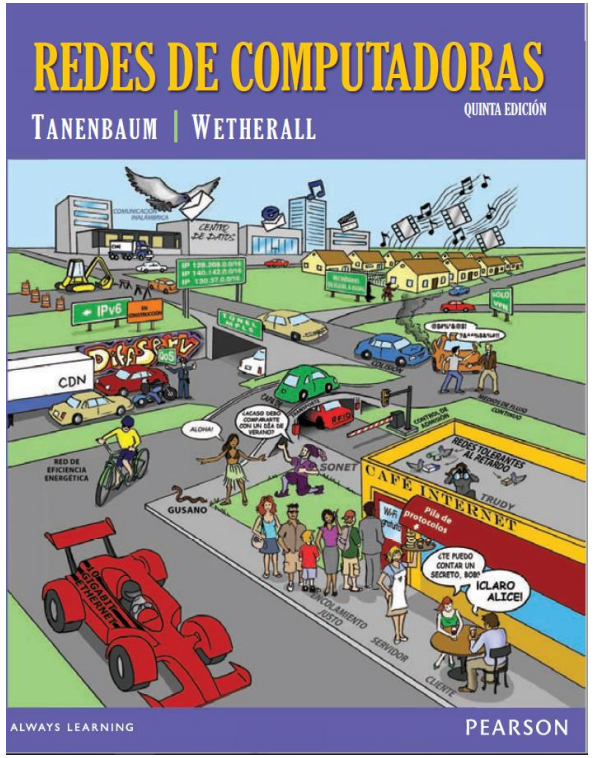
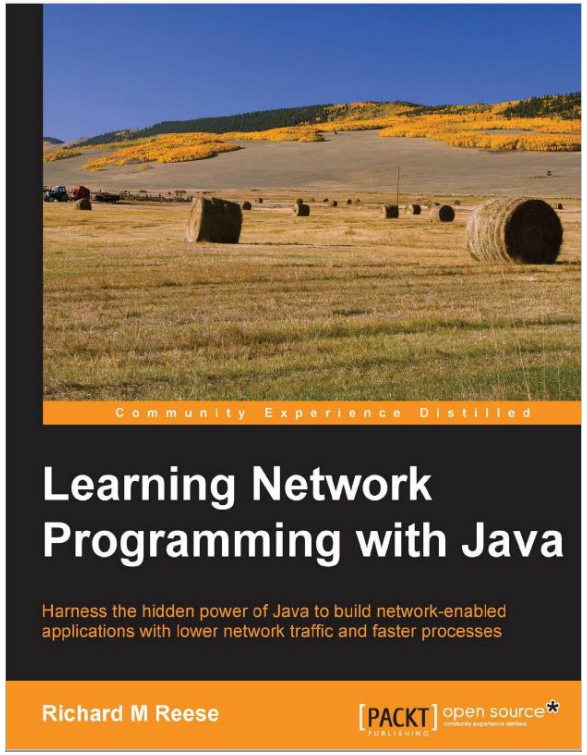
REDES DE COMPUTADORES Y LABORATORIO

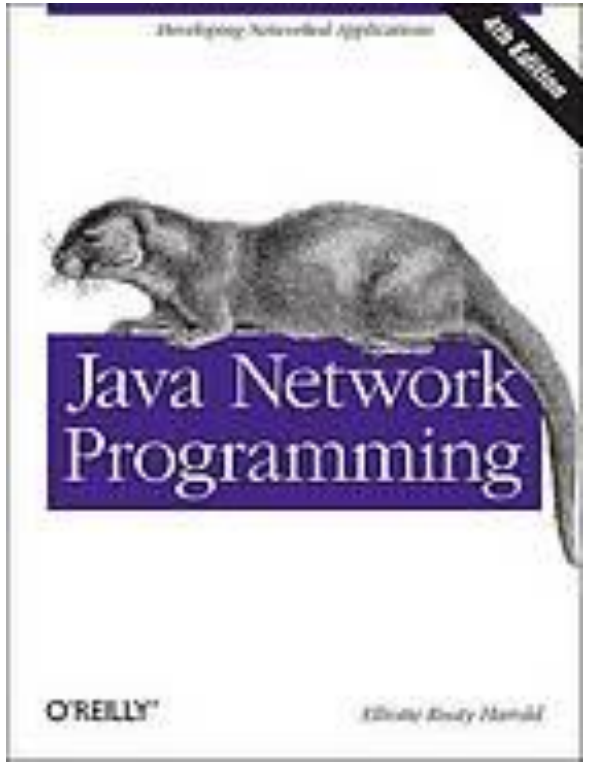
Christian Camilo Urcuqui López, MSc

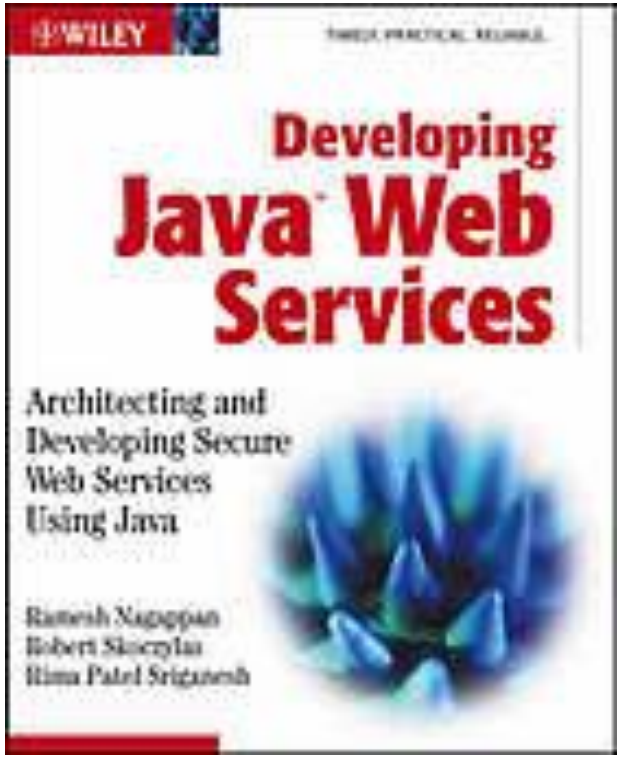
UNIVERSIDAD ICESI | A OTRO NIVEL

BIBLIOGRAFÍA









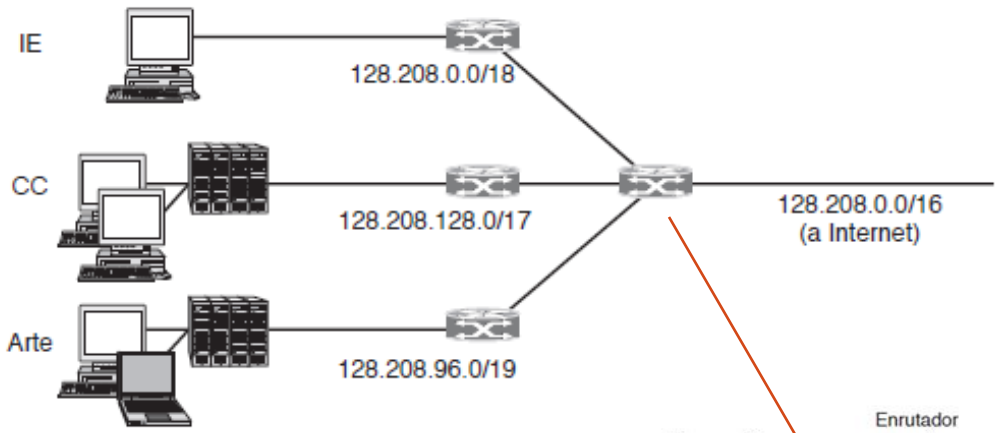
COMPETENCIAS

- Describir NAT
- Describir los protocolos ICMP, ARP y DHCP
- Describir UDP.
- Describir TCP.

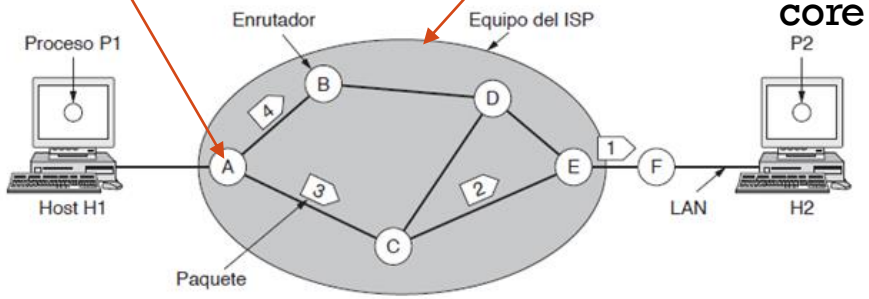
PREGUNTAS

- Suponga que su universidad comenzó con un prefijo de /24 para la red de las salas de computo de los edificios C, D y E; estos edificios cuentan con un aproximado de 255 equipos y se quiere ofrecer la conectividad por lo menos a 9 host adicionales.
- Con base al material estudiado para hoy, ¿Qué técnica aplicaría para resolver este problema?
- Aplique esta técnica a la dirección 192.168.170.10, explique el proceso donde ilustre el resultado de la dirección solo del primer nuevo host.
- ¿Por qué se utiliza NAT?

- Nadie sabe cuántas redes están conectadas a Internet
- Zona libre predeterminada, acá no funcionan las reglas predeterminada



Reglas predeterminadas



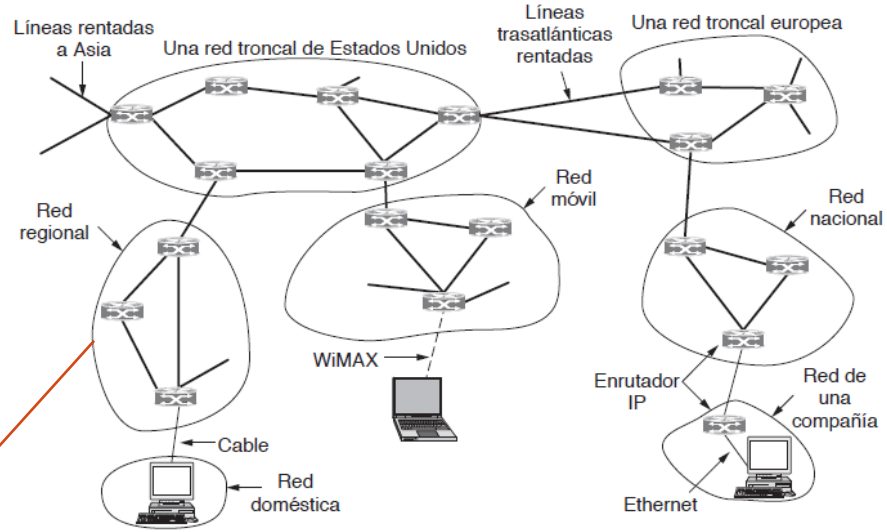


Figura 5-45. Internet es una colección interconectada de muchas redes.

Enrutadores especializados para trabajar con grandes cargas de paquetes en redes backbone – core routers

UNIVERSIDAD ICESI | A OTRO NIVEL

EL PROBLEMA DEL TAMAÑO DE LAS TABLAS DE ENRUTAMIENTO

- El procesamiento aumenta por lo menos en forma lineal con respecto al tamaño de la tabla. Una mayor comunicación aumenta la probabilidad de que algunas partes se pierdan, por lo menos en forma temporal, lo que tal vez conduzca a inestabilidades en el enrutamiento.
- Con el fin de reducir las tablas de enrutamiento se aplica una perspectiva parecida que en las subredes.
- Se combinan varios prefijos pequeños en un solo prefijo más grande. Este proceso se conoce como **agregación de rutas.** El prefijo más grande se le denomina **superred** para contrastar con las otras subredes resultantes. Es decir, la misma dirección IP que el enrutador trata como /22 (2^8 *direcciones*) puede ser tratada por otro enrutador como parte de un prefijo /20 más grande (2^{12} *direcciones*).
- La responsabilidad de tener el prefijo correspondiente es del enrutador.
- Este diseño se conoce como CIDR **(Classless InterDomain Routing)**

CIDR (CLASSLESS INTERDOMAIN ROUTING)

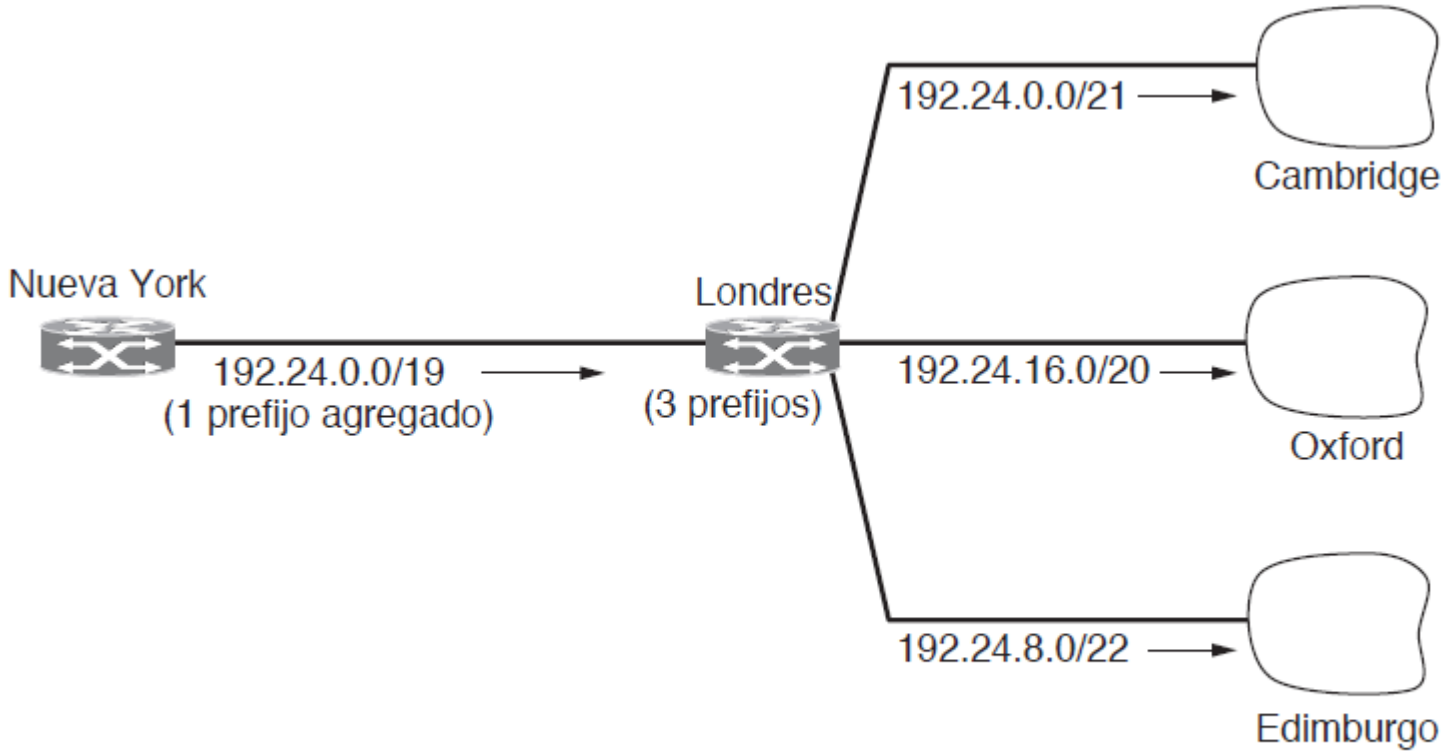


Figura 5-51. Agregación de prefijos IP.

Como hemos visto las direcciones IPv4 tienen un límite y estamos escasos…

NAT (NETWORK ADDRESS TRANSLATION)

- Las direcciones IP son escasas. Un ISP podría tener una dirección con un prefijo de /16, lo cual da 65534 números host. Si tiene más clientes que esos, tiene un problema.
- Una solución es migrar a IPv6, pero, se requerirá mucho tiempo e inversión para lograrlo.
- Mientras tanto, existe otra solución que es la aplicación de NAT (documentada en la RFC 3022).

NAT (NETWORK ADDRESS TRANSLATION)

- El objetivo de la NAT es que el ISP asigne a cada hogar o negocio una dirección IP (puede ser un grupo pequeño) para el tráfico de Internet.
- Dentro de la red del cliente hay solo una dirección IP para enrutar el tráfico interno y antes de salir a Internet esta es traducida a la dirección IP pública compartida.
- Las traducciones hacen uso de tres rangos de direcciones IP que se han declarado como privados.

10.0.0.0	– 10.255.255.255/8	(16,777,216 hosts)
172.16.0.0	– 172.31.255.255/12	(1,048,576 hosts)
192.168.0.0	– 192.168.255.255/16	(65,536 hosts)

NAT (NETWORK ADDRESS TRANSLATION)

- La caja NAT transforma la dirección IP interna, 10.0.0.1 a la dirección verdadera del cliente, 198.60.42.12.
- A menudo las NAT vienen incorporadas en los firewall para el análisis de las paquetes enviados y recibidos. También, se pueden encontrar en los enrutadores.

El puerto es importante para la NAT ya que le permite identificar el proceso emisor y al receptor.

La NAT en su proceso de identificación debe analizar un puerto origen y uno destino.

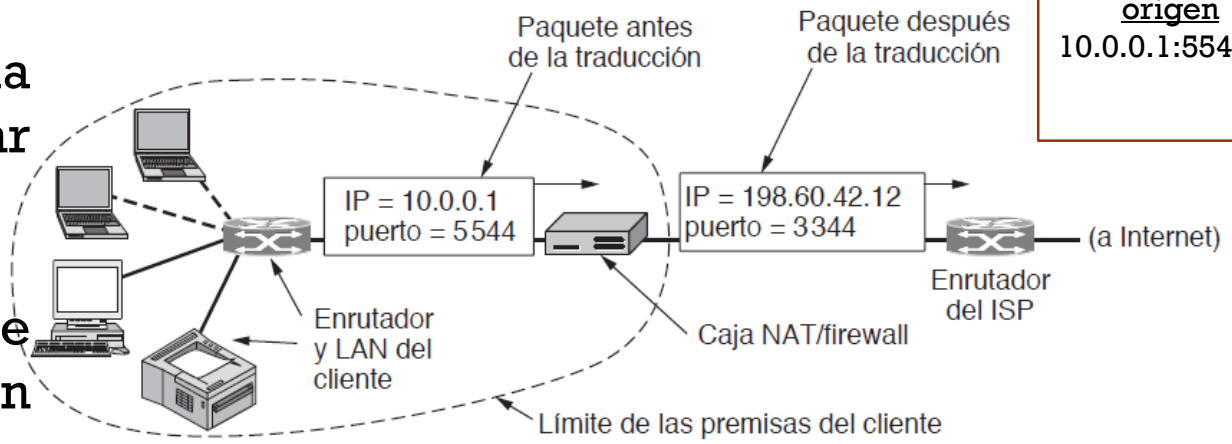
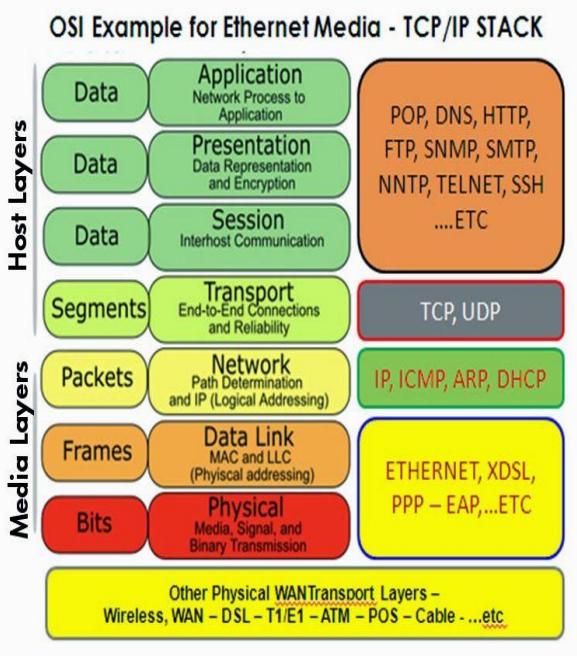


Tabla de la NAT

origen	salida
10.0.0.1:5544	198.60.42.12:3344

Figura 5-55. Colocación y funcionamiento de una caja NAT.

PROTOCOLOS DE CONTROL EN INTERNET

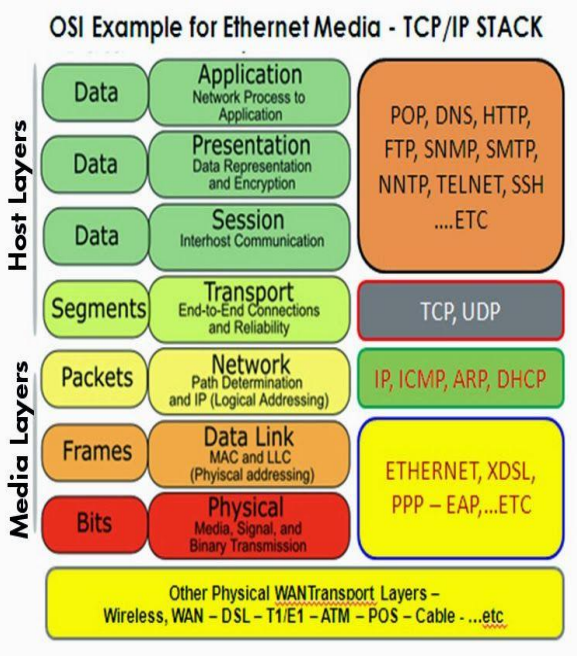


- **ICMP (Internet Control Massage Protocol**) es un protocolo que informa sobre un evento inesperado en el procesamiento de un paquete en un enrutador.
- También es utilizado para probar Internet.

Tipo de mensaje	Descripción
Destination unreachable (Destino inaccesible).	No se pudo entregar el paquete.
Time exceeded (Tiempo excedido).	El tiempo de vida llegó a cero.
Parameter problem (Problema de parámetros).	Campo de encabezado inválido.
Source quench (Fuente disminuida).	Paquete regulador.
Redirect (Redireccionar).	Enseña a un enrutador la geografía.
Echo and echo reply (Eco y respuesta de eco).	Verifica si una máquina está viva.
Timestamp request/reply (Estampa de tiempo, Petición/respuesta).	Igual que solicitud de eco, pero con marca de tiempo.
Router advertisement/solicitation (Enrutamiento anuncio/solicitud).	Busca un enrutador cercano.

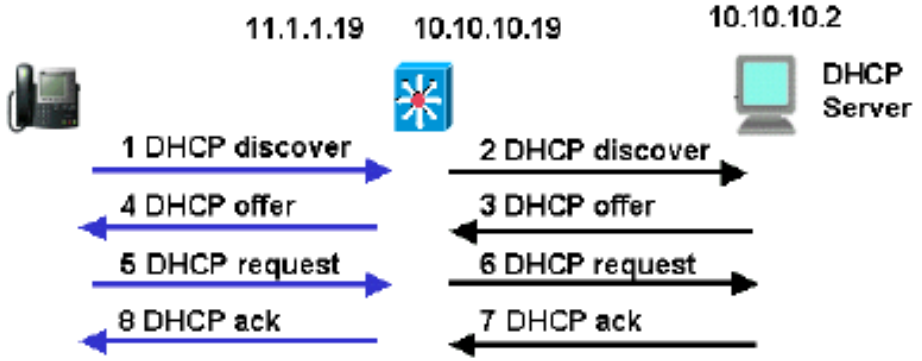
Figura 5-60. Los principales tipos de mensajes ICMP.

PROTOCOLOS DE CONTROL EN INTERNET



- **ARP (Address Resolution Protocol**) encargado de encontrar la dirección de hardware (MAC) que corresponde a una determinada dirección IP.
  - Las máquinas luego de ejecutar ARP almacenan sus resultados en cache.
- **DHCP (Dynamic Host Configuration Protocol).** Es un proceso para configuración dinámica de los host; para ello debe existir un servidor DHCP responsable

La técnica del arrendamiento



LA CAPA DE TRANSPORTE

- Recordemos…. La capa de red provee entrega de paquetes punto a punto mediante el uso de datagramas o circuitos virtuales.
- El objetivo de la capa de transporte es proporcionar un servicio de transmisión de datos eficiente, confiable y económico a sus usuarios, procesos que normalmente son de la capa de aplicación.
- Gracias a esta capa, los programadores pueden escribir código de acuerdo con un conjunto estándar de **primitivas**; estos programas pueden funcionar en una amplia variedad de redes sin necesidad de preocuparse por lidiar con diferentes interfaces de red y distintos niveles de confiabilidad.

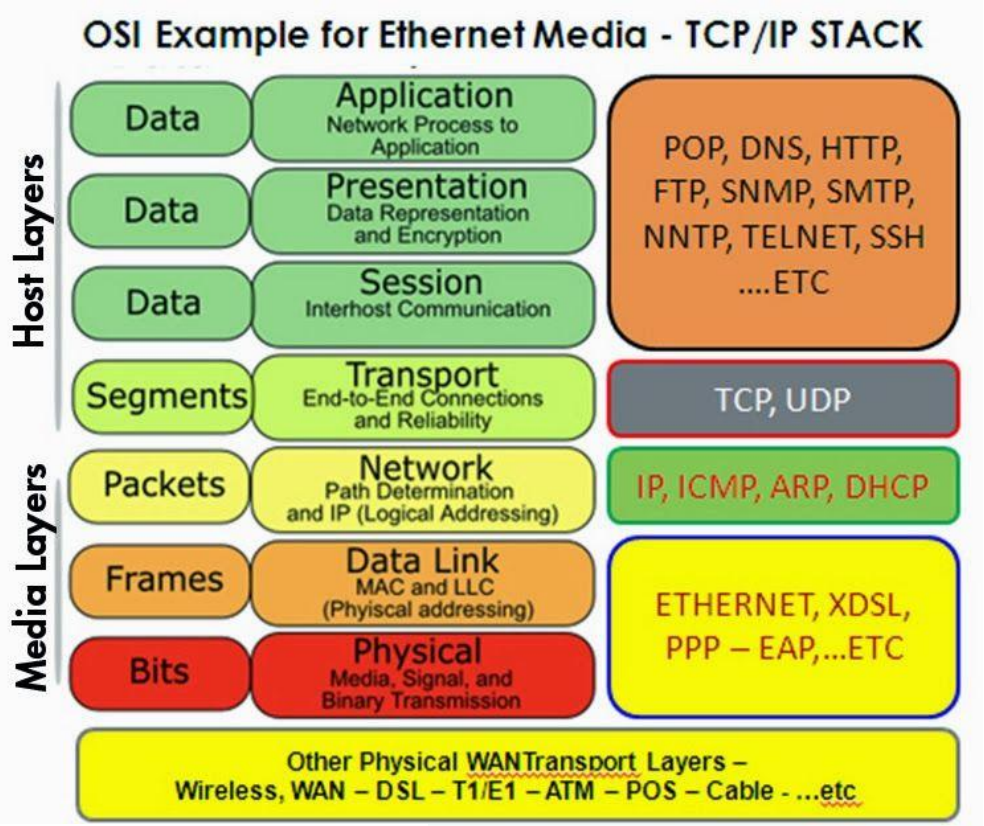
PRIMITIVAS DEL SERVICIO DE TRANSPORTE

- La capa de transporte debe proporcionar algunas operaciones a los programas de aplicación a través de una interfaz de servicios.
- Cada servicio tiene su propia interfaz.
- Interfaz orientada a la conexión.

Primitiva	Paquete enviado	Significado
LISTEN	(ninguno)	Se bloquea hasta que algún proceso intenta conectarse.
CONNECT	CONNECTION REQ.	Intenta activamente establecer una conexión.
SEND	DATA	Envía información.
RECEIVE	(ninguno)	Se bloquea hasta que llegue un paquete DATA.
DISCONNECT	DISCONNECTION REQ.	Solicita que se libere la conexión

- Los mensajes enviados a través de una entidad de transporte a otra se conocen como **segmentos.**

PRIMITIVAS DEL SERVICIO DE TRANSPORTE



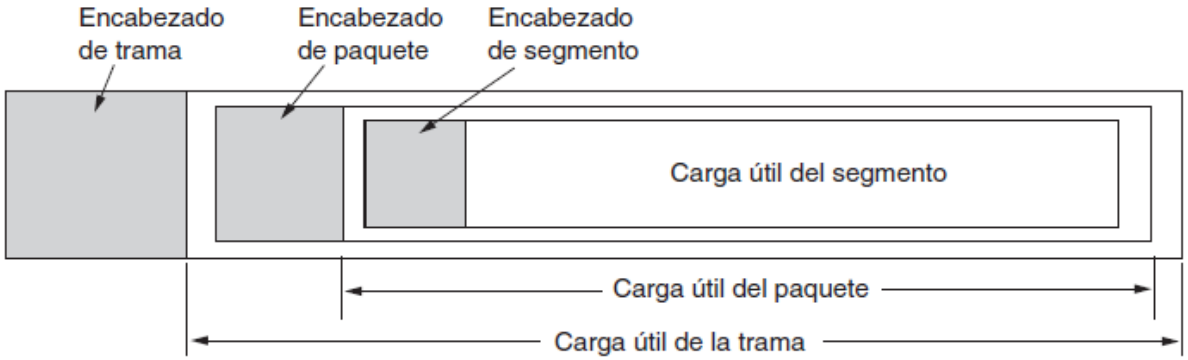


Figura 6-3. Anidamiento de segmentos, paquetes y tramas.

PRIMITIVAS DEL SERVICIO DE TRANSPORTE

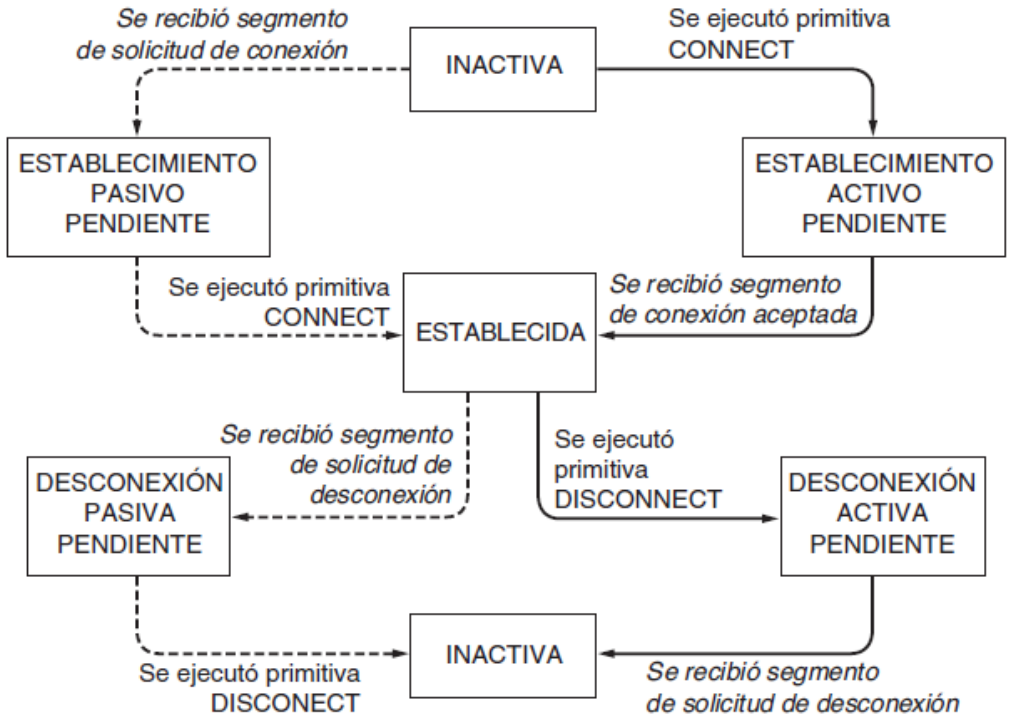


Figura 6-4. Un diagrama de estado para un esquema simple de manejo de conexiones. Las transiciones etiquetadas en cursiva se producen debido a la llegada de paquetes. Las líneas continuas muestran la secuencia de estados del cliente. Las líneas punteadas muestran la secuencia de estados del servidor.

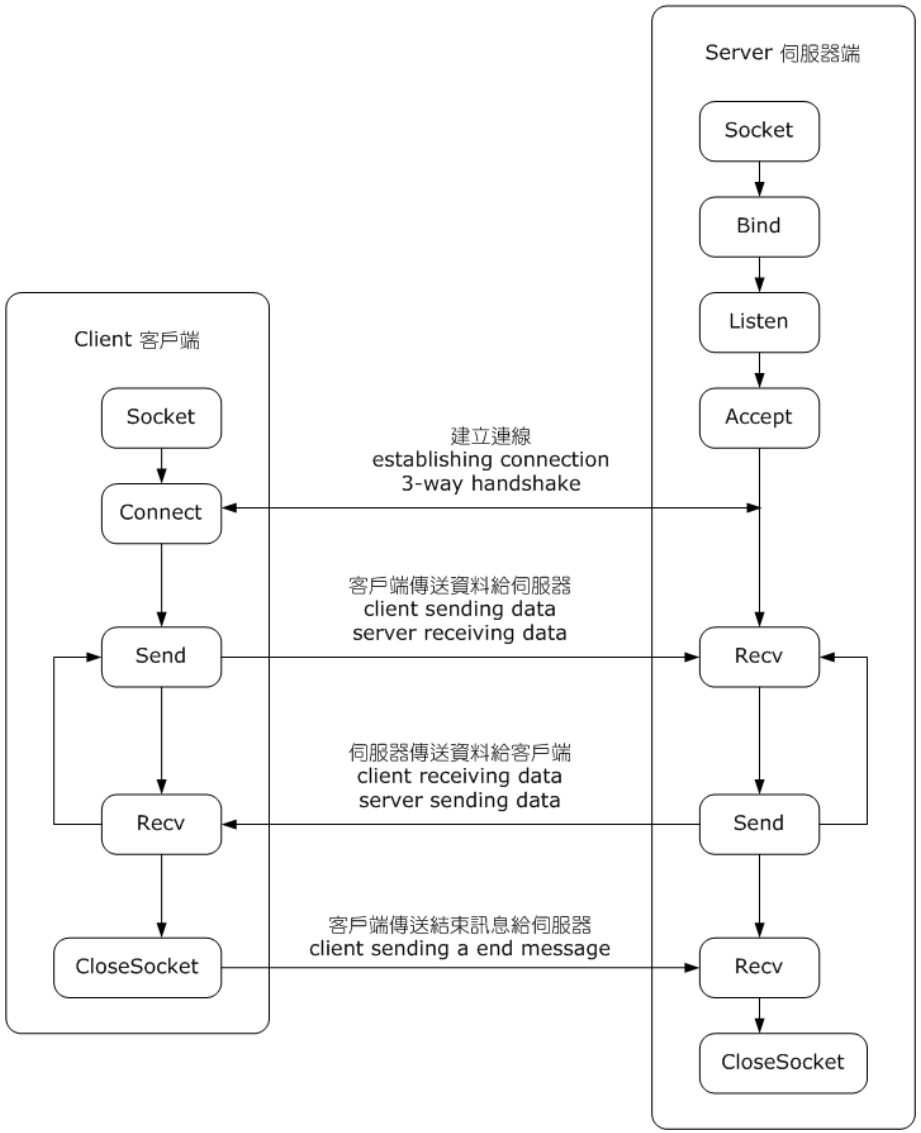
SOCKETS DE BERKERLEY

- Son un conjunto de primitivas de transporte: las primitivas de socket que se utilizan para TCP.

Primitiva	Significado
SOCKET	Crea un nuevo punto terminal de comunicación.
BIND	Asocia una dirección local con un socket.
LISTEN	Anuncia la disposición de aceptar conexiones; indica el tamaño de la cola.
ACCEPT	Establece en forma pasiva una conexión entrante.
CONNECT	Intenta establecer activamente una conexión.
SEND	Envía datos a través de la conexión.
RECEIVE	Recibe datos de la conexión.
CLOSE	Libera la conexión.

Figura 6-5. Las primitivas de socket para TCP.

TCP Socket 基本流程圖
TCP Socket flow diagram



DIRECCIONAMIENTO Y ESTABLECIMIENTO DE CONEXIÓN

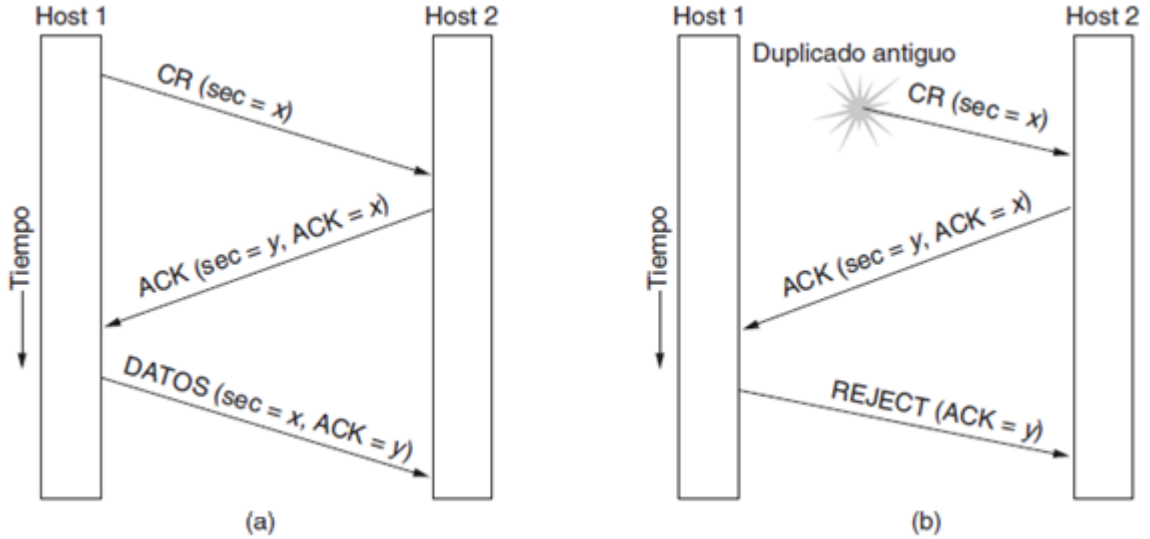
- El método que permite definir las direcciones de transporte en las que los procesos pueden escuchar solicitudes de conexión es a través de puntos terminales conocidos cómo **puertos.**
- **Acuerdo de tres vías** (*three-way handhsake*). Es un protocolo que implica que un igual verifique que la conexión sea realmente la actual.

Algunos segmentos:

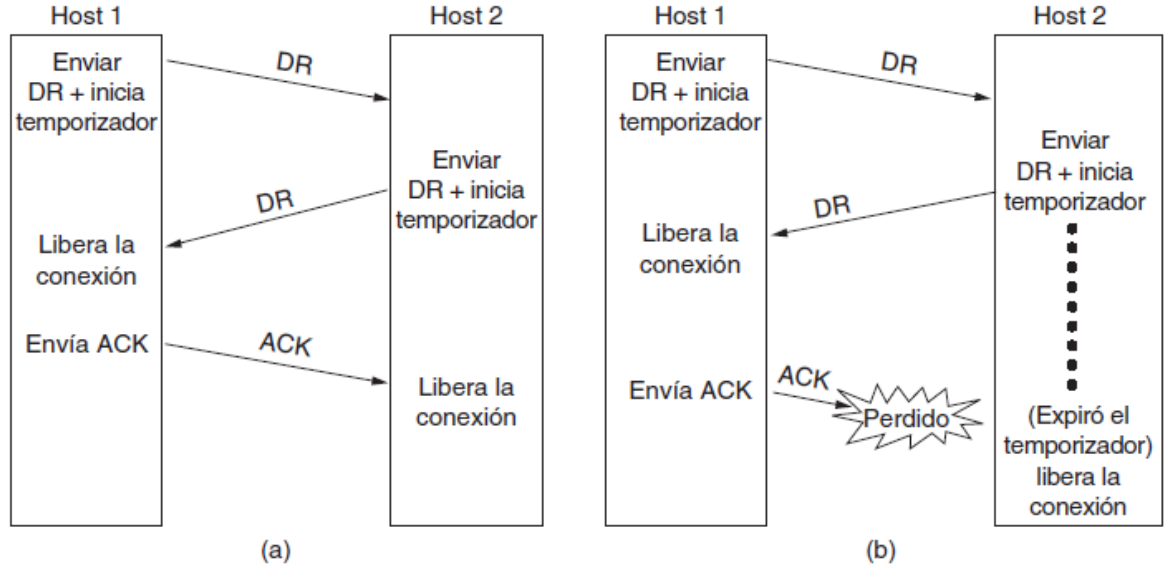
ACK (acknowledgement), es un mensaje que el destino de la comunicación envía al origen de esta para confirmar la recepción del mensaje.

CR (CONNECTION REQUEST)

DR (DISCONNECTION REQUEST)



Establecimiento de una conexión



Liberación de una conexión

LOS PROTOCOLOS DE TRANSPORTE DE INTERNET: UDP

UDP (USER DATAGRAM PROTOCOL)

- Proporciona una forma para que las aplicaciones envíen datagramas IP encapsulados sin tener que establecer una conexión. RFC 768.
- UDP es un protocolo simple para interacciones cliente/servidor y multimedia.
- UDP trasmite segmentos que consisten en un encabezado de 8 bytes seguido de la carga útil.

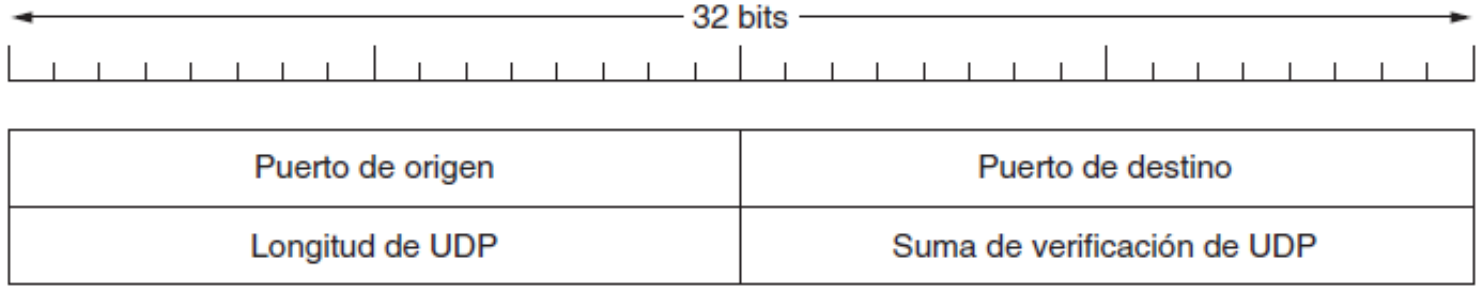


Figura 6-27. El encabezado UDP.

- La longitud incluye el encabezado de 8 bytes y los datos. La longitud mínima es de 8 bytes y la máxima es de 655515 bytes.

LOS PROTOCOLOS DE TRANSPORTE DE INTERNET: TCP

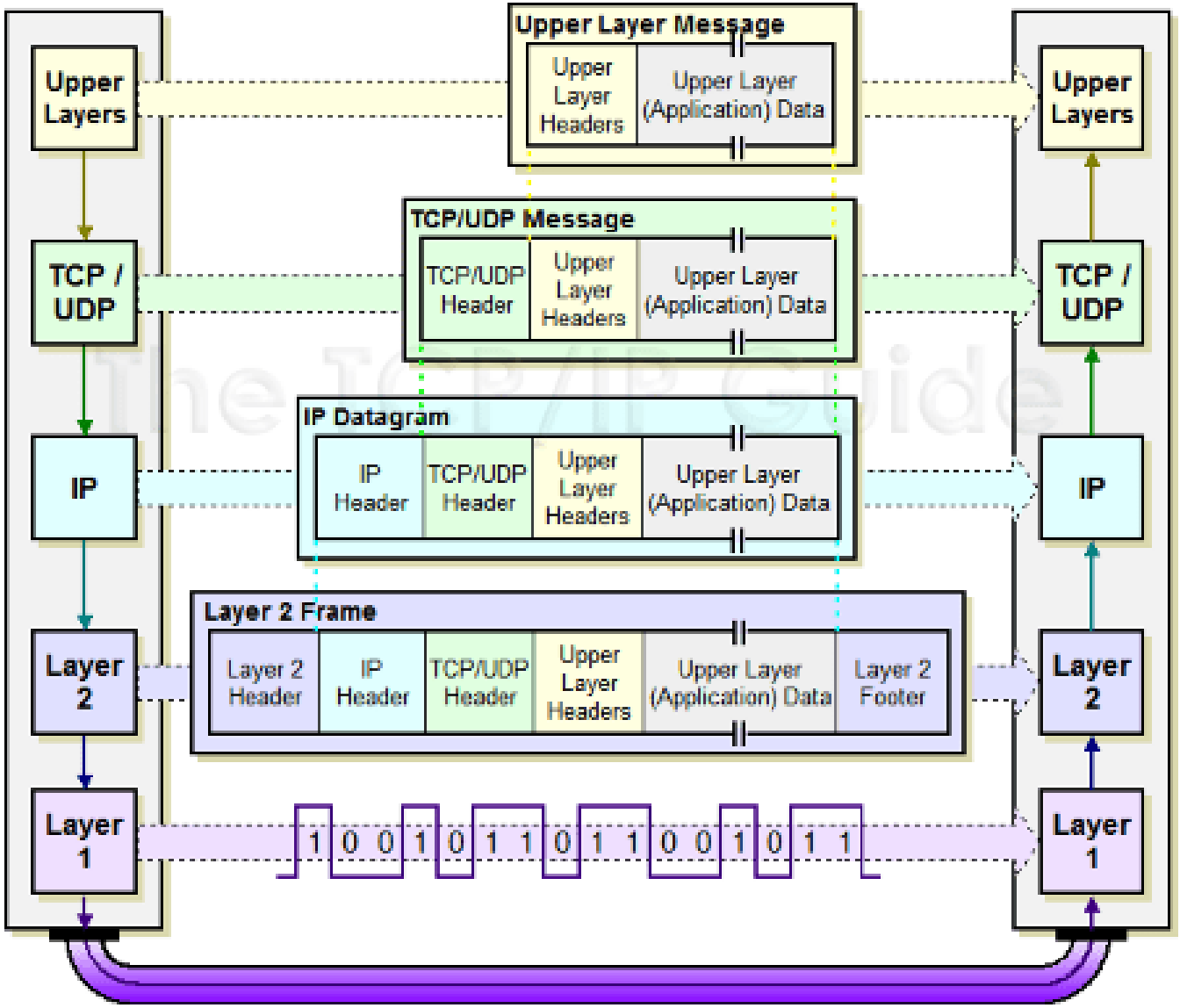
TCP (PROTOCOLO DE CONTROL DE TRANSMISIÓN

- Se diseño con la finalidad de proporcionar un flujo de bytes confiable de extremo a extremo a través de una interred no confiable. Roadmap RFC
- El servicio TCP se obtiene al hacer que tanto el servidor como el receptor creen puntos terminales, llamados **sockets.**
- Cada socket tiene un número (dirección) que consiste en la dirección IP del host y un número de 16 bits que es local para ese host, llamado **puerto**

Puerto	Protocolo	Uso
20, 21	FTP	Transferencia de archivos.
22	SSH	Inicio de sesión remoto, reemplazo de Telnet.
25	SMTP	Correo electrónico.
80	HTTP	World Wide Web.
110	POP-3	Acceso remoto al correo electrónico.
143	IMAP	Acceso remoto al correo electrónico.
443	HTTPS	Acceso seguro a web (HTTP sobre SSL/TLS).
543	RTSP	Control del reproductor de medios.
631	IPP	Compartición de impresoras.

Figura 6-34. Algunos puertos asignados.

La capa IP no ofrece garantía de que los datagramas se entregarán de manera apropiada y en el orden correcto; es trabajo de TCP incorporar los mecanismos que permitan tener un buen desempeño y confiabilidad.



TCP (PROTOCOLO DE CONTROL DE TRANSMISIÓN

- Todas las conexiones TCP son *full dúplex* y punto a punto.
- Una conexión TCP es un flujo de bytes, no un flujo de mensajes.

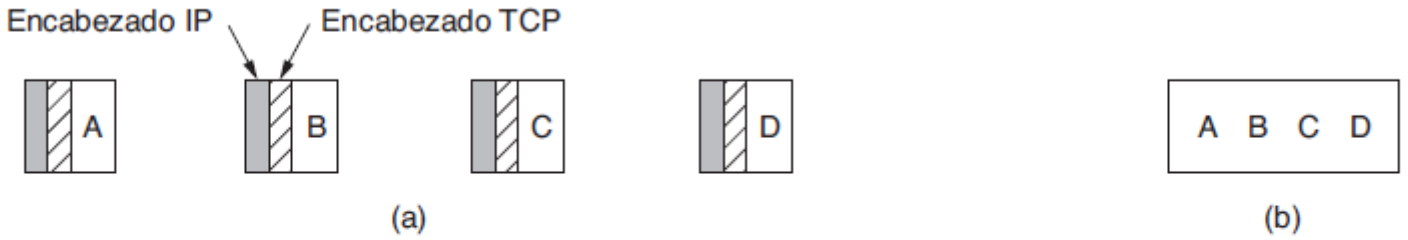


Figura 6-35. (a) Cuatro segmentos de 512 bytes que se envían como diagramas IP separados. (b) Los 2 048 bytes de datos que se entregan a la aplicación en una sola llamada READ.

- Cuando una aplicación pasa datos a TCP, éste decide entre enviarlos de inmediato o almacenarlos en el búfer. La bandera PUSH (PSH) sirve para forzar la salida de datos.

TCP (PROTOCOLO DE CONTROL DE TRANSMISIÓN

- URGENT es otra bandera que le indica a TCP que deje de acumular datos y transmita de inmediato todo lo que tiene para esa conexión (se utiliza cuando de un usuario presiona CTRL-C para interrumpir un cálculo remoto).
- Cada byte de una conexión de TCP tiene su propio número de secuencia de 32 bits.
- Un **segmento TCP** consiste en un encabezado fijo de 20 bytes, es decir, 160 bits (más una parte opcional), seguido de cero o más bytes de datos. **El software de TCP decide qué tan grandes deben ser los segmentos**
- Hay dos límites que restringen el tamaño del segmento.
  1. Cada segmento debe caber en la carga útil de 65515 bytes del IP.
  2. Cada segmento debe caber en la MTU (Unidad Máxima de Transferencia) del emisor y receptor con el fin de evitar fragmentación.

TCP (PROTOCOLO DE CONTROL DE TRANSMISIÓN

- Las implementaciones modernas de TCP realizan el descubrimiento de MTU de la ruta mediante mensajes de error de ICMP con el fin de encontrar la ruta más pequeña

- 5 tupla: protocolo (TCP), dirección IP destino y origen, puerto destino y origen.
- *CWR y ECE* para indicar congestión
- *SYN* se usa para establecer conexiones.
- *RST* se utiliza para reestablecer la conexión.
- *FIN* libera la conexión.

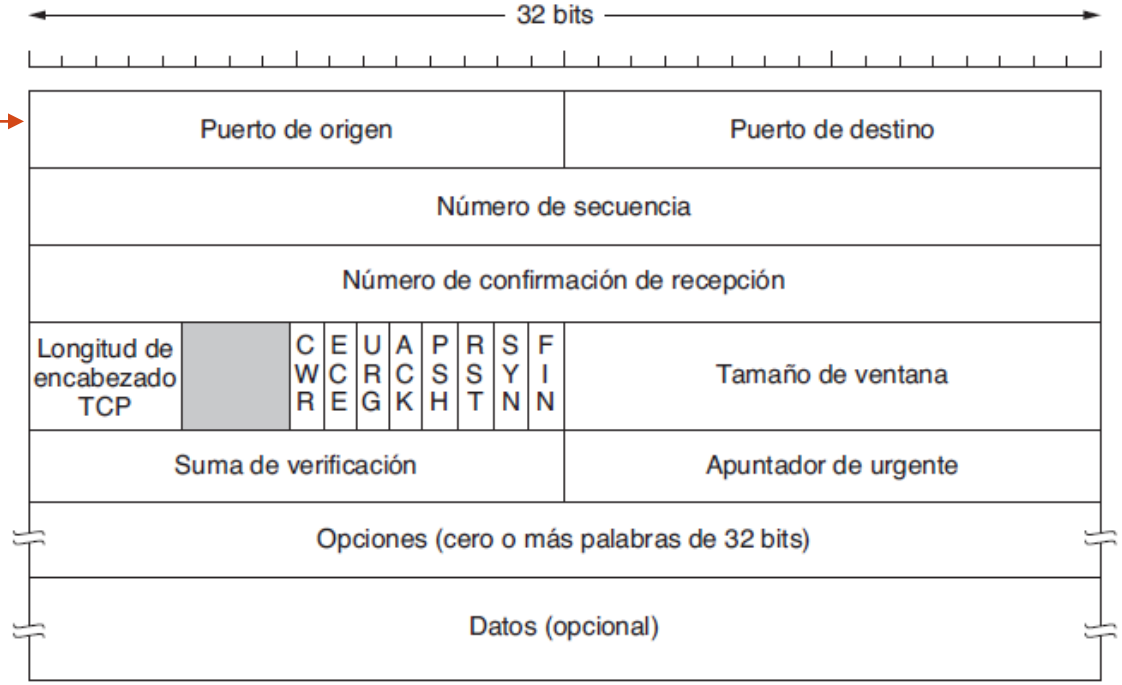


Figura 6-36. El encabezado TCP.

TCP (PROTOCOLO DE CONTROL DE TRANSMISIÓN

- El control de flujo en TCP se maneja mediante una ventana deslizante de tamaño variable.
  - El campo *Tamaño de ventana* indica la cantidad de bytes que se pueden enviar.
  - Un campo de Tamaño de ventana de 0 es válido e indica que se han recibido los bytes hasta *Número de confirmación de recepción*
  - *-1* para cuando el receptor no ha tenido oportunidad de consumir los y ya no desea más.

- *Suma de verificación* para agregar confiabilidad.
- *Opciones* agrega las características adicionales que no están cubiertas por el encabezado normal.
  - MSS (Tamaño Máximo de Segmento) que un host permite aceptar.
  - Tamaño de escala permite al emisor y al receptor negociar un factor de escala de ventana al inicio de la conexión.

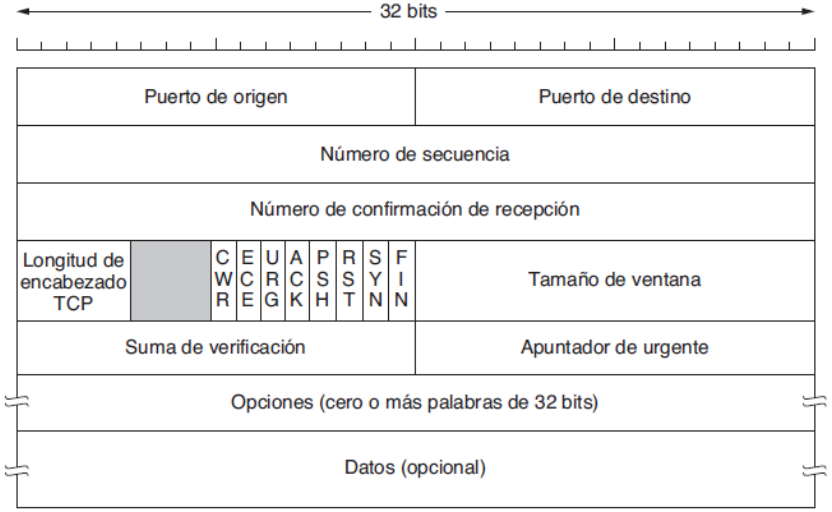
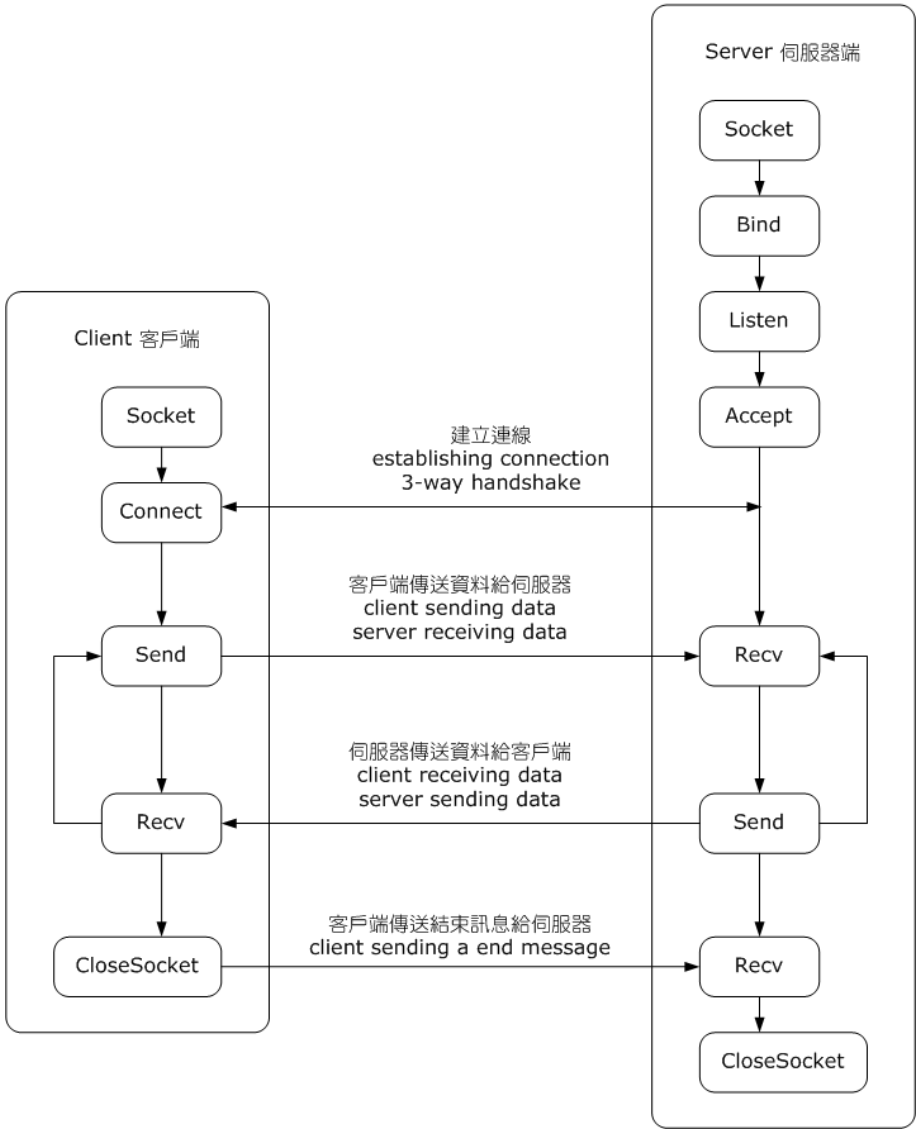


Figura 6-36. El encabezado TCP.

TCP Socket 基本流程圖
TCP Socket flow diagram



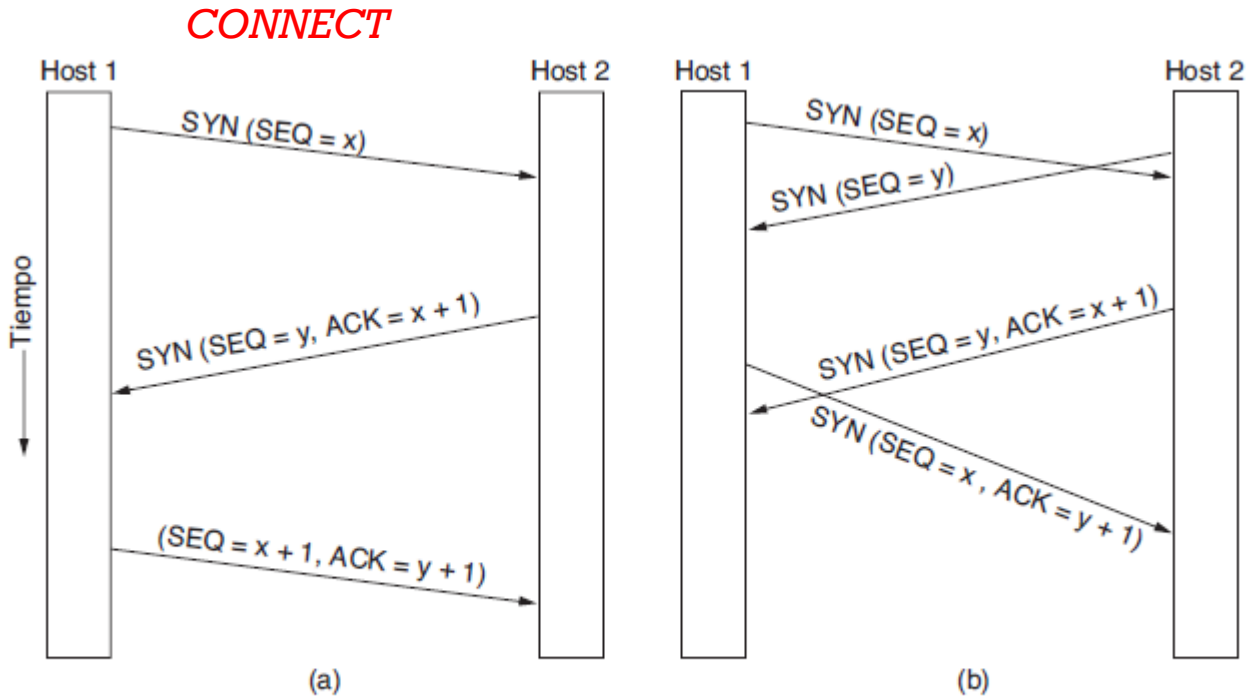


Figura 6-37. (a) Establecimiento de una conexión TCP en el caso normal. (b) Establecimiento de una conexión simultánea en ambos lados.

PRÓXIMA CLASES - COMPETENCIAS

- Describir TCP (**Jueves**)
- Aplicar la clase Multicastsocket en Java. (**Viernes – No hay clase**)
- Aplicar la API de Java la resolución de problemas con UDP Streaming. (**Viernes – No hay clase**)

REFERENCIAS

1. https://www.google.com.co/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwju5o62x-vdAhXjtlkKHaouDcAQjRx6BAgBEAU&url=http%3A%2F%2Feltallerdelbit.com%2Fdireccionamiento-ip%2F&psig=AOvVaw3E_T5IpV-ANtL0eEQbHtkg&ust=1538700259199893
2. https://www.cisco.com/c/dam/en/us/support/docs/ip/dynamic-address-allocation-resolution/19580-dhcp-multintwk-4.gif
3. https://en.wikipedia.org/wiki/Berkeley_sockets#/media/File:InternetSocketBasicDiagram_zhtw.png
4. https://buildingautomationmonthly.com/what-is-the-tcp-ip-stack/