Escuela Politécnica Nacional
Facultad de Ingeniería Eléctrica y Electrónica
Carrera de Ingeniería en Electrónica y Redes de Información
Laboratorio de Telemática 1
http://detri.epn.edu.ec
Quito, Ecuador

LABORATORIO DE TELEMÁTICA 1

HOJA GUÍA

PRACTICA N: 02

1. TEMA

SOFTWARE PARA CAPTURA Y SIMULACIÓN DE PAQUETES

2. OBJETIVOS

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

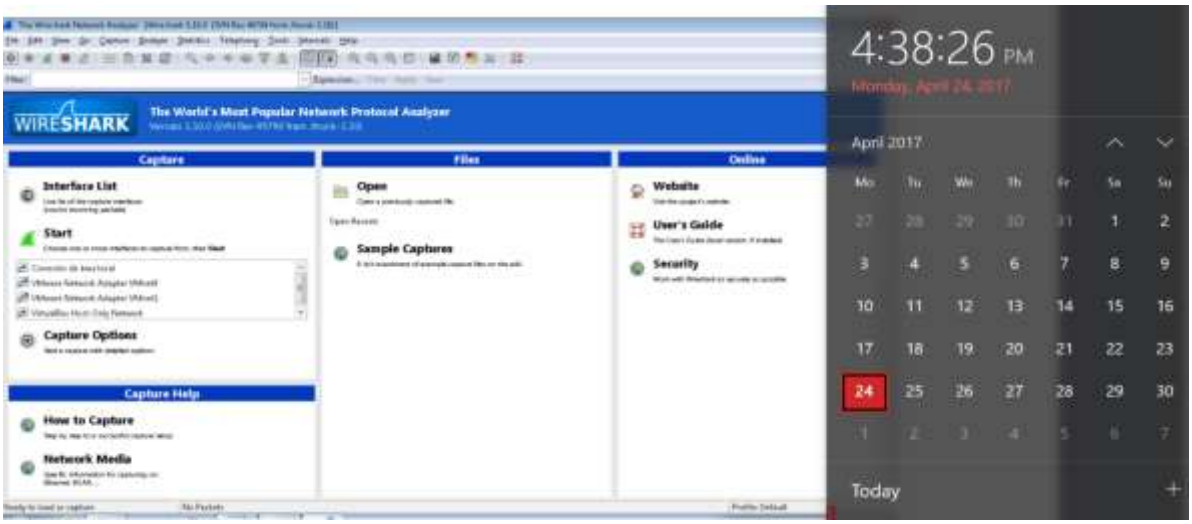
3. INFORMACIÓN

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.

4. TRABAJO PREPARATORIO

Como parte de este preparatorio, Usted debe realizar las siguientes tareas:

1) Investigue qué es el modo promiscuo (aplicable a interfaces de red) (máximo un párrafo).
2) Investigue qué es un analizador de protocolos, y para qué es útil (máximo 1 página).
3) Investigue qué es un simulador de redes, y para qué es útil (máximo 1 página).
4) Investigue sobre 2 herramientas, distintas a Wireshark, que permitan realizar análisis de trafico de red, y escriba una breve descripción de estos (máximo un párrafo por cada una).
5) Instale Wireshark en su equipo, capture una pantalla en la que se muestre el software instalado, en la captura debe verse la fecha y hora de la captura (similar a la figura que se presenta a continuación):



5. EQUIPOS Y MATERIALES

PC

Wireshark

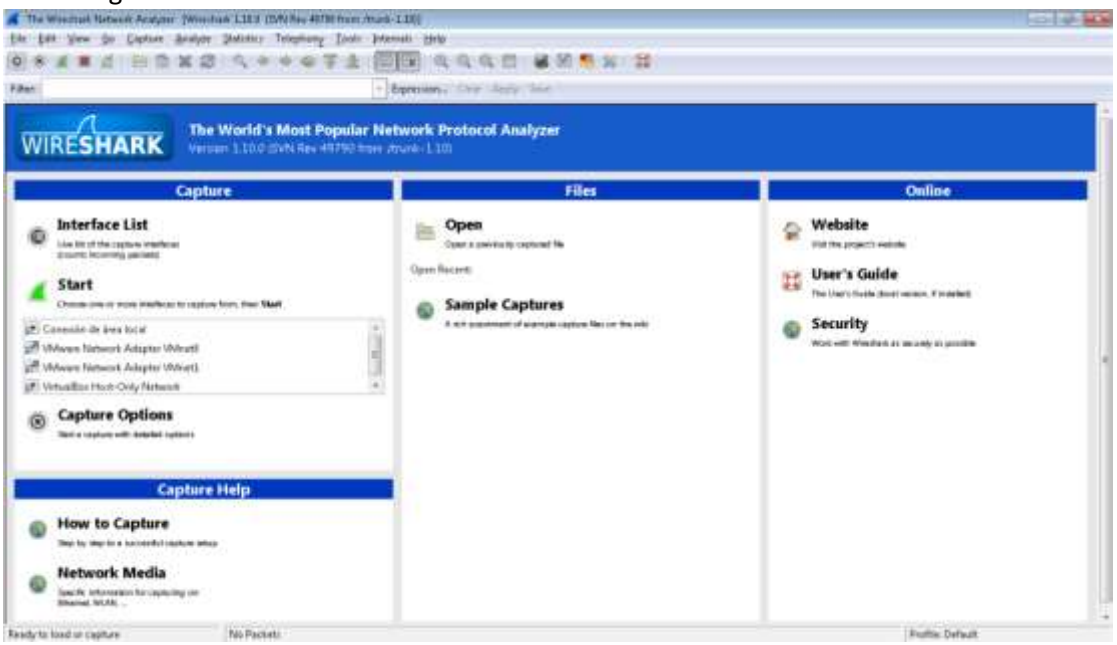
Packet Tracer

6. PROCEDIMIENTO

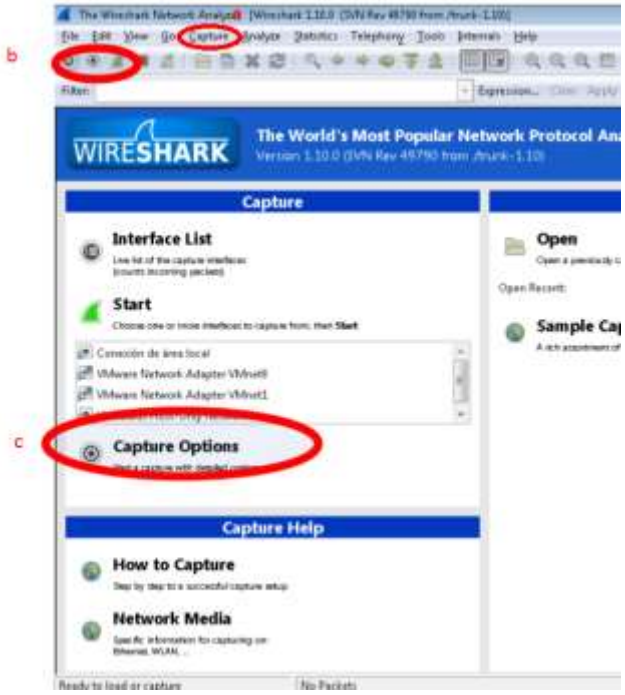
Establezca y verifique la conectividad a Internet, Esto garantiza que su equipo tiene asignado una dirección IP. Para esto abra un explorador web y compruebe que puede acceder a www.google.com. Sino puede hacerlo pida ayuda al instructor.

ETAPA 1: Uso de Wireshark:

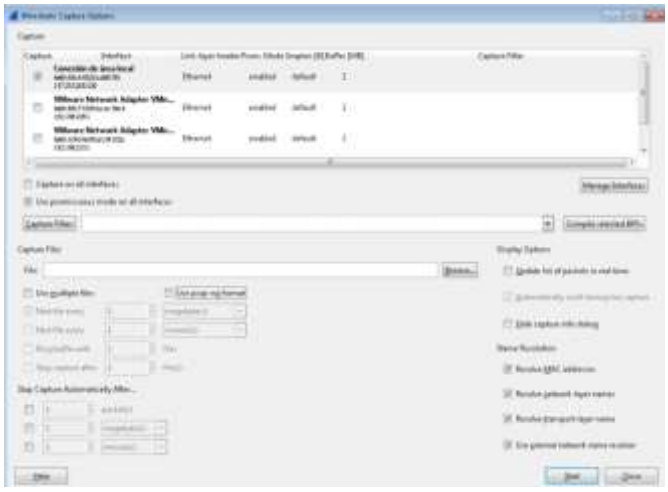
1) Ejecute el programa, encontrará un enlace directo en su escritorio. Debe ejecutarlo con permisos de administrador, así que para iniciarlo, presione botón derecho sobre el icono y escoja "Ejecutar como administrador (*Run as administrator*)". Si no ejecuta el programa con privilegios de administrador, no verá ninguna interfaz al momento de querer captura tráfico. Luego de ejecutarlo verá una pantalla similar a la siguiente:



2) Vamos a usar Wireshark para capturar algo de tráfico. 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"
5) Luego de presionar "Start", Wireshark empezará a capturar paquetes y presentará una ventana con información general de los paquetes capturados, similar a la siguiente:

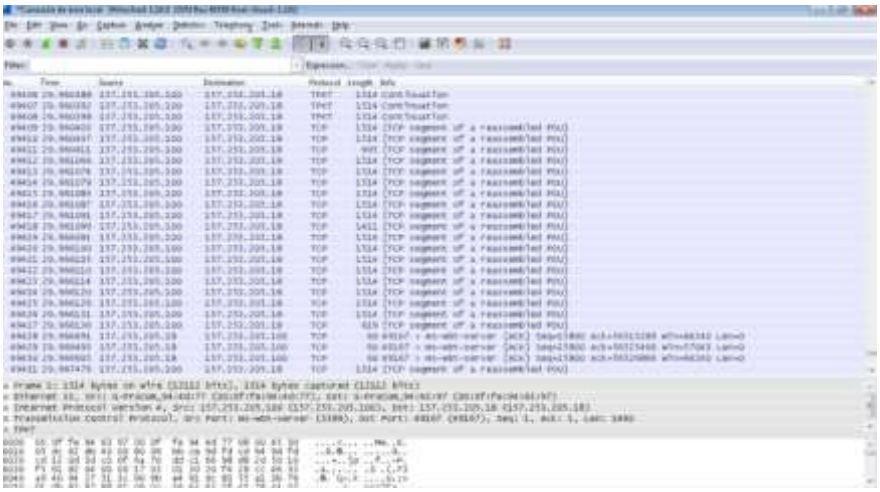
6) Genere una tabla indicando cuantos paquetes fueron capturados en TCP, UDP, ICMP y ARP.
7) Abra una consola y ejecute los siguientes comandos:

```
ping 127.0.0.1
ping www.google.com
ping www.epn.edu.ec
ping www.facebook.com
ping www.youtube.com
```

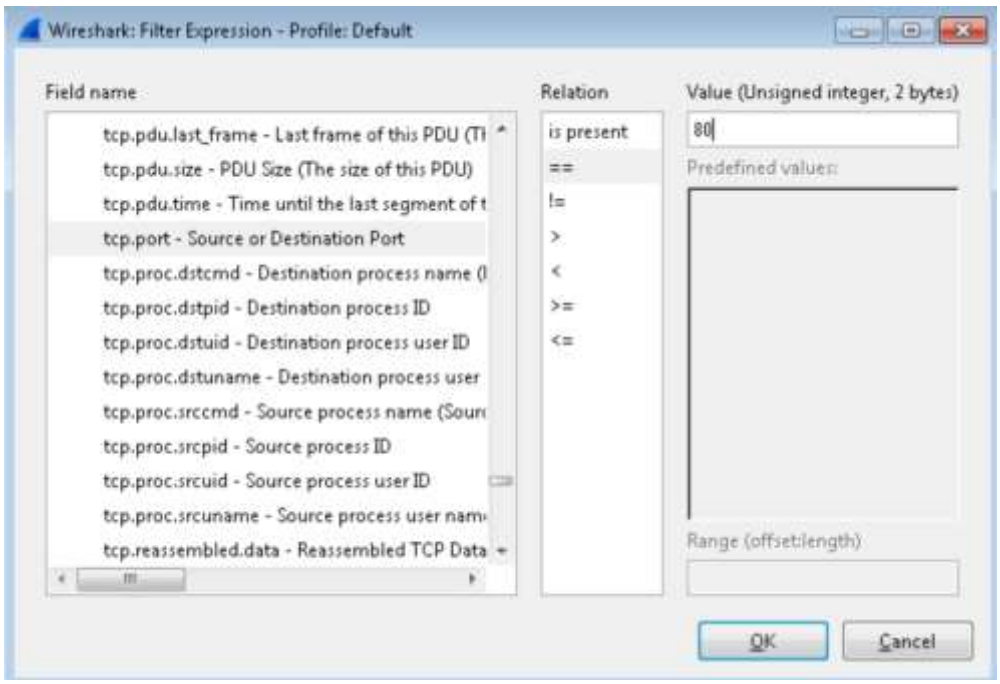
8) Abra un explorador web e ingrese a los siguientes sitios web:

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

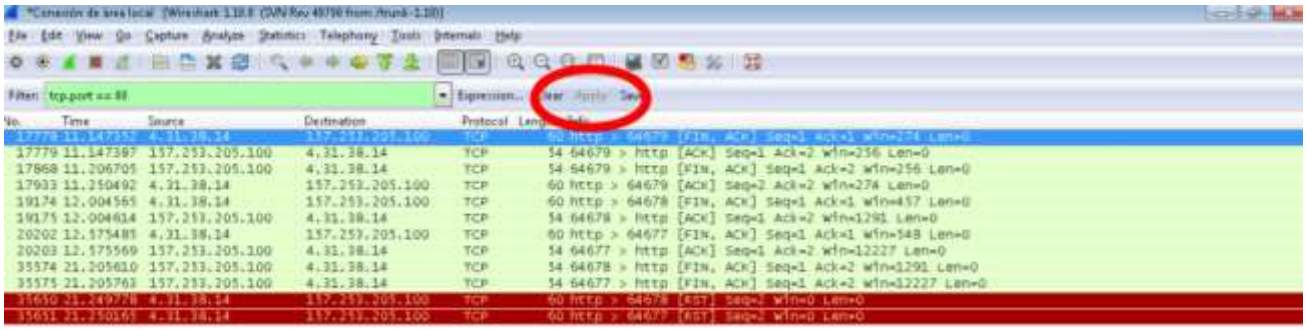
9) Detenga la captura de paquetes, presionando en el botón “Stop”, podrá ver una ventana con resultados similar a la siguiente:
    a. En la parte superior de la pantalla principal verá un listado de todos los paquetes con información como Número de paquete, Tiempo, Origen, Destino, Protocolo, Longitud 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.

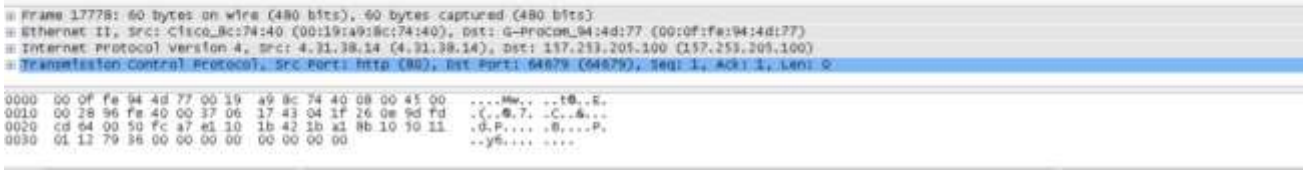


10) Con base en la información presentada, determine:
    Número de paquetes enviados a 127.0.0.1.
    Número de paquetes recibidos en 127.0.0.1.
    Número de paquetes enviados a www.google.com.
    Número de paquetes recibidos de www.google.com.
    Número de paquetes enviados a www.epn.edu.ec.
    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.
    ¿Compare esta información con la obtenida por su compañero, es la misma? Comente sobre los resultados obtenidos.
11) 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".



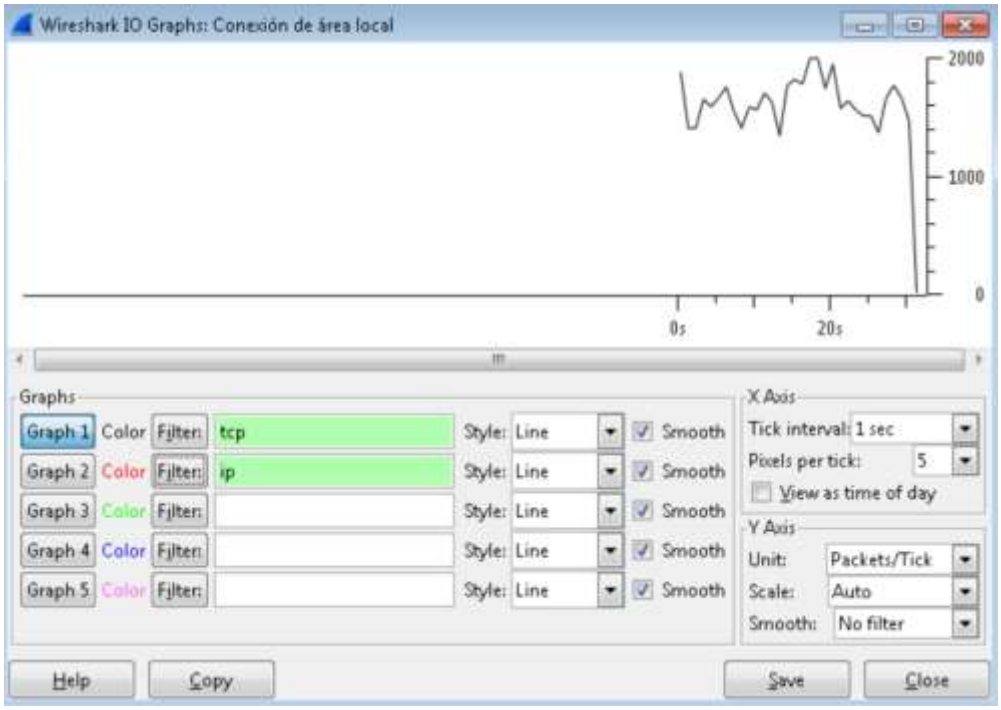
12) Aplique un filtro para presentar paquetes TCP. El resultado puede ser similar al siguiente.





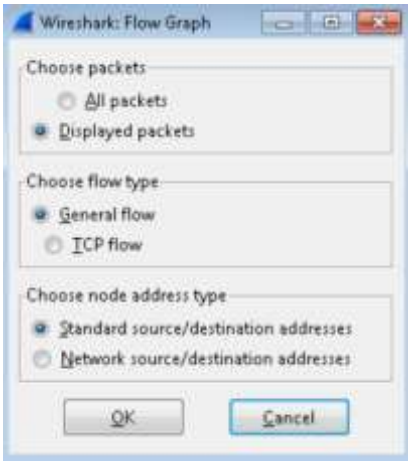
13) Indique cuantos paquetes TCP han sido generados. ¿Compare con la información de su compañero, y responda si es la misma cantidad? Comente sobre los resultados obtenidos. Compare con la información que recolecto en el punto 9, ¿qué puede concluir?
14) Aplique un filtro para presentar paquetes ICMP. Para esto la expresión será: `ip.proto = = 1`, también puede escribir en el "Filter": ICMP.
15) 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?
16) Wireshark posee un conjunto completo de herramientas que permiten obtener estadísticas de los paquetes, entre las cuales están: resúmenes, gráficas, jerarquías de protocolos, conversaciones, etc. Se accede a la mayoría de ellas a través de la opción del menú "Statistics".
17) Primero veremos la opción resumen, para lo cual, haga clic en "Statistics" y a continuación escoja "Summary". Su filtro debe estar configurado en ICMP.
18) 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
19) Compare con la información recolectada por su compañero. ¿Qué puede concluir?
20) Vuelva a aplicar el filtro del punto 11. Obtenga la misma información del punto 18.
21) Compare con la información recolectada por su compañero. ¿Qué puede concluir?

22) 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:

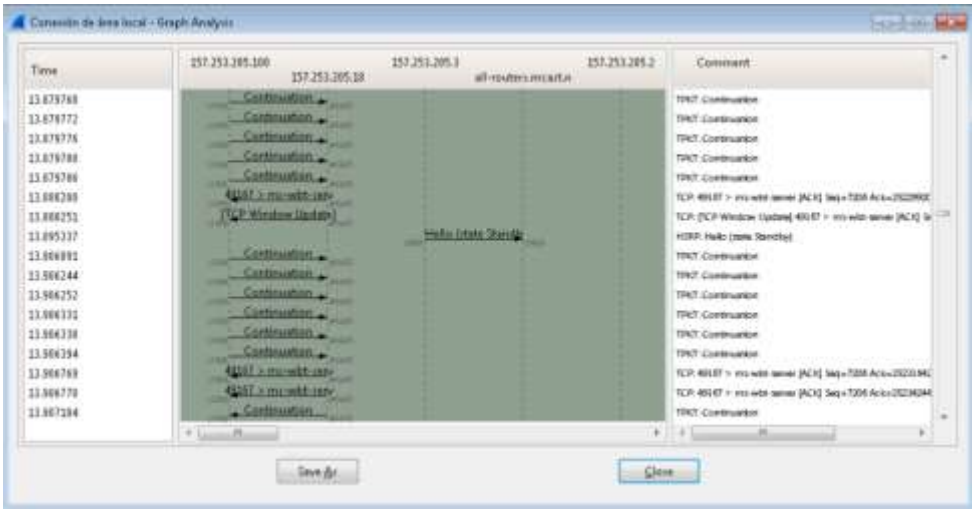


23) Compare su gráfica con la de su compañero, ¿qué puede concluir?

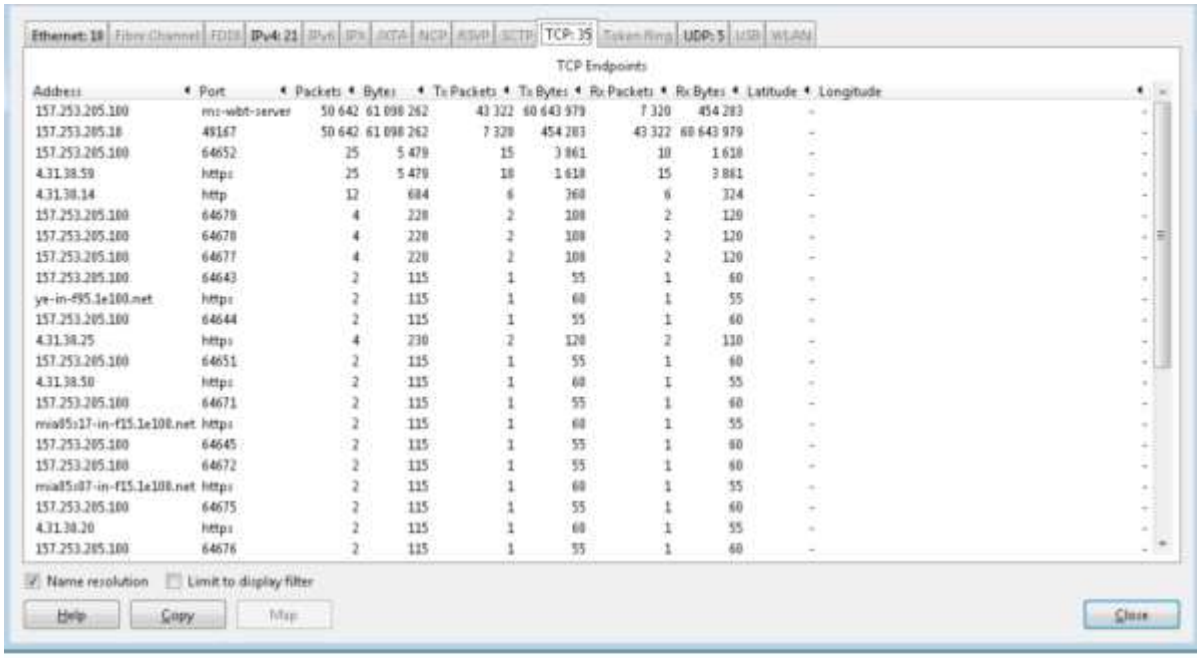
24) Ahora veremos la opción gráfico de flujo, la cual permite ver el flujo de paquetes entre dos o más equipos, en orden cronológico. Esta opción es muy útil para entender el flujo de paquetes y poder hacer troubleshooting. Para acceder a esta opción vaya a "Statistics" y luego escoja "Flow Graph", verá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

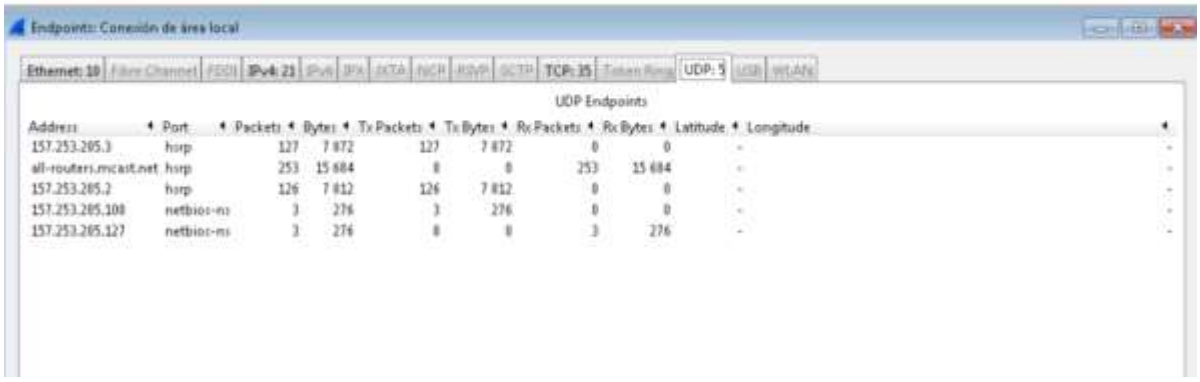


Presione en "Ok", con las opciones indicadas en la figura anterior. A continuación verá una gráfica similar a la siguiente:



25) Compare la gráfica obtenida con la de su compañero, ¿qué puede concluir?
26) 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:

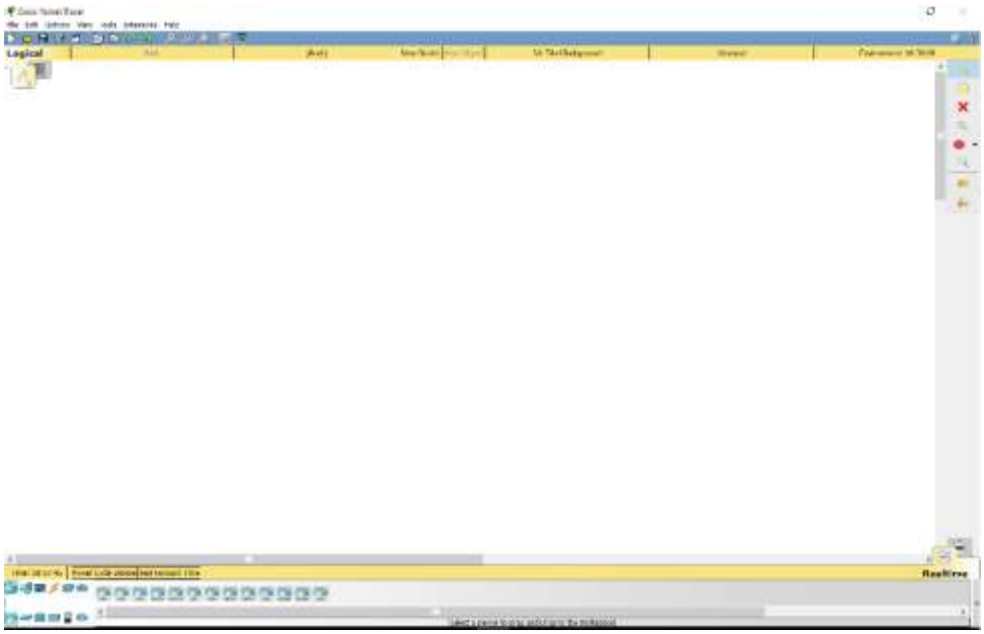




27) Podrá observar estadísticas de TCP en la viñeta “TCP:#” y de UDP en la viñeta “UDP:#”.
28) Recoja lo siguiente:
    Cantidad de paquetes UDP transmitidos
    Cantidad de bytes UDP transmitidos
    Cantidad de paquetes UDP recibidos
    Cantidad de bytes UDP recibidos
    Cantidad de paquetes TCP 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?

ETAPA 2: Uso de Packet Tracer:

1) Packet Tracer es un software para simular redes. Esta herramienta permite crear topologías de red, configurar dispositivos, insertar paquetes y simular una red (analizar su comportamiento o su funcionamiento). En este programa se crea la topología física de la red, simplemente arrastrando los dispositivos a la pantalla. Luego, al hacer clic sobre un equipo se puede ingresar a su consola de configuración. En estas consolas están soportados la mayoría de los comandos del IOS de Cisco, e incluso se puede emplear la tecla TAB para completar los comandos, escribiendo una parte de ellos. Una vez completada la configuración física y lógica, se pueden hacer pruebas de conectividad con ping, traceroute, etc. desde las consolas.
2) 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.

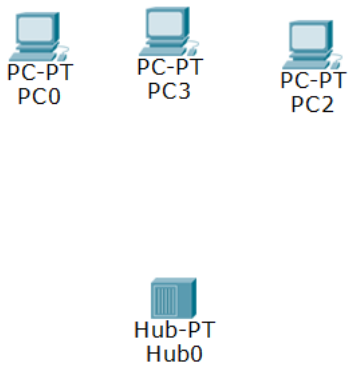
En la parte inferior se encuentra la tercera sección, la cual está dividida en dos partes, la primera ubicada en el lado izquierdo, donde verá dos filas con un conjunto de iconos cada una, y la segunda donde verá un conjunto de iconos en una sola fila, ubicada al lado derecho de la anterior. En la primera 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.

3) A continuación cree una nueva topología, la topología a crear será la red de su casa (escojan una de las dos topologías a desarrollar).
4) Asegúrese de estar en la vista Logical. Luego en la parte inferior presione en “End Devices”, se presentarán los dispositivos que pueden haber en una red, escoja los que existan en su casa, por ejemplo, escoja PC “Generic” y arrástrelo a la ventana principal. Aparecerá un elemento denominado PC-PT PC0 en esta ventana. Presione doble clic en este elemento y se presentará una ventana similar a la siguiente:

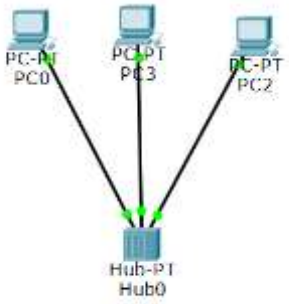
En esta vista Usted dispone de 5 viñetas: Physical, Config, Desktop, Attributes y Software/Services. En la viñeta "Physical", puede agregar las distintas interfaces a su equipo, sean estas cableadas (RJ45, Fibra Óptica, telefonía), inalámbricas, audífonos o micrófono. El equipo por defecto ya tiene una tarjeta de red configurada. En la viñeta "Config" podrá establecer: la configuración del equipo, es decir su nombre, su Gateway, su servidor DNS; la configuración a nivel de TCP; y la configuración de la interfaz de red: estado del puerto, ancho de banda (tasa de transmisión), dúplex, Dirección MAC, Dirección IPv4, Dirección IPv6. En la viñeta "Config" podrá usar herramientas para configurar su equipo, para establecer una conexión Dial Up, para abrir el Terminal de configuración de un equipo de red, para abrir un intérprete de línea de consola, para abrir un explorador web, etc. En la viñeta "Attributes" podrá configurar otros parámetros como por ejemplo el tiempo promedio entre fallas MTBF, el costo, las fuentes de poder, las unidades de rack, la potencia que usa el equipo. Finalmente en la viñeta "Software/Services" se presentarán interfaces para acceder a las aplicaciones o servicios que ha adquirido de Cisco para Packet Tracer.

5) Agregue tantos PC como equipos haya en su red (red de su casa), al menos deben estar dos, el nombre de los otros serán PC1, PC2, y así sucesivamente. Si conoce la información de las direcciones IP de sus equipos configúrela en los PC agregados.

6) Ahora escoja en la opción "Network Devices" el elemento "Hub", y agregue el modelo "Generic". Se agregará el elemento Hub0

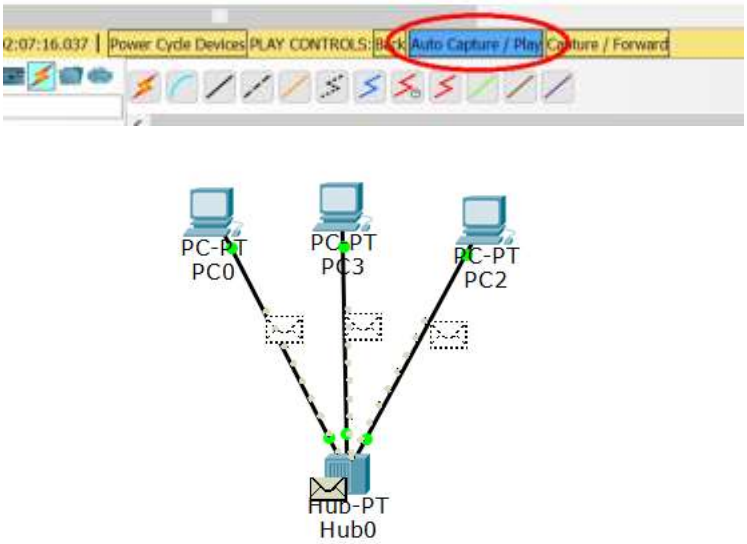


7) Ahora escoja en la opción "Connections" el elemento "Conecction", y de clic en el modelo "Automatic" (su icono es un rayo). El cursor cambiará, indicando que puede conectar equipos de forma automática en los interfaces disponibles (el primero). Con este cursor presione sobre el PC0, y luego presione sobre el Hub0. Repita el proceso con los otros equipos. Su diagrama de red se verá así:



Los puntos verdes representan interfaces activas, los puntos rojos representan interfaces que están apagadas o desconectadas.

8) Como hemos usado un hub, todas las interfaces deben estar activas. Sin embargo, el punto verde no indica que la configuración IP es correcta, por lo que debe revisarla si tiene problemas con lo siguiente. Ahora configuraremos una PDU para realizar la prueba, para lo cual en la barra de herramientas del lado derecho, seleccione el icono que dice "Add Simple PDU (P)", el icono de su cursos cambiará a un sobre, presione sobre el PC1 (origen) y luego sobre el PC2 (destino), repita el proceso con PC1 (origen) y PC3 (destino), y luego con PC2 (origen) y PC3 (destino).
9) Ahora estamos listos para simular, en la parte inferior presione sobre el icono "Simulation", luego presione sobre el botón "Auto Configure / Play", usted verá los mensajes que se están transmitiendo.

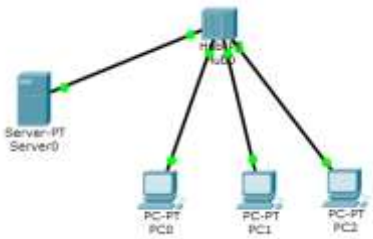


Revise la ventana "Event List" y genere el listado de eventos que sucedieron en la simulación. Haga un diagrama de tiempo en el que se presenten estos eventos.

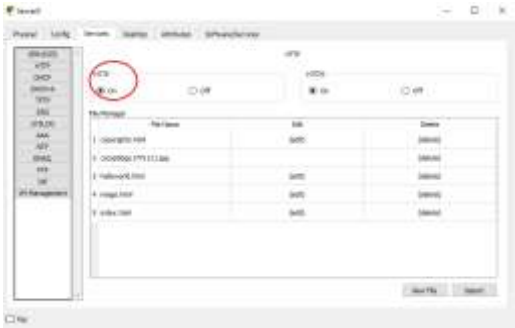
Escoja un paquete del "Event List", presione doble clic sobre la columna "Info", se levantará la ventana "PDU Information at Device …", en la cual verá que pasa con el paquete en cada dispositivo (a nviel de cada una de las capas del modelo OSI).

10) Genere una tabla indicando, para un paquete en particular, que capas están involucradas en cada dispositivo por el cual atravesó el paquete. En la figura anterior usted puede ver las capas de entrada y las capas de salida, por lo que debe hacer un seguimiento del paquete escogido, y dar clic en cada dispositivo por el que paso el paquete e ir almacenado la información de las capas (in - out) por las cuales el paquete atravesó.
11) Ahora agreguen un servidor, el cual se encuentra en la parte inferior dentro de "End Devices".

12) Asigne al servidor una dirección IP adecuada y conecte el equipo a su red implementada.



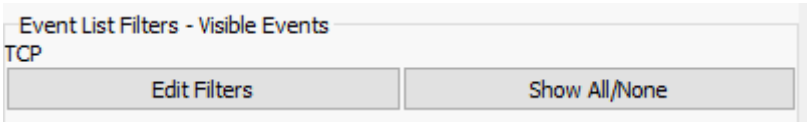
13) Haga doble clic sobre el servidor y en la pantalla que se presenta, en la pestaña de configuración verifique que el servicio HTTP se encuentra habilitado y de no estarlo habilitarlo.



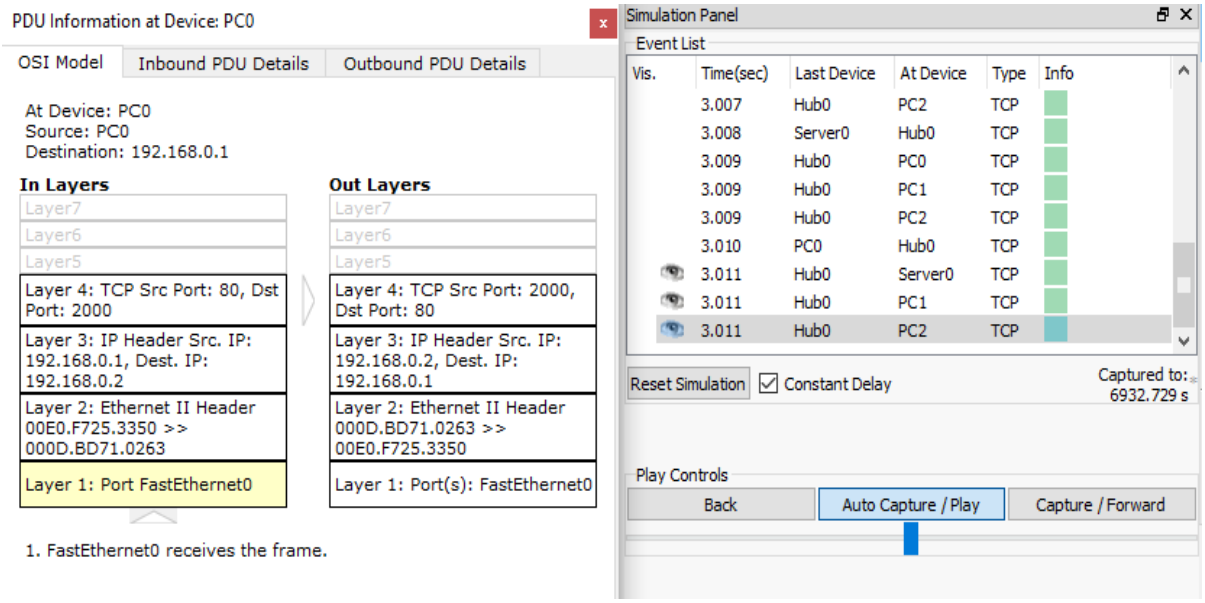
14) Cierre la ventana y seleccione “Complex PDU” del menú de herramientas de la sección derecha de la pantalla.

15) En la pantalla que se despliega cambie la siguiente información:
Seleccione HTTP en “Select Application”
En dirección IP de destino indique la dirección IP del servidor
En dirección IP de origen especifique la dirección IP de uno de los equipos de su red
En puerto de origen indique 2000
En la configuración del tiempo escoja “One Shot” con un tiempo de 10s.

16) En la parte inferior presione sobre el icono “Simulation”, luego establezca el filtro para TCP por medio de la opción “Edit Filters” y finalmente presione sobre el botón “Auto Configure / Play”.



17) En el panel de simulación seleccione un paquete y analice la información de la PDU haciendo doble clic en la columna “info”. ¿Qué diferencia nota con la información obtenida de la simulación del paso 9? ¿Hasta qué capa del modelo OSI presentan información esta PDU?



18) Finalmente guarde su proyecto. Vaya a la opción del menú “File”, y escoja “Save as”, asigne un nombre adecuado (Informe01_NombreA_NombreB.pkt). Este archivo debe subirlo como parte de su informe.

7. 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.

Tanto su archivo digital del informe (en Word o en PDF), como su archivo de simulación (.PKT), deben ser comprimidos y entregados como Informe_01_NombreA_NombreB.

8. REFERENCIAS

Wireshark, “Wireshark Documentation”, http://www.wireshark.org/docs, [Online], revisado en 24/04/2017

Cisco Packet Tracer, “Packet Tracer Documentation”.