Reading Report #6
Paper: Route Flap Damping Exacerbates Internet Routing Convergence
Student: Shuo Yang

The paper heavily focuses on the harmfulness of route flap damping (RFD) and shows strong evidence and analysis of how and why RFD exacerbates Internet routing convergence. However, it only mentions a simple solution for both withdrawal and announcement triggered suppression which is selective RFD. More works needs to be done to follow up their work.

Regardless the harmfulness introduced by RFD, the Internet still benefits from it because RFD can suppress route changes (unstable routes) caused by link flaps. Completely turning off RFD seems to be a bad idea because it may cause more instability of the Internet routing system. The very question we need to ask is: "can we improve RFD algorithms or parameters or policies to accurately distinguish between flapping routes and normal routes so as to make flap damping more effective?".

Among RFD algorithms, parameters and policies, it seems that adjusting parameters would be the simplest approach. Each ISP has its own default route flap damping parameter settings, for example, **Table 1** mentioned in the paper. There are two parameters in the table are regarding to penalty threshold, one is suppression threshold, the other one is reuse threshold. The setting of these two parameters can affect the results of RFD. For example, if we increase the suppression threshold while decreasing reuse threshold, we will end up suppressing less routes. Our goal is to target those unstable routes resulted from link flaps that cause long-term instability of the Internet. We can assume that such unstable routes only take a small portion of the entire Internet routing system. We can verify this assumption by gathering and measuring the real RFD data. But intuitively it makes sense because route flapping are caused by pathological conditions, such as hardware errors, software errors, configuration errors, intermittent errors in communications links, etc. These errors occur with relatively low probabilities. Given this assumption, by increasing the suppression threshold and decreasing the reuse threshold, on the one hand, leads to less suppressed routes, on the other hand, it actually increase the probability of hitting the targets. Because those heavily flapped links tend to produce a burst of routing updates, thus lead to high penalties. Therefore, increasing the suppression threshold lets us capture those link flaps more accurately. On the other hand, those normally-behaved routes (e.g, routes for BGP path exploration, routes to a prefix that is withdrawn exactly once and re-announced) can be filtered because their penalty values cannot be high enough to exceed the suppression threshold.

The benefits of doing this are: 1) it targets those heavily flapped links and eliminates their impact to the Internet routing system; 2) it is very easy to implement since it simply requires changing of parameters. The downside, though, is that we have to miss those targets who are less severe but still contribute to instability of the Internet.

More intelligent work can be done to address such downside. It would be ideal if those parameters are dynamically adaptive under different conditions. Though it requires deep understand of the Internet topology and routing system.