PROTOCOLO IPv6

La versión 4 del protocolo de Internet (IPv4) proporciona los medios de comunicación básica dentro del conjunto de protocolos TCP/IP, pero conforme pasa el tiempo y se vuelve más exigente la forma de comunicación entre redes, así como el crecimiento exponencial en la cantidad de *host* conectados a Internet, este protocolo se va haciendo obsoleto, se necesita añadirle más y mejores características, como por ejemplo aumentar el número de direcciones de Internet, incluir autenticación y encriptación de datos para realizar más segura la comunicación, realizar en forma más rápida la comunicación entre redes, etc., por estos motivos se empezó a trabajar en un nuevo protocolo se comunicación en Internet, llamado protocolo de Internet de próxima generación (IPng) conocido formalmente como IPv6.

Este capítulo se encarga de cubrir los temas concernientes a la nueva versión del protocolo de Internet conocido como protocolo Internet versión 6 o simplemente IPv6. Se explicará y se comparará el antiguo IPv4 con el nuevo IPv6. Se hablará además de las nuevas características del protocolo de mensajes de control de Internet para trabajar con IPv6 conocido como ICMPv6, así como la forma de transporte de los paquetes IPv6 a través de una red Ethernet. Se tocará además el protocolo de descubrimiento de vecinos (ND) el cual viene a reemplazar la tarea del protocolo de resolución de direcciones (ARP).

2.1 Protocolo de Internet Versión 6

La Internet es uno de los grandes medios de comunicación e investigación en la historia, la cual ha tenido un crecimiento exponencial, por esta razón se han agotado las direcciones de IP, y conforme se incorporan mas usuarios y organizaciones se necesita y se quiere mayor seguridad y rapidez en el envío y recepción de información.

El protocolo de Internet versión 6 (IPv6) o llamado inicialmente protocolo de Internet de próxima generación (IPng) es el protocolo diseñado por la IETF – *The Internet Engineering Task Force* - con el fin de reemplazar al protocolo Internet versión 4 (IPv4), y se encuentra estipulado en el RFC 2460 [79].

Los cambios de IPv4 a IPv6 pueden agruparse en las siguientes categorías:

- *Direcciones más largas*. El IPv6 cuadruplica el tamaño de las direcciones del IPv4, de 32 bits a 128 bits.
- *Simplicidad en el formato de encabezado*. Algunos de los campos de IPv4 son suprimidos o colocados opcionalmente, para reducir el costo de procesamiento y el ancho de banda utilizado.

- *Soporte de extensiones y opciones mejoradas*. Opciones en el encabezado permite una entrega eficiente, una menor limitación en la longitud de las opciones y una mayor flexibilidad en la incorporación de nuevas opciones en el futuro.
- *Capacidad para etiquetar el flujo de información*. Reemplaza la especificación del *tipo servicio* del IPv4 con un mecanismo que permite la preasignación de recursos de red. En particular, el nuevo mecanismo soporta aplicaciones como vídeo en tiempo real que requiere una garantía de ancho de banda y retardo.
- *Capacidad de autenticación y privacidad*. Las extensiones incorporadas permiten la autenticación, la integridad de los datos y (opcionalmente) la confidencialidad de los datos.

2.2 IPv4 & IPv6

Para explicar las diferencias entre un *datagrama* IPv6 y un IPv4, se muestra la figura 2.1, en la que los campos que han sido modificados del datagrama IPv4 se colocan de color gris y en blanco los que desaparecen.

<table>
<tr><td colspan="8">0 4 8 16 19 24 31</td></tr>
<tr><td colspan="2">VERS</td><td colspan="2">HLEN</td><td colspan="2">TIPO DE SERVICIO</td><td colspan="2">LONGITUD TOTAL</td></tr>
<tr><td colspan="4">IDENTIFICACIÓN</td><td>BANDERAS</td><td colspan="3">DESPLAZAMIENTO DE FRAGMENTO</td></tr>
<tr><td colspan="2">TIEMPO DE VIDA</td><td colspan="2">PROTOCOLO</td><td colspan="4">SUMA DE VERIFICACIÓN DEL ENCABEZADO</td></tr>
<tr><td colspan="8">DIRECCIÓN IP DE LAFUENTE</td></tr>
<tr><td colspan="8">DIRECCIÓN IP DEL DESTINO</td></tr>
<tr><td colspan="6">OPCIONES (En caso de existir)</td><td colspan="2">RELLENO</td></tr>
</table>

Figura 2.1 Campos modificados y desaparecidos en un *datagrama* IPv4.

El motivo fundamental por el que los campos son eliminados, es la innecesaria redundancia. En el caso del campo DESPLAZAMIENTO DE FRAGMENTO, el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6. En IPv6 los *routers* no realizan la tarea de fragmentación, sino que se realiza en el nodo inicial.

Los campos renombrados son:

- LONGITUD TOTAL por LONGITUD DE CARGA ÚTIL, que es la longitud de los datos y puede ser de hasta 65,536 bytes.
- TIEMPO DE VIDA por LÍMITE DE SALTOS, este campo se decrementa en 1 por cada salto que dé el paquete.
- PROTOCOLO por SIGUIENTE ENCABEZADO, en lugar de usar encabezados de longitud variable se emplea sucesivos encabezados encadenados.

Los nuevos campos que se incorporan son:

- CLASE DE TRÁFICO, llamado primeramente PRIORIDAD en el RFC 1883 (obsoleto, sustituido por el RFC 2460).
- ETIQUETA DE FLUJO, con este campo se permite etiquetar paquetes para brindarles un trato especial.

Estos campos son los que permiten una de las características fundamentales e intrínsecas de IPv6: calidad de servicio (QoS), clase de servicio (CoS), y un mecanismo de Control de flujo para la asignación de prioridades según los tipos de servicios.

Como se puede notar en la figura 2.2 el encabezado de un datagrama IPv6 tiene una longitud de 40 bytes, el doble de un IPv4, pero con muchas más ventajas, al haberse eliminado campos redundantes.

En IPv6, la información de la capa de Internet es codificada en encabezados separados que pueden ser colocados entre el encabezado IPv6 y el encabezado de la capa superior. Un encabezado IPv6 puede tener cero, uno o más encabezados de extensión, cada uno identificado por el número colocado en el campo SIGUIENTE ENCABEZADO. Los encabezados de extensión no son analizados en cada nodo de la ruta, sino sólo en el nodo o nodos finales, con la excepción del encabezado de opciones de salto a salto. Las direcciones fuente y destino identifican interfaces individuales o un conjunto de interfaces, estas direcciones se clasifican en tres tipos: u*nicast, anycast* y m*ulticast*. La *unicast* identifica a una interfaz simple, de esta manera un paquete enviado a una dirección *unicast* es entregado a la interfaz identificada por la dirección. Una dirección *anycast* es un identificador para un conjunto de interfaces, y al enviar un paquete con dirección anycast este es entregado a una de las interfaces identificada por la dirección (a la más "cercana", de acuerdo a la medida de distancia del protocolo de ruteo). Una *multicast* es un identificador de un conjunto de interfaces, y el paquete enviado con este tipo dirección es entregado a todas las interfaces identificadas por la dirección.

<table>
<tr><td colspan="4">0 4 12 16 24
31</td></tr>
<tr><td>VERS</td><td>CLASE DE TRÁFICO</td><td colspan="2">ETIQUETA DE FLUJO</td></tr>
<tr><td colspan="2">LONGITUD DE CARGA ÚTIL</td><td>SIGUIENTE ENCABEZADO</td><td>LÍMITE DE SALTOS</td></tr>
<tr><td colspan="4">DIRECCIÓN IP DE LA FUENTE DE 128 BITS</td></tr>
<tr><td colspan="4">DIRECCIÓN IP DEL DESTINO DE 128 BITS</td></tr>
</table>

Figura 2.2 Formato de un *datagrama* IPv6.

2.3 Transmisión de paquetes IPv6 en redes Ethernet

El RFC 2464 [80] especifica el formato del frame utilizado para la transmisión de paquetes IPv6 en redes Ethernet. Estos paquetes son transmitidos en frames Ethernet estándar, como se muestra en la figura 2.3. Estos frames están formados de la manera siguiente: la dirección Ethernet destino, la dirección Ethernet fuente, el tipo de código Ethernet que especifica el protocolo que se transporta, en este caso este campo contiene un valor hexadecimal de 86DD, después se presenta el encabezado IPv6 seguido por la carga útil y posiblemente bytes de relleno para alcanzar el tamaño mínimo de un frame ethernet.

<table>
<tr><td>Dirección Ethernet Destino</td><td>Dirección Ethernet fuente</td><td>1000011011011101</td><td>Encabezado IPv6 y carga útil</td></tr>
</table>

Figura 2.3 Frame Ethernet que transporta un paquete IPv6.

2.4 Encabezados de extensión de IPv6

En IPv6 la información opcional es colocada en encabezados opcionales que se encuentran entre el encabezado IPv6 y el encabezado de capa superior, como se observa en la figura 2.4. Un paquete IPv6 puede transportar uno o más encabezados de extensión, cada uno identificado por el valor almacenado en el campo SIGUIENTE ENCABEZADO en el encabezado anterior a él. Los encabezados que pueden ser transportados son:

- ***Encabezado de opciones salto a salto*** (*Hop-by-Hop Options Header*). Este encabezado es usado para transportar información opcional que debe ser examinada por cada nodo en la ruta de entrega del paquete. Este encabezado es identificado por el valor de 0 colocado en el campo de SIGUIENTE ENCABEZADO.
- ***Encabezado de ruteo*** (*Routing Header*). Es usado por la fuente IPv6 para listar uno o más nodos intermedios a ser visitados en el camino de entrega del paquete. Este encabezado tiene el valor de 43 en el campo SIGUIENTE ENCABEZADO.
- ***Encabezado de fragmento*** (*Fragment Header*). Es usado por la fuente IPv6 para enviar paquetes largos que se ajusten a la MTU de la ruta destino. Este encabezado es identificado con el valor de 44 en el campo SIGUIENTE ENCABEZADO.
- ***Encabezado de opciones de destino*** (*Destination Options Header*). Este encabezado es usado para llevar información opcional que necesita examinar solo el nodo o los nodos destino. El valor que lo identifica en el campo SIGUIENTE ENCABEZADO es el 60.

El valor 59 en el campo SIGUIENTE ENCABEZADO de IPv6 o en cualquier encabezado de extensión indica que no existe siguiente encabezado

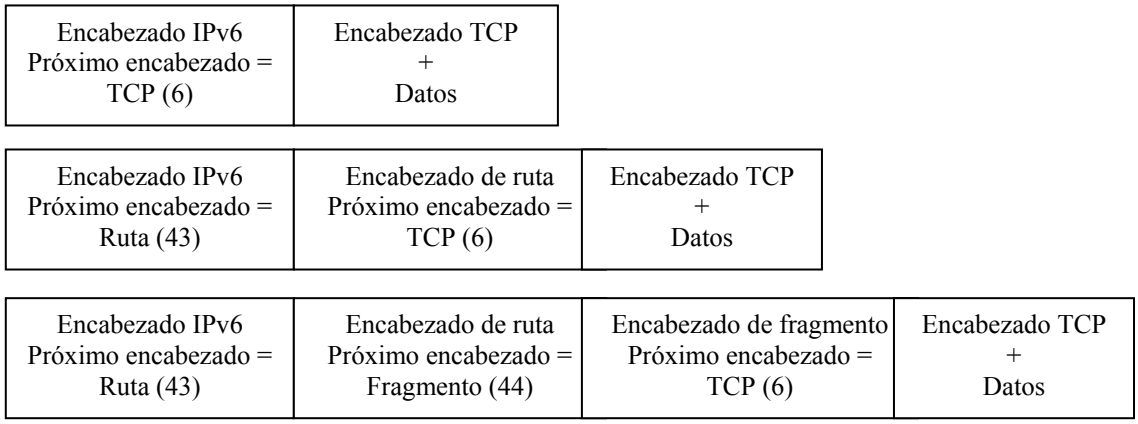

Figura 2.4 Encabezados de extensión en IPv6.

2.5 Orden de los encabezados de extensión

Cuando se utiliza más de un encabezado de extensión en el mismo paquete, se recomienda que estos encabezados aparezcan en el siguiente orden [79]:

1. Encabezado IPv6
2. Encabezado de opciones salto a salto
3. Encabezado de opciones de destino
4. Encabezado de ruteo
5. Encabezado de fragmento
6. Encabezado de autenticación
7. Encabezado de seguridad del encapsulado de la carga útil
8. Encabezado de opciones de destino (para ser procesado por el primer destino)

9. Encabezado de capa superior

Cada encabezado de extensión debe ocurrir al menos una vez, excepto el encabezado de opciones de destino, el cual debe ocurrir al menos un par de veces (antes del encabezado de ruteo y antes del encabezado de capa superior).

Si el encabezado de capa superior es otro encabezado IPv6 (en el caso de que IPv4 sea tuneleado o encapsulado en IPv6), puede ser seguido por su propio encabezado de extensión. Estos encabezados están sujetos al mismo orden recomendado.

Los nodos IPv6 deben aceptar e intentar procesar encabezados de extensión en cualquier orden y cualquier número de veces que ocurran en el mismo paquete, a excepción del encabezado de opciones salto a salto el cual está restringido a aparecer inmediatamente después del encabezado IPv6.

2.6 Protocolo de Mensajes de Control de Internet Versión 6

IPv6 realiza algunos cambios al protocolo de mensaje de control de Internet (ICMP) usado en el IPv4 [68]. El protocolo que resulta es el protocolo ICMPv6 [78], cuyo valor en el campo SIGUIENTE ENCABEZADO de IPv6 es 58.

En la figura 2.5 se muestra el formato general de los mensajes ICMPv6, utilizados por IPv6 para reportar errores generados durante el procesamiento de los paquetes, así como para realizar diagnósticos. Cada uno de los mensajes ICMPv6 esta precedido por un encabezado IPv6 y cero o más encabezados de extensión IPv6.

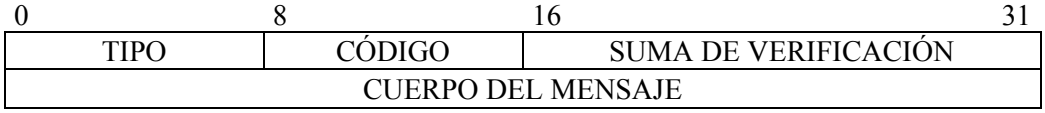

Figura 2.5 Formato general de un mensaje ICMPv6.

Los mensajes ICMPv6 se agrupan en dos clases: mensajes de error y mensajes informativos. Los mensajes de error tienen un cero en el bit de orden mayor en el campo tipo, por lo que sus valores se sitúan entre 0 y 127. Los valores de los mensajes informativos varían entre 128 y 255. Los mensajes definidos por la especificación básica se muestran en la tabla 2.1.

Tipo	Código	Descripción de mensaje ICMPv6
1		Destino inaccesible
	0	No existe ruta al destino
	1	Comunicación con el destino administrativamente prohibida
	2	No asignado
	3	Dirección inalcanzable
	4	Puerto inalcanzable
2		Paquete demasiado grande
3		Tiempo excedido

	0	Límite de saltos excedido
	1	Tiempo excedido en el reensamble del paquete
4		Problema de parámetros
	0	Error en el campo de encabezado
	1	Tipo de siguiente encabezado desconocido
	2	Opción IPv6 desconocida
128	0	Solicitud de eco
129	0	Respuesta de eco

Tabla 2.1 Tipos de mensajes ICMPv6.

Los mensajes ICMP pueden estar sujetos a varios ataques, entre los que se encuentran los siguientes:

1. Los mensajes ICMP pueden estar sujetos a acciones intencionales para causar que el receptor piense que el mensaje viene de una fuente diferente al mensaje original. La protección contra este ataque puede lograrse aplicando el mecanismo de autenticación IPv6 [87] en el mensaje ICMP.
2. Los mensajes ICMP pueden estar sujetos a acciones intencionales para causar que el mensaje o la respuesta vaya a un destino diferente que la intención del mensaje original. El cálculo de la suma de verificación ICMP proporciona un mecanismo de protección en contra de los cambios hechos por interceptores en las direcciones fuente y destino del paquete IP que transporta el mensaje, el campo suma de verificación ICMP proporcionado es protegido en contra de los cambios por autenticación [87] o encriptación [88] del mensaje ICMP.
3. Los mensajes ICMP pueden estar sujetos a cambios en los campos de mensajes, o carga útil. La autenticación [87] o encriptación [88] del mensaje ICMP es una protección en contra de tales acciones.
4. Los mensajes ICMP pueden ser usados como intento para ejecutar ataques de negación de servicio enviando paquetes IP erróneos en forma consecutiva.

La documentación completa de estos tipos de ataques puede ser encontrada en la arquitectura de seguridad IP [89].

2.7 Protocolo de descubrimiento de vecino

En IPv6, el protocolo semejante a ARP en IPv4, es el llamado protocolo de descubrimiento del vecino (ND, *Neighbor Discovery*). Este protocolo es el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros en su mismo enlace, determina sus direcciones en la capa de enlace, localiza los *routers* y mantiene la información de conectividad acerca de las rutas a los vecinos activos [74].

El protocolo ND se emplea también para mantener limpios los caches donde se almacena la información relativa al contexto de la red a la que está conectada un servidor o un *router*, y para detectar cualquier cambio en la misma. Si un *router* o una ruta falla, el servidor buscará alternativas funcionales.

ND emplea los mensajes ICMPv6 para algunos de sus servicios, este protocolo es bastante completo y sofisticado, ya que es la base para permitir el mecanismo de autoconfiguración en IPv6.

Define varios mecanismos, entre ellos: descubrir *routers*, prefijos y parámetros, autoconfiguración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos inalcanzables, detección de direcciones duplicadas o campos, redirección, balanceo de carga entrante, direcciones *anycast,* y anunciación de proxies.

ND define cinco tipos de mensajes ICMPv6:

- Solicitud de *router*. Generado por una interfaz cuando es activada, para pedir a los *routers* que se anuncien inmediatamente. Tipo de mensaje ICMPv6 133 código 0.
- Anunciación de *router*. Generado por los *routers* periódicamente (entre cada 4 y 1800 segundos) o como consecuencia a una solicitud de *router*, a través de multicast, para informar de su presencia así como de otros parámetros de enlace y de Internet, como prefijos (uno o varios), tiempo de vida, configuración de direcciones, límite de salto sugerido, etc. Es importante para permitir la renumeración. Tipo de mensaje ICMPv6 134 código 0.
- Solicitud de vecino. Generado por los nodos para solicitar la dirección en la capa de enlace de la tarjeta de su vecino, o para verificar que el nodo vecino es alcanzable, así como para detectar las direcciones duplicadas. Las solicitudes son multicast cuando el nodo necesita resolver una dirección y unicast cuando el nodo quiere verificar que el vecino es alcanzable. Tipo de mensaje ICMPv6 135 código 0.
- Anunciación de vecino. Generado por los nodos como respuesta a la solicitud de vecino. Tipo de mensaje ICMPv6 136 código 0.
- Redirección. Generado por los *routers* para informar a los *hosts* de un mejor salto para llegar a un destino. Tipo de mensaje ICMPv6 137 código 0.

El protocolo de Descubrimiento de vecinos IPv6 corresponde a una combinación de los protocolos IPv4 ARP, descubrimiento de *router* ICMP, y redirección ICMP. El protocolo ND presenta las siguientes ventajas frente a los mecanismos existentes en IPv4:

- El descubrimiento de *routers* es parte de la base del protocolo, no se tiene que recurrir a los protocolos de encaminado.
- La anunciación del *router* incluye las direcciones de la capa de enlace, no es necesario ningún intercambio adicional de paquetes para su resolución.
- La anunciación del *router* incluye los prefijos para el enlace, por lo que no hay necesidad de un mecanismo adicional para configurar la máscara de red.
- La anunciación de un *router* permite la autoconfiguración de direcciones.
- Los *routers* pueden anunciar a los *host* del mismo enlace la MTU.
- Se extienden las *multicast* de resolución de direcciones entre 2^{32} direcciones, reduciendo de forma importante las interrupciones relativas a la resolución de direcciones en máquinas distintas al objetivo, y evitando las interrupciones en máquinas sin IPv6.

- Las redirecciones contienen la dirección de la capa de enlace del nuevo salto, lo que evita la necesidad de una resolución de dirección adicional.
- Se pueden asignar múltiples prefijos al mismo enlace y por defecto los *host* aprenden todos los prefijos por la anunciación del *router*. Sin embargo, los *routers* pueden ser configurados para omitir parte o todos los prefijos en la anunciación, de forma que las máquinas consideren que los destinos están fuera del enlace; de esta forma, enviarán el tráfico a los *routers*, quien a su vez los redireccionarán según corresponda.
- A diferencia de IPv4, en IPv6 el receptor de una redirección asume que el siguiente salto está en el mismo enlace. Se prevé una gran utilidad en el sentido de no ser deseable o posible que los nodos conozcan todos los prefijos de los destinos en el mismo enlace.
- La detección de vecinos inalcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en *routers*, particiones de enlaces, nodos que cambian sus direcciones, nodos móviles, etc.
- A diferencia de ARP, en ND se pueden detectar fallos de la mitad del enlace, es decir, con conectividad en un solo sentido, evitando el tráfico hacia ellos.
- La detección de vecinos inalcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en *routers*, fallas parciales, nodos que cambian sus direcciones, nodos móviles, etc.
- El uso de direcciones de enlace local para identificar *routers*, permite a las máquinas que mantengan su asociación con los mismos, en el caso de que se realice una renumeración para usar nuevos prefijos globales.
- El límite de saltos es igual a 255, lo que evita que haya envíos accidentales o intencionados desde máquinas fuera del enlace, dado que los *routers* decrementan automáticamente este campo en cada salto.
- Al realizar la resolución de direcciones en la capa ICMP, se independiza el protocolo del medio, permitiendo mecanismos de autenticación y seguridad normalizados.

Por todo lo anterior se puede decir que ND reemplaza a ARP con varias mejoras e importantes ventajas.

2.8 Análisis y captura de un paquete IPv6 con tcpdump

Para llevar a cabo la captura de un paquete IPv6 se utilizó el software tcpdump. Este software es el más viejo de los *sniffers* incorparado en los sistemas UNIX. Tcpdump brinda la facilidad de captura de un tipo determinado de paquete, es decir, podemos incorparle un filtro para la captura, además, podemos indicarle que nos muestre los datos en forma hexadecimal. En el capítulo 3 hablaremos sobre el trabajo de los *sniffers* y tocaremos el punto de tcpdump.

Para realizar la captura de un paquete IPv6 debemos de tener configurada la máquina para que reconozca este tipo de paquete, y contar con una versión de tcpdump que reconozca dichos paquetes. Para esto podemos consultar [48] y adquirir la nueva versión de tcpdump.

Al tener la actualización del software tcpdump y teniendo configurada la máquina para reconocer conexiones IPv6, se pudo capturar el siguiente paquete:

11:42:38.669714 eth0 < 8:0:20:9c:69:ba 0:0:0:0:0:1 ipv6 87:

6000 0000 0021 063c fe80 0000 0000 0000
0a00 20ff fe9c 69ba fe80 0000 0000 0000
0240 d0ff fe0b 102d 0017 0401 1364 8841
a221 04b6 8018 6468 dbc9 0000 0101 080a
00be 9606 005f 74f8 72

Para llevar a cabo el análisis de este paquete realizamos la siguiente división: etiqueta de tiempo, encabezado Ethernet, encabezado IPv6, siguiente encabezado y datos.

Etiqueta de tiempo

Los paquetes capturados con tcpdump bajo las opciones –enx, son precedidos por una etiqueta de tiempo, en formato hh:mm:ss.frac, así el paquete que se muestra fue capturado en el tiempo 11:42:38.669714

Encabezado Ethernet

El encabezado Ethernet como se indica en el RFC 2464 [80] contiene en los primeros 6 bytes la dirección MAC destino, en los siguientes 6 bytes la dirección MAC origen y en los 2 bytes siguientes el código del protocolo encapsulado. En este caso tcpdump realizo la conversion del código 86DD en hexadecimal por el ipv6. La figura 2.6 muestra esta información.

8	0	20	9c	69	ba	0	0	0	0	0	1	86	DD

Figura 2.6 Encabezado Ethernet que transporta un IPv6 capturado con tcpdump.

Encabezado IPv6

1	2	3	4	5	6	7	8	9
60	00	00	00	00	21	06	3c	fe

10	11	12	13	14	15	16	17	18
80	00	00	00	00	00	00	0a	00

19	20	21	22	23	24	25	26	27
20	ff	fe	9c	69	ba	fe	80	00

28	29	30	31	32	33	34	35	36
00	00	00	00	00	02	40	d0	ff

37	38	39	40
fe	0b	10	2d

Figura 2.7 Encabezado IPv6 capturado con tcpdump.

El número en cada cuadro de la figura 2.7 se encuentra en hexadecimal y representa un byte.

El byte número 1

El primer byte (60) está dividido en dos partes de 4 bits. Los primeros 4 bits (el número 6) especifican la versión del datagrama IP que se esta utilizando, como se observa se esta usando IPv6. Los siguientes 4 bits forman parte del campo de *clase de tráfico*.

El byte número 2

Los primero 4 bits (0) del segundo byte junto con los 4 bits del primer byte (0) forman el campo que especifica la *clase de tráfico*. Este campo es parecido al campo de TOS de IPv4, y como se puede notar tiene una longitud de 8 bits. Este campo es utilizado por los nodos origen y/o *routers* para distinguir las diferentes clases o prioridades de los paquetes IPv6. En este caso el valor que aparece es un 00 el cual indica que se solicita un servicio de capa superior.

Los bytes número 3 y 4

Los 4 bits restantes del byte 2 junto con los bytes 3 y 4 forman al campo *etiqueta de flujo* (0 0000). Este campo se ocupa para permitir tráfico con requerimientos de calidad de servicio o tiempo real. Este campo tiene una longitud de 20 bits.

Los bytes número 5 y 6

Los siguientes dos bytes (00 21) definen la *carga útil* o la longitud de los datos, este campo puede tener el valor de hasta 65536 bytes.

El byte número 7

Este byte denota el *siguiente encabezado* que esta incluido en el datagrama IPv6. En este caso especifica que es un *encabezado de capa superior* porque transporta un 06, es decir, un TCP. Otros valores que pueden aparecer se muestran en la tabla 2.2. IPv6 utiliza encabezados sucesivos encadenados, en lugar de usar encabezados de longitud variable. Cada uno de los encabezados tienen un campo que indica el tipo de su suceso.

Valor de byte (en hexadecimal)	Significado
0	Encabezado de opciones salto a salto
43	Encabezado de ruteo
44	Encabezado de fragmento
60	Encabezado de opciones de destino
59	No existe siguiente encabezado
06	TCP
11	UDP
59	ICMPv6

Tabla 2.2 Algunos valores que puede transportar el campo siguiente encabezado.

El byte número 8

Este byte (3c) representa el *límite de saltos* que puede realizar un paquete antes de ser descartado, esto es, si el valor llega a 0 el paquete es descartado, para esto cada nodo que reenvíe el paquete decrementa en 1 este campo.

Los bytes número 9 al 24

Estos bytes corresponden a la dirección IP Origen, como se puede notar la dirección es de 16 bytes (fe80:0000:0000:0000:0a00:20ff:fe9c:69ba).

Los bytes número 25 al 40

Los últimos 16 bytes del 25 al 40 representan la dirección IP destino (fe80:0000:0000:0000:0240:d0ff:fe0b:102d).

Siguiente encabezado

El siguiente encabezado en este caso es un datagrama TCP. Este encabezado tiene una longitud de 20 bytes, y se muestra en la figura 2.8. Este encabezado se analiza con mayor detalle en el capitulo siguiente.

1	2	3	4	5	6	7	8	9	10
00	17	04	01	13	64	88	41	a2	21
11	12	13	14	15	16	17	18	19	20
04	b6	80	18	64	68	db	c9	00	00

Figura 2.8 Encabezado siguiente (TCP) capturado con tcpdump.

Sólo diremos que los bytes del 1 al 4 denotan los número de puertos utilizados en la comunicación. Los primeros dos bytes (00 17) especifican el puerto origen, en este caso es el telnet (23 en decimal) y los dos bytes siguientes (0401) denotan al puerto destino.

Datos

Después de leer los encabezados, en este caso, solo el encabezado TCP, vienen los datos, los cuales en este paquete sólo es uno, ya que como vimos la carga útil del paquete es de 21 bytes, de los cuales 20 bytes corresponden al encabezado TCP.

2.9 Captura de un paquete IPv6 con snoop

El software snoop [61] es un *sniffer* que se encuentra en las máquinas SUN Solaris. Al tener instalada una versión de Solaris que permita el trabajo con paquetes IPv6, se puede utilizar snoop para capturar los paquete de este tipo. A continuación se muestra un paquete IPv6 capturado en una SUN con sistema Solaris 8.0, como se observa este software muestra a detalle cada uno de los campos.

```
ETHER:  ----- Ether Header -----
ETHER:
ETHER:  Packet 9 arrived at 12:10:48.46
ETHER:  Packet size = 86 bytes
ETHER:  Destination = 8:0:20:9c:69:ba, Sun
ETHER:  Source      = 0:40:d0:b:10:2d,
ETHER:  Ethertype = 86DD (IPv6)
ETHER:
IPv6:   ----- IPv6 Header -----
IPv6:
```

```
IPv6:   Version = 6
IPv6:   Traffic Class = 0
IPv6:   Flow label = 0x0
IPv6:   Payload length = 32
IPv6:   Next Header = 6 (TCP)
IPv6:   Hop Limit = 64
IPv6:   Source address = fe80::240:d0ff:fe0b:102d
IPv6:   Destination address = fe80::a00:20ff:fe9c:69ba
IPv6:
TCP:  ----- TCP Header -----
TCP:
TCP:  Source port = 1025
TCP:  Destination port = 23 (TELNET)
TCP:  Sequence number = 2720072880
TCP:  Acknowledgement number = 325355568
TCP:  Data offset = 32 bytes
TCP:  Flags = 0x10
TCP:        ..0. .... = No urgent pointer
TCP:        ...1 .... = Acknowledgement
TCP:        .... 0... = No push
TCP:        .... .0.. = No reset
TCP:        .... ..0. = No Syn
TCP:        .... ...0 = No Fin
TCP:  Window = 31680
TCP:  Checksum = 0x3966
TCP:  Urgent pointer = 0
TCP:  Options: (12 bytes)
TCP:    - No operation
TCP:    - No operation
TCP:    - TS Val = 6255503, TS Echo = 12489883
TCP:
TELNET:  ----- TELNET:   -----
TELNET:
TELNET:  ""
TELNET:
```

Como se puede notar, los protocolos han cambiado, no solo de nombre sino de contenido y algunos otros se han sustituido. En estos días se esta migrando de IPv4 a IPv6 dado que brinda mayor rendimiento y seguridad. Ahora algunos sistemas operativos desde la instalación preguntan si quieres habilitar el IPv6, como por ejemplo el sistema Solaris 8.0 para SUN o para Intel, en otros sistemas como Linux, se necesita reconfigurar el kernel [44] para poder habilitar este nuevo protocolo, y se deben de instalar nuevos paquetes [46][47]. Esto abre un amplio campo de trabajo, tanto en la migración paulatina de las redes como en el desarrollo de nuevas aplicaciones.