Enterprise Traffic Analysis

Andrei Gurtov
Centre for Wireless Communications
University of Oulu, Finland
gurtov@ee.oulu.fi

Abstract

The complexity of modern enterprise networks is ever-increasing, and our understanding of these important networks is not keeping pace. Our insight into intra-subnet traffic (staying within a single LAN) is particularly limited, due to the widespread use of Ethernet switches that preclude ready LAN-wide monitoring. We have recently undertaken an approach to obtaining extensive intra-subnet visibility based on tapping sets of Ethernet switch ports simultaneously. However, doing so leads to a number of measurement calibration issues that require careful consideration to address. First, one must correctly account for redundant copies of packets that appear due to switch flooding, which if not accurately identified can greatly skew subsequent analysis results. We show that a simple, natural rule one might use for doing so in fact introduces systematic errors, but an altered version of the rule performs significantly better. We then employ this revised rule to aid with calibration issues concerning the fidelity of packet timestamps and the amount of measurement loss that our collection apparatus incurred. Additionally, we develop techniques to "map" the monitored network in terms of identifying key topological components, such as subnet boundaries, which hosts were directly monitored, and the presence of "hidden" switches and hubs. Finally, we present initial analyses demonstrating that the magnitude and diversity of traffic at the subnet level is in fact striking, highlighting the importance of obtaining and correctly calibrating switch-level enterprise traces [1,2].

Index Terms: Trace calibration, enterprise networks, network traces, switchbased packet capture.

REFERENCES

[1] B. Nechaev, V. Paxson, M. Allman, A. Gurtov, On Calibrating Enterprise Switch Measurements, in Proc. of ACM SIGCOMM Internet Measurement Conference, November 2009.
[2] B. Nechaev, M. Allman, V. Paxson, A. Gurtov, A Preliminary Analysis of TCP Performance in an Enterprise Network, in Proc. of Internet Network Management Workshop/Workshop on Research on Enterprise Networking, (INM/WREN '10), April 2010.