

Traffic Shaping

mit Linux

Tobias Geiger

Was ist Traffic Shaping?

Traffic Shaping erlaubt es, den Ausgehenden Netzwerkverkehr an einem Netzwerkinterface zu beeinflussen, damit die Austrittsgeschwindigkeit dem Gegenüberliegenden Kommunikationspartner angeglichen werden kann. Ausserdem erlaubt es Vertragsbedingungen (SLA's) zu implementieren, und indirekt (zentral implementiert) auch Downstreamkapazitäten einzuteilen.

Einordnung im Netzwerk-Stack

- NACH Routing
- NACH Netfilter

d.h. die Traffic-Shaping-Queue ist die unmittelbar letzte 'Station' eines Packetes bevor es an das Netzwerkinterface zum versenden gegeben wird.



Prinzipien des Traffic Shaping

1. Wahl der Queueing-Discipline (=qdisc)

Std. unter linux/windows: pfifo

2. Klassifizierung des Traffics



WAS soll gequeued werden?

= Klassifizierung:

Einteilung der Pakete in die gewünschten Klassen.

Dies geschieht z.B. Anhand:

- fw-mark (iptables-Mark)
- u32 (anhand Eigenschaften im IP Packet)
- route
- Rsvp
- tcindex (DSCP)



WIE soll der Traffic behandelt werden?

Classfull qdisc (=Queuing Discipline, innerhalb welcher Klassen gebildet werden können)

- CBQ
 - Komplizierte Implementation
 - Gut skalierbar (mit gewisser Obergrenze)
 - HTB
 - Einfache Implementation
 - Mittlerweile besser skalierbar als CBQ
 - HFSC
 - (noch) relativ Komplizierte Implementation
 - Vorteil: Garantierte Delayzeiten durch entkopplung von
 - Delay und Bandbreite mittels sog. „Servicekurven“
-
-

Classless qdiscs (=Reine Queue, ohne konfigurierbare Klassenstruktur)

- PFIFO

- WFQ

von Cisco entwickelte qdisc

Emuliert TDM

- SFQ (Stochastic Fairness Queue)

Flow-basierte interne Klassen

Versucht Fairness für jeden Flow herzustellen

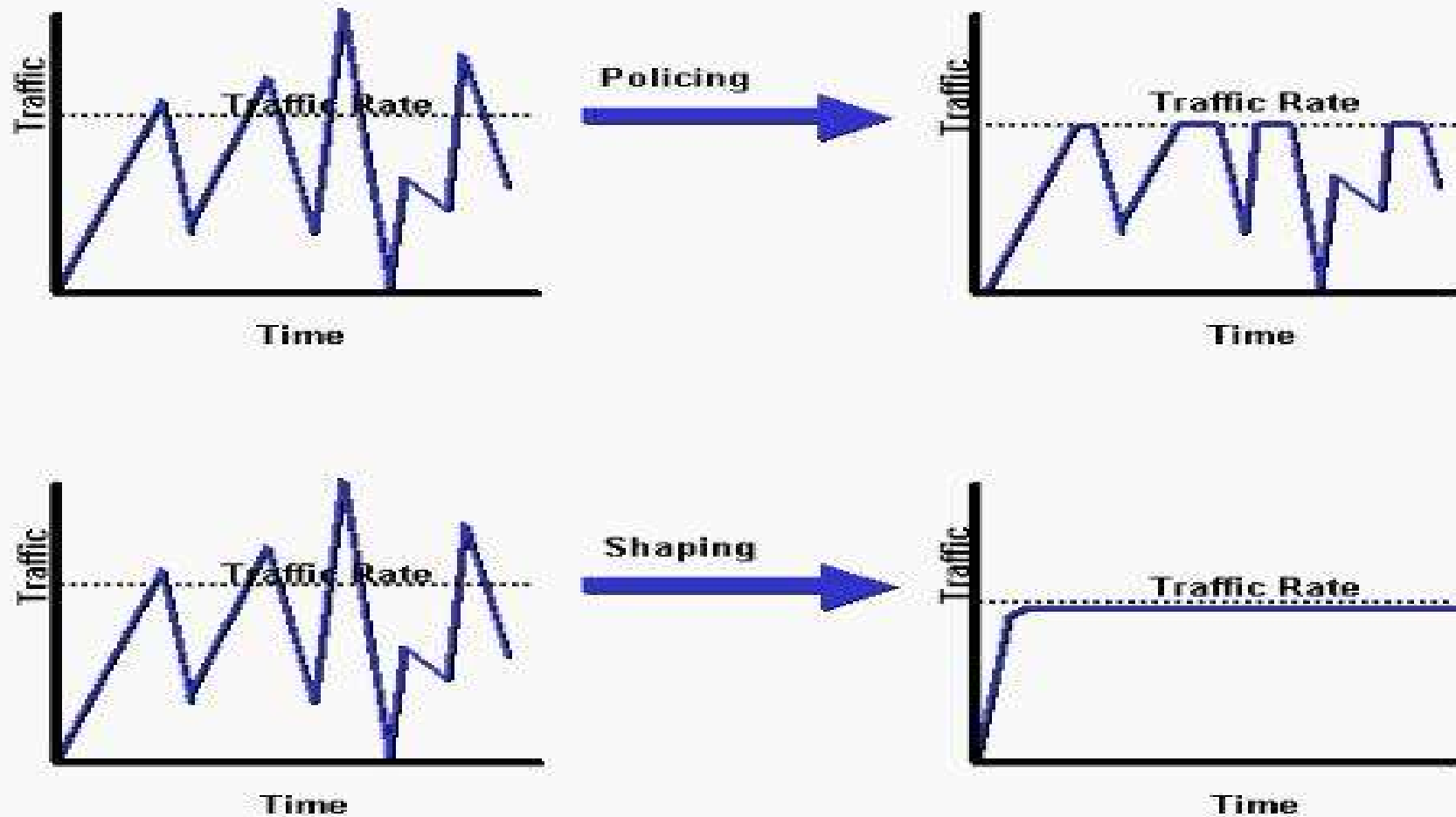
- ESFQ (Enhanced SFQ)

- RED (Random Early Drop)

Versucht Sättigungen zu erkennen und droppt im Vorfeld

Wenig Rechenaufwand => Gut für Backbones

(Exkurs:) Traffic Policing



Policing ist die (beinah) einzig sinnvolle und machbare Möglichkeit,

Incoming Traffic zu beeinflussen:

Da keine Queue für Incoming Traffic existiert, werden hier Packete, die eine bestimmte Bandbreitenbegrenzungen überschreiten gedroppt.

ASK: Ausgangslage

- 2MBit Leitung (Up+Down!) Richtfunk
 - Reel ca. 1,2MBit (durch meist schlechte Witterungsverhältnisse)
 - ca. 80 User
 - Durch Bandbreiten-intensive Anwendungen meist absolut ausgelastete Leitung
 - => Schlechte Interaktivität der Leitung (v.a. ssh/spiele nicht machbar)
-
-

2 mögliche Konzepte

- **Zugesicherte Bandbreite/User**
 - Vorteil: Fest Bandbreite/User
 - Nachteil: Diese Feste Bandbreite wäre zu klein, um sinnvoll zu sein (ca. 1,5kbyte)
- **Priorisierung von Diensten**
 - Vorteil: Interaktivität von bestimmten Diensten kann zugesichert werden
 - Nachteil: keine zugesicherte Bandbreite/User



Technische Realisierung

Realisiert wurde die Lösung 2 (Priorisierung von Diensten), wobei für bestimmte Dienste Bandbreiten zugesichert wurden.

Es wurden einige Positiv- und einige Negativ-Selektionen von Diensten vorgenommen, d.h. Es gibt 3 große Prioritäten:

- hoch (ssh, ACKs, DNS, allgemein Verbindungen <512k)
 - normal (default-Klasse)
 - bulk (mail, ftp, Verbindungen >512k)
-
-

Mögliche Verbesserung durch QoS

- Eindeutig bessere Interaktivität
 - Weniger Beeinflussung durch Bandbreitenintensive Benutzer
 - Schnelleres Antwortverhalten entsprechend priorisierter Dienste
 - (Sicherer Verfügbares Netz)
 - Allgemein verlässlicheres Netzwerk
-
-

Vielen Dank für die Aufmerksamkeit

....Fragen?

