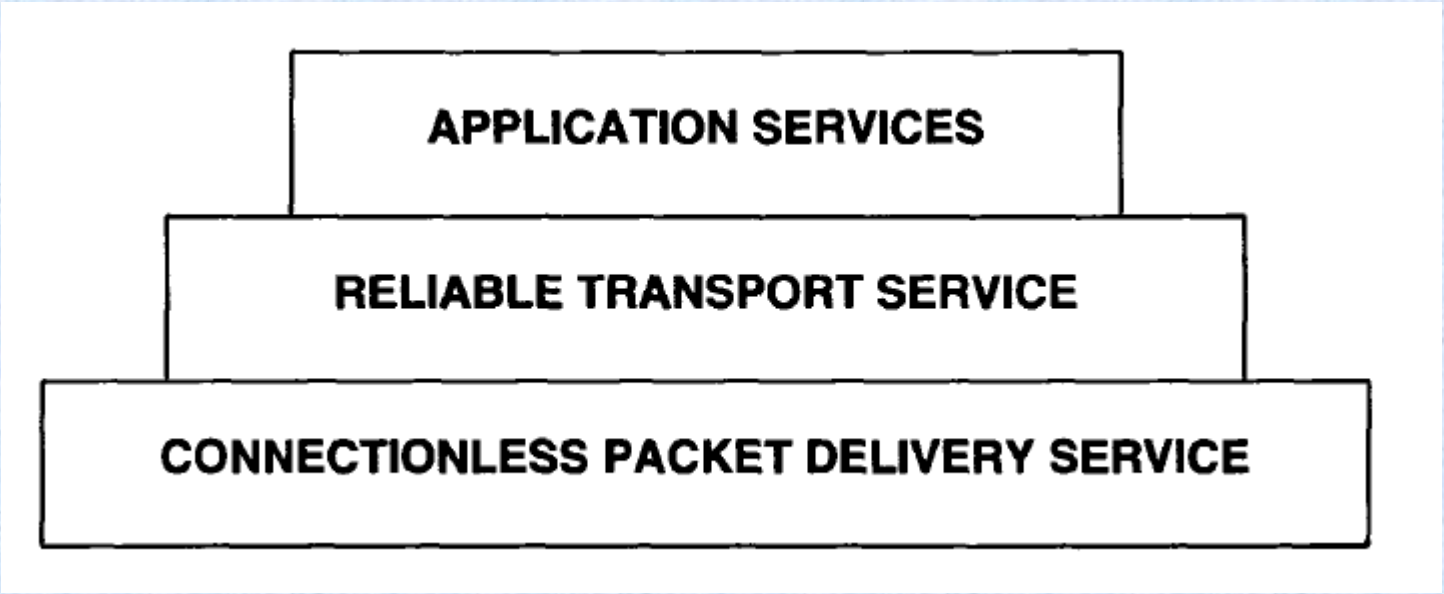
Unidad 4: IP. Temario

- IP
- ARP
- RARP
- ICMP
- IPv6

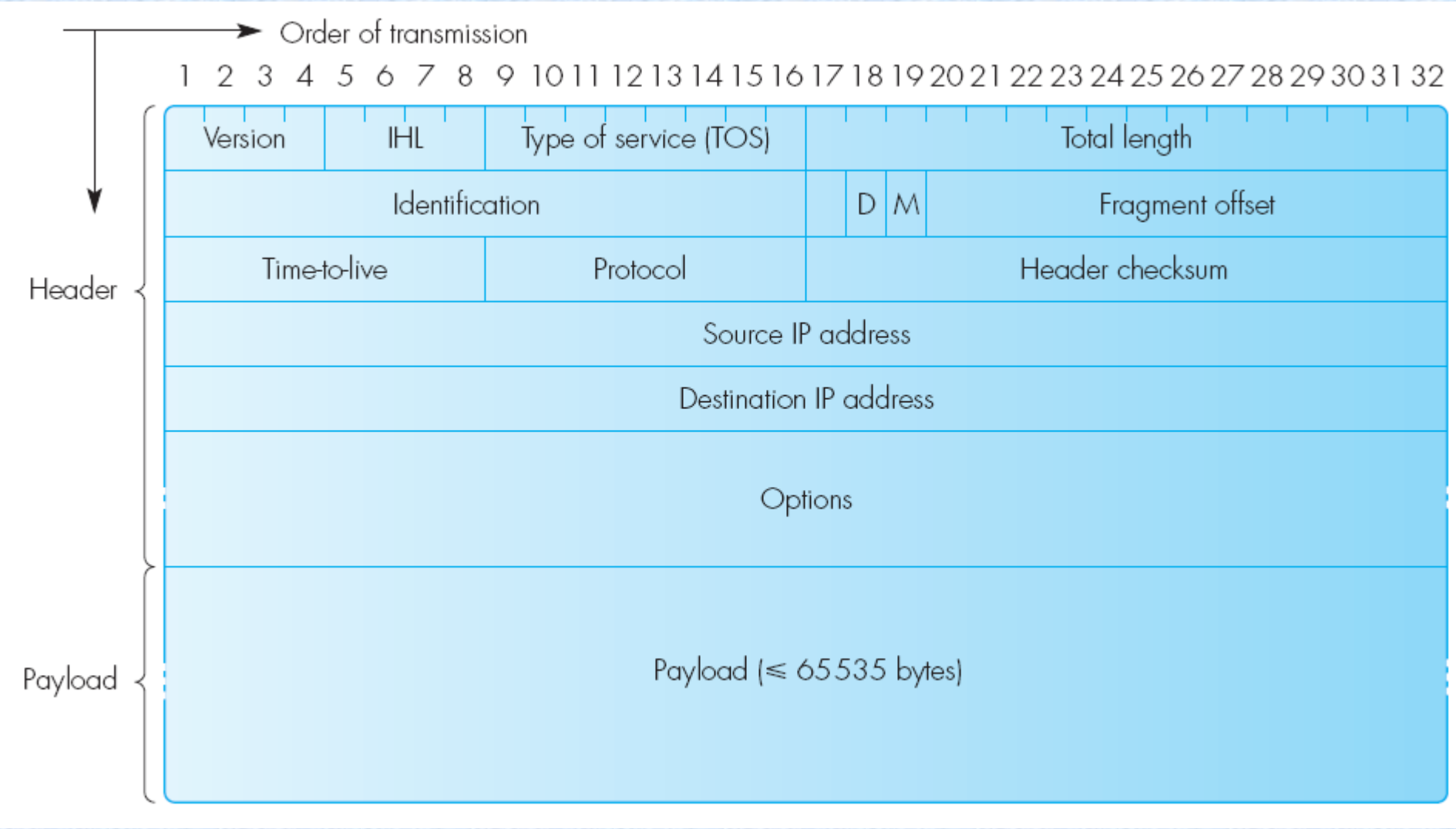
Datagrama IP

- Implementación de servicio de entrega sin conexión no confiable (datagramas)
- Abstracción conceptual



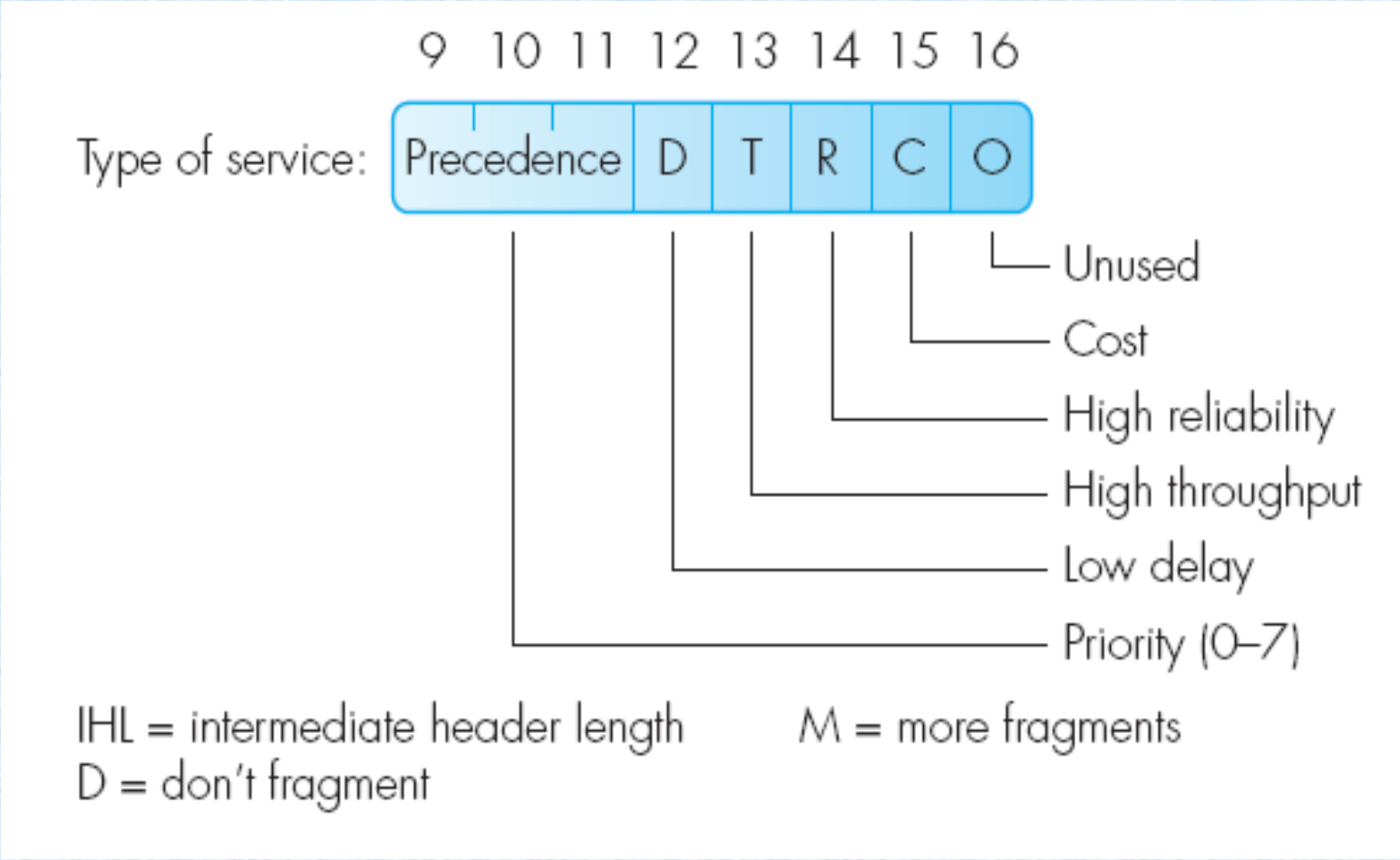
- Formato datagrama

Datagrama IP



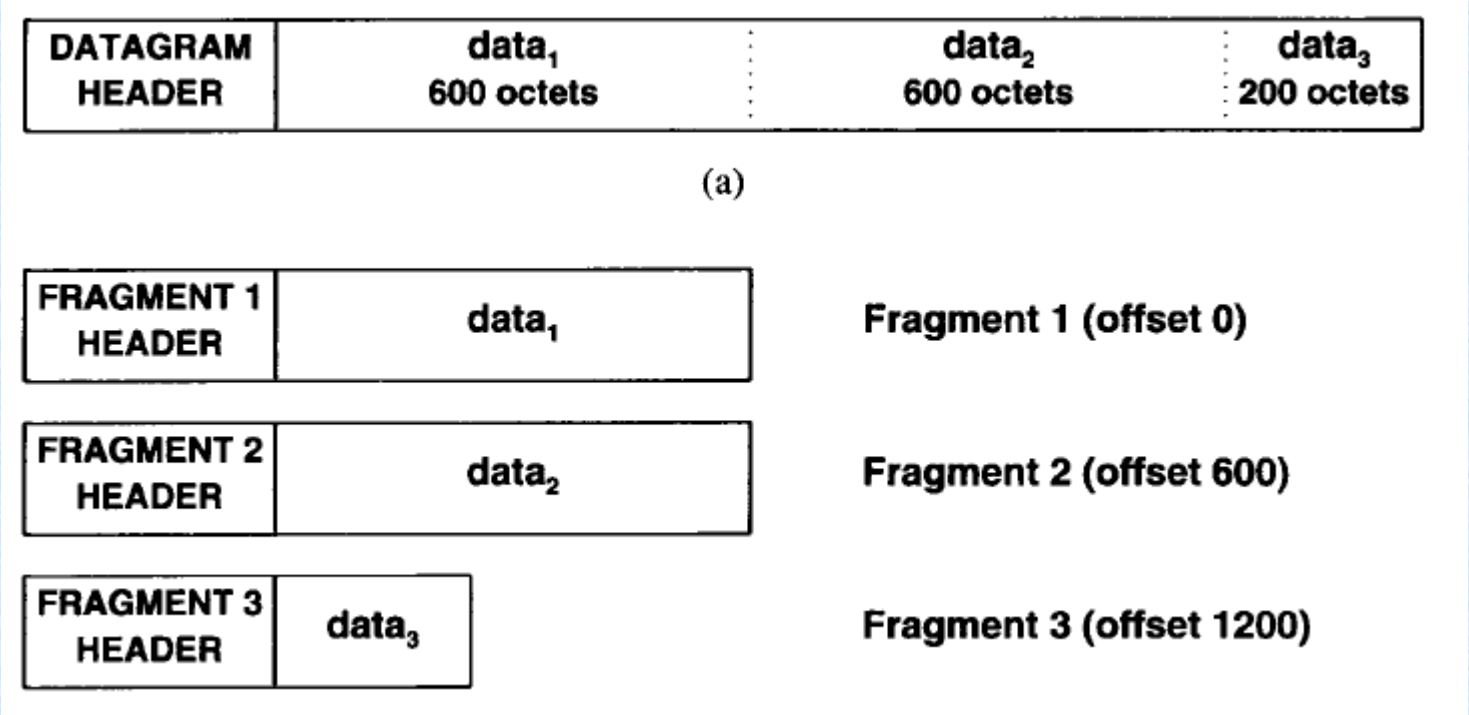
Datagrama IP

- Formato campo TOS original
- Luego fue modificado para acomodar DSCP en DiffServ (RFC 2474). Más en U.6



MTU y Fragmentación en IP

- Cada enlace tiene asignado un atributo muy importante: MTU, o cantidad de bytes que puede tener el payload del enlace. Ej 1500 Ethernet.
- Cuando un dg no puede encapsularse en una trama, se fragmenta. El reensamblado se realiza en el destino! Ejemplo:

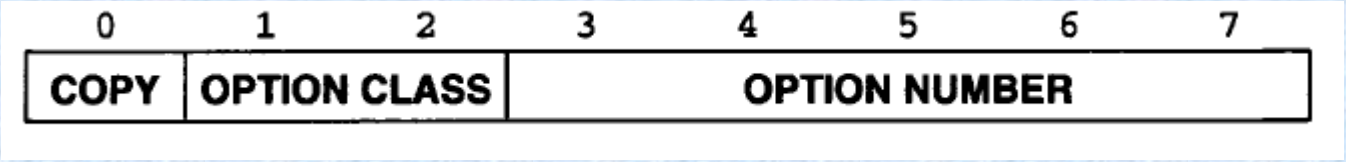


MTU y Fragmentación en IP

- El segundo grupo de 32 bits (ID, Flags, Offset) controla la fragmentación
- El desplazamiento (offset) se cuenta en múltiplos de 8 bytes, por la limitación en la longitud de dicho campo
- La operación de fragmentación consume muchos recursos en los routers
- Puede utilizarse en los hosts finales para montar ataques por DoS (más en U.8)

Opciones en IP

- Longitud variable
- Representan operaciones no siempre necesarias, pero disponibles si se necesitan
- Un dg puede tener 0,1, o más opciones
- Todas tienen el mismo octeto inicial



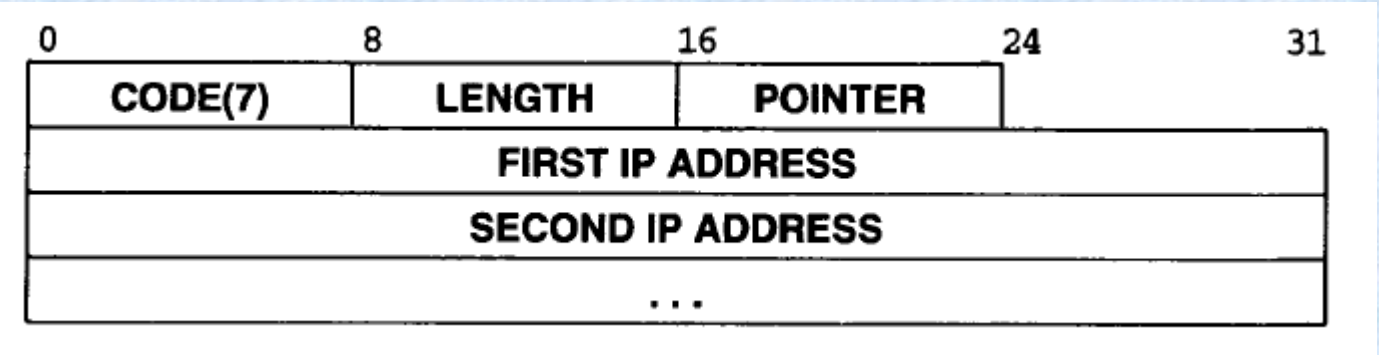
Option Class	Meaning
0	Datagram or network control
1	Reserved for future use
2	Debugging and measurement
3	Reserved for future use

Opciones en IP

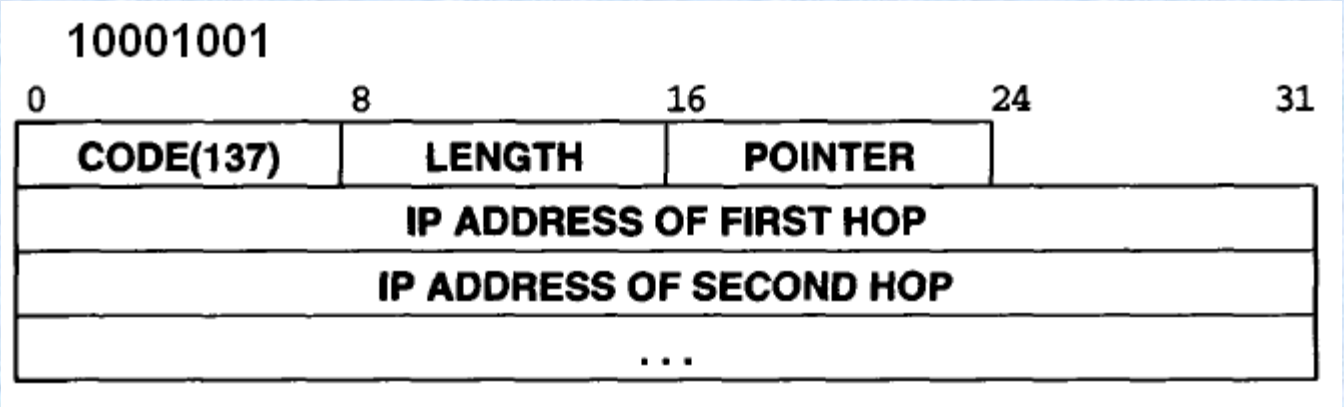
Option Class	Option Number	Length	Description
0	0	-	End of option list. Used if options do not end at end of header (see header padding field for explanation).
0	1	-	No operation. Used to align octets in a list of options.
0	2	11	Security and handling restrictions (for military applications).
0	3	var	Loose source route. Used to request routing that includes the specified routers.
0	7	var	Record route. Used to trace a route.
0	8	4	Stream identifier. Used to carry a SATNET stream identifier (obsolete).
0	9	var	Strict source route. Used to specify a exact path through the internet.
0	11	4	MTU Probe. Used for path MTU discovery.
0	12	4	MTU Reply. Used for path MTU discovery.
0	20	4	Router Alert. Router should examine this datagram even if not an addressee.
2	4	var	Internet timestamp. Used to record timestamps along the route.
2	18	var	Traceroute. Used by traceroute program to find routers along a path.

Fuente: http://www.iana.org/assignments/ip-parameters

Opciones en IP

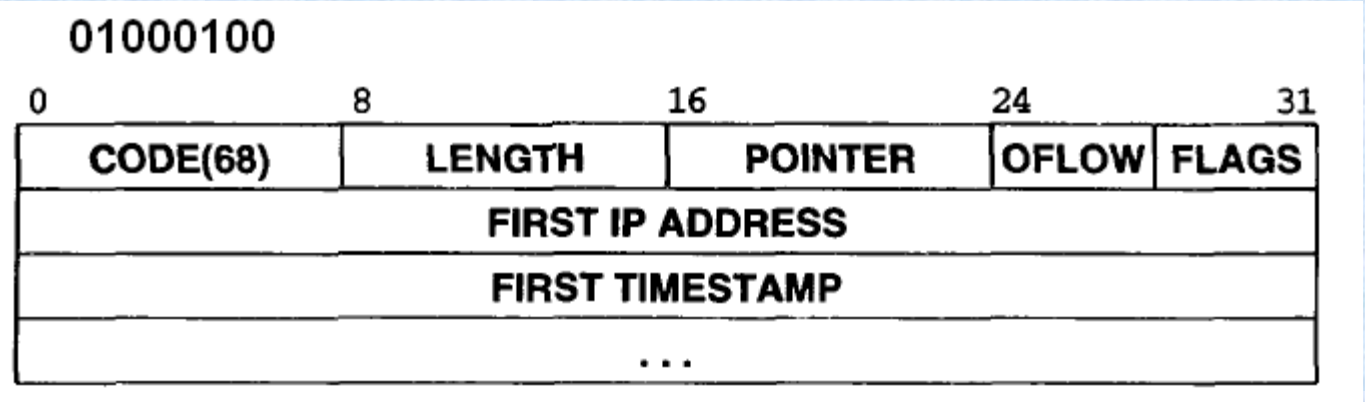


Registro de ruta



Ruteo estricto de fuente

Opciones en IP



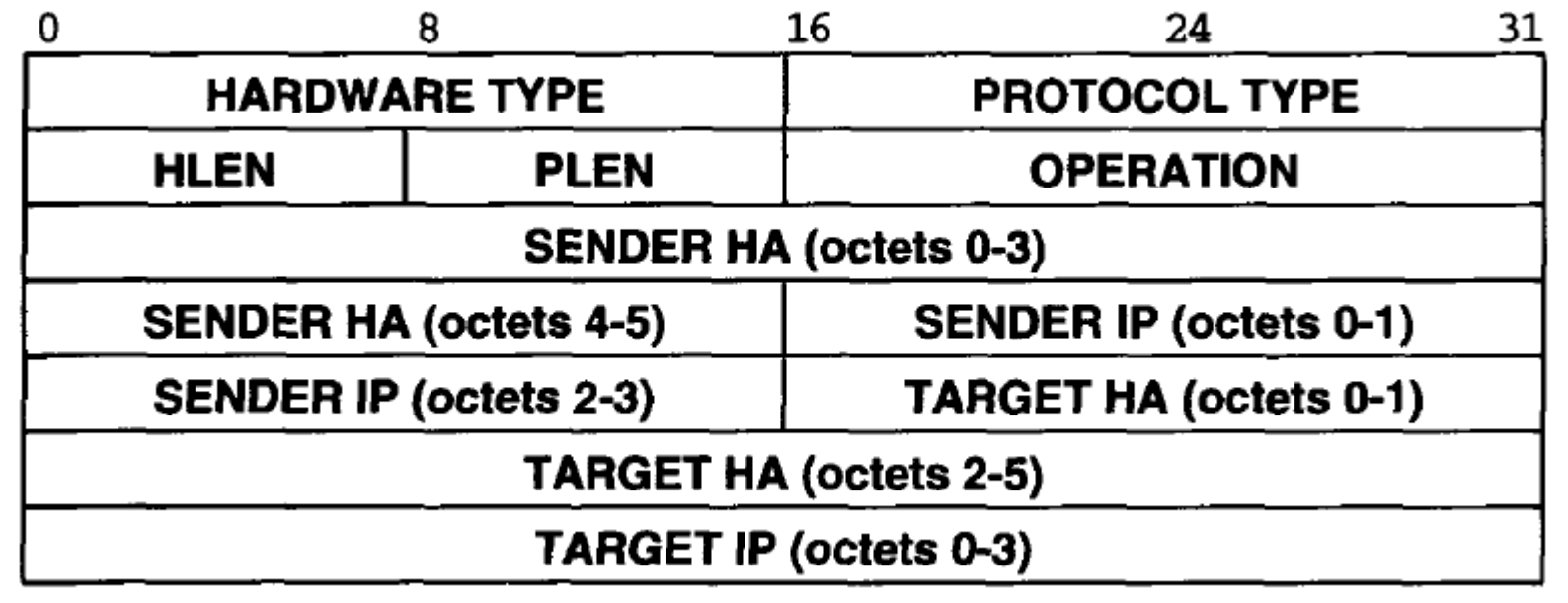
Sello de hora (timestamp)

Flags value	Meaning
0	Record timestamps only; omit IP addresses.
1	Precede each timestamp by an IP address (this is the format shown in Figure 7.15).
3	IP addresses are specified by sender; a router only records a timestamp if the next IP address in the list matches the router's IP address.

Valores del campo FLAGS

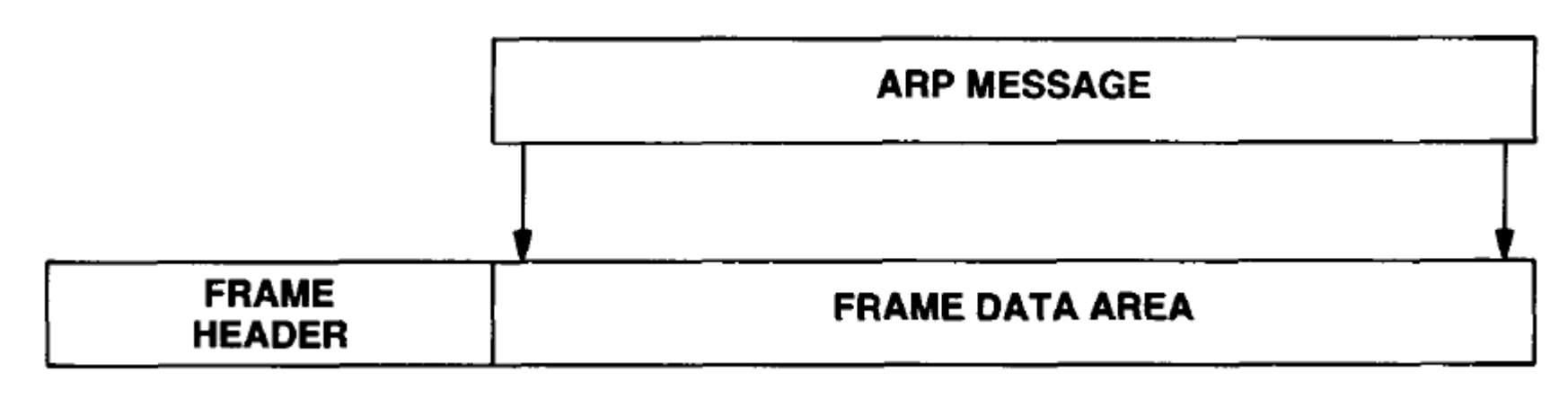
ARP

- Problema: cómo encuentro la dirección física de un DESTINO IP?
- ADDRESS RESOLUTION PROTOCOL
- Asocia una dirección lógica (conocida) a una dirección física (desconocida)
- Se basa en el envío de un mensaje de difusión (broadcast)
- Formato del mensaje

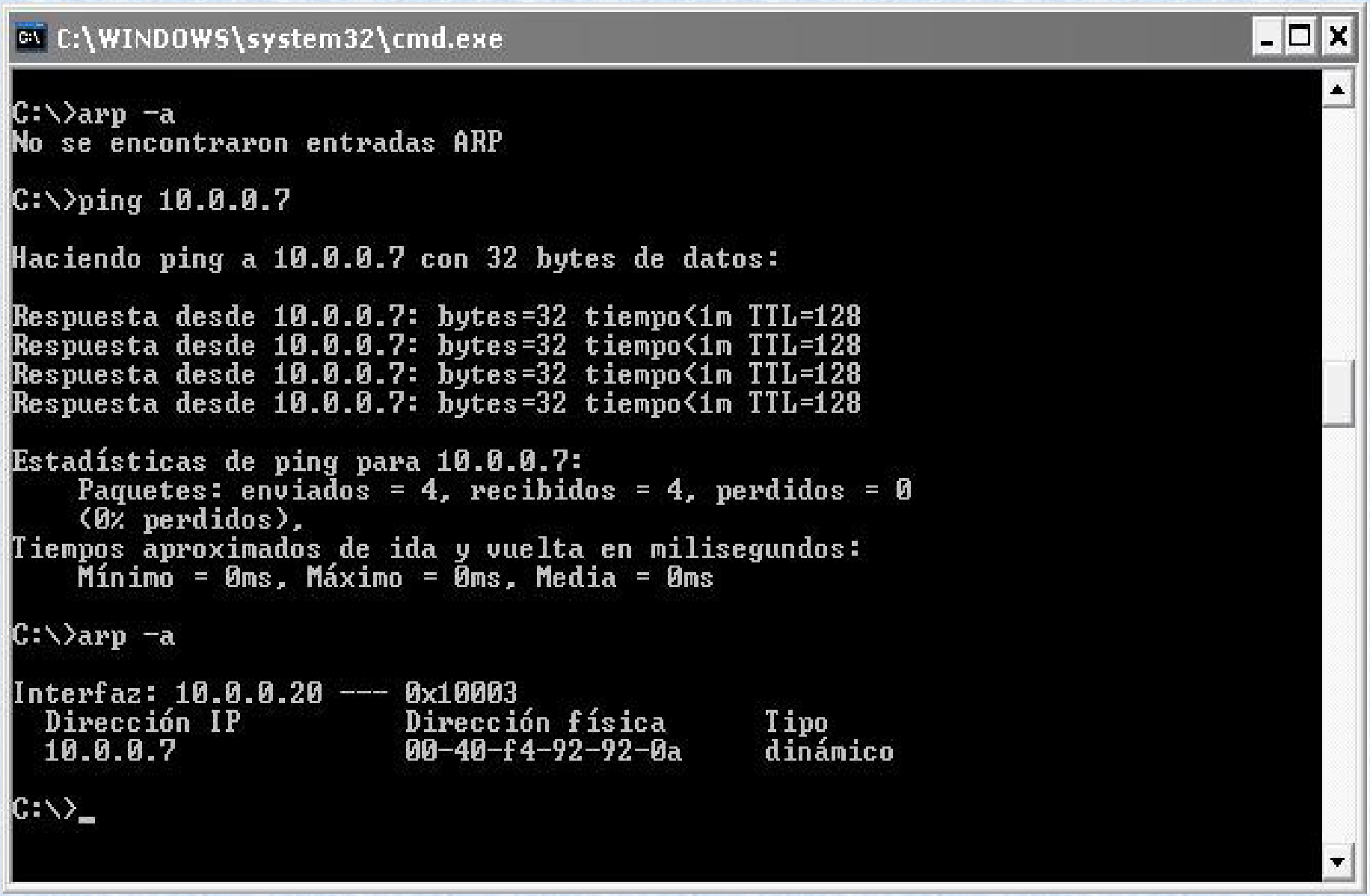


RARP

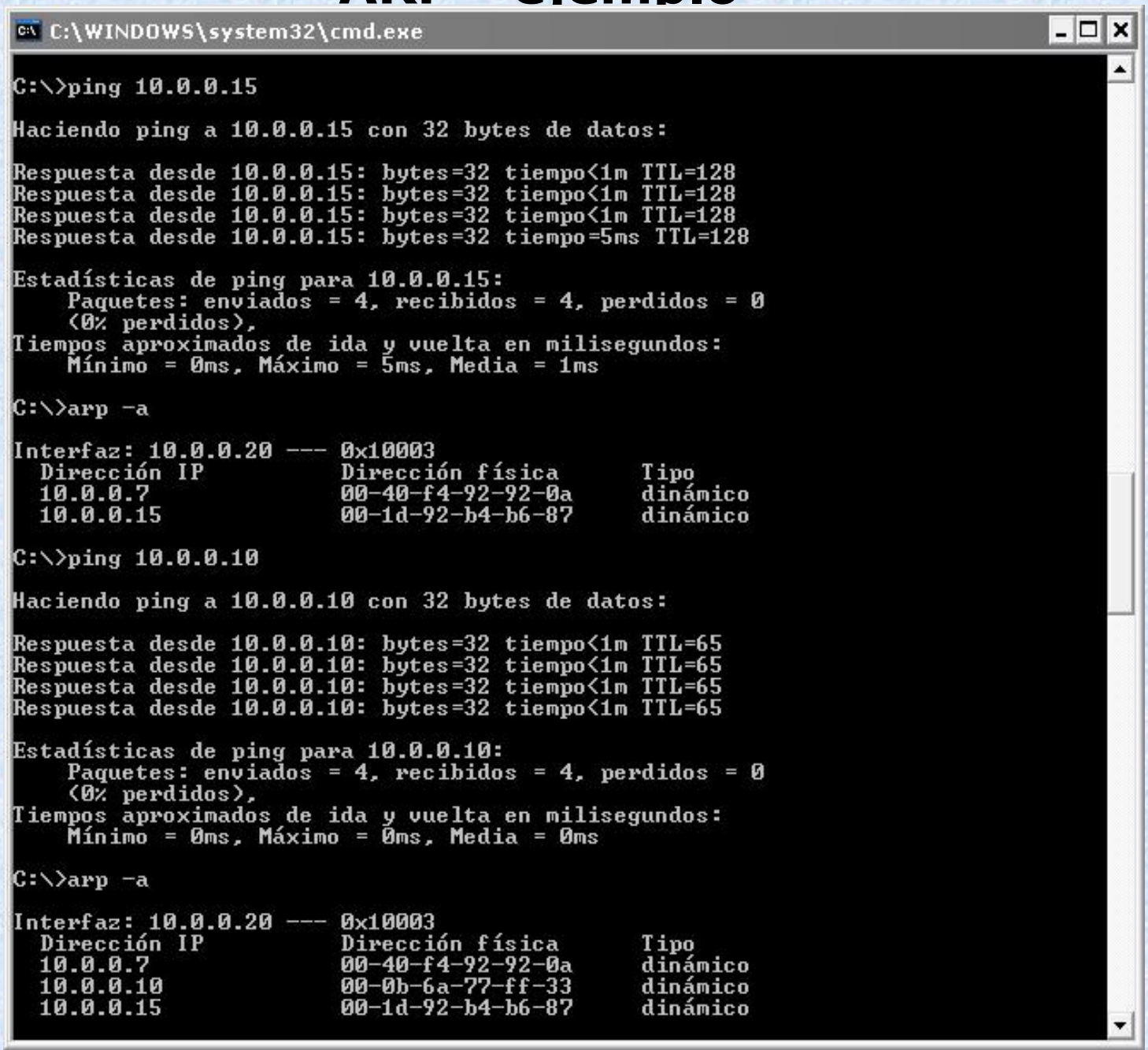
- Qué pasa cuando la estación no conoce SU PROPIA dirección IP? Ej. estaciones diskless
- Reverse ARP
- Se necesita servidor!
- Utiliza el mismo formato de mensaje de ARP, con otras operaciones
- Temporización
- Servidores primarios y secundarios RARP
- Encapsulamiento ARP/RARP



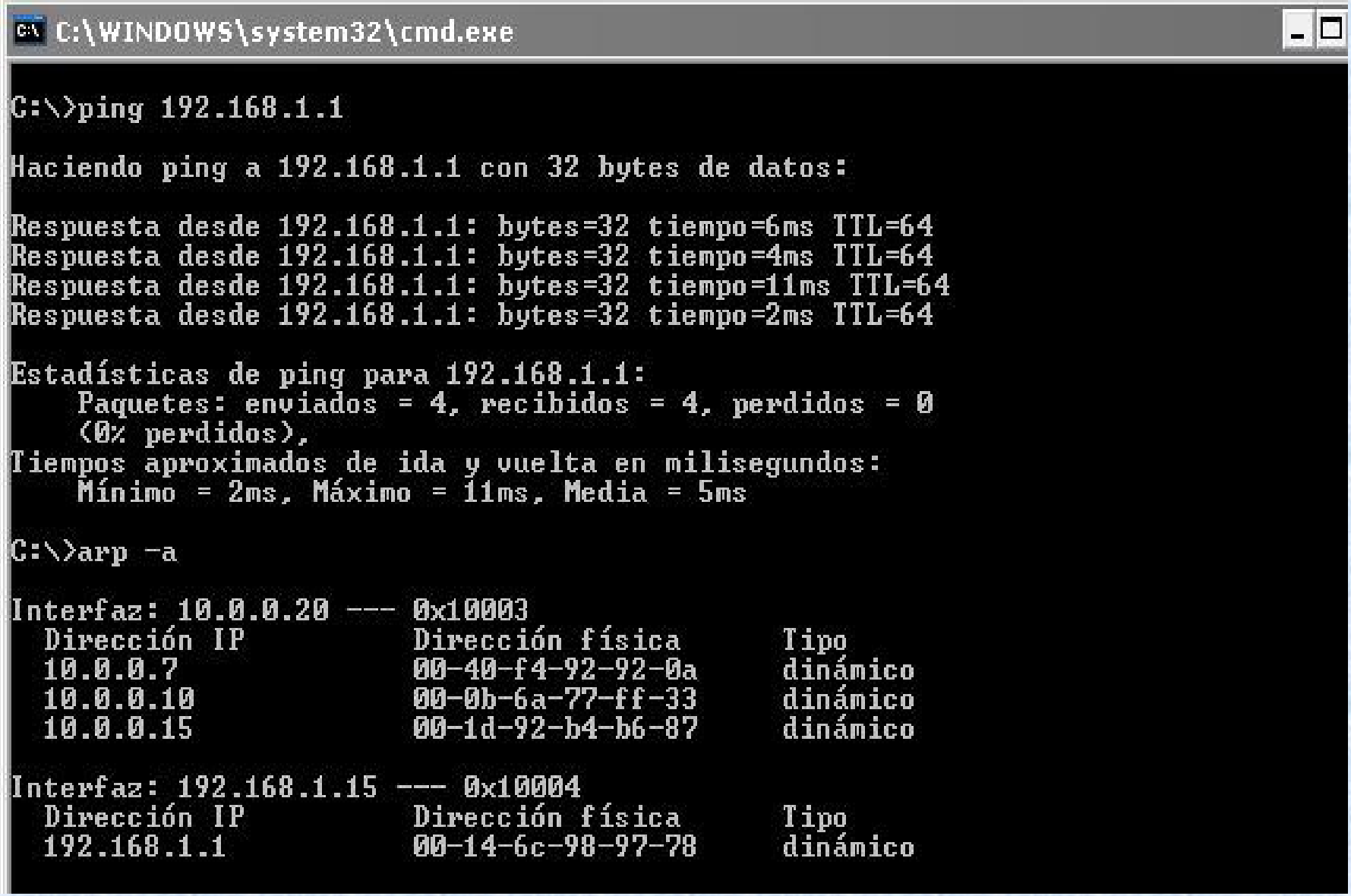
ARP - ejemplo


C:\WINDOWS\system32\cmd.exe
C:\>arp -a
No se encontraron entradas ARP
C:\>ping 10.0.0.7
Haciendo ping a 10.0.0.7 con 32 bytes de datos:
Respuesta desde 10.0.0.7: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.0.7: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.0.7: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.0.7: bytes=32 tiempo<1m TTL=128
Estadísticas de ping para 10.0.0.7:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\>arp -a
Interfaz: 10.0.0.20 --- 0x10003
Dirección IP
Dirección física
Tipo
10.0.0.7
00-40-f4-92-92-0a
dinámico
C:\>

ARP - ejemplo

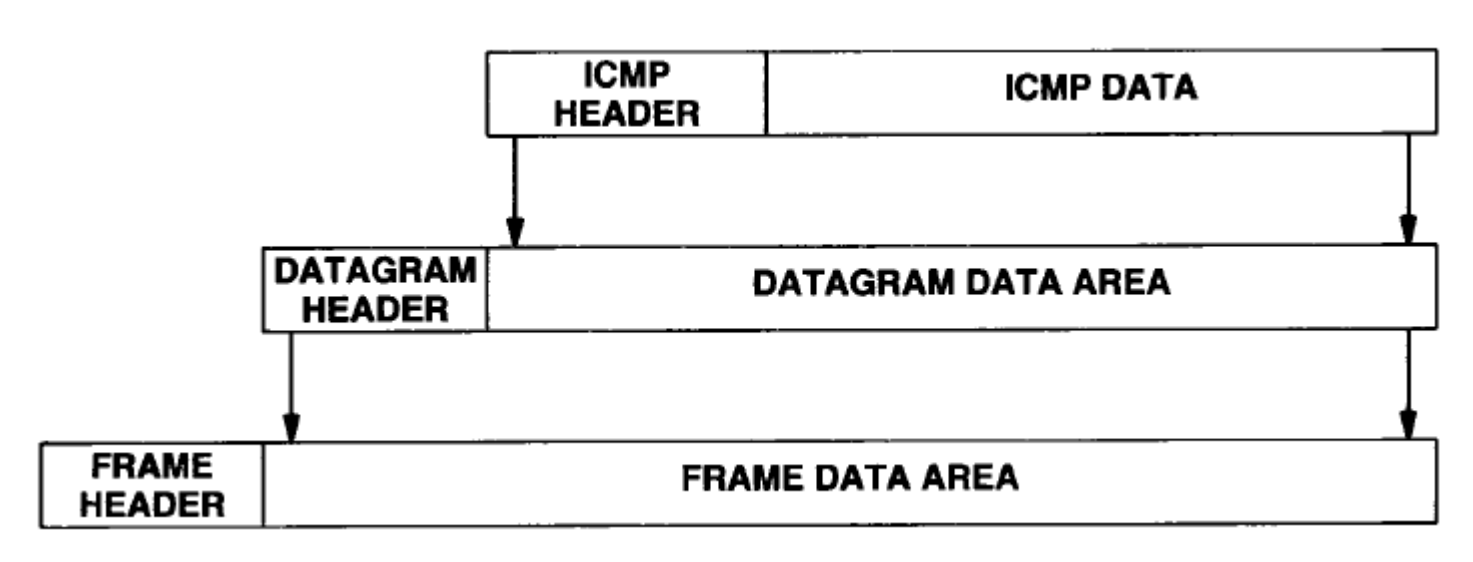

C:\WINDOWS\system32\cmd.exe
C:\>ping 10.0.0.15
Haciendo ping a 10.0.0.15 con 32 bytes de datos:
Respuesta desde 10.0.0.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.0.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.0.15: bytes=32 tiempo<1m TTL=128
Respuesta desde 10.0.0.15: bytes=32 tiempo=5ms TTL=128
Estadísticas de ping para 10.0.0.15:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 5ms, Media = 1ms
C:\>arp -a
Interfaz: 10.0.0.20 --- 0x10003
Dirección IP Dirección física Tipo
10.0.0.7 00-40-f4-92-92-0a dinámico
10.0.0.15 00-1d-92-b4-b6-87 dinámico
C:\>ping 10.0.0.10
Haciendo ping a 10.0.0.10 con 32 bytes de datos:
Respuesta desde 10.0.0.10: bytes=32 tiempo<1m TTL=65
Respuesta desde 10.0.0.10: bytes=32 tiempo<1m TTL=65
Respuesta desde 10.0.0.10: bytes=32 tiempo<1m TTL=65
Respuesta desde 10.0.0.10: bytes=32 tiempo<1m TTL=65
Estadísticas de ping para 10.0.0.10:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
C:\>arp -a
Interfaz: 10.0.0.20 --- 0x10003
Dirección IP Dirección física Tipo
10.0.0.7 00-40-f4-92-92-0a dinámico
10.0.0.10 00-0b-6a-77-ff-33 dinámico
10.0.0.15 00-1d-92-b4-b6-87 dinámico

ARP - ejemplo


C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.1.1
Haciendo ping a 192.168.1.1 con 32 bytes de datos:
Respuesta desde 192.168.1.1: bytes=32 tiempo=6ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=11ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=2ms TTL=64
Estadísticas de ping para 192.168.1.1:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 2ms, Máximo = 11ms, Media = 5ms
C:\>arp -a
Interfaz: 10.0.0.20 --- 0x10003
Dirección IP Dirección física Tipo
10.0.0.7 00-40-f4-92-92-0a dinámico
10.0.0.10 00-0b-6a-77-ff-33 dinámico
10.0.0.15 00-1d-92-b4-b6-87 dinámico
Interfaz: 192.168.1.15 --- 0x10004
Dirección IP Dirección física Tipo
192.168.1.1 00-14-6c-98-97-78 dinámico

ICMP

- Protocolo de mensajes de control de Internet
- Conjunto de funciones no especificadas en IP, pero que mejoran su funcionalidad
- Originalmente servían para reportar condiciones de error al origen! Luego se extendió la funcionalidad
- Se encapsulan en IP (PROTO=1)

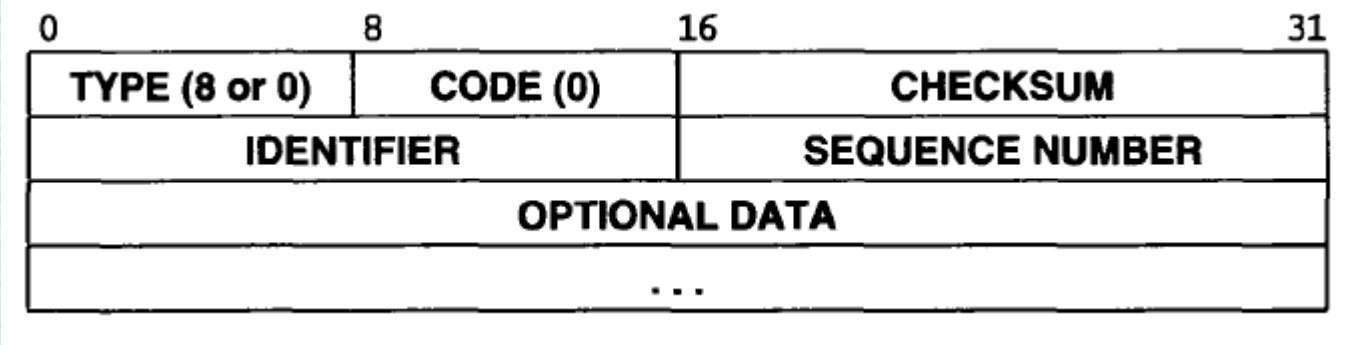


ICMP

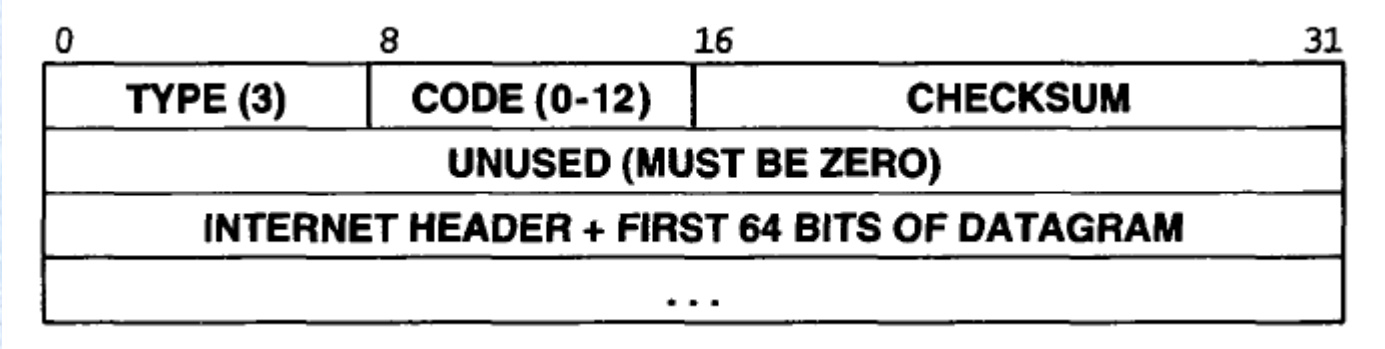
- Si bien cada mensaje tiene su propio formato, todos comienzan con: TYPE (8), CODE (8), CHECKSUM (16)
- El CHECKSUM es importante ya que IP sólo controla errores en el encabezado, no en los datos!

Type Field	ICMP Message Type
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect (change a route)
8	Echo Request
9	Router Advertisement
10	Router Solicitation
11	Time Exceeded for a Datagram
12	Parameter Problem on a Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request (obsolete)
16	Information Reply (obsolete)
17	Address Mask Request
18	Address Mask Reply

ICMP



Solicitud (8)/Respuesta (0) eco (PING)



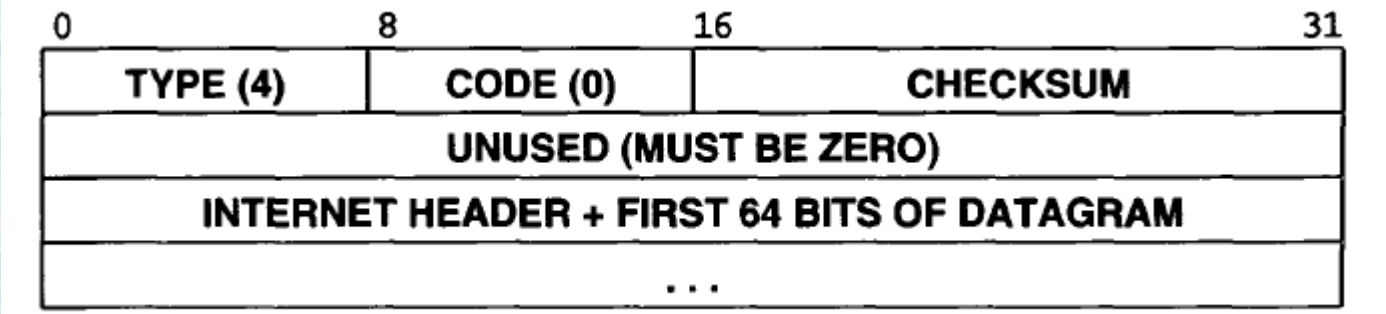
Destino inaccesible

ICMP

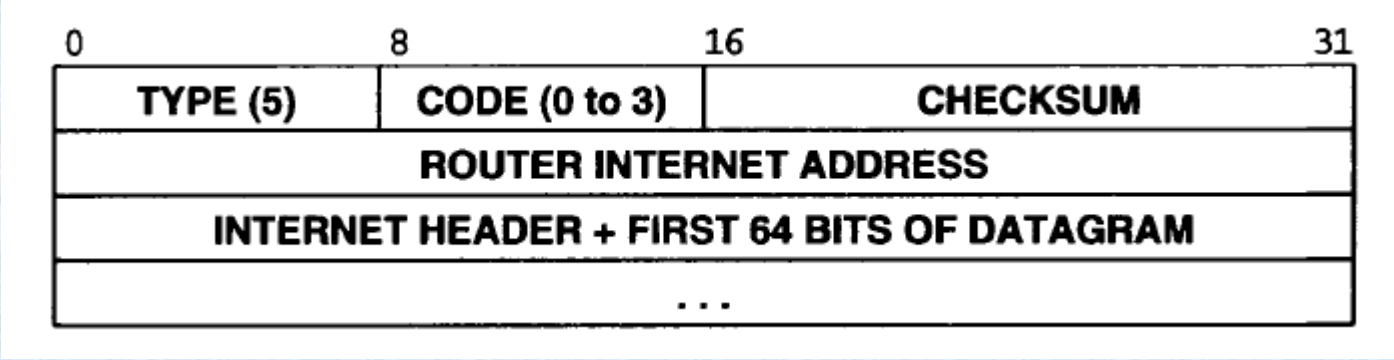
Code Value	Meaning
0	Network unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation needed and DF set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Communication with destination network administratively prohibited
10	Communication with destination host administratively prohibited
11	Network unreachable for type of service
12	Host unreachable for type of service

Destino inaccesible (códigos)

ICMP

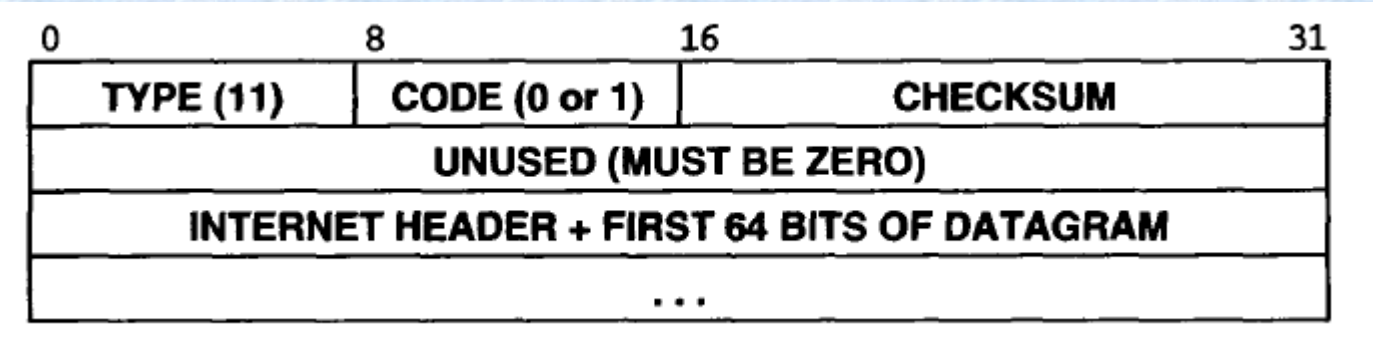


Disminución en origen (Source Quench)



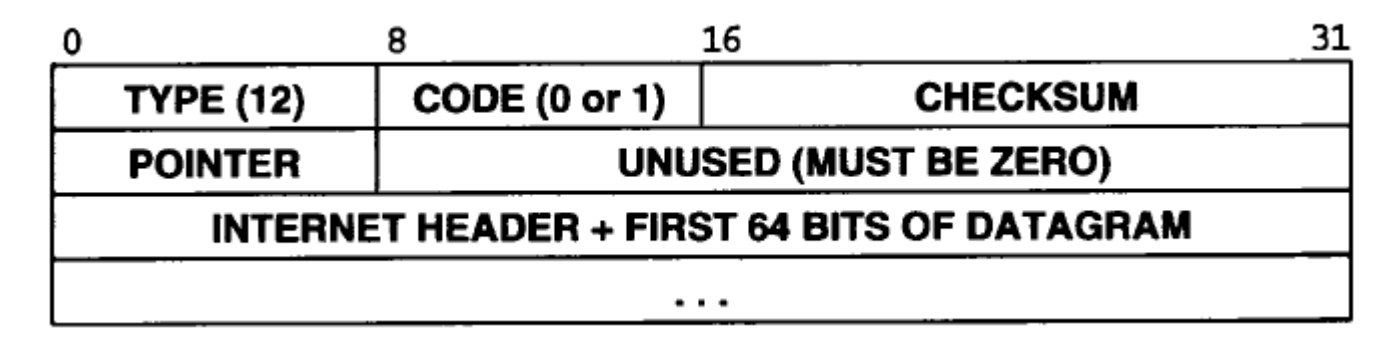
Redireccionamiento – 0 por red (obs)
1 por host
2 por TOS/red
3 por TOS/host

ICMP



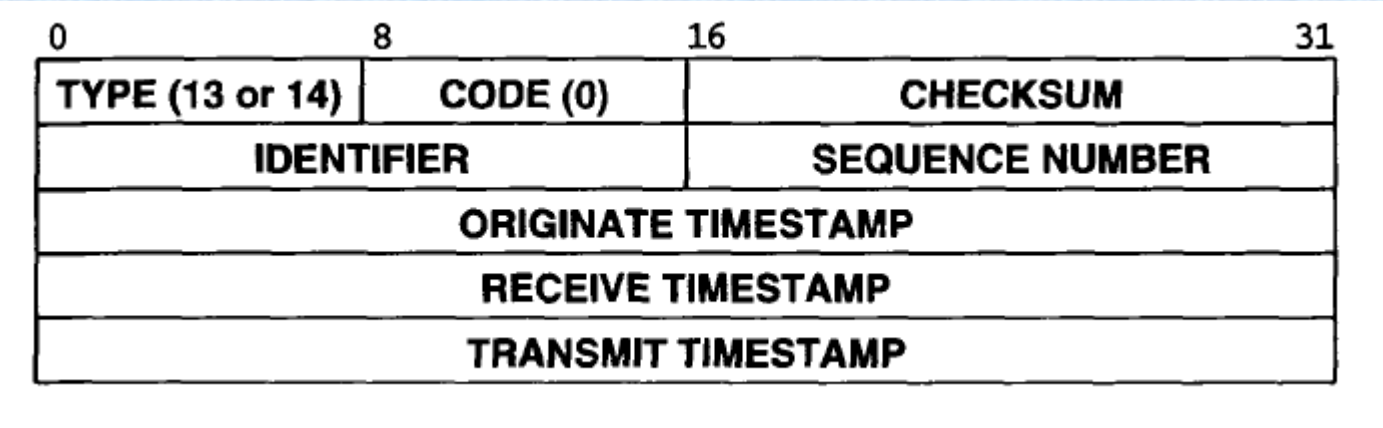
TTL excedido – 0 TTL

1 Fragmentación

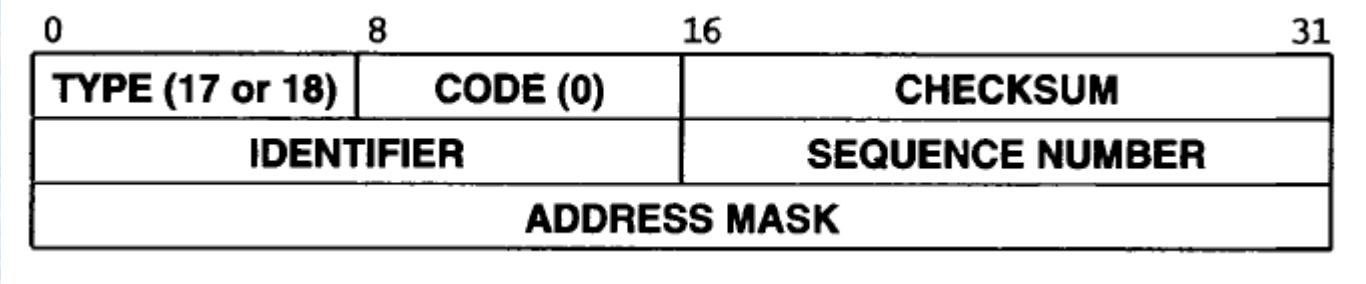


Problema de parámetros

ICMP



Solicitud (13) / Respuesta (14) sello hora

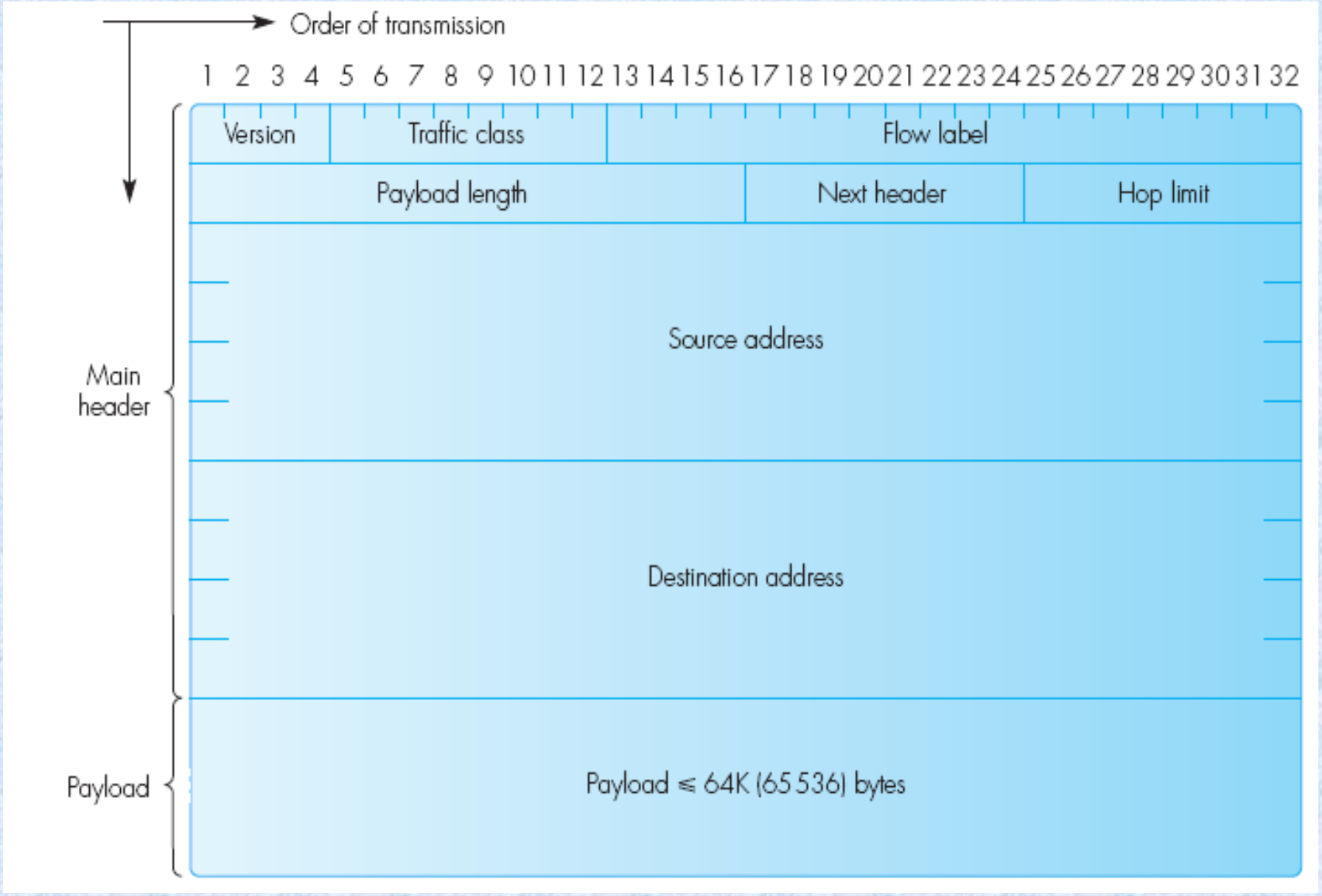


Solicitud (17) / Respuesta (18) máscara

IPv6

- Problema: agotamiento del espacio de direcciones
- Solución propuesta: 32 bits → 128 bits
- Además corregir y adecuar IPv4
- Comenzó como IPng. Documentado RFC 1883-7
- Direcciones jerárquicas
- Formato cabecera simplificado. Cabeceras extendidas, opcionales, no fijas
- Autoconfiguración
- Mayor soporte a variantes IP (móvil, multicast,...)
- Incorporación de características QoS (U.6)
- Características de seguridad e integridad (U.8)

Datagrama IPv6



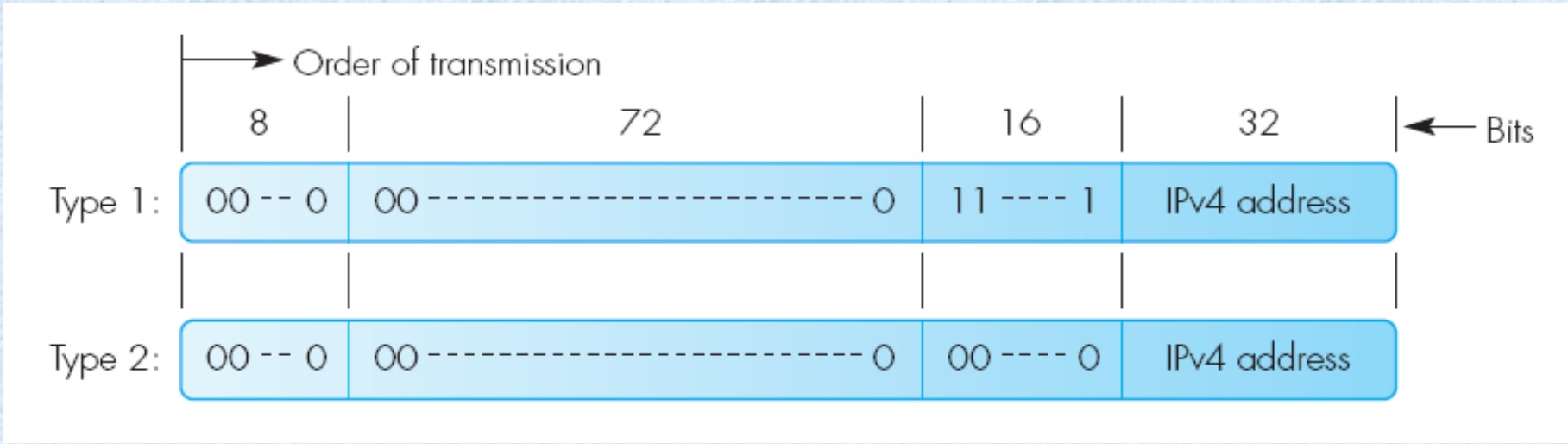
Direcciones IPv6

- Idea general: agrupamiento de direcciones
- Varios prefijos basados en los primeros 8 bits

Prefix format	Usage
0000 0000	Embedded IPv4 address
0000 001	Embedded OSI address
0000 010	Embedded Novell NetWare IPX address
010	Provider-based unicast address
100	Geographic-based unicast address
1111 1110 10	Link local-use address
1111 1110 11	Site local-use address
1111 1111	Multicast address

Direcciones Ipv4 encapsuladas en IPv6

Dos tipos: tuneles y hosts



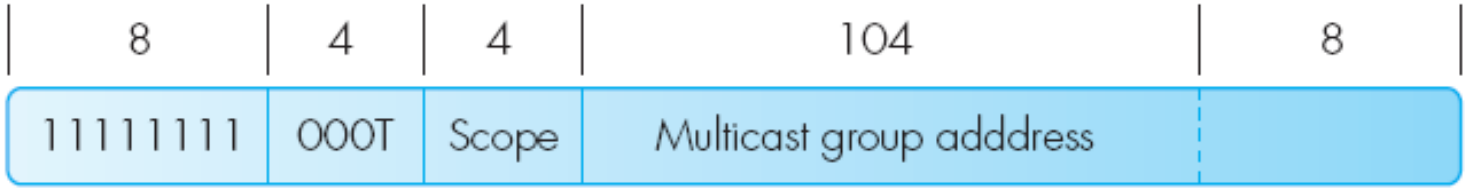
Direcciones IPv6: Unicast

- Direcciones unicast con 3 niveles de agregación (TLA, NLA, SLA). Esquema jerárquico
- Interface ID se divide en subnetID y hostID (subredes en Ipv6!)
- También basado en ubic. Geográfica (100)

Reg. = registry
TLA = top-level aggregator
NLA = next-level aggregator
SLA = site-level aggregator

Direcciones IPv6: Multicast

- Esquema más elaborado que IPv4
- Permite asignaciones temporarias o permanentes



T = 0 = permanently-assigned
(l.s. 8 bits of multicast group address indicate type of multicast group)

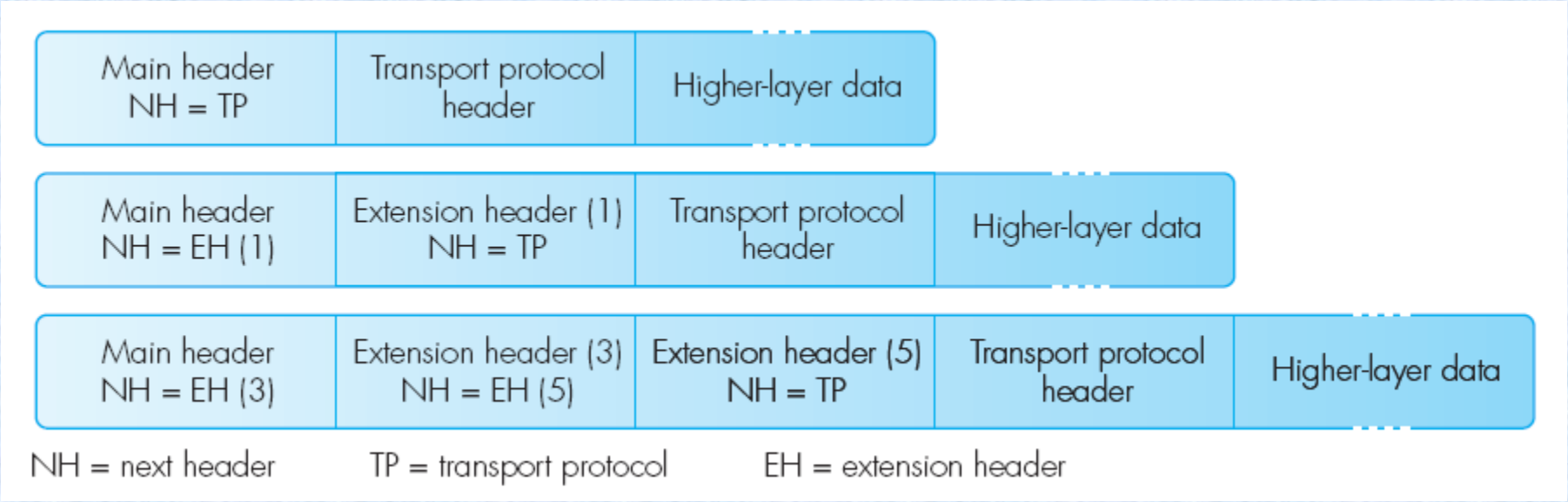
T = 1 = transient, scope = 1 (hex) within node
= 2 link-local
= 5 site-local
= 8 organization-local
= E global
(multicast group address in last 112 bits)

Representación de direcciones IPv6

- En vez de grupos de 8 bits por puntos, 16 bits por dos puntos
- Ej. FEDC:BA98:7654:3210:0000:0000:0000:0089
- Se pueden comprimir, reemplazando 4 ceros consecutivos por ::. En el ejemplo sería FEDC:BA98:7654:3210::0089
- Para una dirección IPv4 encapsulada se puede mantener la notación por puntos, p.ej. ::12.3.0.21

Cabeceras IPv6

- Cada dg tiene al menos la cabecera principal y la de transporte
- Entre ambas se pueden insertar 0,1 o más cabeceras de extensión
- Se definieron 6 tipos de cabeceras de extensión

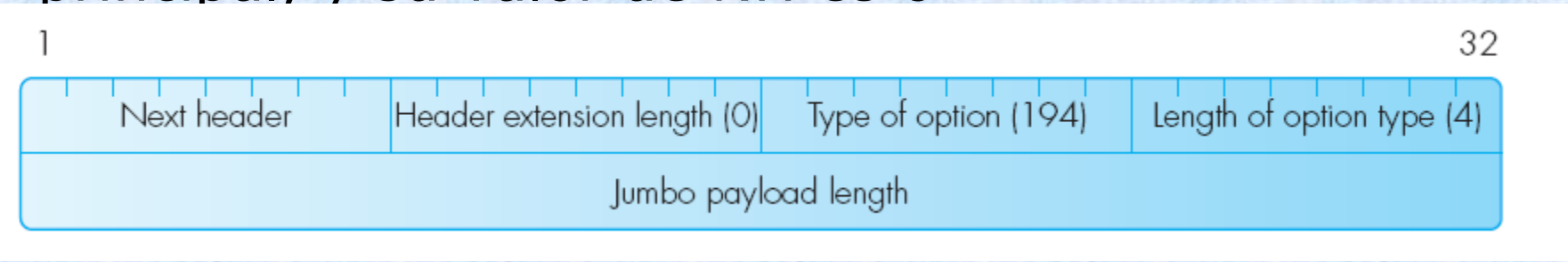


Cabeceras de extensión

- Opciones salto a salto
- Opciones de destino
- Enrutamiento
- Fragmentación
- Autenticación
- Encriptación

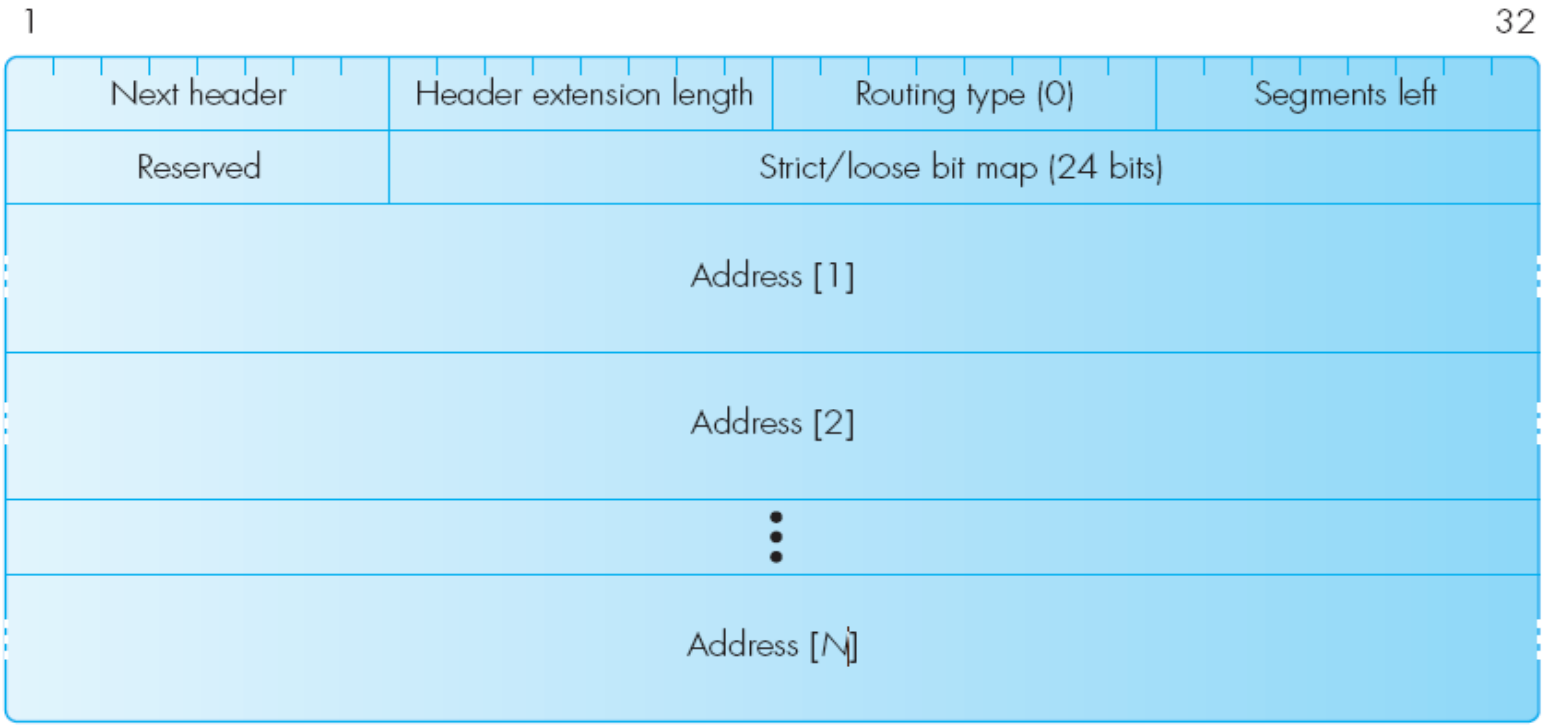
Cabeceras de opciones

- Todas las cabeceras (excepto la de salto-a-salto y enrutamiento) sólo se examinan en el destino
- Como pueden ser variables, se implementa un esquema TLV (tipo-long-valor). Similar a BGP
- El tipo (1er byte) especifica la acción a seguir si no se reconoce: ignorar (00), descartar (01), ICMP (10), ICMP para no multidifusión (11)
- Únicas opciones de destino: relleno (Pad1 ó PadN)
- Única opción salto a salto: jumbograma (194)
- Si existe se procesa inmediatamente luego de la principal, y su valor de NH es 0



Cabeceras de encaminamiento

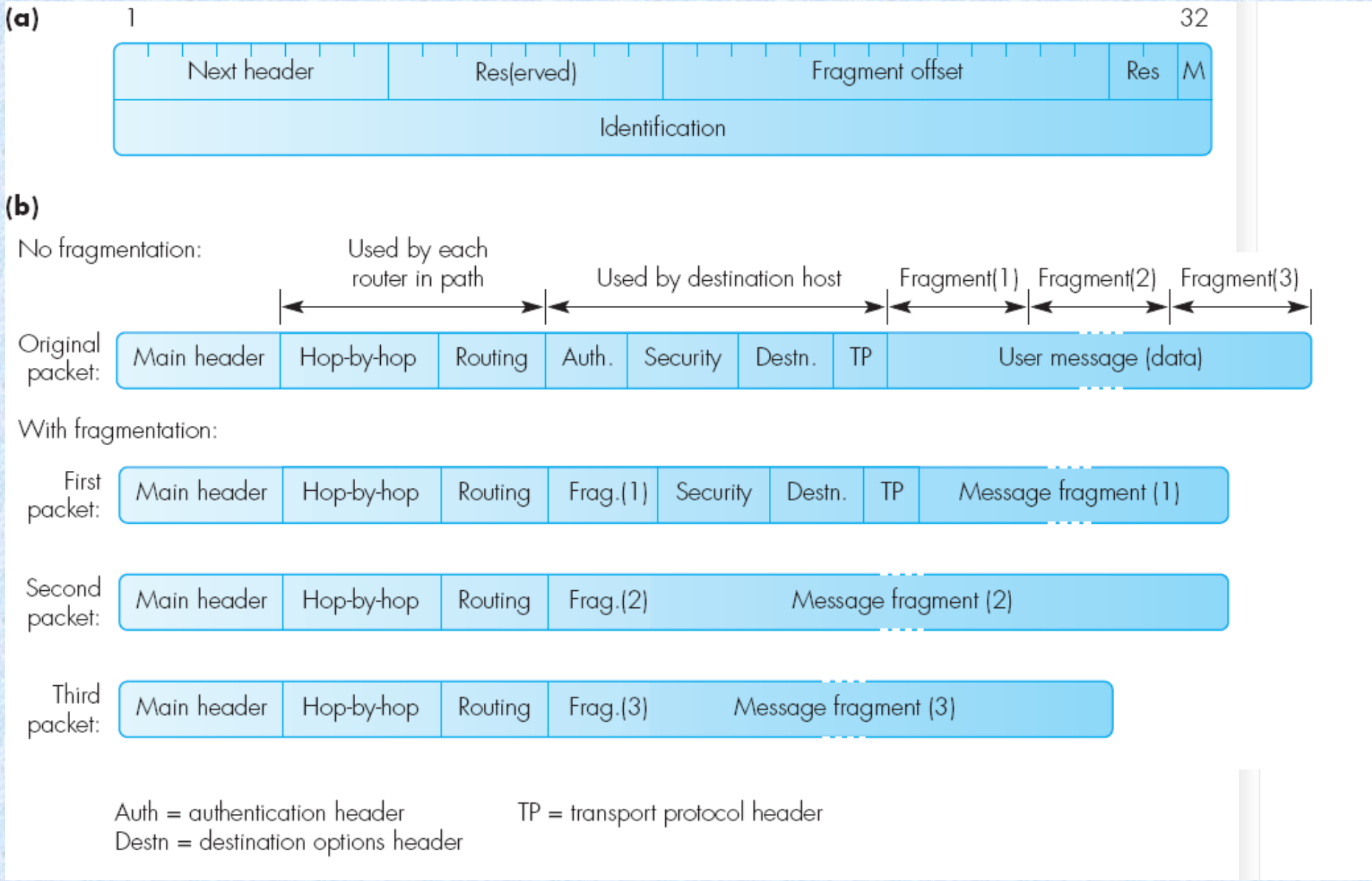
- Similar a ruteo fuente (estricto/no estricto) en IPv4
- Código de NH=43



Cabecera de fragmentación

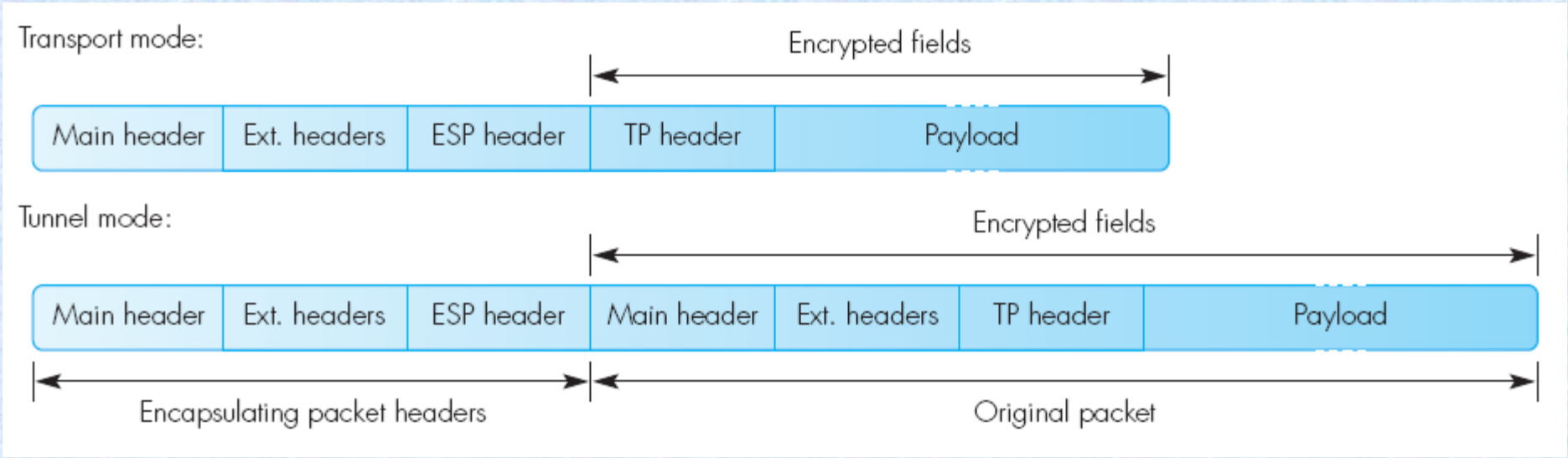
- IPv6 sólo fragmenta en el origen; los routers intermedios descartan y notifican vía ICMPv6
- Por lo tanto, los hosts utilizan MTUs estándar, o bien realizan Path MTU Discovery
- EL reensamblado se realiza en el destino únicamente
- Las cabeceras adicionales (seguridad, etc) se copian solamente en el primer fragmento

Cabecera de fragmentación



Cabecera de autenticación y seguridad

- Se utiliza ESP para encriptar, en modo transporte o en modo túnel (más en U.8)
- Como autenticación, se utiliza el algoritmo de hashing MD5 (más en U.8)

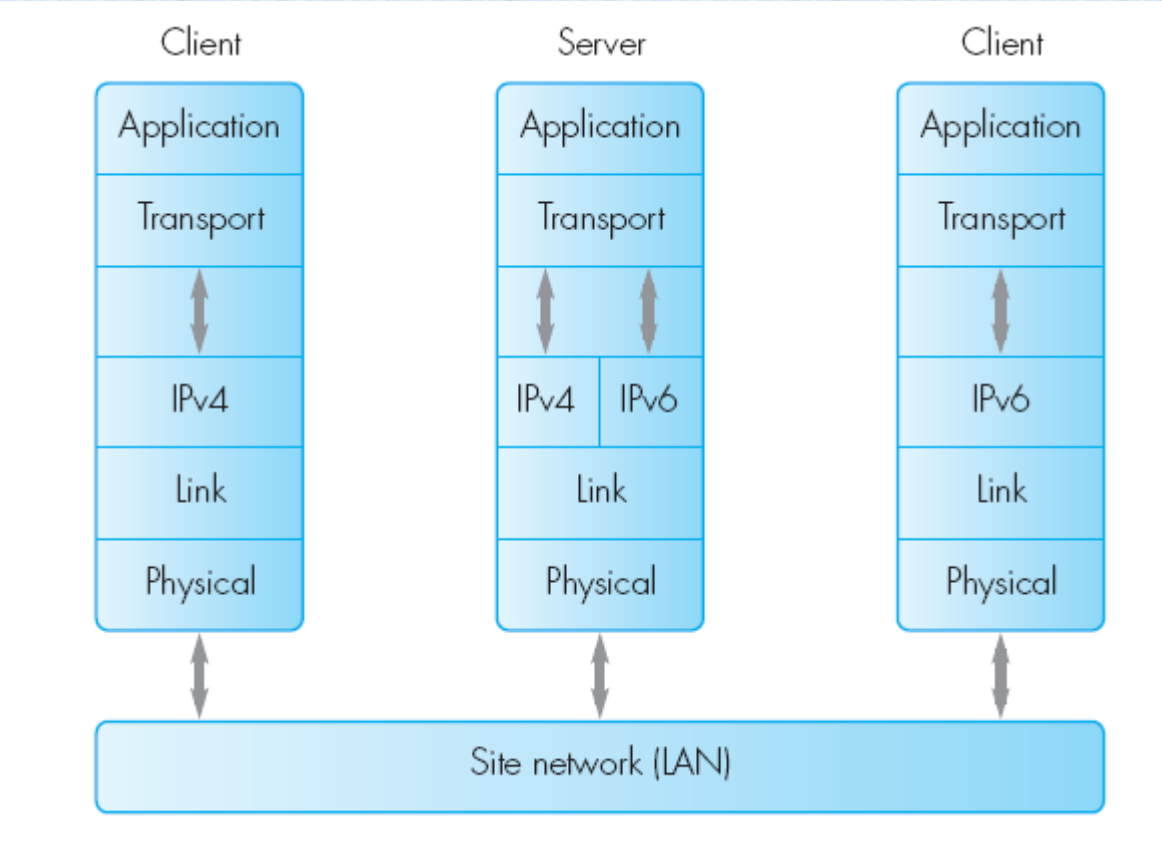


Autoconfiguración

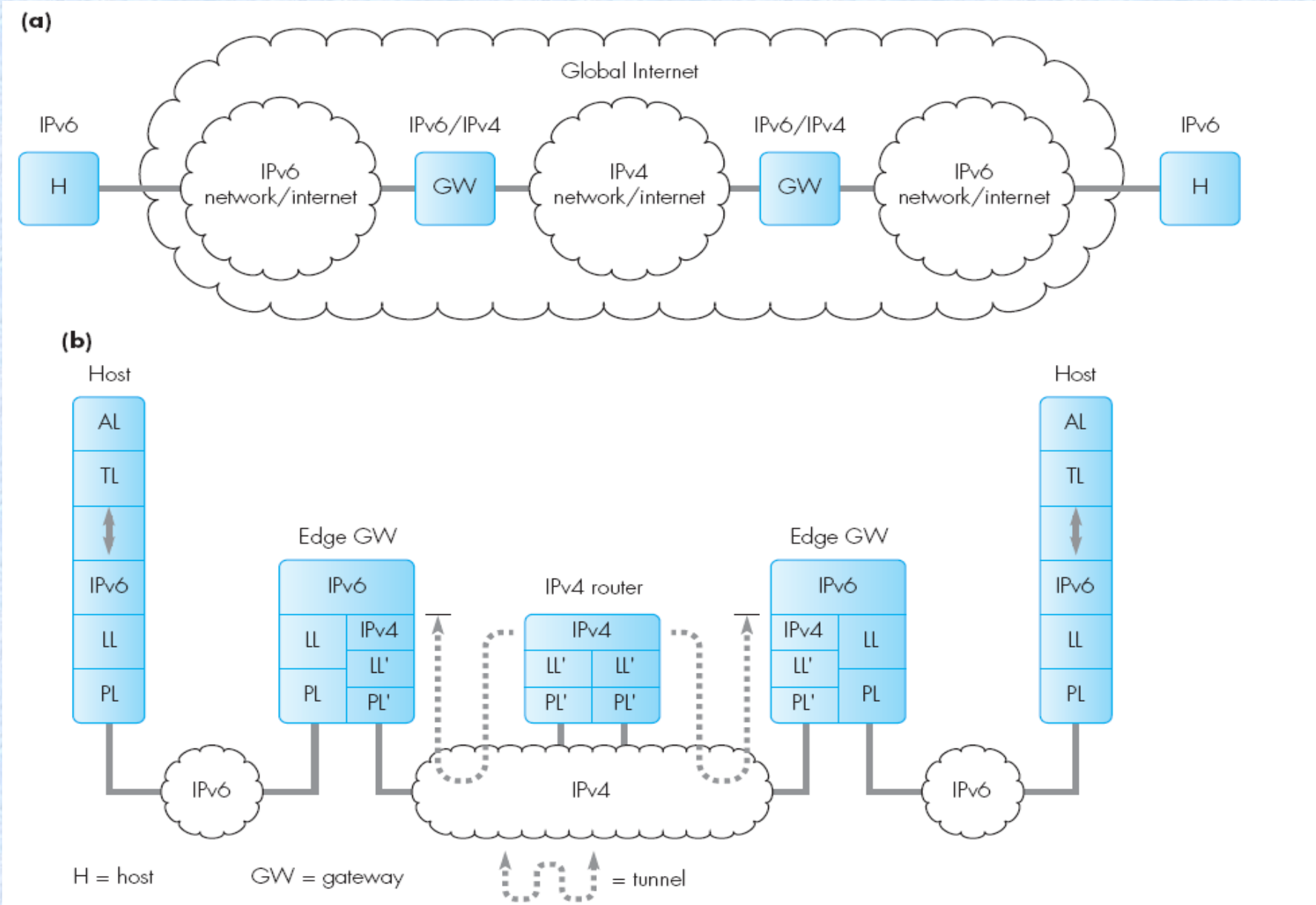
- IPv6 soporta dos mecanismos de autoconfiguración: DHCP (conocido) y ND
- El segundo método se basa en el envío de mensajes ICMPv6 de solicitud/anuncio de router
- Para dirección origen, se concatena la MAC con el prefijo de dirección de enlace local (1111 1111 10)
- Para destino, una dirección de multidifusión local (1111 1111)
- Como respuesta, se envía el netid. El host construye la dirección IPv6 concatenando su MAC al netid recibido
- Similar procedimiento se utiliza para hosts móviles

Interoperatividad V4/V6

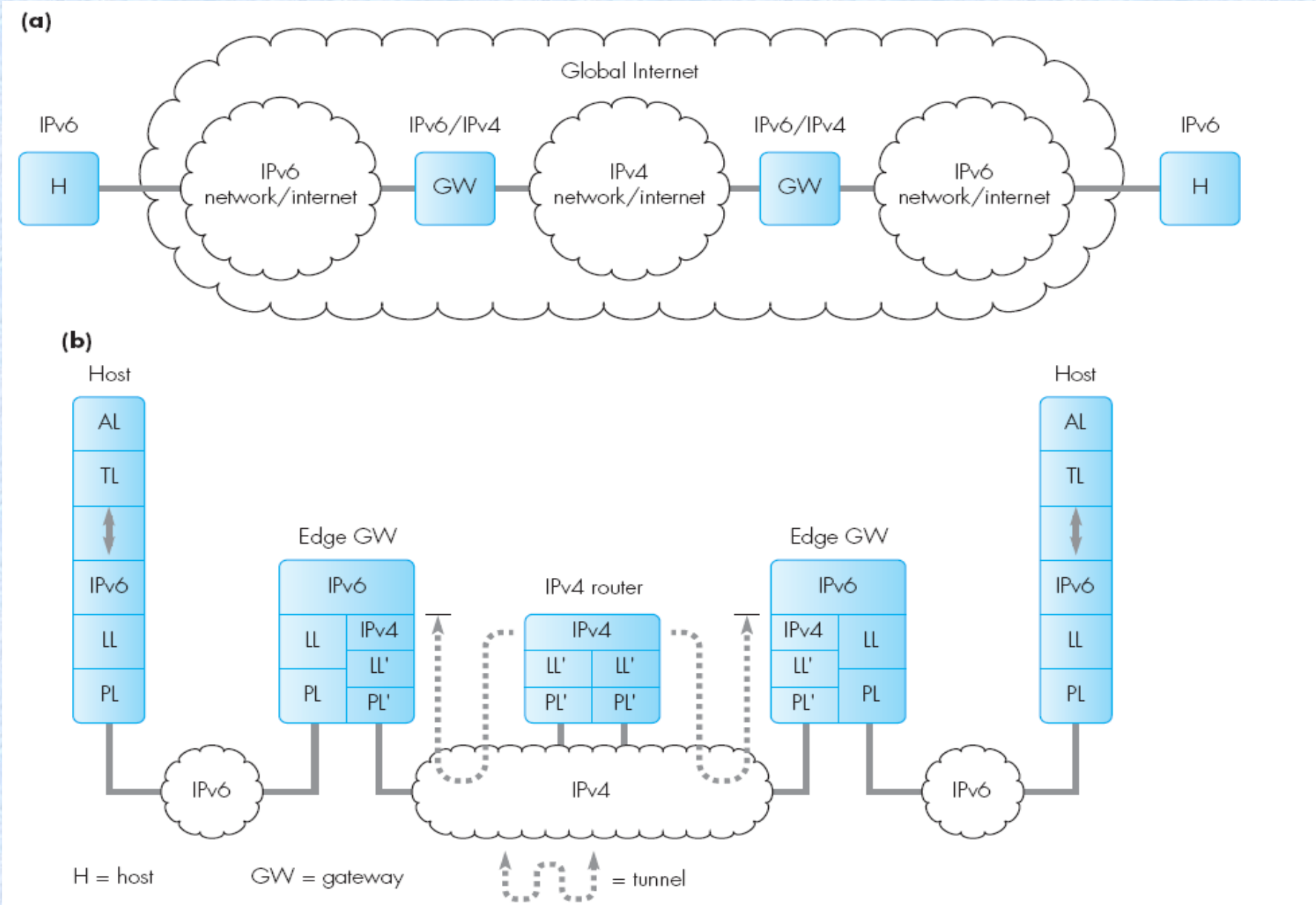
- Necesario para la coexistencia de ambos protocolos durante la transición
- Tres enfoques: pilas duales, túneles, traductores
- Pilas duales: ya utilizado (ej. IP/IPX, ...)



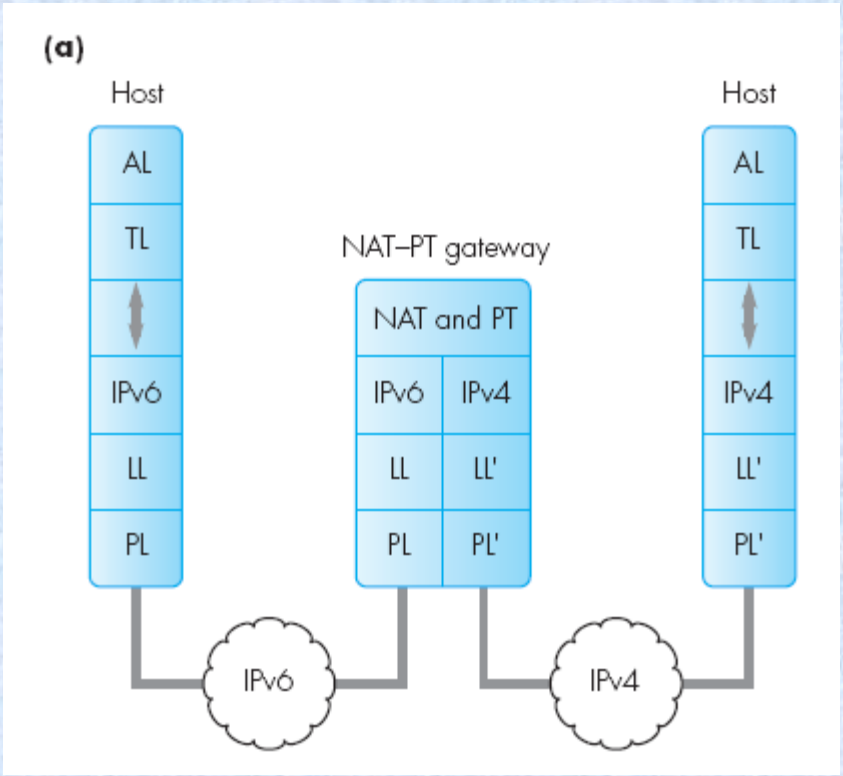
Interoperatividad V4/V6: túneles



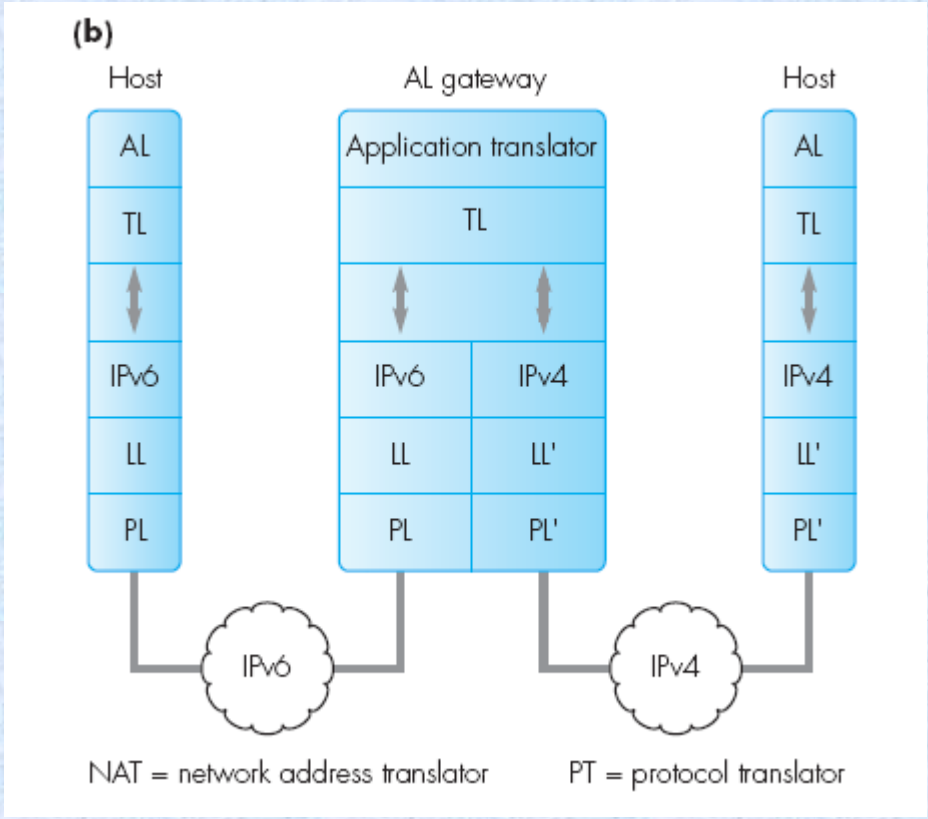
Interoperatividad V4/V6: túneles



Interoperatividad V4/V6: traductores



NAT-PT



ALG

IPv6: conclusiones

- IPv6 fue propuesto a mediados de los 90, y estandarizado finalmente en 1998 (RFC 2460)
- Inicialmente su adopción fue muy lenta
- Principalmente debido a la utilización de técnicas que redujeron la necesidad de direcciones públicas (NAT, direcciones privadas, etc.)
- Pero a partir de 2001 se aceleró la demanda de direcciones (principalmente dispositivos móviles)
- Su interacción con IPv4, si bien posible, dista de ser perfecta
- Lección: reemplazar protocolos de red es como tratar de reemplazar los cimientos de una casa!
- Es mucho más fácil reemplazar protocolos de nivel 4 y superiores (procesos)