

УДК 004.72

Г.М. Мручок

Тернопільський національний технічний університет імені Івана Пулюя, Україна

ОПТИМІЗАЦІЯ МЕРЕЖІ MPLS НА ОСНОВІ МЕТОДІВ TRAFFIC ENGINEERING

H.M. Mruchok

OPTIMIZING MPLS NETWORK BASED METHODS TRAFFIC ENGINEERING

Під терміном Traffic Engineering розуміють методи і механізми збалансованого завантаження всіх ресурсів мережі за рахунок раціонального вибору шляху проходження трафіку через мережу. Механізм управління трафіком надає можливість встановлювати явний шлях, яким передаватимуться потоки даних.

Функція MPLS Traffic Engineering (TE) дозволяє мережі сервіс-провайдеру емулювати можливості інжинірингу трафіку, що існують в мережах 2-го рівня, таких як Frame Relay і ATM. Інжиніринг трафіку на рівні 3 дозволяє контролювати окремі мережеві маршрути, знижуючи ймовірність перезавантаження і підвищуючи економічність передачі IP-трафіку в мережах, що маршрутизуються. Мета інжинірингу трафіку на рівні 3 полягає в тому, щоб максимально задіяти в роботі всі мережеві ресурси.

Технологічно MPLS TE ґрунтується на формуванні маршрутів проходження пакетів (LSP) через мережу за допомогою механізму створення тунелів (MPLS Tunnel), який в свою чергу базується на основі міток (Labels Stack). Примітивний MPLS TE можна забезпечити, вручну встановивши тунелі, відповідні необхідним напрямкам проходження трафіку [1].

Для вирішення завдань мінімізації перевантажень у процесі керування трафіком найбільш перспективними є методи Traffic Engineering (TE). Для спрощення завдання оптимізації вибір шляхів для деякого набору потоків може здійснюватися по черзі, при цьому обмеженням є сумарне завантаження кожного ресурсу мережі.

Зазвичай вважається, що внутрішньої продуктивності маршрутизатора вистачить (в середньому) для обслуговування будь-якого трафіку, який здатні прийняти інтерфейси маршрутизатора. Тому в якості обмеження виступають тільки максимально допустимі значення коефіцієнтів завантаження каналів зв'язку, що встановлюються індивідуально або ж мають спільне значення.

У MPLS TE існує метод відновлення послуг. Це досягається за допомогою функції захисту каналів або швидкої переадресації (Link Protection або Fast Reroute). Функція FRR може захистити від збою індивідуальний канал.

Час комутації захищених каналів FRR підібраний так, щоб відповідати стандартам SONET/SDH (близько 50 мс). Це означає, що кожен канал LSP може бути захищений за допомогою резервного маршруту, який починає працювати з моменту відмови каналу, незалежно від головного маршрутизатора (head-end-router). Ця технологія відрізняється від простого захисту каналу, коли саме головний маршрутизатор активізує роботу резервного каналу.

Література

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов: 3-е изд./ В. Г. Олифер, Н. А.Олифер // – СПб.: Питер, 2006.