STUDY AND IMPLEMENTATION OF PACKET ANALYZER TO ANALYZE THE TRAFFIC FLOW IN LAN

Prepared by: Mohamed Ibrahim

ABSTRACT

The main goal of this project is to develop an IP packet capture program using Windows Sockets 2.0 API (Application Programming Interface); i.e. eliminating the use of traditional PCAP (Berkeley Packet Capture API/ driver and its derivatives) for Windows. Even if the program does not depend on the PCAP driver, the program will be able to write the captured data to disk in PCAP format. When running this program, it needs to input interface to bind and output file name so that the program can capture running packets and save it to the text file and packet format. The underlying idea here is to capture packets based on two other tools called ngSniff and poorSniff. These are two shareware to use packet capturing. The author coded the application using C and Visual Basic 6.0. The networking bits were done using C and this program will be used in a server in a small office network.