

CDA 4506 - LAB 1

Network Protocols Analyzers

Ethereal

Objective: To introduce you with the basic features of *Ethereal*, one of the most popular open source network protocol analyzers.

CONFIGURATION: Lab LAN.

EXPERIMENT:

Ethereal Set Up

1. Start Ethereal.
2. Set up the following trace capture options
 - a. Ethernet interface.
 - b. 68 bytes.
 - c. Capture packets in promiscuous mode.
 - d. Filter all packets but the ones send to and from ??.??.?
 - e. Save trace in two files rotating them every 10 seconds.
 - f. Display packets as captured.
 - g. Capture for 600 sec.

Packet capture

1. Run server at ??.??.?
2. Run client at ??.??.?
3. Transfer 6 numbers
4. Wait for 6 min.

Examining the trace

1. Open the first file
2. Highlight the fifth packet
 - a. Expand the Internet Protocol Layer.
 - b. Identify the version, header length and the differentiated service field.
3. List packets by protocol.
4. Display a summary of the trace.
5. Display the SSDP (Simple Service Discovery Protocol) statistics.

Resources

<http://www.ethereal.com>

http://www.leg.state.fl.us/Statutes/index.cfm?mode=View%20Statutes&SubMenu=1&App_mode=Display_Statut_e&Search_String=&URL=CH0815/Ch0815.HTM

Reference

Matthews J. Computer Networking: Internet Protocols in Action. Wiley. 2005.

IMPORTANT NOTE

When you capture packet in promiscuous mode on a shared network (ours is a private one) you may capture sensitive information being transmitted by others. Therefore, it is essential that you have permission of the network administrator and preferably the consent of network users before capturing packets in promiscuous mode. In the State of Florida, disrupting network traffic is a 2nd/3rd degree felony, punishable with up to 15 years in prison and/or fines.