

Comparative Study on Packet Sniffing Tools

Miss. Shraddha Dilip Sarve¹ and Prof. Shubhangi Mahadik²

Student, Master in Computer Application¹

Assistant Professor, Master in Computer Application²

Bharati Vidyapeeth, Navi Mumbai, Maharashtra, India

Abstract: *With the advancement and widespread use of network technology, network administration, maintenance, and monitoring have become increasingly important in order to maintain the network running smoothly and increase economic efficiency. A packet sniffer is used for this purpose. Network monitoring relies on packet sniffing to troubleshoot and log issues. Both network software engineers and network administrators will gain from network activity. There are a few variety of packet sniffers on the market that can be used to do packet sniffing. The subject of this paper is the fundamentals of a packet sniffer; its operating principle; and the numerous packet sniffing tools and how they work, network monitoring and analysis capabilities.*

Keywords: Packet capture, Network Monitoring, Packet sniffer, Wireshark, Tcpdump.

REFERENCES

- [1]. Adeer M.A., Zahid M., Iqbal A., Siddiqui M.R "Network Traffic Analysis and Intrusion Detection Using Packet Sniffer" ICCSN'10 Second International Conference, (2010), Page(s): 313-317(2010).
- [2]. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov. (2007), Page(s): 158-162(2007).
- [3]. McCanne and V. Jacobson. "The BSD Packet Filter: New Architecture for User Level Packet Capture", USENIX Conference, January, Pages 259-270(1993)
- [4]. About soft perfect network protocol analyzer [Online] Available <http://www.softperfect.com/products/networksniffer/>
- [5]. About Tcpdump [Online] Available [http:// www.tcpdump.org/](http://www.tcpdump.org/).