УДК 391.39

ЗАБЕЗПЕЧЕННЯ QOS В TCP/IP МЕРЕЖАХ

Мєлєхова М.О., Носков В.І.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: maria.melekhova@gmail.com

Providing QoS in TCP / IP networks

Every moment traffic increases, so we need to implement stricter requirements for the quality of services. QoS can be organized using a wide range of instruments on different layers of the OSI model. Classification of the methods proposed in this paper will help for identifying of the methods that regulate the congestions more effectively.

Сучасні мережі висувають все більш жорсткі вимоги до якості обслуговування (QoS). Нові додатки для передачі відео і голосу в режимі реального часу пред'являють досить високі вимоги до якості послуг, що надаються. Затори виникають тоді, коли вимоги до смуги пропускання вище за можливості мережі. При передачі даних по мережі вимога до смуги пропускання мережі може перевищувати її можливості. Це призводить до затору в мережі.

Коли обсяг трафіку перевищує обсяг даних, який може передаватися по мережі, пристрої ставлять пакети в чергу або утримують їх в пам'яті до тих пір, поки ресурси не стануть доступні для передачі. Постановка пакетів в чергу призводить до затримки, оскільки нові пакети не можуть передаватися до тих пір, поки не будуть оброблені попередні. Якщо кількість пакетів, які повинні бути поставлені в чергу, продовжує збільшуватися, черги в пам'яті заповнюються і пакети відкидаються[1].

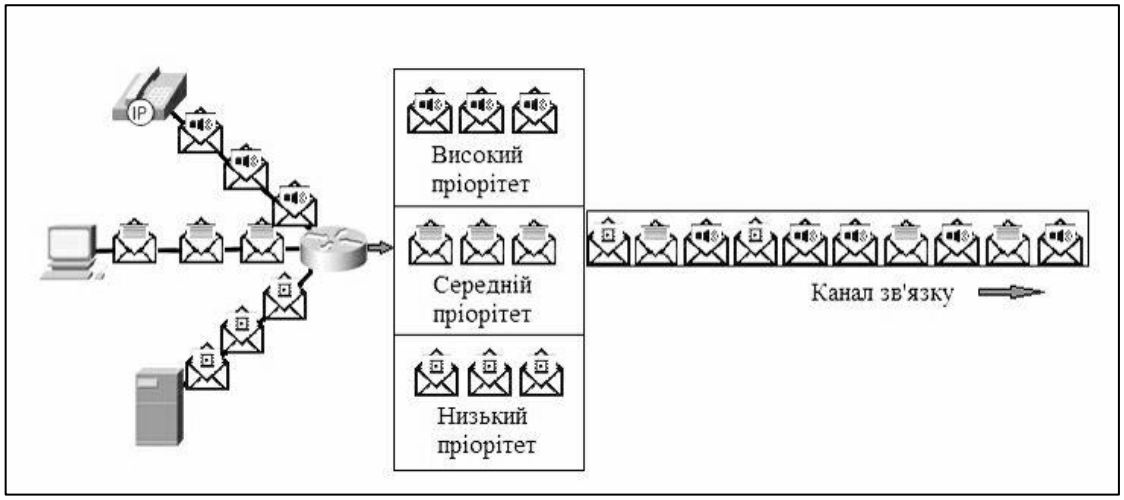

Рис. 1. Використання черг для пріоритизації з'єднань

Для забезпечення необхідної якості передачі трафіку використовують певні інструменти [2], наприклад:

1. *Класифікація і маркування.* Сеанси чи потоки аналізуються на належність певному класу трафіку. Після визначення класу пакети отримують відповідну мітку.

2. *Запобігання заторів*. Для класів трафіку виділяються фрагменти мережевих ресурсів відповідно до політики якості обслуговування. Політика якості обслуговування також визначає порядок видалення, затримки чи перемаркування

деякого трафіку для запобігання заторів. Основним інструментом запобігання перевантаження є Weighted Random Early Detection (WRED), він використовується для регулювання трафіку даних протоколу транспортного рівня Transmission Control Protocol (TCP) з метою оптимізації пропускної здатності і запобігання відкидання останнього елемента через переповнення черги.

3. *Управління заторами.* Коли обсяг трафіку перевищує доступні мережеві ресурси, трафік ставиться в чергу очікування доступних ресурсів (рис.1). Для управління заторами, наприклад на пристроях компанії Cisco, можна використовувати алгоритми Class-Based Weighted Fair Queuing (CBWFQ) і Low Latency Queuing (LLQ)[2].

Класифікація та маркування дозволяють ідентифікувати типи пакетів. Класифікація визначає клас трафіку, до якого належать кадри. Застосовувати політики можна тільки до ідентифікованого трафіку.

Класифікація пакета залежить від реалізації політики якості обслуговування. При класифікації потоків трафіку на рівні 2 і 3 використовуються інтерфейси, списки контролю доступу і карти класів. Трафік також можна класифікувати на рівнях з 4-го по 7-й за допомогою розпізнавання додатків за параметрами мережевого трафіку

Маркування означає додавання деякого значення у заголовок пакету. Пристрої, які приймають пакет, порівнюють значення цього поля зі значенням, визначеним політикою приоритезації. Маркування необхідно проводити максимально близько до вихідного пристрою. Вона встановлює межі довіри [3].

Рішення про маркування трафіку на рівні 2 і 3 має прийматися з урахуванням наступних факторів [2]:

- Маркування рівня 2 для кадрів можна виконувати для не тільки для IP-трафіку.
- Маркування рівня 2 для кадрів є єдиним можливим варіантом реалізації якості обслуговування для комутаторів 2го рівня.
- Маркування рівня 3 забезпечує наскрізну передачу даних про якість обслуговування.

Управління заторами передбачає планування і формування черг, які передбачають буферизацію зайвого трафіку або приміщення його в чергу на час очікування відправки такого трафіку на вихідному інтерфейсі або навіть його видалення. Засоби запобігання заторів легше реалізувати. Вони відстежують розподіл мережевого трафіку, намагаючись передбачити і запобігти затори в типових вузьких місцях у мережі і між мережами до того, як затор перетвориться в серйозну проблему. Вони пропонують пріоритетну обробку для високопріоритетного трафіку при виникненні затору, паралельно максимально збільшуючи використання пропускної здатності мережі і мережевих потужностей і зводячи до мінімуму втрату пакетів і затримки.

Шейпінг трафіку (рис. 2) зберігає зайві пакети в черзі, а потім планує подальшу передачу цих пакетів через певні проміжки часу. Результатом процесу шейпінгу трафіку є більш плавна інтенсивність відправки пакетів.

Для шейпінгу трафіку потрібна наявність черги і достатній обсяг пам'яті для буферизації затриманих пакетів, тоді як для полісінгу трафіку це не потрібно.

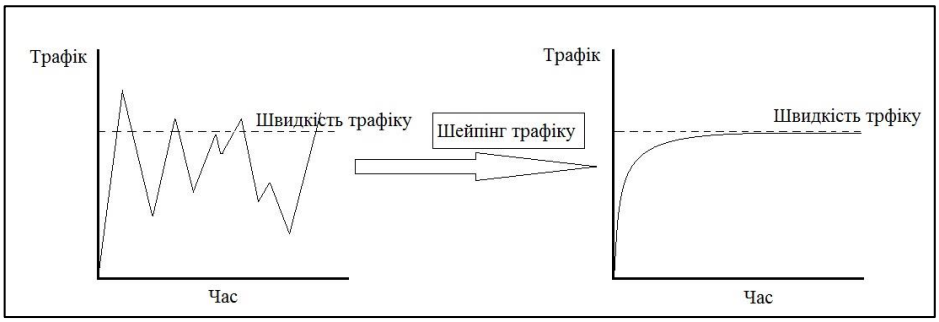

Рис. 2. Приклад шейпінгу трафіку

Полісінг, коли швидкість передачі трафіку досягає встановленого максимуму, зайвий трафік відкидається чи заново маркується. В результаті швидкість передачі має пилкоподібний графік з піками і падіннями (рис.3).

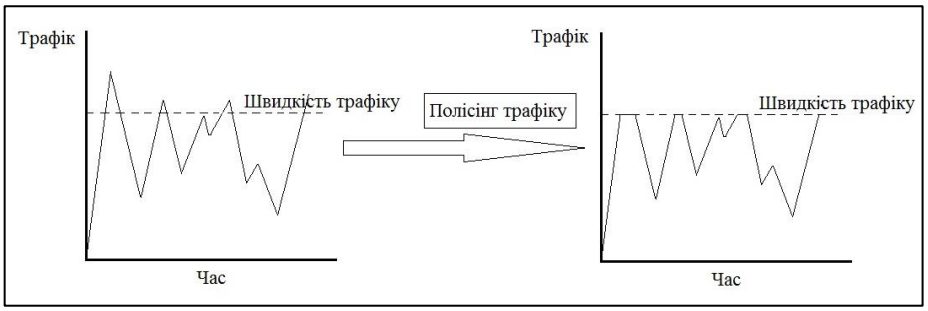

Рис. 3. Приклад полісінга трафіку

Організація черг пов'язана з управлінням вихідним трафіком. Пакети, які виходять через інтерфейс, поміщаються в чергу, і до них може застосовуватися шейпінг трафіку. До вихідного трафіку на інтерфейсі може застосовуватися тільки полісінг[4].

При включенні шейпінгу трафіку необхідно переконатися в наявності достатнього обсягу пам'яті. Крім того, для шейпінгу потрібно функція планування для подальшої передачі всіх відкладених пакетів. Ця функція планування дозволяє розбивати трафік в черзі на кілька черг. Функціями планування є, наприклад, CBWFQ і LLQ[2].

Таким чином, для забезпечення якості обслуговування в IP-мережах використовують наступні методи:

1. Класифікація та маркування, завдяки яким можна ідентифікувати типи пакетів.

2. Використання методів запобігання заторів визначає порядок видалення, затримки чи перемаркування деякого трафіку для запобігання заторів.

3. Управління заторами дозволяє мережі моніторити себе і підлаштовуватись під зміни в залежності від навантаження на мережу. Шейпінг дозволяє забезпечити "плавність" передачі даних, деякий час тримаючи пакети в буфері, що є перевагою особливо при передачі голосового трафіку. Полісінг же дозволяє відкидати пакети, аби при передачі не утворився затор. За допомогою цих механізмів використання мережевих ресурсів є більш ефективним, а можливість утворення заторів є меншою.

Література

1. Вегешна Ш. Качество обслуживания в сетях IP: Пер. с англ. – М.: Изд. дом Вильямс», 2003. – 368 с.
2. Одом У. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCETN/CCNA ICND1 640-822 / Третье издание , 2013 - 720 с.
3. Олифер В., Олифер Н. Искусство оптимизации трафика / Журнал сетевых решений / LAN №12, 2001 - 38-47с.
4. Большаков С. Cisco QoS – классификация и маркировка / [Електронний ресурс] / http://twistedminds.ru/2013/02/cisco-qos-classifying-and-marking/, 2016.