

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG



BÁO CÁO ĐỒ ÁN
Môn: ĐÁNH GIÁ HIỆU NĂNG MẠNG MÁY TÍNH

**Đề tài: Tìm hiểu và đánh giá hiệu năng mạng
với công cụ PRTG**

Giảng viên hướng dẫn : PGS.TS. LÊ TRUNG QUÂN
Lớp : NT531.P11.MMCL

Nhóm thực hiện – Nhóm 12

- | | |
|-------------------|----------------|
| 1. Bùi Thanh Bình | MSSV: 20521113 |
| 2. Hồ Hải Dương | MSSV: 21520202 |

THỦ ĐỨC – 2024

MỤC LỤC NỘI DUNG

A. LỜI MỞ ĐẦU	1
1. BỐI CẢNH CHỌN ĐỀ TÀI.....	1
1.1. Tổng quan	1
1.2. Mục tiêu đồ án.....	1
2. BẢNG PHÂN CHIA CÔNG VIỆC.....	2
B. NỘI DUNG CHÍNH	3
1. CƠ SỞ LÝ THUYẾT	3
1.1. Hiệu năng mạng	3
1.1.1. Tổng quan về hiệu năng mạng.....	3
1.1.2. Các giao thức và công nghệ liên quan	4
1.2. Giao thức SNMP	5
1.2.1. Tổng quan về SNMP.....	5
1.2.2. Các thành phần chính của SNMP	6
1.2.3. Cách thức hoạt động của SNMP	6
1.2.4. Ưu điểm của SNMP	7
1.2.5. Ứng dụng của SNMP trong quản lý mạng.....	7
2. CÔNG CỤ PRTG	8
2.1. Tổng quan	8
2.2. Các tính năng chính của PRTG	8
2.3. Cơ chế hoạt động của PRTG	9
2.3.1. Cơ chế hoạt động	9
2.3.2. Kiến trúc của PRTG.....	10
2.4. Ưu và nhược điểm của PRTG	11
2.5. Ứng dụng của PRTG trong giám sát hiệu năng mạng.....	11
3. QUY TRÌNH THỰC HIỆN.....	12
4. CÁC HÌNH ẢNH DEMO QUAN TRỌNG	14
5. TỔNG KẾT ĐỒ ÁN.....	21
5.1. Kết luận	21
5.2. Định hướng trong tương lai.....	21
LỜI CẢM ƠN.....	22
NGUỒN THAM KHẢO.....	23

A. LỜI MỞ ĐẦU

1. BỐI CẢNH CHỌN ĐỀ TÀI

1.1. Tổng quan

Trong thời đại số hóa, hệ thống mạng ngày càng trở nên quan trọng, đóng vai trò thiết yếu trong mọi hoạt động của các tổ chức, từ việc quản lý dữ liệu, cung cấp dịch vụ trực tuyến đến hỗ trợ giao tiếp và hợp tác toàn cầu. Sự phụ thuộc vào mạng lưới thông tin không chỉ giúp các doanh nghiệp nâng cao năng suất mà còn tạo điều kiện để phát triển những ứng dụng mới, tối ưu hóa quy trình kinh doanh. đối diện với những thách thức lớn hơn bao giờ hết.

Vì thế đòi hỏi các tổ chức phải có phương pháp giám sát và đánh giá hiệu năng mạng một cách chính xác và hiệu quả. Quá trình này không chỉ giúp đảm bảo sự ổn định của mạng mà còn giúp tối ưu hóa các nguồn lực, giảm thiểu sự cố và nâng cao trải nghiệm người dùng. Việc theo dõi hiệu năng mạng cho phép phát hiện sớm các vấn đề, từ đó có các biện pháp khắc phục kịp thời trước khi chúng ảnh hưởng đến hoạt động của tổ chức.

PRTG là một công cụ mạnh mẽ hỗ trợ việc giám sát hiệu năng mạng thông qua các thông số quan trọng như băng thông và lưu lượng dữ liệu. Với giao diện trực quan và khả năng cấu hình linh hoạt, PRTG giúp người dùng dễ dàng theo dõi và quản lý hệ thống mạng, từ đó đưa ra các giải pháp tối ưu hóa hiệu suất một cách hiệu quả.

1.2. Mục tiêu đồ án

Mục tiêu chính của đồ án là giám sát và thu thập các thông tin quan trọng liên quan đến hoạt động của các clients trong hệ thống mạng, chẳng hạn như ping, băng thông, độ trễ, dung lượng của hệ thống và các thông số liên quan khác. Thông qua việc sử dụng công cụ PRTG, đồ án hướng đến khả năng theo dõi liên tục trạng thái kết nối, giúp phát hiện sớm các vấn đề tiềm ẩn có thể ảnh hưởng đến hiệu suất mạng. Việc giám sát này không chỉ hỗ trợ việc đánh giá hiệu năng mạng mà còn góp phần vào việc đảm bảo sự ổn định và tối ưu hóa hoạt động của hệ thống.

Bên cạnh đó, một mục tiêu quan trọng khác là tìm hiểu và nắm vững các giao thức mạng liên quan, điển hình là giao thức SNMP (Simple Network Management Protocol). SNMP đóng vai trò quan trọng trong việc quản lý và giám sát các thiết bị mạng, cho phép truy xuất và điều khiển các thông số kỹ thuật của thiết bị một cách hiệu quả. Việc hiểu rõ các nguyên lý hoạt động và cách thức áp dụng giao thức này giúp nhóm xây dựng được hệ thống giám sát mạnh mẽ và linh hoạt hơn.

2. BẢNG PHÂN CHIA CÔNG VIỆC

STT	Tên	MSSV	Công việc	Hoàn thành
1	Bùi Thanh Bình	20521113	Thực hiện cài đặt và giám sát với PRTG, viết báo cáo, làm powerpoint, thuyết trình.	100%
2	Hồ Hải Dương	21520202	Thực hiện cài đặt và giám sát với PRTG, viết báo cáo, làm powerpoint, thuyết trình.	100%

B. NỘI DUNG CHÍNH

1. CƠ SỞ LÝ THUYẾT

1.1. Hiệu năng mạng

1.1.1. Tổng quan về hiệu năng mạng

Hiệu năng mạng là một chỉ số quan trọng để đo lường chất lượng và khả năng hoạt động của một hệ thống mạng. Hiệu năng mạng bao gồm nhiều yếu tố khác nhau như băng thông, độ trễ, thông lượng, và độ ổn định của các thiết bị và kết nối. Để đảm bảo rằng hệ thống mạng hoạt động hiệu quả, cần phải đánh giá các yếu tố này một cách toàn diện.

- **Băng thông** (Bandwidth): Đây là khối lượng dữ liệu có thể được truyền tải qua mạng trong một khoảng thời gian nhất định. Băng thông cao hơn thường biểu thị khả năng truyền dữ liệu tốt hơn và hiệu suất cao hơn. Tuy nhiên, băng thông lớn không phải lúc nào cũng đảm bảo tốc độ truyền nhanh nếu có nhiều yếu tố khác tác động tiêu cực đến mạng.
- **Độ trễ** (Latency): Độ trễ là thời gian cần để một gói tin đi từ nguồn đến đích. Độ trễ thấp là điều kiện cần thiết để đảm bảo hiệu quả hoạt động của các ứng dụng thời gian thực như video call hay trò chơi trực tuyến. Độ trễ cao có thể gây ra hiện tượng trễ (lag) và làm giảm chất lượng dịch vụ.
- **Thông lượng** (Throughput): Thông lượng là lượng dữ liệu thực tế mà hệ thống mạng có thể xử lý trong một khoảng thời gian. Thông lượng càng cao, khả năng truyền dữ liệu càng hiệu quả. Điều này thường liên quan chặt chẽ đến băng thông nhưng cũng chịu ảnh hưởng của độ trễ và các yếu tố khác như mức độ lỗi trên mạng.
- **Độ trễ mạng** (Jitter): Đây là sự thay đổi về độ trễ của các gói tin khi di chuyển qua mạng. Độ trễ mạng cao có thể dẫn đến tình trạng không đồng bộ, đặc biệt là trong các dịch vụ truyền thông thời gian thực.

Hiệu năng mạng không chỉ đơn thuần là đảm bảo tốc độ và dung lượng dữ liệu lớn mà còn phải đảm bảo tính ổn định, giảm thiểu sự cố và tối ưu hóa trải nghiệm người dùng. Việc đánh giá hiệu năng mạng một cách chính xác giúp xác định các vấn đề tiềm ẩn và điều chỉnh hệ thống để cải thiện hiệu suất.

1.1.2. Các giao thức và công nghệ liên quan

Một yếu tố quan trọng trong việc đánh giá hiệu năng mạng là sử dụng các giao thức mạng để thu thập thông tin về trạng thái và hoạt động của các thiết bị trong hệ thống. Một trong những giao thức phổ biến nhất là SNMP (Simple Network Management Protocol).

SNMP hoạt động dựa trên kiến trúc **client-server**, trong đó quản trị viên mạng (SNMP Manager) sẽ gửi yêu cầu đến các thiết bị mạng (SNMP Agent) để thu thập dữ liệu. Các thiết bị sẽ phản hồi thông tin trạng thái và hoạt động của chúng về cho quản trị viên. SNMP sử dụng các Object Identifier (OID) để xác định các thuộc tính của thiết bị, giúp quản trị viên có thể truy xuất thông tin một cách chính xác.

Ngoài SNMP, còn có nhiều công nghệ và giao thức khác hỗ trợ trong việc giám sát và đánh giá hiệu năng mạng, bao gồm:

- **ICMP (Internet Control Message Protocol)**: Thường được sử dụng để gửi các thông điệp báo cáo lỗi khi không thể truyền các gói tin thành công. ICMP còn được dùng để thực hiện các phép đo thời gian phản hồi qua lệnh **ping**.
- **NetFlow**: Một giao thức được phát triển bởi Cisco, cho phép giám sát lưu lượng mạng và cung cấp thông tin chi tiết về các dòng dữ liệu di chuyển qua router và switch.
- **sFlow**: Một giải pháp giám sát lưu lượng mạng sử dụng phương pháp lấy mẫu dữ liệu để đánh giá hiệu suất mạng mà không tiêu tốn nhiều tài nguyên hệ thống.

Việc hiểu rõ các giao thức này và cách chúng hoạt động là nền tảng quan trọng để áp dụng chúng vào hệ thống giám sát hiệu năng mạng, giúp cải thiện hiệu suất và bảo mật.

Bảng so sánh giữa SNMP, ICMP, NetFlow và sFlow

Tiêu chí	SNMP	ICMP	NetFlow	sFlow
Loại giao thức	Giao thức quản lý mạng	Giao thức điều khiển truyền tải	Giao thức giám sát lưu lượng mạng	Giao thức giám sát lưu lượng mạng
Chức năng chính	Thu thập thông tin quản lý từ các thiết bị mạng (CPU, RAM, băng thông, trạng	Kiểm tra kết nối mạng và báo cáo lỗi qua thông điệp phản hồi (ví dụ: ping)	Thu thập thông tin về các luồng dữ liệu qua mạng	Lấy mẫu lưu lượng mạng để giám sát và phân tích hiệu năng

	thái thiết bị, v.v.)			
Giao thức truyền thông	UDP (cổng 161 cho SNMP, cổng 162 cho Trap)	UDP (ping, echo request/reply)	UDP	UDP
Độ chính xác của dữ liệu	Thu thập dữ liệu chi tiết theo từng đối tượng (OID)	Kiểm tra trạng thái kết nối đơn giản (thời gian phản hồi, trạng thái sống của thiết bị)	Chi tiết về luồng dữ liệu, bao gồm nguồn, đích, loại dịch vụ, v.v.	Lấy mẫu thống kê, không ghi nhận toàn bộ lưu lượng
Ứng dụng chính	Giám sát hiệu năng thiết bị mạng, quản lý thiết bị từ xa	Kiểm tra kết nối mạng, độ trễ và tình trạng kết nối	Phân tích luồng dữ liệu để đánh giá băng thông và các mẫu lưu lượng	Phân tích hiệu năng mạng dựa trên mẫu lưu lượng ngẫu nhiên
Ưu điểm	- Quản lý toàn diện thiết bị mạng - Phản hồi sự kiện nhanh (Trap)	- Đơn giản, dễ sử dụng - Hữu ích cho việc kiểm tra kết nối mạng cơ bản	- Phân tích luồng chi tiết - Hữu ích cho quản lý băng thông và bảo mật mạng	- Lấy mẫu ít tài nguyên - Phù hợp cho mạng lớn
Nhược điểm	- Không mã hóa (trừ SNMPv3) - Giới hạn về bảo mật	- Chỉ kiểm tra kết nối mạng cơ bản - Không giám sát lưu lượng	- Tốn tài nguyên nếu thu thập dữ liệu liên tục - Cần thiết bị hỗ trợ	- Lấy mẫu, không cung cấp dữ liệu toàn bộ - Không chi tiết bằng NetFlow
Phiên bản phổ biến	SNMPv1, SNMPv2c, SNMPv3	ICMPv4, ICMPv6	NetFlow v5, v9	sFlow v5

Bảng 1

1.2. Giao thức SNMP

1.2.1. Tổng quan về SNMP

SNMP (Simple Network Management Protocol) là một giao thức mạng tiêu chuẩn được sử dụng để giám sát, quản lý và kiểm soát các thiết bị trong hệ thống mạng, bao gồm router, switch, máy chủ, và các thiết bị khác. SNMP cho phép các quản trị viên mạng thu thập thông tin về trạng thái hoạt động của các thiết bị này, phát hiện lỗi,

theo dõi hiệu năng và thực hiện các hành động quản lý từ xa. SNMP là một phần quan trọng trong các giải pháp quản lý mạng hiện nay, nhờ vào khả năng truy xuất và điều khiển thiết bị một cách hiệu quả mà không yêu cầu truy cập trực tiếp.

1.2.2. Các thành phần chính của SNMP

SNMP hoạt động dựa trên mô hình quản lý mạng gồm ba thành phần chính:

- **SNMP Manager (Quản trị viên SNMP):** Đây là thành phần chịu trách nhiệm gửi các yêu cầu đến các thiết bị trong mạng và nhận các phản hồi từ chúng. SNMP Manager thường là một máy chủ quản lý hoặc một phần mềm giám sát mạng như PRTG, Nagios, hoặc Zabbix. Quản trị viên mạng sẽ sử dụng SNMP Manager để thu thập thông tin về trạng thái hoạt động và cấu hình của các thiết bị được quản lý.
- **SNMP Agent (Thiết bị SNMP):** SNMP Agent là phần mềm được cài đặt trên các thiết bị mạng (router, switch, máy chủ) để thu thập thông tin về trạng thái và hoạt động của thiết bị. Các thông tin này bao gồm dữ liệu về CPU, bộ nhớ, băng thông, lưu lượng mạng và nhiều chỉ số khác. SNMP Agent phản hồi lại yêu cầu từ SNMP Manager và gửi dữ liệu qua giao thức SNMP.
- **MIB (Management Information Base - Cơ sở thông tin quản lý):** MIB là một cơ sở dữ liệu chứa các đối tượng mà SNMP Agent có thể giám sát hoặc điều khiển. Mỗi đối tượng trong MIB được xác định bởi một Object Identifier (OID), và các OID này đại diện cho các thuộc tính như trạng thái CPU, lưu lượng dữ liệu qua giao diện mạng, hoặc số lượng gói tin đã truyền.

1.2.3. Cách thức hoạt động của SNMP

SNMP sử dụng một tập hợp các thông điệp để truyền thông tin giữa SNMP Manager và SNMP Agent. Các thông điệp phổ biến bao gồm:

- **GetRequest:** SNMP Manager sử dụng GetRequest để yêu cầu SNMP Agent cung cấp giá trị của một hoặc nhiều đối tượng (OID) trong MIB.
- **SetRequest:** SNMP Manager sử dụng SetRequest để điều chỉnh hoặc cấu hình các tham số của thiết bị qua SNMP Agent.
- **Trap:** SNMP Agent có thể gửi thông điệp Trap không mong đợi đến SNMP Manager khi phát hiện một sự kiện hoặc lỗi đặc biệt trên thiết bị.
- **InformRequest:** Đây là phiên bản nâng cao của Trap, cung cấp cơ chế xác nhận thông điệp từ phía SNMP Manager.

- **GetNextRequest và GetBulkRequest:** Dùng để yêu cầu dữ liệu liên tục từ SNMP Agent, đặc biệt hữu ích khi có nhiều dữ liệu cần giám sát.

Giao tiếp giữa SNMP Manager và SNMP Agent sử dụng giao thức **UDP** (User Datagram Protocol), cụ thể là các cổng 161 (cho truyền thông SNMP) và 162 (cho các thông điệp Trap). SNMP có thể hoạt động ở nhiều phiên bản, trong đó phổ biến nhất là **SNMPv1**, **SNMPv2c** và **SNMPv3**. SNMPv3 được sử dụng rộng rãi nhờ tính năng bảo mật mạnh mẽ với khả năng xác thực và mã hóa thông tin.

1.2.4. Ưu điểm của SNMP

Tính mở rộng: SNMP có thể dễ dàng mở rộng để giám sát nhiều thiết bị và mạng lưới khác nhau mà không làm tăng độ phức tạp.

Tương thích: SNMP tương thích với hầu hết các thiết bị mạng và có thể được sử dụng với nhiều hệ điều hành khác nhau.

Tự động hóa: Giao thức hỗ trợ các cơ chế tự động phát hiện và phản hồi sự cố, giúp tăng cường tính hiệu quả trong quản lý mạng.

Phân tích chi tiết: SNMP cung cấp khả năng phân tích chi tiết các thông số thiết bị, cho phép quản trị viên có cái nhìn toàn diện về hiệu năng và trạng thái của hệ thống mạng.

1.2.5. Ứng dụng của SNMP trong quản lý mạng

SNMP được sử dụng rộng rãi trong các công cụ giám sát mạng như PRTG, Zabbix, Nagios, và SolarWinds để thu thập dữ liệu hiệu suất từ các thiết bị mạng. Thông qua các OID trong MIB, quản trị viên có thể giám sát nhiều khía cạnh của hiệu suất hệ thống, từ việc đo lường băng thông, độ trễ mạng đến giám sát trạng thái hoạt động của CPU, bộ nhớ và các ứng dụng.

SNMP cũng hỗ trợ trong việc quản lý sự cố mạng nhờ vào khả năng gửi thông điệp Trap khi có lỗi hoặc sự cố, từ đó giúp quản trị viên phản ứng nhanh chóng để giảm thiểu thời gian ngừng hoạt động và tối ưu hóa hiệu suất mạng.

2. CÔNG CỤ PRTG

2.1. Tổng quan



Hình 1 – Logo của PRTG

PRTG Network Monitor là một công cụ giám sát mạng được phát triển bởi Paessler AG, với mục tiêu cung cấp giải pháp giám sát hiệu năng mạng toàn diện và dễ sử dụng. PRTG hỗ trợ giám sát tất cả các thành phần trong hệ thống mạng, bao gồm router, switch, máy chủ, ứng dụng, và các dịch vụ đám mây. Công cụ này cung cấp một giao diện trực quan cho phép người dùng theo dõi các thông số mạng như băng thông, thời gian phản hồi, lưu lượng, và trạng thái thiết bị.

PRTG được thiết kế theo mô hình "tất cả trong một", với hàng nghìn cảm biến (sensor) có sẵn để giám sát nhiều loại thiết bị và dịch vụ khác nhau mà không cần cài đặt thêm các plugin hay công cụ phụ trợ. Một "sensor" trong PRTG là một đơn vị giám sát nhỏ, mỗi sensor theo dõi một thông số mạng cụ thể, chẳng hạn như trạng thái của cổng trên switch hoặc mức sử dụng CPU của một máy chủ.

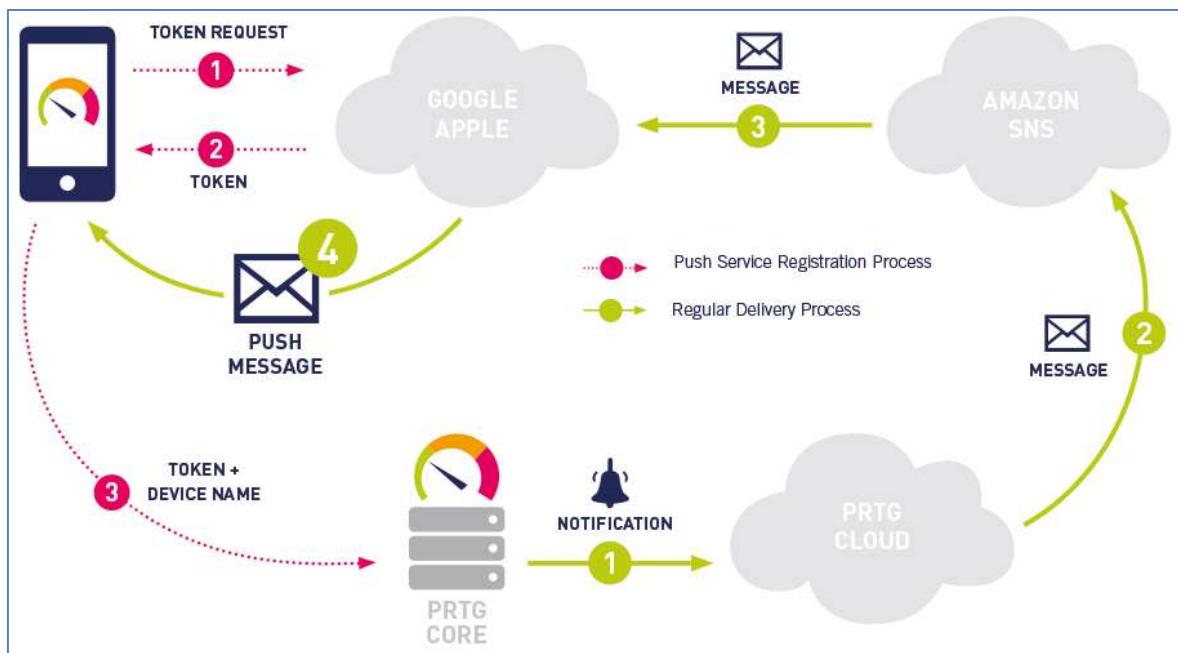
2.2. Các tính năng chính của PRTG

PRTG cung cấp một loạt các tính năng mạnh mẽ để giám sát và quản lý hiệu năng mạng, bao gồm:

- Giám sát băng thông:** PRTG giúp theo dõi lưu lượng dữ liệu qua các cổng mạng và thiết bị, cho phép quản trị viên nắm bắt được thông tin về băng thông sử dụng thực tế so với băng thông khả dụng. Công cụ hỗ trợ các giao thức giám sát băng thông như SNMP, NetFlow, sFlow, và IPFIX.
- Kiểm tra thời gian phản hồi (Ping):** Công cụ sử dụng các sensor để đo lường thời gian phản hồi giữa các thiết bị mạng, từ đó giúp xác định hiệu suất của các kết nối.
- Giám sát máy chủ và ứng dụng:** Ngoài giám sát phần cứng mạng, PRTG cũng cung cấp khả năng theo dõi hoạt động của các máy chủ và ứng dụng, bao

gồm giám sát trạng thái hoạt động, tải CPU, dung lượng bộ nhớ và tình trạng ổ đĩa.

- **Cảnh báo và thông báo:** PRTG tích hợp hệ thống cảnh báo khi phát hiện sự cố hoặc hiệu suất bất thường. Người dùng có thể nhận thông báo qua email, tin nhắn SMS, hoặc thông qua ứng dụng di động của PRTG. Các cảnh báo có thể được tùy chỉnh dựa trên ngưỡng hiệu suất do người dùng đặt ra.
- **Giao diện người dùng trực quan:** Giao diện web và ứng dụng di động của PRTG rất dễ sử dụng, cho phép quản trị viên dễ dàng theo dõi trạng thái mạng thông qua biểu đồ, báo cáo và các bảng điều khiển tùy chỉnh.
- **Báo cáo và phân tích dữ liệu:** PRTG cho phép người dùng xuất báo cáo chi tiết về hiệu năng mạng, bao gồm lịch sử sử dụng băng thông, độ trễ và lưu lượng dữ liệu. Các báo cáo có thể được tạo tự động hoặc theo yêu cầu, cung cấp thông tin cần thiết để tối ưu hóa hệ thống mạng.



Hình 2 – Mô hình cách hoạt động cảnh báo và thông tin của PRTG

2.3. Cơ chế hoạt động của PRTG

2.3.1. Cơ chế hoạt động

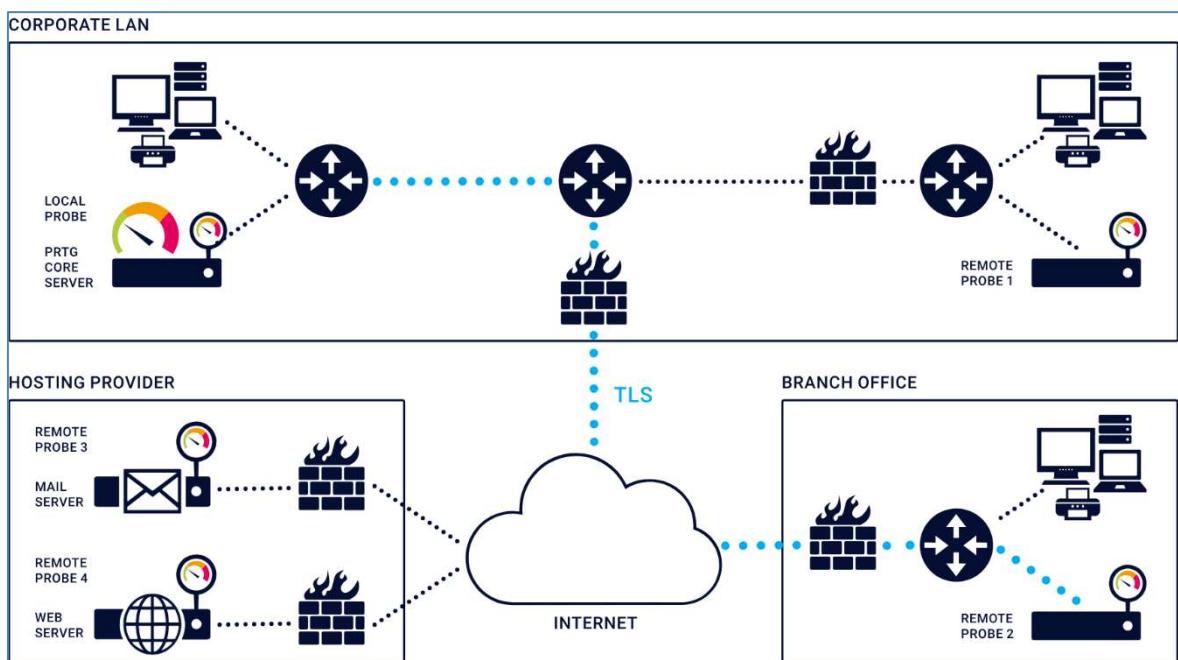
PRTG sử dụng một kiến trúc phân cấp với các cảm biến (sensors) làm đơn vị giám sát cơ bản. Mỗi sensor giám sát một thông số cụ thể trên một thiết bị mạng. PRTG có thể triển khai tại chỗ (on-premise) hoặc trên đám mây, tùy thuộc vào yêu cầu của người dùng.

Công cụ này hỗ trợ nhiều phương pháp giám sát khác nhau, bao gồm SNMP, ICMP, NetFlow, sFlow, WMI (Windows Management Instrumentation), và các giao thức HTTP, SMTP, FTP. Điều này cho phép PRTG tích hợp với hầu hết các thiết bị và dịch vụ mạng hiện nay.

2.3.2. Kiến trúc của PRTG

Có thể phân loại các thành phần của PRTG thành ba loại chính: các bộ phận hệ thống, giao diện người dùng và các công cụ quản trị hệ thống cơ bản (system parts, user interfaces, and basic system administration tools). Kiến trúc bao gồm hai phần chính đó là: PRTG Core Server và PRTG Probe. Trong đó:

- **Core Server** bao gồm quá trình lưu trữ dữ liệu, web server, các báo cáo và hệ thống lưu trữ. Còn Probe thi hành quá trình giám sát, nó nhận các cấu hình từ Core Server và thực thi quá trình xử lý sau đó báo kết quả về cho Core Server.
- **Một Core Server có thể quản lý không giới hạn các Probe** để tăng khả năng giám sát. Network Monitor hỗ trợ việc kiểm tra các mạng lên đến 30.000 sensor và có thể báo cáo về tình hình các kết nối có hội tụ SLA hay không. Hai phần Core và Probe là hai dịch vụ trong Windows chúng chạy bởi hệ điều hành Windows, không yêu cầu login vào user.



Hình 3 – Mô hình cách giám sát cơ bản của một hệ thống PRTG

2.4. Ưu và nhược điểm của PRTG

Bảng liệt kê ưu và nhược điểm của PRTG				
Ưu điểm	PRTG không yêu cầu các kỹ năng kỹ thuật chuyên sâu để cài đặt và sử dụng, nhờ vào giao diện người dùng đơn giản và hàng nghìn cảm biến cài sẵn.	Công cụ hỗ trợ nhiều giao thức và công nghệ giám sát khác nhau, phù hợp với các hệ thống mạng phức tạp và đa dạng.	PRTG cung cấp một giải pháp tất cả trong một, giúp quản trị viên theo dõi hiệu suất mạng, máy chủ, và các dịch vụ khác từ một giao diện duy nhất.	Hệ thống cảnh báo tự động và báo cáo chi tiết giúp quản trị viên nhanh chóng phát hiện và giải quyết sự cố.
Nhược điểm	Mặc dù PRTG có phiên bản miễn phí với giới hạn 100 cảm biến, nhưng phiên bản trả phí có thể khá đắt đỏ đối với các tổ chức có quy mô lớn và cần giám sát nhiều thiết bị.		PRTG có thể tiêu tốn nhiều tài nguyên phần cứng khi giám sát nhiều cảm biến và thiết bị cùng lúc, đặc biệt là khi triển khai trong các hệ thống mạng lớn.	

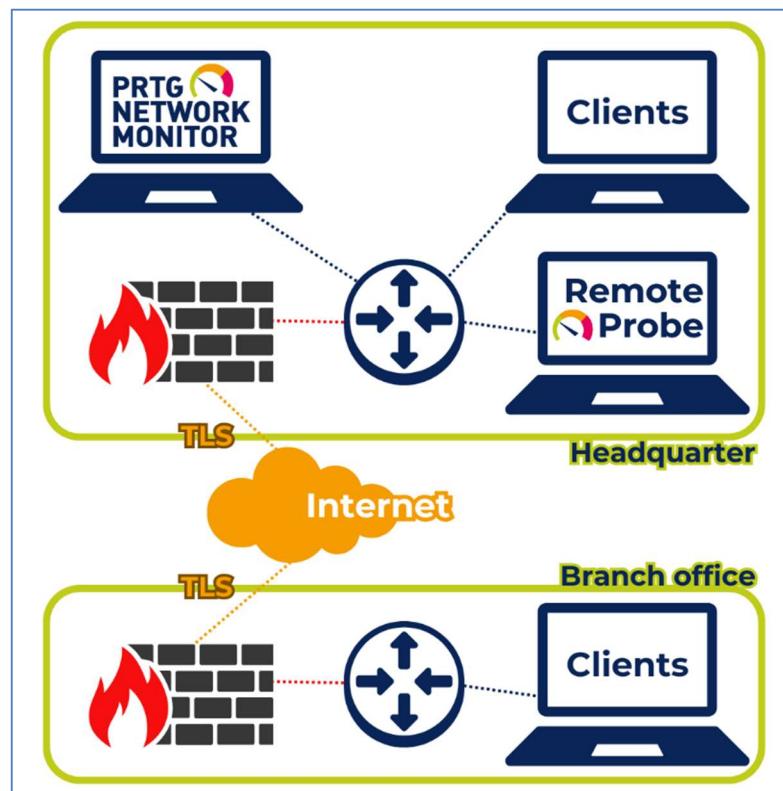
Bảng 2

2.5. Ứng dụng của PRTG trong giám sát hiệu năng mạng

PRTG được sử dụng rộng rãi trong việc giám sát hiệu năng mạng tại các doanh nghiệp, trường học, và các tổ chức lớn nhỏ. Nhờ khả năng giám sát chi tiết và hỗ trợ nhiều loại cảm biến, công cụ này giúp đảm bảo hệ thống mạng luôn hoạt động ổn định và hiệu quả. Quản trị viên có thể sử dụng PRTG để phát hiện sớm các sự cố, từ đó có các biện pháp xử lý kịp thời, giảm thiểu thời gian ngừng hoạt động của hệ thống và tối ưu hóa hiệu suất.

3. QUY TRÌNH THỰC HIỆN

Giả sử kịch bản nhóm có 1 công ty có 1 trụ sở chính và 1 văn phòng chi nhánh, thiết kế hệ thống giám sát với công cụ PRTG như sau:



Hình 4 – Mô hình giám sát của nhóm 12 thực hiện

Trụ sở chính (Headquarter):

- ❖ **PRTG Network Monitor:** Được cài đặt trên một máy chủ tại văn phòng chính, PRTG Core Server có nhiệm vụ giám sát hiệu năng của các thiết bị trong hệ thống mạng. PRTG sử dụng nhiều giao thức và cổng khác nhau để giám sát, bao gồm:
 - **Cổng 161/162 (UDP):** Sử dụng để thu thập dữ liệu qua giao thức SNMP từ các thiết bị như router, switch, và máy chủ.
 - **Cổng 443 (HTTPS):** PRTG sử dụng cổng này để cho phép người quản trị truy cập vào giao diện web an toàn của PRTG thông qua giao thức HTTPS.
 - **Cổng 80 (HTTP):** Được sử dụng trong trường hợp quản trị viên truy cập vào PRTG qua giao thức HTTP, tuy nhiên, việc sử dụng HTTPS được khuyến khích để đảm bảo tính bảo mật.

- **Cổng 8080 (TCP):** Dùng để giao tiếp giữa PRTG Core Server và **Remote Probe** thông qua giao thức mã hóa **TLS**.
- ❖ **Remote Probe:** Được đặt tại văn phòng chính và chịu trách nhiệm thu thập dữ liệu từ các thiết bị ở khu vực gần Core Server. Remote Probe sử dụng cổng **8080 (TCP)** để giao tiếp với PRTG Core Server thông qua mạng nội bộ.
- ❖ **Clients:** Các thiết bị client tại văn phòng chính được giám sát bằng các cảm biến (sensors) thông qua các giao thức như **SNMP**, **Ping (ICMP)**, và **WMI**. Để thu thập dữ liệu này, PRTG sử dụng các cổng 161/162 (SNMP) và cổng ICMP (ping).
- ❖ **Firewall và Router:** Bức tường lửa và router tại văn phòng chính quản lý các luồng dữ liệu đi và đến, bảo vệ hệ thống khỏi các cuộc tấn công từ bên ngoài. Các kết nối từ văn phòng chính đến chi nhánh được mã hóa qua **TLS** và sử dụng cổng **8080** cho giao tiếp an toàn.

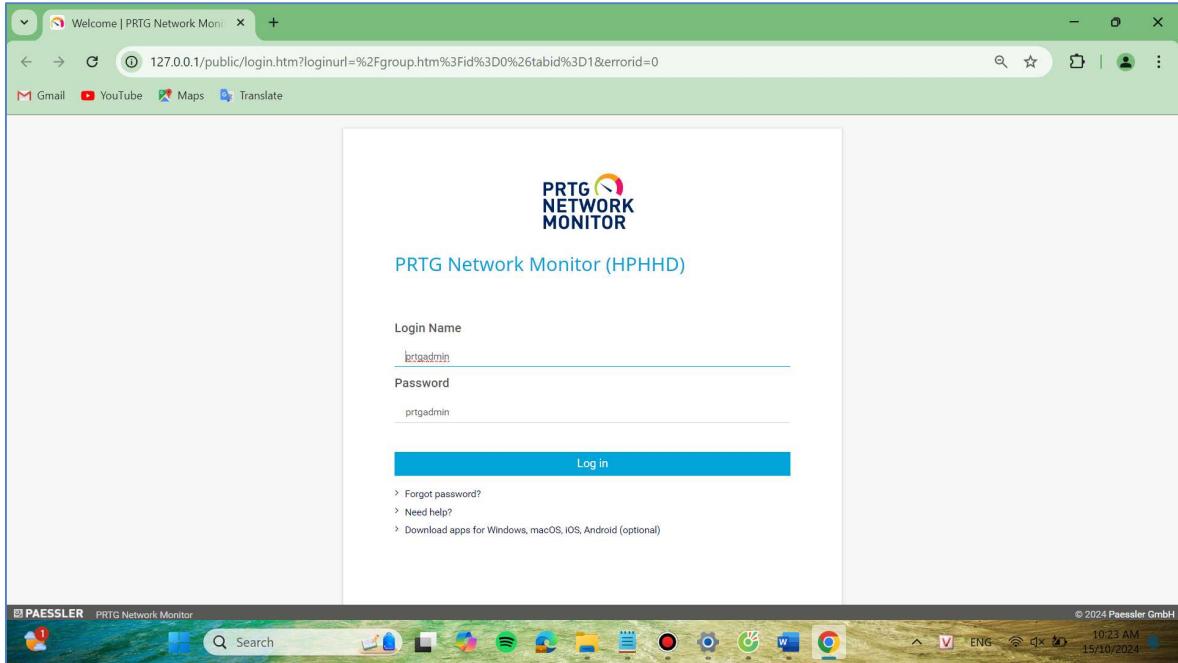
Chi nhánh (Branch office):

- ❖ **Clients:** Các thiết bị client tại chi nhánh được giám sát từ xa bởi PRTG Core Server thông qua kết nối qua Internet. Dữ liệu giám sát, bao gồm **ping (ICMP)**, **SNMP** và các thông số khác, được truyền tải qua Internet với cổng **443 (HTTPS)** được mã hóa.
- ❖ **Firewall và Router:** Chi nhánh có hệ thống tường lửa và router riêng để bảo vệ mạng nội bộ. Kết nối với văn phòng chính diễn ra qua Internet với dữ liệu được mã hóa bằng **TLS** qua cổng **8080 (TCP)**, đảm bảo an toàn trong quá trình trao đổi dữ liệu giữa hai văn phòng.

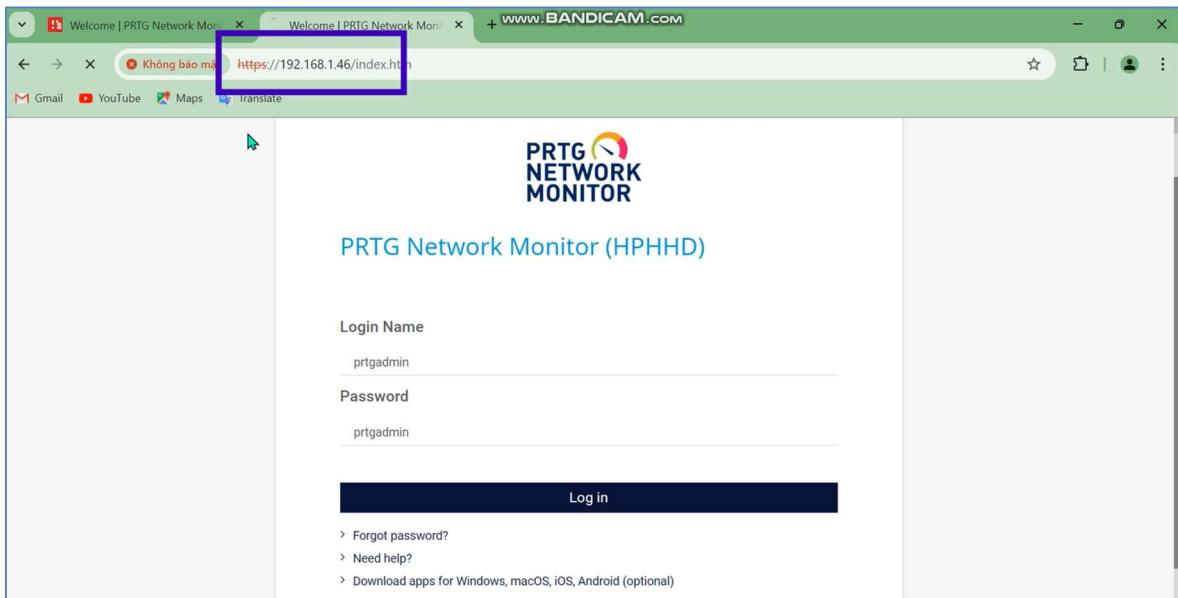
Kết nối Internet:

- ❖ Văn phòng chính và chi nhánh kết nối với nhau qua Internet, và dữ liệu giữa chúng được mã hóa bằng **TLS** để đảm bảo an ninh. Kết nối này sử dụng **cổng 8080 (TCP)** cho việc truyền tải dữ liệu an toàn giữa PRTG Core Server và các thiết bị tại chi nhánh.
- ❖ PRTG giám sát các thiết bị tại chi nhánh thông qua các cổng tiêu chuẩn như **443 (HTTPS)** cho giao diện quản trị, **161/162 (SNMP)** cho thu thập dữ liệu từ các thiết bị và **ICMP** cho kiểm tra ping.

4. CÁC HÌNH ẢNH DEMO QUAN TRỌNG



Hình 5 – Giao diện đăng nhập đầu tiên sau khi cài đặt hoàn tất, với địa chỉ local host là 127.0.0.1



Hình 6 – Switch to SSL, đăng nhập thành công giao diện admin với địa chỉ ip của máy server

System > Optional features

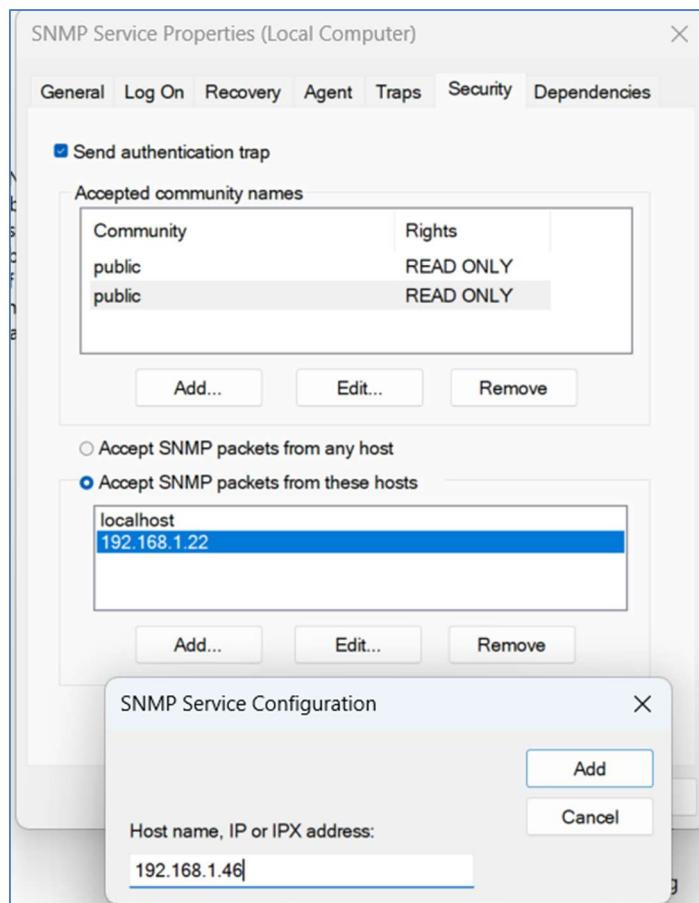
Add an optional feature View features

Optional features history See history

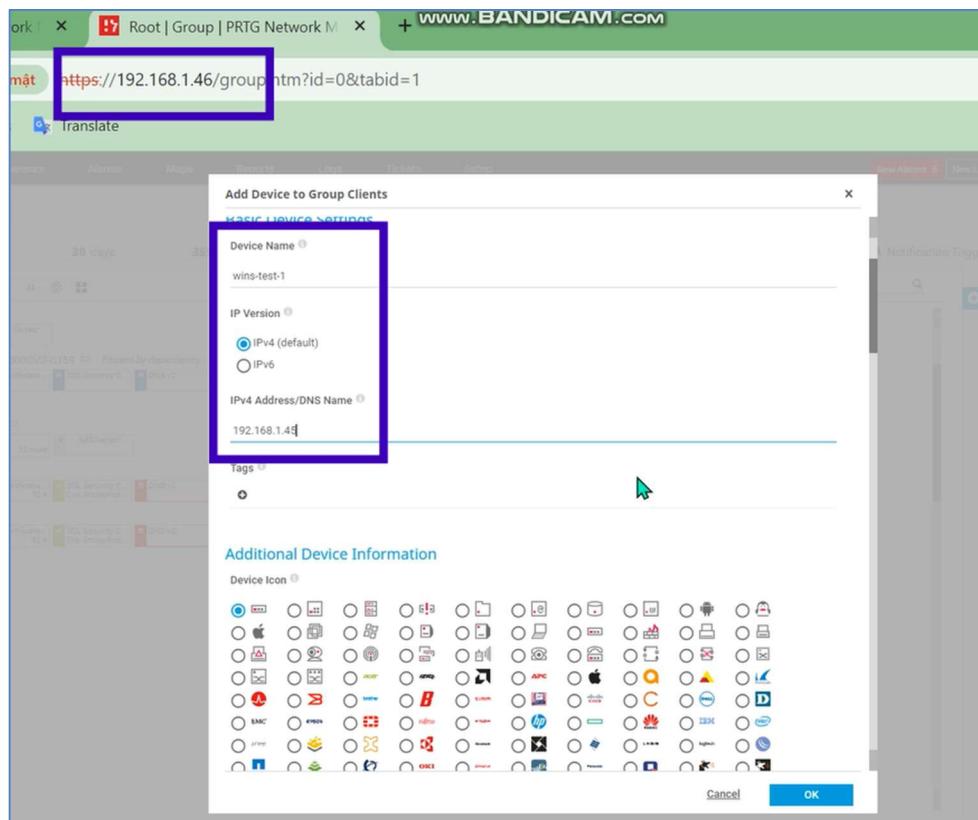
Recent actions

Simple Network Management Protocol (SNMP) Added

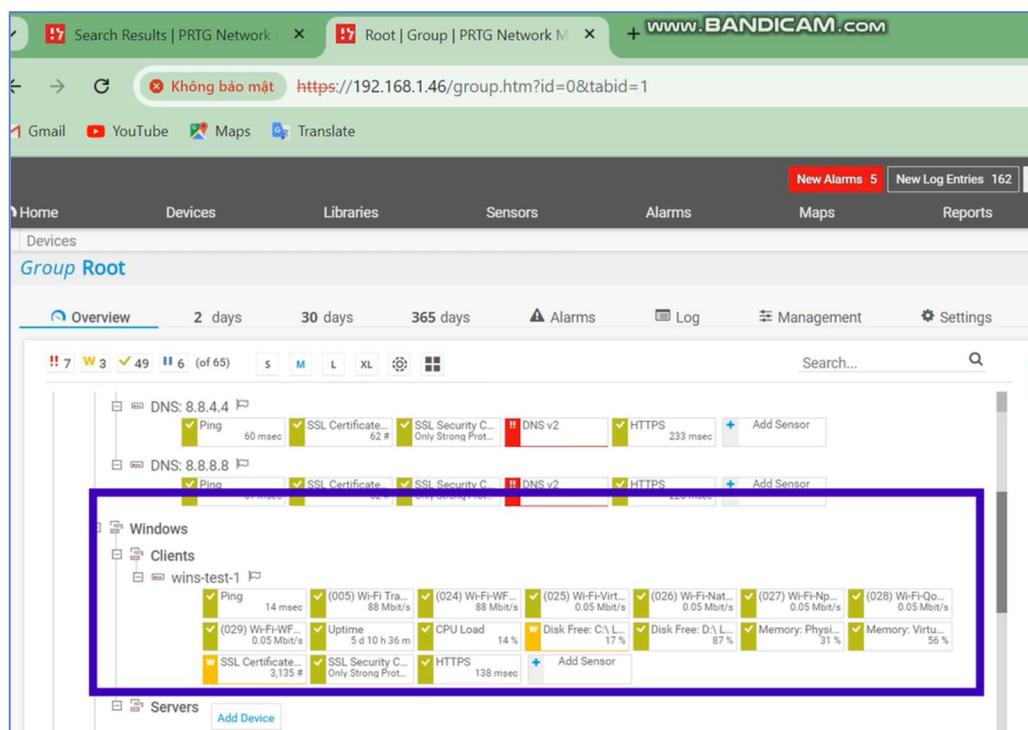
Hình 7 – Cài đặt thêm giao thức SNMP trên client cần giám sát



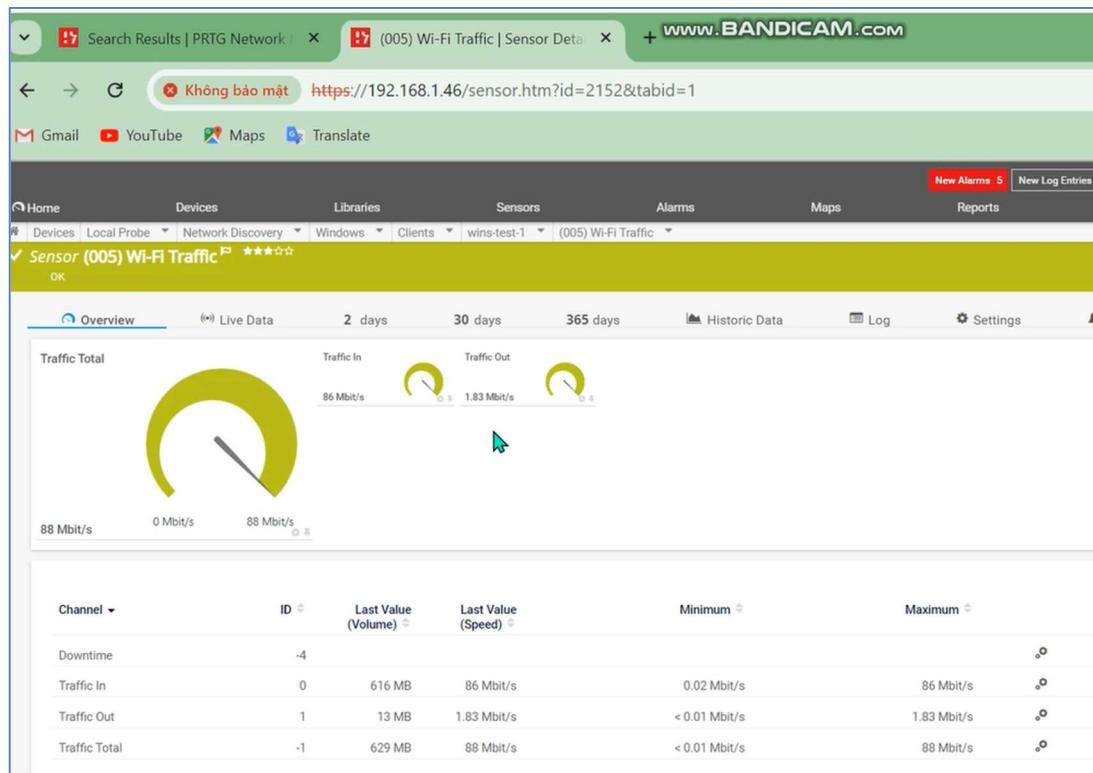
Hình 8 – Cài đặt trên Windows client để có thể kết nối đến PRTG server (trong cùng mạng LAN)



Hình 9 – Thêm thông tin của Windows client trên PRTG server để có thể giám sát



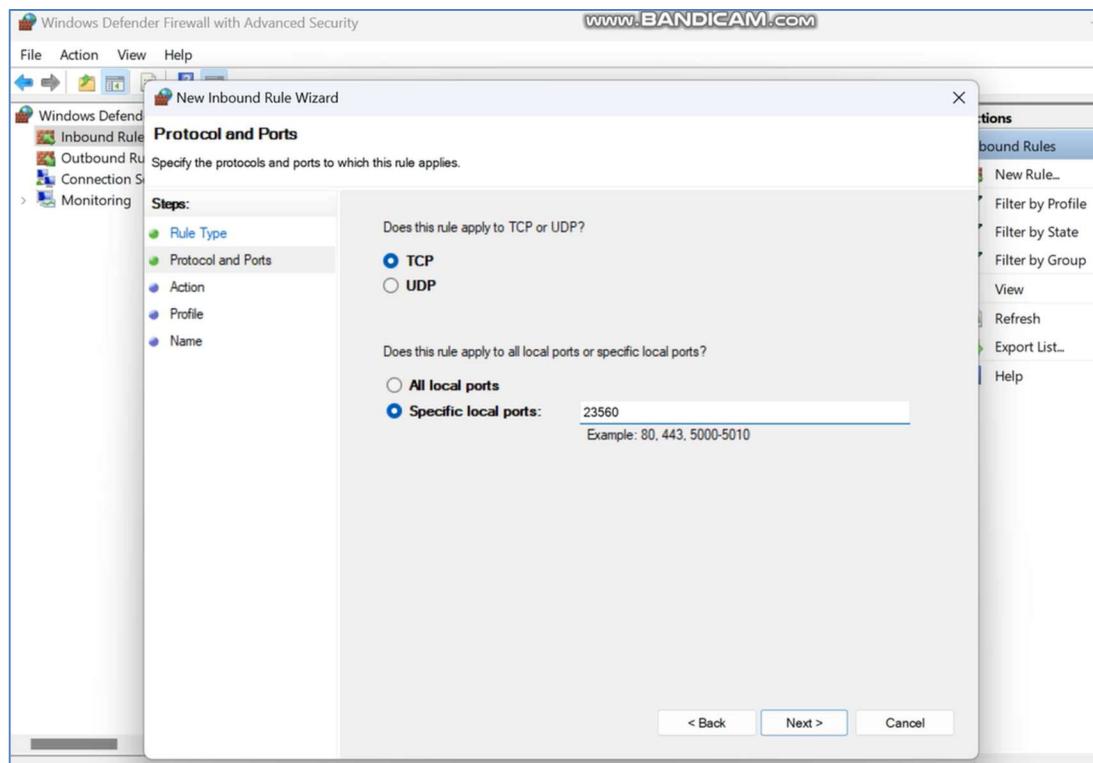
Hình 10 – PRTG server đã kết nối thành công với Windows client để giám sát các thông tin cần thiết bằng cách ẩn vào những sensor đã hiển thị màu xanh



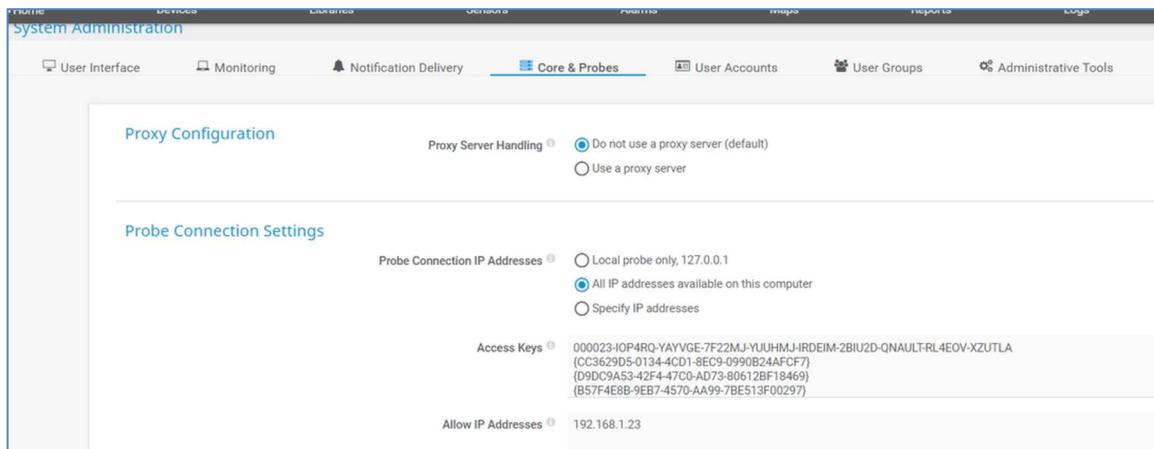
Hình 11 – Ví dụ về xem các thông tin về Wi-Fi traffic của Windows client



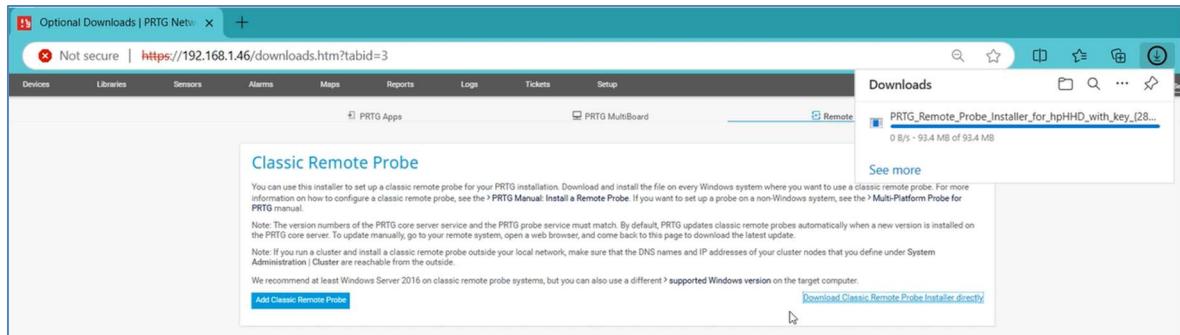
Hình 12 – Chuyển sang xem đồ thị phân tích theo từng thời gian



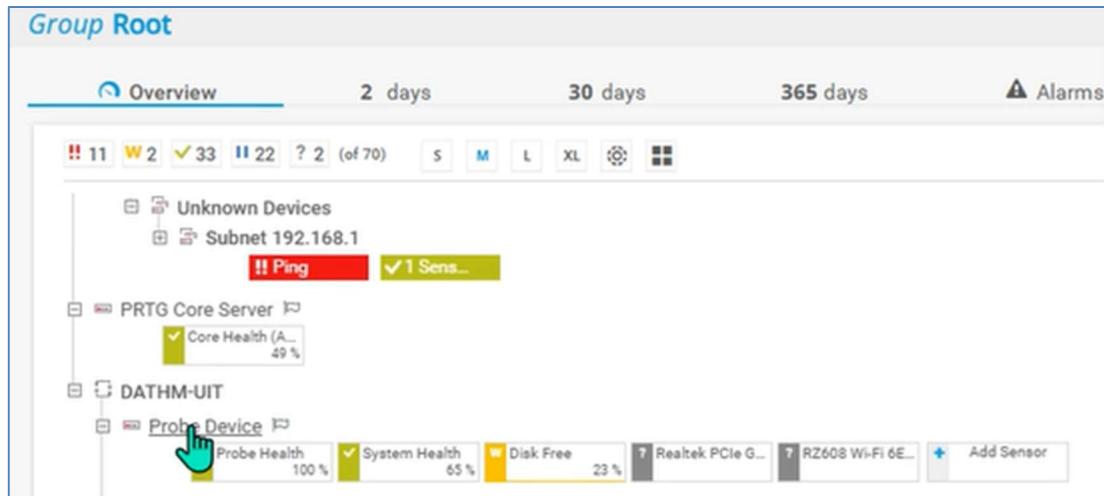
Hình 13 – Cài đặt cấu hình tường lửa và cổng trước khi thiết lập Remote Probe Server



Hình 14 – Cấu hình thông số tại PRTG server trước khi cài đặt Remote Probe cho client khác



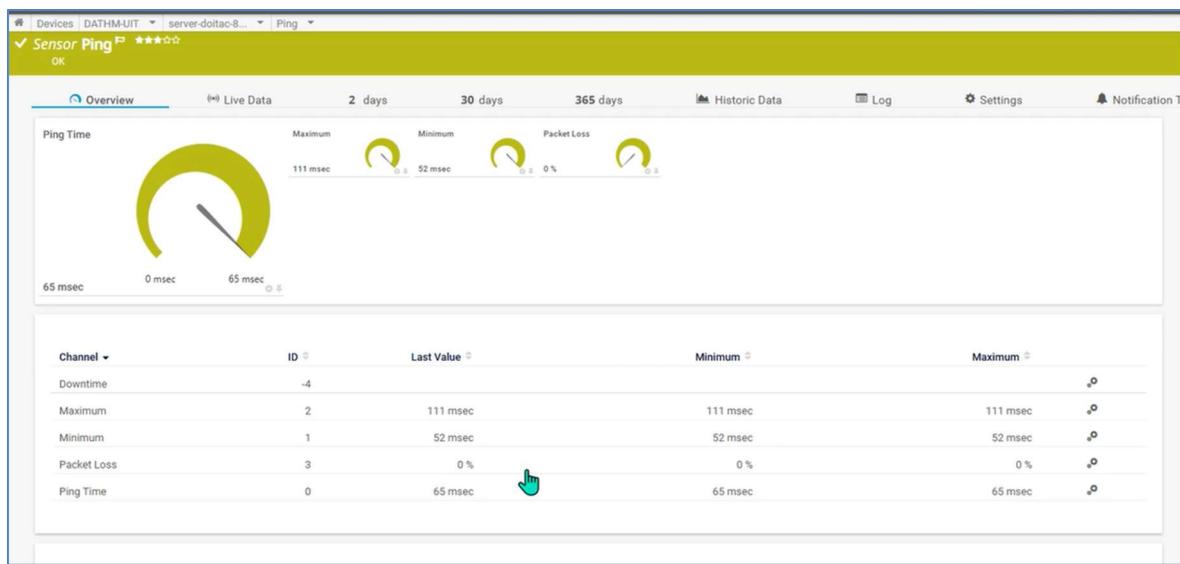
Hình 15 – Tại client khác (trong cùng LAN với PRTG server) tiến hành cài đặt Remote Probe server



Hình 16 – Kết nối thành công để giám sát client ngoài LAN với server

The screenshot shows the 'Add Sensor to Device' configuration dialog. It's 'Step 2 of 2' for adding a sensor to the device 'server-dotdac-6.8.8.8 [8.8.8.8]'. The 'Basic Sensor Settings' section is filled with values: Sensor Name 'Ping', Parent Tags 'pingsensor', and Priority '★★★'. The 'Ping Settings' section includes 'Timeout (Sec.)' set to 5, 'Packet Size (Bytes)' set to 32, 'Ping Method' set to 'Send multiple ping requests (default)', 'Ping Count' set to 5, and 'Ping Delay (ms)' set to 5. The 'Acknowledge Automatically' option is checked with 'Show down status on error (default)'. On the right side, there are sections for 'Active Background Tasks', 'Set a Secure Password', and a note about the trial license expiring in 15 days.

Hình 17 – Thêm một sensor bất kỳ cho client để giám sát



Hình 18 – Thêm sensor thành công và có thể xem các thông tin cần thiết

5. TỔNG KẾT ĐỒ ÁN

5.1. Kết luận

Qua quá trình thực hiện đồ án “Tìm hiểu và đánh giá hiệu năng mạng với công cụ PRTG”, nhóm đã đạt được những kết quả đáng khích lệ trong việc cài đặt và giám sát hiệu năng mạng. Cụ thể, nhóm đã thành công trong việc cấu hình và triển khai các sensor giám sát trên client Windows trong cùng mạng LAN với core server PRTG, giúp giám sát các thông số quan trọng như ping, độ trễ, băng thông,... Đồng thời, nhóm cũng thiết lập thành công Remote Probe để giám sát các chỉ số của máy chủ bên ngoài mạng LAN, điển hình là địa chỉ 8.8.8.8, đảm bảo tính toàn diện trong quá trình giám sát.

Thành công của đồ án không chỉ khẳng định hiệu quả và tính khả thi của việc sử dụng PRTG trong đánh giá hiệu năng mạng mà còn giúp nhóm có cơ hội tiếp cận và làm chủ các giao thức quan trọng như SNMP và ICMP. Qua đó, đồ án đã giúp nhóm không chỉ hiểu sâu hơn về nguyên lý hoạt động của các công cụ giám sát mà còn có khả năng áp dụng vào các hệ thống mạng phức tạp hơn trong tương lai.

5.2. Định hướng trong tương lai

Đồ án có thể được mở rộng để giám sát các hệ thống mạng phức tạp hơn, bao gồm nhiều client và nhiều loại thiết bị khác nhau. Bên cạnh việc tập trung vào các chỉ số cơ bản nhóm có thể tích hợp thêm các thông số khác. Điều này sẽ giúp xây dựng một mô hình giám sát toàn diện hơn, đáp ứng được các yêu cầu khắt khe hơn trong việc quản lý hệ thống mạng hiện đại. Ngoài ra, việc nghiên cứu thêm về các giao thức quản lý mạng khác ngoài SNMP cũng có thể giúp nâng cao hiệu suất giám sát và mở rộng khả năng quản trị hệ thống.

LỜI CẢM ƠN

Nhóm 12 xin gửi lời cảm ơn chân thành đến Khoa Mạng Máy tính và Truyền thông – Trường Đại học Công nghệ Thông tin vì đã thiết kế và đưa môn Đánh giá hiệu năng mạng máy tính vào chương trình giảng dạy. Môn học không chỉ giúp chúng em hiểu rõ về các mô hình đánh giá hiệu năng mạng, đặc trưng của các kiểu kiến trúc mạng, mà còn cung cấp các khái niệm và phương pháp đo lường hiệu năng mạng. Bên cạnh đó, các công cụ được sử dụng trong đánh giá hiệu năng cũng được giới thiệu một cách chi tiết.

Cụ thể hơn, môn học đã trang bị cho chúng em những kỹ thuật mô hình hóa dựa trên phân tích, giúp dự đoán hiệu suất của các hệ thống mạng và máy tính, cũng như xác nhận các tiêu chí thiết kế. Chúng em cũng được tìm hiểu về các kỹ thuật mô hình hóa hiệu suất, quá trình ngẫu nhiên, lý thuyết hàng đợi và các phương pháp giải cho những mô hình phân tích hiệu suất – những kiến thức nền tảng quan trọng trong lĩnh vực này.

Đặc biệt, nhóm xin bày tỏ lòng biết ơn sâu sắc tới thầy Lê Trung Quân, người đã nhiệt tình giảng dạy và truyền đạt những kiến thức quý báu trong suốt thời gian học tập. Thầy cũng đã tận tâm hướng dẫn và đồng hành cùng nhóm trong quá trình triển khai ý tưởng và thực hiện dự án, giúp nhóm hoàn thành đồ án này.

Chúng em nhận thức rằng kiến thức là vô tận, trong khi khả năng tiếp thu của mỗi người là giới hạn. Mặc dù đã cố gắng tìm tòi, nghiên cứu và hoàn thiện đồ án một cách cẩn thận, nhưng chắc chắn không thể tránh khỏi những thiếu sót. Rất mong nhận được những góp ý từ thầy để nhóm có thể cải thiện và tiến bộ hơn trong tương lai.

Cuối cùng, nhóm 12 xin kính chúc thầy sức khỏe, hạnh phúc và nhiều thành công trong sự nghiệp giảng dạy.

Trân trọng,
Nhóm 12.

NGUỒN THAM KHẢO

Sách:

1. Stallings, W. (2014). *Foundations of modern networking: SDN, NFV, QoE, IoT, and cloud*. Pearson.
2. Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer networks* (5th ed.). Pearson.
3. Subramanian, M. (2012). *Network management: Principles and practice*. Pearson.

Nguồn trực tuyến:

4. Paessler AG. (2023). *PRTG Network Monitor*. Retrieved October 7, 2024, from <https://www.paessler.com/prtg>
5. Cisco Systems, Inc. (2023). *Cisco NetFlow*. Retrieved October 7, 2024, from <https://www.cisco.com>
6. Pacisoft. (n.d.). *Kiến trúc PRTG Network Monitor*. Retrieved October 7, 2024, from <https://www.pacisoft.vn/tin-san-pham/prtg-la-gi/>
7. PRTG Tutorials. (n.d.). *PRTG Network Monitor Tutorials* [Video series]. YouTube. Retrieved October 7, 2024, from <https://www.youtube.com/@PRTGtutorials/videos>

HẾT./.