IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

# Web Network Statistics Generator and Analyzer

**B. Sivaranjani[1*], M. Priyadharshini[2]**

[1,2]M.Sc Computer Science, Idhaya College for Women, Kumbakonam, Tamilnadu, India

*Corresponding Author: sivaranjani20@gmail.com*

**Available online at: www.ijcseonline.org**

***Abstract*—**This project **"Web Network Statistics generator and analyzer"** has been developed to provide the better security mechanism for intranet services and reporting. There are a range of functions and reports that provide extensive information on complete process of official mail management and file blocker for different set of users those who are logged into this system. It also handles website status and produce a modification guides. This web tracking system is developing by using the **PHP** as front end with **SQLSERVER** as back end. The project consists of various modules such as admin, user, registration, web upload, web user monitoring, file transfer watcher, Email blocker. It verifies the hidden images and verifies links & URL's Connections. It includes the secured gateway system for the entire server system and transactions performing on the process based actions with perspective to the web product development. This system has a range of functions and reports that provide extensive information on all website status and produce a modification guides. This system is platform independent and can be used by any kind of learner. It is designed with robust and easy to implement in any network places. It is highly scalable and provides the feasible updates to make this project efficient and handle by any kind of user.

***Keywords*—web network, statistics, generator, gateway, file blocker.**

## I. INTRODUCTION

A **network analyzer** is an instrument that measures the network parameters of electrical networks. Today, network analyzers commonly measure parameters because reflection and transmission of electrical networks are easy to measure at high frequencies, but there are other network parameter sets such as y-parameters, z-parameters, and h-parameters. Network analyzers are often used to characterize two-port networks such as amplifiers and filters, but they can be used on networks with an arbitrary number of ports.

Network analyzers are used mostly at high frequencies; operating frequencies can range from 5 Hz to 1.05 THz. Special types of network analyzers can also cover lower frequency ranges down to 1 Hz. These network analyzers can be used for example for the stability analysis of open loops or for the measurement of audio and ultrasonic components.

The Internet is today a network of incredible complexity, connecting systems that are heterogeneous for technologies and applications. Consequently, multiple types of objects and data – at different abstraction-levels – impact network workload, whose inherent complexity is further increased by its temporal evolution, coherently with the evolution of topologies, devices, network technologies, applications, and traffic. Internet workload is therefore the result of a complex mix of sources and it is quite different from the workload that was observed on large networks in the past years. For these reasons, understanding, modeling, and generating network workload are diffi- cult and challenging tasks.
Agilent offers a variety of vector network analyzers with frequency, performance, and versatility to meet your measurement needs. To help you determine which solution is right for you, this selection guide provides an overview and side-by-side comparison of all our network analyzers. In addition, you will find typical network analyzer applications, the measurement needs for those applications, and how Agilent's network analyzers meet those needs.

Agilent network analyzers can be used to characterize and test active components, such as amplifiers, mixers, and frequency converters. They can easily measure commonly specified amplifier parameters such as gain, gain and phase compression, isolation, return loss, and group delay. Harmonic distortion is often used to understand an amplifier's nonlinear behavior, and requires the receiver to be tuned at a different frequency from the source. Frequency-translating devices, such as mixers and frequency converters present unique measurement challenges because their input and output frequencies are different. Network analyzers used for testing these devices need to have a frequency-offset mode (FOM) to detect output frequencies different from the input. Additional instruments and signal conditioning devices may be required for testing with two-tone, higher input and output power, or for other types of measurements including noise figure, ACPR, and EVM. As a result, the test system becomes complicated or requires multiple stations.

Network analyzer measurements made in the field are fundamentally similar to measurements in the lab—users need to test S-parameters of devices such as cables and filters to determine their performance. The main difference is the requirements placed on the network analyzer hardware. Portability is a big challenge in the field. Carrying benchtop instruments on a cart or trying to fit a benchtop instrument in a tight space like an aircraft is difficult. Locating AC power can also be difficult, so a portable and battery-operated analyzer is often vital for field test. In addition, while indoor temperatures may be fairly stable, the weather conditions outdoors are quite variable, so the equipment has to be designed to handle these changes. Any VNA used outdoors also has to be rugged, as it is moved around often. Finally, the measurements made in the field need to match the measurements made in the lab, and have similar accuracy.

Generation of network workload is a fundamental component of several networking research fields: performance of networks and network devices, including middleboxes (e.g., performance enhanced proxies, policy charging and rules function, traffic shapers), security (e.g., firewalls, intrusion and anomaly detection, background and malicious workload), quality of service.The contribution of this paper is twofold. First, we discuss the main features needed for, and the difficulties involved in, the generation of realistic network workload (Section 2). Then, we present a customizable tool for the generation of realistic network workload targeted to emerging networking scenarios that is based on D-ITG and its traffic generation engine [24]. More precisely, we discuss how our tool tackles the main issues challenging the representative replication of network workload (Section 3) and we illustrate its advanced features, which can be used to analyze complex and emerging network scenarios (Section 4). We highlight the design choices we made to integrate in a single and configurable platform (a swissarmy-knife for network workload generation) the discussed main properties, and we illustrate how the solutions we adopted tackle relevant challenges such as the support for different traffic profiles, configurability at multiple layers, scalability, repeatability of experiments, etc.

## II. Related Work

### Realistic network workload generation

In literature a huge amount of work exists on the characterization, modeling and simulation of network workload (e.g., related to e-commerce platforms, live streaming media and YouTube traffic, peer-to-peer file sharing , Web and web caching , malicious and unwanted traffic). Unfortunately, we cannot state the same for the generation of realistic network workload and for the issues associated to this important task. In this work, we focus on the generation of realistic network workload over real networks and using software platforms [19,20]. Approaches for synthetic network workload generation should be able to (i) appropriately capture the complexity of real workload in different scenarios, (ii) customly alter specific properties of such workload for the purpose of the experiment, and (iii) measure indicators of the performance experienced by such workload at network level. In a novel and broader view of realistic network workload generation, towards the implementation of a swiss-army-knife software tool, such objectives could be achieved by combining features already present in literature in various less general approaches, plus adding new specific functionalities. Table 3 shows a (non-exhaustive) list of the platforms that are most used in literature: several powerful platforms exist, each of them with peculiar characteristics, but none of them includes the flexibility,Two main alternative approaches exist in literature for the generation of network workload: (i) trace-based generation (TCPReplay, TCPivo, TCPopera, etc.), in which flows exactly replicate the content and the timings of traffic traces previously collected in real scenarios; (ii) analytical model-based generation (TG, MGEN, RUDE/CRUDE, D-ITG, etc.), in which flow and packet generation processes are based on statistical models. Generation of realistic network workload needs both approaches (as stated in [21] too, in which a simple approach is proposed), depending on the characteristics of the traffic scenario to be replicated. A tool should be able to even combine trace-based and analytical model-based techniques, that is, to generate flows with timings from a trace while filling their packets with configurable content or, viceversa, using content from the trace while inter packet times follow a custom statistical model. Fig. 1 shows the joint use of trace-based and analytical based techniques for different traffic flows. Most workload generators in literature work at either flow level (e.g., [20]) or packet level (e.g., [29,28]), while few of them operate instead at application level (e.g., [41]). Accurate replication of network workload requires the support of both flow-level and packet-level traffic pro- files, with the additional ability to replicate specific traffic properties that are typically chosen by the application, such as, TOS fields (e.g., for experimenting with QoS), protocol ports, and transport-level payload (e.g., for experimenting with security policies, network neutrality, traffic classification). The realistic replication of some scenarios also requires the ability to manipulate headers at a higher protocol level (e.g., support to SIP, RTP). Fig. 1 shows a workload generator able to operate distributedly and to exchange between each source-sink pair several sets of traffic flows with different properties. Moreover, each source or sink is also able to measure performance indicators and to store them locally or remotely. Indeed, besides specifying the characteristics of the traffic to generate, it should be possible to collect measures on the performance experienced by the injected workload. This allows the operator to perform experiments using workload from real applications (i.e. using a pcap trace) and without relying on some external software (e.g., tcpdump + tcptrace) to evaluate network performance parameters such as throughput, latency, jitter, and losses. Fig. 1 contains a list of configurable parameters that it should be possible to separately set for each flow and a set of network-level performance indicators to be measured.

**A Survey of Network Traffic Monitoring and Analysis Tools**

From hundreds to thousands of computers, hubs to switched networks, and Ethernet to either ATM or 10Gbps Ethernet, administrators need more sophisticated network traffic monitoring and analysis tools in order to deal with the increase. These tools are needed, not only to fix network problems on time, but also to prevent network failure, to detect inside and outside threats, and make good decisions for network planning. This paper surveys all possible network traffic monitoring and analysis tools in non-profit and commercial areas. The tools are categorized in three categories based on data acquisition methods: network traffic flow from NetFlow-like network devices and SNMP, and local traffic flow by packet sniffer. The popular tools for each category and their main features and operating system compatibilities are discussed. The feature comparisons on each category are also made.When a network failure occurs, monitoring agents have to detect, isolate, and correct malfunctions in the network and possibly recover the failure. Commonly, the agents should warn the administrators to fix the problems within a minute. With the stable network, the administrators' jobs remain to monitor constantly if there is a threat from either inside or outside network. Moreover, they have to regularly check the network performance if the network devices are overloaded. Before a failure due to the overload, information about network usage can be used to make a network plan for short-term and long-term future improvement There are various kinds of tools dealing with the network monitoring and analysis, such as tools used by Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), Sniffing, and Network flow monitoring and analysis. Given the data packet and network traffic flow information, administrators can understand network behavior, such as application and network usage, utilization of network resources, and network anomalies and security vulnerabilities. In this paper, we survey all possible network traffic monitoring and analysis tools in both public and commercial areas. The organization of this paper is as follows.The link gathers thousands of tools and classifies into eight main groups: Network Monitoring Platforms (NMP), Monitoring Tools Integrated with NMP, Commercial Monitoring Tools not Integrated with an NMP, Public Domain Network Monitoring Tools, Web Tools, Auxiliary Tools to Enable Monitoring, Analysis, Report Creation or Simulation. For commercial network monitoring tools, there are eight subgroups: Analyzer/Sniffer, Application/Services monitoring, Flow monitoring, FTP, Network security, SNMP tools, Topology, and VOIP (Voice Over IP). And fourteen subgroups are classified for public network monitoring tools: Application Monitoring, Finger Printing, FTP (File Transfer Protocol), Mapping, Monitoring Infrastructures, Packet Capture, Path Characterization, Ping, RRDtool (Round Robin Database Tool) , SNMP, Throughput tools, Traceroute.Cisco Systems is a well-known company for enterprise network devices. Cisco Systems was also the first company to develop and sell routers, so the idea of how to retrieve flow information was originally implemented by Cisco Systems. Cisco Systems provides an open but proprietary network protocol running on Cisco IOS (Internetworking Operating System), "Cisco NetFlow", in order to capture network traffic flow information and then send it back to the monitoring hosts. In this section, we describe network traffic flow information from NetFlow-like devices.

## III. METHODOLOGY

- This project shows better solution for websites by its file transfer filter options, loading capacity and cross browser compatibility.
- It provides highly secured and more authorized database system.
- This system gives more importance to user. Using this system the user may come to know the better and quality products to buy over the internet shopping.

**ADVANTAGES:**

- It provides highly secured and more authorized implemented than existing ones.
- It supports the cross browser compatibility.
- It never limited resources.
- It shows the email tracking ability with improved proxy settings.

**MODULES**

This project (Web Network Statistics generator and analyzer) aim is to simplify your website strange. There are a range of functions and reports that provide extensive information on all website status and produce a modification guides.

1. **ABOUT TOOL**
2. **LOGIN**
3. **FILE TRANSFER BLOCKER**
4. **EMAIL WATCHER**
5. **SEARCH MONITORING**
6. **WEB ADMIN**
7. **REPORTS**

**MODULE DESCRIPTION**

**1. ABOUT TOOL**

This modules shows the entire sitemap and index to this upcoming events, ongoing web projects, development sites and also provides the how to use this tool to submit the reports and inspecting details to the system.

**2. LOGIN**

The main objective of this module is to authenticate the logged in clients, clients and others those who are enter into the system for various purposes and they can be authenticated and authorized by the secured mechanism that are enforced by the masonry system.

**3. FILE TRANSFER BLOCKER**

This module mainly dealt to monitor the files that are send and received by the users of the registered servers and the proxy servers are really powerful medium of tracking devices and process flow implementation for further data leakage and verifies the attachment that contains the trajons, malware executable files. It also processes the chat options and that contains any kind of malicious words that damage the server to infinite state.

**4. EMAIL WATCHER**

The major process of this module is to setup a secured email block system that monitors the process of incoming and outgoing emails that are sending and received bythe proxy server that are performing the intrusion emails ,spam mails and executable file data processing system used for the admin tracking mails that was used by the others.

**5. SEARCH MONITORING**

This module monitors the users by applying minimum process of data tracking for those who are doing the performance of search query with malicious words that cause the interruption for the entire system.

**6. WEB ADMIN**

The admin has the overall control of the web statistics and monitoring system. It includes file transfer update options, email blocker, login watcher, allocation and other updates of clients by their request, view log and generate reports.

**7. REPORTS**

The masonry admin of the project generate the reports according to the clients request in different file formats.

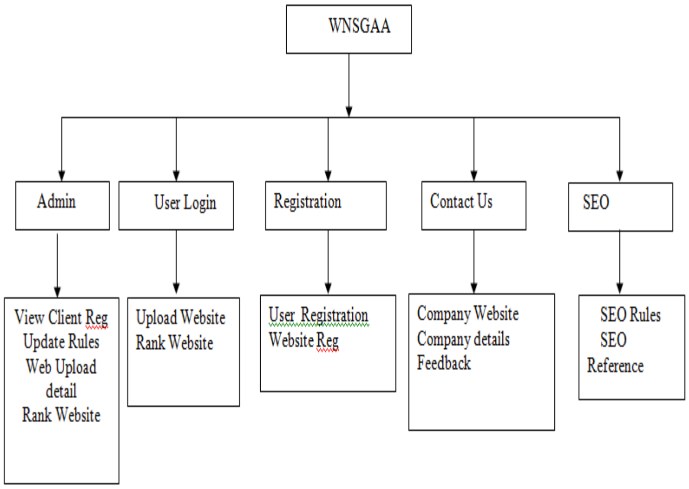

**FIGURE 1: SYSTEM ARCHITECTURE**

## IV. CONCLUSION

The proposed web performance monitor tool had been successfully implemented and tested in different hosting servers. It processed involves web user monitoring, file transfer watcher, Email blocker, Find hidden images and verifies links & URL's Connections. Contents are stored into the central database. They are updated accordingly in the system. The project consists of various modules such as admin, user, registration, web upload. It includes the secured gateway system for the entire server system and transactions performing on the process based actions with perspective to the web product development.

## REFERENCES

[1]. Advanced PHP Programming by Schlossnagle.Sams. Paperback- October 2003.

[2]. Beginning PHP, MySQL and Apache. Wrox Press Ltd. Paperback- 1 June, 2003.

[3]. Making Use of PHP by Appu.John Wiley & Sons Inc. Paperback- 24 July, 2002

[4]. PHP and MySQL Web Development by Luke Welling, Laura Thomson.Sams. Paperback- 30 March, 2001.

[5]. PHP Bible by Converse.John Wiley & Sons Inc. Paperback- 4 October, 2002.