Traffic Engineering: Shaping Vs. Policing

Last updated: March 18, 2024

Written by: Vinicius Fulber-Garcia
(https://www.baeldung.com/cs/author/viniciusfulbergarcia)

Reviewed by: Michal Aibin
(https://www.baeldung.com/cs/editor/michal-author)

Networking (https://www.baeldung.com/cs/category/networking)

1. Introduction

In this tutorial, we'll study traffic engineering (specifically, traffic shaping and traffic policing). Currently, several services and resources are provided online. Due to that, the amount of traffic crossing the core network increased considerably.

Thus, in this scenario, providers can adopt traffic engineering techniques to preserve the quality of the provided services. Among these techniques, we have traffic shaping and traffic policing.

In the following section, we'll investigate what traffic engineering is in a broad sense. So, we'll focus on understanding traffic shaping and policing and discuss some popular implementations. Finally, we outline the most relevant concepts while comparing traffic shaping and policing in a systematic summary.

2. Traffic Engineering

In summary, we can see traffic engineering as a strategy to provide Quality-of-Service (QoS) in computer networks. So, with fast Internet propagation, the discussions and proposals regarding traffic engineering got more frequent and pertinent.

However, before studying traffic engineering, we must define what mean QoS in our context: QoS is a set of technologies and mechanisms to control the network traffic and enforce predefined policies and minimum performance parameters for networked services.

So, in practice, we can implement traffic engineering with network functions (virtualized or not) (/cs/network-function-virtualization) by controlling how packets are forwarded (with Software-Defined Networks, for example) or even as an application running in the servers providing a networked service.

There exist several traffic engineering techniques. Some of the most popular ones are:

- **Shaping**: bandwidth modeling technique to manage network traffic by enqueueing and delaying certain packets
- **Policing**: bandwidth modeling technique to manage network traffic by discarding certain portions of the incoming network traffic
- **Scheduling**: bandwidth modeling technique that enqueues the network traffic in different queues with heterogeneous forwarding policies
- **Washing**: packet modeling technique that discards portions of data from packets which is not mandatory for their processing by the servers

Thus, in the following sections, we'll explore traffic shaping and policing techniques, checking both implementation strategies and working details.

3. Traffic Shaping

Traffic shaping is a bandwidth modeling technique to keep network traffic load at acceptable levels. Network managers and operators, in turn, define what means a proper level of traffic load is for a computing system or service.

This decision, however, depends on several aspects. Among them, we can cite the available bandwidth, the traffic processing power of the computing systems, and the number of requests that a service running on them can tackle in a given time.

So, after configuring and deploying a traffic shaping mechanism, it can act on the network traffic in three ways: forwarding, delaying, or dropping. Let's see when the traffic shaping mechanisms take each one of these actions:

- **Forwarding**: the network traffic load is under the maximum load
- **Delaying**: the network traffic is over the maximum load, and the mechanism queue has free slots
- **Dropping**: the network traffic is over the maximum load, and the mechanism queue has no free slots

In this way, we can presume that traffic shaping mechanisms use a queue to delay exceeding traffic.

Yes, it is right! A traffic shaper does not drop network traffic primarily, as a policier (we'll see in the next section) or a firewall (/cs/firewalls-intro) does. It first tries to delay the exceeding traffic by enqueuing it.

So, when the network traffic load goes under the maximum defined, the traffic shaper forwards the enqueued traffic to its original destination.

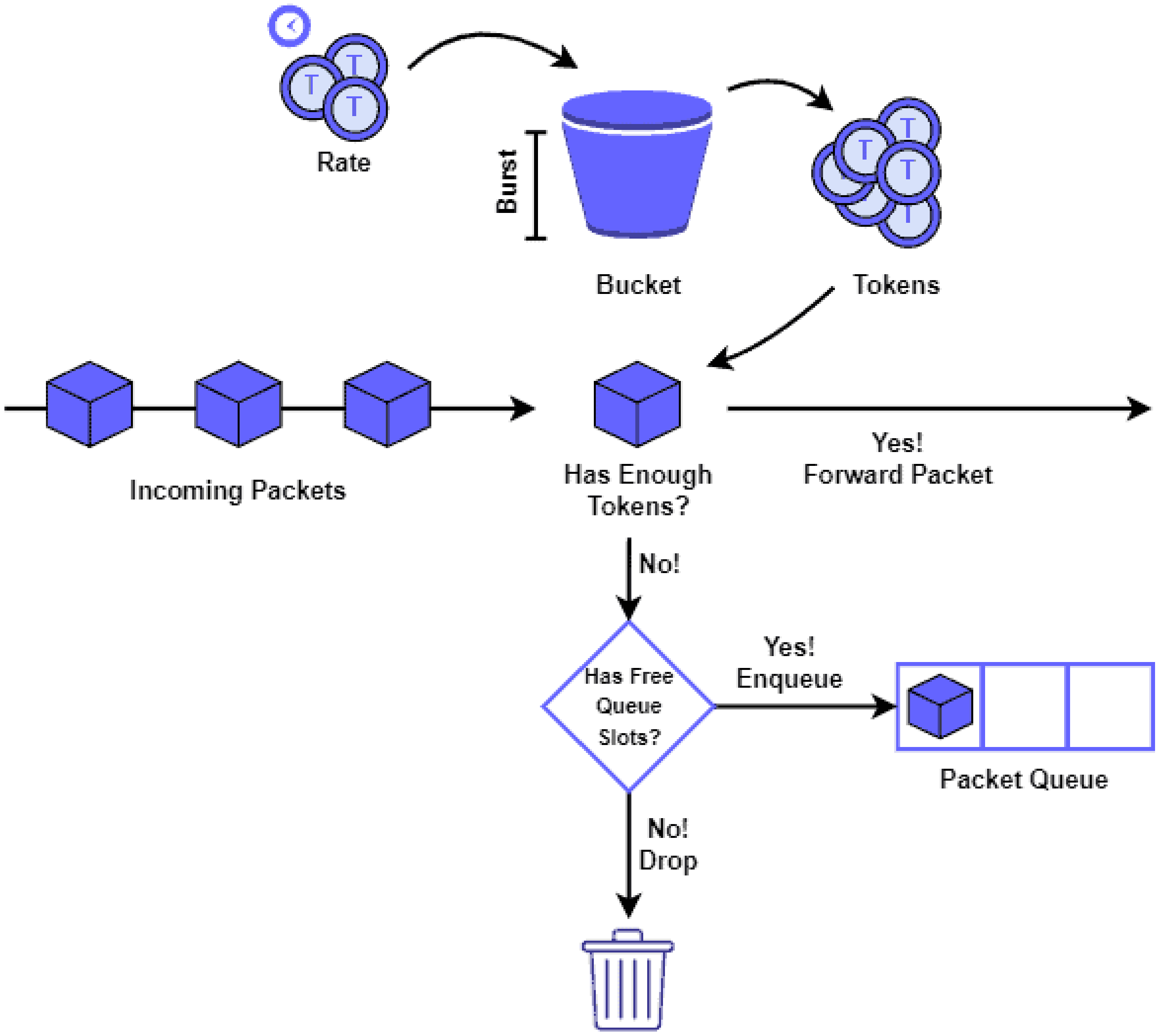
There are multiple types of traffic shapers. The most popular ones are the token bucket shaper and the leaky bucket shaper.

3.1. Token Bucket Shaper

In a token bucket shaper, we work with a bucket abstraction used to keep tokens. So, to forward a frame packet, we'll consume tokens from the bucket (usually, a token means a byte).

The bucket is filled with a predefined number of tokens at a linear interval. We call this rate. Furthermore, the bucket has a maximum number of tokens it can keep, which we call burst.

The following figure depicts the general idea behind a token bucket shaper:



In this way, the shaper forwards a packet if there are enough tokens in the bucket when it arrives. If it does not, but there are free slots in the queue, the shaper thus enqueue the packet. Otherwise, the dropping action is taken.

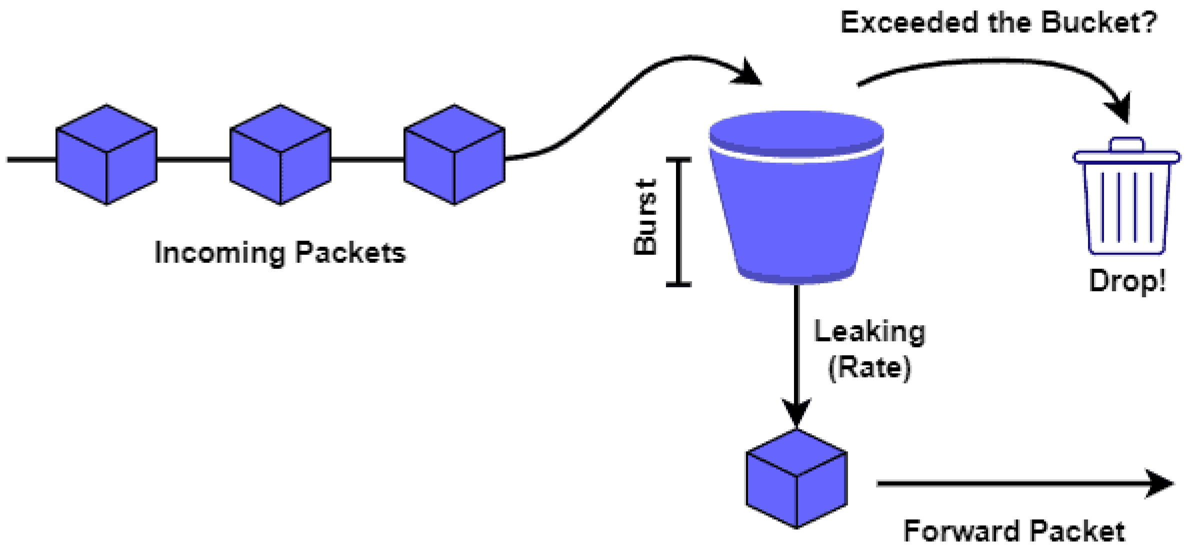
Finally, if the bucket has tokens and the queue has packets after a rate interval, the shaper employs these tokens to forward the enqueued packets.

3.2. Leaky Bucket Shaper

A leaky bucket shaper, similar to the token bucket one, also employs an abstraction of a bucket in its strategy. However, instead of the bucket keeping tokens consumed to forward packets, it keeps the packets themselves.

Technically, the bucket is a queue. Packets in the bucket, in turn, are forwarded with a constant rate in FIFO order (they "leak" from the bucket). Furthermore, the bucket has a maximum size, also called burst.

The following figure shows a representation of the leaky bucket shaper:



In such a way, if the incoming network traffic rate is higher than the leaking rate, the shaper keeps packets in the bucket. If the bucket is already full, however, packets are then dropped.

Finally, if the incoming traffic rate is lower than the leaking rate and there are stored packets in the bucket, they are forwarded, and the bucket gets progressively empty.

4. Traffic Policing

Traffic policing has many similarities with traffic shaping. Among these similarities, we can cite the objective of modeling the bandwidth to keep network traffic load at acceptable levels.

However, instead of enqueueing and delaying the forwarding of the network traffic, traffic policing mechanisms immediately drop the exceeding traffic.

Moreover, traffic policing mechanisms execute only two actions: **forwarding and dropping.**

Thus, the traffic policing general rule is more straightforward when compared to the traffic shaping one: **if the incoming traffic rate is under the maximum allowed, forward all the traffic; if the incoming rate is above the maximum allowed, drop the exceeding traffic.**

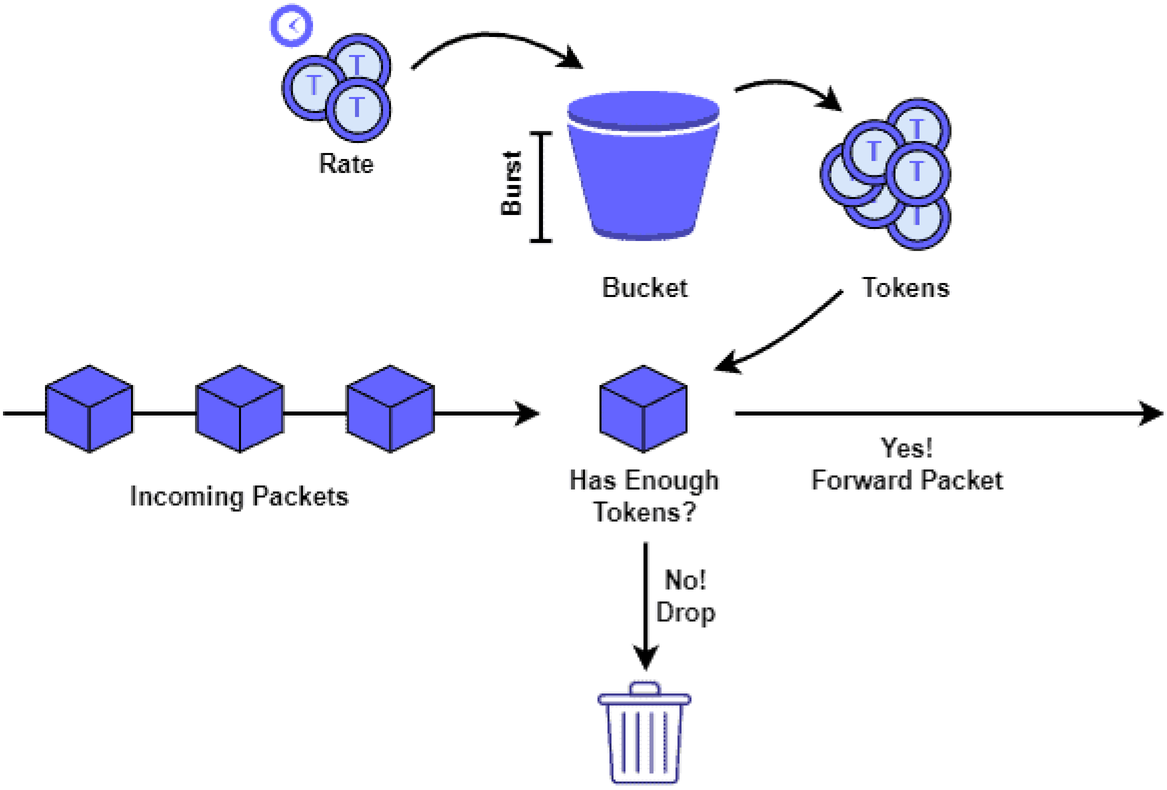
We do have heterogeneous implementations of traffic policing mechanisms. However, token bucket policing is the most common one.

4.1. Token Bucket Policing

The token bucket policing mechanism works similarly to the already discussed token bucket shaper. So, it means that it also works with a bucket of burst size that is filled with tokens considering a predetermined rate.

The mechanism consumes tokens to forward the incoming network traffic. **However, unlike the token bucket shaper, the policing mechanism does not have a queue.**

The following image depicts, on a high level, a generic token bucket policing mechanism:



It is relevant to highlight that, without a queue, the policing mechanism starts to drop the incoming traffic as soon as the bucket runs out of tokens.

5. Systematic Summary

With the popularization of computer networks (mainly the Internet itself), the number of resources and services provided online increased substantially.

As a consequence of this scenario, the network traffic crossing these networks also increased. Thus, providers were required to adopt innovative solutions to keep their activities with high quality of service and experience.

Traffic engineering is one of these innovative solutions. In particular, traffic shaping and policing are the most known techniques in this context.

Both shaping and policing aim to model the bandwidth available for a given service and ensure that the incoming network traffic does not exceed certain limits.

But, shaping and policing mechanisms present some relevant differences between them, which are summarized in the following table:

	Traffic Shaping	**Traffic Policing**
General Objective	Modeling the bandwidth to keep network traffic load at acceptable levels	Modeling the bandwidth to keep network traffic load at acceptable levels
Queue of Packets	Yes	No
Set of Actions	Forwarding; Delaying; Dropping	Forwarding; Dropping
Common Implementations	Token Bucket; Leaky Bucket	Token Bucket

6. Conclusion

In this tutorial, we investigated traffic engineering through traffic shaping and policing techniques. At first, we studied some background concepts about traffic engineering. Thus, we explored traffic shaping and policing specifically. Finally, we compared these techniques in a systematic summary.

We can conclude that, with the increasing demand for computer networks, traffic engineering has become a point of attention for resources and service providers. So, the techniques related to traffic engineering, in particular, traffic shaping and policing, are great alternatives to tackle this demand and keep services continuously online and working with quality.

CATEGORIES

ALGORITHMS (/CS/CATEGORY/ALGORITHMS)
ARTIFICIAL INTELLIGENCE (/CS/CATEGORY/AI)
CORE CONCEPTS (/CS/CATEGORY/CORE-CONCEPTS)
DATA STRUCTURES (/CS/CATEGORY/DATA-STRUCTURES)
LATEX (/CS/CATEGORY/LATEX)
NETWORKING (/CS/CATEGORY/NETWORKING)
SECURITY (/CS/CATEGORY/SECURITY)

SERIES

GRAPHS TUTORIAL (HTTPS://WWW.BAELDUNG.COM/CS/GRAPHS-SERIES)
NEURAL NETWORKS SERIES (HTTPS://WWW.BAELDUNG.COM/CS/NEURAL-NETWORKS-SERIES)
LATEX SERIES (HTTPS://WWW.BAELDUNG.COM/CS/LATEX-SERIES)

ABOUT

ABOUT BAELDUNG (HTTPS://WWW.BAELDUNG.COM/ABOUT)
BAELDUNG ALL ACCESS (/COURSES)
THE FULL ARCHIVE (/CS/FULL_ARCHIVE)
EDITORS (HTTPS://WWW.BAELDUNG.COM/EDITORS)
OUR PARTNERS (HTTPS://WWW.BAELDUNG.COM/PARTNERS/)
PARTNER WITH BAELDUNG (HTTPS://WWW.BAELDUNG.COM/PARTNERS/WORK-WITH-US)
EBOOKS (HTTPS://WWW.BAELDUNG.COM/LIBRARY/)
FAQ (HTTPS://WWW.BAELDUNG.COM/LIBRARY/FAQ)
BAELDUNG PRO (/MEMBERS/)

TERMS OF SERVICE (HTTPS://WWW.BAELDUNG.COM/TERMS-OF-SERVICE)
PRIVACY POLICY (HTTPS://WWW.BAELDUNG.COM/PRIVACY-POLICY)
COMPANY INFO (HTTPS://WWW.BAELDUNG.COM/BAELDUNG-COMPANY-INFO)