Capítulo II. Teoría y métodos de transición IPv4 e IPv6

El objetivo de éste capítulo es dar las bases teóricas para concocer IPv4, saber que es IPv6 y como se compone, así como los cambios en referencia a IPv4, también el capítulo pretende hacer del conocimiento los métodos de transición de IPv4 a IPv6 y la manera de configurar túneles para comunicar equipos IPv4 con equipos IPv6 o comunicar equipos IPv6 a traves de una red IPv4.

En primera instancia para conocer la manera actual de trabajar de las redes actuales, se vé lo que es IPv4, posterior a eso para concocer el nuevo protocolo y saber como funciona se vé IPv6, después comenzando con los métodos de transición, se vé una breve desripción de lo que es NAT y para que nos sirve en IPv6, posteriormente para saber como hacer una migración, se vé cuales son los métodos de transición de IPv4 a IPv6 y finalmente para hacer la implenetación, se vé la manera de configurar los túneles en los equipos y los ruteadores.

2.1.- IPv4

El protocolo IP (*Internet Protocol*) es en el cual se basa la transmisión de datos en Internet, su definición se encuentra en el RFC 791, su base es la transmisión de datagramas a través de la Internet, lo cual hace por medio de un sistema *conectionless* y *unreliable* y da el servicio *best effort*, TCP provee las caracteristicas de confiabilidad y de conexión e IP le delega ese trabajo para no hacer un retrabajo, los protocolos trabajan en conjunto pero cada uno haciendo lo que es necesario para que los datos lleguen con seguridad a su destino sin tener que ser enviados todos los datagramas por el mismo camino.

La capacidad de *best effort* de IP funciona de manera que si existe una falla en el enlace por el cual se están transmitiendo los datos, se tengan caminos alternos por los cuales se pueda transmitir la información por medio de un sistema muy sencillo de solución de errores.

El mecanismo de control de errores es controlado por el *Internet Control Message Protocol* (ICMP), por ejemplo, si a un ruteador le falla un enlace por el cual estaba transmitiendo los datos, elimina el datagrama y manda un mensaje de ICMP al equipo que está enviando los datos y se olvida del datagrama, no trata de retransmitirlo, el equipo que estaba transmitiendo, retransmite el datagrama, no teniendo la información de cual enlace está activo o no.

Cuando el datagrama llega al ruteador él verá la manera de hacerlo llegar a su destino por otro enlace, lo que nos refleja éste tipo de servicio es que no implica fiabilidad (*unreliable*) y no conexión (*conectionless*) por un camino específico.

2.1.1.- Estructura del datagrama IPv4

La estructura de un datagrama IP, se divide en bloques de 32 bits (4 bytes), comenzando de izquierda a derecha y de arriba hacia abajo, el primer bit es el bit 0, el orden es importante ya que dependiendo del equipo al que se está comunicando es su manera de guardar los bits en memoria, ver figura 2.1. A ésta manera de transmitir los bits se le denomina *network byte order*.

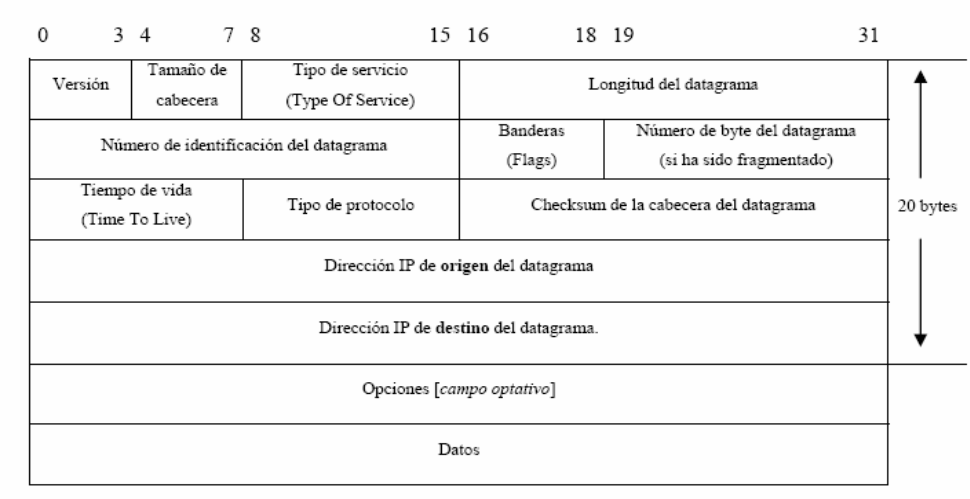

Fig. 2.1: Estructura de un datagrama IPv4

Los datos del encabezado son importantes ya que son la manera de dar a concocer al ruteador o al otro *host* lo que se está enviando. Para tener más claros los campos se detalla su contenido a continuación.

El campo de versión especifíca que formato de versión es el datagrama, ésta información solamente lo utilizan los ruteadores y la capa IP de la conexión, permite que coexistan varias versiones de IP en las diferentes redes conectadas a la Internet sin que el usuario sepa de su existencia.

El campo de tamaño del encabezado indica el número de palabras de 32 bits que ocupa el encabezado, estos 4 bits limitan el tamaño de la encabezado a 60 bytes, sin embargo por lo regular se ocupan 20 bytes.

El campo de tipo de servicio son 8 bits, los primeros 3 no se usan, los siguientes 4 definen el tipo de servicio, el cual se detalla en la tabla 2.2 y el último bit no se utiliza pero debe de tener valor de 0 siempre, en los bits de tipo de servicio, solamente uno puede estar activo a la vez.

El tipo de servicio se tiene para darle a entender al ruteador la política de servicio que se debe de tener con el datagrama, minimizar el retrazo, maximizar el rendimiento, maximizar la fiabilidad del transporte y minimizar el costo económico del transporte.

Tipo de servicio

Tipo de aplicación	Minimizar retraso	Maximizar rendimiento	Maximizar fiabilidad	Minimizar costo	Valor en hexadecimal
TELNET	1	0	0	0	0x10
FTP	0	1	0	0	0x08
SMTP	0	1	0	0	0x08
DNS (UDP)	1	0	0	0	0x10
DNS (TCP)	0	0	0	0	0x00
ICMP	0	0	0	0	0x00
BOOTP	0	0	0	0	0x00

Fig. 2.2: Valores típicos del tipo de servicio según la aplicación [Ver00]

El campo de longitud del datagrama mide 16 bits y dice cuanto espacio se debe guardar en la memoria para la recepción de cada datagrama, también dice cuantos bytes se deben leer por datagrama, con esto se puede tener un control muy sencillo de si los datagramas llegan completos o no, también limita el tamaño máximo de los datagramas a 65515 bytes, el *Maximum Tranfer Unit* (MTU) es 2^{16} bytes 65525 – 20 bytes de encabezado.

En dado caso que un paquete que se quiera enviar por la red excede el máximo disponible para dicha red, se divide en varios pedazos.

El campo de número de identificación del datagrama indica el número de paquete que se esta recibiendo o enviando cuando se tiene que dividir en pedazos un paquete, así cuando se recibe el paquete se puede ordenar adecuadamente, mide 16 bits, por lo que un datagrama se puede dividir hasta en 65535 fragmentos.

El campo de banderas mide 3 bits y especifíca diferentes actividades según el bit que esté encendido, si el primero está encendido quiere decir que el datagrama es parte de un datagrama mayor, si el segundo está encendido quiere decir que el datagrama no debe de ser fragmentado y el tercero no se utiliza, teniendo siempre el valor 0.

El campo de número de byte en el datagrama, indica cual es la posición en bytes que ocupan los datos en el datagrama original, obviamente solo se ocupa si el fragmento es parte de un paquete mayor, mide 13 bits y sirve para reconstruir el paquete original.

El campo de tiempo de vida mide 8 bits y es el que indica cuanto tiempo vivirá el datagrama en transición, es decir, cuanto tiempo tiene el datagrama para llegar a su destino para que los datagramas no circulen para siempre por la red, éste campo tiene un valor máximo de 255 y cada vez que pasa por un ruteador su valor se decrementa en uno, si el valor llega a cero, el ruteador que le toca proporcionar ese valor, envía un ICMP al origen para que el datagrama sea retransmitido.

El campo de tipo de protocolo indica el protocolo superior que se esta utilizando, ya sea TCP, UDP, ICMP, etc. El campo se ocupa ya que todos los protocolos de Internet utilizan IP como medio de transporte y al llegar al destino hay que entregarlo en los medios adecuados.

El campo de suma de comprobación (“checksum”) del encabezado del datagrama se utiliza solo para verificar el encabezado, ya que tanto UTP, TCP y demás protocolos tienen su propio “checksum” y verificarán sus datos de manera autónoma, sirve para verificar que el encabezado llegue completo y no se descarte el datagrama por pérdida de información en el camino.

2.1.2.- Direccionamiento IPv4

La dirección IP origen y la dirección IP destino son dos números de 32 bits, cada una. Cada equipo tiene un número específico, dentro del protocolo IPv4 se denominan 4 octetos de 8 bits separados por un punto para especificar cada equipo en la red. Existen varios tipos de redes los cuales se describen en la figura 2.3:

CLASE	DESDE	HASTA
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Fig. 2.3: Clases de direcciones IPv4 en Internet

Las clases de redes sirven para definir el tamaño de las redes, como se vió en la figura anterior existen 5 clases de redes, en la figura 2.4 se puede ver la cantidad de equipos que se pueden conectar a cada red:

Clase A	0	Identificador de red (7 bits)																												Número de equipo (24 bits)	
Clase B	1	0	Identificador de red (14 bits)																											Número de equipo (16 bits)	
Clase C	1	1	0	Identificador de red (21 bits)																										Número de equipo (8 bits)	
Clase D	1	1	1	0	Identificador de red (28 bits)																										
Clase E	1	1	1	1	0	Reservado para uso futuro (27 bits)																									

Fig. 2.4: Subdivisión de los 32 bits para las clases A, B, C, D Y E

Cabe mencionar que el número máximo en cada octeto es 255 ya que al ser de 8 bits (2^8=256) el rango es entre 0 y 255 para cada octeto.

Se definieron los diferentes tipos de redes para hacer más fácil la ubicación de redes chicas, medianas y grandes, es decir:

- La red clase A es para redes grandes, se pueden tener 128 (2^7) redes de 16,777,216 (2^{24}) equipos conectados en cada una.
- La red clase B es para redes medianas, se pueden tener 16,348 (2^{14}) redes de 65,535 (2^{16}) equipos conectados cada una.
- La red clase C es para redes chicas, se pueden tener 2,097,154 (2^{21}) redes de 256 (2^8) equipos conectados.

- Las redes clase D y E son de *multicast* y reservada respectivamente, también para futuros usos.

La numeración de las direcciones puede variar desde 0.0.0.0 hasta 255.255.255.255, entonces el aprenderse cada una de las direcciones para acceder a ellas sería muy difícil, pera ayudarnos a recordar las direcciones más fácilmente, existen los DNS (*Domain Name Server*), ellos hacen la traducción de la dirección en números a una dirección que se pueda recordar más fácilmente, por ejemplo una dirección 164.149.10.1 sería más fácil recordarla como www.nombre.com.mx.

La estructura también tiene una especificación definida, la última parte define por lo regular donde se encuentra la página, “.mx” es México, “.uk” es Inglaterra, “.es” es España, etc. El único pais que no tiene definida una abreviación es Estados Unidos, ya que ellos generaron la terminología, para éste caso la última parte y en los demás en la penúltima parte, se define el tipo de red, “.gob” para empresas de gobierno, “.net” para empresas de telecomunicaciones, “.com” para empresas del ámbito general, “.mil” para militares y “.edu” para universidades o empresas educativas, se han agregado algunas como “.tv” para la televisión pero no están bien especificadas.

La segunda parte define el nombre de la empresa o la página a donde se quiere acceder.

La primera parte define por lo regular que se está accesando a una página de Internet (WWW), recientemente se ha desechado ésta parte ya que siempre es lo mismo y algunas empresas mejor la ocupan para diferenciar servidores.

2.2.- IPv6

La nueva versión del protocolo IP se enumeró 6 ya que cuando se estaban haciendo las mejoras de la versión 4 se hicieron varias pruebas, extensiones y modificaciones, por lo tanto para evitar confusiones, cuando la versión fue liberada se le asignó el número 6. [Cis02].

El encabezado de la versión 6 es una versión mejorada de la versión 4, no se ha modificado mucho la estructura ni el contenido, sin embargo se han hecho cambios sustanciales en cuanto a seguridad y quitando datos que eran innecesarios o redundantes, dichos cambios se basaron en los 20 años de experiencia que se tuvieron con la versión 4 lo cual arrojó mucha tela de donde cortar.

Los cambios se realizaron principalmente en dos aspectos:

1. Ampliación del campo de dirección IP a 128 bits, aumentando de 32 a 128 bits cada dirección, se aumentó el número de direcciones significativamente.
2. Campos de longitud fija, para facilitar el proceso que se le da a cada datagrama en los ruteadores para encaminarlo hacia su destino, se adoptó un formato fijo el cual agiliza el tráfico de los datagramas y las opciones siguen estando pero ya no como parte del encabezado.

En esencia el protocolo IPv6 sigue teniendo las mismas características de la versión 4 como se puede ver en la figura 2.5, un protocolo no fiable y no orientado a conexión, el servicio que presta funciona y es lo suficientemente flexible para las necesidades de hoy en día y el

delegar la confiabilidad a los protocolos superiores permite mantener las capas del modelo TCP/IP.

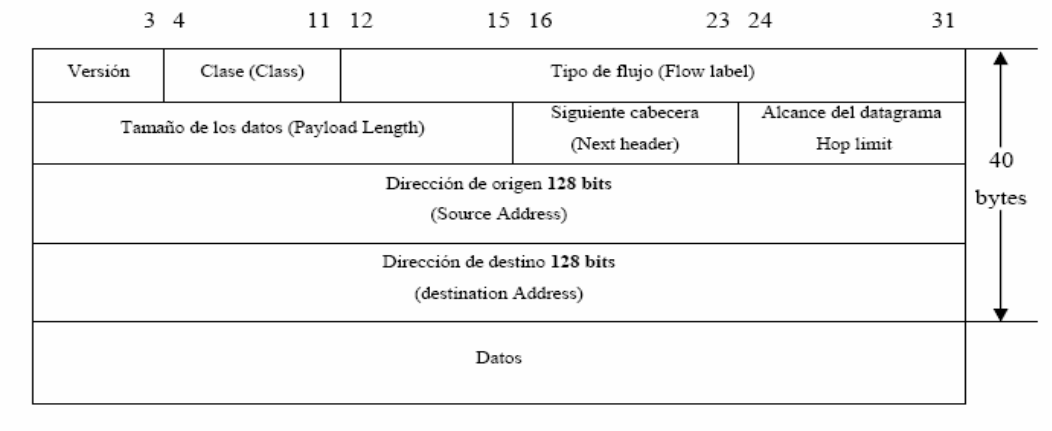

Fig. 2.5: Estructura de un datagrama IPv6

El único campo que no varía su posición y sigue significando lo mismo que en la versión anterior es precisamente el campo de versión ya que durante un buen tiempo convivirán los dos protocolos y así los ruteadores podrán saber inmediatamente que tipo de versión les está hablando y la podrán encaminar de la manera correcta.

El campo de versión sigue siendo un campo de 4 bits que permanece al principio de la encabezado, para mantener consistencia en los dos tipos de encabezados, poder verificar la versión de entrada en los ruteadores y así saber en primera instancia de que versión se está hablando.

Los campos de tamaño de encabezado, tipo de servicio, número de identificación del datagrama, banderas, número de byte del datagrama fragmentado y el “checksum” se

eliminaron, aunado a esto, los campos de longitud del datagrama, tiempo de vida y tipo de protocolo se refinaron.

El campo de clase mide 8 bits y es la que hace referencia a la prioridad del datagrama, éste campo es uno de los que se integraron para mejorar la versión anterior, sirve para dar prioridad a mensajes de telefonía o videoconferencia que tienen que ser en tiempo real, necesitan mas prioridad que un datagrama solamente de datos.

El campo de tipo de flujo mide 16 bits y trabaja en conjunto con el campo de clase en el caso de las aplicaciones en tiempo real ya que especifíca si varios datagramas van de un mismo origen a un mismo destino, por lo cual necesitan el mismo trato.

El campo de tamaño de los datos mide igualmente que en la versión 4, 16 bits, sin embargo, en ésta versión hace referencia solamente a los datos que transporta éste datagrama sin incluir el encabezado.

El campo de siguiente encabezado mide 8 bits e indica al ruteador si después del datagrama existen opciones o extensiones, éste campo sustituye al campo de banderas de la versión 4. En otras palabras, se eliminaron del encabezado la interpretación de las varias opciones que se tienen y se ubicaron fuera del datagrama básico. El hacer este movimiento no complica las cosas al ruteador ya que también se definieron una serie de encabezados de extensión que se ubican después de los datos en forma de cadena y permiten que los datagramas se personalicen, por lo tanto podemos tener varios encabezados solamente con indicarlo en éste campo. Para que el ruteador o switch sepa el tipo de encabezado que está procesando, a

cada tipo de encabezado se le asignó un número y una abreviatura, las cuales pueden ser vistas en la tabla de la figura 2.6.

Valor decimal	**Abreviatura (keyword)**	**Descripción**
0	HBH	Opciones entre saltos
4	IP	IP en IP (encapsulación en IPv4)
5	ST	Stream
6	TCP	Transmisión Control Protocol
17	UDP	User Datagram Protocol
51	AH	Authentication Header
52	ESP	Encrypted Security Payload
59	NULL	No Next Header
60	DO	Destination Options Header
194	JBGR	Jumbogram

Fig. 2.6: Muestra de algunos valores para los tipos de encabezado en IPv6

El campo de alcance del datagrama mide 8 bits es parecido al campo de *time to live* en la versión 4 e indica la cantidad máxima de ruteadores que debe pasar el datagrama antes de llegar a su destino, igualmente, cada vez que pasa por un ruteador se decrementa el valor inicial en uno y si no llega a su destino y el valor llega a cero, se descarta el datagrama.

Una pequeña observación a raíz de éste último campo en la encabezado IP, es curioso que con el aumento de direcciones todavía se siga pensando que para llegar de un origen a un destino, el datagrama no va a tener que pasar por más de 255 ruteadores (2^8), los renovadores de la versión piensan que hay maneras de recortar los recorridos y es muy difícil crear una ruta que cubra más de 255 ruteadores.

2.2.1.- Encabezados del protocolo IP versión 6

El encabezado de IPv6 no contiene opciones a diferencia de la versión 4, sin embargo las opciones son necesarias para dar indicaciones a los ruteadores como tratar a los datagramas. No todos los datagramas que circulan por Internet contienen datos de los usuarios, también hay mensajes de *status* que informan la saturación de la red, rutas perdidas etc.

Por medio de éstos encabezados se pueden dar ordenes muy específicas de cómo tratar el datagrama en el caso de medir un enlace o tener mucha confianza de un enlace que sea nuestro enlace primario, también en casos de enlaces de seguridad, los cuales se necesita que pasen por rutas específicas.

La manera de lograr ésto es indicar en el *next header* el número correspondiente al encabezado a colocar tras el datagrama, así el ruteador sabe que ántes de encaminar el datagrama tiene que tomar en cuenta la información extra del siguiente encabezado.

2.2.1.1.- El encabezado de enrutamiento

Tiene la misma función de la versión 4, a los cuatro bytes que la forman se le agregan varias direcciones de 128 bits que son los ruteadores por los que necesariamente tiene que pasar el datagrama ántes de llegar a su destino, su formato se puede ver en la figura 2.7:

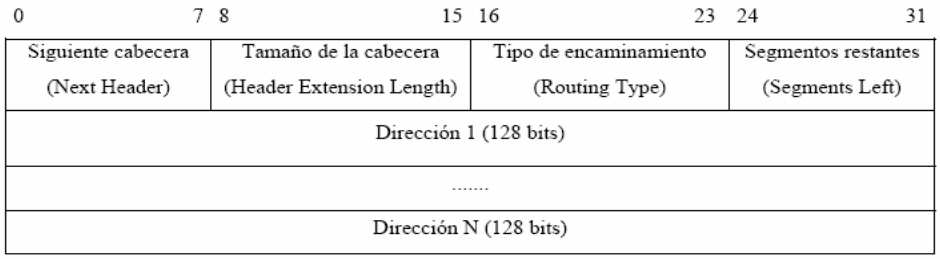

Fig. 2.7: Encabezado de enrutamiento

- El primer campo es de siguiente encabezado ya que se pueden encadenar varios encabezados además de éste.
- El segundo campo es el tamaño del encabezado y es el tamaño del encabezado en palabras de 64 bits, incluye todas las direcciones que se hayan especificado.
- El tercer campo es el tipo de enrutamiento que es la politica que se debe seguir en el enrutamiento, aunque actualmente solo existe el tipo 0, el cual especifíca si el ruteador está en la lista de direcciones, si existe, se quita de la lista, se decrementa el campo de segmentos restantes y busca en la lista cual es el ruteador mas cercano para mandarle el datagrama, si no está en la lista, el ruteador solamente encamina el datagrama ignorando ésta opción.
- El cuarto campo es el de número de segmentos restantes y es un número que indica el número de direcciones de enrutamiento que aun faltan, es decir, cuando éste número llega a cero significa que el datagrama ha llegado a su destino.

2.2.1.2.- El encabezado de fragmentación

Es de gran ayuda en ésta versión del protocolo ya que en la versión anterior no existía un encabezado o un bit de fragmentación y cuando un datagrama llegaba a un ruteador que no lo podía manejar, éste lo fragmentaba y enviaba el mismo datagrama pero fragmentado, si en el camino se perdía alguno de los fragmentos que enviaba el ruteador, se tenía que reenviar todo el datagrama completo, en éstos casos el ruteador generaba mas tráfico en la red y no conviene retransmitir todo un datagrama por un fragmento mínimo que no llegó.

Para ésta versión lo que realiza el protocolo es que en el caso de recibir un datagrama mayor a lo que puede transmitir, lo descarta y envía un datagrama de ICMP al emisor. Sin embargo, para estos problemas existe el encabezado de fragmentación, para que dicha fragmentación se haga en el emisor y no en los ruteadores y los adecúe a las necesidades de los ruteadores, de acuerdo a su MTU.

El primer campo es el de *next header* y especifica el siguiente tipo de encabezado que hay, en el caso de que lo haya, el siguiente campo está reservado y no se utiliza por el momento, después sigue el campo de desplazamiento de fragmento e indica los 13 bits más significativos del desplazamiento, ésto porque la fragmentación se hace en múltiplos de 64, los siguientes 2 bits se han reservado para usos futuros y finalmente el último bit es el más importante ya que indica si hay más fragmentos, si hay mas fragmentos su valor es uno y si no hay mas fragmentos que le sigan, su valor es cero. En la figura 2.8 se puede ver el formato del encabezado.

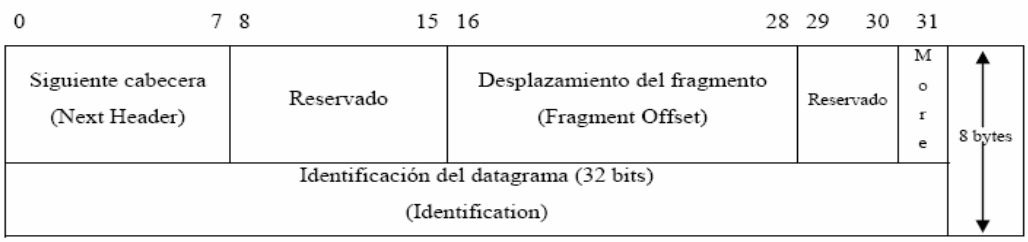

Fig. 2.8: Encabezado de fragmentación de datagramas

2.2.1.3.- El encabezado de opciones de destino

Permite añadir opciones a los datagramas para que sean procesadas por el destinatario, así, si no necesitamos que el ruteador pierda tiempo de procesamiento en leer datos innecesarios, los podemos colocar en éste encabezado.

El primer campo es necesariamente el de *next header* por lo mismo que en las ocasiones anteriores, a continuación está el campo de tamaño del encabezado de 8 bits el cual dice cual es el tamaño del encabezado en palabras de 64 bits sin tomar en cuenta los primeros 64 bits, con esto el valor de éste campo puede ser cero, si el valor fuera diferente a cero, todos los ruteadores por los que pasa tendrían que verificar el campo para ver que sea cero, gastando tiempo de procesador en el ruteador, el último campo de opciones es para el destinatario, pero su formato obliga a que sean palabras de 64 bits, para que sean especificadas en el tamaño del encabezado. En la figura 2.9 se puede ver el formato del encabezado.

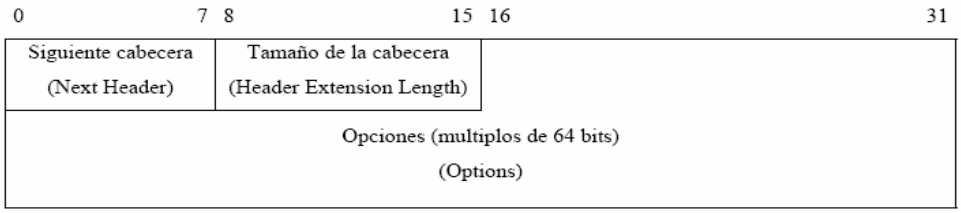

Fig. 2.9: Encabezado de opciones de destino

2.2.1.4.- El encabezado de opciones entre saltos

Permite especificar las opciones que queremos que procesen los ruteadores intermedios, tiene el mismo formato que el encabezado de opciones de destino, la pequeña diferencia es que solamente va a ser interpretado por el destinatario del datagrama.

2.2.1.5.- El encabezado de autenticación

Es una de las mejoras importantes que se mencionaron anteriormente ya que éste encabezado debe estar entre el encabezado IP y los datos del datagrama, no cambia en nada como manejan los datos los protocolos superiores, lo que realiza es proporcionar una seguridad intrínseca en el origen del datagrama, por lo tanto, en cuanto los protocolos de orden superior reciban un datagrama sin la correspondiente autenticación, lo deben desechar.

Después tenemos el campo de tamaño de los dato, el cual se especifíca en palabras de 32 bits, posteriormente un campo de 16 bits que está reservado y su valor debe de ser cero, después tenemos el campo de indice de parámetros de seguridad y el campo de número de secuencia, cada uno de éstos campos ocupa 32 bits, al final está el campo de datos de autenticación, éste es un campo de longitud variable. El formato del encabezado se puede ver en la figura 2.10:

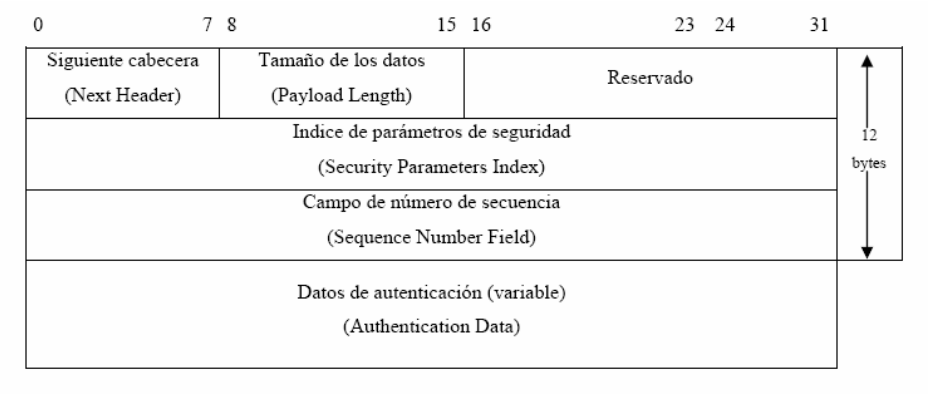

Fig. 2.10: Encabezado de autenticación de la versión 6

Los datagramas pueden tener más de un encabezado, la teoría comenta que no se deben de tener problemas con eso ya que los ruteadores procesan cada encabezado a medida de que van leyendo el datagrama, sin embargo hay encabezados con más importancia que otros ya que por ejemplo el encabezado de autenticación puede hacer que todo un datagrama sea descartado, por lo tanto debería de ir antes que las demás, también el encabezado de fragmentación, ya que sin éste el destinatario o el ruteador no sabría como reensamblar los datagramas, a continuación se coloca una tabla con el orden de los encabezados dependiendo de su importancia, que recomiendan varios autores: [Ver00].

1. Encabezado IP versión 6 (IPv6 Header).
2. Encabezado de opciones entre saltos (Hop-by-hop Options Header).
3. Primera encabezado de opciones de destino (Destination Options Header).
4. Encabezado de enrutamiento (Routing Header).
5. Encabezado de fragmentación (Fragment Header).
6. Encabezado de autenticación (Authentication Header).
7. Segunda encabezado de opciones de destino (Destination Options Header).
8. Encabezado de protocolo de nivel superior (TCP, UDP...).

Cualquiera de los encabezados de opción, como lo dice su nombre, no es imprescindible, es decir puede que no exista un encabezado de opciones entre saltos pero si una de opciones de destino, cabe mencionar que los autores repiten el encabezado de opciones de destino

porque si se necesitan enviar datagramas encapsulados y se desea que se utilicen las opciones por los ruteadores intermedios, se deben de enviar las opciones ántes del enrutamiento, también si queremos que la información sea interpretada solo por el destinatario, se deben colocar las opciones justo antes del encabezado del protocolo del nivel superior.

2.2.2.- ICMP y los mensajes de error

El objetivo del *Internet Control Message Protocol* es el de enviar mensajes entre equipos, éste protocolo ya se utilizaba en la versión 4 de IP, pero para ésta versión ha sufrido un poco de cambios, se puso un formato fijo que es más fácil de manejar por los ruteadores, se le aumentó la capacidad en las direcciones a 128 bits y se quitaron mensajes redundantes o que no se utilizaban. En la figura 2.11 se detalla el formato del encabezado ICMP versión 2, que es el compatible con IPv6:

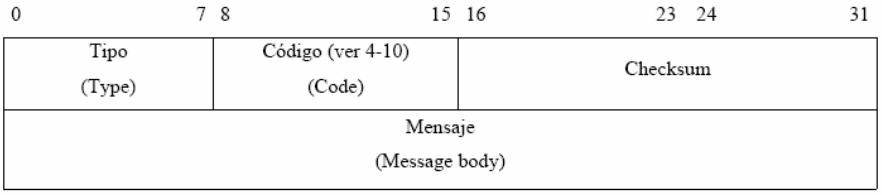

Fig. 2.11: Formato del ICMP versión 2 compatible con la versión 6 de IP

Codigo	**Significado**
1	Destino inalcanzable (Destination Unrechable).
2	Paquete demasiado grande (Packet too big).
3	Tiempo de respuesta agotado (Time Exceded).
4	Parámetros incorrectos (Parameter Problem).
128	Solicitud de ECHO (ECHO Request).
129	Respuesta a ECHO (ECHO reply).
133	Solicitud de ruteador (Ruteador Solicitation).
135	Solicitud de vecino (Neighbor Solicitation).

Fig. 2.12: Tabla con los códigos más relevantes del ICMP versión 2

- El campo código se apega a la tabla en la figura 2.12 para indicar que tipo de mensaje es enviado.
- En éste caso el campo tipo es la versión del protocolo ICMP, cuando es para IPv4 es 1 y cuando es para IPv6 es 2.
- El campo *checksum* es como en todos los casos una suma de control para saber si el campo llega completo o se pierden datos en el camino y descartar el datagrama.
- El campo de mensaje es el que tiene los datos que se le pasan al destinatario, éste campo es de longitud variable.

El que se envíe un mensaje de ICMP por parte de un ruteador hacia quien envió el datagrama, significa que el ruteador descartó un datagrama, los cuatro primeros tipos de código del mensaje dicen los motivos por los cuales el datagrama fue descartado, tal como lo muestra la tabla en la figura 2.11.

Cuando se pierden datagramas que van a varios usuarios el ruteador responde al originador del mensaje con un solo mensaje ICMP para evitar avalanchas de mensajes, el ruteador no contesta mensajes ICMP para evitar que tengamos solamente mensajes de error rondando por la red.

Cabe mencionar que cuando ICMP manda un mensaje de error 2 (datagrama demasiado grande) se puede generar en cualquiera de los ruteadores en el camino hacia el destino del paquete, es decir, cualquier ruteador de internet en el camino que ocupe el paquete puede

mandar ese mensaje de acuerdo a su MTU, pero en cuanto se pasa por todos los ruteadores la transmisión de datos se agiliza enormemente, optimizando la transmisión de los datos.

2.2.3.- Impacto en los protocolos superiores

Al hacer un cambio en la versión IP de 4 a 6 es importante notar que es lo que pasa con los protocolos arriba de IP como TCP o UDP, sin embargo, desde la estructura de encapsulamiento utilizada en la versión 4, los protocolos superiores están separados del encabezado IP.

Sin embargo se ha creado un pseudo-encabezado para TCP y UDP, el cual amplía las direcciones a 128 bits y mantiene la filosofía de mantener los formatos de tamaño fijo para que los ruteadores los puedan manejar más fácilmente. En la figura 2.13 se puede ver la estructura de un pseudo-encabezado de UTP y TCP.

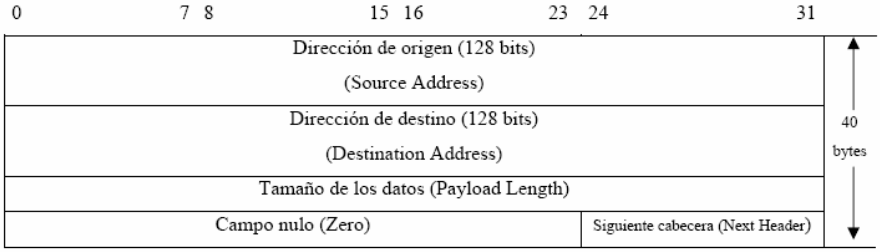

Fig. 2.13: Pseudo-encabezado para TCP y UDP compatible con la versión 6 de IP

En éste pseudo encabezado se puede observar al cambio de las direcciones a 128 bits, que es el cambio primordial del encabezado.

La dirección de origen, es la dirección de donde se está mandando el paquete, la dirección destino es a donde se va a enviar dicho paquete, el tamaño de los datos incluye tanto los

posibles encabezados que se encuentren después de éste pseudo-encabezado como los datos que se están enviando, después hay un campo de 24 bits que no se utiliza y debe de ser cero, finalmente se especifica el siguiente tipo de encabezado que hay en la cadena, como se vio anteriormente se pueden tener varios encabezados encadenados.

En el pseudo-encabezado se ha eliminado el campo de *checksum*, esto es debido a varias observaciones de la versión anterior de IP, las cuales son:

1. En las versiones de encabezados anteriores el *checksum* se utilizaba para verificar el encabezado, lo cual descartaba errores en los datos, éstos no se incluían en el *checksum*.
2. Cada vez que un datagrama pasa por un ruteador, el tiempo de vida se disminuye en uno, por lo tanto se tiene que hacer un nuevo *checksum*, y si queremos aumentar la velocidad en el manejo de paquetes en los ruteadores se tiene que eliminar ésta práctica.
3. Las redes que actualmente se manejan como Ethernet, FDDI, ATM, etc. ya incluyen dentro de sus especificaciones un *checksum* de comprobación, por lo tanto las mismas redes ya proporcionan seguridad en el manejo de los datos.
4. Por ultimo los protocolos TCP y UDP ya incluyen un *checksum* y el incluir otro en el encabezado sería redundante.

2.2.4.- Datagramas que superan los 64K (Jumbogramas)

Una mejora interesante y con visión a futuro de IPv6 es la capacidad de manejar cantidades de datos superiores a los 64K, en éstos momentos no se utiliza porque las redes actuales no

pueden manejar más de 64K pero lo interesante es ver como ya se planea a futuro su manejo, en la figura 2.14 se puede ver el formato del encabezado de un jumbograma.

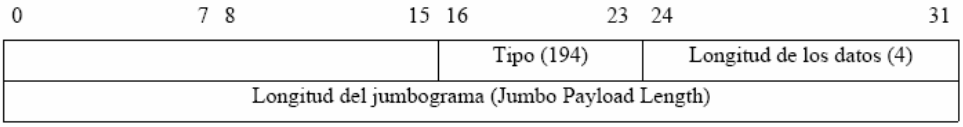

Fig. 2.14: Encabezado de un jumbograma

El manejo de los datos está dado por 16 bits (2^{16} = 65536 = 64K), con lo que el tamaño máximo es de 64K, se deja ese tamaño actualmente para su fácil manejo por parte de los ruteadores. Sin embargo para que poder enviar y recibir datagramas de más de 64K, todos los ruteadores por los cuales va a pasar nuestro datagrama lo deben aceptar, y actualmente eso no pasa.

En los foros de Internet y en la IETF, el uso de los jumbogramas ha sido ampliamente discutido y finalmente aceptado por su poca probabilidad de uso a corto plazo.

La discusión es por el principio de transmisión de datos cortos, ya que si enviamos N bytes de información y solo un bit se pierde en el camino, se tiene que reenviar todo el paquete, si se tienen paquetes grandes, se reenviarán paquetes grandes, al enviar paquetes cortos, se reenviarán paquetes cortos sin causar tanto tráfico en la red.

La forma de especificar un jumbograma en el datagrama IP es poniendo en el tamaño de los datos cero (0) y usar los encabezados encadenados de la versión 6 de IP, el encabezado de jumbograma deberá ser procesada por todos los ruteadores intermedios, así se tienen 32 bits

para la especificación del tamaño del datagrama (2^{32} = 4,294,967,296 = 4 Gb). Como observación, en la tabla de la figura 2.15 se pueden ver los MTUs de diferentes tipos de redes actuales.

Tipo de red	**Tamaño máximo de transacciones (MTU)**
ATM	8192 bytes (para TCP/IP)
Comunicaciones punto a punto (PPP)	296 bytes
X.25	576 bytes
IEEE 802.3/ 802.2	1492 bytes
Ethernet	1500 bytes
FDDI	4352 bytes
Token Ring	4464 bytes
Fast Token Ring	17914 bytes
Hyperchannel	65535 bytes

Fig. 2.15: Tamaño máximo de datos (MTU) de las redes más utilizadas actualmente

2.2.5.- Direccionamiento en IP versión 6

Una de las principales razones del cambio de IPv4 a IPv6 es la falta de direcciones IP en su versión 4, por lo tanto para la versión 6 se hizo un esfuerzo bastante grande por que no vuelva a pasar lo mismo pasando de direcciones de 32 bits a direcciones de 128 bits, sin embargo, hubiera sido muy fácil solamente aumentarle bits a las direcciones de la versión 4 para tener más direcciones, pero, al tener tantas direcciones, el problema sería el enrutamiento a través de Internet. Para el caso de IPv6 se definieron tres tipos de direcciones:

1. **Unicast.** Este grupo de direcciones se caracteriza por identificar un único punto final de destino. Un datagrama enviado a una dirección “unicast” será entregado a un solo punto de destino.
2. **Multicast.** Las direcciones “multicast” agrupan un conjunto de puntos finales de destino. Un datagrama enviado a una dirección “multicast” será entregado a un conjunto de destinos que forman parte de un mismo grupo.
3. **Anycast.** Este grupo de direcciones al igual que el “multicast” agrupa un conjunto de puntos finales de destino. La diferencia principal con el “multicast” está en el sistema de entrega de datagramas.

En la versión 6 de IP las direcciones de 128 bits se representan por 8 grupos de 16 bits cada uno, para que la representación sea más compacta, se utiliza la notación hexadecimal.

Sin embargo, como son representaciones bastante largas, por ejempo, 3FFE:3326:FFFF:FFFF:FFFF:FFFF:FFFF:0001, para hacer referencia a 140.148.10.1 o www.algo.com.mx, lo que se hizo fue recalcar en el uso de los nombres para los usuarios ya que es mucho más fácil de recordar, de cualquier manera, también se acordaron maneras de compactar las direcciones:

1. Todos los ceros a la izquierda que sean redundantes podrán ser eliminados.
2. Si hay varios ceros consecutivos (mas de 4) se podrán simplificar por medio de “::”. Cabe mencionar que solamente se podrá hacer una vez dentro de la misma dirección.
3. En el caso de direcciones IPv4 que pasen por ruteadores IPv6 podrán seguir con su formato, añadiendo ceros a la izquierda, es decir, una dirección 10.0.0.1 se

convertiría en 0:0:0:0:0:0A001 pero se podrá manejar en su formato decimal ::10.0.0.1.

4. Las especificaciones de un prefijo en la versión 6 se harán por la forma dirección_ipv6/prefijo, se debe de tener mucho cuidado cuando se ponen prefijos ya que puede haber confusiones, por ejemplo, si tenemos el prefijo de 40 bits FEDC:BA98:76 en la dirección FEDC:BA98:7600::1 se especificará como FEDC:BA98:7600::1/40, no es lo mismo que tener un prefijo de 64 bits entre FEDC:BA98:0: que la dirección FEDC:BA98:0.

Es un poco rebuscado pero para ejemplificarlo en la figura 2.16 se verá más a detalle, esto puede aclarar un poco más la simplificación de direcciones:

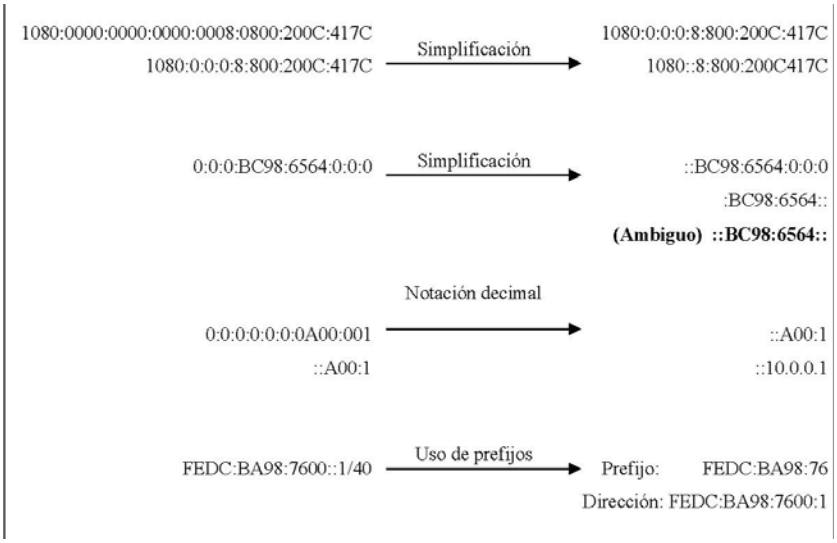

Fig. 2.16: Simplificación de direcciones IPv6

Para el caso de IPv6 las direcciones se particionaron en subgrupos independientes las direcciones de 128 bits, así se reservaron algunos para uso futuro o ampliación de los ya establecidos, por ejemplo, se reservaron prefijos de direcciones para grupos específicos de

direcciones compatibles con NSAP o IPX que puede ser que a futuro necesiten un rango de direccionamiento específico.

Grupo asignado	**Prefijo**	**Fracción del espacio ocupado**
Reservado	0000 0000	1/256
No asignado	0000 0001	1/256
Direcciones NSAP	0000 001	1/128
Direcciones IPX	0000 010	1/128
No asignado	0000 011	1/128
No asignado	0000 1	1/32
No asignado	0001	1/16
No asignado	001	1/8
Direcciones globales unicast	010	1/8
No asignado	011	1/8
Direcciones geográficas unicast	100	1/8
No asignado	101	1/8
No asignado	110	1/8
No asignado	1110	1/16
No asignado	1111 0	1/32
No asignado	1111 10	1/64
No asignado	1111 110	1/128
No asignado	1111 1110 0	1/512
Direcciones locales (Link Local)	1111 1110 10	1/1024
Direcciones locales (Site Local)	1111 1110 11	1/1024
Direcciones Multicast	1111 1111	1/256

Fig. 2.17: Distribución inicial del espacio de direcciones en la versión 6 de IP

También se ha reservado un rango de direccionamiento para un posible direccionamiento geográfico, si se hace eso a un corto plazo, no será necesario preocuparse por la falta de direccionamiento nuevo y migrar a una nueva versión de IP ya que con todo el direccionamiento ya asignado y el que se piensa asignar a corto plazo, queda el 70% libre para futuras asignaciones.

En la tabla de la figura 2.17 se puede ver la tabla de direccionamiento actual, se puede observar que muchos rangos están sin asignar, por lo que se mencionaba anteriormente.

2.2.5.1.- Direcciones “unicast”

Las direcciones “unicast” son aquellas direcciones en las que se especifica un solo punto final en la comunicación, como una sola tarjeta de red, sin embargo, existen cinco subtipos de direcciones especiales:

1. La **dirección no especificada** está compuesta por 16 bytes en cero (0:0:0:0:0:0:0:0) y sólo puede utilizarse como dirección inicial mientras se recibe una dirección fija. También puede utilizarse para funciones internas que requieran la especificación de una dirección IP.
2. La **dirección interna** se define como 15 bytes en creo y un byte con el último bit uno (0:0:0:0:0:0:0:1). Esta dirección es interna y no puede circular por la red o ser dirección de origen o destino de un datagrama. Su uso es para las computadoras que no tengan una conexión de red y quieran simular el comportamiento de conexión a una red mediante una dirección que no saldrá de la propia computadora.
3. **Direcciones tipo IP versión 4** son las direcciones que se obtienen poniendo un prefijo de 96 ceros a una dirección IP versión 4 (por ejemplo 10.0.0.1 cambia en la versión 6 a ::10.0.0.1).
4. **Direcciones locales reservadas** son direcciones reservadas para *intranets*. Estas direcciones no son válidas en Internet y sólo sirven para que una organización o empresa pueda crear una organización de sus redes basada en un esquema TCP/IP sin la necesidad de estar conectados a Internet (en la versión 4 de IP, existen

diferentes clases reservadas para este mismo fin, como por ejemplo 192.168.XXX.YYY)

5. Las **direcciones de inicialización locales reservadas** son direcciones que pueden utilizar los equipos conectados a una misma red local mientras se inicializa y no tiene asignada una dirección IP. La diferencia con la dirección no especificada (0:0:0:0:0:0:0:0) es que la dirección de inicialización local si puede circular por la red, permitiendo por ejemplo obtener el sistema operativo de un servidor en la misma red. Esta característica ya existe en la versión 4 del protocolo IP, que actúa conjuntamente con los protocolos ARP y RARP. Estas direcciones se construyen con el prefijo FE80::/10 y 64 bits que representan la *MAC Address* de la tarjeta de red.

2.2.5.2.- Direcciones “multicast”

Las direcciones “multicast” son el reflejo del uso de las direcciones clase D en IPv4, viendo que su uso era extenso y que las aplicaciones valían la pena, se decidió ponerlas en la versión 6.

Se caracterizan por ser comunes a un grupo de equipos, es decir que la misma dirección se comparte con todos los equipos del grupo, así que un datagrama enviado a ésta dirección, se repartirá en todos los equipos. Las direcciones se forman con el prefijo:

FFXY:ZZZZ:ZZZZ:ZZZZ:ZZZZ:ZZZZ:ZZZZ:ZZZZ/16.

“X” son 4 bits que sirven de bandera en donde se especifican varias opciones, por el momento los tres primeros bits de los 4 están reservados y deben de ser 0, el cuarto

denominado transitorio solamente especifica si la dirección es local, y cuando termina la comunicación debe de ponerse en cero otra vez, sin embargo si la dirección es fija se debe de conservar en uno.

“Y” también son 4 bits, pero éstos definen el alcance de la comunicación para definir rangos en la comunicación y no enviar datagramas a Internet, solamente se envian a Internet lo que necesita salir de la *intranet*.

“Z” son 118 bits los cuales determinan el identificador del grupo, también componen el cuerpo de la dirección de red. En la figura 2.18 se puede ver el formato de una dirección “multicast”.

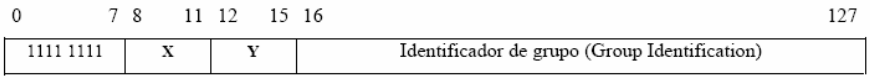

Fig. 2.18: Formato de una dirección de tipo “multicast”

2.2.5.3.- Direcciones “anycast”

El tipo “anycast” es un nuevo tipo de direccionamiento incluido en la versión 6 de IP, debido a su novedad está en fase experimental, a diferencia de las direcciones “multicast” el datagrama no se entrega a todos los equipos del grupo, sino que se entrega al equipo más cercano al orígen del datagrama.

El formato de éste tipo de direcciones es muy sencillo ya que toda la carga la lleva el sistema de enrutamiento, así, para cada ruteador debe de guardar solamente cual es el equipo más cercano del grupo especificado y cuando recibe un mensaje “anycast”,

solamente comprobar la existencia del equipo en su tabla o enrutarlo normalmente. En la figura 2.19 se puede ver el formato de una dirección “anycast”.

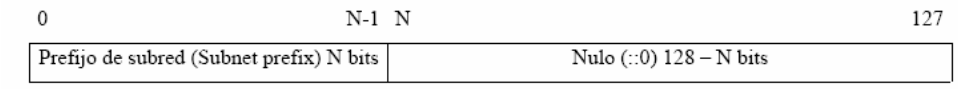

Fig. 2.19: Formato de una dirección de tipo “anycast”

2.3.- NAT en IPv6

Para comenzar, es necesario mencionar la nomeclatura que Cisco hace en la diferencia entre las direcciones IP que se manejan en la red interna y las que tienen acceso a la Internet, es decir, la *intranet* y la Internet, las direcciones utilizadas para la *intranet* se denominan locales y las de acceso a la Internet se denominan globales. Las direcciones locales son únicas en cada empresa pero otra empresa puede tener las mismas direcciones sin causar conflictos en la Internet, las direcciones globales son únicas en la Internet.

Muchos de los problemas que existen actualmente en el *backbone* de la Internet ya están afectando a los usuarios finales y a las empresas que utilizan el direccionamiento IPv4, cuando una empresa no puede resumir sus direcciones, las tablas de ruteo se pueden expandir demasiado, si la empresa no puede tener direcciones globales en la Internet, puede ser forzada a generar direcciones locales, direcciones que no se pueden ver en la Internet, solamente en la *intranet* de la compañía. [WWW58].

Los usuarios con direcciones locales, limitan su acceso al mundo por medio de los *gateways* o los traductores de direcciones de red (*Network Address Translators*, NAT). Los

servicios de NAT están hechos para permitir que una empresa que tiene direcciones IP locales pueda tener acceso a la Internet por medio de pocas direcciones IP globales independientemente de la estructura de red que tenga.

Los NATs se ubican generalmente entre la salida a la Internet de la compañía y la *intranet* de la compañía, para convertir direcciones locales en direcciones globales y así acceder a la Internet como se puede ver en la figura 2.20. Éstas direcciones no tiene que ser la misma cantidad que utiliza la *intranet*, es decir, la cantidad de direcciones locales no tiene que ser igual al número de direcciones globales, por lo regular las direcciones globales son mucho menos que las locales.

NAT es apropiado en las empresas u organizaciones que por lo regular necesitan acceder a la Internet, pero no necesitan que todos sus equipos estén conectados a la Internet, para esas empresas se recomienda el uso de NAT, pero no en exceso ya que si el uso de NAT es demasiado, se puede crear un cuello de botella en la salida y entrada de paquetes desde la Internet. El cuello de botella se crea por la dificultad de integrar y sincronizar varios equipos con direcciones locales a sus respectivas direcciones globales y viceversa.

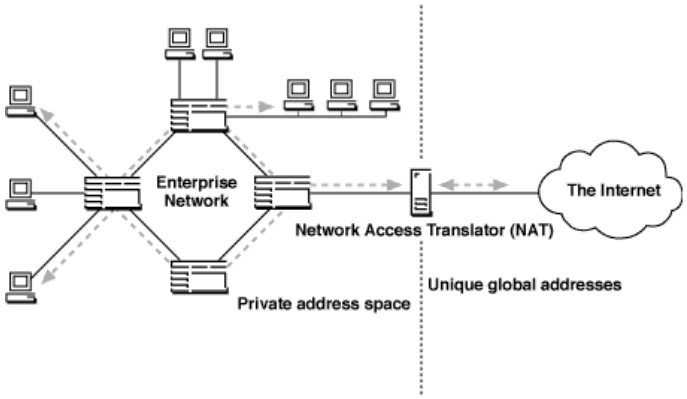

Fig. 2.20: Network Address Translator

Los traductores NAT también pueden causar problemas cuando las aplicaciones capturan su dirección IP en el *packet payload* encima de la capa de red. Éste es el caso de algunas aplicaciones con FTP y el proceso de registro de Windows 95 y NT *Windows Internet Name Service* (WINS).

Solamente que el NAT pudiera encapsular todos los paquetes desde la capa de aplicación, no hay manera de traducir direcciones capturadas, lo cual puede causar errores en la aplicación.

NAT también puede ser vulnerable a fallas en el DNS que funciona arriba de la capa de red, los servicios de NAT pueden ser de utilidad en varios escenarios, pero no se puede promover el uso de NAT como un substituto de las bondades que nos provee IPv6.

El incremento masivo de direcciones que provee IPv6 reduce la necesidad de NATs, debido a que los NATs fueron creados para evitar el consumo masivo de direcciones IPv4, lo más probable es que no sean necesarios en IPv6. [WWW58].

Aunque NAT provee beneficios para los usuarios finales, complican el uso de aplicaciones *End to End* (E2E), sin NAT las aplicaciones como videoconferencias y voz por IP (VoIP) serían más fáciles de implementar ya que se tendría conexión directa entre equipos (IP a IP), la cual podría ser iniciada por cualquiera de los dos *hosts* sin la necesidad de traducciones intermedias por un NAT.

El papel primordial de NAT no es aumentar la cantidad de accesos de direcciones locales a Internet por medio de su traducción a direcciones globales, el aspecto primario de NAT es la seguridad.

NAT proporciona un aspecto de anonimidad dentro de la Internet, es decir, al tener direcciones globales, cualquier persona en la Internet podría saber tu dirección IP y así tener problemas de seguridad en el equipo o en los ruteadores de la empresa, sin embargo, al aplicar un NAT a los mismos, los usuarios conectados a la Internet solamente podrían ver la dirección global, que no está ligada específicamente a un equipo ya que es variable, dependiendo de las que estén disponibles, lo cual agrega un tipo de seguridad a las redes que tienen NATs.

NAT indirectamente provee una capa de seguridad a la red local al hacer inaccesible la dirección IP local a la red pública de la Internet. Sin embargo cuando nuestra red sea atacada todos los intentos de violarla serán por medio del ruteador NAT, tal como los *firewalls* esto provee seguridad ya que es un solo punto de acceso a nuestra red y es el que debe de estar bien protegido, y está por demás decir que un ruteador es mucho más seguro que una PC conectada directamente a la Internet. La configuración de nuestra red local por medio de un ruteador y su acceso a la Internet por medio de un NAT también simplifica el trabajo de mantenimiento a la red, por ejemplo si se decide cambiar de proveedor de Internet, solamente la configuración de las direcciones globales cambiaría, el direccionamiento interno seguiría siendo igual.

Todos los beneficios antes mencionados se vienen abajo al comentar que NAT viola la función fundamental de las direcciones IP e Internet, que es el esquema abierto y accesible por cualquier equipo en la red. NAT tiene varias complicaciones cuando hablamos de VoIP, por ejemplo cuando tratamos de hacer una llamada dentro de una red con NAT.

Hay tres tipos de NAT, NAT estático, NAT por medio de un *pool* y NAT a nivel de puertos (PAT). El NAT estático es el mas sencillo de implementar, cada dirección local está ligada a una dirección global. El NAT por medio de un *pool* define un *pool* de direcciones globales, las cuales se asignan dinámicamente cuando una dirección local necesita acceder a la Internet. PAT hace un mapeo de varias direcciones locales a una sola dirección global pero con un puerto TCP diferente cada una, el puerto lo selecciona el servidor de NAT.

En teoría, NAT no es necesario en IPv6 debido a la cantidad tan grande de direcciones IP disponibles, sin embargo, tomemos un caso práctico para denotar el uso de NAT en IPv6. Tomemos 2 empresas con redes de gran tamaño, las cuales se van a juntar, ambas empresas han crecido desde redes pequeñas hasta las redes grandes, ambas se basan actualmente en direccionamiento IPv4, las cuales son direcciones locales, no globales.

El combinar ambas empresas en una sola estructura de red podría tener un alto costo en reestructuración de esquemas de ruteo, direcciones en los *hosts*, dominios, áreas, protocolos de ruteo externo, etc.

Este escenario es muy común hoy en día, no solo en empresas grandes sino también en empresas externas integradas a una red que no es de su propiedad. Sin embargo, por medio de IPv6, se pueden solucionar los problemas. [WWW58].

La tarea de unir las dos redes de las dos empresas dentro de un solo dominio autónomo de red es un proceso caro y potencialmente engorroso. Para evitar el costo del cambio y redireccionamiento así como el cambio de equipos, las empresas pueden optar por una solución por medio de NAT, en éste caso NAT podría permitir que las dos empresas mantengan sus redes internas en una solución no tan elegante pero si efectiva.

Para lograr ésto NAT debe de realizar una traducción de direcciones para todos los paquetes que se mueven entre las dos empresas. Desafortunadamente la solución incorpora todos los problemas de NAT, incluyendo el desempeño y los cuellos de botella al intercambiar mucha información entre las diferentes redes, el no estar estandarizado y la dificultad inherente en sitios seguros al integrarse a la Internet.

En contraste con NAT, IPv6 provee una solución robusta orientada a crecimiento futuro para la integración de ambas empresas. Para el mejor manejo del ejemplo llamaremos a las empresas, empresa A y empresa B.

El primer paso es determinar cuales *hosts* necesitan acceder ambos lados de la red en la nueva organización, estos *hosts* serán equipados con un *dual stack* IPv4/IPv6, lo que les permitirá conectividad con la red IPv4 original y participar de la nueva red lógica IPv6 que

será creada sobre la infraestructura física de la red IPv4 original como se puede ver en la figura 2.21.

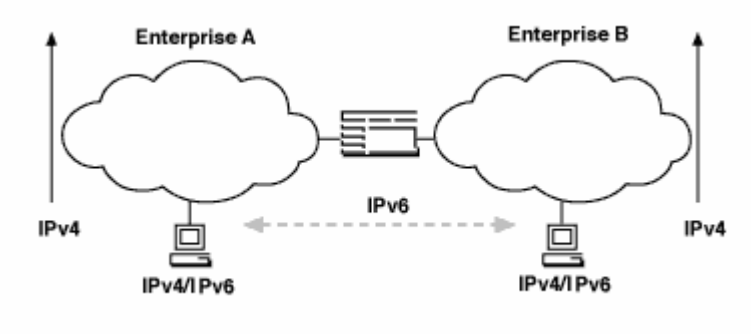

Fig. 2.21: Unión de las dos redes por medio de IPv6

El único requerimiento para la conectividad de IPv6 es que los ruteadores adyacentes a los usuarios de ambas redes deben de ser migrados a IPv6 o su IOS migrado a una versión que soporte IPv6, en donde la conexión IPv6 punto a punto pueda ser realizada.

En éste paso es cuando aplica NAT para hacer la traducción de direcciones IPv4 a direcciones IPv6, siendo las direcciones IPv4 locales y las direcciones IPv6 globales, se puede emplear cualquiera de las técnicas de *tunneling* de IPv4/IPv6.

2.4.- Métodos de transición

Para la mayoría de los usuarios en las empresas actualmente, su necesidad de conectividad radica en el acceso a las bases de datos, el correo electrónico y aplicaciones en servidores locales, en éste caso sería bueno empezar migrando a IPv6 grupos de trabajo en islas y departamentos y después ir migrando poco a poco los ruteadores del *backbone* a medida de que vayan creciendo los usuarios con IPv6. [Cis04].

El desarrollo del protocolo IPv6 es más completo para ruteadores exteriores que para ruteadores del *backbone*, así que es una manera elegante en la cual las empresas pueden empezar a hacer la transición a IPv6. Como se muestra en la figura 2.22, los grupos de trabajo independientes pueden migrar sus clientes y servidores a un *dual stack* IPv4/IPv6 en los *hosts* o *hosts* solo IPv6. Esto crea islas de funcionalidad de IPv6.

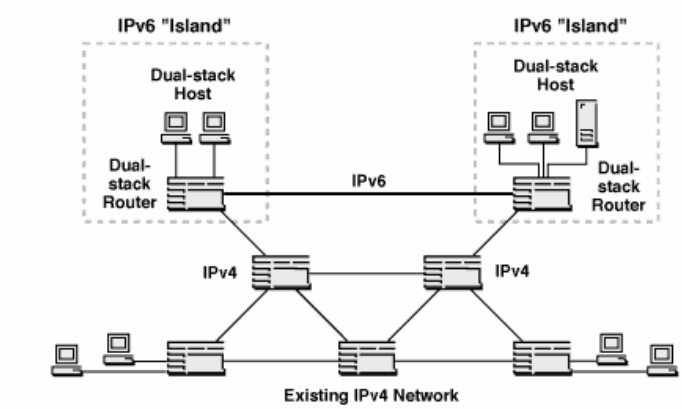

Fig. 2.22: Islas de IPv6

A medida que los protocolos de ruteo externos como *Open Shortest Path First* (OSPF) y *Border Gateway Protocol* (BGP) para IPv6 vayan madurando, el centro del backbone se puede ir desarrollando en IPv6. Después de que los primeros ruteadores IPv6 se vayan colocando, será mejor ir juntando las islas IPv6 mediante túneles de ruteador a ruteador.

En éste caso uno o más ruteadores en cada isla deberán de ser configurados como puntos finales. Cuando los *host*s utilizan la dirección de 128 bits de IPv6, los túneles se configuran manualmente para que los ruteadores que participan en los túneles sepan la dirección de punto final del túnel. Mediante direcciones IPv6 compatibles con IPv4 el *tunneling* automático y sin configuración es posible. [WWW58].

Desde el punto de vista del protocolo de ruteo, los túneles parecen un solo salto en IPv6, aunque el túnel se componga de varios saltos IPv4 a través de varios medios.

Los ruteadores corriendo OSPF pueden propagar mensajes de alcance de estado de enlaces a través de túneles así como lo harían en enlaces punto a punto convencionales, en el ambiente de IPv6, OSPF tendrá la ventaja de manejar métricas flexibles para las rutas de los túneles para asegurar que a cada túnel se le da el peso adecuado dentro de la topología.

En general, los ruteadores hacen las decisiones de envío de paquetes en un ambiente de *tunneling* de la misma manera en que tomarían decisiones de envío en una red solamente de IPv6. Las conexiones IPv4 inferiores son esencialmente transparentes para los protocolos de ruteo IPv6.

2.4.1.- El método de transición *dual-stack*

Una vez que algunos nodos se conviertan a IPv6, es posible que dichos nodos requieran interacción continua con los nodos IPv4 existentes, ésto se puede lograr mediante el método *dual-stack* de IPv4/IPv6.

Muchos de los *host*s y ruteadores actuales en su ambiente de red multiplataforma soportan múltiples componentes de *stack* de red. En primera instancia, la mayoría de los ruteadores soportan varios protocolos, así también las estaciones de trabajo corren una combinación de protocolos, los que incluyen IPv4, IPX, AppleTalk, NetBIOS, SNA, DECnet, etc.

La suma de un protocolo adicional, IPv6, en la estación de trabajo o en el ruteador, no debe de ser de mayor importancia y no debe de tomar mucho tiempo. Cuando se ejecuta un *dual-stack* IPv4/IPv6, un *host* tiene acceso a los recursos tanto de IPv4 como de IPv6, los ruteadores que ejecutan ambos protocolos pueden redireccionar el tráfico hacia los nodos finales de IPv4 o IPv6.

Las máquinas con *dual-stack*, pueden utilizar IPv4 o IPv6 independientemente, o pueden ser configuradas con una dirección IPv6 compatible con IPv4. Los nodos *dual-stack* pueden utilizar la autoconfiguración convencional de IPv4 por medio de DHCP para obtener sus direcciones IPv4. Las direcciones IPv6 pueden ser configuradas manualmente en las tablas de *host* de 128 bits o pueden ser obtenidas a través de los mecanismos de autoconfiguración dependiente del estado de IPv6, si se encuentran disponibles. Se espera que los servidores ejecuten el *dual-stack* indefinidamente, o hasta que los nodos activos se migren a IPv6.

2.4.2.- DNS IPv6

DNS es un punto que los administradores deben de considerar antes de configurar *host*s IPv6 o con *dual-stack*. Los DNS *Servers* de 32 bits no pueden manejar la resolución de nombres para las direcciones de 128 bits que maneja IPv6, para resolver éste problema, los diseñadores de IETF han definido un estándar de DNS para IPv6 (RFC 1886, *DNS Extensions to support IP version 6*), esta especificación crea nuevos registros tipo DNS de 128 bits los cuales son nombrados “AAAA”, los cuales harán el mapeo de los nombres de dominio a las direcciones IPv6.

Las búsquedas de nombres de dominio basados en direcciones de 128 bits también se definieron en el documento. Una vez que un DNS capaz de resolver direcciones IPv6 sea formado, los *host*s *dual-stack* podrán interactuar intercambiando información con nodos IPv6, si un *host dual-stack* hace un requerimiento a un DNS y reciba como respuesta una dirección de 32 bits, se utilizará IPv4, si se recibe una dirección de 128 bits, se utilizará IPv6.

En sitios donde el DNS no se ha migrado a IPv6, los *host*s deberán resolver el mapeo de direcciones a nombre manualmente a través de tablas locales configuradas manualmente.

Las aplicaciones que no accesen directamente al *stack* de la red, no tendrán que ser modificados para correr en el ambiente de *dual-stack*.

Las aplicaciones de red que interactúan directamente con IP y sus componentes relacionados requerirán de migración si van a utilizar el protocolo IPv6, por ejemplo, las aplicaciones que accesan el DNS, deberán de ser mejoradas con la capacidad de requerir los nuevos registros de 128 bits.

2.4.3.- El ruteo en redes IPv6/IPv4

Los ruteadores que ejecuten IPv4 e IPv6 al mismo tiempo deben de ser administrados casi de la misma manera en que se administran ruteadores que ejecutan solamente IPv4.

Actualmente ya existen versiones de los protocolos populares de ruteo como el OSPF y el *Routing Information Protocol* (RIP) para IPv6.

En muchos casos, los administradores elegirán el mantener la topología de IPv6 lógicamente separada de la red IPv4, aunque ambas corran en la misma estructura física, lo que permitirá que ambas sean administradas separadamente, en otros casos, puede ser ventajoso alinear las dos arquitecturas usando los mismos dominios de red, áreas, y organización de subredes.

Ambas perspectivas tiene sus ventajas y desventajas, una arquitectura separada de IPv6 puede ser utilizada para eliminar la ineficiencia en los sistemas de direccionamiento de IPv4 del cual sufren muchas empresas actualmente, una arquitectura independiente de IPv6 presenta la oportunidad de comenzar desde cero un plan de red jerárquico el cual facilitará en gran medida la conexión a uno o varios proveedores de Internet, esto provee las bases para el agregado de renumeración de ruteo y otras metas para una jerarquía de ruteo de Internet avanzada. [WWW58].

En la mayoría de las organizaciones donde se desarrolla IPv6 pausadamente, existe la posibilidad de que todos los *host*s IPv6 no tengan conexión directa entre ellos por medio de los ruteadores IPv6, en la mayoría de los casos habrá islas de topología IPv6 rodeadas por un mar de IPv4, afortunadamente los diseñadores de IPv6 han creado mecanismos de transición que permiten a los *host*s IPv6 comunicarse sobre las redes IPv4 que intervengan, la técnica esencial de éstos mecanismos es el *tunneling* de IPv6 sobre IPv4, el cual encapsula paquetes IPv6 en paquetes IPv4 como lo podemos apreciar en la figura 2.23.

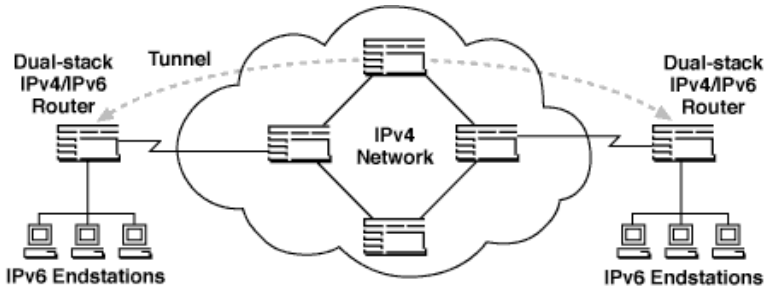

Fig. 2.23: Tunneling de IPv6 sobre IPv4

El *tunneling* permite tomar ventaja de la infraestructura existente de IPv4, sin hacer cambios a los componentes IPv4. Un ruteador o *host* con *dual-stack* en las orillas de la topología IPv6, simplemente adhiere a un encabezado IPv4 a cada paquete IPv6 y envía su tráfico nativo IPv4 a través de las ligas existentes.

Los ruteadores IPv4 reenvian éste tráfico sin conocer que envuelve a IPv6, en el otro lado del túnel, otro ruteador *dual-stack* o *host* desencapsula el paquete IPv6 y lo enruta a su destino final utilizando los protocolos estándar de IPv6.

Para acomodar las diferentes necesidades administrativas, los mecanismos de transición a IPv6 incluyen dos tipos de *tunneling*, los automáticos y los configurados. Para crear túneles configurados se define manualmente el mapeo de direcciones de IPv6 a IPv4 en los puntos finales del túnel.

En cualquiera de los dos lados del túnel, el tráfico se reenvía con direccionamiento completo de 128 bits, en el punto de entrada del túnel una tabla de ruteo es definida manualmente para decidir cuales direcciones IPv4 se usan para cruzar el túnel, esto requiere

un cierto volumen de administración manual en los puntos finales del túnel, pero el tráfico se rutea a través de la topología IPv4 dinámicamente, sin el conocimiento de los ruteadores IPv4, las direcciones de 128 bits no tienen que alinear con las direcciones de 32 bits de ninguna manera.

Otro mecanismo son los túneles automáticos. Los túneles automáticos usan direcciones compatibles con IPv4, las cuales son un híbrido entre las direcciones IPv4 e IPv6, las direcciones compatibles se crean añadiendo ceros a la izquierda a las direcciones IPv4 de 32 bits, para así volverlas de 128 bits.

Cuando el tráfico se reenvía con direcciones compatibles, el aparato en la entrada del túnel puede automáticamente direccionar el tráfico encapsulado simplemente convirtiendo la dirección compatible con IPv4 de 128 bits a una dirección IPv4 de 32 bits, en el otro lado del túnel, el encabezado IPv4 se remueve para revelar la dirección IPv6 original.

El *tunneling* automático permite a los *host*s IPv6 explotar dinámicamente las redes IPv4, pero requiere el uso de direcciones compatibles con IPv4, lo cual no brinda los beneficios del direccionamiento de 128 bits.

Los nodos IPv6 que utilizan direcciones compatibles con IPv4 no toman ventaja del espacio de dirección extendido, pero pueden explotar los otros beneficios de IPv6, los cuales incluyen etiquetas de flujo, autenticación, codificado, “multicast” y “anycast”.

Una vez que un nodo ha sido migrado a IPv6 con direcciones compatibles con IPv4, queda la puerta abierta para un movimiento casi transparente a el usar el direccionamiento IPv6 en su completa extensión, se espera que con la ayuda de un servicio de autoconfiguración de IPv6.

El utilizar direcciones compatibles con IPv4 significa que los administradores pueden agregar nodos IPv6 preservando inicialmente su direccionamiento básico y arquitectura de red.

Los túneles automáticos están disponibles si son necesarios, pero puede que no sean necesarios en los casos donde los ruteadores del *backbone* principales se migren de una sola vez para incluir el *stack* de IPv6. Esto es algo que se puede lograr rapida y eficientemente cuando los ruteadores de *backbone* soportan configuraciones completas remotas y capacidades de mejora.

La combinación de túneles, direcciones compatibles y nodos con *dual-stack* asegura que los administradores de red tendrán la flexibilidad e interoperabilidad necesaria cuando hagan el cambio a IPv6. Los servicios de transición permiten a las empresas dependientes de su red tomar ventaja de las características técnicas de IPv6. [WWW60].

El RFC 2893 define los siguientes tipos de túneles:

- Configurados
- Automáticos

2.5.3.1.- Túneles configurados

Un túnel configurado requiere la configuración manual de los puntos finales del túnel. En un túnel configurado, las direcciones IPv4 de los puntos finales del túnel no derivan de direcciones dentro de las direcciones IPv6 origen y destino o de las direcciones del siguiente salto de la ruta correspondiente. [WWW60].

Tipicamente, las configuraciones de túnel entre ruteadores se configuran manualmente. La configuración de la interfaz del túnel consiste en las direcciones IPv4 de los puntos finales del túnel, las cuales deben de ser configuradas manualmente junto con las rutas estáticas que usa la interfaz del túnel. Para crear manualmente túneles configurados para el protocolo IPv6 para la familia Windows 2003 server o XP, se usa el comando:

netsh interface ipv6 add v6v4 tunnel

Como se define en el RFC 2893, los Túneles Automáticos de IPv6 es el método que utiliza direcciones IPv6 compatibles con IPv4, por ejemplo, cuando un equipo con la dirección IPv4 157.60.91.123 envía tráfico a otro *host* con la dirección IPv4 131.107.210.49, las direcciones IPv4 e IPv6 en el encabezado se listan como se menciona en la tabla de la figura 2.24:

Campo	**Valor**
IPv6 Source Address	::157.60.91.123
IPv6 Destination Address	::131.107.210.49
IPv4 Source Address	157.60.91.123
IPv4 Destination Address	131.107.210.49

Fig. 2.24: Ejemplo de direcciones de Túneles Automáticos IPv6

Para probar la conectividad se utiliza el comando ping, por ejemplo, si el primer equipo quiere localizar el segundo equipo haría lo siguiente:

```
Ping6 ::131.107.210.49
```

El protocolo IPv6 en Windows 2003 Server y Windows XP, no utiliza direcciones compatibles con IPv4 por default, para habilitarlo se usa el comando:

```
Netsh interface ipv6 setstate v4compat=enabled
```

Cuando se habilita el protocolo IPv6 en el servidor Windows 2003 o XP, se facilita la comunicación con direcciones compatibles con IPv4 por medio de la ruta ::/96 en la tabla de ruteo IPv6 que utiliza la pseudo-interface de túneles automáticos.

Ésta ruta indica que todas las direcciones con los primeros 96 bits en cero se reenvían a su dirección destino utilizando la pseudo-interface. La pseudo-interface de túnel automático usa los últimos 32 bits de la dirección IPv6 origen y destino, los cuales corresponden a la dirección IPv4, de los paquetes de salida en IPv4.

2.5.3.2.- Túneles automáticos

Un Túnel Automático es un túnel que no requiere configuración manual. Los puntos finales del túnel se determinan por el uso de las interfáces lógicas del túnel, las rutas y las direcciones IPv6 origen y destino. El protocolo IPv6 para la familia Windows 2003 Server y XP soporta las siguientes tecnologías de túnel automático:

- *6to4*, habilitada por *default*.
- ISATAP, deshabilitada por *default*.

- *6over4*, deshabilitado por *default*.

El protocolo IPv6 para Windows XP también soporta el cliente Teredo cuando se instala Windows XP SP2 o SP1 y el paquete de red avanzado para Windows XP. Teredo se habilita por *default*. [WWW60].

2.5.3.3.- Túneles 6over4

6over4 también se conoce como el *tunnneling* “multicast” IPv4, es una tecnología de túneles automáticos ya sea de equipo a equipo, de equipo a ruteador o de ruteador a equipo, que provee conctividad “unicast” y “multicast” IPv6 entre nodos IPv6 a través de una intranet IPv4. *6over4* está descrita en el RFC 2529, utiliza prefijos válidos de 64 bits para direcciones “unicast” y el identificador de la inteface ::WWXX:YYZZ, donde WWXX:YYZZ es la representación hexadecimal de la dirección IPv4 (w.x.y.z) asignada a la interface.

Por default, los *host*s de *6over4* configuran automáticamente la dirección de enlace local FE80::WWXX:YYZZ en cada interface *6over4*.

6over4 maneja la infraestructura IPv4 como una liga simple con capacidades multicast, esto significa que el proceso de descubrimiento de vecinos como la resolución de direcciones y descubrimiento de ruteadores, trabaja como si hicieran un enlace físico con capacidades “multicast”, para emular un enlace con capacidades “multicast”, la infraestructura IPv4 debe de tener habilitado “multicast” para IPv4 como se puede ver en la figura 2.25.

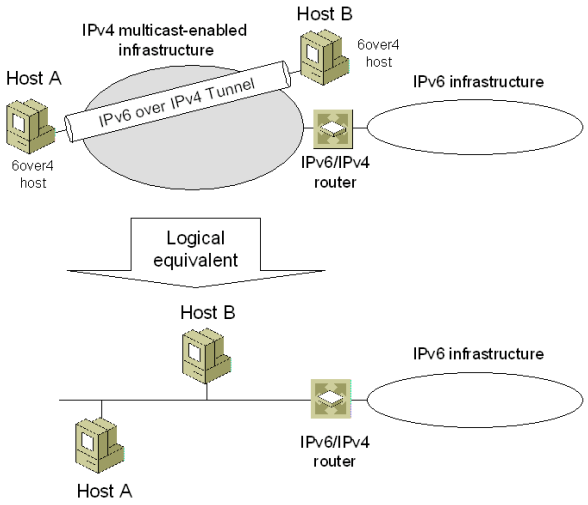

Fig. 2.25: Configuración *6over4*

Para facilitar las comunicaciones “multicast” IPv6 en una infraestructura IPv4 con “multicast” habilitado, se define en el RFC 2529 el siguiente mapeo para traducir una dirección IPv6 “multicast” en una dirección IPv4 “multicast”:

239.191.[penúltimo byte de la dirección IPv6].[último byte de la dirección IPv6]

Los siguientes son ejemplos de mapeo de direcciones “multicast” IPv6:

- FF02::1 (dirección “multicast” o de enlace local en equipos) se mapea a 239.192.0.1
- FF02::2 (dirección “multicast” o de enlace local en ruteadores) se mapea a 239.192.0.2
- FF02::1:FF28:9C5A (dirección “multicast” de un nodo solicitado de ejemplo) se mapea a 239.192.156.90

Cuando se habilita *6over4*, la capa IPv4 utiliza mensajes IGMP (*Internet Group Membership Protocol*) para informar a los ruteadores locales IPv4 de su interés en recibir tráfico “multicast” IPv4 el cual es enviado a las direcciones “multicast” IPv4.

Los equipos con *6over4* habilitado también registran sus *MAC address* adicionalmente a sus adaptadores de red que corresponden a la dirección “multicast” IPv4 mapeada. Por ejemplo, para un adaptador ethernet:

- La dirección MAC “multicast” correspondiente a 239.192.0.1 es 01-00-5E-40-00-01
- La dirección MAC “multicast” correspondiente a 239.192.0.2 es 01-00-5E-40-00-02
- La dirección MAC “multicast” correspondiente a 239.192.156.90 es 01-00-5E-40-9C-5A

Debido a la infraestructura, IPv4 actúa como un enlace con capacidades “multicast”, los equipos pueden usar solicitud de vecindario y mensajes de aviso de vecindad para resolver la capa de enlace de cada dirección.

Las direcciones de la capa de enlace *6over4* son los puntos terminales de los túneles. Los equipos y los ruteadores pueden utilizar mensajes de solicitud de ruteador y de aviso de ruteador para el descubrimiento de ruteadores, prefijos y parámetros.

Para facilitar los mensajes ND, el RFC 2529 define que el formato para las opciones del origen y destino de la capa de enlace.

Por ejemplo, cuando un equipo con dirección IPv4 157.60.91.23 con su correspondiente dirección IPv6 FE80::9D3C:5B7B, envía tráfico a otro equipo con dirección IPv4 131.107.210.49 y correspondiente dirección IPv6 FE80::836B:D231, las direcciones en los encabezados IPv4 e IPv6 quedan como lo muestra la tabla de la figura 2.26:

Campo	**Valor**
IPv6 Source Address	FE80::9D3C:5B7B
IPv6 Destination Address	FE80::836B:D231
IPv4 Source Address	157.60.91.123
IPv4 Destination Address	131.107.210.49

Fig. 2.26: Ejemplo de direcciones *6over4*

El uso de *6over4* para el protocolo IPv6 en la familia Windows 2003 o XP está deshabilitada por default, para habilitarlo, se usa el comando:

```
Netsh interface ipv6 set state 6over4=enabled
```

Éste comando crea una interface de túnel *6over4* para cada dirección IPv4 asignado en la computadora, si se reciben avisos de ruteadores en cada una de éstas interfaces por medio del mecanismo “multicast”, se autoconfiguran las direcciones apropiadas para éstas interfaces en rutas y equipos.

La comunicación de direcciones *6over4* se proporciona por rutas y la interfaz de túneles *6over4*, por ejemplo, el indice de la interfaz para la interfaz de túnel *6over4* de un equipo es 5 (el indice actual para las interfaces de túneles en *6over4* varía dependiendo de la computadora).

Se recibe un aviso de ruteo de un ruteador con una dirección *6over4* de enlace local FE80::C0A8:1501. El aviso de ruteo indica que el ruteador es el ruteador de default y contiene el prefijo de autoconfiguración FEC0:0:0:21A8::/64.

El equipo configura una ruta de default con una dirección de siguiente salto FE80::C0A8:1501 y una ruta de subred para el prefijo FEC0:0:0:21A8::/64, el cual utiliza el indice de prefijo 5.

Cuando los paquetes se envían utilizando las rutas de default FEC0:0:0:21A8::/64, el nodo que envía, usa la dirección *6over4* asignada lógicamente y apropiadamente como destino y usa los últimos 32 bits en la dirección IPv6 origen y destino (correspondientes con las direcciones IPv4 incrustadas) como las direcciones IPv4 origen y destino para el paquete de salida IPv4.

Un paquete que es enviado a un destino que coincide con el prefijo FEC0:0:0:21A8::/64 es enviado a la dirección del siguiente salto del destino usando la interfaz de túnel *6over4*. La interfaz de túnel *6over4* utiliza la resolución de direcciones de direcciones destino para determinar la dirección de capa de enlace origen y destino y su correspondiente dirección IPv4, a usar cuando se envía el paquete IPv6 encapsulado en IPv4.

Para probar la conectividad usando el direccionamiento *6over4*, se utiliza el comando ping. Coinicdentemente con la imagen vista anteriormente, si un el primer equipo quiere localizar al otro equipo usando las direcciones *6over4* de enlace local sería:

```
ping6 FE80::836B:D231%5
```

Debido a que el destino del commando ping es una dirección local de enlace, la porción %ZoneID del comando se utiliza para especificar el indice de interfaz de la interfaz de la cual es enviado el tráfico, en éste caso, %5 especifica interfaz 5, la cual es el indice de interfaz asignado a la interfaz del túnel *6over4* de nuestro ejemplo. [WWW60].

2.5.- Configuración de túneles

El RFC 2893 define las siguientes configuraciones de túneles en los cuales se hacen túneles de tráfico IPv6 entre nodos IPV6/IPv4 sobre una infraestructura IPv4:

- Ruteador a Ruteador
- Equipo a Ruteador o Ruteador a Equipo
- Equipo a Equipo

Los túneles IPv6 sobre IPv4 solo describen el encapsulamiento de paquetes IPv6 con un encabezado IPv4, para que los nodos IPv6 puedan ser alcanzados por medio de una infraestructura IPv4. A diferencia de hacer túneles del Protocolo de Túneles Punto a Punto (*Point-to-Point Tunneling Protocol, PPTP*) y el Protocolo de Túneles de Capa Dos (*Layer Two Tunneling Protocol, L2TP*), no hay intercambio de mensajes para el acondicionamiento, mantenimiento o terminación del túnel. Adicionalmente, les túneles IPv6 sobre IPv4 no proveen seguridad en los paquetes IPv6 que son enviados por el túnel.

2.5.1.- Ruteador a ruteador

En la configuración de túnel de ruteador a ruteador, dos ruteadores IPv6/IPv4 conectan dos infraestructuras IPv4 o IPv6 sobre una infraestructura IPv4. Los puntos finales del túnel expanden un enlace lógico en el camino entre el origen y el destino.

El túnel IPv6 sobre IPv4 entre los dos ruteadores actuan como un salto simple. Las rutas entre cada infraestructura IPv4 o IPv6 apuntan a los ruteadores IPv6/IPv4 en las orillas.

Para cada ruteador IPv6/IPv4, hay una interfaz del túnel que representa el túnel IPv6 sobre IPv4 y enruta el uso de la interfaz del túnel como se puede ver en la figura 2.27.

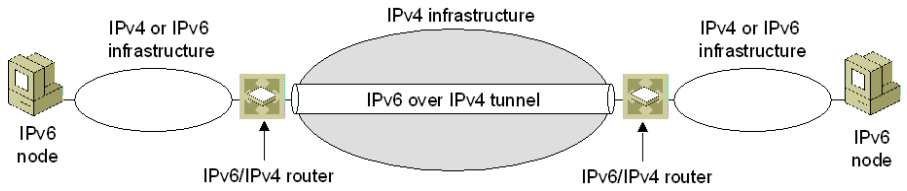

Fig. 2.27: Túnel de Ruteador a Ruteador

Ejemplos de la configuración de estos túneles son:

- Un laboratorio de prueba de solo IPv6 atraves de ina infraestructura de una organización IPv4, que desea alcanzar la Internet IPv6.
- Dos dominios de ruteo solo IPv6 que hacen túnel atraves de la Internet IPv4.
- Un ruteador *6to4* que hace un túnel a traves de la Internet IPv4 para alcanzar otro ruteador *6to4*.

2.5.2.- Equipo a ruteador y ruteador a equipo

En la configuración equipo a ruteador, un nodo IPv6/IPv4 que reside dentro de una infraestructura IPv4 crea un túnel IPV6 sobre IPv4 para alcanzar un ruteador IPv6/IPv4.

Los puntos finales del túnel expanden el primer segmento de la ruta entre los nodos origen y destino, el túnel IPv6 sobre IPv4 entre el nodo IPv6/IPv4 y el ruteador IPv6/IPv4 actúa como un solo salto.

En el nodo IPv6/IPv4, se crea una interfaz del túnel que representa el túnel IPv6 sobre IPv4 y una ruta se añade unsando la interfaz del túnel.

El nodo IPv6/IPv4 envía por el túnel el paquete IPv6 basado en la ruta coincidente, la interfaz del túnel y la dirección de siguiente salto del ruteador IPv6/IPv4.

En la configuración de ruteador a equipo, un ruteador IPv6/IPv4 crea un túnel IPv6 sobre IPv4 a traves de una infraestructura IPv4 para alcanzar un nodo IPv6/IPv4, los puntos finales del túnel expanden el segmento final del camino entre el nodo origen y el nodo destino y el túnel IPv6 sobre IPv4 entre el ruteador IPv6/IPv4 y el nodo IPv6/IPv4 actúa como un solo salto.

En el ruteador IPv6/IPv4, se crea una interfaz de túnel que representa el túnel IPv6 sobre IPv4 y se añade une ruta utilizando la interfaz del túnel, el ruteador IPv6/IPv4 envía por el

túnel el paquete IPv6 basado en la ruta de la subred que coincide y la dirección destino del nodo IPv6 como se puede apreciar en la figura 2.28.

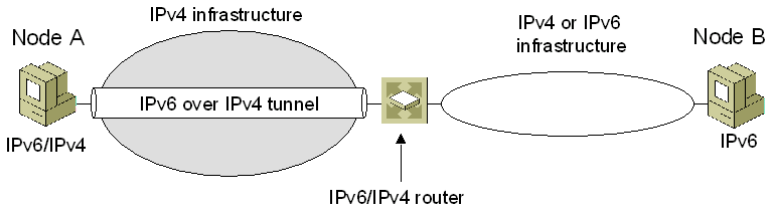

Fig. 2.28: Túneles Equipo a Ruteador y Ruteador a Equipo

Ejemplos de configuraciones Equipo a Ruteador y Ruteador a Equipo:

- Equipos IPv6/IPv4 que hace túneles a traves de una infraestructura IPv4 para alcanzar la Internet IPv6.
- Un *host* ISATAP que hace un túnel a traves de una red IPv4 a un ruteador ISATAP para alcanzar la Internet IPv4, otra red IPv4 o ona red IPv6.
- Un ruteador ISATAP que hace un túnel a traves de una red IPv4 para alcanzar un *host* ISATAP.

2.5.3.- Equipo a equipo

En la configuración del túnel de equipo a equipo, un nodo IPv6/IPv4 que reside en una infraestructura IPv4 crea un túnel IPv6 sobre IPv4 para alcanzar otro nodo IPv6/IPv4 que reside dentro de la misma infraestructura IPv4. Los puntos finales del túnel expanden todo el camino entre el nodo origen y el destino, el túnel IPv6 sobre IPv4 entre los nodos IPv6/IPv4 actúa como un solo salto.

En cada nodo IPv6IPv4, se crea una interfaz que representa el túnel IPv6 sobre IPv4. Las rutas deben de estar presentes para indicar que el nodo destino está en la misma subred lógica definida por la infraestructura IPv4.

Basada en la interfaz que envía, la ruta opcional y la dirección destino, el *host* que envía, manda por el túnel el tráfico IPv6 a su destino como se puede apreciar en la figura 2.29.

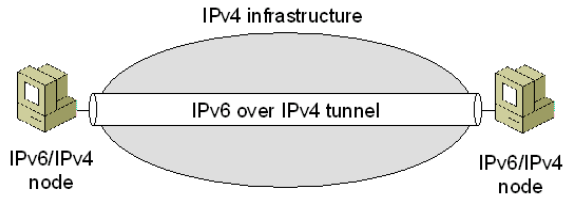

Fig. 2.29: Túneles Equipo a Equipo

Ejemplos de configuración de éste tipo de túneles son:

- Los *host*s IPv6/IPv4 que usan direcciones ISATAP para hacer túneles a traves de la infraestructura IPv4 de la organización.
- Los *host*s IPv6/IPv4 que usan direcciones compatibles con IPv4 para hacer túneles a traves de la infraestructura IPv4 de la organización.

2.5.4.- 6to4

6to4 es una asignación de direcciones y tecnología de túneles automáticos de ruteador a ruteador que se utiliza para proveer conectividad “unicast” IPv6 entre sitios IPv6 y equipos a traves de la Internet IPv4. *6to4* utiliza el prefijo de direccionamiento global:

```
2002:WWXX:YYZZ::/48
```

En el cual WWXX:YYZZ es la representación hexadecimal de una dirección IPv4 pública (w.x.y.z) asignada a un sitio o equipo. La dirección completa *6to4* es:

```
2002:WWXX:YYZZ:SubnetID:InterfaceID
```

6to4 se describe en el RFC 3056, el cual define los siguientes términos:

- *Host 6to4*. Cualquier *host* IPv6 que se configura con por lo menos una dirección *6to4* (una dirección global con el prefijo 2002::/16). Los *host*s *6to4* no requieren ninguna configuración manual y crean direcciones *6to4* usando mecanismos de autoconfiguración de direcciones estandar.
- Ruteador *6to4*. Un ruteador IPv6/IPv4 que soporta el uso de interfaces de túnel *6to4* y es usada típicamente para reenviar tráfico de direcciones *6to4* entre los *host*s *6to4*, dentro de un *site* u otros ruteadores *6to4* o una intranet *6to4*. Los ruteadores *6to4* requieren procesamiento adicional lógico para el correcto encapsulado y decapsulado y pueden requerir configuración manual adicional.

Dentro de un *site*, los ruteadores IPv6 locales promocionan prefijos 2002:WWXX:YYZZ:SubnetID::/64 para que los *host*s puedan crear una dirección *6to4* autoconfigurado y rutas de prefijo de 64 bits que se usan para entregar tráfico entre *host*s *6to4* dentro del *site*.

Los *host*s en las redes individuales son configurados automáticamente con ruta de subred de 64 bits para entrega directa a vecinos y una de default con la dirección de siguiente salto del ruteador que hace la promoción, todo el tráfico IPv6 que no coincide con un prefijo de

64 bits usado por una de las subredes dentro del *site* se reenvían a un ruteador *6to4* en la frontera del *site*.

El ruteador *6to4* en la frontera del *site*, tiene una ruta 220::/16 la cual es usada para reenviar tráfico para otros sitios *6to4* y la ruta de default (::/0) que es usada para reenviar tráfico para un ruteador *6to4* de relay.

En la figura 2.30, los equipos pueden comunicarse entre ellos debido a la ruta de default que utiliza la dirección del siguiente salto del ruteador *6to4* en el sitio 1.

Cuando el *host* A se comunica con el *Host* C en otro *site*, el *host* A envía el tráfico al ruteador *6to4* del *site* 1 como un paquete IPv6, el ruteador *6to4* en el *site* 1 que usa la interfaz del túnel *6to4* y la ruta 2002::/16 en su tabla de ruteo, encapsula el paquete con un encabezado IPv4 y lo envía por el túnel al ruteador *6to4* en el *site* 2.

Cuando el ruteador *6to4* en el *site* 2 recibe el paquete por el túnel, quita el encabezado IPv4 y usando el prefijo de ruta de 64 bits en su tabla de ruteo reenvía el paquete al *host* C.

En el ejemplo, el *host* A con la interfaz ID ID_A reside en la subred 1, dentro del *site* 1 que utiliza la dirección pública 157.60.91.123. El *host* C con la interfaz ID ID_C reside en la subred 2 dentro del *site* 2 que usa la dirección IPv4 pública 131.107.210.49.

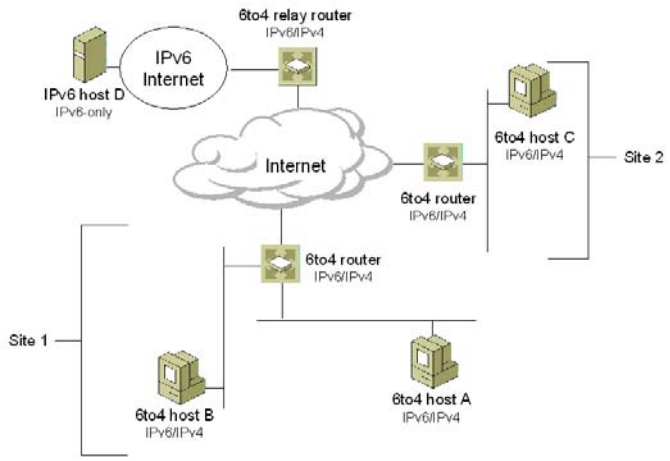

Fig. 2.30: Componentes de *6to4*

Campo	**Valor**
IPv6 Source Address	2002:9D3C:5B7B:1:ID_A
IPv6 Destination Address	2002:836B:D231:2:ID_C
IPv4 Source Address	157.60.91.123
IPv4 Destination Address	131.107.210.49

Fig. 2.31: Lista de encabezados *6to4*

Cuando el paquete IPv6 encapsulado en IPv4 es enviado por el ruteador *6to4* en el *site* 1al ruteador *6to4* en el *site* 2, las direcciones en los encabezados IPv4 e IPv6 se listan en la tabla de la figura 2.31.

Cuando se usan *host*s *6to4*, en la infraestructura de ruteo de IPv6 dentro de un *site*, el ruteador *6to4* en la frontera del *site*, y un ruteador de relay *6to4*, se pueden realizar las siguientes tipos de comunicaciones.

- Un *host 6to4* se puede comunicar con otro *host 6to4* dentro del mismo sitio. Éste tipo de comunicación está disponible usando la infraestructura de ruteo de IPv6, la

cual provee alcanzabilidad a todos los *host*s dentro del *site*. En el ejemplo de la figura 2.30, éste es el tipo de comunicación entre el *host* A y el B.

- Un *host 6to4* se puede comunicar con los *host*s *6to4* en otros *site*s a traves de la Internet IPv4. Éste tipo de comunicación ocurre cuando los *host*s *6to4* en reenvían tráfico IPv6 con destino a un *host 6to4* en otro sitio al ruteador *6to4* del *site* local. El ruteador *6to4* del *site* local envía por el túnel el tráfico IPv6 hacia el ruteador *6to4* del *site* destino en la Internet IPv4. El ruteador *6to4* en el *site* destino quita el encabezado IPv4 y reenvía el paquete IPv6 al *host 6to4* apropiado usando la infraestructura de ruteo IPv6 en el *site* destino. En la figura 2.30 es la comunicación entre el *host* A y el C.
- Un *host 6to4* se puede comunicar con *host*s en la Internet IPv6. Éste tipo de comunicación pasa cuando un *host 6to4* reenvía tráfico IPv6 el cual su destino es un *host* en la Internet IPv6 al ruteador *6to4* del *site* local. El ruteador *6to4* del *site* local envía por el túnel el tráfico IPv6 a un ruteador de relay *6to4* el cual está conectado a ambas redes, la Internet IPv4 y la Internet IPv6. El ruteador de relay *6to4* quita los encabezados IPv4 y reenvía el paquete IPv6 al *host* de la Internet IPv6 apropiado usando la infraestructura de ruteo de la Internet IPv6. En la figura 2.30 sería la comunicación entre el *host* A y el D.

Todos estos tipos de comunicación usan el tráfico IPv6 sin los requerimientos de obtener tanto una conexión directa a la Internet IPv6 como un prefijo de dirección IPv6 global de un Proveedor de servicios de Internet.

A lo largo del capítulo se vió lo que es IPv4, lo que es IPv6, los métodos de transición y la manera de configurarlos. Con la información obtenida se puede concluir que el mejor método de transición para las migraciones es *6over4* ya que proporciona seguridad por medio de direcciones específicas para cada interface y permite al ruteador tener el enlace por medio de IPv4, independizando así la red IPv4 existente de las redes IPv6 que se conectan en los puertos Ethernet del ruteador. Es decir, la mejor opción es *6over4* porque nos permite trabajar sobre la red existente IPv4, sin tener que hacer una inversión fuerte en infraestructura, el cambio se hace solamente en los nodos nuevos o se hace un cambio paulatino en las maqinas existentes, pero dicho cambio no afecta la infraestructura de la red.

Las bondades de IPv6 se puede ir aprovechando poco a poco mientras más equipos se vayan migrando a la nueva red, las aplicaciones punto a punto, la telefonía por IP, etc, se pueden aprovechar más mientras vaya creciendo la red IPv6.