Guía de Laboratorio

Monitorización de redes mediante *Sniffers*

Ejercicio 1:
Los ***sniffers no son fáciles de detectar ni de combatir***, ya que se trata de programas que trabajan en **modo pasivo**.

La monitorización de redes resulta una herramienta fundamental en dos sentidos. Por un lado, permite apreciar de forma realista muchos de los conceptos fundamentales de las redes en general, y de los protocolos TCP/IP en particular (encapsulación, fragmentación, etc). Por otro lado, permite realizar un diagnóstico muy preciso de las redes en funcionamiento, desde la detección de errores, la verificación de los mecanismos de seguridad y la evaluación de prestaciones de la red.

La monitorización de red, o captura de tramas, consiste en la obtención de todas las tramas que aparecen a nivel de LAN. Puesto que el medio de transmisión es, generalmente, una línea de difusión, esto permitirá observar la totalidad de las comunicaciones que tienen lugar a través de esta, y por tanto resulta una herramienta muy potente, tanto desde el punto de vista positivo (diagnóstico de red) como el negativo (compromete la confidencialidad de las comunicaciones).

La cantidad de información obtenida de una monitorización es enorme. Por tanto, es necesario establecer unos **filtros** de aceptación, que permiten que las tramas no consideradas relevantes no se almacenen ni muestren al usuario.

A continuación, realizaremos una captura de paquetes IP y analizaremos los formatos de las tramas generadas que contengan datagramas IP.

Paso 1: Iniciamos una captura y definimos un filtro que capture todas las tramas que contengan datagramas IP que entren o salgan de nuestro computador. Evitar sobrecargar la captura con paquetes de difusión, afinar más el filtro evitando los paquetes IP de broadcast y multicast.

Una vez definido el filtro, se comienza la captura de paquetes pulsando **OK**.

Para generar algo de tráfico en tu máquina, abre un cliente web y realiza una conexión una URL cualquiera. Cuando haya finalizado la descarga de la página seleccionada, detenga la captura.

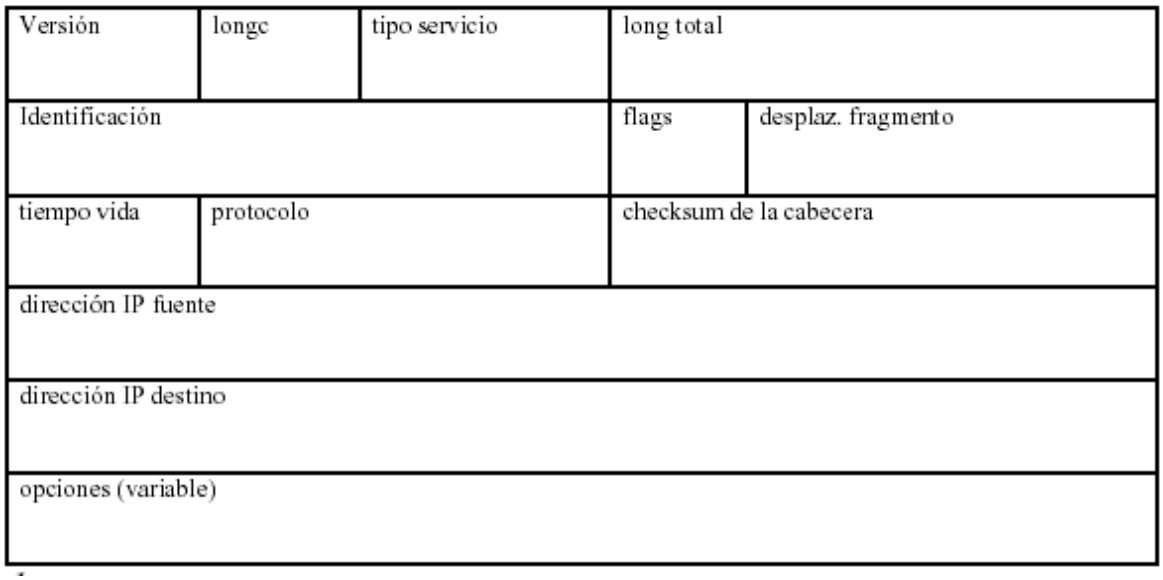
Selecciona en la parte superior de la ventana la primera trama que ha generado tu computador.

Analiza los diferentes campos de la cabecera de la trama Ethernet y de la cabecera IP. A partir de esta información rellena las siguientes tablas:

Cabecera de la trama Ethernet capturada:

Dirección física destino	Dirección física origen	tipo

Paso 2
Cabecera del paquete IP capturado:



*La orden **arp***

El computador que estamos utilizando en esta práctica está conectado a una red de área local Ethernet que, a su vez, se conecta a Internet a través de un *router*. Cuando las aplicaciones en red generan peticiones para otros computadores de Internet, crean paquetes (también llamados datagramas) que contienen la dirección IP de la máquina destino. El uso de direcciones IP (y de los protocolos TCP/IP) crea la ilusión de que todas las máquinas que se comunican pertenecen a una única red común: Internet. Si la dirección IP destino corresponde a una máquina de nuestra propia subred (ejemplo: 192.168.1.xxx), el paquete puede ser entregado directamente a su destino sin más intermediarios. Sin embargo, cuando la dirección IP corresponde a una red o subred externa, la entrega de la información debe realizarse a través del *router*. En primer lugar, habrá que entregar la información al *router* de nuestra red y éste será el encargado de encaminar el paquete para hacerlo llegar a la red destino donde se encuentra el computador referenciado. Como vemos, en cualquiera de los dos casos, en una primera instancia se realiza una transmisión de información a través de la red de área local.

Desafortunadamente, las direcciones IP no son, por sí mismas, válidas para transmitir una trama a través de la red de área local. Las tarjetas adaptadoras de red que conectan las estaciones con el medio no entienden las direcciones IP, sólo entienden direcciones físicas. Por tanto, para que un datagrama IP viaje por la red de área local, este debe encapsularse dentro de una trama (Ethernet en nuestro caso). Esa trama Ethernet contiene la dirección física del siguiente destino que, como hemos visto, puede tratarse del computador final al que van dirigidos los paquetes (origen y destino en la misma red local) o del *router* que encaminará el paquete hacia el exterior (origen y destino distintas redes o subredes).

En TCP/IP se utiliza un protocolo para la obtención de direcciones físicas a partir de direcciones IP dentro de una red de área local. Este protocolo se conoce con el nombre ARP (*Address Resolution Protocol*). En esta práctica nos limitaremos a comprobar la existencia de este protocolo a través de la orden **arp** en la shell.
Esta orden nos permite ver (y modificar) la caché ARP de nuestro computador. La caché ARP es una tabla que almacena temporalmente las relaciones entre direcciones IP y direcciones físicas, que ha conseguido averiguar nuestro computador utilizando el protocolo ARP. Es importante destacar, que la mayoría de estas entradas se generaran automáticamente (y de forma transparente al usuario) cuando se ejecuta una aplicación Internet (ping, cliente web, cliente ftp, etc.). Por tanto, muy rara vez requiere el usuario modificar manualmente esta tabla.
Más concretamente, la orden **arp** permite:

Ver la caché local de ARP (**arp –a**)
Eliminar entradas manualmente de la caché (**arp –d dirección_IP o arp –d ***)
Añadir entradas manualmente a la caché (**arp –s dirección_IP dirección_Física**)

Ejercicio 2:

Paso 1: Desde una ventana de la shell ejecuta la orden **arp –a** para comprobar que la caché ARP está vacía. Si no lo está, cierra todas las aplicaciones que hagan uso de la red y elimina las entradas del a caché ARP usando la orden **arp –d ***, o simplemente esperando un par de minutos (sin ejecutar nuevas aplicaciones en red) y las entradas desaparecerán de la caché. A continuación, ejecuta un ping a otra y examina de nuevo la caché ARP. Anota la información obtenida en la tabla siguiente:

Dirección IP	Dirección Física

Dirección IP Dirección Física
Paso 2: Elimina manualmente las entradas de la caché ARP (o espera un par de minutos) y realiza una conexión a la siguiente URL:http://www.uv.cl

Dirección IP	Dirección Física

Paso 3: Monitoriza la cantidad de paquetes ARP que recibe tu PC.

Instante de tiempo	Paquetes/segundo

¿A qué máquina corresponde la dirección almacenada en la caché? ¿Cree UD. que esta dirección corresponde a la máquina www.uv.cl? ¿Por qué?

Tablas para entregar:

Ejercicio 1:

Dirección física destino	Dirección física origen	tipo

Versión	longc	tipo servicio	long total	
Identificación			flags	desplaz. fragmento
tiempo vida	protocolo		checksum de la cabecera	
dirección IP fuente				
dirección IP destino				
opciones (variable)				

Ejercicio 2:
Paso 1:

Dirección IP	Dirección Física

Paso 2

Dirección IP	Dirección Física

Paso 3:

Instante de tiempo	Paquetes/segundo

Que técnicas de seguridad existen para proteger una red de los “sniffer”, menciónelas e indique cual sería la más adecuada en este caso.

Realice una conexión ssh y extraiga los mensajes asociados a la conexión, explíquela desde la lógica de una conexión TCP/IP y verifique si existe alguna vulnerabilidad asociada a la confidencialidad de la información. Haga lo mismo con una conexión FTP. Lo anterior ejecútelo contra el servidor 10.100.6.58.