SOFTWARE REQUIREMENTS SPECIFICATION

FOR

NETWORK PROTOCOL ANALYSER



BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI

Submitted By : -

AKHIL KUMAR AGRAWAL 2014A7PS024P

GAURANG BANSAL 2014A7PS128P

SUBHAM KUMAR 2014A7PS121P

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

INTRODUCTION

1.1 Purpose

The purpose of this document is to design a Packet Analyser. Packet analysers can help us understand and ascertain network characteristics such as how data is being communicated, discover network congestions, identify possible attacks or malicious activity and much more. The objective of this project to understand and design a basic model of a Network Protocol Analyser which can help the user to understand the working of Network Communication using Protocol Capturing.

This document is intended for enthusiastic developers who aspire to understand and implement a packet analyzer working and use it as a stepping stone for further development.

1.2 Scope

The AGS is an application which works with the objective of capturing and analyzing packets at various layers, all the way from application layer to link layer protocols. The capturing of packets is done in a passive and non-promiscuous manner. The packets are to be analyzed for the purpose of troubleshooting network problems and checking for malicious behaviour. It is not intended for unethical and malicious activities related to sniffing and violating any user’s privacy.

1.3 Definitions.acronyms and abbreviations

//Packet Analyzer

//Protocols

Acronyms

|  |  |
| --- | --- |
| UDP | User Datagram Protocol |
| TCP | Transmission Control Protocol |
| ARP | Address Resolution Protocol |
| ICMP | Internet Control Message Protocol |
| IGMP | Internet Group Message Protocol |
| IP | Internet Protocol |

1.4 References

// Research papers in their respective formats

1.5 Overview

// To be done in the last, after the SRS is complete

1.6 Overall Description

1.6.1 Product Perspective

1.6.1.1. System interfaces

//To be entered as well

1.6.1.2 User Interfaces

* Command Line Interface with options for the user
* Log Text Files containing the output

1.6.1.3 Hardware Interfaces

* Computer connected to the Internet
* Ethernet Adapter
* WiFi Adapter

1.6.1.4 Software Interfaces

* Operating System

Name: Ubuntu

Version number : 16.04

Source:<https://www.ubuntu.com/download>

This Operating System is required for proper management of hardware and ease of access of resources. This helps in understanding of the

* C Library

Name:netinet

This library contains the constants and the various structures required for getting the appropriate information from the packet headers

1.6.1.5 Memory Constraints

//RAM and Physical memory

1.6.1.6 Operations

The user will be able to select the protocols whose packets he wants to analyze by selecting options provided in the interface.

The user will specify a particular time period from during which he wants to capture the packets, during that time he will be able to see the real time update of packets being captured and read

|  |
| --- |
| 1. |
|  |
|  |
|  |
|  |
|  |

Packet capture software is extensively used as tools for protocol analysis. It is a tool comes handy in analyzing, debugging and testing of a new protocol implementation. The key challenge in writing such software is to collect raw packets directly from the interface cards and parsing them to reveal useful information. In normal network programming through sockets, a software module listens on a particular socket for packets intended for its use, hence for a module wanting to sniff for all packets, Also, each protocol layer performs filtering of the traffic, for example, any TCP control packet will not be passes above the TCP layer, any IP control packet is consumed by the IP layer and so on.

The “software hook”, that we mentioned above, exists, in UNIX as the PF\_PACKET socket (libpcap library) and in Windows as the Winpcap library. In our work we make use of the libpcap library to be able to capture raw packets from the interface. The story does not end at being able to capture raw packet. In fact, it is the most basic step. There are certain hurdles in being able to analyze correctly the raw packets which are nothing but a set of hexadecimal gibberish to the uninformed. There are challenges in being able to serialize the data coming in, in network byte order, for storage in the file systems. Also, a major task is to be able to provide an easy to use and elegant user interface for running the software as well as present the packet data in a more human readable form.

It has been designed to be the stepping stone for further design of more complicated tools and also a learning experience for novice programmers to design and implement their own network software. It is basically the foundation bed for more advanced innovations in the future.

1.5 Product Overview

The project will be implemented using C language. Following are some of the functionalities we will implement:

Basic Functionality:

1 Network Monitor [Basic packet capture]

2 Packet Filtering

3 Network Utilities [Ping, TCP Statistics, UDP Statistics]

4 Packet Analysis

|  |  |
| --- | --- |
|  | SPECIFIC REQUIREMENTS |
| 2.1 | External Interface Requirements |
|  | 2.1.1 |
|  | 2.1.2 |
|  | 2.1.3 Software Interfaces  Libpcap Library  Wireshark  Npcap(update to Winpcap) [ Extension to Windows] |
|  | 2.1.4 Protocols  Application Layer: HTTP, FTP, SMTP  Transport Layer: TCP, UDP, DCCP  Network Layer: ICMP, DDP  Link Layer: ARP |
|  |  |
|  |  |
| 2.2 | Network Analysing:  It monitors data flowing over computer network links in real time. It can be a self-contained software program or a hardware device with the appropriate software or [firmware](https://www.lifewire.com/definition-of-firmware-817708) programming. Also sometimes called "network probes" or "snoops," [monitors network traffic](https://www.lifewire.com/what-is-network-monitoring-817816), taking snapshot copies of the data but without redirecting or altering it. In standard, non-promiscuous sniffing, a host is sniffing only traffic that is directly related to it. Only traffic to, from, or routed through the host will be picked up by the sniffer. |
|  | Working:  Packet sniffers work by intercepting and logging network traffic that they can 'see' via the wired or wireless network interface has access to on its host computer.  On a wired network, what can be captured depends on the structure of the network.Once the raw packet data is captured, the packet sniffing software must analyze it and present it in human-readable form so that the person using the packet sniffing software can make sense of it. The person [analyzing the data](https://www.lifewire.com/free-packet-sniffer-software-2486807) can view details of the 'conversation' happening between two or more nodes on the network.  Applications:  Network technicians can use this information to determine where a fault lies, such as determining which device failed to respond to a network request. Sniffers are great tools for diagnosing down-in-the-weeds network problems. |
|  |  |