# ĐỀ XUẤT XÂY DỰNG HỆ THỐNG QUẢN LÝ, GIÁM SÁT VÀ CẢNH BÁO TẬP TRUNG TRONG MẠNG VNPT

**Nguyễn Hữu Phát*, Vũ Đức Dũng†**

*Bộ môn Mạch và Xử lý tín hiệu, Viện Điện tử viễn thông, Đại học Bách Khoa Hà Nội

† Trung tâm Điều hành Thông tin VNPT, Hà Nội

***Tóm tắt:*** Trong bối cảnh hiện nay việc nâng cao chất lượng để cạnh tranh trong thị trường cung cấp dịch vụ viễn thông và công nghệ thông tin là cần thiết. Việc áp dụng các công cụ phần mềm vào quy trình nghiệp vụ nâng cao chất lượng công tác quản lý là một trong những giải pháp mang lại hiệu quả cao. Trong công tác quản lý vận hành khai thác hạ tầng mạng viễn thông và công nghệ thông tin, có rất nhiều loại thiết bị khác nhau với nhiều hệ thống quản lý riêng và có nhiều loại cảnh báo với mức độ khác nhau. Tuy nhiên, nhược điểm của các hệ thống này còn rời rạc và tốn nhiều nhân công. Do vậy việc chủ động phát hiện và xử lý cảnh báo thường gặp nhiều khó khăn. Để thuận tiện cho việc quản lý và phát hiện cảnh báo nhanh cũng như theo dõi được tiến trình xử lý trên mạng viễn thông, bài báo đề xuất xây dựng phần mềm quản lý và giám sát cảnh báo tập trung áp dụng trên các hệ thống khác nhau (MAN-E, PSTN, mạng truyền dẫn IP,...) nhằm trợ giúp các đơn vị khai thác và vận hành hệ thống hạ tầng mạng một cách trực quan, chính xác, tự động hóa cao, tích hợp các hệ thống giám sát và mang lại hiệu quả cao. Kết quả thử nghiệm với dữ liệu hệ thống CCSM nhận được từ 15/9/2019 đến 15/10/2019 chúng tôi nhận thấy nếu theo nhóm cảnh báo thì nhóm băng rộng là nhóm có nguy cơ cao nhất với rủi ro nhiều hơn với 7305 bản tin. Tuy nhiên nếu theo loại bản tin thì bản tin chuyển xuống ($DOWN_TK$) lại là bản tin gửi nhiều hơn với 3189 bản tin.

***Từ khóa:*** Short Message Service, SNMP, SignalR, MVC, CSSM.

## I. ĐẶT VẤN ĐỀ

Thực trạng mạng lưới VNPT hiện nay đang tồn tại các vấn đề như sau [1]–[3]:

- Chưa có một phần nào để giám sát tập trung mạng lưới các thiết bị cung cấp dịch.
- Việc theo dõi, phát hiện cảnh báo còn rời rạc, manh mún chưa tập trung thống nhất, gây khó khăn cho việc tìm kiếm, thống kê và đôn đốc xử lý cảnh báo.
- Chưa có hệ thống thống kê các cảnh báo đã diễn ra theo từng hệ thống khai thác để làm số liệu phân tích, phán đoán các cảnh báo đã diễn ra và có thể xảy ra trong tương lai.
- Việc tiếp nhận và cập nhật lên các hệ thống cảnh báo qua nhiều đơn vị, phòng ban nên gây thời gian phát hiện và xử lý cảnh báo kéo dài.

Do vậy mục tiêu của bài báo là đề xuất xây dựng hệ thống quản lý giám sát cảnh báo tập trung mạng băng rộng, PSTN (Public Switched Telephone Network), và truyền dẫn IP (Internet Protocol) gọi chung là CSSM gồm các chức năng:

- Module phần mềm cho phép cập nhật các sự cố đang diễn ra. Cho phép tổng hợp, thống kê để theo dõi biến động về sự cố.
- Cách thức kết nối và lệnh đọc thông tin sự cố của các thiết bị.
- Công cụ phần mềm tự động, định kỳ kết nối và thực hiện các lệnh khai thác vào thiết bị đọc các thông tin như bản tin sự cố, thời gian, mã loại sự cố của thiết bị, cập nhật vào cơ sở dữ liệu phục vụ theo dõi các biến động của thiết bị.
- Thông tin về sự cố của thiết bị, hệ thống được cập nhật tự động, định kỳ, chính xác, tiết kiệm thời gian và chi phí cập nhật nhân công.
- Quản ký, theo dõi chặt chẽ luồng phiếu, quy trình xử lý đối với các nhóm sự cố.
- Cho phép tìm kiếm, thống kê và lập báo cáo thống kê với từng nhóm sự cố, hệ thống được nhanh chóng và chính xác.
- Hoàn thành quy trình cập nhật, điều hành, quản lý và khai thác hệ thống, sự cố một cách triệt để.

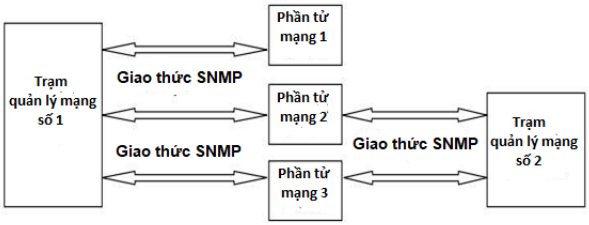
Phần còn lại của bài báo được trình bày như sau. Trong phần II chúng tôi sẽ trình bày về các lý thuyết liên quan đến hệ thống đề xuất. Trong phần III và phần IV, chúng tôi lần lượt trình bày mô hình và đánh giá kết quả của mô hình để ra. Cuối cùng, chúng tôi kết luận bài báo trong phần V.

## II. CƠ SỞ LÝ THUYẾT

Hệ thống sửa dụng hệ quản trị cơ sở dữ liệu (CSDL) SQL Server phiên bản 2014, ngôn ngữ lập trình C và mô hình triển khai web là ASP.NET MVC phiên bản 4.0 trở nên [4]–[6]. Công cụ quét và truy vấn thông tin sự cố trực tiếp sử dụng giao thức SNMP (Simple Network Management Protocol), SSH, SignalR, bảng Entity-MIB là chủ yếu. Dưới đây là mô tả tổng quan về các giao thức, nền tảng công nghệ phục vụ triển khai hệ thống [7].

Tác giả liên hệ: Nguyễn Hữu Phát
Email: phat.nguyenhuu@hust.edu.vn
Đến tòa soạn: 4/2020, chỉnh sửa 05/2020, chấp nhận đăng: 6/2020

SNMP là một tập hợp các thủ tục mà các bên tham gia cần tuân theo để có thể giao tiếp được với nhau [6], [8], [9], [11]. Trong lĩnh vực thông tin, một giao thức quy định cấu trúc, định dạng (format) của dòng dữ liệu trao đổi với nhau và quy định trình tự, thủ tục để trao đổi dòng dữ liệu đó. Nếu một bên tham gia gửi dữ liệu không đúng định dạng hoặc không theo trình tự thì các bên khác sẽ không hiểu hoặc từ chối trao đổi thông tin. SNMP là một giao thức, do đó nó có những quy định riêng mà các thành phần trong mạng phải tuân theo. Một thiết bị hiểu được và hoạt động tuân theo giao thức SNMP được gọi là "có hỗ trợ SNMP" (SNMP supported) hoặc "tương thích SNMP" (SNMP compartible) [14]÷[17].




*Hình 1. Sơ đồ hoạt động của SNMP dựa trên [8], [9].*

SNMP dùng để quản lý, nghĩa là có thể theo dõi, có thể lấy thông tin, có thể được thông báo, và có thể tác động để hệ thống hoạt động như ý muốn. Ví dụ một số khả năng của phần mềm SNMP gồm:

- Theo dõi tốc độ đường truyền của một router, biết được tổng số byte đã truyền/nhận.
- Lấy thông tin máy chủ đang có bao nhiêu ổ cứng, mỗi ổ cứng còn trống bao nhiêu.
- Tự động nhận cảnh báo khi switch có một port bị down.
- Điều khiển tắt (shutdown) các port trên switch.

SNMP là giao thức đơn giản, do nó được thiết kế đơn giản trong cấu trúc bản tin và thủ tục hoạt động, và còn đơn giản trong bảo mật (ngoại trừ SNMP version 3). Sử dụng phần mềm SNMP, người quản trị mạng có thể quản lý, giám sát tập trung từ xa toàn mạng của mình.

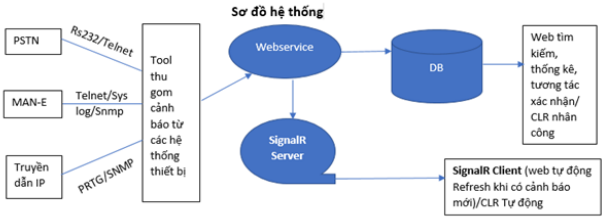
Theo RFC1157 [11], kiến trúc của SNMP bao gồm 2 thành phần: các trạm quản lý mạng (network management station) và các thành tố mạng (network element). Network management station thường là một máy tính chạy phần mềm quản lý SNMP (SNMP management application), dùng để giám sát và điều khiển tập trung các network element như trên hình 1 [14]÷[17].

Network element là các thiết bị, máy tính, hoặc phần mềm tương thích SNMP và được quản lý bởi network management station. Như vậy element bao gồm device, host và application.

Giao thức SNMPv1 có 5 phương thức hoạt động, tương ứng với 5 loại bản tin gồm GetRequest, GetNextRequest, SetRequest, GetResponse, và Trap. Mỗi bản tin đều có chứa OID để cho biết object mang trong nó là gì. OID trong GetRequest cho biết nó muốn lấy thông tin của object nào. OID trong GetResponse cho biết nó mang giá trị của object nào. OID trong SetRequest chỉ ra nó muốn thiết lập giá trị cho object nào. OID trong Trap chỉ ra nó thông báo sự kiện xảy ra đối với object nào.

Bản tin GetRequest được manager gửi đến agent để lấy một thông tin nào đó. Trong GetRequest có chứa OID của object muốn lấy. Ví dụ muốn lấy thông tin tên của Device1 thì manager gửi bản tin GetRequest OID=1.3.6.1.2.1.1.5 đến Device1, tiến trình SNMP agent trên Device1 sẽ nhận được bản tin và tạo bản tin trả lời. Trong một bản tin GetRequest có thể chứa nhiều OID, nghĩa là dùng một GetRequest có thể lấy về cùng lúc nhiều thông tin. Bản tin GetNextRequest cũng dùng để lấy thông tin và cũng có chứa OID, tuy nhiên nó dùng để lấy thông tin của object nằm kế tiếp object được chỉ ra trong bản tin.


*Hình 2. Sơ đồ kiến trúc hệ thống [13].*




*Hình 3. Sơ đồ kết nối tổng quát [13].*

Tại sao phải có phương thức GetNextRequest. Như ta đã biết khi đọc qua những phần trên: một MIB bao gồm nhiều OID được sắp xếp thứ tự nhưng không liên tục, nếu biết một OID thì không xác định được OID kế tiếp. Do đó ta cần GetNextRequest để lấy về giá trị của OID kế tiếp. Nếu thực hiện GetNextRequest liên tục thì ta sẽ lấy được toàn bộ thông tin của agent.

Bản tin SetRequest được manager gửi cho agent để thiết lập giá trị cho một object nào đó. Ví dụ: Có thể đặt lại tên của một máy tính hay router bằng phần mềm SNMP manager, bằng cách gửi bản tin SetRequest có OID là 1.3.6.1.2.1.1.5.0 (sysName.0) và có giá trị là tên mới cần đặt. Có thể shutdown một port trên switch bằng phần mềm SNMP manager, bằng cách gửi bản tin có OID là 1.3.6.1.2.1.2.2.1.7 và có giá trị là 2. Nó có thể mang 3 giá trị là UP (1), DOWN (2) và TESTING (3).

Mỗi khi SNMP agent nhận được các bản tin GetRequest, GetNextRequest hay SetRequest thì nó sẽ gửi lại bản tin GetResponse để trả lời. Trong bản tin GetResponse có chứa OID của object được request và giá trị của object đó.

Bản tin Trap được agent tự động gửi cho manager mỗi khi có sự kiện xảy ra bên trong agent, các sự kiện này không phải là các hoạt động thường xuyên của agent mà là các sự kiện mang tính biến cố. Ví dụ: Khi có một port down, khi có một người dùng login không thành công, hoặc khi thiết bị khởi động lại, agent sẽ gửi trap cho manager.

Để thực hiện công việc quét thông tin vật tư thiết bị băng rộng đang hoạt động trên mạng lưới, bài báo thực hiện nghiên cứu mô tả trong bảng ENTITY-MIB được mô tả trong RFC4133. Với các OID và thông tin được mô tả như bảng I.

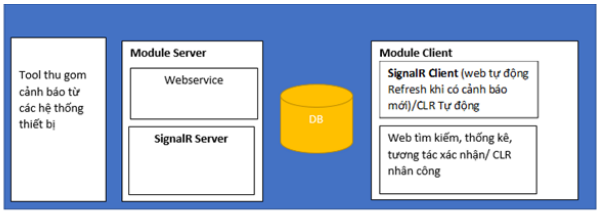
*Bảng I.* BẢNG ENTITY - MIB.

| Đối tượng | ID đối tượng | Loại |
|---|---|---|
| entityMIB | 1.3.6.1.2.1.47 | MODULE-IDENTITY |
| entPhysicalSoftwareRev | 1.3.6.1.2.1.47.1.1.1.1.10 | OBJECT-TYPE |
| entPhysicalSerialNum | 1.3.6.1.2.1.47.1.1.1.1.11 | OBJECT-TYPE |
| entPhysicalMfgName | 1.3.6.1.2.1.47.1.1.1.1.12 | OBJECT-TYPE |
| entPhysicalModelName | 1.3.6.1.2.1.47.1.1.1.1.13 | OBJECT-TYPE |
| entPhysicalVendorType | 1.3.6.1.2.1.47.1.1.1.3 | OBJECT-TYPE |
| entPhysicalContainedIn | 1.3.6.1.2.1.47.1.1.1.4 | OBJECT-TYPE |
| entPhysicalParentRelPos | 1.3.6.1.2.1.47.1.1.1.6 | OBJECT-TYPE |
| entPhysicalHardwareRev | 1.3.6.1.2.1.47.1.1.1.8 | OBJECT-TYPE |
| entAliasLogicalIndexOrZero | 1.3.6.1.2.1.47.1.3.2.1.1 | OBJECT-TYPE |
| entAliasMappingIdentifier | 1.3.6.1.2.1.47.1.3.2.1.2 | OBJECT-TYPE |
| entPhysicalChildIndex | 1.3.6.1.2.1.47.1.3.3.1.1 | OBJECT-TYPE |

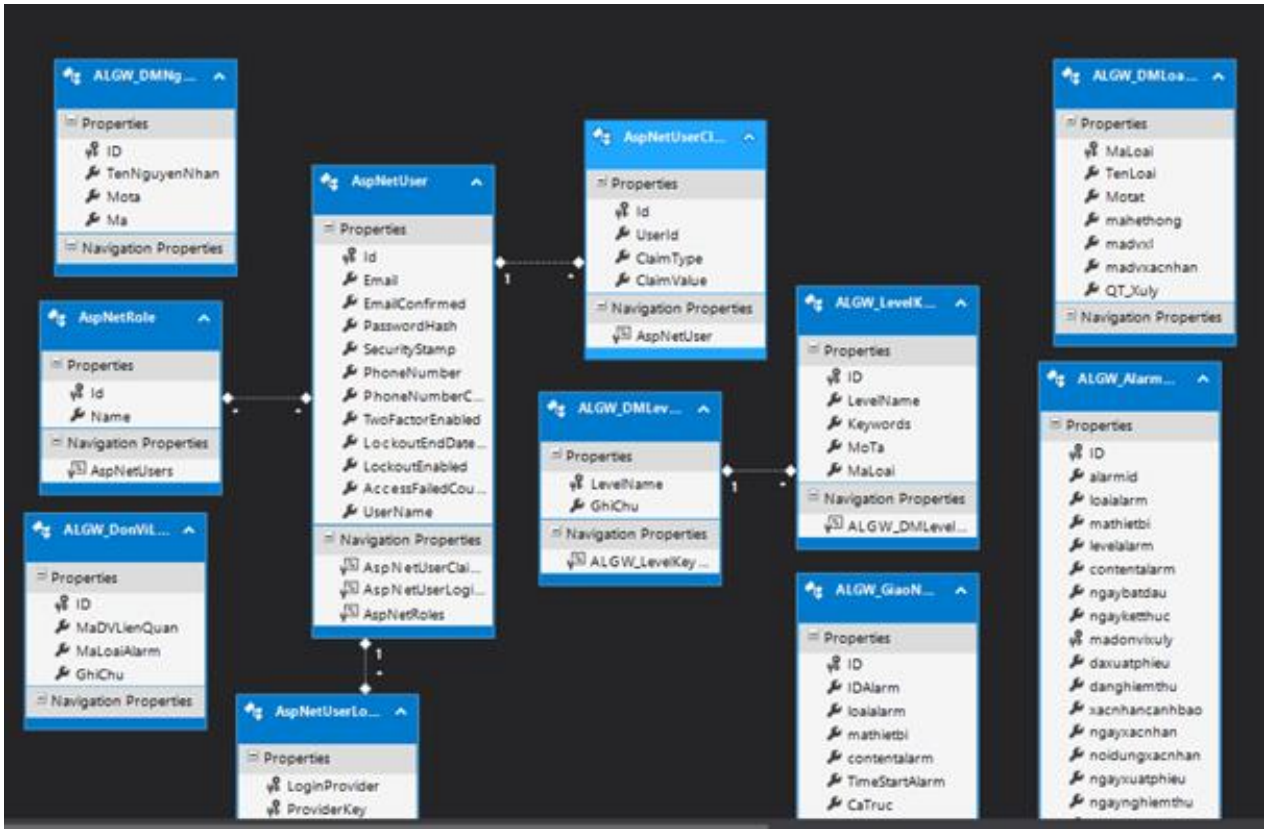
Đối với các thiết bị không hỗ trợ SNMP, nhóm bài báo thực việc kết nối và quét bằng Telnet.và cho phép nhập nhân công Offline đối với các thiết bị không hỗ trợ SNMP và Telnet hoặc không cho phép đọc thông tin vật tư trên thiết bị.

## III. THIẾT KẾ VÀ XÂY DỰNG HỆ THỐNG

### A. Kiến trúc hệ thống




*Hình 4. Sơ đồ đấu nối hệ thống.*




*Hình 5. Sơ đồ thiết kế dữ liệu quan hệ của hệ thống.*

Hệ thống đề xuất trên hình 2 và 3 gồm các module chính sau:

- Module nhận cảnh báo thực hiện nhận và phân tích Syslog hệ thống mạng MANE (Metro Area Network – Ethernet), L2 (Layer 2),G-PON(Gigabit-Passive Optical Network) từ các trạm giám sát
- Module xử lý cảnh báo thực hiện nhận và quét các cảnh báo dựa trên quét suy hao, drop, crc MANE, L2, quét cảnh báo hệ thống mạng PSTN (Public Switched Telephone Network), phân tích mạng truyền dẫn IP
- Module hiển thị và giám sát thực hiện hiển thị hệ thống theo thời gian thực cũng như tìm kiếm, thống kê báo cáo, phân quyền người dùng, phân loại cảnh báo, cấp độ sự cố.
- Module điều hành thực hiện việc cập nhật trạng thái, in thông tin cảnh báo và điều hành chung toàn hệ thống.

### *B. Sơ đồ đấu nối hệ thống*

Đấu nối hệ thống chúng tôi sử dụng **SignalR** [7]. SignalR là một thư viện cho các lập trình viên Asp.Net đơn giản hóa quá trình thêm chức năng web real-time trong phát triển ứng dụng. SignalR có thể sử dụng trong bất kì chức năng web real-time nào. Trong đó ứng dụng chat trên web là một ví dụ điển hình. Ngoài ra, các ứng dụng cho giám sát, tương tác là những gợi ý cho việc sử dụng SignalR. SignalR cung cấp một API đơn giản cho việc tạo giao thức chủ tớ (remote procedure call (RPC)) để gọi những hàm javascript trong trình duyệt và những nền tảng khác. SignalR cũng bao gồm API cho việc quản lý kết nối và những kết nối nhóm. SignalR xử lý quản lý kết nối một cách tự động, và cho bạn truyền đi thông điệp tới tất cả các client đã được kết nối một cách đồng loạt, giống như một chat room. Bạn cũng có thể gửi những thông điệp tới những client được xác định. Kết nối giữa client và server là liên tục, không giống như kết nối HTTP cổ điển, cái mà sẽ thành lập lại kết nối cho mỗi lần giao tiếp.

Sơ đồ đấu nối hệ thống thể hiện như trên hình 4.

Máy chủ CCSM luôn mở giao thức SignalR để lắng nghe, tiếp nhận các bản tin sự cố từ các hệ thống giám sát, ghi thông tin nhận được vào CSDL. Tiếp theo nó mở API cho phép truy vấn thông tin mỗi khi có yêu cầu gửi vào, nhằm liệt kê tất cả các sự cố đang xảy ra trên hệ thống.

### *C. Sơ đồ dữ liệu quan hệ*

Để xây dựng sơ đồ dữ liệu quan hệ chúng tôi sử dụng công cụ Model – View – Controller (MVC) [5], [10]. MVC được sử dụng nhằm chia ứng dụng thành ba thành phần chính: model, view và controller. Nền tảng ASP.NET MVC giúp cho chúng ta có thể tạo được các ứng dụng web áp dụng mô hình MVC thay vì tạo ứng dụng theo mẫu ASP.NET Web Form. Nền tảng ASP.NET MVC có đặc điểm nổi bật là nhẹ (lighweigt), dễ kiểm thử phần giao diện (so với ứng dụng Web Forms), tích hợp các tính năng có sẵn của ASP.NET. Nền tảng ASP.NET MVC được định nghĩa trong namespace System.Web.Mvc và là một phần của name space System.Web [4].

CSDL của hệ thống được thiết kế theo mô hình quan hệ, bao gồm các bảng danh mục mã loại sự cố và các bảng dữ liệu ghi thông sự cố, hệ thống,.. các bảng này quan hệ với các bảng danh mục mã loại sự cố theo quan hệ 1-n như trên hình 5.

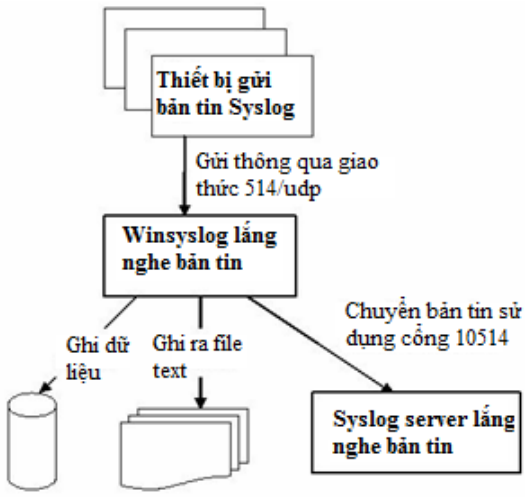
Do trong hệ thống có kết nối và truy nhập đến các thiết bị cung cấp dịch vụ viễn thông và công nghệ thông tin để quét và nhận cảnh báo từ hệ thống, nên vấn đề an toàn bảo mật cho thiết bị cung cấp dịch vụ là rất quan trọng. Vì vậy hệ thống được thiết kế để đảm bảo chỉ cho phép 1 máy tính có quyền truy nhập và thực hiện lệnh quét với thiết bị, các máy tính của người dùng, máy chủ web và CSDL đều không có quyền truy nhập vào thiết bị. Chi tiết thực hiện được mô tả ở phần sau.

## IV. KẾT QUẢ ĐẠT ĐƯỢC

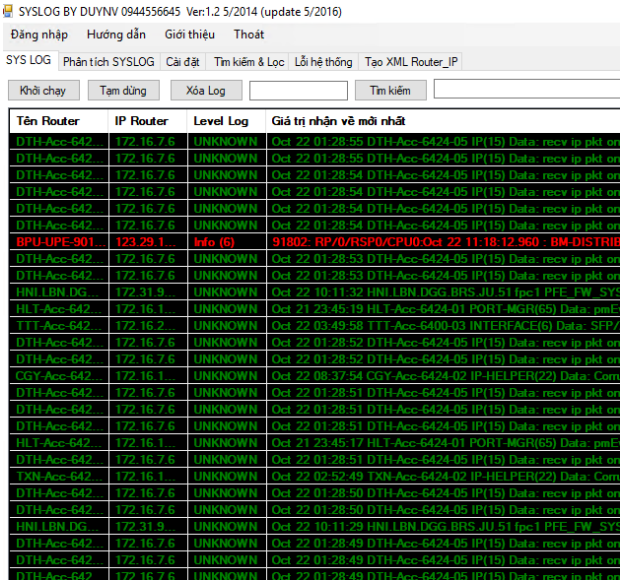
### *A. Module nhận và phân tích mạng*

Module này thực hiện chức năng đón nhận các cảnh báo bất thường, logging từ các hệ thốngqua giao thức UDP (User Datagram Protocol) port 514. Ưu điểm của giao thức syslog là nhận các bản tin log từ thiết bị theo thời gian thực, khi có sự cố hoặc thông tin bất thường. Thiết bị sẽ gửi bản tin ngay đến syslog server. Các chủng loại thiết bị đang giám sát qua giao thức Syslog trên mạng VNPT Hà Nội gồm:

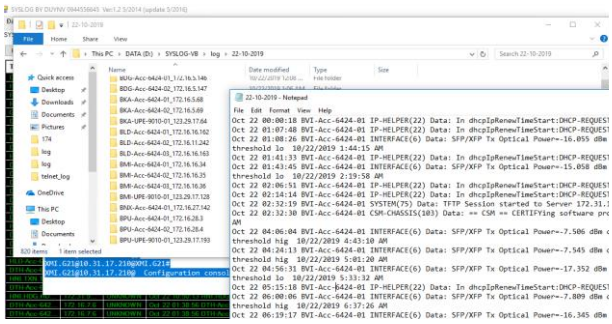
- Thiết bị L2 Switch (2224, 2228,4924,3400,6424...),
- Thiết bị MANE (ASR, 7600, 7609….),
- Thiết bị Bras (Junipter Mx960, 1410),
- Thiết bị Gpon (Alu, ZTE, HW).




*Hình 6. Cách thức hoạt động của module nhận và phân tích Syslog.*



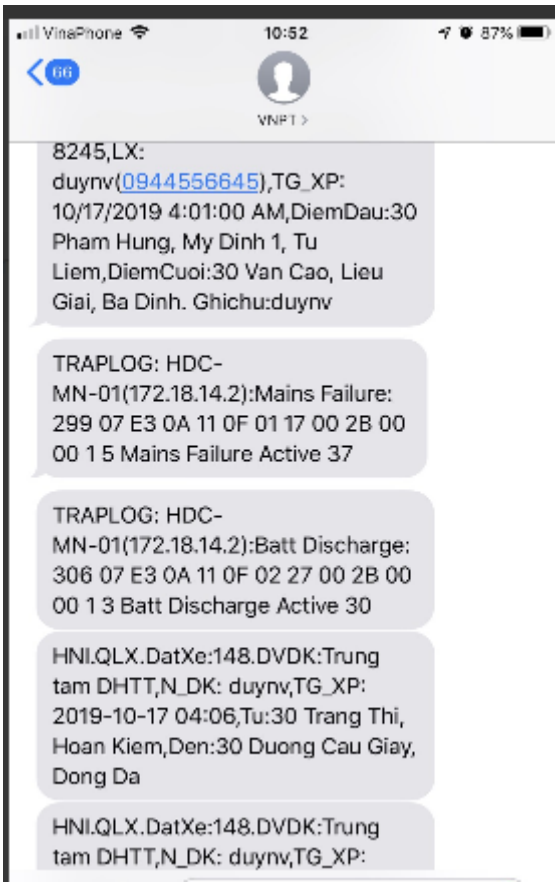

*Hình 7. Giao diện chương trình nhận Syslog.*



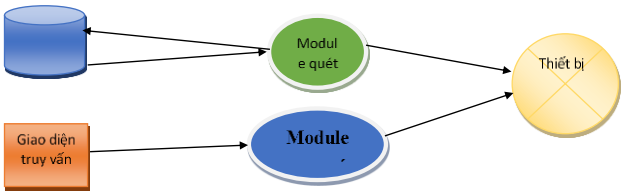
*Hình 8. Giao diện chương trình nhận Syslog.*

Cách thức hoạt động và giao diện của nó thể hiện trên hình 6 và 7.

Hình 8 và 9 thể hiện kết quả đạt được từ module và cảnh báo khi có bất thường xảy ra trên hệ thống.




*Hình 9. Bản tin cảnh báo sms từ hệ thống Syslog.*



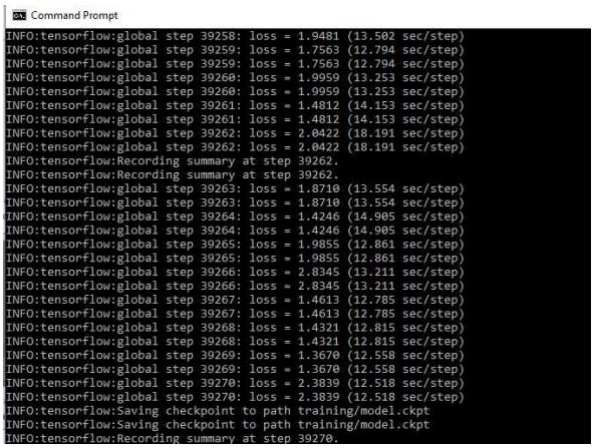

*Hình 10. Sơ đồ hoạt động của module quét suy hao, drop gói tin.*

### *B. Module quét suy hao*

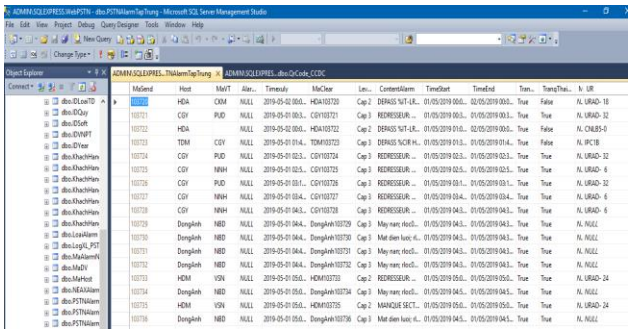
Thực hiện kết nối với thiết bị định kỳ gửi lệnh đo quét các giá trị suy hao, Drop gói tin, CRC Erro trên mạng. Lưu vào cơ sở dữ liệu và so sánh cho giá trị của lần quét tiếp theo. Giao tiếp kết nối với thiết bị sử dụng công nghệ SNMP và Telnet, SSH. Dựa vào các tham số về suy hao, drop, crc erro ta có thể đánh giá được chất lượng đường truyền hoặc chất lượng dịch vụ của thiết bị, đường truyền… Các chủng loại thiết bị đang thực hiện đo quét gồm L2 Switch (6400, 2224) và MANE (ASR, 7600).

Cách thức hoạt động như trên hình 10 gồm:

- Chương trình chạy đo quét thiết bị định kỳ 2h/lần,
- Nhận diện module và định nghĩa ngưỡng suy hao của Module theo chuẩn khuyến nghị của nhà sản xuất,
- Hệ thống gửi cảnh báo sms, email cho bộ phận giám sát, điều hành.




*Hình 11. Bản tin sms cảnh báo.*



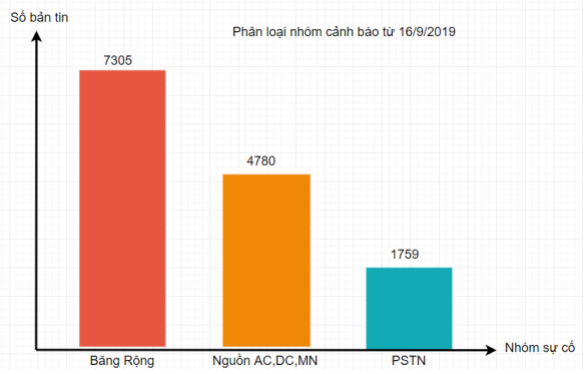
*Hình 12. Bản tin PSTN trên cơ sở dữ liệu CCSM.*

### C. *Module đo quét cảnh báo hệ thống*

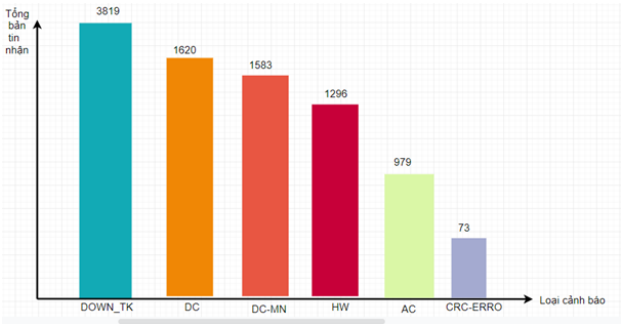
Xây dựng chương trình, module kết nối tới hệ thống mạng PSTN, hệ thống giám sát PSTN để thu thập, nhận diện cảnh báo bất thường, phân tích cảnh báo và giao tiếp với CCSM qua Webservice, SignalR. Chương trình thực hiện chu trình hoàn toàn tự động các chức năng sau:

- Lấy logfile từ các tổng đài Host qua giao thức TCP/IP. Lưu lên server theo các thư mục riêng.
- Xử lý logfile lấy được, phân tích các cảnh báo từ các tổng đài và phân loại cảnh báo. Nội dung cảnh báo là: Tên Host, Mã/Tên Vệ tinh hoặc trạm điều khiển, Loại cảnh báo (là cảnh báo gì), thời gian cảnh báo tổng đài đưa ra, cấp cảnh báo, trạng thái hiện tại của cảnh báo, thời gian chương trình xử lý… Lưu thông tin vào CSDL trên server.
- Kết nối SMS GateWay để gửi tin nhắn SMS (Short Message Service) nội dung cảnh báo cho lãnh đạo, nhân viên trực ca và nhân viên điều hành mạng (tùy chọn) trong trung tâm điều hành thông tin.
- Chương trình tạo kết nối đến SMS GateWay để gửi tin nhắn khi có sự cố:
- Gửi tin nhắn cho lãnh đạo và ca trực biết các cảnh báo mất liên lạc vệ tinh, Host, trạm điều khiển SM.
- Gửi tin nhắn (Cấp 2 và Cấp 3) cho nhân viên trực ca, điều hành mạng (tùy chọn).

Kết quả thể hiện trên hình 11 và 12.




*Hình 13. Thống kê bản tin theo nhóm cảnh báo.*




*Hình 14. Thống kê bản tin theo loại cảnh báo.*

### D. *Module nhận và phân tích mạng*

Nhận diện, phân loại sự cố liên quan đến mạng truyền dẫn IP từ hệ thống PRTG. Phân tích bản tin down/up, thời gian mất liên lạc. Truy vấn và xử lý, phân tích phạm vi ảnh hưởng (Down thiết bị, Down trung kế). Cách thức hoạt động như sau:

- Cài đặt nhận thông tin Down/Up từ hệ thống PRTG.
- Nhận diện loại cảnh báo theo chủng loại thiết bị, ping ip thiết bị để nhận diện thiết bị Down hay Down trung kế.
- Nhận diện băng thông vượt ngưỡng theo phần trăm tổng băng thông đường truyền.

Kết quả dữ liệu hệ thống CCSM nhận được từ 15/9/2019 đến 15/10/2019 như trên hình 13 và 14. Chúng ta nhận thấy nếu theo nhóm cảnh báo thì nhóm băng rộng là nhóm có nguy cơ cao nhất với rủi ro nhiều hơn. Tuy nhiên nếu theo loại bản tin thì bản tin $DOWN_TK$ lại là bản tin gửi nhiều hơn.

## V. KẾT LUẬN

Bài báo đã trình bày những hạn chế của các hệ thống giám sát hiện tại và đề xuất xây dựng một hệ thống quản lý, giám sát sự cố ngày càng hiện đại và thông minh, hướng tới tinh thần cách mạng công nghiệp 4.0. Bài báo cũng là cơ sở để xây dựng, ban hành các quy trình giám sát, điều hành quản lý sự cố. Trong bài báo này chúng tôi đã xây dựng được cấu trúc dữ liệu với các quan hệ chặt chẽ giữa các thông tin sự cố, các hệ thống, thiết bị tạo ra mô hình quản lý khai thác dữ liệu tập trung về thông tin sự cố của các thiết bị, hệ thống đang vận hành khai thác trên mạng lưới của mạng viễn thông hà nội. Đồng thời cũng xây dựng được một hệ thống các giao diện nhập liệu,

khai thác, báo cáo cho phép người sử dụng dễ dàng cập nhật thông tin, tìm kiếm thống kê và lập báo cáo.

Bài báo cũng đã chuẩn hóa lại nhóm sự cố, cấp độ sự cố của các hệ thống, quy trình quy định trước đây để thuận tiện trong việc giám sát, điều hành xử lý sự cố của các hệ thống. Hướng phát triển tiếp theo của chúng tôi là:

- Nghiên cứu xây dựng thêm quy trình theo ma trận rủi ro kiểm soát theo quy chuẩn.
- Nghiên cứu hướng mở rộng phần mềm sử dụng chung.
- Nghiên cứu tối ưu độ ổn định của các tiến trình xử lý, độ ổn định máy chủ giám sát.
- Nghiên cứu đưa hết các cảnh báo tích hợp xuất phiếu theo quy trình, quy định chung.
- Nghiên cứu mở rộng xây dựng ứng dụng cảnh báo trên di động.
- Nghiên cứu xây dựng kịch bản tự động xử lý
- Nghiên cứu xây dựng phần mềm sử dụng trên cùng nền tảng ngôn ngữ lập trình và cơ sở dữ liệu phục vụ việc phát triển phần mềm được nhanh chóng và thống nhất.

## LỜI CẢM ƠN

Nghiên cứu này được thực hiện với sự hỗ trợ từ nguồn dữ liệu được lấy từ đề tài do tập đoàn viễn thông VNPT tài trợ với tiêu đề "Xây dựng hệ thống quản lý giám sát cảnh báo tập trung hệ thống mạng băng rộng, PSTN, và truyền dẫn IP (CCSM)" thực hiện năm 2019. Cảm ơn tập đoàn đã hỗ trợ trong quá trình thực hiện bài báo này.

## TÀI LIỆU THAM KHẢO

[1] P. Le, "Growth, Structural Transformation, and Rural Change in Vietnam: A Rising Dragon on the Move-Edited by Finn Tarp," Asian-Pacific Economic Literature, vol. 33, no. 1, pp. 134–136, May 2019.

[2] N. Q. Sy, "Applying an effective model for vnpt cdn," in 2010 The 12th International Conference on Advanced Communication Technology (ICACT), vol. 1, 2010, pp. 875–878.

[3] H. Bao, "Trung tâm vnpt vinaphone hồ chí minh," 2018.

[4] D. M. Booth, R. Haas, F. G. McCabe, E. Newcomer, I. Champion, C. Ferris, and D. M. Orchard, "Web services architecture, w3c working group note," 2004.

[5] M. Mecella, G. De Giacomo, M. Mecella, and G. De Giacomo, "Tutorial 3: Automatic web service composition," in 2006 IEEE International Conference on Web Services (ICWS'06), 2006, pp. xlii–xlii.

[6] G. Alonso, F. Casati, H. Kuno, and V. Machiraju, "Web Services - Concepts, Architectures and Applications," 01, 2004.

[7] A. Choudhry and A. Premchand, "Real time apps using signalr," 2014.

[8] D. R. Mauro and K. J. Schmidt, Essential SNMP, Second Edition. O'Reilly Media, Inc., 2005.

[9] J. D. Case, M. Fedor, M. L. Schoffstall, and J. Davin, "Rfc1157: Simple network management protocol (snmp)," 1990.

[10] S. Rahaman, N. Meng, and D. Yao, "Tutorial: Principles and practices of secure crypto coding in java," in 2018 IEEE Cybersecurity Development (SecDev), 2018, pp. 122–123.

[11] W. Zhang and P. Sun, "Design of Communication Primitives for Satellites Networks Management," 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), Chengdu, pp. 1-4, 2010.

[12] L. Ye, "The Development of Production Safety Gridding Supervision System," 2014 Fifth International Conference on Intelligent Systems Design and Engineering Applications, Hunan, pp. 1032-1035, 2014.

[13] Xây dựng hệ thống quản lý giám sát cảnh báo tập trung hệ thống mạng băng rộng, PSTN, và truyền dẫn IP (CCSM), Đề tài nghiên cứu khoa học tập đoàn bưu chính viễn thông VNPT, 2019.

[14] A. Davison, "A Standard for the Transmission of IP Datagrams on Avian Carriers," in Humour the Computer , MITP, pp.3-4, 1995.

[15] J. D. Case, "Management of high speed networks with the simple network management protocol (SNMP)," [1990] Proceedings. 15th Conference on Local Computer Networks, Minneapolis, MN, pp. 195-199, 1990.

[16] A. Affandi, D. Riyanto, I. Pratomo and G. Kusrahardjo, "Design and implementation fast response system monitoring server using Simple Network Management Protocol (SNMP)," 2015 International Seminar on Intelligent Technology and Its Applications (ISITIA), Surabaya, pp. 385-390, 2015.

[17] H. Xu, X. Zong, J. Su and Y. Fu, "Formalization of SNMP messages using composite-elements based on extenics for software-defined networking," 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN), Guangzhou, 2017, pp. 989-992, 2017.

## PROPOSING THE MONITORING AND WARNING SYSTEM FOR VNPT NETWORK

***Abstract:*** In the present context, it is necessary to improve the quality to compete in the market of providing telecommunications and information technology services. Applying software tools to business processes to shorten time and improve management quality is one of the solutions that bring high efficiency. In management and operation, there are many devices supporting telecommunications and IT services and each system has different types of alarms. However, the disadvantages of these systems are still fragmented and labor intensive. Therefore, detecting and handling alarms are often difficult. In order to facilitate the management and quick alarm detection as well as monitor the processing progress on the telecommunication network, the paper proposes to develop centralized alert management and monitoring software. Different (PSTN, IP transmission network) to help operators and operators of network infrastructure system intuitively and accurately. Based on the results with CCSM system from September 15, 2019 to October 15, 2019, we show that if warning broadband group is the group with the highest risk (7305 massages). However, the downlink message ($ DOWN_TK $) is sent more with largest numbers (3189 messages).

***Keywords:*** Short Message Service, SNMP, SignalR, MVC, CSSM.

**Nguyen Huu Phat**, nhận bawngff kỹ sư2003), thạc sỹ (2005) ngành Điện tử và Viễn thông tại Đại học Bách Khoa Hà Nội (HUST), Việt Nam và bằng tiến sĩ (2012) về Khoa học Máy tính tại Viện Công nghệ Shibaura, Nhật Bản. Hiện tại, đang là giảng viên tại Viện Điện tử Viễn thông, HUST, Việt Nam. Các nghiên cứu gồm xử lý hình

ảnh và video, mạng không dây, big data, hệ thống giao thông thông minh (ITS), và internet của vạn vật (IoT). Ông đã nhận được giải thưởng bài báo hội nghị tốt nhất trong SoftCOM (2011), giải thưởng tài trợ sinh viên tốt nhất trong APNOMS (2011), giải thưởng danh dự của Viện Công nghệ Shibaura (SIT).

**Vũ Đức Dũng**, Hiện tại Cán bộ kỹ thuật Trung tâm Điều hành Thông tin VNPT, Hà Nội. Hướng nghiên cứu gồm mạng viễn thông, xử lý tín hiệu lớn và các ứng dụng nhà thông minh.