

Trabajo Práctico 1

[TA048] Redes
Primer cuatrimestre de 2025

| Alumno | Padron | Email |
|-------------------------------|--------|---------------------|
| AVALOS, Victoria | 108434 | vavalos@fi.uba.ar |
| CASTRO MARTINEZ, Jose Ignacio | 106957 | jcastrom@fi.uba.ar |
| CIPRIANO, Victor | 106593 | vcipriano@fi.uba.ar |
| DEALBERA, Pablo Andres | 106858 | pdealbera@fi.uba.ar |
| DIEM, Walter Gabriel | 105618 | wdiem@fi.uba.ar |

Contents

| | | |
|----------|--|-----------|
| 1 | Introduccion | 2 |
| 2 | Implementacion | 3 |
| 2.1 | Topología | 3 |
| 2.2 | Especificación del protocolo Stop-and-Wait | 4 |
| 2.2.1 | General | 4 |
| 2.2.2 | Handshake | 4 |
| 2.2.3 | Etapas de configuración y Transferencia | 4 |
| 2.2.4 | Cierre | 5 |
| 3 | Pruebas | 6 |
| 3.1 | Casos de error | 6 |
| 3.2 | Stop & Wait | 6 |
| 3.2.1 | Tabla de Datos de Wireshark | 8 |
| 3.3 | Análisis de la comunicación Stop-and-Wait | 8 |
| 4 | Preguntas a Responder | 9 |
| 4.1 | Describe la arquitectura Cliente-Servidor. | 9 |
| 4.1.1 | Características | 9 |
| 4.1.2 | Ventajas | 9 |
| 4.1.3 | Desventajas | 9 |
| 4.2 | ¿Cuál es la función de un protocolo de capa de aplicación? | 10 |
| 5 | Detalle el protocolo de aplicación desarrollado en este trabajo. | 10 |
| 5.1 | La capa de transporte del stack TCP/IP ofrece dos protocolos: TCP y UDP. | 10 |
| 5.1.1 | ¿Qué servicios proveen dichos protocolos? | 10 |
| 5.1.2 | ¿Cuáles son sus características? | 11 |
| 5.1.3 | ¿Cuando es apropiado utilizar cada uno? | 11 |
| 6 | Dificultades Encontradas | 11 |
| 7 | Conclusión | 11 |
| 8 | Anexo: Fragmentacion IPv4 | 11 |
| 8.1 | Análisis | 11 |

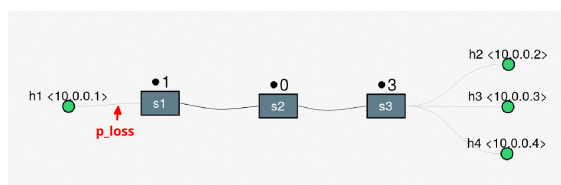
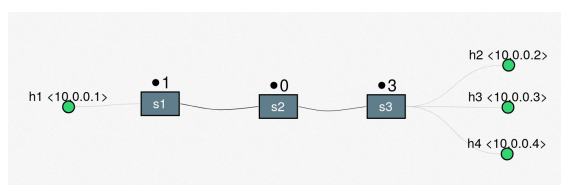
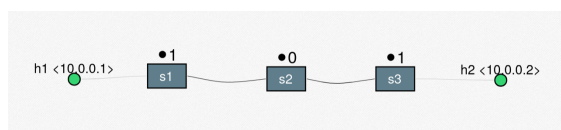
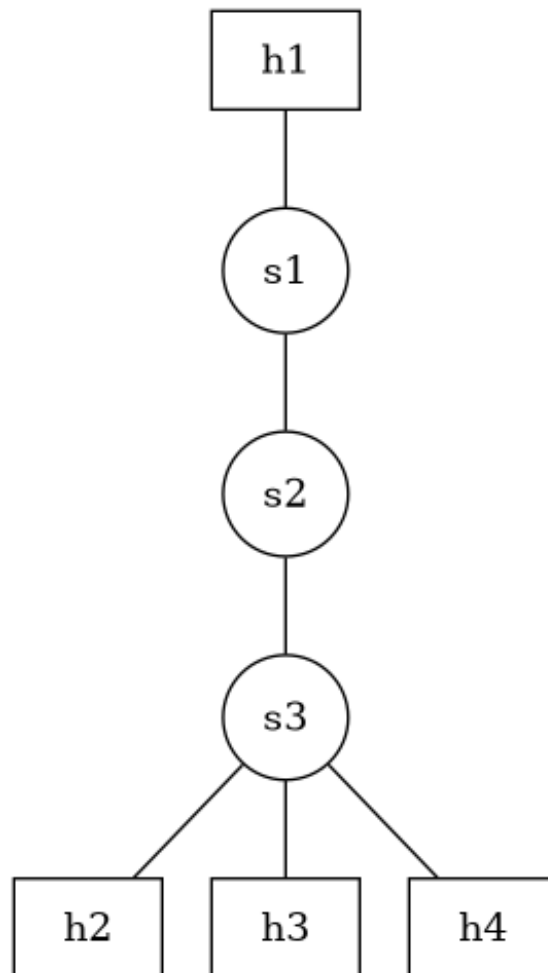
1 Introduccion

- La carga/descarga no va a conservar la metadata del archivo. Es decir, si yo descargo un archivo, ese archivo va a tener metadata como si yo hubiera creado el archivo desde cero usando ‘touch archivo’.
- Si el cliente utiliza otro protocolo para comunicarse con el server, el server debe rechazar este pedido. (`PROTOCOL_MISMATCH`). El header tendra un campo dedicado a esto.
- El argumento de `FILENAME` sera opcional, en caso de no estar, se utiliza el nombre original del archivo.
- Por simplicidad, vamos a guardar todos los archivos en `DIRPATH` sin ningun nivel de subdirectorios.
- Por simplicidad, vamos a tener un tamaño maximo de 2GB para la subida y descarga de archivos.
- Los archivos en proceso de escritura se van a escribir en una ubicacion temporal para evitar que se corrompan en la ubicacion que el cliente pidio.
- Usar seek y bufferear para leer el archivo. Leer con slices del buffer.

Caso borde: Dos clientes cargando y descargando el mismo archivo al mismo tiempo.

2 Implementacion

2.1 Topología



2.2 Especificación del protocolo Stop-and-Wait

2.2.1 General

Tamaño máximo de payload de: 61440 Bytes (60kB). Este número se obtiene teniendo en cuenta que el header de UDP posee un tamaño máximo de payload de 65535 (64kB), dejando espacio para los headers.

Se usa la nomenclatura S para mencionar al servidor y C para el cliente.

2.2.2 Handshake

La idea es usar este handshake para inicialización de recursos del servidor y check de protocolo.

Mensajes para caso Download y caso Upload:

1. $C \rightarrow S$: con flag SYN para declarar una solicitud de conexión y el protocolo

Flujo normal (mismo protocolo):

2. $S \rightarrow C$: con flag de SYN y ACK para declarar que se acepta la conexión y el puerto donde se va a escuchar el resto.
3. $C \rightarrow S$: con flag ACK al mismo welcoming socket. Se declara la operación (OP) en el payload, que puede ser download (1) o upload (2).
4. $S \rightarrow C$: ACK de la operación desde el connection socket

Flujo de error (distinto protocolo):

2. $S \rightarrow C$: con flag FIN para denegar la conexión por usar un protocolo distinto.

Se hace una transferencia de puerto para que el welcoming socket se encargue solamente de establecer conexiones y el nuevo puerto maneje la transferencia de datos del archivo. El último ACK de parte del cliente asegura que se recibió el puerto donde se tiene que comunicar y es seguro hacer el cambio de socket.

2.2.3 Etapa de configuración y Transferencia

El cliente ya sabe que tiene que comunicarse con el nuevo puerto y el servidor ya sabe qué operación se quiere realizar.

Mensajes para caso Download:

3. Mensaje 3 $C \rightarrow S$: filename

Flujo Normal:

4. $S \rightarrow C$: ACK + comienzo de datos (piggybacked)
5. $C \rightarrow S$: ACK
6. $S \rightarrow C$: continuación de datos
7. $C \rightarrow S$: ACK

...

Flujo de error (no existe un archivo con ese nombre):

1. $S \rightarrow C$: FIN
2. $C \rightarrow S$: ACK

3. $C \rightarrow S$: FIN

4. $S \rightarrow C$: ACK

Mensajes para caso Upload:

3. $C \rightarrow S$: filename

Flujo de error (ya existe un archivo con ese nombre):

1. $S \rightarrow C$: FIN

2. $C \rightarrow S$: ACK

3. $C \rightarrow S$: FIN

4. $S \rightarrow C$: ACK

Flujo normal:

4. $S \rightarrow C$: ACK

5. $C \rightarrow S$: filesize

Flujo de error (No hay más espacio en disco):

1. $S \rightarrow C$: FIN

2. $C \rightarrow S$: ACK

3. $C \rightarrow S$: FIN

4. $S \rightarrow C$: ACK

Flujo normal:

6. $S \rightarrow C$: ACK

7. $C \rightarrow S$: comienzo de datos

8. $S \rightarrow C$: ACK

9. $C \rightarrow S$: continuacion de datos

...

2.2.4 Cierre

El flag FIN va piggybacked con la última data para que sea más eficiente. El receptor confirma con un ACK + FIN para que el emisor sepa que le llegó la información, y por si este se pierde está el último ACK para confirmar el cierre de parte del emisor.

Mensajes para caso Download:

1. $S \rightarrow C$: ultima data, va piggybacked el flag FIN

2. $C \rightarrow S$: ACK

3. $C \rightarrow S$: FIN

4. $S \rightarrow C$: ACK

Mensajes para caso Upload:

1. $C \rightarrow S$: ultima data, va piggybacked el flag FIN

2. $S \rightarrow C$: ACK

3. $S \rightarrow C$: FIN

4. $C \rightarrow S$: ACK

3 Pruebas

En esta sección mostraremos capturas de diferentes casos de uso de la aplicación.

3.1 Casos de error

- Protocol Mismatch

```

root@vicky-Lenovo-ideapad-330-15IKB:/home/vicky/Escritorio/TP1-Rede
s# e
./src/start-server.py -H 10.0.0.1 -s ./tmp/server -v -r saw
[17:40:38] [INFO] Server started
[17:40:38] [DEBUG] Protocol: saw
[17:40:38] [DEBUG] [ACCEPT] Waiting for connection on Address(10.0.0.1:7777)
[17:40:42] [INFO] [ACCEPT] Rejecting client Address(10.0.1.1:54700)
due to protocol mismatch, expected saw
[17:40:42] [DEBUG] [ACCEPT] Waiting for connection on Address(10.0.0.1:7777)

root@vicky-Lenovo-ideapad-330-15IKB:/home/vicky/Escritorio/TP1-Rede
s# e
./src/upload.py -H 10.0.0.1 -s ./tmp/client/descarga.pdf -v -r gbn
[17:40:42] [DEBUG] Running on Address(0.0.0.0:54700)
[17:40:42] [INFO] Client started for upload
[17:40:42] [DEBUG] Protocol: gbn
[17:40:42] [DEBUG] UDP socket ready
[17:40:42] [DEBUG] Starting handshake
[17:40:42] [DEBUG] Requesting connection to Address(10.0.0.1:7777)
[17:40:42] [ERROR] Protocol mismatch
[17:40:42] [ERROR] Connection refused from server
[17:40:42] [INFO] Stopping
[17:40:42] [INFO] Press Enter to finish
  
```

Figure 1: Ejemplo de protocol mismatch.

En caso de que un cliente intente conectarse con un servidor utilizando un protocolo diferente al suyo, el servidor lo rechazará. En la imagen se puede observar un ejemplo en el que un servidor que utiliza Stop & Wait rechaza a un cliente que hace una petición con Go Back N.

- Archivo ya existente.

```

root@vicky-Lenovo-ideapad-330-15IKB:/home/vicky/Escritorio/TP1-Rede
s# e
./src/start-server.py -H 10.0.0.1 -s ./tmp/server -v -r saw
[17:37:31] [INFO] Server started
[17:37:31] [DEBUG] Protocol: saw
[17:37:31] [DEBUG] [ACCEPT] Waiting for connection on Address(10.0.0.1:7777)
[17:38:33] [DEBUG] [ACCEPT] Accepting connection for Address(10.0.1.1:41162)
[17:38:33] [DEBUG] [ACCEPT] Transferred to Address(10.0.0.1:52755)
[17:38:33] [DEBUG] [ACCEPT] Handshake completed
[17:38:33] [DEBUG] [CONN:52755] Processing operation intention
[17:38:33] [DEBUG] [CONN:52755] Waiting for connection on Address(10.0.0.1:7777)
[17:38:33] [DEBUG] [CONN:52755] Operation is: UPLOAD
[17:38:33] [DEBUG] [CONN:52755] Confirming operation
[17:38:33] [DEBUG] [CONN:52755] Validating filename
[17:38:33] [WARN] [CONN:52755] Filename received invalid
[17:38:33] [ERROR] [CONN:52755] Client 10.0.1.1:41162 shutting down
due to file 'descarga.pdf' already existing in the server
[17:38:33] [DEBUG] [CONN:52755] Initiating connection close
[17:38:34] [DEBUG] [CONN:52755] Received connection finalization from client
[17:38:34] [INFO] [CONN:52755] Connection closed

root@vicky-Lenovo-ideapad-330-15IKB:/home/vicky/Escritorio/TP1-Rede
s# e
./src/upload.py -H 10.0.0.1 -s ./tmp/client/descarga.pdf -v -r saw
[17:38:33] [DEBUG] Running on Address(0.0.0.0:41162)
[17:38:33] [INFO] Client started for upload
[17:38:33] [DEBUG] Protocol: saw
[17:38:33] [DEBUG] UDP socket ready
[17:38:33] [DEBUG] Starting handshake
[17:38:33] [DEBUG] Requesting connection to Address(10.0.0.1:7777)
[17:38:33] [DEBUG] Connection request accepted
[17:38:33] [DEBUG] Completing handshake with Address(10.0.0.1:7777)
[17:38:33] [DEBUG] Sending operation intention
[17:38:33] [DEBUG] Waiting for operation confirmation
[17:38:33] [DEBUG] Operation accepted
[17:38:33] [DEBUG] Connection established
[17:38:33] [DEBUG] Informing filename: descarga.pdf
[17:38:33] [DEBUG] Waiting for filename confirmation
[17:38:33] [DEBUG] Filename confirmation failed
[17:38:33] [ERROR] File in server already exists
[17:38:33] [DEBUG] Connection finalization received. Confirming it
[17:38:33] [DEBUG] Sending own connection finalization
[17:38:34] [DEBUG] Connection closed
[17:38:34] [INFO] Stopping
[17:38:34] [INFO] Press Enter to finish
  
```

Figure 2: Ejemplo de upload de un archivo que ya existe en el servidor.

Para ambos protocolos, si el cliente intenta subir un archivo que el servidor ya tiene, se rechaza.

3.2 Stop & Wait

Para mostrar el funcionamiento de stop and wait, primero mostraremos los logs de las operaciones upload y download de un archivo pequeño de 5kB a modo de ejemplo, y luego cómo se ve una captura de whireshark de un archivo más grande.

- Upload
- Download

The image shows two terminal windows side-by-side. The left window, titled "Node: h1", shows a server running on IP 10.0.0.1. It starts a server and waits for a connection from 10.0.0.1:7777. Once connected, it receives a file named 'dummy_file.txt' and sends back confirmation messages. The right window, titled "Node: h2", shows a client running on IP 10.0.0.1. It starts an upload process, sends the file in chunks, and receives confirmation messages from the server. The process ends with a 'Press Enter to finish' message.

```

root@vicky-Lenovo-ideapad-330-151KB:/home/vicky/Escritorio/TP1-Redes# e
./src/start-server.py -H 10.0.0.1 -s ./tmp/server -v -r saw
[17:56:03] [INFO] Server started
[17:56:03] [DEBUG] Protocol: saw
[17:56:03] [DEBUG] [ACCEP] Waiting for connection on Address(10.0.0.1:7777)
[17:56:53] [DEBUG] [ACCEP] Accepting connection for Address(10.0.0.1:37343)
[17:56:53] [DEBUG] [ACCEP] Transferred to Address(10.0.0.1:38073)
[17:56:53] [DEBUG] [ACCEP] Handshake completed
[17:56:53] [DEBUG] [CONN:38073] Processing operation intention
[17:56:53] [DEBUG] [CONN:38073] Waiting for connection on Address(10.0.0.1:7777)
[17:56:53] [DEBUG] [CONN:38073] Operation is: UPLOAD
[17:56:53] [DEBUG] [CONN:38073] Confirming operation
[17:56:53] [DEBUG] [CONN:38073] Validating filename
[17:56:53] [DEBUG] [CONN:38073] Filename received valid: dummy_file.txt
[17:56:53] [DEBUG] [CONN:38073] Validating filesize
[17:56:53] [DEBUG] [CONN:38073] Filesize received valid: 5000 bytes
[17:56:53] [DEBUG] [CONN:38073] Ready to receive from Address(10.0.0.1:37343)
[17:56:53] [DEBUG] [CONN:38073] Received chunk 1
[17:56:53] [DEBUG] [CONN:38073] Received chunk 2
[17:56:53] [DEBUG] [CONN:38073] Received chunk 3
[17:56:53] [DEBUG] [CONN:38073] Received chunk 4
[17:56:53] [DEBUG] [CONN:38073] Finished receiving file
[17:56:53] [DEBUG] [CONN:38073] Connection finalization received. Confirming it
[17:56:53] [DEBUG] [CONN:38073] Sending own connection finalization
[17:56:53] [INFO] [CONN:38073] Connection closed
[17:56:53] [INFO] [CONN:38073] Upload completed from client 10.0.0.1:37343

root@vicky-Lenovo-ideapad-330-151KB:/home/vicky/Escritorio/TP1-Redes# ./src/upload.py -H 10.0.0.1 -s ./tmp/client/dummy_file.txt -v -r saw
[17:56:53] [DEBUG] Running on Address(0.0.0.0:37343)
[17:56:53] [INFO] Client started for upload
[17:56:53] [DEBUG] Protocol: saw
[17:56:53] [DEBUG] UDP socket ready
[17:56:53] [DEBUG] Starting handshake
[17:56:53] [DEBUG] Requesting connection to Address(10.0.0.1:7777)
[17:56:53] [DEBUG] Connection request accepted
[17:56:53] [DEBUG] Completing handshake with Address(10.0.0.1:7777)
[17:56:53] [DEBUG] Sending operation intention
[17:56:53] [DEBUG] Waiting for operation confirmation
[17:56:53] [DEBUG] Operation accepted
[17:56:53] [DEBUG] Connection established
[17:56:53] [DEBUG] Informing filename: dummy_file.txt
[17:56:53] [DEBUG] Waiting for filename confirmation
[17:56:53] [DEBUG] Informing filesize: 5000 bytes
[17:56:53] [DEBUG] Waiting for filesize confirmation
[17:56:53] [INFO] Sending file dummy_file.txt of 0.00 MB
[17:56:53] [DEBUG] Sending chunk 1/4 of size 1.39 KB
[17:56:53] [DEBUG] Waiting confirmation for chunk 1/4
[17:56:53] [DEBUG] Sending chunk 2/4 of size 1.39 KB
[17:56:53] [DEBUG] Waiting confirmation for chunk 2/4
[17:56:53] [DEBUG] Sending chunk 3/4 of size 1.39 KB
[17:56:53] [DEBUG] Waiting confirmation for chunk 3/4
[17:56:53] [DEBUG] Sending chunk 4/4 of size 0.71 KB
[17:56:53] [DEBUG] Waiting confirmation for chunk 4/4
[17:56:53] [DEBUG] Waiting for confirmation of last packet
[17:56:53] [INFO] Upload completed
[17:56:53] [DEBUG] Received connection finalization from server
[17:56:53] [INFO] Stopping
[17:56:53] [INFO] Press Enter to finish

```

Figure 3: Ejemplo de Upload con Stop & Wait.

The image shows two terminal windows side-by-side. The left window, titled "Node: h1", shows a server running on IP 10.0.0.1. It starts a server and waits for a connection from 10.0.0.1:40154. Once connected, it receives a file named 'dummy_file.txt' and sends back confirmation messages. The right window, titled "Node: h2", shows a client running on IP 10.0.0.1. It starts a download process, sends the file in chunks, and receives confirmation messages from the server. The process ends with a 'Press Enter to finish' message.

```

root@vicky-Lenovo-ideapad-330-151KB:/home/vicky/Escritorio/TP1-Redes# ./src/start-server.py -H 10.0.0.1 -s ./tmp/server -v -r saw
[18:02:27] [INFO] Server started
[18:02:27] [DEBUG] Protocol: saw
[18:02:27] [DEBUG] [ACCEP] Waiting for connection on Address(10.0.0.1:7777)
[18:02:37] [DEBUG] [ACCEP] Accepting connection for Address(10.0.0.1:40154)
[18:02:37] [DEBUG] [ACCEP] Transferred to Address(10.0.0.1:54821)
[18:02:37] [DEBUG] [ACCEP] Handshake completed
[18:02:37] [DEBUG] [CONN:54821] Processing operation intention
[18:02:37] [DEBUG] [CONN:54821] Waiting for connection on Address(10.0.0.1:7777)
[18:02:37] [DEBUG] [CONN:54821] Operation is: DOWNLOAD
[18:02:37] [DEBUG] [CONN:54821] Confirming operation
[18:02:37] [DEBUG] [CONN:54821] Validating filename
[18:02:37] [DEBUG] [CONN:54821] Filename received valid
[18:02:37] [DEBUG] [CONN:54821] Ready to transmit to Address(10.0.0.1:40154)
[18:02:37] [INFO] [CONN:54821] Sending file dummy_file.txt of 0.00 MB
[18:02:37] [DEBUG] [CONN:54821] Sending chunk 1/4 of size 1.39 KB
[18:02:37] [DEBUG] [CONN:54821] Waiting confirmation for chunk 1
[18:02:37] [DEBUG] [CONN:54821] Sending chunk 2/4 of size 1.39 KB
[18:02:37] [DEBUG] [CONN:54821] Waiting confirmation for chunk 2
[18:02:37] [DEBUG] [CONN:54821] Sending chunk 3/4 of size 1.39 KB
[18:02:37] [DEBUG] [CONN:54821] Waiting confirmation for chunk 3
[18:02:37] [DEBUG] [CONN:54821] Sending chunk 4/4 of size 0.71 KB
[18:02:37] [DEBUG] [CONN:54821] Waiting confirmation for chunk 4
[18:02:37] [DEBUG] [CONN:54821] Waiting for confirmation of last packet
[18:02:37] [INFO] [CONN:54821] File transfer complete
[18:02:37] [DEBUG] [CONN:54821] Received connection finalization from server
[18:02:37] [INFO] [CONN:54821] Download completed to client 10.0.0.1:40154

root@vicky-Lenovo-ideapad-330-151KB:/home/vicky/Escritorio/TP1-Redes# ./src/download.py -H 10.0.0.1 -d ./tmp/client/dummy_file.txt -n dummy_file.txt -v -r saw
[18:02:37] [DEBUG] Running on Address(0.0.0.0:40154)
[18:02:37] [DEBUG] Location to save downloaded file: ./tmp/client/dummy_file.txt
[18:02:37] [INFO] Client started for upload
[18:02:37] [DEBUG] Protocol: saw
[18:02:37] [DEBUG] UDP socket ready
[18:02:37] [DEBUG] Starting handshake
[18:02:37] [DEBUG] Requesting connection to Address(10.0.0.1:7777)
[18:02:37] [DEBUG] Connection request accepted
[18:02:37] [DEBUG] Completing handshake with Address(10.0.0.1:7777)
[18:02:37] [DEBUG] Sending operation intention
[18:02:37] [DEBUG] Waiting for operation confirmation
[18:02:37] [DEBUG] Operation accepted
[18:02:37] [DEBUG] Connection established
[18:02:37] [DEBUG] Informing filename to download: dummy_file.txt
[18:02:37] [DEBUG] Waiting for filename confirmation
[18:02:37] [DEBUG] Received chunk 1
[18:02:37] [DEBUG] Received chunk 2
[18:02:37] [DEBUG] Received chunk 3
[18:02:37] [DEBUG] Received chunk 4
[18:02:37] [INFO] Download completed
[18:02:37] [DEBUG] Connection finalization received. Confirming it
[18:02:37] [DEBUG] Sending own connection finalization
[18:02:37] [INFO] Connection closed
[18:02:37] [INFO] Stopping
[18:02:37] [INFO] Press Enter to finish

```

Figure 4: Ejemplo de Download con Stop & Wait.

3.2.1 Tabla de Datos de Wireshark

-3cm-3cm

| No | Time | Src | Dst | Proto | Len | Type | SEQ | ACK | SYN | FIN | SrcPort |
|-----|-------------|----------|----------|-------|------|---------------|-----|-------|-------|-------|---------|
| 1 | 0.000000000 | 10.0.1.1 | 10.0.0.1 | SAW | 48 | Stop-and-Wait | 0 | False | True | False | 52515 |
| 2 | 0.000191297 | 10.0.0.1 | 10.0.1.1 | SAW | 48 | Stop-and-Wait | 0 | True | True | False | 41367 |
| 3 | 0.002208402 | 10.0.1.1 | 10.0.0.1 | SAW | 50 | Stop-and-Wait | 1 | True | False | False | 52515 |
| 4 | 0.002801150 | 10.0.0.1 | 10.0.1.1 | SAW | 48 | Stop-and-Wait | 1 | True | False | False | 41367 |
| 5 | 0.004355272 | 10.0.1.1 | 10.0.0.1 | SAW | 53 | Stop-and-Wait | 0 | False | False | False | 52515 |
| 6 | 0.004722710 | 10.0.0.1 | 10.0.1.1 | SAW | 48 | Stop-and-Wait | 0 | True | False | False | 41367 |
| 7 | 0.005754904 | 10.0.1.1 | 10.0.0.1 | SAW | 52 | Stop-and-Wait | 1 | False | False | False | 52515 |
| 8 | 0.005879502 | 10.0.0.1 | 10.0.1.1 | SAW | 48 | Stop-and-Wait | 1 | True | False | False | 41367 |
| 9 | 0.006562696 | 10.0.1.1 | 10.0.0.1 | SAW | 1474 | Stop-and-Wait | 0 | False | False | False | 52515 |
| 10 | 0.006634214 | 10.0.0.1 | 10.0.1.1 | SAW | 48 | Stop-and-Wait | 0 | True | False | False | 41367 |
| 11 | 0.006819155 | 10.0.1.1 | 10.0.0.1 | SAW | 1474 | Stop-and-Wait | 1 | False | False | False | 52515 |
| 12 | 0.006887880 | 10.0.0.1 | 10.0.1.1 | SAW | 48 | Stop-and-Wait | 1 | True | False | False | 41367 |
| ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... | ... |
| 384 | 0.036747322 | 10.0.0.1 | 10.0.1.1 | SAW | 48 | Stop-and-Wait | 1 | True | False | False | 41367 |
| 385 | 0.036806828 | 10.0.1.1 | 10.0.0.1 | SAW | 1474 | Stop-and-Wait | 0 | False | False | False | 52515 |
| 386 | 0.036860606 | 10.0.0.1 | 10.0.1.1 | SAW | 48 | Stop-and-Wait | 0 | True | False | False | 41367 |
| 387 | 0.037000220 | 10.0.1.1 | 10.0.0.1 | SAW | 1474 | Stop-and-Wait | 1 | False | False | False | 52515 |
| 388 | 0.037084310 | 10.0.0.1 | 10.0.1.1 | SAW | 48 | Stop-and-Wait | 1 | True | False | False | 41367 |
| 389 | 0.037217987 | 10.0.1.1 | 10.0.0.1 | SAW | 363 | Stop-and-Wait | 0 | False | False | True | 52515 |
| 390 | 0.037459011 | 10.0.0.1 | 10.0.1.1 | SAW | 48 | Stop-and-Wait | 0 | True | False | False | 41367 |
| 391 | 0.037511183 | 10.0.0.1 | 10.0.1.1 | SAW | 48 | Stop-and-Wait | 0 | False | False | True | 41367 |
| 392 | 0.037580397 | 10.0.1.1 | 10.0.0.1 | SAW | 48 | Stop-and-Wait | 1 | True | False | False | 52515 |

3.3 Análisis de la comunicación Stop-and-Wait

La tabla presentada muestra una traza de paquetes intercambiados entre dos nodos de mininet (10.0.1.1 y 10.0.0.1) utilizando el protocolo desarrollado con el esquema Stop-and-Wait. Este protocolo garantiza la entrega ordenada y libre de errores mediante el envío secuencial de paquetes, esperando una confirmación (ACK) por cada uno antes de continuar con el siguiente.

El ciclo de vida de la comunicación puede dividirse en tres fases:

1. Establecimiento de la conexión:

- El cliente (10.0.1.1) inicia la conexión enviando un paquete con la bandera 'SYN' activada.
- El servidor (10.0.0.1) responde con un paquete que contiene tanto 'SYN' como 'ACK', indicando aceptación.
- Finalmente, el cliente responde con un 'ACK', completando el procedimiento de handshake.

2. Transferencia de datos:

- Una vez establecida la conexión, el cliente comienza a enviar datos, alternando los números de secuencia (SEQ) entre 0 y 1. Este comportamiento es característico del protocolo Stop-and-Wait.
- Por cada paquete de datos enviado, el servidor responde con un paquete de confirmación ('ACK') para indicar que ha recibido correctamente el contenido.
- El campo 'Len' refleja el tamaño de los datos transportados, y los puertos de origen y destino se utilizan para mantener la sesión activa entre los procesos involucrados.

3. Finalización de la conexión:

- El cliente inicia el cierre de la sesión enviando un paquete con la bandera ‘FIN’ activada.
- El servidor responde primero con un ‘ACK’, y luego con su propio paquete ‘FIN’, indicando que también desea cerrar la conexión.
- Finalmente, el cliente responde con un ‘ACK’, completando el cierre de la comunicación de manera ordenada.

En resumen, esta captura de paquetes evidencia el funcionamiento correcto de una implementación del protocolo Stop-and-Wait, en donde cada paquete enviado es seguido por una respuesta de confirmación, y el inicio y cierre de la conexión se realizan mediante el protocolo RDT.

4 Preguntas a Responder

4.1 Describa la arquitectura Cliente-Servidor.

La arquitectura Cliente-Servidor es una de dos arquitecturas más comunes. En esta arquitectura hay un *host* (*end system*) llamado *server* que esta siempre encendido que pasivamente escucha *requests* de otros *hosts* llamados *clients* que son agentes activos que inician la comunicación con el *server*.

Un ejemplo de esta arquitectura es una aplicacion Web donde hay un *Web server* que escucha *requests* de navegadores web. El navegador web es el cliente que inicia la comunicación y el *Web server* es el servidor que responde a los *requests*. Estos mensajes tienen el formato de Capa de Aplicación HTTP.

4.1.1 Características

- Los clientes son agentes activos que inician la comunicación.
- Los clientes no se comunican entre si.
- Los clientes no necesitan estar encendidos todo el tiempo ni tener una IP fija.
- Los servidores son pasivos y siempre están encendidos.
- Los servidores **deben** tener una IP fija bien conocida (*well-known IP address*) que se puede resolver con un nombre de dominio DNS (*domain name*).
- Los servidores pueden tener múltiples clientes conectados al mismo tiempo.

4.1.2 Ventajas

- Diseño simple usando protocolos sin estado como HTTP donde el servidor no necesita mantener informacion sobre clientes ya que se puede guardar informacion del cliente en *cookies* del cliente y estos se transmitidos en *headers* HTTP.
- Puede soportar un gran numero de clientes.

4.1.3 Desventajas

- Un solo punto de falla. Si el servidor se cae, el servicio se cae.
- El servidor debe estar encendido todo el tiempo.
- Gran costo para escalar, ya que a medida de que el servicio tiene mas usuarios, el servidor debe tambien aumentar su capacidad de procesar mas clientes.

4.2 ¿Cuál es la función de un protocolo de capa de aplicación?

Un protocolo de capa de aplicación especifica cómo los procesos de una aplicación, que se ejecutan en diferentes sistemas finales, intercambian mensajes entre sí. Este tipo de protocolo define:

- Los tipos de mensajes que se envían, como mensajes de solicitud y de respuesta.
- La sintaxis de los mensajes, es decir, la estructura de los campos dentro de cada mensaje y cómo se separan o identifican esos campos.
- La semántica de los campos, indicando qué significa la información contenida en cada uno.
- Las reglas de comunicación, que establecen cuándo un proceso debe enviar un mensaje y cómo debe reaccionar al recibir uno.

En resumen, los protocolos de capa de aplicación aseguran que las aplicaciones puedan comunicarse correctamente y coordinarse en la red, haciendo posible servicios como el correo electrónico, la web o la transferencia de archivos.

5 Detalle el protocolo de aplicación desarrollado en este trabajo.

5.1 La capa de transporte del stack TCP/IP ofrece dos protocolos: TCP y UDP.

5.1.1 ¿Qué servicios proveen dichos protocolos?

Ambos protocolos proveen los siguientes servicios:

- **Multiplexación/Demultiplexación:** son los mecanismos que permiten extender el servicio de entrega de IP entre dos end systems a un servicio de entrega entre dos procesos que se ejecutan en esos sistemas. Dichos mecanismos permiten identificar a qué proceso pertenece cada segmento recibido.
- **Chequeo de integridad:** se verifica que no haya errores en los datos mediante un campo de checksum en los headers de ambos protocolos.

UDP no realiza ninguna otra función extra. Por lo tanto, su servicio es:

- **No confiable:** no garantiza que la entrega de los paquetes sea exitosa, ni tampoco que lleguen en orden.
- **Sin conexión:**

Por su parte, TCP ofrece las siguientes funcionalidades adicionales:

- **Orientado a la conexión:** antes de que un proceso de aplicación pueda comenzar a enviar datos a otro, ambos procesos deben comunicarse entre sí; es decir, deben enviarse algunos segmentos preliminares para establecer los parámetros de la transferencia de datos subsiguiente. Se trata de una conexión lógica con un estado en común que reside en TCP de los hosts.
- **Transferencia de datos confiable:** garantiza la entrega, el orden y la no corrupción de los datos. Esto lo logra mediante timers, números de secuencia y ACKs (flags que indican que un paquete fue entregado correctamente).
- **Control de congestión:** gestiona que no se saturen los enlaces. Es más bien un servicio para la red.
- **Control de flujo:** para eliminar la posibilidad de que el remitente desborde el búfer del receptor. Hace coincidir la velocidad a la que el remitente envía con la velocidad a la que la aplicación receptora lee.

5.1.2 ¿Cuáles son sus características?

Algunas de las características de UDP son las siguientes:

- **Pequeño overhead de header por paquete:** UDP posee un header pequeño (8 bytes) en comparación con TCP (20 bytes)
- **Sin estado de conexión:** UDP no mantiene un estado de conexión en los end systems, por lo que no rastrea ningún parámetro. Por esta razón, un servidor dedicado a una aplicación específica generalmente puede admitir muchos más clientes activos cuando la aplicación se ejecuta mediante UDP en lugar de TCP.
- **Sin retraso por conexión:** UDP no induce ningún retraso para establecer una conexión, a diferencia de TCP que posee un handshake de tres pasos.

Por su parte, TCP posee las siguientes características:

- **Full-duplex:** dada una conexión TCP entre dos hosts, digamos A y B, la información puede fluir de A a B al mismo tiempo que fluye información de B a A.
- **Conexión point-to-point:** la conexión de TCP únicamente se puede establecer entre un único remitente y un único receptor, no admite multicasting.
- **Three-Way Handshake:** para establecer la conexión mencionada anteriormente se realiza un procedimiento donde se envían tres segmentos.

5.1.3 ¿Cuándo es apropiado utilizar cada uno?

Ninguno de estos protocolos es mejor que el otro. Para decidir cuál de ellos utilizar, se deben tener en cuenta las necesidades de la aplicación. Debido a las características mencionadas anteriormente, UDP resulta más apropiado para aplicaciones que requieran mayor velocidad sin que sea tan sensible a algunas pérdidas de paquetes, por ejemplo plataformas de streaming, y si se tiene un servidor dedicado a una aplicación específica que necesita poder admitir muchos más clientes activos. Por otro lado, TCP es más ventajoso para las aplicaciones que necesitan un transporte confiable de los datos. Algunos ejemplos son el email y la web.

6 Dificultades Encontradas

7 Conclusión

8 Anexo: Fragmentacion IPv4

8.1 Analisis