Redes de Datos
Laboratorio 3 – Capa de Transporte

Universidad ORT Uruguay

Curso 2025

En este laboratorio, analizaremos el protocolo de capa de Transporte TCP, utilizado para ofrecer un servicio orientado a conexión y confiable para la comunicación entre procesos. Estudiaremos el uso de números de secuencia y reconocimiento para mantener el orden y recuperarse ante pérdidas, el uso de otros encabezados TCP (window size), el multiplexado de diferentes conexiones, así como la respuesta de TCP a fallos en el canal de transmisión.

Antes de comenzar la práctica deberá:

- Iniciar VirtualBox y la VM servidor del curso.
- Si desea ver los números *absolutos* de secuencia TCP (nos. de 32 bits completos) en Wireshark, antes de comenzar a capturar debe quitar la opción "Relative Sequence Numbers anb Window Scaling" en el menú *Edit/Preferences/Protocols/TCP*.
- Asegurarse de que su máquina no esté utilizando un Proxy HTTP.

1. Análisis de mensajes y secuencia TCP

1. Inicie una captura de tráfico entre la máquina host y la VM servidor en la host-only network. Acceda mediante el navegador a la página del servidor `http://192.168.56.2`). Luego de obtenida la página, detenga la captura.
2. Identifique el establecimiento de conexión, quién inicia la misma, los números de secuencia (SEQ) inicial de ambas partes, los números de reconocimiento (ACK), el largo del segmento, como así también qué banderas van activas durante la secuencia de segmentos intercambiados.
3. Identifique la finalización de la conexión, quién inicia el mismo, la secuencia de segmentos intercambiados indicando: los números de SEQ y ACK, como así también banderas activas y largo de segmentos.
4. Analice el intercambio request/response HTTP realizado una vez que la conexión está activa. Puede utilizar la opción Analyze/Follow/Follow TCP Stream de Wireshark para ayudarse. ¿Cuántos pedidos HTTP se realizan sobre la misma conexión? ¿Qué respuestas se obtienen?
5. Analizando la captura realizada. ¿En qué momento se incrementan los números de secuencia y en qué valor lo hacen?.
6. Analizando los números de secuencia. ¿Puede deducir cuántos bytes fueron enviados en cada sentido?
7. ¿Puede observar en algún momento la bandera PSH en TCP? ¿Para qué se utiliza?
8. Si una parte de la comunicación desea enviar solamente un reconocimiento y no datos. ¿Cuál número de secuencia debe enviar?
9. Capture nuevamente e intente acceder ahora a la dirección del servidor pero en el puerto 443, utilizando la URL `http://192.168.56.2:443`. ¿Logra conectarse? ¿Por qué sucede esto? ¿Qué bandera se utiliza para señalizar esto?

2. Análisis de las conexiones activas

1. Ejecute el comando `netstat -na` desde una consola de Windows. Detalle brevemente la salida observada.
2. ¿Qué significan los estados "ESTABLISHED" y "LISTENING" que observa?.
3. ¿Describa además que significa el estado "TIME-WAIT".
4. Establezca una conexión Telnet al servidor en otra consola utilizando:

   ```
   > telnet 192.168.56.2
   ```

   y ejecute nuevamente el comando `netstat -na`. Observe la nueva conexión en la salida.

3. Throughput de una conexión TCP

En esta sección se estudiará cómo la capacidad de transferir datos del protocolo TCP es afectada por las características del enlace utilizado.

Para ello se utilizará el programa de línea de comandos de Linux `tc`. Este programa permite degradar la comunicación entre la VM Linux (donde residen los servidores HTTP, FTP, DNS, Telnet, SSH) y el sistema operativo anfitrión, de una forma conocida y controlada.

1. Se comenzará estudiando la transferencia sobre un enlace con las siguientes características:
   - Ancho de banda: 10 Mbps (Mega-bits por segundo)
   - Retardo: 50 ms (milisegundos)

   Para obtener esto, ingrese a la VM, con el usuario y contraseña `redes`, y ejecute la siguiente línea en la terminal de línea de comandos de la VM Linux:

   ```
   $> ./enlace1.sh
   ```

2. Descargue el archivo del servidor mediante HTTP ubicado en la URL:
   `http://192.168.56.2/archivogrande.zip`.
3. Inicie una nueva captura y comience a descargar el archivo. En la captura identifique el comienzo y el fin de conexión y el número de secuencia inicial y final. Indique:
   a) La cantidad de bytes enviados.
   b) El tiempo transcurrido.
   c) Con los datos anteriores, calcule el throughput en Mbps y compárelo con el configurado como límite del enlace.
4. Seleccione el flujo TCP relativo a la descarga. Usando la opción de *Wireshark Statistics/TCP Stream Graph/ time-sequence graph (Stevens)*, observe la evolución del número de secuencia en función del tiempo y verifique el cálculo anterior.
5. Se pasará ahora a utilizar un enlace con las siguientes características:
   - Ancho de banda: 10 Mbps
   - Retardo: 50 ms
   - Tasa de pérdida de paquetes: 0.5 %

   Para obtener esto, ejecute la siguiente línea en la terminal de línea de comandos de la VM Linux:

   ```
   $> ./enlace2.sh
   ```

   Repita ahora las pruebas de descarga. Identifique:

- Los eventos de pérdida y cómo se repone TCP ante ellos. ¿Cuánto tiempo necesita para recuperar?
- ¿Qué ocurre con la ventana de transmisión de TCP ante una pérdida?
- ¿Cuál es el efecto neto de las pérdidas aleatorias en el throughput? Calcule para este caso y compare con el caso sin pérdidas analizado antes.

Nota: para liberar el enlace de las limitaciones de ancho de banda y pérdidas puede utilizar el siguiente comando en la VM:

```
$> ./liberar_enlace.sh
```