Trabajo Práctico N°2

Más conceptos fundamentales de capa física y capa de enlace de datos.

Objetivos:

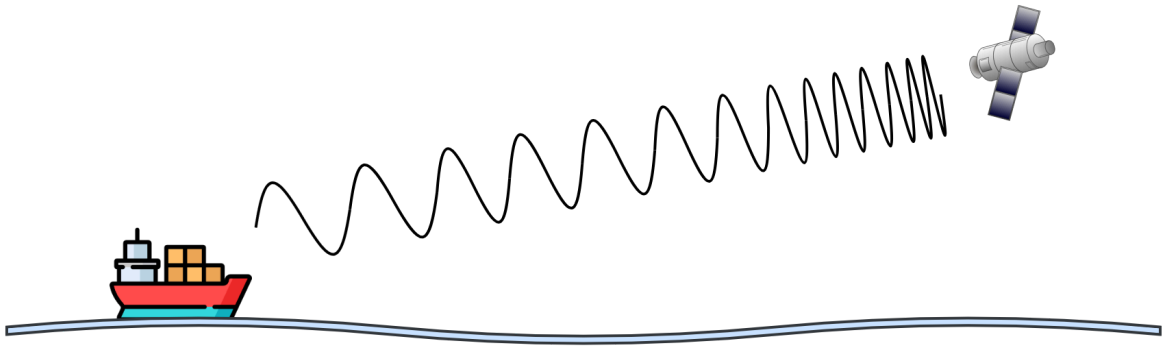
- Terminar de repasar conceptos fundamentales inherentes a la capa **Física (1)**
- Entender los conceptos de la capa de **Enlace de Datos (2)**
- Presentar WireShark, un software analizador de redes.

Requisitos:

- Acceso a una o dos computadoras con Internet.
- Bibliografía de la materia.
- Descargar WireShark y familiarizarse con su uso.

Consignas:

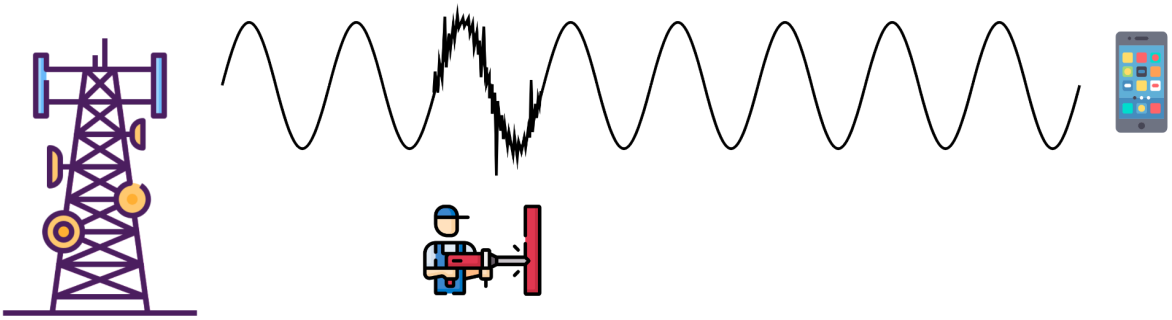
1) Analizar la siguiente Figura:



Y responder:

a) ¿Qué fenómeno físico se está representando en la Figura? ¿Cuáles son las características principales del mismo?
b) Recordando las bandas de transmisión vistas en el TP01, investigar: ¿A qué tipos de transmisión afecta más este fenómeno? ¿Cuáles son más resilientes al mismo?
c) Investigar: ¿Cuáles son las razones por las cuales no se debe encender el celular arriba de un avión? ¿Tiene algo que ver el fenómeno descrito en los puntos anteriores?

2) Analizar la siguiente Figura:



Y responder:

a) ¿Qué fenómeno físico se está representando en la Figura? ¿Cuáles son las características principales del mismo?
b) Recordando las bandas de transmisión vistas en el TP01, investigar: ¿A qué tipos de transmisión afecta más este fenómeno? ¿Cuáles son más resilientes al mismo?
c) ¿Qué es la SNR? ¿Tiene algo que ver con el concepto de BER que vimos en el TP01?

3) Descargar e iniciar WireShark. Explorar la interfaz y opciones. Conectados a internet, capturar tráfico durante unos segundos. Explorar cómo analizar tramas, como exportar datos, como filtrar datos. Luego, resolver los siguientes ítems:

a) ¿Qué es el Ethernet? ¿Cuáles son sus características principales? ¿Cómo se conforma una trama de datos en Ethernet? ¿Qué diferencias hay entre Ethernet, Fast Ethernet, y Gigabit Ethernet?
b) ¿Qué es un cable UTP? ¿Qué relación tiene la construcción de este cable con los conceptos vistos en el ítem 2) de este trabajo? ¿Qué diferencias hay entre un cable UTP "derecho" y uno "cruzado"?
c) Conectado a internet, averiguar la puerta de enlace predeterminada de tu conexión (podés utilizar ipconfig en la línea de comandos en Windows, ifconfig en Linux, o acceder a las opciones de conexión de tu dispositivo). Luego, en wireshark, filtrar los paquetes de esa dirección IP (Ayuda: podés utilizar el filtro **ip.addr** == <**dirección**>). Ejecutar una función ping en la línea de comandos hacia la puerta de enlace, monitorear Wireshark y extraer alguno de los paquetes recibidos. Extraer y documentar en el informe los datos de este paquete, en formato hexadecimal.
d) Extraer de la información del punto anterior la dirección MAC del dispositivo. Documentar la misma e investigar datos del fabricante en internet (utilizar servicios online como este). Documentar el nombre y dirección de la empresa.
e) Repetir los ejercicios c) y d), pero comunicándote con la computadora de un compañero/a. Pueden utilizar el *sender* de paquetes de Wireshark, algún otro emulador, o en última instancia un ping a la IP pública de la otra computadora (si se encuentran de manera remota), o la IP local (si se encuentran en la misma red).

4) Reflexiones finales y conclusiones: según los resultados obtenidos en este trabajo práctico y la información que obtengan de internet, elaborar conclusiones acerca de la privacidad de un dispositivo en la red y la trazabilidad de una dirección MAC. Investigar que es el IMEI y qué similitud tiene con la dirección MAC. Investigar e incluir una respuesta al siguiente interrogante: ¿Una VPN oculta la dirección MAC del dispositivo? No se preocupen si no entienden del todo la respuesta, la veremos cuando sigamos avanzando en las capas del modelo OSI!