



Optimization of PSWAN in Terms of Cost and Bandwidth

Aadil Gani Ganie^{a*}

^a Pondicherry University, India

Keywords :

Optimization,
Bandwidth, Routing
Protocols, Networking
Monitoring, OPNET

Abstract : PSWAN is an internetworking project undertaken by Govt. of India at Pondicherry. It covers a vast area, under it there are various state headquarters and district headquarters. Approximately 3000 systems are using its internet services. Since the number of systems are more and the bandwidth required is less so optimization was needed. Optimization was required without hardware modifications, so we defined some of the parameters through which we can achieve the optimization of this network, these parameters are 1. Type of protocol 2. Type of Topology 3. Access policies 4. Load balancing 5. Traffic bottle neck 6. Bandwidth utilization. To make the network cost effective, some small networks were moved to broadband network so that bandwidth usage can be mitigated and consequently network will get optimized. Since this project (PSWAN) is using the CISCO devices only so it was easy to simulate the network, we used OPNET simulator as it is precise than other simulators. First the operational network was simulated and then the proposed one, proposed model showed evident positive results. The simulation tool used is Opnet. OPNET is extensive and powerful simulation software with wide variety of capabilities. It enables the possibility to simulate entire heterogeneous networks with various protocols [1]

1. Introduction

Network optimization refers to a set of technologies and techniques that are geared towards improving network performance. Network optimization techniques seek to creatively manage bandwidth utilization, minimize latency, packet loss, congestion and jitter.

Network optimization tools or simply network optimizers allow network engineers to monitor and optimize network performance metrics. Network optimizers provide an unprecedented level of control over performance metrics, and the ability to proactively manage network performance.

Network performance metrics are network attributes that point to the health of a network. Network performance metrics like latency, packet loss, jitter, congestion and bandwidth availability are crucial to end user experience. For example, Network latency determines application specific performance metrics like page load times, VoIP call quality, video buffering times and online gaming lag times. Packet loss leads to online games losing frames and jumping

around. Jitter results in cutoffs during VoIP calls.

Historically, network optimization has been a one trick pony. Most current network "optimization" tools are that in name only. They can more accurately be defined as network monitoring platforms, which while providing visibility into network performance, do not provide much functionality in the way of optimizing or controlling network performance.

Network optimization tools tend to be reactive in nature and require manual changes to network topology to affect performance.

Network optimization has always been a core problem domain in operations research, as well as in computer science, applied mathematics, and many fields of engineering and management. The varied applications in these fields not only occur 'naturally' on some transparent physical network, but also in situations that apparently are quite unrelated to networks. Moreover, because network optimization problems arise in so many diverse problem contexts, applications are scattered throughout the literature in

* Corresponding authors
e-mail addresses : ganieaadi195@gmail.com

several fields. Consequently, it is sometimes difficult for the research and practitioner community to fully appreciate the richness and variety of network applications [2].

PSWAN project is currently serving a large number of user and provide them the internet facilities which includes email, file sharing, printing etc. as well as internet services like video conferring, e-billing etc., so considering all above parameters in mind the uploading and downloading demand increases manifold which subsequently demands more bandwidth which of course is an important parameter in any computer networks or in any other communication network. We did an extensive study on existing network be it a topology, protocols, bandwidth, access policies etc. the resultant or observatory study shows that there are some parameters which upon modification will show the better results. After simulating the both networks it has been observed that existing network can show the better performance if some of its parameters will be changed or modified.

2. Literature Review

In recent years bandwidth consumption has become an increasing concern for most of organizations as bandwidth intensive sites and video steaming have become more and more popular. However, understanding the current Internet environment is challenging due to the complexity of Internet applications. In fact, there is no simple way to truly understand the network's behaviors [3]. There are various parameters which contribute to network optimization and performance, these parameters with their brief description will be discussed in this section

1. Bandwidth

Bandwidth utilization is an important factor to improve the network performance. For the effective utilization of bandwidth, pathloss rate and latency should be measured. So that the application can adapt its send rate to the estimated bandwidth. In a college campus network, since many users must share the common bandwidth capacity on the network, there will be a situation in the network where the demand is beyond the capacity. This causes network congestion and has negative effect on the data transmission rate, bandwidth utilization and quality. The most important part of the network is to plan forwarding of data with equal priority, independent on the source and destination. Hence, there is no trivial technique to assure a certain transmission rate [4]. The two common types of techniques to measure available bandwidth and latency are passive and active techniques [5].

A. Passive measurements

Constantinos Dovrolis et.al explains passive measurement techniques may be an attainable strategy to measure network characteristics, like the

available bandwidth and latency [6]. Passive measurement techniques and tools act as observers within a network and generally they will not interfere with any other traffic [7]. These techniques most frequently need control and administrative privileges of the underlying network infrastructure for accessing routers and servers within the network. E.g.: MRTG, IPMON.

B. Active measurements

Instead of using above techniques, we can implement active measurement techniques. In active measurement technique probe traffic is injected into the network at a traffic source and the network's impact is measured at a probe traffic receiver [8]. Therefore, active measurement techniques have an effect on the network traffic itself, conflicting to the passive measurement technique. The active measurement access two hosts, one is the traffic source and other is a traffic receiver. Such techniques are referred to as end-to-end measurement techniques [5].

2. Throughput: - number of messages transmitted per unit time is called throughput. Throughput depends on bandwidth, signal to noise ratio and hardware limitations. Time window is the period over which the throughput is measured.
3. Latency: - latency means delay in the network.
4. Jitter: - the difference in packet delay is called jitter. jitter is measuring time difference in packet inter-arrival time
5. Error rate :- The degree of errors encountered during data transmission over a communications or network connection

Routing Protocols

Choosing the right protocol for any network is very difficult. A routing protocol must not be Configured if factors like complexity of network, multiple vendor devices and future expansion in the network are not thoroughly investigated [9]. Different static and dynamic routing options are available [10]. The chief advantage of dynamic routing over static routing are scalability and adaptability dynamically routed network can grow more quickly and larger, and is able to adapt to changes in the network topology brought about by this growth or by the failure of one or more network components [1]. Routing Information Protocol (RIP), Interior Gateway protocol (IGRP), Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) are examples of some of dynamic routing protocols. Every protocol assigns a parameter value to all available paths to reach to destination network [11]. Simulation-based routing protocol performances have been analyzed by [12] which revealed efficiency of EIGRP over RIP which uses single routing metric and exchanges periodic copies of entire routing table which makes the RIP

network congested [13]. The capability of EIGRP to utilize bandwidth efficiently and its knowledge about the entire network using topology table makes EIGRP an efficient routing option in an enterprise network [1].

Networking Monitor

Computer and network administrators are often confused or uncertain about the behavior of their networks. Traditional analysis using IP ports, addresses, and protocols are insufficient to understand modern computer networks. Here we describe NetADHICT, a tool for better understanding the behavior of network traffic. The key innovation of NetADHICT is that it can identify and present a hierarchical decomposition of traffic that is based upon the learned structure of both packet headers and payloads. In particular, it decomposes traffic without the use of protocol dissectors or other application-specific knowledge [14].

Network and systems administrators have a variety of mature tools to select from for counting packets and flows. From open source solutions such as MRTG [15] and FlowScan [16] to large commercial offerings such as HP Openview [17] and IBM Tivoli [18]. We have developed a tool called NetADHICT (pronounced "net- addict") for extracting and visualizing context-dependent abstractions of network behavior. NetADHICT hierarchically decomposes network traffic: for example, observed packets are first divided into IP and non-IP groups, IP packets are then split into TCP and non-TCP, and so on. What is notable about NetADHICT, though, is that its decomposition is automatically derived from observed traffic; in other words, it learns an appropriate context-dependent hierarchical classification scheme automatically with no built-in knowledge of packet or protocol structure [14].

NetADHICT shows great promise in aiding administrators in understanding network behavior. It provides a new way to separate traffic that is normal from "interesting" traffic that an administrator is interested in analyzing. With new ways to visualize traffic and providing a network "weather" map, NetADHICT allows administrators to see the status of their whole network at a glance, while also providing ways to investigate smaller flows of traffic. While Development and testing are ongoing, by acting as a bridge from higher level analysis tools to low level ones, NetADHICT has the potential to improve how administrators manage network resources [14].

3. Simulation and Analysis

Generally there are two kinds of network modelling 1. Analytical modelling and 2. Computer simulation. The first is by mathematical analysis that characterizes a network as a set of mathematical equations. The main disadvantage is one-dimensional

view of the network and incapability to simulate the dynamic nature of a network as nodes join or leave the network. The second type of computer simulation is broadly classified as continuous time simulator (CTS) and discrete event simulator (DES) [9].

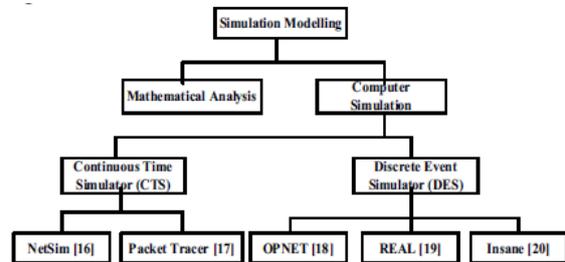


Fig 1. Classification of simulation modelling

There are various tools for simulation it has been observed that OPNET is showing better accuracy and precision as compared to others simulations tools. Since OPNET has been

Used in this project for network analysis and performance issues, we will focus on OPNET in the following section. OPNET provides a comprehensive development environment for the specification, simulation and performance analysis of communication networks [9]. OPNET is extensive and powerful simulation software with wide variety of capabilities. It enables the possibility to simulate entire heterogeneous networks with various protocols [1]. OPNET Modeler is a powerful tool which evaluates the network efficiently and accurately and predicts the network behavior before implementation in real environment [19]. OPNET with its unique approach can provide objective and reliable quantitative basis for network planning and design and it could shorten network construction period, improve the exactitude of decision making on network building and reduce the risk of network construction Investment [20].

Network analysis also known as traffic analysis, protocol analysis, sniffing, eavesdropping and so on is the process of capturing network traffic and inspecting it closely to determine what is happening on the network. A network analyzer decodes the data packets of common protocols and displays the network traffic in readable format. A network analyzer can be standalone hardware device with specialized software, or software that is installed on desktop or laptop computer.

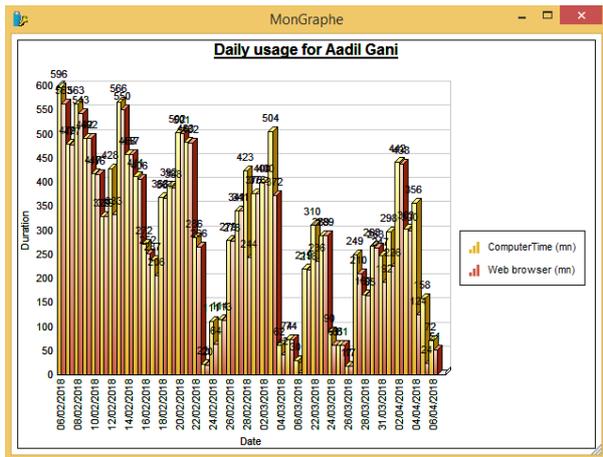
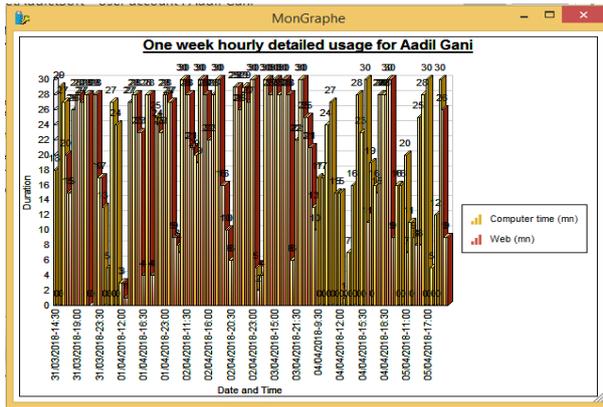


Fig 2. Network analyzer display

Existing Network

PSWAN is an operational network at Directorate of information technology at Pondicherry India. Almost 3000 systems are enjoying the internet services of PSWAN. Since the bandwidth is the main concern in any network same was with this network, number of users are more but the bandwidth required is very less, optimization of network is necessary, in order to optimize the network we pointed out some of the parameters that upon modification or change will provide the better results and subsequently will optimize the network, these parameters are 1. Type of protocol 2. Type of topology 3. Access policies 4. Traffic bottle neck 5. Bandwidth utilization and 6. Load balancing.

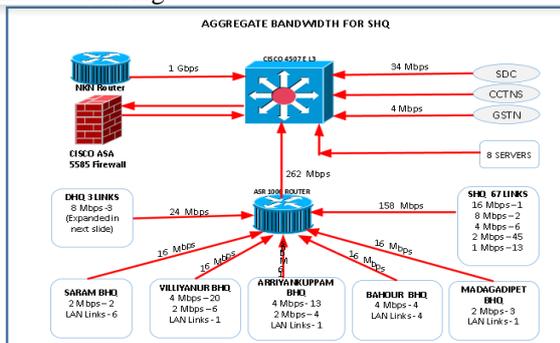


Fig 3. Existing Network

A protocol is the formal definition of external behavior for communicating entities. It defines:

1. Format of PDUs
2. Rules of operation (PDU sent, data delivered, abort)

Examples of protocols are:

1. TCP
2. UDP
3. IP
4. Ethernet

Protocols are connection oriented or connectionless. A connection exists if the communication requires some synchronization of all involved parties before communication can take place. The telephone system is connection oriented: before A can send some information to B, A has to call B (or vice versa) and say "hello". The postal (mail) system is connectionless. If A wants to send

Some information to B, A can write a letter and mail it, even if B is not ready to read it.

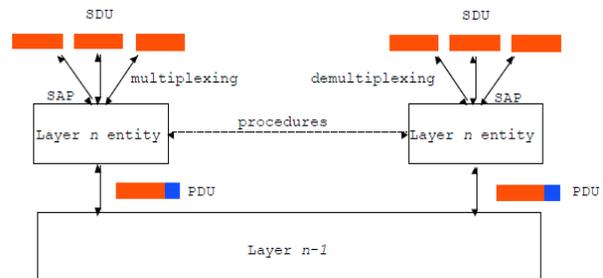


Fig 4. Protocol Architecture

Networking functions are structured as a layered model:

1. Layer n communicates with other layer n entities using layer n PDUs
2. Layer n uses the service of layer n-1 and offers a service to layer n+1.
3. Entities at the same layer are said peer entities
4. Operation rules between peer entities are called procedures

Layering of protocol entities is reflected by the term of a protocol stack. While there is often a "right tool for the job," all routing protocols have their strengths and weaknesses. The different type of protocols are:-

a. RIP V1—Routing Information Protocol

Type of protocol: Distance vector, based on the Bellman-Ford distance vector algorithm
Metric: Hop count

Methodology: Selects routers with the lowest hop count; updates other routers by broadcasting the entire routing table to all routers every 30 seconds

Ideal topology: Smaller networks that aren't very dynamic, have fewer than 15 hops [21]

b. EIGRP—Enhanced Interior Gateway Routing Protocol

Origin: Based only on Cisco's implementation.

Type of protocol: Hybrid distance vector

Metric: Delay, bandwidth, reliability, and load.

Methodology: Sends hello packets every five seconds to neighbors (can interoperate with IGRP) to see if the neighbors are still available; updates other routers by notifying them only when routes change.

Ideal topology: Any network, small to very large; all routers must be Cisco [22].

c. OSPF V2—Open Shortest Path First

[Note that version 1 of OSPF was never implemented.]

Type of protocol: Link-state, runs the Dijkstra algorithm to calculate the shortest-path first (SPF) tree

Metric: Calculates the cost to traverse router links to get to the destination, taking the bandwidth of the links into account

Methodology: Develops adjacencies with its neighbors, periodically sending hello packets to neighbors, flooding changes to neighbors when a link's status changes, and sending "paranoia updates" to neighbors every 30 minutes of all recent link state changes

Ideal topology: Any network, small to very large [23].

Topology can be defined as a geometrically interconnection pattern by which station are connected using suitable transmission medium. There are various types of topologies.

1. Mesh topology: - every device has a dedicated point to point link to every other device. A fully connected Mesh topology has $n(n-1)/2$ physical channels to link n devices.
2. Star topology: - in this topology each device is connected to a central controller called as HUB. The devices are not directly connected to each other as in case of Mesh topology. Dependency on HUB is the main drawback of this topology, if HUB goes down network goes down.
3. Bus topology: - bus topology has a multipoint connection. One long cable acts as a backbone, to which all the devices are connected.
4. Ring topology: - in this topology each device is having dedicated point to point only with two devices on either side of it.
5. Tree topology: - it is an amalgam of Bus and Star topology. It is famous for its scalability and hierarchical communication setup.

PSWAN is currently using star topology, we can go for tree or hybrid which is famous for reliability and scalability.

Access policies: - while observing the existing network, it has been seen that current network is having strict access policies, we cannot further modify them. From 5 pm to 10 pm all the social networking sites get blocked. Currently they are having extended or time based access policies.

Load balancing: - In PSAWN all the networking devices are CISCO devices. All the routers, switches are smart so they are having in-built load balancing, no external load balancer was

needed.

4. Result and Discussion

First of all we simulated the existing network on OPNET software and then simulate the proposed with same parameters. These parameters are taken from global statistics of OPNET. These are:

- a. Email
 - Traffic Received (packets/sec)
 - Traffic Send(packets/sec)
- b. Ethernet
 - Delay (sec)
- c. HTTP
 - Object Response Time (sec)
 - Page Response Time
- d. EIGRP
 - Network Convergence Duration
- e. OSPF
 - Network Convergence Duration

Different_users_EIGRP_DES_1= Proposed network
 Different _users_WITHOUTFIREWALL_DES_1= Existing network

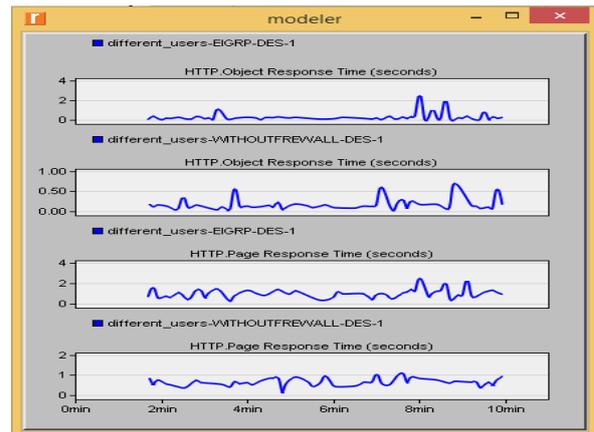


Fig 5. Simulation Result for HTTP

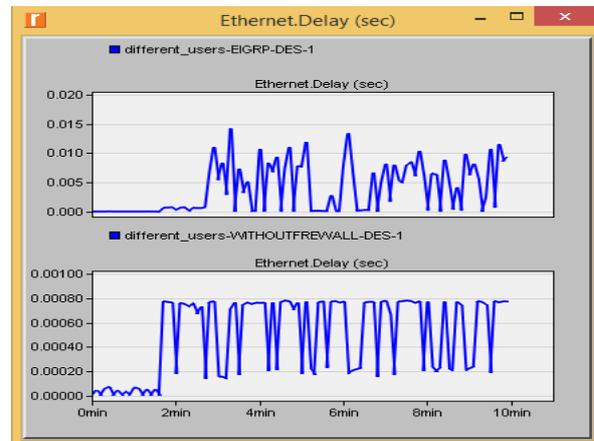


Fig 6. Simulation Result for Ethernet

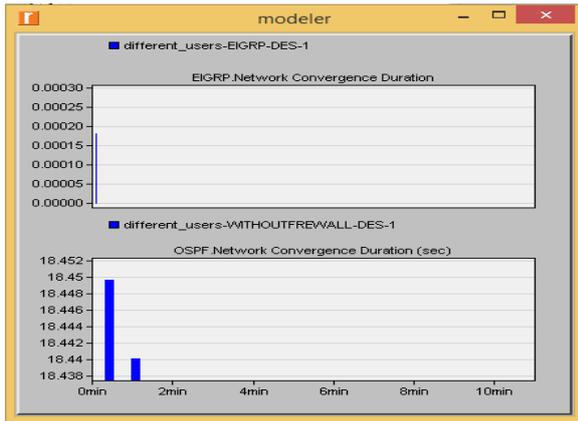


Fig 7. Simulation Result for EIGRP VS OSPF

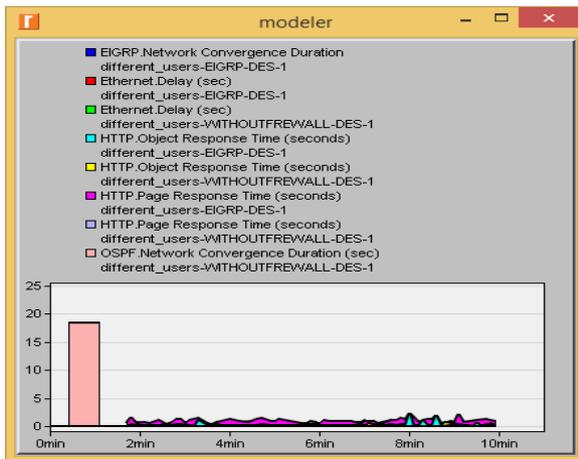


Fig 8. Combined Simulation

It can be observed from simulation that proposed network is performing better than the existing network. If these parameters will be changed in physical network definitely it will show far better results and subsequently we can say that network has been optimized.

5. Conclusion

In this paper a case study of an existing operational network (PSWAN) has been considered. The existing operational network needs to be tuned for better performance. The network performance is heavily dependent on factors like network topology, configuration of network devices and network interface capacity. To optimize the network performance, problems in the existing infrastructure have been identified and after providing appropriate solution new network design has been proposed which overcomes the flaws in the network and enhances network performance. Both existing and proposed network designs have been implemented in OPNET to analyze the results for different performance parameters. The parameters chosen showed better results for proposed network.

6. References

- [1] S. G. Thorenoor, "Dynamic routing protocol implementation decision between EIGRP, OSPF and RIP based on technical background using OPNET modeler," 2nd Int. Conf. Comput. Netw. Technol. ICCNT 2010, pp. 191–195, 2010.
- [2] R. K. Ahuja, T. L. Magnanti, J. B. Orlin, and M. R. Reddy, "Network Models," *Handbooks Oper. Res. Manag. Sci.*, vol. 7, pp. 1–83, 1995.
- [3] Z. Jiang and I. Joe, "Efficient Bandwidth Utilization and Congestion Control through Network Traffic Analysis," pp. 280–283.
- [4] D. M. S and K. N. R. M. Babu, "An Approach to Effective Bandwidth Utilization using Software Define Networking," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 4, pp. 5571–5574, 2014.
- [5] B. Melander, M. Bjorkman, and P. Gunningberg, "Regression-Based Available Bandwidth Measurements," *Int. Symp. Perform. Eval. Comput. Telecommun. Syst.*, pp. 1–25, 2002.
- [6] C. Dovrolis, P. Ramanathan, and D. Moore, "What do packet dispersion techniques measure?," *Proc. - IEEE INFOCOM*, vol. 2, pp. 905–914, 2001.
- [7] M. Jain and C. Dovrolis, "End-to-end available bandwidth: Measurement methodology, dynamics, and relation with TCP throughput BT - ACM SIGCOMM 2002 Conference, August 19, 2002 - August 23, 2002," vol. 32, no. 4, pp. 295–308, 2002.
- [8] C. Dovrolis, P. Ramanathan, and D. Moore, "Packet-dispersion techniques and a capacity-estimation methodology," *IEEE/ACM Trans. Netw.*, vol. 12, no. 6, pp. 963–977, 2004.
- [9] M. A. Shah, G. A. Safdar, C. Maple, and K. Sardar, "Network performance optimization: A case study of enterprise network simulated in OPNET," *Proc. - 2011 9th Int. Conf. Front. Inf. Technol. FIT 2011*, pp. 57–62, 2011.
- [10] Chin-Fu Kuo, Ai-Chun Pang, and Sheng-Kun Chan, "Dynamic Routing with Security Considerations," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 1, pp. 48–58, 2009.
- [11] M. Balasubramanian, L. A. Perkins, S. S. Iyengar, S. Dua, and D. H. Kraft, "Evidence combination for traffic adaptive routing," *Proc. - 18th Int. Conf. Syst. Eng. IICSEng 2005*, vol. 2005, pp. 355–362, 2005.
- [12] G. F. Riley and N. Road, "No Title," no. Riley 2003, pp. 2154–2161, 2006.
- [13] "Cisco." [Online]. Available: <https://www.cisco.com/en/US/docs/Networking/technology/handbook/RIP.html>. [Accessed: 11-Apr-2018].
- [14] H. Inoue, D. Jansens, A. Hijazi, and A. Somayaji, "NetADHICT: A Tool for Understanding Network Traffic," *Lisa*, pp. 39–47, 2007.
- [15] T. Oetiker and D. Rand, "{MRTG:} The Multi Router Traffic Grapher.," *Lisa*, vol. 98, pp. 141–148, 1998.
- [16] D. Plonka, "FlowScan: A Network Traffic Flow Reporting and Visualization Tool," 14th Syst. Adm. Conf. (LISA 2000), pp. 305–318, 2000.
- [17] "Welcome - Micro Focus Software Support." [Online]. Available: <https://softwaresupport.softwaregrp.com/>. [Accessed: 11-Apr-2018].
- [18] "IBM Support - Tivoli supported platforms." [Online]. Available: https://www-01.ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html. [Accessed: 11-Apr-2018].
- [19] V. Kulgachev, M. S. Student, N. Drive, H. Heights, H. Jasani, and D. Ph, "802.11 Networks Performance Evaluation Using OPNET," pp. 149–152, 2010.
- [20] J. Cai and B. Jia, "Network simulation based on OPNET and application," *Proc. 1st Int. Work. Educ. Technol. Comput. Sci. ETCS 2009*, vol. 1, pp. 199–202, 2009.
- [21] "Weblet Importer." [Online]. Available: <http://www.ietf.org/rfc/rfc1058.txt>. [Accessed: 11-Apr-2018].
- [22] "articles - Search Results - TechRepublic." [Online]. Available: <https://www.techrepublic.com/search/?q=articles>. [Accessed: 11-Apr-2018].
- [23] "Weblet Importer." [Online]. Available: <http://www.ietf.org/rfc/rfc2328.txt>. [Accessed: 11-Apr-2018]