Tool release: P4 to Wireshark packet dissector

Georgios Nikolaidis
Barefoot Networks
gnikolaidis@barefootnetworks.com

Networks engineers have been using libpcap to capture network traffic for years. The packet captures are helpful for analyzing the behavior of networked systems, devices, and protocols. The captures become even more valuable when they are fed into Wireshark, a useful tool that makes analysis more visual and easy.

As P4 is adopted by networking software and equipment, developers are able to quickly prototype new protocols. Part of that is coming up with new or modified header definitions. Unfortunately, these modified headers are not recognized by Wireshark and adding support for them is non-trivial. To that end, we present a new tool that allows developers to build a Wireshark packet dissector out of a P4 header definition.

This tool (currently at https://github.com/yo2seol/P4-Wireshark-Dissector) will be released in P4lang and will be incorporated into p4app. It allows developers to quickly analyze traffic that uses their new protocol headers while using the concise header definition of P4.