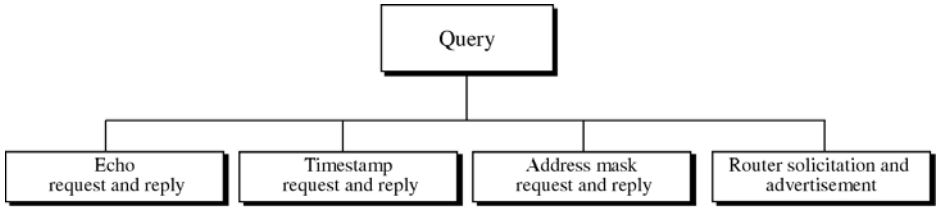
Índice hora 3

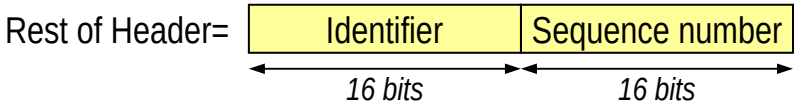
Objetivos

- Entender los esquemas de diagnóstico de una red y su aplicación para la identificación de problemas
- Asimilar el funcionamiento de redes multicast y el soporte necesario de protocolos específicos
- Introducir el futuro del protocolo IP

4.4 Mensajes ICMP petición/respuesta



- Cualquier ICMP request mandado a una máquina IP le hace devolver un ICMP reply.
- Para todos los ICMPs de petición/respuesta:

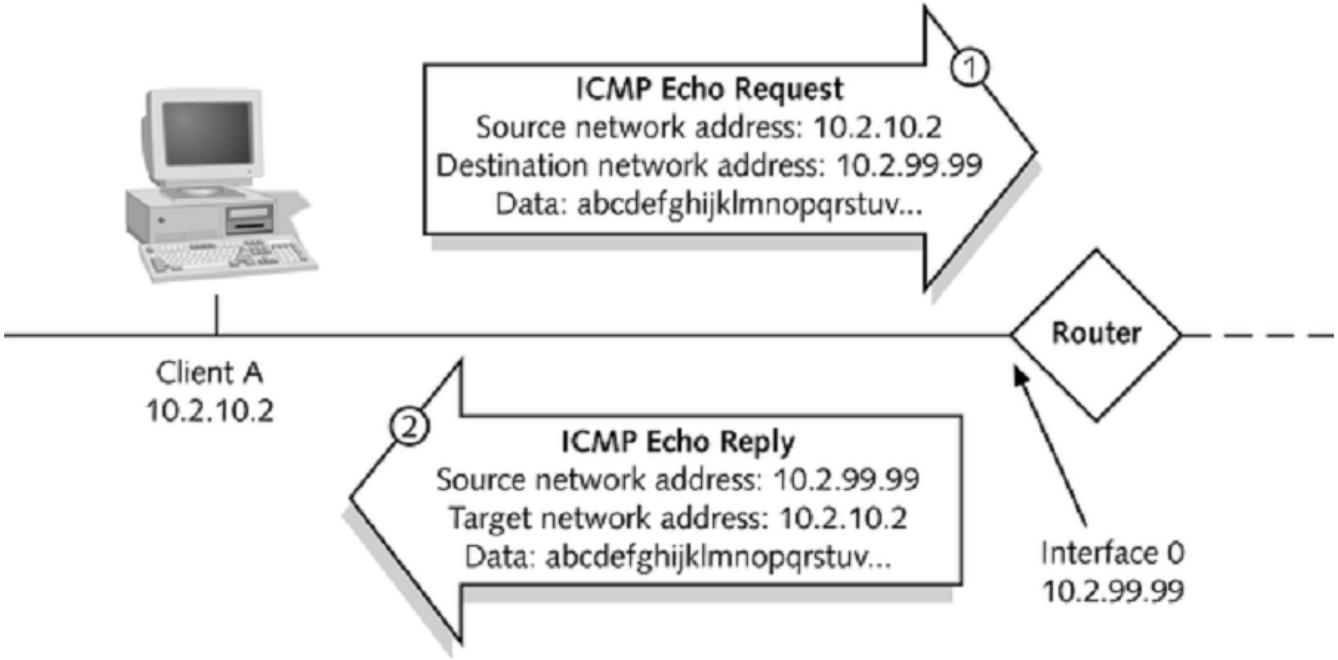


  - Identifier: normalmente el ID del proceso que lo genera.
  - Sequence number: numeración secuencial de los paquetes.

Type	Name	References
0	Echo Reply	RFC 792
1	Unassigned	
2	Unassigned	
3	Destination Unreachable	RFC 792
4	Source Quench	RFC 792
5	Redirect	RFC 792
6	Alternate Host Address	JBP
7	Unassigned	
8	Echo	RFC 792
9	Router Advertisement	RFC 1256
10	Router Solicitation	RFC 1256
11	Time Exceeded	RFC 792
12	Parameter Problem	RFC 792
13	Timestamp	RFC 792
14	Timestamp Reply	RFC 792
15	Information Request	RFC 792
16	Information Reply	RFC 792
17	Address Mask Request	RFC 950
18	Address Mask Reply	RFC 950

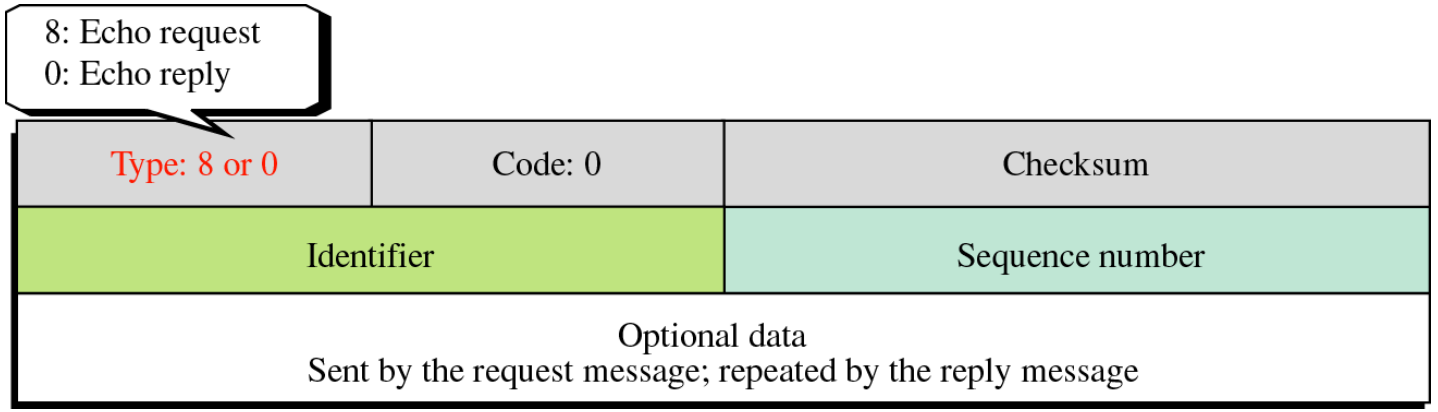
4.4.1 ICMP petición/respuesta: ECHO

- Se utiliza para testear la conectividad con una máquina remota.
- Obligada la implementación del servidor que responda con el echo-reply. Normalmente a nivel de kernel.
- Generador a nivel de aplicación: ping.



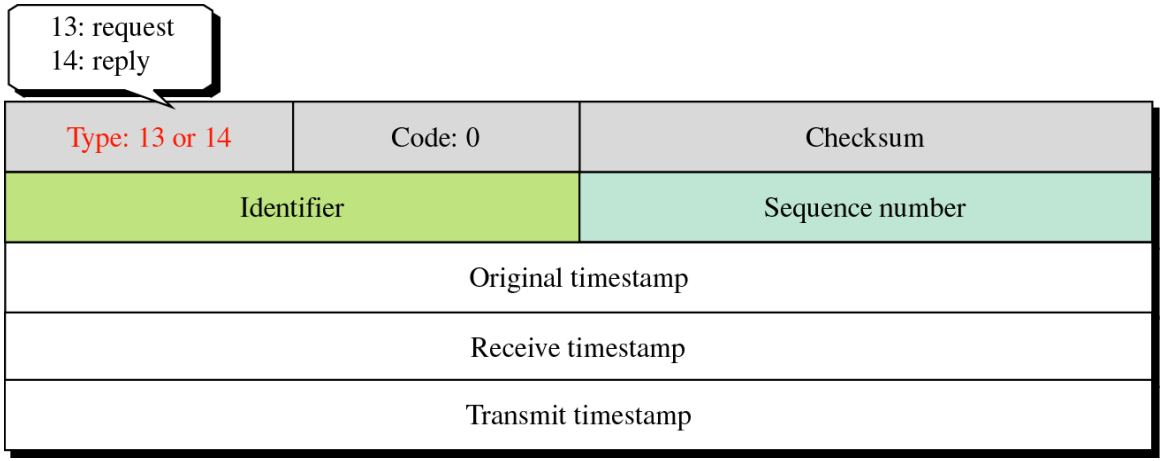
ICMP petición/respuesta: ECHO

- Cabecera ICMP ECHO:
  - Type:
    - 8: Echo request
    - 0: Echo reply
  - Code=0
  - Data section: lo que el Echo-Request mande ahí será copiado en el Echo-Reply.



4.4.2 ICMP petición/respuesta: Timestamp

- Referencias temporales de recepción/envío de paquetes.
  - Type:
    - 13: request
    - 14: reply
  - Code=0
  - Data section:
    - Original timestamp: rellenado por el emisor al enviar el paquete request.
    - Receive timestamp: rellenado por el receptor al recibir el paquete request.
    - Transmit timestamp: rellenado por el receptor al enviar de vuelta el reply.

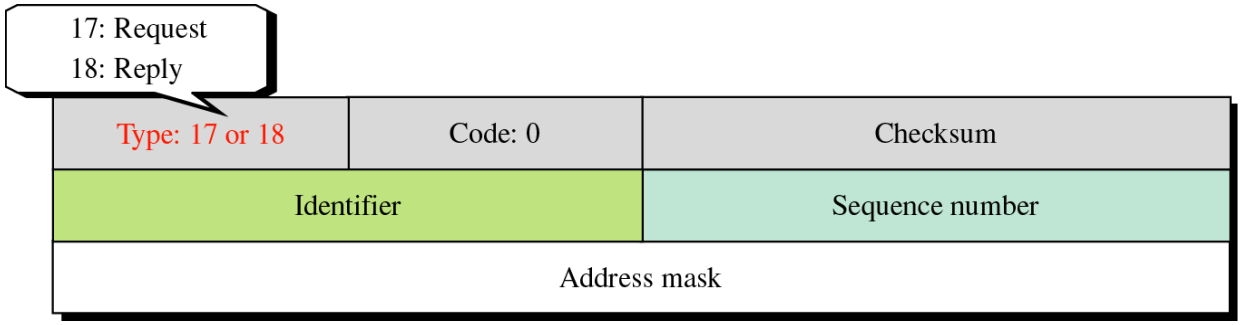


ICMP petición/respuesta: Timestamp

- Timestamps medidos en ms desde medianoche en UTC (Universal Coordinated Time).
- Si relojes de emisor/receptor estuvieran sincronizados:
  - Sending time= Receive timestamp - Original timestamp
  - Receiving time = Tiempo retorno paquete - Transmit timestamp
- Lo habitual es que los relojes no estén sincronizados:
  - Sending time= Receive timestamp - Original timestamp +/- offset
  - Receiving time = Tiempo retorno paquete - Transmit timestamp -/+ offset
  - Round Trip Time: RTT = Sending time + Receiving time
    - El error de sincronización se compensa.

4.4.3 ICMP petición/respuesta: Máscara

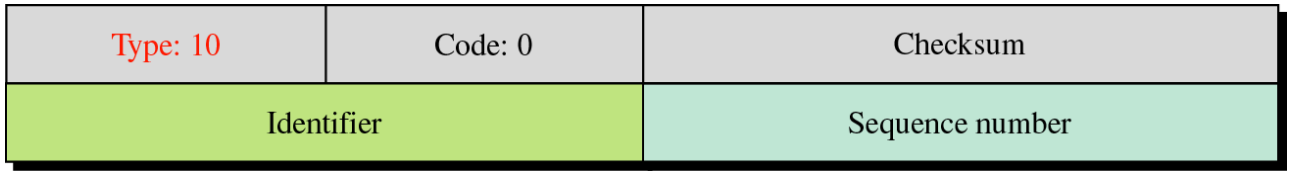
- Si una máquina conoce su dirección IP pero no su máscara de red, se la puede pedir con este ICMP:
  - al router que conozca.
  - o a una dirección de broadcast si desconoce el router.
  - Type:
    - 17: request
    - 18: reply
  - Code=0
  - Data section:
    - 0 en el request.
    - valor de la máscara del emisor en el reply.



4.4.4 ICMP petición/respuesta: Router

- Una máquina puede solicitar quien es el router con este mensaje por broadcast o multicast (solicitation).
- Los routers pueden:
  - Enviar por broadcast el anuncio del router (advertisement) ante un solicitation.
  - Enviar periódicamente todos los routers que conocen.

- Solicitation
  - Type=10
  - Code=0
  - Data Section: no existe.



ICMP petición/respuesta: Router

Type: 9	Code: 0	Checksum
Number of addresses	Address entry size	Lifetime
Router address 1		
Address preference 1		
Router address 2		
Address preference 2		
⋮		

- Advertisement
  - Type=9
  - Code=0
  - Rest of header:
    - Number of addresses: nº de direcciones que se adjunta.
    - Address entry size: tamaño de esas direcciones en palabras de 32 bits. (1 para IPv4)
    - Lifetime: segundos que estas direcciones se consideran válidas. Intervalos habituales de 30 min.
  - Data Section: listado de direcciones de routers junto con su prioridad en su elección. Si el campo de preferencia es 0 es el de por defecto y conforme crezca el valor de preferencia menor prioridad en su asignación.

5 IGMP

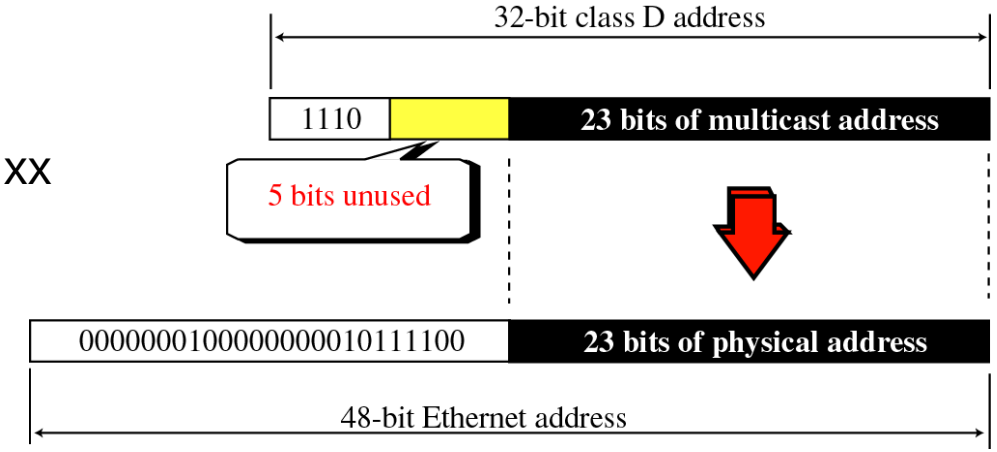
- Internet Group Management Protocol.
- IGMP es el protocolo encargado de gestionar la pertenencia a grupos multicast
  - Cada router mantiene una lista de grupos multicast para cada red en las que hay al menos una máquina participando en el grupo.
- Se encapsula por encima de IP y es de implementación recomendada. Los campos IP que fija son los siguientes:
  - Protocol=2
  - TTL=1, para evitar que los paquetes IGMP salgan de la LAN.
- Versiones
  - v1 [RFC1112], 1989: primitivas de unión a grupo y sondeo periódico.
  - v2 [RFC 2236], 1997: añade primitiva de abandono de grupo.
  - v3 [RFC 3376], 2002: permite recibir grupo multicast pero seleccionar dentro de él el tráfico procedente de ciertas direcciones IP.
- Estudiaremos la v2, más extendida en la actualidad.

IGMP

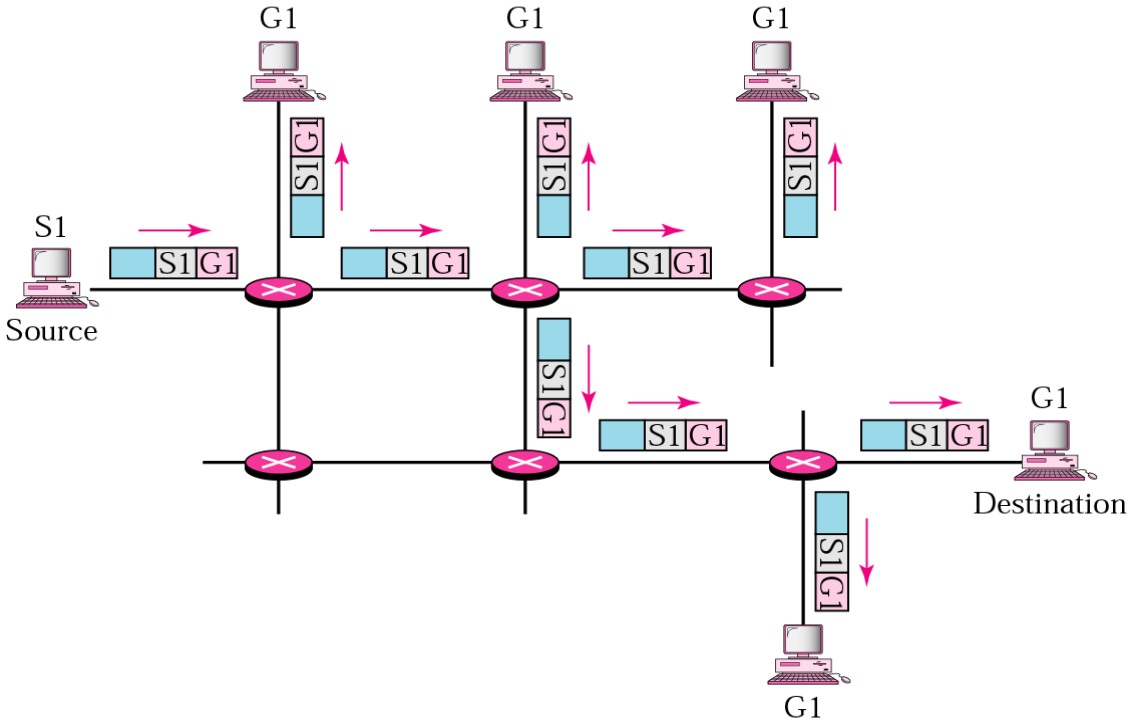
- Direcciones IP destino posibles:
  - 224.0.0.1: todos las máquinas y routers en esta red (ALL-SYSTEMS.MCAST.NET).
  - 224.0.0.2: todos los routers en esta red (ALL-ROUTERS.MCAST.NET).
  - Resto direcciones clase D: dirección de grupo.

- Convenio en el mapeo de direcciones multicast IP a MAC.

01:00:5E:0xx:xx:xx

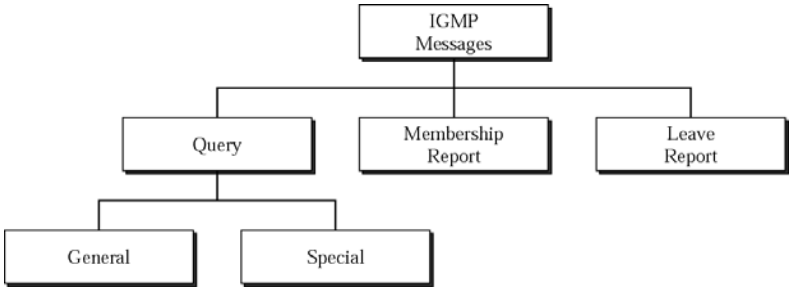


IGMP, multicast

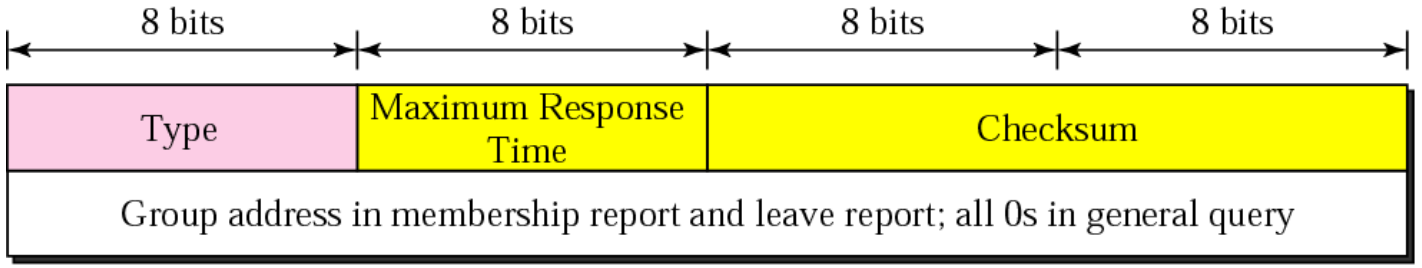


- Cada máquina informa a través de IGMP a su router de en qué grupo multicast está interesada.
- Los routers interaccionan entre sí para recibir los grupos multicast en caso de que en su red haya alguna máquina interesada.
- Protocolos de enrutamiento multicast entre routers:
  - DVMRP (Distance Vector Multicast Routing Protocol)
  - MOSPF (Multicast OSPF)
  - PIM (Protocol Independent Multicast)
  - MBONE (Multicast Backbone)

5.1 Cabecera IGMP v2



- Type (8bits):
  - 0x11 General o Special Query
  - 0x16 Membership Report
  - 0x17 Leave Report
- Maximum Response Time (8bits): define el tiempo máximo en el que debe contestarse a un Query. Se mide en décimas de segundo.
- Checksum (16bits): se calcula sobre los 8 bytes de la cabera IGMP.
- Group address (32bits):
  - 0 en el General Query.
  - Dirección de grupo multicast en el resto Special, Membership y Leave.



5.2 Unión a grupo

- Una máquina o router puede unirse a un grupo para recibir el flujo de paquetes pertenecientes a ese grupo. Para ello mandará un Membership Report con:
  - IP destino (cabecera IP): dirección de grupo multicast.
  - Group address: dirección de grupo multicast.
  - Type: 0x16.
- Se envían siempre 2 veces por si se pierde el primero.
- Los routers deben escuchar todos los grupos multicast para recibir estas peticiones.

5.3 Abandono de grupo

- Para dar de baja un grupo multicast, la máquina o router apuntado manda un Leave Report:
  - IP destino (cabecera IP): 224.0.0.2
  - Group address: dirección de grupo multicast.
  - Type: 0x17.
- Entonces el router se asegura que no hay nadie más escuchando ese grupo mandando un Special Query:
  - IP destino (cabecera IP): 224.0.0.1
  - Group address: dirección de grupo multicast.
  - Type: 0x11.
  - Maximum Response Time: cierto valor. Si nadie responde en el tiempo fijado por este campo elimina el grupo.

5.4 Monitorización de grupo

- Puede ocurrir que una máquina deje de escuchar un grupo sin haber mandado un mensaje de abandono (Ej: se ha apagado).
- Para controlarlo, el router periódicamente (125 sg por defecto) manda un General Query:
  - IP destino (cabecera IP): 224.0.0.1
  - Group address: 0.0.0.0 (no especifica grupo, espera respuesta de todos).
  - Type: 0x11.
  - Maximum Response Time: cierto valor.
- Una máquina que escuche ese grupo contesta con un Membership Report.
- Si ha varias máquinas, sólo una contesta. El que va a transmitir en segundo lugar ha visto el mensaje Membership Report del 1º por lo que cancela su mensaje.

Monitorización de grupo

- Si ninguna máquina contesta en el Maximum Response Time, el grupo se eliminará.
- Para evitar tráfico excesivo en una red con varios routers, sólo uno de ellos se encarga de hacer el General Query, y el resto actualizan de forma pasiva sus listas observando las respuestas.

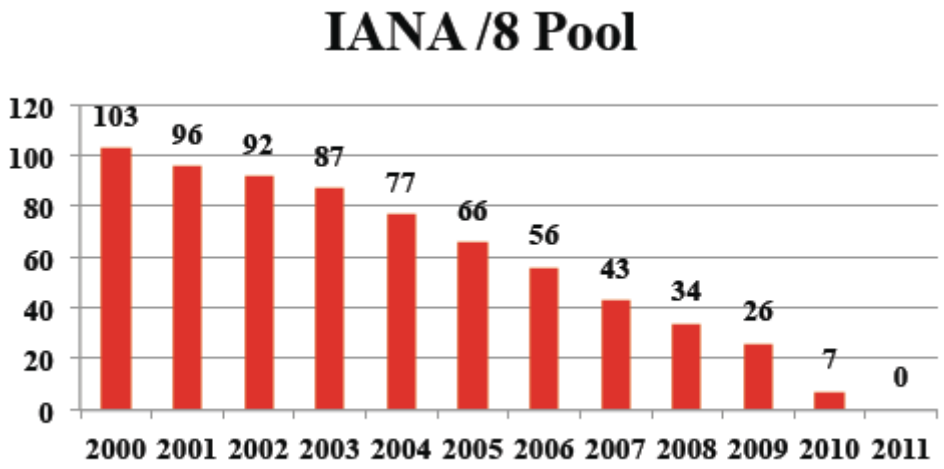
6 Evolucionando IP: IPv6

- Principales deficiencias de IPv4:
  - Falta de espacio de direccionamiento y organización correcta del mismo.
  - Varios campos de la cabecera básica que no se utilizan siempre (por ejemplo, campos relacionados con fragmentación)
  - Existencia de checksum reiterativo con respecto a checksums de niveles inferiores
  - Cabecera de tamaño variable
  - Estrategias de provisión de calidad de servicio: TOS/DS de IPv4 apenas utilizado.
  - Encriptación y autentificación no nativo: IPv4 necesita de un protocolo añadido como IPsec.
  - Muchas modificaciones dispersas en RFCs. Protocolo demasiado “parcheado”.

- IPv6 = IPv4 + más de 40 años de experiencia.

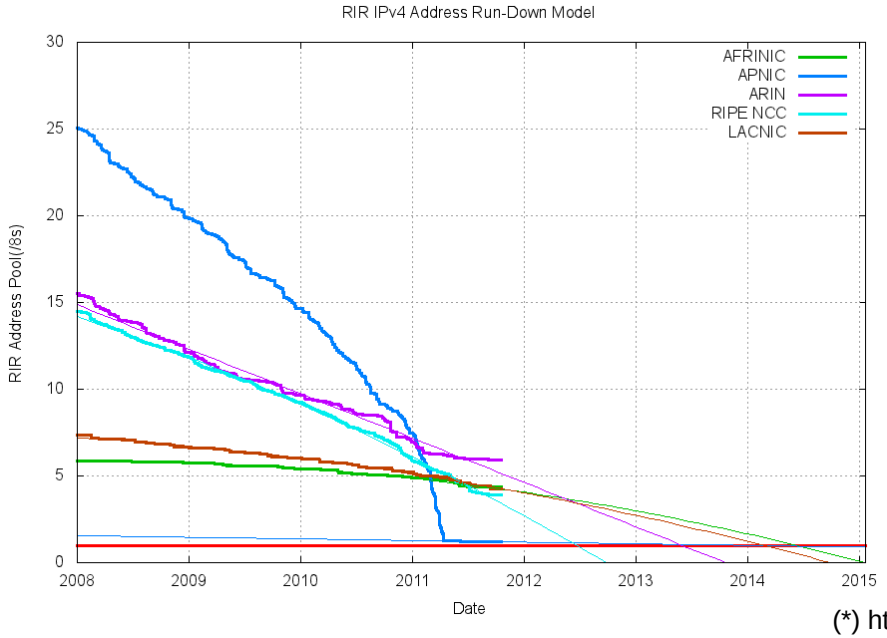
Agotamiento de direcciones IPv4

- Mecanismos como NAT han ido asimilando la demanda de direccionamiento en los últimos años
  - Direccionamiento privado a nivel de ISP o empresa
  - Problemática en el desarrollo de nuevos servicios
- ICANN ya ha asignado todos sus bloques /8 a los registradores regionales (RIRs):
  - 3 de febrero de 2011
  - Posee todavía un rango limitado reservado para nuevos operadores



Agotamiento de direcciones IPv4

- El agotamiento de direcciones IPv4 ya está ocurriendo
  - APNIC: 14 abril 2011
  - RIPE: estimado junio 2012
  - ARIN: estimado junio 2013
  - LACNIC: estimado febrero 2014
  - AfriNIC: estimado junio 2014



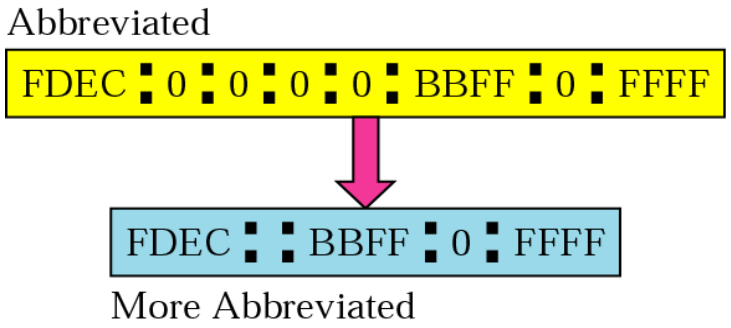
(*) http://www.potaroo.net/tools/ipv4/index.html

6.1 Características IPv6

1. Mayor espacio de direcciones: 128 bits (16 bytes)
2. Mejor formato de la cabecera: tamaño fijo (40 bytes). Las opciones se manejan como cabeceras de protocolos superiores. Mayor rapidez porque los routers muchas veces no las necesitan.
3. Se elimina el checksum (evitar recalcularlo en cada salto, únicamente decremento del hop limit-TTL)
4. Posibilidad de definir opciones/extensiones nuevas con facilidad de cara a futuras mejoras.
5. Mecanismo de reserva de recursos mediante etiquetas de flujo en la cabecera.
6. Opciones de autentificación, integridad de datos y privacidad.
7. Modelo de enrutamiento jerárquico desde el principio.
8. Soluciones de autoconfiguración (plug-and-play).
9. Soluciones para movilidad.

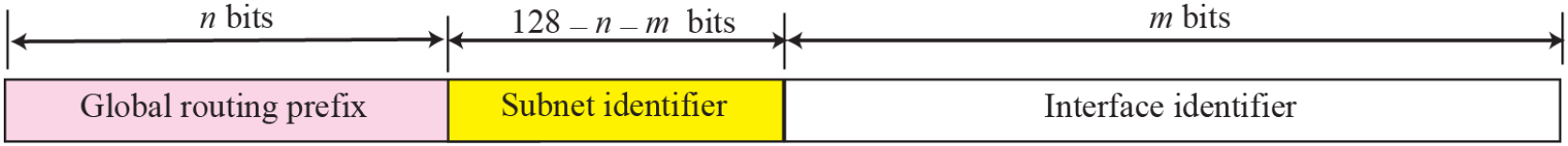
6.2 Direcciones IPv6

- Espacio de direcciones: 128 bits (16 bytes)
  - Representadas en hexadecimal de 2 en 2 bytes separados por ":" (8 palabras
    - Ej1: FDEC:000F:BA98:5555:4321:3742:1111:2222
    - Ej2: FDEC:0000:0000:0000:0000:3742:0000:2222
      - Notación abreviada: FDEC:0:0:0:0:3742:0:2222
      - Notación más abreviada: se puede resumir una secuencia de 0's consecutivos colocando "::" en su lugar: FDEC::3742:0:2222
    - Máscara CIDR como hasta ahora: FDEC::3742:0000:2222 / 60 (máscara con 60 bits a 1 al principio de la misma).



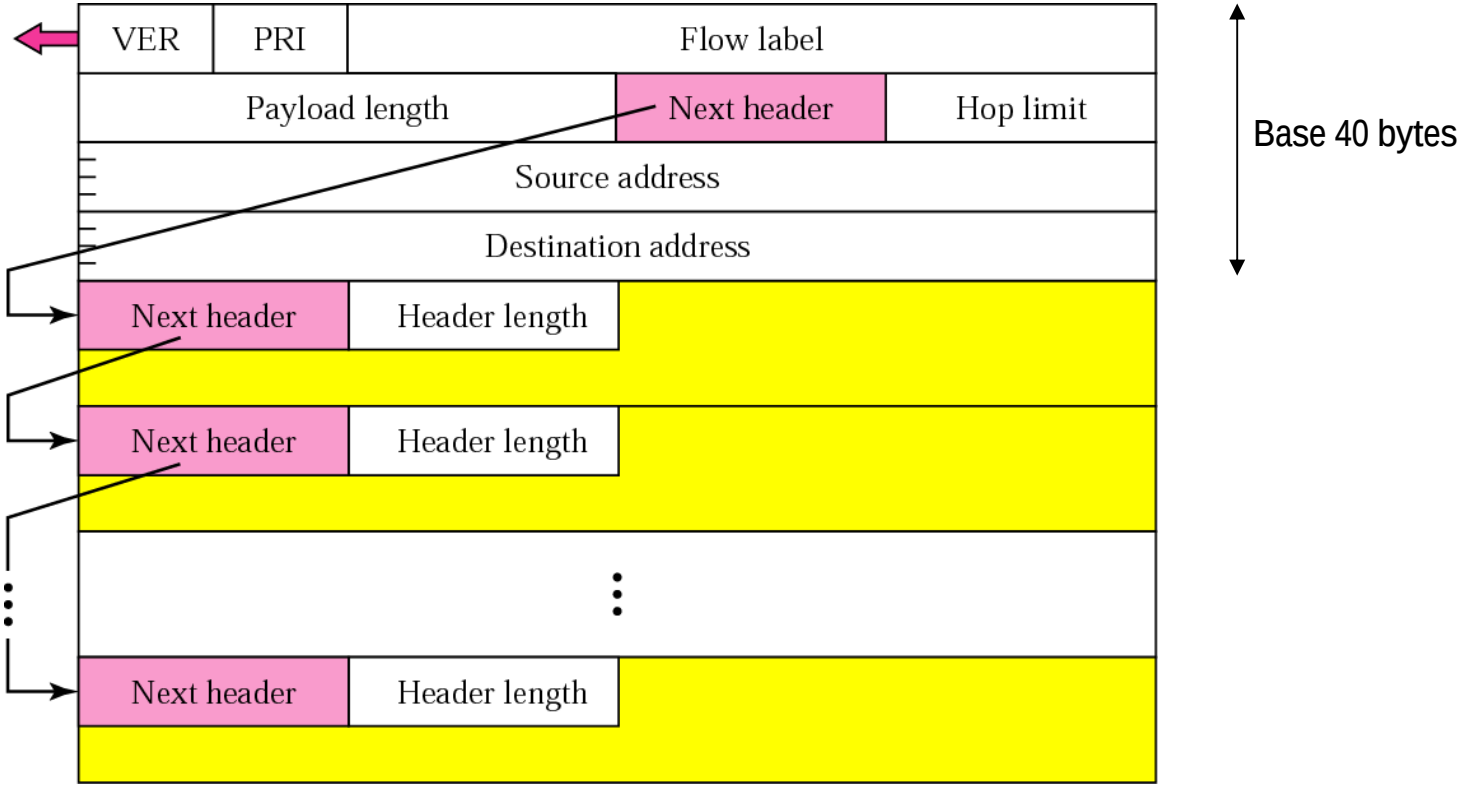
Direcciones IPv6

- El tamaño de 128bits de IPv6 está elegido para poder tener direcciones en cualquier elemento de la vida cotidiana: Internet de las cosas
  - 2^{128}=340.282.366.920.938.463.463.674.607.431.770.000.000 (340 sextillones)
  - Si las direcciones IPv4 se mapeasen en una pelota de golf, las direcciones IPv6 equivaldrían al tamaño del sol
  - Asignado a cada persona del planeta una red /48, se estima su suficiencia en 480 años (antes serían de esperar muchos cambios…)
- Formato de las direcciones:



Block Assignment	*Length*
Global routing prefix (n)	48 bits
Subnet identifier ($128 - n - m$)	16 bits
Interface identifier (m)	64 bits

6.3. Cabecera IPv6

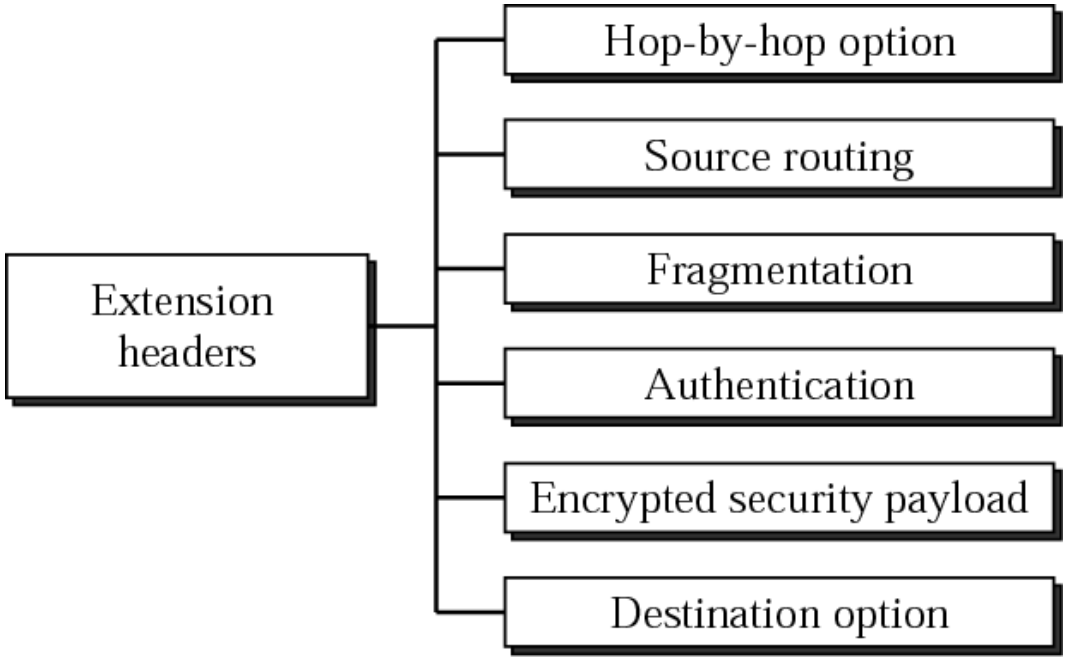


Campos cabecera IPv6

- Version (4bits)
  - 0x6 para IPv6.
- Priority (4bits)
  - Prioridad del paquete ante situaciones de congestión: 0-baja, 7-alta.
- Flow label (24bits)
  - Etiquetado para manejo de flujos con QoS.
- Payload length (16bits)
  - Tamaño total del datagrama IP excluida la cabecera base de 40 bytes (=opciones+datos).
- Next header (8bits)
  - Identifica la siguiente cabecera de extensión opcional y, si no la hay, el protocolo de siguiente nivel que encapsula.
- Hop limit (8bits)
  - Equivalente al campo TTL de IPv4.

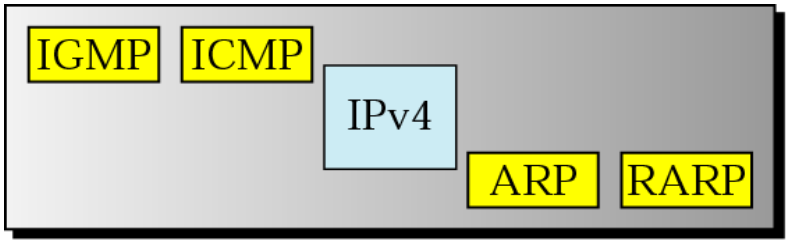
Campos cabecera IPv6

- Source/Destination address (128bits cada uno)
- Extension headers
  - Proveen opciones como IPv4 y nuevas extensiones.

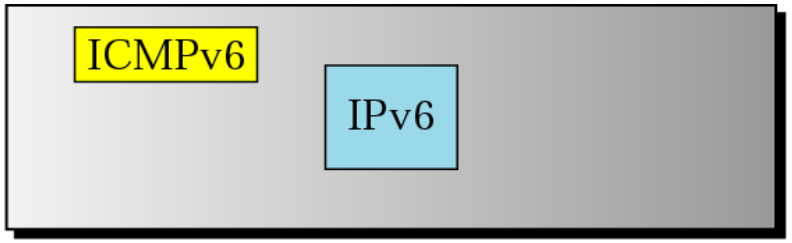


6.4 IPv6 protocolos de soporte

- Necesidad de definir nuevos protocolos de soporte a IPv6. ICMPv6 da las funcionalidades del conjunto de protocolos de IPv4 ARP, RARP, ICMP e IGMP.



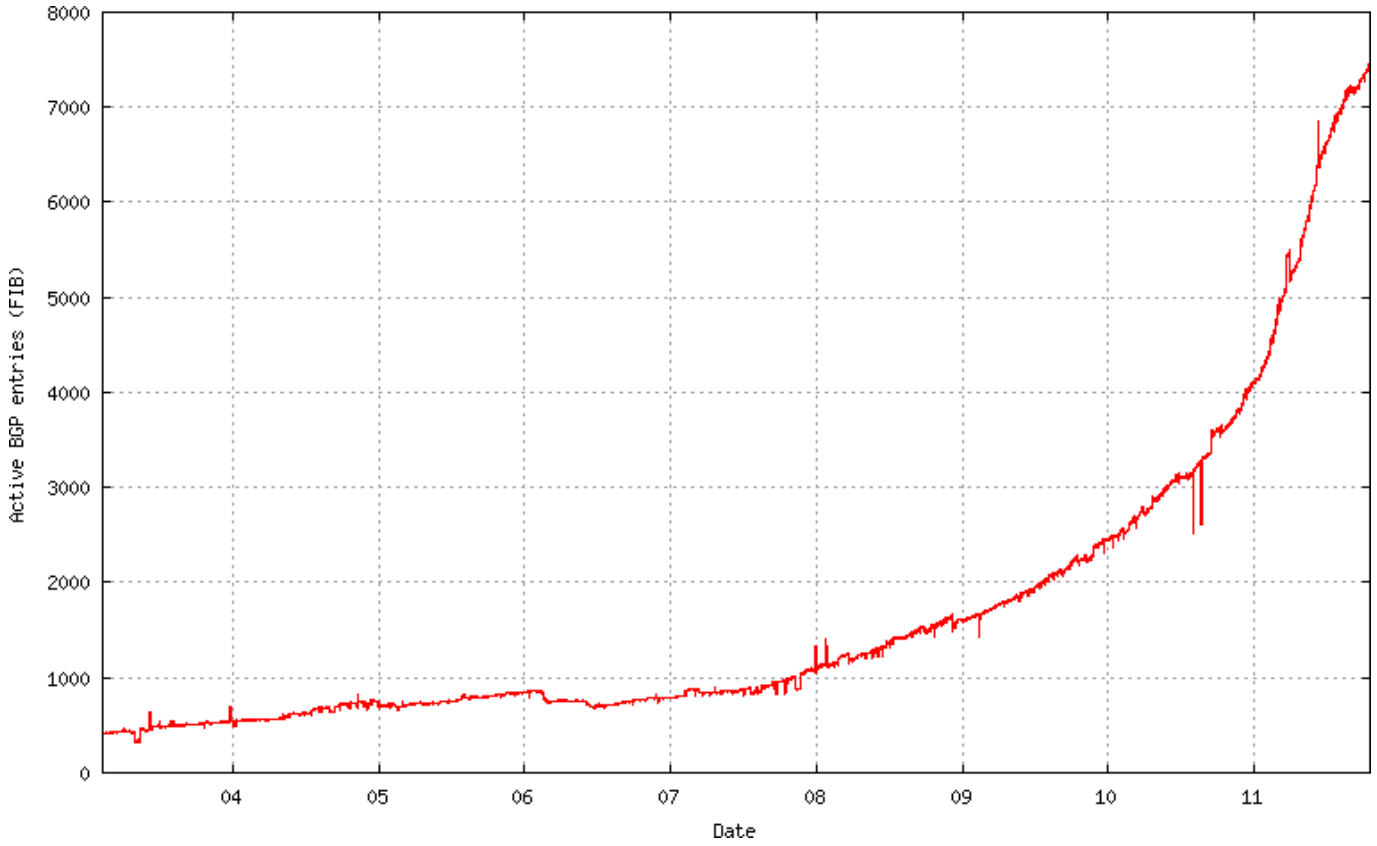
Network layer in version 4



Network layer in version 6

6.5 Grado de implantación de IPv6

- Redes IPv6 anunciadas (muy por debajo de las IPv4 cerca de 400.000)



http://bgp.potaroo.net/v6/as2.0/index.html

Resumen

- ICMP Echo se utiliza para diagnóstico de conectividad
  - Problema de filtrad en routers intermedios, firewalls extremo e incluso en las propias máquinas finales
- IGMP permite a una máquina de una LAN notificar a su router sobre qué flujos multicast está interesada en recibir
  - Entre routers hablan otros protocolos de enrutamiento multicast
- IPv6, con la excusa del agotamiento de direcciones en IPv4, solventa las principales deficiencias de IPv4
  - Direcciones IPv6 de 128bits
  - Cabecera básica con opciones
  - Campos de fragmentación relegados a opcin

Referencias

- [Forouzan]
  - Capítulo 9 “ICMPv4”, secciones 9.1-9.3 “Introduction”, “Messages”, “Debugging tools”
  - Capítulo 12 “Multicasting and Multicasting Routing Protocols”, secciones 12.1-12.3 “Introduction”, “Multicast addresses”, “IGMP”
  - Capítulo 27 “IPv6 Protocol”, secciones 27.1-27.2 “Introduction”, “Packet format”
- [Stevens]
  - Capítulo 7 “Ping Program”
  - Capítulo 13 “IGMP: Internet Group Management Protocol”