Capacitación: Despliegue de IPv6

Teoría Día 1

Alvaro Vives (alvaro.vives@consulintel.es)

ALICE2 – CLARA Technical Training
July 6 to 8, 2020
San Salvador, El Salvador

This project is funded by the European Union

A project implemented by CLARA

Agenda

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

1. Introducción a IPv6

¿Porque un Nuevo Protocolo de Internet?

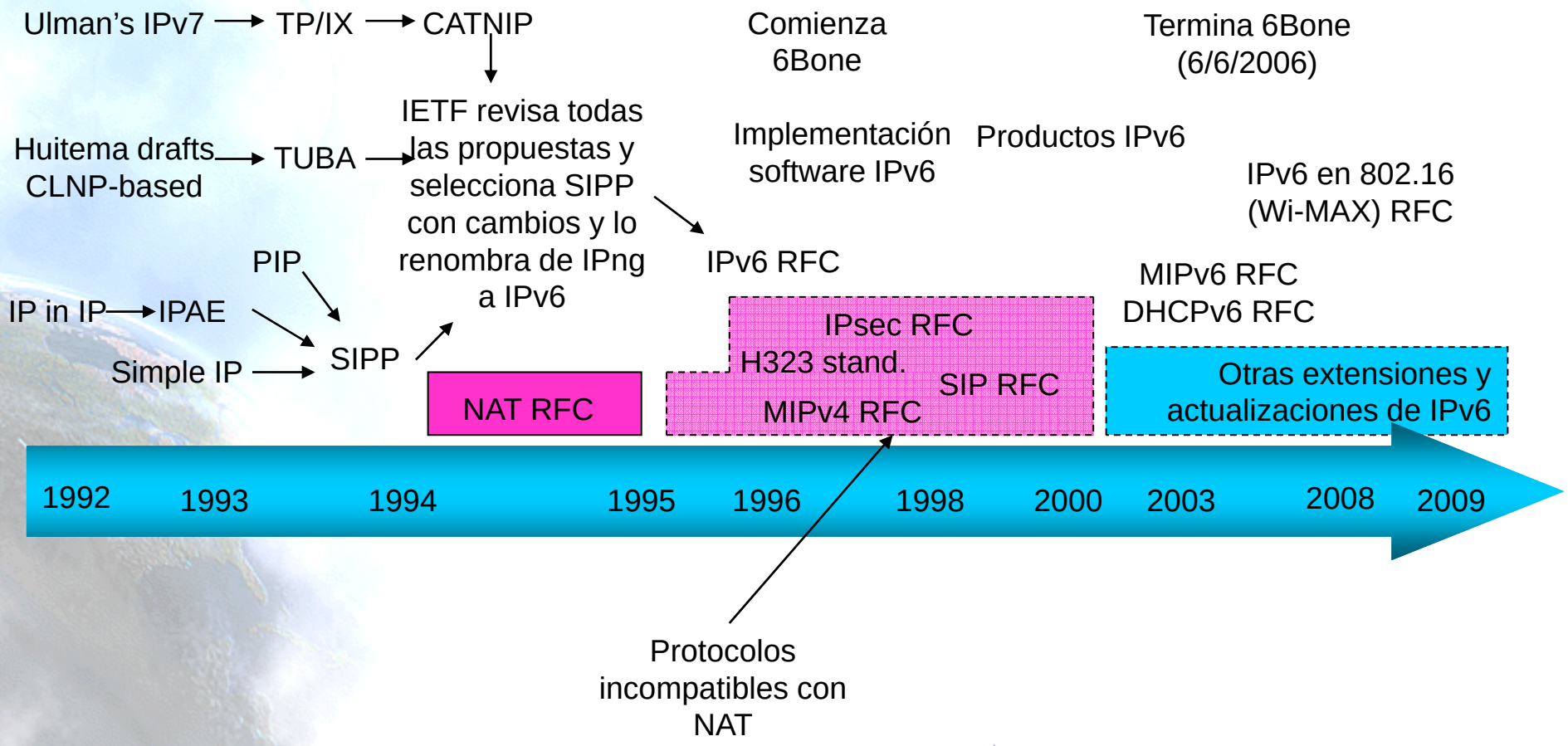
Un único motivo lo impulsó: Más direcciones!

- 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, 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

Evolución de IPng



Agotamiento Direcciones IPv4 (1)

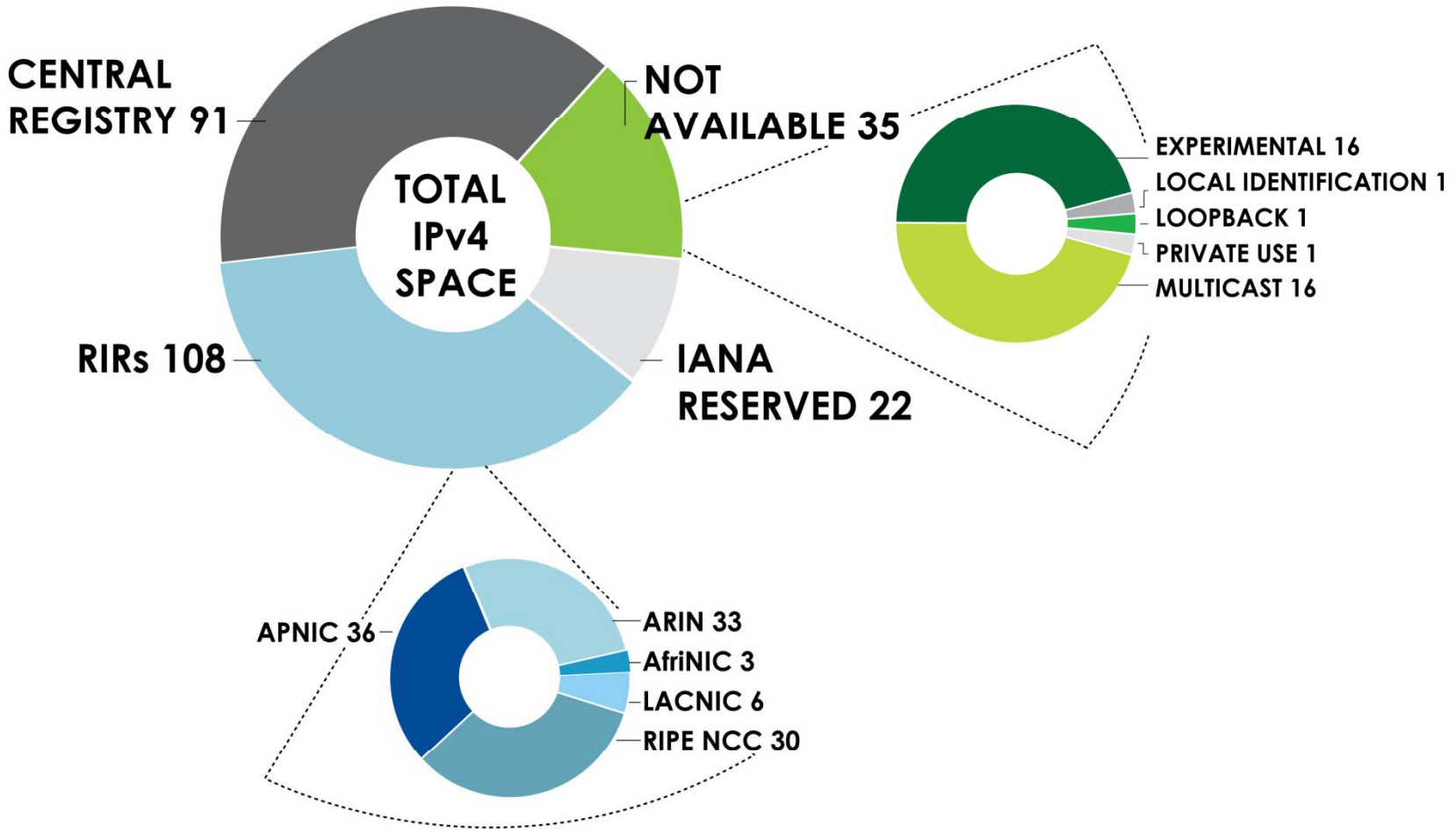
- Opinión extendida: quedan pocos años de direcciones IPv4 públicas -> Debate: Cuando se agotarán?
- Tres estrategias a seguir:
  - Aumentar el uso de NAT -> **introduce problemas técnicos y costes**
  - Tratar de obtener direcciones IPv4 libres o liberadas
  - Implementar IPv6 -> **válida a largo plazo**
- 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)

Año	Mes	/8s Disponibles (IANA)	Consumo Anual
2006	Diciembre	55	12
2007	Diciembre	42	13
2008	Diciembre	34	8
2009	Diciembre	26	8
2010	Marzo	22	4

- 22 /8s significa el 8,6 % de direcciones disponibles
- Fuente http://www.nro.net a 31 de Marzo 2010

Agotamiento Direcciones IPv4 (3)



Fuente http://www.nro.net a 31 de Marzo 2010

Desventajas de NAT

- La traducción se hace compleja a veces (FTP, etc.)
- No es escalable
- Puede dar problemas al unificar varias redes
- Rompe el paradigma end-to-end de Internet
- No funciona con gran número de “servidores”, P2P
- Inhiben el desarrollo de nuevos servicios y aplicaciones
- Problemas con IPsec
- Aumenta el coste de desarrollo de aplicaciones
- Comprometen las prestaciones, robustez, seguridad y manejabilidad de Internet

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)

Resumen de las Principales Ventajas de IPv6

- Capacidades expandidas de direccionamiento
- Autoconfiguración y reconfiguración “sin servidor” (“plug-n-play”)
- Mecanismos de movilidad más eficientes y robustos
- Incorporación de encriptación y autenticación en la capa IP
- Formato de la cabecera simplificado e identificación de flujos
- Soporte mejorado de opciones/extensiones

Motivación (1)

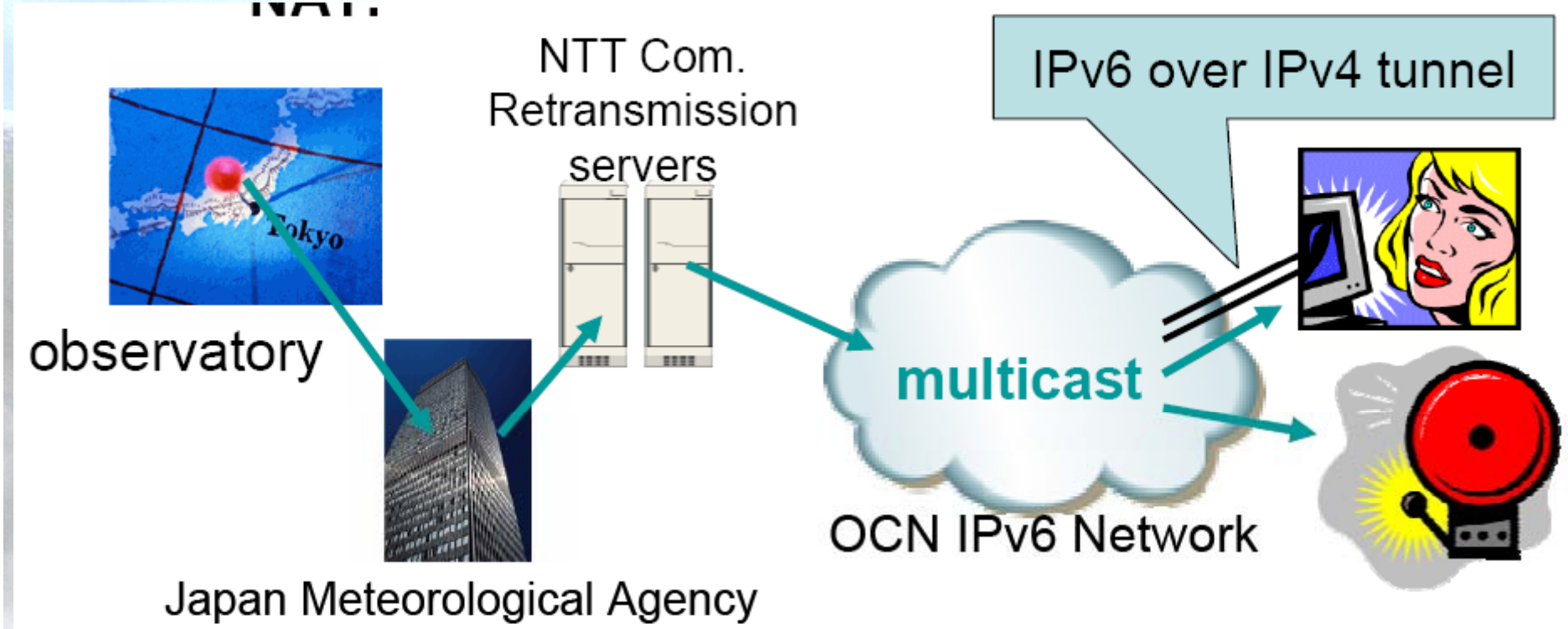
- Hay varias razones para implementar IPv6 en su red de datos operativa:
  - **Recomendación de LACNIC** (20-6-2007): "… los recursos de direcciones IP versión cuatro están en camino de terminarse. Por ello recomendamos preparar los más pronto posible las redes regionales para el uso del protocolo de Internet versión seis."
  - **Agotamiento de direcciones IPv4**: Se calcula que en el 2010 la IANA se quedará sin direcciones públicas
  - **Tecnologías que se conciben con IPv6**: Los estándares de 3G recomiendan el uso de IPv6. La movilidad IP con IPv6 (MIPv6) abre un abanico de posibilidades que pueden aprovecharse para ofrecer nuevos servicios

Motivación (2)

- Hay varias razones para implementar IPv6 en su red de datos operativa (cont.):
  - **Preparados para el futuro**: Lo que esta por venir sin duda se basará en IPv6, hay que estar preparados para ello
  - **Estar a la vanguardia tecnológica de la región**: Oportunidad única para subir un escalón en tecnologías de red y en imagen dentro de Latinoamérica y el Caribe
  - **Nuevas oportunidades**: IPv6 es un “habilitador” de nuevos servicios y por tanto de nuevas oportunidades de negocio

Casos de Éxito: NTT

- Se detecta onda-P y se envía una alerta de onda-S.
- Se usa multicast IPv6. Se consiguen retardos pequeños.
- IPv4 no serviría para este modelo “Push” debido a NAT.
- 5$/mes por casa y 300$/mes por edificio.



2. Formatos de cabeceras y tamaño de paquetes

2.1 Terminología
2.2 Formato cabecera IPv6
2.3 Consideraciones sobre tamaño de paquete

2.1 Terminología

IPv6 (RFC2460)

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

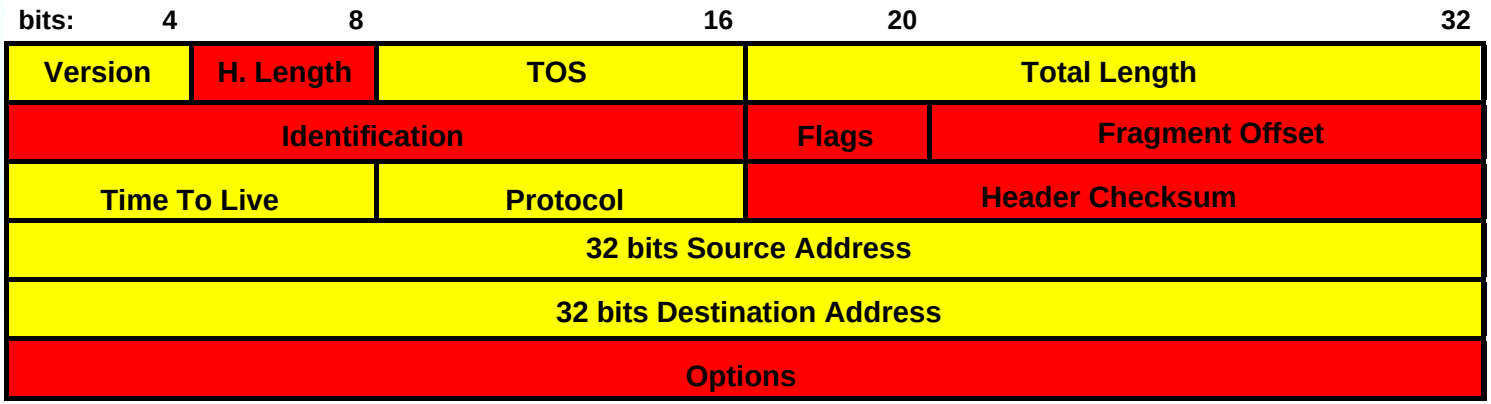
Terminología

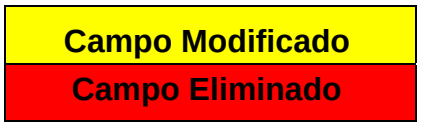
- **Node:** Dispositivo que implementa IPv6
- **Router:** Nodo que reenvía paquetes IPv6
- **Host:** Cualquier otro nodo que no es un router
- **Upper Layer:** Protocolo que está inmediatamente por encima de IPv6
- **Link:** Medio o entidad de comunicación sobre la que los nodos pueden comunicarse a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

2.2 Formato cabecera IPv6

Formato de la Cabecera IPv4

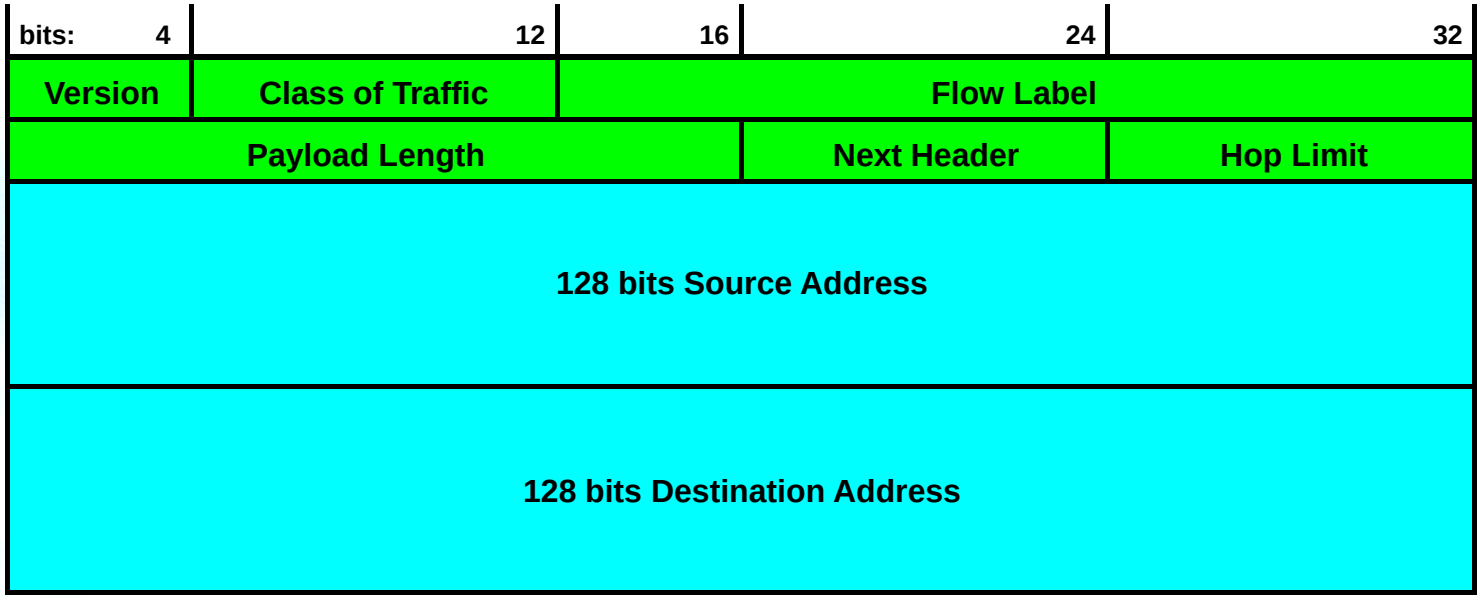
- 20 Bytes + Opciones (40 Bytes máximo)
  - Tamaño variable: 20 Bytes a 60 Bytes





Formato de la Cabecera IPv6

- Reducción de 12 a 8 campos (40 bytes)



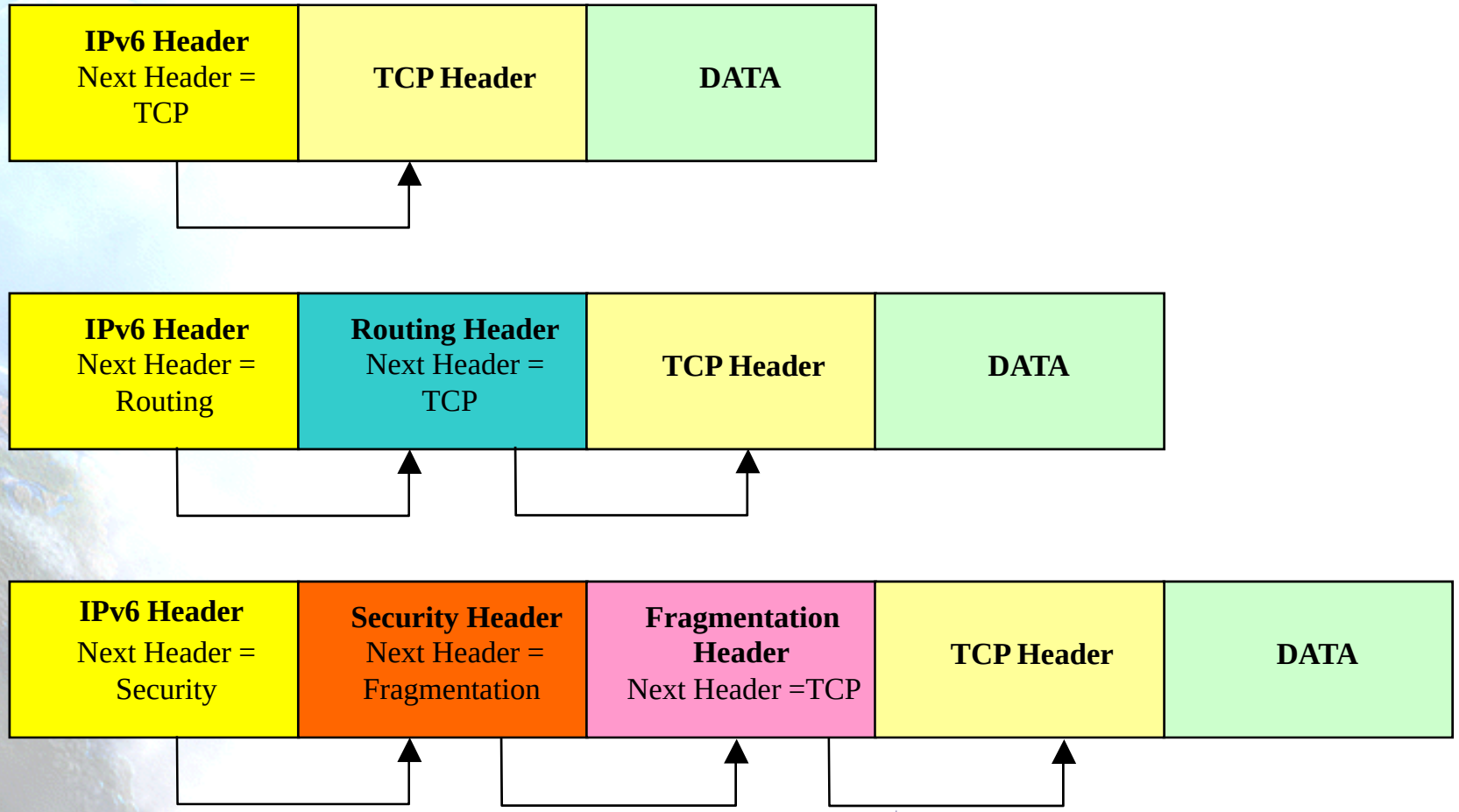
  - Evitamos la redundancia del checksum
  - Fragmentación extremo-a-extremo

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**

Cabeceras de Extensión

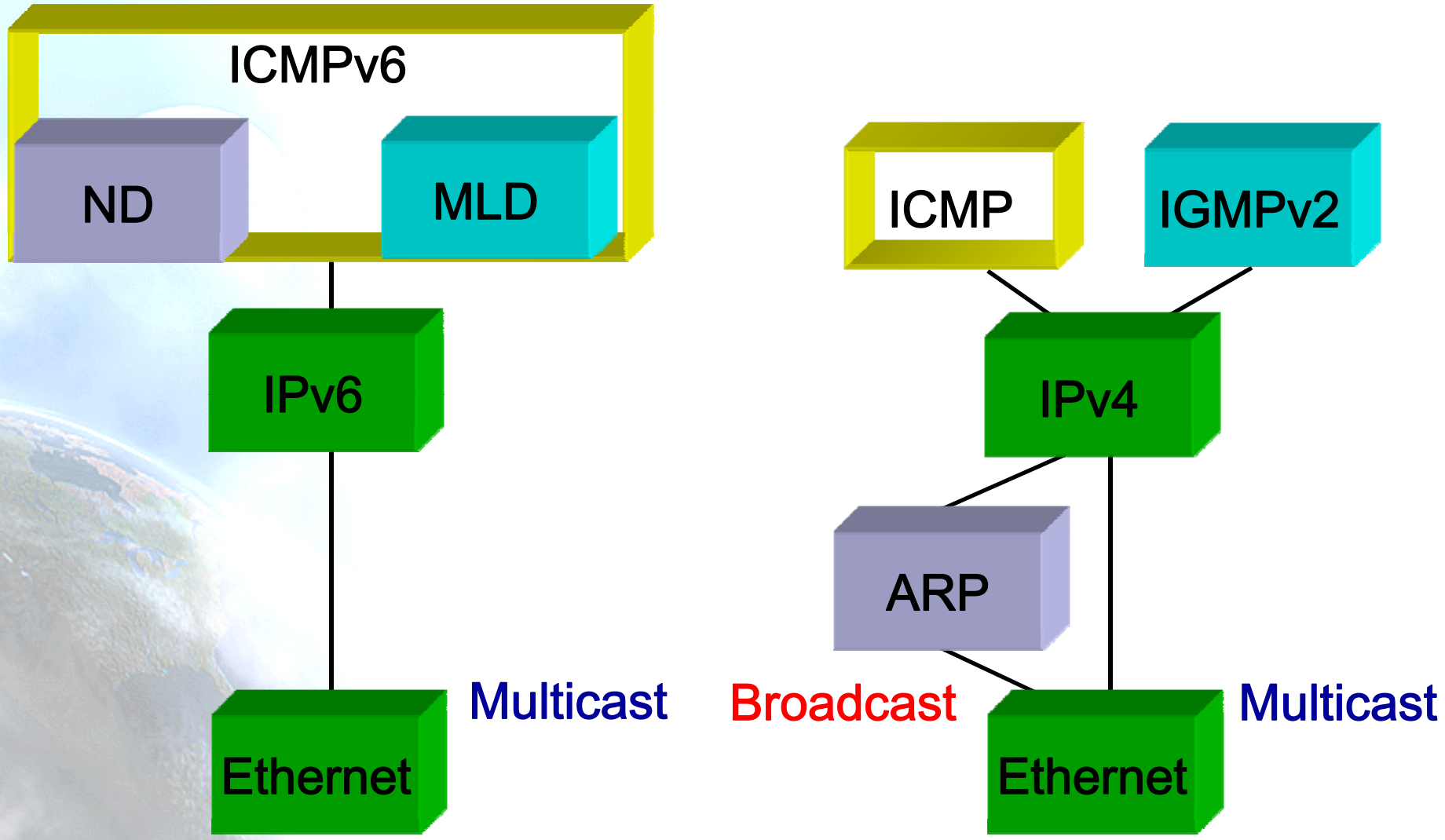
- Campo “Next Header”



Ventajas de las Cabeceras de Extensión

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

Plano de Control IPv4 vs. IPv6



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**

Proceso de Fragmentación

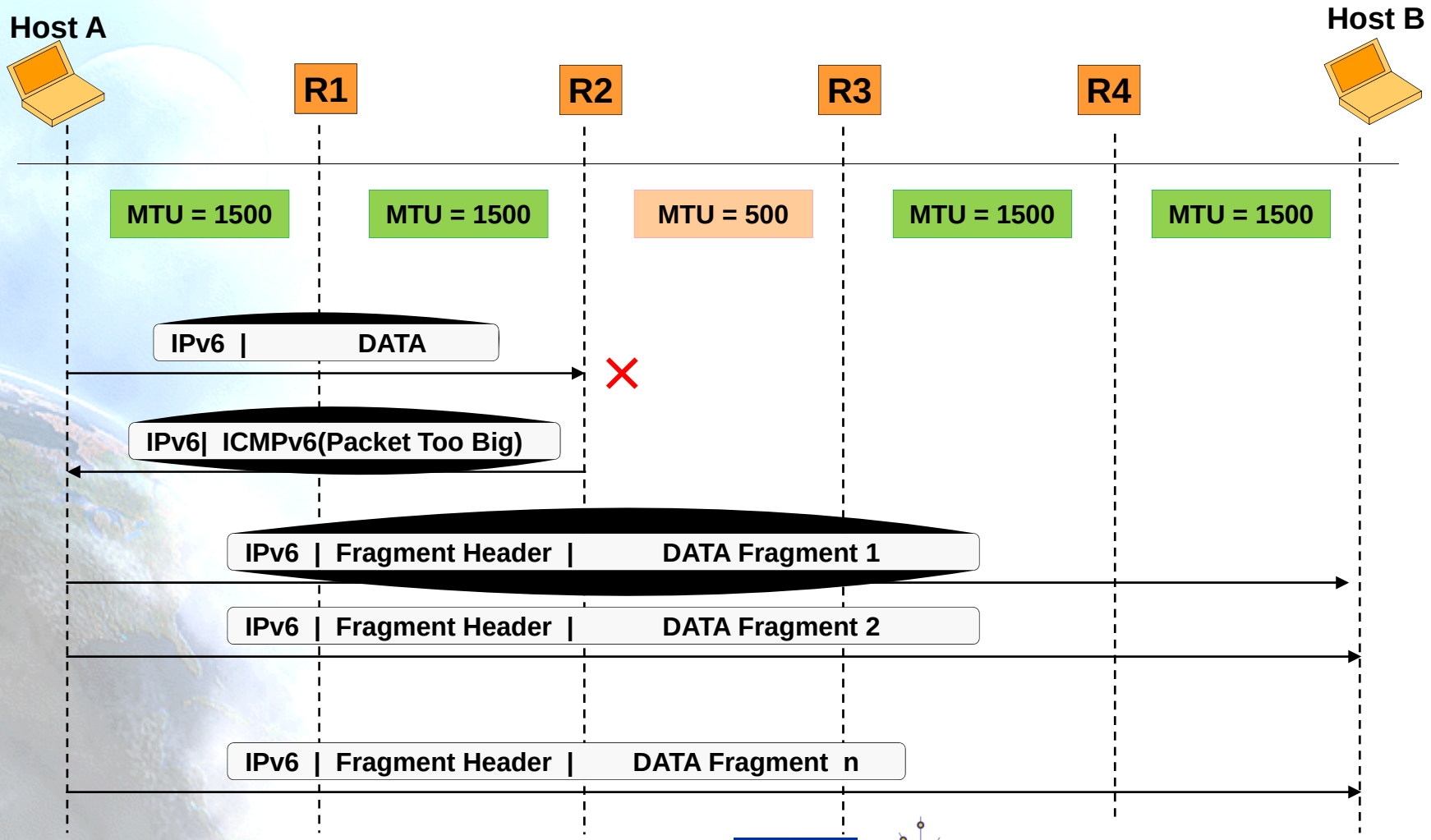
- La parte fragmentable del paquete original se divide en fragmentos de tamaño múltiplo de 8 bytes, excepto el último. Cada fragmento se envía en paquetes separados

Unfragmentable Part	1st Fragment	2nd Fragment	...	Last Fragment

- Paquetes fragmentados:

Unfragmentable Part	Fragment Header	1st Fragment
Unfragmentable Part	Fragment Header	2nd Fragment
• • •		
Unfragmentable Part	Fragment Header	Last Fragment

Fragmentación en Origen



2.3 Consideraciones sobre tamaño de paquete

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.

Descubrimiento del Path MTU (RFC1981)

- Las implementaciones deben realizar el descubrimiento del path MTU enviando paquetes mayores de 1280 bytes.
  - Para cada destino, se comienza asumiendo el MTU del primer salto
  - Si un paquete llega a un link en el que el MTU es menor que su tamaño, se envía al nodo origen un paquete ICMPv6 “packet too big”, informando del MTU de ese link. Dicho MTU se guarda para ese destino específico
  - Ocasionalmente se descartan los valores almacenados de MTU para detectar posibles aumentos del MTU para los diversos destinos
- Las implementaciones minimalistas pueden omitir todo el proceso de descubrimiento de MTU si observan que los paquetes de 1280 bytes pueden llegar al destino.
  - Útil en implementaciones residentes en ROM

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 Planes de direccionamiento
3.7 Gestión de 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

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**

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**

Ejemplos:

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

   Queda: 2001:db8:3003:1::6543:ffe
2. (Alumnos) 2001:0db8:0000:0000:0300:0000:0000:0abc

Prefijos de los Tipos de Direcciones

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

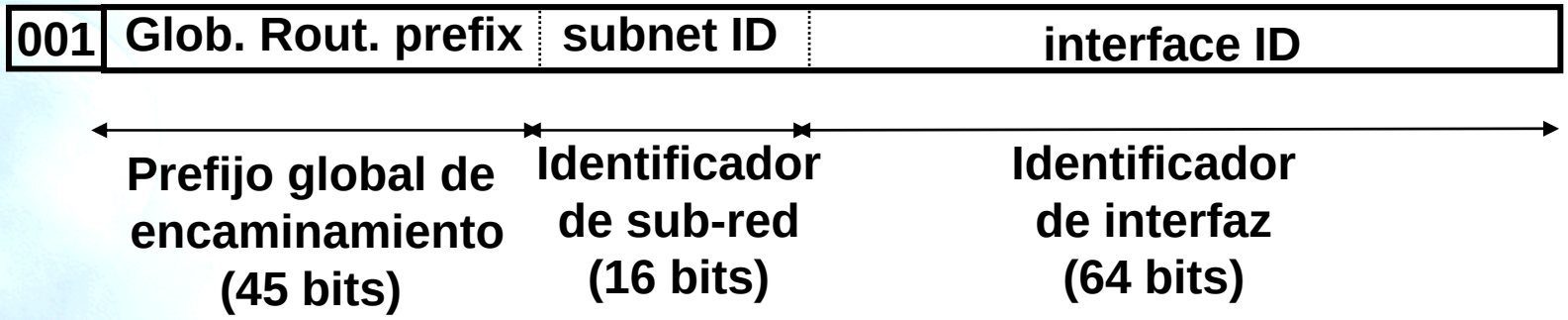
- Direcciones **Anycast** se asignan de los prefijos Unicast

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)

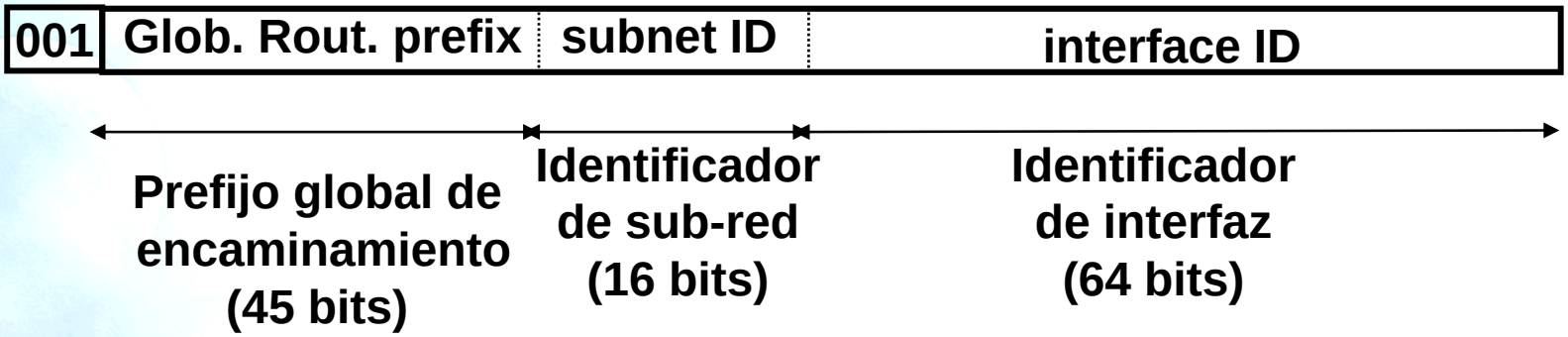
- El prefijo **2000::/3** se esta usando para las asignaciones de direcciones Globales Unicast, todos los demás prefijos están reservados (aprox. 7/8 del total).

Dirección Global Unicast (RFC3587)



- El prefijo de encaminamiento global es un valor asignado a un zona (site), es decir, a un conjunto de sub-redes/links. Se ha diseñado para ser estructurado jerárquicamente por los RIRs e ISPs
- El ID de sub-red es un identificador de una subred dentro de un site. Se ha diseñado para ser estructurado jerárquicamente por el administrador del site
- El identificador de interfaz se construye normalmente según el formato EUI-64

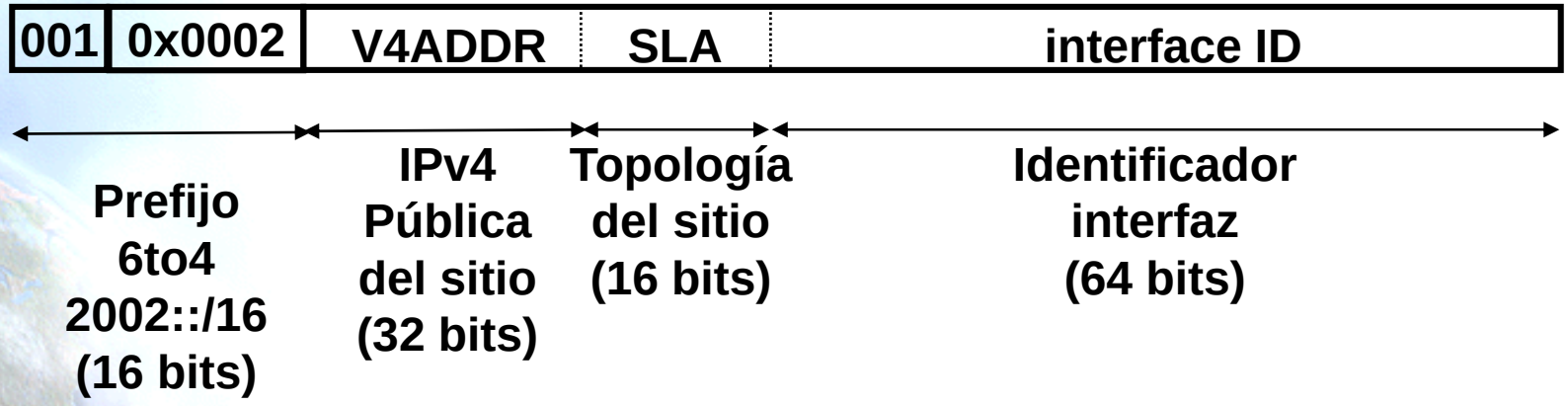
Dirección Global Unicast para Servicios de Producción



- Los ISPs normalmente toman prefijos /32
  - Las direcciones IPv6 de producción empiezan por **2001, 2003, 2400, 2800, etc.**
- Hasta /48 se estructura jerárquicamente por el ISP según el uso interno
- Desde /48 hasta /128 se delega a los usuarios
  - Recomendaciones para la delegación de direcciones (RFC3177)
    - /48 caso general, excepto para abonados grandes
    - /64 si se sabe que una y solo una única red es necesaria
    - /128 si es absolutamente seguro que se va a conectar uno y solo un dispositivo

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)

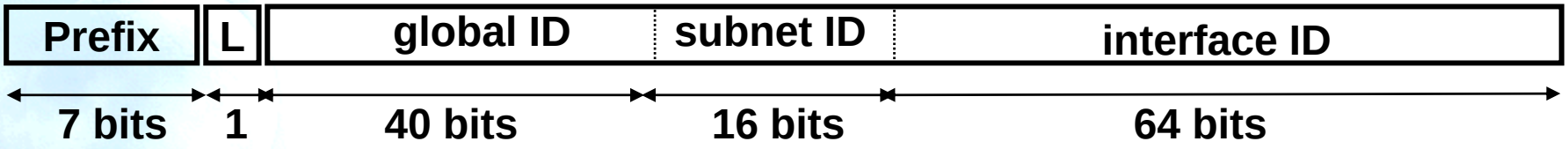
- Prefijo global con alta probabilidad de ser único
- Para comunicaciones locales, normalmente dentro de un “site”
- No son prefijos que vayan a ser encaminados en la Internet Global
- Son prefijos encaminables dentro de un área más limitada, como un determinado “site”
- Incluso podrían ser encaminados 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

ULA Asignadas Centralmente

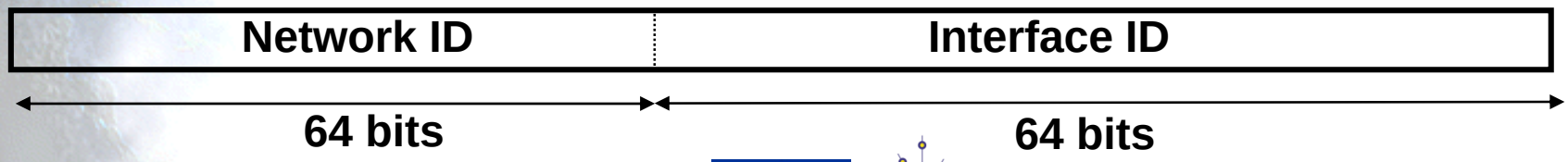
- La principal diferencia entre ambas asignaciones:
  - Las asignadas centralmente son direcciones únicas y la asignación se registra en una base de datos pública (para resolver disputas)
- Recomendación: “sites” que planeen hacer uso de ULA, usen prefijos asignados centralmente para evitar posibilidad de conflicto (no existe obligación, es una recomendación)
- El procedimiento de asignación para crear global-IDs en la asignación centralizada es configurando L=0, mientras que la asignación local es con L=1, según se define en RFC4193
- Más información sobre políticas en RIRs para asignaciones centralizadas
  - http://www.arin.net/meetings/minutes/ARIN_XVIII/ppm2_transcript.html#anchor_3
  - http://www.arin.net/meetings/minutes/ARIN_XIX/ppm1_notes.html

3.4 Identificadores de interfaz

Identificadores de Interfaz

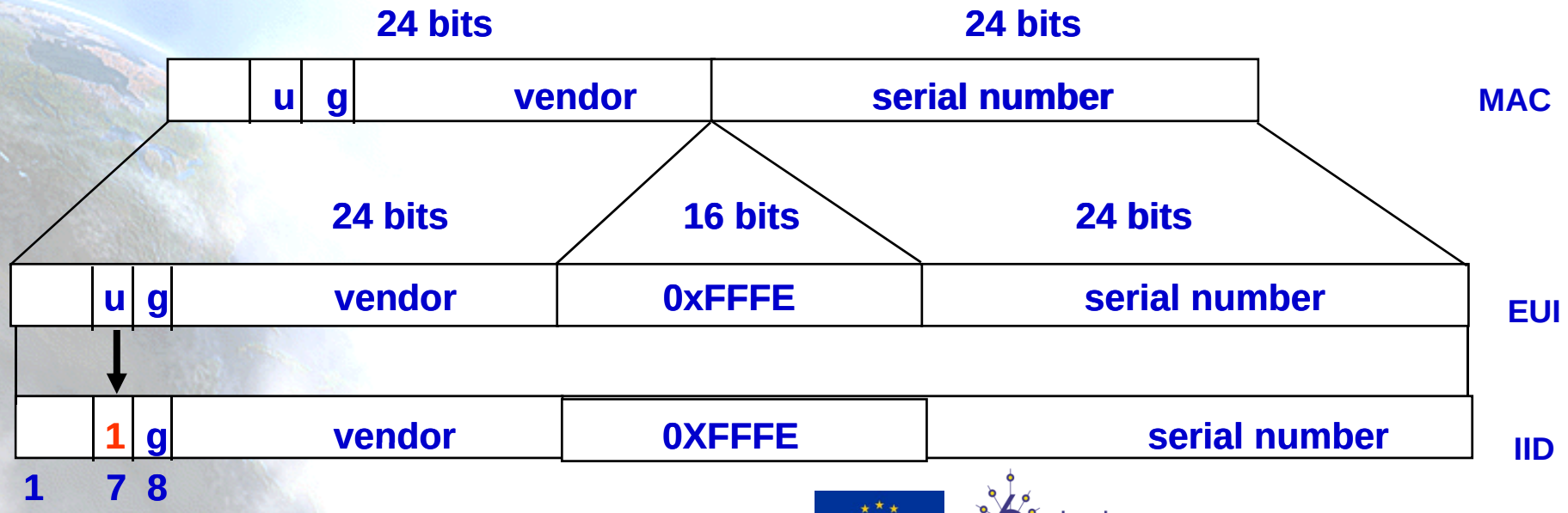
Los 64-bits de menor peso de las direcciones Unicast pueden ser asignados mediante diversos métodos:

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



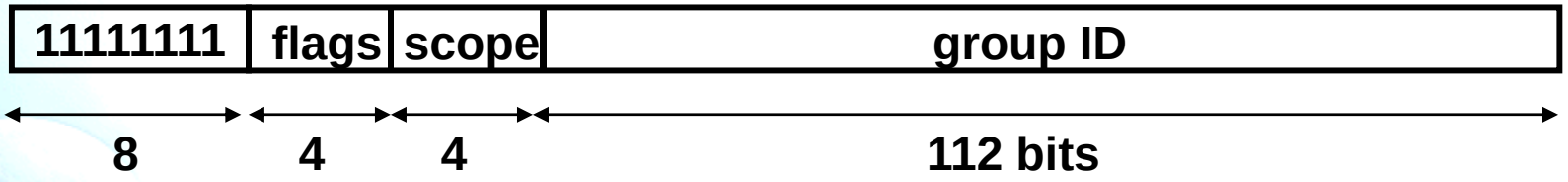
EUI-64

- 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
  - P: Asignación basada, o no, en un prefijo de red
  - R: Dirección de un Rendezvous Point incrustada, o no
- Scope:
  1 - Interface-Local
  2 - link-local
  4 - admin-local
  5 - site-local
  8 - organization-local
  E - global

(3,F reservados)(6,7,9,A,B,C,D sin asignar)

3.6 Planes de direccionamiento

Direcciones Obligatorias Nodo IPv6

- Direcciones obligatorias en un Host IPv6:

1. Dirección Link-Local para cada interfaz.
2. Cualquier otra dirección Unicast y Anycast adicional que se haya configurado en las interfaces del nodo (manual o automáticamente).
3. Dirección de loopback.
4. Direcciones multicast de todos-los-nodos (All-Nodes)(FF01::1, FF02::1).
5. Dirección multicast Solicited-Node para cada una de las direcciones unicast y anycast.
6. Direcciones Multicast de todos los grupos a los que el nodo pertenezca.

- Direcciones obligatorias en un Router IPv6: Host +:

1. Direcciones Anycast Subnet-Router para todas las interfaces para las que este configurado que se comporte como un router.
2. Todas las demás direcciones Anycast que se hayan configurado en el router.
3. Direcciones multicast All-Routers (FF01::2, FF02::2, FF05::2).

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
   - Por ejemplo, podría ser necesario tener redes IPv6 /64 exclusivas para conectar electrodomésticos de la cocina, otra red diferente para sensores de presencia ubicados en las habitaciones del usuario, otra red para dispositivos de seguridad como detectores de humo, gas, etc.

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 (8)

#	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 múltiplo 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 Múltiplo 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 Múltiplo 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

4. ICMPv6, Neighbor Discovery y DHCPv6

4.1 ICMPv6

4.2 Neighbor Discovery

4.3 Autoconfiguración

4.4 DHCPv6

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

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

Tipos de mensajes de error ICMPv6

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

Mensajes ICMP Informativos

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

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

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

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"

Router Advertisements

- En una red (link) con capacidad broadcast, cada encaminador envía periódicamente paquetes multicast RA.
- Un host recibe los RAs de todos los encaminadores, construyendo una lista de encaminadores por defecto.
- El algoritmo de Neighbor Unreachability Detection (NUD) detecta si existen problemas en alcanzar los encaminadores.
- Los RAs contienen una lista de prefijos usados por los hosts para determinar si una dirección destino de un paquete pertenece a dicho link y para la autoconfiguración de direcciones.
- Los RAs y los 'Flags' asociados a cada prefijo permiten a los encaminadores indicar a los hosts como realizar la autoconfiguración (stateless o DHCPv6).

Comparación con IPv4

- IPv6 ND equivaldría a ARP, ICMP Router Discovery e ICMP Redirect en IPv4, con algunas cosas más (NUD).
- ND supone mejoras en muchos aspectos sobre los protocolos usados en IPv4, entre otras:
  - RAs llevan la dirección de la capa de enlace del encaminador, no es necesario resolverla.
  - RAs llevan los prefijos de un enlace, no es necesario un mecanismo para conocer la máscara de red.
  - RAs permiten la Autoconfiguración de direcciones.
  - REDIRECTS llevan la dirección de la capa de enlace del nuevo 'first hop', no es necesario resolverla.
  - El uso de direcciones de enlace local para identificar a los encaminadores, hace que los hosts 'resistan' una renumeración de la red.
  - Usando un 'Hop Limit' de 255 ND es inmune a mensajes ND de fuera del enlace. En IPv4 podían enviar de fuera Redirects y RAs.

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.

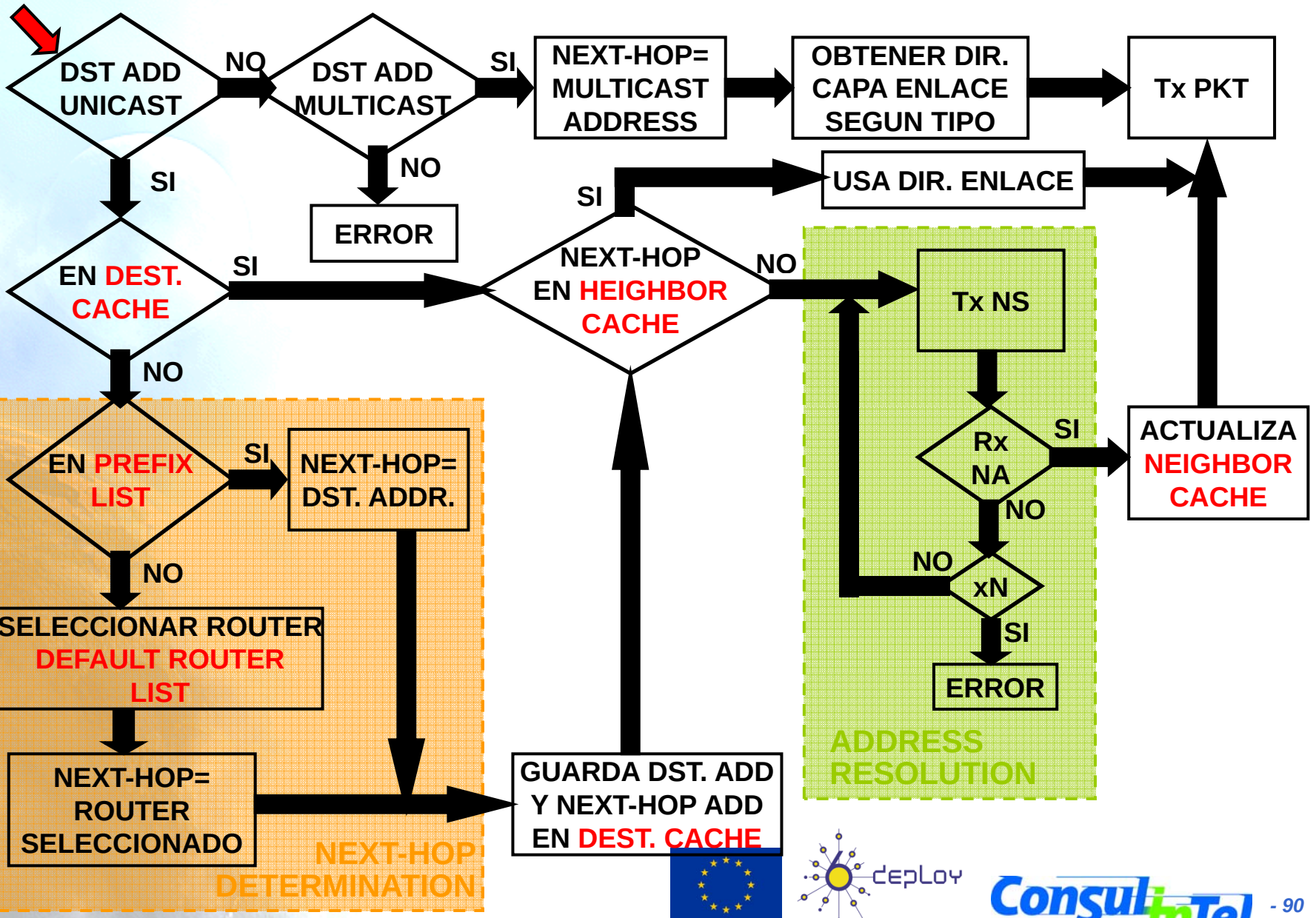
Bits 8	16	32
Type = 137	**Code = 0**	**Checksum**
Reserved = 0		
Target Address		
Destination Address		
Options …		

- 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” (SAAC) no precisa de configuración manual en el host, mínima (si acaso alguna) configuración de encaminadores y ningún servidor adicional

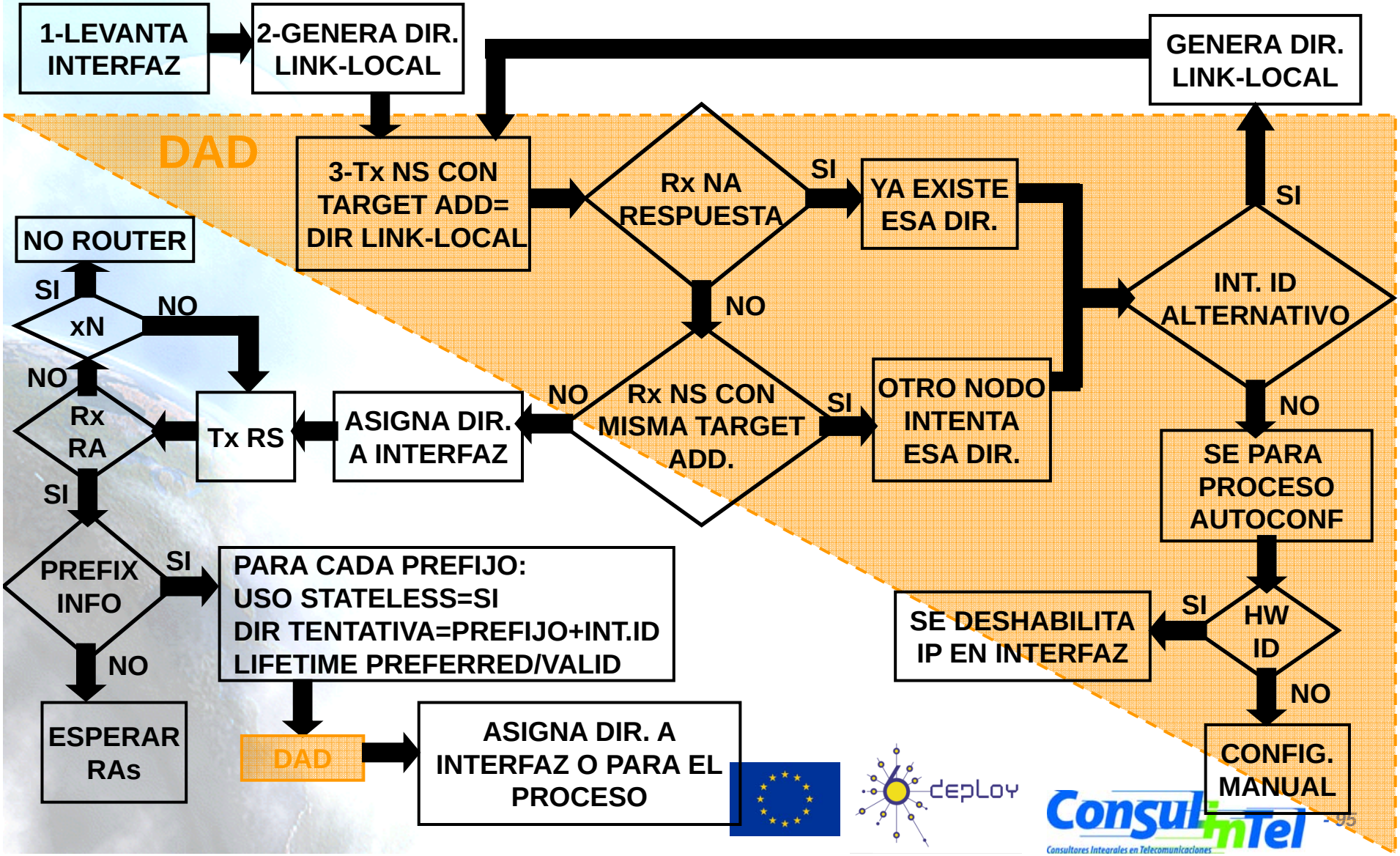
Autoconfiguración Stateless o Serverless (RFC4862)

- El mecanismo “stateless” permite a un host generar su propia dirección usando una combinación de información localmente disponible y de información proporcionada por los encaminadores
- Los **encaminadores anuncian los prefijos de red** que identifican la sub-red asociada a un determinado segmento de red (64 bits)
- Los **hosts generan un identificador de interfaz** que lo identifica de manera única en la subred. Dicho identificador se genera localmente, por ejemplo a partir de la dirección MAC (64 bits)
- Una dirección IPv6 se forma mediante la combinación de ambas informaciones
- En la ausencia de encaminadores, un host puede generar solo las direcciones IPv6 de ámbito local (link-local)
- Las direcciones link-local son suficiente para permitir la comunicación IPv6 entre nodos que están conectados en el mismo segmento de red

Ventajas/Beneficios de la Autoconfiguración Stateless

- La configuración manual de cada máquina antes de conectarla a la red no es necesaria
- Los sitios pequeños compuesto de pocas máquinas conectadas al mismo segmento no necesitarían de un servidor DHCPv6 ni de un encaminador para comunicarse, usarían direcciones link-local
- Un sitio grande con varias subredes no necesitaría de un servidor DHCPv6 para la configuración de direcciones
- Facilita el cambio de prefijo de una sitio mediante el uso de varias direcciones por interfaz y tiempo de vida

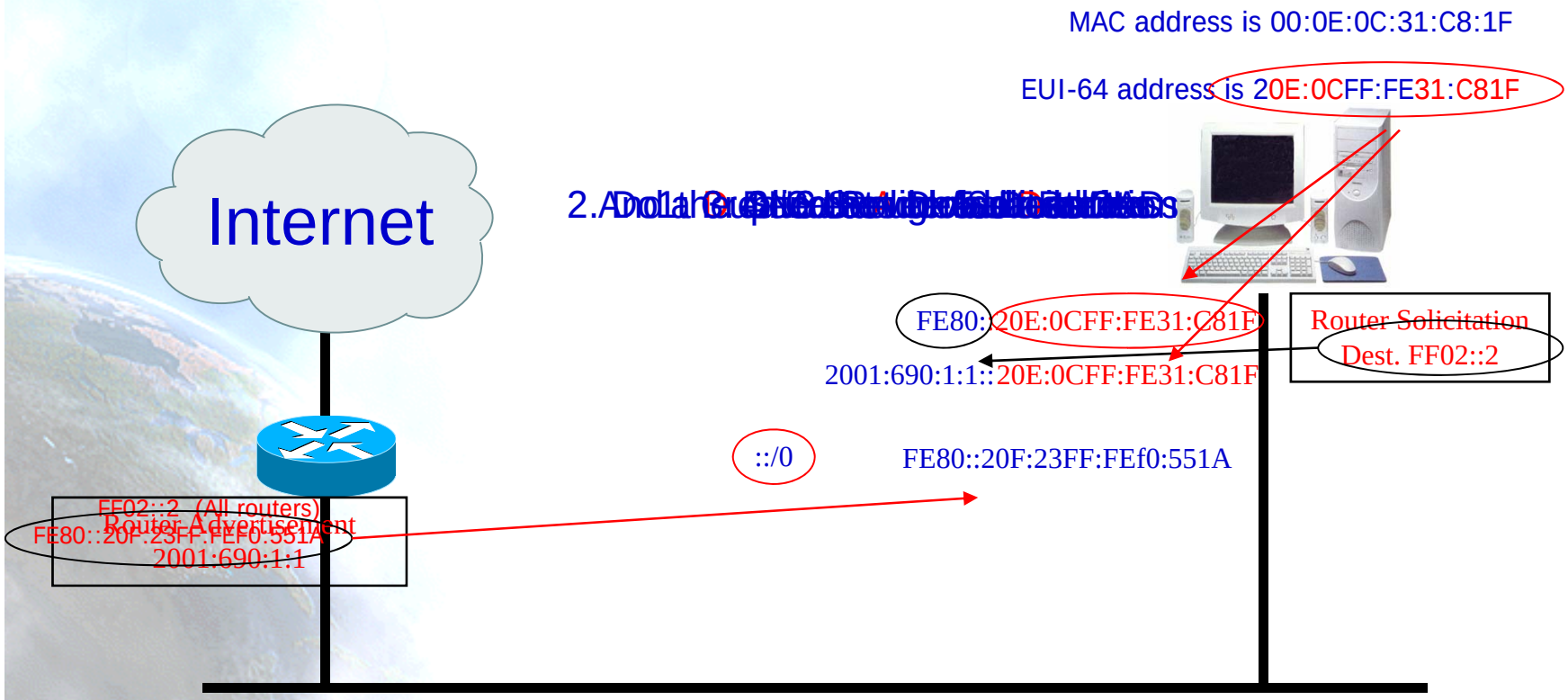
Funcionamiento de la Autoconfiguración Stateless



Tiempo de Validez de las Direcciones

- Las direcciones IPv6 se asignan a un interfaz por un tiempo determinado (posiblemente infinito) que indica el periodo de validez de la asignación
- Cuando el tiempo de asignación expira, la asignación ya no es válida y la dirección puede ser reasignada a otra interfaz de red en cualquier otra red dentro de Internet
- Con el fin de gestionar de una manera adecuada la expiración de las direcciones, una dirección pasa por dos fase distintas mientras está asignada a una interfaz.
  - Inicialmente una dirección es la preferida (preferred), lo cual significa que su uso en una comunicación arbitraria no está restringida
  - Más tarde, una dirección se convierte en “deprecada” anticipándose al hecho de que su asignación al interfaz de red será inválido en breve

Autoconfiguración Stateless

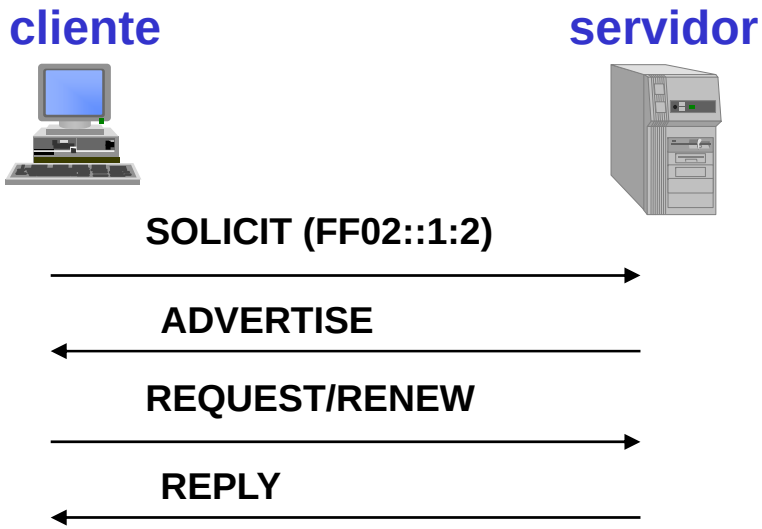


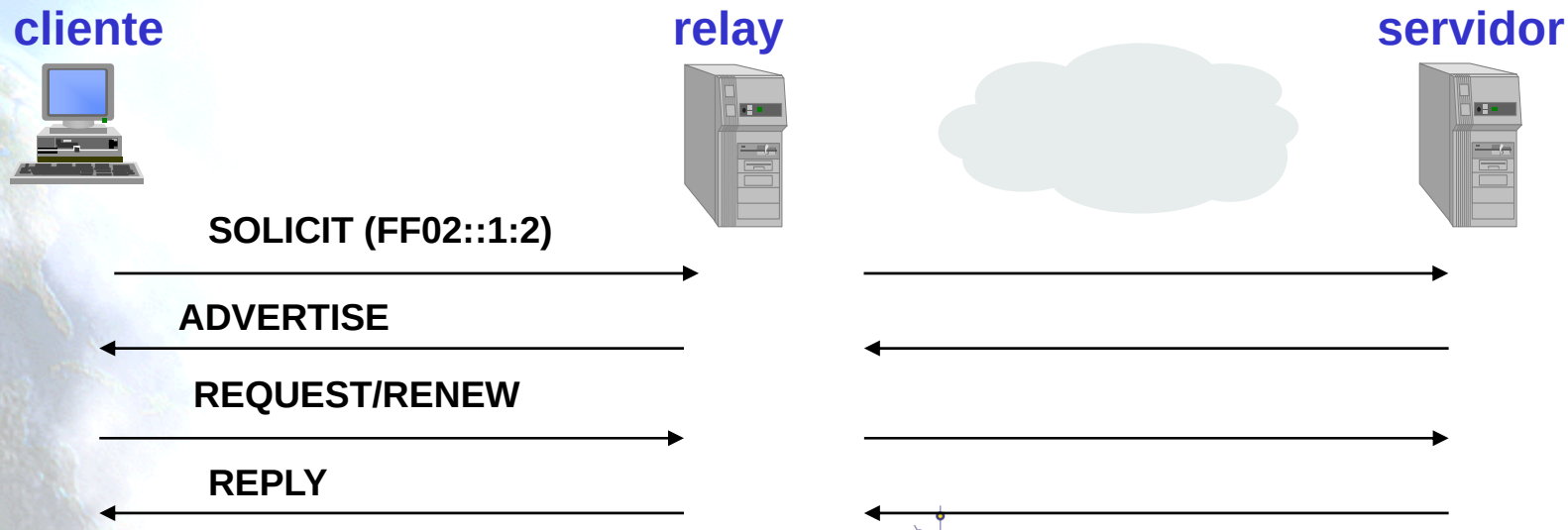
4.4 DHCPv6

DHCPv6

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

Ejemplo Básico de DHCPv6





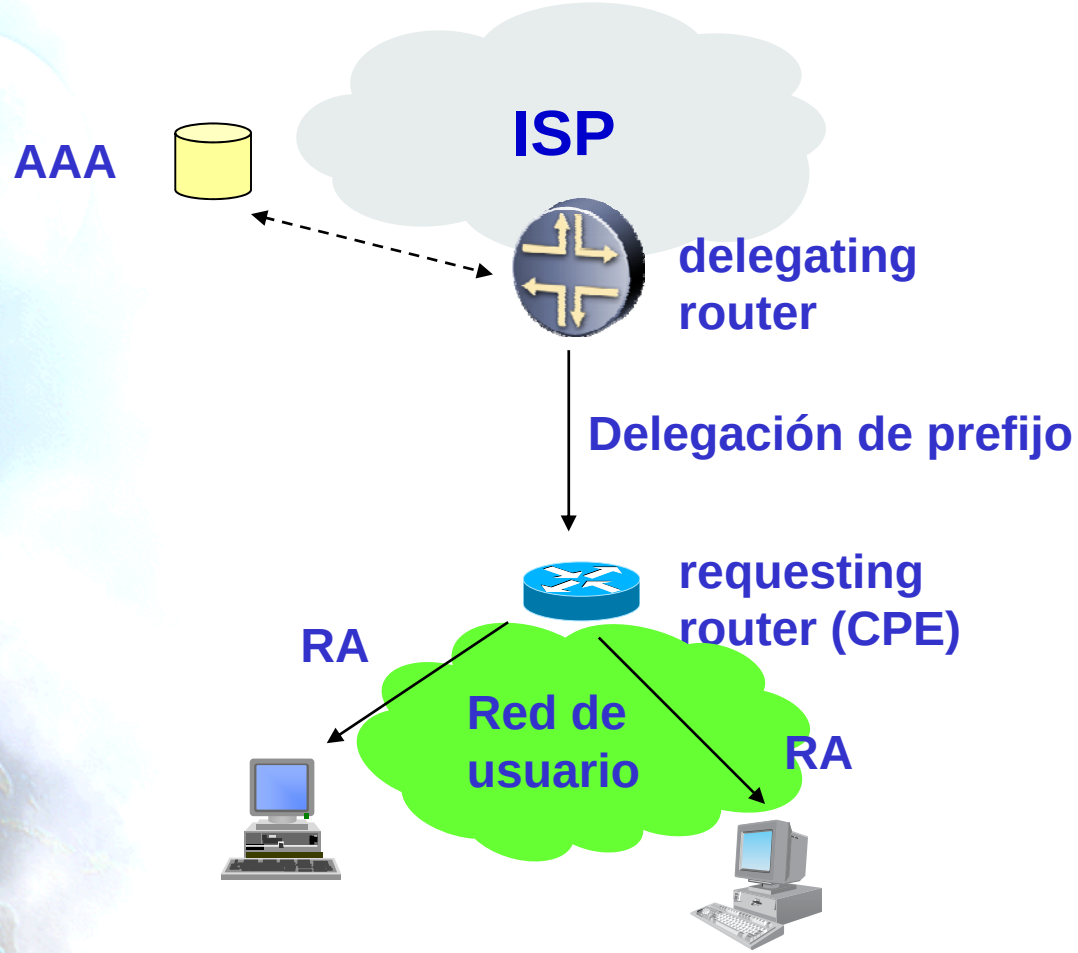
DHCPv6-PD (RFC3633)

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

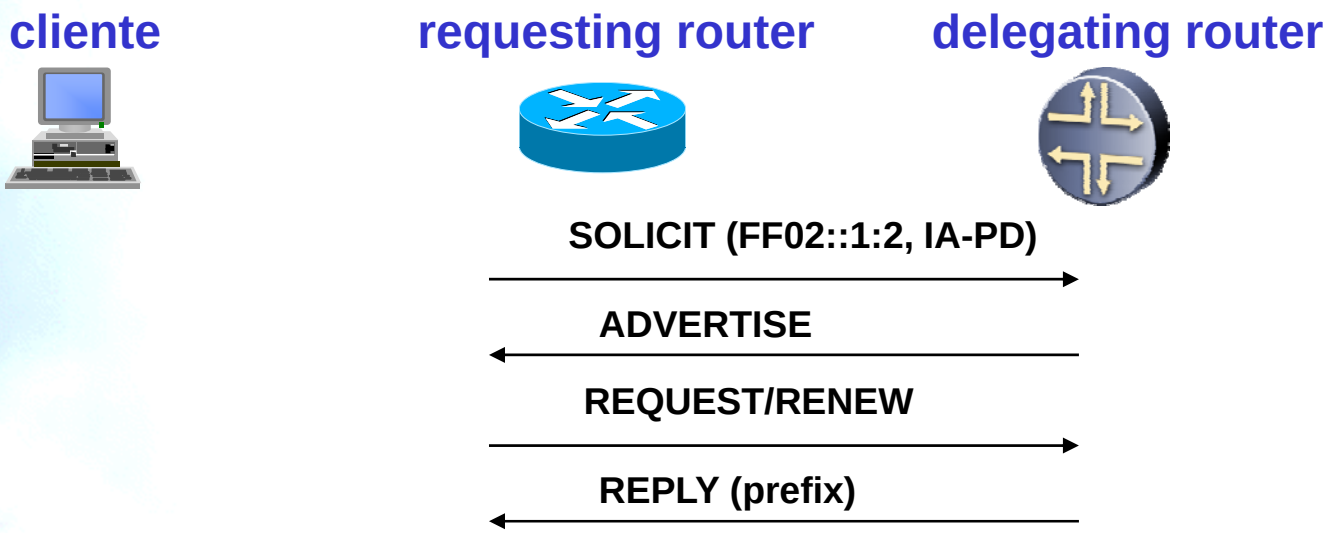
Detalles de DHCPv6-PD

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

Arquitectura de Red para DHCPv6-PD



Ejemplo Básico de DHCPv6-PD



Preguntas?

Gracias!

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

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

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