Internet Protocol version 6

Departamento de Sistemas Telemáticos y Computación (GSyC)

gsyc-profes (arroba) gsyc.es

Marzo de 2012

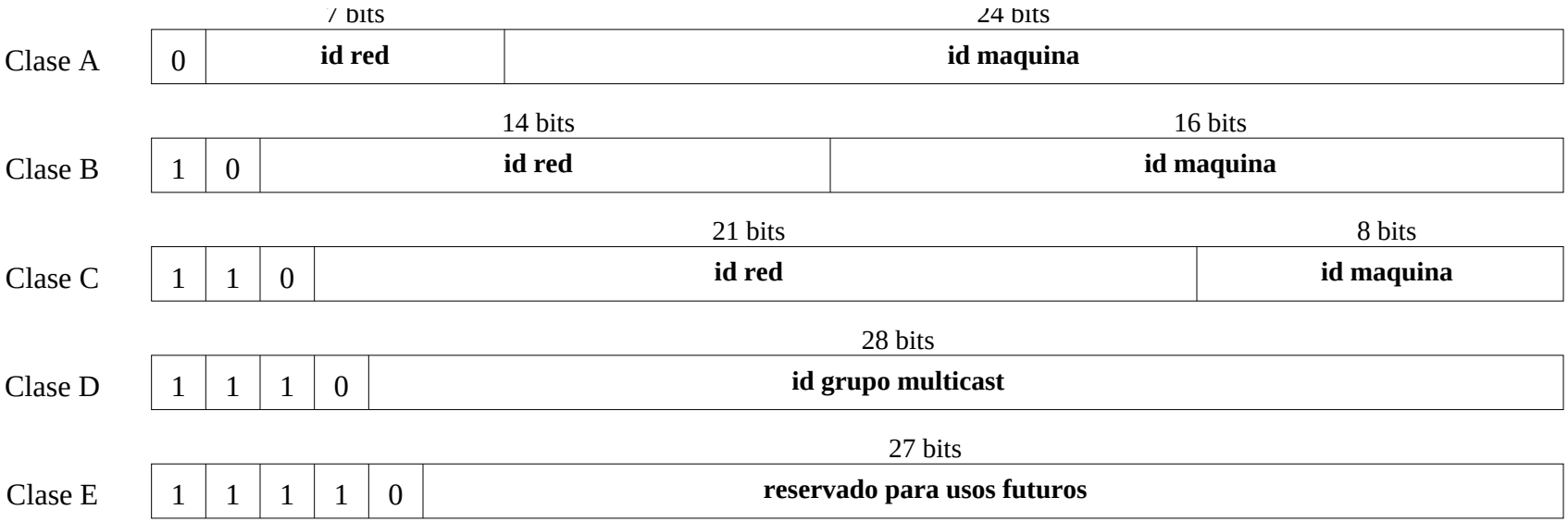
Contenidos

Contenidos

- ARPANET (año 1969), red predecesora de Internet. Empleaba protocolo NCP, *Network Control Program* (Año 1972). No confundir con Netword Control Protocol, protocolo de red por encima de PPP
- INTERNET (año 1983). Protocolo IPv4 tal y como lo conocemos hoy
- IPv4 no fue diseñado para ser *la* red mundial. Las direcciones se agotan

- Número de direcciones potenciales en IPv4: 4200 millones
- Población con acceso a Internet: 14 % (UNCTAD, año 2005)
- Población mundial: 6741 millones (año 2008)
  Pero norteamericanos (5 % población) tienen el 60 %
  Problema especialmente acuciante en Asia

El reparto de direcciones en IPv4 es ineficiente



Clase A:
$2^7 = 128$ redes de $2^{24} = 16777216$ máquinas
Clase B:
$2^{14} = 16384$ redes de $2^{16} = 65536$ máquinas
Clase C:
$2^{21} = 2097152$ redes de $2^8 = 256$ máquinas

- IPv6 (año 1998) emplea direcciones de 16 octetos. El resto es similar a IPv4, con mejoras, pero incompatible
- Admite 2^{128} direcciones (aproximadamente $3{,}4x10^{38}$) Magnitud comparable con
  - Moléculas de la superficie de tierra y océano
  - Granos de arena en el planeta
- Mal repartido, daría para unas 1500 direcciones/m^2

Algunas técnicas han aumentado la vida de IPv4 por encima de las previsiones

- CIDR *Classless Inter-Domain Routing* (RFC 1518, año 1993)
  Desaparecen las clases A, B, C, D, E
  El tamaño de la red es variable (no solo tres tamaños). Se indica explícitamente el número de bits del prefijo de red. Ej: 192.168.0.0/16
- NAT (*Network address translation*) permite compartir direcciones IP, pero tiene muchos inconvenientes
  - No es posible configurar automáticamente las conexiones que entran a la red privada (hay que *abrir puertos*)
  - Es necesario modificar direcciones dentro de cada datagrama. Obliga a conocer protocolos superiores. Si las direcciones están en la zona correspondiente a datos, es prácticamente imposible

Contenidos

- Direccionamiento: Direcciones de 128 bits, asignadas jerárquicamente
- Encaminamiento: jerárquico, agregación de rutas
- Prestaciones. Cabecera simple, alineada a 64 bits
- Versatilidad: Formato flexible de opciones
- Multicast: Obligatorio, control de ámbitos
- Seguridad: Soporta obligatoriamente autentificación y encriptado (IPsec)
- Autoconfiguración: Configuración automática
- Movilidad: Mejora la eficiencia y seguridad
- Multihoming: Facilita el cambio de proveedor de servicio
- Checksums: No se utilizan

Contenidos

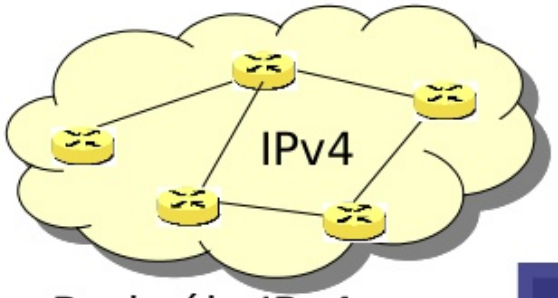
Transición a IPv6

- El 1 de enero de 1983 (flag day) se apagaron todas las máquinas con NCP y se encendieron con TCP/IP
- En 1983 había menos de 1000 máquinas, en la actualidad hay más de 1000 millones
- Transición compleja y gradual (en el nivel de red, no en las aplicaciones)
- El servicio requerido de niveles inferiores es prácticamente el mismo que en IPv4: Basta cambiar ARP
- El servicio ofrecido a niveles superiores tampoco difiere mucho
  - Una aplicación bien hecha requerirá pocos cambios y sencillos. Tal vez ninguno
  - Es necesario modificar DNS. Una respuesta de DNS puede ser dirección IPv4, IPv6 o ambas. El cliente decide qué usará
  - Es necesario modificar cualquier sitio donde se almacene una dirección

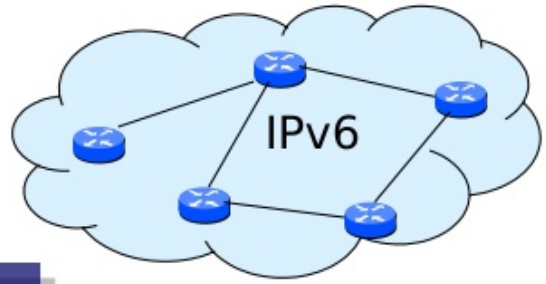
- Por medio de túneles, IPv6 se puede usar aunque no lo ofrezca nuestro ISP.
- Primer uso masivo: juegos olímpicos de Pekín 2008
- Todos los organismos del gobierno federal de Estados Unidos estaban obligados a usarlo desde desde junio de 2008
- Porcentaje de tráfico IPv6 en 2008: Menos del 1 %
- En febrero de 2011 IANA asignó los últimos bloques de direcciones IPv4 a un RIR (*Regional Internet Registry*).
- En primavera de 2012 se estima que los RIR agotarán sus bloques entre 2012 y 2014
- Primer test mundial masivo: *World IPv6 Day*, 8 de junio de 2011

Soporte de IPv6

- Linux: 1996 (experimental) 2005 (apto para producción)
- BSD: 2000 (apto para producción)
- Cisco IOS: 2001
- Microsoft Windows: 1998 (experimental). Windows XP SP1 (2002), Windows Server 2003 (aptos para producción), Windows Vista (2007) activo por omisión,
- MacOS X v10.02 Jaguar (2002) Apple Mac OS X v10.3 Panther (2003) (activo por omisión)

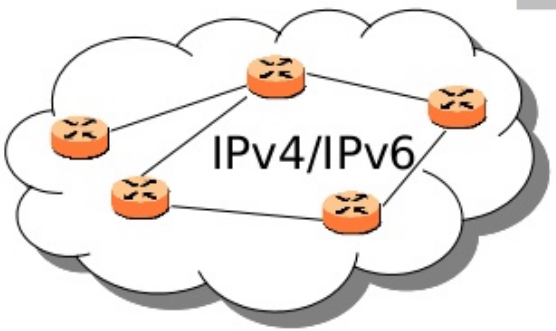


Red sólo IPv4

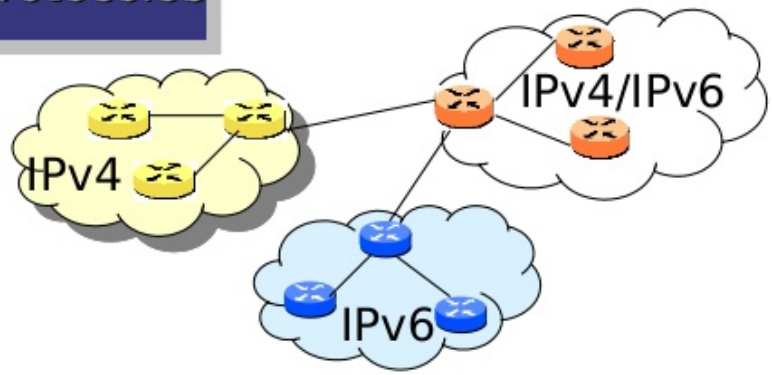


Red sólo IPv6

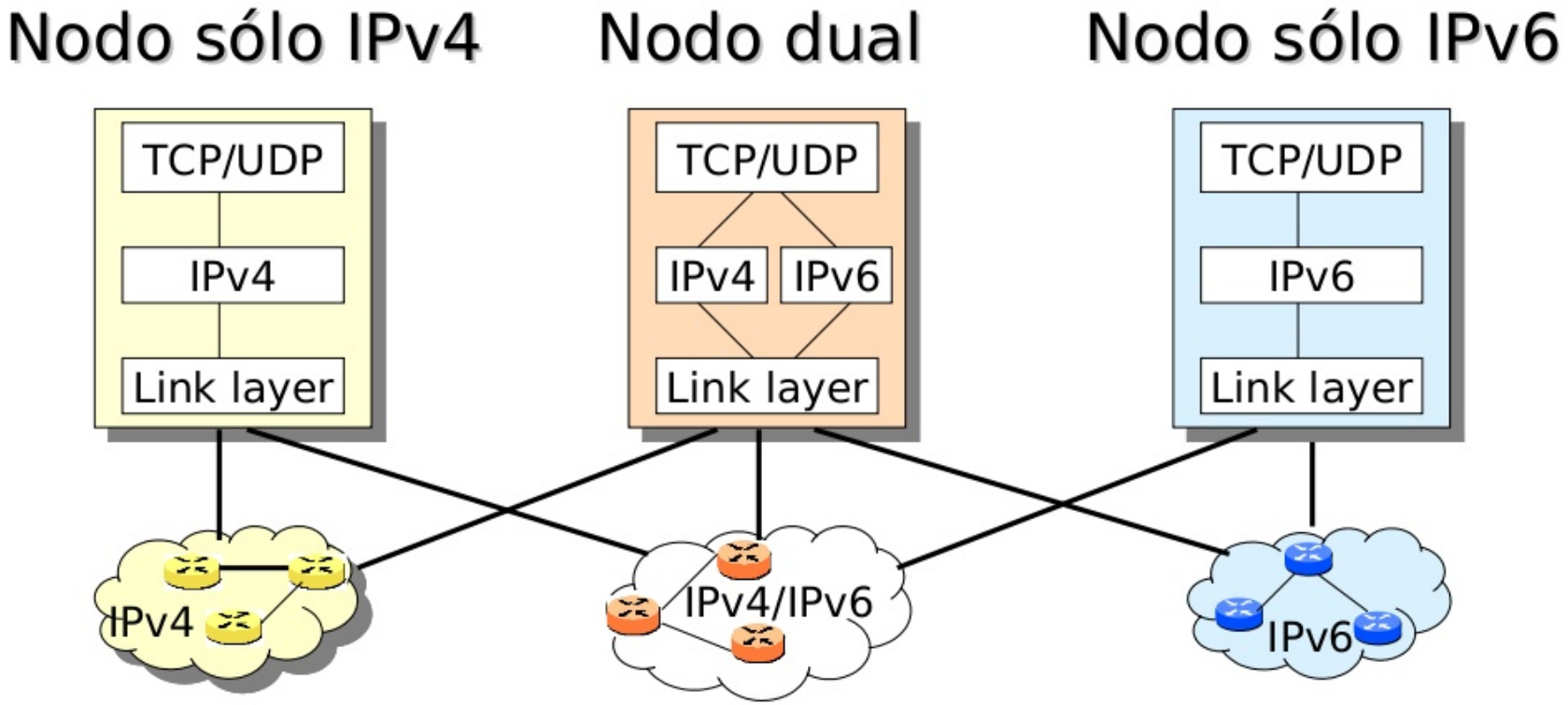
Mecanismos de transición:
Túneles
Traducción de protocolos



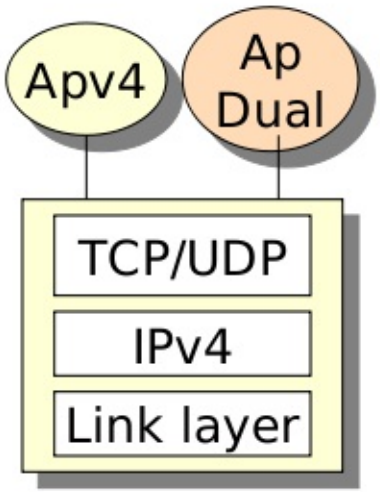
Red dual

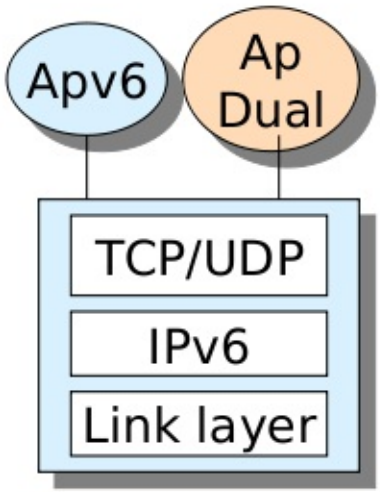


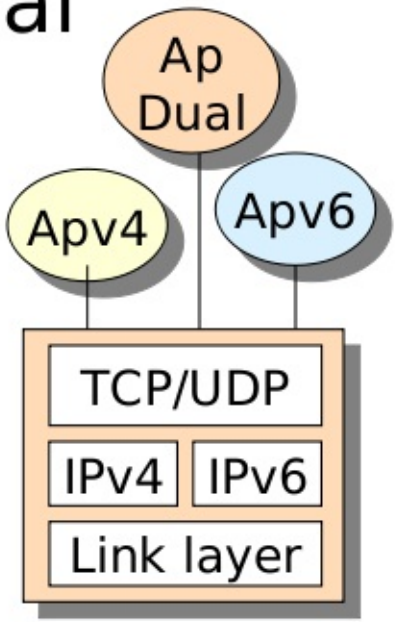
Red heterogénea


Nodo sólo IPv4
Nodo dual
Nodo sólo IPv6
TCP/UDP
IPv4
Link layer
TCP/UDP
IPv4
IPv6
Link layer
TCP/UDP
IPv6
Link layer
IPv4
IPv4/IPv6
IPv6

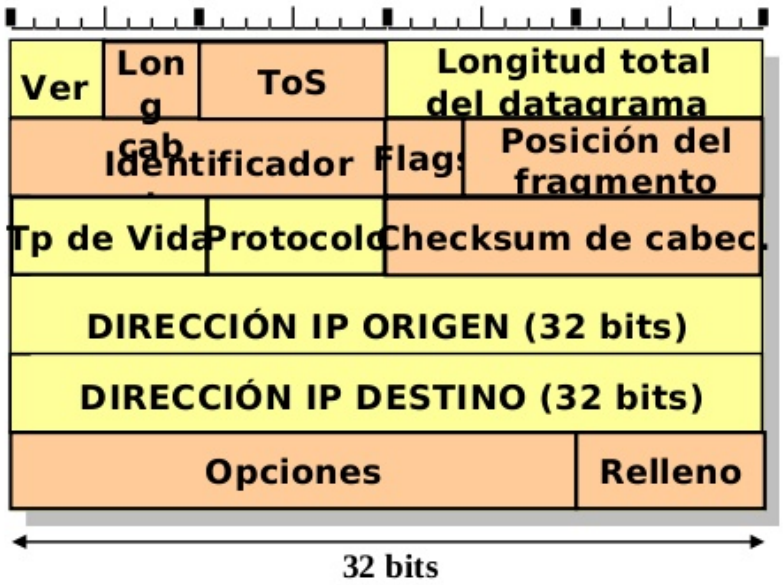
- Aplicaciones sólo IPv4 – Apv4
- Aplicaciones sólo IPv6 – Apv6
- Aplicaciones duales – Ap Dual



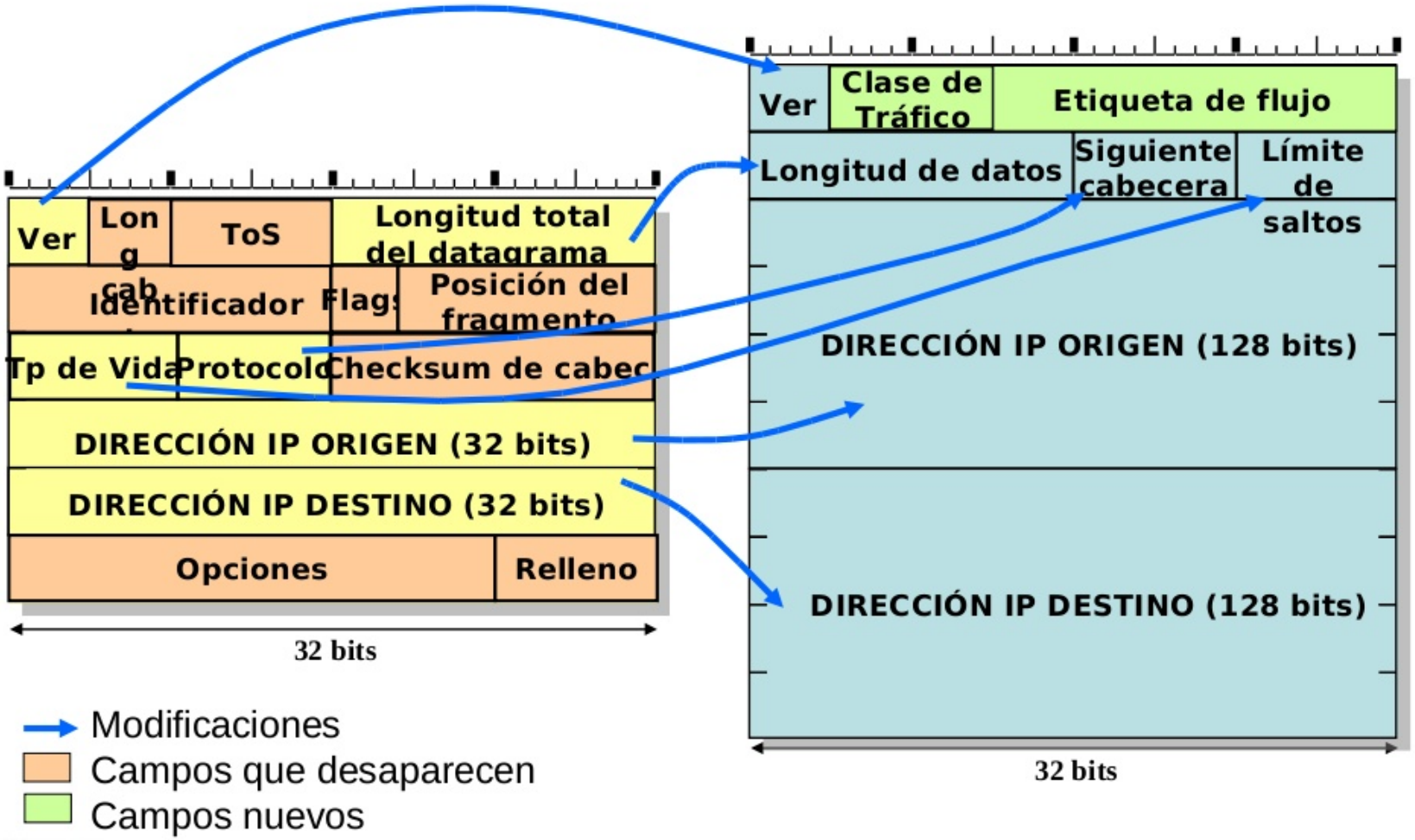




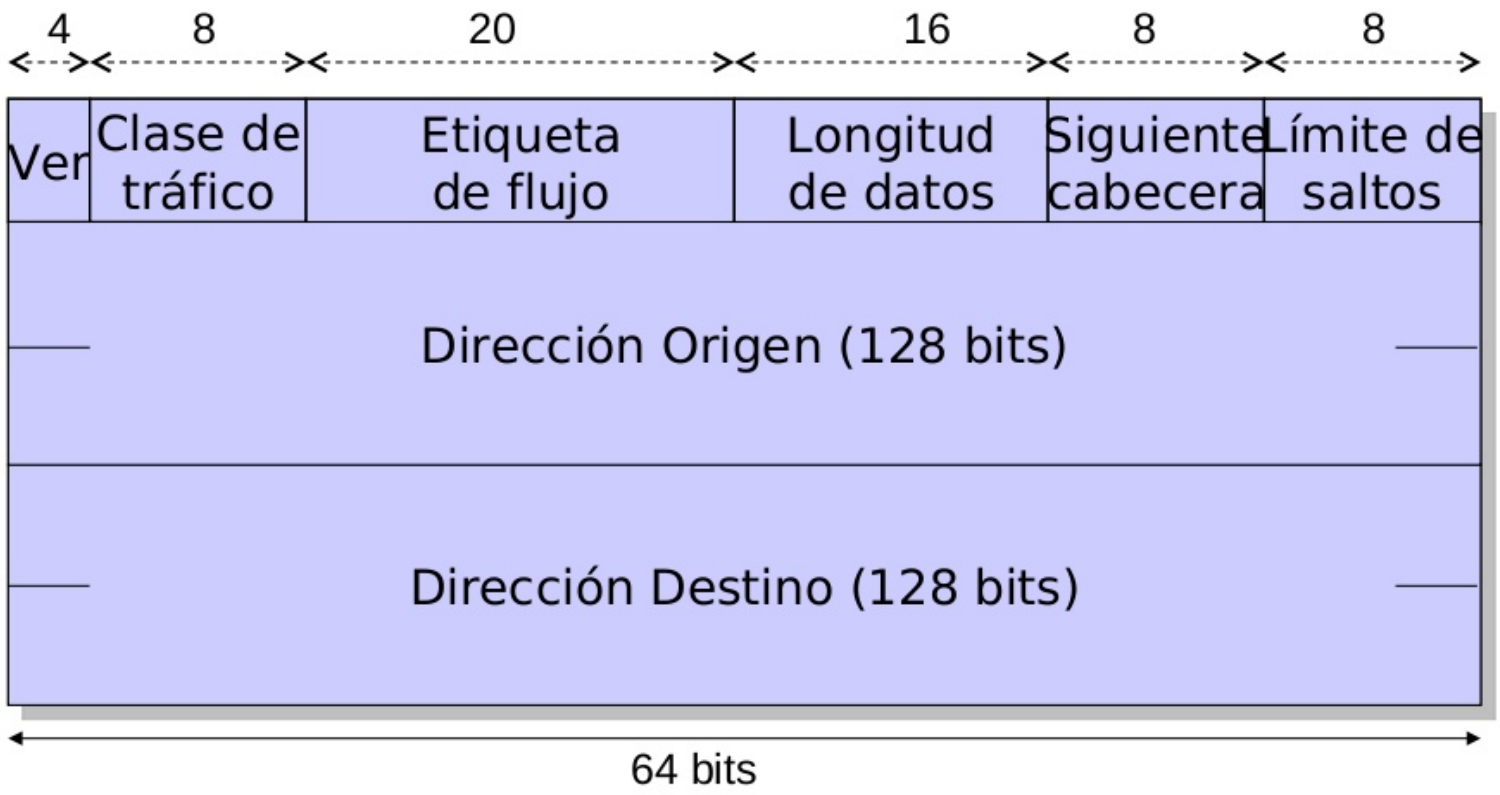
Contenidos



Campos que desaparecen


Ver
Long cab
ToS
Longitud total del datagrama
Identificador
Flags
Posición del fragmento
Tp de Vida
Protocolo
Checksum de cabec
DIRECCIÓN IP ORIGEN (32 bits)
DIRECCIÓN IP DESTINO (32 bits)
Opciones
Relleno
32 bits
Ver
Clase de Tráfico
Etiqueta de flujo
Longitud de datos
Siguiente cabecera
Límite de saltos
DIRECCIÓN IP ORIGEN (128 bits)
DIRECCIÓN IP DESTINO (128 bits)
32 bits
Modificaciones
Campos que desaparecen
Campos nuevos

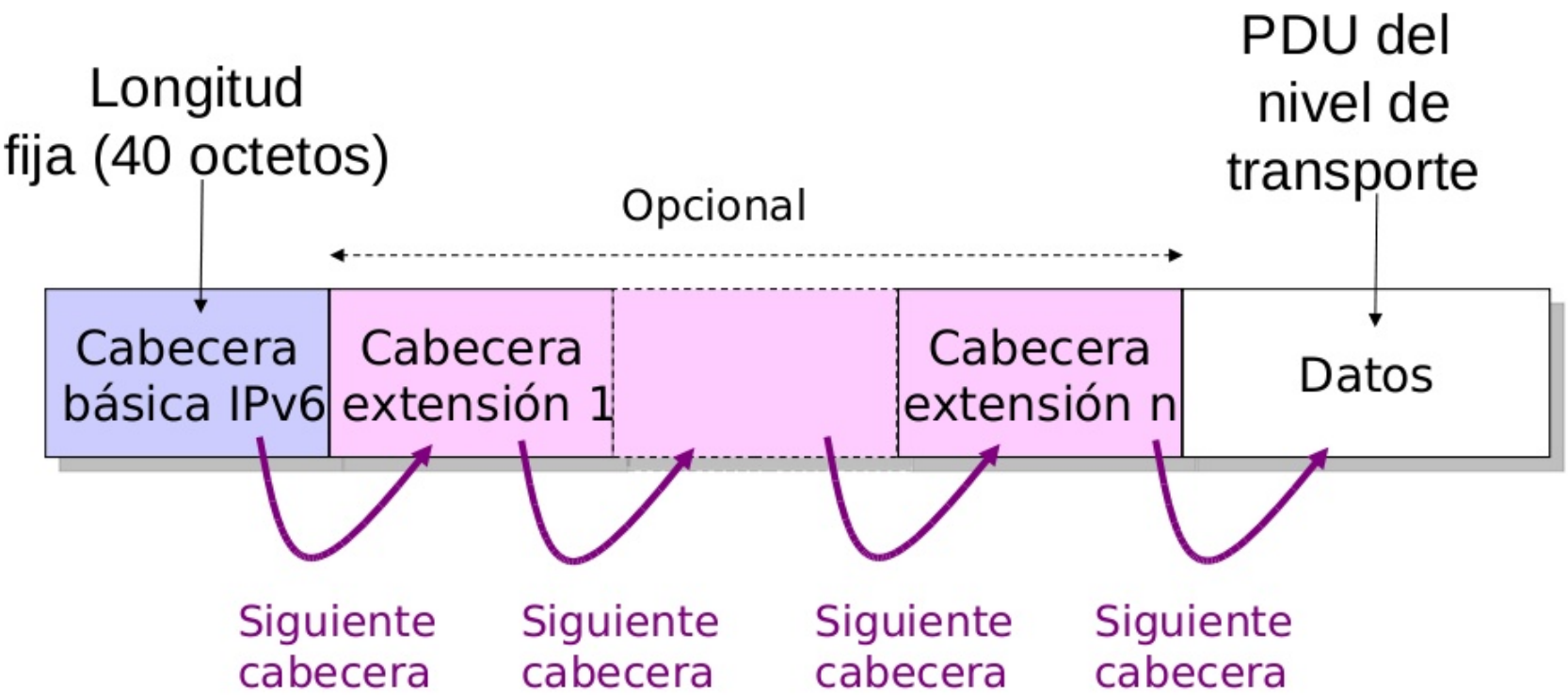
6 campos + 2 direcciones => LONGITUD FIJA (40 octetos)



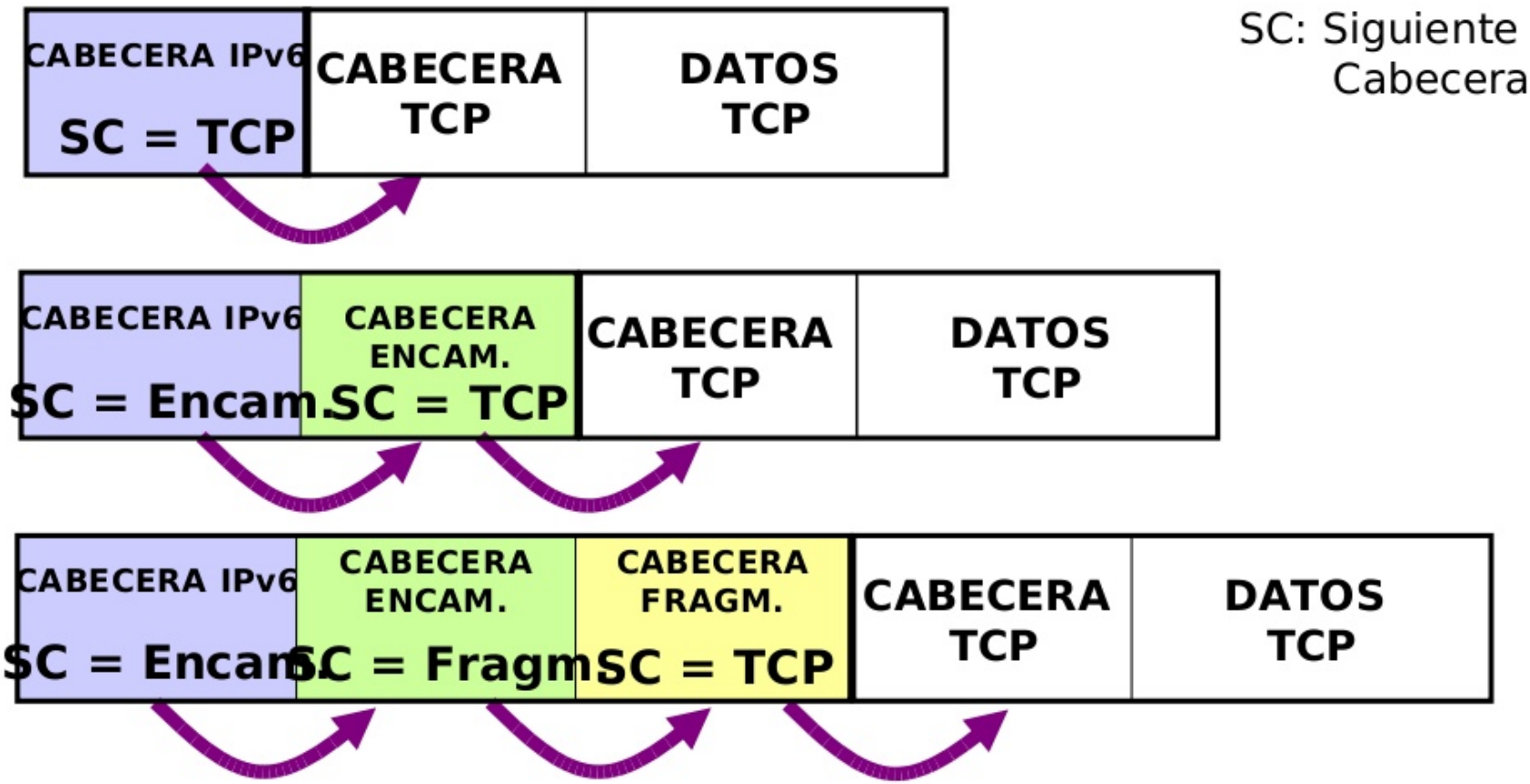
Opciones

- El uso de opciones tiene impacto muy negativo en el rendimiento
  - En algunas arquitecturas, un datagrama sin opciones lo procesa la *electrónica* del router, uno con opciones llega a la CPU principal
- En IPv4 es necesario leer el datagrama entero buscando opciones
- En IPv6 las opciones se ordenan
  - Las que todo router debe leer, van antes
  - Las que solo leen los extremos, van después

- En IPv4 las opciones está prefijadas
- En IPv6 las opciones son flexibles: Campo *siguiente cabecera*
  - El primer byte indica el tipo de la siguiente cabecera
  - El segundo, el tamaño de esa cabecera (nº de bloques de 8 octetos)



PDU: Protocol Data Unit


CABECERA IPv6
SC = TCP
CABECERA TCP
DATOS TCP
SC: Siguiente Cabecera
CABECERA IPv6
SC = Encam.
CABECERA ENCAM.
SC = TCP
CABECERA TCP
DATOS TCP
CABECERA IPv6
SC = Encam.
CABECERA ENCAM.
SC = Fragm
CABECERA FRAGM.
SC = TCP
CABECERA TCP
DATOS TCP

Cabecera de encaminamiento

- El diseño original de IPv6 incluye *routing header*. Permite hacer encaminamiento en origen. Pensado para la depuración
- Su procesamiento es muy costoso
- Resulta ser peligroso
  - Permiten a atacante conocer estructura de red
  - Permiten evitar cortafuegos
  - Permiten ataques por denegación de servicios
- En el año 2007 se elimina esta opción, RFC 5095. Los paquetes con esta opción deben descartarse

Cabecera de flujo

- Útil para el tráfico de tiempo real
- No hace falta procesar todo el datagrama, basta leer el origen y el identificador de flujo
- Todos los datagramas del mismo flujo se tramitan de la misma manera
- Asunto aún no completamente maduro

Contenidos

Direcciones IPv4

- 32 bits. Notación decimal: a.b.c.d
- Tipos de dirección:
  - Unicast
  - Multicast
  - Broadcast

Direcciones IPv6

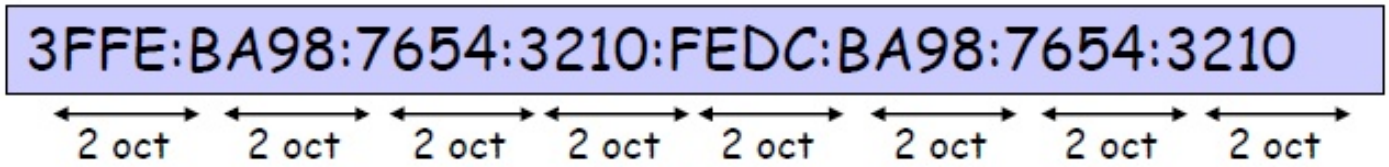
- 128 bits. Notación hexadecimal: xx:xx:xx:xx:xx:xx:xx:xx
- Tipos de dirección:
  - Unicast
    - Globales
    - Locales de enlace
    - Loopback
    - Site local (Obsoletas)
  - Multicast
  - Anycast

Direcciones link local

Las direcciones *Locales de enlace / link local* solamente son válidas en un segmento de red

- Permiten que máquinas contiguas puedan intercambiar tráfico
  - Aunque no tengan dirección IP pública
  - Aunque tampoco tengan ni siquiera dirección IP privada asignada por un servidor de DHCP
- Las máquinas se auto-organizan para usar direcciones en un rango especial
- Este tipo de direcciones están previstas en IPv6
- En el diseño original de IPv4, no existen. Pero se añaden posteriormente
  (*Zero configuration networking*, RFC 3927, año 2005)
  Red 169.254.0.0/16

- 128 bits = se agrupan los octetos de 2 en 2, se separan por ":" y se se representan en hexadecimal:



- Simplificación:

3FFE:1111:0000:0000:0008:0800:200C:417A

3FFE:1111:0:0:8:800:200C:417A

3FFE:1111::8:800:200C:417A

"::" Representa múltiples grupos consecutivos de 16 bits a 0.
Sólo puede usarse una vez en una dirección IPv6

- Representación de prefijos IPv6:
  dirección IPv6/longitud-prefijo

Direcciones IPv6

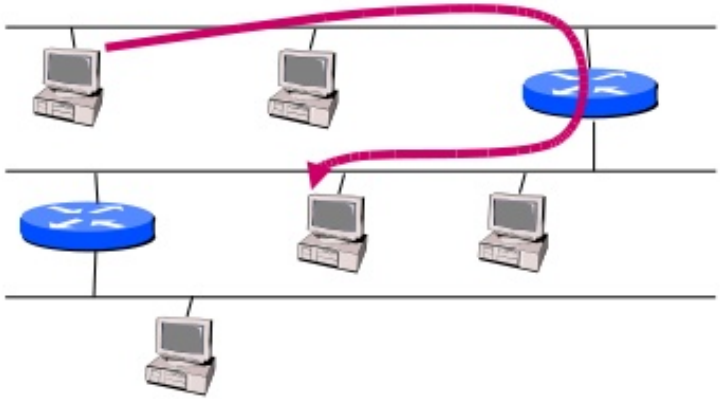
Dirección IPv6
=128 bits
=16 bytes
= 8 *bloques* de 2 bytes separados por ’ : ’
= 8 *bloques* de 4 nibbles separados por ’ : ’

nibble = medio byte = 1 dígito hexadecimal
ejemplo: 2001:db8:fedc:8000:c3a0:3b77:1:80

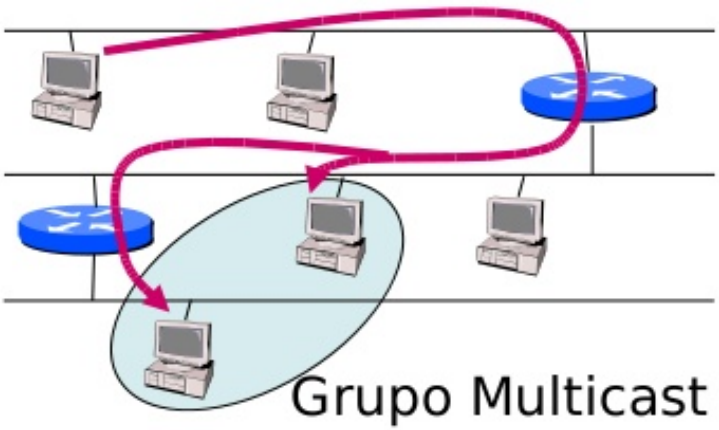
Direcciones Site local

- La definición original de IPv6 incluía direcciones *site local*, pensadas para usarse dentro de una única *organización*
- El concepto *organización* es ambiguo. Fuente de problemas
- La RFC 3879 (año 2004) elimina estas direcciones. Pasan a ser obsoletas

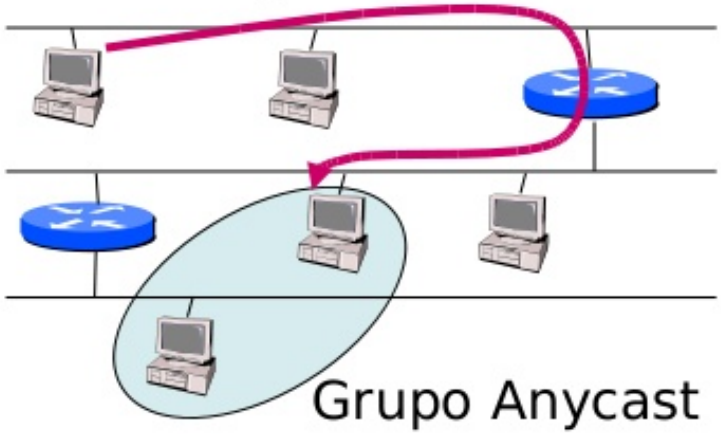
Unicast



Multicast



Anycast



Anycast

- Las direcciones anycast tienen un rango especial
- Está orientado a servicios. Varias máquinas comparten la misma dirección anycast, ofreciendo siempre el mismo servicio
  El datagrama llega solo a una máquina, elegible mediante diversos criterios
  - Proximidad
  - Equilibrio de carga
  - Redundancia
- Dos datagramas enviados a la misma dirección anycast pueden llegar a máquinas ditintas.

En IPv4 se emplea *shared unicast address*. Por ejemplo en los servidores raiz de dns. Más *truculento*. Varias máquinas comparten dirección unicast sin que lo perciba el nivel de red

Multiplicidad de direcciones

- En IPv4 cada interfaz tiene exactamente una dirección IP
- Con el tiempo se ha ido viendo la conveniencia de que un interfaz tenga varias direcciones
  - Cada sistema operativo lo ha ido resolviendo de diferentes formas, similares, no estándar: *alias*, *subinterfaces*, *interfaces virtuales*, *interfaces lógicos*
  - Pero siempre con una dirección *primaria*
- En IPv6, cada interfaz tiene varias direcciones. Las aplicaciones deben tenerlo en cuenta

El hecho de que un interfaz tenga varias direcciones

- En la recepción no supone ningún inconveniente. El interfaz acepta datagramas dirigido a cualquiera de sus direcciones
- Para el envío, el nodo conocerá n direcciones del interfaz origen y n direcciones del interfaz destinatario.
  Debe elegir una dirección origen y una dirección destino de cada para el datagrama
  - Para esta elección hay un algoritmo determinista, descrito en RFC3484
  - El algoritmo es de cierta complejidad. Para un administrador, en general es recomendable considerarlo una *caja negra* y no intentar variar el comportamiento por defecto.

Elección de la dirección del destino

Según lo descrito en la RFC3484, se crea una lista ordenada de direcciones para el destinatario. Se intenta usar cada una de ellas, secuencialmente

```
Rule 1:  Prefer same address.
Rule 2:  Prefer appropriate scope.
Rule 3:  Avoid deprecated addresses.
Rule 4:  Prefer home addresses.
Rule 5:  Prefer outgoing interface.
Rule 6:  Prefer matching label.
Rule 7:  Prefer public addresses.
Rule 8:  Use longest matching prefix.
```

Elección de la dirección del origen

Para cada dirección del destino, se elige (exactamente) una dirección origen

```
Rule 1:  Avoid unusable destinations.
Rule 2:  Prefer matching scope.
Rule 3:  Avoid deprecated addresses.
Rule 4:  Prefer home addresses.
Rule 5:  Prefer matching label.
Rule 6:  Prefer higher precedence.
Rule 7:  Prefer native transport.
Rule 8:  Prefer smaller scope.
Rule 9:  Use longest matching prefix.
Rule 10: Otherwise, leave the order unchanged
```

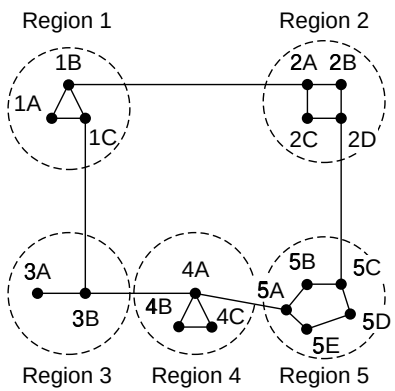
DNS

Es normal y razonable que un mismo nombre tenga varias entradas, IPv4 y/o IPv6

```
www.ejemplo.com          A     212.128.240.25
                         AAAA  2001:db8:aaaa:bbbb:80::80
                         AAAA  2001:db8:aaaa:cccc:80::80

www.ip4.ejemplo.com      A     212.128.240.25
www.ip6.ejemplo.com      AAAA  2001:db8:aaaa:bbbb:80::80
www.ip6.ejemplo.com      AAAA  2001:db8:aaaa:cccc:80::80
```

Máscaras de red



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Fig. 5-17. Hierarchical routing.

- IPv4, IPv6 emplean encaminamiento jerárquico: los routers tienen entradas para redes, no para máquinas individuales
- En este protocolo imaginario, dada una dirección, reconocemos el prefijo de red porque emplea un número, y el identificador de interfaz porque emplea una letra

Máscaras de red (IPv4)

- Dada una dirección, la máscara de red separa el prefijo de red del identificador de interfaz
- En IPv4, el tamaño de las máscaras es variable, lo cual aporta flexibilidad pero también complejidad

Ejemplo: Deseamos enviar datagrama a 156.35.59.5

- Antes de CIDR, al reconocer que la dirección empieza por 10 se sabía que es de clase B y por tanto la máscara son 16 bits
- Desde el año 1993, es necesario que los routers sepan que esta red en particular tiene una máscara de 16 bits

```
     156 .       35 .       59 .        5   Dirección (Dec)
10011100 . 00100011 . 00111011 . 00000101   Dirección (Bin)

11111111 . 11111111 . 00000000 . 00000000   Máscara Clase B
-----------------------------------------
     156 .       35 .        0 .        0   Univ. Oviedo
```

Como una red puede resultar muy grande, en IPv4 pueden hacerse subredes. También de tamaño variable, aportando flexibilidad y complejidad

La máscara de subred

- Se aplica dentro de la organización
- Es inexistente para el resto de Internet

```
     156 .       35 .       59 .        5   Dirección (Dec)
10011100 . 00100011 . 00111011 . 00000101   Dirección (Bin)

11111111 . 11111111 . 00000000 . 00000000   (Máscara Clase B)
11111111 . 11111111 . 11111111 . 00000000   Máscara de Subred
-------------------------------------------
     156 .       35 .       59 .        0   Facultad Medicina
```

Máscaras de red (IPv6)

En direcciones unicast, siempre se emplean máscaras de 64 bits.
Esto simplifica mucho el encaminamiento

```
xxxx:xxxx:xxxx:yyyy   :   zzzz:zzzz:zzzz:zzzz
<----------------->       <----------------->
prefijo de red          identificador de interfaz
```

xx: Prefijo global de encaminamiento. Cada organismo tendrá uno
yy: Identificador de subred. Cada organismo puede distribuirlo como desee
zz: Identificador de interfaz

En IPv6, las ventajas que tenían los afortunados poseedores de una red de clase B, están disponibles para todo el mundo

Contenidos

ICMPv6: Internet Control Message Protocol Version 6

- ICMP para IPv4 notifica errores de servicio o máquina no disponible. Permite ping
- ICMPv6 incluye, adicionalmente
  - MLD *Multicast Listener Discovery*
  - ND *Neighbor Discovery*
  - PMTUD *Path Maximum Transmission Unit Discovery*

  En IPv4 la funcionalidad análoga a esta la hacía otros protocolos (IGMP, ARP)

Multicast Listener Discovery

El multicast es un método de envio de información a varios destinatarios buscando máxima eficiencia. Solo se duplican paquetes cuando es imprescindible

- En IPv4 esta funcionalidad la ofrecía IGMP *Internet Group Management Protocol*. Muy poco soportado, actualmente se emplean otras cosas:
  - No es raro crear n conexiones para n destinatarios
  - Técnicas de distribución de carga
  - Técnicas P2P (*peer to peer*)
- MLD es similar a IGMP. Se beneficia de los tipos de dirección de IPv6

- Unicast
  El interfaz acepta las tramas para 1 dirección MAC (la suya) y descarta el resto
- Multicast
  El interfaz se une a un grupo de direcciones MAC. Acepta las tramas para n direcciones y descarta el resto. Un router en el segmento de red se encarga de anunciar al resto de routers que tiene estaciones inscritas en la dirección multicast
- Broadcast
  El interfaz acepta todas las tramas con una dirección MAC de broadcast.

- Considerando solamente el nivel físico, cuando el medio es compartido (Bluetooth, Ethernet, 802.11) no existe unicast ni multicast, todo es broadcast, todos los interfaces reciben todo
- Considerando niveles superiores, sí existe:
  Soy un host. Recibo un datagrama que no me incumbe (por ejemplo solicitud de servicio que no ofrezco)
  - Llega en una trama con una dirección unicast o multicast que no es mía. La trama se descarta inmediatamente (típicamente lo hace la electrónica de la tarjeta)
  - Llega en una trama con dirección broadcast. El mensaje se procesa, recorre la pila, y es descartado en niveles altos

- Lo que en IPv4 se hacía mediante broadcast, en IPv6 se hace mediante multicast
- Dos direcciones multicast especialmente útiles:

```
ff02::1        all-nodes link-local multicast group
ff02::2        all-routers link-local multicast group
```

Neighbor Discovery

La última versión (año 2007) está descrita en RFC 4861. El protocolo Neighbor Discovery se usa para

- Resolver direcciones de red
- Descubrir routers
- Autoconfigurar direcciones
- Detectar direcciones duplicadas

Definiciones:

- Nodo: Dispositivo que procesa IPv6
- Router: Nodo que, cuando recibe un datagrama que no es para él, lo reenvía al destinatario
- Host: Nodo que no es router

Resolución de direcciones de red

Pregunto a todo mi segmento de red ¿cuál es la dirección MAC de la dirección de red xxxx:xxxx:xxxx:yyyy:zzzz:zzzz:zzzz:zzz?

IPv4

- Protocolo ARP. Envío la pregunta a la dirección de broadcast.

IPv6

- El interfaz de nivel de enlace por la que pregunto se habrá apuntado a una dirección multicast que contiene los últimos 24 bits de su dirección de red (zzzz:zzzz:zzzz)
- Envío la pregunta a esta dirección multicast (zzzz:zzzz:zzzz) (Neighbor Solicitation message)
- Me devuelven Neighbor Advertisement Message

- Los routers envían periódicamente una baliza (*beacon, router advertisement*) anunciando su presencia, parametros de configuración, prefijo de red...
  - La baliza se puede solicitar explícitamente (*router solicitation*)
  - No es nececesario configurar máscara de red, ni manualmente ni mediante DHCP
  - No hace falta que los hosts consulten su tabla de encaminamiento, pueden obtener la información del router
  - Puede cambiar el ISP: el router anuncia nuevo prefijo de red, se mantiene la parte de la dirección correspondiente al host
- Las estaciones envían mensajes *neighbor advertisement*
  - Bien espontáneamente, bien respondiendo a un (*neighbor solicitation*)
  - Esto permite conocer vecindario, resolver direcciones, detectar direcciones duplicadas...

Configuración

- *stateful*. DHCP para ipv6. Alguien me da dirección. Hace falta alguien. Ese alguien conoce mi dirección
  - Más control
- *staless*. Del servidor solo obtengo algunos parametros, fundamentalmente el prefijo de red. Completo la dirección con mi dirección MAC o con valor aleatorio. No necesito a nadie
  - Más sencillo

El router puede

- Indicar que no existe DHCP
- Obligar a usar DHCP
- Indicar que DHCP es opcional

Problemas de DHCP (IPv4)

- Trabaja en nivel de enlace. El tráfico no se puede encaminar normalmente. Es necesario un servidor (muchas veces un relay) en cada enlace
- Normalmente solo hay 1 servidor en cada enlace. Es posible usar varios servidores (p.e. buscando redundancia), pero incrementado la complejidad
  - Los servidores deben coordinarse
  - O bien pueden repartir rangos de direcciones diferentes (un inconveniente cuando las direcciones son escasas)
- Los servidores necesitan mantener estado (recordar qué dirección IP han asignada a qué dirección MAC)
- Un servidor DHCP incorrecto puede hacer mucho daño (en IPv4, un interfaz tiene una única dirección, si es incorrecta, queda incomunicado)

Autoconfiguración

En IPv6, siempre que un host activa un interfaz

- Elige un identificador de interfaz, normalmente derivado de la dirección MAC
- Crea una dirección *link-local* añadiendo prefijo fe80::/64
- Hace detección de duplicados

Adicionalmente, cuando se usa autoconfiguración

- El host envía a todos los routers un *Router Solicitation* (RS) Todos los routers responden *solicited Router Advertisements* (RA), indicando prefijos de red y si ofrecen servicio de encaminamiento
- Para cada prefijo recibido
  - El host concatena prefijo y su propia MAC. Añade esta dirección a la lista de direcciones del interfaz
  - El host permanece a la escucha de *unsolicited router advertisements*, con el que cada router puede actualizar su información

Estados de una dirección

- Tentativo
- Duplicado
- Válido
  - Preferido
  - Obsoleto
- Inválido

Ventajas de la autoconfiguración

- Simplifican el reparto de direcciones
- La redundancia es trivial
- Los routers no tienen estado
- Una dirección incorrecta solo es una dirección incorrecta
- La única coordinación que necesitan los routers es anunciar prefijos distintos
- Es relativamente sencillo cambiar todo el esquema de direcciones de una red

Se puede desactivar la autoconfiguración, pero en general no es recomendable

Inconvenientes de la autoconfiguración

- Nadie conoce la dirección empleada por el host
  - Menos control en la red
  - No es posible acceder remotamente a esa máquina (aceptable para el típico cliente Windows, no para un servidor, o para un cliente Unix)

Soluciones

- No usar solo autoconfiguración, usar también DHCP
- Hacer que el host comunica su dirección al servidor de DNS. (En 2007 no estaba estandarizado, solo hay soluciones experimentales)

DHCP sin estado

En IPv4, DHCP proporciona

1. Dirección IP
2. Máscara de red
3. Dirección del Router
4. Dirección de otros servidores: DNS, NTP, ...

En IPv6

1. Dirección IP: puede proporcionarla o no
2. Máscara de red: No proporciona, no son necesarias
3. Dirección del Router: No proporciona, los router se auncian ellos mismos
4. Dirección de otros servidores: DNS, NTP, ...
   - Esto sigue siendo necesario, aún empleando autoconfiguración
   - Se denomina *DHCP sin estado*

Detección de direcciones duplicadas

- Similar a neighbor solicitation - neighbor advertisement
  Pero en el remite no se pone la dirección sin confirmar (no sabemos si es válida), sino :: (unspecified address)
- La respuesta va a ff02::1 (todos los nodos del segmento de red)

Problema (posible aunque improbable)

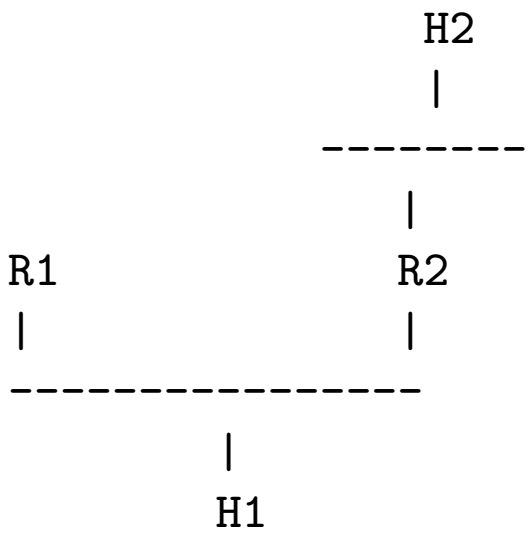
1. Elijo una dirección, que resulta estar ocupada
2. Pregunto, pero el dueño no está online
3. El dueño despierta ¿qué pasa ahora?

Solución:

1. La dirección ahora es mía
2. Cuando es necesario que una dirección pertenezca siempre a la misma máquina, se toma un rango especial, diferente, que nunca se autoconfigura

Redirect Protocol

- En cada enlace puede haber varios routers (p.e. R_1, R_2)
- Un host (p.e. H_1) elegirá uno cualquiera, indistintamente
- Si para enviar datagrama a H_2 elige R_1 (que es subóptimo), R_1 encaminará este datagrama, pero mediante un mensaje ICMP Redirect, notificará a H_1 que en lo sucesivo emplee R_2



Solo los hosts aceptan ICMPv6 redirect, sería muy peligroso que lo hiciera un router

Fragmentación de datagramas

Buscamos responder a

- ¿Qué tamaño damos al paquete?
  - El tamaño original del paquete (sin fragmentar) no lo decide IP, sino el *packetization protocol*: TCP o algún protocolo por encima de UDP
- Si el datagrama es mayor de lo admitido en algún segmento de red ¿Lo fragmentamos a mitad de camino? ¿O lo fragmentamos en origen?
  - En IPv4, en la cabecera se indica si se permite o no se permite fragmentar en un salto intermedio. (Bit DF, *Don't Fragment*)
  - En IPv6 no se permite fragmentar en un salto intermedio, solo en el origen

MTU

El tamaño del datagrama está limitado por el MTU: *Maximum Transmission Unit* . Tamaño máximo de la trama

- Es una característica de cada nivel de enlace
  - ethernet: 1500 bytes
  - PPP: 1500 bytes (por omisión)
  - IEEE 802.11: 2272 bytes
  - jumbogramas ethernet: 1500-9000 bytes
- IPv4 exige un MTU de al menos 68 bytes
  IPv6 exige un MTU de al menos 1280 bytes
  MTU máximo teórico: 65535 bytes
- Si un enlace es un túnel sobre IPv4, el MTU será ligeramente inferior al de un enlace ordinario, pero esto apenas supone un cambio

PMTUD *Path MTU Discovery* (IPv4)

RFC 1191. Año 1990.

- El packetization protocol establece un tamaño tentativo inicial de datagrama
  - El MTU del primer salto si es lo único que conoce
  - Mínimo(MTU primer salto, MTU último salto), en el caso de TCP, que puede conocer el MTU del último salto

Si el tamaño elegido resulta ser demasiado grande para el MTU de alguno de los saltos intermedios

- Cuando DF lo permite (p.e. UDP), el datagrama se fragmenta en ese mismo salto
- Cuando DF no lo permite (p.e. TCP), se envía mensaje de error ICMP

```
Type 3 (Destination Unreachable)
Code 4 (Fragmentation required, and DF flag set)
```

  - En este caso IP no entrega el datagrama, niveles superiores tal vez lo reenvíen, si procede
  - Lo que garantiza el algoritmo es que el tamaño de posteriores datagramas irá convergiendo al valor adecuado

- Naturalmente, diferentes datagramas pueden seguir diferentes caminos con diferentes MTU. Lo relevante es el mínimo MTU
- De vez en cuando (5-10 minutos) se aumenta el tamaño del datagrama por si ha mejorado

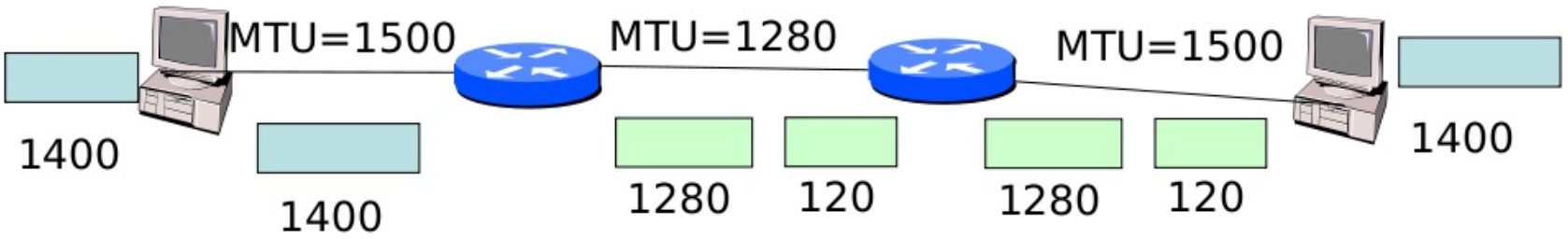
PMTUD *Path MTU Discovery for IPv6*

- RFC 1981, año 1996
- Se demuestra que la fragmentación es muy ineficiente, el bit DF desaparece, el comportamiento de IPv6 es equivalente a IPv4 con el bit activo
- Un nodo no está obligado a usar PMTUD: Puede enviar datagramas de 1280 bytes, mínimo exigido por IPv6

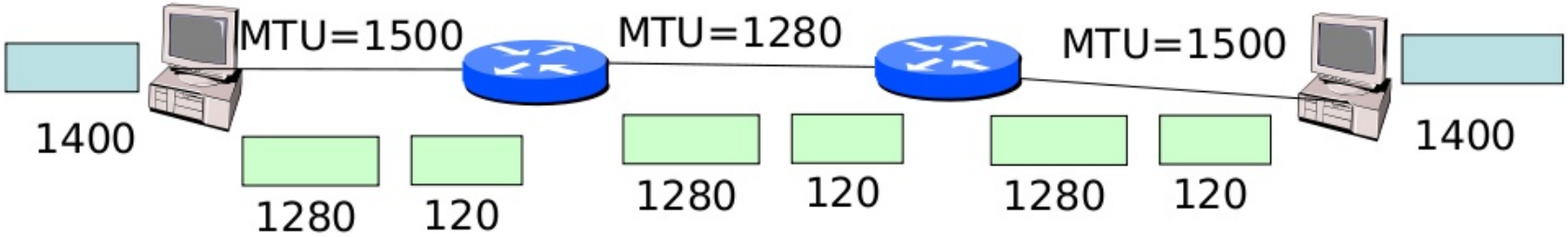
El procedimiento es análogo al de IPv4 con el bit DF activado

- El *packetization protocol* establece un tamaño tentativo inicial de datagrama (el del primer salto, o el mínimo entre primer y último salto)
- Si el tamaño inicial resulta demasiado grande, el router que lo detecta envía error ICMP
  `2-Packet Too Big`
  - En este caso IP no entrega el datagrama, niveles superiores tal vez lo reenvíen, si procede
  - Lo que garantiza el algoritmo es que el tamaño de posteriores datagramas irá convergiendo al valor adecuado
- De vez en cuando (5-10 minutos) se aumenta el tamaño del datagrama por si ha mejorado

IPv4


MTU=1500
MTU=1280
MTU=1500
1400
1400
1280
120
1280
120
1400

IPv6


MTU=1500
MTU=1280
MTU=1500
1400
1280
120
1280
120
1280
120
1400

Contenidos

Encaminamiento en IPv6

IPv6 sigue usando esencialmente los mismos algoritmos de encaminamiento que ipv4

- Como protocolo IGP (Interior Gateway Protocol), RIPng o OSPF
  - Distance Vector
- Como protocolo EGP (External Gateway Protocol), Border Gateway Protocol (BGP)
  - Path Vector Protocol