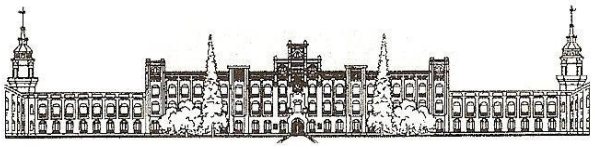

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»

Лабораторна робота №3

з дисципліни «Комп'ютерні мережі»

«Аналіз просування IP-пакетів в об'єднаній мережі з використанням аналізатора трафіку Wireshark. Рівень мережевих інтерфейсів. Фрагментація IP-дейтаграм»

Виконав студент групи: КВ-11

ПІБ: Терентьєв Іван Дмитрович

Перевірив: _____

Київ 2024

Мета роботи

Засвоєння функцій модулів мережевих інтерфейсів, структури заголовку кадру Ethernet, структури мережевого адаптера, процедури фрагментації IP-дейтаграм за допомогою аналізатора мережевого трафіку Wireshark.

План виконання лабораторної роботи

1. Ознайомитися та засвоїти теоретичні відомості, викладені в посібнику до лабораторної роботи.
2. За допомогою аналізатора Wireshark виконати захоплення та провести аналіз фрагментованих мережевих пакетів.

Завдання

1. В лабораторній роботі проводиться дослідження виконання фрагментації на мережевому рівні стеку TCP/IP. При виконанні роботи використовується програмне забезпечення для аналізу протоколів комп'ютерних мереж Wireshark.
2. Визначіть значення максимального розміру пакету MTU, який може бути переданий канальним рівнем без фрагментації на тому інтерфейсі Вашого комп'ютера, на якому буде відбуватися захоплення пакетів програмою Wireshark.

У Windows для цього можна скористатися командою із командного рядка

netsh interface ipv4 show subinterfaces,

а в Unix про значення MTU можна дізнатися за допомогою команди

ifconfig

В мережах типу Ethernet значення MTU зазвичай дорівнює 1500 байтів.

1. Запустіть програму Wireshark. Виберіть інтерфейс для захоплення трафіку (меню Capture/Interface) та активізуйте режим захоплення.
2. Перейдіть в командний рядок і виконайте команду ping, вказавши цільову IP-адресу, наприклад, вашого маршрутизатора і параметр -l xxxx, де значення xxxx має перевищувати значення MTU, щоб була виконана фрагментація (наприклад, 5000).
3. Після захоплення трафіку, який виник в результаті виконання команди ping, зупиніть захоплення програмою Wireshark. Приклад – на рис.3.11. Проведіть аналіз структури фрагментів, що утворилися. Зверніть увагу на процес фрагментації IP-дейтаграм, що відбувся, та на величину блоку корисного навантаження у фрагментованих пакетах.
4. Результати захоплення фрагментованих пакетів занесіть у звіт.

Теоретичні відомості

1. **Протокол IP та його роль** Протокол IP (Internet Protocol) є основним для передачі пакетів даних через мережі. Він відповідає за маршрутизацію пакетів, забезпечуючи їхнє доставлення до пункту призначення незалежно від маршруту, яким вони йдуть через мережу.
2. **Фрагментація IP-дейтаграм** Фрагментація — це процес поділу великих IP-дейтаграм на менші фрагменти, щоб їх можна було передавати через мережі з меншим значенням MTU (Maximum Transmission Unit). Процедура фрагментації відбувається тоді, коли розмір дейтаграми перевищує розмір MTU мережевого інтерфейсу.

Фрагментація виконується наступним чином:

- Якщо дейтаграма перевищує допустимий розмір MTU, вона ділиться на декілька фрагментів.
- Кожен фрагмент має свій IP-заголовок, який містить інформацію про ідентифікатор, прапори фрагментації (MF, DF) та зміщення фрагменту.
- Фрагменти передаються незалежно один від одного, і на кінцевому вузлі вони збираються в оригінальну дейтаграму.

3. **Рівень мережевих інтерфейсів** Мережевий інтерфейс складається з фізичного та канального рівнів. Він забезпечує передачу кадрів між пристроями. Протокол Ethernet найчастіше використовується на канальному рівні для інкапсуляції IP-пакетів у кадри Ethernet.
4. **ARP і MAC-адреси** ARP (Address Resolution Protocol) використовується для визначення MAC-адрес пристроїв у локальній мережі на основі їх IP-адрес. Це дозволяє передавати пакети на фізичному рівні за MAC-адресами.
5. **DNS-запити** DNS (Domain Name System) відповідає за перетворення доменних імен в IP-адреси. Клієнтські пристрої відправляють запити до DNS-серверів для отримання відповідних IP-адрес для доменних імен, таких як www.example.com.

Хід роботи

```
C:\Users\t3ry4>netsh interface ipv4 show subinterfaces

   MTU  MediaSenseState   Bytes In  Bytes Out  Interface
------  ---------------  ---------  ---------  -------------
4294967295                1          0          0  Loopback Pseudo-Interface 1
  1500                1   29389760    2891958  Ethernet
  1500                1          0      17484  Ethernet 2


C:\Users\t3ry4>
```

Рис. 1 – Визначення значення MTU на ОС Microsoft Windows

На рис. 1 можна побачити стандартний розмір MTU для Ethernet, а саме 1500 байтів.

```
C:\Users\t3ry4>netsh interface ipv4 show subinterfaces

   MTU  MediaSenseState   Bytes In  Bytes Out  Interface
------  ---------------  ---------  ---------  -------------
4294967295                1          0          0  Loopback Pseudo-Interface 1
  1500                1   29389760    2891958  Ethernet
  1500                1          0      17484  Ethernet 2


C:\Users\t3ry4>ping -l 5000 192.168.88.1

Pinging 192.168.88.1 with 5000 bytes of data:
Reply from 192.168.88.1: bytes=5000 time=1ms TTL=64
Reply from 192.168.88.1: bytes=5000 time=1ms TTL=64
Reply from 192.168.88.1: bytes=5000 time=1ms TTL=64
Reply from 192.168.88.1: bytes=5000 time=1ms TTL=64

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\t3ry4>
```

Рис. 2 – Виконання виклику ping з розміром MTU 5000 байтів до маршрутизатора

Перед виконанням ping виклику(рис. 2) було запущене захоплення у Wireshark

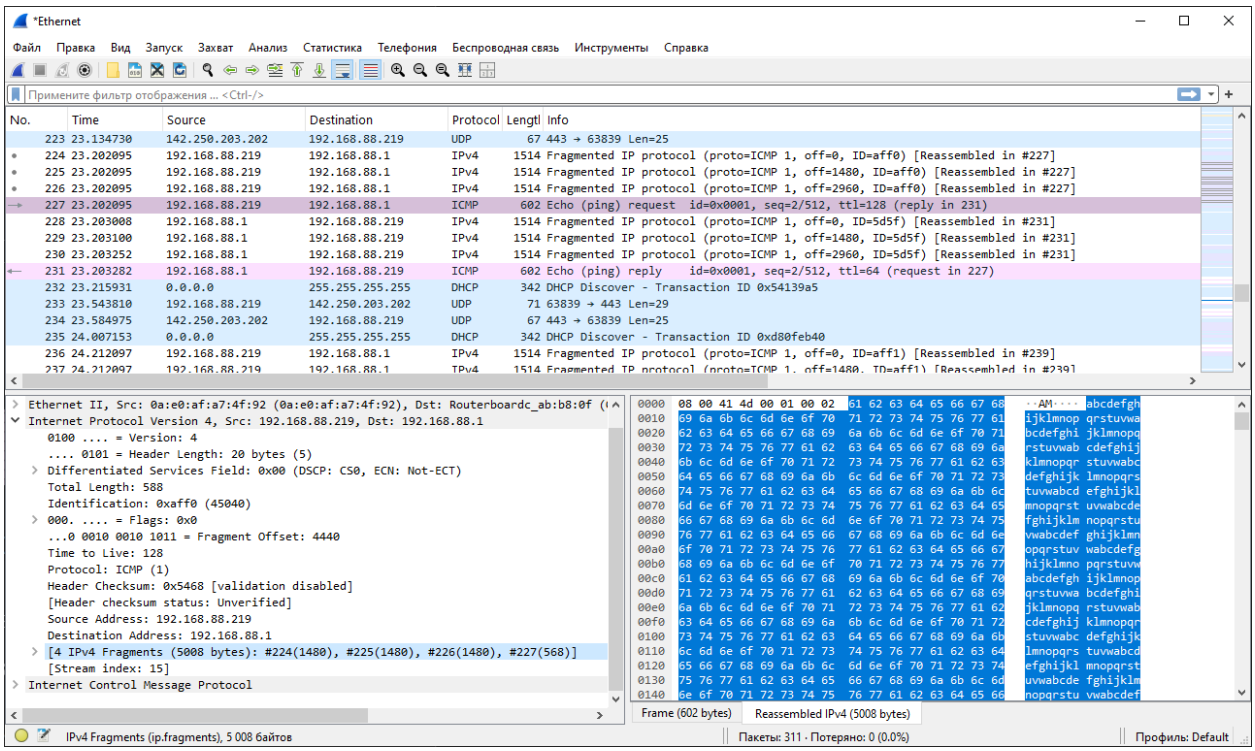

Рис. 3 – Захоплення у Wireshark, виділений перший ping

Як можна побачити на рис. 3 виклик був поділений на фрагменти, сам ping виклик відправляє англійську абетку.

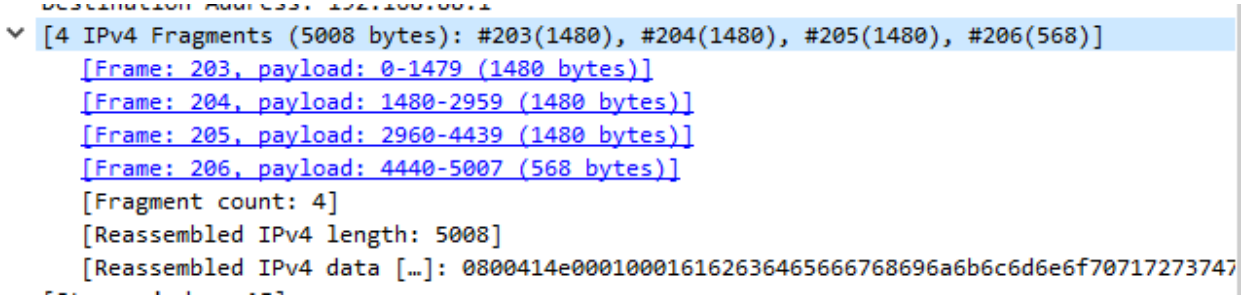

Рис. 4 – Розкрита вкладка фрагментів у Wireshark

Всього було поділено на 4 фрагменти, 3 з яких максимального обсягу, а саме 1480 байтів, та 1 на 568 байтів, та разом зібрано було 5008 байтів, що й зображено на рис. 4.

Висновки

В результаті виконання лабораторної роботи було досліджено процес просування IP-пакетів через об'єднану мережу з використанням аналізатора трафіку Wireshark. Основні аспекти, які вдалося засвоїти:

1. Фрагментація IP-дейтаграм є невід'ємною частиною передачі даних у мережах з різним розміром MTU. В ході експерименту було показано, що при перевищенні розміру MTU відбувається поділ IP-дейтаграми на менші фрагменти, які надсилаються окремо.
2. Аналіз фрагментів у Wireshark продемонстрував, що при передачі великих пакетів даних відбувається їх розбивка на фрагменти, які потім збираються на кінцевому вузлі. Було проаналізовано структуру фрагментованих пакетів і визначено, що кожен фрагмент має свій заголовок, який допомагає кінцевому вузлу зібрати оригінальний пакет.
3. Визначення значення MTU за допомогою командного рядка та аналізатору Wireshark дозволило зрозуміти, як мережевий інтерфейс обмежує розмір переданих даних. Було виявлено, що стандартний розмір MTU для Ethernet складає 1500 байт, а для передачі більших пакетів відбувається фрагментація.
4. Протокол ARP відіграє важливу роль у визначенні MAC-адрес для передачі даних на фізичному рівні. Було показано, як ARP визначає MAC-адреси на основі IP-адрес.

Загалом, лабораторна робота дозволила глибше зрозуміти роботу мережевих інтерфейсів, фрагментацію IP-дейтаграм і їхній аналіз за допомогою Wireshark. Отримані знання можуть бути використані для більш глибокого розуміння функціонування мережевих протоколів і усунення можливих проблем у роботі мереж.