УДК 004.72
Т. Лобур, О. Мацюк, Ю. Шилінська-Лобур
(Тернопільський національний технічний університет імені Івана Пулюя)

АНАЛІЗ МОНІТОРИНГУ ТРАФІКУ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Трафік – це об'єм даних або кількість пакетів, які передаються через мережеві канали за певний проміжок часу. В процесі комунікації користувачів у мережі виникає потік повідомлень, який може бути охарактеризований як кількість переданих бітів.

Важливим завданням при побудові та оптимізації комп'ютерної мережі є правильне налаштування системи моніторингу та діагностики її роботи. Мережевий адміністратор повинен точно підрахувати спожитий трафік для кожного вузла мережі, а також вирішити проблеми безпеки. До них можна віднести захист локальної мережі від зовнішніх атак, обмеження доступу до різних ресурсів (наприклад заборона доступу в соціальні мережі), попередження розповсюдження вірусів, налаштування кешування для зниження навантаження на канали зв'язку, блокування завантаження реклами і певних типів файлів на персональні комп'ютери користувачів.

Вказані задачі вирішуються за допомогою встановлення комплексної системи аналізу трафіку комп'ютерної мережі.

Аналіз трафіку комп'ютерної мережі – це процес перехоплення мережевого трафіку і його перевірка з метою визначення процесів, що відбуваються в мережі.

Система мережевого моніторингу надає можливість відслідковувати дії користувачів в межах локальної комп'ютерної мережі, а також отриманий трафік з глобальної мережі. Аналізатор відслідковує все, що проходить через мережу: інформацію користувачів, електронну пошту, миттєві повідомлення, веб-доступ, завантаження файлів.

Знання принципів роботи комп'ютерних мереж дозволяє на практиці забезпечити постійний контроль за їх роботою, що необхідно для підтримки мережі в робочому стані. На етапі моніторингу виконується збір початкових даних про роботу мережі: статистики про кількість циркулюючих в мережі фреймів та пакетів різних протоколів, стан інтерфейсів комутаторів та маршрутизаторів.

Для того щоб виміряти інтенсивність передачі трафіку в мережах даних, потрібно зареєструвати кожен відправлений і отриманий пакет. Для цього існують спеціальні аналізатори пакетів, які дозволяють виконати більш складний аналіз трафіку, а саме: розмір пакету, визначити час отримання пакету для певного типу протоколу, систематизувати отриману інформацію у вигляді графіків, таблиць і діаграм.

Отримані дані, повинні містити IP адреси відправника і одержувача, номери портів протоколів на транспортному рівні, об'єм переданих даних. Це може відноситись як до окремих пакетів, так і до потоків.

Статистичний аналіз базується на порівнянні поточного стану мережі з визначеними заздалегідь ознаками, які характеризують коректне функціонування мережевої інфраструктури. Методи статистичного аналізу мають різні інтерпретації, засновані на динамічних характеристиках мережевого трафіку.

Аналіз мережевого трафіку потрібно проводити для виявлення аномальної поведінки комп'ютерної мережі: збоїв в роботі, негативної зовнішньої дії, випадкових помилок, а також для моделювання типових атак, та перехоплення потоку даних, якими обмінюються відправник і отримувач. Це вкрай необхідно як для вирішення завдань мережевого адміністрування, так і для моніторингу коректного функціонування інфраструктури комп'ютерних мереж.