Навчально-методична література

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ
УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
КАФЕДРА КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ

МЕТОДИЧНІ ВКАЗІВКИ

для виконання лабораторних робіт
з дисципліни

КОМП'ЮТЕРНІ МЕРЕЖІ

(Модуль 1)

для студентів спеціальності
123 «Комп'ютерна інженерія»

Тернопіль
2023

Методичні вказівки для виконання лабораторних робіт з курсу «Комп’ютерні мережі». Модуль 1. Для студентів спеціальності 123 «Комп’ютерна інженерія» /укл. А. Г. Микитишин, О. С. Голотенко. // ТНТУ. – 2023. – 44 с.

Укладачі: Андрій МИКИТИШИН, канд. техн. наук, доц.
Олександр ГОЛОТЕНКО, канд. техн. наук, доц.

Рецензент: Сергій МАРЦЕНКО, канд. техн. наук, доц.

Відповідальний за випуск: Олександр ГОЛОТЕНКО, канд. техн. наук., доц.

Схвалено та рекомендовано до друку:

Протокол кафедри КТ №1 від 22.08.2023 р.

Протокол НМК факультету прикладних інформаційних технологій та електроінженерії №1 від 30.08.2023 р.

Методичні вказівки призначені для проведення лабораторних робіт з дисципліни «Комп'ютерні мережі» для студентів, які навчаються за спеціальністю 123 «Комп’ютерна інженерія». Викладені матеріали приведені з урахуванням модульної системи навчання, рекомендацій до самостійної роботи і індивідуальних завдань, тем лабораторних занять, тестів, екзаменаційних питань, типової форми та вимог для комплексної перевірки знань з дисципліни.

ЗМІСТ

Лабораторна робота №1.1

Дослідження мережевих стандартів

Мета роботи: Дослідження організацій з мережевих стандартів.

Зауваження

Використовуючи пошукові системи, такі як Google, дослідіть некомерційні організації, які відповідають за розробку та підтримку міжнародних стандартів для мережі Інтернеті та розвиток Інтернет-технологій.

Необхідні ресурси

ПК з доступом до мережі Інтернет

Інструкції

Крок 1: Дослідження організацій з мережних стандартів

На цьому кроці ви визначите основні організації з стандартизації та їх важливі характеристики, такі як час існування, кількість учасників, важливі історичні постаті, деякі обов'язки та зобов'язання, роль організаційного нагляду та місцезнаходження штаб-квартири організації.

Скористайтесь веб-сайтами різних організацій для дослідження інформації про такі організації та людей, що мали важливе значення для їх розвитку.

Ви можете знайти відповіді на запитання, наведені нижче, виконавши пошук таких скорочень назв організацій та термінів: ISO, ITU, ICANN, IANA, IEEE, EIA, TIA, ISOC, IAB, IETF, W3C, RFC, and Wi-Fi Alliance.

1. Хто такий Джонатан Б. Постель (Jonathan B. Postel) і чим він відомий?

2. Які дві пов'язані між собою організації відповідають за керування простором доменних імен верхнього рівня та кореневими серверами доменних імен (DNS) мережі Інтернет?

3. Вінтон Серф (Vinton Cerf) вважається одним із головних засновників інтернету. У якій інтернет-організації він головував або сприяв заснуванню? Які інтернет-технологій він допоміг розробити?

4. Яка організація відповідає за оприлюднення Request for Comments (RFC)?

5. Що спільного між RFC 349 і RFC 1700?

6. Які номери мають RFC ARPAWOCKY? Що це таке?

7. Хто заснував консорціум World Wide Web (W3C)?

8. Назвіть 10 стандартів World Wide Web (WWW), які розробляє і підтримує W3C?

9. Де знаходиться штаб-квартира Інституту інженерів з електротехніки та електроніки (IEEE) і що означає її логотип?

10. Яким є стандарт IEEE для протоколу безпеки Wi-Fi Protected Access 2 (WPA2)?

11. Чи є Wi-Fi альянс неприбутковою організацією зі стандартів? Яка мета її діяльності?

12. Хто такий Хамадун Туре (Hamadoun Touré)?

13. Що таке Міжнародний союз електрозв'язку - International Telecommunication Union (ITU) і де знаходиться його штаб-квартира?

14. Назвіть три сектори ITU.

15. Що означає RS у RS-232 і яка організація його запровадила?

16. Що таке SpaceWire?

17. У чому полягає місія ISOC і де знаходиться його штаб-квартира?

18. Які організації контролює IAB?

19. Яку організацію контролює ISOC?

20. Коли було засновано ISO і де розташована її штаб-квартира?

Крок 2: Аналіз досвіду Інтернету та комп'ютерних мереж

Поміркуйте про сучасний Інтернет по відношенню до організацій і технологій, які ви щойно дослідили.

Після цього дайте відповіді на такі запитання.

1. Як Інтернет-стандарти дозволяють розширити торгівлю? Які потенційні проблеми могли б виникнути, якби не було IEEE?

2. З якими потенційними проблемами ми могли б зіткнутися за відсутності W3C?

3. Що можна дізнатися на прикладі альянсу Wi-Fi щодо необхідності визначення мережних стандартів?

Лабораторна робота №1.2
Дослідження моделей TCP/IP і OSI

Цілі та задачі
Частина 1: Вивчення веб-трафіку HTTP
Частина 2: Відображення складових стеку протоколів TCP/IP

Довідкова інформація

Це завдання з моделювання покликане сформувати засади для розуміння стеку протоколів TCP/IP і його взаємозв'язку з моделлю OSI. Режим симуляції дозволяє переглядати вміст даних на кожному рівні в процесі надсилання мережею.

Під час передавання по мережі дані розбиваються на менші частини та ідентифікуються з метою повторного збирання при надходженні до пункту призначення. Кожному блоку, відповідно до певних рівнів моделей TCP/IP та OSI, призначена власна назва. Режим моделювання Packet Tracer дає можливість переглядати кожен рівень і пов'язані з ним PDU. Наступні кроки познайомлять користувача з процесом запиту веб-сторінки з веб-сервера за допомогою браузера на клієнтському ПК.

Не зважаючи на те, що більшість поданої інформації детально розглядатиметься пізніше, це завдання дає можливість вивчити функціональність Packet Tracer і відтворити процес інкапсуляції.

Інструкції
Частина 1: Дослідження веб-трафіку протоколу HTTP
У Частині 1 цього завдання Ви використаєте Режим моделювання (Simulation mode) Packet Tracer (PT) для створення веб-трафіку та вивчення HTTP.

Крок 1: Перехід з режиму реального часу (Realtime) до режиму моделювання (Simulation mode).

У нижньому правому куті інтерфейсу Packet Tracer розміщені кнопки перемикання між режимами **Realtime** і **Simulation**. PT завжди запускається у режимі **Realtime**, у якому мережні протоколи оперують у реальних часових проміжках. Проте, можливості Packet Tracer дозволяють користувачеві “зупинити час” за допомогою перемикання до режиму моделювання. У цьому режимі пакети відображаються у вигляді конвертів, час керується подіями, а користувач може покроково проходити по мережних подіях.

a. Натисніть на піктограмі **Simulation** аби перемкнутися з режиму реального часу **Realtime** до режиму моделювання **Simulation**.

b. Оберіть **HTTP** у фільтрах переліку подій **(Event List Filters)**.

1) HTTP може бути єдиною подією, яка відображається. Якщо потрібно, натисніть на кнопку **Edit Filters** (Редагувати фільтри), яка знаходиться нижче

панелі моделювання для відображення подій, доступних для перегляду. Додайте позначку для **Show All/None** (Показати все/Нічого) і зауважте, як перемикаються прапорці з позначеного на непозначений і навпаки, залежно від поточного стану.

2) Натискайте на прапорці **Show All/None** допоки не звільняться усі опції, і після цього оберіть **HTTP** у вкладці Misc (Різне) у вікні редагування фільтрів. Натисніть на X у верхньому правому куті для закриття вікна **Edit Filters**. У видимих подіях (Visible Events) зараз повинен відображатися тільки протокол HTTP.

Крок 2: Створення веб-трафіку (HTTP).

Зараз панель моделювання (Simulation Panel) порожня. Вгорі на панелі у списку подій вказані п'ять стовпців. У міру того, як трафік генерується і поступово просувається, у списку з'являтимуться події.

Примітка: Веб-сервер і веб-клієнт відображаються на лівій панелі. Можна регулювати розміри панелей, для цього потрібно навести курсор на смугу прокрутки і при появі двонаправленої стрілки, перетягнути межу ліворуч або праворуч.

a. Натисніть на **Web Client** на дальній лівій панелі.

b. Натисніть на вкладці **Desktop** і відкрийте веб-браузер, натиснувши на піктограмі **Web Browser**.

c. У полі URL введіть **www.osi.local** і натисніть **Go**.

Оскільки час у режимі моделювання залежить від подій, Вам потрібно використовувати кнопку **Capture/Forward** для відображення подій у мережі. Кнопка захоплення і перенаправлення (Capture/Forward) розміщена у лівій частині синьої смуги, нижче вікна топології. Серед наявних трьох кнопок вона розташована праворуч.

d. Чотири рази натисніть кнопку **Capture/Forward** . У списку повинні з'явитися чотири події.

Погляньте на сторінку веб-браузера на Web Client. Чи відбулися якісь зміни?

Крок 3: Дослідіть вміст протокольного блоку даних HTTP.

a. Натисніть на першому кольоровому квадратному полі у списку подій: **Event List** > **колонка Type**. Можливо знадобиться розгорнути **Simulation Panel** або використати смугу прокрутки безпосередньо під **Event List**.

Інформація про PDU для пристрою: відображається вікно Web Client. Оскільки це початок передавання, у вікні є лише дві вкладки: **OSI Model**(модель OSI) і **Outbound PDU Details** (Деталі вихідного PDU). При появі більшої кількості подій, з'явиться ще третя вкладка **Inbound PDU Details** (Деталі вхідного PDU). Після останньої події з потоку трафіку, відображатимуться лише вкладки **OSI Model** і **Inbound PDU Details**.

b. Переконайтесь, що обрано вкладку **OSI Model**.

Під колонкою **Out Layers** (Вихідні рівні), Натисніть на **Layer 7.**

Яка інформація наведена за допомогою пронумерованих записів нижче полів **In Layers** (Вхідні рівні) та **Out Layers** для рівня 7?

Яке значення для **Dst Port** (Порт призначення) для **Layer 4** (Рівень 4) міститься у колонці **Out Layers** ?

Яке значення має **Dest IP**-для **Layer 3**(Рівень 3) у колонці **Out Layers** ?

Яка інформація показана на Layer 2 (рівні 2) у колонці **Out Layers**?

c. Натисніть на вкладці **Outbound PDU Details** .
Інформація, наведена під **PDU Formats** відповідає рівням моделі TCP/IP.
Примітка: Інформація, наведена у розділі **Ethernet II** вкладки Outbound PDU Details більш деталізована, аніж та, що наводиться у вкладці Layer 2 **моделі OSI**. **Outbound PDU Details** містить детальнішу інформацію. Значення у полях **DEST MAC** і **SRC MAC** у частині **Ethernet II PDU Details** з'являється у вкладці **OSI Model** на Layer 2, проте не позначаються як такі.

Яка інформація традиційно міститься у розділі **IP PDU Details** , у порівнянні з інформацією з вкладки **OSI Model** ? З яким рівнем вона пов'язана?

Яка інформація традиційно міститься у розділі **TCP PDU Details**, порівняно з інформацією на вкладці **OSI Model** , і з яким рівнем вона пов'язана?

Який **Вузол** вказаний у розділі **HTTP деталей PDU**? З яким рівнем пов'язана ця інформація у вкладці **OSI Model** ?

d. Натисніть на наступному кольоровому квадраті у **Event List (Список подій)** > **колонка Type**. Активний лише рівень 1 (незабарвлений). Пристрій переміщує кадрі з буфера до мережі.

e. Перейдіть до наступного поля типу **HTTP** у **Event List(Список подій)** і Натисніть на кольоровому квадраті. Це вікно містить як вхідні рівні **In Layers** так і вихідні рівні **Out Layers**. Зверніть увагу на напрямок стрілки безпосередньо у колонці **In Layers**; вона вказує вгору, у напрямку передавання даних. Перейдіть по цих рівнях, зважаючи на елементи, які ми попередньо розглянули. Зверху колонки стрілка вказує праворуч. Це означає, що зараз сервер надсилає інформацію назад до клієнта.

Які основні відмінності можна побачити при порівнянні даних, зображених у колонці **In Layers** з даними колонки **Out Layers**?

f. Перейдіть до вкладки **Inbound and Outbound PDU Details**. Перегляньте деталі PDU.

g. Натисніть на останньому кольоровому квадраті у колонці **Info**.

Скільки вкладок відображається для цієї події? Поясніть.

Інструкції

Частина 2: Відображення елементів стеку протоколів TCP/IP

У частині 2 цього завдання Ви використаєте режим моделювання Packet Tracer для перегляду і вивчення деяких інших протоколів, що належать до стеку TCP/IP.

Крок 1: Перегляд додаткових подій

a. Закрийте усі відкриті вікна з інформацією про PDU.

b. У розділі **Event List Filters** > **Visible Events**, натисніть на **Show All/None**.

Які додаткові типи подій (Event Types) відображаються?

Ці додаткові записи відіграють різні ролі у TCP/IP. Протокол визначення адрес (ARP) надсилає запити про MAC-адреси для вузлів отримувачів. DNS відповідає за визначення IP-адреси для відповідних доменних імен (наприклад, **www.osi.local**). Додаткові події TCP відповідають за встановлення з'єднання (сеансів зв'язку), узгодження параметрів передачі даних і закриття з'єднання (сеансів зв'язку) між пристроями. Ці протоколи вже попередньо згадувалися і будуть обговорюватися далі під час вивчення курсу. На разі наявно більше 35 протоколів (типів подій), доступних для аналізу у Packet Tracer.

c. Натисніть на першій події DNS у колонці **Type**. Розгляньте вкладки **OSI Model** і **PDU Detail** та зверніть увагу на процес інкапсуляції. Якщо поглянути на вкладку **OSI Model**, виділивши **Layer 7**, опис того, що відбувається, буде розміщений безпосередньо нижче **In Layers** і **Out Layers** (“1. DNS клієнт надсилає DNS-запит до DNS-сервера.”). Це дуже важливі дані, які допомагають зрозуміти процеси, які мають місце при передачі даних.

d. Натисніть на вкладці **Outbound PDU Details** .

Яка інформація міститься у полі **NAME**: у розділі запиту DNS QUERY?

e. Натисніть на останньому кольоровому квадраті DNS **Info** у списку подій.

На якому пристрої було захоплено PDU?

Яке значення вказане поряд з **ADDRESS**: у частині DNS ANSWER **Inbound PDU Details**?

f. Знайдіть першу подію **HTTP** у переліку і Натисніть на кольоровому квадраті події **TCP** , розміщеному одразу після цієї події. Оберіть **(Layer 4)** на вкладці **OSI Model**.

Яка інформація відображається у пункті 4 і 5 пронумерованого списку, що міститься безпосередньо під **In Layers** і **Out Layers**?

Окрім інших важливих функцій, TCP керує підключенням і відключенням каналу передавання даних. Саме ця подія відображає, що канал зв'язку налаштовано (ESTABLISHED).

g. Натисніть на останній події TCP. Оберіть layer 4 у вкладці **OSI Model**. Ознайомтесь з записами, наведеними безпосередньо нижче **In Layers** і **Out Layers**.

Вкажіть, яке призначення цієї події, виходячи з інформації, поданої в останньому записі списку (повинен бути запис 4)?

Запитання підвищеної складності

Моделювання демонструє приклад сеансу зв'язку між веб-клієнтом і веб-сервером у локальній мережі. Клієнт робить запити щодо визначених сервісів, запущених на сервері. Сервер повинен бути налаштований на прослуховування конкретних портів у очікуванні запитів від клієнтів. (Підказка: Інформацію про порти можна переглянути за допомогою Layer 4 у вкладці **OSI Model**.)

На підставі інформації, отриманої під час перехоплення за допомогою Packet Tracer, зазначте, який номер порту прослуховує **Web Server**, очікуючи на веб-запити?

Який порт прослуховує **Web Server** щодо DNS-запитів?

Лабораторна робота №2.1

Використання засобу PacketTracer для побудови мережі робочої групи

Мета роботи: Отримати практичні навики в використанні основних функцій програми Packet Tracer.

Зауваження

Щоб інструкції під час виконання вправи відображалися, поставте прапорець Top (Вгорі) в нижньому лівому куті вікна з інструкціями.

Крок 1: Створення логічної схеми мережі з двома комп'ютерами і концентратором

1. У нижньому лівому кутку вікна PacketTracer відображені вісім значків, що представляють категорії або групи пристроїв, наприклад: Маршрутизатори, Комутатори або Кінцеві пристрої.
2. Якщо підвести курсор до категорії пристрої, відобразиться її назва. Перш ніж вибрати пристрій, потрібно визначити категорію. Параметри вибраної категорії відображаються в полі поруч зі списками.
3. Виберіть потрібний варіант пристрою.
4. Виберіть зі списку варіантів в лівому нижньому кутку пункт **End Devices (Кінцеві пристрої)**. Перетягніть у свою робочу зону два комп'ютера **PC**.
5. Виберіть зі списку варіантів в лівому нижньому кутку пункт **Network Device (Мережеві пристрої)** нижче виберіть **Hubs (Концентратори)**. Додайте концентратор в топологію мережі методом перетягування в робочу область.
6. Виберіть у лівому нижньому кутку значок **Connections (Підключення)**. Вибрати **прямий кабель з мідними провідниками**. Клацніть на першому вузлі **PC0** і надайте кабель підключення порту **FastEthernet**. Клацніть на концентраторі **Hub0**, і виберіть порт **Port0**, для підключення до **PC0**.
7. Повторіть даний крок з комп'ютером **PC1** для підключення його до порту **Port1** концентратора.

Крок 2: Налагодження імен вузлів і IP-адрес всіх комп'ютерів

1. Клацніть на значку **PC0**. З'явиться вікно PC0.
2. З вікна PC0 виберіть вкладку **Config (Налаштування)**. Змініть ім'я PC0 на **PC-A**. Виберіть вкладку **FastEthernet** ліворуч і додайте IP-адресу **192.168.1.1** та маску мережі **255.255.255.0**. Закрийте вікно налаштування **PC-A**, клацнувши значок «x» у правому верхньому куті.
3. Клацніть на значку **PC1**.
4. Виберіть вкладку **Config (Налаштування)**. Змініть ім'я комп'ютера на **PC-B**. Виберіть вкладку **FastEthernet** ліворуч і додайте IP-адресу **192.168.1.2** та маску мережі **255.255.255.0**. Закрийте вікно налаштування ПК-B.

Крок 3: Перевірка зв’язку між комп’ютерами PC-A і PC-B

1. Клацніть на інструменті **Select (Вибір)** в правій вертикальній панелі інструментів (Це верхній значок на панелі).
2. Клацніть значок **ПК-А** і виберіть вкладку **Desktop (Настільний комп'ютер)**.
3. Відкрийте в цій вкладці **командний рядок (Command Prompt),** введіть команду **ping 192.168.1.2** і натисніть ENTER.
4. Успішне проходження **ехо-запиту** означає, що мережа налаштована правильно і протокол підтверджує правильність апаратної і програмної конфігурації. Результат успішно виконаного ехо-запиту має такий вигляд:

   PC>**ping 192.168.1.2**

   Pinging 192.168.1.2 with 32 bytes of data:

   Reply from 192.168.1.2: bytes=32 time=14ms TTL=128
   Reply from 192.168.1.2: bytes=32 time=6ms TTL=128
   Reply from 192.168.1.2: bytes=32 time=6ms TTL=128
   Reply from 192.168.1.2: bytes=32 time=6ms TTL=128

   Ping statistics for 192.168.1.2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds:
   Minimum = 6ms, Maximum = 14ms, Average = 8ms

5. Закрийте вікно налаштування.

Лабораторна робота №2.2
Відстеження пакетів у мережі

Мета роботи: Отримати практичні навики в роботі з утилітами діагностики та відслідковування пакетів в мережі за допомогою середовища Packet Tracer.

Крок 1: Перевірка безперервності каналу від вузла-джерела до вузла призначення

Відкрийте командний рядок вузла джерела і відправте адресату echo-запит.

1. Виберіть PC0. Відкрийте вкладку **Desktop (Робочий стіл)** > **Command Prompt (Командний рядок)**.
2. Введіть: **ping 192.168.3.2** і натисніть *ENTER*.

Наявність відповіді підтверджує безперервність каналу від вузла до пристрою призначення. Він не визначає пройдений шлях пакетом. Перші echo-запити можуть затриматися на час завантаження пристроїв. Якщо затримуються всі echo-запити, повторіть команду.

Крок 2: Визначення пройденого шляху пакету за допомогою команди tracert

1. В тому ж вікні **Command Prompt (Командний рядок)** PC0, введіть **tracert 192.168.3.2** і натисніть *ENTER*. Команда **tracert** повинна відобразити чотири ділянки, причому четверта буде відповідати адресату. У даному процесі не тільки перевіряється безперервність каналу, але і вказується точний шлях пакетів.
2. Закрийте вікно налаштування ПК0.

Крок 3: Перегляд шляху пакету в режимі моделювання

1. Відкрийте вкладку **Simulation (Моделювання)**, яка частково прихована за вкладкою **RealTime (У реальному часі)** в правому нижньому кутку. На вкладці є значок таймера.

2. Натисніть кнопку **Add Simple PDU (Додати простий PDU)**. Це значок закритого конверта, який знаходиться в правій вертикальній панелі інструментів. Потім клацніть PC0 і PC1. Добавиться пакет echo-запиту від джерела до адресата.

3. Натисніть кнопку **Edit Filter (Правка фільтрів)** в області **Edit List Filter (Виправлення списку фільтрів).** Після натискання кнопки **Edit Filters** відкриється спливаюче вікно. У цьому вікні поставте прапорець **Show All/None (Показати все / нічого)** для скасування виділення всіх фільтрів. Виберіть лише фільтр ICMP.

4. У вікні робочої області клацніть і розгорніть хмару мережі для її розширення і перегляду маршрутизаторів, що з'єднанні у рамках хмари. Джерело і адресат знаходяться за межами екрану. Показані лише маршрутизатори і пакети в межах хмари, якими обмінюються ці пристрої.

5. Натисніть кнопку **Auto Capture/Play (Автозахват/відтворення)** на панелі **Simulation (Моделювання)** та перегляньте шлях пакету до адресата.

Зверніть увагу, що, згідно зі списком подій, між джерелом і адресатом знаходиться три маршрутизатора. Саме цей шлях відобразився раніше у вікні командного рядка, після подачі команди **tracert**.

Лабораторна робота №3

Обтискання кабелів скрученої пари дротів з дотриманням стандартів TIA/EIA 568 A/B.

Мета роботи: Навчитись обтискати кабелі згідно стандартів TIA/EIA 568A/B.

Порядок виконання роботи.

1. Одержати у викладача матеріали та інсртументи для роботи:
   - Вита пара мідного дроту (UTP) CAT 5;
   - Конектори RJ-45;
   - RJ-45 обжимний інструмент, для встановлення RJ-45 конекторів на кінцях кабелю;
   - Кабель-тестер (Fluke 630);
   - Кусачки;
2. Ознайомитись із стандартом обжимання кабелів TIA/EIA 568 A/B та використовуючи отриманий інструмент, обжати прямий кабель (див. Табл. 1). Для цього потрібно виконати наступні дії:
   - Вирізати частину витої пари мідного дроту CAT5 заданої викладачем довжини.
   - Зачистити на 4 см ізоляцію з кожного кінця кабеля.
   - Розплести пари і встановити їх в порядку згідно з стандартом TIA568-A.
   - Розпрямити провода і обрізати їх в межах 1,8 – 2,2 см від краю ізоляції.
   - Встановити конектор RJ-45 на кінці кабеля. Переконайтесь, що частина ізоляції знаходиться в середині конектора RJ-45.
   - Використовуючи інструмент обжати кабель.
   - Повторити пункти 4-7, щоб обжати інший кінець кабелю використовуючи TIA568-A схему.
3. Провести тестування обтиснутого прямого кабеля використовуючи тестер FLUKE 630.
4. Аналогічно до п. 2 обтиснути крос-кабель (див. Табл. 2).
5. Провести тестування обтиснутого крос-кабеля використовуючи тестер FLUKE630.
6. Показати результи викладачу.
7. Оформити звіт по виконаній роботі.

Прямий кабель (straight-through cable) призначений для з'єднання різнотипного обладнання (типу "комп'ютер-концентратор", "комп'ютер-комутатор" і т.д. Прямий кабель виконується у відповідності з стандартом TIA/EIA-568 A для 10BASE-T Ethernet, який визначає колір для кожного роз'єму (табл. 1). Кабель повинен завершуватись RJ-45 конекторами на кожному кінці.

Таблиця 1 TIA568-A стандарту

Роз’єм	Пара	Функція	Колір проводу	100BASE-T Ethernet?	1000BASE-T Ethernet?
1	3	Передача	Біло-зелений	Так	Так
2	3	Передача	Зелений	Так	Так
3	2	Прийом	Біло-оранжевий	Так	Так
4	1	Не використовується	Синій	Ні	Так
5	1	Не використовується	Біло-синій	Ні	Так
6	2	Прийом	Оранжевий	Так	Так
7	4	Не використовується	Біло-коричневий	Ні	Так
8	4	Не використовується	Коричневий	Ні	Так

Крос-кабель (crossover cable) призначений для з’єднання однотипного обладнання (типу “комп’ютер- комп’ютер”, “концентратор - концентратор” і т.д. Даний кабель виконується у відповідності з стандартом TIA/EIA-568 A/B для 10BASE-T Ethernet, який визначає колір для кожного роз’єму. Крос-кабель отримується, якщо один кінець кабелю обжати у відповідності з TIA/EIA568-A, а інший у відповідності з TIA/EIA568-B (табл. 2). Кабель повинен завершуватись RJ-45 конекторами на кожному кінці.

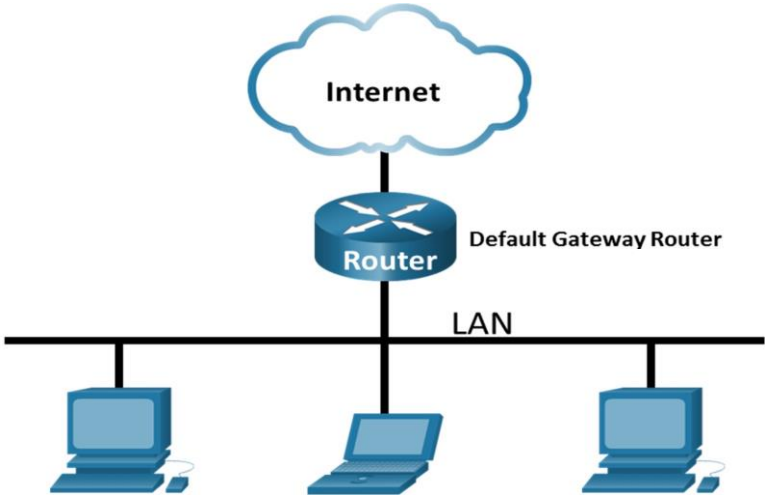
Таблиця 2 TIA568-B стандарту

Роз’єм	Пара	Функція	Колір проводу	100 BASE-T Ethernet?	1000 BASE-T Ethernet?
1	2	Передача	Біло-оранжевий	Так	Так
2	2	Передача	Оранжевий	Так	Так
3	3	Прийом	Біло-зелений	Так	Так
4	1	Не використовується	Синій	Ні	Так
5	1	Не використовується	Біло-синій	Ні	Так
6	3	Прийом	Зелений	Так	Так
7	4	Не використовується	Біло-коричневий	Ні	Так
8	4	Не використовується	Коричневий	Ні	Так

Лабораторна робота №4

Використання Wireshark для перегляду мережевого трафіку

Топологія



Цілі та задачі
Частина 1: Завантажити та встановити Wireshark
Частина 2: Перехоплення та аналіз локальних ICMP-даних за допомогою Wireshark
Частина 3: Перехоплення та аналіз віддалених ICMP-даних за допомогою Wireshark

Довідкова інформація / Сценарій

Wireshark - це програмний аналізатор протоколів або програма "пакетний сніфер", яка використовується для пошуку та усунення несправностей мережі, аналізу повідомлень, розробки програм та протоколів, а також для навчання. Під час передачі даних через мережу, сніфер "захоплює" кожен протокольний блок даних (PDU) і може декодувати та аналізувати його вміст згідно з відповідними RFC або іншими специфікаціями.

Wireshark є корисним інструментом для всіх, хто працює з мережами, і його можна використовувати в більшості лабораторних робіт для аналізу даних, пошуку та усунення несправностей. Ця лабораторна робота містить інструкції щодо завантаження та встановлення Wireshark. Також у цій лабораторній роботі Ви будете використовувати Wireshark для перехоплення IP-адрес з ICMP-повідомлення та MAC-адрес з Ethernet-кадра.

Необхідні ресурси

- 1 ПК з ОС Windows та доступом до мережі Інтернет

- Додаткові ПК в локальній мережі будуть використовуватись для відповідей на ping-запити.
- 1 ПК з ОС Windows та доступом до мережі Інтернет

Частина 1: Завантажити та встановити Wireshark

Крок 1: Завантаження Wireshark.

a. Wireshark можна завантажити з сайту www.wireshark.org.

b. Оберіть необхідну версію програмного продукту, враховуючи архітектуру та операційну систему Вашого комп'ютера. Наприклад, якщо у вас 64-розрядний ПК з операційною системою Windows, виберіть **Windows Installer (64-bit)**.

   Щойно вибір зроблено, завантаження має розпочатися. Розташування завантаженого файлу залежить від використовуваного браузера та операційної системи. Для користувачів Windows за замовчуванням використовується папка **Downloads**.

Крок 2: Встановлення Wireshark.

a. Завантажений файл має назву **Wireshark-win64-x.x.x.exe**, де **x** - це номер версії, якщо Ви завантажили 64-бітну версію. Двічі натисніть на значку файла, щоб розпочати процес встановлення.

   Відповідайте на будь-які повідомлення безпеки, які можуть відображатися на екрані. Якщо копія Wireshark вже встановлена на Вашому ПК, Вам буде запропоновано видалити стару версію перед встановленням нової версії. Перед встановленням іншої версії рекомендується видалити стару версію Wireshark. Натисніть**Yes**, щоб видалити попередню версію Wireshark.

b. Якщо Ви встановлюєте Wireshark вперше або після завершення процесу видалення попередньої версії, Ви перейдете до Wireshark Setup Wizard. Натисніть **Next**.

c. Продовжуйте процес встановлення. Натисніть **I Agree**, коли з'явиться вікно ліцензійної угоди.

d. Залиште налаштування за замовчуванням у вікні «Вибір компонентів» і натисніть **Next**.

e. Виберіть потрібні параметри і натисніть **Next**.

f. Ви можете змінити розташування Wireshark, але якщо у Вас достатньо вільного місця на диску, рекомендується зберегти розташування за замовчуванням. Натисніть **Next**, щоб продовжити.

g. Для захоплення даних в реальному часі на Вашому комп'ютері повинен бути встановлений Npcap. Якщо на Вашому комп'ютері Npcap вже встановлено, опція Встановити не буде зазначена. Якщо у Вас встановлена версія Npcap старіша ніж версія, яка йде в комплекті з Wireshark,

рекомендується встановити нову версію, вибравши опцію **Install Npcap x.x.x** (номер версії). Натисніть **Next**, щоб продовжити.

h. **НЕ** встановлюйте USBPcap для захоплення звичайного трафіку. **НЕ обирайте опцію Встановити USBPcap**. USBPcap є експериментальним, і це може спричинити проблеми з використанням USB на ПК. Натисніть **Install** , щоб продовжити.

i. Wireshark починає встановлювати свої файли та відображати стан встановлення.

j. В окремому вікні прийміть ліцензійні умови в Npcap Setup Wizard, якщо встановлюєте Npcap. Натисніть **I Agree**, щоб продовжити. Натисніть **Install** , щоб встановити Npcap. Натисніть **Next** , щоб завершити встановлення Npcap і натисніть **Finish**, щоб вийти з процесу встановлення Npcap.

k. Натисніть **Next**, коли встановлення Wireshark буде завершено.

l. Натисніть **Finish**, щоб завершити процес встановлення Wireshark. Перезавантажте комп'ютер, якщо це необхідно.

Частина 2: Перехоплення та аналіз локальних ICMP-даних за допомогою Wireshark

У Частині 1 цієї лабораторної роботи Ви перевірите зв'язок з іншим ПК локальній мережі за допомогою команди ping та перехопите згенеровані ICMP-запити та ICMP-відповіді, використовуючи Wireshark. Ви також розглянете вміст перехоплених кадрів для отримання певної інформації. Цей аналіз має допомогти Вам з'ясувати, як заголовки повідомлень використовуються для транспортування даних до місця призначення.

Крок 1: Визначення адрес мережної плати Вашого ПК.

В цій лабораторній роботі Вам необхідно визначити логічну та фізичну адреси, тобто IP-адресу та MACадресу мережної плати/інтерфейсу Вашого ПК.

a. У командному рядку введіть команду **ipconfig /all**, щоб переглянути IP-адресу, MAC-адресу, опис мережної плати Вашого ПК.

C:\Users\Student> **ipconfig /all**

```
Windows IP Configuration
    Host Name . . . . . . . . . . . . : DESKTOP-NB48BTC
    Primary DNS Suffix . . . . . . . :
  Node Type . . . . . . . . . . . . : Hybrid
  IP Routing Enabled. . . . . . . . : No
  WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:
```

```
   Connection-specific DNS Suffix . :
   Description . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . :00-26-B9-DD-00-91
   DHCP Enabled. . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.1.1
<output omitted>
```

b. Запитайте члена або членів команди про IP-адресу їх ПК та надайте їм IP-адресу свого ПК. На цьому етапі не повідомляйте їм свою MAC-адресу.

Крок 2: Запуск Wireshark і початок перехоплення даних.

a. Перейдіть до Wireshark. Двічі натисніть на потрібному інтерфейсі, щоб розпочати перехоплення повідомлень. Переконайтеся, що на потрібний інтерфейс надходить трафік.

b. У верхній частині вікна Wireshark рядки даних почнуть прокручуватися донизу. Рядки даних, залежно від протоколу, матимуть різне забарвлення.

   Вони можуть прокручуватися дуже швидко. Швидкість залежатиме від інтенсивності спілкування, яке зараз відбувається між Вашим ПК та іншими вузлами локальної мережі. Для полегшення перегляду даних, які перехоплює Wireshark, та подальшого їх опрацювання можна застосувати фільтри.
   У цій лабораторній роботі нас цікавить відображення лише повідомлень протоколу ICMP (ping). Наберіть **icmp** у полі **Filter** у верхній частині вікна Wireshark і натисніть або **Enter,** або кнопку **Apply** (значок стрілочки), щоб переглядати тільки ICMP-повідомлення.

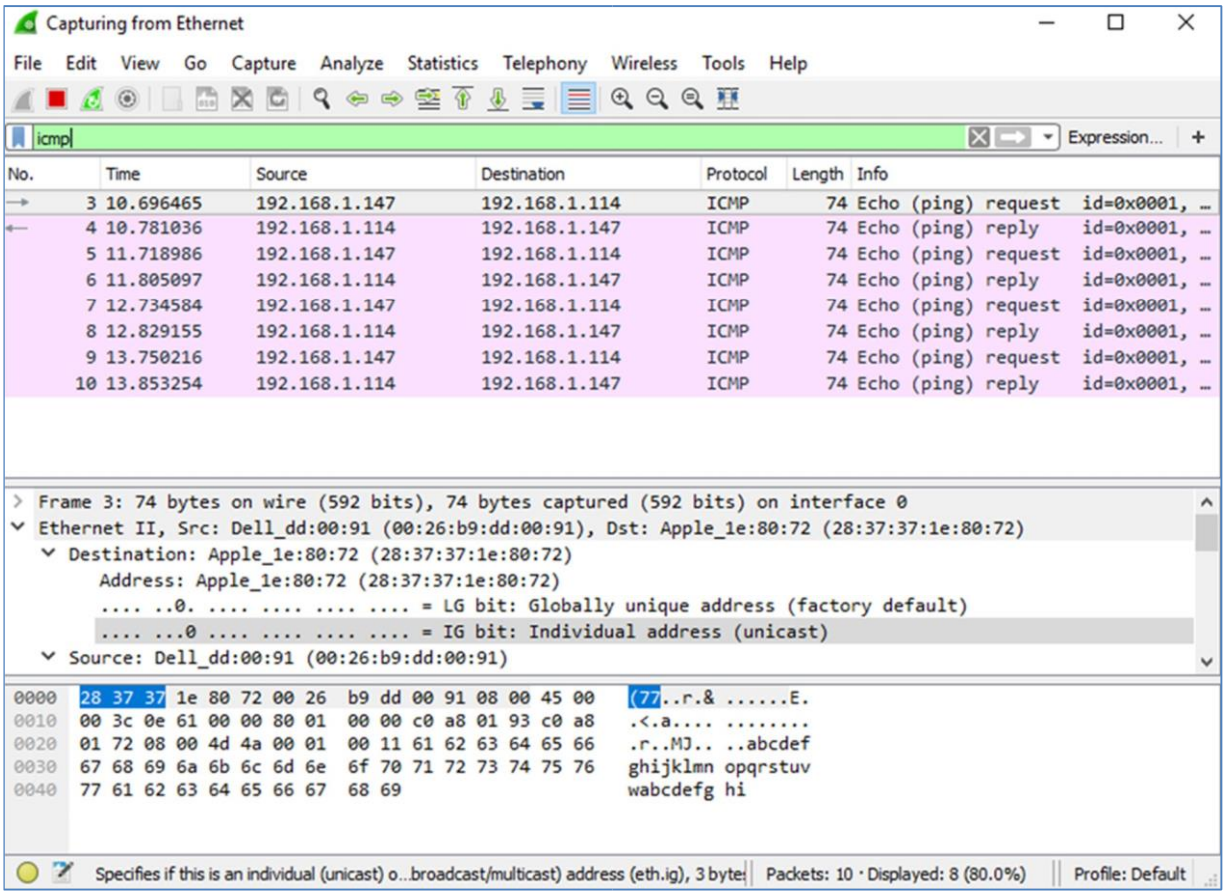
c. Як наслідок застосування цього фільтру всі дані у верхній частині вікна зникнуть, але процес перехоплення трафіку на мережній платі/інтерфейсі продовжується. Перейдіть до вікна командного рядка та пропінгуйте IP-адресу, надану членом Вашої команди.

```
C:\> ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128
Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.114:
```

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Зверніть увагу на те, що дані знову з’являються у верхній частині вікна Wireshark.



Примітка: Якщо ПК члена Вашої команди не відповідає на Ваші ping-запити, причиною може бути блокування цих запитів його міжмережним екраном. Будь ласка, в Додаток A: Дозвіл передачі ICMPтрафіку через міжмережний екран ОС Windows знайдіть і перегляньте інформацію про те, як дозволити передачу ICMP-трафіку через міжмережний екран в ОС Windows.

d. Зупиніть перехоплення даних, натиснувши значок **Stop Capture**.

Крок 3: Дослідження перехоплених даних.

На Кроці 3 виконується перегляд даних, які були згенеровані ping-запитами ПК члена Вашої команди. Дані Wireshark відображаються у трьох секціях: 1) у верхній секції відображається перелік перехоплених кадрів з узагальненням даних IP-пакета; 2) у середній секції відображаються дані кадру, вибраного у верхній частині екрана і перехоплений кадр розділяється на підсекції відповідно до протокольних рівнів; 3) нижня секція відображає

необроблені дані кожного рівня. Необроблені дані відображаються як у шістнадцятковій, так і у десятковій формах.

a. У верхній частині вікна Wireshark натисніть на кадр, що містить перший ICMP-запит. Зауважте, що стовпчик **Source** містить IP-адресу Вашого ПК, а стовпчик **Destination** містить IP-адресу ПК Вашого колеги по команді (саме того ПК, який Ви пінгували).

b. Якщо цей кадр все ще вибраний, перейдіть до середньої частини. Натисніть на значок стрілки ліворуч від рядка Ethernet II, щоб переглянути MAC-адреси отримувача та відправника кадру.

Чи співпадає MAC-адреса відправника з MAC-адресою мережної плати/інтерфейсу Вашого ПК?

Чи відповідає у Wireshark MAC-адреса отримувача MAC-адресі ПК Вашого колеги по команді?

Як Ваш ПК отримав MAC-адресу пропінгованого ПК?

Примітка: У попередньому прикладі із перехоплення ICMP-запиту, дані протоколу ICMP інкапсулюються в IPv4-пакет (додається заголовок IPv4), який потім інкапсулюється у кадр Ethernet II (додаються заголовок та трейлер - контрольна сума Ethernet II) для передачі через локальну мережу.

Частина 3: Перехоплення та аналіз віддалених ICMP-даних за допомогою Wireshark

У Частині 2 цієї лабораторної роботи Ви за допомогою команди ping перевірите зв'язок з віддаленими вузлами (вузлами, які не належать до Вашої локальної мережі) та дослідите отримані дані. Потім Ви маєте визначити чим відрізняються ці дані від даних, які досліджувалися у Частині 1.

Крок 1: Початок перехоплення даних на мережній платі/інтерфейсі.

a. Розпочніть перехоплення даних знову.

b. Wireshark запропонує Вам зберегти раніше перехоплені дані перед початком іншого перехоплення. Зберігати ці дані не обов’язково. Натисніть **Continue without Saving**.

c. Після активізації перехоплення у командному рядку Windows виконайте команду ping для таких трьох URL-адрес веб-сайтів:

1) www.yahoo.com

2) www.cisco.com

3) www.google.com

Примітка: Коли Ви пінгуєте перелічені URL-адреси, зауважте, що DNS-сервер транслює ці URL в IPадреси. Зверніть увагу на IP-адреси, отримані для кожної URL-адреси.

d. Ви можете зупинити перехоплення даних, натиснувши **Stop Capture**.

Крок 2: Дослідіть та проаналізуйте дані з віддалених вузлів.

Перегляньте перехоплені дані в Wireshark та дослідіть IP-адреси та MAC-адреси трьох веб-сайтів, з якими Ви перевіряли зв'язок. Запишіть IP-адреси та MAC-адреси отримувачів для трьох веб-сайтів, з якими Ви перевіряли зв'язок.

IP-адреса для **www.yahoo.com**:

MAC-адреса для **www.yahoo.com**:

IP-адреса для **www.cisco.com**:

MAC-адреса для **www.cisco.com**:

IP-адреса для **www.google.com**:

MAC-адреса для **www.google.com**:

Що важливе в цій інформації?

Чим ця інформація відрізняється від інформації, яку Ви отримали в Частині 1?

Питання для самоперевірки

Чому Wireshark показує реальні MAC-адреси вузлів локальної мережі, але не показує реальні MACадреси вузлів віддалених мереж?

Додаток A: Дозвіл передачі ICMP-трафіку через міжмережевий екран ОС Windows

Якщо члени Вашої команди не можуть виконати ping-запити до Вашого ПК, ймовірно саме міжмережний екран блокує ці запити. У цьому додатку наведено опис створення правила на міжмережному екрані, яке дозволяє виконання ping-

запитів. Також наведено опис відключення створеного ICMP-правила після завершення виконання лабораторної роботи.

Частина 1: Створення нового вхідного правила, яке дозволить ICMP-трафіку пройти через міжмережний екран.

a. Перейдіть до **Control Panel** і натисніть опцію **System and Security** в Category view.

b. У вікні **System and Security**, натисніть **Windows Defender Firewall** або **Windows Firewall**.

c. На лівій панелі **Windows Defender Firewall** або вікна **Windows Firewall** натисніть **Advanced settings**.

d. У вікні **Advanced Security** на лівій бічній панелі виберіть опцію **Inbound Rules** і потім натисніть **New Rule…** на правій бічній панелі.

e. Запустіть **New Inbound Rule Wizard**. У вікні **Rule Type** спочатку натисніть кнопку **Custom**, а потім – кнопку **Next**.

f. На лівій панелі вікна виберіть параметр **Protocol and Ports** і, використовуючи спадне меню **Protocol Type**, виберіть **ICMPv4**, а потім натисніть **Next**.

g. Переконайтесь, що як для локальних так і для віддалених адрес вибрано **Any IP address**. Натисніть **Next**, щоб продовжити.

h. Виберіть **Allow the connection**. Натисніть **Next**, щоб продовжити.

i. За замовчуванням це правило застосовується для всіх профілів ОС. Натисніть **Next**, щоб продовжити.

j. Задайте назву правила **Allow ICMP Requests**. Натисніть **Finish** щоб завершити. Це нове правило дозволить членам Вашої команди отримувати від Вашого ПК відповіді на їх ping-запити.

Частина 2: Вимкнення або видалення ICMP-правила.

Після завершення лабораторної роботи Ви можете вимкнути або навіть видалити правило, створене на Кроці 1. Для вимкнення правила використовуйте параметр **Disable Rule**, це дозволить Вам пізніше увімкнути правило знову. Видалення правила повністю видаляє його зі списку вхідних правил.

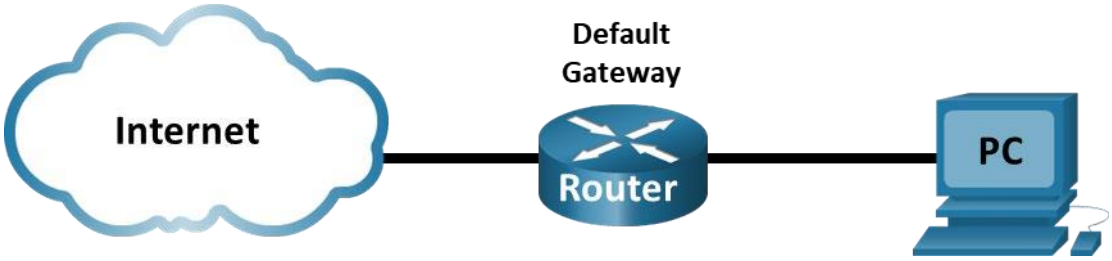
a. У вікні **Advanced Security** натисніть **Inbound Rules** на лівій бічній панелі та знайдіть правило, створене Вами раніше.

b. Правою кнопкою миші виберіть ICMP-правило і виберіть **Disable Rule**, якщо Ви вирішили його відключити. Ви також можете вибрати **Delete**, якщо Ви вирішили видалити правило назавжди. Якщо Ви вибрали цей варіант, то потім доведеться знову створювати правило, якщо буде потрібно дозволити надсилати ICMP-відповіді.

Лабораторна робота №5

Використання Wireshark для дослідження кадрів Ethernet

Топологія



Цілі та задачі

Частина 1: Дослідження полів заголовку кадру Ethernet II

Частина 2: Використання Wireshark для захоплення та аналізу кадрів Ethernet

Довідкова інформація / Сценарій

Коли протоколи верхнього рівня взаємодіють між собою, дані проходять вниз по моделі взаємодії відкритих систем (OSI) та інкапсулюються до кадру Рівня 2. Склад кадру залежить від типу доступу до середовища передавання даних. Наприклад, якщо протоколами верхнього рівня є TCP і IP, а доступ до середовища передавання даних Ethernet, то інкапсуляція кадру Рівня 2 буде Ethernet II. Це характерно для локальної мережі.

Вивчаючи концепції Рівня 2, корисно аналізувати інформацію заголовка кадру. У першій частині цієї лабораторної роботи Ви проаналізуєте поля, що містяться в кадрі Ethernet II. В частині 2 Ви будете використовувати Wireshark для захоплення і аналізу полів заголовка кадру Ethernet II для локального та віддаленого трафіку.

Необхідні ресурси

• 1 ПК (з Windows, з доступом в Інтернет і встановленим Wireshark)

Інструкції:

Частина 1: Дослідження полів заголовку кадру Ethernet II

В Частині 1 Ви будете досліджувати поля заголовку та вміст кадру Ethernet II. Для вивчення вмісту цих полів буде використано захоплення трафіку за допомогою Wireshark.

Крок 1: Ознайомлення з описом і довжиною полів заголовку Ethernet II.

Преамбула	Адреса призначення	Адреса отримувача	Тип кадру	Дані	FCS

8 байтів	6 байтів	6 байтів	2 байти	46 – 1500 байтів	4 байти

Крок 2: Дослідження мережних налаштувань ПК.

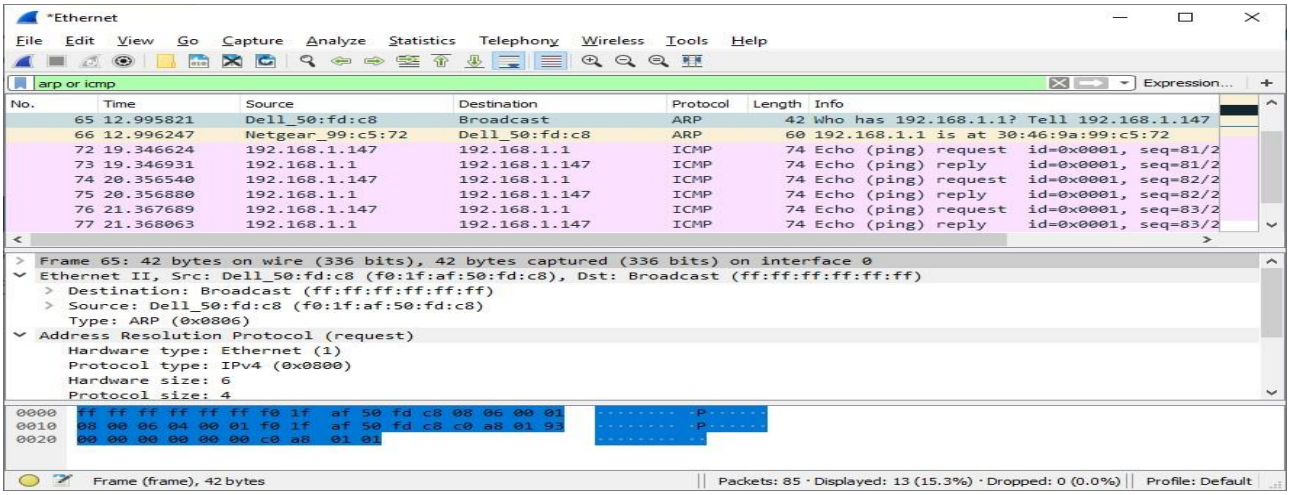
У цьому прикладі IP-адреса ПК 192.168.1.147, а шлюз за замовчуванням має IP-адресу 192.168.1.1.

C:\> **ipconfig /all**
Ethernet adapter
Ethernet:
Connection-specific DNS
Suffix . :
Description . . . . . : Intel(R) 82579LM Gigabit Network Connection
Physical Address. . . . . : F0-1F-AF-50-FD-C8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::58c5:45f2:7e5e:29c2%11(Preferred)
IPv4 Address. . . . . : 192.168.1.147(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, September 6, 2019 11:08:36 AM
Lease Expires . . . . . : Saturday, September 7, 2019 11:08:36 AM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
<output omitted>

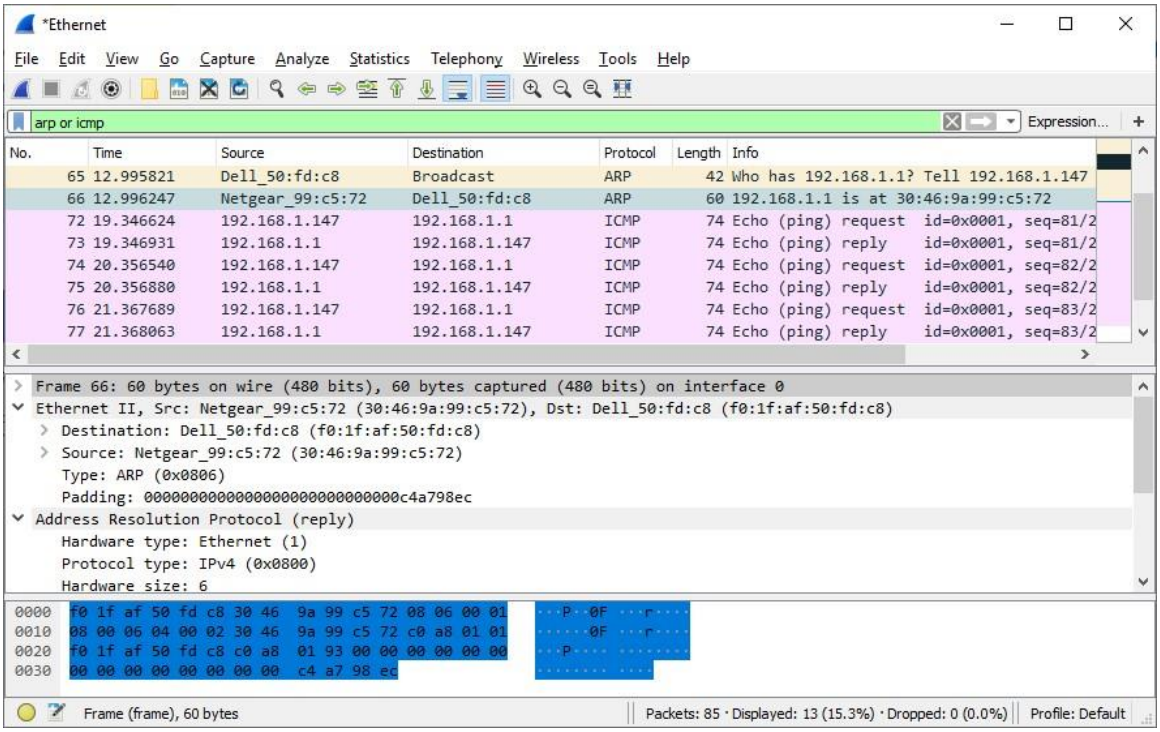
Крок 3: Дослідження кадрів Ethernet у перехопленому трафіку Wireshark.

Нижче на скріншотах перехоплення Wireshark показані пакети, згенеровані на ПК командою ping на його шлюз за замовчуванням. До Wireshark було застосовано фільтр для перегляду лише протоколів ARP і ICMP. ARP означає Address Resolution Protocol (Протокол визначення адрес). ARP - це комунікаційний протокол, який використовується для визначення MAC-адреси, пов'язаної з певною IP-адресою. Сеанс починається з ARP-запиту і відповіді щодо MAC-адреси маршрутизатора-шлюзу, за яким слідують чотири ехо-запити та відповіді.

На цьому скріншоті виділені деталі кадру для ARP-запиту.



На цьому скріншоті виділені деталі кадру для ARP-відповіді.



Крок 4: Дослідження вмісту заголовку Ethernet II ARP-запиту.

Наступна таблиця заповнена даними з першого кадру в захоплені Wireshark і відображає дані в полях заголовку Ethernet II.

Поле	Значення	Опис
Преамбула	Не показано в результатах захоплення	Це поле містить синхронізуючі біти, які обробляються апаратним забезпеченням NIC.

Адреса призначення (Destination Address) Адреса джерела (Source Address)	Broadcast (ff:ff:ff:ff:ff:ff) Netgear_99:c5:72 (30:46:9a:99:c5:72)	Адреси Рівня 2 для кадру. Кожна адреса довжиною 48 біт, або 6 октетів, представлених у вигляді 12 шістнадцяткових цифр, 0-9, A-F. Поширеним форматом є 12:34:56:78:9A:BC. Перші шість шістнадцяткових цифр вказують на виробника мережної інтерфейсної плати (NIC), останні шість шістнадцяткових цифр - серійний номер NIC. Адреса призначення може бути broadcast, яка містить всі одиниці, або індивідуальною. Адреса джерела завжди є індивідуальною.
Тип кадру	0x0806	Для кадрів Ethernet II це поле містить шістнадцяткове значення, яке використовується для позначення типу протоколу верхнього рівня, інкапсульованого в полі даних. Ethernet II підтримує багато протоколів верхніх рівнів. Два поширених типи кадру: Значення Опис 0x0800 Протокол IPv4 0x0806 Address Resolution Protocol (ARP)
Дані	ARP	Містить інкапсульований протокол верхнього рівня. Поле даних містить від 46 до 1 500 байт.
FCS	Не показано в результатах захоплення	Контрольна послідовність кадру, використовується NIC для виявлення помилок, які виникли під час передавання. Значення обчислюється відправником, охоплюючи адресні поля, тип і поле даних кадру. Перевіряється отримувачем.

Що важливого Ви помітили щодо вмісту поля адреси призначення?

Чому ПК надсилає широкомовний ARP-запит перед відправкою першого ping-запиту?

Яка MAC-адреса джерела записана у першому кадрі?

Який Vendor ID (OUI) у NIC джерела в ARP-відповіді?

Яка частина MAC-адреси визначає OUI?

Який серійний номер NIC джерела?

Частина 2: Використання Wireshark для захоплення та аналізу кадрів Ethernet

В Частині 2 Ви будете використовувати Wireshark для захоплення локальних і віддалених кадрів Ethernet. Потім ви будете досліджувати інформацію, яка міститься в полях заголовку кадру.

Крок 1: Визначення IP-адреси шлюзу за замовчуванням на Вашому ПК.

Відкрийте вікно командного рядка Windows і виконайте команду **ipconfig** . Яка IP адреса шлюзу за замовчуванням?

Крок 2: Початкове захоплення трафіку на NIC Вашого ПК.

a. Відкрийте Wireshark, щоб почати захоплення даних.
b. Спостерігайте за трафіком, який з'являється у вікні з переліком пакетів.

Крок 3: Фільтрування трафіка у Wireshark для відображення тільки повідомлень протоколу ICMP.

Ви можете використовувати в Wireshark фільтр для блокування відображення небажаного трафіку. Фільтр не блокує захоплення небажаних даних, він лише фільтрує те, що ви хочете відобразити на екрані. Зараз відображається лише трафік ICMP.

В полі Wireshark **Filter** введіть **icmp**. Поле має набути зеленого кольору, якщо ви правильно ввели значення для фільтру. Якщо поле зеленого кольору, натисніть кнопку **Apply** (стрілка праворуч), щоб застосувати цей фільтр.

Крок 4: Перевірка зв'язку зі шлюзом за замовчуванням вашого ПК за допомогою команди ping.

У вікні командного рядку пропінгуйте шлюз за замовчуванням, використовуючи IP-адресу, записану на Кроці 1.

Крок 5: Припинення захоплення трафіку на NIC.

Натисніть на значок **Stop Capturing Packets**, щоб зупинити захоплення трафіку.

Крок 6: Дослідження першого Echo (ping) запиту в Wireshark.

Головне вікно Wireshark поділено на три частини: панель **переліку пакетів** (вгорі), панель **відомостей про пакет - Packet Details** (посередині) і панель **байтів пакету - Packet Bytes** (внизу). Якщо ви правильно вибрали інтерфейс для захоплення пакетів на попередньому кроці, Wireshark має вивести ICMP інформацію у вікні переліку пакетів Wireshark.

a. В панелі переліку пакетів (верхня частина) клацніть на першому кадрі у переліку. Ви маєте побачити **Echo (ping) запит** під заголовком **Info** . Рядок тепер має бути виділений.

b. Перевірте перший рядок в області відомостей про пакет (середня частина). У цьому рядку відображається довжина кадру.

c. Другий рядок в області відомостей про пакет показує, що це кадр Ethernet II. MAC-адреси джерела та призначення також представлені.

   Яка MAC-адреса у NIC Вашого ПК?

   Яка MAC-адреса шлюзу по замовчуванню?

d. Ви можете натиснути знак «більше» (>) на початку другого рядка, щоб отримати більше інформації про кадр Ethernet II.

   Який тип кадру відображається?

e. Останні два рядки, що відображаються в середній частині, надають інформацію про поле даних кадру. Зверніть увагу, що дані містять інформацію про IPv4-адресу джерела і призначення.

   Яка IP-адреса джерела?

   Яка IP-адреса призначення?

f. Ви можете вибрати будь-який рядок у середній частині, щоб виділити цю частину кадру (шістнадцяткова система числення і ASCII) на панелі **Байти пакету - Packet Bytes** (нижня частина). Виберіть рядок **Internet Control Message Protocol** в середній частині і дослідіть, що виділено в області **Байти пакету - Packet Bytes**.

   Що написано у двох останніх виділених октетах?

g. Виберіть наступний кадр у верхній частині та дослідіть кадр Echo-відповіді. Зверніть увагу, що MACадреси джерела і призначення помінялись місцями, тому що цей кадр був відправлений з маршрутизатора, який виконує роль шлюзу за замовчуванням, у відповідь на перший ping.

   Який пристрій і MAC-адреса відображаються як адреса призначення?

Крок 7: Захоплення пакетів для віддаленого вузла.

a. Натисніть значок **Start Capture**, щоб розпочати нове захоплення Wireshark. Ви отримаєте спливаюче вікно із запитанням про те, чи бажаєте ви зберегти раніше захоплені пакети до файлу перед початком нового захоплення. Натисніть **Continue without Saving**.

b. У вікні командного рядку Window напишіть ping www.cisco.com.

c. Припиніть захоплення пакетів.

d. Дослідіть нові дані в панелі переліку пакетів Wireshark.

У кадрі першого echo (ping) запиту, які MAC-адреси джерела та призначення?
MAC-адреса джерела:

MAC-адреса призначення:

Які IP-адреси джерела і призначення містяться в полі даних кадру?
IP-адреса джерела:

IP-адреса призначення:

Порівняйте ці адреси з адресами, які ви отримали на Кроці 6. Єдина адреса, яка змінилася, це IPадреса призначення. Чому змінилася IP-адреса призначення, в той час як MAC-адреса призначення залишилась незмінною?

Питання для самоперевірки

Wireshark не відображає поле преамбули заголовку кадру. Що містить преамбула?

Лабораторна робота №6

Аналіз трафіку різних типів розсилки

Цілі та задачі:

Частина 1. Генерування трафіку одноадресної передачі

Частина 2. Генерування трафіку широкомовної розсилки

Частина 3. Аналіз трафіку багато адресної розсилки

Вихідні дані:

Ця вправа дає можливість вивчити властивості одноадресної передачі, широкомовної і багато адресної розсилки. Трафік у мережі найчастіше є одноадресним. Коли комп'ютер відправляє ехо-запит ICMP на віддалений маршрутизатор, адресою відправника в заголовку IP-пакета є IP-адреса комп'ютера, що надсилає ехо-запит. Адреса отримувача в заголовку IP-пакета - це IP-адреса інтерфейсу на віддаленому маршрутизаторі. Пакет надсилається тільки до потрібного вузла-адресата.

За допомогою команди **ping** або функції Add Complex PDU програми Packet Tracer можна безпосередньо перевірити широкомовні адреси для перегляду широкомовного трафіку.

Для багатоадресного трафіку буде відображений трафік EIGRP. EIGRP використовується маршрутизаторами Cisco для обміну відомостями про маршрутизацію між маршрутизаторами. Маршрутизатори, що використовують EIGRP, відправляють пакети на адресу групи 224.0.0.10, яка представляє групу маршрутизаторів EIGRP. Незважаючи на те, що ці пакети отримуються іншими пристроями, пакети відкидаються на рівні 3 усіма пристроями, крім маршрутизаторів EIGRP, і при цьому подальша їх обробка не потрібна.

Частина 1: Генерування трафіку одноадресної передачі

Крок 1: Використання команди ping для генерування трафіку.

а) Виберіть **ПК 1**, відкрийте вкладку **Desktop** (**робочий стіл**) і виберіть **Command Prompt** (**командний рядок**).

б) Виконайте команду **ping 10.0.3.2**. Команда ping повинна бути успішно виконана. Запишіть результат виконання команди ping

Крок 2: Перехід в режим моделювання.

а) Відкрийте вкладку **Simulation** (Моделювання), щоб перейти в режим моделювання.

б) Натисніть кнопку **Edit Filters** і переконайтеся, що вибрано тільки події ICMP і EIGRP.

в) Виберіть **ПК1** і виконайте команду **ping 10.0.3.2**.

Крок 3: Аналіз трафіку одноадресної передачі.

Пакет PDU на **ПК 1** - це ехо-запит ICMP, призначений для послідовного інтерфейсу на маршрутизаторі **Router3**.

а) Натисніть кнопку **Capture/Forward** ще раз і подивіться, як ехо-запит відправляється на маршрутизатор **Router3** і ехо-відповідь повертається на **ПК1**. Зупиніть моделювання, коли перша відповідь надійде на ПК1.

Через які пристрої пройшов пакет в ході індивідуальної розсилки?

б) У розділі списку подій панелі моделювання останній стовбець містить кольоровий квадрат, який забезпечує доступ до докладних відомостей про подію. Виберіть кольоровий квадрат в останньому стовпці для першої події. Відкриється вікно відомостей про PDU.

На якому рівні починається ця передача даних і чому?

в) Вивчіть відомості рівня 3 для всіх подій. Зверніть увагу, що IP-адреси відправника і отримувача є адресами індивідуальної розсилки, що вказують на ПК1 і послідовний інтерфейс маршрутизатора Router3.

Які дві зміни відбуваються на рівні 3, коли пакет досягає маршрутизатора Router3?

г) Натисніть кнопку **Reset Simulation**.

Частина 2: Генерування трафіку широкомовної розсилки

Крок 1: Добавлення складного PDU.

а) Натисніть кнопку **Add Complex PDU** (Додати складний PDU). Значок цього пакету знаходиться на правій панелі інструментів і має вигляд відкритого конверта.

б) Наведіть курсор миші на топологію, і курсор прийме вигляд конверта зі знаком плюс (+).

в) Виберіть **ПК1**, який буде відправником для цього текстового повідомлення. Відкриється діалогове вікно **Create Complex PDU** (Створення складного PDU).

Введіть наступні значення:

- Destination IP Address: **255.255.255.255** (адреса широкомовної розсилки)
- Sequence Number: 1
- One Shot Time: **0**

У параметрах PDU значення за замовчуванням для **Select Application**: PING.

Які інші додатки (як мінімум 3) доступні для використання?

г) Натисніть кнопку **Create PDU** (Створити PDU). Цей тестовий пакет широкомовної розсилки тепер з'явиться в списку подій на панелі моделювання. Він також буде показаний у вікні PDU List. Це перший PDU для сценарію 0.

д) Два рази натисніть кнопку **Capture/Forward** (Захопити/Переслати). Цей пакет відправляється на комутатор, а потім широкомовно розсилається на **ПК2**, **ПК3** і **Router1**. Вивчіть відомості рівня 3 для всіх подій. Зверніть увагу, що IP-адреса отримувача - 255.255.255.255. Це широкомовна адреса, яка була налаштований при створенні складного PDU.

Проаналізуйте дані моделі OSI і запишіть, які зміни відбуваються з даними на рівні 3 в стовбці "Out Layers" на вузлах Router1, ПК2 и ПК3?

е) Натисніть кнопку **Capture/Forward** (Захопити/Переслати) ще раз. Чи пересилається широкомовний PDU на маршрутизатор Router2 або Router3? Чому?

ж) Після аналізу поведінки широкомовної розсилки видаліть тестовий пакет, натиснувши кнопку **Delete** під **Scenario 0**.

Частина 3: Аналіз трафіку багатоадресної розсилки

Крок 1: Перевірка трафіку, створеного протоколами маршрутизації.

а) Натисніть кнопку **Capture/Forward**. Пакети EIGRP на маршрутизаторі Router 1 очікують відправки в багатоадресній розсилці на всіх інтерфейсах.

б) Вивчіть вміст цих пакетів, відкривши вікно PDU Information, і натисніть ще раз кнопку **Capture/Forward**. Пакети відправляються до двох інших маршрутизаторів і до комутатора. Маршрутизатори приймають і обробляють пакети, оскільки вони входять до групи багатомовлення. Комутатор перешле пакети на комп'ютери.

в) Натискайте кнопку **Capture/Forward** до тих пір, поки не побачите, що пакет EIGRP поступив на комп'ютери. Що вузли роблять з пакетами?

Вивчіть дані рівнів 3 і 4 для всіх подій EIGRP.

Запишіть адресу отримувача для кожного з пакетів. Запишіть значення поля **Protocol** в заголовку пакетів.

г) Виберіть один з пакетів, доставлених на один з комп'ютерів. Що сталося з цими пакетами?

Проаналізувавши трафік, створений трьома типами IP-пакетів, запишіть, в чому полягають основні відмінності доставки пакетів кожного типу комунікації?

Лабораторна робота №7.1

Перегляд інформації про дротові та бездротові NIC

Цілі та задачі

Частина 1: Визначення та зміна параметрів мережевих інтерфейсних плат (NIC) комп'ютера

Частина 2: Визначення піктограми мережі в системній панелі повідомлень (системний трей) та її використання

Довідкова інформація / Сценарій

В цій лабораторній роботі вам потрібно визначити наявність та стан мережних інтерфейсних карт (NIC), тобто мережних адаптерів, на комп'ютері, який ви використовуєте. Windows надає цілий ряд способів перегляду та роботи з вашими NIC.

У цій лабораторній роботі ви отримаєте доступ до інформації про NIC вашого комп'ютера та змінюватимете їх стан.

Необхідні ресурси

1 ПК (Windows з двома мережними NIC - дротовим і бездротовим) та бездротове з'єднання.

Примітка: На початку цієї лабораторної роботи дротовий NIC Ethernet на ПК було під'єднано до одного з інтегрованих портів комутатора на бездротовому маршрутизаторі і активовано під'єднання по локальній мережі (дротове). Бездротовий NIC був відключений на початку. Якщо дротові та бездротові мережні пристрої ввімкнуто одночасно, ПК отримуватиме дві різні IP-адреси, а бездротовий NIC матиме пріоритет.

Інструкції

Частина 1: Визначення та зміна параметрів мережних інтерфейсних плат (NIC) комп'ютера

У Частині 1 ви визначатимете типи NIC на ПК, який ви використовуєте. Ви розглянете різні способи отримання інформації про ці NIC та способи їх активації і деактивації.

Примітка: Ця лабораторна робота була виконана на ПК, що працює під керуванням операційної системи Windows 10. Ви повинні мати можливість виконувати лабораторну роботу на одній з перерахованих операційних систем Windows; проте вибір меню та екранні форми можуть відрізнятися.

Крок 1: Використовуйте Центр управління мережами і загальним доступом.

a. Перейдіть до **Панелі управління (Control Panel)**. Натисніть **Перегляд стану мережі та з'єднання (View network status and tasks)** в розділі **Мережа та Інтернет (Network and Internet)**.

b. В лівій панелі натисніть на посилання **Змінити налаштування адаптера (Change adapter settings)**.

c. У вікні **Мережеві підключення (Network Connections)** відображається перелік мережевих адаптерів, доступних на цьому ПК. Знайдіть свої адаптери Wi-Fi.

Примітка: В цьому вікні також можуть відображатись адаптер віртуальної приватної мережі (VPN) та інші типи мережевих з'єднань.

Крок 2: Попрацюйте з бездротовим NIC.

a. Знайдіть під'єднання до бездротової мережі. Якщо воно відключене, натисніть правою кнопко миші (ПКМ) та виберіть **Увімкнути (Enable)**, щоб активувати ваш бездротовий NIC.

b. Якщо бездротове з'єднання на під'єднане, натисніть ПКМ та виберіть **Під'єднати/від'єднати (Connect/Disconnect)**, щоб вибрати ідентифікатор бездротової мережі SSID (Service Set Identifier), до якого маєте авторизований доступ.

c. Натисніть ПКМ на бездротовому з'єднанні та виберіть **Стан (Status)**.

d. Вікно **Стан (Status)** бездротового мережного з'єднання показує інформацію про ваш бездротовий зв'язок.

Що таке ідентифікатор бездротової мережі (SSID) для бездротового маршрутизатора вашого з'єднання?

Яка швидкість вашого бездротового з'єднання?

e. Натисніть **Відомості (Details)**, щоб відобразити вікно Інформації про мережне з'єднання (Network Connection Details).

Яка MAC-адреса вашого бездротового NIC?

Чи є у вашому переліку кілька IPv4 DNS-серверів? Якщо так, то чому їх декілька?

f. Відкрийте Командний рядок (Command Prompt) у Windows та введіть команду **ipconfig /all**.

Зауважте, що відображена інформація тут співпадає з інформацією у вікні Інформації про мережеве з'єднання (Network Connection Details) на Кроці e.

g. Закрийте вікно Командного рядка та вікно Інформації про мережне з'єднання. Ви повернетесь у вікно **Стан (Status)** для Wi-Fi. Натисніть **Властивості бездротової мережі (Wireless Properties)**.

h. У вікні **Властивості бездротової мережі (Wireless Properties)** виберіть вкладку **Безпека (Security)**.

i. Тут показано тип захисту, який реалізує під'єднаний бездротовий маршрутизатор. Виберіть прапорець **Показувати символи (Show characters)**, щоб відобразити фактичний ключ безпеки мережі замість прихованих символів, а потім натисніть кнопку **OK**.

j. Закрийте вікна Властивості бездротової мережі (Wireless Properties) та Стан Wi-Fi (Wi-Fi Status). Виберіть і натисніть ПКМ на пункт меню **Wi-Fi** > **Під'єднати/від'єднати (Connect/Disconnect)**. У нижньому правому куті робочого столу повинно з'явитися спливаюче вікно, яке показує ваше поточне з'єднання, а також список SSID, які знаходяться в межах доступу бездротового NIC вашого ПК. Якщо в правій частині цього вікна з'являється смуга прокрутки, ви можете використовувати її для відображення додаткових SSID.

k. Щоб приєднатися до одного з перелічених SSID бездротових мереж, натисніть SSID, до якого потрібно приєднатися, а потім натисніть **Під'єднати (Connect)**.

l. Якщо ви вибрали захищений SSID, вам буде запропоновано ввести **Ключ безпеки (Security key)** для SSID. Введіть ключ безпеки для SSID та натисніть **OK**. Ви можете вибрати прапорець **Приховати символи (Hide characters)**, щоб ніхто не побачив, що ви вводите в полі **Ключ безпеки (Security key)**.

Крок 3: Попрацюйте з дротовим NIC.

a. У вікні Мережних з'єднань (Network Connections) виберіть і натисніть правою кнопкою миші опцію **Ethernet**, щоб побачити випадаючий список. Якщо NIC вимкнено, увімкніть його, а потім виберіть параметр **Стан (Status)**.

Примітка: Щоб побачити стан, мережний адаптер вашого ПК повинен бути приєднаний до комутатора чи аналогічного пристрою кабелем Ethernet. Багато бездротових маршрутизаторів мають вбудований невеликий 4-портовий Ethernet-комутатор. Ви можете під'єднатися до одного з його портів за допомогою прямого кабеля Ethernet.

b. У вікні Стан (Status) відображається інформація про ваше дротове з'єднання з локальною мережею.

c. Натисніть **Відомості (Details)**, щоб переглянути інформацію про адресу для вашого з'єднання з локальною мережею.

d. Відкрийте вікно Командного рядка та введіть **ipconfig /all**. Знайдіть інформацію про адаптер Ethernet та порівняйте її з інформацією, що відображається у вікні Інформації про мережне з'єднання (Network Connection Details).

```
C:\Users\ITE> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-VITJF61    Primary
Dns Suffix . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (4) I219-LM
   Physical Address. . . . . . . . . : 08-00-27-80-91-DB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d829:6d18:e229:a705%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.10 (Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, September 4, 2019 1:19:07 PM    Lease
Expires . . . . . . . . . . : Thursday, September 5, 2019 1:19:08 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 50855975
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-21-BA-64-08-00-27-80-91-DB
   DNS Servers . . . . . . . . . . . : 68.105.28.16
                                       68.105.29.16    NetBIOS over Tcpip.
. . . . . . . : Enabled
```

e. Закрийте всі вікна на Робочому столі.

Частина 2: Визначення піктограми мережі в системній панелі повідомлень (системний трей) та її використання

В Частині 2, ви будете використовувати піктограми мережі системній панелі повідомлень для визначення та управління NIC на вашому ПК.

Крок 1: Використовуйте піктограму мережі.

a. Знайдіть системну панель повідомлень (системний трей). Натисніть піктограму мережі, щоб побачити спливаюче вікно, в якому відображаються SSID, які знаходяться в межах доступу вашого бездротового NIC.

b. Натисніть **Мережа та Інтернет (Network and Internet)**.

c. У вікні налаштувань Settings під заголовком Змінити налаштування мережі (Change your network settings) натисніть **Змінити параметри адаптера (Change adapter settings)**.

d. У вікні Мережні з'єднання (Network Connections) натисніть правою кнопкою миші на **Wi-Fi** та виберіть **Вимкнути (Disable)**.

e. Перевірте системну панель повідомлень. Натисніть піктограму **Мережа (Network)** знову. Якщо вимкнено Wi-Fi, бездротові мережі тепер поза зоною дії і недоступні для бездротового з'єднання.

f. Ви також можете відключити мережу Ethernet, вимкнувши адаптери Ethernet.

Крок 2: Знайдіть піктограму Проблеми з мережею (Network Problem).

a. У вікні Мережні з'єднання (Network Connections) вимкніть усі адаптери **Wi-Fi** та **Ethernet**.

b. Тепер у системній панелі повідомлень відображається піктограма **Мережа відключена (Network Disabled)**, яка вказує на те, що з'єднання з мережею було вимкнене.

c. Ви можете натиснути на цей значок, щоб повернутися до налаштувань мережі та Інтернету.

d. У вікні налаштувань Мережі та Інтернету (Network and Internet) ви можете натиснути на опцію **Діагностики неполадок (Troubleshoot)**, щоб використати засоби ПК для вирішення проблеми з мережею.

e. Якщо при усуненні несправностей не було ввімкнено один із ваших NIC, слід зробити це вручну, щоб відновити мережне з'єднання вашого ПК.

Примітка: Якщо мережний адаптер увімкнено, а NIC не в змозі встановити мережне з'єднання, то в системній панелі повідомлень з’являється значок **Проблеми з мережею (Network Problem)**.

Якщо з'явиться така піктограма, ви можете вирішити цю проблему так само, як робили на Кроці 2c.

Питання для самоперевірки

Навіщо вам активувати більше одного мережного адаптера на ПК?

Лабораторна робота №7.2

Під'єднання дротової і бездротової локальної мережі

Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Під'єднується до
Cloud	Eth6	N/A	F0/0
	Coax7	N/A	Port0
Cable Modem	Port0	N/A	Coax7
	Port1	N/A	Internet
Router0	Console	N/A	RS232
	F0/0	192.168.2.1/24	Eth6
	F0/1	10.0.0.1/24	F0
	Ser0/0/0	172.31.0.1/24	Ser0/0
Router1	Ser0/0	172.31.0.2/24	Ser0/0/0
	F1/0	172.16.0.1/24	F0/1
WirelessRouter	Internet	192.168.2.2/24	Port 1
	Eth1	192.168.1.1	F0
Family PC	F0	192.168.1.102	Eth1
Switch	F0/1	172.16.0.2	F1/0
Netacad.pka	F0	10.0.0.254	F0/1
Configuration Terminal	RS232	N/A	Console

Цілі та задачі

Частина 1: Під'єднання до хмари Cloud

Частина 2: Під'єднання маршрутизатора Router0

Частина 3: Під'єднання решти пристроїв

Частина 4: Перевірка з'єднання

Частина 5: Вивчення фізичної топології

Довідкова інформація

При роботі в Packet Tracer (в умовах лабораторії або на підприємстві) слід знати, як підібрати відповідний кабель і як правильно під'єднувати пристрої.

В цій практичній роботі ми розглянемо налаштування пристроїв у Packet Tracer, вибір відповідного кабелю на основі конфігурації та під'єднання пристроїв. Також розглянемо фізичне представлення мережі в Packet Tracer.

Частина 1: Під'єднання до хмари Cloud

Крок 1: Під'єднайте хмару до Router0.

a. Унизу ліворуч натисніть значок помаранчевої блискавки, щоб відкрити доступні з'єднання **Connections**.

b. Виберіть правильний кабель для під'єднання **Router0 F0/0** до **Cloud Eth6**. **Cloud** - це тип комутатора, тому використовуйте з'єднання прямим мідним кабелем **Copper Straight-Through**. Якщо ви під'єднали правильний кабель, на кабелі загоряється індикатор зеленого кольору.

Крок 2: Під'єднайте хмару до кабельного модему Cable Modem.

Виберіть правильний кабель для з'єднання **Cloud Coax7** з **Modem Port0**.
Якщо ви під'єднали правильний кабель, на кабелі загоряється індикатор зеленого кольору.

Частина 2: Під'єднання маршрутизатора Router0

Крок 1: Під'єднайте Router0 до Router1.

Виберіть правильний кабель для під'єднання **Router0 Ser0/0/0** до **Router1 Ser0/0**. Використовуйте один з доступних послідовних кабелів **Serial**.
Якщо ви під'єднали правильний кабель, на кабелі загоряється індикатор зеленого кольору.

Крок 2: Під'єднайте Router0 до netacad.pka.

Виберіть правильний кабель для під'єднання **Router0 F0/1** до **netacad.pka F0**. Маршрутизатори і комп'ютери традиційно використовують однакові дроти для передачі (1 і 2) і прийому (3 і 6). У правильно обраного кабеля ці пари дротів перехрещені (міняються місцями). Хоча багато мережних адаптерів тепер можуть автовизначати, яка пара використовується для передачі і прийому, **Router0** і **netacad.pka** не мають автовизначення у NIC.
Якщо ви під'єднали правильний кабель, на кабелі загоряється індикатор зеленого кольору.

Крок 3: Під'єднайте Router0 до терміналу Configuration Terminal.

Виберіть правильний кабель для під'єднання **Router0 Console** до **Configuration Terminal RS232**. Цей кабель не забезпечує мережний доступ до **Configuration Terminal**, але дозволяє налаштувати **Router0** через його термінал.
Якщо ви під'єднали правильний кабель, на кабелі загоряється індикатор чорного кольору.

Частина 3: Під'єднання решти пристроїв

Крок 1: Під'єднайте Router1 до комутатора.

Виберіть правильний кабель для під'єднання **Router1 F1/0** до **Switch F0/1**.
Якщо ви під'єднали правильний кабель, на кабелі загоряється індикатор зеленого кольору. Зачекайте кілька секунд, щоб індикатор змінив колір з жовтого на зелений.

Крок 2: Під'єднайте Cable Modem до Wireless Router.

Виберіть правильний кабель для під'єднання **Cable Modem Port1** до **Wireless Router Internet**.
Якщо ви під'єднали правильний кабель, на кабелі загориться індикатор зеленого кольору.

Крок 3: Під'єднайте Wireless Router до FamilyPC.

Виберіть правильний кабель для під'єднання **Wireless Router Ethernet 1** до **Family PC**.
Якщо ви під'єднали правильний кабель, на кабелі загоряється індикатор зеленого кольору.

Частина 4: Перевірка з'єднання

Крок 1: Перевірте з'єднання Family PC з netacad.pka.

a. Відкрийте командний рядок на **Family PC** і надішліть запит ping на **netacad.pka**.

b. Відкрийте **Web Browser** і введіть веб-адресу **http://netacad.pka**.

Крок 2: Пропінгуйте Switch з Home PC.

Відкрийте командний рядок на **Home PC** і надішліть запит ping на IP-адресу **Switch**, щоб перевірити з'єднання.

Крок 3: Відкрийте Router0 з Configuration Terminal.

a. Відкрийте **Terminal** на **Configuration Terminal** і прийміть параметри за замовчуванням.

b. Натисніть **Enter**, щоб перейти у командний рядок **Router0** .

c. Введіть команду **show ip interface brief**, щоб переглянути стани інтерфейсів.

Частина 5: Вивчення фізичної топології

Крок 1: Перегляньте хмару Cloud.

a. Перейдіть на вкладку **Physical Workspace** або натискайте **Shift+P** і **Shift+L**, щоб переключатися між логічною і фізичною топологіями.

b. Натисніть значок **Home City**.

c. Натисніть значок **Cloud**.

Скільки дротів під'єднано до комутатора в синій стійці?

d. Натисніть кнопку **Back**, щоб повернутися до **Home City**.

Крок 2: Перегляньте первинну мережу PrimaryNetwork.

a. Натисніть значок **Primary Network**. Утримуйте курсор миші на різних кабелях.

Що знаходиться в таблиці праворуч від синьої стійки?

b. Натисніть кнопку **Back**, щоб повернутися до **Home City**.

Крок 3: Перегляньте вторинну мережу Secondary Network.

a. Натисніть значок **Secondary Network**. Утримуйте курсор миші на різних кабелях.

Чому до кожного пристрою під'єднано два помаранчевих кабелі?

b. Натисніть кнопку **Back**, щоб повернутися до **Home City**.

Крок 4: Перегляньте домашню мережу Home Network.

a. Натисніть значок **Home Network**.

Чому немає стійки для обладнання?

b. Перейдіть на вкладку **Logical Workspace**, щоб повернутися до логічної топології.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Микитишин А.Г. Комп'ютерні мережі. Книга 1.: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006». 2013. – 256 с.
2. Микитишин А.Г. Комп'ютерні мережі. Книга 2.: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів: «Магнолія 2006». 2013. – 328 с.
3. Микитишин А.Г. Телекомунікаційні системи та мережі / Микитишин А.Г., Митник М.М., Стухляк. П.Д. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 384 с.
4. Микитишин А.Г. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерно-інтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.
5. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1 / Буров Є.В., Митник М.М.; За заг. ред. Пасічника В.В. – Львів: «Магнолія 2006». 2019. – 334 с.
6. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: Підручник для вищих навчальних закладів. – К.: САММІТ-КНИГА, 2010. – 640 с.
7. ISO/IEC 11801 Information technology – Generic cabling for customer premises – Edition 2. 2.
8. EN 50173– Information Technology – Generic cabling systems.
9. TIA/EIA–568–C Commercial Building Telecommunications Cabling Standard.
10. ISO/IEC TR 14763–2. Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation.
11. ISO/IEC 14763–1 Information technology – Implementation and operation of customer premises cabling – Part 1: Administration.
12. Barry J Elliott Designing a structured cabling system to ISO 11801 2nd edition 2002, Published by Wood head Publishing Limited, Abington Hall, Abington Cambridge, England.