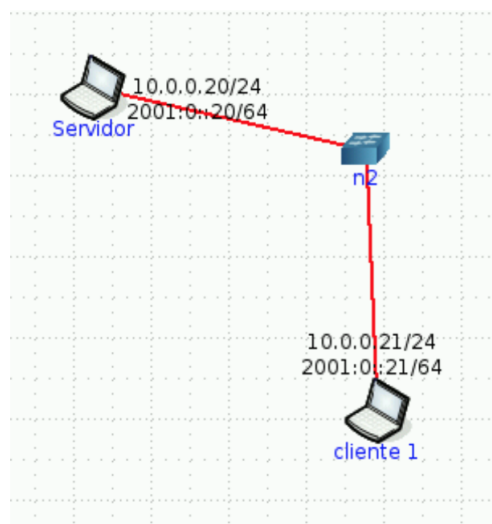


Práctica 5

Capa de Transporte - Parte I

1. ¿Cuál es la función de la capa de transporte?
2. Describa la estructura del segmento TCP y UDP.
3. ¿Cuál es el objetivo del uso de puertos en el modelo TCP/IP?
4. Compare TCP y UDP en cuanto a:
 - a. Confiabilidad.
 - b. Multiplexación.
 - c. Orientado a la conexión.
 - d. Controles de congestión.
 - e. Utilización de puertos.
 - f. ¿Cuál es el campo del datagrama IP y los valores que se utilizan en este para diferenciar que se transporta TCP o UDP? (Ayuda: buscar en /etc/protocols y contrastarlo con una captura de tráfico).
5. La PDU de la capa de transporte es el segmento. Sin embargo, en algunos contextos suele utilizarse el término datagrama. Indique cuando.
6. Describa el saludo de tres vías de TCP.
7. Investigue qué es el ISN (Initial Sequence Number). Relaciónelo con el saludo de tres vías.
8. Utilice el comando **ss** (reemplazo de netstat) para obtener la siguiente información de su PC:
 - a. Para listar las comunicaciones TCP establecidas.
 - b. Para listar las comunicaciones UDP establecidas.
 - c. Obtener sólo los servicios TCP que están esperando comunicaciones
 - d. Obtener sólo los servicios UDP que están esperando comunicaciones.
 - e. Repetir los anteriores para visualizar el proceso del sistema asociado a la conexión.
 - f. Obtenga la misma información planteada en los ítems anteriores usando el comando **netstat**.
9. ¿Qué sucede si llega un segmento TCP a un host que no tiene ningún proceso esperando en el puerto destino de dicho segmento (es decir, que dicho puerto no está en estado LISTEN)?
 - a. Utilice **hping3** para enviar paquetes TCP al puerto destino 22 de la máquina virtual con el flag SYN activado.
 - b. Utilice **hping3** para enviar paquetes TCP al puerto destino 40 de la máquina virtual con el flag SYN activado.

- c. ¿Qué diferencias nota en las respuestas obtenidas en los dos casos anteriores? ¿Puede explicar a qué se debe? (Ayuda: utilice el comando `ss` visto anteriormente).
10. ¿Qué sucede si llega un datagrama UDP a un host que no tiene a ningún proceso esperando en el puerto destino de dicho datagrama (es decir, que dicho puerto no está en estado LISTEN)?
- Utilice **hping3** para enviar datagramas UDP al puerto destino 68 de la máquina virtual.
 - Utilice **hping3** para enviar datagramas UDP al puerto destino 40 de la máquina virtual.
 - ¿Qué diferencias nota en las respuestas obtenidas en los dos casos anteriores? ¿Puede explicar a qué se debe? (Ayuda: utilice el comando `ss` visto anteriormente).
11. 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?
12. Use CORE para armar una topología como la siguiente, sobre la cual deberá realizar:
- En ambos equipos inspeccionar el estado de las conexiones y mantener abiertas ambas ventanas con el comando corriendo para poder visualizar los cambios a medida que se realiza el ejercicio. Ayuda: `watch -n1 'ss -nat'`.
 - En Servidor, utilice la herramienta **ncat** para levantar un servicio que escuche en el puerto 8001/TCP. Utilice la opción `-k` para que el servicio sea persistente. Verifique el estado de las conexiones.



- Desde CLIENTE1 conectarse a dicho servicio utilizando también la herramienta `ncat`. Inspeccione el estado de las conexiones.
- Iniciar otra conexión desde CLIENTE1 de la misma manera que la anterior y verificar el estado de las conexiones. ¿De qué manera puede identificar cada conexión?

- e. En base a lo observado en el ítem anterior, ¿es posible iniciar más de una conexión desde el cliente al servidor en el mismo puerto destino? ¿Por qué? ¿Cómo se garantiza que los datos de una conexión no se mezclarán con los de la otra?
- f. Cerrar la última conexión establecida desde CLIENTE1 y ver los estados de las conexiones en ambos equipos.
- g. Cortar el servicio de ncat en el servidor (Ctrl+C) y ver los estados de las conexiones en ambos equipos. Luego, cerrar la conexión en el cliente y verificar nuevamente los estados de las conexiones.
13. De acuerdo a la captura 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]

14. 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

15. Completar los datos que faltan en el intercambio de mensajes del siguiente diagrama de flujo TCP:

