

# Práctica 4 - Capa de Transporte

Revisión 2.4

1. ¿Cuáles son las funciones de la capa de transporte en el modelo OSI? ¿Cuáles implementan TCP y cuáles UDP? ¿Existen otros protocolos de transporte en el stack TCP/IP? ¿Cuáles son los más utilizados? ¿En qué protocolo se encapsulan y en qué parte de un sistema se los suele encontrar: en el kernel del SO, en espacio de usuario, cómo microservicios fuera del kernel?
2. Indique que asumen TCP y UDP con respecto a los servicios provistos por la capa de Red/Internetworking sobre la cual se implementan. ¿Cuál es el campo del datagrama IP y los valores utilizados para diferenciarlos en la multiplexación (Hint: buscar en `/etc/protocols`)?
3. La PDU de la capa de transporte es nombrada de forma genérica segmento. Indique para los protocolos indicados en los puntos anteriores cómo se llaman específicamente las unidades de datos y realice un diagrama de su estructura.
4. Responder:
  - a) ¿Qué sucede si llega un datagrama IPv6 a un host y éste no tiene implementado IPv6?
  - b) ¿Qué sucede si llega un segmento TCP a un host que no tiene soporte de este protocolo de transporte?
  - c) ¿Qué sucede si llega un segmento TCP a un host y éste no tiene un proceso esperando en el puerto destino indicado? ¿Qué sucede si el mensaje es UDP?
5. ¿En qué se diferencian los checksum de UDP, TCP, IPv4 e IPv6?
6. Un proceso desde 10.0.0.10 inicia una conexión TCP, por ejemplo mediante el comando telnet, hacia un servidor 192.168.1.10. Al mismo tiempo otro proceso desde 10.0.0.10 inicia otra conexión TCP hacia el mismo servicio. Ambas conexiones se establecen.
  - a) Indicar direcciones y números de puerto origen y destino de la primera conexión.
  - b) Indicar direcciones y números de puerto origen y destino para la segunda conexión.
  - c) Si genera una nueva conexión desde 10.0.0.11 hacia el mismo servicio, indicar direcciones y números de puerto origen y destino utilizados.
  - d) Indicar la cantidad de segmentos TCP transmitidos en total.
  - e) Indicar los "flags" que se verán en los segmentos TCP transmitidos.
  - f) Indicar cantidad de segmentos TCP totales (inicio, datos y cierre) en caso que solo dos conexiones transmiten 1 byte c/u y luego cierran las 3.
  - g) Indicar la cantidad de datagramas transmitidos en caso de que las transferencias se realicen utilizando UDP.
  - h) Hacer una simulación de los escenarios, con nc (netcat) o telnet.

7. Dada la siguiente salida del comando (netstat o ss), responder:

```
# netstat -atun
Active Internet connections (servers and established)
Proto R-Q S-Q Local Address      Foreign Address    State
tcp    0  0  127.0.0.1:43695    0.0.0.0:*          LISTEN
tcp    0  0  127.0.0.1:7634     0.0.0.0:*          LISTEN
tcp    0  0  0.0.0.0:22         0.0.0.0:*          LISTEN
tcp    0  0  127.0.0.1:631     0.0.0.0:*          LISTEN
tcp    0  0  0.0.0.0:17500      0.0.0.0:*          LISTEN
tcp    0  0  0.0.0.0:8000       0.0.0.0:*          LISTEN
tcp    0  0  127.0.0.1:40963    0.0.0.0:*          LISTEN
tcp    0  0  127.0.0.1:2628     0.0.0.0:*          LISTEN
tcp    0  0  10.168.1.163:51222 173.194.42.54:443  ESTABLISHED
tcp    0  0  127.0.0.1:43695    127.0.0.1:45547    ESTABLISHED
tcp    1  0  10.168.1.163:50120 191.189.39.14:80   CLOSE_WAIT
tcp    0  0  127.0.0.1:8000     127.0.0.1:35250    ESTABLISHED
tcp    0  0  127.0.0.1:35250    127.0.0.1:8000     ESTABLISHED
tcp    0  1  10.168.1.163:45123 1.1.1.1:9000       SYN_SENT
tcp    0  0  10.168.1.163:40123 99.59.148.17:443   TIME_WAIT
tcp    1  1  10.168.1.163:58432 104.154.94.81:443  LAST_ACK
tcp    0  0  10.168.1.163:36121 138.160.162.116:7  ESTABLISHED
tcp    1  0  10.168.1.163:58433 205.154.94.81:443  CLOSE_WAIT
tcp    0  0  10.168.1.163:60123 91.189.89.76:443   ESTABLISHED
tcp    0  0  10.168.1.163:42133 173.194.42.33:443  ESTABLISHED
tcp    0  0  10.168.1.163:50121 199.16.156.83:443  ESTABLISHED
tcp    0  0  127.0.0.1:45547    127.0.0.1:43695    ESTABLISHED
tcp6   0  0  :::80              :::*               LISTEN
tcp6   0  0  :::22              :::*               LISTEN
tcp6   0  0  :::1:631           :::*               LISTEN
udp    0  0  0.0.0.0:68         0.0.0.0:*          *
udp    0  0  0.0.0.0:69         0.0.0.0:*          *
udp    0  0  0.0.0.0:59744      0.0.0.0:*          *
udp    0  0  0.0.0.0:17500      0.0.0.0:*          *
udp    0  0  0.0.0.0:5353       0.0.0.0:*          *
udp6   0  0  :::59695           :::*               *
udp6   0  0  :::5353            :::*               *
```

- ¿Cuántas conexiones TCP hay establecidas?
- ¿Cuántas conexiones TCP hay establecidas solo como cliente y cuántas como servidor?
- ¿Cuántas conexiones TCP están aún pendientes por establecerse?
- ¿A qué servicios bien conocidos (puertos 0 a 1023) tiene el host conexiones TCP establecidas?
- ¿Qué servicios bien conocidos (TCP y UDP) tiene corriendo el host (esperando por recibir información)? (Ver RFC1700)
- ¿Cuántas conexiones están en proceso de cierre?
- ¿Cuáles conexiones TCP tuvieron el cierre iniciado por el host local y cuáles por el remoto?
- ¿En qué puertos podría recibir datos sobre IPv6 desde otros hosts, tanto TCP6 como UDP6?

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]

Figura 1: Captura TCP 1

8. De acuerdo a la captura de la figura 1 indicar los valores de los campos que están difuminados ("blur").
9. De acuerdo a la siguiente salida del comando netstat responder:

```
# netstat -atunp
Active Internet connections (servers and established)
Proto . Local Address      Foreign Address    State
tcp    0.0.0.0:22           0.0.0.0:*          LISTEN  999/sshd
tcp    127.0.0.1:631        0.0.0.0:*          LISTEN  11351/cupsd
tcp    13.10.0.14:5217     91.189.95.73:443   CLOSE_  10418/remot
tcp    13.10.0.14:22       11.191.89.18:49357 ESTABL  11696/sshd:
tcp6   :::80               :::*              LISTEN  1847/apache2
tcp6   :::22               :::*              LISTEN  999/sshd
tcp6   :::1:631            :::*              LISTEN  11351/cupsd
```

- a) ¿Cuál es el proceso asignado al port de servicios de impresión de red? (Hint: buscar en /etc/services).
- b) ¿Se podría enviar a imprimir al servidor de impresión de este equipo a través de la red desde otros equipos?
- c) ¿Qué servicios pueden recibir conexiones sobre IPv6?

10. Dadas las salidas de los siguientes comandos ejecutados en el cliente y el servidor, responder:

```

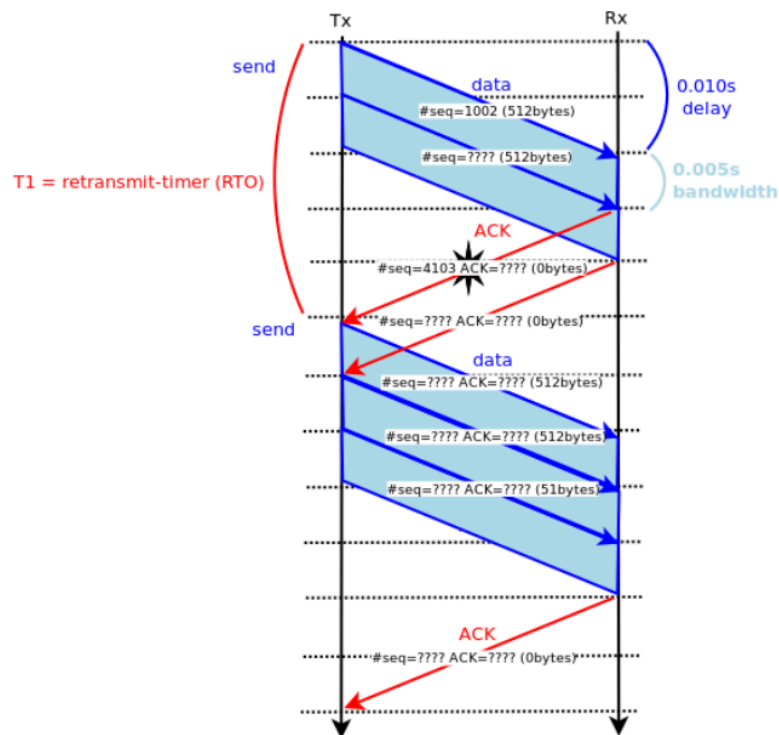
srv# netstat -atun | grep 4500
tcp    0      0  0.0.0.0:4500          0.0.0.0:*            LISTEN
tcp    0      0  157.0.0.1:4500       157.0.11.1:52843     SYN_RECV

cli# netstat -atun | grep 4500
tcp    0      1  157.0.11.1:52843     157.0.0.1:4500       SYN_SENT

```

- ¿Qué paquetes llegaron y cuáles parecen que se están perdiendo en la red?
- ¿Cómo quedará el estado en ambos lados si no logra establecerse la conexión?

11. Dado el diagrama de intercambio de segmentos de la figura 2 y suponiendo que se aplica el mecanismo de ARQ Go-Back-N numerando por bytes, responder:



**Figura 2: Control de Errores Go-Back-N**

- ¿Cuál es el ancho de banda digital (throughput) que se está obteniendo?
- ¿Cuál debería ser el valor óptimo del T1 (RTO, Timer de retransmisión) suponiendo que el delay se mantiene constante? ¿Cómo se soluciona cuando el delay no es constante?

- c) ¿Cuál sería un tamaño de ventana óptimo?
- d) ¿Cuántos bytes lograron transferirse de forma efectiva?
- e) Suponiendo que el primer ACK se pierde, completar los valores indicados con signos de interrogación.
12. El host A desea establecer una sesión TCP con el host B. A selecciona un ISN de 50430, MSS de 1400 bytes y un tamaño de ventana de 64KB; B, por su parte, tiene un ISN de 68900, MSS de 1000 bytes y un tamaño de ventana de 32KB. Responder:
- a) ¿Cómo sería el intercambio de mensajes para establecer la sesión?
- b) ¿Cuántos segmentos de tamaño máximo le puede enviar A a B sin esperar un ACK? ¿Y B a A? (Considere primero que no se aplica control de congestión tradicional y luego aplicándolo).
13. Se tiene una conexión TCP entre dos hosts, A y B. B ya recibió correctamente de A todos los bytes hasta el byte 225. A se conecta desde el port 1986 al port 22 de B. Responder:
- a) ¿Qué valor indicará B en el campo ACK para reconocer esta condición? ¿Qué ports utilizará?
- b) Si A le envía dos segmentos a B de 100 y 120 bytes respectivamente, ¿cuáles son los números de secuencia de los dos segmentos?
- c) Si B envía un ACK por cada segmento recibido, ¿cuáles serían los números de ACKs seteados? ¿Y si envía uno solo por los dos segmentos?
- d) Si el segundo segmento de datos (el de 120 bytes) arriba antes que el primer segmento, en el ACK del primer segmento recibido, ¿cuál es el valor del número de ACK?
14. Dada la sesión TCP de la figura 3 completar los valores marcados con un signo de interrogación.

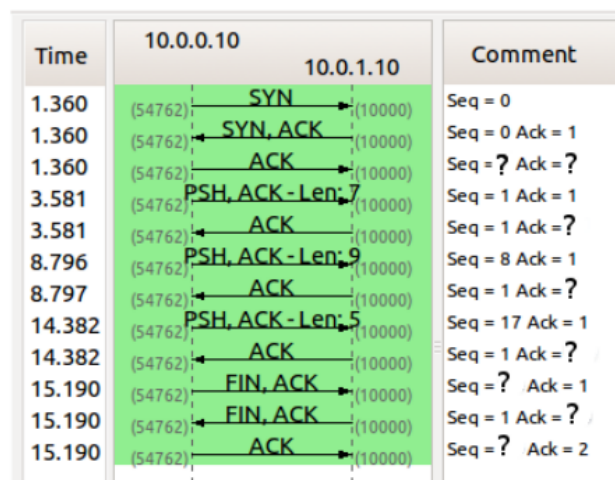
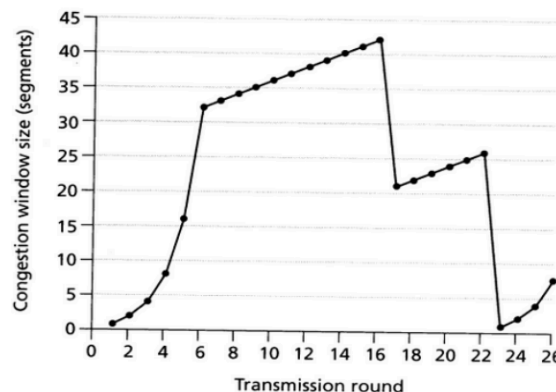


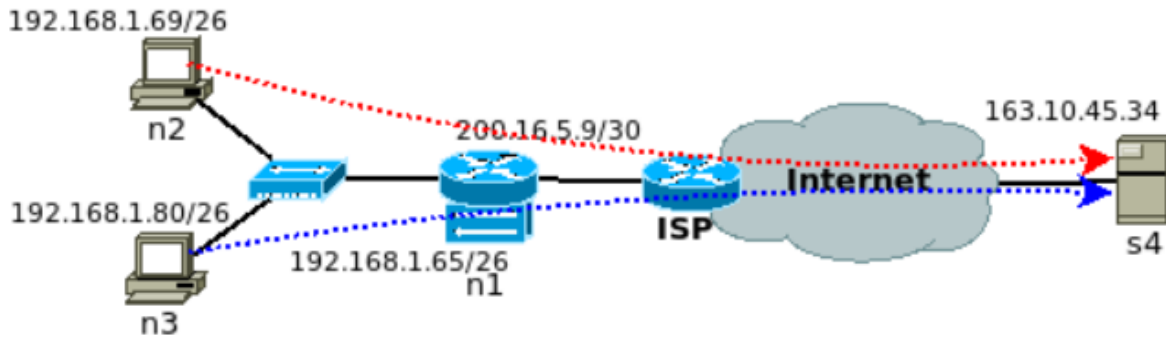
Figura 3: Sesión TCP

15. A partir de las capturas `tcp-init.pcap` y `tcp-init2.pcap` indicar qué opciones se intercambiaron en TCP. Indicar los ISN (Initial Sequence Number) de cada extremo y el port del cliente y del servidor. Investigar en la captura `tcp-init3.pcap` el intercambio del MSS (Maximum Segment Size) y comparar la diferencia con las anteriores, ¿a qué puede deberse?
16. Se tiene un enlace no congestionado con un RTT de 10ms. La ventana de recepción es de 12KB, y el  $cwnd = IW = 1 \times MSS$ , MSS es de 1KB. Si el Ssthresh inicia de 16KB y el emisor envía datos continuamente, ¿cuánto tiempo le toma a la ventana utilizada,  $\min(cwnd, rwnd)$ , alcanzar su máximo? Hacer el diagrama.
17. Suponga que la ventana de congestión de TCP está seteada en 18KB y que, en ese momento, se vence el RTO de una transmisión. Si el tamaño máximo del segmento es 1KB, ¿qué tan grande será la ventana si las próximas 4 ráfagas de transmisión son exitosas?
18. Observar el gráfico de la fig. 4, que ejecuta TCP Reno y responder:



**Figura 4: TCP Reno - Control de Congestión**

- a) ¿Cuáles son los intervalos en los que se ejecuta Slow-Start?
  - b) ¿Cuáles son los intervalos en los que se ejecuta Congestion Avoidance?
  - c) ¿Qué evento se produce en el momento 16? ¿Y en el 22?
  - d) ¿Cuál es el valor de la variable (Ssthresh) SStreshold inicialmente? ¿Y en los momentos 18 y 24?
19. A partir de las capturas **tcp\*.pcap.gz** indicar en cuáles y cuándo se detecta que se activó el control de flujo y en cuáles el control de congestión.
  20. NAT/NAPT: Dado el diagrama de la figura 5 indicar como quedaría la tabla de NAT/NAPT del router n1 si este hace "overloading" con su única IP pública y se generan las dos conexiones TCP desde los hosts n2 y n3 hacia el servidor s4.



**Figura 5: Diagrama de NAT**

21. Para el ejercicio 7 indicar si hay indicios que se está realizando NAT/NAPT. Cómo quedaría la tabla de NAT/NATP del router por donde pasa el tráfico para las tres primeras conexiones de salida en estado ESTABLISHED en caso que se haga overloading/masquerading y en el caso que solo se haga NAT básico. (Considere que IPs debería administrar el router).

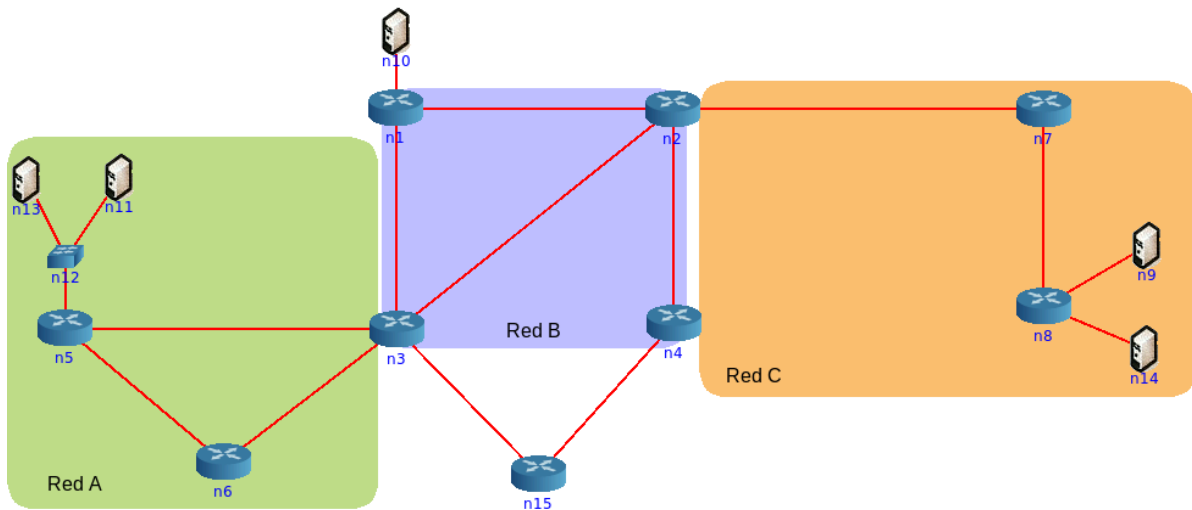
**22. Ejercicios UDP a entregar. Correr sobre la topología de la figura 6:**

- Levantar un servicio UDP con la herramienta nc (netcat) en el host n9 y enviar información desde n13 usando el mismo comando. Ver el estado de los sockets en ambos extremos. ¿Qué significa el estado ESTABLISHED en UDP?
- Levantar en el super daemon inetd o similar con el servicio UDP echo y probar con un cliente programado en el lenguaje de su elección mediante la API socket contra este servicio. Inspeccionar el estado. Ver de generar datos hacia el “servidor” desde más de un Nodo.
- Enviar información desde n13 a n9 a un port UDP donde no existe un proceso esperando por recibir datos. ¿Cómo notifica el stack TCP/IP de este hecho? Investigue la herramienta traceroute que ports utiliza y cómo usa estos mensajes (Ver ejercicio de IP con ruteo estático).
- Para las pruebas anteriores capturar tráfico y ver el formato de los datagramas UDP y como se encapsulan en IP.

**23. Ejercicios TCP a entregar. Correr sobre la topología de la figura 6 (continuación de lo que venían realizando en la topología en la práctica anterior):**

- Programar en el lenguaje de su elección mediante la API socket un servidor TCP que escuche conexiones en el puerto 9000 y que los datos que reciba los descarte. Correr en el nodo n9 y enviar datos desde otro nodo usando la herramienta nc (netcat) o telnet.
- En el nodo n9 levantar con el super daemon inetd algunos servicios extras, como tcp echo, discard y otros. Chequear los servicios TCP y UDP activos.
- Desde el nodo n13 realizar una conexión TCP y enviar datos mediante un programa cliente de su elección al servicio discard, y al echo. Capturar el tráfico con la herramienta tcpdump o wireshark y analizar la cantidad de segmentos, los flags utilizados y las opciones extras que llevan los encabezados tcp.
- Sin cerrar las conexiones chequear los servicios activos y ver los Estados.

- e ) Generar nuevas conexiones hacia el nodo n9 e inspeccionar los estados. Por ejemplo realizar varias conexiones simultáneas al servicio tcp echo desde el mismo origen y desde otros nodos.
- f) Intentar generar conexiones a un puerto donde no existe un proceso esperando por recibir datos. ¿Cómo notifica TCP de este hecho (ver flags)?
- g ) Cerrar las conexiones y ver el estado de los servicios en ambos lados. ¿En qué estado queda el que hace el cierre activo?
- h) Observando la captura indicar la cantidad de segmentos y los flags utilizados. ¿Con cuántos segmentos se cerró la conexión? ¿Existen otras variantes de cierre?
- i) Hacer un diagrama de los segmentos intercambiados con los números de secuencia absolutos para una de las sesiones TCP (Se puede usar la herramienta wireshark u otra).
- j ) Alternativo: Realizar una conexión mediante nc indicando un puerto específico para el cliente. Luego cerrar la conexión desde el cliente e intentar abrirla nuevamente. ¿En qué estado está el socket? Investigar valor del 2MSL en la plataforma sobre la cual está haciendo los tests.



**Figura 6: Diagrama de topología a entregar**