1) Tarjeta de Interfaz de red (Dirección física o MAC):

La capa física del modelo OSI contiene las descripciones normalizadas de los medios de transmisión o medios de internetworking por los cuales pasan las señales de datos transmitidas (medios alámbricos o inalámbricos). La cantidad y velocidad de transmisión de los datos dependerán de la naturaleza de ese medio. La capa física contempla los mecanismos de codificación de los datos, y también las herramientas para la transmisión de esos paquetes (características eléctricas, mecánicas, funcionales y de procedimiento).
La capa de enlace de datos o capa dos del modelo OSI, facilita el acceso al medio, brindando un tránsito confiable de datos a través de un enlace físico.
Esta capa se corresponde con el direccionamiento físico, la topología de la red, la disciplina de línea, notificación y recuperación de errores, entrega ordenada de frames y control de flujo. La IEEE dividió en sus estándares para redes LAN a ésta capa en dos sub-capas: la subcapa MAC y la subcapa LLC.

¿Cómo direccionar los dispositivos dentro de una red?
Cada dispositivo tiene una forma única de identificarse que es la "dirección física" o "dirección de hardware" ó "dirección MAC" (Medium access conection), dirección estandarizada en la capa de enlace de datos, necesaria para cada puerto o dispositivo conectado a una LAN. (Puerto: interfaz en un dispositivo de internetworking, tal como un router). Otros dispositivos en la red utilizan estas direcciones para localizar puertos específicos en la red, y para crear y actualizar tablas de enrutamiento y estructuras de datos. Las direcciones MAC son controladas por la IEEE, y tienen una longitud de 6 bytes, escritas en sistema hexadecimal, en uno u otro de los dos formatos usuales:
Ej.: 0000.0c12.3456 ó 00-00-0c-12-34-56

¿Dónde residen las direcciones MAC?
Las direcciones MAC se graban en forma permanente en un chip de la "tarjeta de interfaz de red" ó NIC (network interface card), por el fabricante de los chips (fiscaliza la IEEE).
La NIC provee a un dispositivo comunicación hacia y desde la red.
Desde el punto de vista del modelo OSI, la tarjeta NIC está ubicada en la **capa de enlace de datos (capa 2**) por ser donde se conectan los medios de transmisión, es decir que está contigua a la capa física. Esta dirección MAC es única para cada NIC, por lo tanto si a una máquina se le cambia su NIC, cambia su dirección MAC ("dirección física").

¿Cómo se transmiten datos a una dirección destino dentro de una red?
En una red Ethernet, cuando un dispositivo envía datos, abre una ruta de comunicación utilizando su dirección MAC. El origen envía los datos a la dirección MAC de destino (encapsulado de la frame –trama-). A medida que éstos viajan por los medios de red, la tarjeta NIC de cada dispositivo verifica si su dirección coincide con la del paquete. Si no es así, ignora el paquete de datos, y éste sigue por la red a la estación siguiente. Cuando concuerdan las direcciones MAC del paquete y del dispositivo destino, la tarjeta NIC hace una copia del paquete y la coloca en la capa de enlace de la computadora donde reside. El paquete original continúa a través de la red para ver si existe otra coincidencia. (Difusión: todas las estaciones de la red "ven" el frame)
Por un cable, sólo puede viajar un paquete de datos a la vez, lo que hace que éste esquema funcione bien en redes relativamente pequeñas (Sino, las colisiones provocan la caída dramática del rendimiento).

2) Dispositivos de Internetworking:

Los dispositivos de internetworking son productos que se utilizan para conectar redes. Al mismo ritmo que las redes de computadoras crecen en tamaño y en complejidad, crecen los dispositivos de internetworking que se emplean para conectarlas. Sin embargo, independientemente del tipo de dispositivo de internetworking empleado, todas comparten uno o más propósitos en común:

- Permiten conectar un número mayor de nodos a la red.
- Alargan la distancia sobre la cual puede extenderse una red.
- Localizan el tráfico de la red.
- Pueden fusionar redes existentes.
- Pueden aislar problemas de red de modo que sea más fácil su diagnóstico

Los dispositivos LAN incluyen bridges, hubs, switches Ethernet, routers, y switches ATM.

Ilustración 1: Redes y dispositivos de área local

Ilustración 2: Redes y dispositivos de área amplia

2.1) Repetidores (HUBS):

Dispositivos que regeneran y propagan señales eléctricas entre dos segmentos de la red.
En internetworking, dos de los problemas más comunes que existen es que hay demasiados nodos o que no hay cable suficiente. Un repetidor puede brindar una solución simple si existe alguno de estos dos problemas.
Para comprender cómo funciona un repetidor, es importante comprender primero que a medida que los datos salen del origen y viajan por la red se transforman en impulsos eléctricos o bien en impulsos luminosos que pasan por los medios de networking. Estos impulsos se denominan señales. Cuando las

señales salen por primera vez de una estación transmisora, están limpias y son claramente reconocibles. Sin embargo, cuanto mayor es la extensión del cable más se debilitan y deterioran las señales a medida que atraviesan los medios de networking. Por ejemplo, las especificaciones para un cable Ethernet de par trenzado categoría 5 establecen que la distancia máxima que las señales pueden recorrer por la red es de 100 metros. Si una señal recorre una distancia mayor, no hay garantías de que la tarjeta NIC pueda leerla.

Para que las señales no sean irreconocibles para los dispositivos que las reciben en la red, los repetidores toman las señales debilitadas, las limpian, las amplifican y las envían para que continúen su camino por la red. Utilizando repetidores, se extiende la distancia sobre la cual puede operar una red. Al igual que los medios de networking, **los repetidores están en la capa física, capa 1, del modelo OSI.** Existe un proceso similar cuando hay demasiados dispositivos conectados a una red. Cada dispositivo conectado a los medios de red produce una leve degradación de la señal. Si una señal debe atravesar demasiadas estaciones o nodos, puede debilitarse al extremo de llegar a ser irreconocible para los dispositivos que la reciben. Como en el caso antes descripto, los repetidores toman las señales debilitadas, las limpian, las amplifican y las envían nuevamente para que continúen su camino por la red. Utilizando repetidores de esta manera se pueden conectar un número mayor de nodos a la red. Los repetidores multipuerto se denominan comúnmente hubs o en Ethernet, concentradores. Los hubs son dispositivos de internetworking muy comunes. En términos generales, el término hub se utiliza en lugar de repetidor para referirse al dispositivo que sirve como centro de una red de topología en estrella.

No es un dispositivo “inteligente”. (Retransmite los datos recibidos por un puerto, indiscriminadamente por todos sus otros puertos)

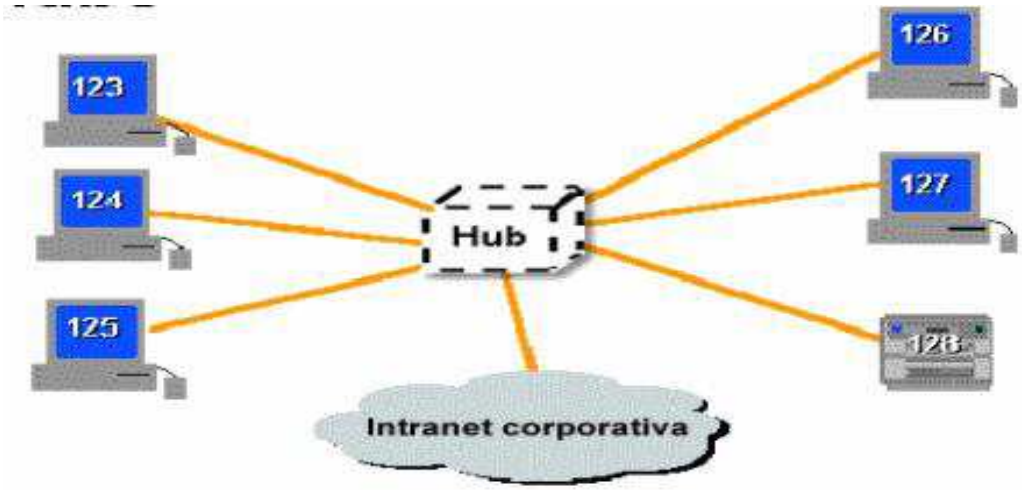

Ilustración 3: Hubs

En resumen:

- Operan en la capa física del modelo OSI.
- Aumentan el número potencial de nodos de la red, y la extensión de la misma.
- Amplifican y resincronizan las señales eléctricas que llegan a un puerto del Hub, retransmitiéndolas por todos los otros puertos del repetidor.
- Propagan los datos por todos los otros segmentos de la LAN, deban llegar ahí o no. NO determinan o conmutan rutas, ya que no siendo dispositivos inteligentes, NO pueden filtrar (decidir si envían o no tráfico de red según ciertas características, por ejemplo dirección origen, dirección destino, tipo de protocolo, etc.)
- Se utilizan como puntos de concentración de la red.

Si el tráfico por la red es intenso, aparecen problemas serios:
Habiendo un solo cable y diferentes segmentos conectados por dispositivos que no filtran (repetidores), dan lugar a que más de un usuario intente enviar datos a través de la red al mismo tiempo.
En Ethernet (protocolo CSMA/CD): si más de un nodo intenta transmitir al mismo tiempo, se produce una **colisión**, impactándose los datos y dañándose los mismos. Ésta área de red donde las frames se dañaron se denomina **dominio de colisión**.
La tarjeta NIC emite una postergación. Como las tarjetas NIC se basan en un algoritmo, el retraso es diferente en cada dispositivo, minimizando así la posibilidad de otra colisión.
Si el tráfico es intenso, la reiteración de colisiones (que son propagadas por los Hubs a todos los segmentos) origina permanentes postergaciones, por lo que el tráfico se hace lento y la red ineficiente.

2.2) "Bridges" (Puentes):

Una forma de solucionar el problema del exceso de tráfico en una red y del exceso de colisiones es el uso de un dispositivo de internetworking llamado bridge

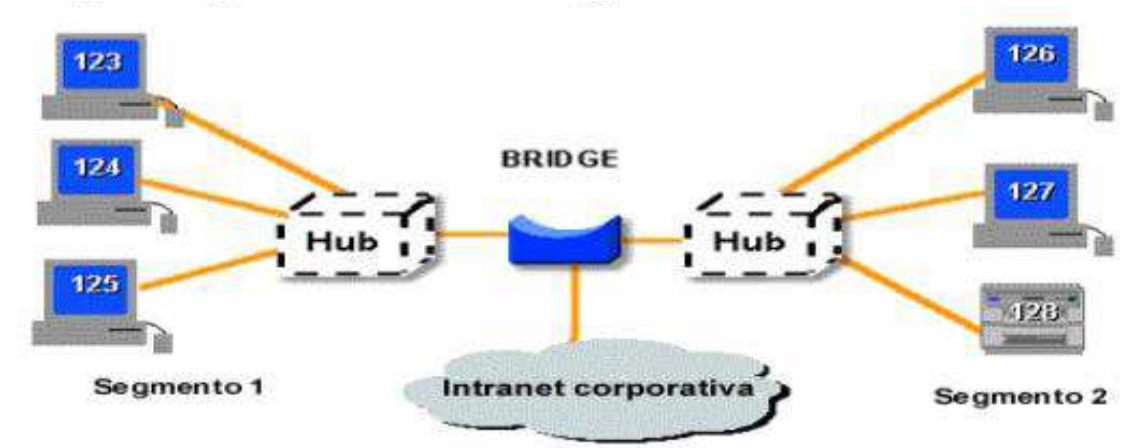

Ilustración 4: Ejemplo de un bridge

Un bridge es un dispositivo de internetworking que conecta y pasa paquetes entre dos segmentos de red que utilicen el mismo protocolo de comunicaciones.
Un bridge elimina el tráfico innecesario y minimiza las posibilidades de que se produzcan colisiones en la red dividiéndola en segmentos y filtrando el tráfico en base a la estación o a la dirección MAC.
Los bridges sólo se encargan de pasar paquetes o de no pasar paquetes según su dirección MAC de destino. De hecho, los bridges a menudo pasan paquetes entre redes que operan bajo diferentes protocolos de capa 2.
Por el hecho de filtrar o no información, teniendo en cuenta el direccionamiento MAC, los bridges son dispositivos de internetworking más "inteligentes" que los hubs.
Como los bridges **operan en la capa de enlace de datos**, capa 2, no requieren examinar la información de la capa superior. Los bridges filtran el tráfico de la red mirando solamente la dirección MAC. Los bridges no se preocupan por los protocolos. De hecho es común que un bridge mueva protocolos y demás tráfico entre dos o más redes. Debido a que los bridges miran sólo las direcciones MAC pueden enviar rápidamente el tráfico que represente cualquier protocolo de capa de red.
Para filtrar o entregar selectivamente el tráfico de una red, los bridges construyen tablas con todas las direcciones MAC de una red y de otras redes y hacen un mapeo con ellas. Si pasan datos a través de los medios de la red, un bridge compara la dirección MAC destino que llevan los datos con las direcciones MAC que contienen sus tablas. Si el bridge determina que la dirección MAC de destino de los datos proviene del mismo segmento de red que el origen, no envía los datos a otros segmentos de la red. Si el bridge determina que la dirección MAC de destino de los datos no es del mismo segmento de

red que el origen, envía los datos a todos los otros segmentos de la red. De este modo, los bridges pueden reducir significativamente el tráfico entre los segmentos de la red eliminando el tráfico innecesario.

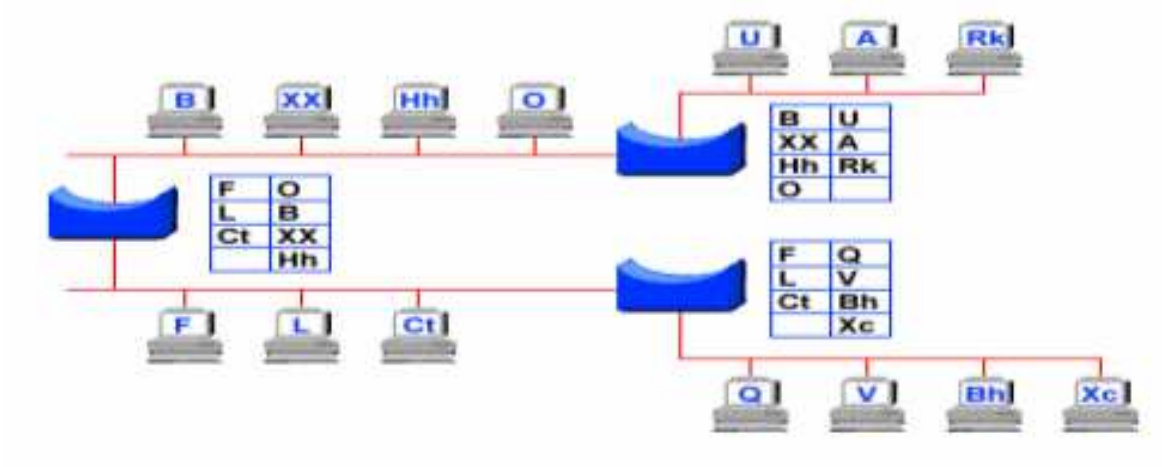

Ilustración 5: Segmentación utilizando bridges

En el ejemplo de la Ilustración 5, si la máquina V envía datos a la máquina Xc, el frame inunda el segmento al que pertenece V, al mismo tiempo que el correspondiente bridge verifica en sus tablas que ambas estaciones están en el mismo segmento, por lo que no propaga el frame hacia los demás segmentos.
En cambio, si la máquina V envía datos a la máquina A, los bridges irán propagando el frame hasta que alcance el segmento de red destino.
Aunque los bridges utilizan tablas para determinar si enviar o no los datos a otros segmentos de la red, los tipos de comparaciones y decisiones que toman son de un nivel relativamente bajo y de carácter simple. Si bien los bridges pueden determinar si una dirección MAC de destino que transportan los datos no forma parte del mismo segmento de red que su origen, no determinan respecto del segmento de red al cual deberían ser enviados los datos. Los bridges indiscriminadamente pasan los datos a todos los otros segmentos de la red. Obviamente, en grandes redes o en redes compuestas por varios segmentos dicho envío indiscriminado de tráfico de la red no puede ser eficiente o rápido. Eventualmente, los datos llegarían a su destino pero después de un viaje prolongado y largo.

¿Qué tipos de problemas de tráfico de red es incapaz de resolver un bridge?
Los bridges trabajan mejor cuando el tráfico desde un segmento de la red a otro segmento no es demasiado grande. Sin embargo, cuando el tráfico entre los segmentos de la red es muy pesado, el bridge puede convertirse en un cuello de botella y hacer la comunicación más lenta.
Existe otro problema potencial cuando se utilizan bridges. Los bridges siempre extienden y multiplican un tipo especial de paquete de datos. Estos paquetes de datos se producen cuando un dispositivo de una red quiere llegar a otro dispositivo de la red pero no conoce la dirección de destino. Cuando esto sucede, con frecuencia el origen envía lo que se llama **broadcast**. (Broadcast: paquete de datos que se enviará a todos los nodos de una red. Los broadcast se identifican por medio de direcciones de broadcast)
Como su nombre lo indica, el broadcast se envía a todos los dispositivos de la red. Como todos los dispositivos de la red deben prestar atención a dichos broadcasts, los bridges siempre los envían a todos y a cada uno de los segmentos conectados. Si demasiadas estaciones envían broadcasts a través de la red, tratando de determinar la dirección desconocida de un cierto dispositivo con el cual se desean comunicar, en tales casos puede producirse una **tormenta de broadcast** (Tormenta de broadcast: Evento de red indeseable, en el cual se envían simultáneamente muchos broadcast a través de todos los segmentos de la red. Una tormenta de broadcast utiliza un ancho de banda sustancial de la red y, típicamente, produce una condición de tiempo vencido –time out-)

Si se produce una tormenta de broadcast, esta puede producir tiempos vencidos en la red. En dichos casos, el tráfico de la red se hace más lento y la red funciona con un desempeño que no llega a ser el óptimo.
Para comprender cómo se han resuelto estos problemas mediante el uso de **routers**, deberemos entender primero los esquemas de direccionamiento que se utilizan en networking.

2.3) "Routers" (Enrutadores)

2.3.1) Esquemas de direccionamiento:

En direccionamiento de redes, se utilizan dos niveles:

- Direcciones MAC, que ya han sido descriptas.
- Direcciones IP, basadas en un protocolo de internet.

Toda LAN debe tener su propia y única dirección IP. Una dirección IP es esencial para que se realice el internetworking a través de una WAN. Una dirección IP es una dirección de 32 bits asignada a los hosts que utilizan TCP/IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D, o E) y se escribe en forma de 4 octetos separados con puntos (formato decimal con punto). Cada dirección consiste en un número de red, un número opcional de subred, y un número de host. Los números de red y de subred se utilizan conjuntamente para el enrutamiento, mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Para extraer la información de la red y de la subred de la dirección IP se utiliza una máscara de subred. También denominada ***dirección de Internet***.

¿En qué se diferencian las direcciones IP de las direcciones MAC? Al igual que las direcciones MAC, cada dirección IP es única. No existe la posibilidad de que dos direcciones IP sean iguales. Sin embargo, mientras las direcciones MAC son direcciones físicas que tienen una codificación rígida en la tarjeta NIC y pueden ocurrir en la capa de enlace de datos, las direcciones IP se implementan en el software y ocurren en la **capa de red del modelo OSI**. En general es el administrador de la red el responsable de asignar las direcciones IP a todos los dispositivos de la red que controla.
Como Ud. recordará, las direcciones MAC son tres números hexadecimales de cuatro dígitos. Un ejemplo de dirección MAC es el número 0000.0c12.3456. Al igual que el número de Documento Nacional de Identidad, las direcciones MAC son ejemplos de esquema de direccionamiento plano. Son únicos. Se emiten en forma secuencial. Para organizarlos no se utiliza ninguna jerarquía.
Los esquemas de direccionamiento IP son más complejos que los esquemas de direccionamiento MAC. Las direcciones IP utilizan un esquema de direccionamiento jerárquico. Este esquema es como el que utiliza el sistema telefónico nacional, con códigos de país, de área e intercambios locales.
Como se indicó anteriormente, las direcciones MAC identifican dispositivos específicos y son utilizadas por los bridges para emitir direcciones simples de bajo nivel para los datos que viajan por la red. Por el contrario, las direcciones IP, brindan un esquema de direccionamiento que no sólo contiene la dirección del dispositivo en sí sino también la red en la cual está ubicado el dispositivo. Como este es el caso, si un dispositivo pasa de una red a una red diferente, la dirección IP del dispositivo deberá ser modificada en función del cambio realizado.

Comparando las direcciones MAC e IP:

IP	MAC
• Es única • Se implementa en el software • Se ubica en la capa de red del modelo OSI • El administrador de red es el responsable de asignar las direcciones IP a todos los dispositivos de la red. • Son binarias • Son complejas • Esquema de direccionamiento jerárquico • El esquema de direccionamiento contiene la dirección del dispositivo, y la red en la cual está ubicado ese dispositivo. • Si el dispositivo cambia de red, la dirección IP será modificada.	• Es única • Dirección física, que tiene una codificación rígida en la tarjeta NIC. • Se ubica en la capa de enlace de datos del modelo OSI. • Son hexadecimales • Esquema de direccionamiento no jerárquico. • Identifican a un dispositivo específico. Son utilizadas por los bridges para tomar decisiones de bajo nivel para los datos que viajan por la red. • Si se reemplaza la tarjeta NIC, la dirección MAC cambiará.

2.3.2) “Routers” (Enrutadores) (“Gateways”):

Los routers son otro tipo de dispositivo de internetworking. Estos dispositivos pasan paquetes de datos entre las redes en base a la información de la capa de protocolo de red o capa 3. Los routers tienen la capacidad de tomar decisiones inteligentes respecto de cuál es la mejor ruta para entregar los datos a través de la red

Ilustración 6: Direccionamiento en capa 3.

Ilustración 7: Direccionamiento - red y nodo.

Los routers constituyen la mejor solución al excesivo tráfico de broadcast, porque no envían frames de broadcast a menos que específicamente se les indique.

¿En qué se diferencian los routers de los bridges?

Los routers se diferencian de los bridges en diversos aspectos. En primer término, el bridging se produce en la capa de enlace de datos o capa 2 mientras que el enrutamiento se produce en la capa de red o capa 3 del modelo OSI.

En segundo lugar, los bridges utilizan direcciones físicas o MAC para tomar decisiones sobre el envío de datos. Los routers utilizan un esquema de direccionamiento diferente que se produce en la capa tres para adoptar las medidas relativas al envío. Utilizan direcciones IP direcciones lógicas en lugar de direcciones MAC. Como las direcciones IP se implementan en el software y se refieren a la red en la cual está ubicado un dispositivo, a menudo estas direcciones de capa 3 se denominan direcciones de protocolo o direcciones de red. Las direcciones físicas o MAC normalmente son asignadas por el fabricante de la tarjeta NIC y tienen una codificación rígida dentro de la tarjeta NIC. Por el contrario, las direcciones IP normalmente son asignadas por el administrador de la red. Al asignar las direcciones IP, no es inusual que el administrador de una red agrupe dispositivos en el esquema de direccionamiento IP en función de su ubicación geográfica, el departamento o el piso que ocupan dentro de un edificio. Como están implementadas en el software, las direcciones IP son relativamente fáciles de cambiar.

Por último, los bridges se utilizan principalmente para conectar segmentos de una red. Los routers se utilizan para conectar diferentes redes y para acceder a la Internet mundial. Lo hacen brindando enrutamiento extremo a extremo

¿Cómo funcionan los routers?

Los routers se utilizan para conectar dos o más redes. Para que el enrutamiento sea exitoso, cada red debe tener un número de red único. Recuerde que este número de red único está incorporado en la dirección IP asignada a cada dispositivo conectado a la red .Así, si una red tuviera un número de red único A con cuatro dispositivos conectados a dicha red, la dirección IP de cada dispositivo sería A1, A2, A3, y A4. Como la interfaz donde el router se conecta con una red se considera parte de dicha red, la dirección IP del puerto donde el router se conecta con la red A debería ser A5.

Si otra red con un número de red único B y con cuatro dispositivos conectados también se conectara al mismo router en otra de sus interfaces, la dirección IP de cada dispositivo de esta red sería B1, B2, B3, y B4, y la dirección IP de la segunda interfaz del router sería B5.

Imagine que los datos se envían de una red a otra. La red de origen es la red A y la red de destino es la red B, y el router está conectado a las redes A, B, C, y D. Cuando los datos, denominados frame, que provienen de la red A llegan al router, el router realiza las siguientes funciones. Primero el router separa el encabezado de enlace de datos que lleva el frame. El encabezado de enlace de datos contiene las direcciones IP del origen y del destino de los datos.

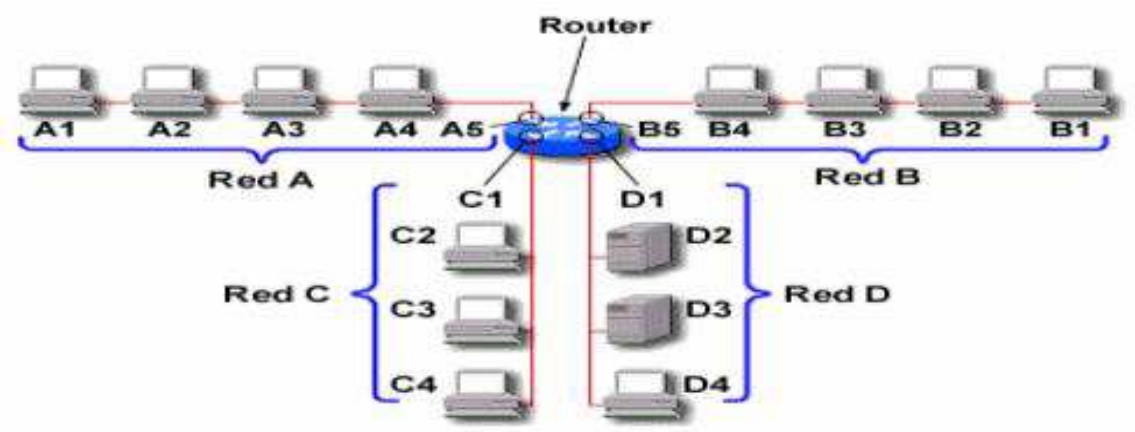

Ilustración 8: Ejemplo de encaminamiento mediante un Router

Esto permite que el router examine la capa de red para determinar la red de destino. Luego, el router consulta sus tablas de enrutamiento para determinar cuál de sus puertos necesitará para enviar los datos para que lleguen a su red de destino. De este modo, en el anterior ejemplo, el router determinaría enviar los datos de la red A a la red B a través de su puerto que tiene la dirección IP B5, encapsulando antes los datos en el correspondiente frame de enlace de datos.