# МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Національний університет “Львівська політехніка”**



**Інститут післядипломної освіти**

**ЗВІТ**

**Про виконання лабораторної роботи №2**

**«Дослідження роботи протоколів ІР та ІСМР»**

**з дисципліни «Організація комп'ютерних мереж»**

Виконав:

слухач групи ПЗС-11

Гринчук Тарас

Прийняв:

ст. викл. Тушницький Р.Б.

« »\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 р.

∑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

ЛЬВІВ – 2014

**Тема роботи**: Дослідження роботи протоколів ІР та ІСМР.

## 1. Теоретичні відомості

Протокол IP знаходиться на міжмережевому рівні стеку протоколів TCP / IP. Функції протоколу IP визначені в стандарті RFC - 791 наступним чином: "Протокол IP забезпечує передачу блоків даних , званих дейтаграмами, від відправника до одержувачів, де відправники й одержувачі є комп'ютерами, ідентифікованими адресами фіксованої довжини (IP- адресами ) . Протокол IP забезпечує при необхідності також фрагментацію і збірку дейтаграм для передачі даних через мережі з малим розміром пакетів" .

Протокол IP є ненадійним протоколом без встановлення з'єднання. Це означає , що протокол IP не підтверджує доставку даних , не контролює цілісність отриманих даних і не виробляє операцію квитування ( handshaking ) - обміну службовими повідомленнями , що підтверджують установку з'єднання з вузлом призначення та його готовність до прийому даних. Протокол IP обробляє кожну дейтаграму як незалежну одиницю , яка не має зв'язку ні з якими іншими дейтаграмами в Інтернет. Після того , як дейтаграма відправляється в мережу , її подальша доля ніяк не контролюється відправником ( на рівні протоколу IP). Якщо дейтаграма не може бути доставлена ​​, вона знищується. Вузол , що знищив дейтаграму, може відравити за зворотньою адресою ICMP- повідомлення про причину збою.

Гарантію правильної передачі даних надають протоколи вищого рівня (наприклад, протокол TCP), які мають для цього необхідні механізми.

Одне з основних завдань, що вирішуються протоколом IP - маршрутизація дейтаграм , тобто визначення шляху проходження дейтаграми від одного вузла мережі до іншого на основі адреси одержувача.

Загальний сценарій роботи модуля IP на якому-небудь вузлі мережі, що приймає дейтаграму з мережі, такий:

* з одного з інтерфейсів рівня доступу до середовища передачі ( наприклад , з Ethernet- інтерфейсу ) в модуль IP надходить дейтаграма;
* модуль IP аналізує заголовок дейтаграми;
* якщо пунктом призначення дейтаграми є даний комп'ютер:
  + якщо дейтаграмма є фрагментом більшої дейтаграми, очікуються інші фрагменти, після чого з них збирається вихідна велика дейтаграма;
  + з дейтаграми витягуються дані і спрямовуються на обробку одного з протоколів вищого рівня (якому саме - вказується в заголовку дейтаграми);
* якщо дейтаграма не спрямована ні на один з IP- адрес даного вузла, то подальші дії залежать від того, дозволена або заборонена ретрансляція (forwarding) "чужих" дейтаграм;
* якщо ретрансляція дозволена, то визначаються наступний вузол мережі , на який повинна бути переправлена ​​дейтаграмма для доставки її за призначенням, і інтерфейс нижнього рівня , після чого дейтаграмма передається на нижній рівень цього інтерфейсу для відправки; при необхідності може бути проведена фрагментація дейтаграми;
* Якщо ж дейтаграмма хибна або з якихось причин не може бути доставлена​​, вона знищується; при цьому, як правило, відправнику дейтаграми відсилається ICMP- повідомлення про помилку.

При отриманні даних від вищестоящого рівня для відправки їх по мережі IP-модуль формує дейтаграму з цими даними, в заголовок якої заносяться адреси відправника і одержувача (також отримані від транспортного рівня) та інша інформація; після чого виконуються наступні кроки:

* якщо дейтаграма призначена цьому ж вузлу, з неї витягуються дані і спрямовуються на обробку одного з протоколів транспортного рівня (якому саме - вказується в заголовку дейтаграми ) ;
* якщо дейтаграма не спрямована ні на один з IP- адрес даного вузла , то визначаються наступний вузол мережі, на який повинна бути переправлена ​​дейтаграма для доставки її за призначенням , і інтерфейс нижнього рівня , після чого дейтаграма передається на нижній рівень цього інтерфейсу для відправки; при необхідності може бути проведена фрагментація дейтаграми;
* Якщо ж дейтаграма хибна або з якихось причин не може бути доставлена​​, вона знищується.

Тут і далі вузлом мережі називається комп'ютер, підключений до мережі і підтримує протокол IP. Вузол мережі може мати один і більше IP- інтерфейсів , підключених до однієї або різних мереж , кожен такий інтерфейс ідентифікується унікальним IP -адресою.

ICMP (англ. Internet Control Message Protocol — міжмережевий протокол керуючих повідомлень) — мережевий протокол, що входить в стек протоколів TCP/IP. В основному ICMP використовується для передачі повідомлень про помилки й інші виняткові ситуації, що виникли при передачі даних. Також на ICMP покладають деякі сервісні функції, зокрема на основі цього протоколу заснована дія таких загальновідомих утиліт як ping та traceroute.

Протокол ICMP описаний в RFC 792 (з доповненнями в RFC 950) і є стандартом Інтернету (входить в стандарт STD 5 разом з протоколом IP). Хоча формально ICMP використовує IP (ICMP пакети інкапсулюються в IP пакети), він є невід'ємною частиною IP й обов'язковий при реалізації стека TCP/IP. Поточна версія ICMP для IPv4 називається ICMPv4. В IPv6 існує аналогічний протокол ICMPv6.

Протокол ICMP не є протоколом, що орієнтованим на з'єднання(як наприклад TCP), тобто при втраті пакету ICMP не буде робити ніяких спроб по його відновленню. ICMP повідомлення (тип 12) генеруються при знаходженні помилок у заголовку IP пакета (за винятком самих ICMP пакетів, щоб не призвести до нескінченно зростаючого потоку ICMP повідомлень про ICMP повідомлення).

## 2. Хід роботи

1. За допомогою аналізатора протоколів дослідимо заголовок ІР пакетів та фрагментацію ІР пакетів при використанні утиліти ping, на прикладі ya.ru.

**ping** — службова комп'ютерна програма, призначена для перевірки з'єднань в мережах на основі TCP/IP.

Вона відправляє запити (англ. Echo-Request) протоколу ICMP зазначеному вузлу мережі й фіксує відповіді (англ. Echo-Reply). Час між відправленням запиту й одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати двосторонні затримки у маршруті й частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв.

Виконаємо команду Пуск/Выполнить. Наберемо ім’я команди: cmd. У Консолі виконаємо команду: ping ya.ru. Результат виконання зображено на рис. 2.1.

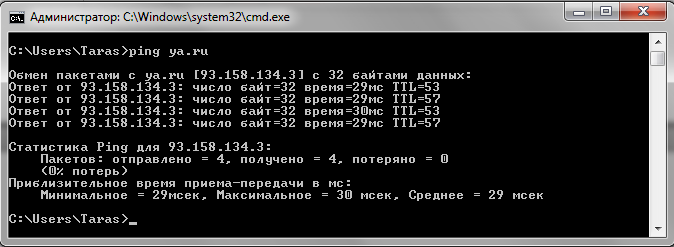


Рис. 2.1. ping ya.ru

**Traceroute** - це службова комп'ютерна програма, призначена для визначення маршрутів прямування даних в мережах TCP / IP. Traceroute може використовувати різні протоколи передачі даних в залежності від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп'ютери з встановленою операційною системою Windows використовують ICMP-протокол, при цьому операційні системи Linux і маршрутизатори Cisco - протокол UDP.

У Консолі виконаємо команду: tracert ya.ru. Результат виконання зображено на рис. 2.2.

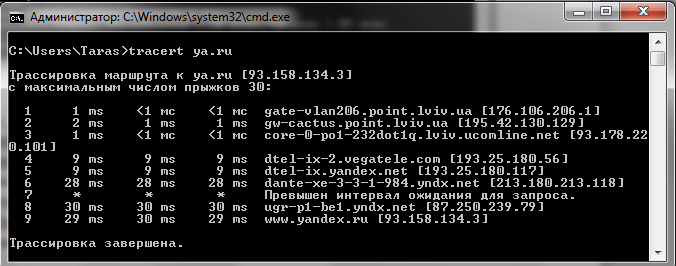


Рис. 2.2. tracert ya.ru

Вигляд заголовків ІР пакетів в аналізаторі протоколів Wireshark, при використанні утиліти ping зображено на рис. 2.3.

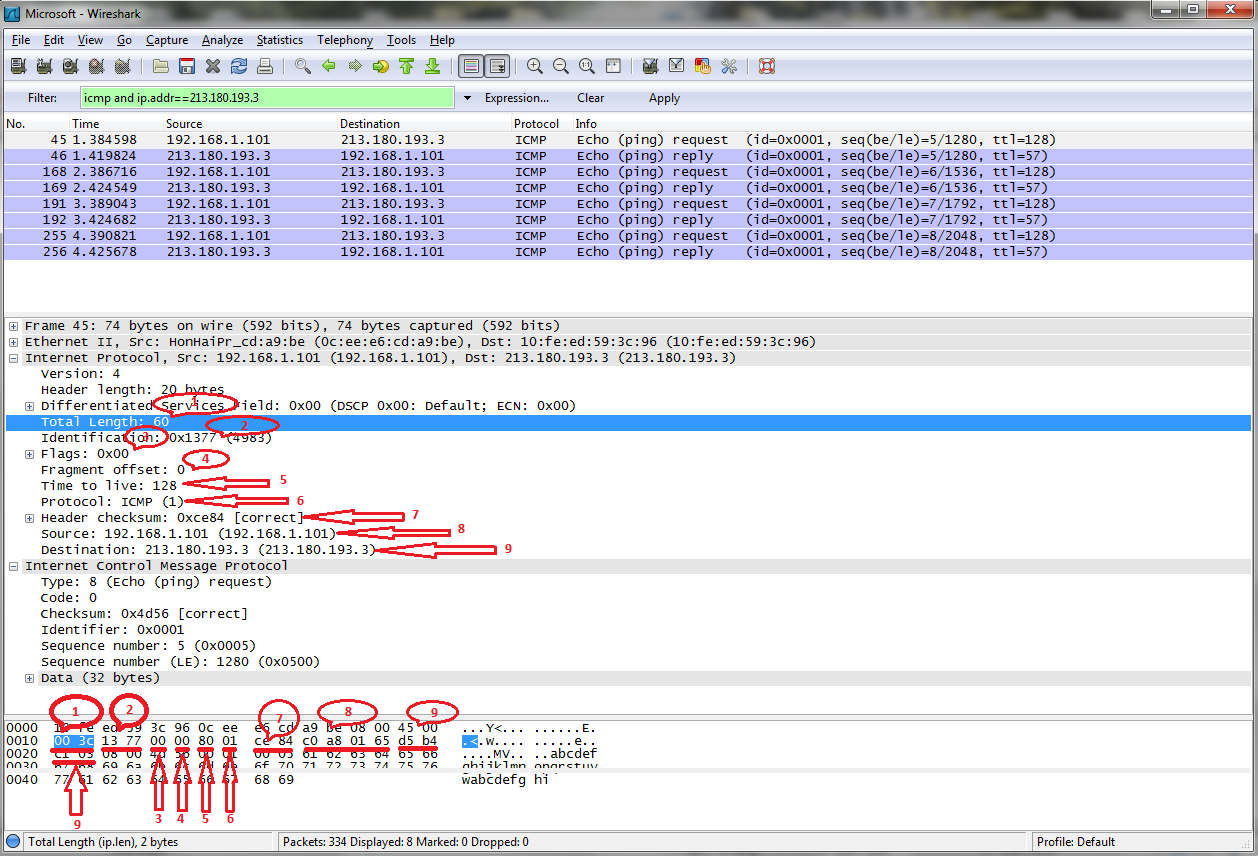


Рис. 2.3. Вигляд заголовків ІР пакетів в Wireshark

для ping ya.ru

1. Довжина пакета/Total Length — довжина пакета в октеках, включаючи заголовок та дані. Мінімальне коректне значення для цього поля рівне 20, максимальне - 65 535. Значення поля рівне 60.
2. Ідентификатор — значення, назначене відправником пакету і призначене для визначення коректної послідовності фрагментів при збірці пакету. Для фрагментованого пакету всі фрагменти мають одинаковий ідентификатор. Значення поля рівне 4983.
3. 3 біта прапорів. Перший біт завжди повинен бути рівний нулю, другий біт DF (don’t fragment) оприділяє можливість фрагментації пакету і третій біт MF (more fragments) показує, чи є цей пакет останнім у ланцюзі пакетів.

Значення полів рівне 0.

1. Зміщення фрагменту — значення, що оприділяє позицію фрагмента в потоці данних. Зміщення задається кількістю вісьмибайтових блоків, тому це значення потребує множення на 8 для переводу в байти. Значення поля рівне 0.
2. Час життя (TTL) — кількість маршрутизаторів, які може пройти даний пакет. При прохождені маршрутизатора це число зменшується на одиницю. Якщо значення цього поля рівне нулю то це пакет повинен бути відкинутий і відправнику пакету може бути відправлене повідомлення Time Exceeded (ICMP тип 11 код 0). Значення поля рівне 128.
3. протокол — ідентифікатор интернет-протокола наступного рівня показує, дані якого протокола містить пакет, наприклад, TCP чи ICMP. Значення поля рівне 01.
4. Контрольна сума заголовка — вираховується у відповідності з RFC 1071. Значення поля рівне 0xce84.
5. IP-адреса відправника — унікальний числовий номер мережевого рівня, відправника пакета Значення поля рівне 192.168.1.101.
6. IP-адреса отримувача - унікальний числовий номер мережевого рівня, отримувача пакета. Значення поля рівне 213.180.193.3.
7. За допомогою аналізатора протоколів Wireshark дослідимо заголовки та основні типи повідомлень ІСМР при використанні утиліт ping та tracert.

Утиліта **ping**, що служить для перевірки можливості доставки IP-пакетів, використовують ICMP-повідомлення і типом 8 (эхо-запит) и 0 (эхо-відповідь).

Утиліта **Traceroute**, що відображає шлях слідування IP-пакетів, використовують ICMP-повідомлення з типом 11.

Дослідження повідомлень ICMP-пакета, при використанні ping, echo request 8, зображено на рис. 2.4.

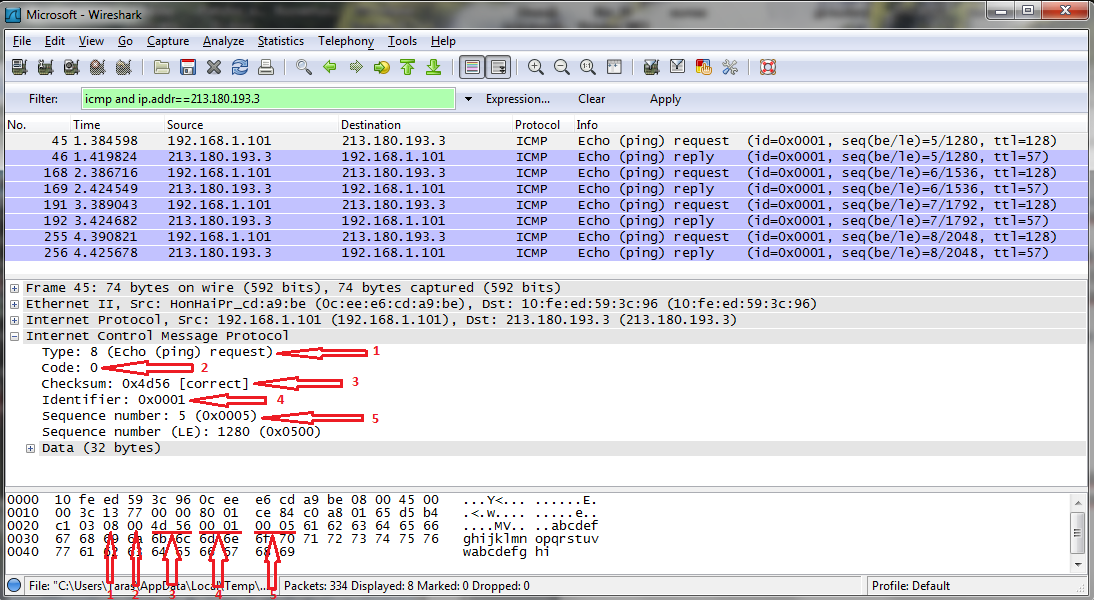


Рис. 2.4. ping ya.ru, echo request 8

1. Тип / Type — Байт що оприділяє тип пакета. Значення поля рівне 8.
2. Код / Code — Байт що оприділяє код операції. Значення поля рівне 0.
3. Контрольна сума заголовка/ Checksum — вираховується у відповідності з RFC 1071. Значення поля рівне 0x4d56.
4. Ідентифікатор / Identifier. Значення поля рівне 0x0001.
5. Послідовність / Sequence number. Значення поля рівне 0x0005.

Дослідження повідомлень ICMP-пакета, при використанні ping, echo replay 0, зображено на рис. 2.5.

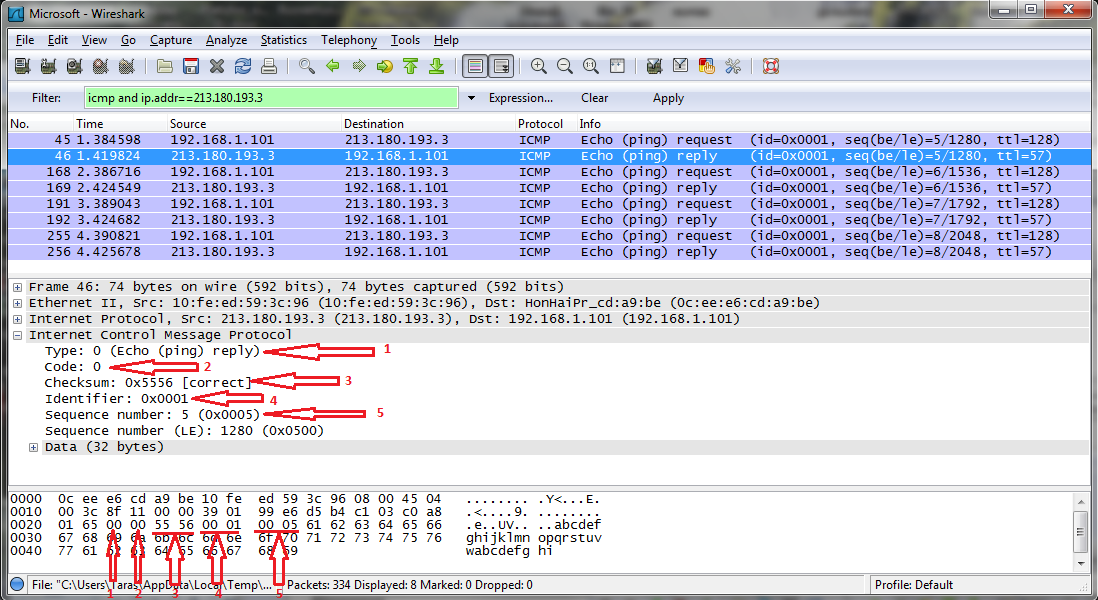


Рис. 2.5. ping ya.ru, echo replay 0

1. Тип / Type — Байт що оприділяє тип пакета. Значення поля рівне 0.
2. Код / Code — Байт що оприділяє код операції. Значення поля рівне 0.
3. Контрольна сума заголовка/ Checksum — вираховується у відповідності з RFC 1071. Значення поля рівне 0x5556.
4. Ідентифікатор / Identifier. Значення поля рівне 0x0001.
5. Послідовність / Sequence number. Значення поля рівне 0x0005.

Дослідження повідомлень ICMP-пакета, при використанні tracert, time-to-live ecceeded 11, зображено на рис. 2.6.

1. Тип / Type — Байт що оприділяє тип пакета. Значення поля рівне 11.
2. Код / Code — Байт що оприділяє код операції. Значення поля рівне 0.
3. Контрольна сума заголовка/ Checksum — вираховується у відповідності з RFC 1071. Значення поля рівне 0xf4ff.

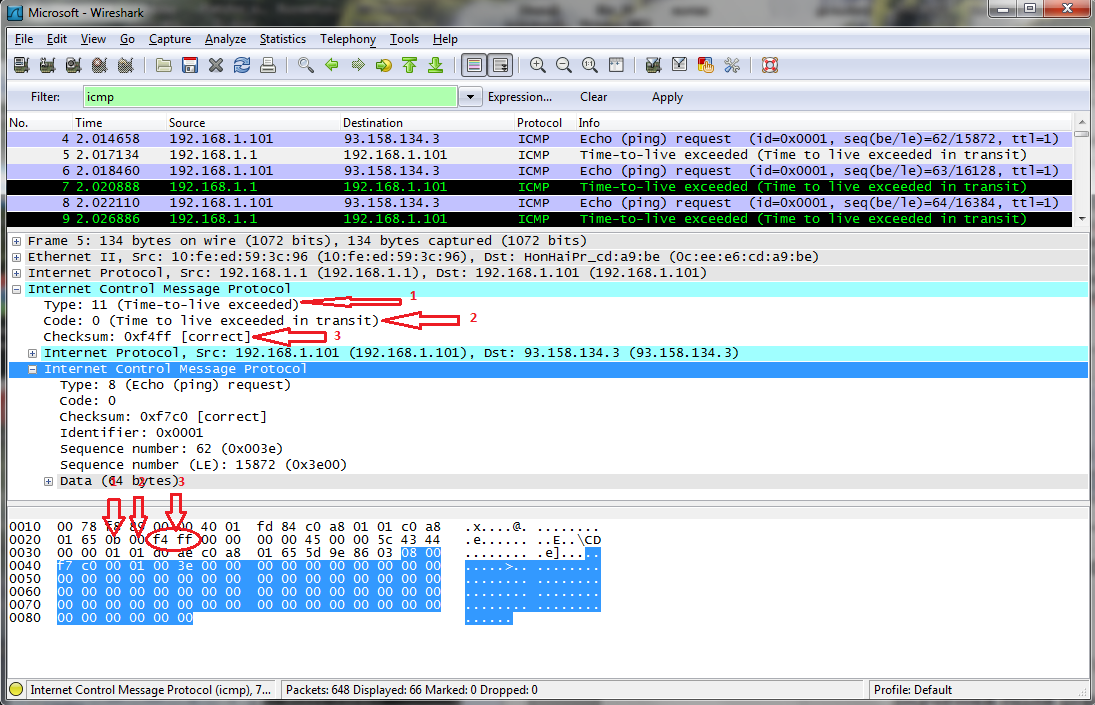


Рис. 2.6. tracert ya.ru, time-to-live ecceeded 11

## ВИСНОВКИ

На даній лабораторній роботі я дослідив роботу протоколів IP та ICMP, дізнався про роботу улитіт ping та tracert. З допомогою з програми wireshark перехопив та відфільтрував потік даних що містив запити по протоколу ICMP, та дослідив структуру заголовків пакетів IP та ICMP.