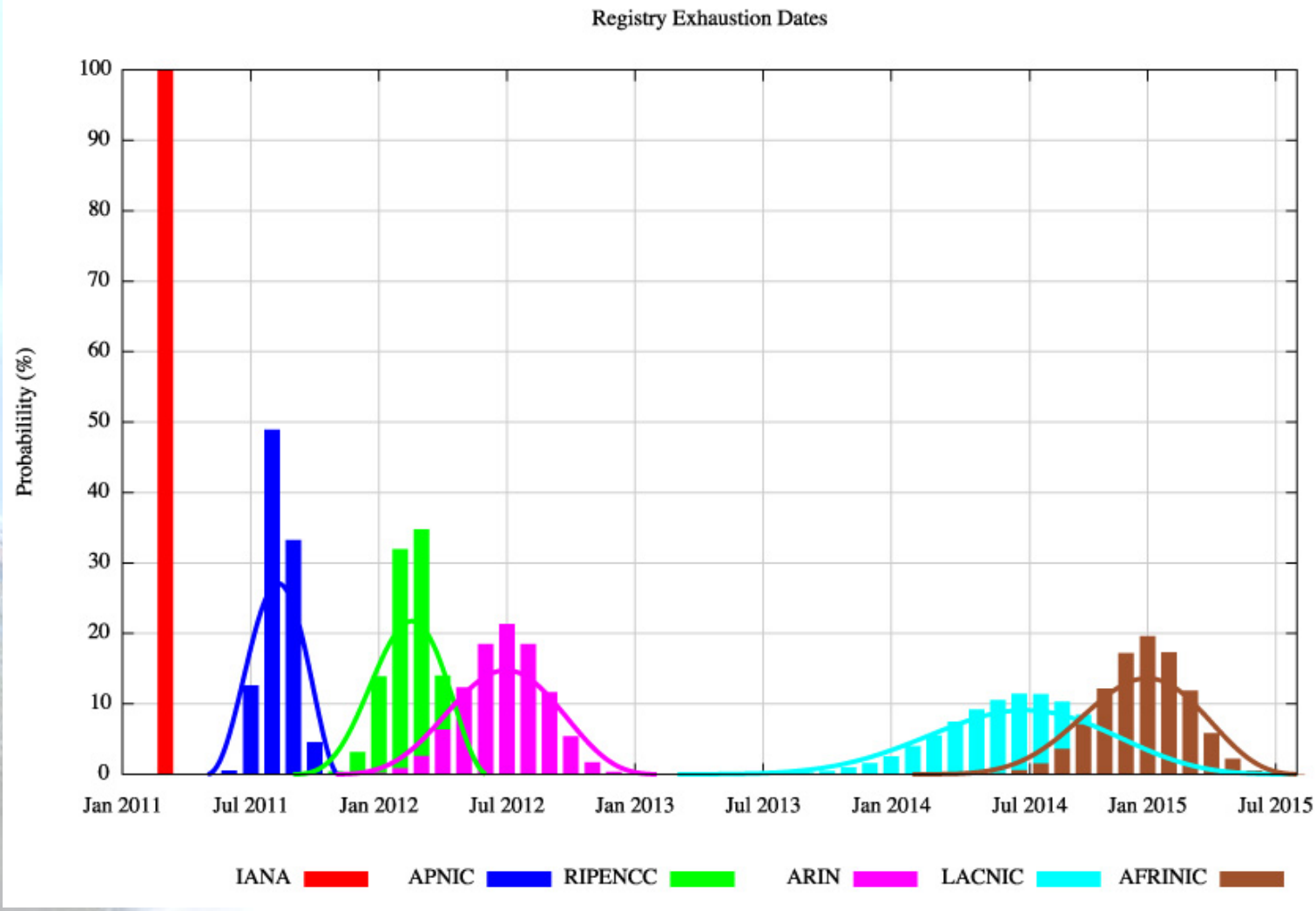
- 3 Febrero 2011 se agotó el pool de IPv4 de IANA

Agotamiento Direcciones IPv4 (4)



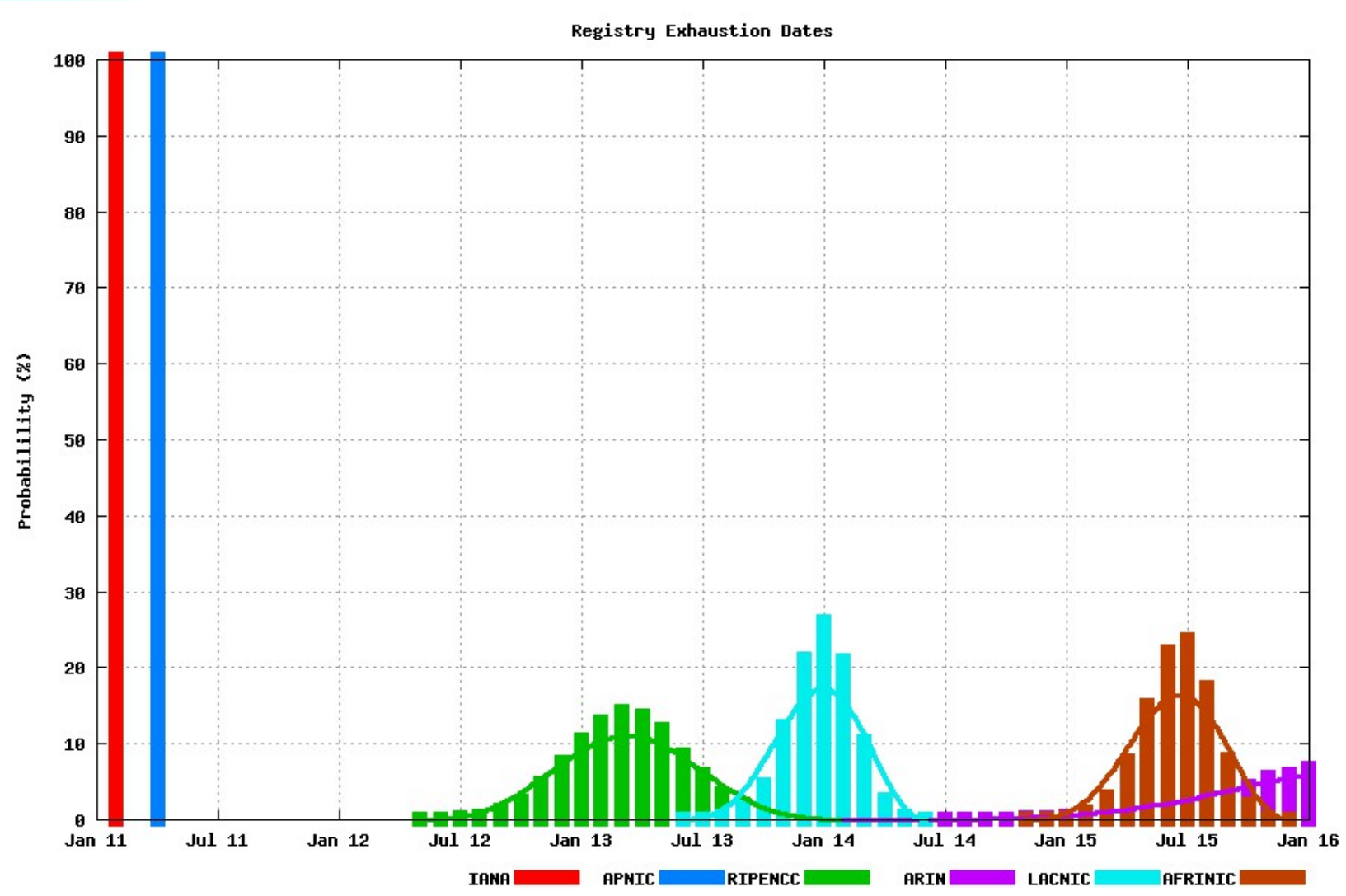
Fuente http://www.nro.net a 31 de Marzo 2011

Agotamiento Direcciones IPv4 (5)



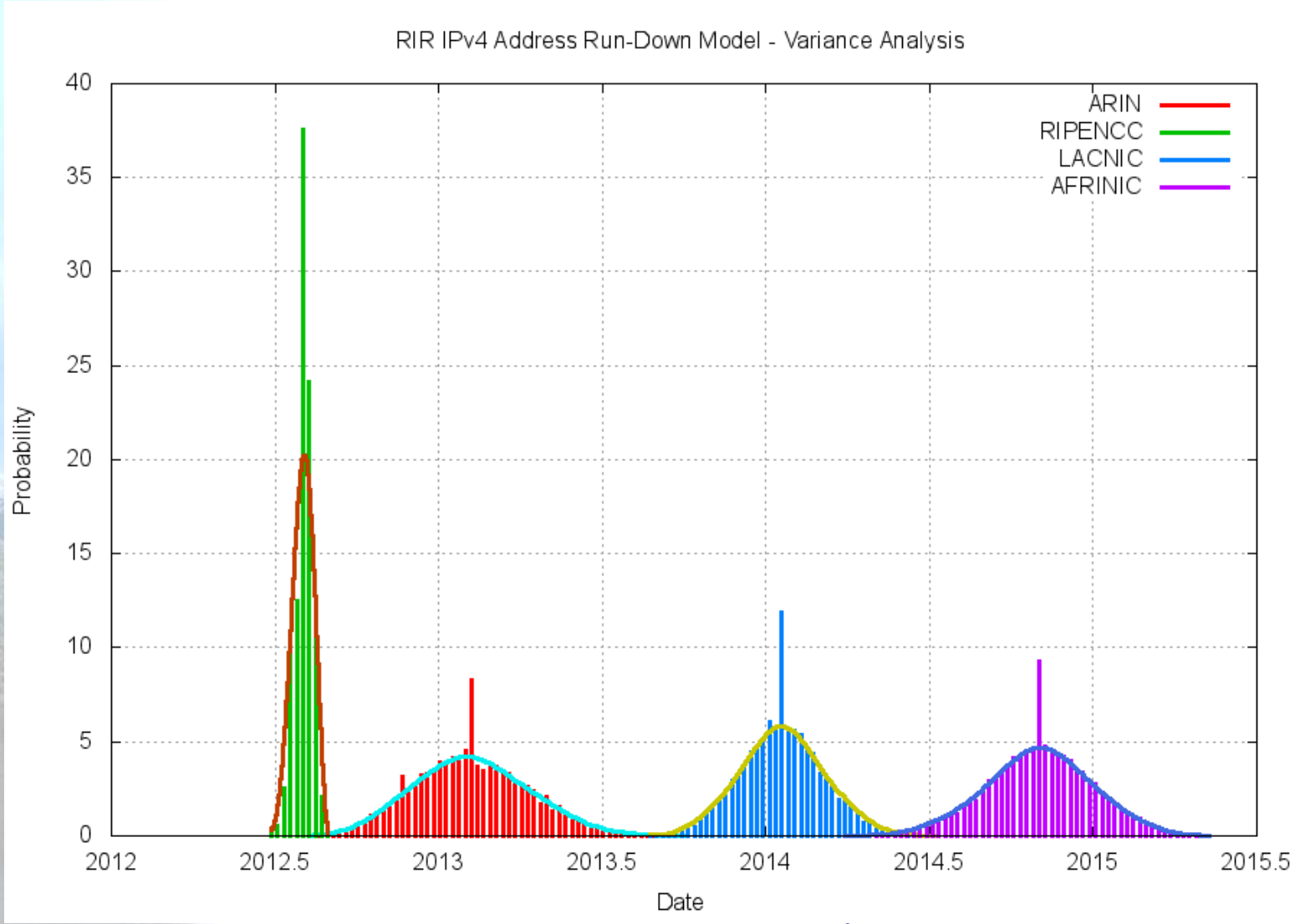
http://www.potaroo.net/tools/ipv4/rir.jpg (24-02-2011)

Agotamiento Direcciones IPv4 (6)



http://www.potaroo.net/tools/ipv4/rir.jpg (4-10-2011)

Agotamiento Direcciones IPv4 (7)

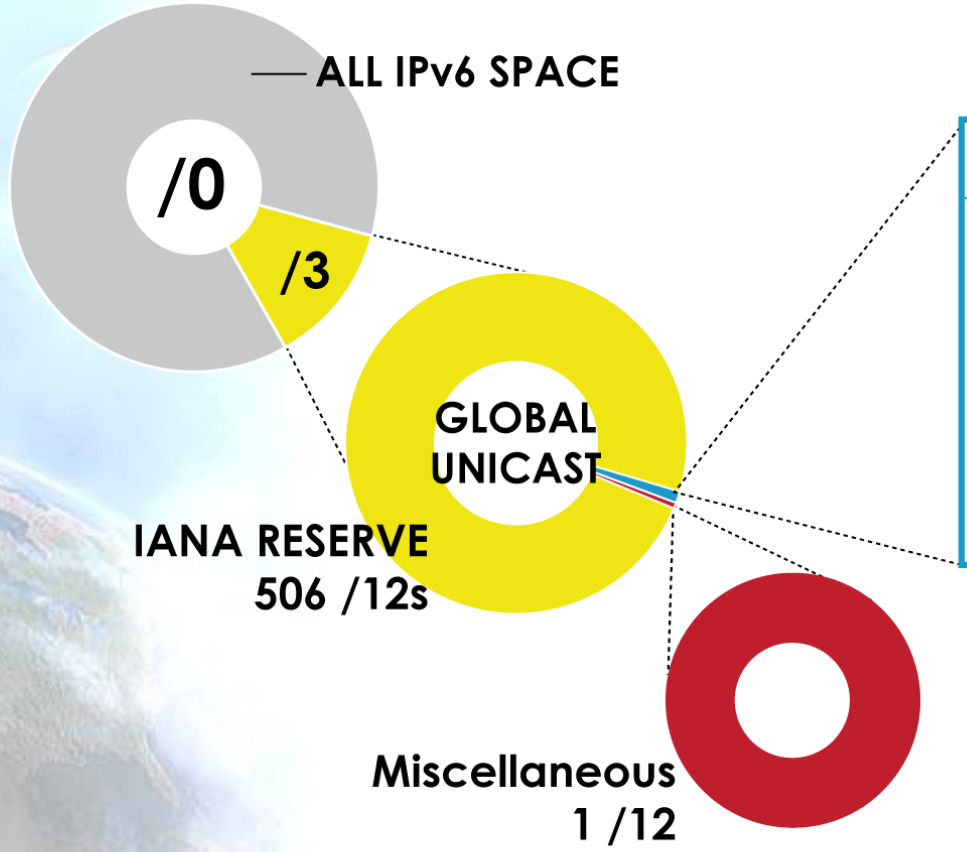


http://www.potaroo.net/tools/ipv4/plotvar.png (26-7-2012)

¿Cuándo se produce el agotamiento real?

- ¡Ya esta ocurriendo!
  - El 19 de Abril 2011 en Asia Pacífico (APNIC)
  - El 14 de Septiembre 2012 (RIPE NCC)
  - Aproximadamente 10 meses después en Norteamérica (ARIN)
  - En 18-24 meses en Latinoamérica y Caribe (LACNIC)
  - En 24-30 meses en África (AfriNIC)

Direcciones IPv6



RIRs 5 /12s (October 2006)

RIR	IPv6 ADDRESS
AfriNIC	2C00:0000::/12
APNIC	2400:0000::/12
ARIN	2600:0000::/12
LACNIC	2800:0000::/12
RIPE NCC	2A00:0000::/12

Fuente http://www.nro.net a 31 de Marzo 2011

Ventajas Adicionales con Direcciones Mayores

- Facilidad para la auto-configuración
- Facilidad para la gestión/delegación de las direcciones
- Espacio para más niveles de jerarquía y para la agregación de rutas
- Habilidad para las comunicaciones extremo-a-extremo con IPsec (porque no necesitamos NATs)

2. Formatos de cabeceras y tamaño de paquetes

2.1 Formato cabecera IPv6

2.2 Cabeceras de Extensión

2.3 MTU

2.4 Fragmentación

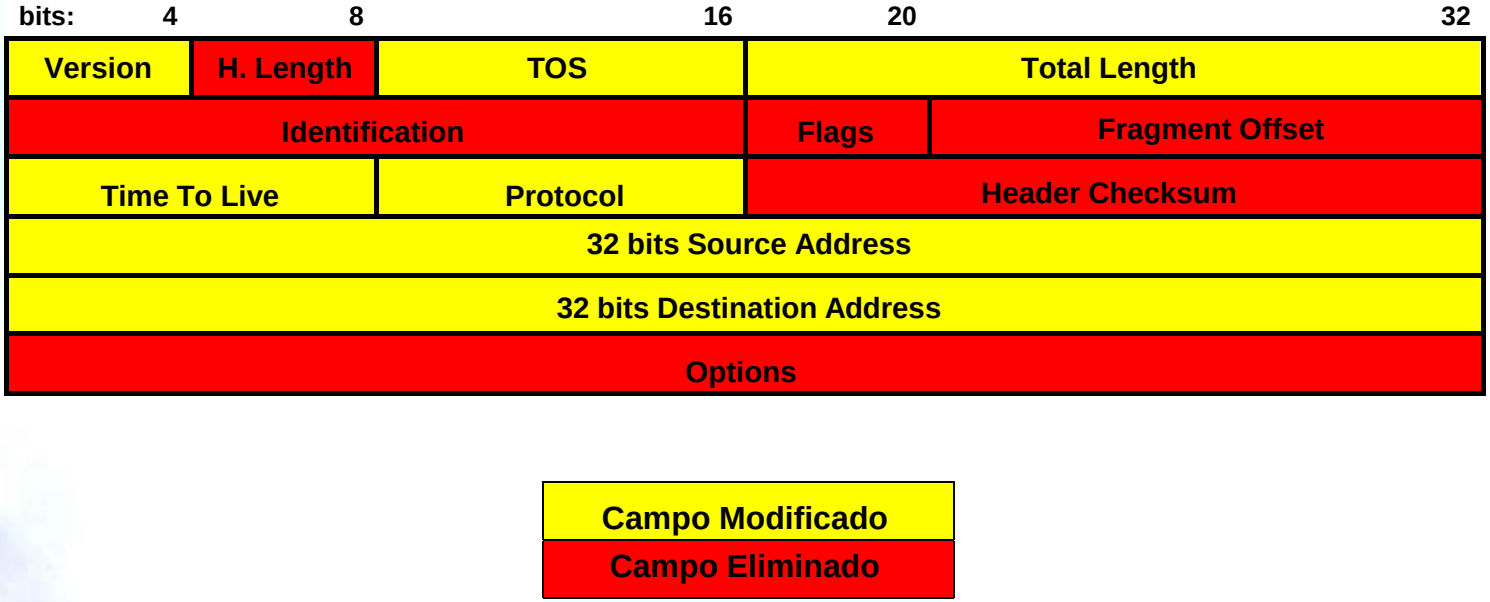
IPv6 (RFC2460)

- 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

2.1 Formato cabecera IPv6

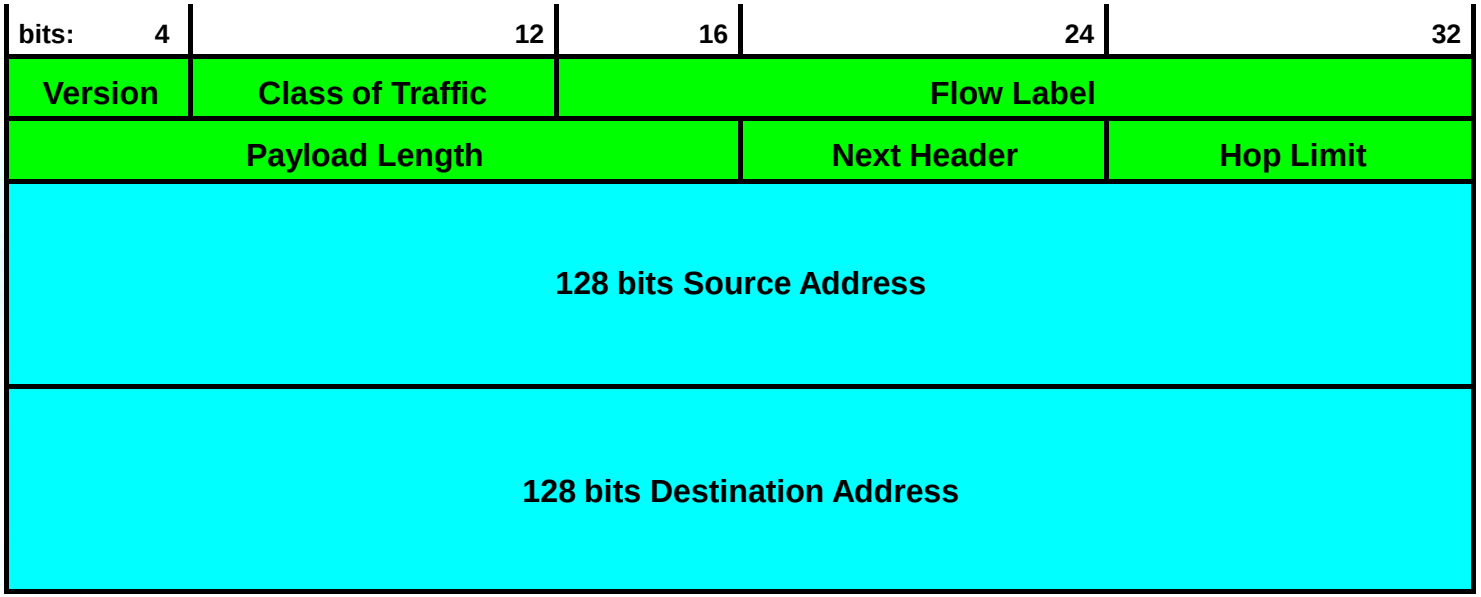
Formato de la Cabecera IPv4

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



Formato de la Cabecera IPv6

- Reducción de 12 a 8 campos (40 bytes)



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

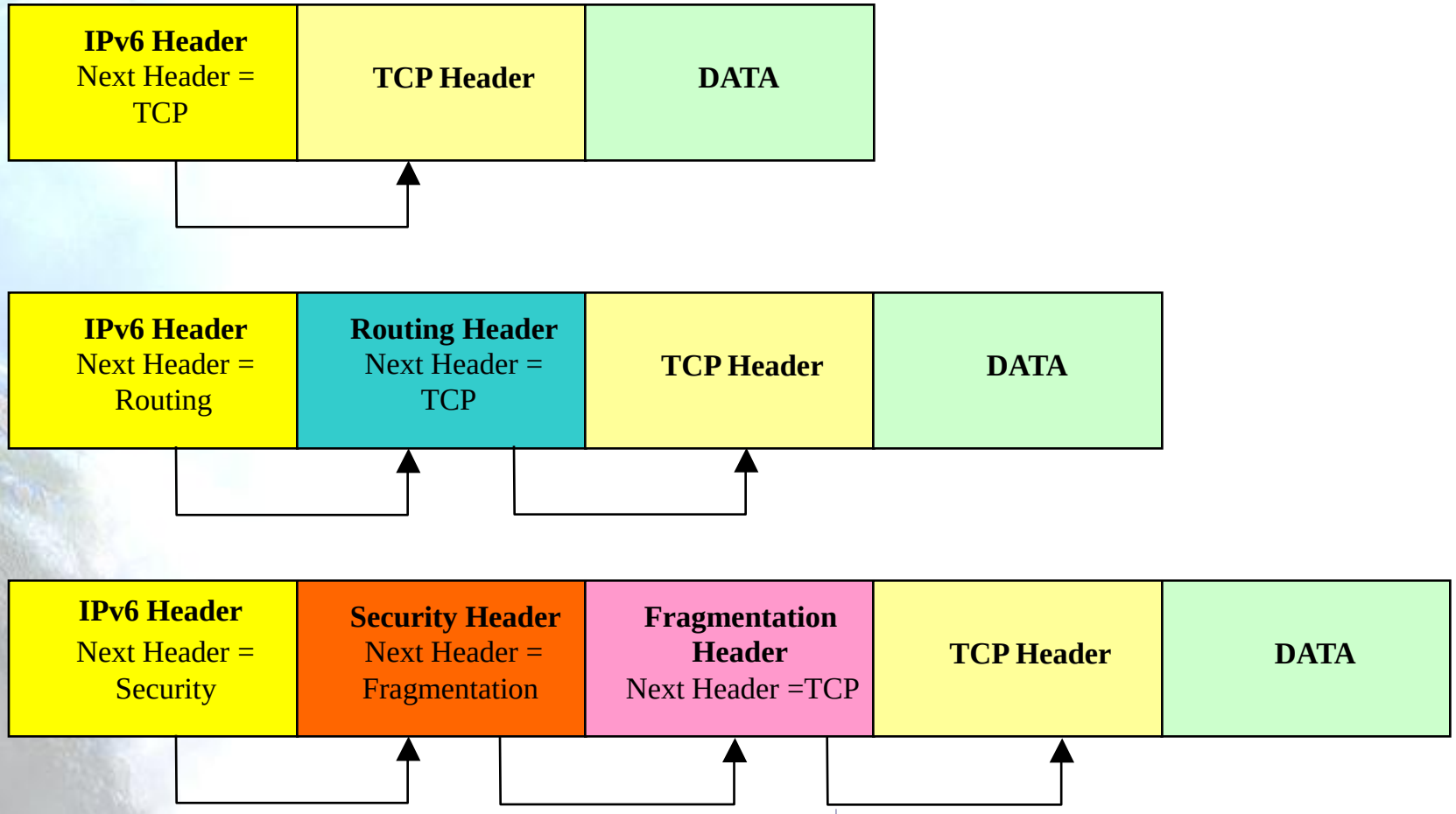
Resumen de los cambios de la Cabecera

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

2.2 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)

2.3 MTU

MTU Mínimo

- Link MTU:
  - El máximo MTU del link, es decir, el tamaño máximo del paquete IP que puede transmitirse sobre el link.
- Path MTU:
  - El mínimo MTU de todos los links en la ruta desde el nodo origen hasta el nodo destino.
- El mínimo link MTU para IPv6 es de 1280 bytes en vez de 68 bytes como en el caso de IPv4.
- En links donde Path MTU < 1280, es necesario usar fragmentación y reensamblado en el nivel de enlace.
- En links donde se puede configurar el MTU, se recomienda usar el valor de 1500 bytes.

2.4 Fragmentación

Cabecera de Fragmentación

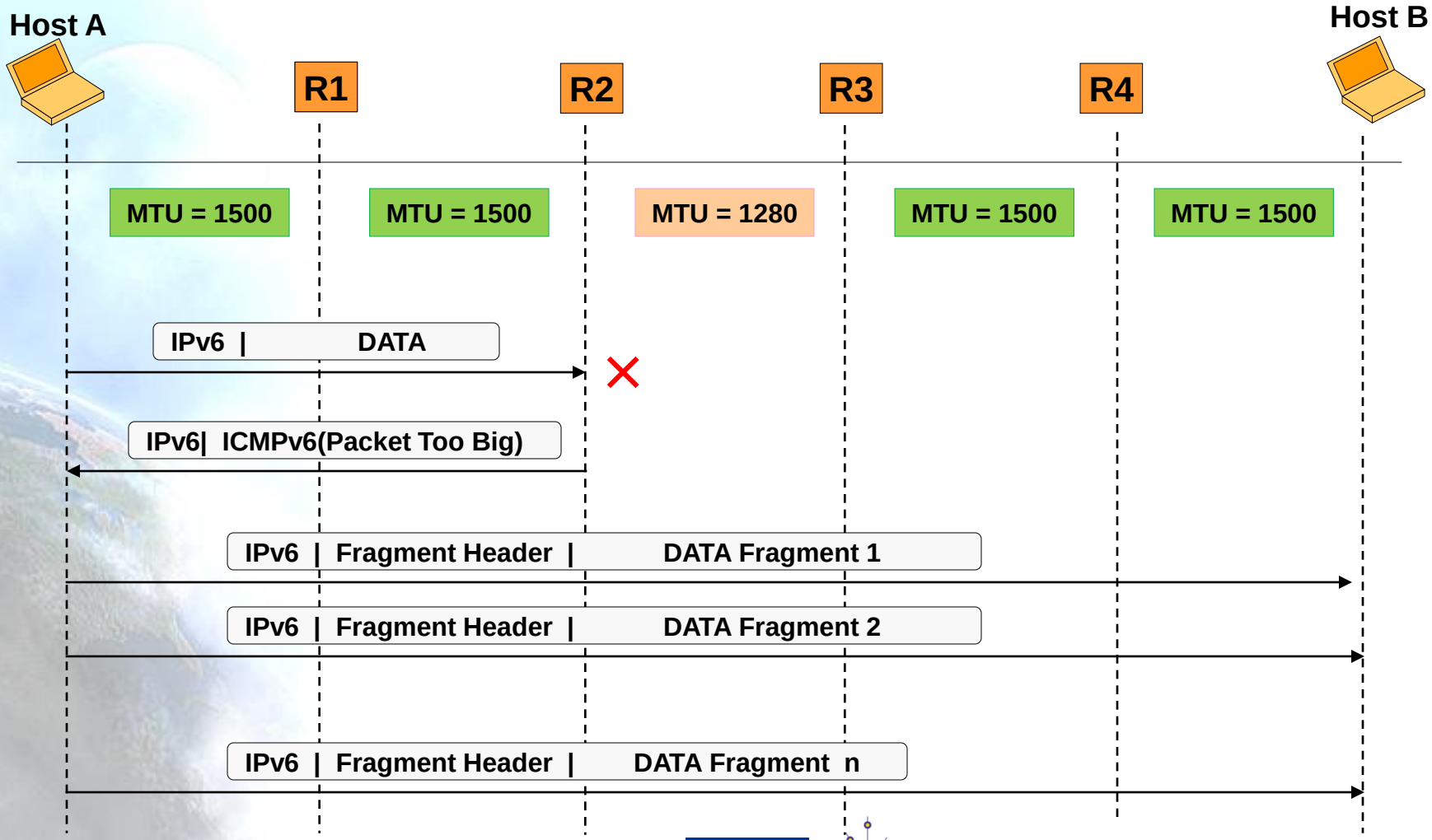
- Se emplea cuando el paquete que se desea transmitir es mayor que el Path MTU existente hacia el destino
- En IPv6 la fragmentación se realiza en el origen, nunca en los nodos intermedios
- Next Header = 44

8 bits	8 bits	13 bits unsigned	2 bits	1 bit
Next Header	**Reserved = 0**	**Fragment Offset**	**Res. = 0**	**M**
Identification				

- Paquete Original (no fragmentado):

Unfragmentable Part	**Fragmentable Part**

Fragmentación en Origen



3. Direccionamiento IPv6

3.1 Tipos de Direcciones
3.2 Prefijo y representación
3.3 Direcciones IPv6 Unique Local
3.4 Identificadores de interfaz
3.5 Direcciones Multicast
3.6 Plan de direccionamiento
3.7 Gestión de direcciones
3.8 Ejercicios con direcciones

3.1 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

3.2 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**
5. No se distinguen mayúsculas/minúsculas

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

Representación Textual de las Direcciones (3)

Se ha visto que hay mucha “flexibilidad” a la hora de representar direcciones, lo que puede acarrear problemas:

1. Al realizar búsquedas de direcciones
2. Al comprobar configuraciones o ficheros de logs
3. Verificaciones hechas por algunos protocolos, por ejemplo certificados X.509 que incluyan direcciones

[RFC5952] da recomendaciones:

1. Eliminar siempre ceros a la izda en un grupo de 16 bits
2. Usar “::” para comprimir al máximo, NO usarlo para un solo grupo de ceros
3. Usar minúsculas para las letras hexadecimales

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

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**
- (IPv4: 192.0.2.0/24 [RFC5735] Jan 2010)

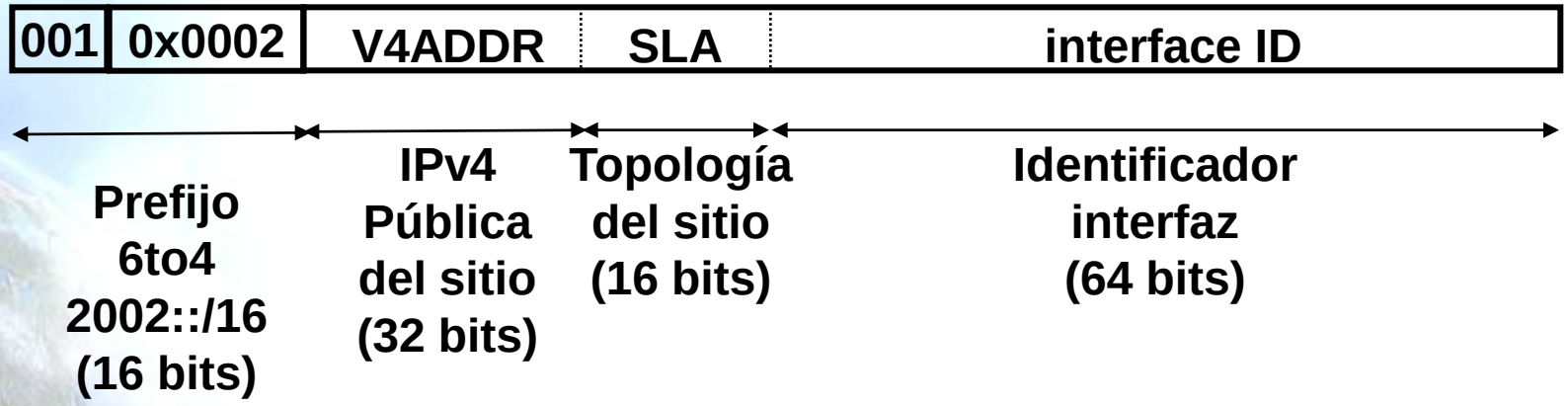
Prefijos Globales Unicast

Tipo de Dirección	Prefijo Binario
IPv4-compatible	0000...0 (96 zero bits) (desaprobada)
IPv4-mapped	00…0FFFF (80 zero+ 16 one bits)
Global unicast	001
ULA	1111 110x (1= Asignado localmente) (0=Asignado centralmente)

- El prefijo **2000::/3** se esta usando para las asignaciones de direcciones Globales Unicast, todos los demás prefijos están reservados (aprox. 7/8 del total).

Direcciones 6to4 (RFC3056)

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



Direcciones Link-Local y Site-Local

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

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

3.3 Direcciones IPv6 Unique Local

Unique Local IPv6 Unicast Addresses - IPv6 ULA (RFC4193)

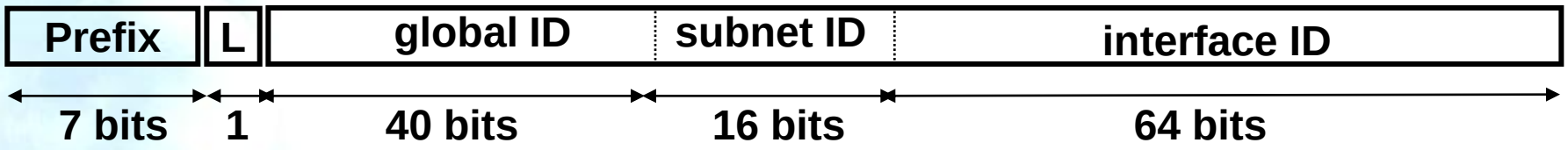
- Prefijo global con alta probabilidad de ser único
- Para comunicaciones locales, normalmente dentro de un “site”
- No son prefijos que vayan a ser encaminados en la Internet Global
- Son prefijos encaminables dentro de un área más limitada, como un determinado “site”
- Incluso podrían ser encaminados entre un conjunto limitado de “sites”
- Direcciones locales localmente asignadas
  - vs direcciones locales centralmente asignadas

Características IPv6 ULA

- Prefijos “bien-conocidos” que facilitan su filtrado en las fronteras de los “sites”
- Son independientes del ISP y se pueden usar para comunicaciones dentro de un “site” que tiene conectividad a Internet intermitente o incluso no tiene
- Si el prefijo se extiende accidentalmente fuera del “site”, vía routing o DNS, no hay ningún conflicto con otras direcciones
- En la práctica, las aplicaciones pues tratar estas direcciones como direcciones de ámbito global

Formato IPv6 ULA

- Formato:

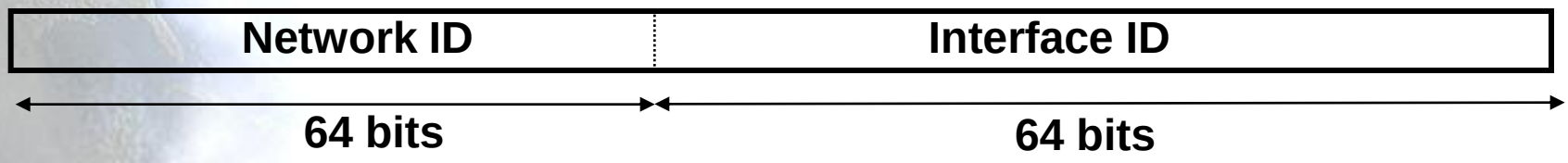


- FC00::/7 Prefijo indicativo de direcciones unicast IPv6 locales
- L = 1 se asigna localmente
- L = 0 Según el RFC4193 puede ser definido en el futuro. En la práctica se usa para especificar asignaciones centrales
- ULA se crea usando una asignación pseudo-aleatorio para el ID global
  - Esto asegura que no hay ninguna relación entre las asignaciones y deja claro que estos prefijos no son para ser encaminados globalmente

3.4 Identificadores de interfaz

Identificadores de Interfaz (1)

- Los identificadores de interfaz (IID) de una dirección IPv6 Unicast se usan para identificar interfaces en un enlace
- Deben ser únicos en una subred
- Hay IIDs o rangos de IID definidos para usos concretos y no deben ser usados por un nodo IPv6 (ver [RFC5453]



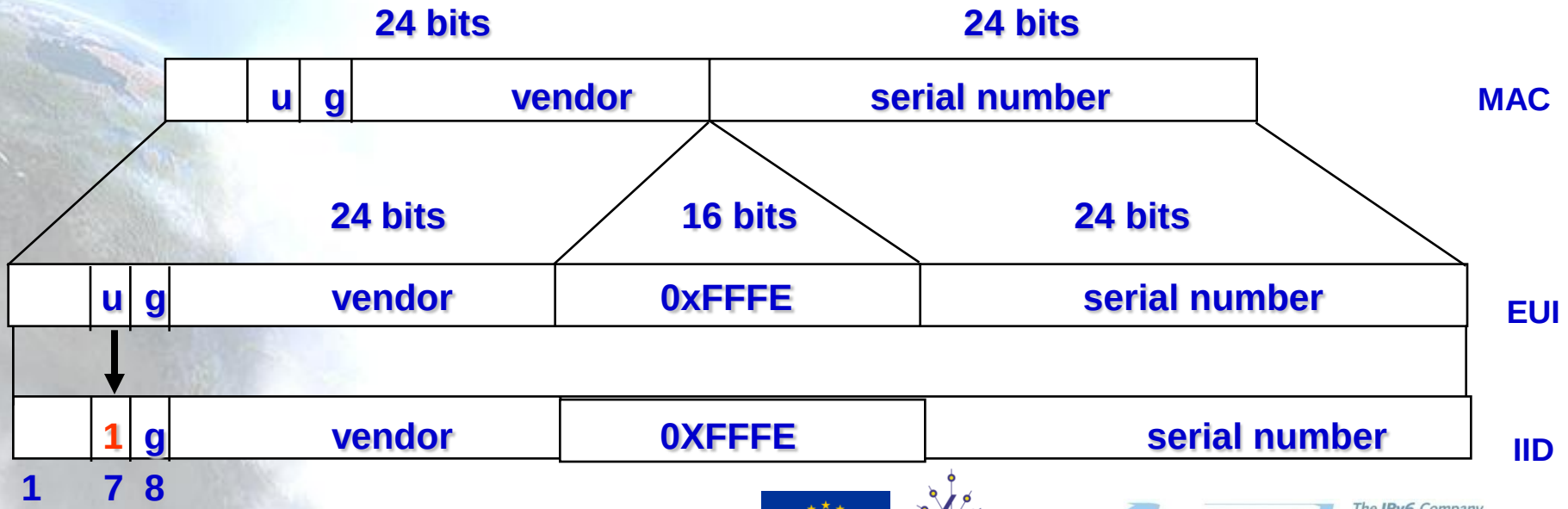
Identificadores de Interfaz (2)

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

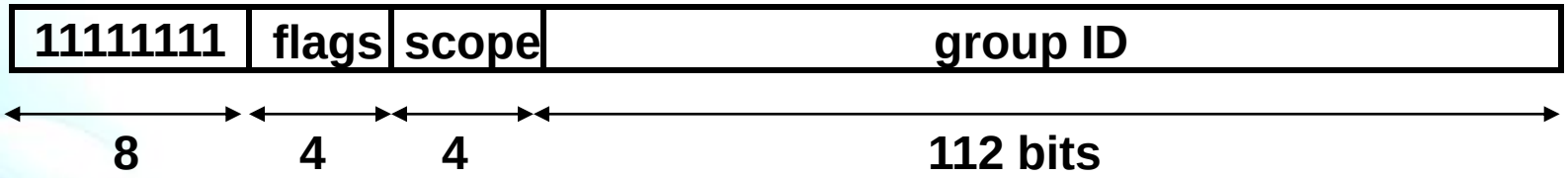
EUI-64

- 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



3.5 Direcciones Multicast

Direcciones Multicast



- Flags: **0RPT**: El flag de más peso está reservado y debe inicializarse a 0
  - T: Asignación Transitoria, o no (well-known)[RFC4291]
  - P: Asignación basada, o no, en un prefijo de red [RFC3306]
  - R: Dirección de un Rendezvous Point incrustada, o no [RFC3956]
- 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)

Direcciones Multicast Reservadas (1)

- Node-Local Scope
  - FF01::1 Todos los nodos de la red
  - FF01::2 Todos los encaminadores de la red

- Link-Local Scope
  - FF02::1 Todos los nodos de la red
  - FF02::2 Todos los encaminadores de la red
  - FF02::4 Encaminadores DVMRP
  - FF02::5 Encaminadores OSPFIGP
  - FF02::6 Encaminadores designados OSPFIGP
  - FF02::9 Encaminadores RIP
  - FF02::B Mobile-Agents
  - FF02::D Todos los encaminadores PIM
  - FF02::1:2 Todos los DHCP-agents
  - FF02::1:FFXX:XXXX Solicited-Node Address

Direcciones Multicast Reservadas (2)

- Site-Local Scope
  - FF05::2 Todos los encaminadores
  - FF05::1:3 Todos los DHCP-servers
  - FF05::1:4 Todos los DHCP-relays

- Variable Scope Multicast Addresses
  - FF0X::101 Network Time Protocol (NTP)
  - FF0X::129 Gatekeeper
  - FF0X::2:0000-FF0X::2:7FFD Multimedia Conference Calls
  - FF0X::2:7FFE SAPv1 Announcements
  - FF0X::2:8000-FF0X::2:FFFF SAP Dynamic Assignments

Direcciones Multicast Importantes

- FF01::1, FF02::1 Todos los nodos
- FF01::2, FF02::2, FF05::2 Todos los encaminadores

- Dirección (SN) multicast a partir de la unicast
  - Si la dirección acaba en “XY:ZTUV”
  - La SN es: FF02::1:FFXY:ZTUV

- Cada nodo IPv6 debe unir la dirección SN a todas sus direcciones unicast y anycast.

3.6 Plan de direccionamiento

Plan de Direccionamiento (1)

- El plan de direccionamiento o numeración tiene como objetivo la asignación de direcciones del espacio de direccionamiento IPv6 asignado por un RIR
  - Dicha asignación es para las diferentes redes y subredes existentes en una red operativa así como las planeadas a futuro
- Para ello se pueden considerar los siguientes criterios (**RFC3177 y tendencias reales**)
  - Todas las redes internas que vayan a desplegar IPv6 tendrán un prefijo /64
    - Necesario para la construcción automática de direcciones IPv6 de tipo Unicast y/o Anycast
  - Los usuarios finales, clientes residenciales (acceso xDSL, FTTx, etc.), como corporativos (empresas, ISPs, Universidad, etc.) podrán recibir prefijos de longitud /48
    - Posibilita crear hasta 2^{16} (65.536) subredes IPv6 de prefijo /64

Plan de Direccionamiento (2)

- La asignación de 65.536 posibles subredes IPv6 de prefijo /64 puede parecer “a priori” excesiva, sin embargo existen varias razones para ello

1. El despliegue futuro de redes NGN facilitará la implementación de servicios nuevos como VoIP, IPTV, etc., cuya distribución puede requerir el uso de redes /64 específicas para cada usuario final
2. Es previsible la llegada en los próximos años de nuevas aplicaciones y/o servicios, aun inimaginables, basadas en domótica, inteligencia ambiental, etc. que requieran un espacio de direccionamiento propio y separado del resto de tráfico, en la red del usuario final

Plan de Direccionamiento (3)

- Para la elaboración del plan de direccionamiento se deben tener en cuenta las diversas subredes existentes susceptibles de desplegar IPv6 en algún momento, éstas pueden incluir
  - Subredes susceptibles de ser nativas IPv6 desde el primer momento del despliegue de IPv6
  - Subredes susceptibles de ser nativas IPv6 a medio o largo plazo, no necesariamente desde el comienzo del despliegue de IPv6
  - Servicios de transición a IPv6

- El objetivo es tratar de garantizar que no se requerirá modificar la estructura del plan de direccionamiento en el futuro, cuando el despliegue de IPv6 en la red se haga de forma masiva
- Existen dos aproximaciones para la distribución de direcciones: por servicios o geográfica. No son excluyentes.

Plan de Direccionamiento (4)

- A continuación se presenta un ejemplo de plan de direccionamiento inicial basado en un prefijo /32
- Con este prefijo /32 y los criterios anteriormente descritos se tiene capacidad de proporcionar prefijos /48 a más de 50 000 usuarios de manera simultánea

- Partiendo del prefijo 32 se forman varios grupos diferentes de los 64 posibles prefijos /38 para las diferentes subredes consideradas, atendiendo a los siguientes criterios
  - Grupos de redes que sean independientes de otras
  - Grupos de redes que tengan similitudes en cuanto a su topología
  - Grupos de prefijos /38 libres para proporcionar flexibilidad al plan y posibilitar crecimientos inmediatos

Plan de Direccionamiento (5)

- Un ejemplo típico podría incluir 6 grupos de prefijos /38
  1. Red troncales y redes internas
     - Encaminamiento
     - Servicios básico
     - Redes internas
     - WiFi
     - Enlaces
     - Movilidad
     - Data Center
  2. Túneles
  3. Clientes corporativos e ISPs
  4. Usuarios residenciales (ADSL-FTTH)
  5. GPRS/3G
  6. Prefijos Libres

Plan de Direccionamiento (6)

#	Prefijo	Categoría	Número de prefijos	Longitud prefijos
0	2001:DB8:0000::/38	Encaminamiento, Servicios básico, Redes internas, WiFi, Enlaces, Movilidad, Data Center		
1	2001:DB8:0400::/38	Libre	1	/38
2	2001:DB8:0800::/38	Túneles		
	2001:DB8:0C00::/38 2001:DB8:1000::/38	Libres	2	/38
5	2001:DB8:1400::/38	Clientes corporativos e ISPs	1.024	/48
6	2001:DB8:1800::/38	Clientes corporativos e ISPs	1.024	/48
7	2001:DB8:1C00::/38	Clientes corporativos e ISPs	1.024	/48
	2001:DB8:2000::/38 ... 2001:DB8:3C00::/38	Libres	8	/38
16	2001:DB8:4000::/38	Usuarios ADSL-FTTH	1.024	/48
	Hasta	Usuarios ADSL-FTTH	1.024	/48
35	2001:DB8:8C00::/38	Usuarios ADSL-FTTH	1.024	/48
	2001:DB8:9000::/38 2001:DB8:9400::/38 2001:DB8:9800::/38	Libres	3	/38
39	2001:DB8:9C00::/38	GPRS/3G	67.108.864	/64
	2001:DB8:A000::/38 2001:DB8:A400::/38	Libres	2	/38
42	2001:DB8:A800::/38	GPRS/3G	1.024	/48
	Hasta	GPRS/3G	1.024	/48
61	2001:DB8:F400::/38	GPRS/3G	1.024	/48
	2001:DB8:F800::/38 2001:DB8:FC00::/38	Libres	2	/38
		Total prefijos /38 Libres	18	

3.7 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:db8:0080::/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

3.8 Ejercicios con Direcciones

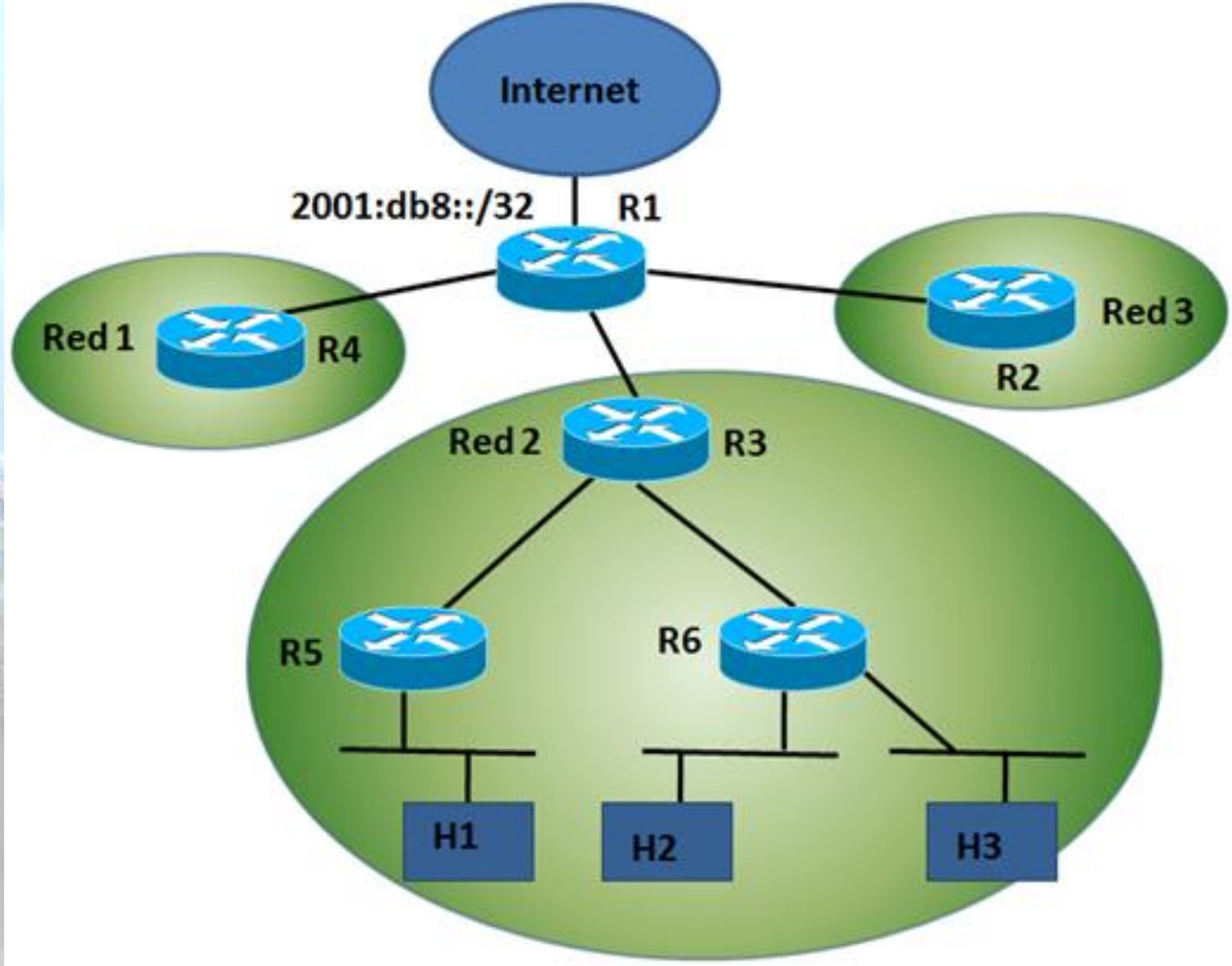
Ejercicios Direcciones (1)

- Indicar a qué tipo de direcciones pertenece cada una de las siguientes:
  - 2001:db8:fe80:ffff::a:b:c
  - 2a01:48:1:1:2c0:26ff:fe26:4ba
  - fe80::9ce4:ecde:cf33:a2a2
  - fe80::2c0:26ff:fe26:4ba
  - 2002:1bc3:1b::1:2
  - ::1
  - FD00:a:b:17c2::1
  - FF0E::1:2:3:4
  - FF05::a:b:c

Ejercicios Direcciones (2)

- Comprimir al máximo las siguientes direcciones
  - 2001:0db8:0000:1200:0fe0:0000:0000:0002
  - 2001:0db8::faba:0000:2000
  - 2001:db8:fab0:0fab:0000:0000:0100:ab
- Descomprimir al máximo las siguientes direcciones
  - 2001:db8:0:a0::1:abc
  - 2001:db8:1::2
  - 2001:db8:400::fff:0110

Ejercicios Direcciones (3)



Ejercicios Direcciones (4)

Descripción	Prefijo / Dirección
Infraestructura de encaminamiento	/48
Gestión y monitorización	/48
Red 1	/48
Red 2	/48
Red 3	/48
Prefijo R5	/56
Prefijo R6	/56
Prefijo Subred H1	/64
Prefijo Subred H2	/64
Prefijo Subred H3	/64
IPv6 H1	/64
IPv6 H2	/64
IPv6 H3	/64

4. ICMPv6, Neighbor Discovery y DHCPv6

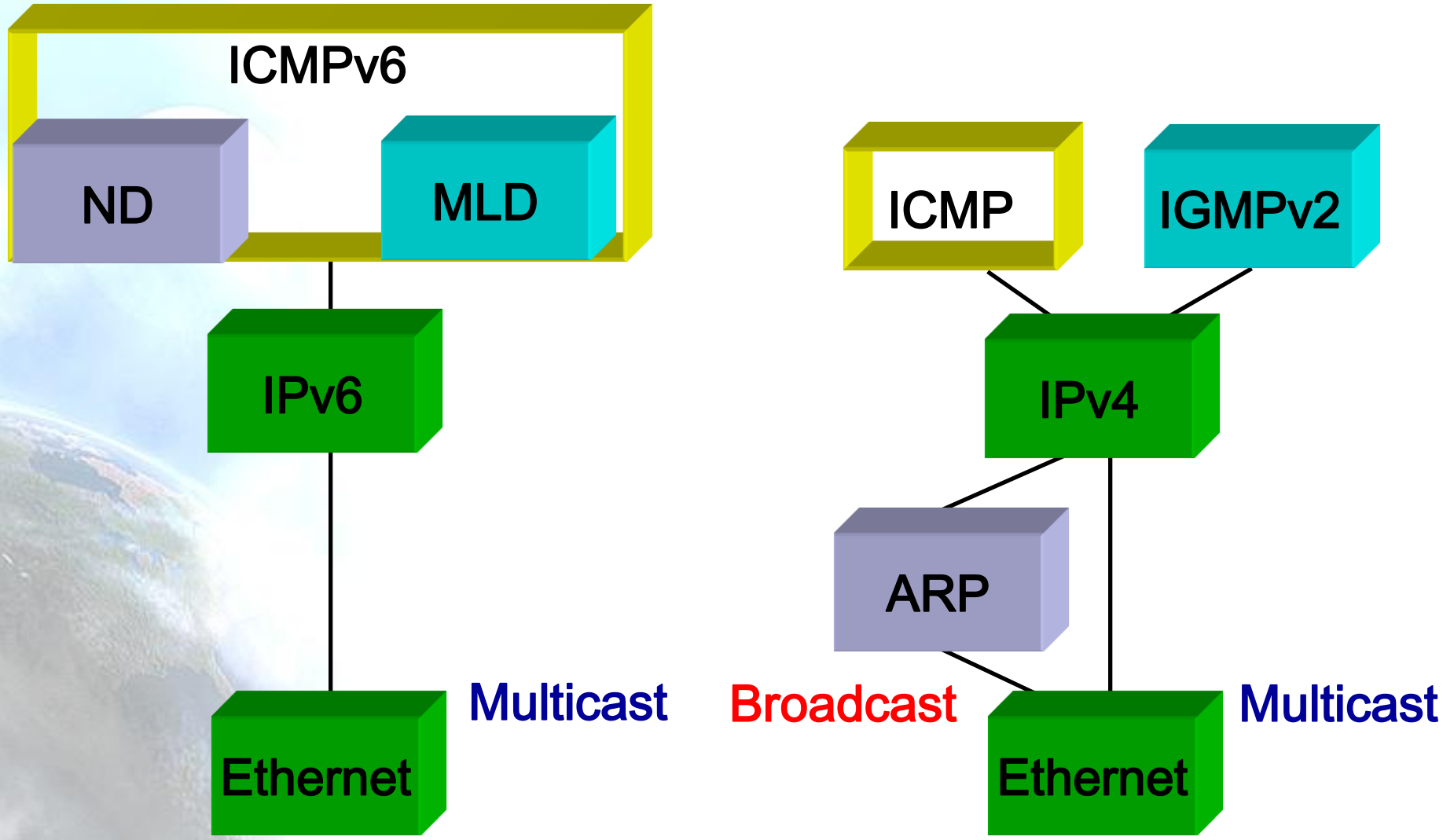
4.1 ICMPv6

4.2 Neighbor Discovery

4.3 Autoconfiguración

4.4 DHCPv6

Plano de Control IPv4 vs. IPv6



4.1 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.

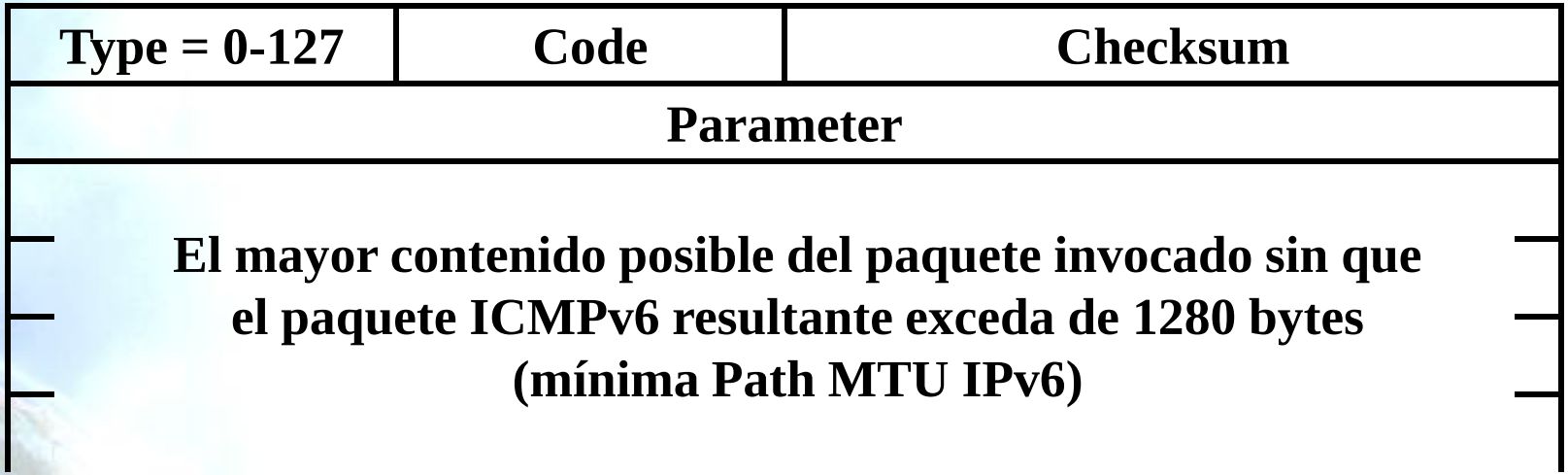
Mensajes ICMPv6

- 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



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):

4.2 Neighbor Discovery

ND (RFC4861)

- Define el protocolo Neighbor Discovery (ND) (Descubrimiento de Vecinos) en IPv6.
- Los nodos usan ND para determinar la dirección de la capa de enlace de los nodos que se sabe que están en el mismo segmento de red y para purgar rápidamente los valores almacenados inválidos.
- Los hosts también usan ND para encontrar encaminadores vecinos que retransmitirán los paquetes que se les envíen.
- Los nodos usan el protocolo para tener conocimiento de los vecinos que son alcanzables y los que no y para detectar cambios de sus direcciones en la capa de enlace.
- ND habilita el mecanismo de autoconfiguración en IPv6.

Interacción Entre Nodos

- Define el mecanismo para solventar:
  - Descubrimiento de encaminadores
  - Descubrimiento de prefijos de red
  - Descubrimiento de parámetros
  - Autoconfiguración de direcciones
  - Resolución de direcciones
  - Determinación del “Next-Hop”
  - Detección de Vecinos Inalcanzables (NUD).
  - Detección de Direcciones Duplicadas (DAD).
  - Redirección del “First-Hop”.

Nuevos Tipos de Paquetes ICMP

- ND define 5 tipos de paquetes:
  - "Router Solicitation" (RS)
  - "Router Advertisement" (RA)
  - "Neighbor Solicitation" (NS)
  - "Neighbor Advertisement" (NA)
  - "Redirect"

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.

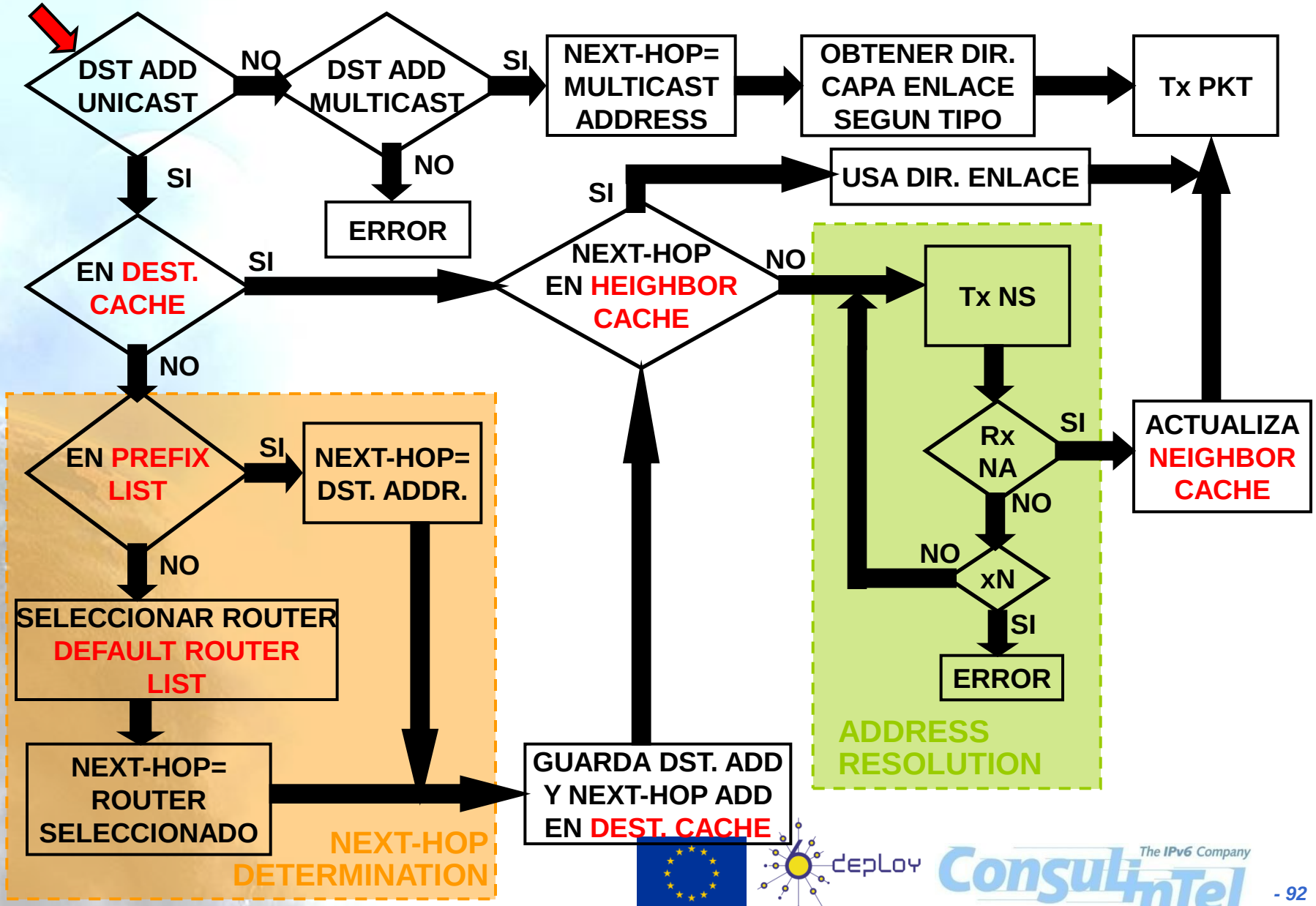
Bits 8	16	32
Type = 137	**Code = 0**	**Checksum**
Reserved = 0		
Target Address		
Destination Address		
Options …		

- 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



4.3 Autoconfiguración

Autoconfiguración

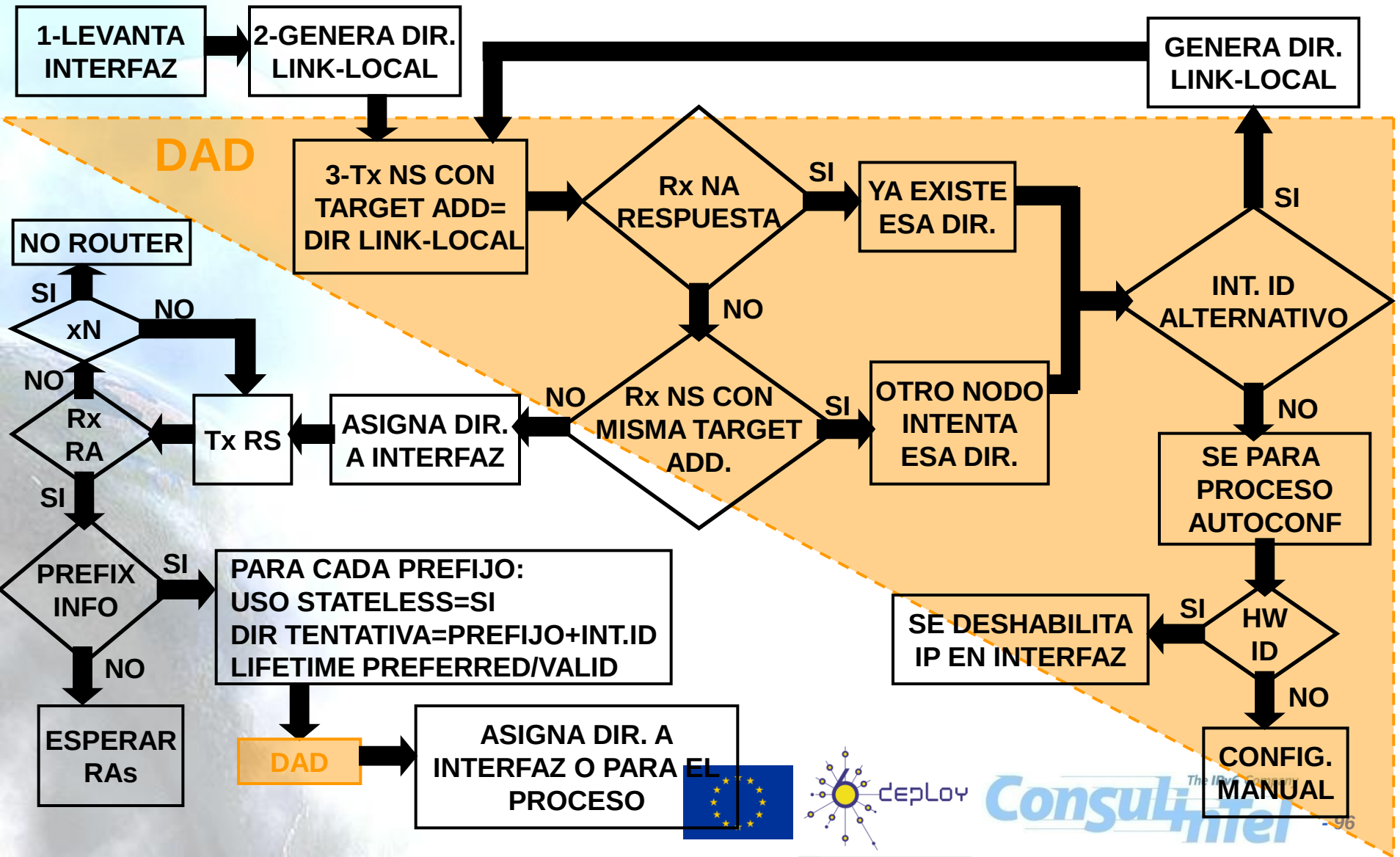
- El estándar especifica los pasos que un host debe seguir para decidir cómo auto-configurar sus interfaces de red en IPv6
- El proceso de auto-configuración incluye la creación de una dirección IPv6 de ámbito local (link-local) y la verificación de que no está duplicada en el mismo segmento de red, 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

RA: Flags M y O

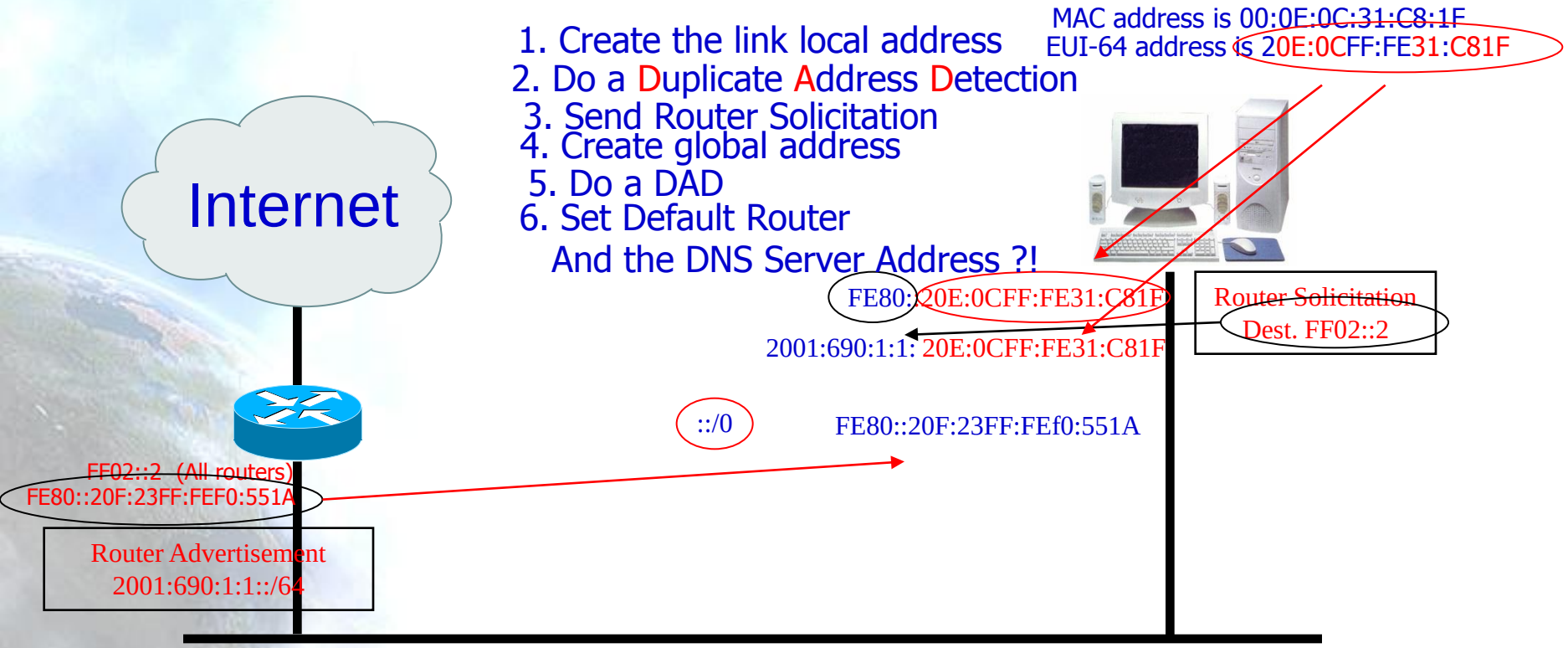
- Los flags M y O de los RA indican cómo deben comportarse los hosts con respecto a la autoconfiguración de los parámetros de red
- M indica como configurar la dirección IP
- O indica cómo configurar otros parámetros: DNS, etc.

Dir. / Otros	M	O	Comentario
SLAAC / SLAAC	0	0	Si dual-stack, se puede usar IPv4 para DNS
SLAAC / DHCPv6	0	1	DHCPv6 Stateless
DHCPv6 / SLAAC	1	0	Si dual-stack, se puede usar IPv4 para DNS
DHCPv6 / DHCPv6	1	1	El gateway se aprende del RA

Funcionamiento de la Autoconfiguración Stateless



Autoconfiguración Stateless



Formato Prefix Information Option

Bits 8	16	24	32
Type = 3	**Length = 4**	**Prefix Length**	**L** **A** **Reserved1 = 0**
Valid Lifetime			
Preferred Lifetime			
Reserved2 = 0			
Prefix			

- **L**(1bit): **on-link flag**=1 indica que este prefijo se puede usar para “on-link determination”
- **A**(1bit): **autonomous address-configuration flag**=1 indica que este prefijo se puede usar para stateless address autoconfiguration.
- **Valid Lifetime**: Tiempo en secs. Que el prefijo es válido para usarse en on-link determination. También usado en stateless address autoconfiguration.
- **Preferred Lifetime**: Tiempo en secs. Que las direcciones generadas con el prefijo mediante SLAAC siguen como *preferred*
- **Prefix** (128 bits): Dirección o prefijo de una dirección IPv6

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 se define 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)

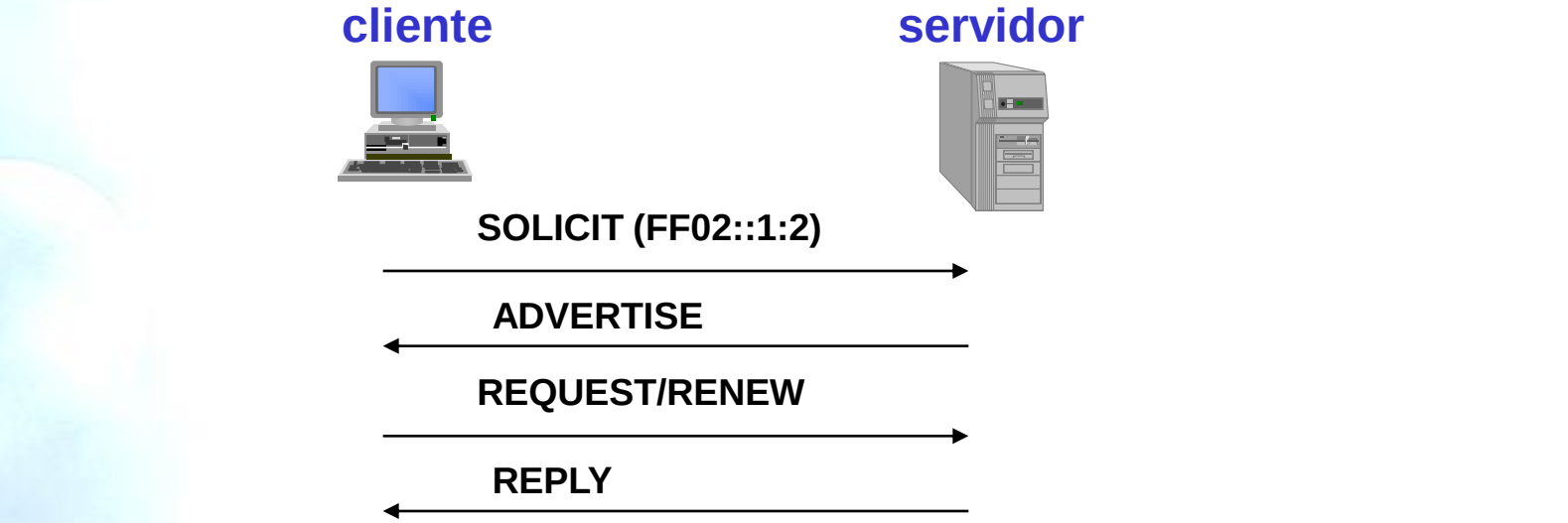
- Funciona de la misma manera en que se aprenden los prefijos y routers usando ND: IPv6 Sateless Address Autoconfiguration [RFC4862]
- Con la opción RDNSS el nodo aprende, con solo un mensaje:
  - Prefjo para usar en la autoconfiguración
  - Gateway IP
  - Servidores DNS Recursivos
- Si, además de la 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

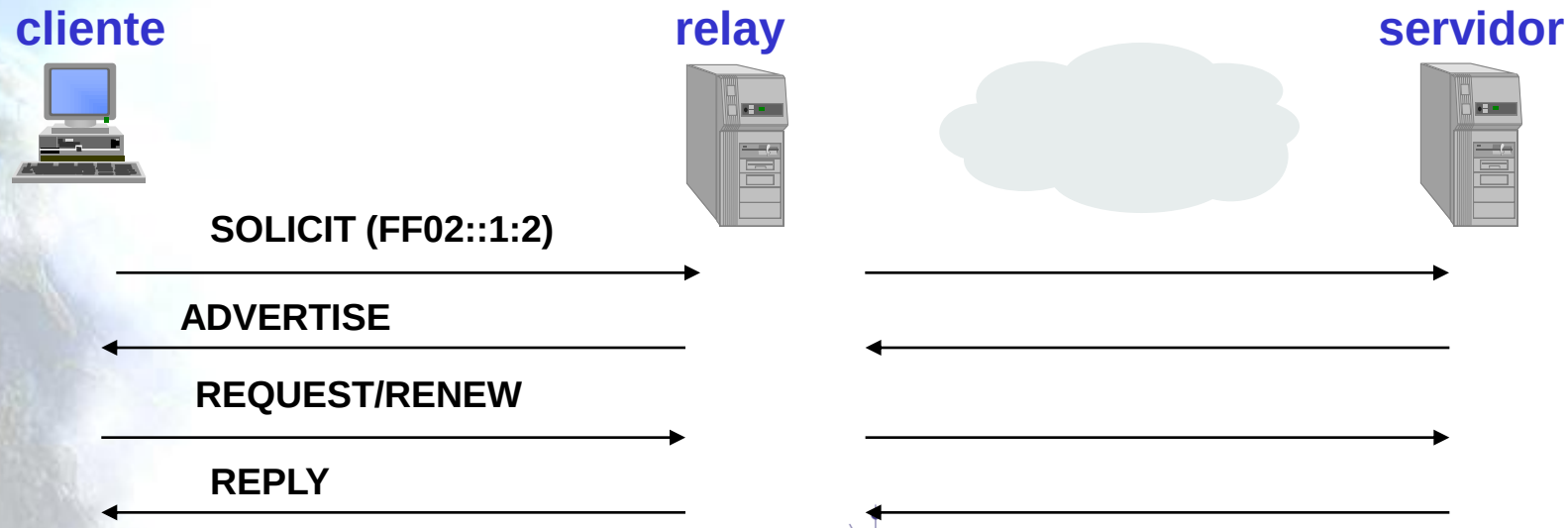
4.4 DHCPv6

DHCPv6

- DHCPv6 [RFC3315] se usa cuando:
  - No hay router
  - Lo indica el RA (ManagedFlag (**M**) y OtherConfigFlag **(O)**)
- 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

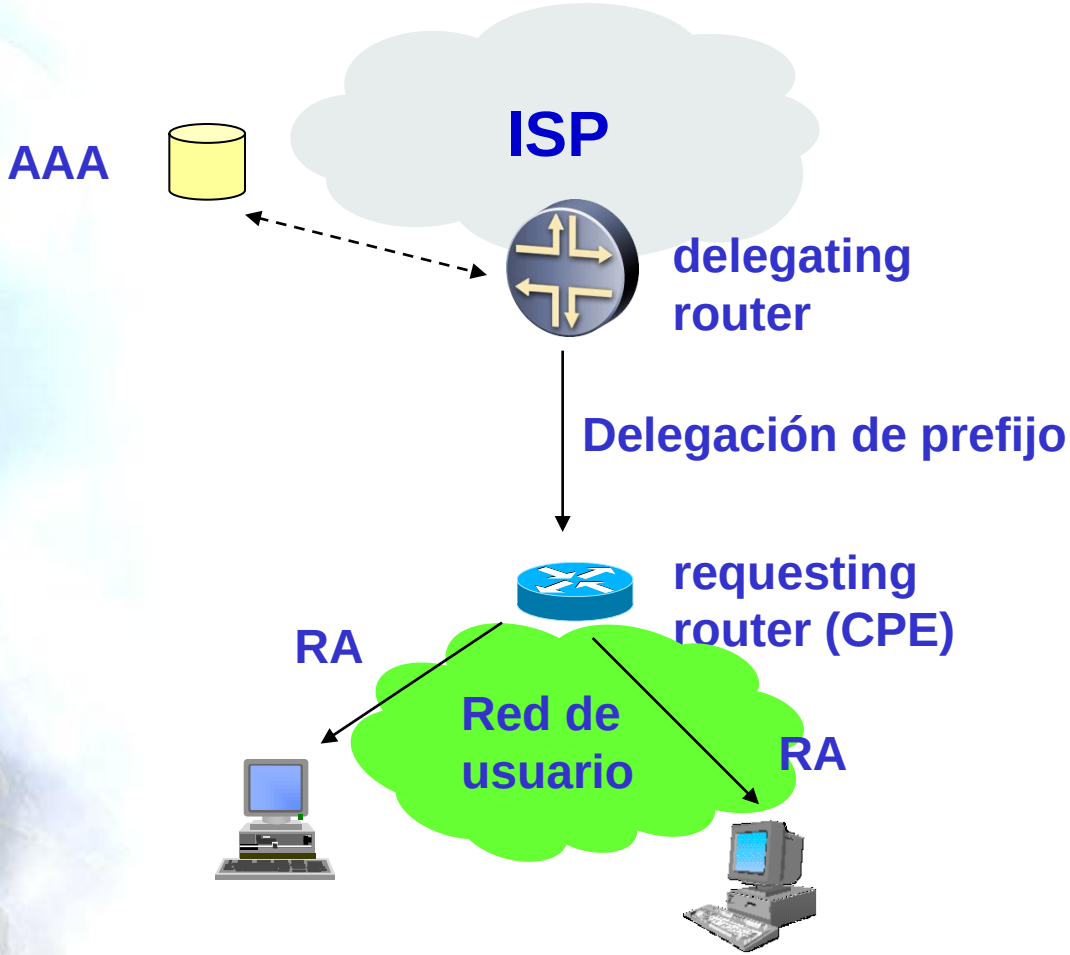




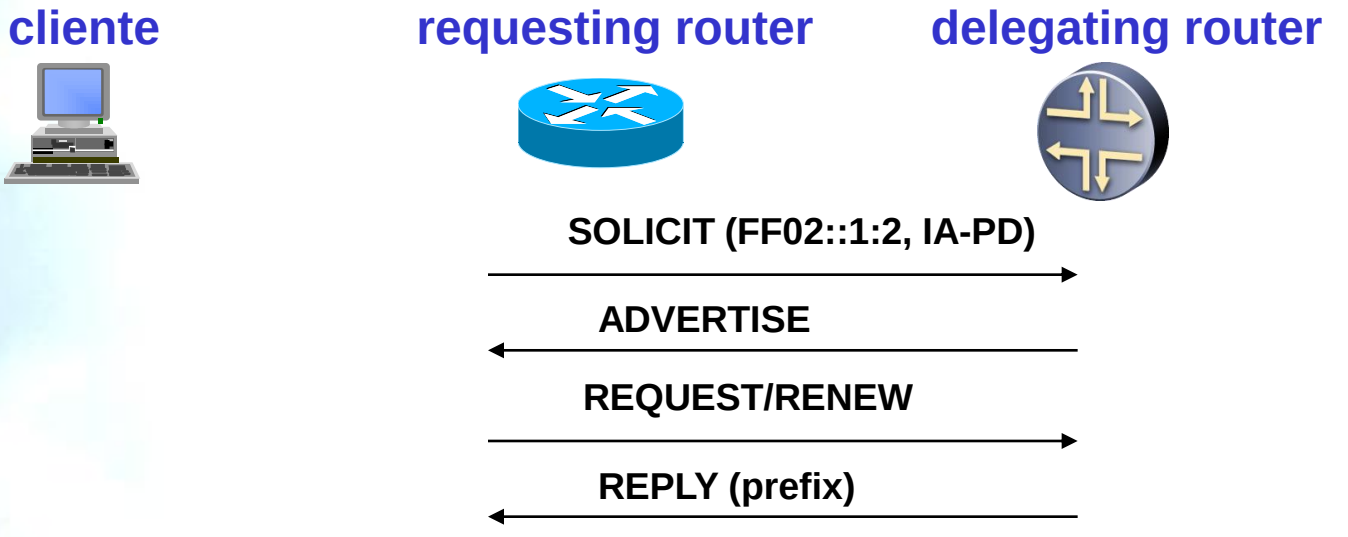
DHCPv6-PD (RFC3633)

- 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

Arquitectura de Red para DHCPv6-PD



Ejemplo Básico de DHCPv6-PD



5. Mecanismos de Transición

- 5.1 Estrategias coexistencia IPv4-IPv6
- 5.2 Doble Pila
- 5.x Túneles
- 5.10 Traducción
- 5.11 NAT64
- 5.12 NAT66 (NPT)
- 5.13 solo-IPv6

5.1 Estrategias coexistencia IPv4-IPv6

Técnicas Transición/Coexistencia (1)

- 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 (o viceversa). 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**

Técnicas Transición/Coexistencia (3)

- Proveedor de contenido o de servicios a través de Internet debe hacerse **visible** por IPv6:
  1. Cada vez habrá más usuarios solo-IPv6
  2. Cada vez habrá más usuarios con acceso IPv4 ”degradado”
  3. Tendrá más peticiones de clientes pidiendo IPv6
  4. Seguirá teniendo clientes IPv4… por ahora

- Debe tenerse en cuenta que habra usuarios solo-IPv4, doble-pila y solo-IPv6. Incluso habra algunos que pasen de solo-IPv4 a solo-IPv6, y viceversa.

Técnicas Transición/Coexistencia (4)

- Más puntos a tener en cuenta:

1. IPv6 debe implementarse para ser capaz de funcionar “solo-IPv6”, preparado para el futuro
2. Hay que averiguar “roadmap” de fabricantes de SW y HW en cuanto al soporte completo de IPv6
3. Es muy importante la formación
4. Puede ser my util tener una red de pruebas IPv4-IPv6

¿Qué ocurre si NO despliego IPv6?

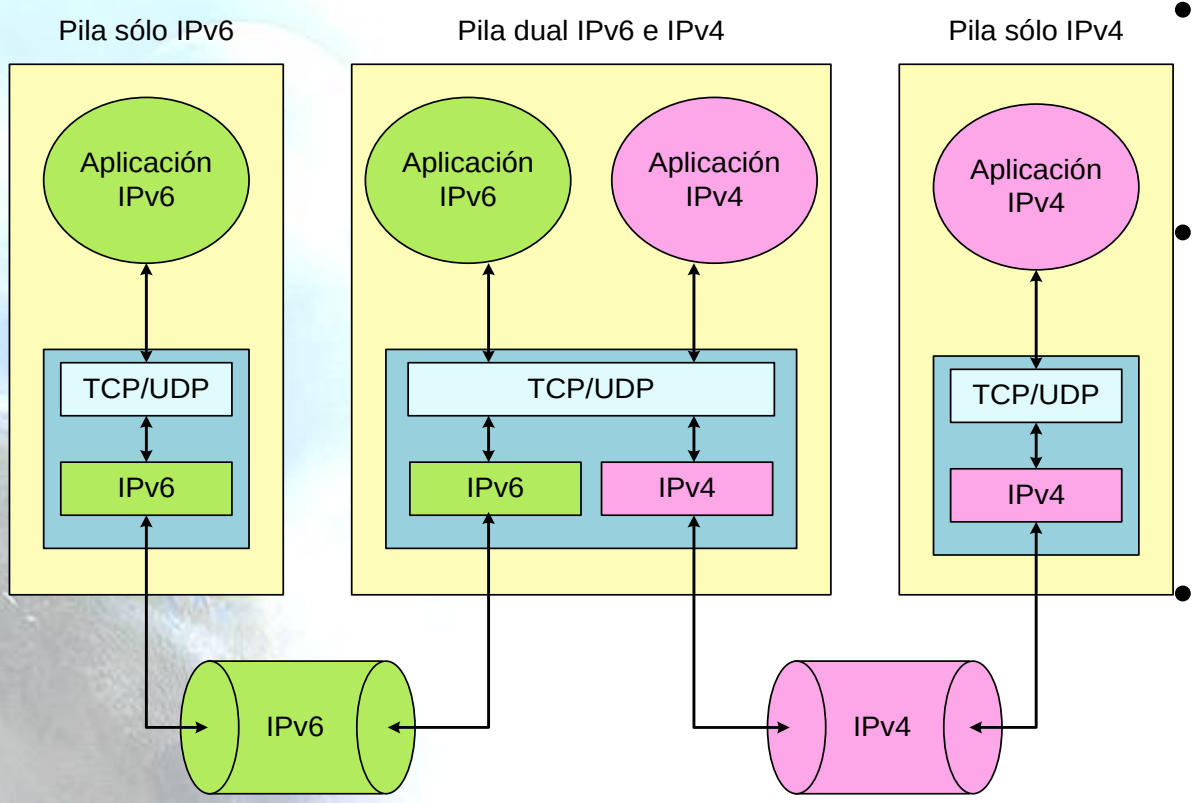
- Otros lo están desplegando
  - NO HAY ALTERNATIVA
- Aquellos servicios que no son visibles con IPv6 (cualquier página web, banca electrónica, gobierno electrónico, etc.), se diluye en la red … deja de ser visible en una parte del mundo, cada vez mayor
  - Es cuestión de meses, a lo sumo 1-2 años para que tenga un impacto importante en cualquier negocio
- Igualmente dejaremos de acceder a servicios sólo-IPv6, si sólo tenemos IPv4

5.2 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

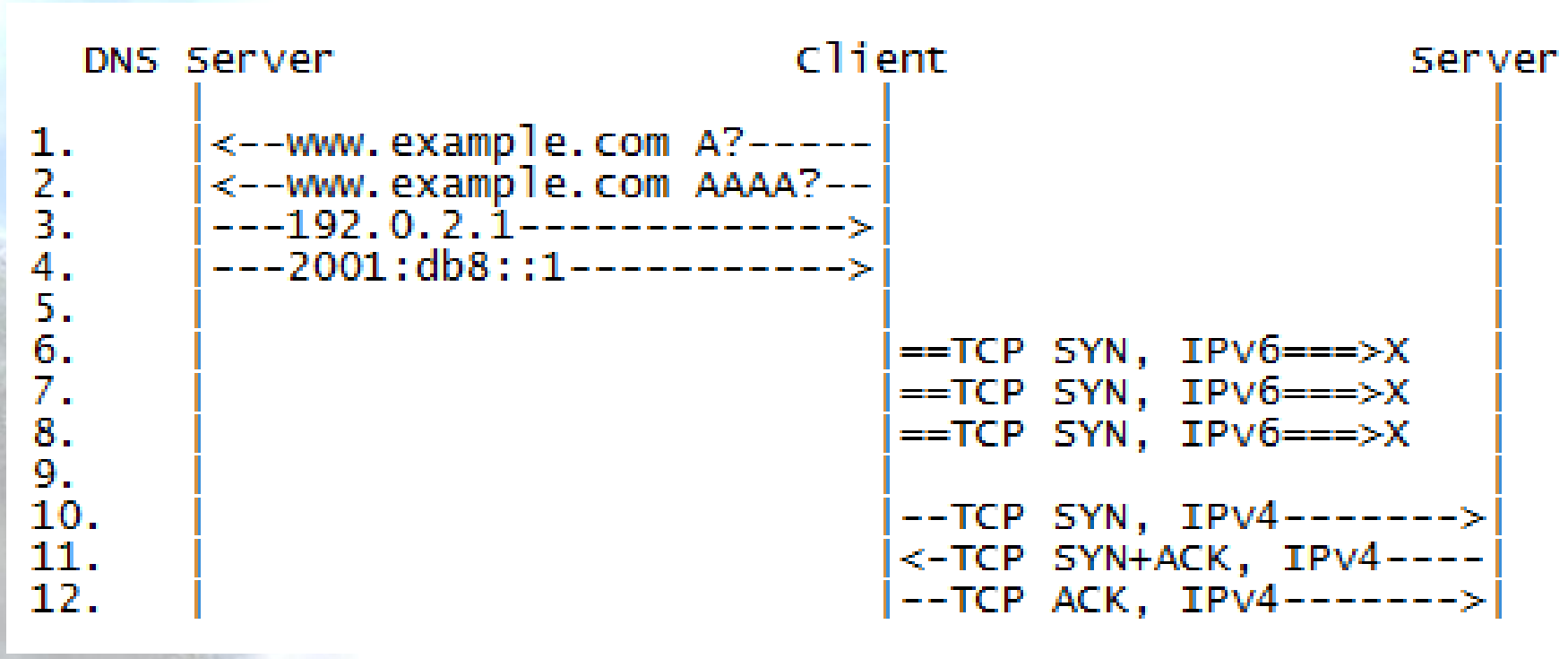
- Los nodos tienen implementadas las pilas IPv4 e IPv6
- Comunicaciones con nodos solo IPv6 ==> Pila IPv6, asumiendo soporte IPv6 en la red
- Comunicaciones con nodos solo IPv4 ==> Pila IPv4

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 (, Windows 8)

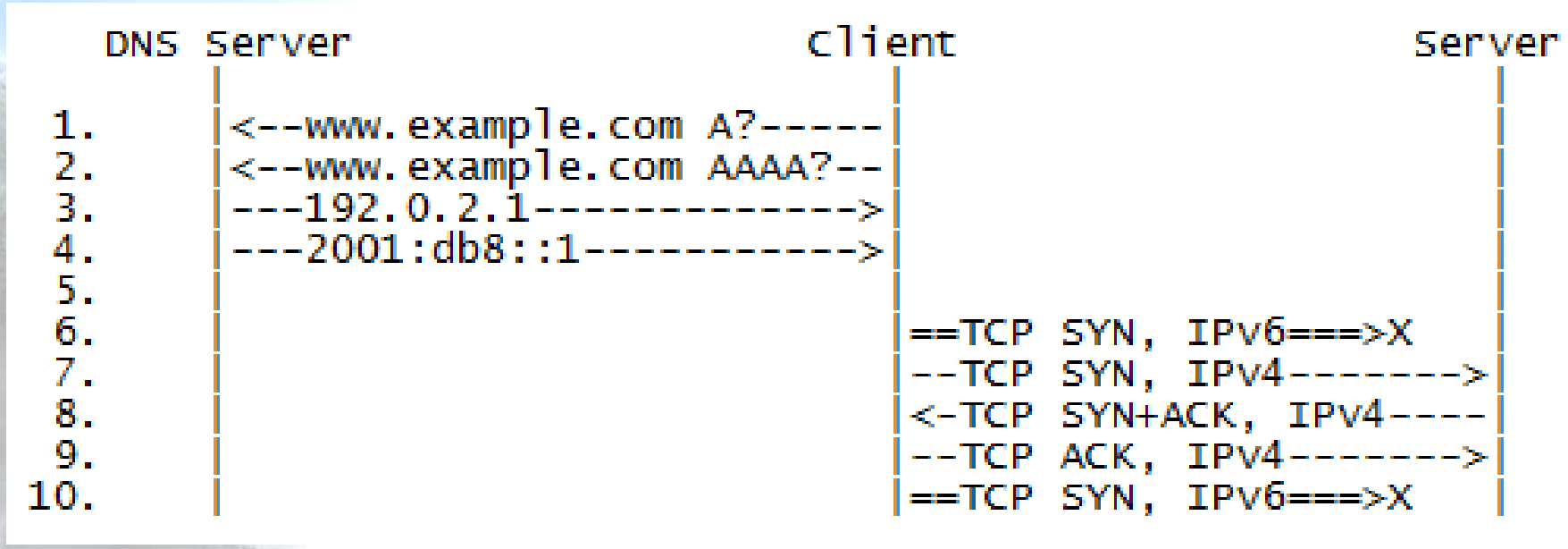
Happy-eyeballs (2)

- Funcionamiento habitual:



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

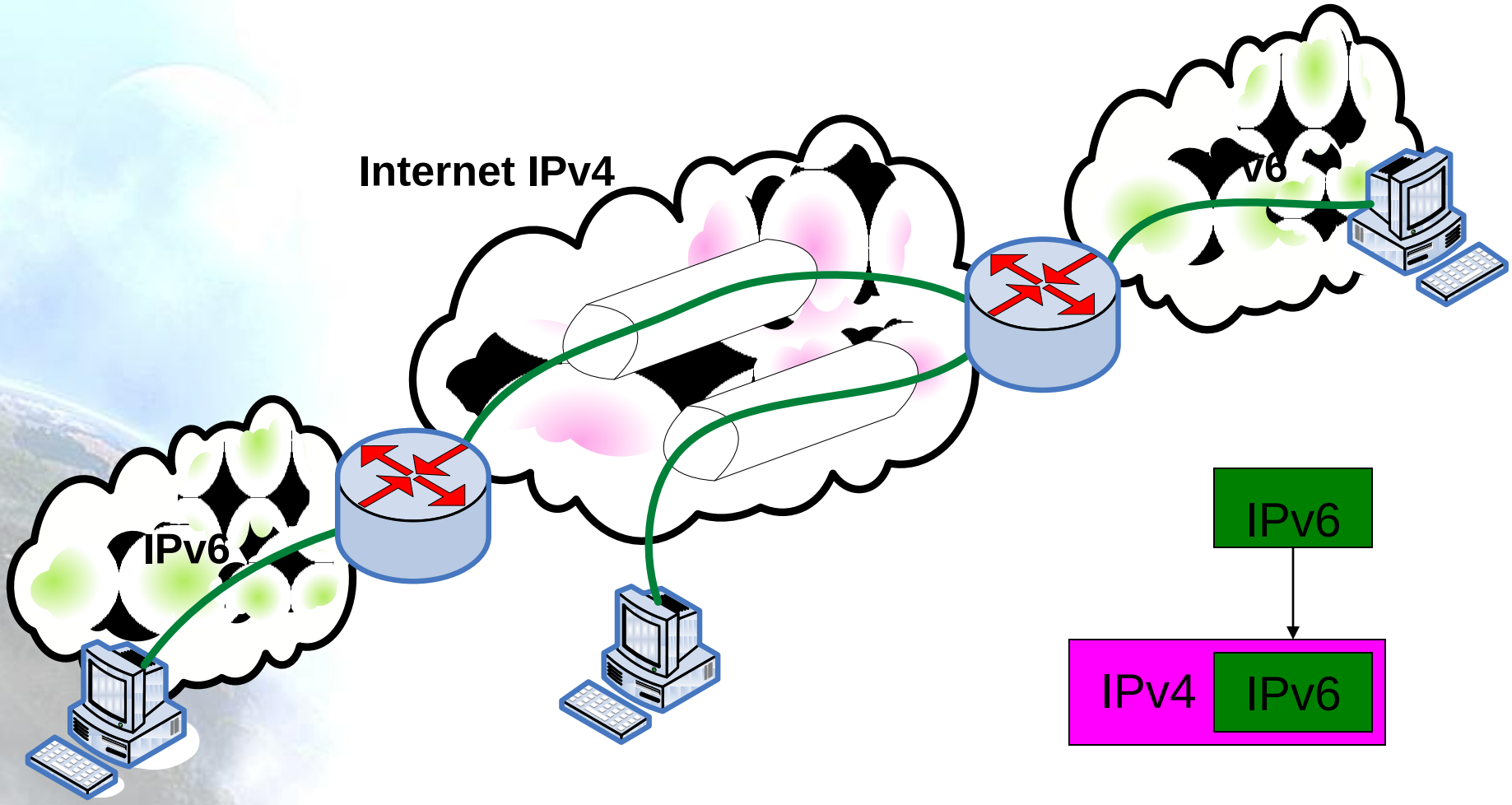


5.3 Túneles

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

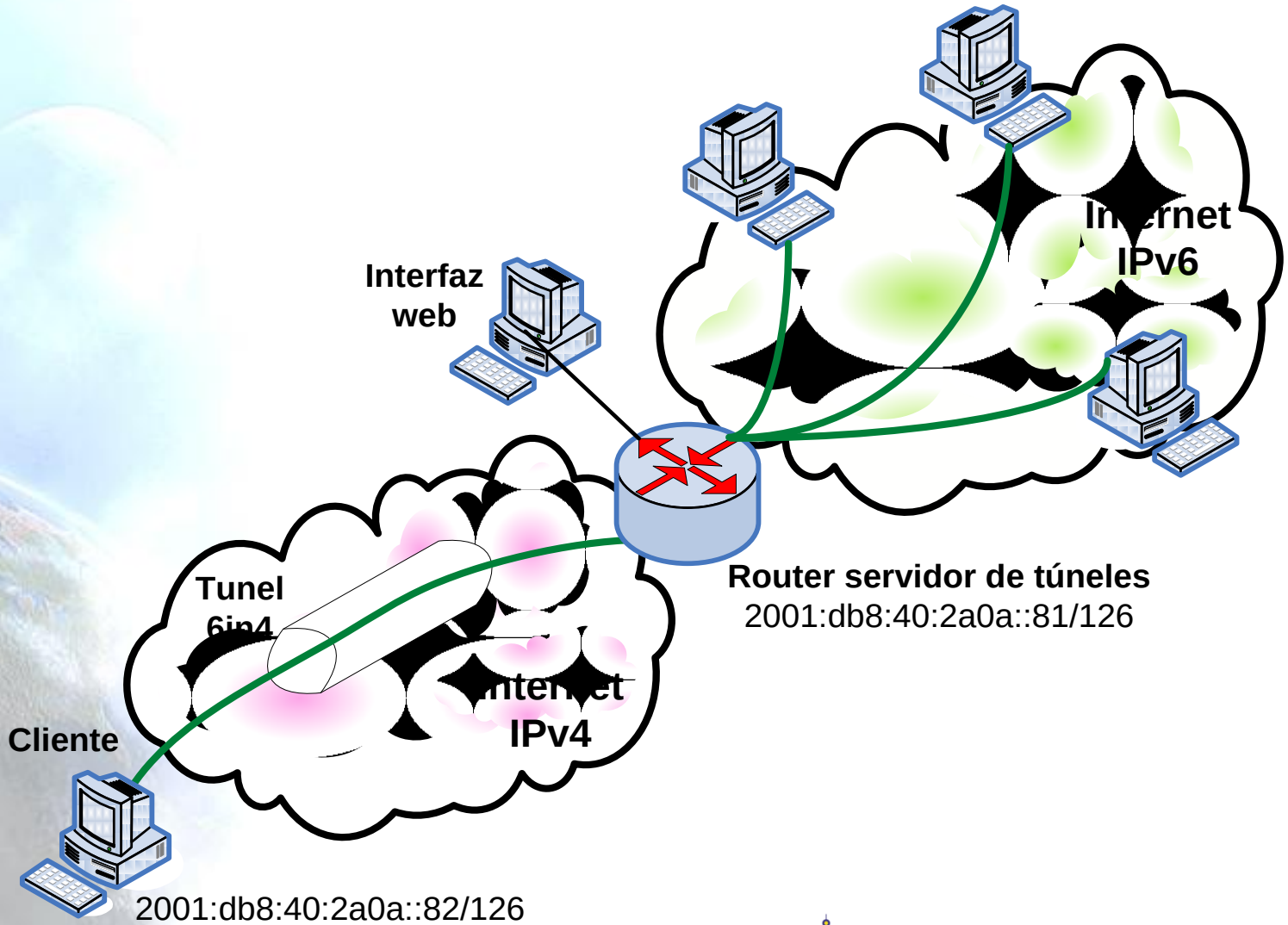
Túneles IPv6 en IPv4 (6in4) (1)



Mécanismo basado en túneles

5.4 Tunnel Broker

Tunnel Broker (RFC3053) (1)



Tunnel Broker (RFC3053) (2)

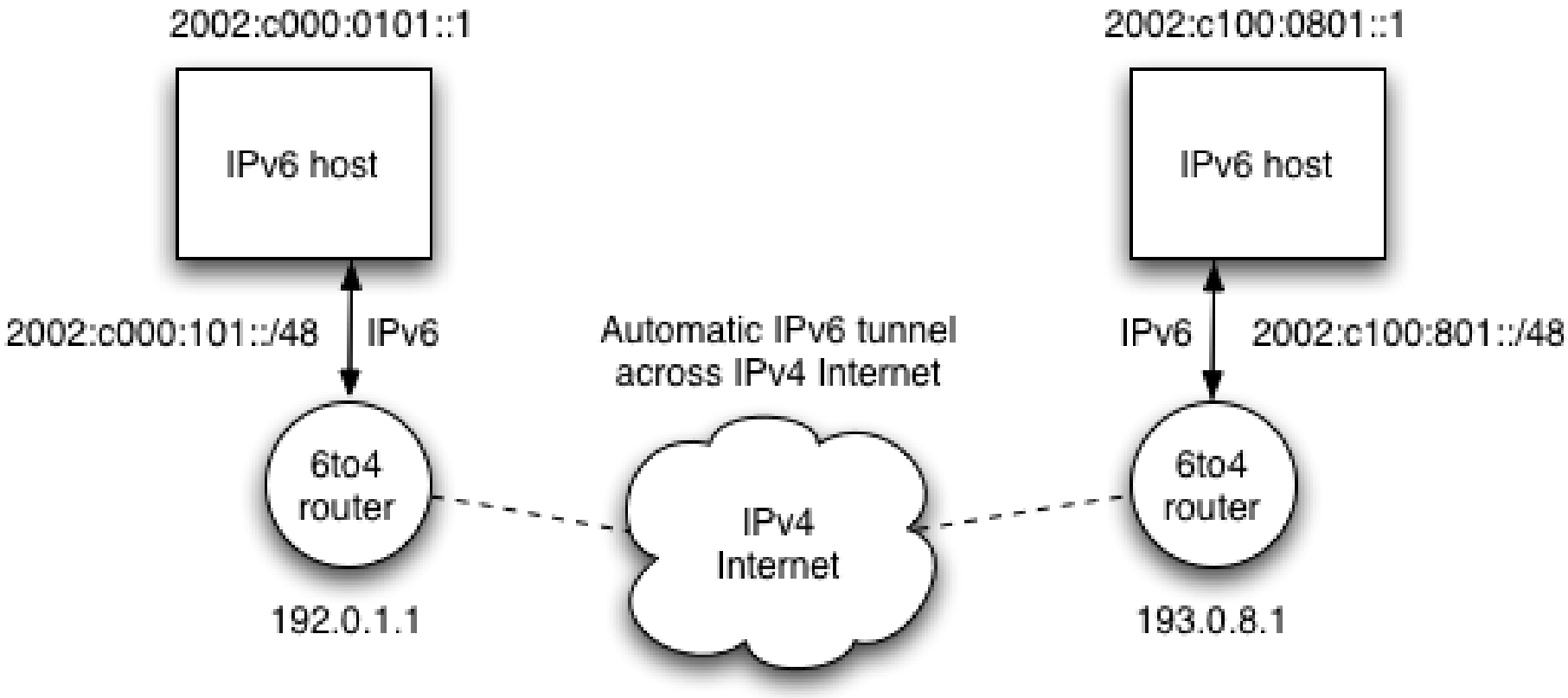
- Los túneles 6in4 requieren la configuración manual de los equipos involucrados en el túnel
- Para facilitar la asignación de direcciones y creación de túneles IPv6, se ha desarrollado el concepto de Tunnel Broker (TB).
  - Es un intermediario al que el usuario final se conecta, normalmente con un interfaz 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.

5.5 6to4

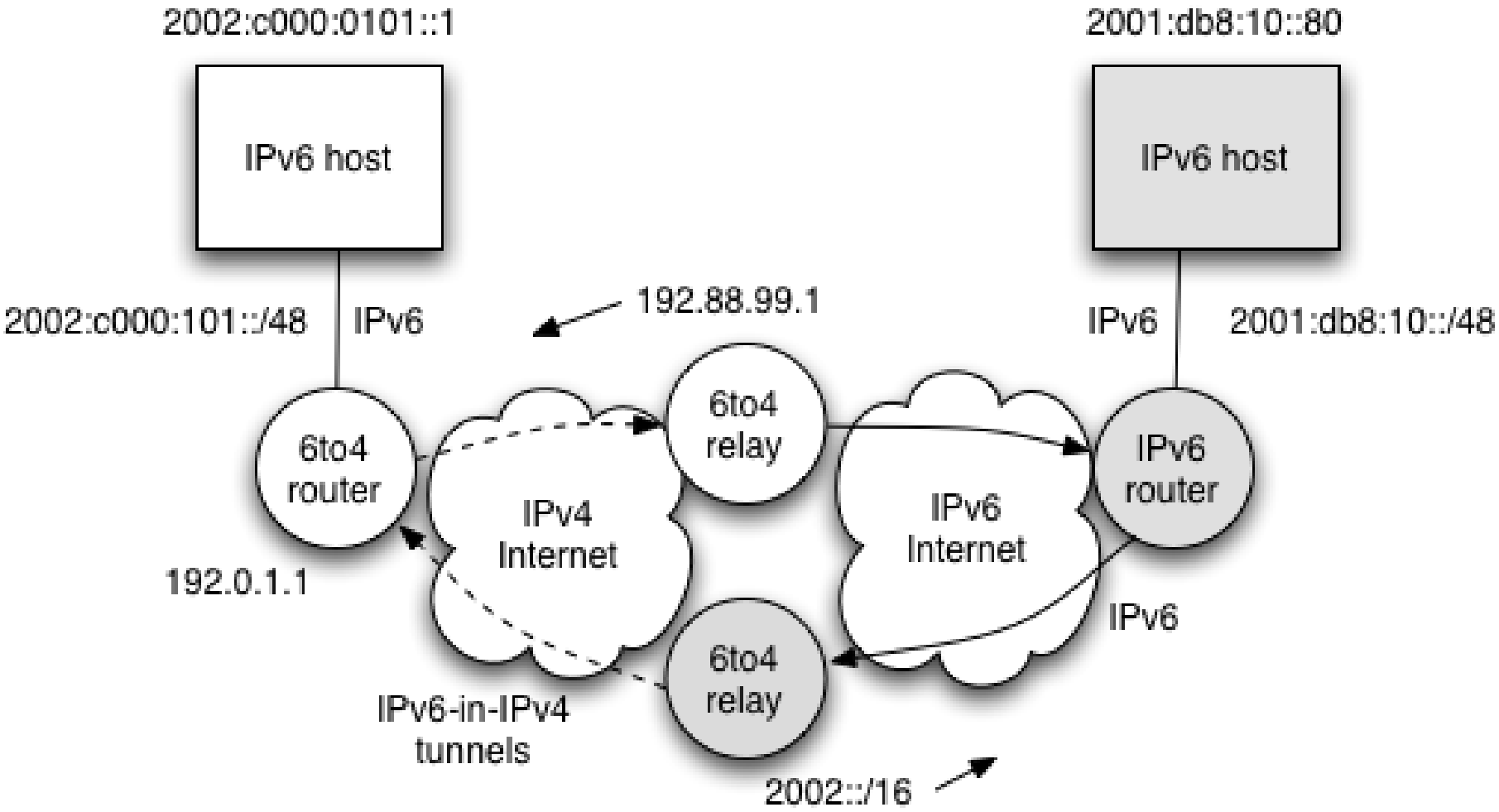
Túneles 6to4 (1)

- 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)



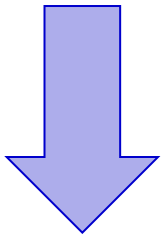
5.6 6RD

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*

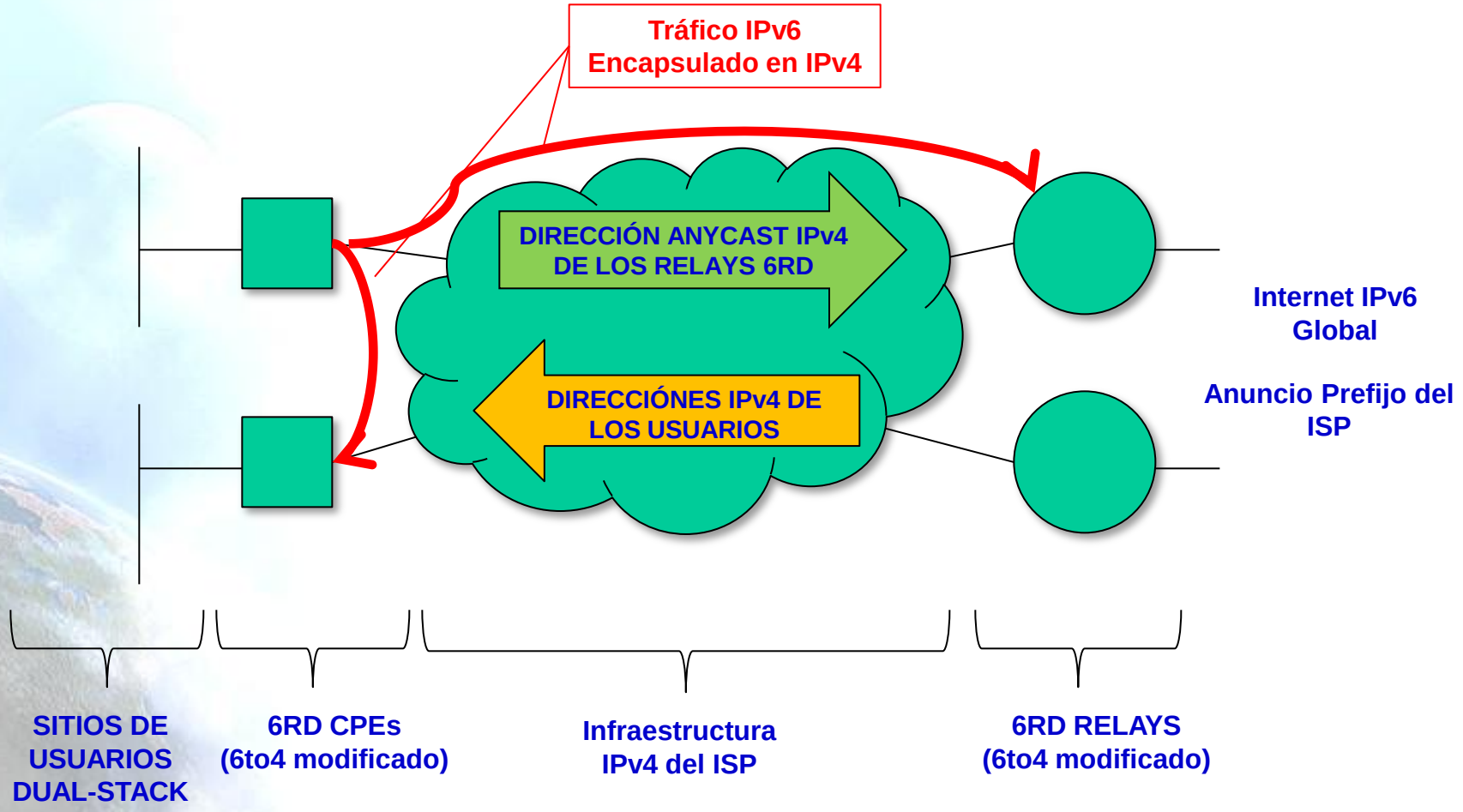
6RD: Pros & Cons

- 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

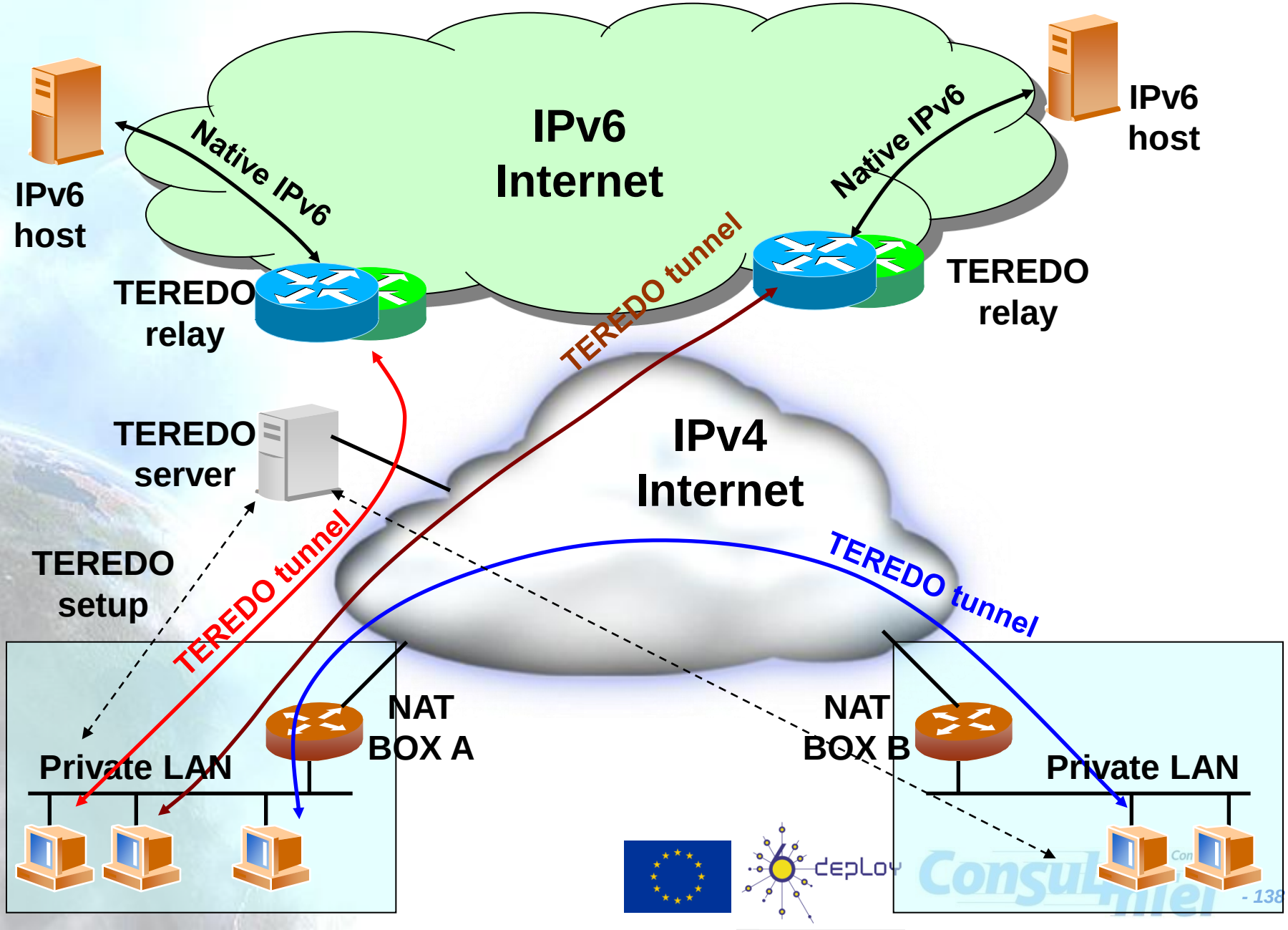


5.7 Teredo

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)



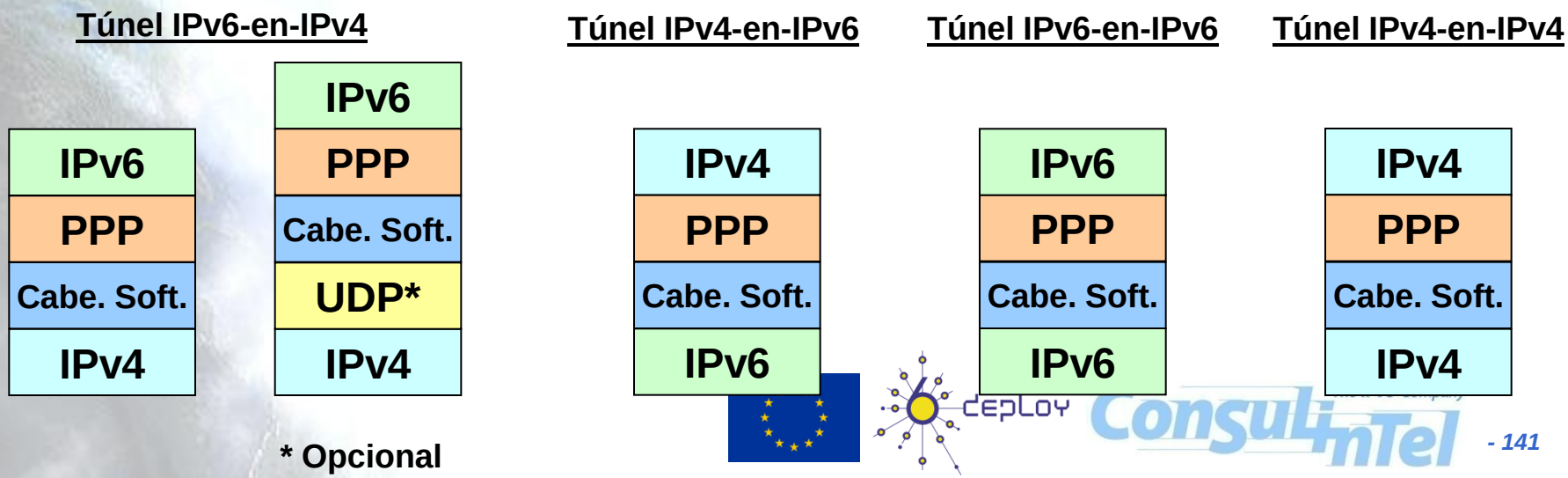
5.8 Softwires

Softwires

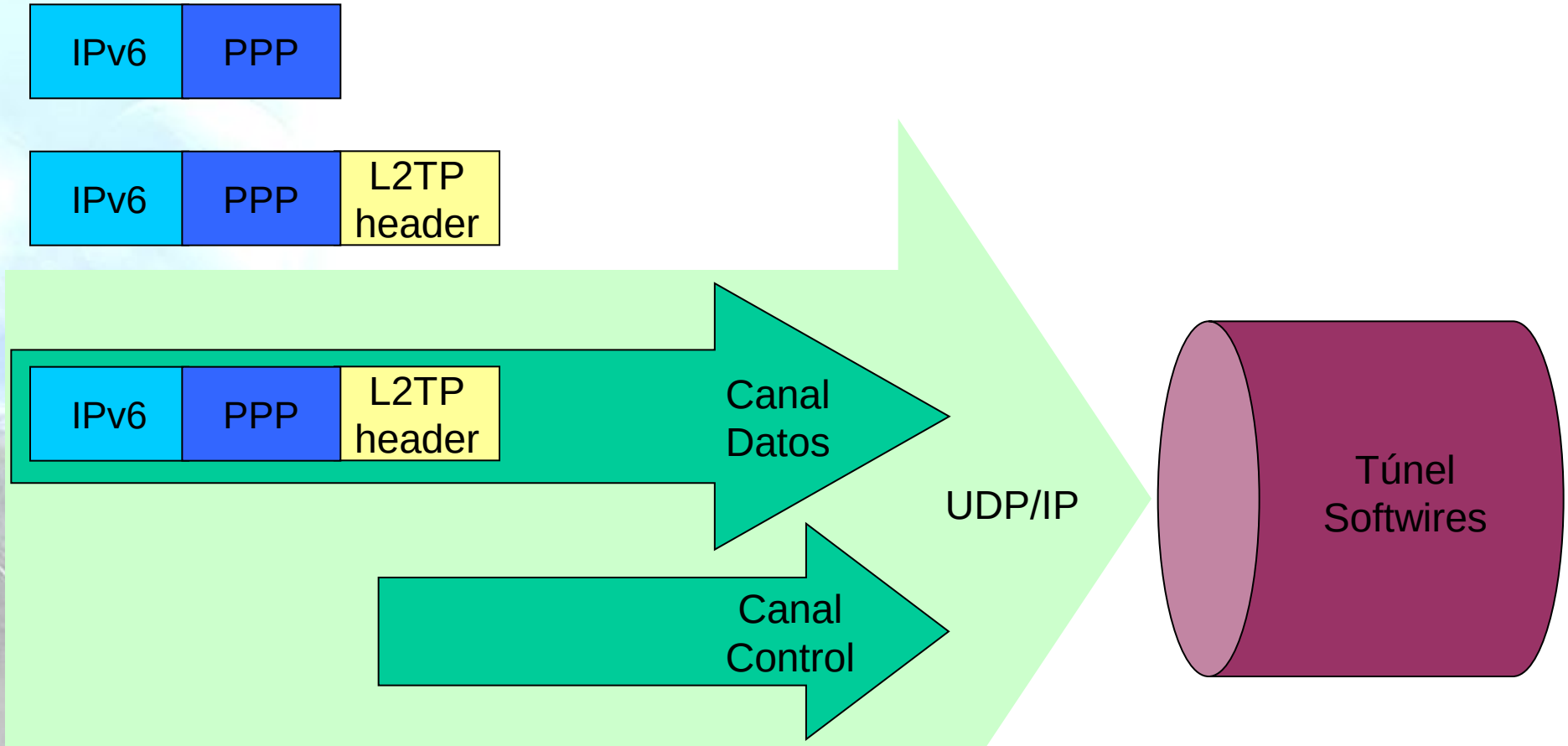
- Protocolo propuesto por el grupo de trabajo Softwire del IETF. Presenta las siguientes características:
  - Mecanismo de transición “universal” basado en la creación de túneles
    - IPv6-en-IPv4, IPv6-en-IPv6, IPv4-en-IPv6, IPv4-en-IPv4
    - Permite atravesar NATs en las redes de acceso
    - Proporciona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

- Descrito en el RFC5571
- 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



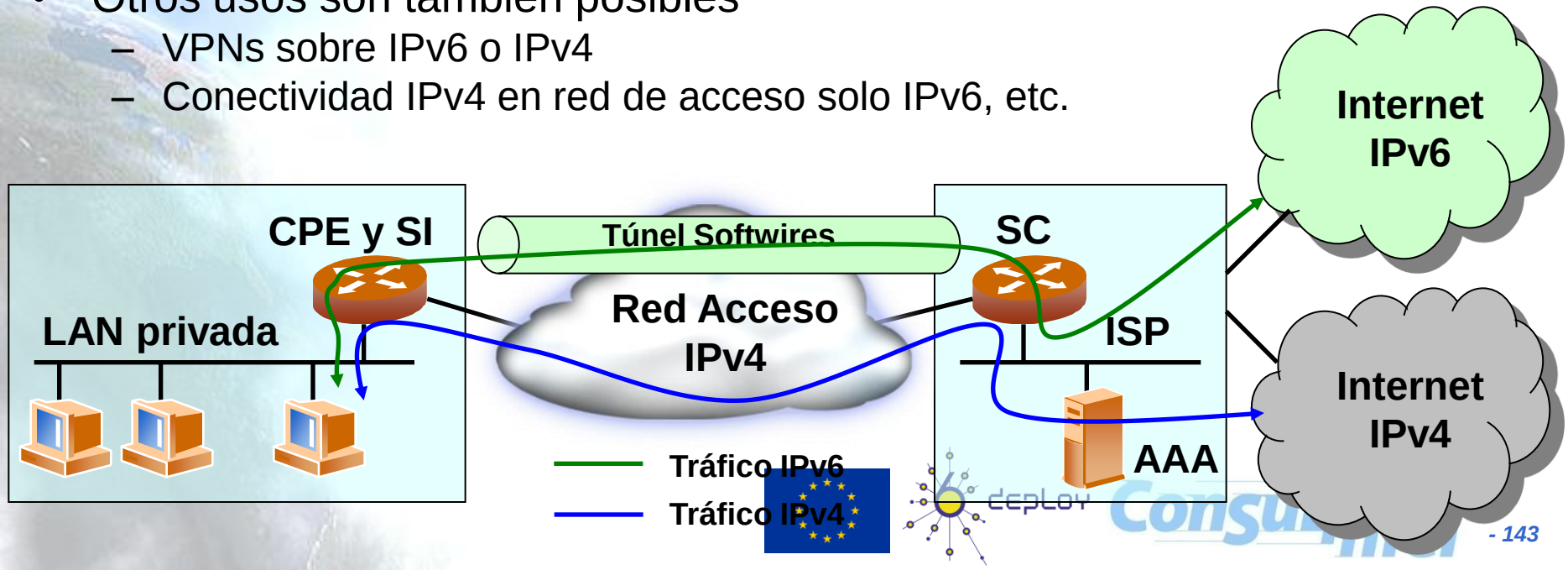
Softwires basado en L2TPv2



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

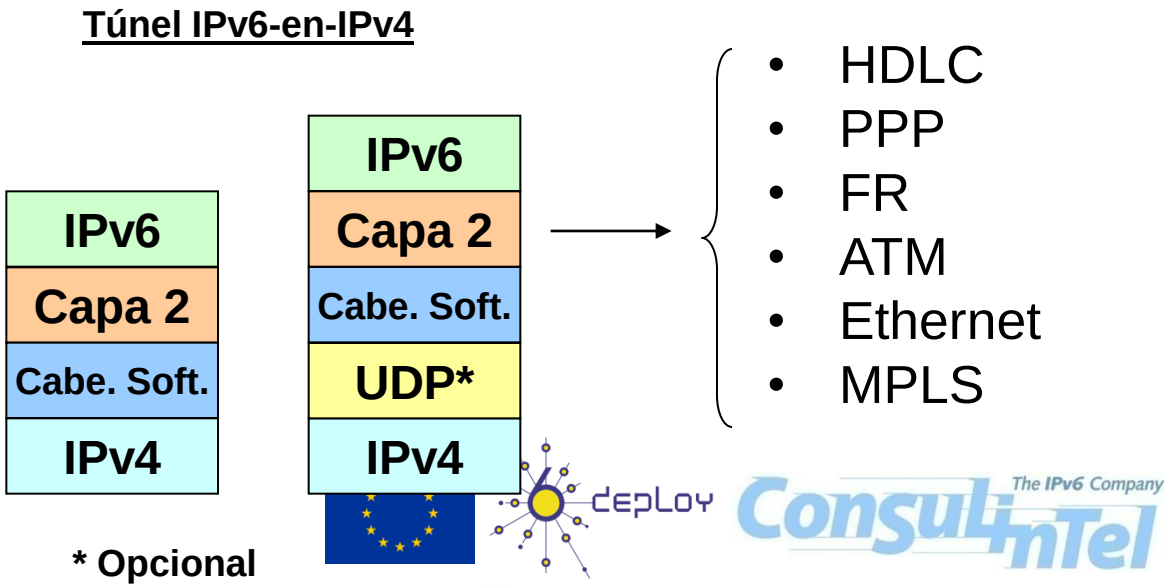
Ejemplo de uso de Softwires

- 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

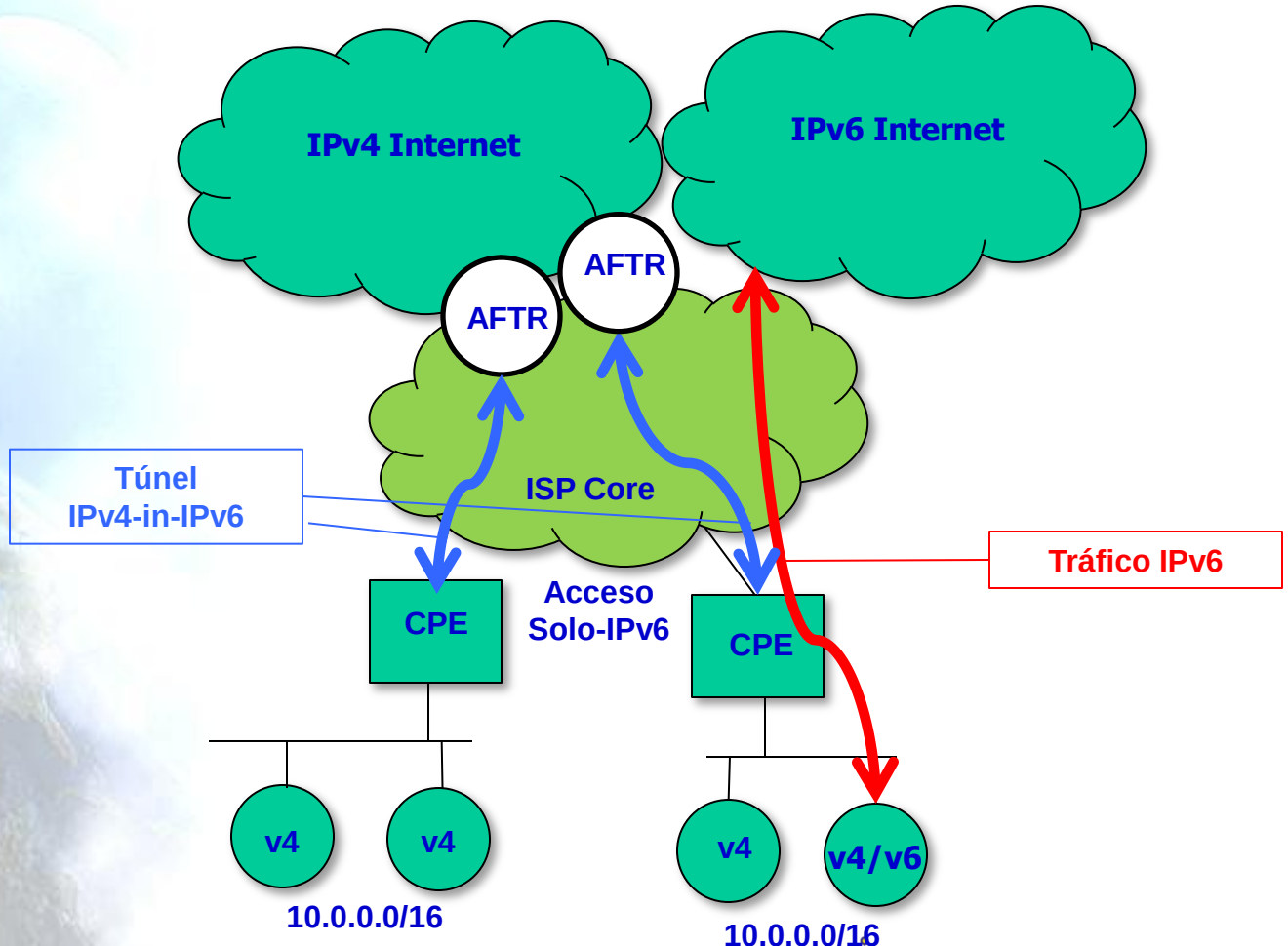


5.9 DS-Lite

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)

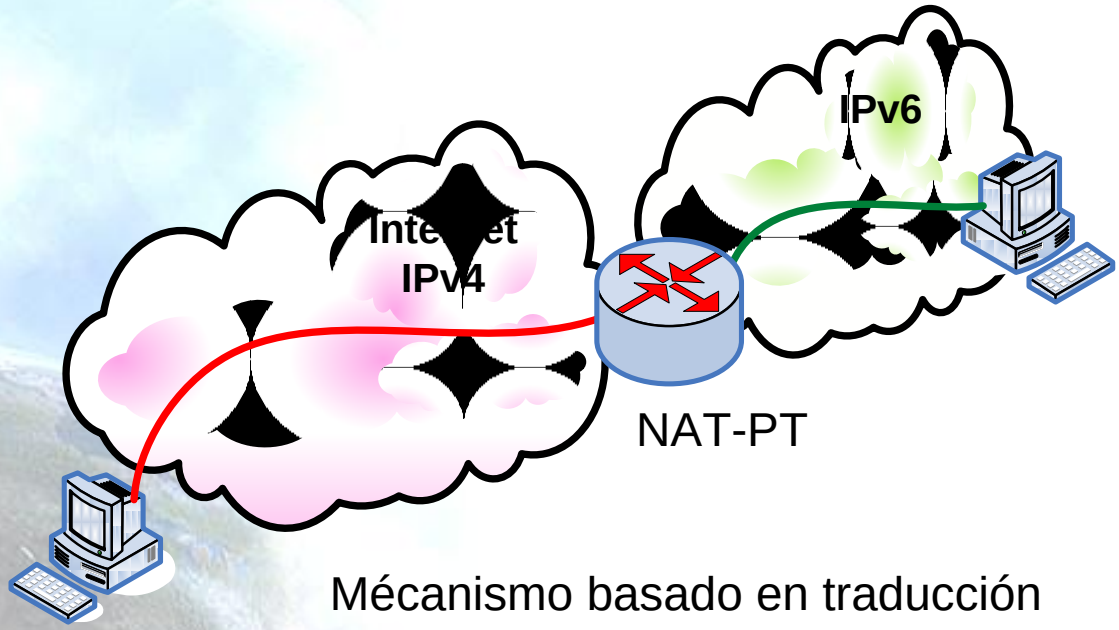


5.10 Traducción

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)



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.

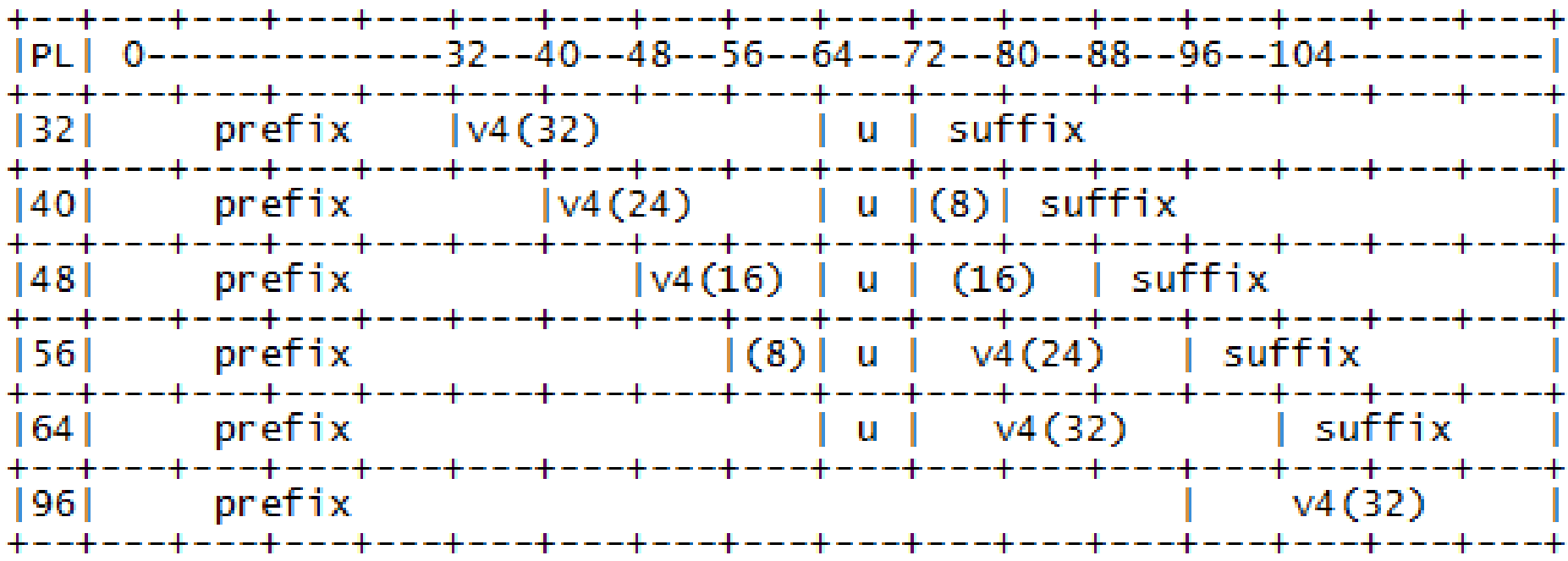
5.11 NAT64

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

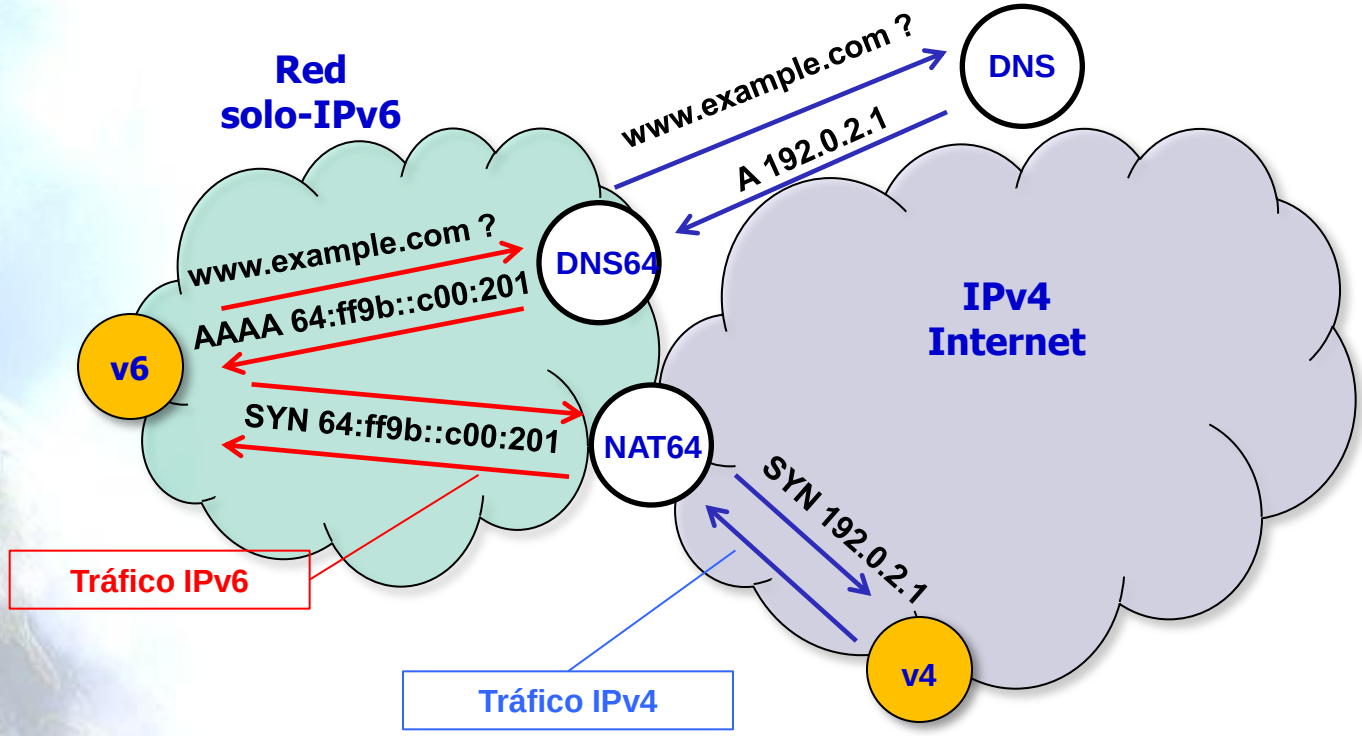


DNS64

- 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

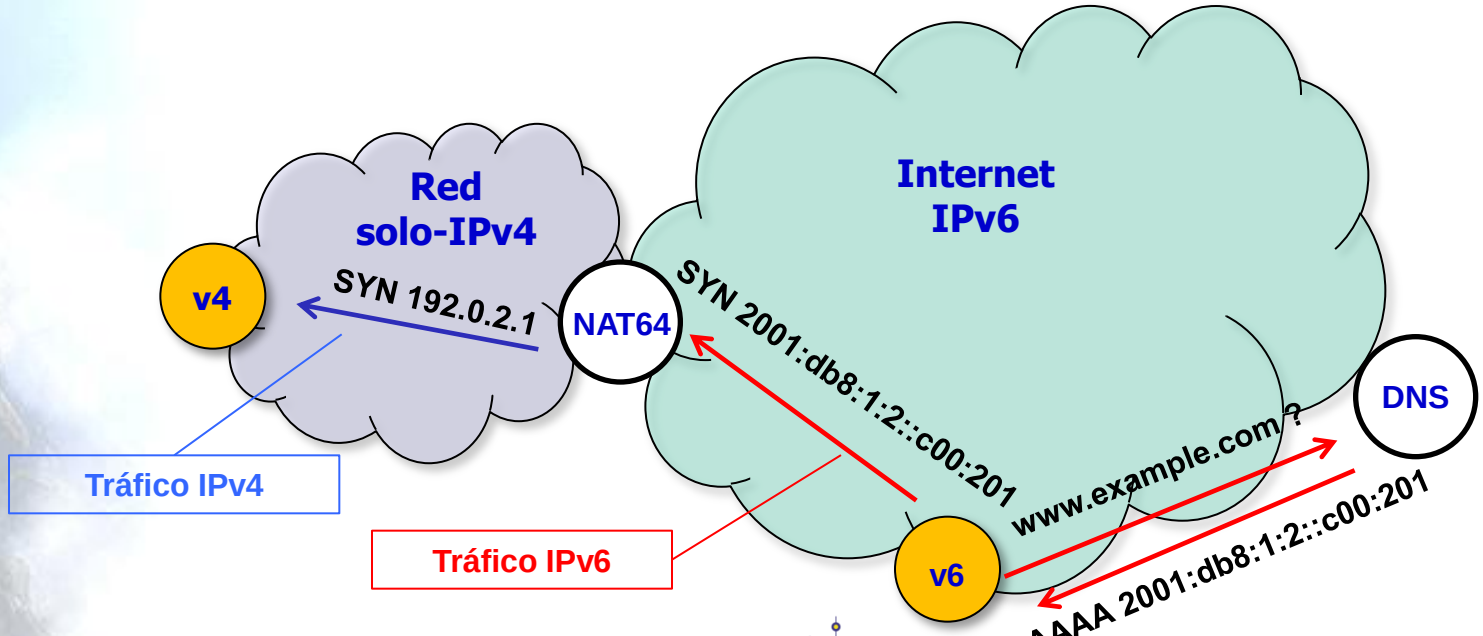
Stateful NAT64

- 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.

5.12 NAT66 (NPT)

NAT66 / NPT (1)

- NAT se usaba en IPv4 para traducir direcciones, para poder dar servicio a muchas IPs privadas con pocas públicas (NAPT incluyendo el uso de puerto)
- Con IPv6 no hay necesidad de más direcciones y se pretendía defender el paradigma extremo a extremo del Internet inicial
- Pero sigue habiendo gente que pide NAT para IPv6 alegando que aporta beneficios, sin valorar inconvenientes:
  - "Oculta la red" o "NAT da seguridad": Esto es falso y se obtiene algo mejor utilizando firewalls
  - "Facilita la renumeración", no en todos los casos. Para IPv6 existe la posibilidad de usar prefijos PI
  - Permite Mutlihoming sin incrementar tablas rutas. En IPv6 se puede usar routing (BGP) o PI. (SHIM6, LISP)
- Otro argumento es que los fabricantes van a implementar IPv6 de todas formas y no se debe repetir el error de no estandarizarlo antes

NAT66 / NPT (2)

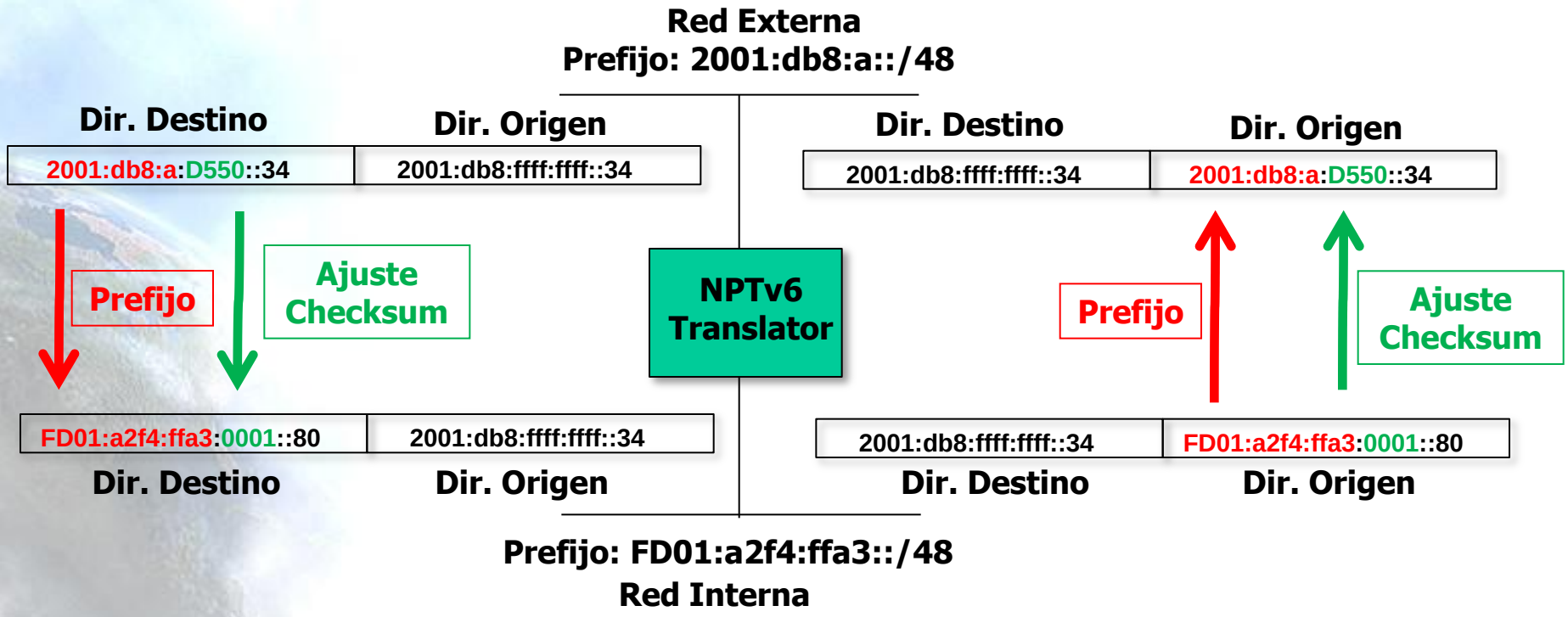
- Se define el NPTv6 (Network Prefix Translation) [RFC6296] con las siguientes características:
  - Stateless: no mantiene info de estado por nodo o por conexión
  - Independiente del transporte
  - Ofrece independencia de direcciones, como NAT44: no renumeración *dentro* y enrutamiento “forzado” por upstreams no necesario
  - Proporciona una relación 1:1 entre direcciones de *dentro* y *fuera*
  - Por lo anterior, no hay necesidad puertos y otros parámetros de transporte
  - Preserva la alcanzabilidad extremo-a-extremo en la capa de red
  - No ofrece los “beneficios de seguridad” de NAT44, usar FW
  - Si se usar varios, como no hay estado, no necesitan comunicarse y se puede hacer la traducción algorítmica igual en todos. Pueden por tanto encaminar asimétricamente, balancear carga y *fail-over*
  - Únicamente función de traducción algorítmica, neutral para el *checksum,* de dos sentidos
  - No toca nada de la capa de transporte (corrige *checksum* con campo de 16 bit cambiado adicionalmente a la dirección IPv6)

NAT66 / NPT (3)

- A pesar de tener ventajas con respecto a NAT44:
  - Modifica cabeceras IP en tránsito, posible problema con IPsec AH
  - Problema con aplicaciones que utilizan direcciones IP-> ALGs
  - El uso de dos prefijos (interno y externo) complica DNS -> Split DNS
  - Existen otras desventajas del uso de traducción (ver [RFC4864,RFC5902]) por lo que se debe tratar de usar otra solución

NPTv6 (1)

- **NPTv6 Translator**: Elemento que realiza la traducción de un prefijo IPv6 a otro. El prefijo más largo será el que marque la longitud (normalmente serán iguales)
- Se traduce en ambos sentidos, entre dos redes que pueden ser publica-privada o privada-privada



5.13 Solo-IPv6

Solo-IPv6 (1)

- Es una de las opciones existentes
- En algunos casos se optará por implementar redes solamente IPv6:
  - Facilidad de gestión y configuración
  - Falta de direcciones IPv4 públicas
  - Despliegue de nuevas redes para servicios novedosos (WSN – 6Lowpan)
  - Granjas de servidores solo-IPv6 con front-end doble-pila
  - Implementación válida “para siempre”
- Hay que habilitar una forma de acceder a contenido IPv4 a los nodos solo-IPv6: NAT64/DNS64
- A medida que proveedores de contenido principales implementen IPv6, menos problemas

Gracias !!

Contacto:

- Alvaro Vives (Consulintel): alvaro.vives@consulintel.es