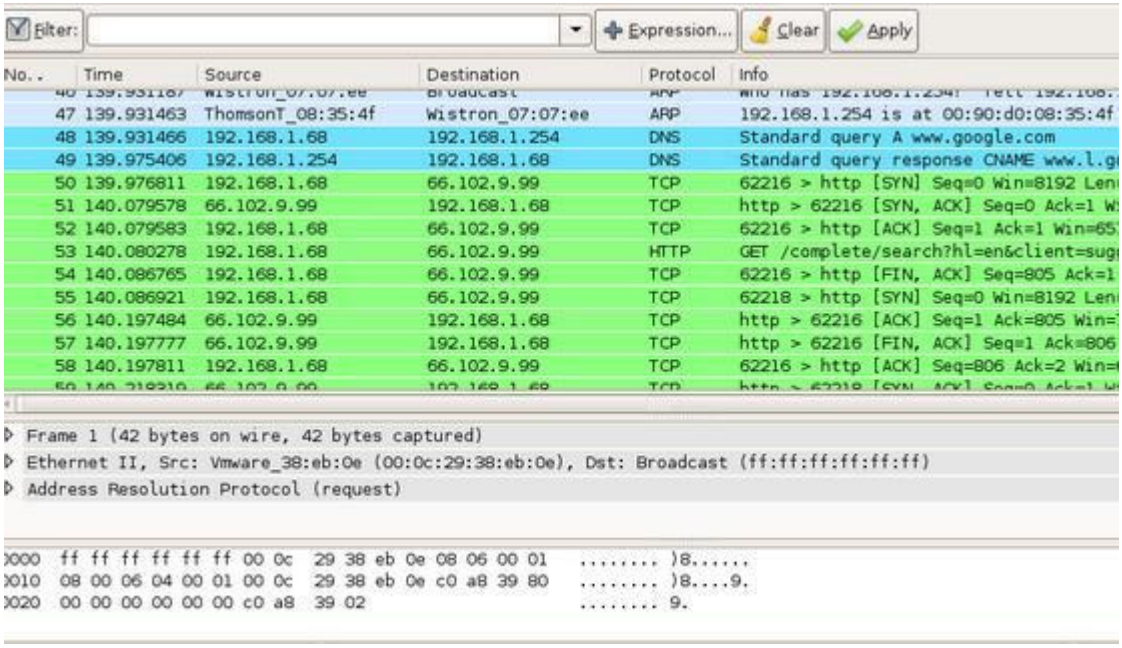
Network Packet Sniffer Java Project

Network packet sniffer or simply packet sniffer is a packet analyzer software that monitors all network traffic. The proposed project is implemented in Java programming language, and using this application admin of the system can capture network packet and analyze data received/sent from/to the network.

Developed as a desktop application, packet sniffer facilitates web-based monitoring of network packets which are traveling over the system network. The primary data captured by this software is the packets source and destination addresses.

In this article, the project has been briefly discussed explaining its scope, features, and system specifications. Full project synopsis along with complete Java source code can be downloaded from the link below. Documentation, project report, and ppt of this project are not available at the moment.

About Network Packet Sniffer:



Network packet sniffer is simply a web-based application that monitors all traffic over a network. Unlike other standard network hosts that only track traffic sent particularly to them, this software captures each packet, eventually decoding and analyzing its data as the data streams flow across the system network.

This project, developed in Java, shows mainly two things:

1. how real-time network connection behavior can be modeled as chromosomes
2. how the parameters in genetic algorithm can be defined in this respect.

The objective of the proposed project is to create a set of rules during run time so that hackers and intruders cannot attack the system software with virus and malwares. So, for networking purposes, network packet sniffer monitors all LAN data packets and mirrors all packets that are being passed through a shared bus.

Existing System:

In the existing system, network administration and monitoring is done by an admin. Admins are mainly assigned the task of identify, diagnosing, and solving network problems, but this overall becomes a very tedious task as network administration needs to put a lot of effort to identify traffic.

Additionally, the existing system is very time taking and uneconomical. There is no such thing as automatic network control because the network administrator must always be present to monitor traffic over the network.

Proposed System:

As a network analyzer, the proposed packet sniffer software makes it easy to identify, diagnose, and solve network problems. With the software's information-rich and intuitive tab views, it can track all incoming and outgoing calls over the network.

The key **features** of packet sniffer application are listed below:

- real-time packet capturing
- 24×7 network monitoring
- advanced protocol analyzing
- comprehensive packet decoding
- automatic expert diagnosing
- complex network analyzing
- conduct packet level analysis
- solve network problems

Modules Used:

Network packet sniffer is made up of 3 **modules**:

1. **User Interface Module**: It provides all the Graphical Interfaces components required by the user to interact with the system.
2. **Packet Analysis Module**: It analyzes all the incoming packets into the desktop, and upon proper identification and clarification, passes the data into statistics module.
3. **Statistics Module**: This module is responsible for all the necessary calculation based on the data, information, or content received from packet analysis module. It then produces information that can be understood by the system user.

System Specifications/Requirements:

Hardware Specifications:

- Processor : Pentium IV with 800 MHZ Clock Speed
- Hard Disk : 40 GB
- RAM : 256 MB
- Network Interface Card : 32 bit PCI/ISA Ethernet or Modem

Software Specifications:

- Operating System : WINDOWS 98/XP or LINUX
- Languages/Packages : Java (Swings)
- JDK version : JDK1.6.0
- Communication Protocol : HTTP Protocol

So, in conclusion, with the proposed network packet sniffer software, network administrator can monitor the packets anywhere throughout the the world. System performance will be enhanced and traffic will be controlled. Further, reports can be generated immediately and graphical data is readily available to analyze the network.