МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАТИКА, МАТЕМАТИКА, АВТОМАТИКА

IMA :: 2016

МАТЕРІАЛИ
та програма

НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

(Суми, 18–22 квітня 2016 року)

Суми
Сумський державний університет
2016

Програмні засоби аналізу мережевого трафіку у корпоративних мережах

Кручиніна Д. М., *студент*; Великодний Д.В., *старший викладач*
Сумський державний університет, м. Суми

Постійний контроль за роботою корпоративної мережі, необхідний для підтримки її у робочому стані та забезпечення максимальної ефективності використання ресурсів.

Потреба реалізації аналізу мережевого трафіку визначається тим, що в роботі комп'ютерної мережі і мережевого стека вузлів періодично виникають проблеми, причину яких важко виявити загальновідомими утилітами для збору статистики і стандартними додатками на основі протоколу ICMP. У подібних випадках для діагностики неполадок часто доводиться використовувати більш специфічні засоби, які дозволяють відобразити мережевий трафік та проаналізувати його передачу на рівні протоколів.

Створення віртуальної моделі мережі в симуляторах дозволяє вивчити можливості популярних аналізаторів протоколів, а також характеристики, які є необхідними для оцінки якості передачі чутливого до затримок трафіка. У результаті були оцінені переваги і недоліки таких аналізаторів протоколів як Wireshark і CommView. Обидва аналізатора дають змогу на однаково високому рівні забезпечити адміністраторів мережі інформацією для виконання troubleshooting-а, виявлення несанкціонованого використання ресурсів мережі. Процес перехоплення пакетів відбувається за допомогою маніпулювання пакетами безпосередньо на рівні їх «конструювання».

Засобами платформи .Net, мови програмування C# і середовища розробки Visual Studio 2010 була створена програма-аналізатор трафіку Simple Sniffer. Можливості даної програми дозволяють отримати детальну інформацію про структуру IP, TCP / UDP пакетів, вибрати порт хоста для аналізу трафіку. Програма дозволяє виявити джерело розсилки мережевих пакетів та проаналізувати принципи інкапсуляції даних на різних рівнях мережевої моделі. Для створення даного програмного забезпечення використовувалась технологія raw-сокетів – пакет безпосередньо передається додатку і обробляється ефективніше ніж при проході через головний стек протоколів клієнта.