Nivel de transporte

Nivel de transporte - Introducción y el protocolo TCP

Profesor

Juan Ignacio Iturbe A.

Resultados de aprendizaje unidad 2

"Analizar críticamente el funcionamiento y la seguridad de los principales protocolos de los niveles de aplicación y transporte articulando problemáticas asociadas y soluciones propuestas"

Hoy

Introduciré los protocolos de nivel de transporte

Analizaremos el funcionamiento de TCP

Utilizaremos ejemplos de protocolos de nivel de aplicación

Utilizaremos simulaciones de software para revisar su funcionamiento

Introducción

- El protocolo de transporte proporciona un servicio de transferencia de datos extremo a extremo.
- Este aísla las capas superiores de los detalles de la red.

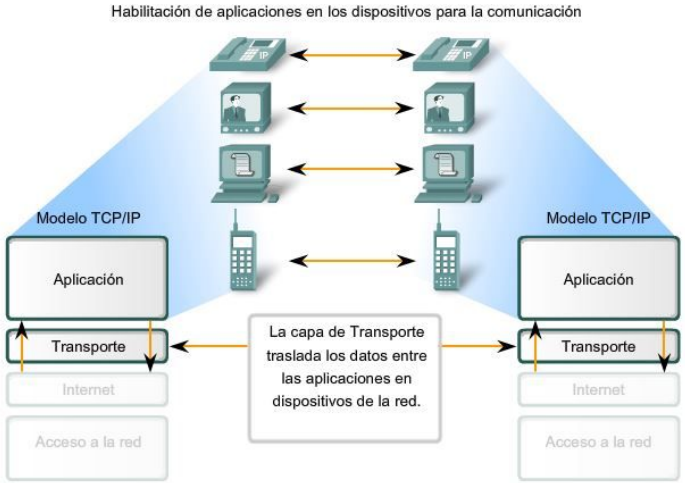


Imagen extraída de
https://sites.google.com/site/sabyrodriguezgamez/unidad2/2-2-capa-de-transporte

Introducción

- Un protocolo de transporte puede ser orientado a la conexión, o no orientado a la conexión.

Introducción

- Si el protocolo de red no es fiable (como es el caso de IP), un protocolo de transporte orientado a la conexión resulta ser muy complejo.

Introducción

- La causa básica de esta complejidad es por:
  - Retardo variables y relativamente altos que se experimentan en los sistemas finales,
  - Estos problemas complican a las técnicas:
    - Control de flujo
    - Control de errores

Nivel de transporte

Objetivo:

- Proporcionar un servicio de transferencia de datos fiable y efectivo en coste, que mantiene la calidad de servicio.

Nivel de transporte

Al desempeñar este servicio:

- Apela al nivel de red para que le proporcione una trayectoria aceptable
- Esto a través de la red o redes interconectadas que median
- Para que los dos usuarios finales puedan comunicarse.

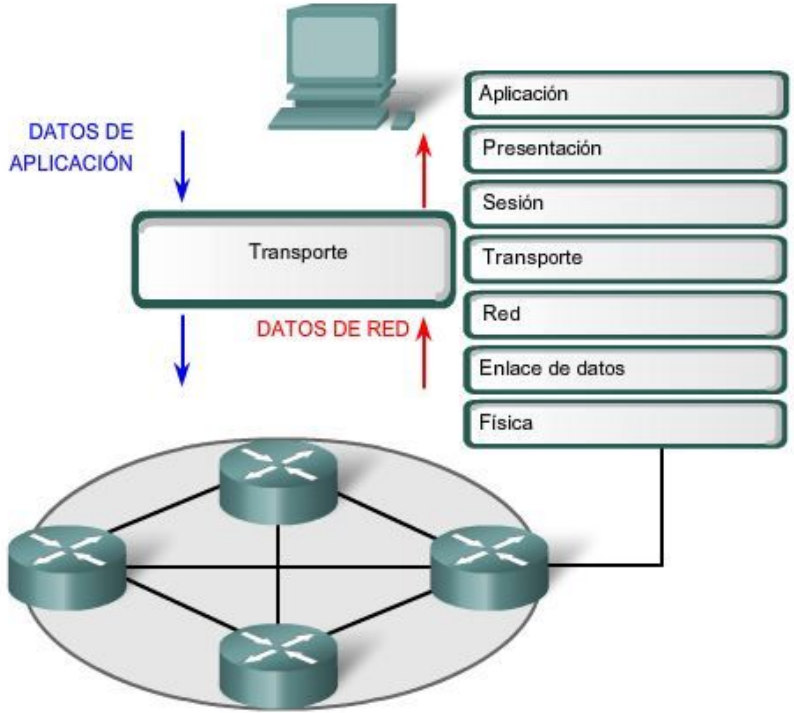


Imagen extraída de https://sites.google.com/site/sabyrodriguezgamez/unidad2/2-2-capa-de-transporte

Protocolos de Transporte

- Algunos protocolos de transporte son:
  - el estándar de OSI TP (Transport Protocol), con 5 clases definidas para este protocolo
  - UDP
  - TCP

Protocolos de Transporte

User Datagram Protocol (UDP)

- RFC 768 (link)
- No orientado a la conexión

INTERNET STANDARD

RFC 768 — J. Postel, ISI, 28 August 1980

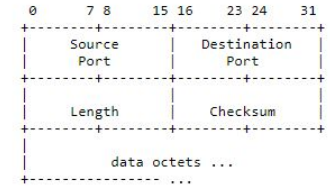
User Datagram Protocol

Introduction

This User Datagram Protocol (UDP) is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) [1] is used as the underlying protocol.

This protocol provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP) [2].

Format



User Datagram Header Format

Fields

Protocolos de Transporte

Transmission Control Protocol (TCP)

- RFC 793 (link)
- Orientado a la conexión

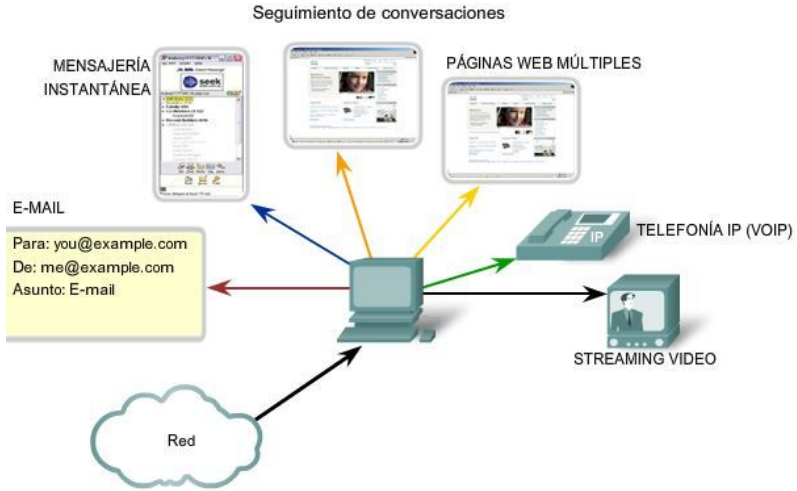


Imagen extraída de https://sites.google.com/site/sabyrodriguezgamez/unidad2/2-2-capa-de-transporte

Comparación de segmentos TCP y UDP

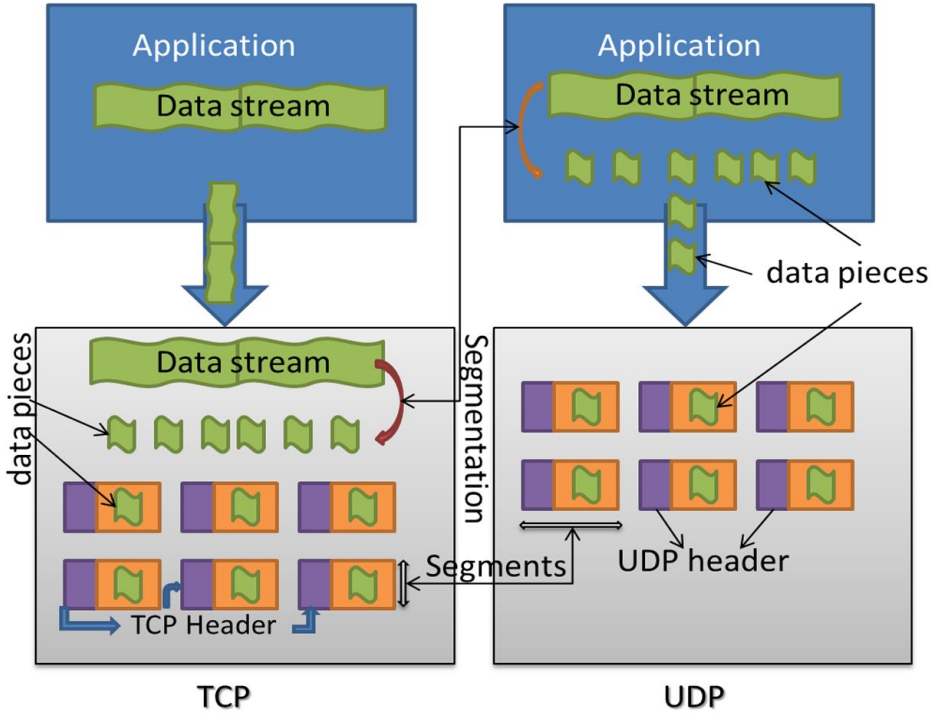
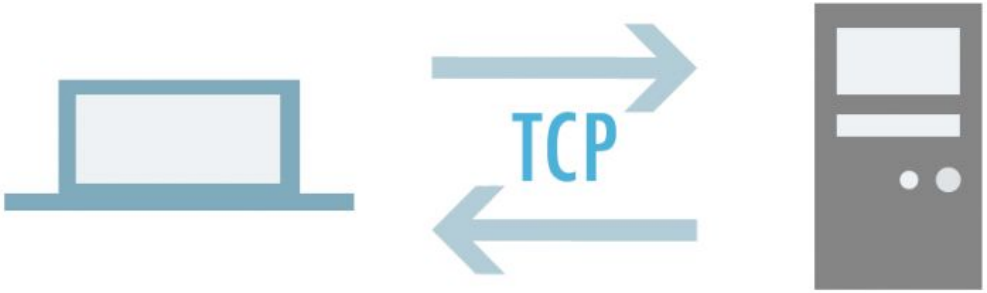


Figura tomada de https://www.computernetworkingnotes.com/ccna-study-guide/segmentation-explained-with-tcp-and-udp-header.html

Transport Control Protocol (TCP)

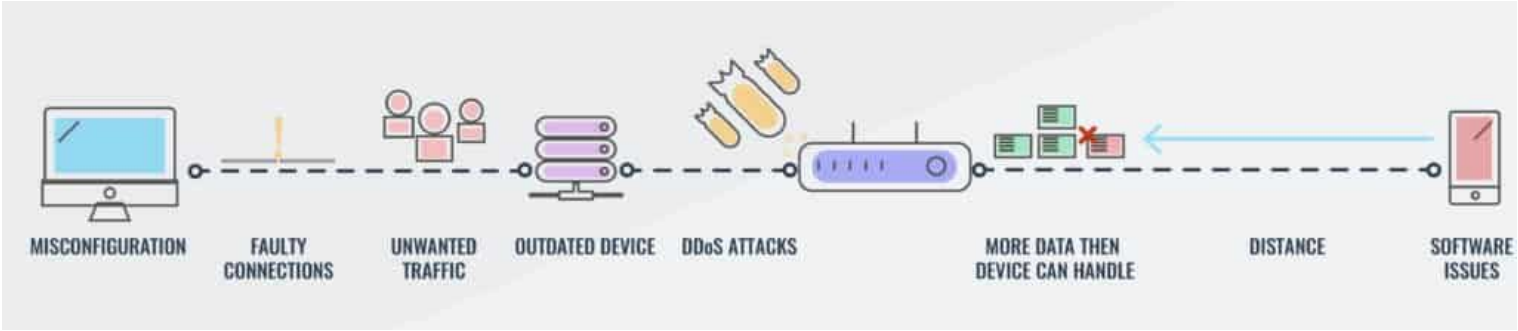


TCP

- El propósito de TCP es proporcionar
  - un servicio de transferencia de datos entre dos usuarios
  - orientado a conexiones
  - que entregue datos de manera confiable y en orden secuencial

TCP

- TCP está diseñado para usarse
  - con redes de conmutación de paquetes o
  - conjuntos interconectados de dichas redes,
- En un ámbito donde las redes mismas no pueden tomarse en cuenta para la entrega confiable y ordenada de datos



TCP

- TCP emplea una técnica de control de flujo basada en créditos.
- Donde se separa las confirmaciones y la gestión del tamaño de la ventana deslizante.

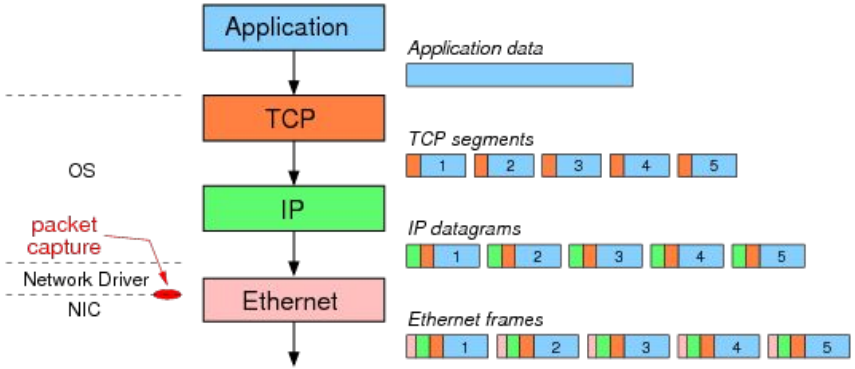
TCP

- Transporte fiable extremo a extremo
- Multiplexión, manejo de conexiones, transporte de datos, capacidades especiales, y reporte de errores

```
TCP    127.0.0.1:57820        0.0.0.0:0              LISTENING
TCP    127.0.0.1:57820        127.0.0.1:1054         ESTABLISHED
TCP    127.0.0.1:65001        0.0.0.0:0              LISTENING
TCP    127.0.0.1:65001        127.0.0.1:49707        ESTABLISHED
TCP    127.94.0.1:946         0.0.0.0:0              LISTENING
TCP    127.94.0.2:946         0.0.0.0:0              LISTENING
TCP    172.27.237.213:139     0.0.0.0:0              LISTENING
TCP    172.27.237.213:16882   158.170.53.78:1521     ESTABLISHED
TCP    172.27.237.213:20313   158.170.53.248:1521    ESTABLISHED
TCP    192.168.18.55:139      0.0.0.0:0              LISTENING
TCP    192.168.18.55:1024     cb-in-f95:https        ESTABLISHED
TCP    192.168.18.55:1025     ce-in-f94:https        TIME_WAIT
TCP    192.168.18.55:1026     ec2-52-2-103-152:https  ESTABLISHED
TCP    192.168.18.55:1027     server-13-227-205-153:https  ESTABLISHED
```

TCP

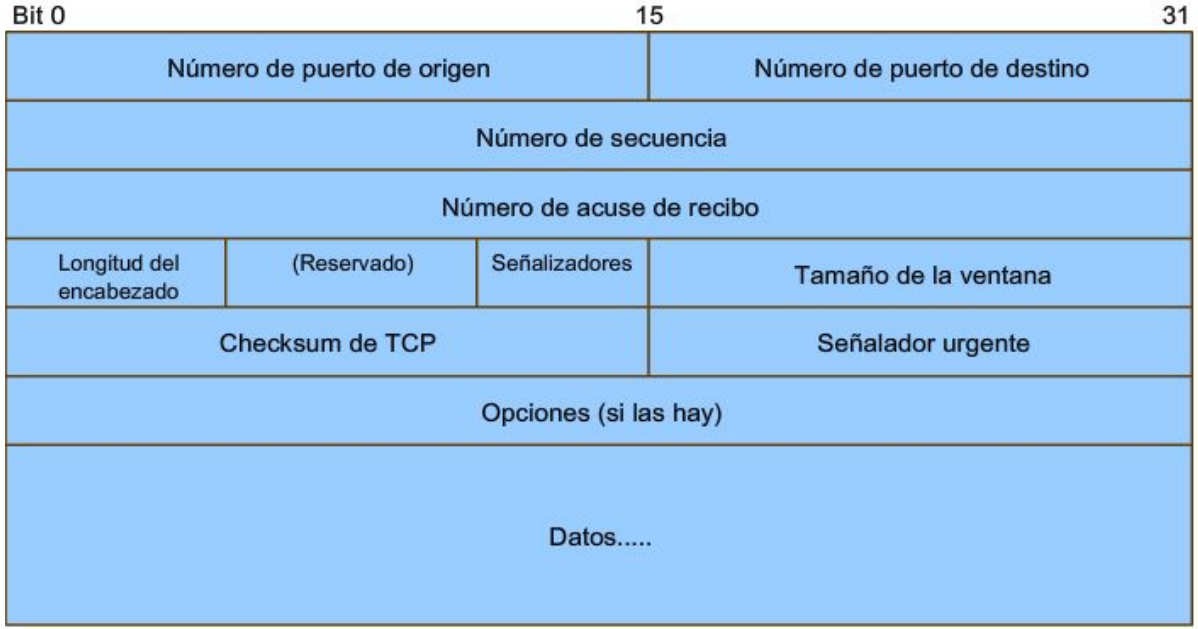
- Datos de salida son lógicamente un *stream* de bytes de usuario
- El Stream se parte en bloques de datos, o segmentos
- TCP acumula bytes de usuario hasta que el segmento es lo suficientemente grande, o los datos están marcados con una bandera de EMPUJAR (flag PUSH)



TCP

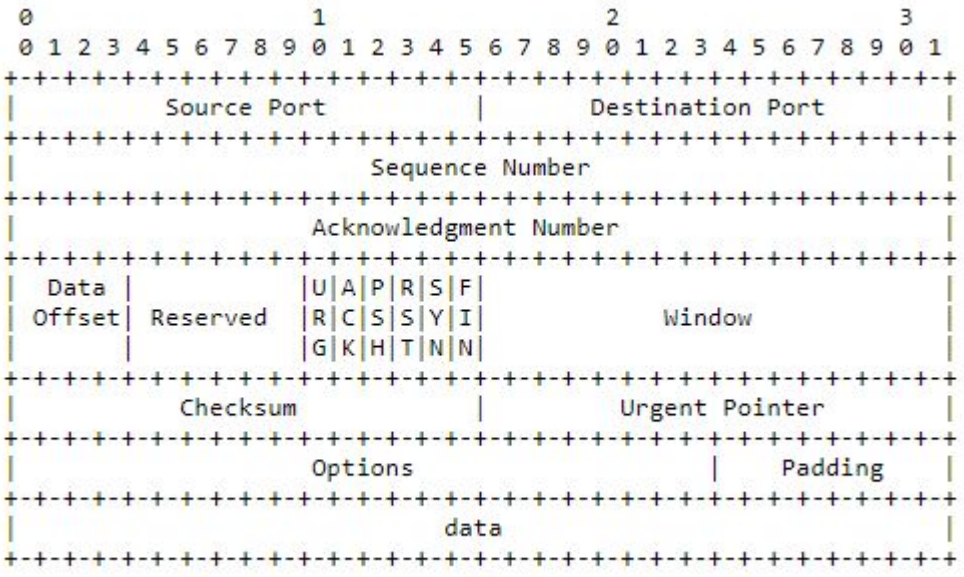
- Similarmente, datos de entrada son un stream de bytes presentados al usuario
- Datos marcados con PUSH activan el envío de datos al usuario, sino TCP decide cuándo enviar datos
- Datos marcados con URGENTE (flag URG) hacen que el usuario sea notificado

Cabecera TCP



Los campos del encabezado de TCP habilitan TCP para suministrar comunicaciones de datos confiables orientados a la comunicación.

Cabecera TCP



TCP Header Format

Quedamos aquí…

Puertos TCP

Números de puerto

Rango de números de puerto	Grupo de puertos
De 0 a 1023	Puertos bien conocidos (Contacto)
De 1024 a 49151	Puertos registrados
De 49152 a 65535	Puertos privados y/o dinámicos

Puertos TCP registrados:
1863 MSN Messenger
8008 HTTP alternativo
8080 HTTP alternativo

Puertos TCP bien conocidos:

21	FTP
23	Telnet
25	SMTP
80	HTTP
110	POP3
194	Internet Relay Chat (IRC)
443	HTTP seguro (HTTPS)

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Números de puertos importantes

Port Number	Protocol	Transport Protocol	Port Number	Protocol	Transport Protocol
20/21	FTP	TCP	110	POP3	TCP
22	SSH	TCP	135	RPC	TCP
23	Telnet	TCP	137–139	NetBIOS	TCP and UDP
25	SMTP	TCP	143	IMAP	TCP
53	DNS	TCP and UDP	161/162	SNMP	UDP
67	DHCP	UDP	389	LDAP	TCP and UDP
69	TFTP	UDP	443	HTTPS	TCP
80	HTTP	TCP	445	SMB	TCP

Investigue: ¿Por qué son importantes?

Multiplexión y manejo de conexión TCP

- Multiplexión
  - TCP puede proveer simultáneamente servicio a múltiples procesos
  - Procesos se identifican con los puertos
- Manejo de Conexiones
  - Establecimiento, mantención, y término de conexiones
  - Establece conexiones lógicas entre sockets (dirección IP + puerto)
  - Término puede ser abrupto o confirmado

Utilice:

> netstat <opción>

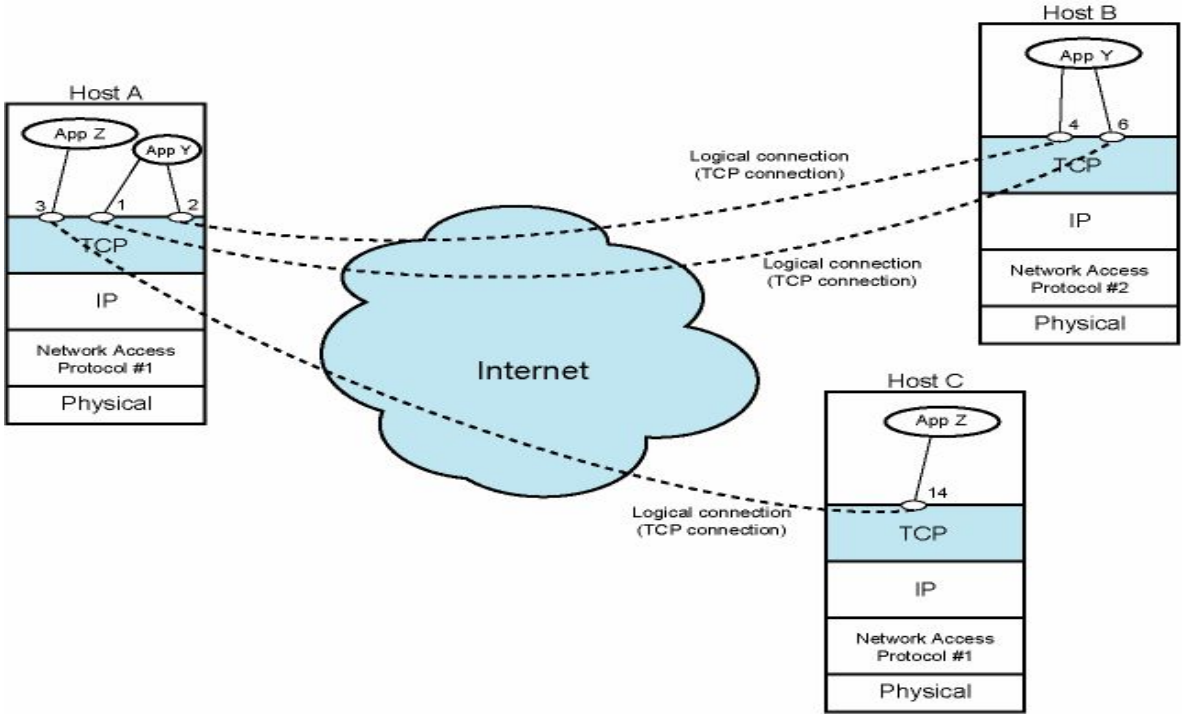
`-an:` se muestran todas las conexiones y puertos de escucha, con las direcciones y los números de puerto en forma numérica

`-b` : puede ver el ejecutable vinculado al puerto abierto

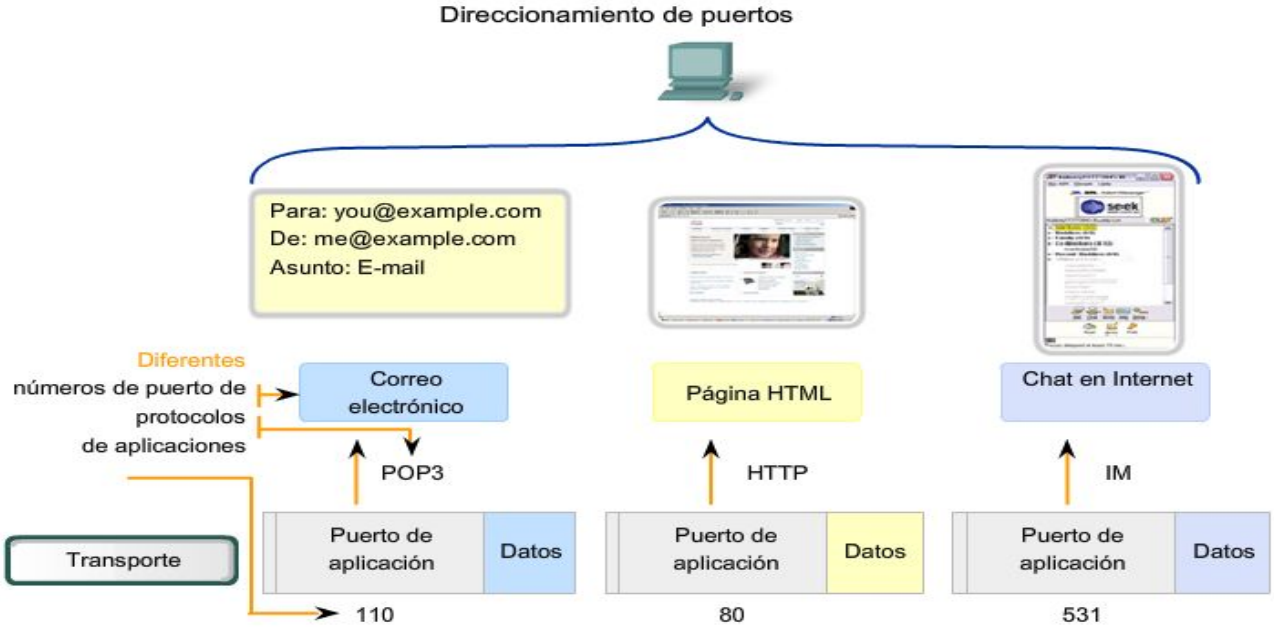
Demostración

- Cierre todo lo que usted crea que está generando tráfico de red (utilizar el comando anterior).
- Ejecute wireshark y escuche la interfaz de red a la cual usted se conecta a Internet.
  - ¿Qué procesos están generando tráfico sin que usted lo sepa?
  - ¿Hay alguno sospechoso?
  - Finalice los procesos que están generando tráfico.
- Conéctese a una página con http. Por ejemplo: http://algebra1.dmcc.usach.cl/
- Filtre la conexión en wireshark de acuerdo a la definición de socket.
- Utilice algún protocolo de capa de aplicación (consulta/respuesta) que utilice UDP. Compare el contenido de este tráfico con la conexión anterior.

Ejemplo de multiplexión

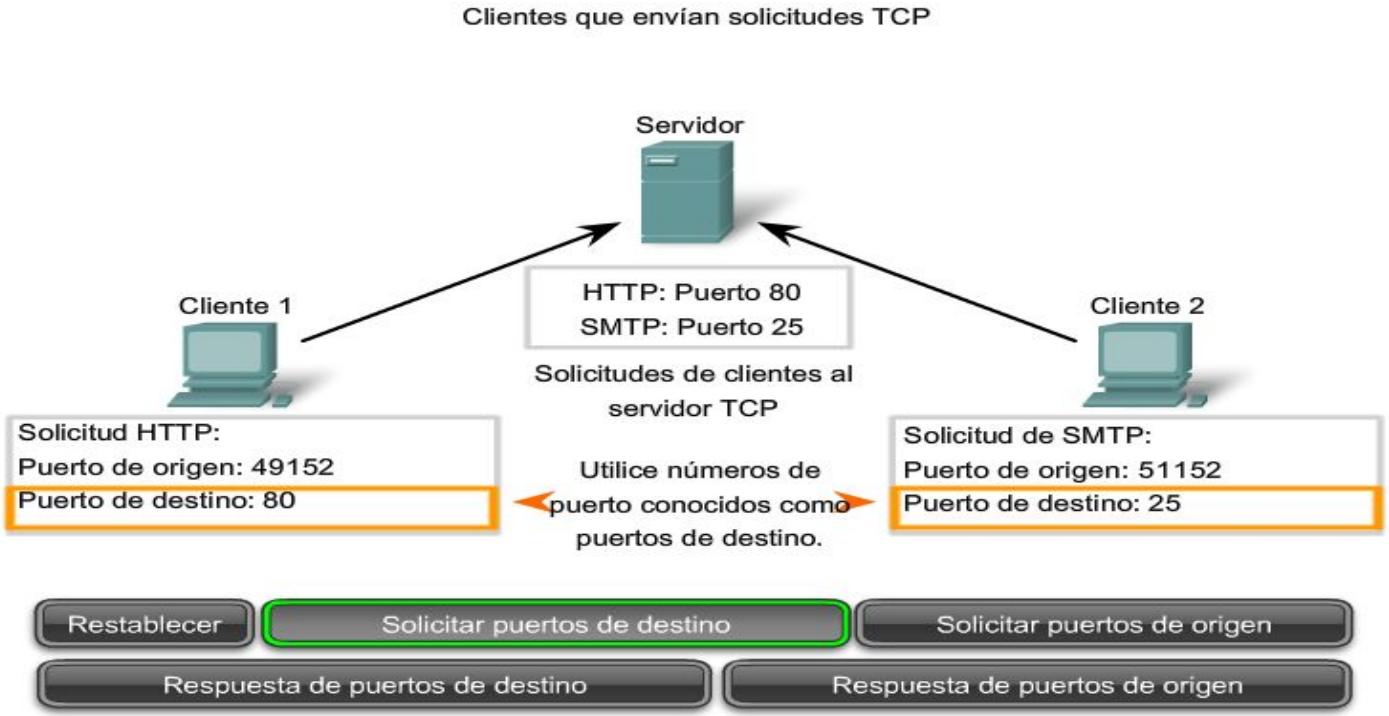


Direccionamiento de puertos

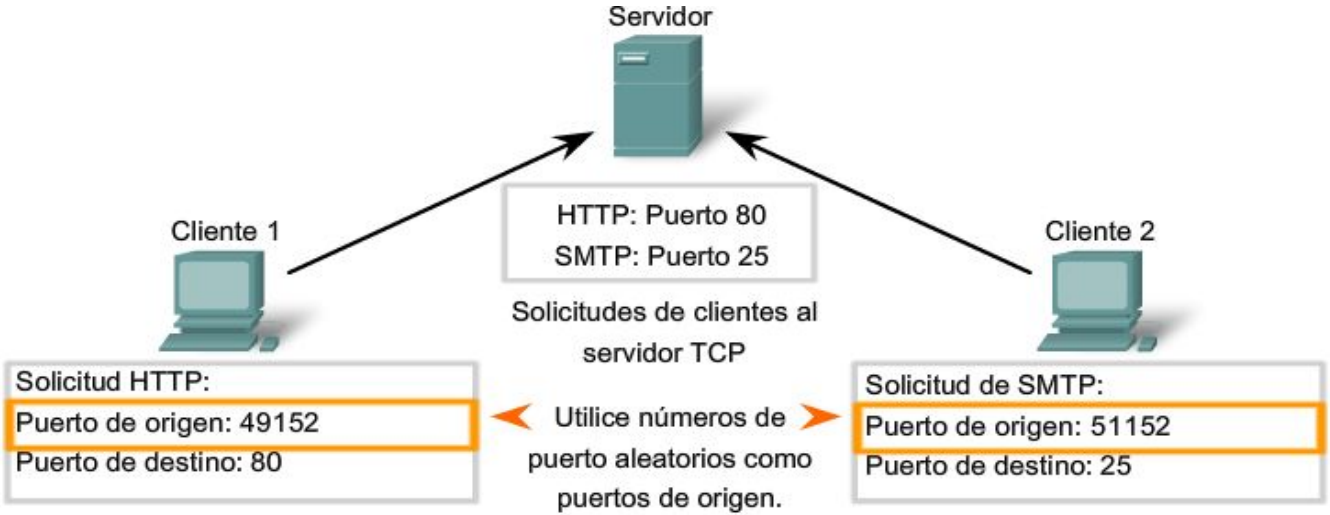


Los datos de las distintas aplicaciones se dirigen a la aplicación correcta, ya que cada aplicación tiene un número de puerto único.

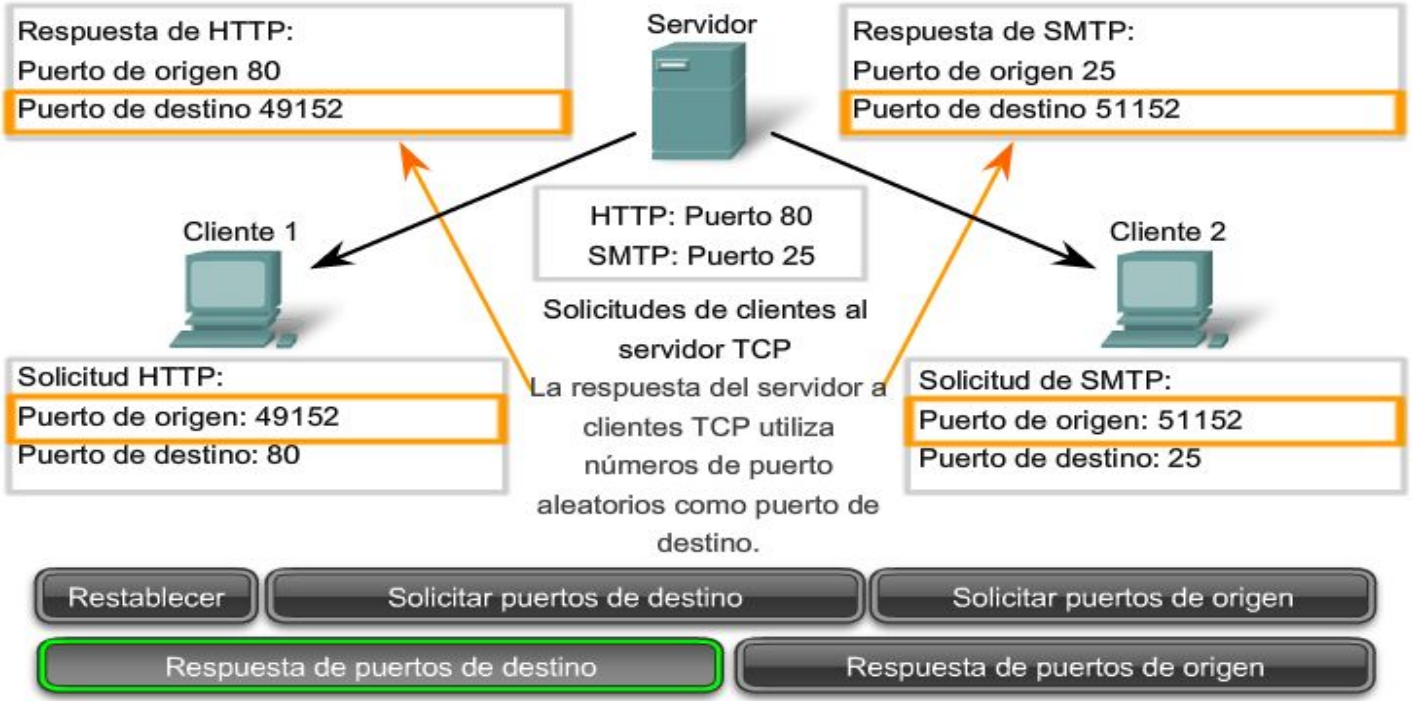
Asignación de puertos TCP



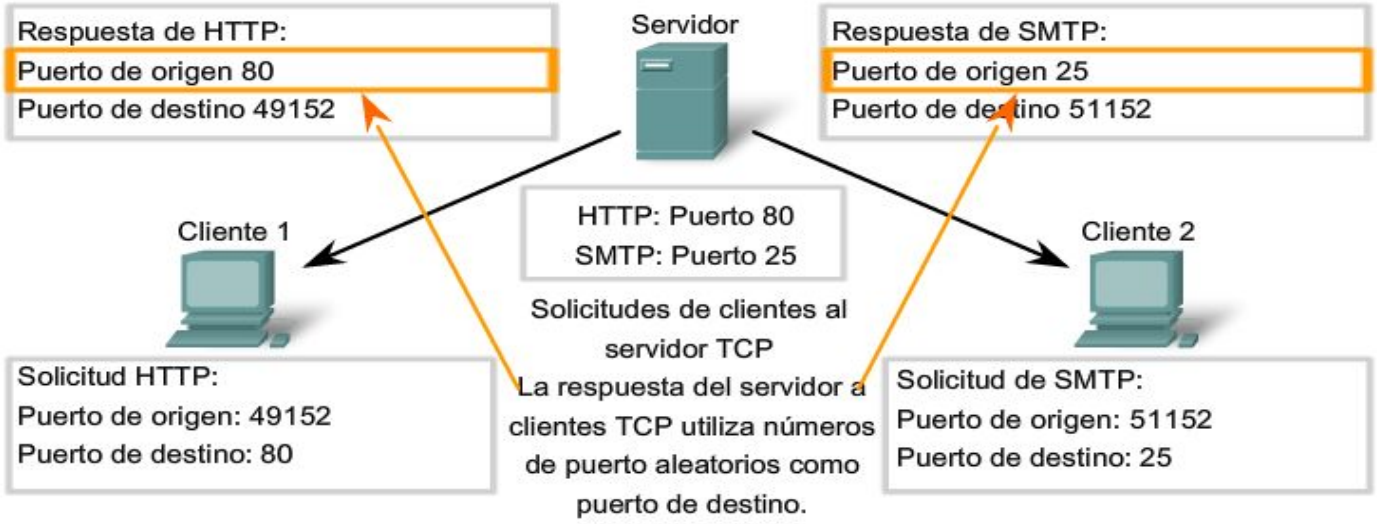
Asignación de puertos TCP



Asignación de puertos TCP



Asignación de puertos TCP



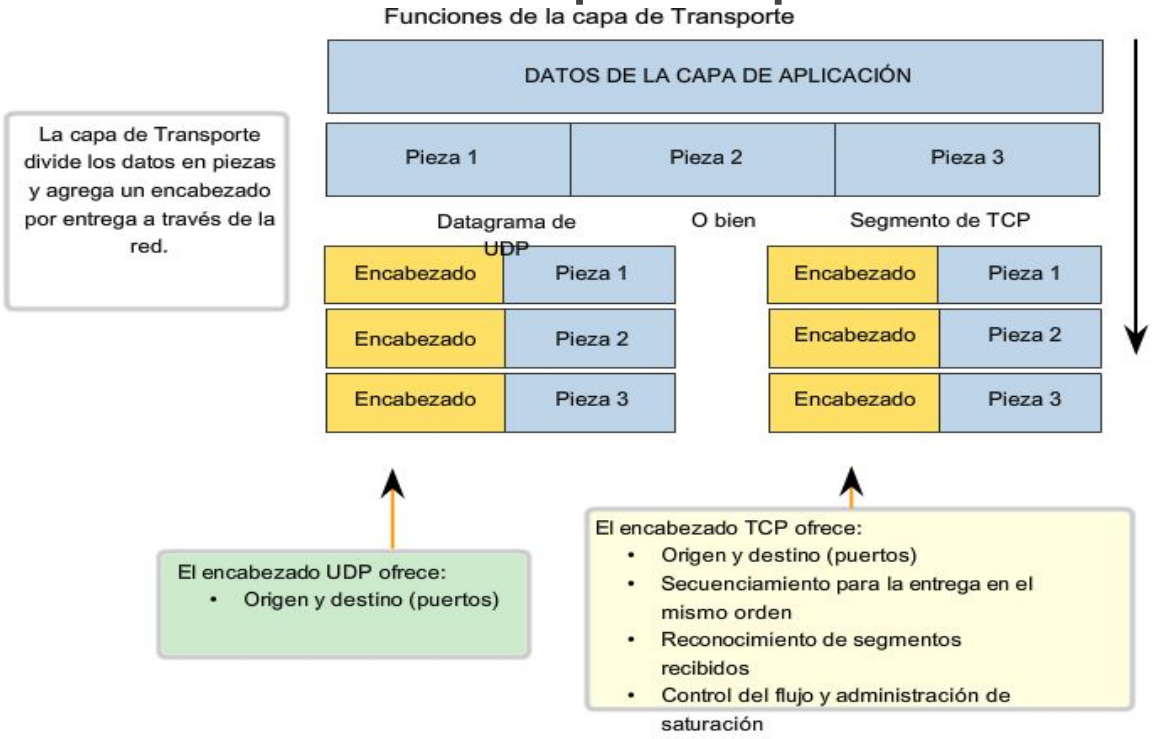
Restablecer | Solicitar puertos de destino | Solicitar puertos de origen

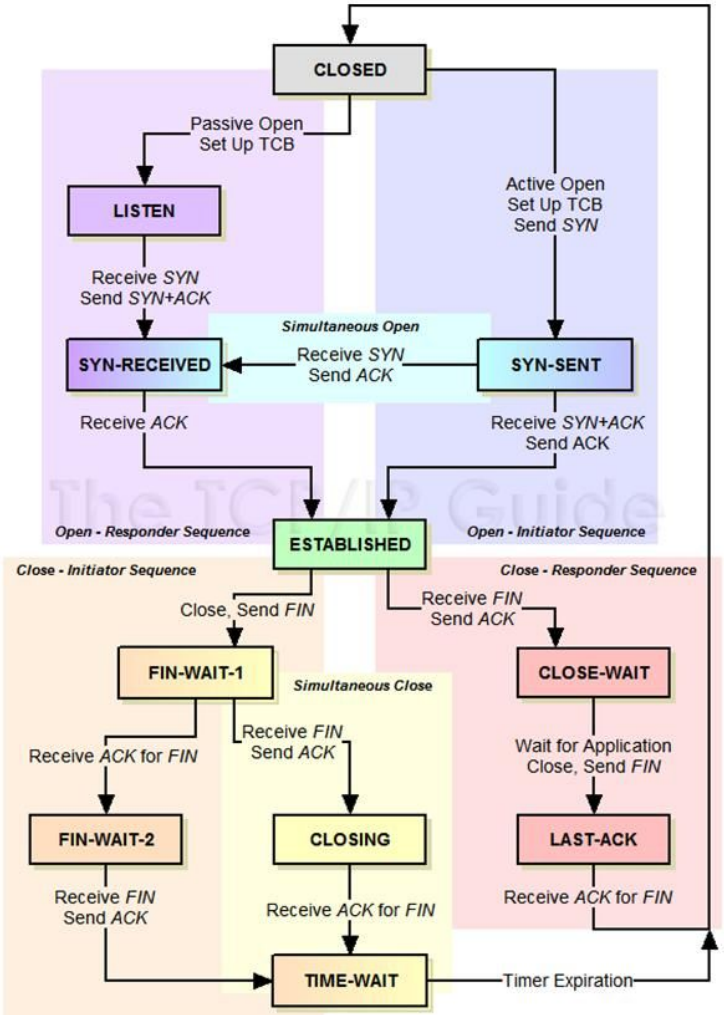
Respuesta de puertos de destino | Respuesta de puertos de origen

Segmentación

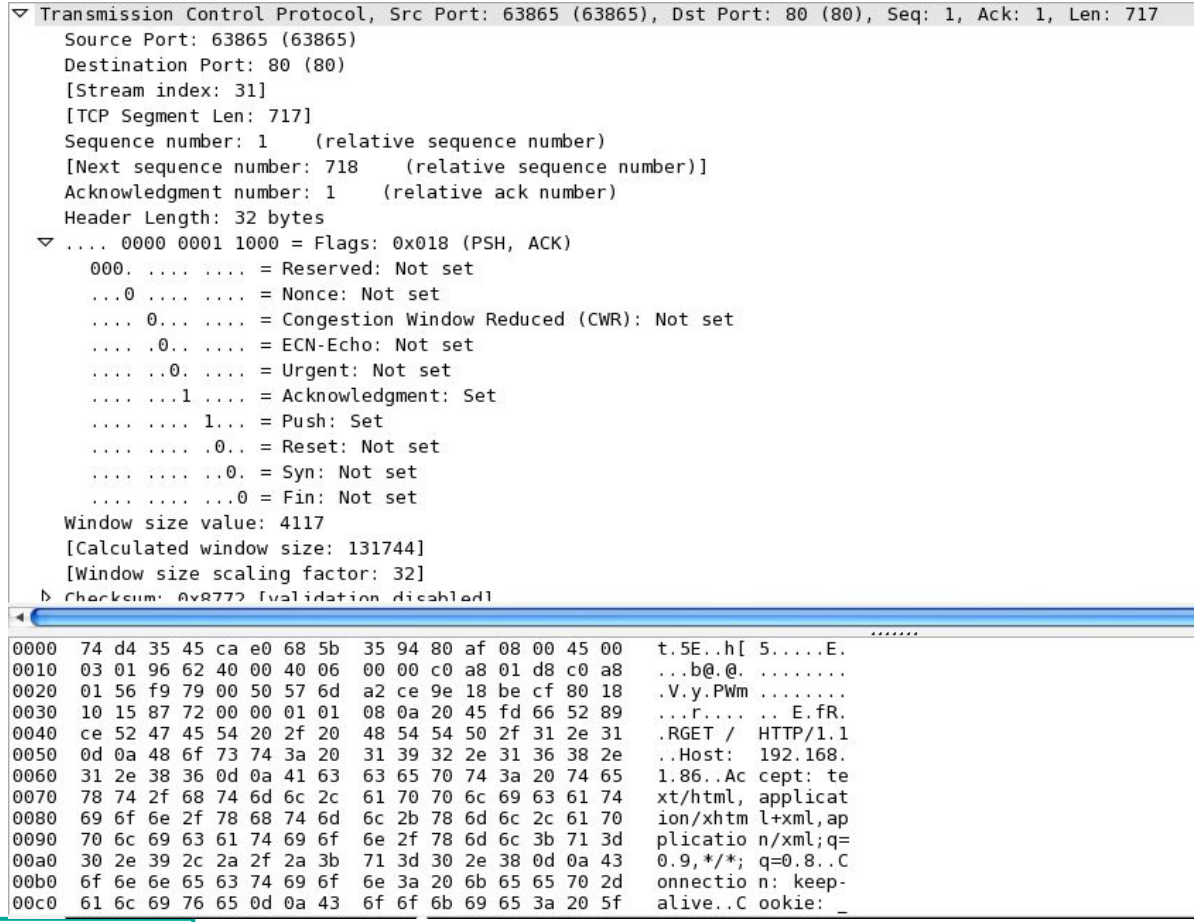
- Dividir los datos de aplicación en secciones garantiza que los datos se transmitan dentro de los límites del medio.
- Los datos de distintas aplicaciones pueden ser multiplexados en el medio.

Segmentación por protocolo




CLOSED
Passive Open
Set Up TCB
Active Open
Set Up TCB
Send SYN
LISTEN
Receive SYN
Send SYN+ACK
Simultaneous Open
SYN-RECEIVED
Receive SYN
Send ACK
SYN-SENT
Receive ACK
Receive SYN+ACK
Send ACK
Open - Responder Sequence
Open - Initiator Sequence
ESTABLISHED
Close - Initiator Sequence
Close - Responder Sequence
Close, Send FIN
Receive FIN
Send ACK
FIN-WAIT-1
Simultaneous Close
CLOSE-WAIT
Receive ACK for FIN
Receive FIN
Send ACK
Wait for Application
Close, Send FIN
FIN-WAIT-2
CLOSING
LAST-ACK
Receive FIN
Send ACK
Receive ACK for FIN
Receive ACK for FIN
TIME-WAIT
Timer Expiration

TCP en wireshark



Actividad formativa

- Observemos el comportamiento anterior en packet tracer.
  - Realizar una conexión TCP.
  - Filtrar el tráfico asociado.
  - Revisar el funcionamiento de la asignación de puertos TCP.
  - Realizar una conexión a una página HTTP y comentar cómo se produce la transferencia de una imagen, javascripts y css.
- Realice el mismo procedimiento anterior en wireshark.
- Suba evidencia de lo realizado en la actividad formativa al curso de uvirtual.

Preguntas

1. ¿Cual es el objetivo de la capa de transporte?
2. ¿Qué tipos de protocolos nos encontramos en esta capa?
3. ¿Qué dificultades enfrenta la capa de transporte?
4. Indique ejemplos de protocolos existentes en esta capa.
5. ¿Cómo se produce la multiplexación en esta capa?

Revisión de lo visto

- Se definió el objetivo de la capa de transporte.
- Se diferenció la orientación de los protocolos de este nivel.
- Se establecieron las dificultades que enfrenta la capa de transporte.
- Se indicaron ejemplos de protocolos existentes en esta capa.
- Se diferenciaron los mecanismos de segmentación entre TCP y UDP
- Se reconocieron los parámetros de la cabecera TCP
- Se estableció el funcionamiento de la asignación de puertos TCP