­­МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”

­­­

Лабораторна робота №2

з курсу «’Комп’ютерні мережі»

для студентів базового напрямку 6.08.04 "Комп’ютерні науки"

(заочна форма навчання)

Варіант 10

Виконав студент гр. КНз-3

Чалий Михайло

­­

Львів 2014

## Мета роботи

Метою роботи є ознайомлення з роботою аналізатора протоколів, отримання практичних навичок аналізувати потоки даних в локальній мережі.

## Теоретичні відомості

Виконання процедур керування в комп’ютерній мережі відбувається на чотирьох рівнях.

* Стеження (Control) – це контроль нижнього рівня, виконується постійно на першому–четвертому рівнях протоколу розподілено багатьма незалежними процедурами керування.
* Менеджмент (Management) – це функції керування сеансового та прикладного рівнів. До них належать налагодження та розірвання сеансу, одержання оплати за сеанси, рестарти.
* Обслуговування (Maintenance) передбачає підтримування мережі в робочому стані, ремонт, діагностування помилок з використанням спеціальних програм та технічних засобів діагностики.
* Адміністрування (Administration) – це нагляд за функціюванням мережі, ії запуск та зупинка; забезпечення ефективності роботи.

Моніторинг та мережеметрія - це безперервний контроль інформаційних та комунікаційних процесів у системі, збирання оперативних (моніторинг) та статистичних (мережеметрія) даних про якість функціювання мережі, використання її ресурсів тощо. Результати моніторингу попередньо опрацьовують та зберігають у спеціальних файлах моніторингу. На підставі цих даних за запитом адміністратора в будь-який час можна сформувати звіти.

Завдання монiторингу (мережеметрiї) та дiагностики КМ тiсно пов’язанi. Їх виконують однаковими засобами одночасно. Детальний монiторинг системи потрібний для шукання причин несправностей чи незадовiльного функцiювання. Для зручностi монiторинг доцiльно вести на рiзних рiвнях протоколу. Зокрема,

* на фiзичному рiвнi дослiджуються параметри кабельної системи;
* на канальному та мережевому рiвнях аналiзують трафiк, декодують та перехоплюють кадри і пакети;
* на верхніх рiвнях протоколу вивчають взаємодiю станцiй з використанням конкретних протоколiв та властивих їм параметрiв;
* на рiвнi застосувань можливий аналiз взаємодiї застосувань (наприклад, клiєнта та сервера бази даних).

Адмiнiстратора iнформацiйної системи передусім цiкавлять параметри взаємодiї застосувань. Однак причини неефективної роботи можуть бути зумовлені i роботою протоколiв нижніх рiвнiв або проблемами обладнання.

Крiм протокольного рiвня аналiзу, системи монiторингу та керування вiдрiзняються сферою дiї (вiд окремого сегмента до великої глобальної мережi), рiвнем iнтелекту та сервiсу (вiд простого перехоплення та вiдображення кадрiв до складних експертних систем аналiзу поведiнки).

Аналiзатор протоколу - це програмно-апаратний блок, безпосередньо приєднаний до мережi. Вiн приймає весь iнформацiйний потiк сегмента, декодує та iнтерпретує його.

Головні операцiї, якi виконує аналiзатор, - це перехоплення, декодування, вiдображення даних, генерування тестових даних. Адмiнiстратор мережi використовує функцiї iнiцiалiзацiї, фiльтрування та вiдображення у рiзних форматах.

Фiльтрування дає змогу видiлити з загального потоку пакети, якi мають певні ознаки. Сучаснi аналiзатори мають до кiлькох тисяч можливих умов фiльтрування, за допомогою яких можна комбiнувати умови i навiть задавати їх вручну.

Iнiцiалiзацiя допомагає пов’язати режими перехоплення та вiдображення з конкретними подiями. Визначена подiя (наприклад, надходження кадру визначеного протоколу або певної довжини чи звертання до заданого сервера) запускає перехоплення потоку.

Генерування тестових даних використовують для створення у мережi тестового потоку визначеного типу пакетiв заданої iнтенсивностi.

## Завдання

1. Запустіть програму аналізатора протоколів та оберіть вказаний адаптер.
2. Ознайомтеся з програмним інтерфейсом та кнопками керування.
3. Запустіть прослуховування потоків на визначений викладачем час (10- 15 хв.)
4. Зупиніть прослуховування.
5. Проаналізуйте загальну структуру передавання у каналі. Поясніть які протоколи використовуються, якій меті служить те чи інше передавання.
6. Проаналізуйте та запротоколюйте приклади структури пакетів найбільш вживаних протоколів – ARP, TCP, IP, ICMP.

Збережіть результати прослуховування на диску.

## Реалізація

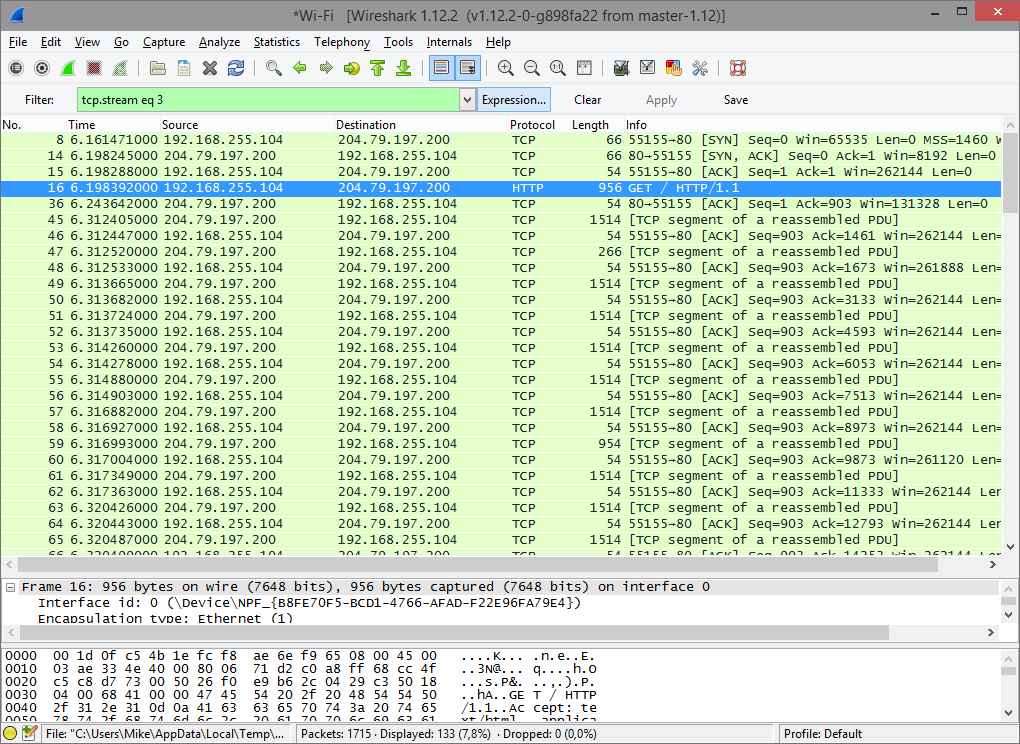


Рис 1. Комунікація через Wi-Fi

## Висновки

Ознайомився з роботою аналізатора протоколів, отримав практичні навички аналізу потоків даних в локальній мережі.