

Redes de Computadoras 2020

Capa 4 performance y casos de uso

Alumnos:

Losano Quintana, Juan Cruz (locxhalosano45@gmail.com)

Piñero, Tomás Santiago (tom-300@hotmail.com)

Docentes:

Natasha Tomattis (natasha.tomattis@mi.unc.edu.ar)

Ayudantes alumnos:

Aguerreberry Matthew, Sulca Sergio, Moral Ramiro, Soriano Juan

Objetivos

Análisis del comportamiento de TCP. Ejercicios de TCP. Comparación con UDP.

Requisitos

- Computadora por cada 2 personas

Consignas

TCP

1. ¿Que utilidad tiene el tamaño de ventana en la sesión tcp? ¿Cómo se calcula? Mostrar un ejemplo mediante captura de pantalla de un segmento TCP en Wireshark.

El tamaño de ventana en la sesión tcp sirve para que el transmisor pueda enviar varios paquetes antes de recibir la respuesta ACK de los mismos.

Al momento de inicio de conexión (3-way handshake) las dos partes se envían información sobre sus ventanas y se completan las opciones TCP. Entre estas opciones, se encuentra una llamada “Window scale”, que indica si el tamaño de la ventana debe multiplicarse por ese factor o no. En caso de que esté disponible, el tamaño calculado de la ventana será el valor recibido multiplicado por 2^{factor} , como lo muestra la Fig. 1.

```
Window size value: 512  
[Calculated window size: 65536]  
[Window size scaling factor: 128]
```

Fig. 1 - Cálculo del tamaño de la ventana.

Como se puede ver en la Fig. 2, el cliente (puerto 34922) tiene una ventana de recepción de 521 bytes, por lo que ese es el tamaño máximo de los paquetes que tendrá que enviar el servidor (puerto 50007).

No.	Time	Source	Destination	Protocol	Window	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	65495 34922 → 50007	[SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM...
2	0.000011980	127.0.0.1	127.0.0.1	TCP	65483 50007 → 34922	[SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=6549...
3	0.000019885	127.0.0.1	127.0.0.1	TCP	512 34922 → 50007	[ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=4248533...
4	0.051579712	127.0.0.1	127.0.0.1	TCP	512 50007 → 34922	[PSH, ACK] Seq=1 Ack=1 Win=65536 Len=2 TSval=42...
5	0.051592916	127.0.0.1	127.0.0.1	TCP	512 34922 → 50007	[ACK] Seq=1 Ack=3 Win=65536 Len=0 TSval=4248533...
6	0.051677781	127.0.0.1	127.0.0.1	TCP	512 50007 → 34922	[PSH, ACK] Seq=3 Ack=1 Win=65536 Len=2 TSval=42...
7	0.051681308	127.0.0.1	127.0.0.1	TCP	512 34922 → 50007	[ACK] Seq=1 Ack=5 Win=65536 Len=0 TSval=4248533...
8	0.051700532	127.0.0.1	127.0.0.1	TCP	512 50007 → 34922	[PSH, ACK] Seq=5 Ack=1 Win=65536 Len=2 TSval=42...
9	0.051702333	127.0.0.1	127.0.0.1	TCP	512 34922 → 50007	[ACK] Seq=1 Ack=7 Win=65536 Len=0 TSval=4248533...
10	0.051717315	127.0.0.1	127.0.0.1	TCP	512 50007 → 34922	[PSH, ACK] Seq=7 Ack=1 Win=65536 Len=2 TSval=42...
11	0.051719006	127.0.0.1	127.0.0.1	TCP	512 34922 → 50007	[ACK] Seq=1 Ack=9 Win=65536 Len=0 TSval=4248533...
12	0.051827947	127.0.0.1	127.0.0.1	TCP	512 50007 → 34922	[PSH, ACK] Seq=9 Ack=1 Win=65536 Len=2 TSval=42...
13	0.051834352	127.0.0.1	127.0.0.1	TCP	512 34922 → 50007	[ACK] Seq=1 Ack=11 Win=65536 Len=0 TSval=424853...
14	0.051870351	127.0.0.1	127.0.0.1	TCP	512 50007 → 34922	[PSH, ACK] Seq=11 Ack=1 Win=65536 Len=2 TSval=4...

▶ Frame 3: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface lo, id 0
 ▶ Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
 ▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
 ▶ Transmission Control Protocol, Src Port: 34922, Dst Port: 50007, Seq: 1, Ack: 1, Len: 0
 Source Port: 34922
 Destination Port: 50007
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 1 (relative sequence number)
 Sequence number (raw): 2536747497
 [Next sequence number: 1 (relative sequence number)]
 Acknowledgment number: 1 (relative ack number)
 Acknowledgment number (raw): 3707648876
 1000 = Header Length: 32 bytes (8)
 Flags: 0x010 (ACK)
 Window size value: 512
 [Calculated window size: 65536]
 [Window size scaling factor: 128]
 Checksum: 0xfe28 [unverified]
 [Checksum Status: Unverified]

Fig. 2 - Captura de comunicación cliente-servidor.

- ¿Es lo mismo control de flujo y control de congestión? Explique brevemente con sus palabras estos efectos en la red y cuales son los métodos para evitarlos.

No es lo mismo, son dos tipos de controles distintos. El control de flujo se utiliza para evitar que el transmisor sobrecargue al receptor con más paquetes de los que pueda procesar. El método consiste en que el receptor indica al transmisor cuál es el tamaño de su ventana continuamente durante la transmisión.

Por otro lado, el control de congestión se usa para evitar la congestión de toda la red mediante los métodos "slow-start", que comienza las transmisiones con una ventana de congestión del tamaño de un segmento (4 bytes) y la va aumentando de a uno luego de cada ACK recibido; y "multiplicative decrease", que reduce la ventana de congestión a la mitad cada vez que ocurre una pérdida.

- ¿Que significa que el tamaño de ventana sea cero?

El tamaño de ventana cero significa que el receptor tiene su buffer lleno, por lo que no puede recibir más paquetes hasta que el buffer se libere.

- Probar el script presentado en clase sobre TCP, modificarlo para poder enviar un archivo. Se pide enviar archivos de diferentes tamaños e ir variando el delay en el cliente. Si deseo enviar un archivo muy grande, se completa la transferencia? Y si usamos un archivo más pequeño?

- a. Analizar el comportamiento de la ventana en ambos casos y explicar en pocas palabras las conclusiones. Justificar con imágenes.

Conclusiones: el tamaño de la ventana es muy chico, sin importar el tiempo del cliente. El tamaño del buffer de 1024 es un pequeño para recibir mensajes (10 MB el tamaño chico). Con un buffer de 5120 y delay de 0.2 terminó 10M en 5 minutos.

No.	Time	Source	Destination	Protocol	Window	Info
16	25.279795474	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] [TCP ACKed unseen segment] 40256 → 50007 [AC...
21	53.695797339	127.0.0.1	127.0.0.1	TCP	512	[TCP Dup ACK 1#4] 50007 → 40256 [ACK] Seq=1 Ack=1 Win=512 Len...
22	53.695715618	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] [TCP ACKed unseen segment] 40256 → 50007 [AC...
23	88.444924471	127.0.0.1	127.0.0.1	TCP	512	[TCP Window Update] [TCP ACKed unseen segment] 40256 → 50007 ...
24	88.444949212	127.0.0.1	127.0.0.1	TCP	512	[TCP Previous segment not captured] 50007 → 40256 [PSH, ACK] ...
25	88.444953401	127.0.0.1	127.0.0.1	TCP	512	50007 → 40256 [PSH, ACK] Seq=29826 Ack=1 Win=512 Len=32768 TS...
26	88.444967209	127.0.0.1	127.0.0.1	TCP	279	[TCP ACKed unseen segment] 40256 → 50007 [ACK] Seq=1 Ack=2082...
27	88.487078421	127.0.0.1	127.0.0.1	TCP	263	40256 → 50007 [ACK] Seq=1 Ack=62594 Win=263 Len=0 TSval=39346...
28	88.487102678	127.0.0.1	127.0.0.1	TCP	512	50007 → 40256 [PSH, ACK] Seq=62594 Ack=1 Win=512 Len=32768 TS...
29	88.531079360	127.0.0.1	127.0.0.1	TCP	7	40256 → 50007 [ACK] Seq=1 Ack=95362 Win=7 Len=0 TSval=3934679...
30	88.759074960	127.0.0.1	127.0.0.1	TCP	512	50007 → 40256 [PSH, ACK] Seq=95362 Ack=1 Win=512 Len=896 TSva...
31	88.759102817	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40256 → 50007 [ACK] Seq=1 Ack=96258 Win=0 Le...
32	88.983104430	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40256 [ACK] Seq=96257 Ack=1 Win=512 ...
33	88.983112092	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40256 → 50007 [ACK] Seq=1 Ack=96258 Win=0 Le...
34	89.439193161	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40256 [ACK] Seq=96257 Ack=1 Win=512 ...
35	90.335440837	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40256 [ACK] Seq=96257 Ack=1 Win=512 ...
36	90.335448828	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40256 → 50007 [ACK] Seq=1 Ack=96258 Win=0 Le...
▶ Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface lo, id 0 ▶ Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00) ▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1 ▼ Transmission Control Protocol, Src Port: 40256, Dst Port: 50007, Seq: 1, Ack: 2, Len: 0 Source Port: 40256 Destination Port: 50007 [Stream index: 0] [TCP Segment Len: 0] Sequence number: 1 (relative sequence number) Sequence number (raw): 3009617521 [Next sequence number: 1 (relative sequence number)] Acknowledgment number: 2 (relative ack number) Acknowledgment number (raw): 387691531 1000 = Header Length: 32 bytes (8) Flags: 0x010 (ACK) ▶ Window size value: 0 [Calculated window size: 0] [Window size scaling factor: -1 (unknown)] Checksum: 0xfe28 [unverified] [Checksum Status: Unverified] Urgent pointer: 0						

Fig. 3 - Ejecución 1: Tiempo: 1s; buffer: 1024. En 15 min completó 692K / 1G.

No.	Time	Source	Destination	Protocol	Window	Info
699	520.697332474	127.0.0.1	127.0.0.1	TCP	512	50007 → 40328 [PSH, ACK] Seq=14337 Ack=1 Win=65536 Len=1024 T...
700	520.697333808	127.0.0.1	127.0.0.1	TCP	447	40328 → 50007 [ACK] Seq=1 Ack=15361 Win=57216 Len=0 TSval=393...
701	520.697337405	127.0.0.1	127.0.0.1	TCP	512	50007 → 40328 [PSH, ACK] Seq=15361 Ack=1 Win=65536 Len=1024 T...
702	520.697338680	127.0.0.1	127.0.0.1	TCP	443	40328 → 50007 [ACK] Seq=1 Ack=16385 Win=56704 Len=0 TSval=393...
703	520.697361285	127.0.0.1	127.0.0.1	TCP	512	50007 → 40328 [PSH, ACK] Seq=16385 Ack=1 Win=65536 Len=1024 T...
704	520.697456959	127.0.0.1	127.0.0.1	TCP	512	50007 → 40328 [PSH, ACK] Seq=17409 Ack=1 Win=65536 Len=32768 ...
705	520.707681188	127.0.0.1	127.0.0.1	TCP	306	40328 → 50007 [ACK] Seq=1 Ack=50177 Win=39168 Len=0 TSval=393...
706	520.707698178	127.0.0.1	127.0.0.1	TCP	512	50007 → 40328 [PSH, ACK] Seq=50177 Ack=1 Win=65536 Len=32768 ...
707	520.751957773	127.0.0.1	127.0.0.1	TCP	50	40328 → 50007 [ACK] Seq=1 Ack=82945 Win=6400 Len=0 TSval=3935...
708	520.963102194	127.0.0.1	127.0.0.1	TCP	512	[TCP Window Full] 50007 → 40328 [PSH, ACK] Seq=82945 Ack=1 Win=...
709	520.963113177	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40328 → 50007 [ACK] Seq=1 Ack=89345 Win=0 Le...
710	521.175257257	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40328 [ACK] Seq=89344 Ack=1 Win=6553...
711	521.175266984	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40328 → 50007 [ACK] Seq=1 Ack=89345 Win=0 Le...
712	521.599672123	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40328 [ACK] Seq=89344 Ack=1 Win=6553...
721	522.463136356	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40328 [ACK] Seq=89344 Ack=1 Win=6553...
722	522.463149754	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40328 → 50007 [ACK] Seq=1 Ack=89345 Win=0 Le...
723	524.159956547	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40328 [ACK] Seq=89344 Ack=1 Win=6553...
724	524.159964626	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40328 → 50007 [ACK] Seq=1 Ack=89345 Win=0 Le...
733	527.551431839	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40328 [ACK] Seq=89344 Ack=1 Win=6553...
734	527.551570254	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40328 → 50007 [ACK] Seq=1 Ack=89345 Win=0 Le...
735	534.463604491	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40328 [ACK] Seq=89344 Ack=1 Win=6553...
736	534.463612266	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40328 → 50007 [ACK] Seq=1 Ack=89345 Win=0 Le...
737	537.972946257	127.0.0.1	127.0.0.1	TCP	512	[TCP Window Update] 40328 → 50007 [ACK] Seq=1 Ack=89345 Win=6...
738	537.972958238	127.0.0.1	127.0.0.1	TCP	512	50007 → 40328 [PSH, ACK] Seq=89345 Ack=1 Win=65536 Len=26368 ...
739	537.972964571	127.0.0.1	127.0.0.1	TCP	512	50007 → 40328 [PSH, ACK] Seq=115713 Ack=1 Win=65536 Len=32768...
740	537.972975613	127.0.0.1	127.0.0.1	TCP	306	40328 → 50007 [ACK] Seq=1 Ack=115713 Win=39168 Len=0 TSval=39...
741	538.015741766	127.0.0.1	127.0.0.1	TCP	276	40328 → 50007 [ACK] Seq=1 Ack=148481 Win=35328 Len=0 TSval=39...
742	538.015763318	127.0.0.1	127.0.0.1	TCP	512	50007 → 40328 [PSH, ACK] Seq=148481 Ack=1 Win=65536 Len=32768...
743	538.059752599	127.0.0.1	127.0.0.1	TCP	20	40328 → 50007 [ACK] Seq=1 Ack=181249 Win=2560 Len=0 TSval=393...
744	538.270508576	127.0.0.1	127.0.0.1	TCP	512	[TCP Window Full] 50007 → 40328 [PSH, ACK] Seq=181249 Ack=1 W...
745	538.270508552	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40328 → 50007 [ACK] Seq=1 Ack=183809 Win=0 L...
746	538.490468982	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40328 [ACK] Seq=183808 Ack=1 Win=655...
747	538.490477020	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40328 → 50007 [ACK] Seq=1 Ack=183809 Win=0 L...
748	538.543337201	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40328 [ACK] Seq=183808 Ack=1 Win=655...

▶ Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface lo, id 0
 ▶ Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
 ▶ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
 ▶ Transmission Control Protocol, Src Port: 40256, Dst Port: 50007, Seq: 1, Ack: 2, Len: 0

Fig. 4 - Ejecución 2: Tiempo: 0.2s; buffer 1024, en 15 min completó 3.4M/1G.

No.	Time	Source	Destination	Protocol	Window	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	65495	40400 → 50007 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM...
2	0.000000856	127.0.0.1	127.0.0.1	TCP	65483	50007 → 40400 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=6549...
3	0.000015777	127.0.0.1	127.0.0.1	TCP	512	40400 → 50007 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3936098...
4	0.000025697	127.0.0.1	127.0.0.1	TCP	512	50007 → 40400 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=1024 TSval...
5	0.000410541	127.0.0.1	127.0.0.1	TCP	512	50007 → 40400 [PSH, ACK] Seq=1025 Ack=1 Win=65536 Len=32768 ...
6	0.004713590	127.0.0.1	127.0.0.1	TCP	504	40400 → 50007 [ACK] Seq=1 Ack=1025 Win=64512 Len=0 TSval=3936...
7	0.004724767	127.0.0.1	127.0.0.1	TCP	248	40400 → 50007 [ACK] Seq=1 Ack=33793 Win=31744 Len=0 TSval=393...
8	0.211732885	127.0.0.1	127.0.0.1	TCP	512	[TCP Window Full] 50007 → 40400 [PSH, ACK] Seq=33793 Ack=1 W...
9	0.211781408	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40400 → 50007 [ACK] Seq=1 Ack=65537 Win=0 Le...
10	0.419179809	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40400 [ACK] Seq=65536 Ack=1 Win=6553...
11	0.419204359	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40400 → 50007 [ACK] Seq=1 Ack=65537 Win=0 Le...
12	0.851257636	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40400 [ACK] Seq=65536 Ack=1 Win=6553...
13	1.683484116	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40400 [ACK] Seq=65536 Ack=1 Win=6553...
14	1.683535310	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40400 → 50007 [ACK] Seq=1 Ack=65537 Win=0 Le...
15	3.346977934	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40400 [ACK] Seq=65536 Ack=1 Win=6553...
16	3.346986226	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40400 → 50007 [ACK] Seq=1 Ack=65537 Win=0 Le...
17	6.803689750	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40400 [ACK] Seq=65536 Ack=1 Win=6553...
18	6.803705811	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40400 → 50007 [ACK] Seq=1 Ack=65537 Win=0 Le...
19	13.458810534	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40400 [ACK] Seq=65536 Ack=1 Win=6553...
20	13.458851787	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40400 → 50007 [ACK] Seq=1 Ack=65537 Win=0 Le...
21	26.771209358	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40400 [ACK] Seq=65536 Ack=1 Win=6553...
22	26.771216764	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40400 → 50007 [ACK] Seq=1 Ack=65537 Win=0 Le...
27	53.650702725	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40400 [ACK] Seq=65536 Ack=1 Win=6553...
28	53.650782444	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40400 → 50007 [ACK] Seq=1 Ack=65537 Win=0 Le...
29	62.091320742	127.0.0.1	127.0.0.1	TCP	512	[TCP Window Update] 40400 → 50007 [ACK] Seq=1 Ack=65537 Win=6...
30	62.091329205	127.0.0.1	127.0.0.1	TCP	512	50007 → 40400 [PSH, ACK] Seq=65537 Ack=1 Win=65536 Len=1024 T...
31	62.091335981	127.0.0.1	127.0.0.1	TCP	512	50007 → 40400 [PSH, ACK] Seq=65561 Ack=1 Win=65536 Len=32768 ...
32	62.091343457	127.0.0.1	127.0.0.1	TCP	504	40400 → 50007 [ACK] Seq=1 Ack=66561 Win=64512 Len=0 TSval=393...
33	62.134962504	127.0.0.1	127.0.0.1	TCP	375	40400 → 50007 [ACK] Seq=1 Ack=99329 Win=48000 Len=0 TSval=393...
34	62.134994876	127.0.0.1	127.0.0.1	TCP	512	50007 → 40400 [PSH, ACK] Seq=99329 Ack=1 Win=65536 Len=32768 ...
35	62.178741581	127.0.0.1	127.0.0.1	TCP	119	40400 → 50007 [ACK] Seq=1 Ack=132097 Win=15232 Len=0 TSval=39...
36	62.394814682	127.0.0.1	127.0.0.1	TCP	512	[TCP Window Full] 50007 → 40400 [PSH, ACK] Seq=132097 Ack=1 W...
37	62.394836355	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40400 → 50007 [ACK] Seq=1 Ack=147329 Win=0 L...
38	62.610873215	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40400 [ACK] Seq=147328 Ack=1 Win=655...

Sequence number (raw): 2726827163
 [Next sequence number: 1 (relative sequence number)]
 Acknowledgment number: 0
 Acknowledgment number (raw): 0
 1010 = Header Length: 40 bytes (10)
 ▶ Flags: 0x002 (SYN)
 Window size value: 65495

Fig. 5 - Ejecución 3: Tiempo: 1s; buffer 1024. No completó los 10M.

No.	Time	Source	Destination	Protocol	Window	Info
4	0.000370833	127.0.0.1	127.0.0.1	TCP	512	50007 → 40404 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=1024 TSval=...
5	0.000431792	127.0.0.1	127.0.0.1	TCP	512	50007 → 40404 [PSH, ACK] Seq=1025 Ack=1 Win=65536 Len=32768 T...
6	0.009299894	127.0.0.1	127.0.0.1	TCP	504	40404 → 50007 [ACK] Seq=1 Ack=1025 Win=64512 Len=0 TSval=3936...
7	0.009221206	127.0.0.1	127.0.0.1	TCP	248	40404 → 50007 [ACK] Seq=1 Ack=33793 Win=31744 Len=0 TSval=393...
8	0.215842101	127.0.0.1	127.0.0.1	TCP	512	[TCP Window Full] 50007 → 40404 [PSH, ACK] Seq=33793 Ack=1 W...
9	0.215861590	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40404 → 50007 [ACK] Seq=1 Ack=65537 Win=0 L...
10	0.423741496	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40404 [ACK] Seq=65536 Ack=1 Win=655...
11	0.423756160	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40404 → 50007 [ACK] Seq=1 Ack=65537 Win=0 L...
13	0.851852637	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40404 [ACK] Seq=65536 Ack=1 Win=655...
21	1.684682456	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40404 [ACK] Seq=65536 Ack=1 Win=655...
22	1.684728392	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40404 → 50007 [ACK] Seq=1 Ack=65537 Win=0 L...
23	3.347915117	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40404 [ACK] Seq=65536 Ack=1 Win=655...
24	3.347955845	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40404 → 50007 [ACK] Seq=1 Ack=65537 Win=0 L...
33	6.675859320	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40404 [ACK] Seq=65536 Ack=1 Win=655...
34	6.675947901	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40404 → 50007 [ACK] Seq=1 Ack=65537 Win=0 L...
35	12.454042945	127.0.0.1	127.0.0.1	TCP	512	[TCP Window Update] 40404 → 50007 [ACK] Seq=1 Ack=65537 Win=6...
36	12.454051792	127.0.0.1	127.0.0.1	TCP	512	50007 → 40404 [PSH, ACK] Seq=65537 Ack=1 Win=65536 Len=1024 T...
37	12.454058276	127.0.0.1	127.0.0.1	TCP	512	50007 → 40404 [PSH, ACK] Seq=65561 Ack=1 Win=65536 Len=32768 ...
38	12.454065668	127.0.0.1	127.0.0.1	TCP	504	40404 → 50007 [ACK] Seq=1 Ack=66561 Win=64512 Len=0 TSval=393...
39	12.495969809	127.0.0.1	127.0.0.1	TCP	375	40404 → 50007 [ACK] Seq=1 Ack=99329 Win=48000 Len=0 TSval=393...
40	12.495982423	127.0.0.1	127.0.0.1	TCP	512	50007 → 40404 [PSH, ACK] Seq=99329 Ack=1 Win=65536 Len=32768 ...
41	12.539930081	127.0.0.1	127.0.0.1	TCP	119	40404 → 50007 [ACK] Seq=1 Ack=132097 Win=15232 Len=0 TSval=39...
42	12.755747828	127.0.0.1	127.0.0.1	TCP	512	[TCP Window Full] 50007 → 40404 [PSH, ACK] Seq=132097 Ack=1 W...
43	12.755759461	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40404 → 50007 [ACK] Seq=1 Ack=147329 Win=0 L...
44	12.972589925	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40404 [ACK] Seq=147328 Ack=1 Win=655...
45	12.972598166	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40404 → 50007 [ACK] Seq=1 Ack=147329 Win=0 L...
46	13.428266374	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40404 [ACK] Seq=147328 Ack=1 Win=655...
47	14.292775691	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40404 [ACK] Seq=147328 Ack=1 Win=655...
48	14.292782908	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40404 → 50007 [ACK] Seq=1 Ack=147329 Win=0 L...
49	16.020249745	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40404 [ACK] Seq=147328 Ack=1 Win=655...
50	16.020300152	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40404 → 50007 [ACK] Seq=1 Ack=147329 Win=0 L...
51	19.476288661	127.0.0.1	127.0.0.1	TCP	512	[TCP Keep-Alive] 50007 → 40404 [ACK] Seq=147328 Ack=1 Win=655...
52	19.476306562	127.0.0.1	127.0.0.1	TCP	0	[TCP ZeroWindow] 40404 → 50007 [ACK] Seq=1 Ack=147329 Win=0 L...

```

Sequence number (raw): 1530669969
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
Window size value: 65495

```

Fig. 6 - Ejecución 4: Tiempo 0,1; buffer 1024 No completó los 10M.

UDP

1. Adaptar el script para UDP, analizar diferentes escenarios donde el servidor tiene delay y se intenta enviar un archivo grande. Comente brevemente sus conclusiones al respecto.

```

26214400 May 14 17:50 pkg.pdf
26210304 May 14 17:55 rcv.pdf

```

Fig. 7 - Comparación entre archivo recibido y enviado.

Como se ve en la Fig. 7, al tener un delay, el archivo recibido no está completo. Esto indica que durante la transmisión del archivo se perdieron datos, lo cual era de esperarse porque UDP realiza su mejor esfuerzo para enviar los datos y no garantiza que se reciban los datos completos.

```

26214400 May 14 17:50 pkg.pdf
704512 May 14 18:48 rcv.pdf

```

Fig. 8 - Comparación entre archivo recibido y enviado con delay en el cliente.

La Fig. 8 muestra cómo se pierde más de la mitad del archivo al ponerse un delay de 0.001 segundos en la recepción del cliente, por lo que con un tiempo mayor, se perderán más datos.

2. ¿Qué campos posee una cabecera UDP? ¿Cuáles de ellos son opcionales?

0	16	31
UDP SOURCE PORT		UDP DESTINATION PORT
UDP MESSAGE LENGTH		UDP CHECKSUM

Fig. 8 - Cabecera UDP.

La cabecera UDP contiene el puerto de origen, el puerto de destino, el largo del mensaje y un checksum del mismo.

Los contenidos opcionales de la cabecera son el puerto origen y el checksum.

3. ¿El checksum en UDP aplica únicamente a la carga útil?

No, el checksum en UDP se aplica tanto a la carga útil como a la cabecera del datagrama.

4. Mencione aplicaciones o servicios que utilizan UDP. Con sus palabras explique por qué cree que utilizan UDP y no otro protocolo de capa de transporte. Ejemplificar con casos de uso de la vida diaria.

Whatsapp voice/videocalls y Skype, utilizan UDP por la velocidad de transmisión, es decir, no es necesario esperar la confirmación del paquete de voz para enviar otro, se tardaría mucho tiempo si se utilizara TCP.

Otras aplicaciones (Opcionales)

1. Capturar tráfico de un video de Youtube. ¿Cuál es el protocolo de transporte?

El protocolo que utiliza Youtube (172.217.172.110) es TCP.

16	0.257587800	172.217.172.110	192.168.31.128	TLSv1.2	64240 Application Data
18	0.278542530	172.217.172.110	192.168.31.128	TLSv1.2	64240 Application Data, Application Data
19	0.282796073	192.168.31.128	172.217.172.110	TCP	65535 34530 → 443 [ACK] Seq=1 Ack=412 Win=65535 Len=0
20	0.282972468	192.168.31.128	172.217.172.110	TLSv1.2	65535 Application Data
21	0.283189017	172.217.172.110	192.168.31.128	TCP	64240 443 → 34530 [ACK] Seq=412 Ack=40 Win=64240 Len=0
280	2.234229856	192.168.31.128	172.217.172.110	TCP	65535 34530 → 443 [ACK] Seq=40 Ack=412 Win=65535 Len=1460 [TCP segm...
281	2.234305042	192.168.31.128	172.217.172.110	TLSv1.2	65535 Application Data
282	2.234480740	172.217.172.110	192.168.31.128	TCP	64240 443 → 34530 [ACK] Seq=412 Ack=1500 Win=64240 Len=0
283	2.234497957	172.217.172.110	192.168.31.128	TCP	64240 443 → 34530 [ACK] Seq=412 Ack=1843 Win=64240 Len=0
284	2.234580227	192.168.31.128	172.217.172.110	TLSv1.2	65535 Application Data
285	2.234704971	172.217.172.110	192.168.31.128	TCP	64240 443 → 34530 [ACK] Seq=412 Ack=2362 Win=64240 Len=0
286	2.236330340	192.168.31.128	172.217.172.110	TLSv1.2	65535 Application Data
287	2.236524584	172.217.172.110	192.168.31.128	TCP	64240 443 → 34530 [ACK] Seq=412 Ack=3426 Win=64240 Len=0
288	2.236635761	192.168.31.128	172.217.172.110	TLSv1.2	65535 Application Data
289	2.236768133	172.217.172.110	192.168.31.128	TCP	64240 443 → 34530 [ACK] Seq=412 Ack=3457 Win=64240 Len=0
290	2.238069349	192.168.31.128	172.217.172.110	TLSv1.2	65535 Application Data
291	2.238251803	172.217.172.110	192.168.31.128	TCP	64240 443 → 34530 [ACK] Seq=412 Ack=3492 Win=64240 Len=0
295	2.296083348	172.217.172.110	192.168.31.128	TLSv1.2	64240 Application Data, Application Data
296	2.296652786	192.168.31.128	172.217.172.110	TLSv1.2	65535 Application Data
297	2.296847465	172.217.172.110	192.168.31.128	TCP	64240 443 → 34530 [ACK] Seq=556 Ack=3531 Win=64240 Len=0
319	2.425958055	172.217.172.110	192.168.31.128	TLSv1.2	64240 Application Data
323	2.435720926	172.217.172.110	192.168.31.128	TLSv1.2	64240 Application Data, Application Data
324	2.436027225	192.168.31.128	172.217.172.110	TCP	65535 34530 → 443 [ACK] Seq=3531 Ack=700 Win=65535 Len=0
325	2.436150271	192.168.31.128	172.217.172.110	TLSv1.2	65535 Application Data
326	2.436329955	172.217.172.110	192.168.31.128	TCP	64240 443 → 34530 [ACK] Seq=700 Ack=3570 Win=64240 Len=0
386	2.645379579	172.217.172.110	192.168.31.128	TLSv1.2	65535 Application Data
387	2.645628210	172.217.172.110	192.168.31.128	TCP	64240 443 → 34530 [ACK] Seq=700 Ack=3756 Win=64240 Len=0

2. A través de una captura del tráfico con wireshark, del streaming de una serie en Netflix se puede ver que el tráfico utiliza TCP como protocolo de transporte. (Si tienen Netflix pueden probar hacer esta captura). ¿Cómo hace Netflix para no saturar al cliente y que el video se vea fluido en cualquier dispositivo hasta con conexiones muy lentas?

Netflix IP: 52.25.243.49

383	6.640729	192.168.0.114	52.25.243.49	TLSv1.2	1777 Application Data
384	6.640870	192.168.0.114	52.25.243.49	TLSv1.2	7811 Application Data
398	6.874763	52.25.243.49	192.168.0.114	TCP	56 443 → 56714 [ACK] Seq=1 Ack=1724 Win=212 Len=0
402	6.903283	52.25.243.49	192.168.0.114	TCP	56 443 → 56714 [ACK] Seq=1 Ack=4628 Win=234 Len=0
403	6.930487	52.25.243.49	192.168.0.114	TCP	56 443 → 56714 [ACK] Seq=1 Ack=7532 Win=257 Len=0
405	6.951784	52.25.243.49	192.168.0.114	TCP	56 443 → 56714 [ACK] Seq=1 Ack=9481 Win=280 Len=0
411	7.105138	52.25.243.49	192.168.0.114	TCP	1506 443 → 56714 [ACK] Seq=1 Ack=9481 Win=280 Len=1452 [TCP segment of a reasse...
412	7.105173	192.168.0.114	52.25.243.49	TCP	54 56714 → 443 [ACK] Seq=9481 Ack=1453 Win=1024 Len=0
413	7.106410	52.25.243.49	192.168.0.114	TCP	1506 443 → 56714 [ACK] Seq=1453 Ack=9481 Win=280 Len=1452 [TCP segment of a rea...
414	7.106497	192.168.0.114	52.25.243.49	TCP	54 56714 → 443 [ACK] Seq=9481 Ack=2905 Win=1024 Len=0
415	7.108450	52.25.243.49	192.168.0.114	TCP	1506 443 → 56714 [ACK] Seq=2905 Ack=9481 Win=280 Len=1452 [TCP segment of a rea...
416	7.108451	52.25.243.49	192.168.0.114	TCP	1506 443 → 56714 [ACK] Seq=4357 Ack=9481 Win=280 Len=1452 [TCP segment of a rea...
417	7.108490	192.168.0.114	52.25.243.49	TCP	54 56714 → 443 [ACK] Seq=9481 Ack=5809 Win=1024 Len=0
418	7.111128	52.25.243.49	192.168.0.114	TCP	1506 443 → 56714 [ACK] Seq=5809 Ack=9481 Win=280 Len=1452 [TCP segment of a rea...
419	7.111129	52.25.243.49	192.168.0.114	TCP	1506 443 → 56714 [ACK] Seq=7261 Ack=9481 Win=280 Len=1452 [TCP segment of a rea...
420	7.111164	192.168.0.114	52.25.243.49	TCP	54 56714 → 443 [ACK] Seq=9481 Ack=8713 Win=1024 Len=0
421	7.111298	52.25.243.49	192.168.0.114	TCP	1506 443 → 56714 [ACK] Seq=8713 Ack=9481 Win=280 Len=1452 [TCP segment of a rea...

Lo hace mediante una API que accede a las CDNs (Content Delivery Network, Red de distribución de contenidos) cercanas al cliente. El cliente testea todas estas conexiones y se queda con la mejor (menor latencia). Este testeo se realiza en todo momento. También hacen uso de TLS para controlar la carga en la CPU y ABS (Adaptive Bitrate Streaming).

[Fuente, Página interesante](#)