Sniffer(Packet Analyzer)

**September 17, 2016**

# Brief Problem Statement:

Sniffer is a network protocol analyzer, it lets you see what’s happening on your network at a microscopic level .It is a computer software that can intercept and log traffic passing over a digital network. It captures all the packets and displays you in real time.

# System Requirements:

1. The amount of resources sniffer needs depends on environment and on the size of the capture file we are analyzing.
2. **Python 2.5+:** python 2.5 version+ will be used to develop the project.
3. **More RAM should be available:** Larger capture files require more RAM.
4. Uses Pcap for packet capture.
5. **UNIX:** Will be compatible with UNIX operating systems.

# Users Profile:

1. Developers use it to debug protocol implementations.
2. Network administrators use it to troubleshoot network problems.
3. People use it to learn Network protocol internals.
4. Network security analysists use it to troubleshoot security issues with network protocols.

# Feature Requirements:

|  |  |  |  |
| --- | --- | --- | --- |
| s.no | Use case name | Description | Release |
| 1 | Capture | Capture live packet data from a network Interface. | R1 |
| 2 | Create | Creating packet for the purpose of testing. | R1 |
| 3 | Open | Open files containing packet data captured with the help of the pcap library. | R2 |
| 4 | Display | Display packets with detailed description. | R2 |
| 5 | User interface | Display the packets on the interface |  |
| 6 | Save | Saves the packets that are captured. | R2 |
| 7 | Import | Import packets from text files containing dumps of packet data. | R3 |
| 8 | Export | Exports packets in different possible formats. | R3 |
| 9 | Filter | Filter packets on some constraints. | R3 |
| 10 | Search | Search option to see packets traffic under constraints. | R4 |
| 11 | analyze | Analyze the network traffic based on the data captured. | R4 |

**Use case description**

|  |  |
| --- | --- |
| Use Case Number: | UC-01 |
| Use Case Name: | Capture |
| Overview: | The analyzer should be able to capture the packets (using pcap library ) that are being broad casted in that particular network. |
| Actors: | User <<Client>> |
| Pre condition: | The user must set the network interface into promiscuous mode. In promiscuous mode, the NIC will pass all frames it receives to the CPU, instead of just those addressed to the NIC’s MAC address. |
| Flow: | The user after setting the NIC into promiscuous mode ,  tries to capture the packets being broadcasted  by executing the code. |
|  | Alternate flow:  if not captured , it means that there is an error in our packet capturing. |
| Post Condition: | The packets get saved into a file. |

|  |  |
| --- | --- |
| Use Case Number: | UC-02 |
| Use Case Name: | Create |
| Overview: | The analyzer should be able to create packets that are destined such that they are captured by our sniffer. |
| Actors: | User <<Client>> |
| Pre condition: | The user must be knowing how to capture packets |
| Flow: | The user creates a packet  assigns all the header fields  sends the packet  this is captured by the sniffer |
|  | Alternate flow:  if not captured , it means that there is an error in our packet capturing. |
| Post Condition: | There is no other flow that depends on this.  This is a part of debugging. |

|  |  |
| --- | --- |
| Use Case Number: | UC-03 |
| Use Case Name: | save |
| Overview: | The Captured packets are saved ina file |
| Actors: | User <<Client>> |
| Pre condition: | The user must collect the data first before saving |
| Flow: | The user tries to capture the packets being broad casted.  Then saved them in a file. |
| Post Condition: | The file now can be opened to view the packets. |

|  |  |
| --- | --- |
| Use Case Number: | UC-04 |
| Use Case Name: | open |
| Overview: | The analyzer should be able to open the packets that are being saved. |
| Actors: | User <<Client>> |
| Pre condition: | The captured packets are saved into a file |
| Flow: | The user captures the packets.  Saves them into a file.  Opens the file to view the packets. |
| Post Condition: | The packets present in the file have to be displayed in raw format. |

|  |  |
| --- | --- |
| Use Case Number: | UC-05 |
| Use Case Name: | display |
| Overview: | The analyzer should be able to displaythe packets that are saved in the file. |
| Actors: | User <<Client>> |
| Pre condition: | There must be packets saved before hand. |
| Flow: | The user checks if there are any packets present in the file to be displayed.  If yes, displays the packets. |
|  | Alternate flow:  if not saved , throws error. |
| Post Condition: | The packets get displayed. |

|  |  |
| --- | --- |
| Use Case Number: | UC-06 |
| Use Case Name: | Import and export |
| Overview: | The user can get data from other files or send the existing data into other files. |
| Actors: | User <<Client>> |
| Pre condition: | The user have the data either in packet captured format or in the other format so that he can export ot import respectively. |
| Flow: | The user after capturing the data , exports it into file of other format or vice viersa. |
| Post Condition: | The packets get saved into a file (regular farmat or exported format). |

|  |  |
| --- | --- |
| Use Case Number: | UC-07 |
| Use Case Name: | Filter |
| Overview: | The analyzer should be able to filter the capture the packets by applying a particular filter. |
| Actors: | User <<Client>> |
| Pre condition: | There must be packets of that type in the network so that they get filtered. |
| Flow: | The user while capturing the packets,  before saving them ,  can apply a filter ( like , capture only Ethernet packets) |
|  | Alternate flow:  if not required , can capture all packets. |
| Post Condition: | The packets get saved into a file. |

|  |  |
| --- | --- |
| Use Case Number: | UC-08 |
| Use Case Name: | Analyze |
| Overview: | The user must be able to analyze the network protocols and should be able to make decisions based on the data captured. |
| Actors: | User <<Client>> |
| Pre condition: | As seen above , there has to be enough data so that more appropriate decisions can be made. |
| Flow: | The user takes all the data that is captured.  Applies algorithms and other parameters and makes decisions. |
| Post Condition: | There is no flow that depends on the data analyzed.its up to the user what he wants to do later. |