RIP
Routing
Information
Protocol

Routing Information Protocol

- Protocolo de vector distancia
- RIP: definido en RFC1058
- RIPv2: Internet Standard (STD) 56 o RFC 2453
- Adecuado como IGP en redes chicas

Funcionamiento

- RIP mantiene una tabla con entradas para cada destino. Las entradas contienen el próximo salto y la distancia
- Periódicamente envía actualizaciones de rutas a sus vecinos con la información de destinos y distancias que conoce
- Cuando recibe una actualización de un vecino, suma el costo recibido de cada destino con el costo del enlace con el vecino
- Si obtiene una distancia menor o igual a la que tenía para el destino, toma la nueva
- Si la distancia es mayor, desestima la información

Métrica

- La métrica usada en RIP es “cantidad de saltos” para indicar la distancia a un destino
- Para atacar el problema del conteo a infinito se limita la cantidad de saltos a 16
- Cuando una entrada llega a una distancia de 16 se considera no accesible
- Utiliza además el mecanismo de horizonte dividido para paliar el problema del conteo a infinito

Actualizaciones

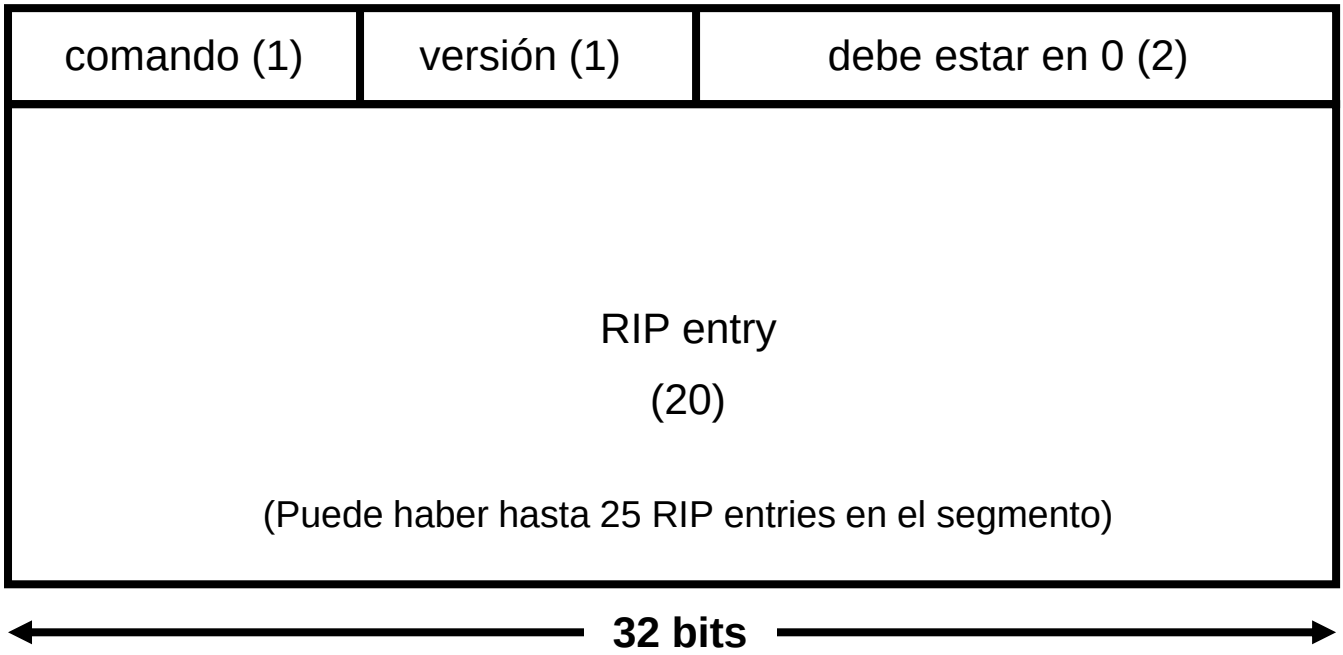
- **Si no se reciben actualizaciones de una determinada ruta por un tiempo (múltiplo del período, por si hay pérdidas) se da de baja la ruta**
- **Se pueden enviar actualizaciones con distancia infinito (16) para indicar que un destino es inaccesible**
- **Cuando un enrutador recibe una actualización y descubre una mejor ruta para un determinado destino, actualiza su tabla de ruteo y envía un paquete de actualización**
- **Con RIP los enrutadores mantienen solamente la mejor ruta para un determinado destino**

Protocolo RIPv1

- **Obsoleto**
- **No soporta máscaras variables, se maneja con las clases A, B y C originales**
- **Para cada destino se almacena en el router al menos la siguiente información:**
  - La dirección IP del destino
  - La métrica (saltos) para llegar a él
  - La dirección IP del próximo salto
  - Banderas para indicar el estado de actualización
  - Temporizadores asociados a la entrada

Mensajes RIPv1

- **RIP usa UDP para enviar los mensajes entre los enrutadores (puerto UDP 520)**
- **Se envía a la dirección de broadcast**
- **Formato del mensaje (tamaños en bytes):**



Contenido de los campos

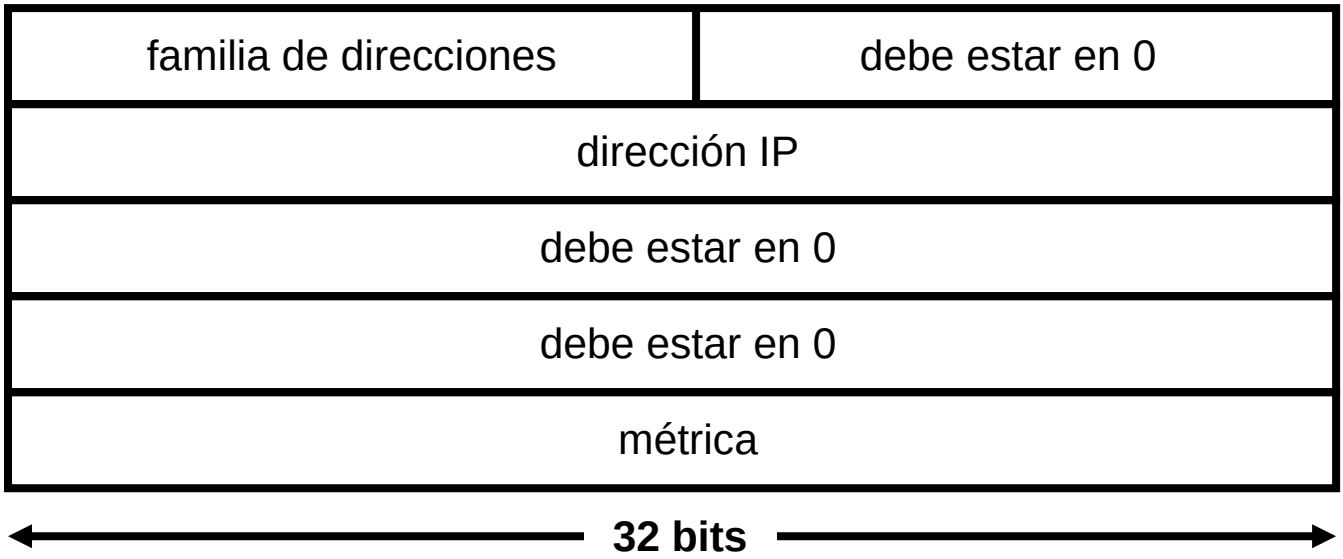
- **Comandos:**
  - **Request (1)**

    Pedido de envío de tabla de rutas. Normalmente se hacen pedidos por broadcast cuando un router arranca, pero pueden ser a un router particular
  - **Response (2)**

    Información de tabla de rutas en respuesta a un "request" o enviadas por un update periódico
  - **Traceon (3), traceoff (4) (obsoletos), reservado para SUN (5)**
- **Versión=1**

RTE (route entry)

- **Las RIP entry para rutas (RTE) tienen el siguiente formato:**



- **Familia de direcciones = IP (2)**
- **Tabla de destinos (dirección IP)**
- **Distancia (métrica)**

Temporizadores

- **Generación de actualizaciones (responses) = 30 segundos**

  Para evitar la sincronización de actualizaciones se agrega un pequeño offset aleatorio

- **Tiempo de vencimiento de ruta = 180 segundos**

  Se marca la ruta como “expirada” (métrica=16) para que los vecinos se enteren (se sigue propagando)

- **Tiempo de “recolección de basura” = 120 segundos**

  Al expirar este tiempo la ruta desaparece de la tabla

Protocolo RIPv2

- **Extiende la funcionalidad de RIPv1**
- **Usa el mismo formato de mensaje pero modifica el formato de las route entries (RTE) y agrega otras RIP entries**
- **Usa direcciones de multicast (en vez de broadcast como RIPv1) para los “requests”. Se usa la dirección de multicast 224.0.0.9**
- **Por compatibilidad, si se recibe un mensaje RIPv1 se responde con respuestas RIPv1 (a menos que se configure “no responder mensajes RIPv1”)**

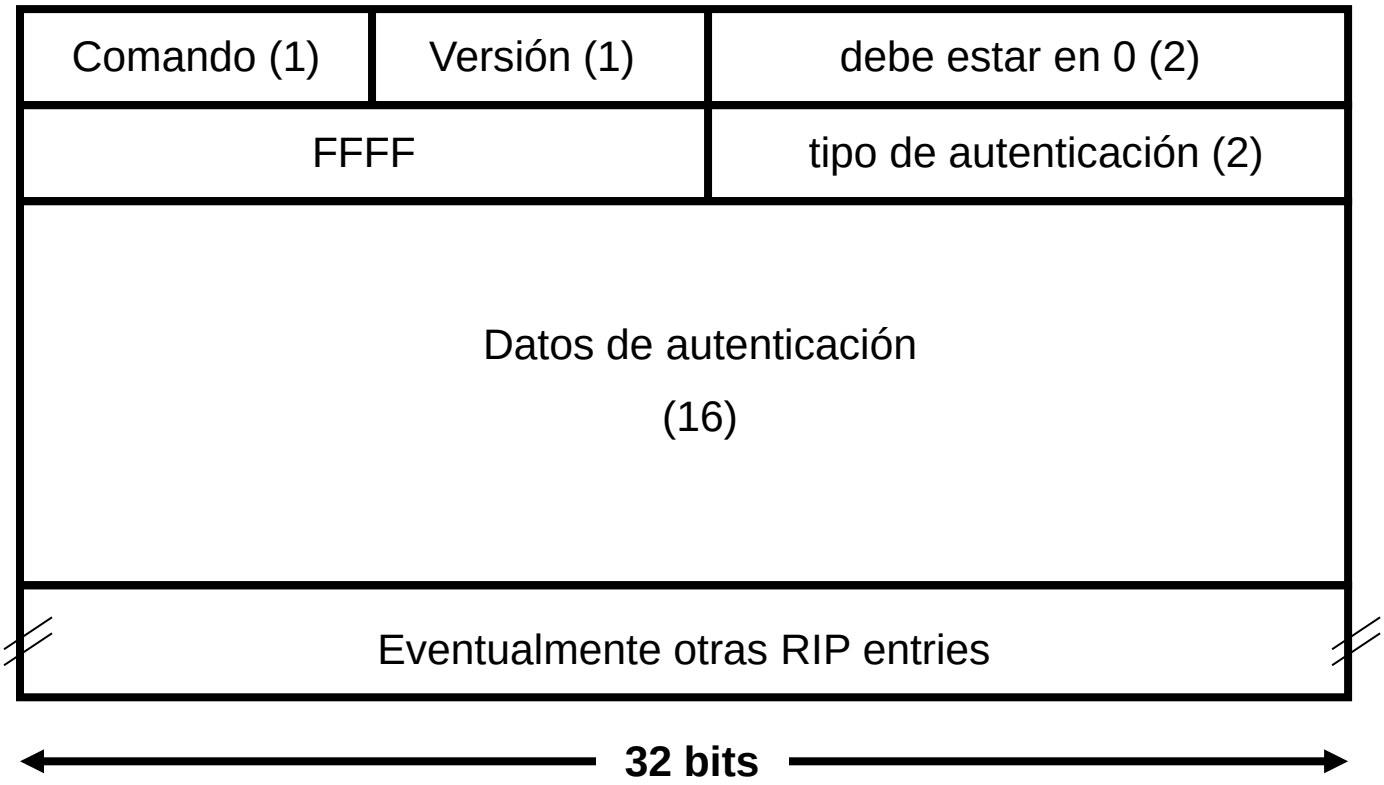
Formato de las RTE

- **Route tag es un atributo que se debe preservar y propagar para esta ruta. Se usa para separar rutas internas (IGP) de externas (EGP) y mejorar la interoperabilidad entre protocolos**
- **Próximo salto (es un “aviso”) permite optimizar si el IP es alcanzable por el receptor, sino se descarta**

Autenticación

- La autenticación es por mensaje y solo hay dos bytes sin uso en el formato del mensaje
- Entonces se usa el espacio de la primer RIP entry para la autenticación
- Para indicarlo, el campo “familia de direcciones” se pone en FFFF
- Solamente puede haber una RIP entry de autenticación por mensaje y debe ser la primera

Mensaje con autenticación



RIP para IPv6

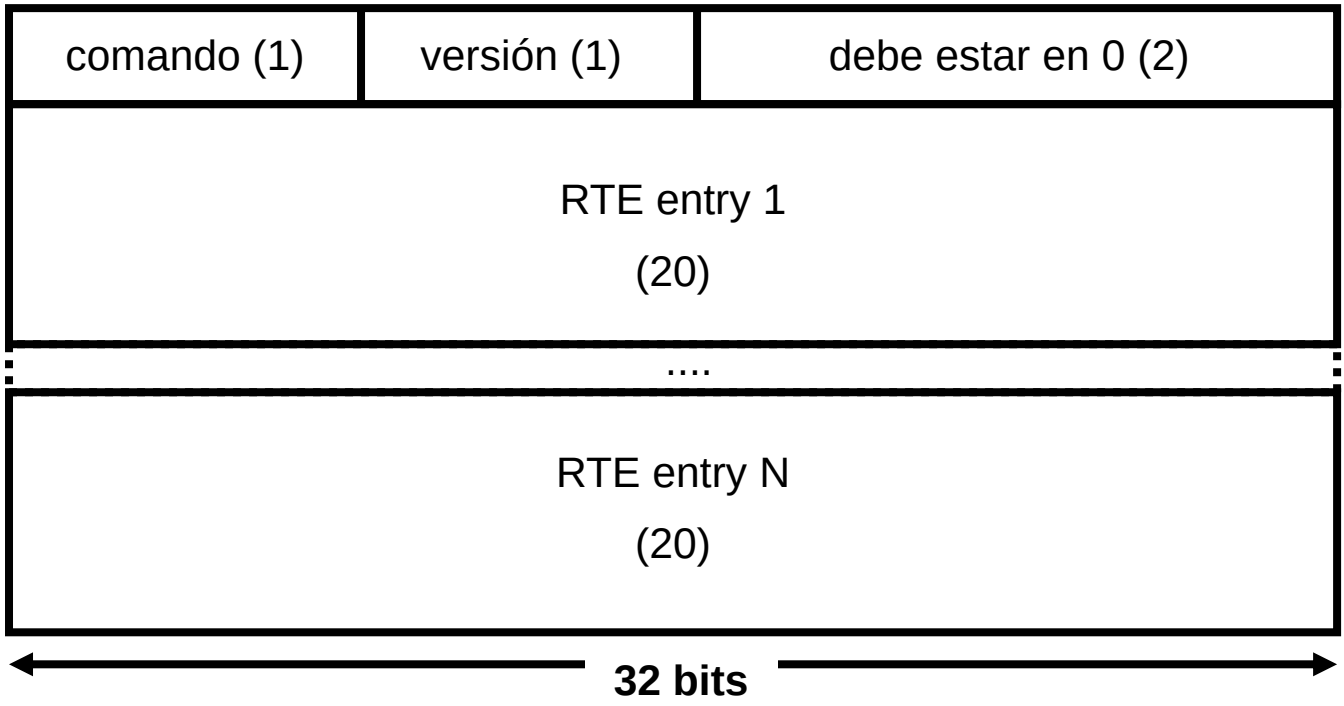
- **RIPng es la adaptación del protocolo RIP para IPv6**
- **Se define en la RFC 2080, RFC 2081**
- **Solamente debería implementarse en enrutadores ya que los mecanismos de “router discovery” de IPv6 resuelven el problema de los hosts**

RIPng

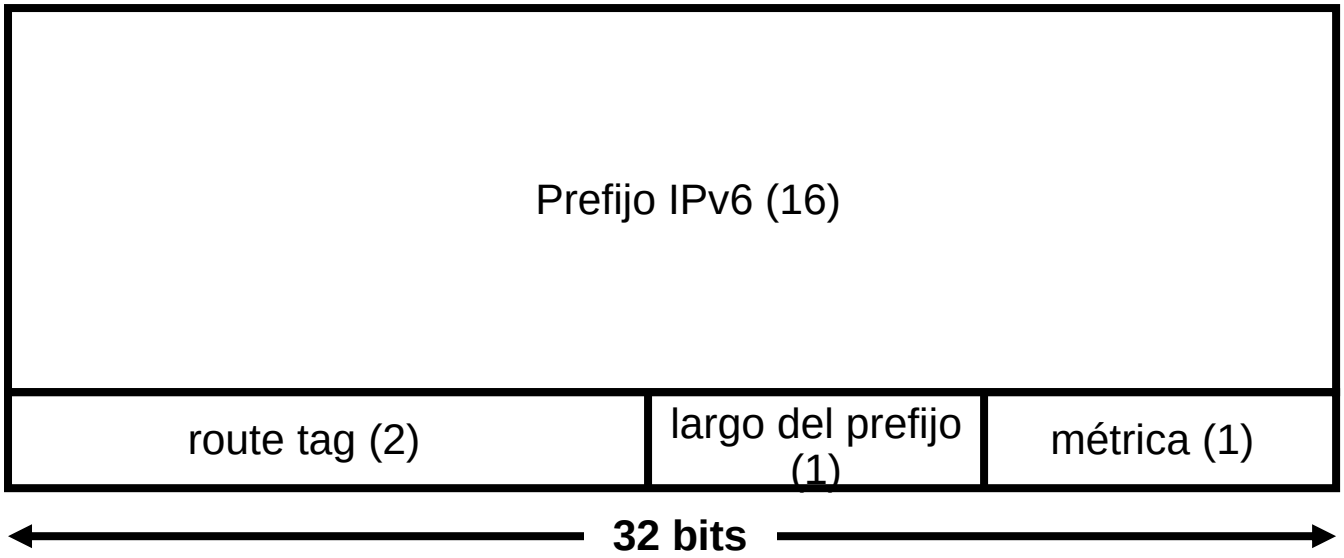
- **Cada entrada en RIPng deberá contener al menos la siguiente información:**
  - El prefijo IPv6 del destino
  - La métrica (saltos) para llegar a ese destino
  - La dirección IPv6 del próximo salto (next_hop)
  - Banderas para indicar el estado de la ruta (route change flag)
  - Temporizadores asociados a la entrada

Mensaje RIPng

- **El formato del mensaje es el mismo que en RIPv2, cambian las RTE (Route Table Entry)**

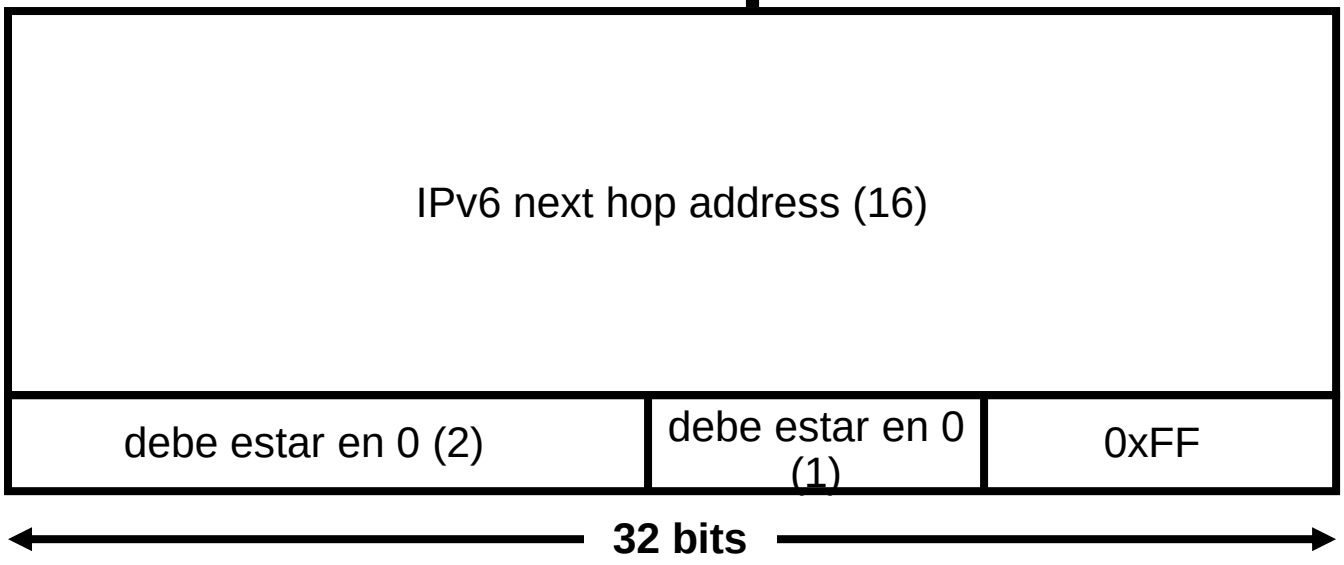


RTE



- **Prefijo = prefijo IPv6 (128 bits)**
- **route tag = atributo asignado a la ruta que debe preservarse y redistribuirse con la ruta. Permite separar las rutas de RIPng internas de las que son importadas de un EGP u otro IGP**
- **Largo del prefijo = 0 a 128**
- **Metrica = 1 a 16 (infinito, no alcanzable)**

Next hop RTE



- **Tiene la misma funcionalidad que en RIPv2, para sugerir el próximo salto**
- **Es válido para todas las RTE que sigan a esta Next hop RTE. Se corta con el fin del mensaje o si aparece otra next hop RTE**
- **El next hop address debe ser una dirección link-local**
- **Si es ::0 significa que la dirección es la de quién envía el mensaje**

Temporizadores

- **Cada 30 ± random(15) segundos, cada enrutador envía un mensaje de respuesta no solicitado con la información de todas las rutas a todos los vecinos**
- **Las entradas no actualizadas en 180 segundos o para las que se reciba una actualización con métrica 16, se marcan para borrar y se siguen propagando con métrica 16 para que el resto se entere. Además se sacan de la tabla de rutas**
- **El tiempo de recolección de basura es de 120 segundos**

Seguridad

- **No se especifica ningún mecanismo de seguridad en RIPng**
- **Se confía en los mecanismos de IPv6:**
  - **IP Authentication Header (AH)**
    - **RFC 4302**
  - **IP Encapsulating Security Payload (ESP)**
    - **RFC 4303**
  - **Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)**
    - **RFC 4835**