

# CSE-556 Internetworking Fall 2002

## Laboratory Assignment 2

### **Objective**

The objective of this laboratory assignment is to get you familiar with the process of capturing packets from a network using a packet sniffer and analyzing them.

### **Theory**

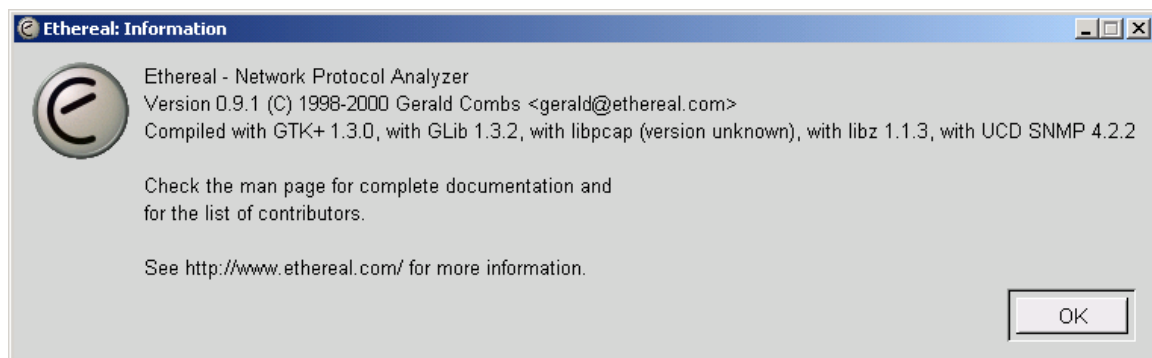
A packet sniffer is a tool that allows one to capture packets from a network link and analyze them. This is very useful in two situations:

1. Learning about networking protocols and
2. Troubleshooting in case there is a problem in network communication

A packet sniffer works in the promiscuous mode of a NIC and passes all the frames being transmitted on the wire to the NIC driver software. Normally a NIC would discard frames not addressed to the MAC address of the NIC. However, in promiscuous mode all frames, regardless of the destination MAC address are passed on to the NIC driver.

Simply capturing all the frames from the network generates too much data to be any useful. That is why a packet sniffer allows one to define rules or filters which control the packets that may be captured. This filters out all the unwanted traffic. For example, if one is interested in looking at the ICMP traffic, a filter will be defined to only capture ICMP traffic.

There are many well known sniffer software packages such as Network Monitor from Microsoft, SnifferPro from Network Associates, TCPDUMP which is an open source packet sniffer for mostly UNIX-based systems and Ethereal which is a multi-platform GUI-based packet sniffer which is also open source. We shall be using Ethereal for this lab.







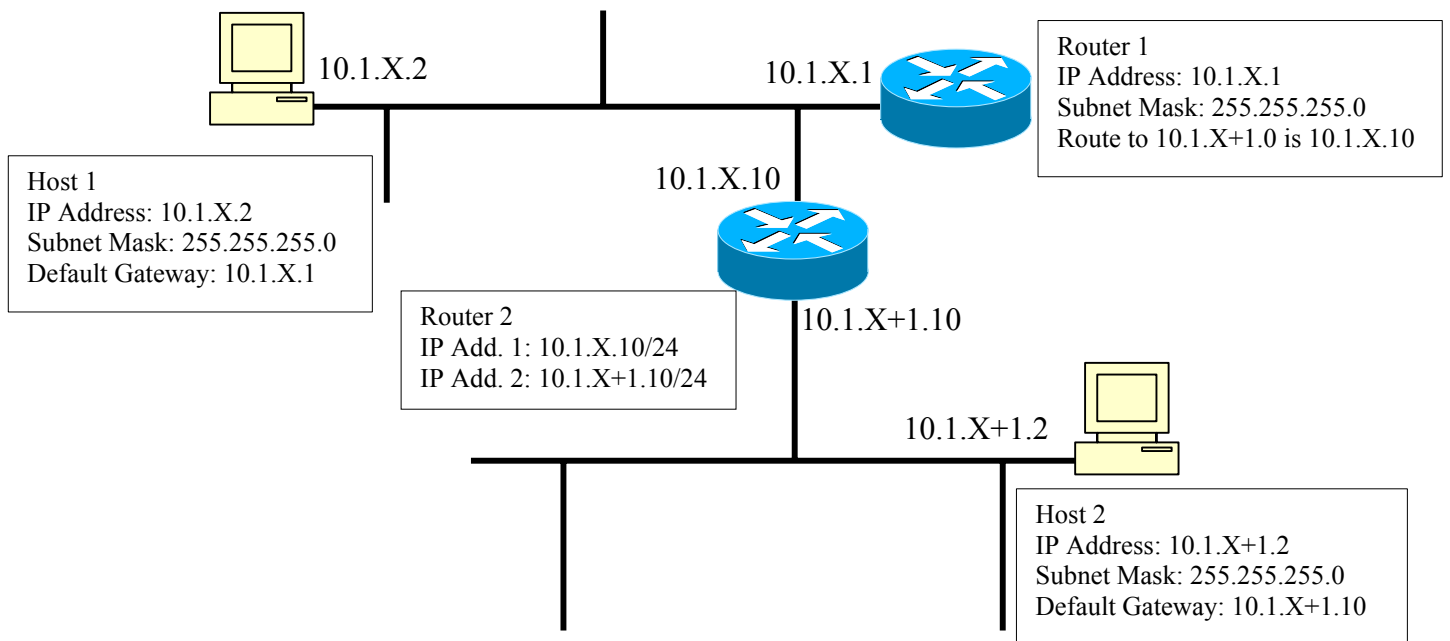


10. What are the Type and Code values for ICMP Echo Request message and Echo Reply messages, respectively? Also list the steps you undertook to achieve this task.

11. How does a UDP segment look like? Please indicate the names of the fields in a UDP message along with their size. Also list the steps you undertook to achieve this task.

12. How does a TCP segment look like? Please indicate the names of the fields in a TCP message along with their size.

13. Set up a network topology as shown in the figure below and capture the ICMP Router Redirection message. What are the Type and Code values for this ICMP message. List the steps you undertook to achieve this task.



14. Capture a complete request and response from your web browser to the web server LABSERVER. Based on it, list the important parts of HTTP request and response messages.