СИСТЕМНІ ДОСЛІДЖЕННЯ

УДК 004.45

ПІКУЛІЦЬКА Юлія, аспірант кафедри економічної кібернетики
та інформаційних систем КНТЕУ

УПРАВЛІННЯ ТРАФІКОМ У МЕРЕЖІ ETHERNET

Проаналізовано засоби управління трафіком у мережі Ethernet. Представлено опис технологій RSVP та MPLS, алгоритмів обробки черг і класифікації трафіку. Виявлено відмінності в управлінні трафіком для протоколів IPv4 та IPv6. Сформульовані основні правила для побудови гнучкої та ефективної системи управління трафіком.

Ключові слова: управління трафіком, якість сервісів, тип сервісу, алгоритми обробки черг, резервування, перевантаження, MPLS, RSVP.

Пикулицкая Ю. Управление траффиком в сети Ethernet. *Проанализированы средства управления траффиком в сети Ethernet. Представлено описание технологий RSVP и MPLS, алгоритмов обработки очередей и классификации траффика. Выявлены отличия в управлении траффиком для протоколов IPv4 и IPv6. Сформулированы основные правила для построения гибкой и эффективной системы управления траффиком.*

Ключевые слова: управление траффиком, качество сервисов, тип сервиса, алгоритмы обработки очередей, резервирование, перегрузки, MPLS, RSVP.

Постановка проблеми. Із року в рік комп'ютерні мережі стають дедалі складнішими, кількість користувачів сервісів мережі невпинно зростає, локальні мережі змінюють призначення, постійно виникають нові додатки, орієнтовані на роботу в мережах. У таких умовах все актуальнішою стає проблема управління трафіком. Адже різні додатки мають свої вимоги до смуги пропускання, своєчасності доставки пакетів, координації. Постійне виникнення колізій сповільнює роботу мережі, а будь-яка багатоадресна розсилка пакетів може значно погіршити або навіть паралізувати її роботу. Тож управління якістю обслуговування, контроль за широкомовним трафіком, резервування пропускної смуги набувають все більшого значення.

Аналіз останніх досліджень і публікацій. Питання щодо управління трафіком розглядалось багатьма вченими із моменту виникнення мережі. Дослідження Я. Ріхтера [1], Е. Белла, А. Сміта, П. Ланджіла, А. Ріджісінхені, К. Маклокгрі [2], Д. Аудачі, Дж. Малколма, Дж. Агогбу, М. О'Дела, Дж. Макмануса [3], Д. Федика [4] покладені в основу стандартів RFC. Постійно публікують результати своєї роботи В. Оліфер, Н. Оліфер [5], А. Велихов, К. Строчников, Б. Леонтьев [6]. В Україні над розв'язанням цієї проблеми працюють Л. Беркман [7], О. Лемешко [8–9], О. Дробот [10], О. Муранов [11–12]. Однак для створення гнучкої системи управління трафіком потрібно визначитися із завданнями, які вона має виконувати, та засобами, необхідними для її побудови. Для цього необхідне чітке розуміння мети та обізнаність у існуючих технологіях.

Метою дослідження є аналіз засобів управління трафіком у мережах Ethernet, що сприятиме визначенню ефективних підходів до управління трафіком.

Методи управління трафіком різняться залежно від завдань, що постають перед адміністратором мережі. Деякі методи спрямовані на розв'язання певної задачі та зовсім не здатні зарадити у інших випадках. Інші доволі універсальні, але не повною мірою розв'язують ту чи іншу проблему, а лише частково покращують ситуацію. Однак у поєднанні з іншими здатні суттєво поліпшити параметри зв'язку.

В Україні комп'ютерні мережі вищих навчальних закладів, як правило, побудовані за технологією Ethernet, отже використовують комутацію пакетів. Пропускна здатність такої мережі невідома, можуть траплятися випадкові затримки. Застосування засобів управління трафіком у мережі із комутацією пакетів дозволяє ефективніше використовувати ресурси мережі, управляти перевантаженнями у разі їхньої появи, надавати смугу пропускання вимогливим до неї додаткам й у цілому підвищити якість обробки та швидкість доставки інформації кінцевому користувачу.

Сучасні системи управління трафіком складаються із таких елементів:

- *класифікація* (classifying) – механізм розподілу пакетів для різноманітної подальшої обробки, можливо, навіть, у різні черги. У процесі прийому, маршрутизації та передачі пакетів вони можуть бути по-різному класифіковані. Це може бути маркування, яке відбувається на межі мережі з єдиним адмініструванням, або може виконуватися на кожному проміжному вузлі окремо;
- *планування* (sceduling) – механізм впорядкування об'єктів між входом і виходом певної черги;
- *маркування* (marking) – механізм зміни пакета;
- *знищення* (dropping) – знищує пакети, наприклад, у разі переповнення буферу даних при використанні обмеження вхідного трафіку;
- *обмеження вхідного трафіку* (policing) – механізм обмеження, який приймає пакети, що не перевищують заданих показників. Над рештою виконується визначена дія (знищення, перекласифікація);

- *обмеження вихідного трафіку* (shaping) – механізм для затримки пакетів перед передачею для підтримки бажаної швидкості передачі.

Відповідно до поставлених цілей, поєднавши деякі або всі ці елементи між собою, можна створити гнучку та ефективну систему управління трафіком.

Класифікація. Будь-який механізм управління трафіком передбачає насамперед класифікацію, адже оброблення всього трафіку мережі як такого, що має однаковий пріоритет, яким би чином воно не відбувалося, буде малоефективним. Залежно від рівня моделі OSI, на якому відбувається класифікація трафіку, існує декілька методів надання пріоритетів.

Для другого (канального) рівня OSI було розроблено стандарт IEEE 802.1p. Він передбачає однорівневу специфікацію маркування пакетів для взаємодії між віртуальними мережами Ethernet. IEEE 802.1p реалізується у мережевих адаптерах і комутаторах для роботи за принципом "зробити якнайкраще, проте без гарантії" (best-effort) та не потребує резервування ресурсів. За ним, замість стандартного поля кадру Ethernet "Тип протоколу" розміщується "Мітка" (*рис. 1*).

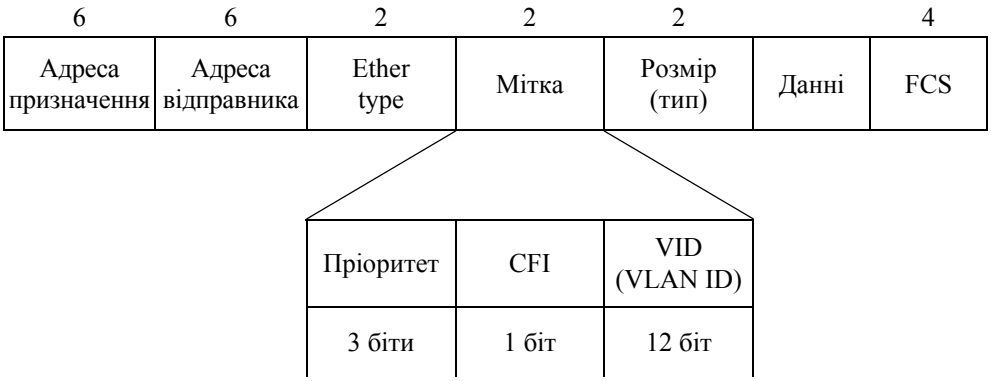

Рис. 1. Формат міток VLAN на рівні L2 (стандарт 802.1p)

Поле пріоритет користувача – 3 біти, 1-бітове поле CFI (індикатор канонічного формату) та 12-бітове поле VID (ідентифікатор віртуальної мережі) називаються TCI (інформація управління тегом). 3-бітове поле IP-пріоритету розміщується тут без проблем. Після введення мітки в кадр потрібно перерахувати контрольну суму FCS. Канальний рівень у цьому випадку повинен підтримувати множинні черги.

На наступному рівні L3 управління трафіком ґрунтується на можливостях транспортних протоколів. Деякі з них (UDP) не мають механізмів керування трафіком, інші (IPX/SPX, RTP/RTCP) вирішують окремі задачі, але не мають суттєвого розповсюдження. Протокол TCP для управління трафіком має в заголовку 6-бітове поле "Прапори" (відповідні значення (зліва направо) представлені в *табл. 1*).

Таблиця 1

Значення бітів поля "Прапори"

Позначення бітів поля "Прапори"	Значення біту, якщо він дорівнює 1
URG	Прапор важливої інформації, поле "Покажчик важливої інформації" має значення, якщо URG=1
ACK	Номер октету, який повинен був прийти наступним
PSH	Цей сегмент вимагає виконання операції push. Одержувач повинен передати ці дані прикладній програмі якомога швидше
RST	Переривання зв'язку
SYN	Прапор для синхронізації номерів сегментів, використовується при встановленні зв'язку
FIN	Відправник закінчив посилку байтів

Ці поля заголовків являють собою основу методів управління трафіком. Протокол TCP застосовують, коли необхідна гарантована доставка повідомлень. Він використовує контрольні суми пакетів для перевірки їх цілісності та звільняє прикладні процеси від необхідності таймаутів та повторних передач для забезпечення надійності.

Для протоколу IP четвертої версії управління трафіком базується на використанні поля заголовку пакета ToS (Type of Service – тип сервісу). Воно має містити дані щодо того, як має оброблятися дейтограма. Формат ToS визначено у RFC-1349, за ним поле складається із шести субполів. Перше субполе "Пріоритет" надає можливість присвоїти код пріоритету кожній дейтограмі.

0 – звичайний рівень;
1 – пріоритетний;
2 – негайний;
3 – терміновий;
4 – екстрений;
5 – критичний;
6 – міжмережеве управління;
7 – мережеве управління.

Наступні біти C, D, T та R характеризують побажання щодо способу доставки дейтограми. Так, D=1 вимагає мінімальної затримки, T=1 – високої пропускної здатності, R=1 – високої надійності, а C=1 – низької вартості. ToS відіграє важливу роль у маршрутизації пакетів. Інтернет не може гарантувати бажаний ToS, але більшість маршрутизаторів враховує ці запити при виборі маршруту (протоколи OSPF та IGRP).

До середини 90-х років минулого століття поле ToS у більшості реалізацій ігнорувалося. Із початком розробок засобів забезпечення якості обслуговування (QoS) увага до нього зросла. З'явилася пропозиція заміни поля ToS на поле DSCP (Differenciated Services Code Point – точка

коду диференційованих послуг), яке, як бачимо на рис. 2, також має 8 біт (RFC-2474). Останні біти (CU) не визначені. Іноді це поле називається байтом DS (Differenttiated Services – диференційовані послуги).

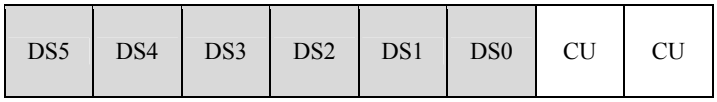

Рис. 2. Формат поля DSCP

Біти DS0-DS5 визначають селектор класу. Значення цього коду наведені в *табл. 2*. Стандартним значенням DSCP є 000000.

Таблиця 2

Значення поля "DSCP"

Селектор класу	DSCP
Пріоритет 1	001000
Пріоритет 2	010000
Пріоритет 3	011000
Пріоритет 4	100000
Пріоритет 5	101000
Пріоритет 6	110000
Пріоритет 7	111000

На базі DSCP розроблена технологія PHB (per Hop Behavior – поведінка на ретрансляційній ділянці). У рамках цієї політики визначаються коди DSCP всередині класів. Наприклад, для політики негайної переадресації EF рекомендоване значення DSCP=101110. Ця політика відповідає найбільш високому рівню обслуговування.

Замість поля DSCP у новому стандарті IPv6 міститься 4-бітове поле пріоритету, що дозволяє швидко ідентифікувати відносний пріоритет пакету. Значення пріоритетів поділяється на два діапазони. Перші 8 значень (від 0 до 7) використовуються для встановлення пріоритету трафіку (*табл. 3*).

Наступні значення від 8 до 15 використовують для визначення пріоритету трафіку, для якого не відбувається зниження потоку у відповідь на сигнал перевантаження мережі. Так, при передачі мультимедійної інформації, де управління швидкістю передачі неможливе, рівень пріоритету трафіку не може бути нижче 8.

Для трафіку, що не контролюється на перевантаження, значення пріоритету 8 має використовуватися для тих пакетів, втрата яких допустима у разі перевантаження мережі (наприклад, відео високої якості), а вище значення (15) варто використовувати для пакетів, втрата яких не бажана (аудіотрафік із низькою надійністю). Зв’язку між відносними пріоритетами із контролем та без контролю перевантаження мережі не існує.

Таблиця 3

Значення кодів пріоритету

Код пріоритету	Значення
0	Нехарактеризований трафік
1	Заповнюючий трафік (наприклад, мережеві новини)
2	Несуттєвий інформаційний трафік (електрона пошта)
3	Резерв
4	Суттєвий трафік (FTP, HTTP, NFS)
5	Резерв
6	Інтерактивний трафік (telnet, x-terminal, SSH)
7	Керуючий трафік (маршрутні протоколи, SNMP)

Ще одне поле заголовку IPv6, що може бути використане для виділення пакетів, обробка яких потребує нестандартної QoS або "real-time" сервісу – 24-бітове поле "Мітки потоку". Потік тут розглядається як послідовність пакетів, що пересилаються від відправника визначеному одержувачу, при цьому всі пакети потоку мають бути оброблені певним чином. Характер такої обробки може бути передано маршрутизатору через протокол управління або всередині самих пакетів, наприклад, в опції hop-by-hop.

Допускається декілька потоків між відправником та одержувачем, а також обмін, що не асоційовано з жодним потоком. Потік однозначно визначається комбінацією адреси відправника та ненульовою міткою потоку. Пакети, що не належать жодному потоку, мають мітку рівну нулю.

Маршрутизатори можуть довільно обирати спосіб обробки потоків даних, якщо отримують пакети із невідомою ненульовою міткою. У такому випадку пакет може бути оброблено так, як і при нульовій мітці. Маршрутизатор може занести в кеш результати такої обробки (адреса відправника та мітка утворюють ключ кешу). Наступні пакети із тією ж адресою відправника та міткою потоку можуть оброблятися із використанням інформації із кешу без детального перегляду всіх полів. Режим обробки пакетів із використанням кешу анулюється не пізніше 6 секунд після встановлення незалежно від того, продовжують поступати пакети даного потоку чи ні. Якщо приходить інший пакет після відміни режиму використання кешу, він оброблюється так само, як перший (як пакет із нульовою міткою), така ситуація може бути причиною повторного формування кеш-режиму.

Для пристроїв, що не підтримують функцію помітки потоків, це поле має при формуванні пакету містити нульове значення, передаватися без змін при переадресації та ігноруватися при отриманні. На даному етапі це експериментальний метод, який може значно змінитися вже найближчим часом.

Планування. Для надання пріоритету певному виду трафіку використовують планування. Цей елемент визначає декілька безкласових алгоритмів обробки черг.

Найпростішим із них є FIFO: перший прийшов – першим пішов. Він використовується в більшості маршрутизаторів та комутаторів. Принцип традиційного алгоритму FIFO полягає в тому, що в разі перевантаження пакети поміщаються у чергу, а при припиненні перевантаження передаються на вихід у тому порядку, в якому поступили, тобто "першим прийшов – першим пішов". Основною перевагою FIFO є простота реалізації та відсутність потреби в конфігурації. Недоліком – неможливість диференційованої обробки пакетів різних потоків, усі пакети стоять у загальній черзі на рівних підставах.

Дещо складнішим є алгоритм SFQ (стохастична справедлива черга). Цей алгоритм використовують у випадках, коли необхідно розподілити порівну можливість передачі даних між довільною кількістю потоків. Це досягається використанням хеш-функції для розподілення трафіку на окремі черги типу FIFO, які потім циклічно оброблюються. Оскільки існує вірогідність співпадіння значення хеш-функції, вона періодично змінюється. Для налаштування SFQ використовують два параметри: sfq-perturb – вказує через який час необхідно змінювати хешуючу функцію визначення під-черг та pcq-allot (quantum), який визначає кількість байтів у під-черзі, зазвичай встановлюється рівним одному максимальному об’єктові передачі.

Цей алгоритм працює за таким принципом: функція вилучення пакетів із під-черг одночасно випускає у вихідний інтерфейс pcq-allot байт, а керуючий алгоритм додає до кожної під-черги pcq-allot байт, при цьому зберігаючи рівновагу та однакову довжину всіх під-черг.

Недолік SFQ полягає в тому, що один додаток може відкрити декілька потоків і "заглушити" інші підключення. Для вирішення цієї проблеми був розроблений алгоритм ESFQ (розширена стохастична справедлива черга). На відміну від SFQ, він дає більше можливостей для управління чергою. Для цього він має такі параметри: depth – максимально можлива кількість "псевдо-черг", limit – кількість пакетів, що зберігаються в буфері, hash – задає тип хешу (classic як і в SFQ, src – за адресою джерела або dst – за адресою одержувача), divisor – задає довжину хеша у бітах.

Більш функціональним, але також окремим випадком SFQ, є алгоритм PCQ (черга за з’єднаннями). Він може не тільки формувати черги за адресами джерела або одержувача, а й використовувати окремі порти джерела або одержувача. Також він має параметри pcq-rate – число, яке вказує в якій пропорції розподіляти трафік за чергами, pcq-limit – довжина під-черги, pcq-total-limit – загальна кількість пакетів у всіх чергах.

Завдяки своїм параметрам алгоритми ESFQ та PCQ достатньо гнучкі, вони дозволяють розділити пропускну смугу між усіма підключеннями та додатками порівну.

По-іншому працює RED (довільне раннє виявлення), цей алгоритм організації черги розроблений для запобігання перевантажень і вирівнювання пропускної смуги. Контролюючи розмір черги, він не дає їй перевищити встановлені розміри шляхом знищення випадково обраних пакетів. Тому він використовується лише для протоколів транспортного рівня, які здатні помітити втрату пакету та відреагувати відповідним чином.

Використання алгоритму RED доцільне на високошвидкісних магістралях зі значною смугою пропускання. Для застосування цього алгоритму необхідно визначити його параметри: min – мінімальна довжина черги в байтах, max – значення, при досягненні якого знищуються всі "зайві" пакети, burst – максимальна кількість пакетів, які можуть бути прийняті до черги понад встановлений ліміт. Додатково можна вказати параметри limit та avpkt. Перший задає обсяг черги, другий – усереднений розмір пакету.

Складнішим алгоритмом обробки черги є TBF (фільтр блоку токенів). Він передає отримані пакети зі швидкістю, яка не перевищує заданий поріг, але з можливістю її перевищення короткими сплесками. Це найкращий алгоритм для обмеження трафіку – при великий точності він не перевантажує мережу та процесор. Алгоритм базується на використанні токенів. Пакети передаються при наявності достатньої їх кількості. При нестачі токенів, пакети переміщуються у буфер, у разі переповнення якого, знищуються. Конфігураційні параметри TBF, які задають довжину черги пакетів – limit (розмір буферу в байтах) та latency (час знаходження пакету в буфері). Розмір буфера токенів завдає параметр burst/buffer/maxburst. Він визначає максимальну кількість байт даних, для яких доступні токени в один момент часу. Ще один параметр – mpu визначає мінімальну кількість токенів, які необхідні для передачі "нульового" пакету. Останній параметр – rate – завдає обмеження смуги пропускання.

Об'єднання елементів. Наступним кроком у розвитку систем управління трафіком стало поєднання класифікації із плануванням. У результаті виникли класові алгоритми обробки черг. Різноманітні фільтри класифікують трафік і здійснюють подальшу обробку відповідно до заданих для цього класу правил.

Найпростішою дисципліною класифікації трафіку є PRIO. Ця черга може розділяти трафік між трьома смугами пропускання, які можуть бути чергами, побудованими за раніше розглянутими алгоритмами. Кожна під-черга має свій пріоритет, який визначає значення handle. Розподіл трафіку заснований на використанні фільтрів або поля ToS. Основні параметри prio-черги це bands (кількість смуг пропускання, як правило три) та priomap – розподіл трафіку залежно від поля ToS.

Організація черги за алгоритмом PRIO корисна, якщо необхідно підвищити загальну пропускну здатність інтерфейсу. Цей алгоритм ефективний у мережах, побудованих на основі UNIX, оскільки додатки Microsoft, як правило, встановлюють у поле ToS привілейоване значення

"Інтерактивний". Звісно, крім поля ToS, можливе використання власних дисциплін класифікації трафіку, однак у такому випадку, простішим варіантом буде застосування складнішого алгоритму.

Найстаршим та одним із найскладніших є алгоритм CBQ (заснована на класах черга). Як і PRIO, цей алгоритм може класифікувати трафік і назначати класам пріоритети. Крім класифікації, ця дисципліна може виконувати шейпінг трафіку. На її основі побудовані найбільш популярні схеми розподілу.

Принцип роботи CBQ полягає у забезпеченні вільного каналу на час, який відповідає заданому обмеженню смуги пропускання. Для цього дисципліна розраховує інтервали часу, які мають витримуватися між передачею пакетів.

Крім обмеження смуги пропускання, CBQ може також розподіляти трафік за класами із різними пріоритетами та відповідним чином їх обробляти. Кожний раз при передачі пакету ініціюється циклічний процес зваженого вибору (WRR), починаючи з класу із найвищим пріоритетом. WRR містить класи, які можуть містити будь-які інші дисципліни. Ці класи отримують ширину каналу відповідно до наданих їм коефіцієнтів. Такі коефіцієнти можна задати у ручному режимі або автоматично, в такому випадку розмір коефіцієнту задається обернено пропорційним обсягу даних, які передаються через клас.

WRR має внутрішній класифікатор, який розподіляє пакети на різні класи. Визначення відправника або одержувача може здійснюватись на основі MAC або IP адрес. MAC адреси можуть використовуватися лише в Ethernet мережах. Прив'язка хостів до класів відбувається автоматично, при появі перших пакетів.

CBQ надає багато можливостей для управління трафіком, але основним її недоліком є недостатня документованість та складність розуміння і налагодження.

Сучаснішою дисципліною є HTB (ієрархічний блок токенів), вона працює так само, як і CBQ, але принцип роботи її базується не на визначені часу простою, а на обчисленні обсягу трафіку. Ця дисципліна, як і TBF, використовує ідею токенів. Завдяки підтримці класів та технології займу смуги пропускання, вона дозволяє організувати складне та тонке управління трафіком.

В основі HTB лежить побудова ієрархії класів. Схематично її можна уявити у вигляді гібридного, розділеного на рівні дерева, кінцевими верхівками якого є користувачі. Трафік класифікується та потрапляє у класи-листя дерева, яке описує ієрархічну структуру регулятора. Внутрішні класи дерева відповідальні за розподіл "надлишків" смуги пропускання. Кореневий клас (весь канал) розподіляє трафік між класами-нащадками, відповідно до їхнього налаштування, а вони, у свою чергу, розподіляють між своїми нащадками.

Таким чином, кожний клас має два параметри – максимальна швидкість (ceil rate) та гарантована швидкість (rate). Перший обмежує ширину смуги пропускання, яку може зайняти нижчий у ієрархії клас у батьківському. Також для кожного класу задається пріоритет (від 0 до 7), який визначає черговість отримання надлишку смуги пропускання класами-нащадками.

Постійно розробляються нові версії HTB. Остання реалізація більш швидка та набагато точніша за CBQ, крім того, набагато простіша і зрозуміліша у налаштуванні.

Маркування та знищення. Для позначення класифікованих пакетів використовується механізм маркування, що дозволяє визначити подальшу долю пакету – шлях його доставки, порядок обробки, знищення у разі неприйнятності.

Знищення отриманих даних, які вже зайняли частину пропускної смуги та згаяли час на свою обробку, є небажаним. Як правило, знищують лише пошкоджені пакети, подальша обробка яких неможлива або може призвести до помилок. У деяких випадках може бути доцільним знищення всіх пакетів, що не відповідають певним параметрам – належать до іншої мережі, завеликі та ін.

Обмеження вхідного та вихідного трафіку. Вхідний трафік обмежується у разі порушення параметрів профілю (перевищення середньої швидкості або тривалості пульсації). Тоді пакети знищуються або маркуються зі зниженням пріоритету. Обмеження вихідного трафіку реалізується шляхом буферезації пакетів й використовується для зменшення пульсації трафіку або обмеження вихідного каналу.

Резервування. Як зазначалось вище, для деяких видів трафіку затримка пакетів є неприпустимою. Виникнення затримки може призвести до обмеження функціонування програм або припинення їхньої роботи. Збільшення пропускної здатності у таких випадках не вирішує проблему, адже непередбачуваний сплеск трафіку може зумовити несвоєчасне отримання пакетів.

Для забезпечення умов, необхідних для функціонування таких додатків, застосовують резервування смуги пропускання. Для цього використовують протокол RSVP (протокол резервування ресурсів). Він був розроблений ще для Windows 2000, його специфікація міститься у RFC 2205. RSVP працює комплексно. Відправник відсилає отримувачу повідомлення PATH, що формує список пристроїв, які проходить, та у відповідь одержує RESV із характеристиками сформованого каналу зв'язку, якщо все обладнання підтримує цей протокол. Якщо ж комутатор не здатен забезпечити пропускну смугу або не підтримує RSVP, повідомлення відхиляється.

Використання RSVP вимагає підтримки від усіх пристроїв та наявності достатньої смуги пропускання, щоб мати можливість, не заважаючи іншим додаткам, резервувати її частину. Велика кількість параметрів,

витрати на встановлення та управління каналом зв'язку частково компенсується при групуванні маршрутів. RSVP-повідомлення одним потоком від відправника прямують до точки групування та розсилаються отримувачам.

Найширші можливості управління трафіком надає технологія MPLS – багатопротокольна комутація за мітками. Вона дозволяє інкапсулювати різні протоколи передачі даних, як у мережах із комутацією каналів, так і комутацією пакетів, та створювати віртуальні канали між вузлами мережі. Принциповою основою MPLS є тунелі. Для її роботи необхідна підтримка протоколу MP-BGP (RFC-2858).

Використання MPLS надає переваги в управлінні потоками даних, підвищує надійність та продуктивність мережі. За цією технологією до кожного пакету (чарунки, фрейму) додається заголовок, що містить одну або декілька міток. Пакет, що отримав мітку, не може залишити межі віртуальної мережі. Декілька міток називають стеком міток. Розміщується стек між заголовками мережевого та канального рівнів. Кожний запис у стеку міток складається із чотирьох полів:

- значення мітки (20 біт);
- поле класу трафіку та повідомлення про перевантаження (3 біти);
- прапор дна стеку (Bottom of Stack) – якщо він встановлений, ця мітка остання у стеку (1 біт);
- поле TTL (8 біт).

Для тих самих вузлів, у разі необхідності, може бути сформовано декілька віртуальних мереж, що використовуватимуть різні мітки, для трафіку із різним рівнем пріоритету. Маршрутизатори на вході або виході MPLS-мережі називають LER (граничний маршрутизатор), вони додають або видаляють мітку пакету даних. Всередині мереж використовуються маршрутизатори LSR (маршрутизатор комутації за мітками), що комутують пакети лише на основі міток. Мітки між LER та LSR розподіляються за допомогою протоколу розподілу міток (LDP). LSR постійно обмінюються інформацією про наявні ресурси і стан мережі. До суб'єктів мережі ця інформація доводиться через IPG (протокол внутрішньої маршрутизації), алгоритм якого базується на стані каналу.

Управління трафіком у мережі MPLS виключає необхідність ручної конфігурації маршрутів. MPLS оцінює смугу каналу та значення трафіку при прокладці маршруту через опорну мережу. Динамічна адаптація дозволяє збільшити стійкість до відмови, здійснюючи корекцію топології мережі. MPLS надає гнучкі засоби моніторингу трафіку в межах VPN.

Для реалізації технології управління трафіком MPLS мережа має підтримувати:

- безпосередньо MPLS;
- IP-переадресацію CEF (швидка комутація Cisco);
- протокол маршрутизації IS-IS (проміжна система до проміжної системи).

Перевантаження. Окремим розділом керування трафіком є управління перевантаженнями. Перевантаження виникають при зверненні багатьох користувачів до одного ресурсу та можуть виражатися у затримках, втраті пакетів чи значному падінні продуктивності мережі.

Проблему перевантаження начебто можна розв'язати збільшенням буферної пам'яті. Однак це лише затримає початок перевантаження. Крім того, великий розмір буферів може значно збільшити затримку передачі пакетів. Контроль за виникненням перевантажень – проблема не з легких, існує багато алгоритмів управління перевантаженнями. У загальному випадку можна розділити їх на два класи: управління із явними втратами (open-loop control) та управління із повторною передачею (closed loop control).

Управління з явними втратами запобігає появі перевантаження, контролюючи, щоб трафік, що генерується відправником, не погіршив характеристики до рівня нижче заданої якості обслуговування. Якщо неможливо гарантувати задану якість обслуговування, мережа відхиляє запропонований трафік. Функція, що вирішує прийняти або відхилити новий трафік, названа "управління доступом". Із іншого боку, управління із повторною передачею реагує на перевантаження, коли воно вже відбувається або збирається з'явитись, регулюючи трафік відповідно до стану мережі.

Останнім часом набуває популярності управління трафіком на рівні об'єднаних потоків або проектування трафіку (traffic engineering), що має за мету розподілити об'єднанні потоки по мережі таким чином, щоб якомога ефективніше використовувати її ресурси. Тут важливими параметрами є швидкість, відстань і рівень завантаження каналів мережі для визначення шляху яким можлива найшвидша доставка повідомлення адресатові.

Висновки. Завдання побудови та впровадження методів управління трафіком не з легких. Необхідно враховувати безліч деталей, щоб максимально використовувати ресурси мережі. Налаштування гнучкої та ефективної системи управління трафіком вимагає часу, знань та значних зусиль, а іноді й коштів. Немає універсальної схеми, яка б задовольнила потреби більшості мереж. Для кожного випадку необхідно здійснювати всебічний аналіз ресурсів мережі та трафіку, за результатами якого проектувати систему управління трафіком. Натомість грамотно спроектована та втілена система здатна підвищити ефективність мережі та подовжити строк її використання.

На основі викладеного можна зробити певні узагальнення.

Першочерговими задачами при управлінні трафіком є мінімізація втрат пакетів і затримок, оптимізація пропускної здатності та узгодження найкращого рівня послуг. Для вирішення цих задач необхідно дотримуватись певних правил.

По-перше, ефективне управління потоками пакетів можливе тільки при неповному завантаженні каналу в обох напрямах. Тобто необхідною умовою є обмеження швидкості каналу. Достатньо заповнити один напрям на 100 %, щоб якість зв'язку помітно погіршилася.

По-друге, для запобігання утворенню черг та максимального контролю над потоком даних маршрутизатор, що обмежує потік до розміру, меншого за реальну пропускну здатність каналу, необхідно встановлювати в найвужчому місці каналу.

По-третє, обмеження швидкості можливе лише для вихідного трафіку. Знищення вхідного трафіку небажане, бо втрачаються вже отримані данні.

По-четверте, кожен інтерфейс мусить використовувати дисципліну обробки черг, а при застосуванні класових дисциплін обов'язково використовувати підкласи.

Перехід на IPv6 значно розширить можливості управління трафіком за рахунок використання міток потоків. Ця властивість буде мати велике значення при обробці мультимедійних даних, наприклад, програм цифрового телебачення, відеоконференцій тощо.

Вибір засобів управління трафіком потребує чіткого розуміння задач, а їх застосування – відповідного рівня знань та підтримки обладнанням обраних технологій.

У подальших дослідження доцільно здійснити порівняльний аналіз протоколів IP четвертої та шостої версій для визначення ефективності їх використання в локальних мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *RFC 2430:* A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE) / T. Li, Y. Rekhter. — 1998, October.
2. *RFC 2674:* Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions / E. Bell, A. Smith, P. Langille, A. Rijhsinghani, K. McCloghrie. — 1999, August.
3. *RFC 2702:* Requirements for Traffic Engineering Over MPLS. D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus. — 1999, September.
4. *RFC 5543:* BGP Traffic Engineering Attribute / H. Ould-Brahim, D. Fedyk, Y. Rekhter. — 2009, May.
5. *Олифер В. Г.* Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. — 4-е изд. — СПб., Питер, 2010. — 943 с.
6. *Велихов А. В.* Компьютерные сети : учеб. пособие / А. В. Велихов, К. С. Строчников, Б. К. Леонтьев. — М. : Новый издат. дом, 2005. — 304 с.
7. *Беркман Л. Н.* Повышение показателей качества систем управления гетерогенными сетями [Доклад] / Беркман Любовь Наумовна // Международный конгресс "Доверие и безопасность в информационном обществе", 2004.
8. *Лемешко А. В.* Повышение масштабируемости управления трафиком и обеспечения качества обслуживания с использованием оверлейных

сетей / А. В. Лемешко, Ахмад М. Хайлан // Проблемы телекоммуникаций. — 2010. — № 1 (1). — С. 35–44.
9. *Многоуровневое* управление трафиком в сети MPLS-TE DiffServ на основе координационного принципа прогнозирования взаимодействий / А. В. Лемешко, О. А. Дробот, Ю. Н. Добрышкин // Проблемы телекоммуникаций. — 2011. — № 1 (3). — С 11–27.
10. *Лемешко А. В.* Модель многопутевой QoS-маршрутизации в мультисервисной телекоммуникационной сети / А. В. Лемешко, О. А. Дробот // Радиотехника: Всеукр. межвед. науч.-техн. сб. — 2006. — Вып. 144. — С. 16–22.
11. *Муранов О. С.* Удосконалення механізму згладжування пакетного трафіку типу "відро токенів" / О. С. Муранов // Проблеми інформатизації та управління : зб. наук. пр. — К. : НАУ, 2009. — № 2 (26). — С. 125–130.
12. *Механізми* керування ресурсами пакетних мереж : тези наук.-практ. конф. "Захист в інформаційно-комунікаційних системах", (Київ, 24–25 травня 2007 р.) / М-во освіти і науки України, Національний авіаційний університет [та ін.]. — К. : НАУ, 2007. — С. 25–26.
13. *RFC 1349:* Type of Service in the Internet Protocol Suite / P. Almquist. — 1992, July.
14. *RFC 2474:* Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers / K. Nichols, S. Blake, F. Baker, D. Black, 1998, December.
15. *RFC 2205:* Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification / R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin. — 1997, September.
16. *RFC 2858:* Multiprotocol Extensions for BGP-4 / T. Bates, Y. Rekhter, R. Chandra, D. Katz. — 2000, June.

Стаття надійшла до редакції 03.06.2012.

Pikulitska J. Traffic management in the Ethernet network.

Problem statement. *The proposed scientific work is devoted to topical issue of traffic management of computer networks. In conditions of the continuous growth and complication of networks, the problem of a choice of ways for management to control traffic acquires actuality.*

Review of scientific sources *of chosen subjects proves the interest in research of traffic management both in Ukraine and abroad. However, the majority of the work considers the general theoretical principles. But solving a specific problem requires an understanding of the goals, a comprehensive analysis of the particular network and resources.*

Research objective *– the analysis of ways of managing traffic on Ethernet networks that will help to define effective approaches to taffic management.*

Results of research*. In the article the technologies of traffic management, their application, features and shortcomings have been considered. The detailed description of all the elements of modern systems of traffic management has been given, the protocols and technologies used to control the quality of service, control of broadcast traffic and reservation of zones have been described.*

Conclusions. *The conducted research highlights the existing technologies of traffic management of computer networks. It makes recommendations on creation of the system of traffic management.*

Key words: traffic management, service quality, service type, reservation, algorithm of line processing, overloading, MPLS, RSVP.

REFERENCES

1. *RFC 2430:* A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE) / T. Li, Y. Rekhter. — 1998, October.
2. *RFC 2674:* Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions / E. Bell, A. Smith, P. Langille, A. Rijhsinghani, K. McCloghrie. — 1999, August.
3. *RFC 2702:* Requirements for Traffic Engineering Over MPLS. D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus. — 1999, September.
4. *RFC 5543:* BGP Traffic Engineering Attribute / H. Ould-Brahim, D. Fedyk, Y. Rekhter. — 2009, May.
5. *Olifer V. G.* Komp'juternye seti. Principy, tehnologii, protokoly / V. G. Olifer, N. A. Olifer. — 4-e izd. — SPb., Piter, 2010. — 943 s.
6. *Velihov A. V.* Komp'juternye seti : ucheb. posobie / A. V. Velihov, K. S. Strochnikov, B. K. Leont'ev. — M. : Novyj izdat. dom, 2005. — 304 s.
7. *Berkman L. N.* Povyshenie pokazatelej kachestva sistem upravlenija geterogennymi setjami [Doklad] / Berkman Ljubov' Naumovna // Mezhdunarodnyj kongress "Doverie i bezopasnost'' v informacionnom obshhestve", 2004.
8. *Lemeshko A. V.* Povyshenie masshtabiruemosti upravlenija trafikom i obespechenija kachestva obsluzhivanija s ispol'zovaniem overlejnyh setej / A. V. Lemeshko, Ahmad M. Hajlan // Problemy telekommunikacij. — 2010. — № 1 (1). — S. 35–44.
9. *Mnogourovnevoe* upravlenie trafikom v seti MPLS-TE DiffServ na osnove koordinacionnogo principa prognozirovanija vzaimodejstvij / A. V. Lemeshko, O. A. Drobot, Ju. N. Dobryshkin // Problemy telekommunikacij. — 2011. — № 1 (3). — S 11–27.
10. *Lemeshko A. V.* Model' mnogoputevoj QoS-marshrutizacii v mul'tiservisnoj telekommunikacionnoj seti / A. V. Lemeshko, O. A. Drobot // Radiotehnika: Vseukr. mezhved. nauch.-tehn. sb. — 2006. — Vyp. 144. — S. 16–22.
11. *Muranov O. S.* Udoskonalennja mehanizmu zgladzhuvannja paketnogo trafiku typu "vidro tokeniv" / O. S. Muranov // Problemy informatyzacii' ta upravlinnja : zb. nauk. pr. — K. : NAU, 2009. — № 2 (26). — S. 125–130.
12. *Mehanizmy* keruvannja resursamy paketnyh merezh : tezy nauk.-prakt. konf. "Zahyst v informacijno-komunikacijnyh systemah", (Kyi'v, 24–25 travnja 2007 r.) / M-vo osvity i nauky Ukrai'ny, Nacional'nyj aviacijnyj universytet [ta in.]. — K. : NAU, 2007. — S. 25–26.
13. *RFC 1349:* Type of Service in the Internet Protocol Suite / P. Almquist. — 1992, July.
14. *RFC 2474:* Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers / K. Nichols, S. Blake, F. Baker, D. Black, 1998, December.
15. *RFC 2205:* Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification / R. Braden, Ed., L. Zhang, S. Berson, S. Herzog, S. Jamin. — 1997, September.
16. *RFC 2858:* Multiprotocol Extensions for BGP-4 / T. Bates, Y. Rekhter, R. Chandra, D. Katz. — 2000, June.