SNMP Based Network Monitoring System Supporting Real-Time Visualization Of Network

A Thesis Submitted By

Sweta A Dargad

12MCEI37

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2014

SNMP Based Network Monitoring System Supporting Real-Time Visualization Of Network

A Major Project

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology in Computer Science and Engineering

(Information and Network Security)

Prepared By

Sweta A Dargad

(12MCEI37)

Guided By

Dr. Sanjay Garg

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INSTITUTE OF TECHNOLOGY

NIRMA UNIVERSITY

AHMEDABAD-382481

May 2014

Certificate

This is to certify that the Major Project Report entitled "**SNMP Based Network Monitoring System Supporting Real Time Visualization Of Network"** submitted by **Sweta A. Dargad (Roll No: 12MCEI37)**, towards the partial fulfillment of the requirements for the degree of Master of Technology in Computer Science and Engineering(INS) of Nirma University, Ahmedabad is the record of work carried out by her under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Dr. A.V. Ravi Kumar
Scientist SF,
Head (Computer Centre),
External Guide,
Institute for Plasma Research,
Gandhinagar.

Prof. Sharada Valiveti
Associate Professor
Coordinator M.Tech - CSE(INS)
CSE Department,
Institute of Technology,
Nirma University, Ahmedabad.

Dr. Sanjay Garg
Professor and Guide,
Head(CSE Department),
Institute of Technology,
Nirma University, Ahmedabad.

Dr K Kotecha
Director,
Institute of Technology,
Nirma University, Ahmedabad

Undertaking for Originality of the Work

I, **Sweta A. Dargad**, Roll. No. **12MCEI37**, give undertaking that the Major Project entitled "**SNMP Based Network Monitoring System Supporting Real-Time Visualization Of Network** " submitted by me, towards the partial fulfillment of the requirements for the degree of Master of Technology in **Computer Science & Engineering (INS)** of Nirma University, Ahmedabad, is the original work carried out by me and I give assurance that no attempt of plagiarism has been made. I understand that in the event of any similarity found subsequently with any published work or any dissertation work elsewhere; it will result in severe disciplinary action.

Signature of Student

Date:

Place:

Endorsed by

Dr. Sanjay Garg

(Signature of Guide)

Acknowledgments

I would like to express special appreciation and thanks to my guide **Dr. Sanjay Garg**, Hon'ble Head of Computer Science and Engineering Department, Institute of Technology, Nirma University, Ahmedabad for being a tremendous mentor for me. The valuable guidance and suggestions he gave throughout this work has been a great support for me. His guidance has triggered and nourished my intellectual maturity.

It would like to thank **Dr. A.V. Ravi**, Hon'ble Head of Computer Center, Institute for Plasma Research, Ahmedabad for his kind support and providing basic infrastructure and healthy research environment. The appreciation and continual support he has imparted would be a great motivation to me in reaching a higher goal

My deepest thank is extended to **Prof. Sharada Valiveti**, PG CSE(INS) - Coordinator, Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad for an exceptional support and continual encouragement throughout the Major Project. She has been a great Mentor and has always given moral support in my ups and downs.

A special thank is expressed to **Dr K Kotecha**, Hon'ble Director, Institute of Technology, Nirma University, Ahmedabad for the unmentionable motivation he has extended throughout course of this work.

I would also thank the Institution, all faculty members of Computer Engineering Department, Nirma University, and Ahmedabad for their special attention and suggestions towards the project work.

The blessings of God and my parents Mr. ArunKumar Dargad and Mrs. Neeta Dargad and my younger brother Meet who have always given strength to me in achieving each and every goal. I am very greatful to my friends who have supported me always.

- Sweta A Dargad

12MCEI37

Abstract

SNMP is the widely used network Monitoring Protocol. Being a defacto standard with its data collection and serving methods, collating with Round Robin Database helps "Network Monitoring System is capable to graph populated information like bandwidth, traffic, memory utilization and CPU utilization of network devices". Routers, Switches, Servers and Workstations are the basic components of a network. SNMP based Network monitoring system intends to get snapshots of resource utilization such as link utilization, traffic class utilization on these network devices. When conducting network testing the statistics so obtained helps in visualization of network. Our interactive Network Monitoring System also real-time status of critical switches. Being extensive for Network Administrator it has modules like Network Map, Graphing, Statistics and Alarms.The system is build on an application framework designed to built an extensive Web Application for Network Administrator's use. Instead of passing commands from his desktop or doing SSH, he can monitor his network ubiquitously using the Web-application built on the framework designed. He can get information about devices which are critical in real-time so as to take necessary steps aforetime.

The user of Network Monitoring system gets an appropriate user interface through which selections of what to monitor can be made on-demand, and real-time traffic graphs can be displayed automatically. With discovery of hosts in the subnets and alerts of critical machine or application going down through email and SMS. This thesis describes how to design such a SNMP based Network monitoring systems, supporting real-time visualization of network with the graphing of network metrices. All these just using low cost tools in the framework along with Net-SNMP and RRD .

Contents

Certificate iii

Undertaking iv

Acknowledgments v

Abstract vi

List of Tables x

List of Figures xii

1 Introduction 1
- 1.1 General . . . 1
- 1.2 Motivation . . . 2
- 1.3 Objective . . . 3
- 1.4 Scope Of The Work . . . 3
- 1.5 Fundamentals of Network Monitoring . . . 4
  - 1.5.1 Network Connectivity . . . 4
  - 1.5.2 Packet Loss . . . 5
  - 1.5.3 Traffic . . . 5
  - 1.5.4 Network Bandwidth . . . 5
- 1.6 Organization Of Thesis . . . 5

2 Literature Survey 7
- 2.1 Related Work . . . 7
  - 2.1.1 RFC 3411 . . . 7
  - 2.1.2 RFC 1155 . . . 8
  - 2.1.3 Designing SNMP Based Monitoring Systems . . . 8
  - 2.1.4 Design and Implementation of Server Monitoring System Based on SNMP . . . 9
  - 2.1.5 SNMP and Beyond . . . 10
  - 2.1.6 Web-Based Automatic Network Discovery / Map Systems . . . 11
  - 2.1.7 SNMP Network Management . . . 11
  - 2.1.8 Essential SNMP . . . 11
  - 2.1.9 SNMP,SNMPv2,SNMPv3 and RMON 1 and 2 . . . 12
- 2.2 SNMP . . . 13
  - 2.2.1 Components Of SNMP Based Monitoring . . . 14
  - 2.2.2 SNMP MIB Tree . . . 16

2.2.3 Net-SNMP Commands . . . 16
2.3 Round Robin Database . . . 17
2.3.1 Handling of Data in RRD . . . 18
2.4 Conclusion . . . 19

3 The Proposed Approach And Tools Used 20
3.1 Steps to Network Monitoring . . . 20
3.1.1 Visualize The Network . . . 21
3.1.2 Alerting And Logging . . . 22
3.1.3 Collecting Historic Information . . . 23
3.1.4 Threshold Monitoring . . . 23
3.1.5 Graphing in Real-Time . . . 24
3.2 Selection Of Tools To Develop Such A SNMP Based Network Monitoring System . . . 25
3.2.1 Overview . . . 25
3.2.2 PHP . . . 25
3.2.3 Net-SNMP v5.7.2 . . . 26
3.2.4 HTTP Server . . . 27
3.2.5 JavaScript Programming . . . 27
3.2.6 Perl Programming Language and graphing libraries . . . 27
3.2.7 RRDTool 1.x . . . 27
3.2.8 PHP-Weathermap v0.97c . . . 28
3.2.9 PHP-Server Monitor v1.0 . . . 28

4 Design and Implementation 29
4.1 Three Level Layered Design . . . 29
4.1.1 Layer 3 . . . 29
4.1.2 Layer 2 . . . 35
4.1.3 Layer 1 . . . 36
4.2 The Methodology To Implement RRD Tool . . . 37
4.2.1 Initialize The Database . . . 38
4.2.2 Collect The Data Sets Over Time . . . 40
4.2.3 Create The Graphs . . . 40

5 SNMS- SNMP based Network Monitoring System 41
5.1 User Registration . . . 41
5.2 Dashboard . . . 42
5.3 Network-Map . . . 43
5.4 Ghraphing . . . 44
5.5 Statistics . . . 44
5.6 Alarming . . . 45

6 Results and Discussions 48
6.1 Results . . . 48
6.1.1 Networkmap . . . 48
6.1.2 Graphing . . . 50
6.1.3 Statistics . . . 52
6.1.4 Alarming . . . 53
6.1.5 Case Study: Denial of Service Attack . . . 53

7 Conclusion **56**
7.1 Issues Resolved 56
7.2 Conclusion 57
7.3 Limitations 57
7.4 Future Scope 58

A SNMP Man Page **59**

B RRD- Round Robin Database **62**

List of Tables

2.1 ifInterface Mib Table 12
2.2 RFC's defining SNMP Versions 14

4.1 Server Statistcs And Related Oids 34

List of Figures

1.1 Network devices and performance metrics 4

2.1 Comparison of various Network monitoring tools 13
2.2 Components of SNMP 15
2.3 Mib Tree 17
2.4 Basic SNMP commands 18
2.5 Life of data in Round Robin Database 18
2.6 RRD's mechanism to plot Data Points 19

4.1 Three Level design model for Network Monitoring Sytem 30
4.2 An example of the Networkmap 32
4.3 An example of the In/Out Traffic of a link 33
4.4 Interface information in a tabular format 35
4.5 PDU format of SNMP Messages 38
4.6 Example of Initializing database 38

5.1 Level0 UseCase of NMS 41
5.2 Data Dictionary for Users Table 42
5.3 Status Of Critical Devices 43
5.4 Level1 UseCase Of NMS 43
5.5 User Level Diagram of Graphing Module 45
5.6 User Level Diagram of statistics Module 46
5.7 Data Dictionary for Logs 47
5.8 User Level Diagram of Alarming Module 47

6.1 Map of Exterior Network 49
6.2 Map of switch Network at NC1cc 50
6.3 graph of the IN/Out traffic between Hostel1 and Guest House 50
6.4 CPU and RAM Usage Bar graph 51
6.5 Memory Utilization Of The Server Last Day 51
6.6 Memory Utilization Of The Server Last Month 52
6.7 Memory Utilization Of The Server Last Year 52
6.8 Interface Configuration Information 52
6.9 Logs Generated 53
6.10 Graph showing Ping Latency of a Switch 54
6.11 Graph Showing Ping Latency Of SwitchB 54
6.12 Graph Showing In/Out Traffic Of Switch A At Interafce1 55
6.13 Graph Showing In/Out Traffic Of Switch A At Interafce3 55

7.1 Issues Resolved 56

B.1 RRD's data structure 63
B.2 Types of Consolidation Functions (CF) 65

Chapter 1

Introduction

1.1 General

As technology has advanced and computers have become less expensive, the networking infrastructure has grown alot. Network Administrator of any organization would want to have acute information of the network and wish to identify bottlenecks as well. He is the person responsible to manage and monitor the network, for which he requires a complete Network Monitoring System. "Network Monitoring System[4] is a combination system of hardware and software, functioning as monitoring and administering tools for heterogeneous networks". "The term Network Monitoring describes the use of a system that can constantly monitor network for slow or failing components and also notify the network administrator in case of problems". "Simple Network Management Protocol (SNMP)[1] is commonly available on all network devices". A network manageged by SNMP is made of management station which can be thought of a server and critical network devices.

A well-monitored network give Organizational Managers, the proactive infrastructure and reduces the work of a Network Administrator. SNMP stores information in the form of MIBs. The "get command collects statistics", " set command changes the values of variables stored within the device" and "trap command reports on unusual events that occur on the SNMP device". This information so received is in the raw form, ie. GAUGE [2], COUNTERS[2] or some values in a text format.

New techniques and solutions are found to represent these information in a meaningful

format so that an administrator can keep a track of data as well as archive it. For this the information can be stored in graphical form and viewed in real time. Network Administrator can easily use a Web based GUI to monitor his whole network ubiquitously. This thesis explains a framework to represent hence received information in graphical and statistical form. Also the framework helps to develop a standard tool SNMS (SNMP based Network Monitoring System) which can graph, alert, show statistics, map network and show real time up-link and down-link status.

1.2 Motivation

"SNMP provides a means to analyze the network device logs and provide statistics". SNMP is very popular Network Management Protocol because of its simplicity and scalability. SNMP is widely used formonitoring specific device[3]. A network consist of network infrastructure devices like routers, switches, servers and workstations. SNMP is integrated into most of these devices. SNMP helps in extending visibility of network by providing data collection services. This is very usefull to network administrator. SNMP can be used to monitor the state of hardware and software.

RRD Tool[14] handles time-series data. It can be usefull to monitor metrices like bandwidth, memory usage, CPU load, etc. The data is stored say in a round-robin database (circular buffer), so that the system storage footprint should be remaining constant over time. Scripts can be written to extract RRD[22] data in a graphical format in many languages like , PHP, Tcl, Perl, Python and Java languages. It requires just to run a cron job to update the database at the intervals specified when creating RRD archives. Using rrdtool graphing utility, graphs filled with real-time data(ofcourse with delay of interval time) can be generated. These graphs can be stored in PNG format and easily viewed on the web browser.

Although good tool like RRD Tool to store time series data and SNMP like protocol is available, there is no proper Network Monitoring System which is open source and easy to use.

1.3 Objective

The objective of this research is to provide a standard framework to use open source and easily avaialble tools and build a Network Monitoring System in Linux like environment and easy-to-use front-end for the same.
Also it needs to fulfill following objectives

- It is simple to implement with database in RRD Tool and storage of other required fields in MySql.
- It is flexible
  - Show Network Map which shows targeted graphs to each device
  - Allows a variety of network devices, Interfaces, Operating sytem to be queried.
  - Provides Ping, and target to measure bandwidth, cpu, web statistics, memory, disk, ups etc.
- Provides a web-based, menu driven presentations of network metrices graphically.
- Discover SNMP attributes about each target.
- Alerts via E-mail or Syslog upon a failure of an added device or service.
- Creates daily, weekly, monthly and yearly graphs. .
- Show Up-link and Down-link status of critical switches and routers.
- Show hosts alive in a subnet along with summary of their statistics.

1.4 Scope Of The Work

To achieve the objective of developing a network monitoring system which employs a protocol like SNMP. The data is collected by querying the network devices from time to time. The information is stored and viewed in graphical format as well as text format.This whole process provides in real time visualization of the network statistics. It must monitor Real-time uplink and downlink status and device health and status. Plotting the graphs for disk and memory usage. Alerting the Network Administrator in case of any high usage of disk or memory. The approach considers designing a Web based

GUI by querying the network devices from time to time.

1.5 Fundamentals of Network Monitoring

"A network monitoring system records values of network performance metrics and measure bandwidth, ping statistics, interface related information and system uptime, CPU load, memory usage, disk statistics etc" . These monitoring capabilities are critical to computer networks, Also because their effectiveness determines that the network is working properly and without any outrages. Important performance metrics that can are monitored include Network Connectivity, Traffic, Packet Loss rate, and Available Bandwidth.

Network performance metrics [4] can be measured at for network devices like CPU, router, switches, servers.

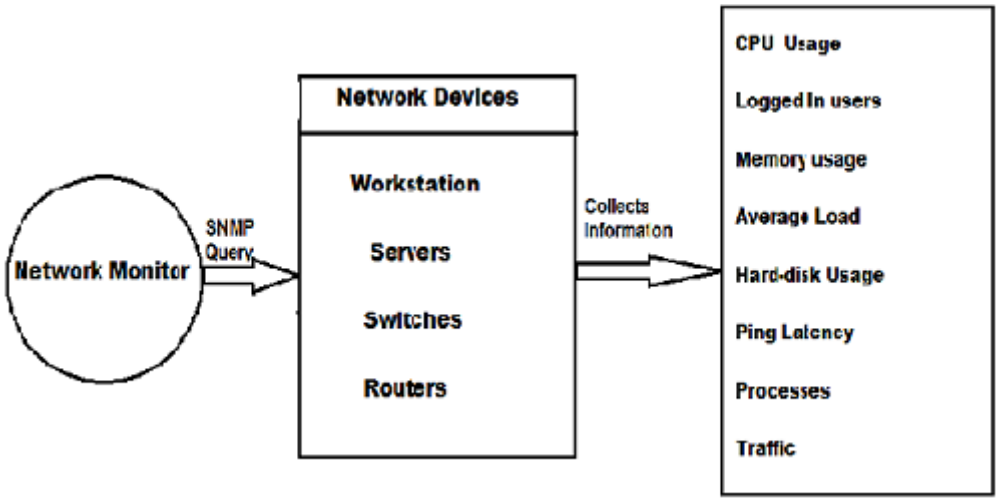


Figure 1.1: Network devices and performance metrics

1.5.1 Network Connectivity

When trying to monitor the network, Network connectivity has been very important metric. All network layers, provide mechanisms to automatically monitor network connectivity because network service has to guarantee that any pair of end nodes can communicate with each other.

1.5.2 Packet Loss

Packet loss should be less when we talk about network as well as network monitoring, refers to the probability that a packet gets dropped while being in the network. we can monitor paket loss using SNMP packet statistics at router interfaces.

1.5.3 Traffic

Traffic monitoring on an device is very important metric because if the traffic flow is not normal or suddenly there is an increase in traffic can be due to a trail to Denial of Service attack. Monitoring traffic can ensure an Administrator to proactively know about any such case.

1.5.4 Network Bandwidth

Network bandwidth is also the most widely used performance metric in today's network devices. It monitors mainly at the end-to-end level using SNMP. Network bandwidth can be used to directly evaluate network path performance, for small data transmissions to larger one.

1.6 Organization Of Thesis

Chapter 1 Introduction of the SNMP and why and how the research is useful. It explains the objective and scope of the research.

Chapter 2 Presents a literature survey of previous work to date in the domains of Network monitoring and use of SNMP to monitor Network devices and how the graphs will show meaningfull data in realtime that is relevant to the work presented in the remainder of the thesis. Also we talk about RFC related to SNMP. Related works on SNMP based monitoring. Also Chapter presents an overview on What is RRD.How is it different from another linear databases. How Round Robin Database is stores raw data and what are functions of RRD.

Chapter 3. The proposed approach and Tools used are explained in this chapter. We discuss the steps to network Monitoring and how and why Network Monitoring is so important. We see how selection of the low cost tools can help design a framework for

Monitoring.
Chapter 4. Describes the design and methodology used in implementing each component of the framework. We design a framework for Monitoring the Network with SNMP and Low Cost Tools. We also discuss about Methodology to implement RRD Tool.

Chapter 5. Description of SNMS - (SNMP Based Network Monitoring System) which is made using the framework is given in this chapter. We discuss our framework and each of its module and implementation and working with respect to SNMS.

Chapter 6. Discussing the experimental results and the conclusions derived from the work along with the graphs is done here. How and why our framework fits properly can clearly be seen here in this chapter.

The thesis ends with Chapter 7. The conclusions derived from the work and explores some future enhancements that can be made to the system is discussed. Also what are the limitation to this project and issues resolved.

At last we have two appendices, Appendix A presents the SNMP MAN page[26] requires to use SNMP commands from command line. Appendix B presents more on RRD Tool[22], about its functions and command.

Chapter 2

Literature Survey

2.1 Related Work

The area of Network Monitoring has remained a great concern for Network Admins and the researchers who want to make NA's life a little bit easier by providing different solutions. Bunch of researches are made on how SNMP came into existence and what are the benefits of the protocol. Some researches shows how SNMP can be used to monitor the network and some want to monitor only the servers using SNMP. While some research focus on centralized monitoring is preferable or distributed.

2.1.1 RFC 3411

D. Harrington, R. Presuhn, B. Wijnen. "RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks" [1]. The discription of architecture for Simple Network Management Protocol (SNMP) Management Frameworks is presented in it. This architecture which is shown to be as a framework is designed to be modular so as to allow the evolution of the SNMP protocol standards and that too over time. The author desrcibes that the major prtion of the architecture are an SNMP engine which is containing a Message Processing Subsystem, an Access Control Subsystem anda Security Subsystem. It says that possibly there are many SNMP applications which may be avialable to support specific functional processing of management data.

2.1.2 RFC 1155

M. Rose, K. McCloghrie. "RFC 1155: Structure and Identification of Management Information for TCP/IP-based Internets" [2], This is a memo which has a description on the common structures and identification scheme. The definition of management information used in managing TCP/IP-based Internet is shown in this paper. The most important information from this document was about defined data-types which included Network Address, Ip Address, Counter, Gauge, Timeticks , Opague, Encoding. The valuable information on passing the snmpget request is in the form of above defined data-types. To know and understand about how these data-types can be converted to get a meaningful information is in this document

Network Address : represents an address from several protocol families which are available. Currently, only one protocol family which is the Internet family is said by this paper.

"Ip Address : 32-bit internet address is Ip Address". OCTET STRING of length 4 represent IP Address, in network byte-order.

"Counter: This application-wide type represents a non-negative integer which monotonically increases until it reaches a maximum value, when it wraps around and starts increasing again from zero". It specifies a maximum value of $2^{32}-1$ (4294967295 decimal) for counters.

"Gauge : This application-wide type represents a non-negative integer, which may increase or decrease, but which latches at a maximum value". This memo specifies a maximum value of $2^{32}-1$ (4294967295 decimal) for gauges.

"TimeTicks : This application-wide type represents a non-negative integer which counts the time in hundredths of a second since some epoch, the description of the object type identifies the reference epoch".

2.1.3 Designing SNMP Based Monitoring Systems

Ranganai Chaparadza [3], "Designing SNMP Based Monitoring Systems presents a noble method which is designing SNMP based monitoring systems supporting ubiquitous access and real-time visualization of traffic flow in the network,using low cost tools". This paper says that SNMP is the protocol which is widely used for device specific monitoring.It has

brought a concept of real-time data collection using SNMP . It also mentions that this capability is way beyond the traditional network management and trends gathering for capacity planning.

It says the user of SNMP based monitoring system most of the time intends to make a selection of variables to be read an MIB for an interval. During this time monitoring is required. Only to have a snapshot of resource utilization metric such as cpu utilization,memory usage or traffic. This is surely done only on selected target critical routers or switches when conducting network testing it is very helpfull indeed.
This kind of monitoring system, which is interactive is always what is asked for.Such a system can provide the to start and stop monitoring facilty all the time. A User interface which is appropriate to have such selections of what to monitor if made on-demand is preferable. If it also display traffic graphs can be which are real-time and automatic will be cherry on the cake. In this paper the above goal is achieved by implementation of a tool called SVM(SNMP-based Visualization Monitor)

2.1.4 Design and Implementation of Server Monitoring System Based on SNMP

Zeng, Wenxian Wang, Yue, [4], in their paper "Design and Implementation of Server Monitoring System Based on SNMP introduce how to monitor servers using a popular protocol like SNMP".They expanded mib sources of server and used multi-threading technique to collect the data and process it.This way they also improved collection efficiency. They used net-snmp to gather information from mibs and "winsnmp" and threading to integrate monitoring and control of servers
By a network management protocol "SNMP", they have made the link between Management Station and agents that reside on the network device. It has included which five SNMP messages: GetRequest, GetNextRequest, SetRequest, GetResponse and trap. Messages like GetRequest, GetNext and Set Request allows the management station to retrieve or set the values of objects at the agent respectively. The acknowledement to the station comes by the agent in the form of GetResponse message. Also an agent can issue a trap message in response to an event that has a possibility to affect the managed

resources.

In their Data Collecting Module here a collecting program runs on a single manager station. The collecting process is creating four threads. Sending thread, preprocessing thread Receiving thread and Storing thread. These four threads are being controlled by a main controlling thread.

2.1.5 SNMP and Beyond

Paul Moceri, [5] in "SNMP and Beyond: A Survey of Network Performance Monitoring Tools writes about the most common class of tools is based on the Simple Network Management Protocol (SNMP), a protocol for sending and transmitting network performance information on IP networks". Other types of network performance monitoring tools have included packet sniffers, flow monitors and application monitors. Examples of the various monitoring tools are SolarWind's Orion SNMP monitoring platform, Ethereal packet capture tool, Webmetrics' GlobalWatch and Cisco's NetFlow flow monitoring tools is also given

He talked about metrics in the networking arena saying they are availability, throughput, bandwidth utilization, and latency (or delay).Though administrators are most of the time have interests only in error rates and the performance of network devices . These performance metrices can be CPU and memory usage, RAM stats and delay (or latency). Each of these metrics can be classified as lower is better (LB), higher is better (HB) or nominal is best (NB). This classification system is taken from [Jain91]

Comparison of Performance Monitoring Tool Types is done and summaries the different types of monitoring tools and highlights the differences among them in a tabular form. The majority of the types are active which makes them much more comprehensive. Also, the different systems vary a great deal in which layer or layers of the network stack they operate in.

2.1.6 Web-Based Automatic Network Discovery / Map Systems

Chakchai Netphakdee, Chinnakorn Wijitsopon, Kasidit [6]In their paper "Web-based Automatic Network Discovery / Map Systems introduced a new automatic network discovery/map system via Web architecture, called WANMS (Web-based Automatic Network discovery/Map Systems)". The system functions as a plug-in for a well-known network management system called Cacti ".Their Enriched features, especially the automatic networking discovery and map module, have been added in order to enhance the efficiency of Cacti embedded with a weather map plug-in.

The discovery process generates XML-based information so that a graph visualization using jQuery via HTML5 can generate a simplified network map using a force-directed layout technique. WANMS is easy-to-use and less complicated, and so lessening the discovery time.

In particular, for performance comparison with OpenMMS and DNMA, which are well known NMS ,WANMS outperforms others in several perspectives, which are faster convergence, better coverage, and more details of types of networking devices. Their system is presently used at the department of Information Technology, Provincial Police Region 4, Thailand.

2.1.7 SNMP Network Management

Paul Simoneau [7]in "SNMP Network Management explains the basic information for understanding how SNMP arrived and its present state". He delves the book into the details of SNMP in different Versions. Also he explains through X.700, the aspects of managing networks using open standard MIB in SNMP. He defines the Network Management, importance of SNMP protocol, MIB-I, MIB-II.

2.1.8 Essential SNMP

Douglas R.Mauro and KevinJ.Schmidt [8]wrote "Essential SNMP ,Book by OREILLY,2009 talks about Simple Network Management Protocol (SNMP) which provides a simple set of operations that allows administrators to easily monitor and manage network devices like routers, switches, servers and printer". The information that can be monitored with SNMP are traffic, bandwidth, temperature, memory usage, system uptime, status of in-

terfaces and many more.

O'Reilly has given a practical introduction to network monitoring. It shows how to install, configure, and manage SNMP. It is specially written for network and system administrators. The book has introduced the basics of SNMP. It surely has offered a technical background. It explains how to use it effectively and efficiently. Essential SNMP explores, and elements like OIDs, MIBs, community strings, and traps in depth.

Name	Type	Access	Description
ifDescr	OCTETSTR	ReadOnly	A textual string having information about interface. It should include the name of the manufacturer, the product name and version of hardware/software.
ifType	INTEGER	ReadOnly	The type of interface
ifSpeed	GAUGE	ReadOnly	An estimate of the interface's current bandwidth in bits per second.
ifOperStatus	INTEGER	ReadOnly	The current operational state of the interface.1-up, 2-down, 3-testing, 4-unknown, 5-dormant, 6-notPresent and 7-lowerLayerDown
ifLastChange	TICKS	ReadOnly	The value of sysUpTime at the time the interface entered its current operational state.
ifInOctets	COUNTER	ReadOnly	The total number of octets received on the interface, including framing characters.
ifOutOctets	COUNTER	ReadOnly	The total number of octets transmitted out of the interface, including framing characters.

Table 2.1: ifInterface Mib Table

The book stores a list of tables explaining about each and every mib and oid and how and where they can be used.

2.1.9 SNMP,SNMPv2,SNMPv3 and RMON 1 and 2

"William Stallings[9] in SNMP,SNMPv2,SNMPv3 and RMON 1 and 2 explains that how organizational growth leads to need of maintaining and monitoring networks". To manage systems and networks, which continue to grow in scale and diversity,into LAN and WAN. He explains fundamental operations related to automated Network Management Tools. How these too ls work in multi-vendor environment and about RMON 1 and 2 of SNMP. No one but William Stallings has seen the pain of using tools which are not free and not easy to use and how multi-vendor environment harm the harmony of those tools.

The figure below is taken as a snapshot from the comparison of various Network Monitoring Tools from Wikipedia

Name	IP SLA Reports	Logical Grouping	Trending	Trend Prediction	Auto Discovery	Agentless	SNMP	Syslog	Plugins	Triggers / Alerts	WebApp	Distributed Monitoring	Inventory	Platform	Data Storage Method	License	Maps
AccelOps	Yes	Yes	Yes	Yes	Yes	Supported	Yes	Yes	Yes	Yes	Full Control	Yes	Yes	Unknown	PostgreSQL	Commercial	Yes
AggreGate Network Manager	Yes	Yes	Yes	Yes	Yes	Supported	Yes	Yes	Yes	Yes	Full Control	Yes	Yes	Java	MySQL, MS SQL, PostgreSQL, Oracle, Firebird, HSQLDB	Limited free, Commercial	Yes
Argus	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Viewing, Acknowledging, Reporting	Yes	Unknown	Perl	Flat file, Berkeley DB	Artistic License	No
BLÉSK	Yes	Yes	Yes	Yes	Yes	Yes[1]	Yes	Yes	Yes	Yes	Yes	Supported	Yes	C, PHP, Perl	MySQL PostgreSQL Elasticsearch RRDTool	Commercial	Yes
CA Spectrum	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Unknown	MySQL	Commercial	Yes
Avaya VPFM	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Full Control	Yes	Yes	Unknown	MySQL	Commercial	Yes
Cacti	Yes	Yes	Yes	Yes	Via plugin	Yes	Yes	Yes	Yes	Yes	Full Control	Yes	Yes	PHP	RRDtool, MySQL	GPL	Plugin
Centina Systems NetOmnia	Yes	Yes	Yes	Yes	Via plugin	Yes	Yes	Yes	Yes	Yes	Full Control	Yes	Yes	Java	MySQL	Commercial	Plugin
collectd	No	No	No	No	Push model; multicast possible	Supported	Yes	Yes	Yes	Yes	Viewing	Yes	No	C	RRDtool	GPLv2	No

Figure 2.1: Comparison of various Network monitoring tools

2.2 SNMP

"Simple Network Management Protocol (SNMP)[5] is used in network management systems to monitor network-attached devices for conditions that require administrative attention". SNMP presents management data in the form of variables on the managed systems[1]. These variables may then be queried (and sometimes set) by managing application. SNMP uses an extensible design, where the available information is defined by Management Information Bases[8] (MIBs) which often proprietary to individual vendors. "MIBs[4] describe the structure of the management data of a device subsystem in a hierarchical structure, namespace containing Object Identifiers[7] (OID)". Each "OID identifies a variable that can be read or set via SNMP". "SNMP-based monitoring [3] involves reading so called Object Identifiers (OIDs) implemented in MIBs by SNMP-enabled systems such as routers, switches, servers and hosts,and presenting the data to the user in some way e.g. serving real-time graphs or OID values"

In 1988 SNMP was first introduced to world. It was designed meet the growing need for a standard so as to manage Internet Protocol (IP) devices. SNMP is a simple set of

operations that provides the ability to query and set the state of some devices to network administrators. Although SNMP is capable of managing a wide variety of network devices (including but not limited to printers, personal computers, servers, power supplies, etc.), it is typically associated with routers and other network devices. SNMP is defined by The Internet Engineering Task Force (IETF) using Request for Comments (RFC) specifications. Currently, there are three versions of SNMP in use. SNMP v1, v2 and V3 are the three versions of SNMP .

SNMP Version	Defining RFC(s)
SNMPv1	RFC 1157 Simple Network Management Protocol
SNMPv2	RFC 1905 Protocol Operations for SNMPv2, RFC 1906 Transport Mappings for SNMPv2, RFC 1907 MIB for SNMPv2
SNMPv3	RFC 2571 Architecture for SNMP Frameworks, RFC 2572 Message Processing and Dispatching, RFC 2573 SNMP Applications,RFC 2574 User-based Security Model, RFC 2575 View-based Access Control Model, RFC 1905 Protocol Operations for SNMPv2, RFC 1906 Transport Mappings for SNMPv2, RFC 1907 MIB for SNMPv2

Table 2.2: RFC's defining SNMP Versions

2.2.1 Components Of SNMP Based Monitoring

An SNMP-managed network[7] consists of three components [10]: Managed Devices[7], Agents[9], and there can be one or more network Management Systems.

- "A Managed Device[8] is an equipment that is in on network and is SNMP compliant. Any device may be Routers, switches, workstations, hubs, ups and printers

are examples of Managed Devices".

- "An Agent[8] is typically software that resides on a Managed Device". It collects data from the managed device and translates that information into a format that can be passed over the network using SNMP. It collects data from the network device. this data is stores it in the MIB of the network device. The agent will be sending the information to the SNMP Manager back as when it is polled.

- "A Network-Management system[9] monitors and controls managed devices".

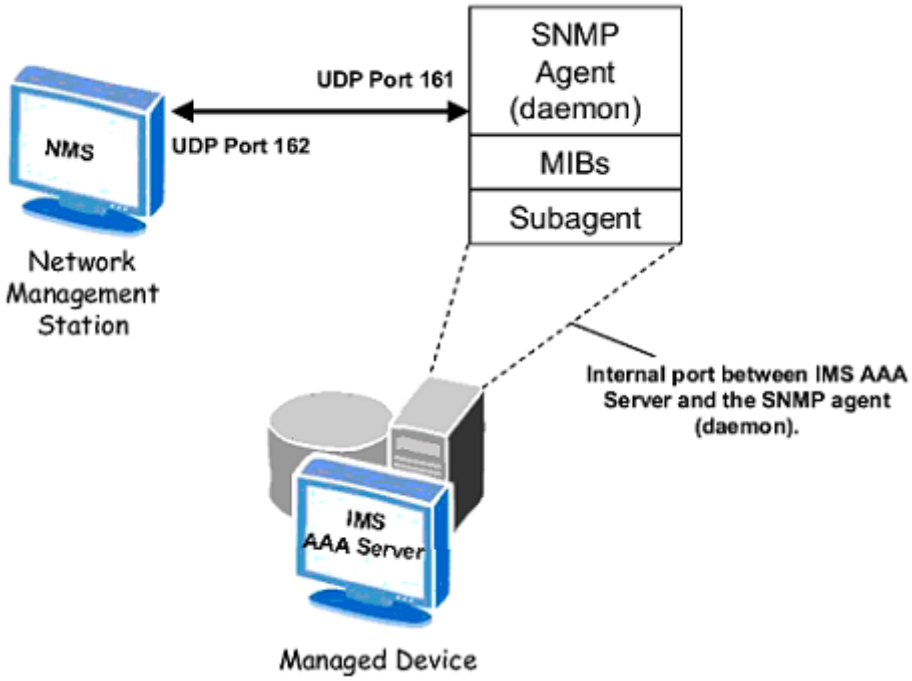


Figure 2.2: Components of SNMP

The above figure[23] shows how the NMS gets information from the managed device. A network Monitoring System uses SNMP to get information from the managed device. NMS sends SNMP request on UDP(User Datagram Protocol) and on port 161 to the SNMP agent which is a daemon[8].SNMP agent contacts the subagents on the device on internal port and collect relevant information of SNMP get request and gives SNMP response on UDP port 162.

2.2.2 SNMP MIB Tree

The SNMP has three components when we talk about it a network management system and those are as follows:

- **Structure of Management Information (SMI)** The Structure of Management Information (SMI)[7] is defined in RFC 1155. The definition of the data types that are allowed in MIB are defined in SMI. It sets always a unique naming structure for every managed object
- **Management Information Base (MIB)**[7] MIB [7]objects have six attributes. "An object has a name, an object identifier, a syntax field, an access field, a status field, and a text description". It sets always a unique naming structure for every managed object in Management Information Base (MIB)[8]. "In RFC 1156 we can see the definition of managed objects contained in MIB". All these information can be accessed using SNMP protocol. Managed objects can store information like system uptime, interface In and Out traffic, system name etc. All these values are stored in tabular form or scalar form

The below figure[4] shows : The MIB tree which is collection of objects which is referred to be a management information bases (MIB). This mib is a tree like structure which gives the oid in numeric form. We may say an Oid to be 0.1.3.6.1 if it is about internet.

2.2.3 Net-SNMP Commands

Net-SNMP is a network management application. This application contains several basic commands, including read, write, trap, and traversal operations. The most basic operations include: Get, GetNext, Set, and Trap

- Get is used to retrieve the value of an object instance from an agent.
- GetNext is used to retrieve the value of the next object instance from a table within an agent. It allows the administrator to step through objects in tabular form.
- The Set function is used to write a value to an object instance within an agent.
- Traps are used by agents to send information to the network management system.

Below figure[8] shows the architecture of how commands between the SNMP manager and SNMP device communicate

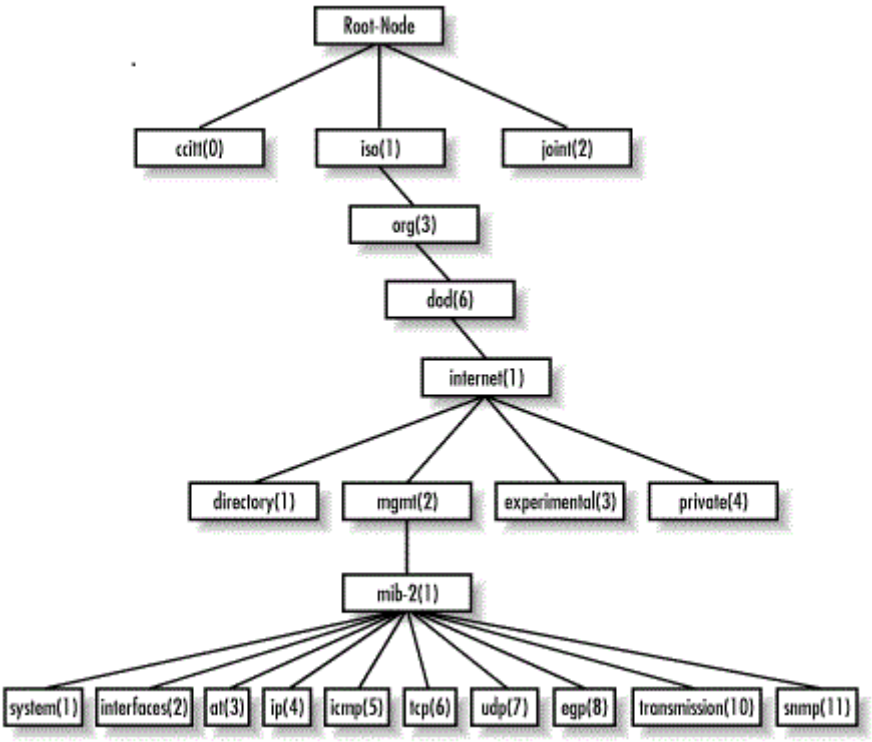


Figure 2.3: Mib Tree

2.3 Round Robin Database

"RRDtool[22] (acronym for round-robin database tool) has aims to handle time-series data like network bandwidth, CPU load, Memory Usage etc". The data stored in a round-robin database is stored in a circular buffer. Over time the system storage footprint remains constant. RRD Tool can be easily integrated in shell scripts, perl, python, ruby, lua or tcl applications. RRD Tool is open source

Usually in a round-robin database (RRD), time-series data like network bandwidth, memory usage, CPU load etc. are stored. The data is stored so that system storage footprint remains constant over time. This actually avoids resource-expensive purge jobs. Also it reduces complexity. MySQL does NOT provide any such kind of storage engine. RRD tool has also the ability to create and feed this database. RRDTool stores data; that makes it a back end tool. The RRDTool command set allows the creation of graphs, that makes it a front end tool as well. Other databases just stores data and can not create graphs.

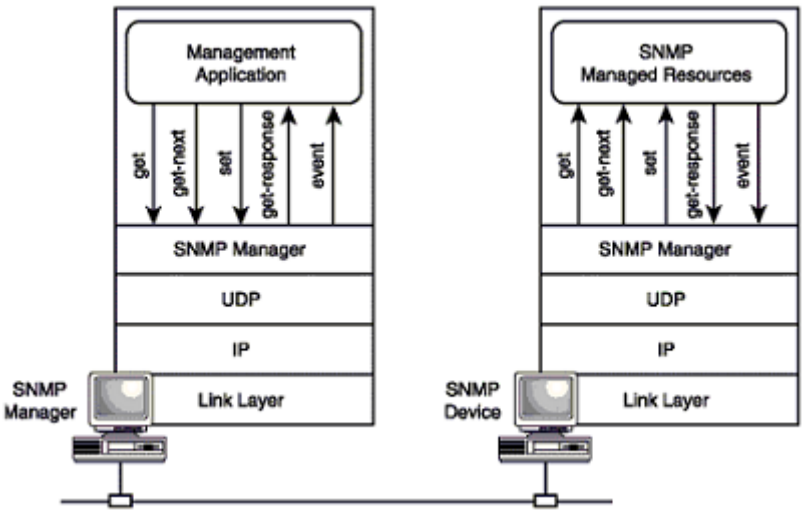


Figure 2.4: Basic SNMP commands

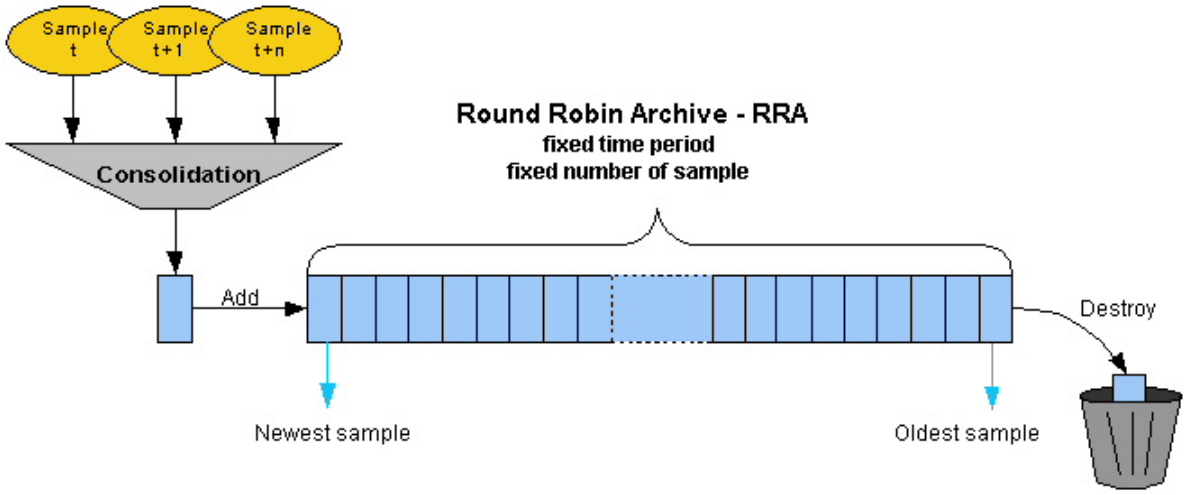


Figure 2.5: Life of data in Round Robin Database

2.3.1 Handling of Data in RRD

RRD Tool does not store data as we hand it, rather it re-samples the data and store the re-sampled version of it. Tools like some Network Monitoring gathers data every 5 minutes but its not always that it can make it possible to gather data at that spur of time. The possible reasons for he same are

1.Query lost

2.Device Down

Data arrive roughly 5 minutes but not exactly. It takes actual arrival time under curve and create new points in time between interval and make a curve beneath that real curve. Thus traffic latency will be same but the numbers shown may differ. You can read more

about how RRD stores data, what are the commands or functions of each object in RRD in appendix B

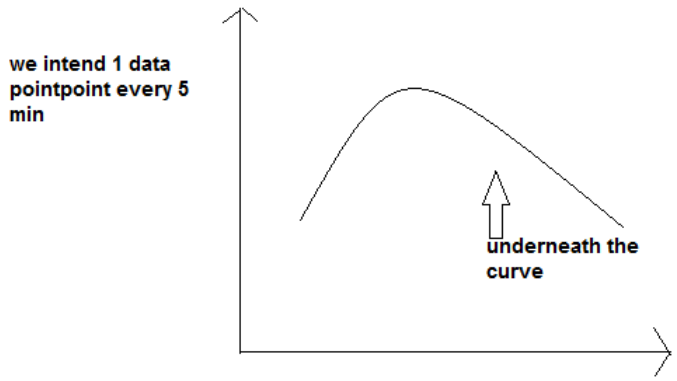


Figure 2.6: RRD's mechanism to plot Data Points

2.4 Conclusion

All the research show that SNMP is efficient enough to be used for designing a framework for Network Monitoring System. Considering the features of SNMP like flexibility and simplicity and less load, A SNMP based NMS can be designed which support ubiquitous access. By quering the network devices at specified intervals information can be received in a raw form. RRDtool can be used for storing the statistics received from the querying.

Real-time visualization of network status in a graphical format, plotting the disk usage, memory usage and traffic analysis of in and out traffic at each interface can be made possible using SNMP, RRD Tool and some other low cost tools.

Chapter 3

The Proposed Approach And Tools Used

SNMP[10]is the most widely used protocol for the management of IP-based networks and internet. The original version, also known as SNMPv1, has been widely deployed. It can monitor and provide statistics about network devices like router, switches, servers and workstation. It uses UDP to send and receive its messages from its agents to monitoring device on port 160 and 161.

NMS(Network Monitoring System) is concerned with the monitoring of network and it should do following things

◇ Show real-time uplink and downlink status

◇ Include discovering network statistics

◇ It must monitor device health and status

◇ Must do network traffic monitoring for each switch and each port with real time traffic graphs

◇ Provide alerts in case of connectivity or looping problem

◇ Create a map of Network

3.1 Steps to Network Monitoring

The following are the steps so as to monitor whole network including servers, switches and other network devices.

Why Network Monitoring System is required

Nowadays the world has become connected, real-world usage of computing is revolving around the concept being able to do networking and so network monitoring has become extremely important. It is surprising to know that many businesses and organizations have failed to spend a quantitative amount of time and capital in being able to set up a really reliable and carefree network monitoring.

Often overlooked fact but which is obvious is that without a consistant network, there can be no proper and reliable networking. Especially when the organization is fully dependent on the network and it wants all its workstations working all the time, there is need of a Network Monitoring system which will help the administrator be aware of the conditions of the network. The details of what the network is doing, how it is performing and where the problematic areas are, are often not available simply to the network administrator.

The importance of a business's network is often overlooked as "simply there", yet the critical nature and growing importance of LANs in a business organization make it obvious why network monitoring system is absolutely vital, and cannot be omitted or neglected. One of the reasons for the small number of network monitoring system in use is the unfamiliarity with the network management approach, and the complexity of many suitable applications in general.

3.1.1 Visualize The Network

To fully and truly understand that how a network is always functioning is by using a network monitoring application which always displays the current representation of your network graphically . Monitoring network health via lists of detected hardware is to be done in network. We need to make a relationship with different graphs. What we need is to built a Networ kmap and that too accurately so as to improve the speed of solving network related problems and able to track back the error. It can always help to trace the spots which may trouble later, and help in deciding where to add new type of hardware mechanism to introduce fault-tolerance in the network.

For this we will built a graphing system to make beautiful and real-time graphs . Here

the only feild the user will need to provide will be Ip address and Community string of the enabled snmp of their network.

3.1.2 Alerting And Logging

We would like to built an alerting mechanism so that if there are any outrages in the network that needs to be known to network administrator as soon as possible. We would firstly need to monitor the status of the switches or routers or even servers and work stations. Now when we do this using SNMP only manageable component of network like network devices which have SNMP installed on it like on server and workstation or manageable router, switches or ups may reply to the polling request of the monitoring server. If possible, the number of unmanageable equipments should be as reduced as possible so that it may not will create black spots. These black spots or say holes are places that the administrator cannot monitor from his desktop.

As we know that all devices in a network cannot be thought of as being of equal importance. Router and switches are of more importance as in terms of how it impacts the network failure ofcourse more than just a printer or a terminal server.
Network Administrator would always want to be updated about the main events occuring in network like power failure of a ups or the router which is the gateway to the internet. He would like to know that switches and router which are critical are working or not. He would not want the Mail server o crash and he knows last. A non-functioning printerif goes down, it is of less importance and can wait - especially when alerting is performed via an e-mail and more when on weekends and holidays.

Network Administrator should only be alerted once about the same failure.A quite regular encountered problem or say side-effect of an intelligent alerting system is that sometimes it proves to be not correct or overassuming, but alsonot so important events may be hidden. Not so important events will not be requiring any adjacent actions but they may indicate problems that are potential in near future. To have a record of the events that are not so important, a logging system is to be made and the logs hence received should be checked by the administrator regularly.

3.1.3 Collecting Historic Information

For Base-lining And Trending Purposes collection of historic information plays an important role. Base-lining is nothing but analysis method in a network that is comparing changes in actual data in accordance to a baseline. Regular requirement of base-lining is that like a tool in performance watching for trend analysis - a metric comparison to some historical value of performance monitoring is similar to finding a style or say a trend that may help in estimation of future needs or performance to find a trend that can be used to estimate near future performance or needs. We need baselining for watching network device health and problems. We need to do is taking some proactive measure to manage faults or atleast monitor them.

First thing is to know the normal behaviour of the network and then detecting anomalies in the network behaviour we can always detect some fault occurance. Here this normal behaviour is the trend or the baseline of the network behaviour. We take and collect the information from different network device and check thier performace for a while say a week or a month. We just need is the raw information but needs to be filtered by some mechanism like graphing these statistics say into a graph showing daily, monthly or yearly basis. This collection of historic data also us to get a clear network picture and its behaviour. Also we may always trace back how the problem occurrance took place in the history, and why and when it may happen again in the nearest time coming. Historic information combined with well-defined threshold monitoring are essentials that help to discover potential problems before they actually occur.

3.1.4 Threshold Monitoring

We need to set up the threhold monitoring. We can have two methods to monitor network as follows they are well defined

- **Monitor Health** This is usually dome by doing the polling of network devices from time to time to know the status of them being up or down at first level. We have

specific MIB defined for each type of device which has lots of information about the device. Being able to view them in a tabular form or a graphical form can really help administrator of the network to analyze the device and its behaviour. We also have SNMP trap which sends reply in case there is some failure, we just need is to enable it. Suppose there is a problem and polling is done from time to time it will show some gradient differnce in the graphs plotted to visiblize the difference.

- To limit the traffic generated by these polling mechanism we may send a probe only at say 5 minutes interval only during Office hours. Even a cron job which will poll between the office hours ie from 10:00 A.M. in morning to 10:00 in evening can be used.

- **Define thresholds**We define threshold to monitor problems that are known in advance. Suppose we have a problem that a server has been hanging again and again, we can moitor the CPU load or the memory usage if not exceeding more than 80As when the values of the polling reponse exceeds the threshold, a kind of alarm is generated and notified to the admin.

3.1.5 Graphing in Real-Time

When we are collecting network statistics graphing of those statistics is very important. We may keep an archival of the network metrices in the form of graphs but what if we want to see current stats. We would like these statistics to be in a graphical form say the CPU load or RAM usage in a bar graph or a pie graph.This type of graphing allows detailed depth analysis of the system. Real-time tables and graphs can serve the users of the system to immediately respond to basic problems as soon as possible.
(SNMP request) will be shooted from the monitoring system to the network devices, to show real-time graphs, Meters or tables. For application servers create files to show CPU usage, RAM usage, logged in user sessions, disk usage, buffer space, slack area etc. For routers definition files to read the ipRouteEntry, ifSpeed, ifInOctet, ifOutOctet table and display the traffic/load per interface graphically.

3.2 Selection Of Tools To Develop Such A SNMP Based Network Monitoring System

Here we will consider tools to be low cost in terms of availability of those tools, development time and amount of resulting code. Also tools that are easily adaptable and maintainable will be used

3.2.1 Overview

When designing the monitoring system,we need tools using which have features such that it has possibility of modifying the monitoring code as well as the user interface. Such a monitor will be comprised of following components:

- A Web-based Monitoring GUI which resides on the Administrator's LINUX machine. This front-end GUI is presenting the network Map to the user so that the user can select target links or nodes to be monitored. An HTTP server for remote access to the monitoring GUI, serving dynamic HTML content such as 'Network Map' and 'traffic graphs', 'Statistics' and 'Alerts'.

- A Back-end Monitoring Server which includes a poller that handles the monitoring of the selected OlDs i.e. Interface statistics of the known IP addresses in the network. Each link on the network Map has to have some rrds bound to it , presented by the monitoring GUI . ALso it can launch snmp requests to the poller which works at back-end.

- Net-SNMP a tool to use SNMP protocol, which is working at backend and its queries are going to collect the data from the devies.

3.2.2 PHP

PHP is aa server side scripting language. It is specially designed for web development. It is open source and PHP commands are directly embedded to HTML source document. But it does not call an external file to process data. We can use command line interface to generate programs in PHP. Its very important feature is that it has so many already

defined functions in it. It has capability to be used as standalone graphical applications. Any PHP code in a requested file is executed by the PHP runtime which makes it run easy and faster. It is used for command-line scripting of client-side graphical user interface (GUI) applications. Hence PHP will be used for making the interactive GUI with the help of HTML.

3.2.3 Net-SNMP v5.7.2

Net-SNMP [17] is a suite of applications. It is used to implement SNMPv1, SNMPv2c and SNMPv3. It uses IPv4 and IPv6 and includes Command-line applications to:

- It has a vast library for developing new SNMP applications, in both C and perl APIs.
- It includes Network management system (NMS) software which runs on the manager of Network monitoring system.
- Information from snmp enabled device is collected by commands like[8]
  - snmpget and snmpgetnext- Retrieve a fixed collection of information from an SNMP-capable device
  - snmpwalk, snmpdelta and snmptable- Retrieve a multiple amount of information from an SNMP-capable device
  - snmpset- Manipulate configuration information on an SNMP-capable device
  - snmptranslate- Convert between numerical and textual forms of MIB OIDs, and display MIB content and structure
  - (snmpdf, snmpnetstat, snmpstatus)- Retrieve a fixed collection of information from an SNMP-capable device.
  - (snmptranslate- Convert between numerical and textual forms of MIB OIDs, and display MIB content and structure .

The monitoring back-end server can use the Perl interface to the freely available Net-SNMP tools [17] or the PHP based API for reading OlDs from the targets. Net-SNMP provides better security mechanisms that would ensure controlled access to the monitor.

3.2.4 HTTP Server

If we want a ubiquitous access for he admin, an HTTP server [18] can always be suplemented with the monitor back-end. The HTTP server can be used to present the GUI through the user's browser for remote access to the monitor. We can always launch monitoring requests From the web-based GUI to selected links/nodes to the monitor. So we can monitor at back-end and always display on the client side. The HTTP server can be used for serving dynamic content such as graphs and statistics of snmp response to the user.

3.2.5 JavaScript Programming

JavaScript (JS)[19] is a computer programming language which is interpreted. It uses Java runtime programing criteria. It allows client-side scripts to interact with the user and control the browser. It can asyncronously communicate and alter the document content that is displayed. We can write java script to do validation of Web pages. Adding these scripts to PHP is also possible. Formating of the Styling layout of webpages is also possible.

3.2.6 Perl Programming Language and graphing libraries

Perl[20] is a scripting language that is suitable for designing the Monitoring Back-end server. Implementing the monitor back-end code in Perl is very less costly in terms of development time and the amount of code than implementing in strongly typed languages such as Java. Perl features as below are helpfull in creating good monitoring server which can interactively contact the web-based GUI. Availability of an API for the freely available Net- SNMP tools[17][and availability of APIs for graphing tools, image production.

3.2.7 RRDTool 1.x

RRD Tool[22] is the Open Source industry standard, high performance data logging and graphing system for time series data. RRD Tool can be easily integrated in shell scripts, perl, python, ruby, lua or tcl applications. It aims to handle time-series data like network bandwidth, temperatures, CPU load, etc. The data are stored in a fixed size round-robin database (circular buffer), thus the system storage footprint remains constant over

time. So it decreases the cost of infinite storage required by linear database like MySQL. Requires no maintanance or a growing disk-size.

3.2.8 PHP-Weathermap v0.97c

PHP-Weathermap[24] is a used as network visualization tool.It takes data that we have in a raw form and help show users a topology of network say in a map form. A map of the network can be designed by by Rich visual graphs, which are visible on just one click on the icons of the weathermap. Also it shows the links between the network devices with color patent of link status and traffic on the link. We can target the graphs on click of these links using RRD Tool. These graphs get updated according to time specified in the crontab.

3.2.9 PHP-Server Monitor v1.0

PHP Server Monitor[25] is an open source tool. It checks the list of servers and services. It checks for them to be up and running. It listens the servers or services on the selected ports. It comes with a web based user interface. Here we can add and remove servers or services. This list is stored in the from the MySQL database. Administrator can manage users for each server with a mobile number and email address.
we have a web based GUI, where we can add and remove servers/services from the database. On the "Add server" page, we can choose whether it's a "service" or a "website". If it is services, a connection is made to the IP or domain which is entered already, on the specified port. We can check in this way that the services on server are running or not machine are still running.

Chapter 4

Design and Implementation

The monitoring system is based on SNMPs management model [3, 4]. A layered structure model to design the monitoring system according to the different parts of the system has been used. The proposed model can be thought of as a framework for Network Monitoring system with different modules and layers. This framework can be used to design a easy-to-use Network Monitoring system with low cost tools and open-source projects.

4.1 Three Level Layered Design

The Network Monitoring System consists of 3 layered architecture. Layer 1 which is NMS Web-based GUI, layer 2 which is of Monitoring server and layer 3 which consist of Net-SNMP. NMS consist of 3 basic parts Web-based Monitoring GUI, Monitoring Server and HTTP and Net-SNMP. This three level design will act as the framework on which we will be designing a Web base Application to check if this framework fits well and can a SNMP based Network Monitoring system can give desired outputs.

4.1.1 Layer 3

The third layer is for Web based GUI which is a part of SNMS that we designed later. It is a layer which is signifying the need of user interface. The user can interact with the system in this layer. This layer is also known as "Interactive Layer". This layer consist of modules like Weathermap, graphing, statistics, and Alarms. This layer signifies the need of a Web application at first place. A network Administrator needs to check his network from any where in the organization or even out-side. He needs to have a ubiquitous access to the network. Also in a very big organization, there can be more

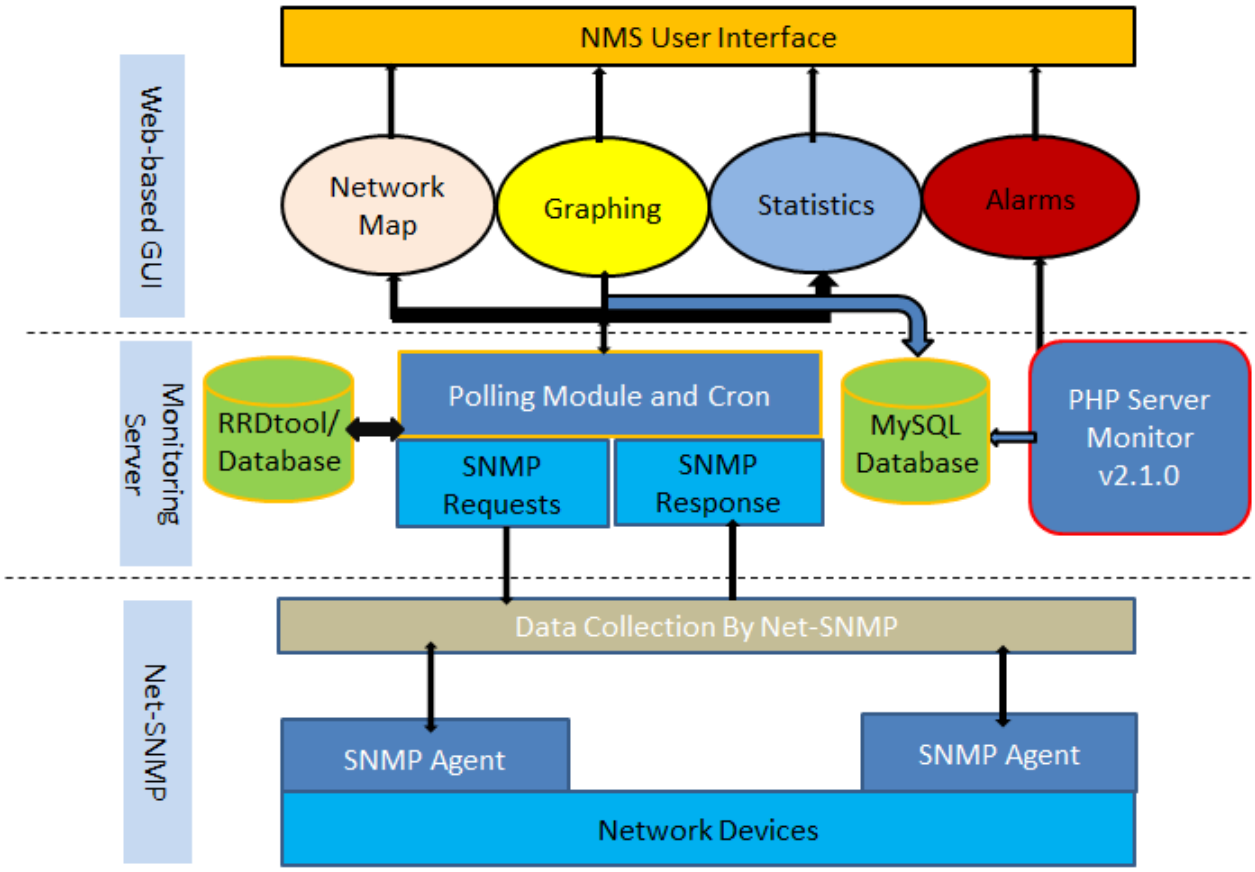


Figure 4.1: Three Level design model for Network Monitoring Sytem

than one Network Administrators, there can be different people keeping different parts of network under observation. For example say a Server Admin who keeps the applications on different Servers, or a Network Admin , the one who keeps the track of routers and switches and who add or change the network topology. For all these people this layer is very important to control and monitor the network at their end or from anywhere in the organization. A web-application can be used as a Network Management Station but which can be accessed from any where in network.

As we discussed in last chapter this layer will help to collect information for base-lining and trending. Also the Alerting and Logging will be done at this layer. The network Network Visualization will also be a part of this layer. Real-time graphing will be the results available to users at this layer. NetworkMap, Graphs, Statistics and Alarms are the modules which can be thought of as fulfilling the objectives to get results in the form of graphs, tables, maps or an email. These modules will be the main menu when

designing a Web-application. Now we will be seeing each and every module in detail to understand the design of each.

NetworkMap Module

- This module is connected to Polling Module, Cron and RRD Tool/Database module at Layer 2.
- For designing this module we have used PHP-Weathermap tool.
- These network maps are HTML pages which show the network devices linked together as the user's network.
- This tool makes beautifully crafted maps of network at different level if we want.
- We need to create a weathermap.conf file and run it.
- The organization of how this configuration file is made is given as an example.conf. Now reading a document on how to add icons and links and targets the design of map, a Network Administrator can easily design this network design.
- Here we can insert icons and labels and links to show the network layout in a beautifully crafted way.
- We need to target the rrd's which we create in Layer 2 using RRD Tool to show the traffic on links between the network devices.

The figure bellow shows an example of such a NetworkMap. This map here in figure in a static map of the external network which is connected to ISP and Internet. Such maps can be helpfull at the time of Network Audits to review the network design. We can add legends and created time to show when the network was updated last. This module fulfills the objective of Visualization of network.

The importance of this module is that the by building network maps as accurate as possible will improve error tracking process and the speed of solving problems. Mapping will help locate trouble spots and help Network Admin to decide where to add new hardware to introduce fault tolerance.

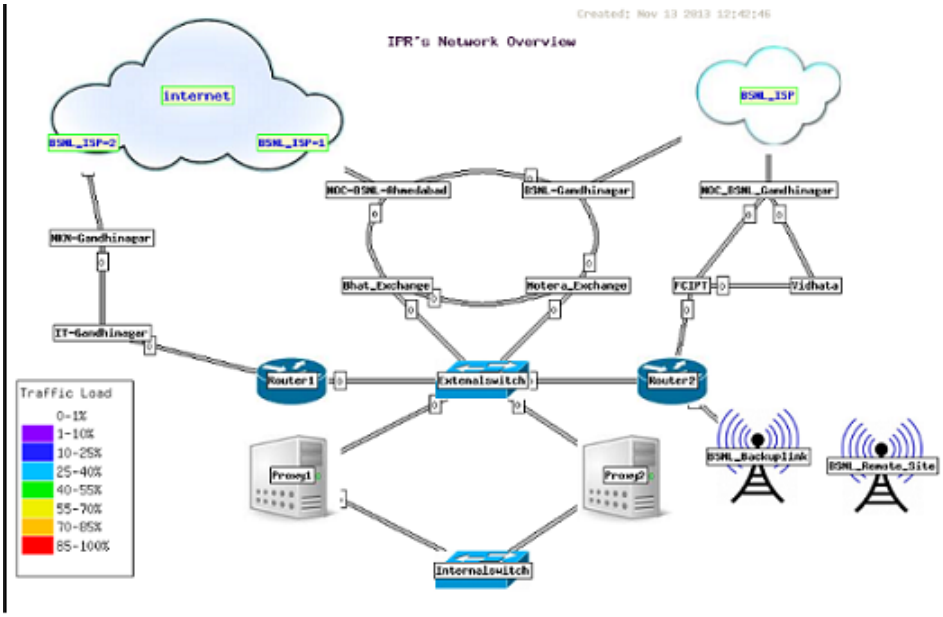


Figure 4.2: An example of the Networkmap

Graphing Module

We collect historic data which can tell us about the network and what can be expected from the network in terms of performance and reliability. In this layer the real-time statistics can be showed in graphical form. This graphing module can help a Network Administrator to immediately respond to basic user requests. He can see the network performance in the form of peaks and valleys in the graphs. These graph can be for last day, last week, last month or last year.

- This module is connected to Polling Module and Cron, RRD Tool/Database module and MySQL database in Layer 2.
- It uses PHP scripts when designed in a SNMS, which in turn create a shell script where rrdcreate is used to create rrd and rrdupdate to update it and the rrdgraph is used to create a graph of the updated rrd.
- These graphs are saved in MySQL database by user which he can view later.
- Also the user will add the shell script to the cron to get updated graphs.
- Also graphs of Memory are made and updated by a script to map the memory of the system

- Realtime CPU Usage and Ram Usage is also calculated simply by "awk" but viewed graphically.
- these graphs are made by using the Perl Graphing libraries which are used by the RRD graph function.

The figure below is a graph showing In/Out traffic of a link. This graph has a very important significance. As the In and Out traffic can show the amount of traffic flowing from that interface of the switch, if there are any outrages ie if there is no flow of traffic signify that the link is unused. Although may be up but if the link is not filled with peaks shows that there is no traffic. Also if there is a very high traffic on the link would be visible to the Network Admin and may be he may use this to know that some traffic needs to be diverted to other links, so as to reduce congestion.

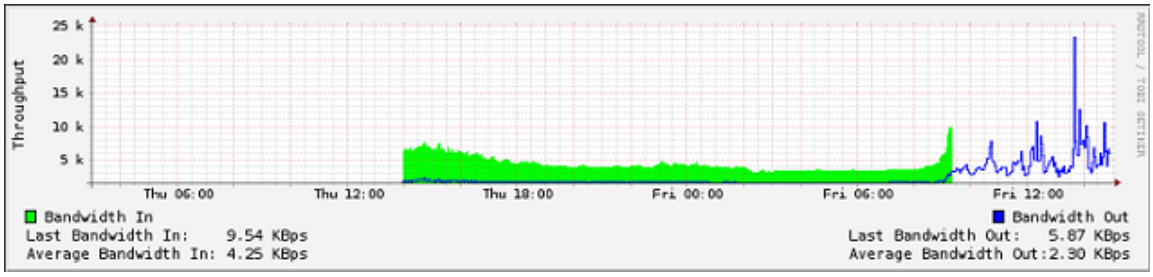


Figure 4.3: An example of the In/Out Traffic of a link

Statistics Module

The user can get statistics in a tabular form which is directly obtained by quering specific Oid of the devices.

- This module is connected to Polling Module.
- Which inturn sends SNMPGet request PDU at back-end to gather information from the network devices in Layer 1
- SNMP Agent on Layer1 sends the SNMPResponse PDU in reply which is viewed in statistics Module by user.

We can get statistics like.

- System Uptime

- No. of Interfaces
- Type of Information
- Speed of the links on the Interface
- In-traffic and Out-traffic of interface
- performance counters

Also information like CPU load, Ram Usage, Disk statistics, Memory Usage etc can be collected in a tabular form using the following Oids

CPU Statistics	Oid Usage	Oid
Load	1 minute Load	.1.3.6.1.4.1.2021.10.1.3.1
	5 minute Load	.1.3.6.1.4.1.2021.10.1.3.2
	15 minute Load	.1.3.6.1.4.1.2021.10.1.3.3
CPU	percentage of user CPU time	.1.3.6.1.4.1.2021.11.9.0
	raw user cpu time	.1.3.6.1.4.1.2021.11.50.0
	percentages of system CPU time	.1.3.6.1.4.1.2021.11.10.0
	raw system cpu time	.1.3.6.1.4.1.2021.11.52.0
	percentages of idle CPU time	.1.3.6.1.4.1.2021.11.11.0
RAM .	Total Swap Size	.1.3.6.1.4.1.2021.4.3.0
	Available Swap Space	.1.3.6.1.4.1.2021.4.4.0

Table 4.1: Server Statistcs And Related Oids

For example: Get information using SNMP snmpget version Community Targetname or Ip Oid This example shows the command which is sent by SNMP Requests module in layer 2 to the Network Devices in the layer 1.

The below figure shows the statistical data The importance of this module is that it can give real-time statistics. Suppose a person coming with a compliant that internet is not working or so, Network Admin can see all the statistics related to ping or interface by just asking for statistics related to Routers or say ifInOctets at the router. Thus he will know if the internet is not working due to problem from ISP. Also it helps in setting the threshold as we can monitor individual devices in this module. Reading SNMP MIB fields also known as Oid of network devices and checking against baseline values to determine potential problems.

All this statistics if available in a proper formatted tabular form that can surely be asy-to-use.

Interface Description:	STRING: FastEthernet0/0
Type of Interface:	INTEGER: ethernetCsmacd(6)
Maximum Transmission Unit:	INTEGER: 1500
Interface current bandwidth in bits/sec:	Gauge32: 100000000
Interface Address at protocol layer:	STRING: 0:1f:ca:5:a4:c0
Current State of Interface:	INTEGER: up(1)
InOctets:	Counter32: 408113613
OutOctets:	Counter32: 2421462273
Mib definitions specific to media:	OID: SNMPv2-SMI::zeroDotZero

Figure 4.4: Interface information in a tabular format

Alarming Module

- This module is connected to PHP-ServerMonitor which stores info in MySQL database.
- It generates alert messages and can send those to user by sms or email.
- It uses POP and SMTP to send mails.
- It checks whether the servers listed or the services added are up and running on the selected ports or not.
- The ports and services are monitored at a fixed interval
- Also Syslogs are generated and stored to keep a track of which service went down at which time.

This module is very important as it makes the Network Monitoring System(SNMS) a proactive step to monitor the network. Keeping track of the Servers and services going down is very important towards Health Monitoring of the Network

4.1.2 Layer 2

The users requests are then sent to second layer which is a Monitoring Server also known as "Functional layer". This layer consist of Polling Module, the SNMP request is sent by

this polling module to the SNMP Agents which lie on layer 3. Also there is Round Robin Database where the data collected from SNMP Response are stored.

As discussed earlier Round Robin database is like a circular buffer so it is best to store the time series data. It is the only database which can store such data. Other than Linear database it has ability to re-sample the data and store re-sampled version of it. Now why this is important, lets suppose a graph is to be plotted of memory usage in the last year. Now if we would have used a linear database, the database would have increased its size to few MB's, also the consolidation of the data would have been difficult. Here our RRD Tool module helps us as it can store as well as consolidate a very large amount of data.

Layer 3 gets all its graphs, weathermap targets, and statistics from this layer. The polling module which is consisting of a cron job which is configured to poll devices from time to time and SNMP Requests and SNMP Responses. These SNMP Requests are sent at a specified time intervals to the data collection module in layer 1. The data from the SNMP Response are sent to Round Robin Database which stores this time series data in form of bit-format files.The data in this database is then going to be fed to generate graphs.

4.1.3 Layer 1

This layer is of Net-SNMP, here data collection is done by Net-SNMP. This layer is also known as "Data layer". As we know Net-SNMP is a suite of applications used to implement SNMP v1, v2 and v3 , this layer of our framework plays an important role in our research for SNMP based Network Monitoring System. It is like a library for developing SNMP based Applications.
This layer also consist of SNMP Agents that reside on the Network Devices. The agent is typically software that resides on a managed device. A managed device[21] can be any piece of equipment that sits on your data network and is SNMP compliant. Routers, switches, hubs, workstations, and printers are all examples of managed devices. The agent collects data from the managed device and translates that information into a format that can be passed over the network using SNMP.

Data is collected from the devices by the SNMP agents that use querying of Net-SNMP. The response that is generated by this Layer is sent to layer 2 in the form of SNMP-Reponse. Also these Agents if SNMPv2 agents can act as Proxy agents. Suppose a SNMPv2 command is issued by our SNMS but it is for SNMPv1 agent, the SNMP get requets will be sent from Layer 2 to the proxy agent. The proxy agent will forward this GET Request to SNMPv1 agent. Thus this module is very important for inter-operability between the different devices in the network.
Agents communicate using messages. SNMPv1 [21]supports five different types of messages: GetRequest, SetRequest, GetNextRequest,GetResponse, and Trap. A single SNMP message is referred to as a Protocol Data Unit (PDU). These messages are constructed using Abstract Syntax Notation One (ASN.1) and translated into binary format using Basic Encoding Rules (BER).

The agent gets the SNMP GetRequest. The query has to specifty the SNMP version, community string, IP Address,and OId example "snmpget versionNo. public Ipaddress Oid ". Here instead of public there can be a community string which is like a private password. Here oid can be in numeric form or text form. SNMP translate can be used to convert textual oid to numeric and numeric to textual. The response in given in the SNMP response form and this data is stored in round robin database.

PDU format for following messages is available:

- SNMP message
- Get/GetNext/Set PDU
- Response PDU
- Trap PDU
- Variable bindings

The pdu format of above messages is show in the figure 5.5

4.2 The Methodology To Implement RRD Tool

RRD Tool is responsible of generating graphs in layer 3. RRD Tool stores the time series data a like network bandwidth, temperatures, CPU load etc. in a circular database. The data is stored in the way that system storage footprint remains constant over time.

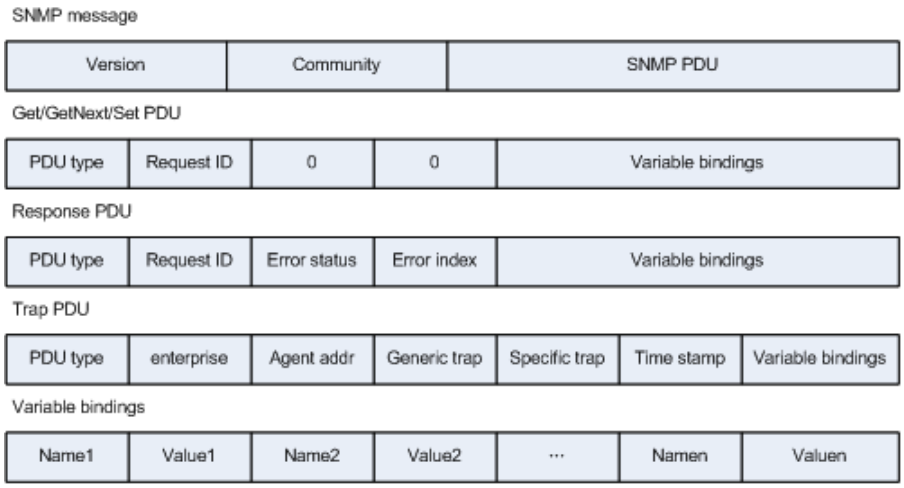


Figure 4.5: PDU format of SNMP Messages

This avoids resource expensive purge jobs and reduces complexity, MySQL does NOT yet provide this kind of storage engine. It does not store data as we hand it, rather it re-samples data and store the re-sampled version of it.

There are three(3) basic steps to setting up RRD Tool and graphing.

4.2.1 Initialize The Database

. Create the rrd database and prepare it to accept data. Need to decide how much data we want to keep, how often the data is going to be updated (step) and what type of data you expect to be collected. We need to decide it.

$$rrdcreate --step 60 - NDS:pl:GAUGE:120:0:100 DS:rtt:GAUGE:120:0:10000000 RRA:MAX:0.5:1:1500$$

Figure 4.6: Example of Initializing database

- step 60 : is the amount of time in seconds we expect data to be updated into the database. update script is going to update the database with the results of the command every 60 seconds using a cron job.
- "start N : is specifying to start Now, here we can specify time in epochs also.
- "DS:pl:GAUGE:120:0:100 " This is our first variable and each option is a colon separated value. Lets take a look at each option. DS says that this is a data set. pl is the variable name we have chosen to stand for "packet loss". GAUGE is a RRD Tool directive to mean the data entered is absolute and should be entered as

is without any manipulation or calculations done to it.120 is the heartbeat timeout in seconds. If data is not entered in at least 120 seconds then zeros are put into this DS record. Since we created a rrd database with a step of 60 seconds (step 60) we would need to miss 2 full "steps" before RRD Tool put in zeros. This time out is important to signify if the system was unable to collect data due to a reboot or system downtime. Missed data will show up on your graph as a blank area with no data graphed. 0 is the minimum value that will be accepted into the data base. Since the variable is for packet loss we expect the value to be between 0100 is the maximum value that is accepted into this field. This variable is packet loss (pl) and we expect to see a value between 0

- "DS:rtt:GAUGE:120:0:10000000" :This is our second variable and each option is a colon separated value. DS says that this is a data set. rtt is the variable name we have chosen to stand for "round trip time". GAUGE is a RRD Tool directive to mean the data entered is absolute and should be entered as is without any manipulation or calculations done to it. 120 is the heartbeat timeout in seconds. If data is not entered in at least 120 seconds then zeros are put into this DS record. Since we created a rrd database with a step of 60 seconds (step 60) we would need to miss 2 full "steps" before RRD Tool put in zeros. 0 is the minimum value that will be accepted into the data base for this field. The rrt variable stands for "round trip time" and can not be negative since that would not make any sense. 10000000 is the maximum value that is accepted into this field. This is just a large enough value so that any oversize " rtt" value will be accepted.

- "RRA:MAX:0.5:1:1500" : This is the round robin archive directive. Each option is a colon separated value. RRA directive defines how many values the the RRD database will archive and for how long. MAX normally means to only accept the maximum value if multiple values are available over multiple "steps". We are using MAX simply to say that we have one variable which will contain one number and it should not be changed or averaged in any way. 0.5 is an internal resolution value and should not be changed. "1" specifies how many steps should be averaged before storing the final value. We specify "1" because we want the value updated in the database to be stored as is; one step equals one database value. 1500 is how many

"steps" we will store in the db. Since we specified a step of 60 seconds (step 60) we will store 1500 samples times 60 seconds which equals 90,000 seconds. This also equals 25 hours. So, we will have 25 hours of 1 minute resolution data that we can graph. This is a nice granularity and will allow us to make a very good looking, and more importantly, visually accurate graph.

4.2.2 Collect The Data Sets Over Time

We update the rrd file after every specified interval. A cron job will run to collect data using a script you will write to enter that data periodically into the database. This is the step that will probably take the most time to get working correctly. In our examples we have done all the work already. For this we wrote a shell script to update the database

4.2.3 Create The Graphs

The last step is to take the data from the rrd database, do any calculationis you want to do on the data and create that actual graph. We also want to run this step using a cron job and move the graph over to a web server directory for easy viewing.

Chapter 5

SNMS- SNMP based Network Monitoring System

In this chapter we will discuss about the Web-based application which we generated using the framework which has a 3 Layer architecture, about which we already discussed in last chapter. Lets call it as SNMS (SNMP based Network Monitoring System). This Application is made of various tools available as open-source under GPU (General Public License). It has been developed under restricted lab environment.

5.1 User Registration

A user can be Server Admin or a Network Admin or say a G-mail Administrator, the first thing he will need to do is register. There will be a table

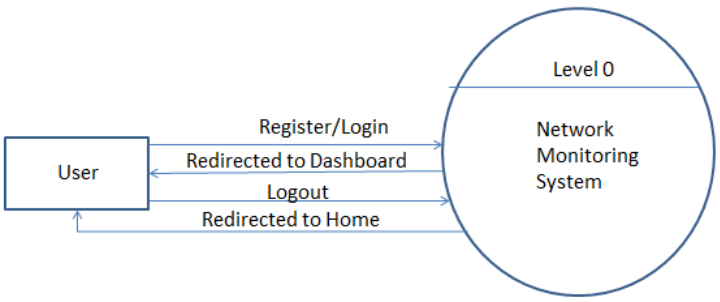
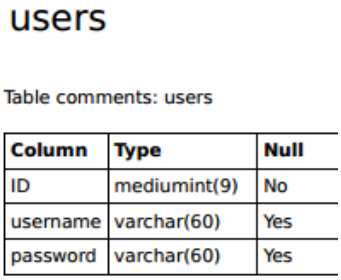


Figure 5.1: Level0 UseCase of NMS

- User Needs to Register if he is a new User, On clicking on "Register"
- User enters his User Name and "Password" and Confirm "Password".

- A php script runs which connects to database "nms" and inserts the UserName and encrypted password into table "users" .
- It also checks if the user is already registered and if so it throws exception "UserName is already in Use".



users

Table comments: users

Column	Type	Null
ID	mediumint(9)	No
username	varchar(60)	Yes
password	varchar(60)	Yes

Figure 5.2: Data Dictionary for Users Table

5.2 Dashboard

- Once User completes registration He can Login and see the Dashboard
- Dashboard contains a view of critical devices, their location and the status of the interfaces.
- This is done just by Nmap of the devices and then snmpget ifOperstatus of the interfaces on each device.
- To reduce time we can do a small aggregation on the nmap command by sending only small probes.
- Also a look on number of the links up in every subnet is shown on the Dashboard.

The below image shows a snapshot of the Dashboard results. This menu of the application is very important from the point of view of any other person in absence of Network Admin, he can just see the dashboard and come to know if any critical device is down. He may immediately call NA for help. These critical devices if go down can hinder proper working of the network. So this can also be used to keep on the big screen so every one in Computer Department can monitor the network. Also anyone after login, seeing Red light will come to know there is an outrage and can try to mitigate the problem as soon as possible. This is somehow a proactive measure to monitor faults.

	Device	Location	Up	Down
1	10.10.4.1	[redacted]	38	296
3	10.10.4.3	[redacted]	3	25
5	10.10.4.5	[redacted]	12	322
7	10.10.4.7	[redacted]	6	328
9	10.10.4.9	[redacted]	7	21
11	10.10.4.11	[redacted]	2	26
13	10.10.4.13	[redacted]	17	11
15	10.10.4.15	[redacted]	11	15

Figure 5.3: Status Of Critical Devices

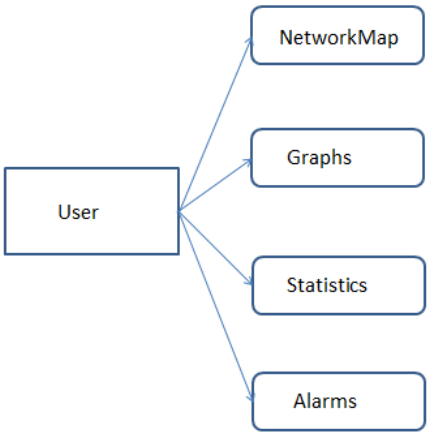


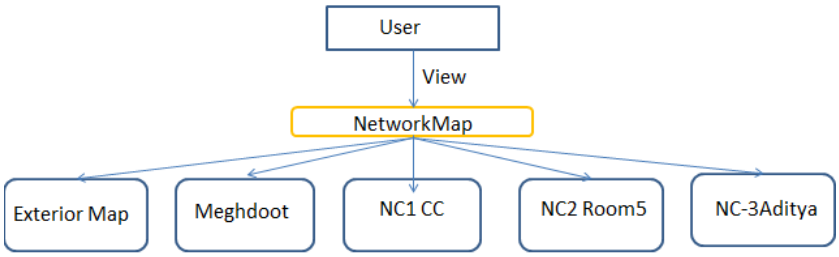
Figure 5.4: Level1 UseCase Of NMS

5.3 Network-Map

This menu in SNMS fulfills the problem of getting a visualization to the network. If one can visualize the network at a glance he can track error and locate trouble spots.

- The User can see the NetworkMap of external network and clicking on the router, he can view the architecture of the network devices connected to internal network in the iframe
- User can click on the links and view the graph of the IN/Out traffic
- User see the link status and average traffic on the first glance itself
- Graphs showing the in and out traffic of the link at one click .

- Also status of the link with current traffic on NetworkMap.



5.4 Ghraphing

This menu in SNMS deals with the performance metrices and graphing of those metrices at realtime and archival of the statistics in a graphical form.

- User Can see the Real-Time Bar graphs of CPU and RAM Usage using a script which runs "cat /proc/stat" to get current CPU info.
- User see Memory usage graphs for which a shell script is run "rrdtool create" to create a rrd, " rrdtool update" by command "awk" and "rrdtool graph" to graph the data.
- User can add new graph to the table "oldgraphs" of any HOST which has SNMP enabled on it and view them later.
- He can create new graphs with names he want to name and using templates like ping, traffic, logged in users.
- He can then specify the IP address of the device he wants to monitor and specifying the Community string given to the device.
- He then needs to select the Graph schedule that is when does he want the graph to be updated ie daily, weekly, monthly, yearly or during office hours from 10 Am to 5 Pm.

5.5 Statistics

This menu gives the real-time statistics. The requests are passed at the same spur of moment and tabular representation of the statistics is obtained. Reading the SNMP

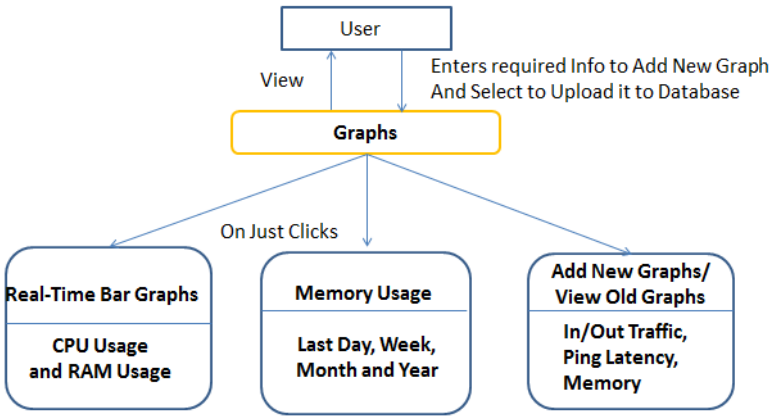


Figure 5.5: User Level Diagram of Graphing Module

MIB fields of network devices. User just needs to pass the IP address and the Community String of the network device. Device specific information can be easily obtained. The summary of the statistics having metrices like System Information, System Load, CPU load, Swap Space, Ram Usage and disk usage of Servers or workstation can be obtained. Also IP Routing information, IP configuration Information and Host Resource information about other network devices can be obtained.

- The user can get statistics in a tabular form which is directly obtained by querying specific Oid of the devices.
  - System Uptime
  - No. of Interfaces
  - Type of Information
  - Speed of the links on the Interface
  - In-traffic and Out-traffic of interfacer
  - performance counters

5.6 Alarming

This menu keeps track of servers or services going down. If a service or a server which is added to be monitored goes down it generates an e-mail and sends it via E-mail server that is configured.

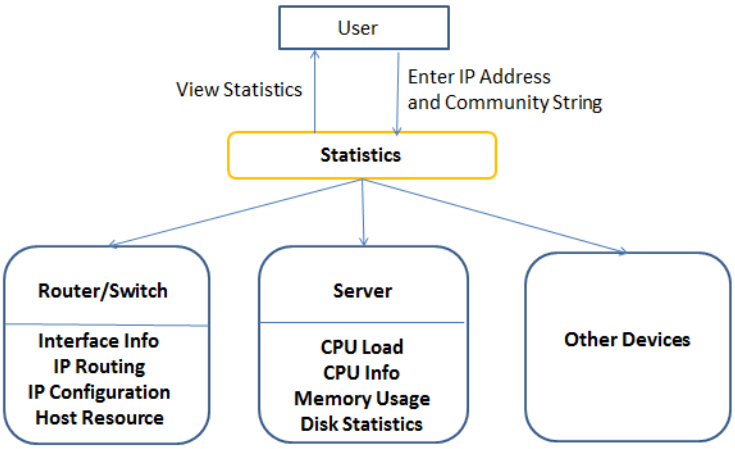


Figure 5.6: User Level Diagram of statistics Module

- User can add Servers and Services to the database servermon and table "psm-startservers" by just click on "ADD" button.
- We need to specify the label , Domain or IP, Port, type of service and search pattern to add new Server/Service.
- Add email of Users to whom the NMS needs to notify in case of flaws to table "psm-startusers".
- View Logs which are stored in "psm-startlog".
- Change Configuration in "psm-startconfig".
- Also Logs can be saved which store the information about the service/server that went down along with the time stamp.

The below figure shows the structure of the table for logging.

log

Table comments: log

Column	Type	Null	Default
logID	bigint(20)	No	
incidentDate	timestamp	No	CURRENT_TIMESTAMP
level	enum('fatal', 'error', 'warning', 'notice', 'info', 'debug')	Yes	*NULL*
user	varchar(100)	No	
subsystem	varchar(100)	No	
remoteAddress	varchar(100)	No	
error	text	No	

Figure 5.7: Data Dictionary for Logs

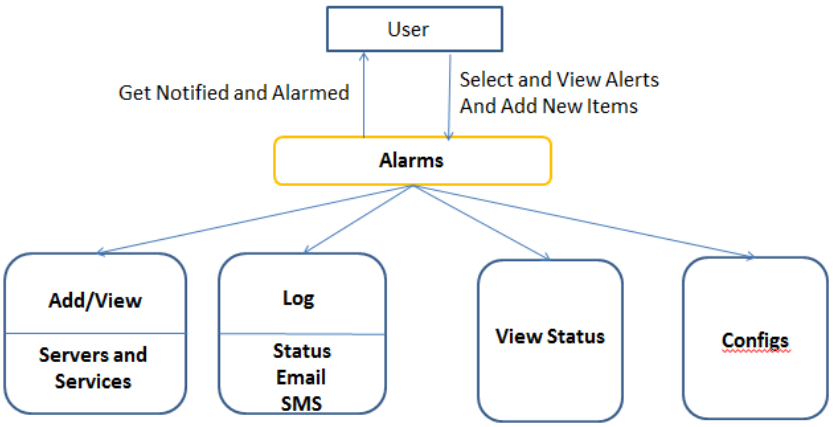


Figure 5.8: User Level Diagram of Alarming Module

Chapter 6

Results and Discussions

This chapter describes the results of the experiments carried out on the experimental setup using SNMS. The chapter also presents the snapshots of the graphs and explains the significance of those graphs and information hence viewed by users. Also how each module in the framework is important is explained in this chapter. For this we have selected specific Hosts in the network and have obtained results from querying those devices only.

6.1 Results

The results show the efficiency of SNMS tool to create graphs of In/Out Traffic, Memory CPU/RAM Usage and statistics in real time. Also the network Map which show the design of network with link statistics and graphs on one click. All this results are consolidated and presented for better understanding.

6.1.1 Networkmap

Networkmap is a network visualization module. Here user can see the maps of network connectivity and links showing In/Out traffic and status of being UP/DOWN

A real-world map donated by Rich visual graphs, which are visible on just one click on the icons of the weathermap. Also it can show the links between the network devices which color legend of link status and traffic on the link. This is the image of weathermap obtained from running the configuration file named weathermap.conf. At first layer of

network we consider the map of the external network ie the network connected to ISP and Internet.

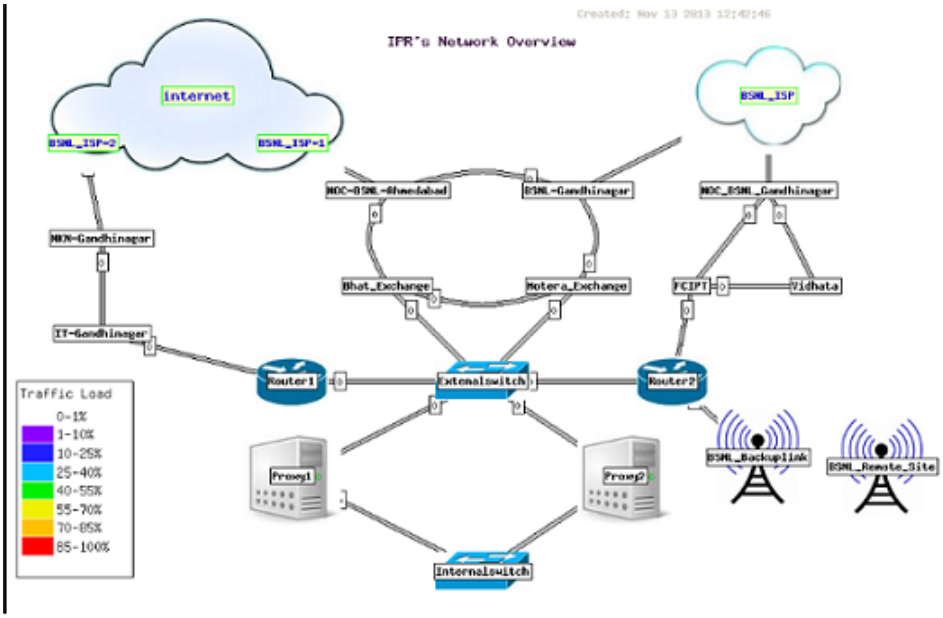


Figure 6.1: Map of Exterior Network

The next map is weathermap html which is just viewed by clicking on the internal router on the first Networkmap page ie Meghdoot here. This map shows the legend the icons of the network devices here switches connected to each other. They have links filled with color which signifies the bandwidth of the link. Also links are targeted with the rrds. These targeting rrd will make sure the data is updated at regular interval of time. Now on clicking NC1cc we are redirected and we can a network map of the the switches connected to NC1cc.When we click on any link we can see the graphs of in/out traffic at that interface.

The significance of this module was to achieve the objective of Visualization of network at a glance and on-clicks of users. This objective has been successfully obtained by this module. Now if there will be a link down or abnormal traffic flow at any interface will be viewable by the Network Administrator and he can easily identify the faulty links. He may then reconfigure the switches or redesign the network.

The graph on clicking on a link between Hostel1 and GuestHouse. It shows the In and Out traffic on the link.The graph clearly shows the In and Out traffic of the interface along with the Last Bandwidth Out to be 199.99 K bps precisely and In bandwidth to be

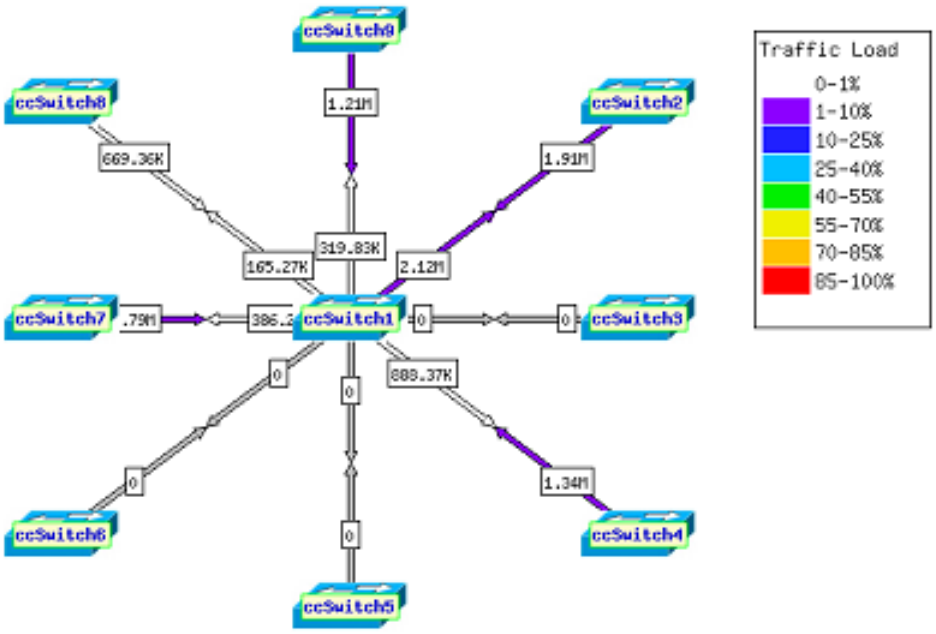


Figure 6.2: Map of switch Network at NC1cc

7.99 K bps. This is obtained by graphing the RRD which updates itself every 5 minutes sending SNMP ifInOctetcs and ifOutOctets requests.

Figure 6.3: graph of the IN/Out traffic between Hostel1 and Guest House

6.1.2 Graphing

This is the module of the layer 3 in architecture of our Network monitoring system. It takes data from Round Robin database which in layer 2 and polls from the polling module in layer 2. This module has been of great importance as the main objective to network monitoring is the graphical representation of the network metrices and successfull archival of the important graphs. These can be filled from last day, week or last month even from last year. The graphs below is the graph obtained from the Round Robin Database which

is filled by the procedure explained in the rrdtool methodology explained in chapter 5. Also We can view bar graphs of CPU usage and RAM usage in Real-Time. Bellow figure shows snapshot of the same. These bar charts are showing the statistics of CPU and RAM usage in beautiful Bar charts which are easy to understand.

We can see graph memory in last day, last week , last month and last year. A graph

Figure 6.4: CPU and RAM Usage Bar graph

of each is shown below. We have used the methodology explained in chapter 5 to graph and define the Line, Area of the graphs.

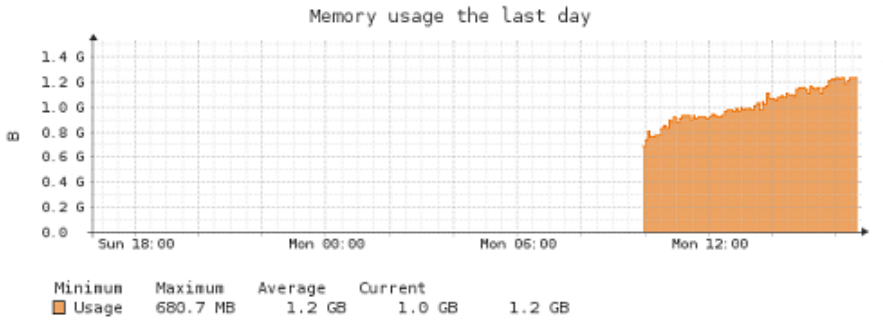


Figure 6.5: Memory Utilization Of The Server Last Day

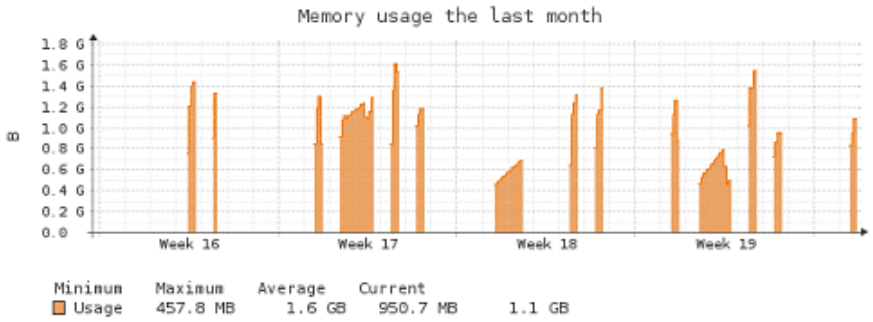


Figure 6.6: Memory Utilization Of The Server Last Month

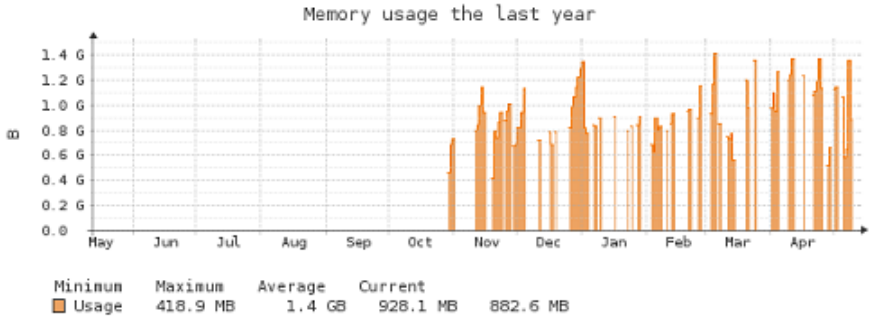


Figure 6.7: Memory Utilization Of The Server Last Year

6.1.3 Statistics

Here user has to just type the IP Address and community string, and click on the hyperlink interface Number. This interface hyperlinks are obtained by a script written in PHP. When the user clicks on the hyperlink only the statistics of that interface is brought on user interface. Also the graph of in and out traffic is viewed. This statistics is obtained from a script written in PHP which brings the raw statistics in a tabular format by querying using net-SNMP querying. As the importance of statistics explained in earlier chapters we will see a tabular representation of the Interface configuration.

Time to Live:	INTEGER: 64
Maximum Fragment reassembly timeout:	INTEGER: 0 seconds
Ip address of this entry:	10.10.4.37
Unique value that identify this entry:	
Subnetmask of this entry:	

Figure 6.8: Interface Configuration Information

6.1.4 Alarming

User can add new servers and services to be monitored and add users to be notified if those servers are down by sms or email and log status. This module has most important feature to detect fault and alert the Administrator. This module justifies the objective to send alerts via Email. In case of a Service/Server being down it will notify by sending emails and also logging the event. A snapshot of its logging ability is shown below

Server	Message	Date
updptest (10.10.2.55:80)	Server 'updptest' is DOWN: ip=10.10.2.55, port=80. Error=No route to host	16:30:03 12-05-14
Gmail SMTP (smtp.gmail.com:465)	Server 'Gmail SMTP' is RUNNING: ip=smtp.gmail.com, port=465	16:30:03 12-05-14
IPR1 (10.10.1.1/24:143)	Server 'IPR1' is DOWN: ip=10.10.1.1/24, port=143. Error=php_network_getaddresses: getaddrinfo failed: Name or service not known	16:30:03 12-05-14
Mail (mail.ipr.res.in:25)	Server 'Mail' is DOWN: ip=mail.ipr.res.in, port=25. Error=Connection refused	16:30:03 12-05-14
SourceForge (http://sourceforge.net/index.php:80)	Server 'SourceForge' is RUNNING: ip=http://sourceforge.net/index.php, port=80	16:30:03 12-05-14

Figure 6.9: Logs Generated

6.1.5 Case Study: Denial of Service Attack

CaseWe study the Denial Of Service attack and detection of the same using a SNMP based Network Monitoring System.

Objective We will see how our SNMS helps in detection of the attack and Visualization of the network by just monitoring the traffic and ping statistics of the switches used to design the network. Also our objective of Collecting Historic Information For Base-lining And Trending Purposes can be fulfilled or not. We will monitor the network and try to get some interesting results. Below diagram shows the network design of the experiment.

- We design a network of three switches connected to each other, say Switch A, Switch B and Switch C.
- We connect these switches to an external switch which is connected to 2 workstation , one of which is a server for our Network Monitoring System , here it is SNMS (SNMP based Network Monitoring System).
- Now we monitor the switches by generating a graph of In/Out traffic on the interfaces of those switches.

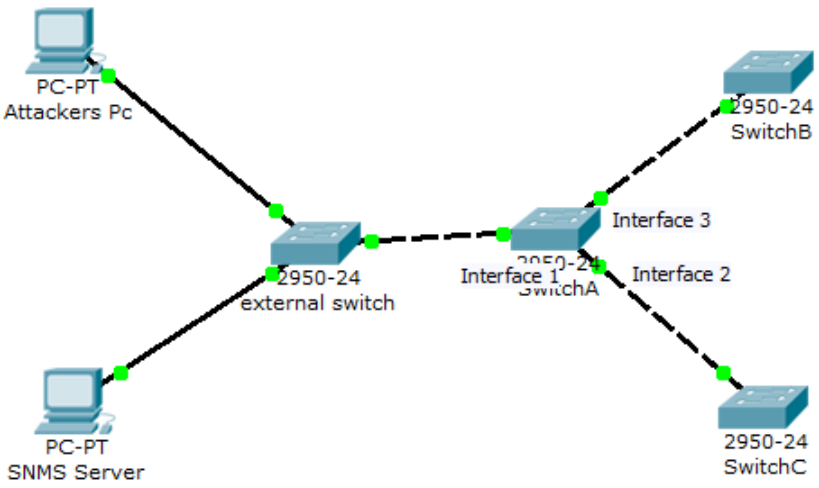


Figure 6.10: Graph showing Ping Latency of a Switch

- We generated a lot of traffic by TCP flooding on the switch B so as to do a DOS attack on it.
- We will see how Network Monitoring system can point towards such attacks also. For this we will see the Traffic graph of the switch before and after the interval of the attack.

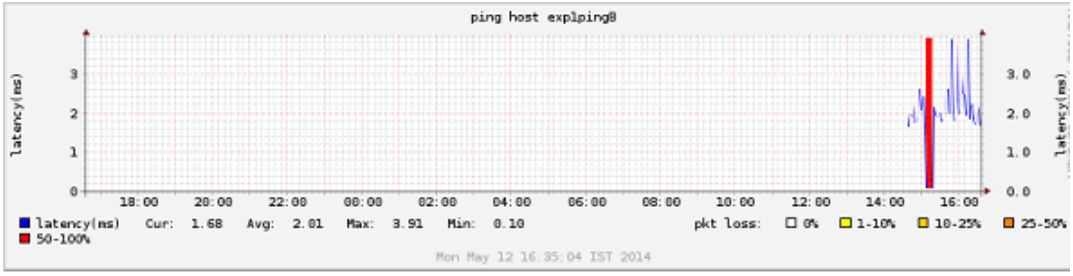


Figure 6.11: Graph Showing Ping Latency Of SwitchB

Result 1 : The above figure is a graph showing ping statistics of a switch which was down nearing 3pm. This is understood because the Red bar shows that there was 50-100 packet loss. The Monitoring Server was trying to ping but it was unavailable. Latency was 3.91 to ping the device.

Result 2 : We can see some more interesting results. We have connected SwitchA to the external network at interface 1 and to Switch B at interface 3. We can see in the graph of Switch A at interface1, its Intraffic is nearly 11 Mbps but at the time of attack

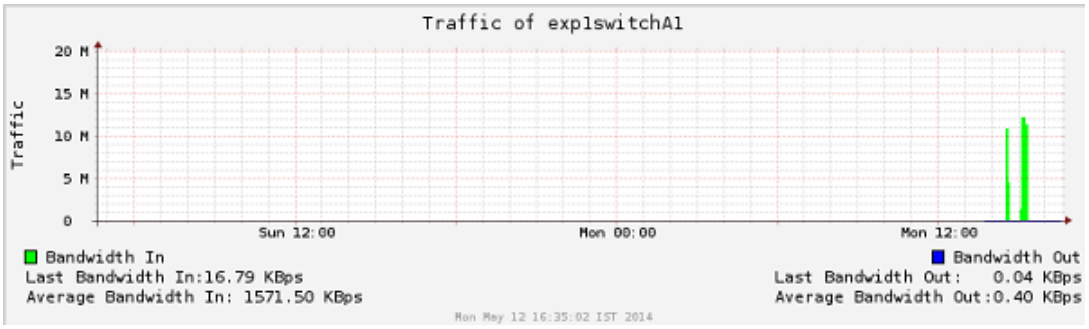


Figure 6.12: Graph Showing In/Out Traffic Of Switch A At Interafce1

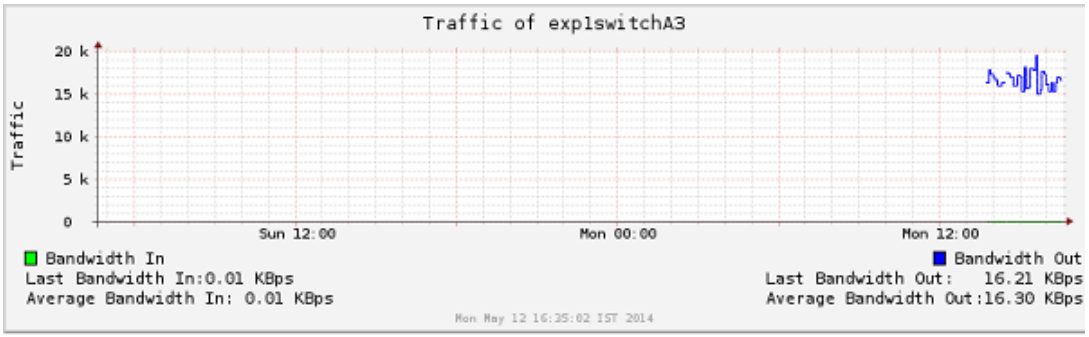


Figure 6.13: Graph Showing In/Out Traffic Of Switch A At Interafce3

, the graph is empty, the SNMS server is unable to send packets at the interval of time when DOS attack was done on SwitchB. This shows the SNMP get Request to graph was unable to get the SNMP reply at the time of DOS attack. Also the next graph which shows traffic of Switch A at interface 3. We can see the Out traffic only. Because the traffic from external network comes to Switch B passing from Switch A.

Chapter 7

Conclusion

This chapter shows the resolved Issues conclusion and future Scope of the project

7.1 Issues Resolved

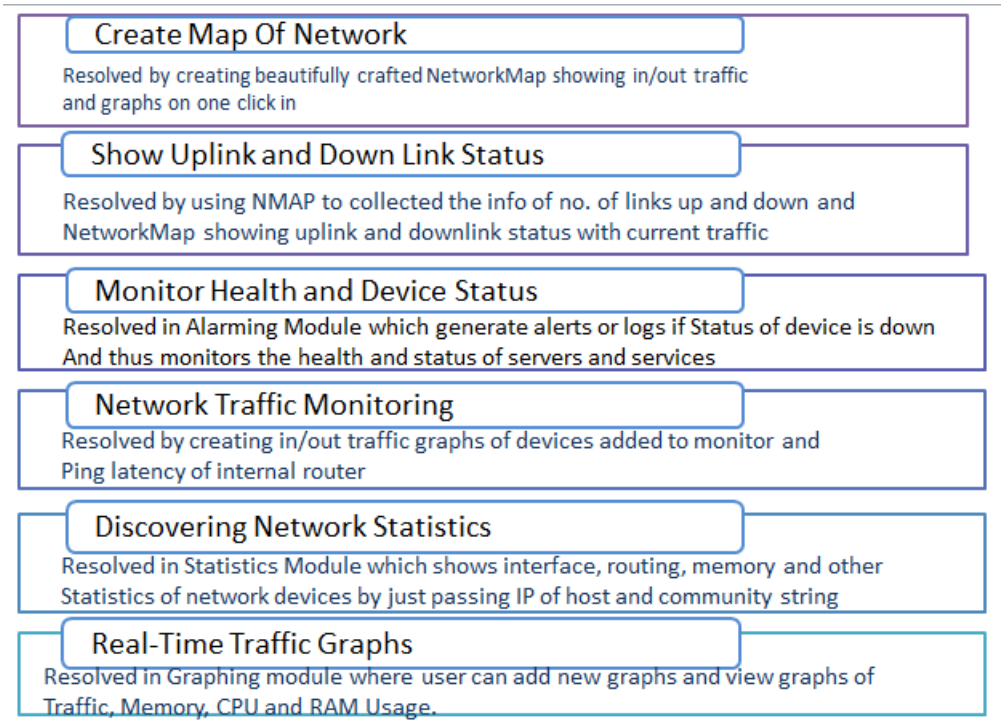


Figure 7.1: Issues Resolved

7.2 Conclusion

- Considering the features of SNMP like flexibility and simplicity and less load, A SNMP based Network monitoring system is designed which supports ubiquitous access.
- By querying the network devices from time to time graphs can be plotted for easy understanding of traffic trend.
- Real-time visualization of graphs can be added of disk usage, memory usage, logged in users and ping latency.
- Real-time Bar graphs showing CPU and RAM Usage of the device on oneclick is possible.
- NetworkMap shows underlying Network Design at a glance with link status and in/out traffic. Also in time of flaws the NMS can send alerts to users in the form of SMS and E-mail.
- In case of loop or any such problem NA can sit on his place and check the device statistics and also can store Ping Latency of important devices like Routers.
- Status of critical switches along with the number of interfaces up and down
- Alerts in case of Server/ Service going down.

7.3 Limitations

- The framework which we have designed for SNMP based Network Monitoring system keeps its Network Monitoring system on a centralized server. All the querying is done from that server itself in a LAN network. What if the network is WAN, In such a network this framework will not be able to monitor the whole picture of network. What if the network is distributed and at different sites, In such environment there would be a need of Distributed Network Monitoring System.
- Nowadays organizations have started adding wireless devices to network a lot. These wireless devices create a IEEE 802.11 wireless networks. In an organiza-

tion such a network needs monitoring. SNMP is capable of monitoring such a network. We have not added wireless devices in our objective to be monitored.

- Our project deals with only the network monitoring and not the Network Management. We have used only SNMP get commands and querying is done from time to time to retrieve graphs. But there is no way where user can set the OId which are READ/WRITE Oids for example System Information like System Name, Location. These information needs to be configured by the Network Admin at the time of setting up a new device. SNMP allows this as its name suggests it is Simple Network Management Protocol.

- Implement SNMPTrap in the Alarm module is not done because of constraints that devices are not configured to support this feature.

7.4 Future Scope

- SNMP based Distributed Network Monitoring.

- SNMP based Network Monitoring of Wireless devices.

- Network Management using SNMP.

Appendix A

SNMP Man Page

OPTIONS:

-h, –help display this help message

-H display configuration file directives understood

-v 1—2c—3 specifies SNMP version to use

-V, –version display package version number

SNMP Version 1 or 2c specific

-c COMMUNITY set the community string

SNMP Version 3 specific

-a PROTOCOL set authentication protocol (MD5—SHA)

-A PASSPHRASE set authentication protocol pass phrase

-e ENGINE-ID set security engine ID (e.g. 800000020109840301)

-E ENGINE-ID set context engine ID (e.g. 800000020109840301)

-l LEVEL set security level (noAuthNoPriv—authNoPriv—authPriv)

-n CONTEXT set context name (e.g. bridge1)

-u USER-NAME set security name (e.g. bert)

-x PROTOCOL set privacy protocol (DES—AES)

-X PASSPHRASE set privacy protocol pass phrase

-Z BOOTS,TIME set destination engine boots/time

General communication options

-r RETRIES set the number of retries

-t TIMEOUT set the request timeout (in seconds)

Debugging

-d dump input/output packets in hexadecimal

-D[TOKEN[,...]] turn on debugging output for the specified TOKENs

(ALL gives extremely verbose debugging output)

General options

-m MIB[:...] load given list of MIBs (ALL loads everything)

-M DIR[:...] look in given list of directories for MIBs

(default: HOME/.snmp/mibs:/usr/local/share/snmp/mibs)

-P MIBOPTS Toggle various defaults controlling MIB parsing:

u: allow the use of underlines in MIB symbols

c: disallow the use of "–" to terminate comments

d: save the DESCRIPTIONs of the MIB objects

e: disable errors when MIB symbols conflict

w: enable warnings when MIB symbols conflict

W: enable detailed warnings when MIB symbols conflict

R: replace MIB symbols from latest module

-O OUTOPTS Toggle various defaults controlling output display:

0: print leading 0 for single-digit hex characters

a: print all strings in ascii format

b: do not break OID indexes down

e: print enums numerically

E: escape quotes in string indices

f: print full OIDs on output

n: print OIDs numerically

q: quick print for easier parsing

Q: quick print with equal-signs

s: print only last symbolic element of OID

S: print MIB module-id plus last element

t: print timeticks unparsed as numeric integers

T: print human-readable text along with hex strings

u: print OIDs using UCD-style prefix suppression

U: don't print units

v: print values only (not OID = value)

x: print all strings in hex format

X: extended index format

-I INOPTS Toggle various defaults controlling input parsing:

b: do best/regex matching to find a MIB node

h: don't apply DISPLAY-HINTs

r: do not check values for range/type legality

R: do random access to OID labels

u: top-level OIDs must have '.' prefix (UCD-style)

s SUFFIX: Append all textual OIDs with SUFFIX before parsing

S PREFIX: Prepend all textual OIDs with PREFIX before parsing

-L LOGOPTS Toggle various defaults controlling logging:

e: log to standard error

o: log to standard output

n: don't log at all

f file: log to the specified file

s facility: log to syslog (via the specified facility)

Appendix B

RRD- Round Robin Database

RRDtool assumes time-variable data in intervals.These interval are of certain length. This interval, is named as step, and specified upon creation of an RRD file whcih cannot be changed afterwards. Because data may not always be come at just the right time, RRDtool will automatically interpolate any submitted data. This is done to fit its internal time-steps.

RRD Database vs Linear Database

Usually in a round-robin database (RRD), time-series data like network bandwidth, memory usage, CPU load etc. are stored. The data is stored so that system storage footprint remains constant over time. This actually avoids resource-expensive purge jobs. Also it reduces complexity. MySQL does NOT provide any such kind of storage engine. RRD tool has also the ability to create and feed this database. RRDTool stores data; that makes it a back end tool. The RRDTool command set allows the creation of graphs, that makes it a front end tool as well. Other databases just stores data and can not create graphs.

RRD's DataStructure

In case of linear databases, new data gets appended at the bottom of the database table. So its size keeps on increasing, but the size of an RRD Tool database is determined at time of creation. Suppose RRD database is a perimeter of a circle. Data is added along the perimeter and when new data reaches the starting point, it overwrites existing data. This way, the size of an RRD Tool database always remains constant. The name Round

Robin stems from this attribute.

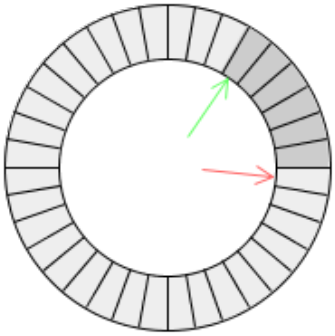


Figure B.1: RRD's data structure

RRD's Data Storage

The value for a specific step, that has been interpolated, is named as a Primary Data Point[14] (PDP). Multiple PDP's may be consolidated according to a Consolidation Function (CF) to form a Consolidated Data Point (CDP)[22]. Typical consolidation functions are average, minimum and maximum.

After the data have been consolidated, the resulting CDP is stored in a round-robin archive (RRA)[22]. A Round-Robin archive stores a fixed number of CDPs and specifies how many PDPs should be consolidated into one CDP and which CF to use. The total time covered by an RRA can be calculated as follows.

$$\text{time covered} = (\#\text{CDPs stored}) * (\#\text{PDPs per CDP}) * \text{steps}$$

Functioning Of RRD

Using the functions below we can create, update, restore, dump etc the rrds.

Functions Used By RRD Tool

1. **create** Sets a new Round Robin Database (RRD).
2. **update** It stores new data values into an RRD.

3. **updatev** It is equivalent to update operationally except for output. It stores output in dev form.

4. **graph** It creates a graph from data stored in one or several RRDs. It uses DEF, CDEF, GPRINT and AREA like functions to make beautiful and colorful graphs .

5. **dump** It dumps the contents of an RRD into plain ASCII. In connection to this with restore so we can use this to move an RRD from one computer architecture to another.

6. **restore** It restores an RRD in XML format to a binary RRD. Helps when any rrd is lost.

7. **fetch** Fetch gets data for a certain time period from a RRD. The graph function uses fetch to retrieve its data from an RRD.

8. **rrdresize** RRDResize changes the size of individual RRAs. This is dangerous. But similar to typecasting in C.

Data Acquisition

When monitoring the state of a system, it is convenient to have the data available at a constant time interval to ensure a constant data flow to update the RRD Tool database. Unfortunately, we may not always be able to fetch data at exactly the time we want to. Therefore RRD Tool lets us update the log file at any time we want. It will automatically interpolate the value of the Data-Source (DS)[22] at the latest official time-slot (interval) and write this interpolated value to the log. The original value we supplied is stored as well and is also taken into account when interpolating the next log entry.

Consolidation(CF)

We may log data at a 1 minute interval, but might also be interested to know the development of the data over the last year. So we can do this by simply storing the data in 1 minute intervals for the whole year. While this would take considerable disk space it would also take a lot of time to analyze the data when we wanted to create a graph covering the whole year. RRD Tool offers a solution to this problem through its data consolidation feature. When setting up an Round Robin Database (RRD), we can define at which interval this consolidation should occur, and what Consolidation Function (CF[22]

should be used to build the consolidated values. We can define any number of different consolidation setups within one RRD. They will all be maintained on the fly when new data is loaded into the RRD. There are four types of consolidation function (CF).

AVERAGE	Average	Take the arithmetic average of the collected values
LAST	Last read value	Take the last collected value
MIN	Minimum read value	Take the smallest collected value
MAX	Maximum read value	Take the highest collected value

Figure B.2: Types of Consolidation Functions (CF)

Round Robin Archives (RRA)

Data values of the same consolidation setup are stored into Round Robin Archives (RRA). This is a very efficient manner to store data for a certain amount of time, while using a known and constant amount of storage space.

For example: If we want to store 10000 values in 5 minute interval, we will allocate space for 10000 data values and a header area using RRD Tool. It will store a pointer telling which slots (value) in the storage area was last written to in the header. New values are written to the Round Robin Archive in, a Round Robin Manner. This automatically limits the history to the last 10000 values (in our example). We can define several RRAs within a single RRD, we can setup another one, for storing 750 data values at a 2 hour interval, for example, and thus keep a log for the last month or last year at a lower resolution.

RRD does not grow over time because RRA guarantees it, and that old data is automatically eliminated. By using the consolidation feature, we can keep data for a very long time, while gradually reducing the resolution of the data along the time axis.

Unknown Data

Sometimes it happens that no new data is available when a value has to be written to the RRD. Data acquisition is not always possible for one reason or other. With RRD Tool one can handle these situations by storing an "UNKNOWN" value into the database. The value 'UNKNOWN' is supported through all the functions of RRD Tooll. When we

are consolidating a data set, the amount of "UNKNOWN" data values is accounted to and when a new consolidated value is ready to be written to its Round Robin Archive (RRA), a validity check is performed to make sure that the percentage of unknown values in the data point is above a configurable level. If not, an "UNKNOWN" value will be written to the RRA.

Graphing

RRD Tool allows us to generate reports in numerical. Also reports in graphical form can be generated based on the data stored in one or several RRDs. The graphing feature is fully configurable. Size, color and contents of the graph can be defined freely using DEF, CDEF, AREA functions. We can do this by using rrdgraph function of RRD Tool.

Nature of Data

In rrd database the tables are stored in separate file(A table may have different Columns).RRD tool allows to consolidate data as it becomes older.

- RRD tool stores data in a binary file. It has dump function,so we can dump data into an xml file , where we can see data.
- It has a fixed size rotating storage.
- It keeps data constant on-disk Size ie., No temporary files.
- The data in the database does not require any maintenance.
- It does on the fly consolidation using consolidation function(CF: Average, Min, Max,Last)

Bibliography

[1] D. Harrington, R. Presuhn, B. Wijnen. "RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks" , IETF, December 2002.

[2] M. Rose, K. McCloghrie. "RFC 1155: Structure and Identification of Management Information for TCP/IP-based Internets" , IETF , May 1990

[3] Ranganai Chaparadza," On designing SNMP based monitoring systems supporting ubiquitous access and real-time visualization of traffic flow in the network,using low cost tools", Jounal 13th IEEE International Conference on Networks,2005

[4] Authors Zeng, Wenxian Wang, Yue " Design and Implementation of Server Monitoring System Based on SNMP", International Joint Conference on Artificial Intelligence, Jounal 2009

[5] Paul Moceri, "SNMP and Beyond: A Survey of Network Performance Monitoring Tools"

[6] Chakchai Netphakdee, Chinnakorn Wijitsopon, Kasidit " Web-based Automatic Network Discovery / Map Systems",Issue Iccaie ,Year 2011.

[7] Paul Simoneau," SNMP Network Management" ,1999 .

[8] Douglas R.Mauro and KevinJ.Schmidt, "Essential SNMP",Book by OREILLY,2009.

[9] W. Stallings," SNMP, SNMPv2, and RMON: Practical Network Management, MA Addison-Wesley, 1996.

[10] William Stallings," SNMP and SNMPv2: The Infrastructure for Network Management",IEEE Communications Magazine, March 1998

[11] M. Rose," The Simple Book: An introduction to Network Management" 3rd ed., Upper Saddle River, NJ: Prentice Hall, 1996.

[12] Moceri, Paul,"SNMP and Beyond : A Survey of Network Performance Monitoring Tools", White paper

[13] Networks, Asante, "SIMPLE NETWORK MANAGEMENT PROTOCOL",Volume 1, RFC 1157,year 2005

[14] Cuddletech TekRef Series, "Getting Started with RRDtool"

[15] Dave Josephen, " iVoyeur :Changing the Game", White paper, Dec 2011.

[16] LaBarre, L., "Structure and Identification of Management Information for the Internet", IETF, Network Information Center, SRI International, Menlo Park, California, April 1988.

[17] Net-SNMP Home Page: http://www.net-snmp.org/

[18] The Apache H'lTP Server: http://www.apache.org/

[19] JavaScript Programming: articles from http:/www.javascript.com/

[20] Perl Programming Language: http://www.perl.com/

[21] A Brief Tour of the Simple Network Management Protocol,CERT Coordination Center

[22] RRD tool Home Page : http://oss.oetiker.ch/rrdtool/

[23] http:// www.juniper.net

[24] www.network-weathermap.com

[25] http://phpservermon.neanderthal-technology.com

[26] http://forums.nas4free.org