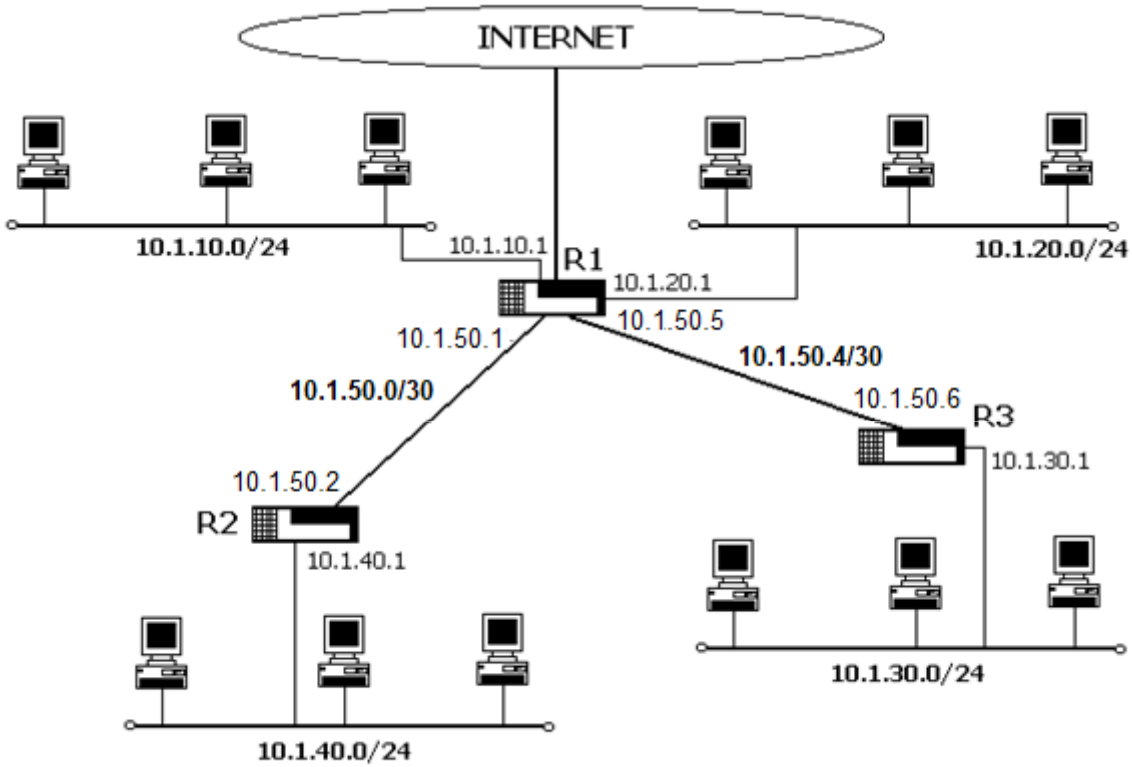
5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.1 Definición de Sistemas Autónomos (Autonomous System - AS)

Red corporativa con conexión a Internet



Sistema autónomo: Conjunto de redes y routers controlados por una única autoridad administrativa (un único gestor de políticas de encaminamiento). Cada AS se identifica con un número, por ejemplo AS 3352 (Telefónica de España S.A.U.).

Política de encaminamiento: Conjunto de estrategias o directrices para decidir cuáles son los caminos óptimos a seguir en una red de comunicaciones.

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.1 Definición de Sistemas Autónomos (AS)

Encaminamiento en sistemas autónomos

Los sistemas autónomos disponen de un conjunto de redes con direccionamiento público y conectividad con cualquier máquina de Internet. Ej: Proveedores de acceso a Internet (ISPs), organismos públicos (Universidades, administración pública, etc).

El encaminamiento óptimo en Internet requiere del intercambio de información de encaminamiento entre todos los routers de Internet: IMPRACTICABLE.

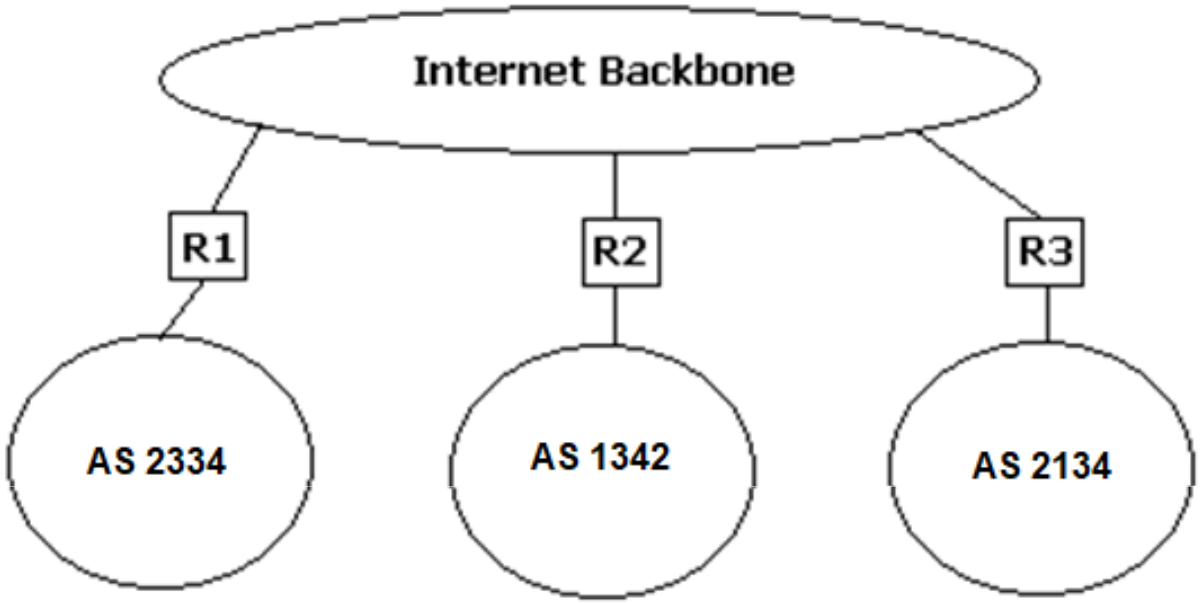
Solución: intercambio de información de encaminamiento a dos niveles

- Intercambio de información de **encaminamiento entre sistemas autónomos** (BGP - Border Gateway Protocol)

- Intercambio de información de **encaminamiento dentro de sistemas autónomos** (RIP - Routing Information Protocol, OSPF - Open Shortest Path First)

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.2 Encaminamiento entre los AS de Internet



El encaminamiento óptimo en Internet requeriría del intercambio de información de encaminamiento entre todas la redes, lo que provocaría:

Tiempo de convergencia de la red elevado: no tolera cambios rápidos en la estructura de la red como fallos en enlaces.

Consumo excesivo de ancho de banda para el intercambio de toda la información de encaminamiento.

5.2 Algoritmos de gestión de tablas de encaminamiento

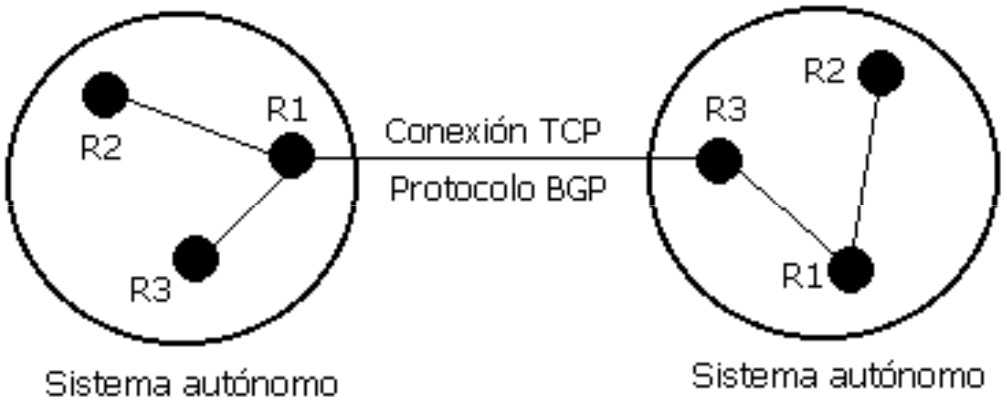
5.2.2 Encaminamiento entre los AS de Internet

Protocolo de encaminamiento BGP (Border Gateway Protocol)

Protocolo para el intercambio de información de encaminamiento entre sistemas autónomos.

Características:

En cada sistema autónomo se especifica un router frontera (o más, en general uno) que dialoga con los routers frontera de otros sistemas autónomos.



La información de encaminamiento se intercambia empleando conexiones TCP (puerto servidor 179) entre routers frontera.

BGP informa acerca de alcanzabilidad y conectividad entre sistemas autónomos (qué redes pertenecen a qué sistemas autónomos)

BGP reduce la información intercambiada comunicando una sola vez todas las redes accesibles a través de un sistema autónomo, y después actualiza la información que se modifica. Además agrupa destinos en una sola denominación.

BGP soporta autenticación para preservar la validez de la información de encaminamiento intercambiada.

5.2 Algoritmos de gestión de tablas de encaminamiento

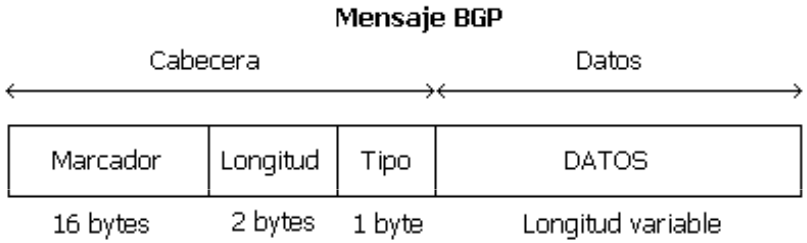
5.2.2 Encaminamiento entre los AS de Internet

Protocolo de encaminamiento BGP (Border Gateway Protocol)

Funcionamiento del protocolo BGP

El protocolo BGP se fundamenta en el establecimiento de una conexión TCP para el intercambio de diferentes mensajes BGP.

Cada mensaje BGP consta de un paquete con cabecera y datos. La cantidad de datos y su formato depende del tipo de mensaje BGP.



Mensaje BGP Open: Es el primer mensaje que se intercambia entre dos routers frontera que establecen la conexión TCP. Se intercambian parámetros como el identificador de sistema autónomo, intervalos de tiempo en el envío de mensajes BGP, etc.

Mensaje BGP Update: Este mensaje informa acerca de destinos existentes en el sistema autónomo y destinos que se han eliminado en el sistema autónomo.

Mensaje BGP Keepalive: Este mensaje informa de que un extremo de la comunicación sigue activo. TCP no controla que los dos extremos estén activos cuando no intercambian datos, por lo que BGP define un mensaje para este propósito.

Mensaje BGP Notification: Este mensaje informa acerca de errores en la comunicación BGP (mensajes BGP con errores: rutas incorrectas o incongruentes) y permite el control en la comunicación (finalización de la conexión, expiración de tiempo de espera de paquetes Keepalive, etc)

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.2 Encaminamiento entre los AS de Internet

Protocolo de encaminamiento BGP (Border Gateway Protocol)

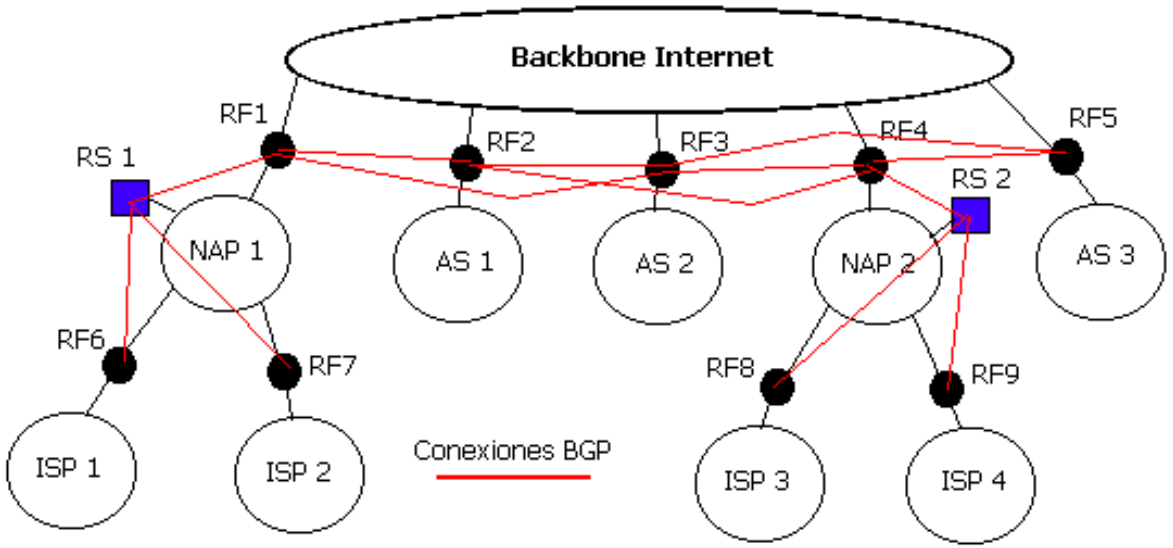
Empleo de BGP en los proveedores de acceso a Internet (ISPs)

Para conseguir conectividad en Internet todos los sistemas autónomos tienen que estar conectados al backbone de Internet para intercambiar mensajes BGP.

No existe disponibilidad para que cualquier ISP esté conectado al backbone de Internet (ARPANET - NSFNET en USA, GEANT en Europa, etc), y existen los denominados Network Access Point (NAPs).

En cada NAP acceden los sistemas autónomos de varios ISPs que intercambian información de encaminamiento con BGP entre el backbone de Internet y los ISPs.

Para evitar inconsistencias en el encaminamiento entre los ISPs, en cada NAP hay un router servidor (RS) con el que dialogan cada uno de los routers frontera de los ISPs para el intercambio de mensajes BGP.



5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.2 Encaminamiento entre los AS de Internet

Protocolo de encaminamiento BGP (Border Gateway Protocol)

Seguridad en el protocolo BGP

La seguridad del protocolo BGP es un elemento crítico en Internet, pues un atacante podría hacer que el tráfico de Internet que circula entre dos países pudiera ser encaminado a través de un tercero intermedio.

Los paquetes BGP son autenticados, por lo que es muy difícil suplantar o modificar un paquete BGP. En la actualidad la principal amenaza es que un router frontera válido emita paquetes BGP con motivos malintencionados (redirección del tráfico en Internet por lugares "no autorizados"). Este tipo de acciones suelen estar asociadas a las agencias de seguridad de los estados para realizar espionaje.


Cases Studies

China acusada de secuestrar el tráfico de Internet usando BGP

Samuel Rodríguez 09/11/2018 Sin comentarios

China ha sido acusada de secuestrar el protocolo de puerta de enlace de frontera o BGP (del inglés Border Gateway Protocol) para llevar a cabo un espionaje encubierto man-in-the-middle a los países y empresas occidentales.

BGP gestiona como se enruta el tráfico entre las subdivisiones de Internet conocidas como **Sistemas Autónomos**. Estos aseguran que el tráfico llega a los servidores correctos, por lo que no tiene que estar andando por ahí, lo que serían malas noticias.

Fuente: cybersecuritynews.es


Los secuestros BGP del gobierno de China

10 noviembre, 2018 Por M. Salinas — Deja un comentario

El gobierno Chino secuestró tráfico de red de usuarios de EEUU para ser redirigido hacía el país Chino.

traceroute from London to Australian Government on May 01, 2017

1	*				0.0
2	x.x.x.x		London	United Kingdom	0.281
3	80.91.248.217	Telia International Carrier	London	United Kingdom	0.318
4	62.115.135.94	Telia Company AB	New York	United States	70.131
5	62.115.137.88	Telia Company AB	Chicago	United States	75.471
6	80.91.248.157	Telia International Carrier	Ashburn	United States	76.056
7	218.30.53.53	Chinanet POP in American	Reston	United States	78.639
8	202.97.49.229	CHINANET backbone network	Los Angeles	United States	240.579
9	202.97.52.189	CHINANET backbone network	Shanghai	China	444.718
10	202.97.63.122	CHINANET backbone network	Hong Kong	Hong Kong	475.377
11	*				0.0
12	*				0.0
13	210.80.3.121	Verizon Asia Pte Limited	Hong Kong	Hong Kong	345.421
14	210.80.49.53	Verizon Asia Pte Limited	Sydney	Australia	430.813
15	210.80.32.98	Verizon Asia Pte Limited	Sydney	Australia	430.653
16	*				0.0
17	*				0.0
18	203.6.76.1	nactmail.defence.gov.au	Sydney	Australia	451.869

Fuente: hispasec.com

La protección ante estos ataques pasa por la vigilancia continua del tráfico BGP en Internet y detectar redirecciones de tráfico "anómalas" entre diferentes regiones del mundo.

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.2 Encaminamiento entre los AS de Internet

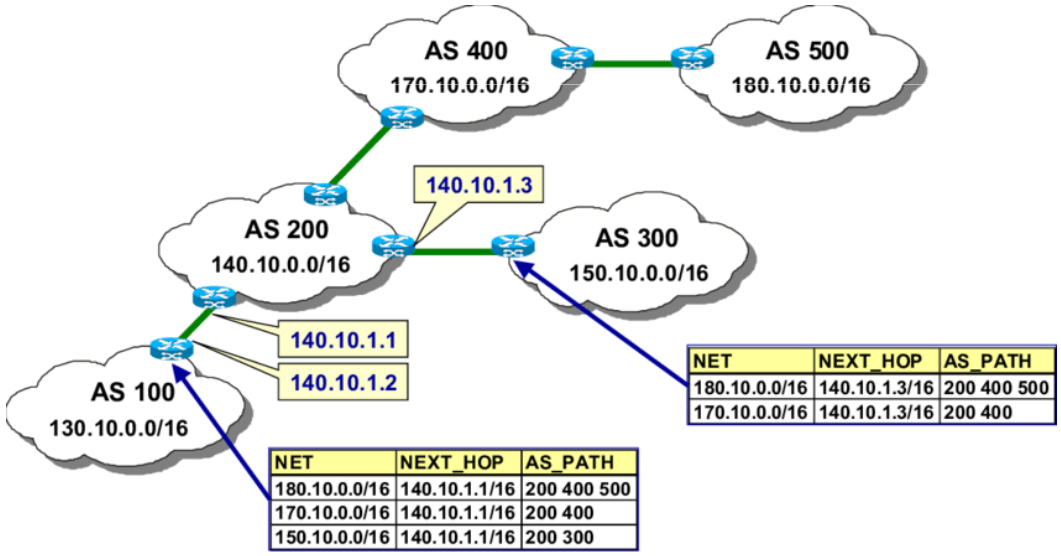
Protocolo de encaminamiento BGP (Border Gateway Protocol)

Conclusiones

BGP sólo informa de accesibilidad, no de rutas a seguir o rutas de menor coste (no entiende métricas).

BGP establece conexiones entre pares de routers frontera, por lo que tiene que existir conectividad entre todos los routers frontera de Internet.

BGP informa sobre destinos existentes y no existentes, evitando así la presencia de mensajes ICMP destino no alcanzable entre diferentes ISPs.



Ejemplo de tablas BGP. Autor: Achim Autenrieth. Fuente: www.researchGate.net

5.2 Algoritmos de gestión de tablas de encaminamiento

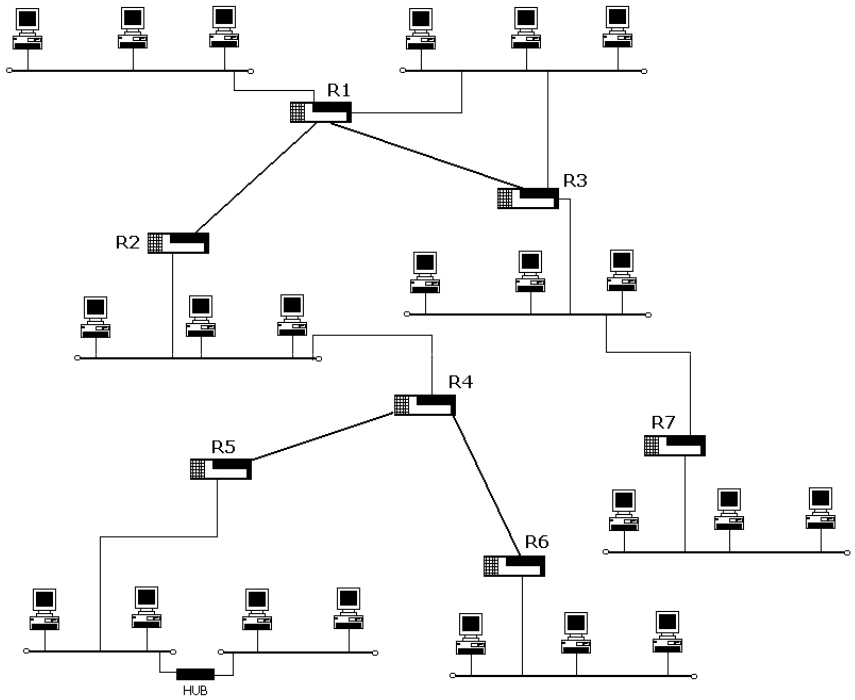
5.2.3 Encaminamiento dentro de los AS de Internet

Tablas de encaminamiento en un sistema autónomo

El encaminamiento estático (tablas de rutas fijas) no es adecuado:

- Cambios en la red implican actualización de tablas en todos los routers (ejemplo: añadir una nueva red)

- Tiempo de respuesta ante fallos elevado (ejemplo: en caso de fallo de un enlace, la actualización de tablas es manual)



Es necesario un mecanismo de configuración y actualización de tablas de encaminamiento automático

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los AS de Internet

Protocolo de Información de Encaminamiento (RIP)

El origen de RIP (Routing information protocol – RFC 1058) está en un sofware desarrollado por la Universidad de Berkeley para proporcionar consistencia y fiabilidad en la interconexión de redes locales con sistema operativo BSD UNIX.

Se fundamenta en un algoritmo de vector de distancia (Algoritmo de Bellman-Ford)

Cada router dispone de una tabla con información de destinos y una métrica (número de saltos) para alcanzar el destino.

Cada router propaga la información de sus rutas conocidas a través de mensajes en la red, y los routers que la reciben actualizan sus tablas si encuentran rutas más cortas a un mismo destino.

Tabla Router K

Destino	Distancia	P. Enlace
Red 1	1	Directa
Red 2	1	Directa
Red 4	8	Router L
Red 17	5	Router M
Red 24	6	Router J
Red 30	2	Router Q
Red 42	2	Router J

Mensaje RIP Router J

Destino	Distancia
Red 1	2
Red 4	3
Red 17	6
Red 21	4
Red 24	5
Red 30	10
Red 42	3

Tabla Router K actualizada

Destino	Distancia	P. Enlace
Red 1	1	Directa
Red 2	1	Directa
Red 4	4	Router J
Red 17	5	Router M
Red 24	6	Router J
Red 30	2	Router Q
Red 42	2	Router J
Red 21	5	Router J

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los AS de Internet

Protocolo de Información de Encaminamiento (RIP)

Al informar el router J que la Red 42 tiene un aumento de coste, indica que ha habido un fallo en algún enlace, por lo que la ruta a la Red 42 en el router K debe ser modificada.

Para solventar este problema, RIP introduce una serie de reglas adicionales:

Para cada entrada en la tabla de rutas (distancia, métrica) existe un temporizador (180 segundos). Si la ruta no es informada (distancia, métrica) de nuevo en ese tiempo, es eliminada. Ej: En el caso anterior, al cabo de 180 segundos la ruta (Red 42, 2) es eliminada, y se sustituirá por (Red 42, 4).

Existe un número máximo de saltos para la métrica de RIP que es 16. Esto evita problemas de convergencia del algoritmo, es decir, llegar a una solución estable.

Propagación de la información con RIP (versión 1 – RFC 1058)

Los mensajes RIP con información de las rutas de un router se envían dentro de paquetes UDP.

Existen mensajes RIP de petición y respuesta, de forma que los paquetes RIP de petición son enviados al puerto UDP 520 del router, y los paquetes RIP de respuesta proceden del puerto UDP 520.

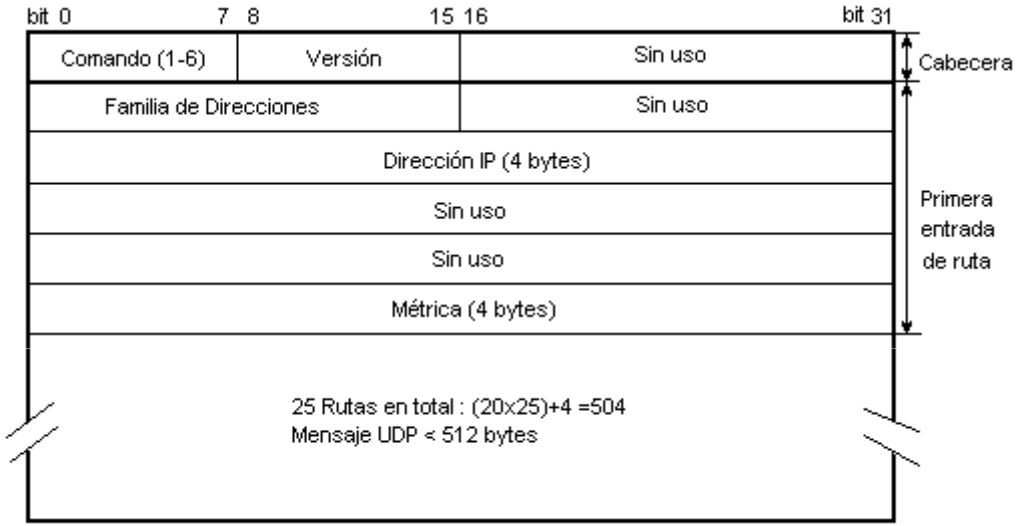
Para que los mensajes RIP lleguen a todas las estaciones del segmento físico (difusión de la información), los paquetes UDP son enviados a la dirección de broadcast de la red IP donde se difunden.

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los AS de Internet

Protocolo de Información de Encaminamiento (RIP)

Formato del mensaje RIP versión 1



No es posible especificar la máscara de red del destino ni el router a través del cual se alcanza el destino.

El envío de mensajes RIP a la dirección de broadcast hace que las máquinas que no soportan RIP procesen paquetes hasta la capa de transporte (UDP).

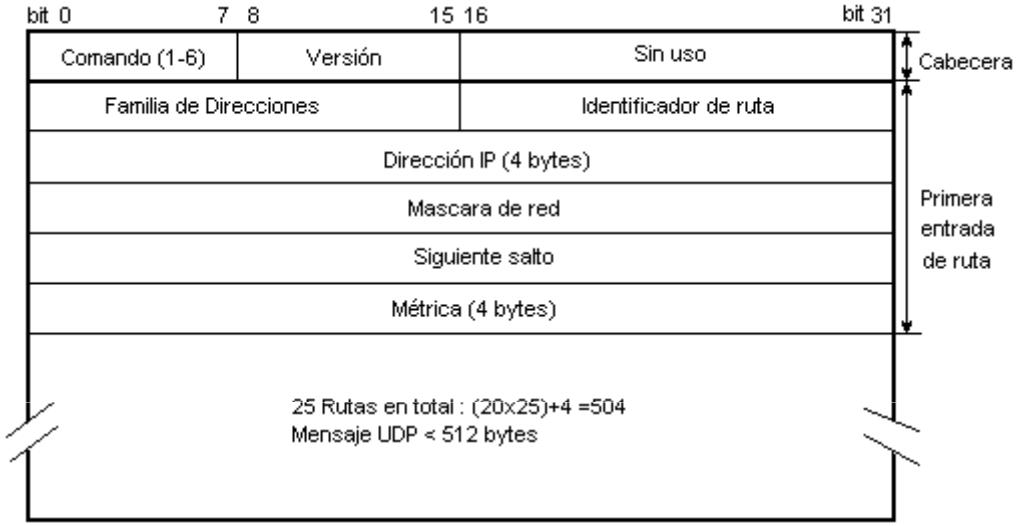
Para solventar estos problemas se introduce la versión 2 de RIP.

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los AS de Internet

Protocolo de Información de Encaminamiento (RIP)

Propagación de la información con RIP (versión 2 – RFC 2453)



Formato del mensaje RIP versión 2

Los mensajes RIP son enviados a la dirección IP 224.0.0.9 (dirección IP de multicast), de forma que sólo las estaciones que tienen habilitado contestar a esa dirección procesan el paquete.

CONCLUSIONES

RIP permite el encaminamiento dinámico en redes de tamaño pequeño (hasta 16 saltos) con una estructura sencilla (inexistencia de muchos bucles).

RIP presenta problemas de convergencia lenta ante cambios en la red y posibilidad de que se introduzcan bucles infinitos. Para evitar esto emplea estrategias como temporizadores y un número máximo de saltos.

5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los AS de Internet

Protocolo Abierto del Camino más Corto Primero (OSPF – RFC 1583)

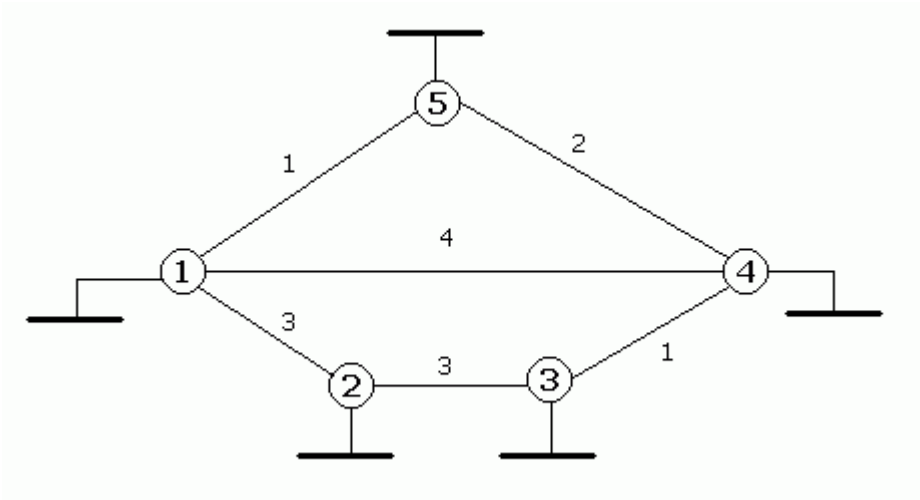
OSPF (Open Shortest Path First) es una alternativa al protocolo RIP a la hora de establecer las métricas de la rutas.

RIP sólo tiene en cuenta el número de saltos, pero no la velocidad de transferencia, por lo que las rutas con menos saltos no tienen porque ser las más rápidas.

OSPF se fundamenta en el denominado estado del enlace, asignando un coste dependiendo de las características del enlace (alta velocidad, baja velocidad, activado, desactivado, etc.).

El conjunto de routers de una red que emplean OSPF conforman un grafo, donde se determinan las rutas más cortas entre cualquier par de nodos (router, o en definitiva redes) del grafo (red).

OSPF emplea el algoritmo de Dijkstra para determinar las rutas de menor coste en la red.



5.2 Algoritmos de gestión de tablas de encaminamiento

5.2.3 Encaminamiento dentro de los AS de Internet

Protocolo Abierto del Camino más Corto Primero (OSPF – RFC 1583)

Para determinar las rutas de menor coste es necesario intercambiar información entre los routers que emplean OSPF. Esta información se intercambia en forma de mensajes de diferentes tipos.

Los mensajes OSPF se encapsulan dentro de paquetes IP dirigidos a la dirección de multicast 224.0.0.5 (todos los routers OSPF) y 224.0.0.6 (routers OSPF designados).

Mensajes OSPF

OSPF Hello: Permite determinar qué vecinos tiene accesible un router.

OSPF Database description: Informa de la topología de la red de comunicaciones.

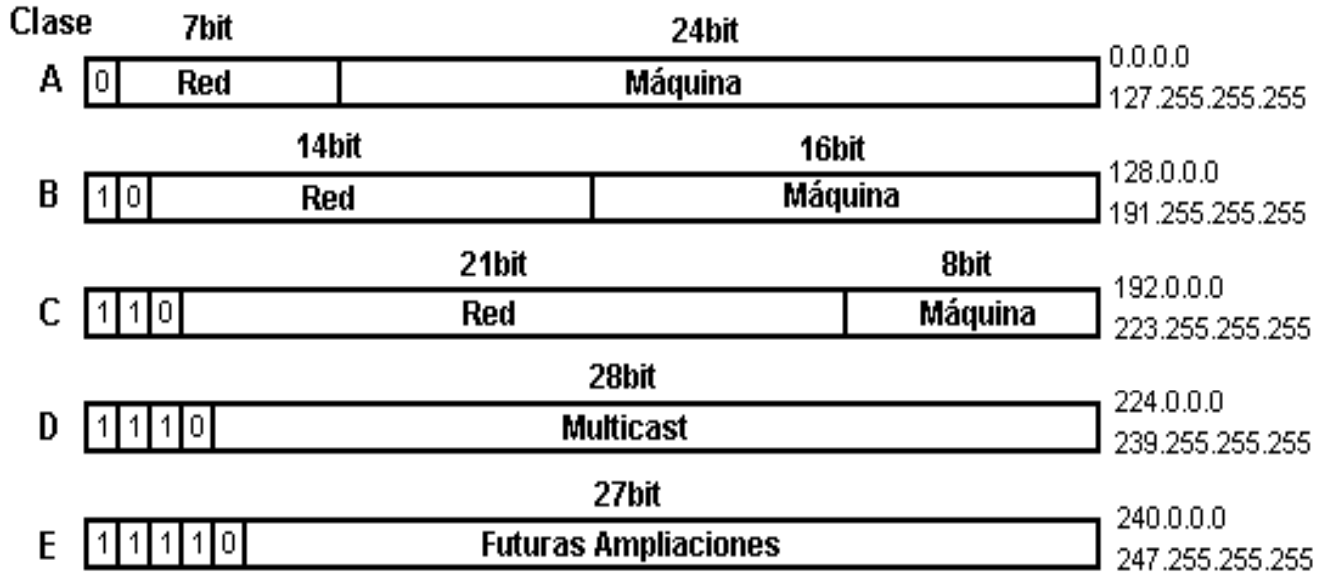
OSPF Link status request: Permite solicitar a los routers vecinos información acerca de los enlace activos.

OSPF Link status update: Un router informa a sus vecinos del estado de sus enlaces.

5.3 Multicasting

5.3.1 Definición

El término multicasting hace referencia a la multidifusión, que es aplicable al direccionamiento IP.



Para este propósito está definida la clase D del direccionamiento IP, pudiendo establecer 2^{28} direcciones de multidifusión, o lo que es lo mismo 2^{28} direcciones de grupos de máquinas.

Cada máquina en Internet procesa los paquetes IP dirigidos a su dirección IP y a la dirección IP de difusión de su red. Adicionalmente, una máquina de Internet puede ser configurada para que pertenezca a cualquier grupo de multidifusión, por lo que también procesaría los paquetes dirigidos al grupo al que pertenezca.

5.3 Multicasting

5.3.1 Definición

Cada dirección de multidifusión tiene asociada una función específica, de forma que cada dirección identifica grupos de máquinas en Internet que llevan a cabo una función común.

Dirección Multicast	Denominación del grupo
224.0.0.0	Reservada
224.0.0.1	Todos los equipos de la subred
224.0.0.2	Todos los routers en la subred
224.0.0.5	Routers OSPF
224.0.0.6	Routers OSPF designados
224.0.0.9	Routers RIPv2

Una máquina que pertenece a un grupo de multicast podría estar en cualquier lugar de Internet, por lo que los routers de interconexión entre redes (routers troncales) tendrían que propagar los paquetes IP dirigidos a direcciones de multicast (hay que habilitar el router para ello).

En la actualidad el encaminamento de paquetes de multidifusión NO está habilitado en los troncales de Internet, debido a la imposibilidad de controlar la seguridad de qué máquinas pertenecen o no a un grupo de multidifusión.

Existe una restricción, y es que los paquetes dirigidos a grupos de gestión de encaminamiento (desde la dirección 224.0.0.1 a la 224.0.0.255) no son propagados nunca (para evitar congestionamiento y problemas de convergencia de los algoritmos de encaminamiento).

5.3 Multicasting

5.3.2 Gestión de la multidifusión

Cuando un paquete IP se envía a una dirección multicast ¿ qué dirección de nivel de enlace se emplea ?

Si el nivel de enlace soporta multicasting (Ej: Ethernet) cada dirección IP de multicast tiene asociada una dirección de enlace de multicast.

Si el nivel de enlace no soporta multicasting cada dirección IP de multicast tendrá asociada la dirección de broadcast del nivel de enlace, o el caso de redes punto a punto el otro extremo del enlace.

IGMP – Protocolo de Gestión de Grupo en Internet

Este protocolo, que al igual que ICMP funciona sobre IP estableciendo diferentes tipos de mensajes IGMP, permite la gestión del encaminamiento con multicasting.

Básicamente, el protocolo define dos funcionalidades básicas:

Cuando una estación se añade a un grupo multicast, envía un mensaje IGMP al grupo indicando que se ha añadido, de forma que los routers del grupo actualizan rutas para enviar paquetes multicast a la nueva estación.

Cada cierto tiempo, los routers de un grupo multicast sondean a los miembros del grupo de su red local para saber si están activos. Si no hay ningún miembro activo, el router informa a los demás routers que en esa red no hay miembros y no hay que reenviar paquetes multicast.

Aplicaciones

Mecanismo de propagación de información en algoritmos de encaminamiento para evitar carga computacional en dispositivos que no son routers y que no emplean el algoritmo.

Reducción de consumo de ancho de banda en la transmisión de streaming de audio y vídeo en los operadores de telecomunicación que ofrecen este servicio, pero NO en proveedores a través de Internet (Youtube, Amazon, Netflix, etc.).

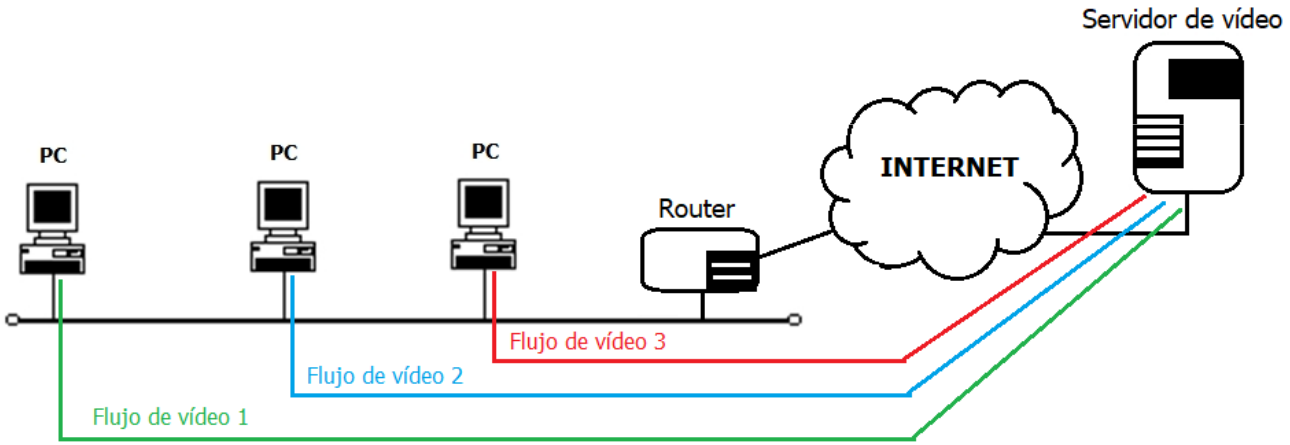
5.3 Multicasting

5.3.3 Transmisión de TV en redes IP

La transmisión de vídeo en Internet (conocido como *streaming*) consiste en la transmisión de flujos de vídeo comprimidos (formato MPEG) encapsulados en paquetes IP.

Los flujos de vídeo se generan en servidores de vídeo en Internet (Youtube, Netflix, etc.) que establecen conexiones TCP o UDP con las direcciones IP de los equipos que los visualizan (unidifusión).

Estos flujos de vídeo se caracterizan por necesitar una velocidad de transmisión para el envío de los paquetes IP de manera que el flujo de vídeo se visualice correctamente. Por ejemplo, un flujo de vídeo de calidad 4K, empleando la compresión MPEG-4, precisa de una velocidad de transmisión de unos 26 Mbps.



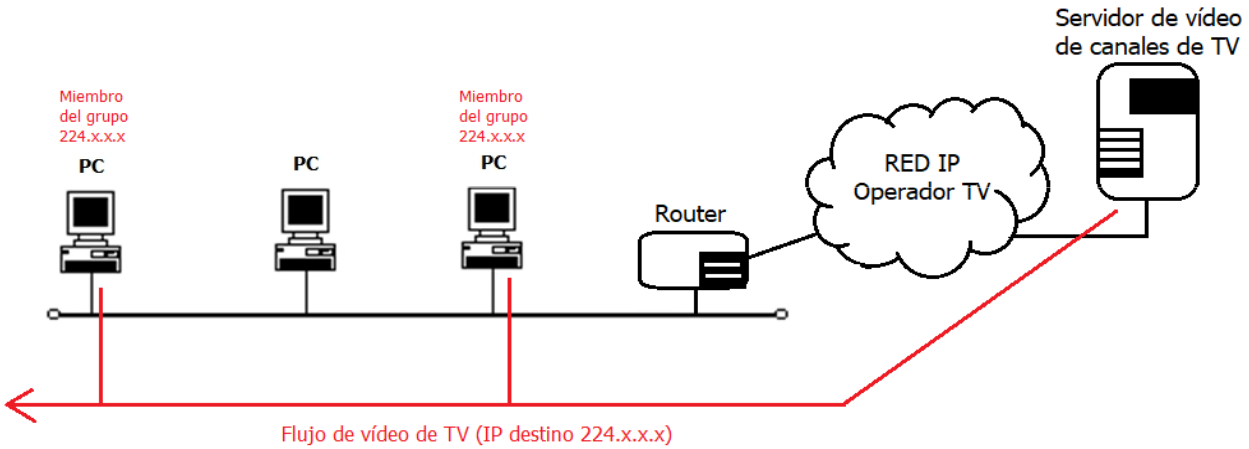
Así, el servidor de vídeo precisa de una conectividad a Internet con una velocidad de transmisión muy elevada, mayor cuantos más flujos de vídeo simultáneos tenga que transmitir.

5.3 Multicasting

5.3.3 Transmisión de TV en redes IP

La transmisión de un canal de TV se caracteriza porque el flujo de vídeo es el mismo a TODOS los equipos. Por ello, la multidifusión puede emplearse para realizar el envío de UN único flujo de vídeo a una dirección IP de multicast (224.x.x.x) que será procesado por aquellos equipos que pertenezcan a esa dirección de grupo.

Sin embargo, la multidifusión no está ACTIVA en Internet a nivel global, por lo que sólo puede ser empleada dentro de cada Sistema Autónomo (AS) como son los operadores de telecomunicaciones que ofrecen servicio de TV (Movistar, MasOrange, Vodafone, etc.).



De esta manera, solo se transmite un único flujo de paquetes IP para cada canal de TV desde el servidor de vídeo y dirigido a una dirección de multidifusión (224.x.x.x). Todos los equipos de la red del operador reciben el flujo de paquetes, de manera que solo los equipos que pertenezcan al grupo de multidifusión del canal de TV (dirección 224.x.x.x) procesan y visualizan el flujo de vídeo.

Este mecanismo reduce notablemente la necesidad de velocidad de transmisión necesaria en el servidor de vídeo.

5.4 IPv6 (RFC 2460)

5.4.1 Limitaciones de IPv4

La principal limitación que ha conducido a la introducción de una nueva versión de protocolo IP es la limitación en el direccionamiento IPv4 a 32 bits.

IPv6 introduce direcciones IP de 128 bits, lo que supone disponer de aproximadamente $6x10^{23}$ direcciones por metro cuadrado de la superficie terrestre.

La fragmentación provoca un efecto nocivo en el rendimiento de la red, por lo que IPv6 no permite la fragmentación de un paquete IP en un router intermedio.

La fragmentación se realiza en el origen, determinando éste el valor de MTU mínimo en el camino de origen a destino, o bien tomando el valor mínimo de MTU que tiene que soportar una red IPv6, 1280 bytes.

IPv6 mejora el campo de opciones de IPv4, permitiendo un uso más eficiente en el encaminamiento.

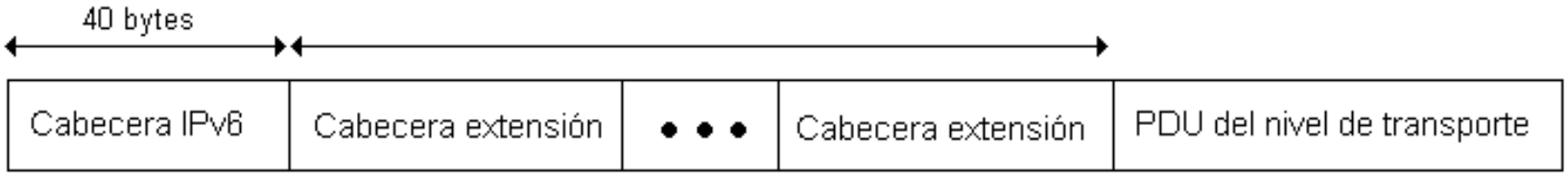
IPv6 mejora la gestión de QoS en IP. Para ello, además de identificar clases de tráfico (prioridades) con un campo equivalente al TOS de la cabecera IPv4, IPv6 identifica flujos de tráfico.

En IPv6 se pueden identificar flujos de tráfico de la misma prioridad, lo que es muy interesante para gestionar en los routers varios flujos de audio y vídeo procedentes de un mismo equipo.

5.4 IPv6 (RFC 2460)

5.4.2 Cabecera IPv6

Una PDU (*Protocol Data Unit* – Unidad de Datos de un Protocolo) de IPv6 consta de una cabecera fija y común a todos los paquetes (cabecera IPv6), un conjunto de cabeceras de extensión y la PDU del nivel superior (transporte).



Se han definido las siguientes cabeceras de extensión:

Cabecera de opciones salto a salto: Define acciones a tomar en cada router que atraviesa el paquete (generar mensajes ICMP, descartar paquetes, priorizar el paquete, etc.)

Cabecera de encaminamiento: Proporciona un encaminamiento adicional, similar al encaminamiento en el origen de IPv4.

Cabecera de fragmentación: La fragmentación en IPv6 se realiza en el origen, y es el destinatario el encargado del reensamblado del paquete. Emplea un mecanismo similar a IPv4.

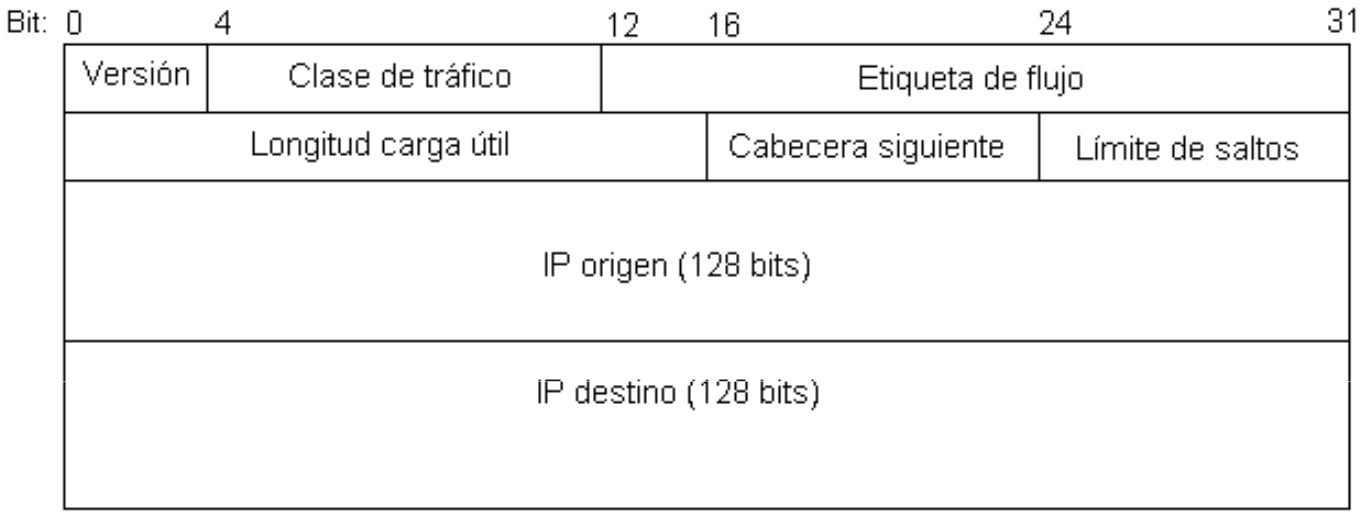
Cabecera de opciones para el destino: Contiene información opcional para ser examinada en el nodo destino.

Cabecera de autenticación y encapsulado de seguridad: Cabeceras AH y ESP de IPSEC (cifrado y autenticación de paquetes IP).

5.4 IPv6 (RFC 2460)

5.4.2 Cabecera IPv6

Formato de la cabecera IPv6



Clase de tráfico: Equivalente al campo TOS de IPv4. Permite establecer clases distintas de tráfico.

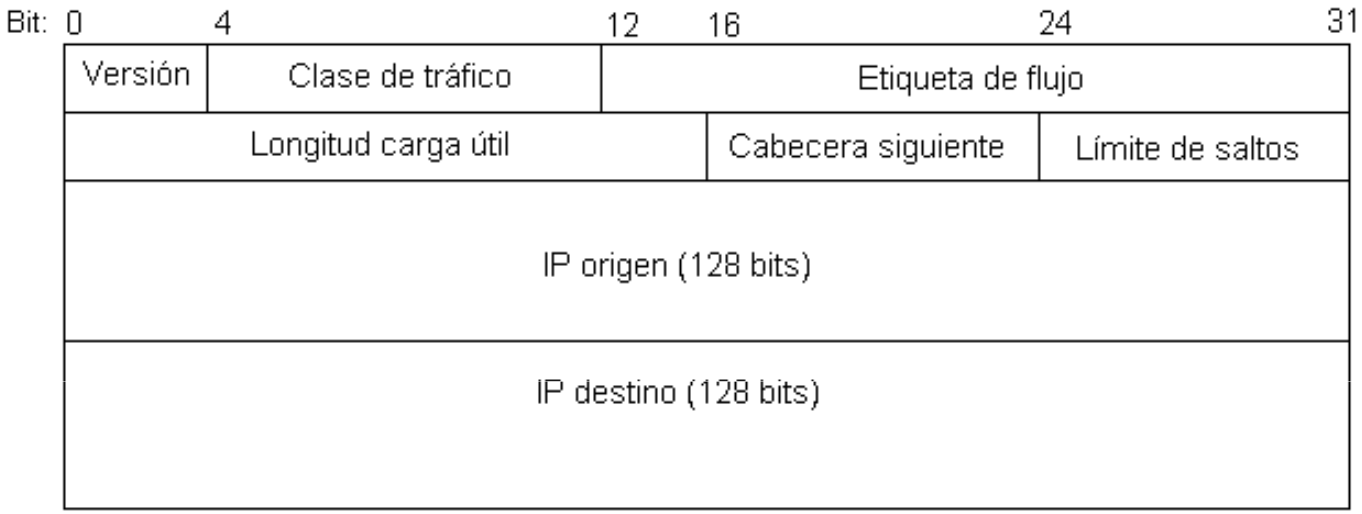
Etiqueta de flujo: Permite identificar flujos de paquetes entre dos aplicaciones origen y destino. Un flujo puede estar compuesto de varias conexiones TCP (intercambio de ficheros con varias conexiones simultáneas). Una aplicación puede generar varios flujos (un aplicación de videoconferencia genera un flujo de audio y otro de vídeo que los routers deben encaminar de manera diferente).

Longitud carga útil: Tamaño en bytes de las cabeceras de extensión y la PDU de nivel superior.

5.4 IPv6 (RFC 2460)

5.4.2 Cabecera IPv6

Formato de la cabecera IPv6



Cabecera siguiente: Especifica qué cabecera sigue a la IPv6. Puede ser una cabecera de extensión o un protocolo de nivel superior (TCP, UDP).

Límite de saltos: Establece el número máximo de saltos de un paquete IP, al igual que en IPv4.

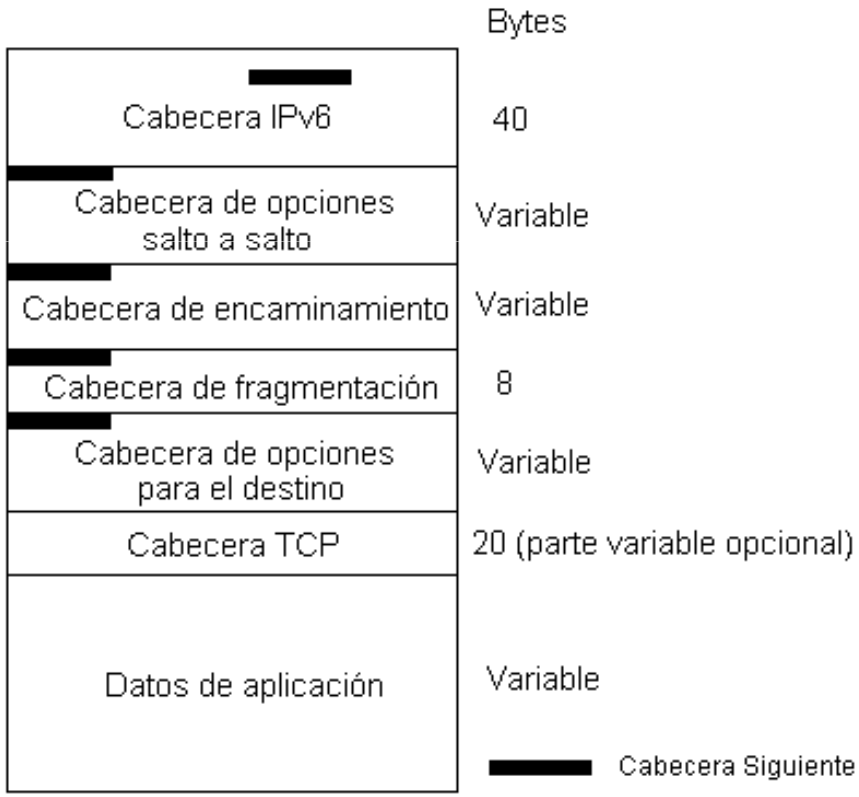
Dirección IP origen y destino: Especifica entre qué interfaces se intercambian los datos.

5.4 IPv6 (RFC 2460)

5.4.2 Cabecera IPv6

Anidamiento de cabeceras extendidas en IPv6

Cuando un dispositivo analiza un paquete IPv6 recorre todas las cabeceras existentes (IPv6 y extendidas) empleando el campo 'cabecera siguiente', hasta que encuentra la cabecera de nivel superior y envía los datos a la capa superior.



5.4 IPv6 (RFC 2460)

5.4.3 Direcciones IPv6 (RFC 2373)

IPv6 introduce un nuevo sistema de direccionamiento conceptualmente distinto al de IPv4.

Al establecer direcciones IP de 128 bits desaparece el problema de la falta de direcciones IP, y el concepto de dirección IPv6 se asigna a un interfaz de comunicación, no a un equipo.

Así, un dispositivo IPv6 está identificado por cualquiera de las direcciones IP de sus interfaces.

Una característica fundamental de las direcciones IPv6 es que son dinámicas y únicas. La dirección IPv6 asignada a un interfaz es un valor de 128 bits combinación de la MAC del interfaz y del proveedor de acceso que emplea.

Así, el proceso de encaminamiento es mucho más rápido en los routers, pues permite establecer jerarquías de direccionamiento más realistas como por operador, proximidad geográfica, etc.

Además, IPv6 permite tres tipos distintos de direcciones IP:

a) Direcciones de unidifusión (*unicast*): Identifican a un interfaz individual.

b) Direcciones de multidifusión (*multicast*): Identifica a un conjunto de interfaces que pertenecen a un grupo definido.

c) Direcciones de monodifusión (*anycast*): Identifica a un conjunto de interfaces que pertenecen a un grupo, pero el paquete sólo se entrega a la interfaz más cercana (según la métrica de distancia de los protocolos de encaminamiento).

5.4 IPv6 (RFC 2460)

5.4.3 Direcciones IPv6 (RFC 2373)

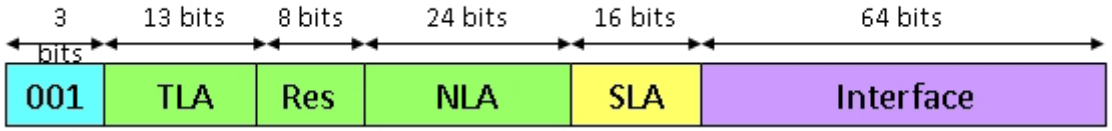
La notación de una dirección IPv6 se establece en 8 grupos de 4 dígitos hexadecimales separados por el símbolo ':'.

2001:BA98:7654:3210:FEDC:BA98:7654:3210

Es posible reducir la notación de una dirección IPv6 omitiendo los grupos que contengan ceros y empleando doble **':'**.

2001:BA98:0000:3210:0000:BA98:0000:3210 ⇔ 2001:BA98::3210::BA98::3210

Formato de una dirección unicast IPv6



TLA: *Top-Level Aggregation*. Identificador asociado a una zona geográfica del planeta (África, Europa, Norteamérica, etc.).

Res: Uso reservado, para ampliar el TLA o NLA.

NLA: *Next-Level Aggregation*. Identificador asociado a proveedores de Internet y empresas globales a nivel nacional o regional (Telefónica, Vodafone, BT, RedIris, etc.).

SLA: *Site-Level Aggregation*. Identificador de redes dentro de un identificador NLA (se pueden crear hasta 65536 subredes).

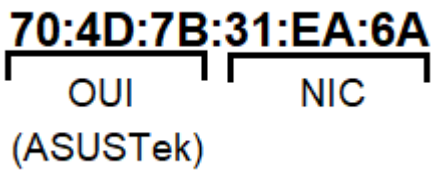
Interface ID: Identificador asociado a un dispositivo, basado en la dirección MAC y con el formato EUI-64.

5.4 IPv6 (RFC 2460)

5.4.3 Direcciones IPv6 (RFC 2373)

Formato EUI-64 de IPv6

Las direcciones MAC (empleadas en la identificación de interfaces Ethernet y Wi-Fi, entre otros) tienen una longitud de 48 bits, divididos en dos grupos de 24 bits: el OUI (Organizationally Unique Identifier) y el NIC (Network Interface Controller).



Los 48 bits de la dirección MAC se emplean para crear el Interface ID de 64 bits añadiendo 16 bits a valor fijo (FF:FE) entre el OUI y el NIC.

70:4D:7B:FF:FE:31:EA:6A

Dirección EUI-64

Con este esquema, cualquier dispositivo conectado a una red IPv6 tiene un valor dinámico (cambia según la red física en la que se conecte – valores TNA, NLA, SLA) pero **único y reservado para él** (debido a la MAC única).

Esta característica facilita la movilidad (conocimiento de la ubicación) y titularidad (identificación) de los dispositivos que emplean el protocolo IPv6.

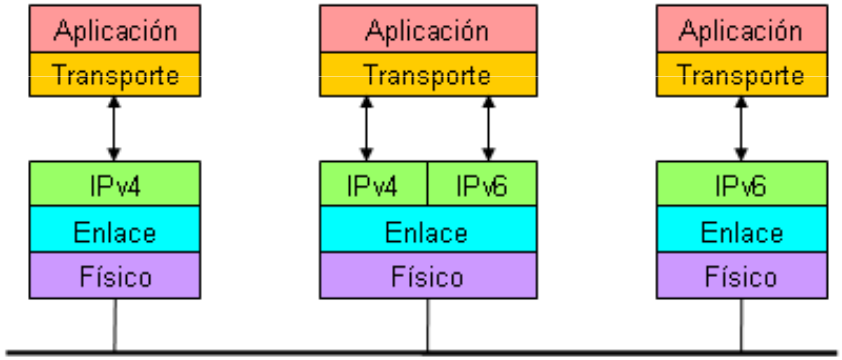
5.4 IPv6 (RFC 2460)

5.4.4 Transición IPv4 – IPv6

Debido a la incompatibilidad entre el protocolo IPv6 e IPv4 (formato de paquete y direccionamiento diferentes) es necesario una estrategia para el cambio de las redes IPv4 a IPv6.

Esta transición, actualmente, está compuesta por troncales de red que operan mayoritariamente en IPv6, dispositivos de usuario final que operan en IPv4 y dispositivos finales que operan en IPv6 (en fase de despliegue).

Un dispositivo IPv4 sólo puede tener conectividad con dispositivos con IPv4, por tanto, si es necesaria conectividad IPv4-IPv6 entre dispositivos es necesario disponer de dos pilas de protocolo IP en paralelo (con una dirección IPv4 y otra IPv6).



Cuando la conectividad es entre equipos con la misma versión de protocolo (IPv4 o IPv6) y deben atravesar una red intermedia con una versión de IP distinta, se recurre al procedimiento del túnel.

Este procedimiento encapsula un paquete IPv4 (IPv6) como dato dentro de un paquete IPv6 (IPv4) para su transporte en esa red intermedia.

Más información: https://www.ripe.net/publications/ipv6-info-centre