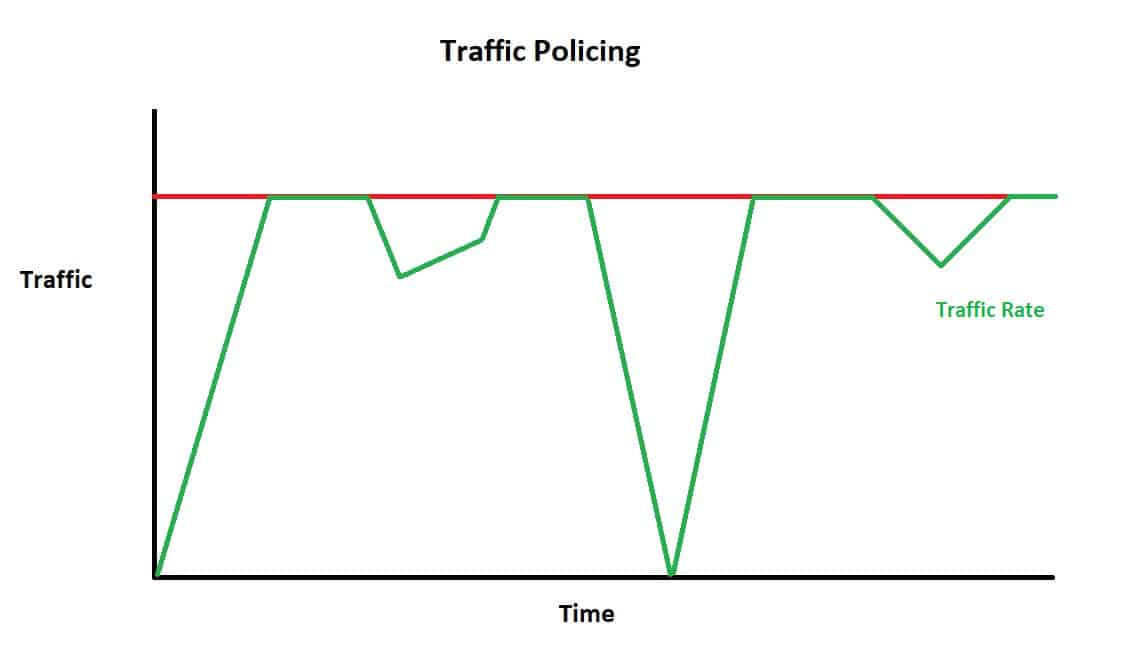
**Các phương pháp đảm bảo tốc độ của đường mạng**

**Phương pháp đảm bảo tốc độ gửi gói tin:**

* **Một trong những nguyên nhân dẫn đến cần đưa ra giải pháp trong việc kiểm soát tốc độ truyền gói tin của đường mạng**
* Tắc nghẽn xảy ra khi quá nhiều dữ liệu cùng được gửi qua một phần của mạng, dẫn đến giảm hiệu suất.
* Chất lượng dịch vụ (QoS) đề cập đến việc cung cấp các mức độ ưu tiên khác nhau cho các loại lưu lượng mạng khác nhau. Điều này cực kỳ quan trọng với các ứng dụng yêu cầu **tính tức thì** hoặc **độ trễ thấp**
* Trong một hệ thống mạng, có nhiều loại lưu lượng với các yêu cầu khác nhau. Một số dịch vụ có thể yêu cầu băng thông cao (ví dụ: truyền tải file lớn), trong khi các dịch vụ khác yêu cầu độ trễ thấp (ví dụ: gọi điện trực tuyến)
* Trong nhiều tổ chức, đặc biệt là các nhà cung cấp dịch vụ mạng, cần có các **thỏa thuận mức dịch vụ (Service Level Agreement - SLA)** để đảm bảo chất lượng dịch vụ đáp ứng các yêu cầu cam kết với khách hàng
* Người dùng cuối mong đợi một trải nghiệm mượt mà và ổn định khi sử dụng các dịch vụ mạng. Nếu không có biện pháp quản lý lưu lượng hiệu quả
* **Giải pháp của những vấn đề trên:**
* Là một hệ thống thuật toán để kiểm soát tốc độ gửi đi của gói tin và lựa chọn xóa bỏ các gói tin trong hàng đợi trước khi được chuyển đi.

1. **Policing:**
2. **Cơ chế cốt lõi:**

* Giúp ngăn chặn ngay lập tức lưu lượng vượt mức, có thể dẫn đến loại bỏ hoặc đánh dấu các gói tin. Thường dùng khi cần kiểm soát nghiêm ngặt và không cần lưu lượng vượt quá.



1. **Cơ chế hoạt động cơ bản:**

Các token được thêm vào "bucket" với một tốc độ không đổi, được điều chỉnh bởi tốc độ dữ liệu trung bình cho phép. Nếu "bucket" đầy đến mức dung lượng của nó, bất kỳ token nào thêm vào đều sẽ bị loại bỏ.

VD: Ví dụ, nếu tốc độ là 10 token mỗi giây và dung lượng "bucket" là 50 token, sẽ mất 5 giây để "bucket" đầy hoàn toàn.

Khi một gói tin (hoặc đơn vị dữ liệu) đến, bộ điều khiển sẽ kiểm tra xem trong "bucket" có đủ token để truyền gói tin hay không.

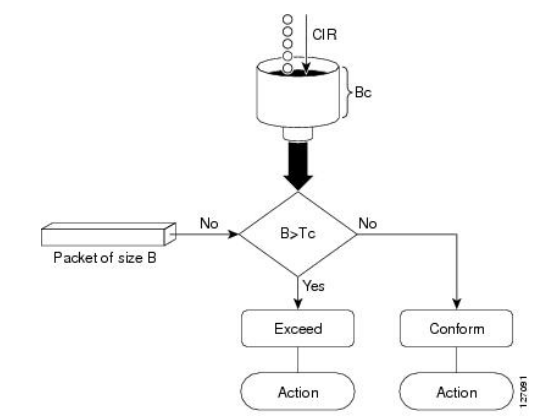
VD: Nếu kích thước gói tin là 500 byte và trong "bucket" có 500 token, gói tin sẽ được truyền ngay lập tức, và 500 token sẽ bị tiêu thụ từ "bucket".Nếu không đủ token, gói tin có thể được đưa vào hàng đợi, bị trì hoãn hoặc bị loại bỏ, tùy thuộc vào cấu hình.

1. **Cơ chế hoạt động chi tiết:**

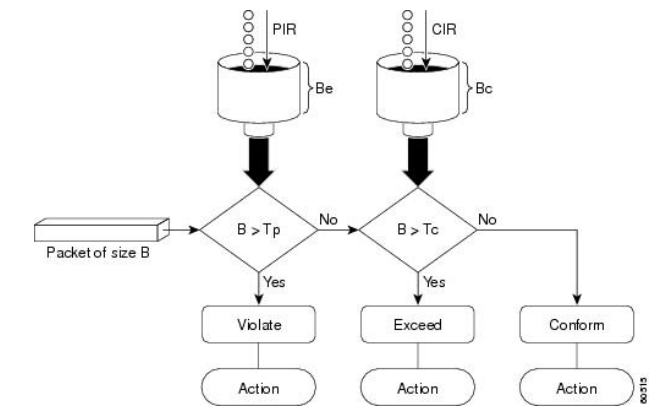
****

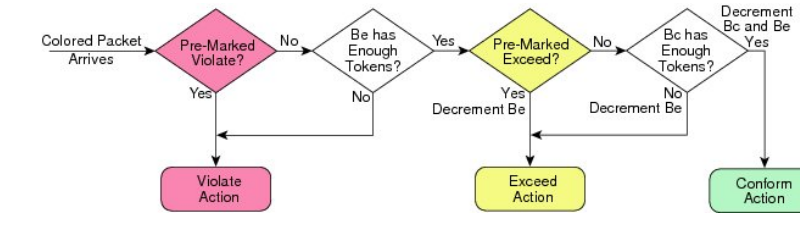
****

**Single Rate Policer**: Là phương pháp Policing đánh dấu và gán nhãn chỉ dựa trên một tiêu chí là CIR (Committed Information Rate) là một chỉ số đường mạng cho phép gói tin đi qua an toàn được tính toán và thay đổi theo thời gian. Các gói tin được gán nhãn dựa trên phương pháp này chỉ mang 2 loại nhãn là Committed và Exceed. Sau khi đã được đánh dấu tùy vào loại gói tin sẽ có những cách xử lí khác nhau ( DSCP là một yếu tố dùng để đánh giá việc xử lí gói tin sau khi gán nhãn cho gói tin đó )



**Two-Rate Policer:** Là phương pháp Policing đánh dấu và gán nhãn chỉ dựa trên hai tiêu chí là CIR (Committed Information Rate chỉ số thông lượng an toàn khi cho gói tin đi qua) và PIR ( peak information rate chỉ số thông lượng tối đa cho phép gói tin đi qua ). Các gói tin được gán nhãn dựa trên phương pháp này chỉ mang 3 loại nhãn là Committed, Exceed và Violated.



**Two-Rate Three-Color (2R3C) Policer:** sau

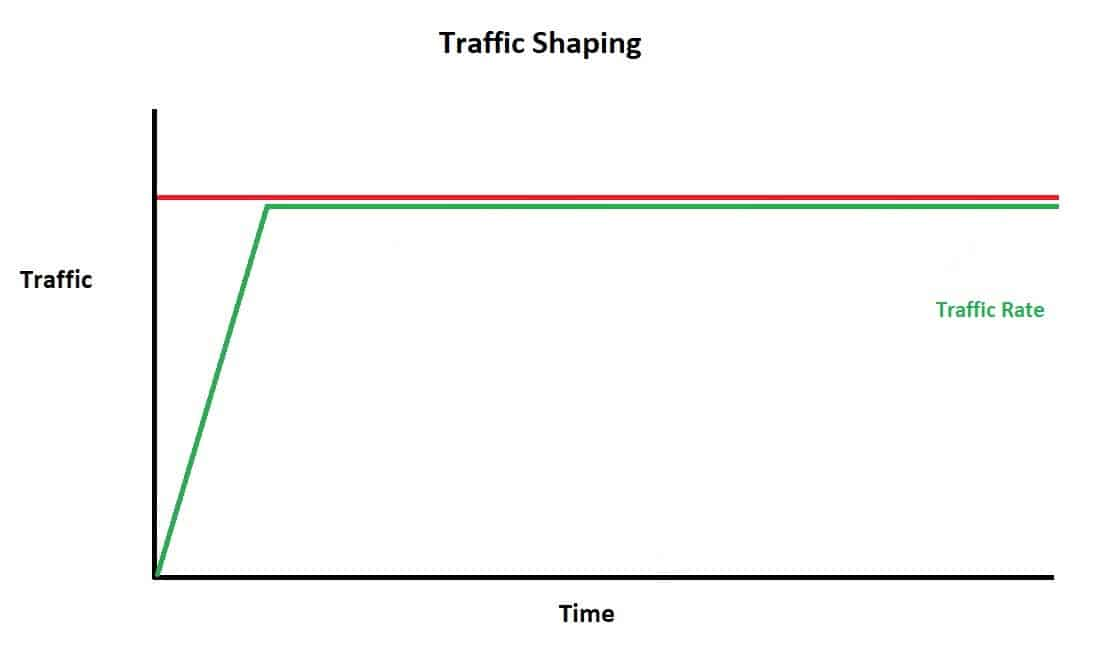
1. Ưu điểm và nhược điểm của Policing Algorithms:

| Quản Lý Tài Nguyên Hiệu Quả:  Traffic policing giúp phân bổ băng thông một cách hợp lý, đảm bảo rằng các ứng dụng quan trọng nhận được đủ tài nguyên cần thiết để hoạt động hiệu quả. | Khó Khăn Trong Việc Định Nghĩa Ngưỡng: Việc xác định ngưỡng băng thông cho các loại lưu lượng khác nhau có thể phức tạp và có thể dẫn đến việc đánh giá sai lưu lượng quan trọng. |
| --- | --- |
| Giảm Thiểu Tắc Nghẽn Mạng: Bằng cách giới hạn lưu lượng vượt quá mức cho phép, traffic policing giúp ngăn ngừa tình trạng tắc nghẽn trong mạng, từ đó cải thiện hiệu suất tổng thể. | Rủi Ro Về Mất Dữ Liệu: Nếu lưu lượng vượt quá ngưỡng cho phép, các gói dữ liệu có thể bị loại bỏ, dẫn đến mất mát thông tin quan trọng và ảnh hưởng đến trải nghiệm người dùng. |
| Tăng Cường Chất Lượng Dịch Vụ (QoS): Các thuật toán này cho phép quản lý lưu lượng theo các lớp dịch vụ khác nhau, giúp duy trì chất lượng dịch vụ cho các ứng dụng nhạy cảm với thời gian như video trực tuyến hoặc hội nghị truyền hình. | Tác Động Tiêu Cực Đến Ứng: Dụng Không Được Đánh Giá Cao Các ứng dụng không được ưu tiên có thể gặp khó khăn trong việc hoạt động hiệu quả, điều này có thể gây ra sự không hài lòng từ phía người dùng. |
| Dễ Dàng Triển Khai:Traffic policing có thể được triển khai dễ dàng trên nhiều loại thiết bị mạng mà không cần thay đổi cấu trúc mạng hiện tại. | Phức Tạp Trong Quản Lý:Việc theo dõi và điều chỉnh các chính sách traffic policing để phù hợp với nhu cầu thay đổi của mạng có thể đòi hỏi nhiều công sức và thời gian. |

**II. Shaping:**

1. **Cơ chế cốt lõi:**

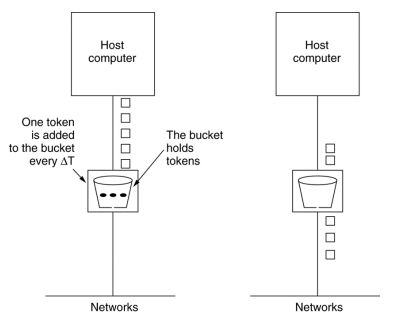
Cơ chế để điều chỉnh lưu lượng quá mức, bằng cách tạm giữ các gói và chờ cho đến khi có đủ token để gửi đi, nhằm duy trì chất lượng dịch vụ mà không gây mất gói, nhưng có thể gây ra độ trễ.

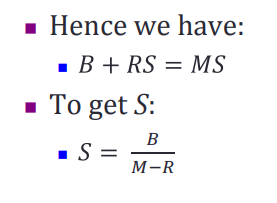
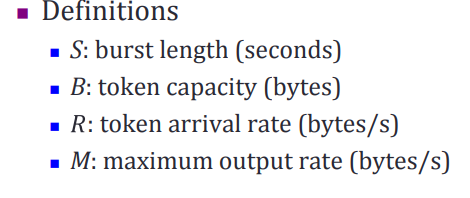


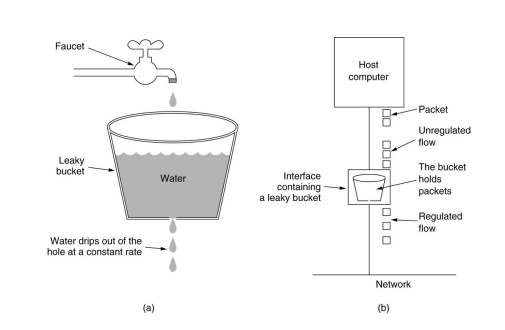
1. **Cơ chế hoạt động cơ bản:**

* **Token Bucket**: có phương thức hoạt động khá giống với Token Bucket của Policing, các token cũng sẽ được thêm vào bucket với một tốc độ xác định biến thiên. Khi các gói tin đến nếu trong bucket có đủ token thì gói tin sẽ được chuyển đi và ngược lại sẽ được hậu xử lí. Sự khác biệt của Shaping Token Bucket và Policing Token Bucket ở pha hậu xử lí.
* Truyền Gói Dữ Liệu: Các gói dữ liệu được truyền đi từ buffer khi có đủ token trong bucket. Điều này đảm bảo rằng lưu lượng được gửi đi một cách ổn định và không vượt quá các giới hạn đã được thiết lập.
* Trì Hoãn Gói Dữ Liệu: Nếu không có đủ token để gửi gói dữ liệu ngay lập tức, các gói này sẽ bị giữ lại trong buffer cho đến khi có đủ token để truyền đi. Điều này giúp tránh tình trạng mất gói và duy trì chất lượng dịch vụ (QoS). Do ở đây xuất hiện buffer nên sẽ xuất hiện thêm một vài vấn đề và sẽ được nói đến trong phần cơ chế chi tiết
* **Token Leak:** Token Leak có các đặc điểm cơ bản gióng với Token Bucket nhưng sự khác biệt nằm ở Bucket lúc này sẽ bị “rò rỉ” có nghĩa là các token không được tiêu thụ sẽ bị loại bỏ sau một khoảng thời gian. Cơ chế rò rỉ này giúp đảm bảo rằng bucket không bị đầy và giữ cho lưu lượng luôn ổn định.

1. **Cơ chế hoạt động chi tiết:**

**Token Bucket:** Các token cũng sẽ được chảy vào bucket theo một tốc độ CIR. Các gói tin khi đi qua cũng sẽ lấy một lượng token tương ứng, nếu gói tin quá lớn thì không đủ lượng token thì lúc đó gói tin trên sẽ được cho vào một buffer. Từ đây xuất hiện các thuật toán lập lịch hàng đợi để truyền gói tin đi  




**Token Leak: Leak**Lea ****

1. **So sánh token bucket và token leak**

| | **Tiêu Chí** | | --- | | | **Token Bucket** | | --- | | | **Leaky Bucket** | | --- | |
| --- | --- | --- | --- | --- | --- |
| **Quản Lý Lưu Lượng** | **Linh hoạt hơn, cho phép lưu lượng đột biến.** | **Tốc độ truyền dữ liệu là cố định, không cho phép lưu lượng đột biến** |
| **Tình Huống Xử Lý Gói Tin** | **Gói tin lớn hơn kích thước token hiện tại sẽ bị trì hoãn hoặc rớt.** | **Gói tin quá khổ sẽ bị trì hoãn hoặc bị loại bỏ nếu không có đủ token.** |
| **Chất Lượng Dịch Vụ** | **Cung cấp khả năng cải thiện QoS bằng cách sử dụng token.** | **Đảm bảo QoS bằng cách kiểm soát tốc độ lưu lượng truyền đi.** |
| **Ứng Dụng Thực Tế** | **Thích hợp cho các ứng dụng yêu cầu độ linh hoạt cao.** | **Thích hợp cho các dịch vụ yêu cầu tính ổn định trong lưu lượng.** |

**Reference:**

[**https://www.geeksforgeeks.org/difference-between-traffic-policing-and-traffic-shaping**](https://www.geeksforgeeks.org/difference-between-traffic-policing-and-traffic-shaping)

[**https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/acls\_4100i-6000-6100/Content/Chp\_Cls\_Pol/tra-pol.htm**](https://www.arubanetworks.com/techdocs/AOS-CX/10.10/HTML/acls_4100i-6000-6100/Content/Chp_Cls_Pol/tra-pol.htm)

[**https://www.cisco.com/c/en/us/td/docs/routers/ncs4000/software/qos/configuration\_guide/b-qos-cg/b-qos-cg\_chapter\_0111.pdf**](https://www.cisco.com/c/en/us/td/docs/routers/ncs4000/software/qos/configuration_guide/b-qos-cg/b-qos-cg_chapter_0111.pdf)

[**https://www.youtube.com/watch?v=Ttd4y3R6J24&t=2s**](https://www.youtube.com/watch?v=Ttd4y3R6J24&t=2s)

[**https://en.wikipedia.org/wiki/Traffic\_shaping**](https://en.wikipedia.org/wiki/Traffic_shaping)

[**https://www.f5.com/glossary/traffic-shaping**](https://www.f5.com/glossary/traffic-shaping)

[**https://www.techtarget.com/whatis/definition/leaky-bucket-algorithm**](https://www.techtarget.com/whatis/definition/leaky-bucket-algorithm)

**https://www.sciencedirect.com/topics/computer-science/leaky-bucket-algorithm**