1.0 INTRODUCTION

A computer network consists of network elements like nodes, links, routers etc. The network administrator (manager) is the person who manages the network. Systems and network administrators require tools that are affordable to ease the management of computer networks. Managing the network means both monitoring and configuring the network. They also maintain and diagnose the network whenever they face problems in the network. Dividing the major task in the network management, network monitoring sees the key role. Network monitoring system plays significant role in the network management. A network monitoring system lets the administrator know how well the network is running during the course of ordinary operations. Network Monitoring is essential in an active network in order to diagnose problems and gather statistics for administration and fine tuning. A network management system provides various monitoring techniques including graphing, notification system and configuration management.

In the proposed system we introduce a session based strategy for the administrator of the network to be able to add or remove clients devices based on their ip address and be set time based frequency to update the statistics of the data usage. The administrator of the system logs in to the browser and a dashboard is presented with the graphical display of the data traffic and tabulated form of client information. The admin is able to do administrative tasks like adding a device, editing, deleting as a part of configuring etc. The proposed system tends to use SNMP v3 (Simple Network Management Protocol) for the monitoring of the client devices which are also called agents. The system also aims to provide configuration management service as well and is intended to provide benefits for small or medium sized organizations and institutions.

2.0 PROBLEM STATEMENT

System and Network administrators are responsible when something goes wrong on the network. They have no information of what may have caused a network failure. This is more so on computer networks that do not have any high grade network monitoring software installed. This scenario is common place in academic institutions because of

mentioned reasons. This was the main purpose for the study and project development. Monitoring data rate and traffic within an organization or an office is must when there is limited availability of various resources and more number of people. Inappropriate traffic can slow the network down or even bring it to a complete shutdown, causing frustration to legitimate users of the traffic.

3.0 OBJECTIVE

The following are the objectives of the network monitoring and configuration system:

- To find the best network monitoring solution from a system administration point of view
- To display the data usage statistics in form of graph for each client in the browser and to compare the data usage statistics between the nodes or client within a day so as to generate the certain session wise report
- To configure and manage client devices from remote and monitor TCP/UDP data traffic that is flowing through various interfaces of the client computer

4.0 SCOPE

The network monitoring system can be widely used in networks of organization where a number of computer systems are connected to each other. These organizations can be software development firms, universities and colleges etc. Also the system can be implemented to small organization or startups where the resources are limited as the enterprise level or advanced software are too much too afford.

5.0 LIMITATION

The network management system is a web application, desktop application is not available. For configuration management part the system highly relies on what type of operating system is the client device running. The network monitoring system is now considered for client devices (computer only), so devices other than mobile or computers like printer, scanner etc..are not yet supported. Skilled manpower is necessary to operate the system. The system will not be able to show information about the resources used in the client

computer like disk usage, RAM usage etc. That is, the system won't be able to perform resource monitoring activities. The proposed system also does not have alert system based on events. Also this system focus on LINUX based environment, so there is limitation on the OS like Windows.

6.0 Methodology

The proposed Network Monitoring System is a system that needs thorough study of the requirements and feasibility tests. The methodology that is going to be followed for the project development, documentation and testing process is going to be the Software Development Life Cycle.

6.1 Study of existing system

Some of the existing works to the proposed Network Monitoring Application are discussed in this part. For each of the system, short description of the system with their pros and cons are discussed in the following section:

6.1.1 Cacti

Cacti is a network monitoring system designed for drawing time-series graphs of performance data on a monitored network. It stores all of the necessary information to create graphs and populate them with data in MySQL database. Data to be graphed in Cacti is collected using SNMP (simple network management protocol) at a specified rate. This defaults to five minutes but with some effort can be reduced to shorter rate. The application draws each graph for a different graph for each monitored data source. A user management system tool is built in so that users can be added and given rights to certain areas of cacti. Cacti doesn't have event detection system or a notification system.

6.1.2 Wireshark

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. It can be thought of as measuring device used to examine what's going on inside a network cable. Wireshark can capture traffic from many different network media types - and despite it's

name - including wireless LAN as well. Which media types are supported depend on many things like the operating system in use. But to understand what's going on inside the network, manual deciphering is necessary. Wireshark will not manipulate things on the network, it will only measure things from it.

6.2 Requirement Identification

6.2.1 Client machine

The client machine can be Windows or Linux based operating system. The client machine should have SNMP-Agent application installed. For LINUX based client devices, net-snmp package installed which is an agent for the application running on the server and similarly in snmp-agent service enabled in the windows operating system. The client machine also should have static ip assigned. Also the client side device will have SSH installed for configuration management.

6.2.2 Server machine

The server machine should have Ruby and Rails installed with a MySQL database server. Works best when operated in Linux based server with minimum of 1GB Random Access Memory and 40GB a Bytes of Hard Disk and processor of Pentium Dual Core or above. Ubuntu 16.04 Xenial Xerus LTS can be used as a server for the application Ruby (latest version) and Rails 5.0.2 is required for the application with Puma Web server is required(default with Rails).Latest MySQL server compatible with Rails application is essential.

6.3 Feasibility Study

6.3.1 Technical

At present it is assumed that the server is configured with LINUX system. Since the server is easily met with server requirements, the system can be assumed that it is technically feasible. The basic requirements of the server are as Rails, MySQL, SSH, Ansible. These all tools are freely available and can be set up easily.

6.3.2 Operational

The proposed system will have constantly operating the system such that it can monitor the data continuously and provide the graph on the certain interval. All the client devices will be automatically connected to the server as they will be assigned static IP. Also this device will be configured via the SSH protocol. The admin will also have certain login system such that unauthorized access will be prevented hence increasing security measure.

6.3.3 Economical

As this system is tended to small organization and startup, the cost limitation factor are essentially considered both within the prospect of the business and developer. Also with the help of little or intermediate knowledge by the non-system admin can also be handled throughout the entire process. Even though if people needs to get trained, the well documented report or manual will provide detail basis to immediately start on hands.

6.3 Tools

6.3.1 Front-End

As the network monitoring system is a web-based application, the front-end of the application is going to implemented using HTML, CSS and JavaScript.

6.3.2 Back-End

The server side programming language of the application is Ruby and the framework we are going to use is Ruby on Rails framework. Ruby is an object oriented programming language which believes in making programmers happy. The Ruby programming language is rich in various libraries that can be used within the application.

6.3.3 Editor

Any editor supporting Rails framework can be used. Mainly we will be using Emacs and Atom throughout the process.

7.0 Design of Proposed System

7.1 Use-CASE diagram

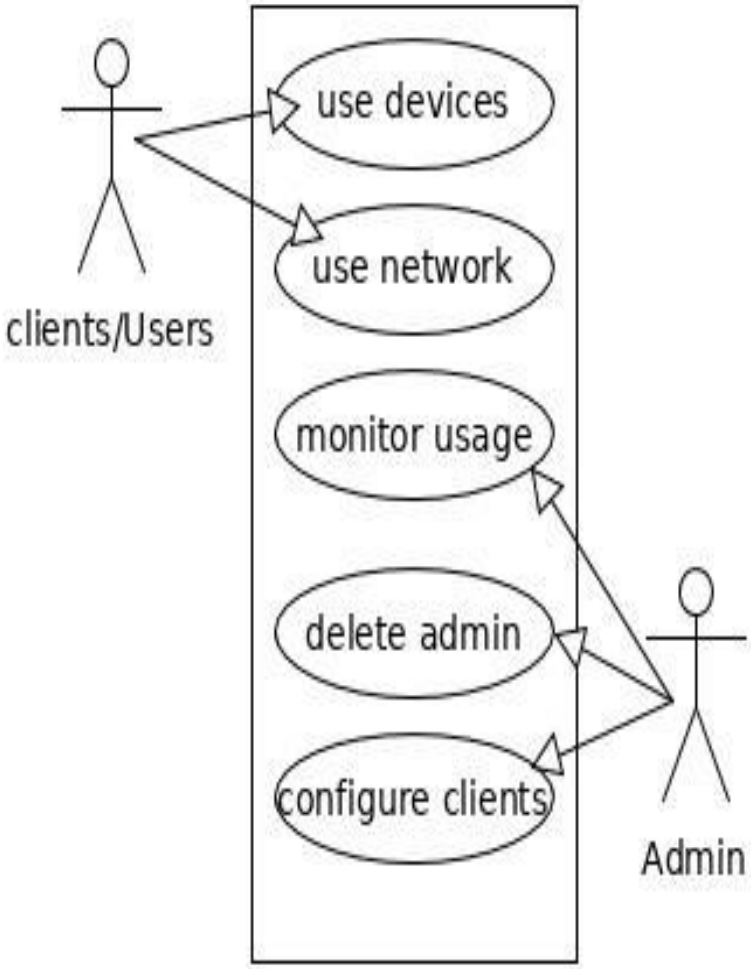

Fig 1: Use Case diagram

7.2 System Activity Diagram

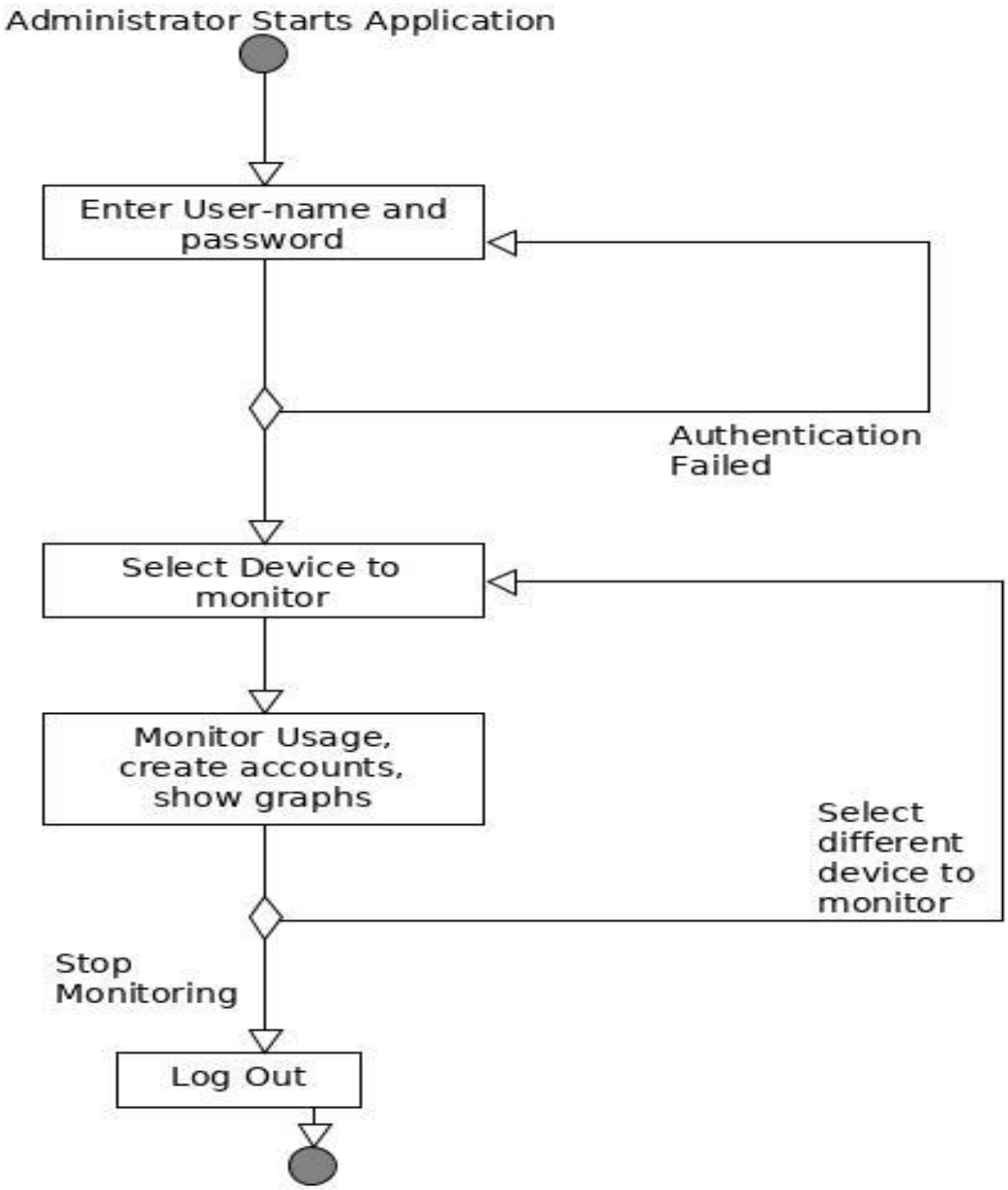

Figure 2: Activity Diagram of the proposed system

8.0 Gantt chart

Table 1: Gantt chart for proposed system timeline

Work/Week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
System Analysis and Design																	
Coding and Database																	
Testing																	
Documentation																	

9.0 Expected System

The proposed system is a network monitoring system based on SNMP protocol. So, the expected system is a well-developed, user friendly web application with all the pre-mentioned features available. The system should be able take in the data usage statistics provided from the SNMP-Agents of the client computers or devices and present those appropriately to the admin dashboard. The proposed system should be able to work concurrently even if large number of devices are connected to the network.