Tạp chí Tin học và Điều khiển học, T. 19, S. 2 (2003), 117–124

XÂY DỰNG HỆ THỐNG THEO DÕI VÀ ĐIỀU KHIỂN CÁC MÁY TÍNH TRÊN MẠNG INTERNET/INTRANET DỰA TRÊN GIAO THỨC SNMP

NGUYỄN VĂN TAM, PHẠM MINH VĨ, PHẠM THANH GIANG

Viện Công nghệ thông tin

Abstract. In this article we present our research into development of MONITOR&CONTROL system based on SNMP protocol that contains Manager subsystem, Agent subsystem and proxy subsystem. This system is being used in some organizations.

Tóm tắt. Bài báo trình bày kết quả nghiên cứu xây dựng hệ thống theo dõi và điều khiển dựa trên giao thức SNMP. Hệ thống bao gồm hệ quản trị, hệ bị quản trị và hệ uỷ quyền. Hệ thống này đang được sử dụng tại một số tổ chức.

1. ĐẶT VẤN ĐỀ

Ngày nay cùng với sự phát triển mạnh mẽ của mạng máy tính các dịch vụ ngày càng tăng lên về số lượng cũng như độ tin cậy. Việc đòi hỏi phải có nhiều dịch vụ trong hệ thống mạng dẫn tới cần có nhiều máy server để phục vụ người sử dụng. Kéo theo đó sẽ là việc tăng giá thành cho việc theo dõi, điều khiển và bảo trì hệ thống máy server này. Do vậy việc xây dựng một phần mềm có thể theo dõi và điều khiển toàn bộ các server trong hệ thống mạng sẽ giảm được số lượng công việc khi phải thao tác trên từng máy, hơn nữa nó đem lại cho người quản trị một cái nhìn toàn diện về hệ thống.

Mục đích của việc xây dựng phần mềm làm nhiệm vụ theo dõi và điều khiển các server trong hệ thống mạng là để thông qua hệ thống phần mềm này có thể biết được tình trạng của các máy server cũng như các thông tin cấu hình của chúng, đồng thời nhà quản trị cũng có thể thay đổi các thông tin này để các máy server làm việc có hiệu quả. Ngoài ra sự an toàn cho hệ thống phải được đảm bảo, các thông tin của hệ thống không thể bị công bố hay thay đổi một cách bất hợp pháp.

Các công việc cần thiết để xây dựng phần mềm theo dõi và điều khiển các máy tính trong hệ thống mạng gồm có xây dựng giao thức trao đổi thông tin, tập lệnh điều khiển giữa máy theo dõi với máy bị theo dõi và xây dựng hệ thống phần mềm thực hiện.

2. XÂY DỰNG GIAO THỨC

2.1. Định nghĩa giao thức

Giao thức là tập hợp các quy tắc được thoả thuận giữa 2 thực thể truyền thông cho phép việc trao đổi thông tin trong mạng được thực hiện đúng đắn và có hiệu quả ([4]).

Như vậy để xây dựng thành công hệ thống theo dõi và điều khiển các máy trong hệ thống mạng, trước hết là phải xây dựng giao thức truyền nhận dữ liệu trong hệ thống. Điều đó đảm bảo cho việc gửi và nhận đúng thông tin. Tiếp đó là xây dựng tập lệnh để có thể có sự

hiểu giữa hệ theo dõi và điều khiển và hệ bị theo dõi.

Giao thức dùng để phát triển hệ thống theo dõi và điều khiển được xây dựng dựa theo giao thức SNMP. Tuy nhiên giao thức quản trị mạng SNMP được xây dựng để quản lý phần lớn các loại thiết bị mạng ([1, 2]). Nhiệm vụ của hệ thống được xây dựng là quản lý các máy server trong hệ thống mạng. Các server này đều là các máy tính có khả năng xử lý thông tin cao. Do vậy giao thức và tập lệnh xây dựng cần phải cho phép sử dụng chính khả năng xử lý của các máy server này để theo dõi và điều khiển chúng. Giao thức và tập lệnh được xây dựng có một số bổ sung để phù hợp với các yêu cầu của hệ thống được xây dựng.

2.2. Một số đặc tính của giao thức

1) Tương tự như giao thức SNMP, giao thức được xây dựng nằm ở tầng ứng dụng, điều đó làm đơn giản việc trao đổi thông tin giữa các các máy trong mạng vì sẽ không phải quan tâm nhiều đến việc điều khiển gói tin ở tầng thấp.

2) Xây dựng giao thức hoạt động dựa trên giao thức UDP/IP, do vậy không phải kết nối trước khi trao đổi dữ liệu, thông tin được truyền nhanh hơn. Do vậy tốc độ của hệ thống sẽ nhanh hơn khi phải quản lý rất nhiều máy trong hệ thống ([4]).

3) Giao thức gồm 2 lệnh cơ bản là: Get-Request, Get-Response, do vậy sẽ đơn giản việc phân tích gói tin. Hơn nữa đối tượng cần quản lý của hệ thống đều là các máy tính, có khả năng xử lý, phần dữ liệu thể hiện các thông tin yêu cầu.

4) Hệ thống theo dõi và điều khiển và hệ thống bị điều khiển trao đổi dữ liệu qua cổng UDP 161.

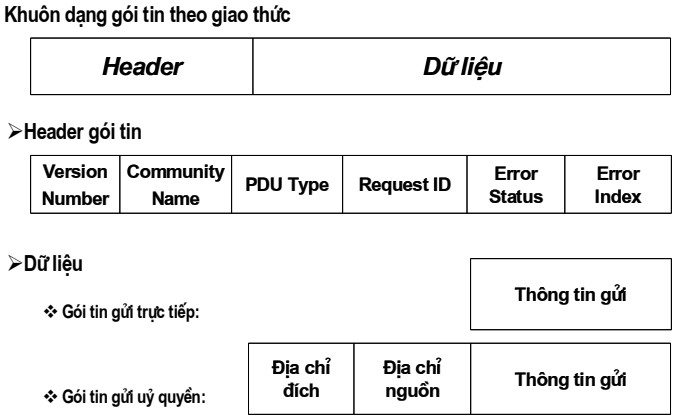
2.3. Khuôn dạng gói tin

Hệ thống phần mềm được xây dựng để theo dõi và điều khiển các máy tính trên mạng INTERNET/INTRANET. Tuy nhiên các máy server thường được bảo vệ bằng cách hạn chế các kết nối hay sử dụng hệ thống bức tường lửa ngăn chặn. Để có thể theo dõi được các server sẽ phải xây dựng hệ thống ủy quyền (proxy). Hệ thống ủy quyền là hệ thống có thể kết nối được với server lại vừa có thể kết nối với hệ theo dõi. Hệ theo dõi và điều khiển sẽ thông qua hệ ủy quyền để quản lý hệ bị theo dõi.

Các máy cần theo dõi và điều khiển thành được phân thành 2 loại là kết nối trực tiếp và kết nối thông qua hệ thống ủy quyền. Các máy bị theo dõi theo kiểu kết nối trực tiếp là các máy có thể kết nối trực tiếp với hệ theo dõi. Các máy bị theo dõi thông qua hệ thống ủy quyền là các máy có thể không kết nối trực tiếp với máy theo dõi. Để có thể quản lý các máy bị theo dõi trong trường hợp này, máy theo dõi phải thông qua ủy quyền để có thể trao đổi thông tin với máy bị theo dõi.

Trong cấu trúc gói tin trao đổi của trường hợp theo dõi thông qua ủy quyền phải có thông tin thêm, làm nhiệm vụ xác định con đường trao đổi thông tin giữa máy theo dõi và máy bị theo dõi.

Cấu trúc gói tin được xây dựng như trên Hình 1. Cấu trúc gói tin bao gồm phần đầu gói tin và phần dữ liệu. Phần đầu gói tin là các thông tin chung về gói tin bao gồm phiên bản, tên cộng đồng (xác định nhóm sử dụng), kiểu gói tin, số hiệu gói tin, chỉ số lỗi và trạng thái lỗi (nếu có). Phần dữ liệu có khác nhau giữa gói tin gửi trực tiếp và gói tin gửi thông qua ủy quyền. Gói tin gửi trực tiếp chỉ mang dữ liệu đơn thuần là thông tin cần trao đổi, còn gói tin gửi thông qua ủy quyền phải có thêm thông tin để xác định đường đi cho gói tin. Thông tin này gồm có địa chỉ đích cần gửi tới và địa chỉ nguồn phát gói tin đi. Trong quá trình gói tin được truyền trong hệ thống, địa chỉ đích sẽ là địa chỉ để hệ thống xác định đường cho gói tin. Địa chỉ nguồn sẽ được dùng trong gói tin trả lời.



Hình 1. Cấu trúc gói tin

3. THIẾT KẾ TẬP LỆNH

Hệ thống xây dựng 2 kênh lệnh:

3.1. Kênh lệnh shell

Hệ thống sử dụng các lệnh shell để tận dụng khả năng của hệ điều hành của chính máy bị theo dõi. Các lệnh này chính là các lệnh của hệ điều hành của máy bị theo dõi. Khi máy bị theo dõi nhận được yêu cầu nó thực hiện các lệnh này bằng các lệnh shell của hệ điều hành. Kết qủa thực hiện được lưu ra tệp, sau đó nội dung tệp này sẽ được gửi lại cho hệ theo dõi. Kết qủa này được chia thành nhiều gói tin nhỏ và gửi theo thứ tự cho hệ theo dõi. Các gói được ký hiệu và đánh số thứ tự để hệ theo dõi và điều khiển có thể xác định được đầu tệp, kết thúc tệp và thứ tự các gói tin. Thông qua thứ tự của các gói tin hệ theo dõi và điều khiển sẽ xác định được việc mất mát gói tin và có thể yêu cầu truyền lại.

Việc chia nhỏ và kiểm soát việc truyền thông tin nhằm nâng cao khả năng an toàn cho việc truyền tin. Đây là công việc rất cần thiết khi việc truyền tin theo kiểu không liên kết (connectionless) hoạt động dựa trên giao thức UDP ([4]).

3.2. Kênh lệnh người dùng (user)

Các lệnh mà hệ thống phải tự định nghĩa và hoạt động. Các lệnh này được gọi là lệnh người dùng. Kênh lệnh người dùng không phải để yêu cầu hệ bị theo dõi thực hiện các lệnh của hệ điều hành, mà các lệnh này sẽ được thực hiện bởi hệ thống bị theo dõi và gửi lại kết qủa cho hệ theo dõi và điều khiển. Các lệnh người dùng được sử dụng như các thông báo của hệ bị theo dõi với hệ theo dõi và điều khiển, và các yêu cầu gửi nhận tệp, cập nhật hay thay đổi cấu hình hệ thống. Các lệnh người dùng được xây dựng sao cho không trùng với các lệnh của hệ điều hành. Sự ưu tiên sẽ dành cho lệnh người dùng nếu có lệnh shell trùng với lệnh người dùng.

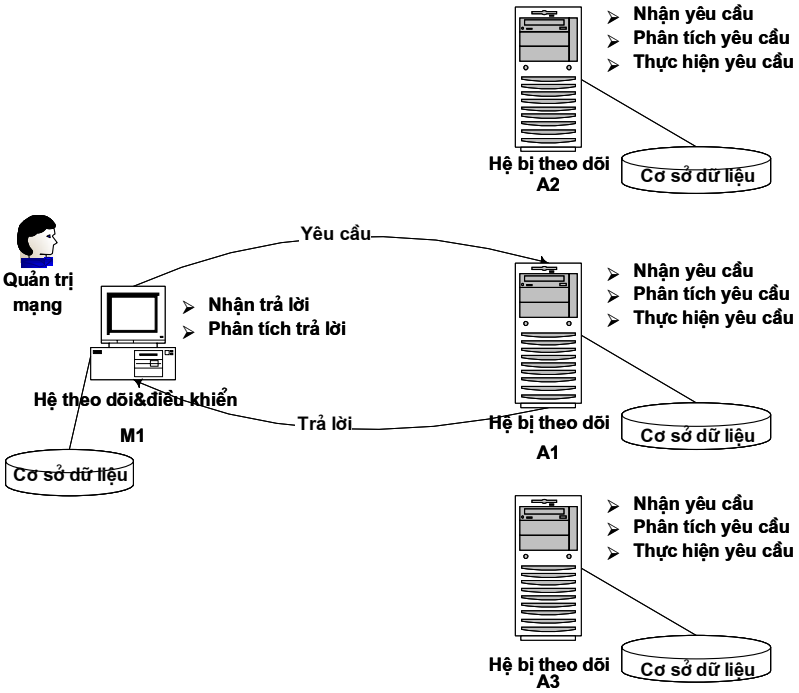
4. XÂY DỰNG PHẦN MỀM

4.1. Mô hình hệ thống

- **Theo dõi và điều khiển trực tiếp**

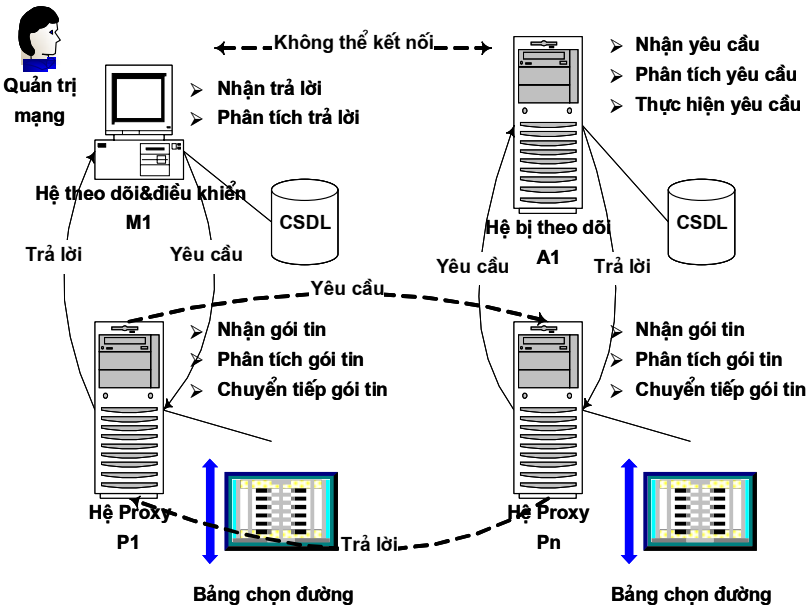
Hệ theo dõi và điều khiển có thể kết nối trực tiếp với hệ bị theo dõi. Người quản trị

thông qua hệ theo dõi và điều khiển đưa ra yêu cầu trực tiếp tới hệ bị theo dõi. Hệ bị theo dõi nhận yêu cầu, phân tích yêu cầu nhận được. Sau đó hệ bị theo dõi thực hiện yêu cầu và gửi kết qủa cho hệ theo dõi và điều khiển. Hệ theo dõi và điều khiển nhận trả lời, phân tích câu trả lời để phục vụ cho hệ thống: hiển thị thông tin, thông báo tình trạng, ...



Hình 2. Mô hình quản lý trực tiếp

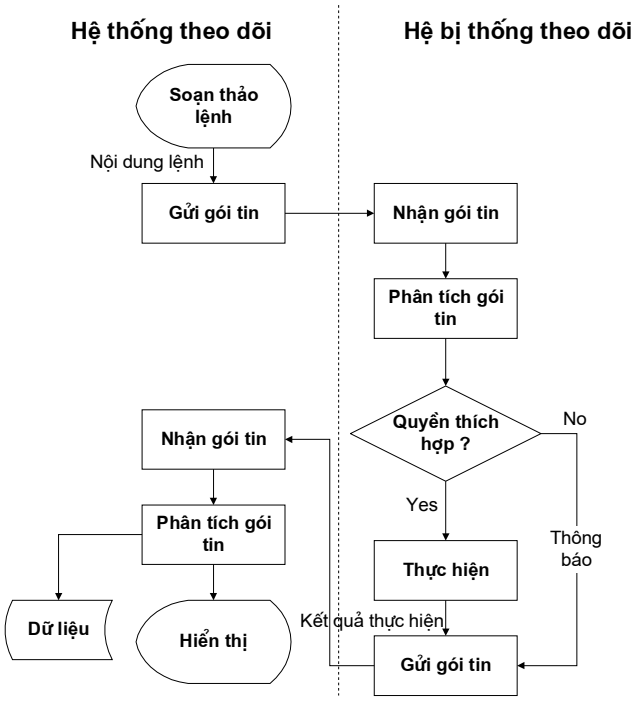
- **Quản lý thông qua ủy quyền**



Hình 3. Mô hình quản lý thông qua hệ ủy quyền

Hệ theo dõi và điều khiển không thể kết nối trực tiếp với hệ bị theo dõi. Hệ theo dõi và điều khiển sẽ thông qua một hệ thống khác để chuyển gói tin là hệ ủy quyền. Hệ ủy quyền sẽ chuyển tiếp gói tin tới máy bị theo dõi. Gói tin từ máy theo dõi và điều khiển tới máy bị theo dõi có thể qua một hay nhiều máy ủy quyền. Hệ ủy quyền có nhiệm vụ chọn đường đi tiếp theo cho gói tin. Khi nhận được gói tin gửi đến hệ ủy quyền đọc gói tin để xác định địa chỉ đích cần đến và căn cứ vào bảng chọn đường để chuyển gói tin đến địa chỉ tiếp theo.

Sơ đồ mô tả trao đổi thông tin giữa hệ theo dõi và hệ bị theo dõi như sau.



Hình 4. Sơ đồ trao đổi thông tin

Các chức năng xử lý thông tin chủ yếu nằm trên hệ theo dõi và điều khiển. Các chức năng của hệ bị theo dõi được thiết kế đơn giản để có thể chạy tự động. Hệ bị theo dõi tự động nhận lệnh, tự động phân tích lệnh, thực hiện và gửi kết qủa trả lời cho hệ thống theo dõi.

4.2. Hệ theo dõi và điều khiển

Hệ theo dõi và điều khiển được thiết kế cho nhà quản trị có thể theo dõi toàn bộ hệ thống. Do vậy chức năng của hệ theo dõi được thiết kế phức tạp để có thể đáp ứng được các yêu cầu của người quản trị. Ngoài ra hệ phải có giao diện đồ hoạ thân thiện nhằm giúp người quản trị có thể dễ dàng khai thác và sử dụng hệ thống. Hệ theo dõi được cài đặt trên Môi trường Window, có giao diện thân thiện.

Các chức năng của hệ theo dõi gồm có:

• Quản lý người dùng

Hệ theo dõi và điều khiển có nhiệm vụ quản lý người sử dụng, phân chia người sử dụng hệ thống theo các nhóm quyền. Việc quản lý người sử dụng nhằm bảo đảm cho sự an toàn của hệ thống, ngăn chặn sự thâm nhập bất hợp pháp. Mỗi người sử dụng mới được đăng ký sẽ được cung cấp một tên truy nhập và mật khẩu truy nhập hệ thống. Mật khẩu mà người dùng được cung cấp sẽ được mã hoá bằng hàm băm để được một chuỗi 64 byte và lưu trên

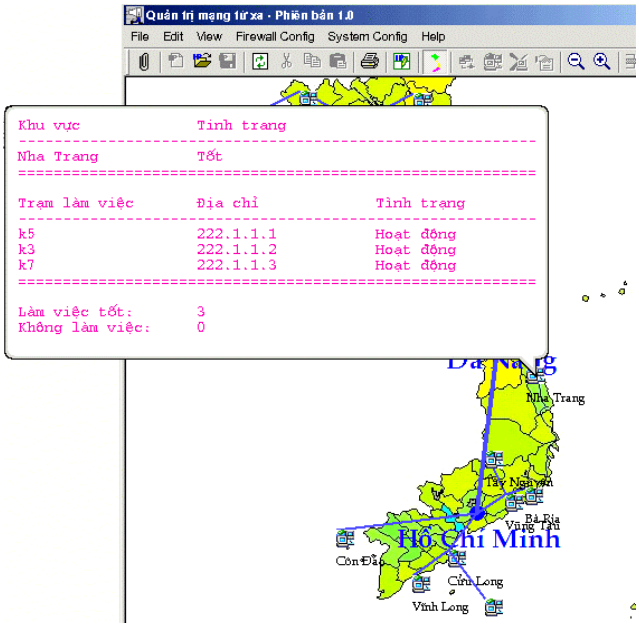
đĩa.

Khi người dùng sử dụng hệ thống phải nhập tên truy nhập và mật khẩu đúng. Hệ thống sẽ căn cứ vào tên truy nhập thuộc nhóm quyền nào để cung cấp cho người sử dụng khả năng sử dụng hệ thống. Hệ thống theo dõi và điều khiển sử dụng 3 nhóm quyền là: quyền quản trị, quyền đọc ghi và quyền chỉ đọc. Mức độ sử dụng hệ thống sẽ giảm theo các quyền này.

- **Quản lý thông tin hệ bị theo dõi**

Quản lý thông tin của hệ bị theo dõi bao gồm các thông tin để xác định địa chỉ của hệ bị theo dõi, cách thức trao đổi thông tin với hệ thống bị theo dõi (trực tiếp hay thông qua ủy quyền), tên cộng đồng (community name) tương ứng với các quyền truy nhập hệ thống bị theo dõi,... Các máy được quản lý theo các trạm, tương ứng với một trạm hay một phòng làm việc trên hệ thống mạng. Mỗi trạm này có thể có một hoặc nhiều máy. Các trạm này cũng được quản lý theo hình cây tương ứng với việc quản lý từ các trung tâm lớn xuống các trung tâm nhỏ.

Như vậy người quản trị sẽ có cái nhìn tổng quan khi theo dõi toàn bộ hệ thống. Căn cứ vào bản đồ hệ thống người quản trị có thể xác định được tình trạng thông mạng trong các trạm và giữa các trạm.

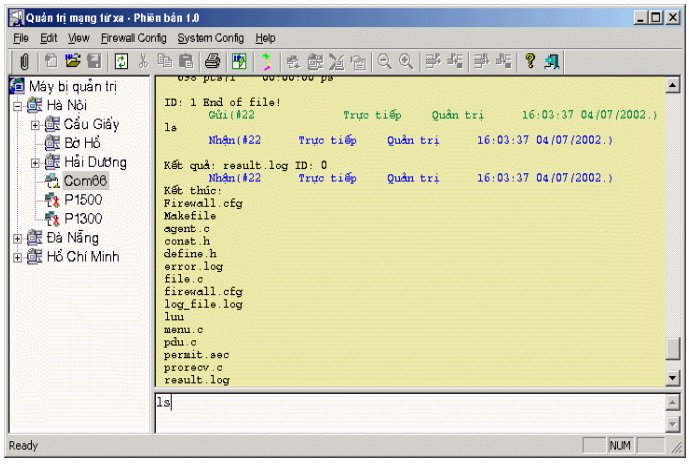


Hình 5. Thông tin về các máy bị theo dõi

- **Theo dõi và điều khiển**

Đây là chức năng cơ bản của hệ theo dõi và điều khiển. Chức năng này có nhiệm vụ cho phép người dùng nhập yêu cầu để gửi tới hệ bị theo dõi nào đó. Sau khi hệ theo dõi sẽ phân tích yêu cầu để tạo ra gói tin có định dạng thích hợp và gửi gói tin đó cho hệ bị theo dõi. Tiếp theo nó sẽ đợi trả lời từ hệ bị theo dõi. Khi nhận được trả lời nó sẽ tiến hành phân tích để nhận được thông tin cần thiết và hiển thị cho người sử dụng.

Như vậy chức năng này sẽ có 2 giao diện, một là giao diện nhập yêu cầu và giao diện hiển thị câu trả lời.



Hình 6. Màn hình làm việc của hệ thống

Thông qua chức năng này người dùng có thể biết được tình trạng của hệ thống bị theo dõi và có thể thay đổi các thông tin này một cách thích hợp.

Các mô đun chính của hệ theo dõi và điều khiển:

- **Môđun gửi nhận gói tin từ tầng UDP/IP**

Môđun gửi nhận gói tin từ tầng UDP/IP có chức năng khởi tạo socket kiểu UDP. Socket này truyền và nhận dữ liệu tại cổng 161. Gửi nhận dữ liệu ở tầng UDP/IP. Ghi lại và thông báo các sự cố ở tầng UDP/IP.

- **Môđun tạo/phân tích gói tin**

Môđun tạo và phân tích gói tin có chức năng là từ thông tin cần gửi và phương thức gửi sẽ đóng gói gói tin theo giao thức đã xây dựng. Đồng thời nó cũng có chức năng phân tích gói tin nhận được để có thông tin hữu ích.

4.3. Hệ thống bị theo dõi

- **Hệ bị theo dõi**

Hệ bị theo dõi giúp nhà quản trị từ hệ thống theo dõi và quản trị có thể nhận được câu trả lời. Do vậy nó có nhiệm vụ tự động nhận yêu cầu, phân tích yêu cầu, thực hiện yêu cầu và gửi lại kết qủa cho hệ theo dõi và điều khiển.

Chức năng quan trọng nhất của hệ bị theo dõi là thực hiện yêu cầu của hệ theo dõi. Hệ bị theo dõi luôn lắng nghe các yêu cầu của hệ theo dõi. Mỗi khi nhận được yêu cầu của hệ theo dõi, hệ bị theo dõi sẽ tiến hành phân tích cấu trúc gói tin. Sau khi phân tích thành công gói tin, hệ này sẽ kiểm tra quyền truy nhập từ xa thông qua tên cộng đồng (community name) của gói tin. Nếu quyền truy nhập thỏa mãn nó sẽ tiến hành thực hiện yêu cầu và gửi lại kết qủa cho hệ theo dõi bằng gói tin được định dạng theo yêu cầu của hệ thống. Việc xác định quyền của người sử dụng đảm bảo cho hệ thống được hoạt động an toàn.

Hệ bị theo dõi còn ghi lại các sự kiện xảy ra như là một tệp nhật ký. Các thông tin được ghi lại là các yêu cầu, thời gian của yêu cầu được gửi đến, các lỗi xảy ra trong hệ thống (lỗi trên đường truyền, lỗi định dạng gói tin) các yêu cầu bất hợp pháp. Người theo dõi có thể xem các thông tin này để từ đó có hướng phát triển cho hệ thống mạng.

- **Hệ ủy quyền**

Nhiệm vụ của hệ thống này đơn giản hơn hai hệ thống trên. Nó chỉ có nhiệm vụ nhận gói tin, phân tích gói tin. Việc phân tích gói tin để nhận được địa chỉ cần gửi tới. Sau đó nó sẽ căn cứ vào bảng chọn đường để tìm ra địa chỉ tiếp theo cần chuyển gói tin tới và chuyển

gói tin tới địa chỉ này.

Trên hệ thống ủy quyền có lưu giữ bảng chọn đường. bảng này gồm thông tin địa chỉ của máy đích (Destination) và địa chỉ cần gửi qua (Next Host) để có thể tới được máy đích.

Destination Address		Next Host Address

Khi hệ ủy quyền nhận được gói tin chuyển đến, nó sẽ so sánh địa chỉ đích của gói tin với địa chỉ của chính nó. Nếu khác, nó sẽ tiếp tục so sánh địa chỉ đích của gói tin với địa chỉ đích trong bảng chọn đường, trong trường hợp tìm thấy nó sẽ chuyển gói tin đến địa chỉ cần gửi qua (Next Host).

Một gói tin có thể qua một hay nhiều hệ ủy quyền. Hệ ủy quyền chỉ biết địa chỉ tiếp theo cần chuyển gói tin tới chứ không biết toàn bộ đường đi của gói tin.

5. KẾT LUẬN

Bài báo trình bày một số kết qủa nghiên cứu và xây dựng hệ thống phần mềm theo dõi và điều khiển các máy tính trong hệ thống mạng INTERNET/INTRANET. Các kết quả chính là: phần mềm hệ theo dõi và điều khiển hoạt động trên hệ điều hành Window [5, 6, 7] có giao diện thân thiện, phần mềm hệ bị theo dõi và hệ ủy quyền hoạt động trên hệ điều hành Linux và có thể chạy tự động như một dịch vụ ([8, 9]). Thông qua hệ thống phần mềm nhà quản trị mạng có thể biết được các thông tin về tài nguyên và cấu hình của các máy bị theo dõi trong hệ thống. Nhà quản trị có thể dừng các dịch vụ, khởi động các dịch vụ và thay đổi cấu hình các máy bị theo dõi.

Hệ thống được xây dựng theo chuẩn của các hệ quản trị mạng và đưa thêm hệ thống uỷ quyền điều khiển nhằm định tuyến các gói tin, uỷ quyền quản lý và cấu hình cho các hệ thống Server được bảo vệ bởi bức tường lửa.

Hệ thống phần mềm này là công cụ hỗ trợ rất đắc lực cho các nhà quản trị mạng theo dõi và điều khiển các server trong hệ thống mạng. Phần mềm này giúp nhà quản trị bớt được thời gian và công sức khi phải di chuyển để quản lý các server này. Hệ thống phần mềm này được ứng dụng cho các hệ thống mạng của các nhà cung cấp dịch vụ lớn hoặc các công ty nhỏ với hệ thống mạng riêng.

TÀI LIỆU THAM KHẢO

[1] J. Case, M. Fedor, M. Schoffstall, J. Davin, *RFC 1157- A Simple Network Management Protocol*, 1990.

[2] M. Rose, K. McCloghrie, *RFC 1065- Structure and Identification of Management Information for TCPIP-based internets*, 1988.

[3] Tổng cục Bưu Điện, Tổng công ty Bưu Chính Viễn thông, *Chuyển mạch số và các hệ thống quản lý*, Nhà xuất bản Khoa học Kỹ thuật, 1997.

[4] Douglas E. Comber, *Internet working with TCP/IP, Principles, Protocol and Architecture*, Vol. 1, Prentice-Hall International, "ISBN 0-13-474321-0", 1991.

[5] Anthony Jones and Jim Ohlund, *Network Programming for Microsoft Windows*, 1999.

[6] Martin Hall, *Window Sockets 2, Application Programming Interface*, Revision 2.0.8, 1995.

[7] David J. Kruglinski, *Programming Microsoft Visual C++*, 1998.

[8] Nguyễn Phương Lan, Hoàng Đức Hải, *Lập trình Linux,* Nhà xuất bản Giáo dục, 1998.

[9] Richard Stevens, *UNIX Network Programming.* PTR Prentice-Hall, Englewood Cliffs, New Jersey 07632, 1990.

Nhận bài ngày 28 - 10 - 2002