REDES DE DATOS LAN

Introducción

Una red de área local (LAN) es una red de "alta" velocidad (decenas de Megabits), generalmente confinada a un mismo piso o edificio.

Los medios de transmisión que utiliza puede ser UTP, Coaxial o fibra óptica principalmente, esto hace posible obtener altas velocidades y baja tasa de errores.

Su utilización en redes empresariales se remonta a 15 a 20 años, lo que implica que hoy en día se considere una tecnología madura aunque están apareciendo nuevas tecnologías de redes LANs como ATM y Gigabit.

Su origen se debió a la necesidad que existía de asignar dinámicamente el ancho de banda entre un número variable de usuarios y aplicaciones, dado que los esquemas de asignación estáticos como TDM y FDM no son adecuados para este tipo de aplicaciones.

Las primeras experiencias con asignación dinámica de ancho de banda fueron desarrolladas con ALOHA, de donde se tomaron las bases para la más ampliamente difundida red de área local conocida como Ethernet o IEEE 802.3. Igualmente existen otros esquemas de redes de área local como alternativas a Ethernet que se han utilizado en ambientes industriales y empresariales.

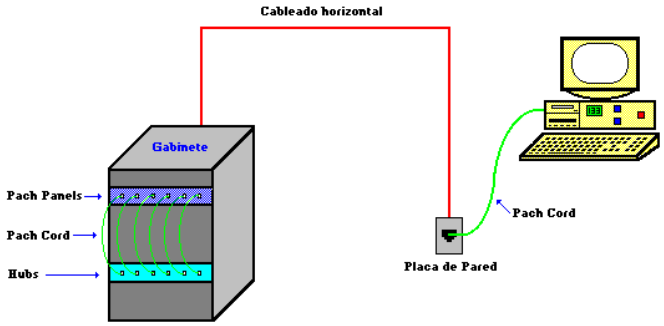
Introducción a las redes de datos

Una red de datos es un sistema que enlaza dos o más puntos (terminales) por un medio físico, el cual sirve para enviar o recibir un determinado flujo de información.

En su estructura básica una red de datos está integrada de diversas partes:
* En algunas veces de un armario o gabinete de telecomunicaciones donde se colocan de manera ordenada los Hubs, y Pach Panels.
* Los servidores en los cuales se encuentra y procesa la información disponible al usuario, es el administrador del sistema.
* Los Hubs, los cuales hacen la función de amplificador de señales, y a los cuales se encuentran conectados los nodos. Dicho enlace o columna vertebral del sistema se recomienda realizar en Fibra Optica o bien en cable UTP, del cual hablaremos más adelante.
* Los "Pach Panel's", los cuales son unos organizadores de cables.
* El "Pach Cord", el cual es un cable del tipo UTP solo que con mayor flexibilidad que el UTP corriente (el empleado en el cableado horizontal), el cual interconecta al "Pach Panel" con el "Hub", así como también a los tomas o placas de pared con cada una de las terminales (PC's).

Finalmente lo que se conoce como Cableado Horizontal en el cual suele utilizarse cable UTP, y enlaza el pach panel con cada una de las placas de pared.

Diagrama de una red de datos



Así pues, a la hora de diseñar el cableado estructurado de una red de datos, se deben de tener en consideración una amplia gama de aspectos tanto desde el punto de vista técnico como económico, dependiendo de los requerimientos del sistema, para lo cual existen diversos tipos de cables y categorías de los mismos, entre los cuales podemos citar los siguientes:
*SPT, *Coaxial, *UTP y ScTP, *Fibra Optica

ANCHO DE BANDA

El ancho de Banda es el rango de frecuencias que se transmiten por un medio. Se define como BW = Frecuencia Máxima - Frecuencia Mínima (aritmética). Por ejemplo en BW telefónico está entre 300Hz y 3400Hz, el BW de audio perceptible por el oído humano está entre 20Hz y 20000Hz, el canal 2 de televisión tiene un BW de 6 Mhz al igual que los otros y esta entre 54 Mhz y 60 Mhz. por lo general aunque no es lo mismo, cuando hablamos de ancho de banda queremos referirnos a la máxima velocidad que puedo transmitir. Lo correcto es hablar de esta máxima velocidad.

Un error que se comete siempre es confundir las unidades en que expresamos esta velocidad de transmisión de información. ¿Que será correcto MHz o Mbps ?. Ambos términos son usados para expresar una velocidad potencial de transmisión, pero difieren sustancialmente en lo que representan.

El Bit rate sólo expresa la cantidad de bit que se pueden transmitir por un canal y depende de la aplicación que se este utilizando así como de la codificación. La codificación es necesaria para una transmisión de datos confiable. Algunos sistemas de codificación permiten un bit rate más alto a pesar de las limitaciones del ancho de banda, de este modo se hace posible transmitir más rápido el dato sobre el mismo link.

El MegaHertz tiene una relación proporcional. Usando diferentes sistemas de codificación, diferentes bit rates pueden ser relacionados por el mismo número de ciclos por segundo (Hz).
Dependiendo del sistema e código usado, el flujo de bit se convierte en una señal con un ancho de banda definido. Una solución fast ethernet 100Mbps usando el sistema de codificación 5B6B (IEEE 802.13) requiere de un BW de 25Mhz. Cuando éste se combina con 4B5B se requiere un 25% más de BW 31.25 Mhz.

La conclusión importante sobre los anteriores conceptos, se resume en que es más adecuado expresar la velocidad en Megahertz, puesto que estamos hablando de la velocidad real del enlace, los bit rate dependerán de la codificación y aplicación especifica.

CATEGORÍAS

El concepto de categoría dentro de las normas EIA/TIA, se refiere a las diferentes velocidades que puede soportar el cableado estructurado en toda su extensión, es decir, cables y accesorios de conexión. Las categorías y sus velocidades son las siguientes:

CATEGORÍA	VELOCIDAD
3	16 MHz
4	20 MHz
5	100 MHz
5e	100 MHz

Decir que un cableado es categoría 5e equivale a decir que soporta una velocidad de 100 MHz, o sea que posee cables y accesorios que soportan 100 MHz y que cumple las especificaciones de instalación y recomendaciones para que se desempeñe óptimamente a esta velocidad.

NIVELES OSI ARQUITECTURA POR CAPAS

El modelo se presenta en siete capas, enumeradas desde la inferior (capa No 1 física) hasta la superior (No 7 Aplicación). A continuación la explicación de cada una de ellas

1 Físico	Este nivel define la forma de los cables, su tamaño, voltajes en los que operan, etc...
2 Enlace de datos	Aquí encontramos el estándar Ethernet, define el formato de las tramas, sus cabeceras, etc. A este nivel hablamos de direcciones MAC (Media Access Control) que son las que identifican a las tarjetas de red de forma única.
3 Red	En esta capa encontramos el protocolo IP. Esta capa es la encargada del enrutamiento y de dirigir los paquetes IP de una red a otra. Normalmente los “routers” se encuentran en esta capa. El protocolo ARP (Address Resolution Protocol) es el que utiliza para mapear direcciones IP a direcciones MAC.
4 Transporte	En esta capa encontramos 2 protocolos, el TCP (Transmission Control Protocol) y el UDP (User Datagram Protocol). Se encargan de dividir la información que envía el usuario en paquetes de tamaño aceptable por la capa inferior. La diferencia entre ambos es sencilla, el TCP esta orientado a conexión, es decir la conexión se establece y se libera, mientras dura una conexión hay un control de lo que se envía y por lo tanto se puede garantizar que los paquetes llegan y están ordenados. El UDP no hace nada de lo anterior, los paquetes se envían y punto, el protocolo se despreocupa si llegan en buen estado etc. El UDP se usa para enviar datos pequeños, rápidamente, mientras que el TCP añade una sobrecarga al tener que controlar los aspectos de la conexión pero “garantiza” la transmisión libre de errores.
5 Sesión	El protocolo de sesión define el formato de los datos que se envían mediante los protocolos de nivel inferior.
6 Presentación	External Data Representation (XDR), se trata de ordenar los datos de una forma estándar ya que por ejemplo los Macintosh no usan el mismo formato de datos que los PCs. Este estándar define pues una forma común para todos de tal forma que dos ordenadores de distinto tipo se entiendan.
7 Aplicación	Da servicio a los usuarios finales, Mail, FTP, Telnet, DNS, NIS, NFS son distintas aplicaciones que encontramos en esta capa.

TCP/IP, como la mayoría del software de red, está modelado en capas. Esta representación conduce al término *pila de protocolos*. Se puede usar para situar (pero *no* para comparar funcionalmente) TCP/IP con otras pilas, como SNA y OSI ("Open System Interconnection"). Las comparaciones funcionales no se pueden extraer con facilidad de estas estructuras, ya que hay diferencias básicas en los modelos de capas de cada una.

Los protocolos de Internet se modelan en cuatro capas:

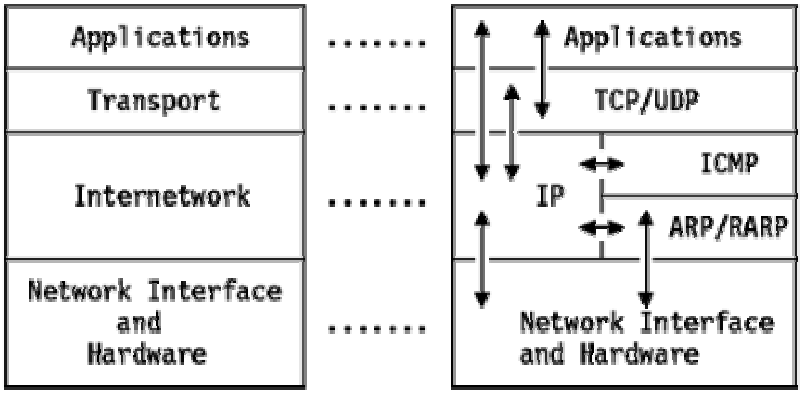


Figura: Modelo arquitectónico - Cada capa representa un "conjunto" de funciones.

Aplicación
: Es a un proceso de usuario que coopera con otro proceso en el mismo o en otro host. Ejemplos son TELNET (un protocolo para la conexión remota de terminales), FTP ("File Transfer Protocol") y SMTP ("Simple Mail Transfer Protocol").

Transporte
: Proporciona la transferencia de datos de entre los extremos. Ejemplo son TCP (*orientado a conexión*) y UDP (*no orientado a conexión*).

"Internetwork"
: También llamada *capa de red*, proporciona la imagen de "red virtual" de Internet (es decir, oculta a los niveles superiores la arquitectura de la red). IP ("Internet Protocol") es el protocolo más importante de esta capa. Es un protocolo *no orientado a conexión que no asume la fiabilidad de las capas inferiores.* No suministra fiabilidad, control de flujo o recuperación de errores. Estas funciones deben proporcionarlas una capa de mayor nivel, bien de transporte con TCP, o de aplicación, si se utiliza UDP como transporte. Una unidad de un mensaje en una red IP se denomina datagrama IP. Es la unidad básica de información transmitida en redes TCP/IP.

Network Interface
: O *capa de enlace* o *capa de enlace de datos*, constituye la interfaz con el hardware de red. Esta interfaz puede proporcionar o no entrega fiable, y puede estar orientada a flujo o a paquetes. De hecho, TCP/IP no especifica ningún protocolo aquí, pero puede usar casi cualquier interfaz de red disponible, lo que ilustra la flexibilidad de la capa IP. Ejemplos son IEEE 802.2, X.25 (que es fiable por sí mismo), ATM, FDDI, PRN ("Packet Radio Networks", como AlohaNet).

Las interacciones reales se muestran con flechas en Figura - Modelo arquitectónico. Un modelo de capas más detallado se muestra en Figura - Modelo arquitectónico detallado.

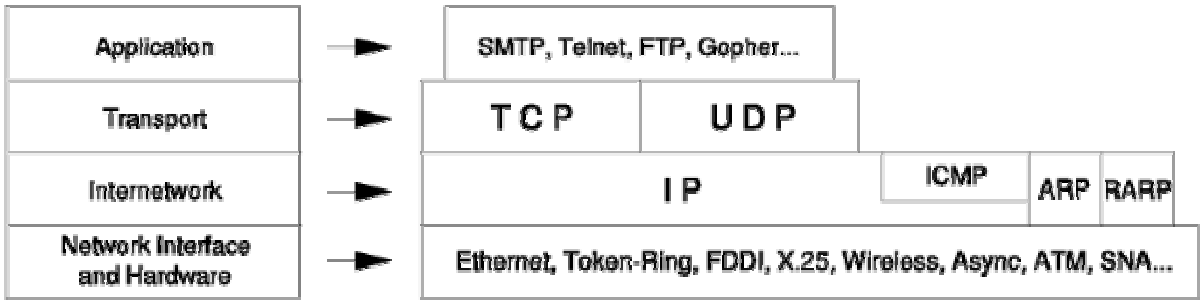
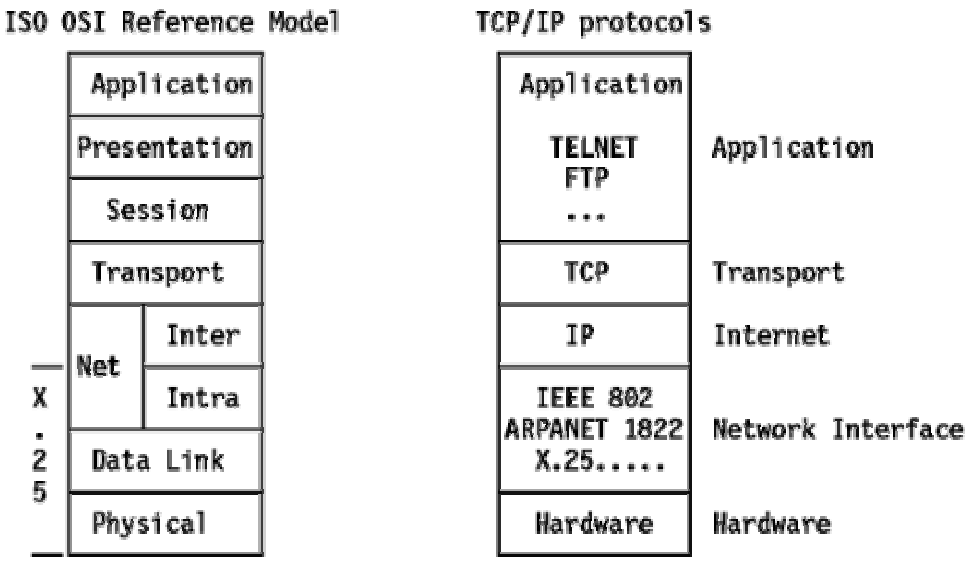


Figura: Modelo arquitectónico detallado

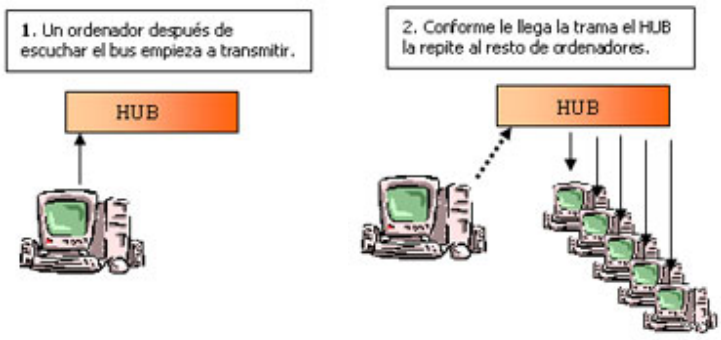


Esta división en capas a veces se simplifica como es el caso del TCP/IP (todo en uno), el ATM y otros que utilizan sus propias derivaciones de esta torre. Ahora que hemos descrito cada capa es necesario ubicar los distintos elementos. Los routers suelen trabajar en la capa de red, es decir, filtran direcciones IP, controlan los puertos, realizan NAPT, NAT y otras cosas, naturalmente se encargan del enrutamiento de los paquetes entre redes. Los “switchs” (conmutadores) domésticos se sitúan en la capa 2, es decir en la capa de “Enlace de datos”. En esta capa todo se realiza a base de tramas (mayoritariamente Ethernet) y direcciones MAC. Finalmente los HUBs están situados en la capa 1, es decir la capa física ya que actúan como repetidores.

Vamos a ver cómo funciona un HUB y cómo funciona un Switch, las cosas que hacen uno y lo que hace otro, así como sus usos.

Hub

Un HUB tal como dice su nombre es un concentrador. Simplemente une conexiones y no altera las tramas que le llegan. Para entender como funciona veamos paso a paso lo que sucede (aproximadamente) cuando llega una trama.



Visto lo anterior podemos sacar las siguientes conclusiones:

1 - El HUB envía información a ordenadores que no están interesados. A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el HUB envía la información a todos los ordenadores que están conectados a él, así seguro que acierta.

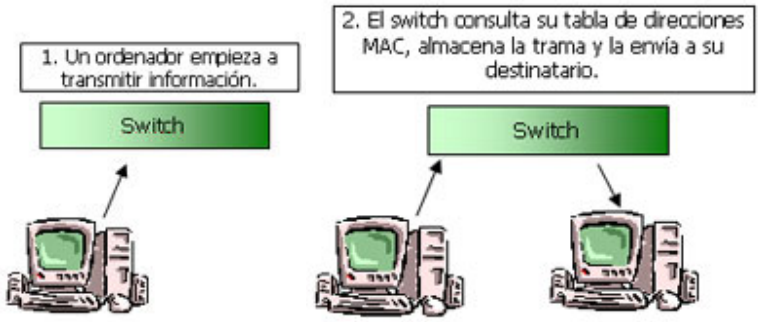
2 - Este tráfico añadido genera más probabilidades de colisión. Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea que otro ordenador que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.

3 - Un HUB funciona a la velocidad del dispositivo más lento de la red. Si observamos cómo funciona vemos que el HUB no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 megabit le trasmitiera a otro de 10 megabit algo se perdería el mensaje. En el caso del ADSL los routers suelen funcionar a 10 megabit, si lo conectamos a nuestra red casera, toda la red funcionará a 10, aunque nuestras tarjetas sean 10/100.

4 - Un HUB es un dispositivo simple, esto influye en dos características. El precio es baratito. El retardo, un HUB casi no añade ningún retardo a los mensajes.

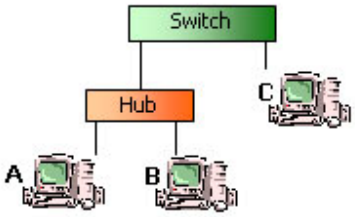
Switch

Cuando hablamos de un switch lo haremos refiriéndonos a uno de nivel 2, es decir, perteneciente a la capa “Enlace de datos”. Normalmente un switch de este tipo no tiene ningún tipo de gestión, es decir, no se puede acceder a él. Sólo algunos switch tienen algún tipo de gestión pero suele ser algo muy simple. Veamos cómo funciona un “switch”.



Puntos que observamos del funcionamiento de los “switch”:

1 - El “switch” conoce los ordenadores que tiene conectados a cada uno de sus puertos (enchufes). Cuando en la especificación del un “switch” leemos algo como “8k MAC address table” se refiere a la memoria que el “switch” destina a almacenar las direcciones. Un “switch” cuando se enchufa no conoce las direcciones de los ordenadores de sus puertos, las aprende a medida que circula información a través de él. Con 8k hay más que suficiente. Por cierto, cuando un “switch” no conoce la dirección MAC de destino envía la trama por todos sus puertos, al igual que un HUB (“Flooding”, inundación). Cuando hay más de un ordenador conectado a un puerto de un “switch” este aprende sus direcciones MAC y cuando se envían información entre ellos no la propaga al resto de la red, a esto se llama filtrado.



El tráfico entre A y B no llega a C. Como decía, esto es el filtrado. Las colisiones que se producen entre A y B tampoco afectan a C. A cada parte de una red separada por un “switch” se le llama segmento.

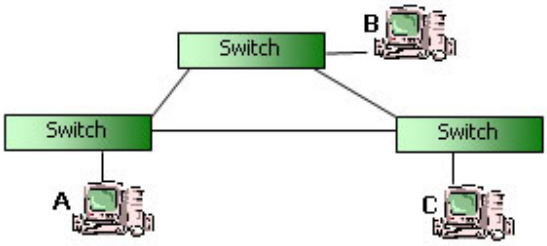
2 - El “switch” almacena la trama antes de reenviarla. A este método se llama “store & forward”, es decir “almacenar y enviar”. Hay otros métodos como por ejemplo “Cut-through” que consiste en recibir los 6 primeros bytes de una trama que contienen la dirección MAC y a partir de aquí ya empezar a enviar al destinatario. “Cut-through” no permite descartar paquetes defectuosos. Un “switch” de tipo “store & forward” controla el CRC de las tramas para comprobar que no tengan error, en caso de ser una trama defectuosa la descarta y ahorra tráfico innecesario. El “store & forward” también permite adaptar velocidades de distintos dispositivos de una forma más cómoda, ya que la memoria interna del “switch” sirve de “**buffer**”. Obviamente si se envía mucha información de un dispositivo rápido a otro lento otra capa superior se encargará de reducir la velocidad.

Finalmente comentar que hay otro método llamado “Fragment-free” que consiste en recibir los primeros 64 bytes de una trama porque es en estos donde se producen la mayoría de colisiones y errores. Así pues cuando vemos que un “switch” tiene 512KB de RAM es para realizar el “store & forward”. Esta RAM suele estar compartida entre todos los puertos, aunque hay modelos que dedican un trozo a cada puerto.

3 - Un “switch” moderno también suele tener lo que se llama “Auto-Negotation”, es decir, negocia con los dispositivos que se conectan a él la velocidad de funcionamiento, 10 megabit ó 100, así como si se funcionara en modo “full-duplex” o “half-duplex”. “Full-duplex” se refiere a que el dispositivo es capaz de enviar y recibir información de forma simultánea, “half-duplex” por otro lado sólo permite enviar o recibir información, pero no a la vez.

4 - Velocidad de proceso: todo lo anterior explicado requiere que el “switch” tenga un procesador y claro, debe ser lo más rápido posible. También hay un parámetro conocido como “back-plane” o plano trasero que define el ancho de banda máximo que soporta un “switch”. El “back plane” dependerá del procesador, del número de tramas que sea capaz de procesar. Si hacemos números vemos lo siguiente: 100megabits x 2 (cada puerto puede enviar 100 megabit y enviar 100 más en modo “full-duplex”) x 8 puertos = 1,6 gigabit. Así pues, un “switch” de 8 puertos debe tener un “back-plane” de 1,6 gigabit para ir bien. Lo que sucede es que para abaratar costes esto se reduce ya que es muy improbable que se produzca la situación de tener los 8 puertos enviando a tope... Pero la probabilidad a veces no es cierta ;)

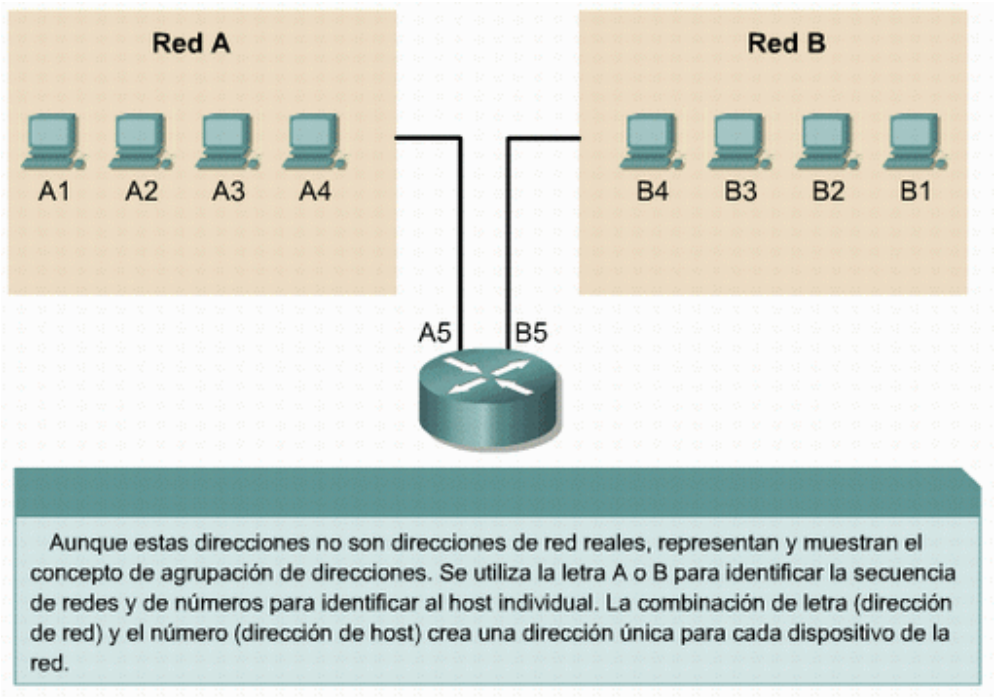
5 - Si un nodo puede tener varias rutas alternativas para llegar a otro un “switch” tiene problemas para aprender su dirección ya que aparecerá en dos de sus entradas. A esto se le llama “loop” y suele haber una lucecita destinada a eso delante de los “switch”. El protocolo de Spanning Tree Protocol IEEE 802.1d se encarga de solucionar este problema, aunque los “switch” domésticos no suelen tenerlo



DIRECCIONAMIENTO IP

Para que dos sistemas se comuniquen, se deben poder identificar y localizar entre sí. Aunque las direcciones de la Figura no son direcciones de red reales, representan el concepto de agrupamiento de las direcciones.

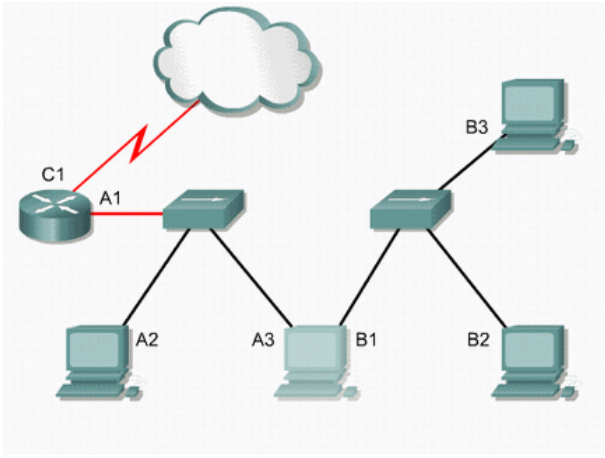
Este utiliza A o B para identificar la red y la secuencia de números para identificar el host individual.



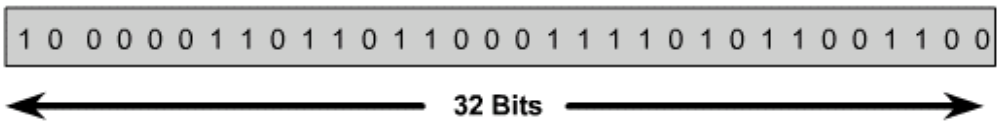
Un computador puede estar conectado a más de una red. En este caso, se le debe asignar al sistema más de una dirección. Cada dirección identificará la conexión del computador a una red diferente. No se suele decir que un dispositivo tiene una dirección sino que cada uno de los puntos de conexión (o interfaces) de dicho dispositivo tiene una dirección en una red. Esto permite que otros computadores localicen el dispositivo en una determinada red.

La combinación de letras (dirección de red) y el número (dirección del host) crean una dirección única para cada dispositivo conectado a la red. Cada computador conectado a una red TCP/IP debe recibir un identificador exclusivo o una dirección IP. Esta dirección, que opera en la Capa 3, permite que un computador localice otro computador en la red.

Todos los computadores también cuentan con una dirección física exclusiva, conocida como dirección MAC. Estas son asignadas por el fabricante de la tarjeta de interfaz de la red. Las direcciones MAC operan en la Capa 2 del modelo OSI.



Una dirección IP es una secuencia de unos y ceros de 32 bits. La Figura muestra un número de 32 bits de muestra.



Para que el uso de la dirección IP sea más sencillo, en general, la dirección aparece escrita en forma de cuatro números decimales separados por puntos. Por ejemplo, la dirección IP de un computador es 192.168.1.2. Otro computador podría tener la dirección 128.10.2.1. Esta forma de escribir una dirección se conoce como formato decimal punteado.

En esta notación, cada dirección IP se escribe en cuatro partes separadas por puntos. Cada parte de la dirección se conoce como octeto porque se compone de ocho dígitos binarios.

Por ejemplo, la dirección IP 192.168.1.8 sería 11000000.10101000.00000001.00001000 en una notación binaria. La notación decimal punteada es un método más sencillo de comprender que el método binario de unos y ceros.

Esta notación decimal punteada también evita que se produzca una gran cantidad de errores por transposición, que sí se produciría si sólo se utilizaran números binarios. El uso de decimales separados por puntos permite una mejor comprensión de los patrones numéricos.

Tanto los números binarios como los decimales de la Figura representan a los mismos valores, pero resulta más sencillo apreciar la notación decimal punteada.

Binario: 11000000.10101000.000000001.00001000 y 11000000.10101000.00000001.00001001

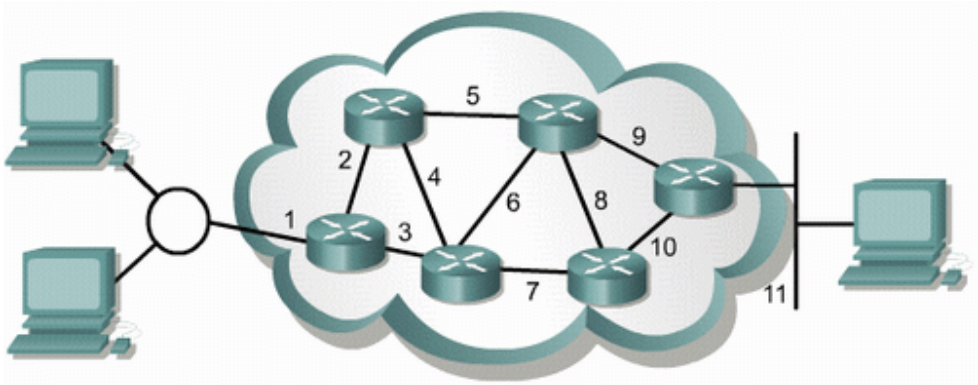
Decimal: 192.168.1.8 y 192.168.1.9

Los números binarios y decimales representan los mismos valores pero es mucho más fácil ver con los valores decimales punteados. Este es uno de los problemas más comunes que se encuentran al trabajar directamente con los números binarios. Las largas cadenas de unos y ceros repetidos aumentan la probabilidad de errores de transposición y omisión.

Este es uno de los problemas frecuentes que se encuentran al trabajar directamente con números binarios. Las largas cadenas de unos y ceros que se repiten hacen que sea más probable que se produzcan errores de transposición y omisión.

Router

Un Router envía los paquetes desde la red origen a la red destino utilizando el protocolo IP. Los paquetes deben incluir un identificador tanto para la red origen como para la red destino.

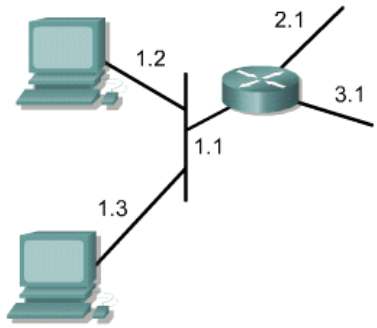


Las direcciones representan la ruta de las conexiones entre medios

Utilizando la dirección IP de una red destino, un Router puede enviar un paquete a la red correcta. Cuando un paquete llega a un Router conectado a la red destino, este utiliza la dirección IP para localizar el computador en particular conectado a la red.

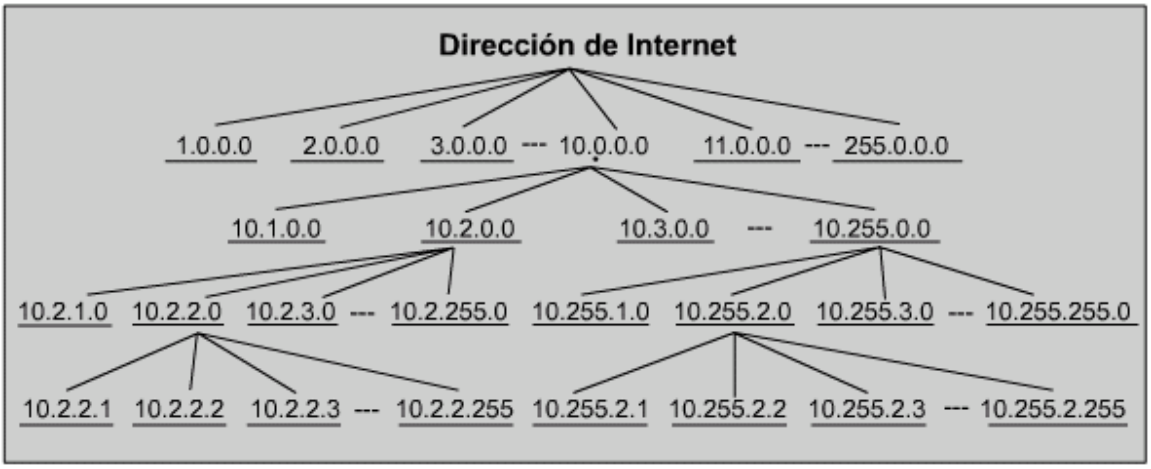
Este sistema funciona de la misma forma que un sistema nacional de correo. Cuando se envía una carta, primero debe enviarse a la oficina de correos de la ciudad destino, utilizando el código postal. Dicha oficina debe entonces localizar el destino final en la misma ciudad utilizando el domicilio. Es un proceso de dos pasos.

De igual manera, cada dirección IP consta de dos partes. Una parte identifica la red donde se conecta el sistema y la segunda identifica el sistema en particular de esa red.



Red	Host
1	1 2 3
2	1
3	1

Como muestra la Figura, cada octeto varía de 0 a 255. Cada uno de los octetos se divide en 256 subgrupos y éstos, a su vez, se dividen en otros 256 subgrupos con 256 direcciones cada uno. Al referirse a una dirección de grupo inmediatamente arriba de un grupo en la jerarquía, se puede hacer referencia a todos los grupos que se ramifican a partir de dicha dirección como si fueran una sola unidad.



Este tipo de dirección recibe el nombre de dirección jerárquica porque contiene diferentes niveles. Una dirección IP combina estos dos identificadores en un solo número. Este número debe ser un número exclusivo, porque las direcciones repetidas harían imposible el enrutamiento.

La primera parte identifica la dirección de la red del sistema. La segunda parte, la parte del host, identifica qué máquina en particular de la red.

Las direcciones IP se dividen en clases para definir las redes de tamaño pequeño, mediano y grande. Las direcciones Clase A se asignan a las redes de mayor tamaño. Las direcciones Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas.

Clase de dirección	Cantidad de redes	Cantidad de hosts por red
A	126 *	16,777,216
B	16, 384	65,535
C	2,097,152	254
D (Multicast)	No es aplicable	No es aplicable

* El intervalo de direcciones 127.x.x.x está reservado como dirección de loopback, con propósitos de prueba y diagnóstico.

Clase de dirección IP:	Bits de mayor peso	Primer intervalo de dirección de octeto	Número de bits en la dirección de red
Clase A	0	0 - 127 *	8
Clase B	10	128 - 191	16
Clase C	110	192 - 223	24
Clase D	1110	224 - 239	28

El primer paso para determinar qué parte de la dirección identifica la red y qué parte identifica el host es identificar la clase de dirección IP.

Clase de dirección	Bits de mayor peso	Intervalo de dirección del primer octeto	Número de bits en la dirección de red	Número de redes	Número de hosts por red
Clase A	0	0-127	8	126	16,777,216
Clase B	10	128-191	16	16,384	65,536
Clase C	110	192-223	24	2,097,152	254
Clase D	1110	224-239	28	No es aplicable	No es aplicable

DIRECCIONES IP CLASE A, B, C, D, Y E

Para adaptarse a redes de distintos tamaños y para ayudar a clasificarlas, las direcciones IP se dividen en grupos llamados clases.

Clase A	Red	Host		
Octet	1	2	3	4

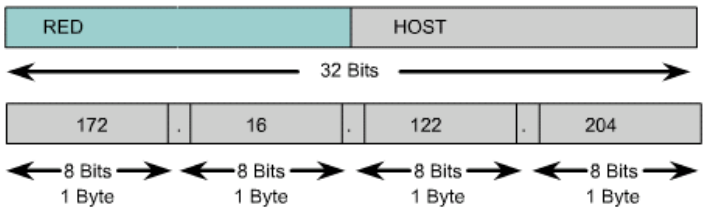
Clase B	Red		Host	
Octet	1	2	3	4

Clase C	Red			Host
Octet	1	2	3	4

Clase D	Host			
Octet	1	2	3	4

Las direcciones Clase D se utilizan para grupos de multicast. No hay necesidad de asignar octetos o bits a las distintas direcciones de red o de host. Las direcciones Clase E se reservan para fines de investigación solamente.

Esto se conoce como direccionamiento classful. Cada dirección IP completa de 32 bits se divide en la parte de la red y parte del host.



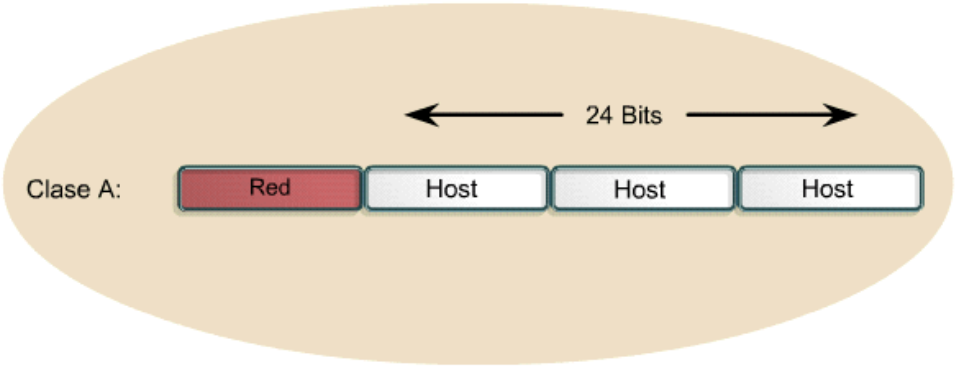
Una dirección IP siempre se divide en una parte de red y una parte de host. En un esquema de direccionamiento con clases, estas divisiones tienen lugar en los límites de los octetos.

Un bit o una secuencia de bits al inicio de cada dirección determinan su clase. Son cinco las clases de direcciones IP como muestra la Figura

Clase de dirección IP	Intervalo de dirección IP (Valor decimal d
Clase A	1-126 (00000001-01111110) *
Clase B	128-191 (10000000-10111111)
Clase C	192-223 (11000000-11011111)
Clase D	224-239 (11100000-11101111)
Clase E	240-255 (11110000-11111111)

Determine la clase basándose en el valor decimal del primer octeto
* 127 (01111111) es una dirección clase A reservada para pruebas loopback y no puede ser asignada a una red

La dirección Clase A se diseñó para admitir redes de tamaño extremadamente grande, de más de 16 millones de direcciones de host disponibles.



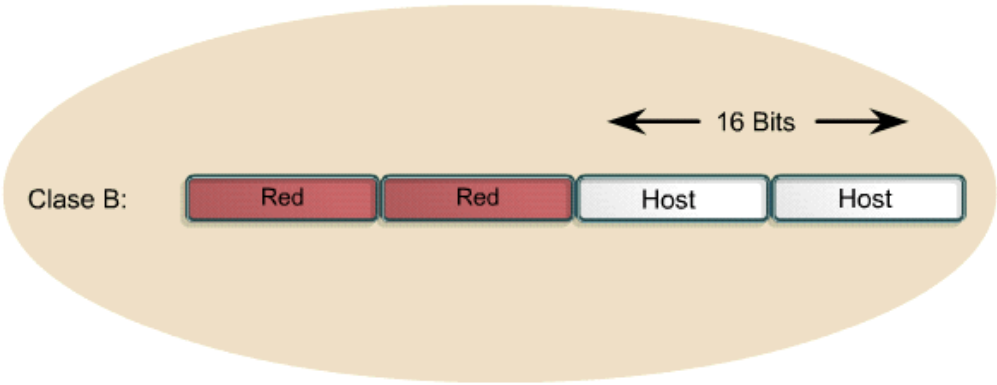
Las direcciones IP Clase A utilizan sólo el primer octeto para indicar la dirección de la red. Los tres octetos restantes son para las direcciones host.

El primer bit de la dirección Clase A siempre es 0. Con dicho primer bit, que es un 0, el menor número que se puede representar es 00000000, 0 decimal.

El valor más alto que se puede representar es 01111111, 127 decimal. Estos números 0 y 127 quedan reservados y no se pueden utilizar como direcciones de red. Cualquier dirección que comience con un valor entre 1 y 126 en el primer octeto es una dirección Clase A.

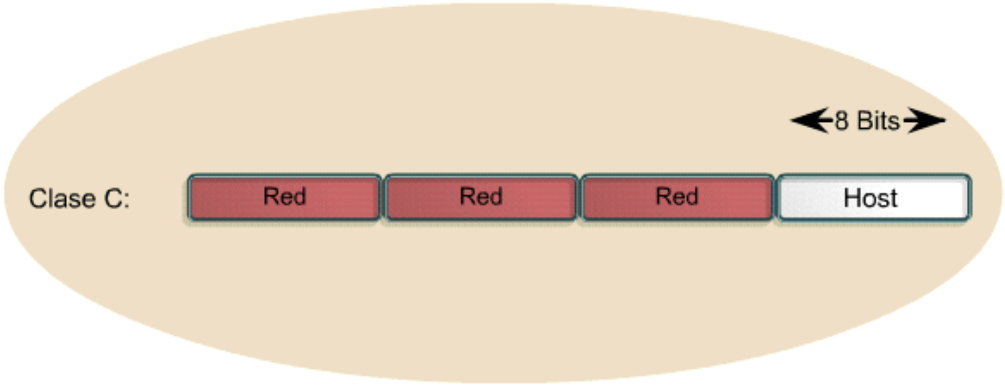
La red 127.0.0.0 se reserva para las pruebas de loopback. Los Routers o las máquinas locales pueden utilizar esta dirección para enviar paquetes nuevamente hacia ellos mismos. Por lo tanto, no se puede asignar este número a una red.

La dirección Clase B se diseñó para cumplir las necesidades de redes de tamaño moderado a grande. Una dirección IP Clase B utiliza los primeros dos de los cuatro octetos para indicar la dirección de la red. Los dos octetos restantes especifican las direcciones del host.



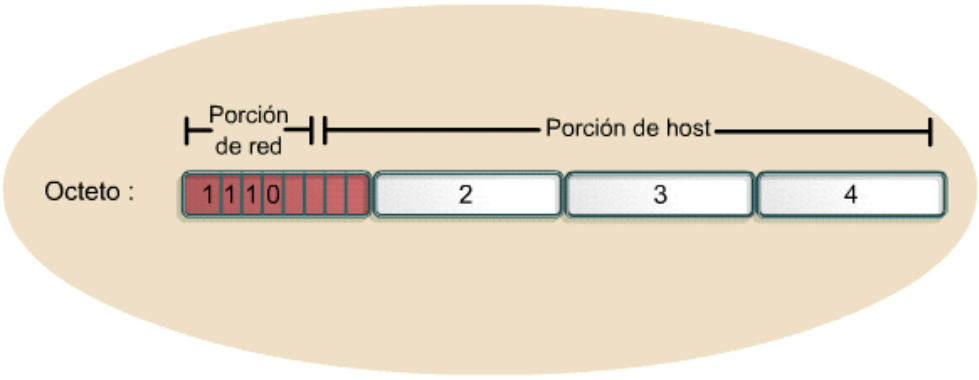
Los primeros dos bits del primer octeto de la dirección Clase B siempre son 10. Los seis bits restantes pueden poblarse con unos o ceros. Por lo tanto, el menor número que puede representarse en una dirección Clase B es 10000000, 128 decimal. El número más alto que puede representarse es 10111111, 191 decimal. Cualquier dirección que comience con un valor entre 128 y 191 en el primer octeto es una dirección Clase B.

El espacio de direccionamiento Clase C es el que se utiliza más frecuentemente en las clases de direcciones originales. Este espacio de direccionamiento tiene el propósito de admitir redes pequeñas con un máximo de 254 hosts.



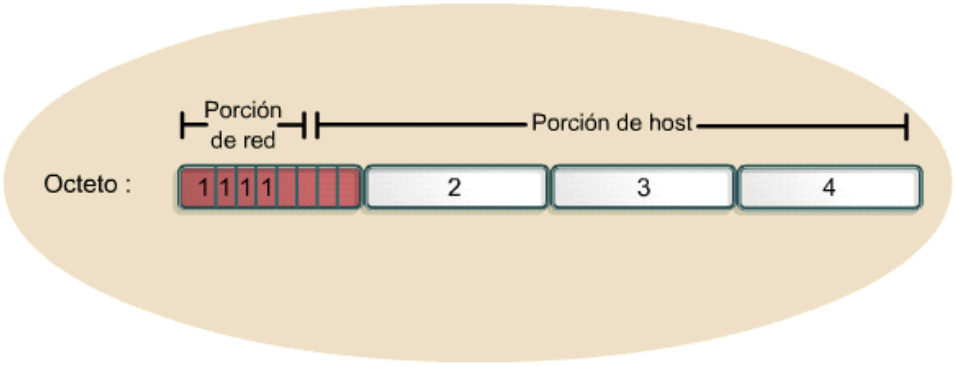
Una dirección Clase C comienza con el binario 110. Por lo tanto, el menor número que puede representarse es 11000000, 192 decimal. El número más alto que puede representarse es 11011111, 223 decimal. Si una dirección contiene un número entre 192 y 223 en el primer octeto, es una dirección de Clase C.

La dirección Clase D se creó para permitir multicast en una dirección IP. Una dirección multicast es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.



El espacio de direccionamiento Clase D, en forma similar a otros espacios de direccionamiento, se encuentra limitado matemáticamente. Los primeros cuatro bits de una dirección Clase D deben ser 1110. Por lo tanto, el primer rango de octeto para las direcciones Clase D es 11100000 a 11101111, o 224 a 239. Una dirección IP que comienza con un valor entre 224 y 239 en el primer octeto es una dirección Clase D.

Se ha definido una dirección Clase E. Sin embargo, la Fuerza de tareas de ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación. Por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet. Los primeros cuatro bits de una dirección Clase E siempre son 1s. Por lo tanto, el rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, o 240 a 255.



Puentes, "routers" y pasarelas

La formación de una red conectando múltiples redes se consigue por medio de los "routers". Es importante distinguir entre un "router", un puente y una pasarela.

Puente

Interconecta segmentos de LAN a nivel de interfaz de red y envía tramas entre ellos. Un puente realiza la función de retransmisión MAC, y es independiente de cualquier capa superior (incluyendo el enlace lógico). Proporciona, si se necesita, conversión de protocolo a nivel MAC.
Un puente es transparente para IP. Es decir, cuando un host envía un datagrama a otro host en una red con el que se conecta a través de un puente, envía el datagrama al host y el datagrama cruza el puente sin que el emisor se dé cuenta.

"Router"

Interconecta redes en el nivel de red y encamina paquetes entre ellas. Debe comprender la estructura de direccionamiento asociada con los protocolos que soporta y tomar la decisión de si se han de enviar, y cómo se ha de hacer, los paquetes. Los "routers" son capaces de elegir las mejores rutas de transmisión así como tamaños óptimos para los paquetes. La función básica de encaminamiento está implementada en la capa IP. Por lo tanto, cualquier estación de trabajo que ejecute TCP/IP se puede usar como "router".
Un "router" es visible para IP. Es decir, cuando un host envía un datagrama IP a otro host en una red conectada por un "router", envía el datagrama al "router" y no directamente al host de destino.

Pasarela

Interconecta redes a niveles superiores que los puentes y los "routers". Una pasarela suele soportar el mapeado de direcciones de una red a otra, así como la transformación de datos entre distintos entornos para conseguir conectividad entre los extremos de la comunicación. Las pasarelas limitan típicamente la conectividad de dos redes a un subconjunto de los protocolos de aplicación soportados en cada una de ellas.
Una pasarela es *opaca* para IP. Es decir, un host no puede enviar un datagrama IP a través de una pasarela: sólo puede enviarlo a la pasarela. La pasarela se ocupa de transmitirlo a la otra red con la información de los protocolos de alto nivel que vaya en él.

Estrechamente ligado al concepto de pasarela, está el de cortafuegos ("firewall") o pasarela cortafuegos, que se usa para restringir el acceso desde Internet a una red o un grupo de ellas, controladas por una organización, por motivos de seguridad.

Como se señaló arriba, un host TCP/IP tiene una funcionalidad básica como "router", incluida en IP. Un "router" de esta clase es adecuado para encaminamiento simple, pero no para redes complejas.

El mecanismo de encaminamiento IP, combinado con el modelo por capas de TCP/IP, se representa en Figura - El "router". Muestra un datagrama IP, que va de una dirección IP (número de red X, host número A) a otra (número de red Y, host número B), a través de dos redes físicas.

Nótese que en el "router" intermedio, sólo están implicados los niveles inferiores de la pila (red e interfaz de red).

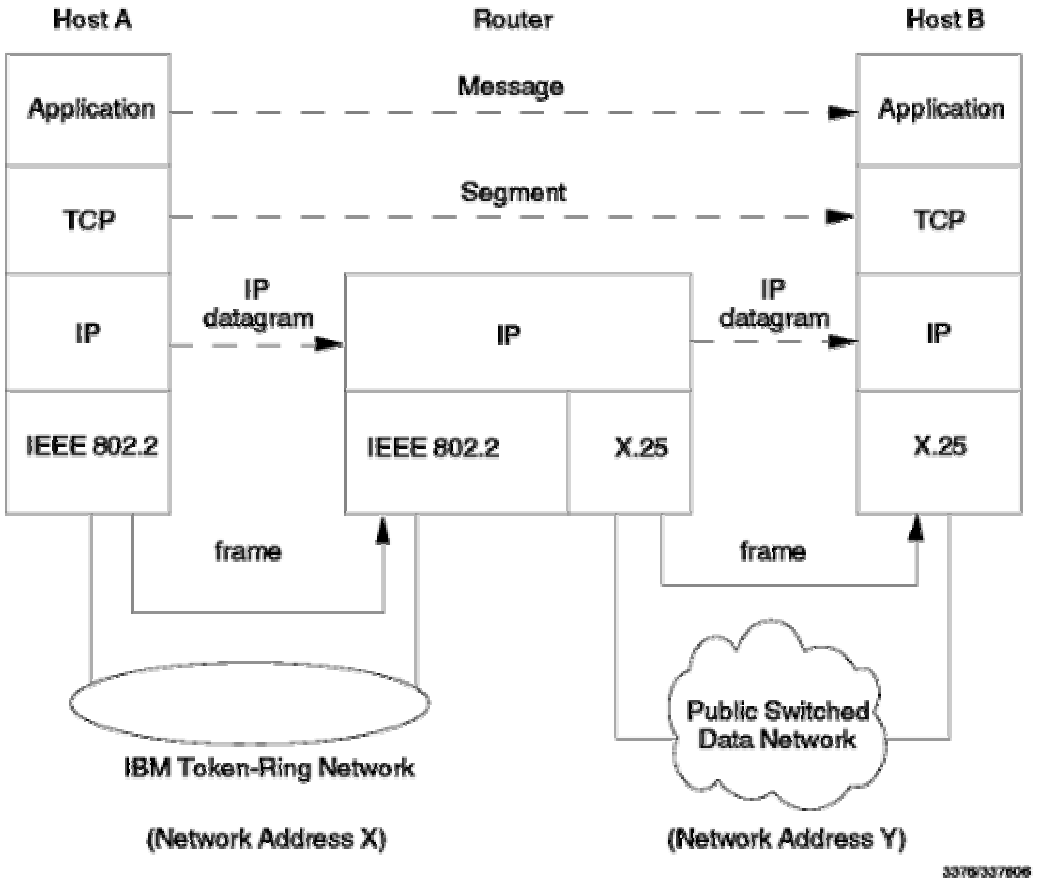


Figura: El "router" - La función de "router" la realiza el protocolo IP.