Ngày: 26/02/2025

Họ và tên SV: Ngô Ngọc Bảo Trân

Lớp: 10_ĐH_CNPM1

MSSV: 1050080079

LAB 01: Wireshark Getting Started

Task 1: Mở đầu về Mạng máy tính

Câu 1: Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng (kèm ảnh minh họa)

1. Router (Bộ định tuyến)

Chức năng:

Định tuyến dữ liệu giữa các mạng khác nhau, giúp kết nối giữa mạng nội bộ (LAN) và Internet.

Cung cấp địa chỉ IP cho các thiết bị trong mạng thông qua DHCP.

Hỗ trợ bảo mật với Firewall, NAT (Network Address Translation).

Một số router có chức năng Wi-Fi để phát tín hiệu không dây.

Ví dụ thực tế:

Router Wi-Fi tại nhà của các hãng như TP-Link, Asus, Tenda, Netgear.

Router chuyên dụng của doanh nghiệp như Cisco, MikroTik.

Hình ảnh minh họa:

2. Switch (Bộ chuyển mạch mạng)

Chức năng:

Kết nối nhiều thiết bị trong cùng một mạng LAN (Local Area Network).

Chuyển tiếp dữ liệu thông minh giữa các thiết bị, giảm tắc nghẽn mạng.

Một số Switch có khả năng quản lý VLAN để chia nhỏ mạng nội bộ.

Ví dụ thực tế:

Các Switch thông dụng của Cisco, TP-Link, D-Link, Aruba.

Dùng trong văn phòng, trung tâm dữ liệu để kết nối nhiều máy tính, máy in, máy chủ.

Hình ảnh minh họa:

3. Modem (Bộ điều chế – giải điều chế)

Chức năng:

Chuyển đổi tín hiệu số từ mạng thành tín hiệu analog (và ngược lại) để truyền qua đường dây viễn thông.

Kết nối Internet từ nhà cung cấp dịch vụ (ISP) đến người dùng.

Một số modem tích hợp cả chức năng router để phát Wi-Fi.

Ví dụ thực tế:

Modem quang của VNPT, Viettel, FPT.

Modem cáp quang GPON, Modem DSL (ADSL/VDSL).

Hình ảnh minh họa:

4. Access Point (AP) - Điểm truy cập không dây

Chức năng:

Kết nối mạng có dây (Ethernet) và phát tín hiệu Wi-Fi cho các thiết bị không dây.

Mở rộng vùng phủ sóng Wi-Fi trong không gian lớn.

Một số Access Point hỗ trợ công nghệ Mesh để phủ sóng toàn bộ tòa nhà.

Ví dụ thực tế:

AP của UniFi, Aruba, Cisco Aironet, TP-Link.

Dùng trong văn phòng, quán café, trung tâm thương mại để mở rộng mạng Wi-Fi.

Hình ảnh minh họa:

5. Network Interface Card (NIC) - Card mạng

Chức năng:

Cho phép máy tính, laptop kết nối với mạng có dây hoặc không dây.

Gồm hai loại chính:

NIC có dây (Ethernet Card): Cắm vào cổng LAN, dùng cáp RJ45 để kết nối.

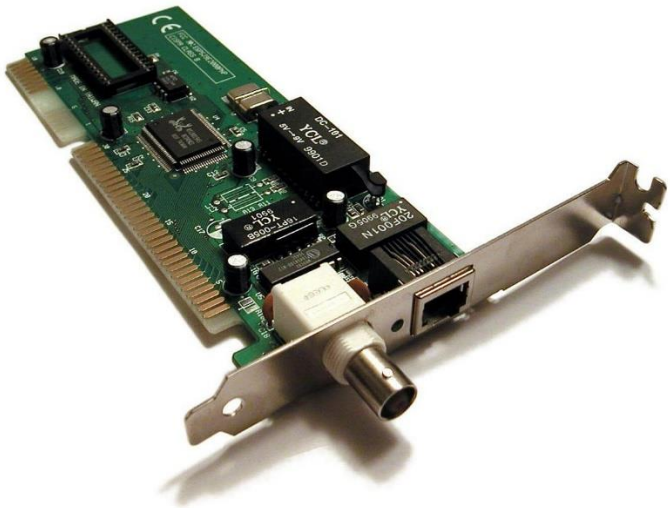
NIC không dây (Wi-Fi Adapter): Kết nối Wi-Fi với Access Point.

Ví dụ thực tế:

Card mạng Intel, Realtek, TP-Link, Asus.

Máy tính để bàn thường dùng NIC có dây, laptop có sẵn NIC Wi-Fi.

Hình ảnh minh họa:



6. Firewall (Tường lửa)

Chức năng:

Lọc và kiểm soát lưu lượng mạng để bảo vệ hệ thống khỏi tấn công.

Chặn truy cập trái phép, bảo vệ dữ liệu nhạy cảm.

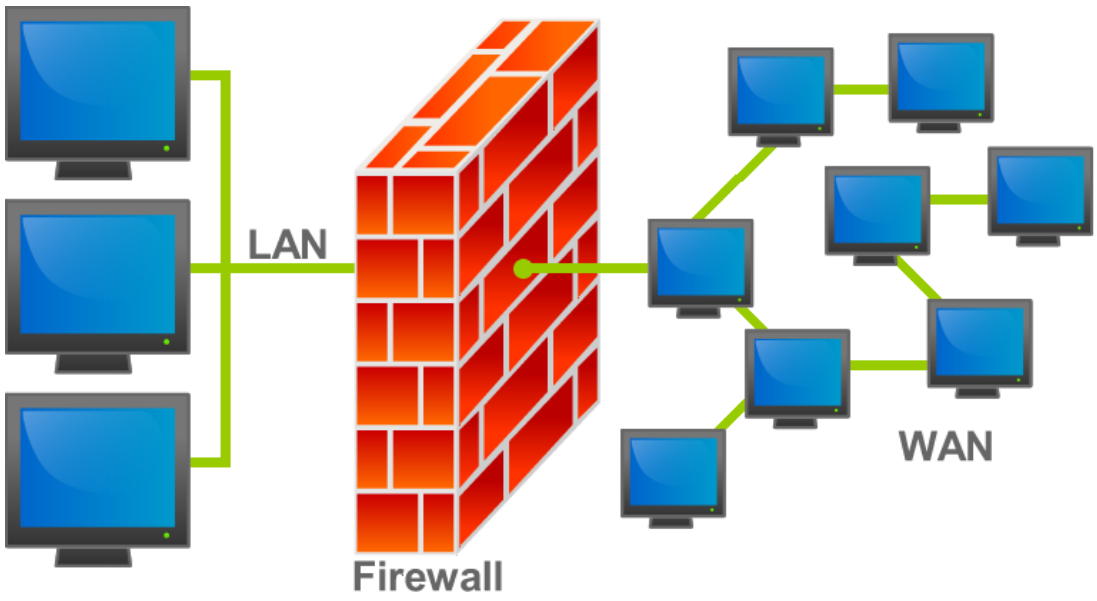
Một số Firewall có tính năng IDS/IPS để phát hiện và ngăn chặn tấn công.

Ví dụ thực tế:

Firewall phần cứng: Cisco ASA, FortiGate, Palo Alto Networks.

Firewall phần mềm: Windows Defender Firewall, pfSense, Sophos XG.

Hình ảnh minh họa:



Câu 2: Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?

1. Ảnh hưởng đến công việc và học tập

Không thể truy cập tài liệu trực tuyến:

- Google Drive, Dropbox, OneDrive không thể tải hoặc lưu tài liệu.
- File Excel/Word dùng chung bị gián đoạn, không thể cập nhật dữ liệu.

Gián đoạn cuộc họp/học online:

- Zoom, Microsoft Teams, Google Meet bị mất kết nối.
- Nếu đang thuyết trình hoặc học bài, bạn có thể bị văng khỏi lớp học/cuộc họp.

Không thể gửi/nhận email:

- Gmail, Outlook không thể gửi hoặc nhận email mới.
- Email quan trọng có thể bị trễ, ảnh hưởng đến công việc.

2. Gián đoạn liên lạc cá nhân và mạng xã hội

Không thể nhắn tin, gọi điện qua Internet:

- Các ứng dụng như Messenger, Zalo, WhatsApp, Telegram không thể gửi tin nhắn.
- Cuộc gọi video/thoại VoIP bị ngắt giữa chừng.

Mất kết nối với mạng xã hội:

- Facebook, Instagram, Twitter không thể tải nội dung mới.
- Bài viết hoặc bình luận có thể bị lỗi tải lên.

3. Gián đoạn giải trí và hoạt động cá nhân

Không thể xem video trực tuyến:

- YouTube, Netflix, TikTok bị đứng hình, không thể tiếp tục xem.
- Video đang xem có thể bị gián đoạn, gây khó chịu.

Game online bị mất kết nối:

- Các trò chơi như Liên Minh Huyền Thoại, PUBG, Valorant có thể bị "văng" khỏi trận đấu.
- Dữ liệu trận đấu có thể không được lưu, mất tiến trình chơi.

4. Không thể truy cập thông tin quan trọng

Không thể tra cứu tin tức, thời tiết, tài liệu học tập:

- Google, Wikipedia không thể tải trang.
- Không thể xem dự báo thời tiết, ảnh hưởng đến kế hoạch đi lại.

Mất quyền truy cập vào hệ thống ngân hàng trực tuyến:

- Không thể kiểm tra số dư tài khoản.
- Không thể thực hiện giao dịch chuyển tiền.

5. Ảnh hưởng đến các thiết bị IoT và hệ thống nhà thông minh

Camera an ninh bị gián đoạn:

- Camera giám sát không thể truyền hình ảnh về điện thoại.
- Nếu có sự cố xảy ra, bạn không thể kiểm tra camera từ xa.

Các thiết bị thông minh mất điều khiển:

- Nhà thông minh (Smart Home) như khóa cửa, đèn, điều hòa, rèm tự động không thể điều khiển qua app.
- Robot hút bụi, loa thông minh (Google Home, Alexa) không hoạt động.

6. Ảnh hưởng đến doanh nghiệp và hệ thống dịch vụ

Website doanh nghiệp có thể bị gián đoạn:

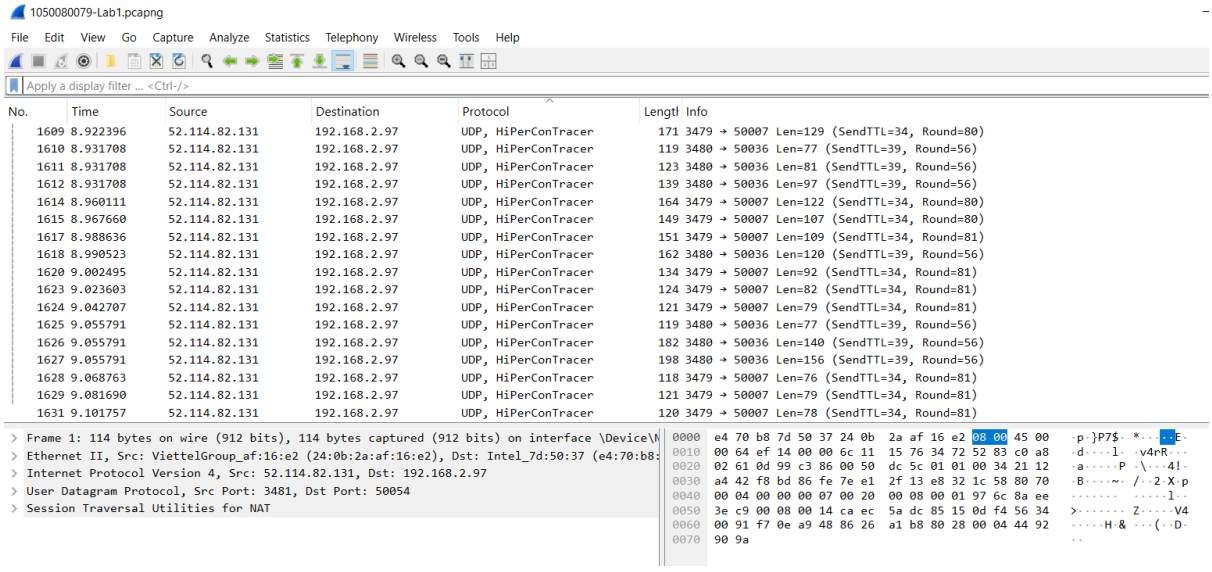
- Nếu máy chủ web của công ty dựa vào kết nối Internet, khách hàng có thể không truy cập được.
- Ảnh hưởng đến doanh thu nếu đó là một trang thương mại điện tử.

Các hệ thống thanh toán bị ngừng hoạt động:

- POS, QR Code thanh toán không thể hoạt động.
- Khách hàng không thể quẹt thẻ, dẫn đến mất doanh thu.

Task 2: Làm quen với Wireshark và thử nghiệm bắt gói tin trong mạng

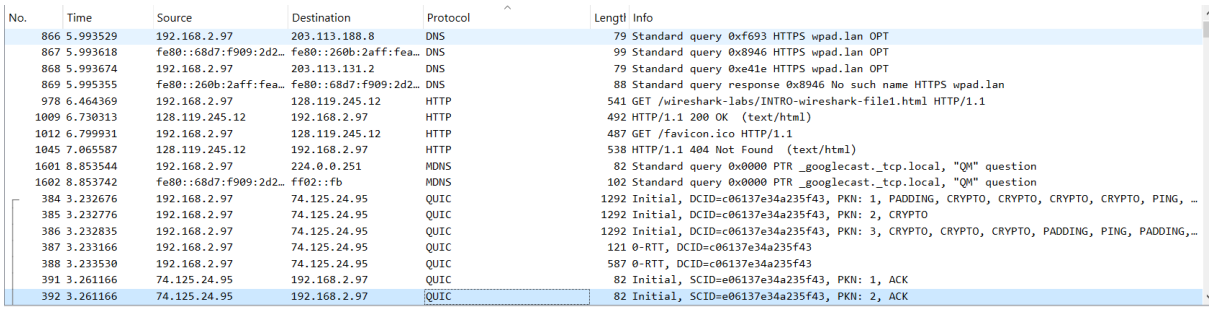
Tổng thời gian bắt gói tin 9s với số gói tin bắt được là 1631.



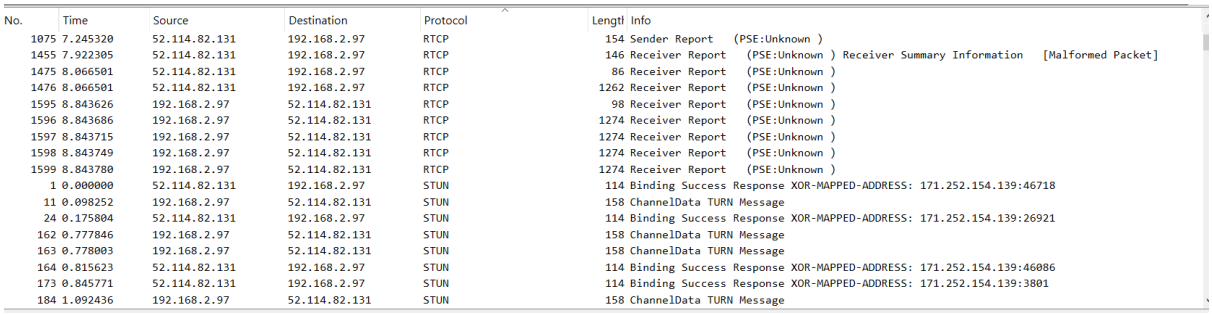
Liệt kê:

- DNS
- HTTP
- MDNS
- QUIC

- RTCP
- STUN

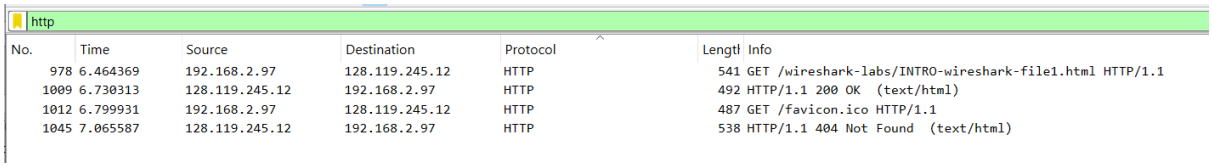


No.	Time	Source	Destination	Protocol	Length	Info
866	5.993529	192.168.2.97	203.113.188.8	DNS	79	Standard query 0xf693 HTTPS wpad.lan OPT
867	5.993618	fe80::68d7:f909:2d2…	fe80::260b:2aff:fea…	DNS	99	Standard query 0x8946 HTTPS wpad.lan OPT
868	5.993674	192.168.2.97	203.113.131.2	DNS	79	Standard query 0xe41e HTTPS wpad.lan OPT
869	5.995355	fe80::260b:2aff:fea…	fe80::68d7:f909:2d2…	DNS	88	Standard query response 0x8946 No such name HTTPS wpad.lan
978	6.464369	192.168.2.97	128.119.245.12	HTTP	541	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1009	6.730313	128.119.245.12	192.168.2.97	HTTP	492	HTTP/1.1 200 OK (text/html)
1012	6.799931	192.168.2.97	128.119.245.12	HTTP	487	GET /favicon.ico HTTP/1.1
1045	7.065587	128.119.245.12	192.168.2.97	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1601	8.853544	192.168.2.97	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
1602	8.853742	fe80::68d7:f909:2d2…	ff02::fb	MDNS	102	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
384	3.232676	192.168.2.97	74.125.24.95	QUIC	1292	Initial, DCID=c06137e34a235f43, PKN: 1, PADDING, CRYPTO, CRYPTO, CRYPTO, CRYPTO, PING, …
385	3.232776	192.168.2.97	74.125.24.95	QUIC	1292	Initial, DCID=c06137e34a235f43, PKN: 2, CRYPTO
386	3.232835	192.168.2.97	74.125.24.95	QUIC	1292	Initial, DCID=c06137e34a235f43, PKN: 3, CRYPTO, CRYPTO, CRYPTO, PADDING, PING, PADDING,…
387	3.233166	192.168.2.97	74.125.24.95	QUIC	121	0-RTT, DCID=c06137e34a235f43
388	3.233530	192.168.2.97	74.125.24.95	QUIC	587	0-RTT, DCID=c06137e34a235f43
391	3.261166	74.125.24.95	192.168.2.97	QUIC	82	Initial, SCID=e06137e34a235f43, PKN: 1, ACK
392	3.261166	74.125.24.95	192.168.2.97	QUIC	82	Initial, SCID=e06137e34a235f43, PKN: 2, ACK



No.	Time	Source	Destination	Protocol	Length	Info
1075	7.245320	52.114.82.131	192.168.2.97	RTCP	154	Sender Report (PSE:Unknown)
1455	7.922305	52.114.82.131	192.168.2.97	RTCP	146	Receiver Report (PSE:Unknown) Receiver Summary Information [Malformed Packet]
1475	8.066501	52.114.82.131	192.168.2.97	RTCP	86	Receiver Report (PSE:Unknown)
1476	8.066501	52.114.82.131	192.168.2.97	RTCP	1262	Receiver Report (PSE:Unknown)
1595	8.843626	192.168.2.97	52.114.82.131	RTCP	98	Receiver Report (PSE:Unknown)
1596	8.843686	192.168.2.97	52.114.82.131	RTCP	1274	Receiver Report (PSE:Unknown)
1597	8.843715	192.168.2.97	52.114.82.131	RTCP	1274	Receiver Report (PSE:Unknown)
1598	8.843749	192.168.2.97	52.114.82.131	RTCP	1274	Receiver Report (PSE:Unknown)
1599	8.843780	192.168.2.97	52.114.82.131	RTCP	1274	Receiver Report (PSE:Unknown)
1	0.000000	52.114.82.131	192.168.2.97	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 171.252.154.139:46718
11	0.098252	192.168.2.97	52.114.82.131	STUN	158	ChannelData TURN Message
24	0.175804	52.114.82.131	192.168.2.97	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 171.252.154.139:26921
162	0.777846	192.168.2.97	52.114.82.131	STUN	158	ChannelData TURN Message
163	0.778003	192.168.2.97	52.114.82.131	STUN	158	ChannelData TURN Message
164	0.815623	52.114.82.131	192.168.2.97	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 171.252.154.139:46086
173	0.845771	52.114.82.131	192.168.2.97	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 171.252.154.139:3801
184	1.092436	192.168.2.97	52.114.82.131	STUN	158	ChannelData TURN Message

Mất 0.3s từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận.



http

No.	Time	Source	Destination	Protocol	Length	Info
978	6.464369	192.168.2.97	128.119.245.12	HTTP	541	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
1009	6.730313	128.119.245.12	192.168.2.97	HTTP	492	HTTP/1.1 200 OK (text/html)
1012	6.799931	192.168.2.97	128.119.245.12	HTTP	487	GET /favicon.ico HTTP/1.1
1045	7.065587	128.119.245.12	192.168.2.97	HTTP	538	HTTP/1.1 404 Not Found (text/html)