Assessment of Network Protocol Packet Analysis in IPv4 and Ipv6 on Local area with TCPDUM command

Preeti Raj Verma[1], Sarvesh Kumar[2]

[1]Assistant Professor, Dept. of Computer Science Engineering, Rama University, Uttar Pradesh, Kanpur,
[2]Assistant Professor, Dept. of Computer Science Engineering, Rama University, Uttar Pradesh, Kanpur

---***---

Abstract - It is observes local area network usage and provides a statistical display of data in a network. The network display monitor displays the information that is TIME STAMP, SOURCE IP, DESTINATION IP, SOURCE MAC, DESTINATION MAC etc. A system packet analyzer will endeavor to catch network packet and attempts to show that packet information as itemized as could be expected under the circumstances. You could think about a system packet analyzer as an estimating device used to inspect what's happening inside a system link, much the same as a voltmeter is utilized by a circuit repairman to look at what's happening inside an electric link (yet at a larger amount, obviously).

Administrators can deal with the movement and screen any irregular use. This apparatus is fundamental to monitor the parcels that sending and getting the framework. This venture can give a statically information of the system movement and consequently we can enhance the effectiveness and execution of the network.

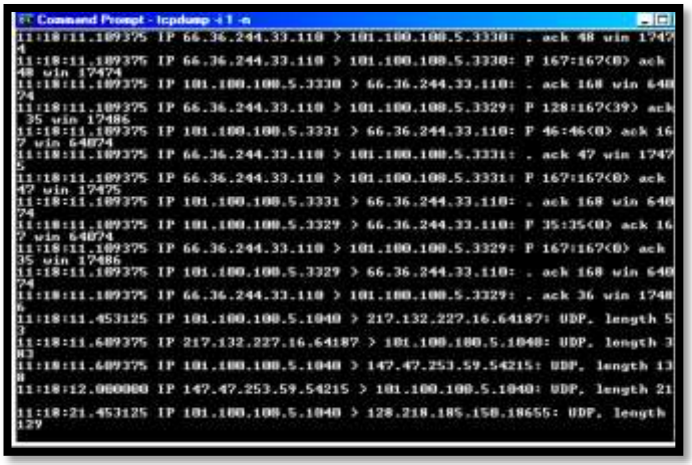
Keywords –*TCP, ARP, UDP, ICMP[3], TCPDUMP, IPv4, IPv6, network performance monitoring, wireless networks*

I. Introduction

Admin can view all the information about network packets after capturing all the packets with the help of TCPDUMP command. It is a big project which is running on business management, big organizations and where the large number of systems available in a network.

A real time network monitoring tool can be widely used in a network of originations where the large number of computer system is established. The first advantage of our tool is the ability to generate measurements in real time and it is the web based application which easily connects high speed network and start monitoring [8] accordingly. Second, the tool can be easily extended to consider several types of network protocols. We have conducted an experimental study to verify the effectiveness of our tool, and to determine its capacity to process large volumes of data provides .This process is observes local area network usage and provides a statistical display of data in a network. It is watches exchange union territory arrange use and gives a factual show of information in a system. The system indicates screen shows the data that is Timestamp, Source IP, and Destination IP, Source Mac address, Destination mac address, Payload length and so forth. The intention of study is to build up an IPv4/IPv6 [5] arrange analyzer otherwise called a Packet analyzer, network monitoring tool[7], network analyzer, protocol analyzer or packet sniffer.

It is an electronic PC application that can block and log movement passing generally speaking an advanced system or some portion of a system. As data streams flow across the network, the sniffer captures packets by TCPDUMP command [1] and if needed decodes the packet's raw data, showing the values of other fields in the IP packet, and analyses its content according to the appropriate logical operator or other specifications. When traffic is captured, either the entire contents of packets can be recorded, or the headers can be recorded without recording the total content of the packet.



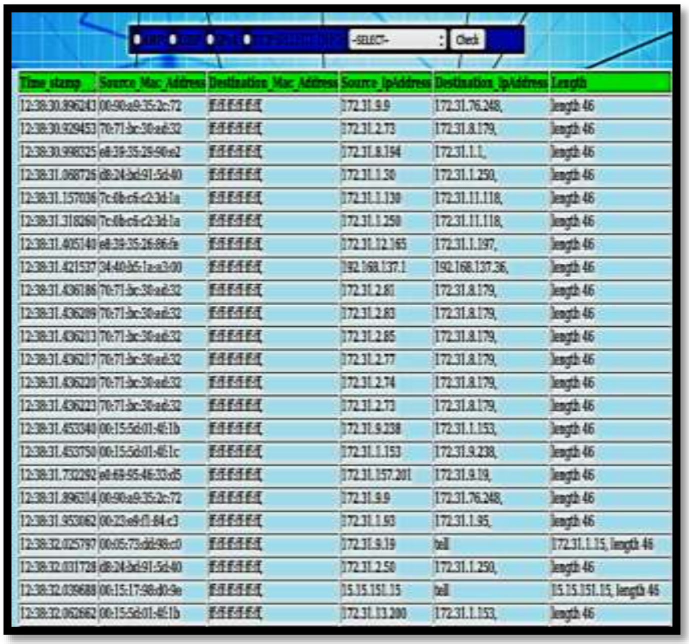
```
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3330: . ack 48 win 1747
4
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3330: P 167:167(0) ack
48 win 17474
11:18:11.109375 IP 101.100.100.5.3330 > 66.36.244.33.110: . ack 168 win 640
74
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: P 128:167(39) ack
 35 win 17486
11:18:11.109375 IP 101.100.100.5.3331 > 66.36.244.33.110: P 46:46(0) ack 16
7 win 64074
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3331: . ack 47 win 1747
5
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3331: P 167:167(0) ack
47 win 17475
11:18:11.109375 IP 101.100.100.5.3331 > 66.36.244.33.110: . ack 168 win 640
74
11:18:11.109375 IP 101.100.100.5.3329 > 66.36.244.33.110: P 35:35(0) ack 16
7 win 64074
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: P 167:167(0) ack
35 win 17486
11:18:11.109375 IP 101.100.100.5.3329 > 66.36.244.33.110: . ack 168 win 640
74
11:18:11.109375 IP 66.36.244.33.110 > 101.100.100.5.3329: . ack 36 win 1748
6
11:18:11.453125 IP 101.100.100.5.1040 > 217.132.227.16.64187: UDP, length 5
3
11:18:11.609375 IP 217.132.227.16.64187 > 101.100.100.5.1040: UDP, length 3
83
11:18:11.609375 IP 101.100.100.5.1040 > 147.47.253.59.54215: UDP, length 13
8
11:18:12.000000 IP 147.47.253.59.54215 > 101.100.100.5.1040: UDP, length 21

11:18:21.453125 IP 101.100.100.5.1040 > 128.210.185.150.10655: UDP, length
129
```

Fig.1 A captured packet with option –x will look

```
15:52:42.475432 00:1d: 09:46:a3:43 > 00:08:02: ee:
1c:08, ether type IPv4 (0x0800), length 74:
172.31.9.56.41120>172.31.9.84.23S2754605757:2754
605757(0) win 5840 <mss 1460, sack OK, timestamp
99293 0, nop, wscale 7>
0x0000:  0008 02ee 1c08 001d 0946 a343 0800 4510
0x0010:  003c 7160 4000 4006 5e81 ac1f 0938
```

How to capture a packet in ipv4/ipv6 with the help of TCPDUMP command

```
#! /bin/bash /usr/sbin/tcpdump -i eth0 -ne -c 50000 > network
```



Time_stamp	Source_Mac_Address	Destination_Mac_Address	Source_IpAddress	Destination_IpAddress	Length
12:38:30.896243	00:90:a9:35:2c:72	ff:ff:ff:ff:ff:ff	172.31.9.9	172.31.76.248,	length 46
12:38:30.929453	70:71:bc:30:ad:32	ff:ff:ff:ff:ff:ff	172.31.2.73	172.31.8.179,	length 46
12:38:30.998325	e8:39:35:29:90:e2	ff:ff:ff:ff:ff:ff	172.31.8.194	172.31.1.1,	length 46
12:38:31.068726	d8:24:bd:91:5d:40	ff:ff:ff:ff:ff:ff	172.31.1.30	172.31.1.250,	length 46
12:38:31.157036	7c:6b:c6:c2:3d:1a	ff:ff:ff:ff:ff:ff	172.31.1.130	172.31.11.118,	length 46
12:38:31.318260	7c:6b:c6:c2:3d:1a	ff:ff:ff:ff:ff:ff	172.31.1.250	172.31.11.118,	length 46
12:38:31.405140	e8:39:35:26:86:fe	ff:ff:ff:ff:ff:ff	172.31.12.165	172.31.1.197,	length 46
12:38:31.421537	34:40:b5:1a:a3:00	ff:ff:ff:ff:ff:ff	192.168.137.1	192.168.137.36,	length 46
12:38:31.436186	70:71:bc:30:ad:32	ff:ff:ff:ff:ff:ff	172.31.2.81	172.31.8.179,	length 46
12:38:31.436209	70:71:bc:30:ad:32	ff:ff:ff:ff:ff:ff	172.31.2.83	172.31.8.179,	length 46
12:38:31.436213	70:71:bc:30:ad:32	ff:ff:ff:ff:ff:ff	172.31.2.85	172.31.8.179,	length 46
12:38:31.436217	70:71:bc:30:ad:32	ff:ff:ff:ff:ff:ff	172.31.2.77	172.31.8.179,	length 46
12:38:31.436220	70:71:bc:30:ad:32	ff:ff:ff:ff:ff:ff	172.31.2.74	172.31.8.179,	length 46
12:38:31.436223	70:71:bc:30:ad:32	ff:ff:ff:ff:ff:ff	172.31.2.73	172.31.8.179,	length 46
12:38:31.453340	00:15:5d:01:4f:1b	ff:ff:ff:ff:ff:ff	172.31.9.238	172.31.1.153,	length 46
12:38:31.453750	00:15:5d:01:4f:1c	ff:ff:ff:ff:ff:ff	172.31.1.153	172.31.9.238,	length 46
12:38:31.732292	e0:69:95:46:33:d5	ff:ff:ff:ff:ff:ff	172.31.157.201	172.31.9.19,	length 46
12:38:31.896314	00:90:a9:35:2c:72	ff:ff:ff:ff:ff:ff	172.31.9.9	172.31.76.248,	length 46
12:38:31.953062	00:23:e9:f1:84:c3	ff:ff:ff:ff:ff:ff	172.31.1.93	172.31.1.95,	length 46
12:38:32.025797	00:05:73:dd:98:c0	ff:ff:ff:ff:ff:ff	172.31.9.19	tell	172.31.1.15, length 46
12:38:32.031728	d8:24:bd:91:5d:40	ff:ff:ff:ff:ff:ff	172.31.2.50	172.31.1.250,	length 46
12:38:32.039688	00:15:17:98:d0:9e	ff:ff:ff:ff:ff:ff	15.15.151.15	tell	15.15.151.15, length 46
12:38:32.062662	00:15:5d:01:4f:1b	ff:ff:ff:ff:ff:ff	172.31.13.200	172.31.1.153,	length 46

Fig-2 Captured packet in command prompt with TCPDUMP command

Here are some examples people use TCPDUMP commands for:

- A real time *network monitoring tool*
- Administrators can deal with the *movement*
- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- QA engineers use it to *verify network applications*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol* internals

Beside these examples TCPDUM command can be helpful in many other situations too.

Features

The following are some of the many features TCPDUM Command provides:

- Available for LINUX and *UNIX* and *Windows*.
- *Capture* live packet data from a network interface.
- *Search* for packets on many criteria
- Import packet from content documents containing hex dumps of packet information.
- Display packet with exceptionally *detailed protocol information*
- Using the GUI to *retrieve useful management*
- *Save* packet data captured.
- *Export* some or all packets in a number of capture file formats.
- *Filter packets* on many criteria.
- Create various *statistics*.

II.OBJECTIVES

The objective of this paper is observes local area network usage and provides a statistical display of data in a network. The network display monitor displays the information that is TIME STAMP, SOURCE IP, DESTINATION IP, SOURCE MAC, DESTINATION MAC etc.

Administrators can deal with the movement and screen any irregular use. This apparatus is fundamental to monitor the parcels that sending and getting the framework. This venture can give a statically information of the system movement and consequently we can enhance the effectiveness and execution of the network.

Capturing is the process by which the network monitor collects the information and all the information is stored in a database and decodes the packet's raw data, showing the values of various fields in the packet, and analyses its content according to the appropriate logical operator or other specifications. When traffic is captured, either the entire contents of packets can be recorded, or the headers can be recorded without recording the total content of the packet.

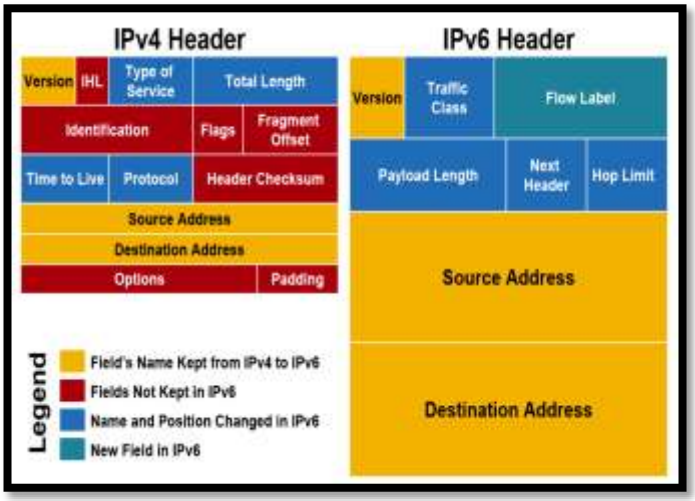


Fig-3 IPv4 header and IPv6 header

III. METHODOLOGY

1-IPV4 (Internet Protocol version 4) One of the major protocols in the TCP/IP[11] protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model. Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.

IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4[2] uses 32-bit logical address.

1.1 Searching protocol analysis

This field will provide the details of packets according to the selected protocol and required fields.

1.2 Top talker analysis

This field will provide the top 5 machines or source IP according to the number of bytes and number of packets.

1.3 Time source IP analysis

This field will provide the details of packets and help to detect the problem according to the given specific time.

1.4 Port number analysis

This field will provide the details or packets and help to find the specific application currently working on which machine.

1.5 Reconstruction analysis

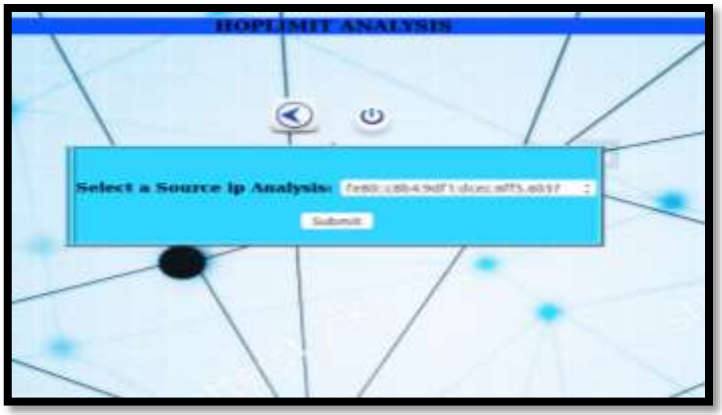
If first and second IP provide and application is selected then it will give the information in particular Page related with the reconstruction the network between two device otherwise it will provide error messages like please provide first IP, please provide second IP, please select the application like DNS 53, HTTP 80 please enter the valid IP in case if we provide wrong IP and any wrong information related with these analysis. This field will use to reconstruct the network communication.

2-IPV6 (Internet Protocol Version 6) The most evident change in IPv6 [4] over IPv4 is that IP addresses are extended from 32 bits to 128 bits. This expansion suspects extensive future development of the Internet and gives alleviation to what was seen as an approaching deficiency of system addresses. IPv6 additionally bolsters auto-arrangement to help amend the vast majority of the inadequacies in form 4, and it has incorporated security and portability highlights.
Today majority of devices running on Internet are using IPv4 [7] and it is not possible to shift them to IPv6 in the coming days. There are mechanisms provided by IPv6, by which IPv4 and IPv6 [6] can co-exist unless the Internet entirely shifts to IPv6 [10].

- Dual IP Stack
- Tunneling (6to4 and 4to6)
- NAT Protocol Translation

2.1 Hop limit analysis for ipv6 only

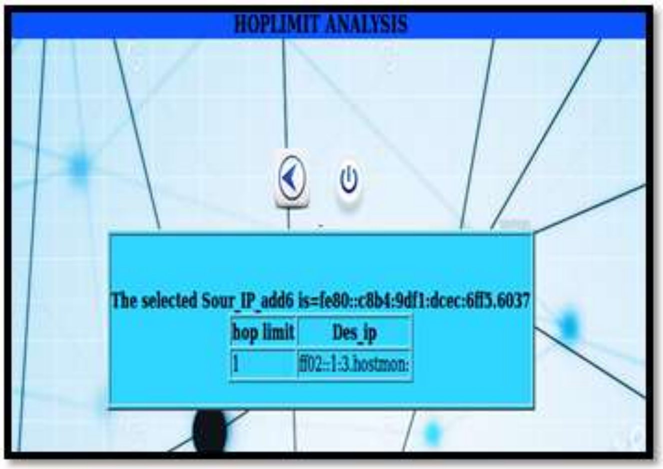
This field will provide the details of hop limit packets and help to find the packet which may be discard in the network. select source IP then after Display hop limit info for particular sourceIP and also fetch all hop limit value from the DB according to selected protocol after that select source IP and submit it so it will fetch the information from the DB according to selected option. For ex- if ADMIN select the source IP then it will fetch hop limit and destination IP from the DB.



HOPLIMIT ANALYSIS

Select a Source Ip Analysis: fe80::c8b4:9df1:dcec:6ff5.6037

Fig 4 Select source IP address



HOPLIMIT ANALYSIS

The selected Sour_IP_add6 is=fe80::c8b4:9df1:dcec:6ff5.6037

hop limit	Des_ip
1	ff02::1:3.hostmon:

Fig-5 Show Final Result hop limit and destination IP

IV. Result & Discussion

Administrators can manage the traffic and monitor [9] any abnormal usage. This tool is Essential to keep the track of the packets that sending and receiving the system. This study can provide a statically data of the network traffic and thus we can improve the efficiency and performance of the network. Capturing is the process by which the network monitor collects the information and all the information is stored in a database and decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate logical operator or other specifications. When traffic is captured, either the entire contents of packets can be recorded, or the headers can be recorded without recording the total content of the packet.

V. Conclusion

The scope of this process is that the System administrators will be able to view a more in-depth status assessment including measures of specific services on a given server and also see all related information about the current running network. A real time network monitoring tool can be widely used in a network of originations where the large number of computer system is established.

1. Anshulgupta, Suresh gyanvihar“**A Research Study on Packet Sniffing Tool TCPDUMP”** International Journal of Communication and Computer Technologies Volume 01 – No.49 Issue: 06 Jul 2013 ISSN NUMBER : 2278-9723.

2. Z.turanyi, A.Valk6 COMET group, Columbia University 2960 Broadway New York **“IPV4+4”** Proceedings of the 10 th IEEE international conference on network protocol (ICNP’02)1092-1648/02.

3. J. Postel, **“Internet Control Message Protocol,”**Internet RFC 792, September 1981.

4. S. Deering, R. Hinden, “**Internet Protocol, Version 6 (IPv6) Specification,”** Internet RFC 2460, December 1998..

5. https://343networks.files.wordpress.com/2010/06/ipv4-ipv6-header.gif. J. Hatcher,
“**Strategies for migrating from IPv4 to IPv6,** 2012Available:
http://datacentremanagement.com/news/view/strategies-for-migrating-from-ipv4-to-ipv6.

6. P. Wu, Y. Cui, J. Wu, J. Liu, C. Metz**, “Transition from IPv4 to IPv6: A State-of-the-Art Survey”,** IEEE Communications Surveys & Tutorials, Vol. 15, no. 3, pp 1407 – 1424, 2012.

7. OD Monitoring] SubrataMazumdar and Aurel A. Lazar **"Objective-Driven Monitoring For Broadband Networks"** IEEE Transactions on Knowledge and Data Engineering v 8 n 3 Jun 1996. P 391-402 A research paper on objective oriented monitorin

8. **[**Tools List] Les Cottrell **"Network Monitoring Tools"** http://www.slac.stanford.edu/~cottrell/tcom/nmtf_tools.html A good list of network monitoringtools.

9. Mr. G.S. Nagaraja, RanjanaR.Chittal, Kamod Kumar **“Study of Network Performance Monitoring Tools-SNMP”** IJCSNS International Journal of Computer Science and Network S 310 ecurity, VOL.7 No.7, July 2007.

10. Daniel ENACHE, Marian ALEXANDRU Transilvania University, Brașov, Romania **A STUDY OF THE TECHNOLOGY TRANSITION FROM IPv4 TO IPv6 FOR AN ISP**, Review of the Air Force Academy No 1 (31) 2016.