Ethereal (WireShark) Packet Analyzer

Bijan Jabbari, PhD

November 26, 2007

Downloading and Installing Ethereal

- Wireshark is the new name for Ethereal (due to trademark issues they no longer use the term Ethereal). However, for simplicity these charts may still refer to Ethereal.
- To download and install Ethereal/Wireshark, go to:

  http://www.wireshark.org/download.html

  (as of Nov 2007, the current stable release of Wireshark is 0.99.6.)
- You can go to one of the listed sites for downloading and follow the instructions
  - For Executable Ethereal, just download "wireshark-setup-*x.y.z*.exe"
- In addition to executable Ethereal, you will need to download and install another package: Windows Packet Capture (WinPcap) library
  - To download and install the WinPcap driver (WinPcap version 4). The latest stable WinPcap version is 4.0.2 recommended), go to the following location:

  http://winpcap.mirror.ethereal.com/install/default.htm

- Enjoy Ethereal (Wireshark) as a great learning tool!

Note: The WinPcap is needed to capture live network traffic

What is WinPcap?

- Traditionally Unix has provided a number of network programming library as tools for packet analysis
- An important and widely used library is **libpcap** which uses a set of Unix kernel functions known as Berkeley Packet Filter (BPF)
- Libpcap is a network capture library for capturing and sending network packets
- For Windows-based platforms WinPcap is used as a network programming API
- WinPcap is a packet capture library that exports a set of functions that are libpcap compatible
- The API component of WinPcap is Packet.dll which provides access to the functions of the BPF driver

What is Ethereal?

- Ethereal is a free tool for network protocol analysis
  - for Unix and Windows platforms
- It allows interactive browsing (via a GUI), viewing summary or detailed information, and analysis of data, on a packet basis, captured from a live network or a file
- Live data can be read from Ethernet, PPP, IEEE 802.11, and loopback interfaces (on some platforms)
- Features include a display filter language and the ability to view the reconstructed stream of a TCP session
  - read capture files from tcpdump (libpcap)
  - data display can be refined using a display filter
  - display filters can also be used to selectively highlight and color packet summary information
  - capture files can be programmatically edited or converted via command-line switches to the "editcap" program