## **LABORATORIO 4 - TRANSPORTE**

Vamos a emular en Packet Tracer una red con una PC y dos servidores. La misma red del LAB1: (1 PC y 2 servidores. IP: 192.168.0.1 (PC) 192.168.0.2 (Servidor Web www.mipc.com) y 192.168.0.3 (Servidor DNS)).

En este caso analizaremos qué tipos de protocolos de transporte utilizan los protocolos de aplicación y cómo es el intercambio de mensajes en cada caso.

## Manejo de el modo Simulación:

Para este ejercicio vamos a utilizar la característica de "simulación" del emulador Packet Tracer.

Simulación: Esta opción se selecciona en el borde inferior derecho de la aplicación:



Esto nos permitirá ejecutar paso a paso el intercambio de mensajes y seleccionar qué protocolos nos interesa observar.

<b>X</b>					i) ?
New Cluster Move Object	Set Tiled Backgrou	nd Vie	ewport	Environment:	21:00:00
<ul> <li>Simu</li> </ul>	ulation Panel			₽×	173
Eve	ent List				
≡ Vis.	Time(sec) Last Devi	ce At Device Type	Info		
	Protocolos				×
	seleccionados, a		Con este b	oton agrega o	Q
	capturar		todos los p	rotocolos	
			<u> </u>		
			1	Captured to:	
Res	et Simulation	ant Delay		(no captures)	
-PT			1		
C	v Controls				
	y controis	Auto Contune / D		no / Familiand	52×
Seleccion	Back			re / Forward	
Individual de					
Protocolos					
Eve	ent List Filters - Visible E	vents			
ACL	Filter, ARP, BGP, CDP, DH	CP, DHCPv6, DNS, D	TP, EIGRP, EIGR	v6, FTP, H.323,	
HSR	P. HSRPv6, HTTP, HTTPS,	, ICMP, ICMPv6, IPS	ec, ISAKMP, IOE	LACP, LLDP, NDP,	
SCC	P, SMTP, SNMP, SSH, ST	P, SYSLOG, TACACS	, TCP, TFTP, Te	het, UDP, VTP	
	Edit Filters		Show All/N	one	
-					
e / Play Capture / Forward			Event I	List Simulat	ion
Generic Generic 1841 2620004	2621XM 2811				
	2911				

Ahora, con "Show all/none" deseleccionamos todos los protocolos a monitorear y en "Edit Filters" elegimos los protocolos que nos interesan para el trabajo. (Recuerden que estos están listados en alguna de las 3 solapas, dependiendo del tipo de protocolo de aplicación que sea).

Ever	nt List					
Vis.	Time(sec)	Last De	vice At Devi	ce Type Info		
			~			
		(	IPv4 IP	v6 Misc		
			ARP	BGP	DHCP	
		1	DNS	EIGRP	HSRP	
			TIONT	OSPE	RIP	
Rese	t Simulation	Cc				
Play	Controls					
,	Back					
Ever	n <mark>t List Filte</mark> rs	- Visibl				
lone.			Edit ACL Filters			
Edit Filters		t Filters	Show All/None			
			A			

Los botones "Auto capture/play" y "Capture/Forward" hace que la simulación paso a paso se inicie. El primero de las funciones lo realiza de forma automática con una demora de tiempo que podemos ajustar con la barra deslizable. La segunda opción lo ejecuta paso a paso a medida que la presionamos.

Los mensajes se ven como sobres () que circulan por la red. Estos los podemos abrir y observar su contenido en cada capa del modelo OSI y cada protocolo para esa capa.

OSI Model	Outbound PDU Detai	ils	0.9	SI Model Outbound PDU Details
At Device: I Source: PC Destination:	PC : 192.168.0.3		P	PDU Formats           TYPE:         DATA (VARIABLE LENGTH)         FCS:           0x800         0x0
n Layers		Out Layers		
		Layer 7: DNS		
		Layer6		10
.ayer5		Layer5		P 0 4 8 16 10 31Bits
ayer4		Layer 4: UDP Src Port: 1026, Dst Port: 53		4 IHL DSCP: 0x0 TL: 56 ID: 0x7 0x0 0x0
ayer3		Layer 3: IP Header Src. IP: 192.168.0.1, Dest. IP: 192.168.0.3		TTL: 128 PRO: 0x11 CHKSUM SRC IP: 192.168.0.1
ayer2		Layer 2: Ethernet II Header 000C.85CA.EC68 >> 0001.63D5.12BE		OPT: 0x0 0x0 DATA (VARIABLE LENGTH)
ayer1.		Layer 1: Port(s): FastEthernet0		UDP 0 16 31Bits
The DNS	client sends a DNS que	ery to the DNS server.		SRC PORT: 1026 DEST PORT: 53 LENGTH: 0x24 CHECKSUM: 0x0 DATA (VARIABLE)
				DNS Header 0 1 5 8 9 12 15 Bits
				OPCODE A T R R Z RCODE QDCOUNT: 1 ANCOUNT: 0

Existen casos donde el mensaje atraviesa un dispositivo en el cual podemos ver el PDU entrante y el saliente del mismo. (Porque hay casos en que un dispositivo modifica las cabeceras de alguna de las capas).

Con los botones Previus y Netx Layer, vamos recorriendo las capas del modelo OSI de ese paquete y el emulador nos brinda información de la capa para ese mensaje.

## Desarrollo del Laboratorio:

El objetivo de este laboratorio es observar la operación de los protocolos de transporte.

Para esto usamos el Lab1 realizado, ponemos el PT en modo simulación. Seleccionamos los protocolos DNS y HTTP.

Ahora desde la PC accedemos al navegador y entramos a la pagina www.mipc.com y damos "GO".

Vamos a la simulación y por medio de Capture Forward hacemos avanzar la simulación!

## Análisis:

1- ¿Cuál es el protocolo de aplicación que primero vemos? ¿Cuál es el protocolo de transporte utilizado?

2- Observando el flujo de datos entre la PC y el servidor: ¿Cuál es la relación que podemos encontrar dentro de las cabeceras del mensaje? ¿Se realiza o no una conexión? Representar entre cuales sockets se realiza el intercambio.

3- En la cabecera de transporte el mensaje el campo DATA: ¿Qué representa? Represente el contenido que se transporta dentro del campo.

4- El mensaje que retorna desde el servidor a la PC: ¿Qué contenido trae en el protocolo de aplicación? ¿Qué cambio se observa en la cabecera de transporte?

5- ¿Cuál es el Segundo protocolo de aplicación? ¿Cuál es el protocolo de transporte utilizado?

6- El flujo de datos entre la PC y el servidor: ¿Cuál es la relación que podemos encontrar dentro de las cabeceras del mensaje? ¿Se realiza o no una conexión? Representar entre cuales sockets se realiza el intercambio.

7- ¿Se observa el saludo de 3 vías de TCP? ¿Estamos observando los mensajes de transporte?

8- Habilitamos ambos protocolos de transporte y nos aparecerá en el historial los mensajes de trasporte que no estábamos observando: ¿Aparecen nuevos mensajes de ambos protocolos de transporte? En caso negativo, ¿De cuál es el que no vemos? ¿Por qué? Representar entre cuáles sockets se realiza el intercambio.

9- ¿Cuáles son los ISN de la PC y el Server en el diálogo HTTP? ¿Qué flags están activos en el mensaje PC-SRV y cuáles en SRV-PC? . ¿A partir de qué número de secuencia de la PC podemos decir que a conexión está establecida? (Capture una imagen del mensaje).

10- ¿A partir de qué número de secuencia se inicia el cierre de la conexión? ¿Cuándo se da por cerrada? (Capture una imagen del mensaje).

11- Describa que da como resultado un netstat en el "Command Prompt" del servidor y del cliente.

12- Configuremos un nuevo cliente (con un nuevo IP y demás) y repetimos la experiencia, preparamos todo los dos navegadores abiertos, el PT en modo simulación (borrando los diálogos viejos con "Reset Simulation") y damos GO a las dos PC a la vez ¿Qué observamos? ¿Cuántas conexiones se establecen?

13- Si realizamos los netstat ¿Qué diferencias observamos? ¿Cuáles son las conexiones existentes durante la ejecución? Represente estas conexiones.