**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 học: ĐÁNH GIÁ HIỆU NĂNG HỆ THỐNG MẠNG MÁY TÍNH**

**Lớp: NT531.P11.MMCL**

**Đề tài**

**Triển khai hệ thống giám sát mạng sử dụng công cụ Observium**

GVHD: **PGS. TS. Lê Trung Quân**

Nhóm: **11**

Thành viên:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Hồ Mạnh Đạt | 21520695 | [21520695@gm.uit.edu.vn](mailto:21520695@gm.uit.edu.vn) |
| 2 | Trần Ngọc Phương Anh | 21521839 | [21521839@gm.uit.edu.vn](mailto:21521839@gm.uit.edu.vn) |

**□□ Tp. Hồ Chí Minh, 10/2024 □□**

# LỜI MỞ ĐẦU

Trong thời đại công nghệ thông tin phát triển mạnh mẽ, việc quản lý và giám sát hệ thống mạng trở thành một yếu tố then chốt để đảm bảo hoạt động ổn định và hiệu quả của các tổ chức, doanh nghiệp. Sự phụ thuộc vào hệ thống mạng ngày càng tăng đòi hỏi các nhà quản trị mạng phải có các công cụ giám sát mạnh mẽ để phát hiện sớm các sự cố, tối ưu hoá hiệu suất và duy trì tính sẵn sàng cao của hệ thống.

Trong bối cảnh đó, việc triển khai một hệ thống giám sát mạng hiệu quả là nhu cầu thiết yếu, nhằm hỗ trợ quản trị viên theo dõi liên tục các hoạt động của mạng, từ việc kiểm tra hiệu suất của các thiết bị như router, switch, đến quản lý lưu lượng và băng thông. Một trong những công cụ giám sát mạng phổ biến và mạnh mẽ hiện nay là **Observium**. Observium cung cấp giao diện trực quan, hỗ trợ nhiều loại thiết bị, cùng khả năng thu thập và phân tích dữ liệu chi tiết về hiệu suất của hệ thống mạng thông qua giao thức SNMP.

Đồ án "Triển khai hệ thống giám sát mạng sử dụng công cụ Observium" nhằm mục đích nghiên cứu, cài đặt và đánh giá hiệu quả của hệ thống giám sát này. Qua đó, cung cấp cái nhìn thực tiễn về khả năng giám sát toàn diện của Observium, giúp tối ưu hóa hiệu suất và tăng cường khả năng quản lý mạng một cách chủ động. Hy vọng rằng kết quả của đồ án sẽ góp phần mang lại giải pháp hữu ích trong việc quản lý hệ thống mạng cho các doanh nghiệp và tổ chức.

Báo cáo đồ án gồm 5 chương:

* Chương 1: Tổng quan về giám sát hiệu năng mạng
* Chương 2: Cơ bản về giao thức SNMP (Simple Network Management Protocol)
* Chương 3: Phát triển hệ thống giám sát mạng với Observium
* Chương 4: Triển khai thực nghiệm và kết quả
* Chương 5: Kết luận và hướng phát triển

**MỤC LỤC**

[LỜI MỞ ĐẦU 2](#_Toc179818418)

[PHÂN CÔNG CÔNG VIỆC TRONG NHÓM 4](#_Toc179818419)

[CHƯƠNG 1: TỔNG QUAN về giám sát hiệu năng mạng 5](#_Toc179818420)

[CHƯƠNG 2: CƠ bản về giao thức snmp (simple network management protocol) 9](#_Toc179818423)

[CHƯƠNG 3: PHÁT TRIỂN HỆ THỐNG GIÁM SÁT MẠNG VỚI OBSERVIUM 12](#_Toc179818432)

[CHƯƠNG 4: TRIỂN KHAI THỰC NGHIỆM VÀ KẾT QUẢ 16](#_Toc179818438)

[CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 16](#_Toc179818451)

[TÀI LIỆU THAM KHẢO 17](#_Toc179818462)

# PHÂN CÔNG CÔNG VIỆC TRONG NHÓM

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Họ và tên | MSSV | Phân công công việc | Hoàn thành |
| 1 | Hồ Mạnh Đạt | 21520695 | * Tìm hiểu kiến thức * Demo * Soạn slide, báo cáo | 100% |
| 2 | Trần Ngọc Phương Anh | 21521839 | * Tìm hiểu kiến thức * Demo * Soạn slide, báo cáo | 100% |

# 

# CHƯƠNG 1: TỔNG QUAN VỀ GIÁM SÁT HIỆU NĂNG MẠNG

Giám sát mạng là quá trình theo dõi và kiểm soát hiệu suất, tính sẵn sàng, và bảo mật của các thiết bị và kết nối mạng để đảm bảo rằng hệ thống mạng hoạt động ổn định, hiệu quả và không bị gián đoạn. Giám sát mạng thu thập các thông tin trên các thành phần của hệ thống, phân tích các thông tin, dấu hiệu nhằm đánh giá và đưa ra các cảnh báo cho người quản trị hệ thống.

## Mục đích của giám sát mạng

* Phát hiện sớm sự cố: Giám sát mạng giúp phát hiện nhanh chóng các sự cố như mất kết nối, thiết bị quá tải hoặc lỗi hệ thống.
* Tối ưu hóa hiệu suất: Qua việc giám sát lưu lượng, băng thông, CPU, bộ nhớ, giúp quản trị viên tối ưu hoá tài nguyên mạng.
* Đảm bảo tính sẵn sàng: Bằng cách liên tục theo dõi trạng thái hoạt động của mạng, giám sát giúp đảm bảo rằng các dịch vụ mạng luôn sẵn sàng.
* Bảo mật: Theo dõi các hành vi bất thường có thể chỉ ra dấu hiệu tấn công hoặc vi phạm an ninh mạng.

## Các thành phần chính của giám sát mạng

* Thiết bị được giám sát (Managed Devices): Bao gồm các router, switch, máy chủ, thiết bị lưu trữ, và thậm chí là các endpoint như PC, laptop.
* Phần mềm giám sát: Là các công cụ quản trị mạng (Network Management Systems - NMS) như Observium, Nagios, Zabbix, Cacti, SolarWinds. Những công cụ này thu thập dữ liệu từ các thiết bị mạng và cung cấp báo cáo chi tiết.
* Giao thức SNMP (Simple Network Management Protocol): Đây là một giao thức phổ biến được sử dụng để thu thập thông tin từ các thiết bị mạng.
* Trạm quản lý (Network Monitoring Station): Đây là nơi mà quản trị viên có thể theo dõi, phân tích, và quản lý hiệu suất hệ thống mạng.
  1. **Quá trình giám sát mạng**
* Thu thập dữ liệu: Các công cụ giám sát sẽ định kỳ lấy thông tin từ các thiết bị mạng (như CPU, bộ nhớ, lưu lượng) thông qua các giao thức như SNMP, NetFlow hoặc ICMP (ping).
* Phân tích dữ liệu: Các công cụ sẽ phân tích dữ liệu này để phát hiện xu hướng, cảnh báo khi có sự cố, hoặc dự đoán các vấn đề sắp xảy ra.
* Cảnh báo: Khi một thông số nào đó vượt quá ngưỡng định trước, hệ thống giám sát sẽ gửi thông báo (qua email, tin nhắn, hoặc cảnh báo trực quan) để quản trị viên kịp thời can thiệp.
  1. **Các phương pháp giám sát**
* Giám sát chủ động (Active Monitoring): Hệ thống chủ động gửi các yêu cầu (ping, SNMP, HTTP requests) tới các thiết bị để kiểm tra trạng thái và hiệu suất của chúng.
* Giám sát bị động (Passive Monitoring): Thu thập dữ liệu mà không gửi yêu cầu trực tiếp, chỉ dựa trên thông tin mà các thiết bị gửi về (ví dụ: NetFlow hoặc sFlow).
  1. **Chỉ số quan trọng cần giám sát**
* Độ trễ (Latency): Thời gian cần thiết để một gói tin đi từ nguồn đến đích và quay trở lại. Độ trễ cao có thể ảnh hưởng đến hiệu năng của các ứng dụng thời gian thực.
* Jitter: Biến thiên độ trễ giữa các gói tin liên tiếp, ảnh hưởng đến các ứng dụng yêu cầu kết nối liên tục như VoIP.
* Tỷ lệ mất gói (Packet Loss): Phản ánh khả năng giao tiếp ổn định của hệ thống mạng.
* Băng thông (Bandwidth): Tổng lượng dữ liệu có thể truyền qua một đường truyền trong một khoảng thời gian nhất định.
* Sử dụng CPU và bộ nhớ: Theo dõi hiệu suất phần cứng của các thiết bị mạng, đặc biệt quan trọng đối với các máy chủ và router.
  1. **Một số công cụ giám sát phổ biến**
* Nagios: Một hệ thống giám sát mã nguồn mở phổ biến với khả năng giám sát các dịch vụ mạng, tài nguyên máy chủ, và các thiết bị.

A computer screen shot of a service status

Description automatically generated

* Zabbix: Cung cấp giám sát thời gian thực với tính năng cảnh báo và trực quan hoá mạnh mẽ.

A screenshot of a computer

Description automatically generated

* Observium: Một công cụ tập trung vào việc theo dõi hiệu suất của các thiết bị sử dụng giao thức SNMP với giao diện đồ họa thân thiện.

A screenshot of a computer

Description automatically generated

* SolarWinds: Một giải pháp trả phí có tính năng giám sát toàn diện với các công cụ tiên tiến như NetFlow Traffic Analyzer.

A screenshot of a computer

Description automatically generated

* Cacti: Công cụ sử dụng RRDTool để vẽ biểu đồ theo dõi các chỉ số hiệu suất mạng theo thời gian.

A screenshot of a computer

Description automatically generated

* 1. **Vai trò của giám sát mạng trong đánh giá hiệu năng**
* Đánh giá liên tục: Thông qua giám sát, quản trị viên có thể thu thập dữ liệu hiệu suất theo thời gian, giúp phân tích xu hướng và đánh giá hiệu năng dài hạn của hệ thống.
* Dự đoán và cải thiện: Giám sát cho phép dự đoán các sự cố hoặc điểm yếu của hệ thống trước khi chúng xảy ra, giúp cải thiện hiệu năng.
* Tối ưu hoá tài nguyên: Dựa trên các báo cáo từ hệ thống giám sát, quản trị viên có thể phân bổ và điều chỉnh tài nguyên hệ thống để đạt hiệu quả tốt nhất.

# CHƯƠNG 2: CƠ BẢN VỀ GIAO THỨC SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

## 2.1. Tổng quan về SNMP

* SNMP (Simple Network Management Protocol) là giao thức tầng ứng dụng được sử dụng để quản lý và giám sát các thiết bị mạng cũng như chức năng của chúng. SNMP cung cấp ngôn ngữ chung cho các thiết bị mạng để chuyển tiếp thông tin quản lý trong cả môi trường single-vendor và multi-vendor trong mạng cục bộ (LAN) hoặc mạng diện rộng (WAN). Phiên bản gần đây nhất của SNMP, version 3, bao gồm các cải tiến bảo mật để xác thực và mã hóa tin nhắn SNMP cũng như bảo vệ các gói trong khi truyền.
* Một trong những giao thức được sử dụng rộng rãi nhất, SNMP được hỗ trợ trên một loạt các loại phần cứng – từ các thiết bị mạng thông thường như bộ định tuyến (router), bộ chuyển mạch (switch) và điểm truy cập không dây (wireless access point) đến các điểm cuối như máy in, scanner và thiết bị IoT (Internet of Things). Ngoài phần cứng, SNMP có thể được sử dụng để giám sát các dịch vụ như Dynamic Host Configuration Protocol (DHCP). Các software agent trên các thiết bị và dịch vụ này giao tiếp với hệ thống quản lý mạng (NMS), còn được gọi là trình quản lý SNMP, thông qua SNMP để chuyển tiếp thông tin trạng thái và thay đổi cấu hình.

## 2.2. Các thành phần chính của SNMP

* Một hệ thống sử dụng SNMP bao gồm 2 thành phần cơ bản: NMS (Network Management Station) và NE (Network Element).
  + SNMP Manager: Là phần mềm chạy trên máy chủ quản lý. Nó chịu trách nhiệm thu thập thông tin từ các agent trên các thiết bị mạng khác nhau và gửi lệnh điều khiển để cấu hình chúng.
  + SNMP Agent : Là phần mềm chạy trên các thiết bị mạng. Agent chịu trách nhiệm cung cấp dữ liệu trạng thái của thiết bị cho manager và thực thi các lệnh từ manager.
* Một SNMP Manager có thể quản lý nhiều SNMP Agent và ngược lại một SNMP Agent có thể chịu sự quản lý của nhiều SNMP Manager.
* Một số khái niệm cơ bản của giao thức SNMP:
  + Object:
    - Mỗi thiết bị có hỗ trợ SNMP cung cấp nhiều thông tin khác nhau, mỗi thông tin đó được gọi là object. Ví dụ: router có các thông tin về tổng số card, tổng số cổng, tổng số bit đã truyền/nhận, tên router, trạng thái tắt/mở của các cổng.
    - Mỗi object có một tên gọi riêng và một mã số Object ID (OID) để nhận dạng object đó. Ví dụ: tên thiết bị được gọi là sysName, OID là 1.3.6.1.2.1.1.5.
    - Mỗi object chỉ có duy nhất một OID nhưng có thể có nhiều tên gọi nên người ta sử dụng một chỉ số sub-id để phân biệt các object. Ví dụ: Tên thiết bị được gọi là sysName, OID là 1.3.6.1.2.1.1.5; nếu thiết bị có 2 tên thì chúng sẽ được gọi là sysName.0 và sysName.1 và có OID lần lượt là 1.3.6.1.2.1.1.5.0 và 1.3.6.1.2.1.1.5.1.
    - Một số object phổ biến thì được chuẩn hóa OID, riêng các object mới được tạo ra theo yêu cầu của cá nhân thì phải được mô tả OID. Để lấy một thông tin có OID đã chuẩn hóa thì ứng dụng SNMP phải gửi một gói tin SNMP có chứa OID của object đó cho SNMP agent, SNMP agent khi nhận được thì nó phải trả lời bằng thông tin ứng với OID đó.
    - Object access quy định quyền truy cập của mỗi object là READ\_ONLY (chỉ cho phép đọc object) hoặc READ\_WRITE (cho phép đọc và thay đổi giá trị object). Ví dụ: tên của một thiết bị (sysName) thì ta có thể thay đổi nên có quyền READ\_WRITE, còn giá tổng số cổng của thiết bị (ifNumber) là READ\_ONLY thì khổng thể đổi.
  + MIB (Management Information Base) là một cấu trúc dữ liệu gồm các object được quản lý, được dùng cho việc quản lý các thiết bị chạy trên nền TCP/IP. MIB được thể hiện thành 1 tập tin (MIB file) và có thể biểu diễn thành 1 cây (MIB tree). Muốn hiểu được một OID thì cần có tập tin MIB mô tả OID đó. Các thiết bị được quản lý bằng SNMP chỉ khi các ứng dụng SNMP manager và SNMP agent cùng hỗ trợ một MIB. Các ứng dụng này cũng có thể hỗ trợ cùng lúc nhiều MIB.

## 2.3. Những phiên bản của SNMP

* Tính đến năm 2024, SNMP có 3 phiên bản khác nhau bao gồm:
  + SNMP phiên bản 1 (SNMPv1): Đây là lần triển khai đầu tiên, hoạt động trong đặc tả thông tin quản lý cấu trúc và được mô tả trong tài liệu RFC 1157.
  + SNMP phiên bản 2 (SNMPv2): Phiên bản này đã được cải tiến để hỗ trợ xử lý lỗi hiệu quả hơn và được mô tả trong RFC 1901. Lần đầu tiên được giới thiệu trong RFC 1441 hay còn thường được gọi là SNMPv2c.
  + SNMP phiên bản 3 (SNMPv3): Phiên bản này cải thiện tính bảo mật cũng như quyền riêng tư và được giới thiệu trong RFC 3410.
* SNMPv2 là phiên bản giao thức SNMP phổ biến nhất trong thời điểm hiện tại. Trong khi đó, phiên bản SNMPv3 là gần nhất và được bổ sung hỗ trợ xác thực, mã hóa tập tin và các tin nhắn SNMP cũng như bảo vệ các gói tin trong quá trình truyền đi.

**2.4. SNMP hoạt động như thế nào?**

SNMPv2 hoạt động dựa trên 7 loại thông điệp:

* **GetRequest**: Manager gửi GetRequest (chứa một hoặc nhiều OID) đến agent để lấy một hoặc nhiều giá trị của object trong MIB.
* **GetNextRequest**: Manager gửi GetNextRequest đến agent dùng để lấy giá trị của object nằm kế tiếp object được chỉ ra trong MIB.
* **GetBulkRequest**: Manager gửi GetBulkRequest đến agent để lấy nhiều giá trị của nhiều object.
* **InformRequest**: Manager gửi InformRequest đến manager nhằm trao đổi thông tin với nhau.
* **SetRequest**: Manager gửi SetRequest đến agent để thiết lập giá trị cho object dựa vào OID. Chỉ những object có quyền READ\_WRITE mới có thể thiết lập giá trị được.
* **GetResponse**: Sau khi Agent nhận được các thông điệp GetRequest, GetNextRequest hay SetRequest thì nó sẽ gửi GetResponse để trả lời. Trong GetResponse có chứa OID của object được yêu cầu và giá trị của object đó.
* **Trap**:
  + Trap được agent tự động gửi đến manager để thông báo trong agent có sự kiện hay biến cố xảy ra. Ví dụ: khi có một cổng bị tắt, người dùng đăng nhập thất bại. Việc gửi hay không gửi khi biến cố xảy ra do hãng sản xuất thiết bị agent quy định.
  + SNMP request/response dùng để quản lý còn SNMP trap dùng để cảnh báo. Nguồn gửi trap được gọi là Trap Sender và nơi nhận trap được gọi là Trap Receiver. Mỗi trap sender có thể gửi nhiều trap đến nhiều trap receiver cùng lúc.
  + Trap gồm 2 loại chính: generic trap (được quy định trong các chuẩn SNMP) và specific trap (do hãng sản xuất tự định nghĩa). Có thể phân biệt loại trap dựa vào mã số là một số nguyên chứa trong gói tin trap. Theo SNMPv1, generic trap có 7 loại sau: coldStart(0), warmStart(1), linkDown(2), linkUp(3), authenticationFailure(4), egpNeighborloss(5), enterpriseSpecific(6).

A diagram of a network

Description automatically generated

# CHƯƠNG 3: PHÁT TRIỂN HỆ THỐNG GIÁM SÁT VỚI OBSERVIUM

## 3.1. Giới thiệu về Observium

**Observium** là một nền tảng giám sát và quản lý mạng mã nguồn mở được thiết kế để giúp các quản trị viên hệ thống theo dõi và quản lý hiệu suất của mạng và các thiết bị trong mạng một cách dễ dàng. Với giao diện web trực quan và khả năng hỗ trợ hàng trăm loại thiết bị từ các nhà cung cấp khác nhau, Observium đã trở thành một công cụ mạnh mẽ trong việc quản lý mạng, đặc biệt cho các tổ chức có hệ thống phức tạp.

* Đặc điểm nổi bật của Observium:
  + **Giao diện người dùng thân thiện**: Observium cung cấp một giao diện web rất trực quan, giúp người dùng dễ dàng theo dõi tình trạng của mạng và các thiết bị trong thời gian thực.
  + **Hỗ trợ đa dạng thiết bị**: Công cụ này có khả năng tự động phát hiện và giám sát nhiều loại thiết bị từ các hãng khác nhau như Cisco, Juniper, Dell, HP, Windows, Linux, và nhiều thiết bị khác sử dụng giao thức SNMP. Điều này giúp Observium phù hợp với hầu hết các môi trường mạng hiện đại.
  + **Giám sát hiệu năng mạng**: Observium thu thập các dữ liệu về hiệu suất từ các thiết bị trong mạng, bao gồm các thông tin như lưu lượng băng thông, độ trễ, mức sử dụng CPU và RAM, và nhiều thông tin khác thông qua giao thức SNMP và các giao thức giám sát khác.
  + **Biểu đồ và báo cáo**: Hệ thống cung cấp các biểu đồ chi tiết giúp quản trị viên dễ dàng theo dõi sự thay đổi trong hiệu suất mạng theo thời gian, từ đó dễ dàng phát hiện và xử lý các vấn đề trước khi chúng trở nên nghiêm trọng.
  + **Cảnh báo và thông báo**: Observium có khả năng gửi thông báo khi phát hiện sự cố hoặc khi một tham số vượt quá ngưỡng đã định, giúp quản trị viên có thể kịp thời can thiệp.
* Các tính năng chính:
  + **Tự động phát hiện thiết bị (Auto-discovery)**: Observium có khả năng tự động phát hiện các thiết bị mới trong mạng và thêm chúng vào hệ thống giám sát mà không cần cấu hình thủ công.
  + **Theo dõi hiệu suất thiết bị**: Nó giám sát tài nguyên hệ thống như CPU, RAM, băng thông và lưu lượng mạng của các thiết bị được kết nối.
  + **Quản lý log**: Giúp thu thập và quản lý nhật ký hệ thống từ các thiết bị, hỗ trợ việc phân tích sự cố.
  + **Giao thức hỗ trợ**: Hỗ trợ nhiều giao thức khác nhau như SNMP, IPMI, và các API của nhà cung cấp để thu thập thông tin từ các thiết bị mạng.
* Lợi ích của Observium:
  + **Tăng hiệu quả quản lý**: Giúp quản trị viên dễ dàng theo dõi tình trạng của toàn bộ hệ thống mạng chỉ từ một giao diện duy nhất.
  + **Giảm thời gian phát hiện và xử lý sự cố**: Với hệ thống cảnh báo và thông báo tức thời, Observium giúp giảm thiểu thời gian phản ứng với các sự cố trong mạng.
  + **Khả năng mở rộng cao**: Observium có thể được triển khai trên các hệ thống mạng từ nhỏ đến lớn, từ các doanh nghiệp nhỏ đến các trung tâm dữ liệu lớn với hàng ngàn thiết bị.
* Ứng dụng trong thực tế:
  + **Giám sát hệ thống mạng doanh nghiệp**: Observium được sử dụng rộng rãi trong các môi trường doanh nghiệp để giám sát và quản lý mạng lưới thiết bị phức tạp.
  + **Giám sát trung tâm dữ liệu**: Công cụ này cũng được sử dụng để quản lý hiệu suất và trạng thái của các trung tâm dữ liệu lớn, bao gồm các máy chủ, thiết bị lưu trữ và các thành phần hạ tầng khác.

## 3.2. Cấu trúc các khối chức năng của ứng dụng Observium

A diagram of a computer network

Description automatically generated

Cấu trúc các khối chức năng của ứng dụng Observium thường gồm các phần chính sau:

1. **SNMP + Agent:**

* Đây là nguồn chính của dữ liệu, nơi Observium thu thập thông tin từ các thiết bị mạng thông qua giao thức SNMP và các agents. SNMP giúp Observium giám sát tình trạng của các thiết bị như router, switch, máy chủ, v.v.

1. **Poller:**

* Khối **Poller** chịu trách nhiệm lấy dữ liệu định kỳ từ các thiết bị mạng. Dữ liệu thu thập được lưu vào bộ nhớ tạm (Memcached) để truy xuất nhanh, giúp tối ưu hóa quá trình hiển thị và quản lý.

1. **Billing Poller:**

* Đây là khối giám sát chuyên biệt cho việc tính toán và theo dõi dữ liệu liên quan đến lưu lượng và mức sử dụng băng thông của các thiết bị. Dữ liệu này cũng được lưu trữ vào các hệ thống lưu trữ như RRD (Round Robin Database) và MySQL.

1. **Discovery:**

* **Discovery** là khối tự động phát hiện các thiết bị mới trong hệ thống mạng. Khi một thiết bị mới xuất hiện, Discovery sẽ tìm và thêm nó vào hệ thống giám sát của Observium mà không cần phải cấu hình thủ công.

1. **Memcached**:

* **Memcached** đóng vai trò là bộ nhớ đệm giúp lưu trữ tạm thời dữ liệu để giảm tải cho cơ sở dữ liệu chính và tăng tốc độ truy xuất thông tin khi quản trị viên cần xem dữ liệu thông qua giao diện web.

1. **RRD (Round Robin Database)**:

* **RRD** là hệ thống lưu trữ dữ liệu thời gian thực, đặc biệt là các thông số hiệu suất mạng theo thời gian. Nó giúp Observium quản lý khối lượng lớn dữ liệu một cách hiệu quả mà không bị tăng kích thước cơ sở dữ liệu quá mức.

1. **MySQL**:

* **MySQL** đóng vai trò lưu trữ thông tin cấu hình, thông tin thiết bị, và các dữ liệu liên quan khác để Observium có thể quản lý và hiển thị trên giao diện.

1. **Web GUI và Graphs**:

* **Web GUI** là giao diện người dùng trực quan, nơi quản trị viên có thể giám sát tình trạng mạng, các thiết bị và dữ liệu hiệu suất. Dữ liệu được hiển thị qua các biểu đồ (**Graphs**) giúp quản trị viên dễ dàng theo dõi và phát hiện các vấn đề trong mạng.

Cấu trúc này giúp Observium dễ dàng mở rộng, hỗ trợ nhiều loại thiết bị và giúp việc quản lý mạng trở nên hiệu quả hơn.

## 3.3. Triển khai cài đặt:

Các bước cài đặt được triển khai theo link: <https://docs.observium.org/install_debian/>

# CHƯƠNG 4: TRIỂN KHAI THỰC NGHIỆM VÀ KẾT QUẢ

## 4.1. Mô hình và kịch bản triển khai

A diagram of a cloud server

Description automatically generated5

## 4.2. Kết quả thực nghiệm

Video Demo: [[NT531.P11.MMCL]-Group11-Observium](https://youtu.be/wnydlZ5dPYg)

# CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

## 5.1. Kết luận

Báo cáo đã nghiên cứu, triển khai và hoàn thành những vấn đề sau:

* Lý thuyết:
  + Về vấn đề giám sát: Đi sâu phân tích về giám sát hệ thống và tầm quan trọng của việc giám sát hệ thống trong môi trường mạng.
  + Về giao thức quản lý mạng: Trình bày về giao thức quản lý mạng đơn giản (Simple Network Management Protocol) bao gồm: khái niệm giao thức quản lý mạng, các thành phần trong giao thức quản lý mạng, và cách hoạt động của giao thức quản lý mạng.
  + Nắm được phương pháp hoạt động và lấy thông tin hệ thống của phần mềm mã nguồn mở Observium.
* Thực nghiệm:
  + Báo cáo đưa ra mô hình triển khai và trình bày toàn bộ các bước cấu hình các hệ thống giám sát theo mô hình triển khai đã đề ra.
  + Về cơ bản đã khai thác được các chức năng chính của phần mềm mã nguồn mở Observium. Những kết quả đạt được:
  + Có các kiến thức về giám sát hệ thống, các giao thức quản lý mạng.
  + Triển khai thành công mô hình giám sát hệ thống bằng phần mềm mã nguồn mở Observium.
  + Có thể cấu hình Router, Switch, ASA, IPS, Windows, Linux phục vụ cho quá trình giám sát.
  + Tích lũy kinh nghiệm trong việc cấu hình các công nghệ trên.

## 5.2. Hướng phát triển

A diagram of a server

Description automatically generated

# TÀI LIỆU THAM KHẢO

[1]<https://www.observium.org/>

[2] <https://suncloud.vn/>

**HẾT.**