Capítulo 2. IP avanzado

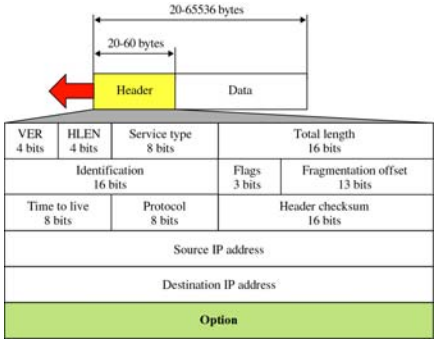
Redes de Ordenadores
5º Ingeniero de Telecomunicación

Índice

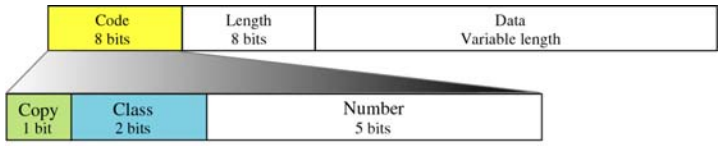
1 Campos opcionales IPv4
2 Direcciones IP especiales
3 NAT
4 Protocolos de soporte a IP
5 ARP
    5.1 Proxy ARP
    5.2 Gratuitous ARP
6 Asignación de direcciones IP
    6.1 RARP
    6.2 BOOTP/DHCP
7 ICMP
    7.1 Paquete ICMP
    7.2 Tipos de mensajes ICMP
        7.2.1 Mensajes ICMP de error
        7.2.2 Mensajes ICMP petición/respuesta
8 IGMP
    8.1 Cabecera IGMP v2
    8.2 Unión a grupo
    8.3 Abandono de grupo
    8.4 Monitorización de grupo
9 Evolucionando IP
    9.1 Mobile IP
    9.2 IPv6
        9.2.1 IPv6 características
        9.2.2 Cabecera IPv6
        9.2.3 IPv6 protocolos de soporte
        9.2.4 Transición a IPv6
        9.2.5 Grado de implantación de IPv6

1 Campos opcionales IPv4

- Options (0-40bytes)
  - Proveen funcionalidades de testeo de la red.
  - Se organizan en una estructura Code+Length+Data. Los datos son de longitud variable.
  - Siempre se realiza padding (relleno) de las opciones a múltiplos de 32 bits (palabras de HLEN).



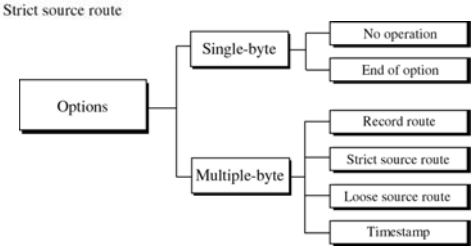
Campos opcionales IPv4



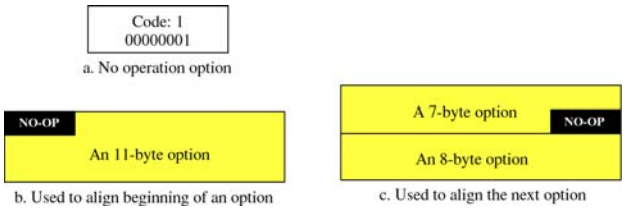
Copy
0 Copy only in first fragment
1 Copy into all fragments

Class
00 Datagram control
01 Reserved
10 Debugging and management
11 Reserved

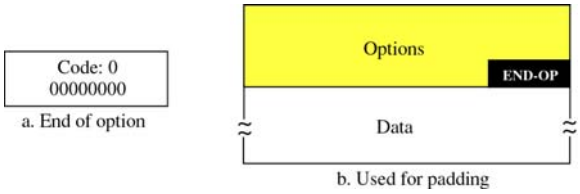
Number
00000 End of option
00001 No operation
00011 Loose source route
00100 Timestamp
00111 Record route
01001 Strict source route



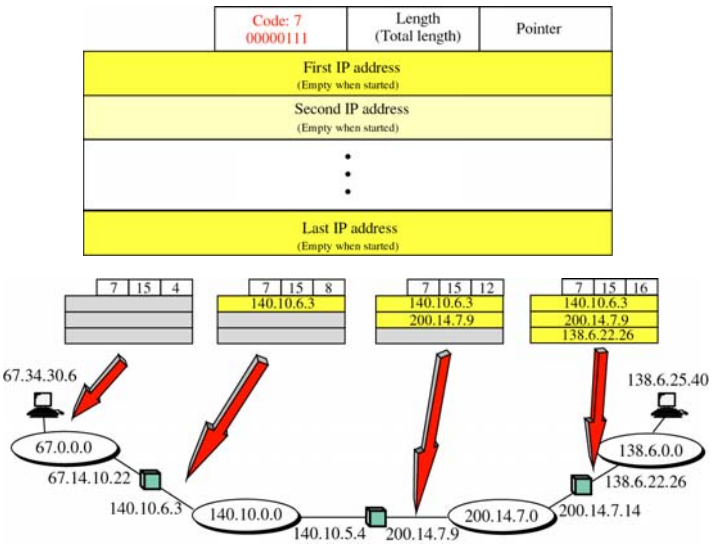
Opción: No operación



Opción: Fin de opciones

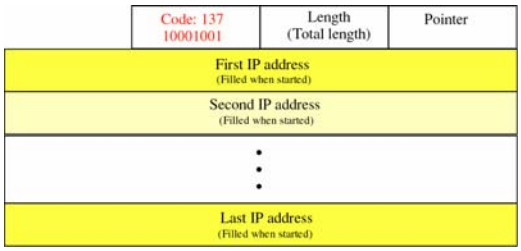


Opción: Record route

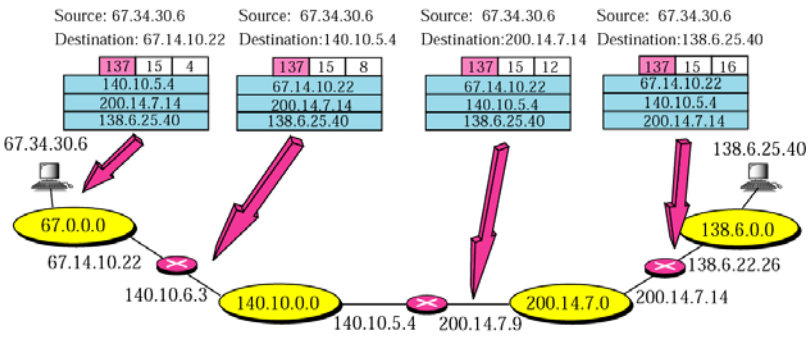


Opción: Enrutamiento fuente estricto

- El origen especifica el camino que ha de seguir el paquete con las IPs de los routers a atravesar. Máximo 9 saltos.
- Si no se puede seguir el camino fijado se tira el paquete.
- El primer salto está en pointer=4.
- Cuando el paquete llega a un router, comprueba que el puntero sea menor que la longitud y reemplaza la IP destino del paquete con la apuntada por el pointer y reemplaza la dirección apuntada por el pointer con la dirección IP de su interfaz de entrada.

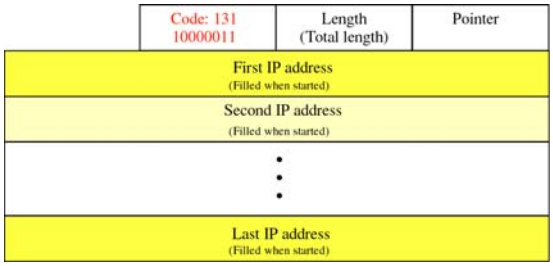


Opción: Enrutamiento fuente estricto



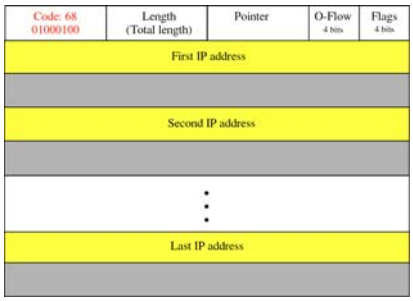
Opción: Enrutamiento fuente débil

- Fija algunas IPs de routers a visitar, pero se pueden atravesar otros routers también.
- Se sigue el mismo procedimiento de reemplazo de direcciones que con el enrutamiento fuente estricto.

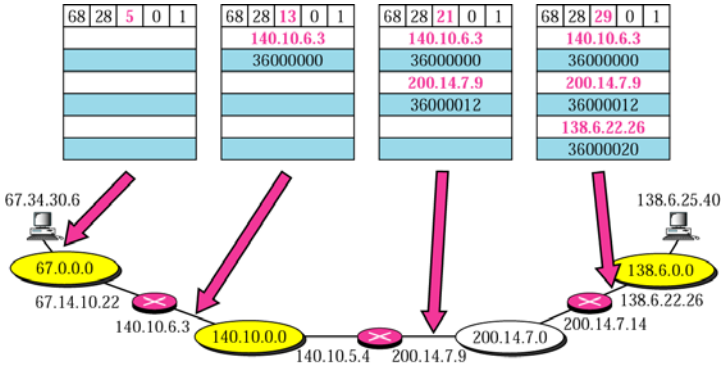


Opción: Timestamp

- Almacena los timestamps de cada router junto con sus direcciones IP.
- Los timestamps son en milisegundos desde medianoche UTC.

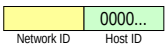


Opción: Timestamp



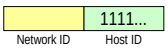
2 Direcciones IP especiales

- Direcciones de red: HostID=0's
  - La primera dirección de una red (HostID=0) hace referencia a la propia red. No se puede utilizar para identificar una máquina.



Ej: 198.200.26.0/24

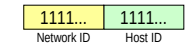
- Direcciones de broadcast dirigidas: HostID=1's
  - Hace referencia a todas las máquinas de la red.
  - Un router lo puede reenviar si procede de otra red (como si fuera un paquete unicast normal) y al llegar a la red destino se envía como broadcast de nivel de enlace.
  - Normalmente esta funcionalidad de reenvío se desactiva (para evitar ataques).



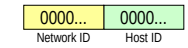
Ej: 198.200.26.255/24

Direcciones IP especiales

- Dirección de broadcast limitado: 255.255.255.255
  - Se interpreta como broadcast a nivel de enlace dentro de la LAN.
  - Los routers no lo reenvían fuera de la misma ⇒ imposible hacer broadcast a todo Internet (exceso de tráfico).
- Esta máquina en esta red: 0.0.0.0
  - Hace referencia a la propia máquina/interfaz.
  - Se utiliza únicamente como dirección origen en momentos donde todavía no se tiene IP (Ej: antes de conseguirla por DHCP).



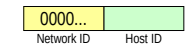
Dirección IP: 255.255.255.255



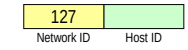
Dirección IP: 0.0.0.0

Direcciones IP especiales

- Determinada máquina en esta red: NetID=0's
  - Se utiliza únicamente como dirección destino, para enviar mensajes a una máquina de la misma red.
  - Nunca se reenvía en los routers.
- Loopback: red 127.0.0.0/8
  - Paquetes enviados a esta dirección no salen de la máquina y se retornan a la misma.
  - Útil para verificar software TCP/IP.
  - localhost



Ej: 0.0.0.3/24



Ej: 127.0.0.1/8

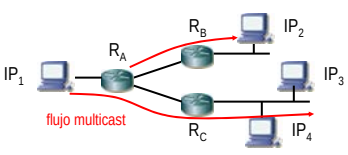
Direcciones IP especiales

- Direcciones privadas [RFC1918]
  - Reservadas para uso interno dentro de organizaciones pero nunca para conectarse a Internet.
  - Se pueden reutilizar en diferentes redes siempre que esas redes no estén conectadas entre sí.
  - Rangos
    - 10.0.0.0/8
    - 172.16.0.0/12
    - 192.168.0.0/16
  - Necesidad de conversión de direcciones: NAT (Network Address Translation), NAPT (Network Address Port Translation) o Proxy.

Direcciones IP especiales

- Direcciones multicast: 224.0.0.0/4
  - Permiten la comunicación uno a varios en contraposición a las direcciones unicast ordinarias que permiten la comunicación uno a uno.
  - Cuando una máquina quiere recibir las emisiones dirigidas a un grupo multicast, debe unirse al grupo mandando un mensaje IGMP (Internet Group Management Protocol) al router. A partir de ahí el router mandará los mensajes multicast a la LAN donde se encuentra la máquina.
  - A un grupo multicast se puede añadir un número ilimitado de máquinas.
  - Son siempre direcciones destino (nunca origen).

  Ej:
  - IP_1 genera un flujo multicast.
  - IP_4 se apunta al grupo y empieza a recibir el flujo.
  - IP_3 se apunta y recibirá los mismos paquetes que IP_4 (no se duplican).
  - IP_2 se apunta y R_A tendrá que duplicar el flujo de paquetes.

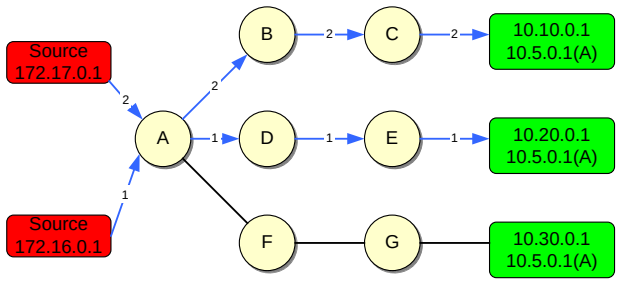


Direcciones IP especiales

- Direcciones públicas/unicast
  - Rango fuera de las privadas, broadcast y multicast
  - Únicas para todo Internet (no se pueden reutilizar entre máquinas distantes)
- Direcciones anycast
  - Una dirección anycast define un grupo de máquinas que comparten la misma dirección IP.
  - Un paquete dirigido a una dirección anycast se entrega únicamente al miembro del grupo con mejor alcanzabilidad.
  - Puede ser cualquier dirección en el rango de las unicast.
  - Aparece especialmente en escenarios IPv6.

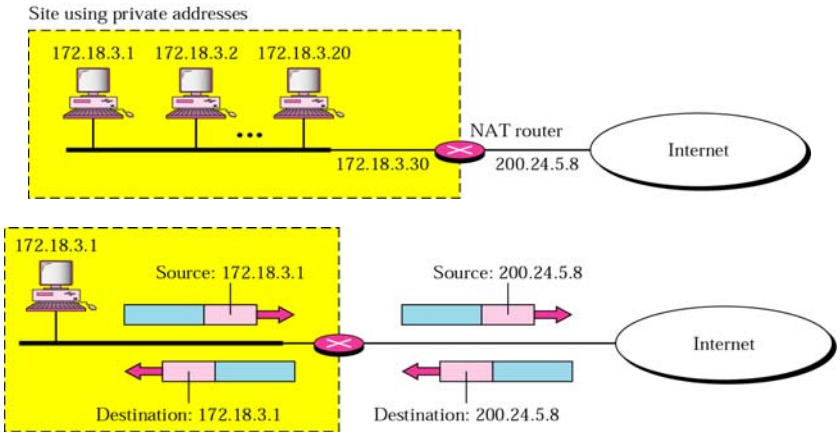
Direcciones IP especiales

- Anycast selecciona el miembro destino dependiendo
  - del origen
  - del número de paquete
  - del estado de las máquinas destino
  - del coste del camino extremo a extremo

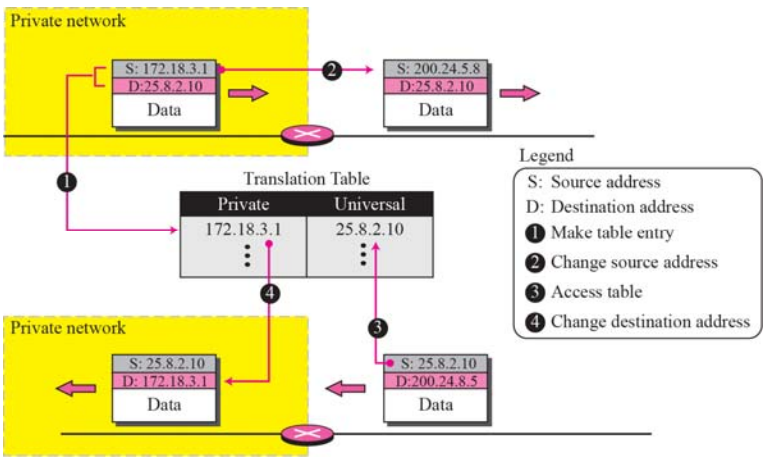


3 NAT

- NAT (Network Address Translation)
  - Mapeo N direcciones privadas en N direccions públicas



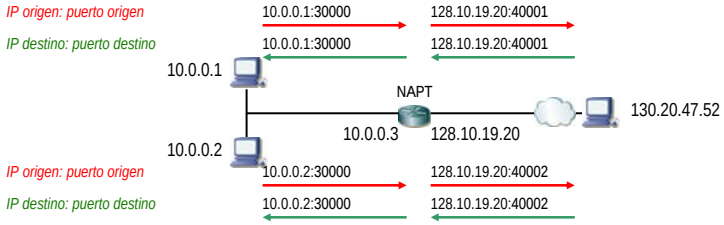
NAT uno a uno



NAPT/PAT

- NAPT (Network Address Port Translation) / PAT (Port Address Translation)
  - Utilizar los puertos UDP/TCP para multiplexar varias máquinas con direccionamiento privado sobre una (o varias) direcciones públicas.

Direction	Fields	Old Value	New Value
out	IP SRC:TCP SRC	10.0.0.1:30000	128.10.19.20:40001
out	IP SRC:TCP SRC	10.0.0.2:30000	128.10.19.20:40002
in	IP DEST:TCP DEST	128.10.19.20:40001	10.0.0.1:30000
in	IP DEST:TCP DEST	128.10.19.20:40002	10.0.0.2:30000



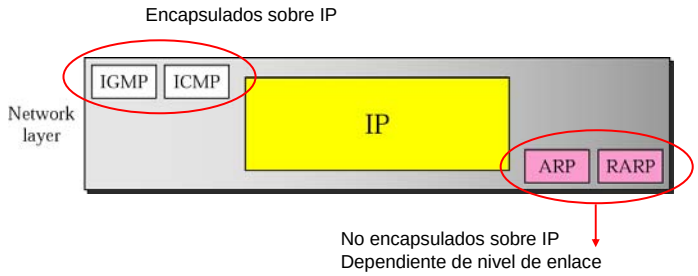
NAT

- Ventajas
  - Reduce el consumo de direcciones IPv4
  - "Oculta" las máquinas internas de cara a accesos externos o ataques
- Inconvenientes
  - Rompe el principio de conectividad extremo a extremo de Internet
  - El NAT modifica los paquetes: direcciones IPs, puertos, CRC
    - Algunas aplicaciones codifican información dependiente de IPs o puertos desconociendo los efectos del NAT: FTP, SIP, H.323, etc.
    - El router puede adaptar los paquetes si conoce el funcionamiento de las aplicaciones. Elevado coste de adaptación y procesado. Application layer gateway (ALG)
  - Dificulta colocar servidores en la red interna
    - Proceso de redirección de puertos o abrir puertos
  - Introduce retardo extra
    - Recalcular checksum de IP y TCP

RFC-1918: Address Allocation for Private Internets
RFC-1631:The IP Network Address Translator (NAT)
RFC-2993: Architectural Implications of NAT
RFC-3027: Protocol Complications with the IP Network Address Translator

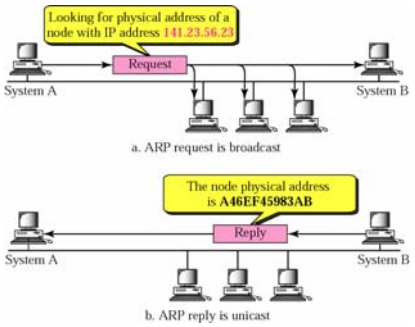
4 Protocolos de soporte a IP

- Para el correcto funcionamiento del protocolo IP se hace necesario utilizar una serie de protocolos complementarios:
  - ARP, RARP, DHCP - mapeo de direcciones físicas (MAC) con lógicas (IP).
  - ICMP - Notificación de problemas y errores. Supervisión del funcionamiento de la red.
  - IGMP - Gestión de grupos multicast.



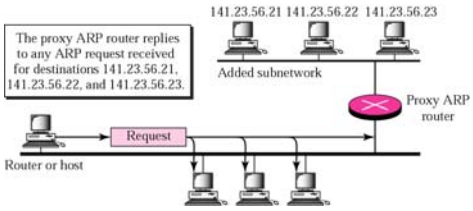
5 ARP

- Al enviar paquetes a una máquina normalmente sólo se conoce su dirección IP o nombre simbólico (DNS).
- Sin embargo, los datagramas IP se encapsulan sobre un nivel de enlace que necesita conocer las direcciones físicas de los equipos implicados.
- Necesidad de un mapeo IP → MAC: ARP (Address Resolution Protocol)



5.1 Proxy ARP

- Los routers trabajan a nivel IP y no reenvían ARPs. Si 2 patas de un router están en la misma red IP pero en 2 segmentos separados, puede interesar que conteste peticiones ARP de un segmento en nombre de máquinas del segundo segmento. Esto es el proxy ARP, promiscuous ARP o ARP hack.
- El router se hace pasar por las máquinas del segundo segmento respondiendo con su MAC a las peticiones del primer segmento.



Proxy ARP

- Cuando el router reciba el paquete dirigido a su MAC pero a una IP del segundo segmento lo reenviará como es habitual.
- Ambos segmentos deben pertenecer a la misma red IP: direcciones IP de las máquinas dentro de la misma red. Se hace necesario por tanto una configuración en el router para indicarle las direcciones IP existentes en cada segmento o dividir la red IP en dos subredes IP diferenciables por el router.
- Ventaja:
  - Bloquea el tráfico de broadcast.
  - Disminuye el tráfico de ARP: una petición de ARP no inunda ambos segmentos, tan sólo uno.
  - Aisla ambos segmentos aunque pertenezcan a la misma red de forma transparente. Útil por ejemplo en implementaciones antiguas de TCP/IP con alguna incompatibilidad, por ejemplo sin soporte de subnetting.

5.2 Gratuitous ARP

- Consiste en lanzar periódicamente un ARP request solicitando la MAC de la IP de la propia máquina para:
  - Comprobar si hay otra máquina en la misma LAN que está utilizando su misma IP. No es admisible duplicidades de máquinas con la misma IP y se podría producir un mal funcionamiento de la red.
  - Actualizar la caché de ARP del resto de máquinas de la red.

6 Asignación de direcciones IP

- El proceso de configuración manual de la información de red para máquinas de una red mediana o grande se convierte en un problema grave de gestión
  - Control de altas/bajas
  - Evitar direcciones IP duplicadas
  - Reparto eficiente del direccionamiento (multiplexación)
- Se hace necesario por tanto un proceso que permita asignar automáticamente la información de red a una máquina en su arranque.
  - Esa información podrá cambiar de un arranque al siguiente
  - Esa información no podrá ser secuestrada por la máquina de forma indefinida (si se apaga por ejemplo)

6.1 RARP

- Reverse Address Resolution Protocol.
- Permite el proceso inverso al ARP de obtención de la dirección IP de la máquina conociendo su dirección MAC.
- Un servidor de RARP contiene el mapeo IP-MAC de todas las máquinas de la red. El RARP request es *broadcast* para llegar a todas las máquinas, pero sólo contesta el servidor RARP de forma *unicast*.
- La cabecera es como la de ARP cambiando sólo el campo de operación:
  - 3: RARP request,
  - 4: RARP reply.
- Utilidad: asignación dinámica de dirección IP a una máquina en función de su MAC. Funcionalidad muy limitada en la actualidad porque la configuración de red va más allá de las dirección IP: máscara, router por defecto, servidores de DNS, etc.

6.2 BOOTP/DHCP

- Protocolos que proveen esas funcionalidades añadidas:
  - BOOTP, Bootstrap Protocol
    - Sobre UDP, puertos 67(servidor)-68(cliente).
    - Solicitud sobre paquete con IP destino broadcast.
    - Permite especificar la máscara, router por defecto, DNS e incluso un fichero con código de arranque para la máquina (descargable vía TFTP).
    - Mapeo fijo IP-MAC en el servidor.
  - DHCP, Dynamic Host Configuration Protocol
    - Como BOOTP pero permite la asignación de direcciones IP temporales o no asignadas a priori a una dirección MAC.

DHCP solicitud inicial

- xid: ID transacción
- ciaddr: dirección IP cliente
- yiaddr: dirección IP asignada
- serverID: dirección IP servidor

DHCPDISCOVER (src MAC = a, dst MAC = 0xffffffffffff, src IP = 0.0.0.0, dst IP = 255.255.255.255, src port = 68, dst port = 67, xid = n, ciaddr = 0.0.0.0)

DHCPOFFER (src MAC = b, dst MAC = 0xffffffffffff, src IP = c, dst IP = 255.255.255.255, src port = 67, dst port = 68, xid = n, ciaddr = 0.0.0.0, yiaddr = x, server ID = c, lease time = 3600 seconds, netmask = 255.255.255.0)

DHCPREQUEST (src MAC = a, dst MAC = 0xffffffffffff, src IP = 0.0.0.0, dst IP = 255.255.255.255, src port = 68, dst port = 67, xid = n+1, ciaddr = 0.0.0.0, yiaddr = x, server ID = c, lease time = 3600 seconds, netmask = 255.255.255.0, requested IP address = x)

DHCPACK (src MAC = b, dst MAC = 0xffffffffffff, src IP = c, dst IP = 255.255.255.255, src port = 67, dst port = 68, xid = n+1, ciaddr = 0.0.0.0, yiaddr = x, server ID = c, lease time = 3600 seconds, netmask = 255.255.255.0)

DHCP renovación

- xid: ID transacción
- ciaddr: dirección IP cliente
- yiaddr: dirección IP asignada
- serverID: dirección IP servidor

DHCPREQUEST (src MAC = a, dst MAC = b, src IP = x, dst IP = c, src port = 68, dst port = 67, xid = n, ciaddr = x, yiaddr = x, server ID = c, lease time = 3600 seconds, netmask = 255.255.255.0,)

DHCPACK (src MAC = b, dst MAC = a, src IP = c, dst IP = x, src port = 67, dst port = 68, xid = n, ciaddr = x, yiaddr = x, server ID = c, lease time = 3600 seconds, netmask = 255.255.255.0)

DHCP opciones

Table 8-1 DHCP Options

Tag	Name	Length	Meaning
0	Pad	0	None
1	Subnet Mask	4	Subnet mask value
2	Time Offset	4	Time offset in seconds from UTC
3	Router	N	N/4 router addresses
4	Time Server	N	N/4 time server addresses
5	Name Server	N	N/4 IEN-116 server addresses
6	Domain Server	N	N/4 DNS server addresses
7	Log Server	N	N/4 logging server addresses
8	Quotes Server	N	N/4 quotes server addresses
9	LPR Server	N	N/4 printer server addresses
10	Impress Server	N	N/4 Impress server addresses
11	RLP Server	N	N/4 RLP server addresses
12	Hostname	N	Hostname string
13	Boot File Size	2	Size of boot file in 512-byte chunks
14	Merit Dump File	N	Client to dump and name the file to dump it to
15	Domain Name	N	DNS domain name of the client
16	Swap Server	N	Swap server address
17	Root Path	N	Path name for root disk
18	Extension File	N	Path name for more BOOTP info
19	Forward On/Off	1	Enable/disable IP forwarding
20	SrcRte On/Off	1	Enable/disable source routing
21	Policy Filter	N	Routing policy filters
22	Max DG Assembly	2	Max datagram reassembly size
23	Default IP TTL	1	Default IP Time to Live
24	MTU Timeout	4	Path MTU aging timeout
25	MTU Plateau	N	Path MTU plateau table
26	MTU Interface	2	Interface MTU size
27	MTU Subnet	1	All subnets are local
28	Broadcast Address	4	Broadcast address
29	Mask Discovery	1	Perform mask discovery
30	Mask Supplier	1	Provide mask to others
31	Router Discovery	1	Perform router discovery
32	Router Request	4	Router solicitation address
33	Static Route	N	Static routing table
34	Trailers	1	Trailer encapsulation

Table 8-1 DHCP Options (continued)

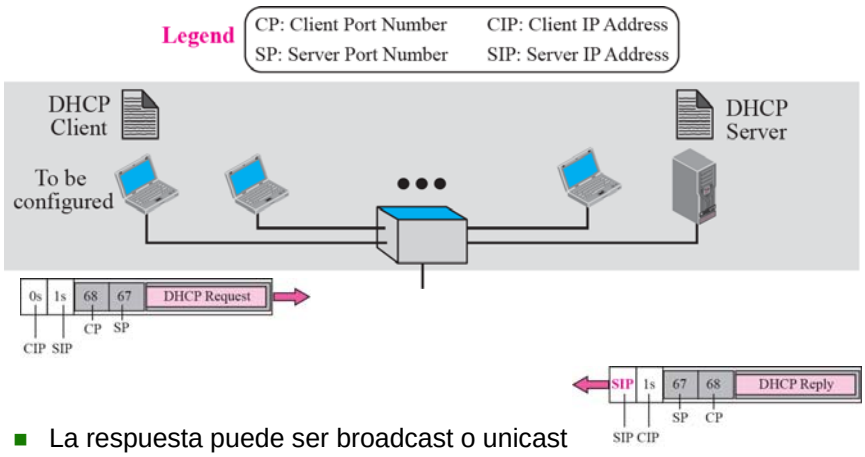
Tag	Name	Length	Meaning
35	ARP Timeout	4	ARP cache timeout
36	Ethernet	1	Ethernet encapsulation
37	Default TCP TTL	1	Default TCP Time to Live
38	Keepalive Time	4	TCP keep-alive interval
39	Keepalive Data	1	TCP keep-alive garbage
40	NIS Domain	N	NIS domain name
41	NIS Servers	N	NIS server addresses
42	NTP Servers	N	NTP server addresses
43	Vendor Specific	N	Vendor-specific information
44	NETBIOS Name Srv	N	NETBIOS name servers
45	NETBIOS Dist Srv	N	NETBIOS datagram distribution
46	NETBIOS Node Type	1	NETBIOS node type
47	NETBIOS Scope	N	NETBIOS scope
48	X Window Font	N	X Window font server
49	X Window Manager	N	X Window display manager
50	Address Request	4	Requested IP address
51	Address Time	4	IP address lease time
52	Overload	1	Overload "sname" or "file"
53	DHCP Msg Type	1	DHCP message type
54	DHCP Server Id	4	DHCP server identification
55	Parameter List	N	Parameter request list
56	DHCP Message	N	DHCP error message
57	DHCP Max Msg Size	2	DHCP maximum message size
58	Renewal Time	4	DHCP renewal time (T1)
59	Rebinding Time	4	DHCP rebinding time (T2)
60	Vendor Class ID	N	Vendor class identifier
61	Client ID	N	Client identifier
62	NetWare/IP Domain	N	NetWare/IP domain name
63	NetWare/IP Option	N	NetWare/IP sub options
64	NIS-Domain-Name	N	NIS+ v3 client domain name
65	NIS-Server-Addr	N	NIS+ v3 server addresses
66	Server-Name	N	TFTP server name
67	Bootfile-Name	N	Boot filename
68	Home-Agent-Addrs	N	Home agent addresses
69	SMTP-Server	N	Simple Mail server addresses

Table 8-1 DHCP Options (continued)

Tag	Name	Length	Meaning
70	POP3-Server	N	Post Office server addresses
71	NNTP-Server	N	Network News server addresses
72	WWW-Server	N	WWW server addresses
73	Finger-Server	N	Finger server addresses
74	IRC-Server	N	Chat server addresses
75	StreetTalk-Server	N	StreetTalk server addresses
76	STDA-Server	N	ST Directory Assistance addresses
77	User-Class	N	User class information
78	Directory Agent	N	Directory agent information
79	Service Scope	N	Service location agent scope
80	Naming Authority	N	Naming authority
81	Client FQDN	N	Fully qualified domain name
82	Agent Circuit ID	N	Agent circuit ID
83	Agent Remote ID	N	Agent remote ID
84	Agent Subnet Mask	N	Agent subnet mask
85	NDS Servers	N	Novell Directory Services
86	NDS Tree Name	N	Novell Directory Services
87	NDS Context	N	Novell Directory Services
88	IEEE 1003.1 POSIX	N	IEEE 1003.1 POSIX time zone
89	FQDN	N	Fully qualified domain name
90	Authentication	N	Authentication
91	Vines TCP/IP	N	Vines TCP/IP server option
92	Server Selection	N	Server selection option
93	Client System	N	Client system architecture
94	Client NDI	N	Client network device interface
95	LDAP	N	Lightweight Directory Access Protocol
96	IPv6 Transitions	N	IPv6 transitions
97	UUID/GUID	N	UUID/GUID-based Client Identifier
98	User-Auth	N	Open Group's user authentication

"N" in length column represents a variable number.

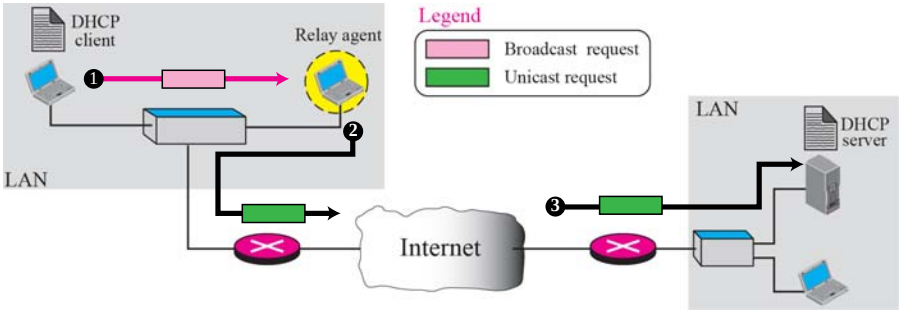
DHCP servidor en la misma red



- La respuesta puede ser broadcast o unicast (se conoce la MAC del cliente)

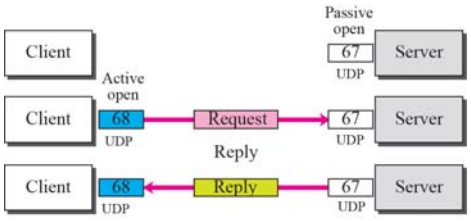
DHCP servidor en distinta red

- El relay agent puede ser una máquina, un switch o un router de la red.
  - Reenvía la solicitud a la IP del servidor DHCP que conoce a priori
  - Un campo de la cabecera DHCP contiene la IP del relay agent
  - La respuesta vuelve al relay que lo vuelca unicast/broadcast a la red



DHCP puerto fijo de cliente

- Como las respuestas pueden ser broadcast, al elegir un puerto efímero para el cliente DHCP podría colisionar con otro cliente (de otro servicio) de otra máquina en el mismo puerto que recibiría los mismos paquetes.

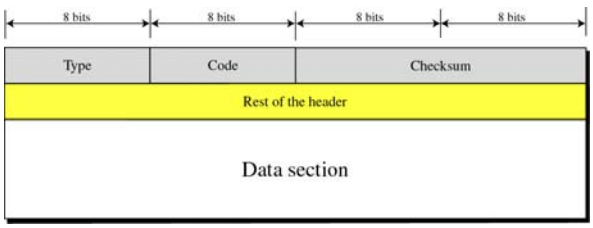


7 ICMP

- Internet Control Message Protocol.
- ICMP compensa las deficiencias de IP en cuanto a:
  - Falta de control de errores.
  - Falta de mecanismos de diagnóstico.
- ICMP es un protocolo que hace funciones de nivel de red pero se encapsula dentro de datagramas IP (Protocol=1 de la cabecera IP).
- Tipos de mensajes ICMP:
  - De error: informa sobre un problema en un router o en una máquina.
  - De petición: útiles para conseguir información específica de un router o una máquina. Se producen por pares petición-respuesta.

7.1 Paquete ICMP

- Type (8bits): tipo de mensaje ICMP.
- Code (8bits): código propio a cada tipo de mensaje ICMP.
- Checksum (16bits): se calcula sobre la cabecera + datos ICMP aplicando el mismo algoritmo de checksum que la cabecera IP.
- Rest of the header (32 bits): campos de cabecera propios para cada tipo de mensaje.
- Data section: tamaño variables con datos propios según tipo.



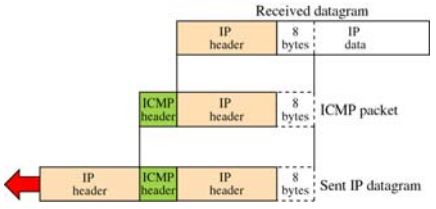
7.2 Tipos de mensajes ICMP

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

7.2.1 Mensajes ICMP de error

- Reporta errores (no los corrige, será labor ésta de niveles superiores).
- Siempre se envían al emisor original del paquete que ocasionó el error, porque se tiene su dirección IP como IP origen del paquete original.
- Todos los mensajes de error ICMP incluyen en el campo *data section* la cabecera IP del datagrama original seguido de los 8 primeros bytes de datos del datagrama original.

Los 8 bytes se eligen porque para TCP/UDP incluyen la información de puertos y número de secuencia (sólo TCP), para que así el origen pueda informar a niveles superiores.

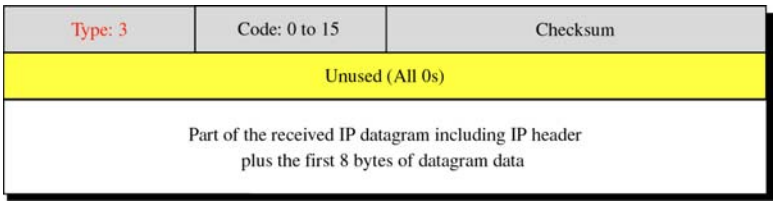


Mensajes ICMP de error

- Para evitar tormentas ICMP de error, nunca se generan en respuesta a:
  - Otro ICMP de error.
  - Un fragmento IP que no sea el primero.
  - Un datagrama destinado a una dirección IP de broadcast o multicast.
  - Un datagrama cuya dirección IP origen no haga referencia a una única máquina: loopback, broadcast, multicast y 0.0.0.0.
- En estos casos el paquete deberá ser descartado silenciosamente y el evento debería quedar registrado (log).

ICMP error: Destino inalcanzable

- Cuando un router no puede encaminar un datagrama o una máquina destino no puede entregarlo a niveles superiores, el datagrama se tira y el router o máquina manda un mensaje de vuelta de este tipo.
- Type=3
- Code=0...16 (⇒)
- Rest of Header=0 (sin uso)



ICMP error: Destino inalcanzable

Code	Definition
0	Net Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragmentation Needed and Don't Fragment was Set
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Source Host Isolated
9	Communication with Destination Network is Administratively Prohibited
10	Communication with Destination Host is Administratively Prohibited
11	Destination Network Unreachable for Type of Service
12	Destination Host Unreachable for Type of Service
13	Communication Administratively Prohibited
14	Host Precedence Violation
15	Precedence Cutoff in Effect

ICMP error: Destino inalcanzable

- 0: Net Unreachable
  - Lo manda un router cuando conoce la red destino pero esa red o un enlace intermedio no está activo en ese momento.
- 1: Host Unreachable
  - Lo manda un router cuando conoce la red destino pero la máquina no está activa.
- 2: Protocol Unreachable
  - Lo manda una máquina (o el router si es el destinatario final) indicando que el protocolo indicado en el paquete no se puede procesar (no soportado o no activo).
- 3: Port Unreachable
  - Lo manda una máquina (o el router si es el destinatario final) indicando que el proceso o aplicación al que se refiere el paquete no se puede alcanzar en ese destino.

ICMP error: Destino inalcanzable

- 4: Fragmentation Needed and Don't Fragment was Set
  - Lo manda un router para indicar que no ha podido enviar el paquete porque el bit Don't Fragment de la cabecera IP está activo y era necesario fragmentar el paquete para poderse reenviar.
- 5: Source Route Failed
  - Lo manda un router para indicar que no puede utilizar el encaminamiento fuente estricto o débil de la cabecera IP.
- 6: Destination Network Unknown
  - Obsoleto. Se utiliza el de código 7 en su lugar.
- 7: Destination Host Unknown
  - Lo manda un router para indicar que no conoce la red destino ni cómo acceder a ella.
- 8: Source Host Isolated
  - Obsoleto. Anteriormente se utilizaba para indicar que la máquina destino se encontraba aislada y no era posible reenviarle paquetes.

ICMP error: Destino inalcanzable

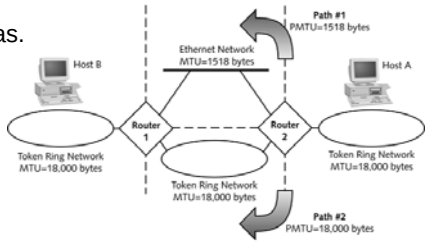
- 9: Communication with Destination Network is Administratively Prohibited
  - Lo manda un router para indicar que fue configurado para bloquear el acceso a la red destino deseada.
- 10: Communication with Destination Host is Administratively Prohibited
  - Lo manda un router para indicar que fue configurado para bloquear el acceso a la máquina destino deseada.
- 11: Destination Network Unreachable for Type of Service
  - Lo manda un router para indicar que no dispone del Tipo de Servicio declarado en la cabecera IP del paquete para acceder a esa red.
- 12: Destination Host Unreachable for Type of Service
  - Lo manda un router para indicar que no dispone del Tipo de Servicio declarado en la cabecera IP del paquete para acceder a esa máquina.

ICMP error: Destino inalcanzable

- 13: Communication Administratively Prohibited [RFC1812]
  - Lo manda un router para indicar al origen que no puede reenviar el paquete porque lo prohiben las reglas de filtrado de paquetes.
- 14: Host Precedence Violation [RFC1812]
  - Lo manda un router para indicar que no puede reenviar el paquete porque el campo prioridad de la cabecera IP no está permitido para ese origen, destino, protocolo o puerto.
- 15: Precedence cutoff in effect [RFC1812]
  - Lo manda un router para indicar que el paquete no tiene el mínimo valor de prioridad de la cabecera IP requerido por el administrador para obtener servicio (situaciones transitorias de congestión).

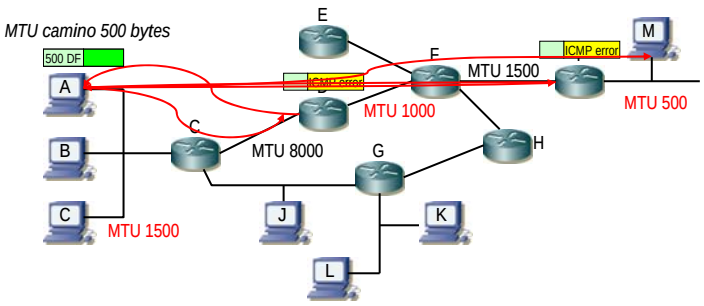
ICMP error: Destino inalcanzable

- Ejemplo de aplicación: ***Descubrimiento de la MTU del camino***
  - Se mandan los paquetes con el bit Don't Fragment de la cabecera IP activo, empezando con tamaño marcado por la MTU de la red origen.
  - Si en algún salto intermedio la MTU es más pequeña, se retornará un paquete ICMP de error de destino inalcanzable de código 4.
  - El origen podrá entonces reducir el tamaño del paquete (teniendo en cuenta los valores de MTUs típicos) hasta encontrar un tamaño de paquete que no reciba el ICMP de error de destino inalcanzable de código 4.
  - Problema: variabilidad de rutas.



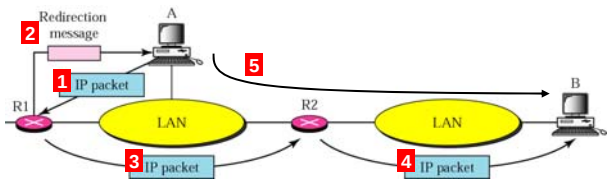
ICMP error: Destino inalcanzable

- Ejemplo de aplicación: ***Descubrimiento de la MTU del camino***



ICMP error: Redirección

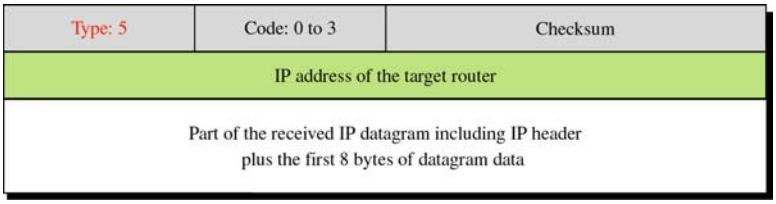
- Normalmente una máquina sólo tiene configurado un router que es el de por defecto. Si la máquina manda un paquete a través de ese router pero el camino es erróneo para alcanzar el destino 1, ese router por defecto mandará un ICMP de redirección al origen informándole de la IP del router de salida correcto 2 .
- Ese primer paquete se reenvía correctamente al destino aunque se mande el ICMP de redirección 3 4: el origen estará enterado para la siguiente vez.
- Para siguientes paquetes, el origen los enviará a través del nuevo router de salida 5.



A quiere enviar a B y tiene como router por defecto R1 que no es el correcto para ese destino.

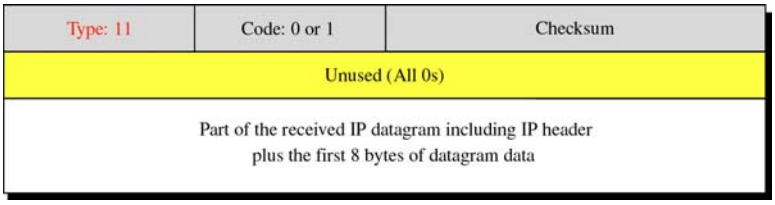
ICMP error: Redirección

- Type=5
- Code:
  - 0: redirección a ruta específica para la red.
  - 1: redirección a ruta específica para la máquina.
  - 3: redirección a ruta específica para la red y el TOS.
  - 4: redirección a ruta específica para la máquina y el TOS.
- Rest of Header: dirección IP del router al que se redirige.



ICMP error: Tiempo excedido

- Type=11
- Code:
  - 0: el TTL del datagrama ha llegado a 0 y se ha descartado.
  - 1: no han llegado al destino todos los fragmentos en el límite de tiempo y se han descartado todos los que había. Debe haber recibido el 1er fragmento para tener los datos que adjunta el ICMP (cabecera IP + 8bytes de datos).
- Rest of Header: 0 (sin uso)
- La aplicación *traceroute* hace uso de este mensaje (code 0).

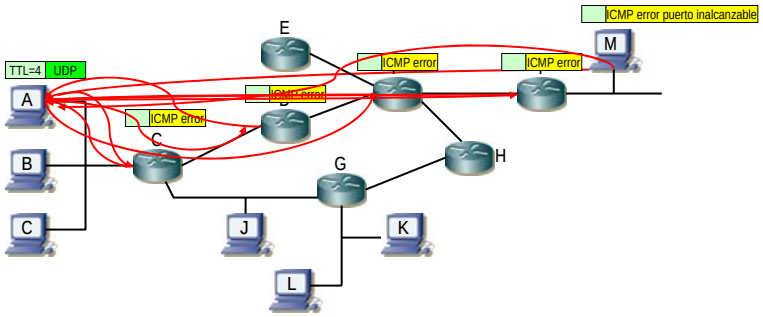


ICMP error: Tiempo excedido

- Ejemplo de aplicación: ***Traceroute***, aplicación que permite determinar una posible ruta entre dos máquinas.
  - La ruta se mide salto a salto con series de paquetes cuyo campo TTL de la cabecera IP va creciendo 1,2,3,...
  - 3 intentos por cada valor de TTL.
  - El paquete es UDP con un puerto destino aleatorio por encima del 30000.
    - Windows (tracert) utiliza ICMP echo request en lugar de UDP.
  - Los nodos correspondientes a los saltos intermedios responderán con un ICMP de error de "tiempo excedido" al agotarse el TTL.
  - El nodo destino responderá con un ICMP de error de "puerto inalcanzable".
- A tener en cuenta:
  - Las rutas pueden variar.
  - Las rutas pueden no ser simétricas.

ICMP error: Tiempo excedido

- Ejemplo de aplicación: ***Traceroute***



A ⇒ C ⇒ D ⇒ F ⇒ I ⇒ M

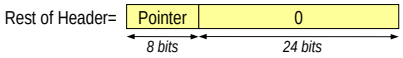
ICMP error: Tiempo excedido

- Ejemplo de aplicación: ***Traceroute*** otilio.tlm.unavarra.es → www.berkeley.edu

```
1  130.206.160.1 (130.206.160.1)  0.545 ms  0.245 ms  0.237 ms
2  s158m25.unavarra.es (130.206.158.25)  0.831 ms  0.647 ms  0.647 ms
3  unavarra-router.red.unavarra.es (130.206.158.1)  1.586 ms  1.726 ms  1.804 ms
4  FE0-1-2.EB-Pamplona0.red.rediris.es (130.206.209.13)  2.367 ms  1.369 ms  1.392 ms
5  NAV.SO2-3-0.EB-Bilbao0.red.rediris.es (130.206.240.61)  4.216 ms  4.675 ms  4.830 ms
6  PAV.SO2-0-0.EB-IRIS2.red.rediris.es (130.206.240.29)  16.489 ms  16.238 ms  20.834 ms
7  SO0-0-0.EB-IRIS4.red.rediris.es (130.206.240.2)  17.708 ms  16.268 ms  16.231 ms
8  * rediris.es1.es.geant.net (62.40.103.61)  16.533 ms  16.642 ms
9  es.fr1.fr.geant.net (62.40.96.10)  35.878 ms  36.273 ms  35.803 ms
10 fr.uk1.uk.geant.net (62.40.96.90)  42.674 ms  42.672 ms *
11 uk.ny1.ny.geant.net (62.40.96.169)  111.568 ms  111.606 ms  111.868 ms
12 198.32.11.61 (198.32.11.61)  111.393 ms  111.345 ms  111.424 ms
13 chinng-nycmng.abilene.ucaid.edu (198.32.8.82)  141.649 ms  141.874 ms  142.034 ms
14 iplsng-chinng.abilene.ucaid.edu (198.32.8.77)  145.938 ms  145.367 ms  161.506 ms
15 kscyng-iplsng.abilene.ucaid.edu (198.32.8.81)  165.320 ms  160.799 ms  154.654 ms
16 dnvrng-kscyng.abilene.ucaid.edu (198.32.8.13)  165.271 ms  165.220 ms  165.260 ms
17 snvang-dnvrng.abilene.ucaid.edu (198.32.8.1)  190.935 ms  190.025 ms  190.406 ms
18 losang-snvang.abilene.ucaid.edu (198.32.8.94)  207.752 ms  197.331 ms  197.689 ms
19 hpr-lax-gsr1--abilene-LA-10ge.cenic.net (137.164.25.2)  197.731 ms  197.567 ms  197.677 ms
20 sac-hpr--lax-hpr-10ge.cenic.net (137.164.25.11)  207.149 ms  207.561 ms  206.863 ms
21 * oak-hpr--sac-hpr-10ge.cenic.net (137.164.25.16)  208.831 ms  208.868 ms
22 hpr-ucb-ge--oak-hpr.cenic.net (137.164.27.130)  208.802 ms  208.746 ms  209.140 ms
23 vlan189.inr-201-eva.Berkeley.EDU (128.32.0.37)  208.850 ms  208.723 ms  208.912 ms
24 g5-1.inr-210-srb.Berkeley.EDU (128.32.255.65)  208.728 ms  208.838 ms  208.736 ms
25 arachne.Berkeley.EDU (169.229.131.109)  208.906 ms  209.256 ms  209.036 ms
```

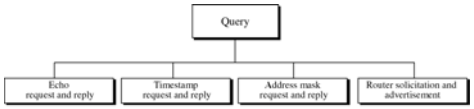

ICMP error: Problema de parámetros

- Type=12
- Code:
  - 0: hay un error o ambiguedad en un campo de la cabecera IP. El puntero del campo Rest of Header apunta al byte con el problema.
  - 1: falta una parte requerida de una opción de la cabecera IP.
- Rest of Header: Pointer (8bits) + 24 bits no usados.

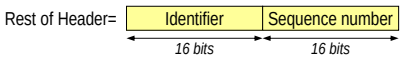


Type: 12	Code: 0 or 1	Checksum
Pointer	Unused (All 0s)	
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

7.2.2 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:

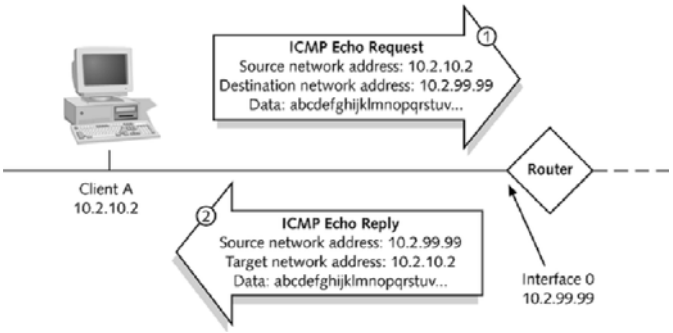


  - Identifier: normalmente el ID del proceso que lo genera.
  - Sequence number: numeración secuencial de los paquetes.

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

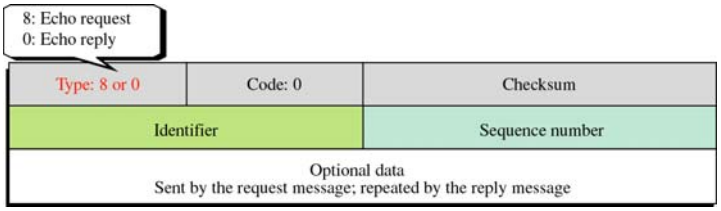
ICMP petición/respuesta: ECHO

- 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.



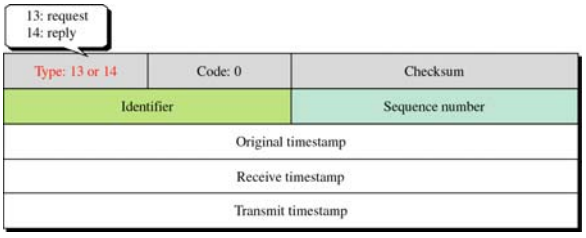
ICMP petición/respuesta: ECHO

- 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.



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.

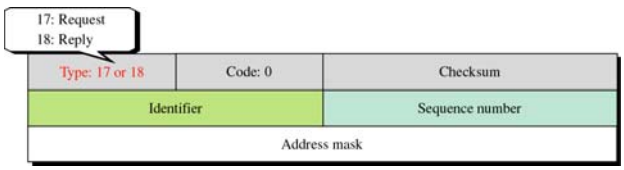


ICMP petición/respuesta: Timestamp

- 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.

ICMP petición/respuesta: Máscara

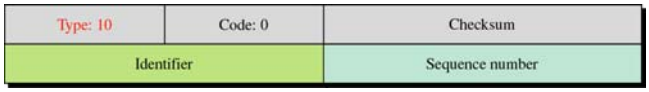
- Si una máquina conoce su dirección IP pero no su máscara de red, se la puede pedir con este ICMP:
  - al router que conozca.
  - o a una dirección de broadcast si desconoce el router.
  - Type:
    - 17: request
    - 18: reply
  - Code=0
  - Data section:
    - 0 en el request.
    - valor de la máscara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



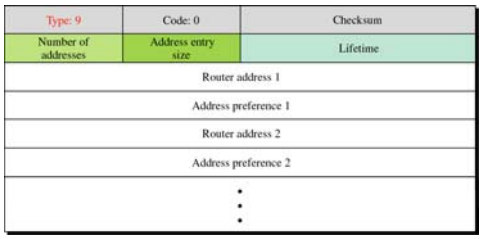
ICMP petición/respuesta: router

- 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.

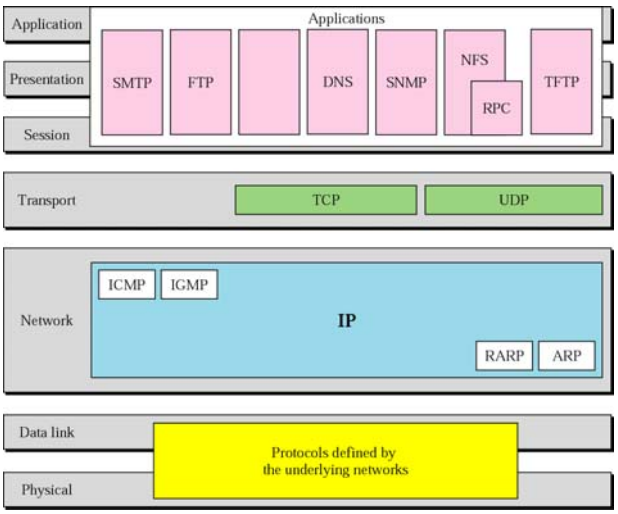


ICMP petición/respuesta: router



- 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.

8 IGMP



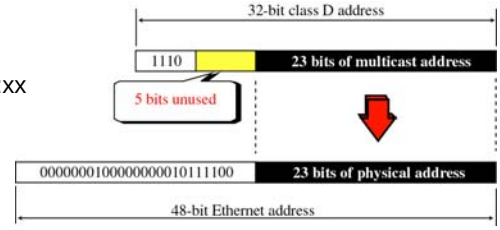
IGMP

- 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.

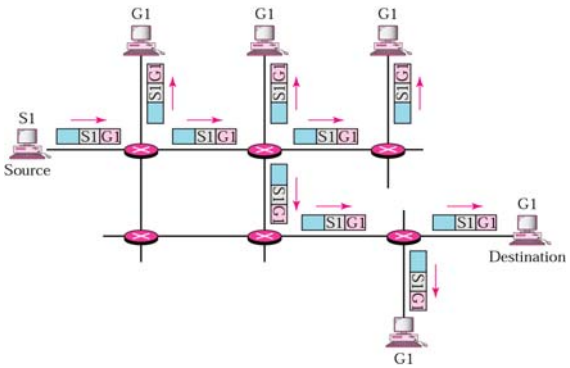
IGMP

- 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

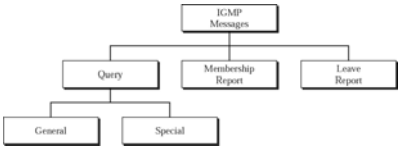


IGMP, multicast

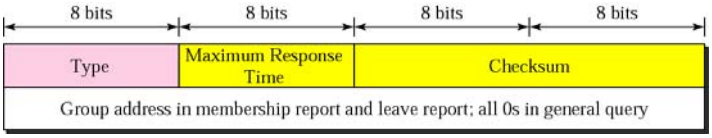


- Cada máquina informa a través de IGMP a su router de en qué grupo multicast está interesada.
- Los routers interaccionan entre sí para recibir los grupos multicast en caso de que en su red haya alguna máquina interesada.
- Protocolos de enrutamiento multicast entre routers:
  - DVMRP (Distance Vector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

8.1 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.



8.2 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.

8.3 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.

8.4 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.

9 Evolucionando IP

- Las direcciones IP de máquinas se encuentran asociadas a las redes en las que se encuentran físicamente conectadas. Según el esquema de direccionamiento vendrá dado por el NetID:
  - Classful.
  - Classless (máscaras).
- Supone que las máquinas tienen que estar fijas en la red de la cual reciben dirección IP.
- ¿Qué ocurre si queremos que la máquina cambie de una red a otra?
  - Escenarios de baja movilidad
    - Servicio de acceso *hot-spots*.
    - Cambio esporádico de red.
  - Escenarios de alta movilidad
    - Máquina en movimiento: PDA o portátil con soporte inalámbrico.
    - Servicio de acceso *info-stations*.

Evolucionando IP

- IP es un protocolo con muchos parches añadidos
  - Pequeñas modificaciones en sucesivas RFCs.
  - Campos de opciones.
  - Seguridad en un protocolo encapsulado: IPsec (cap. 6).
  - Movilidad en otro protocolo asociado: Mobile IP.
  - Deficiencias:
    - Información de fragmentación incluso en paquetes no fragmentados.
    - Cabecera de tamaño variable.

- ¿Qué tal si se redefine IP con todo lo aprendido en estos años de experiencia? IPv6

9.1 Mobile IP

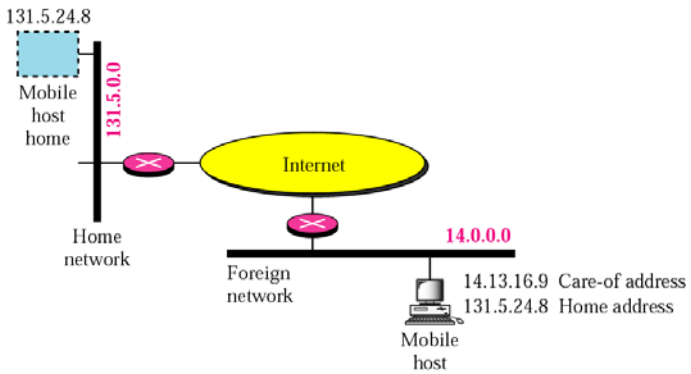
RFC2002

- El direccionamiento IP está diseñado para trabajar con máquinas fijas porque parte de la dirección define la red IP física en la que la máquina se encuentra conectada.
- Si se cambia de red ocasionalmente, sería suficiente con cambiar la dirección IP por una perteneciente a la nueva red (obtenida por DHCP, Dynamic Host Configuration Protocol). Inconvenientes:
  - Se pierden las conexiones abiertas: se interrumpen las comunicaciones.
  - La entrada de DNS (Domain Name System, mapeo IP-nombre) deberá cambiarse dinámicamente.
- Solución para soportar movilidad sin perder conexiones abiertas: Mobile IP.

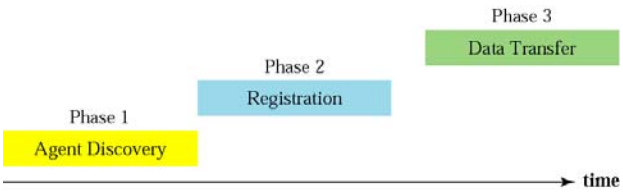
Mobile IP

- Nomenclatura del estándar:
  - Red local (Home network): red original donde se encontraba antes el móvil.
  - Red foránea (Foreign network): red nueva a la que va a parar el móvil.
  - Dirección local (Home address): dirección IP original del móvil en su red local.
  - Dirección auxiliar (Care-of address): dirección IP del móvil en la nueva red.
  - Agente local (Home agent): pasarela que se comporta como el móvil en su red original.
  - Agente foráneo (Foreign agent): pasarela que pasa paquetes al móvil en la nueva red procedentes del agente local.

Mobile IP



Mobile IP, fases

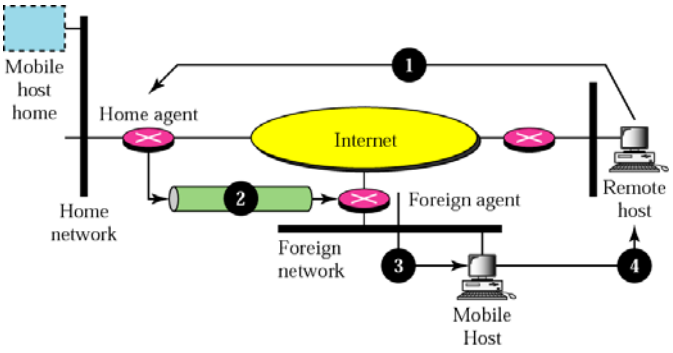


- 1 Descubrimiento de los agentes
  - Antes de que el móvil se mueva debe conocer la IP del agente local.
  - Al moverse a la nueva red descubre la IP del agente foráneo por anuncios de éste último o bajo petición del móvil.

Mobile IP, fases

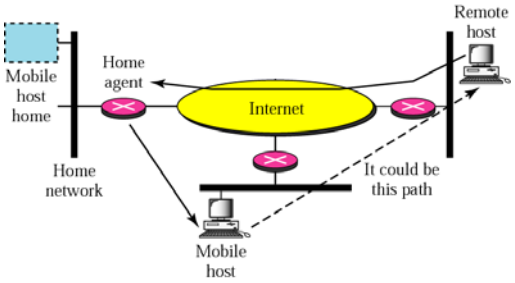
- 2 Registro
  - El móvil se registra en la nueva red con el agente foráneo y le da la IP de su agente local.
  - El agente foráneo registra al móvil en el agente local como perteneciente a la nueva red foránea.
  - El móvil es el encargado de renovar o cancelar esta suscripción.
- 3 Transferencia de datos
  - Si una máquina remota quiere transmitir datos al nodo móvil, mandará los paquetes a la dirección local del mismo. Allí, el agente local intercepta estos paquetes y los manda al agente foráneo que conoce gracias al proceso de registro.
  - El agente foráneo consulta una tabla interna con el mapeo dirección local - dirección auxiliar, y manda el paquete a la dirección auxiliar que es la IP del móvil en la nueva red.

Mobile IP, transferencia de datos



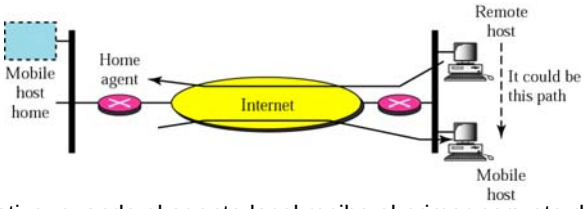
Mobile IP, fases

- 4 Respuesta
  - Al contestar el móvil a la máquina remota, coloca como IP origen la dirección local y como IP destino la dirección de la máquina remota.



Mobile IP

- El movimiento es totalmente transparente para el resto de máquinas remotas: siempre envían paquetes a la dirección local como si el móvil no se hubiera movido de su red original.
- Ineficiencia del sistema: doble cruce



  - Alternativa: cuando el agente local recibe el primer paquete de una máquina remota, le puede informar de la dirección auxiliar del móvil para que le envíe directamente los siguientes paquetes.
    - Si el móvil cambia de red, el agente local podrá actualizar la dirección auxiliar a la máquina remota.
    - Problema: imposibilidad en TCP/IP de mantener conexiones cambiando las direcciones IP.

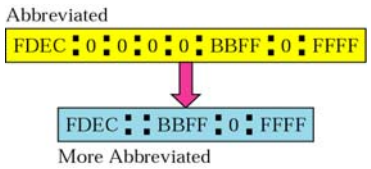
9.2 IPv6

RFC2460, RFC3513

- IPv6 nace para cubrir las principales deficiencias de IPv4:
  - Falta de espacio de direccionamiento y organización correcta del mismo.
  - Estrategias de provisión de calidad de servicio: TOS/DS de IPv4 apenas utilizado.
  - Encriptación y autentificación nativo: IPv4 necesita de un protocolo añadido como IPsec.
  - Muchas modificaciones dispersas en RFCs. Protocolo demasiado "parcheado".
- IPv6 = IPv4 + ~25 años de experiencia.
- IPv6 nace de las propuestas de IP next generation (IPng) con las siguientes características.

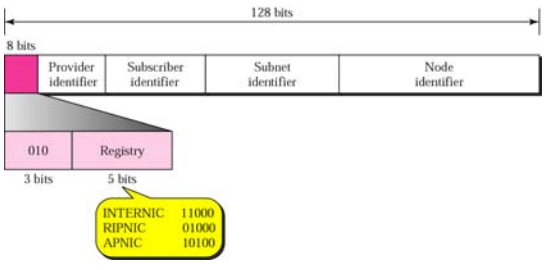
9.2.1 IPv6 características

- 1. Mayor espacio de direcciones: 128 bits (16 bytes)
  - Representadas en hexadecimal de 2 en 2 bytes separados por ":"
    - 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).



IPv6 características

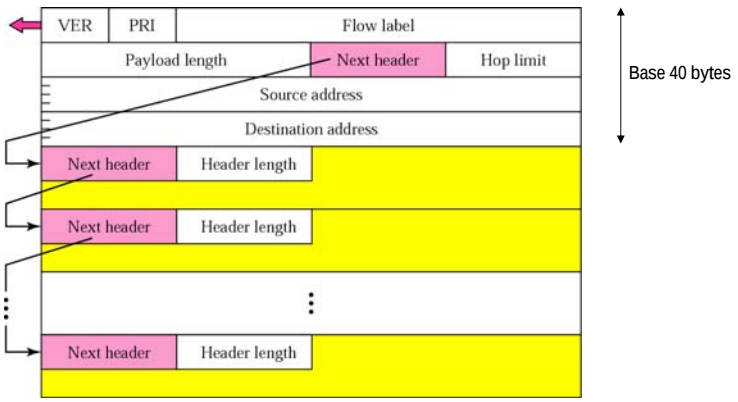
- Formato de las direcciones:
  - Primer byte identifica distintos tipos de direcciones.
    - 010xxxxx : direcciones unicast por proveedor.
    - 11111111: direcciones multicast.
    - 00000000: loopback.
  - Direccíones unicast por proveedor
    - Node identifier: recomendado tamaño de 48 bits para que pueda coincidir con la dirección MAC del interfaz (supuesto Ethernet).



IPv6 características

- 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. Posibilidad de definir extensiones nuevas con facilidad de cara a futuras mejoras.
- 4. Mecanismo de reserva de recursos mediante etiquetas de flujo en la cabecera.
- 5. Opciones de autentificación, integridad de datos y privacidad.
- Otras características:
  - Modelo de enrutamiento jerárquico desde el principio.
  - Soluciones de autoconfiguración (plug-and-play).
  - Soluciones para movilidad.

9.2.2 Cabecera IPv6

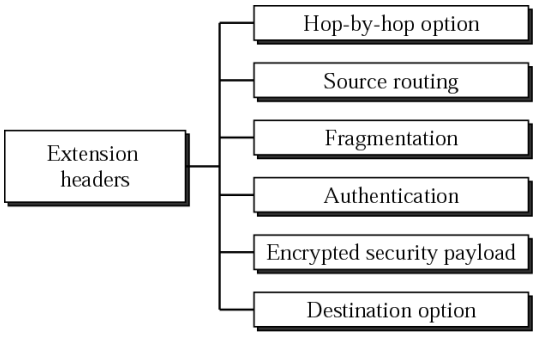


Campos cabecera IPv6

- 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.

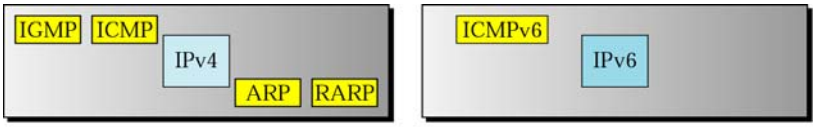
Campos cabecera IPv6

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



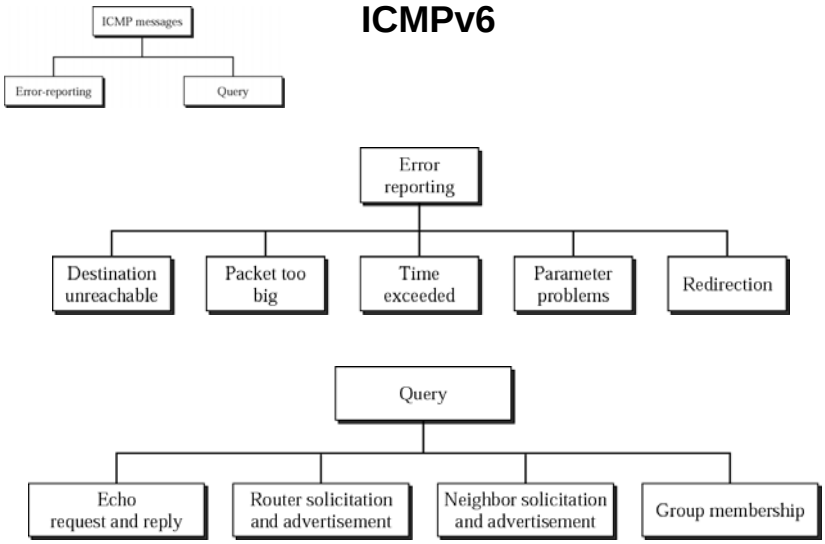
9.2.3 IPv6 protocolos de soporte

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

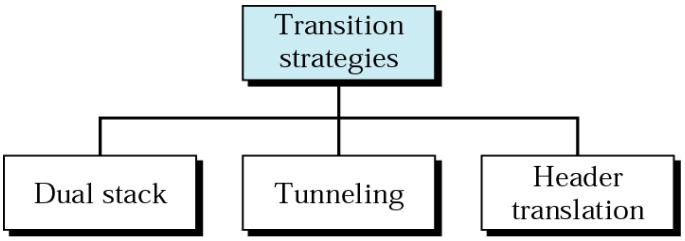


Network layer in version 4 | Network layer in version 6

ICMPv6

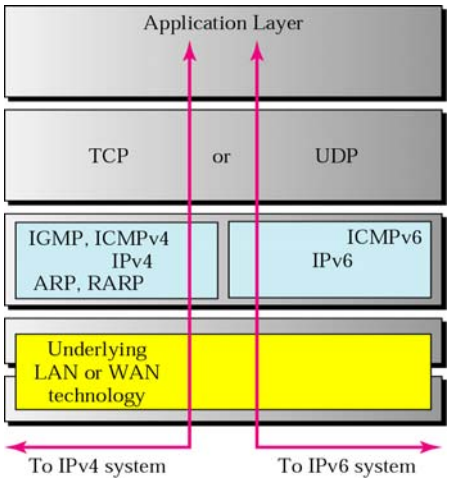


9.2.4 Transición a IPv6



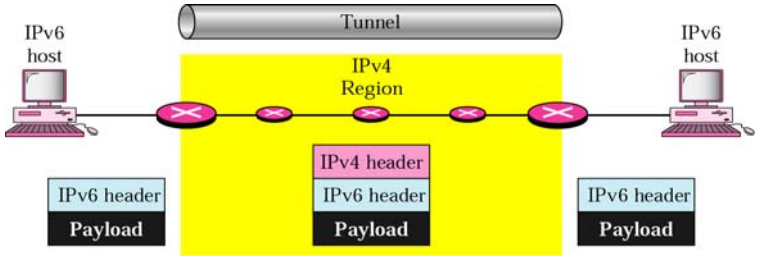
Dual Stack

- Soporte de ambos niveles de red IPv4 y IPv6 en todas las máquinas y routers.



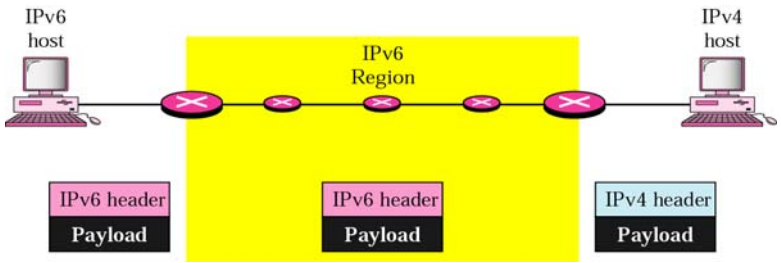
Túneles

- Túneles de IPv6 sobre IPv4 para regiones IPv4 y al contrario.



Traslación de cabeceras

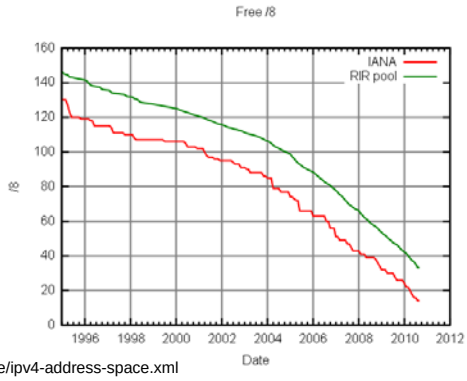
- La cabecera IPv6 es convertida por los routers extremo a IPv4, haciendo uso de las opciones de IPv4 para la información extra.



9.2.5 Grado de implantación de IPv6

- Retraso en la implantación de IPv6 debido al uso de CIDR y NAT
- Posible potenciación por la masiva implantación de dispositivos móviles con conectividad 3G.
- Para cuando agotamiento direcciones IPv4

• Predicción IANA: 05-Jun-2011
• Predicción RIR: 05-Feb-2012 **

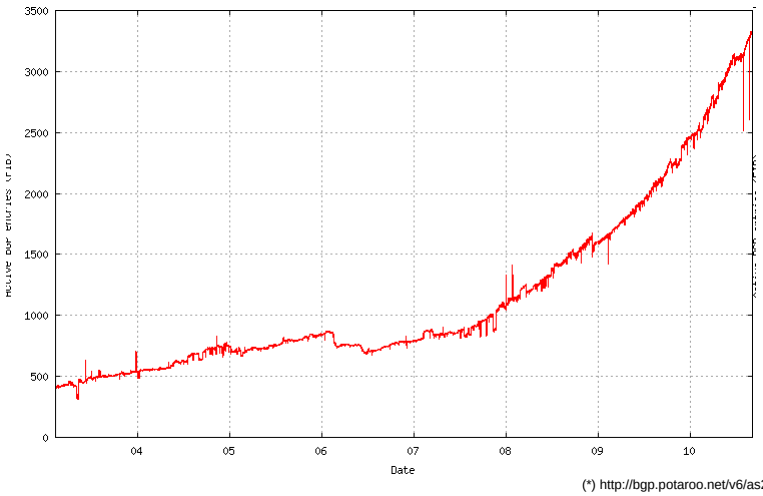


RIR: Regional Internet Registries

(*) http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
(**) http://www.potaroo.net/tools/ipv4/index.html

Grado de implantación de IPv6

Active IPv6 BGP entries



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

Bibliografía

- [Forouzan]
  - Capítulo 7, secciones 7.1, 7.3
  - Capítulo 8, sección 8.3
  - Capítulo 9
  - Capítulo 10
  - Capítulo 27
  - Capítulo 31
- [Stevens]
  - Capítulo 4
  - Capítulo 5
  - Capítulo 6
  - Capítulo 7
  - Capítulo 8
  - Capítulo 13
  - Capítulo 16