Protocolo TCP / IP

Introducción al TCP/IP

Desde sus comienzos, en la Red coexisten computadoras de muy diverso tipo, por lo que se hizo necesario un protocolo común y único, de forma que todas pudieran entender e interpretar correctamente la información que circula. Este protocolo se denominó TCP/IP. En realidad son dos acrónimos distintos; TCP son las siglas de "Transmisión Control Protocol", mientras que IP significa "Internetwork Protocol".

Independientemente de su significado concreto, TCP/IP ha venido a ser casi sinónimo de Internet, si bien la arquitectura se empezó a desarrollar como base de ARPANET (red de comunicaciones militar del gobierno de los EE.UU), con la expansión de la INTERNET se ha convertido en una de las arquitecturas de redes más difundida en todo lo relacionado con la Red y con este tipo de comunicación basado en la conmutación de paquetes (datagramas), a pesar de ser una arquitectura de facto (sin ajustarse a una norma previa), en lugar de ser uno de los estándares definidos por la ISO, IICC, etc...

En la actualidad el concepto TCP/IP engloba toda una filosofía de operación, basada por supuesto en la conmutación de paquetes, pero no esta compuesta por solo dos protocolos, se trata de todo un conjunto "suite" de protocolos que están ligados y que constituyen la base del funcionamiento de Internet.

Concretamente, IP es un estándar que subyace en todas las comunicaciones de la red. Incluye todas las especificaciones necesarias para hacer inteligible a cualquier máquina la información contenida en cada datagrama (paquete) transmitido. Entre otras, el tamaño normalizado de las cabeceras, remitente, códigos de control de integridad, etc. Uno de sus elementos mas destacados, lo constituye un sistema universal y unificado para establecer las "Direcciones" de las computadoras de la red. A esto se le denomina Dirección IP ("Internet Protocol Address").

En principio IP es el encargado de que la transmisión de los datos sea posible de una computadora a otra, mientras que TCP es el encargado de juntar los paquetes, pedir los que faltan (en su caso) y finalmente ordenarlos, puesto que, como hemos visto, la Red no garantiza la llegada de todos los paquetes ni tampoco que su llegada sea en orden. En realidad, TCP se encarga de "negociar" con el equipo remoto determinados parámetros que determinan algunos detalles del modo en que se realizará la transmisión (por ejemplo el tamaño de los paquetes). Una comunicación en Internet es siempre un activo diálogo entre máquinas, incluso cuando aparentemente solo estamos "recibiendo" información, por ejemplo al descargar un archivo.

Antecedentes

Aunque en la actualidad nos parezca sencillo, conectar en red los equipos, es un complicado problema de ingeniería. Durante los años 60 y 70 se crearon muchas tecnologías de redes, cada una basada en un diseño específico de hardware. Estos sistemas eran construidos de una sola pieza, lo que podríamos llamar una arquitectura "monolítica". Esto significa que los diseñadores debían ocuparse de todos los elementos involucrados en el proceso; podemos suponer que estos elementos forman una cadena de transmisión que tiene diversas partes:

Los dispositivos físicos de conexión, los protocolos software y hardware usados en la comunicación; los programas de aplicación que realizaban la comunicación y la interfaz hombre-máquina que permiten al humano utilizar la red.

Este modelo, que considera la cadena como un todo monolítico, es poco práctico, pues el más pequeño cambio puede implicar alterar todos sus elementos.

El diseño original de Internet del Departamento de Defensa americano disponía un esquema de cuatro capas. Aunque data de los 70 es más o menos el que se sigue utilizando:

- *Capa Física* o de Acceso de Red ("Network Access Layer"), responsable del envío de la información sobre el sistema hardware utilizado en cada caso; se utiliza un protocolo distinto según el tipo de red física.

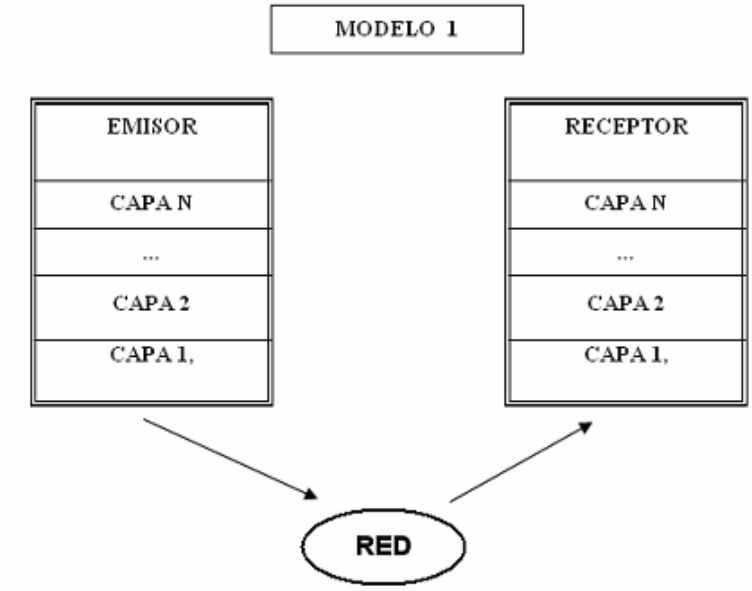
Capa de Red ~~también llamada capa Internet ("Internet Layer"),~~ es la responsable de enviar los datos a través de las distintas redes físicas que pueden conectar una máquina origen con la de destino de la información. Los protocolos de transmisión, como el IP están íntimamente asociados a esta capa.

Capa de transporte ("Host-to-Host Layer") controla el establecimiento y fin de la conexión, control de flujo de datos, retransmisión de datos perdidos y ~~otros detalle~~s de la transmisión entre dos sistemas. Los protocolos mas importantes a este nivel son TCP y UDP (mutuamente excluyentes).

Capa de aplicación ("Application layer"), conformada por los protocolos que sirven directamente a los programas de usuario, navegador, e-mail, FTP, TELNET, etc.

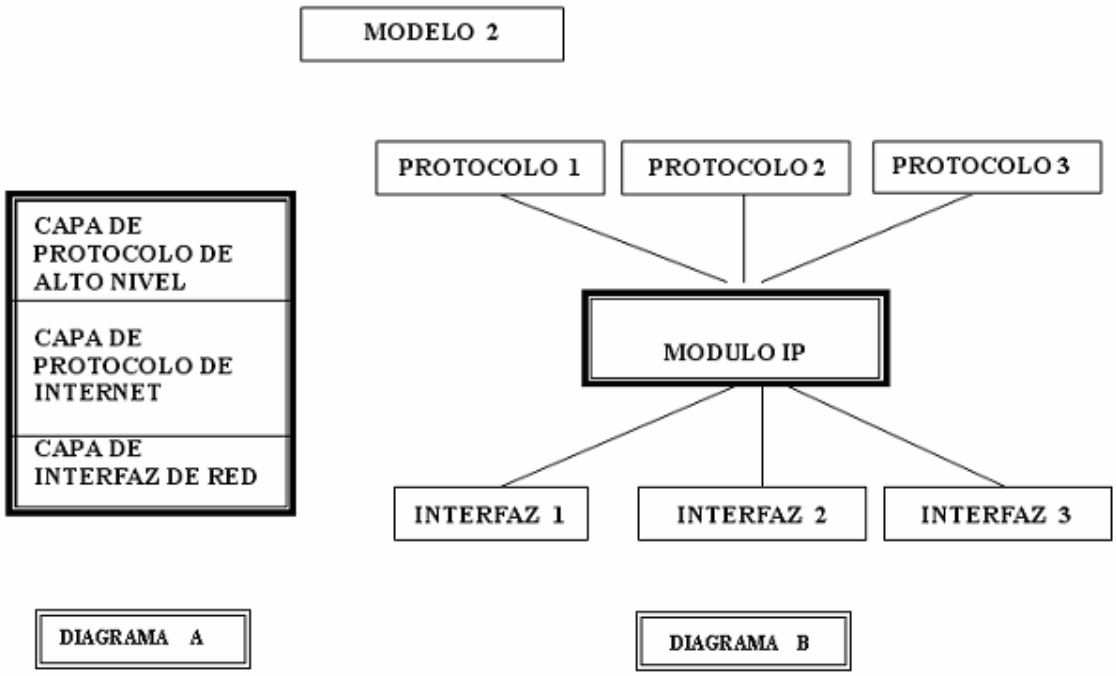
Las Capas Conceptuales Del Software De Protocolos

Pensemos los módulos del software de protocolos en una pila vertical constituida por capas. Cada capa tiene la responsabilidad de manejar una parte del problema.



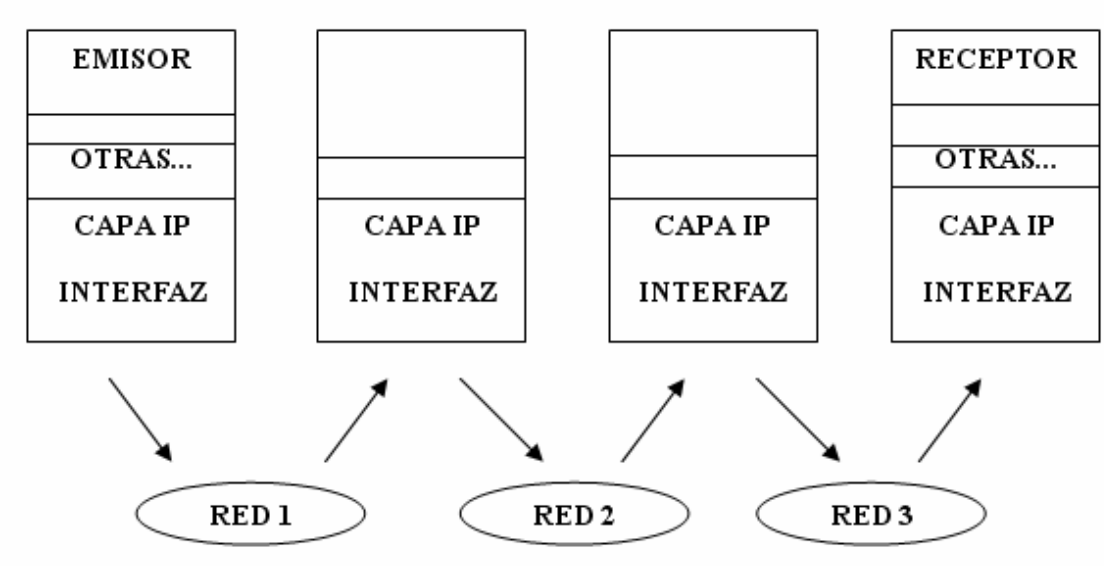
Conceptualmente, enviar un mensaje desde un programa de aplicación en una maquina hacia un programa de aplicaciones en otra, significa transferir el mensaje hacia abajo, por las capas sucesivas del software de protocolo en la maquina emisora, transferir un mensaje a través de la red y luego, transferir el mensaje hacia arriba, a través de las capas sucesivas del software de protocolo en la maquina receptora.

En la práctica, el software es mucho más complejo de lo que se muestra en el modelo 1. Cada capa toma decisiones acerca de lo correcto del mensaje y selecciona una acción apropiada con base en el tipo de mensaje o la dirección de destino. Por ejemplo, una capa en la maquina de recepción debe decidir cuándo tomar un mensaje o enviarlo a otra maquina. Otra capa debe decidir que programa de aplicación deberá recibir el mensaje.



Para entender la diferencia entre la organización conceptual del software de protocolo y los detalles de implantación, consideremos la comparación del Modelo 2. El diagrama conceptual (A) muestra una capa de Internet entre una capa de protocolo de alto nivel y una capa de interfaz de red. El diagrama realista (B) muestra el hecho de que el software IP puede comunicarse con varios módulos de protocolo de alto nivel y con varias interfaces de red.

Aun cuando se presenta un diagrama conceptual de la estratificación por capas, no todos los detalles sirven como ayuda para explicar los conceptos generales. Por ejemplo, el modelo 3 muestra las capas del software de protocolo utilizadas por un mensaje que atraviesa tres redes. El diagrama muestra solo la interfaz de red y las capas de protocolo Internet en los ruteadores debido a que sólo estas capas son necesarias para recibir, rutear y enviar los diagramas. Sé entiende que cualquier maquina conectada hacia dos redes debe tener dos módulos de interfaz de red, aunque el diagrama de estratificación por capas muestra sólo una capa de interfaz de red en cada maquina.



Como se muestra en la figura, el emisor en la maquina original emite un mensaje que la capa del IP coloca en un datagrama y envía a través de la red 1. En las maquinas intermedias el datagrama pasa hacia la capa IP, la cual rutea el datagrama de regreso, nuevamente (hacia una red diferente). Sólo cuando se alcanza la maquina en el destino IP extrae el mensaje y lo pasa hacia arriba, hacia la capa superior del software de protocolos.

Funcionalidad De Las Capas

Una vez que se toma la decisión de subdividir los problemas de comunicación en cuatro sub-problemas y organizar el software de protocolo en módulos, como en el diseño original de Internet del Departamento de Defensa americano, de manera que cada uno maneja un problema, surge la pregunta. "¿Qué tipo de funciones se debe instalar en cada modulo?". La pregunta no es fácil de responder por varias razones. En primer lugar, un grupo de objetivos y condiciones determinan un problema de comunicación en particular, es posible elegir una organización que optimice un software de protocolos para ese problema. Segundo, incluso cuando se consideran los servicios generales al nivel de red, como un transporte confiable es posible seleccionar entre distintas maneras de resolver el problema. Tercero, el diseño de una arquitectura de red y la organización del software de protocolo esta interrelacionado; no se puede diseñar a uno sin considerar al otro.

Modelo De Referencia ISO De 7 Capas
Modelo OSI

Respondiendo a la teoría general imperante del mundo de la computación de diseñar el hardware por módulos y el software por capas, en 1978, la organización ISO (International Standards Organization), propuso un modelo de comunicaciones para redes al que titularon "The reference model of Open Systems Interconnection", generalmente conocido como **modelo *OSI***. Su filosofía se basa en descomponer la funcionalidad de la cadena de transmisión en diversos módulos, cuya interfaz con los adyacentes esté estandarizada. Esta filosofía de diseño presenta una doble ventaja; el cambio de un módulo no afecta necesariamente a la totalidad de la cadena; y además, puede existir una cierta interoperabilidad entre diversos productos y fabricantes hardware/software, dado que los límites y las interfaces están perfectamente definidas. Esto supone por ejemplo, que dos softwares de comunicación distintos puedan utilizar el mismo medio físico de comunicación.

El modelo OSI tiene dos componentes principales:

- Un modelo de red, denominado modelo básico de referencia ("Basic Reference Model") o capa de servicio ("Server-layer").
- Una serie de protocolos concretos.

El modelo de red está basado en un modelo de siete capas, mientras que el primitivo de Internet estaba basado en 4. Actualmente todos los desarrollos se basan en este modelo de 7 niveles, que son los siguientes:

1. Físico
2. Enlace
3. Red
4. Transporte
5. Sesión
6. Presentación
7. Aplicación

Cada nivel realiza una función concreta, y está separado de los adyacentes por interfaces conocidas, sin que le corresponda ningún otro aspecto del total de la comunicación.

Así como este modelo de referencia OSI posee siete niveles (o capas), la arquitectura TCP/IP viene definida por 4 niveles: el nivel de subred [enlace y físico], el nivel de interred [Red, IP], el protocolo proveedor de servicio [Transporte, TCP o UDP], y el nivel de aplicación.

Las capas del modelo OSI

La descripción esquemática de las diversas capas que componen este modelo es como sigue:

1- Capa física

("Physical layer"); es la encargada de transmitir los bits de información por la línea o medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es unidireccional o bidireccional (simplex, duplex o full-duplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas.

Como resumen de los tareas de esta capa, podemos decir que se encarga de transformar un paquete de información binaria ("Frame") en una sucesión de impulsos adecuados al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable); electromagnéticos (transmisión Wireless) o luminosos (transmisón óptica). Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace.

Por ejemplo: Este nivel define las medidas del cable coaxial Ethernet y de los conectores BNC utilizados. Otro ejemplo de estándares relativos a esta capa son RS-232 para comunicaciones serie y X.21

2- Capa de enlace

("Data Link layer"); Puede decirse que esta capa traslada los mensajes hacia/desde la capa física a la capa de red (que veremos a continuación). Especifica como se organizan los datos cuando se transmiten en un medio particular. Por ejemplo, esta capa define como son los cuadros ("Frames"), las direcciones y las sumas de control ("Checksum") de los paquetes Ethernet.

Además del direccionamiento local, se ocupa de la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión. Para esto agrupa la información a transmitir en bloques ("Frames"), e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad. Los datagramas recibidos son comprobados por el receptor. Si algún datagrama se ha corrompido se envía un mensaje de control al remitente solicitando su reenvío. El protocolo PPP (point-to-point protocol) es ejemplo de esta capa.

La capa de enlace puede considerarse dividida en dos subcapas:

Control lógico de enlace LLC ("Logical Link Control") define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.

Control de acceso al medio MAC ("Medium Access Control"). Esta subcapa actúa como controladora del hardware subyacente (el adaptador de red). De hecho el controlador de la tarjeta de red es denominado a veces "MAC driver", y la dirección física contenida en el hardware de la tarjeta es conocida como dirección MAC "MAC address". Su principal tarea (que le proporciona el nombre "control de acceso") consiste en arbitrar la utilización del medio físico para facilitar que varios equipos puedan competir simultáneamente por la utilización de un mismo medio de transporte. El mecanismo CSMA/CD ("Carrier Sense Multiple Access with Collision Detection") utilizado en Ethernet es un típico ejemplo de esta subcapa.

3- Capa de Red

("Network layer"); Esta capa se ocupa de la transmisión de los datagramas (paquetes) y de encaminar cada uno en la dirección adecuada ("Routing"), tarea esta que puede ser complicada en redes grandes como Internet, pero no se ocupa para nada de los errores o pérdidas de paquetes. Por ejemplo, define la estructura de direcciones y rutas de Internet. A este nivel se utilizan dos tipos de paquetes: paquetes de datos y paquetes de actualización de ruta. Como consecuencia esta capa puede considerarse subdividida en dos:

Transporte: Encargada de encapsular los datos a transmitir (de usuario). Utiliza los paquetes de datos. *En esta categoría se encuentra el protocolo IP ("Internet Protocol").*

Conmutación ("Switching"): Esta parte es la encargada de intercambiar información de conectividad específica de la red (su actividad es raramente percibida por el usuario). Los routers son dispositivos que trabajan en este nivel y se benefician de estos paquetes de actualización de ruta. En esta categoría se encuentra el protocolo ICMP ("Internet Control Message Protocol"), responsable de generar mensajes cuando ocurren errores en la transmisión y de un modo especial de eco que puede comprobarse mediante PING ("Packet Internetwork Goper").

Los protocolos más frecuentemente utilizados en esta capa son dos: *X.25 e IP*.

4- Capa de Transporte

("Transport layer"); esta capa se ocupa de garantizar la fiabilidad del servicio, describe la calidad y naturaleza del envío de datos. Por ejemplo, esta capa define cuando y como debe utilizarse la retransmisión para asegurar su llegada. Para ello divide el mensaje recibido de la capa de sesión en trozos (datagramas), los numera correlativamente y los entrega a la capa de red para su envío. Durante la recepción, si la capa de Red utiliza el protocolo IP, la capa de Transporte es responsable de reordenar los paquetes recibidos fuera de secuencia. También puede funcionar en sentido inverso multiplexando una conexión de transporte entre diversas conexiones de datos. Esto permite que los datos provinientes de diversas aplicaciones compartan el mismo flujo hacia la capa de red.

Un ejemplo típico de protocolo usado en esta capa es *TCP* ("Transport Control Protocol"), que con su homólogo IP de la capa de Red, configuran la suite TCP/IP utilizada en Internet, aunque existen otros como UDP ("Universal Datagram Protocol"), una capa de transporte utilizada también en Internet por algunos programas de aplicación.

5- Capa de Sesión

("Session Layer"); es una extensión de la capa de transporte que ofrece control de diálogo y sincronización, aunque en realidad son pocas las aplicaciones que hacen uso de ella. Por ejemplo, las comunicaciones de Internet no la utilizan.

Algunos autores indican que la capa de sesión es meramente una consideración teórica de los autores del modelo sin absolutamente ninguna utilidad práctica conocida.

6- Capa de Presentación

("Presentation layer"); Esta capa se ocupa de los aspectos semánticos de la comunicación (describe la sintaxis de los datos a transmitir), estableciendo los arreglos necesarios para que puedan comunicar máquinas que utilicen diversa representación interna para los datos. Por ejemplo, describe como pueden transferirse números de coma flotante entre equipos que utilizan distintos formatos matemáticos. Esta capa es buena candidata para implementar aplicaciones de criptografía.

En teoría esta capa "presenta" los datos a la capa de aplicación tomando los datos recibidos y transformándolos en formatos como texto, imágenes y sonido.

Esta capa puede estar ausente, ya que son pocas las aplicaciones que hacen uso de ella. Con esta capa ocurre algo parecido a la anterior. En teoría cliente y servidor debían negociar el formato a utilizar, y esta función, y el correspondiente formateo de los datos, sería el objeto de esta capa. Sin embargo, esto, que tenía cierto sentido en la década de los 70, cuando gran parte del trabajo de redes estaba relacionado con la entrada y salida de datos a grandes ordenadores utilizando terminales "Tontas" de diversos tipos (que utilizaban códigos de control ligeramente distintos) no tiene ya mucho sentido.

Actualmente el panorama ha cambiado; solo existe una opción para el formato de datos, a pesar de lo cual el protocolo OSI sigue negociando un esquema de codificación (el único disponible). En Internet, el único servicio que utiliza esta capa es TELNET, que precisamente es un servicio de acceso a servidores desde terminales remotos. En este caso, la capa de presentación es la que se encarga de configurar el terminal para conectar a un servidor de características particulares.

7- Capa de Aplicación

("Application layer"); Proporciona servicios a la aplicaciones. Define la manera como interactúa la aplicación ejecutada con la red; incluye la administración de bases de datos, el correo electrónico y ciertos programas que emulan terminales.

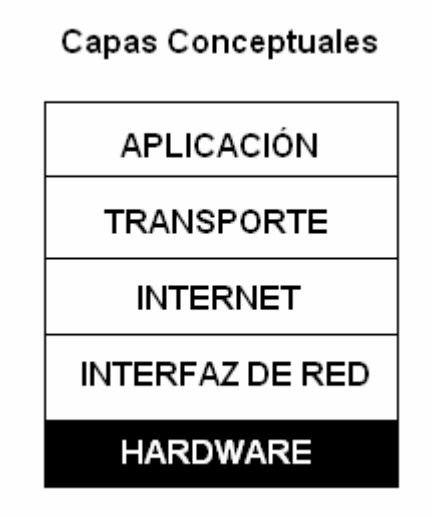
Este nivel es el más cercano al usuario. Es el programa o conjunto de programas que generan información para que esta viaje por la red, por ejemplo el correo electrónico, cuando lo procesamos y enviamos, este puede ir a cualquier lugar del mundo, y ser leído en cualquier tipo de computadora.

Ejemplos de protocolos utilizados por los programas de esta capa son HTTP, SMTP, POP, IMAP, etc.

El Modelo De Estratificación Por Capas De TCP/IP De Internet

Como ya se mencionó, este modelo de estratificación por capas no se origina de un comité de estándares, sino que proviene de las investigaciones que se realizan respecto al conjunto de protocolos de TCP/IP.

En términos generales, el software TCP/IP está organizado en cuatro capas conceptuales que se construyen sobre una quinta capa de hardware. El siguiente esquema muestra las capas conceptuales.



- ***Capa de aplicación***. Es el nivel mas alto, los usuarios llaman a una aplicación que acceda servicios disponibles a través de la red de redes TCP/IP. Una aplicación interactúa con uno de los protocolos de nivel de transporte para enviar o recibir datos. Cada programa de aplicación selecciona el tipo de transporte necesario, el cual puede ser una secuencia de mensajes individuales o un flujo continúo de octetos. El programa de aplicación pasa los datos en la forma requerida hacia el nivel de transporte para su entrega.

- ***Capa de transporte***. La principal tarea de la capa de transporte es proporcionar la comunicación entre un programa de aplicación y otro. Este tipo de comunicación se conoce frecuentemente como comunicación punto a punto. La capa de transporte regula el flujo de información. Puede también proporcionar un transporte confiable, asegurando que los datos lleguen sin errores y en secuencia. Para hacer esto, el software de protocolo de transporte tiene el lado de recepción enviando acuses de recibo de retorno y la parte de envío retransmitiendo los paquetes perdidos. El software de transporte divide el flujo de datos que se está enviando en pequeños fragmentos (por lo general conocidos como paquetes)

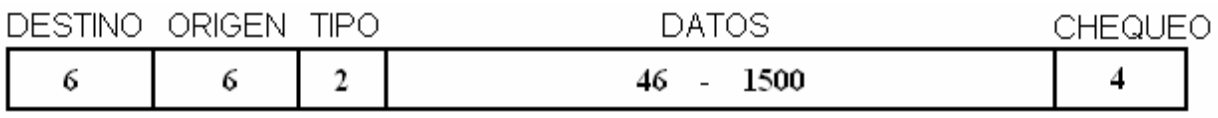
y pasa cada paquete, con una dirección de destino, hacia la siguiente capa de transmisión. Aun cuando en el esquema anterior se utiliza un solo bloque para representar la capa de aplicación, una computadora de propósito general puede tener varios programas de aplicación accesando la red de redes al mismo tiempo. La capa de transporte debe aceptar datos desde varios programas de usuario y enviarlos a la capa del siguiente nivel. Para hacer esto, se añade información adicional a cada paquete, incluyendo códigos que identifican qué programa de aplicación envía y qué programa debe recibir, así como una suma de verificación para verificar que el paquete ha llegado intacto y utiliza el código de destino para identificar el programa de aplicación en el que se debe entregar.

- ***Capa Internet***. La capa Internet maneja la comunicación de una máquina a otra. Esta contiene al protocolo IP y se encarga de aceptar una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina, hacia la que se debe enviar el paquete. La capa Internet también maneja la entrada de datagramas, verifica su validez y utiliza un algoritmo de ruteo para decidir si el datagrama debe procesarse de manera local o debe ser transmitido. Para el caso de los datagramas direccionados hacia la máquina local, el software de la capa de red de redes borra el encabezado del datagrama y selecciona, de entre varios protocolos de transporte, un protocolo con el que manejará el paquete. Por último, la capa Internet envía los mensajes ICMP de error y control necesarios y maneja todos los mensajes ICMP entrantes.

- ***Capa de interfaz de red***. Es la capa inferior de la jerarquía de protocolos de TCP/IP y es equivalente a la capa 1 y 2 del modelo OSI (con algunas funciones de la capa 3). Hay muchos protocolos de acceso a la red (uno por cada estándar físico de red) y su función principal es encapsular Datagramas en Frames y mapear direcciones IP a direcciones físicas.

  - Esta capa se construye con la tarjeta de red, los drivers y los programas asociados
  - Un ejemplo: el Sistema Ethernet
  - Ethernet es una tecnología de redes de área local (LAN) que transmite información entre computadores a una velocidad de 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet) ó 1000 Mbps (Gigabit Ethernet).

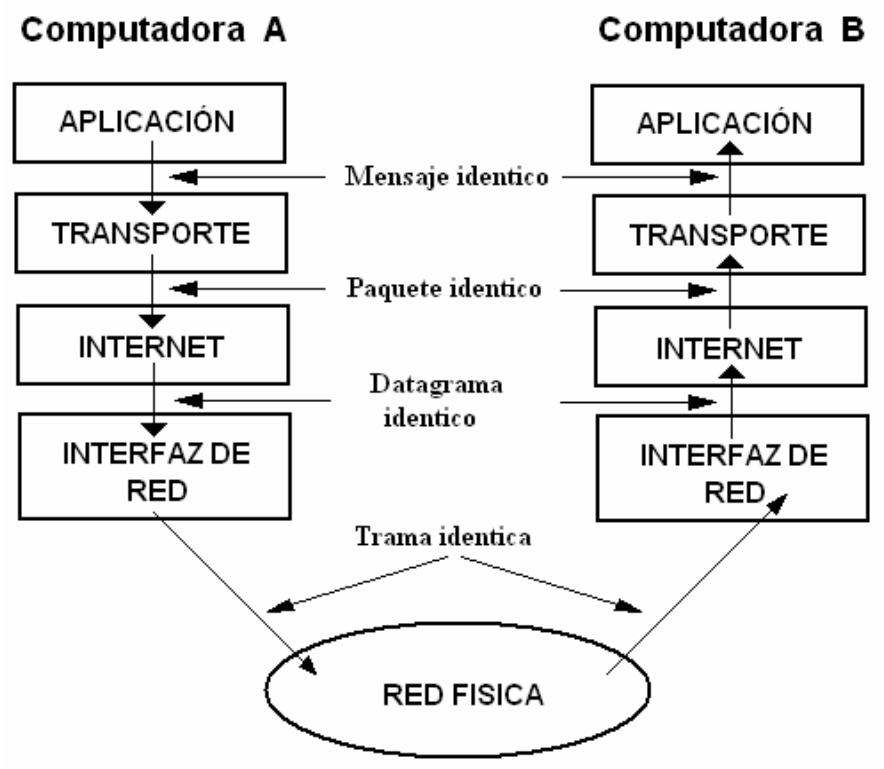
- Los medios que soporta 10 Mbps son coaxial grueso, coaxial delgado, par trenzado y fibra óptica.
- Los medios que soporta 100 Mbps son par trenzado y fibra óptica
- Los medios que soporta 1000 Mbps son par trenzado y fibra óptica
- El frame Ethernet
- El corazón del sistema Ethernet es el frame Ethernet utilizado para llevar datos entre computadores.
- El "frame" consta de varios bits organizados en varios campos.
- Estos campos incluyen la dirección física de las interfaces Ethernet, un campo variable de datos (entre 46 y 1500 bytes) y un campo de chequeo de error.
- El frame Ethernet Versión 2



- Destino: 6 bytes, dirección física del nodo destino (MAC address)
- Origen: 6 bytes, dirección del nodo origen
- Tipo: 2 bytes, especifica el protocolo de la capa superior
- Datos: entre 46 y 1500 bits, información de las capas superiores
- Chequeo: Secuencia de chequeo del frame.
- Cuando un frame Ethernet es enviado al canal todas las interfaces revisan los primeros 6 bytes (48 bits). Si es su dirección MAC (o broadcast) reciben el paquete y lo entregarán al software de red instalado en el computador.
- Las interfaces con diferentes dirección no continuarán leyendo el frame

El Principio De La Estratificacion Por Capas De Protocolos

Independientemente del esquema de estratificación por capas que se utilice o de las funciones de las capas, la operación de los protocolos estratificados por capas se basa en una idea fundamental. La idea, conocida como principio de estratificación por capas puede resumirse de la siguiente forma:

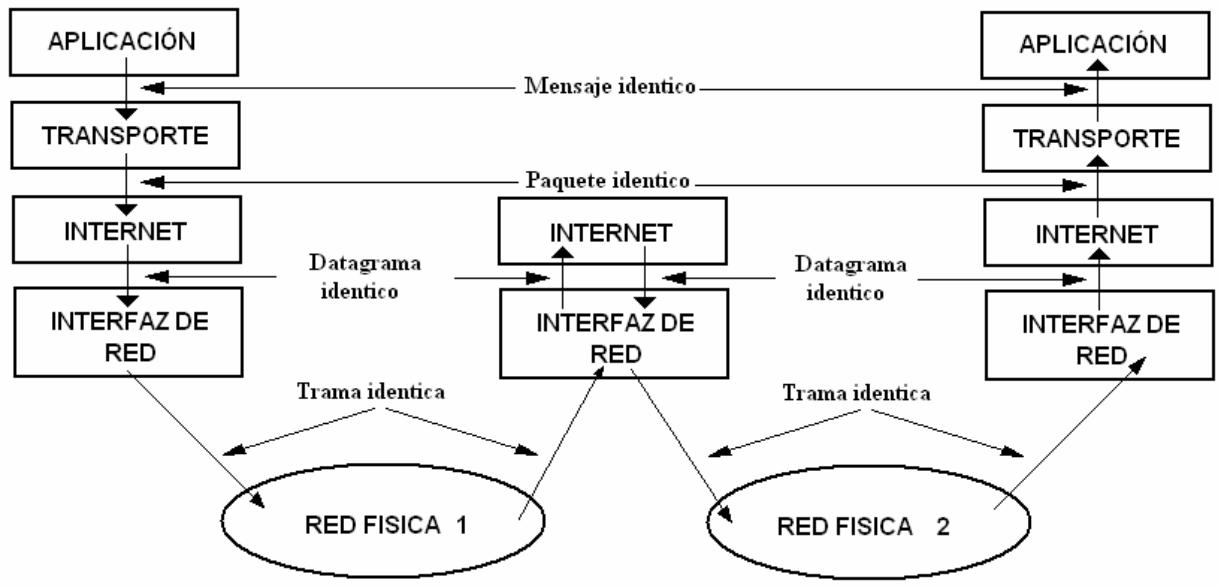


Los protocolos estratificados por capas están diseñados de modo que una *capa n* en el receptor de destino reciba exactamente el mismo objeto enviado por la *correspondiente capa n* de la fuente.

El principio de estratificación por capas explica por que la estratificación por capas es una idea poderosa. Esta permite que el diseñador de protocolos enfoque su atención hacia una capa a la vez, sin preocuparse acerca del desempeño de las capas inferiores. Por ejemplo, cuando se construye una aplicación para transferencia de archivos, el diseñador piensa solo en dos copias del programa de aplicación que se correrá en dos máquinas y se concentrará en los mensajes que se necesitan intercambiar para la transferencia de archivos. El diseñador asume que la aplicación en maquina (computadora) receptora es exactamente la misma que en el maquina emisora.

Estratificación Por Capas En Un Ambiente De Internet TCP/IP

Nuestro planteamiento sobre el principio de estratificación por capas es un tanto vago y la ilustración de la siguiente figura muestra un tema importante dado que permite distinguir entre la transferencia desde una fuente hasta un destino final y la transferencia a través de varias redes. La figura además ilustra la distinción y muestra el trayecto de un mensaje enviado desde un programa de aplicación en una maquina hacia la aplicación en otra a través de un *ruteador*.



Como se muestra en la figura, la entrega del mensaje utiliza dos estructuras de red separadas, una para la transmisión desde la computadora A hasta el ruteador R y otra desde el ruteador R a la computadora B. El siguiente principio de trabajo de estratificación de capas indica que el Frame entregado a R es idéntico al enviado por la computadora A. En contraste, las capas de aplicación y transporte cumplen con la condición punto a punto y están diseñados de modo que el software en la fuente se comunique con su par en el destino final. Así, el principio de la estratificación por capas establece que el paquete recibido por la capa de transporte en el destino final es idéntico al paquete enviado por la capa de transporte en la fuente original.

Es fácil entender que, en las capas superiores, el principio de estratificación por capas se aplica a través de la transferencia punto a punto y que en las capas inferiores se aplica en una sola transferencia de máquina. No es tan fácil ver como el principio de estratificación de capas se aplica a la estratificación Internet. Por un lado, hemos dicho que las computadoras conectadas a una red de redes deben considerarse como una gran red virtual, con los datagramas IP que hacen las veces de tramas de red. Desde este punto de vista, los datagramas viajan desde una fuente original hacia un destino final y el principio de la estratificación por capas garantiza que el destino final reciba exactamente el datagrama que envío la fuente. Por otra parte, sabemos que el encabezado "datagram" contiene campos, como "time to live", que cambia cada vez que el datagrama pasa a través de un ruteador. Así, el destino final no recibirá exactamente el mismo diagrama que envío la fuente. Debemos concluir que, a pesar de que la mayor parte de los datagramas permanecen intactos cuando pasan a través de una red de redes, el principio de estratificación por

capas solo se aplica a los datagramas que realizan transferencias de una sola máquina. Para ser precisos, no debemos considerar que las capas de Internet proporcionen un servicio punto a punto.

Estratificación Por Capas En Presencia De Una Subestructura De Red

Cuando un ruteador recibe un datagrama, este puede entregar el datagrama en su destino o en la red local, o transferir el datagrama a través de una línea serial hacia otro ruteador. La cuestión es la siguiente: "¿Cómo se ajusta el protocolo utilizado en una línea serial con respecto al esquema de estratificación por capas del TCP/IP?" La respuesta depende de como considera el diseñador la interconexión con la línea serial.

Desde la perspectiva del IP, el conjunto de conexiones punto a punto entre ruteadores puede funcionar como un conjunto de redes físicas independientes o funcionar colectivamente como una sola red física. En el primer caso, cada enlace físico es tratado exactamente como cualquier otra red en una red de redes. A esta se le asigna un número único de red (por lo general de clase C) y los dos anfitriones que comparten el enlace tienen cada uno una dirección única IP asignada para su conexión. Los ruteadores se añaden a la tabla de ruteo IP como lo harían para cualquier otra red. Un nuevo módulo de software se añade en la capa de interfaz de red para controlar el nuevo enlace de hardware, pero no se realizan cambios sustanciales en el esquema de estratificación por capas. La principal desventaja del enfoque de redes independientes es la proliferación de números de redes (uno por cada conexión entre dos maquinas), lo que ocasiona que las tablas de ruteo sean tan grandes como sea necesario. Tanto la línea serial IP (Serial Line IP o SLIP) como el protocolo punto a punto (Point to Point Protocol o PPP) tratan a cada enlace serial como una red separada.

El segundo método para ajustar las conexiones punto a punto evita asignar múltiples direcciones IP al cableado físico. En lugar de ello, se tratan a todas las conexiones colectivamente como una sola red independiente IP con su propio formato de trama, esquema de direccionamiento de hardware y protocolos de enlace de datos. Los ruteadores que emplean el segundo método necesitan solo un número de red IP para todas las conexiones punto a punto.

Usar el enfoque de una sola red significa extender el esquema de estratificación por capas de protocolos para añadir una nueva capa de ruteo dentro de la red, entre la capa de interfaz de red y los dispositivos de hardware. Para las máquinas con una sola conexión punto a punto, una capa adicional parece innecesaria.

El proceso seria del siguiente modo, el software de la capa Internet pasa hacia la interfaz de red todos los datagramas que deberá enviarse por cualquier conexión punto a punto. La interfaz los pasa hacia él módulo de ruteo dentro de la red que, además, debe distinguir entre varias conexiones físicas y rutear el datagrama a través de la conexión correcta.

El programador que diseña software de ruteo dentro de la red determina exactamente como selecciona el software un enlace físico. Por lo general, el algoritmo conduce a una tabla de ruteo dentro de la red. La tabla de ruteo dentro de la red es análoga a una tabla de ruteo de una red de redes en la que se especifica una transformación de la dirección de destino hacia la ruta. La tabla contiene pares de enteros, (D, L), donde D es una dirección de destino de un anfitrión y L especifica una de las líneas físicas utilizadas para llegar al destino.

Las diferencias entre una tabla de ruteo de red de redes y una tabla de ruteo dentro de la red son que esta ultima, es mucho más pequeña. Contiene solamente información de ruteo para los anfitriones conectados directamente a la red punto a punto. La razón es simple: la capa Internet realiza la transformación de una dirección de destino arbitraria hacia una ruta de dirección específica antes de pasar el datagrama hacia una interfaz de red. De esta manera, la capa dentro de la red solo debe distinguir entre máquinas en una sola red unto a punto.

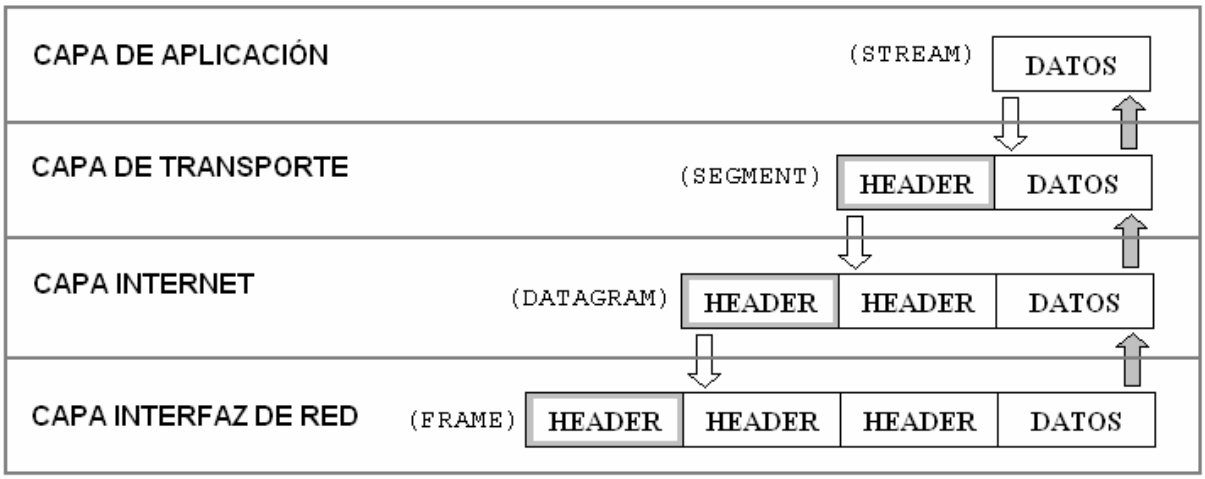
La Desventaja De La Estratificación Por Capas

La estratificación por capas es una idea fundamental que proporciona las bases para el diseño de protocolos. Permite al diseñador dividir un problema complicado en subproblemas y resolver cada parte de manera independiente. Por desgracia, el software resultante de una estratificación por capas estrictas puede ser muy ineficaz. Si se considera el trabajo de la capa de transporte, debe aceptar un flujo de octetos desde un programa de aplicación, dividir el flujo en paquetes y enviar cada paquete a través de la red de redes. Para optimizar la transferencia, la capa de transporte debe seleccionar el tamaño de paquete más grande posible que le permita a un paquete viajar en una trama de red. En particular, si la máquina de destino está conectada a una máquina de la misma red de la fuente, solo la red física se verá involucrada en la transferencia, así, el emisor puede optimizar el tamaño del paquete para esta red. Si el software preserva una estricta estratificación por capas, sin embargo, la capa de transporte no podrá saber como ruteará él modulo de Internet él trafico o que redes están conectadas directamente. Mas aun, la

capa de transporte no comprenderá el datagrama o el formato de trama ni será capaz de determinar como deben ser añadidos muchos octetos de encabezado a un paquete. Así, una estratificación por capas estricta impedirá que la capa de transporte optimice la transferencia.

Por lo general, las implantaciones atenúan el esquema estricto de la estratificación por capas cuando construyen software de protocolo. Permiten que información como la selección de ruta y la MTU de red se propaguen hacia arriba. Cuando los buffers realizan el proceso de asignación, generalmente dejan espacio para encabezados que serán añadidos por los protocolos de las capas de bajo nivel y pueden retener encabezados de las tramas entrantes cuando pasan hacia protocolos de capas superiores. Tal optimización puede producir mejoras notables en la eficiencia siempre y cuando conserve la estructura básica en capas.

Como Funciona Tcp/Ip



TCP suministra una serie de servicios a los niveles superiores. Esta sección presenta brevemente esos servicios.

TCP es un protocolo orientado a conexión. Esto quiere decir que TCP mantiene información del estado de cada cadena de datos de usuario que circula por él. El término utilizado en este contexto significa también que TCP es responsable de la transferencia de datos entre extremos por la red o redes hasta la aplicación de usuario receptora (o el protocolo de nivel superior). TCP debe asegurar que los datos se transmiten y reciben correctamente por los computadores atravesando las correspondientes redes.

Y como TCP es un protocolo orientado a conexión, es también responsable de la transferencia fiable de cada uno de los caracteres (bytes u octetos) que reciben del nivel superior correspondiente. En consecuencia, utiliza números de secuencia y aceptaciones/rechazos.

El término asociado con estos aspectos de los protocolos orientados a conexión es el de circuito virtual.

Cada octeto transmitido lleva asignado un número de secuencia. El módulo TCP receptor utiliza una rutina de checksum para comprobar la posible existencia de daños en los datos producidos en el proceso de transmisión. Si los datos son aceptables, TCP envía una acepción positiva (ACK) al módulo TCP remitente. Si los datos han resultado dañados, el TCP receptor los descarta y utiliza un número de secuencia para informar al TCP remitente del problema. Como muchos otros protocolos orientados a conexión, TCP emplea temporizadores para garantizar que no transcurre un lapso de tiempo demasiado grande antes de la transmisión de aceptaciones desde el nodo receptor y/o de la transmisión de datos desde el nodo transmisor.

TCP recibe datos de un protocolo de nivel superior de forma orientada a cadenas. Esto es diferente a muchos otros protocolos empleados en la industria. Los protocolos orientados a cadenas se diseñan para enviar caracteres separados y no bloques, tramas, datagramas, etc. Los datos son enviados por un protocolo de nivel superior en forma de cadenas, byte a byte. Cuando llegan al nivel TCP, los bytes son agrupados para formar segmentos TCP. Dichos segmentos se transfieren a IP (o a otro protocolo de nivel inferior) para su transmisión al siguiente destino. La longitud de los segmentos la determina TCP, aunque el realizador de un determinado sistema puede determinar la forma en que TCP toma su decisión. Los realizadores de TCP que han trabajado con sistemas orientados a bloques, como los sistemas operativos de IBM, puede que tengan que modificar ligeramente su forma de pensar acerca de las prestaciones de TCP. TCP admite el uso de segmentos de longitud variable, debido a su diseño orientado a cadenas. Por tanto, las aplicaciones que trabajan normalmente con bloques de datos de longitud fija (una aplicación de gestión de personal que envíe registros de empleados de longitud fija o una aplicación de gestión de nóminas con registros de pago también longitud fija) no pueden utilizar TCP para transmitir bloques fijos al receptor. El nivel de aplicación debe ocuparse de configurar los bloques dentro de las cadenas de TCP.

TCP comprueba también la duplicidad de los datos. En el caso de que el TCP remitente decida retransmitir los datos, el TCP descarta los datos redundantes. Estos datos redundantes podrían aparecer en la interred, por ejemplo cuando el TCP receptor no acepta el tráfico de manera temporizada, en cuyo caso el TCP remitente decidirá retransmitir los datos.

Además de la capacidad de transmisión de cadenas, TCP soporta también el concepto de función push. Esta función se utiliza cuando una aplicación desea asegurarse de que todos los datos que han pasado al nivel inferior se han transmitido. Para hacer eso, gobierna la gestión del buffer de TCP. Para obtener esta función,

el protocolo de nivel superior envía una orden a TCP con un identificador de parámetro de push a 1. Esta operación implica que TCP envía todo el tráfico almacenado en forma de segmento o segmentos hacia su destino.

Además de utilizar los números de secuencia para aceptaciones, TCP los utiliza para la reordenación de los segmentos que llegan a su destino fuera de orden. Como TCP descansa sobre un protocolo no orientado a conexión, es bastante posible que en la interred se creen datagramas duplicados. TCP también elimina los segmentos duplicados.

TCP emplea un esquema de aceptación inclusiva. El número de aceptación acepta todos los octetos hasta (e incluyendo) el del número de aceptación menos uno. Este esquema es un método muy sencillo y eficiente de aceptar tráfico, pero presenta una desventaja. Por ejemplo, supongamos que se han transmitido diez segmentos y debido a las operaciones realizadas durante el proceso de encaminamiento llegan desordenados. TCP está obligado aceptar sólo el mayor número de segmentos contiguos recibidos sin error. No está permitido aceptar el segmento de mayor número recibido hasta que hayan llegado todos los segmentos intermedios. Por tanto, como en cualquier otro protocolo orientado a conexión, podría transcurrir el periodo de temporización de aceptaciones y TCP transmisora retransmitiría el tráfico no aceptado todavía. Esas retransmisiones podrían introducir una considerable sobrecarga en la red.

El módulo TCP receptor se ocupa también de controlar el flujo de los datos del transmisor, lo que es muy útil para evitar el desbordamiento de los dispositivos de almacenamiento y la saturación de la máquina receptora. La idea que utiliza TCP es algo poco usual en protocolos de comunicación. Se basa en enviar el dispositivo transmisor un valor de "ventana". Se permite que el transmisor envíe un número máximo de bytes igual al valor de su ventana. Cuando se ha llegado a ese valor, la ventana se cierra y el transmisor debe interrumpir el envío de datos.

Además, TCP posee una facilidad muy útil que permite multiplexar varias sesiones de usuario en un mismo computador. Esta operación se realiza definiendo algunas convenciones para compartir puertos y sockets entre usuarios.

TCP proporciona transmisión en modo dúplex integral entre las entidades que se comunican. De esta forma, la transmisión se puede efectuar en ambos sentidos sin necesidad de esperar a la señal de indicación de cambio de sentido, necesaria en las transmisiones semidúplex. Además, TCP permite a los usuarios especificar niveles de seguridad y prioridades de las conexiones. Aunque esas opciones no están incluidas en todos los protocolos TCP, están definidas en el estándar TCP.

TCP proporciona el cierre seguro de los circuitos virtuales (la conexión lógica entre dos usuarios). El cierre seguro se ocupa

de que todo el tráfico sea reconocido antes de la desactivación del circuito virtual.

Aperturas Activa Y Pasiva

Los puertos TCP pueden establecer dos tipos de conexiones. El modo de apertura pasiva permite que el protocolo de nivel superior (por ejemplo, un servidor) indique al TCP y al sistema operativo del computador que va a esperar la llegada de solicitudes de conexión procedentes del sistema remoto, en lugar de enviar una apertura activa. Tras recibir esta solicitud, el sistema operativo asigna un número de puerto a este extremo. Esta utilidad se puede usar para realizar comunicaciones con usuarios remotos sin tener el retardo de la apertura activa.

Los procesos de aplicaciones que solicitan la apertura pasiva pueden aceptar una solicitud de cualquier usuario (supuesto que se cumplen algunos requisitos de compatibilidad). Si se puede aceptar cualquier llamada (sin requisitos de compatibilidad) el número de socket exterior se pone a ceros. Los números de socket exterior no especificados sólo se permiten en aperturas pasivas.

La segunda forma de establecimiento de conexión es el modo de apertura activa. En esta situación, el protocolo de nivel superior designa específicamente otro socket por el que establecer la conexión. Típicamente, se envía la apertura activa a un puerto con apertura pasiva para establecer un circuito virtual.

TCP admite un escenario en el que se envían dos aperturas activas de un sistema a otro a la vez. TCP realizará la conexión. Esta característica permite que las aplicaciones envíen una apertura en cualquier momento, sin preocuparse de si la otra aplicación ha enviado otra apertura o no.

TCP establece convenciones estrictas sobre cómo se deben utilizar conjuntamente las aperturas activas y pasivas. En primer lugar, una apertura activa identifica un socket específico, así como sus niveles de prioridad y de seguridad. TCP garantiza una apertura si el socket remoto tiene una apertura pasiva compatible, o si ha enviado una apertura activa compatible.

El Bloque De Control De Transmisión (TCB)

Como TCP debe recordar varias cosas de cada conexión virtual, almacena esa información en un Bloque de Control de Transmisión (TCB). Entre la información que se almacena en la TCB destacamos los números de socket local y remoto, los punteros a los buffers de transmisión y recepción, los punteros a la cola de retransmisión, los valores de seguridad y prioridad de la conexión y el segmento en curso. La TCB también contiene varias variables asociadas a los números de secuencia de envío y recepción.

El Segmento TCP (PDU)

Las PDU que se intercambian entre dos módulos TCP se denominan segmentos. El segmento se divide en dos partes, la parte de cabecera y la parte de datos. La parte de datos sigue a la parte de cabecera.

Los primeros dos campos del segmento se denominan puerto de fuente y puerto de destino. Esos campos de 16 bits identifican a los programas de aplicación de nivel superior que utilizan la conexión TCP.

El siguiente campo se denomina número de secuencia. Este campo contiene el número de secuencia del primer octeto del campo de datos de usuario. Su valor especifica la posición de la cadena de bits del módulo transmisor. Dentro del segmento especifica el primer octeto de datos de usuario.

El número de secuencia se utiliza también durante la operación de gestión de la conexión. Si dos entidades TCP utilizan el segmento de solicitud de conexión, entonces el número de secuencia especifica el número de secuencia de envío inicial (ISS) que se utilizará para la numeración subsiguiente de los datos de usuario.

El valor del número de aceptación permite aceptar los datos previamente recibidos. Este campo contiene el valor del número de secuencia del siguiente octeto que se espera recibir del transmisor. Con esa definición permite la aceptación inclusiva, en el sentido de que permite la aceptación de todos los octetos hasta, e incluyendo, el valor de este número menos 1.

El campo de desplazamiento de datos especifica el número de palabras alineadas de 32 bits de que consta la cabecera de TCP. Este campo se utiliza para determinar dónde comienza el campo de datos.

Como puede esperarse, el campo reservado está reservado. Consta de 6 bits que deben valer cero. Estos bits están reservados para usos futuros.

Los seis bits siguientes se denominan indicadores o banderas (flags). Son bits de control de TCP y se utilizan para especificar ciertos servicios o utilidades que se pueden emplear durante la sesión. El valor de algunos de esos bits indica cómo interpretar otros campos de la cabecera. Los seis bits mencionados llevan la siguiente información.

- URG indica que el campo de puntero de urgencia es significativo.
- ACK indica si el campo de aceptación es significativo.
- PSH significa que el módulo va a utilizar la función push.
- RST indica que la conexión se va a inicializar.

- SYN indica que se van a sincronizar los números de secuencia; se utiliza en los segmentos de establecimiento de conexión como indicación de que se van a realizar algunas operaciones de preparación.
- FIN indica que el remitente no tiene más datos para enviar. Es comparable a la señal de fin de transmisión (EOT) en otros protocolos.

El campo siguiente, denominado ventana, se pone a un valor que indica cuántos octetos desea aceptar el receptor. Este valor se establece teniendo en cuenta el valor del campo de aceptación (número de aceptación). La ventana se establece sumando los valores del campo de ventana y del campo de número de aceptación.

El campo de checksum contiene el complemento de 1 a 16 bits del complemento a 1 de la suma de todas las palabras de 16 bits del segmento, incluyendo la cabecera del texto. El propósito de este cálculo es determinar si el segmento procedente del transmisor ha llegado libre de errores.

El siguiente campo del segmento, denominado puntero de urgente, se utiliza sólo si el indicador de URG está a 1. El objeto de este puntero es identificar el octeto de datos al que siguen datos urgentes. Los datos urgentes se denominan datos fuera de banda. TCP no dice lo que hay que hacer con los datos urgentes. Depende de la implementación. Dicho de otro modo, sólo se indica el lugar donde empiezan los datos urgentes, no lo que hay que hacer con ellos. El valor de este campo es un desplazamiento del número de secuencia y apunta al octeto a partir de cual siguen los datos urgentes. El campo de opciones está concebido para posibilitar futuras mejoras de TCP. Está diseñado de forma semejante al campo de opción de los datagramas de IP, en el sentido de que cada opción se especifica mediante un byte que especifica el número de opción, un campo que contiene la longitud de la opción y finalmente, los valores de la opción propiamente dichos.

Actualmente el campo de opción tiene un uso bastante limitado, y el estándar TCP sólo especifica tres opciones:

0 : fin de lista de opciones
1 : no operación
2 : tamaño máximo de segmento

Finalmente, el campo de relleno asegura que la cabecera TCP ocupa un múltiplo par de 32 bits. Finalmente siguen los datos de usuario.

Direcciones IP

Introducción

Ya se planteo una idea básica de lo que son las direcciones IP, pero ahora detallaremos su funcionamiento. Como sabemos para que la información llegue a cada máquina, es necesario que estas tengan una "dirección" dentro de la red. En el caso de Internet estas direcciones se llaman direcciones IP, y en principio a cada máquina de la Red se le asigna una (los mensajes incluyen las direcciones IP de las máquinas origen y destino).

Métodos De Difusión En Tecnología De Redes

Para entender mejor el sistema de direcciones de Internet, comenzaremos diciendo que en tecnología de redes se emplean dos métodos distintos, bridging y routing. En el sistema bridging, las direcciones no contienen ninguna información sobre donde está la máquina a la que va destinado el paquete. El principio de funcionamiento supone que los paquetes circulan por "toda" la red. Todas las máquinas recibirán todos los paquetes, y solo prestarán atención a los que correspondan a su dirección. Esta técnica de transmitir en la que todos los elementos de la red reciban la información se denomina multi-difusión ("Broadcast") y es evidente que no resulta un sistema muy adecuado para redes medianas, grandes o de mucho tráfico, porque la sobrecarga del sistema se hace rápidamente insostenible. Las redes Ethernet y Token Ring pertenecen a esta primera categoría.

El routing por su parte es mas elaborado, se supone que las direcciones contienen información sobre "donde" está la computadora de destino dentro de la red, podríamos decir que se parece al sistema de direcciones del correo ordinario; esto hace posible la existencia de sistemas enrutadores ("Routers") que hacen seguir cada mensaje en la dirección adecuada. Es el sistema utilizado por Internet, ya que el bridging es impracticable para redes muy grandes. Es conveniente tener clara la distinción entre dirección y ruta; en este sistema (routing), la ruta está implícita en la dirección, pero su concreción está contenida en las denominadas tablas de rutas ("Routing tables"). Los sistemas routing suelen tener una estructura de niveles, en cada uno debe haber un equipo que se encargue de las tablas de ruta de ese nivel.

Las Direcciones IP

El sistema de direcciones de Internet estableció un sistema jerárquico de direcciones, asignándose un número (dirección) a cada red (no olvidar que Internet es una red de redes) y un número a cada ordenador particular dentro de la red ("Host address"). El sistema estableció que las direcciones estarían contenidas en una

etiqueta de 32 bits (4 octetos). Resulta así que cada máquina tiene una única dirección, que en binario tendría un aspecto como:

11001100011110110000001001001011

Hay cuatro formatos para la dirección IP, cada uno de los cuales se utiliza dependiendo del tamaño de la red. Los cuatro formatos, Clase A hasta Clase D (aunque últimamente se ha añadido la Clase E para un futuro)

CLASE A

CLASE B

CLASE C

CLASE D

Conceptualmente, cada dirección está compuesta por un par (RED (netid), y Dir. Local (hostid)) en donde se identifica la red y el host dentro de la red.

La clase se identifica mediante las primeras secuencias de bits, a partir de los 3 primeros bits (de orden más alto).

Las direcciones de Clase A corresponden a redes grandes con muchas máquinas. Las direcciones en decimal son 0.1.0.0 hasta la 126.0.0.0 (lo que permite hasta 1.6 millones de hosts).

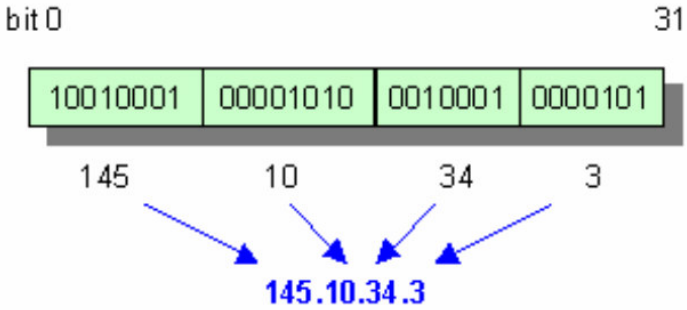
Las direcciones de Clase B sirven para redes de tamaño intermedio, y el rango de direcciones varía desde el 128.0.0.0 hasta el 191.255.0.0. Esto permite tener 16320 redes con 65024 host en cada una.

Las direcciones de Clase C tienen sólo 8 bits para la dirección local o de anfitrión (host) y 21 bits para red. Las direcciones de esta clase están comprendidas entre 192.0.1.0 y 223.255.255.0, lo que permite cerca de 2 millones de redes con 254 hosts cada una.

Por último, las direcciones de Clase D se usan con fines de multidifusión, cuando se quiere una difusión general a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.235.255.

Cabe decir que, las direcciones de clase E (aunque su utilización será futura) comprenden el rango desde 240.0.0.0 hasta el 247.255.255.255.

Esta dirección que es representada en números decimales mediante un conjunto de 4 cantidades separadas por puntos (una por octeto), con un aspecto tal como por ejemplo: 204.123.2.75. Por esta razón este tipo de notación se conoce como representación decimal punteada "Dotted decimal notation". Por supuesto cada conjunto de cifras está comprendido en el rango entre 0 y 255 (cualquier cantidad fuera de dicho rango no corresponde con una dirección IP real). Las cifras de la izquierda son las más significativas y van perdiendo peso hacia la derecha (exactamente igual que el sistema tradicional de numeración).



En la figura se indica el proceso de traducción de los 32 bits a la notación decimal.

La dirección IP es lo mas parecido al número de teléfono de las computadoras de la Red, solo que en esta jerga no se habla de "números de teléfono" sino de "direcciones IP". Cuando el navegador, un programa de descarga de archivos o cualquier otro "llama" a una dirección IP, lo que hace en realidad es conectar (intercambiar paquetes) con el ordenador propietario de tal número (de tal dirección IP). Una estructura como esta (de 32 bits) ofrece un máximo teórico de 2^{32} = 4.294.967.296 direcciones distintas.

Naturalmente, todo esto necesita una supervisión y control. Originariamente, era la NSF (National Science Foundation), la encargada de gestionar lo relativo a la organización de Internet, después delegó en Network Solutions, una compañía USA; esta colaboración recibió el nombre genérico de InterNIC, por último, a partir de 1998 es ICANN, una organización internacional sin fines de lucro.

Protocolo IPv4

El protocolo IP de 4 bytes usado actualmente (versión 4, IPv4) lleva mas de 20 años funcionando en Internet (es de los años 70, aunque la última revisión es de 1981) pero está alcanzando su límite, los expertos pronostican que de seguir el ritmo actual de

expansión, no podrá aguantar mas allá del 2010, por lo que se están estudiando alternativas, como las definidas en la versión 6 (IPv6, también conocida como IPng) que será su sustituto. Entre los motivos principales que se citan para promover el cambio, está el agotamiento de la capacidad de direcciones nuevas en el sistema actual, también la emergencia de nuevas aplicaciones y modos de utilización de la Web, por ejemplo la computación personal portátil (nómada), las aplicaciones de ocio, la calidad del servicio y la seguridad en las comunicaciones (piense en todo lo relacionado con el comercio electrónico, por ejemplo).

Servicio De Nombres De Dominio (DNS)

Introducción

El servicio de direcciones IP se estandarizó en representarse por 32 bits y para facilitar su identificación (humana), este conjunto se considera formado por 4 octetos, que se representan por números separados por puntos, del tipo 145.10.34.3, lo que se denomina la notación decimal punteada ("Dotted-decimal notation").

Para facilitar la introducción y el recordatorio de estas direcciones por los operadores, se usan nemónicos, es decir, nombres que si tienen un significado (del tipo: altavista.digital.com). De forma que a cada nombre (fácil de recordar e introducir) le correspondería una dirección IP; además el sistema de nombres hace mas evidente el sistema jerárquico de la estructura de direcciones ("Routing address") adoptada para Internet que detallamos a continuación, aunque para evitar confusiones, antes puntualizaremos la nomenclatura empleada:

Nomenclatura

- Dirección IP: Un número de 32 bits; generalmente viene expresado en forma decimal punteada. Es importante recordar que estos "números de teléfono" de las computadoras de la red corresponden a una red mundial; aquí no ocurre lo mismo que en el teléfono, donde dos abonados de ciudades o países distintos pueden tener el mismo número. Las direcciones IP son únicas y de su gestión se encarga ICANN, un organismo internacional.

- Nombre de dominio: Nombre alfanumérico que identifica una computadora o conjunto de ellas (sub-red) en Internet (red de redes).

Para entender el resto del asunto, es preciso establecer claramente el concepto de "dominio", que sugiere algo extenso, proviene de que las direcciones primitivas se referían a

computadoras de grandes instituciones, que pronto dejaron de ser computadoras únicas, deviniendo en sitios donde a su vez existían varias computadoras en red (Intranets). Por ejemplo: ucla.edu no era una computadora aislada, sino a una serie de ellas.
Actualmente, la situación ha cambiado en parte, una misma máquina (o conjunto de ellas), sobre todo los sistemas de los ISP (Proveedores de Servicios de Internet), albergan dominios de diversos clientes, por lo que el concepto de dominio se distanció del de máquina concreta o subred de computadoras. En el estado actual, un dominio es meramente una concesión administrativa, se asocia con un nombre (único) y generalmente referencia a una sola máquina en la red.

- Nombre de servicio ("Service name"): Una cadena alfabética corta que identifica un servicio específico de Internet, por ejemplo: HTTP, FTP, TELNET, etc.

El Sistema DNS

Para automatizar el proceso y hacerlo transparente para el usuario, en 1984 se estableció un servicio de traducción de nombres a números (y a la inversa), por el procedimiento de incluir en algunas computadoras del sistema, unas **tablas** que permitieran saber que altavista.digital.com equivale a 204.123.2.75.

Las computadoras que contienen estas tablas se llaman *Servidores de Nombre*, abreviadamente NS "Name Servers"; además de las mencionadas tablas disponen de un software capaz de responder a las peticiones de información. De esta forma, aunque las máquinas usan las direcciones numéricas nosotros podemos utilizar directamente los nombres de dominio. Sin embargo el sistema DNS tiene una finalidad adicional a la mera traducción de nombres a números y viceversa, y es que derivado al crecimiento desmesurado de Internet un servidor de nombres no podía almacenar la tabla completa con la dirección/nombre de todos los computadoras de la red (y menos mantenerla actualizada), por lo que se estableció una estructura jerárquica para los NS de forma que en la cúspide están los servidores de nombres raíz ("Root-Nameservers") que administran los dominios de primer nivel. Estos contienen las direcciones de otros servidores que administran los diferentes dominios de segundo nivel y así sucesivamente. El proceso es parecido al que sigue una carta ordinaria en el sistema postal internacional. En realidad el servicio de Correos de cada país no tiene porqué saber donde está cada destinatario del mundo; en principio le basta saber como enviar una carta a su país de destino. Una vez en el país de destino el servicio central no necesita saber donde está cada dirección, basta que sepa enviarlo

a la ciudad correspondiente. Dentro de esta puede ser redistribuida por zonas. Finalmente el cartero atiende una zona o barrio concreto y es capaz de saber con precisión donde está cada calle, cada número y cada piso.

Al sistema que resultó de todo esto se le denomina **Servicio de Nombres de Dominio** DNS ("Domain Name Service"), es el "servicio" encargado de transformar nombres, como nba.com, en cifras, como 10.25.143.12; como veremos, el DNS también juega un papel importante en el sistema de tráfico del correo de Internet (e-mail).

El Espacio De Nombres

Para los nombres se creó una estructura jerárquica denominada espacio de nombres ("Namespace") y ciertas reglas. Los nombres de dominio pueden estar formados por dos o más palabras separadas por puntos (recuerdan a sus ancestros numéricos), solo podían usarse minúsculas, y normalmente se estructuran de forma que la parte izquierda es la más específica y la derecha la mas general. Por ejemplo, la designación ibm.armonk.ny.us se refiere a un dominio de IBM en la ciudad de Armonk, estado de Nueva York en USA, otra empresa XYZ de la misma ciudad podría tener un dominio de nombre xyz.armonk.ny.us

Las estructuras de nombres dentro de los diversos países muestran grandes diferencias. En cualquier caso la responsabilidad de la administración de nombres de cada terminación es del administrador de cada país. En algunos prácticamente no existe estructura bajo la terminación genérica del país, en cambio en otros, existen clasificaciones genéricas de segundo nivel, con otras terminaciones (por ejemplo: .ac, .co, .go, .re, etc.), en otros existe una organización de segundo nivel basada en geografía política (caso de USA) Finalmente, en otros países, los usuarios están directamente bajo el primer nivel (caso de España), donde todas las terminaciones son del tipo xxxxx.es sin más estructura.

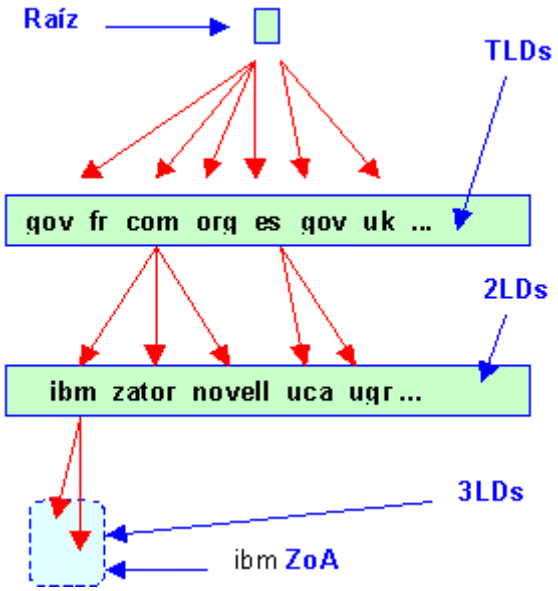
Top Level Domain Names (TLDs)

Para la estructura se adoptó en forma de árbol invertido, a cada rama le corresponde un nombre alfanumérico. Al nivel más alto, la raíz, no se le ha dado ningún nombre especial. Debajo de este están los nombres de dominio de alto nivel, TLDs ("Top Level Domain Names"). En este nivel se establecieron en principio 8 dominios genéricos (una especie de apellidos) que englobarían los diversos dominios según un esquema que dependía del tipo de institución que utiliza el nombre. Los TLDs originales de ARPANET eran 4 a los que posteriormente se añadieron otros 4, son los siguientes:

.com	Empresas comerciales.
.edu	Educacional (Universidades y colegios).
.org	Organizaciones de fin no lucrativo.
.net	Redes de computadoras independientes pero conectadas a Internet
.int	Internacional.
.gov	Gobierno (Organismos oficiales USA)
.mil	Organismos militares USA
.nato	Organización del Tratado del Atlántico Norte (OTAN/NATO).

Con la explosión de Internet, cuando ya había instituciones y organismos de los cinco continentes y prácticamente de todos los países, hubo que ampliar el sistema, utilizando terminaciones que recordaran al país correspondiente, por ejemplo:

.ar	Argentina
.es	España
.uk	Reino Unido
.fr	Francia
.gi	Gibraltar (con protestas por parte de España)
.va	Vaticano



Parece ser que con esto se acaban los nombres "Top Level", pero no es asi, en el año 2000, ICANN introdujo siete nuevos TLDs: .aero, .biz, .coop, .info, .museum, .name, y .pro. Seguramente que se agregaran nuevos en el futuro.

Debajo de estos cuelgan los dominios de segundo nivel (2LDs), por ejemplo ibm.com. Por debajo este segundo nivel se pueden crear estructuras de nombres de tercer nivel (3LDs) pero que son ya responsabilidad de las organizaciones propietarias del dominio de segundo nivel.

Nota: El dominio raíz y los de alto nivel (TLDs) son responsabilidad de las autoridades de registro de nombres de Internet (ICANN).

En el caso de la figura anterior, la interpretación de los nombres de dominio terminados en ibm.com está a la discrecionalidad de IBM, que gobierna el área que pueda colgar de su "rama" (el espacio de su nombre de dominio), también conocido como zona de autoridad ZoA ("Zone of Authority"). Por ejemplo: si la empresa Ford Motors tiene un dominio, digamos ford.com, puede establecer sucesivos niveles correspondientes a sub-redes o máquinas

específicas dentro de su organización: spain.ford.com, international.ford.com, france.ford.com, etc.

ICANN

El organismo internacional que gestiona estos aspectos de Internet es el ICANN (Internet Corporation for Assigned Names and Numbers); una de sus misiones es gestionar la concesión de nombres de dominio, y sus correspondientes direcciones IP, en este sistema telefónico mundial de computadoras que es el sistema DNS.

En el año 2002, el núcleo del sistema de nombres lo constituían 13 servidores especiales, repartidos por el mundo y controlados por la ICANN, que contienen tablas con los nombres de dominio y sus correspondientes direcciones IP de todos los 2LDs del mundo. Estos servidores, denominados servidores raíz o también TNS ("Top Name Servers"), contienen todos la misma información, y constituyen el corazón del sistema de Internet; el hecho de ser 13 es para repartir la carga de trabajo, y el contener todos la misma información permite que cada uno sirva de copia de seguridad a los demás. Sin embargo su distribución no es muy homogénea: diez de ellos están situados en Estados Unidos, dos en Europa (Londres y Estocolmo) y el último en Japón.

Un 2LD puede pertenecer a una institución importante, que físicamente dispone de una computadora propia o incluso toda una sub-red conectada a Internet; también el caso opuesto: una pequeña empresa (o particular) que no mantiene servidor de Internet propio, utilizando para esta función un ordenador (de su ISP) compartido con otros. En cualquier caso, gran empresa (un dominio de varias computadoras) o pequeña (una computadora con varios dominios), ambas tienen una zona potencial de autoridad (ZoA), y son responsables de resolver las direcciones que hubiera en ella. Si se trata de una gran empresa (caso de IBM), esta tiene su propio servidor de nombres para resolver los nombres bajo su ZoA, en cambio, si es pequeña, lo más probable es que no mantenga servidor propio de nombres, delegando esta función en su ISP.

Cuando alguien, en cualquier parte del mundo, pregunta por una dirección, digamos xxx.ibm.com, los TNSs ("Top Name Servers") envían la llamada al servidor ibm.com (ej: 211.163.0.2) que a su vez puede informar sobre cualquier dirección IP relativa al dominio ibm.com, entre ellas la del host que atiende el servicio. Los servidores de nombres de dominio son sistemas que pueden dirigir a otros servidores de nombres que pueden dirigir a otros..., hasta que finalmente se encuentra el que realmente contiene la información buscada (para comenzar las búsquedas los ISP suelen cargar en sus máquinas las direcciones de los servidores de dominio de alto nivel TNS).

El resultado de todo esto es que después de los servidores "*maestros*", existen dispersos por el mundo millares de otras computadoras que periódicamente copian la información de los servidores raíz; son los Servidores de Nombres de Dominio ”DNS Servers” o simplemente “resolvers”. Estos servidores se localizan en redes institucionales o en proveedores de servicios de Internet ISPs (normalmente ISP y servidor DNS son el mismo), de forma que pueden ser consultados fácilmente, devolviendo la dirección IP de cualquier nombre de dominio que se interrogue.

Puesto que existen millones de servidores, es imposible que cada uno tenga actualizada la tabla de conversión, como por otra parte, existen cientos de miles de servidores DNS y no sería práctico ir preguntándoles a todos. La estructura piramidal, tanto en los nombres posibles como en los servidores, estableciéndose unos servidores "raíz" y una estructura de nombres cuyo último eslabón es el "dominio", hace que no sea necesario buscar en todos, sino que con una serie muy pequeña de consultas, se resuelva la incertidumbre.

Ya vimos que ICANN, auxiliada por empresas colaboradoras autorizadas, es la organización encargada de mantener el sistema mundial de servidores de nombres de dominio primarios, pero durante mucho tiempo, cuando la gestión estaba en manos de Network Solutions, existían delegaciones regionales con representación a su vez en cada país; estas representaciones mantenían el servidor encargado de contestar las preguntas de su propia terminación.

Direcciones IP Dinámicas

Hemos visto que las direcciones IP vienen a ser como el "número de teléfono" de las computadoras en la red. Cuando conectamos a Internet por RTB mediante un MODEM, es evidente que si nos llega la información es porque tenemos una "*dirección*" en Internet, esta dirección IP nos la asigna nuestro proveedor ISP de entre un cierto número de ellas que tiene disponibles.

Nota: No confundir esta dirección IP con el número de teléfono convencional de la compañía Telefónica mediante el que realizamos la conexión con nuestro proveedor ISP.

Aprovechando que no están conectados 24 horas al día los 365 días del año, lo que hacen los ISPs con los abonados de conexión telefónica, es utilizar una cualquiera de las que tienen libres para asignarla al cliente que se conecta en ese momento. Esto es lo que se llama asignación dinámica de IPs, o IPs dinámicas. Si por ejemplo, nuestro ISP tiene 255 direcciones IP disponibles, puede aceptar en cualquier momento un máximo de 255 clientes conectados simultáneamente (debe tener por supuesto 255 líneas de

acceso telefónico conectadas a su servidor Web, posiblemente mediante un servidor de terminales "Terminal Server", que es una computadora utilizada para conectar muchos módems con una conexión de red de alta velocidad a otra computadora (host). El servidor de terminales hace el trabajo de atender las llamadas telefónicas de los módems y pasar la comunicación al host (un nodo Internet) por la línea de alta velocidad. Esta función se conoce en informática con el nombre de "Front-End").

Por tanto, resulta más que probable, que no nos corresponda la misma dirección IP para cada conexión sucesiva. De hecho las direcciones IP dinámicas son un método de economizar direcciones compartiéndolas entre muchos usuarios potenciales. La contrapartida es que, como no tenemos siempre el mismo "número de teléfono" en Internet, no podemos decirle de antemano a otro usuario cual es nuestra dirección IP.

Nota: Por lo general existe cierta tendencia a confundir su dirección IP con su dirección de correo. La dirección IP es el "número de teléfono mundial" que nos corresponde en cada conexión que hacemos a Internet, mientras que una dirección E-mail (de correo electrónico) es la dirección de nuestro buzón, que no cambia nunca (a menos que cambiemos de ISP). Cuando alguien nos envía un e-mail, el servidor de correo de nuestro ISP lo deposita en nuestro buzón; mas tarde, cuando arrancamos nuestro cliente de correo (Ej. Microsoft Outlook), este busca automáticamente en nuestro buzón y se "baja" la correspondencia acumulada. Una vez que la transmisión ha finalizado con éxito, el servidor de correo del ISP borra el contenido del buzón en respuesta de una orden que se inicia en nuestro cliente de correo.

DHCP

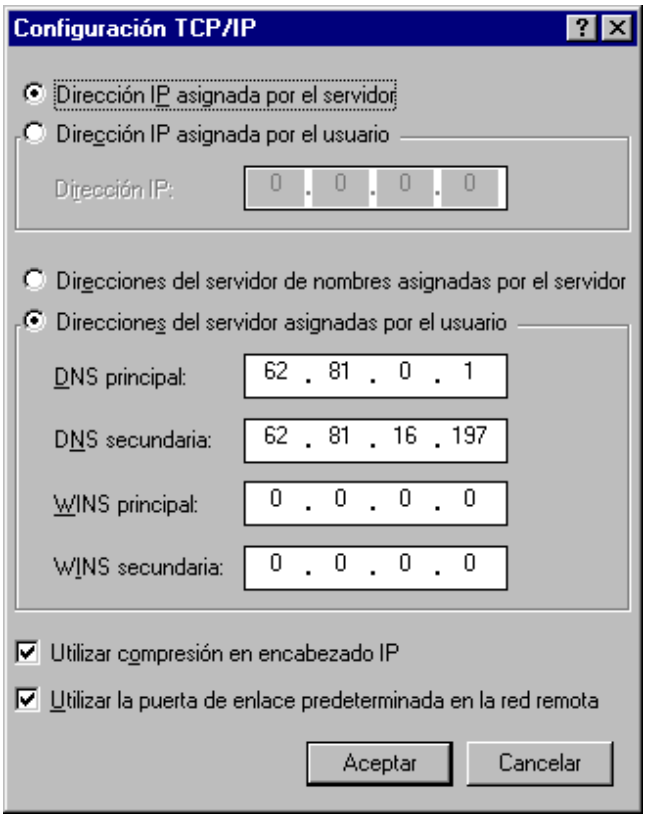
Los servidores que deben proporcionar direcciones IP dinámicas a sus clientes utilizan el protocolo DHCP ("Dynamic Host Configuration Protocol"). Este protocolo fue creado por un grupo de trabajo de la IETF con objeto de simplificar la administración de grandes redes IP, permitiendo que los equipos individuales de una red puedan obtener sus datos de configuración desde un servidor (DHCP). Esta posibilidad es especialmente útil, en especial para aquellos servidores que no tienen información exacta sobre los equipos individuales hasta que estos no recaban la información (caso típico de servidores de ISPs).

Cuando un equipo desea conectarse a Internet necesita una dirección IP, de forma que recaba una al servidor DHCP y este le asigna una de las que tiene disponibles. Los datos enviados son: Dirección IP; máscara de subred ("Subnet mask"), y puerta de enlace predeterminada ("Default Gateway").

Para conectarse a la red cualquier máquina necesita también la dirección de al menos un servidor de nombres (DNS). Esta dirección puede ser suministrada automáticamente por DHCP o permanecer como un dato fijo en la máquina que se conecta.

Nota: Cuando en Windows 95/98 establecemos una conexión telefónica a redes para preparar la conexión a Internet mediante módem, hay que responder ciertas cuestiones acerca de la configuración TCP/IP.

En la figura adjunta se muestra el aspecto del cuadro de diálogo correspondiente. En el ejemplo de la figura se ha señalado la opción **"Dirección IP asignada por el servidor"**; esta es justamente la opción que indica que utilizaremos direcciones IP dinámicas.



A su vez, la dirección del servidor de nombres puede ser asignada por el servidor o por el usuario. En este caso se ha elegido la segunda opción. Los valores indicados corresponden a los servidores DNS primario y secundario del servidor (ISP).

Las casillas en blanco señaladas como WINS principal y WINS secundaria corresponden a las direcciones de los servidores principal y secundario de un servicio análogo a DNS denominado WINS ("Windows Internet Name Service"), corresponde a un tipo de red de Microsoft que también puede utilizar los protocolos TCP/IP pero que no se utiliza para conexión entre redes, solo para pequeñas subredes departamentales o domésticas. En este caso la

conexión se utilizará para Internet y por lo tanto no es de aplicación el servicio WINS.

Conocer La Dirección IP De Una Conexión

Si no disponemos de una IP fija (lo que solo es frecuente en empresas), en ocasiones puede ser interesante conocer la dirección IP que nos ha correspondido en una sesión. Este dato puede ser de utilidad en algunos casos. Por ejemplo para ejecutar juegos en Internet sin necesidad de servidores de juego o para que un amigo realice conexiones FTP con nuestro servidor.

Windows 95/98

Windows 95/98 tienen un programa IPconfig.exe situado normalmente en la carpeta Windows. Este programa debe ejecutarse desde una ventana MS-DOS, y acepta varias opciones en la línea de comando, que pueden obtenerse mediante:

ipconfig /H

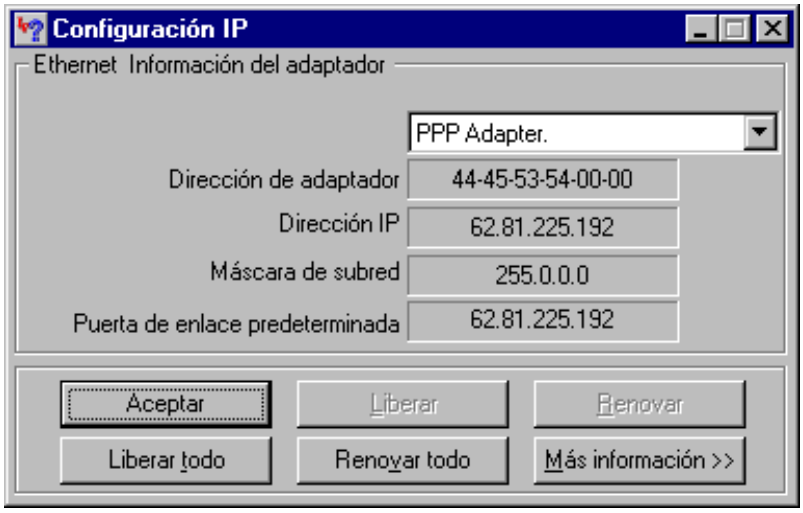
La figura muestra la información proporcionada en el momento de una conexión a Internet a través de un ISP mediante un acceso telefónico a redes (mediante módem).

Configuración IP de Windows 98

```
Nombre del host . . . . . : SIRE
Servidores DNS. . . . . : 62.81.0.1
                                      62.81.16.197
Tipo de nodo. . . . . : Difusion
Id. de ámbito NetBIOS . . . . . :
Enrutamiento IP activado. . . . . : No
WINS Proxy activado . . . . . : No
Resolución NetBIOS usa DNS. . . . . : No

0 Ethernet adaptador :

Descripción . . . . . : PPP Adapter.
Dirección física. . . . . : 44-45-53-54-00-00
DHCP activado . . . . . : Sí
Dirección IP. . . . . : 62.81.225.38
Máscara de subred . . . . . : 255.0.0.0
Puerta de enlace predeterminada . . . : 62.81.225.38
Servidor DHCP . . . . . : 255.255.255.255
Servidor WINS primario  . . . . . :
Servidor WINS secundario. . . . . :
Permiso obtenido. . . . . : 01 01 80 0:00:00
Permiso caduca. . . . . : 01 01 80 0:00:00
```

```
1 Ethernet adaptador :

Descripción . . . . . . . . . . . . . : Xircom Ethernet 10/100 + Modem
56 PC Card
Dirección física. . . . . . . . . . . : 00-10-A4-01-FF-F1
DHCP activado . . . . . . . . . . . . : Sí
Dirección IP. . . . . . . . . . . . . : 169.254.58.226
Máscara de subred . . . . . . . . . . : 255.255.0.0
Puerta de enlace predeterminada . . . :
Servidor DHCP . . . . . . . . . . . . : 255.255.255.255
Servidor WINS primario . . . . . . . :
Servidor WINS secundario. . . . . . . :
Permiso obtenido. . . . . . . . . . . : 09 04 02 7:10:07
Permiso caduca. . . . . . . . . . . . :
```

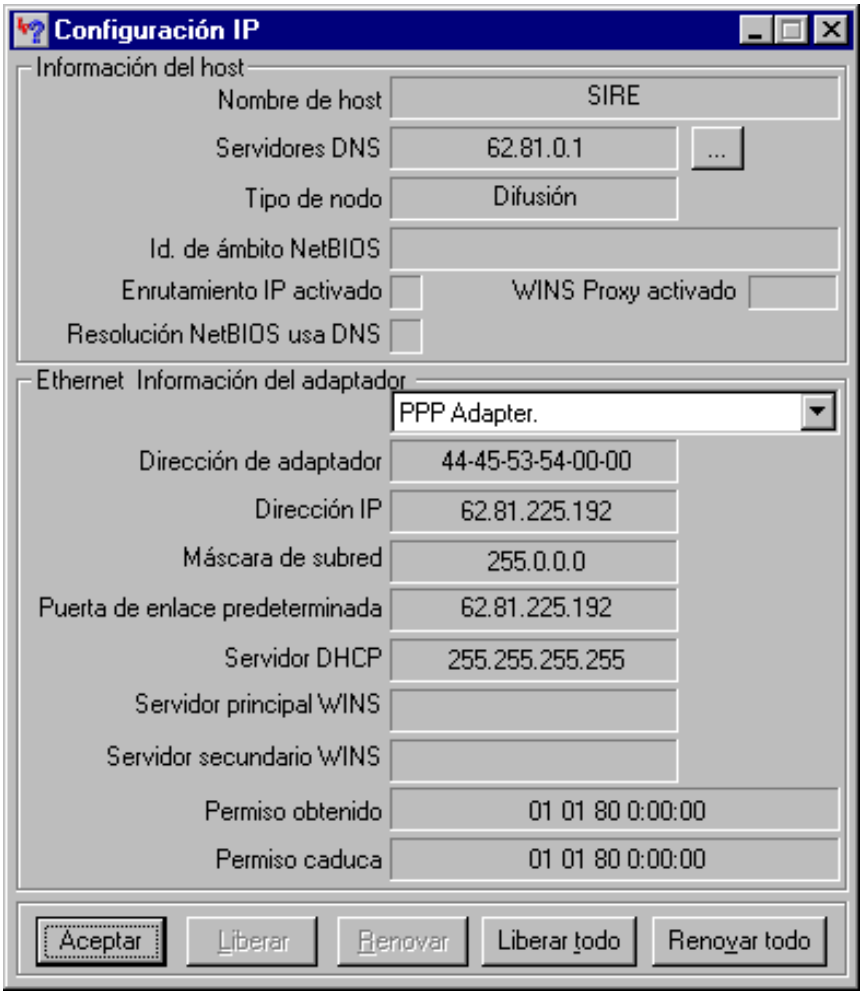
También puede utilizarse la versión Windows, que es el ejecutable Winipcfg.exe (Windows IP Configuration tool).



La figura muestra el resultado en el momento de una conexión análoga a la anteriormente descrita (IPconfig.exe).

La dirección IP indicada en la tercera ventana, en este caso 62.81.225.192, es la que ha correspondido a esta sesión. Como puede verse, aunque obtenida en el mismo equipo, es distinta de la indicada por la versión DOS (62.81.225.38) lo que nos indica que ambos resultados se han obtenido en sesiones de conexión distintas.

El programa ofrece otra pantalla con información ampliada pulsando el botón *Más información*. Esta segunda pantalla, muestra información complementaria sobre el adaptador y sobre el servidor al que estamos conectados, permitiendo comprobar algunos datos adicionales de nuestra conexión IP.



La casilla "Servidor DNS" (con el valor 62.81.0.1 en este caso), se refiere a la dirección IP de los servidores de nombre de dominio (DNS) primario y secundario que estamos utilizando.

Windows NT/2000

Desde el símbolo del sistema ("Command Prompt") escribir: ipconfig /all; el valor buscado aparece en la línea señalada dirección IP ("IP Address").

Linux

Ejecutar el programa ifconfig; el valor buscado aparece indicado como inet addr.

Enmascaramiento

El enmascaramiento ("Masquerading") es una técnica que permite que varias computadoras interconectadas compartan una misma conexión a Internet. Por ejemplo un módem o (preferiblemente) una conexión RDSI o ADSL que está conectado físicamente a una de ellas.

Su finalidad es conseguir que la dirección IP Internet asignada al equipo propietario de la conexión pueda ser compartida por otros para realizar también comunicaciones con la Red, aunque

desde el punto de vista del exterior Internet percibe un solo equipo conectado, el que realiza el enmascaramiento.

En cierta forma el equipo que efectúa la conexión física realiza también funciones de protección o cortafuegos (firewall) del resto, ya que los aísla del exterior, porque sus direcciones no son visibles desde fuera de la red local.

En UNIX y Linux el servicio es denominado enmascaramiento IP, mientras que en Windows se conoce como "Conexión compartida a Internet". En Windows9x es una opción que no se instala por defecto.

Administración TCP/IP

Por lo que vimos TCP/IP es una de las redes más comunes utilizadas para conectar computadoras con sistema UNIX y actualmente muchos sistemas operativos también lo utilizan, sobre todo el direccionamiento IP. Las utilidades de red TCP/IP forman parte de la versión 4, muchas facilidades de red como un sistema UUCP, el sistema de correo, RFS y NFS, pueden utilizar una red TCP/IP para comunicarse con otras máquinas.

Para que la red TCP/IP esté activa y funcionando será necesario:

- Obtener una dirección Internet.
- Instalar las utilidades Internet en el sistema
- Configurar la red para TCP/IP
- Configurar los guiones de arranque TCP/IP
- Identificar otras máquinas ante el sistema
- Configurar la base de datos del ente de STREAMS
- Comenzar a ejecutar TCP/IP.

¿Qué Es Internet?

Internet es una red de computadoras que utiliza convenciones comunes a la hora de nombrar y direccionar sistemas. Es una colección de redes independientes interconectadas; no hay nadie que sea dueño o active Internet al completo.

Las computadoras que componen Internet trabajan en UNIX, el sistema operativo Macintosh, Windows 95, 98, NT, XP y muchos otros. Utilizando TCP/IP y otros protocolos, según veremos dos servicios de red:

- Servicios de Internet a nivel de aplicación
- Servicios de Internet a nivel de red

Servicios De Internet A Nivel De Aplicación

Desde el punto de vista de un usuario, una red de redes TCP/IP aparece como un grupo de programas de aplicación que utilizan la red para llevar a cabo tareas útiles de comunicación. Utilizamos el término interoperabilidad para referirnos a la habilidad que tienen diversos sistemas de computación para cooperar en la resolución de problemas computacionales. Los programas de aplicación de Internet muestran un alto grado de interoperabilidad. La mayoría de usuarios que accesan a Internet lo hacen al correr programas de aplicación sin entender la tecnología TCP/IP, la estructura de la red de redes subyacente o incluso sin entender el camino que siguen los datos hacia su destino. Sólo los programadores que crean los programas de aplicación de red necesitan ver a la red de redes como una red, así como entender parte de la tecnología. Los servicios de aplicación de Internet más populares y difundidos incluyen:

- ***Correo electrónico***. El correo electrónico permite que un usuario componga memorandos y los envíe a individuos o grupos. Otra parte de la aplicación de correo permite que un usuario lea los memorandos que ha recibido. El correo electrónico ha sido tan exitoso que muchos usuarios de Internet dependen de él para su correspondencia normal de negocios. Aunque existen muchos sistemas de correo electrónico, al utilizar TCP/IP se logra que la entrega sea más confiable debido a que no se basa en computadoras intermedias para distribuir los mensajes de correo. Un sistema de entrega de correo TCP/IP opera al hacer que la máquina del transmisor contacte directamente la máquina del receptor. Por lo tanto, el transmisor sabe que, una vez que el mensaje salga de su máquina local, se habrá recibido de manera exitosa en el sitio de destino.

- ***Transferencia de archivos***. Aunque los usuarios algunas veces transfieren archivos por medio del correo electrónico, el correo está diseñado principalmente para mensajes cortos de texto. Los protocolos TCP/IP incluyen un programa de aplicación para transferencia de archivos, el cual permite que lo usuarios envíen o reciban archivos arbitrariamente grandes de programas o de datos. Por ejemplo, al utilizar el programa de transferencia de archivos, se puede copiar de una máquina a otra una gran base de datos que contenga imágenes de satélite, un programa escrito en Pascal o C++, o un diccionario del idioma inglés. El sistema proporciona una manera de verificar que los usuarios cuenten con autorización o, incluso, de impedir el acceso. Como el correo, la transferencia de archivos a través de una red de redes TCP/IP es confiable debido a que las dos máquinas comprendidas se comunican de

manera directa, sin tener que confiar en máquinas intermedias para hacer copias del archivo a lo largo del camino.

- ***Acceso remoto***. El acceso remoto permite que un usuario que esté frente a una computadora se conecte a una máquina remota y establezca una sesión interactiva. El acceso remoto hace aparecer una ventana en la pantalla del usuario, la cual se conecta directamente con la máquina remota al enviar cada golpe de tecla desde el teclado del usuario a una máquina remota y muestra en la ventana del usuario cada carácter que la computadora remoto lo genere. Cuando termina la sesión de acceso remoto, la aplicación regresa al usuario a su sistema local.

Servicios De Internet A Nivel De Red

Un programador que crea programas de aplicación que utilizan protocolos TCP/IP tiene una visión totalmente diferente de una red de redes, con respecto a la visión que tiene un usuario que únicamente ejecuta aplicaciones como el correo electrónico. En el nivel de red, una red de redes proporciona dos grandes tipos de servicios que todos los programas de aplicación utilizan. Aunque no es importante en este momento entender los detalles de estos servicios, no se deben omitir del panorama general del TCP/IP:

- **Servicio sin conexión de entrega de paquetes**. La entrega sin conexión es una abstracción del servicio que la mayoría de las redes de conmutación de paquetes ofrece. Simplemente significa que una red de redes TCP/IP rutea mensajes pequeños de una máquina a otra, basándose en la información de dirección que contiene cada mensaje. Debido a que el servicio sin conexión rutea cada paquete por separado, no garantiza una entrega confiable y en orden. Como por lo general se introduce directamente en el hardware subyacente, el servicio sin conexión es muy eficiente.

- **Servicio de transporte de flujo confiable**. La mayor parte de las aplicaciones necesitan mucho más que sólo la entrega de paquetes, debido a que requieren que el software de comunicaciones se recupere de manera automática de los errores de transmisión, paquetes perdidos o fallas de conmutadores intermedios a lo largo del camino entre el transmisor y el receptor. El servicio de transporte confiable resuelve dichos problemas. Permite que una aplicación en una computadora establezca una "conexión" con una aplicación en otra computadora, para después enviar un gran volumen de datos a través de la conexión como si fuera perramente y directa del hardware.

Muchas redes proporcionan servicios básicos similares a los servicios TCP/IP, pero existen unas características principales que los distingue de los otros servicios:

- **Independencia de la tecnología de red**. Ya que el TCP/IP está basado en una tecnología convencional de conmutación de paquetes, es independiente de cualquier marca de hardware en particular. La Internet global incluye una variedad de tecnologías de red que van de redes diseñadas para operar dentro de un solo edificio a las diseñadas para abarcar grandes distancias. Los protocolos TCP/IP definen la unidad de transmisión de datos, llamada datagrama, y especifican cómo transmitir los datagramas en una red en particular.
- **Interconexión universal**. Una red de redes TCP/IP permite que se comunique cualquier par de computadoras conectadas a ella. Cada computadora tiene asignada una dirección reconocida de manera universal dentro de la red de redes. Cada datagrama lleva en su interior las direcciones de destino para tomar decisiones de ruteo.
- **Acuses de recibo punto-a-punto**. Los protocolos TCP/IP de una red de redes proporcionan acuses de recibo entre la fuente y el último destino en vez de proporcionarlos entre máquinas sucesivas a lo largo del camino, aún cuando las dos máquinas no estén conectadas a la misma red física.
- **Estándares de protocolo de aplicación**. Además de los servicios básicos de nivel de transporte (como las conexiones de flujo confiable), los protocolos TCP/IP incluyen estándares para muchas aplicaciones comunes, incluyendo correo electrónico, transferencia de archivos y acceso remoto. Por lo tanto, cuando se diseñan programas de aplicación que utilizan el TCP/IP, los programadores a menudo se encuentran con que el software ya existente proporciona los servicios de comunicación que necesitan.

Preguntas y Respuestas

1. ¿Qué significa TCP/IP?

En realidad son dos acrónimos distintos; TCP son las siglas de "Transmisión Control Protocol", mientras que IP significa Internetwork Protocol". Si bien son dos protocolos distintos, en la actualidad el concepto TCP/IP engloba toda una filosofía de operación, basada por supuesto en la conmutación de paquetes, pero no esta compuesta por solo dos protocolos, se trata de todo un conjunto "suite" de protocolos que están ligados y que constituyen la base del funcionamiento de Internet.

2. ¿Basicamente, cuál es la función del Protocolo IP?

Concretamente, IP es un estándar que subyace en todas las comunicaciones de la red. Incluye todas las especificaciones necesarias para hacer inteligible a cualquier máquina la información contenida en cada datagrama (paquete) transmitido. Entre otras, el tamaño normalizado de las cabeceras, remitente, códigos de control de integridad, etc.

3. ¿Basicamente, cuál es la función del Protocolo TCP?

TCP se encarga de "negociar" con el equipo remoto determinados parámetros que determinan algunos detalles del modo en que se realizará la transmisión (por ejemplo el tamaño de los paquetes).

4. ¿Cuál es la desventaja de un modelo monolítico?

El modelo, que considera la cadena como un todo monolítico, es poco práctico, porque el más pequeño cambio puede implicar alterar todos sus elementos.

5. ¿Qué es el modelo OSI?

Es un modelo de comunicaciones para redes presentado por la organización ISO (International Standards Organization). Su filosofía se basa en descomponer la funcionalidad de la cadena de

transmisión en diversos módulos llamados 'capas', cuya interfaz con los adyacentes esté estandarizada.

6. ¿Qué ventaja presenta?

Esta filosofía de diseño presenta una doble ventaja; el cambio de un módulo no afecta necesariamente a la totalidad de la cadena; y además, puede existir una cierta interoperabilidad entre diversos productos y fabricantes hardware/software, dado que los límites y las interfaces están perfectamente definidas.

7. ¿Que capas componen el modelo OSI?

1. Físico
2. Enlace
3. Red
4. Transporte
5. Sesión
6. Presentación
7. Aplicación

8. ¿Cuantas componen a la arquitectura TCP / IP?

La arquitectura TCP/IP viene definida por 4 niveles:

Nivel de subred [enlace y físico].

Nivel de interred [Red, IP].

Protocolo proveedor de servicio [Transporte, TCP o UDP].

Nivel de aplicación.

9. Definir aperturas activas y pasivas

Los puertos TCP pueden establecer dos tipos de conexiones. El modo de apertura pasiva permite que el protocolo de nivel superior (por ejemplo, un servidor) indique al TCP y al sistema operativo del computador que va a esperar la llegada de solicitudes de conexión procedentes del sistema remoto. Tras recibir esta solicitud, el sistema operativo asigna un número de puerto a este extremo.

La segunda forma de establecimiento de conexión es el modo de apertura activa. En esta situación, el protocolo de nivel superior designa específicamente otro socket (puerto) por el que establecer la conexión. Típicamente, se envía la apertura activa a un puerto con apertura pasiva para establecer un circuito virtual.

10. ¿Como se compone un segmento?

El segmento se divide en dos partes, la parte de cabecera y la parte de datos.

11. ¿A que hace referencia el sistema bridging?

En el sistema bridging, las direcciones no contienen ninguna información sobre donde está la máquina a la que va destinado el paquete. El principio de funcionamiento supone que los paquetes circulan por "toda" la red. Todas las máquinas recibirán todos los paquetes, y solo prestarán atención a los que correspondan a su dirección. Esta técnica de transmitir en la que todos los elementos de la red reciban la información se denomina multi-difusión ("Broadcast"). Las redes Ethernet y Token Ring pertenecen a esta categoría.

12. ¿En que se diferencia el routing?

El routing por su parte es mas elaborado, se supone que las direcciones contienen información sobre "donde" está la computadora de destino dentro de la red, esto hace posible la existencia de sistemas enrutadores ("Routers") que hacen seguir cada mensaje en la dirección adecuada. Es conveniente tener clara la distinción entre dirección y ruta; en este sistema (routing), la ruta está implícita en la dirección, pero su concreción está contenida en las denominadas tablas de rutas ("Routing tables").

13. ¿Que es la dirección IP?

Es la "dirección" dentro de la red, y en principio a cada máquina de la Red se le asigna una (los mensajes incluyen las direcciones IP de las máquinas origen y destino). esta direccion esta compuesta por 32 bits y es representada en números decimales mediante un conjunto de 4 cantidades separadas por puntos (una por octeto), con un aspecto tal como por ejemplo: 204.123.2.75.

14. ¿Que es el Sistema DNS?

Se utilizó para automatizar el proceso y hacerlo transparente para el usuario, es servicio de traducción de nombres a números (y a la inversa), por el procedimiento de incluir en algunas computadoras del sistema, unas tablas que permitieran saber que altavista.digital.com equivale a 204.123.2.75.

Las computadoras que contienen estas tablas se llaman Servidores de Nombre, abreviadamente NS "Name Server"

15. ¿Que son las direcciones IP dinámicas?

Las direcciones IP dinámicas son un método de economizar direcciones compartiéndolas entre diferentes usuarios que no estan conectados todo el tiempo. Es por eso que se les asigna una cualquiera cuando se conectan. Estas direcciones las asigna el servidor de la red a la que pertenece el usuario.

16. ¿Como lo hace?

Los servidores que deben proporcionar direcciones IP dinámicas a sus clientes utilizan el protocolo DHCP ("Dynamic Host Configuration Protocol"). Cuando un equipo desea conectarse a Internet necesita una dirección IP, de forma que recaba una al servidor DHCP y este le asigna una de las que tiene disponibles. Los datos enviados son: Dirección IP; máscara de subred ("Subnet mask"), y puerta de enlace predeterminada ("Default Gateway").

17. ¿Que es el enmascaramiento?

El enmascaramiento ("Masquerading") es una técnica que permite que varias computadoras interconectadas compartan una misma conexión a Internet. Por ejemplo un módem o (preferiblemente) una conexión RDSI o ADSL que está conectado físicamente a una de ellas. Su finalidad es conseguir que la dirección IP Internet asignada al equipo propietario de la conexión pueda ser compartida por otros para realizar también lacomunicaciones con la Red, aunque desde el punto de vista del exterior, Internet percibe un solo equipo conectado, el que realiza el enmascaramiento.

18. ¿Que Servicios de Internet a nivel de aplicación nos brinda la tecnologia TCP/IP?

Una red de redes TCP/IP aparece como un grupo de programas de aplicación que utilizan la red para llevar a cabo tareas útiles de comunicación. Los servicios de aplicación de Internet más populares y difundidos incluyen: Correo electronico, transferencia de archivos, acceso remoto, etc.

19. ¿Que Servicios de Internet a nivel de red nos brinda la utilización de la 'suite' TCP/IP?

Servicio sin conexión de entrega de paquetes

Servicio de transporte de flujo confiable

Independencia de la tecnología de red

Interconexión universal

Acuses de recibo punto-a-punto

Estándares de protocolo de aplicación

Bibliografía

Los principales referentes de donde se extrajo información son los siguientes:

- http://www.icann.org/
- http://www.zator.com/Internet/index.htm
- http://www.cisco.com
- http://www.hildrum.com/spanish/winipcfgspanish.htm
- http://www.monografias.com/trabajos6/redex/redex.shtml
- http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
- http://www.cienciasmisticas.com.ar/informatica/index.php
- Introduction to TCP/IP -- H. Gilbert
- Internet -- Torrealba Carmen
- Utilización de tecnología de comunicación abierta para el transporte de protocolos heredados -- Eduardo Sotelo Zárate
- Redes de computadores. Protocolos, normas e interfaces -- Uyless Black