Operación de un Router

Capitulo V: Protocolo IP

5.1 Introducción

En las redes datos actuales, ya sean internas o externas, existe un protocolo encargado de la interconexión y ocultamiento de los detalles de hardware y de enlace de datos.

Este conjunto de reglas y mecanismos de interconexión es conocido con el nombre de IP. En su forma mas básica, una red de datos se compone de dispositivos finales (estaciones de trabajo, servidores) y dispositivos intermedios (routers) que tienen la difícil tarea de realizar la interconexión y además acotar el trafico de broadcast a nivel de enlace entre una red y la otra.

Por un momento si imaginamos que una trama Ethernet llegara a todos los usuarios de la red de datos mundial (Internet) existiría un exceso de tráfico que ningún dispositivo de red podría manejar, saturando de esta manera su CPU o su memoria RAM. Pensando en la ley de los grandes números, si cada cajero de un banco se quedara con 10 centavos por cliente, seria insignificante visto desde el punto de vista individual. Ahora si en el día fueron 1000 clientes el monto es mas grande y yendo mas allá los montos serian cuantiosos mensual y anualmente. Esto mismo ocurriría en una red datos, no es lo mismo que una PC reciba el trafico de 100 PCs que el trafico de broadcast generado por miles de millones de estaciones de trabajo.

Una de las formas recientemente vistas empleadas para acotar el trafico a nivel enlace de datos es empleando el concepto de Vlans. En este capitulo ampliamos el concepto donde el trafico se jerarquiza y clasifica en la capa de red, asignándole a cada red compuesta por un conjunto de estaciones de trabajo un prefijo de red. Ahora la interconexión a este nivel es posible entre estaciones de trabajo de distintas redes a la vez que un router acota el tráfico de broadcast a nivel enlace de datos.

Nunca pierda de vista que el trafico que verdaderamente impacta en una red es el broadcast a nivel enlace de datos, porque es el primer bloque de datos o trama que llega a todos los destinatarios. Cuando un dispositivo cualquiera sea, recibe ese tráfico de broadcast (ff-ff-ff-ff-ff-ff) esta obligado a procesar ese trafico. Además, también se lee el campo type de la trama Ethernet para de antemano saber que se esta transportando en la trama Ethernet.

Para comprender el funcionamiento de una VLAN, el broadcast, su acotamiento y la interconexión a un nivel en capa 3, podemos hacer la analogía pensando en dos cursos, uno de Ingles y otro de Frances. Si ambos cursos se dictan en una misma aula la comunicación entre los profesores y alumnos se vera interrumpida el uno con el otro, ya que la exposición de cada profesor (broadcast) interferirá entre si o en el caso de que los alumnos quieran realizar una pregunta.

Para solucionar este problema, el director del instituto de enseñanza dispuso un aula para el curso de ingles y otra aula independendiente para el curso de francés. De esta forma el broadcast de cada profesos solo ira a los alumnos que toman su curso y no interferirá con el resto. No quita que un alumno de ingles pueda tomar también el curso de francés, para lo cual solo tendrá que salir del curso de ingles por la puerta (conocida en ruteo como puerta de enlace) e ingresar al aula de ingles por la puerta (puerta de enlace). La puerta de enlace en esta instancia puede pensarse como el

acceso a un aula donde la única forma de ingresar a ella es por este acceso.

Un protocolo puede estar orientado a la conexión o puede ser orientado a la no conexión.

Si es **Orientado a la Conexión**, antes de comenzar la transmisión de datos entre un origen y un destino es preciso cumplir con el **establecimiento de la conexión**. Esto implica que el origen y el destino se ponen de acuerdo en la forma como se llevara a cabo la transferencia de datos: número de secuencia inicial, capacidad de transmisión para control de flujo, cantidad de paquetes a enviar antes de recibir confirmación, etc.

Una vez llevada a cabo el establecimiento, viene la fase de **transmisión de datos y de mantenimiento de la conexión**. Normalmente el mantenimiento es un control que realizan los pares durante al transmisión de datos para detectar paquetes perdidos, duplicados o desordenados. Este control se conoce como señalización en banda porque va junto con los datos del usuario en algunos campos del encabezado de control.

Finalmente, cuando la trasmisión de datos fue exitosa entre los pares, se procede al cierre ordenado de la transmisión mediante el envío bidireccional de mensajes de **fin de la conexión**.

El problema de este modelo de conexión es que si la transmisión se interrumpe por falta de conexión o por corte en los enlaces o por falla en el equipamiento, los datos se pierden y debe volver a establecerse la comunicación.

Si es el modelo de comunicación es **Orientado a la No Conexión**, ambos pares comienzan la transmisión de manera automática sin ponerse de acuerdo. La ventaja de este tipo de modelos es que ante algún corte de servicio por salida de servicio de equipos o enlaces de fibra óptica la trasmisión de información toma un camino alternativo automáticamente sin que los pares se den cuenta del problema. Este modelo lo emplea el protocolo IP, la unidad de información que transmite se conoce como datagrama IP.

A continuación se detallan las características principales del protocolo IP se detallan a continuación y en las siguientes secciones se describirá cada una.

- Encaminamiento IP
- Segmentación y Reensamblado
- Tiempo de Vida.
- Control de Flujo
- Control de Errores

5.2 Encaminamiento IP

5.2.1 Introducción

Como se sabe, todos los servicios de redes IP utilizan un sistema sin conexión de entrega de paquetes y la unidad básica de transferencia en una red TCP/IP es el datagrama. A continuación veremos los aspectos operacionales de como los enrutadores direccionan y encaminan datagramas IP y cómo los entregan en su destino final.

Operación de un Router

En un sistema de conmutación de paquetes, el ruteo es el proceso de selección de un camino sobre el que se mandarán paquetes y el enrutador es la computadora que hace la selección.

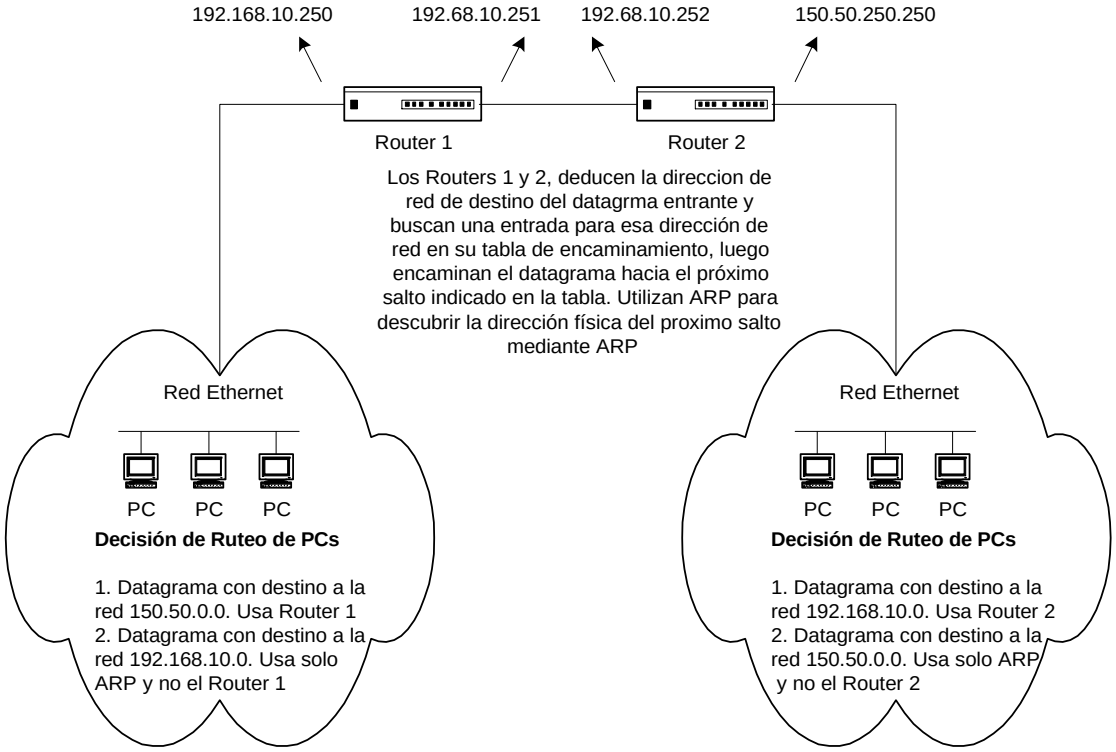


Figura 1: Ejemplo de una conexión de enrutadores y anfitriones

El encaminamiento de datos ocurre en muchos niveles:

1. **Dentro de una red LAN**, los switches o bridges son los encargados de encaminar (realizan proceso de bridging) tramas desde la fuente al destino. Esta clase de encaminamiento esta contenido dentro de la propia red y las máquinas en el exterior(otras redes) no pueden participar en las decisiones de encaminamiento, sino que solo ven a la red como una entidad que entrega paquetes.

2. Recordando que el objetivo del **protocolo IP** es proporcionar una **red virtual** que comprenda muchas redes físicas, son los enrutadores los encargados de encaminar(realizar routing) los paquetes en la Internet o Intranet. El algoritmo de ruteo IP debe escoger un camino por donde enviar un datagrama pasando por muchas redes físicas.

El software de ruteo para seleccionar el mejor camino para el datagrama a lo largo de la Internet, tomaría las decisiones basándose en la carga de la red, la longitud del datagrama o el tipo de servicio. Sin embargo la mayor parte del software de ruteo selecciona las rutas basándose en suposiciones sobre el camino más corto.

Operación de un Router

Recordando que la arquitectura de Internet se compone de muchas redes físicas interconectadas por enrutadores, cada uno tiene conexiones directas hacia dos o más redes. Tanto los anfitriones como los enrutadores participan en el ruteo de datagramas IP que viajan a su destino. Cuando un programa de aplicación en un anfitrión intenta comunicarse, los protocolos TCP/IP eventualmente generan uno o más datagramas IP. El anfitrión debe tomar una decisión de ruteo cuando elige a dónde enviar los datagramas. Por supuesto los enrutadores también toman decisiones de ruteo IP

5.2.2 Encaminamiento directo e indirecto

Estrictamente hablando, podemos definir al proceso de ruteo de un datagrama en dos partes: la entrega directa y la entrega indirecta.

a. Entrega directa

Este tipo de entrega consiste en la transmisión de un datagrama desde una máquina a través de una sola red física hasta otra máquina situada en la misma red física. Dos máquinas solamente pueden llevar a cabo la entrega directa si ambas se conectan directamente al mismo sistema de transmisión física, por ejemplo una red Ethernet (indicada con una nube en la figura 10.2.1 y en la figura 10.3.1).

Como sabemos, una máquina en una red física puede enviar una trama física directamente a otra máquina dentro de la misma red. Para transferir un datagrama IP, el transmisor emplea el protocolo ARP.

Para ello, el transmisor descubre, en base a la dirección IP de destino, la dirección física del receptor(ARP), luego encapsula el datagrama dentro de una trama física y utiliza la red para entregar el datagrama. Por lo tanto:

La transmisión de un datagrama IP entre dos máquinas que comparten una misma red física no involucra a enrutadores.

Para averiguar si un destino reside en una de las redes a la que el transmisor esta directamente conectado(comparten la misma red física), éste extrae la porción de red de la dirección IP de destino y la compara con la porción de red de su propia dirección IP.

Si corresponden, significa que el datagrama se puede enviar de manera directa empleando el protocolo ARP. Esta idea puede observarse en la red de la figura 10.3.1, donde ambos anfitriones (PC A y PC B) residen en la misma red física, ya que ambos comparten la dirección de red 192.168.10.0.

Debido a que las direcciones IP de todas las máquinas dentro de una sola red comparten un prefijo en común la comprobación de que una máquina se puede alcanzar directamente es muy eficiente.

Operación de un Router

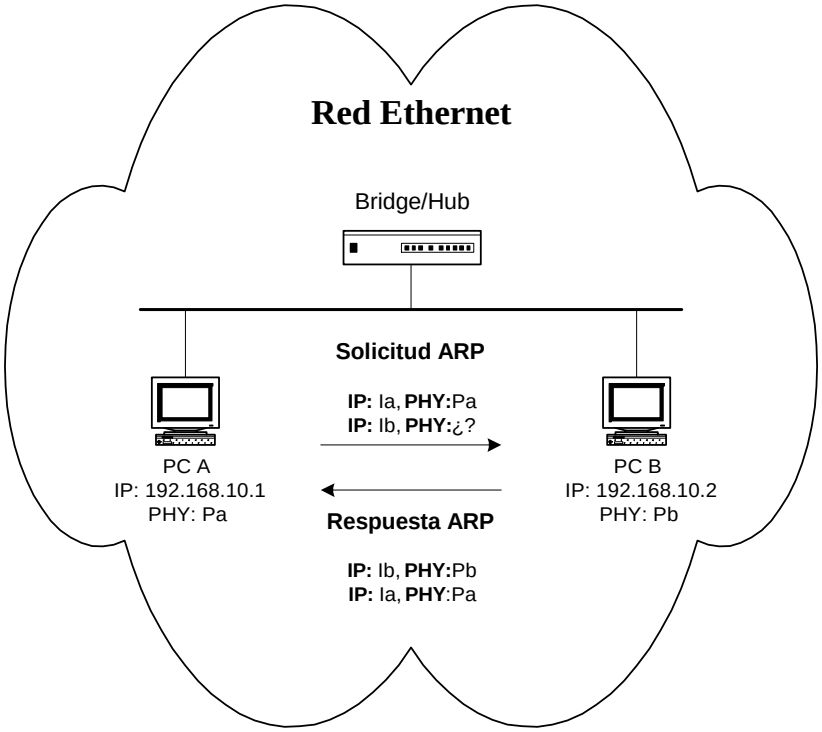


Figura 2: Entrega de datagramas en forma directa

En general, la forma más fácil de pensar en la entrega directa es como el paso final de cualquier transmisión de datagramas, aún si el datagrama debe atravesar muchas redes y enrutadores intermedios. El último enrutador del camino entre la fuente del datagrama y su destino siempre se conectará directamente a la misma red física que la máquina de destino(por lo tanto compartirán un prefijo de red en común).

Por lo tanto el último enrutador será el encargado de entregar el datagrama utilizando la entrega directa. En una ruta directa, un datagrama nunca pasará a través de ningún enrutador intermedio.

b. Entrega Indirecta

La entrega indirecta ocurre cuando el destino no es una red conectada directamente, lo que obliga al transmisor a pasar el datagrama a un enrutador para su entrega. El transmisor del datagrama debe identificar a un ruteador para que éste pueda encaminar el datagrama hacia la red de destino.

Supóngase una gran red con muchas redes físicas interconectadas por medio de enrutadores, pero solo con dos host conectados en sus extremos más distantes. Cuando un anfitrión quiere enviar un datagrama a otro, lo encapsula y lo envía hacia el ruteador más cercano. Esto es posible ya que todas las redes físicas están interconectadas por enrutadores, por lo tanto debe existir un router conectado a cada uno de los anfitriones. Por lo tanto, el anfitrión de origen puede alcanzar un enrutador utilizando una sola red física (a la que ambos están conectados).

Operación de un Router

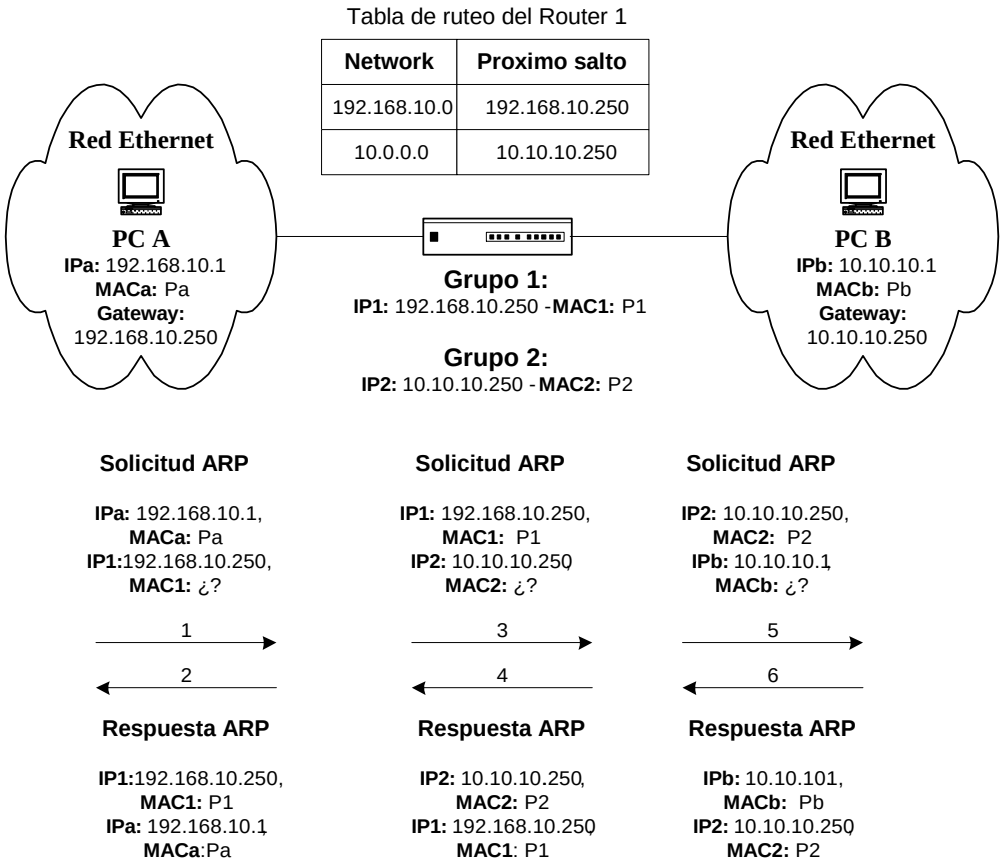


Figura 3: Encaminamiento Indirecto

Una vez que la trama llega al enrutador, el software extrae el datagrama encapsulado y el software IP selecciona el siguiente enrutador a lo largo del camino hacia el destino. De nuevo, se coloca el datagrama en una trama y se envía a través de la siguiente red física hacia un segundo enrutador y así sucesivamente, hasta que se pueda entregar en forma directa.

Todos estos conceptos pueden observarse en la figura 10.3.2. Considérese que la máquina A emite un datagrama con destino a la máquina B. Ambas máquinas se encuentran en redes diferentes.

La máquina A y el Router 1 pueden comunicarse porque comparten una red en común. Además, antes de transmitir el datagrama la PC A debe conocer la dirección física del enrutador 1, empleando para ello el protocolo ARP. Este proceso se realiza en cada salto del datagrama hasta su destino final.

Los enrutadores en una red IP forman una estructura cooperativa e interconectada. Los datagramas pasan de un enrutador a otro hasta llegar a uno que los pueda entrega en forma directa.

Operación de un Router

5.2.3 Ruteo controlado por tablas

El algoritmo de ruteo IP más común emplea una tabla de ruteo IP en cada máquina. Dicha tabla almacena información sobre posibles destinos y sobre cómo alcanzarlos. Debido a que tanto los enrutadores como los anfitriones encaminan datagramas, ambos tienen tablas de ruteo IP. Siempre que el software de ruteo IP necesite transmitir un datagrama, consulta la tabla de ruteo para decidir a dónde enviarlo.

La información almacenada en la tabla de ruteo debe contener la mínima información posible para que los enrutadores tomen las decisiones, ya que de lo contrario:

- Sería imposible mantener actualizadas las tablas de ruteo si se almacenaran en esta las direcciones IP de cada posible destino dentro de una gran red.

- Como el número de destinos posibles es muy grande, las máquinas no tendrían suficiente espacio para almacenar la información.

Por suerte el esquema de direcciones IP nos permite aislar la información sobre anfitriones específicos del ambiente local en el que existen y hace que las máquinas que están lejos encaminen los paquetes hacia ellos sin saber dichos detalles. Esto es posible ya que todas las máquinas conectadas a una misma red física comparten un prefijo en común (la porción de red de la dirección). Es por ello que las tablas de ruteo contiene prefijos de red y no direcciones completas.

5.2.4 Ruteo con salto al siguiente

Utilizar la porción de red de una dirección de destino en vez de toda la dirección de anfitrión hace que el ruteo sea eficiente y mantiene reducidas las tablas de ruteo. También es importante, porque ayuda a ocultar información al mantener los detalles de los anfitriones específicos confinados al ambiente local en el que operan, esto significa que no es necesario conocer las MAC Address de todos las Estaciones de Trabajo.

Por lo general, una tabla de ruteo contiene pares (N,R), siendo N la dirección IP de una red de destino y R la dirección IP del siguiente enrutador en el camino hacia la red N. La idea de utilizar una tabla de ruteo para almacenar un **"salto siguiente"** para alcanzar cada destino es conocida como **"ruteo con salto al siguiente"**. De esta manera un enrutador no conoce el camino completo hacia el destino.

Cada entrada en la tabla de ruteo apunta hacia un enrutador que se puede alcanzar a través de una red común entre ambos enrutadores únicamente. Por lo tanto, todos los enrutadores enumerados en la tabla de ruteo de la máquina M deben residir en las redes con las que M se conecta de manera directa. Cuando un datagrama está listo para dejar M, el software IP localiza la dirección IP de destino y extrae la porción de red. Luego, M utiliza la porción de red para tomar una decisión de ruteo, seleccionando un enrutador que se pueda alcanzar directamente.

En la siguiente figura se muestra un ejemplo que nos ayudará a explicar las tablas de ruteo. La red de ejemplo consiste en cuatro redes físicas (Ethernet) conectadas por tres enrutadores. Además se indica la tabla de enrutamiento para cada enrutador. Por ejemplo como R se encuentra conectado de manera directa a las redes 20.0.0.0 y 30.0.0.0, puede utilizar la entrega directa para llevar a cabo un envío a un anfitrión en cualquiera

de esas redes(utilizando ARP). Teniendo un datagrama destinado para un anfitrión en la red 40.0.0.0, R lo encamina a la dirección 30.0.0.7, que es la dirección del enrutador S. Luego, S entregará el datagrama en forma directa. R puede alcanzar la dirección 30.0.0.7 debido a que tanto R como S se conectan directamente con la red 30.0.0.0.

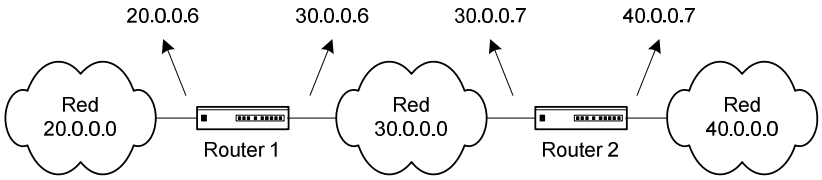


Tabla Router 1 .

Red	Mascara	Gateway
20.0.0.0	255.0.0.0	20.0.0.6
30.0.0.0	255.0.0.0	30.0.0.6
40.0.0.0	255.0.0.0	30.0.0.7

Tabla Router 1 .

Red	Mascara	Gateway
40.0.0.0	255.0.0.0	40.0.0.7
30.0.0.0	255.0.0.0	30.0.0.7
20.0.0.0	255.0.0.0	30.0.0.6

Figura 4: Ejemplo de una red conmutada (nivel IP)

El tamaño de la tabla de ruteo depende del número de redes en la red. Solamente crece cuando se agregan nuevas redes. Sin embargo, el tamaño y el contenido de la tabla son independientes del número de anfitriones individuales conectados a las redes. En síntesis:

Para ocultar información, mantener reducidas las tablas de ruteo y tomar decisiones de ruteo de manera eficiente, el software de ruteo IP sólo puede guardar información sobre las direcciones de las redes de destino, no sobre las direcciones de anfitriones individuales.

Escoger rutas basándose tan sólo en la identificación de la red de destino tiene muchas consecuencias:

1. Significa que todo el tráfico destinado a una cierta red toma el mismo camino. Como resultado, aún cuando existen muchos caminos, quizás no se utilicen constantemente. Todos los tipos de tráfico siguen el mismo camino sin importar el retraso impuesto por las redes físicas.

2. Debido a que solo el último enrutador del camino intenta comunicarse con el anfitrión final, solamente el enrutador puede determinar si el anfitrión existe o está en operación. El enrutador debe enviar reportes sobre los problemas de entrega mediante el ICMP(Protocolo de Control de Gestión en Internet).

3. Debido a que cada enrutador encamina los datos de forma independiente, los datagramas que viajan del anfitrión A al B pueden seguir un camino totalmente distinto al que siguen los datagramas que viajan del anfitrión B hacia el anfitrión A.

5.2.5 Rutas asignadas por defecto

Otra técnica utilizada para ocultar información y mantener reducido el tamaño de las tablas de ruteo, es asociar muchos registros a un ruteador

asignado por omisión o defecto (**0.0.0.0 / 255.255.255.255**). La idea es hacer que el software de ruteo IP busque primero la tabla de ruteo para encontrar la red de destino. Si no aparece una ruta en la tabla, las rutinas de ruteo envían el datagrama a un ruteador asignado por omisión.

Por ejemplo, las rutas asignadas por omisión trabajan bien en máquinas anfitriones que se conectan a una sola red física y alcanzan sólo a un enrutador, que es la puerta de entrada hacia el resto de Internet. Toda la decisión de ruteo consiste en dos comprobaciones: una de la red local y un valor asignado por omisión que apunta hacia el único enrutador posible.

Esta idea puede observarse en la figura 3, donde la PC A desea comunicarse con la PC B de otra red. La PC A al no encontrar a la PC B en su propia red Ethernet, encamina el datagrama (con destino a la PC B) hacia el enrutador 1, el cual constituye la entrada hacia Internet. Para lograr dicho encaminamiento utiliza la puerta de enlace o gateway que se configuro como ruta por omisión.

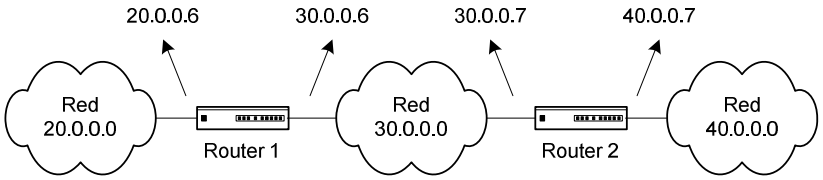


Tabla Router 1 .

Red	Mascara	Gateway
20.0.0.0	255.0.0.0	20.0.0.6
30.0.0.0	255.0.0.0	30.0.0.6
0.0.0.0	/24	30.0.0.7

Tabla Router 1 .

Red	Mascara	Gateway
40.0.0.0	255.0.0.0	40.0.0.7
30.0.0.0	255.0.0.0	30.0.0.7
0.0.0.0	/24	30.0.0.6

Figura 5. Uso de la ruta por defecto (0.0.0.0)

En secciones siguientes analizaremos posibles problemas originados con la configuración de las rutas por defecto.

5.2.6 Rutas por anfitrión especifico

Aunque se dijo que el ruteo esta basado en direcciones de red y no en anfitriones individuales, la mayor parte del software de ruteo IP permite que se especifiquen rutas por anfitrión como caso especial. Esto le otorga al administrador de la red un mayor control sobre el uso de la red y se puede utilizar para controlar el acceso por razones de seguridad(servidor de autenticación).

Operación de un Router

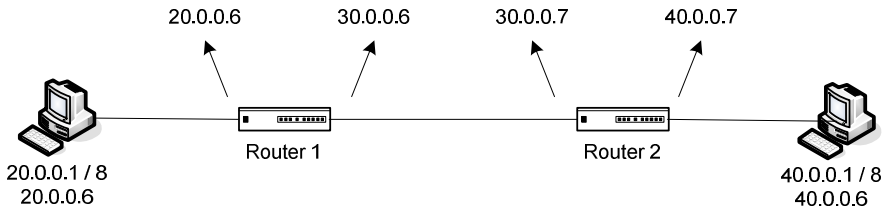


Tabla Router 1

Red	Mascara	Gateway
20.0.0.0	255.0.0.0	20.0.0.6
30.0.0.0	255.0.0.0	30.0.0.6
40.0.0.1	255.255.255.255	30.0.0.7

Tabla Router 1

Red	Mascara	Gateway
20.0.0.0	255.0.0.0	20.0.0.6
30.0.0.0	255.0.0.0	30.0.0.6
20.0.0.1	255.255.255.255	30.0.0.6

Figura 6. Uso de la rutas especificas en las tablas de ruteo

5.2.7 Algoritmo de ruteo IP

En la siguiente figura se presenta el algoritmo de ruteo IP. Por medio de un datagrama y una tablas de ruteo, este algoritmo selecciona el salto siguiente al que se debe enviar el datagrama. Todas las rutas deben especificar un salto siguiente que resida en una red conectada directamente.

Algoritmo de Ruteo IP

RutaDatagrama(Datagrama, Tabla de Ruteo)

Extraer la dirección IP de destino (D) del datagrama y calcular el prefijo de red(N):

- **Si N corresponde a cualquier dirección de red directamente conectada entregar el datagrama al destino D sobre dicha red. (Esto comprende la transformación de D en una dirección física, encapsulando el datagrama y enviando la trama)**
- **De otra forma, si la tabla contiene una ruta con anfitrión especifico para D, enviar el datagrama al salto siguiente especificado en la tabla**
- **De otra forma, si la tabla contiene una ruta para la red N, enviar el datagrama al salto siguiente especificado en la tabla.**
- **De otra forma, si la tabla contiene una ruta asignada por omisión, enviar el datagrama al enrutador asignado por omisión especificado en la tabla**
- **De otra forma, declarar un error en el ruteo.**

Operación de un Router

5.2.8 Ruteo con direcciones IP

Es importante entender que a excepción de la disminución del tiempo de vida y de volver a calcular la suma de verificación, el ruteo IP no altera el datagrama original. En particular, las direcciones de origen y destino del datagrama permanecen sin alteración, estas siempre especifican la dirección IP de la fuente original y la dirección IP del último destino. Cuando el IP ejecuta el algoritmo de ruteo, selecciona una nueva dirección IP, la cual es la dirección de la máquina a la que a continuación se tendrá que enviar el datagrama, conocida como dirección IP del "próximo salto".

La dirección de próximo salto no es almacenada en el datagrama, ya que en éste no existe un lugar reservado para ella. Después de ejecutar el algoritmo de ruteo, el IP pasa el datagrama y la dirección de salto siguiente al software de interfaz de red, responsable de la red física sobre la que el datagrama se debe enviar. En este punto es donde se emplea el protocolo ARP para descubrir cual es la dirección física del siguiente enrutador basándose en la dirección IP del próximo salto obtenida de la tabla de ruteo. Después de utilizar la dirección de salto siguiente para encontrar una dirección física, el software de interfaz de red la descarta.

¿Por que el software IP evita la utilización de direcciones físicas cuando almacena y calcula las rutas?. Existen dos razones importantes:

1. La tabla de ruteo proporciona una interfaz muy transparente entre el software IP que encamina datagramas y el software de alto nivel que manipula las rutas. Para depurar problemas de ruteo, los administradores de red, a menudo necesitan examinar las tablas de ruteo. La utilización de direcciones IP solamente en la tabla de ruteo facilita que los administradores las entiendan, lo mismo para ver donde el software actualizó correctamente las rutas.

2. Todo el sentido del Protocolo Internet (IP) es construir una abstracción que oculte los detalles de las redes físicas subyacentes.

5.2.9 Manejo de datagramas entrantes

Cuando un datagrama IP llega a un anfitrión, el software de interfaz de red lo entrega al software IP para su procesamiento. Si la dirección de destino del datagrama corresponde a la dirección IP del anfitrión, el software IP del anfitrión acepta el datagrama y lo pasa al software de protocolo de alto nivel apropiado, para su procesamiento. Si la dirección IP de destino no corresponde a la del anfitrión, se requiere que éste descarte el datagrama.

Cuando llega un datagrama IP a un enrutador, éste lo entrega al software IP. Si la dirección de destino del datagrama corresponde a la dirección IP, el software IP pasa el datagrama a un software de protocolo de nivel más alto para su procesamiento. Si el datagrama no ha llegado a su destino final, el IP lo encamina utilizando el algoritmo estándar así como la información en la tabla de ruteo local. La determinación sobre si un datagrama IP alcanzó su destino final no es tan trivial, ya que un anfitrión o un enrutador puede tener múltiples interfaces de red, cada una con diferentes direcciones de red IP. Cuando llega un datagrama IP, la máquina debe comparar la dirección de destino de red IP con la dirección IP de cada una de sus conexiones de red. Si alguna corresponde, guarda el datagrama y lo procesa.

Además se deben aceptar los datagramas que se transmitieron por difusión en la red física, si su dirección IP de destino es la dirección IP de difusión limitada o dirigida para esa red. En cualquier caso, si la dirección no corresponde a ninguna de las direcciones de la máquina local, el IP disminuye el campo tiempo de vida en el encabezado del datagrama, descartándolo si el contador llega a cero o calcula una nueva suma de verificación y encamina el datagrama si la cuenta es positiva.

5.2.10 Configuración de un esquema de ruteo Estático empleando Routers.

En las siguientes figuras se observa la interconexión a nivel de red de distintas estaciones de trabajo (PC A, PC B, PC C, PC D, PC E, PC F). Normalmente en un red de datos todas las estaciones de trabajo emiten trafico entre si, ya sea por trafico dirigido (**unicast**) o por trafico de difusión (**broadcast**). De esta forma, tanto los bridges como los switches van aprendiendo información (MAC Address de Origen) de la diferentes estaciones de trabajo conectadas a la misma Vlan, de manera que las próximas comunicaciones entre ellas (las PCs) sean dirigidas y directas entre la computadora de origen y de destino.

Los enrutadores también aprenden información, pero el administrador de la red debe ayudarlo realizando configuraciones en cada equipo que hacen que se inicie el proceso de intercambio de información. Sin la definición de estas configuraciones iniciales no es posible el comienzo del intercambio de información de encaminamiento.

Toda estación de trabajo en una red de datos presenta una dirección IP de **gateway** o **puerta de enlace**. Esta dirección permite dirigir todo el tráfico generado por la estación de trabajo hacia otras redes distintas a las que ella posee. La dirección de Gateway debe ser siempre la del router que la estación de trabajo tiene directamente conectado (tanto la PC como el Router comparten la misma red).

Existen dos tipos de encaminamiento, el directo cuando las estaciones de trabajo están directamente conectadas y comparten la misma red que el router y el indirecto cuando el destino a alcanzar y por donde debe pasar el datagrama a enviar, esta en una red distinta al gateway directamente conectado.

Esta conmutación de tráfico entre redes IP distintas, se realiza en base a las tablas de conmutación IP. La tabla de conmutación IP de un Router contiene al menos tres parámetros mínimos (red de destino, mascara de subred y puerta de enlace o gateway).

- **Red de Destino**. Indica la red de todos los posibles destinos que tiene el sistema autónomo. Esta entrada es comparada con la red de destino del datagrama después de aplicar la mascara de subred a la dirección IP de destino que viene incluida en el datagrama.

- **Mascara de Subred**. Indica la mascara de subred del destino a llegar.

- **Gateway**. Indica la dirección IP del Router a donde enviar el tráfico.

- **Métrica**. Es un valor que representa la calidad de la ruta a alcanzar. Puede estar caracterizada por cantidad de saltos o por

Operación de un Router

estado del enlace (retardo de transmisión o capacidad de transmisión).

A continuación detallaremos paso a paso el armado de las tablas de enrutamiento, el armado de las tablas ARP, el intercambio de información de enrutamiento y los pasos para lograr la comunicación entre la PC A y la PC F. En la figura 5, generalizamos las comunicaciones entre todas las PCs armando las tablas de conmutación de todos los dispositivos.

Paso 1: Definición IP VLANs Router y a las PCs.

1. Lo primero que se define en una red de datos con capacidades de enrutamiento es el plan de numeración IP. En la figura 1 se observa el plan de numeración IP definido para cada red. Cada red constituye una VLAN o dominio de Broadcast diferente en los enrutadores. A un router se le definen tantas Vlans como redes interconecta directamente.
   A cada VLAN en cada Router se le define una dirección IP Unicast independientemente a la cantidad de PCs conectadas a la VLAN. El objetivo de definir el IP a la VLAN es que todas las PCs que conectemos directamente a la VLAN usaran el mismo gateway común para realizar las funciones de enrutamiento. Por ejemplo para el caso de las PC A y B **usaran el Gateway 10.0.0.250** (IP definido a la VLAN con ID 10).

2. A cada PC conectada directamente a una VLAN se la introduce en la misma red que de la Vlan. Como la PC A y la PC B están directamente conectada a la VLAN 10 que posee el IP 10.0.0.250/8, a estas PCs se le definirán los IP 10.0.0.1/8 y 10.0.0.2/8, respectivamente. La PC A y la PC B apuntaran al Gateway o Puerta de enlace 10.0.0.250.

3. Como la PC C y la PC D están directamente conectada a la VLAN 20 que posee el IP 20.0.0.250/8 en el Router 1 y el IP 20.0.0.251/8 en el Router 2, a estas estaciones de trabajo se le definirán los IP 20.0.0.3/8 y 20.0.0.4/8, respectivamente. Ambas PCs podrán usar indistintamente el gateway 20.0.0.250/8 o 20.0.0.251/8 como puerta de salida para efectuar el enrutamiento.

4. Como la PC F y la PC E están directamente conectada a la VLAN 30 que posee el IP 30.0.0.250/8, a estas estaciones de trabajo se les definirán los IP 30.0.0.6/8 y 30.0.0.5/8, respectivamente. La PC E y la PC F apuntaran al Gateway o Puerta de enlace 30.0.0.250.

5. Cada dirección IP tienen asociada una dirección MAC tanto en las PCs como en las Vlans definidas en cada router. En el caso de los routers esta MAC Address es virtual porque al momento de que a la Vlan se le quita el IP o se borra la Vlan la MAC Address desaparece.

Operación de un Router

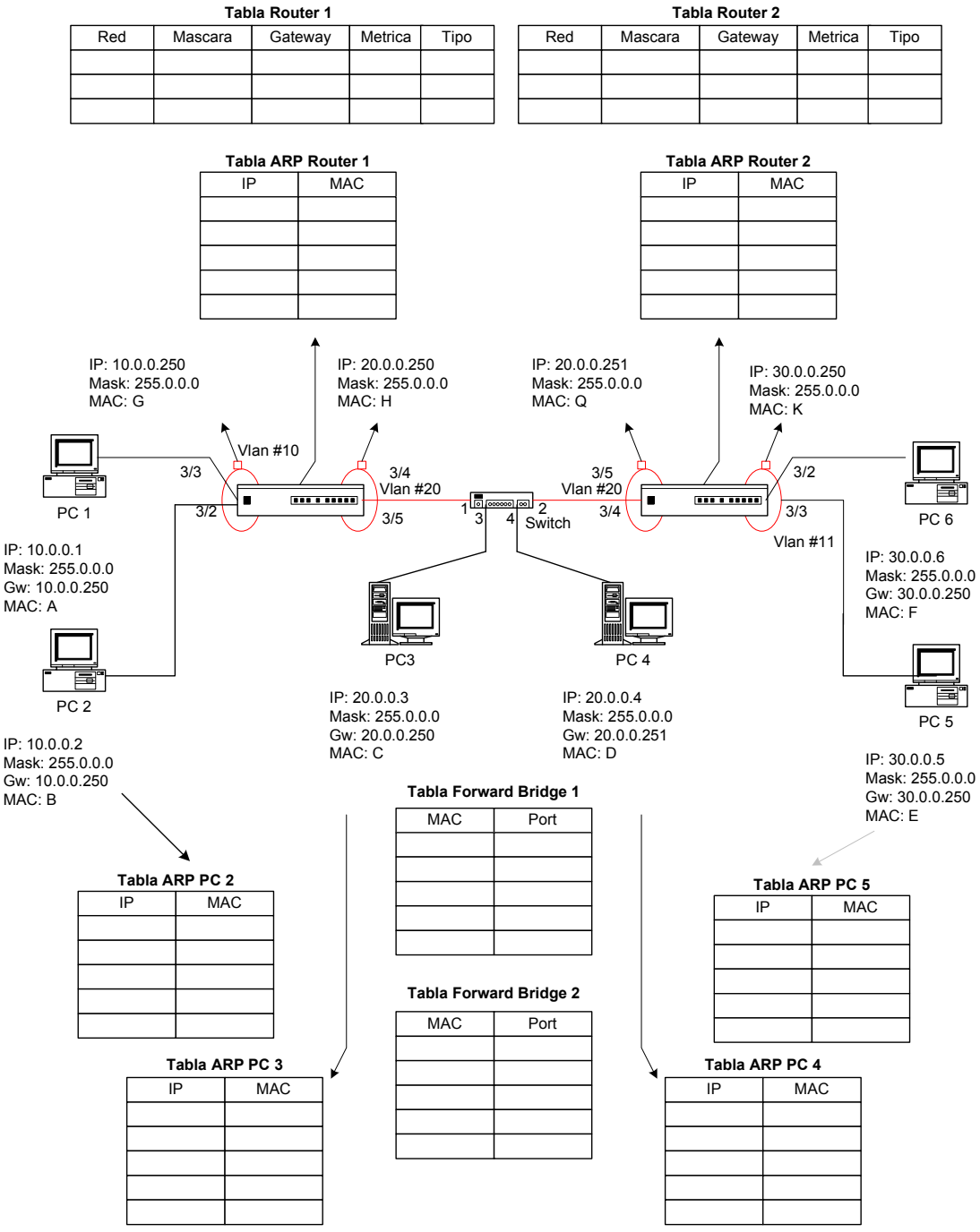


Figura 1: fijas direcciones IP a las Vlans y Estaciones de trabajo

Paso 2: Armado Inicial de la tabla de Enrutamiento.

Operación de un Router

Tabla Router 1

Red	Mascara	Gateway	Metrica	Tipo
10.0.0.0	255.0.0.0	10.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.250	1	Direct

Tabla Router 2

Red	Mascara	Gateway	Metrica	Tipo
30.0.0.0	255.0.0.0	30.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.251	1	Direct

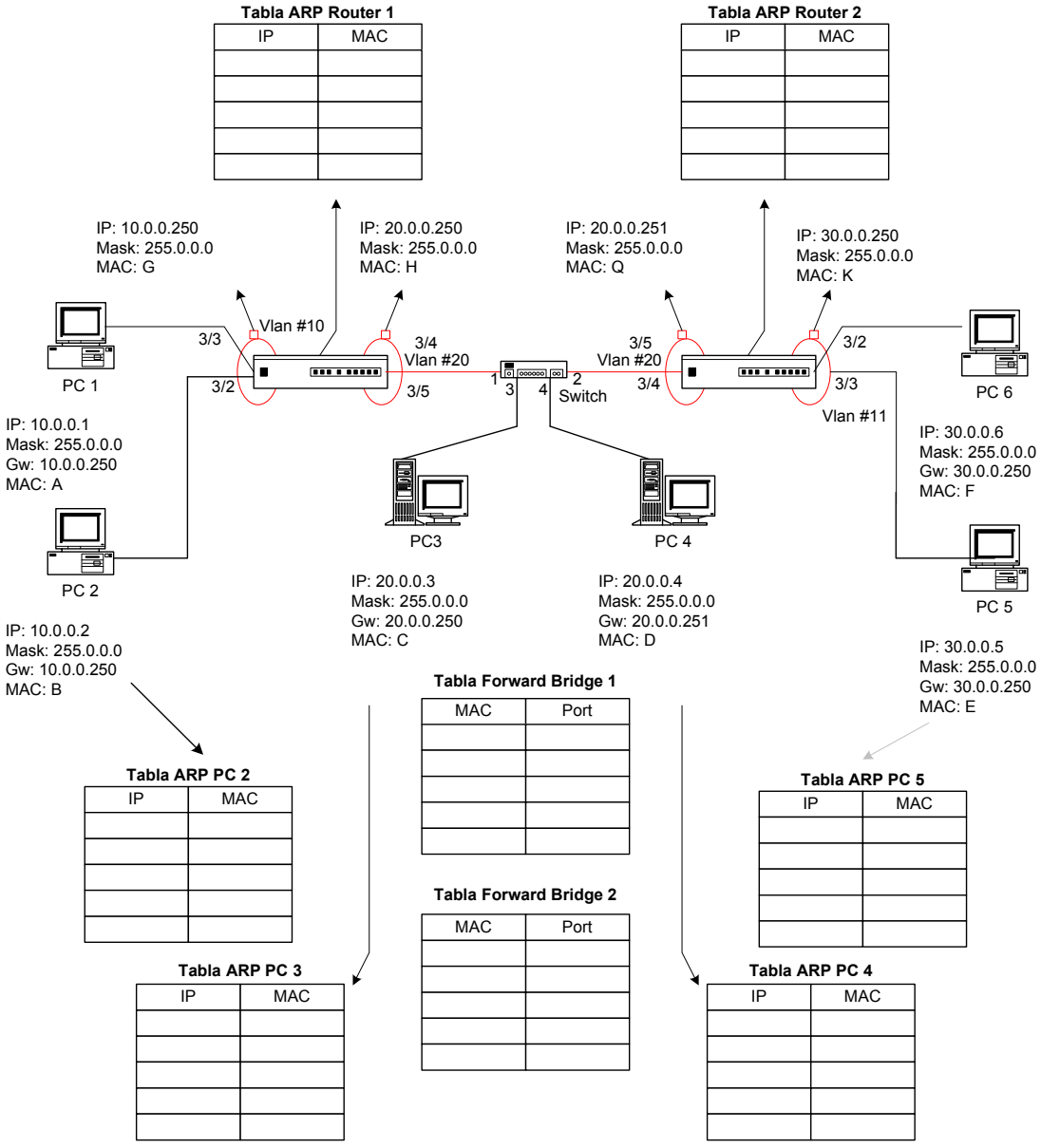


Figura 2. Carga de rutas directamente conectadas al fijar IP a las Vlans

6. Al momento de fijar la dirección IP: 10.0.0.250/8 en la VLAN 10, el **Router 1** comienza a completar su tabla de enrutamiento. Coloca esta dirección IP de la Vlan en la columna de gateway, al momento de finirle la mascara a la Vlan esta se completa en la columna

correspondiente y finalmente el router 1 calcula el prefijo de red de esa direccion IP(10.0.0.250/8) en base a la mascara obteniendo la red de destino 10.0.0.0 que surge de aplicar la AND entre la IP 10.0.0.250 y la mascara de subred 255.0.0.0.

7. Una vez definida la dirección IP y la mascara de subred para la VLAN 10 en el Router 1, esta completa una entrada en su tabla de enrutamiento con estos datos. Esto se indica en la figura 2.

8. Al momento de fijar la dirección IP: 20.0.0.250/8 en la VLAN 20, el **Router 1** comienza a completar su tabla de enrutamiento de la misma forma que el paso 6 y 7. Coloca esta dirección IP como Gateway en la tabla de ruteo, luego completa la macara de subred en la columna correspondiente y posteriormente calcula el prefijo de red 20.0.0.0, que surge de aplicar la AND entre la IP 20.0.0.250 y la mascara de subred 255.0.0.0.

9. Una vez definida la dirección IP y la mascara de subred para la VLAN 20 en el Router 1, se completa otra nueva entrada en la tabla de enrutamiento con estos datos. Esto se indica en la figura 2.

10. Al momento de fijar en el **Router 2**, la dirección IP: 20.0.0.251/8 en la VLAN 20 y la dirección IP: 30.0.0.250/8 en la VLAN 30, el **Router 2** comienza a completar su tabla de enrutamiento. Coloca las direcciones IP como gateway en filas independientes, las mascara de subred correspondiente para cada IP, calculando el Router el prefijo de red para 30.0.0.0 que surge de aplicar la AND entre la IP 30.0.0.250 y la mascara de subred 255.0.0.0 y de la misma forma completa la entrada para la red 20.0.0.0 que surge de aplicar la AND entre la IP 20.0.0.251 y la mascara de subred 255.0.0.0.

11. Las métricas para las redes directamente conectadas siempre es de 1 y el tipo de protocolo por el cual fue aprendida la red es directo, es por ello que normalmente aparece en esta columna "**Direct Connected**".

Paso 3: Agregar rutas estáticas o habilitar enrutamiento dinámico.

12. Ahora llega el momento de definir en cada Router las redes indirectamente conectadas que son parte del Sistema Autónomo. Esta definición se puede realizar de dos maneras: estática o dinámica. Se va a realizar de manera estática cargando en el Router 1 una entrada para la red 30.0.0.0 que no esta directamente conectada a este. Esta entrada se colocara en la columna correspondiente a la red. Posteriormente definimos la mascara de subred 255.0.0.0 de esta red y finalmente la dirección IP del próximo salto que hay que alcanzar para llegar a la red en cuestión, 20.0.0.251. Esta dirección IP del próximo salto indica la dirección IP del router **directamente conectado** que permitirá conocer como llegar, ya sea directa o indirectamente, a la red de destino que se esta queriendo acceder.

Operación de un Router

Tabla Router 1

Red	Mascara	Gateway	Metrica	Tipo
10.0.0.0	255.0.0.0	10.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.250	1	Direct
30.0.0.0	255.0.0.0	20.0.0.251	2	RIP

Tabla Router 2

Red	Mascara	Gateway	Metrica	Tipo
30.0.0.0	255.0.0.0	30.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.251	1	Direct
10.0.0.0	255.0.0.0	20.0.0.250	2	RIP

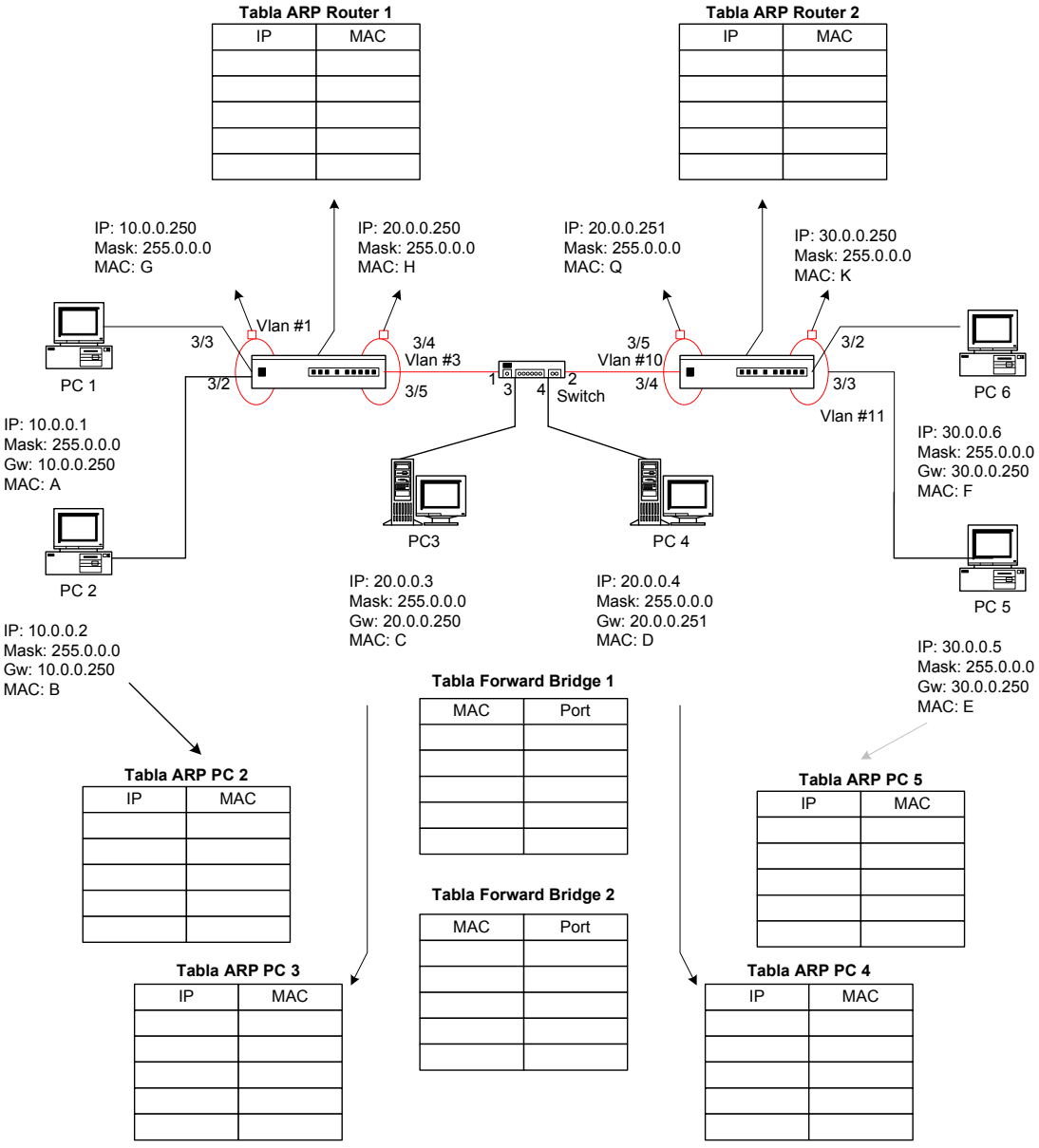


Figura 3: Carga de rutas no directamente conectadas

13. Empleando el mismo procedimiento se cargara en el **Router 2** la red 10.0.0.0, que no se encuentra directamente conectada. En la columna de red se cargara 10.0.0.0, se agregara en la columna de mascara el numero IP 255.0.0.0 y en la columna de próximo salto

Operación de un Router

el IP 20.0.0.250, correspondiente a la dirección IP del **Router 1** que esta directamente conectado al Router 2.

14. Las direcciones de Gateway cargadas en la tabla de enrutamiento de cualquier Router (**en esta caso Router 1 y 2**) solo se emplean para obtener la dirección MAC de esta dirección IP y completar de esta manera el protocolo de comunicaciones TCP/IP y por ende colocar la MAC de Destino en la trama Ethernet donde se reencapsulara el datagrama original enviado por la PC de origen. Este tipo de encamamiento se lo conoce como indirecto. Recordemos que es preciso Reencapsular una datagrama IP en una trama ethernet nueva al momento de la transmisión, ya que al recibir la trama de ingreso el Router descarta los encabezados ethernet y analiza únicamente el datagrama IP.

15. Las métricas en este caso poseen un costo de 2, ya que es preciso pasar por dos routers para alcanzar el destino correspondiente.

Paso 4: Comunicación PC B y PC E

1. Al momento de que la PC B desea enviar un mensaje a la PC E, esta debe encapsular el mensaje en un segmento UDP o TCP según si es un servicio orientado a la conexión o no, que a su vez debe ser encapsularlo en un datagrama IP, que a su vez debe ser encapsulado en una trama Ethernet. La primera tarea que debe realizar la PC B es validar si la red de destino esta en una red distinta a la propia (red de origen). En este ejemplo, la red de origen 10.0.0.0/8 esta en una red distinta a la de destino 30.0.0.0/8. Esta validación necesita realizarla siempre una estación de trabajo para identificar que tipo de encaminamiento usará para llegar el destino. Bajo este escenario la transmisión esta enmarcada en un encaminamiento indirecto ya que ambas redes, de origen y destino, son distintas.

   La PC B posee todos los datos necesarios para completar los encabezados TCP o UDP (conoce los puertos) e IP (conoce las direcciones IP), conoce la MAC de Origen pero necesita de un valor que desconoce: la dirección MAC de destino que debe completar en el encabezado Ethernet. Por tratarse de un encaminamiento indirecto este valor desconocido corresponde a la dirección física del Gateway que posee configurada la PC B. Si se tratara de un encaminamiento directo la PC B simplemente colocaría como MAC la verdadera MAC del destino de la PC E.

   Esta incógnita es develada por la misma PC B empleando mensajes ARP de petición. Para ello, la PC B deja en espera el mensaje a enviar y emite un mensaje ARP a la dirección IP del gateway que tiene cargado para que este le devuelva su dirección física. Una vez que la PC B cuenta con la MAC del Gateway, agrega esta dirección en el encabezado Ethernet y envía el mensaje de pedido de pagina WEB.

Operación de un Router

Tabla Router 1

Red	Mascara	Gateway	Metrica	Tipo
10.0.0.0	255.0.0.0	10.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.250	1	Direct
30.0.0.0	255.0.0.0	20.0.0.251	2	RIP

Tabla Router 2

Red	Mascara	Gateway	Metrica	Tipo
30.0.0.0	255.0.0.0	30.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.251	1	Direct
10.0.0.0	255.0.0.0	20.0.0.250	2	RIP

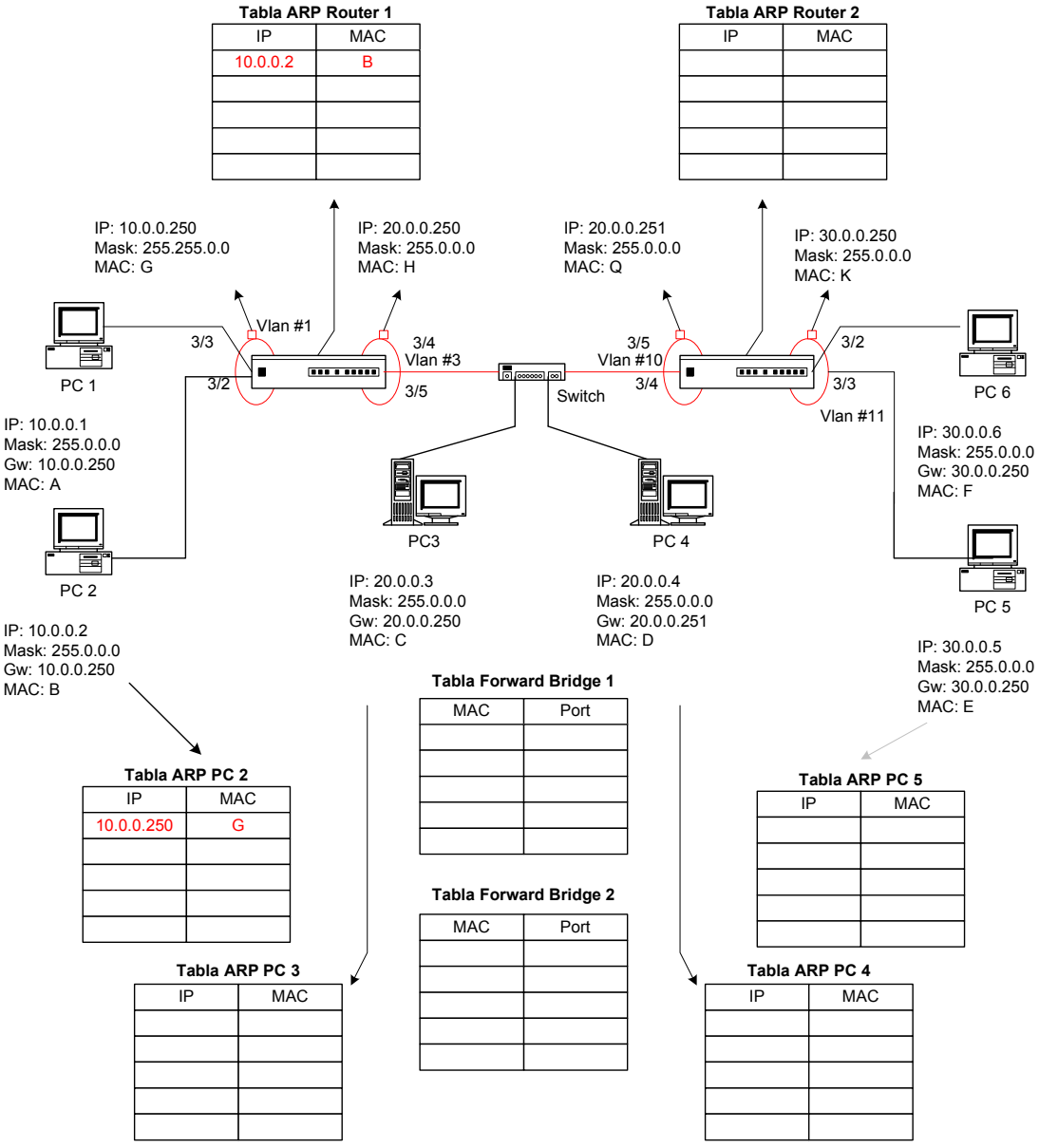


Figura 4. Armado inicial de la tabla de enrutamiento de la PC B y del Router 1.

Paso 5: Armado de tablas ARP

Operación de un Router

16. Una vez definidas los direcciones IPs, la PC B envía una trama Ethernet insertando en la trama su dirección MAC como Origen y la MAC de la PC G como destino.

17. La trama viaja por el cable (ver figura 4) hasta llegar al Router **1**. Este equipo detecta que por el puerto 3/2 esta ingresando información debido a que existe un cambio en los niveles de tensión, se sincroniza con la trama que esta llegando y almacena la trama en su buffer. El buffer permite que varias tramas lleguen simultáneamente al equipo sin que se produzcan colisiones. Una vez llegada la trama al buffer, el **Router 1** detecta que su MAC Address va como destino. Esto lo dice que es necesario realizar una conmutación IP, motivo por el cual descarta el encabezado Ethernet (MAC Destino, MAC Origen, Campo Tipo y CRC) y se queda con la parte de datos que va dentro de la trama Ethernet. Con esta información va a realizar el calculo de Checksum del encabezado del datagrama IP y si es correcto va a leer el IP de destino contenido en el encabezado IP.

18. Una vez determinado el IP de destino del datagrama va a comparar fila por fila de su tabla de ruteo para encontrar una red de destino que le indique el próximo router a alcanzar. Se aplica la mascara de cada fila con el IP de destino. En la primera fila tenemos que la red resultante es la red 30.0.0.0, por lo que al compararla con la red indicada en la misma fila no es la misma. Así que continua con la segunda fila, y aplicando la mascara de subred cargada allí obtenemos la red 30.0.0.0 que tampoco coincide con la red cargada en esa fila. Finalmente, llegando a la tercera fila ahí si encontramos una red de destino igual al resultado de aplicar la mascara cargada en al tercera fila 255.0.0.0, con el IP de destino 30.0.0.5.

19. En este punto, el router busca la dirección IP del próximo router que hay que alcanzar para llegar al destino. Para este caso particular, el IP del Gateway cargado en la tabla del Router 1 es esta en una red distinta (20.0.0.0/8) que el destino a alcanzar (30.0.0.0/8), por lo que se trata de un encaminamiento indirecto. Esto le indica al Router que va a emplear la dirección IP del Gateway cargado en la tabla de ruteo solo para obtener la MAC address del Gateway 20.0.0.251 y de esta forma tener todos los datos para reencapsultar el datagrama original en una nueva trama Ethernet. La diferencia con la trama enviada por la PC B es que ahora las MAC Address cambian (MAC de Origen será H y la MAC de Destino será Q).

20. Cada router habrá completado su tabla ARP con los datos necesarios para que la próxima trama con destino al IP 20.0.0.250 y/o al destino 20.0.0.251/8 no sea necesario realizar una petición ARP evitando de esta manera un trafico de broadcast adicional en la red. Recuerde que las peticiones ARP se realizan colocando como MAC de Destino Broadcast (**FF-FF-FF-FF-FF-FF**) y ese trafico llega a todos los usuarios dentro de la esa red.

21. Ahora el Router 1 envía la trama Ethernet al Router 2, pero antes que eso decrementa en 1 el TTL del datagrama IP. En el caso de que el TTL sea igual a 0 este lo descarta y suspende la trasmisión.

Operación de un Router

Tabla Router 1

Red	Mascara	Gateway	Metrica	Tipo
10.0.0.0	255.0.0.0	10.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.250	1	Direct
30.0.0.0	255.0.0.0	20.0.0.251	2	RIP

Tabla Router 2

Red	Mascara	Gateway	Metrica	Tipo
30.0.0.0	255.0.0.0	30.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.251	1	Direct
10.0.0.0	255.0.0.0	20.0.0.250	2	RIP

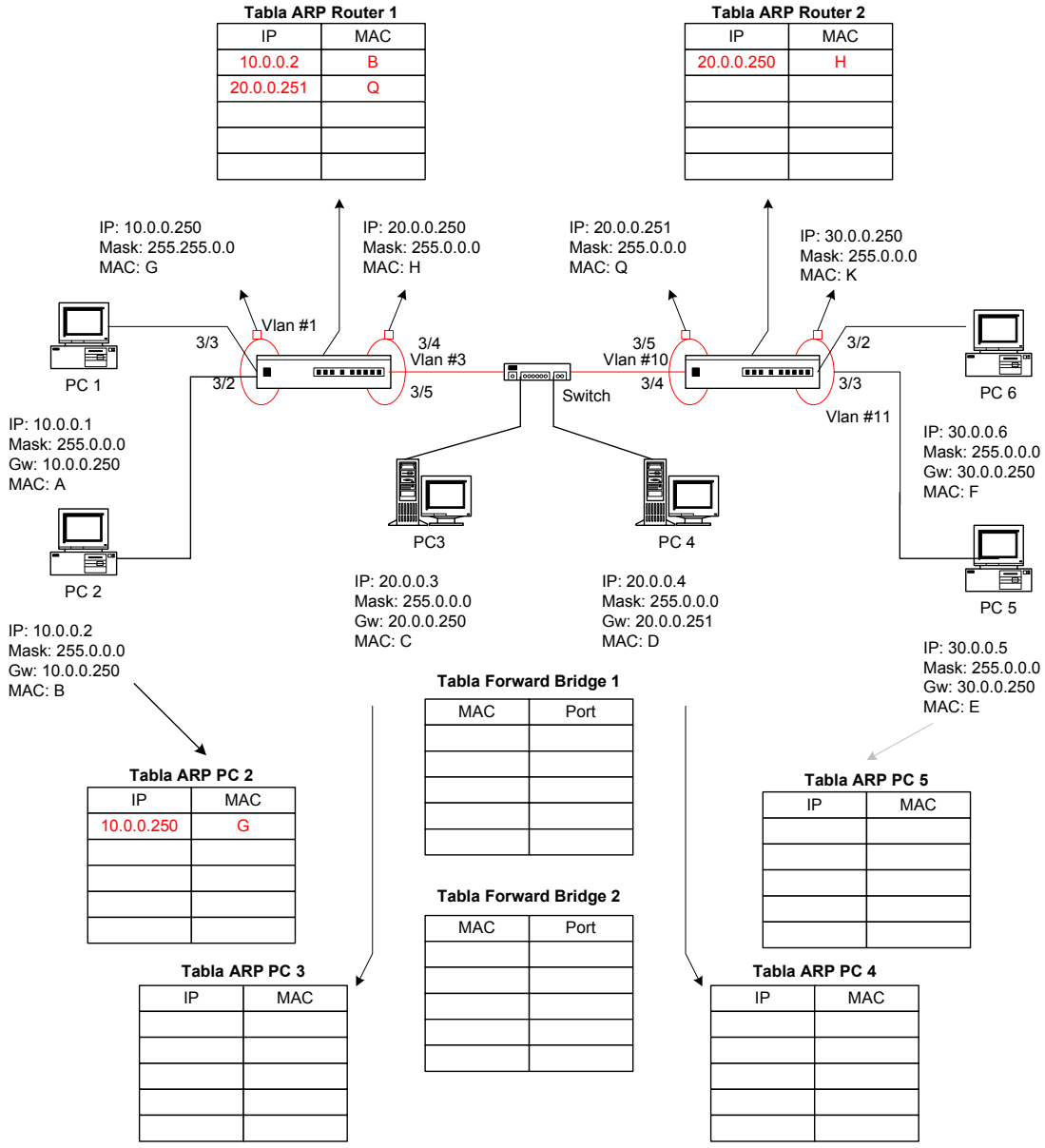


Figura 4. Datagrama reencapsulado en una trama Ethernet y enviado hacia el próximo salto 20.0.0.251.

Operación de un Router

Tabla Router 1

Red	Mascara	Gateway	Metrica	Tipo
10.0.0.0	255.0.0.0	10.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.250	1	Direct
30.0.0.0	255.0.0.0	20.0.0.251	2	RIP

Tabla Router 2

Red	Mascara	Gateway	Metrica	Tipo
30.0.0.0	255.0.0.0	30.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.251	1	Direct
10.0.0.0	255.0.0.0	20.0.0.250	2	RIP

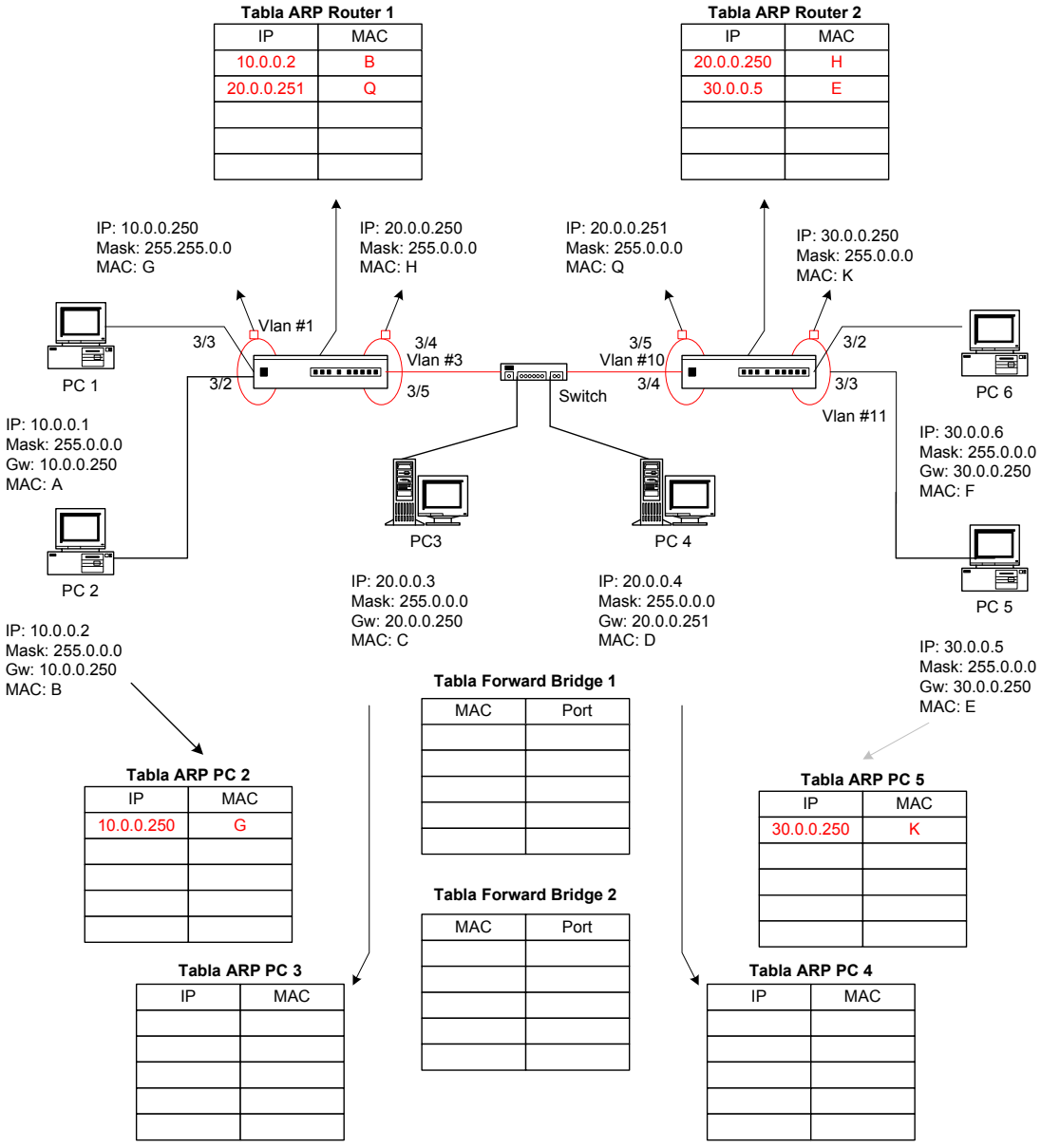


Figura 5. Datagrama reencapsulado en una trama Ethernet y enviado directamente al destino 30.0.0.5.

22. Cuando la trama Ethernet llegar al router 2, este detectara que su MAC esta cargada como MAC de destino, descartara el encabezado Ethernet y se quedara para el análisis del datagrama IP completo. Nuevamente, calcula el checksum del datagrama IP para detectar

Operación de un Router

errores y sino existieran errores finalmente leera la dirección IP de destino. A esta dirección le aplicara cada una de las mascaras de subred cargadas en cada fila de su tabla de enrutamiento, hasta encontrar en la columna de **red** una red de destino que coincida con la red del IP de destino que va cargada en el datagrama IP.

En este caso la primera fila coincide con la red de destino por lo que automáticamente procede a leer la IP del próximo saldo a donde enviar este datagrama. A diferencia del paso anterior, ahora la red del Gateway cargado en al tabla de enrutamiento esta en la misma red que el IP de destino de la PC E. Estamos hablando entonces, de un encaminamiento directo por lo que el router directamente envía un mensaje ARP hacia la PC E consultado su MAC Address. Una vez que el Router 2 obtiene la MAC Address de la PC E, el propio router reencapsula el datagrama original en una nueva trama Ethernet pero ahora las MAC Addres de destino y Origen son K y E, respectivamente. Como sucedió anteriormente, antes de que el Router 2 genere la nueva trama Ethernet, este decrementa en 1 el TTL, descartando el datagrama si este llega a un valor de 0.

Como se observa en toda la cadena transmisión las MAC addres van cambiando al pasar de una red a otra, mientras que las direcciones IP de origen y destino nunca cambian. En la figura 5 se observan las tablas ARP del Router 2 y de la PC E actualizadas después de realizar las correspondientes transacciones (peticio y respuesta) ARP.

23. habrá completado su tabla ARP con los datos necesarios para que la próxima trama con destino al IP 20.0.0.250 y/o al destino 20.0.0.251/8 no sea necesario realizar una petición ARP

Paso 5: Tablas ARP actualizadas

24. Cuando todas las estaciones de trabajo transmitieron, las tablas ARP de las PCs y dispositivos quedaran como se indica en la figura.

25. Las tablas ARP completas que cada dispositivo en las redes actualizan y mantienen permiten evitar a futuro el **broadcast** ARP, consultando directamente en estas tablas locales cual es la MAC Address del IP a alcanzar.

26. Se dijo en anteriores descripciones, las tablas ARP solo tienen significado local para una PC dentro de la red donde ella reside. El único dispositivo que en su tabla ARP contiene distintas redes es el router, ya que va a tener tantas redes distintas en su tabla ARP como redes interconecte directamente.

Operación de un Router

Tabla Router 1

Red	Mascara	Gateway	Metrica	Tipo
10.0.0.0	255.0.0.0	10.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.250	1	Direct
30.0.0.0	255.0.0.0	20.0.0.251	2	RIP

Tabla Router 2

Red	Mascara	Gateway	Metrica	Tipo
30.0.0.0	255.0.0.0	30.0.0.250	1	Direct
20.0.0.0	255.0.0.0	20.0.0.251	1	Direct
10.0.0.0	255.0.0.0	20.0.0.250	2	RIP

Tabla ARP Router 1

IP	MAC
10.0.0.2	B
20.0.0.251	Q
10.0.0.1	A
20.0.0.3	C
20.0.0.4	D

Tabla ARP Router 2

IP	MAC
20.0.0.250	H
30.0.0.5	E
30.0.0.6	F
20.0.0.3	C
20.0.0.4	D

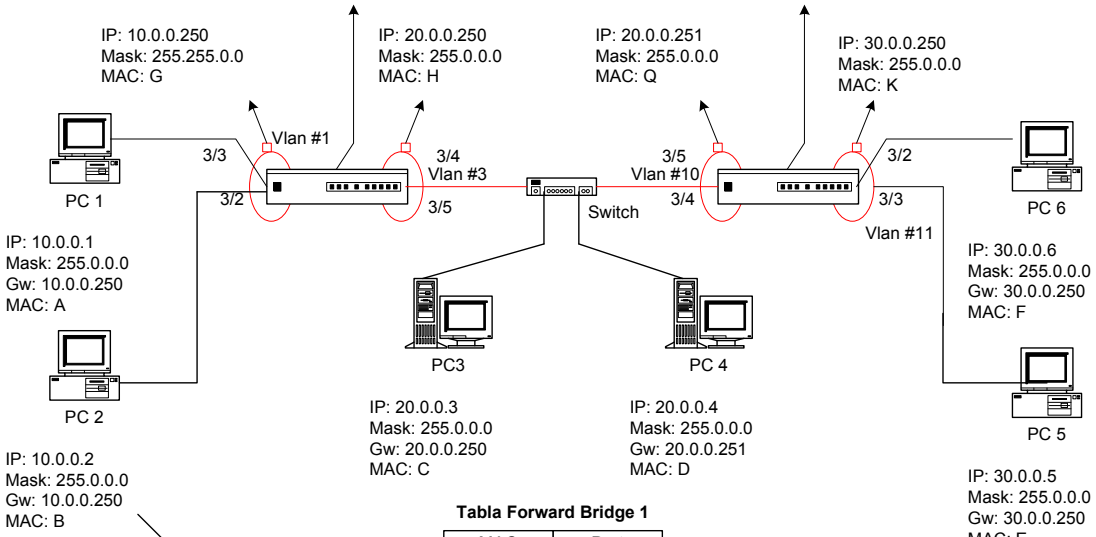


Tabla Forward Bridge 1

MAC	Port

Tabla Forward Bridge 2

MAC	Port

Tabla ARP PC 2

IP	MAC
10.0.0.250	G
10.0.0.1	A

Tabla ARP PC 3

IP	MAC
20.0.0.250	H
20.0.0.251	Q
20.0.0.4	D

Tabla ARP PC 4

IP	MAC
20.0.0.251	Q
20.0.0.250	H
20.0.0.3	C

Tabla ARP PC 5

IP	MAC
30.0.0.250	K
30.0.0.6	F

Figura 6. Tablas ARP de PCs y Routers actualizadas cuando todos los dispositivos generaron trafico.

Paso 6: Completar las tablas de forward de los switches o Bridges

Operación de un Router

27. Una vez completadas las tablas ARP y de conmutación IP, ahora procederemos a completar las tablas de conmutación de capa 2 de los dispositivos indicados en la figura.

28. La pregunta es en que caso el Router trabajara como Bridge o Switch, es decir cuando actuara como un conmutador a nivel enlace de datos. La respuesta es muy sencilla, cuando la IP de Destino y la IP de Origen del datagrama a enviar por una estación de trabajo u otro dispositivo estén en la misma red, donde solo se requiere de un conmutador de capa 2 para lograr la interoperatividad y conmutación entre estas estaciones de trabajo.

29. Suponiendo que la PC A se comunicara con la PC B, se puede observar que estas PCs poseen una misma dirección de red al aplicarle la mascara definida para la Vlan 10. En este caso, la PC A completa su datagrama IP, con IP de Origen 10.0.0.1 e IP de destino 10.0.0.2

30. Cuando la PC A debe encapsular este datagrama en una trama Ethernet lo que debe conseguir es la dirección física de la IP de destino 10.0.0.2. Por este motivo genera un pedido ARP directamente a la IP de Destino 10.0.0.2 consultándole sobre su MAC Address. Como el mensaje ARP de petición emplea una MAC de Destino Broadcast (**FF-FF-FF-FF-FF-FF**) esto hace que la trama llegue a todos los dispositivos conectados a la VLAN 10 incluido el Router 1. Es donde este dispositivo para aprovechar el broadcast de la petición ARP aprende y registra en su tabla ARP la MAC de la PC A, para que si en algún momento el router 1 debe enviar información hacia la PC A el dato de su MAC lo saque de la tabla ARP actualizada, evitando realizar una nueva petición ARP empleando Broadcast. Esto se indica en la figura 6. Además, el bridge 1 actuando en el router 1 también aprende que la MAC A ingreso por el puerto 3/3. Luego el bridge procede a realizar el broadcast indicado como MAC de destino. Ver figura 6.

31. Una vez que la PC B, recibe la petición ARP, procesa y elabora la respuesta y la envía hacia la PC A (ahora la respuesta ya es **unicast** a nivel enlace de datos), esta respuesta ARP ingresara al bridge por el puerto 3/2, dato que es registrado por el dispositivo. Luego el bridge lee la MAC de destino del ARP de respuesta y lo busca en su tabla. Como la PC A ya transmitió anteriormente a este mensaje de respuesta ya esta registrada la MAC de A y por que puerto ingreso. Motivo por el cual el bridge simplemente procede a realizar la transferencia de la trama ARP de respuesta hacia la PC A a través del puerto 3/3 como esta indicado en la tabla de conmutación del bridge 1. Ver figura 7.

32. Finalmente, la PC A recibe la respuesta ARP, completa su tabla ARP local, completa la trama Ethernet con MAC de Destino B y Origen A y transmite la información con destino hacia B. Cuando esta trama llega el Router este ya tiene actualizada su tabla de conmutación de capa 2 gracias a los mensajes ARP de petición y respuesta. Por lo que, la trama que ingresa por el puerto 3/3 es renviada hacia el puerto 3/2, donde esta físicamente conectada la PC B, es decir el destino al que quiero llegar. Ver figura 7.

33. Los mismo sucede con las **PCs C** y **D** en la red 20.0.0.0/8 y con las **PCs E** y **F**, donde cada una generara mensajes ARP de petición y respuesta que Irán actualizando no solo sus tablas ARP, sino también la tabla ARP de los dos Routers 1 y 2 y las tablas de

forward de los dos switches actuando en cada routers. Esto puede verse en la figura 8.

34. Como se observa en las figuras ninguna PC dentro de una Vlan tiene MAC Address de PCs que son parte de otra Vlan y por ende de otra red IP. Ver figura 8.

5.2.11 Enrutamiento Dinámico

El enrutamiento dinámico consiste en el proceso de intercambio de información de enrutamiento en forma automática y sin intervención del administrador de la red. La única tarea que realiza el administrador de la red es la habilitación del protocolo de ruteo dinámico únicamente en aquella **interfase o vlan** que interconecta uno o varios enrutadores para comenzar con el intercambio de información de enrutamiento.

Existen dos protocolos de enrutamiento dinámico que trataremos en este documento: RIP y OSPF. Ambos protocolos son conocidos como IGP o protocolos de pasarela interior.

5.2.11.1 RIP

El protocolo de información de enrutamiento (RIP) es un protocolo que emplea el algoritmo de Bellman Fort para el manejo de rutas y las métricas asociadas a estas. La métrica que emplea es por cantidad de routers que existen entre un origen y un destino sin importar la capacidad o retardo de los enlaces. Es por esto, que normalmente el camino mas corto no siempre es el camino mas rápido o el que menor retardo presenta, pero RIP no discrimina esto.

En la figura se observa un esquema de enrutamiento con tres routers formando interconectados todos contra todos. Esta topología es muy útil porque tiene redundancia y contingencia de fallos de un enlace para que la operación de la red no se interrumpa infinitamente hasta que se repara el corte del enlace. Al contrario, después de 30 segundos la “red” gracias al protocolo de enrutamiento dinámico permite encontrar otro camino alternativo para ir del origen al destino.

En condiciones normales de operación, esto es sin fallas de enlaces ni equipamiento las tablas de enrutamiento se arman de la forma indicada en la figura. Como puede verse en la tabla del router 1, para llegar a la red 30.0.0.0/8 tenemos dos caminos, uno a través del Router 2 mas directa o con menos costo y otra pasando por el Router 3 para posteriormente llegar el router 2. En este ultimo caso puede verse que siempre es mas conveniente ir por el camino mas corto siempre y cuando los enlaces sean de la misma capacidad de transmisión y no diferenciando el retardo entre ellos. Para el caso de la red 50.0.0.0/8 tenemos dos opciones, a través del Router 2 o a través del Router 3, como la métrica es la misma (hay que pasar por dos enrutadores) de igual forma, se adopta la que primero se aprenda.

Operación de un Router

Tabla Router 1

Red	Mascara	Gateway.	Metrica	Protocolo
10.0.0.0	255.0.0.0	10.0.0.6	1	DC
20.0.0.0	255.0.0.0	20.0.0.6	1	DC
40.0.0.0	255.0.0.0	40.0.0.6	1	DC
30.0.0.0	255.0.0.0	20.0.0.7	2	RIP
60.0.0.0	255.0.0.0	40.0.0.7	2	RIP
50.0.0.0	255.0.0.0	20.0.0.7	2	RIP

Tabla Router 2

Red	Mascara	Gateway.	Metrica	Protocolo
30.0.0.0	255.0.0.0	30.0.0.7	1	DC
20.0.0.0	255.0.0.0	20.0.0.7	1	DC
50.0.0.0	255.0.0.0	50.0.0.7	1	DC
60.0.0.0	255.0.0.0	50.0.0.6	2	RIP
10.0.0.0	255.0.0.0	20.0.0.6	2	RIP
40.0.0.0	255.0.0.0	20.0.0.6	2	RIP

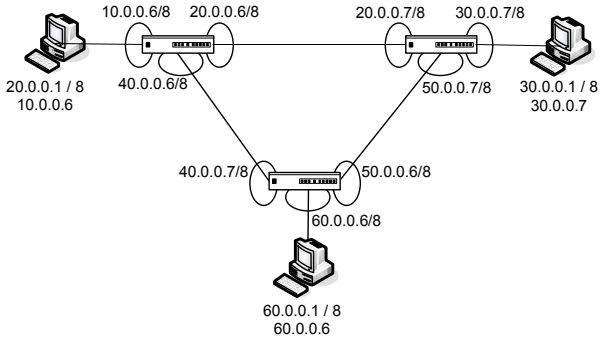


Tabla Router 3

Red	Mascara	Gateway.	Metrica	Protocolo
60.0.0.0	255.0.0.0	60.0.0.6	1	DC
40.0.0.0	255.0.0.0	40.0.0.7	1	DC
50.0.0.0	255.0.0.0	50.0.0.6	1	DC
10.0.0.0	255.0.0.0	40.0.0.6	2	RIP
30.0.0.0	255.0.0.0	50.0.0.7	2	RIP
20.0.0.0	255.0.0.0	50.0.0.7	2	RIP

5.2.11.1.1 RIP

En el siguiente esquema de conexión se muestra el formato de los mensajes rip, los niveles de encapsulado del modelo TCP/IP y como se van armando las tablas.

Paso 1: En este momento se definen las Vlans e interfaces IP de cada Vlan en todos los enrutadores. Posteriormente se habilita el protocolo de enrutamiento RIP únicamente en las Vlans que interconectan enrutadores.

Tabla Router 1

Red	Mascara	Gateway.	Metrica	Protocolo
10.0.0.0	255.0.0.0	10.0.0.6	1	DC
20.0.0.0	255.0.0.0	20.0.0.6	1	DC

Tabla Router 2

Red	Mascara	Gateway.	Metrica	Protocolo
30.0.0.0	255.0.0.0	30.0.0.7	1	DC
20.0.0.0	255.0.0.0	20.0.0.7	1	DC

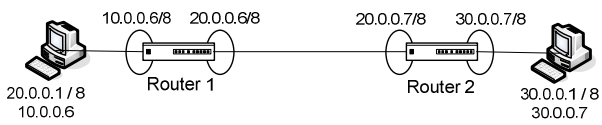


Figura 1. Configuración inicial de los enrutadores.

Operación de un Router

Paso 2. Cada enrutador arma un mensaje de envío RIP indicando en el mensaje inicial las redes que el únicamente conoce como directamente conectadas. Se indica en la figura 2, los encabezados TCP, IP y Ethernet. Donde puede verse que se emplea el puerto UDP 520 para el envío del mensaje, la IP de origen es la de la vlan definida para participar del intercambio de mensajes RIP que como se ve es la que interconecta el router 2, como IP de destino se emplea la dirección de broadcast dirigida dentro de la red 20.0.0.08/8, como MAC de Origen la dirección de la Vlan por donde sale el mensaje RIP y como MAC de Destino inicialmente es la dirección de broadcast Ethernet.

Tabla Router 1

Red	Mascara	Gateway.	Metrica	Protocolo
10.0.0.0	255.0.0.0	10.0.0.6	1	DC
20.0.0.0	255.0.0.0	20.0.0.6	1	DC

Tabla Router 2

Red	Mascara	Gateway.	Metrica	Protocolo
30.0.0.0	255.0.0.0	30.0.0.7	1	DC
20.0.0.0	255.0.0.0	20.0.0.7	1	DC

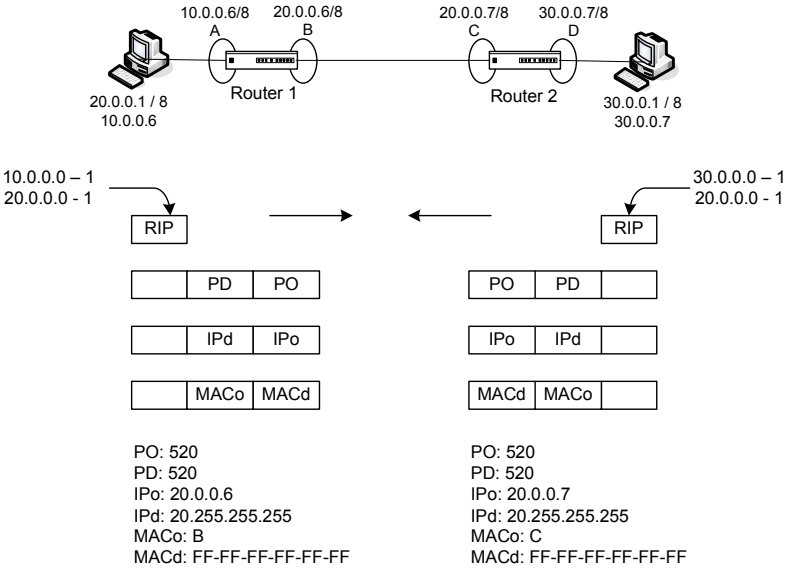


Figura 2. Cada Router Arma un mensaje para comenzar con el envío.

Paso 3. el router 1 recibe el mensaje rip del router 2. Lo primero que hace es validar la MAC de Destino y como es broadcast debe procesarla. Después lee la IP de destino y como es una dirección de broadcast dirigido debe procesarla y finalmente lee el puerto de destino UDP 520 y se da cuenta que es un mensaje RIP para actualizar su tabla de ruteo. Al analizar el mensaje RIP toma la primera entrada y se queda con la red 30.0.0.0.

Como esta red no esta cargada la agrega en una línea nueva, deduciendo la mascara de subred y extrayendo el próximo salto o Gateway del datagrama empleado para enviar este mensaje RIP donde el router 2 agrego su IP de Origen 20.0.0.7. Se suma uno a la métrica que llego en el mensaje. La red 20.0.0.0, no se carga en la tabla de enrutamiento porque ya existe una entrada con una métrica mejor a la que viene cargada en el mensaje RIP.

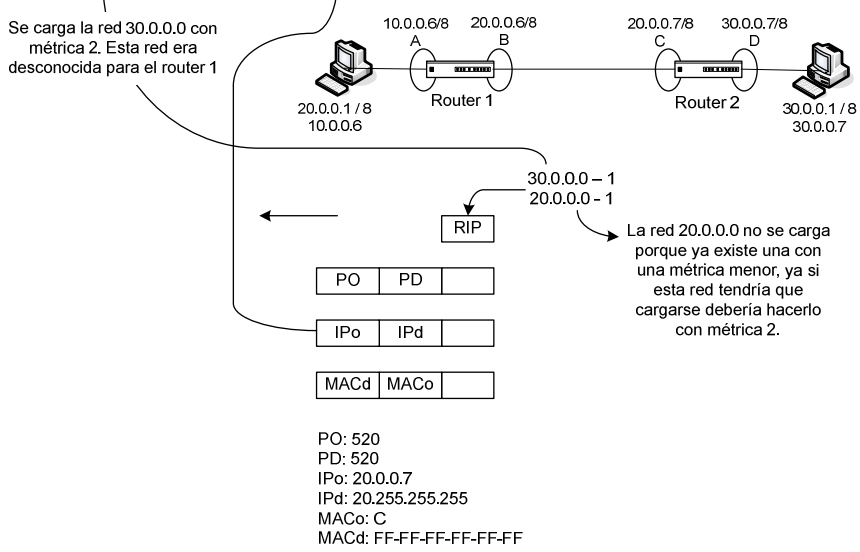
Operación de un Router

Tabla Router 1

Red	Mascara	Gateway.	Metrica	Protocolo
10.0.0.0	255.0.0.0	10.0.0.6	1	DC
20.0.0.0	255.0.0.0	20.0.0.6	1	DC
30.0.0.0	**255.0.0.0**	**20.0.0.7**	**2**	**RIP**

Tabla Router 2

Red	Mascara	Gateway.	Metrica	Protocolo
30.0.0.0	255.0.0.0	30.0.0.7	1	DC
20.0.0.0	255.0.0.0	20.0.0.7	1	DC



PO: 520
PD: 520
IPo: 20.0.0.7
IPd: 20.255.255.255
MACo: C
MACd: FF-FF-FF-FF-FF-FF

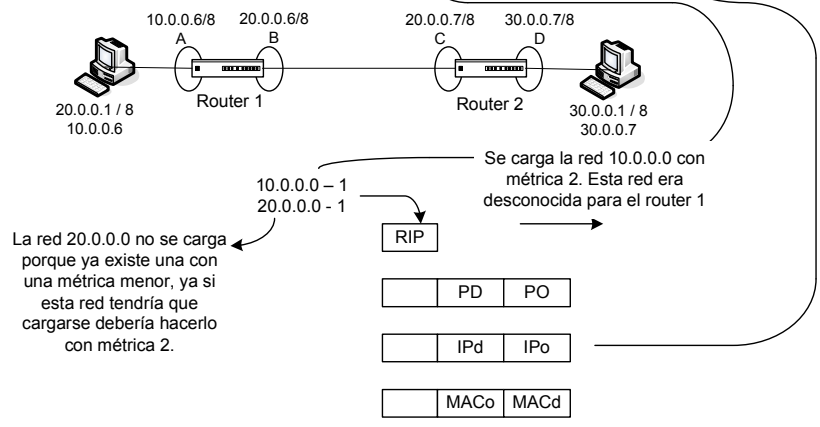
Figura 3. Actualización de la tabla del Router 1.

Tabla Router 1

Red	Mascara	Gateway.	Metrica	Protocolo
10.0.0.0	255.0.0.0	10.0.0.6	1	DC
20.0.0.0	255.0.0.0	20.0.0.6	1	DC
30.0.0.0	**255.0.0.0**	**20.0.0.7**	**2**	**RIP**

Tabla Router 2

Red	Mascara	Gateway.	Metrica	Protocolo
30.0.0.0	255.0.0.0	30.0.0.7	1	DC
20.0.0.0	255.0.0.0	20.0.0.7	1	DC
10.0.0.0	**255.0.0.0**	**20.0.0.6**	**2**	**RIP**



PO: 520
PD: 520
IPo: 20.0.0.6
IPd: 20.255.255.255
MACo: B
MACd: FF-FF-FF-FF-FF-FF

Figura 4. Actualización de la tabla del Router 2.

Operación de un Router

5.2.11.1.2 RIP y Split Horizon

El problema que surge en las redes IP con mensajes RIP es cuando una interfaz IP sale fuera de servicio y es el router el que comienza a recibir la misma red por la **Interfaz IP o Vlan** por donde las enviaba anteriormente. El problema se origina cuando los routers envian la misma red que recibio por la misma interfaz por donde fue recibida. En las siguientes figuras se observa el problema mencionado.

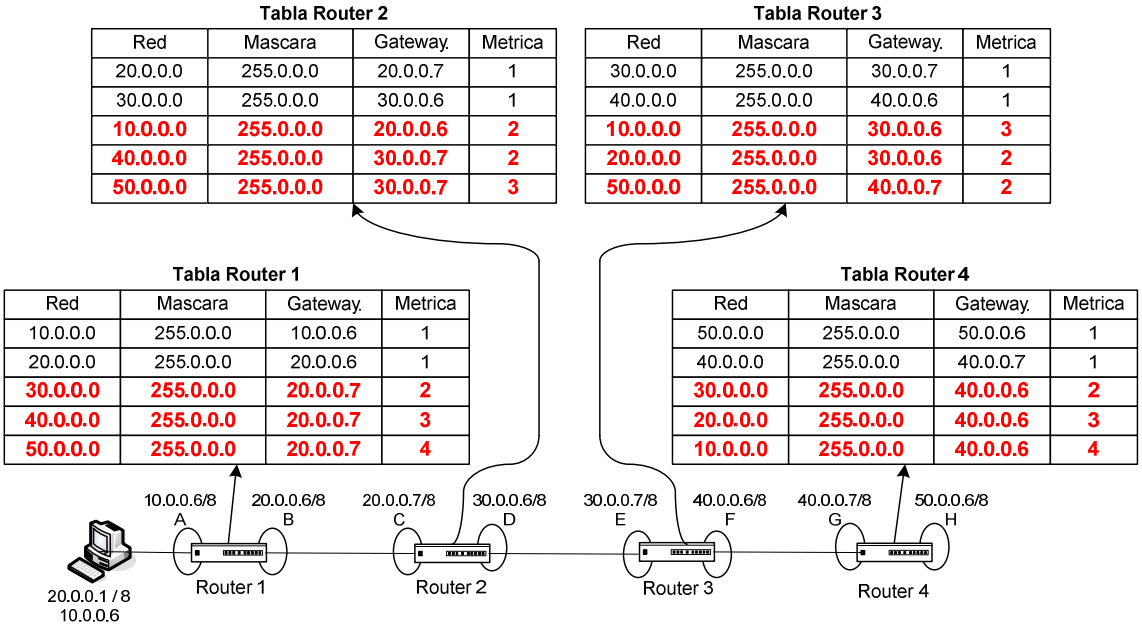


Figura 1: tablas de ruteo coherentes y consistentes.

Operación de un Router

Tabla Router 2

Red	Mascara	Gateway.	Metrica
20.0.0.0	255.0.0.0	20.0.0.7	1
30.0.0.0	255.0.0.0	30.0.0.6	1
10.0.0.0	**255.0.0.0**	**20.0.0.6**	**2**
40.0.0.0	**255.0.0.0**	**30.0.0.7**	**2**
50.0.0.0	**255.0.0.0**	**30.0.0.7**	**3**

Tabla Router 3

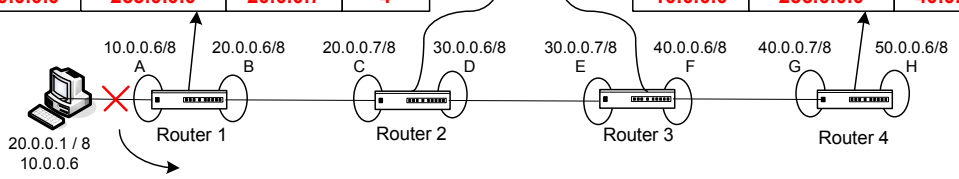
Red	Mascara	Gateway.	Metrica
30.0.0.0	255.0.0.0	30.0.0.7	1
40.0.0.0	255.0.0.0	40.0.0.6	1
10.0.0.0	**255.0.0.0**	**30.0.0.6**	**3**
20.0.0.0	**255.0.0.0**	**30.0.0.6**	**2**
50.0.0.0	**255.0.0.0**	**40.0.0.7**	**2**

Tabla Router 1

Red	Mascara	Gateway.	Metrica
20.0.0.0	255.0.0.0	20.0.0.6	1
30.0.0.0	**255.0.0.0**	**20.0.0.7**	**2**
40.0.0.0	**255.0.0.0**	**20.0.0.7**	**3**
50.0.0.0	**255.0.0.0**	**20.0.0.7**	**4**

Tabla Router 4

Red	Mascara	Gateway.	Metrica
50.0.0.0	255.0.0.0	50.0.0.6	1
40.0.0.0	255.0.0.0	40.0.0.7	1
30.0.0.0	**255.0.0.0**	**40.0.0.6**	**2**
20.0.0.0	**255.0.0.0**	**40.0.0.6**	**3**
10.0.0.0	**255.0.0.0**	**40.0.0.6**	**4**



Suponiendo que la interfaz IP 10.0.0.6 se cae. Esto hace que el Router 1 borre su entrada directa para la red 10.0.0.0. Por este motivo va a comenzar a recibir actualizaciones del router 2 pero a la vez el va a enviar actualizaciones para la red 10.0.0.0. Como R2, R3 y R4 aprendieron actualizaciones de R1 para la red 10.0.0.0 van a comenzar a aprender y a aumentar en 1 la métrica para la red 10.0.0.0 hasta el conteo a infinito (16 saltos).

Figura 2: Salida de servicio de la interfaz IP o Vlan 10.0.0.0.

Operación de un Router

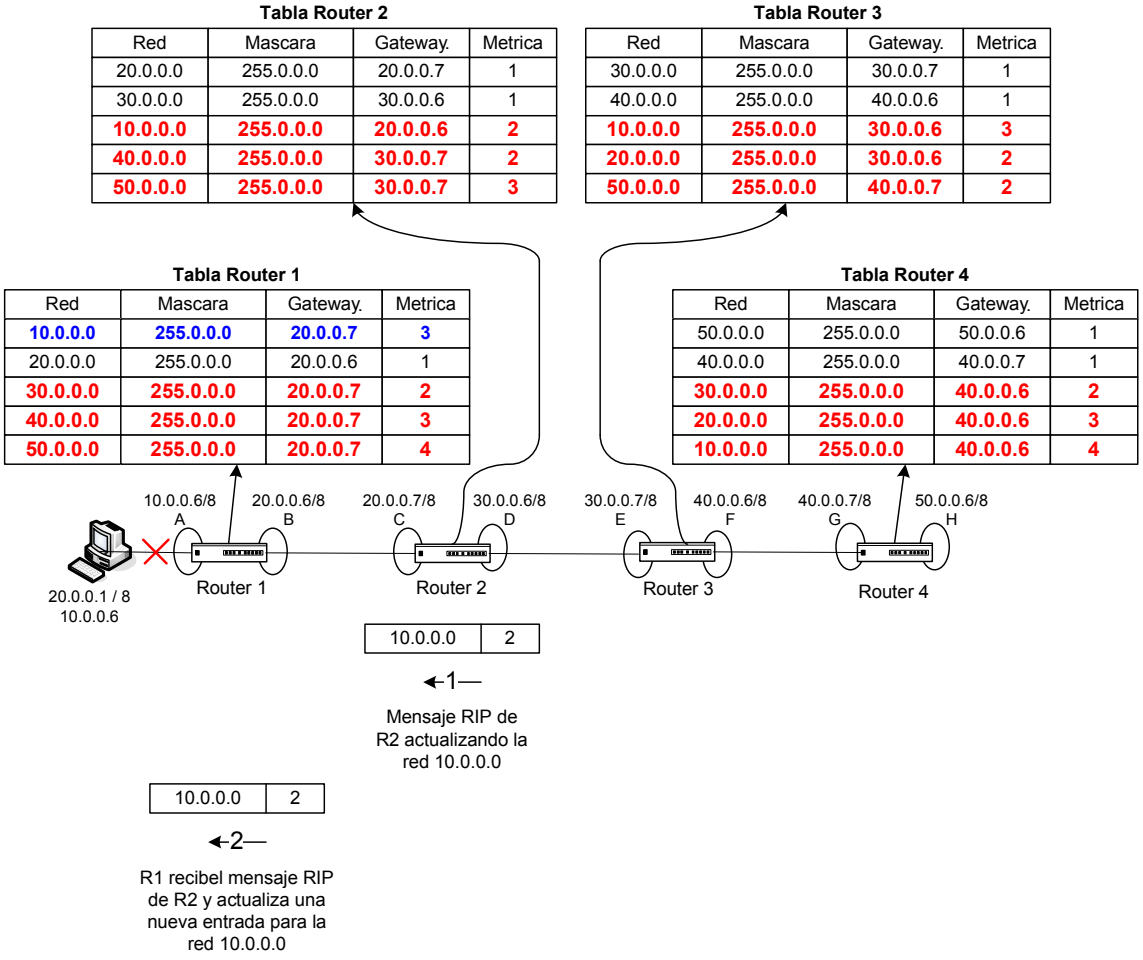


Figura 3: R1 comienza a recibir la actualización de la red 10.0.0.0 por la Vlan 20.

Operación de un Router

Tabla Router 2

Red	Mascara	Gateway.	Metrica
20.0.0.0	255.0.0.0	20.0.0.7	1
30.0.0.0	255.0.0.0	30.0.0.6	1
10.0.0.0	**255.0.0.0**	**20.0.0.6**	**4**
40.0.0.0	**255.0.0.0**	**30.0.0.7**	**2**
50.0.0.0	**255.0.0.0**	**30.0.0.7**	**3**

Tabla Router 3

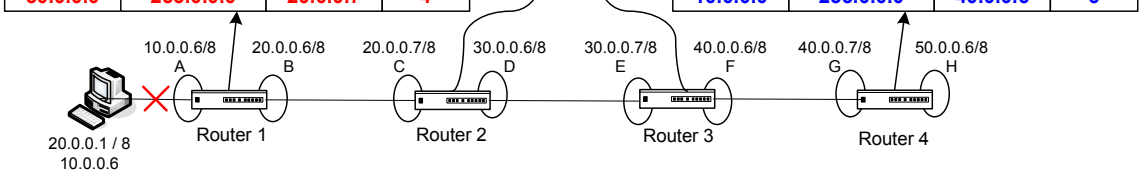
Red	Mascara	Gateway.	Metrica
30.0.0.0	255.0.0.0	30.0.0.7	1
40.0.0.0	255.0.0.0	40.0.0.6	1
10.0.0.0	**255.0.0.0**	**30.0.0.6**	**5**
20.0.0.0	**255.0.0.0**	**30.0.0.6**	**2**
50.0.0.0	**255.0.0.0**	**40.0.0.7**	**2**

Tabla Router 1

Red	Mascara	Gateway.	Metrica
10.0.0.0	**255.0.0.0**	**20.0.0.7**	**3**
20.0.0.0	255.0.0.0	20.0.0.6	1
30.0.0.0	**255.0.0.0**	**20.0.0.7**	**2**
40.0.0.0	**255.0.0.0**	**20.0.0.7**	**3**
50.0.0.0	**255.0.0.0**	**20.0.0.7**	**4**

Tabla Router 4

Red	Mascara	Gateway.	Metrica
50.0.0.0	255.0.0.0	50.0.0.6	1
40.0.0.0	255.0.0.0	40.0.0.7	1
30.0.0.0	**255.0.0.0**	**40.0.0.6**	**2**
20.0.0.0	**255.0.0.0**	**40.0.0.6**	**3**
10.0.0.0	**255.0.0.0**	**40.0.0.6**	**6**



3	10.0.0.0

—3→

R1 envia mensaje RIP actualizando la red 10.0.0.0

3	10.0.0.0

—4→

R1 recibe mensaje de actualización y como antes recibía mensajes de actualización de R1 asume que cambio la metrica.

4	10.0.0.0

—5→

R2 envía mensaje RIP actualizando la red 10.0.0.0

4	10.0.0.0

—6→

R3 recibe mensaje de actualización y como antes recibía mensajes de actualización de R2 asume que cambio la métrica.

5	10.0.0.0

—7→

R2 envía mensaje RIP actualizando la red 10.0.0.0

5	10.0.0.0

—8→

R4 recibe mensaje de actualización y como antes recibía mensajes de actualización de R3 asume que cambio la métrica.

6	10.0.0.0

←9—

R4 envía mensaje RIP actualizando la red 10.0.0.0 porque asume un cambio hacia R3

Figura 4: R1 comienza a recibir la actualización de la red 10.0.0.0 por la Vlan 20. Se observa que van aumentando las métricas en los routers 2, 3 y 4.

Operación de un Router

Tabla Router 2

Red	Mascara	Gateway.	Metrica
20.0.0.0	255.0.0.0	20.0.0.7	1
30.0.0.0	255.0.0.0	30.0.0.6	1
10.0.0.0	**255.0.0.0**	**30.0.0.7**	**8**
40.0.0.0	**255.0.0.0**	**30.0.0.7**	**2**
50.0.0.0	**255.0.0.0**	**30.0.0.7**	**3**

Tabla Router 3

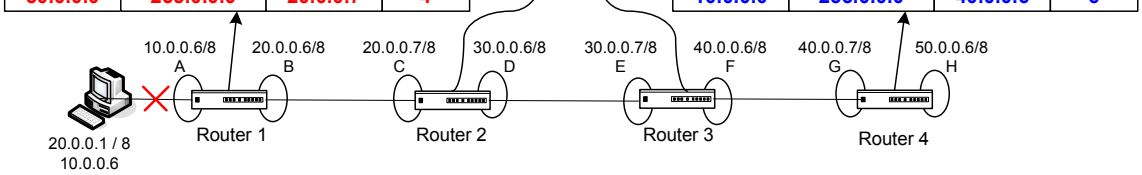
Red	Mascara	Gateway.	Metrica
30.0.0.0	255.0.0.0	30.0.0.7	1
40.0.0.0	255.0.0.0	40.0.0.6	1
10.0.0.0	**255.0.0.0**	**40.0.0.7**	**7**
20.0.0.0	**255.0.0.0**	**30.0.0.6**	**2**
50.0.0.0	**255.0.0.0**	**40.0.0.7**	**2**

Tabla Router 1

Red	Mascara	Gateway.	Metrica
10.0.0.0	**255.0.0.0**	**20.0.0.7**	**9**
20.0.0.0	255.0.0.0	20.0.0.6	1
30.0.0.0	**255.0.0.0**	**20.0.0.7**	**2**
40.0.0.0	**255.0.0.0**	**20.0.0.7**	**3**
50.0.0.0	**255.0.0.0**	**20.0.0.7**	**4**

Tabla Router 4

Red	Mascara	Gateway.	Metrica
50.0.0.0	255.0.0.0	50.0.0.6	1
40.0.0.0	255.0.0.0	40.0.0.7	1
30.0.0.0	**255.0.0.0**	**40.0.0.6**	**2**
20.0.0.0	**255.0.0.0**	**40.0.0.6**	**3**
10.0.0.0	**255.0.0.0**	**40.0.0.6**	**6**



10.0.0.0	6

◄9—

R4 envía mensaje RIP actualizando la red 10.0.0.0 porque asume un cambio hacia R3

10.0.0.0	6

◄10—

R3 recibe mensaje de actualización y como antes recibía mensajes de actualización de R4 asume que cambio la métrica.

10.0.0.0	7

◄11—

R3 envía mensaje RIP actualizando la red 10.0.0.0 porque asume un cambio hacia R2

10.0.0.0	7

◄12—

R2 recibe mensaje de actualización y como antes recibía mensajes de actualización de R3 asume que cambio la métrica.

10.0.0.0	8

◄13—

R2 envía mensaje RIP actualizando la red 10.0.0.0 porque asume un cambio hacia R1

10.0.0.0	8

◄14—

R1 recibe mensaje de actualización y como antes recibía mensajes de actualización de R2 asume que cambio la métrica.

9	10.0.0.0

—15►

R1 envía mensaje RIP actualizando la red 10.0.0.0 porque asume un cambio hacia R2. Y asi sucesivamente.

Figura 5: R4 comienza a enviar actualización de la red 10.0.0.0 por la Vlan 40. Se observa que van aumentando las métricas en los routers 3, 2 y 1.

Operación de un Router

Tabla Router 2

Red	Mascara	Gateway.	Metrica
20.0.0.0	255.0.0.0	20.0.0.7	1
30.0.0.0	255.0.0.0	30.0.0.6	1
10.0.0.0	**255.0.0.0**	**20.0.0.6**	**10**
40.0.0.0	**255.0.0.0**	**30.0.0.7**	**2**
50.0.0.0	**255.0.0.0**	**30.0.0.7**	**3**

Tabla Router 3

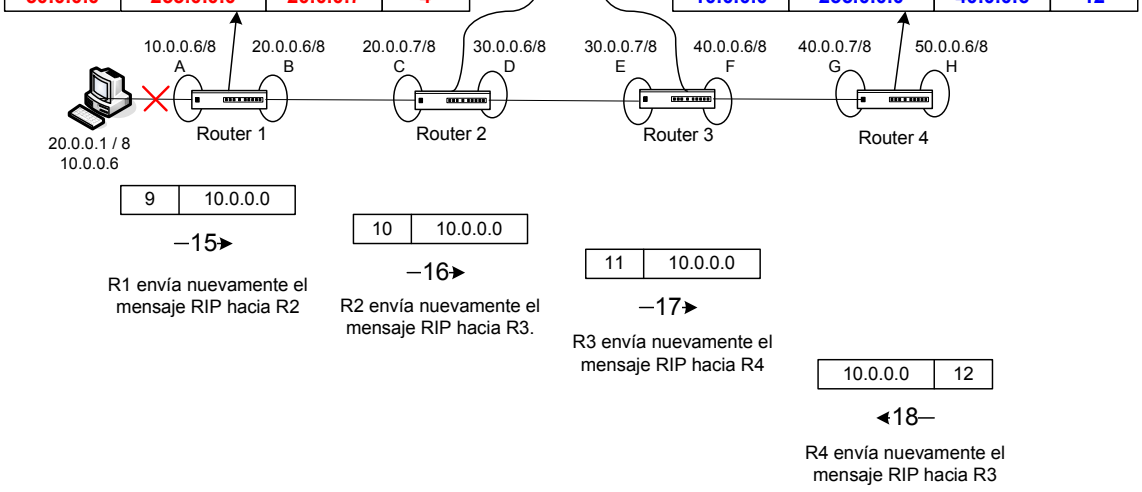
Red	Mascara	Gateway.	Metrica
30.0.0.0	255.0.0.0	30.0.0.7	1
40.0.0.0	255.0.0.0	40.0.0.6	1
10.0.0.0	**255.0.0.0**	**30.0.0.6**	**11**
20.0.0.0	**255.0.0.0**	**30.0.0.6**	**2**
50.0.0.0	**255.0.0.0**	**40.0.0.7**	**2**

Tabla Router 1

Red	Mascara	Gateway.	Metrica
10.0.0.0	**255.0.0.0**	**20.0.0.7**	**9**
20.0.0.0	255.0.0.0	20.0.0.6	1
30.0.0.0	**255.0.0.0**	**20.0.0.7**	**2**
40.0.0.0	**255.0.0.0**	**20.0.0.7**	**3**
50.0.0.0	**255.0.0.0**	**20.0.0.7**	**4**

Tabla Router 4

Red	Mascara	Gateway.	Metrica
50.0.0.0	255.0.0.0	50.0.0.6	1
40.0.0.0	255.0.0.0	40.0.0.7	1
30.0.0.0	**255.0.0.0**	**40.0.0.6**	**2**
20.0.0.0	**255.0.0.0**	**40.0.0.6**	**3**
10.0.0.0	**255.0.0.0**	**40.0.0.6**	**12**



9	10.0.0.0

–15➤

R1 envía nuevamente el mensaje RIP hacia R2

10	10.0.0.0

–16➤

R2 envía nuevamente el mensaje RIP hacia R3.

11	10.0.0.0

–17➤

R3 envía nuevamente el mensaje RIP hacia R4

10.0.0.0	12

◄18–

R4 envía nuevamente el mensaje RIP hacia R3

Figura 6: R1 comienza a enviar actualización de la red 10.0.0.0 por la Vlan 20. Se observa que van aumentando las métricas en los routers 2, 3 y 4.

Operación de un Router

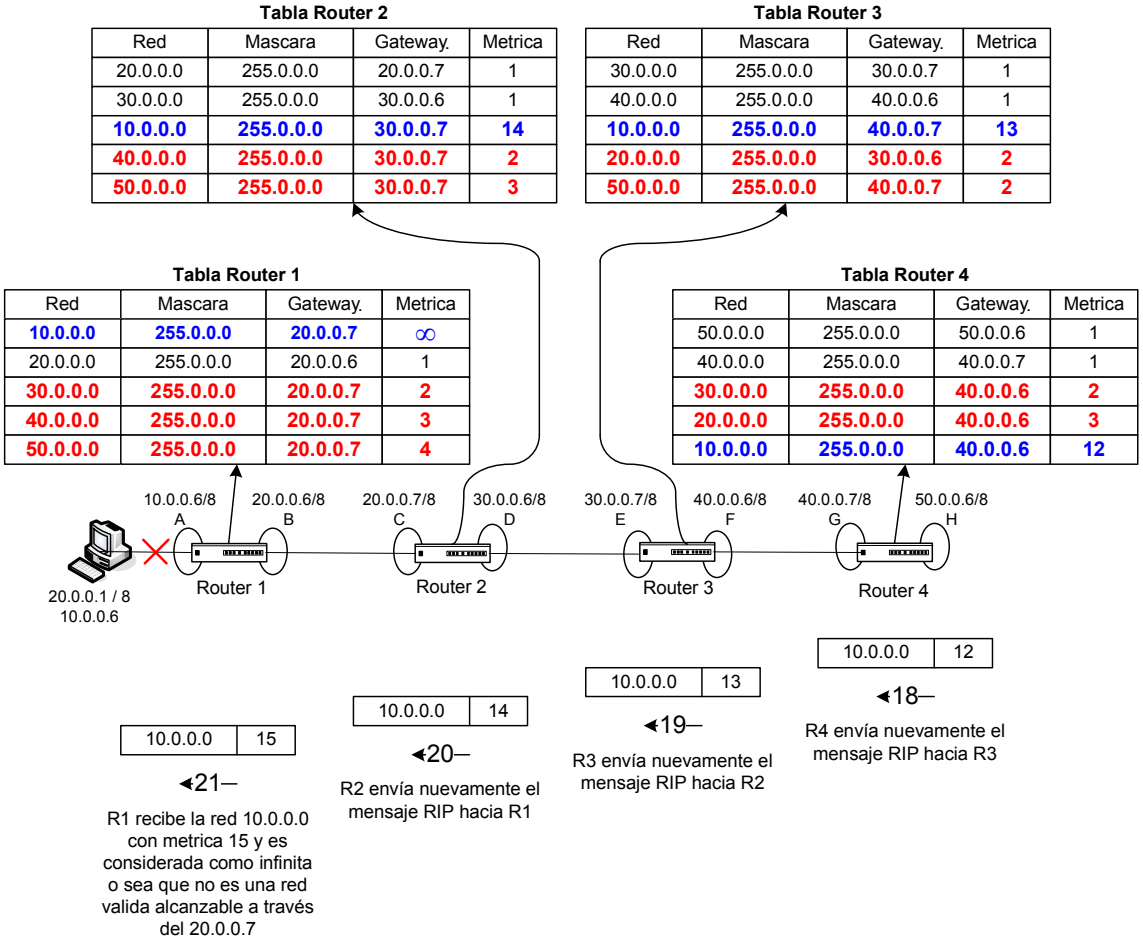


Figura 7: R4 comienza a enviar actualización de la red 10.0.0.0 por la Vlan 40. Se observa que van aumentando las métricas en los routers 3, 2 y 1.

Split Horizon evita este problema no publicando una red IP por la misma interfaz por donde fue recibida. Si emplea poisoned reverse la publica pero con una métrica infinita.

Para evitar los lazos en una red con enrutadores, se implementa el mecanismo de Split Horizon con Poisoned Reverse y con Temporizaciones de Retención. Se espera un segundo mensaje con igual métrica para una misma ruta o red antes de cargarla en la tabla de ruteo).

Ante un cambio de ruta, se disparan actualizaciones de inmediato. Los mensajes de actualizaciones de RIP se emiten cada 30 segundos. Se transmite todo la tabla de enrutamiento completa. Cuando un router recibe una misma red ya aprendida compara las métricas.

Si la métrica que posee ya cargada es menor que la que llega en el mensaje RIP, el router descarta la red que viene en el mensaje, caso contrario actualiza la entrada para esa red particular agregándole uno a la métrica que viene en el mensaje. Si recibe dos o mas mensajes con la misma métrica para una red particular, simplemente agrega la primera que recibe.

Operación de un Router

Los mensajes RIP emplean el puerto UDP 520 de la capa de transporte para el envío de sus mensajes de actualización.

RIPv2 maneja mecanismos de autenticación, ya que para que un router pueda participar del intercambio de información este debe poseer la clave de autenticación. De lo contrario no puede actualizar ni enviar mensajes de actualización. Además, en RIPv2 se envían en los mensajes la red, la métrica pero también la mascara de subred empleada lo que lo hace apto para el trabajo de esquemas de conexión que emplean subredes.

RIP en sus dos versiones se emplea para redes compuesta con enrutadores todos interconectados a la misma capacidad, es decir donde la capacidad de interconexión sea homogénea. Cuando la capacidad de transmisión sea diferente entre los routers es más útil emplear OSPF como protocolo de intercambio de rutas.

5.2.11.1.3 Formato del mensaje RIP

Como se menciono RIP se encapsula en un segmento UDP, que posteriormente se encapsula en un datagrama IP para terminar de encapsularse en una trama Ethernet.

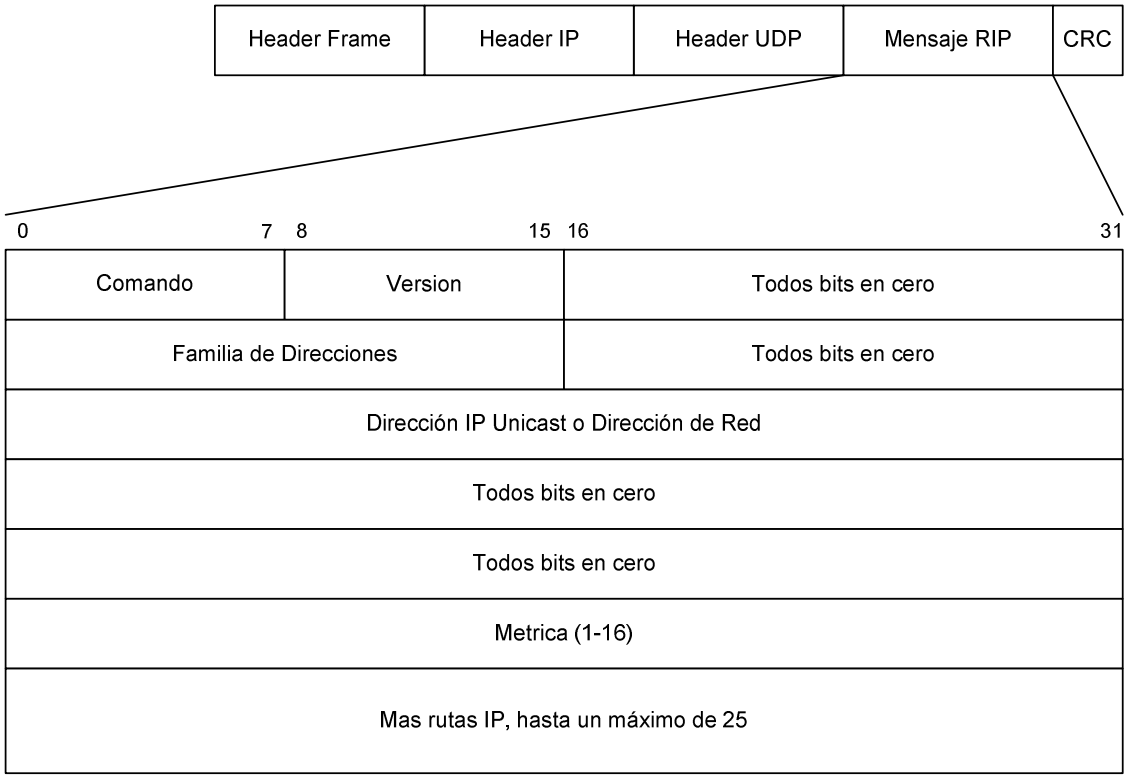


Figura 1. Formato del mensaje RIPv1.

Operación de un Router

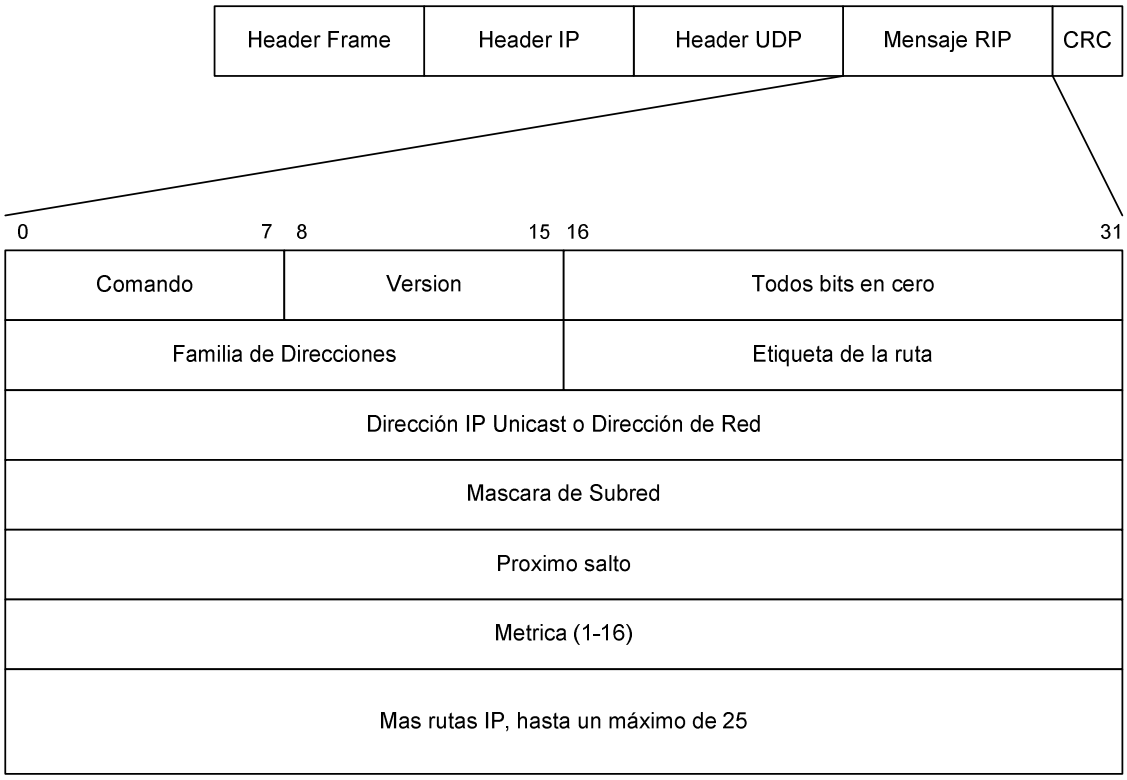


Figura 2. Formato del mensaje RIPv2.

5.2.11.2 OSPF

El protocolo **"Open Short Path First - OSPF"** es una clase de protocolo de enrutamiento dinámico que se encarga de analizar todas las redes de un esquema de ruteo y elegir aquella que presenta la mejor métrica basándose en el retardo de cada enlace.

Esta definido en el estándar de la RFC 2328. Se encapsula dentro de un datagrama IP directamente, **protocol = 89**.

Con este protocolo no necesita conocer la topología completa de la red. OSPF emplea un algoritmo que calcula la métrica de retardo de transmisión desde un router hacia cada red del esquema, tiendo en cuenta cada uno de los posibles caminos desde el router de origen que esta armando la tabla de ruteo hacia la red de destino.

Métrica = costo.

Costo = ∑ci de cada costo de cada enlace hacia los destinos. Se calculan los costos para cada camino y para cada red.

Ci = función del ancho de banda.

Ci = 10^8/ancho de banda(bps)

Se elige el costo menor.

Operación de un Router

Métrica Red 10.0.0.0:
R1= 0 (conectada directa)

Métrica Red 20.0.0.0
R1= 0 (conectada directa)

Métrica Red 40.0.0.0
R1= 0 (conectada directa)

Métrica Red 60.0.0.0
R1->R3->R2 = 0 + 10 + 1= 11 (ruta alternativa)
R1->R2 = 0 + 1 = 1 (mejor métrica)

Métrica Red 50.0.0.0
R1->R3 = 0 + 10 = 10 (ruta alternativa)
R1->R2 = 0 + 1 = 1 (mejor métrica)

Métrica Red 30.0.0.0:
R1->R3 = 0 + 10 = 10 (ruta alternativa)
R1->R2->R3 = 0 + 1 + 1 = 2 (mejor métrica)

Métrica Red 30.0.0.0:
R3= 0 (conectada directa)

Métrica Red 20.0.0.0
R3= 0 (conectada directa)

Métrica Red 50.0.0.0
R3= 0 (conectada directa)

Métrica Red 10.0.0.0
R3->R1 = 0 + 10 = 10 (ruta alternativa)
R3->R2->R1 = 0 + 1 + 1 = 2 (mejor métrica)

Métrica Red 60.0.0.0
R3->R1->R2 = 0 + 10 + 1= 11 (ruta alternativa)
R3->R2 = 0 + 1 = 1 (mejor métrica)

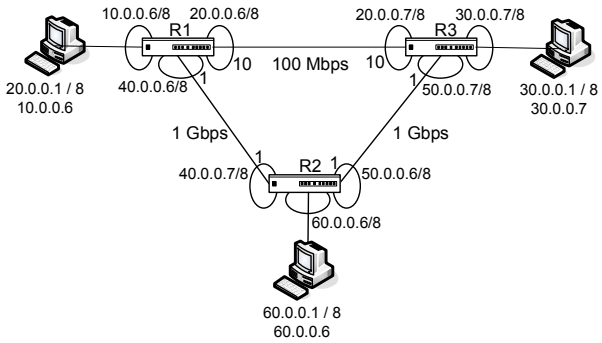
Métrica Red 40.0.0.0:
R3->R1 = 0 + 10 = 10 (ruta alternativa)
R3->R2 = 0 + 1 = 2 (mejor métrica)

Tabla Router 1

Red	Mascara	Gateway.	Metrica	Protocolo
10.0.0.0	255.0.0.0	10.0.0.6	0	DC
20.0.0.0	255.0.0.0	20.0.0.6	0	DC
40.0.0.0	255.0.0.0	40.0.0.6	1	DC
30.0.0.0	255.0.0.0	40.0.0.7	2	OSPF
60.0.0.0	255.0.0.0	40.0.0.7	2	OSPF
50.0.0.0	255.0.0.0	40.0.0.7	1	OSPF

Tabla Router 3

Red	Mascara	Gateway.	Metrica	Protocolo
30.0.0.0	255.0.0.0	30.0.0.7	0	DC
20.0.0.0	255.0.0.0	20.0.0.7	0	DC
50.0.0.0	255.0.0.0	50.0.0.7	0	DC
60.0.0.0	255.0.0.0	50.0.0.6	1	OSPF
10.0.0.0	255.0.0.0	20.0.0.6	2	OSPF
40.0.0.0	255.0.0.0	20.0.0.6	2	OSPF



Métrica Red 60.0.0.0:
R2= 0 (conectada directa)

Métrica Red 40.0.0.0
R2= 0 (conectada directa)

Métrica Red 50.0.0.0
R2= 0 (conectada directa)

Métrica Red 10.0.0.0
R2->R3->R1 = 0 + 1 + 10= 11 (ruta alternativa)
R2->R1 = 0 + 1 = 1 (mejor métrica)

Métrica Red 20.0.0.0
R2->R3 = 0 + 1 = 1 (mejor métrica)
R1->R2 = 0 + 1 = 1 (mejor métrica)

Métrica Red 30.0.0.0:
R2->R3 = 0 + 1 = 1 (mejor métrica)
R2->R1->R3 = 0 + 1 + 10 = 11 (ruta alternativa)

Tabla Router 2

Red	Mascara	Gateway.	Metrica	Protocolo
60.0.0.0	255.0.0.0	60.0.0.6	0	DC
40.0.0.0	255.0.0.0	40.0.0.7	0	DC
50.0.0.0	255.0.0.0	50.0.0.6	0	DC
10.0.0.0	255.0.0.0	40.0.0.6	1	OSPF
30.0.0.0	255.0.0.0	50.0.0.7	1	OSPF
20.0.0.0	255.0.0.0	50.0.0.7	1	OSPF

Figura 1. Armado de tablas de conmutación empleando OSPF.

Operación de un Router

Tabla 1. Métricas en función de la capacidad de los enlaces

Tipo de Red	108 / bps = Costo
Gigabi Ethernet	109 / 1.000.000.000 bps = 1
Fast Ethernet	108 / 100.000.000 bps = 1
Ethernet	108 / 10.000.000 bps = 10
E1	108 / 2.048.000 bps = 48
T1	108 / 1.544.000 bps = 64
128 kbps	108 / 128.000 bps = 781
64 kbps	108 / 64.000 bps = 1562
56 kbps	108 / 56.000 bps = 1785

OSPF emplea mensajes cortos, cada cambio en una red se impacta el cambio automáticamente mediante el triggered update, envio de mensajes multicast cada 30 minutos. Esto exige demasiado procesamiento y memoria para los equipamientos. La performance del protocolo es sensible a la dimensión de la red y un cambio de estado en una interfase arrastra el cálculo de SPF en todos los routers. Para acotar este problema existe una estructura de intercambio de información de ruteo OSPF jerárquica llamada AREA. La performance del protocolo es sensible a la dimensión de la red y un cambio de estado en una interfase arrastra el cálculo de SPF en todos los routers.

En la figura siguiente se observa un esquema de enrutamiento ya resuelto en base al retardo de transmisión. Normalmente los administradores de las redes ospf colocan el costo de cada interfaz en función de la capacidad de transmisión y eso lo que emplea ospf para el calculo de la mejor ruta.

Como puede apreciarse, la conexión entre el Router 1 y el Router 3 tiene una métrica de 10 ya que la capacidad del enlace es de 100 Mbps y la métrica para las conexiones entre el Router 1 y el Router 2 y entre el Router 1 y el Router 3 poseen una métrica de 1 porque la capacidad del enlace es de 1000 Mbps.

Como puede apreciarse en la figura 1, cada enrutador conoce todos los posibles caminos para poder calcular la mejor métrica. Esta información llega a cada router por medio de una inundación empleando direcciones de multicast especiales. Cada router coloca en un mensaje toda su tabla de enrutamiento y la coloca en un mensaje con esta dirección de multicast de destino. Todos los enrutadores que componen la red realizan la misma tarea.

Como puede entenderse, es grande la información que cada router debe procesar, motivo por el cual es necesario que esta inundación sea acotaba a un grupo de enrutadores que emplean OSFP. Este grupo es similar a la función de armar vlans, acotar el tráfico de broadcast a solo un grupo de PCs, las conectadas a una misma vlan.

Como puede verse en la figura a este grupo de routers concentrados en un mismo grupo se los conoce como Areas OSPF de intercambio. También se define un área de backbone que es la encargada de enviar la información entre un área y las otras.

OSPF soporta o puede implementarse en varios tipos de redes detalladas a continuación:

- **Punto a Punto**. Enlaces directos entre los routers.

Operación de un Router

- Direccionables como destino OSPF bajo la dirección multicast 224.0.0.5 (AllSPFRouters).

- **Broadcast**. Ethernet, Token-ring, etc.

- **Multiacceso sin broadcast(NBMA)**. Redes de paquetes WAN, X.25, Frame Relay, ATM. Los mensajes se envían por unicast.

- **Tránsito**. Tienen conectados dos o más routers.

- **Stub**. Redes que tienen sólo un router conectado. OSPF publica los hosts con máscara 255.255.255.255 como redes stub.

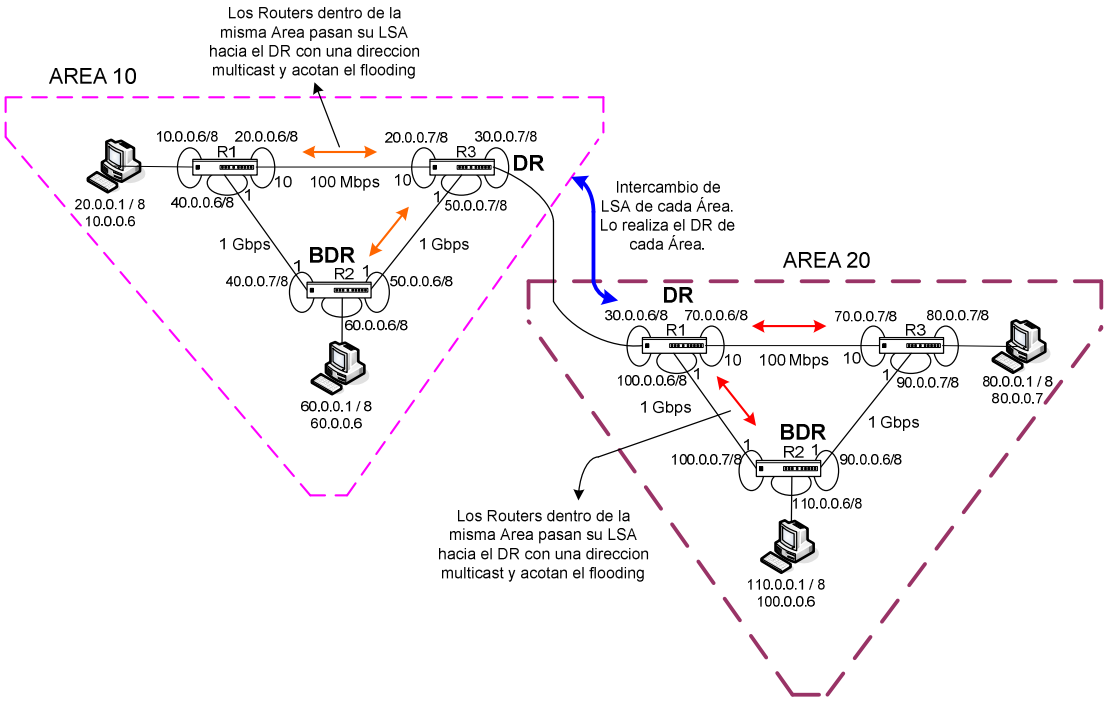
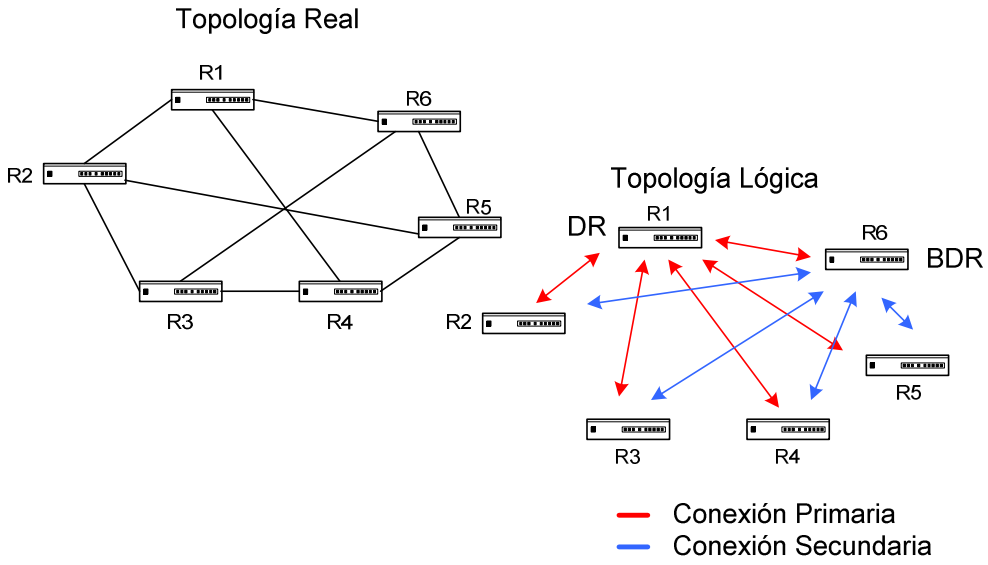


Figura 2: Área OSPF. Acotan el tráfico de inundación.

Operación de un Router



Si n es el número de routers tenemos n*(n-1)/2 adyacencias. Cada router enviará n-1 LSA, resultando n^2 LSAs enviados en total, lo que resulta en um Flooding caótico ya que múltiples copias del mismo LSA en la misma red. Para ello se crea un Designated Router (DR) dentro de cada Area.

Basta un solo router que propague el estado de los enlaces. Uno de ellos se elige como "designado". Representa a la red, al área y a sus routers al resto de las redes. Administra el flooding en la red. La red misma se considera un pseudo nodo o router virtual. La elección resulta del protocolo "hello". Una vez elegido los demás routers envían sus adyacencias al "designado". El "designado" genera una tabla con menor cantidad de entradas. Por criticidad del DR también se elige un Back-up.

- Si un router debe transmitir el estado de un enlace, sólo lo transmite al designado. Utiliza la dirección multicast 224.0.0.6 (AllDRouters).
- Si es un nuevo aviso el "**designado**" lo envía por "flooding" a la dirección multicast 224.0.0.5 (AllRouters) sobre su misma area.
- Dividir la red en sectores independientes interconectados por un "backbone".
- Los sectores son las "áreas". Se comportan como redes independientes.
- La base de datos incluye los enlaces del área.
- El "flooding" se detiene en los bordes del área. Ver figura 1 donde tenemos el área 10, el área 20 y los designados de cada área.
- OSPF, jerarquía:

- El costo resulta proporcional al tamaño del área y no al de la red global.
- Para mantener la integridad de la red existen routers que interconectan el área con el backbone. Son los routers de borde de área.
  - Mantienen varias bases de datos, una para cada área a la que pertenecen.

- Routers que comparten un segmento pueden resultar vecinos.
- Se eligen a través del protocolo hello.
- Se convierten en vecinos cuando se ven así mismos en el paquete hello.
- Condiciones:
  - Deben tener el misma área ID.
  - Misma autentificación.
  - Mismo hello interval y dead interval.
  - Deben coincidir en el flag del área stub.

- Intercambian mensajes "hello".
- Participan en el intercambio de la base de datos.
- Se define entre un router y su DR y BDR en un segmento multiacceso.

5.2.11.2.1 OSPF. Elección del DR

- Es el router con mayor prioridad OSPF.
  - El router con mayor dirección IP loopback.
  - El router con mayor dirección IP, en cualquiera de sus interfases.
- Los routers adyacentes tienen la misma base de datos de enlaces.
- La interfase pasa por varios estados antes de hacerse adyacente a otra de otro router.

- Sumarización inter-área
  - Realizada en los ABR (router borde area).
  - Rutas dentro del AS.

5.2.11.2.2 OSPF. Areas STUB

Las aras de Stub son un único punto de salida, el ruteo fuera del área no es óptimo, no puede ser tránsito para enlaces virtuales, no puede contener ASBR, la base de datos reducida, poseen menor requerimiento de memoria.

Los tipos de áreas mas utilizadas son:

- **Área stub**. Un área stub es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron inyectadas en OSPF desde otro protocolo de enrutamiento. Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento.

- **Área not-so-stubby** (NSSA), constituyen un tipo de área stub que puede importar rutas externas de sistemas autónomos y enviarlas al backbone, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas.

5.2.11.2.3 OSPF. Paquetes de Anuncio de estado del enlace (LSA)

- ***Routers Links***
  - Describen el estado y costo de los links.
  - Generados por todos los routers.
- ***Network Links***
  - Originados por los DR.
  - Definidos para segmentos multiacceso donde hay varios routers.
  - Describen todos los routers en el segmento.

5.2.11.2.4 Formato del mensaje OSPF.

Figura 1. Formato del mensaje OSPFv1

5.2.12 Ruteo: núcleos, pares y algoritmos

5.2.12.1 Introducción

A continuación analizaremos la estructura de las redes IP construidas alrededor de una columna vertebral, considerando las consecuencias de esta topología para el encaminamiento de datagramas. Si bien los ejemplos dados en esta sección provienen de la red global Internet, las ideas se aplican de igual forma a las pequeñas redes IP corporativas.

5.2.12.2 Ruteo con información parcial

La principal diferencia entre los enrutadores y los anfitriones comunes es que estos últimos por lo general saben poco acerca de la estructura de la red IP a la que están conectados. Los anfitriones no tienen un conocimiento completo de todas las direcciones de destino o todas las redes de destino posibles.

De hecho, muchos anfitriones tienen solo dos rutas en su tabla de ruteo: una para la red local y otra por omisión hacia un enrutador cercano. Un anfitrión envía todos los datagramas no locales hacia el enrutador local

Operación de un Router

para su entrega, a través de la configuración de la puerta de enlace o gateway (esto puede observarse en la figura 3).

Un enrutador puede encaminar datagramas con información parcial, únicamente bajo ciertas circunstancias. Imagínese a una red como a un país atravesado por carreteras polvorientas que cuentan con señales de direccionamiento en las intersecciones. Imagine, por otra parte, que usted no tiene mapas, no puede preguntar nada porque no puede hablar el idioma local, tampoco tiene idea de posibles puntos de referencia visibles, pero usted necesita viajar hacia una ciudad llamada Leones. Comienza su jornada siguiendo la única carretera que sale de su población de origen (Rafaela) y poco a poco va viendo las señales de direccionamiento. En la primera señal encuentra el siguiente letrero:

"Rosario hacia la izquierda; Noetinger hacia la derecha; para cualquier otra ciudad siga en línea recta"

Como el destino que usted busca no está nombrado explícitamente, tendrá que continuar en línea recta. En la jerga del ruteo se dice que está siguiendo una ruta por omisión. Luego de varios señalamientos más, finalmente usted encuentra uno en el que puede leer:

"Cañada de Gómez hacia la izquierda; Leones hacia la derecha; para cualquier otra ciudad siga en línea recta"

Usted da vuelta a la derecha siguiendo varios señalamientos más y llega hasta una carretera que desemboca en Leones.

Nuestro viaje imaginario es análogo a la travesía de un datagrama en la red IP y los señalamientos en la carretera son semejantes a las tablas de ruteo en los enrutadores a lo largo del camino. Sin un mapa u otra ayuda de dirección, completar el viaje dependerá completamente de los señalamientos de la carretera, así como el ruteo de un datagrama en una red IP depende de las tablas de ruteo. Está claro que es posible completar el recorrido aun cuando cada señalamiento en la carretera contenga información parcial.

Para que en nuestro ejemplo el viajero pueda llegar a su destino siguiendo los señalamientos, esto va a depender de la topología del sistema de carreteras y del contenido de los señalamientos, pero la idea fundamental es que, tomada en conjunto, la información de los señalamientos debe ser consistente y completa.

Operación de un Router

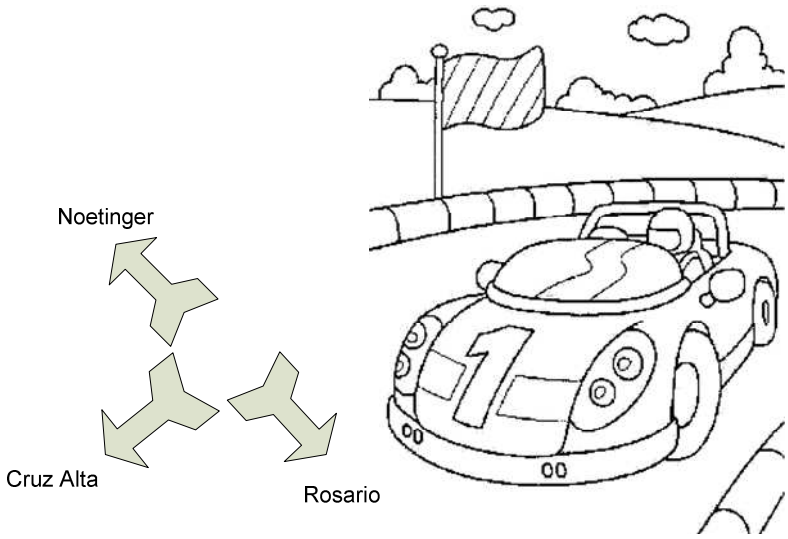


Figura 6: rutas por omisión en las carreteras.

A continuación vemos un ejemplo para entender algunas de las formas en las que se puede lograr la consistencia. Consideremos una topología de red en la que la mitad de una ciudad se encuentra en la parte oriental y la otra mitad en la parte occidental. Supongamos que un solo puente cruza el río que separa al este del oeste.

Imaginemos que las personas que viven en la parte este no simpatizan con las personas de la parte oeste, de tal manera que están deseosas de permitir que los señalamientos de las carreteras indiquen los destinos del este y no los del oeste. Supongamos que la gente que vive en el oeste hace lo mismo de su lado. El ruteo será consistente si todos los señalamientos de las carreteras en el este señalan hacia los destinos del lado este explícitamente y apuntan hacia el puente como una ruta por omisión; en tanto que todos los señalamientos de la carretera en el oeste señalarán hacia los destinos del oeste de manera explícita y apuntaran hacia el puente como una ruta por omisión.

5.2.12.3 Arquitectura y núcleos de Internet originales

Cuando el TCP/IP fue desarrollado por primera vez, las localidades de investigación participantes estaban conectadas a ARPANET, la cual servía como columna vertebral (Backbone) de la red Internet. Durante los experimentos iniciales, cada localidad administraba tablas de ruteo e instalaba rutas hacia otros destinos a mano. Como Internet comenzaba a crecer, se hizo evidente que el mantenimiento manual de rutas no era práctico, por lo tanto fueron necesarios mecanismos automatizados.

Los diseñadores de Internet seleccionaron una arquitectura de ruteo que consistía de pequeños conjuntos centrales de ruteadores que contaban con información completa sobre todos los destinos posibles y un gran conjunto de ruteadores externos que contaban con información parcial. En términos de nuestra analogía es como si se designara a un pequeño conjunto de intersecciones localizadas en el centro para tener señalamientos que listaran todos los destinos y se permitiera a las intersecciones exteriores listar únicamente a los destinos locales. Siguiendo la ruta por omisión, en

cada punto de intersección exterior hacia una de las intersecciones centrales, los viajeros finalmente encontrarían su destino.

La ventaja de usar información parcial en los enrutadores exteriores es que permite a los administradores locales manejar cambios estructurales locales sin afectar a otras partes de Internet. La desventaja es que esto introduce la posibilidad de inconsistencias. En el peor de los casos, un error en un enrutador externo puede hacer que los enrutadores distantes sean inaccesibles. Podemos resumir estas ideas de la siguiente forma:

La tabla de ruteo en un enrutador dado contiene información parcial relacionada con destinos posibles. El ruteo que emplea información parcial permite que las localidades tengan autonomía para hacer cambios locales de ruteo, pero introduce la posibilidad de que se den inconsistencias, con las que algunos destinos podrían volverse inaccesibles para algunas fuentes.

Las inconsistencias entre las tablas de ruteo por lo general son errores en los algoritmos que calculan las tablas de ruteo, información incorrecta proporcionada a estos algoritmos o errores originados cuando se transmiten los resultados hacia otros enrutadores.

5.2.12.4 Enrutadores de núcleo

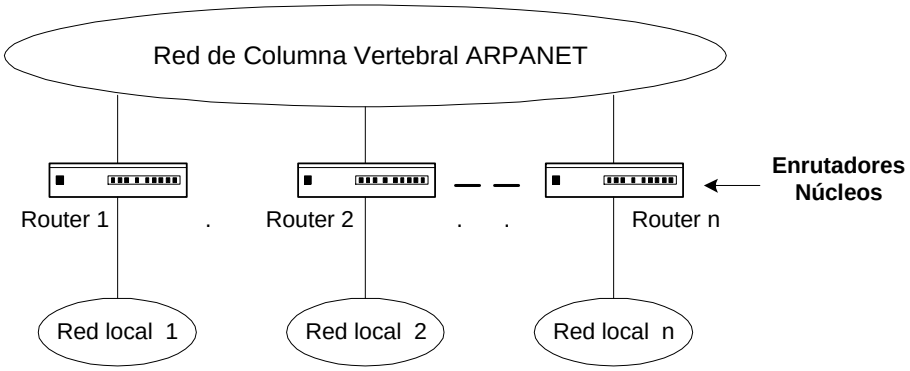


Figura 7: Sistema de ruteo de núcleo visto como un conjunto de ruteadores que conectan redes de área local con ARPANET. Los anfitriones en la red local pasan todo el tráfico no local hacia la ruta de núcleo cercana.

En términos generales, los primeros enrutadores de Internet podrían dividirse en dos grupos: un pequeño conjunto de enrutadores de núcleo, controlados por el Internet Network Operations Center (INOC) y un conjunto extenso de enrutadores no-núcleo, controlados por grupos individuales. El sistema de núcleo estaba diseñado para proporcionar rutas autorizadas consistentes y confiables para todos los destinos posibles; era el pegamento que sostenía unido a Internet y hacia posible la interconexión universal. Por desgracia, cada localidad asignada a una dirección de Internet debía arreglarse para anunciar su dirección hacia el sistema de núcleo. Las rutas de núcleo estaban comunicadas entre ellas, de esta forma podían garantizar que la información que compartían fuera consistente. Dado que una autoridad central monitoreaba y controlaba a los enrutadores de núcleo, éstos eran altamente confiables.

Cuando comenzaron los experimentos de Internet, los diseñadores la construyeron a través de ARPANET como una red de columna vertebral principal. Por ello, gran parte de la motivación del sistema de ruteo de

Operación de un Router

núcleo proviene del deseo de conectar redes locales con ARPANET. La figura siguiente ilustra la idea:

Para entender por que esta arquitectura no permite realizar un ruteo con información parcial, supongamos que una extensa red IP esta compuesta por redes de área local, cada una de ellas conectada a una columna vertebral de la red a través de un enrutador. También imaginemos que algunos de estos enrutadores dependen de rutas asignadas por omisión. Luego consideremos la trayectoria de flujo de un datagrama(línea roja). En la localidad fuente, el ruteador local verifica si hay una ruta explícita hacia el destino, y si no es así, envía el datagrama hacia la trayectoria especificada en su ruta por omisión. Todos los datagramas, para los que el enrutador no tiene una ruta siguen la misma ruta por omisión hacia su destino final. El siguiente enrutador, a lo largo de la trayectoria, desvía datagramas para los que tiene una ruta explícita y envía el resto hacia la ruta por omisión. Para lograr una consistencia global completa, la cadena de rutas por omisión debe alcanzar cualquier ruta en un sitio gigantesco como el que se observa en la figura 10.11.4.2. Es por ello que la arquitectura requiere que todas las localidades coordinen sus rutas por omisión.

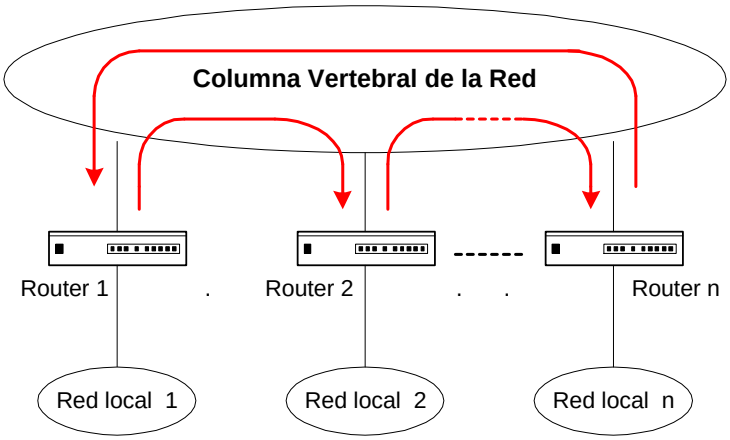


Figura 10.11.4.2: Enrutadores conectados a una columna vertebral de la red que muestra rutas por omisión. El ruteo es ineficiente aun cuando sea consistente

Además, dependiendo de las rutas por omisión estas pueden ser ineficientes aun cuando sean consistentes. Como se muestra en la figura 10.11.4.2, un datagrama, en el peor de los casos, pasará a través de n enrutadores conforme viaje de la fuente al destino en lugar de ir directamente a través de la columna vertebral de la red hacia su destino.

Para evitar la ineficiencia que originan las rutas asignadas por omisión, los diseñadores de Internet arreglaron a todos los enrutadores de núcleo para que sean capaces de intercambiar información de ruteo, de manera que cada uno tenga información completa acerca de las rutas óptimas hacia todos los destinos posibles. Debido a que cada enrutador de núcleo conoce las rutas hacia todos los destinos posibles, no es necesaria una ruta por omisión. Si la dirección de destino en un datagrama no aparece en la tabla de ruteo de un enrutador de núcleo, éste generará un mensaje de destino inalcanzable (ICMP) y eliminará el datagrama. En esencia, el diseño de núcleo evita la ineficiencia al eliminar las rutas por omisión.

Operación de un Router

La figura 10.11.4.3 describe las bases conceptuales de una arquitectura de ruteo de núcleo. La figura muestra un sistema de núcleo central consistente de uno o mas ruteadores de núcleo y un conjunto de enrutadores exteriores (Li) en sitios locales. Los enrutadores exteriores toman información relacionada con los destinos locales y utilizan la ruta por omisión por la que envían datagramas destinados por otras localidades hacia el núcleo.

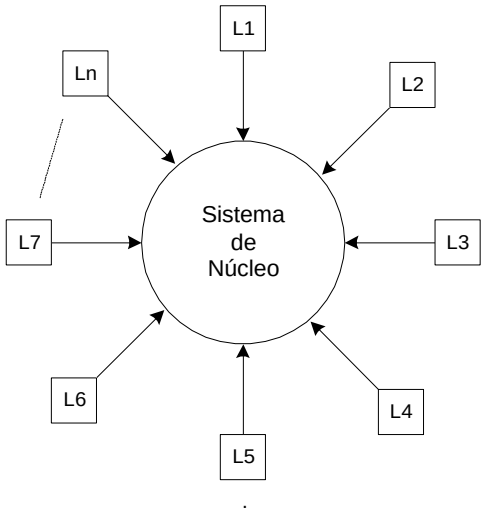


Figura 10.11.4.3: Arquitectura de ruteo en un sistema de ruteo simple que muestra las rutas por omisión. Los enrutadores núcleo no utilizan rutas por omisión, los enrutadores externos, señalados como Li tienen cada uno una ruta por omisión que apunta hacia el núcleo

Existen tres razones por las que la arquitectura de núcleo mostrada en la figura anterior resulta impráctica:

1. Internet crecería como una sola red de columna vertebral de gran alcance administrada centralmente. La topología se haría compleja y los protocolos necesarios para mantener la consistencia entre enrutadores de núcleo también se harían más complejos.

2. No todas las localidades pueden tener un enrutador de núcleo conectado a la columna vertebral, de manera que resultaría necesaria una estructura adicional de ruteo y de protocolos.

3. Como todos los enrutadores de núcleo interactúan para asegurar la consistencia de la información de ruteo, la arquitectura de núcleo no podría extenderse a gran escala.

5.2.13 Sistemas Autónomos

5.2.13.1 Agregar complejidad al modelo arquitectónico

El sistema original de ruteo de núcleo se desarrolló cuando Internet contaba con una sola columna vertebral (backbone). En consecuencia, parte de la motivación de una arquitectura de núcleo fue proporcionar conexiones entre redes de área local y la columna vertebral (ver figura 10.11.4.1).

Operación de un Router

Para una red IP con una sola columna vertebral, mas un conjunto de redes de área local conectadas, no es necesaria una estructura adicional.

Cada enrutador conoce la única red local a la que esta conectado y aprende acerca de todas las otras redes comunicándose a través de la columna vertebral con otros enrutadores. Por desgracia, tener a todos los enrutadores participando de manera directa en un protocolo de actualización de ruteo no es suficiente. En primer lugar, aun cuando cada localidad conectada a la red IP tenga solo una red local, una arquitectura de núcleo es inadecuada ya que ésta no puede crecer para adaptarse a un número arbitrario de localidades. En segundo lugar, la mayor parte de las localidades tiene múltiples redes de área local y enrutadores interconectados. Como un enrutador núcleo se conecta a una sola red en cada localidad, el núcleo sólo tiene conocimientos acerca de una red en la localidad.

En tercer lugar, una red IP extensa interconecta conjuntos de redes administradas por grupos independientes. Una arquitectura de ruteo debe proporcionar la vía para que cada grupo controle de manera independiente el ruteo y el acceso a la red de backbone. Luego de examinar las consecuencias de cada una de estas ideas, aprenderemos como un solo mecanismo de protocolo permite la construcción de una red IP que abarca a varias localidades y permite que estas conserven su autonomía.

5.2.13.2 Una idea fundamental: saltos adicionales

Hasta aquí hemos analizado la arquitectura de una red IP con una columna vertebral conectada por un sistema de ruteo de núcleo. Hemos considerado un sistema de núcleo como un mecanismo de ruteo central al que los enrutadores no-núcleo envían datagramas para su entrega. También hemos dicho que es imposible expandir de manera arbitraria una sola columna vertebral.

Tener menos enrutadores núcleo que redes en una red IP significa que tendremos que modificar nuestra visión de la arquitectura de núcleo o el ruteo será deficiente. Para entender por que, consideremos el ejemplo de la figura 10.12.2.1.

Figura 10.12.2.1: problema del salto extra

En la figura, los enrutadores núcleo R1 y R2 conectan las redes de área local 1 y 2 respectivamente. Dado que intercambian información de ruteo, ambos enrutadores saben como alcanzar ambas redes. Supongamos que el enrutador R3, no-núcleo, considera al núcleo como un sistema de entrega de datagramas y selecciona a uno de los enrutadores núcleo (R1), para entregar todos los datagramas destinados a las redes con las que no tiene contacto. R3 envía datagramas para la red 2 a través de la columna vertebral de la red, para esto selecciona al enrutador núcleo R1 el cual debe enviarlos de regreso a través de la columna vertebral hacia el enrutador 2. La ruta optima por supuesto requeriría que R3 enviara datagramas destinados a la red 2 directamente hacia R2.

Operación de un Router

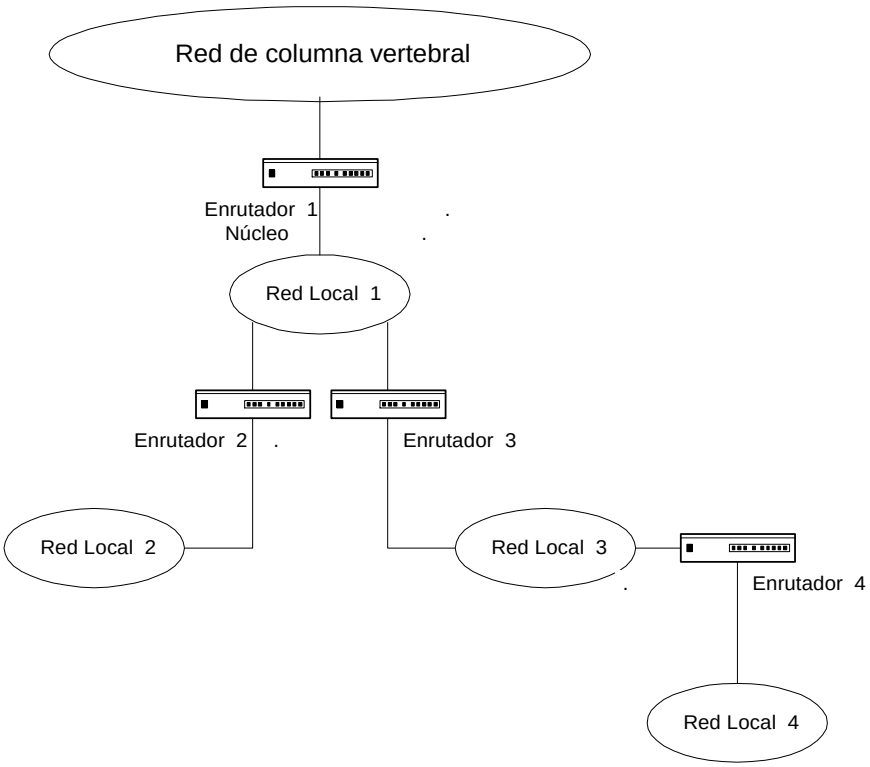


Figura 10.12.2.2: ejemplo de múltiples redes y enrutadores con una sola conexión de columna vertebral de red.

Para resolver este "salto extra" será necesario modificar nuestra visión de la arquitectura de núcleo.

Tratar un sistema de núcleo como un ruteador central introduce un salto extra en la mayor parte del tráfico. Se necesita un mecanismo que permita, a los enrutadores que no pertenecen al núcleo, aprender rutas desde los enrutadores núcleo de manera que puedan seleccionar rutas optimas en la columna vertebral de la red.

Permitir que las localidades tengan múltiples redes y enrutadores significa que el núcleo no está conectado a todas las redes de manera directa, de tal forma que es necesario un mecanismo adicional para permitir que el sistema de núcleo aprenda esto. Consideremos, por ejemplo, el conjunto de redes y enrutadores mostrados en la figura 10.12.2.2. Podemos imaginar una conexión como esta dentro de una compañía o en un campus universitario, donde cada red corresponde a un solo edificio o a un solo departamento.

Supongamos que la localidad tiene instalada sólo la red local 4 y que ha obtenido una dirección de red IP para ésta. También suponemos que los enrutadores R2, R3 y R4 tienen rutas para las cuatro redes locales, así como rutas por omisión que pasan el tráfico externo hacia el enrutador núcleo R1.

Los anfitriones directamente conectados a la red local 4 pueden comunicarse con otras redes y cualquier máquina puede encaminar paquetes hacia el exterior para otras localidades de la columna vertebral. Sin

embargo, debido a que el enrutador R1 esta conectado solamente a la red local 1, no puede tener conocimiento acerca de la red local 4. Decimos que, desde el punto de vista del sistema de núcleo, la red local 4 esta oculta detrás de la red local 1. El punto importante es que:

Como las localidades individuales pueden tener una estructura de complejidad arbitraria, un sistema de núcleo no se conecta directamente hacia todas las redes. Es necesario un mecanismo que permita a los enrutadores no-núcleo, informar al núcleo sobre las redes ocultas.

Recordemos que además de proveerle al núcleo con información sobre redes ocultas, necesitamos un mecanismo que permita a los enrutadores no-núcleo obtener información de ruteo desde el núcleo. En nuestro ejemplo, el enrutador R4 es él más cercano asociado a la red local 4, pero éste se encuentra a dos saltos del enrutador núcleo más cercano. Así, R4 debe depender del enrutador R3 para rutear paquetes hacia la red 4. El punto es que R4 no puede garantizar la accesibilidad de la red local 4 por sí mismo. El enrutador R3 se encuentra a un salto del núcleo y puede garantizar el paso de paquetes, pero no está directamente conectado hacia la red local 4. Así, parece incorrecto otorgar a R3 la responsabilidad de la red 4. Para resolver este dilema debemos introducir un nuevo concepto.

5.2.13.3 Concepto de sistemas autónomos

Las redes (1, 2, 3 y 4) mostradas en la figura 10.12.2.2, las cuales aparecen cuando una localidad en la columna vertebral de la red tiene una compleja estructura local, no deben ser pensadas cada una como múltiples redes independientes, conectadas hacia una red IP, sino como una organización única que tiene múltiples redes bajo su control. Dado que las redes y los enrutadores se encuentran bajo una sola autoridad administrativa, esta autoridad puede garantizar que las rutas internas se mantengan consistentes y viables; mas aun la autoridad administrativa puede seleccionar a una de sus máquinas para servir como la máquina que aparecerá ante el mundo exterior como el acceso hacia la red. En el ejemplo de la figura 10.12.2.2 dado que los enrutadores R2, R3 y R4 están bajo el control de una autoridad administrativa se puede arreglar que R3 anuncie la accesibilidad para las redes 2, 3 y 4 (asumimos que el sistema de núcleo ya tiene conocimiento sobre la red 1 ya que un enrutador núcleo está conectado directamente a ésta)

Para propósitos de ruteo a un grupo de redes y enrutadores controlados por una sola autoridad administrativa se le conoce con el nombre de “Sistema Autónomo”. Los enrutadores dentro de un sistema autónomo son libres de seleccionar sus propios mecanismos de exploración, propagación, validación y verificación de la consistencia de las rutas. Nótese que bajo esta definición el enrutador núcleo en si forma un sistema autónomo.

Conceptualmente la idea de un sistema autónomo es consecuencia directa y natural de la generalización de la arquitectura descrita en la figura 10.12.2.2, con sistemas autónomos reemplazando redes de área local y enrutadores. La figura 10.12.3.1 ilustra esta idea.

Para lograr que las redes ocultas dentro de un sistema autónomo sean accesibles a través de Internet, cada sistema autónomo debe acordar la difusión de la información de la accesibilidad de la red hacia los otros sistemas autónomos. Aun cuando los anuncios puedan ser enviados hacia cualquier sistema autónomo, en una arquitectura de núcleo es crucial que cada sistema autónomo difunda información hacia un enrutador núcleo. Usualmente un enrutador en un sistema autónomo tiene la responsabilidad de

Operación de un Router

anunciar rutas e interactuar de manera directa con uno de los enrutadores núcleo. Es posible, sin embargo, tener varios enrutadores y que cada uno anuncie un subconjunto de redes.

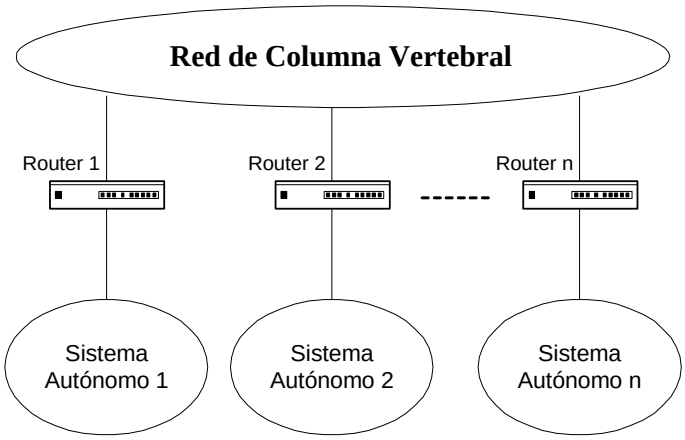


Figura 10.12.3.1: Arquitectura de una red IP con sistemas autónomos en localidades de la columna vertebral de red. Cada Sistema Autónomo esta formado por varias redes y enrutadores bajo una sola autoridad administrativa.

Podría parecer que nuestra definición de sistema autónomo es vaga, pero en la práctica las fronteras entre sistemas autónomos deben ser precisas para permitir que los algoritmos automatizados tomen decisiones de ruteo.

Por ejemplo, un sistema autónomo, propiedad de una compañía, puede seleccionar no rutear paquetes a través de otro sistema autónomo propiedad de otra compañía, aun cuando estén directamente conectados. Para hacer posible que los algoritmos automatizados de ruteo distingan entre sistemas autónomos, a cada uno le asigna un número de sistema autónomo la misma autoridad central que esta a cargo de asignar todas las direcciones de red en Internet. Cuando dos enrutadores intercambian información de accesibilidad de red, el mensaje transporta el identificador de sistema autónomo que el enrutador representa. En síntesis:

Una red extensa basada en los protocolos TCP/IP tiene una estructura adicional para adaptare a las fronteras administrativas: cada colección de redes y enrutadores controlados por una autoridad administrativa se considera como un solo sistema autónomo. Un sistema autónomo tiene la libertad para seleccionar una arquitectura de ruteo interna, pero debe reunir información sobre todas sus redes y designar uno o más enrutadores que habrán de transferir información de accesibilidad hacia otros sistemas autónomos. Debido a que la conexión de Internet se vale de una arquitectura de núcleo, todos los sistemas autónomos deben transferir información de accesibilidad hacia los enrutadores núcleo de Internet.

5.2.13.4 Ruteo entre sistemas autónomos. Protocolos de pasarela exterior (EGP)

A dos enrutadores que intercambian información de ruteo se les conoce como vecinos exteriores, sí pertenecen a dos sistemas autónomos diferentes o vecinos interiores si pertenecen al mismo sistema autónomo. El protocolo que emplea vecinos exteriores para difundir la información de accesibilidad

Operación de un Router

a otros sistemas autónomos se le conoce como Protocolo de Pasarela Exterior (EGP) y los enrutadores que se utilizan se conocen como enrutadores exteriores.

En la conexión de Internet, el EGP es especialmente importante ya que los sistemas autónomos lo emplean para difundir información de accesibilidad hacia el sistema de núcleo.

La figura 10.12.4.1 muestra dos vecinos exteriores que utilizan el EGP. El enrutador R1 recoge información acerca de las redes en el sistema autónomo 1 y reporta esta información al enrutador R2 mediante EGP, mientras que el enrutador R2 reporta información desde el sistema autónomo 2.

El EGP tiene tres características principales:

1. Soporta un mecanismo de adquisición de vecino que permite a un enrutador solicitar a otro un acuerdo para que los dos comuniquen información de accesibilidad. Decimos que un enrutador consigue un par EGP a un vecino EGP. Los pares EGP son vecinos porque éstos intercambian información de ruteo y no por su proximidad geográfica.

2. Un enrutador prueba continuamente si su vecino EGP esta respondiendo Los vecinos EGP intercambian información de accesibilidad de red de manera periódica, transfiriendo un mensaje de actualización de ruteo.

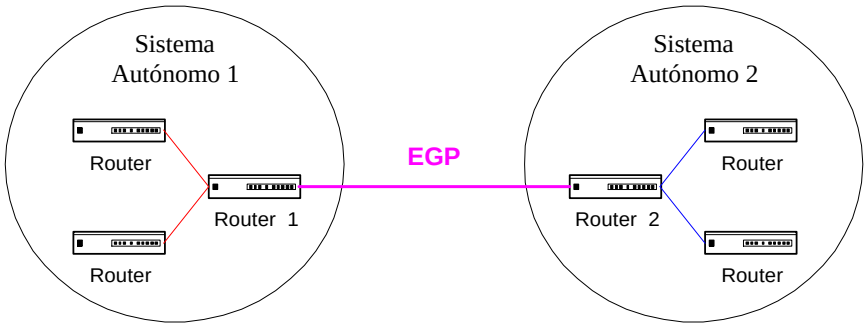


Figura 10.12.4.1: Esquema con dos enrutadores exteriores (R1 y R2) que utilizan el EGP para anunciar redes en sus sistemas autónomos luego de reunir la información.

5.2.13.5 Ruteo dentro de un sistema autónomo. Protocolos de pasarela interior (IGP)

A dos enrutadores dentro de un sistema autónomo se les llama interiores con respecto a otro. Por ejemplo, dos enrutadores núcleo Internet son interiores en comparación con otros debido a que el núcleo forma un solo sistema autónomo. Dos enrutadores en un campus universitario son considerados interiores con respecto a otros mientras que las máquinas en el campus están reunidas dentro de un solo sistema autónomo.

Operación de un Router

Los enrutadores dentro de un sistema autónomo aprenden acerca de las redes dentro del mismo: en forma estática o en forma dinámica. En redes pequeñas cuya topología cambia lentamente, los administradores pueden establecer y modificar rutas a mano. El administrador tiene una tabla de redes y actualiza la tabla si una red nueva se añade o se elimina del sistema autónomo. Por ejemplo, consideremos la redes IP de la pequeña corporación mostrada en la siguiente figura 10.12.5.1.

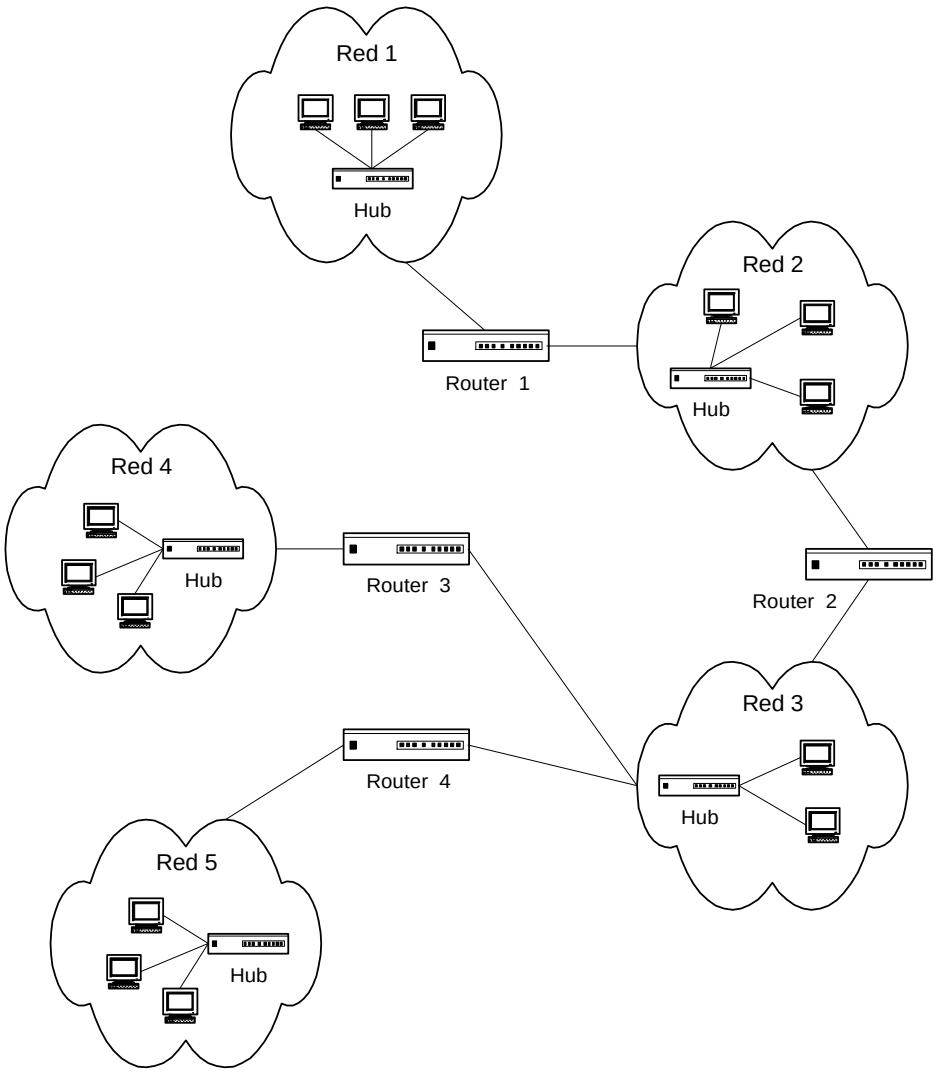


Figura 10.12.5.1: Red formada por cinco redes Ethernet y 4 Enrutadores en una sola localidad

El ruteo para cada red IP es insignificante porque sólo existe una ruta entre cualquiera de los dos puntos. El administrador puede configurar manualmente las rutas en todos los anfitriones o enrutadores. Si la red IP cambia (por ejemplo, si se añade una nueva red), el administrador debe reconfigurar las rutas en todas las máquinas (anfitriones o enrutadores).

Operación de un Router

La desventaja de un sistema manual es obvia, los sistemas manuales no se pueden adaptar al crecimiento o a los cambios rápidos. En un ambiente de cambios rápidos como el de Internet, las personas simplemente no puede responder a los cambios lo suficientemente rápido como para resolver los problemas. Por lo tanto son necesarios métodos automatizados para el armado de las tablas de ruteo. Estos métodos pueden también ayudar a mejorar la confiabilidad y la respuesta a las fallas en pequeñas redes IP que tienen rutas alternativas.

A continuación consideremos lo que sucede si añadimos una ruta adicional a la red de la figura 10.12.5.1 obteniendo la red de la figura 10.12.5.2.

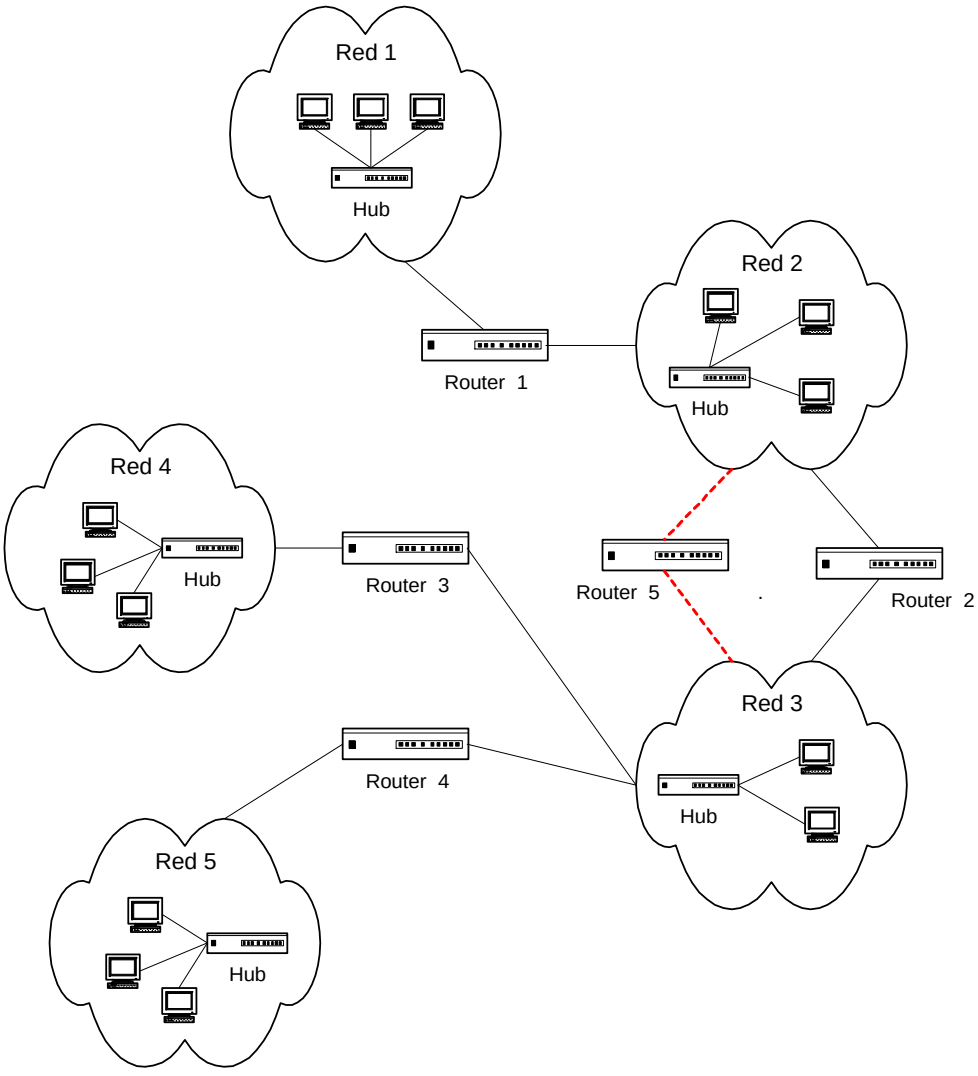


Figura 10.12.5.2: La adición del enrutador R5 introduce una nueva ruta alternativa entre las redes 2 y 3

Operación de un Router

En arquitecturas de red que tienen varias rutas físicas, los administradores por lo regular seleccionan una de ellas como ruta primaria. Sí el enrutador instalado a lo largo de la trayectoria falla, las rutas se deben cambiar para enviar el tráfico hacia una ruta alternativa. Cambiar las rutas manualmente toma tiempo y es una labor propensa a errores. Es por ello que aun dentro de pequeñas redes es aconsejable emplear un sistema automatizado para cambiar las rutas rápidamente y de manera confiable.

Para automatizar de manera segura el intercambio de información sobre la accesibilidad de una red dada, los enrutadores interiores normalmente se comunican con otros, intercambian información de accesibilidad de red o información de ruteo de red, a partir de la cual la accesibilidad se puede deducir. Una vez que la información de accesibilidad para un sistema autónomo se ha ensamblado en forma definitiva, uno de los enrutadores en el sistema puede anunciarlo a otros sistemas autónomos utilizando el EGP.

No se ha desarrollado un solo protocolo que se utilice dentro de los sistemas autónomos, a diferencia del protocolo EGP que proporciona un estándar ampliamente aceptado. Una de las razones de esta diversidad de IGP proviene de la variedad de topologías y tecnologías que se utilizan en los sistemas autónomos. Otra de las razones se deriva del compromiso entre la simplicidad y la funcionalidad, los protocolos que son fáciles de instalar y configurar no proporcionan una funcionalidad sofisticada. Como resultado, sólo un puñado de protocolos se han vuelto populares; la mayoría de los sistemas autónomos utiliza uno de ellos exclusivamente para difundir información de ruteo internamente.

Dado que no se trata de un solo estándar, utilizaremos el término protocolo de pasarela interior (IGP), como una descripción genérica para referirnos a cualquier algoritmo que utilicen los enrutadores interiores cuando intercambian información sobre accesibilidad de red y de ruteo.

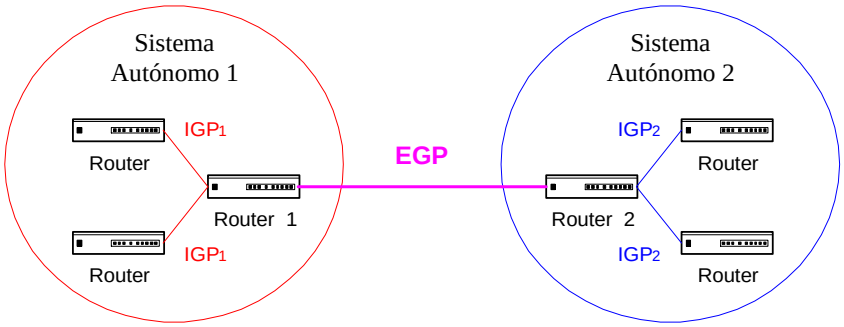


Figura 10.12.5.3: Concepto de dos sistemas autónomos, cada uno utiliza su propio IGP internamente, pero se vale del EGP para realizar la comunicación entre un enrutador exterior y el otro sistema

La figura 10.12.5.3 ilustra un sistema autónomo que utiliza un IGP para difundir accesibilidad entre ruteadores interiores. En dicha figura IGP1 se refiere al protocolo de ruteo que esta utilizando el enrutador interior dentro del sistema autónomo 1 e IGP2 se remite al protocolo utilizado dentro del sistema autónomo 2. En particular, los enrutadores que corren el EGP para anunciar accesibilidad, por lo general necesitan correr también un IGP para obtener información desde el interior del sistema autónomo. En síntesis

Operación de un Router

Un solo enrutador puede utilizar dos diferentes protocolos de ruteo simultáneamente, uno para la comunicación al exterior del sistema autónomo y otro para la comunicación al interior del sistema autónomo.