

de Directorio global distribuida entre los Network Nodes por toda la red, manteniendo cada uno una parte, de forma que un nodo encuentra la localización de un recurso buscando en el orden siguiente:

- En el nodo originario de la petición.
- Si éste es un EN, se busca en su NN servidor.
- Si un NN conoce la LU en una localización remota, reenvía la petición, si se recibe una confirmación, se calcula la ruta óptima.
- Si ningún nodo conocido controla el recurso, se envía una búsqueda no dirigida a todos los NN adyacentes. Éstos, a su vez, propagan la petición hasta que se haya interrogado a todos los NN, una respuesta positiva hace que se calcule la ruta, más una actualización de la BD topológico por el nodo emisor.

Una vez que se ha confirmado el nodo de la LU destino, el NN de la LU origen calcula dinámicamente la ruta preferente. Una vez calculada la ruta, el Control Point pasa esta información a la LU origen, que puede entonces enviar un BIND para activar la sesión. Es entonces cuando usando la sesión, los Transaction Programs (TP) pueden empezar una conversación.

5. EL MODELO TCP/IP.

La pila TCP/IP se llama así por dos de sus protocolos más importantes: TCP («Transmission Control Protocol») de IP («Internet Protocol»). Otro nombre es pila de protocolos de Internet, y es la frase oficial usada en documentos oficiales de estándares.

La primera meta de diseño de TCP/IP fue construir una interconexión de redes que proporcionase servicios de comunicación universales: una red, o Internet. Cada red física tiene su propia interfaz de comunicaciones, dependiente de la tecnología que la implementa, en la forma de una interfaz de programación que proporciona funciones básicas de comunicación (primitivas). Las comunicaciones entre servicios las proporciona el software que se ejecuta entre la red física y la aplicación de usuario, y da a estas aplicaciones una interfaz común, independiente de la estructura de la red física subyacente. La arquitectura de las redes físicas es transparente al usuario.

El segundo objetivo es interconectar distintas redes físicas para formar lo que al usuario le parece una única y gran red. Tal conjunto de redes interconectadas se denomina «internetwork» o Internet. Para poder interconectar dos redes, necesitamos un ordenador que esté conectado a ambas redes y que pueda retransmitir paquetes de una a la otra; tal máquina es un router. El término router IP también se usa porque la función de encaminamiento es parte de la capa IP de la pila TCP/IP. Las propiedades básicas de un router son:

- Desde el punto de vista de la red, es un host normal.
- Desde el punto de vista del usuario, es invisible. El usuario sólo ve una gran red.

Para ser capaz de identificar un host en la red, a cada uno se le asigna una dirección, la dirección IP. Cuando un host tiene múltiples adaptadores de red, cada adaptador tiene una dirección IP separada. La dirección IP consta de dos partes:

dirección IP = <número de red><número de host>

El número de red lo asigna una autoridad central y es unívoco en Internet. La autoridad para asignar el número de host reside en la organización que controla la red identificada por el número de red.

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:

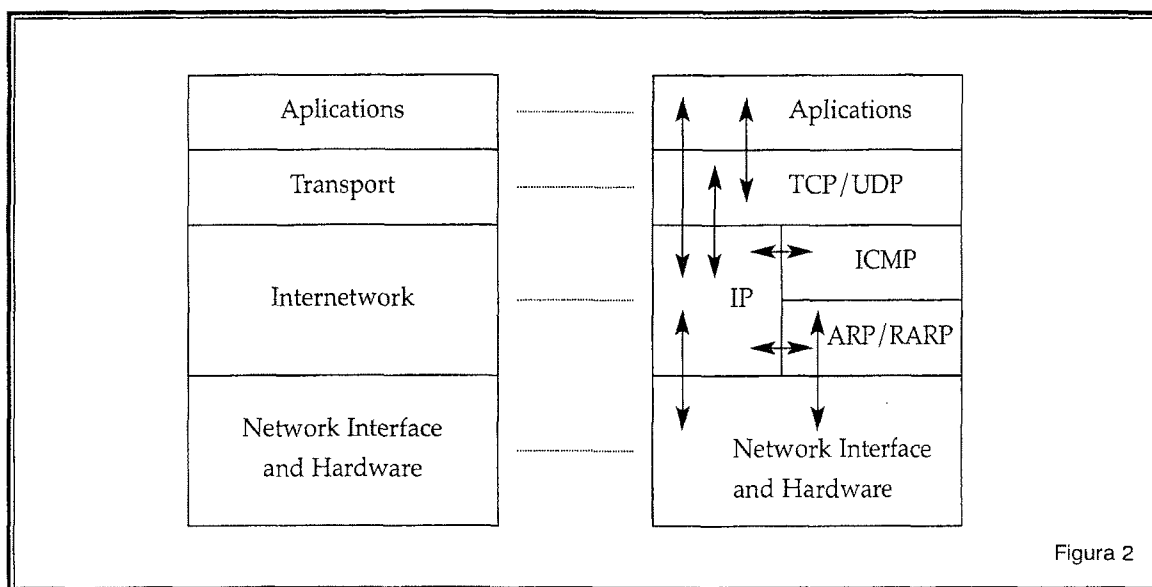


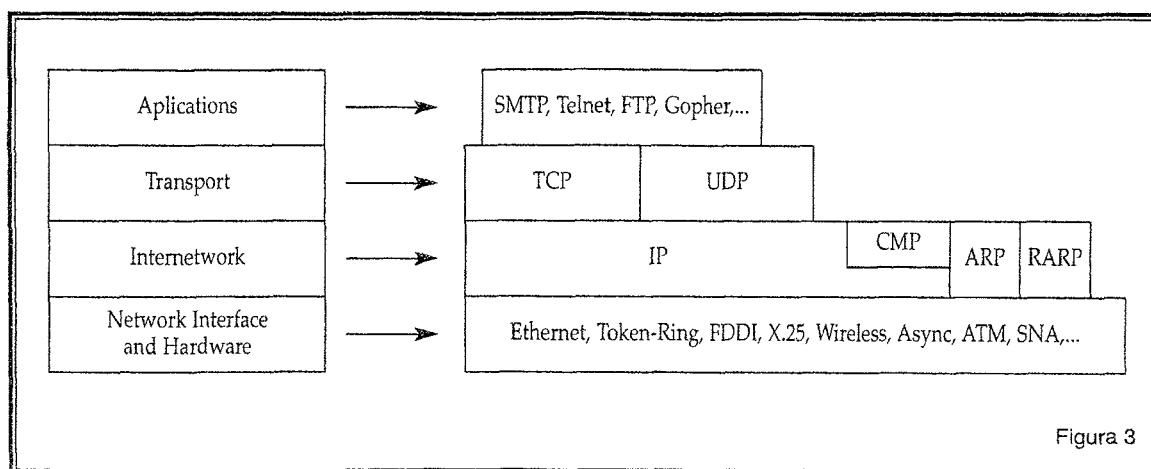
Figura 2

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. Ejemplos 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 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 proporcionarse 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 Networks.

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) incluso SNA.



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.

Encaminamiento IP: los datagramas entrantes se chequean para ver si el host local es el destinatario:

- Sí. El datagrama se pasa a los protocolos de nivel superior.
- No. El datagrama es para un host diferente.

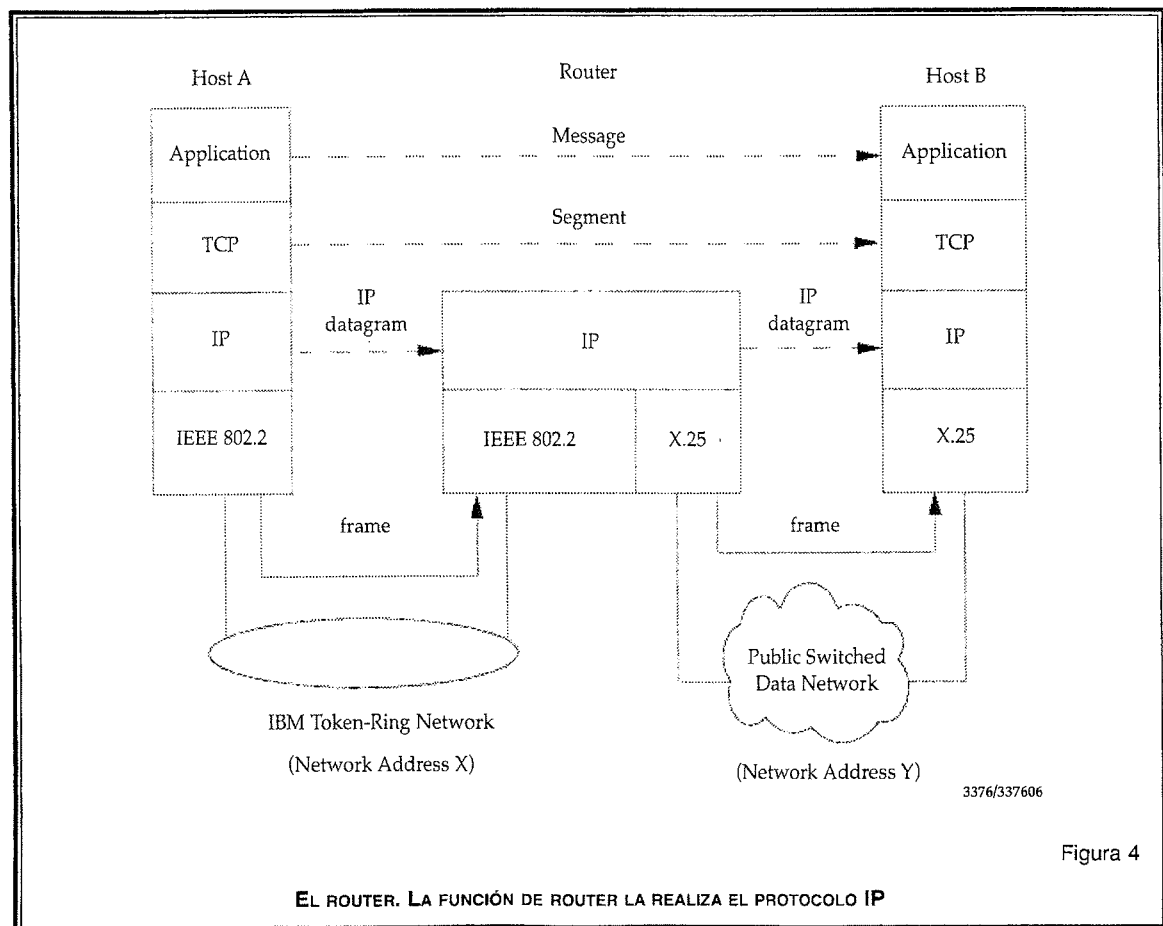
La acción depende del valor del flag «ipforwarding» (retransmisión IP).

- Verdadero. El datagrama se trata como si fuera un datagrama saliente y se encamina el siguiente salto según el algoritmo descrito abajo.
- Falso. El datagrama se desecha.

En el protocolo de red, los datagramas salientes se someten al algoritmo de encaminamiento IP que determina dónde enviar el datagrama de acuerdo con la dirección de destino.

- Si el host tiene una entrada en su tabla de encaminamiento IP que concuerde con la IP de destino, el datagrama se envía a la dirección correspondiente a esa entrada.
- Si el número de red de la dirección IP de destino es el mismo que el de uno de los adaptadores de red del host (están en la misma red) el datagrama se envía a la dirección física del host que tenga la dirección de destino.
- En otro caso, el datagrama se envía a un router por defecto.

Este algoritmo básico, necesario en toda implementación de IP, es suficiente para realizar las funciones de encaminamiento elementales. 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.



La dirección IP: los estándares para las direcciones IP se describen en RFC 1166 Números de Internet. Para ser capaz de identificar una máquina en Internet, a cada interfaz de red de la máquina o host se le asigna una dirección, la dirección IP, o dirección de Internet. Cuando la máquina está conectada a más de una red se le denomina «multi-homed» y tendrá una dirección IP por cada interfaz de red. La dirección IP consiste en un par de números:

IP dirección = <número de red><número de interfaz de red>

La parte de la dirección IP correspondiente al número de red está administrada centralmente por el InterNIC (Internet Network Information Center) y es única en toda la Internet.

Las direcciones IP son números de 32 bits representados habitualmente en formato decimal (la representación decimal de cuatro valores binarios de 8 bits concatenados por puntos). Por ejemplo 128.2.7.9 es una dirección IP, donde 128.2 es el número de red y 7.9 el de la interfaz de red. Las reglas usadas para dividir una dirección de IP en su parte de red y de interfaz de red se explican abajo.

El formato binario para la dirección IP 128.2.7.9 es:

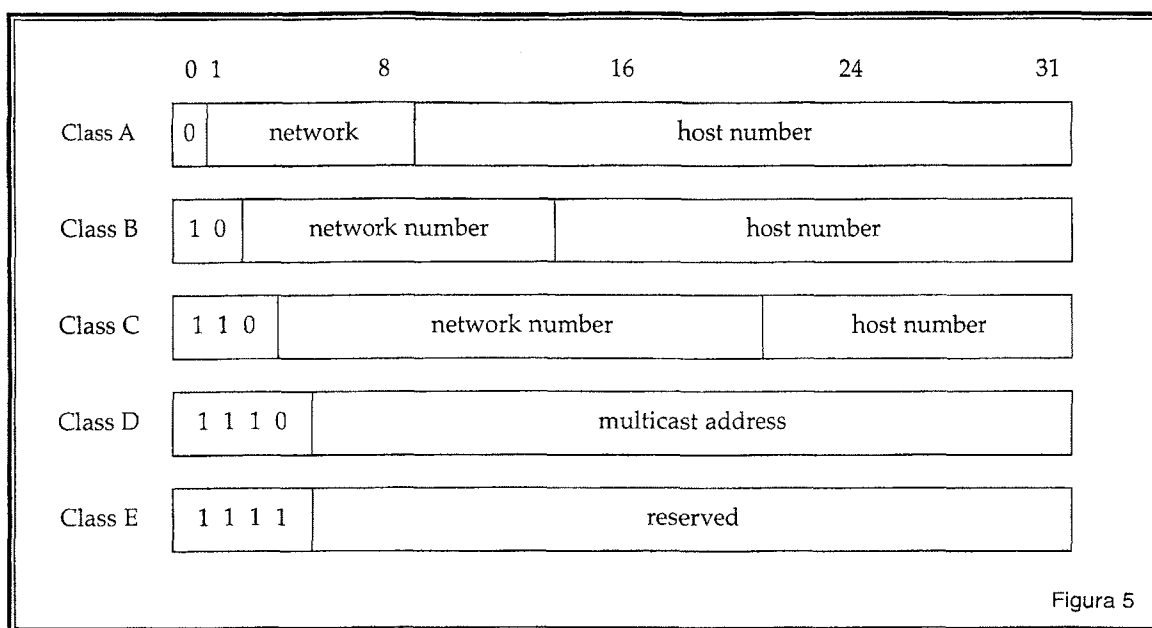
10000000 00000010 00000111 00001001

Las direcciones IP son usadas por el protocolo IP para definir únicamente un host en la red. Los datagramas IP (los paquetes de datos elementales intercambiados entre máquinas) se transmiten a través de alguna red física conectada a la interfaz de la máquina y cada uno de ellos contiene la dirección IP de origen y la dirección IP de destino. Para enviar un datagrama a una dirección IP de destino determinada, la dirección de destino debe ser traducida a una dirección física. Esto puede requerir transmisiones en la red para encontrar la dirección física de destino, por ejemplo, en LAN's el ARP («Address Resolution Protocol» se usa para traducir las direcciones IP a direcciones físicas MAC).

Los primeros bits de las direcciones IP especifican cómo el resto de las direcciones deberían separarse en sus partes de red y de interfaz.

Los términos dirección de red y netID se usan a veces en vez de número de red, pero el término formal, utilizado en RFC 1166, es número de red. Análogamente, los términos dirección de host y hostID se usan ocasionalmente en vez de número de host.

Hay cinco clases de direcciones IP.



Dos de los números de red de cada una de las clases A, B y C, y dos de los números de host de cada red están preasignados: los que tienen todos los bits a 0 y los que tienen todos los bits a 1. Las direcciones de clase A usan 7 bits para el número de red permitiendo 126 posibles redes (veremos posteriormente que de cada par de direcciones de red y de host, dos tienen un significado especial). Los restantes 24 bits se emplean para el número de host, de modo que cada red puede tener hasta 16,777,214 hosts.

- Las direcciones de clase B usan 14 bits para el número de red, y 16 bits para el de host, lo que supone 16.382 redes de hasta 65.534 hosts cada una.
- Las direcciones de clase C usan 21 bits para el número de red y 8 para el de host, lo que supone 2.097,150 redes de hasta 254 hosts cada una.
- Las direcciones de clase D se reservan para multicasting o multidifusión, usada para direccionar grupos de hosts en un área limitada.
- Las direcciones de clase E se reservan para usos en el futuro.

Es obvio que una dirección de clase A sólo se asignará a redes con un elevado número de hosts, y que las direcciones de clase C son adecuadas para redes con pocos hosts. Sin embargo, esto significa que las redes de tamaño medio (aquellas con más de 254 hosts o en las que se espera que en el futuro haya más de 254 hosts) deben usar direcciones de clase IP. El número de redes de tamaño pequeño y medio ha ido creciendo muy rápidamente en los últimos años y se temía que, de haber permitido que se mantuviera este crecimiento, todas las direcciones de clase B se habrían usado para mediados de los 90. Esto es lo que se conoce como el problema del agotamiento de las direcciones IP.

Un hecho a señalar en la división de la dirección IP en dos partes es que esta división, a su vez, divide en dos partes la responsabilidad de elegir una dirección IP. El número de red es asignado por el InterNIC y el de host por la autoridad que controla la red. Como veremos en la siguiente sección, el número de host puede dividirse aún más: esta división también es controlada por la autoridad propietaria de la red, y no por el InterNIC.

Debido al crecimiento explosivo de Internet, el uso de direcciones IP asignadas se volvió demasiado rígido para permitir cambiar con facilidad la configuración de redes locales. Estos cambios podrían ser necesarios cuando:

- Se instala una nueva red física.
- El crecimiento del número de hosts requiere dividir la red local en dos o más redes.

Para evitar tener que solicitar direcciones IP adicionales en estos casos, se introdujo el concepto de subred.

El número de host de la dirección IP se subdivide de nuevo en un número de red y uno de host. Esta segunda red se denomina subred. La red principal consiste ahora en un conjunto de subredes y la dirección IP se interpreta como:

<número de red><número de subred><número de host>

La combinación del número de subred y del host suele denominarse «dirección local» o parte «local». La creación de subredes se implementa de forma que es transparente a redes remotas. Un host dentro de una red con subredes es consciente de la existencia de éstas, pero un host de una red distinta no lo es; sigue considerando la parte local de la dirección IP como un número de host.

La división de la parte local de la dirección IP en números de subred y de host queda a libre elección del administrador local; cualquier serie de bits de la parte local se puede tomar para la subred requerida. La división se efectúa empleando una máscara de subred que es un número de 32 bits. Los bits a cero en esta máscara indican posiciones de bits correspondientes al número de host, y los que están a uno, posiciones de bits correspondientes al número de subred. Las posiciones de la máscara pertenecientes al número de red se ponen a 1 pero no se usan. Al igual que las direcciones IP, las máscaras de red suelen expresarse en formato decimal.

El tratamiento especial de «todos los bits a cero» y «todos los bits a uno» se aplica a cada una de las tres partes de dirección IP con subredes del mismo modo que a una dirección IP que no las tiene. Por ejemplo, una red de clase B con subredes, que tiene un parte local de 16 bits, podría hacer uso de uno de los siguientes esquemas:

- El primer byte es el número de subred, el segundo el de host. Esto proporciona 254 (256 menos dos, al estar los valores 0 y 255 reservados) posibles subredes, de 254 hosts cada una. La máscara de subred es 255.255.255.0.
- Los primeros 12 bits se usan para el número de subred, y los 4 últimos para el de host. Esto proporciona 4.094 posibles subredes (4.096 menos 2), pero sólo 14 host por subred. La máscara de subred es 255.25.255.240. Hay muchas otras posibilidades.

Mientras el administrador es totalmente libre de asignar la parte de subred a la dirección local de cualquier forma legal, el objetivo es asignar un número de bits al número de subred y el resto a la dirección local. Por tanto, es corriente usar un bloque de bits contiguos al comienzo de la parte local para el número de subred, ya que así las direcciones son más legibles (esto es particularmente cierto cuando la subred ocupa 8 o 16 bits). Con este enfoque, cualquiera de las máscaras anteriores es buena, pero no máscaras como 255.255.252.252 o 255.255.255.15.

Hay otra dirección de especial importancia: el número de red de clase A con todos los bits a 1, 127, se reserva para la dirección de loopback. Todo lo que se envíe a una dirección con 127 como valor del byte de mayor orden, por ejemplo 127.0.0.1, no debe encaminarse a través de la red, sino directamente del controlador de salida al de entrada.

La mayoría de las direcciones IP se refieren a un sólo destinatario: se denominan direcciones de unicast. Sin embargo, como se ha señalado anteriormente, hay dos tipos especiales de direcciones IP que se utilizan para direccionar a múltiples destinatarios: las direcciones de broadcast y de multicast. Cualquier protocolo no orientado a conexión puede enviar mensajes de broadcast o de multicast, además de los unicast. Un protocolo orientado a conexión sólo puede usar direcciones de unicast porque la conexión existe entre un par específico de hosts.

DNS («DOMAIN NAME SYSTEM»).

El protocolo DNS es un protocolo estándar. Las configuraciones iniciales de Internet requerían que los usuarios emplearan sólo direcciones IP numéricas. Esto evolucionó hacia el uso de nombres de host simbólicos muy rápidamente. Por ejemplo, en vez de escribir TELNET 128.12.7.14, se podría escribir TELNET edum9, y edum9 se traduciría de alguna forma a la dirección IP 128.12.7.14. Esto introduce el problema de mantener la correspondencia entre direcciones IP y nombres de máquina de alto nivel de forma coordinada y centralizada.

Inicialmente, el NIC («Network Information Center») mantenía el mapeado de nombres a direcciones en un sólo fichero (HOSTS.TXT) que todos los hosts obtenían vía FTP. Se denominó espacio de nombres plano. Debido al crecimiento explosivo del número de hosts, este mecanismo se volvió demasiado tosco (considerar el trabajo necesario sólo para añadir un host a Internet) y fue sustituido por un nuevo concepto: DNS («Domain Name System»). Los hosts pueden seguir usando un espacio de nombres local plano (el fichero HOSTS.LOCAL) en vez o además del DNS, pero fuera de redes pequeñas, el DNS es prácticamente esencial. El DNS permite que un programa, ejecutándose en un host, le haga a otro host el mapeo de un nombre simbólico de nivel superior a una dirección IP, sin que sea necesario que cada host tenga una base de datos completa de los nombres simbólicos y las direcciones IP.

EL ESPACIO DE NOMBRES JERÁRQUICO.

Consideremos la estructura interna de una gran organización. Como el jefe no lo puede hacer todo, la organización tendrá que partirse seguramente en divisiones, cada una de ellas autónoma dentro de ciertos límites. Específicamente, el ejecutivo a cargo de una división tiene autoridad para tomar decisiones sin requerir el permiso de su jefe.

Los nombres de dominio se forman de modo similar, y con frecuencia reflejarán la delegación jerárquica de autoridades usada para asignarlos. Por ejemplo, considerar el nombre:

lcs.mit.edu

Aquí, lcs.mit.edu es el nombre de dominio de nivel inferior, un subdominio de mit.edu, que a su vez es un subdominio de edu («education»), conocido como dominio raíz.

El dominio único que se halla sobre la cima no tiene nombre y se le conoce como dominio raíz. La estructura completa se explica en las siguientes secciones.

Cuando se usa el DNS, es común trabajar con sólo una parte de la jerarquía de dominios, por ejemplo el dominio `ral.ibm.com`. El DNS proporciona un método sencillo para minimizar la cantidad de caracteres a escribir en estos casos. Si el nombre de dominio termina en un punto (por ejemplo `wtscpok.itsc.pok.ibm.com.`) se asume que está completo. Es lo que se llama un FQDN («Fully Qualified Domain Name») o nombre absoluto de dominio. Si, sin embargo, no termina en punto, (por ejemplo `wtscpok.itsc`) estará incompleto y el procesador de nombres del DNS, como se verá más abajo, podrá completarlo, por ejemplo, añadiendo un sufijo como `.pok.ibm.com` al nombre de dominio. Las reglas para hacer esto dependen de la implementación y son configurables localmente.

DOMINIOS GENÉRICOS.

A los tres dominios de la cima se les llama dominios genéricos u organizacionales.

edu	Instituciones educativas
gov	Instituciones gubernamentales
com	Organizaciones comerciales
mil	Grupos militares
net	Redes
int	Organizaciones internacionales
org	Otras organizaciones

Puesto que Internet comenzó en los Estados Unidos, la estructura del espacio de nombres jerárquico tenía inicialmente sólo organizaciones estadounidenses en la cima de la jerarquía, y sigue siendo cierto que gran parte de las organizaciones de la cima de la jerarquía son estadounidenses. Sin embargo, sólo los dominios `.gov` y `.mil` están restringidos a los Estados Unidos.

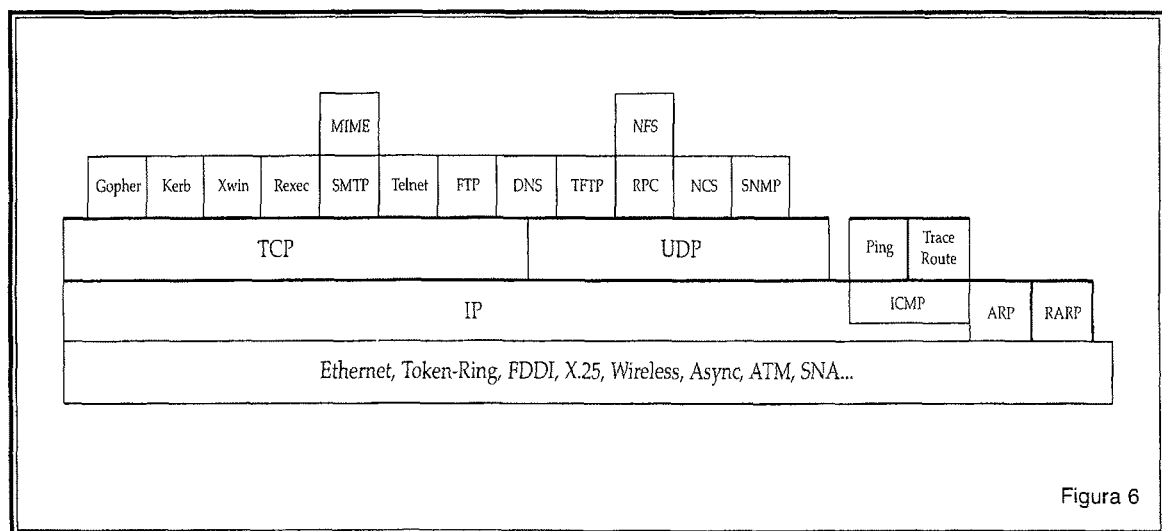
Además, hay dominios de nivel de cima para cada uno de los códigos internacionales de dos caracteres ISO 3166 para países (de `ae` para los Emiratos Árabes Unidos a `zw` para Zimbabwe). Se les conoce como dominios de países o dominios geográficos. Muchos países tienen sus propios dominios de segundo nivel por debajo, paralelamente a los dominios genéricos. Por ejemplo, en el Reino Unido, los dominios equivalentes a `.com` y `.edu` son `.co.uk` y `.ac.uk` («ac» es la abreviatura de «academic»). Está también el dominio `.us`, organizado geográficamente por estados (por ejemplo, `.ny.us` se refiere al estado de New York). El mapeado de nombres a direcciones, proceso denominado resolución de nombres de dominio, lo proporcionan sistemas independientes cooperativos, llamados servidores de nombres. Un servidor de nombres es un programa servidor que responde a peticiones de un cliente llamado procesador de nombres.

El DNS suministra el mapeado de nombres simbólicos a direcciones IP y viceversa. Mientras que en principio es algo sencillo buscar en la base de datos una dirección IP, dado su nombre simbólico, el proceso inverso no se puede hacer respetando la jerarquía. Por este motivo, existe otro espacio de nombres para el mapeado inverso. Se halla en el dominio `in-addr.arpa` («arpa» porque Internet era originalmente la red de ARPA). Como las direcciones IP suelen escribirse en formato decimal con pun-

tos, hay una capa de dominios para cada jerarquía. Sin embargo, debido a que los nombres de dominio tienen primero la parte menos significativa del nombre y el formato decimal con puntos los bytes más significativos primero, la dirección decimal se muestra en orden inverso. Por ejemplo, el dominio del DNS correspondiente a la dirección IP 129.34.139.30 es 30.139.34.129.in-addr.arpa. Dada una dirección IP, el DNS puede utilizarse para encontrar el nombre del host que sea su pareja. Una consulta de nombre de dominio para encontrar los nombres del host asociado a una dirección IP se llama «consulta con puntero».

EL DNS está designado para ser capaz de almacenar una gran cantidad de información. Una de las más importantes es la información del intercambio de correo, usada para el encaminamiento del correo electrónico. Esto aporta dos servicios: transparencia al reencaminar el correo a un host distinto del especificado y la implementación de pasarelas de correo, que pueden recibir correo electrónico y redirigirlo usando un protocolo diferente de aquel con el que lo reciben.

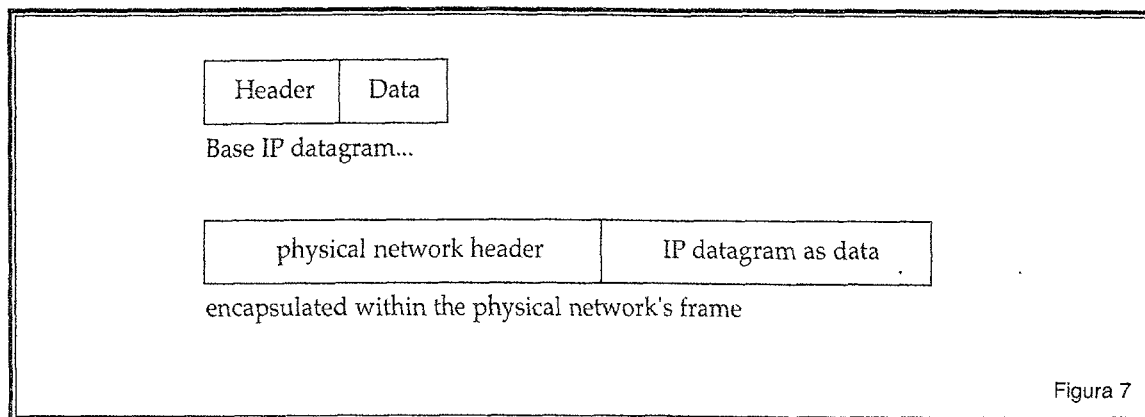
IP («INTERNET PROTOCOL»).



IP es un protocolo estándar con STD 5 que además incluye ICMP e IGMP.

- Su especificación actual se puede encontrar en el RFC 1349.
- IP es el protocolo que oculta la red física subyacente creando una vista de red virtual. Es un protocolo de entrega de paquetes no fiable y no orientado a conexión, y se puede decir que aplica la ley del mínimo esfuerzo.
- No aporta fiabilidad, control de flujo o recuperación de errores a los prots de red inferiores. Los paquetes (datagramas) que envía IP se pueden perder, desordenar, o incluso duplicar, e IP no manejará estas situaciones. El proporcionar estos servicios depende de prots superiores.
- IP asume pocas cosas de las capas inferiores, sólo que los datagramas «probablemente» serán transportados al host de destino.

El datagrama IP es la unidad de transferencia en la pila IP. Tiene una cabecera con información para IP, y los datos relevantes para los protocolos superiores.



El datagrama IP está encapsulado en la trama de red subyacente, que suele tener una longitud máxima, dependiendo del hardware usado. Para Ethernet, será típicamente de 1.500 bytes. En vez de limitar el datagrama a un tamaño máximo, IP puede tratar la fragmentación y el reensamblado de sus datagramas. En particular, el IP no impone un tamaño máximo, pero establece que todas las redes deberían ser capaces de manejar al menos 576 bytes. Los fragmentos de datagramas tienen todos una cabecera, copiada básicamente del datagrama original, y de los datos que la siguen. Se tratan como datagramas normales mientras son transportados a su destino. Nótese, sin embargo, que si uno de los fragmentos se pierde, todo el datagrama se considerará perdido, y los restantes fragmentos se considerarán perdidos.

Cuando un datagrama IP viaja de un host a otro puede cruzar distintas redes físicas. Las redes físicas imponen un tamaño máximo de trama, llamado MTU («Maximum Transmission Unit»), que limita la longitud de un datagrama. Por ello, existe un mecanismo para fragmentar los datagramas IP grandes en otros más pequeños, y luego reensamblarlos en el host de destino. IP requiere que cada enlace tenga un MTU de al menos 68 bytes, de forma que si cualquier red proporciona un valor inferior, la fragmentación y el reensamblado tendrán que implementarse en la capa de la interfaz de red de forma transparente a IP. 68 es la suma de la mayor cabecera IP, de 60 bytes, y del tamaño mínimo posible de los datos en un fragmento, 8 bytes. Las implementaciones de IP no están obligadas a manejar datagrama sin fragmentar mayores de 576 bytes, pero la mayoría podrá manipular valores más grandes, típicamente ligeramente más de 8192 bytes, o incluso mayores, y raramente menos de 1.500.

Una función importante de la capa IP es el encaminamiento. Proporciona los mecanismos básicos para interconectar distintas redes físicas. Esto significa que un host puede actuar simultáneamente como host normal y como router. Un router básico de este tipo se conoce como router con información parcial de encaminamiento, ya que sólo contiene información acerca de cuatro tipos de destino:

- Los hosts conectados directamente a una de las redes físicas a las que está conectado el router.
- Los host o redes para las se le han dado al router definiciones específicas.
- Los hosts o redes para las que el host ha recibido un mensaje ICMP redirect.
- Un destino por defecto para todo lo demás.

Los dos últimos casos permiten a un router básico comenzar con una cantidad muy limitada de información para ir aumentando debido a que un router más avanzado lance un mensaje ICMP redirect cuando reciba un datagrama y conozca un router mejor en la misma red al que dirigir el datagrama. Este proceso se repite cada vez que un router básico se reinicia. Se necesitan protocolos adicionales para implementar un router completamente funcional que pueda intercambiar información con otros routers en redes remotas. Tales routers son esenciales, excepto en redes pequeñas.

DESTINOS DIRECTOS E INDIRECTOS.

Si el host de destino está conectado a una red a la que también está conectado el host fuente, un datagrama IP puede ser enviado directamente, simplemente encapsulando el datagrama IP en una trama. Es lo que se llama encaminamiento directo.

El encaminamiento indirecto ocurre cuando el host de destino no está en una red conectada directamente al host fuente. La única forma de alcanzar el destino es a través de uno o más routers. La dirección del primero de ellos (el primer salto) se llama ruta indirecta. La dirección del primer salto es la única información que necesita el host fuente: el router que reciba el datagrama se responsabiliza del segundo salto, y así sucesivamente.

Un host puede distinguir si una ruta es directa o indirecta examinando el número de red y de subred de la dirección IP.

1. Si coinciden con una de las direcciones IP del host fuente, la ruta es directa.

El host necesita ser capaz de direccionar correctamente el objetivo usando un protocolo inferior a IP. Esto se puede hacer automáticamente, usando un protocolo como ARP, que se usan en LAN's con broadcast, o estáticamente y configurando el host, por ejemplo, cuando un host MVS tiene una conexión TCP/IP sobre un enlace SNA.

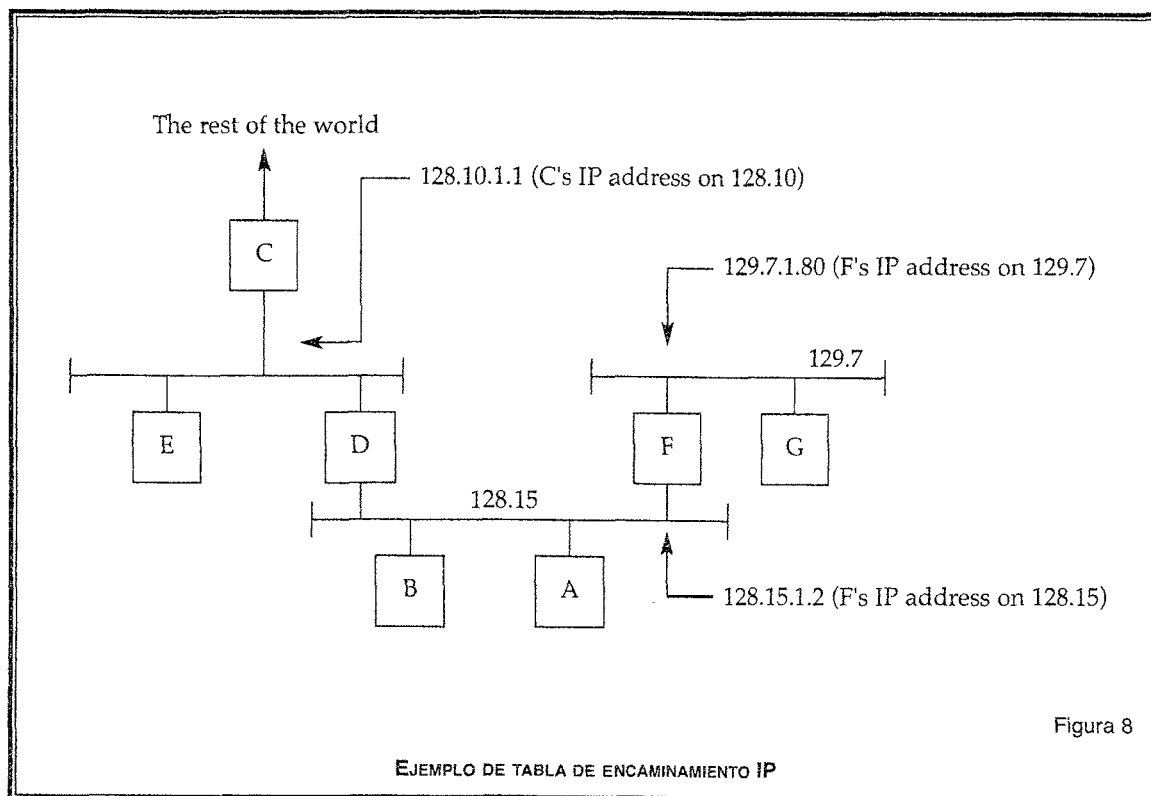
2. Para rutas indirectas, el único conocimiento requerido es la dirección IP de un router que conduzca a la red de destino.

Las implementaciones de IP pueden soportar también rutas explícitas, es decir, una ruta a una dirección IP concreta. En general, sin embargo, la información de encaminamiento se genera sólo mediante los números de red y de subred.

TABLA DE ENCAMINAMIENTO IP.

Cada host guarda el conjunto de mapeados entre las direcciones IP de destino y las direcciones IP del siguiente salto para ese destino en una tabla llamada tabla de encaminamiento IP. En esta tabla se pueden encontrar tres tipos de mapeado:

1. Rutas directas, para redes conectadas localmente.
2. Rutas indirectas, para redes accesibles a través de uno o más routers.
3. Una ruta por defecto, que contiene la IP de un router que todas las direcciones IP no contempladas en las rutas directas e indirectas han de usar.

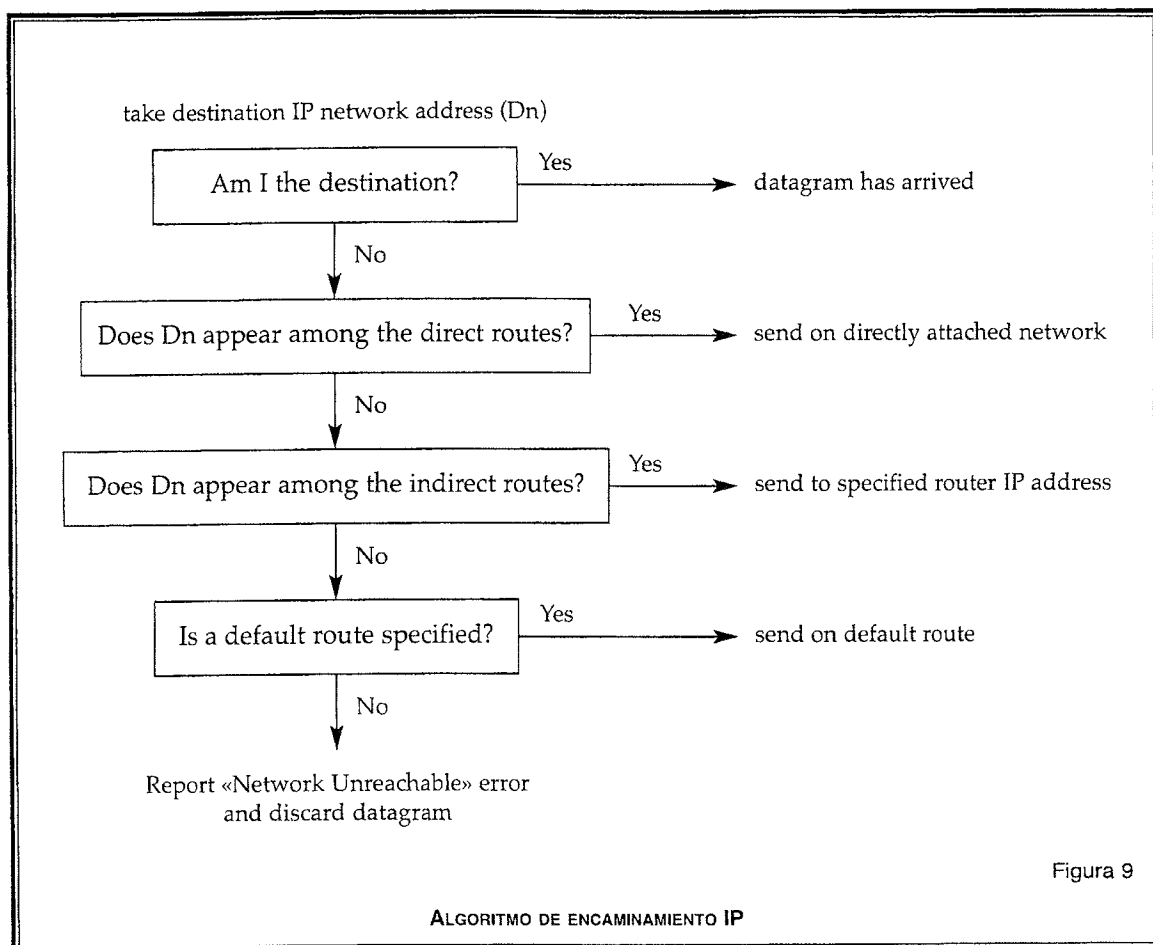


La tabla de encaminamiento contiene las siguientes entradas:

Destination
route via 128.10
direct attachment 128.15
direct attachment 129.7 128.15.1.2
default 128.10.1.1

ALGORITMO DE ENCAMINAMIENTO IP.

De los principios ya comentados de IP, es fácil deducir los pasos que IP debe tomar con el fin de determinar la ruta para un datagrama de salida. Es lo que se denomina algoritmo de encaminamiento IP.



Nótese que se trata de un proceso iterativo. Se aplica a todo host que maneje un datagrama, exceptuando al host al que se entrega finalmente el datagrama.

La función fundamental de encaminamiento está presente en todas las implementaciones de IP:

- Un datagrama IP entrante que especifica una «IP de destino» distinta de la dirección local del host se trata como un datagrama IP saliente normal y corriente.

Este datagrama IP está sujeto al algoritmo de encaminamiento IP del host local, que selecciona el siguiente salto del datagrama (el siguiente host al que se enviará). Este nuevo destino puede estar en cualquiera de las redes físicas con las que el host está conectado. Si es una red física diferente de aquella en la que se recibió el datagrama, resulta que el host que hace de intermediario ha retransmitido el datagrama de una red física a otra.

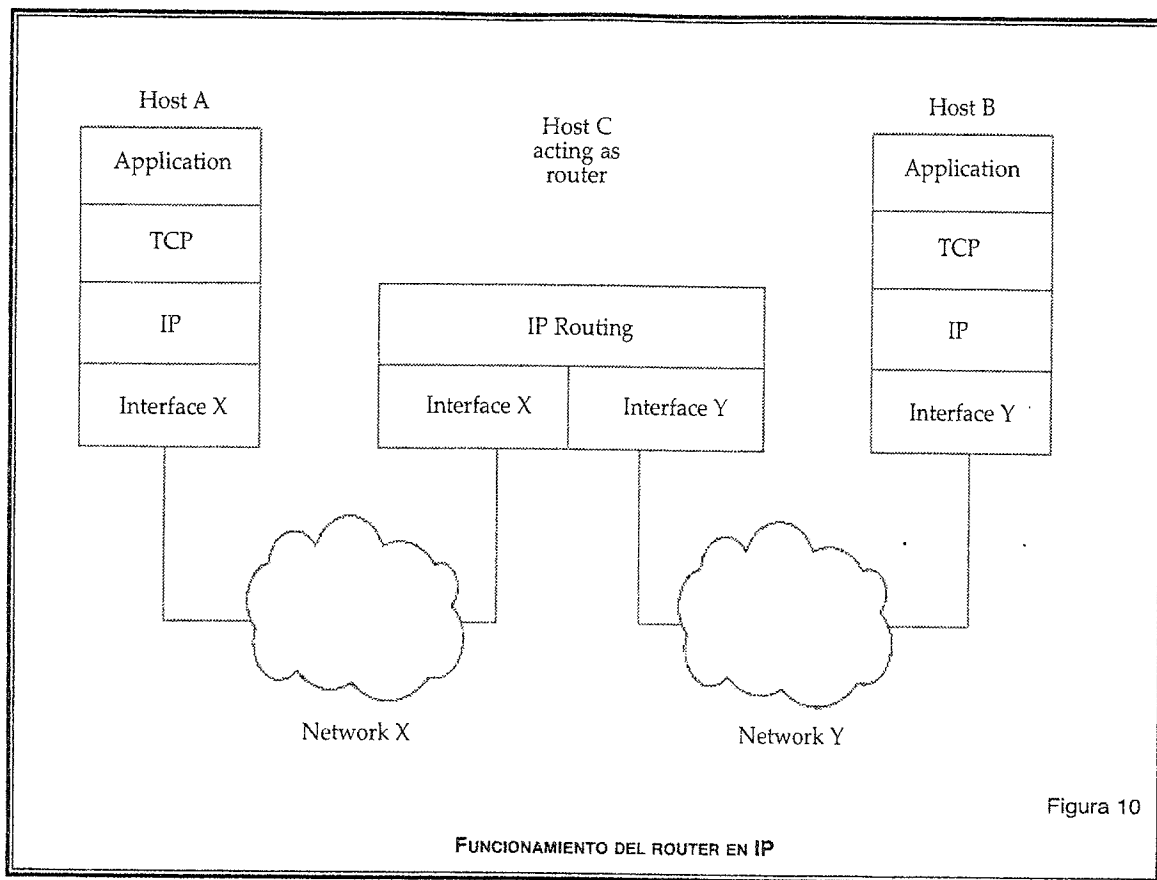


Figura 10

La tabla de encaminamiento IP normal contiene información acerca de las redes conectadas localmente y de las direcciones IP de otros routers localizados en ellas, además de las redes con las que están conectados. Se puede extender con información de las redes IP que se hallan aún más lejos, y tener incluso una ruta por defecto, pero sigue representando una fracción de Internet. Por ello, se le llama router con información parcial de encaminamiento.

A estos routers se les aplican algunas consideraciones:

- No conocen todas las redes de Internet.
- Permiten la autonomía de sitios locales para establecer y modificar rutas.
- Una entrada de encaminamiento errónea en uno de los routers puede introducir inconsistencias, haciendo, por tanto, que parte de la red sea inalcanzable.

Deberían implementar algún mecanismo de informe de errores vía ICMP («Internet Control Message Protocol») descrito en ICMP («Internet Control Message Protocol»). Los siguientes errores deberían poderse enviar al host fuente:

- Destino IP desconocido con un mensaje ICMP Destination Unreachable.
- Redirección del tráfico a routers más adecuados enviando mensajes ICMP Redirect.

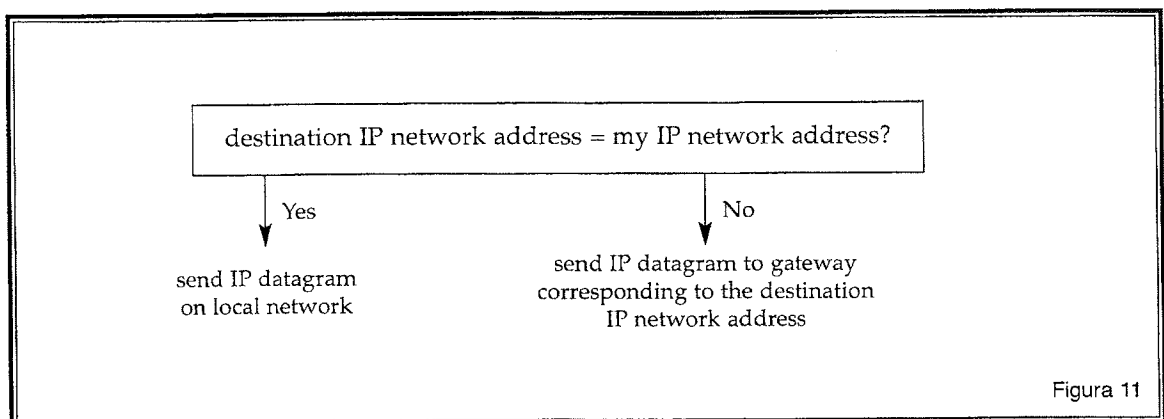
- Problemas de congestión (demasiados datagramas entrantes para el espacio disponible en el buffer) con el mensaje ICMP Source Quench.
- El campo TTL («Time-to-Live») de un datagrama IP ha llegado a cero. Se comunica con el mensaje ICMP Time Exceeded.
- Además, se deberían soportar las siguientes operaciones y mensajes ICMP básicos:
 - Problema de parámetros.
 - Máscara de dirección.
 - TS («Time stamp»).
 - Solicitud/respuesta de información.
 - Solicitud respuesta de eco.

Hace falta un router más inteligente si:

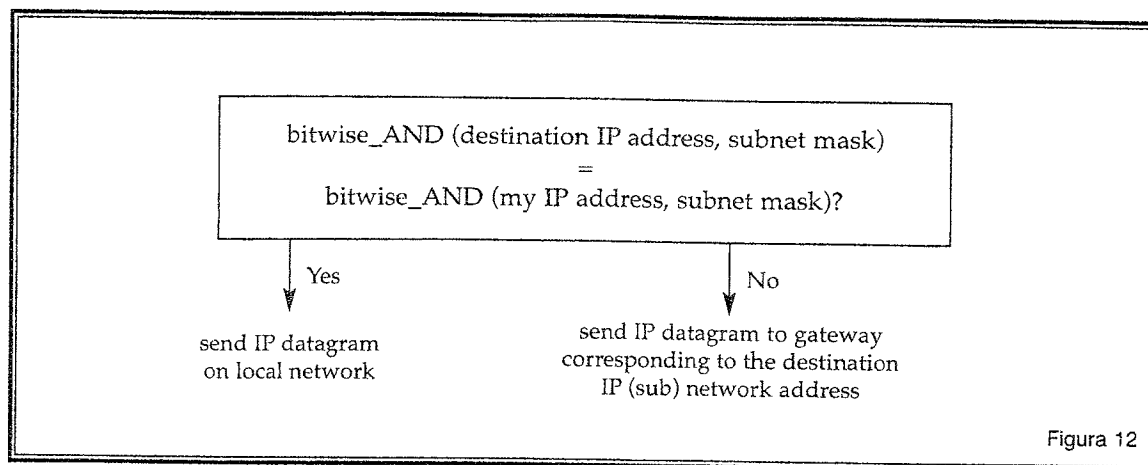
- Ha de conocer las rutas a todas las posibles redes IP, como era el caso de las pasarelas del núcleo de ARPANET.
- El router ha de tener tablas de encaminamiento dinámicas, que se actualizan con poca o ninguna intervención manual.
- El router ha de anunciar los cambios locales a los otros routers.

ENCAMINAMIENTO IP CON SUBREDES.

Para encaminar un datagrama IP en la red, el algoritmo general de encaminamiento IP tiene la forma siguiente:



Para ser capaz de distinguir entre subredes, el algoritmo de encaminamiento IP cambia y adopta la siguiente forma:



Algunas consecuencias de este algoritmo son:

- Es un cambio a algoritmo general. Por tanto, para poder operar de este modo, la correspondiente pasarela debe contener también el nuevo algoritmo. Algunas implementaciones pueden seguir usando el algoritmo general, y no funcionarán dentro de una red con subredes, aunque todavía podrán comunicarse con hosts en otras redes que no empleen «subnetting».
- Ya que el encaminamiento IP se usa en todos los hosts (aunque no en todos los routers), todos los hosts en la subred deben:
 1. Tener un algoritmo IP que soporte «subnetting».
 2. Tener la misma máscara de subred (a menos que existan subredes dentro de la subred).
- Si la implementación de algún host no soporta «subnetting», dicho host sólo podrá comunicarse con hosts de la propia subred, pero no con máquinas que se hallen en otra subred dentro de su misma red. Esto se debe a que el host sólo ve la red IP y su encaminamiento no puede distinguir entre un datagrama IP dirigido a un host de su subred y que se debería enviar a través de un router a una subred diferente.

RFC («REQUEST FOR COMMENTS»).

La pila de protocolos de Internet sigue evolucionando mediante el mecanismo conocido como RFC («Request For Comments»). Los investigadores están diseñando e implementando nuevos protocolos (en su mayoría del nivel de aplicación), que se ponen en conocimiento de la comunidad de Internet en la forma de un RFC. El RFC es descrito por el IAB («Internet Architecture Board»). La mayor fuente de RFC es el IETF («Internet Engineering Task Force») que es una organización subsidiaria del IAB. Sin embargo, cualquiera puede enviar un informe propuesto como RFC al editor de los RFC. Hay una serie de normas que los autores de RFC deben seguir para que su RFC sea aceptado. Estas reglas se describen en un RFC (RFC 1543) que además indica cómo enviar una propuesta de RFC.

Una vez que un RFC ha sido publicado, todas las revisiones y sustituciones se publican como nuevos RFC. Se dice que un nuevo RFC que revisa o sustituye a un RFC ya existente actualiza o desfasa a ese RFC. Asimismo, el RFC original es actualizado o desfasado por el nuevo. Por ejemplo, el RFC 1521 que describe el protocolo MIME es una segunda edición, siendo una revisión del RFC 1341, y el RFC 1590 es una enmienda del 1521. Por tanto, el RFC 1521 se etiqueta del modo siguiente: «Deja obsoleto al RFC 1341; Actualizado por el RFC 1590». En consecuencia, nunca hay confusión sobre si dos personas se refieren a dos versiones distintas de un RFC.

Algunos RFC se califican como documentos informativos mientras que otros describen protocolos de Internet. El IAB («Internet Architecture Board») mantiene una lista de todos los RFC que describen la pila de protocolos. A cada uno de ellos se le asigna un estado y un estatus.

6. PROTOCOLO IPv6.

El problema del agotamiento de las direcciones IP. El número de redes en Internet se ha ido doblando aproximadamente cada año durante varios años. Sin embargo, el uso de las redes de clase A, B y C difiere mucho: la mayoría de las redes asignadas a finales de 1980 eran de clase B, y en 1990 se hizo evidente que, de continuar así la tendencia, el último número de red de clase B sería asignado en 1994. Por otro lado, las redes de clase C apenas se usaban.

La razón de esta tendencia era que la mayoría de los usuarios potenciales hallaban a las redes de clase B lo bastante grandes para sus necesidades previstas, ya que acomoda hasta 65.534 hosts, mientras que una red de clase C, con un máximo de 254 hosts, restringe considerablemente el crecimiento potencial de hasta las redes pequeñas. Es más, la mayoría de las redes de clase B estaban asignadas a redes pequeñas. Hay un número relativamente pequeño de redes que necesiten 65.534 direcciones de hosts, pero muy pocas para que 254 sea un límite adecuado. En resumen, aunque las divisiones de clase A, B y C de las direcciones IP son lógicas y fáciles de usar (puesto que se producen a nivel de byte), en perspectiva no son las más prácticas, ya que las redes de clase C son demasiado pequeñas para la mayoría de las organizaciones mientras que son demasiado grandes para ser bien aprovechadas por nadie, excepto por las organizaciones más grandes.

Las nuevas direcciones son de 128 bits: $3,4 \times 10$ elevado a 38 direcciones distintas ($6,65 \times 10$ elevado a 23 ordenadores por cada metro cuadrado de la superficie terrestre). Las direcciones se escriben en 8 bloques de 16 bits, en hexadecimal, separados por el carácter ":" Pueden omitirse en cada bloque los ceros no significativos: 5A01:0:0:0:8:800:200C:417.^a. Pueden sustituirse las secuencias de bloques consecutivos con los 16 bits a cero en la abreviatura "::". Esto sólo puede hacerse una vez por dirección: 5A01::8:800:200C:417. Con un octeto (ocho bits de la forma 00010111) se pueden representar los números de 0 a 255. Por tanto las direcciones IPv4 se componen de cuatro octetos, o 32 bits, lo cual genera los cuatro millones y pico de direcciones antes mencionadas.

En IPv6 las direcciones se componen de 16 octetos, es decir 128 bits. Esto daría lugar a 2.128 direcciones, más o menos 340 sextillones. No obstante, esta cifra no se alcanza, ya que parte de los dígitos identifican el tipo de dirección, con lo que se quedan en 3.800 millones. En cualquier caso, se garantiza que no se acabarán en un plazo razonable. Hay tres tipos de direcciones: unicast, anycast y multicast. Las direcciones unicast identifican un solo destino. Un paquete que se envía a una dirección unicast llega sólo al ordenador al que corresponda. En el caso de las direcciones anycast se trata de un conjunto de ordenadores o dispositivos, que pueden pertenecer a nodos diferentes. Si se envía un paquete a una de estas direcciones lo recibirá el ordenador más cercano de entre las rutas posibles. Las

direcciones multicast definen un conjunto de direcciones pertenecientes también a nodos diferentes, pero ahora los paquetes llegan a todas las máquinas identificadas por esa dirección. La arquitectura de direccionamiento de IPv6 se describe con detalle en la RFC 2373. Para representar las direcciones IPv6 como cadenas de texto (en lugar de ceros y unos) hay diferentes reglas.

- La primera se denomina preferred form y consiste en listar la dirección completa como 8 números hexadecimales de cuatro cifras (8 paquetes de 16 bits):

FEDC:2A5F:709C:216:AEBC:97:3154:3D12 1030:2A9C:0:0:0:500:200C:3A4

- La otra posibilidad es la forma comprimida o compressed form, en la que las cadenas que sean cero se sustituyen por un par de dos puntos "::" que indican que hay un grupo de ceros. Por ejemplo: FF08:0:0:0:0:0:209A:61 queda F08::209A:61 0:0:0:0:0:0:0:1 queda ::1
- Por último se pueden escribir en forma mixta, con las primeras cifras en hexadecimal y las últimas (las correspondientes a IPv4) en decimal: 0:0:0:0:0:0:193.136.239.163 ::193.136.239.163

Las seis secciones de 16 bits de mayor orden (las de la izquierda) se muestran en hexadecimal, pero el resto se muestra en la familiar notación decimal con puntos.

CARACTERÍSTICAS DE IPv6.

- La nueva versión debe ser capaz de coexistir e interoperar con las especificaciones actuales de IPv4.
- Admite un espacio de direccionamiento exponencialmente mayor que IPv4.
- Los paquetes de IPv6 son más ligeros para facilitar la transmisión por distintos medios.
- IPv6 retiene la mayoría de los conceptos básicos de IPv4.
- Al igual que IPv4, IPv6 es un servicio de entrega de datagramas no confiable y sin conexión.
- El formato de los datagramas en IPv6 es muy diferente al de IPv4.
- IPv6 provee nuevas funcionalidades como autenticación y seguridad.
- IPv6 organiza cada datagrama como una secuencia de encabezados seguida de datos.

Un datagrama siempre comienza con un encabezado base de 40 octetos, el cual contiene las direcciones fuente y destino y un identificador de flujo.

- El encabezado base puede estar seguido de 0 o más encabezados de extensión, seguido de datos.
- Los encabezados de extensión son opcionales; IPv6 los usa para codificar las mayoría de las opciones de IPv4.
- Las direcciones en IPv6 son de 128 bits.
- Las direcciones están divididas en tipos, de manera análoga a las clases en IPv4.

DIFERENCIAS CON LA VERSIÓN 4.

- Capacidad de direccionamiento ampliada.

IPv6 incrementa el tamaño de la dirección desde los 32 bits a los 128 bits, para dar soporte a más niveles de jerarquías de direccionamiento, un mayor número de nodos direccionables, y a una autoconfiguración más sencilla de las direcciones. La escalabilidad del encaminamiento multicast se ve incrementada por la inclusión de un campo «scope» (finalidad) a las direcciones multicast addresses. Y se define un nuevo tipo de dirección denominada «anycast address», usada para enviar un paquete a cualquiera de un grupo de nodos.

- Simplificación del formato de cabecera.

Algunos campos de la cabecera de IPv4 han sido eliminados o convertidos en opcionales para reducir el coste de proceso normal de los paquetes y limitar el coste en ancho de banda de la cabecera IPv6.

- Mayor soporte para extensiones y opciones.

Los cambios en la forma en que se codifican las opciones de la cabecera IP permiten una transmisión más eficiente, menos limitaciones para la longitud de las opciones y mayor flexibilidad para incluir nuevas opciones en un futuro.

- Capacidad de etiquetado de flujo.

Se ha añadido una nueva posibilidad para permitir el etiquetado de paquetes pertenecientes a un determinado «flujo» de tráfico para el que el emisor requiere de un manejo especial, como una calidad diferente de la de por defecto o servicio en tiempo real.

- Utilidades de autenticación y privacidad.

Extensiones para dar soporte de autenticación, integridad de los datos y opcionalmente confidencialidad de los datos.

FORMATO DE CABECERA IPV6.

- Versión. Numero de versión de Internet Protocol (4 bits). Su valor es 6.
- Clase de tráfico. Campo de clase de trafico (8 bits).
- Etiqueta de flujo (20 bits).
- Longitud de carga útil. Entero sin signo de 16 bits. Longitud de la carga útil IPv6, es decir, el resto del paquete que sigue a esta cabecera IPv6, en octetos (notar que cualesquiera de las cabeceras de extensión presente es considerada parte de la carga útil, es decir, incluida en el conteo de la longitud).
- Cabecera siguiente. Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700].
- Límite de salto. Entero sin signo de 8 bits. Decrementado en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el Límite de saltos es decrementado hasta cero.

- Dirección de origen. Dirección de 128 bits del originador del paquete.
- Dirección destino. Dirección de 128 bits del recipiente pretendido del paquete (posiblemente no el último recipiente, si está presente una cabecera Enrutamiento).

Se han mejorado las cabeceras de los paquetes, eliminado algunos campos de la cabecera IPv4, haciendo que otros sean opcionales y utilizando cabeceras de extensión. Las cabeceras de extensión son cabeceras separadas que, con una excepción, no las examina ningún host en la ruta desde el origen al destino, mejorando la eficiencia del enrutamiento.

También permite una mayor flexibilidad en la codificación de opciones y capacidades de expansión para opciones futuras.

En IPv6 se introduce el etiquetado de flujos, lo que permite indicar que los paquetes pertenecen a determinado «flujo» de tráfico. De esta forma se permite manejar QoS y la administración de ancho de banda sin tener que analizar cabeceras de TCP ni de UDP

También se han introducido extensiones que permiten autenticación, asegurar la integridad de los datos y cifrado de paquetes opcional.

En el IPv6, la información de capa Internet opcional se codifica en cabeceras separadas que se pueden colocar entre la cabecera IPv6 y la cabecera de capa superior dentro de un paquete. Hay un número pequeño de tales cabeceras de extensión, cada una identificada por un valor de Cabecera Siguierte distinto. Según esto un paquete IPv6 puede llevar cero, una, o más cabeceras de extensión cada una identificada por el campo Cabecera Siguierte de la cabecera precedente.

