

ĐẠI HỌC ĐÀ NẴNG
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA ĐIỆN TỬ – VIỄN THÔNG

BÁO CÁO
PBL3: MẠNG MÁY TÍNH

ĐỀ TÀI:
QUẢN TRỊ MẠNG SỬ DỤNG RASPBERRY PI

Sinh viên thực hiện:

Trần Anh Toàn – 106220237 – 22KTMT1
Trịnh Minh Việt – 106220241 – 22KTMT1
Trần Lê Long Vũ – 106220242 – 22KTMT1

Giảng viên hướng dẫn:

TS. Trần Thị Minh Hạnh

Đà Nẵng, 12/2025

QUẢN TRỊ MẠNG SỬ DỤNG RASPBERRY PI

Trần Anh Toàn – Trịnh Minh Việt – Trần Lê Long Vũ

toantran1752004@gmail.com – trinhminhviet21052018@gmail.com – longvu1611@gmail.com

Tóm tắt— Báo cáo này trình bày hệ thống giám sát mạng được triển khai trên nền tảng Raspberry Pi. Hệ thống có khả năng thu thập các thông số mạng như lưu lượng truyền, độ trễ và tỉ lệ mứt gói của các thiết bị trong mạng nội bộ, đồng thời hiển thị dữ liệu trực quan trên giao diện web dashboard. Các thông tin được trình bày qua biểu đồ vòng donut thể hiện lưu lượng hiện tại và các biểu đồ theo thời gian, giúp người dùng dễ dàng quan sát và đánh giá tình trạng mạng. Ngoài ra, hệ thống còn hỗ trợ chức năng chặn các địa chỉ IP không mong muốn, giúp nâng cao hiệu quả quản lý và bảo mật mạng.

Từ khóa: Giám sát mạng, Quản trị mạng, Raspberry Pi, Lưu lượng mạng, Độ trễ, Mứt gói, Chặn IP.

1 Giới thiệu

Trong thời đại công nghệ số, mạng máy tính giữ vai trò trung tâm trong hầu hết các hoạt động trao đổi dữ liệu, truyền tải thông tin và kết nối các hệ thống lại với nhau. Từ doanh nghiệp, cơ quan tổ chức cho đến người dùng cá nhân, sự hoạt động ổn định của mạng máy tính trở thành yếu tố thiết yếu giúp duy trì làm việc, truy cập dịch vụ trực tuyến và đảm bảo trải nghiệm liền mạch. Tuy nhiên, hệ thống mạng trong thực tế thường xuyên đối mặt với nhiều vấn đề như nghẽn băng thông, tăng độ trễ, mất kết nối, tỉ lệ mứt gói cao hoặc xuất hiện các truy cập không mong muốn từ những địa chỉ IP lạ. Những sự cố này không chỉ làm gián đoạn hoạt động mà còn ảnh hưởng trực tiếp đến hiệu năng và tính an toàn của toàn bộ hệ thống.

Để giải quyết các vấn đề trên, việc quản trị mạng một cách chủ động và liên tục trở nên vô cùng quan trọng. Về tổng quan, quản trị mạng bao gồm một tập hợp các công việc liên quan đến việc giám sát, quản lý, bảo vệ và duy trì hoạt động của hệ thống mạng. Trước hết, người quản trị cần theo dõi lưu lượng dữ liệu, độ trễ, tỉ lệ mứt gói và mức sử dụng băng thông nhằm phát hiện kịp thời các bất thường trong quá trình truyền dữ liệu. Bên cạnh đó, quản trị mạng còn liên quan đến quản lý và cấu hình các thiết bị mạng như router, switch, điểm truy cập và tường lửa để đảm bảo khả năng truyền thông hiệu quả. Việc quản lý địa chỉ IP, giám sát thiết bị truy cập và phát hiện các kết nối không hợp lệ cũng là một phần quan trọng nhằm duy trì tính ổn định và kiểm soát trong hệ thống. Cuối cùng, công tác bảo mật mạng bao gồm phát hiện truy cập trái phép, ngăn chặn IP độc hại, và thiết lập các cơ chế phòng vệ giúp bảo vệ hệ thống trước những nguy cơ tấn công hoặc thất thoát dữ liệu.

Xuất phát từ nhu cầu thực tế đó, dự án này tập trung xây dựng một hệ thống hỗ trợ quản trị và giám sát mạng dựa trên nền tảng Raspberry Pi. Hệ thống được thiết kế nhằm thu thập và hiển thị trực quan các thông số mạng như lưu lượng truyền tải, độ trễ phản hồi, tỉ lệ mứt gói và phân bố giao thức. Raspberry Pi được cấu hình như một thiết bị cầu (bridge) giúp quan sát toàn bộ lưu lượng đi qua mạng nội bộ. Các module phần mềm do nhóm xây dựng đảm nhiệm việc đo đạc và ghi nhận dữ liệu theo thời gian thực, sau đó tổng hợp và hiển thị trên dashboard web để người dùng dễ dàng theo dõi và đánh giá. Ngoài khả năng giám sát, hệ thống còn tích hợp chức năng chặn các địa chỉ IP không mong muốn, hỗ trợ tăng cường bảo mật và hạn chế truy cập gây ảnh hưởng đến hiệu năng mạng.

Họ và tên	Nhiệm vụ	Phần trăm
Trần Anh Toàn	Thực thi giám sát lưu lượng	33.33%
Trịnh Minh Việt	Thực thi giám sát và chặn IP nguy hiểm	33.33%
Trần Lê Long Vũ	Thực thi hiển thị lưu lượng lên web dashboard	33.33%

2 Các nghiên cứu và phương pháp liên quan

Trong lĩnh vực giám sát và bảo mật mạng, các nghiên cứu ban đầu chủ yếu tập trung vào công cụ phần mềm giám sát lưu lượng và phát hiện sự cố, được triển khai trên các máy chủ trung tâm. Svoboda cùng cộng sự đã tổng hợp và so sánh các phương pháp giám sát mạng truyền thống [1], cho thấy đa số giải pháp phụ thuộc vào phần cứng đắt tiền và thiếu khả năng quan sát toàn bộ luồng dữ liệu trong mạng. Hạn chế này dẫn đến việc khó phát hiện các bất thường cục bộ hoặc đánh giá hiệu suất của từng nút mạng.

Để cải thiện tính trực quan và khả năng phản ứng của người quản trị, Saeed cùng cộng sự phát triển mô hình dashboard giám sát mạng hướng người dùng [2], cho phép biểu diễn dữ liệu mạng thông qua giao diện đồ họa thân thiện. Tuy nhiên, nghiên cứu này chỉ xử lý dữ liệu thu thập được từ các hệ thống có sẵn, chưa tích hợp chức năng thu thập dữ liệu thời gian thực từ phần cứng giám sát.

Nhằm tăng cường khả năng phát hiện sớm các bất thường, Shikhaliyev và Sukhostat áp dụng mô hình học sâu LSTM để dự đoán các hành vi mạng bất thường dựa trên tập dữ liệu CICIDS2017 [3]. Cách tiếp cận này đạt độ chính xác cao nhưng đòi hỏi nguồn dữ liệu đầu vào lớn và hệ thống phần cứng có cấu hình mạnh, khiến việc triển khai thực tế trong các mạng nhỏ gặp khó khăn.

Song song đó, các nghiên cứu hướng đến thiết bị thu thập dữ liệu vật lý chi phí thấp đã xuất hiện, tận dụng các nền tảng máy tính đơn bo mạch (SBC) như Raspberry Pi để thay thế các thiết bị chuyên dụng đắt tiền. Ramalho và các cộng sự đề xuất hệ thống thu thập dữ liệu trong mạng điện thông minh [4], còn Chiang và các cộng sự phát triển module giám sát tình trạng máy móc trong nhà máy thông minh [5]. Tuy nhiên, các công trình này chủ yếu giới hạn trong môi trường IoT hoặc công nghiệp, chưa được mở rộng cho mục đích giám sát lưu lượng mạng máy tính.

Để khắc phục khoảng trống này, Varol và İskifiyeli đã giới thiệu thiết bị Network TAP (Test Access Point) chi phí thấp sử dụng Raspberry Pi 4 [6], có khả năng bắt và phân tích gói tin thời gian thực mà không cần máy tính ngoài. Thiết bị của họ giải quyết được vấn đề chi phí cao của các TAP thương mại (Beckhoff ET2000, Profitap C1AP-1G) và cho phép mở rộng lưu trữ, kết nối giám sát từ xa. Tuy nhiên, hệ thống vẫn thiên về ghi nhận gói tin thô mà chưa có lớp hiển thị trực quan hoặc cơ chế điều khiển chủ động.

Kết thừa và mở rộng các hướng tiếp cận trên, hệ thống giám sát mạng trong nghiên cứu này được triển khai trên nền tảng Raspberry Pi, tích hợp thu thập – phân tích – hiển thị – kiểm soát trong cùng một thiết bị. Hệ thống không chỉ thu thập các thông số mạng như lưu lượng truyền, độ trễ, tỉ lệ mất gói, mà còn hiển thị dữ liệu trực quan trên dashboard web bằng các biểu đồ dạng donut và biểu đồ thời gian. Đồng thời, chức năng chặn địa chỉ IP không mong muốn được bổ sung nhằm tăng tính chủ động trong quản lý và bảo mật. Qua đó, hệ thống này khắc phục hạn chế của các nghiên cứu trước bằng cách hợp nhất khả năng quan sát, phân tích và phản ứng trong một giải pháp thống nhất, chi phí thấp và dễ triển khai.

3 Quản trị mạng sử dụng Raspberry Pi

3.1 Tổng quan phương pháp

Quản trị mạng là lĩnh vực bao gồm toàn bộ các hoạt động nhằm đảm bảo hệ thống mạng máy tính hoạt động ổn định, an toàn và hiệu quả thông qua việc giám sát, quản lý, bảo trì và tối ưu hóa các thành phần mạng. Về mặt lý thuyết, quản trị mạng được chia thành năm lĩnh vực chính theo mô hình FCAPS của ISO: Quản lý lỗi (Fault Management) tập trung vào phát hiện, ghi nhận và khắc phục các sự cố mạng như mất kết nối, lỗi thiết bị hay nghẽn đường truyền; Quản lý cấu hình (Configuration Management) đảm nhiệm việc thiết lập, duy trì và cập nhật cấu hình của các thiết bị mạng như router, switch, firewall để đảm bảo hoạt động đúng chức năng; Quản lý hiệu suất (Performance Management) theo dõi và đánh giá các chỉ số như băng thông, độ trễ, tốc độ truyền tải và tỉ lệ mất gói để tối ưu hóa hiệu suất mạng; Quản lý bảo mật (Security Management) bảo vệ mạng khỏi các mối đe dọa thông qua kiểm soát truy cập, mã hóa dữ liệu, phát hiện xâm nhập và ngăn chặn tấn công; và Quản lý kế toán (Accounting Management) giám sát việc sử dụng tài nguyên mạng của từng người dùng hoặc thiết bị. Trong thực tế, người quản trị mạng sử dụng các giao thức chuẩn như SNMP (Simple Network Management Protocol) để thu thập thông tin từ các thiết bị, các công cụ giám sát như Nagios, Zabbix, Wireshark

để phân tích lưu lượng và phát hiện bất thường, cũng như triển khai các cơ chế bảo mật như IDS/IPS, VPN và firewall để bảo vệ mạng. Quy trình quản trị mạng thường bao gồm giám sát liên tục các thông số mạng, thu thập và phân tích dữ liệu để nhận diện xu hướng và bất thường, phản ứng kịp thời với các sự cố, và thực hiện bảo trì định kỳ như cập nhật firmware, sao lưu cấu hình và nâng cấp hệ thống khi cần thiết, nhằm đảm bảo mạng luôn đáp ứng được yêu cầu về tính sẵn sàng, độ tin cậy và bảo mật.

Dựa trên nền tảng lý thuyết quản trị mạng, nhóm đã triển khai thành công một hệ thống giám sát và quản trị mạng hoàn chỉnh trên nền tảng Raspberry Pi 4. Hệ thống được thiết kế với kiến trúc cầu mạng (bridge), cho phép Raspberry Pi đặt ở vị trí trung gian để quan sát toàn bộ lưu lượng đi qua mạng nội bộ mà không làm gián đoạn kết nối. Về chức năng giám sát, hệ thống có khả năng thu thập và phân tích các thông số mạng quan trọng bao gồm lưu lượng truyền tải (số byte và số gói tin), độ trễ phản hồi, tỉ lệ mất gói, và phân bố giao thức trong mạng. Dữ liệu được xử lý và tổng hợp tự động, sau đó hiển thị trực quan trên giao diện dashboard web thông qua các biểu đồ vòng và biểu đồ theo thời gian, giúp người quản trị dễ dàng theo dõi và đánh giá tình trạng mạng. Ngoài khả năng giám sát thụ động, hệ thống còn tích hợp chức năng bảo mật chủ động với khả năng phát hiện các hành vi bất thường trong mạng như tấn công SYN Flood và tự động chặn các địa chỉ IP không mong muốn, góp phần nâng cao hiệu quả quản lý và bảo vệ hệ thống mạng.

3.2 Giới thiệu phần cứng



Hình 1: Raspberry Pi 4



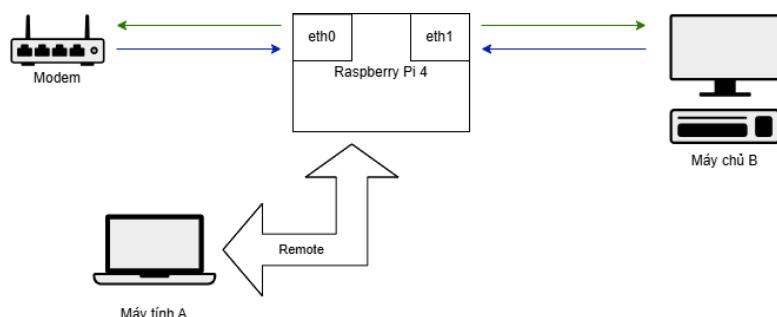
Hình 2: USB to LAN Adapter



Hình 3: Dây LAN

Trong dự án giám sát mạng này, các thiết bị phần cứng chính bao gồm Raspberry Pi 4, USB to LAN adapter và dây cáp mạng được minh họa như Hình 1, Hình 2, Hình 3 mỗi thiết bị đều có vai trò riêng quan trọng. Raspberry Pi 4 là máy tính nhúng nhỏ gọn nhưng mạnh mẽ, được sử dụng làm trung tâm thu thập và xử lý dữ liệu mạng qua đó có thể hiển thị các thông số như lưu lượng, độ trễ và tỉ lệ mất gói. USB to LAN adapter được dùng để mở rộng khả năng kết nối Ethernet, cho phép Raspberry Pi giám sát nhiều thiết bị hoặc phân đoạn mạng khác nhau cùng lúc, đảm bảo dữ liệu được thu thập đầy đủ và đồng bộ. Dây LAN đóng vai trò kết nối vật lý giữa Raspberry Pi, USB to LAN và các thiết bị mạng khác, giúp truyền dữ liệu ổn định, nhanh chóng và đáng tin cậy. Đồng thời, Raspberry Pi sử dụng thẻ nhớ 64GB làm bộ lưu trữ chính cho hệ điều hành và dữ liệu mạng.

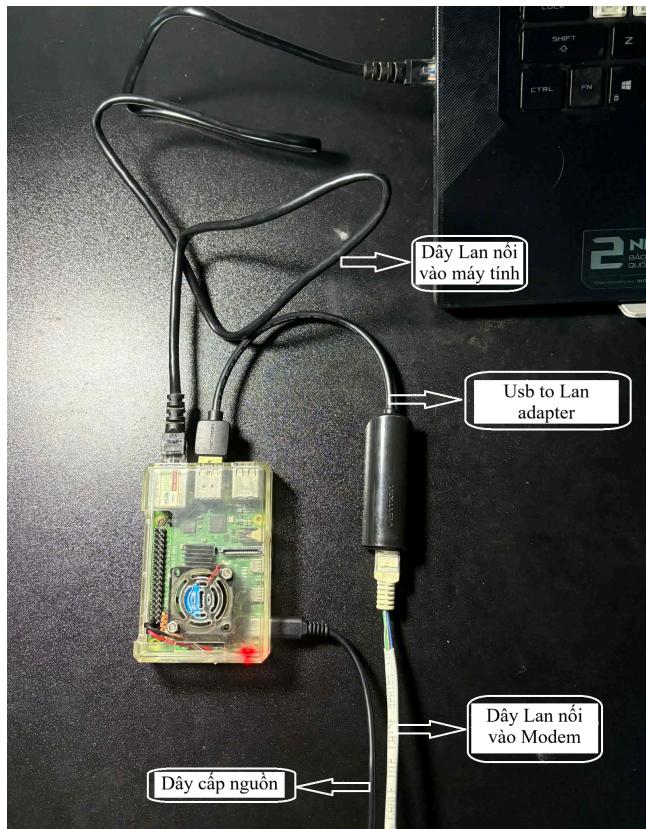
3.3 Sơ đồ kết nối



Hình 4: Topology chính của hệ thống

Hình 4 thể hiện topology chính của hệ thống trong chức năng giám sát lưu lượng cũng như là ngăn chặn IP nguy hiểm. Với việc Raspberry Pi nằm giữa đường LAN nối từ máy chủ B đến modem đóng vai trò như một Man-in-the-Middle là

cầu nối cho giao tiếp giữa máy tính và modem. Để xem cũng như là vận hành Raspberry Pi, sử dụng một máy tính A remote đến nó.



Hình 5: Sơ đồ kết nối thực tế của hệ thống

Hình 5 là sơ đồ kết nối các thiết bị phần cứng thực tế trong hệ thống giám sát mạng, triển khai theo kiểu cầu như topology được thể hiện ở Hình 4. Raspberry Pi 4 đóng vai trò bộ xử lý trung tâm, thu thập, xử lý và lưu trữ dữ liệu mạng, đồng thời cấp nguồn cho các thiết bị kết nối phụ trợ. Do Raspberry Pi chỉ có một cổng LAN, nên dự án sử dụng USB to LAN adapter để mở rộng khả năng kết nối, cho phép một đầu LAN kết nối với máy tính và đầu còn lại kết nối với router Wi-Fi, từ đó bất kỳ thiết bị nào trong cùng mạng cũng có thể truy cập dashboard và xem các thông số mạng. Dây LAN đảm bảo truyền dữ liệu ổn định, còn dữ liệu thu thập được lưu trữ trên thẻ nhớ 64GB của Raspberry Pi và tổng hợp vào các file CSV để hiển thị trực quan trên giao diện web.

Sau khi cấu hình kiểu cầu thực hiện theo các bước được trình bày kĩ hơn ở phụ lục, được kết quả như Hình 6, thể hiện việc cấu hình kết nối cầu trên Raspberry Pi đã được thực hiện thành công. Trong cửa sổ terminal, giao diện bridge0 xuất hiện với trạng thái UP, đồng thời hai giao diện eth0 và eth1 đã được gán vào bridge0, xác nhận rằng chúng đang hoạt động như một cầu mạng thống nhất. Sau khi cầu được thiết lập, máy tính Windows cũng đã nhận mạng LAN thông qua Raspberry Pi, chứng tỏ hệ thống bridge hoạt động ổn định. Việc thiết lập cầu mạng như trong hình 5 mang lại lợi ích quan trọng cho quá trình quản trị mạng bằng Raspberry Pi. Khi Raspberry Pi đóng vai trò bridge, nó có thể theo dõi, thu thập và phân tích toàn bộ lưu lượng đi qua giữa hai cổng mạng. Điều này cho phép triển khai hệ thống Network Monitor một cách hiệu quả. Nhờ vậy, Raspberry Pi đóng vai trò như thiết bị giám sát lưu lượng chuyên dụng trong mô hình quản trị mạng.

```

pi@raspberrypi:~ $ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master bridge0 state UP group default qlen 1000
    link/ether dc:a6:32:b8:34:0c brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether dc:a6:32:d8:34:0e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.14/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
        valid_lft 10724sec preferred_lft 10724sec
    inet6 2402:800:6294:29e9:1f83:cd5b:218b:f05d/64 scope global dynamic noprefixroute
        valid_lft 86309sec preferred_lft 86309sec
    inet6 fe80::6b2c:876d:3ca6:8259/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
4: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel master bridge0 state UP group default qlen 1000
    link/ether 00:24:32:a0:05:4c brd ff:ff:ff:ff:ff:ff
5: bridge0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 5e:0d:e0:97:13:7e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global bridge0
        valid_lft forever preferred_lft forever
    inet6 2402:800:6294:29e9:5c0d:e0ff:fe97:137e/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86309sec preferred_lft 86309sec
    inet6 fe80::5c0d:e0ff:fe97:137e/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
pi@raspberrypi:~ $
```

Hình 6: Kết quả của lệnh ip addr show sau khi kết nối cầu

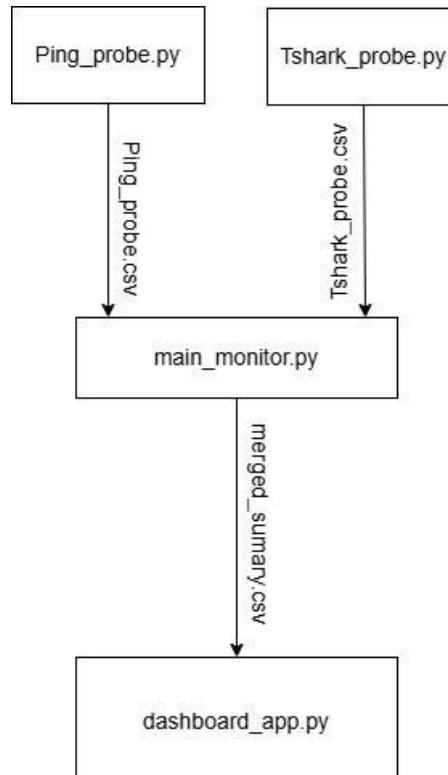
Từ output của lệnh ip addr show, Hình 6 biểu thị rõ ràng trạng thái hoạt động của các interface mạng sau khi thiết lập bridge. Cụ thể, eth0 và eth1 đều ở trạng thái UP và được gắn kết vào bridge0 với vai trò master bridge, điều này chứng minh rằng hai cổng Ethernet vật lý đã được kết nối thành công vào cầu mạng ảo.

Hình 6 cũng biểu thị rằng bridge0 đã được cấp phát địa chỉ IP và hoạt động ổn định trong mạng nội bộ. Interface wlan0 cũng ở trạng thái UP, đảm bảo kết nối không dây song song với bridge để quản lý từ xa.

Như vậy, Hình 6 minh họa việc thiết lập bridge đã hoàn tất và sẵn sàng cho các bước tiếp theo trong việc triển khai hệ thống giám sát mạng, với tất cả các interface đều hoạt động ổn định và có khả năng capture lưu lượng mạng đi qua bridge.

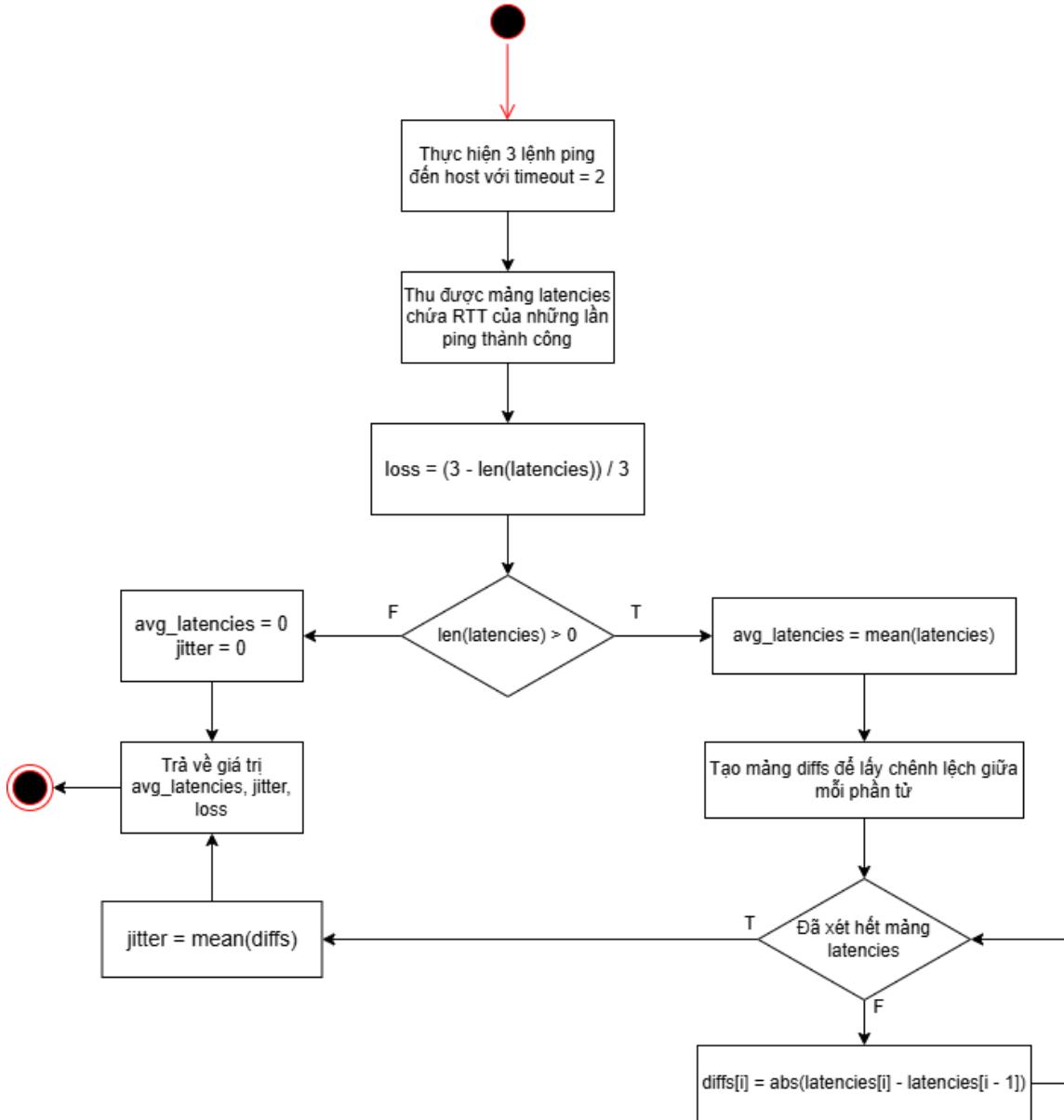
3.4 Giám sát lưu lượng

Hệ thống giám sát mạng được triển khai trên Raspberry Pi được tổ chức theo sơ đồ khối như Hình 7, trong đó mỗi module đảm nhiệm một nhiệm vụ thu thập dữ liệu riêng, sử dụng các thư viện và công cụ chuyên biệt để bảo đảm độ chính xác và tính ổn định của dữ liệu.



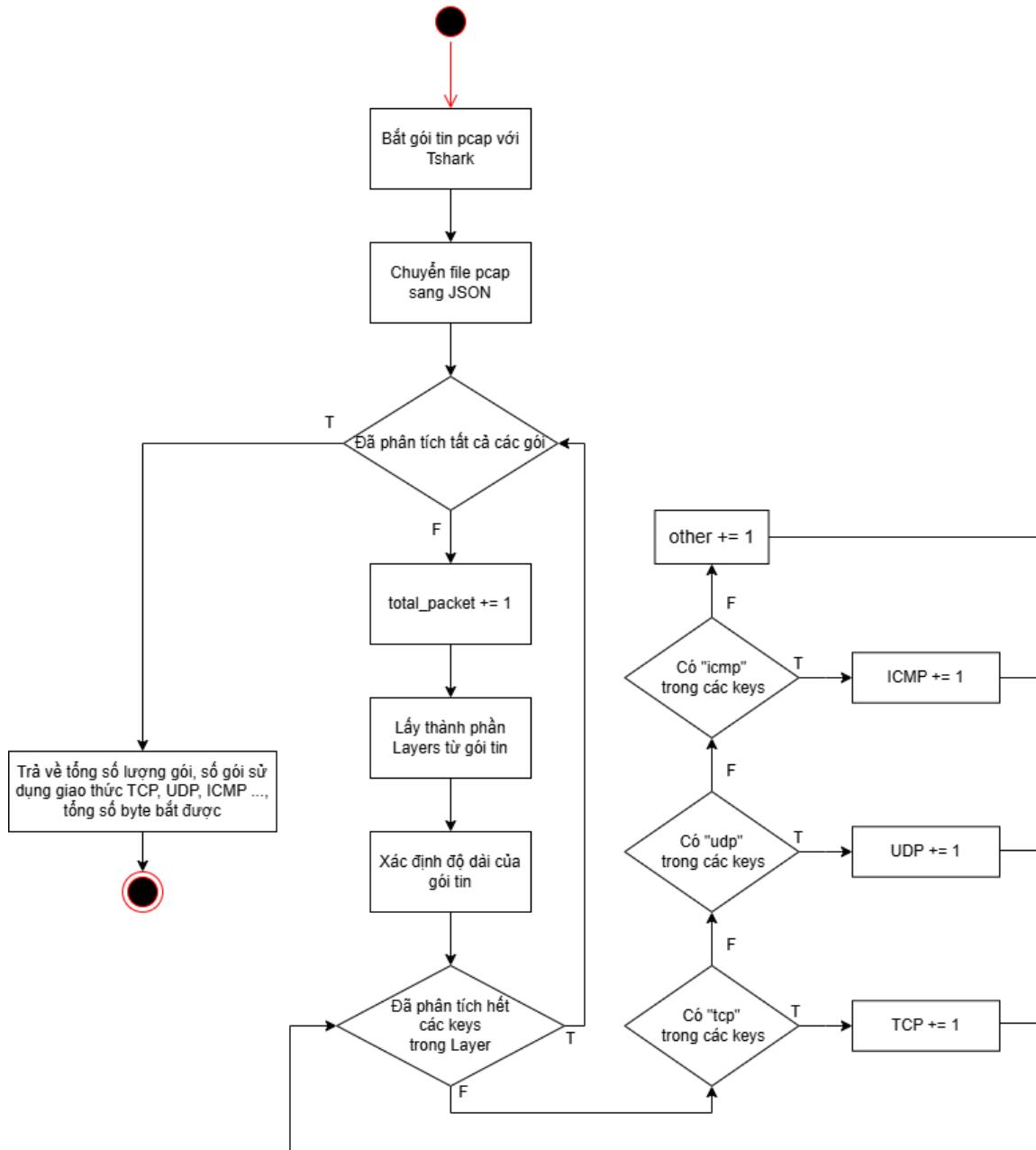
Hình 7: Sơ đồ khái niệm của hệ thống

Đầu tiên, module Ping_probe.py với thuật toán được thể hiện trong Hình 8 phụ trách đo độ trễ (latency) và tỉ lệ mất gói (packet loss), module này sử dụng thư viện ping3, các thông tin này được ghi vào file ping_probe.csv. Song song với đó là việc giám sát các gói tin được thực hiện bởi module và Tshark.py, thuật toán được mô tả như Hình 9, cung cấp khả năng bắt và phân tích gói tin ở mức giao thức, sử dụng trực tiếp công cụ tshark thông qua gọi lệnh hệ thống bằng Python. Công cụ này cho phép trích xuất các trường quan trọng như thời gian gói tin, địa chỉ nguồn – đích, loại giao thức (TCP/UDP/ICMP) hoặc số lượng gói tin trong mỗi khoảng thời gian, kết quả được ghi vào tshark_probe.csv.



Hình 8: Lưu đồ thuật toán của module Ping_probe.py

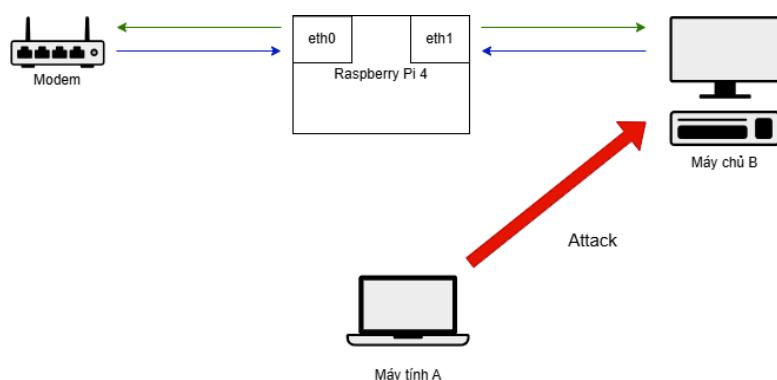
Hai file dữ liệu được tạo bởi các module trên được đưa vào module trung tâm main_monitor.py, nơi toàn bộ dữ liệu được đồng bộ hóa và tổng hợp. Module này đọc dữ liệu từ các file CSV, dựa trên đó hệ thống tính toán các chỉ số tổng hợp như lưu lượng tổng, độ trễ trung bình, tỉ lệ mất gói, số lượng gói tin theo giao thức. Tất cả dữ liệu đã chuẩn hóa và tổng hợp được ghi vào một file duy nhất là merged_summary.csv. File này đóng vai trò như nguồn dữ liệu trung tâm cho dashboard, giúp đơn giản hóa việc truy xuất và hiển thị dữ liệu. Cuối cùng, module dashboard_app.py sử dụng Flask để xây dựng giao diện web hiển thị dữ liệu theo thời gian thực. Ứng dụng sẽ đọc merged_summary.csv theo chu kỳ hoặc thông qua cơ chế gọi API, sau đó chuyển đổi dữ liệu sang các biểu đồ trực quan bằng thư viện Chart.js. Biểu đồ vòng được sử dụng để minh họa lưu lượng hiện tại, trong khi biểu đồ đường theo thời gian thể hiện sự biến động của độ trễ và tỉ lệ mất gói.



Hình 9: Lưu đồ thuật toán của module Tshark_probe.py

3.5 Chặn IP nguy hiểm

3.5.1 Kịch bản mô phỏng tấn công



Hình 10: Topology của kịch bản mô phỏng tấn công SYN Flood

Kịch bản mô phỏng được xây dựng với topology như Hình 10 nhằm đánh giá khả năng phát hiện và ngăn chặn tấn công trong mạng nội bộ bằng Raspberry Pi 4. Hệ thống thí nghiệm gồm ba thành phần chính: máy tính A đóng vai trò là kẻ tấn công, Raspberry Pi 4 đặt ở vị trí trung gian để giám sát lưu lượng, và thiết bị đích là máy chủ B. Đối với kịch bản này, hệ thống được bố trí theo đúng sơ đồ kết nối đã thể hiện trong Hình 4, trong đó Raspberry Pi được đặt ở vị trí trung gian giữa máy tính B và modem WiFi. Máy tính A sẽ đóng vai kẻ tấn công với phương pháp tấn công tới địa chỉ IP của máy B và trên Pi 4 sẽ thực hiện chống tấn công SYN Flood, UDP Flood, ICMP Flood và HTTP Flood bằng cách sniff các gói và xem header nếu có hành vi bất thường nếu vượt ngưỡng cài đặt sẽ tiến hành chặn IP可疑.

Để mở rộng khả năng chống tấn công nhóm đã thêm một máy tấn công C để thử nghiệm tấn công DDoS đến máy chủ B và trên Raspberry Pi triển khai code giám sát và đếm tổng lượng gói trong một khoảng thời gian nếu vượt ngưỡng thì sẽ chặn các IP có số lượng gói tấn công đến lớn nhất từ trên xuống dưới (có thể cài đặt số lượng IP muốn chặn và số gói vượt ngưỡng để chặn 1 IP).

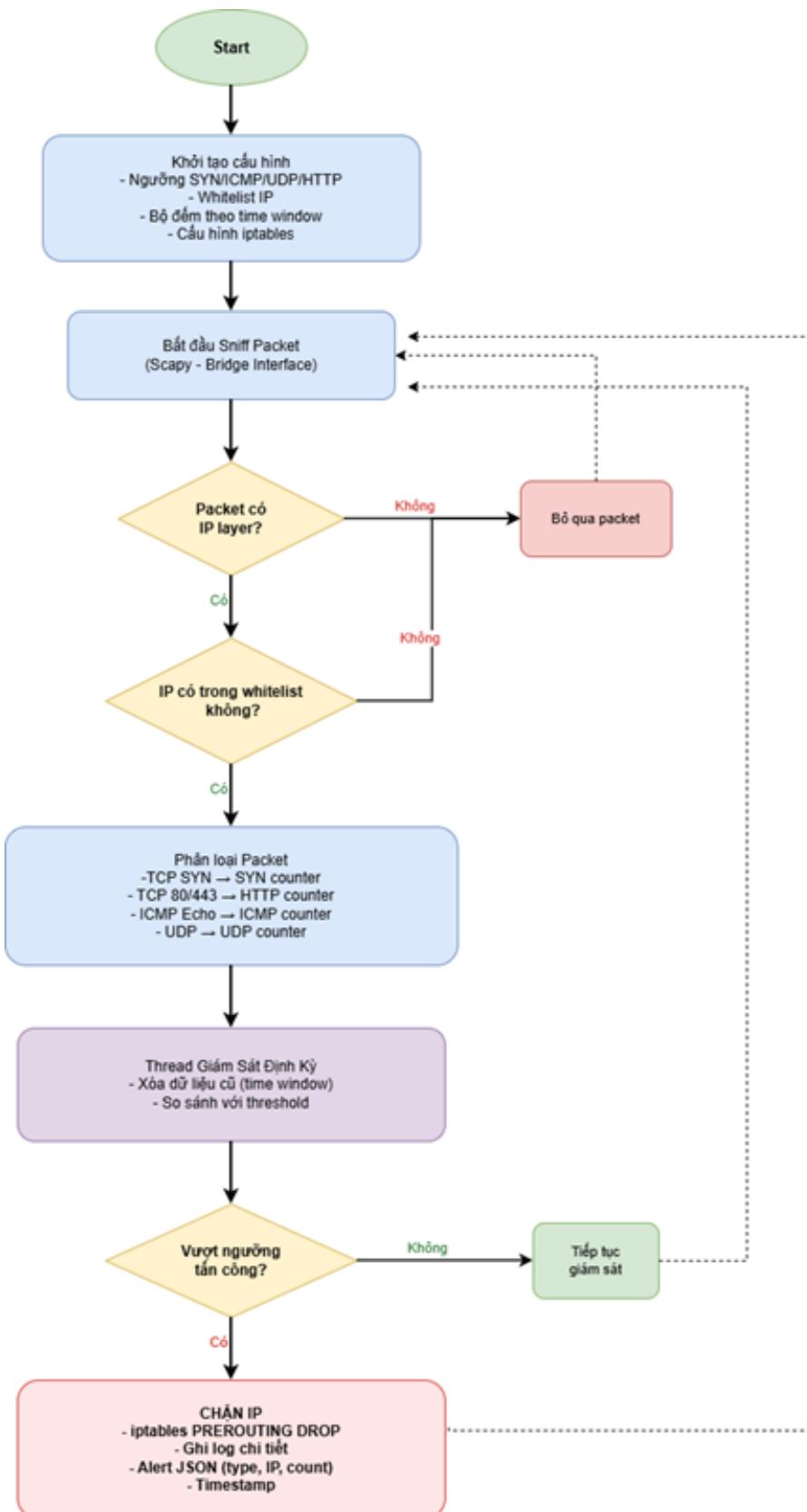
3.5.2 Phương pháp thực hiện

Hệ thống được xây dựng với thuật lưu đồ thuật toán như Hình 11 nhằm phát hiện và ngăn chặn các cuộc tấn công từ chối dịch vụ DoS và DDoS dựa trên việc giám sát lưu lượng mạng theo thời gian thực và phát hiện hành vi bất thường dựa trên ngưỡng trong một cửa sổ thời gian xác định. Phương pháp này không phụ thuộc vào chữ ký tấn công, phù hợp với các mô hình mạng gateway hoặc bridge.

Lưu lượng mạng được giám sát thụ động tại tầng mạng bằng cách bắt các gói tin IP đi qua giao diện bridge. Các gói tin sau đó được phân loại theo giao thức nhằm phát hiện ba dạng tấn công phổ biến gồm TCP SYN Flood, ICMP Flood, UDP Flood và HTTP Flood. Với mỗi địa chỉ IP nguồn, hệ thống theo dõi số lượng gói tin tương ứng trong một khoảng thời gian cố định và so sánh với các ngưỡng đã được thiết lập trước.

Khi số lượng gói tin từ một IP vượt quá ngưỡng cho phép, IP này được xác định là có dấu hiệu tấn công. Hệ thống sẽ thực hiện phản ứng chủ động bằng cách tự động chặn IP nguồn thông qua tường lửa iptables tại bảng raw (chuỗi PREROUTING), nhằm loại bỏ các gói tin độc hại ngay từ giai đoạn sớm, giảm tải xử lý cho kernel.

Ngoài ra, hệ thống hỗ trợ danh sách trắng để tránh chặn nhầm các địa chỉ IP quan trọng và ghi lại các sự kiện phát hiện, chặn tấn công phục vụ cho công tác giám sát và phân tích. Phương pháp này cho phép triển khai đơn giản, hiệu quả và phù hợp cho các hệ thống mạng có quy mô nhỏ và trung bình.



Hình 11: Lưu đồ thuật toán phương pháp chặn IP

4 Thực nghiệm và kết quả

4.1 Kết quả thực hiện giám sát

Khi thực thi các file, nhận được giao diện các file như Hình 12.

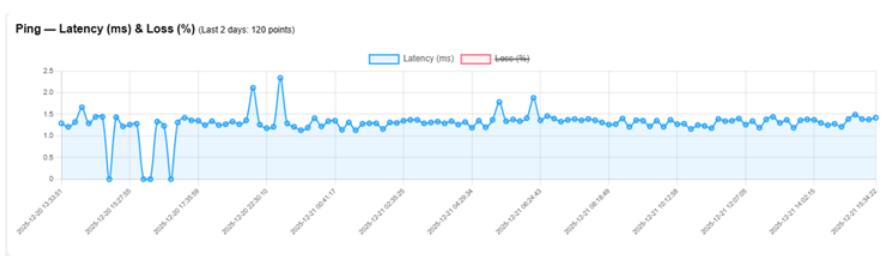


Hình 12: Giao diện Dashboard

Hình 12 biểu thị giao diện dashboard của hệ thống Pi NetWatch, được sử dụng để giám sát và phân tích tình trạng mạng theo thời gian thực. Giao diện bao gồm các biểu đồ trực quan thể hiện tỷ lệ thành công và thất bại của các gói tin ping, độ trễ mạng (latency) và độ dao động trễ (jitter) theo thời gian. Bên cạnh đó, hệ thống còn cung cấp biểu đồ phân bố lưu lượng theo từng giao thức mạng, cho phép người dùng dễ dàng theo dõi mức độ sử dụng của các giao thức như TCP, UDP, ICMP và các giao thức khác.

Ngoài ra, Hình 12 còn cho thấy sự thay đổi của số lượng gói tin và dung lượng dữ liệu truyền tải trong từng khoảng thời gian, giúp người quản trị nhanh chóng phát hiện các bất thường như mất gói, tăng đột biến lưu lượng hoặc suy giảm chất lượng kết nối. Nhờ cách trình bày rõ ràng và trực quan, dashboard hỗ trợ hiệu quả cho việc theo dõi, đánh giá và phân tích hiệu năng mạng của hệ thống.

Sau đây là các biểu đồ chi tiết lưu lượng được ghi từ 13h 20/12/2025 đến 16h ngày 21/12/2025

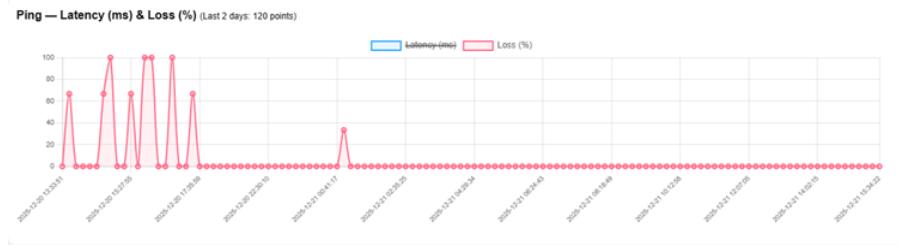


Hình 13: Biểu đồ độ trễ

Hình 13 biểu thị sự thay đổi của độ trễ mạng (latency) trong quá trình giám sát theo thời gian. Kết quả cho thấy giá trị độ trễ nhin chung duy trì ở mức tương đối ổn định, chỉ xuất hiện một số thời điểm tăng đột biến. Những biến động này phản ánh tình trạng dao động tạm thời của đường truyền hoặc ảnh hưởng từ lưu lượng mạng tại các thời điểm khác nhau.

Thông qua Hình 13, có thể nhận thấy hệ thống mạng hoạt động ổn định trong phần lớn thời gian giám sát, không xuất hiện các hiện tượng tăng độ trễ kéo dài. Biểu đồ độ trễ giúp người quản trị đánh giá chất lượng kết nối mạng, đồng thời

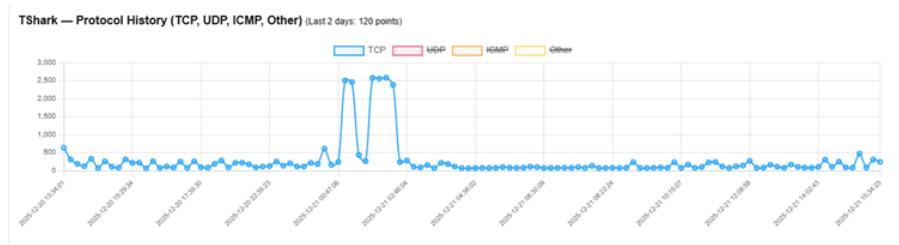
hỗ trợ phát hiện sớm các dấu hiệu bất thường để kịp thời đưa ra biện pháp xử lý phù hợp.



Hình 14: Biểu đồ tần suất mất gói

Hình 14 biểu thị sự biến động của tỷ lệ mất gói (packet loss) trong quá trình giám sát kết nối mạng theo thời gian. Kết quả cho thấy tại một số thời điểm ban đầu xuất hiện hiện tượng mất gói với tỷ lệ cao, trong khi phần lớn các khoảng thời gian còn lại tỷ lệ mất gói duy trì ở mức thấp hoặc bằng không. Điều này cho thấy kết nối mạng nhìn chung ổn định, các sự cố mất gói chỉ xảy ra cục bộ và không kéo dài.

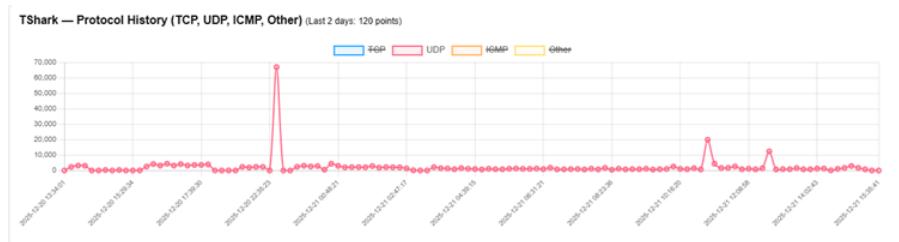
Thông qua Hình 14, hệ thống cho phép người quản trị dễ dàng nhận diện các thời điểm xảy ra suy giảm chất lượng đường truyền, từ đó hỗ trợ phân tích nguyên nhân và đưa ra biện pháp khắc phục phù hợp nhằm đảm bảo độ tin cậy của hệ thống mạng.



Hình 15: Biểu đồ TCP

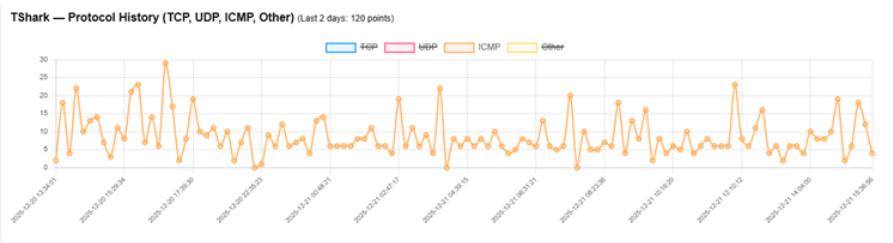
Hình 15 biểu thị sự thay đổi lưu lượng của giao thức TCP trong quá trình giám sát mạng theo thời gian. Kết quả cho thấy lưu lượng TCP chiếm tỷ trọng chủ yếu và duy trì ở mức ổn định trong phần lớn thời gian quan sát. Tuy nhiên, tại một số thời điểm xuất hiện các đinh tăng đột biến, phản ánh sự gia tăng tạm thời của các phiên truyền dữ liệu sử dụng giao thức TCP.

Thông qua Hình 15, có thể nhận thấy giao thức TCP đóng vai trò chính trong việc truyền tải dữ liệu của hệ thống, đồng thời biểu đồ cũng hỗ trợ người quản trị phát hiện các thời điểm lưu lượng bất thường để phục vụ cho việc phân tích và đánh giá hiệu năng mạng.



Hình 16: Biểu đồ UDP

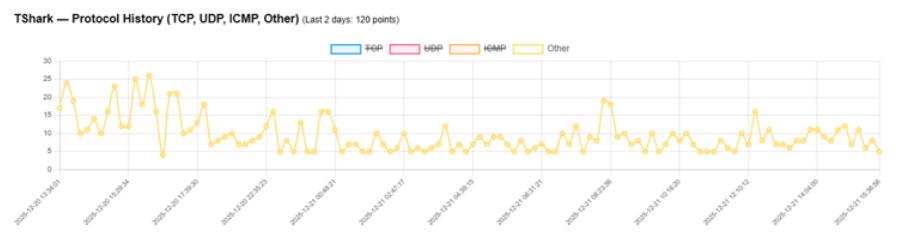
Hình 16 thể hiện lịch sử lưu lượng giao thức UDP trong khoảng thời gian được ghi nhận bằng công cụ TShark. Biểu đồ cho thấy lưu lượng UDP duy trì ở mức tương đối ổn định trong phần lớn thời gian quan sát, tuy nhiên tại một số thời điểm xuất hiện các đợt tăng đột biến rõ rệt. Những đinh lưu lượng này phản ánh các phiên truyền dữ liệu UDP có cường độ cao trong thời gian ngắn, liên quan đến các hoạt động như truyền dữ liệu thời gian thực, broadcast hoặc các ứng dụng yêu cầu độ trễ thấp. Nhìn chung, Hình 16 giúp minh họa xu hướng sử dụng giao thức UDP trong hệ thống mạng và hỗ trợ việc nhận diện các thời điểm lưu lượng bất thường phục vụ cho công tác giám sát và phân tích mạng.



Hình 17: Biểu đồ ICMP

Hình 17 biểu thị sự thay đổi lưu lượng của giao thức ICMP trong quá trình giám sát mạng theo thời gian. Kết quả cho thấy lưu lượng ICMP xuất hiện xuyên suốt giai đoạn quan sát với mức dao động tương đối thường xuyên, tuy không chiếm tỷ trọng lớn so với các giao thức truyền dữ liệu chính. Tại một số thời điểm, lưu lượng ICMP tăng cao hơn mức trung bình, phản ánh các hoạt động như kiểm tra kết nối, phản hồi lỗi hoặc giám sát trạng thái mạng.

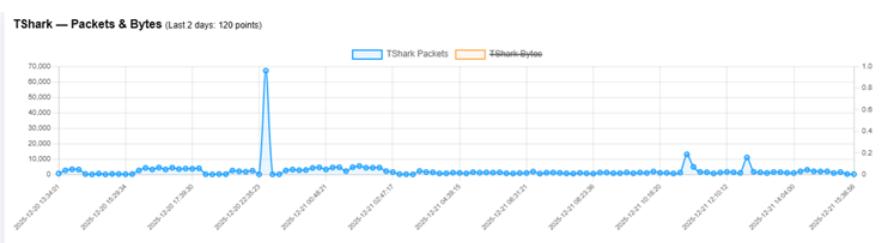
Thông qua Hình 17, có thể nhận thấy giao thức ICMP đóng vai trò hỗ trợ trong việc quản lý và chẩn đoán mạng, đồng thời biểu đồ giúp người quản trị theo dõi tình trạng hoạt động của hệ thống và phát hiện sớm các dấu hiệu bất thường liên quan đến kết nối hoặc cấu hình mạng.



Hình 18: Biểu đồ các giao thức khác

Hình 18 biểu thị sự thay đổi lưu lượng của nhóm giao thức khác trong quá trình giám sát mạng theo thời gian. Kết quả cho thấy lưu lượng của nhóm giao thức này nhìn chung duy trì ở mức thấp và dao động không lớn trong phần lớn thời gian quan sát. Tuy nhiên, tại một số thời điểm vẫn xuất hiện các đợt tăng nhẹ, phản ánh sự phát sinh tạm thời của các giao thức không phổ biến hoặc các loại lưu lượng không thuộc TCP, UDP và ICMP.

Thông qua Hình 18, có thể nhận thấy nhóm giao thức Other không đóng vai trò chính trong hoạt động truyền tải dữ liệu của hệ thống, nhưng việc theo dõi chúng vẫn cần thiết nhằm hỗ trợ người quản trị phát hiện các loại lưu lượng bất thường hoặc các giao thức phát sinh ngoài dự kiến trong quá trình vận hành mạng.



Hình 19: Biểu đồ thể hiện Tshark Packets

Hình 19 biểu thị tổng số gói tin được thu thập bởi TShark trong quá trình giám sát mạng theo thời gian. Kết quả cho thấy số lượng gói tin duy trì ở mức tương đối ổn định trong phần lớn thời gian quan sát, phản ánh trạng thái hoạt động bình thường của hệ thống mạng. Tuy nhiên, tại một số thời điểm xuất hiện các đinh tăng đột biến rõ rệt, cho thấy sự gia tăng tạm thời về lưu lượng gói tin trong hệ thống.

Thông qua Hình 19, có thể nhận thấy biểu đồ tổng số gói tin là cơ sở quan trọng giúp người quản trị đánh giá mức độ tải của mạng, đồng thời hỗ trợ phát hiện các thời điểm bất thường để phục vụ cho việc phân tích nguyên nhân và đánh giá hiệu năng mạng.



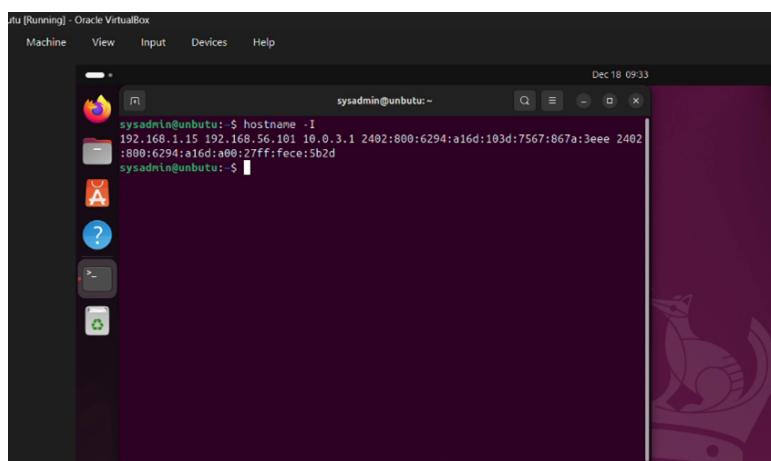
Hình 20: Biểu đồ thê hiện Tshark Bytes

Hình 20 biểu thị sự thay đổi tổng dung lượng dữ liệu (Bytes) được ghi nhận bởi TShark trong quá trình giám sát mạng theo thời gian. Kết quả cho thấy dung lượng dữ liệu truyền tải có xu hướng dao động liên tục, phản ánh sự biến thiên về khối lượng dữ liệu trao đổi trong hệ thống. Trong phần lớn thời gian quan sát, lưu lượng dữ liệu duy trì ở mức trung bình, tuy nhiên tại một số thời điểm xuất hiện các đỉnh tăng cao rõ rệt, cho thấy các phiên truyền dữ liệu có kích thước lớn diễn ra trong thời gian ngắn.

Thông qua Hình 20, có thể nhận thấy việc theo dõi tổng dung lượng dữ liệu giúp người quản trị đánh giá mức độ sử dụng băng thông của mạng, đồng thời hỗ trợ phát hiện các thời điểm lưu lượng bất thường để phục vụ cho việc phân tích, tối ưu và đảm bảo hiệu năng hệ thống mạng.

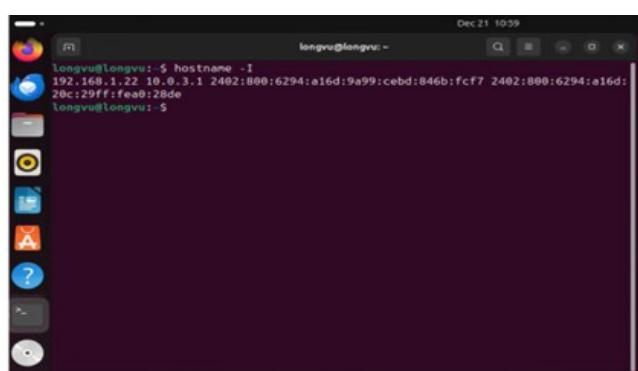
4.2 Chặn IP nguy hiểm

Trước tiên, để chắc chắn rằng IP của máy tấn công bị chặn thì ta phải xem IP của máy tấn công và máy Server.



Hình 21: IP của máy tấn công

Theo hình 21, IP của máy tấn công là 192.168.1.15 sẽ tiến hành tấn công đến Server có IP là 192.168.1.22 như Hình 22 bên dưới.



Hình 22: IP của máy server

Sau khi đã biết được IP của máy tấn công cũng như Server sẽ tiến hành chạy code giám sát để phát hiện tấn công trên Raspberry Pi.

```
pi@raspberrypi:~/anti_attack $ sudo python3 autoblock2.py
2025-12-18 16:33:10,642 - INFO - Giám sát SYN / ICMP / UDP flood trên bridge
```

Hình 23: Pi đang ở chế độ giám sát

Như Hình 23, thì sau khi thực thi code giám sát ta sẽ thấy một dòng log được in ra để thông báo rằng Pi đang ở chế độ giám sát và sẽ chặn tất cả các IP có hành vi đáng ngờ.

Tiếp đến, tiến hành tấn công với hai loại tấn công là SYN Flood và UDP Flood. Tiến hành tấn công SYN Flood trước, ngưỡng để phát hiện tấn công SYN Flood là gửi quá 20 SYN trong thời gian ngắn.

```
Dec 18 09:33
sysadmin@unbutu:~
```

Connexion	IP	Port	Flags	Sequence Number	Window Size	RTT
1	192.168.1.22	80	SA	17	64240	4.7
2	192.168.1.22	80	SA	18	64240	6.7
3	192.168.1.22	80	SA	19	64240	8.7
4	192.168.1.22	80	SA	20	64240	5.6
5	192.168.1.22	80	SA	21	64240	5.8
6	192.168.1.22	80	SA	22	64240	5.7
7	192.168.1.22	80	SA	23	64240	4.2
8	192.168.1.22	80	SA	24	64240	6.1
9	192.168.1.22	80	SA	25	64240	5.0
10	192.168.1.22	80	SA	26	64240	5.4
11	192.168.1.22	80	SA	27	64240	6.1

Hình 24: Log hiển thị trên máy tấn công

```
pi@raspberrypi:~/anti_attack $ sudo python3 autoblock2.py
2025-12-18 16:33:10,642 - INFO - Giám sát SYN / ICMP / UDP flood trên bridge
2025-12-18 16:33:50,649 - WARNING - BLOCK 192.168.1.15: SYN flood 28/60s
```

Hình 25: Log hiển thị trên Pi

Theo Hình 24 và Hình 25, với ngưỡng SYN là 20 request thì khi máy tấn công gửi quá 20 request thì trên Pi đã phát hiện bất thường và tiến hành chặn IP của máy tấn công vĩnh viễn. Nguưỡng là 20 nhưng code thực thi chặn phải mất một thời gian ngắn để thực thi nên sẽ bị chậm hơn và máy A sẽ gửi được nhiều hơn 20 gói rồi mới bị chặn nhưng chỉ trong thời gian ngắn nên không ảnh hưởng gì tới máy Server B.

```
sysadmin@unbutu:~$ sudo hping3 --udp --flood -p 1234 192.168.1.22
HPING 192.168.1.22 (enp0s3 192.168.1.22): udp mode set, 28 headers + 0 data byte
S
hping in flood mode, no replies will be shown
```

Hình 26: Log hiển thị trên máy tấn công (UDP Flood)

```
pi@raspberrypi:~/anti_attack $ sudo python3 autoblock2.py
2025-12-18 16:33:10,642 - INFO - Giám sát SYN / ICMP / UDP flood trên bridge
2025-12-18 16:33:50,649 - WARNING - BLOCK 192.168.1.15: SYN flood 28/60s
^Cpi@raspberrypi:~/anti_attack $ sudo iptables -t raw -L PREROUTING
Chain PREROUTING (policy ACCEPT)
target    prot opt source          destination
DROPOUT all  --  192.168.1.15      anywhere
pi@raspberrypi:~/anti_attack $ sudo iptables -t raw -F PREROUTING
pi@raspberrypi:~/anti_attack $ sudo python3 autoblock2.py
2025-12-18 16:35:14,624 - INFO - Giám sát SYN / ICMP / UDP flood trên bridge
2025-12-18 16:35:34,642 - WARNING - BLOCK 192.168.1.15: UDP flood 5000/60s
```

Hình 27: Log hiển thị trên Pi (UDP Flood)

Theo Hình 26 và Hình 27 thì khi máy tấn công gửi quá 5000 UDP packet tới Server thì Pi sẽ phát hiện và chặn IP đó.

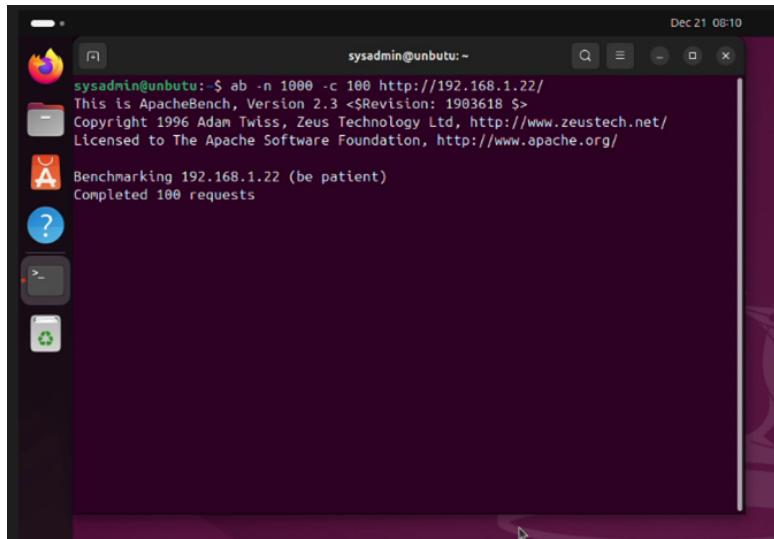
```
sysadmin@unbutu:~$ sudo ping -f 192.168.1.22
PING 192.168.1.22 (192.168.1.22) 56(84) bytes of data.
```

Hình 28: Log hiển thị trên máy tấn công (ICMP Flood)

```
pi@raspberrypi:~/anti_attack $ sudo python3 autoblock_test.py
2025-12-21 15:08:19,943 - INFO - Giám sát SYN / ICMP / UDP / HTTP flood trên bridge
2025-12-21 15:08:39,950 - WARNING - BLOCK 192.168.1.15: ICMP flood 1439/60s
```

Hình 29: Log hiển thị trên Pi (ICMP Flood)

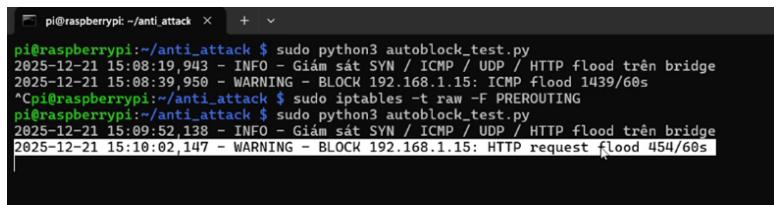
Hình 28 và Hình 29 là log của máy tấn công và Pi khi thực hiện tấn công ICMP Flood, khi lượng gói ICMP tới server vượt ngưỡng thì ngay lập tức chặn IP đó vĩnh viễn và máy tấn công không thể ping tới server được nữa.



```
sysadmin@unbutu:~$ ab -n 1000 -c 100 http://192.168.1.22/
This is ApacheBench, Version 2.3 <$Revision: 1903618 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/
Benchmarking 192.168.1.22 (be patient)
Completed 100 requests
```

Hình 30: Log hiển thị trên máy tấn công (HTTP Flood)

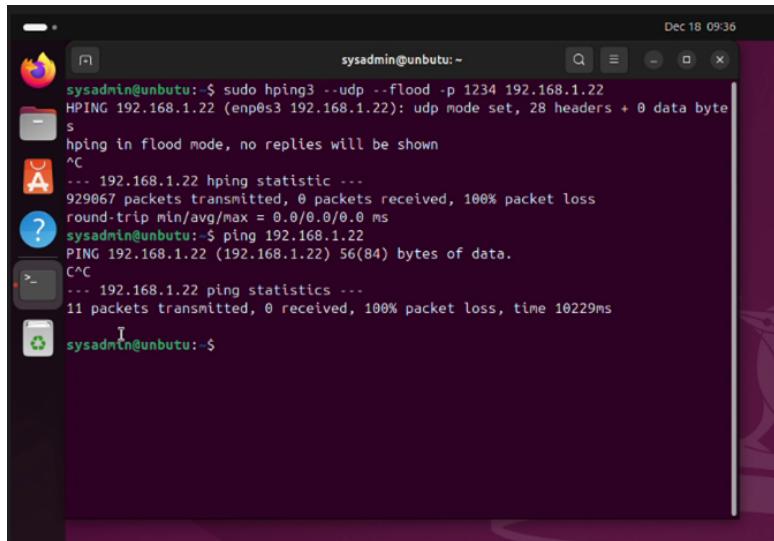
Hình 30, trên máy tấn công chạy lệnh gửi 1000 HTTP requests tới server với 1 lần gửi 100 requests.



```
pi@raspberrypi:~/anti_attack $ sudo python3 autoblock_test.py
2025-12-21 15:08:19,943 - INFO - Giám sát SYN / ICMP / UDP / HTTP flood trên bridge
2025-12-21 15:08:39,950 - WARNING - BLOCK 192.168.1.15: ICMP Flood 1439/60s
*pi@raspberrypi:~/anti_attack $ sudo iptables -t raw -F PREROUTING
pi@raspberrypi:~/anti_attack $ sudo python3 autoblock_test.py
2025-12-21 15:09:52,138 - INFO - Giám sát SYN / ICMP / UDP / HTTP flood trên bridge
2025-12-21 15:10:02,147 - WARNING - BLOCK 192.168.1.15: HTTP request flood 454/60s
```

Hình 31: Log hiển thị trên Pi (HTTP Flood)

Hình 31, IP của máy tấn công bị chặn khi gửi 454 HTTP requests, lượng requests này vượt ngưỡng cài đặt nên IP đã bị chặn.



```
sysadmin@unbutu:~$ sudo hping3 --udp --flood -p 1234 192.168.1.22
HPING 192.168.1.22 (enp0s3 192.168.1.22): udp mode set, 28 headers + 0 data byte
s
hping in flood mode, no replies will be shown
^C
--- 192.168.1.22 hping statistic ---
929067 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
sysadmin@unbutu:~$ ping 192.168.1.22
PING 192.168.1.22 (192.168.1.22) 56(84) bytes of data.
C^C
--- 192.168.1.22 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10229ms
sysadmin@unbutu:~$
```

Hình 32: Log trên máy tấn công khi đã bị chặn (HTTP Flood)

Theo hình 32, Sau khi IP của máy tấn công đã bị chặn, máy tấn công cố gắng ping tới địa chỉ của Server B thì kết quả trả về là đã gửi 11 gói ping đi nhưng Server không nhận được gói nào và Packet Loss là 100

Tiếp theo là thử nghiệm với tấn công DDoS, với máy C có IP là 192.168.1.4

```

sysadmin@unbutu:~$ sudo hping3 -S -p 80 --flood 192.168.1.22
HPING 192.168.1.22 (enp0s3 192.168.1.22): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.22 hping statistic ---
219052 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
sysadmin@unbutu:~$ sudo hping3 -S -p 80 --flood 192.168.1.22
HPING 192.168.1.22 (enp0s3 192.168.1.22): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

```

Hình 33: Log trên máy tấn công A và C khi chạy lệnh tấn công

```

pi@raspberrypi:~/anti_attack $ sudo python3 autoblock_DDoS.py
2025-12-22 16:23:52,759 - INFO - Giảm sát Dos/DDoS: SYN/ICMP/UDP/HTTP flood trên bridge
2025-12-22 16:23:52,768 - INFO - DDoS Detection: ENDED
2025-12-22 16:23:52,770 - CRITICAL - ALERT: DDoS SYN detected: 1895 packets from 4 IPs
2025-12-22 16:23:52,783 - WARNING - BLOCK 192.168.1.4: DDoS SYN detected: 1895 packets from 4 IPs - Contributor: 1000 packets
2025-12-22 16:23:52,795 - WARNING - BLOCK 192.168.1.15: DDoS SYN detected: 1895 packets from 4 IPs - Contributor: 566 packets
2025-12-22 16:23:52,802 - WARNING - DDoS Mode ACTIVE: Blocked 2 IPs permanently

```

Hình 34: Log trên Pi

Hình 33 và hình 34 cho thấy là IP của máy A và máy C đã bị chặn khi tấn công SYN Flood tới Server B và sau khi chặn thì máy A và máy C sẽ không ping tới được Server B như hình 35 và hình 36 bên dưới.

```

sysadmin@unbutu:~$ sudo hping3 -S -p 80 --flood 192.168.1.22
HPING 192.168.1.22 (enp0s3 192.168.1.22): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.22 hping statistic ---
219052 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
sysadmin@unbutu:~$ sudo hping3 -S -p 80 --flood 192.168.1.22
HPING 192.168.1.22 (enp0s3 192.168.1.22): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.22 hping statistic ---
846626 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
sysadmin@unbutu:~$ ping 192.168.1.22
PING 192.168.1.22 (192.168.1.22) 56(84) bytes of data.
^C
--- 192.168.1.22 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7492ms

```

Hình 35: Log trên máy tấn công A và C khi chạy lệnh tấn công

```

mojinn@Mojinn:~$ sudo hping3 -S -p 80 --flood 192.168.1.22
HPING 192.168.1.22 (wlpo20f3 192.168.1.22): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.22 hping statistic ---
284137 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
mojinn@Mojinn:~$ ping 192.168.1.22
PING 192.168.1.22 (192.168.1.22) 56(84) bytes of data.
^C
--- 192.168.1.22 ping statistics ---
13 packets transmitted, 0 received, 100% packet loss, time 12285ms

```

Hình 36: Log trên Pi

5 Kết luận

Dự án đã xây dựng được một hệ thống quản trị và giám sát mạng chạy trên nền tảng Raspberry Pi, cho phép thu thập, phân tích và hiển thị trực quan các thông số mạng như lưu lượng truyền tải, độ trễ, tần số mất gói. Hệ thống hoạt động dưới dạng cầu mảng, giúp Raspberry Pi quan sát toàn bộ lưu lượng đi qua, từ đó cung cấp dữ liệu chính xác và liên tục cho giao diện dashboard. Thông qua các mô-đun xử lý độc lập, dữ liệu được tổng hợp thành một nguồn duy nhất và thể hiện bằng các biểu đồ dạng vòng và biểu đồ thời gian, hỗ trợ người quản trị theo dõi trạng thái mạng một cách rõ ràng và dễ dàng.

Bên cạnh khả năng giám sát, dự án cũng triển khai mô phỏng hai kịch bản tấn công SYN Flood nhằm đánh giá khả năng phát hiện bất thường trong mạng. Raspberry Pi được đặt ở hai vị trí khác nhau để mô phỏng tấn công vào modem WiFi và tấn công vào máy chủ trong LAN. Kết quả cho thấy hệ thống có thể quan sát đúng hành vi tăng đột biến của lưu lượng SYN, đồng thời thực hiện chặn IP tấn công theo ngưỡng đã định. Các thí nghiệm chứng minh rằng Raspberry Pi có thể vừa giám sát, vừa hỗ trợ bảo vệ mạng ở quy mô nhỏ một cách hiệu quả.

Mặc dù đạt được các mục tiêu đặt ra, hệ thống vẫn tồn tại một số hạn chế, bao gồm khả năng xử lý còn phụ thuộc vào phần cứng của Raspberry Pi, thuật toán phát hiện tấn công còn đơn giản và dashboard chưa hỗ trợ nhiều chế độ tương tác nâng cao. Ngoài ra, hệ thống mới thử nghiệm chủ yếu với một dạng tấn công, nên phạm vi đánh giá về mặt an ninh mạng còn hạn chế.

Trong tương lai, nhóm có thể mở rộng hệ thống theo các hướng như tối ưu hóa hiệu năng, bổ sung thuật toán phát hiện nâng cao, hỗ trợ nhiều dạng tấn công khác nhau, và phát triển dashboard theo hướng thời gian thực hoàn chỉnh hơn. Các hướng cải tiến này sẽ giúp Raspberry Pi trở thành một nền tảng mạnh mẽ hơn, đáp ứng tốt nhu cầu giám sát lẫn bảo mật trong các mô hình mạng thực tế.

Tài Liệu Tham Khảo

- [1] J. Svoboda, I. Ghafir, and V. Prenosil, “Network monitoring approaches: An overview,” *Int. J. Adv. Comput. Netw. Secur.*, vol. 5, pp. 88–93, 2015.
- [2] K. A. Saeed, D. Wu, and D. J. Xu, “Effect of designer- versus user-driven network-monitoring dashboard design on user flow experience and performance,” *Information and Management*, vol. 61, no. 3, 2024.
- [3] R. Shikhaliev and L. Sukhostat, “Proactive computer network monitoring based on homogeneous deep neural ensemble,” *Results in Control and Optimization*, vol. 11, 2023.
- [4] L. L. Ramalho et al., “A SBC-based data acquisition system: A case study on smart reclosers and multiagent systems,” *IEEE Access*, vol. 11, pp. 48988–49001, 2023.
- [5] C.-D. Chiang et al., “Development of microcontroller-based status monitoring system for diagnosis and prognosis of smart factory,” in Proc. SICE Festival with Annual Conference (SICE FES), 2024.
- [6] M. Varol and M. İskefiyeli, “A low cost compact network TAP device with Raspberry Pi 4,” *Engineering Science and Technology, an International Journal*, vol. 70, no. 102118, 2025.

A Phụ lục

A.1 Các bước cấu hình cầu mảng (Bridge)

Bước 1: Kích hoạt các dịch vụ mạng cần thiết

```
sudo systemctl enable systemd-networkd
sudo systemctl enable systemd-resolved
sudo systemctl start systemd-networkd
sudo systemctl start systemd-resolved
```

Bước 2: Tạo thư mục cấu hình mạng

```
sudo mkdir -p /etc/systemd/network
```

Bước 3: Tạo thiết bị bridge

```
sudo nano /etc/systemd/network/bridge0.netdev
```

Nội dung file bridge0.netdev:

```
[NetDev]
Name=bridge0
Kind=bridge
```

Bước 4: Cấu hình địa chỉ mạng cho bridge

```
sudo nano /etc/systemd/network/bridge0.network
```

Nội dung file bridge0.network:

```
[Match]
Name=bridge0

[Network]
Address=192.168.1.10/24
Gateway=192.168.1.1
DNS=8.8.8.8
```

Bước 5: Gán giao diện eth0 vào bridge

```
sudo nano /etc/systemd/network/eth0.network
```

Nội dung file eth0.network:

```
[Match]
Name=eth0

[Network]
Bridge=bridge0
```

Bước 6: Gán giao diện eth1 vào bridge

```
sudo nano /etc/systemd/network/eth1.network
```

Nội dung file eth1.network:

```
[Match]
Name=eth1

[Network]
Bridge=bridge0
```

Bước 7: Khởi động lại dịch vụ và kiểm tra

```
sudo systemctl restart systemd-networkd
ip addr show bridge0
sudo reboot
ssh pi@192.168.1.10
```

A.2 Source code

Toàn bộ mã nguồn được nhóm xây dựng bằng Python và Bash, phục vụ cho việc giám sát lưu lượng, phát hiện bất thường và chặn IP nguy hiểm, được trình bày chi tiết trong các link github sau:

https://github.com/Mojinnn/Network_Monitor_Using_RaspberryPi