

Tracking Heavy-hitters

Keeping a state – context – per each flow is an essential task of most network devices such as stateful firewalls, IDS, monitoring probes, QoS appliances and routers. Due to an excessive amount of concurrent flows, keeping per flow state is a challenge. In particular, a flow memory must be large and fast to meet the wire-speed performance. The network measurement studies have showed that a small percentage of flows account for a large share of the traffic (so called heavy-hitters). We propose an adaptive flow cache that utilizes this characteristic to optimize a flow cache management system. A replacement policy is constantly evolved in order to allow for keeping states of heavy-hitters in the flow cache while removing states of low rate flows. This approach proves useful as it allows to

- track heavy-hitters since the start-of-the-day
- stateful and seamless monitoring
- reduce memory consumption

Replacement policy	Cache miss		
	>0.1%	0.1%..0.01%	0.001..0.001%
LRU	28%	27%	15%
SLRU	15%	17%	14%
S3LRU	5%	15%	21%
GARP	3%	7%	13%

The results show that the evolved (GARP) replacement policy performs significantly better to well-known RPs. Only few heavy-hitters which account for more than 0.1%, 0.01% and 0.001% of link capacity witnessed any cache miss.

Published papers:

M. Zadnik et al., Tracking elephant flows in internet backbone traffic with an fpga-based cache, in 19th International Conference on Field Programmable Logic and Applications. Prague, CZ, 2009.