УДК 004.921

Пєтух Анатолій Михайлович,
д.т.н., професор кафедри програмного забезпечення,
Вінницький національний технічний університет, Україна

***Гончарук Віталій Вікторович**, студент групи 1ПЗ-15мі,*
факультет інформаційних технологій та комп'ютерної інженерії,
Вінницький національний технічний університет, Україна

СПОСОБИ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

У статті розглянуто способи аналізу трафіку комп'ютерної мережі.
***Ключові слова:** комп'ютерна мережа, мережевий трафік.*

The article discusses different methods of computer network traffic analysis.
Keywords: computer network, network traffic.

Вступ. Облік мережевого трафіку є актуальним, і для його реалізації існує ряд програмних і технічних засобів. Зокрема, він реалізується в комерційних цілях при наданні послуг доступу до мережі. Однак зібрані при цьому дані не завжди можна вважати досить об'єктивними, так як обидві сторони - постачальники послуг і абоненти мережі - прагнуть змістити показники трафіку в свою користь або ж іноді невірно ідентифікувати об'єкт свого інтересу до мережі. На підставі даних про трафік в багатьох випадках можуть бути зроблені висновки про фактори, що визначають активність користувачів, а також про об'єкти їх найбільшого інтересу. Таким чином, облік мережевого трафіку фактично є частиною політики щодо забезпечення інформаційної та економічної безпеки фірм і організацій.

Мета дослідження – автоматизація процесу моніторингу та аналізу мережевого трафіку.

Об'єктом дослідження є процес отримання доступу до даних про трафік комп'ютерної мережі. **Предметом дослідження** є сучасні засоби реалізації програмних додатків: середовище .NET, мова програмування C#. **Головною задачею роботи** є розробка програмного додатку моніторингу та аналізу трафіку комп'ютерної мережі.

Моніторинг трафіку комп’ютерної мережі. Дослідження мережевого трафіку показали, що він являє собою складний динамічний процес і є суперпозицією багатьох потоків з множинними взаємопов'язаними характеристиками, які генеруються різними протоколами. По-перше, це трафіки, пов'язані з управлінням комп’ютерної мережі (КМ), наприклад, трафік ініціалізації клієнтів, серверний трафік і т.д., які генеруються періодично. По-друге, це трафіки мережевих сервісів, додатків (наприклад, DNS, FTP, сеанс NetBIOS, HTTP, P2P, SMTP і т.д.) і протоколів, які становлять основну частину мережевого трафіку КМ.

Основним етапом визначення класифікаційних характеристик мережевого трафіку є процес вимірювання мережевого трафіку [1]. На підставі вимірювання дослідник може отримати важливу інформацію про властивості мережевого трафіку. При цьому вимірювання можуть бути проведені різними способами, в різних місцях мережі і в різні періоди часу і тривалості. Місце вимірювання вказує на те, яка частина або елемент КМ, а також яка величина вимірюється. При цьому дуже важливо розрізняти вимірювання мережевого трафіку від ідентифікації додатків, так як в першому випадку здійснюються збір і обробка даних, а в другому випадку - розпізнавання і класифікація деяких характеристик мережевого трафіку. В свою чергу ідентифікація мережевого трафіку є невід'ємною частиною класифікації, так як класифікація неможлива без його ідентифікації.

Аналіз мережевого трафіку може бути здійснений на декількох абстрактних рівнях: на рівні номера портів, вмісту пакета, потоку, заголовка пакета і на рівні біта (тобто обсягу трафіку). При цьому характеристики мережевого трафіку на кожному рівні відрізняються, наприклад, на рівні пакета, мережевий трафік характеризується розміром пакета і часовим інтервалом між пакетами [2]. Аналіз на рівні біта стосується кількісних характеристик мережевої мережі, таких як інтенсивність передачі і пропускна здатність обміну в каналах мережі. На рівні пакета розглядається процедура прибуття IP-пакетів, тобто інтенсивність їх затримки і втрати пакетів.

Активний моніторинг повідомляє проблеми в мережі, збираючи вимірювання між двома кінцевими точками [3]. Система активного виміру має справу з такими метриками, як: корисність, маршрутизатори/маршрути, затримка пакетів, повтор пакетів, втрати пакетів, нестійка синхронізація між прибуттям, вимір пропускної здатності.

Головним чином використання інструментів, таких як команда ping, яка вимірює затримку і втрати пакетів, і traceroute, яка допомагає визначити топологію мережі, є прикладом основних активних інструментів вимірювання. Обидва ці інструменту посилають пробні ICMP-пакети до точки призначення і чекають, коли ця точка відповість відправнику. На рисунку 1 показано приклад команди ping, яка використовує активний спосіб вимірювання, посилаючи Echo-запит від джерела через мережу в встановлену точку. Потім одержувач посилає Echo-запит назад джерелу від якого прийшов запит.

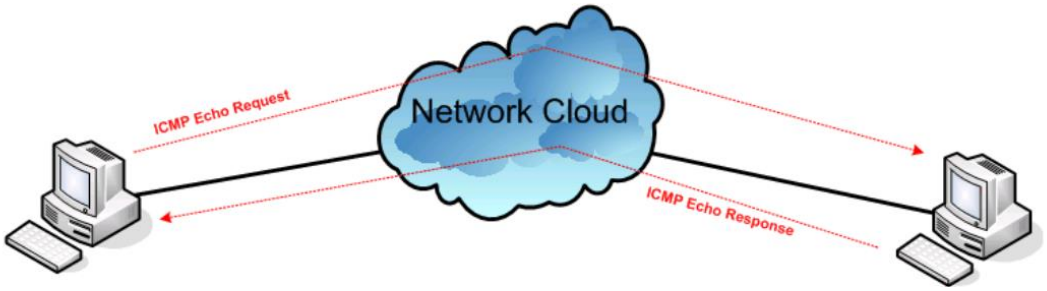

Рисунок 1 – Команда ping (активний моніторинг)

Ще один важливий приклад активного моніторингу - утиліта iperf. Iperf - це утиліта, яка вимірює якість пропускної здатності TCP і UDP протоколів. Вона повідомляє пропускну здатність каналу, існуючу затримку і втрати пакетів. Активний моніторинг - це надзвичайно рідкісний метод моніторингу, взятий окремо. Пасивний моніторинг навпаки не вимагає великих мережевих витрат.

Пасивний моніторинг на відміну від активного не додає трафік в мережу і не змінює трафік, який вже існує в мережі. Також на відміну від активного моніторингу, пасивний збирає інформацію тільки про одну точці в мережі. Вимірювання відбуваються набагато краще, ніж між двома точками, при

активному моніторингу. Рисунок 2 показує установку системи пасивного моніторингу, де монітор розміщений на одиничному каналі між двома кінцевими точками і спостерігає трафік коли той проходить по каналу.

Рисунок 2 – Установка пасивного моніторингу

Пасивні вимірювання мають справу з такою інформацією, як: трафік і суміш протоколів, кількість бітів, синхронізація пакетів і час між прибуттям. Пасивний моніторинг може бути здійснений, за допомогою будь-якої програми, що витягує пакети. Пасивний моніторинг кращий активного тому, що дані службових сигналів не додаються в мережу, але пост-обробка може забирати велику кількість часових витрат. Ось чому існує комбінація цих методів моніторингу.

Висновок. Мережевий трафік є одним з найважливіших фактичних показників роботи КМ і є носієм інформації про поведінку користувачів. На основі статистичного аналізу мережевого трафіку можна побічно визначити статистичні характеристики функціонування КМ.

Список використаної літератури

1. L.Zhanh and J.Tang, Characterization and performance study of IP traffic in WDM networks // Computer communications, 2001, No.24, pp.1702–1713.
2. Мониторинг сети [Електронний ресурс] // Режим доступу до матеріалу: http://www.4stud.info/networking/work2.html
3. Обзор методов анализа и мониторинга сетевого трафика [Електронний ресурс] // Режим доступу до матеріалу: http://it-bloknot.ru/?q=content/обзор-методов-анализа-и-мониторинга-сетевого-трафика.