**Тема**: Дослідження роботи протоколів IP та ICMP.

**Мета**: Ознайомитися з принципами роботи та призначенням протоколів IP та ICMP та за допомогою утиліт ping, tracert та аналізатора протоколів Wireshark ознайомитися зі структурою пакетів цих протоколів.

# 1. Теоретичні відомості

## 1.1. Короткі відомості про TCP/IP

Комп'ютери в мережі обмінюються даними за заздалегідь погодженим стандартом. Такий стандарт в термінах мереж називають *протоколом*. Найбільш розробленими, популярними і реалізованими у всіх операційних системах є протоколи **TCP/IP**.

TCP/IP (Transmission Control Protocol / Internet Protocol – Протокол управління передачею / Протокол Internet ) – це *набір протоколів*, який дозволяє "безшовний" обмін даними між комп'ютерами, незалежно від того, якого типу є ці комп'ютери, яким підмережам вони належать і під якими операційними системами вони функціонують. Слово "безшовний" означає, що вся реалізація передачі даних прихована від користувача і створюється відчуття єдиної мережі. За TCP/IP передається більша частина трафіку у крупних мережах. Саме на TCP/IP тримається Internet. *Набір* (*комплект*, *стек*) протоколів означає, що в сімейство TCP/IP входять *різні* протоколи, основними з яких є TCP і IP. Термін "*стек*", мабуть, є найбільш правильним, оскільки TCP/IP охоплює протоколи *різних рівнів*. При цьому чітко регламентована роль кожного протоколу в цьому сімействі. Дані, якими обмінюються два комп'ютери, *«курсують вгору-вниз»* по стеку TCP/IP у кожному з комп'ютерів. А саме, у комп'ютері-передавачі дані з прикладного (найвищого) рівня (згадайте модель OSI) передаються через ряд модулів TCP/IP, і у кожному з них "обростають" службовою інформацією визначеного формату. Таким чином, після проходження всіх вищих рівнів дані, що підлягають передачі, потрапляють на канальний рівень (рівень ланки даних, що забезпечується мережними інтерфейсними платами) вже "обгорнутими" належним чином і готовими для "мандрів"

по фізичному середовищу, який є найнижчим рівнем в архітектурі мережі. На комп'ютері-одержувачі відбувається зворотний процес – дані поетапно "розпаковуються", проходячи ті ж модулі TCP/IP, але в зворотному порядку, аж поки з них не буде вичитана власне корисна інформація.

До сімейства TCP/IP належать протоколи: ARP, RARP, FTP, ICMP, IGMP, IP, TCP, SMTP, UDP.

TCP є протоколом, що забезпечує *надійну* передачу потоку даних між прикладними програмами, запущеними на різних комп'ютерах у мережі. Для цього потік даних ділиться на *TCP-сегменти* на комп'ютері-відправнику, а на комп'ютері-одержувачі відбувається повторна збірка TCP-сегментів. TCP-сегменти складаються з заголовків TCP і даних. *Надійність* протоколу TCP полягає у тому, що він використовує *контрольні суми* для перевірки цілісності даних і *підтвердження про доставку даних*. Користувацький інтерфейс з TCP може виконувати такі команди як відкрити (OPEN) чи закрити (CLOSE) з'єднання, відправити (SEND) чи прийняти (RECEIVE) дані або одержати статус з'єднання (STATUS). *Саме ж транспортування даних TCP "доручає" IP-протоколу*.

### 1.2. IP-протокол

IP-протокол – базовий протокол мережевого рівня, який забезпечує маршрутизацію та перенос даних від відправника до одержувача. Дані *передаються у формі IP-пакетів* (інша назва – IP-дейтаграми). *Маршрутизація* – це вибір маршруту передачі IP-пакетів в мережі.

Для розуміння роботи IP –протоколу слід ознайомитися зі структурою IP-пакета, яка представлена нижче (рис. 1).

<table>
<tr><td rowspan="2">Номер версії (4 біти)</td><td rowspan="2">Довжина заголовка (4 біти)</td><td colspan="8">Тип сервісу (8 біт)</td><td colspan="3" rowspan="2">Загальна довжина (16 біт)</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td colspan="2"></td><td colspan="3">PR</td><td>D</td><td>T</td><td>R</td><td>C</td><td></td></tr>
<tr><td colspan="8" rowspan="2">Ідентифікатор (16 біт)</td><td colspan="2">Flags (3 біти)</td><td rowspan="2">Зміщення фрагмента (13 біт)</td></tr>
<tr><td></td><td>DF</td><td>MF</td></tr>
<tr><td colspan="3">TTL (8 біт)</td><td colspan="5">Протокол верхнього рівня (8 біт)</td><td colspan="3">Контрольна сума (16 біт)</td></tr>
<tr><td colspan="11">IP-адреса відправника (32 біти)</td></tr>
<tr><td colspan="11">IP-адреса одержувача (32 біти)</td></tr>
<tr><td colspan="11">IP-опції та вирівнювання</td></tr>
<tr><td colspan="11">Дані...</td></tr>
</table>

Рис. 1 Формат IP-пакета

IP-пакет містить заголовок та поля даних. Типова довжина заголовка становить 20 байт. Опис полів поданий нижче.

Поле ***Номер версії*** (***Version***) містить версію протоколу IP. Зараз актуальна версія IPv4, однак, готується  перехід на версію IPv6.

Поле ***Довжина заголовка*** (*IHL*) має типове значення 20 байт, але може бути збільшена (при зростанні обсягу службової інформації) до 60 октетів за рахунок використання додаткових байтів у полі IP-опції.

Поле ***Тип сервісу*** (***Type of Service***, ***ToS***) вказує, як слід обробляти IP-пакет. Це поле містить 6 субполів: PR, D, T, R, C і один біт, що не використовується. Субполе ***PR*** (***Priority*** – приоритет) займає 3 біти, якими кодується пріоритет IP-пакета. Усього є 8 значень пріоритету (0 – найнижчий, 7 – найвищий):

0 – нормальний рівень;

1 – пріоритетний

2 – негайний

3 – терміновий

4 – екстрений

5 – ceitic/ecp

6 – міжмережеве управління

7 – мережеве управління

Біти ***D***, ***T***, ***R***, ***C*** характеризують побажання відносно способу доставки IP-пакета. При D = 1 вимагається мінімальна затримка, при T = 1 – висока пропускна здатність, при R = 1 – висока надійність, а при C = 1 – низька вартість. Інтернет не гарантує таку доставку пакетів, що визначена в полі ToS, однак, більшість маршрутизаторів враховують зазначені побажання при виборі маршруту. При цьому є зміст встановлювати лише один з цих чотирьох бітів, оскільки покращення одного з параметрів тягне погіршання іншого. За замовчанням біти D, T, R, C не встановлені (рівні 0).

Поле ***Загальна довжина*** (***Total Length***) визначає загальну довжину пакета (заголовок та поля даних в сумі). Максимально можлива загальна довжина IP-пакета становить 65535 байт. Однак, реально такі крупні пакети на практиці не використовуються через обмеження, продиктовані рівнем мережі, що лежить нижче за мережевий рівень, на якому функціонує IP-протокол. При передачі даних через мережі різного типу довжина IP-пакета вибирається з урахуванням максимальної довжини пакета протоколу нижнього рівня, за рахунок якого переносяться IP-пакети. Наприклад, нехай дані передаються через мережу Ethernet, тобто, IP-пакет має бути вкладений у поле даних кадру Ehertnet. Тоді, щоб IP-пакет міг поміститися в поле даних Ethernet-кадру, його довжина не повинна перевищувати 1500 байт.

Поле ***Ідентифікатор пакета*** (***Identification***) – важливе поле, що використовується для правильної збірки пакетів, утворених в результаті фрагментації вихідного пакета. Усі пакети, одержані шляхом фрагментації, повинні мати однакове значення поля Identification.

Поле ***Прапорці*** (***Flags***) об’єднує три прапорці, перший з яких зарезервований і повинен бути рівний 0, а два інші (***DF*** і ***MF***) містять вказівки маршрутизатору щодо фрагментації. Встановлений біт ***DF*** (***Do not Fragment***) забороняє маршрутизатору піддавати фрагментації цей IP-пакет. Відповідно, якщо без фрагментації неможливо обійтися, то такий пакет просто не буде доставлений. Встановлений біт ***MF*** (***More***

***Fragments***) вказує на те, що даний пакет є проміжним (тобто, не останнім) фрагментом. Якщо ж MF = 0, то або пакет нефрагментований, або це останній серед фрагментованих пакетів.

Поле ***Зміщення фрагмента*** (***Fragment Offset***) використовується при фрагментації пакетів та їхній подальшій збірці; воно задає зміщення (у байтах) поля даних цього IP-пакета від початку спільного поля даних вихідного пакету, що був підданий фрагментації. Зміщення першого фрагмента завжди рівне 0.

Поле ***Час життя*** (***Time to Live, TTL***) задає максимальний термін (в секундах), протягом якого IP-пакет може переміщатися в мережі. Цей час задається відправником пакета і зменшується на 1 при проходженні кожного маршрутизатора чи будь-якого іншого вузла в мережі (навіть якщо пакет реально обробляється там менше 1 секунди). Фактично, можна вважати, що TTL – це максимальна кількість вузлів, яку пакету дозволено пройти у мережі. Якщо TTL стане рівним 0 до того, як пакет дійде до одержувача, цей пакет буде знищений. TTL допомагає запобігти зациклюванню пакетів. При перерахунку TTL має перераховуватися також контрольна сума.

Поле ***Протокол верхнього рівня*** (***Protocol***) вказує, якому протоколу верхнього рівня належить інформація, розміщена у полі даних пакета. Значенням цього поля є код, заздалегідь визначений документом RFC “Assigned Numbers”. Наприклад, кодом для TCP є 6, а UDP має код 17.

Поле ***Контрольна сума*** (***Header Checksum***) розраховується тільки за полями заголовка (але не полями даних) і перевіряється та перераховується щоразу, як в процесі передачі пакета IP-заголовок проходить процесс обробки. Контрольна сума обчислюється як доповнення до сумі усіх 16-бітових слів заголовка. При обчисленні контрольної суми значення поля Header Checksum встановлюється в нуль. Пакет з неправильною контрольною сумою відкидається.

Поле ***IP-опції*** є необов’язковим і використовується переважно при відлагодженні мережі. Поле складається з декількох субполів, кожне з яких може бути одного з 8 наперед визначених типів. В залежності від того, які саме опції застосовуються, розмір поля IP-опції може бути різним. Якщо використовуються декілька опцій, вони

записуються підряд без будь-яких роздільників. Якщо місце, зайняте опціями, не є кратним 4 октетам, то в кінці поля IP-опції додається декілька байт для вирівнювання заголовка пакета до 32-бітної границі.

Поле ***Вирівнювання*** (***Padding***) застосовується при потребі доповнення IP-заголовка до 32-бітної границі (вирівнювання здійснюється нулями).

### 1.2.1 Фрагментація IP-пакетів

IP-протокол забезпечує перенос IP-пакетів від відправника до одержувача. Однак, можливо, що на шляху від відправника до одержувача дані повинні пройти через *ряд підмереж різного типу*. Мережі різного типу характеризуються рядом відмінностей, серед яких фігурує таке поняття, як ***максимальна одиниця транспортування*** (***Maximum Transfer Unit, MTU***) – максимальний розмір поля даних пакета. Наприклад, для мережі Ethernet MTU становить 1500 байт, а для мережі FDDI – 4096 байт. У функції IP-протоколу входить розбиття IP-пакетів на коротші IP-пакети, розміри яких не перевищують допустимі для даної підмережі. Таке розбиття називається ***фрагментацією***.

Для фрагментації використовуються поля вже розглянуті поля IP-пакета ***Ідентифікатор*** (***Identification***), ***Прапорці*** (***Flags***) та ***Зміщення фрагмента*** (***Fragment Offset***). Як вже було сказано, поле ***Ідентифікатор*** повинно бути однаковим для всіх фрагментованих пакетів, оскільки саме за цим значенням власне розпізнається, що IP-пакети є складовими частинами іншого IP-пакета, що був підданий фрагментації. Поле ***Зміщення фрагмента***, фактично, вказує, в якому порядку слід «поскладати» фрагментовані пакети, щоб відтворити оригінальний IP-пакет. Зокрема, завдяки полю ***Зміщення фрагмента*** можливо правильно зібрати оригінальний IP-пакет і тоді, коли фрагментовані пакети приходять по мережі в довільному порядку. Зрештою, прапорець ***MF*** вказує, чи є даний IP-пакет останнім серед ряду пакетів-фрагментів вихідного IP-пакета.

Слід зазначити, що маршрутизатори ***не*** збирають пакети в більш крупні, навіть якщо збираються відправити ці пакети в мережу, яка дозволяє таке укрупнення. Річ у тім,

що окремі фрагменти повідомлення можуть переміщатися по мережі різними маршрутами, а тому немає гарантії, що всі фрагменти проходять саме через даний маршрутизатор.

### 1.3. Протокол ICMP

***ICMP*** (*Internet Control Message Protocol* – протокол обміну керуючими повідомленнями) – це протокол повідомлення про помилки, тобто, протокол, що дозволяє маршрутизатору повідомити кінцевому вузлу про помилки, з якими маршрутизатор зіткнувся при передачі якогось IP-пакета від даного кінцевого вузла. ICMP не призначений для виправлення помилок, хоча результати його роботи можуть бути використані кінцевим вузлом для усунення помилок.

Керуючі повідомлення ICMP не відправляються проміжному маршрутизатору, що брав участь в передачі «проблемного» IP-пакета, адже IP-пакет несе лише адресу відправника та адресу одержувача, однак у нього не записуються адреси проміжних маршрутизаторів.

Кожне повідомлення протоколу ICMP передається по мережі всередині IP-пакета. Оскільки, як вже говорилося, протокол IP не дає гарантії доставки, то і повідомлення ICMP теж можуть втрачатися.

Для уникнення лавини ICMP-пакетів виконуються наступні правила:

1. При втраті IP-пакета ніколи не генерується новий.
2. ICMP-пакети ніколи не генеруються у відповідь на IP-пакети з широкомовною або груповою адресою
3. При пошкодженні фрагментованого IP-пакета ICMP-повідомлення відправляється лише після одержання першого пошкодженого фрагмента, оскільки відправник все одно надішле повторно весь IP-пакет, що підлягав фрагментації.

Повідомлення ICMP бувають декількох типів. В залежності від типу, повідомлення можуть мати різний формат, однак перші три поля (***Тип повідомлення***, ***Код*** та

***Контрольна сума***) для всіх повідомлень ICMP є однотипні. В найбільш загальному вигляді ICMP-пакет має формат, представлений на рис. 2.


Рис. 2 Структура ICMP-пакета

### 1.4. Утиліта ping

Утиліта ping призначена для перевірки з'єднань у мережах, побудованих на основі TCP/IP і постачається разом з усіма мережевими операційними системами (крім того, функціональність ping реалізована в частині маршрутизаторів). Слово "ping" має і декілька інших значень, зокрема, так називають і сам запит.

Утиліта надсилає запити протоколу ICMP (ICMP Echo-Request) вказаному вузлу мережі та фіксує відповіді (ICMP Echo-Reply). Час між відправленням запиту та одержанням відповіді (Round Trip Time, RRT) дозволяє визначити двосторонні затримки в маршруті і, таким чином, є непрямою характеристикою завантаженості каналів передачі даних. Крім того, за утилітою ping визначають частоту втрати пакетів.

З результатів, які видає утиліта ping, випливає, що її можна використовувати для того, щоб:

- дізнатися IP-адресу за доменним іменем;
- дізнатися, чи є зв'язок з сервером та чи працює сервер.

Команда ping має ряд параметрів, що записуються в наступному форматі:

**ping [-t] [-a] [-n число] [-l число] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j список_вузлів | [-k список_вузлів]] [-w таймаут] Кінцеве_Ім'я**

Параметри описані у таблиці 1.

*Таблиця 1. Параметри команди ping*

| | |
|---|---|
| -t | Відправлення пакетів на вказаний вузол до команди переривання. Для виводу статистики слід натиснути Ctrl+Break, для припинення – Ctrl+C |
| -a | Визначення адрес за іменами вузлів |
| -n число | Число запитів, що відправляється |
| -l розмір | Розмір буфера відправлення |
| -f | Встановлення прапорця DF |
| -i TTL | Час життя пакета в секундах (за замовчанням 2 секунди) |
| -v ToS | Поле Тип сервісу |
| -r число | Запис маршрутів для вказаного числа переходів |
| -s число | Штамп часу для вказаного числа переходів |
| -j списокВузлів | Вільний вибір маршруту за списком вузлів |
| -k списокВузлів | Жорсткий вибір маршруту за списком вузлів |
| -w таймаут | Тайм-аут кожної відповіді в мілісекундах |

Квадратні дужки у зазначеному форматі команди означає, що параметр може бути, а може не бути. Однак, має бути використано все, що вказано в квадратних дужках. Зокрема, якщо вказано –n, то через пробіл слід вказати і відповідне число (кількість запитів, що відправляється).

**Приклади**. Для перевірки з’єднання з вузлом www.google.com.ua запит показаний на рис. 3.

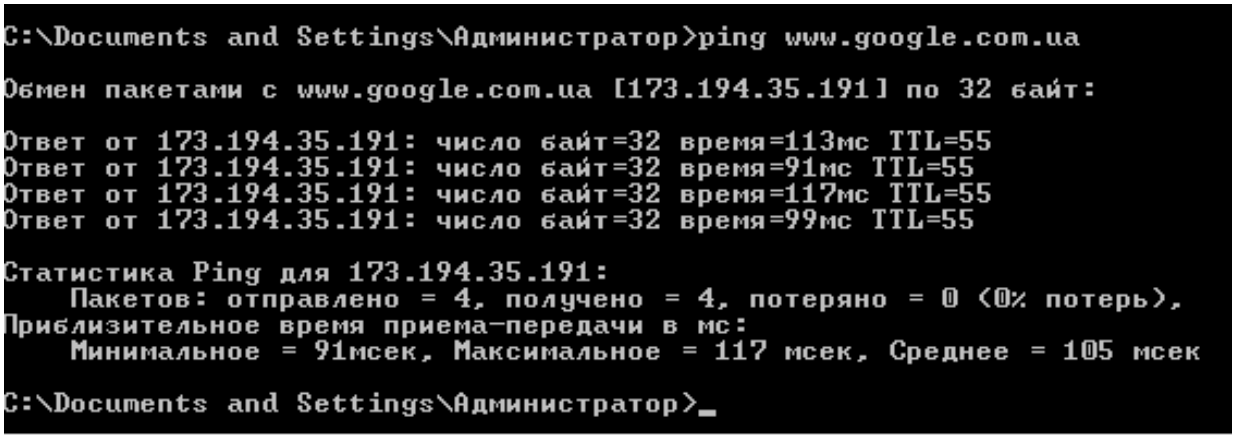


Рис. 3 Приклад команди ping

Нехай потрібно переслати 2 пакети вузлу www.google.com.ua. Відповідна команда:

**ping –n 2 www.google.com.ua**

Нехай потрібно вказати час життя 5 с (запит ICMP вважатиметься успішним, якщо ехо-відповідь буде одержана в межах зазначеного параметра TTL). Тоді команда виглядатиме так:

**ping –n 2 –i 5 www.google.com.ua**

### 1.5. Утиліта tracert

Утиліта tracert призначена для відстеження маршруту пакета. У випадках неодержання відповіді ця команда є більш інформативною, ніж ping, оскільки дозволяє визначити, в якій саме частині маршруту є проблеми зі зв’язком.

Формат команди tracert є наступним:

**tracert [-d] [-h максимальне число переходів] [-j список_вузлів] [-w число] IP-адреса або ім’я вузла-одержувача**

Параметри команди tracert описані в таблиці 2.

*Таблиця 2. Параметри команди tracert*

| | |
|---|---|
| -d | Запобігає встановленню командою tracert доменних імен проміжних маршрутизаторів за їхніми IP-адресами (і таким чином пришвидшує роботу tracert) |
| -h | Максимальне число переходів (від англ. hop – стрибок) до досягнення вузла-одержувача (за замовчанням 30). |
| -j список_вузлів | Вказує для повідомлень з Echo-Request використання вільної маршрутизації в заголовку IP з набором проміжних адресатів, вказаних у списку вузлів. При вільній маршрутизації успішні проміжні адресати можуть бути розділені одним чи декількома маршрутизаторами. Максимум у списку може бути 9 адрес (або імен). |
| -w інтервал | Час очікування відповіді (в мілісекундах) |
| ім'я_вузла_одержувача | IP-адреса або доменне ім’я |

Шлях пакета визначається з аналізу повідомлень ICMP про те, що час сплив. Ці повідомлення пересилаються від проміжних маршрутизаторів, однак деякі маршрутизатори не надсилають повідомлень для пакетів з TTL=0, і в цьому випадку для переходу відображаються символи «*».

**Приклад**.

Для відстеження маршруту пакета, відправленого вузлу www.google.com.ua виконуємо команду, яка (разом з результатом) показана на рис. 4.

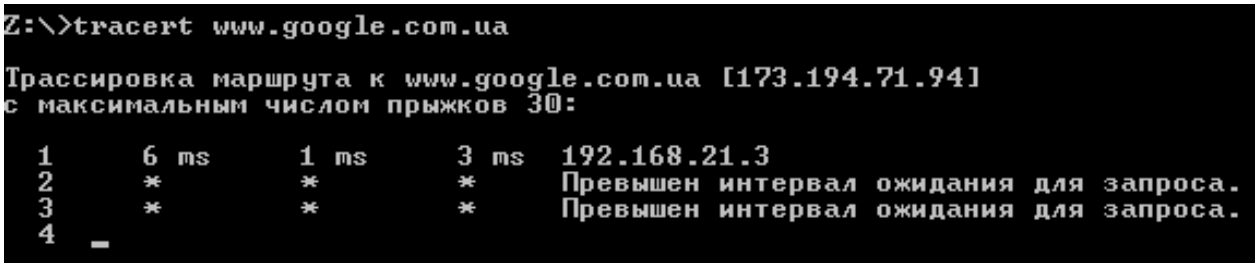


Рис. 4. Приклад команди tracert

З результатів видно, що пакет дійшов лише до одного вузла (ймовірно, це адреса основного шлюзу, для пересвідчення у чому слід скористатися командою ipconfig /all).

### 1.6. Засоби вивчення структури IP-пакетів і ICMP-повідомлень

Для дослідження пакетів ICMP та IP за допомогою утиліт ping і tracert та аналізатора протоколів Wireshark варто запустити пакет Wireshark, почати перехоплення пакетів, встановити фільтр протоколів (наприклад, лише icmp або icmp та ip) і з командного рядка (Start => Run = > у вікні задати cmd) задавати з відповідними параметрами команди ping tracert та стежити за змінами у таблиці перехоплених пакетів у Wireshark.

Наприклад, якщо командою ping відправлено 2 пакети вузлу ru.wikipedia.org (рис. 5), то у таблиці захоплених пакетів Wireshark появляються 2 записи (рис. 6).

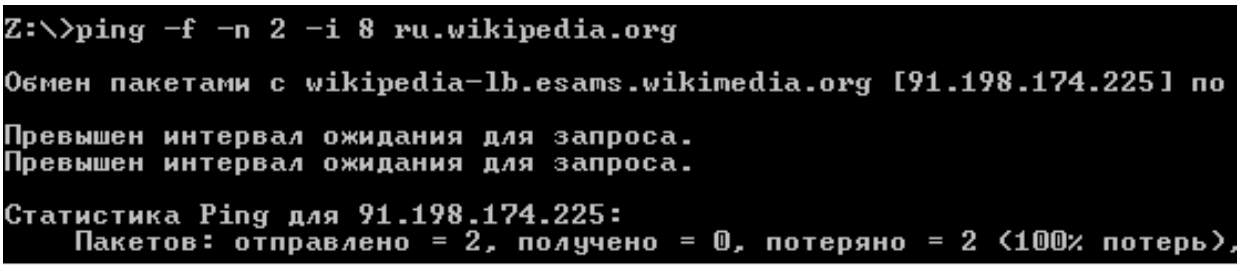


Рис. 5. Відправлення запиту ping

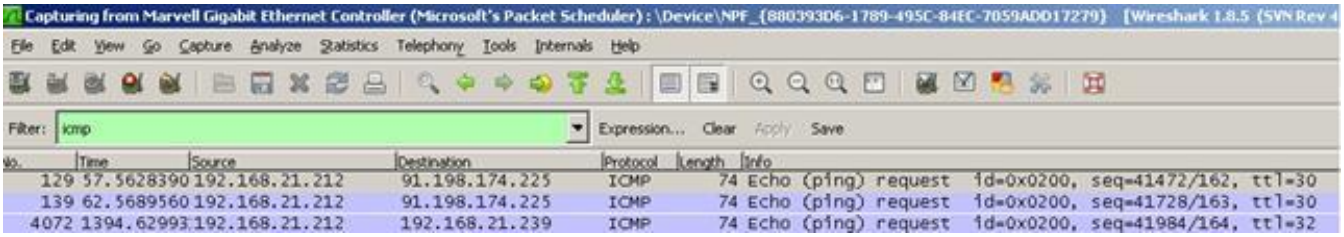


Рис. 6. Відстеження пакетів у Wireshark

Звісно, при зіставленні результатів команди ping і значення поля Destination у Wireshark IP-адреса одержувача буде та сама.

Щоб дізнатися деталі про пакет, слід виділити його – у вікні нижче відобразиться інформація про пакет (рис. 7). Нагадаємо, що IP-пакети «подорожують» в мережі у складі кадрів протоколів нижчого рівня (наприклад, Ethernet), а ICMP-повідомлення, у свою чергу, вкладаються в IP-пакети. Відповідно, для перехопленого пакета відображаються окремо пункти, що стосуються опису пакетів кожного з протоколів до ICMP. Для детального ознайомлення з IP-пакетом слід розкрити дерево Internet Protocol Version 4… (рис. 8), а ICMP-повідомлення – відповідний пункт (рис. 9).

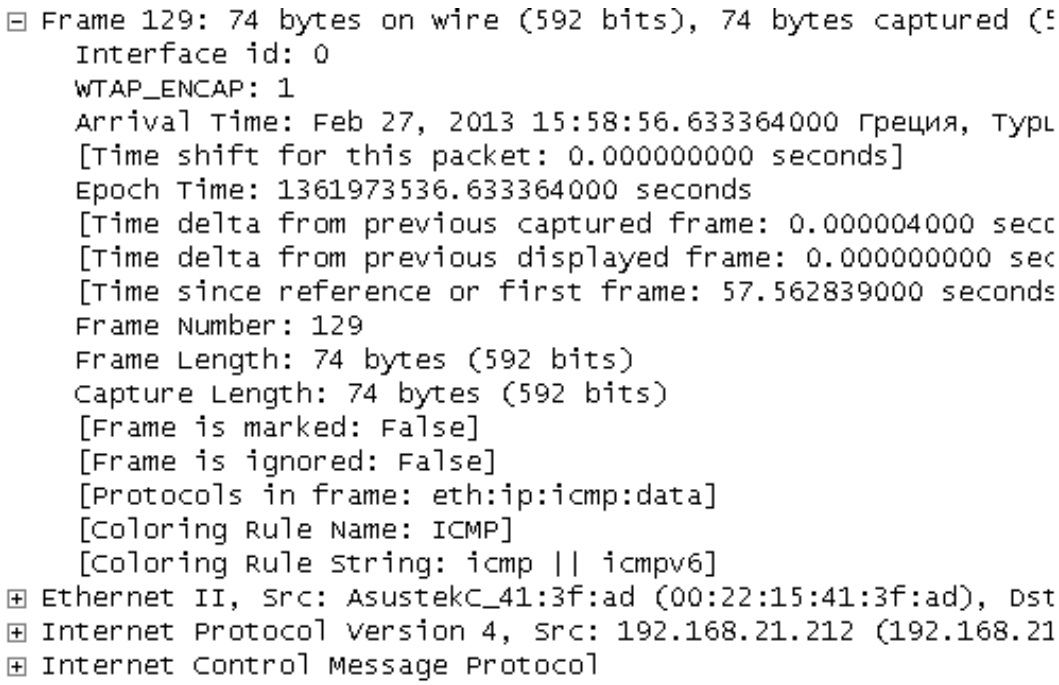


Рис. 7. Детальна інформація про перехоплені пакети

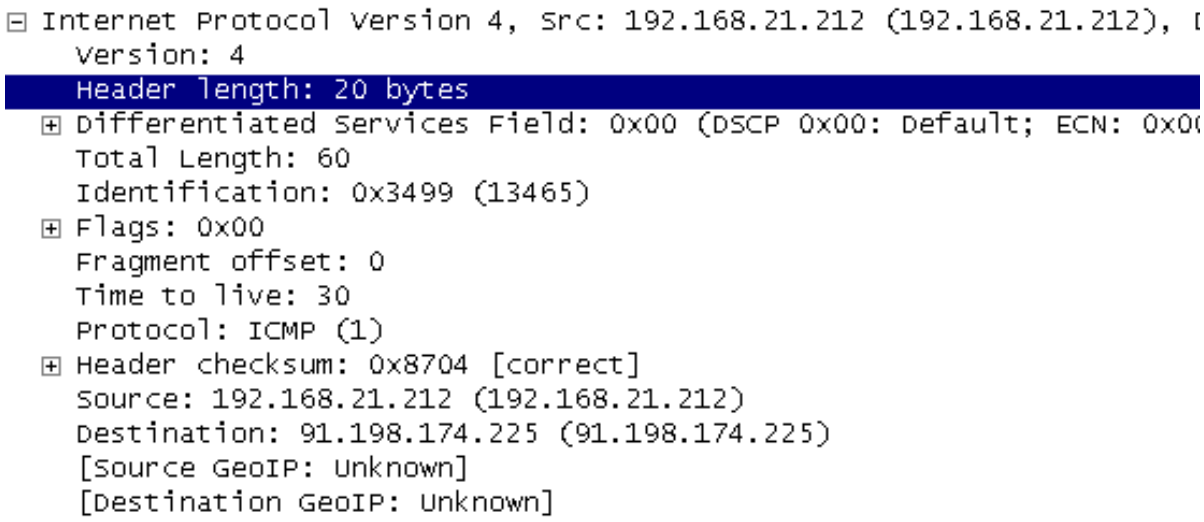


Рис. 8. Деталі IP-пакета

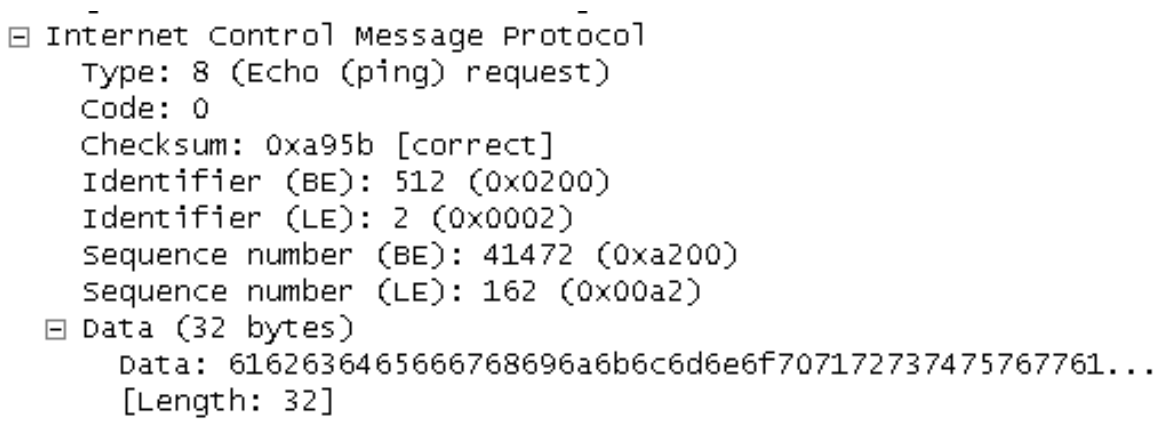


Рис. 9. Деталі ICMP-повідомлення

## Контрольні запитання

1. Чому TCP/IP називають стеком протоколів?
2. Опишіть структуру IP-пакета
3. Поясніть механізм фрагментації та вкажіть, які поля пакета використовуються для неї.
4. Як вказати маршрутизатору побажання стосовно доставки пакета?
5. Для чого потрібна фрагментація?
6. За рахунок чого TCP гарантує доставку?
7. Які параметри є в команди ping?
8. Які параметри має команда tracert?
9. Для чого призначений протокол ICMP?
10. Що трапляється з пакетом, для якого TTL = 0?

11. Які є правила генерування ICMP-повідомлень?
12. Чим продиктовані правила генерування ICMP-повідомлень?
13. Чи IP-протокол гарантує доставку?
14. Яка інформація міститься в полі Protocol IP-пакета?
15. Що означає MF=0?
16. Що означає DF=1?
17. Які поля завжди присутні у повідомленнях ICMP?
18. Яка максимальна довжина IP-пакета?
19. Для чого служить контрольна сума?
20. Що трапляється з пакетами, в яких контрольна сума неправильна?

**Хід роботи**

1. Ознайомтеся з теоретичними відомостями.
2. Випробуйте всі параметри команди ping (в яких комбінаціях перевіряти параметри – це залишається на розсуд виконавця). Почніть з мінімуму параметрів (тільки назва команди та доменне ім'я вузла-одержувача). Прочитайте інформацію про IP-пакети, перехоплені аналізатором протоколів Wireshark і переконайтеся в розумінні значень всіх полів IP-пакета. Для кожної випробуваної комбінації параметрів дослідіть структуру перехопленого IP-пакета. У звіті відобразіть екранні знімки всіх спроб виконати ping та вміст IP—пакетів, відповідних цим спробам. Якщо команда ping була неуспішною (не було відповіді на запит), з'ясуйте причину цього.
3. Аналогічним чином випробуйте параметри команди tracert і результати відобразіть у звіті.
4. Самостійно знайдіть детальну інформацію про всі типи ICMP-пакетів (підказка: документ RFC), дослідіть структуру перехоплених аналізатором протоколів пакетів і визначте тип кожного з досліджених пакетів.
5. Самостійно знайдіть відповідь на одне з наступних запитань (варіант запитання відповідає номеру студента в журналі) та представте цю відповідь у звіті:
    - Які операційні системи належать до мережевих?
    - Які протоколи належать до сімейства TCP/IP (отримайте найповніший список)?
    - Яким чином обчислюється контрольна сума? Наведіть приклади.
    - Якими документами RFC регламентуються протоколи TCP, IP, ICMP?
    - Виберіть з десяток протоколів сімейства TCP/IP та дізнайтеся, які коди у полі Protocol IP-пакета відповідають цим протоколам.
    - Яка інформація може міститися у полі IP-опції IP-пакета?
    - В якому форматі розміщається інформація в полі IP-опції IP-пакета?
    - Як записується маршрутна інформація в полі IP-опції IP-пакета?
    - Які пристрої можуть бути проміжними вузлами в мережі?
    - Що таке розширена команда ping?
    - Які ще діагностичні команди (крім ping і tracert) існують?
6. Сформуйте звіт зі структурою, аналогічною до звіту з лабораторної роботи №1. У теоретичних відомостях слід дати відповіді на 3 вибрані викладачем запитання з числа контрольних запитань. У висновку слід подати результати осмислення одержаних результатів, опис неуспішних спроб виконання команд ping і tracert та пояснення причин.