



UNIVERSIDAD SIMÓN BOLÍVAR
REDES DE COMPUTADORAS
EC5751
Práctica I

Objetivos:

Conocer y manejar comandos básicos de los sistemas operativos para validar la conexión de equipos a las redes.

Aprender a manejar herramientas para el monitoreo y administración de redes: Wireshark

Aprender a modelar redes simples usando el GNS3

Configurar el enrutamiento sencillo de una red Ethernet

Verificar conectividad de un equipo en una red Ethernet

Desarrollar las habilidades y destrezas fundamentales para identificar fallas en una red Ethernet

Requerimientos:

- PC con al menos 4 GB de ram

- 5 GB de espacio libre en disco

- Sistema operativo: Linux, Mac OS X, Windows 7 o superior, o cualquiera que soporte las herramientas a utilizar.

- Wireshark: <https://www.wireshark.org/#download>

- GNS3: <https://www.gns3.com/>

- Manuales de programación de Switch Cisco. Se consiguen en la página de Cisco (www.cisco.com), aunque por toda la web hay páginas con detalles y tutoriales sobre la programación de switches de todos los proveedores.

Pre Laboratorio:






Las siguientes tareas deben realizarse en su casa y con tiempo, a fin de aprender a manejar las herramientas que se utilizarán en las prácticas de laboratorio. Hay muchos tutoriales en internet (youtube) sobre el manejo de las mismas. Aun así, Si tiene alguna duda en los procesos contacte a su profesor

Primera Parte: manejo del analizador de Protocolos Wireshark

- **Descargar e instalar el Wireshark:** Si se utiliza el paquete suministrado en la carpeta para instalar el gns3, no será necesario ya que lo hace de forma automática, pero se puede descargar de forma individual en la dirección indicada arriba.

Wireshark es un programa que, ejecutado en un sistema final es capaz de capturar todo el tráfico de red recibido o enviado por dicho sistema a través de su interfaz de red, es decir, las tramas o E_PDUs (Electronic Protocol Data Units) que llegan o salen de la interfaz de red del equipo en el que se esté ejecutando. Es una herramienta de gran utilidad, pues no sólo captura el tráfico sino que además es capaz de analizarlo mostrando al usuario información detallada de los protocolos de cada uno de los niveles (desde el nivel de enlace de datos hasta el nivel de aplicación). Es por ello que recibe el nombre de analizador de protocolos.

Pasos:

1. Haga doble clic en el icono del escritorio para arrancar el analizador de protocolos Wireshark. En la Figura 1 se muestra la pantalla inicial que aparece al arrancar Wireshark y la Tabla 1 muestra un resumen de los iconos de Wireshark que más se van a utilizar en las prácticas.
2. Puede iniciar una captura de diversas formas. La primera forma es seleccionar en la pantalla inicial de Wireshark (si no estuviera ya seleccionada), la Conexión de área local y luego hacer clic en **Start**. Otra manera es hacer clic sobre el icono  que aparece en el menú. Y la otra manera es hacer clic en el icono del menú  para abrir una ventana en la que aparece el listado de todas las interfaces de red que se pueden usar, seleccionar la que nos interesa (en esta caso la que conecta a la red de área local, en sus casas puede ser la interfaz inalámbrica) y luego pulsar el botón **Start**. Sabiendo esto, ponga a Wireshark a capturar tráfico usando el método que prefiera. Si todo lo ha hecho bien, le aparecerá en una ventana las tramas que en ese momento están llegando o saliendo de su PC, las cuales están siendo capturadas por Wireshark.
3. Abra el navegador de su preferencia y acceda a la página <http://www.labc.usb.ve>, ubicada en un servidor web de la Intranet del laboratorio.
4. Espere unos segundos y detenga la captura de Wireshark haciendo clic en el icono . Guarde la captura en un archivo para llevársela cuando acabe la práctica. Para ello haga clic sobre el icono , introduzca el nombre del archivo que desee y luego presione sobre guardar. Para cargar esta captura previa sólo tendría que abrirla pulsando sobre el icono  e indicar la ubicación del fichero con la captura para que Wireshark la muestre.

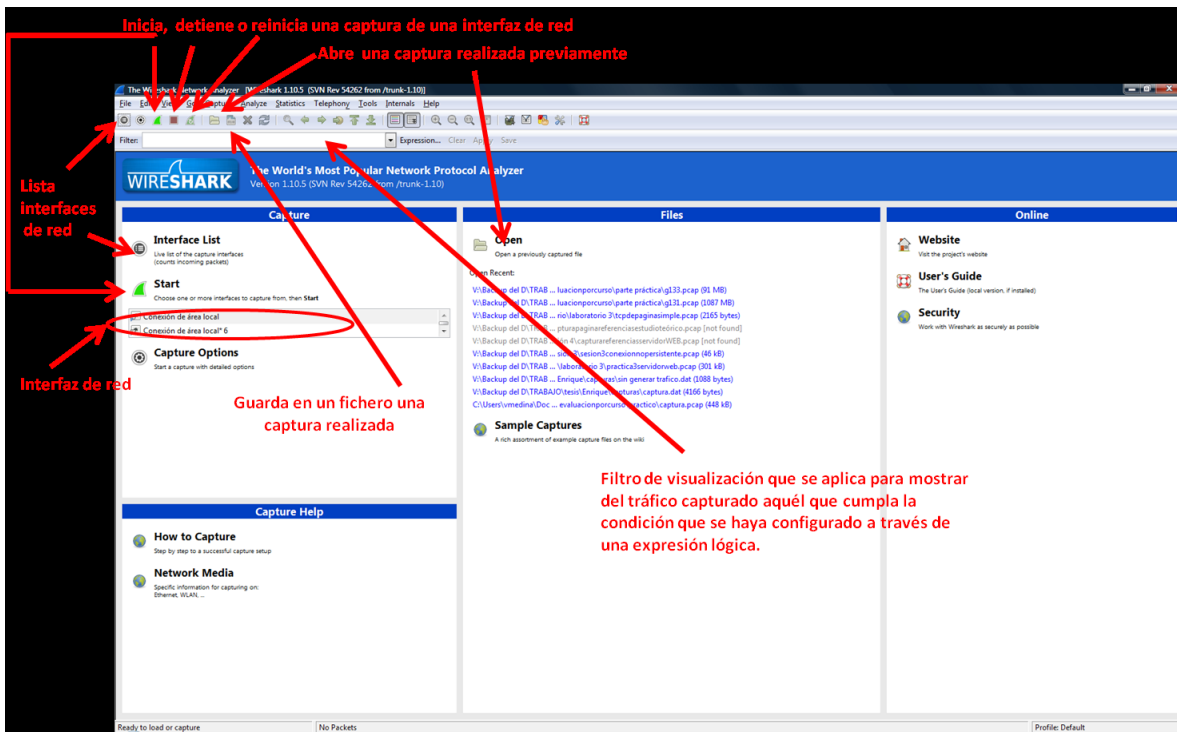








Figura 1: Pantalla inicial al arrancar Wireshark.

Iconos más usados en Wireshark:

-  Muestra las interfaces disponibles para capturar
-  Reinicia una captura (detiene la actual e inicia una nueva)
-  Detiene una captura
-  Inicia una captura
-  Abre un archivo con una captura previa
-  Guarda un fichero con la captura actual

5. Fíjese en las tres partes de la ventana principal (listado de tramas, detalles de tramas y octetos que forman la trama) donde se ven la captura que ha realizado. En la Figura 2 se detalla lo que se muestra en cada parte.
6. Muévase por el listado de tramas y, usando la información que aparece en "Protocol" busque tramas que encapsulen PDUs de los protocolos típicos de Internet como lo son HTTP, DNS, TCP, UDP e IP (investigue que significan estas siglas), Si hace clic en el nombre de la columna "Protocol" ordenará el listado de tramas por este campo. Tenga en cuenta que a nivel de enlace todas las tramas capturadas usan el protocolo Ethernet.

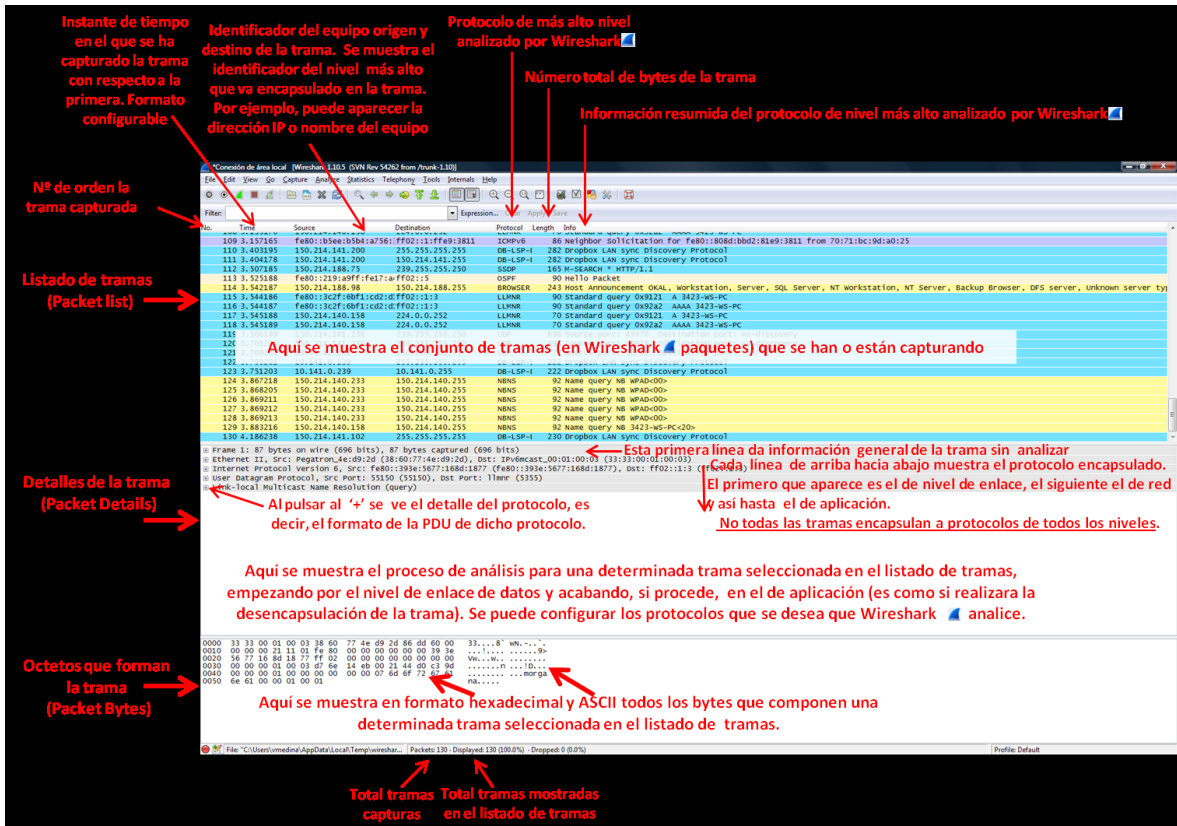





Figura 2: Descripción de las diferentes partes que componen la herramienta.

7. Wireshark es capaz de utilizar los servicios de DNS (investigue que es DNS y para qué sirve) para, en sus diversas ventanas, mostrarnos siempre nombres de host y dominio, en lugar de mostrarnos las direcciones IP equivalentes, en el formato numérico xxx.xxx.xxx.xxx habitual. Esa característica es de mucha utilidad en la práctica. Entre en "Edit" → "Preferences", pulse "Name Resolution" en el panel de la izquierda, active la opción "Resolve Network (IP) addresses". Wireshark también es capaz de mostrarnos, en lugar de los números de puerto TCP y UDP, el nombre del protocolo que usa habitualmente dicho número de puerto. En esta práctica concreta no nos interesa habilitar esta funcionalidad de Wireshark. Entre en "Edit" → "Preferences", pulse "Name Resolution" en el panel de la izquierda, desactive la opción "Resolve Transport Name" y pulse "OK" para cerrar la ventana y que tengan efecto los cambios.
8. En el listado de tramas podemos ver mucha información de cada trama, organizada en columnas. Las que aparecen por defecto son:
 - a) La primera columna se llama "No." y nos muestra el número de orden en el que se han ido capturando las tramas, de la 1 a la N.
 - b) La segunda columna se llama "Time" y en ella Wireshark nos muestra, en segundos, información temporal del instante en que fue capturada esa trama. Por defecto este tiempo se mide desde el instante en que se capturo la primera trama, por lo que en la trama número 1 es 0.000000.

- c) La columna "Source" muestra información del equipo que envió la trama (o el que envió alguna PDU encapsulada en dicha trama, depende de cómo hayamos configurado Wireshark).
 - d) La columna "Destination" es análoga a la anterior, mostrándonos información del equipo destino.
 - e) La columna "Protocol" muestra información de protocolo de más alto nivel encapsulado en esa trama y que es capaz de analizar.
 - f) La columna "Length" muestra el número de bytes de la trama.
 - g) La columna "Info" muestra información resumida del protocolo de más alto nivel que es capaz de analizar en esa trama.
9. Es posible quitar y añadir columnas de información al listado de tramas, para adaptarlo a nuestras necesidades en cada momento. Vamos a practicar añadiendo dos nuevas columnas que nos presenten información de los puertos de origen y de destino de las T_PDU de los protocolos TCP y UDP. Con esto podremos identificar el número de puerto usado para identificar al proceso de aplicación cliente y servidor en una trama que encapsule protocolos hasta el nivel de aplicación. Para hacerlo debe seguir Estas instrucciones:
- a) Entre en "Edit" → "Preferences", y pulse en la rama "Columns" (dentro de "User Interface" en el panel de la izquierda).
 - b) Pulse el botón "Add" una vez para añadir una nueva columna.
 - c) Haga clic en el texto "New column" que ha aparecido, y edítelo escribiendo como título de la nueva columna el texto "SrcPort" y pulsando "Intro" en el teclado.
 - d) En el campo "Field Type" debe seleccionar de la lista desplegable el valor "Src Port (unresolved)".
 - e) Repita los pasos b), c) y d) para crear otra columna con título "DstPort" y que tenga "Dest Port (unresolved)" de "Field Type".
 - f) Pulse "OK" para cerrar la ventana "Preferences".
 - g) Observe que en el listado de tramas aparecen las dos nuevas columnas en la parte de la derecha (si no puede verlas desplácese hacia la derecha). Utilice el ratón para reordenar las columnas y colocar las dos nuevas delante de la columna "Info" o bien ajuste el ancho de la columna "Info" para que se muestren todas ellas en pantalla sin tener que desplazarse.
10. Recordemos que la ventana principal de Wireshark está dividida en tres paneles. Ya hemos repasado el panel superior, el listado de tramas. Los otros dos paneles están muy relacionados con el panel superior, pues nos muestran información de la trama que hayamos seleccionado en el listado de tramas.
11. El panel central, "Detalles de la trama", muestra diversa información de la trama y de su contenido, de forma ordenada y estructurada por niveles. En primer lugar se muestra información de la trama completa y luego se va mostrando información de cada uno de los niveles, empezando desde el nivel de enlace, a continuación red, transporte y aplicación (si es que aparecen todos, cosa que no siempre ocurre). En cada línea hay un "+" a la izquierda para desplegar la información del protocolo asociada a cada nivel (una vez interpretada por la herramienta). No toda la información que aparece de un

determinado protocolo forma realmente parte de dicho protocolo. A veces Wireshark añade información que ha determinado como resultado de un análisis que ha realizado a nivel global, en cuyo caso esta información aparece entre corchetes []. Por otro lado, tampoco todo lo que aparece detrás de un "+" es necesariamente un protocolo. Por ejemplo, Wireshark es capaz de analizar diferentes formatos de ficheros como GIF, PNG, JPG, etc. y los muestra a la derecha de un "+". Seleccione con el ratón una trama que en la columna "Protocol" muestre HTTP y fíjese en los nombres de los protocolos que aparecen en el panel central. En caso de no encontrar ninguna, deberá volver a iniciar la captura en Wireshark y recargar en el explorador la misma página (<http://www.labc.usb.ve>), pulsando sobre el icono de recarga . Espere a que acabe la carga y detenga la captura en Wireshark.

12. El panel inferior, "Bytes de la trama", muestra un volcado en hexadecimal y en ASCII del contenido de la trama seleccionada. Los datos en hexadecimal (en la parte izquierda) se presentan en filas de 16 bytes, junto con una primera columna que indica la posición relativa (dentro de la trama) del primer octeto de la fila. Si en el panel central se hace clic en alguno de los niveles (o en algún campo dentro de estos) se resaltan con fondo oscuro en el panel inferior los bytes asociados a aquello sobre lo que hemos hecho clic. Al revés también funciona, pulsando sobre bytes del panel inferior y viendo en el panel central como se selecciona el campo de información correspondiente. Haga clic en "detalles de trama" en "Hipertext Transfer Protocol" para seleccionar el protocolo HTTP. ¿Qué información aparece en ASCII en "bytes de tramas"? Pulse sobre el "+" que aparece al lado de "Hipertext Transfer Protocol" en "detalles de trama", observara el contenido de la HTTP_PDU. Haga clic varias veces en diferentes líneas de cabecera y observe como se ve en ASCII esa información. ¿Como se muestra en ASCII los códigos de control '\r' y '\n'?
13. Como sabe, el contenido mostrado en el listado de tramas puede ser guardado en un archivo (entrando en File → Save o haciendo clic en ), el cual puede ser cargado en cualquier otro momento (entrando en File → Open o haciendo clic en ). Esto le puede ser de gran utilidad si le faltase tiempo para completar esta práctica, pues se puede guardar lo capturado y utilizarse en otro momento. Respecto a las marcas de tiempo, mostradas en la columna "Time" del listado de tramas, la primera trama tiene por defecto la marca 0.000000 segundos y el resto de marcas van incrementándose respecto a esta. No obstante, es posible establecer una marca de referencia en cualquier trama de forma que sea el "cero" para todas las tramas a continuación de ella, que verán su marca de tiempo modificado considerando esa referencia, lo cual es útil para medir tiempos entre tramas desde una primera que será la que tomemos como "referencia". Para ello seleccionamos la trama que queremos marcar como referencia con clic derecho y elegimos "Set Time Reference (Toggle)", apareciendo *REF* en esa trama y modificándose el tiempo de las tramas siguientes. Si repetimos la operación

se quita la referencia de esa trama. Tenga en cuenta que puede haber varias "referencias locales" en el listado de tramas.

14. Fíjese que en el listado de tramas hay varias tramas que contienen PDUs del protocolo HTTP (fíjese en el valor de la columna "Protocol"). Concretamente, debe encontrar una trama que muestre en la columna "Info" que contiene una petición GET (buscar una página web) del protocolo HTTP.
15. La petición GET la ha emitido el proceso cliente, que está asociado a un determinado puerto en el host origen ("source host"). Gracias a la columna SrcPort (puerto fuente o puerto origen) podemos averiguar con facilidad el número de puerto asociado al proceso cliente.
16. Compruebe que el valor numérico de la columna DstPort de la trama que encapsula el GET es el valor habitual usado por un proceso servidor del protocolo HTTP. Anótelo.
17. Compruebe también en la columna "Destination" el nombre que aparece como nombre del servidor del laboratorio C.
18. Ahora vamos a hacer que la trama con el GET pase a ser la "referencia temporal" con respecto a la cual medir los tiempos de captura de las tramas capturadas detrás de ella. Para ello seleccione dicha trama haciendo clic sobre ella con el botón derecho del ratón y seleccione en el menú contextual que le aparece la opción "Set Time Reference (Toggle)". Fíjense que ahora esa trama no tiene marca de tiempo en la columna "Time" sino que aparece el texto *REF*. Es posible anular esta operación repitiendo los mismos pasos que hemos dado sobre esa trama.
19. Localice, detrás de la trama del GET, una trama que encapsule la respuesta HTTP a dicho GET. En la columna "Info" de la respuesta debe aparecer la línea de estado "HTTP/1.1 200 OK" o bien la línea de estado "HTTP/1.1 304 Not modified", dependiendo de las circunstancias en que se generó el GET con el navegador.
20. Compruebe que en la respuesta se usan los mismos puertos que en la solicitud, pero puerto origen es ahora puerto destino y viceversa.
21. Compruebe que ocurre lo mismo con los valores de las columnas "Source" y "Destination".
22. Como hemos hecho que la trama del GET sea la referencia temporal de todas las tramas que le siguen, es muy fácil medir el tiempo transcurrido entre la emisión del GET y la recepción de la respuesta. Este tiempo se denomina RTT y es lo que tarda el mensaje en ir desde el computador al servidor, y volver la respuesta. Anote su valor.
23. Wireshark es capaz de, a partir de una trama cualquiera que contenga una T_PDU del protocolo TCP (o UDP), localizar todas las demás T_PDU que se transmitieron en la misma conexión TCP que ella (o en el caso de UDP, las T_PDU entre el mismo cliente y servidor usando una determinada pareja de puertos UDP). Gracias a eso puede mostrarnos el flujo de bytes transmitidos a través de esa conexión TCP por los procesos cliente y servidor (o el intercambio de A_PDUs en el caso de UDP). Seleccione la trama del GET haciendo clic sobre ella con el botón derecho del ratón y seleccione en el menú contextual que le aparece la herramienta "Follow TCP Stream". (Nota: Para UDP sería "Follow UDP Stream")

24. En la ventana "Follow TCP Stream" podemos ver en color rosa los bytes enviados por el proceso cliente y de color morado los bytes enviado por el proceso servidor. Si el cliente y el servidor mantienen un dialogo "largo" a través de una misma conexión (como en las conexiones HTTP persistentes) podría verse como se van alternando los mensajes del cliente y del servidor.
25. Ahora vamos a ver los **Filtros de visualización**
En el cuadro de texto etiquetado "Filter:" que aparece bajo la barra de iconos de Wireshark se puede escribir una expresión lógica con una determinada sintaxis, que hace que se muestren en el listado de tramas solo aquellas que hacen que la expresión lógica sea cierta. Esta expresión lógica recibe el nombre de "**filtro**" y solo afecta a lo que se muestra en el listado de trama, es decir, ni elimina una trama ya capturada ni tampoco es tenido en cuenta a la hora de decidir si una trama debe o no capturarse. Se trata solo de un filtro de visualización ("display filter") y no de un filtro de captura ("capture filter").
26. Hay muchas expresiones de filtrado que podemos introducir para cada protocolo reconocido por Wireshark. Puede ver todas las expresiones que hay para cada protocolo, haciendo clic en el botón "Expression...", pero si conoce la expresión puede escribirla directamente en el cuadro de texto "Filter:".
27. Wireshark va mostrando una ayuda con las expresiones compatibles con lo que ya lleva escrito e incluso las autocompleta a medida que las escribe. Si la expresión es correcta aparecerá con fondo VERDE y si es incorrecta el fondo será ROJO. Para que Wireshark utilice el filtro que acabamos de escribir, es necesario pulsar sobre "Apply", opción que podemos ver a la derecha del filtro. Si deseamos volver a ver todas las tramas basta con pulsar sobre "Clear". Pulse ahora sobre "Clear" si el cuadro de texto "Filter:" mostrase algun filtro. Algunas expresiones básicas son:
- a) "**ip.addr == 193.1.10.1**", que muestra tramas que contienen R_PDUs cuya dirección IP origen o destino sea la 193.1.10.1.
 - b) "**tcp.port == 80**", para mostrar el trafico con numero de puerto origen o destino el 80.
 - c) "**udp.port == 53**", que hace lo mismo pero con UDP.
 - d) "**ip.src**" y "**ip.dst**" son parecidos a "ip.addr" pero solo se fijan en que la IP especificada este en el origen o en el destino.
 - e) "**tcp.dstport**" y "**tcp.srcport**" se fijan solamente en el puerto destino o el origen.
 - f) "**http**", "**dns**", "**tcp**", "**udp**" y "**icmp**" son expresiones sencillas que hacen que solo se muestren tramas que encapsulen PDUs de esos protocolos.
28. Es posible construir expresiones lógicas complejas combinando expresiones sencillas con los operadores lógicos "**and**", "**or**" y "**not**". Por ejemplo "**http or dns**" captura tramas que hacen que la expresión lógica "combinada" sea cierta. Es decir, aquellas que hacen que "http" sea cierta y también aquellas que hacen que "dns" sea cierta. También es posible utilizar el operador "**contains**" que permite buscar cadenas dentro de la PDU de un protocolo,

por ejemplo, "**http contains GET**" permitiría ver todas las tramas que encapsulan PDUs HTTP que contienen la palabra "GET". Otro ejemplo con este operador sería "**dns contains www**" que nos dejaría ver solo las tramas con PDUs DNS en las que aparezca la cadena "www".

Fijese que si marca una trama como referencia temporal con *REF* (recuerde el apartado 22), esa trama siempre se visualiza en el listado de tramas, sea cual sea el filtro de visualización aplicado.

29. Vamos a probarlo: Si no tiene una captura hecha que le llene completamente el listado de tramas, haga una nueva generando el tráfico de red que sea necesario y luego detenga la captura.
30. Escriba un filtro sencillo, como "http", "tcp", "udp", etc. y aplíquelo.
31. Observe como en el borde inferior de la ventana de Wireshark aparece el texto "Packets:" indicando el número total de tramas capturadas y el texto "Displayed:" indicando el número de tramas que han pasado el filtro de visualización y pueden verse en el listado de tramas.
32. Haga clic en "Clear" para borrar el filtro de visualización y volver a ver todas las tramas capturadas.
33. Aplique un filtro que muestre solo el tráfico de nivel de red con origen o destino su propia IP. En un momento explicare como conseguir la dirección IP de su máquina

Segunda Parte: Manejo del GNS3

- **Descargar e Instalar gns3:** Para descargar gns3 (pagina señalada arriba) es necesario registrarse, proporcionando una dirección de correo electrónico y una contraseña.

Como es usual, se envía un correo a la brevedad que hay que confirmar para hacer efectivo el registro. Se puede omitir este paso y utilizar el paquete suministrado en clases hay dos versiones:

- o GNS3-1.3.13-all-in-one para windows de 32 bits.
- o GNS3-1.5.3rc1-all-in-one para windows de 64 bits.

Luego instale la versión correspondiente a su sistema operativo.

Gns3 es una herramienta que nos permite virtualizar redes a través de la emulación e interconexión de dispositivos.

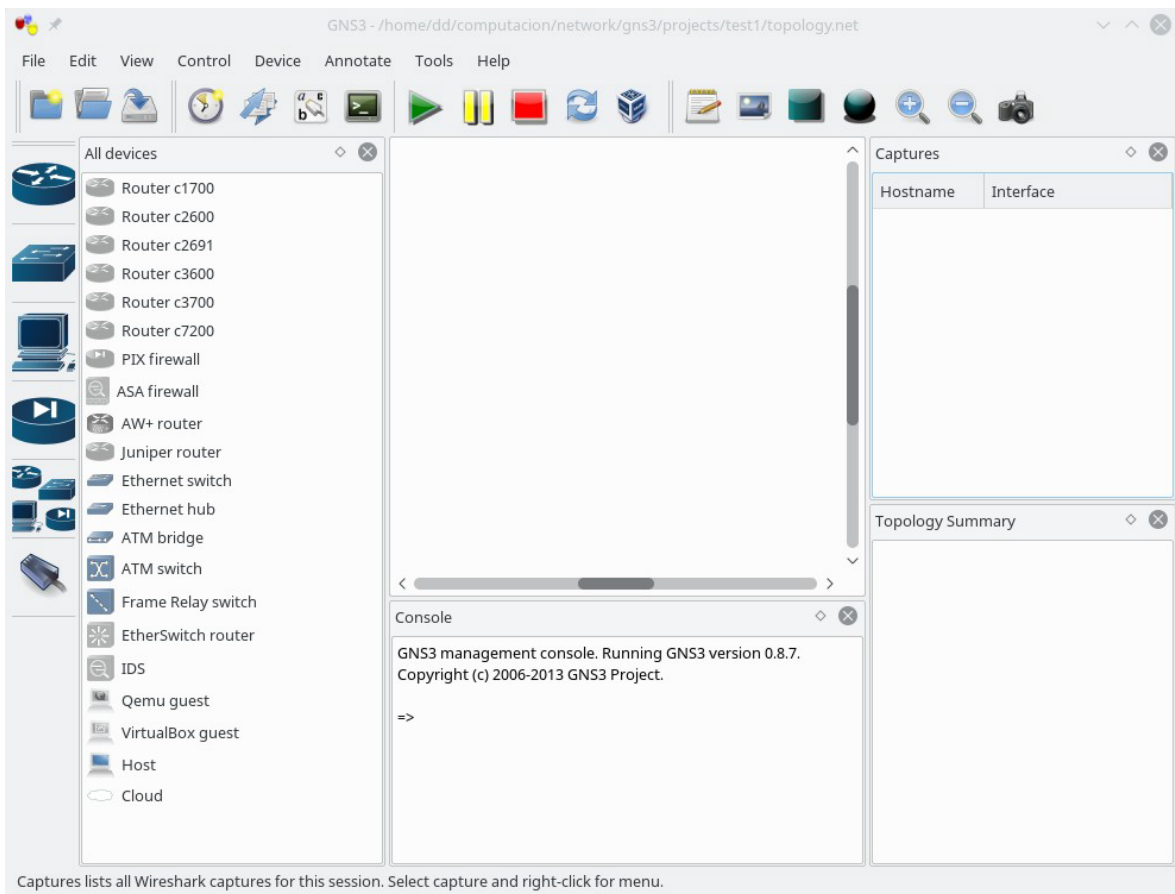
Nota: el paquete suministrado en clases contiene todo lo necesario, no se requieren otros elementos. Debe instalarse todo lo contenido.

Recomiendo ampliamente ver los tutoriales que están en youtube sobre el producto, ayudan bastante a conocerlo e iniciar en su uso. Uno de los mejores esta en:

https://www.youtube.com/watch?v=vVYWrgAOke4&index=1&list=PL3UpcvaDU_Fkfu9wnEBvF_XBR6KeMg8jv

Son 30 videos pero los 11 primeros explican la herramienta.

- Una vez instalado, el gns3 se debe ver más o menos así:



Ya aquí están instalados diversos dispositivos, en su versión probablemente no haya ninguno.

Para eso se suministra un paquete comprimido que contiene múltiples dispositivos: GNS3 IOS

Cuando es seleccionado el penúltimo ítem de la columna izquierda muestra todos los dispositivos. Los dispositivos pueden estar en color opaco cuando no tienen imágenes o roms instalados (en las versiones más nuevas no aparecen), por ende no pueden ser seleccionados o utilizados.

En esta práctica solo vamos a utilizar equipos que ya están en el paquete básico.

Tercera parte: Uso de IPCONFIG

En cualquier arquitectura básica de red se requiere tener configurados, como mínimo, los siguientes tres parámetros en el nivel de red:

- Una dirección de nivel de red propia (dirección IP) que lo identifique de manera única.

- La dirección de nivel de red de un router frontera que le de acceso a Internet, conocida en Windows como puerta de enlace predeterminada.
- Una máscara de subred.

(Nota: el significado y uso de estos parámetros se verá más adelante en la asignatura, pero se requiere su uso para las prácticas de laboratorio)

Los parámetros anteriores, y algunos más, forman parte de lo que se conoce como configuración TCP/IP. La configuración TCP/IP de un PC puede ser introducida manualmente o bien ser obtenida de forma automática por el propio PC. Si se hace de forma automática, la configuración TCP/IP se obtiene generalmente de un servidor DHCP usando el protocolo DHCP. Como curiosidad puede investigar que esto pero se verá más adelante en las clases.

Para ver los parámetros de la configuración TCP/IP de su PC, y de un servidor, puede utilizar el comando **ipconfig**, disponible en la mayoría de los SO Windows. Para ello:

1. Abra una ventana de Símbolo del sistema (Command Prompt) y ejecute en ella el comando **ipconfig /all** para ver toda la configuración TCP/IP de su PC. Puede abrir una ventana de Símbolo del sistema haciendo doble clic sobre el icono presente en el escritorio o bien siguiendo "Inicio" > "Todos los programas" > "Accesorios" > "Símbolo del sistema". Tenga en cuenta que la única información del comando ipconfig que nos va a interesar es la relativa al Adaptador de Ethernet Conexión de área local, por lo que no debe prestar atención a la información de los otros dos adaptadores etiquetados Adaptador de túnel. Por otro lado, tenga en cuenta que el comando ipconfig "a secas" ofrece un resumen con la información más importante de la configuración TCP/IP, pero que para verla toda hace falta el comando ipconfig /all.
2. ¿Cuál es la dirección IP asignada a su PC?
3. ¿Cuál es la máscara de subred?
4. ¿Cuál es la dirección IP de su puerta de enlace predeterminada (router frontera)?
5. ¿Cuál es la dirección IP del servidor DHCP?
6. La configuración TCP/IP obtenida automáticamente desde un servidor no tiene normalmente una validez "infinita" sino que el servidor nos concede una "licencia" de uso que expira al cabo de un tiempo (aunque podemos ir renovando dicha "licencia" de uso). ¿Cuántas horas o minutos de "licencia" de uso tiene su PC sobre la configuración TCP/IP actual?
7. Indique lo que ocurre al ejecutar el comando **ipconfig /release** en una ventana de Símbolo del sistema, (fíjese bien en los tres parámetros básicos de su configuración TCP/IP). A continuación ejecute también el comando **ipconfig /all** y piense en lo que ha conseguido al hacer el "release" de la configuración (liberación).
8. Indique lo que ocurre al ejecutar el comando **ipconfig /renew** (fíjese bien en los tres parámetros básicos de su configuración TCP/IP). A continuación ejecute de nuevo el comando **ipconfig /all** y piense en lo que ha conseguido al hacer el "renew" de la configuración (renovación).
9. En el área de notificación de la barra de tareas existe un icono que informa sobre el estado de la Conexión de área local, cambiando a veces su aspecto.

Si hace clic sobre ese icono y luego clic sobre Abrir Centro de redes y recursos compartidos y a continuación hace clic en el texto Conexión de área local le aparecerá una ventana titulada Estado de Conexión de área local en la que podrá ver el estado de la conexión. ¿Cuál es el ancho de banda (R) de su conexión?

10. Desconecte el cable de red de su PC o de la roseta de la pared (o apague el wifi de su máquina) y observe que el icono cambia de aspecto. Además, si mueve el ratón sobre el icono le aparece un mensaje y si hace clic sobre él también podrá ver un mensaje. Fíjese bien en esos mensajes informativos y en el aspecto del icono.
11. Conecte de nuevo el cable (o encienda el wifi) y observe que el icono vuelve a cambiar de aspecto. Además, si mueve el ratón sobre el icono le aparece un mensaje y si hace clic sobre él también podrá ver un mensaje. Fíjese bien en esos mensajes informativos y en el aspecto del icono.
12. ¿Es posible saber si el cable está conectado/desconectado observando este icono? Esto sería una prueba de funcionamiento del nivel físico, conocida como "conectividad de nivel físico".
13. En los VPC del GNS3 el comando a usar es **ip** (es una simplificación de ipconfig), trabaja de forma similar pero basta ejecutar, desde su consola, **ip x.x.x.x/y** para asignar una dirección IP a uno de los VPC. Averigüe las demás funciones del comando IP en los VPC.

Cuarta Parte: Uso de PING

Si bien estamos trabajando a nivel de capa 2, necesitamos de un comando de un nivel un poco más alto para generar tráfico cuando lo deseemos, por ello vamos a utilizar el comando ping. Este sirve para probar que dos equipos que tengan conectividad en el nivel de red y pueden intercambiar entre ellos las PDU de ese nivel (R_PDU), es decir, permite realizar una prueba de conectividad de nivel de red. Al ejecutar este comando desde un equipo origen hacia un equipo destino, el origen envía al destino una R_PDU especial (solicitud de eco), que cuando la recibe está obligado a responder al origen con otra R_PDU especial (respuesta de eco).

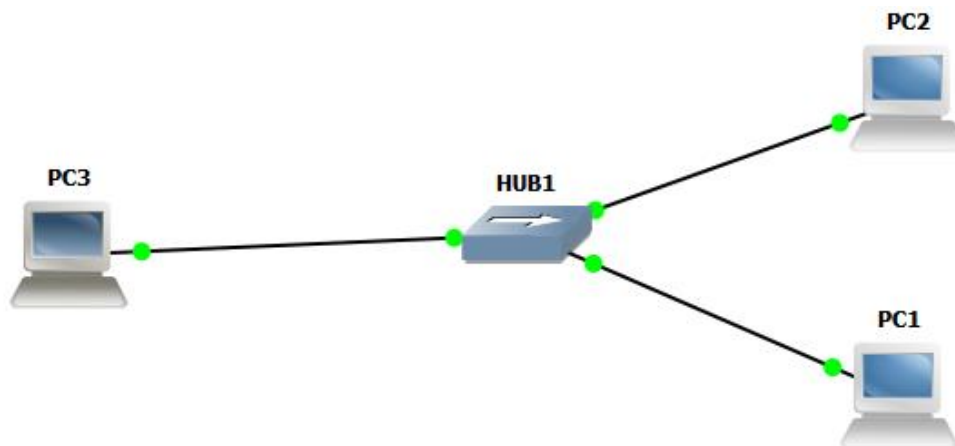
1. El comando ping se debe ejecutar en una ventana "Command Prompt", pero en los VPC se puede hacer desde la consola de cada uno, requiere como parámetro obligatorio la dirección IP o el nombre del equipo destino.
2. Como ejercicio haga un ping desde su PC usando como dirección de destino su router frontera (véase el ipconfig). Por defecto, el comando ping de Windows envía cuatro R_PDUs al equipo destino, es decir, realiza cuatro pruebas de conectividad de nivel de red. El comando ping nos muestra en pantalla una línea de información para cada una de las cuatro solicitudes de eco enviadas. Si de una solicitud de eco ha recibido una respuesta de eco, la línea de información empieza por "Respuesta desde" y a continuación aparece la IP del equipo que nos ha enviado la R_PDU. ¿Cuántas respuestas del router frontera ha recibido el comando ping que acaba de ejecutar?

3. ¿Es obligatorio que en el otro extremo (equipo destino) exista una entidad par de nivel de red para que el comando ping reciba respuesta?
4. ¿Utiliza el comando ping los servicios de algún nivel para enviar la R_PDU? En caso afirmativo indique el nombre del nivel y el porqué.
5. Haga un ping al equipo 8.8.8.8. Observe como en la información que ofrece el comando ping cuando recibe la respuesta de cada una de las solicitudes de eco informa del tiempo transcurrido desde que se inició el envío de la R_PDU en el equipo origen hasta que se recibió la R_PDU de respuesta de eco. Comprueba si las cuatro solicitudes han obtenido respuesta y si lo han hecho en el mismo tiempo.
6. La R_PDU en su viaje de ida y vuelta atraviesa varios nodos intermedios (routers), cada uno de los cuales contribuye con su retardo nodal al retardo que nos muestra el comando ping. ¿Qué fuentes de retardo contribuyen al retardo nodal?

Laboratorio:

1) Captura y observación de paquetes en una red Ethernet básica:

- a) Ejecute GNS3 y construya la siguiente configuración: El HUB es el que viene incluido con la herramienta (no se necesita cargar un dispositivo nuevo). Utilice los VPC como maquinas de trabajo. Investigue para que sirven los otros dos equipos: HOST y CLOUD.



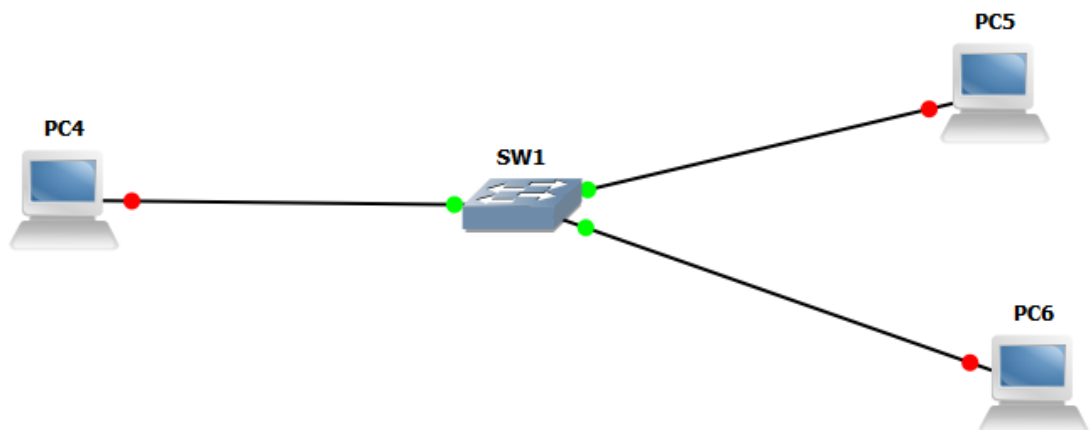
- b) Note que su pantalla las interfaces del switch está en rojo. Eso indica que los equipos no están encendidos. En la barra superior de gns3 se encuentra la opción de encender todos los equipos.
- c) Una vez seleccionada dicha opción, inmediatamente se colocan las interfaces en verde.
- d) Cada objeto tiene accesible diversas propiedades cuando es seleccionado con el botón derecho del ratón. Obviamente según su

naturaleza se puede disponer de diferentes opciones. También permite entrar en su consola de programación

- e) A los VPC's asígneles direcciones IP sencillas (Pe: 10.10.10.1/24, por su puesto distintas una a cada uno).
- f) Conecte los VPC's en cualquiera de los puertos del HUB (para uno de ellos no use puertos continuos).
- g) Capture la data con el Wireshark (si activa el botón derecho sobre el VPC o sobre un puerto específico del HUB, le permitirá capturar datos con el Wireshark) en uno de los puertos del HUB donde esté conectado un VPC, para generar datos desde ese VPC envíe "Ping" a otro equipo de la red.
- h) Revise los paquetes capturados y trate de identificar las tramas Ethernet y sus distintos campos (anexe esas tramas en la tarea indicando sus partes).
- i) Envíe un ping al tercer VPC, pero capture data en un puerto del HUB donde esté conectado el otro VPC (al que no envió el ping), ¿Qué sucede?

2) Captura y observación de paquetes en una red switch Ethernet:

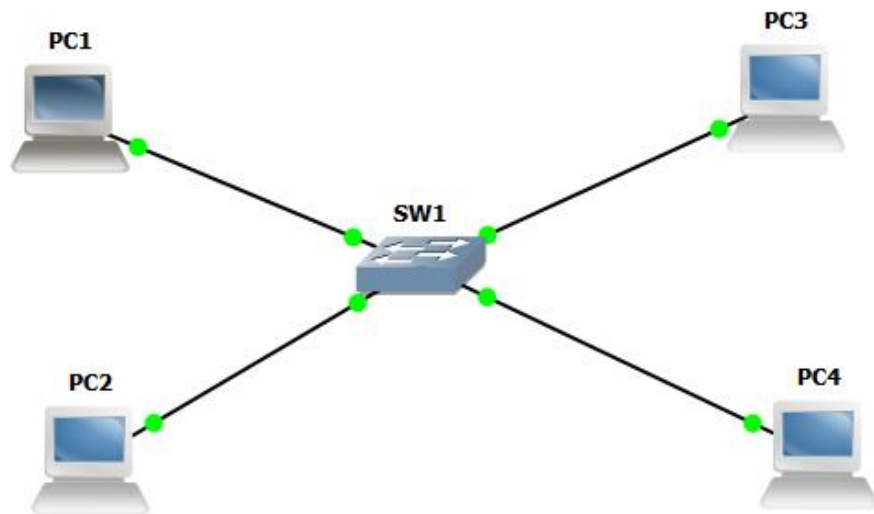
- a) Ahora construya la siguiente configuración (recomiendo salvar el proyecto anterior y crear uno nuevo): El Switch a utilizar será el Ethernet básico que viene incluido en gns3.



- b) Igual al caso anterior asigne direcciones IP a los VPC's y conéctelos al Sw en cualquier puerto (para uno de ellos no use puertos continuos)
- c) Capture la data en uno de los puertos del Sw donde esté conectado un VPC (igual al caso anterior envíe ping a otro de los VPC's).
- d) Envíe un ping al tercer VPC, pero capture data en un puerto del Sw donde esté conectado el otro VPC (al que no envió el ping), ¿Qué sucede?
- e) Compare con el caso 1, Indique si hay diferencias entre un caso y otro.

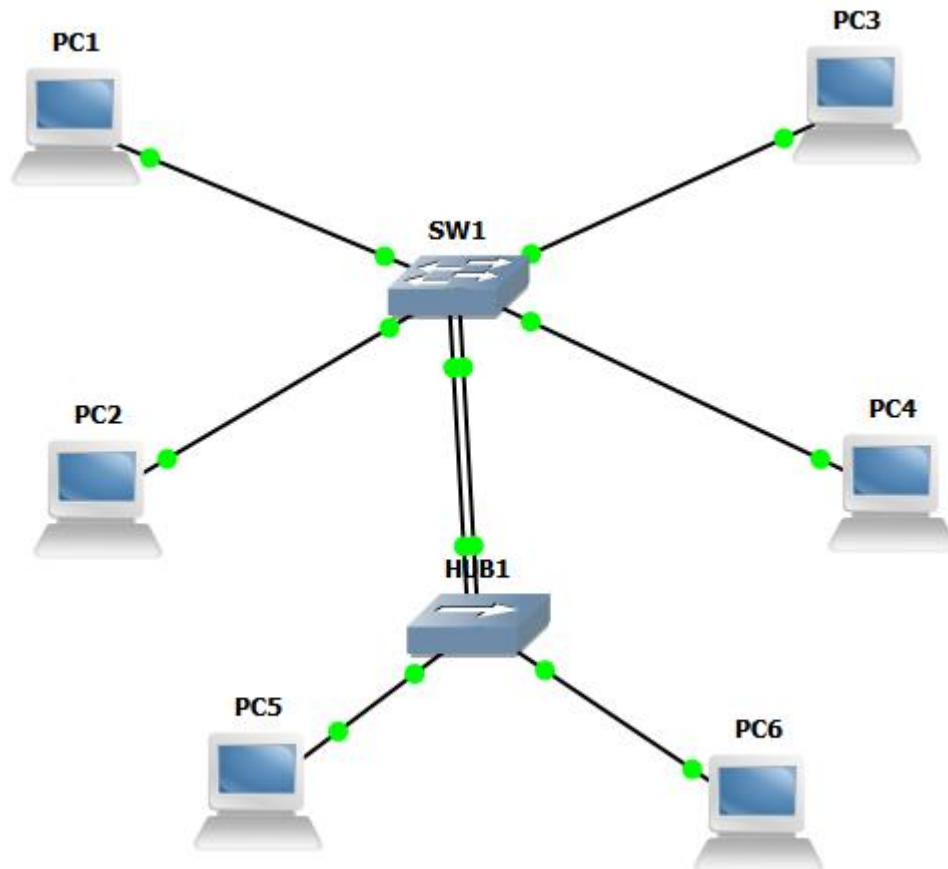
3) Captura y observación de paquetes en una red switch Ethernet con VLAN's:

- a) Ahora vamos con una nueva configuración (recuerde salvar la anterior). De nuevo utilizaremos el Switch básico.



- b) Con el botón derecho vaya a la configuración del SW1 y en la ventana de los puertos asigne los puertos impares del SW a una VLAN (por ejemplo VLAN 1, por lo general todos están ya en esa) y los puertos pares a otra VLAN distinta (Pe VLAN 2, 3 o 4). Conecte los VPC 1 y 3 a los puertos impares y los VPC 2 y 4 a los pares. Igual al caso anterior asigne direcciones IP a los VPC's, pero ahora use las IP 10.10.10.X/24 para los impares y 10.10.15.X/24 para los pares.
- c) Capture la data en uno de los puertos del Sw donde esté conectado un VPC (igual al caso anterior envíe ping a otro de los VPC's). Pero dentro de la misma VLAN.
- d) Envíe un ping a un PC que pertenezca a otra VLAN. Recuerde colocar el Wireshark para capturar los envíos. ¿Qué sucede?
- e) Haga pruebas enviando ping entre los distintos equipos, desde cuales se acepta y hay respuesta y desde cuáles no. ¿Por qué sucede eso?
- f) Ahora cambien la IP de un equipo par de la red 10.10.15.X (el 2 o el 4) a una dirección de la red 10.10.10.X, intentemos hacerle ping desde varios VPC's de ambas redes lógicas, ¿Qué sucede?
- g) Vuelva a colocar las direcciones IP como al inicio, pero agregue un HUB como se muestra en la imagen siguiente, y conecte uno de los puertos del HUB a un puerto de la VLAN par del Sw y otro a un puerto de la VLAN impar, en otras palabras está conectado físicamente las dos VLAN's. Luego agregue dos VPC's mas pero conéctelos en el HUB, a uno de

- estos VPC colóquele una IP de la red 10.10.10.X y a otro de la red 10.10.15.X. ¿Se logra que así que todos los puertos se comuniquen?
- h) Vea el trafico en los dos puertos del HUB conectados al Sw haciendo ping a los distintos VPC's de ambas VLAN, ¿qué ocurre?, ¿en qué casos se ve el trafico en cada puerto?



- i) Ahora cambien la IP de un equipo par de la red 10.10.15.X (el 2 o el 4) a una dirección de la red 10.10.10.X, intentemos hacerle ping desde varios VPC's de ambas redes lógicas, ¿Que sucede?
- j) ¿Cómo se soluciona que todos los equipos de distintas VLAN se puedan comunicar?

Con esto concluye la práctica, elabore el informe como fue indicado.

Para la entrega del informe se le dará acceso, a usted y a su compañero de laboratorio, a una carpeta identificada con su grupo, la cual estará abierta desde la fecha de la práctica hasta el lunes siguiente a las 8:00 am. Si no sube el informe antes del cierre, será como si no hubiese participado en la misma y su evaluación practica quedara sin nota.