**Capa de Transporte - Parte I Redes y comunicaciones - 2022**

**Práctica 5**

**Capa de Transporte - Parte I**

**13**

**1. ¿Cuál es la función de la capa de transporte?**

Provee un sistema de comunicación lógico entre procesos, que se ejecutan en máquinas distintas interconectadas mediante una red.

Los datos de las aplicaciones del usuario se empaquetan, transportan y entregan al servidor, o aplicación de destino. Los procesos de la **capa de Transporte** aceptan datos de la capa de aplicación y los preparan para el direccionamiento en la capa de red, es decir, es responsable de la transferencia de extremo a extremo de los datos de aplicación. Lo que se busca es lograr “una comunicación lógica entre procesos”, es decir que, desde la perspectiva de la aplicación, es como si los hosts que ejecutan los procesos estuvieran conectados directamente.

La capa de Transporte permite la segmentación de datos y brinda el control necesario para reensamblar las partes dentro de los distintos streams de comunicación. Las responsabilidades que debe cumplir son:

- Seguimiento de la comunicación individual entre aplicaciones en los host origen y destino.

- Segmentación de datos y gestión de cada porción.

- Reensamble de segmentos en flujos de datos de aplicación.

- Identificación de las diferentes aplicaciones. (los datos de las distintas aplicaciones que están ejecutándose en la misma computadora no deben mezclarse).

Existen varios protocolos para la esta capa. Para algunas aplicaciones, los segmentos deben

llegar en una secuencia específica. En algunos casos, todos los datos deben recibirse para ser utilizados. En otros, una aplicación puede tolerar cierta pérdida de datos durante la transmisión a través de la red.

En general, todos los protocolos de la capa incluyen:

**- Segmentación y reensamblaje:** se dividen los datos de las aplicaciones en bloques de tamaño adecuado para poder enviarlos. En el destino, deben volver a ensamblarse.

**- Multiplexación de conversaciones:** debido a que puede haber varias aplicaciones corriendo en la misma computadora, a cada una se le asigna una dirección (puerto) para que la capa de Transporte pueda determinar con qué aplicación o servicio se identifican los datos.

Estas funciones son posibles gracias a los encabezados de la información que se comparte.

Algunas características de la capa de transporte son:

* MUX/DEMUX App. to App. (puertos, Ports). El nº de puerto identifica los procesos que corren y usan servicios de puerto
* Soporte de datos de tamaños arbitrarios. IP no ofrece eso, maneja paquetes autocontenidos (Datagramas)
* Control y Detección de Errores, pérdida, duplicación, se corrompen.
* ¿Cómo enviar info sobre la red de acuerdo al estado de la misma? ¿Cuándo y Cómo una App. Debe enviar datos? Cuando el receptor puede recibirla y la red mandarla
  + Control de Flujo.
  + Control de Congestión.
* Dos modelos:
  + Modelo Confiable: TCP🡪Da seguridad
  + Modelo NO Confiable: UDP🡪Implementa lo mínimo sobre IP

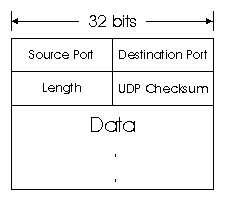
**2. Describa la estructura del segmento TCP y UDP.**

UDP

Datagrama (UDP)

Puertos: MUX/DEMUX.

Longitud: UDP HDR + Payload.



* **Source port**: 16 bits, puerto origen. Opcional, ya que UDP no solicita respuestas; si no se usa puede ponerse en 0.
* **Destination port**: 16 bits, puerto destino
* **Length**: 16 bits, longitud del segmento (encabezados + datos). Valor mínimo: 8 bytes.
* **UDP checksum**: 16 bits son la suma de verificación del segmento. Evita errores relacionados a datos que se corrompieron o bits que se cambiaron, en este caso se descartan silenciosamente. Evita errores de un bit, más no, hay otros controles mejores en capa de enlace, así que puede deshabilitarse en IPV4 si se pone 0x0000. Se calcula en origen y destino.

**Checksum**

• Calculo Ca1, Opcional. 0 = Sin checksum.

• Calculado HDR + PseudoHDR + Payload.

• PseudoHDR: IP.SRC + IP.DST + Zero + IP.PROTO + UDP.LENGTH.

• PseudoHDR: proteccion contra paquetes mal enrutados.

• Aplicaciones de LAN por eficiencia lo podrían deshabilitar.

• Si tiene error se descarta silenciosamente.

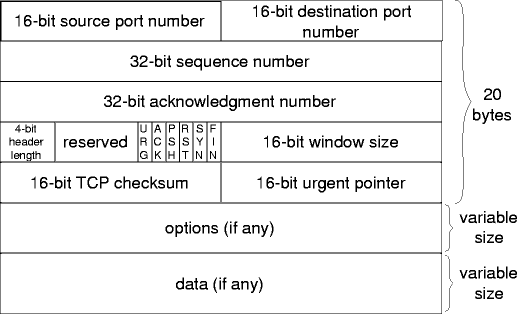
**TCP**

* Puertos: MUX/DEMUX.
* No tiene Longitud total, si de HDR LEN (variable, max 60B Unit=4B).
* Total LEN se computa para PseudoHDR, no viaja en el segmento.

**Checksum:**

• Calculo Ca1. Obligatorio, calculado, igual que UDP.

• Si tiene error podría pedir retransmisión, implementación de TCP descarta y espera RTO (Retransmission Timer).

* Necesidad de manejar Timers, RTO (tmout. por cada segmento). (implementaciones lo manejan más eficiente).
* Permite Opciones y Negociación.
* TCP entrega y envía lo datos agrupados o separados de forma disasociada de la aplicación:
* **Source port number:** 16 bits, puerto origen
* **Destination port number:** 16 bits, puerto destino. Estos dos se usan para multiplexar y demultiplexar los datos y para las aplicaciones de la capa superior.
* **Sequence number:** 32 bits, número de secuencia del segmento. Se usa para asegurar que los datos llegan en orden. Al inicio de la conexión, se le asigna un valor aleatorio
* **Acknowledgment number:** 32 bits, número de recibo del segmento. Almacena el número de segmento, del siguiente byte que el receptor espera recibir.

Cuando el receptor envía el valor X, significa que recibió todos los índices menores a X. Cuando se recibe cada paquete, toma numSecuencia + 1 y lo envía al emisor

* **Header length**: 4 bits, longitud del encabezado (Se aclara porque una parte es opcional).
* **Reserved**: 6 bits reservados, no se usan
* **Flag URG**: 1 bit. Si está en 1, los datos recibidos en el segmento son urgentes
* **Flag ACK (Campo de Control de Errores):** Si está en 1, el número de recibo es válido. Vale 1 en todos los segmentos, menos el de solicitud (al iniciar una conexión usando saludo de 3 vías)
* **Flag PSH**: Si está en 1, el receptor enviará inmediatamente el buffer entero a la capa de aplicación (sin esperar a que se llene). Luego, lo vaciará. No prioriza los datos, y éstos pueden llegar desordenados a la capa de aplicación, si aún no fueron ordenados. Ejemplo de la información que maneja es la pulsación de teclas.
* **Flag RST**: Si está en 1, el receptor finalizará la conexión de forma abrupta (Condición anómala). Ambos liberarán sus recursos, y pueden perderse los datos que estaban viajando. Se usa cuando hay errores irrecuperables, y no se puede finalizar la conexión de forma limpia.
* **Flag SYN (Campo de sesión):** Si está en 1, significa que el número de secuencia es el inicial de la conexión, se quiere establecer una conexión nueva. Vale 0 en todos los segmentos, menos el de solicitud (al iniciar una conexión usando saludo de tres vías)
* **Flag FIN (Campo de sesión):** Si está en 1, significa que el emisor quiere finalizar la conexión limpiamente. Vale 0 en todos los segmentos, menos el de finalización.
* **Windows size (Campo de Control de Flujo):** 16 bits, longitud de la ventana de recepción del emisor. Almacena la cantidad máxima de bytes que el emisor puede recibir sin enterarse explícitamente. Controles de flujo y envío de información eficiente. Se incrementa hasta detectar congestiones, donde se reduce para evitar perder paquetes.
* **TCP checksum (Campo de Deteccion de Errores):** 16 bits, suma de verificación del segmento. Lo mismo que UDP, pero acá es obligatorio. Se usa para verificar si los datos llegaron correctamente. Sino, el receptor lo rechaza y solicita que se vuelvan a enviar. Se calcula usando CRC
* **Urgent pointer:** 16 bits, puntero urgente. Almacena la cantidad de bytes urgentes, contenidos en el segmento. Al sumarlo al número de secuencia, se obtiene el primer byte no-urgente. Se usa sólo cuando el flag URG es 1
* El campo opciones es opcional y de longitud variable. Se utiliza cuando un emisor y un receptor negocian el tamaño máximo de segmento (MSS) o como un factor de escala de la ventana en las redes de alta velocidad. También se define una opción de marca temporal.
* **Opcionalmente, pueden incluirse otras opciones (Tamaño variable):**
  + Timestamp: Sirve para ordenar segmentos, cuando más de uno tiene el mismo número de secuencia. También se usa para que ambos extremos calculen el RTT con el otro
  + Extensión de longitud de ventana: Permite que el emisor notifique que puede recibir más de 2^16-1 bytes sin enterarse (máximo 2^32-1)
  + Negociación de parámetros: El emisor y el receptor establecen al inicio su longitud máxima de segmento, etc
  + Relleno: Bytes nulos que se agregan al final, para que la longitud total de los headers sea múltiplo de 4
* **Data:** Tamaño variable, datos que se desean enviar

**3. ¿Cuál es el objetivo del uso de puertos en el modelo TCP/IP?**

Brindar múltiples canales de comunicación a través de una misma conexión física. Un proceso de la máquina A se comunicará con uno de la B usando uno de estos canales

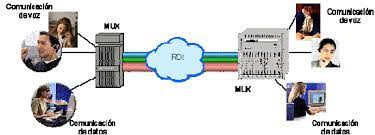
Un proceso puede tener uno o más sockets, puertas por las que pasan los datos de la red al proceso, y viceversa. Por tanto, la capa de transporte del host receptor realmente no entrega los datos directamente a un proceso, sino a un socket intermedio, que a su vez tiene un identificador único (ya que puede haber más de uno por host).

Cada segmento de la capa de transporte contiene campos para identificar el socket apropiado (entre otros). En el extremo receptor, la capa de transporte examina estos campos para identificar el socket receptor y, a continuación, envía el segmento a dicho socket. Esta tarea de entregar los datos contenidos en un segmento de la capa de transporte al socket correcto es lo que se conoce como **demultiplexación**.

Reunir los fragmentos de datos en el host de origen desde los diferentes sockets (en caso de que el proceso cuente con diferentes sockets), encapsulando cada fragmento de datos con la información de cabecera (el cual se utilizará después en el proceso de demultiplexación) para crear los segmentos y pasarlos a la capa de red es lo que se denomina **multiplexación**. Es importante darse cuenta de que estas técnicas son necesarias siempre que un único protocolo en una capa (cualquiera) sea utilizado por varios protocolos de la capa inmediatamente superior.

Sabemos que la operación de **multiplexación** que se lleva a cabo en la capa de transporte requiere que los sockets tengan identificadores únicos y que cada segmento tenga campos especiales que indiquen el socket al que tiene que entregarse el segmento. Estos campos especiales, son el campo número de puerto origen y número de puerto destino.

En Resumen: se usan los puertos para poder identificar los procesos (socket) con los que se mantiene una conexión y se intercambian mensajes.



**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.**

**a. Confiabilidad.**

El protocolo IP proporciona una comunicación lógica entre hosts. IP hace todo lo que puede por entregar los segmentos entre los hosts que se están comunicando, pero no garantiza la entrega. Por lo tanto, IP es un servicio NO FIABLE.

|  |  |
| --- | --- |
| UDP | TCP |
| ● Servicio no fiable.  ● No garantiza que los segmentos lleguen a destino.  ● Tampoco garantiza que lleguen en orden ni sin errores.  ● La comprobación de errores es responsabilidad de la aplicación. | ● Transferencia de datos fiable mediante control de flujo, números de secuencia, mensajes de reconocimiento y temporizadores.  ● Garantiza que los datos transmitidos sean entregados correctamente y en orden. Reenviará cada segmento hasta que la recepción sea confirmada. |

**b. Multiplexación.**

|  |  |
| --- | --- |
| UDP | TCP |
| ● Utiliza multiplexación y demultiplexación SIN conexión.  ● Creamos sockets indicando el número de puerto.  ● El segmento (de UDP + IP) identifica el socket destino mediante dos campos de cabecera: IP Destino y Nro. Puerto Destino.  ● El segmento tiene una “dirección de retorno”, por si el receptor desea devolver un segmento al emisor.  ● Si dos segmentos UDP con diferentes sockets de origen (Dirección IP y/o Nro. Puerto) poseen igual IP y puerto de destino, entonces los dos segmentos se enviarán al mismo proceso de destino a través del mismo socket de destino.  ● Cabeceras de 8 bytes. Más pequeñas. | ● Utiliza multiplexación y demultiplexación orientada a la conexión.  ● El socket, se identifica por cuatro elementos: IP Origen, Puerto Origen, IP Destino, Puerto Destino.  ● Dos segmentos entrantes con direcciones IP de origen o números de puerto de origen diferentes (con la excepción de un segmento TCP que transporte la solicitud original de establecimiento de conexión) serán dirigidos a dos sockets distintos.  ● Cuando un cliente se quiere comunicar con un servidor, debe enviar una solicitud en un puerto de destino y bits de establecimiento de conexión en la cabecera. Cuando el SO del servidor recibe el segmento de entrada de solicitud de conexión con ese puerto de destino, localiza el proceso de servidor que está esperando una conexión en dicho puerto. El proceso servidor crea un nuevo puerto. Además, la capa de transporte recuerda los valores contenidos en el segmento de solicitud de conexión (IPO, PO, IPD/su propia IP, PD). El socket de conexión recién creado queda identificado por estos cuatro valores. Los segmentos que lleguen después con estos valores serán enviados a este socket. Establecida la conexión, el cliente y el servidor podrán enviarse datos.  ● Cabecera de 20 bytes (es variable). Más del doble que UDP. |

**c. Orientado a la conexión.**

|  |  |
| --- | --- |
| UDP | TCP |
| ● Protocolo sin conexión.  ● No establecimiento de conexión entre emisor y receptor previo al envío del segmento, por lo que inicia la transmisión sin ningún retardo por esto.  ● No mantiene estado de la conexión.  ● Suele soportar más clientes activos cuando la aplicación se ejecuta sobre UDP. | ● Establecimiento de la conexión en tres fases antes de la transferencia de datos.  ● Mantiene estado de la conexión, en los sistemas terminales y no en los elementos intermedios de la red (routers y switches).  ● Servicio full-dupex: si hay una conexión, los datos entre el proceso A en el host 1 y el proceso B en el host 2, pueden fluir en ambas direcciones en simultaneo.  ● Conexión (casi siempre) punto a punto (emisor y receptor únicos). La “multidifusión” no es posible.  ● **Handshaking** (intercambio de mensajes de control). Inicializa ambos procesos antes del intercambio de datos.  ● Cada lado de la conexión tiene buffer de emisión y de recepción.  ● Consta de buffers, variables y un socket de conexión por cada proceso en un host. |

**d. Controles de congestión y de flujo.**

|  |  |
| --- | --- |
| UDP | TCP |
| ● No posee. | ● Regula el flujo del emisor cuando alguno/s de los enlaces entre los hosts de origen y de destino están excesivamente congestionados.  ● Control de flujo para que no se pueda desbordar el buffer del receptor  ● Adaptación de velocidades entre la transmisión del emisor y la lectura de la aplicación receptora.  ● El emisor dispone (y determina el tamaño) de una ventana de recepción que le da información al emisor sobre cuanto espacio libre hay en el buffer receptor. Debido a que la conexión es full dúplex, cada proceso dispone de una ventana de recepción diferente. |

**e. Utilización de puertos.**

|  |  |
| --- | --- |
| UDP | TCP |
| ● Socket definido por el nº de puerto e la IP del destino.  ● Muchos clientes pueden enviar datos por un mismo socket. | ● Socket definido para cada extremo de la conexión por los cuatro campos (IPOrigen, PuertoOrigen, IPDestino, PuertoDestino). Esto quiere decir que  por cada socket solo pueden intercambiar datos dos procesos (conexión punto a punto).  ● Debido a que la conexión solo puede ser punto a punto (porque identifica por esos 4 campos, no puede usar multicast). |

**Los sockets pueden verse como las puertas de los procesos.**

|  |  |  |
| --- | --- | --- |
|  | **TCP** | **UDP** |
| **Confiabilidad** | Alta | Baja |
| **Multiplexación** | Soportada (orientada a conexión) | Soportada (no orientada a conexión) |
| **Orientado a la conexión** | Sí | No |
| **Controles de congestión** | Sí | No |

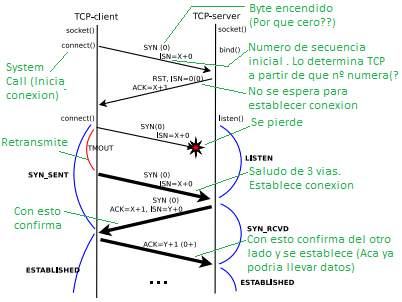
**5. La PDU de la capa de transporte es el segmento. Sin embargo, en algunos contextos suele utilizarse el**

**término datagrama. Indique cuando.**

PDU: Unidad de datos de protocolo.

Se llama datagrama cuando usamos el protocolo UDP (User Datagram Protocol), que técnicamente sigue siendo un segmento, pero al tener tan poca información se le dice Datagrama. También con SCTP.

**6. Describa el saludo de tres vías de TCP. ¿Se utiliza algo similar en UDP?**



TCP Establecimiento de Conexión

* Flags: SYN (Synchronize), ACK (Acknowledge) y RST (Reset).
* En el 3 segmento se puede enviar info.
* el ISN (Initial Sequence Number), se utiliza un contador que se incrementa cada 4 mseg.
* RST si no hay proceso en estado LISTEN.
* Open Pasivo (servidor) y Activo (cliente).
* Open simultaneo

**De la practica larga:**

Cuando dos hosts se comunican mediante TCP, se establece una conexión antes de enviar datos. Al completar la transferencia, se cierran las sesiones y la conexión finaliza. Los mecanismos de conexión y sesión habilitan la función de confiabilidad del TCP.

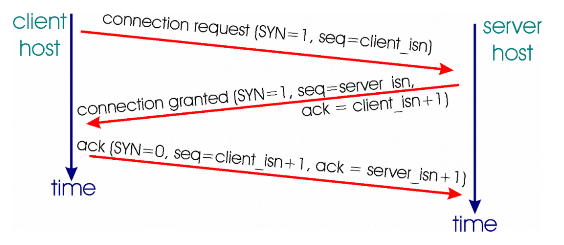
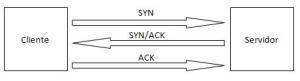
Para establecer la conexión se realiza el **saludo de tres vías** oacuerdo en tres fases. Los bits de control en el encabezado TCP indican el progreso y estado de la conexión.

El cliente envía un segmento TCP especial; el servidor responde con un segundo segmento TCP especial (Estos dos no llevan datos) y, por último, el cliente responde de nuevo con tercer segmento especial, que puede llevar datos de la aplicación.

1. Un cliente TCP comienza el enlace de tres vías enviando un segmento con SYN (Sincronizar números de secuencia) establecido, indicando un valor inicial en el campo de número de secuencia del encabezado, conocido como número de secuencia inicial (ISN), se elige aleatoriamente y rastrea el flujo de datos desde el cliente al servidor para esta sesión.
2. El servidor TCP reconoce la recepción del segmento SYN del cliente para establecer la sesión, enviando un segmento al cliente con el señalizador ACK establecido indicando que el número de acuse de recibo es significativo. Con esto, el cliente entiende que el servidor recibió el SYN enviado. El servidor manda su propio SYN.
3. Por último, el cliente envía un segmento que contiene un ACK como que actúa como respuesta al SYN del servidor. Pueden no enviarse datos en este segmento.

El valor del ACK (número de acuse de recibo) contiene uno más que el número de secuencia inicial (es decir, **ACK = SEQ\_SV + 1**) recibido. Una vez establecidas ambas sesiones, todos los segmentos adicionales que se intercambien tendrán establecido el señalizador ACK.

Completado esto, cliente y servidor pueden enviarse segmentos que contengan datos.



* **ACK o “acknowledge” (1 bit):** El campo con el número de acuse de recibo es válido (si no, es ignorado). Es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado.
* **SYN o “synchronize” (1 bit):** Activa/desactiva la sincronización de los números de secuencia. Se usa para sincronizar los números de secuencia en tres tipos de segmentos: petición de conexión, confirmación de conexión (con ACK activo) y la recepción de la confirmación (con ACK activo).
* **RST o “reset” (1 bit):** En 1, termina la conexión sin esperar respuesta. Es un bit que se encuentra en el campo del código en el protocolo TCP, y se utiliza para reiniciar la conexión. Se usa cuando a un servidor le llega un paquete a un puerto no válido: este responde con el RST activado.

Otra práctica:

La secuencia es:

* El cliente envía un segmento al servidor (SYN = true; ACK = false) y espera un segmento de respuesta. El segmento de solicitud tiene Número de secuencia inicial (ISN), que es un número aleatorio de 32 bits, generado por el cliente.
* Luego de enviarse, queda incrementado en 1
* Flag SYN en 1: Le indica a un extremo que este segmento contiene el ISN usado por el otro extremo, y se lo está enviando para sincronizarlos
* Longitud máxima de segmento: Cantidad máxima de bytes que un extremo puede enviar y recibir. Se almacena en el campo Options
* Tamaño de la ventana de recepción: Cantidad máxima de bytes que un extremo puede recibir. Se almacena en su campo respectivo
* El servidor lo recibe y le responde con el segmento de respuesta (SYN = true; ACK = true), que contiene: Número de secuencia inicial (ISN), que es un número aleatorio de 32 bits, generado por el servidor. Luego de enviarse, queda incrementado en 1, porque el hecho de enviarlo “consume” una unidad. Cuando se usa FIN también incrementa 1 (igual caso que el SYN) **VER ESTO POR QUE EN EL OTRO LO INCREMENTA EN EL TERCERO**

[**Protocolo de enlace triple a través de TCP/IP - Windows Server | Microsoft Learn**](https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/three-way-handshake-via-tcpip)

****

* Número de recibo del segmento: Almacena el número de segmento, del siguiente byte que el receptor espera recibir. El valor que le pone el servidor, es el recibido por el cliente, incrementado en 1.
* Flag ACK en 1: Indica que el número de recibo de este segmento es válido
* La conexión Full Duplex queda establecida.

En UDP no se usa, ya que es un protocolo sin conexión previa

**7. Investigue qué es el ISN (Initial Sequence Number). Relaciónelo con el saludo de tres vías.**

Número de 32 bits (0 - 4.294.967.265), generado aleatoriamente por el emisor, que se asigna para cada nueva conexión TCP (Al inicio de un saludo de tres vías). Es único para cada conexión y cada dispositivo este número se le asigna al ACK, a partir de ahí el ACK va a ir aumentando.

El número de secuencia del cliente es distinto al número de secuencia del servidor, pero se relacionan los ack: Si el ack del servidor es 17, quiere decir que espera el seq 17.

**8. Investigue qué es el MSS. ¿Cuándo y cómo se negocia?**

MSS, o tamaño máximo de segmento, es la cantidad máxima de bytes o carga útil de datos más grande que un dispositivo aceptará de una conexión de red, es decir, lo máximo que se puede enviar o recibir.

Si se recibe una cantidad mayor, se produce **fragmentación**, lo cual suma overhead.

Se envía dentro de Options, ya que sólo se negocia una vez por conexión.

Según la RFC-879, el valor mínimo recomendado es de 536 bytes, usando una Unidad de Transmisión Máxima (MTU) de 576 bytes, y 40 bytes de cabeceras TCP/IP

MTU - (encabezado TCP + encabezado IP) = MSS

El MSS se negocia en el saludo de 3 vías.

**9. Utilice el comando ss (reemplazo de netstat) para obtener la siguiente información de su PC:**

**a. Para listar las comunicaciones TCP establecidas.**

ss –t

ss --tcp –processes

**b. Para listar las comunicaciones UDP establecidas.**

ss –u

ss --udp –processes

**c. Obtener sólo los servicios TCP que están esperando comunicaciones**

ss -t –l

ss --tcp --processes –listening

**d. Obtener sólo los servicios UDP que están esperando comunicaciones.**

ss -u –l

ss --udp --processes –listening

**e. Repetir los anteriores para visualizar el proceso del sistema asociado a la conexión.**

ss -t -l -p

ss -u -l -p

El parámetro -p: Show process using socket. Para que muestre la información de interés es necesario ser sudo.

**f. Obtenga la misma información planteada en los items anteriores usando el comando netstat.**

Inciso A: netstat –t

Inciso B: netstat -u

Inciso C: netstat -t -l

Inciso D: netstat -u -l

Inciso E: netstat -t -l -p

netstat -u -l –p

netstat --all --tcp

netstat --all --udp

netstat --listening --tcp

netstat --listening --udp

**10. ¿Qué sucede si llega un segmento TCP con el flag SYN activo 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)?**

No se podrá efectuar la conexión, ya que debe haber un proceso (con un socket) escuchando para aceptar el segmento SYN, dando comienzo al saludo de tres vías.

El host enviará al origen un segmento especial de reinicio. Este segmento TCP tiene el bit indicador RST

puesto a 1. Por tanto, cuando un host envía un segmento de reinicio, le está diciendo al emisor “No tengo un socket para ese segmento. Por favor, no reenvíes el segmento.”

Agrego caso UDP: Cuando un host recibe un paquete UDP en el que el número de puerto de destino no se

corresponde con un socket UDP activo, el host envía un datagrama ICMP especial (puerto inalcanzable).

**a. Utilice hping3 para enviar paquetes TCP al puerto destino 22 de la máquina virtual con el flag SYN**

**activado.**

Hping3 es una aplicación de terminal para Linux que permite analizar y ensamblar paquetes TCP/IP. A diferencia de un Ping convencional que se utiliza para enviar paquetes ICMP, esta aplicación permite el envío de paquetes TCP, UDP y RAW-IP.

Los campos de información que se maneja con el comando hping3 son:

● id es el campo ip id.

● win representa el tamaño de la ventana TCP. Indica la capacidad que tiene la aplicación del otro lado para recibir datos. Por ejemplo, win=20 indica que la aplicación puede recibir 20 datos. Al momento de enviarle datos a esta aplicación, el valor de win se irá decrementando (porque está recibiendo, y debe procesarlos). A medida que los procesa, el valor de win se incrementará y puede alcanzar su límite máximo. Esto se da porque la aplicación cuenta con un buffer limitado.

● rtt es el round trip time en milisegundos, es decir, tiempo que un paquete de datos tarda en volver a su emisor habiendo pasado por su destino.

● If the reply contains DF the IP header has the don't fragment bit set.

● len is the size, in bytes, of the data captured from the data link layer excluding the data link header size.

● flags are the TCP flags, R for RESET, S for SYN, A for ACK, F for FIN, P for PUSH, U for URGENT, X for not standard 0x40, Y for not standard 0x80.

● ttl: tiempo de vida. Evita que un paquete quede dando vuelta por la red indefinidamente.

*sudo hping3 localhost --destport 22 –syn //o sudo hping3 -S localhost -p 22*

HPING localhost (lo 127.0.0.1): S set, 40 headers + 0 data bytes

len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=22 flags=**SA** seq=0 win=65495 rtt=7.7 ms

len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=22 flags=**SA** seq=1 win=65495 rtt=3.5 ms

len=44 ip=127.0.0.1 ttl=64 DF id=0 sport=22 flags=**SA** seq=2 win=65495 rtt=3.2 ms

^C

--- localhost hping statistic ---

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 3.2/4.8/7.7 ms

**b. Utilice hping3 para enviar paquetes TCP al puerto destino 40 de la máquina virtual con el flag SYN**

**activado.**

*sudo hping3 localhost --destport 40 –syn //o sudo hping3 -S localhost -p 40*

HPING localhost (lo 127.0.0.1): S set, 40 headers + 0 data bytes

len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=40 flags=**RA** seq=0 win=0 rtt=3.9 ms

len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=40 flags=**RA** seq=1 win=0 rtt=3.7 ms

len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=40 flags=**RA** seq=2 win=0 rtt=7.4 ms

^C

--- localhost hping statistic ---

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 3.7/5.0/7.4 ms

**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).**

En el primer caso, el puerto está abierto. El servidor responde con los flags **SA** (SYN y ACK) activados, lo que significa que es un segmento de respuesta, y que ese puerto está abierto → se puede establecer la conexión

En el segundo caso, el puerto está cerrado. El servidor responde con los flags **RA** (RST y ACK) activados, lo que significa que es un segmento de cierre de conexión forzada, porque ese puerto está cerrado→ no se establece la conexión porque no hay nadie escuchando

* Len: En el primer caso el tamaño en bytes es 44, y en el segundo 40.
* Sport: la diferencia se da por la solitud en el comando. En el primer caso se pide el puerto 22 y en el segundo el 40.
* Id: en el primer caso, siempre es 0. En el segundo caso va variando.
* Win: en el primer caso, nunca es 0. En el segundo sí.

**11. ¿Qué sucede si llega un datagrama UDP a un host que no tiene ningún proceso esperando en el puerto destino de dicho datagrama (es decir, que dicho puerto no está en estado LISTEN)?**

Cuando un host recibe un paquete UDP en el que el número de puerto de destino no se corresponde con un socket UDP activo, el host envía un datagrama ICMP especial (port unreachable, o puerto inalcanzable).

**a. Utilice hping3 para enviar datagramas UDP al puerto destino 5353 de la máquina virtual.**

*sudo hping3 localhost --destport 5353 –udp //o sudo hping3 localhost -p 68 -2 (2 es para ponerlo en udp)*

HPING localhost (lo 127.0.0.1): udp mode set, 28 headers + 0 data bytes

^C

--- localhost hping statistic ---

**3 packets transmitted, 0 packets received, 100% packet loss**

round-trip min/avg/max = 0.0/0.0/0.0 ms

Nota: No hay respuesta.

**b. Utilice hping3 para enviar datagramas UDP al puerto destino 40 de la máquina virtual.**

*sudo hping3 localhost --destport 40 –udp//o sudo hping3 localhost -p 40 -2*

HPING localhost (lo 127.0.0.1): udp mode set, 28 headers + 0 data bytes

**ICMP Port Unreachable from ip=127.0.0.1 name=localhost**

status=0 port=2330 seq=0

**ICMP Port Unreachable from ip=127.0.0.1 name=localhost**

status=0 port=2331 seq=1

**ICMP Port Unreachable from ip=127.0.0.1 name=localhost**

status=0 port=2332 seq=2

^C

--- localhost hping statistic ---

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 3.8/6.6/8.3 ms

En este caso sí hay respuesta: “ICMP Port Unreachable from ip=127.0.0.1 name=localhost”

**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).**

En el primer caso “hay un servicio escuchando en el puerto”, por lo que se transmitieron todos los paquetes, pero no se puede saber si los recibió correctamente o se perdieron en el camino ya que UDP no tiene mensajes de retorno por reconocimiento

En el segundo caso, como no hay un servicio escuchando en el puerto, no se puede alcanzar este y UDP responde informando esto con un paquete ICMP Port Unreachable

**12. Investigue los distintos tipos de estado que puede tener una conexión TCP.**

**Ver** [**https://users.cs.northwestern.edu/~agupta/cs340/project2/TCPIP\_State\_Transition\_Diagram.pdf**](https://users.cs.northwestern.edu/~agupta/cs340/project2/TCPIP_State_Transition_Diagram.pdf)

Literalmente el link de arriba traducido:

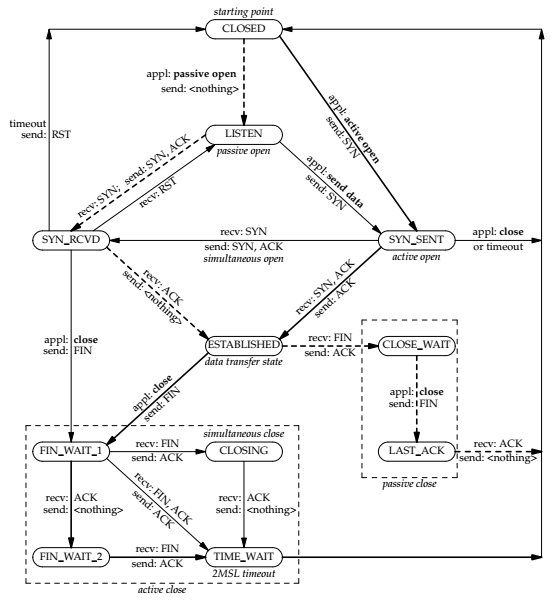
Una conexión tiene de una serie de estados durante su vida útil:

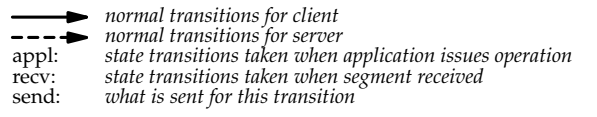
* LISTEN: espera una solicitud de conexión desde cualquier puerto TCP remoto.
* SYN-SENT: espera de una solicitud de conexión coincidente después de haber enviado una solicitud de conexión.
* SYN-RECEIVED: la espera de un reconocimiento de solicitud de conexión de confirmación después de tener ambos recibido y enviado una solicitud de conexión.
* ESTABLISHED: conexión abierta, los datos recibidos pueden ser entregados al usuario. el estado normal para la fase de transferencia de datos de la conexión.
* FIN-WAIT-1: espera de una solicitud de terminación de conexión del TCP remoto, o un acuse de recibo de la solicitud de terminación de conexión enviada previamente.
* FIN-WAIT-2: espera de una solicitud de terminación de conexión del TCP remoto.
* CLOSE-WAIT: espera de una solicitud de terminación de conexión del usuario local.
* CIERRE: espera de una confirmación de solicitud de terminación de conexión del control remoto TCP.
* LAST-ACK: espera de un reconocimiento de la solicitud de finalización de la conexión previamente enviado al TCP remoto (que incluye un reconocimiento de su terminación de conexión

pedido).

* TIME-WAIT: representa esperar a que pase suficiente tiempo para asegurarse de que el TCP remoto recibió el acuse de recibo de su solicitud de terminación de conexión.
* CERRADO/CLOSED: Estado ficticio que representa el estado cuando no hay TCB, y por lo tanto, no hay conexión representa ningún estado de conexión en absoluto.

Una conexión TCP progresa de un estado a otro en respuesta a eventos. Los eventos son las llamadas del usuario, OPEN, SEND, RECEIVE, CLOSE, ABORT y STATUS; los segmentos entrantes, particularmente aquellos que contienen las banderas SYN, ACK, RST y FIN; y tiempos de espera.





Traducción de las flechitas: transiciones normales para el cliente

transiciones normales para el servidor

appl: transiciones de estado tomadas cuando la aplicación emite una operación

recv: transiciones de estado tomadas cuando se recibió el segmento

enviar: lo que se envía para esta transición

**13. Use CORE para armar una topología como la siguiente, sobre la cual deberá realizar:**

**a. 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’.**

root@Servidor:/tmp/pycore.34739/Servidor.conf# ncat --listen --keep-open 8001

root@Servidor:/tmp/pycore.34739/Servidor.conf# ss -nat

State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

root@Cliente:/tmp/pycore.34739/Cliente.conf# ss -nat

State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

\*-\*-\*-\*-

NOTAS:

- ss is another utility to investigate sockets

- ss is used to dump socket statistics. It allows showing information similar to

netstat. It can display more TCP and state informations than other tools.- El comando watch ejecuta un comando repetidas veces (en este caso “n1” = “cada

un segundo”). Haciendo “watch -n1 ’ss -nat’” se está ejecutando el comando ss para

verificar el estado de las conexiones.

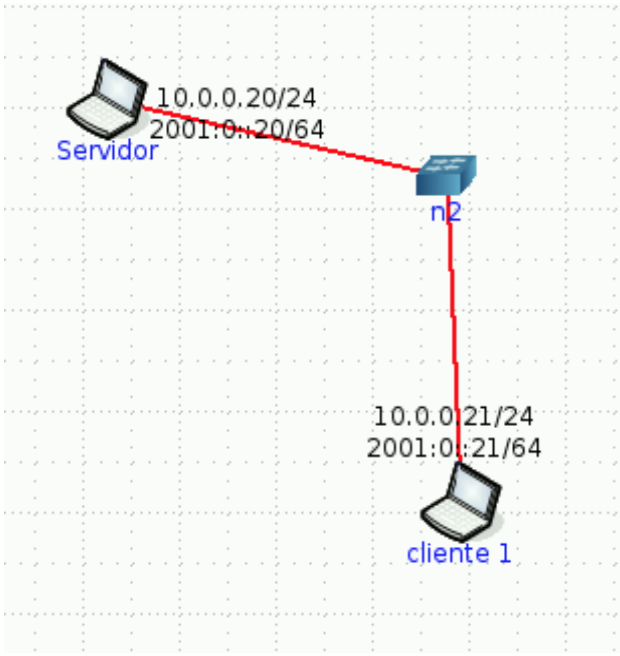
- Una vez graficada la topologìa le di play al ‘run session’ y al hacer click derecho

sobre cada host optè por la opción view shell para mandarle el comando

especificado tanto al cliente como al server.

**b. En Servidor, utilice la herramienta ncat para levantar un servicio que escuche en el puerto 8001/TCP.**

**Utilice la opcion -k para que el servicio sea persistente. Verifique el estado de las conexiones.**



root@Cliente:/tmp/pycore.34739/Cliente.conf# ncat 10.0.0.10 8001

root@Servidor:/tmp/pycore.34739/Servidor.conf# ss -nat

State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

LISTEN 0 10 0.0.0.0:8001 0.0.0.0:\*

LISTEN 0 10 [::]:8001 [::]:\*

\*-\*-\*-\*-\*

Se utilizó el comando ncat -l -k 8001 (en una nueva terminal).

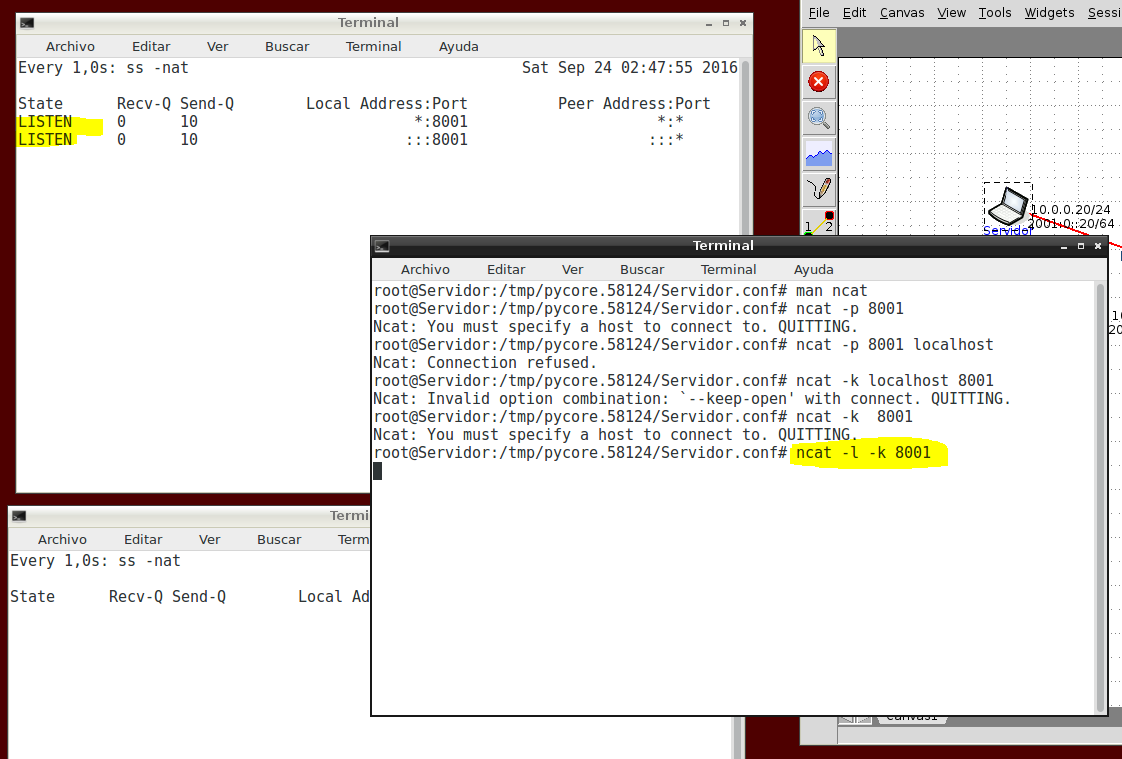
→ -l es para LISTEN

→ -k es para que las conexiones sean persistentes

→ Puerto 8001

→ Protocolo TCP (por defecto)

Ahora el servidor aparece escuchando en el puerto 8001



**c. Desde CLIENTE1 conectarse a dicho servicio utilizando también la herramienta ncat. Inspeccione**

**el estado de las conexiones.**

root@Cliente:/tmp/pycore.34739/Cliente.conf# ncat 10.0.0.10 8001

root@Servidor:/tmp/pycore.34739/Servidor.conf# ss -nat

State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

LISTEN 0 10 0.0.0.0:8001 0.0.0.0:\*

ESTAB 0 0 10.0.0.10:8001 10.0.0.20:46858

LISTEN 0 10 [::]:8001 [::]:\*

root@Cliente:/tmp/pycore.34739/Servidor.conf# ss -nat

State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

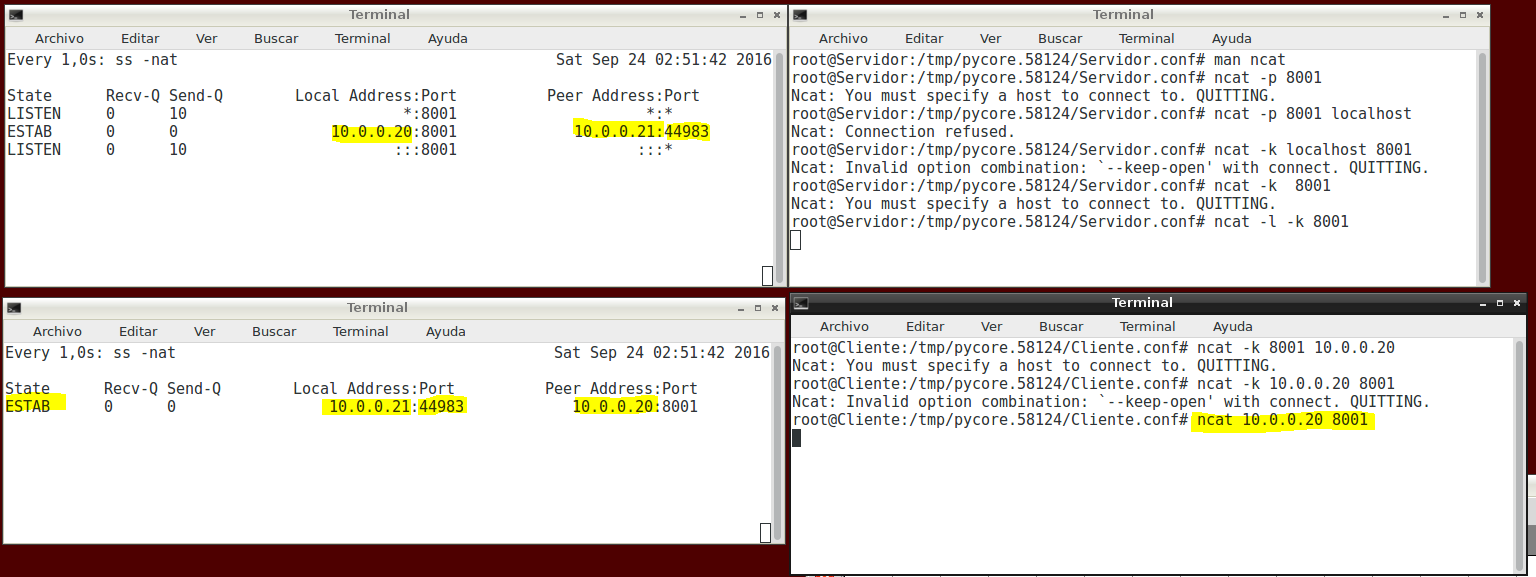
ESTAB 0 0 10.0.0.20:46858 10.0.0.10:8001

\*-\*-\*-\*-\*-\*-

Se utilizó de nuevo el comando ncat pero esta vez indicando el host destino y el puerto:

Ncat 10.0.0.20 8001

NOTA: ncat - Concatenate and redirect sockets



**d. 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?**

root@Cliente:/tmp/pycore.34739/Cliente.conf# ncat 10.0.0.10 8001

root@Servidor:/tmp/pycore.34739/Servidor.conf# ss -nat

State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

LISTEN 0 10 0.0.0.0:8001 0.0.0.0:\*

ESTAB 0 0 10.0.0.10:8001 10.0.0.20:46858

ESTAB 0 0 10.0.0.10:8001 10.0.0.20:37716

LISTEN 0 10 [::]:8001 [::]:\*

root@Cliente:/tmp/pycore.34739/Cliente.conf# ss -nat

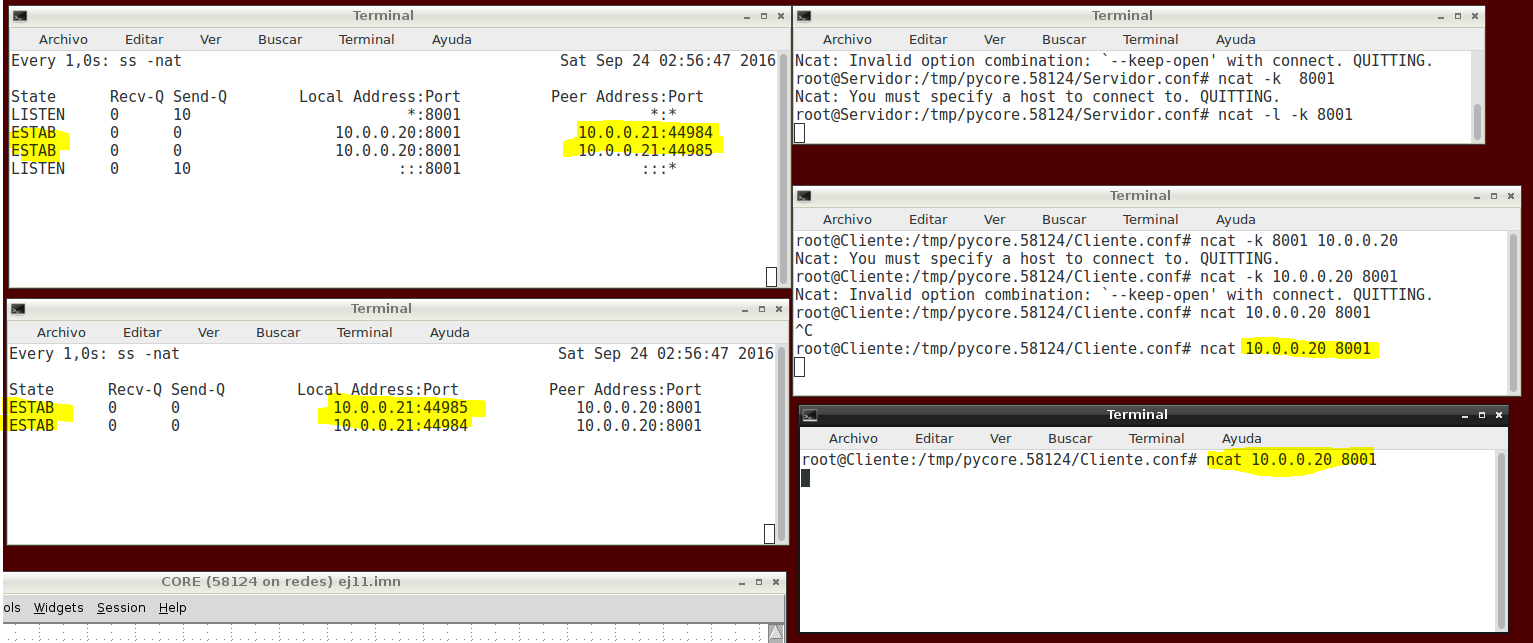
State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

ESTAB 0 0 10.0.0.20:46858 10.0.0.10:8001

ESTAB 0 0 10.0.0.20:37716 10.0.0.10:8001

-\*-\*-\*-\*-

Cambia el puerto origen, así es como se identifican.



**e. En base a lo observado en el item 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?**

Es posible, porque en los headers de los segmentos transferidos en cada conexión, se guarda el puerto origen y destino (que entre ambas forman un identificador unívoco)

\*-\*-\*-\*-\*

Sí, es posible iniciar más de una conexión desde el cliente al servidor en el mismo puerto destino, ya que lo que termina identificando a cada una es el puerto origen, el cual es distinto. Es por esto que no se mezclan los datos de una con otra, ya que en la cabecera de los segmentos figuran ips origen destino y puertos origen destino.Aclaración: Anteriormente vimos que en UDP el campo puerto origen es opcional.

Esto NO es algo normal. Si no tenemos el puerto destino, no podemos enviarle información, y por ende, siempre se configura.

**f. Analice en el tráfico de red, los flags de los segmentos TCP que ocurren cuando:**

**i. Cierra la última conexión establecida desde CLIENTE1. Evalúe los estados de las conexiones**

**en ambos equipos.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Paquete** | **Sentido** | **URG** | **ACK** | **PSH** | **RST** | **SYN** | **FIN** |
| 1 | C → S | false | false | false | false | true | false |
| 2 | S → C | false | true | false | false | true | false |
| 3 | C → S | false | true | false | false | false | false |

El estado de las conexiones es similar a 13.C)

-\*-\*-\*-\*--\*-

Apreté control C en una de las terminales del cliente donde había hecho la conexión y esa

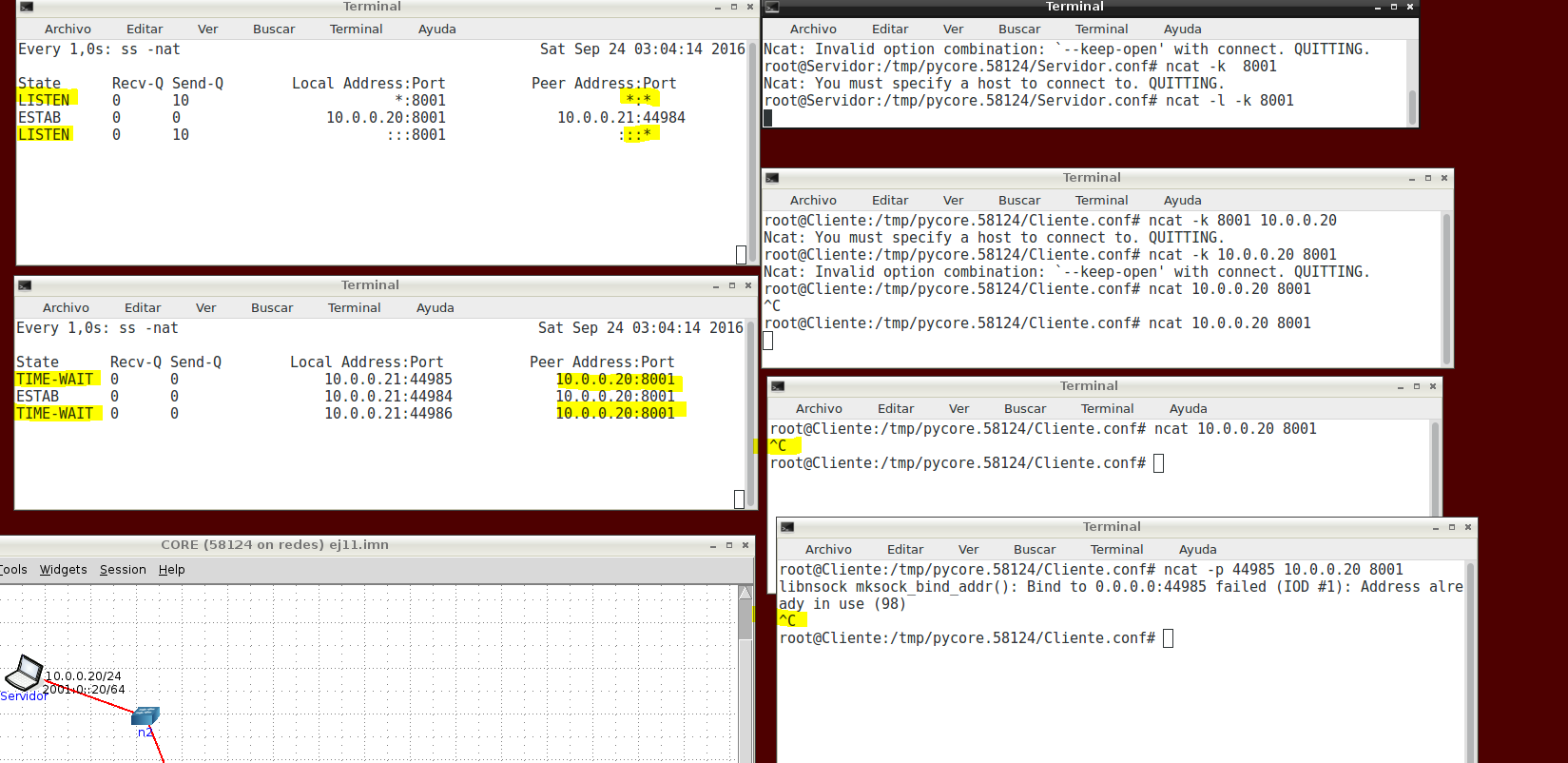
fue la forma de cerrarla.

El servidor dejo de mostrar estado de ESTABLISHED en ese puerto origen y el cliente

mostró durante unos minutos el estado TIME-WAIT en la conexión y luego nada.

Si el cliente cierra la conexión, desde el lado del cliente se puede ver el estado TIME-WAIT

por unos segundos hasta que desaparece de la lista.



**ii. Corta el servicio de ncat en el servidor (Ctrl+C). Evalúe los estados de las conexiones en ambos**

**equipos.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Paquete** | **Sentido** | **URG** | **ACK** | **PSH** | **RST** | **SYN** | **FIN** |
| 1 | S → C | false | true | false | false | false | true |
| 2 | S → C | false | true | false | true | false | false |
| 3 | C → S | false | true | false | false | false | false |

Estado de las conexiones:

root@Servidor:/tmp/pycore.34739/Servidor.conf# ss -nat

State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

root@Cliente:/tmp/pycore.34739/Servidor.conf# ss -nat

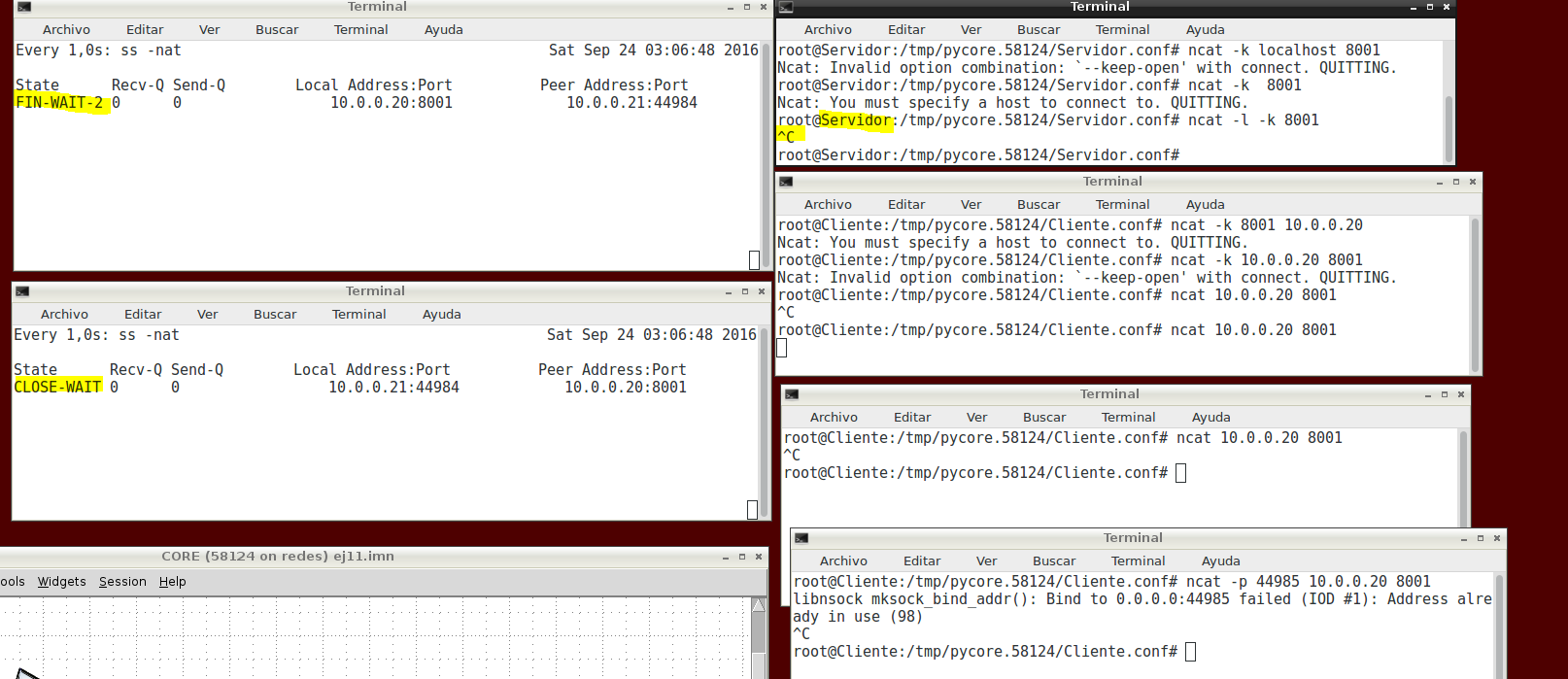
State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

CLOSE-WAIT 0 0 10.0.0.20:43456 10.0.0.10:8001

CLOSE-WAIT 0 0 10.0.0.20:41442 10.0.0.10:8001

CLOSE-WAIT 0 0 10.0.0.20:46724 10.0.0.10:8001

--\*-\*-\*-\*-\*-\*-\*-



Si la conexión se cierra primero desde el servidor, entonces se queda en estado FIN-WAIT y

hasta que no se cierra desde el cliente no se deja de listar; desde el cliente se puede ver el

estado CLOSE-WAIT.

**iii. Cierra la conexión en el cliente. Evalúe nuevamente los estados de las conexiones.**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Paquete** | **Sentido** | **URG** | **ACK** | **PSH** | **RST** | **SYN** | **FIN** |
| 1 | C → S | false | true | false | false | false | true |
| 2 | S → C | false | true | false | false | false | true |
| 3 | C → S | false | true | false | false | false | false |

El estado de la conexión cliente es similar a 13.A)

El de servidor, no:

root@Servidor:/tmp/pycore.34739/Servidor.conf# ss -nat

State Recv-Q Send-Q Local Address:Port Peer Address:Port Process

LISTEN 0 128 0.0.0.0:22 0.0.0.0:\*

LISTEN 0 10 0.0.0.0:8001 0.0.0.0:\*

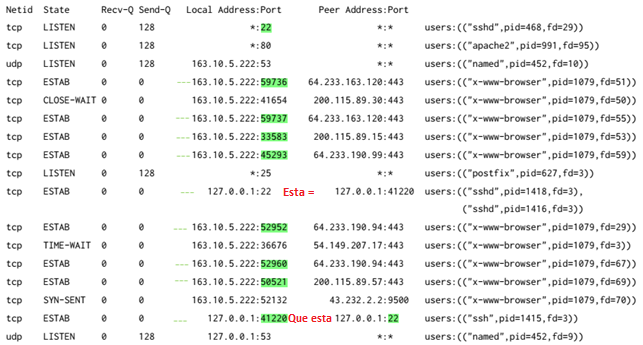
CLOSE-WAIT 1 0 10.0.0.10:8001 10.0.0.20:60136

LISTEN 0 128 [::]:22 [::]:\*

LISTEN 0 10 [::]:8001 [::]:\*

Uno puede quedar en TIME-WAIT, porque espera recibir la confirmación de cierre del otro extremo (segmento que aún no llegó), o por si hay segmentos aún viajando (si justo se abre una nueva conexion en ese puerto, para que no se confundan los paquetes)

**14. Dada la siguiente salida del comando ss, responda:**

****

**a. ¿Cuántas conexiones hay establecidas?**

8. Una de las ESTAB está repetida, se ve desde ambos lados (127.0.0.1:41220 a 127.0.0.1:22)

**b. ¿Cuántos puertos hay abiertos a la espera de posibles nuevas conexiones?**

5, considera LISTEN

**c. El cliente y el servidor de las comunicaciones HTTPS (puerto 443), ¿residen en la misma máquina?**

No, el cliente y el servidor no residen en la misma máquina, ya que el local address y el peer address son diferentes (Distintas IPs)

**d. El cliente y el servidor de la comunicación SSH (puerto 22), ¿residen en la misma máquina?**

Residen en la misma, ya que tienen misma IP (127.0.0.1, o localhost)

**e. Liste los nombres de todos los procesos asociados con cada comunicación. Indique para cada uno**

**si se trata de un proceso cliente o uno servidor.**

|  |  |  |
| --- | --- | --- |
| **Proceso** | **Puerto local** | **Rol** |
| x-www-browser | 59736 | Cliente |
| x-www-browser | 59737 | Cliente |
| x-www-browser | 33583 | Cliente |
| x-www-browser | 45293 | Cliente |
| sshd | 22 | Servidor |
| x-www-browser | 52952 | Cliente |
| x-www-browser | 52960 | Cliente |
| x-www-browser | 50521 | Cliente |
| ssh | 41220 | Cliente |

SSH funciona mediante la conexión de un programa cliente a un servidor ssh, llamado sshd.

ssh era el programa cliente.

Asumo que se da cuenta si es cliente o servidor porque el cliente está desde un puerto no privilegiado (Mayor a 1023).

**f. ¿Cuáles conexiones tuvieron el cierre iniciado por el host local y cuáles por el remoto?**

|  |  |  |  |
| --- | --- | --- | --- |
| **Proceso** | **Puerto local** | **Estado** | **Cerrado por** |
| x-www-browser | 41654 | CLOSE-WAIT | Cliente |
| x-www-browser | 36676 | TIME-WAIT | Servidor |

* CLOSE-WAIT representa la espera de una solicitud de terminación de conexión del usuario local.
* El CIERRE representa la espera de una confirmación de solicitud de terminación de conexión del control remoto TCP.
* TIME-WAIT representa esperar a que pase suficiente tiempo para asegurarse de que el TCP remoto recibió el acuse de recibo de su solicitud de terminación de conexión.

**g. ¿Cuántas conexiones están aún pendientes por establecerse?**

1

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

**servidor# ss -natu | grep 110**

**tcp LISTEN 0 0 \*:110 \*:\***

**tcp SYN-RECV 0 0 157.0.0.1:110 157.0.11.1:52843**

**cliente# ss -natu | grep 110**

**tcp SYN-SENT 0 1 157.0.11.1:52843 157.0.0.1:110**

**a. ¿Qué segmentos llegaron y cuáles se están perdiendo en la red?**

El primer mensaje (cliente a servidor) llega correctamente, el servidor lo procesa

La respuesta del servidor es la que se pierden en el camino

O

Creería que se están perdiendo todos los datos, porque el servidor no estan estado de

Establecida.

**b. ¿A qué protocolo de capa de aplicación y de transporte se está intentando conectar el cliente?**

El protocolo de la capa de aplicación y la de transporte, te lo indica el número de puerto al

que se están conectando en este caso es el 110: POP3

De aplicación: POP

De transporte: TCP (porque existe el saludo de tres vías, con sus estados, y además la primera columna lo dice explícitamente)

**c. ¿Qué flags tendría seteado el segmento perdido?**

SYN y ACK en 1.