Instituto Politécnico Nacional

Unidad Profesional Interdisciplinaria de Ingeniería y Tecnologías Avanzadas

Práctica 1: Implementación de un Sniffer.

Alumno:
Rojas Gómez Ian

Grupo: 2TM8
Profesor: Enriquez Ortiz Cyntia Eugenia
Unidad de Aprendizaje: Protocolos de Internet.
Fecha de Entrega: Martes 22 de Febrero del 2022.

Introducción

La evolución de Internet ha traído grandes avances a la tecnología así como una comunicación rápida y eficiente, pero para que todo esto sea posible, se tuvieron que crear estándares y reglas para que la comunicación entre las computadoras fuera lo mas claro y rápido posible, a pesar de que solo requerimos un cable para poder estar conectados a lared, va mas allá de eso, que detrás de tanta simpleza se tenga un mundo fascinante. Si bien los datos que transmitimos se tienen que enviar en tramas o paquetes de datos, a continuación se van a explicar los paquetes mas utilizados en el mundo de la informática.

Ethernet

En una red Ethernet los dispositivos se intercambian paquetes de datos entre sí, los llamados paquetes Ethernet. En su contenido se incluye la trama Ethernet (a menudo denominada también trama de datos), que a su vez se divide en varios conjuntos de datos. Estos registros consisten en código binario que proporciona información importante, incluyendo direcciones, información de control, datos de uso y sumas de comprobación. Dependiendo del estandar, este puede variar en su estructura, y puede contener mas o menos campos de datos dependiendo del protocolo de Red.

Ethernet II

Una trama Ethernet debe tener al menos 64 bytes para que funcione la detección de colisiones y pueda tener un máximo de 1518 byte. Se define de la siguiente manera:

1. Se comienza con un preámbulo, que controla la sincronización entre el emisor y el receptor y un Start Frame Delimiter (SFD), que define la trama.

2. Se contienen las direcciones de origen y destino en formato MAC.

3. SE contiene la información de control (En el caso de Ethernet OO el campo de tipo, una especificación de longitud)-

4. Seguida por un registro de datos que se envía.

5. Una secuencia de comprobación de trama (FCS) que es un código de errores que cierra la trama.

Ethernet II utiliza la estructura de trama clásica con un campo de tipo (Type) que define varios protocolos en la capa de red. La trama Ethernet II se definió en 1982 y ha constituido la base de todos los desarrollos posteriores de tramas. Sin embargo, el formato sigue gozando de gran popularidad, sobre todo porque ofrece al campo de datos una gran cantidad de espacio (hasta 1 500 bytes).

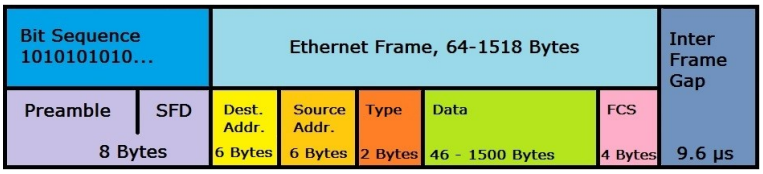


Figure 1: Trama Ethernet II.

IEEE 802.3

Esta versión estandarizada de la trama Ethernet 802.3 puede definir hasta 256 protodolos compatibles . Además, se incluyen "Punto de acceso al servicio de destino" (DSAP) y "Punto de acceso al servicio de origen" (SSAP) y el nuevo campo de control define el "Logical Link" (LLC) del protocolo.
Ethernet IEEE 802.3 es la estrucutra de trama LAN más popular y ampliamente utilizada en la actualidad. [1]

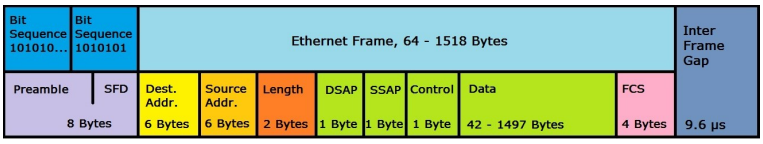


Figure 2: Trama de Ethernet IEEE 802.3.

0.0.1 Tecnologías de transmisión

Las tecnologías de tranmisión son parte fundamental debido a que las tramas deben tenerlas para saber que tipo de protocolo seguir y procesar. Existen 3 tipos de tecnologías básicas para las tramas Ethernet:

- **Broadcast(Difusión)**: Es la transferencia de información desde un nodo emisor a una multitud de nodos receptores. [2]
- **Unicast (Unidifusión)**: Es la tranferencia que se realiza desde un único emisor a un único receptor, sin importar si tiene lugar en ambas direcciones. [3]
- **Multicast (Multidifusión)**: Se refiere a la entrega de la información a multiples destinos. [4]

Modo promiscuo

Después de fundamentarnos acerca de lo que vamos a estar analizando en nuestro sniffer, hay que tener en cuenta una configuración de nuestra NIC que sería el **Modo Promiscuo**.
El **Modo Promiscuo** es una configuración de NIC que pasa todos los paquetes al conttrolador del adaptador de red y a la plia de protocolos. Es compatible con muchos adaptadores de red cablados e inalámbricos y sus controladores. Esto va a permitir que nuestra máquina este a la escucha de todos los paquetes que esten pasando por la red, aunque dichos paquetes no sean para nosotros. [5]

Sniffer

Un Sniffer es una aplicación especial para redes informáticas (un software) que se encarga de capturar y analizar paquetes en tránsito (entrada y/o salida) en una red de comunicaciones entre dispositivos.
Sniffer, del inglés sniff: olfatear, rastrear, puede entenderse como un programa con la capacidad de observar el flujo de datos en tránsito por una red, y obtener información de éste; está diseñado para analizar los paquetes de datos que pasan por la red y no están destinados para él, lo que bajo ciertas circunstancias es muy útil, y bajo otras, a la vez, muy peligroso. [6]

Documentación

A continuación se van a mostrar unos diagramas realizados en UML donde se puede apreciar como se desarrollo el programa. Si bien no estan enfocados al 100% al modelado UML sirvieron para el entendimiento del desarrollo.

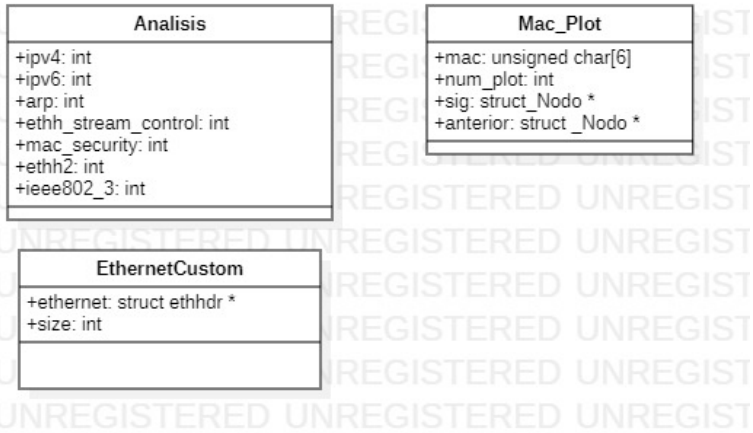
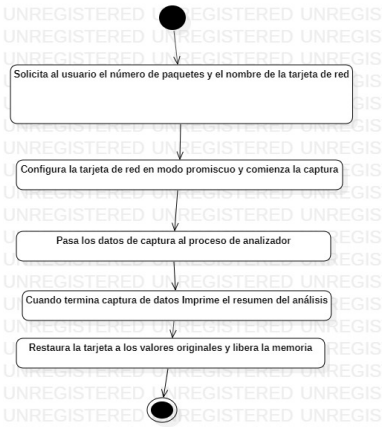
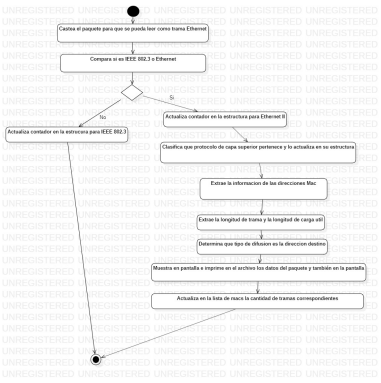


Figure 3: Estructuras utilizadas para almacenar datos y facilitar el desarrollo.



(a) Diagrama del proceso capturador.



(b) Diagrama del proceso analizador.

Figure 4: Diagramas de estado de los dos procesos que van a estar definiendo la funcionalidad del sniffer.

Resultados

A continuación se van a mostrar los datos obtenidos de un análisis de 20 paquetes.

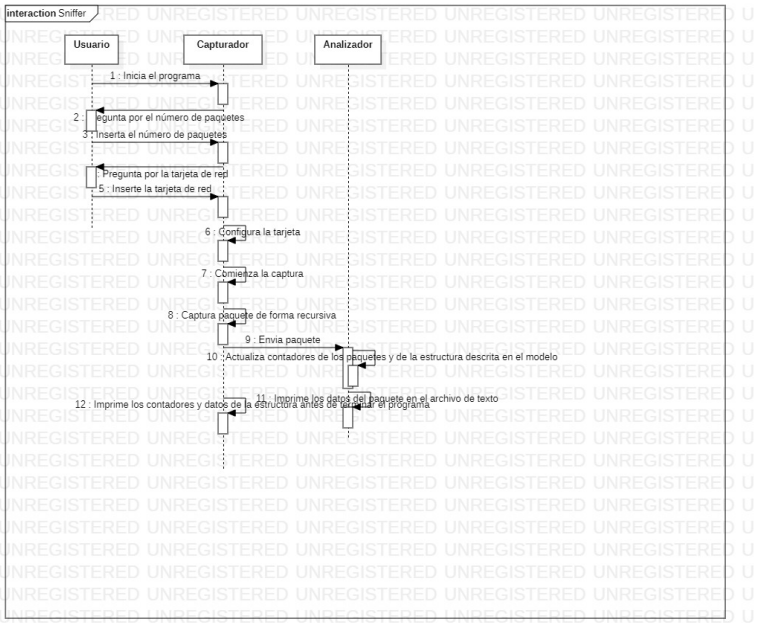


Figure 5: Diagrama de secuencia de convivencia entre el usuario, el proceso capturador y el proceso analizador.

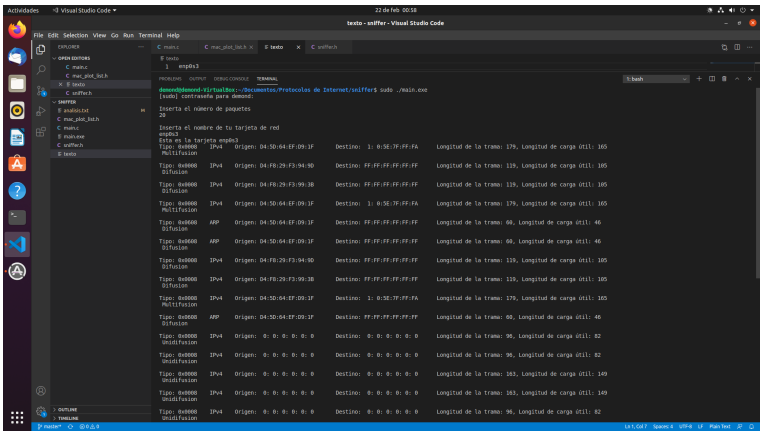


Figure 6: Análisis de 20 paquetes.

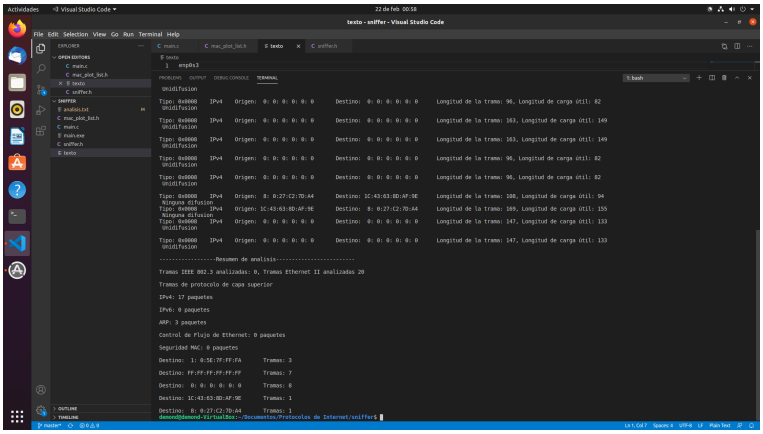


Figure 7: Resumen de análisis de 20 paquetes.

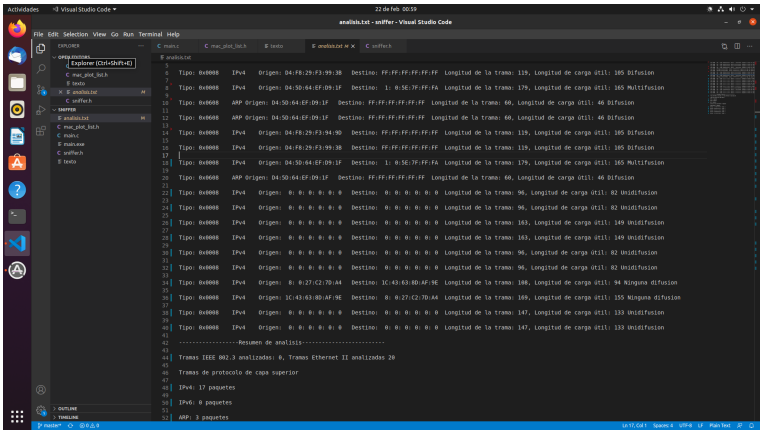


Figure 8: Generación de archivo.

Bibliography

[1] know how, "Trama ehernet: definición, estructura y variantes." last accessed 22 february 2022. [Online]. Available: https://www.ionos.mx/digitalguide/servidores/know-how/trama-ethernet/

[2] admin, "Qué es broadcast." last accessed 22 february 2022. [Online]. Available: http://huribroadcast.com/que-es-broadcast/

[3] K. How, "Unicast: conexión dirigida entre dos puntos." last accessed 22 february 2022. [Online]. Available: https://www.ionos.mx/digitalguide/servidores/know-how/unicast/#:~:text=Una%20unicast%2C%20tambi%C3%A9n%20denominada%20difusi%C3%B3n,tiene%20lugar%20en%20ambas%20direcciones.

[4] H. H. G. Hernández Palacios Raul, "Comunicaciones multicast," last accessed 22 february 2022. [Online]. Available: https://www.uaeh.edu.mx/scige/boletin/huejutla/n9/r1.html#:~:text=Multicast%20se%20refiere%20a%20la,%C3%BAnico%20nodo%20receptor%20de%20destino.

[5] netinbag, "¿qué es el modo promiscuo?" last accessed 22 february 2022. [Online]. Available: https://www.netinbag.com/es/internet/what-is-promiscuous-mode.html

[6] infotecs, "¿qué es un sniffer?" last accessed 22 february 2022. [Online]. Available: https://infotecs.mx/blog/que-es-un-sniffer.html#:~:text=Un%20Sniffer%20es%20una%20aplicaci%C3%B3n,red%20de%20comunicaciones%20entre%20dispositivos.