Introducción a TCP/IP. Parte 1

Nombre: _____

1. Análisis de frames Ethernet

Habilite la captura de frames en el sniffer (wireshark) de su PC y ejecute el comando ping utilizando la dirección IP del host vecino y la de su default gateway. Analice los distintos campos del frame Ethernet direccionamiento, tipo de frame, etc y escriba sus comentarios.

_____

_____

_____

_____

_____

2. Análisis de protocolo ARP

La primera vez que se envía un frame IP a otro nodo dentro del mismo segmento, es necesario averiguar la dirección Ethernet (MAC) mediante un ARP request, que es un frame no IP, enviado a la dirección de broadcast. Para evitar realizar broadcasts con mucha frecuencia, todos los nodos mantienen una tabla de ARP, observe la tabla de ARP de su PC con el comando **arp –a.** Tome nota de las direcciones MAC e IP asociadas a los distintos hosts:

Nombre Host	**MAC**	**IP**
Mi Host		
Router		

3. Análisis de protocolo IP

Estudie para qué sirven y cómo cambian los paquetes IP utilizando las siguientes opciones de ping:

Comando	**Observaciones**
ping –t	
ping -f	
ping –r	
ping –s	

4. Análisis de protocolo TCP

Con el Sniffer previamente activado, capture el tráfico generado y observe los frames capturados al generar en la red, utilizando los programas de aplicación típicos de Internet como Telnet, ssh, FTP, http.

Analice la sesión telnet y ftp y determine como viaja la información ingresada y en especial visualice el password ingresado.

Active el Sniffer y capture el inicio de una conexión TCP. Observe los primeros 3 frames de una conexión TCP, observando los flags de estos frames y como se establecen inicialmente los números de SEQ y ACK

Anote los números SEQ y ACK iniciales y observe como se incrementan en los segmentos TCP sucesivos:

¿Qué relación existe entre el SEQ enviado por un nodo y el ACK respectivo enviado como respuesta?

¿Cómo se incrementan estos números después de esto tres frames iniciales?

¿Cuál es el "overhead" completo introducido por Ethernet, IP y TCP?

Inicie una sesión FTP y observe las puertas utilizadas. ¿Cuál es la puerta TCP usada?

¿Qué ocurre al iniciar una transferencia de datos?

Inicie una sesión telnet a la primera puerta utilizada por FTP en el paso anterior y verifique con el sniffer qué ocurre, al intentar iniciar una transferencia de datos.

Inicie una sesión http con Internet Explorer y verifique con el sniffer qué ocurre, que datos se intercambian.

Inicie una sesión http con Mozilla y verifique con el sniffer qué ocurre, hay diferencia con el caso anterior, el contenido desplegado es el mismo?.