***Unidad 9. Protocolos de capa de Internet.***

Unidad 9. Protocolos de capa de Internet.

1 - Protocolo ARP. Resolución de dirección IP a MAC.

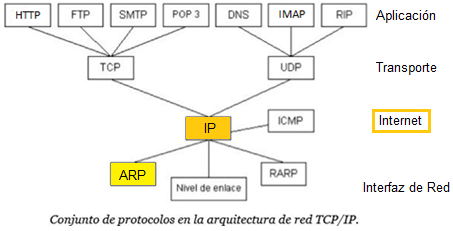
2 - Protocolo IPv4. Protocolo de Internet versión 4.

3 - Proceso de Encapsulamiento.

4 - MTU. Tamaño de datagrama. Fragmentación.

5 - Fragmentación y Reensamblado de fragmentos.

6 - Protocolo IPv6. Protocolo de Internet versión 6.



***Tema 1: Protocolo ARP, (Protocolo de Resolución de Direcciones).***

“ARP” son las siglas en inglés de Address Resolution Protocol.

ARP es un protocolo que trabaja en el límite entre la Capa de Interfaz de Red y la Capa de Internet de la familia de protocolos “TCP/IP”, y es responsable de encontrar la Dirección Física, (MAC Address), que corresponde a una determinada dirección IP.

Para ello se envía una trama de solicitud, (ARP request), a la dirección de difusión de la red, (MAC: FF.FF.FF.FF.FF.FF), que contiene la dirección IP por la que se consulta, y la estación a la cual corresponde esa dirección IP devuelve una trama de respuesta, (ARP reply), en la cual consta su Dirección de Física.

Cada estación mantiene en su memoria Caché una tabla, con las direcciones descubiertas para así agilizar el envío de paquetes. Las entradas de esa tabla se van perdiendo por envejecimiento. Es decir, después de cierto tiempo durante el cual no se ha utilizado una entrada, ésta de borra.

Para observar la Tabla Arp almacenada en la memoria Caché, se ejecuta el comando **C:> arp -a** , en una sesión Dos, (comando: cmd).

El protocolo ARP entonces, se encarga de resolver o traducir direcciones IP a direcciones Físicas, y se utiliza en los siguientes casos:

1. Si dos hosts están en la misma red, y uno quiere enviar un paquete a otro.
2. Si dos hosts están en redes diferentes y usan un Router intermedio.
3. Cuando un Router debe enviar un paquete a un host a través de otro Router.
4. Cuando un Router debe enviar un paquete a un host de la misma Red.

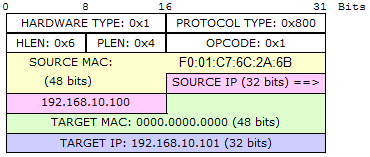
Veamos el caso 2, en el cual deben intervenir uno o más Routers.

Si la estación “A” debe enviar un paquete de información a una estación “B”, que no se encuentra en la misma red, el paquete deberá salir de la red original. Entonces la estación “A” envía la trama a la dirección física del Router, obtenida a partir de un mensaje ARP.

Una vez en el Router, éste consultará su tabla de enrutamiento obteniendo el próximo Router, (salto), para llegar a destino. Esto se repite en todos los Routers, hasta llegar al último, que es el que comparte el medio con la estación destino, “B”. Éste Router mediante una trama de solicitud ARP request, consultará la dirección física de “B”, utilizando la Dirección IP de “B”.

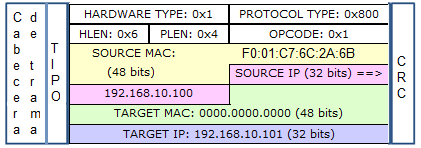
De esta forma la trama que salió desde la estación “A”, llega finalmente a la estación “B” que se encuentra en una red distinta a la de la estación “A”.

***Estructura del mensaje ARP:*** está constituida por los siguientes campos:



* El campo **Hardware Type** indica qué Tipo de Dirección de Hardware, interviene en el mensaje. Esto es debido a que el protocolo ARP, puede resolver o traducir cualquier tipo de Dirección de Protocolo, (Dirección IP), a cualquier tipo de Dirección de Hardware, (Dirección Física). En este caso del ejemplo está configurado con el valor en hexadecimal 0x1, esto confirma que la Dirección Física responde a la norma Ethernet.
* El campo **Protocol Type** indica qué Tipo de Dirección de Protocolo, interviene en el mensaje. En este caso del ejemplo está configurado con el valor en hexadecimal 0x800, lo que confirma que la Dirección de Protocolo corresponde a una dirección IP.
* El campo **Hlen,** hace referencia al largo en bytes de la Dirección Física, que en la norma Ethernet es de 6 bytes, por eso contiene el valor hexadecimal 0x6.
* El campo **Plen,** hace referencia al largo en bytes de la Dirección de Protocolo, que en la dirección IP es de 4 bytes, por eso contiene el valor hexadecimal 0x4.
* El campo **Opcode,** indica que tipo de mensaje se está enviando. Si es una solicitud ARP request se fija el valor 0x1, y es una respuesta ARP reply, es 0x2.
* El siguiente es el campo **Source Mac,** indicando la dirección física, (Mac), origen. Este campo por supuesto tiene una extensión de 6 bytes, 48 bits.
* Luego sigue el campo **Source IP,** indicando la dirección de protocolo, (dirección IP), origen. Este campo tiene una extensión de 4 bytes, 32 bits.
* Sigue el campo **Target Mac,** que indica la dirección Física, (Mac), destino, que en un mensaje de solicitud es ignorado, es lo que se consulta, por eso en ese caso, se lo completa con todos ceros.
* Por último se encuentra el campo **Target IP**, que corresponde a la dirección de protocolo, (dirección IP), destino.

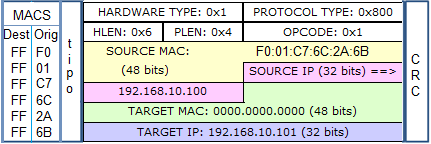
El mensaje ARP, es transmitido encapsulado dentro de una trama Ethernet.

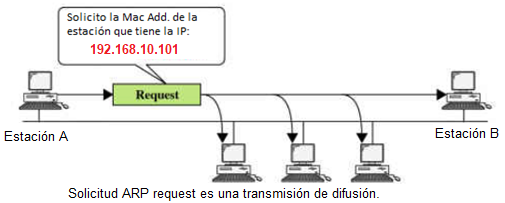


***Ejemplo:***

La estación A, solicita la dirección Mac de la estación que tenga la dirección IP: 192.168.10.101. Para ello envía una trama de difusión a la red. En la cabecera de la trama Ethernet, coloca como Mac de Destino la dirección “FF: FF: FF: FF: FF: FF”, que es la dirección de Difusión de la capa de Interfaz de Red, por lo cual todas las estaciones de la red tienen que recibir esa trama.

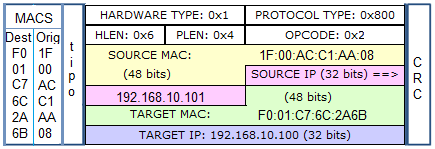
También en el campo Opcode del mensaje ARP, coloca el valor hexadecimal 0x1, indicando que es una solicitud ARP request. En los campos Source Mac y Source IP, coloca sus propias direcciones Mac e IP respectivamente. En el campo Target Mac, coloca todos ceros, ya que ésta es la dirección desconocida que está solicitando. Por último en el campo Target IP coloca la dirección IP de la estación de la cual, necesita conocer su dirección Mac.

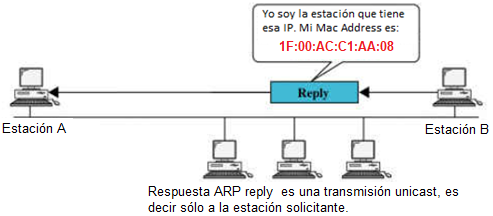




La estación B recibe la solicitud ARP request, y como corresponde a ella la dirección IP solicitada, devuelve una respuesta ARP reply directamente a la estación que la solicitó, ya que recibe su identificación en el mensaje de solicitud.

Modifica el campo Opcode, colocando el valor hexadecimal 0x2, indicando que se trata de una respuesta ARP reply, y completa los campos Source Mac y Source IP, con sus propias direcciones Mac e IP. Quedando resuelta la Dirección IP a la Dirección Mac correspondiente de la estación B.

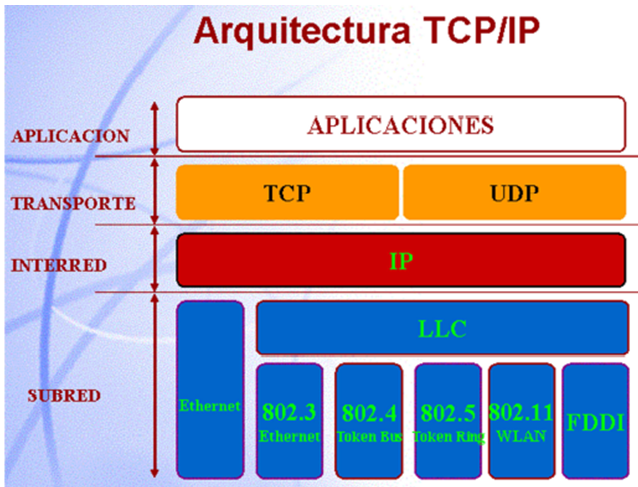




Para

***Tema 2: Protocolo IP, (Protocolo de Internet). Datagrama IP.***

IP es el protocolo más famoso de Internet. Se trata de un protocolo que opera en la capa de Internet, (nivel 2, según la arquitectura TCP/IP). Su labor principal consiste en transportar la información desde la estación Origen de la comunicación hasta el destinatario, a través de la Red de comunicaciones. El protocolo IP se utiliza para mover los datagramas, (nombre que toman los paquetes IP), desde el origen hasta el destino, pasando por un entramado complejo de Redes y Routers.



Las funciones principales que proporciona el protocolo IP, para acometer este objetivo son:

1. ***Direccionamiento.*** Mediante esta función, el protocolo permite identificar de forma única a cada uno de los equipos conectados a la red, definiendo el formato de las Direcciones IP, formato universal que respetan todos los dispositivos conectados a cualquier red, y por supuesto a todos los conectados a la Red de Redes, Internet. La dirección IP es única en cualquier dispositivo conectado a Internet, en cualquier lugar del mundo.
2. ***Encaminamiento.*** Esta función permite identificar un camino posible de comunicación entre el origen y el destino. Esta tarea es realizada por los Routers y otros dispositivos de interconexión, que mediante el análisis de la Dirección IP destino de cada datagrama, permite el envío del mismo por el camino más conveniente. Esta función fundamental que cumplen los Routers es posible gracias a los servicios prestados por el protocolo IP, para que esos encaminamientos o enrutamientos sean posibles.
3. ***Segmentación y Reensamblado.*** Esta funciónpermite adaptar el tamaño de los datagramas a las condiciones de transporte de las subredes que atraviesan, de forma que cuando un Router debe reenviar un datagrama por una Red donde no quepa, debido a que el datagrama excede el tamaño máximo que soporta esta Red, procederá a dividir, (segmentar), dicho datagrama en dos o más, para poder cursar dicha información Del mismo modo, el receptor ensamblará los datagramas previamente segmentados, para obtener el datagrama original.

El protocolo IP para cumplir con sus funciones, ofrece un Servicio ***No Orientado a la Conexión y No Confirmado.***

En los protocolos de red ***no orientados a conexión***, no es necesario establecer una conexión previa para transmitir información, semejante al servicio postal. Para operar de este modo todos los Datagramas deben transportar explícitamente la información completa de origen y destino. En el caso del protocolo IP, todos los datagramas transportan la dirección IP origen y destino. Los routers, por lo tanto, encaminan cada datagrama apoyándose en la dirección IP destino, y así determinan el mejor camino hacia el destino.

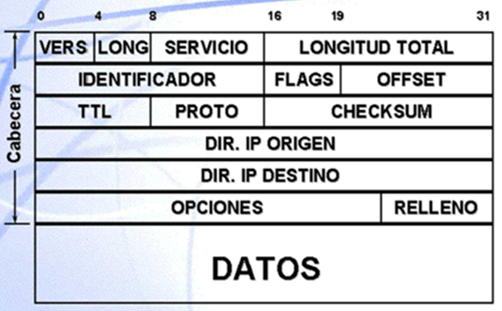
Este mecanismo de funcionamiento hace posible que los datagramas se pierdan, dupliquen o desordenen. Se dice que el protocolo IP ofrece un servicio de ***mejor esfuerzo***, (Best Effort), es decir que hace lo que puede para entregar los datagramas al destinatario, pero no se garantiza que esto suceda. Es decir, si un datagrama se pierde, el protocolo IP no hace nada para recuperarse frente a este error. Son otros protocolos de capas superiores los encargados de corregir estos errores, (Protocolo TCP de la capa de Transporte).

Actualmente existen dos versiones del protocolo IP:

***IPv4***, actualmente implementado en Internet y todas las redes públicas o privadas.

***IPv6***, actualmente implementándose para sustituir a IPv4, dado que ya no alcanzan la cantidad de direcciones IP públicas, dado el crecimiento de dispositivos de red incorporados masivamente. IPv4 utiliza 32 bits para identificar direcciones, mientras que IPv6 amplía el rango a 128 bits.

***Cabecera del protocolo IPv4. Representación gráfica.***



Esta cabecera del protocolo IPv4, es la que corresponde a la capa de Internet, de la familia de protocolos TCP/IP. En la representación gráfica está dispuesta en filas de 32 bits cada una. Cada una de las filas se denominan “Palabras de 32 bits”. Es decir que al finalizar la Palabra 1, comienza la Palabra 2, que es colocada en la segunda fila para comodidad de la representación gráfica, y así sucesivamente.

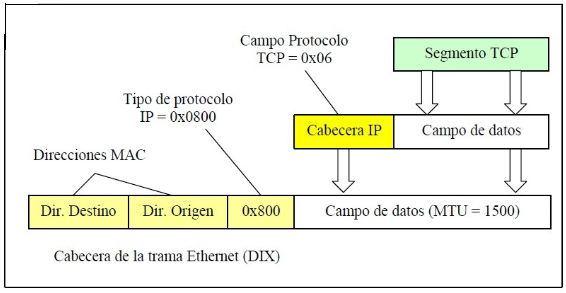
Entonces si está completa la cabecera IPv4, estará constituida por 6 palabras. Sucede que en los casos más habituales la palabra 6, “Opciones y Relleno”, no se utiliza, es decir no aparece en la cabecera. En estos casos la cabecera IPv4 queda conformada por 5 palabras de 32 bits.

***Descripción de los campos de la cabecera del Protocolo IPv4.***

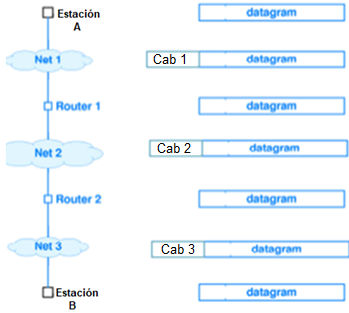
|  |  |
| --- | --- |
| Versión | Versión del protocolo IP, 4 o 6. |
| Longitud: | Longitud de cabecera en palabras de 32 bits. |
| Servicio: | Tipo de servicio. No es considerado por los Routers. No se utiliza. |
| Longitud total: | Longitud total del datagrama, incluidos los datos. |
| Identificador: | Identificador de Datagrama. Se utiliza en la segmentación de datagramas. |
| Flags: | Se utilizan para indicar si hay o no fragmentación. |
| Offset: | Identifica la posición de un fragmento, cuando hay fragmentación. |
| TTL: | Tiempo de vida.Cada Router lo disminuye 1. Si llega a "0" se descarta el datagrama |
| Protocolo: | Tipo de datos de nivel superior que transporta, (ej.: TCP,UDP,ICMP,etc.). |
| Checksum: | Chequeo para determinar si hay errores en el datagrama. |
| Dir IP Origen: | Dirección IP origen del Datagrama. Identifica el origen de la comunicación. |
| Dir IP Destino: | Dirección IP destino del Datagrama. Identifica el destino de la comunicación. |
| Opciones: | Opciones adicionales del protocolo IP. Generalmente no se utiliza. |
| Relleno: | Utilizado junto al anterior para completar la palabra de 32 bits. Se rellena con ceros. |

El Datagrama IP se transmite encapsulado, (oculto), dentro del campo de datos de la trama Ethernet. El datagrama IP consta de la Cabecera IP y el Campo de datos.





***Ejemplo de transmisión de un datagrama a través de tres Redes de Internet:***



A medida que el datagrama viaja por las redes mantiene inalterables las direcciones IP Destino y Origen, sin embargo las direcciones MAC, van cambiando de red en red.

Si la estación “A” conectada a la Red1, debe enviar un paquete de información a la estación “B”, que se encuentra en la Red3, entonces la estación “A” envía la trama a la dirección física del Router1, obtenida a partir de un mensaje ARP. Conformando la Cabecera1 de la trama Ethernet, quedando el datagrama intacto:

Cabecera1:

MAC Destino: Mac del Router1

MAC Origen: Mac de Estación A

Una vez en el Router1, éste consultará su tabla de enrutamiento que tiene asignado el Router2 como siguiente salto, para llevar el paquete a su destino. El Router1 envía la trama al Router2, con la siguiente cabecera de trama Ethernet:

Cabecera2:

MAC Destino: Mac del Router2

MAC Origen: Mac del Router1

Al ingresar la trama al Router2, que comparte la red con la estación destino “B”, envía solicitud ARP request, consultando la dirección física de “B”, utilizando la Dirección IP de “B”, estableciendo la siguiente cabecera de trama:

Cabecera3:

MAC Destino: Mac de Estación B

MAC Origen: Mac del Router2

De esta forma la trama que salió de la estación “A”, llega finalmente a la estación “B” que se encuentra en una red distinta a la de la estación “A”.

***Tema 3: Fragmentación y Reensamblaje del Datagrama.***

***Fragmentación.***

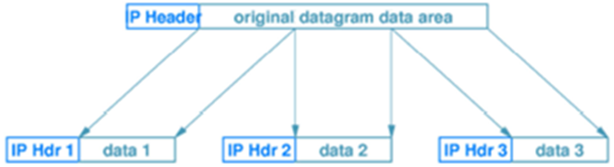
Cada Red que atraviesa un Datagrama tiene su propia tecnología de hardware, que fija la cantidad máxima de datos que puede soportar. Esto se denomina ***Unidad de Transferencia Máxima, (MTU).***  La figura siguiente ilustra un Router que conecta dos Redes con MTU diferentes.



Si el Host 2 envía un datagrama con 1000 octetos, al llegar al Router, éste lo transmite sin inconvenientes al Host 1.

Sin embargo si el Host 1 envía un datagrama con 1500 octetos, el Router no podrá transmitirlo al Host 2, debido a que el MTU de la Red 2 no admite más que 1000 octetos.

En este caso el Router tiene que utilizar la técnica conocida como ***Fragmentación***, que consiste en lo siguiente: Cuando un ***datagrama*** es más grande que la ***MTU*** de la Red que debe atravesar, el Router lo divide en fragmentos más pequeños que son enviados por separado:



Para fragmentar un datagrama el Router debe calcular cuántos fragmentos se requieren. Entonces la cabecera original se copia en las cabeceras de cada uno de los segmentos, y se modifican los siguientes campos en las cabeceras de los fragmentos:

|  |  |
| --- | --- |
| Identificador: | Identificador de Datagrama. Todos los segmentos tendrán el mismo |
| Identificador para poder ser luego reconstruido en el Host Destino. |
| Flags: | Se coloca en “1”, para indicar que es un fragmento. |
| Offset: | Identifica la posición del fragmento. |
| Longitud total: | Longitud total del fragmento, incluidos los datos. |

***Fragmentación de fragmentos.***

Si un Router realiza una fragmentación y ese datagrama tiene que viajar por una red de un MTU todavía más pequeño, el nuevo Router puede fragmentar el fragmento. Cada arquitectura de red de transmisión tiene un límite físico del número de bytes de datos que pueden estar contenidos, esto se denomina MTU. En la siguiente tabla mostramos algunas arquitecturas de red con su correspondiente MTU.

***Arquitectura de Red MTU en Bytes***

802.3 Ethernet 1500

Token Ring 16 Mb 17914

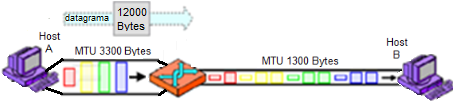
FDDI 4352

***Reensamble.***

El proceso de rearmado se realiza únicamente en el Host Destino, y es un sistema de reensamble del tipo “Todo o Nada”. Es decir, el Receptor cuando recibe un fragmento, dispara un contador que comienza a correr, mientras espera la recepción de todos los fragmentos del datagrama IP. Si al llegar el contador a cero, todos los fragmentos han llegado, se procede al ensamble del datagrama correspondiente.

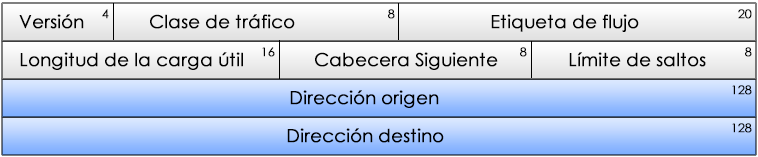
Si en cambio, al llegar el contador a cero, falta uno o varios fragmentos, el Host Destino descarta todos los fragmentos y debe procederse a un nuevo envío del datagrama.

**Gráfico de Fragmentación de fragmentos.**



**Tema 4: Protocolo IPv6. Cabecera IPv6.**

La cabecera del Protocolo IPv6, es más simple que la de IPv4. Está compuesta por diez palabras de 32 bytes. Las dos primeras palabras corresponden a campos específicos, que ha continuación explicaremos. Las ocho siguientes palabras corresponden a las direcciones IPv6.



**Definición de los campos:**

* **Versión:**

Especifica la versión del protocolo, en este caso 6. Requiere 4 bits.

* **Clase de tráfico:**

Mediante este valor podemos definir la prioridad con que los Routers deben gestionar los datagramas, por ejemplo datos como streaming que requieren un flujo de datos ininterrumpido para la correcta transmisión de audio y vídeo. Prioridad baja valor 1 a 7. Prioridad alta valor 8 a 15. Requiere 8 bits.

* **Etiqueta de flujo:**

Mediante la etiqueta de flujo se configura la Calidad de Servicio, (QoS), que consiste en asignar distintas prioridades a las diversas aplicaciones que se ejecutan entre emisor y receptor en redes Wan. Utiliza 20 bits.

* **Longitud de la carga útil:**

Es el tamaño del propio paquete sin incluir la cabecera. En caso de tener cabeceras de extensión, este tamaño si irá incluido en la carga útil. El tamaño máximo del datagrama IPv6 es de 64 Kbytes, y si está configurado como “jumbograma” podrá alcanzar un tamaño de 4Gb. Requiere de 16 bits.

* **Cabecera siguiente:**

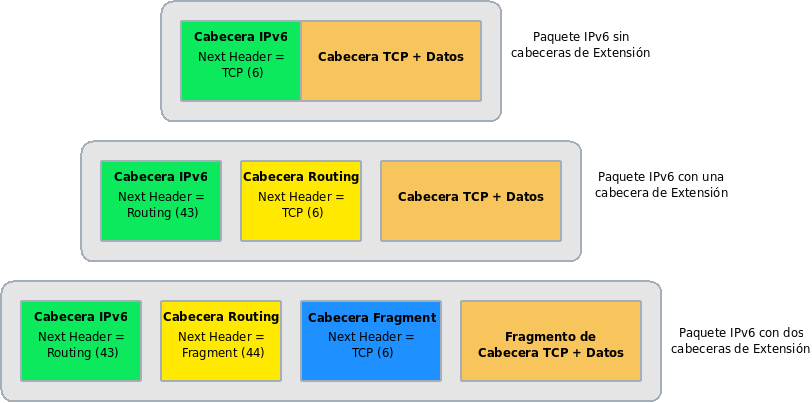
Este valor identifica el siguiente encabezado. Puede no tener siguiente encabezado de IPv6, en ese caso se define como siguiente encabezado la cabecera del protocolo de capa de transporte, (TCP o UDP). Si tiene uno o más encabezados IPv6, cada uno de ellos tiene una función especial, definida por el protocolo IPv6. Requiere de 8 bits.

* **Límite de saltos:**

Equivale al campo Time To Live,(TTL), de IPv4, y cada vez que el datagrama atraviesa un Router es decrementado en 1 bit. Al llegar a 0 el paquete será descartado y se enviará un error ICMPv6 a la estación emisora. Usa 8 Bits.

**Cabeceras de Extensión en IPv6.**

En IPv6 las opciones se manejan por medio de las llamadas Cabeceras de Extensión, (Extension Headers). En la siguiente figura se pueden ver varios casos de utilización de cabeceras de Extensión.



En el primer datagrama hay una única cabecera IPv6 que precede a la cabecera y los datos de la capa superior de transporte.

En el segundo paquete se ha insertado una tercera cabecera entre las dos anteriores. Ahora, la cabecera IPv6 indica que la siguiente cabecera es una cabecera de Extensión del tipo Routing, cuyo código identificativo es el 43 y que se utiliza para dar una lista de uno o más nodos que deben estar en la ruta seguida por un paquete.  
En el campo Next Header de esa cabecera de Routing se indica que a continuación va la cabecera y los datos de TCP.

En el tercer paquete se ha insertado una cabecera más. En este caso es una cabecera de Extensión de Fragmento, cuyo código es el 44, lo que ya ha producido una fragmentación.

**Cuestiones generales relativas a las cabeceras de Extensión.**

* En un paquete IPv6 puede haber cero, una o más cabeceras de Extensión.
* Estas cabeceras se sitúan entre la cabecera IPv6 y la cabecera del protocolo de la capa superior, (capa de transporte).
* Las cabeceras existentes deben ser procesadas en el orden exacto en que aparecen en la cabecera del paquete.
* Cada cabecera de Extensión es identificada por el campo “Next Header” de la cabecera precedente.
* Las cabeceras de extensión son procesadas solo por la Nodo Destino. Pero existe una excepción. Si la cabecera de Extensión es del tipo “Opciones Hop-by-Hop”, ésta cabecera debe ser procesada por cada uno de los nodos que atraviesa el datagrama. Esta cabecera debe seguir inmediatamente a la cabecera IPv6 y su valor de "Next Header" es 0.
* La longitud de cada cabecera de Extensión es un múltiplo de 8 bytes, (2 palabras de 32 bits), de forma que, independientemente del número de ellas que se utilicen, siempre quedan alineadas.

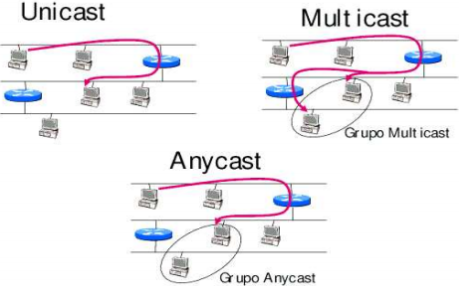
**Tipos de cabeceras IPv6.**

Los tipos principales de cabeceras de Extensión son:

1. De opción ***Hop-by-Hop*** (RFC 2460). La información de esta cabecera debe ser examinada Salto-a-Salto, es decir, en cada uno de los nodos de la ruta que ha de seguir el paquete.
2. De ***Enrutado*** (RFC 2460). Se utiliza para dar una lista de uno o más nodos que deben estar en la ruta seguida por un paquete.
3. De ***Fragmento*** (RFC 2460). Un host IPv6 que quiere enviar un paquete a un destino IPv6, utiliza el llamado “Path MTU discovery” para determinar el tamaño máximo de paquete, que se puede utilizar hasta ese destino. Si el paquete que hay que enviar es más grande que el MTU soportado, el host origen fragmenta el paquete. Gracias a esta forma de actuar, la fragmentación se gestiona de extremo a extremo, liberando a los routers de este trabajo.  
   En caso que el "Path MTU discovery" falle, se usará el valor mínimo de "Path MTU" en IPv6, 1280 bytes. El valor máximo es de 64 Kbytes, en los cuales se incluye la carga o payload del datagrama y los 40 bytes de la cabecera.
4. De opciones de ***Destino*** (RFC 2460). Estas cabeceras llevan información que será procesada, exclusivamente, por el nodo de destino.
5. De ***Autenticación*** (AH) (RFC 4302). Proporciona integridad y autenticación, (no confidencialidad), para todos los paquetes de datos IP.
6. De ***Seguridad Encriptada.*** (Encrypted Security Payload),(RFC 4303). Proporciona integridad, confidencialidad, autenticación de datos y otras funciones para todos los paquetes de datos IP.

**Direcciones IPv6.**

Existen tres tipos de direcciones:



***Unicast:*** Identifica un único Nodo Destino IPv6. Un paquete enviado a una dirección unicast es entregado a la interfaz identificada por dicha dirección.

***Anycast:*** Una dirección anycast es una dirección asignada a más de un interfaz, (generalmente de diferentes nodos), con el propósito de que un paquete que sea enviado a una de estas direcciones sea encaminado hasta el interfaz más cercano que responda a dicha dirección.

***Multicast:*** Una dirección multicast identifica a un grupo de nodos. Un paquete enviado a una dirección multicast es entregado a todos los miembros del grupo. En IPv6 no existe la dirección de broadcast. Su función es reemplazada por el direccionamiento multicast.

**Direcciones multicast comunes:**

Dirección “All Nodes”. FF02:0:0:0:0:0:0:1

Esta dirección identifica al grupo 0:0:0:0:0:0:1, o sea grupo ::1 Todos los nodos, alcance “enlace” (campo scope 2)

Dirección “All Routers” FF02:0:0:0:0:0:0:2

Esta dirección identifica al grupo :2 todos los routers, alcance “enlace” (scope=2)

Dirección “All Routers” FF05:0:0:0:0:0:0:2

Esta dirección identifica al grupo 2 Todos los routers, alcance “sitio” (scope=5)

**Dirección de Loopback. [::1]**

La dirección 0:0:0:0:0:0:0:1 se denomina loopback, sirve para enviar un paquete de IPv6 de un nodo a sí mismo. No puede ser asignada a ningún interfaz físico.

Redes de computadoras, internet e interredes de Douglas E. Comer.

**Fin de la Unidad 9**

**Anexo, para leer.**

**Direcciones Multicast.**

Las direcciones multicast tienen el siguiente formato:



***Campo Prefijo 11111111 ó 0xFF*** identifica la dirección como multicast.

***Campo Flags*** no se usa. ***0000.***

***Campo scope*** indica el alcance de la dirección, desde interfaz hasta alcance global.

***Campo group ID*** identifica al grupo multicast.

Dirección “Solicited-Node”. FF02:0:0:0:0:1:FF**XX:XXXX**

Se fijan los últimos 24 bits de la direcciones de todos los nodos que formarán parte del grupo. Por ejemplo los siguientes nodos serán parte un grupo multicast. Todos tienen sus últimos 24 bits idénticos **0E:8C6C**

IPv6 address 4037::01:800:20**0E:8C6C**

IPv6 address 3539::02:700:20**0E:8C6C**

IPv6 address 6579::05:400:20**0E:8C6C**

Cuando se quiere enviar un datagrama al grupo, se agrega al prefijo multicast, la identificación del grupo: **0E:8C6C**

Prefijo Multicast ***FF02:0:0:0:0:1:FF***00:0000 ***/ 104***

Dirección Multicast del grupo **0E:8C6C**  *FF02:0:0:0:0:1:FF***0E:8C6C** */ 104*

Entonces los nodos que reciban el datagrama con esta dirección multicast, tendrán que tomarlo si pertenecen al grupo **0E:8C6C,** por ejemplo los nodos anteriormente mencionados:

IPv6 address 4037::01:800:20**0E:8C6C**

IPv6 address 3539::02:700:20**0E:8C6C**

IPv6 address 6579::05:400:20**0E:8C6C**

**Direcciones IPv6 que contienen direcciones IPv4.**

Existen dos tipos de estas direcciones. La primera de ellas, denominada **“IPv4-compatible IPv6 address”** fue definida para ayudar en los mecanismos de transición. Su formato es:



El segundo tipo de direcciones conocida como **“IPv4-mapped IPv6 address”**, son las que representan las direcciones de nodos que sólo soportan IPv4 en formato IPv6. Su formato es:



**Direcciones IPv6 con MAC incorporado, identificando el host.**

Un ejemplo de dirección IPv6 con IEEE 802 48-bit MAC incorporado es:

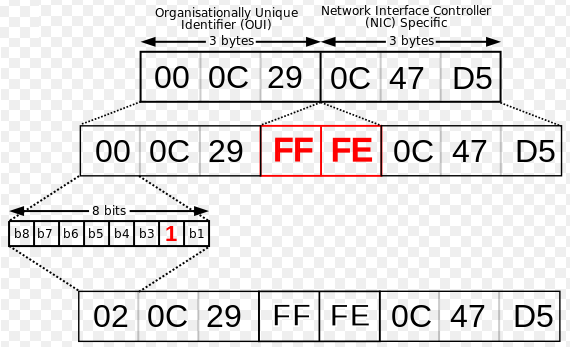


Donde “c” son los bits que identifican a la compañía que desarrolla el hardware, “0” es el valor dado al bit universal/local, (1/0), que indica el alcance de la dirección, “g” es un bit que indica si es una dirección grupo/individual, (1/0), y “m” son los bits del identificador de interfaz elegido por el fabricante. A partir de esta dirección, se obtiene el “Interface ID”.



Donde se ha cambiado el bit global/local para especificarlo como de alcance global y se han añadido los dígitos 0xFFFE para alcanzar los 64 bits necesarios.

Ejemplo:

****

**fin unidad 9.**