Capítulo 3

Introducción a TCP/IP

En este tercer capítulo vamos a adentrarnos en el mundo del protocolo TCP/IP. Este protocolo es el más ampliamente utilizado en la actualidad y es la base del funcionamiento tanto de Internet como de las grandes redes WAN y de las redes locales. A lo largo de la historia de las redes informáticas han existido y existen muchos protocolos de comunicaciones distintos pero TCP/IP se ha situado como el estándar actual en las redes informáticas.

Es un protocolo que proporciona transmisión fiable de paquetes de datos a través de las redes de ordenadores. El nombre TCP/IP proviene de dos protocolos importantes de la familia, el Protocolo de Control de Transmisión (TCP) y el Protocolo Internet (IP). El total de protocolos incluidos en la pila TCP/IP superan los cien.

Un protocolo es un conjunto de normas y especificaciones que permiten que dispositivos de red de distintos fabricantes y con diferentes sistemas operativos puedan comunicarse. Cuando las redes informáticas comenzaron a expandirse surgió la problemática de las diferentes especificaciones e implementaciones de cada fabricante que impedían que dispositivos de distintos fabricantes pudieran convivir. Enseguida se vio la necesidad de crear un protocolo de trabajo común universal para todos los dispositivos que los independizara del hardware y el software del que disponían cada uno.

El ejemplo más claro de esto es Internet, la red más grande que existe y que abarca dispositivos de todo tipo así como redes muy diferentes que funcionan sobre medios también diferentes como cable, aire, satélite, etc. Así pues Internet no es dependiente de los sistemas que tiene conectados.

Tenemos que tener presente que cuando hablamos del protocolo TCP/IP estamos hablando de la pila de protocolos TCP/IP, ya que como hemos comentado antes son muchos los protocolos que la integran, cada uno con una función diferente según el tipo de comunicación que queramos realizar.

Los diferentes protocolos de la pila TCP/IP están distribuidos, según su función, entre las distintas capas del modelo TCP/IP. Como veremos en las siguientes lecciones, el protocolo TCP/IP trabaja en varias capas distintas del modelo TCP/IP.

El protocolo TCP/IP resulta una referencia útil a la hora de tratar con otros protocolos ya que incluye elementos que son representativos de otros protocolos.

Al finalizar el estudio de estas lecciones serás capaz de:

- ✓ Definir que es el protocolo TCP/IP
- ✓ Explicar la historia del protocolo TCP/IP
- ✓ Explicar cuáles son las capas del protocolo TCP/P y su funcionamiento

Lección 1

Historia del protocolo TCP/IP

A principios de los años 60 varios investigadores intentaban encontrar una forma de compartir recursos informáticos de una forma más eficiente. En 1961 Leonard Klienrock introdujo el concepto de conmutación de paquetes. La idea se basaba en que la comunicación entre dos sistemas se dividiera en paquetes para una mejor comunicación.

En 1969 la Agencia de Proyectos de Investigación Avanzada (Defense Advanced Research Projects Agency o DARPA) del ejército de los EEUU desarrolla la ARPAnet. La finalidad de la creación de esta red es que resistiera un ataque de la URSS. De este modo no importaba si algún ordenador se destruía, la red seguiría funcionando. Sin embargo esta red no era tan buena como se creía pues estaba sujeta a periódicas caídas del sistema. Entonces se empezó a crear un conjunto de protocolos de uso fácil para ella.

TCP/IP fue desarrollado y presentado por el Departamento de Defensa de EEUU en 1972 y fue aplicado en ARPANET (Advanced Research Projects Agency Network) que era la red de área extensa del Departamento de Defensa como medio de comunicación para los diferentes organismos de EEUU. La transición hacia TCP/IP en ARPANET se concretó en 1983.

Con el funcionamiento de esta red se dieron cuenta que era posible que esta fuera utilizada como una oficina postal para los empleados, utilización que se hizo muy popular para enviar mensajes personales.

Poco a poco fue creciendo debido a su estructura descentralizada y que cualquier ordenador con el protocolo de comunicación podía conectarse a ella.

El protocolo original de comunicación que era utilizado por los ordenadores de la red fue el NCP (Network Control Protocol) pero fue después reemplazado por el protocolo TCP/IP mucho más avanzado.

El TCP/IP adquirió muchas ventajas en comparación con otros protocolos, alguno de ellas es que consume pocos recursos de red, gracias a esto TCP/IP empezó a tener una gran popularidad. En 1983 TCP/IP se integró en los sistemas Unix de Berkeley y su integración comercial en Unix llegó pronto.

Poco a poco ARPAnet dejó de tener un uso exclusivamente militar y se permitió que centros de investigación, universidades y empresas se conectaran a la red. Por entonces ya comenzaba a hablarse de Internet y en 1990 ARPAnet dejó de existir oficialmente.

En los siguientes años y hasta ahora las redes troncales y los nodos de interconexión han aumentado exponencialmente. Internet se expande de forma imparable, eso sí, con un punto común: el protocolo TCP/IP. El enorme crecimiento de Internet ha provocado que el protocolo TCP/IP se haya convertido en el estándar de Internet, de las redes locales y de todas las aplicaciones que necesitan del uso de una red.

Precisamente es en las redes locales donde el TCP/IP se hace cada vez mas fuerte siendo cada día más importante. La importancia actual del protocolo TCP/IP se debe principalmente a una serie de **características** muy necesarias hoy en día:

- Los estándares del protocolo TCP/IP son **abiertos y soportados por todo tipo de sistemas**, lo que los hace compatibles con todo tipo de hardware y software de los distintos fabricantes.
- TCP/IP funciona prácticamente **sobre cualquier medio**, ya sea una red Ethernet, una conexión ADSL o fibra óptica.
- TCP/IP emplea un tipo de direccionamiento que asigna un **identificador único** en toda la red, que es la dirección IP, aunque sea en una red tan grande como Internet.

Todos los estándares existentes para los protocolos TCP/IP están publicados como RFC (Request for Comments) que detallan todo lo relacionado con los diferentes aspectos en las que se basa Internet como los protocolos, comunicaciones, etc.

Lección 2

Capa de acceso a la red

La capa de acceso a la red determina la manera en que los dispositivos de red envían y reciben datos a través del medio físico proporcionado por la capa anterior y maneja todos los aspectos que un paquete IP requiere para efectuar un enlace físico real con los medios de la red. Esta capa incluye los detalles de la tecnología LAN y WAN y todos los detalles de las capas físicas y de enlace de datos del modelo OSI.

Los controladores para las aplicaciones de software, las tarjetas de red y otros dispositivos trabajan en la capa de acceso de red. La capa de acceso de red define los procedimientos para interactuar con el hardware de red y para tener acceso al medio. Existen muchos protocolos que operan en esta capa aunque la mayoría de los protocolos reconocibles operan en las capas de transporte y de Internet o red del modelo TCP/IP.

En esta capa es donde se establece como se produce la encapsulación de un datagrama IP en una trama que pueda ser transmitida por la red, siendo en la gran mayoría de redes locales una trama Ethernet.

Otra función importante de esta capa es asociar las direcciones lógicas IP a las direcciones físicas (MAC) de las tarjetas de red (NIC). La dirección IP es elegida por el usuario mientras que la dirección MAC no puede cambiarse ya que viene "grabada" en la tarjeta de red y sirve para identificarla de manera inequívoca en la red Ethernet.

Dentro de esta capa opera el protocolo ARP (Address Resolution Protocol) que se encarga de asociar direcciones IP con direcciones físicas Ethernet, aunque este protocolo también actúa en la capa de red.

Lección 3

Capa de red

La capa de red o Internet de la pila TCP/IP corresponde a la capa de red del modelo OSI. La capa de red es responsable de llevar paquetes a través de la red utilizando direccionamiento por software.

La capa de red o Internet se encuentra justo encima de la capa de acceso a red. Son varios los protocolos TCP/IP que actúan en la capa de red, el más importante de todos ellos es el protocolo IP que es el encargado de facilitar la ruta al destino, no le interesa el contenido de los paquetes solo que lleguen a su destino.

Existen varias versiones del protocolo IP, la versión IPv4 es la más utilizada actualmente aunque el enorme crecimiento de las redes cada vez hace más difícil su continuidad ya que el número que IPv4 puede direccional comienza a quedarse corto. Para solucionar este problema se desarrolló hace unos años la versión IPv6, con una capacidad de direccionamiento mucho mayor pero incompatible con la versión IPv4.

El protocolo IP se ha diseñado para redes de paquetes conmutados no orientados a conexión, esto quiere decir que el protocolo no se preocupa de establecer una conexión entre los extremos para enviar el paquete de datos. De la misma manera tampoco se preocupa de comprobar si ha habido errores en el envío de los datos y deja que se encarguen de ello las capas superiores. Así pues un paquete IP dispone de la información suficiente para enviarse de un extremo a otro sin crear conexiones entre los diferentes dispositivos.

Igualmente existen diversos protocolos que actúan en la capa de red como el protocolo ARP que determina cual es la dirección de la capa de enlace de datos (MAC) que corresponde a una determinada dirección IP. También hay varios protocolos que se utilizan en la resolución de problemas en esta capa como el protocolo ICMP, que proporciona capacidades de control y mensajería y sirve entre otras cosas para comprobar la comunicación IP entre dos sistemas a través del comando Ping.

La unidad de datos de la capa de red es el paquete. Una vez que la capa de acceso a red ha encapsulado los datos en una trama los pasa a la capa de red la cual añade su propia información y los encapsula en un paquete IP que pasa a la capa de transporte. Los campos que conforman la cabecera de un paquete IP son los siguientes:

Formato de la Cabecera IP (Versión 4)

<table>
<tr><td>0-3</td><td>4-7</td><td>8-15</td><td>16-18</td><td>19-31</td></tr>
<tr><td>Versión</td><td>Tamaño Cabecera</td><td>Tipo de Servicio</td><td colspan="2">Longitud Total</td></tr>
<tr><td colspan="3">Identificador</td><td>Indicadores</td><td>Posición de Fragmento</td></tr>
<tr><td>Checksun Cabecera</td><td colspan="4"></td></tr>
<tr><td colspan="5">Dirección IP de Origen</td></tr>
<tr><td colspan="5">Dirección IP de Destino</td></tr>
<tr><td colspan="4">Opciones</td><td>Relleno</td></tr>
</table>

Formato de un paquete IP

La cabecera es la información que añade la capa de red, la cual es anexada a la trama proporcionada por la capa de acceso a red y todo junto se encapsula formando el paquete IP.

El paquete IP dispone de campos que son iguales en las otras capas como el Checksum que comprueba el correcto estado del paquete, el tamaño de la cabecera o la longitud total del paquete.

En la cabecera del paquete IP los campos más importantes son los que llevan la información de la dirección IP de origen y la dirección IP de destino. Estas direcciones son las que va a usar la capa de red para saber a dónde tiene que enviar el paquete, quien envía el paquete y determinar cuál es la mejor ruta al destino.

La dirección IP de origen se utilizara para devolver un mensaje de error al remitente en el caso de que no se pueda alcanzar el destino por un lado y por otro se convertirá en la dirección IP de destino cuando el destinatario del paquete le envíe de vuelta una respuesta.

La dirección IP de destino se utiliza para determinar la ruta a seguir para alcanzar el destino así como para realizar la entrega del paquete al destinatario. Si la dirección IP de destino pertenece a una red local conectada directamente a una interfaz de red del host se realiza el envío del paquete a través de esa interfaz. Previamente se utiliza el protocolo ARP para determinar la dirección MAC del destino.

Si la dirección IP de destino no pertenece a una red directamente conectada el host debe hacer uso de la tabla de enrutamiento para verificar si existe una entrada que indique por donde debe enviarse para alcanzar dicha red. Todos los host disponen de una tabla de enrutamiento donde aparecen todas las redes que se conocen y las interfaces por las cuales son alcanzables. Si se encuentra alguna entrada para el destino especificado se envía el paquete a la interfaz indicada en dicha entrada. Una vez el paquete ha sido enviado el host se despreocupa de si llega o no a su destino final y deberán ser los siguientes host en la cadena los que se encarguen uno o uno de hacer llegar el paquete a su destino definitivo.

Si no se encuentra una entrada en la tabla de enrutamiento, si existe una ruta por defecto se envía el paquete a la interfaz indicada en la misma (default gateway). Si tampoco existe una ruta por defecto, como no hay información suficiente para enviar el paquete se devolverá al host origen un mensaje de destino inaccesible.

El paso de una red a otra a través del default gateway o puerta de enlace se denomina "salto". Un paquete o datagrama IP puede realizar varios saltos a través de muchas redes hasta llegar a su destino. El camino que sigue un paquete IP hasta llegar al destino puede ser diferente de otro enviado por el mismo host, el camino vendrá determinado, como hemos comentado antes, por el proceso de enrutamiento, según los datos disponibles en la tabla de enrutamiento de cada host. De hecho a las puertas de enlace se les llama enrutadores (Routers).

También la capa de red trabaja el protocolo ICMP (Internet control Message Protocol) que es junto con el protocolo IP uno de los importantes en esta capa ya que es el encargado de diversas funciones como el control de flujo y pruebas de conectividad para resolución de problemas. Con más detalle son las siguientes:

- **Control de flujo**: Si los paquetes IP que envía el emisor llegan a demasiada velocidad a su destino, el host receptor envía al host origen un mensaje ICMP pidiéndole parar la transmisión de datos de forma temporal.
- **Detección de destinos inalcanzables**: Si la dirección IP de destino no pertenece a ninguna ruta conocida o alcanzable el host emisor recibirá un mensaje ICMP indicándole que el destino es inalcanzable.
- **Redireccionamiento de rutas**: En el caso de que haya más de una puerta de enlace disponible para alcanzar otras redes, un router puede enviar al host origen un mensaje ICMP para hacerle saber que hay una opción mejor para enviar los datos.
- **Pruebas de conectividad**: Es la parte mas conocida y utilizada por los administradores de redes locales ya para ello se utiliza el comando ping (packet Internet Groper). Para realizar la prueba de conectividad un host ejecuta el comando ping hacía una dirección IP de destino, es decir, un mensaje ICMP "con eco", entonces desde el destino o desde el último host alcanzable se devuelve el mensaje de forma inmediata al origen indicando si se ha alcanzado el destino o la razón por la que no ha sido alcanzado.

El comando ping suele presentar diferencias en cuanto a sus opciones según el sistema o equipo desde el que se ejecute. En el caso del sistema operativo Windows el comando envía por defecto cuatro paquetes ICMP de 32 bytes que en el caso de alcanzar su destino, el host receptor los recibe y responde a cada uno de ellos.

Lección 4

Capa de host a host

La capa de host a host o capa de transporte permite a un dispositivo segmentar los datos de una o varias aplicaciones para incluirlos en el mismo flujo de datos de la capa 4 y permite que el dispositivo de destino junte de nuevo los segmentos de aplicación de la capa superior. El flujo de datos de la capa 4 es una conexión lógica entre los dos extremos de una red y proporciona servicios de transporte desde un host origen a un host destino. Este servicio se conoce a veces como servicio de extremo a extremo.

La capa de transporte ofrece dos protocolos principales:

1. **TCP**. Es un protocolo confiable orientado a la conexión que proporciona el control de flujo mediante ventanas deslizantes y que proporciona fiabilidad ofreciendo números de secuencia y acuses de recibo. TCP vuelve a enviar cualquier cosa que no se reconozca y suministra un circuito virtual entre las aplicaciones de los usuarios finales. La ventaja de TCP es que ofrece la entrega garantizada de segmentos.
2. **UDP**. Es un protocolo no orientado a conexión y no fiable que es responsable de transmitir mensajes pero no proporciona comprobación de errores ni si la entrega se realiza correctamente. La venta de UDP es la velocidad. Como UDP no ofrece acuses de recibo se envía menos tráfico de control a través de la red acelerando la transferencia.

32 BITS

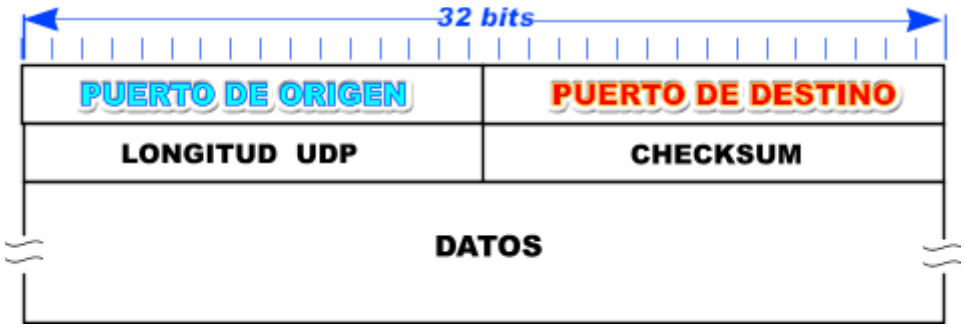
PUERTO FUENTE (16)								PUERTO DE DESTINO (16)
NÚMERO DE SECUENCIA (32)								
NÚMERO DE ACEPTACIÓN (32)								
DESPLAZA-MIENTO DE DATOS (4)	RESERVADO (6)	URG	ACK	PSH	RST	SVN	FIN	VENTANA (16)
CHECKSUM (16)								PUNTERO DE URGENTE (16)
OPCIONES (VARIABLE)								RELLENO
DATOS (VARIABLE)								

Formato de un segmento TCP

Como podemos ver en la imagen anterior un segmento TCP está compuesto de diversos campos que contienen la información necesaria que la capa de transporte debe proporcionar. A los datos en si mismos tiene que añadir una serie de campos de los cuales los principales son:

1. **Puerto de origen**: El número de puerto origen de este segmento.
2. **Puerto de destino**: El número de puerto de destino de este segmento.
3. **Número de secuencia**: El número utilizado para asegurar que los datos llegan en el orden correcto.
4. **Número de acuse de recibo**: El siguiente segmento esperado.
5. **Checksum o suma de comprobación**: Una suma que certifica que el segmento en el destino tiene el mismo tamaño y los mismos datos que en el origen.

Cuando se utiliza UDP la fiabilidad, si se precisa, deben proporcionarla las aplicaciones. UDP no utiliza ventanas ni acuses de recibo. Está pensado para aplicaciones que no necesitan que sus datos lleguen en un orden correcto. Al no necesitar tantos campos un segmento UDP es bastante más pequeño que el TCP.



Formato de un segmento UDP

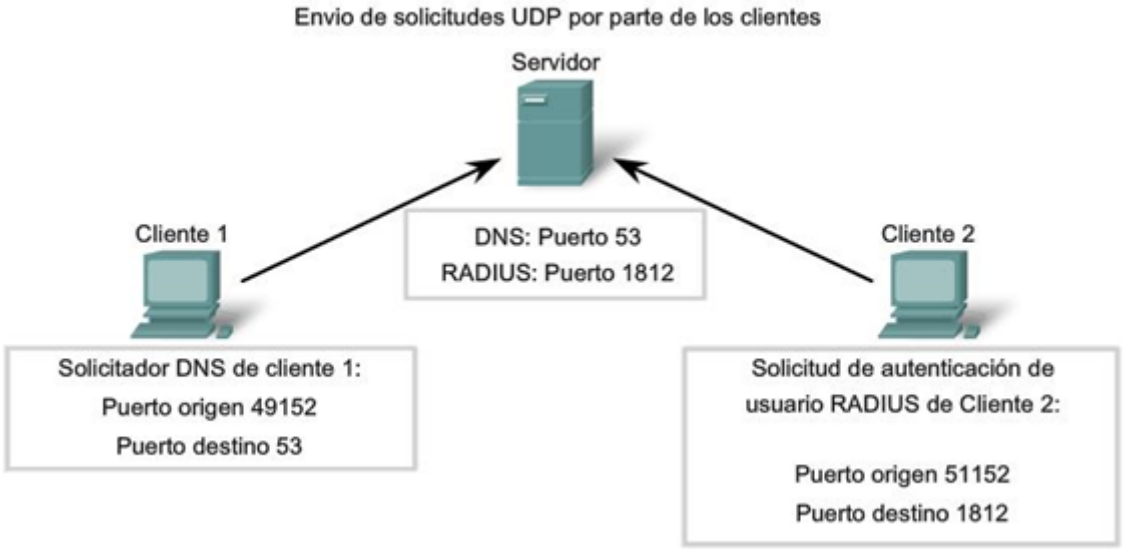
Unos ejemplos de protocolos que utilizan UDP son TFTP, SNMP, NFS y DNS. Todos estos protocolos así como el SMTP en el que se basa el correo electrónico no se preocupan de si el destino está disponible o no, los datos se envían de todos modos y en el caso de detectar un fallo en el envío se reintentará de nuevo posteriormente.

Tanto TCP como UDP utilizan número de puerto para pasar información a las capas superiores. Los números de puerto se utilizan para permitir el envío a diferentes aplicaciones al mismo host en el mismo momento, de otra manera las comunicaciones con las aplicaciones deberían realizarse de una en una.

Los programadores de las aplicaciones de software han acordado utilizar los números de puerto bien conocidos que están definidos en la norma RFC 1700. Por ejemplo, una comunicación con destino a la aplicación Telnet para la conexión remota a un dispositivo utilizará el puerto estándar número 23.

Las comunicaciones que no implican una aplicación con un número de puerto bien conocido se asignan en su lugar a números de puerto que se eligen aleatoriamente dentro de un rango específico. Estos números de puerto se utilizan como direcciones de origen y destino en el segmento TCP.

En la siguiente imagen podemos ver como dos clientes realizan sendas solicitudes a un servidor a diferentes servicios cada uno, a través del puerto correspondiente a cada servicio.



Algunos puertos TCP y UDP están reservados aunque es posible que las aplicaciones no los admitan. Los números de puerto tienen los siguientes rangos asignados:

- ✓ Los números inferiores a 255 son para aplicaciones públicas
- ✓ Los números entre 255 y 1023 están asignados a las compañías con aplicaciones comerciales
- ✓ Los números superiores a 1023 no están regulados

A la hora de enviar datos a un sistema de destino, el puerto de destino será el de la aplicación que recibe los datos mientras que el puerto de origen lo asigna aleatoriamente el host origen.

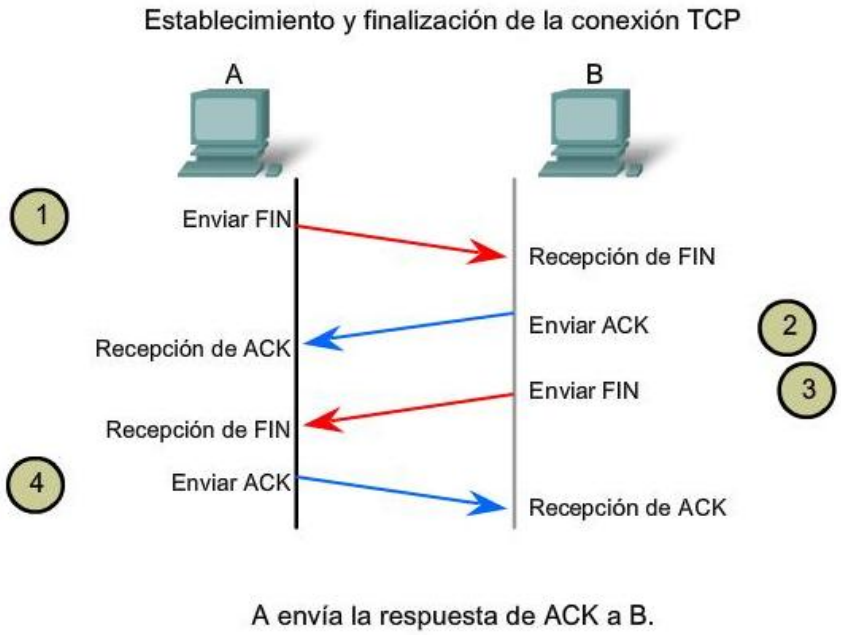
Conexión TCP de tres vías

Como hemos comentado TCP es un protocolo orientado a conexión lo que quiere decir que antes de comenzar a enviar datos debe establecer una conexión con el host de destino. Para ello los dos sistemas finales deben sincronizar entre si el número de secuencia inicial del segmento TCP de la otra. Estos números se utilizan para seguir el orden de los paquetes y cerciorarse de que no se pierde ninguno en la transmisión. El intercambio de números de secuencia iniciales durante la conexión asegura que los datos perdidos se puedan recuperar.

La sincronización comienza intercambiando los segmentos con un bit de control llamado SYN que significa sincronizar. Una conexión satisfactoria necesita un mecanismo apropiado para seleccionar la secuencia inicial y un intercambio de respuestas llamadas desafíos. Cada lado debe enviar su número de secuencia y esperar un acuse de recibo (ACK) de confirmación en un orden específico:

1. De Host A a Host B - Mi número de secuencia es X
2. De Host B a Host A - Tu número de secuencia es X y espero el X+1
   - Mi número de secuencia es Y
3. De Host A a Host B - Tu número de secuencia es Y y espero el Y+1

Estos tres pasos se conocen como conexión de tres vías por desafío / conexión abierta. En este punto cualquier lado puede empezar a enviar datos y cualquier lado puede romper la conexión ya que es una conexión de igual a igual.



Conexión TCP de tres vías por desafío / conexión abierta

Acuse de recibo y windowing

Para administrar el flujo de datos entre dispositivos de red, TCP usa un mecanismo de control del flujo de datos. La capa TCP del sistema receptor de su tamaño de ventana al host origen. El tamaño de ventana indica el número de bytes, comenzando por el número de acuse de recibo que la capa TCP del host receptor está actualmente preparada para recibir.

El tamaño de la ventana se refiere al número de bytes que se pueden enviar antes de recibir un acuse de recibo. Una vez que se han enviado el número de bytes que indica la ventana, antes de enviar de nuevo el host origen de esperar la recepción de un acuse de recibo.

El tamaño de la ventana indica por tanto cuando bytes puede aceptar el host de destino antes de enviar un acuse de recibo, una ventana de 1 indica que solo se debe enviar 1 byte de datos antes de recibir el acuse de recibo.

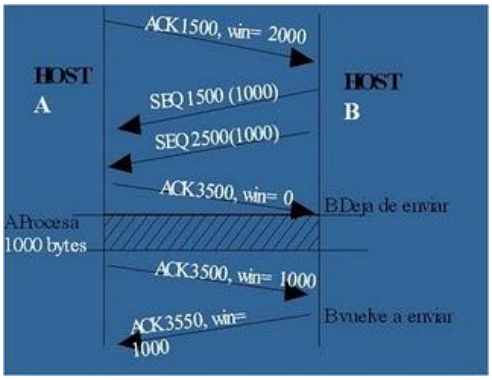
El propósito del windowing es mejorar el control y la fiabilidad del flujo de datos por lo que un tamaño de ventana de 1 hará que el aprovechamiento del ancho de banda sea ineficiente.

Para solucionar esto existe la Ventana Deslizante TCP. La ventana deslizante permite modificar el tamaño de la ventana de tal manera que se aumenta el número de bytes de datos que el origen puede enviar antes de recibir un acuse de recibo. Esta ventana deslizante se negocia dinámicamente durante la sesión TCP e implica un aprovechamiento del ancho de banda más eficiente ya que una ventana mayor, como hemos comentado permite enviar más datos sin tener que esperar la confirmación

Como vemos en esta imagen de abajo, el host A envía un acuse de recibo (ACK 1500) y el tamaño de la ventana (win=2000) con lo que le indica al host B que ya puede enviar más datos y cuantos puede enviar.

A continuación el host B envía dos secuencias de datos, según lo indicado en la ventana (1000+1000) y espera el acuse de recibo del host A.

En la respuesta del host A, la ventana es 0 lo que indica al host B que deje de enviar datos, ya que necesita tiempo para procesar los datos que ya tiene. Cuando ha terminado envía otro acuse de recibo con un nuevo valor de ventana más reducido (lo que host A puede procesar sin problemas) para que el host B envíe de nuevo.



Funcionamiento de Ventana TCP

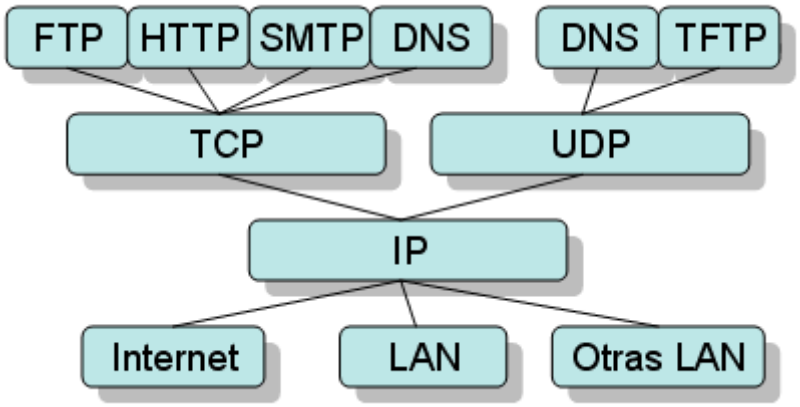
Lección 5

Capa de aplicación

La capa de aplicación de TCP/IP combina las funciones que realizan las capas de sesión, presentación y aplicación del modelo OSI. TCP/IP tiene protocolos que soportan la transferencia de archivos, correo electrónico y conexión remota.

En la capa de aplicación es donde trabajan los usuarios introduciendo datos en las aplicaciones. Al abarcar la capa de aplicación TCP/IP las funciones de las capas de sesión, presentación y aplicación, las aplicaciones son las encargadas de gestionar los datos y convertirlos al formato adecuado para una vez listos pasárselos a la capa de transporte para su envío al host de destino.

En este proceso parte de la información que se le ha de pasar a la capa de transporte es el número de puerto, ya sea TCP o UDP, por el que tiene que enviar los datos al destino. Cada aplicación trabaja con un puerto concreto que en el caso de los servicios y aplicaciones públicas como, el DNS, el FTP o el HTTP utilizan los números de puertos bien conocidos que van desde el 1 al 1023 mientras que las aplicaciones privadas utilizan puertos aleatorios por encima de ese número.



Servicios de capa de aplicación que usan puertos para la capa de transporte

En la capa de aplicación trabajan, aparte de las propias aplicaciones, todos aquellos servicios de red que requieren de la intervención de un administrador, aunque a veces por el tipo de función que realizan pudiera parecer que trabajan en capas inferiores como la capa 3. Un ejemplo de estos servicios sería, el DNS que asocia nombres de host con direcciones IP y el DHCP que realiza la asignación automática de direcciones IP a los dispositivos de red.

Como la capa de aplicación es la más alta en el modelo TCP/IP no ofrece servicios a ninguna otra capa y sin embargo depende por completo de las capas inferiores, por lo que cualquier error en cualquiera del resto de capas afectara a la capa de aplicación.

Así pues cuando surge un problema en esta capa para realizar la resolución de problemas hay que comprobar todas las demás ya que normalmente los fallos se suelen encontrar en las capas inferiores, sin descartar un posible problema de configuración en las propias aplicaciones.

En la siguiente imagen podemos observar, por ejemplo, como un correo electrónico generado en una aplicación de correo debe desplazarse por todas las capas para ser enviado al exterior. Si el proceso falla en alguna de las capas inferiores el correo no llegará a salir del ordenador origen.