Packet Analyst

Requirements:

To develop Packet Capturing tool in Linux which must be capable of:

1. Capture and display/log details of all incoming packets
2. Display/log to be formatted
3. Support for filters - user should be able to specify to log only packets from certain parameters like:
   - IP address
   - Protocol type -
     Port number
4. Maintain and print statistics whenever requested.

Packet Capture – Identifying the utility

Options found :

1. Raw Socket
2. Winpcap library

Winpcap over Raw Socket:

1. The Packet Capture(pcap) library provides a high level interface to packet capture systems.
2. Winpcap library provides an internal buffer for storing a number of packets along with filtering ability while capturing packets from the interface.
3. Winpcap provides the timestamp information of each packet.
4. Winpcap provides a list of interfaces on the system that can be used for live capture of packets
5. Winpcap provides an API for setting the NIC to promiscuous mode with ease.

Multi-threading

The application requires simultaneous capture and display of packets, hence, 2 threads are created from the main thread. The main thread is used to GUI implementation.
In order to provide inter-process communication between these threads, message queue is used. In addition, message queue also balances the speed gap between the display and capture threads.

GUI

Since this application involves a lot of user interaction, a better user experience can be provided by GUI.

Options found:

1. HTML.
2. GTK
3. Tkinter

Why GTK?

HTML requires an IPC mechanism for the interaction between the GUI code and the C code. Tkinter requires the C code to be imported as a subprocess in a script. However, GTK allows direct extension of the C code to support GUI. The GTK APIs could be directly written in the C code. Also, the GTK has a front end tool called Glade for developing the GUI layout.

GTK for multi – threaded application

For GTK to be incorporated in a multi – threaded application, we need to have a GDK thread safe mechanism. Wherever, the GTK calls are made, the code must be enclosed within gdk_threads_enter() and gdk_threads_leave().