LoLa & ACME STAR

Thomas Fossati, Diego De Aguilar Cañellas

(Nokia, TID, MAMI Project)

Latency-Loss Tradeoff (LLT)

Latency Loss Tradeoff PHB Group
draft-you-tsvwg-latency-loss-tradeoff-00

Abstract

   This document defines a PHB (Per-Hop Behavior) group called Latency
   Loss Tradeoff (LLT). The LLT group is intended to provide delivery
   of IP packets in two classes of services: a low-loss service (Lo
   service) and a low-latency service (La service). The LLT group
   enables an application to request treatment for either low-loss or
   low-latency at a congested network link.

DiffServ made simple

- LLT is a DiffServ (RFC 2475) marking scheme that provides a radical simplification of the DiffServ model
- Traffic belongs to one of two classes:
  - loss-sensitive (Lo), or
  - latency-sensitive (La)
- That's it: mark your traffic appropriately and let the network do the right thing

Explicit cooperation from endpoints

- The difficult part is convincing applications that marking their (encrypted) packets appropriately provides an advantage to them

- The main reason why we are doing this is to create the experiments that allow us to understand whether this mechanism actually works in practice

- (And resume a conversation that was interrupted after the MarNEW workshop and the ACCORD BoF.)

Saturday

- We have the flow mix and queueing already in place
- So the focus at this round was on data analysis:
    - Run a flow mix through the queues, take raw packet captures at various places, correlate them when needed, visualise interesting stats
    - In particular, queueing latency and drop patterns in relation to the flow mix
- In practice a couple hundred lines of tshark, Awk and R (the latter was a first for me and I have enjoyed it a lot)

ACME STAR

ACME Working Group   Y. Sheffer
Internet-Draft   Intuit
Intended status: Standards Track   D. Lopez
Expires: December 18, 2017   O. Gonzalez de Dios
                                                       A. Pastor Perales
                                                        Telefonica I+D
                                                             T. Fossati
                                                                 Nokia
                                                         June 16, 2017

     Use of Short-Term, Automatically-Renewed (STAR) Certificates to Delegate
                        Authority over Web Sites
                       draft-ietf-acme-star-00

Abstract

   This memo proposes an ACME extension to enable the issuance of short-
   term and automatically renewed certificates. This allows a domain
   name owner to delegate the use of certificates to another party,
   while retaining the capability to cancel this delegation at any time
   with no need to rely on certificate revocation mechanisms.

Automate certificate renewal

- Extension to the ACME protocol to automate certificate renewal
- A generally useful extension, that we'd like to use in combination with draft-sheffer-acme-star-request to allow a CDN / Cloud service to obtain certificates for HTTPS delivery bearing the content provider name

Sunday

- Diego has worked (remotely) on the ACME STAR code extending Boulder and Certbot, while I did the STAR LURK bits from scratch.

- There are still some moving parts (especially on my side), but we have enough beef to start integrating the two parts in an end-to-end demo that comprises a portable mini-CDN with DNS based redirection and HTTPS delivery

- This work has just started, will try to have the setup complete by IETF 100