GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

OPEN SURVEY: NETWORK MONITORING SYSTEM

Priyanka Rao[*1], Satyam Gupta[2]& Akhilesh Pandey[3]
[*1]M. tech Scholar Department of Digital Communication, Axis Collage, Kanpur, India
[2]M. Tech Scholar Department of Computer Science Kanpur Institute of Technology, Kanpur, India
[3]Department of Computer Science Kanpur Institute of Technology, Kanpur, India

ABSTRACT

Network Monitoring Tool useful for log and monitor data flow in and out of the network. The service runs as a local service that is helpful for network engineer to perform daily routines duty. The basic task of network engineer to check congestion in the network and find out root cause for it. It can be useful in troubleshooting packets loss and latency. The tool is basically designed for TCP (Transmission Control Protocol), UDP (User Datagram Protocol) and ARP (Address Resolution Protocol). It traces timestamp, source-MAC, destination-MAC, and source IP, destination IP, source port, and destination port and packet length. To keep all data and information which used to transfer data from source to destination, network engineer mostly used various types of tools. These tools continually monitor network actives and notify the network engineer. Network Monitoring Tool informs us how well network is running during the various actives (operations) on different time. It is mainly useful for analyzing and monitoring the network traffic between various terminals and system that are in network and also get information into data files. After dumping of data it is used by network engineer to analyze for any problem in face by end user machine connected across the network. If any user machines behaved abnormally we can easily fetch the dumped data which is associated with that machine in order to resolve to that machine. If required another tool which are decryption of data can be used to find the problem.

Keywords: *Network Monitoring System(NMS), Benefits, Working process, Implementations of NMS.*

I. INTRODUCTION

Now everybody need to connected internet because of its useful and useless desire, so every second in network, millions of users are start and stop various services over network. It is very difficult task for system administrator to monitor the status of its services every second. So the basic need of administrator is software which performs it job easily and increases the network productivity. Because of unbalance network, network administrator cannot provide proper support to user with uninterrupted network services without using any tool.

Network Monitoring Tool enables monitor data flowing in and out of the network. The program runs as a local service. It helps administrator to check for congestion in the network and the root cause for it. It can be useful in troubleshooting packet loss and latency.

Network monitoring tool is very important task of network administrator/system administer with the help of monitoring they will increase the perform employee productive and infrastructure cost.

This tool can be used by network administrator to monitor the traffic and report any unusual anomaly usage. It also helps in maintaining overall performance of the network. Packet sniffers or protocol analyzers are tools that are commonly used by network technicians to diagnose network related problems.

ISSN 2348 – 8034
Impact Factor- 5.070

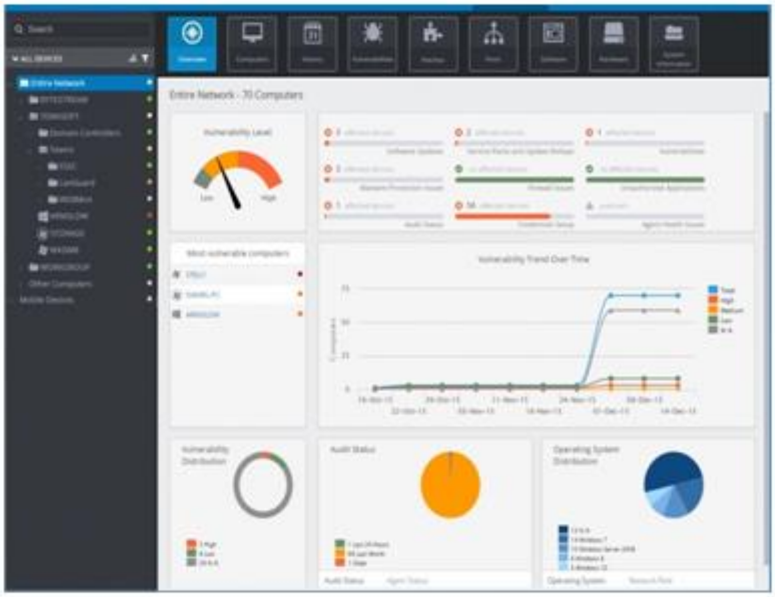

Search
ALL DEVICES
Entire Network
Entire Network - 70 Computers
Vulnerability Level
Low
High
Most vulnerable computers
Vulnerability Trend Over Time
Audit Status
Operating System Distribution

Fig 1. Network Monitoring System

Network monitoring can be achieve with the help of various types of software tool or set of plug and play hardware and software combination network monitoring system use to identifies various type of daily network problem. Monitoring of network is also increase the quickly solve the problem. There are various types of networking monitoring tool are available that time in market that tool performance differ to difference type of tool some tools are use only check the connectivity between the nodes, some tools are use only check the performance of various networking devices that are also known as in real network as nodes, some tools are used to check the uploading and downloading speed of data transmission in various node.

Network monitoring tool describe the information which is used by network administrator to identify what are the various nodes in network which transfer data in the network, what bandwidth they are use to transmit the data in the tool we are also monitor sender and receiver information, and also define what types of data they are transmitted, what method they are use to transmit the data and define the rate of packet data.

II. BENEFITS

If network work properly no issue then administrator gets call and get news is network is down then whole network team face challenge. This time network gets performance issue. Meaning network team are feel network fine whenever user not complain. So to increases the performance of network team monitor network is very important and it will also troubleshoot easily.

- Stay ahead of outages
- Fix issues faster and easily
- Gain immediate ROI
- Manage growing, changing network

A. Stay ahead of outages

Human error, configuration issues, and environment factors all contribute on it. Implement network monitoring system is basic and simple ways to prevent these from happening. It has potential to visibility to one step solving problem. By show live network performance easily detect why network is slow down.

B. Fix issues faster and easily

In down time of network some users not provide money when services are down. So if we monitor network then we find out the factor behind it very easily and fix problem.

C. Gain immediate ROI

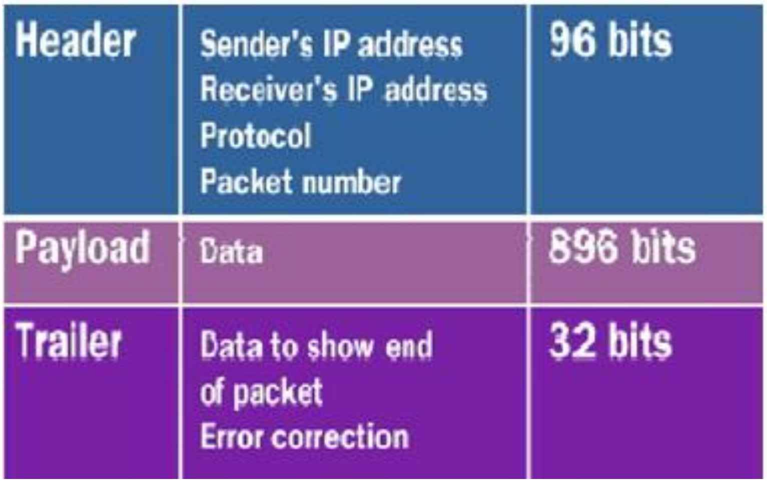
In today industry face the problem of money, so they don't have more staff to check network manually and it is not good practice also to check network manually because of critical network is not easily check by human so they use network monitoring software.

D. Manage growing , changing network

Due to innovation in network, number of user increases and problems is also increases so if we monitor network properly then only we solve the problem.

III. WORKING PROCESS

We understand that in network only transfer various information from one device to other device with the help of packet because packet is only thing which run over the network. Basically network monitoring system in which packet is filter as user required packet containing so much information some information is useful but not all so we filter different type of packets. Size of packet is mostly between 1000 to 1500 byte.



Header	Sender's IP address Receiver's IP address Protocol Packet number	96 bits
Payload	Data	896 bits
Trailer	Data to show end of packet Error correction	32 bits

Fig 2. Packet

As stated earlier, in order to design a network monitoring tool the first and the most important step is to fetch all the data that is sent across the network is sent in the form of data unit that called packet. In other terms is a method of growing data which is transmitted all over a digital network into packet.

A packet is powerful part of data that is routed between origin and receiver on the network or internet. When we transfer any file (e-mail, web pages, mp3, graphics file URL and many more) is sent from one place to another over the network, The Transmission control protocol (TCP) layer of TCP/IP divide file into some small parts that is known as "chunks" for routing in network. Each of these packets is containing address of destination. After addressing packed is transport over network and consider different path of network to reach its desire destination. Some "Packet" is called datagram because protocol like TCP, the User datagram protocol (UDP) know the term datagram.

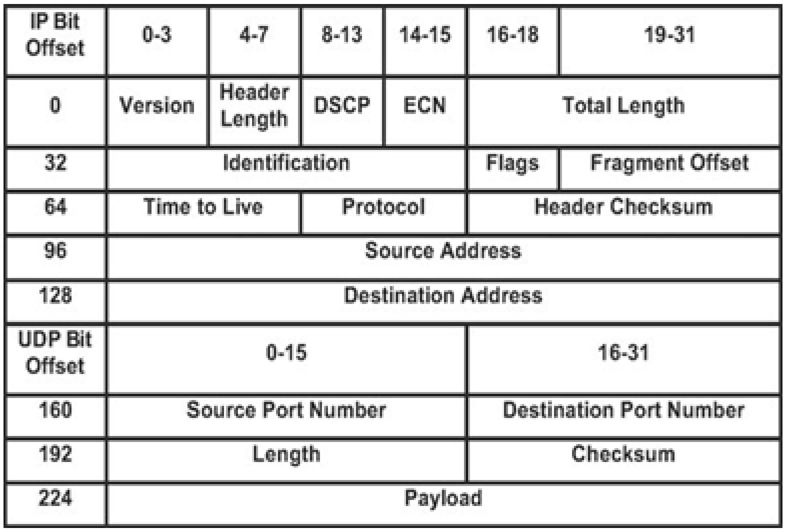
Packet is divided into three parts:-

□ Packet Header
□ Payload/Data
□ Packet Trailer

A. Packet Header

Header contains information about data take by the packet. Header contains the basic information of data which is useful for transfer data into network. Header includes instruction which is contained.

□ Sender Information
□ Destination information
□ Protocol
□ Packet number
□ Synchronization
□ Length of packet



IP Bit Offset	0-3	4-7	8-13	14-15	16-18	19-31
0	Version	Header Length	DSCP	ECN	Total Length	
32	Identification				Flags	Fragment Offset
64	Time to Live		Protocol		Header Checksum	
96	Source Address					
128	Destination Address					
UDP Bit Offset	0-15				16-31	
160	Source Port Number				Destination Port Number	
192	Length				Checksum	
224	Payload					

B. Payload/Data

Payload is the actual data which is send by sender to receiver if packet is fixed length payload can be padded with Blank information.

C. Packet Trailer

Trailer is also known as footer of the packet to receiving device. This part is basically containing useful information which used in receiver side. It contains error detection information. After receiving message receiver check the data and use trailer part for error detection if any error on data then receiver discard receiver data and inform sender to send data again otherwise receiver accept data and send acknowledge message to sender.

IV. IMPLEMENTAION

There are various platforms available to develop network monitoring system. In all platform the common part is all network monitoring system.

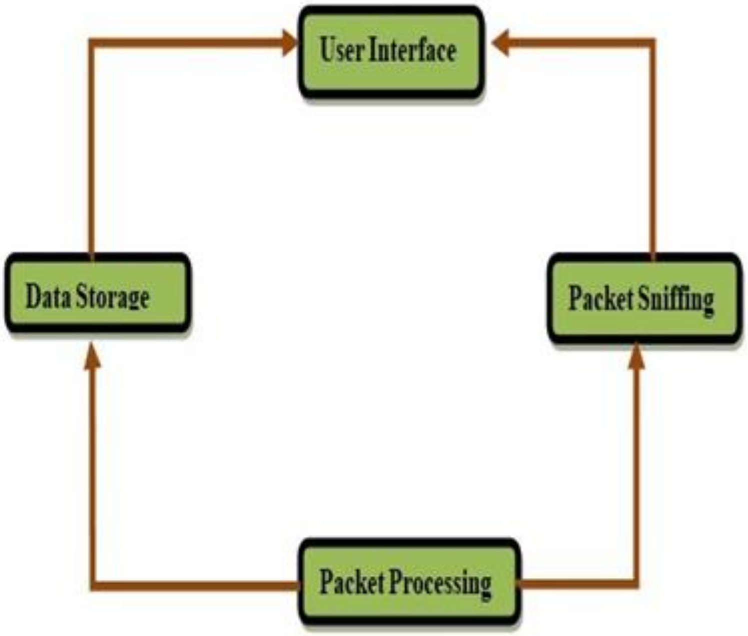
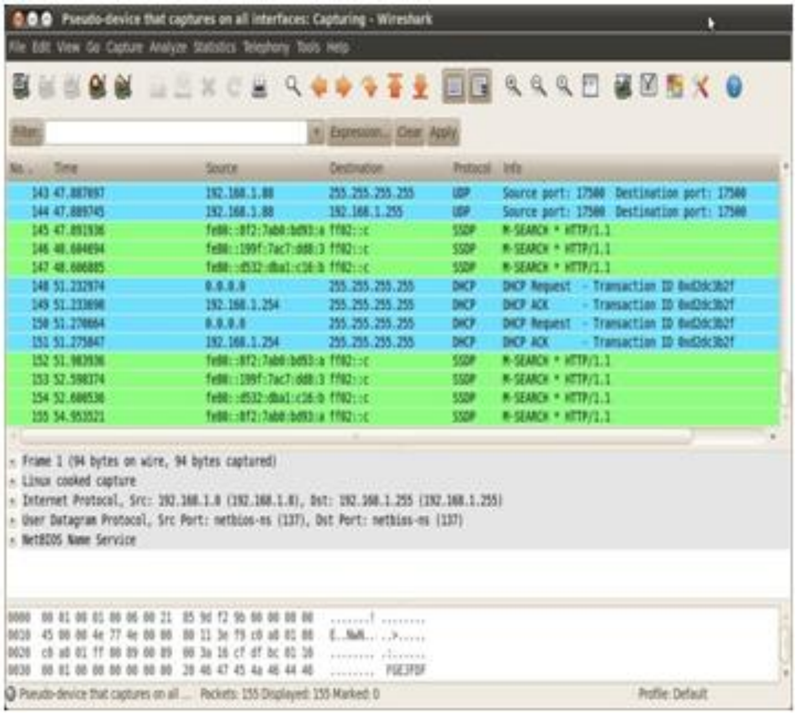


Fig 4. Implementation

A. User Interface

The user interface is platform where network administrator and its team interact with monitoring system. It will be develop with programming language.


Pseudo-device that captures on all interfaces: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time         Source                 Destination        Protocol  Info
   143 47.887097    192.168.1.88           255.255.255.255    UDP       Source port: 17500  Destination port: 17500
   144 47.889745    192.168.1.88           192.168.1.255      UDP       Source port: 17500  Destination port: 17500
   145 47.891936    fe80::8f2:7ab0:bd93:a  ff02::c            SSDP      M-SEARCH * HTTP/1.1
   146 48.604694    fe80::199f:7ac7:d88:3  ff02::c            SSDP      M-SEARCH * HTTP/1.1
   147 48.606885    fe80::d532:dba1:c16:b  ff02::c            SSDP      M-SEARCH * HTTP/1.1
   148 51.232974    0.0.0.0                255.255.255.255    DHCP      DHCP Request  - Transaction ID 0xd2dc3b2f
   149 51.233698    192.168.1.254          255.255.255.255    DHCP      DHCP ACK      - Transaction ID 0xd2dc3b2f
   150 51.270664    0.0.0.0                255.255.255.255    DHCP      DHCP Request  - Transaction ID 0xd2dc3b2f
   151 51.275047    192.168.1.254          255.255.255.255    DHCP      DHCP ACK      - Transaction ID 0xd2dc3b2f
   152 51.983936    fe80::8f2:7ab0:bd93:a  ff02::c            SSDP      M-SEARCH * HTTP/1.1
   153 52.598374    fe80::199f:7ac7:d88:3  ff02::c            SSDP      M-SEARCH * HTTP/1.1
   154 52.600536    fe80::d532:dba1:c16:b  ff02::c            SSDP      M-SEARCH * HTTP/1.1
   155 54.953521    fe80::8f2:7ab0:bd93:a  ff02::c            SSDP      M-SEARCH * HTTP/1.1

+ Frame 1 (94 bytes on wire, 94 bytes captured)
+ Linux cooked capture
+ Internet Protocol, Src: 192.168.1.8 (192.168.1.8), Dst: 192.168.1.255 (192.168.1.255)
+ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
+ NetBIOS Name Service

0000  00 01 00 01 00 06 00 21  85 9d f2 9b 00 00 00 00   .......! ........
0010  45 00 00 4e 77 4e 00 00  80 11 3e f9 c0 a8 01 08   E..NwN.. ..>.....
0020  c0 a8 01 ff 00 89 00 89  00 3a 16 cf df bc 01 10   ........ .:......
0030  00 01 00 00 00 00 00 00  20 46 47 45 4a 46 44 46   ........  FGEJFDF

Pseudo-device that captures on all...   Packets: 155 Displayed: 155 Marked: 0        Profile: Default
```

Fig 5. User Interface

B. Packet Sniffing

That is user to capture packet from real network.

C. Packet Processing

Using packet processing we filter only useful packet which come from sniffing.

D. Data Storage

Now after packet processing the relevant information which is use in future by administrator that is store in file or database.

V. CONCLUSION

Features such as flexibility, reusability, fast development of networks create endless new and thrilling areas for network monitoring. In future, this wide range where networks can be applied would take an integral place in our life. But still, monitoring network needs to fulfill the constraints brought by dominating factors such as scalability issues, fault tolerance, cost of production, change in the layout of network and power consumption. In this survey paper, we describe the brief overview regarding monitoring, their applications and the factors influencing the network design.

REFERENCES

1. *https://searchnetworking.techtarget.com/definition/pack et*
2. *https://www.oreilly.com/library/view/building-internet- firewalls/1565928717/ch04.html*
3. *https://computer.howstuffworks.com/question5251.htm*
4. *http://www.linfo.org/packet_header.html*
5. *http://classgist.com/projectdetails.aspx?id=73*
6. *https://www.helpsystems.com/resources/articles/top- benefits-network-monitoring*

7. https://www.google.co.in/search?ei=xSBoXJ_zJYv9vA SFrqzgAQ&q=benefits+of+network+monitoring&oq=u se+of+network+monitoring&gs_l=psy-ab.1.0.0i71l8.0.0..62373...0.0..0.0.0.......0......gws- wiz.5wwyfRSbauc
8. http://www.on-time.com/rtos-32-docs/rtip- 32/programming-manual/tcp-ip-networking/ip-packet-types.htm