VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Wandati Richard Kagia

Open source network management

Technology and Communication
2010

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Degree Programme

ABSTRACT

Author	Wandati Richard Kagia
Title	Open Source Network Management
Year	2010
Language	English
Pages	39 + 2 Appendices
Name of Supervisor:	Gao Chao (Dr. Eng.)

The objective of this thesis was to research on open source program that is capable of monitoring network that will show the uptime information by the querying the traffic using SNMP. I was to create network with two routers and two switches together with the server.

I was able to implement the required features with open source Nagios core. Nagios is an open source that customized using the plugin's that Nagios community have already is capable of doing a lot of work in the network management.

Having installed Nagios core server and customized it I was able to come up with the desired results.

Nagios is strong and stable open source program used wisely and widely can be recommended to technology companies and institutions for their network management.

Keywords Open source, network management

CONTENTS

ABBREVIATIONS

ASN.1	Abstract Syntax Notation One
API	Application Programming Interface
CGI	Common Gateway Interface
GNU	General Public License (GPL)
HTML	Hyper Text Markup Language
HTTP	Hyper Terminal Transmission Protocol
ISO/OSI	International Organization for Standardization/Open System Interconnection
LAN	Local Area Network
SNMP	Simple Network Management Protocol
TCP/IP	Transmission control protocol/internet protocol
MIB	Management Information Base
OID	Object Identifier
PDU	Protocol Data Unit
PHP	Hypertext pre-processor
RFC	Request for Comment
WAN	Wide Area Network
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language

LIST OF FIGURES

LISTS OF TABLES

1 INTRODUCTION

Technicians and programmes are working hard to come up with new technology inventions every day, with that technology is changing with a rapid speed. Everything is becoming networked from basic house devices to complex company's devices. The challenge now lies on how to make sure that everything is working fine how to control and manage the network.

It could be difficult or close to impossible to manage network by just making network connections and assume that by looking with our naked eyes or following the link status from one place to the other things will be okay.

The free and open source community has played a significant role in developing network management applications that can handle the networking management services like the program NAGIOS am going to check onto.

The objective of this project is to research and implement on open software Nagios which is capable of showing the status of uptime and downtime information of the network and also monitoring the routers/switches by sending a queries via SNMP for network traffic.

Nagios is the program designed to show this features easily after connecting with switches and routers.

1.1 Networking/Network Management

Linking two or more devices for the purpose of sharing data is called networking. Networks are built with a mix of computer hardware and computer software. Networks are categorized in several different ways, Local area networks (LANs), for example reach across single home, whereas wide area networks (WANs), reach across cities and states or even across the world. Networks are designed in two type's client-server and peer to peer. Client-server networks feature centralized server computers that stores email, web pages, files or application. On peer to peer computers tend to support the same functions commonly found in homes.

The communication language used by computer devices is called protocol. Networks often implement multiple protocols to support specific application the popular protocol include TCP/IP. Transmission control protocol/internet protocol is the mostly commonly used protocol on internet.

TCP/IP data are transferred without interferences; the protocol is independent of physical medium used to transmit data which most ends up with Ethernet frames. In LAN, the Ethernet is the most common hardware with a speed of 10, 100 to 1000 megabits per second. [1] Most organizations need an IT network to process and store huge amount of data that's why they work on servers, databases, routers, etc. The data been transferred is important for the intended operation, it is therefore necessary to utilize network management software which will protect the network from any faults and system errors.

Network management are the activities, methods, procedures and tools that pertains operation, administration and maintenance of networked systems.

1.2 Open–Source

A programme becomes open source if the source code is available or is accessible for changes or modification. We can call software free or open source if it follows the open source initiative license and supports the GNU licence. That means any parties are not bound after modification to sell the licence or give away the software licence without any royalty or any fee for that sale.

Most people define open source based on various needs or usage to meet their intended purpose. Some commercial companies use the open source to make similar open source software for commercial purposes.

1.3 Requirement and Specification of the Project

The main requirement on this project is to explore on the open source world and find a good program that will be able to monitor network. A program that will be capable of showing the uptime and down time status of the network, and also which will be able to get information of the network through the queries of the traffic information of the network.

Nagios core is one of the stable open source programs that will be used to explore and find out whether it will be able to meet the requirements of the project.

The main task of the project will be to create a network with two Cisco routers and two Cisco catalyst switches to form three LANs which will be monitored by the program. In this task the routers and switches will be configured and meet the required results for the project.

1.4 Outline of the Study

Chapter 2 presents the technological requirements for the project.

Chapter 3 presents how network is organized.

Chapter 4 presents the methods used in installations and configurations.

Chapter 5 presents conclusion and evaluation followed by list of references and with appendices.

2 TECHNOLOGICAL REQUIREMENTS

2.1 Nagios Definition

Nagios is a monitoring system that enables identify and resolve IT infrastructure problems before they get to critical stage. Nagios monitors entire IT infrastructure and ensures system services, applications are functioning properly, in case of failure Nagios is able to notify the concerned administrator in order to rectify the problems.

Nagios monitors the applications, services, operating systems, network protocols and system metrics. It is fast in detecting the infrastructure outages. Alerts can be delivered to technical staff.

In case there is problem alert acknowledgement provides communication on known issues and problem response, Nagios has event handlers which allow automatic restart of failed applications and services.

Nagios is a customizable code that is open software full of access which is released under the GPL licence. It has a powerful script API which allows easy monitoring of in-house and custom applications, services, and systems.

Nagios uses Plugins, Plugins are compiled executables scripts (Perl, shell, C, java, etc.) that can be run from command line check the status, host or service. Nagios uses the results from plugins to determine the current status or hosts and services on the network. Nagios uses CGI scripts which is web scripting facility which can be used with any programming language [2]

2.2 Nagios Architecture

Nagios is built on server/agents architecture. Nagios server runs on the host, and plugins sends information to the server, which displays them in Graphical user interface (GUI) as shown in Figure 1 below. Nagios is composed of three parts:

- A scheduler, the server part of Nagios, at regular interval the, the scheduler checks the plugins and according, to the results do some action.

- A GUI is the interface of Nagios with configurations and alerts it displayed in web pages generated by CGI, it can be state buttons (green, Ok/red, Error)

- The plugins, they are configured by the user; they check service and return results to the Nagios server.

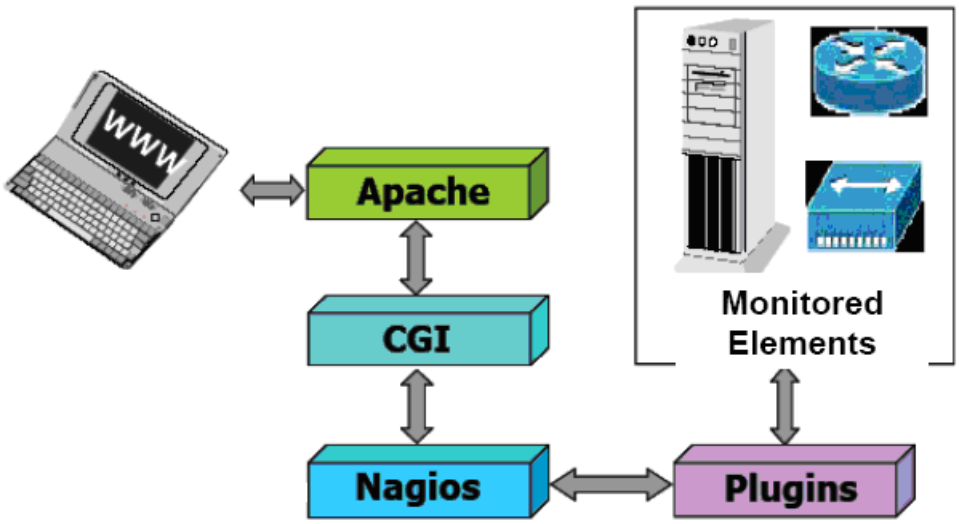

Figure 1. Nagios architecture

2.3 Operating System

Nagios was originally created under the name NetSaint was written and maintained by Ethan Galstad, along with other developers who maintained both official and unofficial plugins. NAGIOS acronym “Nagios aint gonna insist on Saint-hood”

Nagios was originally designed to run under GNU/Linux but it also runs well on Windows and Mac operating systems. The Nagios supports different operating systems distributions namely:

- Ubuntu
- Suse
- Federo
- Debian
- PLD Linux
- OpenBSD
- DragonFly BSD
- Mandriva
- Free BSD

The open source Debian distribution, Ubuntu 9.10 is used to set up Nagios server and with proper installation it will run on it.

2.4 Apache

Apache is prerequisite for Nagios to work; to display any information a web server apache is required. With so much growth of World Wide Web Apache has played a big role, Apache is HTTP server which was developed and maintained by open source developers, it allows the web page to be displayed in the World Wide Web using a web browser. Apache is available for windows and Unix Operating systems and the latest version being Apache2, it can be downloaded and installed for free. Apache is the most widely used web server than all the web servers.

Apache is compatible with most scripting languages like Hypertext Pre-processor (PHP), Python, Perl and many others. Installation of Apache 2 is done by using command prompt and typing *"sudo apt-get install apache2"* by this command the apache 2 is installed. To confirm the Installation the following command is used to test and start Apache2 *"sudo /etc/init.d/apache2 start"* if everything is fine it will give ok response.

2.5 PHP

Nagios use PHP for the web interface, without PHP the web interface will not be available. PHP is widely used scripting language which is well suited for web development which is easily embedded in HTML. PHP is an open source scripting language; it is used as server-side scripting where you need three components to make this work PHP parser, web server and a web browser. It is also used as a command line scripting which does not require any server to run all that is needed is PHP parser. PHP is used in most operating systems. The Nagios uses different scripting languages and PHP is one of them.

PHP support web server apache 2 hence the installation on Ubuntu 9.10 as a pre-requisite to the installation of Nagios, it is also capable of outputting different files like HTML, XHTML, XML, images and PDF.

PHP has support for talking with other services using protocols such as HTTP and SNMP. PHP5 is the latest version which is installed in this project. The command for installing PHP5 is: *"sudo apt-get install php5 libapache2-mod-php"* [3]

2.6 SNMP

2.6.1 Purpose of SNMP

SNMP (Simple network management protocol) was introduced in 1988 to meet the growing need for a standard for managing the TCP/IP devices.

SNMP is a simple set of operations and the set of the information these operations gathers that gives the administrators the ability to change the state of SNMP based devices. SNMP can be used in different ways for example, if you want to know

how much traffic is flowing through a network device one needs to poll the device using SNMP, SNMP is also used to shutdown the interface of routers or check the speed at which the Ethernet interface is operating at. In general any device that allows the retrieval of SNMP information can be managed from one console. [4]

The purpose of SNMP is to poll information from the managed devices. Nagios uses this protocol to trap information from the devices that are been managed.

2.6.2 Architecture of SNMP

SNMP consists of three important components, managed device, Agent (software which runs on a managed device) and the network management system (NMS) which is software that runs on the manager for example Nagios. Managers have the task to monitor or manage devices or a group of hosts on a computer network, each managed systems executes, at all times, a software component called an agent which reports information via SNMP to the manager. SNMP agents expose management data on the managed system as variables; SNMP also permits active management tasks like modifying and applying new configurations through remote modifications of these variables. These variables are accessible via SNMP which are organized in hierarchies; these hierarchies and other metadata like type and description of variable are described by Management Information Bases (MIBs). [5] SNMP allows managers and agents to communicate for the purpose of accessing these objects.

MIB is a collection of information organised hierarchically, when management station requests information from the managed device, the agent receives the request and retrieves the appropriate information from the MIBs. In general we can define a MIB as a database that stores management information about a device.

Figure 2 [6] shows SNMP management system architecture, NMS communicates with SNMP Agent MIBs. In the figure the manager is the NMS and the MIB is the managed device (Cisco router/switches).

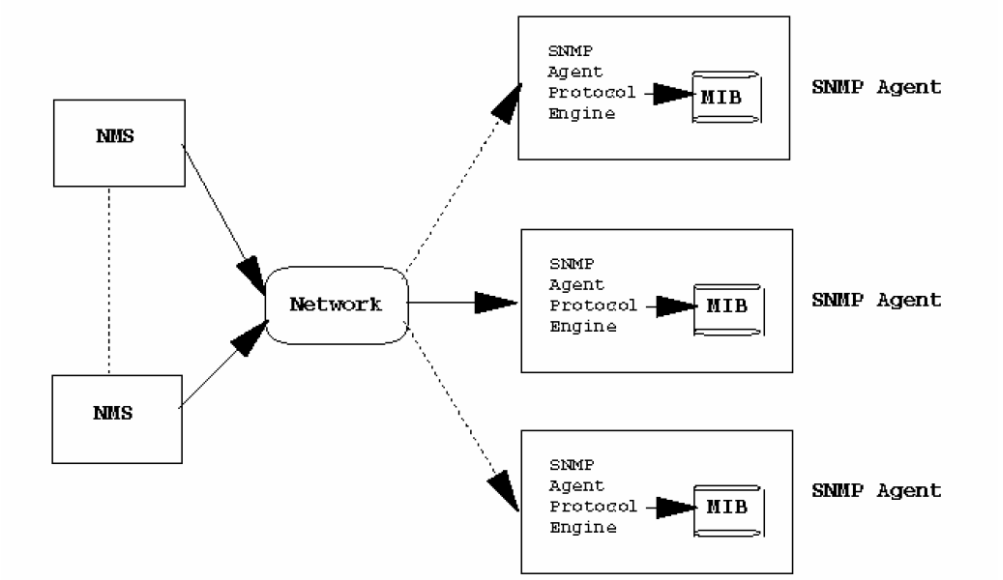

Figure 2. Architecture of SNMP management System.

2.6.3 SNMP Protocol Details

SNMP facilitates the exchange of management information between networked devices operating at application layer of ISO/OSI model. It's intended to operate over the user datagram protocol (UDP). UDP port 160 is capable of SNMP messages and UDP uses port 162 for listening to the SNMP trap messages.

SNMP defines client/server relationship; the client program called the SNMP manager makes connection to a server program called the SNMP agent which resides on a remote network device for example a Cisco router, which serves information to the network manager regarding the status of the device. SNMP is like a service to manage distributed objects.

SNMP manager maintains the central database (MIB) that is fed by queries to the SNMP agents which are all over the network. SNMP is based on request and response commands. A management system sends a Get or GetNext command to request values of MIB variables from an agent, or set request to modify the value of a variable. Once the data is collected, management system can present views of the information or take action in response to the information provided by the SNMP agents. [7] An example when a manager wants to know the CPU utilization information of a Cisco router/switch, the manager sends a request to the

agent; if the agent gets information from the CISCO-PROCESS MIB which contains cpmCPUTotal5minRev MIB as an object. The agent responds to the manager with the objects for action. When the manager receives the object and checks what the object corresponds to in the MIB database for views.

2.6.4 SNMP Messages Types

There are five types of messages exchanged in SNMP, there are referred to by Protocol Data Unit (PDU). The SNMP PDU is defined by the ASN.1 (Abstract Syntax Notation one) data types.

Get-request

Retrieves the value of a MIB variable stored on the agent device it can be an integer, string, or address of another MIB variable. (Manager to agent)

Get-next-request

Retrieves the next specified MIB variables. (Manager to agent)

Set-request

Changes value of the MIB variables. (Manager to agent)

Get-response

Returns value of the MIB variables. (Agent to manager)

Trap

Agent notifies the manager of unsolicited notification, something unexpected, like an error.

In Figure 3[6] below shows the SNMP message format, each variable binding contains an identifier, a type and a value.

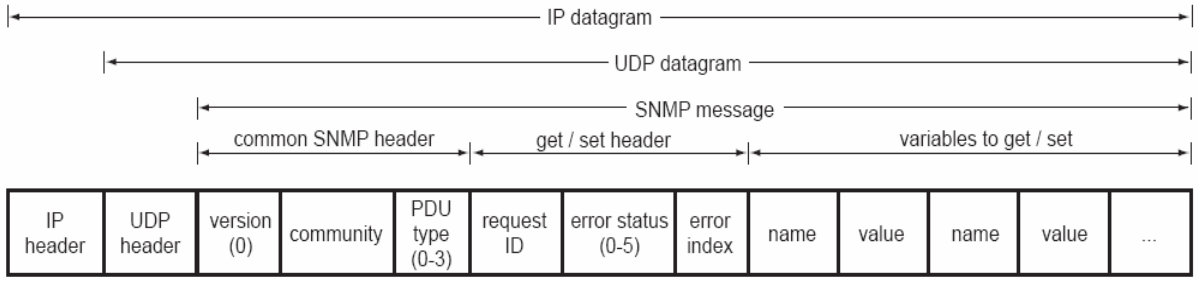

Figure 3. SNMP message format

The Varbind or variable binding is a sequence of two specific fields; the first is an OBJECT INDENTIFIER (OID) which addresses specific parameter, the second field contains values of a specified parameter. In Get-request value is null with length 0x00. This null data is placeholder for the value data that the SNMP agent returns using the Get-response. Table 1 [8] explains more of each field.

Field	Description
SNMP message	A Sequence representing the entire SNMP message consisting of the SNMP version, Community String, and SNMP PDU.
SNMP Version	An Integer that identifies the version of SNMP. SNMPv1 = 0
SNMP Community String	An Octet String that may contain a string used to add security to SNMP devices.
SNMP PDU	An SNMP PDU contains the body of the SNMP message. There are several types of PDUs. Three common PDUs are GetRequest, GetResponse, SetRequest.
Request ID	An Integer that identifies a particular SNMP request. This index is echoed back in the response from the SNMP agent, allowing the SNMP manager to match an incoming response to the appropriate request.
Error	An Integer set to 0x00 in the request sent by the SNMP manager. The SNMP agent places an error code in this field in the response message if an error occurred processing the request. Some error codes include:
	• 0x00 -- No error occurred
	• 0x01 -- Response message too large to transport
	• 0x02 -- The name of the requested object was not found

	• 0x03 -- A data type in the request did not match the data type in the SNMP agent
	• 0x04 -- The SNMP manager attempted to set a read-only parameter
	• 0x05 -- General Error (some error other than the ones listed above)
Error Index	If an Error occurs, the Error Index holds a pointer to the Object that caused the error; otherwise the Error Index is 0x00.
Varbind List	A Sequence of Varbinds.
Varbind	A Sequence of two fields, an Object ID and the value for/from that Object ID.
Object Identifier	An Object Identifier that points to a particular parameter in the SNMP agent.
Value	SetRequest PDU -- Value is applied to the specified OID of the SNMP agent.
	GetRequest PDU -- Value is a Null that acts as a place-holder for the return data.
	GetResponse PDU -- The returned Value from the specified OID of the SNMP agent.

Table 1. Fields in the SNMP message

2.6.5 SNMP Management Information Base (MIB)

MIB as a database, contains different manageable objects that have properties, e.g. on the Cisco Routers/switches has a standard MIB Object called "sysUPTime" stores a value that outlines how long a device has been running since the last boot. REQUEST FOR COMMENT (RFC 1213) defines the standard MIB that contains various objects, MIBs are defined as tree structure, and every MIB Object is defined according to a name and associated OID number. The standard SNMP MIB, known as MIB-II, is indentified by the OID 1.3.6.1.2.1. It can also be identified by its name as iso.org.dod.internet.mgmt.mib-2. Cisco devices have an OID branch which begins at 1.3.6.4.1.9 but it can also have its own private MIB objects. [9]

The Figure 4 [10] shows example of how the MIBs are represented as a tree structure according to a name and associated objects.

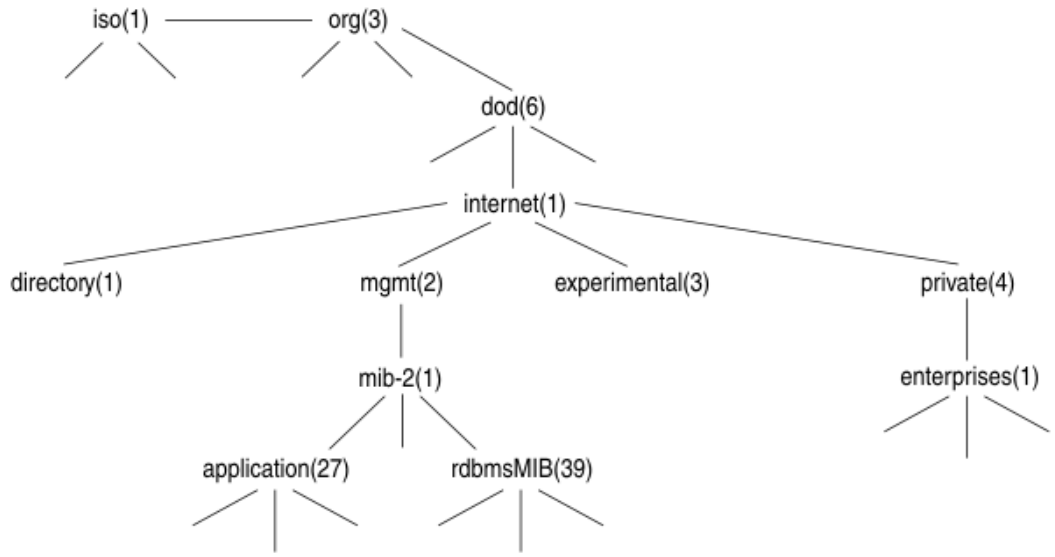

Figure 4. MIB Hierarchy

3 NETWORK ORGANISATION

3.1 Network Architecture

The network architecture of this project consists of two routers and two switches connected to each other with one server. Three subnets are used in this network with the same mask. All the three subnets are on the same network. See Figure 5 and Table 2 for more information.

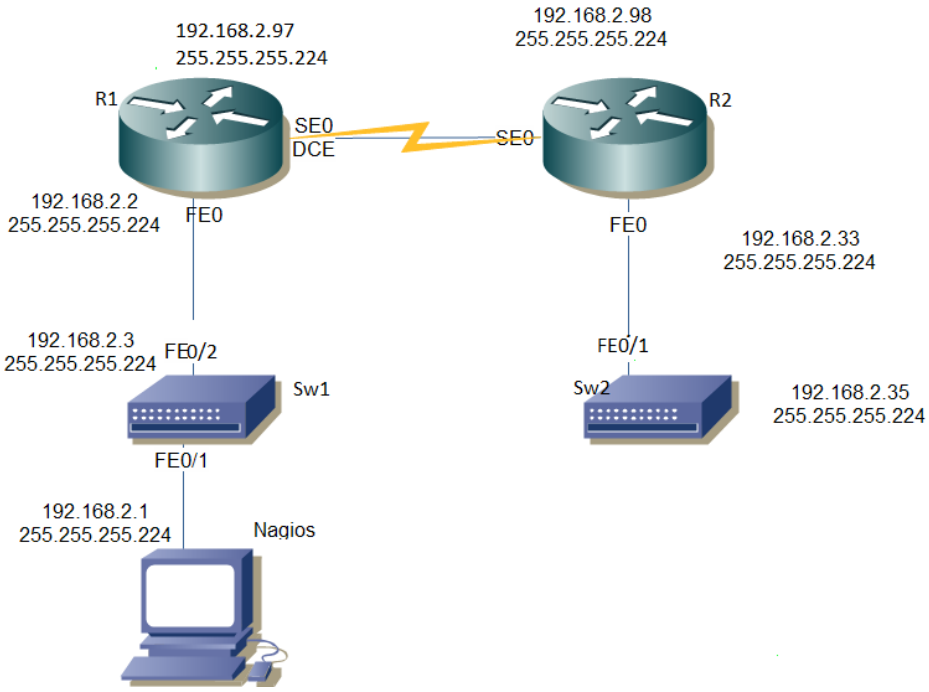

Figure 5. Architecture of test network

Device	Interface	IP Address	Subnet Mask	Default Gateway
Switch 1	Vlan 10	192.168.2.3	255.255.255.224	
Switch 2	Vlan 10	192.168.2.35	255.255.255.224	
Router 1	FE0	192.168.2.2	255.255.255.224	
	SE0	192.168.2.97	255.255.255.224	
Router 2	FE0	192.168.2.33	255.255.255.224	
	SE0	192.168.2.98	255.255.255.224	
PC /Nagios	-----	192.168.2.1	255.255.255.224	192.168.2.2

Table 2. Network addressing topology

3.2 Cisco Switch Configuration

In this project Cisco catalyst 2960 is used which is combatable with Nagios server, IP address is assigned to the two switches which is done by configuring the Vlans in both switches and assigning IP address to them. See *Appendices 1* for more details in the configurations of the two switches.

3.3 Cisco Router Configuration

In this project Cisco 2800 routers are used, Cisco devices by default there have SNMP utilities installed therefore they support SNMP; Cisco uses MIB-2 by default. [11] The only thing that should be clear is how to set the community string which should correspond to the settings of the host. In this project I use community string as public. The host address should be included to allow all the traps to be forwarded to the host. See *Appendix 2* for more details on configurations.

snmp-server host 192.168.2.1 traps snmpv2

snmp-server community public – This is the community string that is been set.

snmp-server enable traps snmp warmstart linkdown linkup coldstart

Commands configurations above, first command line allows all the traps to be sent to the manager (Nagios), the second command is setting the community string and the last is enabling the traps in the Cisco device.

4 METHODS

4.1 Nagios

A). Nagios Installation

Having installed the Apache 2 and PHP the next thing is to create account information for Nagios to use the service and group to run external commands, in command prompt we type

```
sudo useradd -m nagios
sudo passwd nagios
sudo groupadd nagcmd
sudo usermod -a -G nagcmd nagios
sudo usermod -a -G nagcmd www-data
```

The next step is to download the latest Nagios and plugins from Nagios website www.nagios.org. After downloading I install the Nagios tar balls with the command tar *-zxvf nagios-3.2.3.tar.gz* then change directory to the extracted folder and install.

```
cd nagios-3.2.3
sudo ./configure –with-command-group=nagcmd
sudo make all
sudo make install
sudo make install-init
sudo make install-config
sudo make install-commandmode
sudo make install-webconfs
```

Next I add the user for the Nagios interface: *sudo mkdir /usr/local/nagios/etc*

Then I create a new password: s*udo htpasswd -c usr/local/nagios/etc/htpasswd.users nagiosadmin* after that I restart the Apache2 config to make changes of the web interface to take effect *sudo etc/init.d/apache2 restart*

Having installed Nagios the next thing is to install the plugins, I change directory to the extracted folder and install.

```
cd nagios-plugins-1.4.15
sudo ./configure –with-nagios-user=nagios—with-nagios-group=nagios
sudo make
sudo make install
```

After that I will create a link to start the service: *sudo ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios*

To verify the configurations run the command*: sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg*

If configuration shows no errors or warnings Nagios can be started by: *sudo /etc/init.d/nagios start* in the command prompt.

In the browser I can start the Nagios in the web interface at local host address and everything should be fine. The Figure 6 shows how to access on Nagios server.

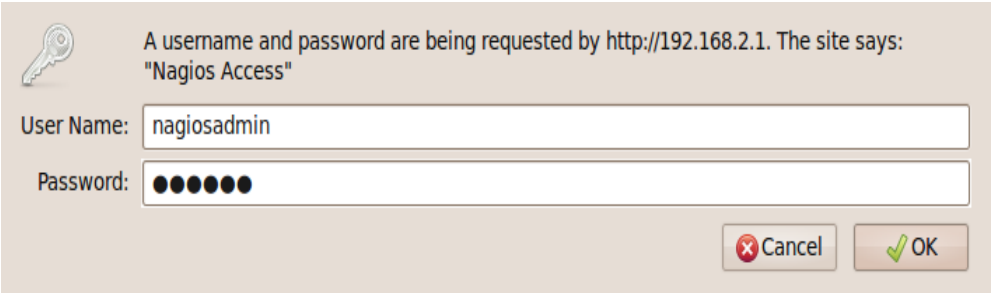

Figure 6. Accesses to Nagios sever.

Figure 7 illustrates the front page of the Nagios on the left panel showing the control features of the server.

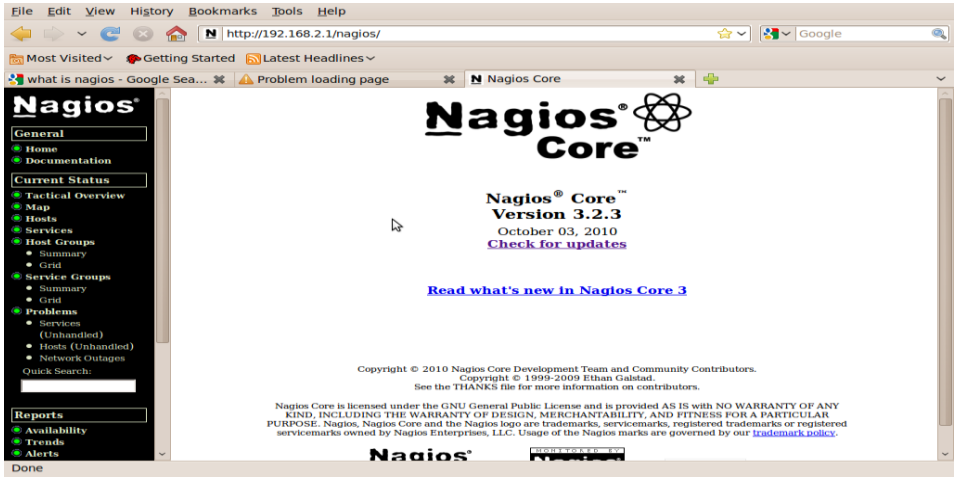

Figure 7. Front page of Nagios

B). SNMP-Installation

Net-SNMP is a suite of applications that is used to implement SNMP v1, SNMP v2 and SNMP v3 using both IPv4 and IPv6. In this project SNMP v2 is used. The suite installed in the server includes applications; snmpget is capable of retrieving SNMP from devices. Snmptrapd is a daemon application for receiving notifications, and snmptranslate is capable of translating numerical and textual forms of MIB OIDs. Net-SNMP is installed by downloading the latest version from http://net-snmp.sourceforge.net/ and running the *1.) . /configure 2.) Make 3.)Make install* in command prompt. [12] By having the suite installed it will allow the Nagios server to send traps as well as send request to the Cisco routers and Switches depending on the MIBs information required.

4.2 Nagios Configurations

Nagios has different configuration files; Nagios uses object configuration file for monitoring; it contains definition for hosts, host groups, services, commands, and so on. Template file is used by Nagios periodically for updating comment data, status data e.tc it is normally deleted when not in use.

Resource file is used to specify the an optional resource file that can contain macro definitions, macros are computer instructions that result in a series of instructions in a machine language, macros are important for storing usernames, passwords and items commonly used in command definitions.

However not all macros may be valid, Nagios has valid macros as follows: service checks, service notifications, host checks host notifications, service event handlers and many others.

Downtime file allows Nagios user to schedule periods of planned downtime for hosts and service been monitored this is very useful especially if one knows he is taking the server down for upgrade. Notifications and alerts are not sent when in down time. [13]

Figure 8 below illustrates how downtime is configured in Nagios.

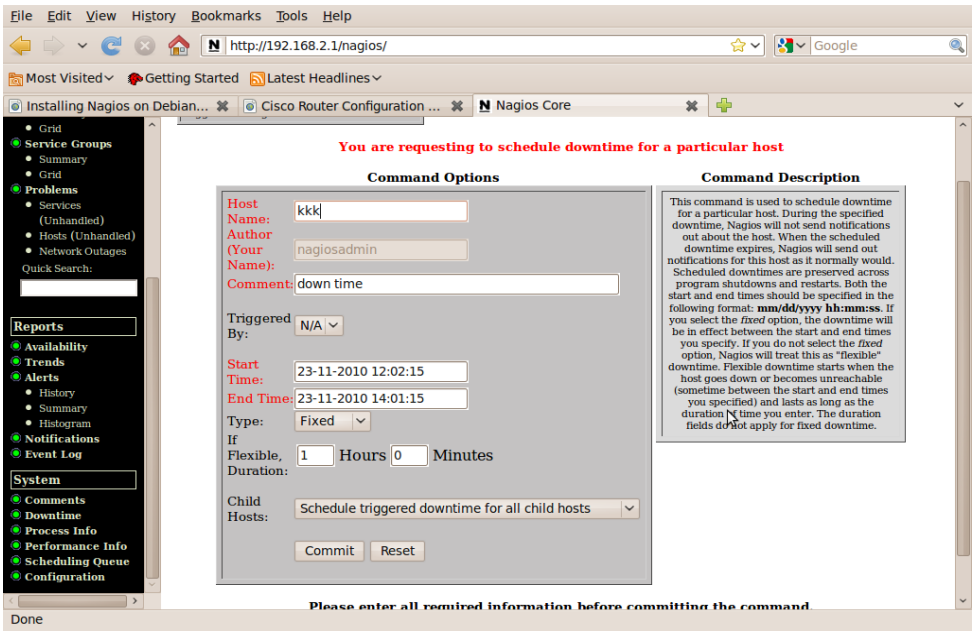

Figure 8. Downtime configuration

4.2.1 Definition of Switches/Routers in Nagios

Both Switches to be monitored in this project are defined in Nagios; this is done by defining the host which is the switch and assigning the IP addresses.

```
define host{
        use             generic-switch
        host_name       Cisco-Switch1
        alias           Sw1 Switch
        address         192.168.2.3
        hostgroups      switches
        }
```

The routers to be monitored are defined the same way as switches with assigning of the IP address respectively.

A template is defined for switches/routers

```
define host{
        name            generic-switch    ; The name of this host template
        use             generic-host      ; Inherit default values
        check_period            24x7      ; By default, switches are monitored
        check_interval          2         ; Switches are checked every 5 min
        retry_interval          1         ; Schedule host check retries at 1 min
        max_check_attempts      10        ; Check each switch 10 times (max)
        check_command           check-host-alive  ; Default command check
        notification_period     24x7          ; Send notifications at any time
        notification_interval   30    ; Resend notifications every 30 minutes
```

The name of the host monitored is defined which inherits the default values from generic-host template; it checks the switch/routers 24/7 and sends notifications all the time.

4.2.2 Enabling Services in Nagios

Below shows an example of the definition of the services to be monitored in this project for retrieving the Uptime information.

```
define service{
        use                     generic-service ; Inherit values from a template
        host_name               Cisco-Switch1,Cisco-Switch2
        service_description     Uptime
        check_command           check_snmp!-C public -o sysUpTime.0

        }
```

In the check command directive of the service definition, the -C public tells the plugin that the SNMP community string to be used is Public, and the -o sysUPTime.0 indicates which OID should be checked in the devices which is

defined in RFC MIBs.

The command definition for the service above is

```
define command{
        command_name    check_snmp
        command_line    $USER1$/check_snmp -H $HOSTADDRESS$ $ARG1$

        }
```

Another example of a service which can be monitored in Cisco routers and Switches is system description which will show the description of the device. this service use the same command definition as above.

```
define service{
        use                     generic-service ; Inherit values from a template
        host_name               Cisco-Switch1,Cisco-Switch2
        Service_description     System Description
        check_command           check_snmp!-C public -o sysDescr.0

        }
```

When all the configuration have been done without errors and all devices are reachable we are able to see all the services sending alerts in Nagios server showing all is ok.

4.2.3 Monitoring Network with Nagios

After making configurations to switches/routers connections are made, in this project different services are monitored in the local host; ping, HTTP, current load, root partitioning, and users are monitored.

There several services monitored in Cisco switches and routers via SNMP as shown on Table 3;

Service	Description
Uptime	It the time the device has been up since the last boot
ports link status	Shows the status of the ports in the routers and switches.
CPU utilization	This service checks the load of CPU, for instance if there is high CPU utilization it can be caused by security issue on the network.
IP Datagram	This shows how many IP Datagram's have been received and how many have been sent out in a device.
Vlans in switches	Retrieves the information of how many Vlans are residing in a particular device.
Memory utilization	This service checks the memory usage in a device.
Routing protocols in routers	The service is able to retrieve the routing protocols used in a particular device.
Interface status	This service shows the interface bandwidth of a device.
Power supply	Checks how the power is supplied in the devices.
Fan status	Checks the speed of the fun in a particular device.
Description of devices	Gives the full information of the device.
Environment of devices	Describes the status of environmental monitoring of a device
Etc	

Table 3. Services monitored in Cisco devices

There are other services which can be monitored by Nagios, e.g. bandwidth by integrating MRTG via log files, and also integrating CACTI to poll data from Nagios and plot it up.

In this project the following services below are enabled to give a clear view of how the MIBs can be retrieved via SNMP on the network. Table 4 Describes services enabled.

Service	Description
UpTime	Shows the information of the device since the last boot
Name	This retrieves the name of each device
CPU	The value of sysUpTime at the time of the last deletion of an entry in the table. if the number of entries has been un-changed since the last re-initialization.
Interfaces	Shows the interfaces status how many are Up and Down.
System Description	Shows the IOS of the device and net-work software.
Traffic Load interfaces	Shows the bandwidth of a particular interface in the device.

Table 4. Enabled services in Nagios

Figure 9 below shows the map of the monitored hosts, when the colour is green it shows that all the hosts are in upstate, if the colour changes to red it means that the host is critical or unreachable

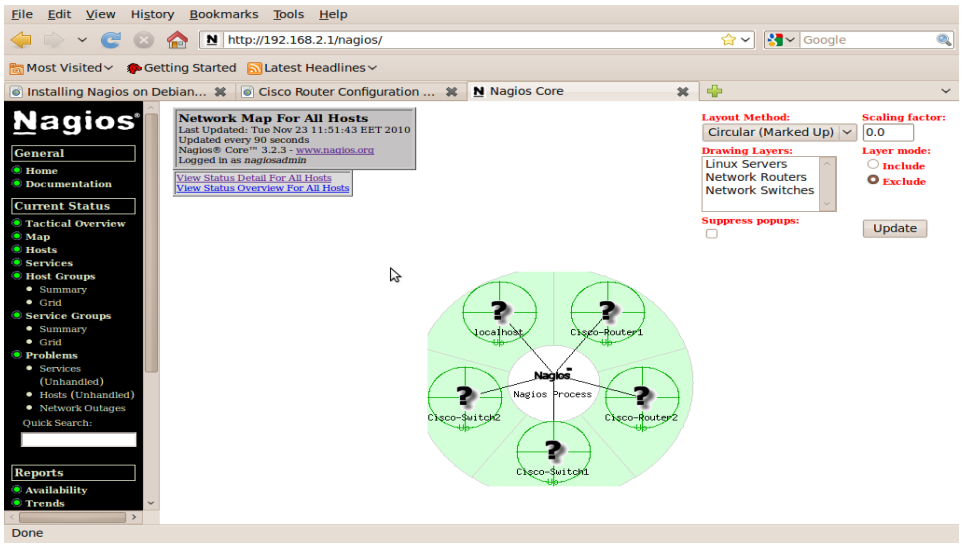

Figure 9. Network map for all hosts

4.2.4 SNMP Configurations in Nagios

In Nagios there is already *check_snmp* plugin which contains the MIBs to be checked on the Cisco Routers/Switches. There are several plugins for SNMP which the Nagios community have made them available for download depending on what one wants to use them for. Figure 10 shows status information of the network services.

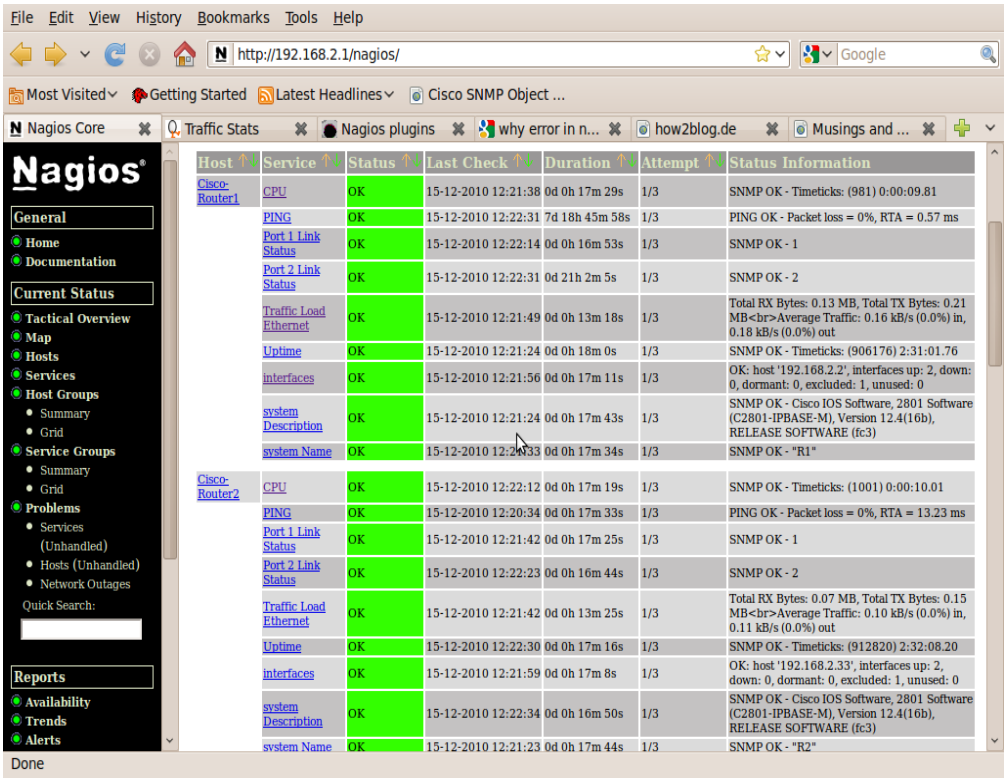

Figure 10. Services information status

When SNMP cannot get information from the network nor is unavailable in any of the devices the information is shown on the status information column like in Figure 11 below.

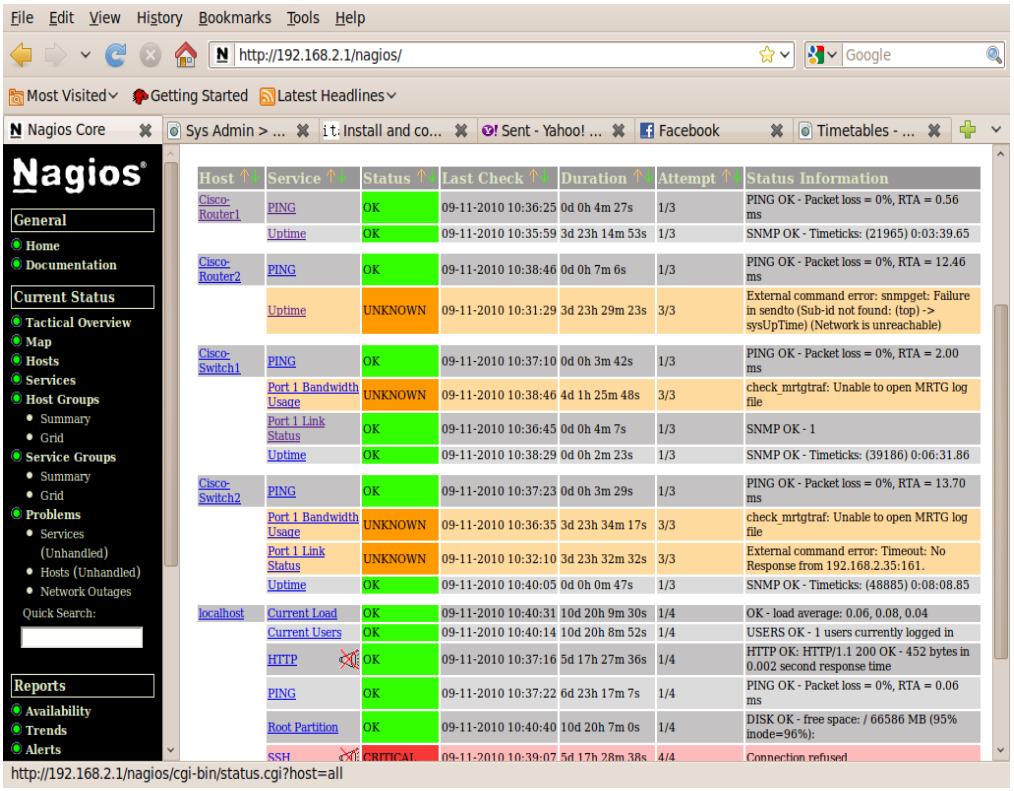

Figure 11. Status information

More details of SNMP received information are shown on the next Figure 12, which shows the Port link performance data showing the port links in up status. If the information is received the SNMP responds with ok status and if not an error status is received.

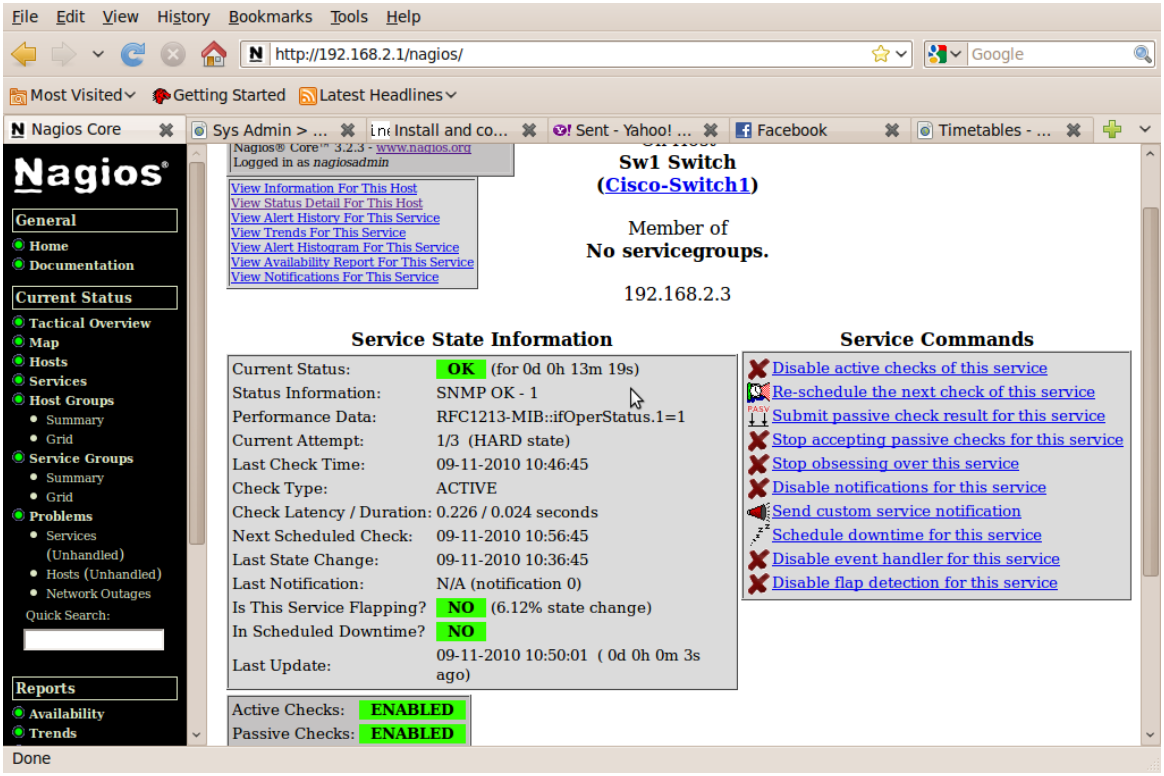

Figure 12. Port link performance data

4.2.5 Wireshark captures

To check that all configurations and everything are running as required, the following wireshark captures shows the Get requests, Get response and Traps in the test network.

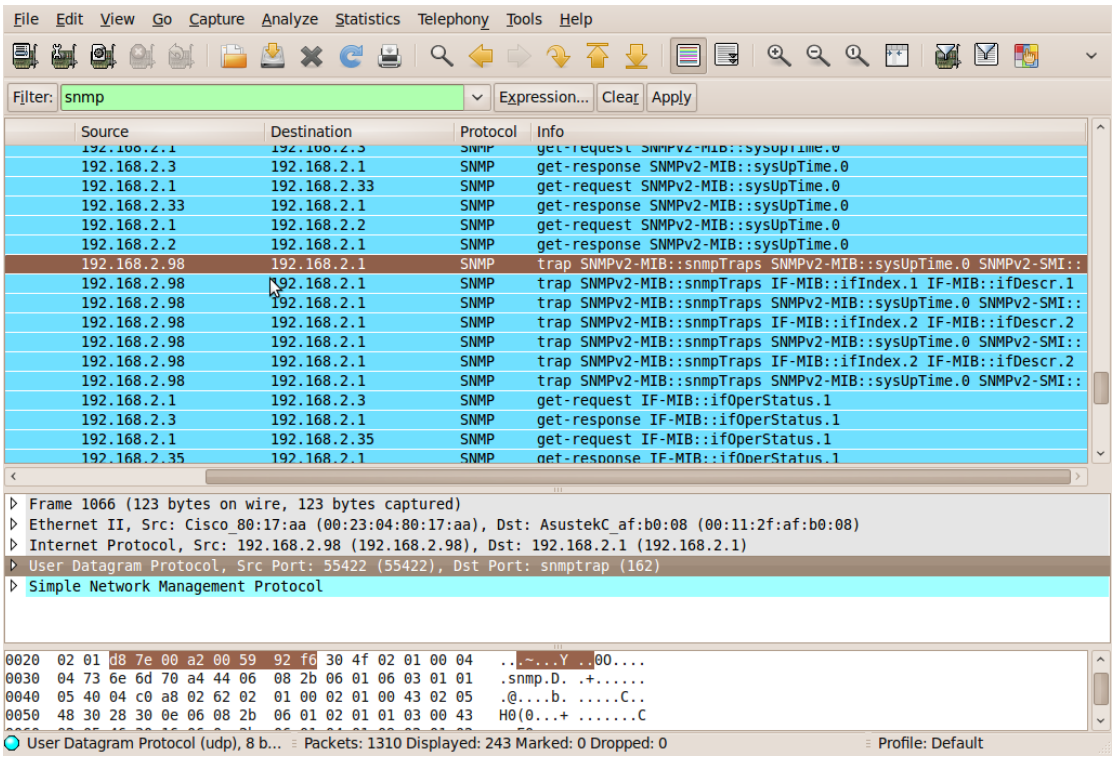

Figure 13. SNMP get-request and get-response capture

In Figure 13 above shows Wireshark capture of SNMP get-request, get-response, and Traps from the network monitored. In the next Figure 14 shows response of Router 2 with address 192.168.2.33 to the Nagios host address 192.168.2.1, the variable binding been SNMPv2-MIB that has an object identifier as sysUpTime which returns no errors.

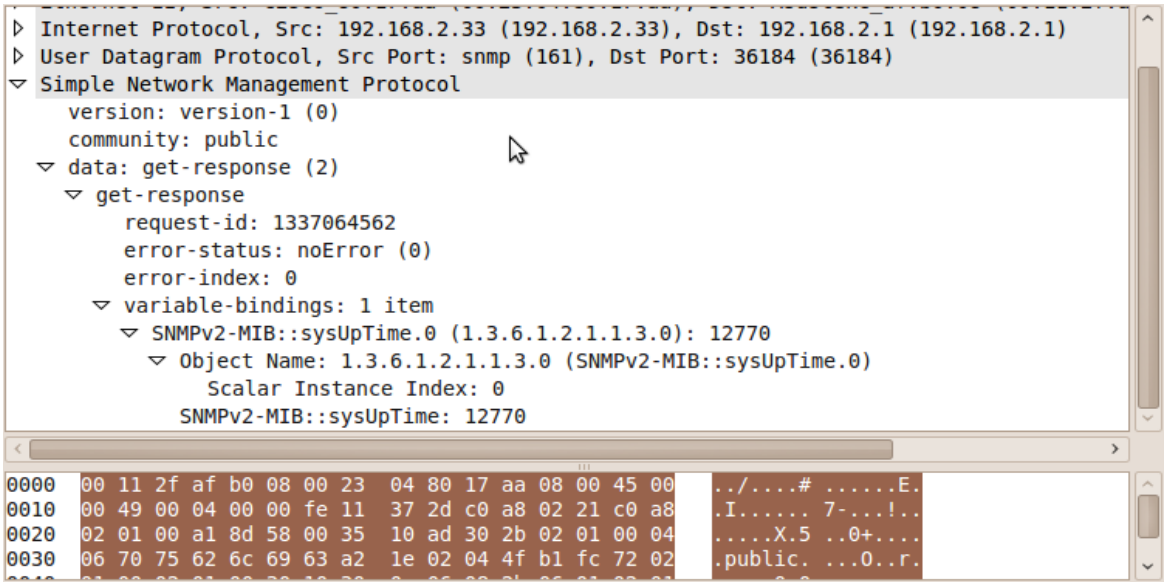

Figure 14. Get-request and Get-response capture

Figure 15 shows the traps received from the agent with address 192.168.2.98 which generates the trap and sends to the address of the host 192.168.2.1, the generic trap sent is coldStart, with variable binding been SNMPv2-MIB with object identifier as snmpTraps.

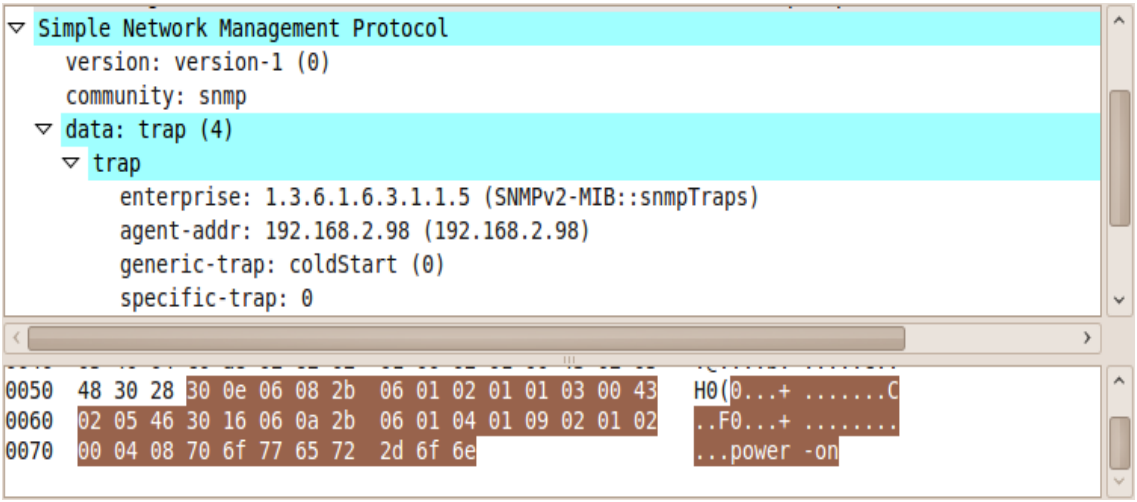

Figure 15. Trap capture

5 CONCLUSION

The purpose of the project was to research on open source program Nagios capable of monitoring network by sending queries to the network and retrieving the information via SNMP. The project was carried out fine and successfully completed; Setting up the Ubuntu server, installing of Nagios server and creating test network to be monitored.

With Nagios so much can be done on the network like setting alerts to be sent to the administrator with status of the network this feature needs internet hence more work should be done to achieve these. I can conclude that Nagios is a perfect tool for network administrators.

Finally I can recommend institutions and companies to use Nagios as a monitoring tool to their network, since it’s free and access of source code is available for changes to meet own required needs.

REFERENCES

[1] Bradley Mitchell, LAN – Local Area Network 2010.

<URL: http://compnetworking.about.com/cs/lanvlanwan/g/bldef_lan.htm>

[2] Nagios community, 2010

<URL: http://www.nagios.org/about/features/ >

[3] Friedhelm Betz, Antony Dovgal, PHP Manual; Edited by Philip Olson 12/11/2010

<URL: http://fi2.php.net/manual/en/intro-whatcando.php>

[4] Douglas R. Mauro and Kevin J. Schmidt, Essential SNMP, July 2001.

<URL: http://docstore.mik.ua/orelly/networking_2ndEd/snmp/index.htm>

[5] J.D.Case, M.Fedor, J.Davin, Simple Network Management Protocol, 1990.

<URL: http://networkshared.com/simple-network-management-protocol/ >

[6] Jean Parrend, SNMP.pdf

<URL: http://www.rzo.free.fr/docs_jean/snmp.pdf >

[7] Andreas Steffen, SNMP 2000–2001, Zürcher Hochschule Winterthu

<URL: http://www.strongsec.com/zhw/KSy_SNMP.pdf >

[8] Douglas Bruey, Simple Network Management Protocol (2005)

<URL: http://www.rane.com/note161.html>

[9] Dan Dinicola, SNMP Management Information Base, 16/05/2007

<URL: http://www.2000trainers.com/ccda-study-guide/management-information-base-mib/ >

[10] IBM Informix SNMP SUBAGENT GUIDE, 2/11/2005

<URL:http://publib.boulder.ibm.com/infocenter/idshelp/v10/index.jsp?topic=/com.ibm.s%20nmp.doc/snmp05.htm>

[11] Cisco system documentation, 2007

<URL:http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

[12] NET-SNMP, by Carnegie Mellon University 2000

<URL: http://net-snmp.sourceforge.net/>

[13] Ethan Galstad, Nagios 1999-2009

<URL: http://nagios.sourceforge.net/>

CISCO SWITCH 1 CONFIGURAION FILE

```
hostname sw1
!
vlan 10
!
ip subnet-zero
vtp domain labra
vtp mode transparent
!
spanning-tree extend system-id
!
!
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
no ip address
!
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
no ip address
spanning-tree portfast
!
interface Vlan10
ip address 192.168.2.3 255.255.255.224
no ip route-cache
```

```
no shutdown
!
ip default-gateway 192.168.2.2
ip http server
!
snmp-server host 192.168.2.1 traps snmpv2
snmp-server community public
snmp-server enable traps snmp warmstart linkdown linkup coldstart
!
line con 0
line vty 0 4
password cisco
login
line vty 5 15
login
```

CISCO SWITCH 2 CONFIGURAION FILE

```
hostname sw2
vlan 10
!
ip subnet-zero
vtp domain labra
vtp mode transparent
!
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 no ip address
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
 no ip address
 spanning-tree portfast
!
interface Vlan10
 ip address 192.168.2.35 255.255.255.224
 no ip route-cache
```

```
no shutdown
!
ip default-gateway 192.168.2.33
ip http server
!
snmp-server host 192.168.2.1 traps snmpv2
snmp-server community public
snmp-server enable traps snmp warmstart linkdown linkup coldstart


!
line con 0
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
```

CISCO ROUTER 1 CONFIGURAION FILE

```
hostname R1
boot-start-marker
boot-end-marker
no aaa new-model
ip cef
!
interface FastEthernet0/0
description R1 lan
 ip address 192.168.2.2 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface Serial0/3/0
 description link to R2
 ip address 192.168.2.97 255.255.255.224
 no fair-queue
 clock rate 125000
interface Serial0/3/1
 no ip address
 shutdown
```

```
 clock rate 125000
!
router rip
 version 2
 network 192.168.2.0
!
ip http server
snmp-server community public RO
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server host 192.168.2.1 snmpv2
control-plane
line con 0
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end
```

CISCO ROUTER 2 CONFIGURAION FILE

```
hostname R2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
interface FastEthernet0/0
 description R2 lan
 ip address 192.168.2.33 255.255.255.224
 duplex auto
 speed auto
!
interface Serial0/3/0
 ip address 192.168.2.98 255.255.255.224
!
interface Serial0/3/1
 no ip address
 shutdown
 clock rate 125000
!
router rip
 version 2
 network 192.168.2.32
```

```
 no auto-summary
!
ip http server
!
snmp-server community public RO
snmp-server enable traps snmp linkdown linkup coldstart warmstart
snmp-server host 192.168.2.1 snmpv2
!
control-plane
line con 0
line aux 0
line vty 0 4
 login
scheduler allocate 20000 1000
end
```