IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 7, July 2023, Pages 70-75

DOI: 10.17148/IJARCCE.2023.12711

NETWORK STAT INTERPRETER WITH SYNCHRONIZATION

Rithesh P G[1], Usha M[2]

Master of Computer Applications, Bangalore Institute of Technology, Bengaluru -560004[1]

Master of Computer Applications, Bangalore Institute of Technology, Bengaluru -560004[2]

Abstract: Computer networking is broadly considered including hardware, software, procedures and people. Networking encompasses many activities, such as, creation of network products, distribution processes, user activities, and supporting services like marketing, documentation, information services and maintenance. Network management covers both the establishment of networking operations and actual operation of the network facilities. It includes all management functions performed at such network nodes as computing centres, documentation facilities, and service distribution centres. In the present-day complex networks, network monitoring and measurement has grown in significance. In past decades, administrators could have simply monitored a small number of PCs or network devices.

Keywords: Network Managing System, Synchronized Network, Network Analysis, Nagios.

I. INTRODUCTION

The term "network" has been interpreted quite broadly. A network is a collection of processing nodes, communications links, hardware, software, people and their organizational ties, as well as a number of rules, laws, and regulations that enable the components of the network to function properly and interact.

In the formative and conceptual stage of network development, this wide definition is employed to provide an integrated approach to the entire system development. Some nodes may be resource-oriented centers that provide the network with particular resources, such as one-of-a-kind data bases or exceptional computing power.

An efficient and automatic network monitoring is always required for large organizations like universities, companies and other business sectors where the manual network monitoring is very difficult. Since large organizations have a big network topology, the manual network problem.

For huge organizations like colleges, corporations, and other business sectors where manual network monitoring is extr emely complicated, an effective and automatic networked computer system monitoring is always necessary.

Since large enterprises have complex network topologies, manual network monitoring wastes time when endeavoring to pinpoint the site of problems.

A crucial component of a network administrator's job is the challenging and demanding process of network monitoring. Keeping their networks running smoothly is a continual goal for network managers. A company's productivity would suffer if a network went down, even for a little period of time, and public sector departments' capacity to deliver crucial services would be jeopardized. Administrators must keep track of network performance and traffic flow in order to be proactive rather than reactive. They also need to make sure that no security gaps exist on the network.

Monitoring agents must find, isolate, and fix network issues when a failure occurs, and they may also need to recover the failure. The administrators should typically be warned by the agents to rectify any issues within a minute. The administrators' duties still include regularly checking for threats coming from the inside or outside of the network despite the reliable network. Additionally, if the network devices are overloaded, they must often verify the network performance. Information regarding network consumption may be utilized to create a network plan for short- and long-term enhancements in the future before a failure due to overload.

This article gives readers an overview of the current network monitoring techniques, as well as their topologies, characteristics, and features. Additionally, it provides a comparison of such strategies.

II. LITERATURE SURVEY

A review of the literature on network monitoring systems reveals several important conclusions. The information from the search results is summarized as follows:

Completion: A network monitoring system ought to be thorough and cover every facet of network security.

Critical analysis: There is a critical analysis of popular applications of current network monitoring techniques available. Visualization: One popular technique for spotting malicious activity on a network is network monitoring through visualization.

Open source software: A literature review discusses the use of open source software for monitoring networks.

Data gathering: A survey on network data gathering is available, and it rates the effectiveness of earlier findings.

The literature review as a whole emphasizes the significance of thorough network monitoring systems that cover all facets of network security. There is a need for more research in the field of network data collection. Popular methods of network monitoring include visualization and the use of open source software.

III. METHODOLOGY

The design and implementation of a network stat interpreter tool may be discussed in this paper.

Data Gathering and Analysis: In order to produce network statistics for the paper, data from network devices may need to be gathered and examined.

Statistical Analysis: To interpret the network statistics, the paper may employ statistical analysis methods.

Methodologies for Visualization: The paper may examine techniques for visualizing the network statistics.

Assessment of Accuracy: The paper may evaluate the veracity of the network statistics and how they were interpreted.

IV. NETWORK MONITORING SYSTEMS

The term "network management" refers to the wide topic of managing telecommunications and computer networks. It has a reputation for monitoring network hardware and ensuring that a network is always accessible to users. The NMS's history may be found at the subject of network management may be traced back. However, NMS are crucial for managing sophisticated computer networks since they make sure all network defects are identified and help the network administrator repair them. Additionally, NMS may keep an eye on network issues including traffic, latency, performance, and availability. They are intended to facilitate the human oversight and troubleshooting of network devices, as well as alert network managers (through email and SMS) in the event of outages. NMS are a crucial method for raising a network's performance, reachability, and availability.

In network management, material or information collecting serves this purpose.Network monitoring software gathers d ata for network management applications.The goal of network monitoring is to gather all relevant network data that can be used to effectively manage and regulate how people utilize the network.Remotely situated network equipment is use d.The network management program cannot easily monitor the condition of these devices since it is uncommon for the m to have directly linked terminals.Network managers may now easily assess network utilization on their network devi ces thanks to the development of various ways to aid in the control of network usage.

"The process of recording, reviewing, and analyzing network traffic for the purpose of performance, security, and/or general network operations and management," is one definition of network traffic analysis. The goal of the analysis as well as time (or frequency) parameters may classify an analysis in general as well as network traffic analysis. Any network traffic analysis may be grouped into one of the three main categories: instantaneous examination, batched analysis, and forensics analysis. Time-based analysis can be divided into time and frequency categories.

A. Real-time evaluation: To effectively analyze data, it is either done over the data as it is acquired or utilizing short batches, often known as buffers. This requires the analysis and reporting of data based on the information that is already

DOI: 10.17148/IJARCCE.2023.12711

accessible, often within a minute of when it was really utilized. Due to real-time analysis being totally automated, it has a high reaction time, or in other words, there is little latency in data acquisition. However, real-time analysis often requires a lot of processing power.

B. Batched analysis: This method analyzes data at intervals long enough for the data to gather into what are known as data batches. Depending on the batching policies, the response time and related computational resource requirements may be higher or lower, but generally speaking, they provide a greater reaction time and minor computational property requirements than real-time study (although they require more storage capacity).

C. Forensics analysis: Also known as triggered analysis, forensics analysis is analysis that is carried out in response to a specific occurrence. When an intrusion is discovered on a specific host, forensics investigation is often carried out. This kind of analysis necessitates the use of previously recorded data as well as possible human interaction.

Network header fields are examined in packets as part of network data inspection methods, which then calculate these fields and provide outputs or results. To evaluate network traffic, a variety of tools are utilized. In today's networks, it is crucial to do traffic analysis and inspection at all layers, including layers 3 and 4. Among the tools that are most often used are Wireshark, Colasoft Capsa, TCPdump, etc.

V. AUTOMATIC NETWORK MONITORING

A description of the autonomous network monitoring and management system discussed in this study.In the network, C ISCO switches that support SNMP were used.These network switches are programmable, and several services, such pin g, ssh, and others, are used on them.

The nagios program also defines all of the characteristics of switches and routers.Nagios checks all the services that are used by the switches once every 10 seconds (a predetermined time).If a service seems to be down, Nagios is set up to make 5 triesAn alert is produced in Nagios after 5 unsuccessful tries, and this alert creates a ticket in RT.The RT server is always in communication with the ISP (internet service provider)As soon as a ticket is created in RT, information ab out the malfunctioning switch is included in the email that is sent to the network administrator.To address the ticket, the administrator may log into the RT server from a distance [10].If the administrator does not address the issue within an hour, it is passed on to the next accountable person on the priority list, and so forth.

VI. NETWORK MONITORING BY NAGIOS

Nagios is a web-based, open source network monitoring program. It keeps track of network nodes and any services used on them, updating the network. whenever a network change occurs, notify the administrator. Although Nagios works best in a linux environment, it may also be used with other systems. Nagios is a safe and simple to use program that offers a pleasant online interface, automated alerts when a condition changes, and a number of notification choices. Nagios sends email or SMS notifications to the network administrator whenever a node or service in the network encounters an issue. The GNU General Public License is used in the development of Nagios, which supports a variety of services including HTTP, NNTP, Ping, SMTP, and others. Nagios enables administrators to create a comprehensive network topology and specify the parent-child connection between nodes. Nagios is able to send only one message when a parent node goes down, informing users that any child nodes that were previously inaccessible have now become available. a standard network topology produced by nagios.

Nagios uses two elements to determine the status of nodes and services: "status" and "type of state." The kind of state may be either a soft state or a hard state, and the status can be either up, down, critical, or unreachable. The kind of condition is crucial for the alerting procedure. Before sending out a notice, it makes a decision on the ultimate status. Nagios checks the nodes and services a pre-determined number of times before deeming them to have a serious issue in order to prevent false alerts. The "max_check_attempts" option in the node and service specifications allows for the management of the number of tries. If a status check returns a non-OK condition but fewer tries have been made than the maximum number allowed ("max_check_attempts"), the node or service is deemed to be in soft state. This is often referred to as the "soft error state." The node or service returns from the "soft error state" in the "soft recovery state." If status check fails for the number of times provided in "max_check_attempts," the node or service is deemed to be in a hard state. When the node is either down or inaccessible, this is sometimes referred to as the "hard error state." The node or service returns from the "hard error state" in the "hard recovery state." If the status check changes from a hard OK state to a hard nonOK state or vice versa, the hard state of the node or service will also change.

DOI: 10.17148/IJARCCE.2023.12711

The hard node or service fault is noted and the administrator is informed of the issue if the node or service is declared in a non-OK state during the hard state change. However, if the node or service is declared in the OK state during the hard state transition, the hard node or service recovery is documented, and the administrator is informed about the recovery. Additionally, the administrator is now again alerted to the issue whenever a hard state shift from one non-OK state to another happens.

VII. COMPARISON OF NETWORK TRAFFIC ANALYSIS TOOLS

A. BandwidthD: -
With bandwidthD, TCP/IP network consumption is tracked and data that has been sniffed is shown in the form of tables and graphs for various time frames.Each protocol, including HTTP, UDP, and ICMP, is color-coded for better identification.

Due to BandwidthD's low dependency count and discrete background service operation [9], static mode may be set up quickly and easily.

Database mode can effectively analyze thousands of IP addresses and offers filtering via the use of numerous sensors, subnet, custom reports, and intervals.
It does not monitor the state of any specific connection; instead, it tracks every individual IP address and subnet.

B. Capsa Free: -
With Capsa Free, network traffic is sniffed and analysis of recorded packets is possible, making it simpler to solve network difficulties.A complete network analyzer with strong capabilities that offers indepth network analysis is Capsa free.
Only Windows OS 9 and 12 are supported, and data is presented in simple graph.

C. Fiddler:-
Fiddler may be used to easily analyze incoming and outgoing data so that changes can be made to replies and requests before they are transmitted to the browser. It can also be used to record HTTP traffic between specific machines and the Internet.Fiddler provides more thorough information.Due to its ability to decrypt HTTPS traffic and support for altering and replaying system requests, Fiddler 135 is also useful for security and performance testing on websites and online apps . Post variables may be simply transformed into tables.

D. Splunk: -
Is a platform that enables users to collect, monitor, and also analyze network data from various sources.Event logs, gadgets, services, and many other things are examples of data sources.Splunk is costly because of the high setup expenses in terms of both money and complexity.

E. The most recent iteration of the wellknown network traffic analyzer known as ntop is known as ntopng ('ng' stands for 'next generation'). ntopng will collect network traffic in the background and then present network use data and statistics in a Web UI.

F. Ethereal (also known as Wireshark): -
Enables realtime data from a network to be sniffed and then saved for study.One can sniff quite a few protocols using Ethereal, including IPX, SMTP, IGRP, ATM, PPP, and many more.It records information from live packets in both promiscuous and non-promiscuous modes.

It displays every network interface and gives the option to record data from each one.
The statistics of the packets that were received are also shown.The captured packets may be saved.
It has the ability to recover data from previously stored packet capture (Pcap) files.
It may display the TCP flow graph created from the TCP packets that were received.
The only decoding protocols supported are 14, and hex.

G. PRTG: - PRTG's robust monitoring engine can keep track of thousands of sensors at once.

Each sensor has the ability to be "tagged," making it simple to browse through a big list of sensors.

A webbased front end, a Windows application, the iPhone, or other mobile devices may be used to retrieve network and bandwidth monitoring data produced by PRTG Network Monitor 16.

DOI: 10.17148/IJARCCE.2023.12711

VIII. TESTING AND RESULTS

According to the rule of normal distribution, regardless of the size of N, the distribution of sample means is normal and unbiased given random and independent samples of N observations [16]. In accordance with the rule of normalcy, the sample number N during the system testing was equal to 4. Four network administrators from the computer science department tested the system. Based on the suggested anticipated findings, the outcome would still be normal and impartial even if the N size of network administrators was more than 4.

Additionally, network managers were urged to pay closer attention to the system's usability, responsiveness, and capacity to recover from faults.

Availability Testing

Users experienced availability when they could get the desired results. The system could detect when a connection became live or when a network's status changed, when a cable was cut, the causes of a network's change, and it could also provide the port numbers of an interface. Basically, the following methods were used to verify network availability:

❖ Up /Down thresholds
❖ Removal of a network cable
❖ Rebooting Device

Up/Down threshold

We used two sets of commands to test this threshold: "shutdown" and "no shutdown."
The following traps were acquired for up threshold (no shutdown):

❖ Interface 0/0 has changed from down to up (or vice versa).
❖ However, we were able to acquire the following traps for down threshold (shutdownAdministrative interface 0/0 down/down).
❖ These two different sorts of traps indicate if a network interface is accessible or not.

Rebooting Device

Rebooting was also used to see whether the system would work after a cold start.
This was accomplished by turning off the network device, and the format of the trap that was returned was (System Uptime), which only measures how long a device has been operational and accessible.

CONCLUSIONS

An effective and automated network monitoring and management system that alerts the network administrator right away in the event of a problem has been provided in this research.

Nagios is set up to create and keep track of the whole network topology and to issue alerts if a state changes anywhere on the network. In RT, these messages will produce tickets.

RT handles the additional network administration duty.The administrator simply needs to check his emails since this network monitoring solution is entirely automated.The intelligent network monitoring solution that is being shown can immediately locate the location of a problem in the network and its impact on the rest of the network.As a result, it isquite effective and gives the network total control.

REFERENCES

[1] D. Ten, S. Manickam, S. Ramadass, and H. A. Bazar, “Study on Advanced Visualization Tools In Network Monitoring Platform,” in Third UKSim European Symposium on Computer Modeling and Simulation, EMS ‘09’, Minden Penang, Malaysia, December 2009.

[2] L. Chang, W.L. Chan, J. Chang, P. Ting, M. Netrakanti, “A network status monitoring system using personal computer,” presented at IEEE Global Telecommunications Conference, August 2002.

[3] R. Talpade, G. Kim, and S. Khurana, “NOMAD: traffic-based network monitoring framework for anomaly detection,” IEEE International Symposium on Computers and Communications vol. 9, Morristown, NJ, August 2002.

[4] Cottrell, L.: Passive vs. Active Monitoring [online]. [cit. 2015-04-21]. URL, https://www.slac.stanford.edu/comp/net/wanmon/passive-vsactive.html.

[5] Worrall, A.; Carter, B.;Widley, G.: Network monitor and method. 2008 [cit. 2015-04-21], URL, http://www.google.com/patents/US7411946.

DOI: 10.17148/IJARCCE.2023.12711

[6] CaptureSetup/Ethernet – TheWiresharkWiki [online]. [cit. 2015-04-21]. URL, http://wiki.wireshark.org/CaptureSetup/Ethernet.

[7] http://cs.sru.edu/~mullins/cpsc100book/module08_networks/module08-01_networks.html. [Accessed 04 December 2016].

[8] Hemlata Patel, Pallavi Asrodia, "Network Traffic Analysis Using Packet Sniffer," Pallavi Asrodia, Hemlata Patel/International ISBN: 978-1-4673-6942-8/16/$31.00 ©2016 IEEE Journal of Engineering Research and Applications, vol. 2, no. 3, pp. 854-856,2012.

[9] A. Tabona, "The Top 20 Free Network Monitoring and Analysis Tools for Sys Admins," 23 July 2013. [Online]. Available: http j Iwww.gfi.com/blo glthe-top-20 -free-network -mon itoring -andanalysis-tools-for-sys-adm ins!. [Accessed 14 April 20 IS].

[10] M. Biswas, "Microsoft Network Monitor," 2015. [Online]. Available: http://microsoft-network-monitor.software.informer.com/. [Accessed IS April 20 IS].