Chapter VII

Ethereal: A Tool for Making the Abstract Protocol a Concrete Reality

David Bremer, Otago Polytechnic, New Zealand

Abstract

Learning the nature of data communication and networks requires understanding of how a theoretical protocol is implemented as actual communication. Taking ARP as a simple example, it is one thing to be able to understand its purpose and operation from readings and lectures. It is another thing entirely to be able to identify the actual ARP traffic from a sample of packets, identify any unusual behavior, and perform troubleshooting activities based on previous practical experience. A theoretical understanding may be enough to describe a particular aspect of networking, perhaps even enough to pass an exam. Practical knowledge, however, shows a deeper understanding that comes from actual experience with the protocol, beyond that of reading and discussion. One issue for educators in the field of networking is the problem of giving the students an “up close and personal” interaction with protocols that are so heavily immersed in theory. How do we make the theoretical protocol a more concrete reality for the students?
Learning Objectives

After completing this chapter, you will be able to:

- Recognise the difficulty that students face in becoming familiar with networking protocols when approached from a purely theoretical perspective.
- Explain how a packet sniffer tool such as Ethereal can be used to make the protocols more accessible to students and ease the learning process.
- Critically consider one example for designing a series of related lessons.
- Suggest further enhancements to laboratory activities that make use of packet analysis.

Introduction

Learning the nature of data communication and networks requires understanding of how a theoretical protocol is implemented as actual communication. Taking ARP as a simple example, it is one thing to be able to understand its purpose and operation from readings and lectures. It is another thing entirely to be able to identify the actual ARP traffic from a sample of packets, identify any unusual behavior, and perform troubleshooting activities based on previous practical experience.

A theoretical understanding may be enough to describe a particular aspect of networking, perhaps even enough to pass an exam. Practical knowledge, however, shows a deeper understanding that comes from actual experience with the protocol, beyond that of reading and discussion. One issue for educators in the field of networking is the problem of giving the students an “up close and personal” interaction with protocols that are so heavily immersed in theory. How do we make the theoretical protocol a more concrete reality for the students?

Background and Motivation

Within the field of general education, it is fairly well established that it is desirable to have students work with a “real” system in order to learn the theoretical foundations of that system. Proponents of making the theoretical concrete include Dewey (1987), Kolb and Fry (1975), and Papert (1980). These educationalists advocated the avoidance, or perhaps the postponement, of actually