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.

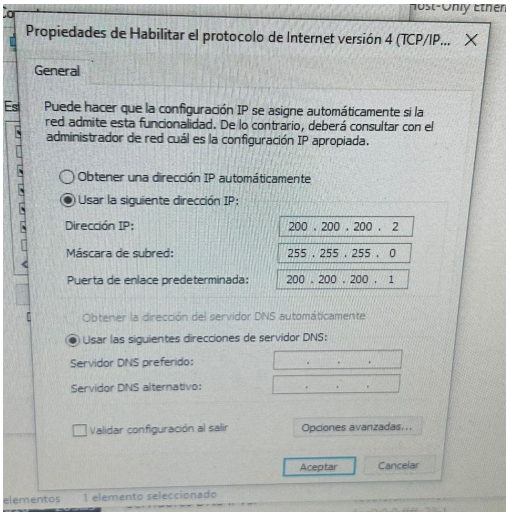

Fig. 1. IPv4 privada, maquina 1

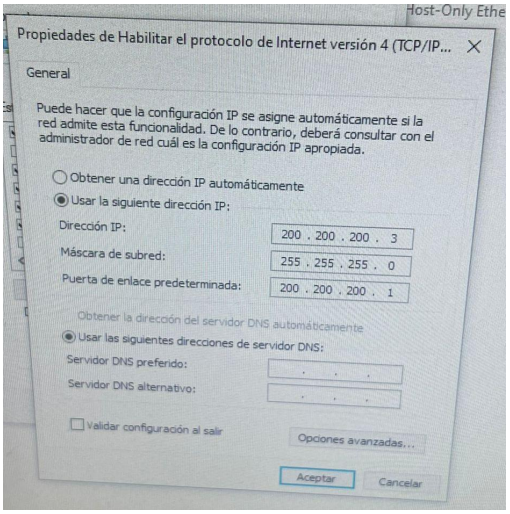

Fig. 2. IPv4 privada, maquina 2

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:

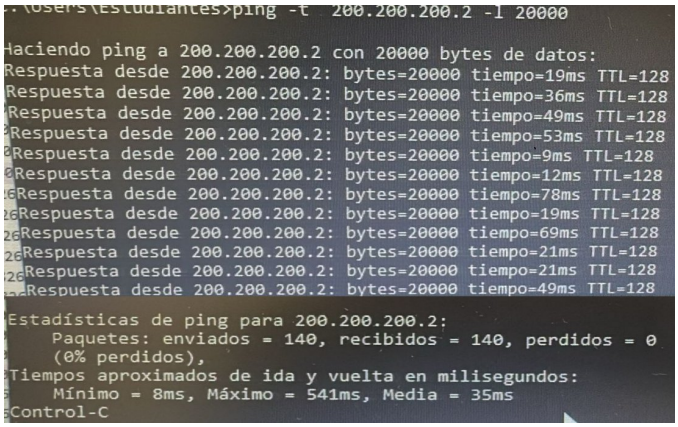

Fig. 3. Ping Wifi - Lan, 20000

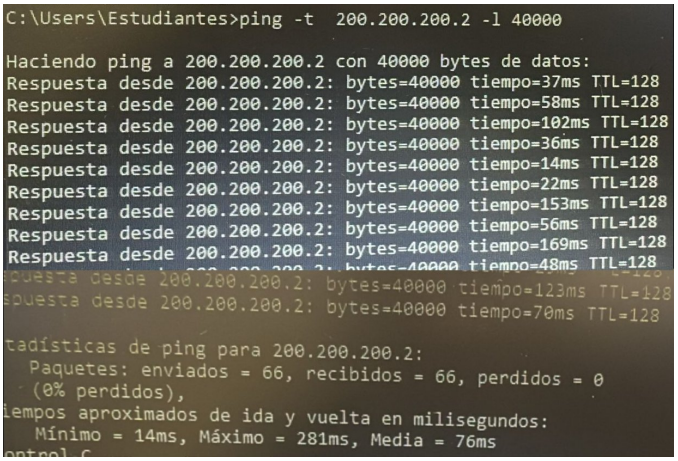

Fig. 4. Ping Wifi - Lan, 40000

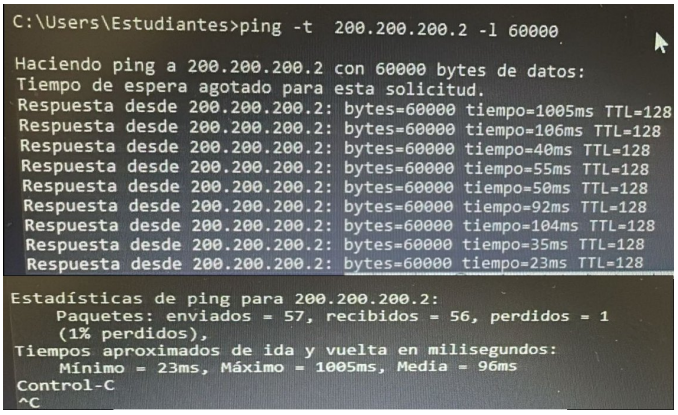

Fig. 5. Ping Wifi - Lan, 60000

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

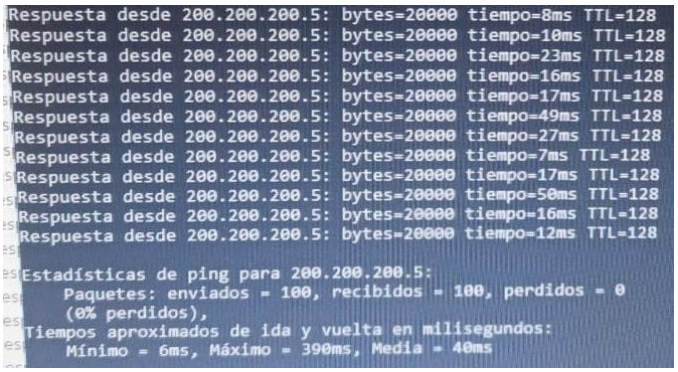

Fig. 6. Ping Lan - Wifi, 20000

3) Wifi - Wifi: Se hicieron prebas de ping Wifi - Wifi con diferentes paquetes:

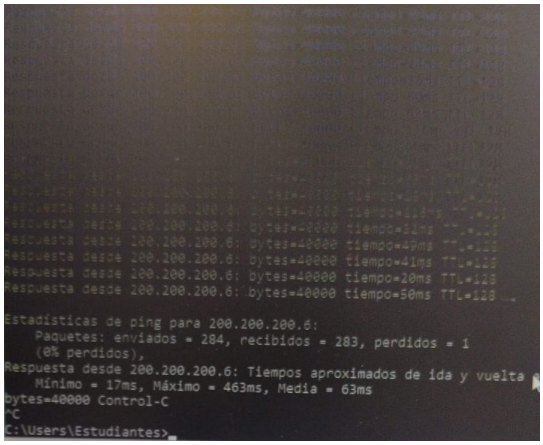

Fig. 7. Ping Wifi - Wifi, 40000

Fig. 8. Ping Wifi - Wifi, 60000

Tamano($bytes$)	$t(ms)$	Destino	P	$V(Mbps)$
60000	80	200.200.200.6	802.11	6
40000	57	200.200.200.5	802.11	5.61
30000	48	200.200.200.6	802.11	5
20000	40	200.200.200.5	802.11	4
60000	12	200.200.200.3	802.3	40
40000	8	200.200.200.2	802.3	40
30000	6	200.200.200.3	802.3	10
20000	5	200.200.200.2	802.3	32

TABLE I
TABLA DE VELOCIDADES

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

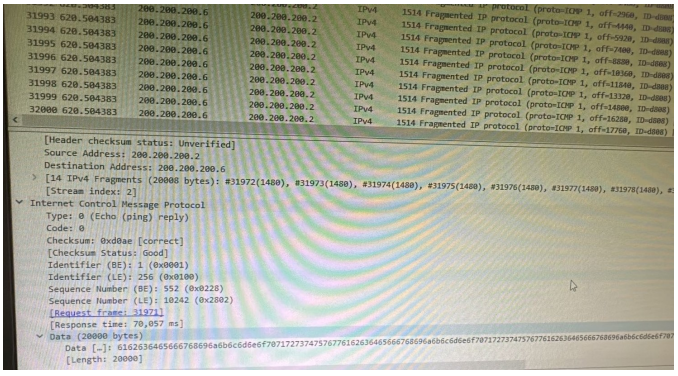

Fig. 9. Wireshark Wifi - Lan, 20000

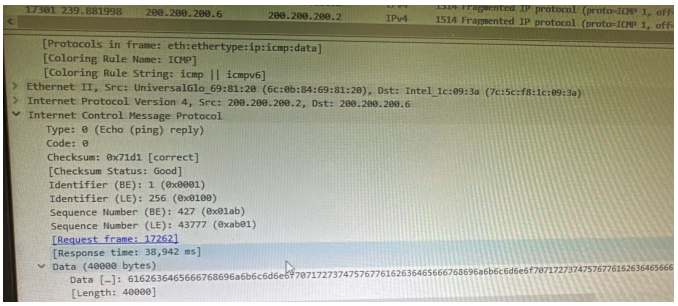

Fig. 10. Wireshark Wifi - Lan, 40000

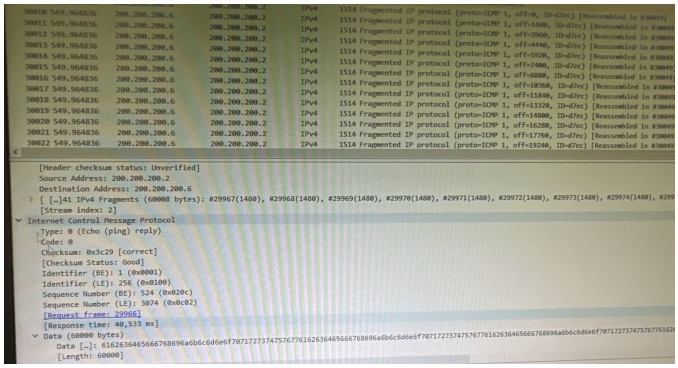

Fig. 11. Wireshark Wifi - Lan, 60000

D. Montaje

E. Aplicación IA

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

IV. SEGURIDAD INFORMÁTICA

A. Ataque Flood

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

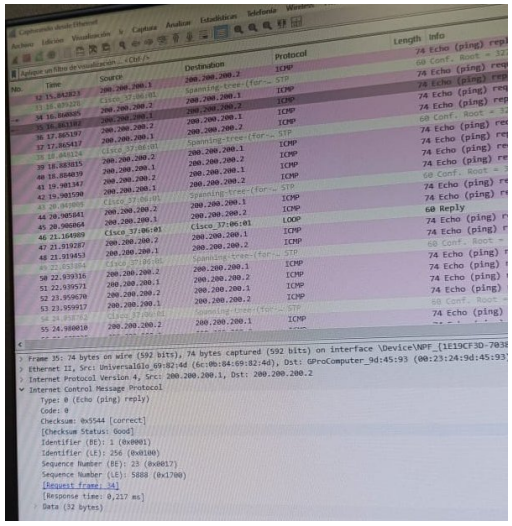

Fig. 12. Captura Wireshark, previo ataque.

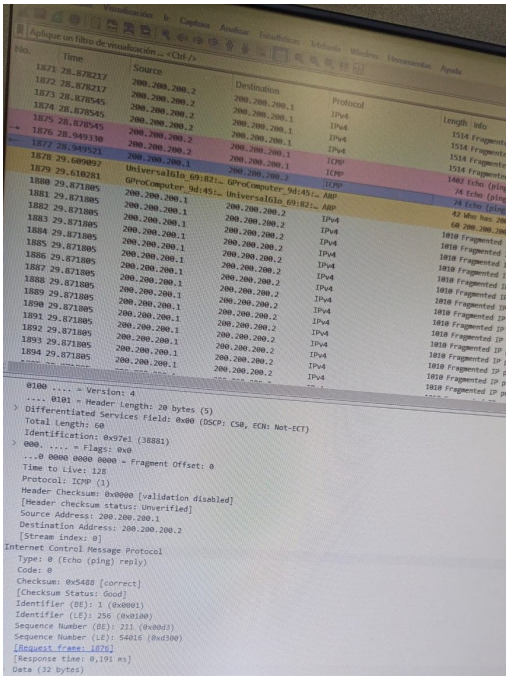

Fig. 13. Ataque flood.

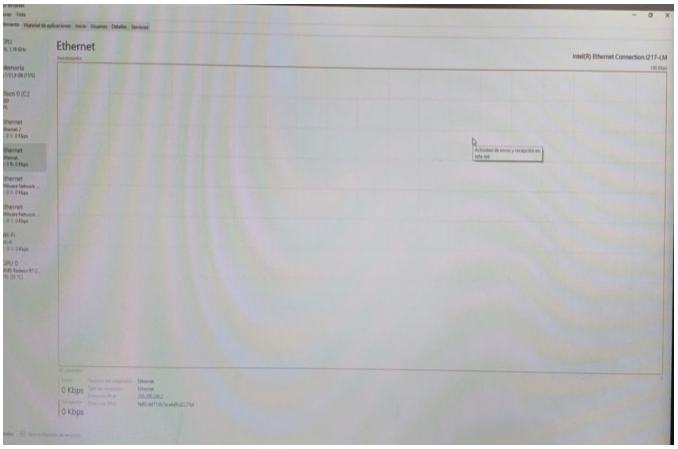

Fig. 14. Red previo al ataque.

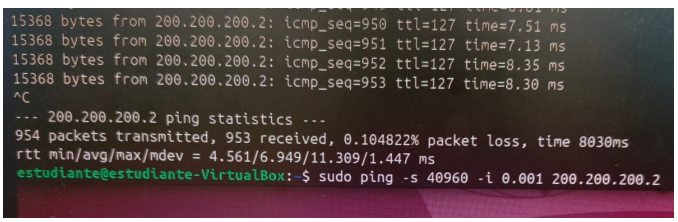

Fig. 15. Ataque desde Linux

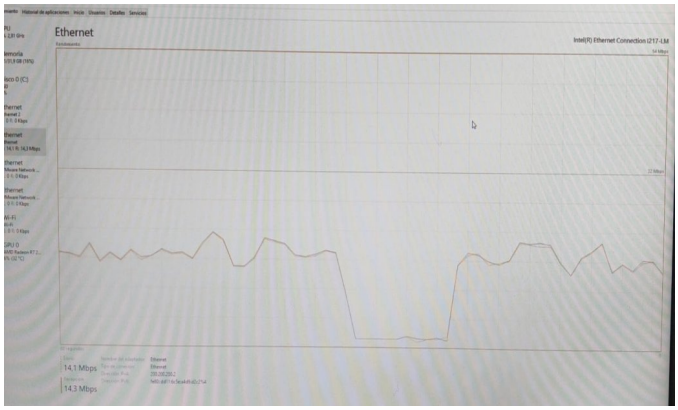

Fig. 16. Red en el ataque.

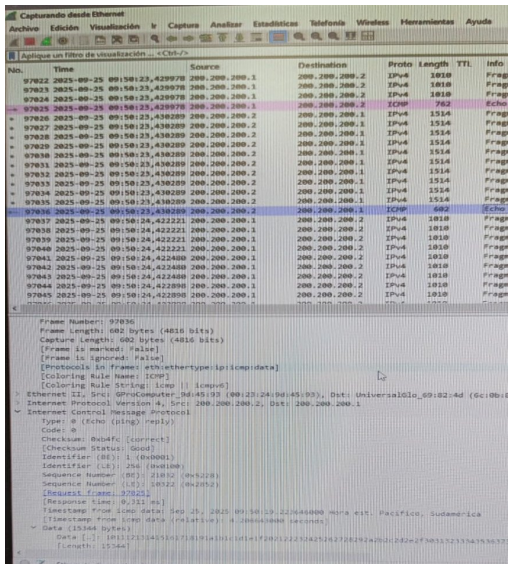

Fig. 17. Captura Wireshark, ataque.

B. Firewall

Diseñe 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**

Una universidad planea implementar una red híbrida:

- Ethernet (IEEE 802.3) para laboratorios de alta capacidad.
- WiFi (IEEE 802.11) para áreas comunes.

Requisitos

1) 5000 usuarios simultáneos.
2) Soporte a videoconferencia con ¡100 ms de latencia.
3) Protección contra ataques ICMP.
4) Priorización de tráfico académico sobre recreativo.

A. *Plan de direccionamiento*

Se propone un plan de direccionamiento IPv4 privado con subredes, usando la red privada 10.0.0.0/8 para tener un amplio rango de direcciones.

Subredes propuestas:

- Red administrativa y servidores: 10.0.1.0/24
- Laboratorios (Ethernet): 10.0.2.0/23 a 10.0.10.0/23 (varias subredes según laboratorios)
- WiFi áreas comunes: 10.0.20.0/22 (para hasta 1000 usuarios por segmento)
- WiFi invitados: 10.0.30.0/24
- Dispositivos IoT y control: 10.0.40.0/24
- Infraestructura de red (routers, switches, AP): 10.0.254.0/24

Con este esquema se soportan más de 5000 usuarios, con espacio para expansión.

B. *Políticas de seguridad informática*

Diseñar políticas de seguridad informática (firewall, segmentación de redes IP, IDS/IPS).

*1) **Arquitectura de Seguridad General**:* Defensa en Profundidad:

- **Capa 1:** Firewall perimetral
- **Capa 2:** Segmentación con VLANs
- **Capa 3:** IDS/IPS interno
- **Capa 4:** Seguridad en endpoints

*2) **Configuración Detallada de Firewall**:*

Bloqueo ICMP específico:

```
# Ping flood
deny icmp any any echo-request
# Respuestas no solicitadas
deny icmp any any echo-reply
# ICMP interno permitido
allow icmp 10.0.0.0/16 any
```

Acceso administrativo:

```
# SSH solo desde red admin
allow tcp 10.0.0.0/24 any eq 22
# HTTPS admin
allow tcp 10.0.0.0/24 any eq 443
```

Servicios públicos:

```
# Web HTTP/HTTPS
allow tcp any any eq 80,443
# DNS
allow udp any any eq 53
# NTP
allow udp any any eq 123
```

Videoconferencia:

```
# RTP/RTSP
allow tcp any any range 5000-6000
# Puertos multimedia
allow udp any any range 10000-20000
```

Bloqueo general:

```
# Denegar todo lo no permitido
deny ip any any
```

*3) **Reglas de Salida (Outbound)**:*

Tráfico académico prioritario:

```
allow tcp 10.0.0.0/16 any
eq 80,443,22,23,25,110,143
allow udp 10.0.0.0/16 any
eq 53,123,161,162
```

Restricciones WiFi invitados:

```
allow tcp 10.0.32.0/21 any eq 80,443,53
deny tcp 10.0.32.0/21 10.0.0.0/16
# No acceso a red interna
```

C. *Mecanismos de calidad de Servicio*

Implementar mecanismos de calidad de Servicio, Quality Of servive , QoS. (ej. DSCP, colas de prioridad) en el prototipo (escenario de redes IEEE 802.3 e IEEE 802.11).

D. *Esquema visual de la red*

Aplicación IA: solicitar a una herramienta de IA la generación de un esquema visual de la red y presente algunas características de gestión de red (velocidades de Tx, desempeños, errores, ataques, logs... entre otros).