

## Deber 3

Pamela Pupiales 213871

### Pregunta 1

#### Parte A

The screenshot shows a Wireshark capture of ICMP traffic and a Windows Command Prompt window. The Wireshark packet list shows five ICMP echo requests from 192.168.100.7 to 192.168.0.164. The packet details pane shows the first packet's structure: Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The Command Prompt window shows the output of the 'tracert google.com' command, which displays the path from the local host to the destination.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
2	0.000000	192.168.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
3	3.020305	192.168.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
4	7.032634	192.168.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
5	15.039469	192.168.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)

The screenshot shows a Wireshark capture of ICMP traffic. The packet list shows five ICMP echo requests from 192.168.100.7 to 192.168.0.164. The packet details pane shows the first packet's structure: Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane shows the raw data of the first packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
2	0.000000	192.168.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
3	3.020305	192.168.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
4	7.032634	192.168.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
5	15.039469	192.168.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)

Capturando desde Wi-Fi (icmp)

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
2	0.000000	192.168.0.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
3	0.020305	192.168.0.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
4	7.023634	192.168.0.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
5	15.038469	192.168.0.100.7	192.168.0.164	ICMP	94	Destination unreachable (Host unreachable)
6	237.958390	192.168.0.164	142.250.78.110	ICMP	106	Echo (ping) request id=0x0001, seq=506/64001, ttl=1 (no response found)
7	237.960677	192.168.0.100.1	192.168.0.164	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
8	237.961934	192.168.0.164	142.250.78.110	ICMP	106	Echo (ping) request id=0x0001, seq=507/64257, ttl=1 (no response found)
9	237.963724	192.168.0.100.1	192.168.0.164	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
10	237.964968	192.168.0.164	142.250.78.110	ICMP	106	Echo (ping) request id=0x0001, seq=508/64513, ttl=1 (no response found)
11	237.966689	192.168.0.100.1	192.168.0.164	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
12	240.150881	192.168.0.164	142.250.78.110	ICMP	106	Echo (ping) request id=0x0001, seq=509/64769, ttl=1 (no response found)
13	240.152124	192.168.0.100.1	192.168.0.164	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
14	240.153610	192.168.0.164	142.250.78.110	ICMP	106	Echo (ping) request id=0x0001, seq=510/65025, ttl=1 (no response found)
15	240.155359	192.168.0.100.1	192.168.0.164	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
16	240.156964	192.168.0.164	142.250.78.110	ICMP	106	Echo (ping) request id=0x0001, seq=511/65281, ttl=1 (no response found)
17	240.158432	192.168.0.100.1	192.168.0.164	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
18	242.036403	192.168.0.164	142.250.78.110	ICMP	106	Echo (ping) request id=0x0001, seq=512/2, ttl=1 (no response found)
19	242.038035	192.168.0.100.1	192.168.0.164	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
20	242.039368	192.168.0.164	142.250.78.110	ICMP	106	Echo (ping) request id=0x0001, seq=513/258, ttl=1 (no response found)

Frame 1: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF\_{E9368912-A...} Ethernet II, Src: D-LinkIn\_cb:06:08 (78:32:1b:cb:06:08), Dst: IntelCor\_bf:c7:78 (3c:58:c2:bf:c7:78) Internet Protocol Version 4, Src: 192.168.100.7, Dst: 192.168.0.164 Internet Control Message Protocol

Wi-Fi: <live capture in progress> Paquetes: 512 · Mostrado: 512 (100.0%) Perfil: Default

## Resultados del análisis completo

AnalisisTracert.xlsx

## Parte B

Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

not tis and not dns and not arp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.164	142.250.78.163	TCP	55	53263 → 443 [ACK] Seq=1 Ack=1 Win=500 Len=1 [TCP segment of a reassembled PDU]
2	0.016125	142.250.78.163	192.168.0.164	TCP	66	443 → 53263 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
3	1.209125	192.168.0.164	142.250.78.67	TCP	55	53220 → 443 [ACK] Seq=1 Ack=1 Win=511 Len=1 [TCP segment of a reassembled PDU]
4	1.305826	142.250.78.67	192.168.0.164	TCP	66	443 → 53220 [ACK] Seq=1 Ack=2 Win=1579 Len=0 SLE=1 SRE=2
5	1.618387	192.168.0.164	142.250.78.163	TCP	55	53354 → 443 [ACK] Seq=1 Ack=1 Win=500 Len=1 [TCP segment of a reassembled PDU]
6	1.630251	142.250.78.163	192.168.0.164	TCP	66	443 → 53354 [ACK] Seq=1 Ack=2 Win=421 Len=0 SLE=1 SRE=2
8	4.609640	192.168.0.164	172.217.28.106	TCP	54	53221 → 443 [FIN, ACK] Seq=1 Ack=74 Win=500 Len=0
9	4.604548	172.217.28.106	192.168.0.164	TCP	54	443 → 53221 [FIN, ACK] Seq=74 Ack=2 Win=273 Len=0
10	4.606358	192.168.0.164	172.217.28.106	TCP	54	53221 → 443 [ACK] Seq=2 Ack=75 Win=500 Len=0
12	4.723958	192.168.0.164	142.250.78.142	TCP	54	53247 → 443 [FIN, ACK] Seq=1 Ack=74 Win=100 Len=0
13	4.742956	142.250.78.142	192.168.0.164	TCP	54	443 → 53247 [FIN, ACK] Seq=74 Ack=2 Win=265 Len=0
14	4.744040	192.168.0.164	142.250.78.142	TCP	54	53247 → 443 [ACK] Seq=2 Ack=75 Win=500 Len=0
16	4.963439	192.168.0.164	142.250.78.42	TCP	54	53248 → 443 [FIN, ACK] Seq=1 Ack=74 Win=510 Len=0
17	4.978911	142.250.78.42	192.168.0.164	TCP	54	443 → 53248 [FIN, ACK] Seq=74 Ack=2 Win=276 Len=0
18	4.979246	192.168.0.164	142.250.78.42	TCP	54	53248 → 443 [ACK] Seq=2 Ack=75 Win=510 Len=0
19	5.201131	192.168.0.164	172.217.173.35	TCP	55	53344 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
20	5.275519	172.217.173.35	192.168.0.164	TCP	66	443 → 53344 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
21	5.818241	192.168.0.164	172.217.173.35	TCP	55	53336 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=0 [TCP segment of a reassembled PDU]
22	5.835849	172.217.173.35	192.168.0.164	TCP	66	443 → 53336 [ACK] Seq=1 Ack=2 Win=269 Len=0 SLE=1 SRE=2
23	6.297256	192.168.0.164	185.199.109.154	TCP	55	53291 → 443 [ACK] Seq=1 Ack=1 Win=500 Len=1 [TCP segment of a reassembled PDU]
24	6.342925	192.168.0.164	142.250.78.131	TCP	55	53231 → 443 [ACK] Seq=1 Ack=1 Win=512 Len=1 [TCP segment of a reassembled PDU]
25	6.393014	142.250.78.131	192.168.0.164	TCP	66	443 → 53231 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
26	6.414037	185.199.109.154	192.168.0.164	TCP	66	443 → 53291 [ACK] Seq=1 Ack=2 Win=332 Len=0 SLE=1 SRE=2
27	6.803452	192.168.0.164	185.199.108.133	TCP	55	53292 → 443 [ACK] Seq=1 Ack=1 Win=510 Len=1 [TCP segment of a reassembled PDU]
28	6.993681	185.199.108.133	192.168.0.164	TCP	66	443 → 53292 [ACK] Seq=1 Ack=2 Win=292 Len=0 SLE=1 SRE=2

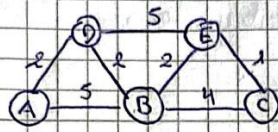
Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF\_{E9368912-A1D7-4A18-AB20-...} Ethernet II, Src: IntelCor\_bf:c7:78 (3c:58:c2:bf:c7:78), Dst: D-LinkIn\_cb:06:08 (78:32:1b:cb:06:08) Internet Protocol Version 4, Src: 192.168.0.164, Dst: 142.250.78.163 Transmission Control Protocol, Src Port: 53263, Dst Port: 443, Seq: 1, Ack: 1, Len: 1

Address Resolution Protocol: Protocol Paquetes: 10264 · Mostrado: 8230 (80.2%) · Perdido: 0 (0.0%) Perfil: Default

## Resultados del análisis completo

TCPhandshake.xlsx

## Pregunta 2



Representación en matriz de adyacencia.

	A	B	C	D	E
A	0	5	$\infty$	2	$\infty$
B	5	0	4	2	2
C	$\infty$	4	0	$\infty$	1
D	2	2	$\infty$	0	5
E	$\infty$	2	1	5	0

Tabla empujamiento (Nodo A)

Se visita el nodo A

Distancias Mínimas.

A	B	C	D	E
0	5	$\infty$	2	$\infty$

Se visita nodo D

Distancias mínimas

A	B	C	D	E
(A→D)	(A→D→B)	(A→D→E→C)		(A→D→E)
2	4	7	2	6

Se visita nodo B

Distancias mínimas

A	B	C	D	E
	(A→D→B)	(A→D→B→E→C)	(A→D→B)	(A→B→E)
2	4	7	2	6

Se visita nodo C

A	B	C	D	E
2	4	7	2	6



Se visita nodo E

A	B	C	D	E
2	4	7	2	6

Tabla enrutamiento final.

Destino	Ruta corta	Peso
B	A → D → B	4
C	A → D → B → E → C	7
D	A → D	2
E	A → D → B → E	6

Tabla enrutamiento (Nodo B)

Se visita nodo B

Distancias minimas.

A	B	C	D	E
(B → A)		(B → C)	(B → D)	(B → E)
5	0	4	2	2

Se visita el nodo E

A	B	C	D	E
5	0	4	2	2

Se visita nodo C

A	B	C	D	E
		(B → E → C)		
5	0	3	2	2

Se visita nodo A

A	B	C	D	E
(B → D → A)				
4	0	3	2	2

Tabla enrutamiento final

Destino	Ruta corta	Peso
A	B → D → A	4
C	B → E → C	3
D	B → D	2
E	B → E	2

Tabla de enrutamiento (Nodo E)				
Se visita nodo A				
A	B	C	D	E
(E → B → D → A)	2	1	4	0
6				
El proceso termina ya que evaluar lo mismo para los otros nodos queda de la misma forma				
Tabla enrutamiento final				
Destino	Ruta corta	Peso		
A	E → B → D → A	6		
B	E → B	2		
C	E → C	1		
D	E → B → D	4		

### Pregunta 3

No hay forma de determinar si un paquete llegó en el primer intento o si se perdió y se retransmitió. Hacer que el receptor responda inmediatamente y medir los tiempos transcurridos ayudaría con otras implementaciones, pero verificar que uno tenía tal implementación es difícil.

Para explicar más el tema de retransmisión TCP implementa este mecanismo para paquetes perdidos, cuando esto sucede en la red, el receptor envía una señal al remitente solicitando su retransmisión. Entonces, aunque se puedan perder algunos paquetes, TCP se encargará de solicitar y reenviarlos, lo que ocultará la pérdida de paquetes al host que intenta medir la confiabilidad del enlace.

Por otro lado, cuando se detecta congestión, TCP reduce la tasa de transmisión, lo que puede afectar la medición de la confiabilidad del enlace. Si la congestión es alta, el porcentaje de paquetes recibidos puede ser bajo, lo que no necesariamente refleja calidad

Finalmente, una vez que se establece la conexión con este protocolo, los paquetes pueden transmitirse en ambas direcciones sin interrupción. En una medición de confiabilidad del enlace, puede resultar difícil separar los paquetes enviados.

#### Pregunta 4

El problema se basa en aumentar con gradualidad el tamaño de la ventana de congestión (cwnd) con esto se aprovecha el ancho de banda y también se puede disminuir en caso que se detecte congestión en la red.

- a) El  $cwnd = 1$  y en cada ronda se envía un grupo de paquetes con tamaño igual al valor actual del  $cwnd$

$$ACK \rightarrow cwnd = cwnd + \left(\frac{1}{cwnd}\right)$$

$$\text{tiempo muerto} \rightarrow cwnd = \min\left(1, \frac{cwnd}{2}\right)$$

b)

RTT	1	2	3	4
enviado	1	2-3	4-6	7-10

Se pierde paquete 9

RTT	5	6	7	8	9
enviado	9-10	11-13	14-17	18-22	23-28

Se pierde paquete 25

RTT	10	11
enviado	25-27	28-31

Se pierde paquete 30

RTT	12	13	14
enviado	30-31	32-34	35-38

Se pierde paquete 38

RTT	15	16	17	18
enviado	38-39	40-42	43-46	47-50

Se pierde paquete 50

RTT	19
enviado	50

