Resumen #4 - (r4)

Esteban Ignacio Durán Vargas - 2020388144

IC - 7602 - 2023 I Semestre

La capa red de internet

5.6.4 OSPF—Protocolos de enrutamiento de puerta de enlace interior

El algoritmo de enrutamiento dentro de un sistema autónomo se llama protocolo de puerta de enlace interior (IGP) y entre sistemas es (EGP). El puerto de enlace interior de Internet era un Vector de distancia (RIP) heredado de ARPANET. No servía bien en sistemas grandes y tenía problemas de cuenta hasta infinito y convergencia lenta. La fuerza de tarea de ingeniería de Internet hizo OSPF (Abrir primero la ruta más corta) y se hio norma en 1990. De literatura abierta y apoya una variedad de métrica de distancia y tenía que ser dinámico. Además, como nuevo, era enrutado por servicio (tráfico real y los demás diferentes); balancear la carga en líneas múltiples, necesitaba apoyo de sistemas jerárquicos (ningún enrutador conoce la ruta) y finalmente se necesitó una prevennción para tratar con enrutadores que se conectaban a internet por un tunel. Soporta 3 conexiones: punto a punto entre 2 enrutadores, redes de multiacceso con difusión y sin difusión. En multiacceso se pueden tener múltiples enrutadores que se pueden conectar con otros directamente (LAN/WAN). OSPF resume redes locales, enrutadores y líneas con un costo (distancia, retardo) y calcula la ruta más corta. Usa un nodo para la red y otro para los enrutadores. OSPF divide sistemas autónomos en áreas numeradas; no se traslapan y algunos ni pertenecen a una. Cada sistema autónomo tiene una red dorsal (0) para que cualquier area se conecte a otra. Si 1 enrutador se conecta a 2 áreas es parte de la red dorsal. Dentro de una área cada enrutador tiene la misma base de datos del estado del enlace y ejecuta el mismo algoritmo para calcular la ruta hasta cualquier enrutador (con su respectiva base). 3 tipos de ruta: entre área, dentro y entre sistemas. Entre areas: de origen a dorsal hasta área de destino. OSPF distingue 4 enrutadores: internos (área), límite de área, dorsal y fronterios de sistemas autónomos. Se pueden traslapar. Un enrutador inicia y envía un HELLO a todas sus lineas punto a punto. Según respuestas se conocen a los vecinos. OSPF intercambia información entre enrutadores adyacentes. Se designa un *designado* y es adyacente todos los demás. Los vecinos no intercambian información. Siempre se guarda un designado de respaldo. Cada enrutador inunda periódicamente con *LINK STATE UPDATE* a sus enrutadores adyacentes. Proporciona costos e información. Se confirma la recepción de mensajes de inundación (ack). Los DATABASE DESCRIPTION dan la secuencia de todas las entradas de estado del enlace para el emisor actual para ver quiénes tienen los más recientes. *Link State request* pide información de enlace para verificar los más receintes.

5.6.5 BGP—Protocolo de Puerta de Enlace de Frontera

Entre sistemas se utiliza Protocolo de Puerta de Enlace de Frontera (BGP). Se preocupa por política (no tránsito en ciertos sistemas, o seguridad nacional) y se configura manual. 2 sistemas se consideran conectados si hay una línea entre un enrutador fronterizo en cada uno. 3 categorías de redes: stud, sólo conexión con el grafo de BGP y no transportan tráfico; redes multiconectadas que pueden transportarlo a menos que rechcen; y las de tránsito como dorsales que se ocupan de paquetes de terceros. Los BGP se comunican por TCP. Cada enrutador BGP guarda el registro de la ruta y es un protocolo de vector de ruta y dice qué ruta está usando.

5.6.6 Multidifusión de Internet

Enviar a gran cantidad de receptores con direcciones clase D para un grupo de hosts. 28 bits para identificarlos. No garantiz que se entregue. 2 tipos de direcciones: permanentes (no se preparan y tienen dirección permanente) y temporales (se crean antes de usarse; se unen y se salen). Se implementa mediante enrutadores. Cada minuto se envía multidifusión de hardware y responden con los grupos a los que pertencen. Utilizan IGMP (Protocolo de Administración de Grupo de Internet) con paquetes de pregunta y respuesta. El enrutamiento se crea con árboles de difusión y cad enrutador de difusión intercambia información con sus vecinos con un protocolo de vector de distancia. Se usan optimizaciones para eliminar redes que no interesen.

5.6.7 IP móvil

Las computadoras portatiles deben permanecer conectados si se mueven. Se preparó (IETF) que un host móvil use su dirección en cualquier parte, no se permite cambiar software a hosts fijos, no se permitan cambios de software ni tablas de routing, que la mayoría de hosts no hagan desvío de ruta y que nno haya sobrecarga cuando esté en su casa. Cuando visita un lugar foraneo, contacta a un host foraneo y se registra; este contacta a un agente de base del usuario y da una dirección temporal (propia del agente foráneo). Con un paquete ARP se le pregunta al enrutador para encontrar al agente principal para que el host lo entregue al móvil. Con *ARP gratuito* se reemplaza una entrada del caché que va a quedar inválida porque el móvil va a salir. Cada agente transmite su dirección periódicamente y sus servicios y un host móvil escucha estos anuncios. Por seguridad se usan protoolos de autenticación criptográficos.

5.6.8 IPv6

Se acabarán las IPv4. La IETF propuso una versión que nunca se acabaría que maneje miles de millones de hosts, reduzca el tamaño de tablas de enrutamiento, simplifique protocolos, proporciones seguridad y mayor atención al tipo de servicio, multidifusión (especificación de alcances), que un host sea móvil y no cambie de dirección, que evolucioens y que el viejo coexista. Se tomó la propuesta llamada SIPP (Protocolo Simple de Internet Mejorado), y se le dio la designación Ipv6. Cumple los objetivos pero no es compatible con IPv4. Tiene direcciones más grandes de 16 bytes, se simplifica el encabezado lo cual da rapidez a los paquetes y mejora la velocidad de transporte. Mejor apoyo de opciones (campos obligatorios son opcionales). Además de la autenticación y privacidad y mayor calidad de servicio.

El encabezado principal del IPv6

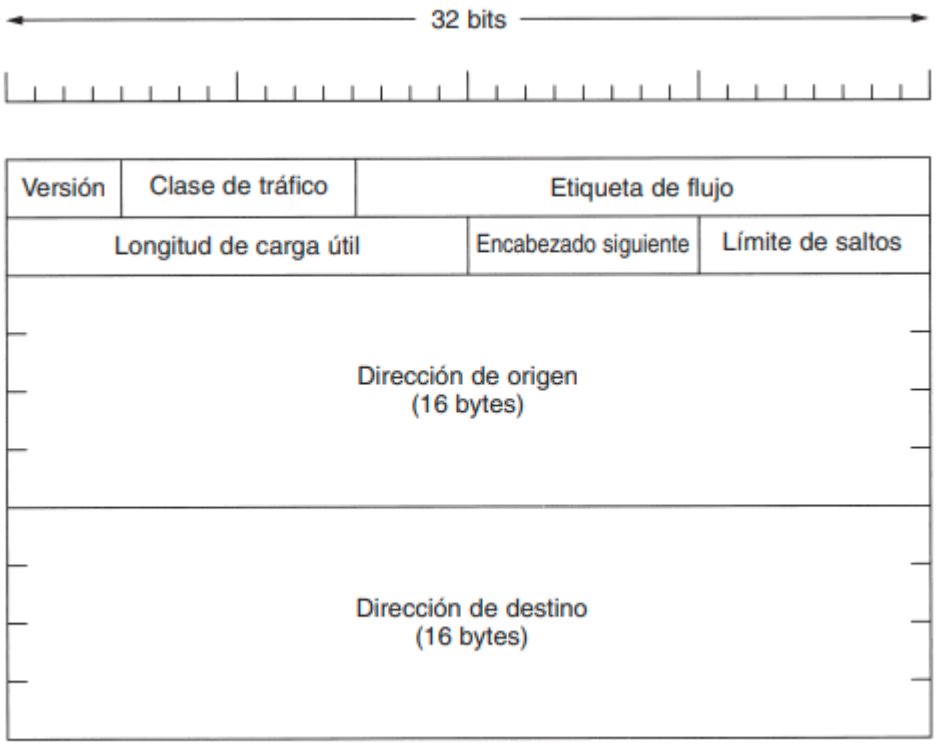

Figura 5-68. Encabezado fijo del IPv6 (obligatorio).

El campo de versión siempre es 6. Clase de tráfico distingue paquetes con requisitos de entrega diferentes en tiempo real (entrega de multimedia). Etiqueta de flujo (experimental) permite a un origen y destino establecer una pseudoconexión con propiedades y requisitos particulares. Cuando es diferente de 0 todos los enrutadores pueden buscarla en sus tablas internas para ver el tratamiento que requiere. Cada flujo está designado por la direcciónde origen, de destino y el número de flujo (varios flujos entre un par de direcciones). Si 2 flujos vienen de hosts diferentes con el mismo número de flujos, el enrutador puede distinguirlos con su dirección de origen y destino. El número de flujo se escoge al azar. Longitud de carga útil indica cuántos bytes siguen al encabeado de 40 bytes. Encabezado siguiente revela el secreto. Puede tener encabezados de extensión siguientesy si es el último se indica el protocolo de transporte. El límite de saltos evita que los paquetes vivan eternamente (tiempo de vida). Dirección de origen y destino de 16 bytes: 8 grupos de 4 hexadecimales que se resumen si hay muchos ceros con :: u omitir ceros a la izquierda. Las IPv4 pueden escribirse con :: antes de la dirección. Comparado con IPv4 se elimnaron los campos IHL (tiene longitud fija), Protocolo (por Encabezado siguiente), los de fragmentación (los hosts determinan dinámicamente el tamaño del datagrama y en vez de fragmentar paquetes grandes devuelve mensaje de error) y el de suma de verificación (ya las capas de data link y de transporte tienen).

Encabezados de extensión

Encabezado de extensión	Descripción
Opciones salto por salto	Información diversa para los enrutadores
Opciones de destino	Información adicional para el destino
Enrutamiento	Ruta total o parcial a seguir
Fragmentación	Manejo de fragmentos de datagramas
Autenticación	Verificación de la identidad del emisor
Carga útil de seguridad encriptada	Información sobre el contenido encriptado

Pueden usarse para información extra. Tienen formato fijo y están codificado como tupla. El tipo es de un byte; los dos primeros bits tienen indican la opción (saltar, descartar paquete y enviar de regreso). La Longitud de 1 byte indica la lognitud y el valor es la información de hasta 255 bytes. El de salto por salto los usan los enrutadores de ruta para: manejo de datagramas de más de 64K y el de longitud se pone en 0. Usa 1 byte para el tipo de encabezado, el siguiente indica la longitud del encabezado. Los 2 bytes siguientes indican el tamaño de datagrama, los últimos 4 bytes indican el tamaño del datagrama. No se permiten menores de 65,536 que harán que el primer enrutador descarte el paquete y devuelva un error de ICMP. Se les conoce como jumbogramas (supercomputadoras). El de opciones de destino son para campos que son interpretados por el host destino. Es para asegurarse para ese nuevo enrutamiento y el software host lo maneje. El de enrutamiento lista los enrutadores que deben visitarse en camino. Los primeros 4 bytes contienen cuatro enteros de 1 byte. El de tipo de enrutamiento da el formato del resto del encabezado. 0 es una palabra reservada de 32 bits a la primera palabra, seguida por algún número de direcciones de IPv6. El de segmentos restantes registra cuántas direcciones de la lista que no ha visto. El de fragmento maneja fragmentación contiene el identificador, número de fragmento y un bit de si siguen más. El host origen puede fragmentar paquetes, los enrutadores no pueden. El autenticación asegura al receptor quién lo envió.

Controversias

El largo de las longitudes queda de 16 bytes. El límite de saltos sentían mal el límite (muy grande) pero tampoco podía ser pequeño. La respuesta fue hacer aumento a todos los campos. Conforme más crezca el internet, más enlaces a larga distancia y haya más saltos. Otro fue el tamaño máximo del paquete. Las supercomputadoras querían más de 64 KB, pero no se puede porque bloquean la línea los muy pequeños. La solución eran los de extensión. Luego la desaparición de la suma de verificación porque ya habían en las capas y gastaba tiempo calculándose. Los hosts móviles que tuvieran la misma dirección de IPv6 o uno foráneo, se trató de incluir soporte explícito a los hosts móviles pero falló por falta de propuestas. Lo principal fue la seguridad. Se quería poner en la de red para que se volviera un servicio estándar pero que las aplicaciones quieren solo de terminal a terminal. La respuesta fue nada más no usar la implementación de seguridad de IP. También se hablaba de que muchos países tienen leyes estrictas de exportación para criptografía por lo que no se podrían extraer de algunos clientes. No hubo controversia en el cambio de 4 a 6. Primero serían islas aisladas de 6 y con el tiempo se expandirán.