**BDRPC187**

**BỘ TRUYỀN THÔNG & THÔNG TIN**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH & VIỄN THÔNG**

**THÀNH PHỐ HỒ CHÍ MINH**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**BÁO CÁO THỰC TẬP TỐT NGHIỆP**

**ĐỀ TÀI : Nghiên cứu và phát triển hệ thống giám sát truy cập Internet và cảnh báo an toàn thông tin C#**

**Giảng viên hướng dẫn: Ths. Huỳnh Trung Trụ**

**Sinh viên thực hiện: Hà Lê Anh Tuấn**

**Lớp: D14CQIS01**

**MSSV: N14DCCN038**

***TP.HCM ,Ngày 09 Tháng 07 năm***

LỜI MỞ ĐẦU

☺☺☺☺

Nhà trường mà cụ thể là khoa CNTT trường Học viện công nghệ Bưu Chính Viễn Thông cơ sở TP.HCM đã tạo điều kiện cho sinh viên được tiếp xúc với môi trường làm việc thực tế, thông qua quá trình thực tập kéo dài 1 tháng tại Công ty Saigonlab. Trong quá trình thực tập đã giúp em tìm hiểu, làm quen, và nắm được hoạt động của nhân viên trong Công ty cũng như sự phân công công việc cụ thể cho từng phòng ban và chức vụ cụ thể. Đồng thời biết được quá trình áp dụng những kiến thức đã học trong trường lớp vào thực tế công việc của Công ty.

Chúng ta đang sống trong thời đại mới, thời đại phát triển rực rỡ của công nghệ thông tin. Công nghệ thông tin đã ở một bước phát triển cao đó là số hóa tất cả các dữ liệu thông tin, luân chuyển mạnh mẽ và kết nối tất cả chúng ta lại với nhau. Mọi loại thông tin, số liệu âm thanh, hình ảnh có thể được đưa về dạng kỹ thuật số để bất kỳ máy tính nào cũng có thể lưu trữ và chuyển tiếp cho nhiều người. Từ dữ liệu được số hóa sẽ trở thành những tài nguyên được chia sẻ chung trong hệ thống mạng cũng như internet. Chính vì vậy quản lý tài nguyên và truy cập internet của người sử dụng là một bài toán tổng quan và phổ biến hiện nay. Quản lý tài nguyên và truy cập internet của người sử dụng cần đáp ứng được các nhu cầu quản lý khác nhau của các đơn vị, tổ chức hoặc các doanh nghiệp mà chọn các giải pháp khác nhau. Quản lý tài nguyên và truy cập internet của người sử dụng nhằm một mục đích là làm cho việc sử dụng tài nguyên và truy cập internet hiệu quả hơn và trong sáng hơn. Rõ ràng là như vậy khi bạn không muốn người sử dụng truy cập internet và tài nguyên không lành mạnh thì cần quản lý được nội dung truy cập của người sử dụng. Và như vậy sẽ tăng hiệu năng làm việc cũng như khả năng học tập của người sử dụng. Quản lý tài nguyên và truy cập internet cũng là phải quản lý được lưu lượng sử dụng cũng như dung lượng sử dụng của người sử dụng, tránh làm ảnh hưởng đến chất lượng của hệ thống cũng như việc sử dụng của các cá nhân khác. Quản lý tài nguyên và truy cập internet của người sử dụng cũng là việc làm sao phải bảo đảm an toàn và bảo mật thông tin của người sử dụng khi hoạt động trong hệ thống. Quản lý tài nguyên và truy cập internet của người sử dụng cũng là quản lý số người truy cập tài nguyên và internet. Muốn quản lý tài nguyên và truy cập internet của người sử dụng cần phải xây dựng một hệ thống quản lý tài nguyên và truy cập internet

Từ đó ta có mục tiêu được đặt ra là Nghiên cứu và phát triển hệ thống giám sát truy cập Internet và cảnh báo an toàn thông tin

Qua đây em xin gửi lời cảm ơn chân thành đến các anh chị em Công ty Saigonlab đã hết lòng huớng dẫn, giúp đỡ và chỉ dạy cho tôi có thể hoàn thành tốt công việc được giao trong suốt quá trình thực tập cũng như lời cảm ơn sâu sắc đến thầy Huỳnh Trung Trụ đã tận tình huớng dẫn hoàn thành đồ án thực tập này.

Contents

[**Chương 1** **C# và .Net Framework** 5](#_Toc521059143)

[**Nền tảng của .NET** 5](#_Toc521059144)

[**.NET Framework** 6](#_Toc521059145)

[1.2 Biên dịch ngôn ngữ trung gian (MSIL) 8](#_Toc521059146)

[**Ngôn ngữ C#** 8](#_Toc521059147)

[CHƯƠNG 2: CÔNG NGHỆ SỬ DỤNG TRONG ĐỀ TÀI 9](#_Toc521059148)

[**1.** **DevExpress:** 9](#_Toc521059149)

[**2.** **Giao thức SNMP (Simple Network Management)** 10](#_Toc521059150)

[**CHƯƠNG 3: NHỮNG PHẦN ĐÃ HOÀN THÀNH TRONG ĐỒ ÁN** 16](#_Toc521059151)

[**1.** **Phần Giao diện chính của chương trình:** 16](#_Toc521059152)

[**Các công cụ hổ trợ việc quét IP từ các máy đã đăng nhập vào mạng:** 30](#_Toc521059153)

[CHƯƠNG 4. XÂY DỰNG CÔNG CỤ DEMO QUẢN TRỊ MẠNG SỬ DỤNG SNMP 30](#_Toc521059154)

[**4.1.** **Cấu hình SNMP agent trên hệ điều hành Windows** 30](#_Toc521059155)

[**Thiết kế chương trình demo** 34](#_Toc521059156)

[KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 37](#_Toc521059157)

# **Chương 1 C# và .Net Framework**

Mục tiêu của C# là cung cấp một ngôn ngữ lập trình đơn giản, an toàn, hiện đại, hướng đối tượng, đặt trọng tâm vào Internet, có khả năng thực thi cao cho môi trường .NET. C# là một ngôn ngữ mới, nhưng tích hợp trong nó những tinh hoa của ba thập kỷ phát triển của ngôn ngữ lập trình. Ta có thể dể dàng thầy trong C# có những đặc trưng quen thuộc của Java, C++, Visual Basic, …

Đề tài này đặt trọng tâm giới thiệu ngôn ngữ C# và cách dùng nó như là một công cụ lập trình trên nền tảng .NET. Với ngôn ngữ C++, khi học nó ta không cần quan tâm đến môi trường thực thi. Với ngôn ngữ C#, ta học để tạo một ứng dụng .NET, nếu lơ là ý này có thể bỏ lỡ quan điểm chính của ngôn ngữ này. Do đó, trong đề tài này xét C# tập trung trong ngữ cảnh cụ thể là nền tảng .NET của Microsoft và trong các ứng dụng máy tính để bàn và ứng dụng Internet.

Chương này trình bày chung về hai phần là ngôn ngữ C# và nền tảng .NET, bao gồm cả khung ứng dụng .NET (.NET Framework)

## **Nền tảng của .NET**

Khi Microsoft công bố C# vào tháng 7 năm 2000, việc khánh thành nó chỉ là một phần trong số rất nhiều sự kiện mà nền tảng .Net được công công bố. Nền tảng .Net là bô khung phát triển ứng dụng mới, nó cung cấp một giao diện lập trình ứng dụng (Application Programming Interface - API) mới mẽ cho các dịch vụ và hệ điều hành Windows, cụ thể là Windows 2000, nó cũng mang lại nhiều kỹ thuật khác nổi bật của Microsoft suốt từ những năm 90. Trong số đó có các dịch vụ COM+, công nghệ ASP, XML và thiết kế hướng đối tượng, hỗ trợ các giao thức dịch vụ web mới như SOAP, WSDL và UDDL với trọng tâm là Internet, tất cả được tích hợp trong kiến trúc DNA.

Nền tảng .NET bao gồm bốn nhóm sau:

* + 1. Một tập các ngôn ngữ, bao gồm C# và Visual Basic .Net; một tập các công cụ phát triển bao gồm Visual Studio .Net; một tập đầy đủ các thư viện phục vụ cho việc xây dựng các ứng dụng web, các dịch vụ web và các ứng dụng Windows; còn có CLR - Common Language Runtime: (ngôn ngữ thực thi dùng chung) để thực thi các đối tượng được xây dựng trên bô khung này.
    2. Một tập các Server Xí nghiệp .Net như SQL Server 2000. Exchange 2000, BizTalk 2000, … chúng cung cấp các chức năng cho việc lưu trữ dữ liệu quan hệ, thư điện tử, thương mại điện tử B2B, …
    3. Các dịch vụ web thương mại miễn phí, vừa được công bố gần đậy như là dự án Hailstorm; nhà phát triển có thể dùng các dịch vụ này để xây dựng các ứng dụng đòi hỏi tri thức về định danh người dùng…
    4. .NET cho các thiết bị không phải PC như điện thoại (cell phone), thiết bị game

## **.NET Framework**

.Net hỗ trợ tích hợp ngôn ngữ, tức là ta có thể kế thừa các lớp, bắt các biệt lệ, đa hình thông qua nhiều ngôn ngữ. .NET Framework thực hiện được việc này nhờ vào đặc tả Common Type System - CTS (hệ thống kiểu chung) mà tất cả các thành phần

.Net đều tuân theo. Ví dụ, mọi thứ trong .Net đều là đối tượng, thừa kế từ lớp gốc System.Object.

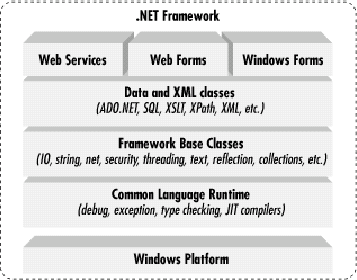
Ngoài ra .Net còn bao gồm Common Language Specification - CLS (đặc tả ngôn ngữ chung). Nó cung cấp các qui tắc cơ bản mà ngôn ngữ muốn tích hợp phải thỏa mãn. CLS chỉ ra các yêu cầu tối thiểu của ngôn ngữ hỗ trợ .Net. Trình biên dịch tuân theo CLS sẽ tạo các đối tượng có thể tương hợp với các đối tượng khác. Bộ thư viện lớp của khung ứng dụng (Framework Class Library - FCL) có thể được dùng bởi bất kỳ ngôn ngữ nào tuân theo CLS.

.NET Framework nằm ở tầng trên của hệ điều hành (bất kỳ hệ điều hành nào không chỉ là Windows). .NET Framework bao bao gồm:

* Bốn ngôn ngữ chính thức: C#, VB.Net, C++, và Jscript.NET
* Common Language Runtime - CLR, nền tảng hướng đối tượng cho phát triển

ứng dụng Windows và web mà các ngôn ngữ có thể chia sẻ sử dụng.

* Bộ thư viện Framework Class Library - FCL.



**Hình 1-1 Kiến trúc khung ứng dụng .Net**

Thành phần quan trọng nhất của .NET Framework là CLR, nó cung cấp môi trường cho ứng dụng thực thi, CLR là một máy ảo, tương tự máy ảo Java. CLR kích hoạt đối tượng, thực hiện kiểm tra bảo mật, cấp phát bộ nhớ, thực thi và thu dọn chúng.

Trong Hình 1-1 tầng trên của CLR bao gồm:

* Các lớp cơ sở
* Các lớp dữ liệu và XML
* Các lớp cho dịch vụ web, web form, và Windows form.

Các lớp này được gọi chung là FCL, Framework Class Library, cung cấp API hướng đối tượng cho tất cả các chức năng của .NET Framework (hơn 5000 lớp).

Các lớp cơ sở tương tự với các lớp trong Java. Các lớp này hỗ trợ các thao tác nhập xuất, thao tác chuổi, văn bản, quản lý bảo mật, truyền thông mạng, quản lý tiểu trình và các chức năng tổng hợp khác …

Trên mức này là lớp dữ liệu và XML. Lớp dữ liệu hỗ trợ việc thao tác các dữ liệu trên cơ sở dữ liệu. Các lớp này bao gồm các lớp SQL (Structure Query Language: ngôn ngữ truy vấn có cấu trúc) cho phép ta thao tác dữ liệu thông qua một giao tiếp SQL chuẩn. Ngoài ra còn một tập các lớp gọi là ADO.Net cũng cho phép thao tác dữ liệu. Lớp XML hỗ trợ thao tác dữ liệu XML, tìm kiếm và diễn dịch XML.

Trên lớp dữ liệu và XML là lớp hỗ trợ xây dựng các ứng dụng Windows (Windows forms), ứng dụng Web (Web forms) và dịch vụ Web (Web services).

### Biên dịch ngôn ngữ trung gian (MSIL)

Với .NET chương trình không biên dịch thành tập tin thực thi, mà biên dịch thành ngôn ngữ trung gian (MSIL - Microsoft Intermediate Language, viết tắt là IL), sau đó chúng được CLR thực thi. Các tập tin IL biên dịch từ C# đồng nhất với các tập tin IL biên dịch từ ngôn ngữ .Net khác.

Khi biên dịch dự án, mã nguồn C# được chuyển thành tập tin IL lưu trên đĩa. Khi chạy chương trình thì IL được biên dịch (hay thông dịch) một lần nữa bằng trình *Just In Time* - JIT, khi này kết quả là mã máy và bộ xử lý sẽ thực thi.

Trình biên dịch JIT chỉ chạy khi có yêu cầu. Khi một phương thức được gọi, JIT phân tích IL và sinh ra mã máy tối ưu cho từng loại máy. JIT có thể nhận biết mã nguồn đã được biên dịch chưa, để có thể chạy ngay ứng dụng hay phải biên dịch lại.

CLS có nghĩa là các ngôn ngữ .Net cùng sinh ra mã IL. Các đối tượng được tạo theo một ngôn ngữ nào đó sẽ được truy cập và thừa kế bởi các đối tượng của ngôn ngữ khác. Vì vậy ta có thể tạo được một lớp cơ sở trong VB.Net và thừa kế nó từ C#.

## **Ngôn ngữ C#**

C# là một ngôn ngữ rất đơn giản, với khoảng 80 từ khoá và hơn mười kiểu dữ liệu dựng sẵn, nhưng C# có tính diễn đạt cao. C# hỗ trợ lập trình có cấu trúc, hướng đối tượng, hướng thành phần (component oriented).

Trọng tâm của ngôn ngữ hướng đối tượng là lớp. Lớp định nghĩa kiểu dữ liệu mới, cho phép mở rộng ngôn ngữ theo hướng cần giải quyết. C# có những từ khoá dành cho việc khai báo lớp, phương thức, thuộc tính (property) mới. C# hỗ trợ đầy đủ khái niệm trụ cột trong lập trình hướng đối tượng: đóng gói, thừa kế, đa hình.

Định nghĩa lớp trong C# không đòi hỏi tách rời tập tin tiêu đề với tập tin cài đặt như C++. Hơn thế, C# hỗ trợ kiểu sưu liệu mới, cho phép sưu liệu trực tiếp trong tập tin mã nguồn. Đến khi biên dịch sẽ tạo tập tin sưu liệu theo định dạng XML.

C# hỗ trợ khái niệm giao diện, *interfaces* (tương tự Java). Một lớp chỉ có thể kế thừa duy nhất một lớp cha nhưng có thế cài đặt nhiều giao diện.

C# có kiểu *cấu trúc,* struct (không giống C++). Cấu trúc là kiểu hạng nhẹ và bị giới hạn.Cấu trúc không thể thừa kế lớp hay được kế thừa nhưng có thể cài đặt giao diện.

C# cung cấp những đặc trưng lập trình hướng thành phần như property, sự kiện và dẫn hướng khai báo (được gọi là *attribute*). Lập trình hướng component được hỗ trợ bởi CLR thông qua siêu dữ liệu (metadata). Siêu dữ liệu mô tả các lớp bao gồm các phương thức và thuộc tính, các thông tin bảo mật ….

*Assembly* là một tập hợp các tập tin mà theo cách nhìn của lập trình viên là các thư viện liên kết động (DLL) hay tập tin thực thi (EXE). Trong .NET một assembly là một đon vị của việc tái sử dụng, xác định phiên bản, bảo mật, và phân phối. CLR cung cấp một số các lớp để thao tác với assembly.

C# cũng cho truy cập trực tiếp bộ nhớ dùng con trỏ kiểu C++, nhưng vùng mã đó được xem như không an toàn. CLR sẽ không thực thi việc thu dọn rác tự động các đối tượng được tham chiếu bởi con trỏ cho đến khi lập trình viên tự giải phóng.

# CHƯƠNG 2: CÔNG NGHỆ SỬ DỤNG TRONG ĐỀ TÀI

1. **DevExpress:**

* DevExpress là bộ control  rất hữu ích cho việc thiết kế và phát triển phần mềm, website,  đối với .NET nó thay thế hầu hết các control của bộ visual studio, nó không những giúp thiết kế được form đẹp hơn mà còn giúp cho công việc lập trình nhẹ nhàng hơn, nhất là trong việc tương tác dữ liệu.
* DevExpress được phát triển bởi Developer Express Inc (DevExpress) là công ty phát triển phần mềm được thành lập năm 1998, có trụ sở tại Glendale, California. Thời gian đầu, DevExpress phát triển UI Controls cho Borland Delphi/C++ Builder và ActiveX Controls cho Microsoft Visual Studio. Hiện nay thì sản phẩm của DevExpress hướng tới những lập trình viên sử dụng Delphi/c++ Builder, Visual Studio và HTML5/Javascript.
* Một số tính năng:
* Rating control: Rating control là một control mới được giới thiệu trong Version này, Rating Control giúp người dùng cuối tạo những feedback và những đánh giá
* TimeSpan Editor: TimeSpan Editor là thiết kế touch-friendly rất đơn giản và dễ dùng để người dùng có thể chọn thời gian chính xác tới đơn vị giây.
* SQL Data Access Component: Với phiên bản này bạn có thể sử dụng Winforms SqlDatasource mới để tương tác với database Sql, cấu hình kết nối dữ liệu và đưa dữ liệu vào các control như Gridcontrol, TreeList…
* Workspace Manager: Với Workspace Manager giúp người dùng cuối sao lưu và phục hồi không gian làm việc, layouts theo cách riêng của mình bao gồm Bar Managers, Ribbon Controls, Navigation Bars, Document và Dock Managers
* XtraGrid control: Gridcontrol có lẻ là control mà tôi ấn tượng nhất của DevExpress, không những nó giúp hiển thị dữ liệu kiểu bảng như DataGrid control của bộ Visual mà nó còn có nhiều tùy chọn khác khá hay
* Ngoài ra còn một số tính năng khác như:
* New Windows® 8 Inspired Grid TileView
* Excel® Inspired Conditional Formatting
* Excel Inspired Conditional Formatting
* New Excel® Data Export Engine
* Controls within Grid Cells

1. **Giao thức SNMP (Simple Network Management)**

SNMP là “giao thức quản lý mạng đơn giản”, dịch từ cụm từ “Simple Network Management Protocol”. Là giao thức được sử dụng rất phổ biến để giám sát và điều khiển thiết bị mạng như switch, router, server ...

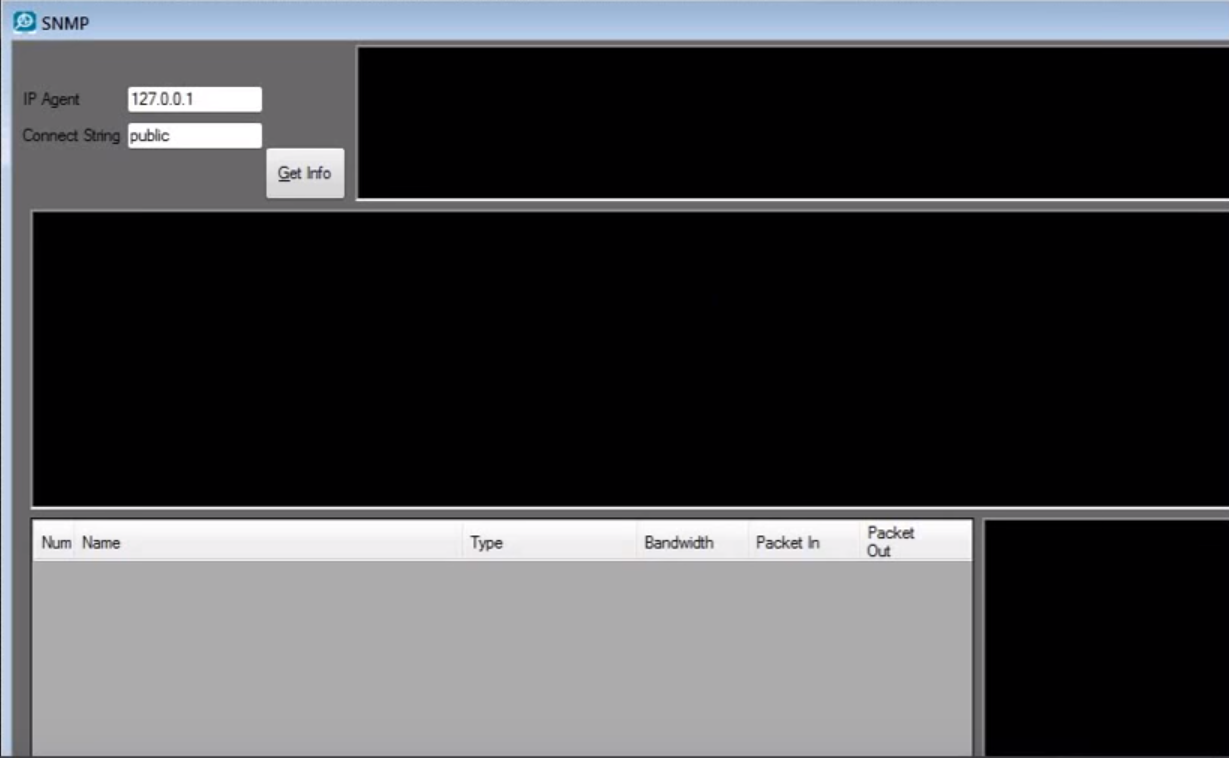
Giao thức SNMP được thiết kế để cung cấp một phương thức đơn giản để quản lý tập trung mạng TCP/IP. Nếu bạn muốn quản lý các thiết bị từ 1 vị trí tập trung, giao thức SNMP sẽ vận chuyển dữ liệu từ client (thiết bị mà bạn đang giám sát) đến server nơi mà dữ liệu được lưu trong log file nhằm phân tích dễ dàng hơn  
SNMP dùng để quản lý tức 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. VD một số khả năng của phần mềm SNMP :  
+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.  
Hoạt động của SNMP:  
Có 2 nhân tố chính trong SNMP: Manager và Agent. Các SNMP agent sẽ giữ một sơ sở dữ liệu, được gọi là Management Information Base (MIB), trong đó chứa các thông tin khác nhau về hoạt động của thiết bị mà agent đang giám sát. Phần mềm quản trị SNMP Manager sẽ thu thập thông tin này qua giao thức SNMP.  
Ưu điểm khi thiết kế hệ thống quản trị với SNMP sẽ giúp đơn giản hóa các quá trình quản lý các thành phần trong mạng, giảm chi phí triển khai.SNMP được thiết kế để có thể mở rộng các chức năng quản lý, giám sát. SNMP được thiết kế để có thể hoạt động độc lập với các kiến trúc và cơ chế của các thiết bị hỗ trợ SNMP.  
Các cơ chế bảo mật cho SNMP  
Một SNMP management station có thể quản lý/giám sát nhiều SNMP element, thông qua hoạt động gửi request và nhận trap. Tuy nhiên một SNMP element có thể được cấu hình để chỉ cho phép các SNMP   
management station nào đó được phép quản lý/giám sát mình.  
Các cơ chế bảo mật đơn giản này gồm có : community string, view và SNMP access control list.  
Community String  
Community string là một chuỗi ký tự được cài đặt giống nhau trên cả SNMP manager và SNMP agent, đóng vai trò như “mật khẩu” giữa 2 bên khi trao đổi dữ liệu. Community string có 3 loại : Read-community, Write-Community và Trap-Community.  
View  
Một view phải gắn liền với một community string. Tùy vào community string nhận được là gì mà agent xử lý trên view tương ứng.  
SNMP access control list  
SNMP ACL là một danh sách các địa chỉ IP được phép quản lý/giám sát agent, nó chỉ áp dụng riêng cho giao thức SNMP và được cài trên agent. Nếu một manager có IP không được phép trong ACL gửi request thì agent sẽ không xử lý, dù request có community string là đúng.  
Đa số các thiết bị tương thích SNMP đều cho phép thiết lập SNMP ACL.  
Các phiên bản SNMP  
SNMP có 4 phiên bản : SNMPv1, SNMPv2c, SNMPv2u và SNMPv3. Các phiên bản này khác nhau một chút ở định dạng bản tin và phương thức hoạt động.  
Mô tả Phiên bản SNMP:  
1 Dùng SMIv1 dùng phương thức xác thực đơn giản với community nhưng chỉ dùng MIB-I.  
2 ùng SMIv2. Loại bỏ việc sử dụng communities thêm vào các thông điệp Getbulk và Inform nhưng đã bắt đầu với phiên bản MIB-II.  
2c Phiên bản giả cho phép SNMPv1 giao tiếp với SNMPv2. Tương đương với SNMPv2.  
3 Phần lớn tương tự như SNMPv2 nhưng thêm vào các tính năng bảo mật. Hỗ trợ tương thích ngược. Dùng MIB-II.  
Các phương thức SNMP  
Các giao thức SNMPv1 và SNMPv2 định nghĩa cách thức mà một phần mềm manager và một tác nhân agent có thể giao tiếp với nhau. Ví dụ, một manager có thể dùng ba thông điệp khác nhau để lấy các thông tin MIB từ các tác nhân agents với một thông điệp SNMP response được trả về từ tác nhân agent. SNMP dùng UDP để truyền thông tin, dùng thông tin SNMP response để cung cấp thông tin và công nhận (ack) việc nhận các thông điệp khác.  
Các phương thức và tác dụng  
GetRequest Manager gửi GetRequest cho agent để yêu cầu agent cung cấp thông tinnào đó dựa vào ObjectID (trong GetRequest có chứa OID)  
GetNextRequest Manager gửi GetNextRequest có chứa một ObjectID cho agent để yêu cầu cung cấp thông tin nằm kế tiếp ObjectID đó trong MIB.  
SetRequest Manager gửi SetRequest cho agent để đặt giá trị cho đối tượng của agent dựa vào ObjectID.  
GetResponse Agent gửi GetResponse cho Manager để trả lời khi nhận được GetRequest/GetNextRequest  
Trap Agent tự động gửi Trap cho Manager khi có một sự kiện xảy ra đối với một object nào đó trong agent.

Giao Thức DHCP:

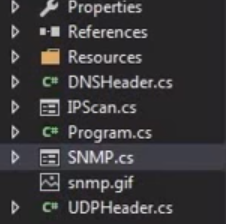
DHCP (dynamic host configuration protocol): Giao thức cấu hình địa chỉ động được thiết kế làm giảm thời gian chỉnh cấu hình cho mạng TCP/IP bằng cách tự động gán các địa chỉ IP cho người sử dụng khi họ vào mạng. Dịch vụ DHCP là một thuận lợi rất lớn đối với người điều hành mạng. Nó làm yên tâm về các vấn đề cố hữu phát sinh khi phải khai báo cấu hình thủ công. Nói một cách tổng quan hơn DHCP là dịch vụ mang đến cho chúng ta nhiều lợi điểm trong công tác quản trị và duy trì một mạng TCP/IP như: + Tập trung quản trị thông tin về cấu hình IP. + Cấu hình động các máy. + Cấu hình IP cho các máy một cách liền mạch + Sự linh hoạt + Khả năng mở rộng Chức năng: – Mỗi thiết bị trên mạng cơ sở TCP/IP phải có một địa chỉ IP duy nhất để truy cập mạng và các tài nguyên của nó. Không có DHCP, cấu hình IP phải được thực hiện một cách thủ công cho các máy tính mới, các máy tính di chuyển từ mạng con này sang mạng con khác, và các máy tính được loại bỏ khỏi mạng. – Bằng việc phát triển DHCP trên mạng, toàn bộ tiến trình này được quản lý tự động và tập trung. DHCP server bảo quản vùng của các địa chỉ IP và giải phóng một địa chỉ với bất cứ DHCP client có thể khi nó có thể ghi lên mạng. Bởi vì các địa chỉ IP là động 4 hơn tĩnh, các địa chỉ không còn được trả lại một cách tự động trong sử dụng đối với các vùng cấp phát lại. Các thuật ngữ trong DHCP: – DHCP Server: máy quản lý việc cấu hình và cấp phát địa chỉ IP cho Client – DHCP Client: máy trạm nhận thông tin cấu hình IP từ DHCP Server – Scope: phạm vi liên tiếp của các địa chỉ IP có thể cho một mạng. – Exclusion Scope: là dải địa chỉ nằm trong Scope không được cấp phát động cho Clients. – Reservation: Địa chỉ đặt trước dành riêng cho máy tính hoặc thiết bị chạy các dịch vụ (tùy chọn này thường được thiết lập để cấp phát địa chỉ cho các Server, Printer,…..) – Scope Options: các thông số được cấu hình thêm khi cấp phát IP động cho Client như DNS Server(006), Router(003). Phương thức hoạt động của dịch vụ DHCP Dịch vụ DHCP hoạt động theo mô hình Client / Server. Theo đó quá trình tương tác giữa DHCP client và server sẽ diễn ra theo các bước sau. Bước 1: Khi máy Client khởi động, máy sẽ gửi broadcast gói tin DHCP DISCOVER, yêu cầu một Server phục vụ mình. Gói tin này cũng chứa địa chỉ MAC của client. Nếu client không liên lạc được với DHCP Server thì sau 4 lần truy vấn không thành công nó sẽ tự động phát sinh ra 1 địa chỉ IP riêng cho chính mình nằm trong dãy 169.254.0.0 đến 169.254.255.255 dùng để liên lạc tạm thời. Và client vẫn duy trì việc phát tín hiệu Broadcast sau mỗi 5 phút để xin cấp IP từ DHCP Server. Bước 2: Các máy Server trên mạng khi nhận được yêu cầu đó. Nếu còn khả năng cung cấp địa chỉ IP, đều gửi lại cho máy Client một gói tin DHCP OFFER, đề nghị cho thuê một địa chỉ IP trong một khoảng thời gian nhất định, kèm theo là một Subnet Mask và địa chỉ của Server. Server sẽ không cấp phát địa chỉ IP vừa đề nghị cho client thuê trống suốt thời gian thương thuyết. Bước 3: Máy Client sẽ lựa chọn một trong những lời đề nghị (DHCP OFFER) và gửi broadcast lại gói tin DHCP REQUEST và chấp nhận lời đề nghị đó. Điều này cho phép các lời đề nghị không được chấp nhận sẽ được các Server rút lại và dùng để cấp phát cho các Client khác. Bước 4: Máy Server được Client chấp nhận sẽ gửi ngược lại một gói tin DHCP ACK như một lời xác nhận, cho biết địa chỉ IP đó, Subnet Mask đó và thời hạn cho sử dụng đó sẽ chính thức được áp dụng. Ngoài ra server còn gửi kèm những thông tin bổ sung như địa chỉ Gateway mặc định, địa chỉ DNS Server… 1.1.2. LDAP LDAP (Lightweight Directory Access Protocol) – là giao thức truy cập nhanh các dịch vụ thư mục - là một chuẩn mở rộng cho nghi thức truy cập thư mục. LDAP là một giao thức tìm, truy nhập các thông tin dạng thư mục trên server. Nó dùng giao thức dạng Client/Server để truy cập dịch vụ thư mục. LDAP chạy trên TCP/IP hoặc các dịch vụ hướng kết nối khác. Ngoài ra, LDAP được tạo ra đặc biệt cho hành động "đọc". Bởi thế, xác thực người 5 dùng bằng phương tiện "lookup" LDAP nhanh, hiệu suất, ít tốn tài nguyên, đơn giản hơn là query 1 user account trên CSDL Có các LDAP Server như: OpenLDAP, OPENDS, Active Directory, … Phương thức hoạt động của LDAP Ldap dùng giao thức giao tiếp client/server Giao thức giao tiếp client/server là một mô hình giao thức giữa một chương trình client chạy trên một máy tính gởi một yêu cầu qua mạng đến cho một máy tính khác đang chạy một chương trình server (phục vụ). Chương trình server này nhận lấy yêu cầu và thực hiện sau đó nó trả lại kết quả cho chương trình client. Ý tưởng cơ bản của giao thức client/server là công việc được gán cho những máy tính đã được tối ưu hóa để thực hiện công việc đó. Một máy server LDAP cần có rất nhiều RAM (bộ nhớ) dùng để lưu trữ nội dung các thư mục cho các thao tác thực thi nhanh và máy này cũng cần đĩa cứng và các bộ vi xử lý ở tốc độ cao. Đây là một tiến trình hoạt động trao đổi LDAP client/server: Hình 1.1: Mô hình kết nối giữa client/server Client mở một kết nối TCP đến LDAP server và thực hiện một thao tác bind. Thao tác bind bao gồm tên của một directory entry, và ủy nhiệm thư sẽ được sử dụng trong quá trình xác thực, ủy nhiệm thư thông thường là password nhưng cũng có thể là chứng chỉ điện tử dùng để xác thực client. Sau khi thư mục có được sự xác định của thao tác bind, kết quả của thao tác bind được trả về cho client. Client phát ra các yêu cầu tìm kiếm. Server thực hiện xử lý và trả về kết quả cho client. Server gởi thông điệp kết thúc việc tìm kiếm. Client phát ra yêu cầu unbind, với yêu cầu này server biết rằng client muốn hủy bỏ kết nối. Server đóng kết nối. LDAP là một giao thức hướng thông điệp 6 Do client và server giao tiếp thông qua các thông điệp, client tạo một thông điệp (LDAP message) chứa yêu cầu và gởi nó đến cho server. Server nhận được thông điệp và xử lý yêu cầu của client sau đó gởi trả cho client cũng bằng một thông điệp LDAP. Ví dụ: Khi LDAP client muốn tìm kiếm trên thư mục, client tạo LDAP tìm kiếm và gởi thông điệp cho server. Sever tìm trong cơ sở dữ liệu và gởi kết quả cho client trong một thông điệp LDAP Hình 1.2: Thao tác tìm kiếm cơ bản Nếu client tìm kiếm thư mục và nhiều kết quả được tìm thấy, thì các kết quả này được gởi đến client bằng nhiều thông điệp. Hình 1.3: Những thông điệp Client gửi cho server Do nghi thức LDAP là giao thức hướng thông điệp nên client được phép phát ra nhiều thông điệp yêu cầu đồng thời cùng một lúc. Trong LDAP, message ID dùng để phân biệt các yêu cầu của client và kết quả trả về của server. Hình 1.4: Nhiều kết quả tìm kiếm được trả về Việc cho phép nhiều thông điệp cùng xử lý đồng thời làm cho LDAP linh động hơn các nghi thức khác. 7 Ví dụ như HTTP, với mỗi yêu cầu từ client phải được trả lời trước khi một yêu cầu khác được gởi đi, một HTTP client program như là Web browser muốn tải xuống cùng lúc nhiều file thì Web browser phải thực hiện mở từng kết nối cho từng file, LDAP thực hiện theo cách hoàn toàn khác, quản lý tất cả thao tác trên một kết nối

# **CHƯƠNG 3: NHỮNG PHẦN ĐÃ HOÀN THÀNH TRONG ĐỒ ÁN**

* + 1. **Phần Giao diện chính của chương trình:**



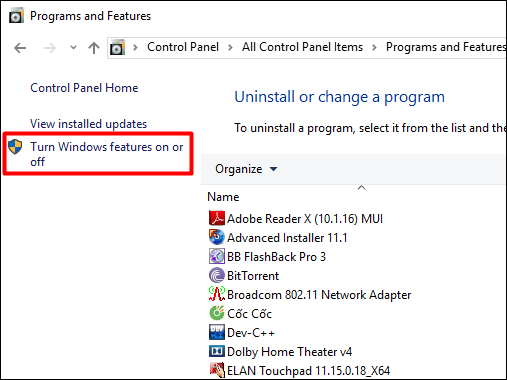
## **Các công cụ hổ trợ việc quét IP từ các máy đã đăng nhập vào mạng:**



# CHƯƠNG 4. XÂY DỰNG CÔNG CỤ DEMO QUẢN TRỊ MẠNG SỬ DỤNG SNMP

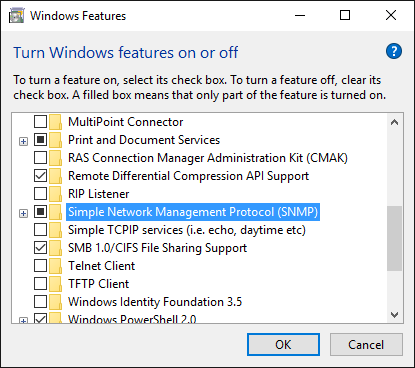
* 1. **Cấu hình SNMP agent trên hệ điều hành Windows**

Tính năng SNMP trên hệ điều hành Windows phải được cài đặt và cấu hình trước có thể giám sát nó bằng một phần mềm SNMP manager. SNMP Service trên Windows là một SNMP agent, nó sẽ đáp ứng các request của phần mềm giám sát, giúp phần mềm giám sát lấy được các thông tin từ một máy chủ Windows.

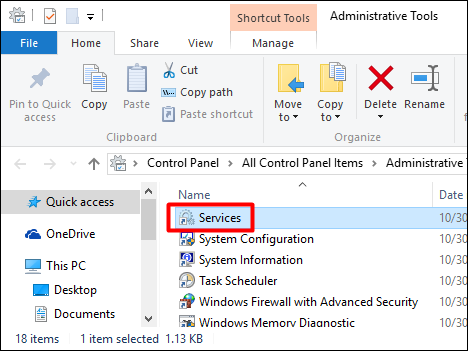
Để cài đặt dịch vụ SNMP, vào [Programs and Features] trong [Control Panel], chọn [Turn Windows features on or off]

Hình 4.1. Turn Windows features on or off

Trong hộp thoại [Windows Features], chọn [Simple Network Management Protocol (SNMP)], nhấn OK để cài đặt dịch vụ SNMP.

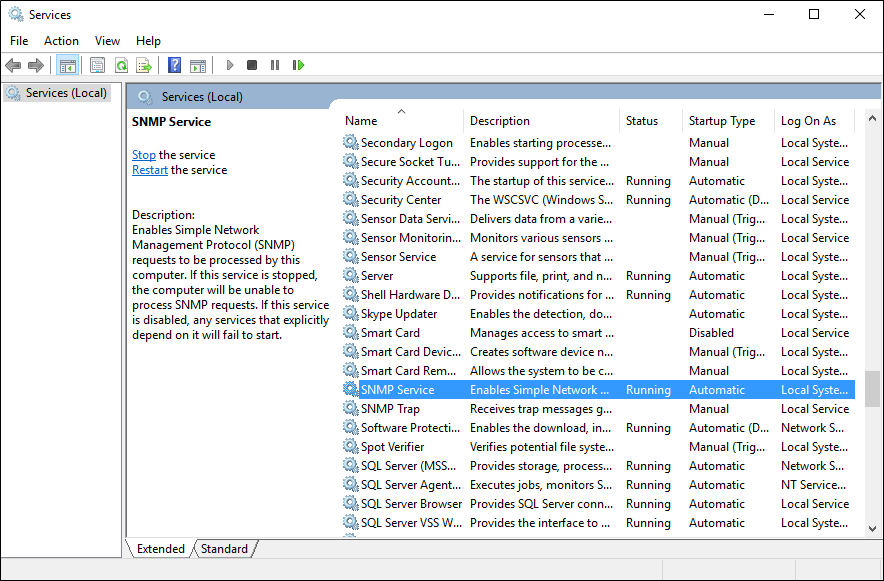


Hình 4.2. Chọn kích hoạt dịch vụ SNMP

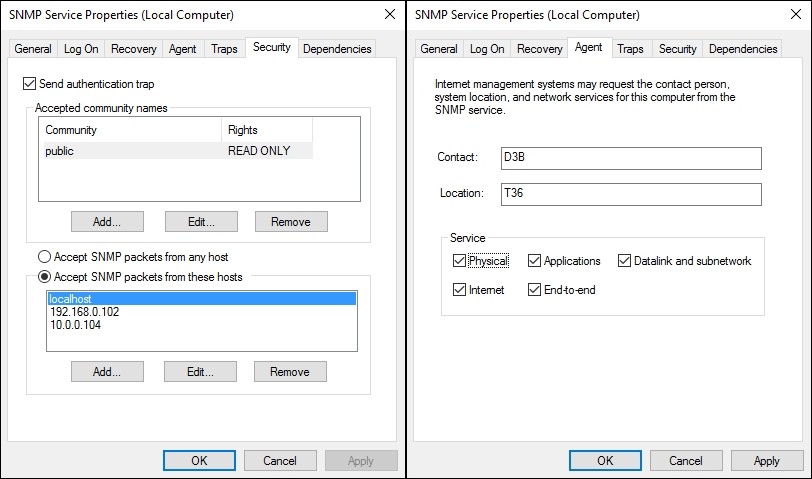
Để kiểm tra và cấu hình SNMP Service, chọn [Administrative Tools] trong [Control Panel], kích đúp chọn [Sevices].

Hình 4.3. Mở Services

SNMP Service đang hoạt động sẽ báo trạng thái Running. Kích đúp vào SNMP Service để vào [SNMP Service Properties].

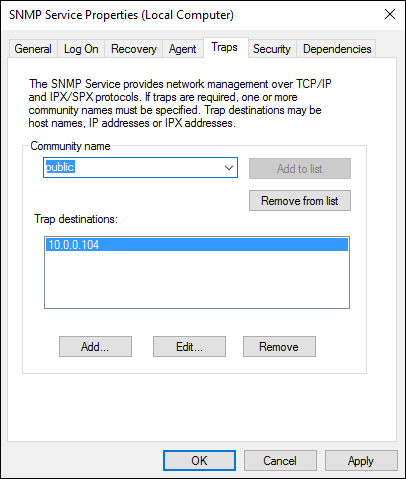


Hình 4.4. Cấu hình SNMP Service

Chuyển qua tab [Security]. Groupbox [Accepted community names] là nơi tạo các community. Danh sách “Accept SNMP packets from these hosts” cho phép đặt SNMP ACL, chỉ cho phép một số SNMP manager nào đó quản lý. Chuyển qua tab [Agent] để khái báo location, contact,...

Hình 4.5. Cấu hình SNMP Agent và Sercurity

Cuối cùng là cấu hình Trap, chuyển qua tab [Traps], nhập vào conmunity name của bản tin trap và nơi nhận trap.

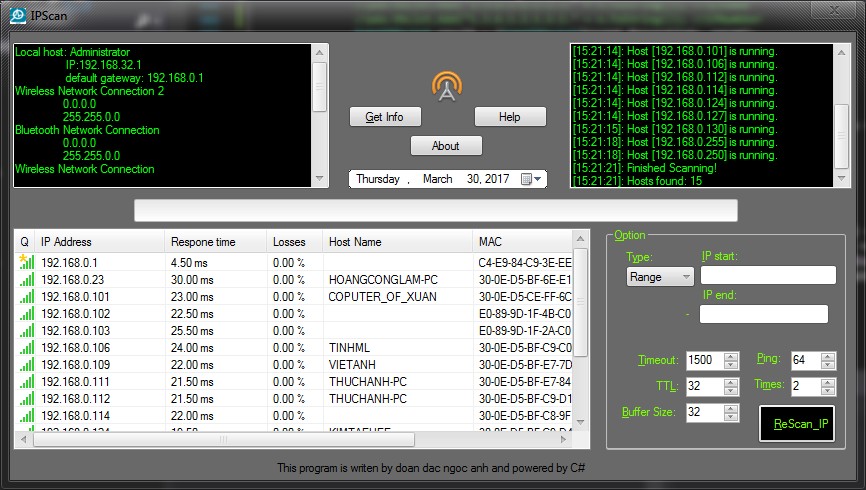


Hình 4.6. Cấu hình SNMP Traps

## **Thiết kế chương trình demo**

Chương trình Demo sử dụng giao thức SNMP được xây dựng trên cơ sở các dịch vụ mà giao thức SNMP hỗ trợ và tham khảo các chức năng của hai phần mềm là Solarwind và PRTG (đã trình bày ở chương 2 và chương 3).

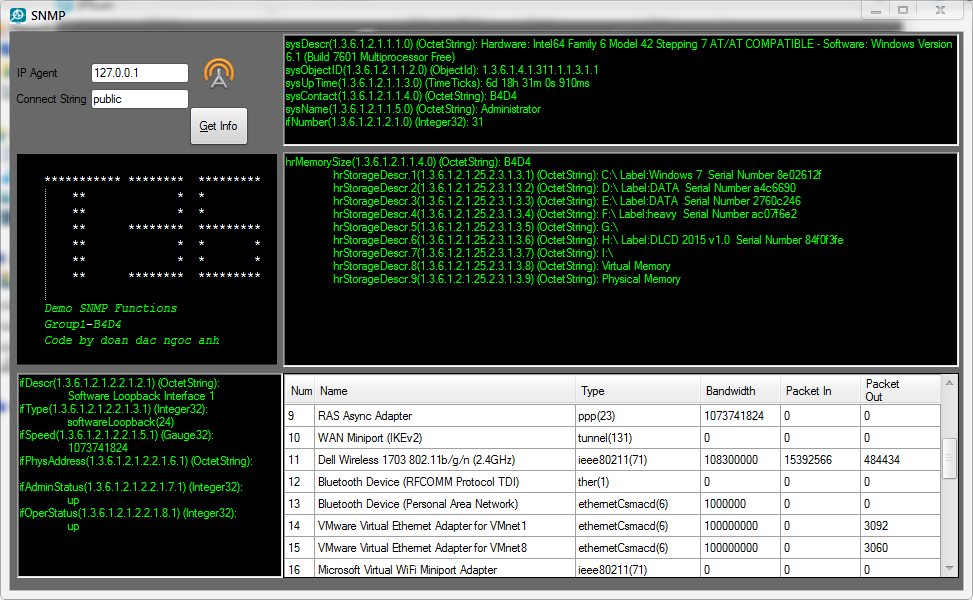
Đầu tiên đó là việc quản lý danh sách thiết bị kết nối đến mạng bằng việc sử dụng công cụ IPScan. Khi khởi động chương trình lên, công cụ sẽ tự tìm ra ip của local host và subnet mask của nó (tương tự như lệnh ipconfig trong windows hoặc ifconfig trên linux), sau đó gửi thử gói ping đến tất cả các ip trong mạng. Thông tin trả về được thống kê trên giao diện của công cụ. Ở góc phía trên bên trái là các thông tin về localhost (bao gồm địa chỉ ip, subnet mask và default gateway của từng card mạng). Ở góc trên bên phải là thống kê các địa chỉ ip đang hoạt động.



Hình 4.7. Chức năng scan ip

Bằng công cụ này chúng ta có thể kiểm tra các địa chỉ ip đang được sử dụng trong một dải mạng hay một lớp mạng cụ thể, tên thiết bị và địa chỉ MAC của nó. Ta có thể thay đổi một số thông số của gói tin ICMP như timeout, số lần ping thành công để xác định địa chỉ ip … từ đó chúng ta có thể xác định danh sách các thiết bị kết nối đến mạng để quản lý. Người dùng có thể tùy chọn sử dụng scan lại ip bằng các option ở góc dưới bên phải. Bằng cách hiệu chỉnh các thông số địa chỉ bắt đầu, địa chỉ đích (hoặc subnet mask) và các thông số gói ping để ReScan các máy trong mạng lại một lần nữa.

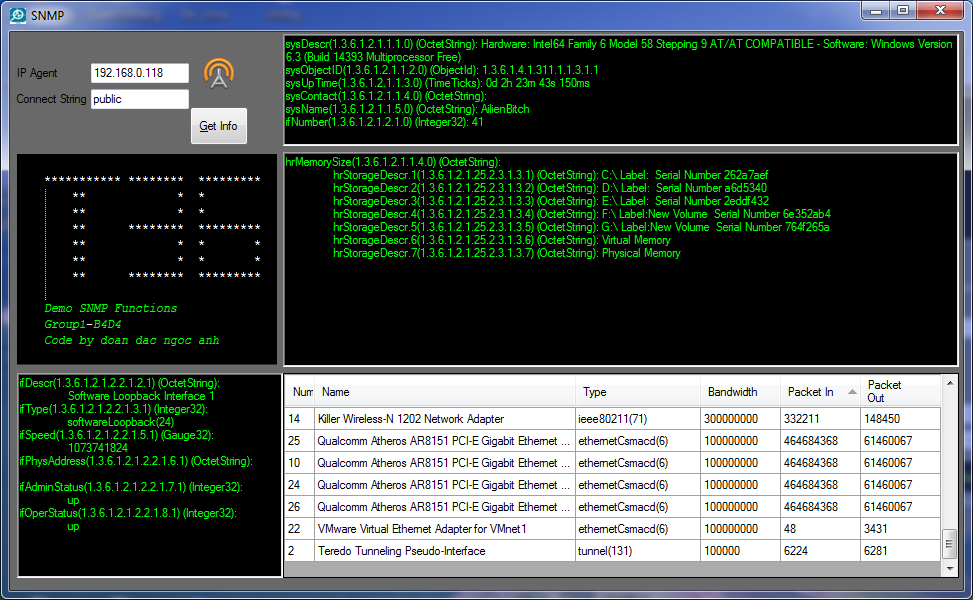
Một chức năng khác của chương trình đó là lấy thông tin từ ip nhập vào, với điều kiện là thiết bị có hỗ trợ SNMP và đã được cấu hình (trình bày ở phần 3.1). Dưới đây là hình ảnh công cụ lấy thông tin từ localhost.



Hình 4.8. Chức năng lấy thông tin trên localhost

Bằng giao thức SNMP và connect string là “public” ta có thể lấy được các thông tin về ngày giờ hệ thống, phần cứng, phần mềm, các thông tin về phân vùng ổ đĩa. Phần giao diện góc dưới bên phải thống kê các cổng thiết bị, loại thiết bị, băng thông và số lượng gói tin gửi vào và gửi ra qua cổng interface đó. Khi nhấn chuột vào mỗi thiết bị thì góc bên trái sẽ hiển thị thông tin chi tiết tương ứng. Từ đó ta có thể xác định một interface có hoạt động hay không qua số lượng gói tin trao đổi qua interface.

Muốn nhận thông tin từ các máy trong cùng mạng thì sau khi mở dịch vụ SNMP cần phải cài đặt community name và Accept SNMP packet from cho máy đích. Kết quả nhận được trên máy quản lý như sau:



Hình 4.9. Chức năng lấy thông tin trên một IP Agent cùng mạng

# KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Sau thời gian thực hiện, đề tài “Nghiên cứu và xây dựng ứng dụng giám sát truy cập Internet”

Đề tài đã thực hiện được các nội dung sau:

* Giới thiệu hai phương thức giám sát mạng cơ bản. Trình bày một số khái niệm nền tảng của giao thức SNMP, các phương thức, cơ chế bảo mật của giao thức này.
* Trình bày tổng quan về hai phần mềm quản trị mạng tiêu biểu là SolarWinds và PRTG, cách cài đặt, cấu hình và sử dụng hai phần mềm này.
* Hướng dẫn cài đặt, cấu hình SNMP agent trên hệ điều hành Window, xây dựng công cụ quản trị mạng demo trên ngôn ngữ lập trình C#.

Trong quá trình thực hiện, mặc dù nhóm sinh viên đã có nhiều cố gắng nhưng do hạn chế về kỹ năng và thời gian thực hiện nên đề tài chỉ tìm hiểu về những mặt cơ bản nhất của giao thức SNMP cũng như hai phần mềm quản trị mạng đã nêu và cũng không tránh khỏi thiếu sót.

Lợi thế của nhóm là đã được tham khảo đề tài và chương trình demo của nhóm sinh viên khóa trước. Hướng phát triển của đề tài là tiếp tục tìm hiểu sâu hơn về giao thức SNMP, hoàn thiện chương trình demo để ứng dụng hỗ trợ trong thực tế.

**TÀI LIỆU THAM KHẢO**

[1] Sergey Poznyakoff, “Gnu Radius Reference Manual”, Published by Free Software Foundation, 2003

[2] Ralph Droms, Ted Lemon, “The DHCP Handbook”, 2nd Edition, SAMS, November 2002

[3] R. Droms, W. Arbaugh, “Authentication for DHCP Messages”, RFC 3118, June 2001

[4] Chirag Sheth, Rajesh Thakker, “Performance Evaluation and Comparative Analysis of Network Firewalls”, 2011 IEEE

[5] Christopher M. Buechler, Jim Pingle, “The Definitive Guide to the PFSense Open Source Firewall and Router Distribution”, 2009

[6] Matt Williamson, “PFSense2 Cookbook”, 2011 Packt Publishing [7] The FreeRADIUS Server Project and Contributors, 2014, <http://freeradius.org/doc/>

[8] Benny Czarny, “Network Access Control Technologies”, OPSWAT Inc,

[9]https://www.opswat.com/sites/default/files/Network\_Access\_Control\_Technolo gies.pdf [10]http://en.wikipedia.org/wiki/Network\_Admission\_Control [11]http://en.wikipedia.org/wiki/Network\_Access\_Protection [12]http://en.wikipedia.org/wiki/Trusted\_Network\_Connect

[13]Đinh Hồng Ngọc (2014), Nâng cao hiệu quả quản lý truy cập mạng cho hệ thống firewall PFSense với tập người dùng động, Luận văn Thạc sĩ, Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội. [14]http://cait.vnu.edu.vn/giai-phap/28/squid-proxy-cho-quan-ly-truy-cap-internet