

Taller 1 - Redes de comunicaciones I

Juan Esteban Oviedo Sandoval - 20192020064

jeoviedos@udistrital.edu.co

I. INTRODUCCIÓN

II. OBJETIVOS

- 1) Analizar en profundidad el funcionamiento de IEEE 802.3, IEEE 802.11, IPv4 e ICMP.
- 2) Experimentar con la aplicación ping como herramienta de diagnóstico y análisis de red.
- 3) Evaluar la influencia de velocidades de transmisión, anchos de banda, latencia y QoS en el rendimiento de redes.
- 4) Explorar vulnerabilidades y soluciones de seguridad informática en estos protocolos.
- 5) Integrar y aplicar herramientas de IA para interpretar capturas de tráfico, calcular métricas y generar explicaciones avanzadas de seguridad informática, calidad de servicio y desempeño de redes de comunicaciones IEEE 802.3, IEEE 802.11 e Internet.

III. LABORATORIO PRÁCTICO CON PING, WIRESHARK

A. Configuración LAN (WLAN)

Se configura la red LAN con IPv4 privadas.

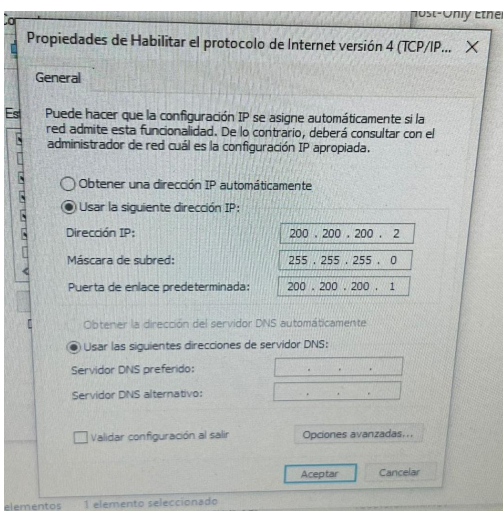


Fig. 1. IPv4 privada, maquina 1

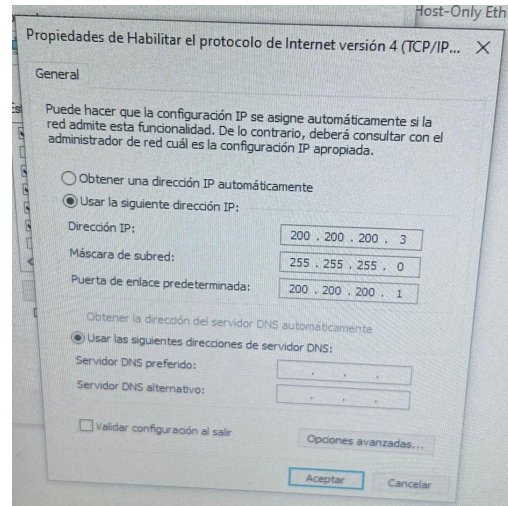


Fig. 2. IPv4 privada, maquina 2

B. Ping

Se ejecuta pruebas de ping entre ambas bajo IEEE 802.3 (cable) y IEEE 802.11 (WiFi). Los pings se ejecutan de diferentes tamaños (Ej: ping -t x.x.x.x -l 60000).

1) **Wifi - Lan:** Se hicieron prebas de ping Wifi - Lan con diferentes paquetes:

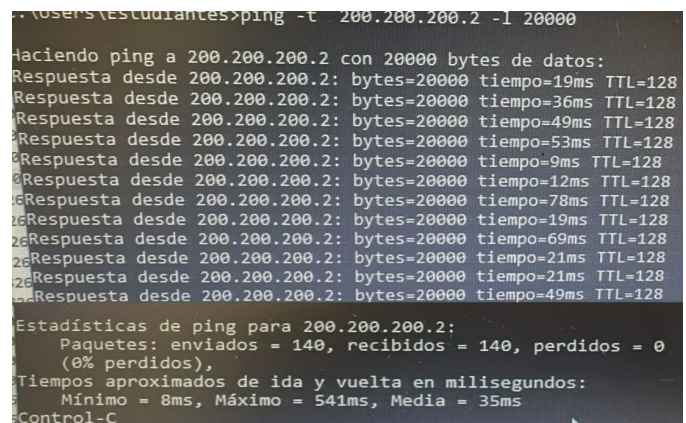


Fig. 3. Ping Wifi - Lan, 20000

O(Mbps)	P	V(Mbps)	T(Mbps)
4.0 - 6.0	802.11	11 (802.11b)	5-7
4.0 - 6.0	802.11	54 (802.11g) si señal mala	20-25 **
32.0 - 40.0	802.3	100 (Fast Ethernet)	70-95 *
32.0 - 40.0	802.3	1000 (si negocia 1G)	940 *

TABLE II
DIFERENCIA, VELOCIDAD PRÁCTICA Y TEÓRICA

- O: Observable
- P: Protocolo
- V: Velocidad teórica probable (PHY)
- T: Throughput practico típico
- **: Si buena
- *: Ideal

C. Wireshark

Se captura el tráfico con Wireshark

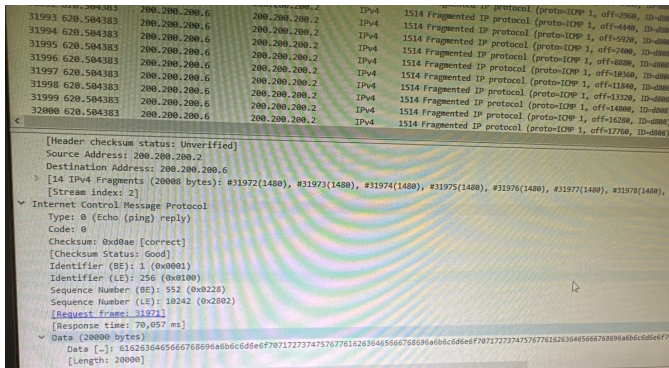


Fig. 9. Wireshark Wifi - Lan, 20000

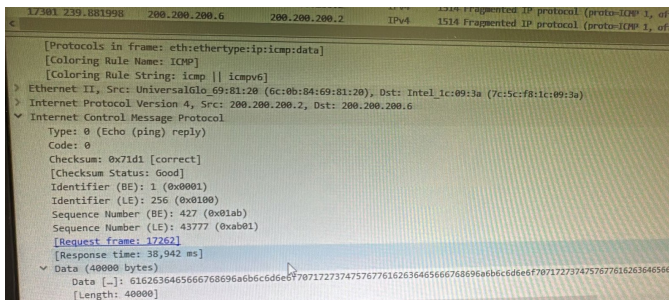


Fig. 10. Wireshark Wifi - Lan, 40000

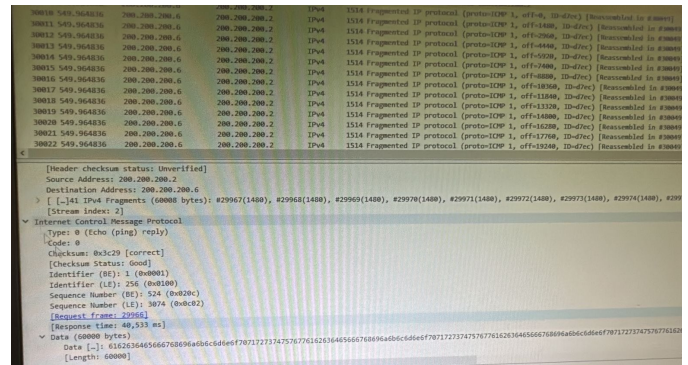


Fig. 11. Wireshark Wifi - Lan, 60000

D. Montaje

E. Aplicación IA

Se exportar la captura. pcap y usar una herramienta de IA que explique los patrones de tráfico, anomalías y latencias.

IV. SEGURIDAD INFORMÁTICA

A. Ataque Flood

Implementa y configura ataques basados en ICMP (Ping Flood, Smurf Attack).

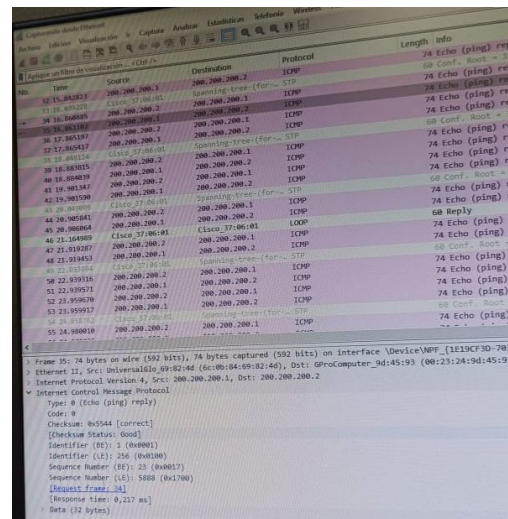


Fig. 12. Captura Wireshark, previo ataque.

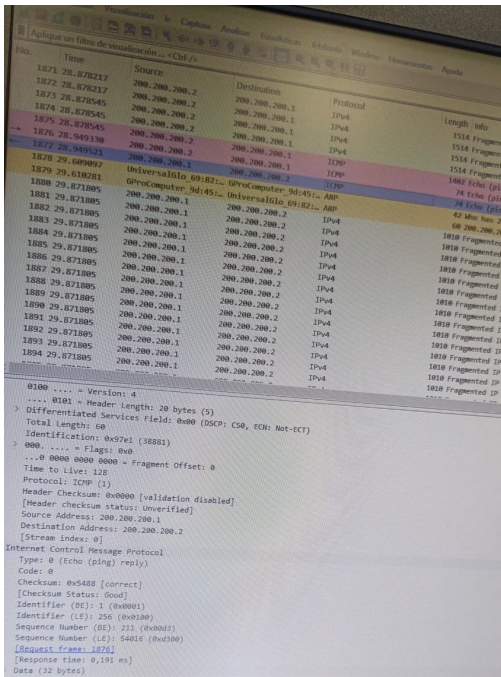


Fig. 13. Ataque flood.

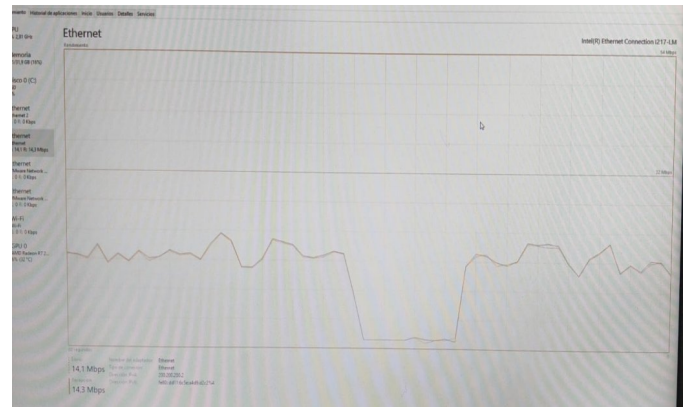


Fig. 16. Red en el ataque.

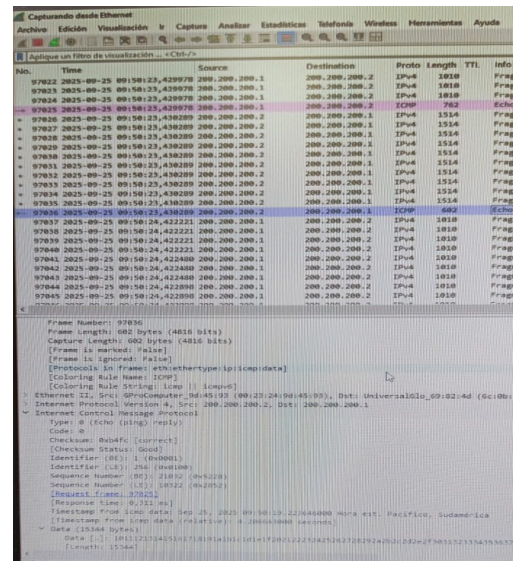


Fig. 17. Captura Wireshark, ataque.

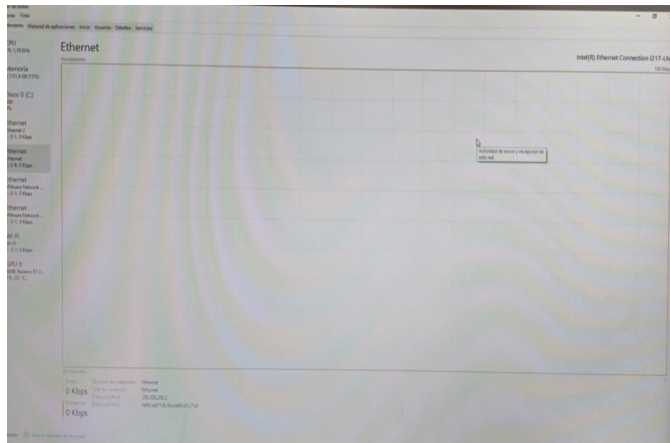


Fig. 14. Red previo al ataque.

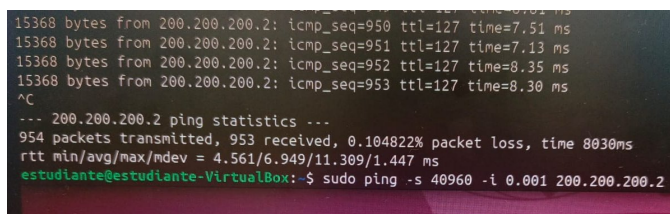


Fig. 15. Ataque desde Linux

B. Firewall

Diseña una regla de firewall que permita ping en LAN (IEEE 802.3) pero lo bloquee desde Internet.

C. Aplicación IA

Se pidió a la IA generar un script de reglas de firewall en Linux/Windows y luego revisarlo para detectar los ataques mencionados ((Ping Flood, Smurf Attack).

V. CÁLCULOS DE QOS Y ANCHO DE BANDA

VI. PROYECTO INTEGRADOR CON IA