

IPv6

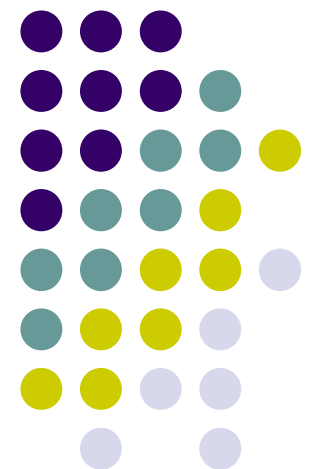
2012

Comunicaciones

LCC

UNR

bulacio@cifasis-conicet.gov.ar





Bibliografía

- IPv6.br , Material Teórico, Curso IPv6 Básico,
<http://ipv6.br/download/>
- TCP/IP Tutorial and Technical Overview, ibm.com/redbooks
- The ABCs of IP Version 6, www.cisco.com/go/abc
- Tutorial de IPv6, Consulintel, IPv6 Forum.
- Guía de administración del sistema: servicios IP, *SUN* Microsystems.



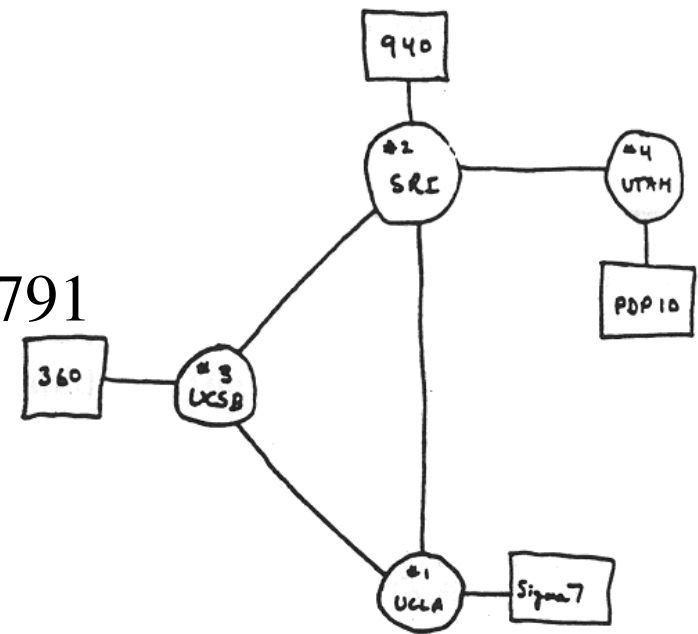
IPv6: Contenido

- Motivaciones y Orígenes de IPv6
- Objetivos de Diseño
- Datagrama - Cabeceras
- Direcciones
- Funcionalidades
 - ICMP/
 - Neighbor Discovery/
 - Autoconfiguration/
 - PMTUD/ QoS/
 - Coexistence issues



Internet

- 1969 – Inicio de ARPANET: 4 computadoras con cables dedicados
- 1981 – Definición de IPv4 en la RFC 791
- 1983 – ARPANET adopta TCP/IP
- 1990 – Primeros estudios sobre el agotamiento de las direcciones
- 1993 – Internet comienza a ser explotada comercialmente

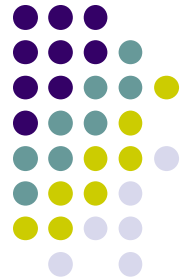


THE ARPA NETWORK

DEC 1969

4 NODES

FIGURE 6.2 Drawing of 4 Node Network
(Courtesy of Alex McKenzie)



Problemas en IPv4

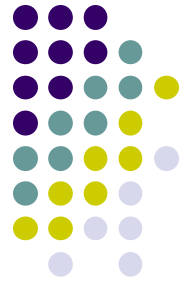
- 32 bits de direcciones (~ 4000 millones)

Clase	Net	Host	Dirs.#	Hosts
A	1 oct.	3 oct.	126	16.387.064
B	2 oct.	2 oct.	16.383	64.516
C	3 oct.	1 oct.	1.097.151	254

- Asignación INEFICIENTE.

Clase A: IBM, AT&T, Xerox, HP, Apple, MIT, Ford, el Departamento de Defensa de Estados Unidos...

Agotamiento del espacio total



Soluciones paliativas

- **1992 – La IETF crea el grupo ROAD (*RO*uting and *AD*ddressing)**
 - Classless Inter-Domain Routing, CIDR (Enrutamiento entre dominios sin Clases, RFC 4632)
 - Fin del uso de clases = bloques de tamaño apropiado.
 - Dirección de red = **a.b.c.d/x**
 - Agregación de rutas = reduce el tamaño de la tabla de rutas.
- **DHCP (*Dynamic Host Configuration Protocol*, RFC 2131)**
 - Dir. IP temporarias
- **NAT (*Network Address Translation*, RFC 1631) + RFC 1918 (*Address Allocation for Private Internets*)**
 - Permite conectar toda una red de computadoras usando una sola dirección válida en Internet...



Soluciones paliativas

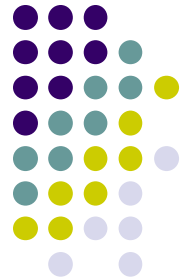
NAT (Network Address Traslation, RFC 3022)

- **Ventajas:**

- Reduce la necesidad de direcciones públicas;
- Facilita la numeración interna de las redes;
- Oculta la topología de las redes;
- Solo permite la entrada de paquetes generados en respuesta a un pedido de la red.

- **Desventajas:**

- Rompe con el modelo **end-to-end** de Internet;
- Dificulta el funcionamiento de una serie de aplicaciones (P2P,...);
- No es escalable;
- Aumento del procesamiento en el dispositivo traductor;
- Imposibilidad de rastrear el camino del paquete (traceroute);
- Imposibilita el uso de seguridad como IPSec.



Soluciones

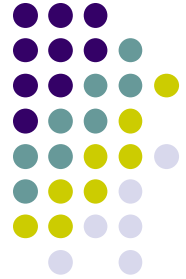
Estas medidas han permitido contar con más tiempo para desarrollar una nueva versión de IP.

- 1992 – La IETF crea el grupo IPng (*IP Next Generation*)
- Aspectos principales:
 - Escalabilidad;
 - Seguridad;
 - Configuración y administración de redes;
 - Soporte para QoS;
 - Movilidad;
 - Políticas de enrutamiento;
 - Transición.
- 1993 surge la RFC 1550 IP: Next Generation (IPng) White Paper Solicitation...



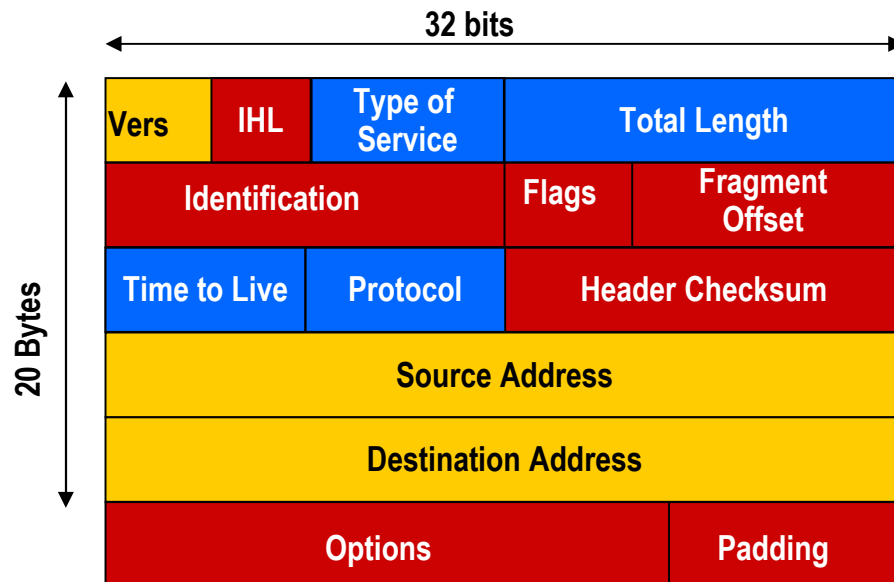
Objetivos de Diseño (IETF)

- Datagrama Eficiente: Base + Extensión
- Direccionamiento: Mayor número de direcciones
- Fragmentación en origen-destino
- Identificador de flujos (QoS)
- Mecanismos que faciliten la configuración (plug $\neg$ play)
- Seguridad incorporada: autenticación y cifrado
- Compatibilidad con IPv4
- ...



Cabeceras IPv4

IPv4



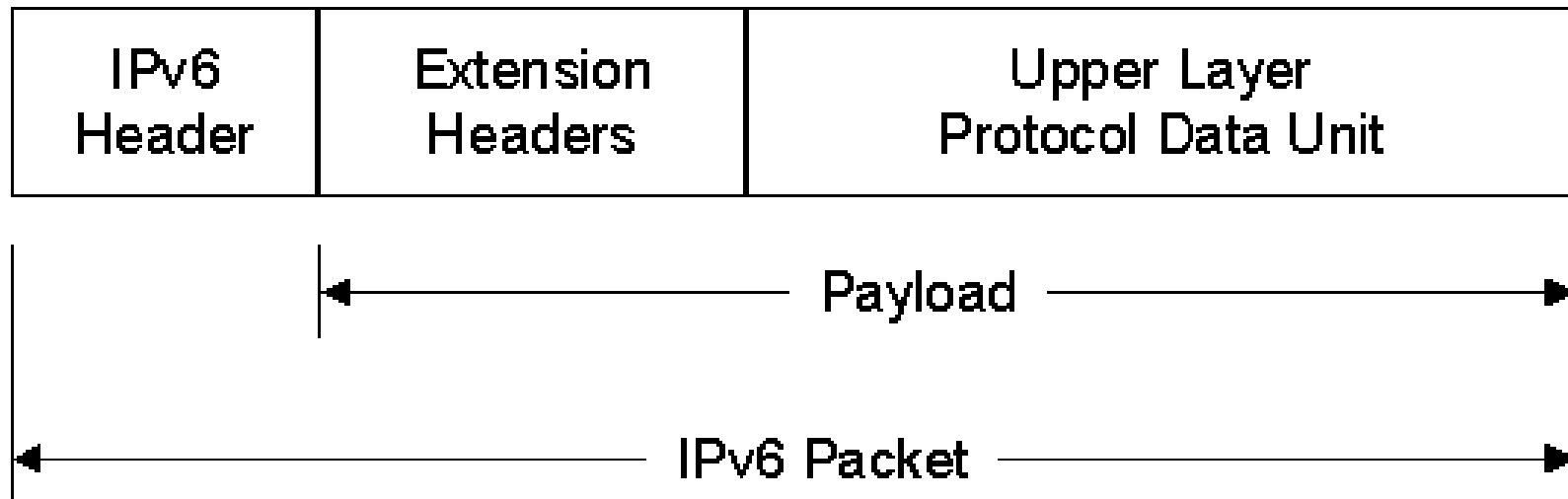
- Campos que mantienen los nombres
- Campos eliminados
- Nombre y posición cambiados
- Campo nuevo

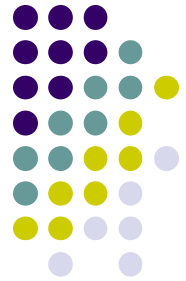
IPv4: 12 campos fijos que pueden tener opciones => cabecera de tamaño entre 20 y 60 bytes



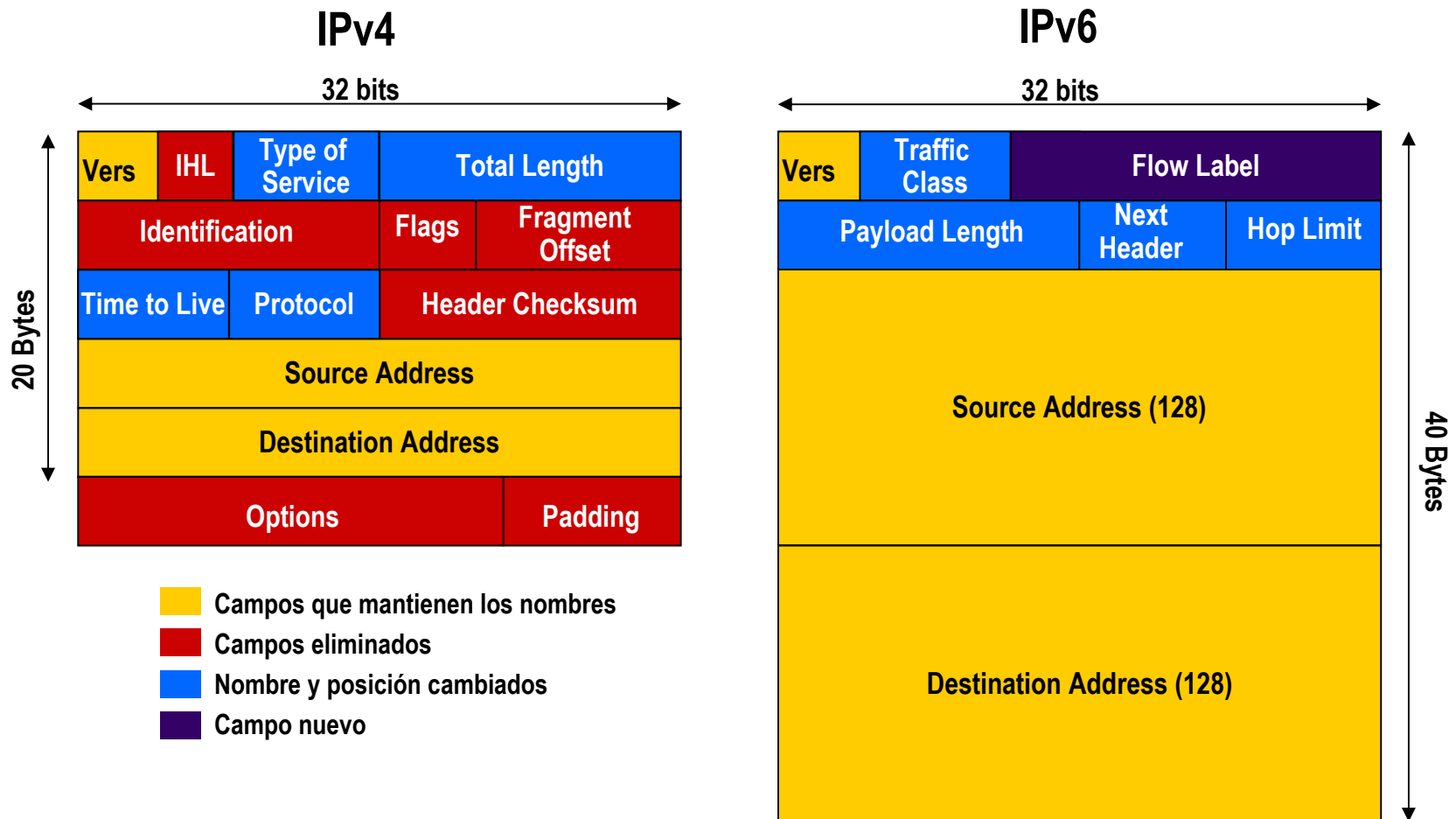
Datagrama IPv6 (RFC2460)

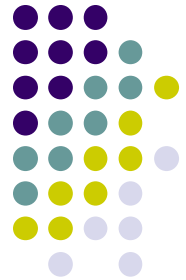
- + **Simple:** 40 bytes fijos
- + **Flexible:** cabeceras opcionales
- + **Eficiente:** minimiza el *overhead*



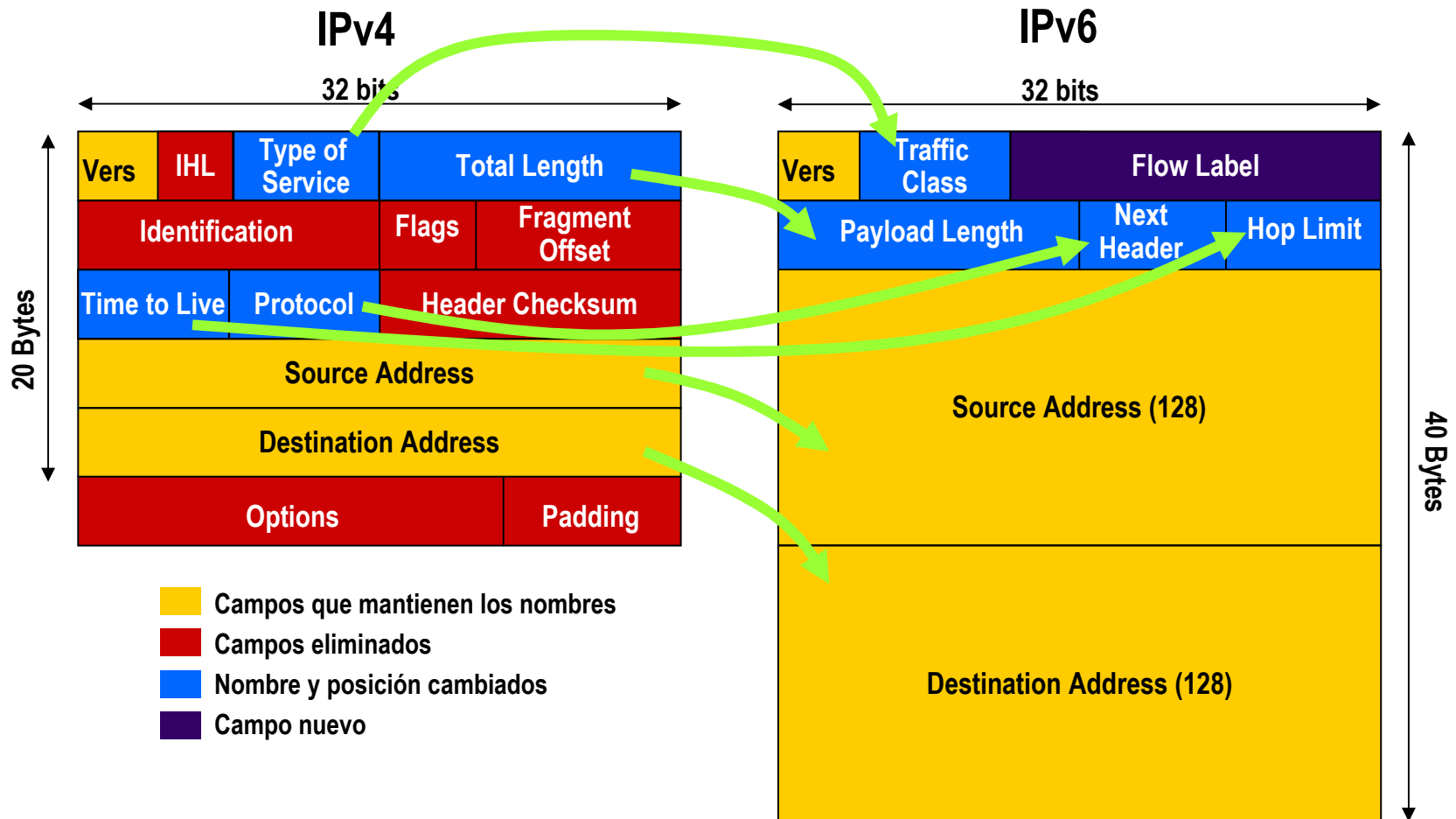


Cabeceras IPv4 - IPv6





Cabeceras IPv4 - IPv6





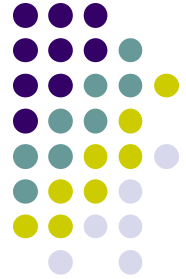
Cabeceras IPv4 - IPv6

IPv4	IPv6
Tipo de Servicio	→ Clase de Tráfico
Tamaño Total	→ Tamaño de los Datos
Tiempo de Vida (TTL)	→ Límite de Encaminamiento
Protocolo	→ Siguiendo Encabezado

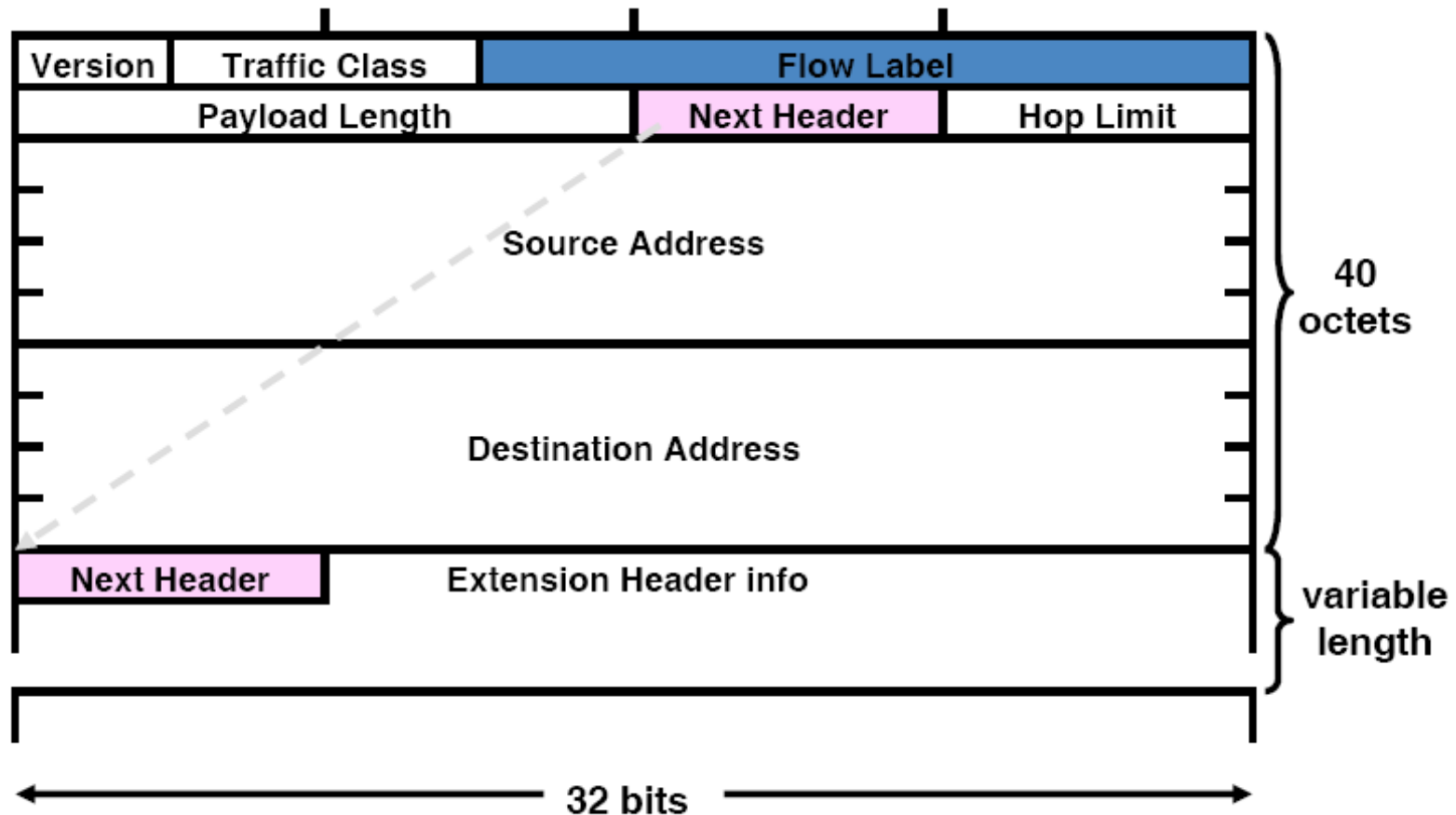


Cuadro de diferencias de Headers

IPv4 Header 20bytes+opt	IPv6 Header 40 bytes
Version	=
Internet Header Length	Removido , la longitud es fija (40 bytes)
Type of Service	Remplazado por Traffic Class en IPv6.
Total Length	Remplazado por el campo Payload Length , que sólo indica la longitud del payload.
Identification Fragmentation Flags Fragment Offset	Removido , la lx de fragmentación está en la cabecera de Fragmentation.
Time to Live	Remplazado por el campo Hop Limit .
Protocol	Remplazado por el campo Next Header .
Header Checksum	Removido puesto que la detección de bit-level Error es realizada en el paquete completo por la capa de enlace
Source Address 32 bits	Incrementado a 128 bits.
Destination Address	Incrementado a 128 bits.
Options	Reemplazado por cabeceras de extensión



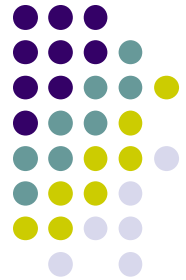
Cabecera Base-Extensión IPv6



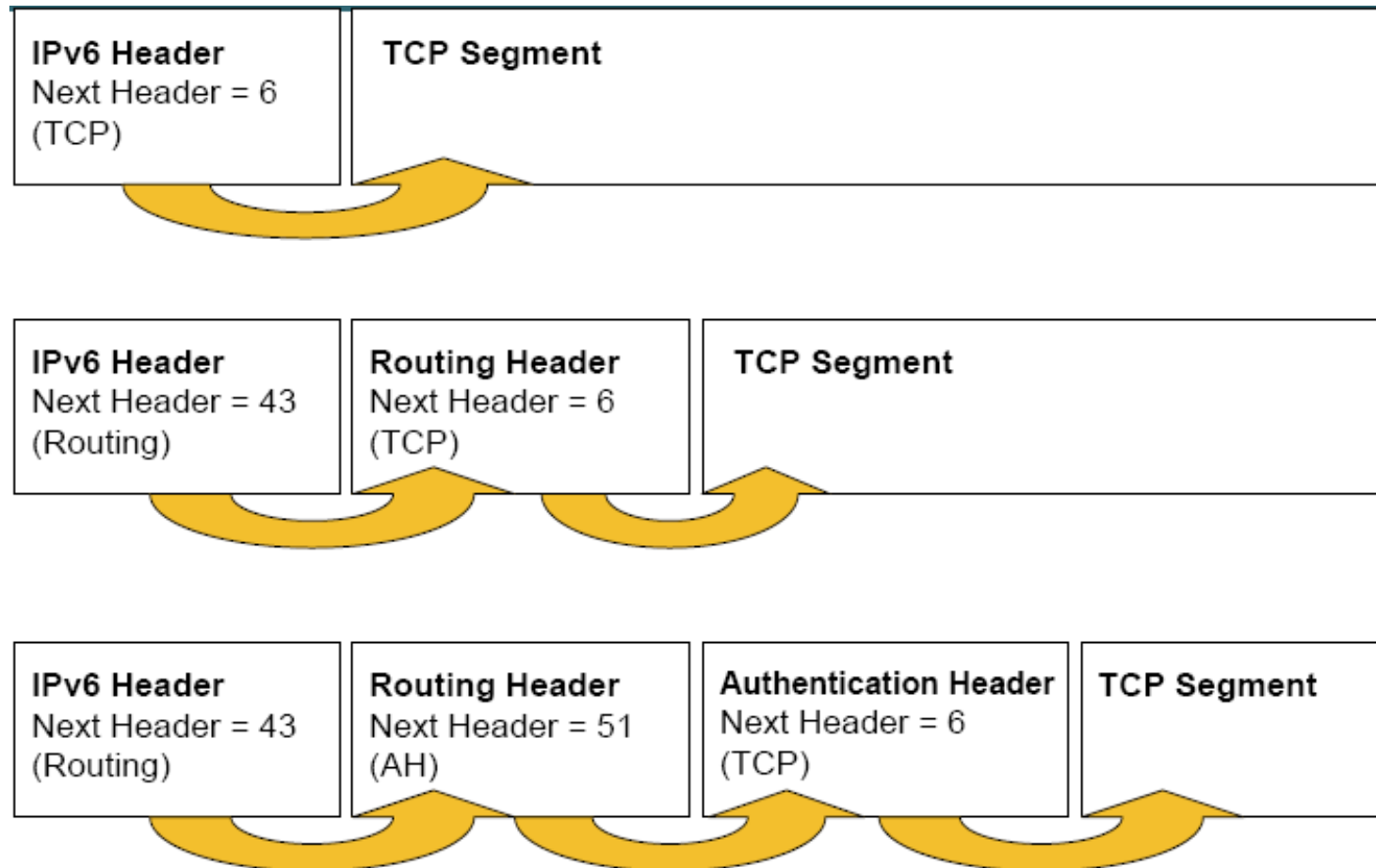


Cabeceras de Extensión

- Son identificados por **Next Header**
 1. *Hop-by-Hop Options,*
 2. *Routing,*
 3. *Fragmentation,*
 4. *Authentication Header,*
 5. *Encapsulating Security Payload,*
 6. *Destination Options.*
- La longitud varia (múltiplo de 8)
- Cada tipo puede aparecer una vez en un paquete
- El orden es importante para el procesado eficiente en los routers intermedios
- En cada nodo sólo se analizan *Hop-by-Hop* y *Routing*

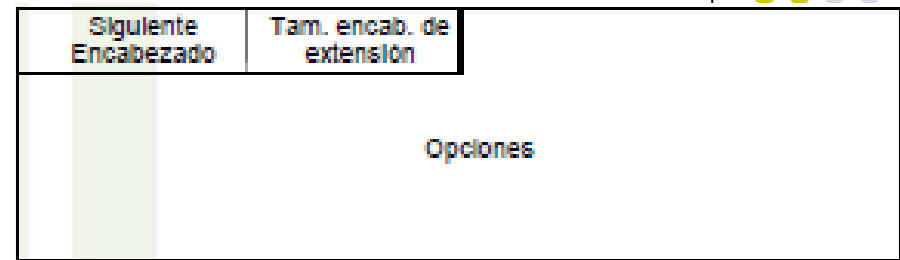


Cabeceras de Extensión:





Extensión: Hop-by-Hop

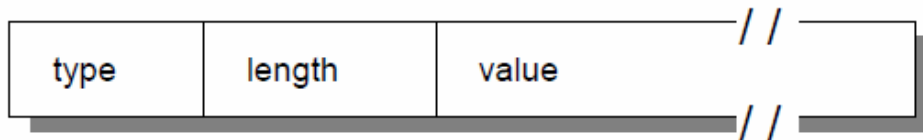


- **Identificado** por Next Header = 0
- **Procesado** por todos los nodos en la ruta del paquete.
- **Tamaño del Encabezado** (1 byte): Tamaño del encabezado *Hop-by-Hop* en unidades de 8 bytes, excluyendo los ocho primeros.
- **Opciones:** Contiene una o más opciones.
 - **Type:** Los 2 primeros bits codifican qué hacer en caso que el nodo no reconozca la opción:
 - 00: ignorar y continuar el procesamiento.
 - 01: descartar el paquete.
 - 10: descartar el paquete y enviar un mensaje ICMP *Parameter Problem* a la dirección de origen del paquete.
 - 11: descartar el paquete y enviar un mensaje ICMP *Parameter Problem* a la dir. de origen del paquete, solamente si el destino no es una dirección *multicast*.



Ej.: Hop-by-Hop

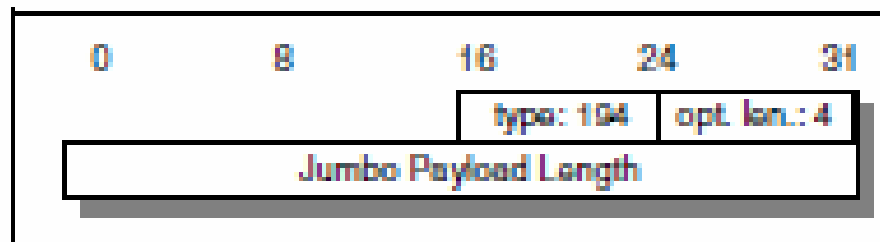
- Opciones:
 - Router Alert: informa Mx con tratamiento especial (RSVP, Resource Reservation Protocol)
 - Jumbogram: Payload > $2^{16} = 65535$ bytes Jumbo

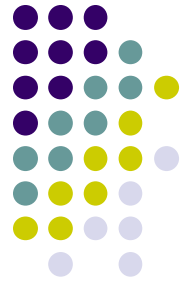


Type: 194 (8 bits)

Length: 4 (8 bits)

value: Jumbo Payload length (4 bytes)





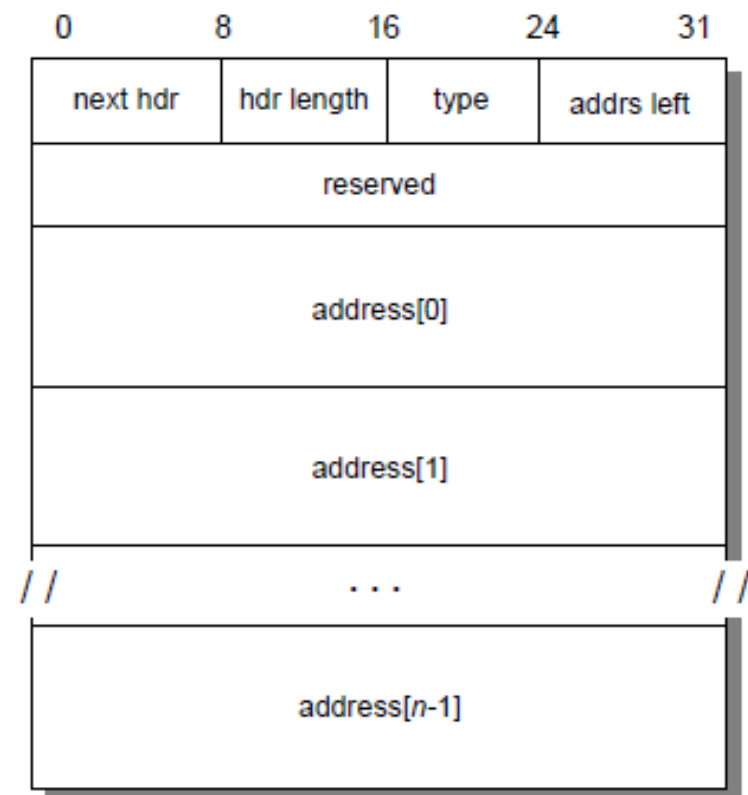
Extensión: Routing header

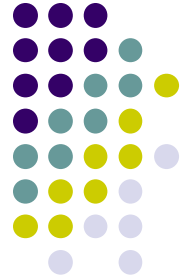
Identificado por Next Header: 43

Routing type 0: ruta predefinida

- El 1er salto es la dir. del header base.
- Cdo llega a esa dirección, el router cambia la dirección destino de la cabecera base con la próxima dirección (**address[i]**), y
- Decrementa **addrs left**.

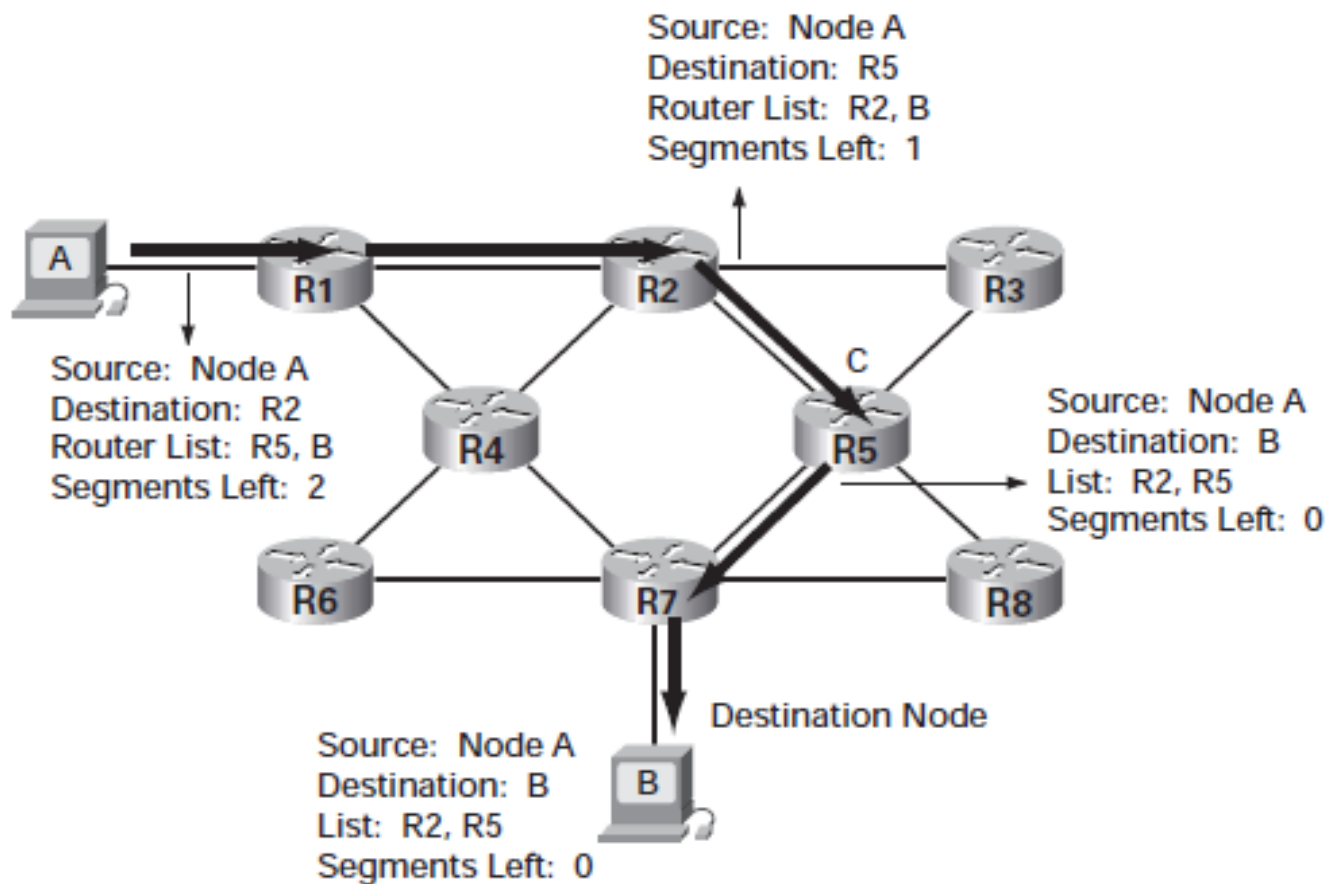
Problemas de seguridad

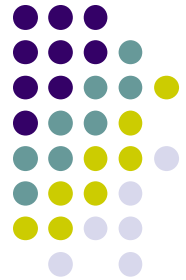




Ej. Routing header

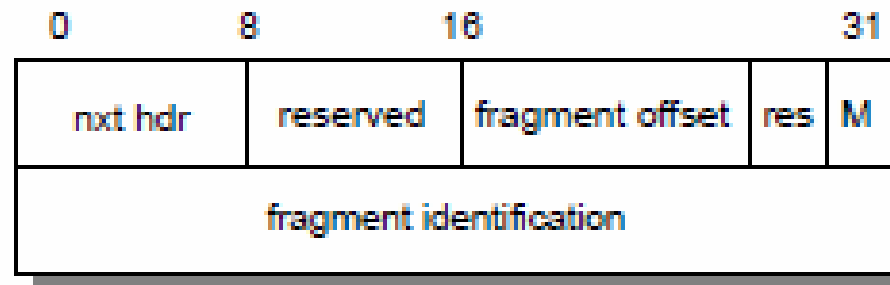
Figure 5: IPv6 Routing Header





Extensión: Fragment

- Identificado por Next Header=44
- Requiere el Path MTU (maximum transmission unit), RFC 1191.
- IPv6 MTU ≥ 1280 bytes.



Fragment offset, 13 bits: offset en unidades de 8 bytes la posición del fragmento actual respecto al datagrama original

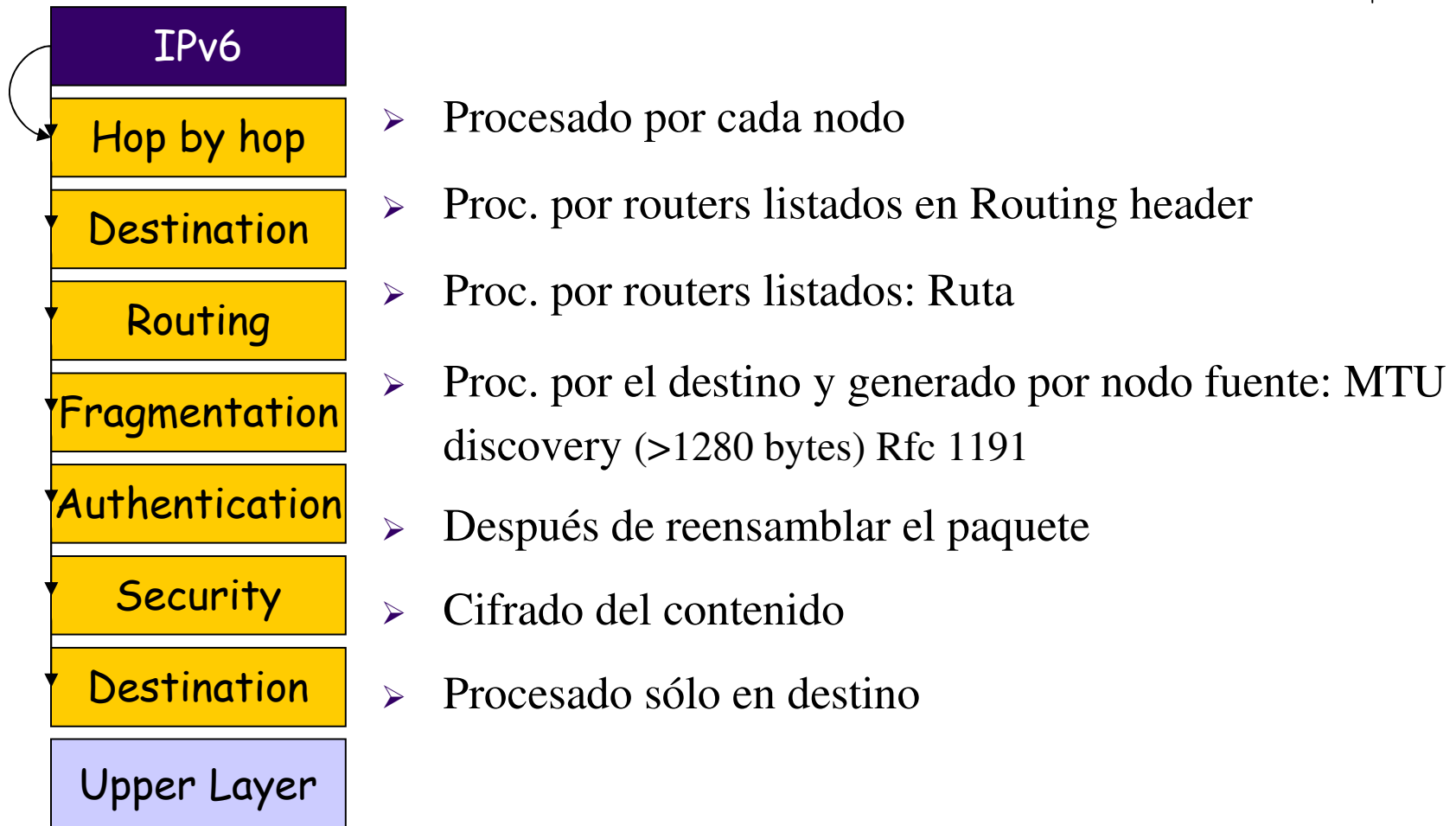
Frag. ID: identificador de los fragmentos de un mismo datagrama

M: si hay más fragmentos

Identificación: valor único generado por el nodo origen para identificar fragmentos del mismo datagrama



Procesado y orden





IPv6: Cabeceras

- Resumen de Ventajas:
 - Escalable en el número/tipo de opciones
 - Procesamiento ordenado/eficiente
 - Distribución de la complejidad
 - Cabeceras procesadas por elementos de red intermedios (**routers**)
 - Cabeceras procesadas en **destino**



Revisión Cabecera

1. Describa qué campos se eliminaron/modificaron respecto a la cabecera IPv4-IPv6. Por qué?
2. Para qué se separa en cabecera base y de extensión?
3. Qué cabeceras son analizadas en los routers intermedios?
4. Describa las siguientes características de la cabecera base de IPv6: tamaño posible, información y utilidad de los campos `Traffic class`, `Flow label`, `Next header`.



IPv6: Contenido

- Motivaciones y Orígenes de IPv6
- Objetivos de Diseño
- Datagrama - Cabeceras
- **Direcciones**
- Funcionalidades
 - ICMP/
 - Neighbor Discovery/
 - Autoconfiguration/
 - PMTUD/ QoS/
 - Coexistence issues

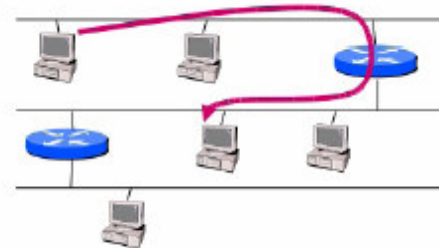


Direccionamiento

IPv6.br , Curso IPv6 Básico, Apostilas e outros materiais

Guía de administración del sistema: servicios IP,
SUN Microsystems

Componentes



- **Nodo:** Dispositivo con dirección (interfaz) IPv6. Término genérico que se aplica a hosts y routers.
- **Encaminador o router IPv6:** Nodo que reenvía paquetes de IPv6. Para admitir IPv6, debe configurarse como mínimo una de las interfaces del router. Un router de IPv6 también puede anunciar el prefijo de sitio IPv6 registrado para la empresa en la red interna.
- **host de IPv6:** Nodo con al menos una dirección IPv6. Al igual que en IPv4, los hosts de IPv6 no reenvían paquetes.
- **Vínculo o link o enlace:** Un solo soporte contiguo de red conectado por un encaminador en cualquiera de sus extremos.
- **Vecino:** Nodo de IPv6 que se encuentra en el mismo vínculo que el nodo local.



Direcciones IPv6: Rfc 4291

- Una dirección IPv4 está formada por **32** bits.

$$2^{32} = 4.294.967.296$$

- Una dirección IPv6 está formada por **128** bits.

$$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$$

~ $5,6 \times 10^{28}$ direcciones IP por cada ser humano.

~ $7,9 \times 10^{28}$ de direcciones más que en IPv4



Direcciones IPv6

Formato: 8 campos de 16 bits, escritos en Hexa, separados por “:”

2001 : 0DB8 : AD1F : 25E2 : CADE : CAFE : F0CA : 84C1

En la representación de una dirección IPv6 está permitido:

- Utilizar caracteres en mayúscula o minúscula;
- Omitir los ceros a la izquierda; y
- Representar los ceros continuos mediante “::”

Ej. Compactación

2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

2001:0db8:3c4d:0015:0:0:1a2f:1a2b

2001:0db8:3c4d:0015::1a2f:1a2b



Direcciones IPv6

Ej. Compactación

- FF01:0000:0000:0000:0000:0000:0000:0001 ?
- 2001:0000:1234:0000:0000:C1c0:ABCD:0876 ?



Direcciones IPv6

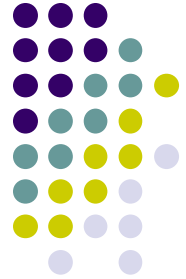
- Ej. Compactación

- FF01:0000:0000:0000:0000:0000:0000:0001
 - FF01::1
- 2001:0000:1234:0000:0000:C1c0:ABCD:0876 ?
 - 2001:0:1234:0:0:C1c0:ABCD:0876 ?
 - 2001::1234::C1c0:ABCD:0876 ?
 - 2001:0:1234::C1c0:ABCD:0876 ?

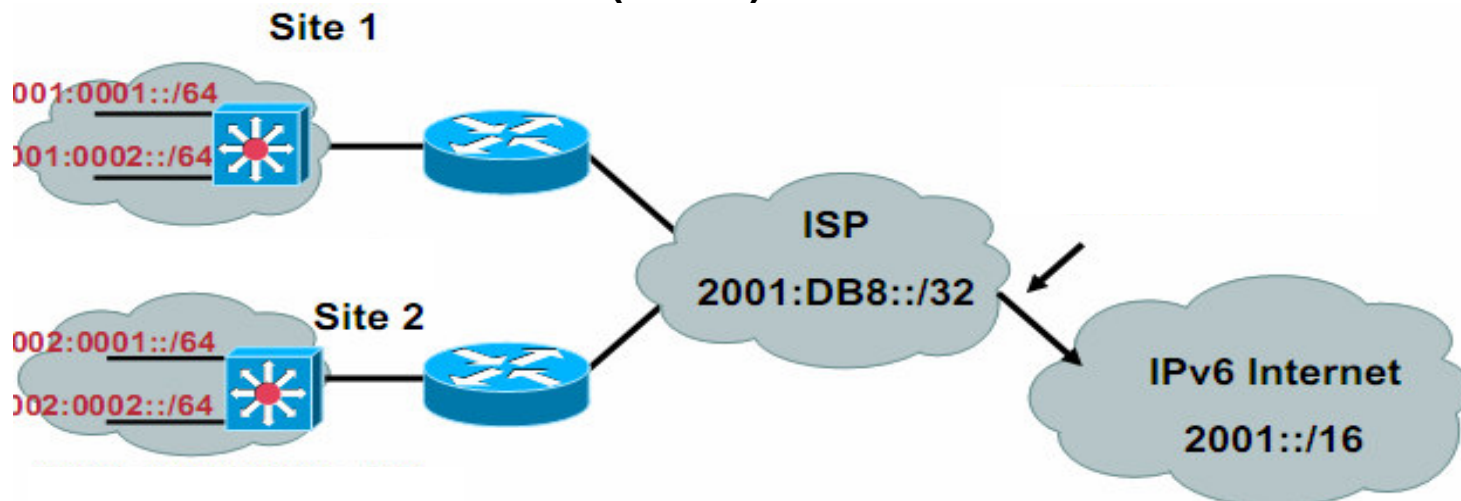
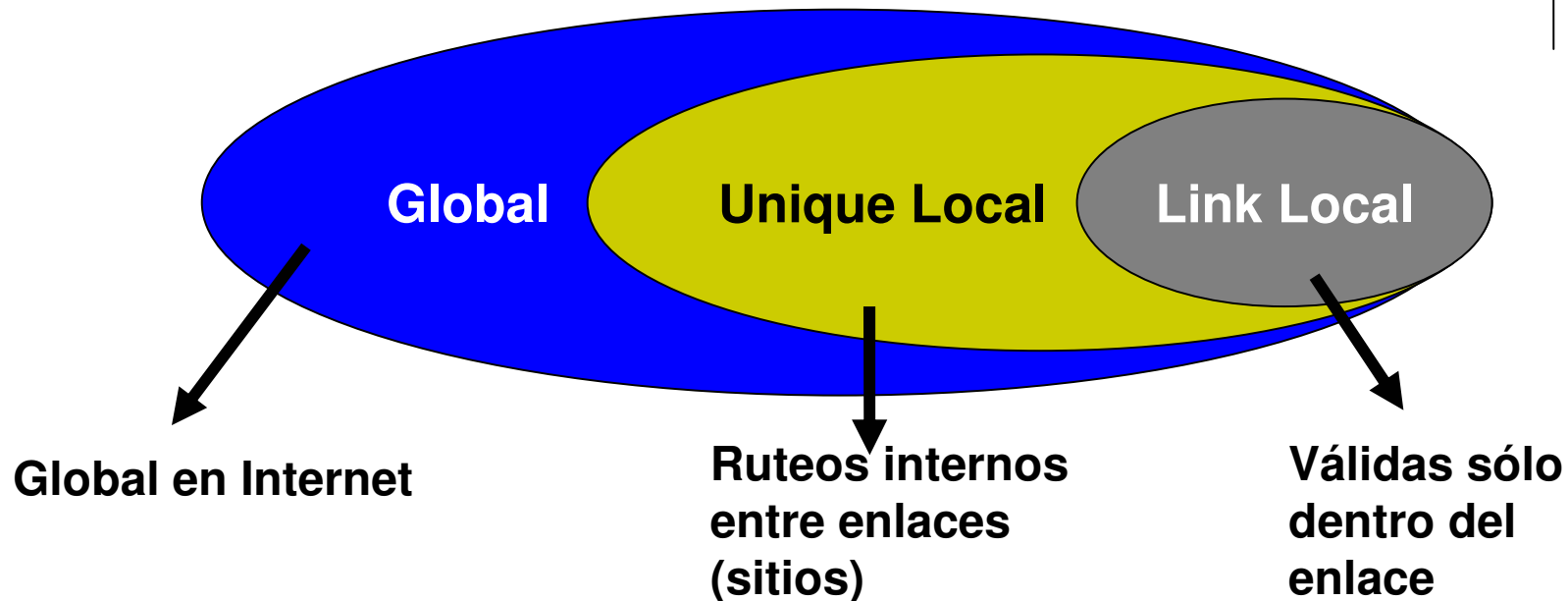


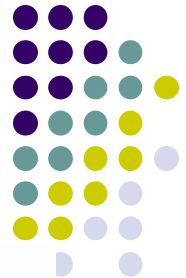
Direcciones IPv6: Scope

- Las direcciones se asignan a interfaces (idem a IPv4)
- Las interfaces pueden “naturalmente” tener varias direcciones
- Alcance de las direcciones:
 - Link Local (locales a subred)
 - Site Local (locales a organización)
 - Globales



Direcciones: Alcance

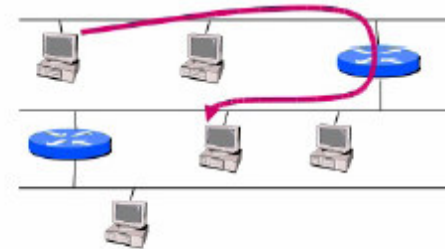




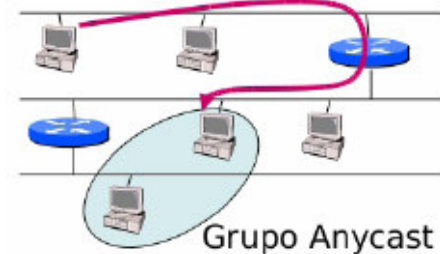
Tipos de direcciones

- **Unicast:** identifican a una interfaz de un solo nodo (de uno a otro)
- **Anycast:** identifican a un conjunto de interfaces, en general de nodos distintos (de uno a alguno ...)
- **Multicast:** identifican a un conjunto de interfaces (de uno a todos los del grupo ...)

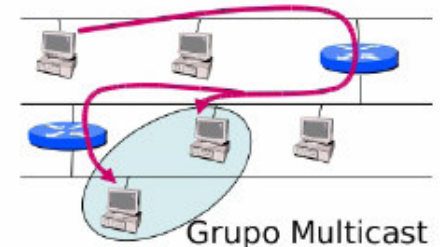
Unicast

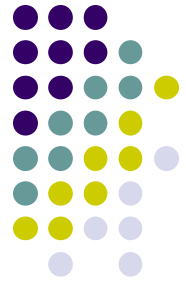


Anycast



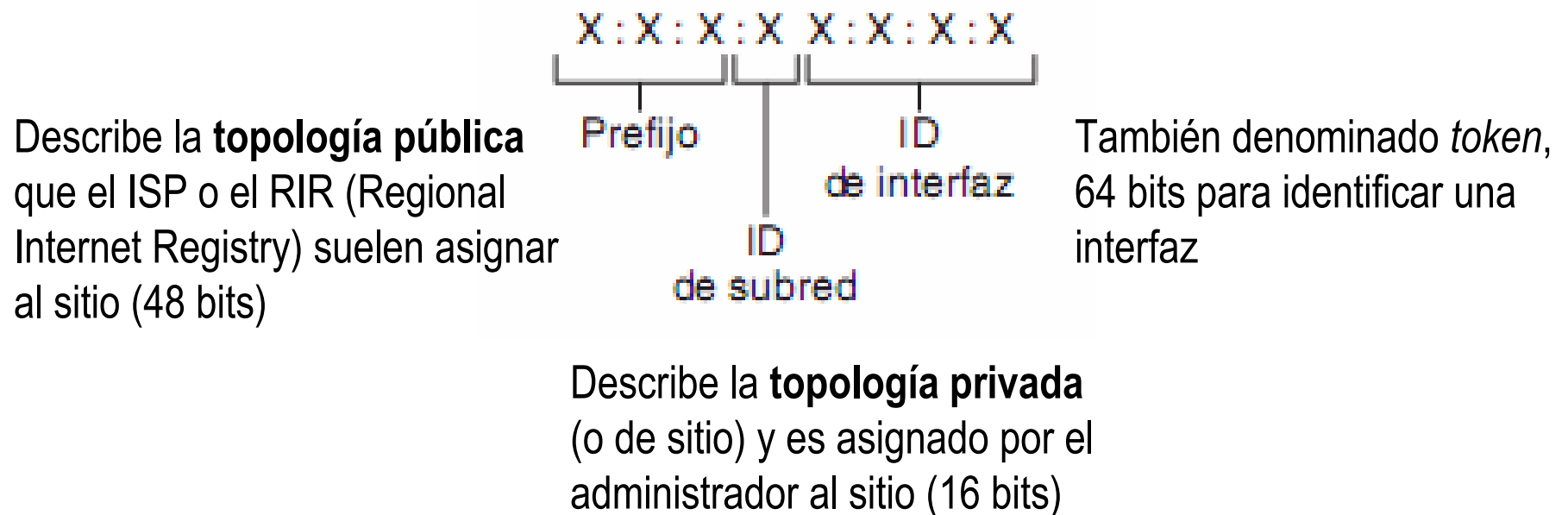
Multicast



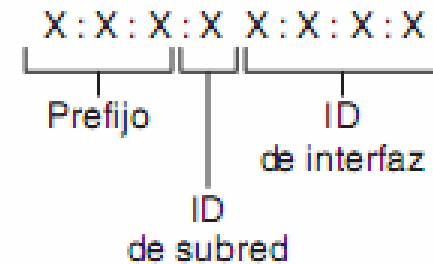


Direcciones IPv6

Formato básico:



Direcciones: Prefijos



- El **prefijo global** se usa para encaminar paquetes IPv6, 48 bits en Global Unicast
- El **prefijo de subred** en un cliente que se le da un bloque /48 tiene 16 bits (65536 redes); en un /56 tiene 8 bits (256 redes); en un /64 no tiene subredes.
- El **prefijo de interfaz** contiene 64 bits



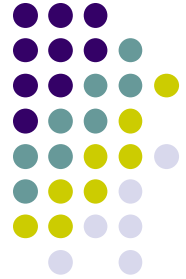
Direcciones de una interfaz

- Loopback
- Link local
- Unique-Local
- Autoconfigurada IPv4 compatible
- Multicast
- Global

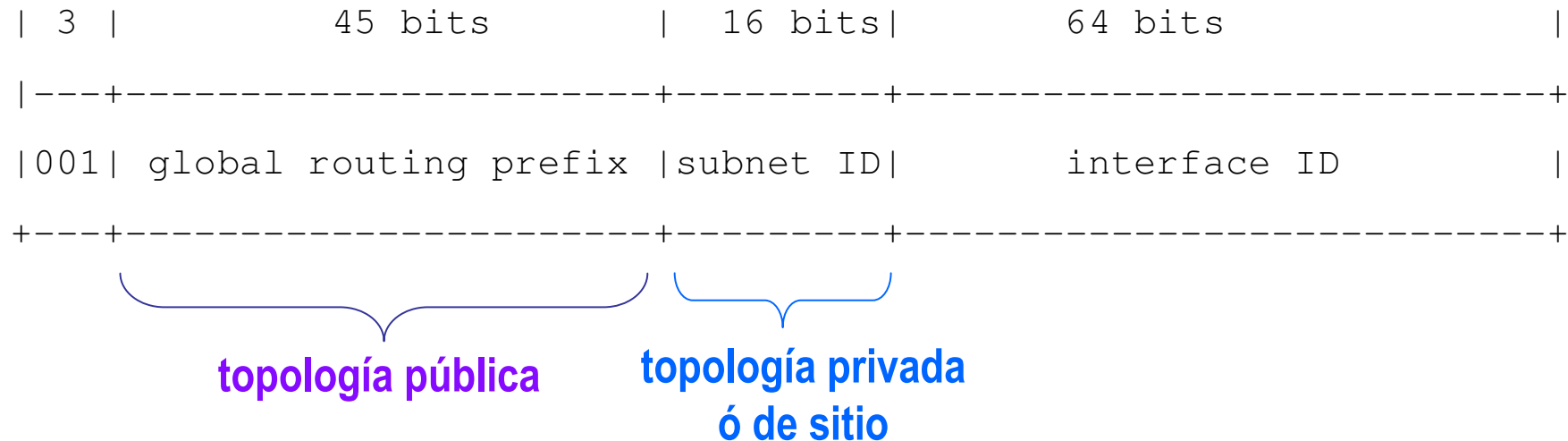


Unicast

Global
Link-Local
Unique-Local
Especiales



Unicast Global 2000::/3



- Globalmente ruteables (equivale a dir. IPv4 públicas)
- Formada por 3 partes:
 - Prefijo de encaminamiento global (asignado por el RIR, Regional Internet Registry)
 - Prefijo de subred: usado para identificar un enlace en una red
 - ID de interfaz (/64): identifica una única interfaz dentro de un enlace

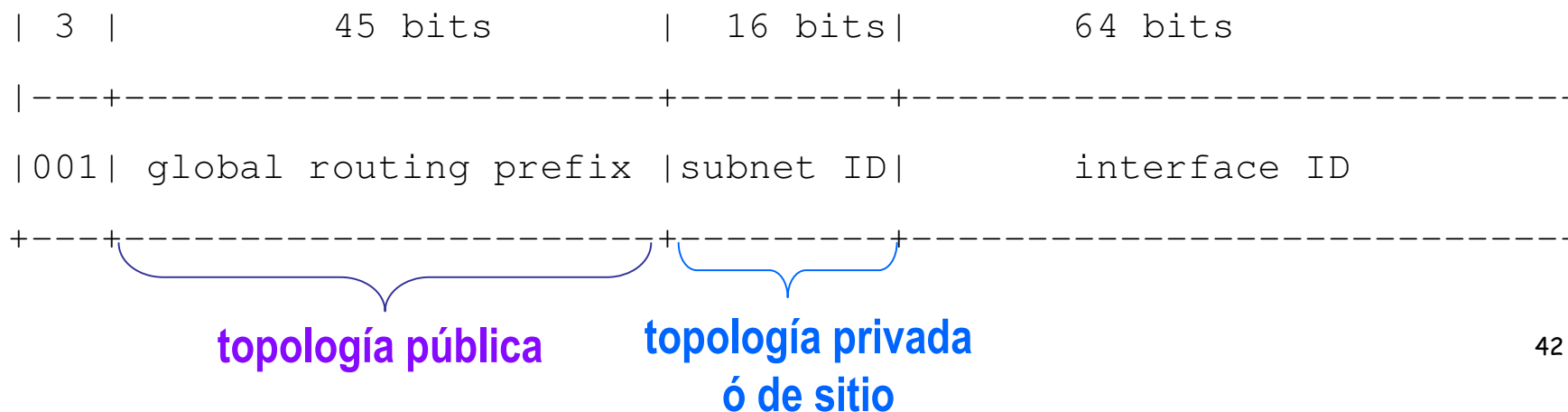


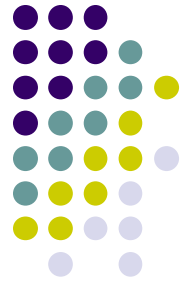
Ejemplo Unicast global

- Formato básico:

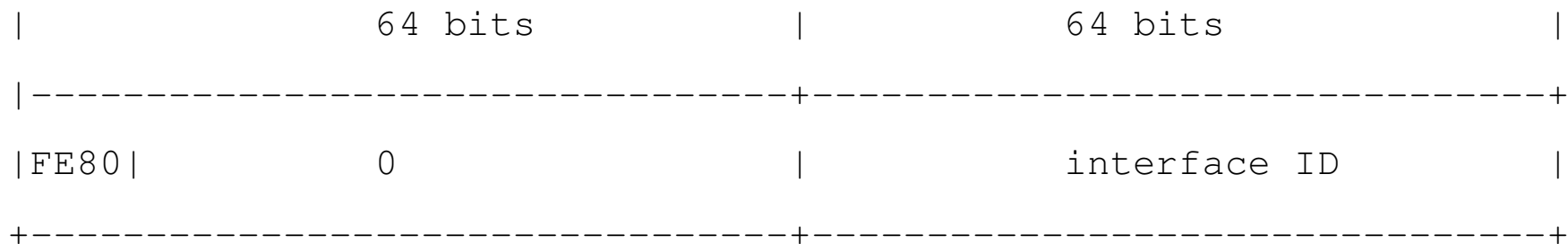
2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

- **2001:0db8:3c4d** ↔ topología pública
- **0015** ↔ topología privada
- **0000:0000:1a2f:1a2b** ↔ ID de subred

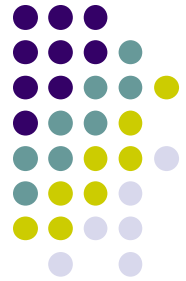




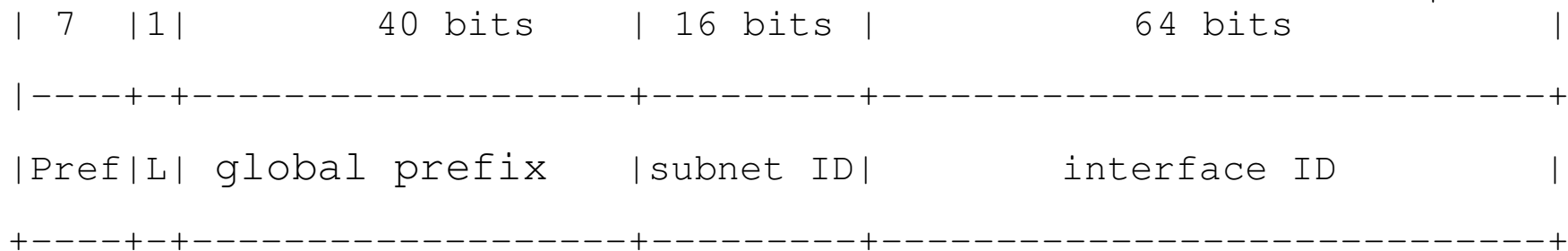
Unicast Link-Local



- Sólo válidas en el enlace local donde la interfaz está conectada
- => **JAMÁS SE RUTEAN HACIA OTROS ENLACES**
- **USO:** Para tareas administrativas, Ej., Descubrimiento de vecinos.
- **Generada** automáticamente (autoconf. Stateless)



Unicast Unique-Local



- **Pref:** FC00::/7 (1111110)
- **L=1** (11111101, FD00) asignación local; **L=0** (FC00) asignado por “alguien” (IANA)
- **Global Prefix:** pseudo aleatorio, probablemente único
- **USO:** Ruteos internos dentro de un enlace o conjunto de enlaces
 - Permite que cualquier **enlace** tenga un **prefijo /48 privado** y globalmente único INDEPENDIENTE del ISP
 - Puede interconectar dos redes sin conflictos; puede haber comunicación sin Internet
- **NO RUTEABLE EN INTERNET GLOBAL**



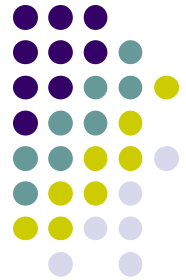
Unicast: Identificador de interfaz (IID)

- Deben ser únicos dentro del mismo prefijo de subred
- El mismo IID se puede usar en múltiples interfaces de un mismo nodo si están en subredes distintas
- Normalmente se usa un IID de 64 bits generado:
 - Manualmente
 - Autoconfiguración stateless
 - Basado en la MAC (Formato EUI-64)

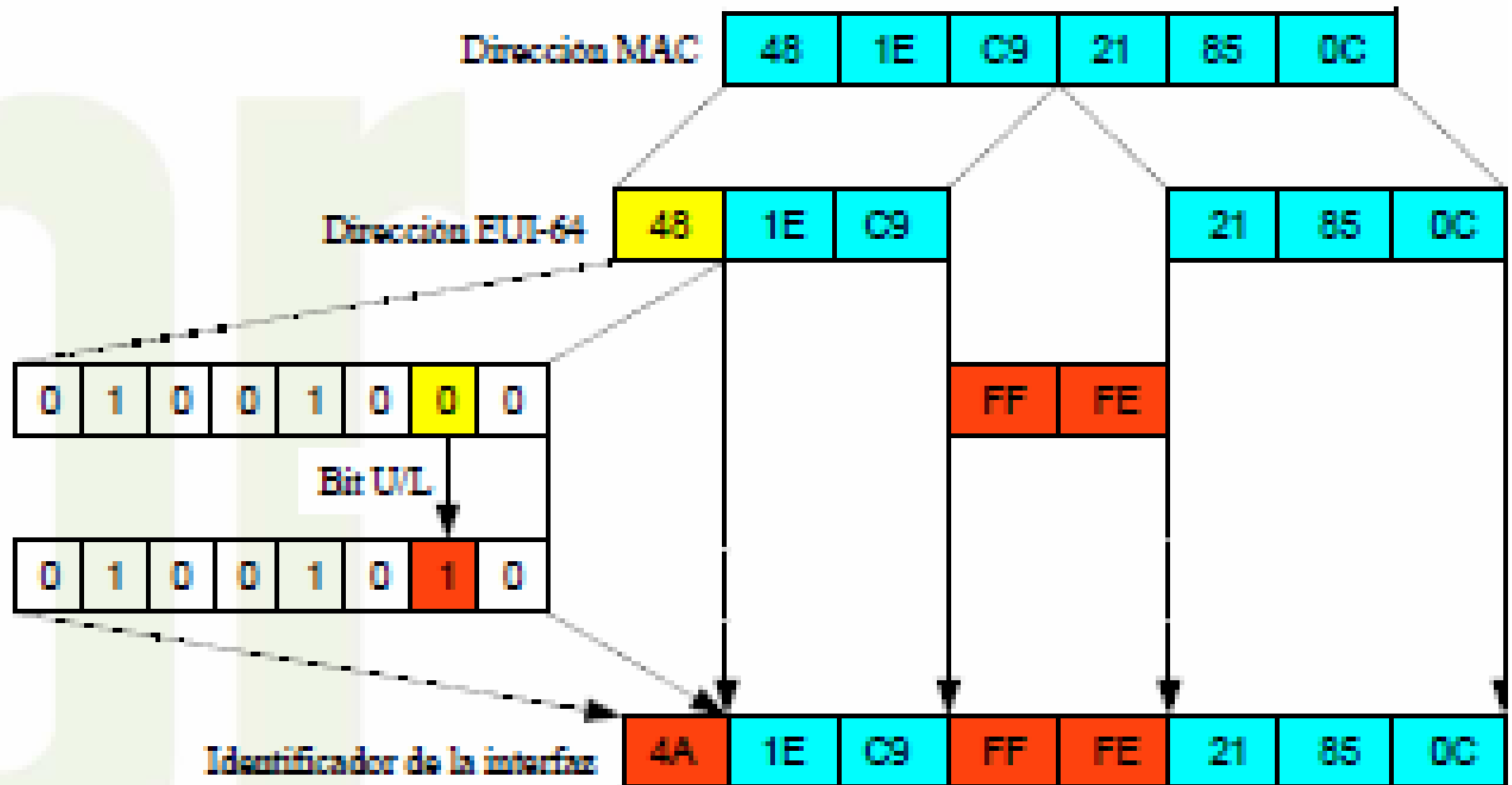


Unicast: IID EUI-64

- Si la MAC es de 64 bits (EUI-64):
 1. Cambiar el bit U/L; 7mo bit más significativo ($1 \rightarrow 0$, $0 \rightarrow 1$)
- Si la MAC es de 48 bits (IEEE 802):
 1. Agregar FF FE en el medio (3er 4to byte) $\rightarrow$ EUI 64
 2. Cambiar el bit U/L



Unicast: IID EUI-64





Unicast: IID EUI-64

- Ej. IID=4A-1E-C9-FF-FE-21-85-0C

Cuál es la dirección *Link-Local* atribuida a dicha interfaz?

- Ej. MAC 6C-F0-49-6F-C5-AB

Cuál es la IID?; cuál es la dir. *Link-Local*?



Unicast: Direcciones especiales

- Loopback $::1/128$
($0:0:0:0:0:0:0:1$)

Usada para pruebas internas (en IPv4 127.0.0.1)

To find if your IPv6 stack works: **>Ping6 ::1**

- No especificada $::/128$
($0:0:0:0:0:0:0:0$)

Nunca debe ser asignada ya que indica ausencia de dirección.

Se usa como dir. Origen en el proceso de inicialización

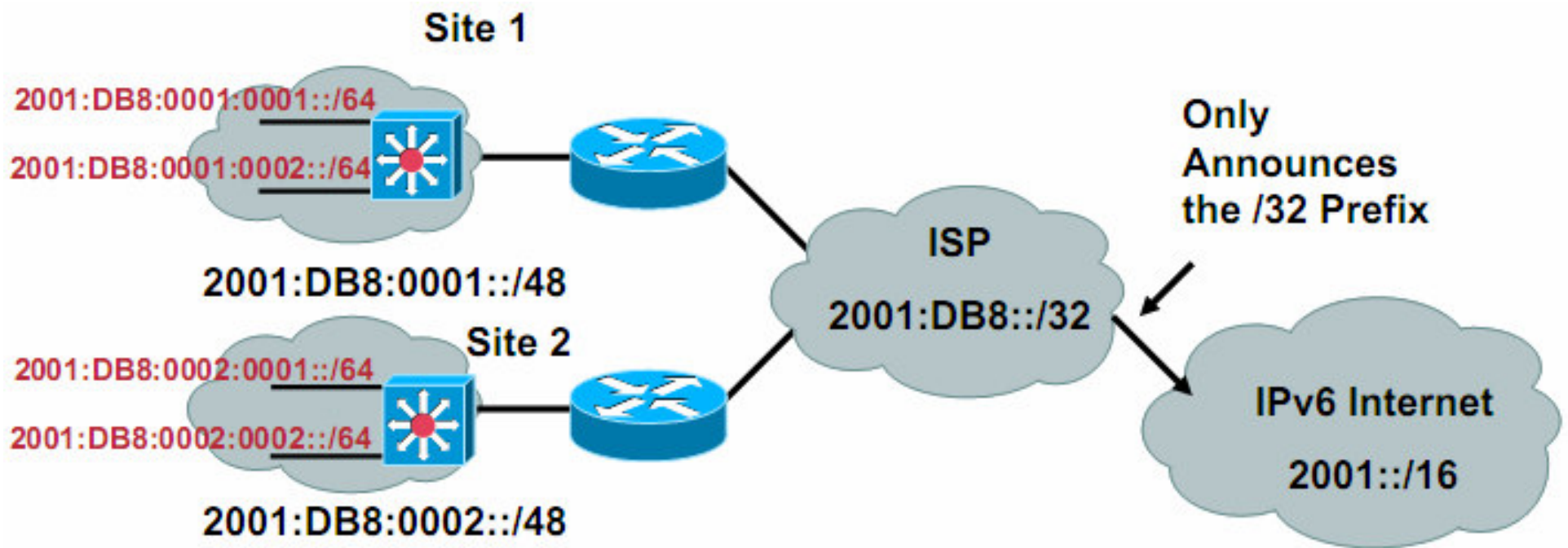
- Mapeada a IPv4 $::FFFF:wxyz$

wxyz son los 32 bits de la dir. IPv4 en decimal. Por ej.,

$::FFFF:192.168.100.1$



Ejemplo





Anycast Multicast

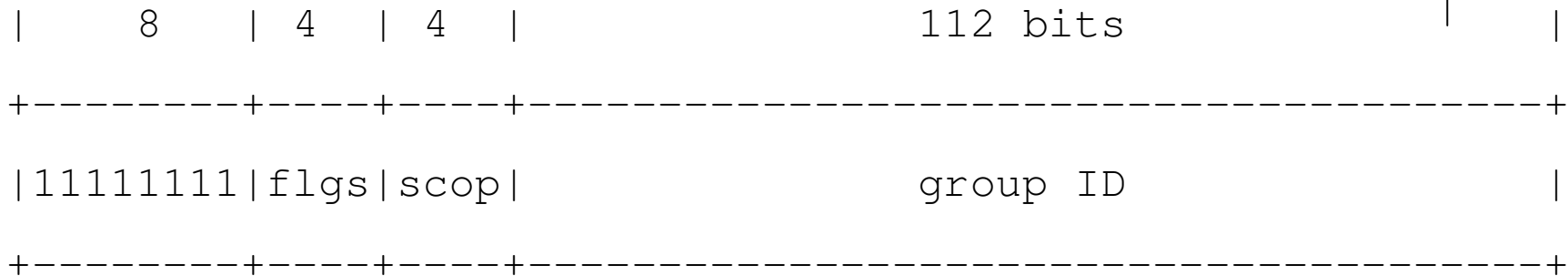


Anycast

- Identifica un grupo de interfaces
 - Entrega el paquete solo a la interfaz más cercana al origen.
- Asignadas a partir de direcciones *unicast* (igual sintaxis)
- **Usos:**
 - Descubrir servicios en la red (DNS, *proxy* HTTP, etc.);
 - Balanceo de carga;
 - Localizar routers que proveen acceso a una determinada subred;
- Anycast Subnet-Router: formadas por el prefijo de la subred + el IID en 0 (ej., **2001:db8:cafe:dad0::/64**)
 - Un paquete enviado a esta dir. Es entregado al router más próximo al origen dentro de la misma subred.



Multicast



- Identifica un grupo de interfaces.
- Prefijo **FF** + 4 bits de *flags* + 4 bits que definen el alcance de la dirección *multicast*.
- El soporte para *multicast* es obligatorio en todos los nodos IPv6.
- La dirección *multicast* deriva del bloque **FF00::/8**.
- Los 112 bits restantes se utilizan para identificar el grupo *multicast*.



Multicast flgs

flgs is a set of 4 flags:

+--+--+--+

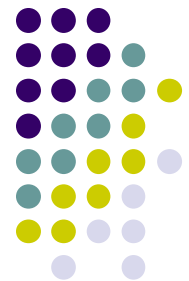
|0|R|P|T|

+--+--+--+

T = 0: multicast permanente (asignada por IANA)

T = 1: multicast temporaria (no asignada por IANA)

P see in [RFC3306], R see [RFC3956].



Multicast scope

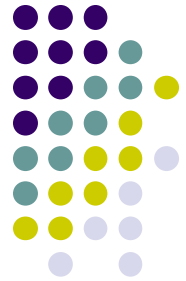
Valor	Descripción
1	Interfaz
2	(loopback)
Enlace	
3	Subred
4	Admin (configurado)
5	Site
8	Organización
E	Global
0,F	Reservados
6,7,9,A	No distribuídos
B,C,D	

Dirección	Alcance	Descripción
FF01::1	Interfaz	Todas las interfaces (<i>all-nodes</i>)
FF01::2	Interfaz	Todos los routers (<i>all-routers</i>)
FF02::1	Enlace	Todos los nodos (<i>all-nodes</i>)
FF02::2	Enlace	Todos los routers (<i>all-routers</i>)
FF02::5	Enlace	Routers OSFP
FF02::6	Enlace	Routers OSPF designados
FF02::9	Enlace	Routers RIP
FF02::D	Enlace	Routers PIM
FF02::1:2	Enlace	Agentes DHCP
FF02::1:FFXX:XXXX	Enlace	<i>Solicited-node</i>
FF05::2	Site	Todos los routers (<i>all-routers</i>)
FF05::1:3	Site	Servidores DHCP en un site
FF05::1:4	Site	Agentes DHCP en un site
FF0X::101	Variado	NTP (<i>Network Time Protocol</i>)



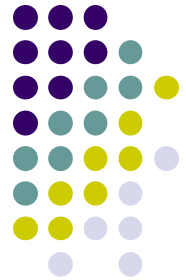
Multicast Solicited-Node

- Todos los nodos deben formar parte de este grupo;
- Se forma agregando el prefijo **FF02::1:FF00:0000/104** a los 24 bits más a la derecha del IID;
- Utilizado por el protocolo de Descubrimiento de Vecinos (*Neighbor Discovery*).



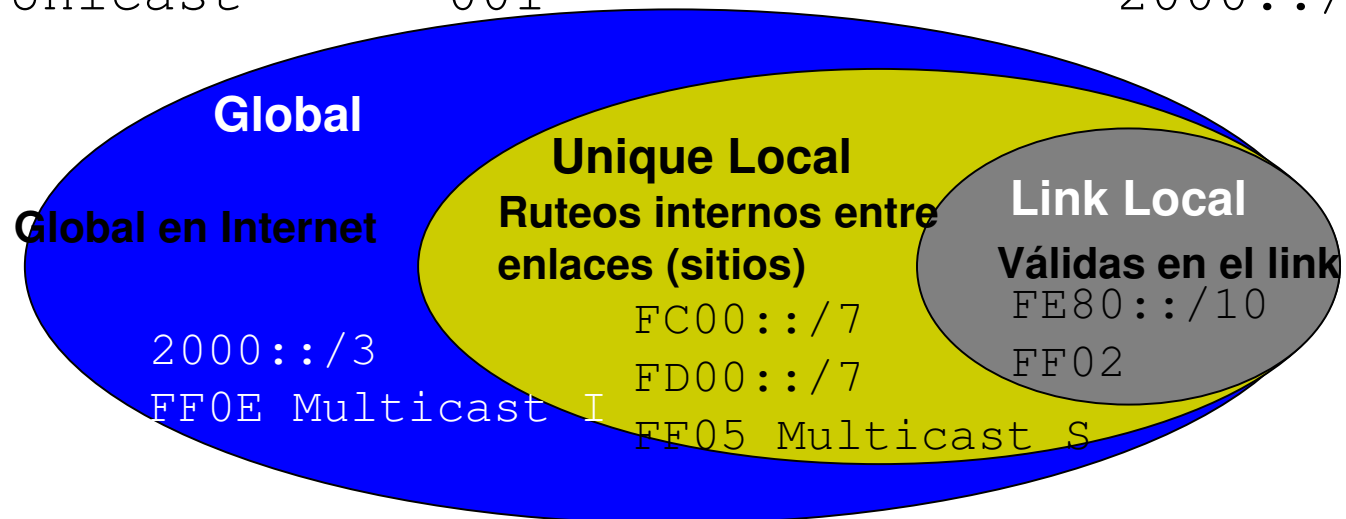
Direccionamiento:

- Al igual que en IPv4, las direcciones IPv6 se asignan a interfaces físicas y no a nodos.
- Con IPv6 es posible atribuir una única interfaz a múltiples direcciones, independientemente de su tipo.
- Así un nodo se puede identificar a través de cualquier dirección de sus interfaces.
 - Loopback **::1**
 - Link Local **FE80:....**
 - Unique local **FD07:...**
 - Global **2001:....**



Direcciones de una interfaz

Address type	Binary prefix	IPv6 notation
-----	-----	-----
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111 (8 bits)	FF00::/8
Link-Local unicast	1111111010	FE80::/10
Unique-Local unicast	11111110	FC00::/7
Global Unicast	001	2000::/3





Revisión direcciones

1. Describa los distintos tipos de direcciones: scopes.
2. Por qué tipo de direcciones se cambiaron las broadcast?
3. Si tengo un servidores de tiempo (NTS) con una dirección de grupo fija ID=101 hexa: cuál es la dirección que debe usar un nodo fuente para enviarles un mensaje a todos los NTSs de su mismo link? Y si quiere enviarles a todos los del mismo sitio?

Table 24. IPv6 - Format prefix allocation

Allocation	Prefix (bin)	Start of address range (hex)	Mask length (bits)	Fraction of address space
Reserved	0000 0000	0::/8	8	1/256
Reserved for NSAP	0000 001	200::/7	7	1/128
Reserved for IPX	0000 010	400::/7	7	1/128
Aggregatable Global Unicast Addresses	001	2000::/3	3	1/8
Link-local Unicast	1111 1110 10	FE80::/10	10	1/1024
Site-local Unicast	1111 1110 11	FEC0::/10	10	1/1024
Multicast	1111 1111	FF00::/8	8	1/256
Total Allocation				15%



ICMP/Neighbor Discovery- Autoconfiguration/PMTUD/ QoS/Coexistence issues

Internet Control Message Protocol
v6



- **ICMP/**
- Neighbor Discovery-Autoconfiguration/
- PMTUD/
- QoS/
- Coexistence issues



ICMPv6 RFC 4443

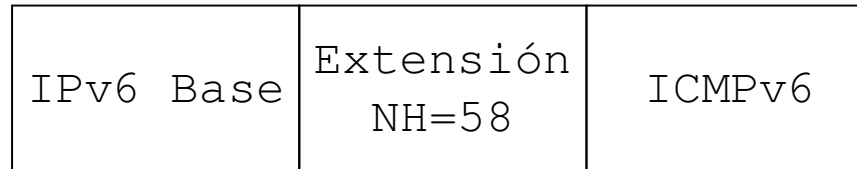
Internet Control Message Protocol

- Mismas funciones que ICMPv4 (pero no compatibles):
 - Informar características de la red;
 - Realizar diagnósticos;
 - Informar errores en el procesamiento de paquetes.
- Asume las funcionalidades de otros protocolos:
 - ARP/RARP (*Address Resolution Protocol*)
 - IGMP (*Internet Group Management Protocol*)
 - Identificado por Next Header = 58
 - Se **debe** implementar en todos los nodos



ICMPv6

- Está después del encabezado base y extensión



- Utilizado para las funcionalidades IPv6:
 - Gestión de grupos multicast (Multicast Listener Discovery)
 - Descubrimiento de vecinos (Neighbor Discovery, ND)
 - Movilidad IPv6
 - Descubrimiento de la Path MTU (Maximun Transmisit Unit)



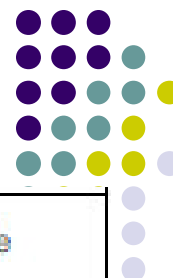
ICMPv6

Tipo	Nombre	Descripción
1	Destination Unreachable	Indica fallas en la entrega del paquete (como dirección o puerto desconocido) o problemas en la comunicación.
2	Packet Too Big	Indica que el tamaño del paquete es mayor que la Unidad Máxima de Transferencia (MTU) de un enlace.
3	Time Exceeded	Indica que el Límite de Direccionamiento o el tiempo de ensamble del paquete fue excedido.
4	Parameter Problem	Indica un error en alguno de los campos del encabezado IPv6 o que el tipo indicado en el campo Siguiendo Encabezado no fue reconocido.
100-101		Uso experimental
102-126		No utilizados
127		Reservado para la expansión de mensajes de error ICMPv6



Tipo	Nombre	Descripción
128	Echo Request	Utilizados por el comando ping.
129	Echo Reply	
130	Multicast Listener Query	Utilizados en la gestión de grupos <i>multicast</i> .
131	Multicast Listener Report	
132	Multicast Listener Done	
133	Router Solicitation	Utilizados con el protocolo de Descubrimiento de Vecinos.
134	Router Advertisement	
135	Neighbor Solicitation	
136	Neighbor Advertisement	
137	Redirect Message	
138	Router Renumbering	Utilizado en el mecanismo de re-direccionamiento(<i>Renumbering</i>) de routers.
139	ICMP Node Information Query	Utilizados para descubrir datos sobre nombres y direcciones, actualmente están limitados a herramientas de diagnóstico, depuración y gestión de redes.
140	ICMP Node Information Response	

Motivaciones y Orígenes de Ppv6 - Objetivos de Diseño - Datagrama y Cabeceras – Direcciones -
Funcionalidades



141	Inverse ND Solicitation Message	Utilizados en una extensión del protocolo de Descubrimiento de Vecinos.
142	Inverse ND Advertisement Message	
143	Version 2 Multicast Listener Report	Utilizado en la gestión de grupos <i>multicast</i> .
144	HA Address Discovery Req. Message	Utilizados en el mecanismo de Movilidad IPv6.
145	HA Address Discovery Reply Message	
146	Mobile Prefix Solicitation	
147	Mobile Prefix Advertisement	
148	Certification Path Solicitation Message	Utilizados por el protocolo SEND.
149	Cert. Path Advertisement Message	
150		Utilizado experimentalmente con protocolos de movilidad como <i>Seamoby</i> .
151	Multicast Router Advertisement	Utilizados por el mecanismo <i>Multicast Router Discovery</i>
152	Multicast Router Solicitation	
153	Multicast Router Termination	

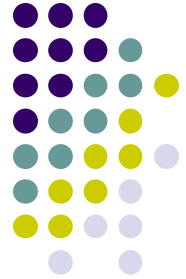


- ICMP/
- **Neighbor Discovery-Autoconfiguration/**
- PMTUD/
- QoS/
- Coexistence issues



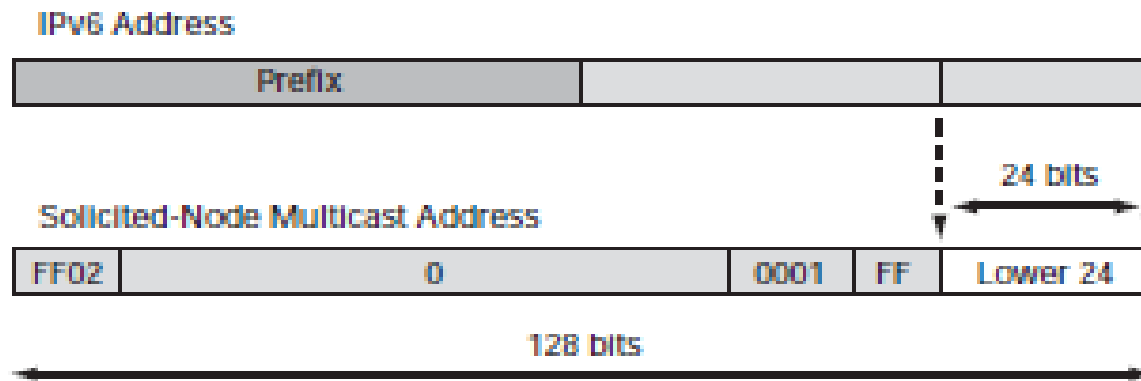
Descubrimiento de vecinos (RFC 4861)

- Utilizado por los *hosts* y routers para:
 - A. Determinar la MAC de los nodos de la red;
 - B. Encontrar routers vecinos;
 - C. Determinar prefijos y otros datos de configuración de la red;
 - D. Detectar direcciones duplicadas;
 - E. Determinar la accesibilidad de los routers;
 - F. Redireccionamiento de paquetes;
 - G. Autoconfiguración de direcciones

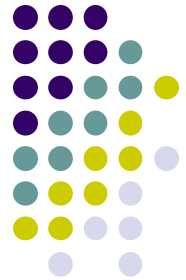


Multicast Solicited-Node

Figure 13: IPv6 Solicited-Node Multicast Address Format

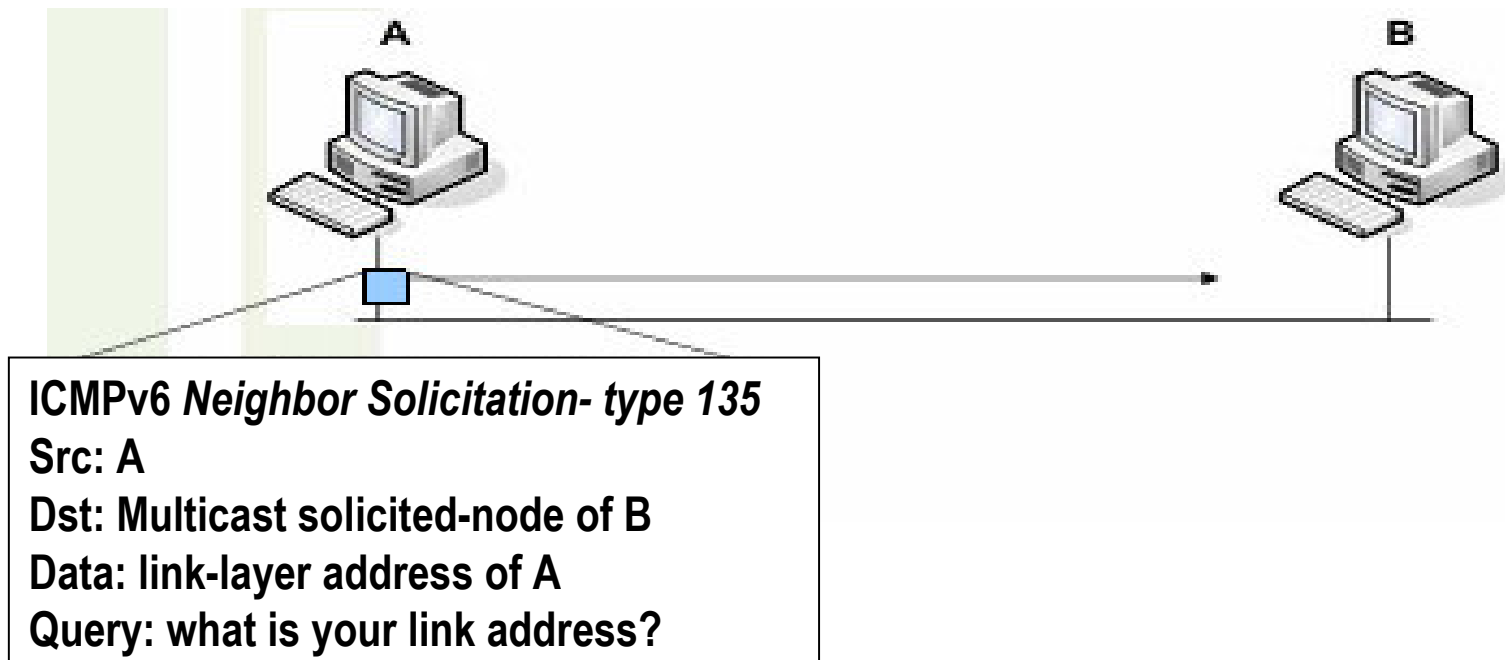


- For example, the solicited-node multicast address corresponding to the IPv6 address 2037::01:800:200E:8C6C is FF02::1:FF0E:8C6C.



ND A- Descubrimiento de MACs

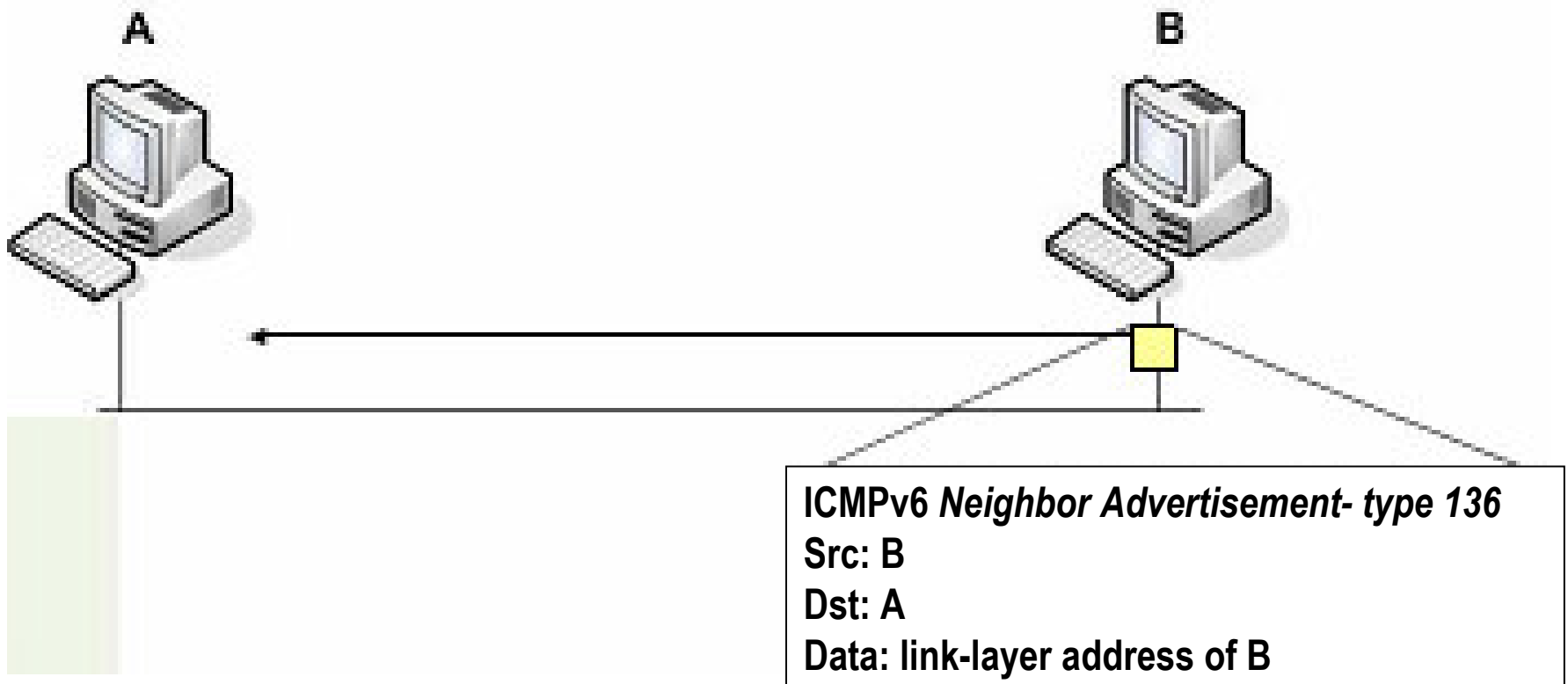
- Determina la MAC de los vecinos del mismo enlace (ARP en IPv4).
 - Usa la dir. de multidifusión de nodo solicitado (**multicast solicited-node**) en lugar de la dir. broadcast.
1. El host envía un mensaje NS informando su dirección MAC y solicita la dirección MAC del vecino.



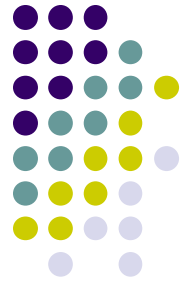


ND A- Descubrimiento de MACs

1. El vecino responde enviando un mensaje NA informando su dirección MAC.

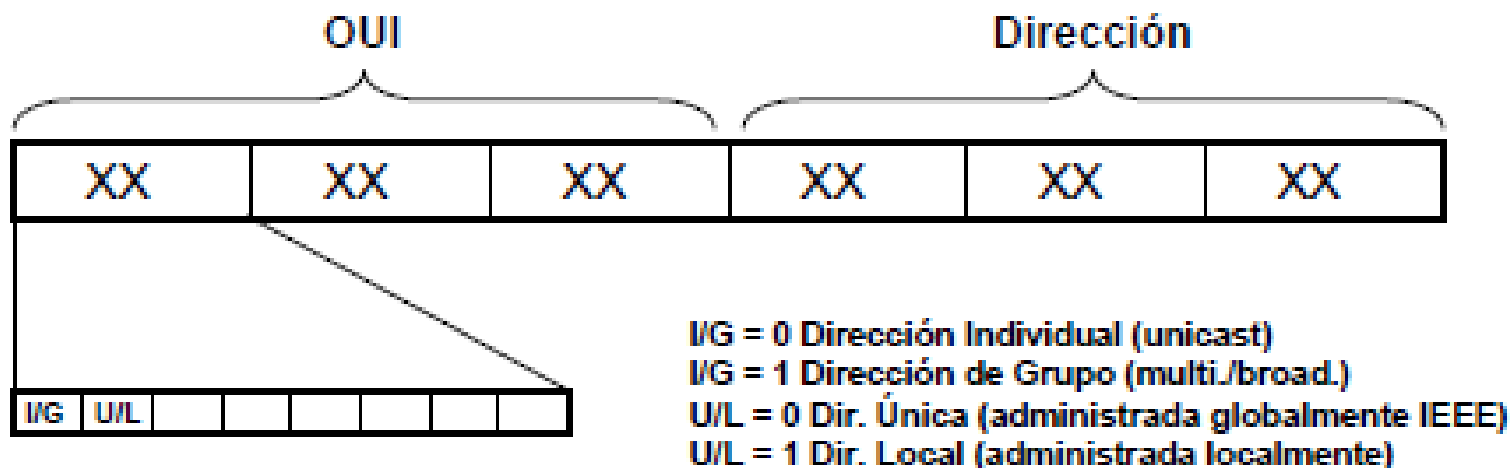






ND: IPv6 Multicast and Layer 2

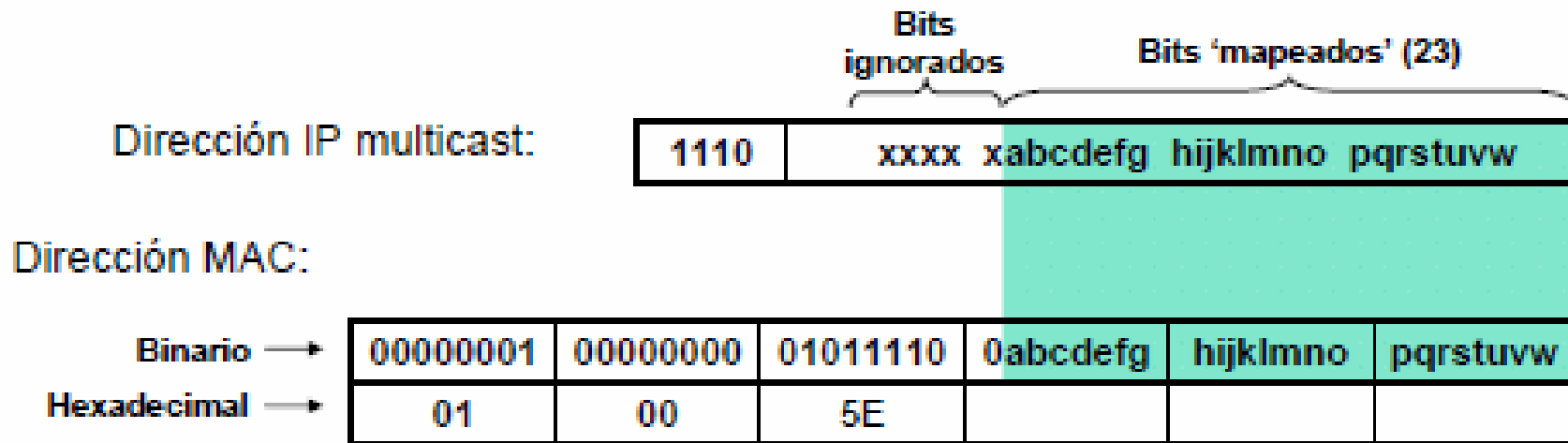
Direcciones multicast en Ethernet:



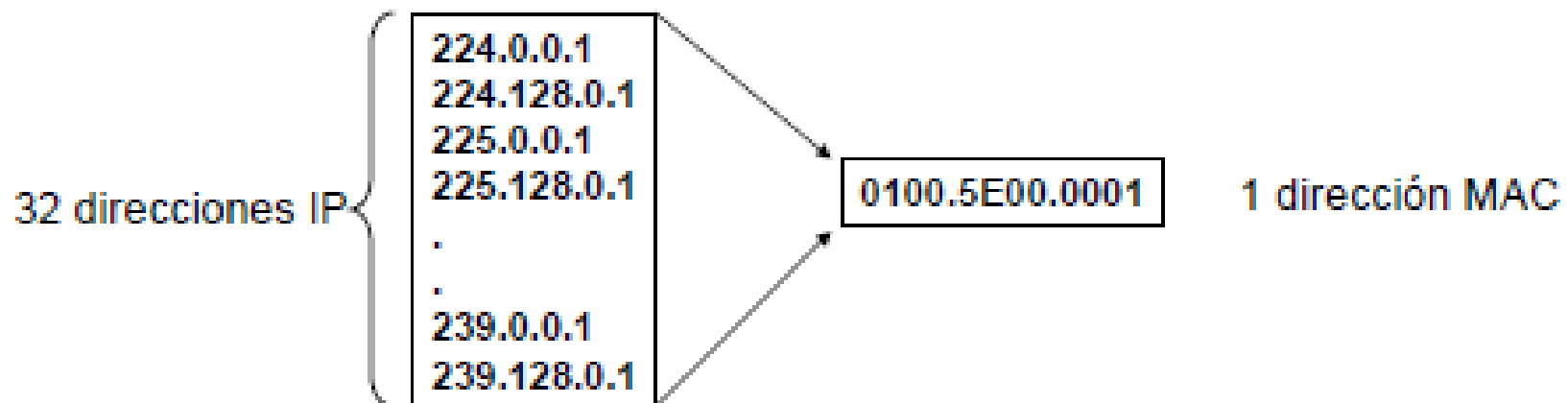
- En Ethernet los bits dentro de cada byte se representan en orden inverso. Por tanto el bit I/G es el último del primer byte.



Resolución direcciones multicast IP-Ethernet



Correspondencia no biunívoca:

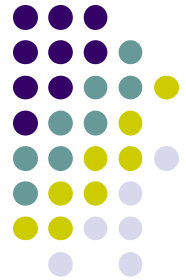




ND B- Encontrar routers vecinos;

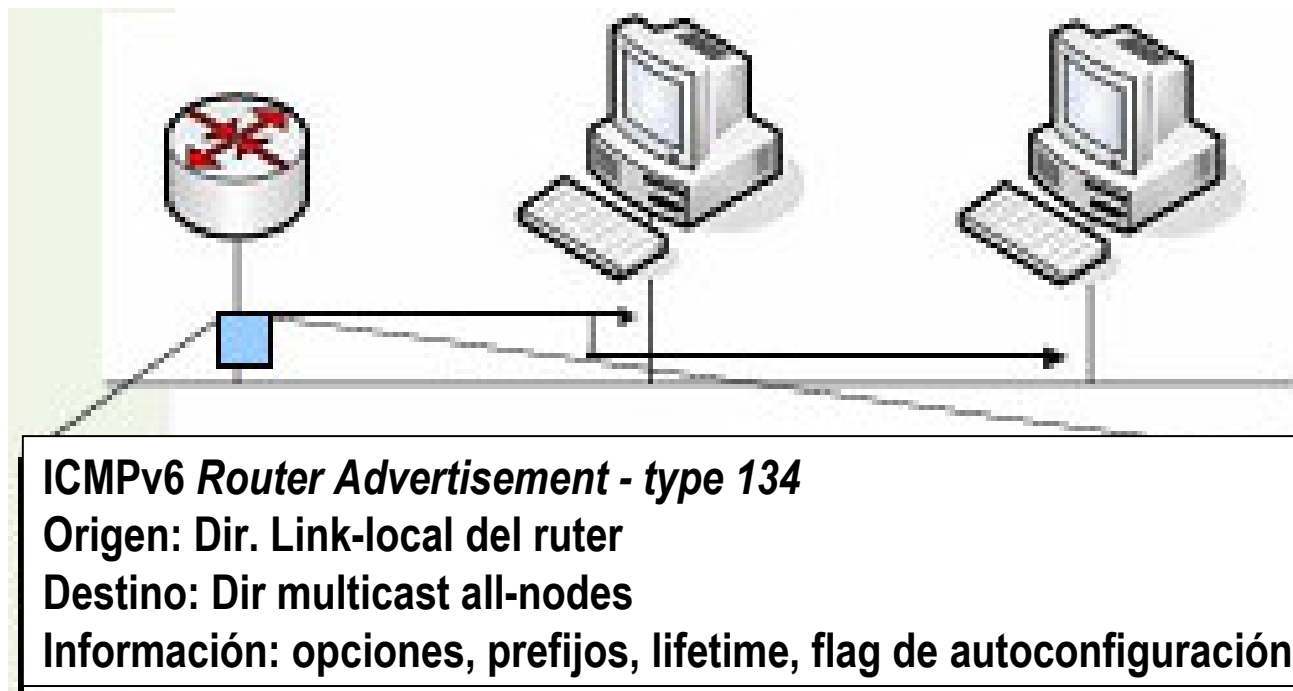
IPv6 router discovery is a process used by IPv6 nodes **to discover the routers** on the local link. The IPv6 router discovery process uses the following messages:

- Router advertisements
- Router solicitations



ND B- Descubrimiento de routers y prefijos

- Localizar routers vecinos dentro del mismo enlace.
- Determina prefijos y parámetros relacionados con la autoconfiguración de direcciones.
- Los routers envían periódicamente mensajes RA a la dirección multicast all-nodes (FF02::1).





Autoconfiguración

Mecanismo seguido por un HOST para autoconfigurar interfaces IPv6

- **Stateful:** provista por un servidor de dir. (DHCPv6)
- **Stateless:** un HOST genera su propia dir. Combinando la Ix local disponible + la brindada por los routers (que anuncian prefijos de subred asociados al enlace)



ND G- Autoconfiguración de direcciones

- Mecanismo para asignar direcciones *unicast* a los nodos...
 - sin configuraciones manuales.
 - sin servidores adicionales.
 - con una configuración mínima de los routers.
- Se generan direcciones IP a partir de información de los routers (Router Advertisement) y la dirección MAC.
 - Genera una dirección para cada prefijo informado en los mensajes RA.
 - Si no hay routers presentes en la red solamente se genera una dirección *link local*: FE80::/64+IID(MAC).



ND G- Autoconfiguración de direcciones

- 1) Se genera una dirección *link-local*.
Prefijo **FE80::/64** + IID(MAC)
- 2) Esta dirección pasa a formar parte de los grupos *multicast solicited-node* y *all-node*.
- 3) Se verifica la unicidad de la dirección
 - Si la dirección ya está siendo utilizada el proceso se interrumpe, requiriéndose una configuración manual.
 - Si la dirección es única y válida, se atribuye a la interfaz.
- 4) El *host* envía un mensaje Router Solicitation al grupo *multicast all-routers*.
- 5) Todos los routers del enlace responden con mensajes Router Advertisement informando: lista de prefijos, MTUs,...



- ICMP/
- Neighbor Discovery-Autoconfiguration/
- **PMTUD/**
- QoS/
- Coexistence issues



Ej: MTU Path Discovery (RFC 1191)

- Objetivo: evitar la fragmentación averiguando la Mínima MTU de todos los caminos entre el origen y el destino

¿Cómo conseguirlo?

- Se establece un tamaño tentativo inicial de datagrama: el del primer 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
 - El algoritmo garantiza convergencia de tamaño de datagramas



Path MTU Discovery: PMTUD

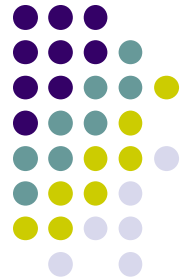
- Path MTU Discovery – Busca garantizar que el paquete encaminado sea del mayor tamaño posible.
- MTU - Maximum Transmit Unit – Tamaño máximo de paquete que puede atravesar el enlace entre una fuente y un destino.
- Fragmentación – Permite enviar paquetes mayores que la MTU de un enlace.
 - IPv4 – Todos los routers pueden fragmentar paquetes mayores que la MTU del siguiente enlace=> IPv4 puede fragmentar más de una vez durante su trayecto.
 - **IPv6 – La fragmentación se realiza solamente en el origen.**
- Todos los nodos IPv6 deben soportar PMTUD.
- Las implementaciones mínimas de IPv6 pueden omitir este soporte, utilizando 1280 bytes como máximo tamaño de paquete.



PMTU Discovery Process

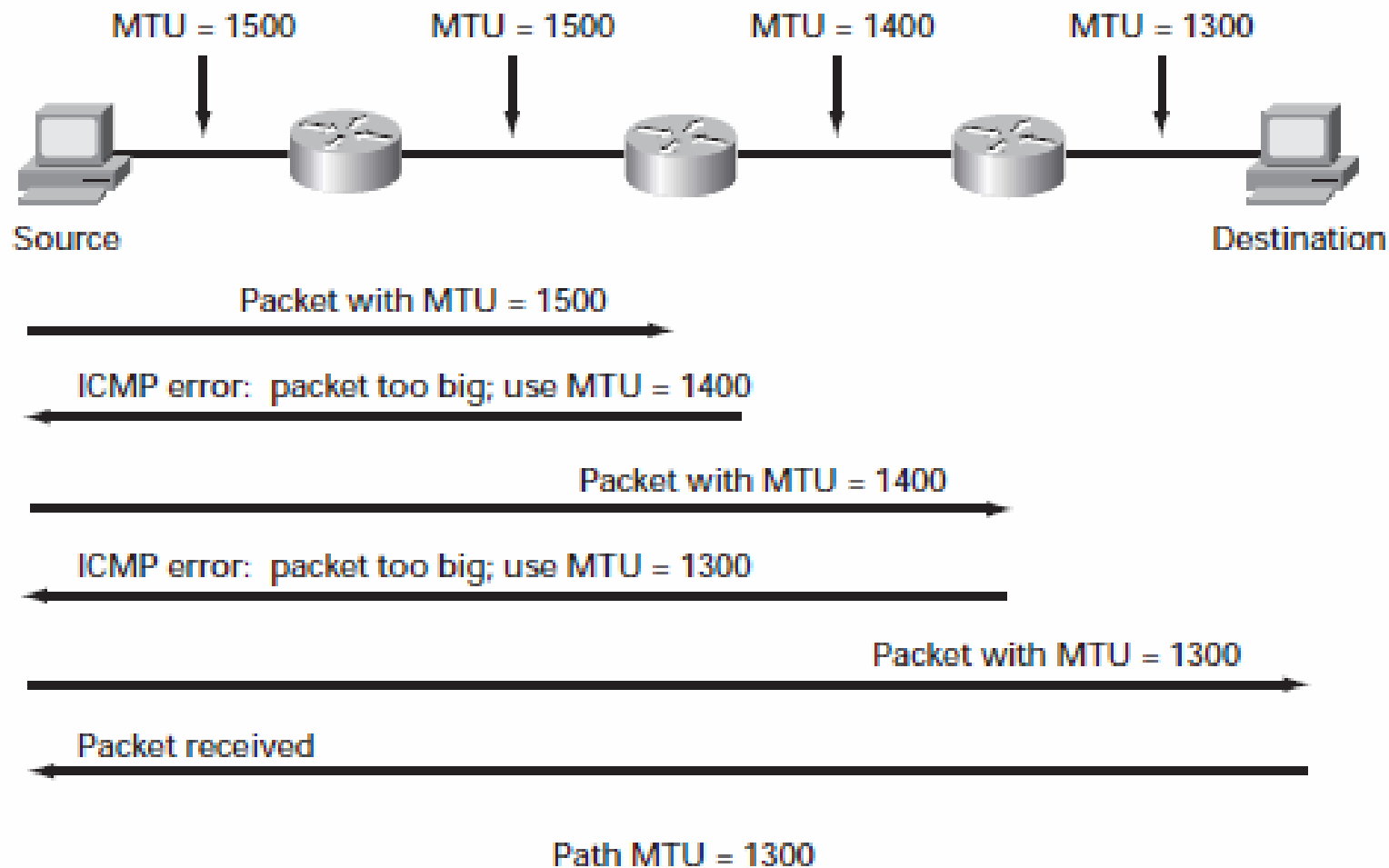
1. Send a message to the destination with MTU of your link;
2. If receive a ICMP error message, then resend the message with the new MTU;
3. Do 1 and 2 until response from destination;
4. Last MTU is the Path MTU.

Los paquetes enviados a un grupo multicast utilizan un tamaño igual a la menor PMTU de todo el conjunto de destinos



Ej. Fragmentación (ABCs of IP Version 6)

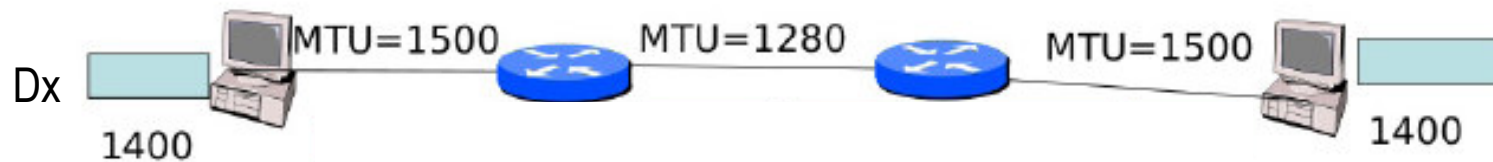
Figure 16: Path MTU Discovery



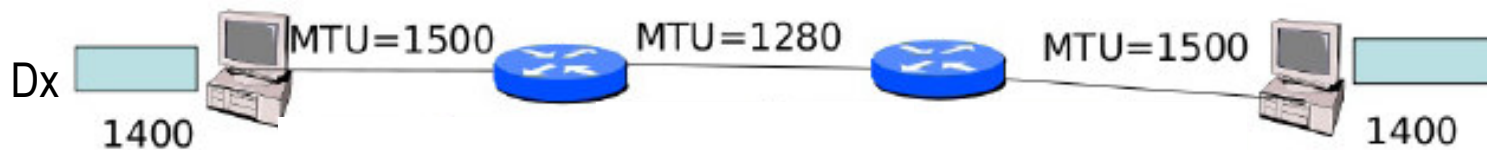


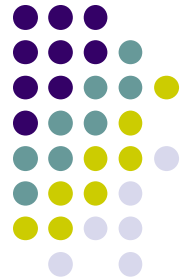
Ej. Fragmentación

IPv4



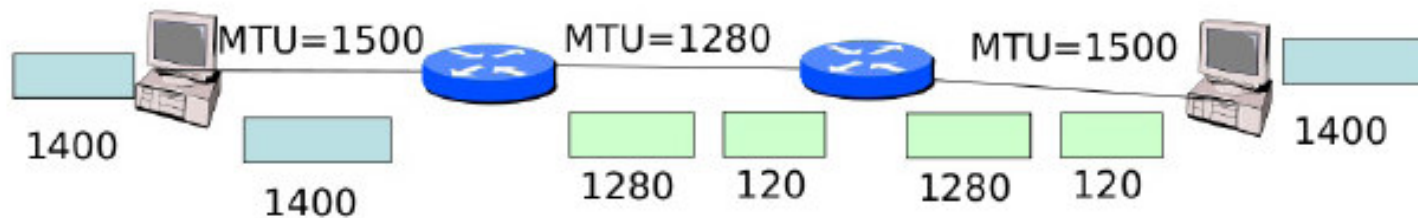
IPv6



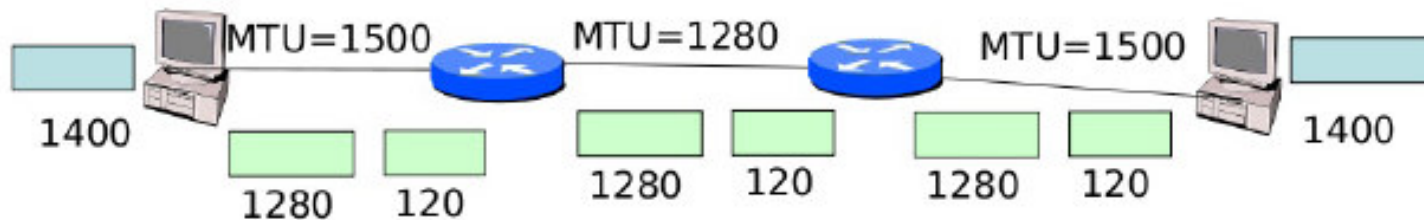


Ej. Fragmentación

IPv4



IPv6

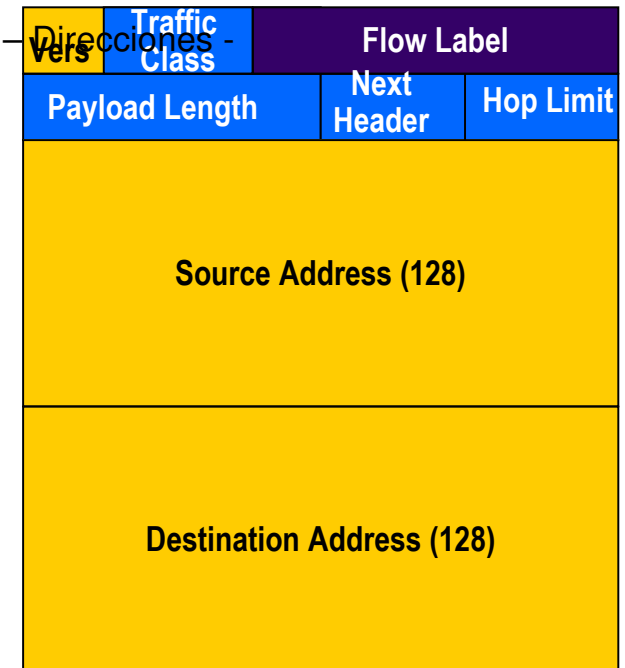




- ICMP/
- Neighbor Discovery-Autoconfiguration/
- PMTUD/
- **QoS/**
- Coexistence issues

Calidad de Servicio:

- 2 campos para QoS:



- **Clase de Tráfico:** utilizado en DiffServ (DSCP)
- **Identificador de Flujo:** identifica flujos desde un origen a un destino con una determinada QoS



Modelos de Calidad de Servicio

1. Best Effort Internet
2. Integrated Services (IntServ)
3. Differentiated Services (DifServ)



1. Best Effort

- Todos los paquetes son tratados igual
- No provee calidad o garantía de tráfico
 - AB, retardo, jitter no predecibles

Las garantías se proveen con
sobre-provisionamiento



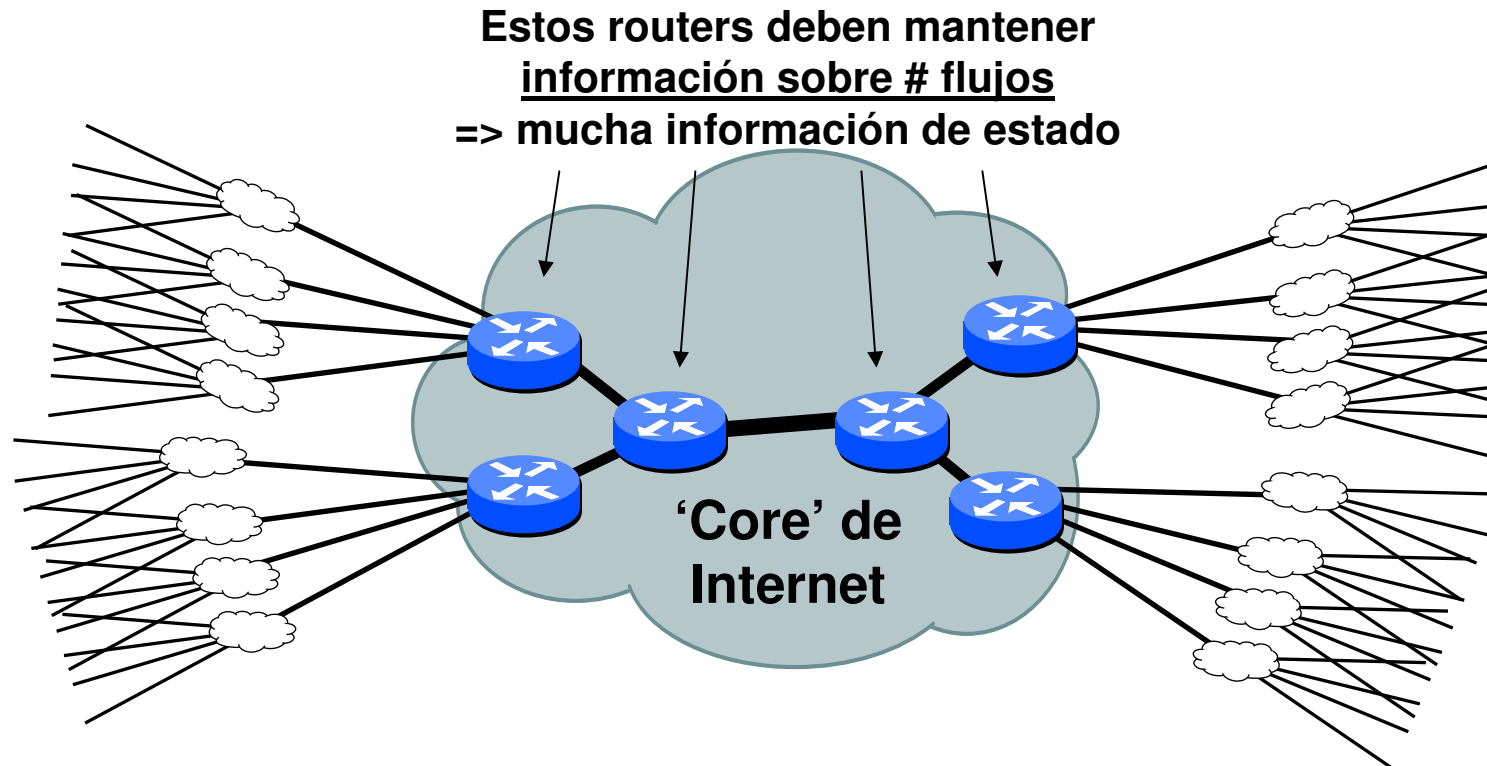
2. Integrated Services

- Para intercambiar Ix con QoS hacen reserva de recursos (RSVP).
- Desventajas:
 - **Señalización y reserva** por cada flujo
 - Deben enviarse Mxs de **refresco**
 - **RSVP** es complejo
 - Necesidad de mantener **información de estado** en cada router de cada flujo



2. Integrated Services

- Problemas de escalabilidad





3. Differentiated Services

- Intenta evitar los problemas de escalabilidad que plantea IntServ/RSVP.
- **Modelo basado en el mercado de paquetes según la QoS.**



3. DiffServ RFC 2474

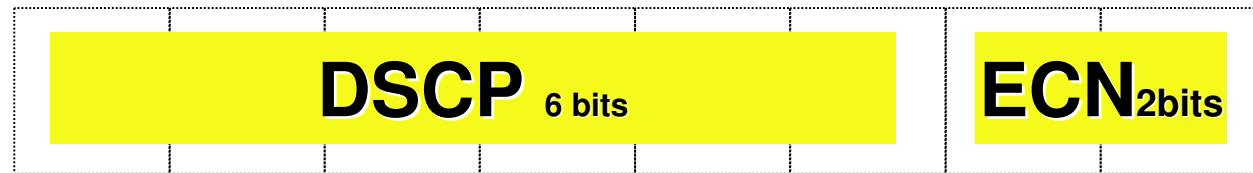
- Conjunto de **categorías**.
- Codificación en el **DSCP** (DiffServ Code Point).
- Contrato de servicio usuario-proveedor: **SLA** (Service Level Agreement).
- Dominios **DS** con **políticas comunes** de suministro de servicios.
- Los routers **no guardar información**.



DiffServ: Campo DS (traffic Class)



Campo DS



- **DSCP:** 3 bits codifican la clase + 3 bits detalles de la clase.
- **ECN:** Explicit congestion Notification (2 bits), indica congestión en un nodo.

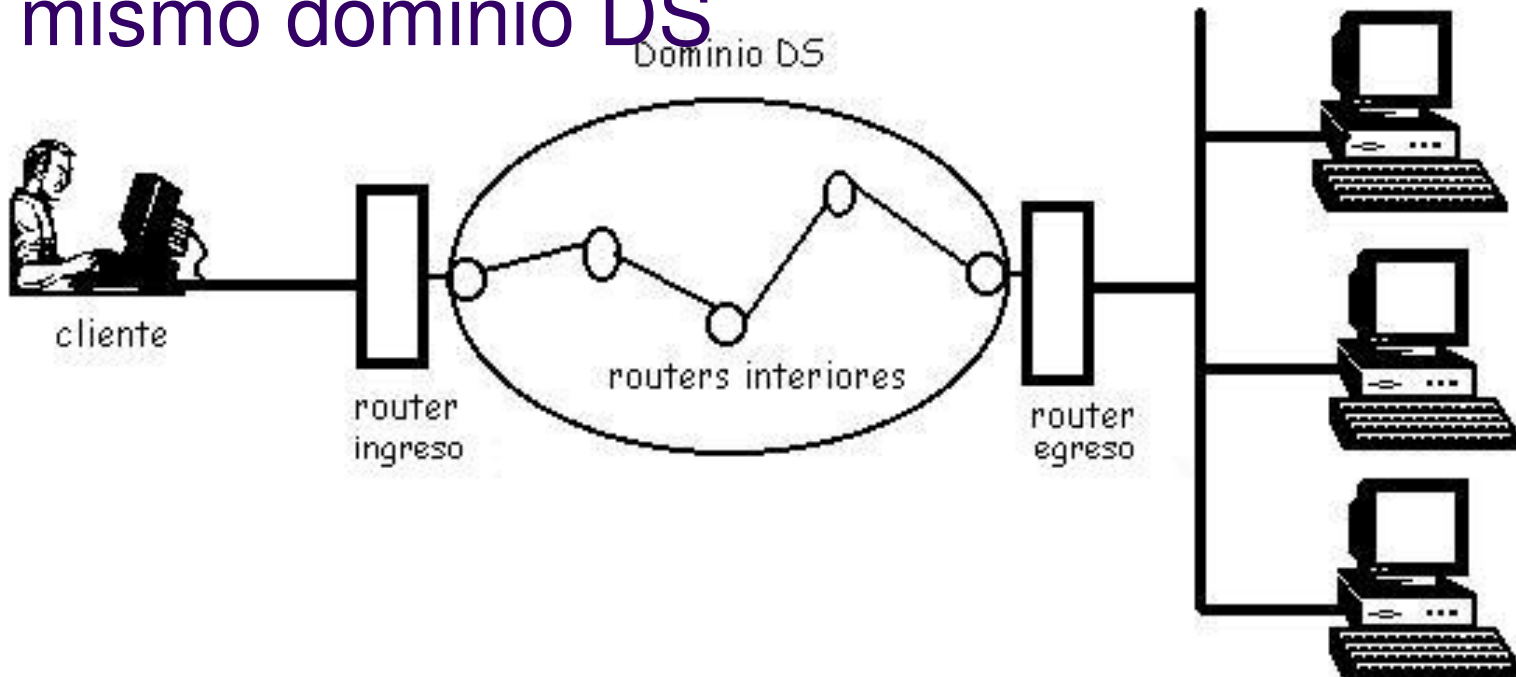


Clases de Servicio en DiffServ

(según valor de los DSCP)

Servicio	Características
‘Expedited Forwarding’ o ‘Premium’	- Es el que da más garantías. <u>Equivaldría a una línea dedicada</u> - Garantiza Caudal, tasa de pérdidas, retardo y jitter - DSCP en 101110
‘Assured Forwarding’	- Asegura un trato preferente, pero sin fijar garantías (no hay SLA) - Se definen cuatro clases y en cada una tres niveles de descarte de paquetes
‘Best Effort’ con prioridad	- Sin garantías, pero obtendrá trato preferente frente a ‘best effort sin prioridad’ - DSCP 000xxx
‘Best Effort’ sin prioridad	- Ninguna garantía - DSCP 000000

DiffServ: Ej. de comunicación en un mismo dominio DS

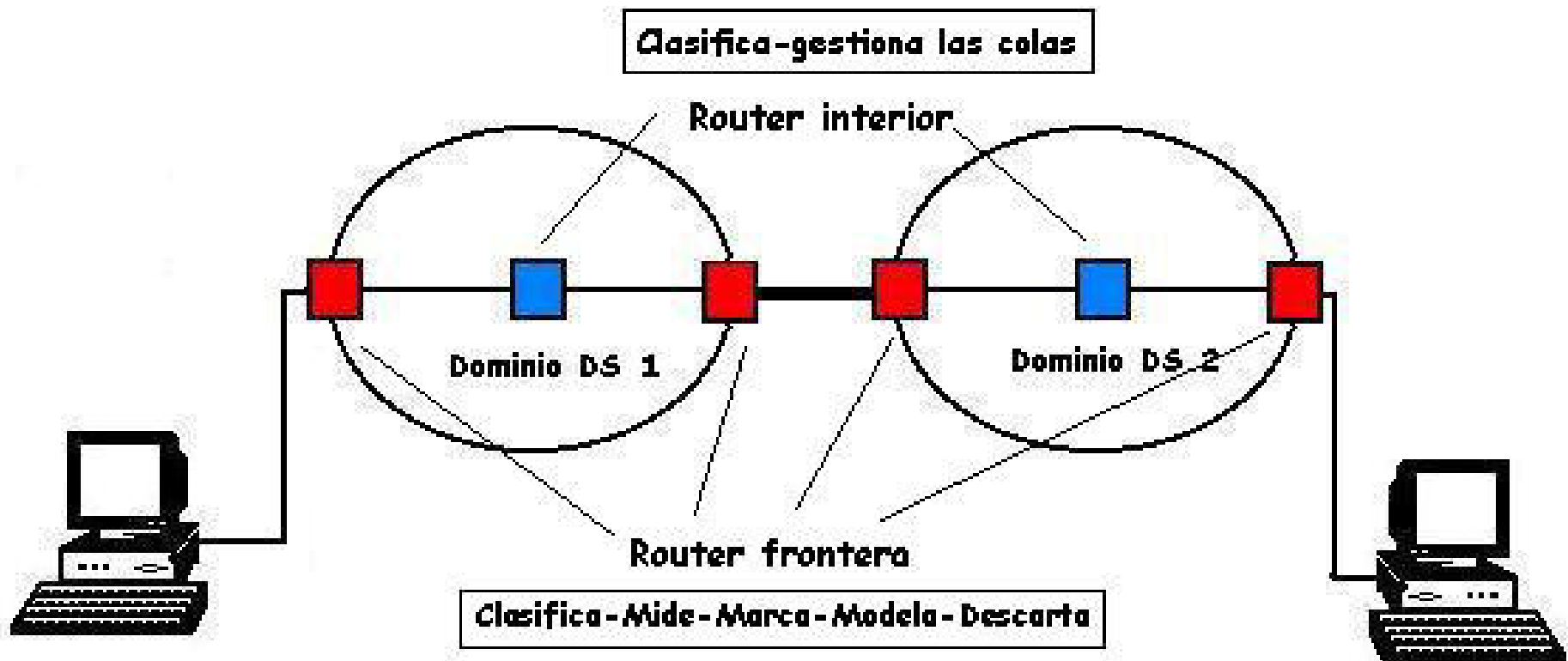


- El cliente pre-marca (DS) la información con una QoS.
- Router de entrada: clasifica el flujo y verifica el SLA.
En caso de no concordar:
 - Descarta (policing).
 - Acepta, pero modifica su prioridad en función del SLA (marking).



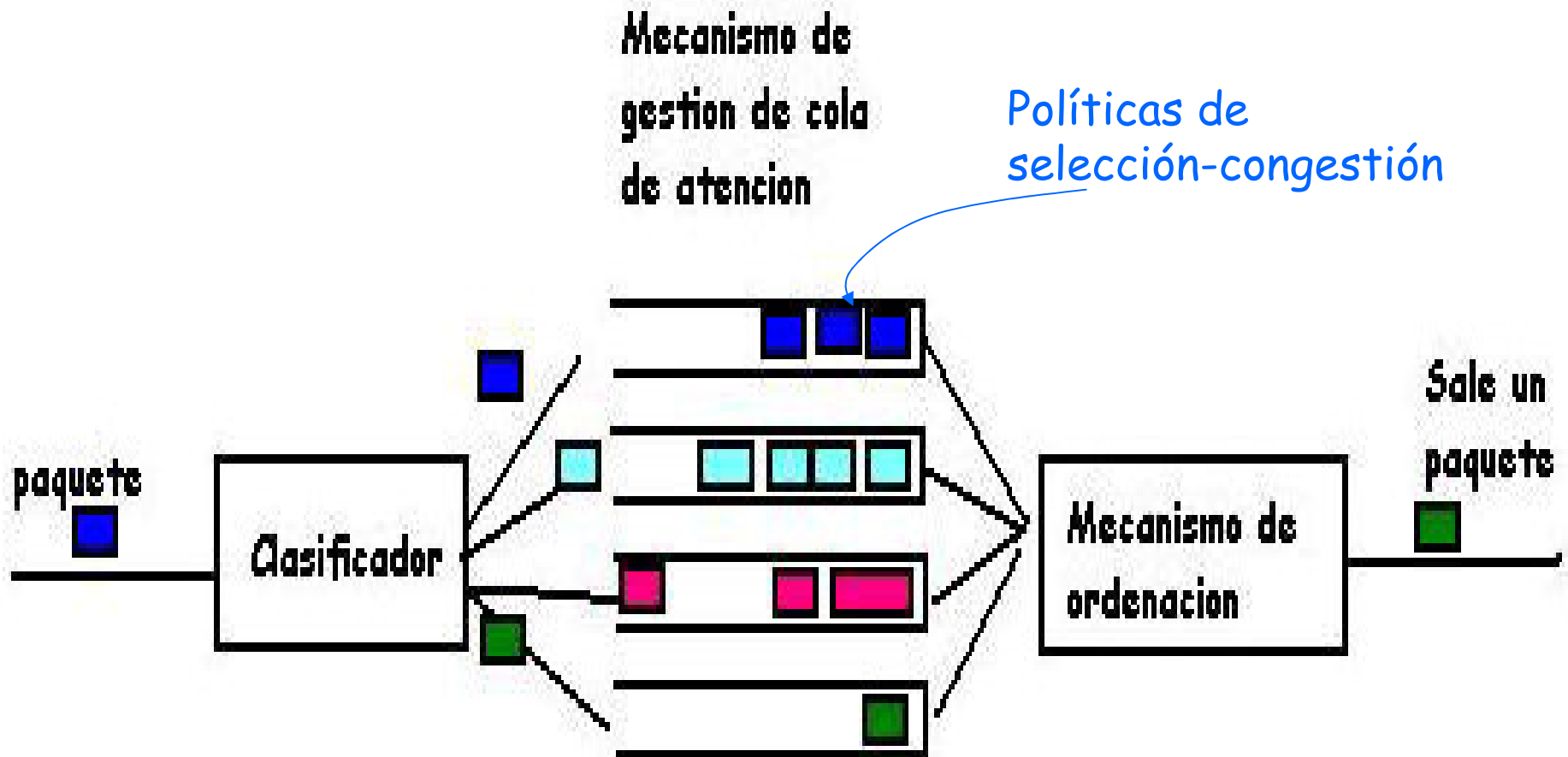


DiffServ: funciones de routers

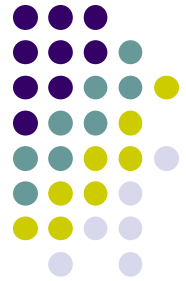




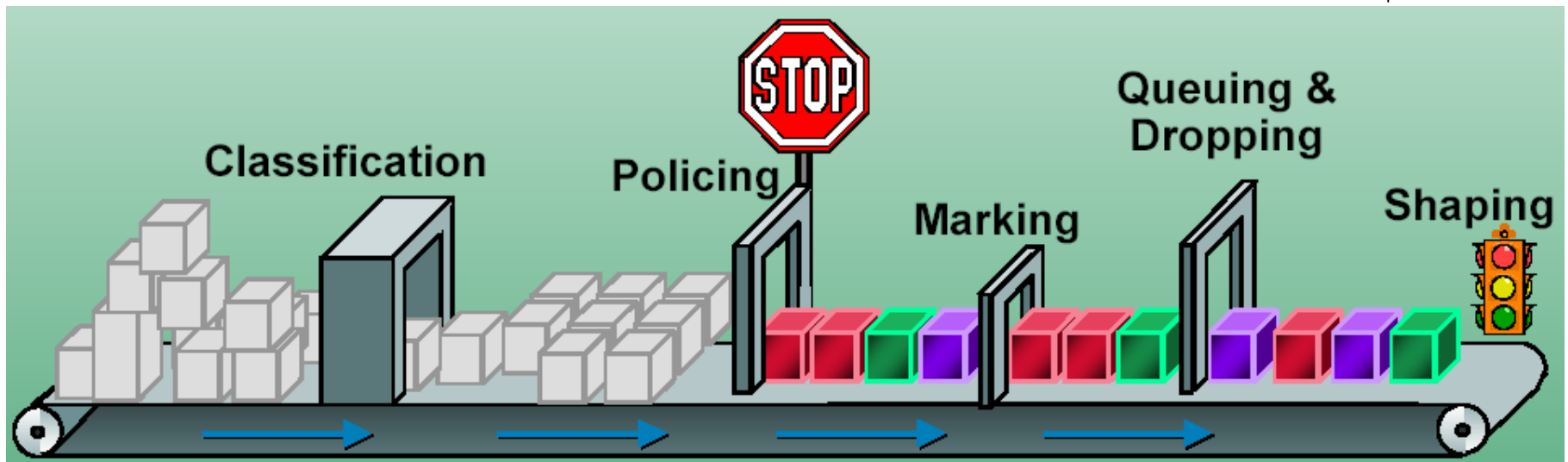
DiffServ: router interior



No modifican el valor del DS



Routers frontera DS: DiffServ



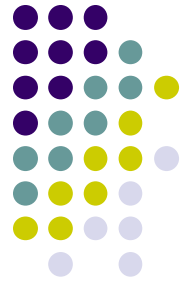
Classification:
Identifica y
separa tráfico
según clases

Policing (medidor):
verifica el caudal
de flujo de cada
clase vs. SLA,
Descarta tráfico
anómalo para
garantizar la
integridad de la red

Marking:
Marca tráfico,
si es
necesario.
Asigna al
DSCP el valor
que
corresponde

Q & D:
Prioriza y
aísla
tráfico

Shaping:
Controla
ráfagas y
retardos



Gestión de Colas

Método FIFO (First Input First Output)

- El primero que llega es el primero en ser atendido, si llega un paquete y no encuentra lugar en el buffer será eliminado.

Método RED (Random Early Detection)

Detecta una congestión incipiente computando el valor medio del tamaño de cola avg.

- **Fase1: Operación Normal**

Si el avg < minimum threshold, los paquetes avanzan en la red.

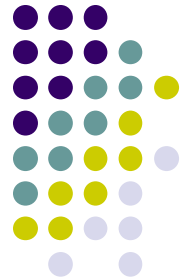
- **Fase2: Congestion Evitable**

Si el mínimo thr < avg < máximo thr, los paquetes son eliminados con una cierta probabilidad.

- **Fase3: Control de la Congestion (setea ECN)**

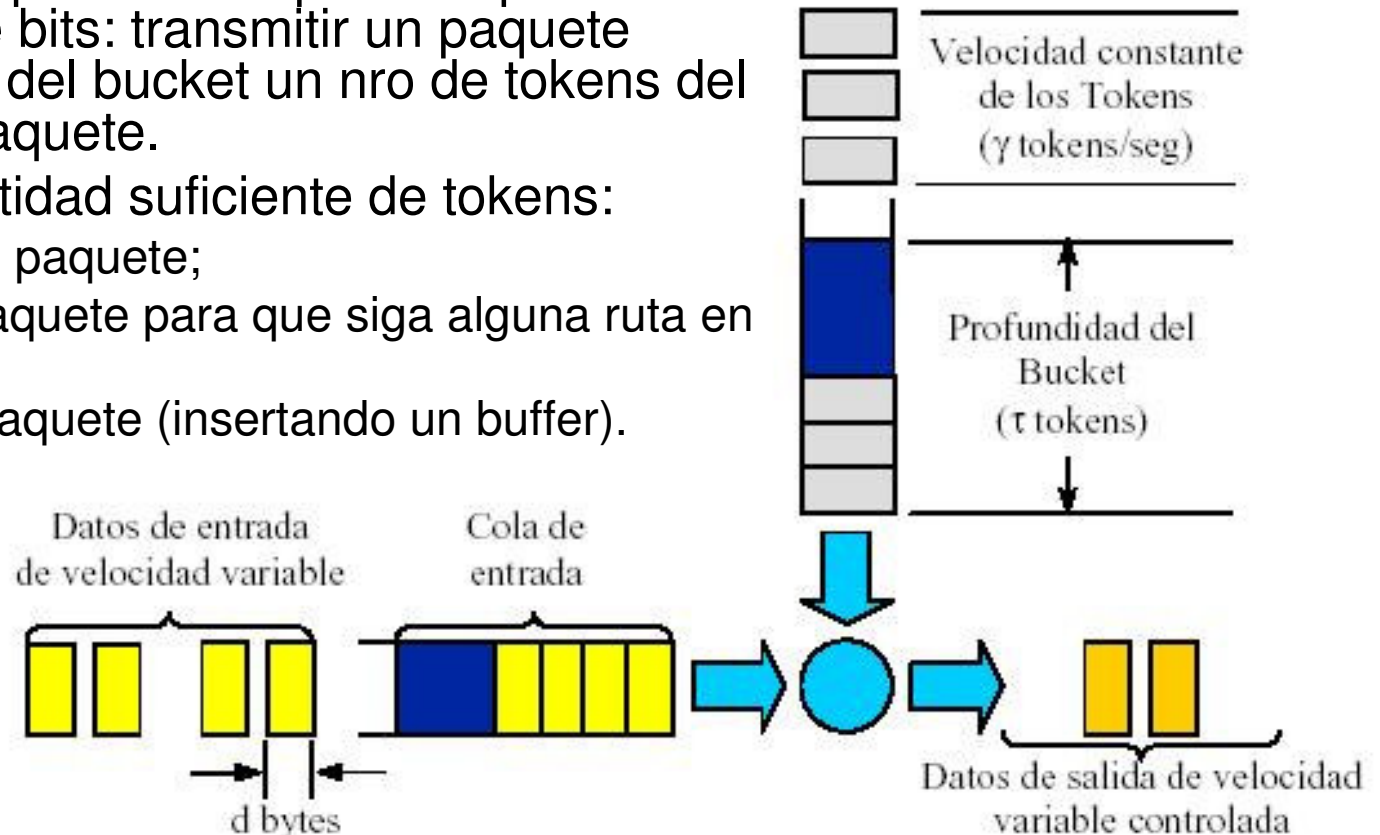
Si el avg > máximo thr, todos los paquetes entrantes son eliminados.

RED utiliza el azar para eliminar paquetes, así las eliminaciones sucesivas son evitadas.



Moldeador (shaper) Token Bucket

- Opera con 2 flujos: los paquetes y los tokens a una tasa γ .
- Cada token equivale a un permiso para transmitir un número de bits: transmitir un paquete implica tomar del bucket un nro de tokens del tamaño del paquete.
- Si no hay cantidad suficiente de tokens:
 1. Descartar al paquete;
 2. Marcar al paquete para que siga alguna ruta en particular;
 3. Encolar al paquete (insertando un buffer).

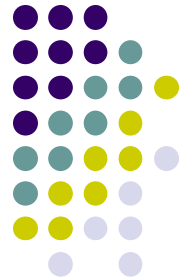




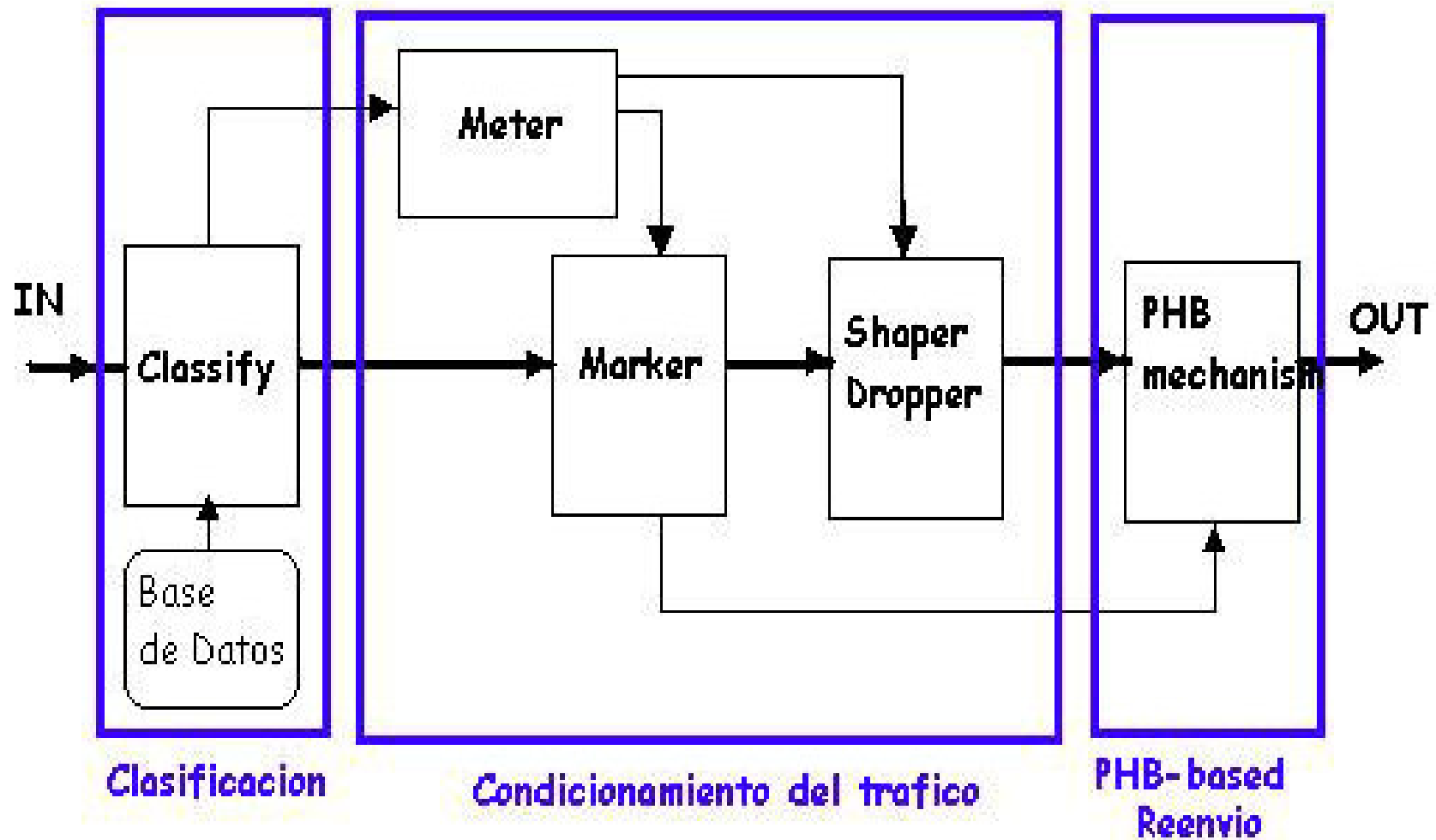
Shaper Token Bucket

Parámetros:

- γ es la tasa a la cual el flujo de datos saldrá del bucket.
- τ es la profundidad del bucket o máxima cantidad de información que puede salir del bucket en un burst.



DiffServ: funcionamiento





- ICMP/
- Neighbor Discovery-Autoconfiguration/
- PMTUD/
- QoS/
- **Coexistence issues**



Transición IPv4-IPv6

Mecanismos (RFC 1933)

- Capa IP dual: los routers y los host soportan IPv4 e IPv6
- Túneles de IPv6 sobre IPv4: los paquetes IPv6 se encapsulan con encabezados de IPV4

Coexistencia y transición ver

IPv6.br Módulo 7



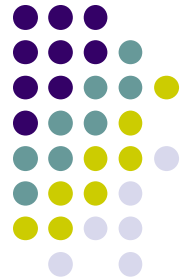
- Toda la estructura de Internet está basada en IPv4.
- Un cambio inmediato de protocolo es inviable debido al tamaño y a la proporción que tiene esta red.
- La adopción de IPv6 se debe realizar de manera gradual.
- Inicialmente habrá un período de transición y de coexistencia entre los dos protocolos.
- Las redes IPv4 necesitarán comunicarse con las redes IPv6 y viceversa.
- Para facilitar este proceso se han desarrollado algunas técnicas que buscan mantener la compatibilidad de toda la base instalada de redes IPv4 con el nuevo protocolo IPv6.



Coexistencia y transición

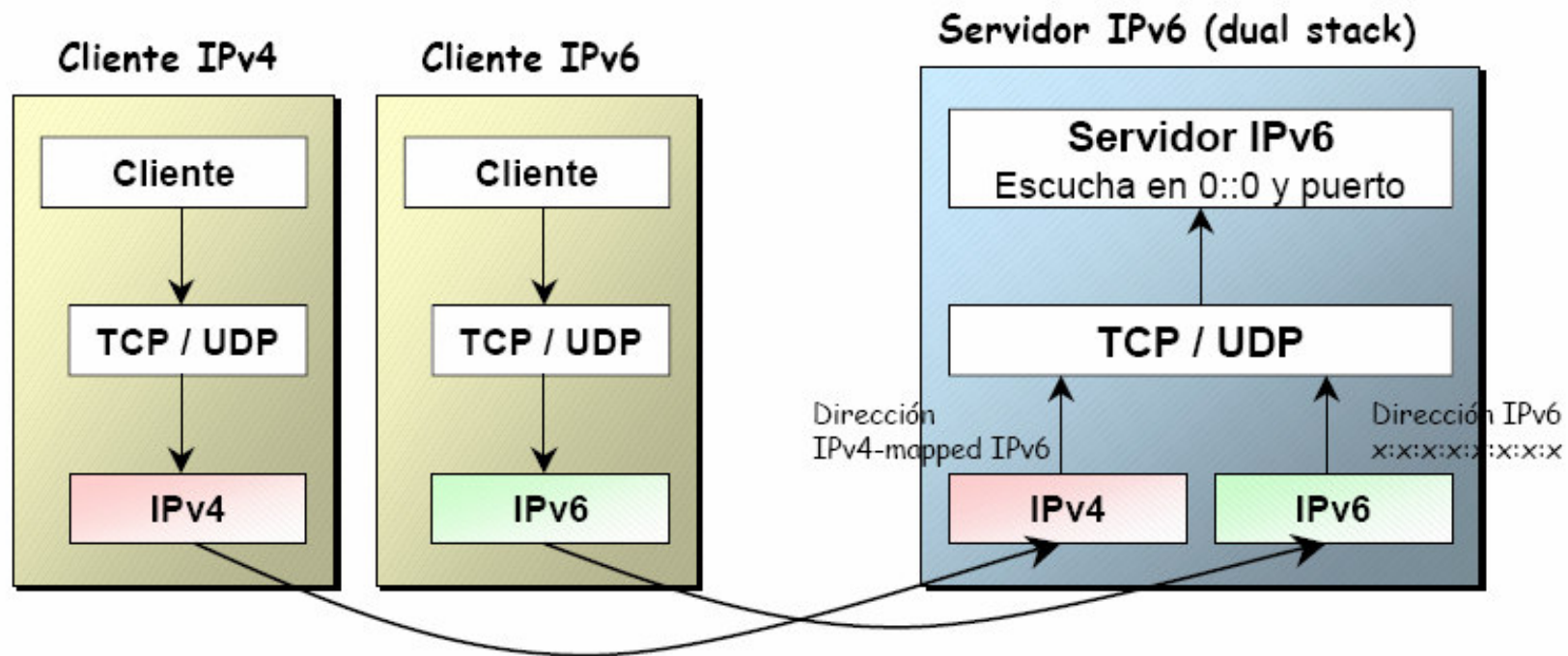
Estas técnicas de transición se dividen en 3 categorías:

- **Doble pila**
 - Provee soporte a ambos protocolos en el mismo dispositivo.
- **Tunelización**
 - Permite el tráfico de paquetes IPv6 sobre la estructura de la red IPv4 existente.
- **Traducción**
 - Permite la comunicación entre nodos que solo soportan IPv6 y nodos que solo soportan IPv4..



Cliente IPv4 - Servidor IPV6

- Servidores IPv6 sobre una máquina con dual stack aceptan conexiones de clientes IPv4 e IPv6.
- Necesitan al menos una dirección para cada pila. Para IPv4, p.ej., DHCP; para IPv6 , p.ej., autoconfiguraciónstateless



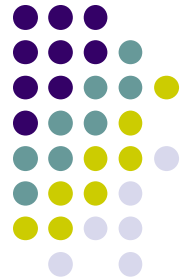


Doble Pila

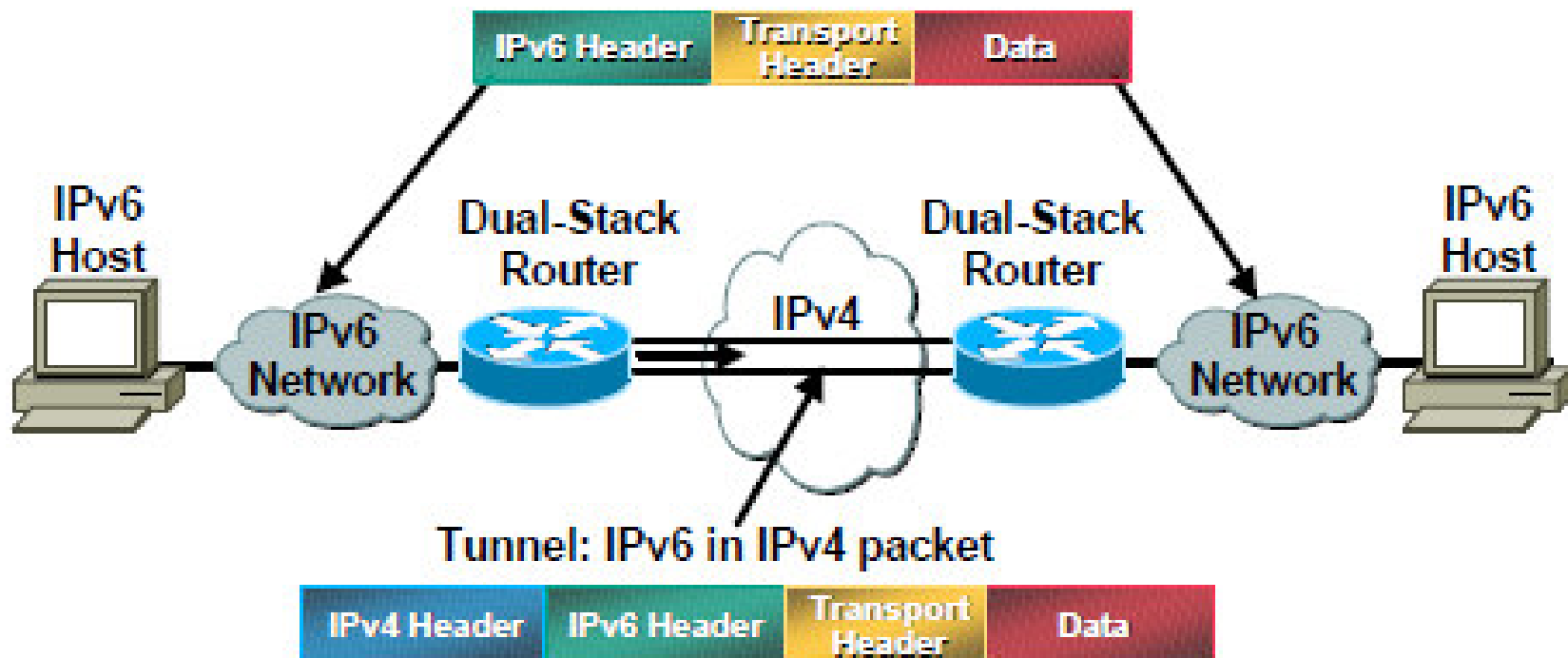
Una red doble pila es una infraestructura capaz de encaminar ambos tipos de paquetes.

Exige analizar algunos aspectos:

- Configuración de los servidores de DNS;
- Configuración de los protocolos de enrutamiento;
- Configuración de los *firewalls*;
- Cambios en la administración de las redes.



Tunneling





Tunneling

- También llamado encapsulamiento.
- El contenido del paquete IPv6 se encapsula en un paquete IPv4.
- Se pueden clasificar de la siguiente manera:
 - *Router-a-Router*
 - *Host-a-Router*
 - *Router-a-Host*
 - *Host-a-Host*



Tunneling: técnicas

Existen diferentes formas de encapsulamiento:

- Paquetes IPv6 encapsulados en paquetes IPv4;
 - Protocolo 41.
 - 6to4, ISATAP y *Tunnel Brokers*.
- Paquetes IPv6 encapsulados en paquetes GRE;
 - Protocolo GRE.
- Paquetes IPv6 encapsulados en paquetes UDP;
 - TEREDO.



Traducción RFC 4966

- Posibilitan un enrutamiento transparente en la comunicación entre los nodos de una red IPv6 y los nodos de una red IPv4 y viceversa.
- Pueden actuar de diversas maneras y en capas distintas:
 - Traduciendo encabezados IPv4 en encabezados IPv6 y viceversa;
 - Convirtiendo direcciones;
 - Convirtiendo APIs de programación;
 - Actuando en el intercambio de tráfico TCP o UDP

Revisión Funcionalidades



1. Describa para qué se usan y cómo son los mecanismos de:
 - Descubrimiento de vecinos
 - Autoconfiguración
 - Path MTU discovery
2. Describa los campos de la cabecera usados para proveer calidad de servicio
3. Describa los distintos tipos de servicio
4. Describa los mecanismos de coexistencia IPV6-IPV4



Técnicas de Traducción

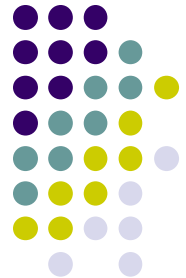
- SIIT (*Stateless IP/ICMP Translation*, RFC 2765) - Permite la comunicación entre nodos que solo soportan IPv6 y nodos que solo soportan IPv4.
- BIS (*Bump in the Stack*, RFC 2767) - Este método permite la comunicación de aplicaciones IPv4 con nodos IPv6.



Bibliografía

- TCP/IP Tutorial and Technical Overview. Rodriguez, Gatrell, Karas, Peschke. Ibm Redbooks, 2006.
- IPv6: The New Internet Protocol. Christian Huitema. Prentice Hall, 1998.
- IPng and the TCP/IP Protocols. Stephen A. Thomas. JohnWiley & Sons, 1996.
- IP Next Generation. <http://playground.sun.com/pub/ipng/tml/ipng-min.html>
- IPv6 Forum. <http://www.ipv6forum.com>
- IP Next Generation. R.M. Hinden. Connexions, vol. 9, núm. 3, Marzo 1995
- Kame distribution: <http://www.kame.net/>
- IPv6 applications: <ftp://ftp.kame.net/pub/kame/misc/>
- MRTd routing daemon: <http://www.mrtd.net/>
- Tunnel server: <http://www.freenet6.net>
- Tunnel broker: <http://carmen.cselt.it/ipv6/download.html>
- Viagénie's IPv6 project: <http://www.viagenie.qc.ca/>

RFC



- **"Core spec"**
 - RFC2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden, Draft standard, 1998-12-01.
 - RFC2461, Neighbor Discovery for IP Version 6 (IPv6), T. Narten, E. Nordmark, W. Simpson, Draft standard, 1998-12-01.
 - RFC2462, IPv6 Stateless Address Autoconfiguration, S. Thomson, T. Narten, Draft Standard, 1998-12-01.
 - RFC2463, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, A. Conta, S. Deering, Draft standard, 1998-12-01.
 - RFC1981, Path MTU Discovery for IP version 6, J. McCann, S. Deering, J. Mogul, Proposed standard, 1996-08-01.
- **Addressing**
 - RFC2373, IP Version 6 Addressing Architecture, R. Hinden, S. Deering, 1998-07-01.
 - RFC2374, An IPv6 Aggregatable Global Unicast Address Format, R. Hinden, M. O'Dell, S. Deering, Proposed standard, 1998-07-01.
 - RFC2450, Proposed TLA and NLA Assignment Rule, R. Hinden, Informational, 1998-12-01

RFC



- **Routing**
 - RFC2080, RIPng for IPv6, G. Malkin, R. Minnear, Proposed Standard, 1997-01-01
 - RFC2283, Multiprotocol Extensions for BGP-4, T. Bates, R. Chandra, D. Katz, Y. Rekhter, Proposed Standard, 1998-02-01
 - RFC2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing, P. Marques, F. Dupont, Proposed standard, 1999-03-01.
- **Transition scenarios**
 - RFC1933, Transition Mechanisms for IPv6 Hosts and Routers, R. Gilligan, E. Nordmark, Proposed standard, 1996-04-01.
 - RFC2185, Routing Aspects of IPv6 Transition, R. Callon, D. Haskin, Informational, 1997-09-01
 - RFC2529, Transmission of IPv6 over IPv4 Domains without Explicit Tunnels, B. Carpenter, C. Jung, Proposed standard, 1999-03-01.
- **API**
 - RFC2292, Advanced Sockets API for IPv6, W. Stevens, M. Thomas, Informational, 1998-02-01
 - RFC2553, Basic Socket Interface Extensions for IPv6, R. Gilligan, S. Thomson, J. Bound, W. Stevens, Informational, 1999-03-01.

RFC



- **IPv6 over "foo"**
 - RFC2472, IP Version 6 over PPP, D. Haskin, E. Allen, Proposed standard, 1998-12-01
 - RFC2464, Transmission of IPv6 Packets over Ethernet Networks, M. Crawford, Proposed standard, 1998-12-01.
 - RFC2467, Transmission of IPv6 Packets over FDDI Networks, M.Crawford, Proposed standard, 1998-12-01.
 - RFC2470, Transmission of IPv6 Packets over Token Ring Networks, M. Crawford, T. Narten, S. Thomas, Proposed standard, 1998-12-01.
 - RFC 2491, IPv6 over Non-Broadcast Multiple Access (NBMA) networks, G. Armitage, P. Schulter, M. Jork, G. Harter, Proposed standard, 1999-01-01.
 - RFC2492, IPv6 over ATM Networks, G. Armitage, P. Schulter, M. Jork, Proposed standard, 1999-01-01.
 - RFC2497, Transmission of IPv6 Packets over ARCnet Networks, I. Souvatzis, Proposed standard, 1999-01-01.
- **DNS**
 - RFC1886, DNS Extensions to support IP version 6, S. Thomson, C. Huitema, proposed standard, 1995-12-01

RFC



- **MIBs**

- RFC2465, Management Information Base for IP Version 6: Textual Conventions and General Group, D. Haskin, S. Onishi, Proposed standard, 1998-12-01.
- RFC2466, Management Information Base for IP Version 6: ICMPv6 Group, D. Haskin, S. Onishi, Proposed standard, 1998-12-01.
- RFC2452, IP Version 6 Management Information Base for the Transmission Control Protocol, M. Daniele, Proposed standard, 1998-12-01.
- RFC2454, IP Version 6 Management Information Base for the User Datagram Protocol, M. Daniele, Proposed standard, 1998-12-01.

- **Others**

- RFC2147, TCP and UDP over IPv6 Jumbograms, D. Borman, Proposed standard, 1997-05-01
- RFC2375, IPv6 Multicast Address Assignments, R. Hinden, S. Deering, 1998-07-01.
- RFC2473, Generic Packet Tunneling in IPv6 Specification, A. Conta, S. Deering, Proposed Standard, 1998-12-01
- RFC2526, Reserved IPv6 Subnet Anycast Addresses, D. Johnson, S. Deering, Proposed standard, 1999-03-01.

Ej. Configuración Win

http://www.cu.ipv6tf.org/pdf/6sos_instalacion_ipv6_windows_v4_0.pdf



C:\>netsh interface ipv6 install

```
prompt>netsh interface ipv6
```

Los siguientes comandos estan disponibles:

Comandos en este contexto:

6to4	- Cambia al contexto 'netsh interface ipv6 6to4'.
?	- Muestra una lista de comandos.
add	- Agrega una entrada de configuración en la tabla.
delete	- Elimina una entrada de configuración en la tabla.
dump	- Muestra una secuencia de comandos de configuración.
help	- Muestra una lista de comandos.
install	- Instala IPv6.
isatap	- Cambia al contexto 'netsh interface ipv6 isatap'.
renew	- Reinicia las interfaces IPv6.
reset	- Restablece el estado de configuración de IPv6.
set	- Establece la configuración de la información.
show	- Muestra información.
uninstall	- Desinstala IPv6.

Los siguientes subcontextos están disponibles:

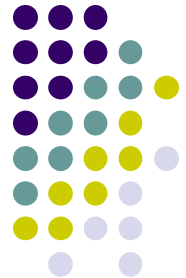
6to4 isatap

Para ver más ayuda acerca de un comando, escríbalo seguido de un espacio y después escriba ?.

```
prompt>
```

Ej. Configuración LINUX

http://www.cu.ipv6tf.org/pdf/6SOS_Instalacion_IPv6_Linux_v4_0.pdf



Instalación de IPv6 en plataformas Linux

2) Soporte IPv6

Para comprobar que el kernel soporta IPv6, habrá que comprobar que existe la siguiente entrada:

```
/proc/net/if_inet6
```

Si no existe, se puede intentar cargar el módulo ipv6 con:

```
#> modprobe ipv6
```

Si se ha cargado correctamente debe existir la entrada mencionada arriba.

- **Nota:** Descargar el módulo puede, a veces, provocar la caída del sistema. Aunque en versiones actuales de los módulos (kernel 2.4.19 adelante) el soporte es muy estable.

Para que cargue de forma automática el módulo IPv6 cuando se demande, se añade al fichero `/etc/modules.conf` la siguiente línea:

```
alias net-pf-10 ipv6
alias sit0 ipv6
alias sit1 ipv6
alias tun6to4 ipv6
```

