Redes de Datos 2

Protocolo IPv6

Protocolo IPv6

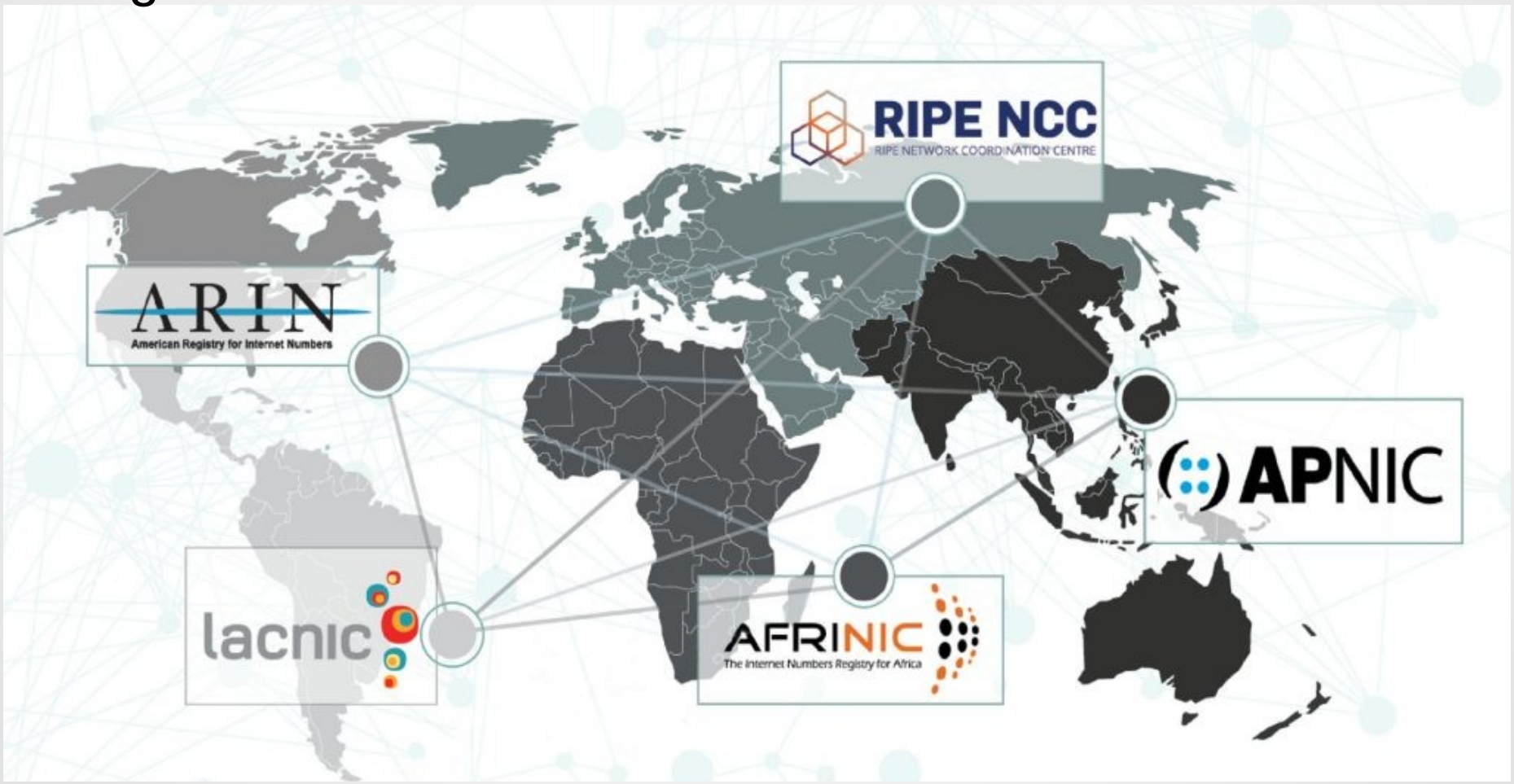
- Por qué IPv6?
- Formato encabezado IPv6
- ICMPv6
- Direccionamiento IPv6
- Neighbor Discovery
- Auto configuración
- DHCP para IPv6
- Impacto del cambio IPv4 – IPv6 en capas superiores
- Transición IPv4 - IPv6

Escasez de direcciones IPv4

- Crecimiento del uso de Internet
- Expansión a nivel comercial
- Aumento de equipos móviles
- Internet de las cosas (IoT)
- Uso ineficiente de direcciones IPv4
- Crecimiento de las tablas de rutas por asignación de rangos pequeños y multihoming
- Paliativos: CIDR (Classless Inter Domain Routing) y NAT (Network/Port Address Translation)
- Solución: Nuevo protocolo IPv6

Regional Internet Registries - RIRs

- Organización de los recursos de Internet

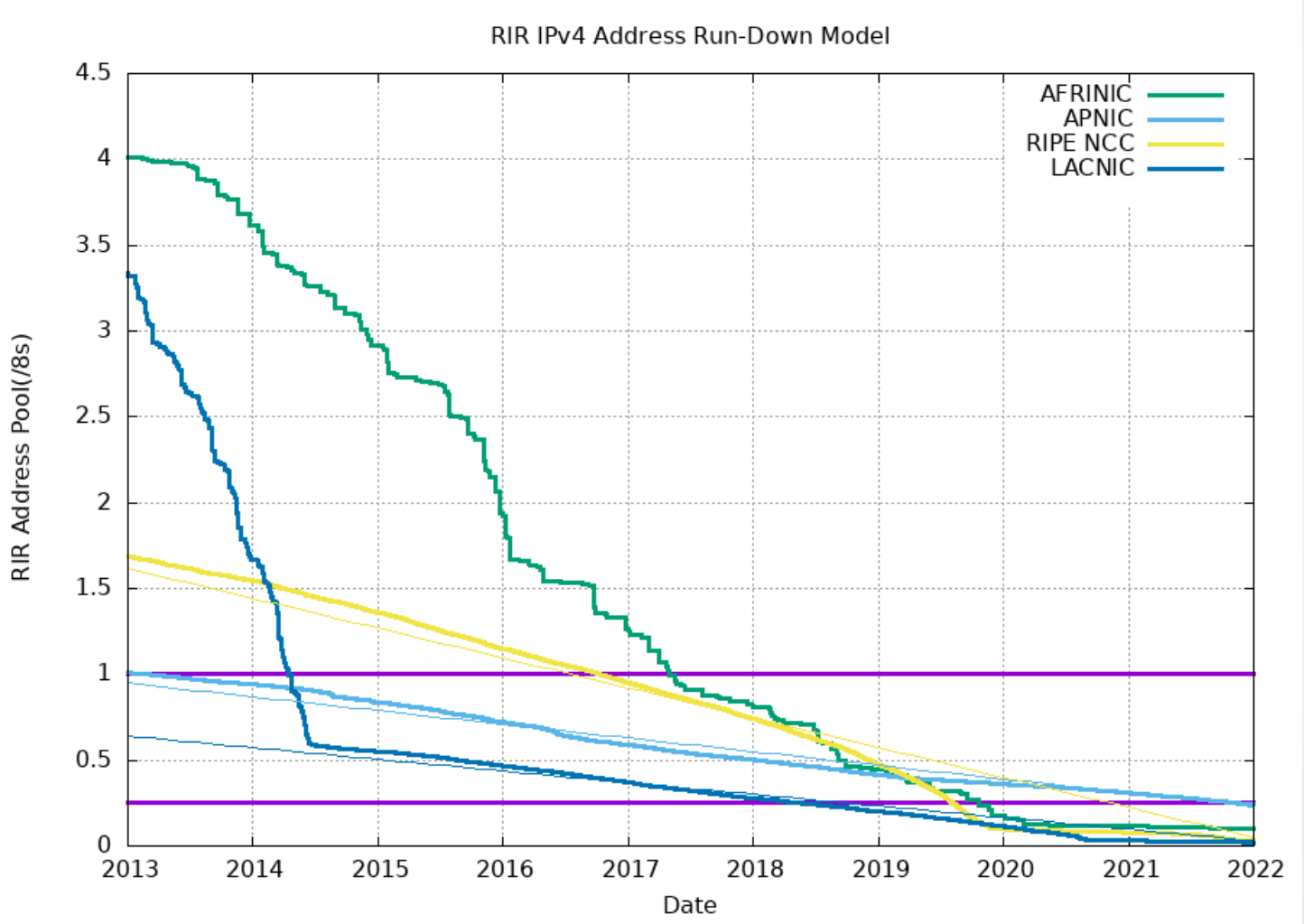


Agotamiento de direcciones IPv4

- El espacio de bloques no asignados por IANA se agotó el 03-Feb-2011
- Proyecciones de agotamiento de cada RIR (fuente IPv4 Address Report, https://www.potaroo.net/tools/ipv4/, Febrero 2024)

RIRz	Fecha prevista de agotamiento	Rangos /8 remanentes
APNIC	19-Apr-2011 (real)	0.1389
RIPE NCC	14-Sep-2012 (real)	0.0002
LACNIC	10-Jun-2014 (real)	0.0001
ARIN	24 Sep-2015 (real)	0.0005
AFRINIC	31-Dec-2021	0.0694

Proyección de consumo de remanentes



Necesidad de adoptar IPv6

- La cantidad de usuarios de Internet sigue creciendo
- La cantidad de dispositivos que se conectan a internet sigue creciendo
- Si no se adopta el protocolo IPv6, se obstaculizaría:
  - El crecimiento de la red
  - La inclusión digital
  - La posibilidad de ofrecer nuevos servicios
- El costo de no adoptar IPv6 podría ser superior al de adoptarlo

Ventajas de IPv6

- Aumento del espacio de direcciones pasando de 32 a 128-bits (16 bytes) evitando la necesidad de NAT
- Nuevo formato de paquete para hacer más eficiente el forwarding
- Facilidades para la auto configuración de los equipos
- Seguridad integrada permitiendo usar IPSec de origen a destino (la diferencia con IPv4 es que es mandatorio implementarlo)
- Infraestructura de direccionamiento y ruteo más eficiente y jerárquica con múltiples niveles de ISPs (esto último no se ha materializado)
- Mejor soporte para priorizar tráfico usando los campos Flow Label y Traffic Class
- Soporte para evolución y nuevas prestaciones mediante encabezados de extensión

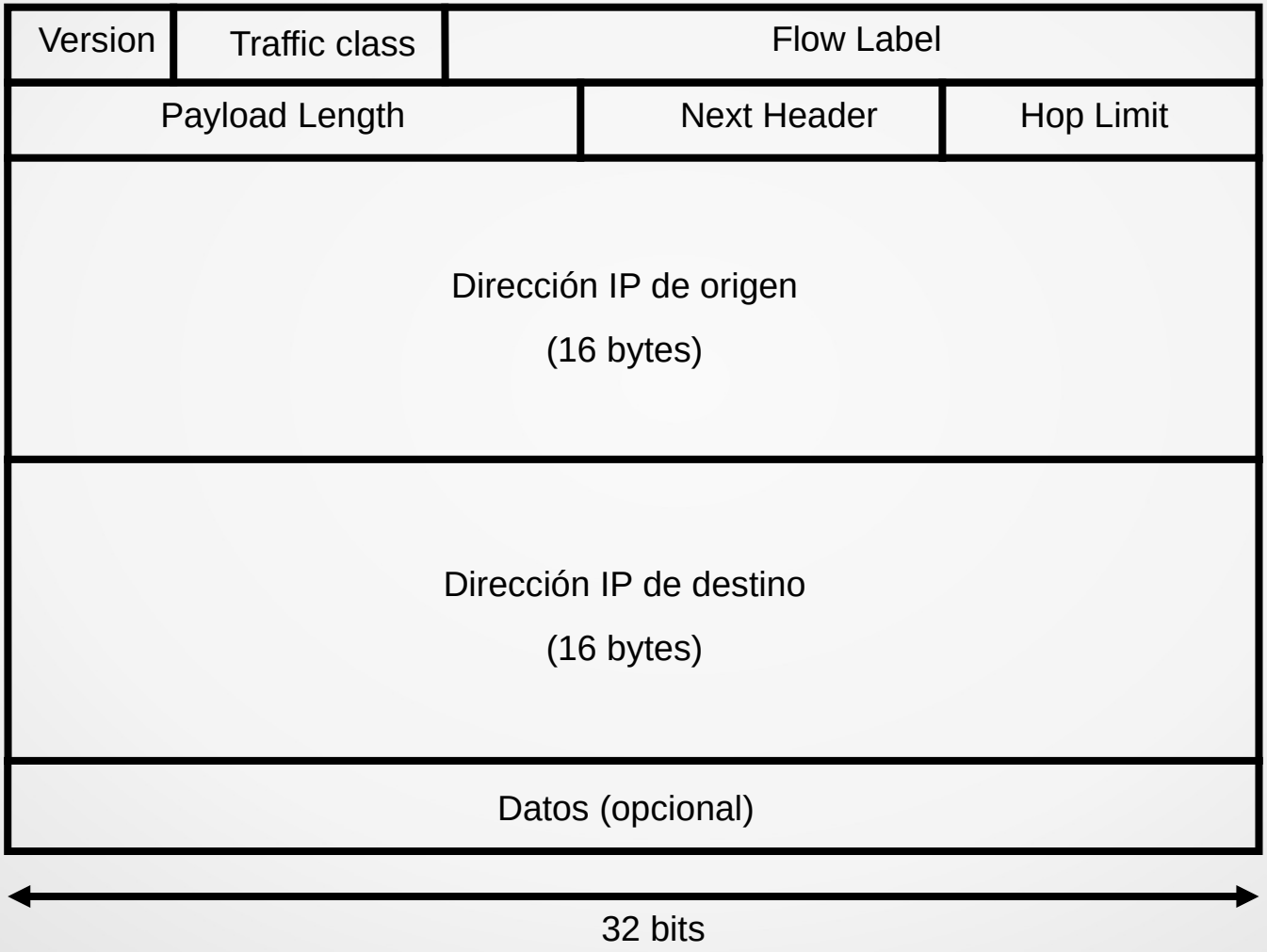
Protocolo IPv6

- Por qué IPv6?
- Formato encabezado IPv6
- ICMPv6
- Direccionamiento IPv6
- Neighbor Discovery
- Auto configuración
- DHCP para IPv6
- Impacto del cambio IPv4 – IPv6 en capas superiores
- Transición IPv4 - IPv6

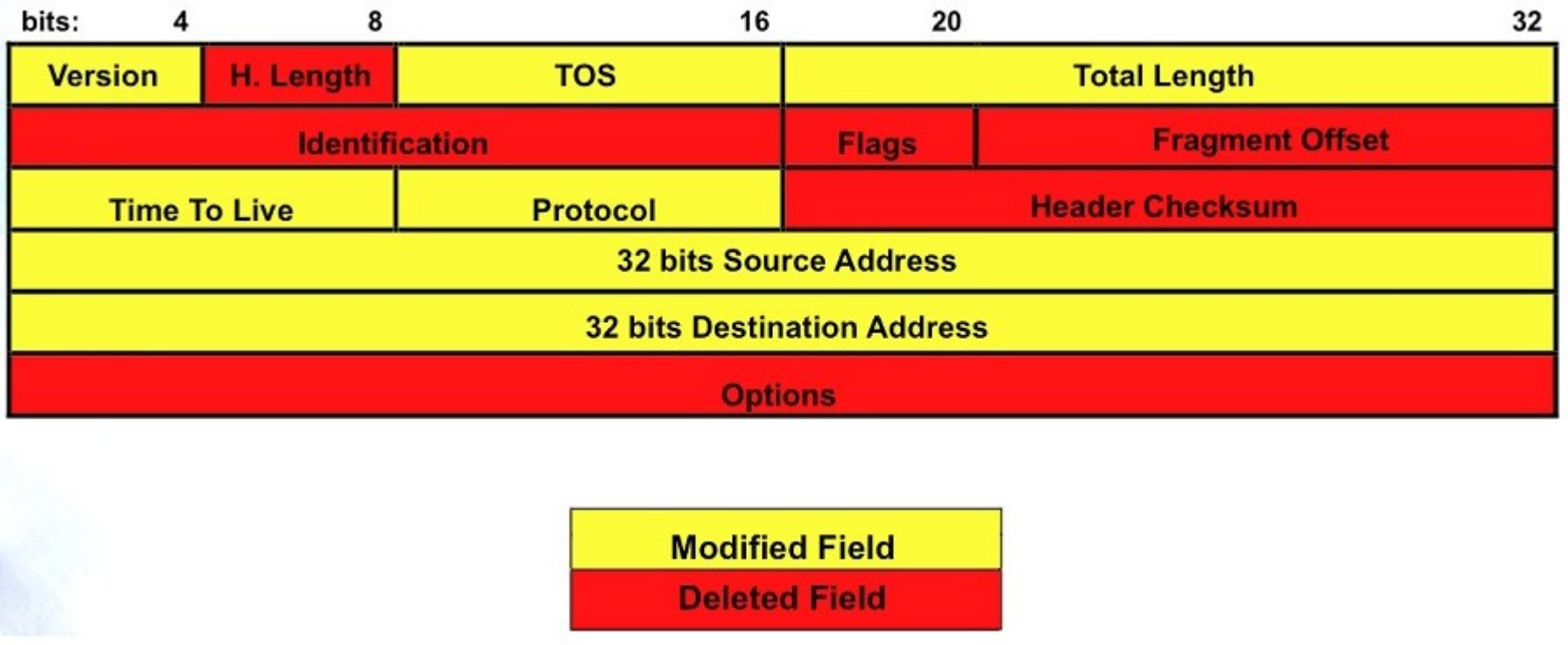
Principales RFCs sobre IPv6

- Protocolo básico definido en 1998 (RFC 2460, obsoleta). En julio de 2017 se aprobó RFC 8200 como STD 86: “Internet Protocol, Version 6 (IPv6) Specification”
- Requerimientos para los nodos (RFC 8504)
- Arquitectura de las direcciones (RFC 4291) y posteriores revisiones
- DHCPv6 (RFC 8415)
- Mobile IPv6 (RFC 6275)
- Especificación de etiquetas de flujo (RFC 6437)
- API básica de sockets (RFC 3493)

Datagrama IPv6 (RFC 8200)



Comparación encabezados IPv4 - IPv6



Comparación encabezados IPv4 - IPv6

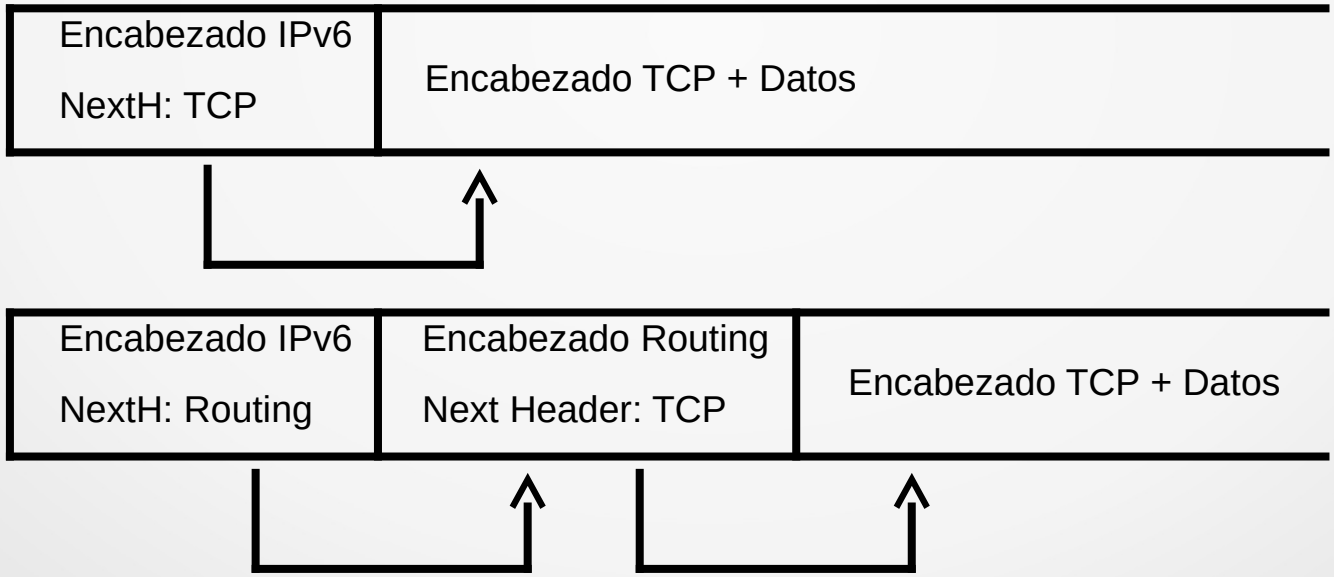
- Aumento de capacidad de direccionamiento.
  Las direcciones pasan de 32 bits a 128 bits => 7×10^{23} direcciones por m^2 de planeta!
- Tamaño fijo de encabezado (40 bytes)
- Eliminación del checksum
- No se permite fragmentación en equipos intermedios
- Revisión de parámetros: largo (de carga útil), protocolo (next header), TTL (hop limit), versión
- Nuevos campos: flow label, traffic class (tipo de servicio)
- Opciones se manejan con encabezados de extensión (extension headers)

Flow label / Traffic class

- Flow Label
  - Permite que el origen marque secuencias de paquetes que deberían ser tratados como un único flujo
  - La RFC 6437 especifica los requerimientos de este campo
  - Permite usar la 3-tupla (Flow Label, IP origen, IP destino) para clasificación de flujos y balanceo de carga
- Traffic Class
  - Permite clasificar el tráfico para diferenciar servicios
  - Traffic Class field for Differentiated Services and Explicit Congestion Notification RFC 2474 y RFC 3168

Encabezados de extensión

- Sustituyen a las opciones del encabezado en IPv4
- Los encabezados de extensión se encadenan usando el campo Next Header del encabezado anterior

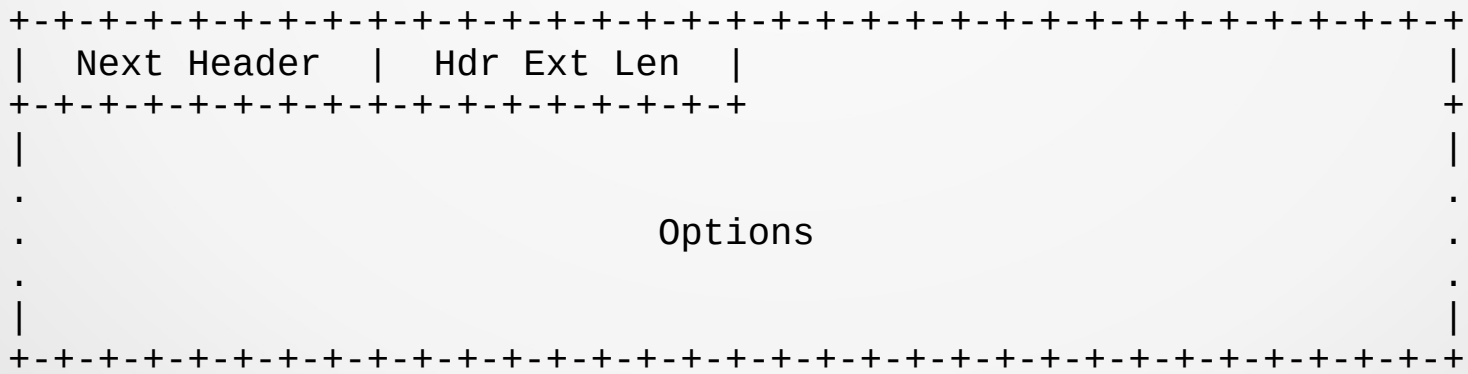


Encabezados de extensión

- Hay definidos 6 tipos de encabezados de extensión:
  - hop-by-hop options (información entre routers)
  - fragment (fragmentación en origen)
  - destination options (opciones para el destino)
  - routing (equivalente a source routing)
  - authentication (firma de originador)
  - encapsulating security payload (paquete encriptado)

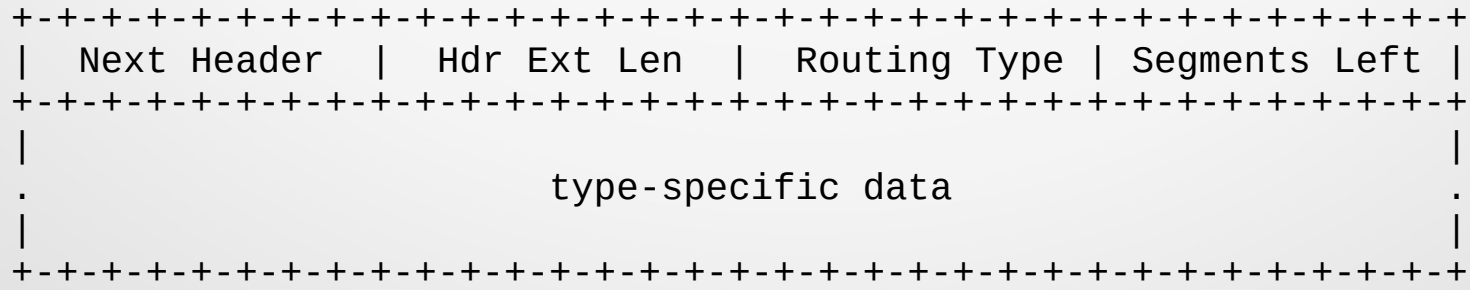
Encabezados de extensión

- Encabezado Hop-by-hop
- Next-Header = 0 (en encabezado anterior)
- Lleva información que debe ser procesada por todos los nodos intermedios => slow path!



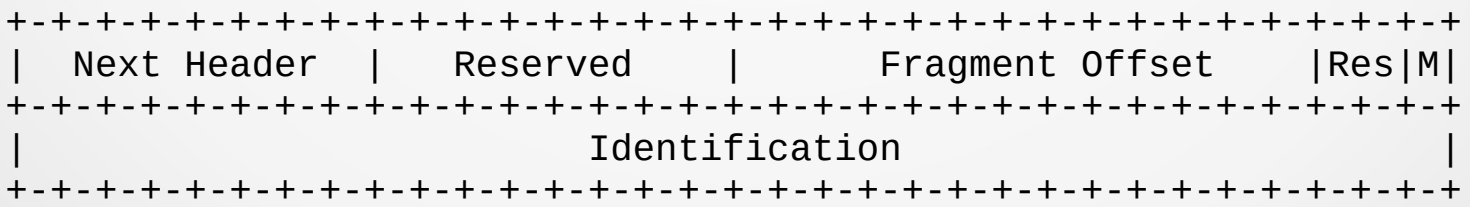
Encabezados de extensión

- Encabezado de Routing
- Next-Header = 43 (en encabezado anterior)
- Inicialmente creado para especificar a través de qué nodos debía pasar el paquete (source routing).
  Routing Type = 0 (Obsoleto por RFC 5095)
- Actualmente utilizado como parte de los mecanismos de movilidad en IPv6 para indicar la “Home Address”.
  Routing Type = 2 (RFC 6275)



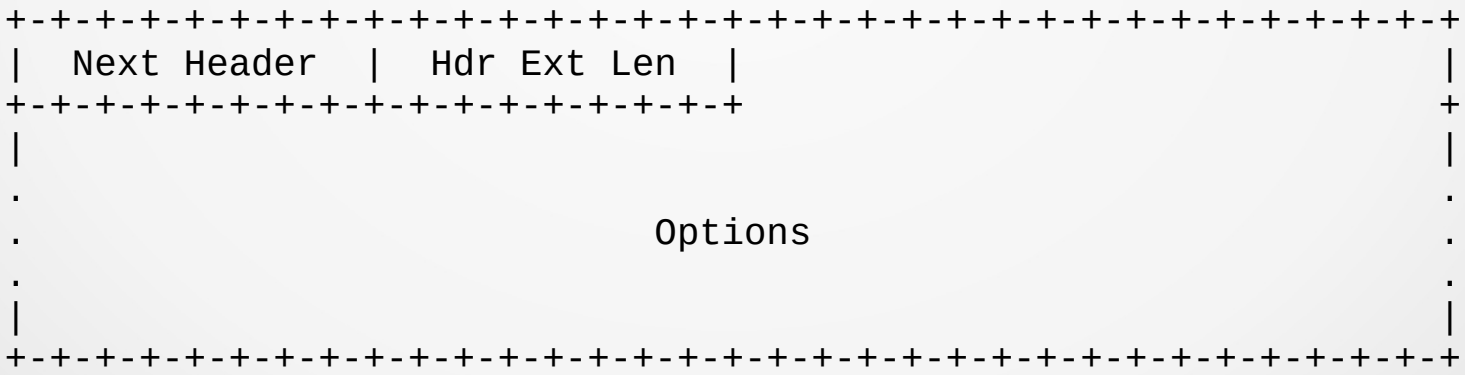
Encabezados de extensión

- Encabezado de Fragmentación
- Next-Header = 44 (en encabezado anterior)
- Utilizado para enviar paquetes de tamaños mayores al “path MTU” hasta el destinatario
- Veremos más adelante la determinación del path MTU con protocolo “Path MTU discovery”



Encabezados de extensión

- Encabezado de opciones de destino
- Next-Header = 60 (en encabezado anterior)
- Lleva información que debe ser procesada en el destino del paquete



Encabezados de extensión

- Para evitar el procesamiento innecesario, se establece un orden de anidado para que los nodos intermedios puedan analizar hasta cierto nivel:

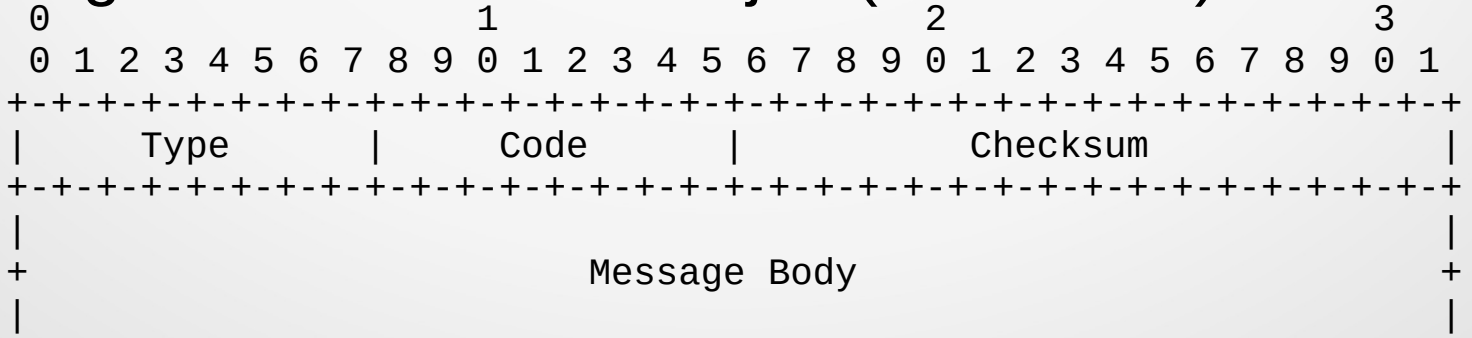
1. Encabezado IPv6
2. Encabezado hop-by-hop
3. Encabezado opciones de destino (en caso de túneles)
4. Encabezado de routing
5. Encabezado de fragmentación
6. Encabezado de autenticación/encripción
   - Autenticación [RFC4302] – Encripción [RFC4303]
7. Encabezado de opciones de destino
8. Encabezado de capas superiores

Protocolo IPv6

- Por qué IPv6?
- Formato encabezado IPv6
- ICMPv6
- Direccionamiento IPv6
- Neighbor Discovery
- Auto configuración
- DHCP para IPv6
- Impacto del cambio IPv4 – IPv6 en capas superiores
- Transición IPv4 - IPv6

Evolución de ICMP

- El protocolo ICMPv6 incluye:
  - Mensajes ICMP existentes en IPv4
  - Soporte para multicast (IGMP en IPv4)
  - Soporte para auto configuración
  - Soporte para descubrimiento de vecinos (ARP en IPv4)
  - Soporte para movilidad
- Forma general de los mensajes (RFC 4443)



Mensajes ICMPv6 (type)

- 0 Reserved
- 1 Destination Unreachable
- 2 Packet Too Big
- 3 Time Exceeded
- 4 Parameter Problem
- ... Reservados, experimentales, no asignados
- 128 Echo Request
- 129 Echo Reply
- 130 Multicast Listener Query
- 131 Multicast Listener Report
- 132 Multicast Listener Done
- 133 Router Solicitation
- 134 Router Advertisement
- 135 Neighbor Solicitation
- 136 Neighbor Advertisement
- 137 Redirect Message
- 138 Router Renumbering
- 139 ICMP Node Information Query
- 140 ICMP Node Information Response
- 141 Inverse Neighbor Discovery Solicitation Message
- 142 Inverse Neighbor Discovery Advertisement Message
- 143 Version 2 Multicast Listener Report
- 144 Home Agent Address Discovery Request Message
- 145 Home Agent Address Discovery Reply Message
- 146 Mobile Prefix Solicitation
- 147 Mobile Prefix Advertisement
- 148 Certification Path Solicitation Message
- 149 Certification Path Advertisement Message
- 150 ICMP messages utilized by experimental mobility protocols
- 151 Multicast Router Advertisement
- 152 Multicast Router Solicitation
- 153 Multicast Router Termination
- 154 FMIPv6 Messages
- 155 RPL Control Message
- 156 ILNPv6 Locator Update Message
- 157 Duplicate Address Request
- 158 Duplicate Address Confirmation
- 159 MPL Control Message
- ... Reservados, experimentales, no asignados

Mensajes ICMPv6 (type)

- 0 Reserved
- 1 Destination Unreachable
- 2 Packet Too Big
- 3 Time Exceeded
- 4 Parameter Problem
- ... Reservados, experimentales, no asignados
- 128 Echo Request
- 129 Echo Reply
- 130 Multicast Listener Query
- 131 Multicast Listener Report
- 132 Multicast Listener Done
- 133 Router Solicitation
- 134 Router Advertisement
- 135 Neighbor Solicitation
- 136 Neighbor Advertisement
- 137 Redirect Message
- 138 Router Renumbering
- 139 ICMP Node Information Query
- 140 ICMP Node Information Response
- 141 Inverse Neighbor Discovery Solicitation Message
- 142 Inverse Neighbor Discovery Advertisement Message

Existentes en ICMPv4

- 143 Version 2 Multicast Listener Report
- 144 Home Agent Address Discovery Request Message
- 145 Home Agent Address Discovery Reply Message
- 146 Mobile Prefix Solicitation
- 147 Mobile Prefix Advertisement
- 148 Certification Path Solicitation Message
- 149 Certification Path Advertisement Message
- 150 ICMP messages utilized by experimental mobility protocols
- 151 Multicast Router Advertisement
- 152 Multicast Router Solicitation
- 153 Multicast Router Termination
- 154 FMIPv6 Messages
- 155 RPL Control Message
- 156 ILNPv6 Locator Update Message
- 157 Duplicate Address Request
- 158 Duplicate Address Confirmation
- 159 MPL Control Message
- ... Reservados, experimentales, no asignados

Mensajes ICMPv6

- 0 Reserved
- 1 Destination Unreachable
- 2 Packet Too Big
- 3 Time Exceeded
- 4 Parameter Problem
- ... Reservados, experimentales, no asignados
- 128 Echo Request
- 129 Echo Reply
- 130 Multicast Listener Query
- 131 Multicast Listener Report
- 132 Multicast Listener Done
- 133 Router Solicitation
- 134 Router Advertisement
- 135 Neighbor Solicitation
- 136 Neighbor Advertisement
- 137 Redirect Message
- 138 Router Renumbering
- 139 ICMP Node Information Query
- 140 ICMP Node Information Response
- 141 Inverse Neighbor Discovery Solicitation Message
- 142 Inverse Neighbor Discovery Advertisement Message

Multicast reemplazan a IGMP y agregan funcionalidades

- 143 Version 2 Multicast Listener Report
- 144 Home Agent Address Discovery Request Message
- 145 Home Agent Address Discovery Reply Message
- 146 Mobile Prefix Solicitation
- 147 Mobile Prefix Advertisement
- 148 Certification Path Solicitation Message
- 149 Certification Path Advertisement Message
- 150 ICMP messages utilized by experimental mobility protocols
- 151 Multicast Router Advertisement
- 152 Multicast Router Solicitation
- 153 Multicast Router Termination
- 154 FMIPv6 Messages
- 155 RPL Control Message
- 156 ILNPv6 Locator Update Message
- 157 Duplicate Address Request
- 158 Duplicate Address Confirmation
- 159 MPL Control Message
- ... Reservados, experimentales, no asignados

Mensajes ICMPv6

Neighbor Discovery reemplazan a ARP y agregan funcionalidad para auto configuración

- 0 Reserved
- 1 Destination Unreachable
- 2 Packet Too Big
- 3 Time Exceeded
- 4 Parameter Problem
- ... Reservados, experimentales, no asignados
- 128 Echo Request
- 129 Echo Reply
- 130 Multicast Listener Query
- 131 Multicast Listener Report
- 132 Multicast Listener Done
- 133 Router Solicitation
- 134 Router Advertisement
- 135 Neighbor Solicitation
- 136 Neighbor Advertisement
- 137 Redirect Message
- 138 Router Renumbering
- 139 ICMP Node Information Query
- 140 ICMP Node Information Response
- 141 Inverse Neighbor Discovery Solicitation Message
- 142 Inverse Neighbor Discovery Advertisement Message
- 143 Version 2 Multicast Listener Report
- 144 Home Agent Address Discovery Request Message
- 145 Home Agent Address Discovery Reply Message
- 146 Mobile Prefix Solicitation
- 147 Mobile Prefix Advertisement
- 148 Certification Path Solicitation Message
- 149 Certification Path Advertisement Message
- 150 ICMP messages utilized by experimental mobility protocols
- 151 Multicast Router Advertisement
- 152 Multicast Router Solicitation
- 153 Multicast Router Termination
- 154 FMIPv6 Messages
- 155 RPL Control Message
- 156 ILNPv6 Locator Update Message
- 157 Duplicate Address Request
- 158 Duplicate Address Confirmation
- 159 MPL Control Message
- ... Reservados, experimentales, no asignados

Mensajes ICMPv6

- 0 Reserved
- 1 Destination Unreachable
- 2 Packet Too Big
- 3 Time Exceeded
- 4 Parameter Problem
- ... Reservados, experimentales, no asignados
- 128 Echo Request
- 129 Echo Reply
- 130 Multicast Listener Query
- 131 Multicast Listener Report
- 132 Multicast Listener Done
- 133 Router Solicitation
- 134 Router Advertisement
- 135 Neighbor Solicitation
- 136 Neighbor Advertisement
- 137 Redirect Message
- 138 Router Renumbering
- 139 ICMP Node Information Query
- 140 ICMP Node Information Response
- 141 Inverse Neighbor Discovery Solicitation Message
- 142 Inverse Neighbor Discovery Advertisement Message

Movilidad

- 143 Version 2 Multicast Listener Report
- 144 Home Agent Address Discovery Request Message
- 145 Home Agent Address Discovery Reply Message
- 146 Mobile Prefix Solicitation
- 147 Mobile Prefix Advertisement
- 148 Certification Path Solicitation Message
- 149 Certification Path Advertisement Message
- 150 ICMP messages utilized by experimental mobility protocols
- 151 Multicast Router Advertisement
- 152 Multicast Router Solicitation
- 153 Multicast Router Termination
- 154 FMIPv6 Messages
- 155 RPL Control Message
- 156 ILNPv6 Locator Update Message
- 157 Duplicate Address Request
- 158 Duplicate Address Confirmation
- 159 MPL Control Message
- ... Reservados, experimentales, no asignados

Path MTU discovery

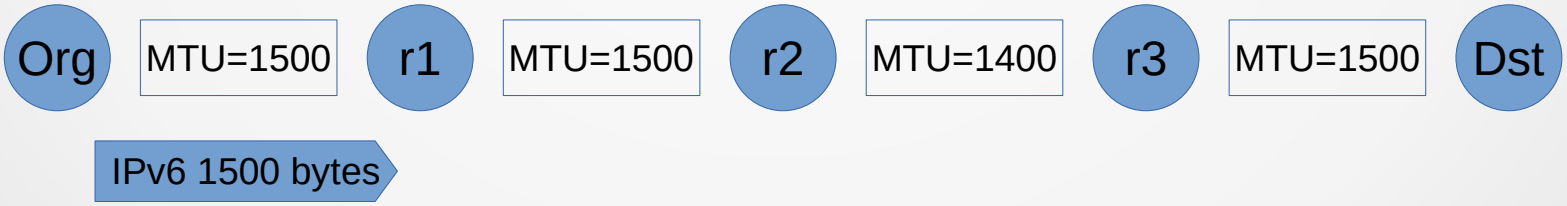
- MTU = Maximum Transmission Unit
  - Link MTU = máximo tamaño en bytes del paquete IP
  - Path MTU = menor link MTU de un origen a un destino
- En IPv6 el link MTU mínimo es de 1280 bytes (en IPv4 son 68 bytes)
- La MTU es importante en IPv6 porque:
  - No se permite la fragmentación en tránsito (solo en origen mediante encabezados de extensión)
  - Es frecuente el encapsulado (túneles) lo que reduce la MTU disponible

Path MTU discovery

- Es un mecanismo para descubrir el Path MTU entre un origen y un destino
- Se comienza enviando con la MTU del primer link y si en el camino hay algún link con MTU menor, se recibirá un mensaje ICMPv6 indicando cuál es el valor de la MTU
- El originador bajará la MTU a ese valor

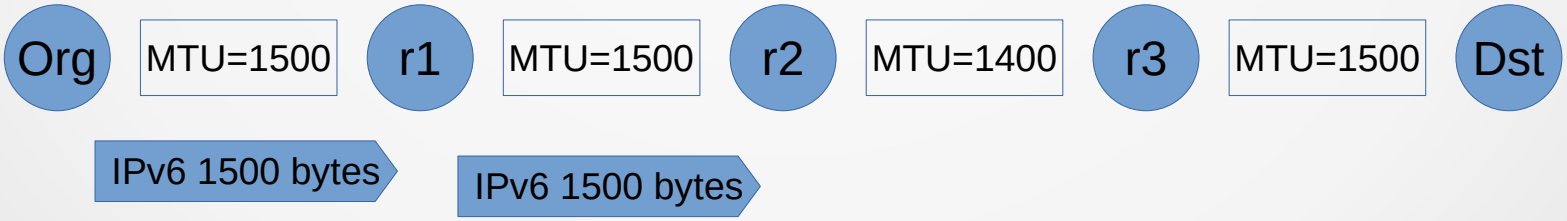
Path MTU discovery

- Es un mecanismo para descubrir el Path MTU entre un origen y un destino
- Se comienza enviando con la MTU del primer link y si en el camino hay algún link con MTU menor, se recibirá un mensaje ICMPv6 indicando cuál es el valor de la MTU
- El originador bajará la MTU a ese valor



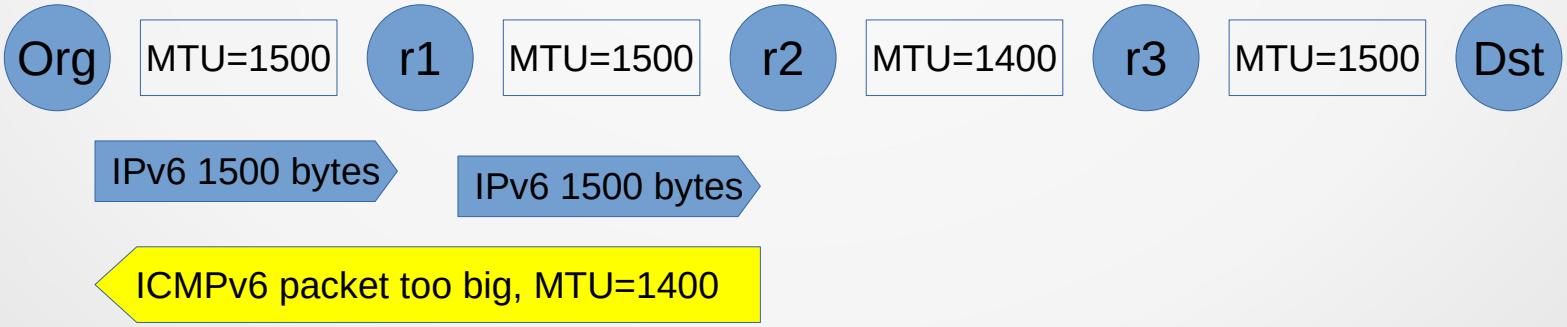
Path MTU discovery

- Es un mecanismo para descubrir el Path MTU entre un origen y un destino
- Se comienza enviando con la MTU del primer link y si en el camino hay algún link con MTU menor, se recibirá un mensaje ICMPv6 indicando cuál es el valor de la MTU
- El originador bajará la MTU a ese valor



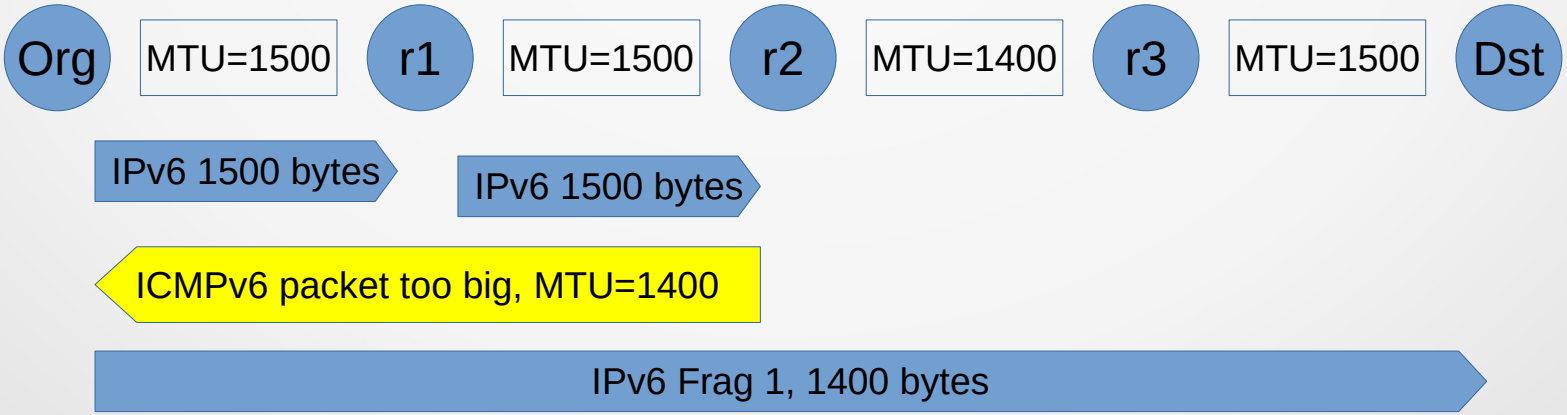
Path MTU discovery

- Es un mecanismo para descubrir el Path MTU entre un origen y un destino
- Se comienza enviando con la MTU del primer link y si en el camino hay algún link con MTU menor, se recibirá un mensaje ICMPv6 indicando cuál es el valor de la MTU
- El originador bajará la MTU a ese valor



Path MTU discovery

- Es un mecanismo para descubrir el Path MTU entre un origen y un destino
- Se comienza enviando con la MTU del primer link y si en el camino hay algún link con MTU menor, se recibirá un mensaje ICMPv6 indicando cuál es el valor de la MTU
- El originador bajará la MTU a ese valor



Protocolo IPv6

- Por qué IPv6?
- Formato encabezado IPv6
- ICMPv6
- Direccionamiento IPv6
- Neighbor Discovery
- Auto configuración
- DHCP para IPv6
- Impacto del cambio IPv4 – IPv6 en capas superiores
- Transición IPv4 - IPv6

Direccionamiento IPv6

- Notación de direcciones IPv6
- Prefijos IPv6
- Tipos de direcciones IPv6
- Identificadores de interfaz (IID)
- Tiempo de vida de las direcciones IPv6

Notación de direcciones

- Formas de representar las direcciones IPv6 (RFC 5952)
  - Ocho enteros de 16 bits en hexadecimal separados por “:”
    - Ej: abcd:0000:0000:0000:9abc:0700:c035:0453
  - Ceros a la izquierda de cada palabra de 16 bits se suprimen:
    - Ej: abcd:0:0:0:9abc:700:c035:453
  - Simplificación de cadenas de ceros:
    - Ej: abcd::9abc:700:c035:453
    - La dirección de loopback: 0:0:0:0:0:0:0:1 quedaría ::1
    - Un único 0000 debe reemplazarse por 0 y no por ::
    - El :: solo se puede usar una vez en la cadena más larga
  - Para entornos mixtos IPv4 e IPv6 se pueden representar los últimos 4 bytes en “dotted-decimal”.
    - Ej: abcd::9abc:700:192.53.4.83

Notación de direcciones

- Formas de representar las direcciones IPv6 (RFC 5952)
  - Ocho enteros de 16 bits en hexadecimal separados por “:”
    - Ej: abcd:0000:0000:0000:9abc:0700:c035:0453
  - Ceros a la izquierda de cada palabra de 16 bits se suprimen:
    - Ej: abcd:0:0:0:9abc:700:c035:453
  - Simplificación de cadenas de ceros:
    - Ej: abcd::9abc:700:c035:453
    - La dirección de loopback: 0:0:0:0:0:0:0:1 quedaría ::1
    - Un único 0000 debe reemplazarse por 0 y no por ::
    - El :: solo se puede usar una vez en la cadena más larga
  - Para entornos mixtos IPv4 e IPv6 se pueden representar los últimos 4 bytes en “dotted-decimal”.
    - Ej: abcd::9abc:700:192.53.4.83

Notación de direcciones

- Formas de representar las direcciones IPv6 (RFC 5952)
  - Ocho enteros de 16 bits en hexadecimal separados por “:”
    - Ej: abcd:0000:0000:0000:9abc:0700:c035:0453
  - Ceros a la izquierda de cada palabra de 16 bits se suprimen:
    - Ej: abcd:0:0:0:9abc:700:c035:453
  - Simplificación de cadenas de ceros:
    - Ej: abcd::9abc:700:c035:453
    - La dirección de loopback: 0:0:0:0:0:0:0:1 quedaría ::1
    - Un único 0000 debe reemplazarse por 0 y no por ::
    - El :: solo se puede usar una vez en la cadena más larga
  - Para entornos mixtos IPv4 e IPv6 se pueden representar los últimos 4 bytes en “dotted-decimal”.
    - Ej: abcd::9abc:700:192.53.4.83

Notación de direcciones

- Formas de representar las direcciones IPv6 (RFC 5952)
  - Ocho enteros de 16 bits en hexadecimal separados por “:”
    - Ej: abcd:0000:0000:0000:9abc:0700:c035:0453
  - Ceros a la izquierda de cada palabra de 16 bits se suprimen:
    - Ej: abcd:0:0:0:9abc:700:c035:453
  - Simplificación de cadenas de ceros:
    - Ej: abcd::9abc:700:c035:453
    - La dirección de loopback: 0:0:0:0:0:0:0:1 quedaría ::1
    - Un único 0000 debe reemplazarse por 0 y no por ::
    - El :: solo se puede usar una vez en la cadena más larga
  - Para entornos mixtos IPv4 e IPv6 se pueden representar los últimos 4 bytes en “dotted-decimal”.
    - Ej: abcd::9abc:700:192.53.4.83

Notación de direcciones

- Formas de representar las direcciones IPv6 (RFC 5952)
  - Ocho enteros de 16 bits en hexadecimal separados por “:”
    - Ej: abcd:0000:0000:0000:9abc:0700:c035:0453
  - Ceros a la izquierda de cada palabra de 16 bits se suprimen:
    - Ej: abcd:0:0:0:9abc:700:c035:453
  - Simplificación de cadenas de ceros:
    - Ej: abcd::9abc:700:c035:453
    - La dirección de loopback: 0:0:0:0:0:0:0:1 quedaría ::1
    - Un único 0000 debe reemplazarse por 0 y no por ::
    - El :: solo se puede usar una vez en la cadena más larga
  - Para entornos mixtos IPv4 e IPv6 se pueden representar los últimos 4 bytes en “dotted-decimal”.
    - Ej: abcd::9abc:700:192.53.4.83

Notación de direcciones

- Formas de representar las direcciones IPv6 (RFC 5952)
  - Ocho enteros de 16 bits en hexadecimal separados por “:”
    - Ej: abcd:0000:0000:0000:9abc:0700:c035:0453
  - Ceros a la izquierda de cada palabra de 16 bits se suprimen:
    - Ej: abcd:0:0:0:9abc:700:c035:453
  - Simplificación de cadenas de ceros:
    - Ej: abcd::9abc:700:c035:453
    - La dirección de loopback: 0:0:0:0:0:0:0:1 quedaría ::1
    - Un único 0000 debe reemplazarse por 0 y no por ::
    - El :: solo se puede usar una vez en la cadena más larga
  - Para entornos mixtos IPv4 e IPv6 se pueden representar los últimos 4 bytes en “dotted-decimal”.
    - Ej: abcd::9abc:700:192.53.4.83

Notación de direcciones

- Formas de representar las direcciones IPv6 (RFC 5952)
  - Ocho enteros de 16 bits en hexadecimal separados por “:”
    - Ej: abcd:0000:0000:0000:9abc:0700:c035:0453
  - Ceros a la izquierda de cada palabra de 16 bits se suprimen:
    - Ej: abcd:0:0:0:9abc:700:c035:453
  - Simplificación de cadenas de ceros:
    - Ej: abcd::9abc:700:c035:453
    - La dirección de loopback: 0:0:0:0:0:0:0:1 quedaría ::1
    - Un único 0000 debe reemplazarse por 0 y no por ::
    - El :: solo se puede usar una vez en la cadena más larga
  - Para entornos mixtos IPv4 e IPv6 se pueden representar los últimos 4 bytes en “dotted-decimal”.
    - Ej: abcd::9abc:700:192.53.4.83

Prefijos IPv6

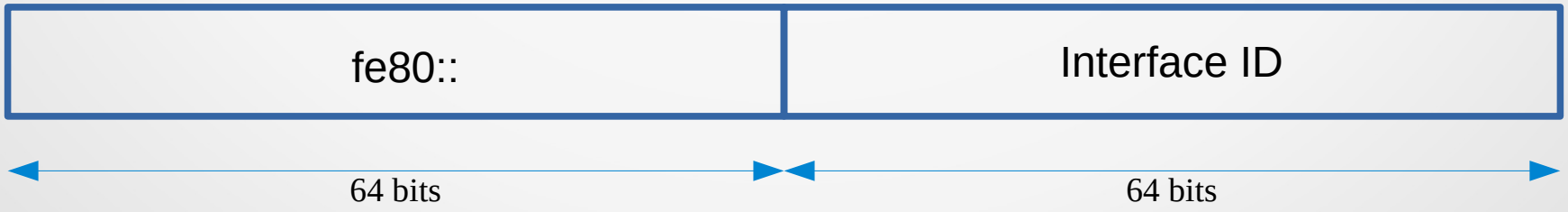
- Se usa la notación CIDR: prefijo/largo de la máscara
- Ejemplos:
  - abcd:ab8::**/32** => abcd:0ab8:0000:0000:0000:0000:0000:0000
  - abcd:ab8:1200::**/40** => abcd:0ab8:1200:0000:0000:0000:0000:0000
  - abcd:ab8:1200::**/48** => abcd:0ab8:1200:0000:0000:0000:0000:0000
- Subnetting con bits a la derecha del prefijo
  - Primeros dos prefijos /36 a partir del /32
  - abcd:ab8:**0**000:0000:0000:0000:0000:0000/36 =>abcd:0ab8:**0**::/36
  - abcd:ab8:**1**000:0000:0000:0000:0000:0000/36 =>abcd:0ab8:**1000**::/36

Tipos de direcciones IPv6

- Unicast (uno a uno, asignada a una interfaz)
  - Link Local: fe80::/10 (en un enlace, alcance local)
  - Unique Local (ULA): fc00::/7 (redes privadas)
  - IPv4-mapped: ::ffff:IPv4/128
  - Global (GUA, Global Unicast Address): 2000::/3 (direcciones globales)
  - Site Local e IPv4-compatible (obsoletas)
- Multicast (uno a varios, grupo de interfaces): ff00::/8
- Anycast (uno al más cercano, puede asociarse a varias interfaces de diferentes equipos) (parte del espacio unicast)
- Reservado
  - Documentación (2001:db8::/32) (RFC 3849)
  - Loopback (::1/128)
  - no especificado (::/128)

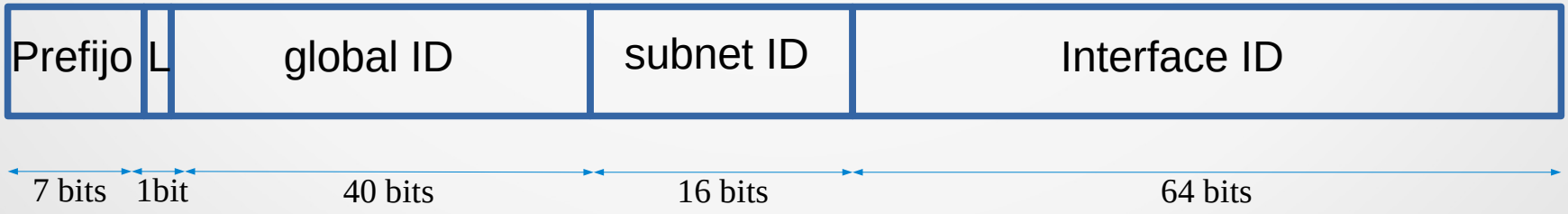
Direcciones Link Local

- Válidas solo en un enlace
- Se utiliza en la etapa de pre-configuración, como origen en los protocolos de ruteo o para pruebas
- Siempre presentes en una interfaz con IPv6 habilitado
- En la práctica se usa fe80::/64
- El Interface ID se genera localmente en el host a partir de la MAC o aleatoriamente



Direcciones Unique Local - ULA

- Prefijo fc00::/7
- L=1 prefijo asignado localmente
  - L=0 se reserva para uso futuro
- global ID: generado pseudo-aleatoriamente (único)
- RFC 4193 “Unique Local IPv6 Unicast Addresses”

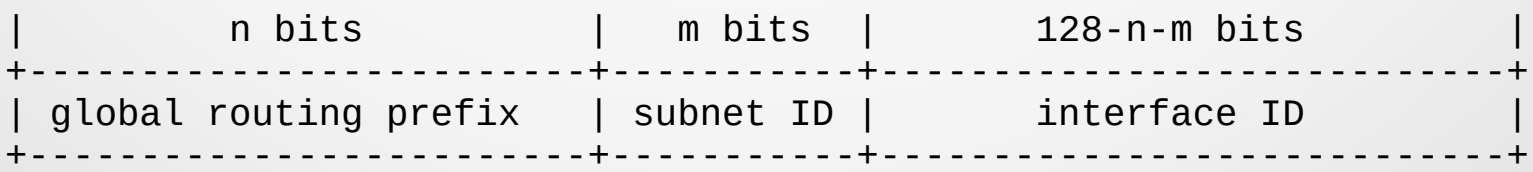


Direcciones IPv4 mapped

- Usadas para representar las direcciones de nodos IPv4 como nodos IPv6
- Se usa para aplicaciones en equipos dual-stack
- Se rellena con 80 ceros y dos bytes en FF
  - Ej: 192.168.1.1 queda como ::FFFF:192.168.1.1
- RFC 4038 “Application Aspects of IPv6 Transition”.

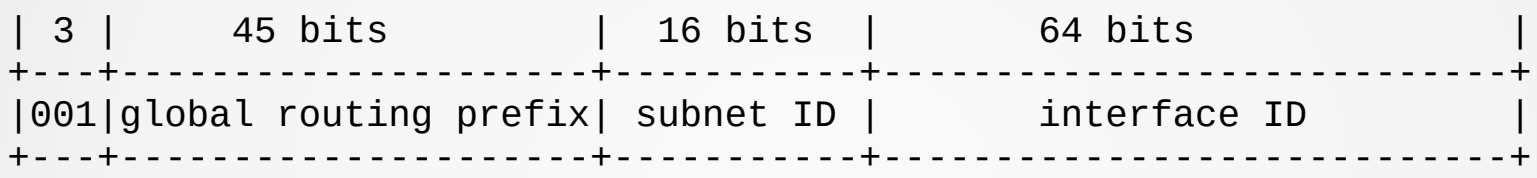
Direcciones Globales

- GUA – Global Unicast Address (RFC 3587)
- Global routing prefix es asignado a un sitio (cluster de subredes/links) por la IANA (Internet Assigned Numbers Authority) a través de los RIRs (Regional Internet Registries: AfrNIC, ARIN, APNIC, LACNIC & RIPE NCC)
  - Estructurado jerárquicamente por RIRs e ISPs
  - http://www.iana.org/assignments/ipv6-address-space
- El Subnet ID es usado por los administradores del sitio



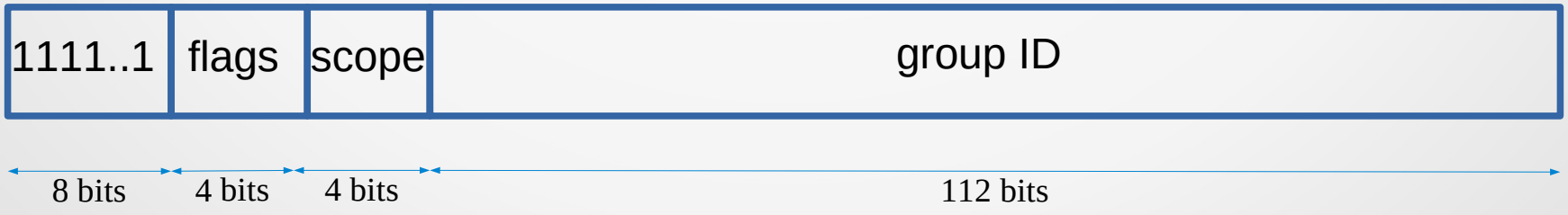
Direcciones Globales

- Ejemplo: con el prefijo 2000::/3 actualmente delegado por IANA una dirección global quedaría:



Direcciones Multicast

- Prefijo ff00::/8
- Flags: usadas para enrutamiento y servicios multicast
- Scope (ámbito de validez):
  - 1: interface-local, 2: link-local, 4: admin-local, 5: site-local, 8: organization-local, E: global
- group ID: grupo de multicast



Direcciones Multicast especiales

- No existe la dirección de broadcast, en su lugar se definen algunas direcciones multicast “bien conocidas”
  - FF01::1, FF02::1 => Todos los nodos (con diferentes ámbitos)
  - FF01::2, FF02::2, FF05::2 => Todos los enrutadores (con diferentes ámbitos)
- Cada nodo debe escuchar en una dirección multicast llamada Solicited Node (SN) que se crea a partir de la dirección unicast (o anycast) usadas por el nodo
  - Si la unicast termina en XY:ZTUV
  - La SN es: FF02::1:FFXY:ZTUV

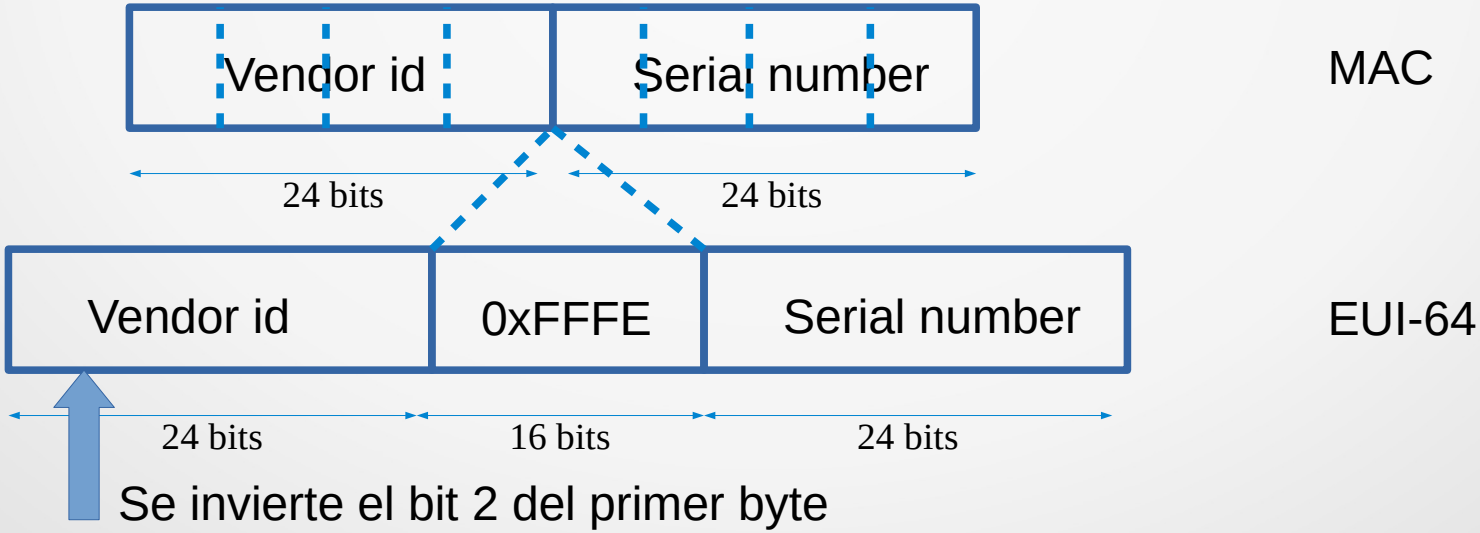
  Se usa en el DAD (Duplicate Address Detection) en el NDP (Neighbor Discovery Protocol)

Identificadores de interfaz (IID)

- Los identificadores de interfaz (Interface ID) son los 64 bits menos significativos de una dirección IPv6
- El prefijo en una LAN será /64 y esta es la unidad mínima en un plan de numeración IPv6
- Los IID se pueden generar de varias formas:
  - A partir de la dirección MAC, formato EUI-64 (RFC 4291)
  - Automáticamente mediante algún algoritmo (ej. aleatoriamente RFC 4941)
  - Manualmente
  - Asignado por DHCPv6 que genera la dirección completa
  - Recommendation on Stable IPv6 Interface Identifiers (RFC 8064)

Identificadores de interfaz EUI-64

- La IEEE define el mecanismo para crear un IID EUI-64 a partir de una dirección MAC Ethernet
- Además de agregar 0xFFFE entre el Vendor ID y el Serial Number, se invierte el bit 2 del primer byte.
  - Ese bit en una MAC es 0 si es global y 1 si es local



Tiempo de vida de las direcciones

- Las direcciones tienen una validez asignada (puede ser infinita)
- La validez está dada por dos temporizadores:
  - Preferred
  - Valid Lifetime (> que Preferred)
- En t <= Preferred, la dirección se puede usar sin problema
- En Preferred < t <= Valid la dirección está “deprecated”, se puede usar para comunicaciones existentes pero no para iniciar nuevas
- En t > Valid ya no se puede usar

Protocolo IPv6

- Por qué IPv6?
- Formato encabezado IPv6
- ICMPv6
- Direccionamiento IPv6
- Neighbor Discovery
- Auto configuración
- DHCP para IPv6
- Impacto del cambio IPv4 – IPv6 en capas superiores
- Transición IPv4 - IPv6

Neighbor Discovery Protocol - NDP

- NDP ofrece varios servicios en una LAN
  - Descubrimiento de routers, prefijos, parámetros de la red
  - Auto configuración
  - Address resolution, equivalente a ARP en IPv4
  - Duplicate address detection, DAD
  - Neighbor unreachability detection, NUD
- Este protocolo usa 5 mensajes ICMPv6
  - NS: Neighbor solicitation (host a host)
  - NA: Neighbor advertisement (host a host)
  - RS: Router solicitation (host a router)
  - RA: Router advertisement (router a host)

Neighbor Discovery Protocol - NDP

- Un host envía NS (Neighbor solicitation):
  - Para resolver la MAC de un neighbor (ARP en IPv4)
  - Para comprobar la alcanzabilidad de un destino unicast
- Un host envía un NA (Neighbor advertisement):
  - En respuesta a un NS
  - Para propagar una información de forma no solicitada
- Un host envia RS (Router solicitation):
  - Al levantar una interfaz
  - Destinado a la dirección multicast de todos los routers
- Un router envia RA (Router advertisement):
  - En respuesta a un RS
  - Periódicamente para informar los parámetros de la red

Multicast Listener Discovery - MLD

- Es equivalente a IGMP para IPv4
- Se utiliza en una LAN para que los routers descubran los equipos que escuchan en algún grupo multicast
- Hay dos versiones MLDv1 y MLDv2
- Los mensajes utilizados son:
  - Query: lo envía un router para que los host que escuchan multicast se reporten
  - Report: respuesta al Query indicando los grupos a escuchar
  - Done: cuando ya no se desea seguir escuchando en un grupo de multicast

Protocolo IPv6

- Por qué IPv6?
- Formato encabezado IPv6
- ICMPv6
- Direccionamiento IPv6
- Neighbor Discovery
- Auto configuración
- DHCP para IPv6
- Impacto del cambio IPv4 – IPv6 en capas superiores
- Transición IPv4 - IPv6

Auto configuración

- IPv6 permite una mínima intervención del administrador para que un equipo se comunique
- La auto configuración en IPv4 solo se podía hacer con DHCP, pero en IPv6 hay más opciones
- Escenario con router:
  - El router envía un RA usando las banderas M y O
    - M: gestión de direcciones, O: otros parámetros (DNS, etc)
  - Los hosts ven el RA y se autoconfiguran
- Escenario sin router:
  - Se puede usar DHCPv6 para configurar la IP y el DNS
- Siempre se puede hacer configuración manual (ej. para servidores)

Dos opciones de auto configuración

- Auto configuración Stateless (Stateless Address Auto configuration, SLAAC) (RFC 4862)
- Auto configuración Stateful o DHCPv6 (RFC 8415)

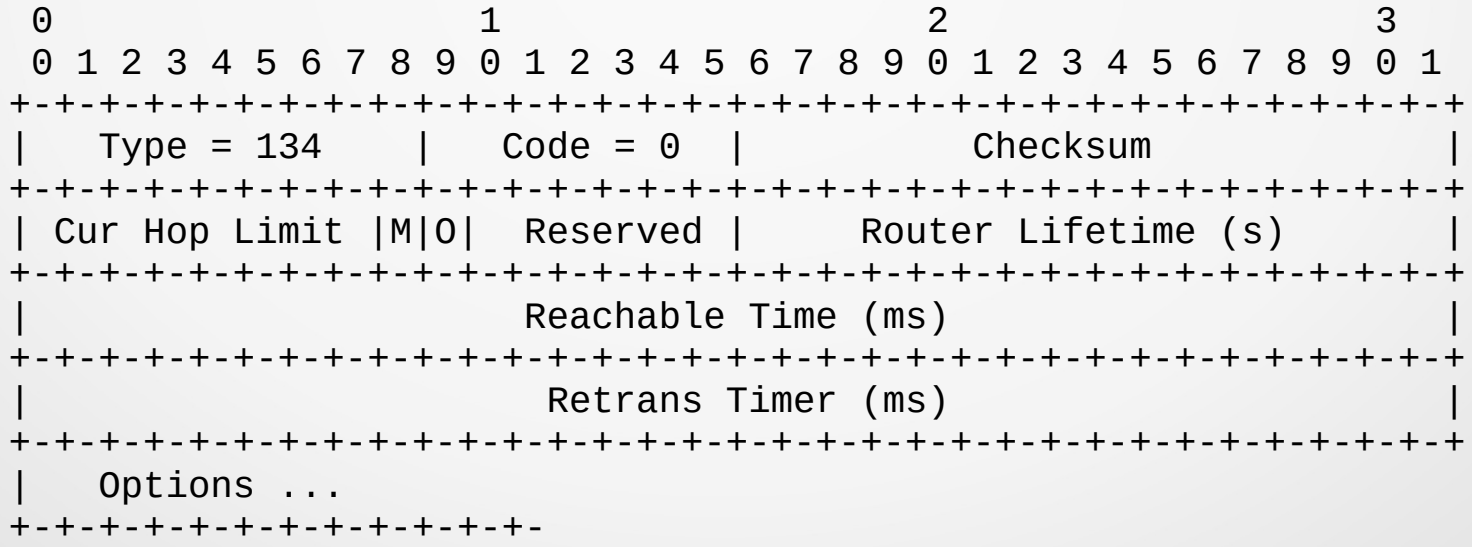
Dirección IP / Otros parámetros	Flag M	Flag O	Comentario
SLAAC / SLAAC	0	0	Si es dual-stack puede usar IPv4 para DNS
SLAAC / DHCPv6	0	1	DHCPv6 stateless (no necesita estado de leases)
DHCPv6 / SLAAC	1	0	Si es dual-stack puede usar IPv4 para DNS
DHCPv6 / DHCPv6	1	1	El router por defecto se aprende a partir del RA

Auto configuración stateless - SLAAC

- Se utiliza para configurar automáticamente los parámetros de la red
- El router envía un RA indicando a los hosts cómo configurarse
- Bandera M "Managed address configuration"
- Bandera O "Other configuration"
- M=0, O=0 => SLAAC para IP y otros parámetros
- M=0, O=1 => SLAAC para IP
- M=1, O=0 => SLAAC para otros parámetros (no se usa)
- La puerta de enlace o router por defecto se aprende también por RA o manualmente

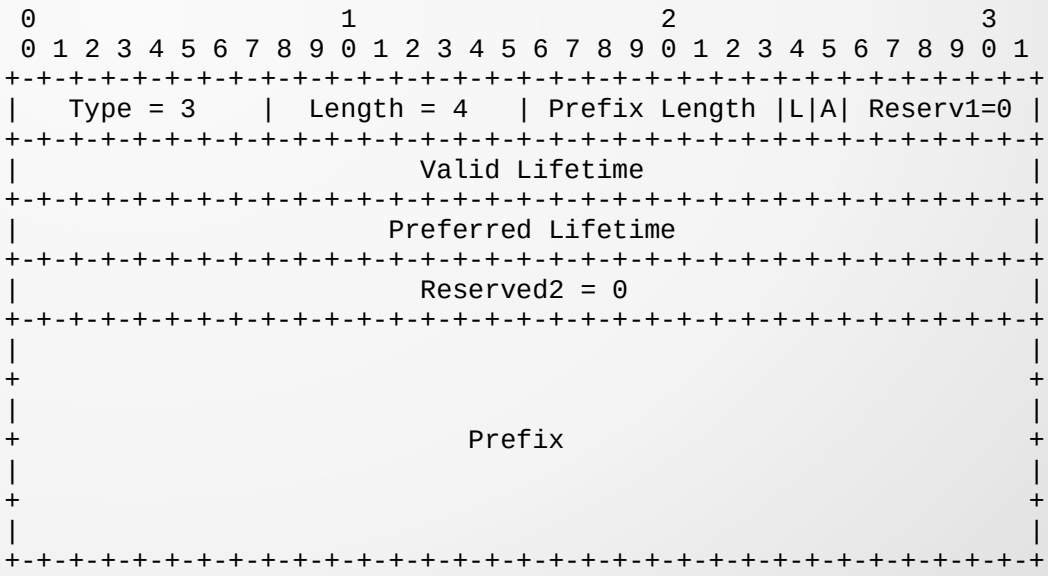
Formato RA

- Cur Hop Limit: valor por defecto del Hop Count de los paquetes IPv6 a enviar por el host. Si es 0, no especificado por este router
- Options: Source link-layer address del router, MTU (solo si es variable), Prefix Information



Prefix information option

- Asigna Prefix/Prefix Length con tiempos Preferred y Valid
- L (on link flag)=1 indica que equipos con este mismo prefijo son alcanzables directamente (en el mismo link)
- Si L=0, habrá que encaminar los paquetes hacia el router
- A=1 (autonomous address configuration) indica que el prefijo se puede usar para “stateless address configuration”. Si A=0 se ignora el prefijo



Ejemplo: Auto configuración SLAAC

- Un equipo se conecta a una red con un router
- El RA enviado tiene M=0 y O=0

1. Generación de la dirección link-local
   - Generación del Interface ID, por ejemplo usando EUI-64 a partir de la MAC address
     - MAC: 60:a4:4c:5c:8a:de
     - IID: 62a4:4cff:fe5c:8ade
   - Agrega el prefijo para direcciones link-local: fe80::/10
   - IPv6 link-local generada: fe80::62a4:4cff:fe5c:8ade

Ejemplo

2. Verificación de unicidad: DAD, Duplicate Address Detection
   - Envía un mensaje de NS (ICMP Code 135) con destino a la dirección Solicited Node correspondiente a la IP generada
   - Este mensaje será respondido por un NA (ICMP Code 136) si la dirección está siendo usada.
3. Si es única, la configura en la interfaz
4. Determinar si hay enrutadores presentes
   - Envía un Router Solicitation (ICMP Code 133) a la dirección multicast conocida de todos los routers: ff02::2
   - Espera un Router Advertisement (ICMP Code 134)
   - Si no hay router, debe ir a un método stateful

Ejemplo

5. Si hay router, este enviará un RA conteniendo
   - Las banderas M y O (en este ejemplo ambas en 0) lo que indica que se debe usar SLAAC tanto para la IP como para otros parámetros
   - La opción de prefijo, por ejemplo 2001:db8:1:1::/64
   - La información de DNS
6. Se genera la dirección IPv6 global con el prefijo y el IID
   - 2001:db8:1:1:62a4:4cff:fe5c:8ade
7. Verificación de unicidad: DAD
8. Si es única, la configura en la interfaz

Ejemplo

9. Configuración de la ruta por defecto
   - La ruta por defecto es: ::/0 y el próximo salto es la dirección link-local del router (dirección origen del RA)
10. Configuración del DNS
   - La IP del DNS se puede obtener del RA (opción RDNSS)
   - En la práctica SLAAC con DNS no está disponible en varios sistemas operativos
   - Se puede usar el DNS de IPv4 si tenemos dual-stack
   - O configurarlo por DHCPv6 (en el RA vendrá O=1) y el host enviará una petición DHCPv6 para obtener el DNS

Protocolo IPv6

- Por qué IPv6?
- Formato encabezado IPv6
- ICMPv6
- Direccionamiento IPv6
- Neighbor Discovery
- Auto configuración
- DHCP para IPv6
- Impacto del cambio IPv4 – IPv6 en capas superiores
- Transición IPv4 - IPv6

Auto configuración stateful: DHCPv6

- Funcionamiento similar al del DHCPv4
  - Modo cliente-servidor
  - Comunicación sobre UDP
  - Existe también el modo relay
- Usa puerto 546/udp para los clientes y 547/udp para los servidores o relays
- Los servidores escuchan en direcciones IPv6 conocidas:
  - FF02::1:2 (todos los servidores o relays DHCP en un enlace)
    - Usada por los clientes para comunicarse con el servidor o relay
  - FF05::1:3 (todos los servidores DHCP)
    - Usada por los relays para encontrar a los servidores
- DHCPv6 stateless cuando solo proporciona los “otros parámetros” y no la IP. No necesita almacenar la información de leases, etc

Auto configuración stateful: DHCPv6

- Si el cliente está en la misma LAN que el servidor:
  1. Cliente envía mensaje SOLICIT para pedir un recurso
  2. Servidor envía ADVERTISE ofreciendo el recurso solicitado
  3. Cliente confirma el ofrecimiento con un REQUEST
  4. Servidor lo asigna con REPLY
- Si no está en la misma LAN el SOLICIT lo atiende un relay que oficiará de intermediario en la comunicación entre el cliente y el servidor

Diferencias con DHCPv4

- DHCPv6 no da información sobre ruta por defecto
  - Debe resolverse por los RA o manualmente
- DHCPv6 un utiliza DUID (DHCP Unique ID) para identificar a clientes y servidores (en DHCPv4 se utilizan las MACs)
- Existe la posibilidad de delegar prefijos a routers mediante DHCPv6-PD (prefix delegation)
  - El router de un cliente puede solicitar un recurso IA_PD (Identity Association for Prefix Delegation) al ISP, obteniendo un prefijo que luego puede dividir y asignar a las redes internas

Ejemplo: auto configuración con DHCP

- Un equipo se conecta a una red donde hay un router y un relay DHCPv6
- Típicamente el RA enviado tendrá M=1 y O=1 (IP y “otros” desde DHCPv6)

1. Generación de la dirección link-local
   - Generación del Interface ID, por ejemplo usando EUI-64
     - MAC: 60:a4:4c:5c:8a:de
     - IID: 62a4:4cff:fe5c:8ade
   - Agrega el prefijo para direcciones link-local: fe80::/10
   - IPv6 link-local generada: fe80::62a4:4cff:fe5c:8ade

Ejemplo

2. Verificación de unicidad: Duplicate Address Detection
   - Envía un mensaje de NS (ICMP Code 135) con destino a la dirección Solicited Node correspondiente a la IP generada
   - Este mensaje será respondido por un NA (ICMP Code 136) si la dirección está siendo usada.
3. Si es única, la configura en la interfaz
4. Determinar si hay enrutadores presentes
   - Envía un Router Solicitation (ICMP Code 133) a la dirección multicast conocida de todos los routers: ff02::2
   - Espera un Router Advertisement (ICMP Code 134)

Ejemplo

5. El router enviará un RA conteniendo
   - Las banderas M y O (en este ejemplo ambas en 1) lo que indica que se debe usar DHCPv6 tanto para la IP como para otros parámetros
6. El host enviará un SOLICIT a la dirección multicast de todos los servers/relays DHCPv6 que continuará con ADVERTISE, REQUEST, REPLY
7. El servidor DHCPv6 proporcionará entonces la dirección IP a utilizar y las IPv6 de los servidores DNS
8. Se verifica la unicidad con DAD
9. Se configura la dirección en la interfaz
10. Configuración de la ruta por defecto
    - La ruta por defecto es: ::/0 y el próximo salto es la dirección link-local del router (dirección origen del RA)

Otras combinaciones

- La combinación M=0, O=1 es la que se usa en el caso de SLAAC para obtener la IP por RA y el DNS por DHCPv6
- La otra opción M=1, O=0 que sería configurar la IP por DHCPv6 y el DNS por SLAAC, no está disponible en varios sistemas operativos

Protocolo IPv6

- Por qué IPv6?
- Formato encabezado IPv6
- ICMPv6
- Direccionamiento IPv6
- Neighbor Discovery
- Auto configuración
- DHCP para IPv6
- Impacto del cambio IPv4 – IPv6 en capas superiores
- Transición IPv4 - IPv6

¿Qué implica cambiar el protocolo IP?

- Cambiar el protocolo IP impacta en las capas superiores porque el modelo de capas ideal no existe
- Hay que hacer cambios en la capa de transporte y en la capa de aplicación
- Hay que modificar o extender los protocolos de ruteo dinámico
- No cambia la forma en que se hace el forwarding en capa de red
  - Se sigue usando el longest-prefix-match

Impacto de IPv6 en TCP y UDP

- El cálculo del checksum de TCP y UDP incluye el pseudo-header donde están las direcciones IP
  - Hay que modificar estos protocolos para que ahora usen las direcciones IPv6 en el pseudo-header

Impacto de IPv6 en el DNS

- Nuevo tipo de registro: AAAA
  - Asocia una etiqueta con una dirección IPv6
  - Funciona igual que el registro A para IPv4
- Nueva rama para la resolución inversa: **ip6.arpa**

  (equivalente al in-addr.arpa usado en IPv4)
- Las direcciones se representan en hexadecimal y se representan todos los dígitos, en orden inverso, separados por puntos
- Por ejemplo:
  - para la dirección 2001:4860:4802:34::a, debo buscar el registro PTR correspondiente a:
  - a.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.3.0.0.2.0.8.4.0.6.8.4.1.0.0.2.ip6.arpa.

Protocolo IPv6

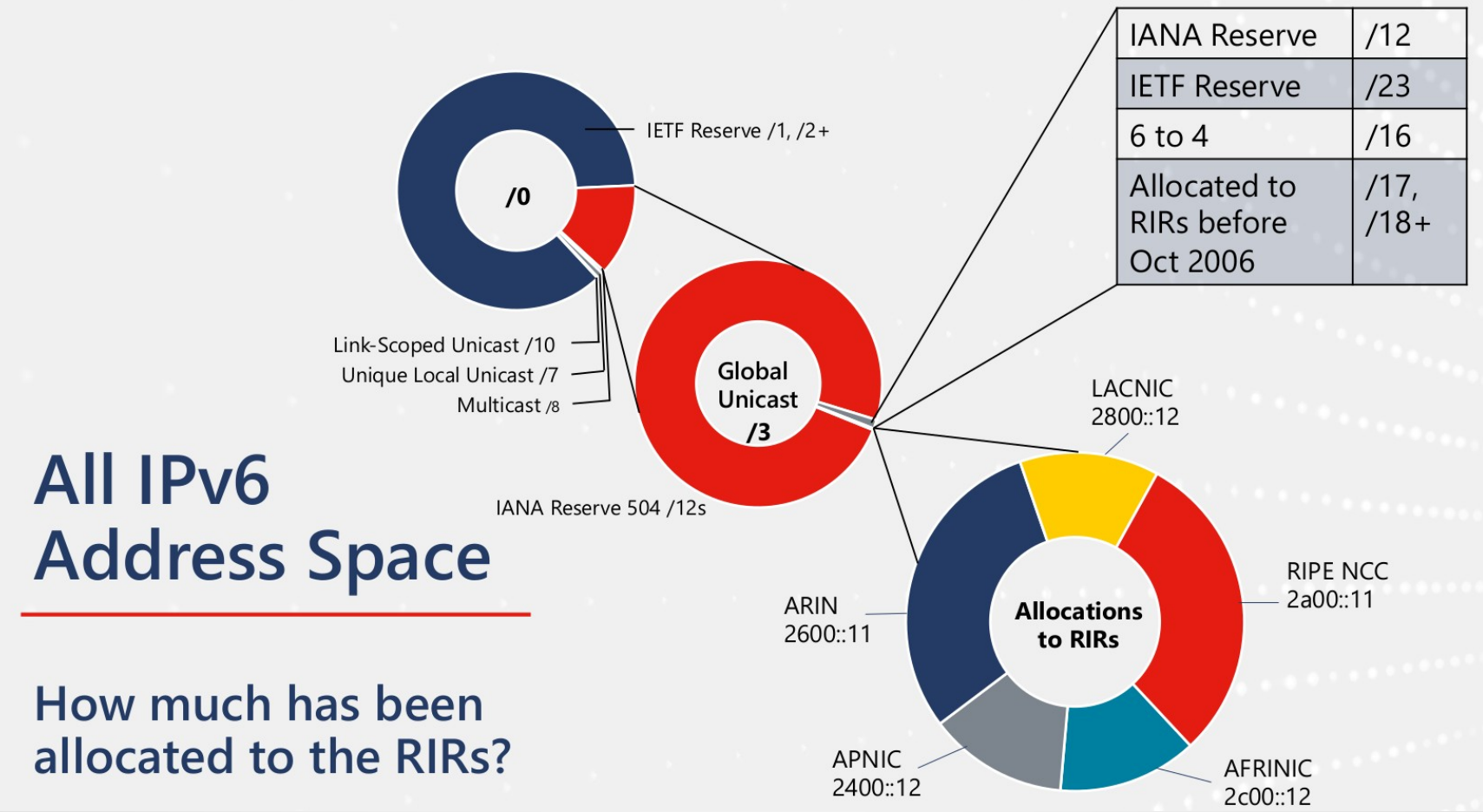
- Por qué IPv6?
- Formato encabezado IPv6
- ICMPv6
- Direccionamiento IPv6
- Neighbor Discovery
- Auto configuración
- DHCP para IPv6
- Impacto del cambio IPv4 – IPv6 en capas superiores
- Transición IPv4 - IPv6

Transición IPv4 a IPv6

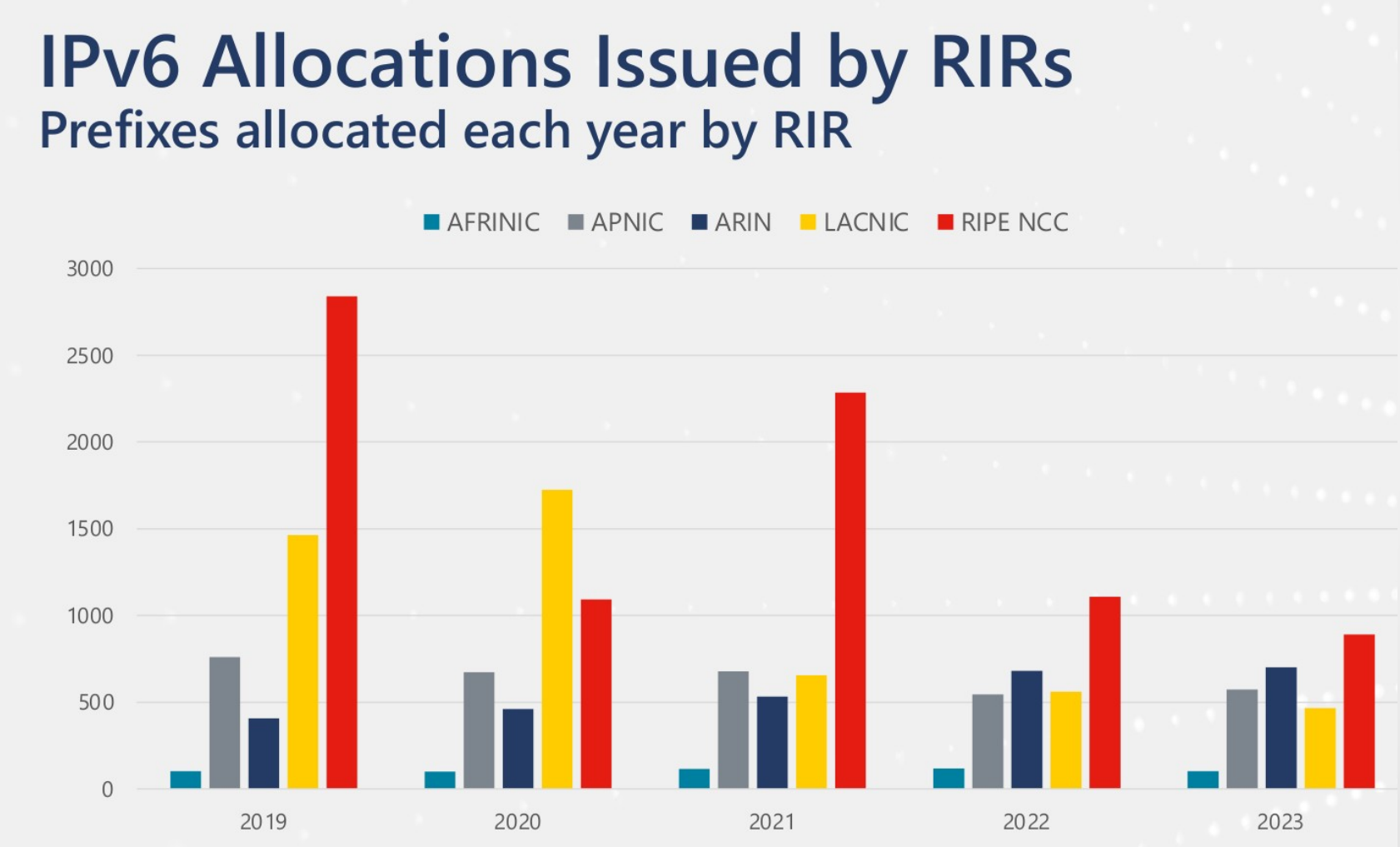
- IPv6 fue diseñado pensando que conviviría con IPv4
- Se esperaba tener redes IPv4 que gradualmente se pasaran a IPv6
- Pero esa adopción viene siendo muy lenta a pesar que las IPv4 se agotan
- Hay que ofrecer mecanismos que permitan a nodos IPv4 acceder a nodos IPv6
- Y también hay que ver cómo hacer para que nodos IPv6 accedan a redes que sólo poseen IPv4

Espacio IPv6 asignado a RIRs

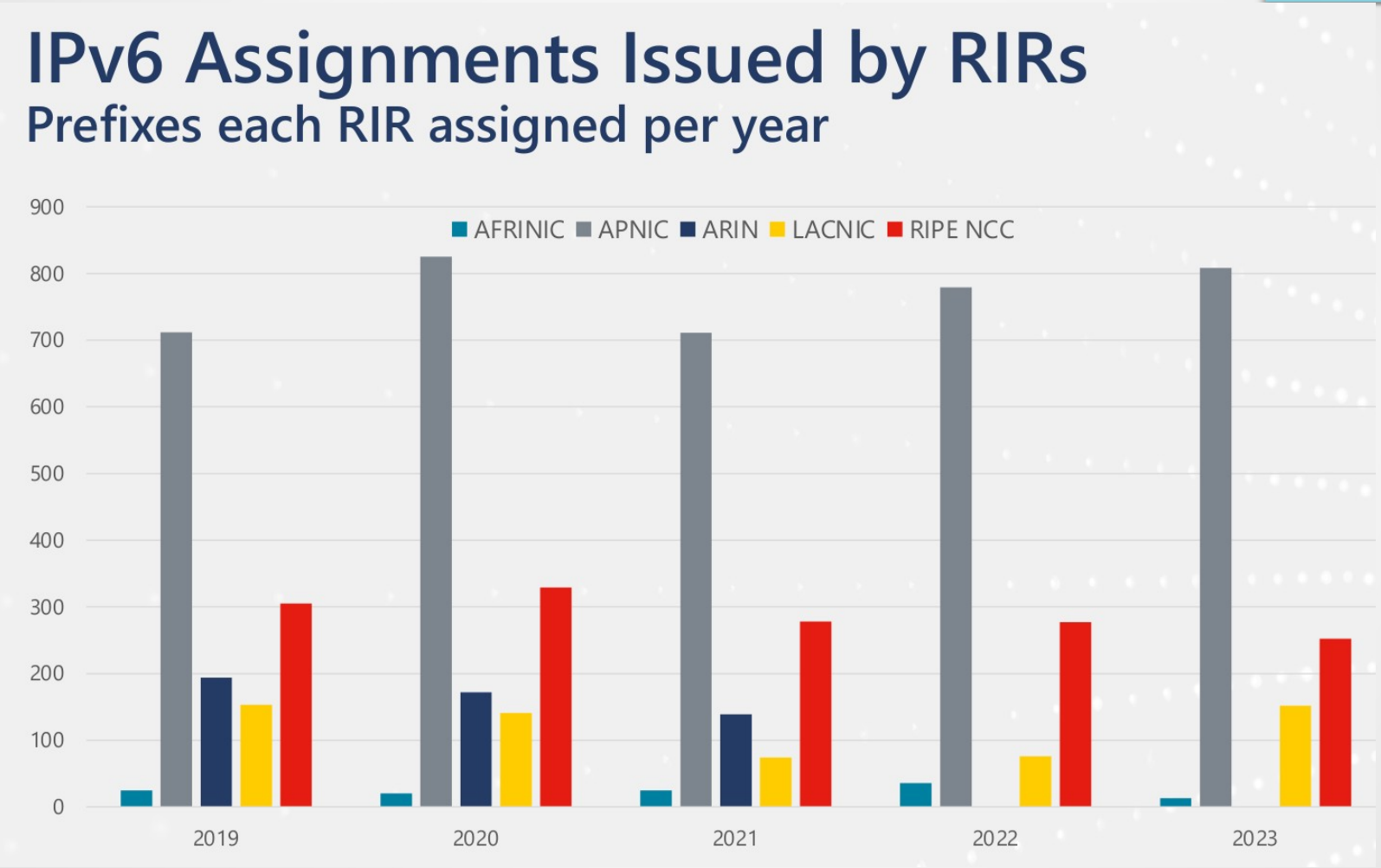
- Internet Number Resource Status Report - 31/12/2023 - www.nro.net



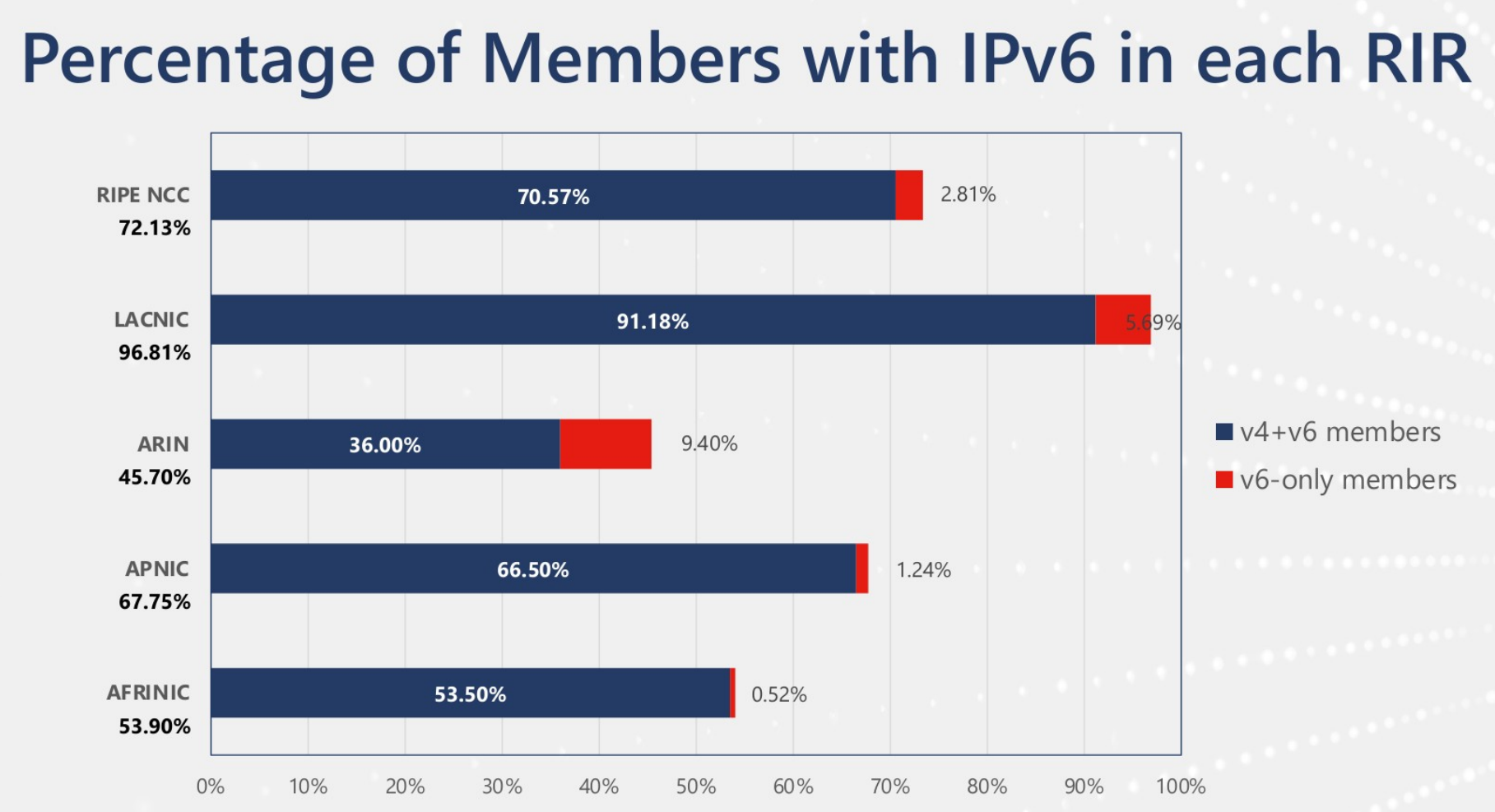
Distribución de prefijos a RIRs



Asignaciones por RIR

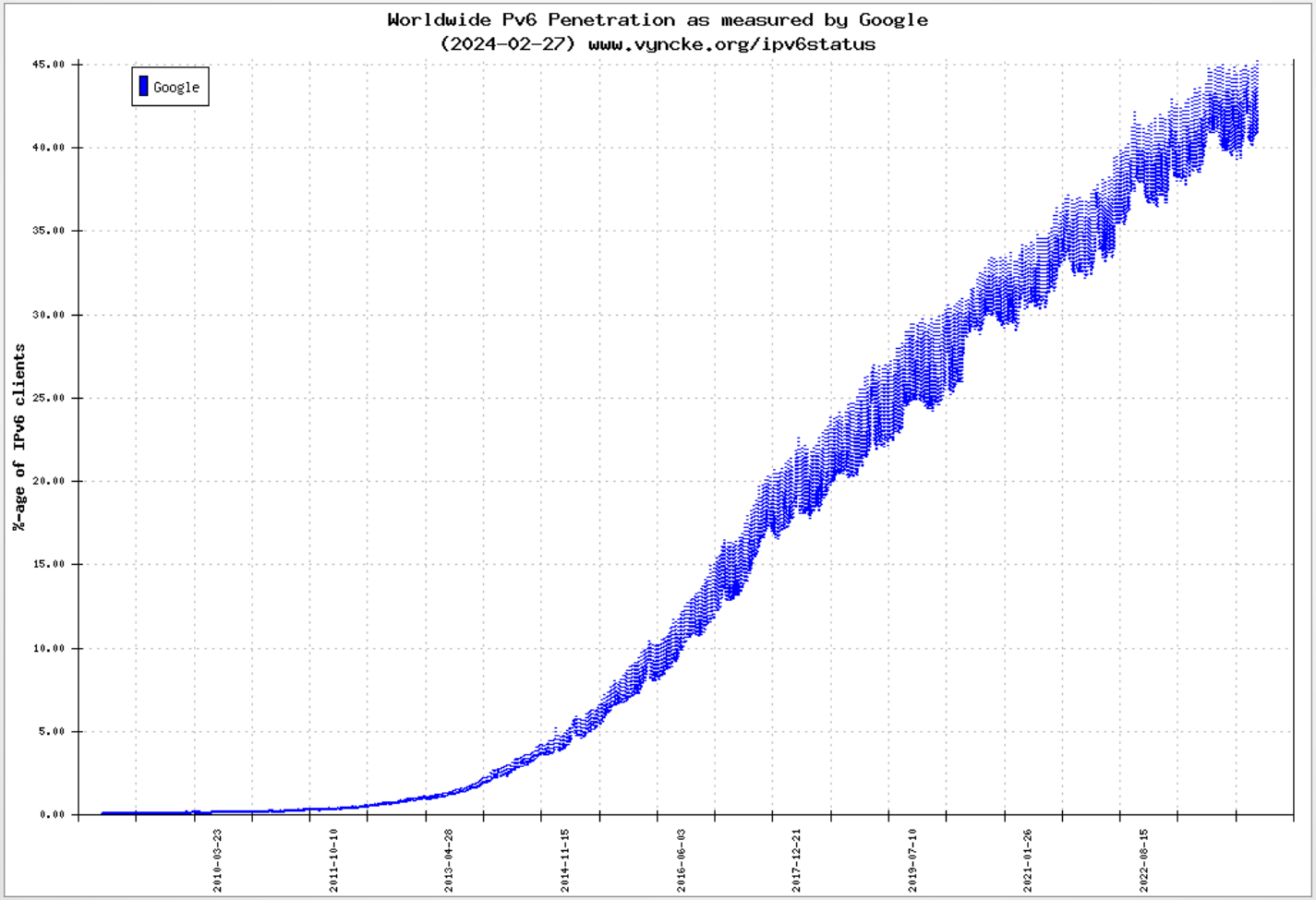


Miembros con IPv6 en cada RIR



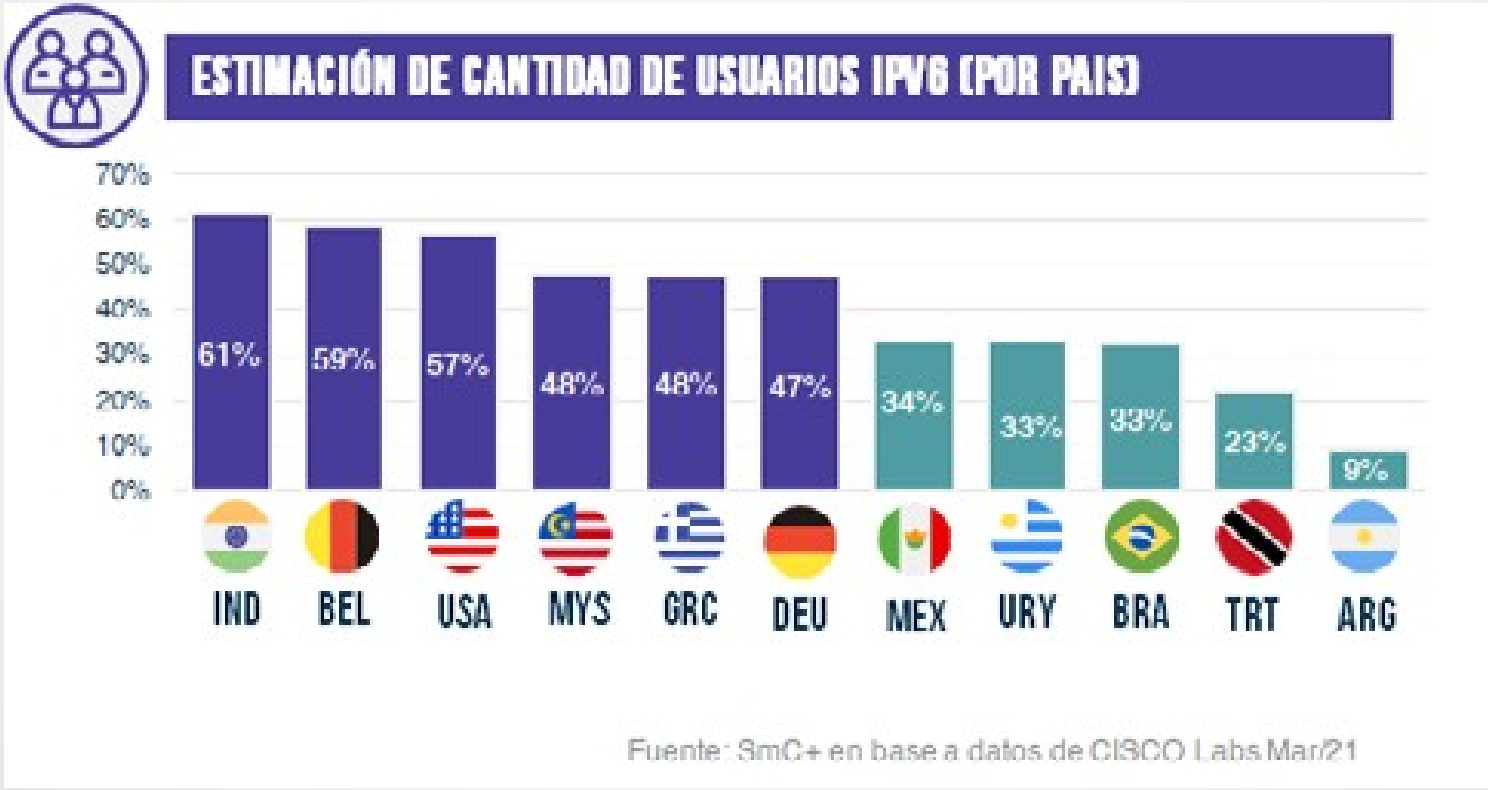
Estadísticas de adopción de IPv6

- https://www.vyncke.org/ipv6status/

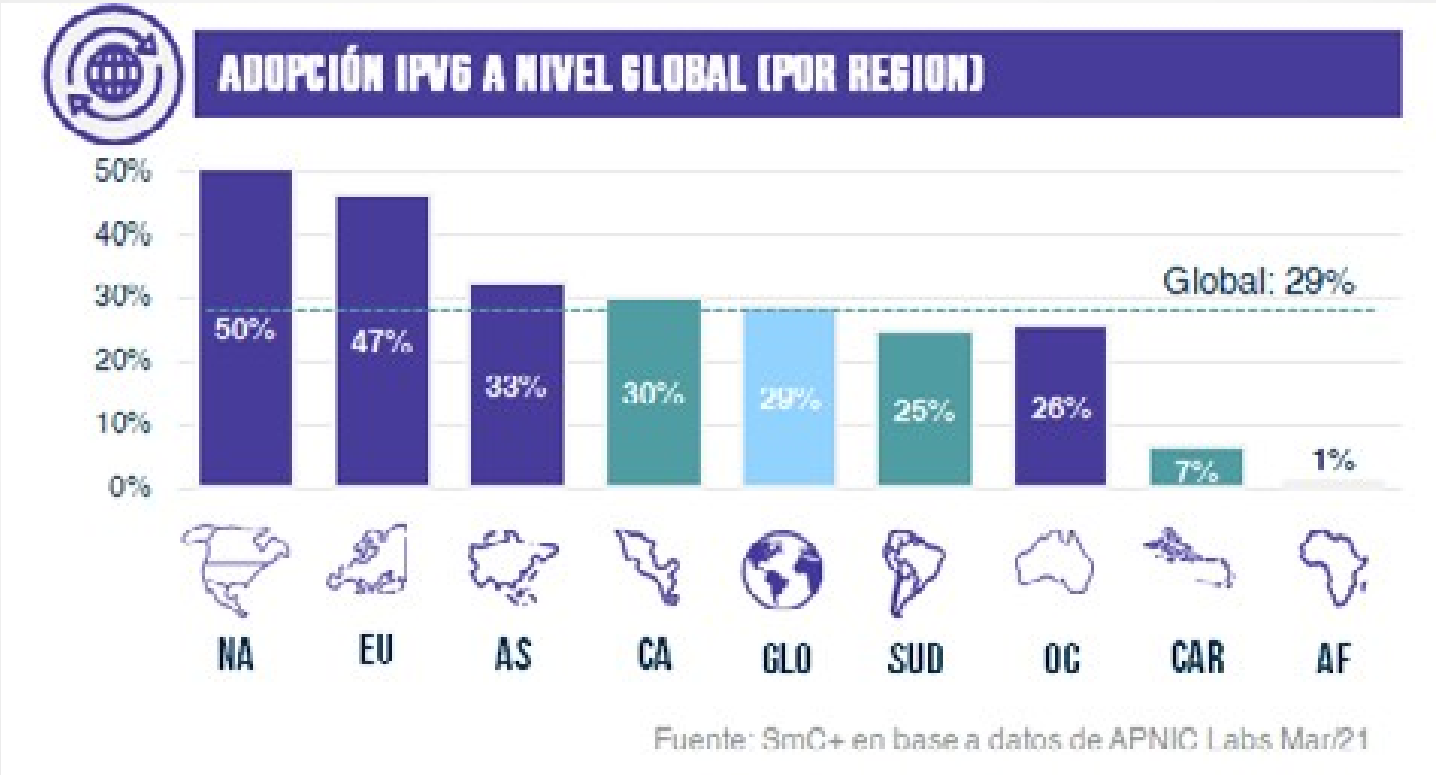


Estadísticas de adopción de IPv6

- ESTADÍSTICAS Y TENDENCIAS: EL DESPLIEGUE DE IPV6 EN AMÉRICA LATINA Y EL CARIBE – Marzo 2021

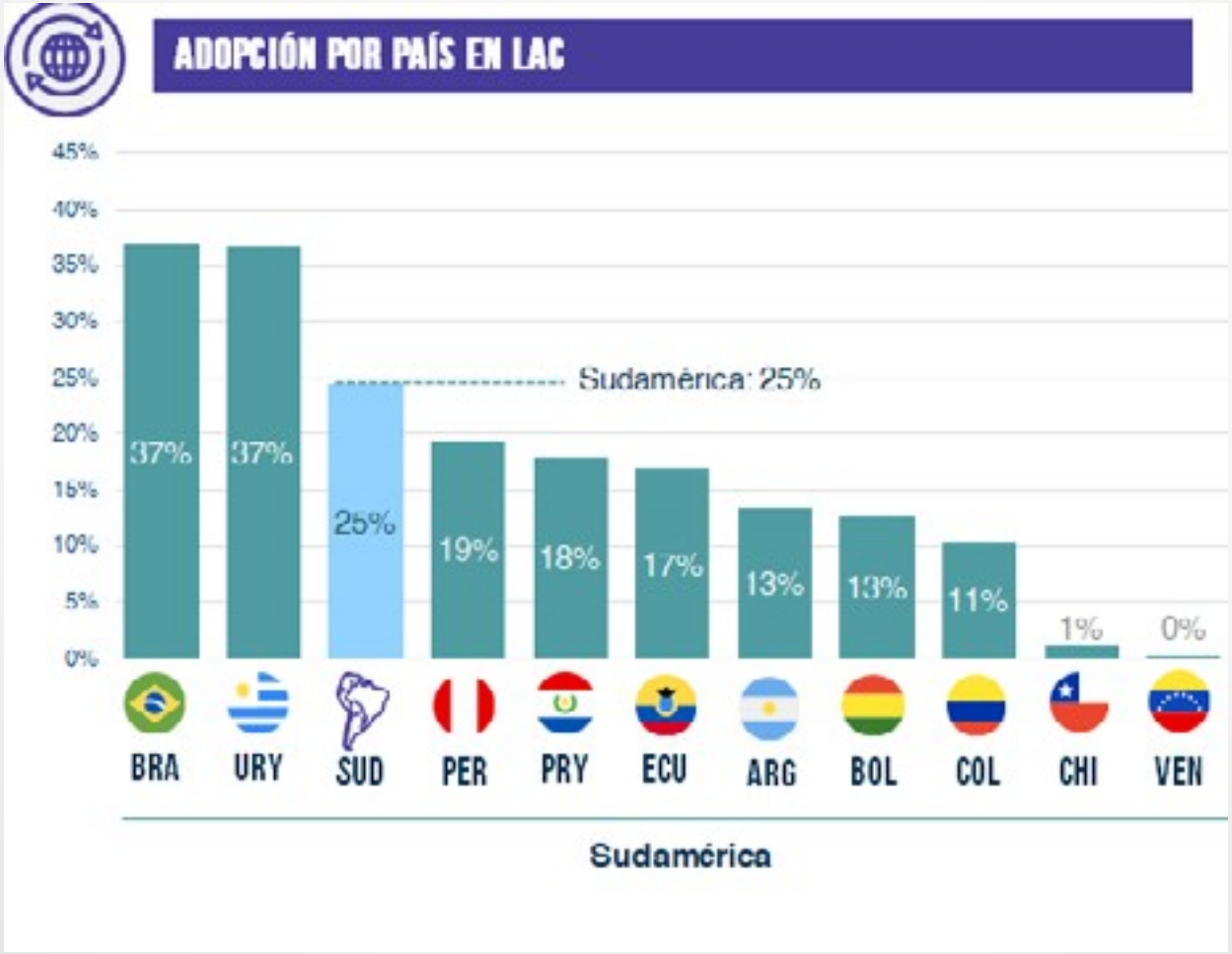


Estadísticas de adopción de IPv6



Estadísticas de adopción de IPv6

- Región Latino América y Caribe



Mecanismos de transición

- Hay que diseñar estrategias de transición hacia IPv6

  … en un contexto de agotamiento de las direcciones IPv4
- Tres estrategias principales ordenadas por preferencia:
  - IPv6 nativo: IPv6 de origen a destino, los nodos pueden ser “solo-IPv6” o “dual-stack” (entienden IPv6 e IPv4)
  - Túneles: Encapsular una versión de IP en la otra
  - Traducción: Para que hable un nodo solo IPv4 con otro solo IPv6
- Las estrategias se pueden combinar según el caso

Mecanismos de transición

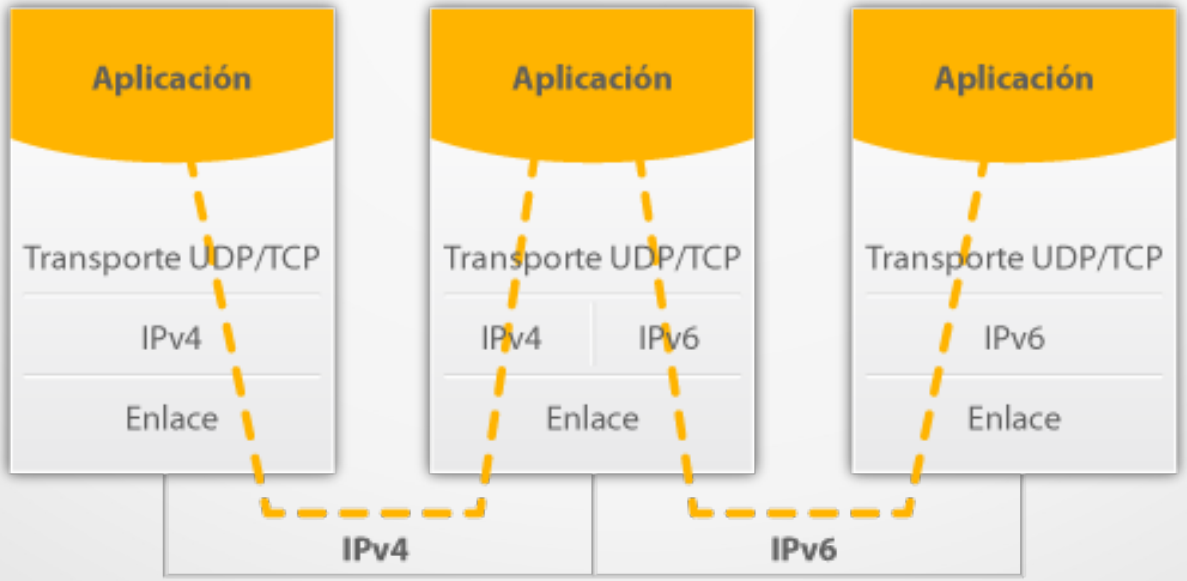
- Inicialmente teníamos redes IPv4 que gradualmente incorporaban IPv6, pero a medida que el agotamiento de IPv4 se extiende, los proveedores comienzan a pensar en redes de acceso exclusivamente IPv6
- Esto implica ofrecer mecanismos que permitan continuar accediendo a aquellas redes que sólo poseen IPv4
- Existe una gran variedad de mecanismos de transición propuestos y muchos de ellos están actualmente en discusión en la IETF
  - Muchos ya han caído en desuso (“deprecados”)
  - Siguen apareciendo nuevas propuestas

IPv6 nativo

- Toda la red con IPv6, sin encapsulado ni traducción
- Solución definitiva
- Pero ... requiere que todos los dispositivos hablen IPv6
- Dos opciones:
  - Dual-stack: se agrega soporte IPv6 a los nodos que ya soportan IPv4
    - Permite transición gradual
    - El cliente elige si usa IPv4 o IPv6, ambos están disponibles
    - La preferencia actual es IPv6 – IPv4 – MT de IPv6
  - IPv6-only: solo nodos IPv6
    - El acceso a IPv4 hay que hacerlo con túneles o traducción

Dual Stack

- Si el destino es sólo IPv4, se utiliza la conectividad IPv4
- Si el destino tiene IPv6, se utilizará la red IPv6
- En caso que el destino tenga ambos protocolos, normalmente se preferirá primero IPv6 y después IPv4

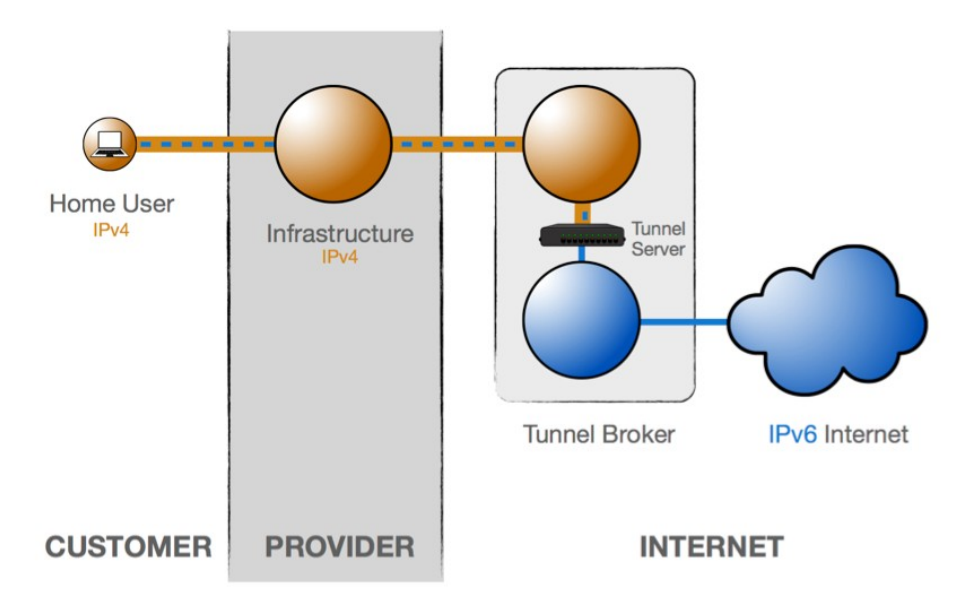


Mecanismos de transición: Túneles

- Permiten atravesar una red que solo soporta IPvX
- Se encapsula una versión de IP en otra
- Pueden ser:
  - estáticos o automáticos
  - punto a punto o multipunto
- Hay muchas propuestas, muchas en desarrollo y muchas obsoletas
- Se puede encapsular:
  - IPv6 sobre IPv4
  - IPv6 sobre GRE (Generic Routing Encapsulation) sobre IPv4
  - IPv6 sobre UDP sobre IPv4
  - IPv4 sobre IPv6

Mecanismos de transición: Túneles

- 6in4: Encapsula IPv6 en IPv4 (directamente o con GRE)
  - Punto a punto
  - Túneles manualmente configurados - Simple pero no escalable
  - Existe mecanismo Tunnel broker si el proveedor no brinda IPv6

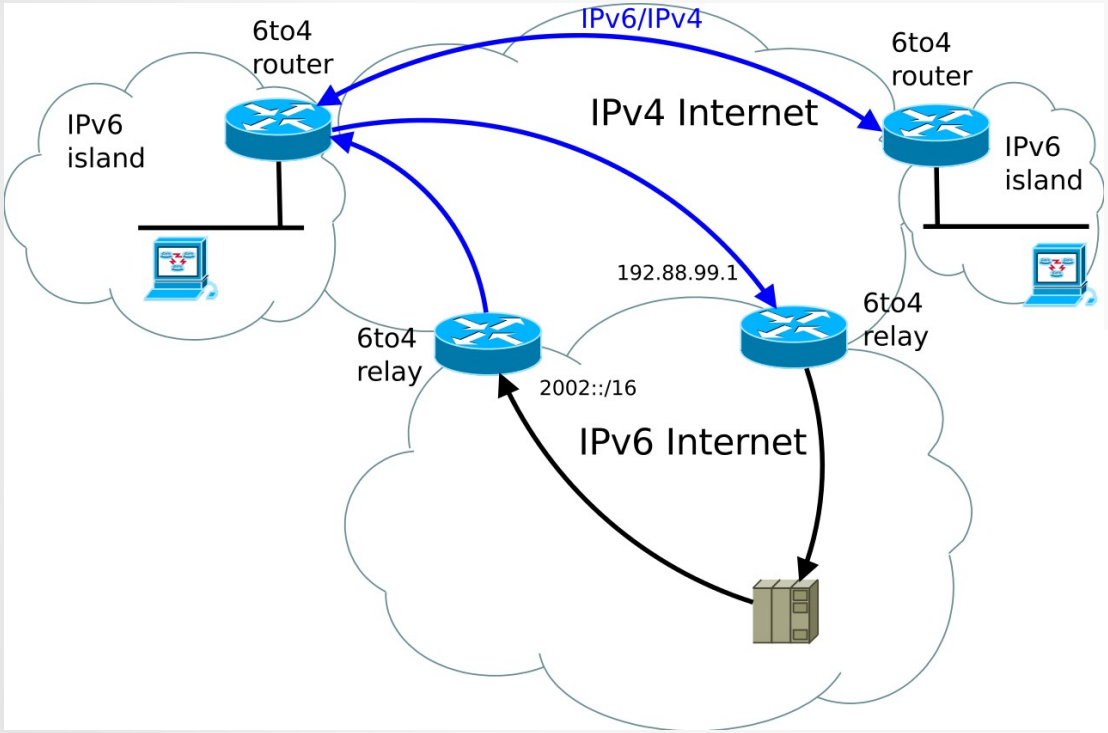


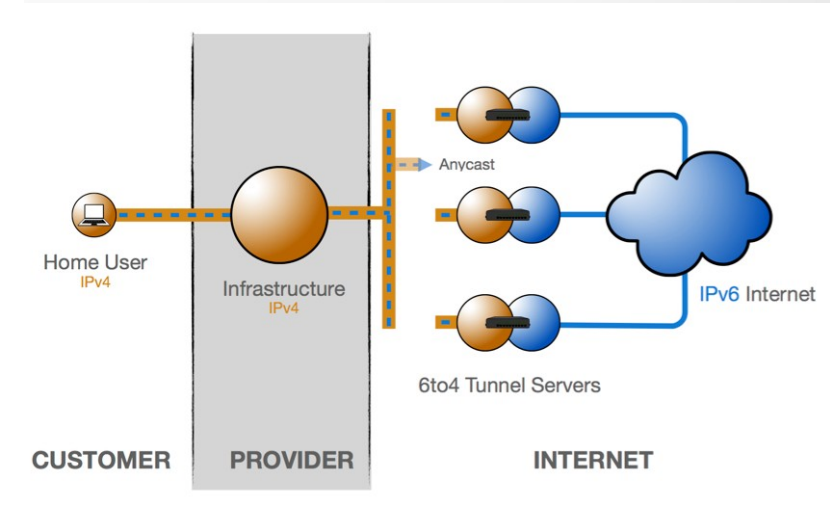
Mecanismos de transición: Túneles

- 6to4: Encapsula IPv6 en IPv4 (ya no se usa más)
  - Automático, Multipunto
  - Permite escalabilidad (mejora respecto a 6in4)
  - 6to4 realiza 3 funciones principales:
    - Asigna direcciones IPv6 a cualquier nodo o red que tenga direcciones globales IPv4
    - Encapsula paquetes IPv6 en IPv4 para ser enviados sobre una red IPv4
    - Encamina trafico entre 6to4 y una red IPv6 nativa (relay 6to4)
  - Muy difundido en su momento y es la base de 6RD
  - Ya no se usa más por problemas de seguridad y latencia

Mecanismos de transición: Túneles

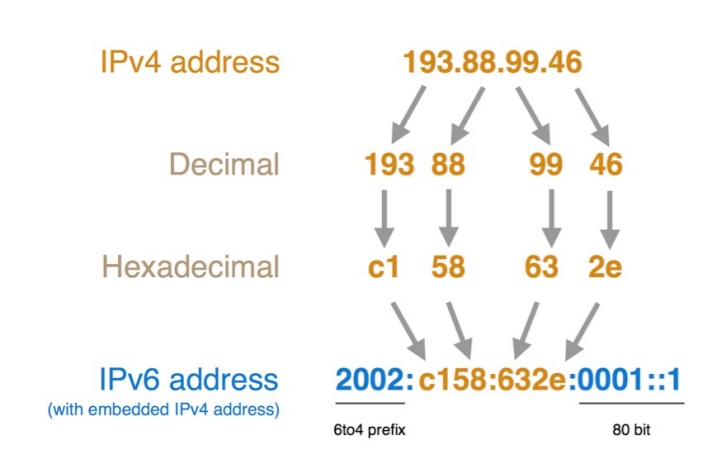
- 6to4: escenarios





Mecanismos de transición: Túneles

- 6to4
  - A partir de la IPv4 pública el router genera un prefijo: 2002::/16 + IPv4/32 => /48 y configura una interfaz virtual para encapsular/desencapsular IPv6 en IPv4

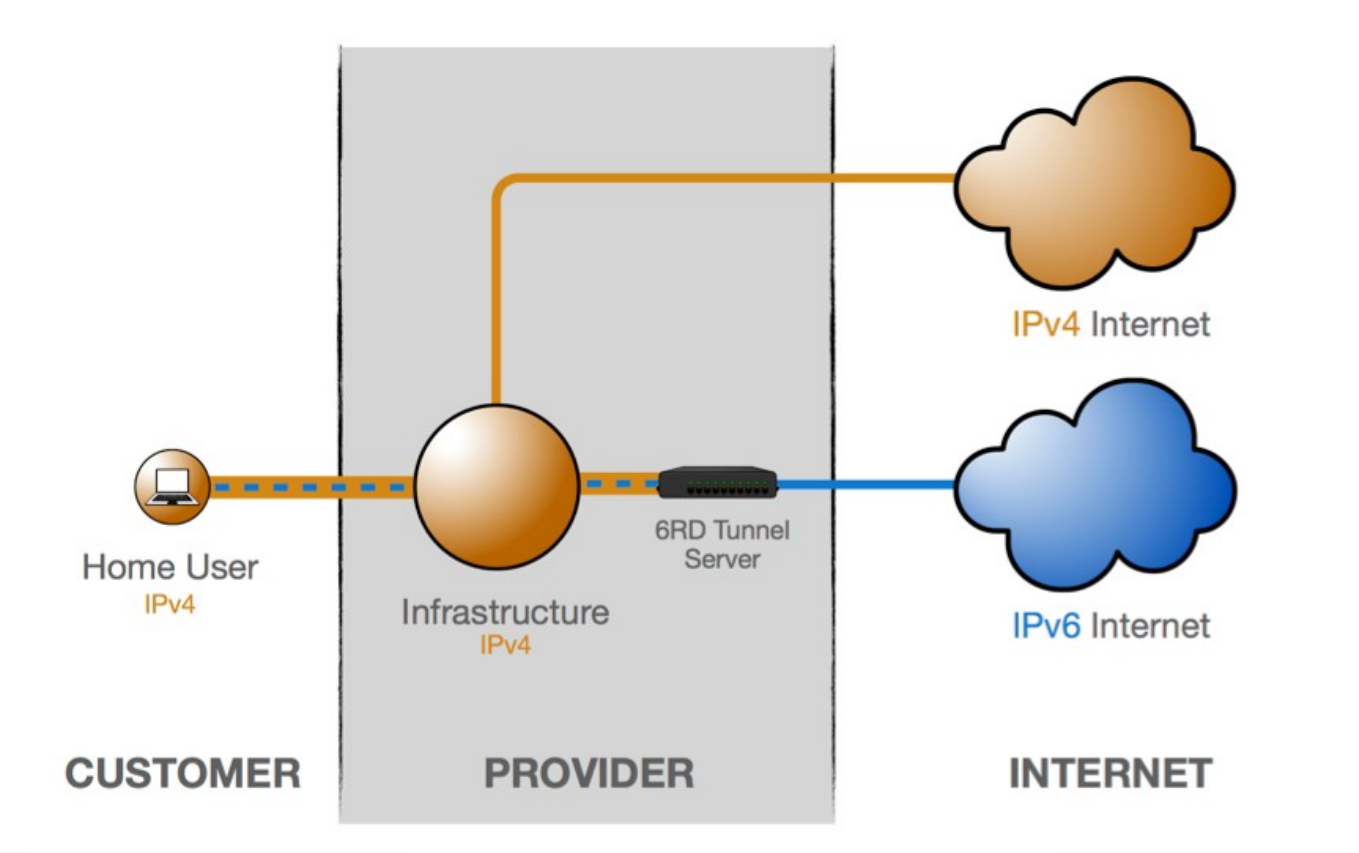


Mecanismos de transición: Túneles

- 6RD: Encapsula IPv6 en IPv4
  - Automático, Multipunto
  - Evolución de 6to4
    - Mejora latencia del 6to4
    - No necesita un prefijo reservado, usa GUA
    - Se puede usar con IPv4 privadas en ámbitos privados
    - Calcula igual el prefijo: Pref GUA+IPv4 -> pref 6RD
  - Usado por los ISPs

Mecanismos de transición: Túneles

- 6RD

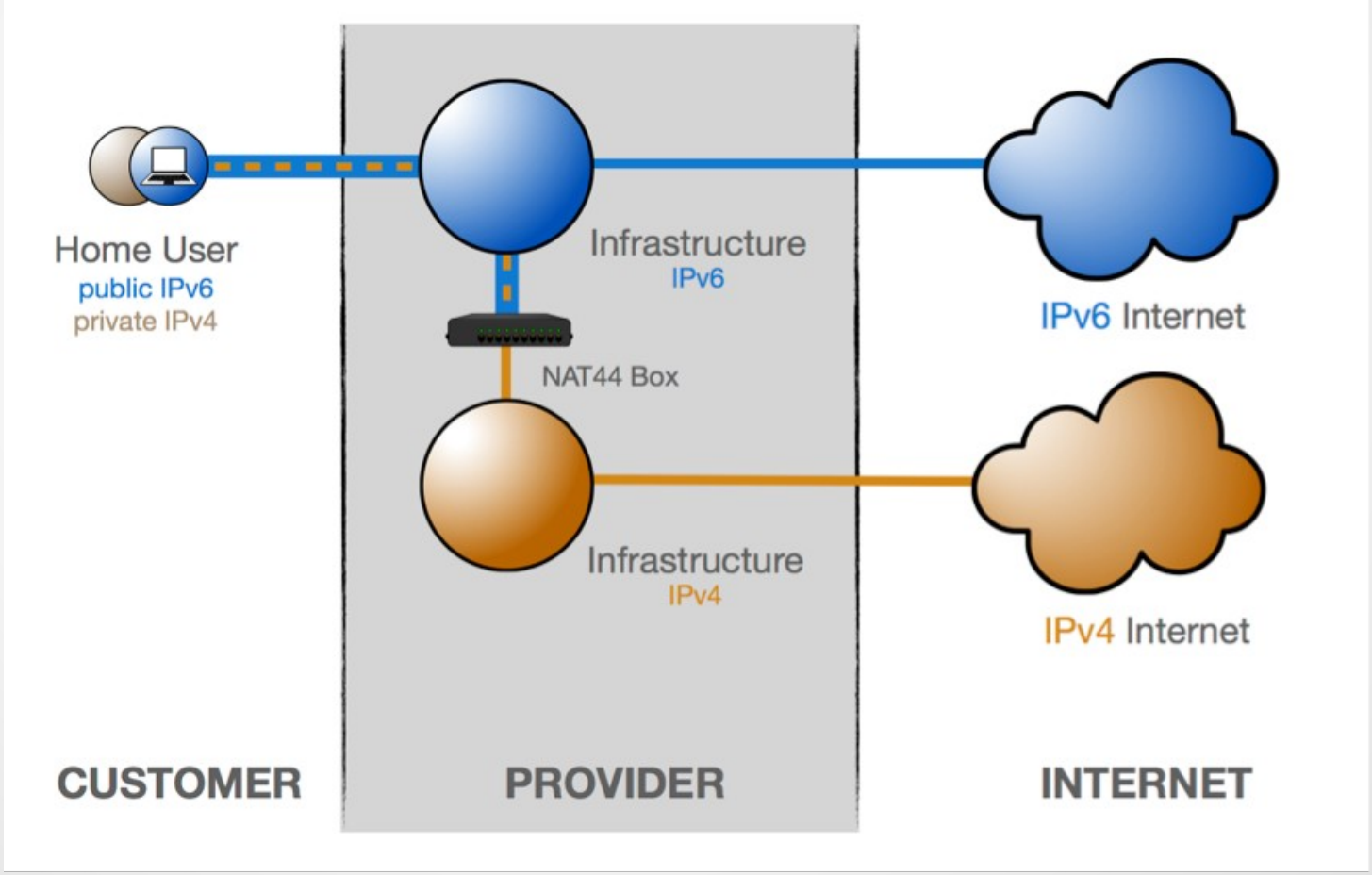


Mecanismos de transición: Túneles

- DS-lite: Encapsula IPv4 sobre IPv6
  - El principal propósito de DS-lite es para que el ISP pueda evitar el despliegue de direcciones IPv4 públicas al equipo del cliente (CPE). Solo se le asignan direcciones IPv6 globales
  - Se usa para compartir IPv4 públicas usando NAT (Address Family Transition Router, Carrier Grade NAT, Large Scale NAT). El ISP distribuye IPv4 privadas a sus clientes
- 6PE: Conexión de islas IPv6 sobre IPv4 MPLS (se verá más adelante)

Mecanismos de transición: Túneles

- DS-lite



Mecanismos de transición: Traducción

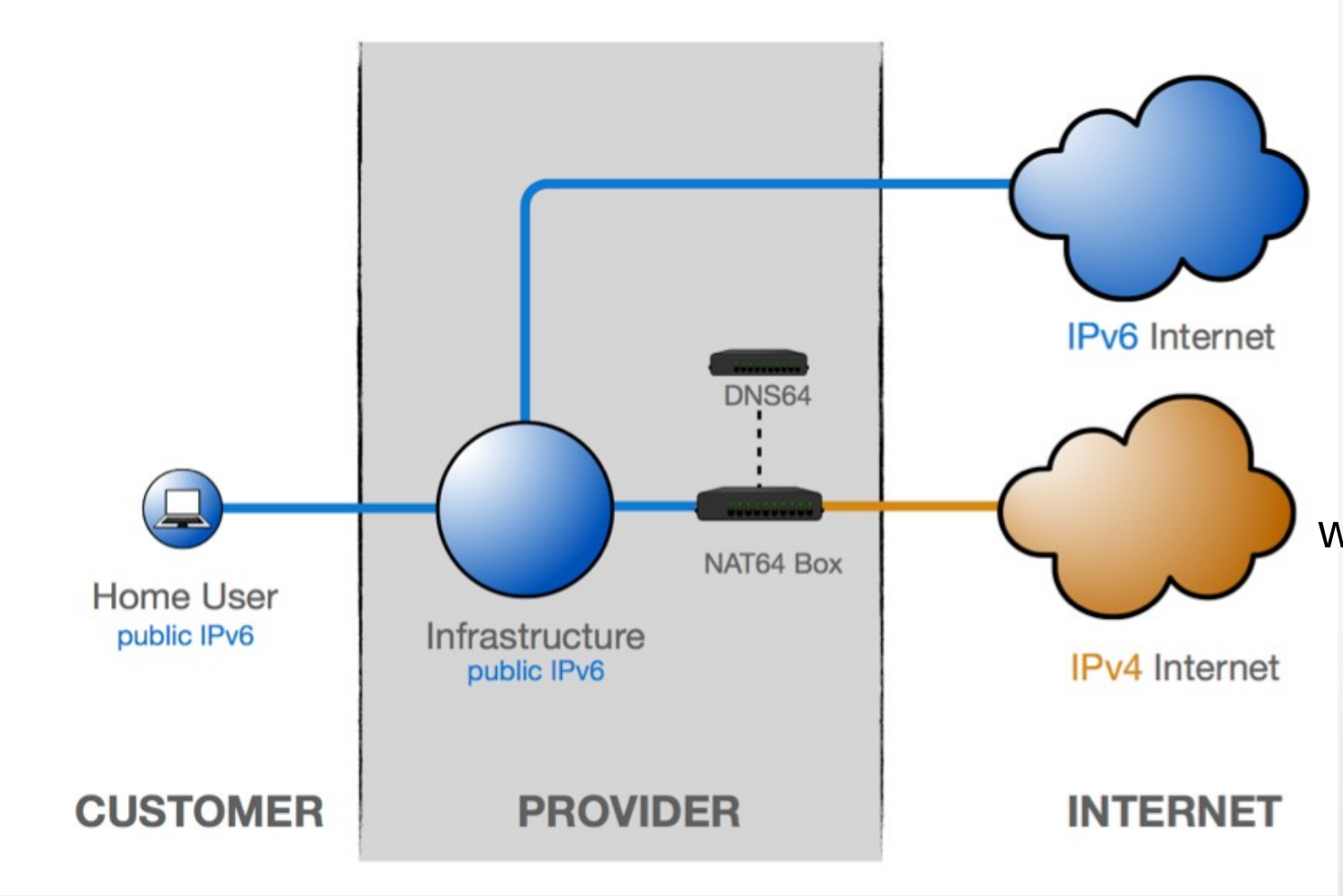
- Son los menos recomendados
- Son necesarios cuando se necesita comunicar un host solo-IPv4 con otro solo-IPv6
- Es necesario un mecanismo de traducción entre las dos redes
- Si la comunicación es IPv4->IPv6 se debe brindar conectividad IPv6 al nodo origen. Otras propuestas fueron declaradas obsoletas
- Si la comunicación es iniciada por el nodo IPv6 existen mecanismos para realizarlo

Mecanismos de transición: Traducción

- **NAT64/DNS64: IPv6 hacia IPv4** (RFC6146/RFC6147)
  - NAT64 solo se define para unicast TCP, UDP e ICMP
  - Se comparten direcciones IPv4 públicas
  - Se traducen automáticamente las direcciones
  - Lo más usado es concatenar un prefijo conocido 64:ff9b::/96 con la dirección IPv4/32
  - Los nodos IPv6 creen que los nodos solo-IPv4 son alcanzables por IPv6
  - Aparece entonces DNS64 para crear respuestas falsas de DNS con la IPv4 traducida automáticamente a IPv6 (caso Stateful)
  - Sin DNS64, el servidor pone el registro AAAA con la IPv4 embebida (Stateless)

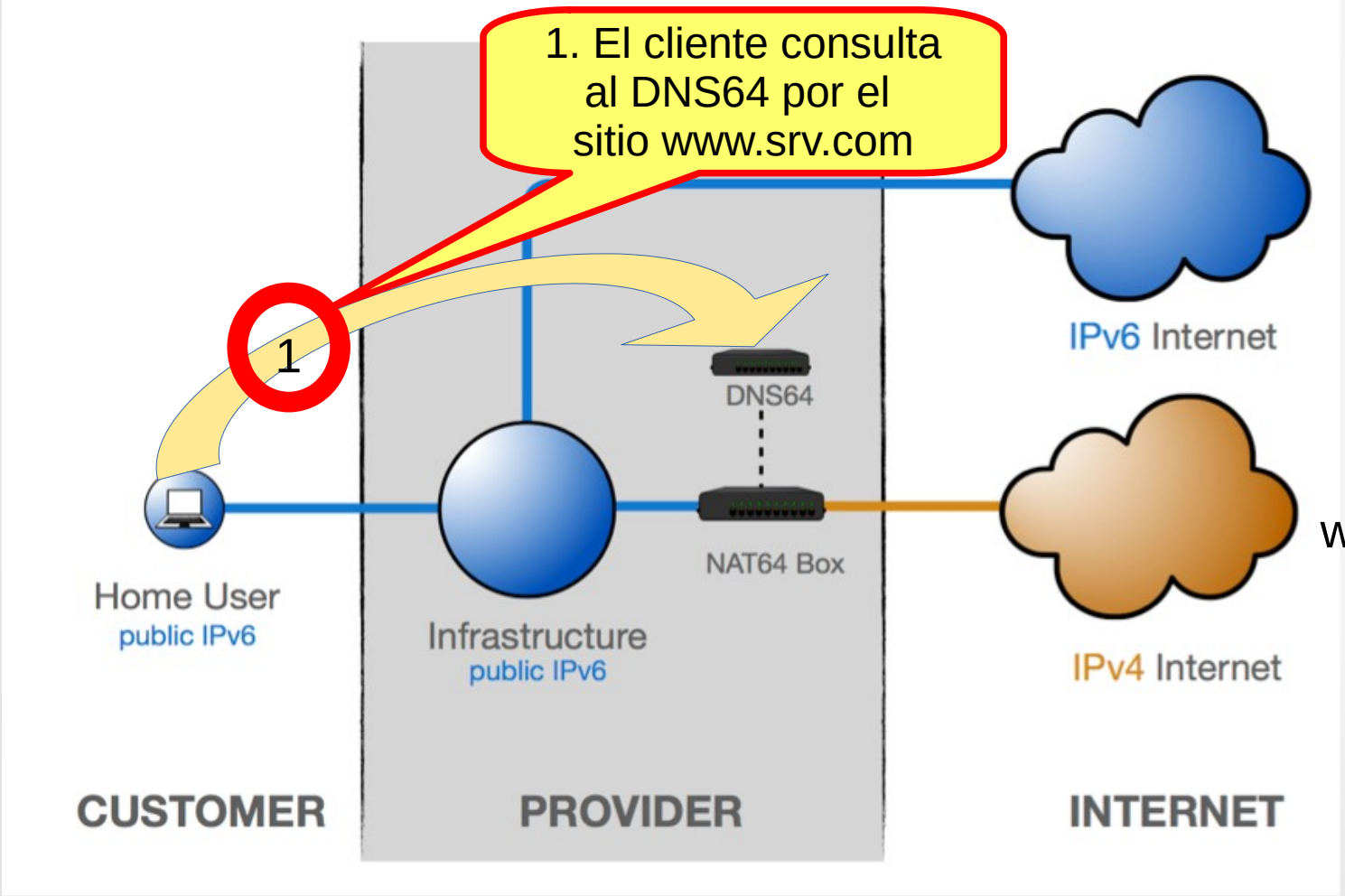
Mecanismos de transición: Traducción

- NAT64/DNS64



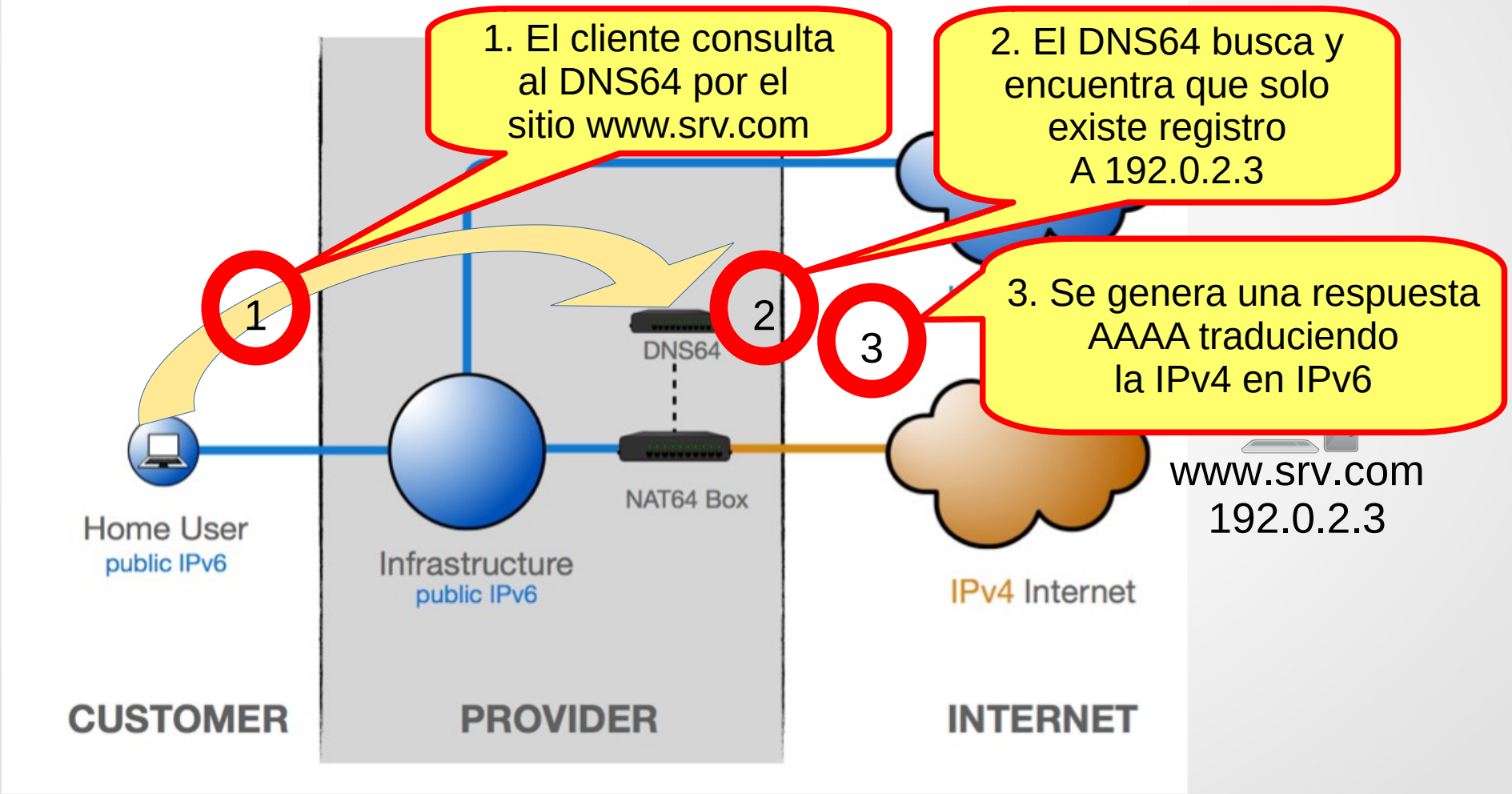
Mecanismos de transición: Traducción

- NAT64/DNS64



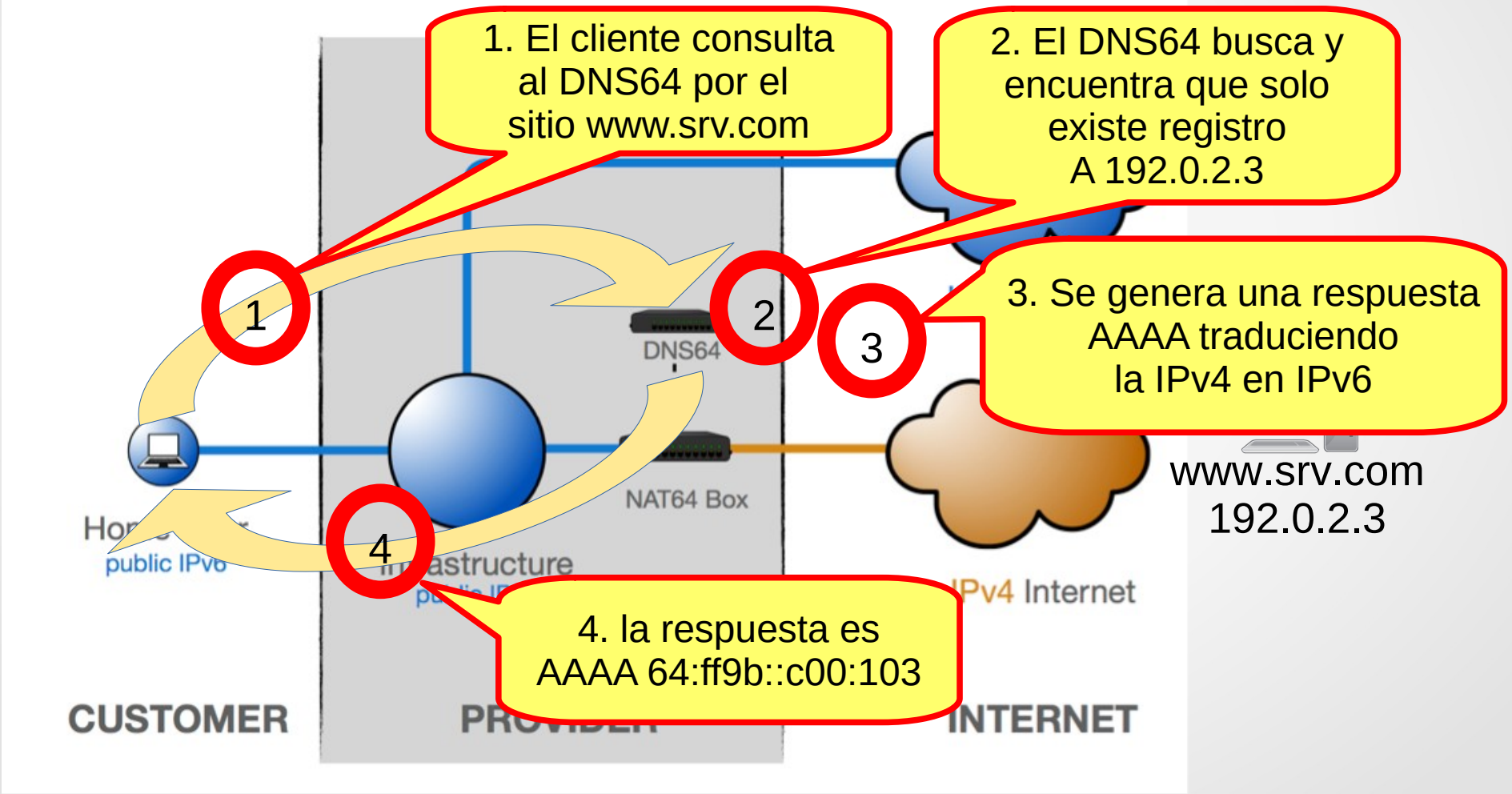
Mecanismos de transición: Traducción

- NAT64/DNS64



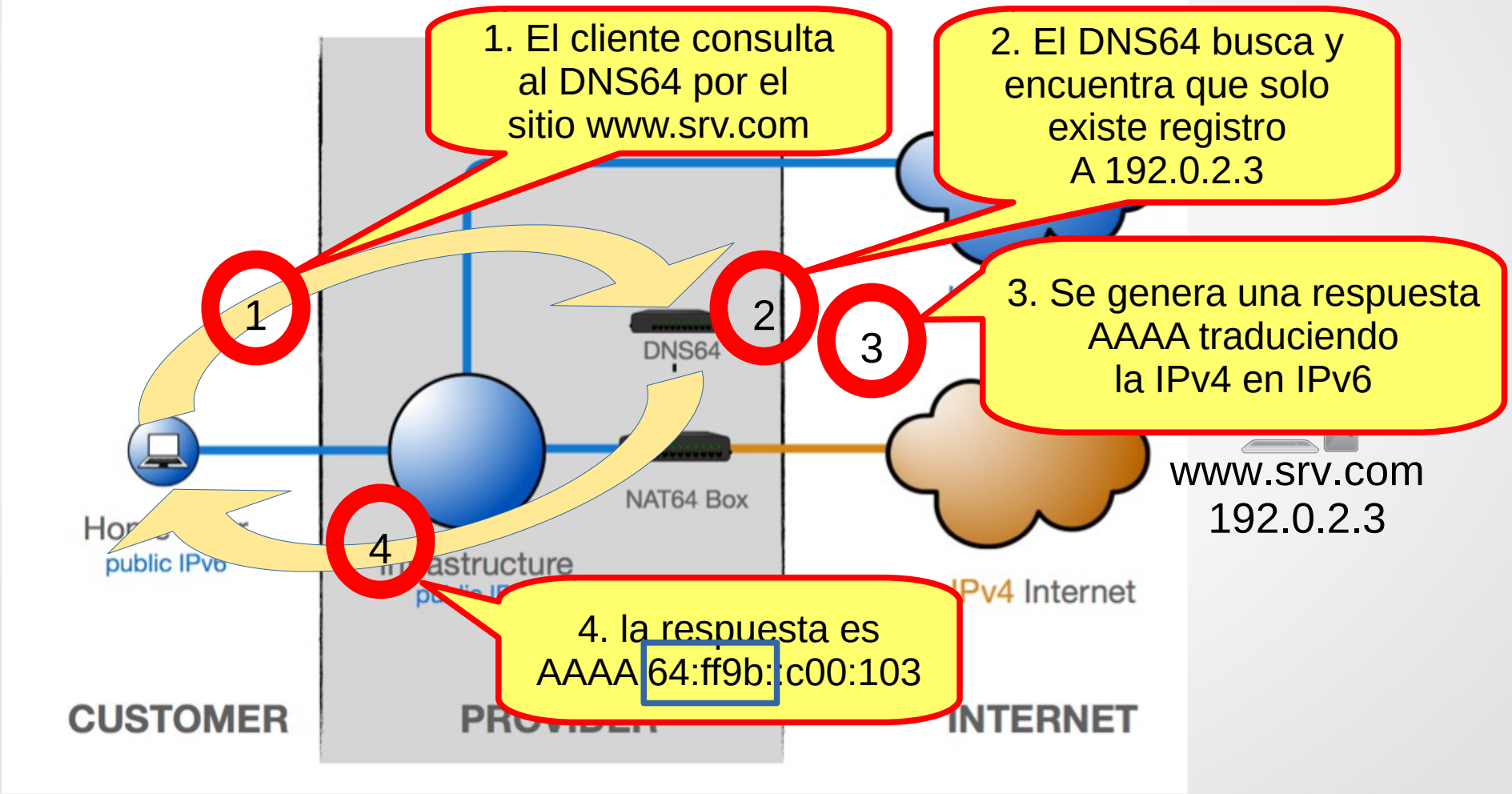
Mecanismos de transición: Traducción

- NAT64/DNS64



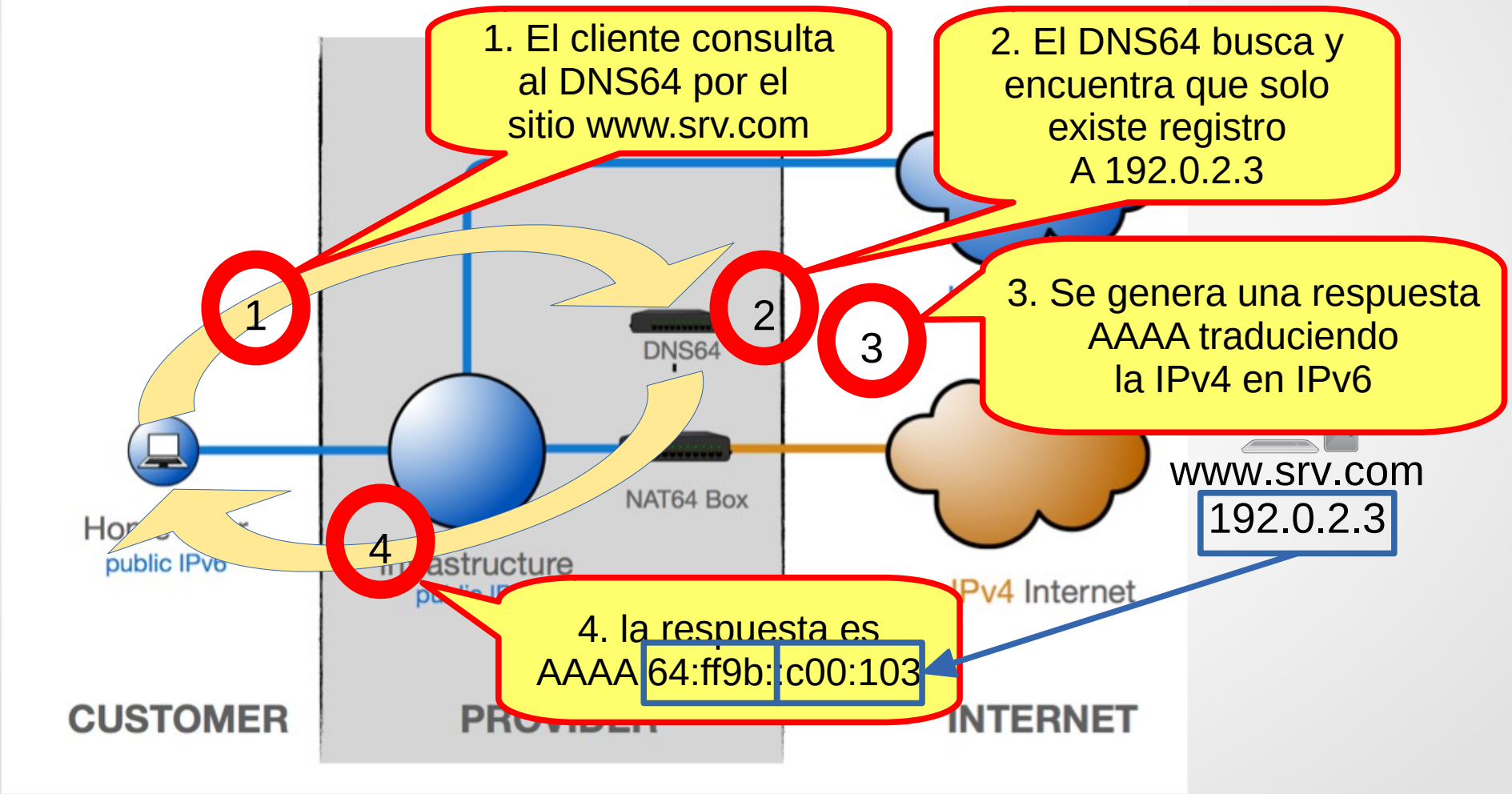
Mecanismos de transición: Traducción

- NAT64/DNS64



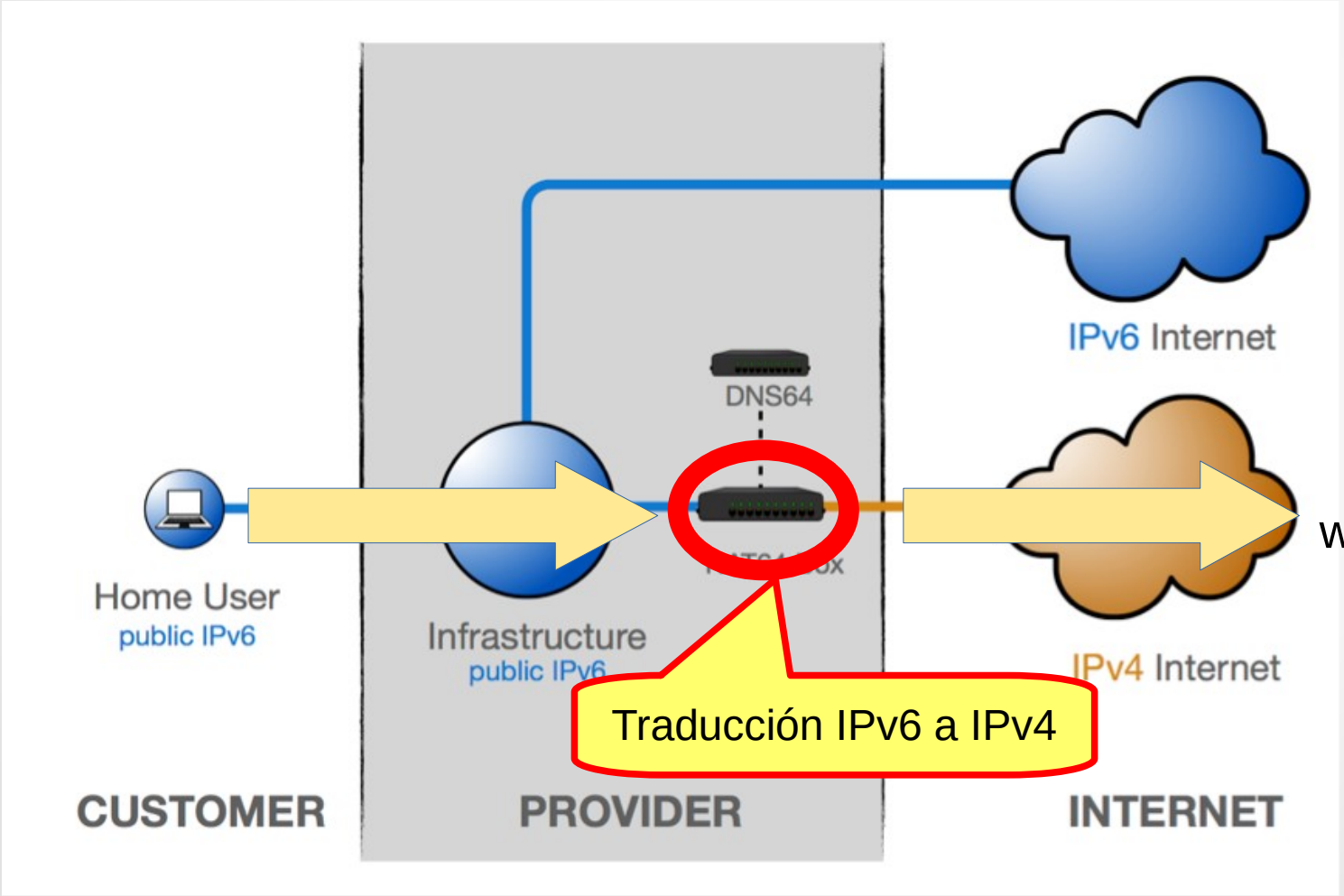
Mecanismos de transición: Traducción

- NAT64/DNS64



Mecanismos de transición: Traducción

- NAT64/DNS64



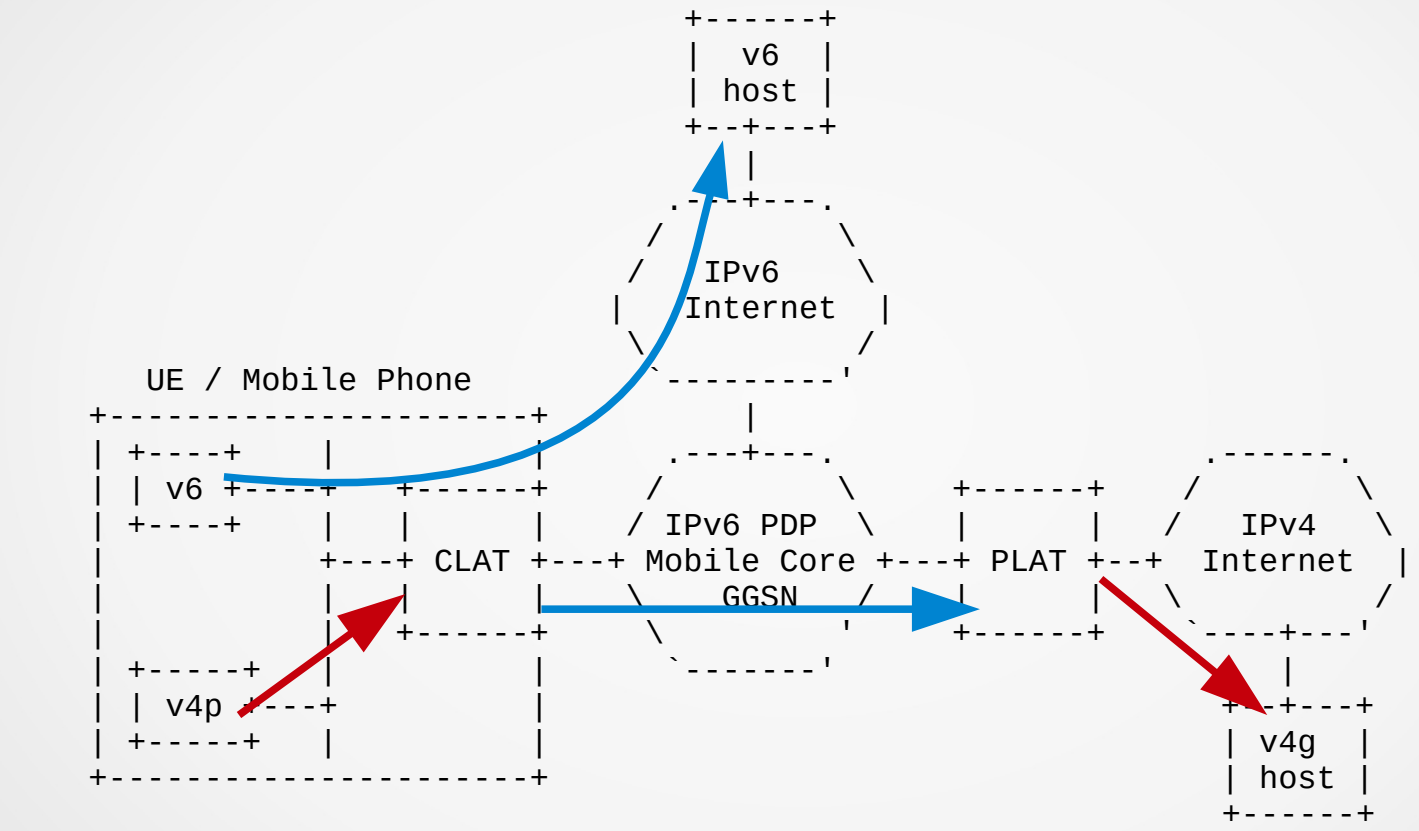
Mecanismos de transición: Traducción

- NAT64/DNS64 tiene varias limitaciones:
  - NAT64 solo se define para unicast TCP, UDP e ICMP
  - Problema con aplicaciones que embeben la IP (FTP, SIP)
  - Se necesitan nuevos dispositivos agregados a la red
  - No funciona si se usa la IP directamente, hay que pasar por el DNS

Mecanismos de transición: Traducción

- 464XLAT (RFC6877)
  - Se usa en los siguientes escenarios:
    - Móvil: una aplicación solo IPv4 en un móvil con conectividad IPv6
    - Fijo: el CPE tiene solo IPv6 pero conecta nodos IPv4 e IPv6
  - Solo soporta IPv4 en modo cliente-servidor cuando el servidor tiene una IPv4 global
  - Se basa en la técnica anterior, con una doble traducción, combinando un stateful NAT64 en el core y un stateless NAT64 en el borde
    - CLAT: Customer-side translator – traduce 1:1 una IPv4 privada en una IPv6 pública (en ambos sentidos)
    - PLAT: Provider-site translator – traduce N:1 direcciones IPv6 globales en direcciones IPv4 públicas (en ambos sentidos)

Mecanismos de transición: Traducción



Tráfico IPv6

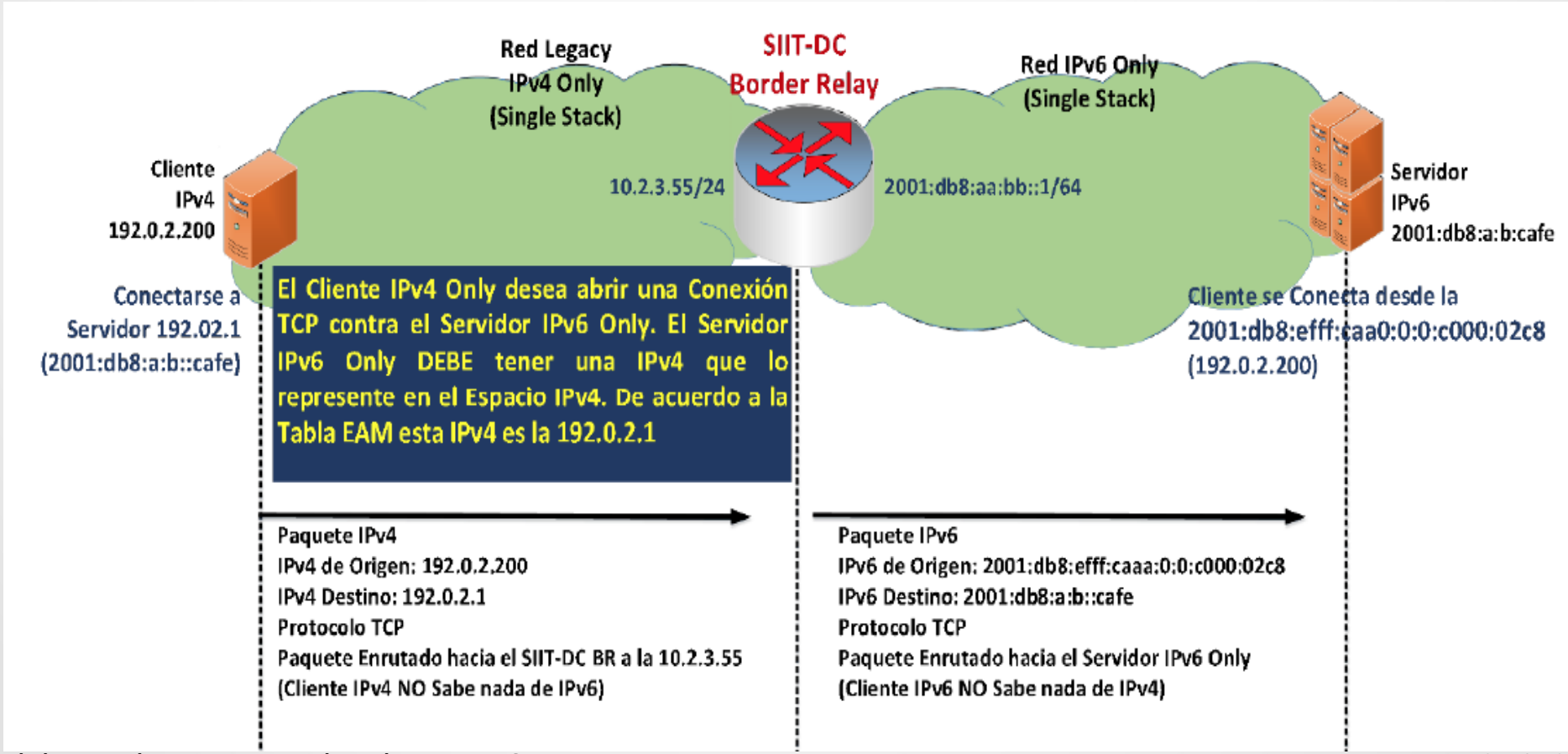
Tráfico IPv4

Mecanismos de transición: Traducción

- SIIT-DC: RFC7755
- Stateless IP/ICMP Translation Algorithm (SIIT) in an IPv6 Internet Data Center (IDC)
- Para el proveedor, no es conveniente la red dual-stack
  - Tiene doble gestión, enrutamiento, planificación, etc
  - No ahorra direcciones IPv4
- Aparece el SIIT-DC BR (Border Relay) que
  - opera en modo stateless
  - traduce direcciones IPv4 a/de IPv6 de forma 1:1
  - Usa una tabla EAM (explicit address mapping) (RFC6052)

Mecanismos de transición: Traducción

- SIIT-DC

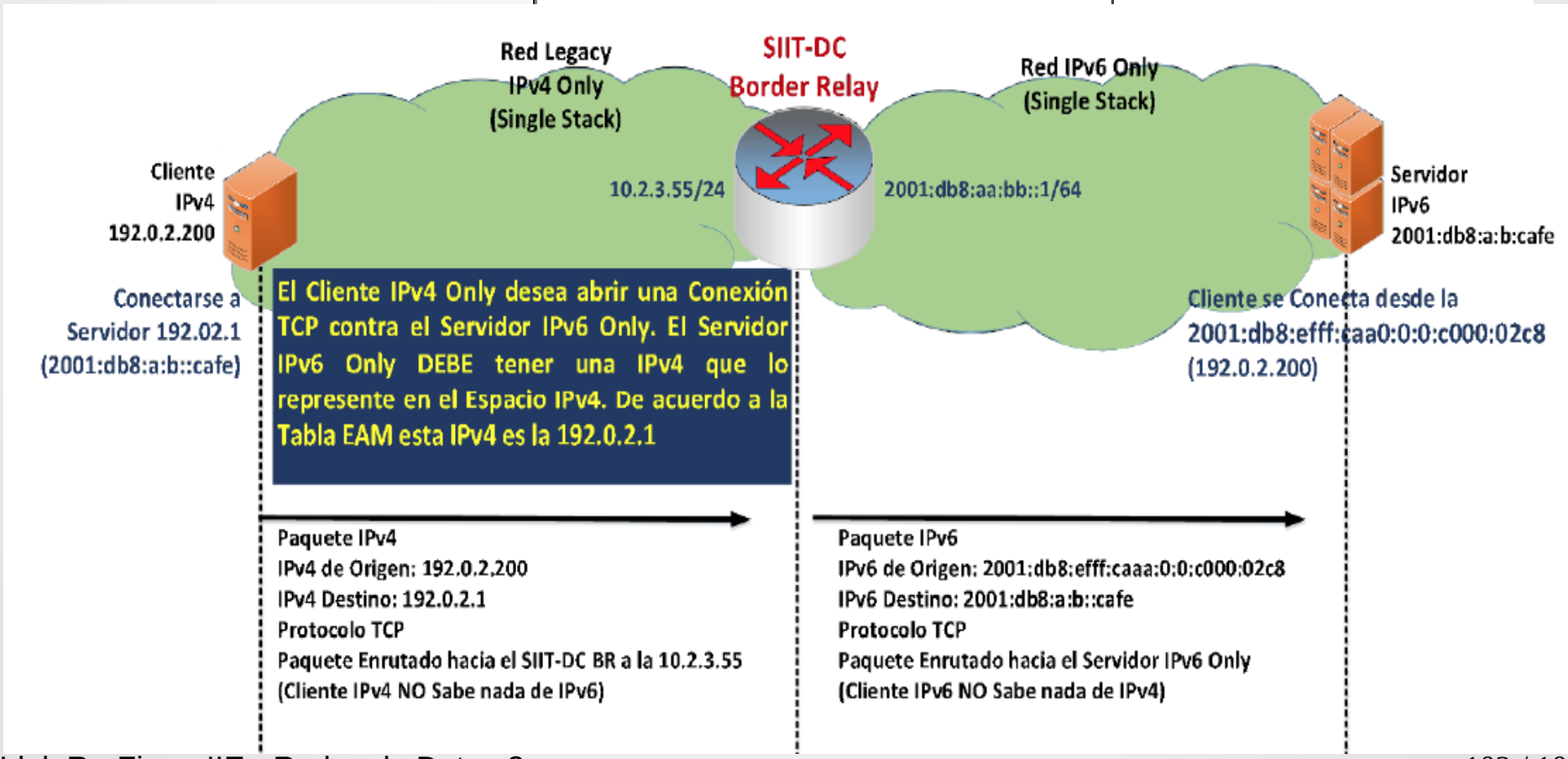


Mecanismos de

- SIIT-DC

SIIT-DC BR - Tabla EAM

Prefijo IPv4	Prefijo IPv6
192.0.2.1	2001:db8:a:b::cafe
192.0.2.2/32	2001:db8:cc:dd::ee33/128
192.0.2.16/28	2001:db8:cc35:cc35::/124
192.0.2.128/26	2001:db8:cafa::/64
192.0.2.192/28	2001:db8:efff:caa0::/96



Mecanismos de transición: Traducción

- SIIT-DC
- Ventajas:
  - Stateless (velocidad)
  - Los nodos IPv4 e IPv6 involucrados no tienen que hacer nada
- Desventajas
  - Problemas con la MTU si en ambos mundos es la habitual de 1500
  - Problemas con apps que embeben la IP en la capa de aplicación