**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG THƯƠNG TP HỒ CHÍ MINH**

**KHOA CÔNG NGHỆ THÔNG TIN**



----o0o----

**HỌC PHẦN: GIÁM SÁT VÀ ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN**

**ĐỀ TÀI: TÌM HIỂU VÀ TRIỂN KHAI HỆ THỐNG GIÁM SÁT VỚI MRTG**

|  |  |  |
| --- | --- | --- |
| **DANH SÁCH THÀNH VIÊN NHÓM 17** | | |
| Họ và Tên | MSSV | Công Việc |
| Lý Tiến Đạt (NT) | 2033216386 | Nội Dung |
| Lê Quốc Anh | 2033216341 | Mô Hình + demo |
| Mai Nhựt Trường | 2033207467 | Demo |

**GVBM: TS. Vũ Đức Thịnh**

*Tp.HCM Ngày 15 tháng 07 năm 2024*

**LỜI CAM ĐOAN**

Nhóm chúng em xin cam đoan đây là bài báo cáo tiểu luận của nhóm chúng em. Các số liệu, kết quả bên trong “Bài báo cáo tiểu luận” điều là trung thực.

Chúng em xin cam đoan rằng mọi sự giúp đỡ cho việc thực hiện “Bài báo cáo tiểu luận” này đã được cảm ơn và các thông tin được trích dẫn trong báo cáo đã được chỉ rõ nguồn gốc.

## Nhóm sinh viên thực hiện Báo cáo

*(Đã ký và và ghi rõ họ tên)*

**LỜI CẢM ƠN**

Qua một thời gian nghiên cứu, phân công công việc và tiến hành thực hiện đến nay, đề tài “MRTG” đã hoàn thành. Chúng em xin chân thành cảm các thầy cô đã trang bị kiến thức quý báu cho chúng em trong suốt quá trình học. Đặc biệt là các thầy các cô trong khoa Công nghệ thông tin đã tận tình giảng dạy, chỉ bảo, trang bị cho chúng em những kiến thức cần thiết nhất trong suốt quá trình học tập và nghiên cứu tại khoa, đã tạo mọi điều kiện thuận lợi giúp chúng em.

Chúng em cũng xin chân thành cảm ơn giảng viên Vũ Đức Thịnh đã tận tình giảng dạy và hướng dẫn chúng em hoàn thành tốt đề tài này và một thành phần không thể thiếu được chính là sự nỗ lực của các thành viên trong nhóm.

Trong quá trình thực hiện đề tài, chúng em không tránh khỏi những thiếu xót cũng như những hạn chế nhất định. Chúng em mong nhận được sự đóng góp ý kiến, chỉ bảo tận tình của các thầy và các bạn để đề tài của chúng em hoàn thiện hơn và thiết thực hơn.

**MỤC LỤC**

[LỜI CẢM ƠN 2](#_Toc16505)

[I. PHẦN MỞ ĐẦU 4](#_Toc1078)

[A. LÝ DO CHỌN ĐỀ TÀI 4](#_Toc22050)

[B. MỤC TIÊU CỦA ĐỀ TÀI 4](#_Toc8359)

[C. LỊCH SỬ RA ĐỜI CỦA MRTG 5](#_Toc31020)

[II. TỔNG QUAN VỀ CÔNG CỤ GIÁM SÁT MRTG 6](#_Toc7315)

[A. KHÁI NIỆM VÀ CÁC THÀNH PHẦN CHÍNH CỦA MRTG 6](#_Toc27629)

[B. SO SÁNH MRTG VỚI CÁC CÔNG CỤ GIÁM SÁT KHÁC 8](#_Toc20448)

[C. ĐẶC ĐIỂM CƠ BẢN CỦA MRTG 9](#_Toc29174)

[D. CÀI ĐẶT VÀ CẤU HÌNH MRTG 11](#_Toc5655)

[E. GIÁM SÁT PHẦN CỨNG TRÊN MÁY CHỦ. 14](#_Toc28157)

[F. CÁC TÍNH NĂNG CHÍNH CỦA MRTG. 21](#_Toc12062)

[G. ƯU ĐIỂM VÀ NHƯỢC ĐIỂM CỦA VIỆC SỬ DỤNG MRTG TRONG GIÁM SÁT MẠNG. 22](#_Toc4144)

[H. ỨNG DỤNG THỰC TIỄN CỦA MRTG 2](#_Toc17093)3

[III. KẾT LUẬN 2](#_Toc8213)4

[A. TÓM TẮT CÁC ĐIỂM CHÍNH VỀ MRTG 2](#_Toc1448)4

[B. TRIỂN VỌNG VÀ TRONG TƯƠNG LAI 2](#_Toc1626)5

[IV. DEMO 2](#_Toc12851)5

[A. KỊCH BẢN 1 ( ATTACKER TẤN CÔNG TỪ BÊN NGOÀI DMZ) 2](#_Toc7753)5

[B. KỊCH BẢN 2 ( ATTACKER TẤN CÔNG TỪ BÊN LAN VÀO DMZ) 2](#_Toc21435)6

[V. TÀI LIỆU THAM KHẢO 2](#_Toc17049)7

## 

## PHẦN MỞ ĐẦU

### LÝ DO CHỌN ĐỀ TÀI

- Trong thế giới kỹ thuật số hiện nay, mạng máy tính trở thành một phần không thể thiếu trong hoạt động của các tổ chức và doanh nghiệp. Việc giám sát mạng không chỉ giúp duy trì hiệu suất hoạt động mà còn đảm bảo an toàn thông tin, ngăn chặn các mối đe dọa tiềm ẩn.

- Khi có sự cố xảy ra, quản trị viên có thể phản ứng nhanh chóng để khắc phục, giảm thiểu thời gian gián đoạn dịch vụ và lập kế hoạch mở rộng hạ tầng. Vì vậy MRTG là một trong những công cụ mạnh mẽ và hiệu quả giúp duy trì hiệu suất, tối ưu hóa tài nguyên và đảm bảo an toàn cho hệ thống mạng

### MỤC TIÊU CỦA ĐỀ TÀI

- Tiểu luận này nhằm mục đích tìm hiểu sâu hơn về MRTG, từ các tính năng cơ bản nghiên cứu đến hiểu rõ về công cụ và tiềm năng phát triển. Bằng cách nắm vững kiến thức về MRTG, chúng ta có thể hiểu rõ hơn về vai trò và ứng dụng của nó trong thế giới công nghệ hiện đại.

- Qua các phần tiếp theo của tiểu luận, chúng ta sẽ khám phá chi tiết hơn về MRTG và cách nó ảnh hưởng đến việc giám sát và phát triển phần mềm.

- Bài trình bày này bao gồm các hướng dẫn cách thiết lập giám sát máy chủ cơ bản của máy chủ chạy hệ điều hành dựa trên Microsoft Windows bằng MRTG để thu thập số liệu thống kê từ máy mục tiêu thông qua SNMP. Thiết lập tối thiểu này thiết lập đường cơ sở nền tảng quan trọng cần được xem xét thường xuyên như một phần của chiến lược chủ động nhằm quản lý hoạt động hàng ngày của môi trường máy chủ.

### LỊCH SỬ RA ĐỜI CỦA MRTG

- MRTG đã trải qua nhiều giai đoạn phát triển và cải tiến để trở thành một trong những công cụ giám sát mạng phổ biến nhất. Năm 1994 được Tobias Oetiker, một kỹ sư hệ thống từ Thụy Sĩ, bắt đầu phát triển MRTG. Ban đầu, công cụ này được tạo ra để giải quyết nhu cầu cá nhân của Tobias trong việc giám sát lưu lượng mạng của các router mà anh quản lý. Động lực chính là cung cấp một cách trực quan để theo dõi và phân tích lưu lượng mạng.

- Năm 1995, phiên bản đầu tiên của MRTG được phát hành. MRTG nhanh chóng thu hút sự chú ý của cộng đồng quản trị mạng nhờ vào khả năng tạo ra các đồ thị lưu lượng mạng một cách tự động và dễ dàng. Giai đoạn 1996-1999, MRTG liên tục được cập nhật và cải tiến với các tính năng mới và sửa lỗi. Các phiên bản mới của MRTG được phát hành đều đặn, mỗi phiên bản mang đến các cải tiến về hiệu suất, khả năng mở rộng và tính ổn định.

- Đầu những năm 2000: MRTG trở thành một trong những công cụ giám sát mạng được sử dụng rộng rãi nhất trên toàn thế giới. Nhiều tổ chức, từ các doanh nghiệp nhỏ đến các tập đoàn lớn, đã áp dụng MRTG để giám sát và quản lý lưu lượng mạng. MRTG phản ánh sự tiến hóa liên tục và sự cải tiến không ngừng. Từ một công cụ đơn giản được phát triển để phục vụ nhu cầu cá nhân, MRTG đã trở thành một công cụ phổ biến và đáng tin cậy trong quản lý mạng, đóng góp lớn vào việc duy trì hiệu suất và bảo mật mạng trên toàn thế giới.

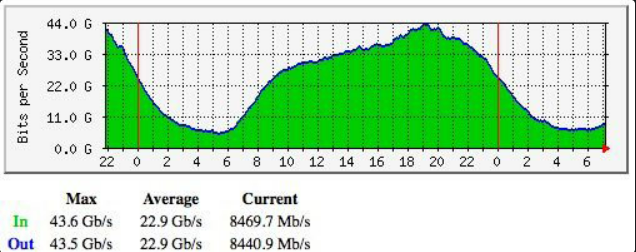


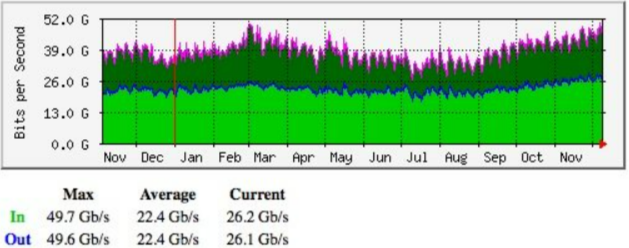
## TỔNG QUAN VỀ CÔNG CỤ GIÁM SÁT MRTG

### KHÁI NIỆM VÀ CÁC THÀNH PHẦN CHÍNH CỦA MRTG

- MRTG (Multi Router Traffic Grapher) là một công cụ mã nguồn mở được sử dụng rộng rãi để giám sát và hiển thị lưu lượng mạng. MRTG giúp các quản trị viên mạng theo dõi lưu lượng mạng qua các đồ thị trực quan. Công cụ giám sát này chủ yếu sử dụng SNMP (Simple Network Management Protocol) để thu thập dữ liệu từ các thiết bị mạng như router, switch và máy chủ, sau đó tạo ra các đồ thị HTML để hiển thị thông tin về lưu lượng.

- Trong hình A, bạn có thể xem dữ liệu hàng ngày của một router được giám sát bởi MRTG. Hình B hiển thị một đồ thị, thể hiện thông tin đã thu thập được trong vòng một năm. Đây chính là sức mạnh thực sự của những công cụ này – chúng cung cấp cho người dùng dữ liệu cần thiết để đưa ra quyết định cho các dịch vụ và cơ sở hạ tầng.

  
Hình A: Đồ thị biểu hiện dữ liệu hàng ngày MRTG thu được.

  
Hình B: Sử dụng đồ thị biểu hiện dữ liệu hàng năm để lên kế hoạch dài hạn.

***\* Các thành phần chính của MRTG:***

* **SNMP Daemon:** Là phần mềm SNMP được cài đặt trên các thiết bị mạng để cung cấp thông tin lưu lượng mạng.
* **MRTG Daemon:** Là quá trình chính của MRTG, thực hiện các hoạt động thu thập dữ liệu, lưu trữ và tạo đồ thị.
* **Các file cấu hình:** MRTG sử dụng các tệp cấu hình để xác định các thiết bị mạng cần giám sát, các thông số thu thập (như địa chỉ IP, cổng SNMP), và cách thức hiển thị đồ thị.
* **Các file log và dữ liệu RRD**: Dữ liệu thu thập được lưu trữ trong các file log và sử dụng RRDTool (Round-Robin Database Tool) để tổ chức và lưu trữ dữ liệu dưới dạng cơ sở dữ liệu vòng tròn.
* **Giao diện web:** MRTG cung cấp giao diện web để người dùng có thể truy cập và xem các đồ thị lưu lượng mạng.

### SO SÁNH MRTG VỚI CÁC CÔNG CỤ GIÁM SÁT KHÁC

- Ví dụ như phần mềm Zabbix:

MRTG và Zabbix là hai công cụ giám sát có nhu cầu sử dụng và tính năng khác nhau.

|  |  |  |
| --- | --- | --- |
| Đặc điểm | MRTG | ZABBIX |
| 1. Khả năng giám sát | Chủ yếu tập trung vào giám sát và hiển thị lưu lượng mạng thông qua các đồ thị. | Không chỉ giám sát lưu lượng mạng mà còn cung cấp khả năng giám sát toàn diện cho hệ thống, bao gồm cả máy chủ, ứng dụng và các thành phần mạng khác. |
| 1. Mức độ phù hợp và độ linh hoạt | Thích hợp cho các môi trường cần giám sát và phân tích lưu lượng mạng cơ bản. | Thích hợp cho các môi trường phức tạp và đòi hỏi giám sát toàn diện hơn, bao gồm cả hệ thống máy chủ, ứng dụng và mạng. |
| 1. Khả năng tùy chỉnh | Có cách thức cấu hình đơn giản hơn nên hỗ trợ ít tính năng tùy chỉnh. | Với hỗ trợ plugin, cho phép người dùng mở rộng chức năng giám sát theo nhu cầu cụ thể. |
| 1. Bảo mật và hiệu suất | Không phù hợp cho các môi trường yêu cầu bảo mật cao. | Cung cấp các tính năng bảo mật mạnh mẽ như xác thực và mã hóa dữ liệu, phù hợp cho các môi trường yêu cầu bảo mật cao. |

### ĐẶC ĐIỂM CƠ BẢN CỦA MRTG

- Phần mềm MRTG được viết bằng ngôn ngữ lập trình Perl và C, có thể chạy trên hệ điều hành Windows và UNIX. Kịch bản Perl được sử dụng để đọc lưu lượng và chương trình C được dùng để ghi lưu lượng vào file và vẽ biểu đồ biểu thị lưu lượng ra các file ảnh. Những ảnh này được nhúng vào trang web và người quản trị có thể xem toàn bộ thông tin giám sát qua web.

- MRTG có thể ghi lưu lượng theo ngày, 7 ngày, 4 tuần, và một năm gần đây. Ngoài ra, dữ liệu trong log file không bị lớn lên theo thời gian, giúp tiết kiệm tài nguyên hệ thống.

- MRTG không chỉ giám sát lưu lượng trên mạng mà còn có thể sử dụng để giám sát các thông số lấy được thông qua giao thức SNMP. Chúng ta có thể sử dụng MRTG để giám sát các thông số về tải hệ thống, phiên đăng nhập, và nhiều thông số khác. MRTG cho phép tích hợp nhiều kiểu dữ liệu vào trong một đồ thị.

**Đặc Điểm Nổi Bật của MRTG:**

* Di động (Portable): MRTG có thể chạy trên cả UNIX và Windows.
* Tích hợp với SNMP: MRTG tích hợp sẵn gói phần mềm về giao thức SNMP được viết sẵn bằng Perl, vì vậy không cần sử dụng bất kỳ bộ công cụ về SNMP nào khác.
* Hỗ trợ SNMP version 2: MRTG có thể đọc biến kiểu counter của SNMPv2.
* Xác định các giao diện của thiết bị dễ dàng: Các giao diện trên thiết bị có thể xác định bởi địa chỉ IP, mô tả và địa chỉ Ethernet hoặc số thứ tự của giao diện.
* Kích thước file không thay đổi: File dữ liệu mà MRTG sử dụng không thay đổi kích thước, giúp tiết kiệm tài nguyên hệ thống và truy xuất dữ liệu nhanh chóng.
* Cấu hình tự động: MRTG cung cấp một bộ công cụ để tạo file cấu hình, giúp việc cài đặt trở nên đơn giản.
* Hiệu quả: Phần xử lý dữ liệu được viết hoàn toàn bằng C, tăng tốc độ xử lý.
* Có khả năng tuỳ biến cao: Giao diện hiển thị có thể tuỳ biến một cách dễ dàng thông qua các thẻ HTML.
* Tích hợp bộ công cụ RRDTool: MRTG tích hợp với RRDTool (Round Robin Database) để lưu trữ và xử lý dữ liệu mềm dẻo hơn.

**Ngoài ra:** MRTG còn là công cụ mã nguồn mở, MRTG không yêu cầu chi phí bản quyền, đồng thời cho phép tùy chỉnh và mở rộng theo nhu cầu cụ thể của tổ chức.

- MRTG cung cấp các đồ thị trực quan giúp quản trị viên dễ dàng theo dõi và phân tích xu hướng lưu lượng mạng. Điều này giúp phát hiện sớm các vấn đề về hiệu suất và bảo mật.

- Sử dụng giao thức SNMP để thu thập dữ liệu từ các thiết bị mạng. SNMP là một giao thức phổ biến cho việc giám sát và quản lý các thiết bị mạng, cho phép MRTG truy xuất thông tin về lưu lượng truyền tải qua các giao diện mạng.

- MRTG lưu trữ dữ liệu lịch sử, cho phép phân tích xu hướng sử dụng băng thông qua thời gian, từ đó giúp lập kế hoạch và tối ưu hóa tài nguyên mạng.

- Nhờ tính mã nguồn mở, MRTG có khả năng mở rộng và tùy chỉnh cao. Người dùng có thể thêm vào các module hoặc script tùy chỉnh để mở rộng chức năng của MRTG theo nhu cầu cụ thể.

### CÀI ĐẶT VÀ CẤU HÌNH MRTG

* 1. **Điều kiện để cài đặt:**

Để MRTG hoạt động trên Windows, cần những thứ sau:

* Một bản sao hiện tại của Perl. Ví dụ ActivePerl 5.8.8 từ ActiveState: <http://www.activestate.com/store/activeperl/download/>
* Phiên bản mới nhất của MRTG từ <http://oss.oetiker.ch/mrtg/pub>. Tìm mrtg-2.17.10.zip hoặc tốt hơn. Kho lưu trữ cũng chứa bản sao được biên dịch trước của rateup.exe cho Win32.

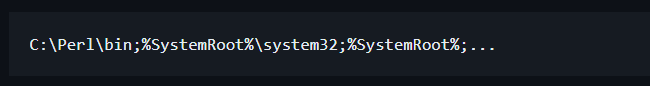
**4.2 Quá trình cài đặt MRTG:**

Đầu tiên

Giải nén MRTG vào C:\mrtg-2.17.10 trên máy tính Windows .

Kế tiếp

Cài đặt Perl trên cùng một máy Windows. Có thể muốn đảm bảo rằng thư mục nhị phân Perl được liệt kê trong đường dẫn hệ thống của bạn.



Ngoài ra có thể kiểm tra thủ công bằng cách vào:

[Control Panel]->[System]->[Environment]

Để xem mọi thứ đã được cài đặt đúng cách chưa, có thể mở Command Shell và vào c:\mrtg-2.17.10\bin . Nhập: perl mrtg



Điều này sẽ cung cấp cho một thông báo lỗi thân thiện phàn nàn về tệp cấu hình MRTG bị thiếu. Bây giờ, đã cài đặt MRTG và Perl thành công.

**4.3. Cấu hình MRTG.**

- Trước khi bắt đầu, cần biết một vài điều. Hãy tận dụng cơ hội để thu thập thông tin sau:

* Địa chỉ IP hoặc tên máy chủ và số cổng SNMP (nếu không chuẩn) của thiết bị bạn muốn theo dõi.
* Nếu bạn muốn theo dõi thứ gì đó khác ngoài byte vào và ra, cũng phải biết SNMPOID của thứ mình muốn theo dõi.
* Cuối cùng, cần biết chuỗi cộng đồng SNMP chỉ đọc cho thiết bị của mình. Nếu không biết, hãy thử public , đó là mặc định.

Đối với phần còn lại sẽ sử dụng thiết bị 10.10.10.1 (CISCO Catalyst 5000) với chuỗi Community public . Chủ yếu quan tâm đến việc theo dõi lưu lượng truy cập và tải CPU.

- Điều đầu tiên chúng ta làm khi thiết lập MRTG là tạo một tệp cấu hình mặc định. Đến dấu nhắc cmd và chuyển đến thư mục c:\mrtg-2.17.10\bin . Nhập lệnh sau:



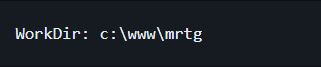
- Thao tác này tạo ra một tệp cấu hình MRTG ban đầu. Lưu ý rằng trong tệp này, tất cả các giao diện của bộ định tuyến của ta sẽ được lưu trữ theo số. Thật không may, những con số này có thể thay đổi bất cứ khi nào bạn cấu hình lại bộ định tuyến của mình. Để giải quyết vấn đề này, có thể yêu cầu cfgmaker tạo ra một cấu hình dựa trên số IP hoặc thậm chí là Mô tả giao diện.

- Nếu nhận được thông báo lỗi phàn nàn rằng không có tên như vậy hoặc không có phản hồi , thì có thể tên cộng đồng của bạn đã sai.

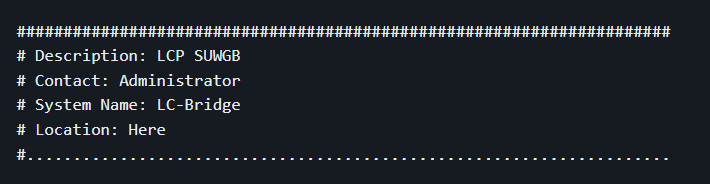
- Bây giờ, chúng ta hãy xem tệp mrtg.cfg đã được tạo.

Trong Perl, a #là chú thích, đồng nghĩa với REMtrong DOS.

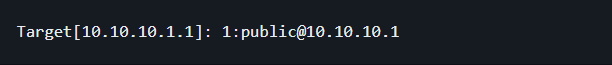
Thêm nội dung sau vào đầu tệp mrtg.cfg:



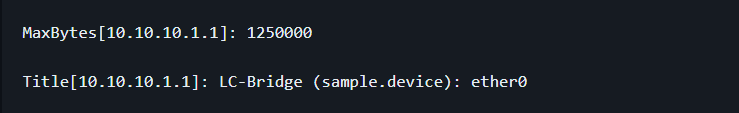
Đây là nơi các trang web được tạo ra, thường là gốc web.



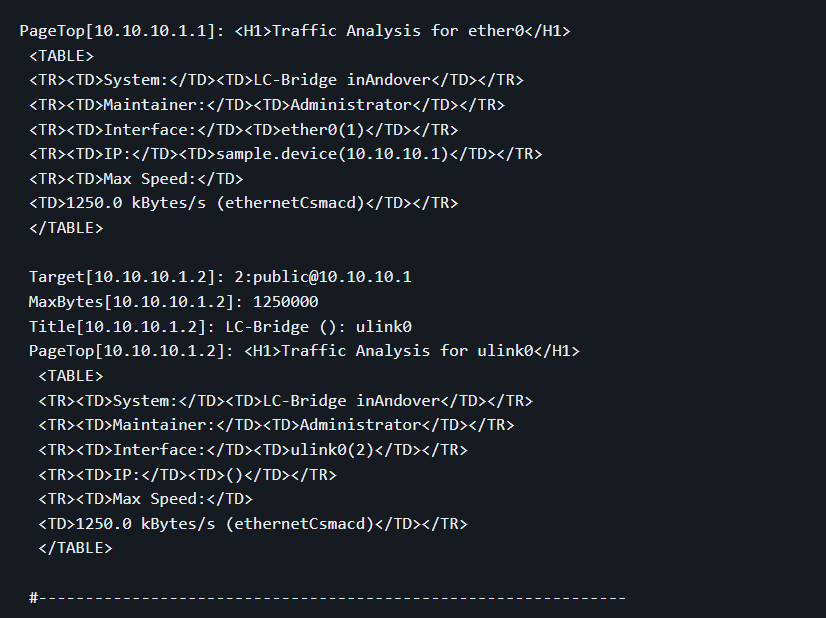
Địa chỉ IP của TargetDevice:Số giao diện:Cộng đồng:Địa chỉ IP



Đây là tốc độ giao diện (Mặc định là 10 megabit; đối với thiết bị 100Mbit, sử dụng 12500000, v.v...)



Phần này xác định tiêu đề trang web sẽ trông như thế nào



Và đó là một tệp cấu hình MRTG rất cơ bản. Bạn có thể chạy tệp này và xem kết quả bằng cách vào thư mục c:\mrtg-2.17.10\bin và nhập:



Cấu hình thành công.

- Sau khi MRTG đã được cài đặt và thiết lập, phần còn lại của nỗ lực bao gồm việc thiết lập các hệ thống để được giám sát và sửa đổi các tệp cấu hình. Khi thực hiện thay đổi đối với tệp cấu hình, MRTG sẽ cần phải dừng và khởi động lại để đọc cài đặt mới.

### GIÁM SÁT PHẦN CỨNG TRÊN MÁY CHỦ.

**Nên theo dõi thông tin tối thiểu nào về máy chủ?**

Thông tin tối thiểu cần được theo dõi trên hầu hết các máy chủ là mức sử dụng dung lượng ổ đĩa, mức sử dụng bộ nhớ, mức sử dụng CPU và mức sử dụng mạng. Có nhiều số liệu thống kê hữu ích hơn có thể áp dụng cho một máy chủ hoặc môi trường cụ thể, nhưng từ góc độ vận hành, những chi tiết tối thiểu này sẽ hữu ích cho việc sử dụng hàng ngày và giúp thiết lập cơ sở để hiểu các thông số vận hành bình thường của hệ thống mà chịu trách nhiệm quản lý và cung cấp các chỉ báo cảnh báo sớm khi hệ thống vượt quá khả năng phần cứng của nó.

**Sử dụng công cụ nào để lấy dữ liệu SNMP?**

Snmpget và snmpwalk là những cách trực tiếp nhất để truy vấn dữ liệu snmp từ dòng lệnh. Có sẵn phiên bản Unix và Windows của công cụ này. Tuy nhiên, có những khác biệt nhỏ giữa quá trình triển khai và phiên bản, do đó kết quả sẽ báo cáo hơi khác nhau hoặc dòng lệnh sẽ khác nhau giữa các phiên bản. Snmpget thường được sử dụng khi bạn biết OID đầy đủ của dữ liệu bạn muốn truy vấn. Snmpwalk rất hữu ích khi bạn muốn xem cây OID bắt đầu từ một giá trị được xác định trước đó. Điều này đặc biệt hữu ích trong việc tìm hiểu những giá trị nào có sẵn sau một điểm nhất định trong cấu trúc OID nếu bạn không biết giá trị OID hoàn chỉnh cho dữ liệu bạn muốn.

• snmpget

Cách sử dụng: snmpget [-Cf] [options...] <hostname>

{<cộng đồng>} [< objectID > …]

• snmpwalk

Cách sử dụng: snmpwalk [tùy chọn...] <tên máy chủ>

{<cộng đồng>} [< objectID >]

• \*Có sẵn phiên bản nix và Windows

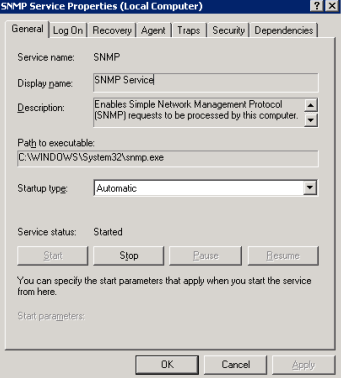
– http://net -snmp.sourceforge.net /

• Có nhiều công cụ dựa trên GUI khác nhau cho SNMP

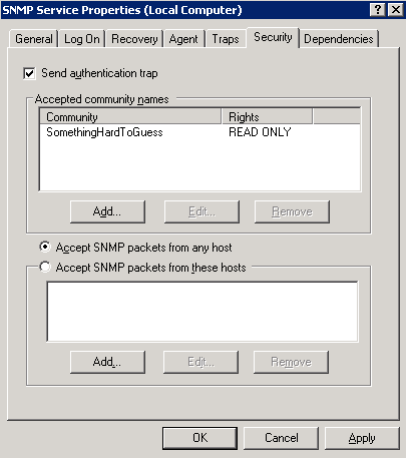
duyệt

**SNMP-Information**

Để bắt đầu truy vấn máy chủ Windows qua SNMP nhằm thu thập số liệu thống kê hữu ích, dịch vụ SNMP cần được bật và định cấu hình đúng cách. Để thực hiện việc này, hãy mở công cụ quản trị “Services” và định vị Máy chủ SNMP. Đảm bảo dịch vụ được đặt để tự động khởi động.



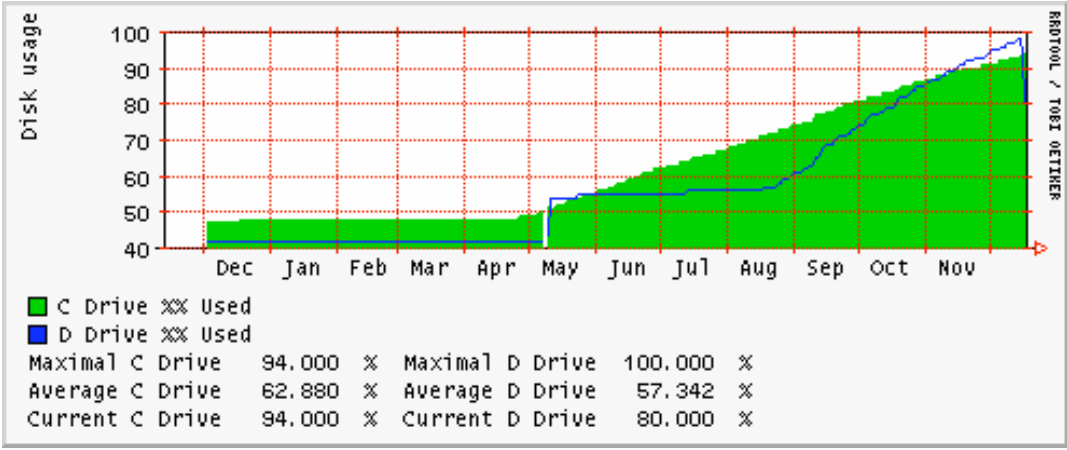
Kiểm tra tab bảo mật và đảm bảo rằng có tên cộng đồng Chỉ đọc (tối thiểu) đã được tạo cho máy chủ. Cuối cùng, chọn tùy chọn “Chấp nhận gói SNMP từ bất kỳ hosts này” hoặc đảm bảo rằng các hệ thống được ủy quyền mà từ đó truy vấn SNMP sẽ được nhập vào hộp bên dưới “Chấp nhận gói SNMP từ các hots này”



Mặc dù bạn có thể bắt đầu truy vấn một số dữ liệu cơ bản thông qua SNMP sau khi hoàn thành bước này, nhưng trước đây đã từng xảy ra sự cố trong đó các OID cụ thể quan trọng cần truy vấn hệ thống Microsoft để biết các thay đổi chi tiết phần cứng do khởi động lại, cấp độ bản vá hoặc các vấn đề dường như tùy ý khác. sự kiện. Để giải quyết vấn đề này, phiên bản cơ bản của snmp-informant (miễn phí) cần được cài đặt. Bằng cách này, chúng tôi đảm bảo rằng các OID mà chúng tôi sẽ giám sát bằng MRTG thông qua SNMP sẽ không đổi.

1. **Disk Utilization - Giám sát không gian đĩa:**

Lý do chính để theo dõi việc sử dụng ổ đĩa là để xác định khi nào hệ thống sắp hết dung lượng ổ đĩa. Lý tưởng nhất là hệ thống thường không được sử dụng quá 80%. Sau khi thực hiện được điều đó, bạn nên lập kế hoạch để tăng dung lượng ổ đĩa hoặc xóa các tệp cũ không cần lưu trữ trên đĩa nữa. Bằng cách giám sát các biểu đồ cơ sở hiển thị số liệu thống kê về việc sử dụng ổ đĩa trong một khoảng thời gian dài, việc dự đoán khi nào các vấn đề về dung lượng này sẽ trở thành vấn đề và thực hiện hành động trước khi chúng ảnh hưởng đến khả năng hoạt động của hệ thống sẽ trở nên dễ dàng hơn



1. **Memory Utilization - Sử dụng bộ nhớ**

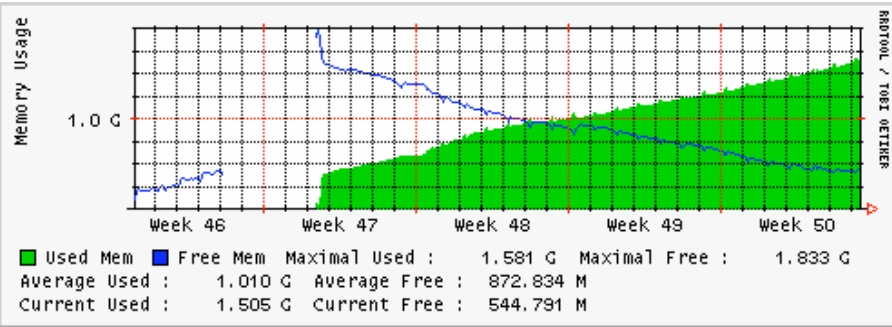
Việc xem lại các biểu đồ về mức sử dụng bộ nhớ rất hiệu quả trong việc xác định các rò rỉ bộ nhớ, chẳng hạn như biểu đồ được hiển thị trên biểu đồ trong trang chiếu. Thông tin này rất hữu ích trong việc duy trì chức năng hoạt động của hệ thống có đặc điểm rò rỉ bộ nhớ. Vấn đề này thường được giải quyết theo một trong những cách sau:

- Xác định và sửa mã là nguyên nhân cốt lõi gây rò rỉ bộ nhớ

- Triển khai khởi động lại theo lịch trình để “reset” hệ thống và giảm tác động của rò rỉ bộ nhớ

- Kéo dài khoảng thời gian hệ thống duy trì khả năng hoạt động bằng cách tăng dung lượng bộ nhớ trong hệ thống.

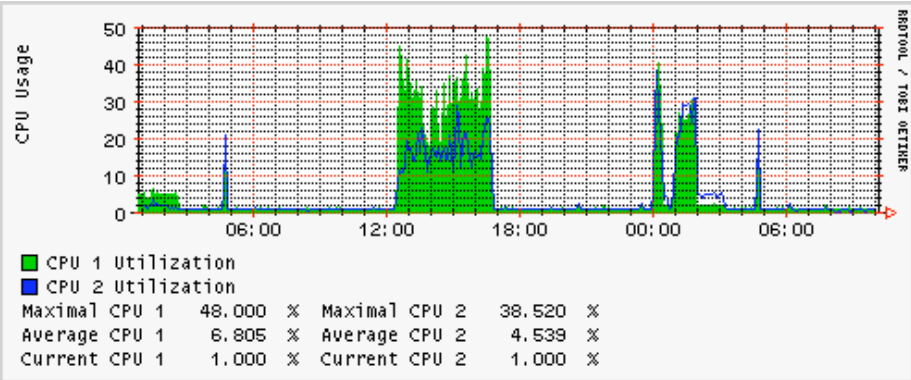
Đồng thời, biểu đồ này cung cấp thông tin hữu ích khi xác định xem bộ nhớ có sẵn trong hệ thống có đủ cho mục đích của nó hay không. Nếu dung lượng bộ nhớ trống cực kỳ thấp ngay cả sau khi khởi động lại mới, hệ thống có thể cần thêm bộ nhớ.



1. **CPU Utilization - sử dụng CPU**

Khi xem mức sử dụng CPU, chúng ta chủ yếu sẽ tìm kiếm những khoảng thời gian mà mức sử dụng bộ xử lý ở mức rất cao và duy trì như vậy. Điều này có thể cho thấy ứng dụng bị treo, bộ xử lý không đủ đáp ứng nhu cầu của hệ thống hoặc xác định khoảng thời gian mà các tác vụ đã lên lịch có thể cần được xem xét cẩn thận để có

một số sự kiện nhất định xảy ra trong giờ thấp điểm. Cuối cùng, những biểu đồ này giúp thiết lập đường cơ sở về hành vi bình thường cho hệ thống đang được giám sát. Đối với biểu đồ được minh họa trong slide, đây là dấu hiệu cho thấy hành vi sao lưu bình thường xảy ra trên hệ thống đích. Biểu đồ này được lấy từ biểu đồ sử dụng hàng ngày của một hệ thống vào sáng Chủ nhật. Vào thứ Bảy, vào khoảng 12:30 trưa, một bản sao lưu đầy đủ đã được khởi tạo trên hệ thống đích. Quá trình sao lưu đầy đủ này mất khoảng 4 giờ. Sáng Chủ nhật tuần sau ngay sau nửa đêm, một bản sao lưu gia tăng đã được bắt đầu. Sao lưu không thành công sau khoảng 20 phút. Quá trình sao lưu gia tăng sau đó được khởi động lại và mất khoảng 1 giờ để hoàn thành. Đối với hệ thống này, đây là hành vi sử dụng bộ xử lý thông thường dựa trên các sự kiện đã lên lịch được biết là sẽ xảy ra cho hệ thống.



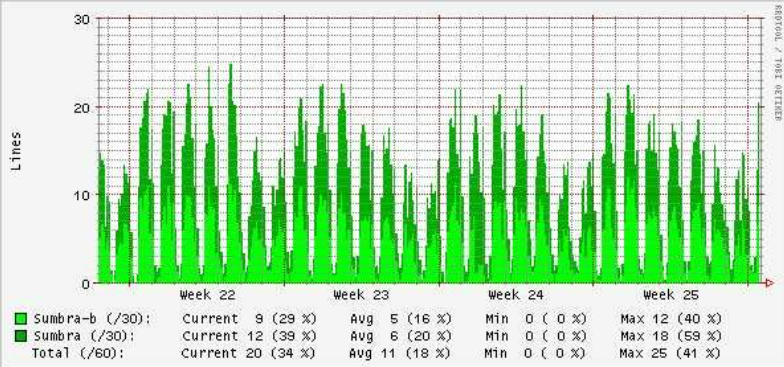
1. **Network Utilization - Việc sử dụng mạng**

Lưu Lượng Vào (Inbound Traffic): Theo dõi lượng dữ liệu được nhận từ mạng. Điều này giúp xác định mức độ sử dụng tài nguyên mạng từ các nguồn bên ngoài và phát hiện các vấn đề như tấn công DDoS.

Lưu Lượng Ra (Outbound Traffic): Giám sát lượng dữ liệu mà máy chủ gửi đi. Điều này giúp theo dõi mức độ sử dụng băng thông của máy chủ đối với các dịch vụ bên ngoài.

Tốc Độ Truyền Tải (Bandwidth Utilization Percentage): Tỷ lệ phần trăm của băng thông mạng đang được sử dụng. Điều này giúp đảm bảo rằng mạng không bị quá tải và các dịch vụ mạng hoạt động trơn tru.

Tỷ Lệ Lỗi Mạng (Network Error Rate): Giám sát số lượng lỗi truyền tải và nhận gói tin để phát hiện sớm các vấn đề phần cứng hoặc cấu hình mạng.



### CÁC TÍNH NĂNG CHÍNH CỦA MRTG.

**5.1. Giám sát lưu lượng mạng:**

* Thu thập dữ liệu SNMP: MRTG sử dụng giao thức SNMP để thu thập dữ liệu về lưu lượng mạng từ các thiết bị như router, switch, và firewall.
* Biểu đồ đồ thị: Dữ liệu được hiển thị dưới dạng đồ thị dễ hiểu, cho phép người dùng theo dõi lưu lượng mạng qua thời gian.

**5.2. Hỗ trợ nhiều thiết bị:**

* Tương thích SNMP: MRTG có thể giám sát bất kỳ thiết bị nào hỗ trợ SNMP, bao gồm các thiết bị của nhiều nhà sản xuất khác nhau.

**5.3. Tính năng lưu trữ dữ liệu:**

* RRDTool: Sử dụng RRDTool để lưu trữ dữ liệu lịch sử và tối ưu hóa việc quản lý dữ liệu lâu dài.

**5.4. Cấu hình đơn giản:**

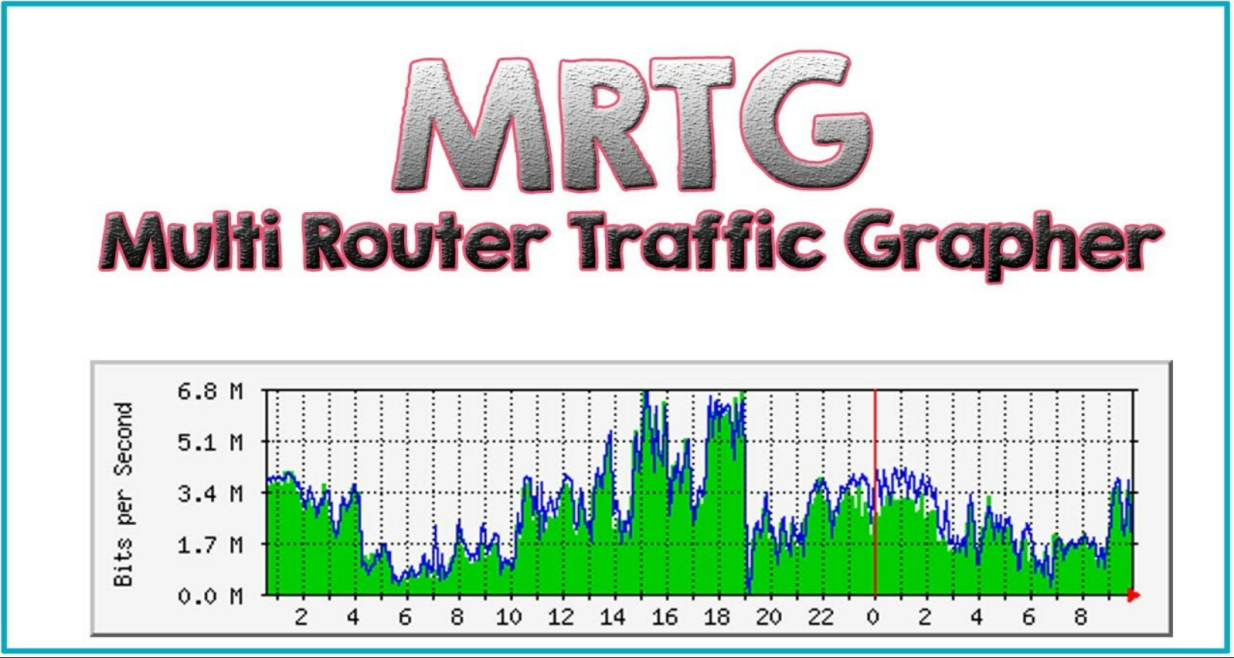
* Tệp cấu hình dễ chỉnh sửa: Các tệp cấu hình đơn giản và dễ hiểu, cho phép người dùng nhanh chóng thiết lập và tùy chỉnh giám sát mạng.
* Tự động hóa cấu hình: Công cụ cfgmaker tự động tạo cấu hình từ thiết bị mạng, giúp tiết kiệm thời gian cấu hình ban đầu.

**5.5. Giao diện web:**

* Truy cập từ xa: Giao diện web cho phép người dùng truy cập và theo dõi dữ liệu từ bất kỳ đâu có kết nối internet.
* Tích hợp dễ dàng: Các đồ thị có thể dễ dàng tích hợp vào các trang web hoặc hệ thống quản lý mạng hiện có.

**5.6. Tùy chỉnh và mở rộng:**

* Đa dạng tùy chọn đồ thị: Người dùng có thể tùy chỉnh các tùy chọn đồ thị theo ý muốn.
* Hỗ trợ nhiều ngôn ngữ lập trình: Có thể tích hợp với các ngôn ngữ lập trình như Perl để mở rộng tính năng.



### ƯU ĐIỂM VÀ NHƯỢC ĐIỂM CỦA VIỆC SỬ DỤNG MRTG TRONG GIÁM SÁT MẠNG.

**ƯU ĐIỂM:**

**Hiểu rõ lưu lượng mạng:**

- Giám sát thời gian thực: Cho phép quản trị viên mạng theo dõi lưu lượng mạng theo thời gian thực, phát hiện kịp thời các vấn đề như quá tải hoặc sự cố mạng.

- Phân tích lịch sử: Dữ liệu lịch sử giúp quản trị viên phân tích xu hướng và đưa ra các quyết định tối ưu hóa mạng.

**Tăng cường hiệu quả quản lý mạng:**

- Phát hiện sự cố nhanh chóng: Giúp phát hiện và xử lý sự cố mạng nhanh chóng trước khi chúng ảnh hưởng lớn đến hệ thống.

- Giảm thời gian downtime: Bằng cách theo dõi và dự đoán các vấn đề tiềm ẩn, MRTG giúp giảm thiểu thời gian ngừng hoạt động của mạng.

**Tối ưu hóa tài nguyên:**

- Quản lý băng thông: Giúp quản trị viên hiểu rõ cách sử dụng băng thông, từ đó tối ưu hóa việc phân bổ tài nguyên mạng.

- Dự đoán nhu cầu: Phân tích xu hướng lưu lượng giúp dự đoán nhu cầu tương lai và lên kế hoạch mở rộng hoặc nâng cấp hệ thống.

**Cải thiện bảo mật mạng:**

- Giám sát các hành vi bất thường: Phát hiện các hành vi bất thường trong lưu lượng mạng, có thể chỉ ra các cuộc tấn công mạng hoặc vi phạm an ninh.

- Cảnh báo kịp thời: Thiết lập cảnh báo khi lưu lượng vượt ngưỡng cho phép, giúp quản trị viên phản ứng kịp thời với các sự cố.

**Chi phí thấp và dễ triển khai:**

- Mã nguồn mở và miễn phí: MRTG là phần mềm mã nguồn mở và miễn phí, giúp tiết kiệm chi phí triển khai và vận hành.

- Dễ cài đặt và cấu hình: Với tệp cấu hình đơn giản và công cụ tự động tạo cấu hình, việc triển khai MRTG dễ dàng và nhanh chóng.

**NHƯỢC ĐIỂM:**

**Giới Hạn Tính Năng:**

- So với các công cụ giám sát mạng khác như Zabbix hay Nagios, MRTG có ít tính năng hơn và thiếu các chức năng giám sát nâng cao như cảnh báo tự động và quản lý sự cố.

**Khó khăn trong việc phát hiện các cuộc tấn công mới:**

- Mặc dù giám sát có thể giúp phát hiện các cuộc tấn công đã biết, nhưng khó khăn để phát hiện các cuộc tấn công mới và chưa được biết đến.

**Khó Khăn Trong Việc Mở Rộng:**

- Khi số lượng thiết bị và các chỉ số giám sát tăng lên, việc mở rộng hệ thống MRTG có thể gặp khó khăn và phức tạp.

**Không Hỗ Trợ Nhiều Loại Dữ Liệu:**

- MRTG chủ yếu được thiết kế để giám sát lưu lượng mạng và các chỉ số SNMP cơ bản, không hỗ trợ tốt cho các loại dữ liệu giám sát khác.

**Khả Năng Cảnh Báo Hạn Chế:**

- MRTG thiếu các tính năng cảnh báo tự động và quản lý sự cố nâng cao, khiến cho việc phát hiện và phản ứng với các sự cố mạng trở nên khó khăn hơn.

**Cần Kiến Thức Về SNMP:**

- Để cấu hình MRTG hiệu quả, quản trị viên cần có kiến thức về SNMP và các OID cụ thể của các thiết bị mạng.

### ỨNG DỤNG THỰC TIỄN CỦA MRTG

* Quản lý băng thông: Doanh nghiệp sử dụng MRTG để giám sát lưu lượng mạng nhằm quản lý và phân bổ băng thông hợp lý. Điều này giúp ngăn chặn tình trạng nghẽn mạng và đảm bảo các ứng dụng quan trọng luôn có băng thông đủ dùng.
* Quản lý dịch vụ khách hàng: ISP có thể sử dụng MRTG để giám sát lưu lượng mạng của các khách hàng. Điều này giúp họ nhanh chóng phát hiện và xử lý các vấn đề mạng, đảm bảo dịch vụ internet ổn định cho khách hàng.
* Quản lý mạng trường học: Các trường học và tổ chức giáo dục có thể sử dụng MRTG để giám sát lưu lượng mạng giữa các tòa nhà hoặc khu vực trong khuôn viên. Điều này giúp đảm bảo hệ thống mạng hoạt động ổn định, hỗ trợ cho việc học tập và nghiên cứu.
* Đảm bảo hệ thống y tế hoạt động liên tục: Bệnh viện và các tổ chức y tế có thể sử dụng MRTG để giám sát hệ thống mạng, đảm bảo các ứng dụng y tế như hệ thống quản lý bệnh nhân và thiết bị y tế kết nối mạng luôn hoạt động ổn định.

## KẾT LUẬN

### TÓM TẮT CÁC ĐIỂM CHÍNH VỀ MRTG

- MRTG vẫn là một công cụ hữu ích và phổ biến trong giám sát mạng, đặc biệt là đối với các tổ chức và doanh nghiệp có nhu cầu giám sát lưu lượng mạng một cách cơ bản và hiệu quả về chi phí. Với sự dễ dàng cài đặt, cấu hình và khả năng hiển thị đồ thị lưu lượng mạng rõ ràng, MRTG vẫn giữ vai trò quan trọng trong việc giúp quản trị viên mạng duy trì hiệu suất và an ninh mạng.

- Đặc điểm mô tả những thuộc tính cố hữu và khả năng của công cụ, trong khi chức năng mô tả các nhiệm vụ và hoạt động cụ thể mà công cụ thực hiện. Hiểu rõ sự khác biệt này giúp quản trị viên mạng đánh giá toàn diện công cụ và tận dụng tối đa khả năng của MRTG trong việc giám sát và quản lý mạng.

- Việc tiếp tục nghiên cứu và phát triển MRTG sẽ giúp nâng cao khả năng giám sát và quản lý mạng, đáp ứng tốt hơn các nhu cầu ngày càng phức tạp của các doanh nghiệp và tổ chức. Tuy vậy, đối với các yêu cầu giám sát phức tạp và mở rộng, các công cụ giám sát hiện đại hơn như Zabbix hay Nagios có thể là lựa chọn tốt hơn nhờ vào tính năng phong phú và khả năng mở rộng cao hơn.

### TRIỂN VỌNG VÀ TRONG TƯƠNG LAI

* MRTG không ngừng phát triển và cải thiện để đáp ứng nhu cầu ngày càng tăng của người dùng trong việc giám sát trên nền tảng Windows hay Linux.
* Với tính ổn định cao và được nhiều người dùng biết tới, MRTG có triển vọng lớn trong tương lai và có thể trở thành một công cụ giám sát quan trọng trong các lĩnh vực công nghiệp khác nhau và tổ chức trên toàn thế giới.

## DEMO

**Mô hình và mô tả thực nghiệm**

### KỊCH BẢN 1 ( ATTACKER TẤN CÔNG TỪ BÊN NGOÀI DMZ)

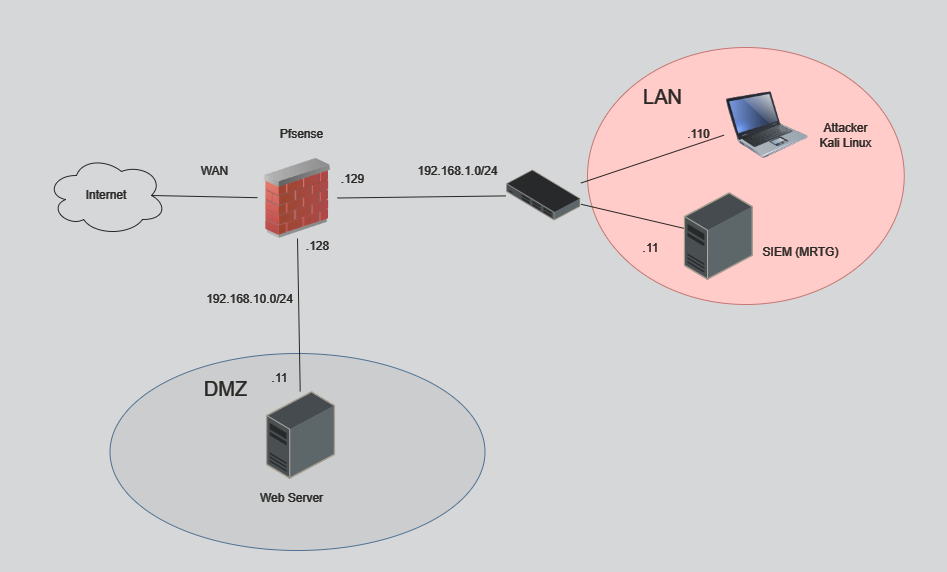
Attacker sử dụng kali linux, sau khi đã thực hiện các biện pháp information gathering đã nắm bắt được mô hình mạng đã triển khai. Attacker nhắm mục tiêu vào Webserver thực hiện tấn công DOS làm server quá tải, khi đó người quản lý hệ thống phải có những công cụ để phát hiện kịp thời sự cố, cùng với đó là đưa ra những biện pháp khắc phục hợp lý. Với sự giúp đỡ của công cụ MRTG, người quản lý có thể phát hiện sự gia tăng đột biến lưu lượng mạng trên các thiết bị của hệ thống.

## IMG_256

Hình 1 Mô hình kịch bản 1

### KỊCH BẢN 2 ( ATTACKER TẤN CÔNG TỪ BÊN LAN VÀO DMZ)

Attacker sử dụng kali linux, sau khi có thể xâm nhập vào hệ thống mạng và có quyền truy cập từ mạng LAN. Attacker nhắm mục tiêu vào Webserver thực hiện tấn công DOS làm server quá tải, khi đó người quản lý hệ thống phải có những công cụ để phát hiện kịp thời sự cố, cùng với đó là đưa ra những biện pháp khắc phục hợp lý. Với sự giúp đỡ của công cụ MRTG, người quản lý có thể phát hiện sự gia tăng đột biến lưu lượng mạng trên các thiết bị của hệ thống

****

Hình 2 Mô hình kịch bản 2

## V. TÀI LIỆU THAM KHẢO

* *Bộ sách nhiều tác giả nxb Bách Khoa Hà Nội.*
* *Essential SNMP & MRTG: Help for System and Network Administrators*
* *SANS Institute Masters, by T.Biran Granier: MRTG used for Basic Server Monitoring*
* [*https://stackoverflow.com/questions/tagged/mrtg*](https://stackoverflow.com/questions/tagged/mrtg)
* [*https://www.youtube.com/watch?v=gZSRd3MU3Vc*](https://www.youtube.com/watch?v=gZSRd3MU3Vc)
* *MRTG - The Multi Router Traffic Grapher*