**Capítulo 4**

**R19. Compare y contraste los campos de cabecera de IPv4 e IPv6. ¿Tienen campos en común?**

Hay varios cambios en el encabezado de IPv4 e IPv6.

Ajustes importantes:

1. IPv4 es de largo variable mientras IPv6 tiene largo fijo de 40 bytes.
2. Cambian los campos para las direcciones (IPv4 es de 32 bits - IPv6 es de 128 bits).
3. Se eliminaron los campos de fragmentación y las opciones.
4. En IPv4 se indicaba el tamaño del header+payload (total length), ahora se indica solo el payload efectivo (payload length) ya que el header es fijo de 40 bytes.
5. En IPv6 se elimina el campo de checksum del encabezado.
6. La alineación cambia de 32 a 64 bits
7. Nuevos campo en IPv6:

-> **FLOW LABEL**

1. Puntos revisados:

* TTL (time to live) -> **HOP LIMIT** (límite de saltos)
* Protocol -> **NEXT HEADER** (próximo encabezado)
* Precedencia y TOS -> **TRAFFIC CLASS**

FLOW LABEL

En IPv6 se utiliza una definición más amplia de flujo que en IPv4.

Se permite etiquetar los paquetes que pertenecen a determinados flujos para los que el emisor solicita un tratamiento especial, como por ejemplo un servicio en tiempo real o una calidad de servicio determinada.

Se prevé la necesidad de poder diferenciar entre los flujos.

Encabezados de extensión de IPv6 (extension headers)

- Las opciones de IPv6 son manejadas a través de los encabezados de extensión.

- Los mismos son “enganchados” utilizando el campo Next Header (se ubican entre el encabezado de IPv6 y el encabezado de capa de transporte de un paquete).

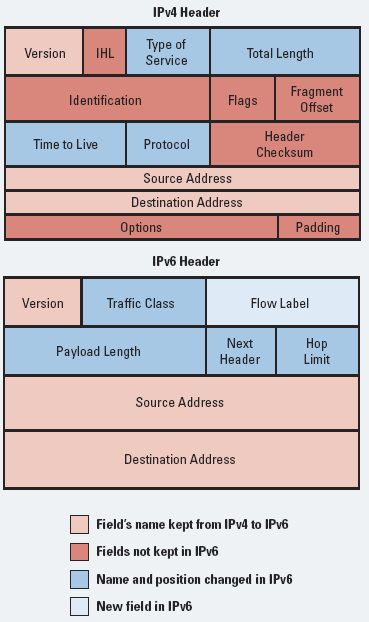
- Ningún enrutador procesa ni examina la mayoría de los encabezados de extensión de IPv6 durante el recorrido de distribución del paquete hasta que éste llega a su destino. Esta función supone una mejora importante en el rendimiento de los enrutadores en paquetes que contienen opciones. En IPv4, la presencia de cualquier opción hace que el enrutador examine todas las opciones.

- A diferencia de las opciones de IPv4, los encabezados de extensión de IPv6 pueden tener un tamaño arbitrario. Asimismo, la cantidad de opciones que lleva un paquete no se limita a 40 bytes.

- Las opciones de IPv6 consideran funciones que no estaban viables en IPv4.

- Algunos encabezados de extensión de IPv6:

* Fragmentación: fragmentación y montaje.
* Autenticación: integridad y autenticación, y seguridad.
* Encapsulado de carga útil: confidencialidad.
* Opciones de destino: información opcional que el nodo de destino debe examinar



**R22. Explique cómo la organización jerárquica de Internet ha hecho posible el escalar la red a millones de usuarios.**

Los routers son agrupan en sistemas autónomos (SA), normalmente todos bajo el mismo control administrativo.

Dentro de un AS, todos los routers deben corren un mismo protocolo de enrutamiento, llamados protocolos intra-SA (interiores SA).

Para poder conectar los SA entre sí, existen routers especiales de salida en los diferentes SA, llamados routers de pasarela (gateway routers) que tiene un enlace con un extremo en un SA y el otro extremo en otro SA.

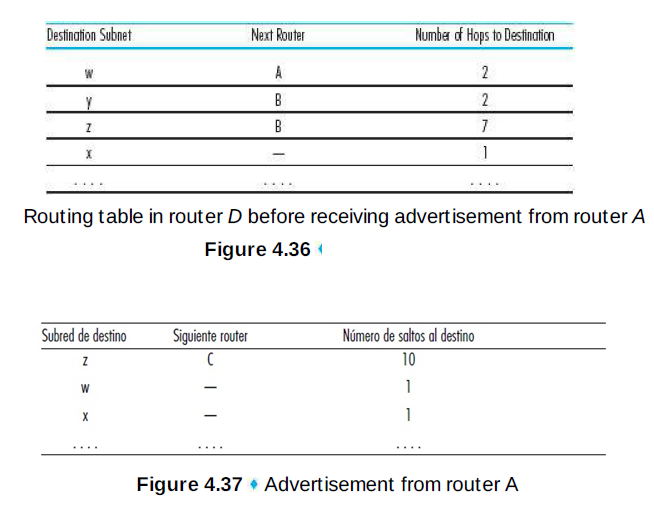
Los routers de pasarela ejecutan un protocolo de enrutamiento externo a los SA, llamados inter-SA, que determina las rutas entre los SA.

El problema de la gran escalabilidad se resuelve ya que un router intra-AS sólo necesita saber acerca de los routers dentro de su propio SA y conocer cómo llegar al router de pasarela de su propio SA.

**SECCIÓN 4.6**

**R24. Comenzando con la tabla original en D (Figura 4.36), suponga que D recibe de A el siguiente anuncio (Figura 4.37):**

**¿Cambiará la tabla en el router D? En caso afirmativo, ¿cómo?**



No ya que las rutas ofrecidas por A a D son peores que las que ya posee D.

Caso a caso.

- A ofrece a D una ruta hacia z de costo 10, si D incorpora esta ruta para D tendrá costo **11**, mientras que la actual ruta que D tiene hacia z es de costo **7**.

- A ofrece a D una ruta hacia w de costo 1, si D incorpora esta ruta para D tendrá costo **2**, la actual ruta que D tiene hacia w es de costo **2**.

- A ofrece a D una ruta hacia x de costo 1, si D incorpora esta ruta para D tendrá costo **2**, la actual ruta que D tiene hacia x es de costo **1**.

**R27. ¿Por qué es diferente el protocolo de enrutamiento interno de un AS del protocolo de enrutamiento entre sistemas autónomos de Internet?**

**Intra-SA:**

Un protocolo de enrutamiento interno a un sistema autónomo ofrece rutas a redes dentro del SA.

**Inter-SA:**

Un protocolo de enrutamiento entre sistemas autónomos ofrece prefijos pertenecientes a otros SA’s.

**R28. ¿Por qué no son tan importantes las consideraciones de políticas en los protocolos de enrutamiento internos de los sistemas autónomos, como OSPF y RIP, como lo son para el protocolo de enrutamiento entre sistemas autónomos BGP?**

Fuera del SA

Como los SA cuentan con diferentes controles administrativos, puede ser importante que el tráfico originado en un determinado SA no pueda atravesar otro SA específico.

De forma similar, un SA dado puede desear controlar el tráfico de tránsito transportado entre otros SA que pasa a través suyo.

Dentro de un SA

Dentro de un AS, todo está bajo el mismo control administrativo y, por tanto, las políticas desempeñan un papel mucho menos importante en la elección de rutas dentro del AS.

**R33. Para cada uno de los tres métodos generales que hemos estudiado para la difusión (inundación no controlada, inundación controlada y mediante árbol de recubrimiento) indique si las siguientes afirmaciones son verdaderas o falsas. Puede suponer que no se pierde ningún paquete por desbordamiento del buffer y que todos los paquetes son entregados a través de un enlace en el mismo orden en que fueron enviados.**

**Inundación no controlada (flooding)**

Cuando un nodo recibe un paquete de difusión, reenvía copias a todos sus vecinos (excepto al vecino que se lo mando).

**Inundación controlada (controlled flooding)**

Intenta evitar las tormenta de broadcast, decidiendo cuando hacer flooding y cuando no.

**Árbol de recubrimiento (spanning tree)**

Aunque la inundación controlada evitar las tormenta de broadcast, no evitan completamente la transmisión de paquetes de difusión redundantes.

1. **Un nodo puede recibir varias copias del mismo paquete.**

Inundación no controlada: SI

Inundación controlada: SI

Árbol de recubrimiento: NO

1. **Un nodo puede reenviar múltiples copias de un paquete a través del mismo enlace de salida.**

Inundación no controlada: SI

Inundación controlada: NO

Árbol de recubrimiento: NO

**Capítulo 5**

**R13. Suponga que un adaptador a 10 Mbps envía por un canal un flujo infinito de unos (1s) utilizando codificación Manchester. ¿Cuántas transiciones por segundo tiene la señal de salida del adaptador?**

La codificación Manchester tiene una transición en la mitad del periodo de cada bit (los ‘0’ son cambiados por ‘10’ y los ‘1’ son cambiados por ‘01’).

Como la emisión es un flujo infinito de 1s, serán codificados como un flujo de ‘01s’, por lo que por cada 1 enviado hay 2 transiciones.

Dado que el adaptador envía a 10 Mbps, la señal de salida del adaptador será de 20 millones de transiciones por segundo.

**R14. En CSMA/CD, después de la quinta colisión, ¿cuál es la probabilidad de que un nodo seleccione K = 4? ¿A cuántos segundos de retardo corresponde el resultado K = 4 en una red Ethernet a 10 Mbps?**

Como la colisión fue la número 5, el adaptador selecciona aleatoriamente un numero K entre {0, 1, 2,. . ., - 1}, o sea entre {0, 1, 2,. . ., 31}.

Cualquiera de estos valores es elegido con probabilidad 1/32, es decir que la probabilidad de que K sea 4 es **1/32 = 3,13%**.

El tiempo a esperar será (K\*512\*tiempo de un bit) = (4\*512\*tiempo de un bit)

Como la red es de 10 Mbps, en 1 segundo se transmiten 10 Mbits = bits.

Por lo tanto, el tiempo de un bit es 1/ = 0,1 microsegundos.

Concluyendo que el tiempo a esperar será (4\*512\*0,1 microsegundos) = **204,8 microseg**.