TABLA DE CONTENIDO

i

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ICMPV6

El ICMPV6 (Protocolo de control de mensajes de Internet versión 6) es parte integral de la arquitectura de IPV6 y es un soporte completo para todas las implementaciones que soporte IPV6.

ICMPV6 combina funciones previamente subdivididas entre diferentes protocolos, como son el ICMP (Internet Control Message Protocol version 4), IGMP (Internet Group Membership Protocol), y ARP (Address Resolution Protocol), esto introduce ciertas simplificaciones porque se eliminan mensajes obsoletos que ya están en desuso.

En este anexo se analizara las principales características y el formato de los paquetes.

A-1. Apreciación global del protocolo.

ICMPV6 (al cual se hará referencia como ICMP) es un protocolo multipropósito por ejemplo, es utilizado para reportar errores encontrados en el procesamiento de paquetes, realizar diagnósticos, realizar el descubrimiento del vecindario, y reportar miembros del grupo multicast. Por esta razón, los mensajes ICMP están subdivididos en dos clases: Mensajes de error y mensajes de información.

Los mensajes ICMP son transportados dentro del paquete IPv6. Un mensaje ICMP es identificado por un valor de 58 en el campo *Next Header* de la cabecera IPV6.

A-2. Formato de los paquetes.

Los paquetes ICMPv6 muestran el formato indicado en la Figura A-1. El campo de 8 bits denominado type (tipo) indica el tipo de mensaje. Si el bit de mayor orden tiene el valor de cero (estos valores están en el rango de 0 a 127), significa que es un mensaje de error, si tiene un valor de 1 (valores en el rango de 128 a 255), es un mensaje de información. Una lista de los mensajes se muestra en la Tabla A-1.

El contenido del campo de 8 bits denominado *Code* (código*)* depende del tipo de mensaje, y es utilizado para crear un nivel adicional. El campo *checksum* (chequeo) es utilizado para detectar errores en el mensaje ICMP y en parte del mensaje IPv6.

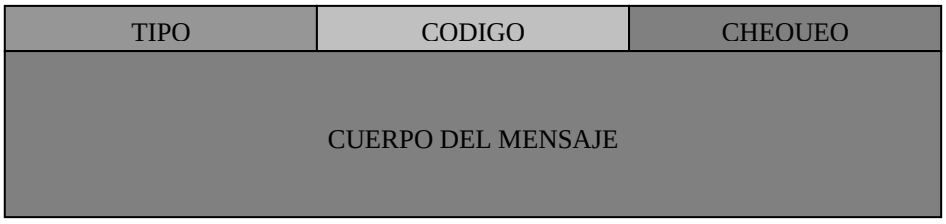

Figura A-1: Formato de un mensaje ICMPV6

TIPO	SIGNIFICADO
1	Destino no asequible.
2	Paquete demasiado grande.
3	Tiempo excedido.
4	Problema de parámetro.
128	Solicitud Eco.
129	Respuesta Eco.
130	Solicitud de afiliación al grupo.
131	Reporte de afiliación al grupo.
132	Reducción de afiliación al grupo.
133	Solicitud de enrutador.
134	Anuncio de enrutador.
135	Solicitud de vecindario.
136	Anuncio de vecindario.
137	Reenviar.

Tabla A-1: Tipos de mensaje ICMP

A-3. Mensaje de transmisión icmp.

Un nodo que recibe un mensaje ICMP tiene que determinar la fuente y el destino de la dirección IPv6 para ese mensaje ICMP. Se debe tener particular cuidado en la selección de la dirección fuente. Si un nodo tiene mas de una dirección unicast , se debe realizar lo siguiente:

- Si el mensaje es una respuesta a otro mensaje enviado a un nodo con dirección unicast, la dirección de origen de la respuesta debe ser la misma del mensaje enviado.
- Si el mensaje es una respuesta a un mensaje con destino multicast o anycast, que son direcciones de un grupo al cual pertenece el nodo, la dirección fuente de la respuesta debe ser una dirección unicast perteneciente a la interfaz en donde el paquete multicast o anycast fue recibido.
- Si el mensaje es una respuesta a un mensaje enviado a una dirección que no pertenece a determinado nodo, la dirección fuente debe ser la unicast perteneciente al nodo que permita encontrar el error de pertenencia.

- En otros casos las tablas de enrutamiento deben ser examinadas, para determinar cual interfaz debe ser utilizada para transmitir el mensaje a su destino, la dirección unicast perteneciente a esa interfaz debe ser utilizada como dirección fuente del mensaje.

Cuando un nodo ICMP recibe un paquete se deben emprender las siguientes acciones que dependen del tipo del mensaje. Más aun, el protocolo ICMP debe limitar el número de mensajes de error enviados al mismo destino para con ello descongestionar la red. Un mensaje de error ICMP nunca debe ser enviado como respuesta a otro mensaje de error ICMP.

A-4. Mensajes de error.

Los mensajes de error en ICMPv6 son similares a los que se utilizaban en ICMPv4. Estos pertenecen a cuatro categorías: Destino irreconocible, Paquete demasiado grande, tiempo excedido, y problemas de parámetros, se describirán seguidamente:

A-4.1. Destino no reconocido.

Este tipo de mensaje, es generado cuando la red debe descargar un paquete IPv6 en un destino desconocido. El destino IPv6 de un paquete ICMP es por consiguiente la dirección fuente del paquete.

En La Figura A-2 podemos ver los diferentes campos, el campo de la trama llamado tipo se pone a un valor de 1. El campo código puede tomar valores como los reportados en la tabla A-2. El campo sin utilizar es inicializado a cero durante la transmisión e ignorado en la recepción. La primera parte de un paquete IPv6 es el responsable de la generación del paquete ICMP. De esta manera hay una puesta a punto para transmitir el paquete ICMP y cualquier enlace debe ser posible, el paquete no debe exceder un número de octetos establecido en 576 (esto podría incluir, dado el caso a la cabecera IPv6 y eventuales extensiones de la misma).

Este tipo de mensajes puede ser generado por un enrutador o por un nodo destino, si no se puede entregar el mensaje, el enrutador o el nodo, es forzado a desechar el mensaje.

Un paquete desechado sin generar mensajes al respecto, si la red esta congestionada, generando un mensaje ICMP, se hará la congestión aun peor. Las razones para el fallo en la entrega de paquetes son las siguientes:

- No hay ruta de destino: Un enrutador no puede encontrar una maquina para la dirección de destino en su tabla de enrutamiento, y por lo tanto no sabe a cual interfaz retransmitir el paquete.
- Comunicaciones con destino prohibido por el administrador: El mensaje es generado por un firewall esto es por un enrutador que contiene una serie de especificaciones para prohibir ciertas comunicaciones.
- Falla por falta de vecindario: El mensaje contiene una cabecera de enrutamiento, la dirección de destino próxima que no pertenece a ninguno de los enrutadores preestablecidos (no es un vecindario).

- Dirección irreconocible: La dirección de destino es irreconocible por ejemplo: Por un error de interfaz o por la inhabilidad de computar la dirección de capa de enlace del nodo destino.
- Puerto irreconocible: El paquete alcanza el nodo destino, pero la capa protocolo (por ejemplo UDP) ha donde el paquete debe ser entregado tiene un puerto irreconocible.

Figura A-2: Mensaje de destino no reconocido

A-4.2. Paquete demasiado grande.

El mensaje que hace referencia a un paquete demasiado grande, ver Figura A-3, es generado cuando la red debe desechar un paquete IPV6 debido a que su tamaño excede los parámetros normales. La información contenida en el paquete ICMP es utilizada como parte del procedimiento de descubrimiento. La dirección de destino IPV6 del paquete ICMP es tomada como la dirección fuente del paquete desechado.

El campo tipo un valor de 2.
El campo código siempre tiene un valor de cero.
El campo de 32-bits MTU indica el MTU del enlace en el cual la transmisión del paquete fue imposible.
La primera parte del paquete IPV6 que causo que siguiera el paquete ICMP, ya que la transmisión de los paquetes ICMP debe ser posible en cualquier enlace, no debe exceder los 576 octetos.

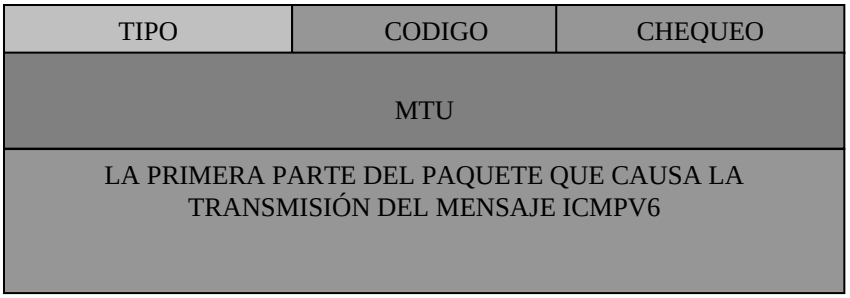

Figura A-3: Paquete demasiado grande

CÓDIGO	SIGNIFICADO
0	No hay ruta de destino
1	Comunicación con el destino prohibida por el administrador
2	No hay vecindario
3	Dirección inasequible
4	Puerto inasequible

Tabla A-2: Destino no reconocido

A-4.3. Tiempo excedido.

El mensaje de tiempo excedido, ver Figura A-4, es generado cuando un enrutador debe desechar un paquete IPv6 que tiene su campo *Hop Limit* en cero o se decrementa a cero. Este mensaje indica que el valor inicial del campo *Hop Limit* es muy pequeño.

Otra razón es la imposibilidad de reensamblar un paquete fragmentado dentro del tiempo limite. Cuando esto sucede la dirección destino del paquete IPV6 es la misma de la dirección fuente, que será el destino del paquete.

El campo tipo toma un valor de 3.
El campo código puede tener los valores mostrados en la Tabla A-3.

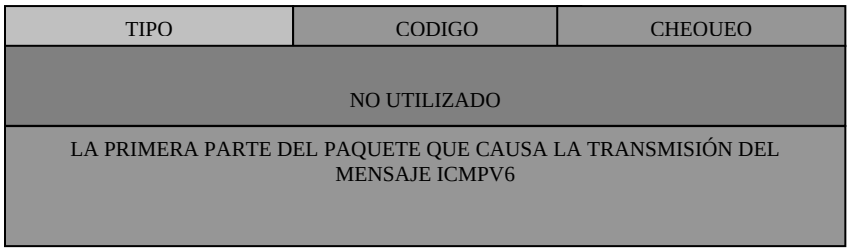

Figura A-4: Mensaje de tiempo excedido

CODIGO	SIGNIFICADO
0	Limite de saltos en transito excedido
1	Tiempo excedido en reensamble de fragmentos

Tabla A-3: Tiempo excedido, valores que puede tomar el campo código

A-4.4. Problemas de parámetros.

El mensaje de problemas de parámetros, ver Figura A-5, es generado cuando un nodo IPv6 debe desechar un paquete, debido a que detecta problemas en un campo de la cabecera IPv6 o en una extensión de la cabecera. La dirección de destino IPv6 del paquete ICMP es entonces la fuente de destino del paquete desechado.

El campo tipo toma un valor de 4.
El campo Código puede contener los valores de la Tabla A-4.

CODIGO	SIGNIFICADO
0	Campo de cabecera erróneo
1	Siguiente cabecera irreconocible
2	Opción IPv6 irreconocible

Tabla A-4: Valores que puede tomar el campo code cuando se presentan errores de parámetros

El campo puntero identifica el octeto en el mensaje original donde se detecto el error.

Los siguientes errores pueden ser detectados:

- Próxima cabecera no reconocida: La cabecera siguiente no es reconocida por la implementación IPv6 presente en el nodo.
- Opción IPv6 no reconocida: El paquete sostiene una opción no reconocida para la implementación IPv6 presente en el nodo.

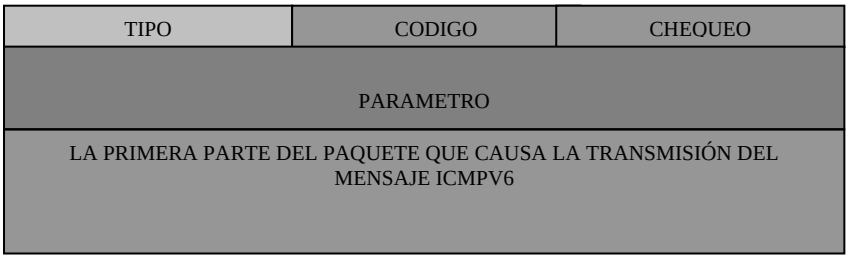

Figura A-5: Mensaje de problemas de parámetros

A-5. Mensajes de información.

Una segunda clase de mensajes ICMP son los mensajes de información. Estos mensajes están subdivididos en tres grupos: Mensajes de diagnostico, mensajes de gestión de grupos multicast y mensajes de descubrimiento de vecindario.

A-5.1. Mensaje de demanda de eco.

El mensaje de demanda de eco y su correspondiente mensaje de respuesta de eco son mensajes de diagnostico ICMP. En particular, estos dos mensajes son usados para implementar un diagnostico de ping, y así poder rastrear y probar un determinado enlace. El formato de estos dos mensajes es el mismo.

La dirección de destino IPv6 puede ser cualquier dirección IPv6 valida.
El campo tipo toma el valor de 129.
El campo código toma el valor de cero.

El campo identificador es un identificador usado para determinar una relación entre los mensajes eco de requerimiento y respuesta. El campo de secuencia de números es una secuencia usada para establecer la relación entre los dos mensajes ecos. Tanto el campo identificador como el campo de secuencia de números pueden ser cero.

El campo datos contiene cero o mas octetos de datos arbitrariamente generados por el procedimiento de diagnostico.

A-5.2. Mensaje de respuesta eco.
Cada nodo IPv6 debe implementar un mensaje de respuesta ICMP eco, para corresponder a los mensajes de requerimiento eco. La dirección de destino IPv6 es establecida igual a la dirección fuente IPv6 de la respuesta eco.

El campo tipo toma el valor de 129.
El campo código toma el valor de cero.

Los campos identificador y secuencia de números tienen funciones similares a los del mensaje de requerimiento eco. El campo de datos es similar al del mensaje de requerimiento de eco, los mensajes eco de petición y respuesta se muestran en la Figura A-6.

A-5.3. Mensaje de número de miembros de un grupo.
Los mensajes ICMP de número de miembros de un grupo son utilizados para llevar información a un grupo multicast que provenga de nodos o de sus enrutadores de vecindario, (conectados al mismo enlace).

La dirección de destino IPv6 cambia en función de los diferentes tipos de mensajes:

- En el mensaje de solicitud de numero de miembros de un grupo, ver Figura A-7, la dirección destino es igual a la dirección multicast del grupo sobre el cual se ha hecho la pregunta o igual a la dirección local de todos los nodos (FF02::1) dirección multicast.
- En un reporte de reducción de alguno grupo, la dirección de destino es igual a la dirección multicast del grupo reportado o terminado.

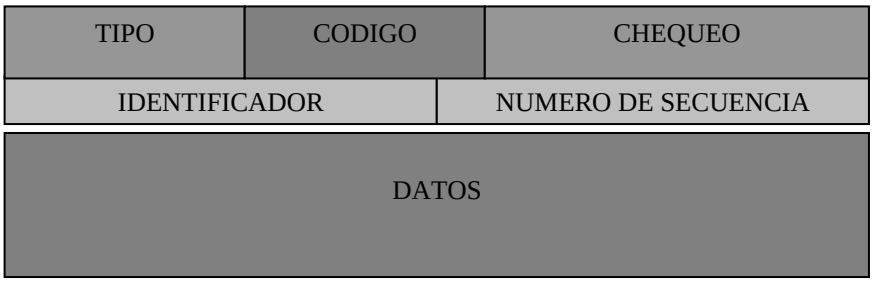

Figura A-6: Formato de mensaje eco de petición y respuesta

Figura A-7: Mensaje de número de miembros de un grupo

El limite de saltos de la cabecera IPv6 es puesta en 1 (los paquetes son intercambiados entre nodos adyacentes).

El campo tipo toma el valor de 130 (Pregunta de número de miembros de un grupo), 131 (Reporte de numero de miembros de un grupo), o 132 (Reducción de número de miembros de un grupo).
El campo código tiene un valor de cero.

El campo de máximo retardo en la respuesta expresa ese valor de retardo. En los mensajes de pregunta de número de miembros de un grupo, este campo indica lo máximo que el mensaje de reporte puede retrasarse. En los mensajes de reporte y reducción este campo es inicializado a cero por el que envía e ignorado por el que recibe. El campo no utilizado debe ser inicializado a cero e ignorado por el receptor.

A-5.4. Mensajes de solicitud del enrutador.

Los mensajes ICMP a los que se hará referencia de aquí en adelante son mensajes de descubrimiento de vecindario (especificados por el RFC 1970). Se analizaran los diferentes formatos de los diferentes mensajes con más detalle.

Los nodos IPv6 transmiten los mensajes de solicitud del enrutador de una manera inmediata. Ver figura A-8

La dirección de origen de la solicitud del enrutador es cualquiera de las direcciones unicast de la interfaz de donde el mensaje es enviado, si esta dirección no existe, se la determina como una dirección no especificada, la dirección de destino es típicamente (FF02::2) que es la dirección multicast para los enrutadores que pertenecen a determinado grupo.

Figura A-8: Formato del mensaje de solicitud de un enrutador

El campo de límite de saltos de la cabecera IPv6 es colocado en 255. Este valor representa una forma de protección contra ataques de hackers. De hecho, los enrutadores deben verificar si este campo tiene el valor de 255, si no es así, el paquete se desecha. Un hacker nunca puede enviar un mensaje con este campo puesto a un valor de 255, desde fuera de la LAN, debido a que el enrutador decrementa esta cabecera en uno. Únicamente paquetes generados en la LAN pueden tener este campo a un valor de 255.

El campo Prioridad en la cabecera IPv6 toma un valor de 15.
El campo tipo es igual a 133.
El campo código es igual a cero.
El campo de reserva no es utilizado, debe ser inicializado a cero durante la transmisión e ignorado en la recepción.
En el campo opciones puede aparecer la dirección del nodo fuente.

A-5.5. Mensaje de anuncio del enrutador.

Los enrutadores envían mensajes de anuncio periódicamente en respuesta a un mensaje de solicitud. El formato de este mensaje se muestra en la Figura A-9.

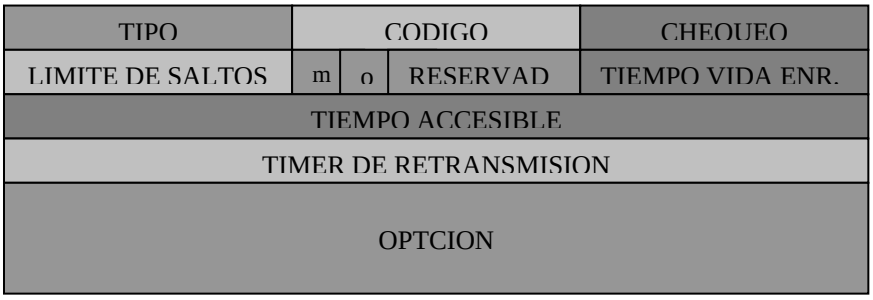

Figura A-9: Formato del mensaje de anuncio del enrutador

La dirección fuente de IPv6 es puesta igual que la dirección de enlace local de la interfaz a la cual es enviado el mensaje, Y la dirección destino es igual a la dirección del nodo que solicita el mensaje o sino a la dirección multicast de todos los nodos (FF02::1).

El campo limite de saltos de la cabecera IPv6 es colocado a 255.
El campo prioridad de la cabecera IPv6 es colocado a 15.
El campo tipo es igual a 134.
El campo código es igual a cero.

El campo de 8 bits límite de saltos mostrado en la Figura A-9 especifica, que nodos van a recibir este mensaje. Un valor de cero significa que el que el enrutador que envía no determina ningún valor por defecto.

El campo de 1 bit M (Managed address configuration*)*, cuando se utiliza, indica los nodos que recibirán el mensaje y que utilizan el protocolo stateful para la autoconfiguración de direcciones en adición a la autoconfiguración de la dirección sin estado.

El campo de 1-bit O (*Other Stateful configuration*), cuando se utiliza, indica los nodos que deben utilizar el protocolo de autoconfiguración stateful para proveer información adicional.

El campo reservado no es utilizado, debe ser inicializado a cero por el que envía e ignorado por el receptor.

El campo de 16-bits tiempo de vida del enrutador, contiene el periodo de tiempo en segundos por el cual el enrutador puede ser utilizado como el enrutador por defecto por los nodos receptores. Si este campo es igual a cero, el enrutador no puede ser utilizado como enrutador por defecto.

El campo de 32-bits tiempo accesible contiene el tiempo en milisegundos, que un nodo asume un vecindario como rastreable después de haber recibido una confirmación de rastreabilidad. Este parámetro es utilizado por el algoritmo de rastreo del vecindario.

El campo de 32-bits tiempo de retransmisión contiene el tiempo en milisegundos entre la solicitud de retransmisión de determinado vecindario. Esto es utilizado por los algoritmos de detección de vecindario y resolución de direcciones. Las siguientes opciones son utilizadas en el capo opciones:

- La opción que especifica la dirección del nodo fuente.
- La opción que especifica el enlace MTU.
- La información de prefijo que especifica los prefijos a ser utilizados para la autoconfiguración de direcciones.

A-5.6. Mensaje de solicitud del vecindario.
Los mensajes IPv6 de solicitud de vecindario, ver Figura A-10, requieren la dirección de la capa de enlace de los nodos objetivo, los mensajes de solicitud del vecindario son enviados a direcciones multicast.

La dirección origen de este mensaje es una dirección unicast de la interfaz que transmite el mensaje.

El campo limite de saltos en la cabecera IPv6 es colocado a 255.
El campo prioridad de la cabecera IPv6 es puesto a 15.
El campo tipo es igual a 135.
El campo código es igual a cero.
El campo reservado no es utilizado, debe ser inicializado a cero por el que envía el mensaje e ignorado por el receptor.

El campo de 128-bits dirección destino especifica la dirección del nodo destino, esto es la dirección IPv6 del nodo al cual el mensaje de solicitud del vecindario ha sido enviado.

En el campo opciones puede estar presente la opción que especifica la dirección de la capa de enlace de la fuente.

Figura A- 10: Formato del mensaje de solicitud del vecindario

A-5.7. Mensaje de anuncio del vecindario.
Cuando el estado de un nodo cambia este envía el mensaje de anuncio del vecindario, ver Figura A-11, de esta manera se propagan las modificaciones rápidamente y también sirve como respuesta al mensaje de solicitud de vecindario.

El campo dirección fuente IPv6 es colocado a la dirección de la interfaz de donde el mensaje fue enviado, y la dirección destino es igual a la dirección del nodo que solicita el mensaje o sino ha todos los nodos (FF02::1), dirección multicast.

El campo límite se saltos de la cabecera IPv6 es colocado a 255.
El campo prioridad de la cabecera IPv6 es colocado a 15.
El campo tipo es colocado a 136.

El campo código es igual a cero.
El campo de 1-bit R (Router flag) indica, si el nodo fuente es un enrutador.
El campo de 1-bit S (Solicited flag), indica si el mensaje ha sido enviado como una respuesta a un mensaje de solicitud de vecindario.
El campo de 1-bit O (Override flag) indica que el mensaje debe actualizar al cache con la dirección de capa de enlace.
El campo de 29-bits reservado no es utilizado; debe ser inicializado a cero por el que envía e ignorado por el que recibe.
El campo de 128-bits dirección objetivo especifica, por solicitud, la dirección del nodo que envía el anuncio.
El campo opción puede contener la opción que especifica la dirección de capa de enlace de destino, ósea la dirección del nodo que envía el anuncio del vecindario.

Figura A-11: Formato del mensaje de anuncio del vecindario

A-5.8. Mensajes de redirección.
Los enrutadores transmiten este tipo de mensajes para informar acerca de un mejor camino hacia el destino. Puede ser pasando por otro enrutador conectado al mismo enlace, pero comúnmente la redirección se hace a otro vecindario.

La dirección fuente IPv6 es igual a la dirección de enlace local de la interfaz de donde el mensaje ha sido enviado, y la dirección destino es igual a la dirección fuente del paquete que causa que se genere el mensaje de redirección.

El campo limite de saltos de la cabecera IPv6 es colocado a 255.
El campo prioridad de la cabecera IPv6 es colocado a 15.
El campo tipo es igual a 137.
El campo código es igual a cero.
El campo reservado no es utilizado, debe ser inicializado a cero por el que envía e ignorado por el que recibe.

Figura A-12: Formato del mensaje de redirección

El campo de 128-bits dirección objetivo contiene, como respuesta a solicitud, la dirección del nodo que solicita la respuesta. Cuando la dirección destino es el punto final de la comunicación, esto es el destino es un vecindario, el campo dirección objetivo debe contener los mismos valores del campo dirección destino. Por otra parte, la dirección destino es la dirección de enlace local del primer y enrutador hacia el destino.El campo de 128-bits dirección destino contiene la dirección IPv6 del destino.

En el campo opciones podemos tener:

- La dirección de capa de enlace del destino
- La cabecera de redirección, esto es la opción contiene la parte inicial del paquete que causa el mensaje de redirección, teniendo en cuenta, claro esta, el límite de octetos de un mensaje ICMP.

A-5.9. Formato de opciones.

Los mensajes de descubrimiento de vecindario pueden incluir el cero, uno, o más opciones. Algunas opciones pueden aparecer en múltiples tiempos en el mismo mensaje. Todas las opciones tienen el mismo formato, ver Figura A-13.

El campo de 8-bits tipo específica el tipo de opción.
El campo de 8-bits longitud, específica la longitud de la opción en octetos. El valor cero es inválido, así que los nodos que reciben un paquete de descubrimiento de vecindario con longitud cero, deben desecharlo.

A-5.9.1. Fuente / destino, opción de dirección de capa de enlace.

Tipo 1 (dirección fuente) y tipo 2 (Dirección destino) estos dos tipos tienen idénticos formatos, ilustrados en la Figura A-14. La dirección de capa de enlace tiene una longitud variable. La longitud mínima (Length = 1) reserva 48 bits para la dirección de capa de enlace, esta longitud es ideal para transportar las direcciones MAC de las LANs.

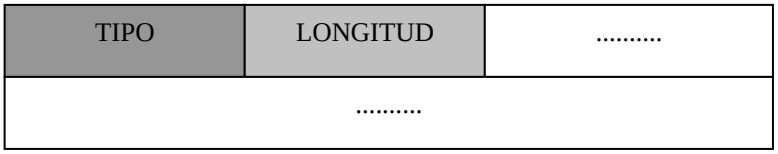

Figura A-13: Formato de opciones

TIPO	NOMBRE DE LA OPCION
1	Dirección de la capa de enlace de la fuente.
2	Dirección de la capa de enlace del objetivo.
3	Información del prefijo.
4	Cabecera de redirección.
5	MTU

Tabla A-4: Posibles valores del campo TIPO

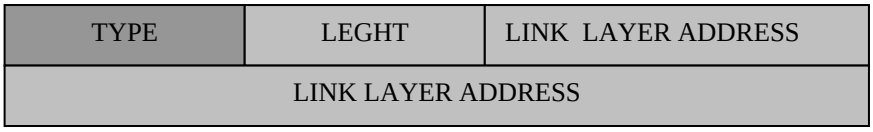

Figura A-14: Formato de Fuente / destino, opción de dirección de capa de enlace

La opción, dirección de la capa de enlace, de la fuente contiene la dirección de la capa de enlace del que envía el paquete. Esta opción es utilizada en la solicitud del enrutador, y en los mensajes de solicitud del vecindario.

La dirección de la capa de enlace del objetivo contiene como su nombre lo indica la dirección del destino. Esta opción es utilizada en los anuncios de vecindario y en la redirección de mensajes.

A-5.9.2. Opción de información de prefijos.
La opción de información de prefijos provee a los hosts con prefijos de enlace la opción de autoconfiguración. El formato de la información de prefijos es ilustrado en la Figura A-15.

El campo de 8-bits *Prefix Length* contiene la longitud de los prefijos, los valores validos están entre el rango de 0 a 128.

El campo de 1-bit L (on-Link flag), indica, si se utiliza, que todas las direcciones que tienen ese prefijo pertenecen a determinado enlace. Cuando este campo no es utilizado algunas direcciones pueden ser on link y otras off link (fuera del enlace).

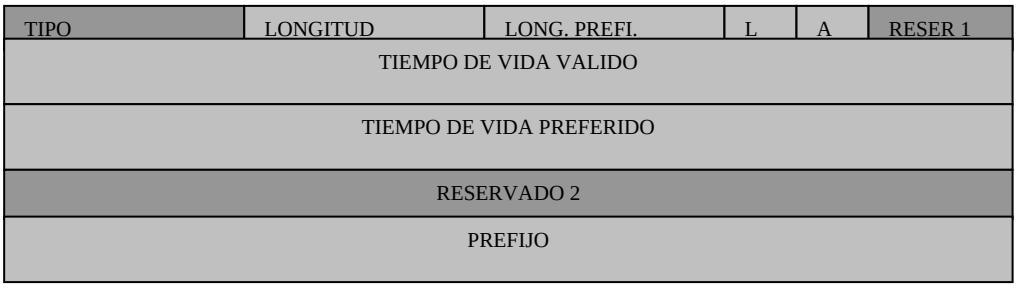

Figura A-15: Formato de la opción información de prefijo

El campo de 1bit A (Autonomous address configuration flag) indica, si se utiliza, que el prefijo puede ser utilizado para la configuración autónoma de dirección.
El campo de 6-bits Reser. 1 no es utilizado, debe ser inicializado a cero por el que envía e ignorado por quien lo recibe.
El campo de 32-bits, tiempo de vida valido contiene el número de segundos en que la dirección generada del prefijo vía autoconfiguración, continua siendo valida. El valor FFFFFFFF representa inifinito.
El campo de 32-bits, tiempo de vida preferido, contiene el número de segundos en los que una dirección generada mediante el prefijo utiliazado la autoconfiguración, permanece como "preferida". El valor hexadecimal FFFFFFFF representa infinito.
El campo de 32-bits, reservado, no es utilizado, debe ser inicializado a cero por el que envia e ignorado por el receptor.
El campo de 128-bits, prefijo, contiene una dirección IPv6 o un prefijo de una dirección IPv6. Para la longitud del primer prefijo, unicamente son tenidos en cuenta los bits más significativos, los otros deben ser ignorados e inicializados a cero.

A-5.9.3. Opción de cabecera de redirección.

Esta opción es utilizada en los paquetes de redirección ICMP, que contienen la primera parte del mensaje que causa la demanda de redirección. El formato de esta opción es mostrado en la Figura A-16.
El campo de 48-bits, Reservado, no es utilizado, se debe inicializar a cero por el que envia e ignorado por el que recibe.
El campo cabecera IP + datos, contiene el paquete que genera el mensaje de re dirección. El paquete original es truncado para asegurar que el tamaño del mensaje de redirección no exeda los 576 octetos.

Figura A-16: Formato de la opción cabecera de redirección

A-5.9.4. La opción MTU.

Esta opción es utilizado en los mensajes de anuncios de enrutadores para asegurar que, en enlaces con valores de MTU variables, todos los nodos utilicen el mismo valor de MTU. El formato de la opción MTU es ilustrado en la Figura A-17.
El campo de 16-bit Reservado no es utilizado, debe ser inicializado a cero por el que envia e igonorado por el receptor.
El campo de 32-bits, máxima transmisión de unidad (MTU) contiene el MTU recomendado para el enlace.

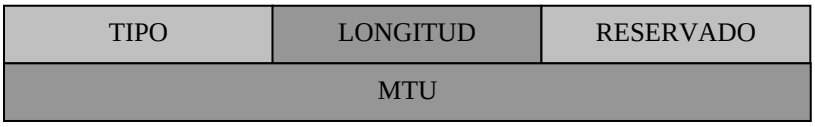

Figura A-17: Formato de la opción MTU

BIBLIOGRAFIA

Referencias Impresas.

- Silvano Gai. “Internetworking IPv6 with Cisco Routers”.
  McGraw-Hill Computer Communications Series, 1998.

- Mark A. Millar, P.E. “Implementing IPV6: Supporting the Next Generation Internet Protocols” Second Edition.
  The M&T IP Library,