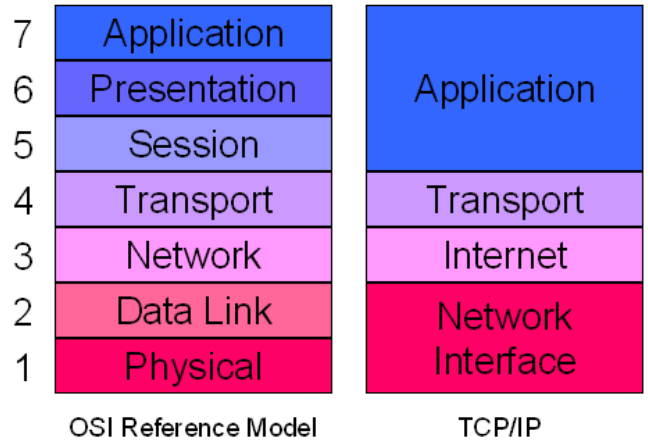
Funcionamiento del protocolo TCP/IP

TCP/IP es el protocolo de red más utilizado hoy en día. Para abordar su funcionamiento básico lo contrastaremos con el modelo de referencia OSI.

TCP/IP no es realmente un solo protocolo, sino un conjunto de protocolos distribuidos en diferentes pilas de protocolos. Su nombre hace referencia a sus dos protocolos principales, TCP (Transmission Control Protocol) e IP (Protocolo de Internet). Hay otros protocolos relacionados con TCP/IP, como FTP, HTTP, SMTP y UDP, sólo para nombrar los más populares.

Arquitectura de TCP / IP



Como se observa, en este caso y por simplicidad adoptaremos un modelo TCP/IP de **cuatro** capas (una variante de la bibliografía tradicional de 5 capas). El **software** específico de comunicaciones se comunica con la **capa de aplicación** en donde se encuentran los protocolos de aplicación tales como **SMTP** (correo electrónico), **FTP** (transferencia de archivos) y **HTTP** (navegación web). Cada **tipo** de programa se comunica con un **protocolo de aplicación diferente**, dependiendo de la finalidad del mismo.

Después de procesar la solicitud del programa, el protocolo de la capa de aplicación invocado se comunicará con algún protocolo de la capa de transporte, por lo general **TCP**. Esta capa se encarga de tomar los datos que vienen de la capa superior, dividirlos en bloques y enviarlos a la capa inferior, la de **Internet**. En la recepción de datos, esta capa se encarga de enviar los paquetes a la capa superior, recibidos desde la **red**, en orden (ya que pueden ser recibidas fuera de orden) y también comprobar si los contenidos están intactos.

En la capa de **Internet** tenemos el protocolo **IP** (Protocolo de Internet), el cual toma los paquetes entregados por la capa de transporte y añade información tal como la dirección virtual (lógica), es decir, añade la dirección del equipo que envía los datos y la dirección del equipo que va a recibir estos datos. Estas direcciones virtuales se denominan **direcciones IP**. Luego, el paquete se envía a la capa inferior, de **Interfaz de Red**. En esta capa, la de **Internet**, los bloques de mensajes se denominan **datagramas**.

La interfaz de red obtendrá los datagramas de la capa de de Internet y procede a enviarlos por la red (o recibirlos de la red, si el equipo es el receptor). El funcionamiento de esta capa dependerá del tipo de red al que equipo esté utilizando. Hoy en día casi todos los equipos utilizan la tecnología **Ethernet** (que está disponible en variedad de velocidades diferentes o las redes inalámbricas que son también redes Ethernet) y por lo tanto se encuentran en esta capa las que corresponden a esta tecnología (IEEE 802), que son la de Control Lógico de Enlace (LLC), la de Control de Acceso a medios (MAC) y la Física. Los bloques transmitidos por la red se denominan **tramas**.

La Capa de aplicación

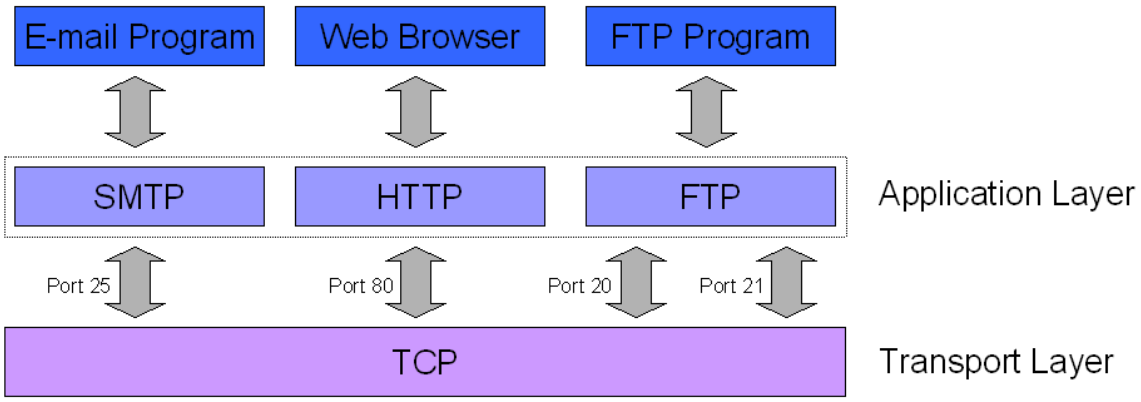
Esta capa establece la comunicación ***entre los programas y los protocolos de transporte.*** Hay varios protocolos diferentes que trabajan en la capa de aplicación. Los más conocidos son HTTP (HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol), DNS (Domain Name System) y Telnet entre otros.

Cuando por ejemplo, un *programa* de correo electrónico (denominado cliente de correo electrónico) descarga mensajes desde la casilla de correo desde un servidor de correo, solicitará esta tarea a la capa de aplicación TCP/IP, en la que se encuentra el protocolo SMTP. Cuando se escribe una dirección web en el navegador para acceder a una página web, el navegador solicitará esta tarea a la capa de aplicación TCP/IP, a través del protocolo HTTP y así según la necesidad de la aplicación.

La interacción de la capa de *aplicación* con la capa de *transporte* se hace a través de un **puerto**. Los puertos están numerados y **las aplicaciones estándar siempre utilizan el mismo puerto**. Por ejemplo, el protocolo SMTP utiliza siempre el puerto 25, el protocolo HTTP el puerto 80 y protocolo FTP utilice siempre los puertos 20 (para la transmisión de datos) y 21 (para el control).

El uso de un *número de puerto* permite el protocolo de transporte (normalmente TCP) saber qué *tipo de contenidos* se encuentra dentro del paquete (por ejemplo, para

saber que los datos sean transportados son de correo) que le permite saber del lado de recepción a que el protocolo de aplicación deberá entregar los datos recibidos. Así, cuando se recibe un paquete en el puerto 25, el protocolo TCP sabrá que debe entregar los datos al protocolo conectado a este puerto, por lo general SMTP, que a su vez entregará los datos al programa que lo solicitó (el programa de correo electrónico).



La Capa de Transporte

Cuando se envían datos, la capa de transporte toma los datos de la capa de aplicación y los divide en varios bloques. TCP (Transmission Control Protocol) es el protocolo más utilizado en la capa de transporte. En la recepción de datos, el protocolo **TCP** recibe los paquetes enviados desde la capa de Internet y **los ordena**, ya que pueden llegar al destino fuera de orden, y también **comprueba** si el contenido de cada paquete recibido está intacto para luego enviar una **señal de reconocimiento al transmisor**, lo que le permite saber que el paquete correctamente al destino. Si no se recibe ninguna confirmación (ya sea porque no llegó al destino o porque TCP encontró datos con error), el transmisor volverá a enviar el paquete perdido.

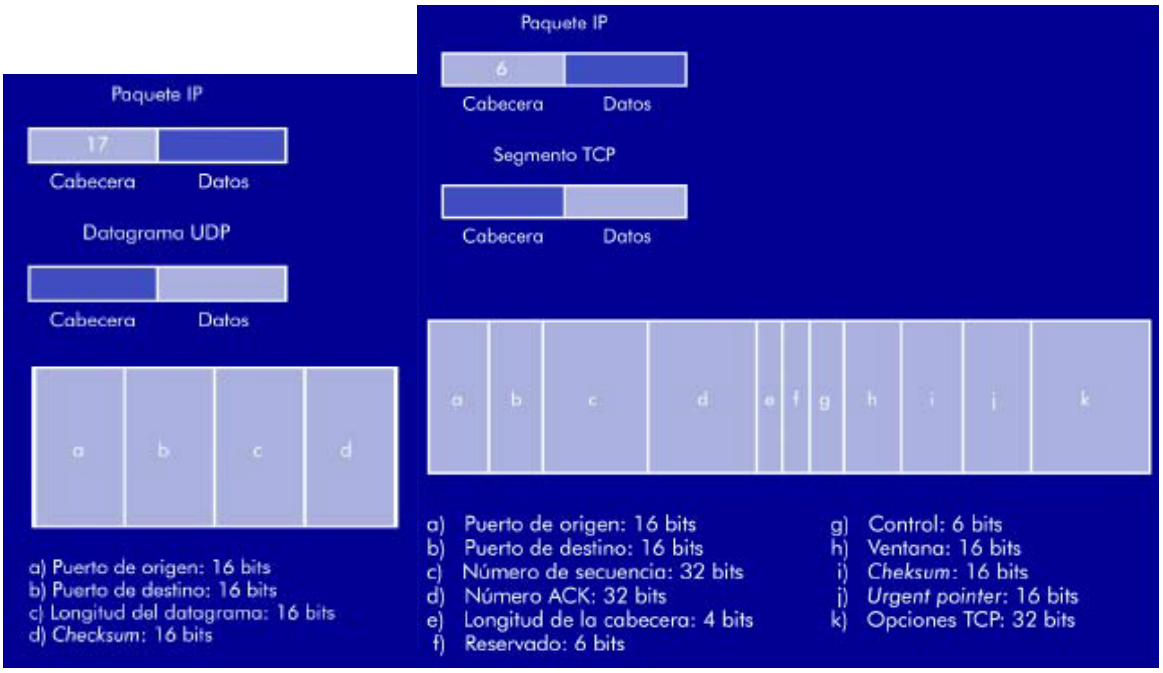
Mientras TCP reordena los paquetes y usa el sistema de confirmación que se mencionó, lo cual es deseable cuando se transmiten datos, hay otro protocolo que funciona en esta capa que **no tiene estas dos características**. Este protocolo se llama **UDP** (User Datagram Protocol).

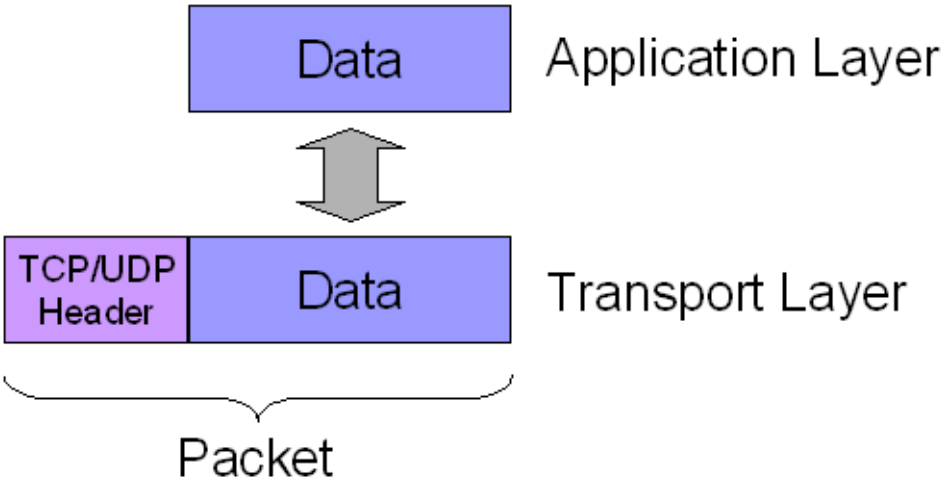
Por lo tanto TCP se considera un protocolo **fiable**, mientras que UDP es considerado un protocolo **no fiable**. UDP se utiliza normalmente cuando se transmiten datos no importantes, por lo general consultas DNS (Domain Name System). Debido a

que no implementa la reordenación ni un sistema de confirmación, **UDP es más rápido que TCP**.

Cuando se utiliza **UDP**, la **aplicación** que solicitó la transmisión **se encargará de comprobar si llegaron los datos y si están intactos o no, así como también reordenar los paquetes recibidos**, es decir, la aplicación *realiza la tarea de TCP*.

Ambos UDP y TCP obtendrán los datos de la capa de Aplicación y los pasará a la de Internet, agregando un encabezado cuando envían datos. En la recepción, la cabecera se eliminará antes de enviar datos al puerto adecuado. En esta cabecera hay información de **control**, en particular el **número de puerto de origen, el número de puerto de destino**, un número de **secuencia** (para el reconocer y sistemas de reordenación utilizadas en TCP) y una **suma de comprobación**. La cabecera UDP tiene 8 bytes mientras cabecera TCP tiene 20 o 24 bytes (si el campo de opciones no es utilizado).





La Capa de Internet

En las redes TCP/IP cada equipo (host) se identifica con una **dirección virtual única** denominada **dirección IP**. La capa de Internet se encarga de añadir una cabecera al paquete de datos que le llega desde la capa de transporte en la que, entre otros datos de control, agregará la dirección IP de origen y de destino.

La placa de red (NIC) de cada equipo tiene una dirección física asignada. Esta dirección está escrita en la memoria ROM de la placa de red y se denomina dirección MAC. Así que en una *red de área local* siempre que un equipo A quiera enviar datos al B, tendrá que conocer la dirección MAC del mismo. Mientras que en una red LAN se puede averiguar fácilmente la dirección MAC de cada equipo, esto no es una tarea simple en una red WAN de alcance mundial como lo es Internet.

Si no se usaran direcciones lógicas (virtuales), se tendría que conocer la dirección MAC del equipo de destino, tarea difícil que tampoco ayuda a fines del enrutamiento de paquetes, ya que no utiliza una estructura Red/Host. En otras palabras, mientras que las direcciones virtuales en los equipos de la misma red tendrán direcciones secuenciales, si se utilizaran direcciones MAC para cada equipo, la siguiente dirección MAC podría estar en otro país, por ejemplo.

El **enrutamiento** o ruteo es la **ruta que un paquete de datos debe utilizar para llegar al destino**. Al solicitar los datos desde un servidor de Internet, estos datos pasan por varios equipos intermedios (llamados enrutadores o routers) antes de llegar al equipo local. Si se quiere verificar esto, se puede probar desde la consola de Windows. En el símbolo del sistema escriba el comando “tracert www.google.com” en la consola. El

resultado será una lista del camino entre su equipo y el servidor web de Google. Se puede ver como el paquete de datos pasa a través de varios routers diferentes antes de llegar a su destino. Cada router en el medio de la carretera también se llama *salto (hop)*.

Cada red que está conectada a Internet a través un equipo llamado **router**, que hace de **puente entre los equipos de la red LAN e Internet**. Cada router tiene una tabla con sus redes conocidas (las que tiene por cada puerto físico de entrada/salida) y también una configuración llamada ***puerta de enlace predeterminada*** que señala a otro router en Internet. Cuando el equipo envía un paquete de datos a Internet, el router conectado a la red primero mira si conoce al equipo de destino, en otras palabras, si el equipo de destino se encuentra en la misma red o en una red conocida. Si no, se enviará el paquete a su puerta de enlace predeterminada, es decir, a otro router. A continuación, el proceso se repite hasta que el paquete de datos llegue a su destino.

Hay varios protocolos que funcionan en la capa de Internet: IP (Protocolo de Internet), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol) y RARP (Reverse Address Resolution Protocol). **Los paquetes de datos se envían a través del protocolo IP**.

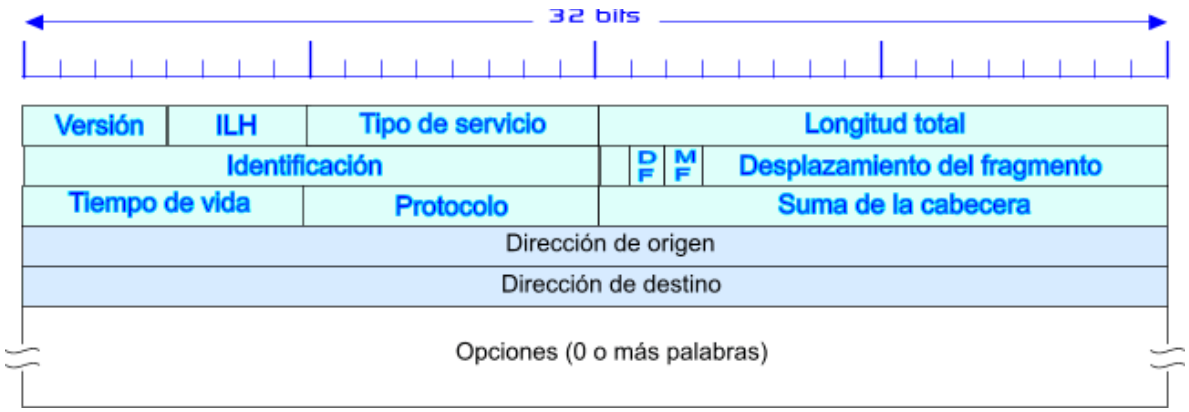
El protocolo IP toma los bloques de la capa de transporte (TCP si está transmitiendo datos tales como correos electrónicos o archivos) y los divide en datagramas. Un **Datagrama es un paquete que no tiene ningún tipo sistema de confirmación**, lo que significa que **IP** no lo implementa siendo de esta manera un protocolo no fiable.

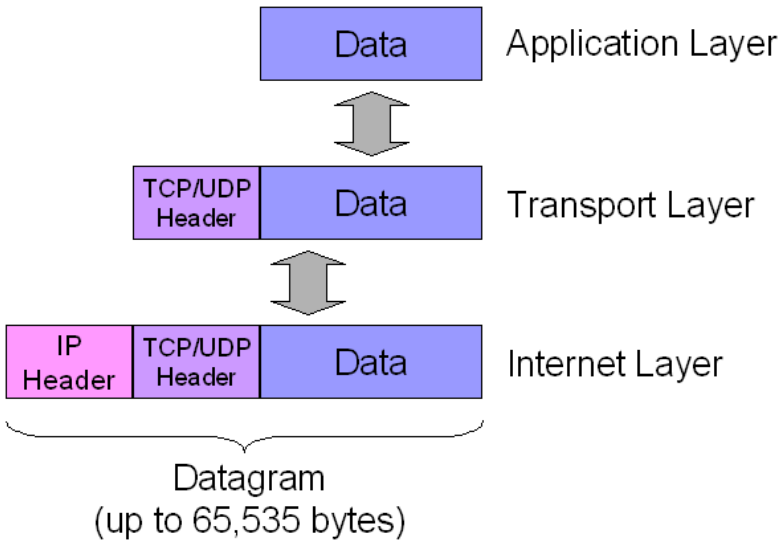
Se debe notar que cuando se utiliza en la capa de transporte el protocolo TCP es justamente éste quien controla las confirmaciones. Por lo tanto, aunque el protocolo IP no comprueba si el datagrama llega a su destino, el protocolo TCP sí lo hará. La conexión será entonces fiable, a pesar de protocolo IP por sí solo no es fiable.

Cada **datagrama IP** puede tener un **tamaño máximo de 65.535 bytes**, incluyendo su cabecera, que puede utilizar 20 o 24 bytes, dependiendo de si un campo llamado "opciones" se utiliza o no. De esta forma los datagramas IP pueden transportar hasta 65,515 o 65,511 bytes de datos. Si el paquete de datos recibido desde la capa de transporte es mayor que 65,515 o 65,511 bytes, el protocolo IP utilizará tantos datagramas como sean necesarios.

Es interesante notar que lo que la capa de Internet ve como "datos" es el bloque que le llegó desde capa de transporte, que incluye la cabecera TCP o UDP. Este datagrama se enviará a la capa de interfaz de red (si estamos transmitiendo datos).

Como mencionamos, la cabecera añadida por el protocolo IP incluye la dirección IP de origen, la dirección IP de destino y datos de control adicionales.





Si se presta atención, el datagrama IP puede tener un máximo de 65.535 bytes. Esto significa que el campo de datos del datagrama no tiene un tamaño fijo. Ya que los datagramas se envían por la red dentro de las tramas que genera la capa de **Interfaz de Red**, por lo general el sistema operativo configurará el tamaño para maximizar el campo de datos de los datagramas IP. El tamaño máximo del campo de datos de las **tramas** que se envían a través de la red se denomina **MTU**, Maximum Transfer Unit.

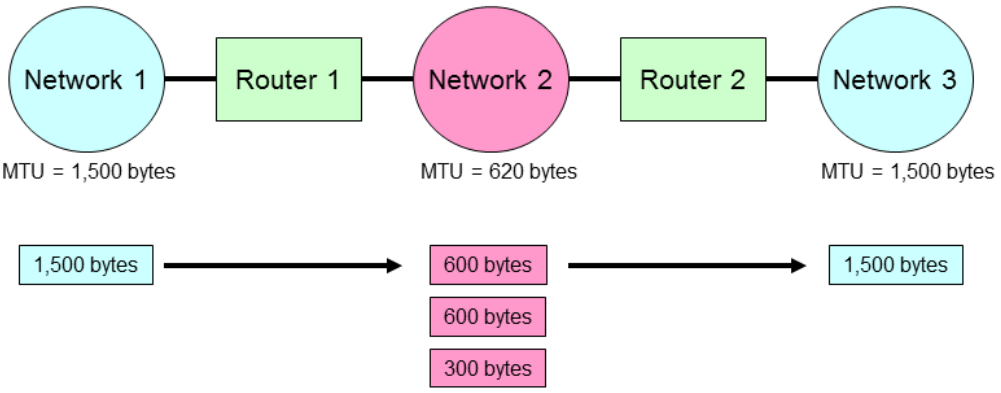
Las redes **Ethernet**, que son el tipo más común de red disponible incluyendo su variante inalámbrica, pueden transportar hasta 1.500 bytes de datos, es decir, su MTU es de 1.500 bytes. Entonces por lo general el sistema operativo configura automáticamente el protocolo IP para crear datagramas IP que son 1.500 bytes de longitud, en lugar de 65535. En la siguiente sección se verá que el tamaño real es de 1.497 o 1.492 bytes, ya que la capa LLC usa 3 o 5 bytes para añadir su encabezado.

Una aclaración, *puede haber una confusión acerca de cómo una red puede ser clasificada como TCP/IP y Ethernet al mismo tiempo*. TCP/IP es un conjunto de protocolos que se ocupa de las capas 3 a 7 del modelo de referencia OSI. Ethernet es un conjunto de protocolos que se ocupa de las capas 1 y 2 del modelo de referencia OSI (IEEE 802), significando esto que Ethernet trata con el aspecto físico de la transmisión de datos. Así que se complementan entre sí, ya que necesitamos de las siete capas (o sus equivalentes) para establecer una conexión de red.

Otra característica que permite el protocolo IP es la fragmentación. Como se comentó, hasta llegar a su destino, el datagrama IP probablemente atraviese otras redes en su camino (ruta). Si todas las redes en la ruta entre el equipo de transmisión y el de recepción usan del mismo tipo de red (por ejemplo, Ethernet), entonces la proceso se simplifica, ya que todos los routers funcionan con la misma estructura de trama (es decir, el mismo tamaño MTU).

Sin embargo, si esas otras redes no son redes Ethernet entonces pueden utilizar un tamaño de MTU diferente. Si eso ocurre, el router que está recibiendo las tramas con MTU de 1.500 bytes cortará el datagrama IP como sea necesario con el fin de adaptarlo a una red con el tamaño de MTU pequeña. Al llegar a otro router que tiene su salida conectada a una red Ethernet, este router volverá a armar el datagrama original.

La trama original utiliza una MTU de 1500 bytes. Cuando se llega a una red con



un tamaño de MTU de 620 bytes, cada trama tiene que ser dividida en tres partes (dos

con 600 bytes y una con 300 bytes). Luego el router a la salida de esta red (router 2) vuelva a armar el datagrama original.

Por supuesto, la cabecera IP tiene un campo para controlar la fragmentación.

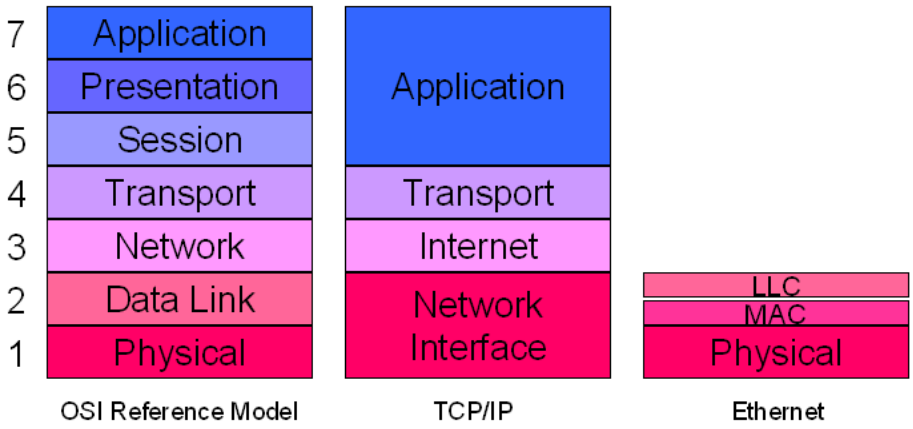
La Capa de interfaz de red

Los datagramas de la capa de **Internet** se pasan a la capa de Interfaz de Red en la transmisión, o se toman desde la capa de Interfaz de en la recepción de datos.

Esta capa **se define por el tipo de red física** al está conectado el equipo. Casi siempre será una red **Ethernet** (las redes inalámbricas son también redes Ethernet).

Como se mencionó con anterioridad, TCP/IP es un conjunto de protocolos que abarca de las capas 3 a 7 del modelo de referencia OSI, mientras que Ethernet es un conjunto de protocolos que se ocupa de las capas 1 y 2 del modelo de referencia (IEEE 802).

Ethernet tiene tres capas: Control Lógico de Enlace (LLC), Control de Acceso al Medio (MAC) y Física. Las capas LLC y MAC corresponden a la segunda del modelo de referencia OSI.



La capa de Control Lógico de Enlace (**LLC**) es la encargada de la agregar información acerca de qué protocolo se está usando en la capa de superior o de Internet, por lo que al recibir una trama de la red el equipo receptor tiene que saber a qué protocolo de Internet debe entregar los datos (IEEE 802.2)

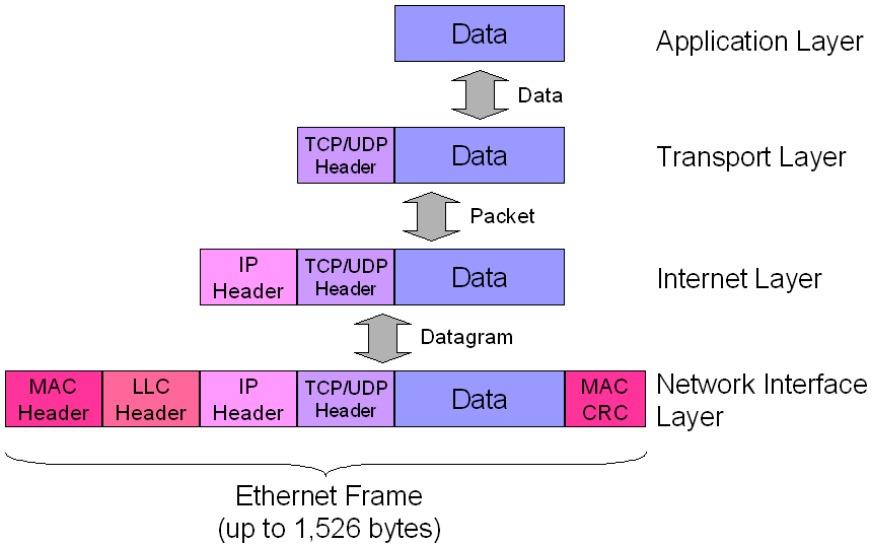
La capa de Control de Acceso al Medio (**MAC**) está a cargo del ensamblado de la trama que se envía a través de la red. Esta capa se encarga de agregar la dirección MAC de origen y destino (dirección MAC es la dirección física de la placa de red NIC). Las tramas que están dirigidas a otra red utilizaran la dirección MAC del router como dirección

de destino. Esta capa está definida en IEEE 802.3 si se está utilizando una red cableada, o por IEEE 802.11 si se está utilizando una red inalámbrica.

La capa F**ísica** es responsable de la conversión de la trama generada por la capa MAC en una señal (si se está utilizando una red cableada o sea generar el código de línea correspondiente) o en ondas electromagnéticas (si se está utilizando una red inalámbrica). Esta capa (física) también se define por el protocolo IEEE 802.3 si se está utilizando una red cableada, o por IEEE 802.11 si se está utilizando una red inalámbrica.

Las capas LLC y MAC añaden sus propias cabeceras a los datagramas que reciben de la capa de Internet. Así una estructura completa de las tramas generadas por estas dos capas se puede en la figura siguiente. Obsérvese que las cabeceras agregadas por las capas superiores se ven como "datos" por la capa LLC. Lo mismo ocurre con la cabecera introducida por la capa LLC, que se verá como los datos de la capa MAC.

La capa LLC añade una cabecera de 3 o 5 bytes y su datagrama tiene un tamaño máximo total de 1.500 bytes, dejando un máximo de 1.497 o 1.492 bytes para los datos. La capa MAC añade una cabecera de 22 bytes y un campo de 4 bytes para CRC (detección de errores) al final del datagrama recibido desde la capa LLC, formando la trama Ethernet. Así, el tamaño máximo de una trama Ethernet es de 1.526 bytes.

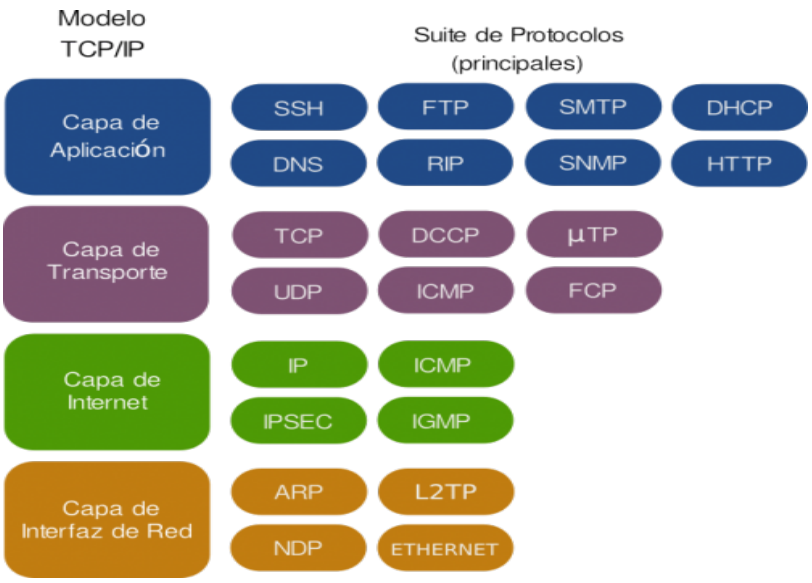


Otros protocolos

Introducción

Hasta ahora se ha descripto la arquitectura básica del protocolo TCP/IP y sus protocolos principales (como TCP, UDP e IP). Ahora es el momento profundizar un poco más explicando otros protocolos y otras funcionalidades TCP/IP que no cubrimos antes, como Telnet, SSH, TFTP, DHCP, DNS, ICMP, RIP, OSPF, BGP, ARP y más.

Es importante tener en cuenta que hay varios otros protocolos relacionados con la pila TCP/IP y sólo se comentan los más importantes.



Servicios de Terminal

Los servicios de Terminal o Consola Remota, permiten acceder de forma remota a un servidor y tener acceso a su Shell (es decir, a su línea de comandos o consola) como si se estuviera personalmente frente al teclado y monitor. Los tres protocolos de terminal más comunes son Telnet, rlogin y SSH (Secure Shell). Todos hacen lo mismo, pero las conexiones SSH están encriptadas y por lo tanto son más seguras. Si se tiene que administrar un servidor de forma remota es preferible usar SSH en lugar de telnet o rlogin, ya que las conexiones Telnet y rlogin no están cifradas y un intruso, utilizando un programa "sniffer" (que es un tipo de programa que permite a un hacker leer los paquetes que están siendo transitando por la red) pueda leer todo lo que escriba, incluyendo contraseñas.

Telnet, rlogin y SSH son protocolos de capa de aplicación y usan TCP en la capa de transporte, Telnet utiliza el puerto 23, Rlogin el puerto 513 y SSH el puerto 22.

Uno de los programas clientes más famosos de este tipo permite realizar Telnet, rlogin y conexiones SSH es PuTTY (Windows viene con una utilidad de Telnet pero no viene con un SSH).

TFTP (Trivial File Transfer Protocol)

En la primera parte de este apunte se ha comentado sobre FTP, un protocolo de capa de aplicación para la transferencia de archivos mediante el uso de TCP en la capa de transporte.

TFTP es un protocolo para el mismo tipo de aplicación - la transferencia de archivos - pero basado en el protocolo UDP en la capa de transporte.

Como se recordará, la diferencia entre TCP y UDP es que mientras que TCP comprueba si cada paquete de datos llegó correctamente a destino, UDP no lo hace. Otra diferencia es que TCP puede reordenar los paquetes que lleguen fuera de orden mientras que UDP no lo hace.

Como no se utiliza un sistema de reconocimiento ni de reordenación, los paquetes UDP son más pequeños (la cabecera UDP es más pequeña que la cabecera TCP) y también requieren menos potencia de cálculo para ser procesados, no hay que reordenar ni confirmar. **Será entonces la aplicación y no el protocolo, la que estará a cargo de estas funciones a nivel superior**.

Para uso corriente el protocolo TFTP no es útil como lo es FTP, que es fiable. Sin embargo, hay un tipo de aplicación que utiliza TFTP: el Inicio Remoto sin disco (también conocido como RIPL, Remote Initial Program Loading).

Se puede tener un equipo sin unidad de disco y configurarlo para que arranque desde la red, es decir, cargar el sistema operativo y los programas desde un servidor. El programa para cargar el sistema operativo de forma remota necesita estar almacenado en una memoria ROM muy pequeña que se encuentra en la NIC de este equipo sin disco. Como se necesita un protocolo para la transferencia de archivos, TFTP se adapta mejor que FTP, ya que los clientes TFTP son mucho más pequeños que los clientes FTP. Para tener una idea, el tamaño de las ROM más grandes es de sólo 64 KB.

En resumen, TFTP es un protocolo de capa de aplicación que usa UDP (a través del puerto 69) en la capa de transporte.

DHCP (Dynamic Host Configuration Protocol)

Todos los equipos conectados a una red TCP/IP deben configurarse con una dirección IP, sin esta no se pueden comunicar con otro equipo de la red.

Imagínese una gran red con cientos de equipos. Configurarlos uno por uno sería caótico y tedioso. Además, considérese a los proveedores de servicios de Internet (ISP): tendrían que instruir a todos sus clientes acerca de cómo configurar su equipo y asignarles direcciones IP por teléfono, por ejemplo, y realizar un seguimiento de estas direcciones, ya que dos equipos no pueden tener la misma dirección IP.

Con el fin de hacer más fácil esta configuración, existe un protocolo llamado DHCP, que permite que los equipos reciban su configuración a través de un servidor DHCP. Esta es la configuración por defecto para la mayoría las computadoras en la actualidad. Así que cuando se enciende una computadora, se pide al servidor DHCP de su red una dirección IP y entonces el equipo estará configurado. Si se ha construido una pequeña red con un router de banda ancha (NAT), el router también incorpora un servidor DHCP, por lo que será el encargado de asignar direcciones IP a los equipos conectados a él.

Además de la dirección IP que asigna el servidor DHCP, también envía **otra** información de configuración, como la dirección IP del servidor DNS que su computadora deberá utilizar (se explicará más adelante), la puerta de enlace predeterminada (la dirección IP del router de su red, es decir, si el equipo no puede encontrar el destino en su red local enviará el datagrama a esta dirección y la máscara de subred que se utiliza para fines de ruteo.

Usando un servidor DHCP el administrador de red puede configurar todos los equipos de una red desde una ubicación central.

DHCP es un protocolo de capa de aplicación, que usa el protocolo UDP en la capa de transporte. Se utiliza los puertos 67 y 68. DHCP sustituye un viejo protocolo llamado BOOTP. Todo lo que se dice acerca de BOOTP es válida para DHCP, DHCP es 100% compatible con BOOTP (DHCP ofrece más opciones que BOOTP).

DNS (Domain Name System-Sistema de Nombres de Dominio)

Como se sabe, en las redes TCP/IP cada equipo tiene una dirección virtual única, denominada dirección IP. Sin embargo, para el corriente de los seres humanos, los nombres son más fáciles de recordar que los números.

DNS permite usar nombres como **alias** de las direcciones IP. Por ejemplo, es más fácil de memorizar el nombre de un sitio web que su dirección IP.

Cuando se escribe un nombre en la barra de direcciones del navegador web, el protocolo DNS entra en acción y se contacta con un servidor DNS para pedirle la dirección IP asociada al nombre (URL – Uniform Resource Locator). El servidor DNS responderá con la IP solicitada a usar en esa conexión.

El servidor DNS que el navegador web usará es el servidor DNS configurado en el equipo, todos los equipos que están conectados a Internet tienen un campo para la configuración de la dirección IP de al menos un servidor DNS. Por lo general, esta configuración se realiza automáticamente por medio de DHCP.

Si el servidor DNS no reconoce el nombre que solicitado, se pondrá en contacto con otro servidor DNS con una jerarquía superior con el fin de averiguar la relación nombre/dirección que se pidió.

Todas las entradas en los servidores de DNS tienen un campo "tiempo de vida" (también conocido como TTL), que le dice al servidor por cuánto tiempo la información es válida. Cuando ha caducado dicha información debe actualizarse contactando nuevamente un servidor DNS con una jerarquía superior.

DNS es un protocolo de capa de aplicación y las consultas DNS se realizan a través del puerto UDP 53 en la capa de transporte. Como se ha explicado, UDP no comprueba si el paquete llegó o no a destino pero, por otro lado, es más rápido.

Una manera fácil de jugar con las consultas DNS es a través del uso del comando **nslookup**, disponible tanto en el símbolo de sistema de Windows como en los sistemas Unix (en Linux, dependiendo de su distribución este comando se puede llamar host y no nslookup).

Se puede probar en Windows usando nslookup con un nombre (url) y con una dirección IP pública

Por cierto, el protocolo DNS permite que más de un nombre se asocie con una dirección IP determinada. Esto le permite alojar más de un sitio web en un único servidor, por ejemplo. Cuando acceda a un servidor que tiene más de un sitio web alojado, el navegador web averiguará la IP (a través de una consulta DNS), mientras que el servidor que se está accediendo el que responderá con el sitio web adecuado utilizando el nombre escrito en el navegador.

ICMP (Internet Control Message Protocol)

ICMP se utiliza para **enviar mensajes de control a los routers**. Es un protocolo de capa de Internet, en colaboración con el protocolo IP. Puede ser utilizado en varias

situaciones para que un router instruya sobre alguna situación a otro router, por lo general cuando un router recibe un datagrama que no puede entregar, se responde de nuevo al router que envía el datagrama con un mensaje ICMP explicando la razón por la que no se pudo hacerlo.

Algunos de los mensajes de control que pueden ser enviados usando ICMP son:

- **Echo**: Se utiliza para comprobar si la ruta entre el receptor y el transmisor está bien. El uso más conocido de este mensaje es a través del comando **Ping**.

- **Anfitrión inalcanzable (Host unreachable)**: Dentro de este mensaje, el router puede decir exactamente lo que salió mal, como que la red es inalcanzable, el equipo inalcanzable, el protocolo inalcanzable, el puerto inalcanzable, la red de destino es desconocida, equipo de destino desconocido, el administrador de la red ha bloqueado la red específica o un equipo, problemas de enrutamiento, etc .
- **Reducción de velocidad (speed reduction)**: se envía este mensaje si el router está sobrecargado, es decir, que está recibiendo más datagramas de los que es capaz de procesar, con el fin de hacer que el router que envía los datagramas reduzca la tasa de datagramas enviados al router sobrecargado.
- **Redirección solicitada (redirection requested)**: Este mensaje se utiliza generalmente cuando un router se entera de que hay una mejor ruta para llegar al destino, actualizando al router que transmite. Esta característica sólo funciona en redes de área local, no funciona en grandes redes que interconectan otras redes, como Internet.
- **Se ha alcanzado el tiempo de vida (TTL)**: Todos los datagramas IP tienen un campo de tiempo de vida (TTL), que dice hasta cuantos saltos (por ejemplo, enrutadores) el datagrama puede pasar desde el equipo de transmisión a la que recibe. Si un datagrama se establece con un TTL de 20, esto significa que si no llega a su destino dentro de los 20 saltos, el datagrama debe ser desechado. Esto se hace con el fin de evitar que los datagramas circulen eternamente en la red o en Internet si la red no está configurada correctamente y el datagrama está vagando sin llegar a su destino.
- **Hora**: Los routers (y computadoras) pueden pedir la hora a otro router o equipo que tiene la hora en su reloj en tiempo real. Se usa para sincronizar los relojes de

los ambos equipos. Esta sincronización no es perfecta, ya que existe un pequeño retardo introducido por la red (en el orden de milisegundos). Este mensaje también puede ser usado para medir el tiempo de retardo entre dos equipos de la red, si se sincronizan sus relojes.

Protocolos de enrutamiento: RIP, OSPF y BGP

El enrutamiento puede ser **estático o dinámico**. Mientras que en las redes pequeñas se usa el enrutamiento estático, es decir que los datagramas viajan siempre por la misma ruta exacta para llegar a su destino, en Internet o en redes grandes es necesario usar enrutamiento dinámico.

Con el enrutamiento **dinámico**, los **routers pueden cambiar rutas sobre la marcha** si ven que existen mejores caminos para llegar a un destino determinado. Por ejemplo, si hay más de un camino para llegar a un determinado destino y la ruta actual es más larga que otra ruta disponible, los enrutadores pueden reconfigurarse para utilizar la ruta más corta. Aquí **"largo" y "corto" se refiere al número de saltos existentes** (por ejemplo, enrutadores) en el camino. Rutas más cortas no son necesariamente las más rápidas, como se explicara.

La comunicación entre los routers, con el fin de reprogramar sus tablas de enrutamiento, se realiza utilizando un protocolo de enrutamiento. Los tres protocolos de enrutamiento dinámico más conocidos son **RIP** (Protocolo de información de enrutamiento), **OSPF** (Open Shortest Path First) y **BGP** (Border Gateway Protocol).

Si los routers están utilizando protocolo **RIP**, van a enviar sus tablas de enrutamiento a todos los routers que tienen acceso cada 30 segundos. La tabla de enrutamiento es una tabla que contiene todas las redes a las que los routers saben cómo llegar y también la distancia (saltos).

Cuando se recibe una nueva tabla de enrutamiento de otro router, el router puede ver si hay alguna red en esa lista que tiene un camino más corto que el que está configurado actualmente para su uso. Si existe, el router se reconfigurará para utilizar este nuevo camino más corto.

El problema es que los caminos más cortos no siempre son los mejores. El protocolo RIP no implementa alguna forma de comprobar el **rendimiento** de ese camino y tampoco comprueba la **congestión** o si la ruta está realmente **disponible**. Así que una ruta más larga puede ser más rápida.

RIP utiliza UDP en el puerto 520.

A pesar de su nombre, el protocolo **OSPF** no busca el camino más corto, pero sí **los más rápidos**. Cuando los enrutadores utilizan el protocolo OSPF, comprueban el estado de otros routers, a los que tienen acceso, de vez en cuando con el envío de un mensaje de saludo. A partir de ese mensaje es que ellos saben si un router está en línea y cuál es su estado. Otra diferencia es que el uso de los enrutadores OSPF **conocen todos los caminos** que se pueden utilizar para llegar a un destino dado, mientras que los routers RIP sólo conocen el camino más corto. Los routers basados en RIP envían sus tablas de enrutamiento cada 30 segundos lo cual eleva el tráfico de red.

Otra diferencia notoria es que los routers basados en OSPF permiten el **equilibrio de carga**: si hay más de una ruta a un destino dado, el router puede dividir datagramas entre ellas con el fin de reducir el tráfico individual por cada uno de ellas.

OSPF trabaja directamente en la capa de Internet con el protocolo IP, por lo que no utiliza TCP o UDP.

BGP es un protocolo orientado a las **redes grandes**, como Internet y de hecho BGP es el protocolo utilizado por los routers en la Red. Como tal, se clasifica como un protocolo de puerta de enlace (gateway) externo, mientras RIP y OSPF se clasifican como protocolos de gateway interior, ya que se utilizan en las redes que están bajo la misma administración.

Los grupos de routers BGP y equipos que están bajo la misma administración están en una unidad llamada Sistema Autónomo (AS), por ejemplo, todos los routers y computadoras que pertenecen o están conectados con el mismo proveedor de servicios de Internet (ISP) son parte del mismo AS. Mientras se ejecuta dentro del mismo sistema autónomo BGP se llama IBGP (Interno), mientras que corre entre dos sistemas autónomos diferentes BGP se llama EBGP (externo).

BGP es mucho más complejo que RIP y OSPF, ya que utiliza varios criterios diferentes (llamadas atributos) para determinar cuál es la mejor ruta a tomar.

A diferencia de RIP, los routers basados en BGP sólo se envía lo que es nuevo en sus tablas de enrutamiento en lugar de enviar toda la tabla de vez en cuando, lo que ayuda a disminuir el tráfico de red. Otra diferencia entre BGP y RIP es que BGP comprueba de vez en cuando si una trayectoria dada está disponible o no.

BGP utiliza TCP en el puerto 179.

ARP y RARP

ARP (Address Resolution Protocol) está a cargo de averiguar la dirección MAC (la dirección física) de un equipo que tiene una dada dirección IP y RARP (Reverse Address Resolution Protocol) hace lo contrario: es el encargado de descubrir cuál es la dirección IP de un equipo con una dirección MAC dada.

Mientras que un datagrama se transmite a través de Internet, la dirección MAC del equipo de destino no se necesita, los routers que están en el camino sólo están interesados en la entrega del datagrama a la red de destino. Pero una vez que el paquete llega la red de destino, el router conectado a esa red necesita saber la dirección MAC del equipo de destino, ya que entregará el datagrama localmente (probablemente mediante el protocolo Ethernet).

Por ejemplo, si la dirección IP de destino es 67.67.67.67, cuando el datagrama llega al enrutador de la red 67.67.67.0, se le pedirá a todos los equipos (mensaje de difusión) usando ARP protocolo: ¿qué equipo es que tiene la dirección IP 67.67.67.67? A continuación, el equipo que está utilizando esa dirección IP responderá "¡soy yo!".

Por supuesto el envío de mensajes de información de todo el tiempo congestiona la red, por lo que en el router se mantiene una tabla de direcciones IP conocidas y sus correspondientes direcciones MAC y de esa forma no tendrá que hacer la misma pregunta otra vez cuando recibe un nuevo datagrama dirigido a 69.69 .69.69.

RARP, por otro lado, se utilizó en el pasado por PCs sin disco usando arranque remoto. Dado que este tipo de equipo no tiene un sistema operativo instalado, no sabe la dirección IP que utilizará, por lo que necesitan saber qué dirección IP debe utilizar con el fin de comenzar a cargar el sistema operativo desde el servidor de arranque. Como se puede ver, este es exactamente el mismo papel que hace DHCP y como hoy en día todas las redes utilizan un servidor DHCP, el uso de RARP quedó relegado.

Tanto ARP y RARP trabajan en la capa de interfaz de red.

Otros Protocolos y funcionalidades

A continuación encontrará una lista de otros protocolos "famosos" relacionados con TCP/IP y funcionalidades que se pueden escuchar acerca de:

- **NAT (Network Address Translation**): Teóricamente cada equipo conectado a Internet requeriría una dirección IP "pública" válida. NAT permite a una red local usar una única dirección IP "pública". Por ejemplo, cuando se conecta la red doméstica o de oficina a Internet mediante un router de banda ancha, el router

utilizará la dirección IP única asignada por su proveedor de Internet, mientras que los equipos utilizarán direcciones IP que son válidas sólo dentro de la red (la así llamado "direcciones IP mágicas", por lo general dentro del rango 192.168.xx). Desde el punto de vista de Internet, todos los equipos de la red están utilizando la misma dirección IP. Así que enviaremos los datos de uno de los equipos, el equipo de origen utilizará la dirección IP del router y cuando este datagrama llega al router, que reemplazará su dirección IP con la dirección IP privada del equipo de destino, que es válida sólo en el interior su red. Esta técnica se llama NAT.

- **IGMP (Internet Group Management Protocol)**: Mientras que el envío de un mismo datagrama a todos los equipos de una red se denomina difusión, el envío de un mismo datagrama para un grupo de equipos se llama multidifusión. La multidifusión TCP/IP se puede hacer incluso si las computadoras se encuentran en diferentes redes. Estos grupos se gestionan mediante mensajes de control IGMP. IGMP utiliza el protocolo IP, que trabaja en la capa de Internet.
- **SNMP (Simple Network Management Protocol)**: Protocolo utilizado para el control de los dispositivos de hardware conectados a redes TCP/IP que implementan este protocolo. SNMP es un protocolo de capa de Aplicación que utiliza UDP en los puertos 161 y 162.
- **Finger**: Este es un protocolo de capa de Aplicación que utiliza TCP en el puerto 79 y se utiliza para descubrir información sobre un determinado usuario en el servidor. Dado que tener acceso a la información personal de todos los usuarios es una falla de seguridad, este servicio está casi siempre desactivado.