Network Traffic Monitoring and Analysis using Packet Sniffer

Apri Siswanto[1], Abdul Syukur[2], Evizal Abdul Kadir[3], Suratin[4]
[1,2,3,4]Department of Informatics Engineering, Faculty of Engineering
Universitas Islam Riau, Indonesia

aprisiswanto@eng.uir.ac.id, abdulsyukur@eng.uir.ac.id, evizal@eng.uir.ac.id, suratin@student.uir.ac.id

***Abstract*—Traffic analysis using the internet is an activity to record data from user activities in using the Internet. This study aims to obtain data about the results of traffic in a graphical form so that it can find out the number of users who access the internet and use bandwidth. In this study, researchers also noted when the peak internet usage time in Telkom Vocational School Pekanbaru. The method used to get the results of the study is the packet sniffing method. Researchers can filter data packets from the http protocol application. Since, user activity is more dominant in finding and downloading sites on the Internet. The tool used is wireshark, this application is greatly helpful with features that are truly supportive and easy to analyze networks.**

Keywords— Packet snipper, Network Traffic, Monitoring, Internet, Wireshark

I. INTRODUCTION

The internet is a collection of interconnected networks throughout the world. The internet connects a collection of Local Area Networks (LAN) and Wide Area Networks (WAN). Both LAN and WAN can be connected via copper cable, fiber optic cable, and wireless transmission [1]. One important thing to consider in the use of internet technology is service. For example bandwidth management services. The amount of bandwidth used can affect the download and upload speed in exchanging data. This is very useful both in the field of business and education. Through the internet network, students are usually used to access the internet in searching for assignments and the use of e learning [2].

The usage of internet access in the Telkom Vocational High School, Pekanbaru, Indonesia is quite high. Internet usage has become a necessity for Telkom Vocational students due to student activities in learning activities using e-learning systems. For this reason, network monitoring and management of network traffic is a very important task in the field of computer networks [3].This traffic analysis is used to monitor the traffic of internet access usage, which is used by students and teachers of Telkom Vocational School, Pekanbaru to access websites, social media and others. In this case, only register users can access the Internet so that they can find out how much data bandwidth is used for internet needs at Telkom Vocational Schools. In this study, the authors conducted bandwidth measurements and network access monitoring in the Hypertext Transfer Protocol (HTTP) application so that the highest bandwidth usage traffic can be identified at a certain time.

To monitor and analyses data traffic, a packet sniffer tool is used. Packet sniffing is a technique of monitoring every packet that crosses the network. The tools commonly used to do packet sniffing techniques are generally Wireshark and Netcut. Packet sniffing is usually done by hackers or malicious intruders to carry out prohibited actions such as stealing passwords, and retrieving other important data. Then for the way the packet sniffing works is divided into three process, namely collecting, conversion, analysis, and data theft [4]. Nevertheless, in this study the sniffing packet was only used for monitoring and analysing network traffic.

II. LITERATURE REVIEW

A. Related Research

In this study to obtain optimal output research, literature review conducted related previous studies, so that it can be used as a reference in research. There are several research studies that have been carried out by previous researchers, such as [3], they discussed packet analysis and network traffic monitoring over TCP protocol used wireshark packet sniffer. The data analyzed are TCP time sequence graph, TCP Throughput graph, TCP round trip time graph. Based on data analysis of traffic on the network. The researchers proposed several recommendations for network traffic management. Similarly, [5] proposed a new method of monitoring systems. It can provide detailed information based on traffic behavior methods and a history of connected traffic. While comprehensive information on internet traffic used is monitored for analysis.

Qadeer, et al. [6] developed packet sniffer on the Linux platform for Intrusion Detection. The focus of this research is to analyze the bottleneck scenario that arises in the network. Then the next focus is to detect the presence of the software on the network and handle it in an efficient way. Lizarti, et al. [7] discuss traffic analysis in VPN using Simple Network Management Protocol (SNMP). In this study network traffic applications generate reports real-time traffic based on TCP ports and UDP and can be accessed privately with utilizing VPN technology so that it can help network administrators inside monitor and analyze problems that occur on the network.

B. Network Monitoring

Monitoring an operational network can provide a network administrator with information to proactively manage the network and to report network usage statistics to others. Link activity, error rates, and link status are a few of the factors that help a network administrator determine the health and usage of a network. Collecting and reviewing this information over time enables a network administrator to see and project growth, and may enable the administrator to detect and replace a failing part before it completely fails. SNMP is commonly used to collect device information [8].

978-1-5386-8317-0/19/$31.00 ©2019 IEEE

Simple Network Management Protocol (SNMP) was developed to allow administrators to manage nodes such as servers, workstations, routers, switches, and security appliances, on an IP network. It enables network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth. SNMP is an application layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of three elements : SNMP manager, SNMP agents (managed node) and Management Information Base (MIB) [9].

C. *Packet Sniffing*

Packet sniffing is tools that are used as monitoring data packet when a packet crosses a network. There are packet sniffing in the form of software, but there are also hardware-based devices that are installed directly along the network. Sniffer can handle data sent specifically to them. Sniffer can be used legally on the network by system administrators to monitor and solve traffic problems in their own networks. For example, if a computer has a communication problem with another computer, a administrators can view packet from one machine to another and determine the cause of the problem [10].

The packet sniffer consists of the following components [11]:

1. Hardware : standard network adapters .
2. Capture Filter : This is the most important part . It captures the network traffic from the wire, filters it for the particular traffic you want, then stores the data in a buffer.
3. Buffers : used to store the frames captured by the Capture Filter .
4. Real-time analyzer: a module in the packet sniffer program used for traffic analysis and to shift the traffic for intrusion detection.
5. Decoder : Protocol Analysis

Several examples of packet sniffing tools are wireshark kismet, tcpdump, cain and abel, ettercap, dsniff, netstumbler, ntop, ngrep, etherape and kisMAc. Wireshark is a network packet analyzer. A network packet analysis will capture network packets and display data packets as detailed as possible. The user can assume network packet analysis as a measuring device used to check what happens inside a network cable, such as a voltmeter used by an electrician to check what is happening in an electrical cable. In the past, tools like the good were very expensive, exclusive or both. However, with the emergence of the Wireshark all that has changed. Wireshark is one of the best open source analysis data packets available today [12].

III. RESEARCH METHODOLOGY

The system development method used in this study is the Network Development Life Cycle (NDLC), which is a process approach in data communication that describes a cycle that has no beginning and end in observing the network. Like the following stages:

1. Analyzed the need for conducting research, existing problems and analyze network topologies at Pekanbaru Telkom Vocational Schools.
2. Designing a network monitoring schedule on a specific time scale.
3. Conducts research execution (network monitoring), implementation of analysis and recording of the results of monitoring with capture.
4. Evaluation of result monitoring
   Management advice and conclusion see in Figure 1.

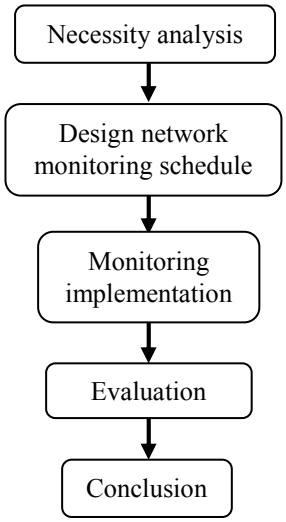

Fig 1. Research Method

A. *Network Topology in Telkom Vocational school, Pekanbaru, Indonesia*

The Internet system provider used at the Pekanbaru Telkom Vocational School is a telkom network. The fiber optic cable from the telkom ISP center is connected at the School Laboratory and then subdivided using access control on the proxy, then directed to the switches and access points of each Laboratory in Schools. The Internet network in Lab also uses a login access system by using a server as a tool to filter data on students and teachers. to find out the increasing number of data access and Internet needs of students and teachers, we analyze the Internet usage traffic at Telkom Vocational Schools based on hypertext transfer protocol (HTTP). For more details see figure 2.

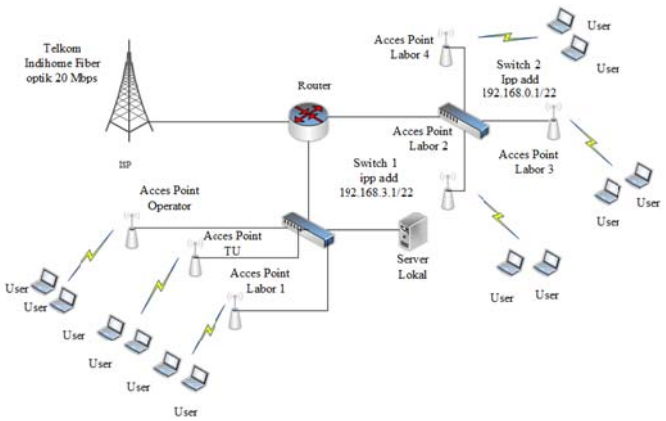

Fig. 2. Network topology in Telkom vocational school

The design of the monitoring scheme that will be carried out in the study uses port lines on routers that are connected to the Internet Service Provider (ISP) provided by Telkom with a bandwidth of 20 Mbps. The router port will be connected to the Personal Computer (PC) monitoring in

order to analyze internet usage traffic at telkom Vocational School. The tools used, will be installed on the PC monitoring tools that are used, namely wireshark. Figure 3 shows the monitoring system scheme.

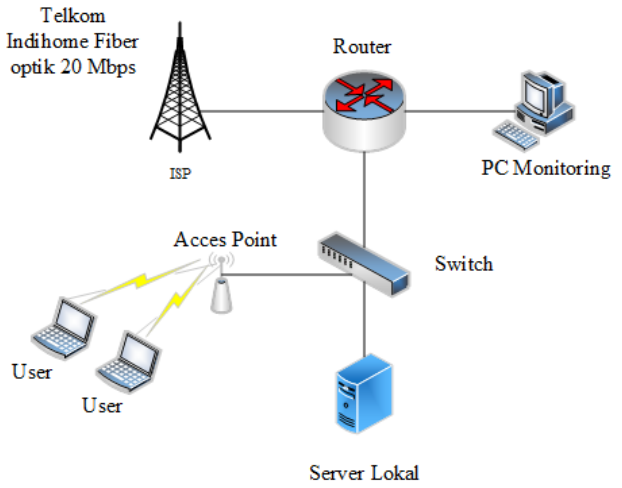

Fig. 3. Monitoring system scheme

To facilitate monitoring at Telkom Vocational Network, user must know the IP address of Switch 1 and Switch 2, see table 1

Table 1. IP Address monitoring

Switch 1	**IP Address**
Lab 1	-
Administration Room	-
Operator Room	192.168.3.1/22
Switch 2	**IP address**
Lab 2	-
Lab 3	-
Lab 4	192.168.0.1/22
Network Hardware	192.168.3.1/22- 192.168.0.1/22

IV. Result and Discussion

In the process of building an optimum network, the results of analysing Internet usage by the user are very much needed. Because the data analysis results can be used to evaluate the design of a network system that is more optimal in managing bandwidth for user requirements. In this research, the researcher analyses Internet usage traffic by using wireshark. These tools used to sniff on routers and proxy to get packets from a network and filter HTTP packet data. Packet Sniffer captures all HTTP requests / responses that are sent between a Web browser and a Web server and displays them in a simple table. For each HTTP request, the information displayed is Host Name, HTTP method (GET, POST, HEAD), URL Path, User Agent, Response Code, Response String, Content Type, Referrer, Content Encoding, Transfer Encoding, Server Name, Content Length , String Cookies, and others. We can easily select one or more lines of HTTP information, and then export it to a text / html / xml / csv file or copy it to the clipboard and then paste it into Microsoft Excel [13].

In this study, researchers conducted a study to analyse the Internet traffic usage in Telkom vocational during two weeks or fourteen days. The results of this study are in the form of traffic from bandwidth usage by users in school. The results of the graph displayed are only the first day, the eighth and the last day. First day's researches were conducted on Monday, October 8, 2018, the highest access time at 10:33 WIB and the bandwidth size accessed by users were 25966 bytes / second, and the average bandwidth speed accessed 637 bytes / second and total bandwidth usage / day 3563328 Bytes (see figure 4)

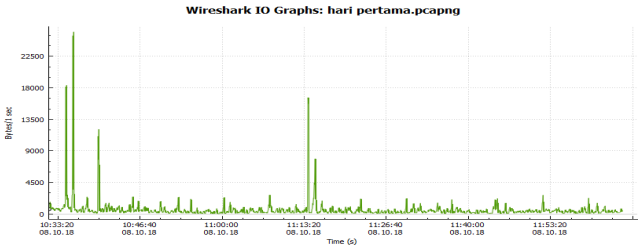

Fig. 4 Result graph of monitoring in first day

Then, the results of the data traffic analysis on the 8th day are carried out on Monday, October 15, 2018, the highest access time is at 10:10 WIB and the bandwidth size accessed by users is 67480 Bytes / second, the average bandwidth speed is accessed 13k Bytes / second and total bandwidth usage / day 138400867 Bytes. See in figure 5.

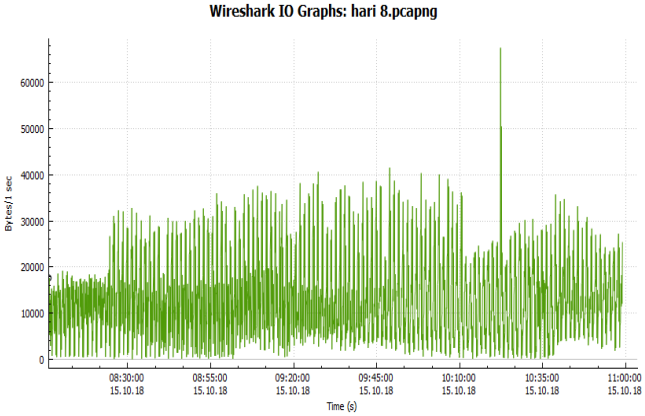

Fig. 5. The result graph of monitoring 8th day

After that, the results of traffic analysis data on day 14 are carried out on Sunday 21 October 2018, the highest access time is at 11:26 WIB and the bandwidth size accessed by users is 35128 Bytes / second, the average bandwidth speed accessed is 2630 Bytes / second and total bandwidth usage / day 62262684 Bytes. See picture 6.

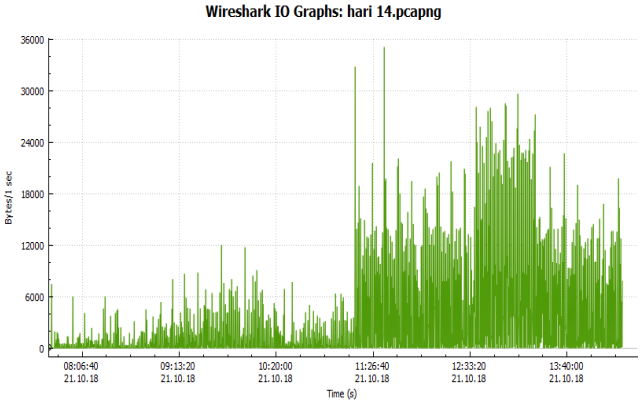

Fig. 6. The result graph of monitoring last day

Based on the results of analysis of internet usage traffic in Telkom vocational school, Pekanbaru for two weeks can be summarized such as data in table 2.

Table 2. Traffic Analysis Results.

Date	Bandwith highest access (bps)	Bandwith average (bps)	Total bandwith access (bps)	The number of IP Address user
8/10/2018	25966	5100	3563328	77
9/10/2018	540483	65536	77.323.912	466
10/10/2018	207313	235520	52566146	141
11/10/2018	3302	3472	561909	52
12/10/2018	57051	107520	27986432	91
13/10/2018	119220	91136	94346555	99
14/10/2018	10808	5870	2744025	38
15/10/2018	67480	108544	138400867	108
16/10/2018	967436	236544	51192592	122
17/10/2018	882388	88064	143385889	135
18/10/2018	42669	59392	95546745	131
19/10/2018	304971	48128	42837893	82
20/10/2018	45108	6611	11366544	90
21/10/2018	35128	21504	62262684	119
Average		13 Mbps		125

The results of the average bandwidth for fourteen days is 13 / Mbps. The list of user ip recorded when accessing the highest and lowest bandwidth is as follows:

1. List of IP users recorded accessing the internet on the school network on October 9, 2018 the number of IPs is 466 users.
2. List of IP users recorded accessing the internet on the school network on October 14, 2018 the number of IPs is 38 users.

V. CONCLUSION

Based on the data obtained, the average bandwidth usage per second is 13 Mbps from an average of 125 users. This means that there are still 7 Mbps spaces that are not used by the user. Nevertheless, if you assume the number of users is 500 users, then the average user gets 40 Kbps, allowing for convenient the Internet browsing access. If for users to access information systems or cloud-based systems, the user needs at least 200 Kbps. While the user for video streaming needs 300 Kbps. Thus, based on the analysis of current traffic data, 20 Mbps is still sufficient for Telkom Vocational school needs, Pekanbaru, although ideally if there are 500 users with medium users, it is better to use 100 Mbps internet bandwidth packages.

REFERENCES

[1] C. N. A. Program, *Introduction to Networks Companion Guide*: Pearson Education, 2013.

[2] A. Siswanto and A. Tedyyana, "Manajemen Bandwidth dan Monitoring Akses Data," in *Seminar Nasional Teknologi Informasi dan Komunikasi*, Medan, 2014, pp. 24-28.

[3] A. Bhandari, S. Gautam, T. K. Koirala, and M. R. Islam, "Packet Sniffing and Network Traffic Analysis Using TCP—A New Approach," in *Advances in Electronics, Communication and Computing*, ed: Springer, 2018, pp. 273-280.

[4] S. Ansari, S. Rajeev, and H. Chandrashekar, "Packet sniffing: a brief introduction," *IEEE potentials,* vol. 21, pp. 17-19, 2002.

[5] S. L. Rosa and E. A. Kadir, "Abnormal internet usage detection in LAN Islamic University of Riau Indonesia," in *Proceedings of the International Conference on Intelligent Science and Technology*, 2018, pp. 17-22.

[6] M. A. Qadeer, A. Iqbal, M. Zahid, and M. R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on*, 2010, pp. 313-317.

[7] N. Lizarti and W. Agustin, "Aplikasi Network Traffic Monitoring Menggunakan Simple Network Management Protocol (SNMP) pada Jaringan Virtual Private Network (VPN)," *SATIN-Sains dan Teknologi Informasi,* vol. 1, pp. 27-34, 2015.

[8] T. Lammle, *CCNA Routing and Switching Study Guide: Exams 100-101, 200-101, and 200-120*: John Wiley & Sons, 2013.

[9] T. Lammle, *CCNA Cisco Certified Network Associate Deluxe Study Guide*: John Wiley & Sons, 2011.

[10] T. King, "Packet sniffing in a switched environment," *SANS Institute, GESC practical,* vol. 1, 2002.

[11] P. Asrodia and H. Patel, "Analysis of various packet sniffing tools for network monitoring and analysis," *International Journal of Electrical, Electronics and Computer Engineering,* vol. 1, pp. 55-58, 2012.

[12] L. Chappell and G. Combs, *Wireshark network analysis: the official Wireshark certified network analyst study guide*: Protocol Analysis Institute, Chappell University, 2010.

[13] M. Belshe, R. Peon, and M. Thomson, "Hypertext transfer protocol version 2 (http/2)," 2070-1721, 2015.