Львівський національний університет імені Івана Франка

Факультет прикладної математики та інформатики

Кафедра дискретного аналізу

**Комп’ютерні інформаційні мережі**

**Лабораторна робота №7**

Виконав:

Студент групи ПМі-33

Тимчишин Ярема

Прийняв:

Ас. Жировецький В.В.

Львів 2023

**Тема:** Wireshark (Network Layer).

**Мета роботи:** Здобути практичні навички з інтерпретації ІР-пакетів і повідомлень керуючих протоколів, а також використання консольних утиліт для діагностики мережі на мережевому рівні.

**Хід роботи**

1. Ознайомився з базовою мережевою конфігурацією мого комп’ютера, виконавши в консолі команду ipconfig:

Зображення, що містить текст, знімок екрана, Шрифт

Автоматично згенерований опис

1. Для отримання більш детальної конфігурації виконав команду ipconfig /all.

Зображення, що містить текст, знімок екрана

Автоматично згенерований опис

1. Користуючись відкритими джерелами, описав призначення команд ipconfig /renew та ipconfig /release:

* Команда ipconfig /release відпускає IP-адресу, що була надана комп'ютеру по DHCP. Після виконання цієї команди комп'ютер втрачає свою поточну IP-адресу і відключається від мережі.
* Команда ipconfig /renew намагається знову отримати IP-адресу від DHCP-сервера. Після виконання цієї команди комп'ютер пробує підключитися до мережі та отримати нову IP-адресу від DHCP-сервера.

1. Переглянув активні ТСР-з’єднання за допомогою команди netstat:

Зображення, що містить текст, знімок екрана, дизайн

Автоматично згенерований опис

Описав що означає кожен зі станів (TIME\_WAIT, ESTABLISHED, SYN\_SENT тощо):

* ESTABLISHED – цей стан показує активне та встановлене з'єднання між двома комп'ютерами. Дані можуть вільно передаватися між ними.
* SYN\_SENT – цей стан вказує на те, що комп'ютер ініціює з'єднання з іншим комп'ютером, але ще не отримав підтвердження про початок з'єднання від іншої сторони. Це початковий етап установки з'єднання.
* TIME\_WAIT – цей стан вказує на час очікування завершення з'єднання. Після закриття з'єднання одна сторона переходить в стан TIME\_WAIT, де вона очікує певний час, щоб переконатися, що всі пакети, пов'язані з цим з'єднанням, були оброблені повністю.
* CLOSE\_WAIT – цей стан вказує на те, що інша сторона закрила з'єднання, але місцевий комп'ютер ще не закрив свою частину з'єднання.

Дав відповідь на питання, як зміниться зміст і відображення з’єднань, якщо виконати команди netstat -n та netstat -a?

* Команда netstat -n показує стан з'єднань, протокол та порт у числовому форматі без відображення символьних імен (наприклад, вона не розглядає імена хостів або послуг). Вона виводить лише IP-адреси та порти в числовому форматі, що може спрощувати відображення, але робить інформацію менш зрозумілою для людини.
* Команда netstat -a виводить всі з'єднання та стани портів для всіх протоколів (TCP, UDP і т. д.). Вона також показує імена хостів, адреси, які використовуються для кожного з'єднання, та стани портів. Це дає більш деталізовану інформацію, включаючи стани портів та інші деталі, що можуть бути корисними для розуміння активних мережевих з'єднань.

1. Для отримання статистики про отримані/відправлені пакети виконав команду netstat -е.

Зображення, що містить текст, знімок екрана

Автоматично згенерований опис

З моєю мережею немає жодних фізичних проблем, помилки і відмови рівні нулю. Для отримання детальнішої статистики виконав команду netstat -s.

1. Запустив Wireshark у режимі адміністратора.
2. Від’єднався від мережі.
3. Почав захоплення пакетів.
4. Під’єднався до мережі.
5. Здійснив активність у браузері.
6. Закінчив захоплення пакетів та зберіг результат у файл.
7. Вибрав пакет для аналізу, клацнув на рядок Internet Protocol version 4 ... в області “Ієрархічний вміст пакета”. В області “Бітове подання” підсвітилися біти, які відповідають заголовку IP-пакета:

Зображення, що містить текст, число, програмне забезпечення, ряд

Автоматично згенерований опис

1. Розгорнувши заголовок, описав інформацію, яку надає кожне його поле.

Зображення, що містить текст, Шрифт, число, знімок екрана

Автоматично згенерований опис

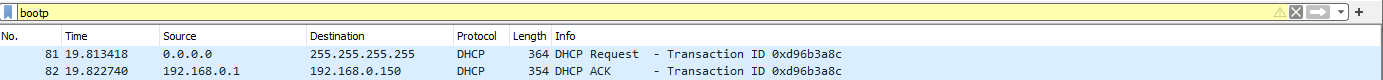
* 0100 .... = Version: 4 - Це поле вказує версію протоколу IP, у даному випадку, це IPv4.
* .... 0101 = Header Length: 20 bytes (5) - Це поле вказує довжину заголовка у 32-бітних словах. У даному випадку, заголовок має довжину 5 слів (20 байт).
* Total Length 671 - Це поле вказує загальну довжину пакету, включаючи заголовок та дані.
* Identification: 0x3873 (14451) - Це поле містить ідентифікатор пакета, який може використовуватися для реєстрації та відновлення фрагментів пакета.
* Flags 010. .... = Flags: 0x2, Don't fragment - Це поле містить флаги, такі як фрагментація. У даному випадку, встановлений флаг "Don't fragment", що означає, що пакет не повинен фрагментуватися.
* Fragment Offset: ...0 0000 0000 0000 = Fragment Offset: 0 - Це поле вказує зсув фрагменту у відношенні до початку пакета.
* Time to Live: 128 - Це поле вказує кількість маршрутизаторів, які пакет може перетнути, перед тим як бути видаленим.
* Protocol: TCP (6) - Це поле вказує верхній рівень протоколу, який використовується для транспорту даних. У даному випадку, це TCP.
* Header Checksum : 0x0000 [validation disabled] - Це поле містить контрольну суму заголовка для перевірки цілісності даних в заголовку.
* Source Address: 192.168.0.150 - Це поле містить IP-адресу відправника пакета.
* Destination Address : 51.104.176.40 - Це поле містить IP-адресу отримувача пакета.

1. Дав відповідь на запитання “Біти 0100 поля Версія (Version) дають десяткове число 4, яке відповідає протоколу IPv4. Чому тоді біти 0101 (десяткове число 5) поля Довжина заголовку (Header Length) відповідають значенню 20 байт, а не 5 байт?”.
   * Поле "Довжина заголовку" (Header Length) у заголовку IPv4 не вимірюється в десятковому форматі, а вказує на кількість 32-бітних слів, які складають заголовок. Значення 5 у полі "Довжина заголовку" вказує на кількість 32-бітних слів, які становлять заголовок IP. Оскільки кожне слово має розмір 32 біти (4 байти), множення 5 на розмір 4 байти дає загальну довжину заголовка у 20 байт (5 \* 4 = 20).
2. Дав відповідь на запитання (на прикладі свого пакету, а не на прикладі пакету, який досліджується тут) “Який розмір корисних даних?”.
   * 671 (Total Length) - 20 (розмір заголовка) = 651 байт корисних даних.
3. Дав відповідь на запитання (на прикладі свого пакету, а не на прикладі пакету, який досліджується тут) “Що Ви можете сказати про одержувача та відправника за виглядом їхніх ІР-адрес?”.
   * Адреса відправника належить до діапазону 192.168.x.x, що зазвичай використовується для локальних мереж, зазвичай в домашніх чи офісних середовищах.
   * Адреса одержувача належить до діапазону мультикастових адрес, що використовуються для групової комунікації, коли один передавач може відправити повідомлення кільком одержувачам одночасно.
4. Відшукав у відкритих джерелах інформацію про поле Тип обслуговування (раніше воно називалося ToS, тепер DSCP). Описав, з яких частин воно складається і яку інформацію несуть біти кожної частини:
   * Поле Differentiated Services (DSCP) в заголовку IPv4 містить інформацію про обробку пакета в мережі. Це поле складається з двох частин: Differentiated Services Codepoint (DSCP) і Explicit Congestion Notification (ECN).
     + Differentiated Services Codepoint (DSCP): Ця частина поля DSCP (шифрується в перших шести бітах) використовується для визначення класу обслуговування пакета. У моєму випадку, значення 000000 вказує на Default (загальний) клас обслуговування. Цей шестикодовий біт визначає пріоритетність обробки пакета мережею.
     + Explicit Congestion Notification (ECN): Ця частина поля (останні два біти) використовується для управління перенавантаженням мережі. У моєму випадку, значення 00 показує, що транспортний протокол не підтримує ECN або не використовує його для вказаного пакета. ECN дозволяє розпізнавати перенавантаження в мережі та зменшувати його, щоб уникнути втрати пакетів.

Зображення, що містить текст, знімок екрана, Шрифт, ряд

Автоматично згенерований опис

1. Дослідив протокол динамічної конфігурації хостів (DНCP). Для відображення пакетів цього протоколу скористався фільтром bootp:



1. Пояснив IP-адреси відправника та отримувача у DHCP-запиті:

Зображення, що містить текст, знімок екрана, Шрифт, число

Автоматично згенерований опис

* + IP-адреса відправника (Source Address): 0.0.0.0 - пристрій, який щойно підключився до мережі або хоче оновити свою IP-адресу, відправляє запит з нульовою IP-адресою в якості джерела, означаючи, що він ще не отримав IP-адресу.
  + IP-адреса отримувача (Destination Address): 255.255.255.255 - Це широкомовна (broadcast) адреса, яка призначена для спрощення розсилки повідомлення всім пристроям в мережі. У випадку DHCP-запиту, це означає, що запит адресований усім пристроям в мережі з метою отримання відповіді від DHCP-сервера.

1. Пояснив IP-адреси відправника та отримувача у DHCP-відповіді:

Зображення, що містить текст, знімок екрана, Шрифт, число

Автоматично згенерований опис

* + IP-адреса відправника (Source Address): 192.168.0.1 - Це IP-адреса DHCP-сервера, яка відправляє відповідь. DHCP-сервер призначає IP-адресу пристрою, який подав запит, і надсила відповідь зі своєю IP-адресою як джерелом.
  + IP-адреса отримувача (Destination Address): 192.168.0.150 - Це IP-адреса пристрою, який подав DHCP-запит і очікує відповідь від сервера. Цей пристрій стає отримувачем DHCP-відповіді.
  + Отже, в контексті DHCP-відповіді, IP-адреса відправника вказує на DHCP-сервер, який надіслав відповідь, а IP-адреса отримувача вказує на пристрій, який очікує та приймає відповідь від DHCP-сервера.

1. Розгортаючи по черзі опції, зазначив, яка інформація передається у DHCP-запиті:

Зображення, що містить текст, знімок екрана, Шрифт, число

Автоматично згенерований опис

* + Option: (53) DHCP Message Type (Request): Цей параметр вказує на тип DHCP-повідомлення, в даному випадку, це DHCP-запит.
  + Option: (61) Client Identifier: Цей параметр ідентифікує клієнта. У цьому випадку, це Ethernet-адреса клієнта (98:fa:9b:5b:b0:7a).
  + Option: (50) Requested IP Address: Цей параметр вказує на те, яку IP-адресу клієнт хоче отримати від DHCP-сервера. У цьому випадку, це 192.168.0.150.
  + Option: (12) Host Name: Цей параметр вказує на ім'я хоста (комп'ютера). У цьому випадку, ім'я хоста - DESKTOP-LTQSC69.
  + Option: (81) Client Fully Qualified Domain Name: Цей параметр містить повністю обліковий доменне ім'я клієнта, а також деяку іншу інформацію.
  + Option: (60) Vendor Class Identifier: Цей параметр вказує на ідентифікатор класу вендора (виробника) пристрою, у цьому випадку, MSFT 5.0.
  + Option: (55) Parameter Request List: Цей параметр містить перелік параметрів, які клієнт хоче отримати від DHCP-сервера. У вашому випадку, це включає підмережу, маршрутизатор, DNS-сервер, домен, інші параметри.
  + Option: (255) End: Цей параметр вказує на кінець списку параметрів у DHCP-запиті.

1. Виконав в консолі команду hostname і переконався що ім’я комп’ютера збігається з іменем у DHCP-запиті та з іменем у пункті 2.
2. Розгортаючи по черзі опції, зазначив, яка інформація передається у DHCP-відповіді:

Зображення, що містить текст, знімок екрана, документ, Шрифт

Автоматично згенерований опис

* + Option: (53) DHCP Message Type (ACK): Цей параметр вказує на тип DHCP-повідомлення, в даному випадку, це підтвердження (ACK) наданої IP-адреси.
  + Option: (54) DHCP Server Identifier: Цей параметр містить IP-адресу DHCP-сервера, який призначив IP-адресу клієнту.
  + Option: (51) IP Address Lease Time: Цей параметр вказує на той час, на який надано IP-адресу клієнту. У цьому випадку, це 7200 секунд (2 години).
  + Option: (58) Renewal Time Value: Цей параметр вказує на час, через який клієнт може знову запитати продовження оренди IP-адреси. У цьому випадку, це 3600 секунд (1 година).
  + Option: (59) Rebinding Time Value: Цей параметр вказує на час, через який клієнт може знову перевірити статус своєї IP-адреси, якщо сервер не відповідає на запит про оновлення. У цьому випадку, це 6300 секунд (1 година 45 хвилин).
  + Option: (1) Subnet Mask: Цей параметр містить підмережу, до якої належить IP-адреса клієнта.
  + Option: (28) Broadcast Address: Цей параметр вказує на широкомовну адресу відповідної підмережі.
  + Option: (6) Domain Name Server: Цей параметр містить IP-адресу DNS-сервера, яку клієнт повинен використовувати.
  + Option: (81) Client Fully Qualified Domain Name: Цей параметр містить повністю обліковий доменне ім'я клієнта та пов'язану інформацію.
  + Option: (3) Router: Цей параметр вказує на IP-адресу маршрутизатора, який клієнт повинен використовувати.
  + Option: (255) End: Цей параметр вказує на кінець списку параметрів у DHCP-відповіді.

1. Дослідив пакети міжмережевого протоколу керуючих повідомлень ICMP. Застосування фільтру icmp не дав бажаного результату:

Зображення, що містить текст, знімок екрана, програмне забезпечення, Шрифт

Автоматично згенерований опис

1. Для перехоплення ICMP-пакетів запустив заново Wireshark і після старту захоплення пакетів скористався консольною утилітою ping, яка працює на основі протоколу ICMP:

Зображення, що містить текст, знімок екрана, Шрифт

Автоматично згенерований опис

1. Для отримання ІР-адреси за заданим доменним іменем скористувався командою nslookup:

Зображення, що містить текст, Шрифт, знімок екрана

Автоматично згенерований опис

1. Зупинив захоплення пакетів і, відфільтрувавши їх з допомогою фільтру icmp, переконався, що тепер результат не порожній:

Зображення, що містить текст, знімок екрана, Шрифт, число

Автоматично згенерований опис

1. Дав відповідь на запитання “Чому поле TTL у запиті та відповіді мають різні значення?”.
   * Кожен маршрутизатор на шляху пакета зменшує значення TTL на одиницю. Таким чином, пакет може мати різні значення TTL у запиті та відповіді, залежно від кількості маршрутизаторів, які він пройшов.
2. Отримав повідомлення іншого типу, для цього під час запуску утиліти ping задав час життя пакету TTL = 1:

Зображення, що містить текст, знімок екрана, Шрифт

Автоматично згенерований опис

Зображення, що містить текст, знімок екрана, Шрифт, число

Автоматично згенерований опис

Порівняв ІР-адреси відправників відповідей у цих пакетах і пакетах, захоплених попереднього разу і пояснив відмінності:

* + Після команди ping google.com відправник має IP-адресу 216.58.209.14, це адреса пов'язана з google.com.
  + Після команди ping -i 1 google.com відправник має IP-адресу 192.168.0.1, тому що комп'ютер намагається спочатку використати локальні маршрутизатори (192.168.0.1), щоб встановити зв'язок зі стороннім сервером, таким як Google, замість надсилання запитів безпосередньо на сервер Google.

1. Для визначення маршруту, яким проходить пакет від мене до отримувача, скористався утилітою tracert. Запустив її у командному рядку, передавши аргументом google.com:

Зображення, що містить текст, знімок екрана, Шрифт

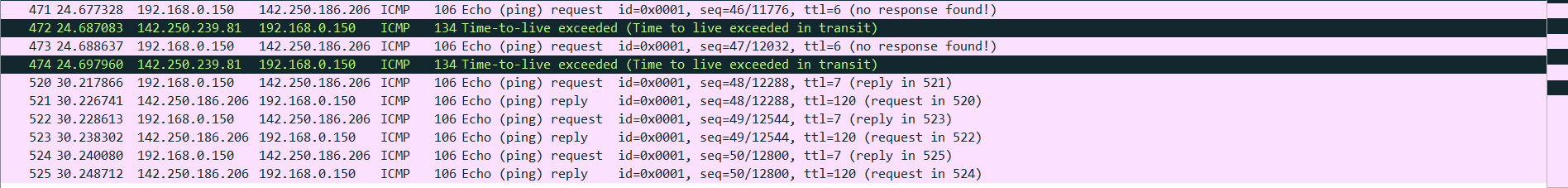
Автоматично згенерований опис

* + Щоб пакет потратив до сервера google.com з IP-адресою 142.250.186.206, йому потрібно пройти 6 проміжних маршрутизаторів.

1. Перехопив за допомогою Wireshark ICMP-пакети утиліти tracert/traceroute. У кожному запиті відмови зберігається IP-адрес проміжного маршрутизатора і з кожним разом TTL збільшується на один, якщо проміжний маршрутизатор стає іншим.

Зображення, що містить текст, знімок екрана, Паралель, Шрифт

Автоматично згенерований опис



**Висновок:** Під час виконання цієї лабораторної роботи, я здобув практичні навички з інтерпретації ІР-пакетів і повідомлень керуючих протоколів, а також використання консольних утиліт для діагностики мережі на мережевому рівні.