# Objetivos

Esta experiencia tiene como objetivo que el alumno pueda aprender de manera práctica el envío de datos y el funcionamiento de protocolos a nivel de capa de enlace.

# 

# Instrucciones

1. Fecha de entrega: **Viernes 14 de mayo de 2021 hasta las 23:55.**
2. La entrega consta de un informe PDF que contiene el desarrollo de las actividades.
3. La entrega del informe se realiza a través de la plataforma Uvirtual.
4. Cualquier copia detectada entre los trabajos será calificada con nota mínima y será causal de sumario.
5. Los comandos utilizados pueden tener variaciones dependiendo del sistema operativo que esté usando.

**Herramientas**

GNU/Linux. En este laboratorio se usarán varias herramientas para analizar redes que generalmente están disponibles en las distribuciones GNU/Linux. Otros sistemas operativos pueden ofrecer herramientas similares pero queda bajo su responsabilidad buscar el soporte.

[Nmap](https://nmap.org/). Se utilizará para averiguar la topología de la red. Utiliza diferentes técnicas y protocolos para determinar qué computadores están activos, qué puertos están abiertos y qué servicios hay disponibles. Posee una interfaz gráfica llamada zenmap, aunque basta con utilizar la línea de comandos. Se instala fácilmente en cualquier sistema Linux. Esta utilidad tiene muchas opciones, se recomienda leer la documentación para más detalles.

En la mayoría de las distribuciones GNU/Linux encontramos los comandos arp, ifconfig, ip, ping. Los paquetes net-tools, iputils e iproute2 deberían proveer estos programas.

[Iperf3](https://iperf.fr/). Es una utilidad para medir la velocidad de un enlace en internet. Se instala en dos dispositivos donde uno hace de servidor y otro de cliente. Está disponible para instalar en la mayoría de las distribuciones GNU/Linux. También tiene una aplicación para Android, y también existe Magic iPerf. Otra aplicación móvil de utilidad es Network Analyzer.

[Wireshark](https://www.wireshark.org/). Es un analizador de protocolos que permite realizar capturas de tráfico de la red en tiempo real y obtener todos los datos de cada paquete involucrado. Vea el anexo con una guía de uso de este programa.

**Desarrollo**

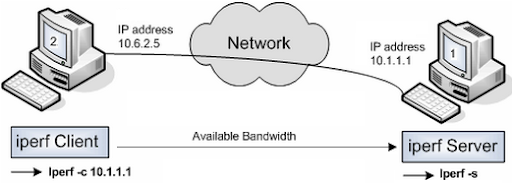
Utilizando las herramientas mencionadas, realice las siguientes actividades. En lo posible realice las pruebas en un ambiente controlado, en particular evite usar otros programas que generan tráfico en la red (torrent, descargas, streaming, sincronización de archivos, etc). Registre todos los procedimientos y resultados, pues serán de utilidad en su informe.

1. **Capa física y de enlace** : El objetivo es obtener un mapa detallado de su red local y analizar la capacidad de la red.
   1. Utilice el comando **ifconfig** para conocer la IP de su computador y el rango de direcciones de su red local.
   2. Encienda y conecte algunos dispositivos (ej. su celular y notebook) a la misma red.
   3. Utilice nmap (ej: **nmap -sn <rango-ip>**) para detectar todos los dispositivos que están conectados en su red local. Reporte los resultados en una tabla como la **Tabla 1.**
   4. Realice una inspección de los dispositivos y/o use alguna aplicación para determinar cómo los dispositivos de la red local están conectados en la capa física. Determine: tecnología de capa física, protocolo de capa física, protocolo de capa de enlace, velocidad del enlace. Agregue los resultados en la **Tabla 1.**

**Tabla 1.** Dispositivos conectados en la red local

|  |  |  |  |
| --- | --- | --- | --- |
| Dispositivo | Capa física | Dirección MAC | Dirección IP |
| *Ej: Marca, modelo y descripción del equipo* | *Ej: Conexión (versión wifi, frecuencia, canal), velocidad, protocolos* | *Ej: FF:FF:FF:FF* | *Ej: 1.1.1.1* |

* 1. Con la información de la Tabla 1 realice un diagrama de la red. Agregue toda la información relevante al diagrama.
  2. Utilice **iperf3** para realizar un test de velocidad entre dos dispositivos de su red local (ver Fig. 1).
     1. En el dispositivo servidor ejecute: **iperf3 -s**
     2. En el dispositivo cliente ejecute: **iperf3 -c <IP\_SERVER> -u -b <N>M**
        1. <IP\_SERVER> es la IP del dispositivo que actúa como servidor
        2. <N> es la tasa de datos objetivo. Varíe este parámetro entre 1 y 1000.
     3. Realice varias pruebas variando el parámetro N. Reporte sus resultados a través de gráficos (tasa de datos, % pérdidas).
     4. Analice los resultados obtenidos. Compare las tasas de datos obtenidas con las capacidades de los enlaces (Tabla 1), explique los resultados. Existen pérdidas de datagramas ¿Por qué?.



**Figura 1**. Esquema de uso de Iperf3

1. **Protocolo ARP.** En esta sección estudiaremos el funcionamiento del protocolo ARP. Lea y comprenda las instrucciones antes de ejecutar la actividad.
   1. Inicie la captura de paquetes ARP con Wireshark en la interfaz de red que está usando. Utilice un filtro para el protocolo ARP.
   2. Vacié la tabla ARP con el siguiente comando **sudo ip -s -s neigh flush all**
   3. Obtenga la tabla arp actual con el siguiente comando: **arp -n**
      1. Registre y analice los resultados. ¿Qué dispositivos aparecen en la tabla? ¿Por qué?
   4. Trate de conectarse a alguno de los dispositivos de la red local que no aparecen en la tabla ARP, por ejemplo usando el comando **ping <ip>.** Observe el tráfico en Wireshark y capture los paquetes de pregunta-respuesta ARP relacionada con la conexión anterior. Guarde y/o detenga la captura para analizar los resultados.
   5. Obtenga nuevamente tabla arp actual con el siguiente comando: **arp -n**
      1. Registre y analice los nuevos resultados. ¿Qué dispositivos aparecen en la tabla? ¿Por qué?
   6. Presente un análisis de los paquetes ARP capturas en el punto D. Describa los campos de los mensajes y la secuencia de los mensajes. ¿A quién van dirigidos los mensajes? ¿Quién responde los mensajes?
   7. Analice en general el tráfico ARP observado durante la prueba. ¿Qué ocurre en su red? ¿Qué dispositivos generan y responden los mensajes? ¿Cree que su tráfico es normal?,¿por qué?.

**Informe**

Se debe enviar un informe de laboratorio en formato PDF con todo el trabajo realizado y que incluya al menos las siguientes secciones:

* **Introducción** (0.5 - 1.0 página): Contexto, objetivos e información bibliográfica de relevancia (no es necesario repetir información que existe en la bibliografía, pero sí citar y/o sintetizar). *¿Qué se hará y por qué?*
* **Marco Teórico:** Explicaciones básicas sobre todos los temas y tópicos tratados en la actividad. Tenga presente que las herramientas utilizadas no son parte del marco teórico.
* **Desarrollo y resultados**: Explicación del trabajo realizado, respondiendo todos los puntos y preguntas. Incluir algoritmos y/o códigos (extractos, resumen), diagramas, imágenes y tablas. *¿Qué se hizo y qué se obtuvo?*
* **Análisis de resultados**: Análisis de cada resultado, ¿está correcto?, ¿por qué salió ese resultado?, relacionar resultados con los contenidos del curso. *¿Tienen sentido mis resultados?, ¿por qué obtuve estos resultados?*
* **Conclusiones** (0.5 - 1.0 página): Síntesis de los principales resultados encontrados y su relación con los contenidos vistos en clases. Problemas encontrados y cómo fueron solucionados. Conclusiones personales. ¿*Qué aprendí con este trabajo*?
* **Bibliografía**: Listado de referencias usadas en el trabajo. ¡Todas!. Libros (indicando capítulos), publicaciones, sitios web y videos (enlace y fecha de última visita), material de clases, etc. Formato APA. *¿Qué fuentes utilicé en este trabajo?*

**Recomendaciones**:

1. Si luego de capturar los datos desconecta y conecta dispositivos recuerde que es probable que la dirección IP cambie.

**Notas**

1. Dudas y consultas serán respondidas por medio de Uvirtual.
2. Sea conciso y ordenado para entregar la información.
3. Gestione bien su tiempo.

# 

# ANEXOS

## Guía rápida de uso de Wireshark:

* **Panel de lista de paquetes**: Muestra todos los paquetes encontrados luego de la captura de tráfico. Se pueden encontrar las direcciones IP de origen y destino, el protocolo usado, el largo del paquete y un resumen de la información transmitida. Wireshark permite aplicar filtros individuales basados en detalles específicos y seguir flujos de datos basados en el tipo de protocolo haciendo clic derecho en el elemento deseado.
* **Panel de detalles del paquete:** Muestra los protocolos y campos de protocolo del paquete seleccionado en el panel de lista de paquetes. El paquete se separa en las diferentes capas del modelo TCP/IP. Los protocolos y campos del paquete que se muestran en un árbol que se pueden expandir y contraer.
* **Panel de bytes del paquete:** Muestra los datos sin procesar del paquete seleccionado en un formato hexadecimal. La selección de una parte específica de estos datos resalta automáticamente su sección correspondiente en el panel de detalles del paquete y viceversa. Si es posible se muestra la información en texto plano (ASCII)
* Recordar que para la realización de las actividades relacionadas a Wireshark en términos de comandos se debe anteponer el “sudo” para así tener los permisos adecuados.

