Chapter 1

Modelos de red

Las redes permiter que los hosts conectados -computadoras- compartan recursos y accedan recursos. El sharing host -un servidor- corre un software espacial que permite al accesing host -un cliente- obtener el recurso deseado. Ese recurso puede ser varias cosas, desde una página Web en el internet hasta archivos en los servidores de tu oficina. Inclusive puede ser una impresora o una cámara.

Los profesionales de redes usan modelos para conceptualizar las muchas partes de una red, apoyándose principalmente del modelo Open Systems Interconnection (OSI) de siete capas.

El modelo OSI da dos herramientas que son fundamentales. Primero, el modelo OSI da una poderosa herramienta mental para diagnosticar problemas. Entender el modelo OSI permite identificar en qué capa ocurre un error y permite acercanos a una solución sin muchas vueltas. Segundo, el modelo OSI da un lenguaje común para que la genete que se dedica a las redes pueda hablar sobre funciones específicas de la red.

1.1 El modelo OSI en una red sencilla

Cada capa en el modelo OSI de siete capas define una función importante de las redes de computadoras, y los protocolos que operan en esa capa dan soluciones a esa función. Los **protocolos** son conjuntos de reglas, regulaciones, estándares y procedimientos bien definidos que permiten que los

desarrolladores de hardware y software hagan dispositivos y aplicaciones que funciones correctamente en una capa particular. El modelo OSI propicia el diseño modular en las redes, lo que significa que cada capa tiene que hacer la menor cantidad posible de operaciones en las demás capas. Las siete capas del modelo OSI son:

- **Capa 7** Aplicación
- **Capa 6** Presentación
- **Capa 5** Sesión
- **Capa 4** Transporte
- **Capa 3** Red
- **Capa 2** Enlace de datos
- **Capa 1** Fisica

Las capas del modelo OSI no son leyes de la física, cualquiera puede diseñar una red de otra manera. Aunque muchos protocolos encajan exactamente en una capa, no todos lo hacen.

La mejor manera de entender las capas del modelo OSI es verlas en acción. Vamos a verlas en acción con una compañía ficticia llamada MHTechEd Inc.

1.1.1 ¡Bienvenido a MHTechED!

MHTechED tiene una pequeña red de PCs corriendo Windows, una situación típica de muchos negocios de hoy en día. Windows viene con todo el software de redes necesarios para conectarse a una red. Todas las computadoras de MHTechED están conectadas por un cable especial de red.
Como en la mayoría de oficinas, todos en MHTechED tienen su propia PC. Por el tipo de trabajo que hacen, Shannon y Scott (los administradores) tienen que mandarse datos entre sus computadoras. En este momento, Shannon acava de completar un handbook en Word para los empleados y quiere que Scott lo cheque para ver que sea preciso. Veamos en detalle cada paso del proceso que permite que Scott tenga un acceso directo a la computadora

de Shannon, para que copie el documento de Word del sistema de Shannon al suyo. Mucho antes de que Shannon siquiera salvara el documento de Word en su sistema alguien que sabía lo que estaba haciendo configuró todos los sistemas de MHTechED para que sean parte de una red común. Toda esta configuración resultó en múltiples capas de hardware y software que pueden trabajar juntas detrás de escenas para que el documento de Word del sistema de Shannon llegue al sistema de Scott. Examinemos las distintas partes de la red.

1.2 Hardware de la red y capas 1-2

Claramente la red necesita de un canal físico a través del cual se puedan mover bits de datos entre los sistemas. La mayoría de redes usan un cable llamado unshielded twisted pair (UTP), que usualmente contiene cuatro pares de cables que pueden transmitir y recibir datos.
Otra pieza clave que utiliza la red es un dispositivo en forma de caja que maneja el flujo de los datos desde cada computadora hacia cualquier otra. Esta caja suele estar encerrada en un closet o un cuarto de equipo. La tecnología de la "central box" ha cambiado con el tiempo. Cada sistema tiene un cable que llega a la caja central.
La capa 1 del modelo OSI define el método para mover datos entre computadoras, así que los cables y la "central box" son parte de la *capa física* (capa 1). Cualquier cosa que mueve datos de un sistema a otro, como cables de cobre, fibra óptica u ondas de radio es parte de la capa física del modelo OSI. La capa 1 no se preocupa sobre qué datos pasan por ella; solo mueve datos de un sistema a otro.
La verdadera magia de las redes empieza con la *network interface card* (NIC), que sirve como la interfaz entre la PC y la red. Las hay de distintas formas y tamaños. En los sistemas más viejos, la NIC era en verdad una tarjeta que se conectaba a un slot de expansión en la tarjeta madre. Los cables y las cajas centrales definen la capa física de la red, y las NIC dan una interfaz para la PC. Podríamos estar tentados a categorizar las NIC como parte de la capa física. La NIC es claramente necesaria para que ocurra la conexión física. Muchos autores las ponen en la capa 2, así que hay algo interesante pasando con ellas.

1.2.1 La NIC

Para entender las redes, necesitamos entender cómo funcionan las NIC. La red debe proveer un mecanismo que le da a cada sistema un identificador único -como un número telefónico- para que los datos puedan llega al sistema correcto. Ese es uno de los trabajos más importantes de la NIC. Adentro de cada NIC, quemado dentro de algún chip ROM (Read Only Memory), hay un firmware especial que contiene un identificador único de 48-bits (6 bytes) que es llamado la dirección Media Access Control (MAC) de la NIC.
No hay dos NICs con la misma dirección MAC, nunca. Cualquier compañía que hace NICs debe contactar al Institute of Electrical and Electronic Engineers (IEEE) y pedir un bloque de direcciones MAC, que la compañía luego quema en los ROMs de sus NICs. Muchos creadores de NICs también imprimen la dirección MAC en la superficie de sus NICs. Notemos que las NICs muestran la dirección MAC en notación hexadecimal. Cada dígito de un número hexadecimal puede almacenar hasta 16 números, es decir, usa 4 bits de espacio y, como la dirección MAC es un número de 48-bits, entonces utiliza 12 dígitos hexadecimales. Las direcciones MAC son del estilo "9c:fc:e8:f3:8a:27". Los primeros seis dígitos, en este ejemplo "9c:fc:e8" representan el número del manufactor del NIC. Una vez que el IEEE asigna esos seis dígitos a un manufactor -referidos como el Organizationally Unique Identifier (OUI)- ningún otro manufactor los puede usar. Los últimos seis dígitos son el número de serie de esa NIC; a esta parte de la MAC le llamamos el Device ID.
Si tenemos un sistema Windows, podemos usar el comando **ipconfig /all** desde la terminal para mostrar la dirección MAC. Nota que ipconfig le llama dirección física a la dirección MAC, lo cual es una distinción importante. Para mac (o linux) podemos usar el comando **ifconfig** y para linux podemos usar este mismo (si tenemos netutils instalado) o **ip a**.

1.2.2 MAC-48 y EUI-48

El Institue of Electrial and Electronic Engineers (IEEE) forma las direcciones MAC de un numbering name space originalmente llamado MAC-48, que simplemente significa que la mac es de 48 bits, con los primeros 24 bits definiendo el Organizationally Unique Identifier (OUI), como se describió. El término actual para este numbering name space es EUI-48. EUI significa Extended Unique Identifier. La mayoría de personas les llaman simplemente

deirecciones MAC. Entonces, cada NIC en el mundo tiene una única dirección MAC, pero ¿cómo se utiliza? Aquí es donde comienza la diversión. Recordemos que los datos de computadoras son binarios, lo que significa que están hechos de líneas de ceros y unos. Los NICs mandan y reciben estos datos binarios como pulsos de electricidad, luz u ondas de radio. Consideremos los NICs que usan electricidad para mandar y recibir los datos. El proceso exacto mediante el cual un NIC utiliza electricidad para mandar y recibir datos es excesivamente complicado. En su lugar, pensemos una carga en un cable como un 1 y la ausencia de una carga como un 0. Una vez que entendemos cómo se mueven los datos a lo largo del cable, la siguiente pregunta es, ¿cómo la red manda los datos correctos al sistema correcto? Todas las redes mandan los datos rompiendo lo que sea que se esté moviendo a través de la capa física en cachos discretos llamados *frames*. Un *frame* es básicamente un contenedor para un pedazo de datos que se mueven por una red. Un frame *encapsula* la información y los datos para que tenga una transmisión más sencilla. La NIC crea y manda, así como recibe y lee estos frames.
Aquí es cuando las direcciones MAC se vuelven importantes. A continuación vemos una representación de un frame genérico, una versión simplificada de la tecnología de red cableada llamada ethernet. Aunque un frame es una

Figure 1.1: Frame genérico

string de ceros y unos, frecuentemente dibujamos a los frames como una serie de rectángulos, cada rectánuglo representando una parte del string de ceros y unos.
Notemos que el frame comienza con la dirección MAC de la NIC a la cual se le enviaron los datos, seguido de la dirección MAC del emisor. Despuès viene un campo *Type field*, que indica lo que está encapsulado en el frame. Después biene el campo de *Data* que contiene los datos que están siendo encapsulados, seguido de un cacho especial de chequeo de información llamado el *frame check sequence* (FCS). EL FCS usa un tipo de matemática binaria llamada *cyclic redundancy check* (CRC) que el NIC receptor usa para verificar que los datos llegaron intactos.
Podemos pensar un frame como teniendo tres secciones. El header, que contiene la dirección MAC del receptor, la dirección MAC del emisor y el campo

data type, en ese orden; el payload, que es lo que está siendo encapsulado por el frame y el triales, que es el frame check sequence (FCS).
Así que, ¿qué esta dentro de la parte data en el frame? El NIC ni sabe ni le importa. Los datos podrían ser parte de un archivo, un cacho de un sitio web o un trabajo de impresión. A los NICs no les importa el contenido. El NIC simplemente toma los datos que le pasan mediante su device driver y lo manda al sistema correcto. Software especial se encarga de qué datos en envían y qué pasa con los datos cuando llegan.
Como una caja, un frame sólo puede guardar una cierta cantidad de datos. Distintos tipos de redes usan distintos tamaños de frames, pero los frames utilizados en redes Ethernet guarda, a lo más, 1500 bytes de información. Esto genera una nueva pregunta, ¿qué pasa si queremos enviar más datos que lo que permite el tamaño del frame? Bueno, el software del sistema emisor debe romper los datos en cachos del tamaño de un frame, que luego pasa al NIC para su emisión. Conforme el receptor empieza a aceptar información, el software del receptor recombina los cachos de datos conforme llegan de la red.

1.2.3 A la caja central

Cuando un sistema manda un frame hacia la red, el frame llega a la caja central. Lo que pasa después depende de la tecnología de la caja central.
En el principio de las redes, la caja central era llamada un *hub*. Un hub era un dispositivo tonto, esencialemente un repetidor. Cuando recibía un frame, el hub hacía una copia exacta de ese frame y mandaba una copia del frame original a través de todos los puertos conectados salvo el puerto en el que se originó el mensaje.
La parte interesante del proceso era cuando la copia del frame llegaba a todos los sistemas. Sólo la NIC a la cual iba dirigido el mensaje procesaba ese frame, las otras NICs simplemente lo tiraban cuando veían que no estaba dirigido a su dirección MAC. Esto es importante de apreciar: con un hub, cada frame mandado por la red era recibido por cada NIC, pero sólo la NIC con la dirección MAC correspondiente procesaba ese frame.
Las redes posteriores reemplazaron los hubs con un dispositivo más inteligente llamado switch. Los switches, como veremos más adelante, filtran el tráfico por dirección MAC. En lugar de mandar todos los frames a todas las NICs conectadas, un switch manda el frame sólo a la NIC con la MAC correspondienteprocesaba ese frame, las otras NICs simplemente lo tiraban cuando veían

que no estaba dirigido a su dirección MAC. Esto es importante de apreciar: con un hub, cada frame mandado por la red era recibido por cada NIC, pero sólo la NIC con la dirección MAC correspondiente procesaba ese frame.
Las redes posteriores reemplazaron los hubs con un dispositivo más inteligente llamado switch. Los switches, como veremos más adelante, filtran el tráfico por dirección MAC. En lugar de mandar todos los frames a todas las NICs conectadas, un switch manda el frame sólo a la NIC con la MAC correspondiente.

1.2.4 FCS a profundidad

Todos los Frame Check Sequence (FCS) tienen sólo 4 bytes, sin embargo los frames tienen, a lo más, 1500 bytes de datos. ¿Cómo pueden 4 bytes decir si los 1500 bytes en los datos son correctos? Aquí entra la magia matemática del Cyclic Redundancy Check (CRC). Sin entrar en detalles, podemos pensar en el CRC como un problema de residuo tras la división. El NIC que manda el frame hace la matemática para crear el CRC. El NIC receptor aplica la misma matemática, si el resultado es igual al CRC, sabe que los datos llegaron bien, de lo contrario, tira el frame.

1.2.5 Llevando los datos a la línea

El proceso de llevar los datos al cable y luego agarrar esos datos del mismo es increiblemente complejo. Por ejemplo, ¿qué pasa para que dos NICs no hablen al mismo tiempo? Como todos los datos mandados por una NIC son leídas por todas las demás de la red, sólo un sistema puede hablar a la vez en las redes cableadas viejas. Las redes usan frames para restringir la cantidad de datos que una NIC puede mandar a la vez, dándole a todos los NICs un espacio para que manden sus frames por la red en un tiempo razonable. Tratar con estos y otros problemas requiere de electrónicos sofisticados, pero las NICs manejan estos problemas por su propia cuenta.

1.2.6 Empezando a conocerte

Usar las direcciones MAC es una gran manera de mover los dato, pero esto genera una pregunta importante. ¿Cómo puede una NIC emisora saber cual es la direccion MAC de la NIC a la que le está enviando los datos? En la mayoría de los casos, el sistema emisor ya sabe la dirección MAC pues,

probablemente, se habían comunicado antes y cada sistema guarda estos datos. Si no conoce la dirección MAC, una NIC puede mandar un *broadcast* a la red para preguntarlo. La direccion MAC ff:ff:ff:ff:ff:ff es la dirección de broadcast de la capa 2 -si una NIC manda un frame a la dirección de broadcast, cada NIC en la red procesa ese frame. Los datos de ese frame de broadcast contiene una petición para la dirección MAC de un sistema. Sin saber la dirección MAC para empezar, la computadora emisora usará una dirección IP para localizar la computadora de entre todas. El sistema con la dirección MAC que está buscando el sistema leerá la petición en el frame de broadcast y responderá con su dirección MAC.

1.2.7 El movimiento de un frame

Ahora que hemos visto todas las partes que se utilizan para mandar y recibir frames, pongamos todas las piezas donde van y veamos como llega un frame de un sistema a otro. El proceso de emisión/recepción básico es como sigue. Primero, el sistema operativo del sistema emisor pasa algunos datos a su NIC. La NIC construye un frame para transportar los datos al NIC receptor. Una vez creado el frame, añade el Frame Check Sequence (FCS) y pone los datos en el frame. Después, el NIC pone su propia dirección MAC en el frame seguida de la dirección MAC receptora. Luego manda este frame por los cables de la red.

Nota 1 *Cualquier frame que va dirigido específicamente a la dirección MAC de otro dispositivo es llamado un frame unicast.*

El frame se propaga por el cable de la red hacia la caja central. El switch manda frames unicast a la dirección MAC y manda broadcast frames a cada sistema de la red. La NIC recibe el frame. La NIC le quita la información del frame al frame y manda los datos al software - el sistema operativo- para procesarse. A la NIC receptora no le imprta qué hace el software con los datos, su trabajo acaba en el momento en el que pasa los datos al software. Cualquier dispositivo que trabaja con direcciones MAC es parte de la capa de enlace de datos del modelo OSI o la capa 2.
Notemos que el cableado y los hubs son parte de la capa física. Los switches manejan el tráfico usando direcciones MAC, así que operan en ç la capa 2. Esa es la forma en la que funcionan las redes cableadas modernas. El NIC está en la capa de enalce de datos y en la capa física.

1.2.8 Los dos aspectos de las NIC

Consideremos como se mueven los datos hacia dentro y hacia afuera de la NIC. Por un lado, los frames entran y salen de la NIC por su cable de red. Por otro lado, los datos se mueven hacia arriba y hacia abajo entre la NIC y el software de red del sistema operativo. Los muchos paso sque la NIC hace para mantener estos datos en movimiento - mandar y recibir datos por el cable, crear frames salientes, recibir frames y agregarles las direcciones MAC- están divididos en dos trabajos distintos.
El primer trabajo es llamado Logical Link Control (LLC). El LLC es el aspecto de la NIC que habla con el sistema operativo (usalmente mediante drivers del dispositivo). El LLC maneja múltiples protocolos de red y provee control de flujo.
El segundo trabajo es llamado Media Access Control (MAC), que crea y dirige los frames. Añade su propia dirección MAC y las direcciones MAC a los frames. La subcapa de MAC añade o checa el Frame Check Sequence (FCS). La MAC también se asegura de que los frames, ahora completos con su dirección MAC, sean mandados por los cables de la red.

1.2.9 NIC y capas

La mayoría de materiales de redes que describen el modelo OSI ponen a las NICs en la capa de enlace de datos del modelo. Es en la subcapa MAC, después de todo, que los datos son encapsulados en un frame, las MACs de destino y emisión son agregadas al frame y ocurre el chequeo de errores. Lo que molesta a muchos estudiantes de poner las NICs únicamente en la capa de enlace de datos es la obvia tarea de las NICs de poner ceros y unos en el cable o en el aire. Pero las NICs operan en ambos niveles.

1.3 Más allá del cable -software de red y capas 3-7

Llevar datos de un sistema a otro en una red simple (una en la que todas las computadoras están conectadas al mismo switch) toma poco esfuerzo por parte de las NICs. Pero un problema con las redes simples es que las computadoras deben hacer broadcast para obtener las direcciones MAC. Funciona para redes pequeñas, pero que pasa si las redes son grandes, como del

tamaño de todo el internet.
De igual manera, los datos fluyen usando muchas tecnologías, no solo Ethernet. Estas tecnologías no saben que hacer con las direcciones MAC del Ethernet. Cuando las redes se vuelven grandes, no podemos usar direcciones MAC.
Las redes grandes necesitan un método de logical addressing, como un código postal o un esquema de números telefónicos, que ignora el hardware y permite romper la red completa en cachos más pequeños llamados subredes.
Para movernos más allá de las direcciones MAC y empezar a usar logical addressing, se requiere un software espacial llamado protoclo de red. Los protocolos de red existen en cada sistema operativo. Un protocolo de red no sólo debe crear identificadores únicos para cada sistema, pero debe también crear un conjunto de reglas de comunicación para problemas como cómo manejar datos que están rotos en múliples paquetes y cómo asegurarse de que los paquetes lleguen de una subred a otra. Tomemos un momento para aprender un poco sobre la colección más famosa de protocolos de red -TCP/IP- y su sistema de unique addressing universal.

Nota 2 *Las direcciones MAC son también llamadas direcciones físicas*

Para ser precisos, TCP/IP es, en realidad, varios protocolos diseñados para trabajar juntos, mejor conocido como una suite de protocolos, pero dos protocolos, TCP e IP hacen tanto trabajo que decidieron llamar a la suite con este nombre.
TCP significa *Transmission Control Protocol* e IP significa *Internet Protocol*. IP es el protocolo de red que debemos discutir primero.

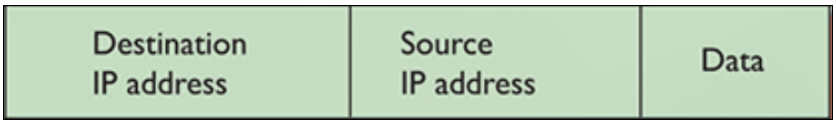
1.3.1 IP-jugando en la capa 3

En la capa de red, la capa 3, los contenedores llamados paquetes son creados y dirigidos para que puedan llegar de una red a otra. El Internet Protocol es el protocolo de logical addressing principal para TCP/IP. IP se asegura de que un pedazo de datos llegue a donde tiene que llegar en la red. Hace esto dándole a cada dispositivo en la red un identificador numérico único llamado dirección IP. Una dirección IP es conocida como dirección lógica, para distinguirla de las direcciones físicas, las direcciones MAC de las NICs. IP usa una notación decimal basada en cuatro numeros de 8-bits. Cada número de 8 bits está en el rango de 0 a 255 y los números están separados

por puntos. Un ejemplo de dirección IP es *192.168.1.76*.
No hay dos sistemas en la misma red que compartan direcciones IP; si dos máquinas reciben la misma dirección IP por accidente, podrían ocurrir efectos no deseados. Estas direcciones IP no aparecen mágicamente -deben ser configuradas por el administrados.
Lo que hace poderoso al logical addressing es otra caja mágica, llamada router, que conecta cada una de las subredes. Los routers usan las direcciones IP, no las direcciones MAC, para mandar los datos. Esto permite que las redes se conecten a lo largo de líneas de datos que no usan Ethernet, como las lineas de teléfono. Cada tipo de red (como Ethernet, SONET y otros) usan un frame único.
En una red TCP/IP, cada sistema tiene dos identificadores únicos: la direcciòn MAC y la dirección IP. La dirección MAC (la dirección física) literalmente está quemada en los chips de las NICs, mientras que las IP (la dirección lógica) está almacenada en el software del sistema. Las direcciones MAC vienen con las NICs, así que no hay que configurarlas, pero las direcciones IP sí hay que configurarlas.

1.3.2 Paquetes dentro de frames

Para que una red TCP/IP mande información correctamente, los datos deben estár envueltos en dos contenedores distintos. Un frame de algún tipo permite que los datos se muevan de un dispositivo a otro. Dentro de ese frame hay tanto un contenedor IP-específico que permite que lo routers determinen a dónde mandar los datos, como los datos mismos. En TCP/IP, ese contenedor interno es un paquete.



Cada paquete IP es pasado a la NIC, que después envuelve ese paquete IP en un frame regular, creando, en esencia, un paquete dentro de un frame. Cuando mandamos datos de una computadora a otra en una red TCP/IP como el internet, esos datos pueden pasar por muchos routers antes de llegar a su destino. Cada router quita el frame, determina a dónde mandar los datos de acuerdo con la dirección IP del paquete, crea un nuevo frame, y luego manda el paquete dentro del frame al siguiente lugar. El nuevo tipo

de frame es de la tecnología adecuada según la tecnología que conecta al siguiente router. Eso podría ser un cable o una conexión de red DSL, por ejemplo. El paquete IP, por otro lado, se mantiene sin cambiar.
Una vez que el paquete llega al router de la subred de destino, ese router quita el frame que llegó, ve la dirección IP, y añade otro frame con la dirección MAC de destino adecuada que encaja con la dirección IP de destino. La NIC receptora quira el Ethernet frame y pasa el resto del paquete al software. El software de red del sistema operativo maneja el resto del trabajo. El software del driver del NIC es la interconexión entre el hardware y el software. El driver del NIC sabe como comunicarse con el NIC para mandar y recibir frames, pero no puede hacer nada con el paquete. En su lugar, el driver del NIC manda el paquete a otros servicios que saben cómo manejar los paquetes separados y convertirlos en páginas web, mensajes de mail, archivos y otros.

1.3.3 Segmentación y reensamble - Capa 4, la capa de transporte

Como la mayoría de cachos de datos son más grandes que un sólo paquete, deben romperse antes de mandarse por una red. Cuando una computadora servidor recibe una petición por algunos datos, debe ser capaz de romper los datos en cachos que caben en un paquete y, eventualmente en un frame de un NIC, organizar los paquetes para el beneficio del sistema receptor, y dárselos al NIC para mandarlos. Esto es llamado segmentación. El sistema receptor hace el reensamble de los paquetes. Debe reconocer una serie de paquetes que llegan como una sola transmisión de datos, reensablar los paquetes correctamente basado en la información incluida en lo s paquetes por el sistema emisor, y verificar que todos los paquetes de los datos llegaron de manera correcta.
Esta parte es relativamente sencilla - el protocolo de transporte rompe los datos en chunks llamados segmentos y le da a cada segmento un tipo de nùmero. (Los datagramas, también creados en la capa 4, son más simples y no se rompen en cachos o tienen números de secuencia). Encajado en los datos de cada paquete que contiene un segmento hay un número de secuencia. Leyendo el número de secuencia, el sistema receptor sabe tanto el número total de segmentos como el cómo ponerlos en su lugar.
La capa de transporte, la capa 4 del modelo OSI, tiene un trabajo grande: es el software de segmentación/reensamblado. Como parte de su trabajo,

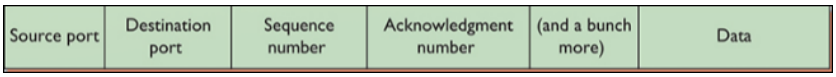
la capa de transporte también inicia peticiones para paquetes que no fueron recibidos en el orden correcto.

1.3.4 Comunicación orientada a la conexión vs sin conexión

Algunos protocolos, como Simple Mail Transfer Protocol (SMTP) usado para mandar mensajes de e-mail, requieren que el cliente y el servidor verifiquen que hay una conexión antes de mandar un mensaje. Esto hace sentido, pues no queremos que nuestro correo llegue todo corrupto.
Alternativamente, un número de protocolos de TCP/IP mandan datos sin esparar a verificar que el sistema receptor esté listo. Cuando usamos Voice over IP (VoIP), por ejemplo, la llamada se hace sin verificar primero que el otro dispositivo esté ahí. El protocolo orientado a la conexión es el Transmission Control Protocol. El protocolo sin conexión es el User Datagram Protocol (UDP).

1.3.5 Segmentos dentro de los paquetes

Para ver la capa de transporte en acción, hay que quitarle las direcciones IP a un paquete IP. Lo que queda es un bloque de datos en otro contenedor llamado un segmento TCP. Los segmentos TCP tienen muchos otros campos para asegurarse de que los datos lleguen a su destino en el orden correcto. Estos campos tienen nombres como puerto de origen, puerto de destino, numero de secuencia y número de Acknowladgement.



En este contexto, un puerto - un número entre 1 y 65,536- es un valor lógico asignado a aplicaciones o servicios específicos. Muchos segmentos TCP entran a una computadora. La computadora necesita una forma de determinar qué segmentos de TCP van a qué aplicaciones. Un servidor web, por ejmplo, ve mucho tráfico, pero escucha segmentos TCP con puertos de destino 80 o 443, toma esos segmentos y los procesa. De igual manera, cada segmento TCP contiene otro número de puerto, el puerto de emisión, para que el cliente sepa que hacer para regresar información.
Los datos vienen de la capa de aplicación. La capa de transporete rompe los datos en bloques, añadiendo números de puertos, números de secuencia y de

ackwnloadgement, creando el segmento TCP. La capa de transporte luego pasa el segmento TCP a la capa de red, que crea un paquete IP. Aunque mucho tráfico en una red TCP/IP usa TCP en la capa de transporte, también existe UDP. Siguiendo el mismo proceso, la capa de transporte añade los números de puertos, número de longitud y un checksum como un header y lo combina todo para crear un contenedor llamado un datagrama UDP. Un datagrama UDP carece de la mayoría de los campos que tiene un segmento TCP, simplemente porque a UDP no le importa si la computadora receptora recibe los datos.