Performance Analysis of Open Source Solution "ntop" for Active and Passive Packet Analysis Relating to Application and Transport Layer

Sirajuddin Qureshi[1], Dr Gordhan Das[2] Saima Tunio[3], Faheem Ullah[4], Ahsan Nazir[5], Ahsan Wajahat[6]
Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China[1]
Information Technology Centre, Sindh Agriculture University Tandojam, Sindh, Pakistan[2, 3]
Faculty of Information Technology, Beijing University of Technology, Beijing, 100124, China[4, 5, 6]

***Abstract*—A key issue facing operators around the globe is the most appropriate way to deal with spotting black in networks. For this purpose, the technique of passive network monitoring is very appropriate; this can be utilized to deal with incisive problems within individual network devices, problems relating to the whole LAN (Local Area Network) or core network. This technique, however, is not just relevant for troubleshooting, but it can also be castoff for crafting network statistics and analyzing network enactment. In real time network scenarios, a lot of applications and/or processes simultaneously download and upload data. Sometimes, it is very difficult to keep track of all the uploaded and downloaded data. Wireshark is a tool that is normally used to track packets for analysis between two particular hosts during two particular sessions on the same network. However, Wireshark as some limitations such as it is not a good tool for keeping track of bulky network data transferred among various endpoints. On the other side, an open source solution "ntop" offers active as well as passive packet analysis which can be handy for system administrators, networkers and IT managers. Additionally, with ntop VoIP traffic can also be monitored. In this research work, the ntop solution has been deployed to a network facility and performance analysis of ntop solution for various application processes (on application layer) such as HTTP, SSDP (based on HTTPU) against their associated protocols such as TCP/IP, UDP, and VoIP have been analyzed. Additionally, above said processes and protocols have been comprehensively analyzed relating with their client/server breakdown, duration of the connection, actual throughput, total bytes (bytes received and sent) and total bandwidth consumed. This study has been helpful to see the weakest and strongest areas of a particular network in terms of analyzing and deploying network policies. This research work will help the research community to deploy ntop solution for real-time monitoring actively and passively.**

Keywords—ntop; network monitoring; packet analysis; the application layer; transport layer

I. Introduction

Today's internet-enabled infrastructure has resulted in the vast majority of applications to require networks of some sort [1–9]. All kinds of networks require essential security ensure communication is transmitted through appropriately protected means [10–13]. Fig. 1 shows the difference between intranet and extranet.

Tracking and investigating traffic can be carried out for various reasons (Fig. 2) to examine the usage of network resources, measure the performance of network applications, adjust Quality of Service (QoS) policies in the network, log the traffic to fulfil the law, or create accurate models of traffic for academic reasons [14–21].

In order to examine where network resources are being consumed, there are a number of steps. The first step is to analyze the performance levels of network applications, adjusting Quality of Service network policies, recording the details of traffic according to regulations, or create accurate models of incoming and outgoing traffic for the purposes of academic objectives.

In order to fulfil all objectives, the scope and extent of research questions need to be identified. This concerns methods for appropriately classifying traffic, which may be applied to process big data near instantly, with reduced CPU and memory means. Other questions may be related to techniques related to the real-time approximation of the application of Quality of Service.

It is essential for all network operators to be aware of the performance levels of their network, in order to deliver reliability on the services they offer their customers.

Active and passive measurements are also a tool to troubleshoot their networks, in addition to simply measuring performance [22–27]. In certain instances, network faults may result in traffic being routed the wrong way. One way to tackle this can be through faults generating artificial traffic flows to inspect the behavior of traffic.

The Internet services are deep-seated part of higher education institutes [28-46]. Access to higher education is always beneficial for the public since higher education institutions maintain a foundation mission of research that is available through Internet high speed in higher education's environments. Table I shows some of the Popular Online Education Initiatives taken so far recently.

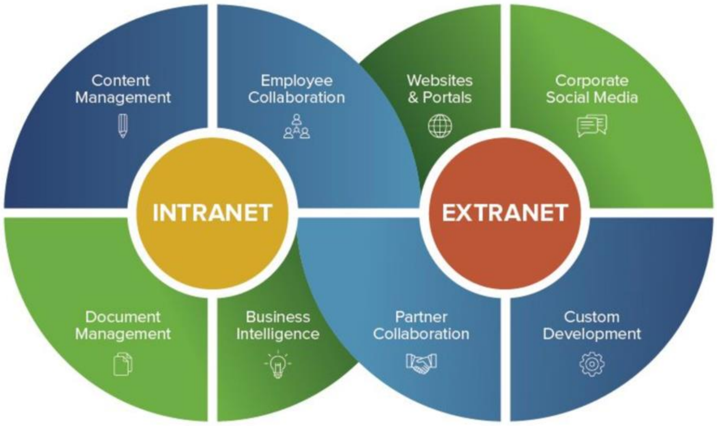
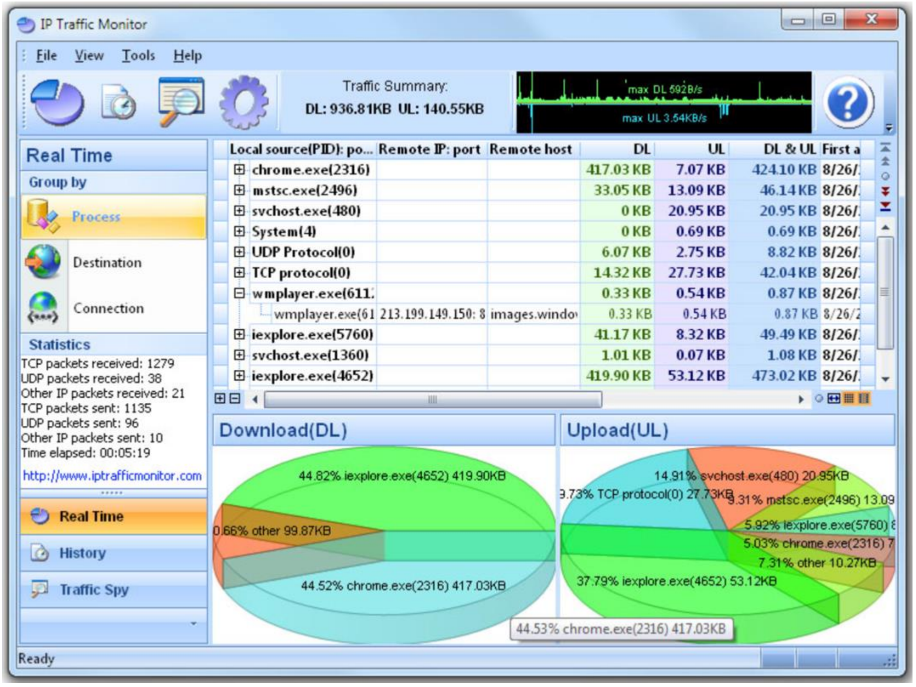


Fig. 1. Difference between Intranet and Extranet.


IP Traffic Monitor
File
View
Tools
Help
max DL 592B/s
max UL 3.54KB/s
Real Time
Group by
Process
Destination
Connection
Real Time
History
Traffic Spy
Download(DL)
44.82% iexplore.exe(4652) 419.90KB
0.66% other 99.87KB
44.52% chrome.exe(2316) 417.03KB
Upload(UL)
14.91% svchost.exe(480) 20.95KB
3.73% TCP protocol(0) 27.73KB
9.31% mstsc.exe(2496) 13.09
5.92% iexplore.exe(5760) 8
5.03% chrome.exe(2316) 7
7.31% other 10.27KB
37.79% iexplore.exe(4652) 53.12KB
44.53% chrome.exe(2316) 417.03KB
Ready

Traffic Summary:
DL: 936.81KB UL: 140.55KB

Local source(PID): po...	Remote IP: port	Remote host	DL	UL	DL & UL	First a
⊞ chrome.exe(2316)			417.03 KB	7.07 KB	424.10 KB	8/26/.
⊞ mstsc.exe(2496)			33.05 KB	13.09 KB	46.14 KB	8/26/.
⊞ svchost.exe(480)			0 KB	20.95 KB	20.95 KB	8/26/.
⊞ System(4)			0 KB	0.69 KB	0.69 KB	8/26/.
⊞ UDP Protocol(0)			6.07 KB	2.75 KB	8.82 KB	8/26/.
⊞ TCP protocol(0)			14.32 KB	27.73 KB	42.04 KB	8/26/.
⊟ wmplayer.exe(611.			0.33 KB	0.54 KB	0.87 KB	8/26/.
wmplayer.exe(61	213.199.149.150: 8	images.windo	0.33 KB	0.54 KB	0.87 KB	8/26/2
⊞ iexplore.exe(5760)			41.17 KB	8.32 KB	49.49 KB	8/26/.
⊞ svchost.exe(1360)			1.01 KB	0.07 KB	1.08 KB	8/26/.
⊞ iexplore.exe(4652)			419.90 KB	53.12 KB	473.02 KB	8/26/.

Statistics
TCP packets received: 1279
UDP packets received: 38
Other IP packets received: 21
TCP packets sent: 1135
UDP packets sent: 96
Other IP packets sent: 10
Time elapsed: 00:05:19
http://www.iptrafficmonitor.com

Fig. 2. Analysis of Internet Traffic in Real Time.

Nowadays, a new educational system introduced in the real-world distance education system, Virtual Education System, online education system, actual state and trends for the future education system. Education can become transformative when teachers and students synthesize information across subjects and experiences, critically weigh significantly different perspectives, and incorporate various inquiries. Educators are able to construct such possibilities by fostering critical learning spaces, in which students are encouraged to increase their capacities of analysis, imagination, critical synthesis, creative expression, self-awareness, and intentionality.

As a result of these approaches, there are bonus benefits that can help the global community at large, as seen in the creation of online courses from the United States. Called Massively Open Online Courses (MOOCs), these are now increasingly common at online platforms. Platforms offer these in a fully online, or through blended options that combine online and classroom learning. The Pew Research Centre (2011) shows statistics that nearly 90% of American colleges or universities offered some courses of this nature.

Wireshark is a tool that is normally used to track packets for analysis between two particular hosts or between two particular sessions on the same network [47–50]. Fig. 3 shows the Wireshark Network Analyzer display windows. A typical network analyzer displays captured traffic in three panes:

1) Summary: This pane displays a one-line summary of the capture. Fields include the date, time, source address, destination address, and the name and information about the highest-layer protocol.

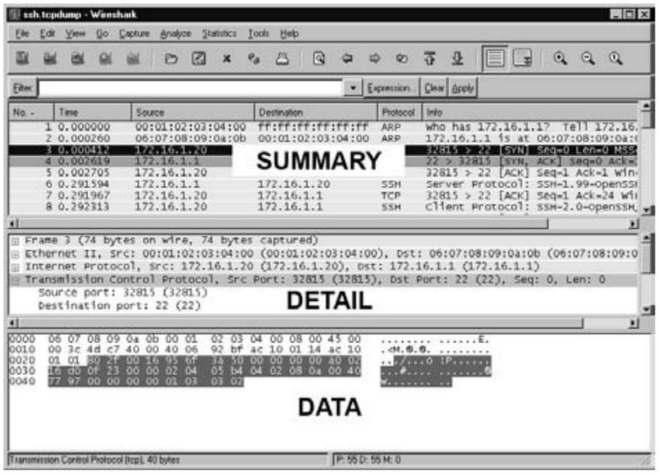
2) Detail: This pane provides all of the details (in a tree-like structure) for each of the layers contained inside the captured packet.

3) Data: This pane displays the raw captured data in both hexadecimal and text format.

Wireshark open source data packet analyzer. It is used for software, communication protocols, Ethernet and whole network analysis monitoring does not provide all features for analysis of the same network on Wireshark tool. However, Wireshark has some limitations such as it is not a good tool for keeping track of bulky network data transferred among various endpoints. Wireshark is not for intrusion detection system IDs, someone strange things on your network not show for warm. Wireshark doesn't manipulate on the network.

A network analyzer is a combination of hardware and software. Although there are differences in each product, a network analyzer is composed of five basic parts:

Hardware: Most network analyzers are software-based and work with standard operating systems (OSes) and network interface cards (NICs). However, some hardware network analyzers offer additional benefits such as analyzing hardware faults (e.g., cyclic redundancy check (CRC) errors, voltage problems, cable problems, jitter, jabber, negotiation errors, and so on). Some network analyzers only support Ethernet or wireless adapters, while others support multiple adapters and allow users to customize their configurations. Depending on the situation, you may also need a hub or a cable tap to connect to the existing cable.



```
No. -  Time      Source             Destination        Protocol  Info
     1 0.000000  00:01:02:03:04:00  ff:ff:ff:ff:ff:ff  ARP       Who has 172.16.1.1?  Tell 172.16.
     2 0.000260  06:07:08:09:0a:0b  00:01:02:03:04:00  ARP       172.16.1.1 is at 06:07:08:09:0a:
     3 0.000412  172.16.1.20                                     32815 > 22 [SYN] Seq=0 Len=0 MSS
     4 0.002619  172.16.1.1                                      22 > 32815 [SYN, ACK] Seq=0 Ack=
     5 0.002705  172.16.1.20                                     32815 > 22 [ACK] Seq=1 Ack=1 Win
     6 0.291594  172.16.1.1         172.16.1.20        SSH       Server Protocol: SSH-1.99-OpenSS
     7 0.291967  172.16.1.20        172.16.1.1         TCP       32815 > 22 [ACK] Seq=1 Ack=24 Wi
     8 0.292313  172.16.1.20        172.16.1.1         SSH       Client Protocol: SSH-2.0-OpenSSH_

⊞ Frame 3 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: 00:01:02:03:04:00 (00:01:02:03:04:00), Dst: 06:07:08:09:0a:0b (06:07:08:09:0
⊞ Internet Protocol, Src: 172.16.1.20 (172.16.1.20), Dst: 172.16.1.1 (172.16.1.1)
⊟ Transmission Control Protocol, Src Port: 32815 (32815), Dst Port: 22 (22), Seq: 0, Len: 0
    Source port: 32815 (32815)
    Destination port: 22 (22)

0000  06 07 08 09 0a 0b 00 01  02 03 04 00 08 00 45 00   ........ ......E.
0010  00 3c 4d c7 40 00 40 06  92 bf ac 10 01 14 ac 10   .<M.@.@. ........
0020  01 01 80 2f 00 16 95 6f  3a 50 00 00 00 00 a0 02   .../...o :P......
0030  16 d0 0f 23 00 00 02 04  05 b4 04 02 08 0a 00 40   ...#.... .......@
0040  77 97 00 00 00 00 01 03  03 02                     w....... ..

Transmission Control Protocol (tcp), 40 bytes     P: 55 D: 55 M: 0
```

Fig. 3. Network Analyzer Display.

TABLE I. SOME POPULAR ONLINE EDUCATION INITIATIVES

Name	Sponsor	Year	Fees
Coursera	Joint efforts by Princeton University, Stanford University, University of California Berkeley, University of Michigan-Ann Arbor, & University of Pennsylvania	2011	private
eduMOOC	University of Illinois Springfield	2011	Free
edx	Harvard University & MIT	2012	Non -profit
iTunes U	Apple Corporation	2012	For-profit
Khan Academy	Salman Khan (Hedge Fund manager)	2007	Non-profit
Minerva	Minerva project and Keck Graduate Institute (KIG). (Larry Summers, former Harvard University President & United States Secretary Of the Treasury, chaired its first advisory board)	2012	Private
MITx	Joint efforts by Harvard University and edX	2001	Non-profit
Peer 2 Peer University (P2PU)	Funding from the Hewlett Foundation & the Shuttle worth Foundation	2009	Non-profit
Saylor	Michael J. Saylor (Chairman, CEO, & President Of the business intelligence company MicroStrategy)	2008	Non-profit
TED-Ed	Sapling Foundation	1984	Private Non-profit
Udacity	Sebastian Thrun	2012	For-profit
Udemy	Eren Bali	About 2010	Some are free; some are for a tuition fee
University Of the people	Shai Reshef (educational entrepreneur)	2009	Non-profit

Sources: Schroeder, 2012; official websites of individual initiatives

II. Related Work

Gupta, U. [51] conducted the development of Monitoring in IOT enabled devices. He has developed Internet of things technologies complex network and heterogeneous environment. Monitoring the multi-router traffic, management information base, Zenoss, NTOP and Nagios implantation applications, process, events and logs observations are better in case of IOT.

Kokila S., Sathish, A., & Shankar, R. [52] conducted survey of a Comparative Analysis of Internet Traffic Identification Methods. They survey the main techniques and problems of IP packet based traffic analysis and focuses on application detection. Internet-based applications used more bandwidth increase of news user of Internet provider ISP increase network bandwidth interest of the user.

Nilsson, S., & Eriksson, J. [53] proposed the studied test Estimating Application Energy Consumption through Packet Trace Analysis. Their analysed power consumption utilised different applications calculating more accurate estimation mean power. Samsung Galaxy S4 battery 3G developing application transmission improvement the maximum through packet traces analysis.

Antichi, G., et al. [54] proposed a system architecture studied Enabling open-source high-speed network monitoring on netfpga. The monitoring system based on cooperative netfpga architecture positively with widely-recognised commercial system traffic considerably low cost. It provided open source instruments devices for capable high-performance monitoring system supporting 10 Gigabit per post base.

Garcıa-Dorado, J. L. et al. [55] conducted survey High-performance network traffic processing systems using commodity hardware. Their studied compared successful implementations of packet capture engines required throughput and availability of processing cores in the system. High- performance network system used equipment to limitation and bottlenecks solutions packet processing.

Leung, C. M, & Schormans, J. A. [56] proposed methodology of Measurement-based traffic characteristic estimation for QoS-oriented IP networks. They studied two major points facilitate accurate perditions of network performance loss and delay through the measured buffer, and packet traffic bandwidth provided the best network performance. It used an algorithm for IP packets Internets WAN connectivity loss and delay less affected customers.

III. Capture Driver

The capture driver is responsible to capture raw network traffic from the data cable. It filters unwanted traffic, and stores the remaining in a buffer. This is the most important, core element of a network analyzer, without data collection is impossible.

1) Buffer: The buffer stores captured data until its entire storage capacity has been reached. An alternative storage method is the rotation method when most recent data replaces previously stored data. Buffers are memory-based or disk-based.

2) Real-time Analysis: This is a tool to analyze data, as soon as it is received off the cable. It can be used to find network performance issues and even applied to intrusion detection systems to investigate suspicious activity within networks.

3) Decode: The Decode part shows and explains the contents of the network traffic in order to ensure it is readable. These are unique to every protocol, as a result of which network analyzers offer different numbers of supported decodes. These lists are renewed constantly to include more decodes.

This research has been helpful to see the weakest and strongest areas of a particular network in terms of analyzing and deploying network policies. This research work will further help to deploy the ntop solution for real-time monitoring actively and passively.

IV. Experimental Details

“ntop” is basically a web-based application user-friendly environment. The range of options “ntop” includes a graphical user interface as well as command line options, which make ntop as a priority of the network administrator who is already working in the Linux network environment. Based on the friendliness of ntop application, it easily installed the application and after configuration, it will start of packet capturing without wasting any time. Open source entities are getting importance in users day by day. It is almost easier to add plugins for the ntop to increase their functionality. The IP range is fully supported by ntop including IPV version 4 and 6.

A packet monitoring stage has been presented where different stages of packet monitoring have been depicted. The first stage is the network part where packets are captured.

Network part contains observation points. Observation points could anything ranging from network cards/interfaces to monitoring devices that forward packets to other points in the network under study. The second point in the network is server machines which work a packet aggregator. As data about a stream that was seen at a perception point, which may incorporate both trademark properties of a stream (e.g., IP addresses and port numbers) and measured properties (e.g., parcel and byte counters). They can be envisioned as records or lines in a common database, with one section for every property.

The metering and exporting procedures are by far the same which are normally taken to achieve this type of work and by firmly related exporting of data. Therefore, in this connection, we present these procedures. In Fig. 4, the process after achieving the data capture procedure has been presented. After capturing packet, all packets are time stamped and truncation is performed. After this packet sampling and packet filtering flow of a loop starts. In this research study, packet observing flow has been followed through this procedure.

This research work is done based on the IPV4 based network configuration. Easy installation and configuration process effortlessly open sources both window based and Linux based platform installation. Hardware requirement of 2.4 GHz process, 1GB RAM, 20 MB minimum hard desk.

Normally, network applications and their associated protocols are not studied together relating to network parameters. In earlier studies, network connectivity was done through standard switching environment as can be seen in Fig. 1.

However, in this work, not only network applications but their associated hosts (which are using the application) shall be analyzed against network protocols and network activities are monitoring through router environment. Routing tables perform excellent help in the ntop environment and fully supported through NetFlow. It can be seen in the Fig. 5, that P0 and P1 are points where network monitoring could be possibly studied. This is the added advantage of the ntop which offers the great facility to actively perform monitoring even sitting many miles away from the network. The client environment is also supported through VPN Client/Server breakdown is also very important to study, since bandwidth before not reflect any particular application, process or protocol responsible for its consumption. This client/server breakdown shall help to optimize server resources for a number of clients/nodes attached to it at any given time. Conclusively, this study shall be handy to explore new analysis techniques grouped together under one plate form “ntop” for taking informed network decision and network policies in the coming years.

Distinctive instruments for framework checking, for instance, network monitoring tests offer impelled programming vernaculars for separating framework streams and building quantifiable event records. Appallingly, these gadgets have been planned for analyzing comprehended framework streams. However, it is not for the most part easy to consider what mastermind resources will be attacked. Nearby a couple of exclusions, for instance, security-related inspections various security contraptions available on the Internet are by and large planned for recognizing attacks against a lone host regularly the one where the device has been incited. This infers they don't give sort out/subnet area/protection nor incorporate development watching and estimation workplaces. Subnets are the most vulnerable part of the network which can be attacked while performing network monitoring options.

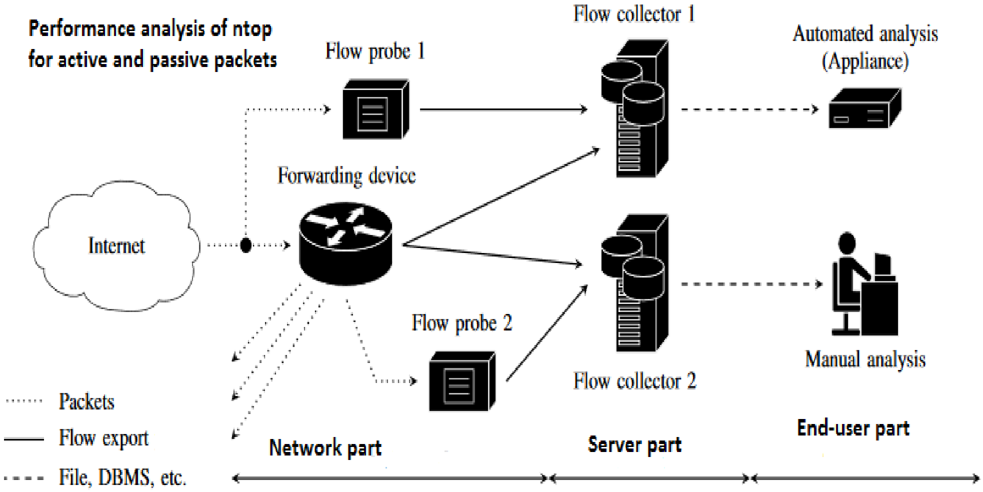


Fig. 4. Performance Analysis of Ntop for Active and Passive Packets.

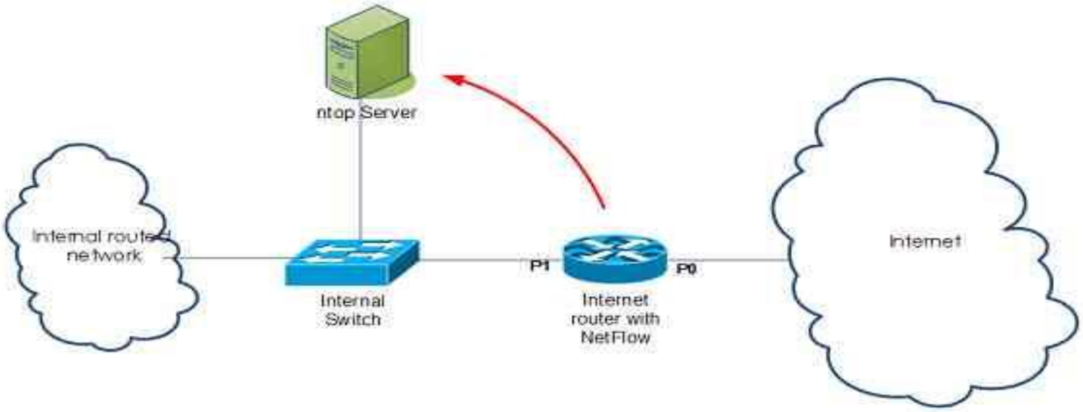


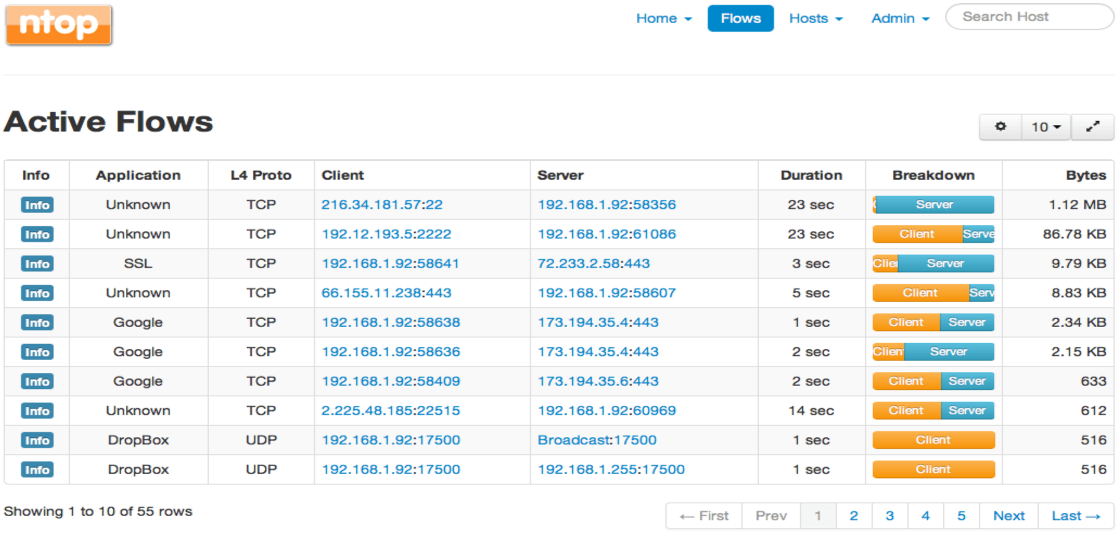
Fig. 5. Network Architect Scenario of Ntop Server Along with Applications within Routing and Switching Environment.

V. Results and Discussion

The data has been taken after implementing *ntop* software network environment at Sindh Agriculture University Tandojam. In the following, the active flow has been described as per data set of ntop parameters shown in Fig. 6.

In Fig. 7, it can be easily deduced that whether data is related with client or server, *ntop* regardless of its type captures the details for further workout.

In this research work, *ntop* has been implemented to achieve run time monitoring of the whole network. Active flows of network connection along with the detail throughput details have been presented.



Active Flows

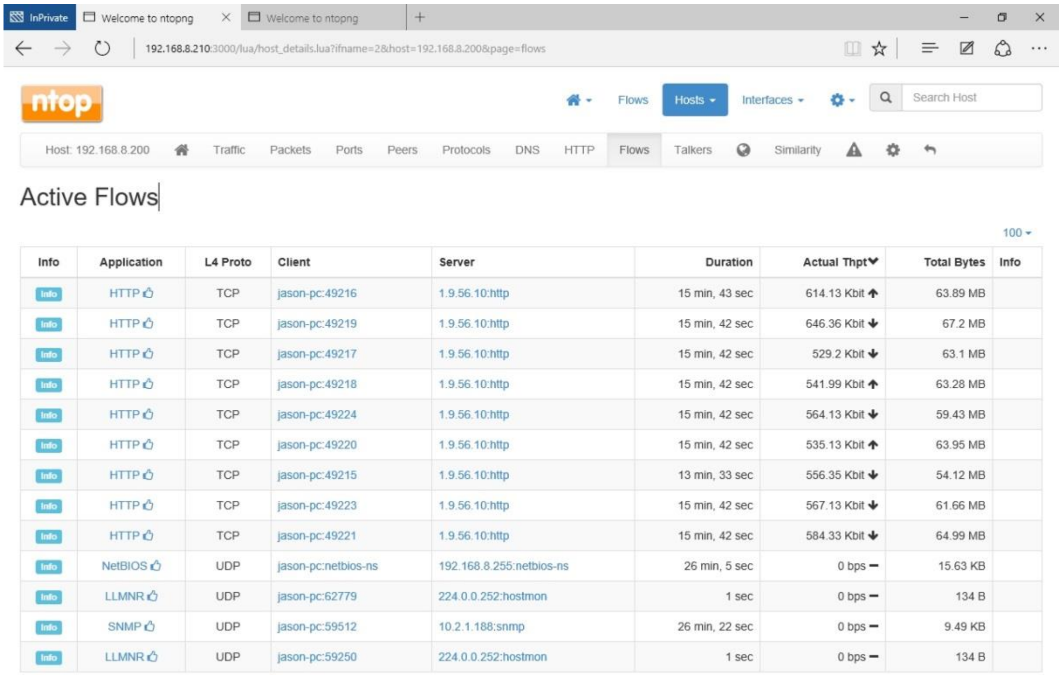
10

Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Bytes
Info	Unknown	TCP	216.34.181.57:22	192.168.1.92:58356	23 sec	Server	1.12 MB
Info	Unknown	TCP	192.12.193.5:2222	192.168.1.92:61086	23 sec	Client Serve	86.78 KB
Info	SSL	TCP	192.168.1.92:58641	72.233.2.58:443	3 sec	Clie Server	9.79 KB
Info	Unknown	TCP	66.155.11.238:443	192.168.1.92:58607	5 sec	Client Serv	8.83 KB
Info	Google	TCP	192.168.1.92:58638	173.194.35.4:443	1 sec	Client Server	2.34 KB
Info	Google	TCP	192.168.1.92:58636	173.194.35.4:443	2 sec	Clien Server	2.15 KB
Info	Google	TCP	192.168.1.92:58409	173.194.35.6:443	2 sec	Client Server	633
Info	Unknown	TCP	2.225.48.185:22515	192.168.1.92:60969	14 sec	Client Server	612
Info	DropBox	UDP	192.168.1.92:17500	Broadcast:17500	1 sec	Client	516
Info	DropBox	UDP	192.168.1.92:17500	192.168.1.255:17500	1 sec	Client	516

Showing 1 to 10 of 55 rows

← First | Prev | 1 | 2 | 3 | 4 | 5 | Next | Last →

Fig. 6. Data Related with Active Flow has been Captured During the Experimentation Phase of thesis Works.



192.168.8.210:3000/lua/host_details.lua?ifname=2&host=192.168.8.200&page=flows

Host: 192.168.8.200

Active Flows

100

Info	Application	L4 Proto	Client	Server	Duration	Actual Thpt	Total Bytes	Info
Info	HTTP	TCP	jason-pc:49216	1.9.56.10:http	15 min, 43 sec	614.13 Kbit ↑	63.89 MB	
Info	HTTP	TCP	jason-pc:49219	1.9.56.10:http	15 min, 42 sec	646.36 Kbit ↓	67.2 MB	
Info	HTTP	TCP	jason-pc:49217	1.9.56.10:http	15 min, 42 sec	529.2 Kbit ↓	63.1 MB	
Info	HTTP	TCP	jason-pc:49218	1.9.56.10:http	15 min, 42 sec	541.99 Kbit ↑	63.28 MB	
Info	HTTP	TCP	jason-pc:49224	1.9.56.10:http	15 min, 42 sec	564.13 Kbit ↓	59.43 MB	
Info	HTTP	TCP	jason-pc:49220	1.9.56.10:http	15 min, 42 sec	535.13 Kbit ↑	63.95 MB	
Info	HTTP	TCP	jason-pc:49215	1.9.56.10:http	13 min, 33 sec	556.35 Kbit ↓	54.12 MB	
Info	HTTP	TCP	jason-pc:49223	1.9.56.10:http	15 min, 42 sec	567.13 Kbit ↓	61.66 MB	
Info	HTTP	TCP	jason-pc:49221	1.9.56.10:http	15 min, 42 sec	584.33 Kbit ↓	64.99 MB	
Info	NetBIOS	UDP	jason-pc:netbios-ns	192.168.8.255:netbios-ns	26 min, 5 sec	0 bps –	15.63 KB	
Info	LLMNR	UDP	jason-pc:62779	224.0.0.252:hostmon	1 sec	0 bps –	134 B	
Info	SNMP	UDP	jason-pc:59512	10.2.1.188:snmp	26 min, 22 sec	0 bps –	9.49 KB	
Info	LLMNR	UDP	jason-pc:59250	224.0.0.252:hostmon	1 sec	0 bps –	134 B	

Fig. 7. Active Flows of Network Connection along with details of throughput and Duration of the Connections.

VI. Conclusion

It is the worst thing for a network administrator or manager to receive a call from an end user complaining about the health of the network. Additionally, we only know that any particular node is down on our network until someone complains about that. After receiving the complaint, the time to resolve that issue starts tickling. All the presented arguments are normally part of IT companies. Furthermore, performance analysis of any network is the key area for any organization. However, effective network monitoring gives you an added advantage of knowing the faults, congestion, and outage within the network in real time. In this research work, a practical approach for network analysis based on active and passive packet analysis is taken into consideration with the support of network monitoring tool called *ntop*. To achieve this research work "*ntop*" open source solution has been deployed and configured to a network facility under study which is the Information Technology Centre (ITC). Normally, network applications and their associated protocols are not studied together relating to network parameters. Particularly, a packet monitoring process has been well defined in this research work where different stages of packet monitoring have been properly outlined. The network monitoring process outlined in this research work is so flexible that can easily be modified for a different network architecture as per need. Conclusively, this research study proved handy to explore new analysis techniques grouped together under one platform "ntop" for taking informed network decision and network policies in the coming years.

References

[1] C. G. Bell, A. N. Habermann, J. McCredie, R. Rutledge, and W. Wulf, "Computer Networks," Computer (Long. Beach. Calif)., 1970.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Comput. Networks, 2008.

[3] P. M. Buscema, G. Massini, M. Breda, W. A. Lodwick, F. Newman, and M. Asadi-Zeydabadi, "Artificial neural networks," in Studies in Systems, Decision and Control, 2018.

[4] R. M. Neal, "Pattern Recognition and Machine Learning," Technometrics, 2009.

[5] J. Ahmad, H. Farman, and Z. Jan, "Deep Learning Methods and Applications," in SpringerBriefs in Computer Science, 2019.

[6] A. L. Caterini and D. E. Chang, "Recurrent neural networks," in SpringerBriefs in Computer Science, 2018.

[7] Y. Igarashi, T. Altman, M. Funada, and B. Kamiyama, "Computer Networks," in Computing, 2014.

[8] J. Sen, "A survey on wireless sensor network security," Int. J. Commun. Networks Inf. Secur., 2009.

[9] N. M. M. K. Chowdhury and R. Boutaba, "A survey of network virtualization," Comput. Networks, 2010.

[10] M. A. Mahmood, W. K. G. Seah, and I. Welch, "Reliability in wireless sensor networks: A survey and challenges ahead," Computer Networks. 2015.

[11] M. A. Devmane and N. K. Rana, "Security issues of online social networks," in Communications in Computer and Information Science, 2013.

[12] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," IEEE Commun. Surv. Tutorials, 2013.

[13] R. Zhang, J. Q. Chen, and C. A. Jaejung Lee, "Mobile commerce and consumer privacy concerns," J. Comput. Inf. Syst., 2013.

[14] V. Paxson, "Bro: A system for detecting network intruders in real-time," Comput. Networks, 1999.

[15] M. A. Kafi, Y. Challal, D. Djenouri, M. Doudou, A. Bouabdallah, and N. Badache, "A study of wireless sensor networks for urban traffic monitoring: Applications and architectures," in Procedia Computer Science, 2013.

[16] M. A. Kafi, Y. Challal, D. Djenouri, A. Bouabdallah, L. Khelladi, and N. Badache, "A study of wireless sensor network architectures and projects for traffic light monitoring," in Procedia Computer Science, 2012.

[17] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," J. Comput. Sci., 2009.

[18] A. Cecil, "A Summary of Network Traffic Monitoring and Analysis Techniques," in Computer Systems Analysis, 2006.

[19] A. K. Marnerides, A. Schaeffer-Filho, and A. Mauthe, "Traffic anomaly diagnosis in Internet backbone networks: A survey," Computer Networks. 2014.

[20] F. Olivier, G. Carlos, and N. Florent, "New Security Architecture for IoT Network," Procedia Comput. Sci., 2015.

[21] X. Laisheng, P. Xiaohong, W. Zhengxia, X. Bing, and H. Pengzhi, "Research on traffic monitoring network and its traffic flow forecast and congestion control model based on wireless sensor networks," in 2009 International Conference on Measuring Technology and Mechatronics Automation, ICMTMA 2009, 2009.

[22] S. Lee, K. Levanti, and H. S. Kim, "Network monitoring: Present and future," Computer Networks. 2014.

[23] E. Marín-Tordera, X. Masip-Bruin, J. García-Almiñana, A. Jukan, G. J. Ren, and J. Zhu, "Do we all really know what a fog node is? Current trends towards an open definition," Comput. Commun., 2017.

[24] H. Zhang, Y. Xiao, S. Bu, D. Niyato, F. R. Yu, and Z. Han, "Computing Resource Allocation in Three-Tier IoT Fog Networks: A Joint Optimization Approach Combining Stackelberg Game and Matching," IEEE Internet Things J., 2017.

[25] E. Vaadia and N. Birbaumer, "Grand challenges of brain computer interfaces in the years to come," Front. Neurosci., 2009.

[26] V. Mohan, Y. R. J. Reddy, and K. Kalpana, "Active and Passive Network Measurements : A Survey," Comput. Sci. Inf. Technol., 2011.

[27] J. Wang, Computer Network Security Theory and Practice. 2009.

[28] A. Forkosh-Baruch and A. Hershkovitz, "A case study of Israeli higher-education institutes sharing scholarly information with the community via social networks," Internet High. Educ., 2012.

[29] T. Govindasamy, "Successful implementation of e-Learning Pedagogical considerations," Internet High. Educ., 2001.

[30] R. J. C. Chu and C. C. Tsai, "Self-directed learning readiness, Internet self-efficacy and preferences towards constructivist Internet-based learning environments among higher-aged adults," J. Comput. Assist. Learn., 2009.

[31] E. D. Cassidy, A. Colmenares, G. Jones, T. Manolovitz, L. Shen, and S. Vieira, "Higher education and emerging technologies: Shifting trends in student usage," J. Acad. Librariansh., 2014.

[32] C. Jones and B. Shao, "The Net Generation and Digital Natives Implications for Higher Education," High. Educ. Acad., 2011.

[33] A. Y. Noaman, A. H. M. Ragab, A. I. Madbouly, A. M. Khedra, and A. G. Fayoumi, "Higher education quality assessment model: towards achieving educational quality standard," Stud. High. Educ., 2017.

[34] M. H. Harun, "Integrating e-Learning into the workplace," Internet High. Educ., 2001.

[35] H. E. Institutes, "A Framework for Supporting Adults in Distance Learning," Adult Learn. Irish J. Adult Community Educ., 2004.

[36] J. B. Roberts, L. A. Crittenden, and J. C. Crittenden, "Students with disabilities and online learning: A cross-institutional study of perceived satisfaction with accessibility compliance and services," Internet High. Educ., 2011.

[37] A. P. Rovai, "A practical framework for evaluating online distance education programs," Internet High. Educ., 2003.

[38] L. Shen, T. Manolovitz, G. Griffin, J. Britsch, E. D. Cassidy, and L. Turney, "Higher Education and Emerging Technologies," Ref. User Serv. Q., 2013.

[39] P. Krish, S. Hussin, M. R. Manap, and Z. Amir, “Mobile learning readiness among Malaysian students at higher learning institutes,” Asian Soc. Sci., 2012.

[40] A. Kukulska-Hulme, “How should the higher education workforce adapt to advancements in technology for teaching and learning?,” Internet High. Educ., 2012.

[41] K. Bohle Carbonell, A. Dailey-Hebert, and W. Gijselaers, “Unleashing the creative potential of faculty to create blended learning,” Internet High. Educ., 2013.

[42] A. Usman, “The Impact of Service Quality on Students’ Satisfaction in Higher Education Institutes of Punjab,” J. Manag. Res., 2014.

[43] R. Jain, G. Sinha, and S. Sahney, “Conceptualizing service quality in higher education,” Asian J. Qual., 2011.

[44] S. Hussin, M. Radzi Manap, Z. Amir, and P. Krish, “Mobile Learning Readiness among Malaysian Students at Higher Learning Institutes,” Asian Soc. Sci., 2012.

[45] R. Afreen, “Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges,” Int. J. Emerg. Trends Technol. Comput. Sci., 2014.

[46] J. J. Kidwell, K. M. V. Linde, and S. L. Johnson, “Knowledge Management Practices in Higher Education,” Educ. Q., 2000.

[47] S. Akhiria, “Wireshark,” Jar. Komput., 2013.

[48] J. F. Kurose and K. W. Ross, “Wireshark Lab: Getting Started,” Comput. Neworking A Top - Down Approach, 2010.

[49] U. Banerjee, A. Vashishtha, and M. Saxena, “Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection,” Int. J. Comput. Appl., 2010.

[50] P. T. Files, “Wireshark Network Analysis The Official Wireshark Network Analyst Study Guide,” Analysis. 2010.

[51] Gupta, Udit. "Monitoring in IOT enabled devices." arXiv preprint arXiv:1507.03780 (2015).

[52] Kokila, S., A. Sathish, and R. Shankar. "Comparative Analysis of Internet Traffic Identification Methods."In Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications. 2015.

[53] Nilsson, Samuel, and Joakim Eriksson. "Estimating Application Energy Consumption Through Packet Trace Analysis." (2014).

[54] Antichi, Gianni, Stefano Giordano, David J. Miller, and Andrew W. Moore. "Enabling open-source high speed network monitoring on NetFPGA." In 2012 IEEE Network Operations and Management Symposium, pp. 1029-1035. IEEE, 2012.

[55] García-Dorado, José Luis, Felipe Mata, Javier Ramos, Pedro M. Santiago del Río, Victor Moreno, and Javier Aracil. "High-performance network traffic processing systems using commodity hardware." In Data traffic monitoring and analysis, pp. 3-27. Springer, Berlin, Heidelberg, 2013.

[56] Leung, C. M., and John A. Schormans. "Measurement-based traffic characteristic estimation for QoS-oriented IP networks." JOURNAL-COMMUNICATIONS NETWORK 1, no. 2 (2002): 14-18.