1. Principios de la interconexión entre redes

a) Requisitos

- Proporcionar un enlace entre redes.
- Proporcionar encaminamientos y entrega de datos entre procesos de diferentes redes.
- Mantener un mecanismo de contabilidad y estado de redes y encaminamientos.
- Proporcionar estos servicios sin tener que cambiar la arquitectura de la red.

Para esto, los sistemas se tienen que acomodar a las diferencias entre las redes con:

- Diferentes esquemas de direccionamiento.
- Diferente tamaño máximo de bloque.
- Diferentes mecanismos de acceso a la red.
- Diferentes valores de expiración de los temporizadores.
- Recuperación de errores.
- Informes de estado.
- Técnicas de encaminamiento.
- Control de acceso al usuario.
- Funcionamiento con conexión, sin conexión.

b) Enfoques sobre la arquitectura

El modo de funcionamiento (en datagramas o en circuitos virtuales) determina la arquitectura de la red.

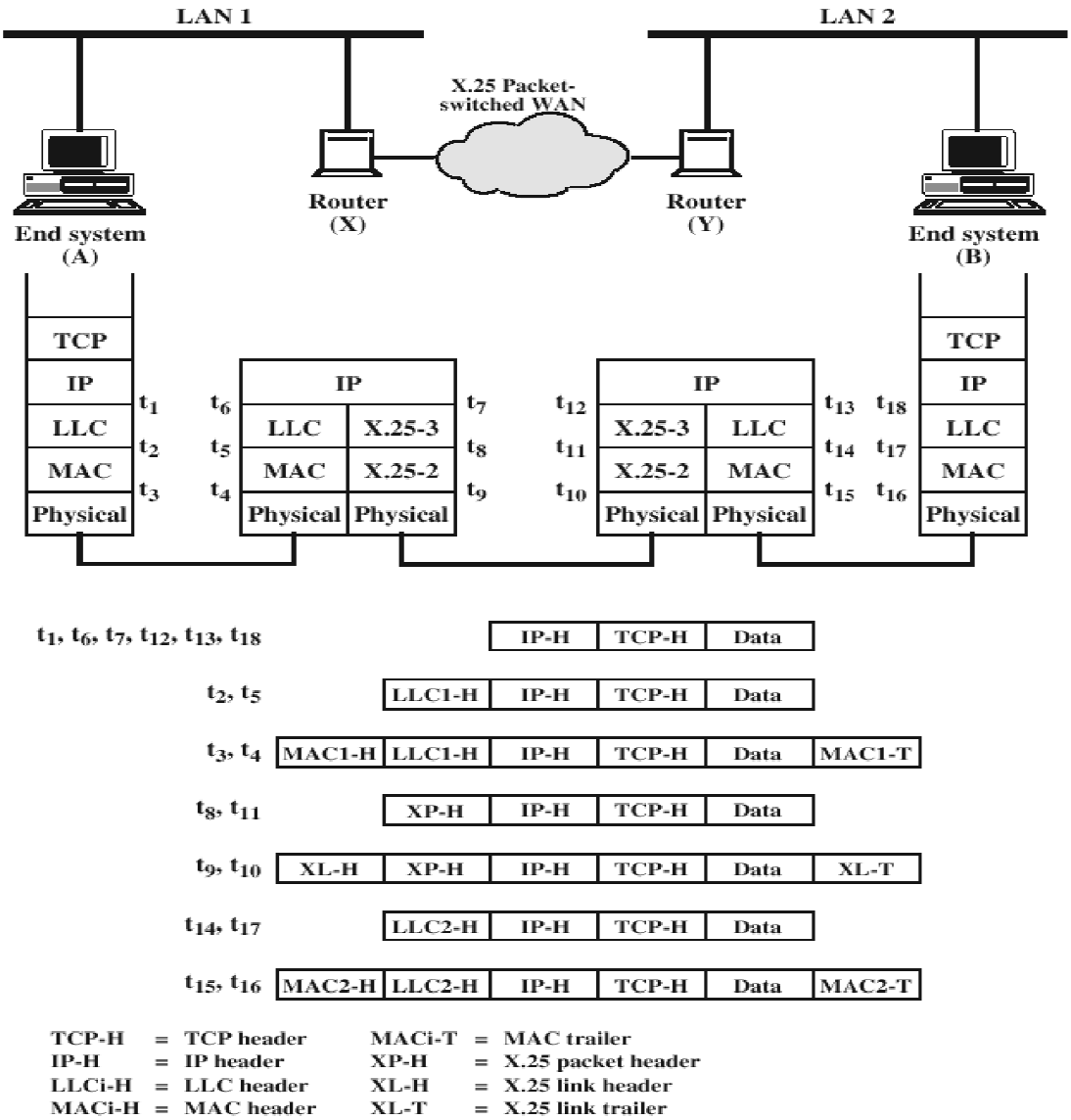
- Modo de funcionamiento con conexión: cuando se emplea este tipo de funcionamiento (generalmente en circuitos virtuales) cada sistema intermedio conecta dos subredes. Para pasar información desde un emisor hasta un receptor, ambos sistemas establecen un circuito lógico a través de una serie de sistemas intermedios Estos sistemas intermedios son los mismos y únicos para cada conexión de los dos equipos conectados.
  Para los usuarios emisor y receptor, parece que la conexión es punto a punto. Para hacer esto posible, la capa de red del emisor, receptor y sistemas intermedios deben de proporcionar funciones similares.
- Modo de funcionamiento sin conexión: en funcionamiento sin conexión (generalmente en datagramas) el emisor envía un bloque a la red y cada sistema intermedio repite el bloque para encaminarlo al sistema final. De esta forma, es posible que el mismo bloque llegue al destino varias veces y por distintos caminos.
  En cada unidad de encaminamiento se decide el mejor camino a seguir por cada bloque, independientemente de que pertenezca al mismo emisor y al mismo destino. Para esto es necesario que todos los sistemas emisor, receptor e intermedios tenga un protocolo similar de red (IP).
- Enfoque utilizando puentes: mediante los puentes (“bridges”), es la capa MAC (debajo de la de red) la encargada de la retransmisión de los bloques. Para esto, los sistemas inicial y final deben compartir la capa de red y transporte. Además, todas las redes deben usar el mismo protocolo en la capa de enlace.

c) <u>Interconexión entre redes sin conexión</u>

IP proporciona un servicio sin conexión (con datagramas) con las siguientes ventajas:

- Es un sistema flexible ya que permite trabajar con muchos tipos de redes. Algunas incluso con conexión.
- Es un sistema muy robusto.
- Es el mejor sistema para un protocolo de transporte sin conexión.

Ejemplo: sean dos sistemas (A y B) que pertenecen a dos redes distintas conectadas por medio de otra red WAN. (<u>Ilustración 1</u>).



<u>Ilustración 1: Operación del Protocolo Internet</u>

La red WAN es de conmutación de paquetes. Los sistemas A y B deben de tener el mismo protocolo IP de red e idénticos protocolos superiores (de transporte y de aplicación). Los dispositivos de encaminamiento sólo deben de implementar las capas de red e inferiores. El protocolo IP de A recibe bloques de datos y les añade una cabecera de dirección global de red (dirección de red de la estación B). De esta forma, se construye un datagrama. Este datagrama se pasa a la red y es recibido por el primer sistema de encaminamiento, que lee la cabecera IP y pone la cabecera necesaria para poder ser

leído por la WAN. La WAN lo recibe y lo pasa al sistema de encaminamiento que lo va a guiar a la estación final. Este sistema de encaminamiento quita la cabecera de la WAN y pone la de IP para enviarlo al sistema final donde llegará a su protocolo IP (y será pasado sin cabecera IP a su capa superior). Bajo el protocolo IP está el LLC, el MAC y el físico. Cada uno de estos protocolos va añadiendo su propia cabecera que será quitada y puesta otra vez por cada uno de los sistemas de encaminamiento. El sistema final hace lo mismo. Cuando un dispositivo de encaminamiento lee la cabecera IP del datagrama que tiene que encaminar y no sabe dónde enviarlo, devuelve un datagrama con la información del error.
Cada nueva unidad de datos se pone en cola de su capa inferior hasta que le llega el turno de ser enviada. Si hay dos redes conectadas por un sistema de encaminamiento, éste puede desechar datagramas de su cola para así no perjudicar la red más rápida esperando datagramas de la más lenta.
IP no garantiza que los datos lleguen a su destino y en orden. Es TCP la que se encarga de esto.
IP, al no garantizar el orden y llegada de datos, funcionará con cualquier tipo de red ya que los datos pueden seguir caminos múltiples antes de llegar a su destino. Esto le permite además, cambiar de rutas cuando hay congestión o algún tipo de incompatibilidad.

d) Cuestiones de diseño

La arquitectura de interconexión de redes es similar, en su ámbito, a la arquitectura de red de conmutación de paquetes. Los dispositivos de encaminamiento son similares en su funcionamiento a los nodos de conmutación de paquetes y usan las redes intermedias de una forma semejante a los enlaces de transmisión.

- Encaminamiento: se implementa mediante una tabla en cada sistema de encaminamiento y en cada sistema final. Por cada red de destino, se tabula el siguiente dispositivo de encaminamiento al que hay que enviar el datagrama. Las tablas pueden ser estáticas o dinámicas, siendo las dinámicas mejores porque se pueden actualizar para cuando hay congestión o sistemas intermedios en mal funcionamiento. En las tablas se puede incluir sistemas para manejar la seguridad (se le puede impedir el acceso a ciertas redes a ciertas estaciones no acreditadas). Pude hacerse encaminamiento en la fuente, indicando ésta en el datagrama el camino a seguir. En los propios datagramas, los sistemas de encaminamiento pueden adjuntar información de su dirección para difundirla en la red.
- Tiempo de vida de los datagramas: para evitar que un datagrama circule indefinidamente por la red, se puede adjuntar un contador de saltos (hops) (que se decrementa cada vez que salta a un dispositivo de encaminamiento) o un contador de tiempo que pasado un cierto tiempo, haga que el datagrama sea destruido por un dispositivo de encaminamiento.
- Segmentación y ensamblado: puede ser necesario que los paquetes, al pasar de unas redes a otras, deban de ser fragmentados por necesidades propias de dichas redes. Se puede dejar que el sistema final los vuelca a ensamblar, pero esto hace que haya demasiado trabajo para él y además, puede que haya subredes intermedias que puedan trabajar con bloques más grandes que los suministrados por la red anterior, de forma que se pierde eficiencia. Pero las ventajas de este sistema de ensamblado al final es que los dispositivos de encaminamiento no tienen que mantener en memoria los sucesivos fragmentos del datagrama y además se permite encaminamiento dinámico (ya que los sucesivos fragmentos no tienen por qué tomar el mismo encaminamiento). En IP se hace ensamblado final. El sistema final debe de tener la suficiente memoria para ir guardando los trozos para ensamblarlos cuando lleguen todos. Como IP no garantiza la llegada de todos los datos, se debe utilizar un sistema de temporización (bien usando un tiempo propio desde la llegada del primer trozo del datagrama o bien usando los datos de temporización incluidos en la cabecera del datagrama).

- Control de errores: IP no garantiza la llegada de un datagrama, pero debe de informar a la estación o dispositivo de encaminamiento del error.
- Control de flujo: el control de flujo en servicios sin conexión se realiza enviando tramas de retención a los dispositivos anteriores para que éstos paren de enviar datos.

2. El protocolo Internet

a) Servicios IP

Los servicios que proporciona IP a TCP son: "**Send"** (envío) y "**Deliver"** (entrega).
TCP utiliza Send para solicitar el envío de una unidad de datos y Deliver es utilizada por IP para notificar a TCP que una unidad de datos ha llegado.
Los campos incluidos en estas dos llamadas son: dirección origen y destino de los datos, usuario IP, identificador de bloque de datos, indicador sobre si está permitida la segmentación del bloque, tipo de servicio, tiempo de vida, longitud de los datos, datos. Algunos campos no son necesarios para Deliver.
El tipo de servicio solicitado puede ser de encaminamiento lo más rápido posible, lo más seguro posible, prioridad, etc.

b) Protocolo IP

El datagrama IPv4 (Protocolo IP versión 4) tiene varios campos, entre los que se encuentran:

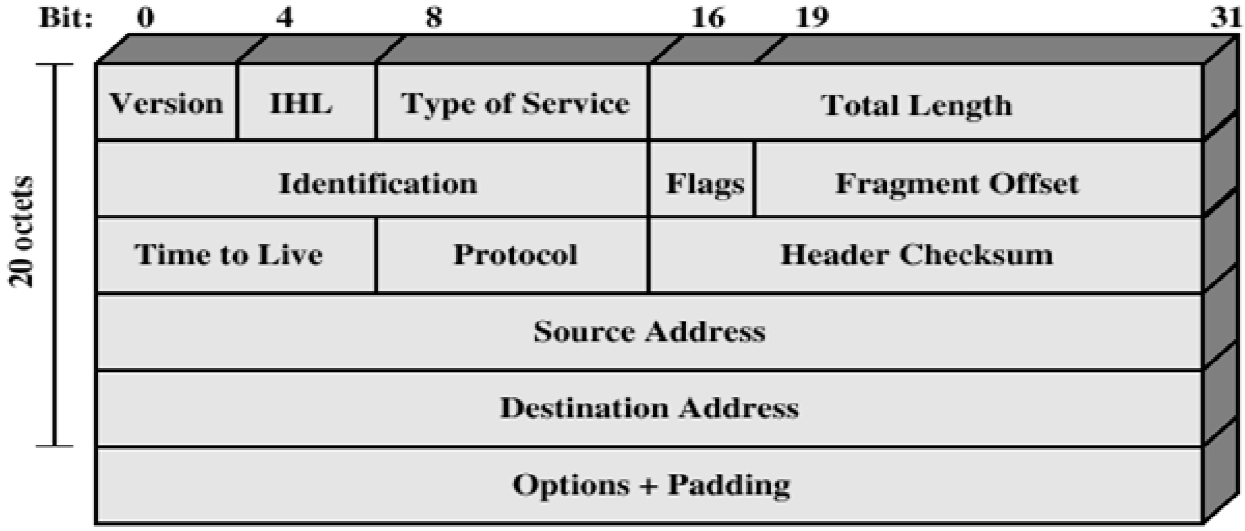


Ilustración 2: Cabecera de datagrama IPv4

- Versión: para futuras versiones.
- Longitud de la cabecera Internet ("Internet Header Lenght")
- Tipo de servicio: seguridad, prioridades, etc.
- Longitud total del datagrama.
- Identificador del datagrama.
- Indicadores de permiso de segmentación ("flags"): para poder usarse en sistemas en los que se deba segmentar en el destino o en dispositivos intermedios.
- Desplazamiento del fragmento ("fragment offset"): identifica dónde va el fragmento dentro del datagrama fragmentado.
- Tiempo de vida: tiempo de espera antes de destruir el datagrama.
- Suma de comprobación de la cabecera para detección de errores.
- Dirección de origen.

- Dirección de destino.
- Opciones variadas: solicitadas por el usuario que envía los datos.
- Relleno ("padding"): bits para asegurar la multiplicidad en 32 bits.
- Datos: datos de usuario.

Se grafica en la Ilustración 3 la cabecera del datagrama IPv6 (IP versión 6), que trabaja con direcciones de 128 bits, en lugar de 32 bits como la IPv4.

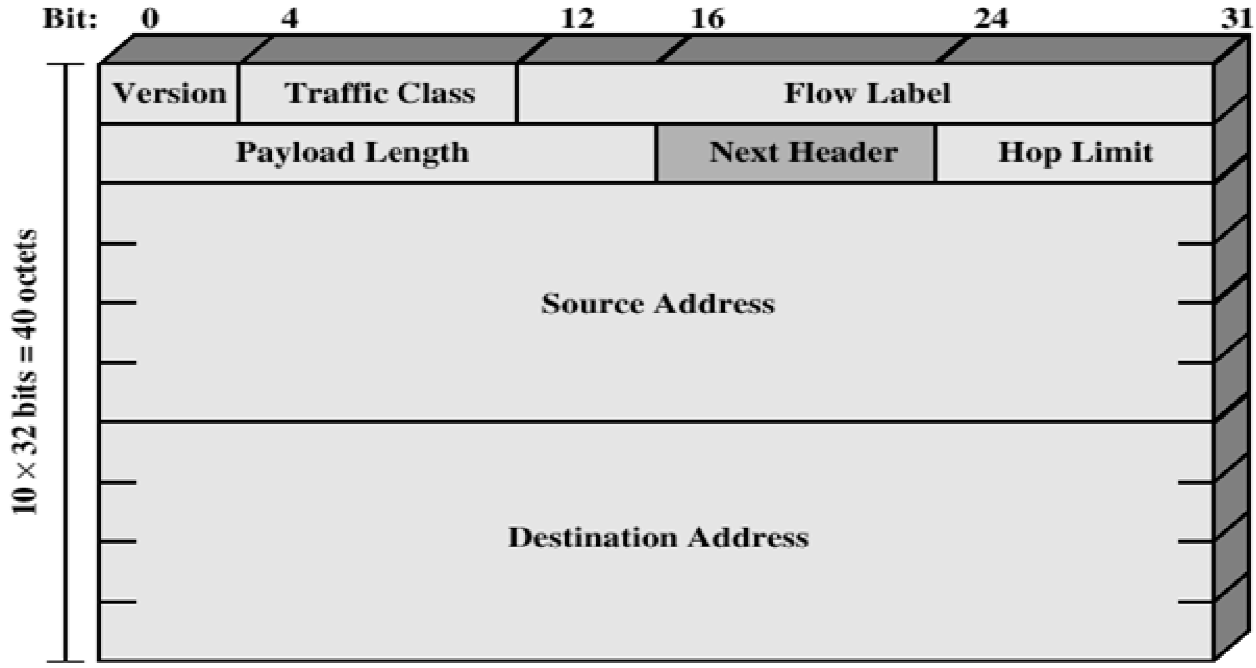


Ilustración 3: Cabecera del datagrama IPv6.

c) Direcciones IP

La dirección de origen y destino en la cabecera IP es una dirección global de Internet de 32 bits. De estos 32 bits, algunos identifican al computador y el resto a la red. Estos campos son variables en extensión para poder ser flexibles al asignar direcciones de red. Hay diferentes tipos de redes que se pueden implantar en la dirección de red. Unas son grandes (con muchas subredes), otras medianas y otras pequeñas. Es posible y adecuado mezclar en una dirección los tres tipos de clases de redes.

3. ENRUTAMIENTO (ROUTING) EN PROTOCOLO IP

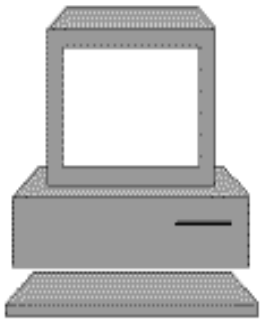
Antes de que los datos se envíen a los medios de transmisión (networking) (capa física), se encapsulan y llevan consigo información necesaria para hallar el destino correcto. Durante el proceso de encapsulación cada capa del modelo OSI conserva los datos que recibió de la capa inmediatamente superior con toda su información de modo que esta información pueda ser interpretada por la misma capa en el extremo receptor. De este modo, los datos que bajan por las capas de red se encapsulan con la información que se produce en la capa de red o capa 3.
Los datos que pasan a través de la capa de red se encapsulan de modo de contener la información sobre la dirección IP tanto de origen como de destino.

Cuando los datos pasan por la capa de enlace de datos se encapsulan de modo de contener información acerca de la dirección MAC tanto de origen como de destino A medida que pasa a través de los medios de networking, el paquete de datos lleva consigo toda la información antes descripta
Cada dispositivo de la red está obligado a mirar el paquete de datos a medida que pasa para ver si la dirección MAC de destino que lleva concuerda con la del dispositivo. El lugar donde se producen dichas comparaciones se conoce como capa de enlace de datos o capa 2 del modelo OSI. Si el dispositivo descubre que su dirección MAC concuerda con la dirección MAC de destino que lleva el paquete de datos, el dispositivo copia el paquete en la computadora. Allí separa la capa de enlace de datos o capa 2 de la encapsulación, conocida como encabezado de enlace, y copia el paquete de datos en la siguiente capa, la capa de red o capa 3. Ahí el dispositivo verifica si la dirección IP de destino que lleva el paquete de datos concuerda con su dirección IP. Si ambas concuerdan, el dispositivo separa el encabezado de la capa de red o capa 3 y envía el paquete de datos hacia la siguiente capa del modelo OSI. El proceso se repite hasta que el resto del paquete llega a la aplicación donde se leerán los datos.
Las direcciones MAC identifican a un dispositivo específico independientemente de la red a la cual pertenezcan. Las direcciones IP se utilizan para identificar a las redes y a los dispositivos conectados a dichas redes. De este modo, las direcciones IP son esenciales para que se produzca el internetworking a través de WAN o de varias LAN.

¿Cómo saben los dispositivos cuándo copiar los datos para que pasen por la capa de red del modelo OSI? Los protocolos determinan si los datos se envían por la capa de red hacia los niveles más altos del modelo OSI. Básicamente, para que esto suceda, el paquete de datos debe contener tanto la dirección MAC como la dirección IP. Si una u otra faltan, los datos no se pasarán a los niveles superiores.

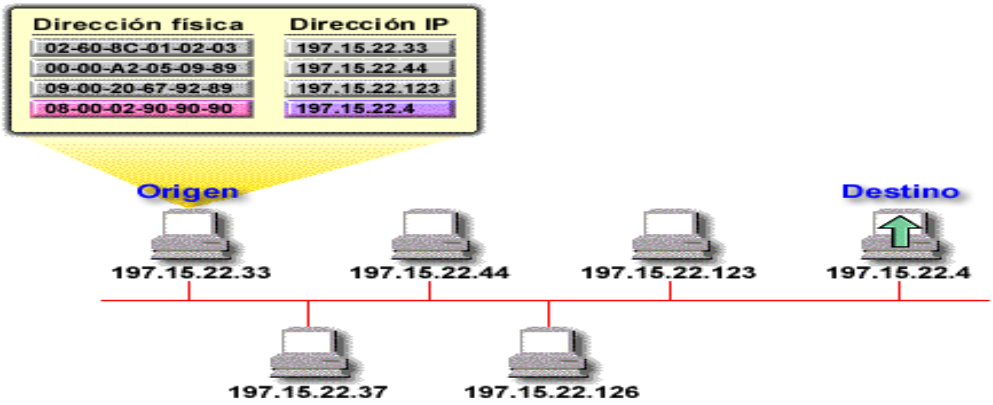
¿Cómo saben los dispositivos de una red de área local las direcciones MAC y las direcciones IP de otros dispositivos? Una vez que un dispositivo sabe la dirección IP de destino donde desea enviar los datos también debe agregar la dirección MAC de destino al paquete de datos. ¿Cómo determina qué dirección MAC agregar a los datos encapsulados?

Algunos dispositivos tienen tablas que contienen todas las direcciones MAC y todas las direcciones IP de los demás dispositivos conectados a la misma LAN. Estas tablas no son más que una sección de memoria RAM de cada dispositivo.



Dirección física	Dirección IP
02-60-8C-01-02-03	197.15.22.33
00-00-A2-05-09-89	197.15.22.44
09-00-20-67-92-89	197.15.22.123
08-00-02-90-90-90	197.15.22.4

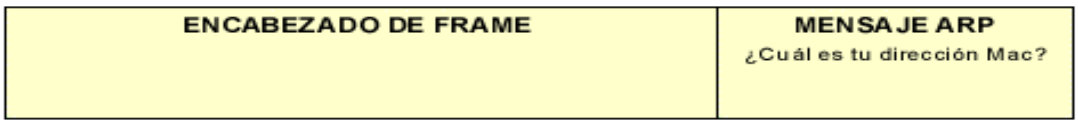
Se las denomina tablas *ARP ("Address resolution protocol")* porque se utiliza un lenguaje conocido como *Protocolo de Resolución de Direcciones* para mapear las direcciones IP en las direcciones MAC. En su mayoría, las tablas ARP se conservan en la memoria caché en forma automática. Es raro que el administrador de una red modifique una tabla en forma manual. Cada computadora de una red lleva su propia tabla ARP. Cada vez que un dispositivo de la red desea enviar datos a la red utiliza la información que tiene su tabla ARP para lograrlo.



¿Cómo utilizan los dispositivos las tablas ARP para enviar datos? Una vez que el origen ha determinado la dirección IP de destino, el protocolo de Internet del origen mira su tabla de ARP para ubicar la dirección MAC de destino. Si el protocolo de internet ubica un mapeo de dirección IP de destino con la dirección MAC de destino en su tabla, enlaza la dirección IP con la dirección MAC y las utiliza para encapsular los datos. A continuación, el paquete de datos se transmite a los medios de networking para luego ser tomados por el destino.

¿Qué sucede si el dispositivo no logra ubicar la dirección MAC de destino en su tabla ARP? Un dispositivo de origen quiere enviar datos a otro dispositivo. El origen sabe la dirección IP de destino pero no puede ubicar la correspondiente dirección MAC en su propia tabla ARP. Si el destino debe retener los datos y pasarlos a los niveles superiores del modelo OSI, el origen debe utilizar tanto la dirección MAC de destino como la dirección IP de destino. Por lo tanto, el dispositivo inicia un proceso denominado *solicitud ARP* diseñado para ayudarlo a descubrir cuál es la dirección MAC de destino. Primero el dispositivo construye un paquete de solicitud ARP y lo envía a todos los dispositivos de la red. Para garantizar que el paquete de solicitud ARP será visto por todos los dispositivos de la red, el origen utiliza una dirección MAC de broadcast. La dirección de broadcast que se utiliza en un esquema de direccionamiento MAC resulta cuando todos los lugares se predeterminan en F. Así, una dirección MAC de broadcast tendría la forma FF-FF-FF-FF-FF-FF.

¿Qué información contiene una solicitud ARP? Las solicitudes ARP están estructuradas de una manera particular. Como el protocolo de resolución de direcciones funciona en las capas inferiores del modelo OSI, el mensaje que contiene la solicitud ARP debe estar encapsulado dentro del frame de protocolo del hardware. Conceptualmente, esto puede representarse diciendo que el frame de solicitud ARP está dividido en dos partes llamadas: encabezado del frame y mensaje ARP.



ESTRUCTURA DE SOLICITUD ARP

El encabezado del frame puede subdividirse a su vez en lo que se conoce como *encabezado MAC* y *encabezado IP*.

ENCABEZADO MAC		ENCABEZADO IP		MENSAJE DE SOLICITUD ARP
Destino	Origen	Destino	Origen	¿Cuál es tu dirección MAC?
FF-FF-FF-FF-FF-FF	02-60-8C-01-02-03	197.15.22.126	197.15.22.33	

ESTRUCTURA DE SOLICITUD ARP

¿Qué sucede cuando el origen envía una solicitud ARP a través de la red? Como el paquete de solicitud ARP se envía en modo broadcast, todos los dispositivos de la red local reciben el paquete y lo pasan a la capa de red para ser examinado. Si la dirección IP del dispositivo concuerda con la dirección IP que contiene la solicitud ARP, el dispositivo responde enviando al origen su dirección MAC. Esto se conoce como *respuesta ARP*. En el ejemplo donde el origen 197.15.22.33 pregunta la dirección MAC del destino cuya dirección IP es 197.15.22.126, el destino tomaría la solicitud ARP y respondería mediante una respuesta ARP que contenga su dirección MAC.

ENCABEZADO MAC		ENCABEZADO IP		MENSAJE DE RESPUESTA ARP
Destino	Origen	Destino	Origen	Esta es mi dirección MAC.
02-60-8C-01-02-03	08-00-02-89-90-80	197.15.22.33	197.15.22.126	

ESTRUCTURA DE RESPUESTA ARP

¿Qué sucede cuando la respuesta ARP se envía nuevamente al dispositivo de origen de la red? Una vez que el dispositivo que originó la solicitud ARP recibe la respuesta ARP, extrae la dirección MAC del encabezado y actualiza su tabla ARP. Ahora que tiene toda la información que necesita, el dispositivo puede direccionar correctamente sus datos, tanto con la dirección MAC de destino como con la dirección IP de destino. Utiliza esta nueva información para encapsular los datos antes de enviarlos a través de la red. Esta vez, cuando los datos llegan a destino, se establece una coincidencia en la capa de enlace de datos. La capa de enlace de datos separa el encabezado MAC y transfiere los datos a la próxima capa superior, la capa de red. La capa de red examina los datos y detecta que su dirección IP concuerda con la dirección IP de destino que lleva en el encabezado IP de los datos. La capa de red separa el encabezado IP y transfiere los datos a la siguiente capa superior del modelo OSI, la capa de transporte. El proceso se repite hasta que el resto del paquete llega a la capa de aplicación donde se leerán los datos.

ENCABEZADO MAC		ENCABEZADO IP		DATOS
Destino	Origen	Destino	Origen	
08-00-02-89-90-80	02-60-8C-01-02-03	197.15.22.126	197.15.22.33	

ESTRUCTURA DEL FRAME DE DATOS

¿Qué hacen los otros dispositivos de la red cuando se envía una respuesta ARP? Cualquier dispositivo de la red que haya recibido la solicitud ARP de broadcast ve la información que lleva la solicitud ARP. Los dispositivos utilizan la información de origen para actualizar sus tablas ARP.

¿Por qué es importante que los dispositivos de la red actualicen sus tablas ARP? Si los dispositivos no mantienen tablas ARP el proceso de emisión de una solicitud ARP y de una respuesta ARP debería repetirse cada vez que un dispositivo desea enviar datos a otro dispositivo de la red. Esto sería sumamente ineficiente y aumentaría el tráfico de la red. Para evitarlo, cada dispositivo tiene su propia tabla ARP.
Las tablas ARP deben actualizarse periódicamente de modo que estén vigentes. El proceso de actualización de las tablas ARP no sólo incluye el agregado de información sino también la eliminación de información. Como el envío de información a través de las redes depende de la información más actualizada disponible, los dispositivos están configurados para eliminar toda información de las tablas ARP que exceda un límite de tiempo en particular. Este proceso se conoce como "envejecimiento". Para reemplazar la información eliminada de las tablas ARP, los dispositivos las actualizan constantemente con la información que obtienen de sus propias solicitudes ARP y de las solicitudes que provienen de otros dispositivos de la red local. Como ARP permite que los protocolos mantengan actualizadas sus tablas ARP, esto ayuda a limitar la cantidad de tráfico de broadcast que circula por la red local.

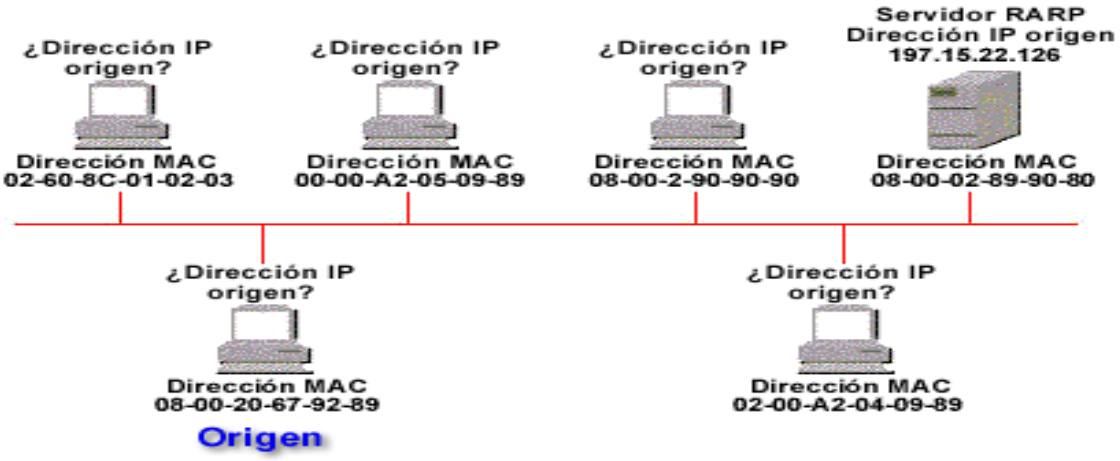
¿Qué es RARP? Deben conocerse tanto las direcciones IP como las direcciones MAC antes de que los dispositivos de la red envíen los datos a la capa cuatro, la capa de transporte, del modelo OSI. Para que el destino que recibe el paquete de datos sepa a quién responder, el paquete de datos también debe llevar tanto la dirección MAC de origen como la dirección IP de origen. Pero, ¿qué sucede cuando un origen conoce su dirección MAC pero no conoce su dirección IP? El protocolo que utiliza un dispositivo cuando no conoce su propia dirección IP es el *Protocolo de Resolución de Dirección Inversa*, comúnmente llamado *RARP.(Reverse Address Resolution Protocol)* Al igual que el ARP, el RARP une las direcciones MAC a las direcciones IP de modo que los dispositivos de la red las puedan utilizar para encapsular los datos antes de enviarlos a través de la red.

¿Qué tipo de dispositivos necesitarían utilizar RARP? ¿Cuándo conocería un dispositivo su dirección MAC pero no su dirección IP? Esto sucede en las estaciones de trabajo sin disco o en las terminales no inteligentes. Cada vez que una estación de trabajo sin disco termina una sesión y se apaga, lo que tiene en su memoria caché desaparece porque no tiene disco rígido. Por lo tanto, las estaciones de trabajo sin disco o las terminales no inteligentes que se enciendan por primera vez no tendrán tablas de ARP a las cuales referirse ni direcciones IP para referencia propia.

¿Qué requieren los dispositivos que utilizan RARP? Los dispositivos que utilizan RARP requieren la presencia de un *servidor RARP* en la red para responder a las solicitudes
En general, hay muchas estaciones de trabajo sin disco conectadas a la misma red.
De este modo, si es improbable que una estación de trabajo sin disco conectada a la red conozca su dirección IP habrá otras con igual improbabilidad de tener esta información y no podrán informarla en respuesta a las solicitudes RARP.
Por lo tanto, se necesitan servidores designados que posean memoria caché y discos capaces de almacenar tablas ARP para responder a las solicitudes RARP.

¿Qué es una solicitud RARP? Un dispositivo de origen desea enviar datos a otro dispositivo. El origen conoce su propia dirección MAC pero no puede ubicar su dirección IP en la tabla ARP. Si el destino debe retener los datos, pasarlos a las capas superiores del modelo OSI y responder al dispositivo que originó los datos, el origen debe incluir tanto su dirección MAC como su dirección IP. Por lo tanto, el origen da inicio a un proceso denominado *solicitud RARP* diseñado para ayudarle a descubrir cuál es su dirección IP. En primer término, el dispositivo construye un paquete de solicitud RARP y lo envía a la red. Para garantizar que la solicitud RARP será vista por todos los dispositivos

de la red, el origen utiliza una dirección IP de broadcast.



(Se colocan todos 1 binarios en la porción de host de la dirección IP de destino para garantizar que los datos se envíen en modo broadcast a todos los nodos de la red.)

¿Cuál sería la dirección de broadcast de la red 197.15.22.0? Respuesta: La dirección IP de broadcast de la red 197.15.22.0 sería 197.15.22.255.

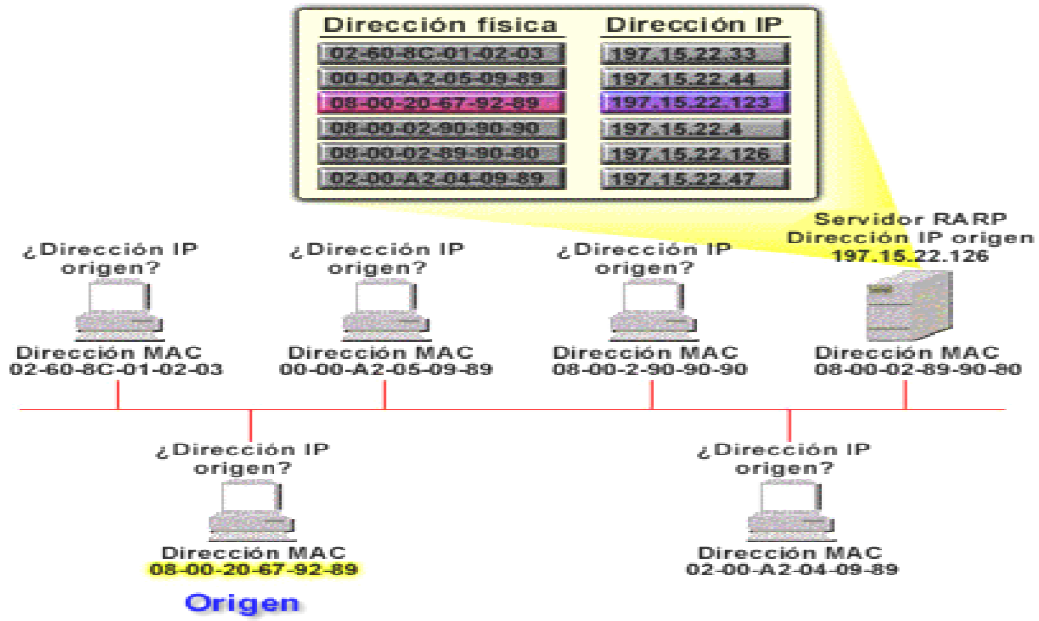
¿Qué información contiene una solicitud RARP? Las solicitudes RARP tienen la misma estructura que las solicitudes ARP. Por lo tanto, las solicitudes RARP consisten en un encabezado MAC, un encabezado IP, y el mensaje de solicitud RARP. La única diferencia que tiene el formato de un paquete RARP es que tanto la dirección MAC de destino como de origen deben estar completas. El campo de dirección IP de origen queda vacío. Como se lo va a enviar en modo broadcast a todos los dispositivos de la red, la dirección IP de destino será todos 1 binarios.

ENCABEZADO MAC		ENCABEZADO IP		MENSAJE DE SOLICITUD RARP
Destino	Origen	Destino	Origen	¿Cuál es mi dirección IP?
00-40-33-2B-35-77	01-60-8C-01-02-03	11111111	?????????	

ESTRUCTURA DE SOLICITUD RARP

¿Qué sucede cuando el origen envía una solicitud RARP a la red? Como el frame de la solicitud RARP se envía en modo broadcast, lo verán todos los dispositivos de la red. Sin embargo, sólo el servidor RARP designado puede responder a la solicitud RARP. El servidor RARP designado responde enviando una respuesta RARP que contiene la dirección IP del dispositivo que originó la solicitud RARP.

¿Qué estructura tienen las respuestas RARP y qué información contiene cada uno de los encabezados? Las respuestas RARP tienen la misma estructura que las respuestas ARP. Las respuestas RARP contienen un mensaje de respuesta RARP y están encapsuladas en un encabezado MAC y en un encabezado IP. Cuando el dispositivo donde se originó la solicitud RARP recibe la respuesta RARP encuentra su propia dirección IP. Para ver cómo funciona esto, imaginar que un servidor designado cuya dirección IP sea 197.15.22.126 responde a una solicitud IP de una estación sin disco cuya dirección MAC es 08-00-20-67-92-89.

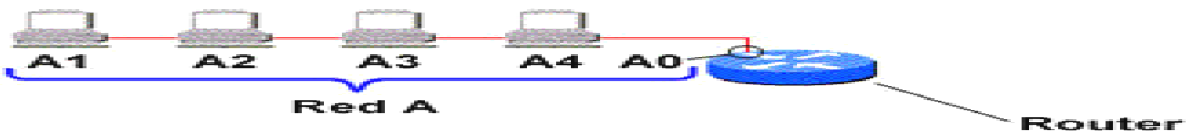


¿Qué información aparecería en el encabezado IP de esta respuesta RARP para el origen? Respuesta: La dirección IP de origen 197.15.22.126 aparecería en el encabezado IP de la respuesta RARP.

¿Qué información aparecería en el encabezado IP de esta respuesta RARP para el destino? Respuesta: La dirección IP de destino 197.15.22.123 aparecería en el encabezado IP.

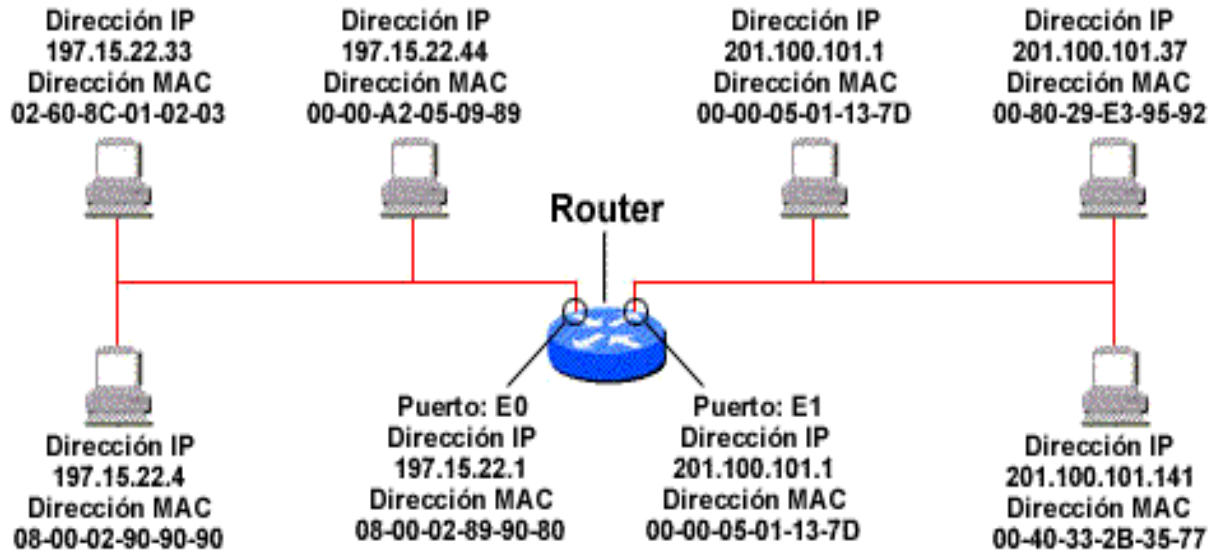
¿Qué hace el dispositivo que originó la solicitud RARP cuando recibe la respuesta RARP? Cuando el dispositivo que originó la solicitud RARP recibe la respuesta RARP copia su dirección IP en su memoria caché donde residirá mientras dure la sesión. Sin embargo, cuando se apaga la terminal, esta información vuelve a desaparecer. Mientras dure la sesión, la estación de trabajo sin disco que originó la solicitud RARP puede utilizar la información que obtuvo de este modo para enviar y recibir datos a través de la red.

¿Qué dispositivos de internetworking tienen tablas ARP? El puerto o interfaz donde un router está conectado a una red se considera parte de dicha red. Por lo tanto, la interfaz del router conectada a la red tiene una dirección IP para dicha red. Como los routers, al igual que cualquier otro dispositivo de una red, envían y reciben datos a través de la red, crean tablas ARP que mapean las direcciones IP a las direcciones MAC.



¿En qué se diferencian las tablas ARP que llevan los routers de las tablas ARP que llevan otros dispositivos de una red? Los routers pueden estar conectados a múltiples redes o subredes. En términos generales, los dispositivos de la red mapean las direcciones IP y las direcciones MAC que ven de manera regular y repetida. En resumen, esto significa que un dispositivo típico contiene información de mapeo que pertenece sólo a los dispositivos de su propia red. Es poco lo que sabe de los dispositivos que están fuera de su red de área local. Como los routers crean tablas que describen

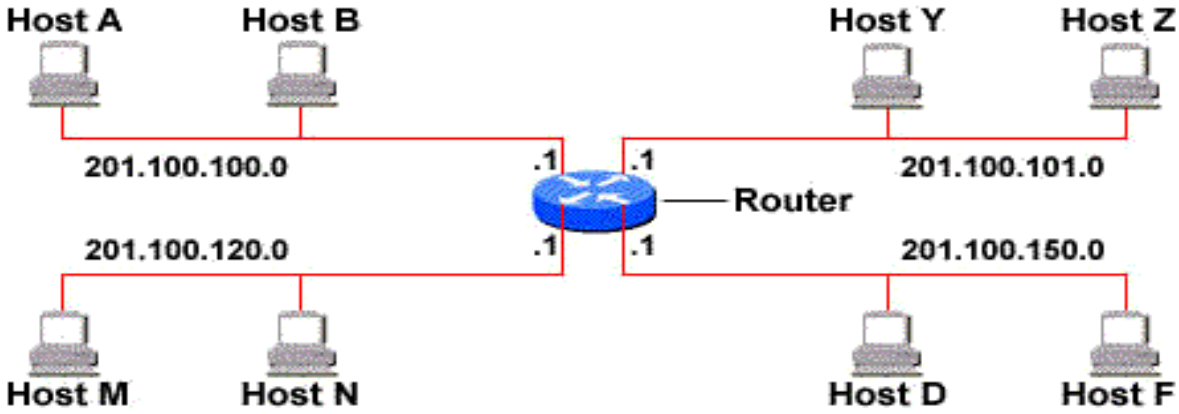
todas las redes conectadas a los mismos, las tablas de ARP que llevan los routers pueden contener las direcciones IP y las direcciones MAC de los dispositivos ubicados en más de una red



Protocolo	Dirección	Dirección MAC	Interfaz
IP	197.15.22.33	02-60-8c-01-02-03	ethernet 0
IP	197.15.22.44	00-00-A2-05-09-89	ethernet 0
IP	197.15.22.4	08-00-02-90-90-90	ethernet 0
IP	197.15.22.1	08-00-02-89-90-80	ethernet 0
IP	201.100.101.37	00-80-29-e3-95-92	ethernet 1
IP	201.100.101.1	00-00-05-01-13-7d	ethernet 1
IP	201.100.101.141	00-40-33-2b-35-77	ethernet 1
IP	201.100.101.163	00-40-33-29-43-eb	ethernet 1

TABLA DEL ROUTER INCLUYENDO INFORMACIÓN ARP

ROUTERS: TABLAS DE ENRUTAMIENTO



RED DE DESTINO	PUERTO DEL ROUTER
201.100.100.0	201.100.100.1
201.100.101.0	201.100.101.1
201.100.120.0	201.100.120.1
201.100.150.0	201.100.150.1

Además de mapear las direcciones IP en direcciones MAC, las tablas de los routers también mapean los puertos. ¿Por qué razón los routers necesitarían hacer esto?

SUGERENCIA: Estudiar el gráfico que describe la tabla de ARP del router, siguiente.

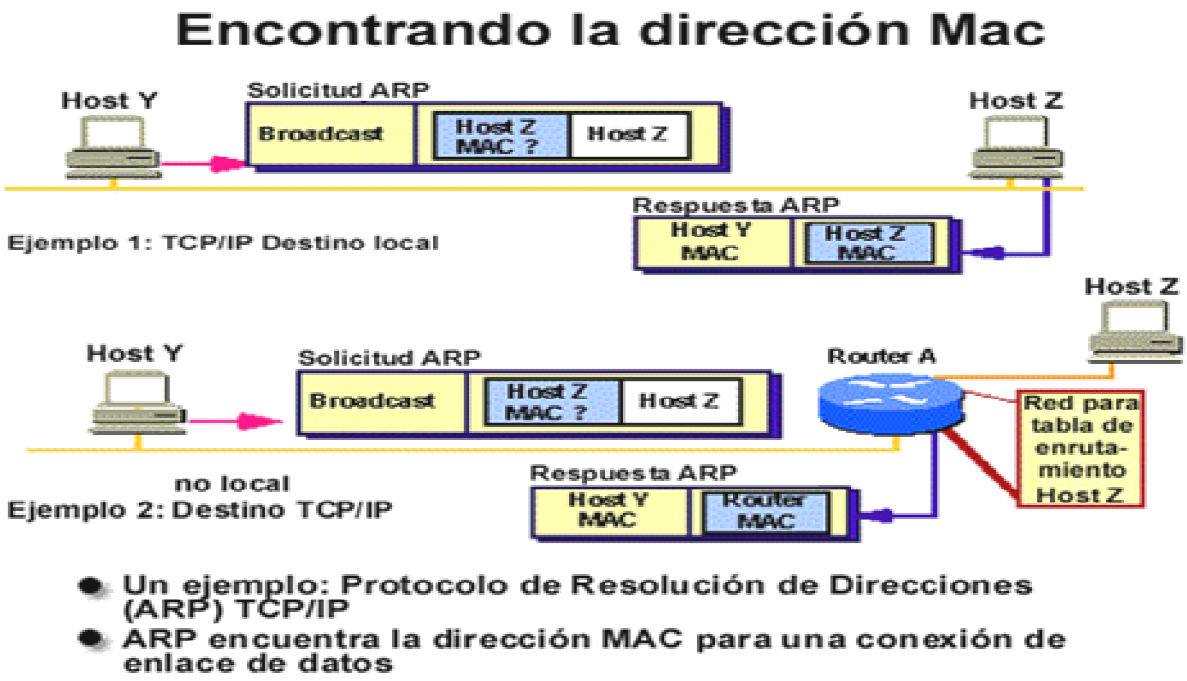
Protocolo	Dirección	Dirección MAC	Interfaz
IP	197.15.22.33	02-60-8c-01-02-03	ethernet 0
IP	197.15.22.44	00-00-A2-05-09-89	ethernet 0
IP	197.15.22.4	08-00-02-90-90-90	ethernet 0
IP	197.15.22.1	08-00-02-89-90-80	ethernet 0
IP	201.100.101.37	00-80-29-e3-95-92	ethernet 1
IP	201.100.101.1	00-00-05-01-13-7d	ethernet 1
IP	201.100.101.141	00-40-33-2b-35-77	ethernet 1
IP	201.100.101.163	00-40-33-29-43-eb	ethernet 1

TABLA DEL ROUTER INCLUYENDO INFORMACIÓN ARP

Respuesta: Como el router de este ejemplo tiene más de una dirección IP, la tabla del router mapea cada dirección IP a la dirección MAC correspondiente. De esta forma, el router utiliza las direcciones IP de la red para seleccionar rutas para poder enviar datos de una red a otra.

¿Qué otras direcciones contienen los routers en sus tablas? ¿Qué sucede si un paquete de datos llega a un router teniendo como destino una red a la cual no está conectado el router? Además de las direcciones IP y de las direcciones MAC de los dispositivos de la red a la cual está conectado, un router posee también las direcciones IP y las direcciones MAC de otros routers. Utiliza estas direcciones para direccionar los datos hacia su destino final. Si un router recibe un paquete cuyas direcciones de destino no están en su tabla de enrutamiento, envía el paquete a las direcciones de otros routers que supuestamente podrían contener información sobre el host de destino en sus tablas de enrutamiento.

¿Qué sucede cuando un dispositivo de una subred no conoce la dirección MAC de destino de un dispositivo de otra subred? En términos generales, un dispositivo de una red no puede enviar una solicitud ARP a un dispositivo de otra red. ¿Por que razón esto es así?
Respuesta: Porque las solicitudes ARP se envían en modo broadcast, los routers no las envían a otras redes.
Pero, ¿qué sucede en el caso de las subredes? ¿Puede un dispositivo descubrir la dirección MAC de un dispositivo de otra subred? La respuesta es sí, siempre y cuando el origen dirija su pregunta al router. Este trabajo con la intervención de un tercero que se denomina *ARP proxy*[1], es lo que permite hacerlo. Esencialmente, el router actúa como *gateway*[2] por defecto.

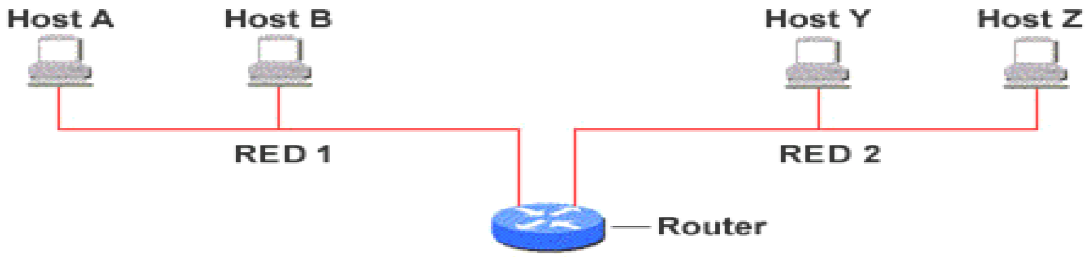


¿Cuándo un dispositivo busca los servicios de un router? Si el origen reside en una red con un número de red diferente al del destino deseado y si el origen no conoce la dirección MAC del destino, tendrá que utilizar los servicios de un router para que sus datos lleguen al destino. Cuando los routers

[1] **ARP Proxy** - Protocolo de resolución de direcciones proxy. Variación del protocolo ARP en el cual un dispositivo intermedio (por ejemplo, un router) envía una respuesta ARP en nombre de un nodo extremo al host solicitante. ARP proxy puede disminuir el uso del ancho de banda en enlaces WAN de baja velocidad

[2] **Gateway** - En la comunidad IP, un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, se utiliza el término *router* para describir los nodos que realizan esta función, mientras que *gateway* se refiere a un dispositivo para fines especiales que convierte información de la capa de aplicación de un stack de protocolo a otro.

se utilizan de este modo se los denomina *gateway por defecto*. Para obtener los servicios de un gateway por defecto, el origen encapsula los datos de modo que contengan la dirección MAC de destino del router. Sin embargo, como quiere que los datos lleguen a un dispositivo y no a un router, el origen utiliza la dirección IP de destino del dispositivo y no la del router en el encabezado IP.



Paquete de datos del Host A al Host Z

Cuando el router toma los datos, separa la información de la capa de enlace de datos que se utilizó en la encapsulación. Pasa los datos a la capa de red donde examina la dirección IP de destino. Luego compara la dirección IP de destino con la información que contienen sus tablas de enrutamiento.
Si el router ubica la dirección IP y la dirección MAC de destino mapeadas y sabe que la red de destino está ubicada o conectada a uno de sus puertos, encapsula los datos con la nueva información de la dirección MAC y los envía al destino correcto.
Si el router no puede ubicar la dirección de destino mapeada y la dirección MAC del dispositivo al cual están destinados los datos, ubica la dirección MAC de otro router que pueda cumplir esta función y envía los datos a dicho router.
Este tipo de enrutamiento se denomina *enrutamiento indirecto*.

¿Qué sucede si el dispositivo no conoce la dirección MAC del router que desea utilizar para los servicios de enrutamiento indirecto? ARP sólo se utiliza en la red local. Pero, ¿qué sucede si un dispositivo de una red desea pedirle a un router no local que preste servicios de enrutamiento indirecto y no conoce la dirección MAC del router no local?
Cuando un origen no conoce la dirección MAC de un router no local, emite una solicitud ARP. La solicitud ARP es tomada por un router conectado a la misma red que el origen. El router emite una respuesta ARP al dispositivo que originó la solicitud ARP. La respuesta contiene la dirección MAC del router no local. De este modo, sin que la solicitud ARP salga en ningún momento de la red local, el origen logra obtener la información de dirección que necesita para enviar datos a dispositivos ubicados en redes distantes.

¿Cuál es la diferencia entre los protocolos enrutados y los protocolos de enrutamiento? Los protocolos son como los lenguajes. Un protocolo es por ejemplo, el protocolo IP, o protocolo de Internet que es un protocolo de capa de red.
Hasta ahora, nos hemos concentrado en las características de los protocolos IP para el direccionamiento. Sin embargo este protocolo también tiene prestaciones para la especificación de tipo de servicio, de fragmentación y de reensamblaje.

Como el protocolo IP se enruta a través de una internetwork, es lo que se denomina un *protocolo enrutado*. IPX de Novel y Appletalk son ejemplos de otros tipos de protocolos enrutados.

Variantes de direccionamiento de protocolos

Ejemplo general

Red	Nodo
1	1

Ejemplo TCP/IP

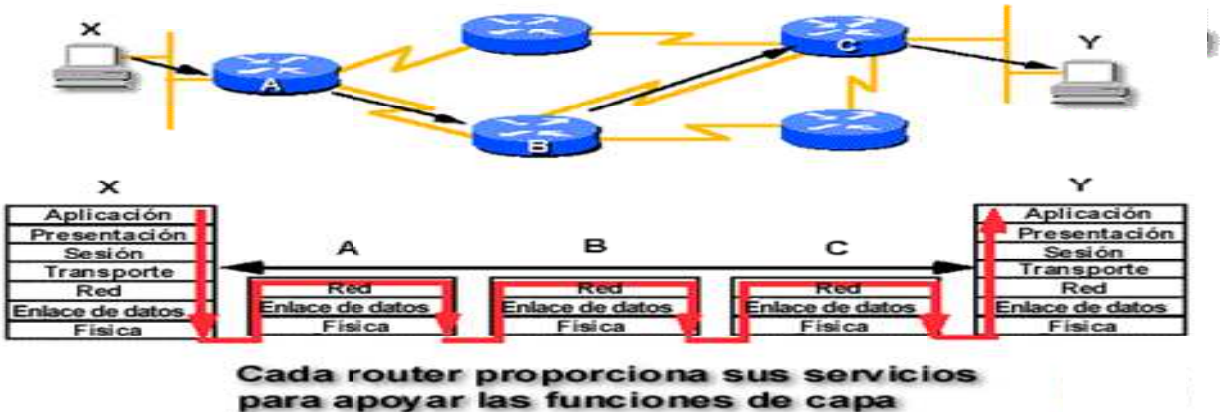
Red	Host
10.	8.2.48

(Máscara 255.0.0.0)

Ejemplo Novell IPX

Red	Nodo
1aceb0b.	0000.0c00.6e25

Protocolo enrutado versus protocolo de enrutamiento
Operaciones de protocolo de capa de red



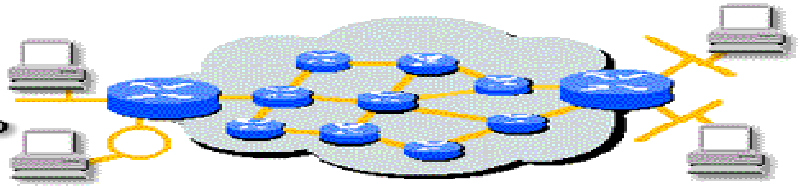
Cada router proporciona sus servicios para apoyar las funciones de capa

Los routers utilizan protocolos de enrutamiento para intercambiar tablas de enrutamiento y compartir información de enrutamiento. En otras palabras, los protocolos de enrutamiento son protocolos que determinan la forma en que se enrutan los protocolos enrutados.

Protocolo enrutado versus protocolo de enrutamiento

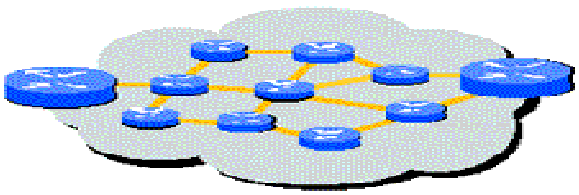
- Protocolo enrutado utilizado entre routers para dividir el tráfico del usuario

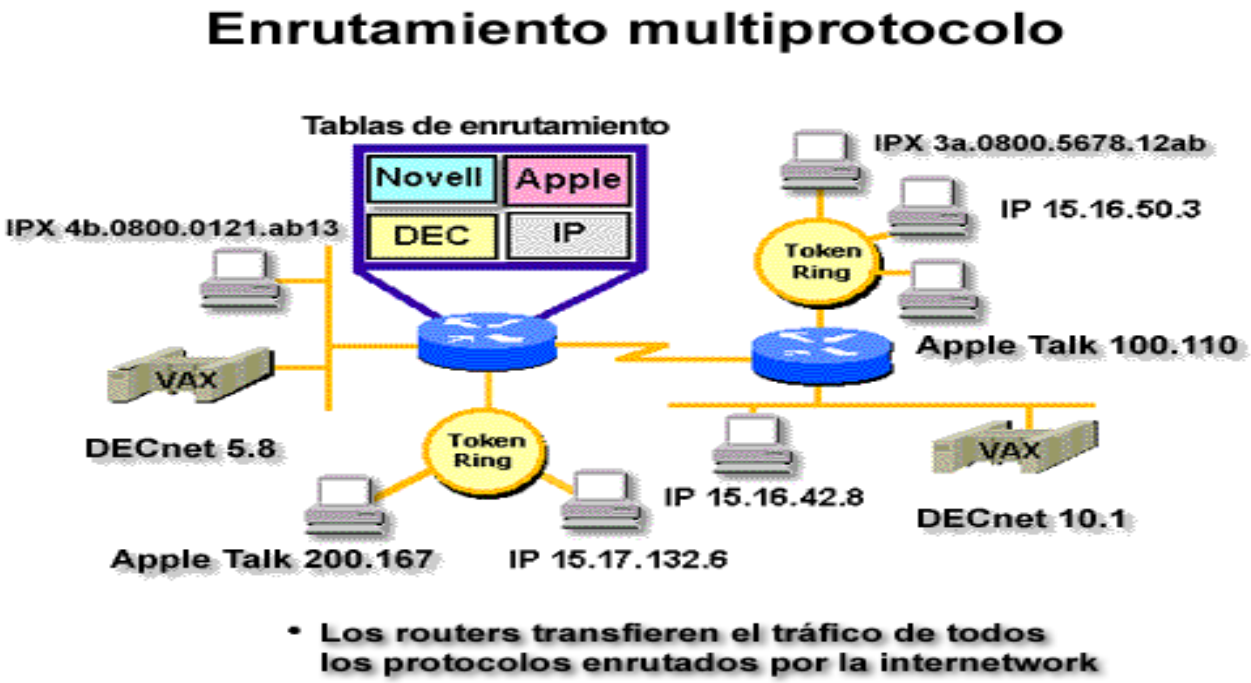
  Ejemplos: IP, IPX



- Protocolo de enrutamiento utilizado únicamente entre routers para mantener las tablas

  Ejemplos: RIP, IGRP, OSPF





Entre los ejemplos de protocolos de enrutamiento se pueden citar el *Protocolo de información de enrutamiento o RIP*[3], el *Protocolo de enrutamiento de Gateway interior o IGRP*[4], *el Protocolo de enrutamiento de Gateway interior mejorado o EIGRP*[5], y *Primero la ruta más corta o OSPF*[6]. Los protocolos de enrutamiento permiten que los routers dibujen internamente un mapa de toda la interconexión de redes a los fines del enrutamiento. Dichos mapas pasan a formar parte de la tabla de enrutamiento de cada router.

¿Cuál es la diferencia entre los IGP y los EGP? Dos tipos de protocolos de enrutamiento son los Protocolos de Gateway interior o IGP7s y los Protocolos de Gateway exterior o EGP8s.
RIP, IGRP, EIGRP, y OSPF son ejemplos de IGP. Los protocolos de gateway interior se utilizan para enrutar los datos dentro de un sistema autónomo, dentro de las redes que han sido divididas en subredes.

---

[3] **RIP** - *(Routing Information Protocol)*. Protocolo de la información de enrutamiento. IGP provisto con los sistemas UNIX BSD. El IGP más común de la Internet. RIP utiliza el número de saltos como métrica de enrutamiento.
[4] **IGRP** - *(Interior Gateway Routing Protocol)*. IGP desarrollado por Cisco para tratar los problemas relacionados con el enrutamiento en redes heterogéneas de gran magnitud.
[5] **IGRP mejorado** - *(Enhanced Interior Gateway Routing Protocol)*. Protocolo de enrutamiento de gateway interno mejorado. Versión avanzada de IGRP desarrollada por Cisco. Provee propiedades de convergencia superior y eficacia operativa, y combina las ventajas de los protocolos de estado de enlace con aquéllas de los protocolos por vector de distancia.
[6] **OSPF** - *(Open Shortest Path First)*.Primero la ruta libre más corta. Algoritmo de enrutamiento IGP jerárquico de estado de enlace propuesto como sucesor de RIP en la comunidad de Internet. Entre las características de OSPF se incluyen el enrutamiento de menor costo, el enrutamiento de múltiples rutas, y el equilibrio de la carga. OSPF surge a partir de una versión anterior del protocolo ISIS.
[7] **IGP** - *(Interior Gateway Protocol)*. Protocolo de internet que se utiliza para intercambiar información de enrutamiento dentro de un sistema autónomo. IGRP, OSPF, y RIP son ejemplos de IGPs de Internet comunes.
[8] **EGP** - *(Exterior Gateway Protocol)*. Protocolo de gateway exterior. Protocolo de Internet para intercambiar información de enrutamiento entre sistemas autónomos. Documentado en RFC 904. No debe confundirse con el término general *protocolo de gateway exterior*. EGP es un protocolo obsoleto que ha sido reemplazado por BGP.

Los protocolos de gateway exterior se utilizan para enrutar los datos entre distintos sistemas autónomos. Los EGP se utilizan para enrutar entre redes.

¿Qué es RIP y cómo funciona? Dentro de una red, el método más común que se utiliza para transferir información de enrutamiento entre los routers ubicados en la misma red es el RIP. Este protocolo de gateway interior calcula las distancias hasta el destino. El RIP permite que los routers que utilizan este protocolo actualicen sus propias tablas de enrutamiento a un intervalo programable, en general cada treinta segundos. Como el RIP conecta constantemente entre los routers vecinos puede provocar una acumulación del tráfico de la red.
El RIP permite que los routers determinen la ruta que se utilizará para enviar los datos en base a un concepto conocido como vector de distancia. Para explicarlo de manera más simple, cada vez que los datos deben pasar por un router y, en consecuencia a través de un nuevo número de red, se considera que equivale a un salto[9]. Una ruta que tiene un número de saltos[10] igual a cuatro indicaría que los datos que viajan por dicha ruta deberían pasar a través de cuatro routers antes de llegar a su destino final en la red.
Si existen múltiples rutas hacia un destino, cuando se utiliza el RIP el router elige la ruta con menor número de saltos. Como el número de saltos es la única métrica de enrutamiento que utiliza el RIP para determinar la mejor ruta, ésta no es necesariamente la mejor ruta para llegar a un destino.
Sin embargo, el RIP sigue siendo muy popular y su implementación está muy difundida. Esto se debe principalmente a que fue uno de los primeros protocolos de enrutamiento que se desarrolló. Otro problema que plantea el uso del RIP es que un destino puede estar ubicado muy alejado como para ser alcanzado. Con el RIP, el número de saltos máximo al cual pueden enviarse los datos es de quince. A causa de esto, si la red de destino está a más de quince routers de distancia, se la considera inalcanzable.

¿Qué son el IGRP y el EIGRP? IGRP y EIGRP son protocolos de enrutamiento desarrollados por Cisco. Por lo tanto, se los puede considerar protocolos de enrutamiento patentados. El IGRP se desarrolló específicamente para abordar los problemas relacionados con el enrutamiento en grandes redes de varios proveedores que planteaban problemas que escapaban al alcance de otros protocolos, por ejemplo el protocolo RIP. Al igual que el protocolo RIP, el IGRP es un protocolo por vector de distancia, sin embargo, tiene en cuenta aspectos tales como el ancho de banda, la carga, la demora y la confiabilidad para determinar la mejor ruta. El EIGRP es una versión avanzada del IGRP. Específicamente, el protocolo EIGRP tiene una eficiencia operativa superior y combina las ventajas de los protocolos de estado de enlace[11] con las de los protocolos por vector de distancia[12].

---

[9] **Salto** - Término que describe el paso de un paquete de datos entre dos nodos de red (por ejemplo, entre dos routers).
[10] **Número de saltos** - Métrica de enrutamiento utilizada para medir la distancia entre un origen y un destino. RIP utiliza el número de saltos como su única métrica.
[11] **Algoritmo de enrutamiento del estado de enlace** - Algoritmo de enrutamiento en el cual cada router realiza un broadcast o multicast de información referente al costo de hacer llegar a cada uno de sus vecinos a todos los nodos de la internetwork. Los algoritmos de estado de enlace crean una vista consistente de la red y por lo tanto no son propensos a bucles de enrutamiento, pero logran esto al costo de dificultades computacionales relativamente mayores y un tráfico más diseminado (comparado con los algoritmos de enrutamiento por vector de distancia).
[12] **Algoritmo de enrutamiento por vector de distancia** - Clase de algoritmos de enrutamiento que iteran sobre el número de saltos en una ruta para encontrar un spanning-tree del camino más corto. Los algoritmos de enrutamiento por vector de distancia piden a cada router que envíe su tabla de enrutamiento total en cada actualización, pero solamente a sus vecinos. Los algoritmos de enrutamiento por vector de distancia pueden ser propensos a los bucles de enrutamiento, pero son computacionalmente más simples que los algoritmos de enrutamiento del estado de enlace. También denominados *algoritmo de enrutamiento Bellman-Ford*.

¿Qué es el OSPF? Aunque OSPF significa *abrir primero la ruta más corta*, una mejor descripción de este acrónimo sería la determinación de la ruta óptima ya que este protocolo de gateway interior en realidad utiliza varios criterios para determinar la mejor ruta hacia un destino. Entre estos criterios se incluyen las métricas de costo que influyen en factores tales como velocidad de la ruta, tráfico, confiabilidad y seguridad

¿Cómo conocen los routers las redes? Básicamente, existen dos formas en las que los routers pueden conocer la información de la ruta. Se denominan enrutamiento estático y dinámico. Los datos manuales que se colocan en una tabla de enrutamiento son ejemplos de enrutamiento estático. Cuando las rutas se aprenden automáticamente se lo denomina enrutamiento dinámico.

Cuáles son algunos ejemplos de cuándo se utilizaría el enrutamiento estático? Si los routers pueden conocer la información de enrutamiento en forma automática, parecería inútil ingresar información manualmente en las tablas de enrutamiento de un router. Sin embargo, dichos datos manuales de las tablas de enrutamiento pueden ser útiles en cualquier momento en que el administrador de una red desee controlar la ruta que elegirá un router.
Por ejemplo, las tablas de enrutamiento basadas en información estática podrían utilizarse para probar un enlace en particular de la red o para conservar el ancho de banda de área amplia. El enrutamiento estático[13] es también el método que se prefiere para mantener las tablas de enrutamiento cada vez que hay una única ruta hacia un destino, como sucedería en el caso de una red de conexión única[14.] Esto se debe a que en las redes de conexión única la mejor ruta es la única ruta.

¿Cuál es un ejemplo de cuándo se utilizaría el enrutamiento dinámico? El enrutamiento adaptable o enrutamiento dinámico[15] se produce cuando los routers se envían entre sí mensajes periódicos de actualización de enrutamiento. Cada vez que se recibe un mensaje de este tipo con nueva información, el router vuelve a calcular la mejor ruta y envía la nueva información de actualización a los otros routers. Mediante el enrutamiento dinámico los routers pueden adaptarse a las cambiantes condiciones de la red.
Antes del advenimiento de la actualización dinámica de las tablas de enrutamiento, los proveedores debían mantener las tablas de enrutamiento de sus clientes. Esto significaba que los proveedores debían ingresar manualmente los números de red, las distancias asociadas, y los números de puerto en las tablas del router de todos los equipos que vendían o alquilaban a sus clientes. A medida que las redes fueron creciendo, esta tarea era cada vez más pesada e implicaba una gran pérdida de tiempo, sin mencionar los costos. El enrutamiento dinámico elimina la necesidad de que los administradores o proveedores de redes ingresen manualmente la información en las tablas de enrutamiento. Se las utiliza mejor cuando el ancho de banda y la gran cantidad de tráfico de la red no son temas preocupantes. RIP, IGRP, EIGRP, y OSPF son ejemplos de protocolo de enrutamiento dinámico ya que permiten que se realice este proceso.

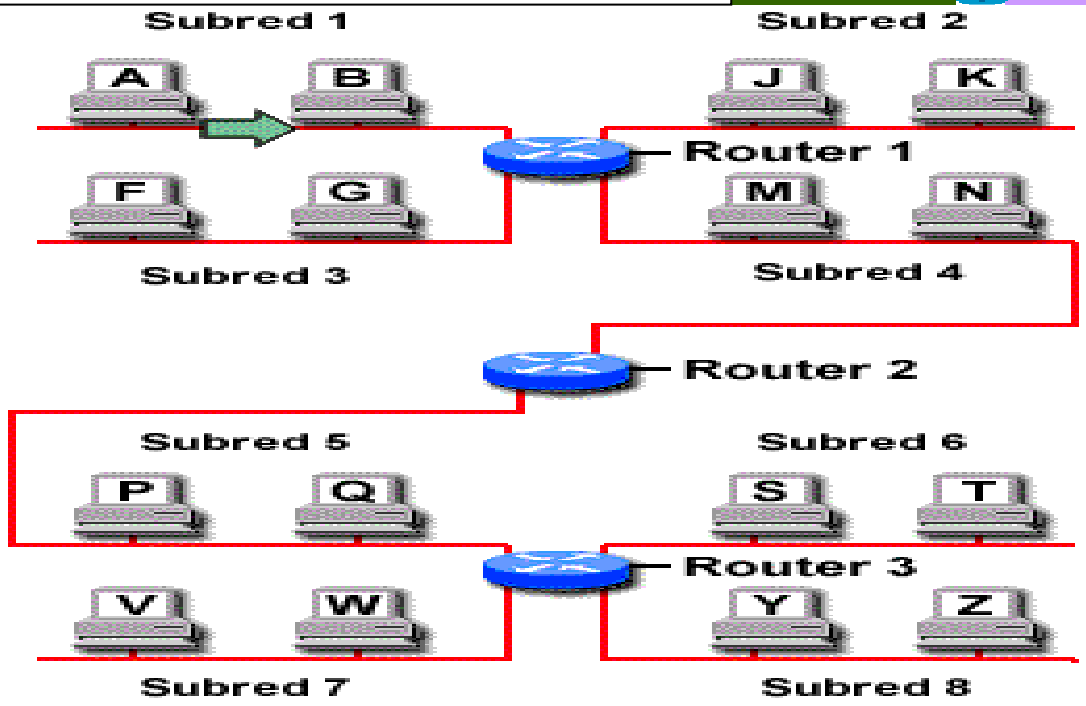
¿Cómo utilizan los routers los protocolos de enrutamiento del tipo RIP para enrutar los datos a través de las redes? Sea una red clase "B" dividida en ocho subredes conectadas por tres routers.

---

[13] **Ruta estática** - Ruta explícitamente configurada e ingresada en la tabla de enrutamiento. Las rutas estáticas tienen prioridad sobre las rutas elegidas por los protocolos de enrutamiento dinámico.

[14] **Red de conexión única** - Red que tiene una única conexión a un router.

[15] **Enrutamiento dinámico** - Enrutamiento que se ajusta automáticamente a la topología de la red o a los cambios de tráfico. También denominado *enrutamiento adaptable*.



El host A tiene los datos que desea enviar al host Z. A medida que los datos bajan en el modelo OSI de la capa de aplicación a la capa de enlace de datos, el host A encapsula los datos con la información provista por cada capa. Cuando los datos llegan a la capa de red, el origen A utiliza su propia dirección IP y la dirección IP de destino del host Z porque ahí es donde quiere enviar los datos. Luego el host A pasa los datos a la capa de enlace de datos.

En la capa de enlace de datos, el origen A coloca la dirección MAC de destino del router al cual está conectado y su propia dirección MAC en el encabezado MAC. El origen A hace esto porque ve a la subred 8 como una red separada. Sabe que no puede enviar los datos directamente a una red diferente sino que debe pasar los datos a través de un gateway por defecto. En este ejemplo, el gateway por defecto para el origen A es el router 1.

El paquete de datos viaja a través de la red 1. Es examinado por todos los hosts por los cuales pasa pero éstos no lo copian cuando ven que la dirección MAC de destino no coincide con la propia. El paquete de datos continúa por la subred 1 hasta que llega al router 1. Al igual que los otros dispositivos de la subred 1, el router 1 ve el paquete de datos. Sin embargo, esta vez el router toma el paquete de datos porque reconoce que su propia dirección MAC es la misma que la dirección MAC de destino. El router 1 separa el encabezado MAC de los datos y pasa los datos hacia la capa de red donde mira la dirección IP de destino que lleva el encabezado IP. Luego el router busca en sus tablas de enrutamiento. Mapea la dirección de red de la dirección de destino a la dirección MAC del router conectado a la subred 8. Como el router está utilizando el RIP como protocolo de enrutamiento, determina que la mejor ruta para enviar los datos es la que coloca el destino a una distancia de tres saltos. A continuación el router determina que el paquete de datos debe ser enviado a través de su puerto conectado a la subred 4 para que se lo pueda enrutar hacia el destino a través de la ruta seleccionada. El router pasa los datos a la capa de enlace de datos donde coloca un nuevo encabezado MAC en el paquete de datos. El nuevo encabezado MAC contiene la dirección MAC de destino del router 2 y la dirección MAC del primer router que se convirtió en el nuevo origen. El encabezado IP no se modifica. Luego el primer router pasa el paquete de datos a través del puerto que seleccionó hacia la subred 4. Los datos pasan a través de la subred 4. Allí los datos son examinados por todos los hosts por los cuales pasan pero no se copian en los mismos hasta que éstos vean que la dirección MAC de destino coincide con la propia. El paquete de datos continúa pasando por la subred 4 hasta llegar al router 2. Al igual que los otros dispositivos de la subred 4, el segundo router ve el paquete de datos.

Sin embargo, esta vez el router toma el paquete de datos ya que reconoce que su propia dirección MAC coincide con la dirección MAC de destino. En la capa de enlace de datos, el router separa el encabezado MAC. Luego pasa los datos hacia la capa de red. Ahí examina la dirección IP de la red de destino. Mira su tabla de enrutamiento. Como el router utiliza el RIP como protocolo de enrutamiento, determina que la mejor ruta a través la cual se pueden enviar los datos es la que coloca el destino a una distancia de dos saltos. A continuación el router determina que el paquete de datos debe enviarse a través de su puerto que está conectado a la subred 5 para su enrutamiento hacia el destino a través de la ruta seleccionada. El router pasa los datos a la capa de enlace de datos donde coloca un nuevo encabezado MAC en el paquete de datos. El nuevo encabezado MAC contiene la dirección MAC de destino del router 3 y la dirección MAC del router 2 como origen. El encabezado IP no sufre modificaciones. Luego, el primer router pasa el paquete de datos a través del puerto seleccionado hacia la subred 5. Los datos pasan por la subred 5. Allí son examinados por todos los host por los cuales atraviesa pero no se copian hasta tanto éstos vean que la dirección MAC de destino coincide con su propia dirección. El paquete de datos continúa su paso por la subred 5 hasta llegar al router 3. Al igual que los otros dispositivos de la subred 5, el router 3 ve el paquete de datos. Sin embargo, esta vez el router toma el paquete de datos ya que reconoce que su propia dirección MAC coincide con la dirección MAC de destino. En la capa de enlace de datos el router separa el encabezado MAC. Luego pasa los datos a la capa de red. Ahí ve si la dirección IP de destino coincide con la de un host ubicado en una de las subredes a la cual está conectado. Determina que necesita enviar los datos a través de su puerto conectado a la subred 8 para llegar a la dirección IP de destino. Coloca un nuevo encabezado MAC en los datos. Esta vez el encabezado MAC contiene la dirección MAC de destino del host Z del router 3 como origen. Como antes, el encabezado IP no sufre modificaciones. El tercer router envía los datos a través del puerto conectado a la subred 8. El paquete de datos viaja por la subred 8. Allí los datos son examinados por todos los hosts por los cuales atraviesa pero éstos no lo copian porque ven que la dirección MAC de destino no coincide con la propia. Finalmente, los datos llegan al host Z. El host Z toma los datos porque ve que su dirección MAC coincide con la dirección MAC de destino que lleva el encabezado MAC del paquete de datos El host separa el encabezado MAC y pasa el paquete de datos a la capa de red. En la capa de red, el host Z ve que su dirección IP y la dirección IP de destino que lleva el encabezado IP coinciden. El host Z separa el encabezado IP y pasa los datos a la capa de transporte del modelo OSI. El host Z continúa separando las cápsulas que encapsulan el paquete de datos y pasando los datos a la siguiente capa del modelo OSI. Esto se continúa hasta que los datos finalmente llegan a la capa superior, la capa de aplicación del modelo OSI.