

A Step on Developing Network Monitoring Tools

Ahmed Kijazi

School of Information and Communication Science and Engineering, Nelson Mandela Institution of Science and Technology P.O. Box 447, Arusha, Tanzania

Tel:+255712307240 Email:kijazia@nm-aist.ac.tz,ahmed_kijazi@yahoo.com

Kisangiri Michael

School of Information and Communication Science and Engineering, Nelson Mandela Institution of Science and Technology P.O. Box 447, Arusha, Tanzania

Tel:+255788744023 Email:kisangiri.michael@nm-aist.ac.tz

Abstract:

Network Monitoring involves Using Software or hardware based Systems or a combination of both to constantly observe the status of network devices and hosts, and notifies the network administrator via email, SMS or other alarms in case of error or fail. Observing the status of network device and hosts is done when the Monitoring System speaks with the networking devices or hosts using different protocols within the protocols stack (OSI Layer) ,see Figure1.The aim of this paper is to provide a footstep on developing a network monitoring tool for monitoring network devices and hosts. This is a software based Network Monitoring tool using a combination of Simple network Monitoring Protocol (SNMP), Internet Control Message Protocol (ICMP) and Port scanning concept.

Key words: SNMP Manager, MIB, SNMP Agent, ICMP, Port Scanning, DNS, DHCP, SMTP, HTTP, Service;

1. Introduction

Network Monitoring is not only concerned with Monitoring of the physical network and host device such as routers, bridges, hubs and computers, but also concerned with monitoring of services which are running on some of these devices. These services they provide data storage, manipulation, presentation, communication services and they are running in the network Layer and above. In fact, this paper Monitor the application layers service not otherwise, which are Domain name service (DNS), Dynamic host control protocol (DHCP), Simple Message Transfer protocol (SMTP), Hypertext transfer protocol (HTTP). These application Layer services, they are running on most important Servers on the Computer network such as Web Servers, Mail Servers, IP addresses Servers and name resolution Servers. Monitoring of application service availability involves port scanning technique while monitoring of network device and hosts use SNMP and ICMP protocols concept respectively. SNMP is an industry standard management protocol that originated for TCP/IP networks. However, all these three concepts they are implemented Using Java in one software package which then form a network monitoring tool.

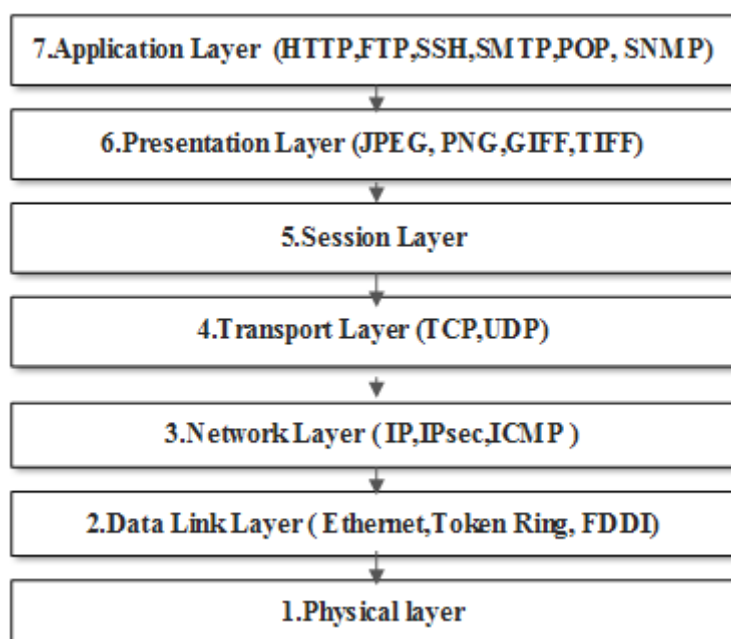


Figure1. A diagram for OSI 7 layers and services.

2. Methodology

Consider Figure 2. It is a monitored LAN which consists of three key elements:

- i. A managed device
- ii. Agent - software which runs on the Managed device.
- iii. Network management system (NMS) — software which runs on the manager

A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional access to node-specific information (read-write). Managed devices exchange node-specific information with the NMSs [8]. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers [8]. An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP specific form. A network management system (NMS) executes applications that monitor and control managed devices, in this paper we call that application as a network monitoring tool. NMS provides the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network [8].

The developed network monitoring tool (SNMP Manager) is installed in the Network Management Station (NMS). The System is used to Monitor Mail Server, Web Server, DNS Server, CISCO Switch 2960-S, Gateway device and internet connection as shown in the Figure 2. The monitoring process is performed by the SNMP Manager when sending and receiving packets via ICMP and SNMP to and from the network devices and hosts within the network, but also port scanning techniques for Server Services. The monitoring process is categorized into three parts as follows:

- i. Monitoring of device availability
These do not care about the services running on the devices, just monitoring their availability only. These apply to all devices in the network
- ii. Monitoring of Service availability
Monitoring of Services, are based on monitoring of availability of Services running on the Servers. These Services are the ones providing different functionalities in the network such as Mail, Address resolution and Web based functionalities. These services operate in the application Layer.
- iii. Monitoring of other parameters.
Other parameter are those apart from Services and device availability, these are Status of all ports of the switch, bandwidth allocated in all ports of the switch, tracking the location of all devices using location names, tracking the elapse time since the devices are up, determining the number of users configured in each server, Determining the amount of physical memory available in each Server, Reading the current operation temperature value from the switch, Checking the fan status from the switch and determining the OS version which running in all devices.

Figure (2), it's a sample network diagram where by network devices such as routers and switch and host devices such as Web, Mail and DNS servers are Monitored by the Network Management Station (NMS).

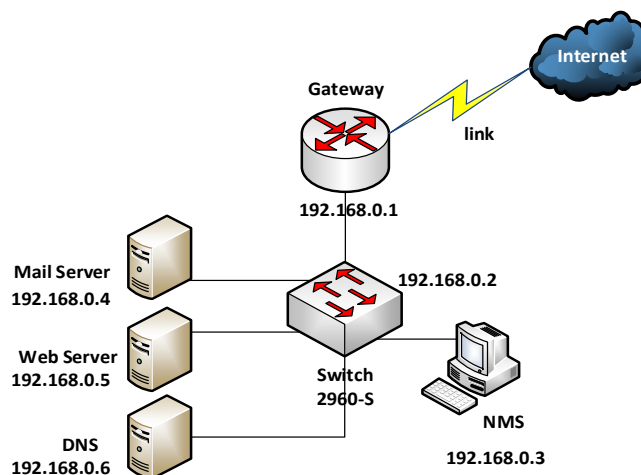


Figure 2. Monitored LAN

i. Monitoring of device availability

Monitoring of device availability is done, by using the ICMP protocol. A part of the network monitoring software is programmed in such a way it utilizes the ICMP ping packets to detect the availability of any devices in the network [5] [6]. The software periodically automatically detects the devices by sending the echo request to each device using IP address and then device respond with echo reply, see Figure 3. If the device echo reply indicates not reachable means the device is down and if an echo reply indicate reachable means the device is up [5] [6]. In order for the program to send the ICMP ping the programmer does not need to have deep knowledge about the ICMP packet structure. Fortunately, Java provides libraries for sending a ping packet to the devices using their IP addresses [5]. More examples are available in the internet.

Figure (3) present how the Network Management Station (NMS) sends ping packets to the network device and hosts [10]. Through this process NMS can detect the availability of both network device and hosts in the monitored network Figure (2).

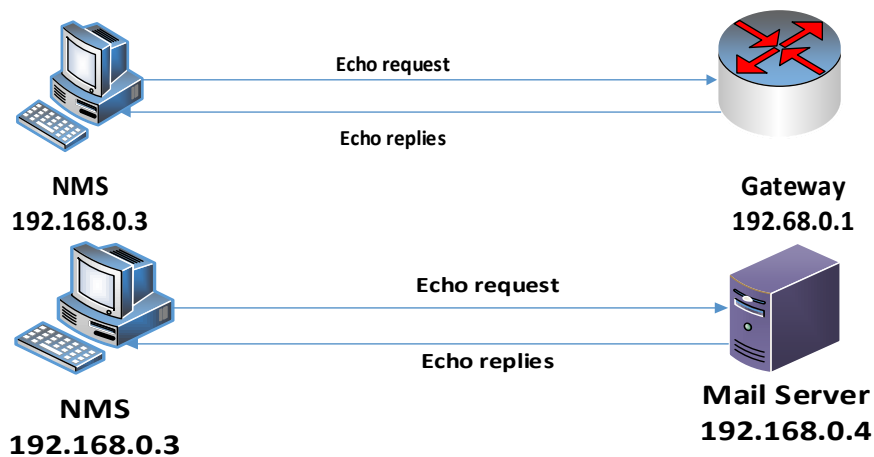
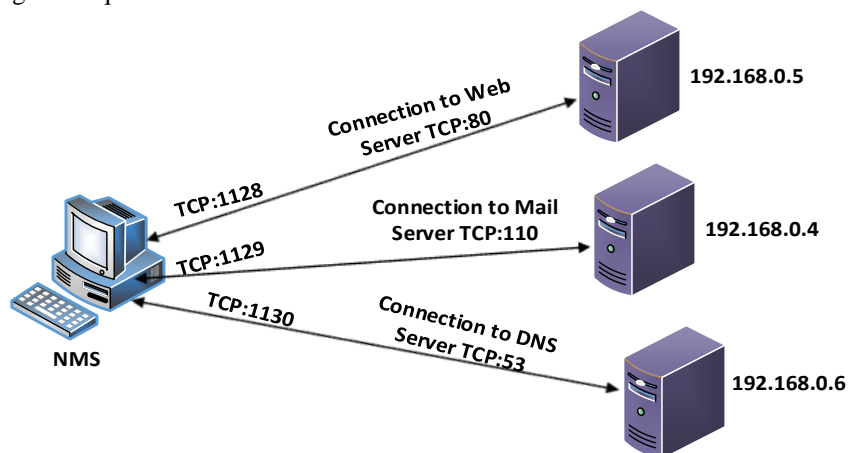


Figure 3. Echo request and replies from the devices

ii. Monitoring of Service availability.

Monitoring of Service availability is done by using port scanning technique. A service monitoring module in the SNMP Manage does port scanning by periodically establishing connection to the Servers using Socket programming, see Figure4 [7]. A socket comprises of IP address and a port number of the Services that SNMP Manager wishes to establish a connection with them. Socket class is available in the java.net.* package so this should be imported to the net beans IDE during programming. The socket should enclose within the try and catch block so that any disconnection will be caught while connection remains in the try block [3].

Figure (4), it is a network monitoring tool installed on the NMS detecting Web, Mail and DNS availability using TCP port scanning technique.



↔ Indicates TCP Connection.

Figure 4. NMS identifies Server application by establishing a TCP connection to their ports

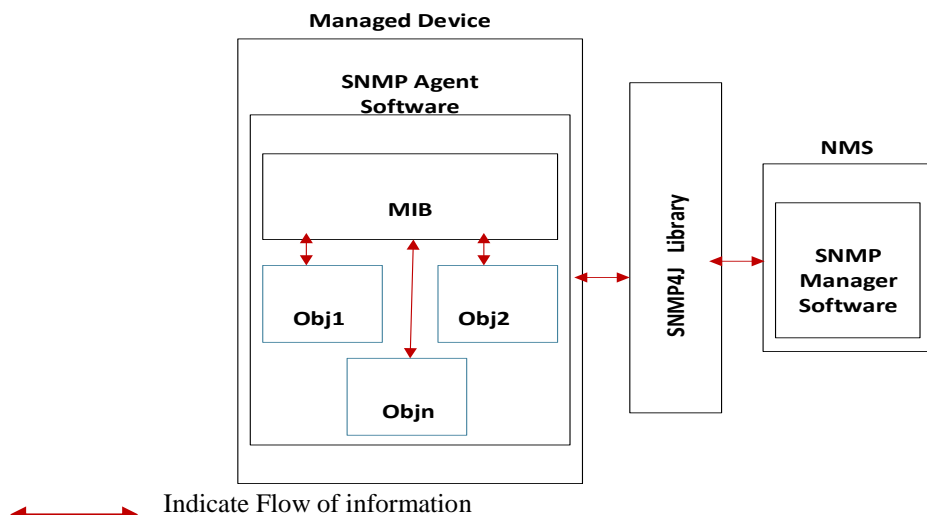
iii. Monitoring of other parameters.

Monitoring of other parameters is done using SNMP protocol. Simple Network Monitoring control protocol is an application Layer protocol operates in port number 161 by default. SNMP is disabled in the devices which

support SNMP capabilities, in order for this protocol to work it should be enabled, a programmer required to read the SNMP device manual before further development of software. In this paper Cisco switch 2960-S is used as an example to explain the concept [4]. Java does not know anything about SNMP, in order to program any SNMP Manager a software developer is required to download and import an SNMP library in the net beans. More SNMP libraries are available online, but in this paper SNMP4J libraries have been used. Any Software which Uses SNMP to manage the device, it is called an SNMP Manager. The management is done in cooperation with agents and MIBS. An SNMP manager refers to a system that runs a managing application or suite of applications. These applications depend on MIB objects for information that resides on the managed systems. Managers generate requests for this MIB information, and an SNMP agent on the managed system responds to these requests [4].

A request can either be the retrieval or modification of MIB information. By accessing the MIB objects, the SNMP agent allows configuration, performance, and problem management data to be managed by the SNMP manager. This is how the agent makes network and system information available to other systems [4]. SNMP agents reside on systems that are managed. The agent receives requests to either retrieve or change management information by referencing MIB objects. Management Information Base (MIB) objects are units of information that provide information about the system and the network to the managing system. MIB objects are referenced by the agent whenever a valid request from an SNMP manager is received [4].

Figure (5), SNMP Manager communicates with managed device using SNMP4J libraries.



Indicate Flow of information

Figure 5. SNMP Manager communicates with SNMP agent via SNMP4J Library

Fig (6), Express the Management information base (MIB) files organized in a tree structure. Each set of circles from the top indicates a particular configuration in a device.

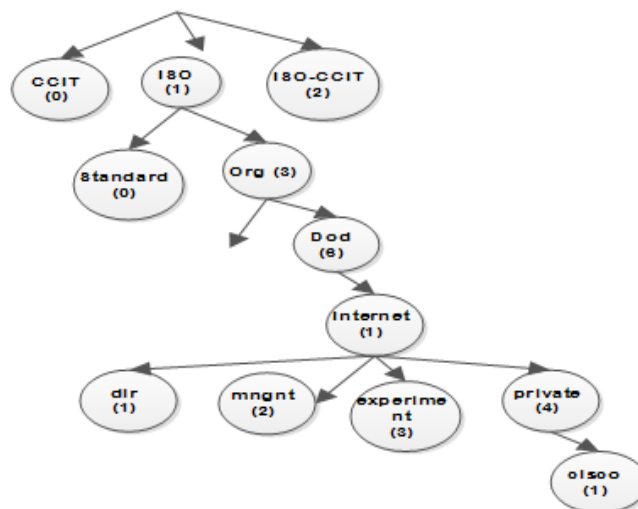


Figure 6. MIB configuration organization structure

MIB stores device configuration in the tree structure as shown in the Fig 6. Each series of this configuration indicates a certain configuration in the device. The all parts indicate the general configuration for all devices, but

start from the private circle indicates specific configurations from different companies. For example, any CISCO configuration start with OID number 1.3.6.1.4.1 see Fig6. The following are the OIDS of different configuration from different devices and the configuration information they indicated.

Table (1), explain the configuration numbers (OIDs) from the devices and their meaning

OID number	Configuration	Device
.1.3.6.1.2.1.2.2.1.8	Shows Switch port status	CISCO (2960-S)
.1.3.6.1.2.1.2.2.1.5	Switch ports bandwidth	CISCO (2960-S)
.1.3.6.1.2.1.1.6.0	Device, Location	Any
.1.3.6.1.2.1.1.3.0	Time elapse since the device is up	Any
.1.3.6.1.2.1.25.1.5.0	Current Number of Users in the System	Any
.1.3.6.1.2.1.25.2.2.0	Amount of Physical Memory	Any
.1.3.6.1.4.1.9.9.13.1.4.1.3	Fan status	CISCO (2960-S)
.1.3.6.1.4.1.9.9.13.1.3.1.3	Device Current working Temperature	CISCO (2960-S)
.1.3.6.1.2.1.1.1.0	OS Description	Any

Table1.OID numbers and respectively Managed configuration

3. Tools needed.

Normally it is very difficult to find the correct OID number in a given MIB configuration file because of their complex content organization. In order to find the correct OID number in the MIB configuration file you need to have MIB browser tools. Using the MIB browser software you can browse any MIB file in the device using device IP address and get the correct OID number with description. In this paper a free MIB browser called MIB browser engine is proposed [9] see Fig 7.

Figure (7), It is Manage engine free tool which is used to browse the device configuration files and extract OIDs and their meaning.

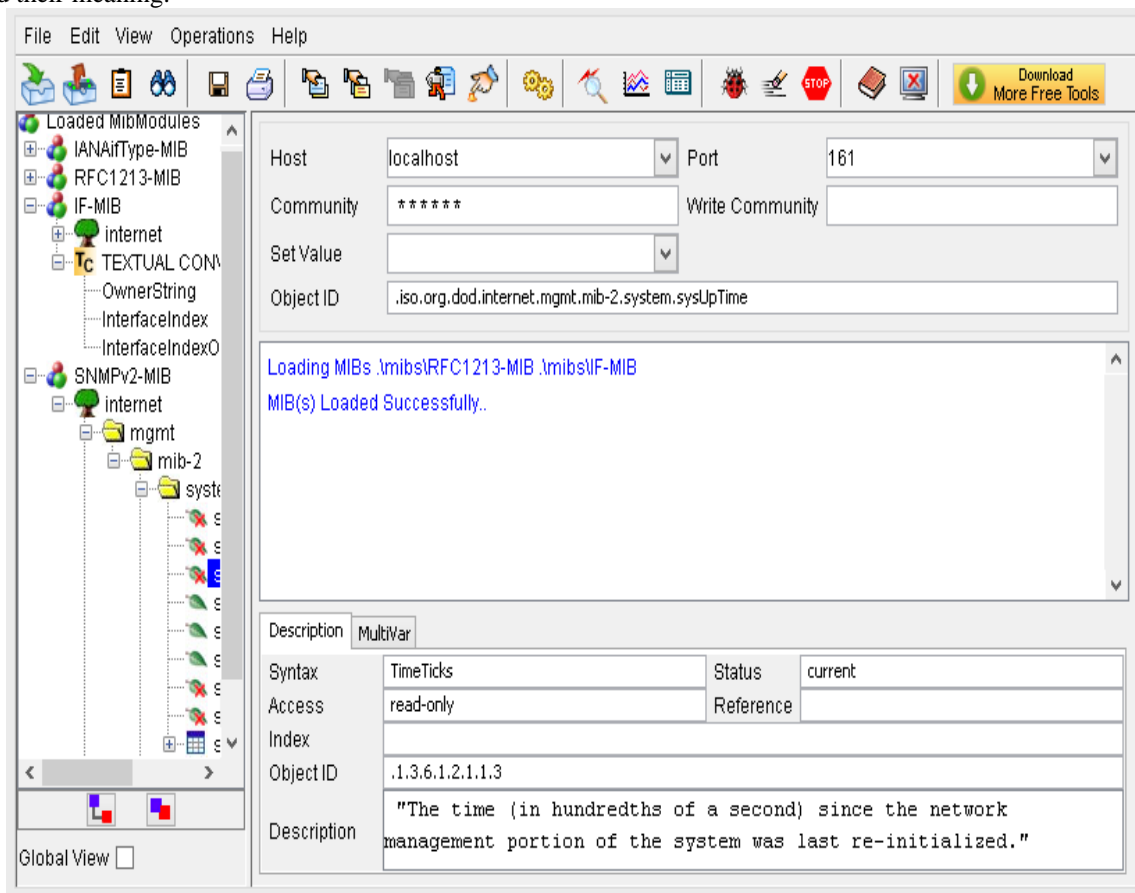


Figure 7. Manage Engine Free Tool

For doing coding a net bean IDE is required, but in order for your coding to communicate with SNMP enabled device SNMP library for Java must be imported in the net beans. These libraries are different classes and functions which enable Java to communicate with SNMP enabled devices with combination of device IP Address and SNMP port number which is 161 by default.

Figure (8), it is a graphical use interface of the netbean IDE, it is used for network programming using Java SE.

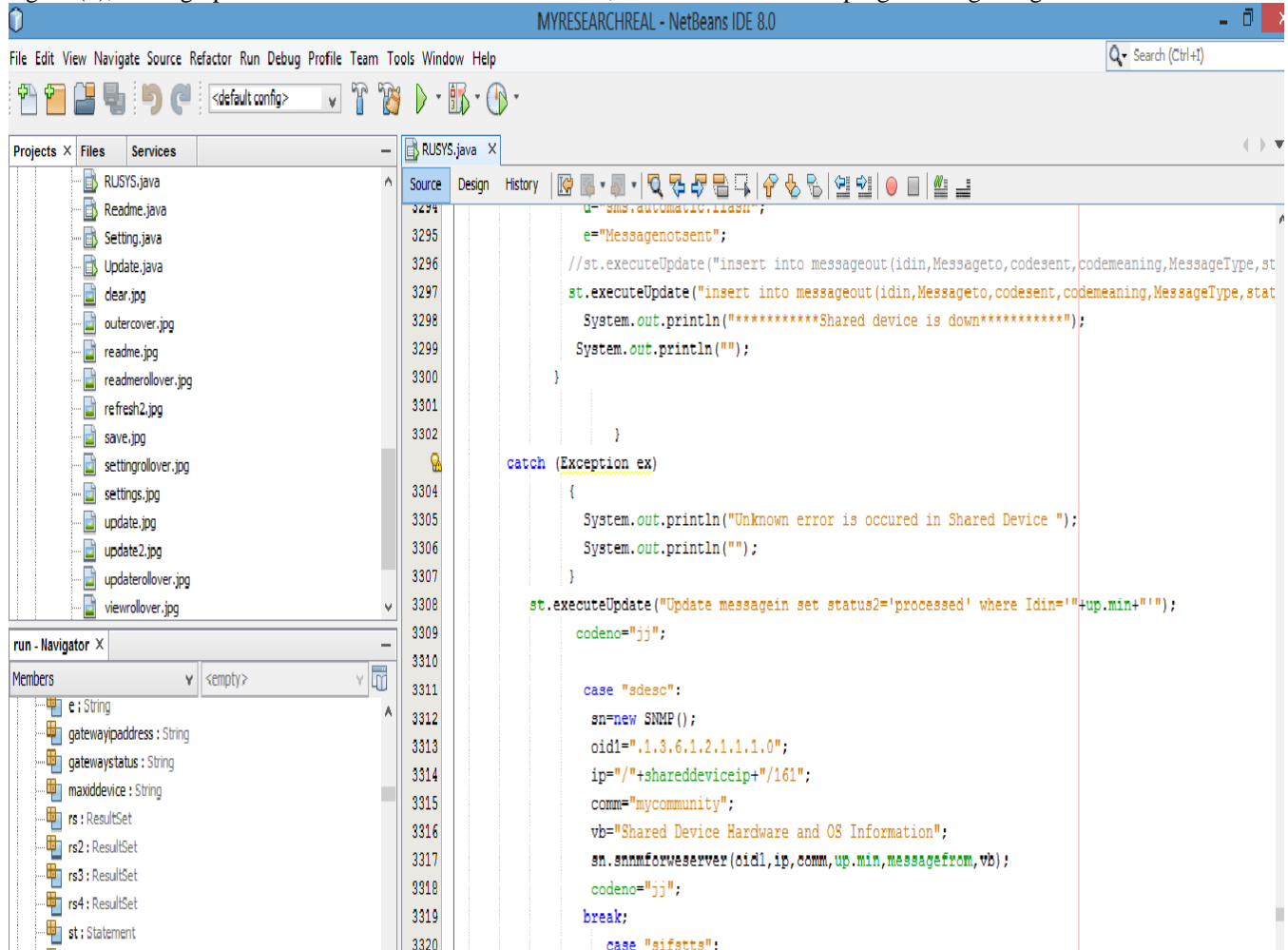
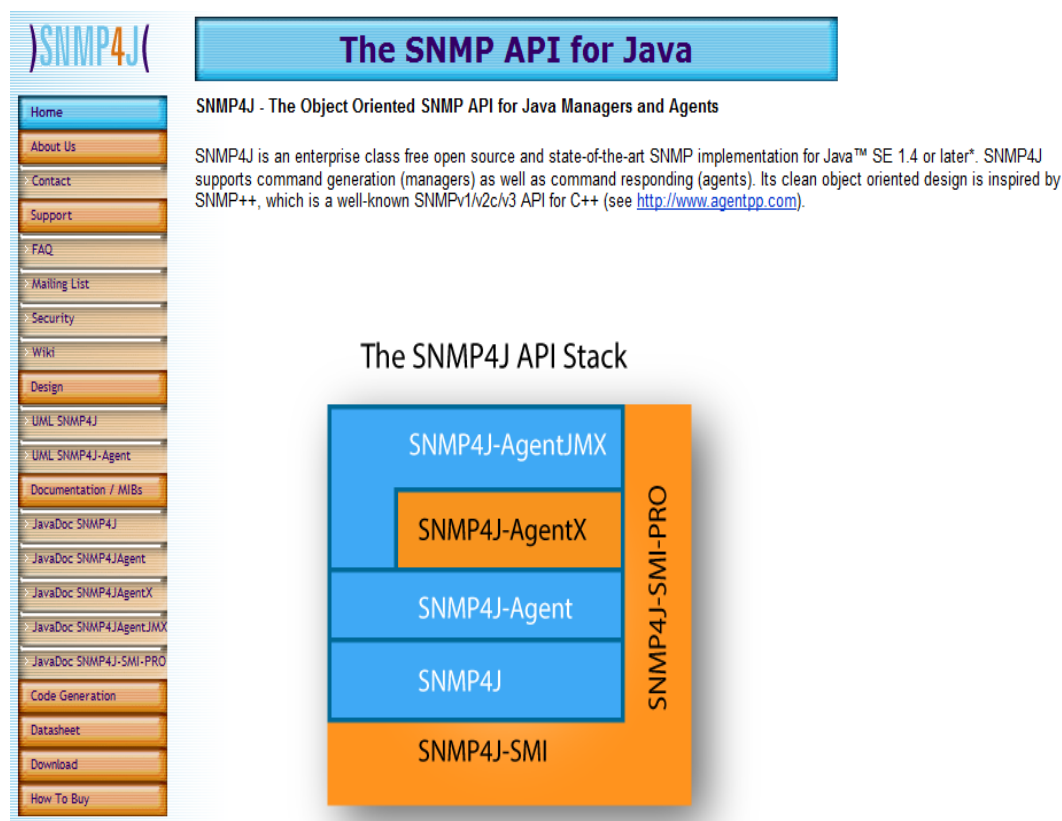


Figure 8. Net bean IDE

Figure (9) Graphical user interface of a website which you can download SNMP4J libraries. These libraries they enable Java based program to communicate with SNMP enabled devices using the SNMP protocol.

Figure 9. SNMP for Java Library



The screenshot shows the website for SNMP4J. The main heading is "The SNMP API for Java". Below it, the text reads: "SNMP4J - The Object Oriented SNMP API for Java Managers and Agents". A description follows: "SNMP4J is an enterprise class free open source and state-of-the-art SNMP implementation for Java™ SE 1.4 or later*. SNMP4J supports command generation (managers) as well as command responding (agents). Its clean object oriented design is inspired by SNMP++, which is a well-known SNMPv1/v2c/v3 API for C++ (see <http://www.agentpp.com>)." To the left is a navigation menu with items like Home, About Us, Contact, Support, FAQ, Mailing List, Security, Wiki, Design, UML SNMP4J, UML SNMP4J-Agent, Documentation / MIBs, JavaDoc SNMP4J, JavaDoc SNMP4J-Agent, JavaDoc SNMP4J-AgentX, JavaDoc SNMP4J-AgentJMX, JavaDoc SNMP4J-SMI-PRO, Code Generation, Datasheet, Download, and How To Buy. Below the website screenshot is a diagram titled "The SNMP4J API Stack". The stack consists of several layers: a bottom orange layer labeled "SNMP4J-SMI", followed by a blue layer "SNMP4J", another blue layer "SNMP4J-Agent", a blue layer "SNMP4J-AgentX", and a top blue layer "SNMP4J-AgentJMX". To the right of the stack is a vertical orange bar labeled "SNMP4J-SMI-PRO".

4. Conclusion.

This paper will provide a footstep on how to develop network monitoring tools for non expertise network programmer for Monitoring network as well as Hosts devices.

5. Reference:

- [1]. G. Ravi, M. Mohamed Surputhee, Dr. R. Srinivasan (2012). Securing Wireless Sensor Networks using Concealed Data Aggregation, Secret Sharing and Randomized Dispersive Routes. International Journal of Computational Intelligence and Information Security,1837-7823
- [2].SNMP, a protocol capable of managing any network device, which stands for Simple Network Management Protocol. www.rane.com/note161.html. (July 27,2014)
- [3]. David Reily and Michael Reily (2002) . Network programming and distributed computing. Addison Wesley Pub ISBN: 0-201-71037-4
- [4]. IBM .Simple Network Management Protocol (SNMP) Support version 4
- [5].Configuring for Network Management Applications by CISCO. www.cisco.com/.../application-networking.(July 27,2014).
- [6]. Ahsan Habib, Mohamed M. Hefeeda, and Bharat K. Bhargavav CERIAS. Detecting Service Violations and DOS Attacks.Department of Computer Sciences Purdue University, West Lafayette, IN 47907.
- [7]. Lanier Watkins, Cherita Corbett, Benjamin Salazar, and Kevin Fairbanks .Using Network Traffic to Remotely Identify the Type of Applications Executing on Mobile Devices.Johns Hopkins University Applied Physics Laboratory Laurel, MD USA
- [8]. M. Mohamed Surputheen1, G.Ravi2, Dr.R.Srinivasan(2012). Route Optimization using SNMP for Automatic Discovery of Network Topology.International Journal of Computational Intelligence and Information Security.1837-7823
- [9]. A free MIB browser tool. www.manageengine.com/products/mibbrowser-free-tool/(July 6,2014).
- [10]. Amir Sheikh, Rahul Hendawe, Rajnish Singh, Jayashree Shiral, Anmol Rohan. Remote Monitoring, Controlling and Lost Hardware Detecting through GSM (2012). International Journal of Advanced Research in Computer Engineering & Technology. 2278 – 1323

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
<http://www.iiste.org>

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: <http://www.iiste.org/journals/> All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: <http://www.iiste.org/book/>

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digital Library, NewJour, Google Scholar

