Escuela Politécnica Nacional
Facultad de Ingeniería Eléctrica y Electrónica Carrera de Ingeniería en Electrónica y Redes de Información
Laboratorio de Redes TCP/IP
http://detri.epn.edu.ec
Quito, Ecuador

LABORATORIO DE REDES TCP/IP

PRACTICA N: 03

FECHA: 21/11/2017

1. TEMA

Softwars para la captura de paquetes y simulación de redes

2. OBJETIVOS

- Aprender sobre el funcionamiento del analizador de protocolos Wireshark
- Aprender sobre el funcionamiento de un simulador de redes

3. PREPARATORIO

- Investigue qué es un analizador de protocolos, y para qué es útil.
- Consultar las características y funcionamiento del Software para análisis de paquetes **Wireshark**
- *Consultar los campos que constituyen un paquete IP*
- *Consultar los campos que constituyen un segmento TCP*
- *Consultar los campos que constituyen un segmento UDP*
- Investigue qué es un simulador de redes, y para qué es útil.
- Consultar las características y funcionamiento del software **Packet Tracer**

4. INFORMACIÓN

Esta práctica de laboratorio se va a realizar utilizando el sistema operativo Windows, y usando dos herramientas: Wireshark, la cual permite capturar paquetes, y Packet Tracer, la cual permite simular redes.

5. PROCEDIMIENTO

Verifique la conectividad a Internet, esto garantiza que su equipo tiene asignado una dirección IP. Para esto abra un explorador web y compruebe que puede acceder a www.google.com. Sino puede hacerlo pida ayuda al instructor**.**

Uso de Wireshark:

1) Ejecute el programa, debe ejecutarlo con permisos de administrador. Si no ejecuta el programa con privilegios de administrador, no verá ninguna interfaz al momento de querer captura tráfico.

2) Para iniciar una captura realice una de las siguientes tareas:

a. Escoja la opción del menú llamada “Capture”, y en el submenú seleccione la opción “Capture Options”.
b. En la barra de herramientas, busque el icono que tiene un círculo negro rodeado de una circunferencia negra.
c. En la pantalla principal, panel del lado izquierdo, escoja la opción “Capture Options”.
En la figura puede ver óvalos rojos sobre los elementos indicados.

3) En la ventana "Wireshark: Capture Options" realice lo siguiente:

a. Seleccione la tarjeta de red a usar para capturar los paquetes. Es probable que el nombre de la interfaz sea "Conexión de área local"

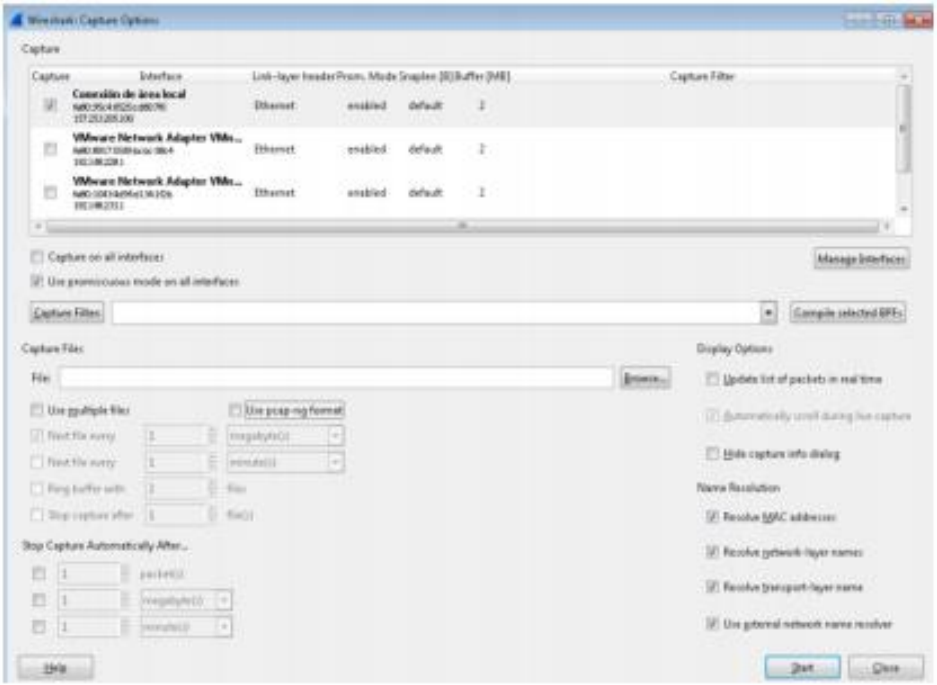
b. Seleccione la opción para capturar paquetes en modo promiscuo ("promiscous mode").

c. Verifique que no haya ningún filtro definido en "Capture Filter", si hay alguno elimínelo.

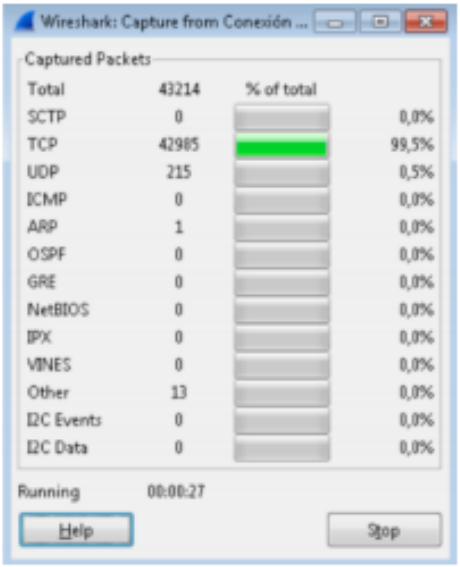
d. Verifique que las opciones seleccionadas en "Name Resolution" involucren: direcciones MAC, direcciones de capa de red y direcciones de capa de transporte.

e. Deseleccionar la opción "Use pcap-ng format".

f. Deseleccione las opciones bajo "Display Options".



4) Una vez que esté seguro, de que todo está de acuerdo a lo indicado, presione "Start". Luego de presionar "Start", Wireshark empezará a capturar paquetes y presentará una ventana con información general de los paquetes capturados, similar a la siguiente:



5) Genere una tabla indicando cuantos paquetes fueron capturados en TCP, UDP, ICMP y ARP.

6) Abra una consola y ejecute los siguientes comandos:
ping 127.0.0.1
ping www.google.com
ping www.epn.edu.ec
ping www.facebook.com
ping www.youtube.com

7) Abra un explorador web e ingrese a los siguientes sitios web:

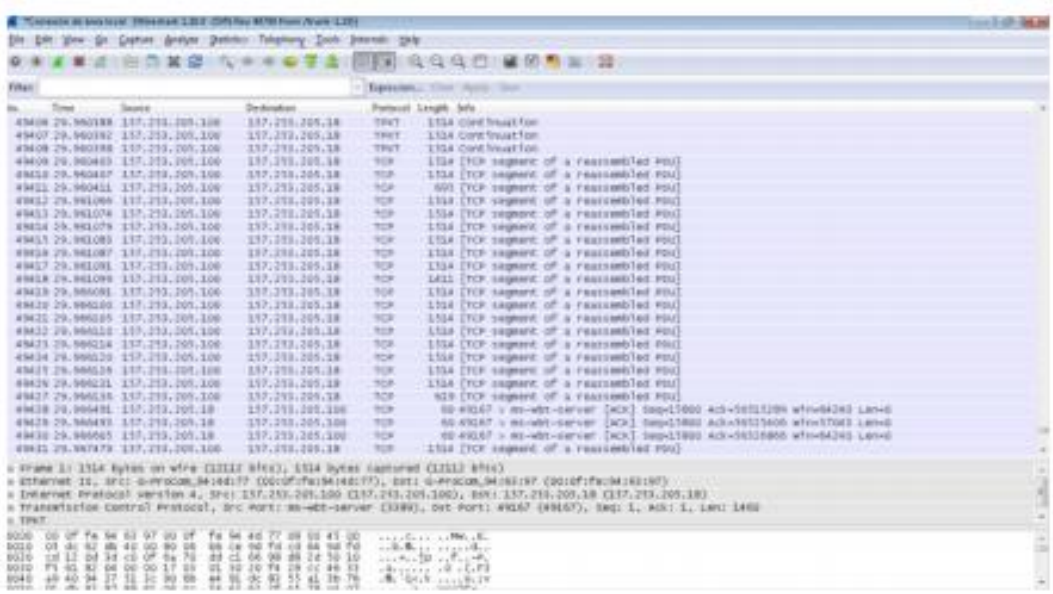
www.google.com
www.epn.edu.ec
www.facebook.com
www.youtube.com

8) Detenga la captura de paquetes, presionando en el botón "Stop", podrá ver una ventana con resultados similar a la siguiente:

a. En la parte superior de la pantalla principal verá un listado de todos los paquetes con información como Número de paquete, Tiempo, Origen, Destino, Protocolo, Longitud e Información.

b. Al seleccionar un paquete del listado, en la parte intermedia, aparecerá información detallada de cada campo que conforma el paquete.

c. En la parte inferior podrá ver la representación en hexadecimal del contenido del paquete, así como la interpretación en formato ASCII.



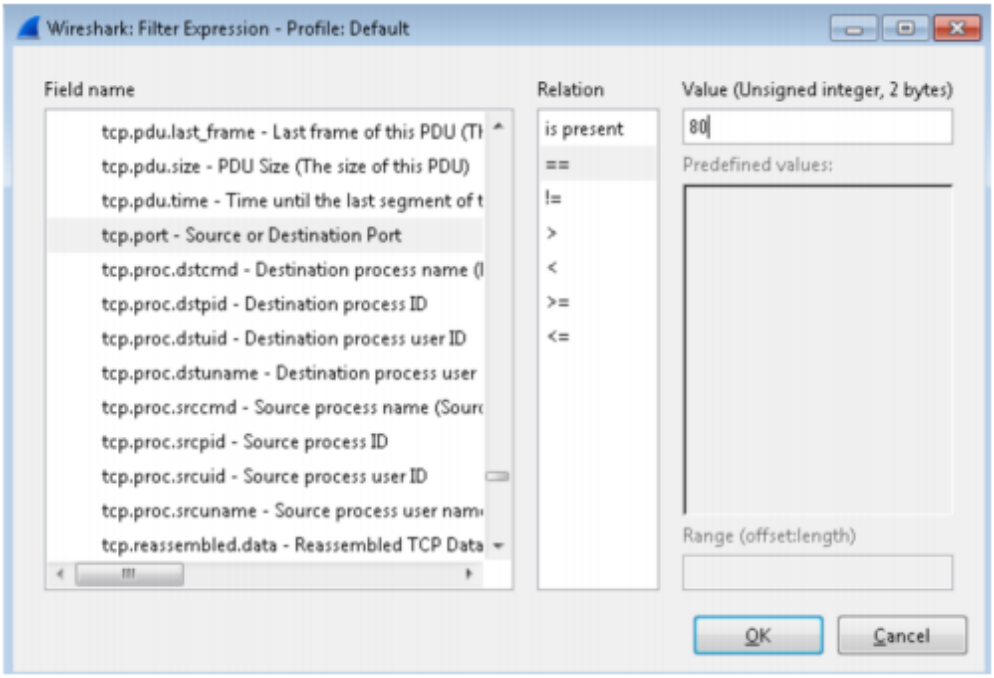
9) Con base en la información presentada, determine:

Número de paquetes enviados a 127.0.0.1.
Número de paquetes recibidos en 127.0.0.1.
Número de paquetes enviados a www.google.com.
Número de paquetes recibidos de www.google.com.
Número de paquetes enviados a www.epn.edu.ec.
Número de paquetes recibidos de www.epn.edu.ec.
Número de paquetes enviados a www.facebook.com.
Número de paquetes recibidos de www.facebook.com.
Número de paquetes enviados a www.youtube.com.
Número de paquetes recibidos de www.youtube.com.

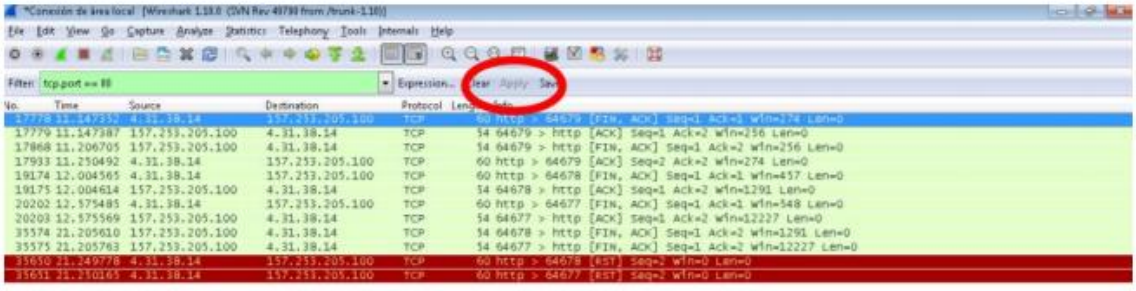
10)) El filtrado de tráfico permite desplegar solo aquellos paquetes que son de nuestro interés. Para esto, en la barra de herramientas se encuentra un combobox denominado

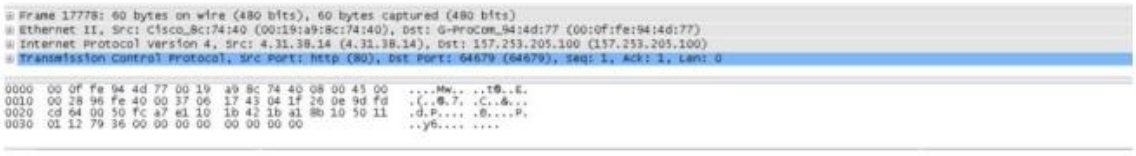
"Filter". Se puede escribir directamente sobre este control la condición que cumplirán los paquetes a ser desplegados, o se puede usar la ventana asociada al botón "Expression…". En esta nueva ventana selecciona el nombre del campo, su relación y el un valor.

A continuación se muestra el filtro de paquetes especificando al puerto 80 TCP como origen o como destino. Para que un filtro tenga efecto, se debe hacer clic en "Apply". Si se desea nuevamente mostrar todos los paquetes, se debe hacer clic en "Clear".



11) Aplique un filtro para presentar paquetes TCP. El resultado puede ser similar al siguiente.





12) Indique cuantos paquetes TCP han sido generados. ¿Compare con la información de su compañero, y responda si es la misma cantidad? Comente sobre los resultados obtenidos. Compare con la información que recolecto en el punto 9, ¿qué puede concluir?

13) Aplique un filtro para presentar paquetes ICMP. Para esto la expresión será:
ip.proto = = 1, también puede escribir en el "Filter": ICMP.

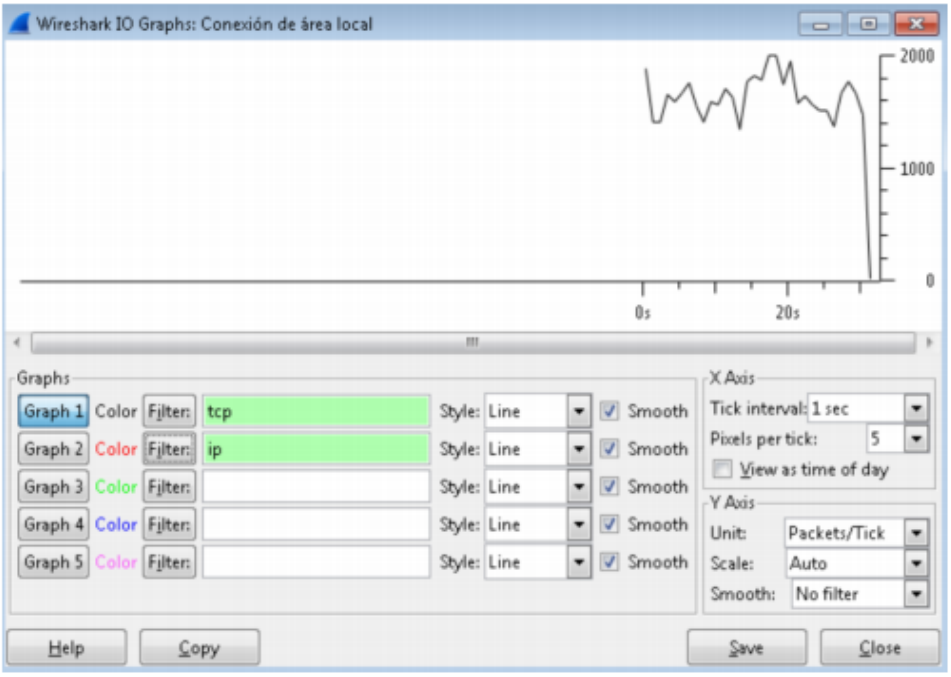
14) Indique cuantos paquetes ICMP han sido generados. ¿Compare con la información de su compañero, y responda si es la misma cantidad? Comente sobre los resultados obtenidos. Compare con la información que recolecto en el punto 9, ¿qué puede concluir?

15) Veremos la opción resumen, para lo cual, haga clic en "Statistics" y a continuación escoja "Summary". Su filtro debe estar configurado en ICMP.

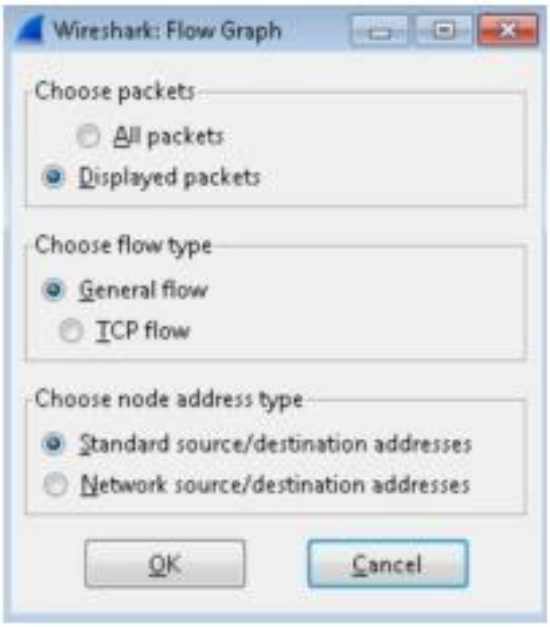
16) Obtenga la siguiente información:
Número de paquetes Diferencia de tiempo entre el primer y último paquete
Paquetes promedio por segundo
Tamaño promedio de paquete
Cantidad de Bytes Promedio de bytes por segundo

17) Vuelva a aplicar el filtro del punto 10. Obtenga la misma información del punto 16.

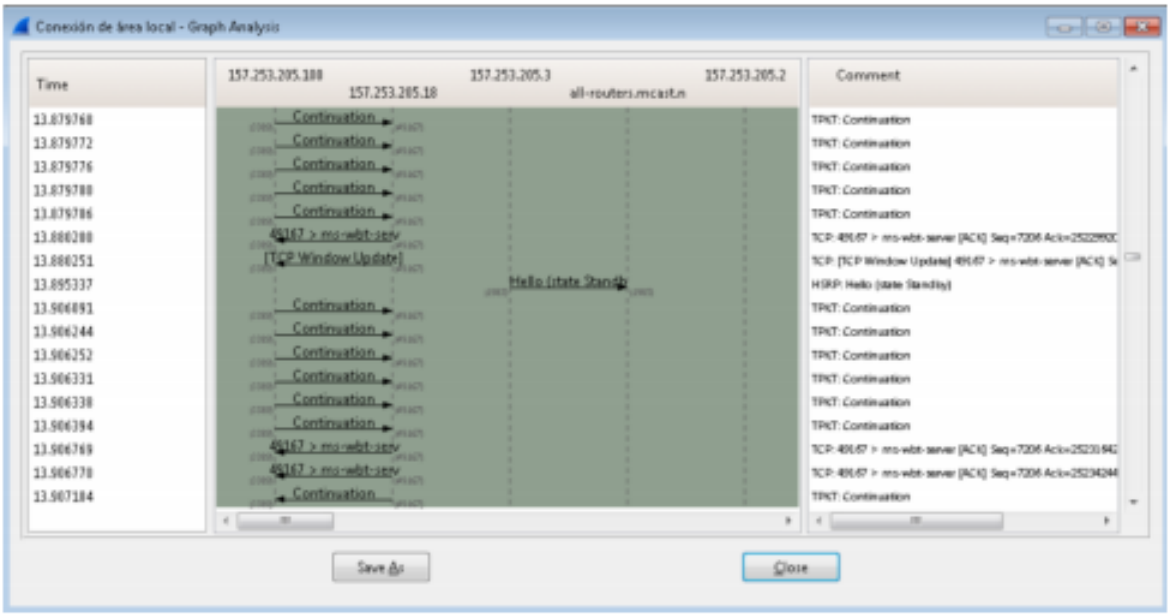
18) Ahora veremos la opción gráficos, para lo cual, haga clic en "Statistics" y a continuación escoja "IO Graphs". En los filtros escoja TCP e IP, como se ve en la gráfica:



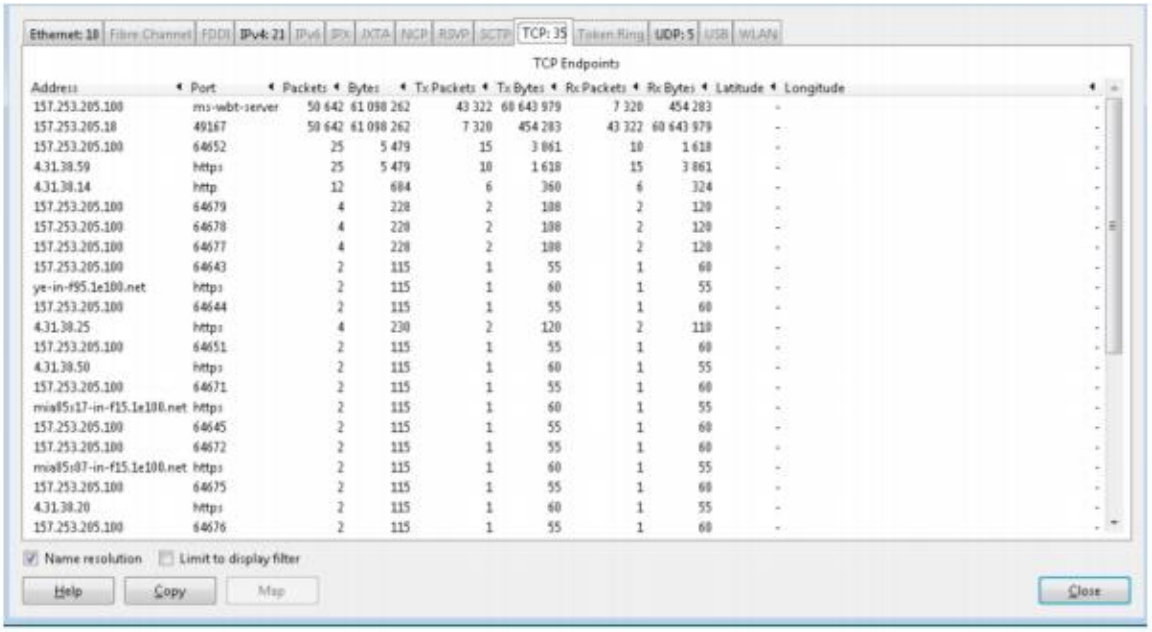
19) La opción gráfico de flujo, permite ver el flujo de paquetes entre dos o más equipos, en orden cronológico. Esta opción es muy útil para entender el flujo de paquetes y poder hacer troubleshooting. Para acceder a esta opción vaya a "Statistics" y luego escoja "Flow Graph", verá una ventana similar a la siguiente:



Presione en "Ok", con las opciones indicadas en la figura anterior. A continuación verá una gráfica similar a la siguiente:



20) Finalmente veremos las gráficas de puntos finales (endpoints) tanto para TCP como para UDP. Para esto, escoja la opción "Statistics" y luego "Endpoints", verá una ventana similar a la siguiente:



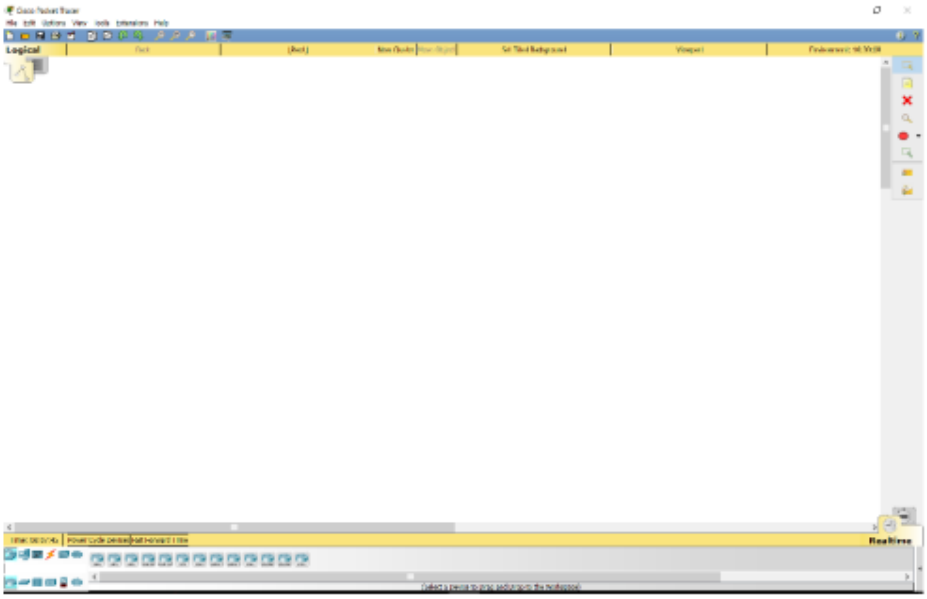
Podrá observar estadísticas de TCP en la viñeta “TCP:#” y de UDP en la viñeta “UDP:#”.

21)) Recoja lo siguiente:

Cantidad de paquetes UDP transmitidos
Cantidad de bytes UDP transmitidos
Cantidad de paquetes UDP recibidos
Cantidad de bytes UDP recibidos
Cantidad de paquetes TCP transmitidos
Cantidad de bytes TCP transmitidos
Cantidad de paquetes TCP recibidos
Cantidad de bytes TCP recibidos
¿Cuál es el tráfico más prominente recibido? TCP o UDP?
¿Cuál es el tráfico más prominente transmitido? TCP o UDP?
Compare con los resultados de su compañero.
¿Qué puede concluir?

Uso de Packet Tracer:

1) Ejecute Packet Tracer, haga doble clic sobre el ícono de su escritorio. Verá una pantalla similar a la siguiente:



En la pantalla puede ver varias secciones, la primera en la parte superior está la barra de menú, seguida de la barra de herramientas. La segunda sección está localizada en la parte inferior de la barra de herramientas, donde ese encuentra la ventana principal, que tiene un botón que permite cambiar entre la vista lógica de la red (logical), y la vista física de la red (physical), además en la parte derecha verá otra barra de herramientas con opciones para seleccionar un equipo, colocar una nota, eliminar, inspeccionar, dibujar figuras geométricas, cambiar tamaño, configurar una PDU simple o compleja. En la parte inferior se encuentra la tercera sección, la cual está dividida en dos partes, la primera ubicada en el lado izquierdo, donde verá dos filas con un conjunto de iconos cada una, y la segunda donde verá un conjunto de iconos en una sola fila, ubicada al lado derecho de la anterior. En la primera parte, en la primera fila están los tipos de dispositivos: dispositivos de red, dispositivos finales, componentes, conexiones, misceláneo, conexión multiusuario; en la segunda fila, se presentan equipos basados en lo escogido en los tipos de dispositivos, por ejemplo, si selecciona dispositivos de red, en esta fila verá: routers, switches, hubs, dispositivos inalámbricos, dispositivos de seguridad, emuladores de WAN; en la segunda parte de esta sección verá los modelos de equipos de un tipo específico, por ejemplo, si selecciono routers, verá: 1941, 2901, 2911, etc. Finalmente al lado derecho de esta sección verá dos opciones: Realtime o Simulation. El modo Realtime permite ubicar los equipos, y establecer su configuración; y el modo Simulation en el cual se pone a correr la red implementada.

2) A continuación cree una nueva topología, la topología a crear será la red de su casa, y siga las instrucciones del profesor.

6. INFORME

- En el procedimiento se detallaron los datos que deben ser obtenidos, así como algunas preguntas que deberán ser respondidas en el informe de acuerdo al formato establecido. Además en su informe deben existir capturas de pantalla con información

de resúmenes, gráficas, etc. Obtenidas en Wireshark. No olviden incluir conclusiones, recomendaciones y bibliografía.

- Realice una topología de red (similar a la hecha en clase) en Packet Tracer, y mediante capturas de pantalla explique lo realizado.

No olviden incluir conclusiones, recomendaciones y bibliografía

7. REFERENCIAS

Wireshark, "Wireshark Documentation", http://www.wireshark.org/docs, [Online].
Cisco Packet Tracer, "Packet Tracer Documentation".