
Internet

Jorge Juan Chico <jjchico@dte.us.es>, Julián Viejo Cortés <julian@dte.us.es> 2011-19
Departamento de Tecnología Electrónica
Universidad de Sevilla

Usted es libre de copiar, distribuir y comunicar públicamente la obra y de hacer obras derivadas siempre que se cite la fuente y se respeten las condiciones de la licencia Attribution-Share alike de Creative Commons. Puede consultar el texto completo de la licencia en <http://creativecommons.org/licenses/by-sa/3.0/>

Objetivos

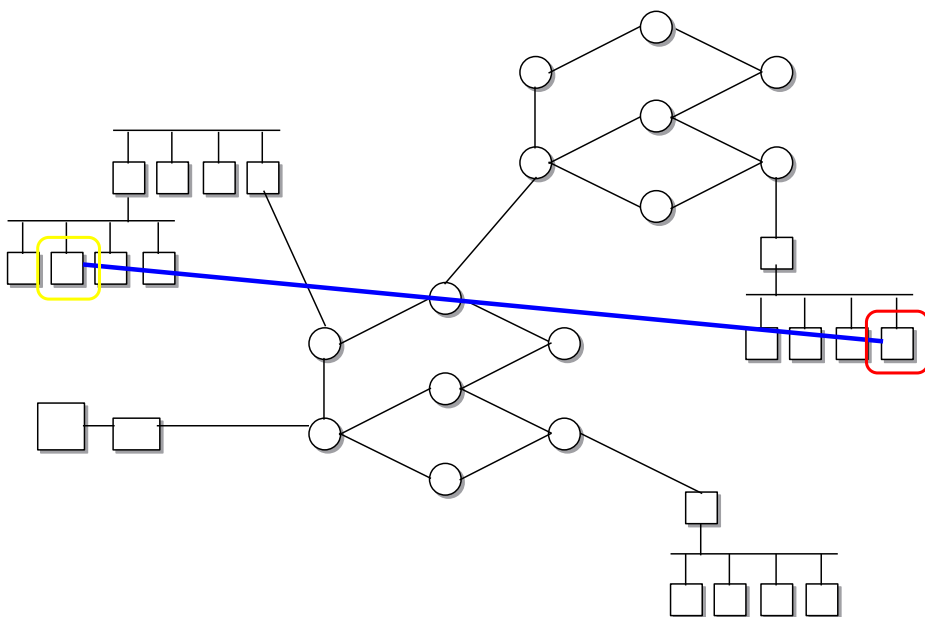
- Comprender el funcionamiento de Internet y los protocolos que la hacen funcionar
- Valorar la estrategia de dividir un problema general en problemas más simples
- Conocer los parámetros de configuración de un ordenador conectado a Internet
- Tomar conciencia de la dimensión técnica y social de Internet

Contenidos

- Estructura y objetivo
- Protocolo IP
- Protocolo TCP
- Otros protocolos de Internet
- Servicio de nombres de dominio (DNS)
- Elementos de configuración

3

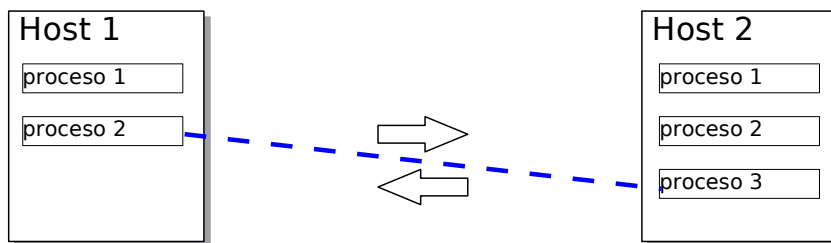
Internet. Estructura



4

Internet. Objetivo

- Red universal para la interconexión de ordenadores y equipos:
 - trabajo remoto, acceso a datos, comunicación (e-mail), etc.
- Limitaciones de las redes locales:
 - extensión limitada
 - multitud de tipos: heterogeneidad
- Aprovechamiento de redes existentes
- Objetivo técnico: proporcionar un mecanismo para establecer conexiones "virtuales" entre ordenadores conectados a la red.



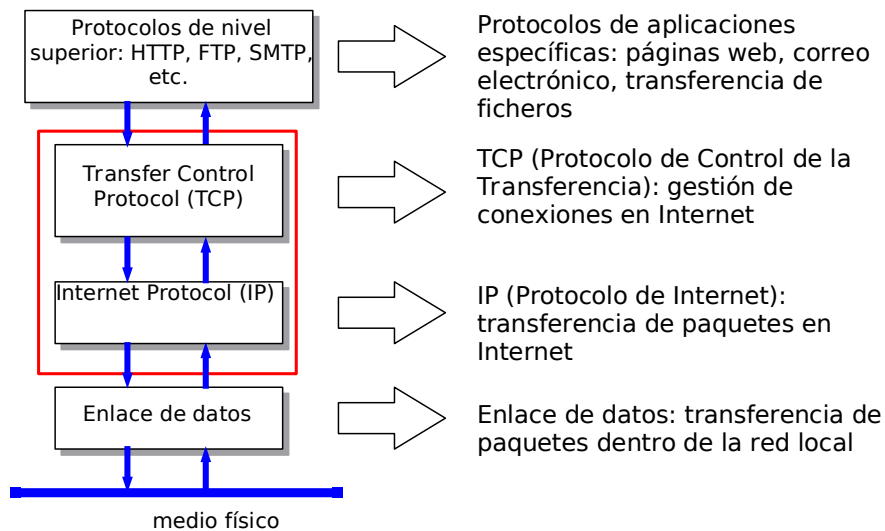
5

Internet. Conceptos

- **internet:** red formada por la interconexión de distintos tipos de redes físicas y que emplea en su conjunto una tecnología común para la transferencia de información conocida como "protocolos de internet".
- **La Internet:** internet de ámbito global que interconecta los ordenadores de multitud de organismos, empresas y particulares a lo largo de todo el mundo.
- **Host:** ordenador o dispositivo conectado a la internet
- **Interfaz de red:** elemento de conexión a una red o enlace físicos (ethernet, modem, etc.)

6

Internet: protocolos TCP/IP



7

Protocolo IP. Generalidades

- Cada paquete lleva una cabecera con la dirección de destino y de origen
- Cada paquete se trata de forma independiente
- Puede haber fragmentación y reensamblado para adaptar el tamaño del paquete a la red física
- Técnica del mejor esfuerzo:
 - No se confirma la llegada de los paquetes
 - No se asegura la llegada de los paquetes a su destino

8

Protocolo IP. Paquete IP

4	4	8	16
vers	HLEN	TOS	longitud
ident		flags	offset (13)
TTL	protocolo	checksum	
origen			
destino			
opciones			relleno
...			
datos			
...			

vers: versión de IP (4, 6, etc.)

HLEN: tamaño de la cabecera en bloques de 32b. Típicamente 5 = 20B

TOS (Type Of Service): tipo de paquete, prioridad, etc.

longitud: del paquete completo en bytes

ident, flags y offset: usados para fragmentación. Opcionales.

TTL (Time To Live): número máximo de "saltos". Típicamente 64

protocolo: protocolo de destino: 6=TCP, 17=UDP

checksum: código de detección de errores

origen: dirección de origen del paquete

destino: dirección de destino del paquete

opciones+relleno: no suelen usarse

datos: normalmente, un paquete de protocolo de nivel superior (TCP, UDP)

9

Protocolo IP. Direcciones IP

- Direcciones de 32 bits (4 bytes).
 - Ej: 150.214.144.12
- Parte de la dirección de un host es común a todos los hosts de la misma subred.
- Máscara de subred: 32 bits, los n primeros a "1" y el resto a "0". Los bits a "1" indican la parte de la dirección común a la subred.
- Una dirección con la parte del host todo a "0" indica la dirección de la subred.
- Una dirección con la parte del host todo a "1" indica como destino todos los hosts de la subred.

11

Direcciones IP. Ejemplo

IP:	10010110 11010110 10010000 00001100	150.214.144.12
MASK:	11111111 11111111 11111111 00000000	255.255.255.0
RED:	10010110 11010110 10010000 00000000	150.214.144.0
Broadcast:	10010110 11010110 10010000 11111111	150.214.144.255

Notación abreviada:

dirección IP / nº bits a 1 máscara

Ej: 150.214.144.12/24

12

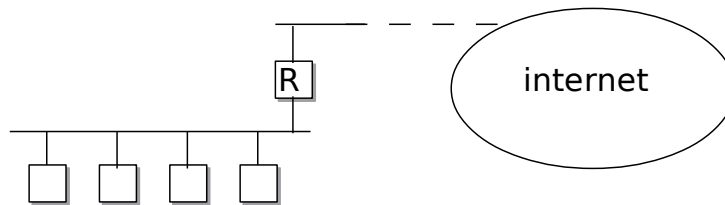
Direcciones IP privadas

- Existen rangos de direcciones IP "reservadas" que no deben ser usadas por ordenadores conectados a Internet
- Estas direcciones pueden usarse para redes IP no conectadas "directamente" a Internet: Intranets
 - 10/8: 10.0.0.0 - 10.255.255.255
 - 172.16/12: 172.16.0.0 - 172.31.255.255
 - 192.168/16: 192.168.0.0 - 192.168.255.255
- Otro rango de direcciones especial es:
 - 127/8: 127.0.0.0 - 127.255.255.255
 - está reservado para direcciones locales dentro de la misma máquina.
 - no deben circular paquetes por la red con estas direcciones.

13

Protocolo IP. Routing

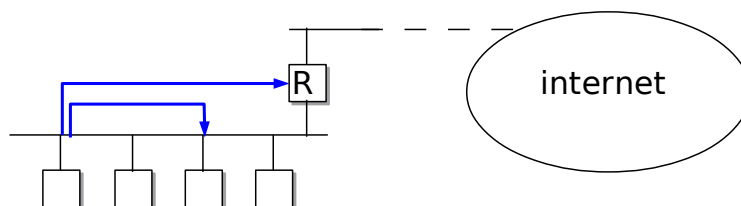
- Mecanismo para dirigir un paquete a través de los "routers" adecuados hasta alcanzar el host de destino final
 - todo datagrama (paquete) contiene una dirección IP de destino
 - la parte de red de una dirección IP identifica unívocamente una subred física que es parte de la internet
 - todas las máquinas con la misma parte de red en su dirección IP están conectadas a la misma red física y pueden intercambiar "frames" directamente
 - toda red física tiene al menos un router conectado a otra red física que puede intercambiar paquetes en ambas redes físicas



14

Protocolo IP. Routing en un host

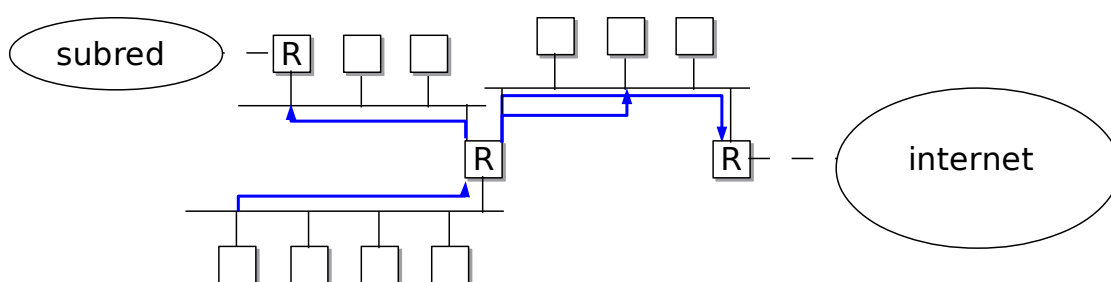
- Si la dirección IP de destino está en la misma subred (se averigua usando la máscara de subred), envía el paquete directamente al destino, mediante un "frame" con la dirección física del destino.
 - Si la dirección IP de destino no está en la misma subred, envía el paquete al router por defecto conectado al exterior (gateway), mediante un "frame" con la dirección física de la gateway.
 - Se necesita algún mecanismo para traducir direcciones IP locales en las correspondientes direcciones físicas: ARP



15

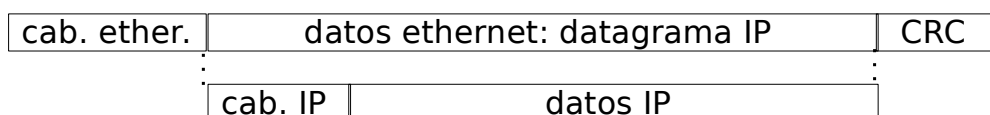
Protocolo IP. Routing en un router

- Un router dispone de varios interfaces conectados a diferentes subredes. Posee una dirección IP para cada interfaz.
 - El router recibe un datagrama IP
 - si la dirección de destino está en la misma subred que alguno de los interfaces del router, envía el paquete por ese interfaz
 - si la dirección de destino está en la tabla de rutas del router, envía el paquete por el interfaz o dirección indicado en la tabla de rutas
 - en caso contrario, envía el paquete al router por defecto (si lo hay)



16

Protocolo IP ARP (Address Resolution Protocol)



- En la red física, los paquetes IP (datagramas) se envían encapsulados en paquetes de la red física (frames)
 - La dirección física del frame debe corresponder con la del ordenador al que va destinado el datagrama IP (host, router, gateway, etc.).
 - Cada host guarda una tabla de traducción IP -> dir. física
 - Las entradas se borran cada 15min. para adaptarse a cambios en la red.
 - Si un host no conoce la dirección física correspondiente a una dirección IP, se envía un paquete especial ARP a todos los hosts de la red local (broadcast).
 - El host que posee la dirección IP requerida, responde con un paquete ARP de respuesta informando de su dirección física.
 - El host que preguntó actualiza su tabla de traducción.

17

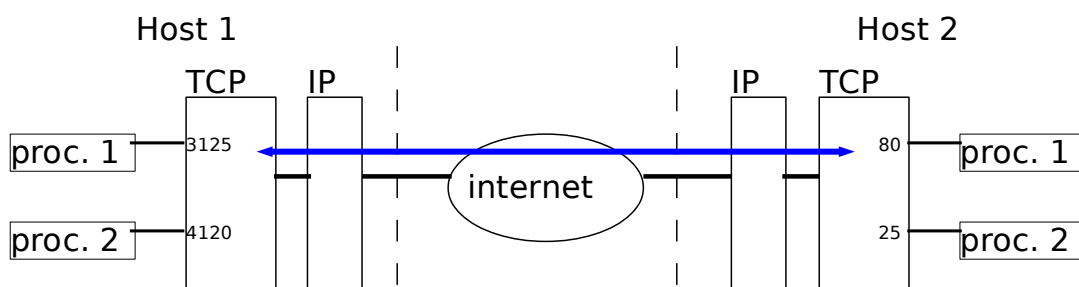
TCP. Generalidades

- Orientado a conexión: proporciona conexiones virtuales entre procesos en hosts conectados a una internet.
 - Usa paquetes TCP que se llaman "segmentos".
 - Emplea las funciones que proporciona IP para la transferencia de paquetes.
- Proporciona fiabilidad:
 - detección de errores
 - retransmisión
 - control de flujo
- Usado directamente por las aplicaciones

18

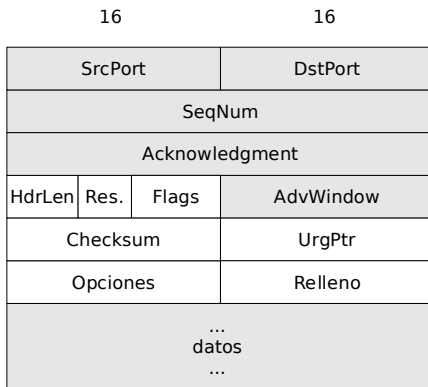
TCP. Puertos

- TCP permite múltiples conexiones a un mismo host.
- Procesos servidores "escuchan" a la espera de conexiones de clientes.
- A cada proceso servidor se asigna un número de puerto.
 - Dirección IP + puerto = localizador universal (socket) de un servicio en la red
 - Servicios con puertos "conocidos":
 - FTP(21) telnet(23) SMTP-correo e.(25) HTTP-web(80)
 - HTTPS(443) POP3(110) NetBIOS(137,138,139)



19

TCP. Paquete TCP



Flags:

- URG:** UrgPtr significativo
- ACK:** Acknowledgment significativo
- PSH:** función PUSH
- RST:** reset de conexión
- SYN:** sincronizar números de secuencia
- FIN:** fin de datos del emisor

SrcPort: puerto de origen.

DstPort: puerto de destino.

SeqNum: número de secuencia del primer byte de datos en este segmento.

Acknowledgment: número de secuencia del siguiente byte esperado.

HdrLen: longitud de la cabecera en nº de palabras de 32 bits.

Res(ervado): 6 bits a cero, reservados para usos futuros.

Flags: bits de control.

AdvWindow: nº de bytes que el emisor está dispuesto a aceptar

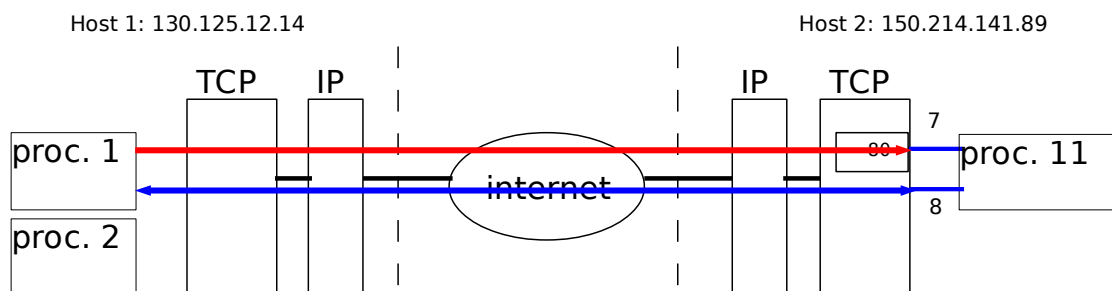
Checksum: detección de errores

UrgPtr: nº de byte donde hay datos urgentes

Opciones+Relleno: parámetros opcionales.

20

TCP. Inicio de conexión (visión del servidor)



El proceso 11 en el host 2 abre un conector (socket) con el software TCP. Recibe un número de conector (ej. 7)

El proceso 11 en el host 2 solicita al software TCP que conecte el conector 7 al puerto 80 en estado de escucha (LISTEN)

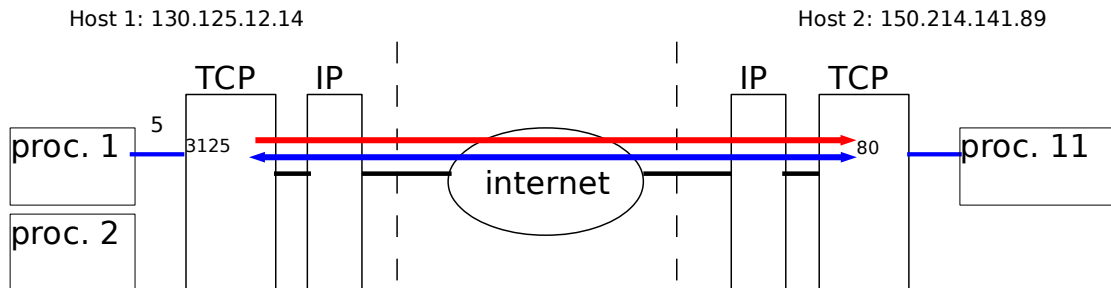
Llega una petición de conexión al puerto 80.

El proceso 11 la acepta y recibe un nuevo socket (8) con el que puede intercambiar datos con el cliente como si de un fichero se tratase.

El proceso 11 sigue escuchando en el socket 7 (puerto 80)

21

TCP. Inicio de conexión (visión del cliente)



El proceso 1 en el host 1 abre un conector (socket) con el software TCP. Recibe un número de conector (ej. 5)

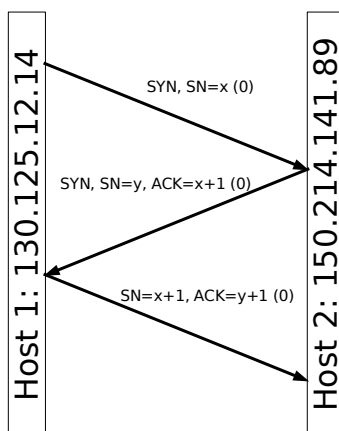
El proceso 1 en el host 1 solicita al software TCP que conecte el conector 5 al puerto 80 del host 2 (URL: 150.214.141.89:80).

El software TCP activa un número de puerto no utilizado (ej. 3125) y establece una conexión con el puerto 80 del equipo remoto.

El proceso 1 del host 1 recibe una confirmación de la conexión. Puede leer y escribir datos del conector 5 como si de un fichero de tratase.

22

TCP. Inicio de conexión (visión del protocolo)



El software TCP en H1 recibe una orden "connect" del proceso 1. Envía a H2 un paquete indicando el número de puerto y con la señal SYN.

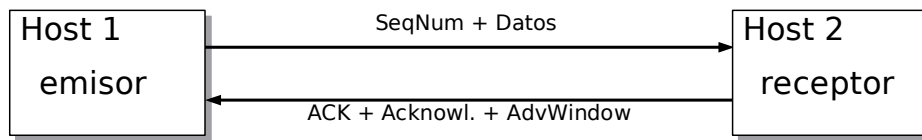
H2 recibe el paquete, comprueba que el puerto 80 está abierto. El proceso 11 acepta la conexión. Se envía a H1 un paquete con SYN+ACK para confirmar la conexión.

H1 recibe el paquete con SYN+ACK y envía un paquete con ACK para confirmar. Da la conexión por establecida e informa a P1.

H2 recibe el ACK, da la conexión por establecida.

23

TCP. Intercambio de datos



Los procesos leen y escriben datos en la conexión de forma "continua", en secuencias de bytes de longitud arbitraria. El software TCP divide los datos en segmentos que intercambia con el otro host.

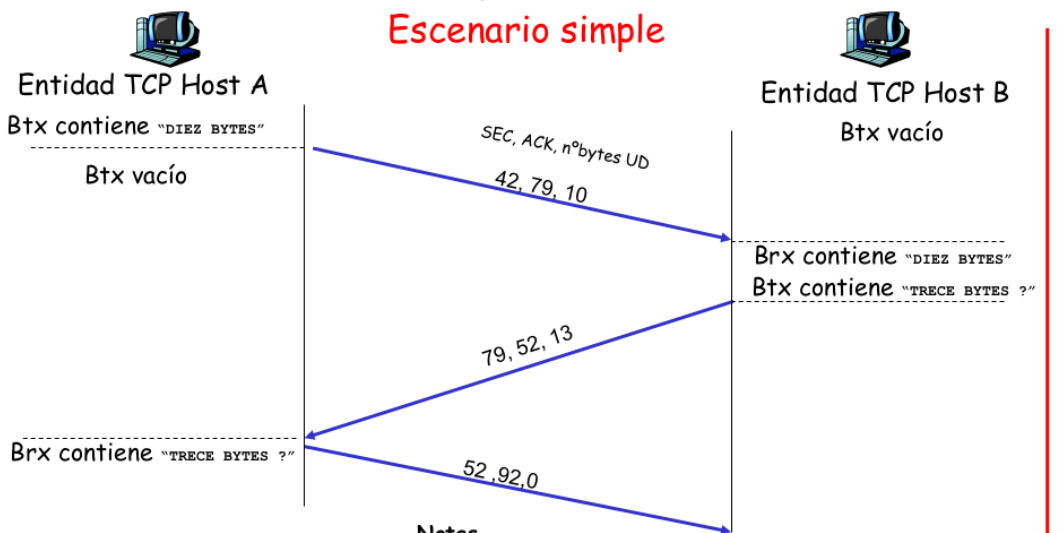
El emisor incluye en cada segmento enviado el número de orden del primer byte de datos y un conjunto de datos.

El receptor devuelve un paquete de confirmación (ACK) indicando el último byte recibido correctamente (Acknowledgement) y el número máximo de bytes que está dispuesto a recibir en el próximo paquete de datos (AdvWindow).

Ambas tareas se hacen simultáneamente: se confirma un paquete recibido y se envía nuevos datos. Si pasado un tiempo no se recibe un ACK de un paquete, éste se reenvía.

24

Nº de secuencia y de ACK en TCP(II)



Notas

- El gráfico muestra intercambio de TCP_PDU's (segmentos). El buffer de transmisión (Btx) contiene los UD solicitados por el nivel de aplicación a través del T_SAP. El buffer de recepción (Brx) se vaciará cuando a través del T_SAP lo solicite el nivel de aplicación
- TCP envía el ACK "superpuesto" en su PDU de datos ("piggybacking"), como aparece en los dos primeros segmentos que ambos host han enviado.

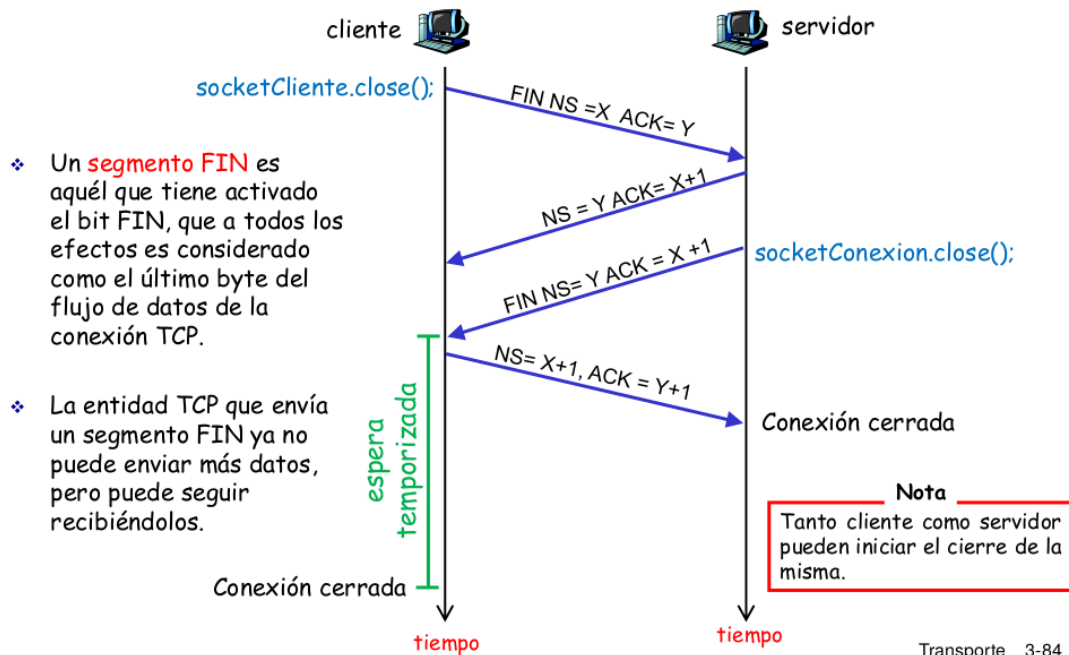
tiempo

Transporte 3-60

25

Gestión de la conexión en TCP: Cierre de la conexión

Cierre de la conexión TCP



❖ Un **segmento FIN** es aquél que tiene activado el bit FIN, que a todos los efectos es considerado como el último byte del flujo de datos de la conexión TCP.

❖ La entidad TCP que envía un segmento FIN ya no puede enviar más datos, pero puede seguir recibiendo los.

Transporte 3-84

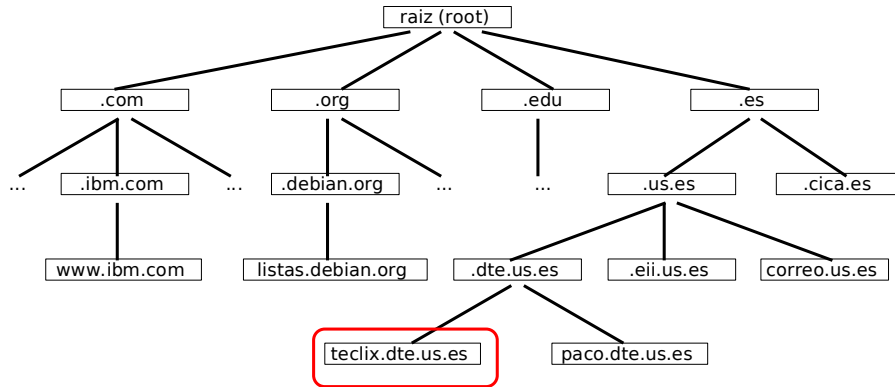
26

Optimizaciones

- Pipelining
 - Envío de múltiples paquetes antes de recibir las confirmaciones de los primeros
 - Se basa en la estimación del RTT (Round-Trip Time)
- ACK acumulados
 - Un mismo ACK confirma datos
 -
- Piggybacking
 - Envío y confirmación combinados en un mismo segmento

27

Servicio de nombres de dominio (DNS)



- Proporciona un mecanismo para identificar ordenadores conectados a Internet mediante un nombre, en vez de mediante una dirección IP.
- Los nombres se organizan gerárquicamente en dominios y subdominios.
- La organización o entidad que posee un subdominio, es libre de asignar nuevos nombre y subdominios dentro de su subdominio

28

Servicio de nombres de dominio (DNS)

- Servidor de Nombres de Dominio (DNS): máquina conectada a Internet que traduce nombres de dominio a sus direcciones IP correspondientes, y viceversa.
 - Podemos acceder a servicios en Internet usando nombres de dominio si conocemos la dirección IP de un servidor de nombres que haga la traducción de nombres a direcciones IP.
 - Cuando el software TCP/IP está configurado con un servidor de nombres, es equivalente emplear el nombre de una máquina o su dirección IP. El software TCP/IP traducirá automáticamente el nombre a la dirección IP correspondiente preguntando al/los servidores de nombres conocidos.
 - Ej: `http://www.dte.us.es/` <=> `http://150.214.141.89/`
 - A menudo, un servidor de nombres sólo tiene información "autorizada" sobre su propio dominio, pero es capaz de "resolver" cualquier otro nombre preguntando a otros servidores de nombres de la jerarquía.

29

Elementos de configuración TCP/IP

- Conexión física
 - red cableada, red inalámbrica (wifi), modem, etc.
- Configuración protocolos TCP/IP
 - dirección IP
 - máscara de subred
 - dirección de router por defecto (gateway, puerta de enlace, ...)
 - dirección IP de uno o más servidores de nombre (opcional)
 - nombre y dominio del ordenador (opcional)
- Servicio DHCP
 - normalmente instalado en un router o servidor dedicado
 - proporciona configuración automática de TCP/IP a los ordenadores de la red local
 - estática
 - dinámica