

## Práctica 6

### Capa de Transporte - Parte II

1. ¿Cuál es el puerto por defecto que se utiliza en los siguientes servicios?

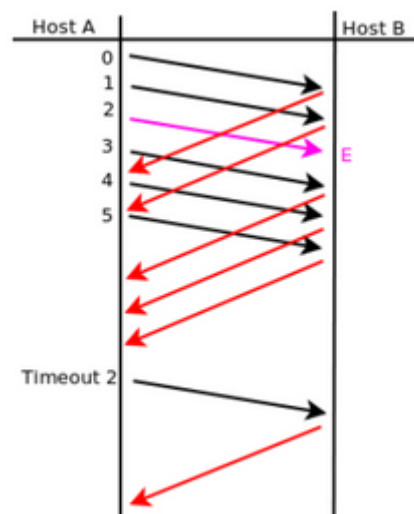
Web / SSH / DNS / Web Seguro / POP3 / IMAP / SMTP

Investigue en qué lugar en Linux y en Windows está descrita la asociación utilizada por defecto para cada servicio.

2. Investigue qué es multicast. ¿Sobre cuál de los protocolos de capa de transporte funciona? ¿Se podría adaptar para que funcione sobre el otro protocolo de capa de transporte? ¿Por qué?

3. Investigue cómo funciona el protocolo de aplicación FTP teniendo en cuenta las diferencias en su funcionamiento cuando se utiliza el modo activo de cuando se utiliza el modo pasivo ¿En qué se diferencian estos tipos de comunicaciones del resto de los protocolos de aplicación vistos?

4. Suponiendo Selective Repeat; tamaño de ventana 4 y sabiendo que E indica que el mensaje llegó con errores. Indique en el siguiente gráfico, la numeración de los ACK que el host B envía al Host A.



5. ¿Qué restricción existe sobre el tamaño de ventanas en el protocolo Selective Repeat?

6. De acuerdo a la captura TCP de la siguiente figura, indique los valores de los campos borroneados.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.20.1.1	172.20.1.100	TCP	74	41749 > vce [ ] Seq= Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=270132 TSecr=0
2	0.001264	172.20.1.100	172.20.1.1	TCP	74	vce > 41749 [SYN, ACK] Seq=1047471501 Ack=3933822138 Win=5792 Len=0 MSS=1460 SACK_PERM=1
3	0.001341			TCP	66	> [ ] Seq= Ack= Win=5888 Len=0 TSval=270132 TSecr=1877442

Internet Protocol Version 4, Src: 172.20.1.100 (172.20.1.100), Dst: 172.20.1.1 (172.20.1.1)

Transmission Control Protocol, Src Port: vce (11111), Dst Port: 41749 (41749), Seq: 1047471501, Ack: 3933822138, Len: 0

Source port: vce (11111)  
Destination port: 41749 (41749)  
[Stream index: 0]  
Sequence number: 1047471501  
Acknowledgement number: 3933822138  
Header length: 40 bytes

Flags: 0x012 (SYN, ACK)

000. .... = Reserved: Not set  
...0 .... = Nonce: Not set  
...0 .... = Congestion Window Reduced (CWR): Not set  
...0 .... = ECN-Echo: Not set  
...0 .... = Urgent: Not set  
...1 .... = Acknowledgement: Set  
...0 .... = Push: Not set  
...0 .... = Reset: Not set  
...1 .... = Syn: Set  
...0 .... = Fin: Not set  
Window size value: 5792  
[Calculated window size: 5792]  
Checksum: 0x9803 [validation disabled]

7. Dada la sesión TCP de la figura, completar los valores marcados con un signo de interrogación.

Time	10.0.0.10	10.0.1.10	Comment
1.360	(54762)	SYN → (10000)	Seq = 0
1.360	(54762)	← SYN, ACK (10000)	Seq = 0 Ack = 1
1.360	(54762)	← ACK → (10000)	Seq = ? Ack = ?
3.581	(54762)	PSH, ACK - Len: 7 → (10000)	Seq = 1 Ack = 1
3.581	(54762)	← ACK → (10000)	Seq = 1 Ack = ?
8.796	(54762)	PSH, ACK - Len: 9 → (10000)	Seq = 8 Ack = 1
8.797	(54762)	← ACK → (10000)	Seq = 1 Ack = ?
14.382	(54762)	PSH, ACK - Len: 5 → (10000)	Seq = 17 Ack = 1
14.382	(54762)	← ACK → (10000)	Seq = 1 Ack = ?
15.190	(54762)	FIN, ACK → (10000)	Seq = ? Ack = 1
15.190	(54762)	← FIN, ACK → (10000)	Seq = 1 Ack = ?
15.190	(54762)	← ACK → (10000)	Seq = ? Ack = 2

8. ¿Qué es el RTT y cómo se calcula? Investigue la opción TCP timestamp y los campos TSval y TSecr.

9. Para la captura *tcp-captura.pcap*, responder las siguientes preguntas.

- ¿Cuántos intentos de conexiones TCP hay?
- ¿Cuáles son la fuente y el destino (IP:port) para c/u?
- ¿Cuántas conexiones TCP exitosas hay en la captura? ¿Cómo diferencia las exitosas de las que no lo son? ¿Cuáles flags encuentra en cada una?
- Dada la primera conexión exitosa responder:

- i. ¿Quién inicia la conexión?
  - ii. ¿Quién es el servidor y quién el cliente?
  - iii. ¿En qué segmentos se ve el 3-way handshake?
  - iv. ¿Cuáles ISNs se intercambian?
  - v. ¿Cuál MSS se negoció?
  - vi. ¿Cuál de los dos hosts envía la mayor cantidad de datos (IP:port)?
- e. Identificar primer segmento de datos (origen, destino, tiempo, número de fila y número de secuencia TCP).
- i. ¿Cuántos datos lleva?
  - ii. ¿Cuándo es confirmado (tiempo, número de fila y número de secuencia TCP)?
  - iii. La confirmación, ¿qué cantidad de bytes confirma?
- f. ¿Quién inicia el cierre de la conexión? ¿Qué flags se utilizan? ¿En cuáles segmentos se ve (tiempo, número de fila y número de secuencia TCP)?
10. Responda las siguientes preguntas respecto del mecanismo de control de flujo.
- a. ¿Quién lo activa? ¿De qué forma lo hace?
  - b. ¿Qué problema resuelve?
  - c. ¿Cuánto tiempo dura activo y qué situación lo desactiva?
11. Responda las siguientes preguntas respecto del mecanismo de control de congestión.
- a. ¿Quién activa el mecanismo de control de congestión? ¿Cuáles son los posibles disparadores?
  - b. ¿Qué problema resuelve?
  - c. Diferencie slow start de congestion-avoidance.
12. Para la captura *udp-captura.pcap*, responder las siguientes preguntas.
- a. ¿Cuántas comunicaciones (srcIP,srcPort,dstIP,dstPort) UDP hay en la captura?
  - b. ¿Cómo se podrían identificar las exitosas de las que no lo son?
  - c. ¿UDP puede utilizar el modelo cliente/servidor?
  - d. ¿Qué servicios o aplicaciones suelen utilizar este protocolo? ¿Qué requerimientos tienen?
  - e. ¿Qué hace el protocolo UDP en relación al control de errores?
  - f. Con respecto a los puertos vistos en las capturas, ¿observa algo particular que lo diferencie de TCP?

g. Dada la primera comunicación en la cual se ven datos en ambos sentidos (identificar el primer datagrama):

- i. ¿Cuál es la dirección IP que envía el primer datagrama?, ¿desde cuál puerto?
- ii. ¿Cuántos datos se envían en un sentido y en el otro?

13. Dada la salida que se muestra en la imagen, responda los ítems debajo.

Netid	State	Local Address:Port	Peer Address:Port	
udp	UNCONN	*:68	*:*	((("dhclient",671,5))
udp	UNCONN	*:123	*:*	((("ntpd",2138,16))
udp	UNCONN	:::123	:::*	((("ntpd",2138,17))
tcp	LISTEN	*:80	*:*	((("nginx",23653,19),("nginx",23652,19))
tcp	LISTEN	*:22	*:*	((("sshd",1151,3))
tcp	LISTEN	127.0.0.1:25	*:*	((("master",11457,12))
tcp	LISTEN	*:443	*:*	((("nginx",23653,20),("nginx",23652,20))
tcp	LISTEN	*:3306	*:*	((("mysqld",4556,13))
tcp	ESTAB	127.0.0.1:3306	127.0.0.1:34338	((("mysqld",4556,14))
tcp	TIME-WAIT	10.100.25.135:443	43.226.162.110:29148	
tcp	ESTAB	127.0.0.1:48717	127.0.0.1:3306	((("ruby",28615,10))
tcp	ESTAB	127.0.0.1:3306	127.0.0.1:48717	((("mysqld",4556,17))
tcp	ESTAB	127.0.0.1:34338	127.0.0.1:3306	((("ruby",28610,9))
tcp	ESTAB	10.100.25.135:22	200.100.120.210:61576	((("sshd",13756,3),("sshd",13654,3))
tcp	LISTEN	:::22	:::*	((("sshd",1151,4))
tcp	LISTEN	:1:25	:::*	((("master",11457,13))

- Suponga que ejecuta los siguientes comandos desde un host con la IP 10.100.25.90. Responda qué devuelve la ejecución de los siguientes comandos y, en caso que corresponda, especifique los flags.
  - a. hping3 -p 3306 -udp 10.100.25.135
  - b. hping3 -S -p 25 10.100.25.135
  - c. hping3 -S -p 22 10.100.25.135
  - d. hping3 -S -p 110 10.100.25.135
- ¿Cuántas conexiones distintas hay establecidas? Justifique.