

УДК 004.7

Контроль якості послуг комп'ютерних мереж

Бельков Д.В., Єдемська Є.М.
Донецький національний технічний університет
belkov@telenet.dn.ua

Abstract

Belkov D.V., Edemskaya E.N. The control quality of service. Quality of Service (QoS) is the term used to define the ability of a network to provide different levels of service assurances to the various forms of traffic. It enables network administrators to assign certain traffic priority over others or actual levels of quality with respect to network bandwidth or end-to-end delay. The analysis of methods QoS control is proposed in this article.

Вступ

Довгий час з моменту появи мереж пакетної комутації розробка стандартів була зосереджена на протоколах взаємодії, а не на обміні інформації, тому аспекти якості обслуговування (QoS) випадали з контексту стандартизації. Недоліки протоколів з відсутністю QoS більш виразно виявляються в ситуаціях з високим навантаженням мереж. Зараз концепції QoS приділяється багато уваги, наприклад, в стандартах ATM (Asynchronous Transfer Mode). Сучасною тенденцією є перехід від різномірних мереж, кожна з яких призначена для виконання вузького кола послуг, до мультисервісних мереж наступного покоління (NGN). Невід'ємною частиною системи керування такої мережі повинна бути система керування QoS. Існує багато публікацій [1,2], що присвячено забезпеченню якості обслуговування. Проте, проблема керування якістю послуг комп'ютерних мереж залишається актуальною.

Метою даної роботи є аналіз методів і засобів контролю якості послуг сучасних комп'ютерних мереж. У ній розглядаються задачі, що виникають у системі керування QoS.

Особливості контролю якості послуг

Задача контролю якості в комп'ютерних мережах виникає внаслідок складної поведінки мережі при зміні навантаження і профілю трафіку. Системи зв'язку на основі технології IP є дуже складними завдяки використуванню в них принципів динамічної маршрутизації.

Проблеми експлуатації мереж NGN в загальному випадку зводяться до дуже емкої формули: будь-які параметри роботи мереж NGN знаходяться в прямій залежності від профілю трафіку в мережі. Сам же профіль трафіку динамічно змінюється і, як наслідок, змінюються параметри. NGN є технологією динамічною і сильно корельованою. З цієї причини зміни в мережах NGN можуть носити непередбачуваний

і лавиноподібний характер. Може виникати „ефект доміно”, коли робота цілих сегментів починає бути нестійкою. Профіль навантаження визначається наступними п'ятьма параметрами потоку (у разі потоку датаграм IP):

- Рівня інтенсивності трафіку (GAP);
- Довжини датаграми (L);
- Пріоритетності комутації датаграм (Pr);
- Адреси каналного (MAC) і мережевого (IP) рівня.

Норми на QoS відповідно до рекомендацій RFC-2544, використані для паспортизації потоку в даний час включають наступні параметри:

- Пропускню спроможність (Throughput - Th);
- Затримку передачі даних (Latency -Lat) і її розподіл (Latency Distribution – LD);
- Кількість помилок в потоці (Frame Errors – FE).

В результаті при описі динаміки зміни параметрів якості навіть одного потоку, має місце наступна залежність

$$\vec{S}(Th, Lat, LD, FE) = f(GAP, L, Pr, MAC, IP),$$

тобто 9-мірний фазовий простір явища. Враховуючи, що весь профіль навантаження впливає на параметри якості не менше, ніж самі параметри потоку, це свідчить про теоретичну неможливість сформулювати повний опис поведінки параметрів якості мультисервісних мереж, оскільки має місце багатовимірне представлення і кількість вимірювань, що прагне до нескінченності. Таким чином навіть в найпростіших моделях NGN стикаються з багатопараметричною системою, поведінку якої не можливо моделювати з будь-якою точністю. З цієї причини всі спроби вирішити задачу планування розгортання NGN тільки модельними і обчислювальними засобами не є коректними.

Вихід з теоретичної безвиході може бути знайдено в практичному експерименті. В умовах, коли параметри якості виявляються залежними

від рівня навантаження на мережу, єдиним методом їх вимірювання є поєднання методів аналізу QoS з детальною трафіковою імітацією.

Метод трафікової імітації є складним експериментом, що вимагає глибоких знань про технологію, але його можна застосовувати на всіх етапах розвитку мережі:

1. Вибір устаткування під конкретну задачу;
2. Наладка при введенні нового сегменту;
3. Експлуатація, розвиток і модернізація мережі;

Методи вибіркового і суцільного контролю якості

Існує два підходи до контролю якості, що зв'язані із застосуванням методик вибіркового або суцільного контролю.

Вибірковий контроль якості може здійснюватися двома основними методами:

1. Розподілена система контролю на основі регламентних вимірювань;
2. Автоматична система вибіркового контролю.

В обох методах передбачається, що знання параметрів якості для певних частин системи дозволяє робити висновок про якість всієї мережі в цілому. Розподілена система, що заснована на регламентних вимірюваннях контролю припускає:

1. Наявність в кожній точці мережі вимірювальних засобів;
2. Наявність в кожній точці мережі експлуатуючого персоналу, здібного до проведення якісних і адекватних вимірювань параметрів якості;
3. Наявність загальної політики в області контролю якості, тобто схеми звітності, графіка проведення регламентних вимірювань, єдиної бази даних результатів;
4. Наявність експертної системи верхнього рівня, яка забезпечує виявлення трендів у роботі системи зв'язку.

Система має наступні недоліки:

1. У системі контролю якості задіється багато дорогої техніки і кваліфікованого персоналу;
2. Система вимагає великої роботи по підготовці фахівців і виробленню норм внутрішнього документообігу;
3. Система не забезпечує швидкої ідентифікації трендів в системі якості, оскільки заснована на ручних методах отримання результатів;
4. Система є негнучкою, так що будь-яка модифікація в системі контролю якості (збільшення кількості вимірюваних параметрів, зміна графіка вимірювань) вимагає перегляду роботи

всієї системи експлуатації.

Такі недоліки роблять практично недоцільним використання розподіленої системи контролю якості в умовах динамічної IP-мережі. Проте перевагою розподіленої системи на основі регламентних вимірювань є низька вартість апаратних засобів.

Вказаних недоліків позбавлена система, заснована на вибіркових вимірюваннях, що проводяться в автоматичному режимі. Основною ідеєю системи є імітація користувачів мережі автоматичними елементами (пробами), які фіксують параметри якості зв'язку та передають інформацію в автоматичному режимі в центр обробки даних, де проводиться статистичний аналіз даних.

Перевагами автоматичної системи контролю є:

1. Максимальна наближеність до користувача, імітація його роботи;
2. Автоматичний режим роботи, який не вимагає присутності персоналу на видалених вузлах;
3. Висока гнучкість, оскільки сценарії роботи пристроїв передаються автоматично з центру, так що будь-яка зміна процедури контролю якості робиться швидко;
4. Оперативність аналізу трендів в параметрах якості системи зв'язку, так що експлуатація може вжити заходи до пошуку і усунення несправностей.

Основними недоліками системи є:

1. Необхідність створення системи „розподіленого інтелекту”, тому проекти системи виявляються дорогими;
2. Необхідність використання засобів трафікової імітації, так що система контролю якості виявляється активним генератором службового трафіку і сама по собі може впливати на параметри якості;
3. Загальна для всіх методів вибіркового контролю проблема екстраполяції результатів вибіркового контролю на параметри якості всієї мережі.

Таким чином, для регламентних і автоматичних систем контролю якості існує паритет між оперативністю реакції системи і її вартістю.

Ідея суцільного контролю якості базується на принципі повного знання про всі елементарні компоненти мережі. Основним компонентом, навколо якого створюється система суцільного контролю якості є база даних, яку можна назвати базою даних xDR у разі контролю параметрів комутованої мережі. Як засіб збору інформації виступає територіально розподілений вимірювальний комплекс (ТРВК).

Ідеологія ТРВК ґрунтується на використуванні системи вимірювальних засобів, об'єднаних в мережу обробки даних.

Централізована система контролю на базі ТРВК показана на рисунку 1.

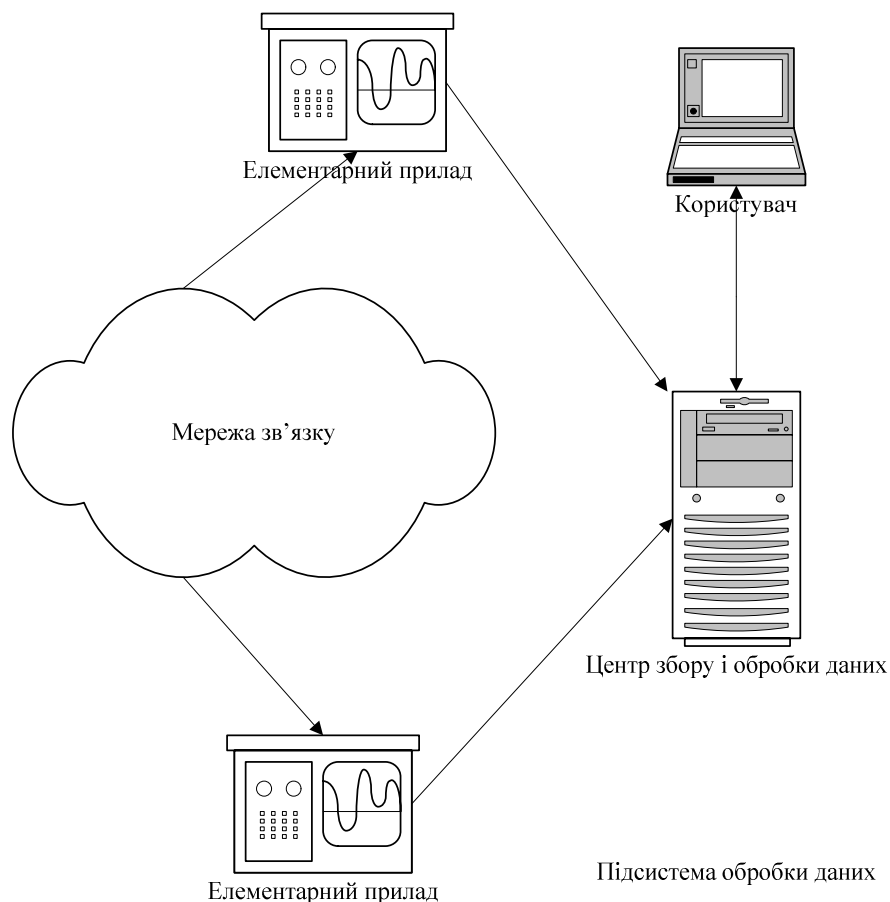


Рисунок 1 – Система контролю з ТРВК

ТРВК складається з двох підсистем: підсистеми збору і підсистеми обробки даних. Підсистема збору даних складається зі сукупності елементарних приладів (ЕП), що мають визначені методики вимірювань і тестові сценарії, інтерфейсів підключення ЕП до мережі, каналів обміну даними між ЕП і системою обробки даних. Підсистема обробки даних включає центр збору даних від ЕП, бази даних xDR, засоби обробки статистичними методами даних від ЕП, пристрої і програмне забезпечення верхнього рівня, що забезпечує ефективне використання ТРВК.

Побудова централізованої системи контролю якості може бути виконана не тільки на основі ТРВК, але і на базі вбудованих діагностичних засобів у складі устаткування (OSS). Структура системи контролю включає три основні елементи:

- Вбудовані пристрої діагностики в складі устаткування систем передачі і комутації;
- Єдиний сервер з базою даних про стан і параметри ресурсу каналів з програмним

забезпеченням;

- Пристрої конвертації форматів даних.

Для конвертації форматів даних застосовуються програмно-апаратні засоби, що виконують перетворення даних в єдиний формат системи управління OSS.

Функціональність системи контролю ресурсу на основі вбудованих систем діагностики залежить від функціональності сенсорів у складі устаткування передачі і комутації. Важливим недоліком побудови системи контролю з орієнтацією на сенсори у складі устаткування є необхідність використання великої кількості конвертерів формату даних. Для кожного типу устаткування повинен існувати свій унікальний програмно-апаратний модуль.

Порівняний аналіз побудови різних варіантів централізованої системи показано у таблиці 1.

Таблиця 1. Варіанти побудови системи

Параметр	Система на основі OSS	Система на основі ТРВК
Підключення до мережі	До сенсорів устаткування	До каналів передачі трафіку
Необхідність конвертації даних	Існує	Немає необхідності
Можливість активної реконфігурації	Є	Немає, пасивна система
Зміна ПЗ пристроїв	Впливає на роботу системи	Не впливає на роботу системи
Оперативність діагностики	Висока	Висока
Оперативність реакції персоналу	Висока	Низька

Обґрунтування стратегії контролю якості для систем IP

У цьому розділі пропонується аналіз варіантів побудови системи контролю якості з урахуванням специфіки сучасних мереж IP.

На відміну від телефонних мереж, де кількість викликів пов'язана з кількістю

користувачів і має об'єктивні обмеження, в мережах IP кількість транзакцій, що генеруються одним користувачем надто велика. З цієї причини виникають наступні проблеми з побудовою централізованих систем експлуатації мереж IP:

1. Розмір бази xDR є критичним параметром;
2. Об'єм трафіку мережі IP якісно відрізняється від об'єму телефонного трафіку;
3. Розмір бази xDR не дозволяє створити оперативного рішення. Об'єм бази значно уповільнює оперативність обробки звернень до неї.
4. Розмір централізованої системи контролю якості об'єктивно впливає на вартість такої системи.
5. Вартість системи суцільного контролю у разі мереж IP наблизатиметься до вартості самої мережі.

Аналіз вказаних проблем приводить до висновку, що для побудови систем контролю якості сучасних мереж IP неможливе застосування методів суцільного контролю на основі єдиної бази даних xDR. Систему варто засновувати на методах вибіркового контролю якості.

Класифікація систем контролю якості, що пропонується у даній роботі, показана на рисунку 2.



Рисунок 2- Класифікація систем контролю якості

Ефективним методом контролю якості є імітація крайового користувача при зверненні його до різних послуг. Компанія PR-GROUP [3,4] пропонує для цієї мети в мережі IP використовувати аналізатор якості послуг Avalanche 220/2200.

Прилад Avalanche є одночасно генератором і аналізатором трафіку верхніх рівнів і може бути застосованим для вимірювань якості послуг. Він має мережеве розширення з використанням ПЗ Scheduler, що дозволяє об'єднувати будь-яку кількість Avalanche в єдину

систему контролю якості, діючи за певним сценарієм. Аналізатор Avalanche імітує роботу користувача, формуючи еталонні запити на надання послуг. Відповідний додаток мережі відповідає на запит і параметри якості надання послуги (затримка, пропускна спроможність додатку, параметри якості додатку) аналізуються. Тестовий трафік від аналізатора Avalanche може „підмішуватися” до трафіку користувачів. Принцип заміру якості за допомогою Avalanche показано на рисунку 3.

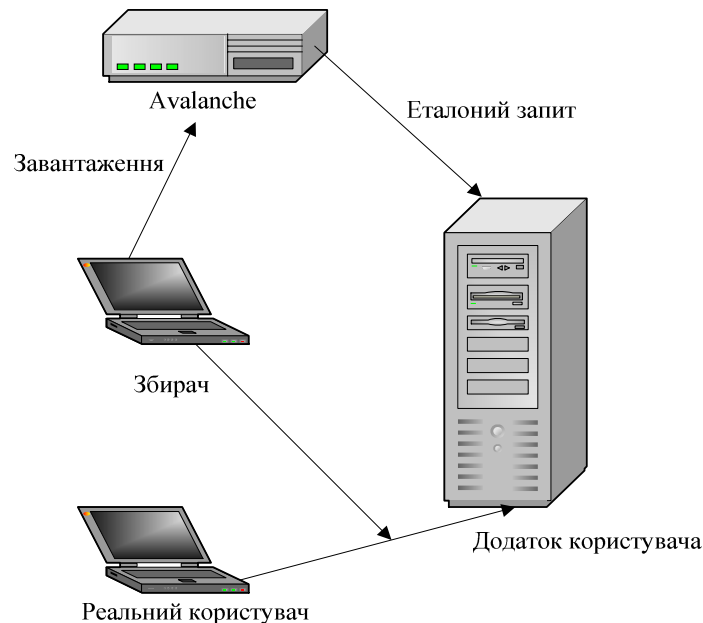


Рисунок 3- Використання Avalanche

Основні характеристики аналізатора [5]:

- Точна імітація поведінки користувача в мережі
- Підтримка всіх основних протоколів
- Об'єднання функцій аналізатора, редактора звітів і спеціалізованого аналізатора
- Підтримка необмеженої кількості віртуальних користувачів
- Зручне графічне меню установки параметрів тесту

Аналізатор дозволяє виконувати наступні дії:

- Аналіз роботи будь-яких Інтернет-додатків в мережі оператора
- Тестування продуктивності сайтів і порталів
- Контроль безпеки обміну даними через Інтернет
- Тестування різних програмно-апаратних компонентів сайту
- Контроль якості основних і додаткових послуг в сітках передачі даних
- Контроль транспортної мережі

Аналізатор Avalanche є засобом для формування і редагування звітів. Аналізатор Avalanche дозволяє виміряти параметри якості послуг в пакетній мережі і відобразити дані будь-якого типу аналізаторів сімейства Avalanche. Основними функціями аналізатора Avalanche є:

- Аналіз трендов в зміні параметрів якості послуг в мережі

- Формування сценарію заходів для поліпшення роботи окремих додатків і мережі в цілому
- Формування звітів для системи експлуатації мережі

Для аналізатору Avalanche розроблені методи контролю додатків безпеки, методи контролю доступу до сайтів і контролю послуг e-mail. Аналізатор Avalanche може розглядатися як еталонний користувач.

Система на основі аналізаторів Avalanche може розгортатися поступово, вона не вимагає зв'язку з OSS і фіксації різних профілів трафіку. Проте у такої системи методика вимірювань параметрів якості рівня додатків має важливий недолік. У разі виникнення несправності на верхньому рівні в складі ПЗ додатку практично неможливо ідентифікувати її причину. Розділення несправностей між транспортною мережею і додатком є істотною проблемою застосування аналізаторів класу Avalanche. Щоб виключити вплив несправностей верхніх рівнів доцільне створення не тільки еталонного користувача, але і еталонного додатку.

Застосування еталонного додатку виключає вплив ПЗ верхнього рівня на погіршення якості послуг. З урахуванням необхідності контролю якості по кожному напрямку доцільно використовувати в кожній точці контролю VPN пари Avalanche/Reflector, як показано на рисунку 4.

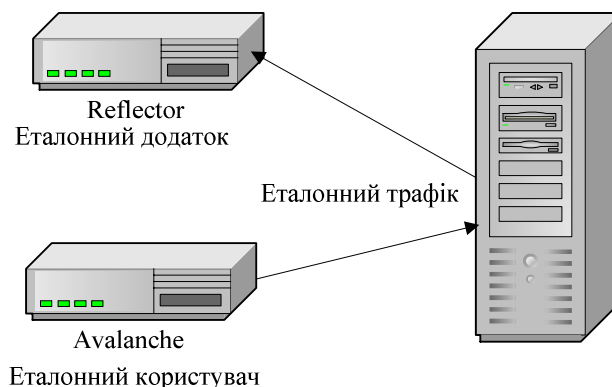


Рисунок 4- Використання Avalanche/Reflector

Основу системи складають аналізатори Avalanche/Reflector, використовувані парами при генерації запитів/відповідей в прямому і зворотному напрямі. Аналізатори розміщуються в місцях надання послуг. Генеруючи трафік з різними адресами IP та установками, кожен аналізатор Avalanche дозволяє тестувати до декількох сотень VPN. Тестовий трафік „підмішується” до трафіку мережі і використовується для моніторингу параметрів якості в режимі реального часу. Формування сценарію, збір даних про параметри якості і формування звітів виконується мережевим ПЗ Scheduler.

Для формування централізованої системи контролю якості компанія PR-GROUP [3] пропонує дві основні системи: SmartSight і Avalanche. Порівняння двох систем показує, що система SmartSight є повнофункціональною системою моніторингу якості, що має значно більшу функціональність в порівнянні з системою Avalanche. Проте вимога тісної прив'язки системи до OSS оператора і відповідних вимог до функціональності розгорненої OSS робить проект її розгортання досить дорогим. У протилежність системі SmartSight система Avalanche може бути реалізована на мережі будь-якого оператора мультисервісної мережі.

Висновки

В роботі запропоновано класифікацію систем контролю якості послуг комп'ютерних мереж, проаналізовані переваги і недоліки методів вибіркового і суцільного контролю якості. Отримані наступні результати:

1. Розвиток сучасних мультисервісних мереж висуває вимогу створення систем контролю якості в мережах IP.
2. Для формування систем контролю якості існують розподілені і централізовані рішення.
3. Критичним для роботи системи експлуатації недоліком розподіленої системи є її низька реакція на зміну параметрів якості. Тому єдиним варіантом побудови системи контролю якості є централізована система.
4. Специфіка мереж IP накладає певні обмеження на централізовані системи контролю якості. На відміну від систем контролю якості в телефонній мережі ці системи не можуть створюватися на основі єдиної бази даних xDR.
5. Централізовані системи контролю якості IP не можуть реалізувати принципи суцільного контролю.
6. Пріоритетним напрямом щодо розгортання системи контролю якості мережі IP, є використання системи Avalanche.

Література

1. Flannagan M. Administering Cisco QoS in IP networks. – NY.: Syngress, 2003. – 561p.
2. Танненбаум Э. Компьютерные сети. – СПб.: Питер, 2003. – 992с.
3. Принципы контроля качества услуг в сетях IP. // [Електронний ресурс], 2008. – Режим доступу: http://www.pr-group.ru/qos_scope/index.html
4. Магдэйд К. Анализ и сравнение контроля QoS (качества услуг). // [Електронний ресурс], 2007. – Режим доступу: http://www.wireless-e.ru/assets/files/pdf/2008_4_44.pdf
5. Портативный анализатор приложений Avalanche 220. // [Електронний ресурс], 2009. – Режим доступу: <http://www.kuravida.com/portable/avalanche/avalanche-220.html>

Надійшла до редакції 30.03.2010