Міністерство освіти і науки України

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні вказівки до лабораторних занять
для здобувачів першого (бакалаврського) рівня вищої освіти
освітньої програми «Комп'ютерна інженерія «
галузь знані 12 Інформаційні технології
спеціальності 123 Комп'ютерна інженерія
денної та заочної форм навчання

Луцьк 2025

УДК 004.65(07)
Б17

Рекомендовано до видання вченою радою факультету КІТ ЛНТУ,
протокол № _____ від « _____ « _____ 20 25 року.

Голова вченої ради факультету КІТ _____ Інна КОНДІУС

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ

Директор бібліотеки _____ Наталія ПОЛІЩУК

Розглянуто і схвалено на засіданні кафедри комп'ютерної інженерії та безпеки ЛНТУ, протокол № _____ від « _____ « _____ 20 25 року.

Завідувач кафедри КІБ _____ Тарас ТЕРЛЕЦЬКИЙ

Укладач: _____ Наталія БАГНЮК, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ
_____ Катерина БОРТНИК, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

Рецензент: _____ Олександр РОЙКО, кандидат технічних наук, голова циклової комісії комп'ютерної та програмної інженерії відокремленого структурного підрозділу «Волинський фаховий коледж Національного університету харчових технологій»

Відповідальний за випуск: _____ Тарас ТЕРЛЕЦЬКИЙ, кандидат технічних наук, доцент кафедри комп'ютерної інженерії та безпеки ЛНТУ

К17 Комп'ютерні мережі: методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп'ютерна інженерія» галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія денної та заочної форм навчання / уклад. Н. В. Багнюк, К. Я. Бортник. Луцьк: ЛНТУ, 2025.118 с.

Методичне видання до лабораторних занять з дисципліни «Комп'ютерні мережі» складено відповідно до діючої програми курсу.

Призначене для здобувачів вищої освіти спеціальності 123 Комп'ютерна інженерія освітньої програми «Комп'ютерна інженерія».

ЗМІСТ

ВСТУП

Метою виконання лабораторних робіт є закріплення теоретичних знань та практичних навичок, набутих під час вивчення дисципліни «Комп'ютерні мережі», а також застосування їх при вирішенні прикладних завдань, пов'язаних із проєктуванням, налаштуванням і тестуванням мережевої інфраструктури.

У процесі виконання роботи здобувач вищої освіти повинен працювати з навчальною літературою, інструкціями до мережевого обладнання та програмними симуляторами, знаходити алгоритми вирішення технічних завдань і застосовувати їх для налаштування топологій, протоколів та мережевих сервісів.

Необхідне програмне забезпечення: Cisco Packet Tracer або його аналоги, інтерфейс командного рядка (CLI), засоби для трасування та діагностики мереж, утиліти TCP/IP.

Лабораторні роботи спрямовані на всебічне формування прикладних компетентностей у галузі мережевих технологій, які є базовими для підготовки фахівців з комп'ютерної інженерії.

Завдяки виконанню лабораторних завдань здобувачі вищої освіти мають змогу закріпити знання щодо основ побудови комп'ютерних мереж, ознайомитися з типами мережевих топологій, структурою та призначенням активного й пасивного мережевого обладнання, принципами функціонування мережевих протоколів та моделі OSI та TCP/IP. Особлива увага приділяється розвитку навичок конфігурування комутаторів і маршрутизаторів, реалізації протоколів маршрутизації (зокрема статичної та динамічної OSPF), організації логічного поділу мережі за допомогою VLAN, налаштуванню адресації за протоколами IPv4 та IPv6, використанню служб DHCP, NAT, а також створенню віртуальних приватних мереж (VPN) з метою підвищення безпеки передавання даних.

Виконання лабораторних робіт сприяє формуванню навичок роботи з інтерфейсом командного рядка мережевих пристроїв, аналізу таблиць маршрутизації, діагностики несправностей за допомогою утиліт ping, tracert, ipconfig, а також засвоєнню засобів резервного копіювання та збереження конфігурацій у NVRAM. Студенти вчаться грамотно документувати результати налаштувань, аналізувати структуру конфігураційних файлів і забезпечувати стабільну взаємодію між мережевими вузлами в різних середовищах.

Окрім технічних навичок, лабораторні заняття спрямовані на розвиток логічного та алгоритмічного мислення, уміння працювати з технічною документацією, застосовувати стандарти і протоколи у практичних умовах, приймати інженерні рішення щодо оптимального розгортання мережевої інфраструктури з урахуванням продуктивності, надійності, масштабованості та захищеності мережі.

При виконанні лабораторних робіт рекомендується використовувати академічні джерела, документацію Cisco, приклади конфігурацій, симуляційні сценарії, а також розглядати практичні кейси для кращого засвоєння матеріалу та підготовки до реальних умов професійної діяльності.

Лабораторна робота 1
Побудова мережі з двома сегментами

Мета роботи: ознайомити студентів з мережевим обладнанням, побудувати мережу з двома сегментами та перевірити її працездатність.

Завдання 1. Ознайомити студентів з мережевим обладнанням (викладач пояснює в аудиторіїі з використанням мережевого обладнання).

Завдання 2. У даному завданні необхідно з'єднати обладнання, як показано на схемі топології (рис. 1) та налаштувати пристрої у відповідності до схеми (рис. 3) [1].

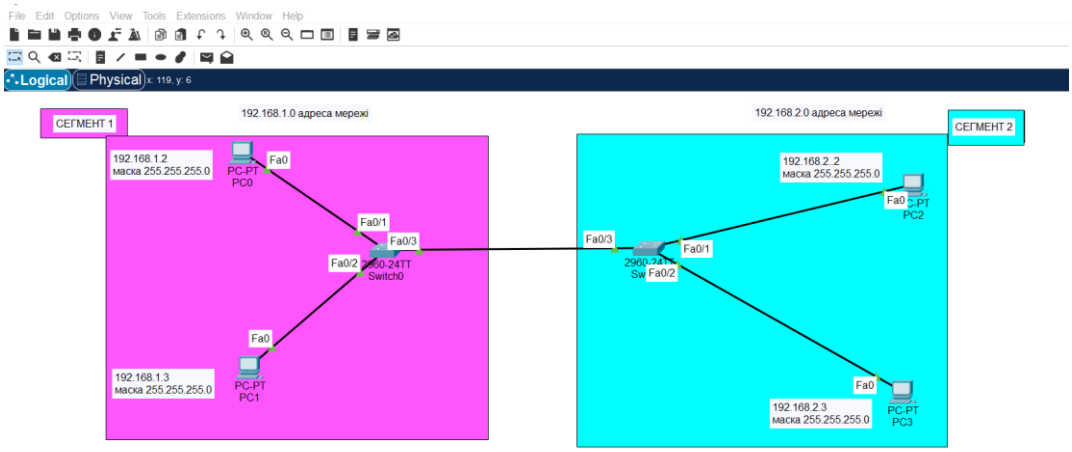


Рисунок 1 – Топологія мережі

Після збереження налаштувань, потрібно перевірити виконані конфігурації, протестувавши під'єднання до мережі:

– налаштування топології та ініціалізація пристроїв;

– налаштування пристроїв та перевірка з'єднання

– зберегти конфігурацію в енергонезалежну пам'ять NVRAM (це комп'ютерна пам'ять, яка може зберігати інформацію при відсутності живлення) в превілейованому режимі командами **#write memory** (або скорочено **#wr m**) або **#copy running-config startup-config** (або скорочено **#cop run st**).

Примітка. Також використовувати дані команди для збереження конфігурації при виконанні всіх лабораторних робіт в курсі.

Для позначення підмереж на схемі в Packet Tracer різними кольорами (рис. 2), використати піктограму  або  .

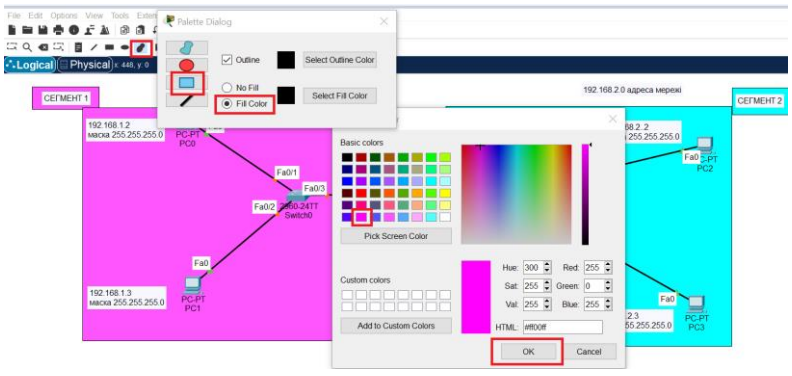


Рисунок 2 – Створення кольорових областей

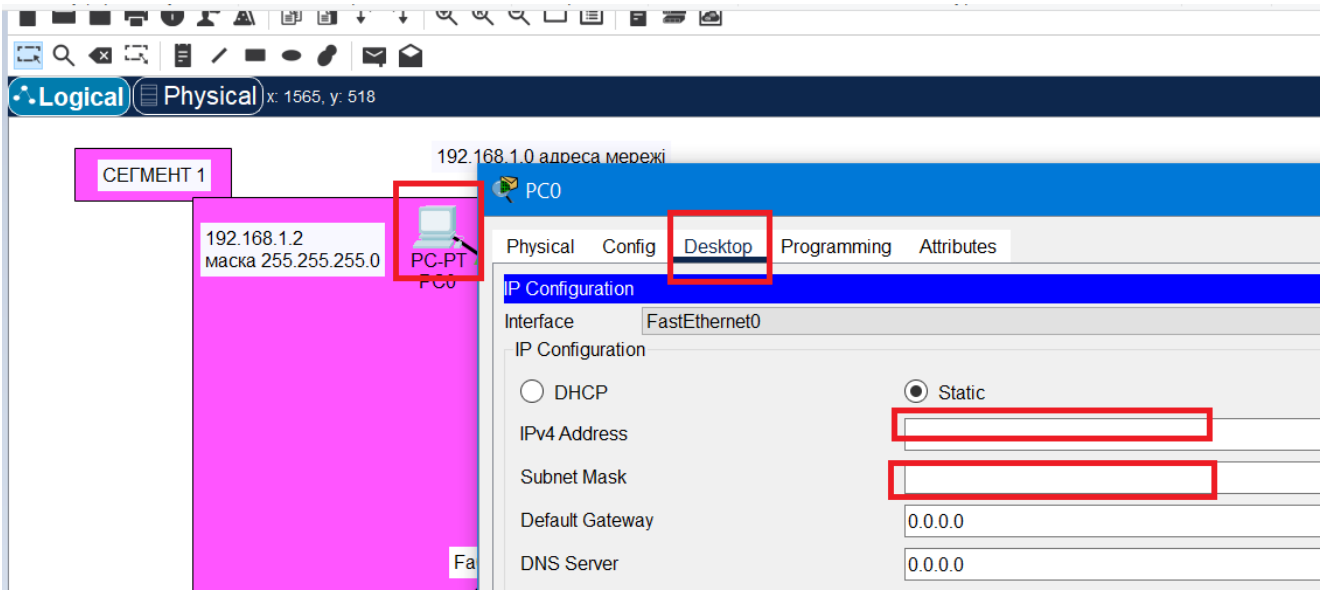


Рисунок 3 – Налаштування статичної IP-адреси на комп'ютері

Хід роботи

1. Завдання виконати згідно варіанту (обрати IP-адреси підмереж згідно варіанту), поданому в таблиці 1. Маска підмереж 255.255.255.0 (/24). З'єднайте пристрої у мережу, як показано на топології (рис. 1).

2. Налаштування пристроїв та перевірка з'єднання: призначте **статичні** IP-адреси для інтерфейсів ПК:

– налаштуйте IP-адресу та маску підмережі на PC-0 192.168.1.2, маска підмережі 255.255.255.0;

– налаштуйте IP-адресу та маску підмережі на PC-1 192.168.1.3, маска підмережі 255.255.255.0;

– налаштуйте IP-адресу та маску підмережі на PC-2 192.168.2.2, маска підмережі 255.255.255.0;

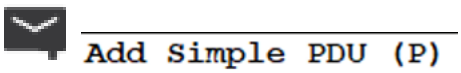
– налаштуйте IP-адресу та маску підмережі на PC-3 192.168.2.3, маска підмережі 255.255.255.0.

3. Пропінгуйте PC-0 з режиму командного рядка на PC-1. Чому запит ping був вдалим або невдалим?

4. Пропінгуйте PC-2 з режиму командного рядка на PC-3. Чому запит ping був вдалим або невдалим?

5. Пропінгуйте PC-0 з режиму командного рядка на PC-3. Чому запит ping був вдалим або невдалим?

6. На PC-3 змініть адресу на 192.168.1.4, маска підмережі 255.255.255.0 та пропінгуйте PC-3 та PC-0. Чому запит ping був вдалим або невдалим?

Примітка. В подальшому можна використовувати для команди ping піктограму на панелі інструментів 

(рис. 4).

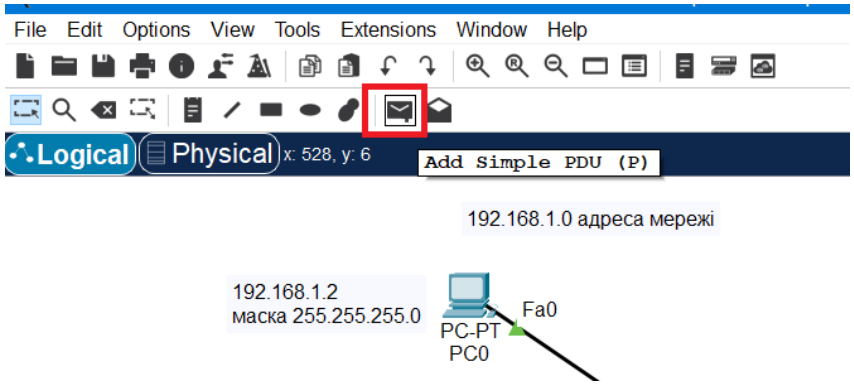


Рисунок 4 – Команда ping

Індивідуальне завдання

1. З'єднайте пристрої у мережу, як показано на топології (рис. 1) [1].
2. Налаштування пристроїв та перевірка з'єднання: призначте **статичні** IP-адреси для інтерфейсів ПК:

– налаштуйте IP-адресу та маску підмережі на PC-0 ***адреса мережі згідно варіанту (СЕГМЕНТ 1)***.2, маска підмережі 255.255.255.0;

– налаштуйте IP-адресу та маску підмережі на PC-1 ***адреса мережі згідно варіанту(СЕГМЕНТ 1)***.3, маска підмережі 255.255.255.0;

– налаштуйте IP-адресу та маску підмережі на PC-2 ***адреса мережі згідно варіанту(СЕГМЕНТ 2)***.2, маска підмережі 255.255.255.0;

– налаштуйте IP-адресу та маску підмережі на PC-3 ***адреса мережі згідно варіанту(СЕГМЕНТ 2)***.3, маска підмережі 255.255.255.0.

3. Пропінгуйте PC-0 з режиму командного рядка на PC-1.

Чому запит ping був вдалим або невдалим?

4. Пропінгуйте PC-2 з режиму командного рядка на PC-3.

Чому запит ping був вдалим або невдалим?

5. Пропінгуйте PC-0 з режиму командного рядка на PC-3.

Чому запит ping був вдалим або невдалим?

6. На PC-3 змініть адресу на ***адреса мережі згідно варіанту(СЕГМЕНТ 1)***.4, маска підмережі 255.255.255.0 та пропінгуйте PC-3 та PC-0.
7. Чому запит ping був вдалим або невдалим?
8. Звіт по роботі оформити в вигляді скрінів з описом та відповідями на питання.

Варіант завдання

Таблиця 1 – Варіанти завдань

Номер варіанту	Мережева адреса сегменту 1, маска /24	Мережева адреса сегменту 2, маска /24
1.	192.168.3.0	192.168.4.0
2.	192.168.5.0	192.168.6.0
3.	192.168.7.0	192.168.8.0
4.	192.168.9.0	192.168.10.0
5.	192.168.11.0	192.168.12.0
6.	192.168.13.0	192.168.14.0
7.	192.168.15.0	192.168.16.0

Продовження таблиці 1

Номер варіанту	Мережева адреса сегменту 1	Мережева адреса сегменту 2
8.	192.168.17.0	192.168.18.0
9.	192.168.19.0	192.168.20.0
10.	192.168.21.0	192.168.22.0
11.	192.168.23.0	192.168.24.0
12.	192.168.25.0	192.168.26.0
13.	192.168.27.0	192.168.28.0
14.	192.168.29.0	192.168.30.0
15.	192.168.31.0	192.168.32.0
16.	192.168.33.0	192.168.34.0
17.	192.168.35.0	192.168.36.0
18.	192.168.37.0	192.168.38.0
19.	192.168.39.0	192.168.40.0
20.	192.168.41.0	192.168.42.0
21.	192.168.43.0	192.168.44.0
22.	192.168.45.0	192.168.46.0
23.	192.168.47.0	192.168.48.0
24.	192.168.49.0	192.168.50.0
25.	192.168.51.0	192.168.52.0
26.	192.168.53.0	192.168.54.0
27.	192.168.55.0	192.168.56.0
28.	192.168.57.0	192.168.58.0
29.	192.168.59.0	192.168.60.0
30.	192.168.61.0	192.168.62.0
31.	192.168.63.0	192.168.64.0
32.	192.168.65.0	192.168.66.0
33.	192.168.67.0	192.168.68.0
34.	192.168.69.0	192.168.70.0
35.	192.168.71.0	192.168.72.0
36.	192.168.73.0	192.168.74.0
37.	192.168.75.0	192.168.76.0
38.	192.168.77.0	192.168.78.0
39.	192.168.79.0	192.168.80.0
40.	192.168.81.0	192.168.82.0
41.	192.168.83.0	192.168.84.0
42.	192.168.85.0	192.168.86.0
43.	192.168.87.0	192.168.88.0
44.	192.168.89.0	192.168.90.0
45.	192.168.91.0	192.168.92.0
46.	192.168.93.0	192.168.94.0
47.	192.168.95.0	192.168.96.0
48.	192.168.97.0	192.168.98.0
49.	192.168.99.0	192.168.100.0
50.	192.168.101.0	192.168.102.0
51.	192.168.103.0	192.168.104.0
52.	192.168.105.0	192.168.106.0
53.	192.168.107.0	192.168.108.0
54.	192.168.109.0	192.168.110.0
55.	192.168.111.0	192.168.112.0

Продовження таблиці 1

Номер варіанту	Мережева адреса сегменту 1	Мережева адреса сегменту 2
56.	192.168.113.0	192.168.114.0
57.	192.168.115.0	192.168.116.0
58.	192.168.117.0	192.168.118.0
59.	192.168.119.0	192.168.120.0
60.	192.168.121.0	192.168.122.0
61.	192.168.123.0	192.168.124.0
62.	192.168.125.0	192.168.126.0
63.	192.168.127.0	192.168.128.0
64.	192.168.129.0	192.168.130.0

Примітка. Комбінація клавіш **Ctrl Shift 6** − дозволяє користувачеві перервати процес IOS, наприклад, ping або traceroute.

Лабораторна робота 2
Налаштування початкових параметрів комутатора на прикладі комутатора Cisco Catalyst 2960

Мета роботи: навчитися здійснювати базові налаштування комутатора.

Завдання: перевірити конфігурацію комутатора за замовчуванням та налаштувати його базові параметри.

Хід роботи

1. Увійти в привілейований режим EXEC [2].

Можна отримати доступ до всіх команд комутатора з привілейованого режиму EXEC. Однак, оскільки багато команд привілейованого режиму налаштовують поточні параметри, привілейований доступ повинен бути захищений паролем, щоб запобігти несанкціонованому використанню. Набір команд привілейованого режиму EXEC включає в себе команди, доступні в користувацькому режимі EXEC, безліч додаткових команд і команду configure, за допомогою якої забезпечується доступ до режимів конфігурації (рис. 1).

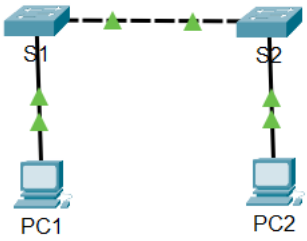


Рисунок 1 – Топологія мережі

2. Натиснути на схемі (схема додається викладачем) на S1 і перейти на вкладку CLI (інтерфейс командного рядка).

3. Натиснути Enter.

4. Увійдіть у привілейований режим EXEC, використовуючи команду enable:

Switch> enable
Switch#

Зверніть увагу, що змінився вигляд командного рядка, щоб відобразити привілейований режим EXEC.

5. Дослідіть поточну конфігурацію комутатора, ввівши команду show running-config.

Switch# show running-config

Дайте відповідь на наступні запитання: скільки інтерфейсів Fast Ethernet має комутатор, скільки інтерфейсів Gigabit Ethernet має комутатор, який діапазон значень показано для ліній vty, яка команда відображає поточний вміст енергонезалежної оперативної пам’яті (NVRAM), чому комутатор відповідає повідомленням “startup-config is not present?”

Налаштування основних параметрів комутатора

6. Призначте комутатору ім’я.

Для налаштування параметрів комутатора може знадобитися переходити між різними режимами конфігурації. Зверніть увагу, як змінюється вигляд командного рядка при переході між режимами командного рядка комутатора.

Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit
S1#

7. Забезпечте безпечний доступ до консолі.

Для безпечного доступу до консолі перейдіть в режим config-line і встановіть для консолі пароль **letmein**.

S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# line console 0
S1(config-line)# password letmein
S1(config-line)# login
S1(config-line)# exit
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#

Дайте відповідь на питання. Для чого потрібна команда login?

8. Переконайтеся, що доступ до консолі захищений.

Вийдіть з привілейованого режиму, щоб переконатися, що для консольного порту встановлено пароль.

S1# exit
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>

Примітка: Якщо комутатор не виводить запит на введення пароля, значить, ви не налаштували параметр login.

9. Забезпечте безпечний доступ до привілейованого режиму.

Встановіть для enable пароль **c1$c0**. Цей пароль обмежує доступ до привілейованого режиму.

Примітка: Символ 0 в c1$c0 - це нуль, а не велика літера «O». Налаштування пароля буде оцінено як виконане успішно тільки після того, як ви зашифруєте його в наступних кроках.

S1> enable
S1# configure terminal
S1(config)# enable password c1$c0
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#

10. Переконайтеся, що доступ до привілейованого режиму захищений.

Виконайте команду exit ще раз, щоб вийти з комутатора. Натисніть <Enter>, після чого вам буде запропоновано ввести пароль.

User Access Verification
Password:

Перший пароль − це пароль для консолі, який був заданий для line con 0. Введіть цей пароль, щоб повернутися в користувацький режим EXEC.

Введіть команду для доступу до привілейованого режиму.

Введіть другий пароль, який був заданий для обмеження доступу до привілейованого режиму EXEC.

Перевірте конфігурацію, переглянувши вміст файлу running-configuration:

S1# show running-config

Зверніть увагу, що паролі для консолі і привілейованого режиму відображаються у вигляді звичайного тексту. Це може становити загрозу безпеці, якщо хтось підглядає через ваше плече або отримує доступ до файлів конфігурації, що зберігаються в резервному сховищі.

11. Налаштуйте зашифрований пароль для доступу до привілейованого режиму.

Пароль Enable password потрібно замінити на новий зашифрований пароль за допомогою команди enable secret . Встановіть з enable secret пароль itsasecret.

S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
S1#

Примітка: Пароль enable secret має пріоритет перед паролем enable. Якщо для комутатора задані обидва паролі, потрібно ввести пароль enable secret для переходу в привілейований режим EXEC.

12. Переконайтеся в тому, що пароль enable secret додано в файл конфігурації.

Введіть команду show running-config ще раз, щоб перевірити, чи налаштовано новий пароль enable secret.

Примітка: Команду show running-config можна скоротити до

S1# show run

Дайте відповідь на питання. Що відображається в якості пароля enable secret? Чому пароль enable secret відображається не так, як було задано?

13. Зашифруйте паролі enable і console.

В попередніх налаштуваннях видно, що пароль enable secret зашифрований, а паролі enable та console зберігаються у вигляді звичайного тексту. Зашифруйте ці відкриті паролі за допомогою команди service password-encryption.

S1# config t
S1(config)# service password-encryption
S1(config)# exit

Дайте відповідь на питання. Якщо встановити на комутаторі інші паролі, вони будуть зберігатися в файлі конфігурації у вигляді звичайного тексту чи в зашифрованому вигляді? Поясніть.

14. Налаштуйте банер MOTD (повідомлення дня).

У набір команд Cisco IOS входить команда, що дозволяє налаштувати повідомлення, яке бачитимуть всі, хто входить в систему на комутаторі. Це повідомлення називається повідомленням дня або банером MOTD (Message Of The Day). Текст банера потрібно обмежити подвійними лапками або використовувати роздільник, відмінний від будь-якого символу в рядку MOTD.

S1# config t
S1(config)# banner motd "This is a secure system. Authorized Access Only!"
S1(config)# exit
%SYS-5-CONFIG_I: Configured from console by console
S1#

Дайте відповідь на питання. Коли буде відображатися цей банер? Навіщо на всіх комутаторах потрібно налаштувати банер MOTD?

15. Збереження файлів конфігурації в NVRAM

Перевірте правильність конфігурації за допомогою команди show run.

Збережіть файл конфігурації. Ви завершили основне налаштування комутатора. Тепер зробіть резервну копію файлу поточної конфігурації в NVRAM, щоб переконатися, що внесені зміни не втратяться при перезавантаженні системи або втраті живлення.

S1# copy running-config startup-config
Destination filename [startup-config]?[Enter]
Building configuration...
[OK]

Примітка. Також для збереження поточної конфігурації пристрою в постійну пам’ять (NVRAM) можна використовувати команду **write memory** або

її скорочену версію **wr m**. Аналогічно можна використовувати скорочену версію команди copy running-config startup-config − **cop r s.**

Дайте відповідь на питання. Дослідіть файл стартової конфігурації. Яка команда відображає вміст NVRAM? Чи всі внесені зміни були записані у файл?

16. Налаштування комутатора S2

Налаштуйте для комутатора S2 наступні параметри:

- ім’я пристрою: S2;
- захистіть доступ до консолі паролем letmein;
- встановіть в якості пароля enable password c1$c0 , а в якості пароля enable secret - itsasecret;
- налаштуйте відповідне повідомлення для тих, хто під'єднується до комутатора;
- зашифруйте всі відкриті паролі;
- переконайтесь, що конфігурація правильна;
- збережіть файл конфігурації, щоб не втратити її у випадку відключення живлення комутатора.крийте вікно конфігурації для S2

Лабораторна робота 3
Обчислення підмереж IPv4

Мета роботи: закріплення знань щодо визначення IP-адреси мережі на основі заданої IP-адреси та маски підмережі.

Заповніть наведені нижче таблиці відповідями про задану IPv4-адресу вузла, вихідну та нову маски підмережі [2].

Завдання 1.

Дано:	
IP-адреса вузла:	192.168.200.139
Вихідна маска підмережі:	255.255.255.0
Нова маска підмережі:	255.255.255.224

Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	
IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Завдання 2.

Дано:	
IP-адреса вузла:	10.101.99.228
Вихідна маска підмережі:	255.0.0.0
Нова маска підмережі:	255.255.128.0

Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	

IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Завдання 3.

Дано:	
IP-адреса вузла:	172.22.32.12
Вихідна маска підмережі:	255.255.0.0
Нова маска підмережі:	255.255.224.0

Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	
IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Завдання 4.

Дано:	
IP-адреса вузла:	192.168.1.245
Вихідна маска підмережі:	255.255.255.0
Нова маска підмережі:	255.255.255.252

Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	
IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Завдання 5.

Дано:	
IP-адреса вузла:	128.107.0.55
Вихідна маска підмережі:	255.255.0.0
Нова маска підмережі:	255.255.255.0

Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	
IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Завдання 6.

Дано:	
IP-адреса вузла:	192.135.250.180
Вихідна маска підмережі:	255.255.255.0
Нова маска підмережі:	255.255.255.248

Знайти:	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	
Мережна адреса цієї підмережі	
IPv4-адреса першого вузла в цій підмережі	
IPv4-адреса останнього вузла в цій підмережі	
Широкомовна IPv4-адреса цієї підмережі	

Дайте відповідь на запитання. Дайте характеристику маски підмережі. Чому маска підмережі так важлива при аналізі IPv4-адреси?

Лабораторна робота 4
Розподіл мережі на підмережі

Мета роботи: розподілити мережу на декілька підмереж та налаштувати обмін даними між підмережами.

Завдання. Розподілити мережу на декілька підмереж. Варіант завдання дивитись нижче в таблиці 2. В кожній підмережі має бути два комп'ютери. Вихідна маска підмережі 255.255.255.0 (/24). Нову маску підмережі визначити з врахуванням завдання. Маршрутизатор назвати Вашим ***прізвищем*** в налаштуваннях та на схемі.

1. Виконати адресацію мережі та внести дані в таблицю 1 згідно виданого варіанту.

Таблиця 1 – Адресація мережі

Вихідна маска підмережі в десятковому форматі	255.255.255.0
Вихідна маска підмережі в десятковому форматі	/24
Написати варіант згідно таблиці 2	***Написати IP-адресу та кількість підмереж згідно завдання в таблиці 2***
Нова маска підмережі в десятковому форматі	
Нова маска підмережі в префіксному форматі	
Кількість бітів у підмережі	
Кількість створених підмереж	
Кількість вузлових бітів у підмережі	
Кількість вузлів у підмережі	

Номер підмережі	Адреса підмережі	Діапазон усіх IP адрес	Перша IP хоста	Остання IP хоста	Широкомовна адреса	Шлюз за замовчуванням
1						
2						
….						
n						

де n – це кількість підмереж.

2. Відобразити назви інтерфейсів: меню Options → Preferences → поставити галочку ☑ Always Show Port Labels in Logical Workspace (рис. 1).

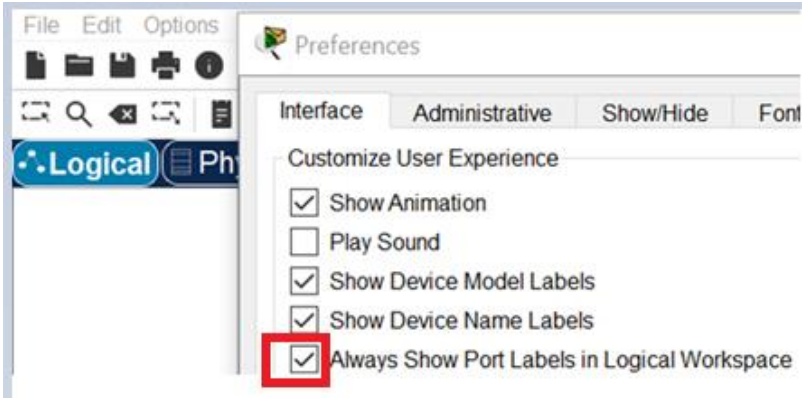


Рисунок 1 – Відображення назви інтерфейсів

3. Спроєктувати мережу згідно завдання. На схемі в Packet Tracer до всіх підмереж в текстовому полі  зазначити адресу мережі, діапазон хостових адрес, шлюз за замовчування, широкомовну адресу та маску мережі в десятковому та префіксному вигляді. Орієнтовний приклад мережі дивіться на рисунках 3, 4.

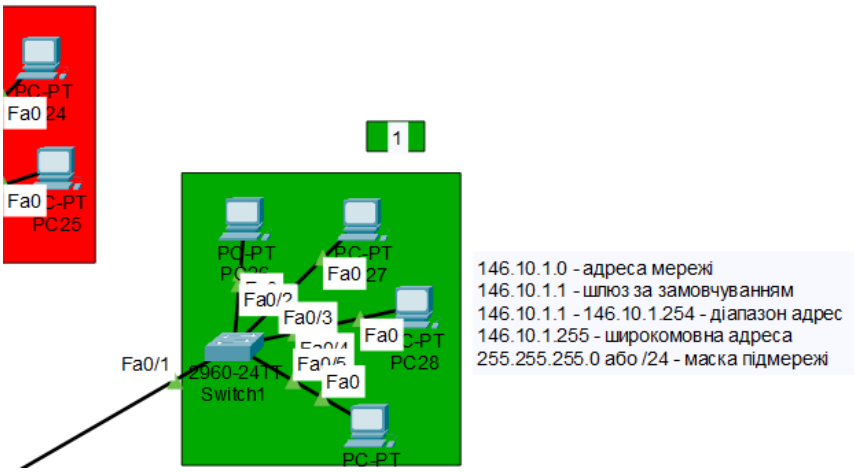


Рисунок 2 – Вигляд схеми підмережі в Packet Tracer (в текстовому полі зазначити адресу мережі, діапазон хостових адрес, шлюз за замовчування, широкомовну адресу та маску мережі)

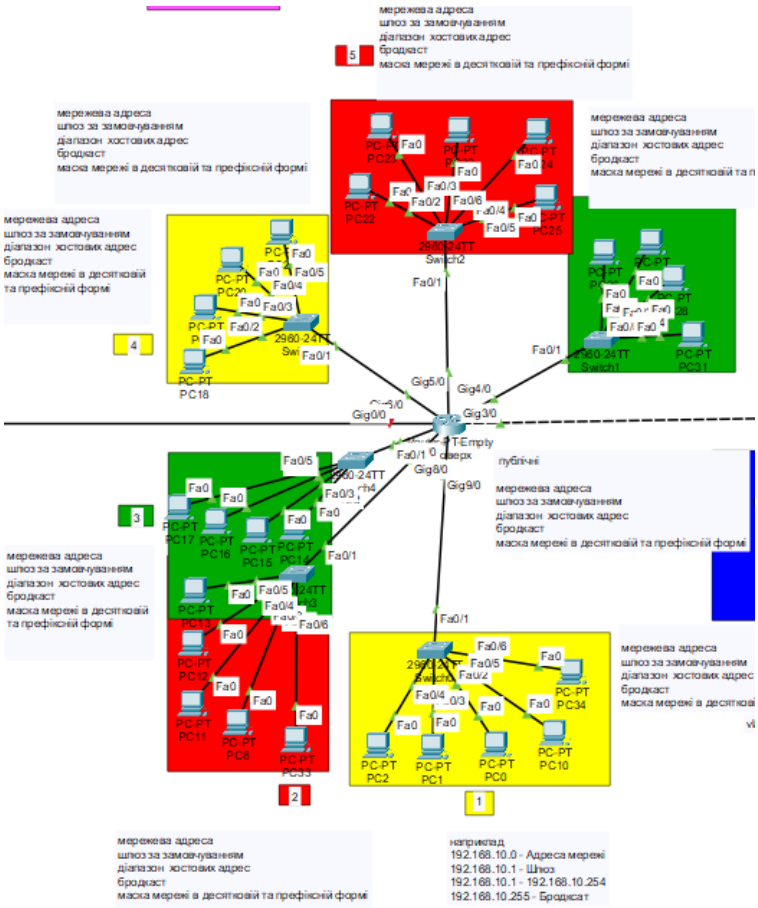


Рисунок 3 – Загальний вигляд схеми підмережі в Packet Tracer (в текстовому полі зазначити адресу мережі, діапазон адрес, шлюз за замовчування, широкомовну адресу та маску мережі)

4. Всі підмережі позначити на схемі в Packet Tracer різними кольорами (рисунок 2, 3, 4), використавши для цього піктограму (рис. 4) та назвати в текстовому полі (рис. 4) (М1 – мережа 1, М2 – мережа 2 і т.д.).

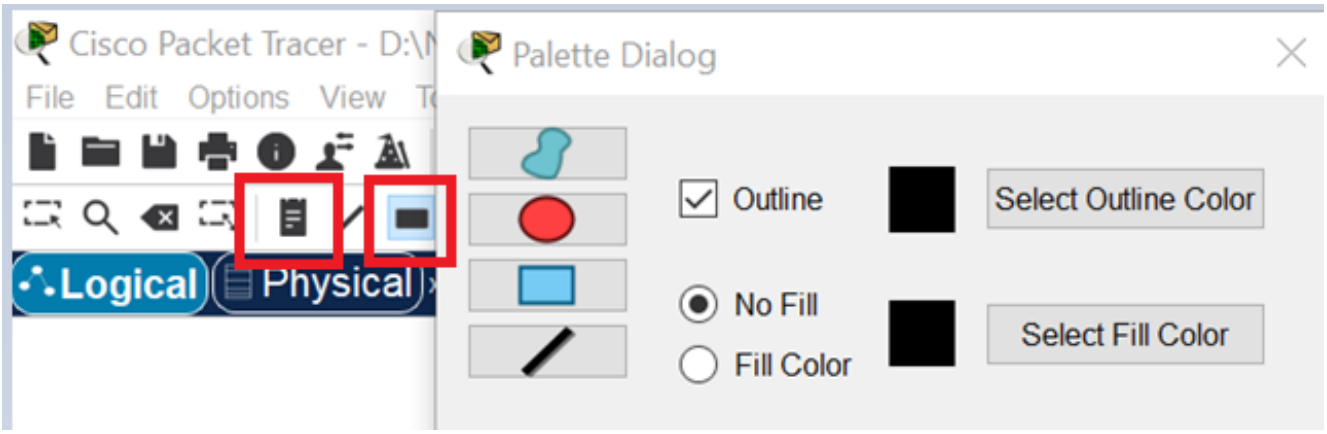


Рисунок 4 – Створення кольорових областей

5. Налаштувати IP-адреси на інтерфейсах маршрутизатора та ввімкнути їх (рис. 5). Обрати для шлюза за замовчуванням **першу** хостову адресу в мережі:

```
Router(config)# interface type-and-number
Router(config-if)# description description-text
Router(config-if)# ip address ipv4-address subnet-mask
Router(config-if)# no shutdown
```

Рисунок 5 – Команди для налаштування IP-адреси на інтерфейсах маршрутизатора [2]

6. На комп'ютерах налаштувати IP-адреси статично.

7. Зберегти конфігурацію на маршрутизаторі в енергонезалежну пам'ять NVRAM (це комп'ютерна пам'ять, яка може зберігати інформацію при відсутності живлення) в превілейованому режимі командами **#write memory** (або скорочено **#wr m**) або **#copy running-config startup-config** (або скорочено **#cop run st**).

Примітка. Також використовувати дані команди для збереження конфігурації при виконанні всіх лабораторних робіт в курсі.

8. Пропінгувати всі сегменти з режиму командного рядка та додати скріни в звіт з лабораторної роботи. Для звіту підготувати файл в ворді та Packet Tracer.

Варіанти завдання

Таблиця 2 – Варіанти завдань

Варіант	Мережева адреса	Кількість підмереж	Варіант	Мережева адреса	Кількість підмереж
1.	192.168.3.0	4	33	192.168.4.0	4
2.	192.168.5.0	5	34	192.168.6.0	5
3.	192.168.7.0	6	35	192.168.8.0	6
4.	192.168.9.0	7	36	192.168.10.0	7
5.	192.168.11.0	4	37	192.168.12.0	4

Продовження таблиці 2

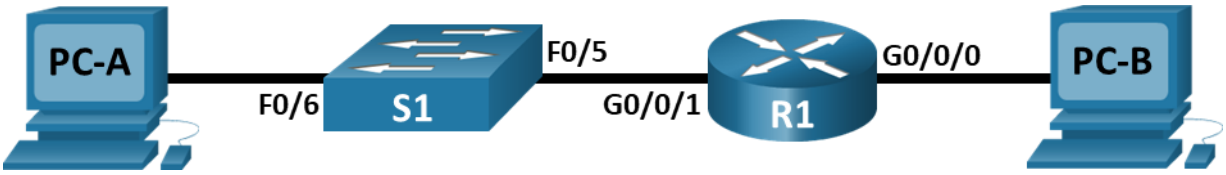
Варіант	Мережева адреса	Кількість підмереж	Варіант	Мережева адреса	Кількість підмереж
6.	192.168.13.0	5	38	192.168.14.0	5
7.	192.168.15.0	6	39	192.168.16.0	6
8.	192.168.17.0	7	40	192.168.18.0	7
9.	192.168.19.0	4	41	192.168.20.0	4
10.	192.168.21.0	5	42	192.168.22.0	5
11.	192.168.23.0	6	43	192.168.24.0	6
12.	192.168.25.0	7	44	192.168.26.0	7
13.	192.168.27.0	4	45	192.168.28.0	4
14.	192.168.29.0	5	46	192.168.30.0	5
15.	192.168.31.0	6	47	192.168.32.0	6
16.	192.168.33.0	7	48	192.168.34.0	7
17.	192.168.35.0	4	49	192.168.36.0	4
18.	192.168.37.0	5	50	192.168.38.0	5
19.	192.168.39.0	6	51	192.168.40.0	6
20.	192.168.41.0	7	52	192.168.42.0	7
21.	192.168.43.0	4	53	192.168.44.0	4
22.	192.168.45.0	5	54	192.168.46.0	5
23.	192.168.47.0	6	55	192.168.48.0	6
24.	192.168.49.0	7	56	192.168.50.0	7
25.	192.168.51.0	4	57	192.168.52.0	4
26.	192.168.53.0	5	58	192.168.54.0	5
27.	192.168.55.0	6	59	192.168.56.0	6
28.	192.168.57.0	7	60	192.168.58.0	7
29.	192.168.59.0	4	61	192.168.60.0	4
30.	192.168.61.0	5	62	192.168.62.0	5
31.	192.168.63.0	6	63	192.168.64.0	6
32.	192.168.65.0	7	64	192.168.66.0	7

Лабораторна робота 5
Побудова мережі з комутатором і маршрутизатором на базі обладнання Cisco

Мета роботи: навчити студентів налаштовувати мережу на прикладі обладнання Cisco

Завдання: налаштувати топології, ініціалізацію пристроїв та перевірити з'єднання.

Топологія



Таблиця адресації

Пристрій	Інтерфейс	IP-адреса / Префікс	Шлюз за замовчуванням
R1	G0/0/0	192.168.0.1 /24	N/A
		2001:db8:acad::1/64	
		fe80::1	
	G0/0/1	192.168.1.1 /24	N/A
		200:db8:acad:1::1/64	
		fe80::1	
S1	VLAN 1	192.168.1.2 /24	192.168.1.1
PC-A	NIC	192.168.1.3 /24	192.168.1.1
		2001:db8:acad:1::3/64	fe80::1
PC-B	NIC	192.168.0.3 /24	192.168.0.1
		2001:db8:acad::3/64	fe80::1

Примітка. Маршрутизатори, що використовуються − це Cisco 4321 [2].

У цьому завданні необхідно з'єднати обладнання, як показано на схемі топології. Потім потрібно налаштувати пристрої у відповідності до таблиці адресації. Після збереження налаштувань, перевірити виконані конфігурації, протестувавши під'єднання до мережі.

Після налаштування пристроїв та перевірки під'єднання до мережі скористатись командами IOS для отримання інформації від пристроїв, щоб відповісти на запитання щодо мережевого обладнання.

Шаблон **default bias**, який використовується за замовчуванням в диспетчері баз даних комутатора (SDM, Switch Database Manager), не забезпечує підтримки для IPv6-адрес. Переконайтеся, що SDM використовує

шаблон **dual-ipv4-and-ipv6** або шаблон **lanbase-routing**. Новий шаблон буде застосований після перезавантаження, навіть якщо конфігурація не збережена.

S1# show sdm prefer

Використовуйте наведені нижче команди, щоб призначити **dual-ipv4-ipv6** як шаблон SDM за замовчуванням.

S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload

Хід роботи

1. Налаштувати топології та ініціалізацію пристроїв.

2. З'єднайте пристрої у мережу, як показано на топології. Приєднайте пристрої, показані на схемі топології.

3. Налаштування пристроїв та перевірка з'єднання. Зверніться до **Топології** та **Таблиці адресації** на початку цієї лабораторної роботи, щоб отримати інформацію про назви пристроїв та адреси.

4. Призначте статичну IP-адресу для інтерфейсів ПК. Налаштуйте IP-адресу, маску підмережі та параметри шлюзу за замовчуванням на PC-A та PC-B. Пропінгуйте PC-B з режиму командного рядка на PC-A. Результати відобразіть в вигляді скріна.

Дайте відповідь на запитання. Чому запит ping був невдалим?

5. Налаштуйте маршрутизатор. Під'єднайтесь до консольного порту, налаштуйте консольне з'єднання із маршрутизатором і увійдіть в привілейований режим EXEC.

Router> enable

Увійдіть у режим конфігурації.

Router# config terminal

Призначте маршрутизатору ім'я.

Router(config)# hostname R1

Вимкніть пошук DNS, щоб упередити маршрутизатор від спроби перетворення неправильно введених команд:

R1(config)# no ip domain lookup

Призначте **class** як зашифрований пароль привілейованого режиму EXEC.

R1(config)# enable secret class

Призначте **cisco** як пароль доступу до консолі і активуйте авторизацію.

R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login

Призначте **cisco** як пароль для віртуальних ліній і активуйте авторизацію.

R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login

Зашифруйте всі відкриті текстові паролі.

R1(config)# service password-encryption

Створіть банер, який попереджатиме всіх, хто має доступ до пристрою, про те, що несанкціонований доступ заборонено.

R1(config)# banner motd $ Authorized Users Only! $

Налаштуйте і активуйте обидва інтерфейси на маршрутизаторі.

R1(config)# interface g0/0/0
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad::1/64
R1(config-if)# ipv6 address FE80::1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface g0/0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit

Налаштуйте опис інтерфейсу, що для кожного інтерфейсу зазначає пристрій, який до нього під'єднаний.

R1(config)# interface g0/0/1
R1(config-if)# description Connected to F0/5 on S1
R1(config-if)# exit
R1(config)# interface g0/0/0
R1(config-if)# description Connected to Host PC-B
R1(config-if)# exit

Для увімкнення маршрутизації IPv6, введіть команду ipv6 unicast- routing.

R1(config)# **ipv6 unicast-routing**

Збережіть поточну конфігурацію у файл стартової конфігурації.

R1(config)# exit
R1# copy running-config startup-config

Встановіть годинник на маршрутизаторі.

R1# clock set 15:30:00 27 Aug 2025

Примітка: Використовуйте знак питання (**?**), щоб отримати підказку з правильною послідовністю параметрів, необхідних для виконання цієї команди.

6. Пропінгуйте PC-B з режиму командного рядка на PC-A. Відобразіть результат в вигляді скріна.

Дайте відповідь на запитання. Чи було пінгування вдалим? Поясніть.

7. Налаштуйте комутатор.На цьому кроці ви налаштуєте ім'я хоста, інтерфейс VLAN 1 і його шлюз за замовчуванням. Під'єднайте комутатор через консольний кабель і увійдіть в привілейований режим EXEC.

Switch> enable

Увійдіть в режим конфігурації.

Switch# configure terminal

Призначте комутатору ім'я.

Switch(config)# hostname S1

Вимкніть пошук DNS, щоб упередити маршрутизатор від спроби перетворення неправильно введених команд.

S1(config)# no ip domain-lookup

Налаштуйте і активуйте інтерфейс VLAN на комутаторі S1.

S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit

Налаштуйте шлюз за замовчуванням для комутатора S1.

S1(config)# ip default-gateway 192.168.1.1
S1(config-if)# exit

Збережіть поточну конфігурацію у файл стартової конфігурації.

8. Перевірте наскрізне з'єднання. З PC-A надішліть запит ping на PC-B. З S1 надішліть запит ping на PC-B. Усі запити ping повинні бути успішними. Відобразіть результа в роботі в вигляді скрінів.

9. Відображення інформації про пристрій. Використайте команди **show** для отримання інформації про інтерфейс і маршрутизацію від маршрутизатора і комутатора.

10. Відобразіть таблицю маршрутизації маршрутизатора. Введіть команду **show ip route** на маршрутизаторі R1, щоб відповісти на подальші запитання.

R1# show ip route

Дайте відповіді на запитання. Який код використовується в таблиці маршрутизації для позначення безпосередньо під'єднаної мережі? Скільки записів про маршрути в таблиці маршрутизації мають код C? Які типи інтерфейсів пов'язані з маршрутами, що мають код C?

11. Введіть команду **show ipv6 route** на маршрутизаторі R1 для відображення маршрутів IPv6.

R1# show ipv6 route

12. Відобразіть інформацію про інтерфейс на маршрутизаторі R1.

Введіть команду **show ip interface g0/0/1**, щоб відповісти на подальші запитання.

R1# show ip interface g0/0/1

Дайте відповіді на запитання. Який поточний стан інтерфейсу G0/0/1? Яке значення адреси керування доступом до середовища (MAC) інтерфейсу G0/0/1? Який вигляд має в цій команді Інтернет-адреса?

13. Для відображення інформації про IPv6 введіть команду **show ipv6 interface *interface*** .

R1# show ipv6 interface g0/0/1

14. Відобразіть загальний список інтерфейсів на маршрутизаторі та комутаторі. Існує кілька команд, які можна використовувати для перевірки налаштування інтерфейсу. Однією з найбільш корисних є команда **show ip interface brief**. В результаті виконання команди відображається загальний список інтерфейсів на пристрої та надається негайний відгук про стан кожного інтерфейсу.

Введіть **show ip interface brief** на маршрутизаторі R1.

R1# **show ip interface brief**

Щоб побачити інформацію про інтерфейс по IPv6 , введіть команду **show ipv6 interface brief** на R1.

R1# show ipv6 interface brief

Введіть команду **show ip interface brief** на комутаторі S1.

S1# show ip interface brief

Питання для самоперевірки

Якщо інформація про інтерфейс G0/0/1 показує, що він був адміністративно вимкнений (administratively down), яку команду налаштування інтерфейсу ви б використали для його активації?

Що станеться, якщо на маршрутизаторі неправильно налаштувати на інтерфейсі G0/0/1 IP-адресу 192.168.1.2?

Лабораторна робота 6
Налаштування IPv6-адресації

Мета роботи: навчитись налаштовувати IPv6-адресацію на маршрутизаторі, серверах і клієнтських вузлах.

Завдання: налаштувати адресацію IPv6 на маршрутизаторі, серверах, клієнтських вузлах, протестувати мережу та перевірити зв'язок в мережі (рис. 1).

Пристрій	**Інтерфейс**	**IPv6-адреса/префікс**	**Шлюз за замовчуванням**
R1	G0/0	2001:db8:1:1::1/64	N/A
		fe80::1	
	G0/1	2001:db8:1:2::1/64	N/A
		fe80::1	
	S0/0/0	2001:db8:1:a001::2/64	N/A
		fe80::1	
Sales	NIC	2001:db8:1:1::2/64	fe80::1
Billing	NIC	2001:db8:1:1::3/64	fe80::1
Accounting	NIC	2001:db8:1:1::4/64	fe80::1
Design	NIC	2001:db8:1:2::2/64	fe80::1
Engineering	NIC	2001:db8:1:2::3/64	fe80::1
CAD	NIC	2001:db8:1:2::4/64	fe80::1
ISP	S0/0/0	2001:db8:1:a001::1	fe80::1

Топологія

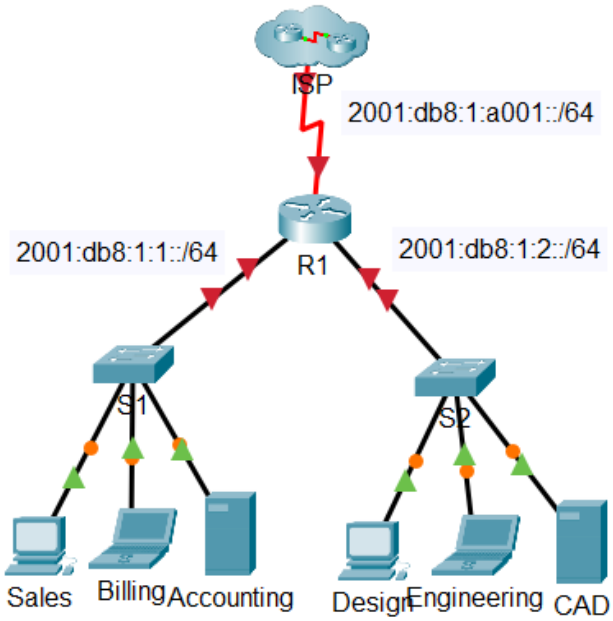


Рисунок 1 – Топологія мережі

Хід роботи

1. Налаштування адресації IPv6 на маршрутизаторі [2]. Увімкнути перенаправлення IPv6-пакетів на маршрутизаторі.

– натиснути на **R1** і перейти на вкладку **CLI**. Натиснути клавішу **Enter**;

– увійти до привілейованого режиму EXEC;

– ввести команду **ipv6 unicast-routing** в режимі глобальної конфігурації. Дана команда необхідна для включення перенаправлення пакетів IPv6 на маршрутизаторі;

R1(config)# ipv6 unicast-routing.

2. Налаштувати адресацію IPv6 на GigabitEthernet0/0. Ввести необхідні команди для переходу в режим налаштування інтерфейсуGigabitEthernet0/0:

– налаштувати адресу IPv6 за допомогою такої команди:

R1(config-if)# ipv6 address 2001:db8:1:1::1/64

– налаштувати локальну IPv6-адресу каналу за допомогою такої команди:

R1(config-if)# ipv6 address fe80::1 link-local

– активувати інтерфейс:

R1(config-if)# no shutdown

3. Налаштувати адресацію IPv6 на GigabitEthernet0/1:

– ввести необхідні команди для переходу в режим налаштування інтерфейсу GigabitEthernet0/1;

– потрібні IPv6-адреси дивіться у **таблиці адресації**;

– налаштувати адресу IPv6, локальну адресу каналу та активувати інтерфейс.

4. Налаштувати адреси IPv6 на Serial0/0/0:

– ввести необхідні команди для переходу в режим налаштування інтерфейсу Serial0/0/0;

– потрібні IPv6-адреси дивіться у таблиці адресації;

– налаштувати адресу IPv6, локальну адресу каналу та активувати інтерфейс.

5. Перевірити адресацію IPv6 на маршрутизаторі R1. Після завершення процесу адресації рекомендується перевірити налаштовані значення шляхом їх порівняння зі значеннями в таблиці адресації:

– вийти з режиму налаштування на маршрутизаторі R1;

– перевірити налаштування адресації за допомогою команди:

R1# show ipv6 interface brief

Якщо відображаються невідповідні адреси, для внесення змін повторіть зазначені вище дії.

Примітка. Щоб змінити параметри адресації необхідно спершу видалити невідповідну адресу, інакше на інтерфейсі залишаться налаштованими як правильна, так і неправильна адреса.

Наприклад:

R1(config-if)# no ipv6 address 2001:db8:1:5::1/64

– зберегти налаштування маршрутизатора в пам’ять NVRAM;

– закрити вікно налаштувань.

6. Налаштування адресації IPv6 на серверах:

1) налаштувати адресацію IPv6 на **Accounting** Server: натиснути на **Accounting** і перейти на вкладку **Desktop > IP Configuration**:

– як IPv6-адресу встановити значення **2001:db8:1:1::4** з префіксом **/64**;
– як IPv6-адресу шлюзу за замовчуванням встановити локальну адресу **fe80::1**;

2) налаштувати адресацію IPv6 на CAD Server:

– налаштувати на CAD Server адреси, потрібні IPv6-адреси оберіть у **таблиці адресації**.

7. Налаштування адресації IPv6 на клієнтських вузлах:

1) налаштувати адресацію IPv6 на Sales та Billing Clients:

– натиснути на Billing Clients і перейти на вкладку Desktop > IP Configuration;
– як IPv6-адресу встановити значення **2001:db8:1:1::3** з префіксом /**64**;
– як IPv6-адресу шлюзу за замовчуванням встановити локальну адресу **fe80::1**;
– повторити кроки для вузла Sales. Потрібні IPv6-адреси оберіть у **таблиці адресації**.

8. Налаштувати адресацію IPv6 на Engineering та Design:

– натиснути на Engineering і перейти на вкладку Desktop> IP Configuration;
– як IPv6-адресу встановити значення **2001:db8:1:2::3** з префіксом **/64**;
– як IPv6-адресу шлюзу за замовчуванням встановити локальну адресу **fe80::1**;
– повторити кроки для вузла Design. Потрібні IPv6-адреси оберіть у таблиці адресації.

9. Тестування та перевірка зв’язку в мережі:

1) відкрити веб-сторінки сервера на клієнтських вузлах:

– натиснути на Sales і перейти на вкладку Desktop. Закрити вікно IP Configuration, якщо це необхідно.
– натиснути на Web Browser. Ввести 2001:db8:1:1::4 у рядку URL і натиснути Go. Повинен відкритися сайт Accounting.
– ввести 2001:db8:1:2::4 у рядку URL і натиснути Go. Повинен відкритися сайт CAD.
– повторити кроки для інших клієнтських вузлів;

2) перевірити зв’язок з ISP:

– натиснути на будь-який клієнтський вузол;
– у вкладці Desktop, вибрати > Command Prompt;
– перевірити зв’язок із ISP за допомогою такої команди:

PC> ping 2001:db8:1:a001::1

– продовжуйте виконувати команду ping на інших клієнтських вузлах, допоки не переконаєтеся, що у всіх вузлів є зв’язок з інтернет-провайдером.

10. Скріни виведення команд помістити в звіт по роботі.

Лабораторна робота 7
Перевірка адресації IPv4 і IPv6

Мета роботи: дослідити реалізацію подвійного стека IPv4 і IPv6, включаючи документування, перевірку з'єднання та трасування.

Завдання: доповнити документування таблиці адресації, перевірити з'єднання за допомогою команди ping, виявити шляхи трасуванням маршруту (рис. 1).

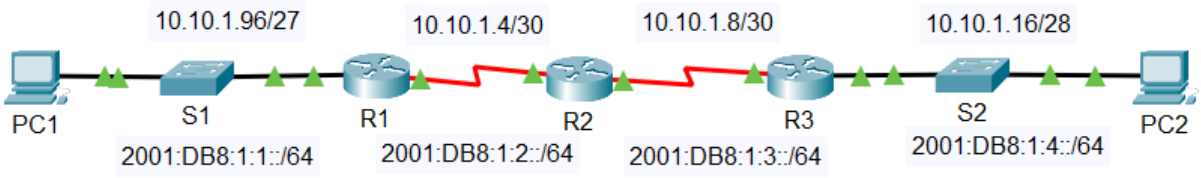


Рисунок 1– Топологія мережі

Таблиця 1 – Таблиця адресації

Пристрій	Інтерфейс	IP-адреса/Префікс		Шлюз за замовчуванням
R1	G0/0	10.10.1.97	255.255.255.224	N/A
		2001:db8:1:1::1/64		
	S0/0/1	10.10.1.6	255.255.255.252	N/A
		2001:db8:1:2::2/64		
		fe80::1		
R2	S0/0/0	10.10.1.5	255.255.255.252	N/A
		2001:db8:1:2::1/64		
	S0/0/1	10.10.1.9	255.255.255.252	N/A
		2001:db8:1:3::1/64		
		fe80::2		
R3	G0/0	10.10.1.17	255.255.255.240	N/A
		2001:db8:1:4::1/64		
	S0/0/1	10.10.1.10	255.255.255.252	N/A
		2001:db8:1:3::2/64		
		fe80::3		
PC1	NIC			
PC2	NIC			

Хід роботи

Доповнення документування таблиці адресації (табл. 1).

1. Використати команду ipconfig для перевірки адресації IPv4 [2]:

– натисніть на **PC1** та відкрийте **Command Prompt;**

– введіть команду **ipconfig /all** для збору даних про IPv4. Внесіть дані в **таблицю адресації** вказавши IPv4-адресу, маску підмережі та шлюз за замовчуванням;

– натисніть на **PC2** та відкрийте **Command Prompt;**

– введіть команду **ipconfig /all** для збору даних про IPv4. Внесіть дані в **таблицю адресації** вказавши IPv4-адресу, маску підмережі та шлюз за замовчуванням.

2. Використати команду ipv6config для перевірки адресації IPv6:

– на **PC1**, введіть команду **ipv6config /all** для збору даних про IPv6. Внесіть дані в **таблицю адресації** вказавши IPv6-адресу, префікс підмережі та шлюз за замовчуванням;

– на **PC2**, введіть команду **ipv6config /all** для збору даних про IPv6. Внесіть дані в **таблицю адресації** вказавши IPv6-адресу, префікс підмережі та шлюз за замовчуванням.

3. Перевірка з'єднання. Використати команду **ping** для перевірки IPv4-з'єднання:

– з **PC1** пропінгуйте IPv4-адресу **PC2** (д***одати скрін виконання команди та пояснити результат?);***

– з **PC2** пропінгуйте IPv4-адресу **PC1** (д***одати скрін виконання команди та пояснити результат?).***

4. Використати команду ping для перевірки IPv6-з'єднання.

– з **PC1** пропінгуйте IPv6-адресу **PC2** (д***одати скрін виконання команди та пояснити результат?);***

– з **PC2** пропінгуйте IPv6-адресу **PC1** (д***одати скрін виконання команди та пояснити результат?).***

5. Виявлення шляху трасуванням маршруту. Використати команду **tracert** для виявлення шляху IPv4.

– з **PC1** виконайте трасування маршруту до **PC2**:

PC> tracert 10.10.1.20

Дайте відповіді на питання. Які адреси зустрічалися на шляху? Яким інтерфейсам відповідають ці адреси? Додати в звіт скріни виконання команди.

– з **PC2** виконайте трасування маршруту до **PC1**.

Дайте відповіді на питання. Які адреси зустрічалися на шляху? Яким інтерфейсам відповідають ці адреси? Додати в звіт скріни виконання команди;

6. Використати команду tracert для виявлення шляху IPv6:

– з **PC1** виконайте трасування маршруту до IPv6-адреси **PC2**:

PC> tracert 2001:db8:1:4::a

Дайте відповіді на питання. Які адреси зустрічалися на шляху? Яким інтерфейсам відповідають ці адреси? Додати в звіт скріни виконання команди;

– З **PC2** виконайте трасування маршруту до IPv6-адреси **PC1**.

Дайте відповіді на питання. Які адреси зустрічалися на шляху? Яким інтерфейсам відповідають ці адреси? Додати в звіт скріни виконання команди;

Лабораторна робота 8
Використання Wireshark для перегляду мережного трафіку

Мета роботи: навчитися аналізувати трафік, використовуючи програмний аналізатор протоколів (або програма «пакетний сніфер») Wireshark.

Завдання: перехопити та проаналізувати локальні та віддалені ICMP-дані за допомогою Wireshark (рис. 1).

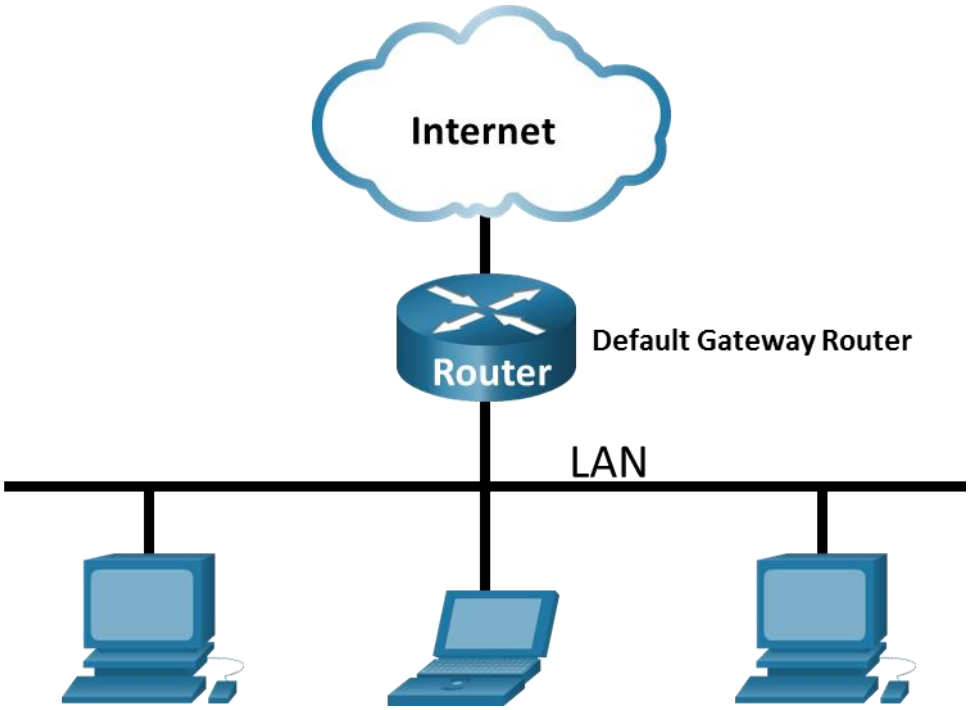


Рисунок 1 – Топологія мережі

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. У цій лабораторній роботі Ви будете використовувати Wireshark для перехоплення IP-адрес з ICMP-повідомлення та MAC-адрес з Ethernet-кадра [2].

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

Перехоплення та аналіз локальних ICMP-даних за допомогою Wireshark. У даній лабораторній роботі потрібно перевірити зв’язок з іншим ПК в локальній мережі за допомогою команди ping та перехопити згенеровані ICMP-запити та ICMP-відповіді, використовуючи Wireshark. Також розглянути вміст перехоплених кадрів для отримання певної інформації. Цей аналіз має допомогти з’ясувати, як заголовки повідомлень використовуються для транспортування даних до місця призначення.

Хід роботи

1. Визначення адрес мережної плати ПК:

– відкрити вікно командного рядка Windows;

– у командному рядку ввести команду ipconfig /all, щоб переглянути IP-адресу, MAC-адресу, опис мережної плати ПК (рис. 1).

```
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>
```

Рисунок 1 – Перегляд IP-адреси, MAC-адреси та опис мережної плати ПК

Примітка. 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.

2. Запуск Wireshark і початок перехоплення даних.

Перейдіть до Wireshark. Двічі натисніть на потрібному інтерфейсі, щоб розпочати перехоплення повідомлень. Переконайтеся, що на потрібний інтерфейс надходить трафік. 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. 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 (рис. 2).

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
```

Рисунок 2 – Пінг IP-адреси

Зверніть увагу на те, що дані знову з’являються у верхній частині вікна Wireshark (рис. 3).

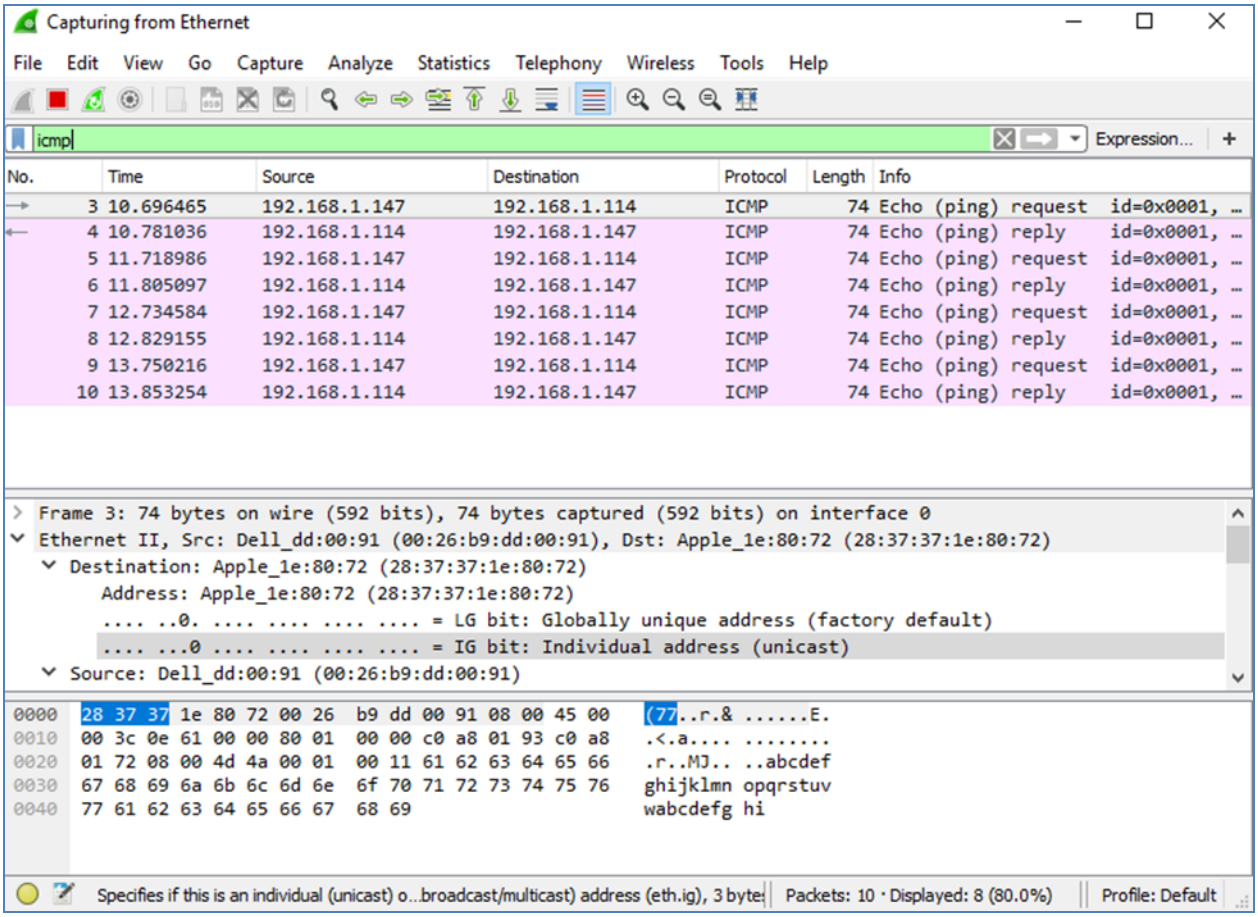


Рисунок 3 – Вікно Wireshark з даними

Примітка. Якщо ПК члена Вашої команди не відповідає на Ваші ping-запити, причиною може бути блокування цих запитів його міжмережним екраном. В Додаток А

Дозвіл передачі ICMP-трафіку через міжмережний екран ОС Windows знайдіть і перегляньте інформацію про те, як дозволити передачу ICMP-трафіку через міжмережний екран в ОС Windows.

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

4. Дослідження перехоплених даних.

Виконати 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.

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).

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.

Дайте відповідь на питання. 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? ***Напишіть тут свою відповідь та відобразіть у звіті скріни виконання команди.***

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.

5. Перехоплення та аналіз віддалених ICMP-даних за допомогою Wireshark.

За допомогою команди ping потрібно перевірите зв’язок з віддаленими вузлами (вузлами, які не належать до Вашої локальної мережі) та дослідити отримані дані. Визначити чим відрізняються ці дані від даних, які досліджувалися у роботі вище:

– початок перехоплення даних на мережній платі/інтерфейсі: розпочніть перехоплення даних знову. Wireshark запропонує Вам зберегти раніше перехоплені дані перед початком іншого перехоплення. Зберігати ці дані не обов’язково. Натисніть **Continue without Saving**. Після активізації перехоплення у командному рядку Windows виконайте команду ping для таких URL-адрес веб-сайтів: відкрийте вікно командного рядка Windows

www.cisco.com

www.google.com

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

отримані для кожної URL-адреси. Ви можете зупинити перехоплення даних, натиснувши **Stop Capture**.

– дослідіть та проаналізуйте дані з віддалених вузлів: перегляньте перехоплені дані в Wireshark та дослідіть IP-адреси та MAC-адреси веб-сайтів, з якими Ви перевіряли зв'язок. Запишіть IP-адреси та MAC-адреси отримувачів для веб-сайтів, з якими Ви перевіряли зв'язок.

IP-адреса для **www.cisco.com**:

Напишіть тут свою відповідь.

MAC-адреса для **www.cisco.com**:

Напишіть тут свою відповідь.

IP-адреса для **www.google.com**:

Напишіть тут свою відповідь.

MAC-адреса для **www.google.com**:

Напишіть тут свою відповідь.

Додайте ще один веб-сайт на Ваш вибір, та виконайте аналогічні кроки.

Дайте відповідь на запитання. Що важливе в цій інформації? Чим ця інформація відрізняється від інформації, яку Ви отримали в роботі вище?

Напишіть тут свою відповідь.

Питання для самоперевірки

Чому Wireshark показує реальні MAC-адреси вузлів локальної мережі, але не показує реальні MAC-адреси вузлів віддалених мереж? Напишіть тут свою відповідь.

Додаток А
Дозвіл передачі ICMP-трафіку через міжмережний 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.

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

– перейдіть до **Control Panel** і натисніть опцію **System and Security** в Category view;

– у вікні **System and Security**, натисніть **Windows Defender Firewall** або **Windows Firewall**;

– на лівій панелі **Windows Defender Firewall** або вікна **Windows Firewall** натисніть **Advanced settings**;

– у вікні **Advanced Security** на лівій бічній панелі виберіть опцію **Inbound Rules** і потім натисніть **New Rule…** на правій бічній панелі;

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

– на лівій панелі вікна виберіть параметр **Protocol and Ports** і, використовуючи спадне меню **Protocol Type**, виберіть **ICMPv4**, а потім натисніть **Next**;

– переконайтесь, що як для локальних так і для віддалених адрес вибрано **Any IP address**. Натисніть **Next**, щоб продовжити;
– виберіть **Allow the connection**. Натисніть **Next**, щоб продовжити;
– за замовчуванням це правило застосовується для всіх профілів ОС. Натисніть **Next**, щоб продовжити;
– 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.

Вимкнення або видалення ICMP-правила.

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

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

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 9
Впровадження маршрутизації між VLAN

Мета роботи: опанування принципи логічного поділу мережі за допомогою віртуальних локальних мереж (VLAN), набути практичні навички налаштування маршрутизації між VLAN для забезпечення взаємодії між різними сегментами мережі.

Завдання: налаштувати базові параметрів пристрою, створити мережі VLAN і призначити порти комутатора, налаштувати магістральний канал 802.1Q між комутаторами, налаштування маршрутизацію між VLAN на маршрутизаторі, перевірити працездатність маршрутизації між VLAN (рис. 1).

Хід роботи

Створити топологію як на рисунку 1, налаштувати адресацію згідно таблиці 1 та створити vlan згідно таблиці 2 [3].

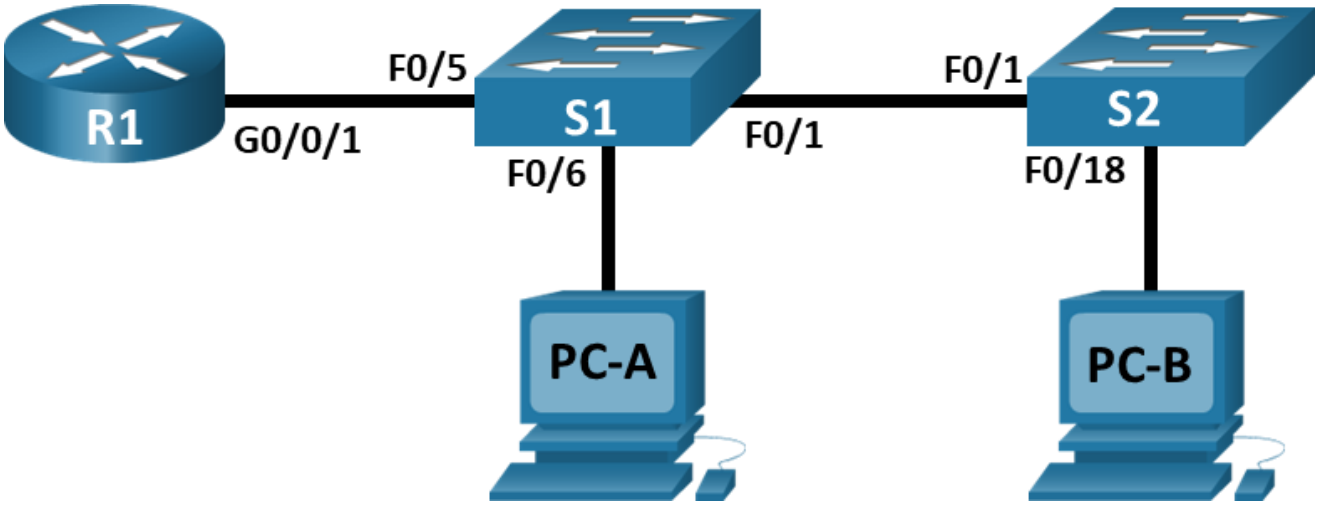


Рисунок 1 – Топологія мережі

Таблиця 1 − Таблиця адресації

Пристрій	Інтерфейс	IP-адреса	Маска підмережі	Шлюз за замовчуванням
R1	G0/0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/0/1.20	192.168.20.1	255.255.255.0	
	G0/0/1.30	192.168.30.1	255.255.255.0	
	G0/0/1.1000	N/A	N/A	
S1	VLAN 10	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 10	192.168.10.12	255.255.255.0	192.168.10.1
PC-A	NIC	192.168.20.3	255.255.255.0	192.168.20.1
PC-B	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Таблиця 2 − Таблиця VLAN

VLAN	Ім’я	Призначений інтерфейс
10	Management	S1: VLAN 10 S2: VLAN 10
20	Sales	S1: F0/6
30	Operations	S2: F0/18
999	Parking_Lot	S1: F0/2-4, F0/7-24, G0/1-2 S2: F0/2-17, F0/19-24, G0/1-2
1000	Native	N/A

Сучасні комутатори використовують віртуальні локальні мережі (VLAN) для поліпшення продуктивності мережі, розділяючи великі широкомовні домени рівня 2 на менші. VLAN також можна використовувати як засіб безпеки, відокремлюючи трафік конфіденційних даних від решти мережі. Загалом, VLAN спрощують проєктування мережі для досягнення цілей організації. Для зв’язку між VLAN потрібен пристрій, що працює на рівні 3 моделі OSI. Додавання маршрутизатора між VLAN дозволяє організації розмежувати і розділяти широкомовні домени, одночасно дозволяючи їм спілкуватися один з одним.

Магістральні канали VLAN використовуються для поширення VLAN на декілька пристроїв. Магістральні канали дозволяють трафіку з декількох VLAN рухатися по одному каналу, зберігаючи ідентифікацію та сегментацію VLAN незмінними. Особливий вид маршрутизації між VLAN, названий «Router-On-A-Stick», використовує магістральний канал від маршрутизатора до комутатора, щоб всі VLAN могли проходити на маршрутизатор.

У цій лабораторній роботі ви створите VLAN на обох комутаторах в топології, призначите VLAN для портів доступу комутатора, переконаєтесь, що VLAN працюють належним чином, створите магістральні канали VLAN між двома комутаторами і між S1 і R1, а також налаштуєте маршрутизацію між VLAN на R1, щоб дозволити вузлам в різних VLAN спілкуватися, незалежно від того, в якій підмережі знаходиться вузол.

Примітка. Маршрутизатори, що використовуються в лабораторній роботі − Cisco 4321, комутатори − Cisco Catalyst 2960.

Виконати наступні пункти:

1) створіть мережу та налаштуйте базові параметрів пристрою:

– з’єднайте пристрої у мережу, відповідно до схеми топології;

– приєднайте пристрої необхідними кабелями, як показано на схемі топології;

2) налаштуйте основні параметри на маршрутизаторі:

– підключіть консольне з’єднання до маршрутизатора і увійдіть в привілейований режим EXEC;

Router> enable

– увійдіть до режиму конфігурації;

Router# config terminal

– призначте маршрутизатору ім’я;

Router(config)# hostname R1

– вимкніть пошук DNS, щоб упередити маршрутизатор від спроби неправильно перекласти введені команди: ніби вони є іменами хостів;

R1(config)# no ip domain lookup

– призначте class як зашифрований пароль привілейованого режиму EXEC;

R1(config)# enable secret class

– призначте cisco як пароль доступу до консолі і активуйте авторизацію;

R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login

– призначте cisco як пароль для віртуальних ліній і активуйте авторизацію;

R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login

– зашифруйте всі відкриті текстові паролі;

R1(config)# service password-encryption

– створіть банер, який попереджатиме всіх, хто має доступ до пристрою, про те, що несанкціонований доступ заборонено;

R1(config)# banner motd $ Authorized Users Only! $

– збережіть поточну конфігурацію у файл стартової конфігурації;

R1(config)# exit
R1# copy running-config startup-config

– встановіть час на маршрутизаторі;

R1# clock set 14:30:00 27 Aug 2025

– закрийте вікно конфігурації.

3) налаштуйте базові параметри для кожного комутатора:

– призначте комутатору ім’я;

switch(config)# hostname S1
switch(config)# hostname S2

– вимкніть пошук DNS, щоб упередити комутатор від спроби неправильно перекласти введені команди: ніби вони є іменами хостів;

S1(config)# no ip domain-lookup
S2(config)# no ip domain-lookup

– призначте class як зашифрований пароль на привілейований режим EXEC;

S1(config)# enable secret class
S2(config)# enable secret class

– призначте cisco як пароль на консольній лінії і активуйте авторизацію;

S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login

S2(config)# line console 0
S2(config-line)# password cisco
S2(config-line)# login

– призначте cisco як пароль для віртуальних ліній і активуйте авторизацію;

S1(config)# line vty 0 4

S1(config-line)# password cisco
S1(config-line)# login

S2(config)# line vty 0 4
S2(config-line)# password cisco
S2(config-line)# login

– зашифруйте всі відкриті текстові паролі;

S1(config)# service password-encryption
S2(config)# service password-encryption

– створіть банер, який попереджатиме всіх, хто під'єднується до пристрою, про те, що несанкціонований доступ заборонено;

S1(config)# banner motd $ Authorized Users Only! $
S2(config)# exit
S2(config)# banner motd $ Authorized Users Only! $
S2(config)# exit

– встановіть час на комутаторі;

S1# clock set 14:30:00 27 Aug 2025
S2# clock set 14:30:00 27 Aug 2025

– збережіть поточні налаштування у файлі початкової конфігурації;

S1# copy running-config startup-config
S2# copy running-config startup-config

4) налаштуйте вузли PC:

– зверніться до таблиці адресації для визначення адресної інформації вузлів.

5) створення мереж VLAN і призначення портів комутатора:

– створіть VLAN, як зазначено в таблиці вище, на обох комутаторах, призначите VLAN відповідному інтерфейсу і перевірите свої налаштування конфігурації. Виконайте наступні налаштування на кожному комутаторі;

– Створіть і назвіть необхідні VLAN на кожному комутаторі з таблиці вище.

S1(config)# vlan 10
S1(config-vlan)# name Management
S1(config-vlan)# vlan 20
S1(config-vlan)# name Sales
S1(config-vlan)# vlan 30
S1(config-vlan)# name Operations
S1(config-vlan)# vlan 999
S1(config-vlan)# name Parking_Lot
S1(config-vlan)# vlan 1000
S2(config-vlan)# name Native
S1(config-vlan)# exit

S2(config)# vlan 10
S2(config-vlan)# name Management
S2(config-vlan)# vlan 20
S2(config-vlan)# name Sales
S2(config-vlan)# vlan 30
S2(config-vlan)# name Operations

S2(config-vlan)# vlan 999
S2(config-vlan)# name Parking_Lot
S2(config-vlan)# vlan 1000
S2(config-vlan)# name Native
S2(config-vlan)# exit

– налаштуйте інтерфейс керування та шлюз за замовчуванням на кожному комутаторі, використовуючи відомості про IP-адресу в таблиці адресації;

S1(config)# interface vlan 10
S1(config-if)# ip address 192.168.10.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.10.1

S2(config)# interface vlan 10
S2(config-if)# ip address 192.168.10.12 255.255.255.0
S2(config-if)# no shutdown
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.10.1

– призначте всі невикористані порти на обох комутаторах у ParkingLot VLAN, налаштуйте їх на статичний режим доступу і адміністративно дезактивуйте.

Примітка. Команда interface range корисна для виконання цього завдання з якомога меншою кількістю команд.

S1(config)# interface range f0/2 - 4 , f0/7 - 24 , g0/1 - 2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown

S2(config)# interface range f0/2 - 17, f0/19 - 24 , g0/1 - 2
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 999
S2(config-if-range)# shutdown

6) призначте VLAN відповідним інтерфейсам комутатора:

– призначте використовувані порти відповідній VLAN (зазначеній у таблиці VLAN вище) та налаштуйте їх на статичний режим доступу;

S1(config)# interface f0/6
S1(config-if)# switchport mode acces
S1(config-if)# switchport access vlan 20

S2(config)# interface f0/18
S2(config-if)# switchport mode acces
S2(config-if)# switchport access vlan 30

– переконайтеся, що VLAN призначені правильним інтерфейсам;

S1# show vlan brief

```
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/5
```

```
10 Management active
20 Sales active Fa0/6
30 Operations active
999 Parking_Lot active Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
1000 Native active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddi-default act/unsup
1005 trnet-default act/unsup
```

S2# show vlan brief

```
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1
10 Management active
20 Sales active
30 Operations active Fa0/18
999 Parking_Lot active Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
1000 Native active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddi-default act/unsup
1005 trnet-default act/unsup
```

7) налаштуйте інтерфейс магістрального каналу F0/1 вручну на комутаторах S1 і S2:

– налаштуйте статичний магістральний канал на інтерфейсі F0/1 для обох комутаторів;

S1(config)# interface f0/1
S1(config-if)# switchport mode trunk

S2(config)# interface f0/1
S2(config-if)# switchport mode trunk

– встановіть для native VLAN 1000 на обох комутаторах;

S1(config-if)# switchport trunk native vlan 1000

S2(config-if)# switchport trunk native vlan 1000

– уточніть, що VLAN 10, 20, 30 і 1000 дозволені на магістральному каналі;

S1(config-if)# switchport trunk allowed vlan 10,20,30,1000

S2(config-if)# switchport trunk allowed vlan 10,20,30,1000

– перевірте магістральні порти, Native VLAN і дозволені VLAN на магістральному каналі;

S1# show interfaces trunk

```
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1000

Port Vlans allowed on trunk
Fa0/1 10,20,30,1000

Port Vlans allowed and active in management domain
Fa0/1 10,20,30,1000

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 10,20,30,1000
```

S2# show interfaces trunk

```
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 1000

Port Vlans allowed on trunk
Fa0/1 10,20,30,1000

Port Vlans allowed and active in management domain
Fa0/1 10,20,30,1000

Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 10,20,30,1000
```

9) вручну налаштуйте магістральний інтерфейс S1 F0/5:

– налаштуйте інтерфейс S1 F0/5 з тими ж параметрами магістралі, що і F0/1. Це магістральний канал до маршрутизатора;

– збережіть поточні налаштування у файлі початкової конфігурації;

S1# copy running-config startup-config

S2# copy running-config startup-config

– перевірка магістрального каналу.

Дайте відповідь на запитання. Що станеться, якщо G0/0/1 на R1 вимкнеться?

10) налаштуйте маршрутизацію між VLAN на маршрутизаторі:

– активуйте інтерфейс G0/0/1 на маршрутизаторі;

R1(config)# interface g0/0/1
R1(config-if)# no shutdown
R1(config-if)# exit

– налаштуйте підінтерфейси для кожної VLAN, як зазначено в таблиці IP-адресації. Всі підінтерфейси використовують інкапсуляцію 802.1Q. Переконайтеся, що підінтерфейс для native VLAN не має IP-адреси. Налаштуйте опис для кожного під-інтерфейсу;

R1(config)# interface g0/0/1.10
R1(config-subif)# description Management Network
R1(config-subif) # encapsulation dot1q 10

R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# interface g0/0/1.20
R1(config-subif)# encapsulation dot1q 20
R1(config-subif)# description Sales Network
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# interface g0/0/1.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# description Operations Network
R1(config-subif)# ip address 192.168.30.1 255.255.255.0
R1(config-subif)# interface g0/0/1.1000
R1(config-subif)# encapsulation dot1q 1000 native
R1(config-subif)# description Native VLAN

– перевірте, чи працюють під-інтерфейси;

R1# show ip interface brief

```
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 unassigned YES NVRAM down down
GigabitEthernet0/0/1 unassigned YES NVRAM up up
Gi0/0/1.10 192.168.10.1 YES manual up up
Gi0/0/1.20 192.168.20.1 YES manual up up
Gi0/0/1.30 192.168.30.1 YES manual up up
Gi0/0/1.1000 unassigned YES unset up up
GigabitEthernet0 unassigned YES NVRAM down down
```

11) перевірка працездатності маршрутизації між VLAN:

Проведіть наступні тести з PC-A. Усі повинні бути успішними:

Примітка. Для успішного використання ping може знадобитися тимчасово відключити брандмауер Windows.

– відправте запит ping від PC-A до його шлюзу за замовчуванням;

– відправте запит ping від PC-A до PC-B;

– відправте запит ping від PC-A до S2.

Проведіть наступні тести з PC-B:

– у командному рядку на PC-B виконайте команду tracert на адресу PC-A.

Дайте відповідь на запитання. Які проміжні IP-адреси відображаються в результатах?

Примітка. Щоб дізнатися, як налаштований маршрутизатор, подивіться на інтерфейси, щоб визначити тип маршрутизатора та скільки інтерфейсів у маршрутизатора.

Лабораторна робота 10
Налаштування DHCP з використанням VLAN

Мета роботи: ознайомлення з принципами функціонування протоколу DHCP (Dynamic Host Configuration Protocol) у комп'ютерних мережах, набуття практичних навичок на прикладі використання обладнання Cisco з налаштування DHCP в локальному мережному середовищі.

Завдання. Створити діапазон роздачі IP-адрес і задати основні мережеві параметри (маска підмережі, шлюз, DNS-сервер), провести налаштування DHCP-клієнтів і перевірити отримання мережевих параметрів автоматично (рис. 1).

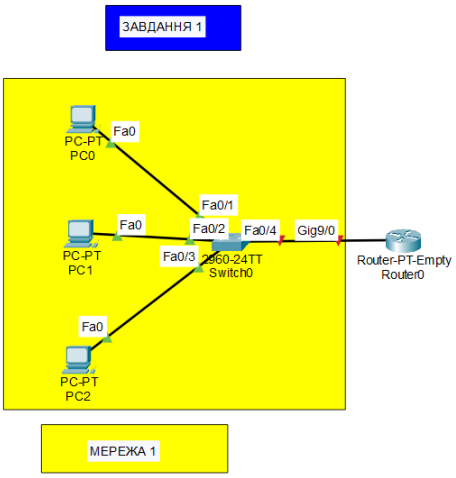


Рисунок 1 – Топологія мережі

Хід роботи

1. Опрацювати матеріа [4]. Завдання виконати згідно варіанту, поданому в таблиці 1. Створити схему мережі та з'єднати обладнання, як показано на схемі топології (рис. 1) . Комутатор, що використовуються в лабораторній роботі Catalyst 2960 та маршрутизатор PT-Empty (вимкнути живлення, додати до даного маршрутизатора порт PT-ROUTER-NM-1CGE, ввімкнути живлення, рис. 2). Назвати маршрутизатор **Вашим прізвищем**.

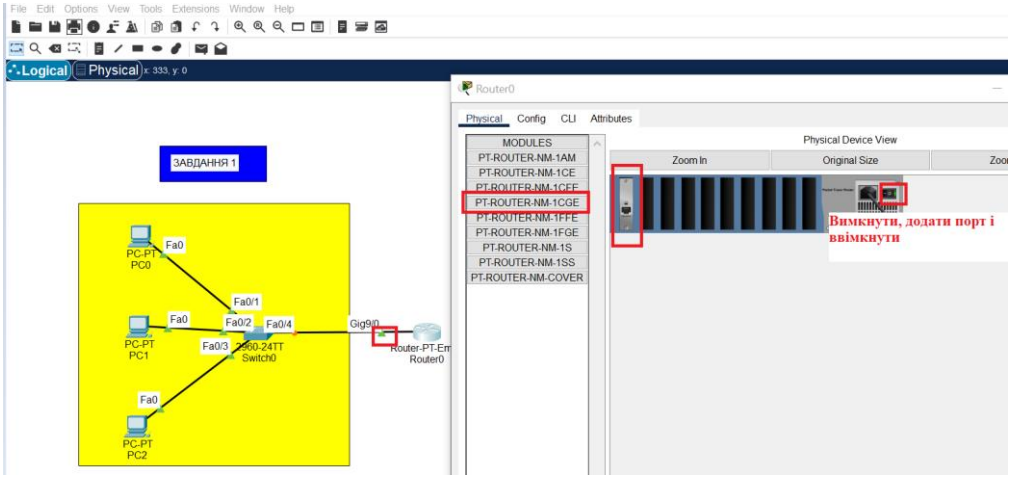


Рисунок 2 – Додавання порту на маршрутизаторі

2. Опрацювати матеріал [5]. Налаштувати шлюз за замовчуванням, використавши першу хостову адресу.

3. Створити dhcp-pool з ім’ям **M1**.

Ваше прізвище(config)#ip dhcp pool M1

Наприклад

C(config)#ip dhcp pool M1

4. Зазначаємо адресу мережі та маску.

Ваше прізвище(dhcp-config)#network *«адреса мережі» «маска підмережі»*

Наприклад:

Karpenko(dhcp-config)#network 192.168.1.0 255.255.255.0

3. Далі необхідно видати йому дефолтний маршрут. В даному випадку вказуємо ip-адресу нашого маршрутизатора, оскільки саме він є шлюзом за замовчуванням для комп’ютера.

Ваше прізвище(dhcp-config)#default-router шлюзом за замовчуванням

Наприклад:

Karpenko(dhcp-config)#default-router 192.168.1.1

де 192.168.1.1 –в кожного буде свій шлюзом за замовчуванням згідно завдання з пулу даної підмережі.

4. Для доступ до мережі Інтернет необхідно вказати dns-сервер. В даному прикладі задамо ip-адресу dns-сервера Google 8.8.8.8.

Ваше прізвище(dhcp-config)#dns-server 8.8.8.8

Наприклад:

Karpenko(dhcp-config)#dns-server 8.8.8.8

5. Виключимо ip-адресу з видачі DHCP, щоб цю ip-адресу не забрав якийсь комп’ютер. Зокрема, в даному випадку включимо із видачі DHCP адресу шлюзу за замовчуванням (будьте уважні, в кожного вона своя в залежності від варіанту).

Ваше прізвище (config)#ip dhcp excluded-address шлюзом за замовчуванням

Наприклад:

Karpenko(config)#ip dhcp excluded-address 192.168.1.1

6. Налаштувати комп’ютери, ввійшовши в вкладку IP configuration (рис. 3).

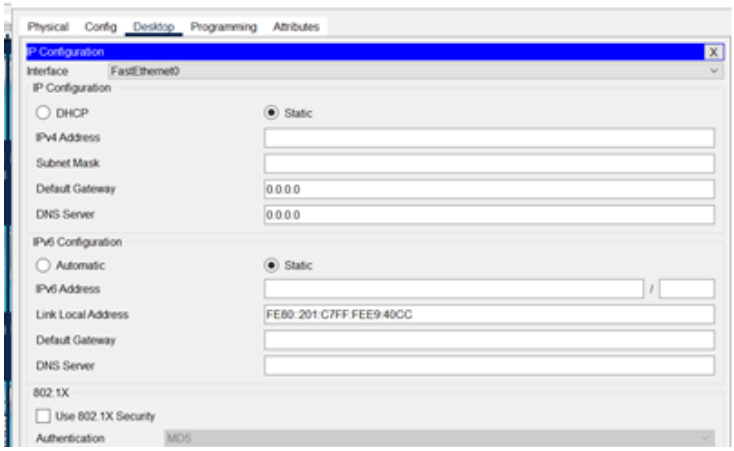


Рисунок 3 – Вкладку IP configuration

Як бачимо, за замовчуванням виставлено параметр Static (рис. 4), хоча насправді на реальних комп'ютерах завжди за замовчуванням встановлено параметр DHCP. Перемикаємо на параметр DHCP і комп'ютері повинен отримав ip-адресу з відповідного пулу.

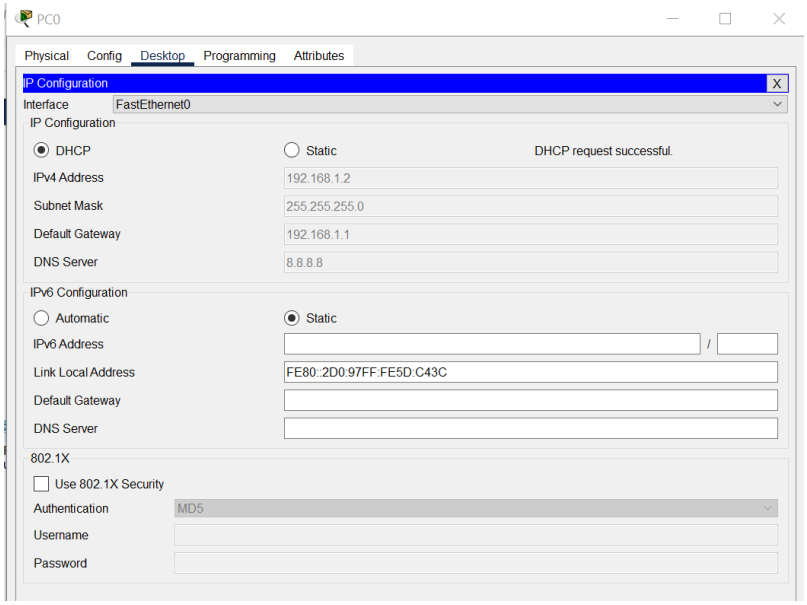


Рисунок 4 – Комп'ютері повинен отримав ip-адресу з відповідного пулу

Отже, роздачу ip-адрес по протоколу DHCP в Завдання 1 налаштовано.

Завдання 2. У даному завданні необхідно з'єднати обладнання, як показано на схемі топології (рис. 5) та налаштувати пристрої у відповідності до схеми. Після збереження налаштувань, потрібно перевірити виконані конфігурації, протестувавши під'єднання до мережі.

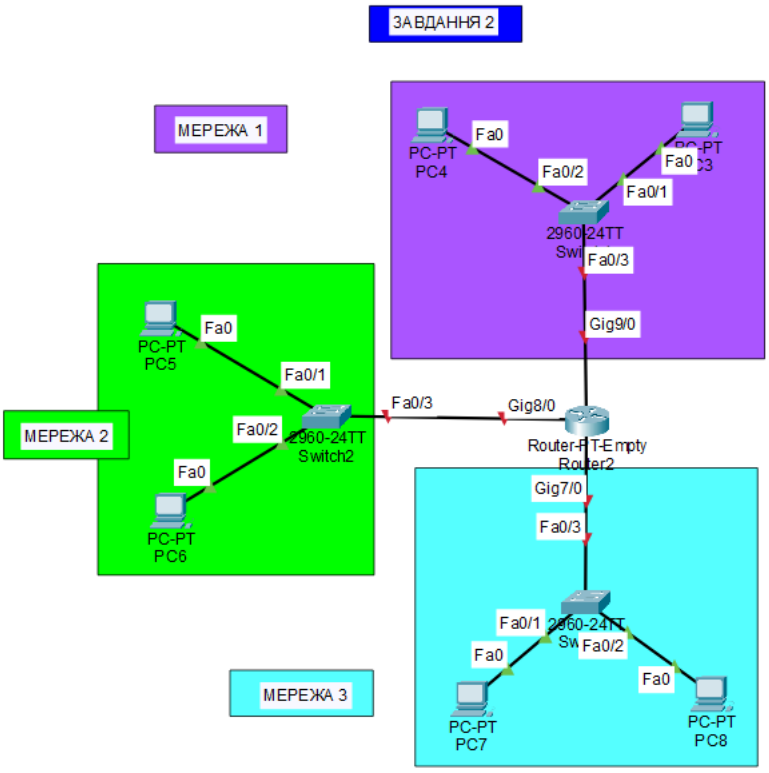


Рисунок 5 – Топологія мережі

Налаштування DHCP та Vlan і обмеження доступу до деяких маршрутів мережі на обладнанні Cisco

Опрацювати матеріал [6].В даному прикладі існує чотири сегменти мережі (рис. 6): vlan 2, vlan 3, vlan 4 (в яких згідно завдання є по три комп'ютери в кожному) і vlan 5, в якому знаходиться dhcp-сервер (зазвичай краще відділяти dhcp-сервер в окремий сегмент відмінний від сегментів користувачів).

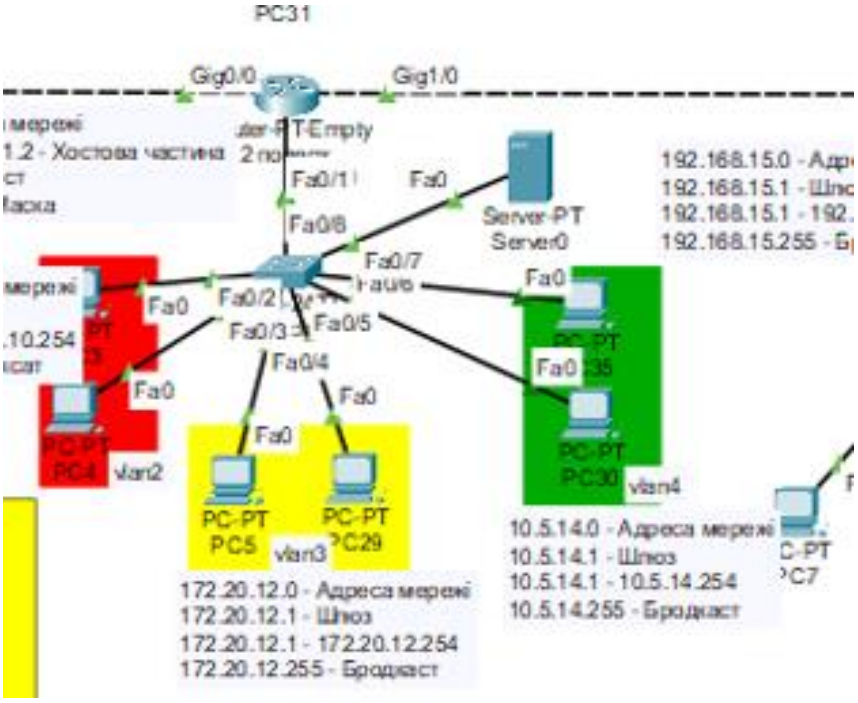


Рисунок 6 – Орієнтовна схема другого поверху

1. Налаштуємо комутатор, щоб сегментувати нашу мережу. Створимо vlan (табл. 1, рис. 7, 8).

Таблиця 1 – Синтаксис команд Cisco IOS, які використовуються для створення VLAN на комутаторі та її іменування [2]

Завдання	Команда IOS
Перехід до режиму глобальної конфігурації	`Switch# configure terminal`
Створення VLAN з відповідним ідентифікатором	`Switch(config)# vlan vlan-id`
Зазначення унікального імені для ідентифікації VLAN	`Switch(config-vlan)# name vlan-name`
Повернення до привілейованого режиму EXEC	`Switch(config-vlan)# end`

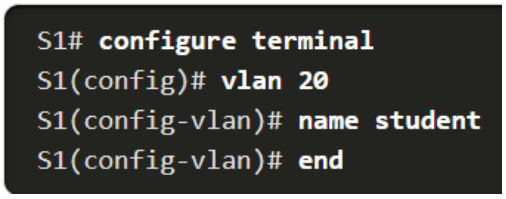


Рисунок 7 – Приклад створення VLAN [2]

Примітка: крім введення одного ідентифікатора VLAN, за допомогою команди vlan vlan-id через кому можна вводити послідовність ідентифікаторів VLAN або діапазон ідентифікаторів VLAN, розділених дефісами. Наприклад, введення команди vlan 100,102,105-107 у режимі глобальної конфігурації створить VLAN з ідентифікаторами 100, 102, 105, 106 і 107. [4]

Після створення VLAN наступним кроком є налаштування належності портів до VLAN.

У таблиці наведено синтаксис команд (табл. 2), що застосовуються для встановлення ролі порту як порту доступу і налаштування належності його до відповідної VLAN. Команда **switchport mode access** є необов'язковою, але як кращу практику безпеки наполегливо рекомендується її використовувати. За допомогою цієї команди виконується переведення порта комутатора у режим доступу на постійній основі.

Таблиця 2 – Команди налаштування належності портів до VLAN [2]

Завдання	Команда IOS
Увійдіть до режиму глобальної конфігурації	`Switch# configure terminal`
Увійдіть до режиму конфігурації інтерфейсу.	`Switch(config)# interface interface-id`
Переведення порту до режиму доступу	`Switch(config-if)# switchport mode access`
Налаштування належності порту до VLAN	`Switch(config-if)# switchport access vlan vlan-id`
Повернення до привілейованого режиму EXEC	`Switch(config-if)# end`

Примітка. Використовуйте команду **interface range** для одночасного налаштування декількох інтерфейсів [2].

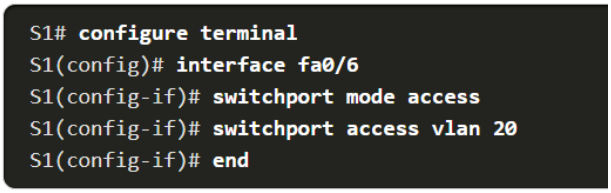


Рисунок 8 – Приклад налаштування належності порту до VLAN [2]

Транковий канал VLAN (VLAN trunk) – це канал зв'язку (2-го рівня моделі OSI) між двома комутаторами, що переносить трафік всіх VLAN (якщо вручну або динамічно не встановлено обмеження для певного переліку VLAN) [2].

Для активації транкового каналу (рис. 9-11) необхідно налаштувати взаємопов'язані порти за допомогою команд конфігурації інтерфейсу, перелік яких наведений у таблиці 3 [2].

Таблиця 3 – Команди налаштування транкового каналу [2]

Завдання	Команда IOS
Перехід до режиму глобальної конфігурації	`Switch# configure terminal`
Перехід до режиму налаштування інтерфейсу	`Switch(config)# interface interface-id`
Переведення порту до режиму постійного транкування.	`Switch(config-if)# switchport mode trunk`
Налаштування Native VLAN як VLAN, відмінну ніж VLAN 1.	`Switch(config-if)# switchport trunk native vlan vlan-id`
Формування списку VLAN, трафік яких дозволено передавати по транковому каналу.	`Switch(config-if)# switchport trunk allowed vlan vlan-list`
Повернення до привілейованого режиму EXEC	`Switch(config-if)# end`

```
S1(config)# interface fastEthernet 0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

Рисунок 9 – Приклад налаштування транкового каналу [2]

```
interface FastEthernet0/1
 switchport trunk allowed vlan 2-5
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
```

Рисунок 10 – Приклад налаштування належності порту до vlan 2 та налаштування транкового каналу vlan 2-5

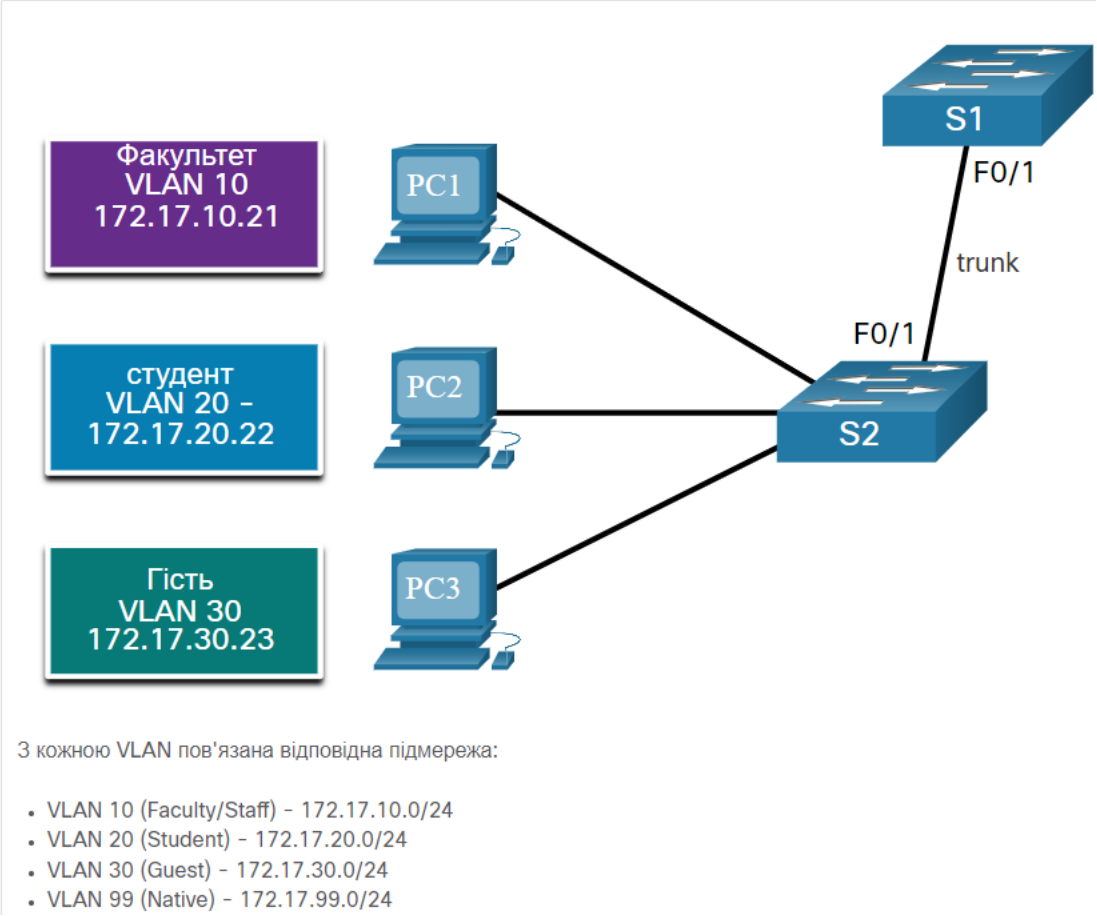


Рисунок 11 – Приклад схеми відображення транкового каналу [2]

На рисунку наведено топологію мережі (рис. 11), комп’ютери якої PC1, PC2 та PC3 належать до VLAN 10, 20 і 30 (Faculty, Student, Guest відповідно). Порт F0/1 комутатора S1 налаштовується як транковий порт і забезпечує передавання трафіку VLAN 10, 20 та 30. VLAN 99 налаштовується як Native VLAN [1].

Топологія мережі відображає три вузли, які підключені до одного комутатора S2, але належать до різних VLAN. Комп’ютер PC1 належить до VLAN 10 (Faculty) і має адресу 172.17.10.21. Комп’ютер PC2 належить до VLAN 20 (Student) і має адресу 172.17.20.22. Комп’ютер PC3 належить до

VLAN 30 (Guest) і має адресу 172.17.30.23. Порт F0/1 комутатора S2 підключається до порту F0/1 комутатора S1. Це з'єднання позначене як транковий канал (Trunk) [1].

2. На маршрутизаторі налаштуємо саб-інтерфейси (саб-інтерфейси дозволяють розділити один фізичний інтерфейс на декілька віртуальних інтерфейсів, кожний зі своєю конфігурацією) (рис. 12).

```
!
interface GigabitEthernet2/0.2
 encapsulation dot1Q 2
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.15.2
!
interface GigabitEthernet2/0.3
 encapsulation dot1Q 3
 ip address 172.20.12.1 255.255.255.0
 ip helper-address 192.168.15.2
!
interface GigabitEthernet2/0.4
 encapsulation dot1Q 4
 ip address 10.5.14.1 255.255.255.0
 ip helper-address 192.168.15.2
!
interface GigabitEthernet2/0.5
 encapsulation dot1Q 5
 ip address 192.168.15.1 255.255.255.0
!
```

Рисунок 12 – Приклад налаштування саб-інтерфейсів на маршрутизаторі на другому поверсі

Примітка. Відповідно в даних налаштуваннях будуть відрізнятись IP-адреси (так як обираються довільні приватні ip- адреси згідно завдання) та ip-helper-address, де ip-helper-address це – статична адреса dhcp-сервера.

1. Ввімкнути фізичний інтерфейс командою **no shutdown.**

2. Налаштувати DHCP сервер. Призначити йому статичну ip-адресу (другу в діапазоні адрес, рисунок 13), маску та шлюз за замовчуванням (перша адреса в діапазоні адрес, рисунок 13).

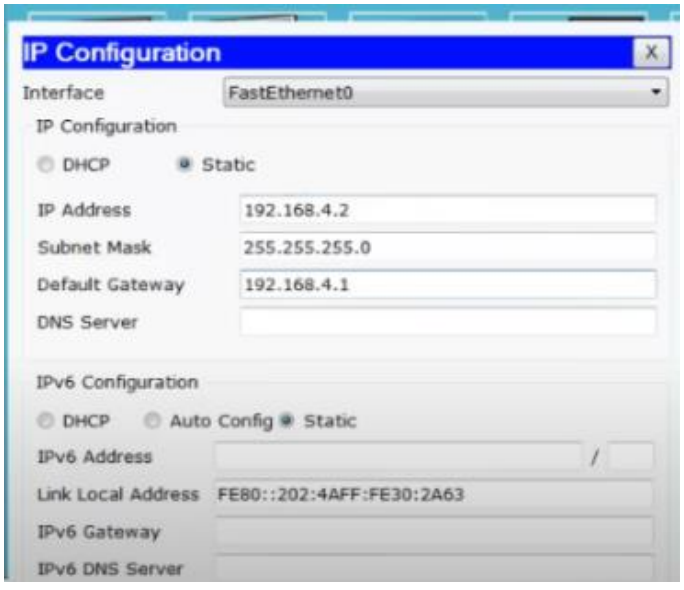


Рисунок 13 – Налаштування адресації на сервері

3. Перейти на сервері у вкладку налаштування DHCP (рис. 14).

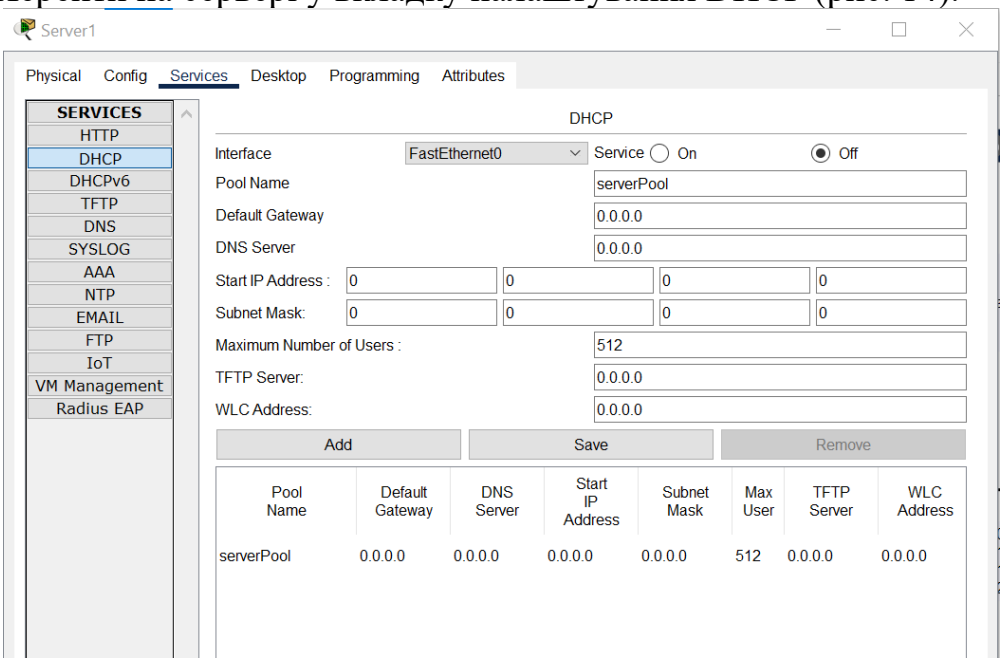


Рисунок 14 – Вкладка налаштування DHCP

На початку є створений один дефолтний сервер-пул. Цей пул залишається і далі створити нові, тобто, VLAN2, VLAN3, VLAN4 (рис. 15) та кнопкою Add їх додаємо (адресація обирається студентом самостійно з приватного пулу IPv4 адрес, див. вище).

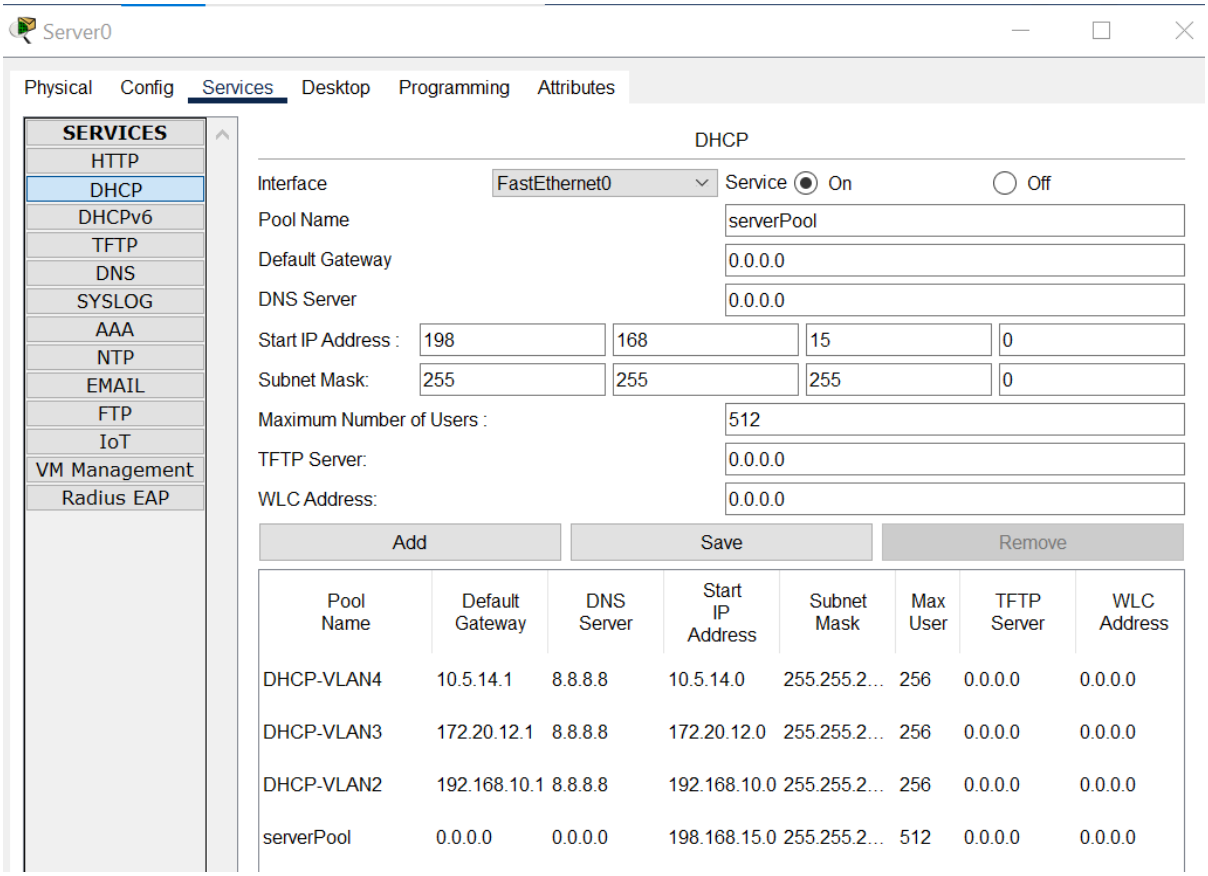


Рисунок 15 – Вкладка налаштування DHCP

В даному випадку dhcp сервер знаходиться в окремому сегменті. Оскільки комп'ютери і dhcp-сервер знаходяться в різних сегментах, потрібно переадресувати запити комп'ютерів на dhcp-сервер через маршрутизатор. Тобто, перенаправлення DHCP-запитів налаштовується на маршрутизаторі з використанням команди **ip helper address.** В даному прикладі необхідно для кожного саб-інтерфейсу налаштувати перенаправлення DHCP-запитів на існуючий dhcp-сервер (див. рисунок 12).

Варіант роботи

Таблиця 1 – Вибір варіанту

	Мережева адреса vlan 2, маска /24	Мережева адреса vlan 3, маска /24	Мережева адреса vlan 4, маска /24
1.	192.168.3.0	192.168.4.0	192.168.67.0
2.	192.168.5.0	192.168.6.0	192.168.68.0
3.	192.168.7.0	192.168.8.0	192.168.69.0
4.	192.168.9.0	192.168.10.0	192.168.70.0
5.	192.168.11.0	192.168.12.0	192.168.71.0
6.	192.168.13.0	192.168.14.0	192.168.72.0
7.	192.168.15.0	192.168.16.0	192.168.73.0
8.	192.168.17.0	192.168.18.0	192.168.74.0
9.	192.168.19.0	192.168.20.0	192.168.75.0
10.	192.168.21.0	192.168.22.0	192.168.76.0
11.	192.168.23.0	192.168.24.0	192.168.77.0
12.	192.168.25.0	192.168.26.0	192.168.78.0
13.	192.168.27.0	192.168.28.0	192.168.79.0
14.	192.168.29.0	192.168.30.0	192.168.80.0
15.	192.168.31.0	192.168.32.0	192.168.81.0
16.	192.168.33.0	192.168.34.0	192.168.82.0
17.	192.168.35.0	192.168.36.0	192.168.83.0
18.	192.168.37.0	192.168.38.0	192.168.84.0
19.	192.168.39.0	192.168.40.0	192.168.85.0
20.	192.168.41.0	192.168.42.0	192.168.86.0
21.	192.168.43.0	192.168.44.0	192.168.87.0
22.	192.168.45.0	192.168.46.0	192.168.88.0
23.	192.168.47.0	192.168.48.0	192.168.89.0
24.	192.168.49.0	192.168.50.0	192.168.90.0
25.	192.168.51.0	192.168.52.0	192.168.91.0
26.	192.168.53.0	192.168.54.0	192.168.92.0
27.	192.168.55.0	192.168.56.0	192.168.93.0
28.	192.168.57.0	192.168.58.0	192.168.94.0
29.	192.168.59.0	192.168.60.0	192.168.95.0
30.	192.168.61.0	192.168.62.0	192.168.96.0
31.	192.168.63.0	192.168.64.0	192.168.97.0
32.	192.168.65.0	192.168.66.0	192.168.98.0

Для сервера DHCP підібрати довільну IP-адресу з пулу приватних IPv4-адрес і щоб вона не повторювала видані для vlan.

Лабораторна робота 11
Налаштування протоколу SSH для доступу до мережевого пристрою

Мета роботи: ознайомити студентів з налаштуванням протоколу SSH для доступу до мережевого пристрою на прикладі обладнання Cisco.

Завдання: виконати базове налаштування SSH на мережевому пристрої шляхом конфігурування відповідного інтерфейсу та параметрів доступу, створити облікові записи користувачів та задати відповідні параметри безпеки, перевірити працездатність SSH-з'єднання з різних клієнтських пристроїв за допомогою термінальних утиліт.

I. Налаштування маршрутизатора:

Завдання1:

1. опрацювати матеріал [7, 8]; з'єднати обладнання, як показано на схемі топології (рис. 1);

Топологія

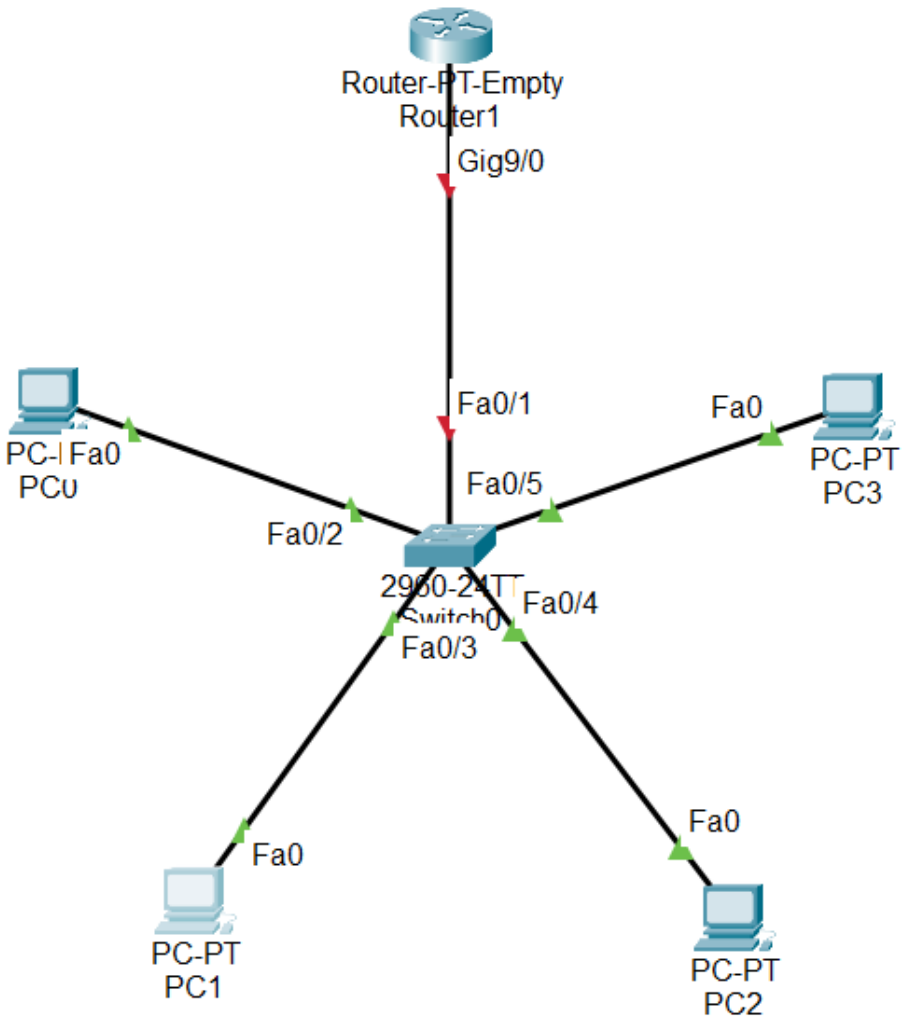


Рисунок 1 – Топологія мережі

2. комп'ютерам задати IP-адреси статично, адресу мережі обрати згідно варіату в таблиці 1, маска мережі 255.255.255.0 або /24;
3. дати ім'я маршрутизатору – прізвище студента;

Router(config)#hostname Karpenko

4. налаштувати інтерфейс на марштутизаторі (ввімкнути його та призначити IP-адресу). IP-адреса маршутизатора має бути перша хостова адреса. Адресу мережі обрати згідно варіату в таблиці 1. Маска мережі 255.255.255.0 або /24;

Karpenko(config)#interface g9/0
Karpenko(config-if)#ip address 192.168.1.1 255.255.255.0
Karpenko(config-if)#no shutdown
Karpenko#wr m
Building configuration...
[OK]

5. ввести команду **no ip domain-lookup** (для того, щоб маршрутизатор не реагував на невірно введені команди);

Karpenko(config)#no ip domain-lookup

6. надати ім'я домену командою **ip domain name Admin*ПрізвищеСтудента;***

Karpenko(config)#ip domain-name AdminKarpenko

7. створити логін і пароль, які будемо використовувати для авторизації на маршрутизаторі (в даній лабораторній роботі будемо використовувати пароль 123);

Karpenko(config)#username Admin password 123

8. зашифрувати паролі;

Karpenko(config)#service password-encryption

9. налаштувати пароль для захисту привілейованого режиму (в даній лабораторній роботі будемо використовувати пароль 123456);

Karpenko(config)#enable secret 123456

10. вибрати версію протоколу SSH – version 2;

Karpenko(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.

11. згенерувати ключ rsa 512 біт;

Karpenko(config)#crypto key generate rsa
The name for the keys will be: Karpenko.AdminKarpenko
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: **512**
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]
Karpenko(config)#

12. активувати службу aaa;

Karpenko(config)#aaa new-model

13. налаштувати інтерфейс vty;

Karpenko(config)#line vty 0 15
Karpenko(config-line)#transport input ssh

14. з будь якого комп'ютера з режиму командної стрічки перевірити досяжність маршрутизатора (пінг має бути вдалим) (рис. 2);

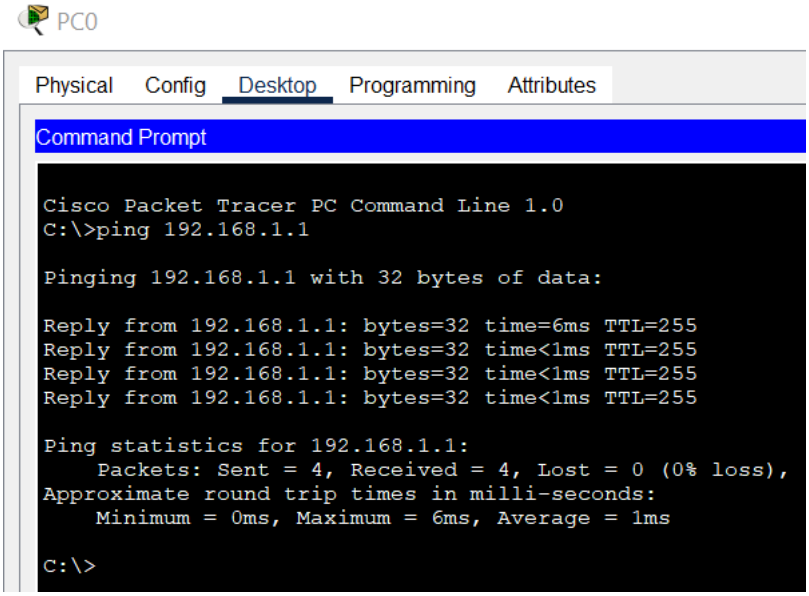


Рисунок 2 – Перевірка досяжності маршрутизатора з PC0

15. далі ввести команду logging synchronous, яка забороняє виведення будь-яких консольних повідомлень, які можуть перервати введення команд у консольному режимі;

Karpenko(config-line)#logging synchronous

16. ввести команду exec-timeout, яка означає, що при бездіяльності користувача протягом 5-ти (в даному прикладі обрано 5 хвилин) хвилин відбудеться процес розлогування;

Karpenko(config-line)#exec-timeout 5

17. ввійти на маршрутизатор з використанням команди ssh **C:\>ssh -l Admin 192.168.1.1** (рис. 3-4) та переглянути налаштування з використанням команди show startup-config (рис. 5), ввести пароль 123 для входу по ssh на маршрутизатор та пароль 123456 для входу в превілейований режим;

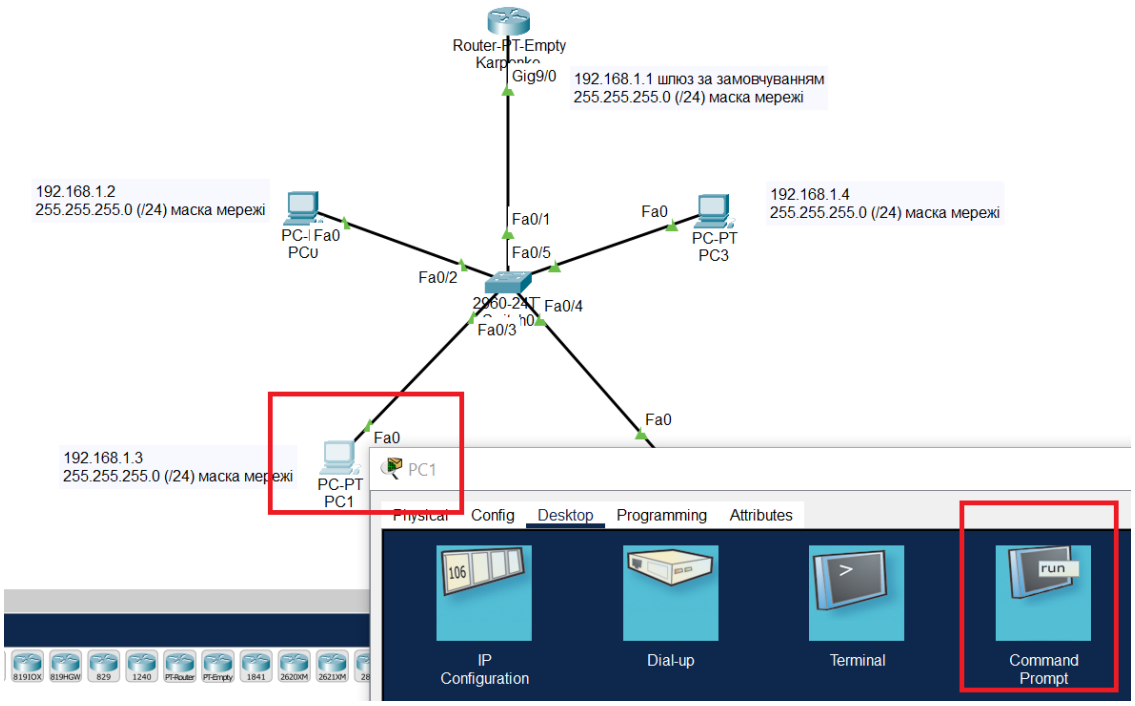


Рисунок 3 – Перевірка досяжності маршрутизатора з PC0

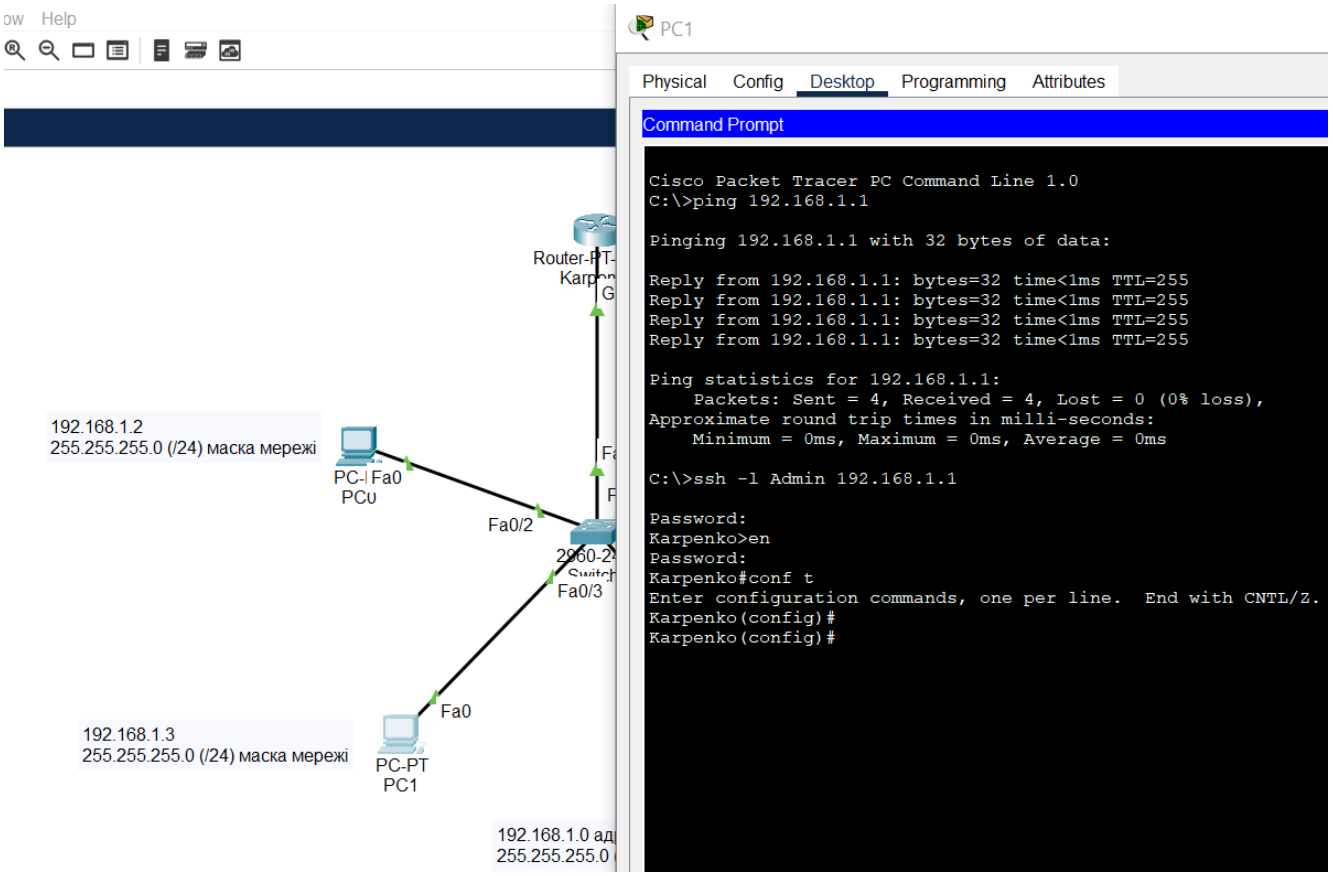


Рисунок 4 – Вхід на маршрутизатор з використанням команди ssh

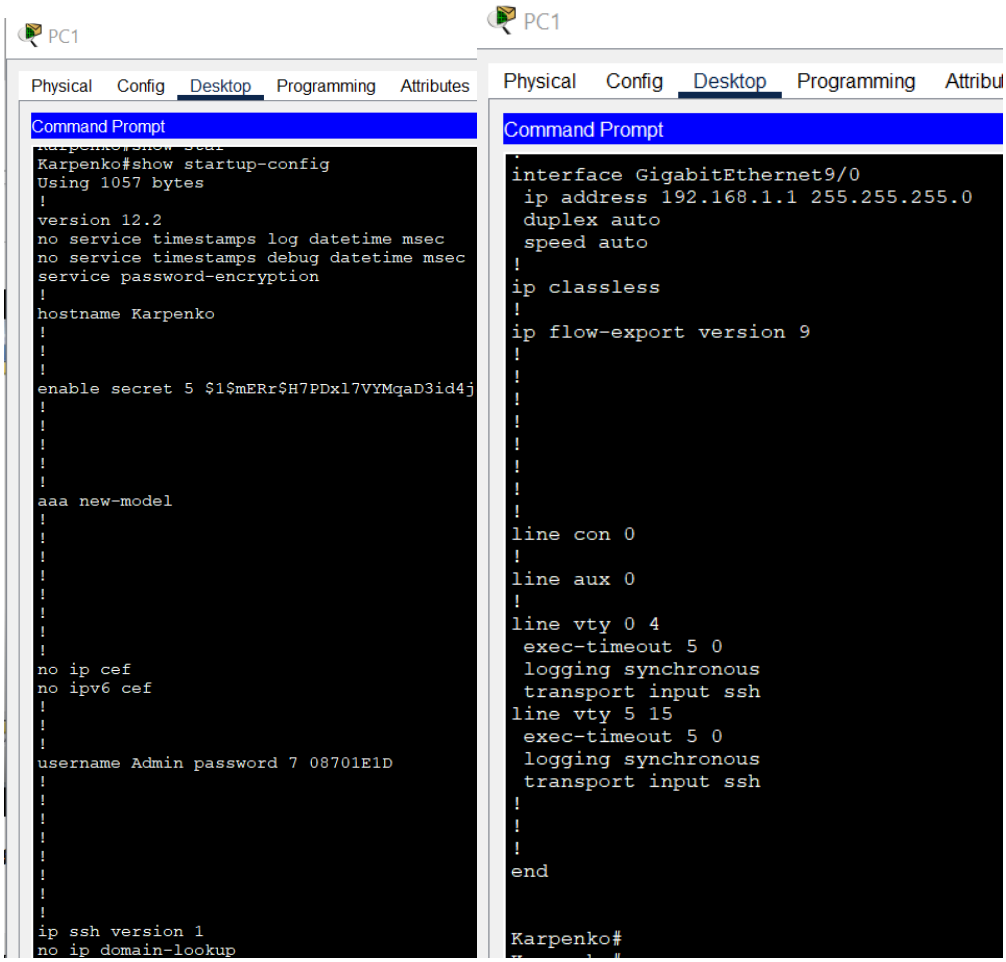


Рисунок 5 – Перегляд налаштувань

Завдання 2

1. З’єднати маршрутизатор та будь який комп’ютер консольним кабелем (рис. 6);

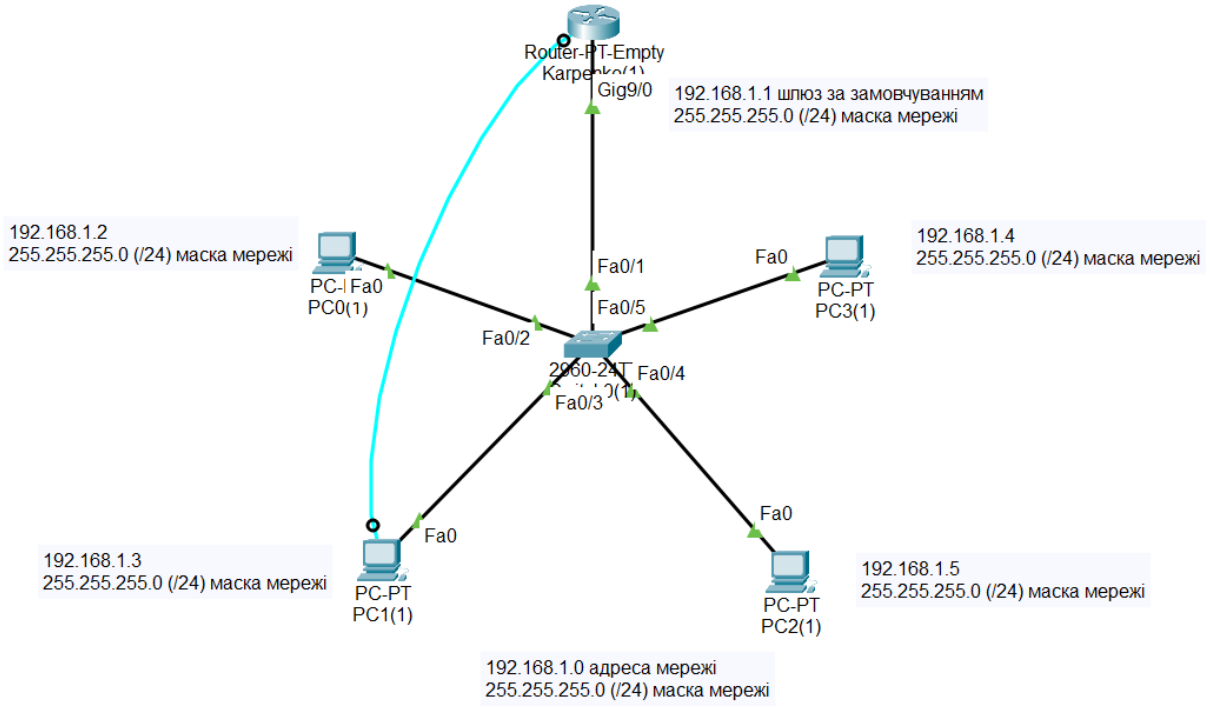


Рисунок 6 – Топологія мережі з консольним з’єднанням

2. ввійти в режим симуляції терміналу (рис. 7);

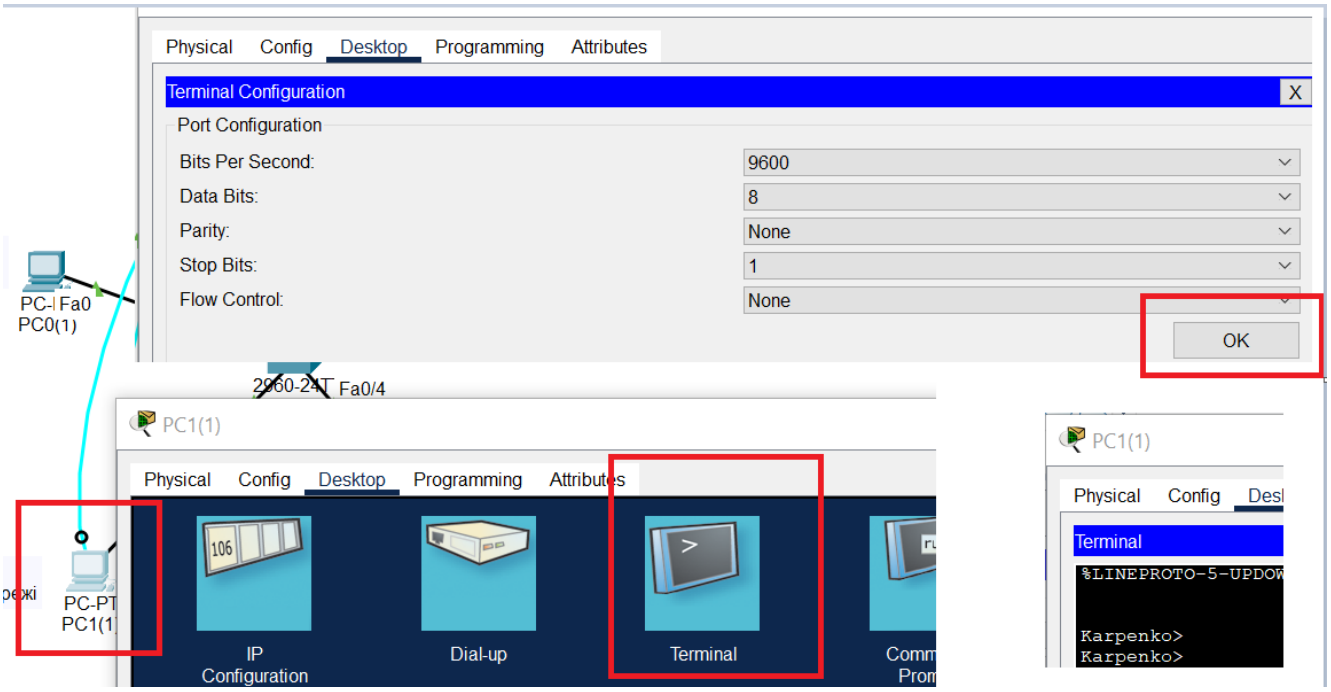


Рисунок 7 – Режим симуляції терміналу

3. захистити паролем вхід на пристрій по консолі (так як ввімкнено **aaa**, то в даному випадку команди будуть відрізнятись від стандартних команд, які призначенні для створення захисту по консольній лінії);

– створимо лист з логінами, які будуть використовуватись для авторизації на маршрутизаторі (Admin – назва листа)

Karpenko(config)#aaa authentication login Admin local

– налаштуємо пароль на вхід на пристрій по консолі

Karpenko(config)#line console 0

Karpenko(config-line)#login authentication Admin

Karpenko(config-line)#logging synchronous

4. ввести команду для розлогінювання через певний проміжок часу;

Karpenko(config-line)#exec-timeout 5

5. зайти на комп'ютера в режим емуляції терміналу, розлогінитись і перевірити чи пристрій буде запитувати пароль. Якщо налаштування виконані вірно, то пристрій запитає логін (в даному випадку Admin), пароль (в даному випадку 123) та пароль привілейованого режиму(в даному випадку 123456) (рис. 8).

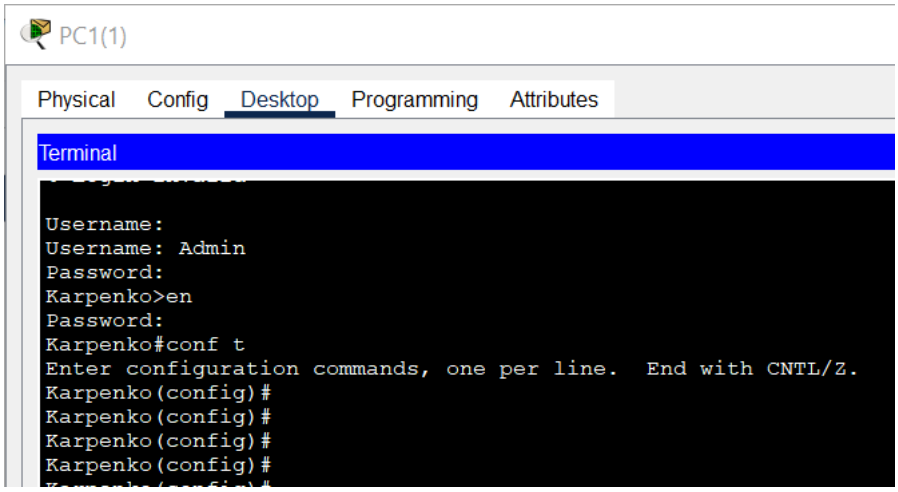


Рисунок 8 – Перевірка налаштувань пристрою

II. Налаштування комутатора

1. дати ім'я комутатору – ім'я студента (в даному прикладі Oleg);
2. створити vlan (назвати довільно), призначити IP-адресу та помісти в нього відповідні порти;

Oleg(config)#vlan 45

Oleg(config)#interface vlan 45

Oleg(config-if)#ip address 192.168.1.254 255.255.255.0

Oleg(config-if)#no shutdown

Oleg(config)#interface range fastEthernet 0/2-24

Oleg(config-if-range)#switchport mode access

Oleg(config-if-range)#switchport access vlan 45

3. перевірити чи є з'єднання між комп'ютерами та vlan 1 (пінг має бути вдалим, рис. 9);

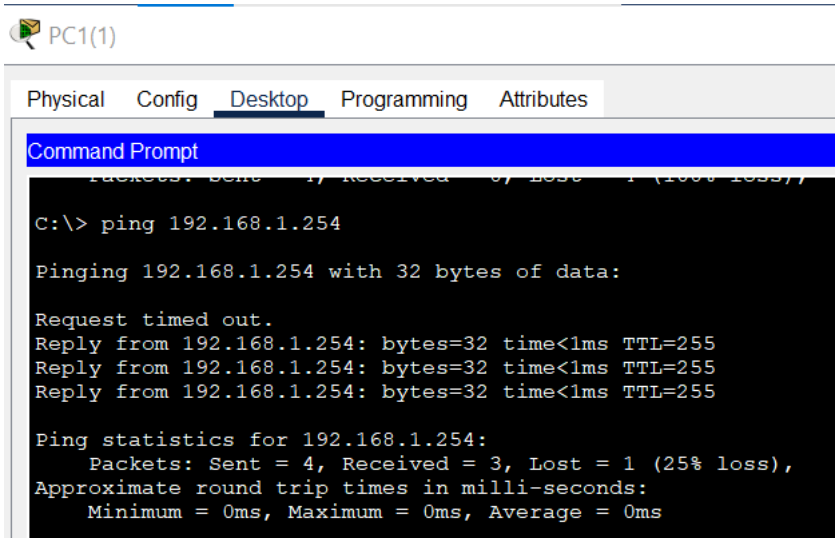


Рисунок 9 – Перевірка з'єднання між комп'ютерами та vlan 1

4. налаштувати протокол ssh. Спочатку вказати користувача, пароль, та створити домен;

Oleg(config)#username AdminKarpenko password 123

Oleg(config)#ip domain name AdminSwitch

5. налаштувати ssh командою:

Oleg(config)#ip ssh version 2

Please create RSA keys (of at least 768 bits size) to enable SSH v2

6. задати ключ 512:

Oleg(config)#crypto key generate rsa

(назва комутатора має бути – ім'я студента, потрібно було виконати на початку налаштувань)

Oleg(config)#crypto key generate rsa

The name for the keys will be: Oleg.AdminSwitch

Choose the size of the key modulus in the range of 360 to 4096 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: **512**

% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

Oleg(config)#

7. налаштувати інтерфейс;

Oleg(config-line)#line vty 0 15

Oleg(config-line)#transport input ssh

Oleg(config-line)#login local

Oleg(config-line)#logging synchronous

Oleg(config-line)#exec-timeout 5

8. перевірити підключення до комутатора за допомогою ssh (рис. 10):

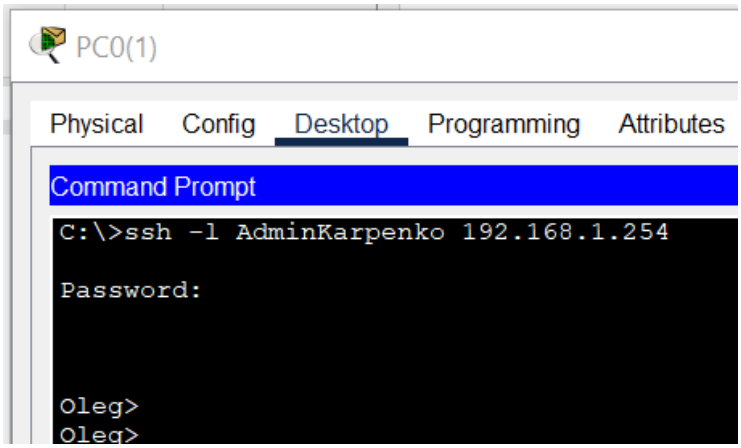


Рисунок 10 – Перевірка підключення до комутатора за допомогою ssh

Варіант завдання

Таблиця 1 – Варіанти завдань

Варіант	Мережева адреса	Варіант	Мережева адреса
1.	192.168.3.0	33	192.168.4.0
2.	192.168.5.0	34	192.168.6.0
3.	192.168.7.0	35	192.168.8.0
4.	192.168.9.0	36	192.168.10.0
5.	192.168.11.0	37	192.168.12.0
6.	192.168.13.0	38	192.168.14.0
7.	192.168.15.0	39	192.168.16.0
8.	192.168.17.0	40	192.168.18.0
9.	192.168.19.0	41	192.168.20.0
10.	192.168.21.0	42	192.168.22.0
11.	192.168.23.0	43	192.168.24.0
12.	192.168.25.0	44	192.168.26.0
13.	192.168.27.0	45	192.168.28.0
14.	192.168.29.0	46	192.168.30.0
15.	192.168.31.0	47	192.168.32.0
16.	192.168.33.0	48	192.168.34.0
17.	192.168.35.0	49	192.168.36.0
18.	192.168.37.0	50	192.168.38.0
19.	192.168.39.0	51	192.168.40.0
20.	192.168.41.0	52	192.168.42.0
21.	192.168.43.0	53	192.168.44.0
22.	192.168.45.0	54	192.168.46.0
23.	192.168.47.0	55	192.168.48.0
24.	192.168.49.0	56	192.168.50.0
25.	192.168.51.0	57	192.168.52.0
26.	192.168.53.0	58	192.168.54.0
27.	192.168.55.0	59	192.168.56.0
28.	192.168.57.0	60	192.168.58.0
29.	192.168.59.0	61	192.168.60.0
30.	192.168.61.0	62	192.168.62.0
31.	192.168.63.0	63	192.168.64.0
32.	192.168.65.0	64	192.168.66.0

Примітка. Комбінація клавіш **Ctrl Shift 6** – дозволяє користувачеві перервати процес IOS, наприклад, ping або traceroute.

Лабораторна робота 12
Відстеження DNS-перетворень

Мета роботи: набуття практичних навичок моніторингу та аналізу процесу перетворення доменних імен у IP-адреси за допомогою системи доменних імен (DNS), а також дослідження особливостей функціонування DNS-запитів і відповідей у комп'ютерній мережі шляхом використання мережевих утиліт і засобів трасування.

Завдання: зробити огляд перетворення за допомогою протоколу DNS URL-адреси на IP-адресу, дослідити DNS-пошук адреси веб-сайту та поштових серверів за допомогою команди nslookup.

Теоретичний матеріал

Система доменних імен (Domain Name System, DNS) викликається під час уведення в адресному рядку веб-браузера Уніфікованого покажчика ресурсів (Uniform Resource Locator, URL), наприклад **http://www.cisco.com**. Перша частина URL описує протокол, який використовується. Традиційно до них належать протокол передавання гіпертексту (HTTP), протокол передавання гіпертексту через рівень захищених сокетів (Secure Socket Layer, SSL) - (HTTPS) і протокол передавання файлів (FTP) [2].

DNS використовує другу частину URL-адреси, у даному прикладі - www.cisco.com. DNS перетворює доменне ім'я (www.cisco.com) на IP-адресу, щоб вихідний вузол зміг досягти кінцевого сервера. У цій лабораторній роботі ви матимете можливість спостерігати за протоколом DNS у дії і скористаєтесь командою **nslookup** (пошук сервера імен) для отримання додаткової інформації про DNS.

Необхідні ресурси

PC (Windows із доступом до Інтернету і режиму командного рядка)

Хід роботи

Спостереження за перетвореннями протоколу DNS URL-адрес на IP-адреси:

1) відкрийте вікно командного рядка Windows;

2) у командному рядку пропінгуйте URL-адресу Інтернет-корпорації з призначення імен і номерів (ICANN) за адресою **www.icann.org**. ICANN координує DNS, IP-адреси, системи керування доменними іменами верхнього рівня та функції керування кореневими серверами. Комп'ютеру потрібно перетворити cisco.com на IP-адресу, щоб знати, куди надсилати пакети Інтернет-протоколу керуючих повідомлень (Internet Control Message Protocol, ICMP).

Перший рядок виводу відображає виконане за допомогою DNS перетворення **www.icann.org** на IP-адресу (рис. 1). Результат роботи DNS повинен бути доступний для перегляду, навіть якщо у вашому закладі використовується міжмережний екран, який запобігає пінгуванню, або якщо сервер призначення забороняє звертатися за допомогою команди ping до свого веб-сервера.

Примітка. Якщо ім’я домену перетворюється на адресу IPv6, використовуйте команду **ping -4 www.icann.org** для переходу на адресу IPv4, якщо потрібно.

```
C:\ > ping www.icann.org

Pinging www.vip.icann.org [2620:0:2d0:200::7] with 32 bytes of data:
Reply from 2620:0:2d0:200::7: time=43ms
Reply from 2620:0:2d0:200::7: time=41ms
Reply from 2620:0:2d0:200::7: time=44ms
Reply from 2620:0:2d0:200::7: time=39ms

Ping statistics for 2620:0:2d0:200::7:
      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 44ms, Average = 41ms

C:\> ping -4 www.icann.org

Pinging www.vip.icann.org [192.0.32.7] with 32 bytes of data:
Reply from 192.0.32.7: bytes=32 time=41ms TTL=241
Reply from 192.0.32.7: bytes=32 time=42ms TTL=241
Reply from 192.0.32.7: bytes=32 time=42ms TTL=241
Reply from 192.0.32.7: bytes=32 time=43ms TTL=241

Ping statistics for 192.0.32.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 41ms, Maximum = 43ms, Average = 42ms
```

Рисунок 1 − Виконане за допомогою DNS перетворення

Дайте відповідь на запитання. Запишіть IP-адреси для www.icann.org.

3) замість URL-адреси використайте для звернення у веб-браузері адреси IPv4 з пункту 2. Введіть **https://192.0.32.7** у веб-браузері. Якщо вдалося отримати IPv6-адресу, її також можна застосувати: **https://[2620:0:2d0:200::7]**.

4) зверніть увагу, що домашня веб-сторінка ICANN відображається без використання DNS. Людям здебільшого легше запам’ятовувати слова, аніж цифри. Якщо ви скажете комусь перейти на **www.icann.org**, вони, ймовірно, пам’ятатимуть саме цю адресу, а не 192.0.32.7, яка, мабуть, важча для сприйняття. Комп’ютери оперують числами. DNS − це процес перекладу слів у числа. Окрім цього, має місце ще одне перетворення інформації. Люди сприймають десяткові числа. Комп’ютери обробляють дані у двійковому форматі. Десяткова IP-адреса 192.0.32.7 у двійковому форматі має вигляд 11000000.00000000.00100000.00000111.

Дайте відповідь на запитання. Що станеться, якщо скопіювати ці двійкові значення і використати їх у браузері?

4) у режимі командного рядка пропінгуйте **www.cisco.com** (рис. 2).

***Примітка**:* Якщо для доменного імені визначено адресу IPv6, скористайтесь командою **ping -4 www.cisco.com** для перетворення на IPv4, якщо потрібно.

C:\> ping www.cisco.com

```
C:\> ping www.cisco.com

Pinging origin-www.cisco.com [2600:1408:7:1:9300::90] with 32 bytes of data:
Reply from 2600:1408:7:1:9300::90: time=70ms
Reply from 2600:1408:7:1:9300::90: time=74ms
Reply from 2600:1408:7:1:9300::90: time=72ms
Reply from 2600:1408:7:1:9300::90: time=71ms

Ping statistics for 2600:1408:7:1:9300::90:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 70ms, Maximum = 74ms, Average = 71ms
C:\> ping -4 www.cisco.com

Pinging e2867.dsca.akamaiedge.net [172.230.155.162] with 32 bytes of data:
Reply from 172.230.155.162: bytes=32 time=7ms TTL=54
Reply from 172.230.155.162: bytes=32 time=6ms TTL=54
Reply from 172.230.155.162: bytes=32 time=7ms TTL=54
Reply from 172.230.155.162: bytes=32 time=6ms TTL=54

Ping statistics for 172.230.155.162:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Рисунок 2 – Перевірка з’єднання з www.cisco.com

Дайте відповідь на запитання. 1. При використанні команди ping www.cisco.com чи отримали ви таку ж IP-адресу, що й у прикладі? Поясніть. 2. У адресному рядку браузера введіть IP-адресу, яку ви отримали при пінгуванні www.cisco.com. Чи відображається веб-сайт? Поясніть.

5) дослідження DNS-пошуку адреси веб-сайту за допомогою команди nslookup:

– у командному рядку введіть команду nslookup. Ваш результат може відрізнятися від наведеного у прикладі.

```
C:\> nslookup
Default Server: one.one.one.one
Address: 1.1.1.1
```

Рисунок 3 – Результат виконання команди nslookup

Дайте відповідь на запитання. Який DNS-сервер використовується за замовчуванням?

6) зверніть увагу на зміну позначки командного рядка на більше (>). Це ознака команди nslookup. З появою цієї позначки можна вводити команди, пов'язані з DNS. У полі курсора введіть ? для перегляду списку всіх команд, доступних для використання у режимі nslookup .

Введіть **www.cisco.com** (рис. 4).

```
> www.cisco.com
Default Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
Name: e2867.dsca.akamaiedge.net
Addresses: 2600:1404:a:395::b33
          2600:1404:a:38e:b33
          172.230.155.162
Aliases: www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgikey.net
          wwwds.cisco.com.edgakey.net.globalredir.akadns.net
```

Рисунок 3 – Результат виконання команди www.cisco.com

Дайте відповідь на запитання. Яка адреса IPv4 відповідає уведеному доменному імені? (Для визначеного розташування, 172.230.155.162).

Примітка. IP-адреса, що відповідає вашому розташуванню, найімовірніше, буде відрізнятися, оскільки Cisco використовує дзеркальні сервери у різних локаціях по всьому світу.

Дайте відповідь на запитання. Чи збігається вона з IP-адресою, виявленою за допомогою команди **ping**?

Окрім IP-адреси 172.230.155.162, відображаються такі числа: 2600:1404:a:395::b33 і 2600:1404:a:38e::b33. Що вони позначають?

7) У режимі nslookup введіть IP-адресу веб-сервера Cisco, яку ви щойно виявили. За допомогою **nslookup** можна отримати доменне ім'я, якщо URL-адреса вам невідома.

> **172.230.155.162**
Default Server: one.one.one.one
Address: 1.1.1.1

Name: a172-230-155-162.deploy.static.akamaitechnologies.com
Address: 172.230.155.162

Інструмент **nslookup** можна використовувати для перетворення доменних імен на IP-адреси. Також він дозволяє виконувати зворотні перетворення IP-адрес на доменні імена.

Дайте відповідь на питання. Використовуючи інструмент **nslookup**, запишіть IP-адреси, пов'язані з **www.google.com**.

6) дослідження DNS-пошуку поштових серверів за допомогою команди nslookup:

– у режимі nslookup введіть **set type=mx**, щоб використати nslookup для визначення поштових серверів:

> **set type=mx**

– у режимі nslookup введіть cisco.com (рис. 4):

```
> cisco.com
Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
cisco.com MX preference = 20, mail exchanger = rcdn-mx-01.cisco.com
cisco.com MX preference = 30, mail exchanger = aer-mx-01.cisco.com
cisco.com MX preference = 10, mail exchanger = alln-mx-01.cisco.com
```

Рисунок 4 – Результат виконання команди www.cisco.com

Резервування (налаштування більше одного поштового сервера) є одним з основоположних принципів побудови мережі. За його впровадження, у разі відмови одного з поштових серверів, комп'ютер намагається звернутися із запитом до іншого поштового сервера. Адміністратори електронної пошти використовують параметр MX preference аби визначити, до якого поштового сервера слід звертатися у першу чергу. Насамперед звертаються до поштового сервера з найнижчим показником MX preference.

Дайте відповідь на запитання. Беручи до уваги отримані вище дані, до якого поштового сервера спершу йтиме звернення при надсиланні листа до cisco.com?

– у режимі nslookup введіть, щоб повернутися до звичайного режиму командного рядка ПК;

– введіть ipconfig /all.

Дайте відповідь на питання. Запишіть IP-адреси усіх DNS-серверів, які використовує ваш навчальний заклад. Яке основне призначення DNS
?

Оформіть звіт до роботи.

Лабораторна робота 13
Базові налаштування протоколу OSPF

Мета роботи: засвоїти принципи роботи протоколу внутрішньої маршрутизації OSPF у межах однієї зони, навчитися здійснювати базове конфігурування маршрутизаторів для обміну маршрутною інформацією.

Завдання: реалізувати OSPF для однієї зони у мережах типу «точка-точка» (рис. 1, табл. 1).

Хід роботи

Опрацюйте матеріал [9, 10]. Протоколи динамічної маршрутизації дають змогу обмінюватися маршрутами автоматично, спрощуючи обслуговування мереж. Також динамічні протоколи маршрутизації самі визначають оптимальний маршрут для надсилання пакетів (можна впливати на це за потреби) і обирати альтернативний маршрут у разі падіння якогось каналу (рис. 1, табл. 1).

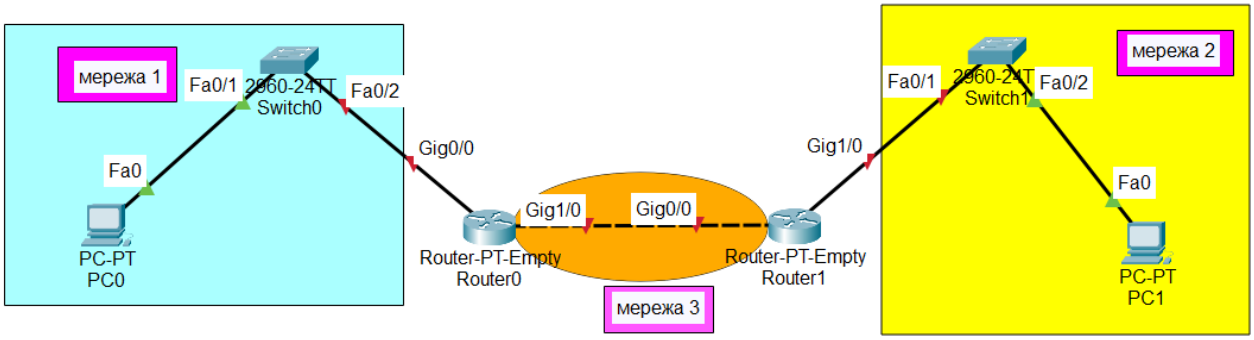


Рисунок 1 – Топологія мережі

Налаштувати функціонування протоколу маршрутизації OSPF згідно варіанту, наведеному в таблиці 1.

…

Router>enable

Router#configure terminal

Router(config)#router ospf 1 (*запуск процесу ospf*)

*Остання цифра, в даному випадку **1**, – це ідентифікатор процесу, який може відрізнятися для різних маршрутизаторів. Для зручності краще використовувати один і той самий номер. Різні ідентифікатори потрібні для того, щоб можна було на одному девайсі запускати кілька процесів ospf. [http://surl.li/tmval]*

Router(config)# router-id 1.1.1.1

Команда router-id необхідна для ідентифікації маршрутизатора серед інших маршрутизаторів OSPF.

Router(config-router)#network *номер мережі інверсна маска* area *номер зони*

Наприклад:

Router(config-router)#network 195.168.2.0 0.0.0.3 area 0

За допомогою команди network можна зробити дві речі: вказати, які мережі потрібно оголосити іншим маршрутизаторам через OSPF, і які інтерфейси будуть використовуватися для надсилання hello-пакетів.

Router(config-router)#exit

Router(config)#exit

Router #wr m

Маршрутизатор буде автоматично розсилати пакети також і в сторону підмережі. З точки зору безпеки не коректно розсилати службову інформацію в сторону користувачів.

Для заборони відносин суміжності із сусідніми пристроями можна використовувати команду passive-interface. Існують дві основні причини включення команди passive-interface:

– заборонити небажаний трафік оновлення, наприклад коли інтерфейс є інтерфейсом локальної мережі без інших підключених маршрутизаторів;

– покращити елементи безпеки, наприклад, забороняючи невідомим стороннім пристроям маршрутизації отримувати оновлення *ospf*.

Router(config-router)#passive-interface interface-type interface-number

Наприклад:

Router(config-router)#passive-interface gigabitEthernet 0/0/0

Після налаштування маршрутизації, виконавши команду, **#show ip route,** отримаємо орієнтовно такий результат (рис. 2).

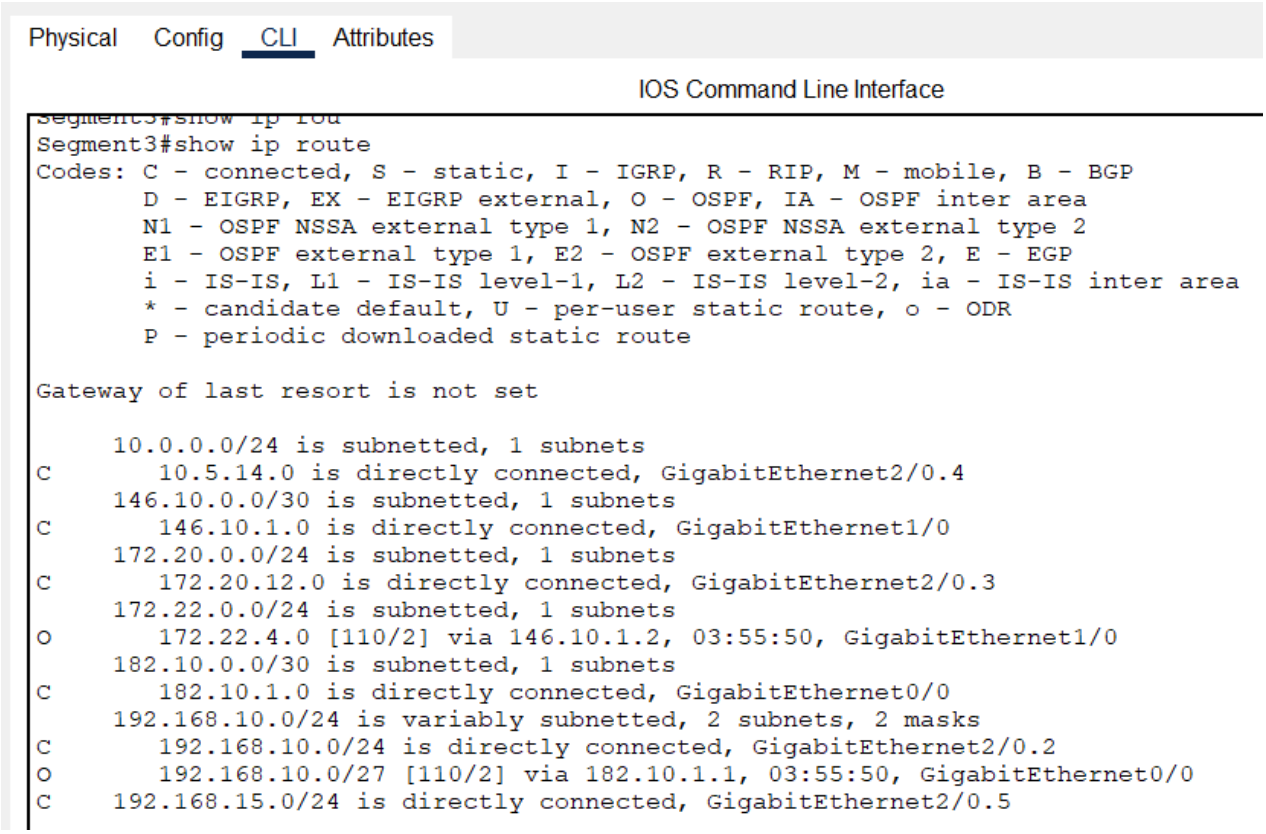


Рисунок 2 – Таблиця маршрутизації

В звіті до роботи вивести результат виконання команди на кожному маршрутизаторі, як показвно на рисунку 2.

Варіант завдання

Таблиця 1 – Варіанти завдань

№	Мережева адреса мережі 1, маска /24	Мережева адреса мережі 2, маска /24	Мережева адреса мережі 3, маска /30
1	10.172.33.0	192.168.14.0	18.219.45.0
2	10.5.200.0	192.168.1.0	142.250.180.0
3	10.200.15.0	192.168.20.0	52.47.23.0
4	10.100.1.0	192.168.55.0	185.199.109.0
5	10.34.78.0	192.168.7.0	93.184.220.0
6	10.0.45.0	192.168.5.0	64.233.191.0
7	10.250.33.0	192.168.10.0	9.2.4.0
8	10.111.22.0	192.168.200.0	216.58.209.0
9	10.23.65.0	192.168.31.0	198.51.100.0
10	10.10.10.0	192.168.19.0	7.4.1.0
11	10.3.3.0	192.168.12.0	17.172.224.0
12	10.143.144.0	192.168.88.0	40.112.72.0
13	10.77.66.0	192.168.3.0	52.94.225.0
14	10.123.45.0	192.168.24.0	91.198.174.0
15	10.9.8.0	192.168.77.0	208.80.154.0
16	10.9.8.0	192.168.42.0	185.60.216.0
17	10.222.10.0	192.168.99.0	44.240.60.0
18	10.19.19.0	192.168.2.0	157.240.22.0
19	10.101.102.0	192.168.17.0	52.109.76.0
20	10.202.203.0	192.168.5.0	185.199.108.0
21	10.255.255.0	192.168.25.0	31.13.71.0
22	10.66.77.0	192.168.21.0	13.107.246.0
23	10.1.2.0	192.168.4.0	172.217.5.0
24	10.210.22.0	192.168.21.0	203.0.113.0
25	10.98.99.0	192.168.12.0	23.45.67.0
26	10.88.77.0	192.168.55.0	20.49.104.0
27	10.190.180.0	192.168.32.0	13.35.15.0
28	10.75.64.0	192.168.14.0	69.63.176.0
29	10.33.44.0	192.168.111.0	52.216.22.0
30	10.200.200.0	192.168.69.0	18.164.118.0
31	10.101.100.0	192.168.16.0	104.244.42.0
32	10.61.62.0	192.168.6.0	13.230.60.0

Лабораторна робота 14
Налаштування протоколу OSPF у межах однієї зони

Мета роботи: засвоїти принципи роботи протоколу внутрішньої маршрутизації OSPF у межах однієї зони, навчитися здійснювати базове конфігурування маршрутизаторів для обміну маршрутною інформацією.

Завдання: реалізувати OSPF для однієї зони у мережах типу «точка-точка» і широкомовних мережах з множинним доступом (рис. 1) [11].

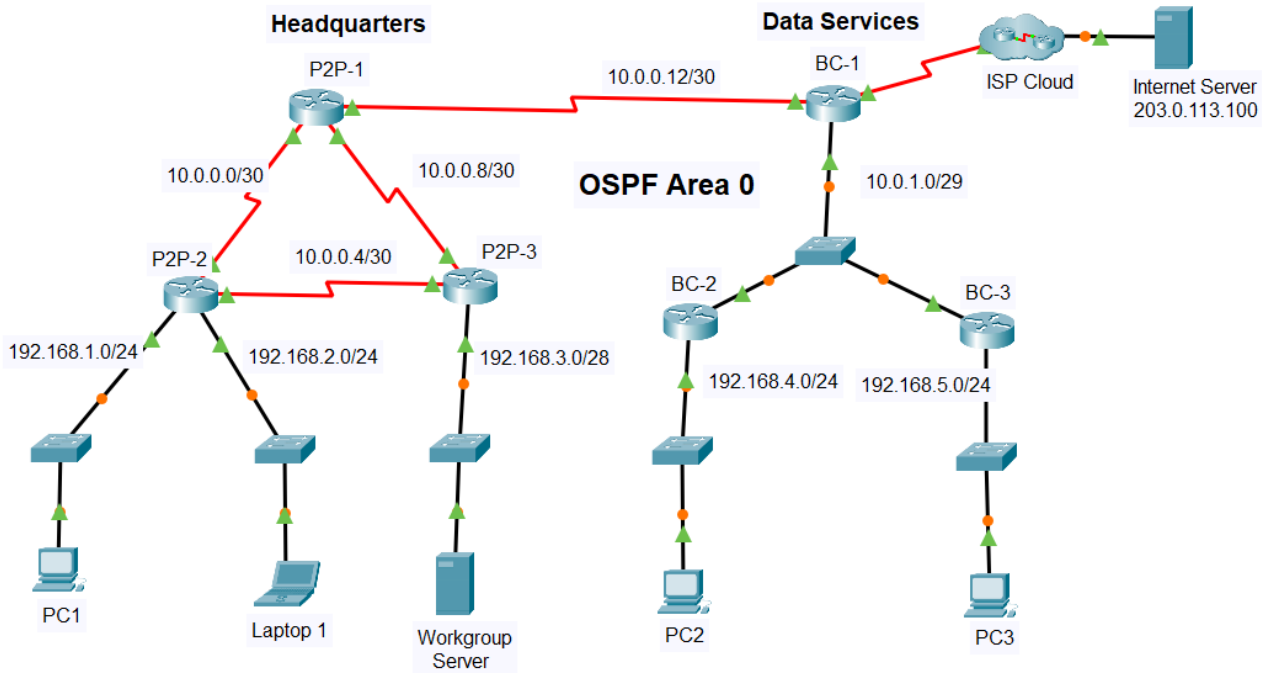


Рисунок 1 – Топологія мережі

Таблиця 1 – Таблиця адресації

Пристрій	Інтерфейс	IP-адреса/Префікс
P2P-1	S0/1/0	10.0.0.1/30
P2P-1	S0/1/1	10.0.0.9/30
P2P-1	S0/2/0	10.0.0.13/30
P2P-2	S0/1/0	10.0.0.2/30
P2P-2	S0/1/1	10.0.0.5/30
P2P-2	G0/0/0	192.168.1.1/24
P2P-2	G0/0/1	192.168.2.1/24
P2P-3	S0/1/0	10.0.0.6/30
P2P-3	S0/1/1	10.0.0.10/30

Продовження таблиці 1

Пристрій	Інтерфейс	IP-адреса/Префікс
P2P-3	G0/0/0	192.168.3.1/28
BC-1	S0/1/0	10.0.0.14/30
BC-1	S0/1/1	64.0.100.2/30
BC-1	G0/0/0	10.0.1.1/29
BC-2	G0/0/0	192.168.4.1/30
BC-2	G0/0/1	10.0.1.2/29
BC-3	G0/0/0	192.168.5.1/24
BC-3	G0/0/1	10.0.1.3/29
Internet Server	NIC	203.0.113.100/24
PC 1	NIC	192.168.1.10/24
Laptop 1	NIC	192.168.2.20/24
Workgroup Server	NIC	192.168.3.14/28
PC 2	NIC	192.168.4.40/24
PC 3	NIC	192.168.5.50/24

Потрібно протестувати налаштований OSPF, створивши мережу в лабораторії за місцем роботи. Після під'єднання пристроїв, налаштування інтерфейсів має бути зв'язок у локальних мережах. Задача полягає в тому, щоб завершити налаштування OSPF відповідно до вимог.

Скористайтеся наданою інформацією та списком вимог для налаштування тестової мережі. У разі успішного завершення, всі вузли повинні мати можливість пінгувати інтернет-сервер.

Хід роботи

1) Використовуйте ID процесу 10 для активації OSPF на всіх маршрутизаторах.

2) Активуйте OSPF за допомогою команди network та шаблонних масок на маршрутизаторах в мережі "Headquarters".

3) Активуйте OSPF, налаштувавши необхідні інтерфейси мережних пристроїв в мережі Data Service.

4) Налаштуйте ідентифікатори маршрутизаторів на мережних маршрутизаторах з множинним доступом:

– BC-1: 6.6.6.6;

– BC-2: 5.5.5.5;

– BC-3: 4.4.4.4.

5) Налаштуйте OSPF так, щоб оновлення маршрутизації не надсилалися в мережі, де вони не потрібні.

6) Налаштуйте маршрутизатор BC-1 з найвищим пріоритетом інтерфейсу OSPF так, щоб він завжди був призначеним маршрутизатором в мережі з множинним доступом.

7) Налаштуйте маршрут за замовчуванням до ISP cloud, використовуючи в якості аргументу команди вихідний інтерфейс.

8) Автоматично анонсуйте маршрут за замовчуванням на всі маршрутизатори в мережі.

9) Налаштуйте маршрутизатори OSPF так, щоб вартість інтерфейсу Gigabit Ethernet становила 10, а вартість Fast Ethernet - 100.

10) Налаштуйте значення вартості OSPF для інтерфейсу Serial0/1/1 маршрутизатора P2P-1 − 50.

11) Налаштуйте для інтерфейсів, які з’єднують P2P-1 та BC-1, значення таймерів hello та dead в двічі більшими значень за замовчуванням.

Лабораторна робота 15
Налаштування бездротової мережі

Мета роботи: отримати навички налаштування бездротового маршрутизатора і точки доступу для обслуговування бездротових клієнтів і забезпечення маршрутизації IP-пакетів.

Завдання: під'єднати та налаштувати бездротовий маршрутизатор, під'єднати дротовий пристрій до бездротового маршрутизатора, додати точки доступу до мережі для розширення покриття бездротової мережі (рис. 1)[3].

Хід роботи

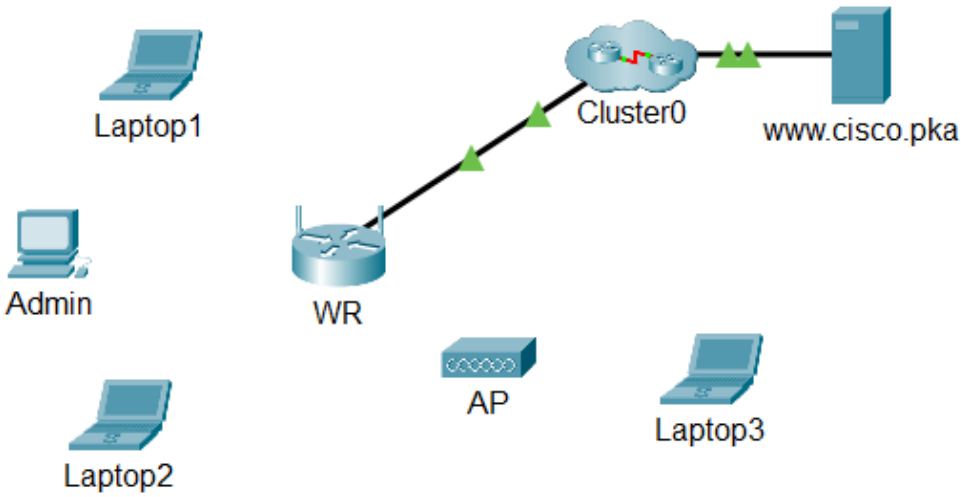


Рисунок 1 – Топологія мережі

Під'єднання до бездротового маршрутизатора

1) під'єднайте комп'ютер Admin до бездротового маршрутизатора WR:

– під'єднайте Admin до WR, використовуючи прямий кабель Ethernet, через порти Ethernet. У нижньому лівому куті екрану середовища Packet Tracer виберіть піктограму блискавки − пункт Connections (з'єднання). Виберіть кабель Copper Straight-Through (мідний прямий), зображений у вигляді суцільної чорної лінії.

– коли курсор перейде в режим приєднання, натисніть на Admin і виберіть FastEthernet0. Натисніть на WR і виберіть доступний порт Ethernet, щоб під'єднати інший кінець кабеля;

– WR працюватиме як комутатор для пристроїв, під'єднаних до локальної мережі, і як маршрутизатор для з'єднання з Інтернетом. Комп'ютер Admin тепер під'єднаний до мережі LAN (GigabitEthernet 1). Коли у вікні Packet Tracer з'являться зелені трикутники з обох сторін з'єднання між Admin та WR, переходьте до наступного кроку.

Примітка. Якщо зелених трикутників немає, переконайтесь, що вибрано Show Link Lights (показувати індикатори з'єднання) в меню Options (Сервіс) >

Preferences (параметри). Можна також натиснути на Fast Forward Time (прискорити) прямо над вікном Connections (з'єднання) на жовтій панелі.

2) налаштуйте комп'ютер Admin для використання протоколу DHCP:

– щоб потрапити на сторінку керування WR, комп'ютер Admin повинен бути під'єднаний до мережі. Бездротовий маршрутизатор зазвичай виконує функції DHCP-сервера, який за замовчуванням увімкнений у мережі LAN. Admin отримає інформацію про IP-адресу від DHCP-сервера на маршрутизаторі WR:

– натисніть на Admin і виберіть вкладку Desktop (робочий стіл);

– натисніть на IP Configuration (налаштування IP-адреси) і виберіть DHCP.

Дайте відповідь на запитання. Яка IP-адреса у даного комп'ютера? Яка маска підмережі у даного комп'ютера? Яка адреса шлюзу за замовчуванням (default gateway) у даного комп'ютера?

– закрийте вікно IP Configuration (Налаштування IP-адреси).

Примітка. Значення можуть змінюватися у межах діапазону адрес мережі при нормальній роботі DHCP.

3) під'єднайтесь до веб-інтерфейсу WR:

– на вкладці Desktop (робочий стіл) на комп'ютері Admin виберіть Web Browser;

– в поле URL-адреси введіть 192.168.0.1, щоб відкрити веб-сторінку налаштування бездротового маршрутизатора;

– введіть admin як ім'я користувача та пароль;

– під заголовком Network Setup (налаштування мережі) на сторінці Basic Setup (базове налаштування) перегляньте діапазон IP-адрес DHCP-сервера.

Дайте відповідь на запитання. Чи знаходиться IP-адреса комп'ютера Admin в цьому діапазоні? Чи повинна знаходитись?

4) налаштуйте Інтернет-порт маршрутизатора WR *(*цей крок передбачає налаштування маршрутизації на маршрутизаторі WR для надсилання пакетів від бездротових клієнтів до Інтернету. Для цього необхідно налаштувати порт Internet на маршрутизаторі WR):

– на вкладці Internet Setup (налаштування Інтернет-з'єднання)у верхній частині сторінки Basic Setup (базове налаштування) змініть спосіб налаштування IP-адреси Internet з Automatic Configuration – DHCP (автоматичне налаштування - DHCP) на Static IP (татична IP-адреса).

– введіть IP-адресу, щоб призначити її Інтернет-інтерфейсу:

Internet IP Address (IP-адреса Internet): 209.165.c200.225
Subnet Mask (маска підмережі): 255.255.255.252
Default Gateway (шлюз за замовчуванням): 209.165.200.226
DNS Server (DNS-сервер): 209.165.201.1

– прокрутіть донизу сторінки та натисніть Save Settings (зберегти параметри);

Примітка. При отриманні повідомлення Request Timeout закрийте вікно Admin і дочекайтеся, коли помаранчеві індикатори перетворяться на зелені трикутники. Щоб прискорити процес, натисніть на кнопку перемотування вперед. Потім знову під'єднайтеся до маршрутизатора WR з веб-браузера Admin, виконавши процедуру, описану в пункті 3.

– щоб перевірити з'єднання, відкрийте новий веб-браузер і перейдіть на сервер www.cisco.pka.

Примітка. Під'єднання до мережі може тривати кілька секунд. Для прискорення процесу натисніть Fast Forward Time (Прискорення) або Alt + D.

5) налаштування параметрів бездротового з'єднання *(в* цьому завданні ви налаштуєте параметри бездротового з'єднання суто для частоти 2,4 ГГц). ***Налаштуйте ідентифікатор SSID маршрутизатора WR:***

– перейдіть у графічний інтерфейс WR на 192.168.0.1 у веб-браузері комп'ютера Admin;

– перейдіть до Wireless (бездротове з'єднання) > Basic Wireless Settings (основні параметри бездротової мережі);

– змініть Network Name (SSID) на aCompany тільки для частоти 2,4 ГГц. Зверніть увагу, що ідентифікатор SSID чутливий до регістру;

– змініть Standard Channel на 6 – 2.437 GHz;

– у цьому завданні вимкніть обидві частоти 5 ГГц. Інші параметри залишіть без змін;

– прокрутіть донизу вікна і натисніть Save Settings (зберегти параметри).

6) налаштуйте параметри безпеки бездротового зв'язку (у цьому завданні ви налаштуєте параметри безпеки бездротової мережі, використовуючи режим безпеки WPA2 з шифруванням і парольною фразою):

– перейдіть до Wireless (бездротове з'єднання)> Wireless Security (безпека бездротової мережі);

– під заголовком 2.4 GHz виберіть для режиму безпеки Security Mode налаштування WPA2 Personal;

– у полі Encryption (шифрування) залишіть налаштування за замовчуванням AES;

– у полі Passphrase введіть парольну фразу Cisco123!;

– натисніть Save Settings (зберегти параметри);

– перевірте, чи налаштування на сторінках базових параметрів бездротового доступу Basic Wireless Settings і безпеки бездротового доступу Wireless Security правильні та збережені;

7) під'єднайте бездротових клієнтів:

– відкрийте Laptop1. Виберіть вкладку Desktop. Натисніть на PC Wireless;

– виберіть вкладку Connect. За необхідності натисніть Refresh. Виберіть ім'я бездротової мережі aCompany;

– введіть пароль або парольну фразу, налаштовану на попередньому кроці. Введіть Cisco123! у полі PSK (наперед визначений спільний ключ, Pre-Shared Key) і натисніть Connect. Закрийте вікно PC Wireless;

– відкрийте веб-браузер і переконайтесь, що ви можете перейти на сервер www.cisco.pka;

– повторіть наведені вище кроки для під'єднання ноутбука Laptop2 до бездротової мережі;

7) під'єднання бездротових клієнтів до точки доступу (точка доступу (Access Point, AP) − це пристрій, що дозволяє розширити покриття локальної бездротової мережі. Точка доступу під'єднується до дротового маршрутизатора

за допомогою кабелю Ethernet, щоб передавати сигнал у потрібне місце). ***Налаштуйте точку доступу:***

– з'єднайте Port 0 точки доступу AP з доступним портом Ethernet бездротового маршрутизатора WR за допомогою прямого кабелю Ethernet;

– натисніть на AP. Виберіть вкладку Config;

– під заголовком INTERFACE виберіть Port 1;

– у поле SSID введіть aCompany;

– виберіть WPA2-PSK. Введіть парольну фразу Cisco123! у полі Pass Phrase;

– залишіть AES як метод шифрування Encryption Type за замовчуванням.

8) під'єднайте бездротових клієнтів:

– відкрийте Laptop3. Виберіть вкладку Desktop. Натисніть PC Wireless;

– виберіть вкладку Connect. За необхідності натисніть Refresh. Виберіть ім'я бездротової мережі Wireless Network Name aCompany з найсильнішим сигналом (Channel 1) і натисніть Connect;

– відкрийте веб-браузер і перевірте, чи можете ви перейти на сервер www.cisco.pka.

9) змініть пароль доступу до WR:

– перейдіть у графічний інтерфейс WR на 192.168.0.1;

– перейдіть до Administration > Management і змініть поточний пароль маршрутизатора Router Password на cisco;

– прокрутіть донизу вікна і натисніть Save Settings;

– для входу на бездротовий маршрутизатор використовуйте ім'я користувача admin і новий пароль cisco. Натисніть OK, щоб продовжити;

– натисніть Continue і перейдіть до наступного кроку;

9)змініть діапазон DHCP-адрес на маршрутизаторі WR (у цьому завданні потрібно змінити внутрішню мережну адресу з 192.168.0.0/24 на 192.168.50.0/24. Під час зміни мережної адреси LAN необхідно оновити IP-адреси пристроїв у мережах LAN і WLAN, щоб нові IP-адреси були отримані до закінчення терміну оренди)**:**

– перейдіть у Setup > Basic Setup;

– прокрутіть вниз сторінки до параметрів налаштування мережі Network Setup;

– маршрутизатору Router IP призначено IP-адресу 192.168.0.1. Змініть її на 192.168.50.1. Перевірте, чи IP-адреси починаються з .100, а в пулі DHCP є 50 IP-адрес;

– додайте до налаштувань DHCP адресу DNS-сервера 209.165.201.1;

– прокрутіть донизу вікна і натисніть Save Settings;

Дайте відповідь на запитання. Зверніть увагу, що діапазон адрес DHCP був автоматично оновлений відповідно до зміни IP-адреси. Невдовзі у веб-браузері з'явиться повідомлення про закінчення часу очікування запиту **Request Timeout**. Чому?

– закрийте веб-браузер на Admin.

– у вкладці Admin Desktop, натисніть Command Prompt.

– введіть ipconfig /renew , щоб Admin знов отримав інформацію про IP-адресу через DHCP.

Дайте відповідь на запитання:

– зазначте нову IP-адресу комп’ютера Admin;

– відкрийте веб-браузер і перевірте, чи можете ви перейти на сервер www.cisco.pka;

– оновіть IP-адреси на інших ноутбуках і перевірте, чи можете ви перейти на сервер www.cisco.pka;

– зверніть увагу, що ноутбук Laptop1 під’єднаний до точки доступу AP, а не до бездротового маршрутизатора WR. Чому?

Лабораторна робота 16
Під’єднання дротової і бездротової локальної мережі

Мета роботи: опанування принципів побудови змішаних локальних мереж шляхом інтеграції дротових (Ethernet) і бездротових (Wi-Fi) технологій для забезпечення коректного взаємодії між сегментами різних типів у єдиному мережевому середовищі.

Завдання: виконати налаштування базових параметрів дротової та бездротової локальної мережі (рис. 1) [3].

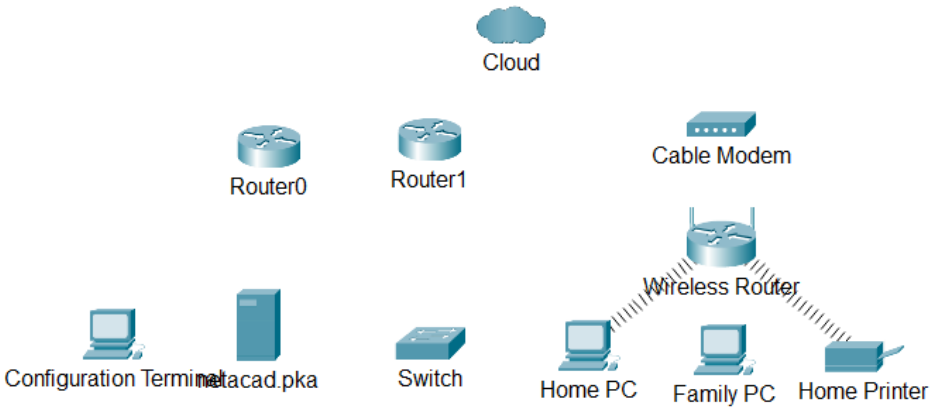


Рисунок 1 – Топологія мережі

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

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 розглянуто налаштування пристроїв у Packet Tracer, вибір відповідного кабелю на основі конфігурації та під'єднання пристроїв. Також розглянемо фізичне представлення мережі в Packet Tracer.

Хід роботи

Під'єднання до хмари Cloud

1) Під'єднайте хмару до Router0:

– унизу ліворуч натисніть значок помаранчевої блискавки, щоб відкрити доступні з'єднання Connections;

– 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.

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.

Під'єднання маршрутизатора Router0

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.

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.

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.

Під'єднання решти пристроїв

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.

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.

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.

Перевірка з’єднання

1) Перевірте з’єднання Family PC з netacad.pka:

– відкрийте командний рядок на Family PC і надішліть запит ping на netacad.pka;

– відкрийте Web Browser і введіть веб-адресу http://netacad.pka.

2) Пропінгуйте Switch з Home PC:

– відкрийте командний рядок на Home PC і надішліть запит ping на IP-адресу Switch, щоб перевірити з’єднання.

3) Відкрийте Router0 з Configuration Terminal:

– відкрийте Terminal на Configuration Terminal і прийміть параметри за замовчуванням;

– натисніть Enter, щоб перейти у командний рядок Router0;

– введіть команду show ip interface brief, щоб переглянути стани інтерфейсів.

Вивчення фізичної топології

1) Перегляньте хмару Cloud:

– перейдіть на вкладку Physical Workspace або натискайте Shift+P і Shift+L, щоб переключатися між логічною і фізичною топологіями;

– натисніть значок Home City;

– натисніть значок Cloud. ***Дайте відповідь на питання***. Скільки дротів під’єднано до комутатора в синій стійці?;

– натисніть кнопку Back, щоб повернутися до Home City.

2) Перегляньте первинну мережу PrimaryNetwork:

натисніть значок Primary Network. Утримуйте курсор миші на різних кабелях. ***Дайте відповідь на питання***. Що знаходиться в таблиці праворуч від синьої стійки?;

– натисніть кнопку Back, щоб повернутися до Home City.

3) Перегляньте вторинну мережу Secondary Network:

– натисніть значок Secondary Network. Утримуйте курсор миші на різних кабелях. ***Дайте відповідь на питання.*** Чому до кожного пристрою під’єднано два помаранчевих кабелі?;

– натисніть кнопку Back, щоб повернутися до Home City.

4) Перегляньте домашню мережу Home Network:

– натисніть значок Home Network. ***Дайте відповідь на питання.*** Чому немає стійки для обладнання?

– перейдіть на вкладку Logical Workspace, щоб повернутися до логічної топології.

Оформіть звіт до роботи.

Лабораторна робота 17
Налаштування NAT

Мета роботи: ознайомлення з принципами функціонування бездротових точок доступу та технології трансляції мережевих адрес (NAT), а також набуття практичних навичок налаштування бездротового доступу до локальної мережі й реалізації NAT для забезпечення виходу клієнтських пристроїв до глобальної мережі Інтернет.

Завдання: виконати базове налаштування бездротової точки доступу (SSID, тип автентифікації, параметри безпеки), підключити клієнтські пристрої до бездротової мережі та перевірити їх IP-адресацію, налаштувати NAT на маршрутизаторі для забезпечення доступу до зовнішньої мережі, виконати перевірку коректності маршрутизації та трансляції адрес за допомогою утиліт командного рядка (ping, tracert).

Хід роботи

Опрацюйте матеріал [12-15].

Виконати налаштування згідно варіанту, поданому в таблиці 1.

Створити мережу, топологія якої зображена на рис. 1.

1. Створити vlan10, vlan20, vlan30. vlan 40. У vlan10 має бути два комп'ютери, у vlan20 – принтер, vlan30 – сервер, vlan40 – бездротова точка доступу, ноутбук і смартфон.

2. На комутаторі налаштувати порти в відповідні vlan.

3. На маршрутизаторі налаштувати підінтерфейси для vlan та зовнішній інтерфейс для підключення до інтернет-провайдера

4. Налаштувати на маршрутизаторі протокол DHCP.

5. Налаштувати NAT.

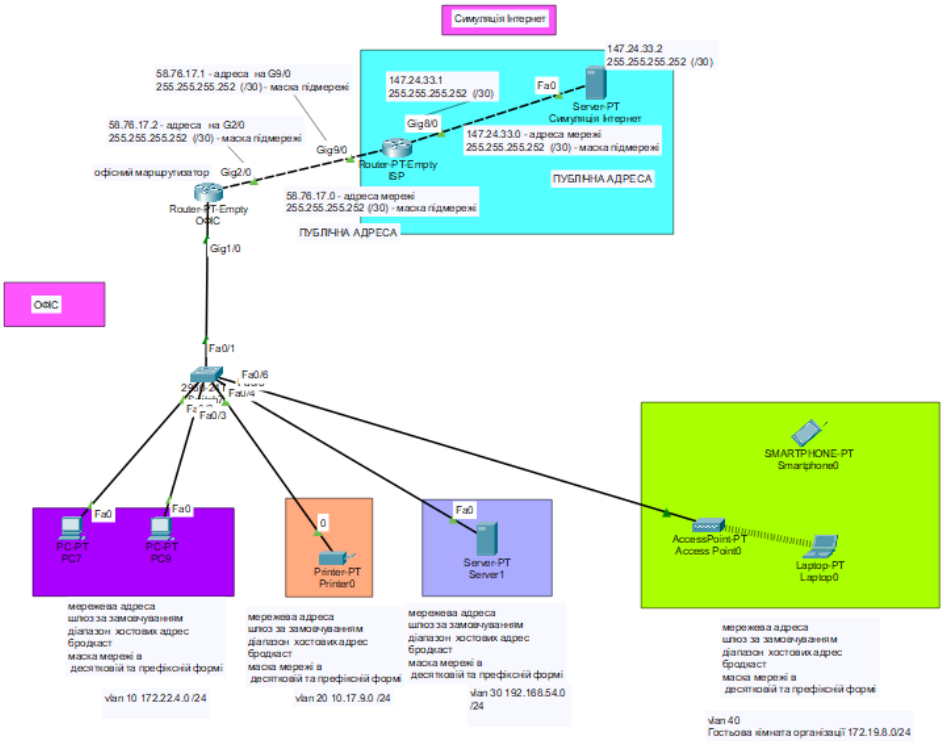


Рисунок 1 – Приклад топології Офісу

Створимо гостьову кімнату у вже існуючій мережі організації з використанням точок доступу. Для цього перейдіть у вкладку ***Wirelless Devices*** та розмістіть точку доступу (рис. 2). Далі потрібно з'єднати точку доступу з комутатором.

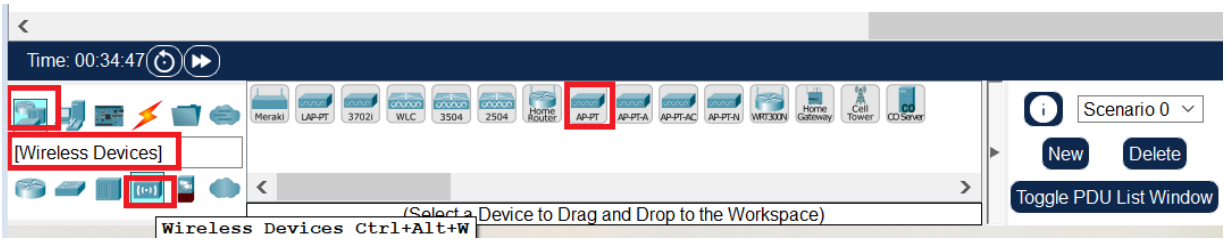


Рисунок 2 – Приклад додавання точки доступу

Встановити гігабітний порт на точці доступу (рис. 3)

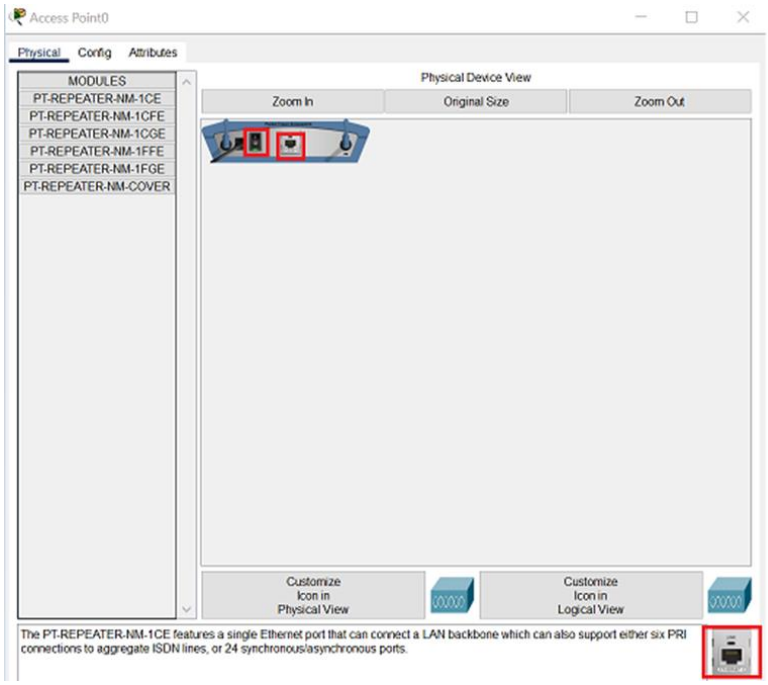


Рисунок 3 – Приклад встановлення гігабітного порту на точці доступу

Налаштувати точку доступу (рис. 4): ім'я мережі – VLAN40, шифрування – WPA2-PSK, PSK Pass Phrase − network123.

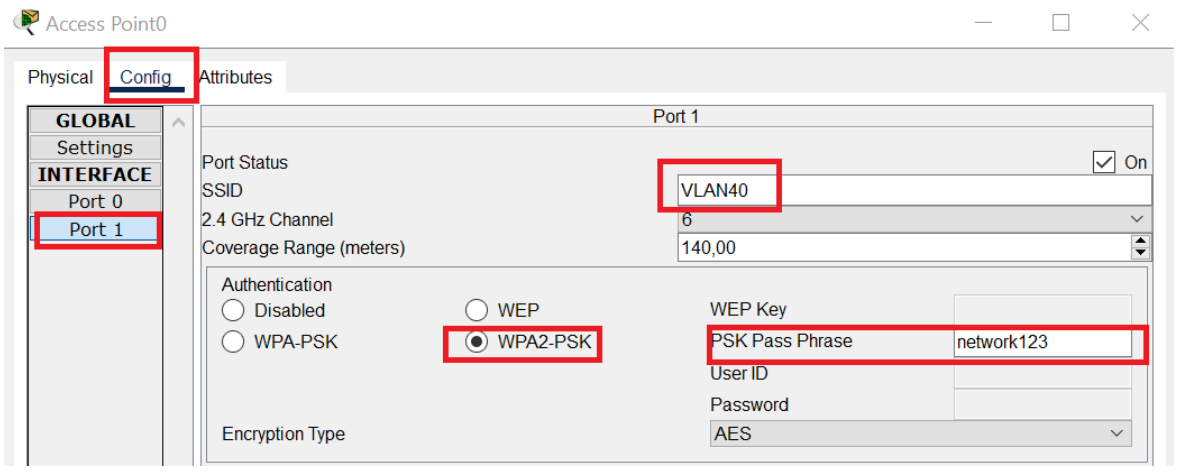


Рисунок 4 – Налаштування точки доступу

Налаштувати ноутбук (рис. 5): вимкнути ноутбук, замінити модуль Ehternet на модуль радіоканалу, включити ноутбук, зробити підключення до існуючої мережі.

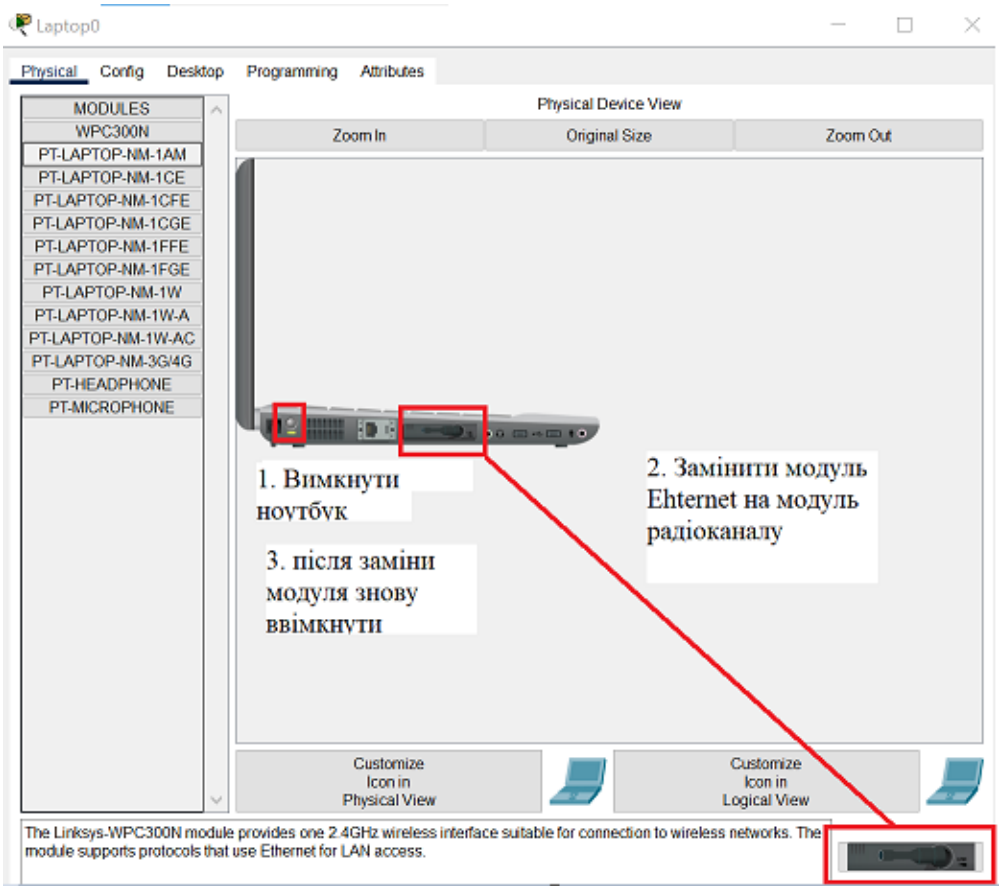


Рисунок 5 – Налаштування ноутбука

Під’єднаємо до існуючої мережі (рис. 6-8)

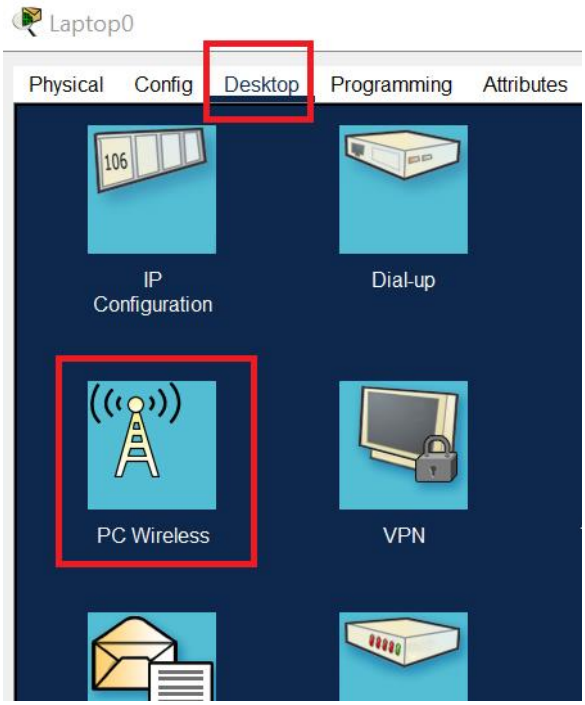


Рисунок 6 – Під’єднання до існуючої мережі

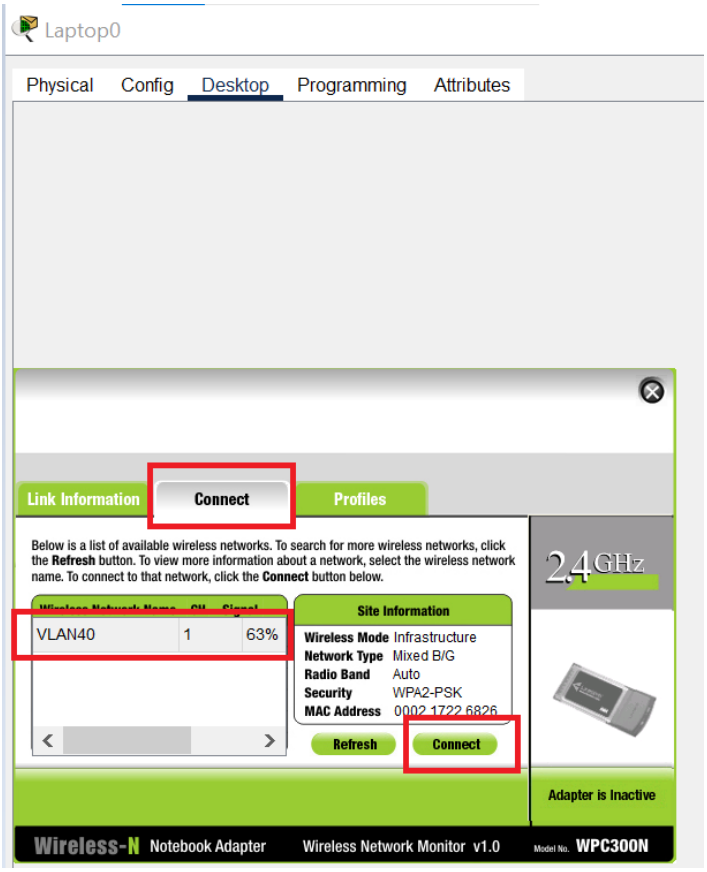


Рисунок 7 – Під’єднання до існуючої мережі

Вводимо ключове слово network123.

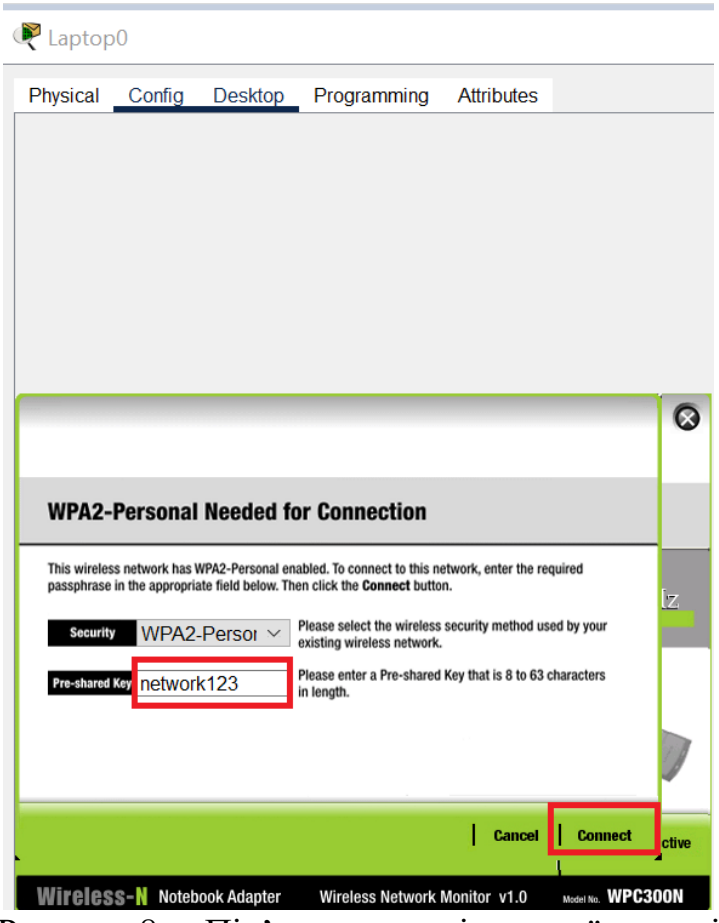


Рисунок 8 – Під’єднання до існуючої мережі

Як бачимо на схемі, підключення успішне

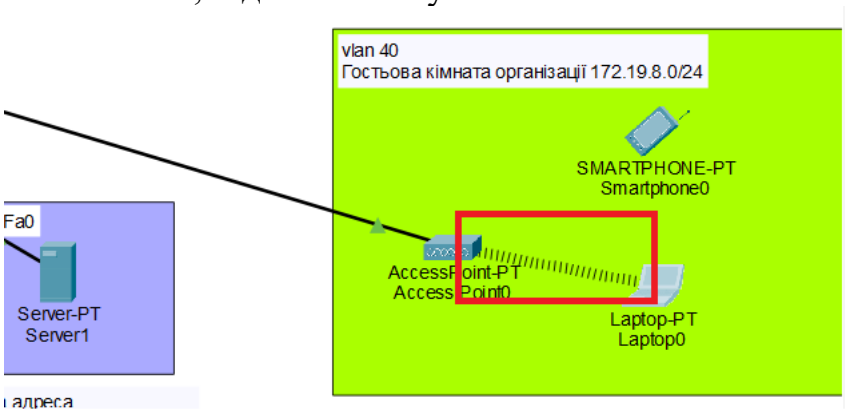


Рисунок 9 – З'єднання між ноутбуком та віддаленим сервером

Після налаштування точки доступу та ноутбука, з'єднання між ноутбуком та віддаленим сервером має бути успішним (рис. 9-10). Дане з'єднання буде успішним після того, коли буде налаштовано NAT (описано нижче по тексту)

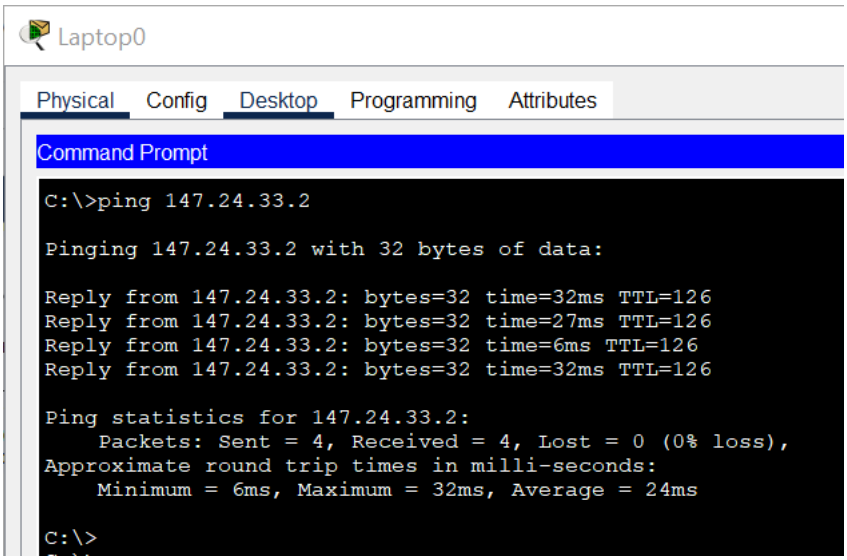


Рисунок 10 – З'єднання між ноутбуком та віддаленим сервером

Далі налаштувати на маршрутизаторі протокол DHCP (вивчено в попередніх лабораторних роботах).

Налаштування NAT. Для того, щоб забезпечити підключення з локальної мережі до мережі Інтернет, потрібно налаштувати NAT. В реальному житті спочатку потрібно звернутись до провайдера для приєднання по фізичній лінії та виділення публічної (білої) IP-адреси. В середовищі Packet Tracer симулюємо замість провайдера маршрутизатор ISP та сервер, які матимуть публічні IP-адреси.

Налаштуємо порти на маршрутизаторі мережі та маршрутизаторі провайдера, призначивши їм публічні адреси IPv4, маска мережі 255.255.255.252 (/30).

На маршрутизаторі провайдера ISP на інтерфейсі G9/0 (рис. 11) провайдер присвоїв IP-адресу 58.76.17.1, маска підмережі 255.255.255.252 (/30).

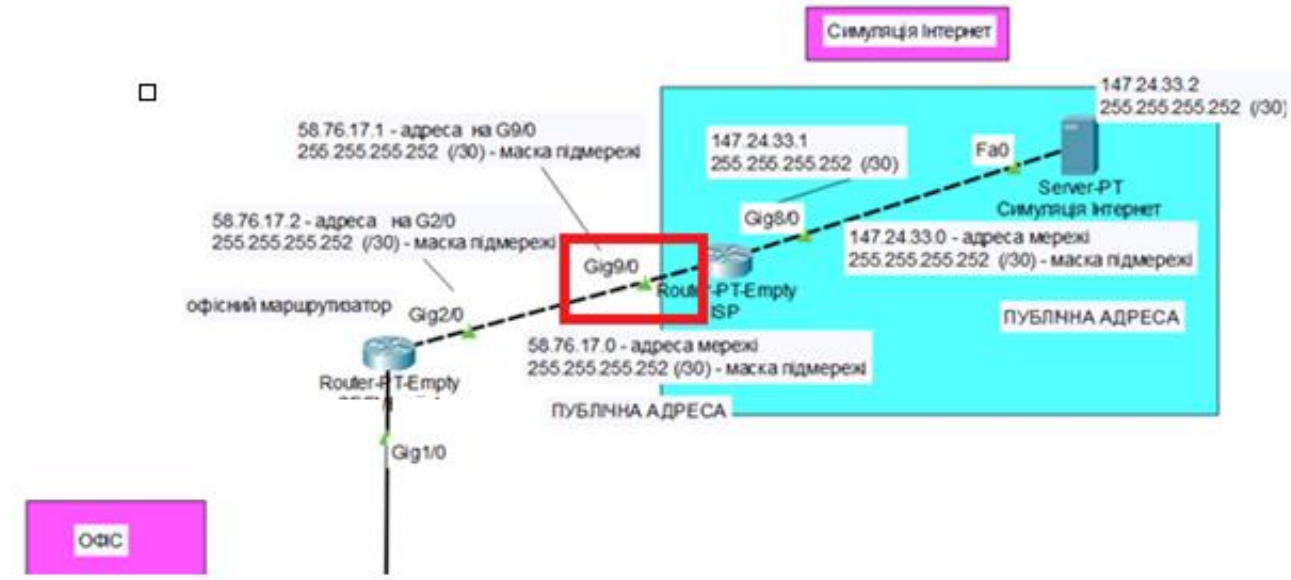


Рисунок 11 – Налаштування інтерфейсу G9/0

За маршрутизатором провайдера в даному завданні знаходиться деякий сервер, який також має публічну IP-адресу, тому на інтерфейсі G8/0 (рис. 12) пропишемо IP-адресу 147.24.33.1 та маску 255.255.255.252 (/30).

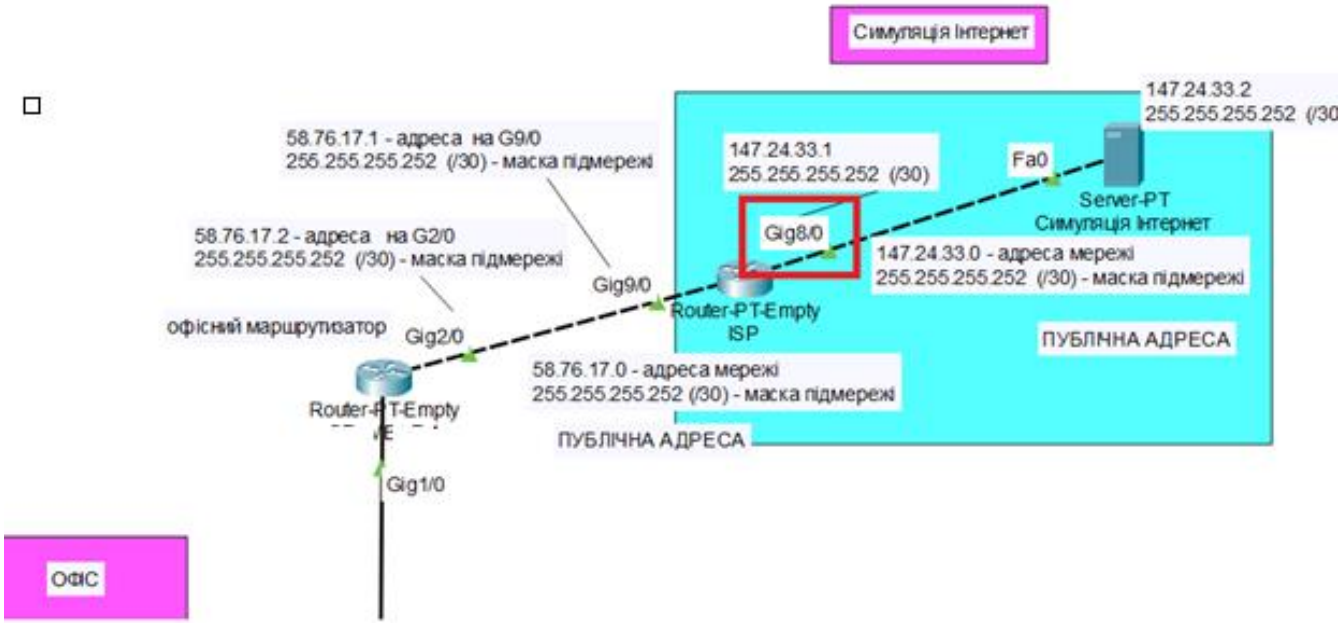


Рисунок 12 – Налаштування інтерфейсу G8/0

Налаштуємо сервер. Призначити серверу (рис. 13) статичну IP-адресу, обравши другу хостову з даної мережі (рис. 14), тобто, 147.24.33.2, маска мережі 255.255.255.252 (/30).

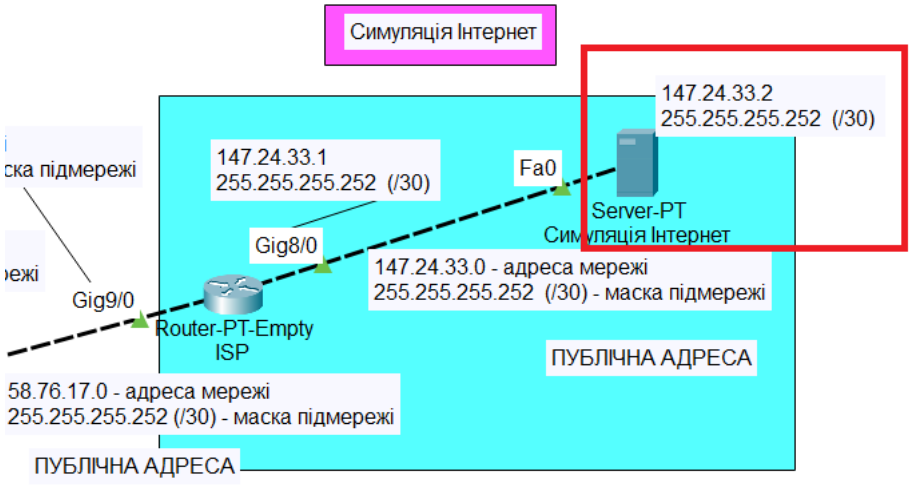


Рисунок 13 – Віддалений сервер

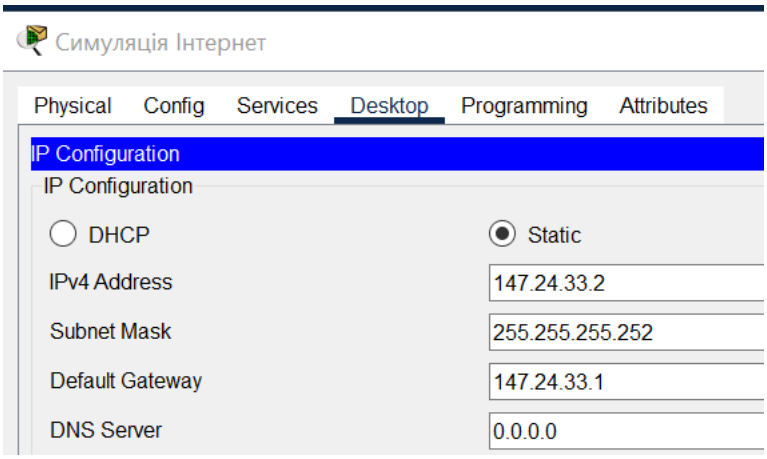


Рисунок 14 – Призначення серверу статичної IP-адреси

Перейти на маршрутизатор мережі (рис. 15) та налаштувати на порті G2/0 IP-адресу 58.76.17.2 та маску 255.255.255.252 (/30).

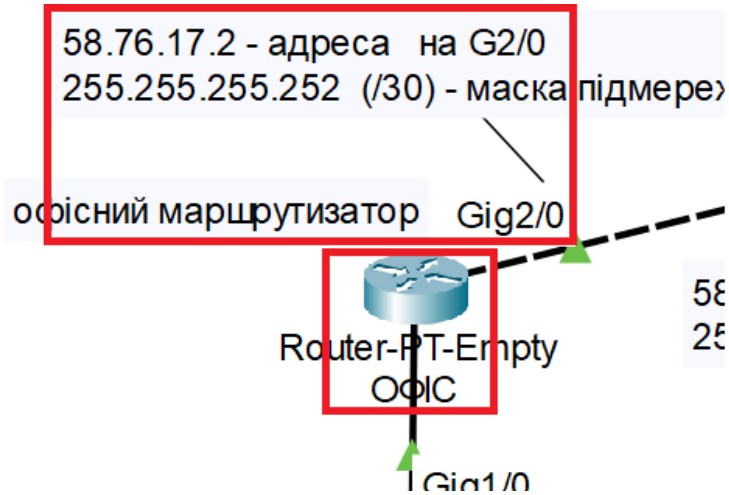


Рисунок 15 – Налаштування інтерфейсу G2/0

Також налаштуємо шлюз за замовчуванням на маршрутизаторі мережі (рис. 16), який буде IP-адресою провайдера **office(config)#ip route 0.0.0.0 0.0.0.0 58.76.17.1,** де **0.0.0.0 0.0.0.0** – маршрутом за замовчуванням (default route). Маршрутизація за замовчуванням використовується у випадку, коли необхідно

проводити пересилку пакетів у віддалену мережу призначення, записів про яку немає в маршрутизаторі наступного переходу. Такий тип маршрутизації можна використовувати в мережах, які мають тупикові сегменти/підмережі (Stub Networks).

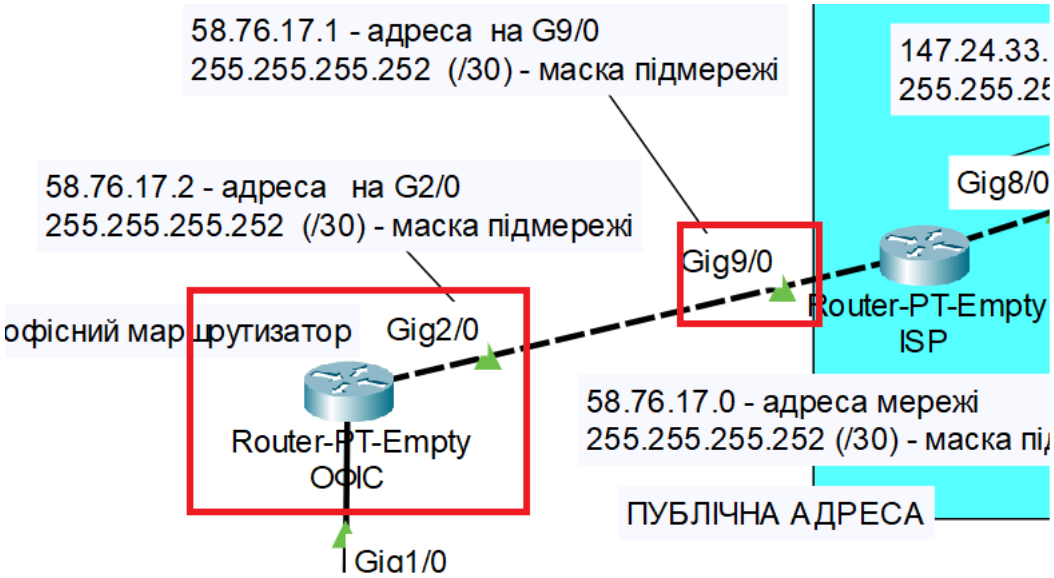


Рисунок 16 – Налаштування шлюзу за замовчуванням на маршрутизаторі мережі

Якщо налаштування виконані вірно, то має пінгуватись маршрутизатор ОФІС з ISP маршрутизатором, але якщо ми будемо пінгувати з локального комп'ютера ОФІСу сервер, то зв'язку не буде, так як в локальній мережі використана приватна адресація, і маршрутизатор ISP про неї нічого не знає. За допомогою технології NAT забезпечимо доступ комп'ютерам ОФІСу в мережу Інтернет, тобто, в нашому завданні до тестового сервера (Симуляція Інтернет).

В даному випадку визначаємо (рис. 17), який інтерфейс буде зовнішнім, а який внутрішнім для NAT.

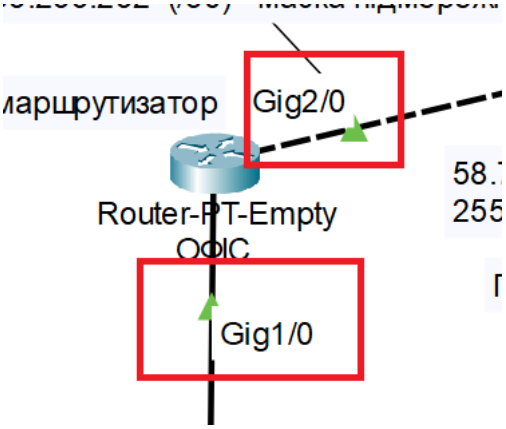


Рисунок 17 – Визначення внутрішніх та зовнішніх інтерфейсів

Інтерфейс G2/0 – налаштувати як **office(config-if)#ip nat outside** (рис. 18).

Примітка: далі назва маршрутизатора на скрінах замість **office** ***буде Segment4, але Ви в роботі використовуєте назву*** **office.**

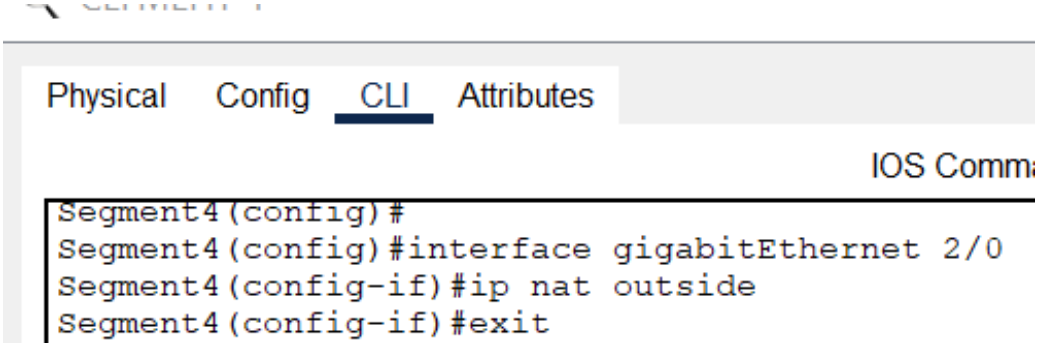


Рисунок 18 – Налаштування інтерфейсу G2/0

Підінтерфейси G1/0.10, G1/0.20, G1/0.30, G1/0.40 (рис. 19) – налаштувати як **office(config-subif)#ip nat inside.**

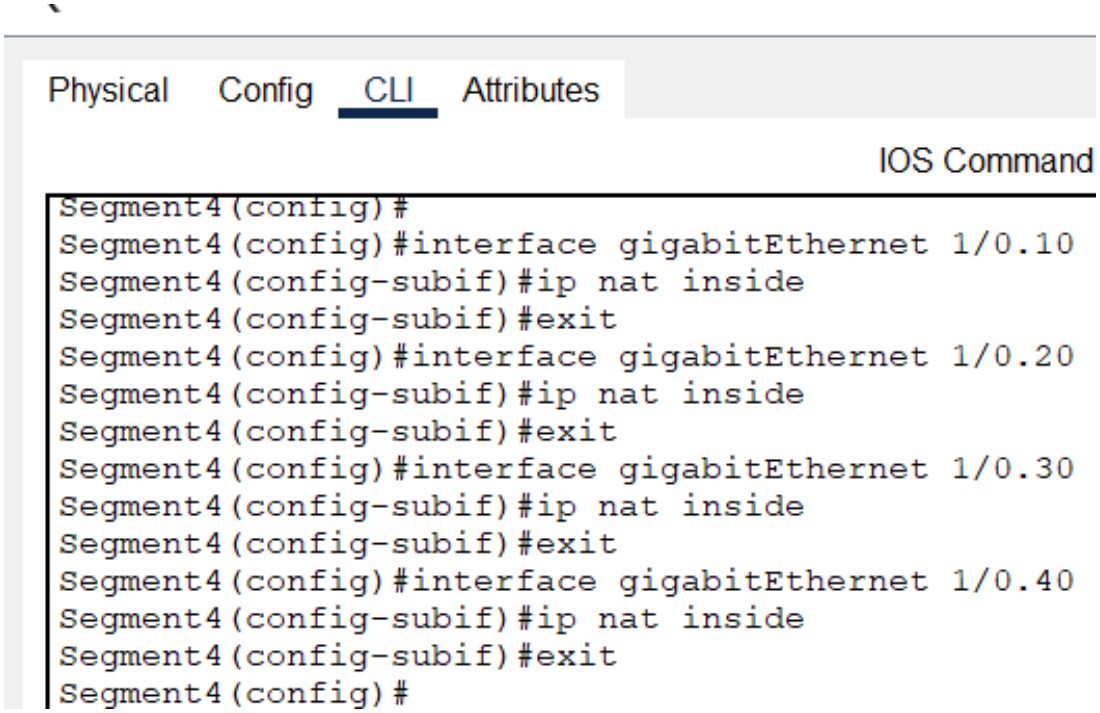


Рисунок 19 – Налаштування підінтерфейсів G1/0.10, G1/0.20, G1/0.30, G1/0.40

Тепер потрібно створити access-list, який буде характеризувати, який саме трафік будемо «натити» (рис. 20-21).

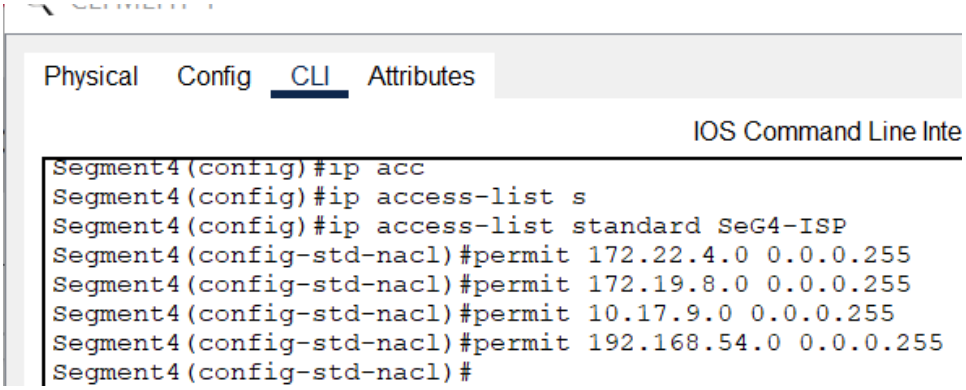


Рисунок 20 – Створення access-list

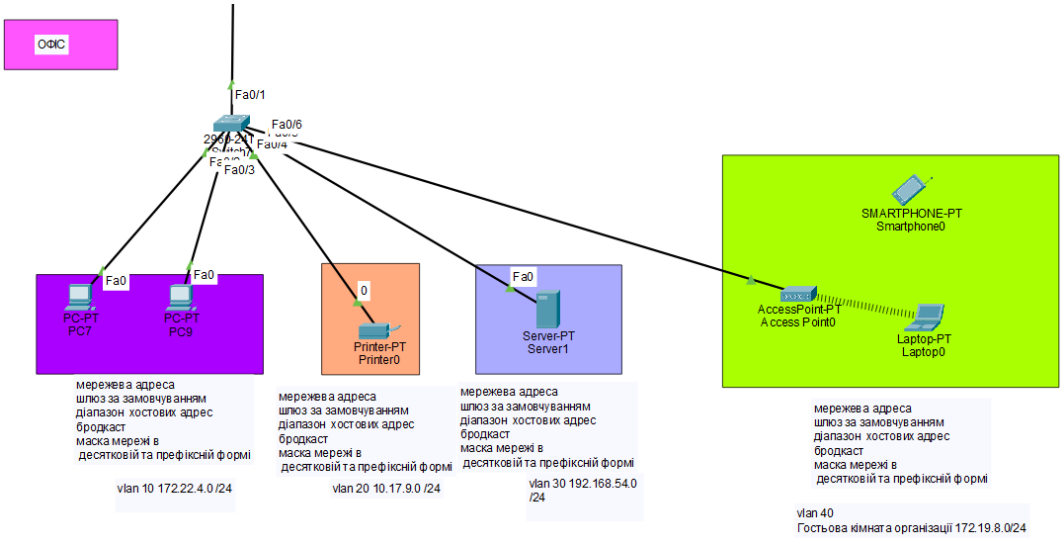


Рисунок 21 – Схема для створення access-list

Та прописати наступну команду (рис. 22):

office(config)#ip nat inside source list SeG4-ISP interface gigabitEthernet 2/0 overload

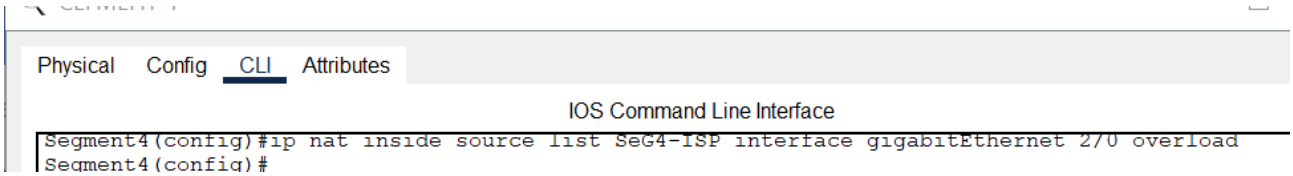


Рисунок 22 – Команда ip nat inside source list SeG4-ISP interface gigabitEthernet 2/0 overload

Якщо налаштування виконані вірно, то при перевірці з'єднання пінг між елементами мережі, позначеними на рис. 23, буде вдалим, наприклад, як на рис. 24.

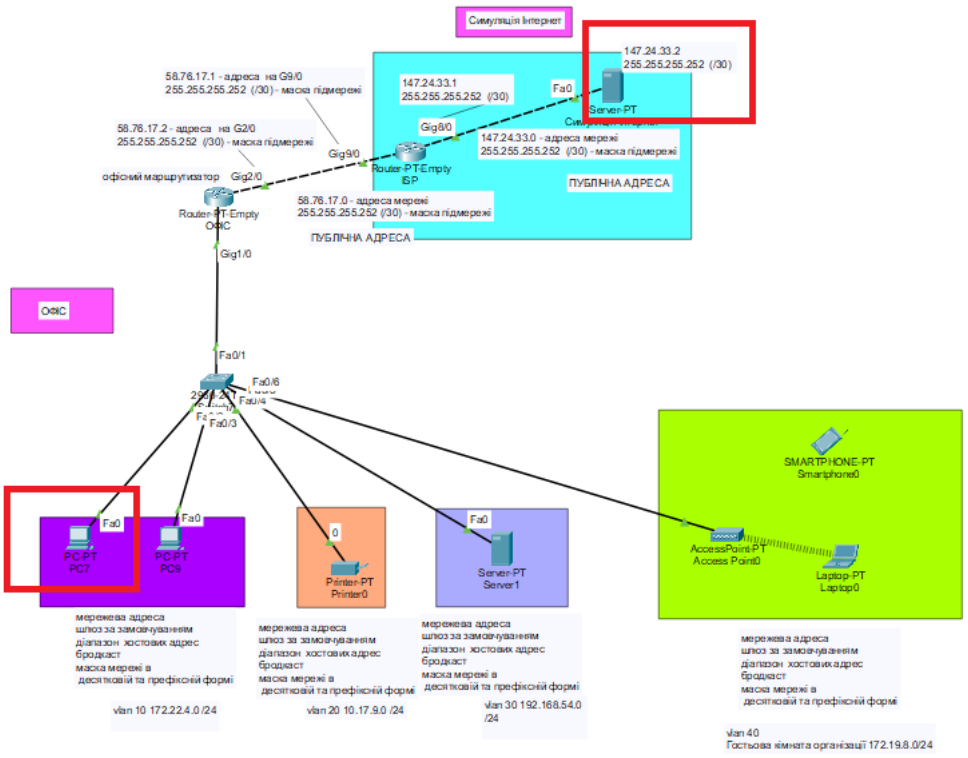


Рисунок 23 – Перевірка зв'язку з локальної мережі до віддаленого сервера

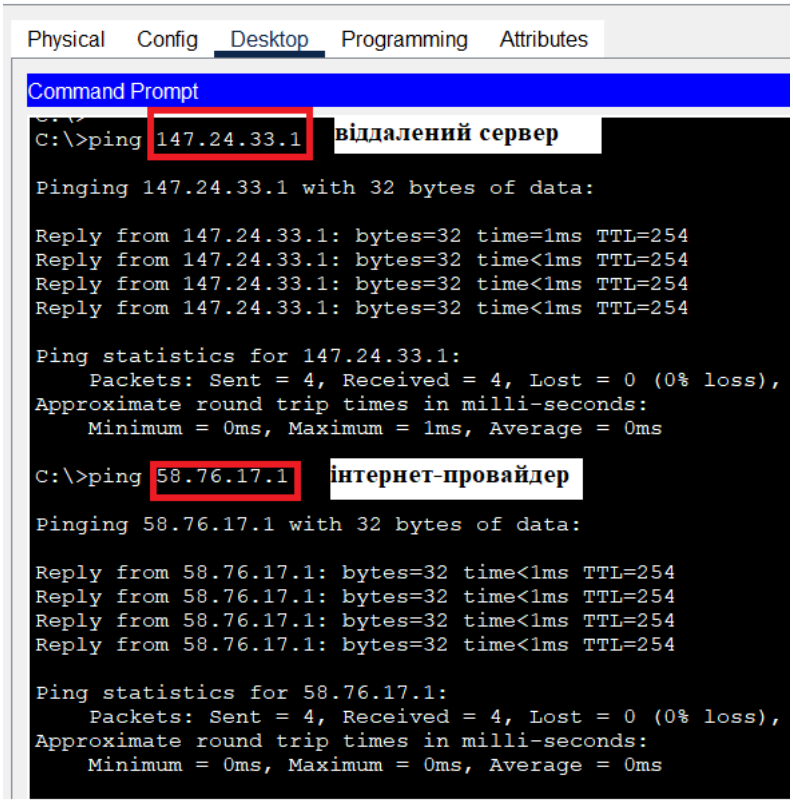


Рисунок 24 – Перевірка зв'язку з локальної мережі до віддаленого сервера

Застосуємо на маршрутизаторі ОФІС команду **office#show ip nat translations** і побачимо трансляцію NAT (рис. 25).

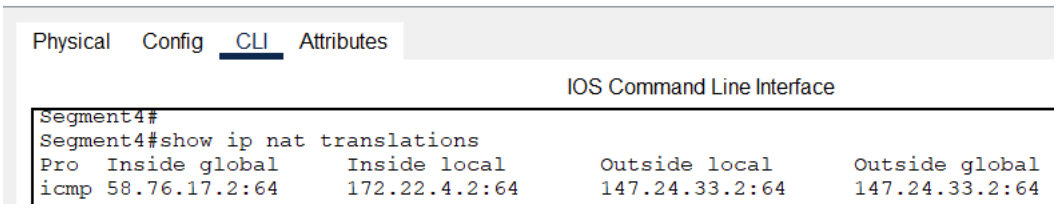


Рисунок 25 – Трансляція NAT

Як бачимо, пінг з комп'ютера з адресою 172.22.4.2 транслюється в адресу 58.76.17.2, а вже тоді іде на сервер 147.24.33.2.

Налаштувати з'єднання з смартфона з віддаленим сервером.

Варіант завдання

Таблиця 1 – Варіанти завдань

Адресація vlan 10, маска/24	Адресація vlan 20, маска/24	Адресація vlan 30, маска/24	Адресація vlan 40, маска/24	Адресація між маршрутизатором офіс та ISP, маска/30	Адресація між ISP та віддаленим сервером, маска/30
10.196.178.0	10.118.210.0	10.38.26.0	10.121.116.0	23.86.76.0	120.2.133.0
172.26.242.0	192.168.69.0	10.157.113.0	172.17.227.0	100.185.112.0	187.132.140.0
10.219.183.0	192.168.143.0	172.21.79.0	192.168.240.0	47.142.203.0	143.163.191.0
10.178.230.0	10.59.73.0	10.39.10.0	192.168.224.0	43.190.249.0	41.250.34.0
172.19.115.0	192.168.16.0	172.21.114.0	172.21.99.0	194.150.33.0	185.51.18.0

Продовження таблиці 1

Адресація vlan 10, маска/24	Адресація vlan 20, маска/24	Адресація vlan 30, маска/24	Адресація vlan 40, маска/24	Адресація між маршрутизатором офіс та ISP, маска/30	Адресація між ISP та віддаленим сервером, маска/30
10.117.69.0	10.39.166.0	172.19.197.0	172.16.60.0	4.92.197.0	209.187.156.0
10.52.61.0	10.94.8.0	10.37.225.0	172.24.91.0	184.196.10.0	113.41.188.0
192.168.174.0	192.168.117.0	172.19.167.0	172.26.189.0	182.45.44.0	54.24.104.0
10.21.152.0	10.68.182.0	10.51.238.0	10.196.174.0	97.224.49.0	81.115.228.0
10.173.120.0	172.29.162.0	10.246.110.0	172.23.252.0	83.176.51.0	163.161.223.0
10.89.12.0	10.34.114.0	10.191.203.0	10.24.164.0	131.149.23.0	128.121.2.0
10.135.24.0	192.168.108.0	172.31.99.0	10.212.54.0	84.173.40.0	166.186.13.0
10.224.89.0	10.60.161.0	10.55.171.0	192.168.247.0	85.215.43.0	128.164.187.0
10.87.84.0	10.235.178.0	10.145.104.0	192.168.235.0	119.174.77.0	138.204.152.0
192.168.97.0	172.19.158.0	172.18.103.0	192.168.9.0	78.205.106.0	151.151.107.0
192.168.197.0	10.93.24.0	192.168.124.0	172.26.177.0	90.170.23.0	198.83.86.0
172.29.186.0	192.168.88.0	172.23.61.0	10.135.11.0	108.20.22.0	3.142.121.0
192.168.24.0	192.168.62.0	10.2.210.0	192.168.135.0	26.35.194.0	31.217.156.0
192.168.94.0	192.168.127.0	172.21.10.0	10.84.116.0	29.94.160.0	69.61.11.0
192.168.142.0	192.168.241.0	10.207.155.0	172.29.201.0	77.23.87.0	45.121.228.0
172.20.37.0	192.168.54.0	10.52.114.0	172.17.139.0	109.122.107.0	157.188.209.0
172.25.38.0	172.24.83.0	192.168.163.0	192.168.51.0	186.121.73.0	57.53.42.0
192.168.223.0	172.23.223.0	172.28.175.0	192.168.191.0	107.35.148.0	64.196.8.0
10.108.53.0	192.168.220.0	172.18.194.0	192.168.34.0	62.132.246.0	158.234.64.0
192.168.208.0	10.95.211.0	172.29.13.0	10.237.217.0	118.241.176.0	128.89.191.0
192.168.52.0	10.151.198.0	10.24.177.0	172.29.86.0	215.49.224.0	113.23.168.0
192.168.137.0	172.23.182.0	10.234.165.0	10.115.158.0	221.80.91.0	176.242.49.0
192.168.70.0	172.18.234.0	172.27.33.0	192.168.227.0	14.145.242.0	67.214.22.0
192.168.199.0	172.20.194.0	192.168.53.0	172.23.247.0	104.160.55.0	168.253.16.0
192.168.56.0	192.168.123.0	10.245.12.0	172.26.69.0	137.118.255.0	180.129.106.0
10.184.154.0	172.19.78.0	10.227.186.0	172.22.102.0	171.230.124.0	16.209.180.0
192.168.120.0	172.26.162.0	10.209.155.0	192.168.148.0	186.134.61.0	185.32.74.0

Лабораторна робота 18
Налаштування Site-to-Site VPN

Мета роботи: ознайомити студентів з налаштуванням Site-to-Site VPN від центрального офісу до філіалу з використанням протоколу GRE.

Завдання: виконати конфігурування GRE-тунелю на маршрутизаторах для створення VPN-з'єднання між двома віддаленими мережами, налаштувати статичну або динамічну маршрутизацію для забезпечення передачі даних через GRE-тунель, перевірити працездатність встановленого GRE-тунелю, перевіривши доступність ресурсів обох сегментів мережі через VPN, проаналізувати ефективність та обмеження використання GRE для маршрутизації між віддаленими мережами.

Теоретична частина

Опрацюйте матеріал [16].

«**VPN (Virtual Private Network)** – це віртуальна приватна мережа, яка забезпечує шифрування трафіку між клієнтом та VPN-сервером і зміну IP-адреси. При підключенні до VPN створюється захищений канал між комп'ютером користувача і VPN-сервером. Дані в ньому надійно зашифровані: ваш інте'рнет-провайдер не дізнається вашої локації та вебресурсів, які ви відвідали».

Site-to-Site VPN (віртуальна приватна мережа між сайтами) − це технологія, що дозволяє з'єднувати різні локальні мережі (LAN) через Інтернет, створюючи віртуальний тунель між ними. Зазвичай ця технологія використовується для об'єднання офісів однієї компанії, що розташовані в різних географічних точках [2].

Site-to-Site VPN створюється, коли на кінцевих пристроях VPN, які ще називають VPN-шлюзами, попередньо налаштовано інформацію для створення безпечного тунелю. Трафік VPN зашифрований тільки між цими пристроями. Внутрішні вузли не знають, що використовується VPN (рис. 1) [3].

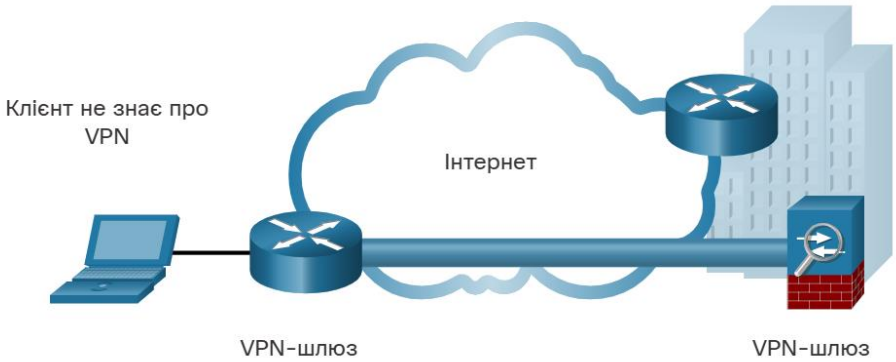


Рисунок 1 – Site-to-Site VPN [3]

I. Основні характеристики Site-to-Site VPN:

1) віртуальний тунель:

– Site-to-Site VPN створює захищений тунель через Інтернет, який з'єднує мережі двох або більше фізичних локацій;

– через цей тунель передаються всі дані, що обмінюються між офісами, і вони захищені за допомогою шифрування;

2) об'єднання мереж:

– користувачі, підключені до різних мереж, можуть працювати з ресурсами іншого офісу так, ніби вони підключені до тієї ж локальної мережі;
– це забезпечує спільний доступ до серверів, баз даних, файлових систем та інших ресурсів між офісами;

3) типи реалізації:

– Intranet VPN: використовується для об'єднання офісів однієї організації;
– Extranet VPN: використовується для безпечного з'єднання між мережами різних організацій, які співпрацюють між собою.

II. Реалізація Site-to-Site VPN

1) обладнання:

– для реалізації Site-to-Site VPN потрібні спеціальні маршрутизатори або брандмауери (firewalls), які підтримують VPN. Вони відповідають за створення і підтримку VPN-з'єднання;
– в обох кінцях VPN-з'єднання встановлюються VPN-шлюзи (VPN gateways) – пристрої або сервери, які шифрують і розшифровують трафік;

2) протоколи:

– IPSec: найпоширеніший протокол для реалізації Site-to-Site VPN. Він забезпечує захищене з'єднання між двома точками (наприклад, між офісами) за допомогою шифрування та автентифікації;
– GRE (Generic Routing Encapsulation): використовується разом з IPSec для тунелювання інших протоколів через Інтернет;

3) налаштування:

– створення VPN-тунелю: визначаються кінцеві точки (IP-адреси) для тунелю, що буде з'єднувати дві мережі;
– шифрування: налаштовується шифрування трафіку між кінцевими точками тунелю, що забезпечує захист даних;
– маршрутизація: налаштовуються маршрути, які вказують, що весь трафік, призначений для віддаленої мережі, має йти через VPN-тунель;

4) моніторинг і підтримка:

– після налаштування Site-to-Site VPN потрібно регулярно моніторити з'єднання, щоб забезпечити стабільну роботу та своєчасне виявлення будь-яких проблем;

5) приклад сценарію використання

Уявімо, що компанія має головний офіс у Києві та філію в Одесі. Site-to-Site VPN дозволить співробітникам з одеського офісу отримувати доступ до серверів, що знаходяться в київському офісі, через захищене з'єднання. Це з'єднання буде виглядати як одне спільне віртуальне робоче середовище, незалежно від фізичної відстані між офісами;

6) переваги Site-to-Site VPN

– безпека: шифрування даних забезпечує високий рівень захисту від зловмисників;
– скорочення витрат: замість оренди дорогих виділених ліній компанія може використовувати Інтернет для об'єднання своїх офісів;

– простота доступу: співробітники можуть легко обмінюватися інформацією і працювати з ресурсами компанії, незалежно від їхнього місцезнаходження.

В даній роботі створюється GRE-тунель між двома маршрутизаторами для об'єднання двох сегментів мережі.

Протокол GRE (англ. Generic Routing Encapsulation − загальна інкапсуляція маршрутів) − протокол тунелювання мережевих пакетів, розроблений компанією Cisco Systems. Його основне призначення − інкапсуляція пакетів мережевого рівня мережевої моделі OSI в IP пакети [4].

В даній роботі є два відділення організації (головний офіс та філіал), що об'єднані між собою мережею інтернет-провайдера, тому потрібно забезпечити зв'язок між головним офісом та філіалом та не дозволити доступ до них з інших мереж.

Хід роботи

Практична частина:

1. створити топологію мережі, зображену на рис. 2;

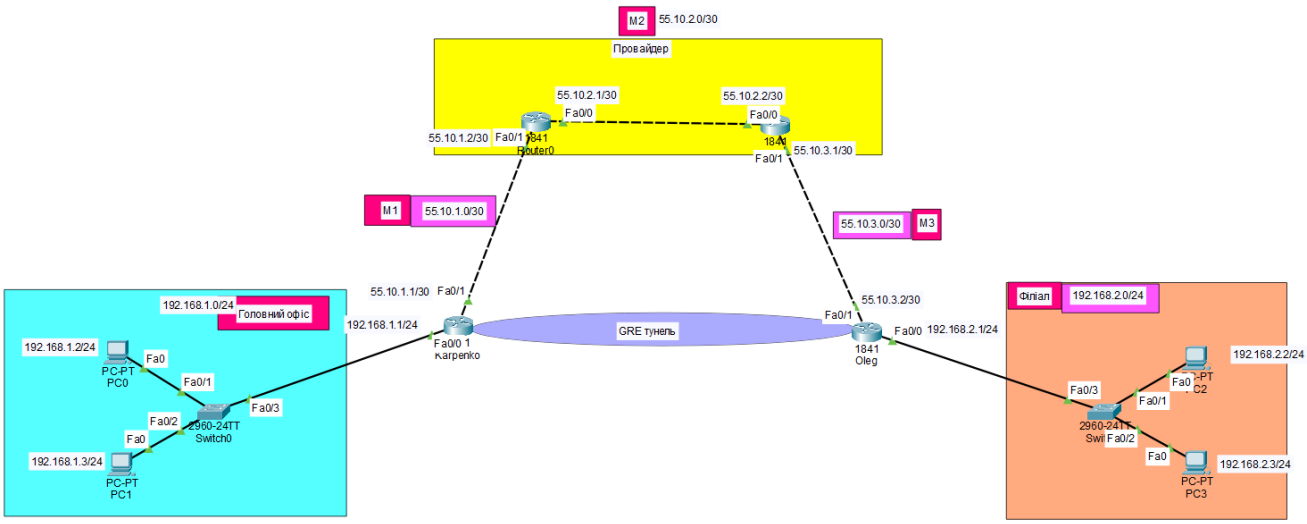


Рисунок 2 – Топологія мережі

2. адресацію використати згідно варіанту, поданому в таблиці 1;
3. налаштувати статично інтерфейси комп'ютерів;
4. призначити ім'я маршрутизатору головного офісу – ***прізвище студента*;**
5. призначити ім'я маршрутизатору філіалу – ***ім'я студента*;**
6. призначити ім'я маршрутизаторам провайдера відповідно **– ISP1 та ISP2;**
7. призначити IP-адреси на інтерфейсах маршрутизаторів згідно варіанту, поданому в таблиці 1, та ввімкнути їх;
8. ввести на маршрутизаторах команду **no ip domain-lookup,** щоб маршрутизатори ігнорували невірно введені команди.

Після налаштування інтерфейсів, потрібно налаштувати маршрутизацію. В даному завданні мережа провайдера складається з маршрутизаторів ISP1 та ISP2.

Взаємодію даних маршрутизаторів в межах мережі налаштувати за допомогою протоколу ospf:

1. налаштування маршрутизатора ISP1:

ISP1(config)#router ospf 1
ISP1(config-router)#passive-interface fastEthernet 0/1 *(дана команда вводиться для того, щоб на інтерфейси, до яких підключаються маршрутизатори організації, тобто, в даному завданні це маршрутизатори, які названі прізвищем та ім'ям студента, не проводилась розсилка службових пакетів протоколу ospf)*
ISP1(config-router)#router-id 2.2.2.2
ISP1(config-router)#network 55.10.1.0 0.0.0.3 area 0
ISP1(config-router)#network 55.10.2.0 0.0.0.3 area 0
ISP1(config-router)#exit
ISP1(config)#exit
ISP1#
ISP1#wr
Building configuration...
[OK]
ISP1#

Виконати команду **ISP1#show ip routeта** розмістити в звіт по роботі виведені налаштування.

2. налаштування маршрутизатора ISP2:

ISP2(config)#router ospf 1
ISP2(config-router)#passive-interface fastEthernet 0/1 *(дана команда вводиться для того, щоб на інтерфейси, до яких підключаються маршрутизатори організації, тобто, в даному завданні це маршрутизатори, які названі прізвищем та ім'ям студента, не проводилась розсилка службових пакетів протоколу ospf)*
ISP2(config-router)#router-id 3.3.3.3
ISP2(config-router)#network 55.10.2.0 0.0.0.3 area 0
01:33:04: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthernet0/0 from LOADING to FULL, Loading Done
ISP2(config-router)#network 55.10.3.0 0.0.0.3 area 0
ISP2(config-router)#exit
ISP2(config)#exit
ISP2#
%SYS-5-CONFIG_I: Configured from console by console
ISP2#wr
Building configuration...
[OK]
ISP2#

Виконати команду **ISP2#show ip route** та розмістити в звіт по роботі виведені налаштування.

Сконфігурувати маршрути за замовчування на маршрутизаторах офісу та філіалу для скерування трафіку в мережу провайдера (ці маршрутизатори належать організації і їх завданням є підключення відділ організації до мережі провайдера).

1. налаштування маршруту за замовчуванням на маршрутизаторі ISP1:

Karpenko(config)#ip route 0.0.0.0 0.0.0.0 55.10.1.2 (для маршрутизатора офісу адреса шлюзу за замовчуванням – адреса інтерфейсу fastEthernet 0/1 на маршрутизаторі ISP1);

2. налаштування маршруту за замовчуванням на маршрутизаторі ISP2:

Oleg(config)#ip route 0.0.0.0 0.0.0.0 55.10.3.1 (для маршрутизатора офісу адреса шлюзу за замовчуванням – адреса інтерфейсу fastEthernet 0/1 на маршрутизаторі ISP2).

Після налаштування даної частини роботи, провести тестування роботоздатності даної мережі (рис. 3), застосувавши команду ping з маршрутизатора офісу (Karpenko) до IP-адресу інтерфейсу fastEthernet 0/1 маршрутизатора ISP2.

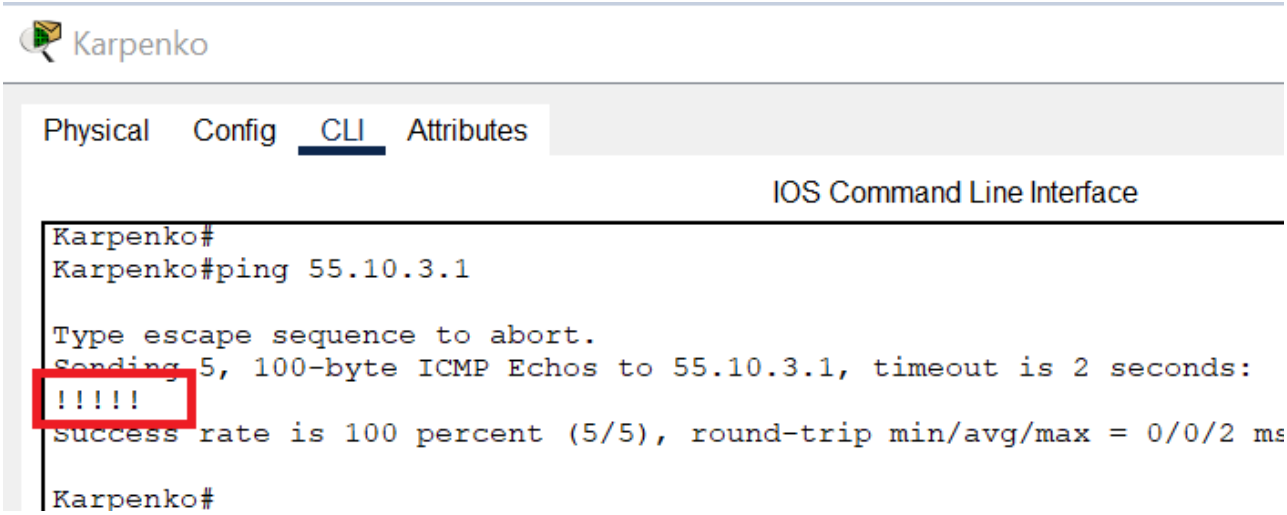


Рисунок 3 – Тестування роботоздатності мережі

Якщо при виведенні результатів даної команди є знаки оклику, то тестування успішне.

Але на даному етапі налаштування мережі зв'язку між комп'ютерами офісу і філіалу не буде (рис. 4), так як маршрутизатор головного офісу не знає шлях в мережу віддаленого офісу.

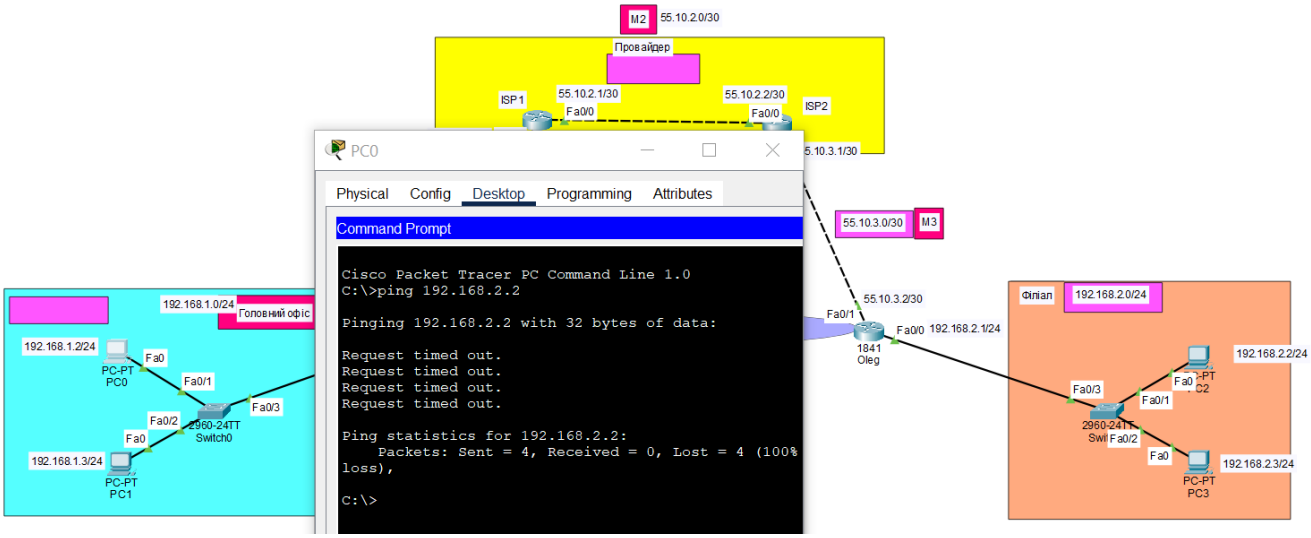


Рисунок 4 – Перевірка з'єднання між головним офісом та філіалом

Тому використаємо в налаштуваннях протокол GRE (англ. Generic Routing Encapsulation − загальна інкапсуляція маршрутів), який дозволить створити віртуальний тунель, що забезпечить взаємодію мереж головного офісу та філіалу (рис. 5).

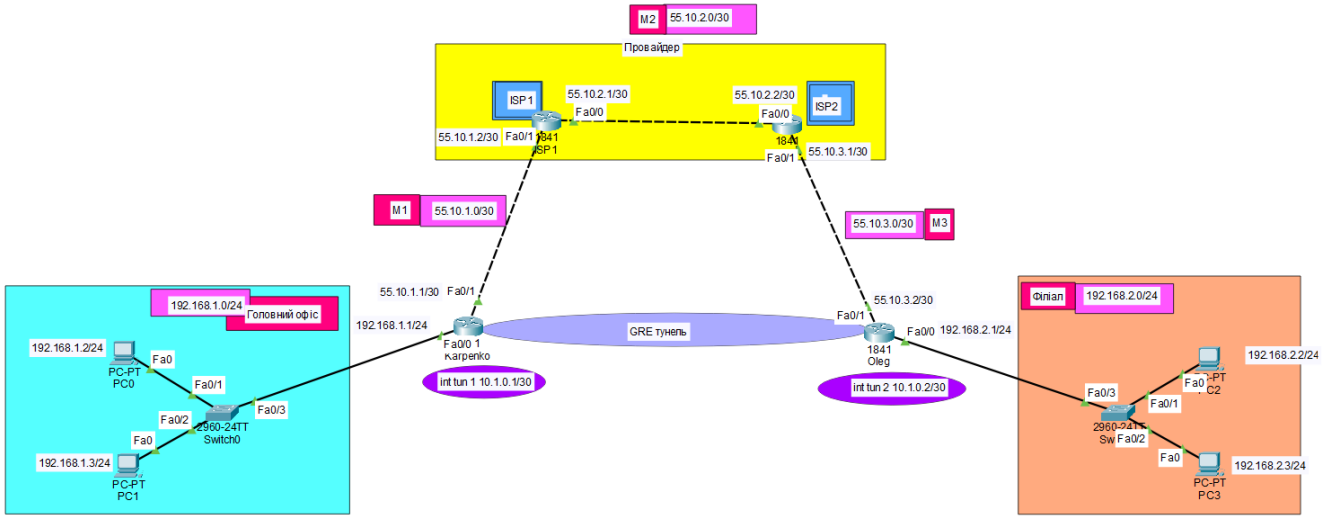


Рисунок 5 – Створення GRE-тунелю

Почнемо створення даного віртуального тунелю з налаштування маршрутизатора офісу (Karpenko):

1. створити новий інтерфейс **tunnel 1**;

Karpenko(config)#interface tunnel 1

Karpenko(config-if)#

%LINK-5-CHANGED: Interface Tunnel1, changed state to up

2. надати інтерфейсу **tunnel 1** IP-адресу;

Karpenko(config-if)#ip address 10.1.0.1 255.255.255.252

3. вказати початок та кінець тунелю;

Karpenko(config-if)#tunnel source fastEthernet 0/1 *(в даній команді fastEthernet 0/1 є інтеффейсом маршрутизатора головного офісу)*

Karpenko(config-if)#tunnel destination 55.10.3.2 *(де 55.10.3.2 – IP-адреса інтерфейсу fastEthernet 0/1 маршрутизатора філіалу, в даному прикладі буде назва Oleg)*

Karpenko(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up (виведення даного пояснення говорить про те, що тунель запрацював в одному напрямку)

Karpenko(config-if)#

Аналогічні налаштування виконати на маршрутизаторі офісу (Oleg):

1. створити новий інтерфейс **tunnel 2**;

Oleg(config)#interface tunnel 2

Oleg(config-if)#

%LINK-5-CHANGED: Interface Tunnel2, changed state to up

2. надати інтерфейсу **tunnel 2** IP-адресу;

Oleg(config-if)#ip address 10.1.0.2 255.255.255.252

3. вказати початок та кінець тунелю;

Oleg(config-if)#tunnel source fastEthernet 0/1 *(в даній команді fastEthernet 0/1 є інтеффейсом маршрутизатора філіалу)*
Oleg(config-if)#tunnel destination 55.10.1.1 *(де 55.10.1.1 – IP-адреса інтерфейсу fastEthernet 0/1 маршрутизатора головного офісу, в даному прикладі буде назва Karpenko)*
Oleg(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel2, changed state to up
Oleg(config-if)#

Після проведених налаштувань потрібно прописати статичний маршрут для обміну пакетами між головним офісом та філіалом:

1. на маршрутизаторі головного офісу (Karpenko)

Karpenko(config)#ip route 192.168.2.0 255.255.255.0 10.1.0.2 *(де 192.168.2.0 255.255.255.0 – відповідно адреса мережі та маска філіалу, а 10.1.0.2 – IP-адреса інтерфейсу тунелю, налаштованому на маршрутизаторі філіалу, в даному випадку назва Oleg)*

2. на маршрутизаторі філіалу (Oleg)

Oleg(config)#ip route 192.168.1.0 255.255.255.0 10.1.0.1 *(де 192.168.1.0 255.255.255.0 – відповідно адреса мережі та маска головного офісу, а 10.1.0.1 – IP-адреса інтерфейсу тунелю, налаштованому на маршрутизаторі головного офісу, в даному випадку назва Karpenko)*

Відправимо в режимі реального часу icmp-пакети з комп'ютера мережі головного офісу на комп'ютер філіалу. Даний пінг повинен бути вдалим (рис. 6). Результати виконання даної перевірки мають бути в звіті до роботи.

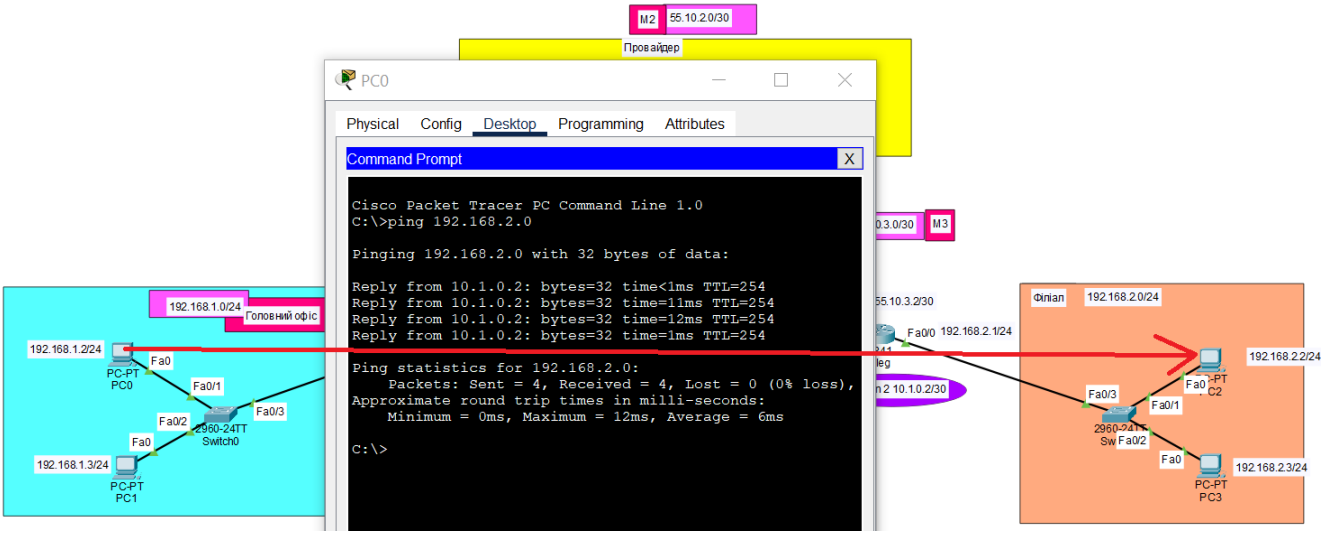


Рисунок 6 – Перевірка з'єднання між головним офісом та філіалом

Також переглянемо трасування командою tracert 192.168.2.2 (адреса PC2 філіалу) для того, щоб подивитись, через які маршрутизатори буде проходити пакет (рис. 7).

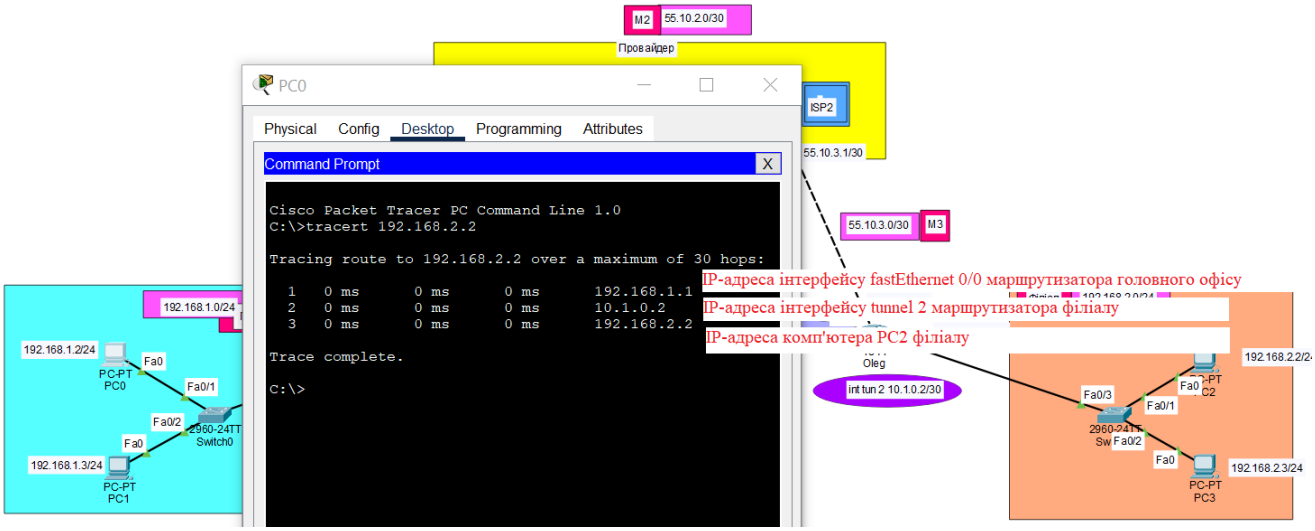


Рисунок 7 – Трасування командою tracert

Як бачимо з рис. 7, в трасуванні не відображені маршрутизатори провайдера.

Перегляд налаштувань в режимі симуляції

1. Перейти в режим симуляції (рис. 8) та відобразити в звіті в вигляді скрінів, що відбувається з пакетами при їх переміщенні по мережі.

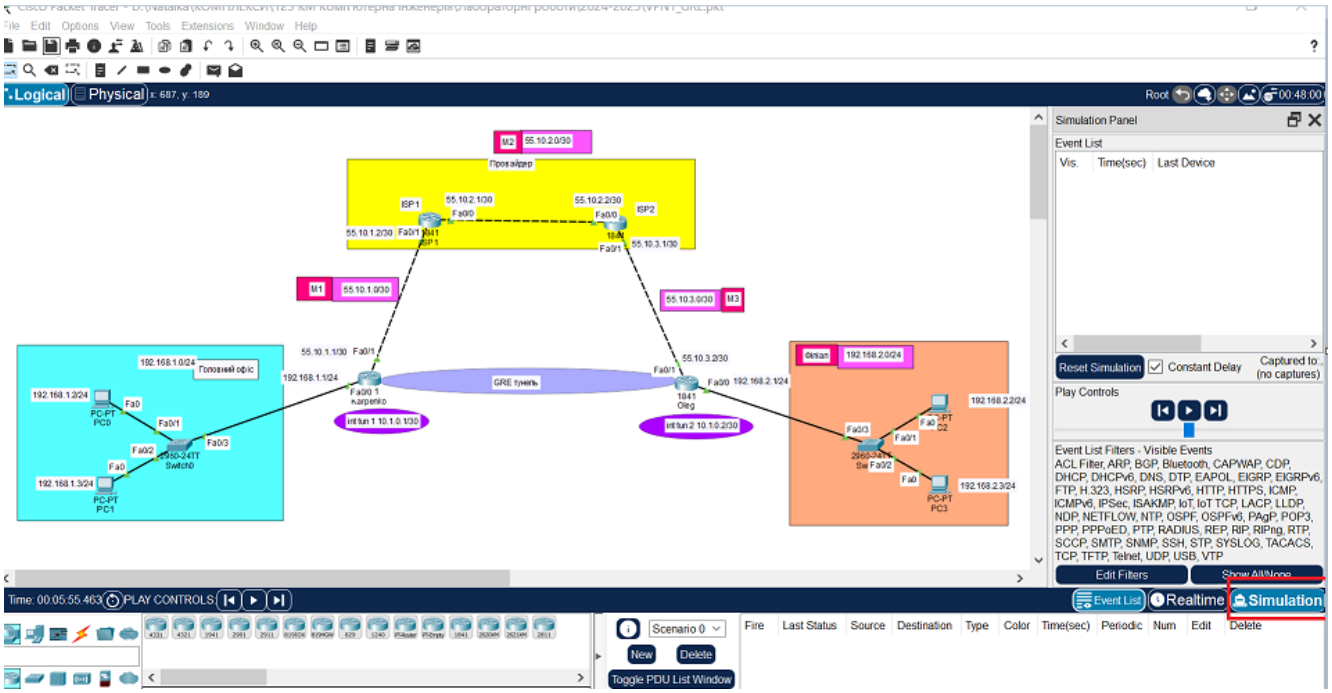


Рисунок 8 – Режим симуляції

В даному завданні в якості джерела обрати комп’ютер PC0 головного офісу, а в якості призначення комп’ютер PC2 філіалу. В фільтрах виставити відображати тільки пакети протоколу ICMP (рис. 9). Пропінгувати PC0 та PC2 (рис. 10), використавши кнопку .

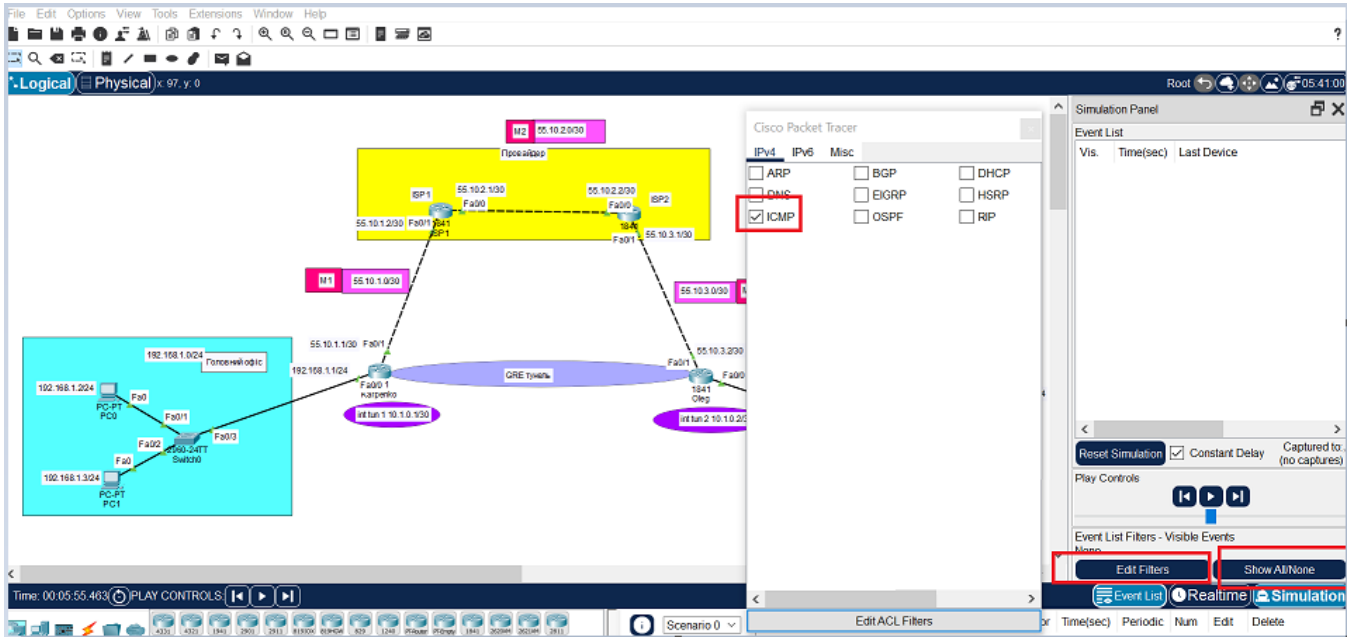


Рисунок 9 – В фільтрах відображати тільки пакети протоколу ICMP

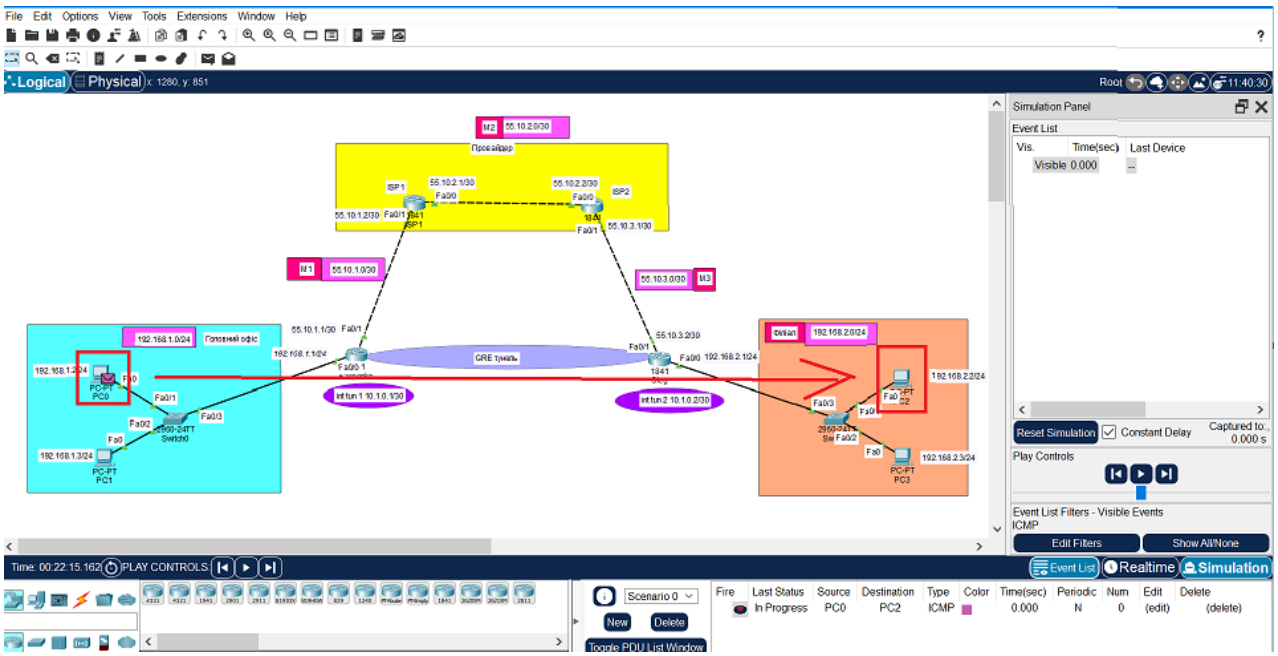


Рисунок 10 – Пропінгувати PC0 та PC2

Натиснути кнопку  (Capture) два рази (рис. 11), переглянути, що відбувається з пакетом. Спочатку пакет переміститься на комутатор, а потім на маршрутизатор. Клацнути по пакету на маршрутизаторі один раз для того, щоб подивитись, що знаходиться в середині пакету (рис. 12).

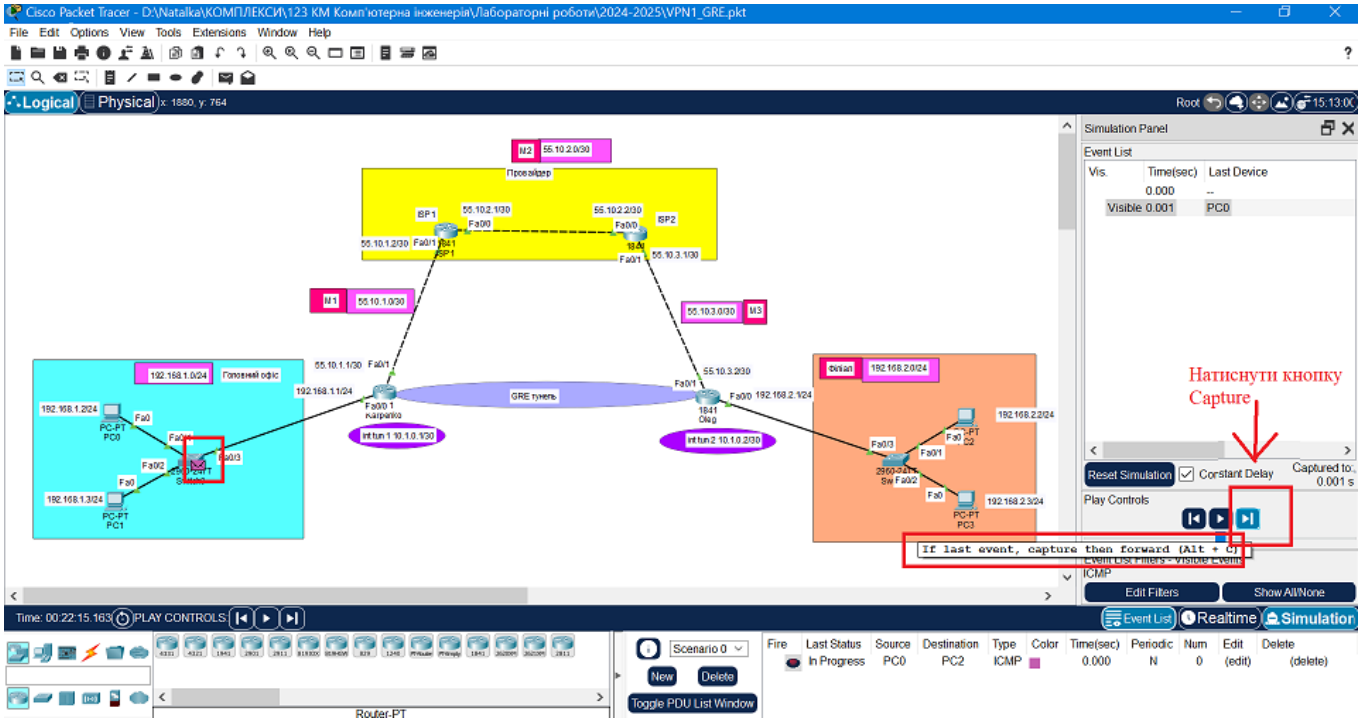


Рисунок 11 – Перегляд переміщення пакету з комп’ютера на комутатор

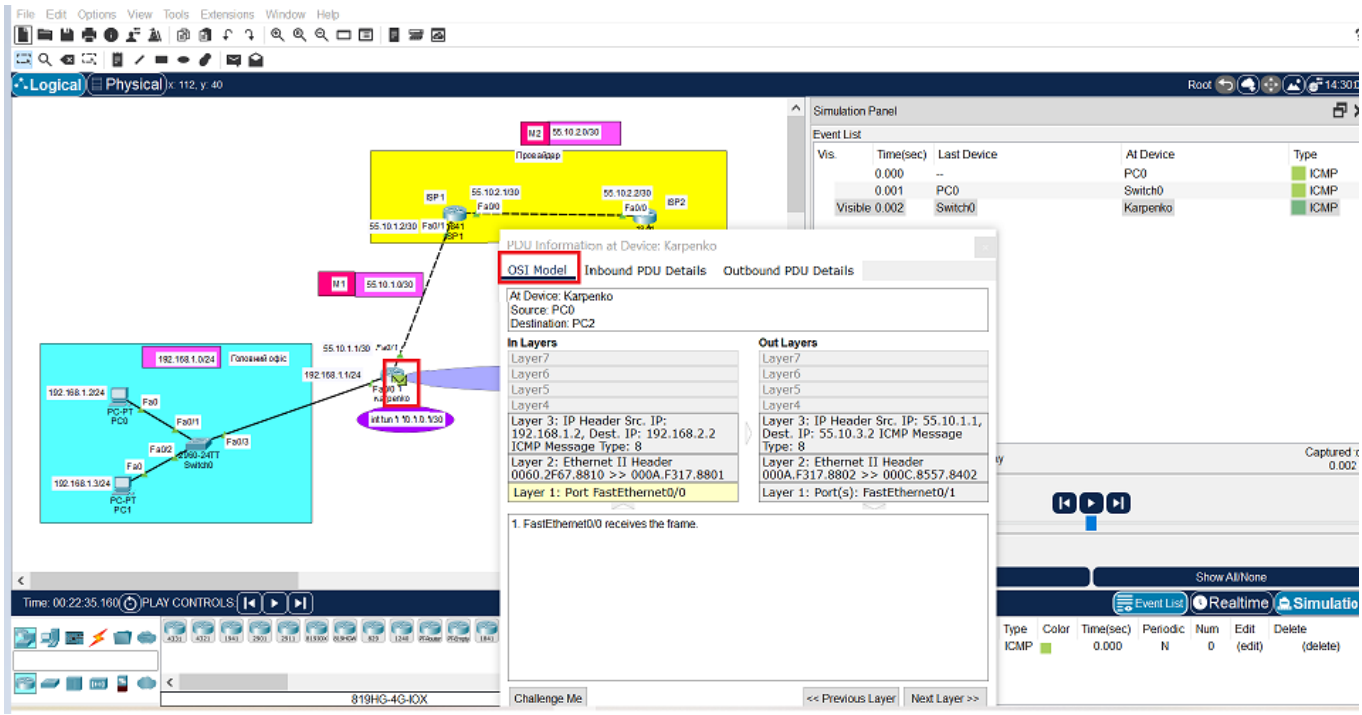


Рисунок 12 – Перегляд вмісту пакету на маршрутизаторі головного офісу

Розглядаючи вміст даного пакету (рис. 13), бачимо, що на вході в маршрутизатор в якості джерела вказана IP-адреса комп’ютера PC0 192.168.1.2 головного офісу, а в якості отримувача − IP-адреса комп’ютера PC2 192.168.2.2 філіалу.

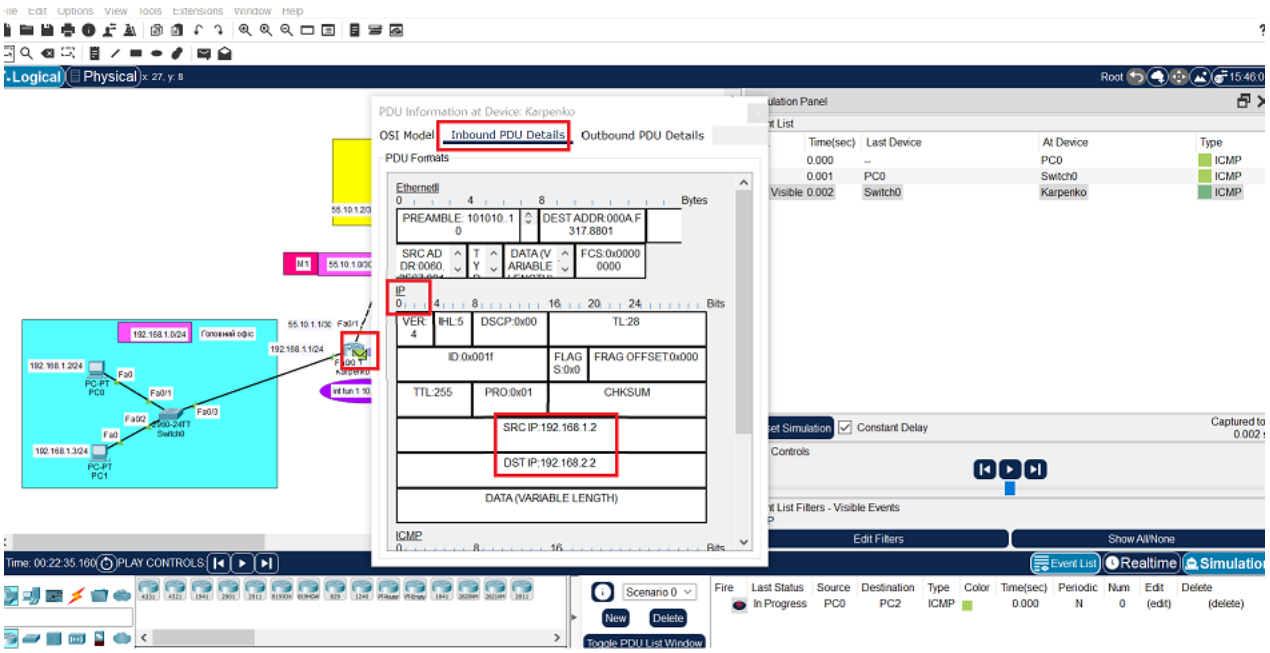


Рисунок 13 – Вхідний пакет з мережі на маршрутизатор

На виході пакета з маршрутизатора (рис. 14) можемо спостерігати процес інкапсуляції, тобто, пакет, який був надісланий з PC0 упакувався в інший пакет, і вже в якості джерела вказана IP-адреса інтерфейсу fastEthernet 0/1 маршрутизатора головного офісу 55.10.1.1, а в якості призначення вказана IP-адреса інтерфейсу fastEthernet 0/1 маршрутизатора філіалу 55.10.3.2.

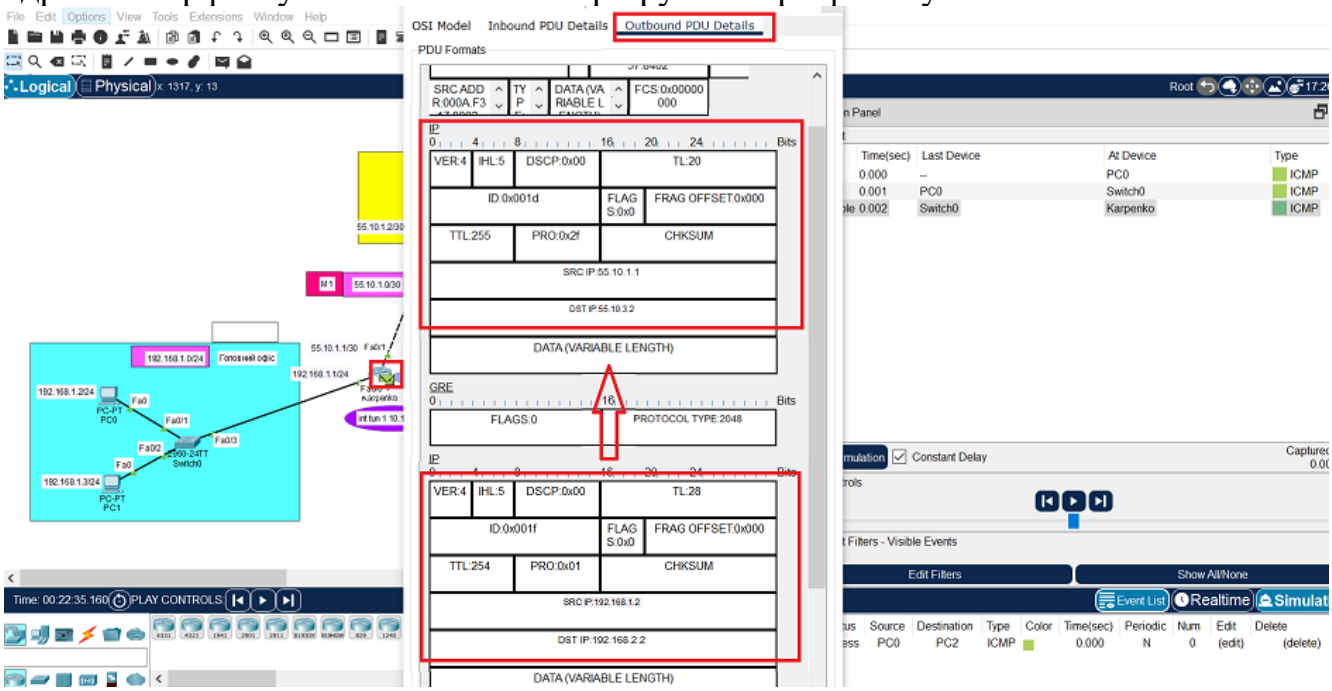


Рисунок 14 – Інформація про вихідний пакет з маршрутизатора головного офісу

Натиснути ще один раз кнопку  (Capture). Пакет перемістився з маршрутизатора головного офісу на маршрутизатор провайдера ISP1. В якості джерела та отримувача вміст пакету не змінився (рис. 15-17).

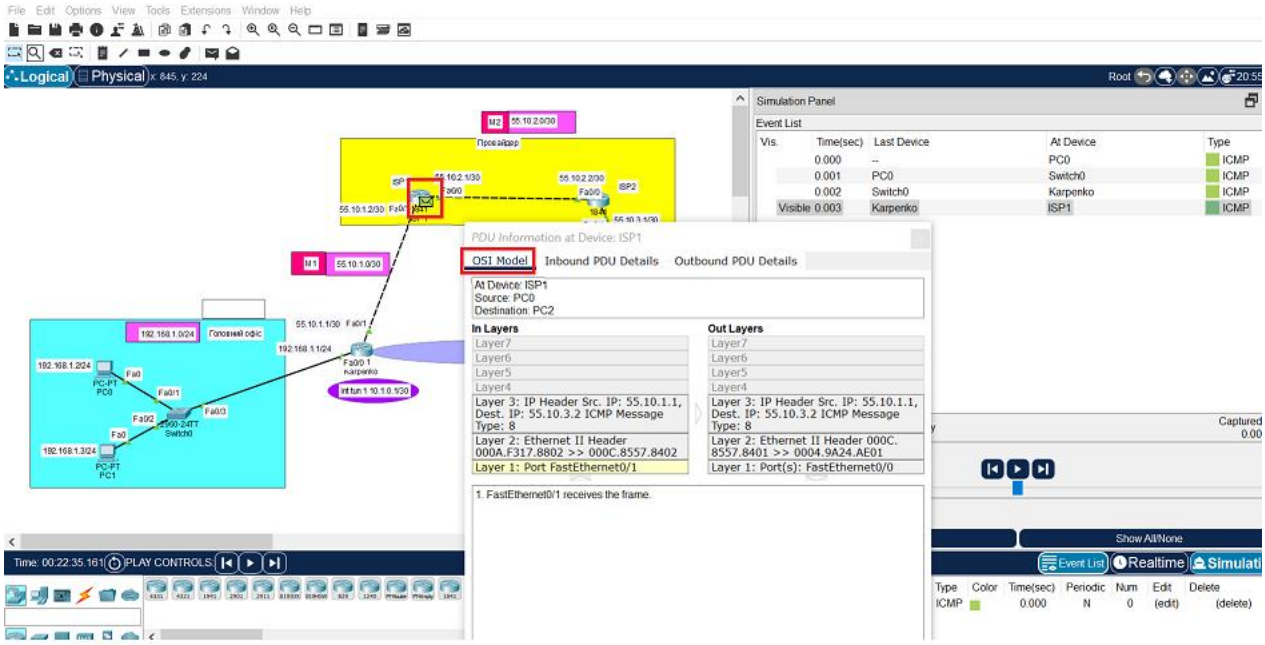


Рисунок 15 – Інформація про пакет на маршрутизаторі ISP1

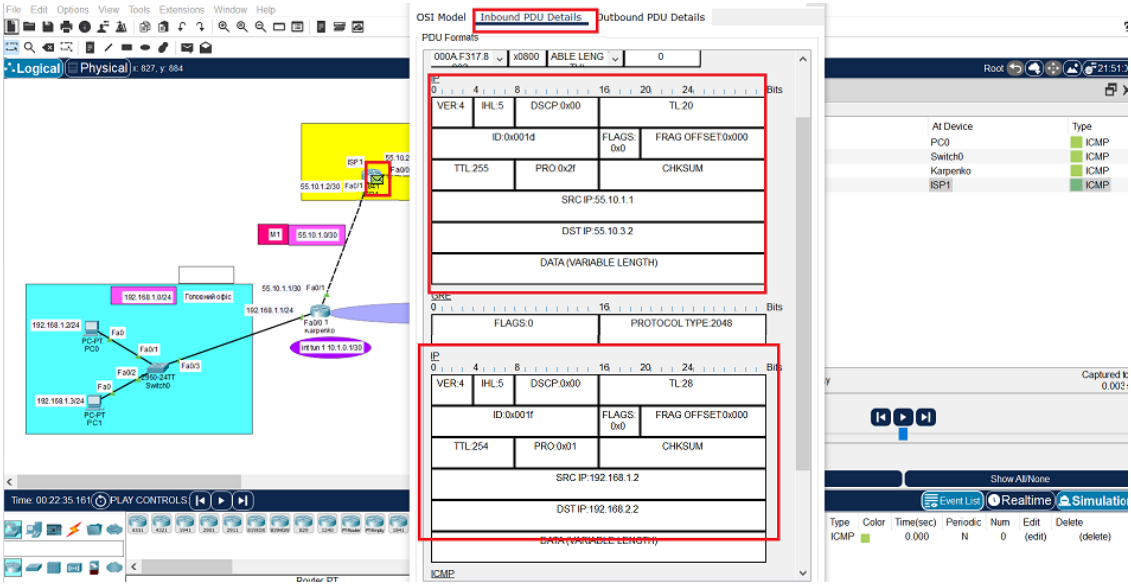


Рисунок 16 – Вхідний пакет з мережі на маршрутизаторі ISP1

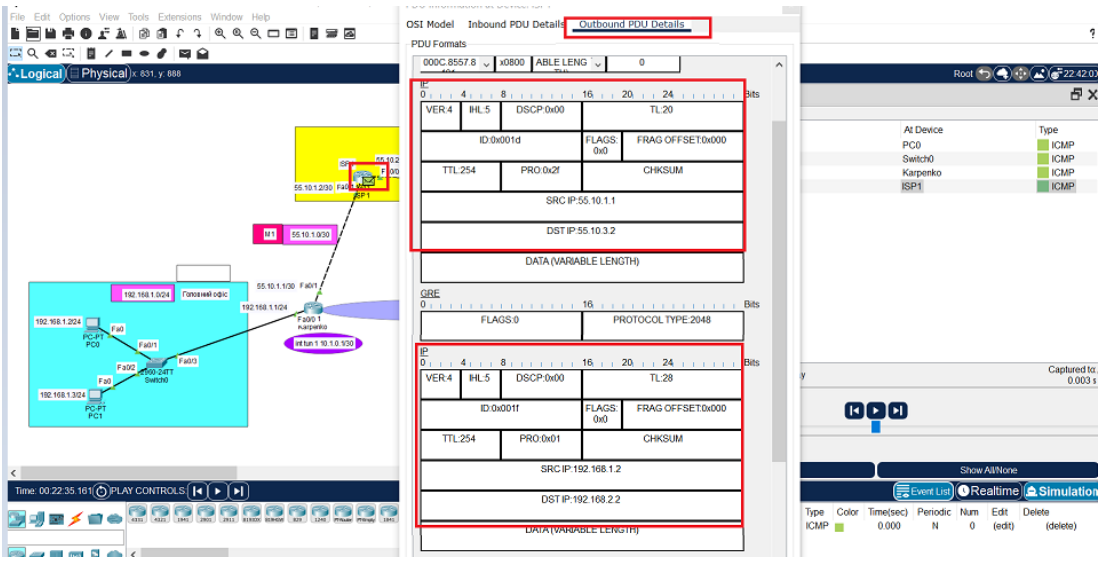


Рисунок 17 – Вихідний пакет з мережі на маршрутизаторі ISP1

Натиснути ще два рази кнопку  (Capture). Пакет перемістився з маршрутизатора ISP1 на маршрутизатор філіалу (рис. 18).

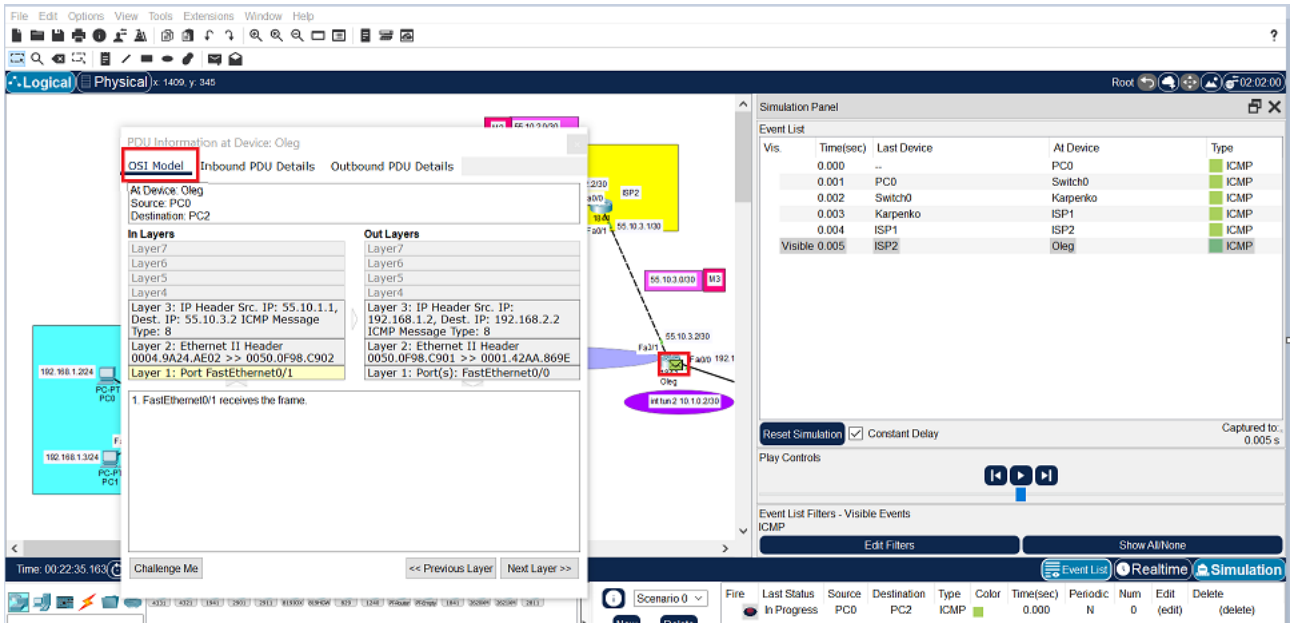


Рисунок 18 – Інформація про пакет на маршрутизаторі філіалу

На вході в маршрутизатор філіалу пакет все ще інкапсульований (рис. 19), а на виході (рис. 20) вже спостерігається процес деінкапсуляції, тобто, пакет розпакувався і знову в якості джерела вказана IP-адреса комп'ютера PC0 192.168.1.2 головного офісу, а в якості отримувача − IP-адреса комп'ютера PC2 192.168.2.2 філіалу.

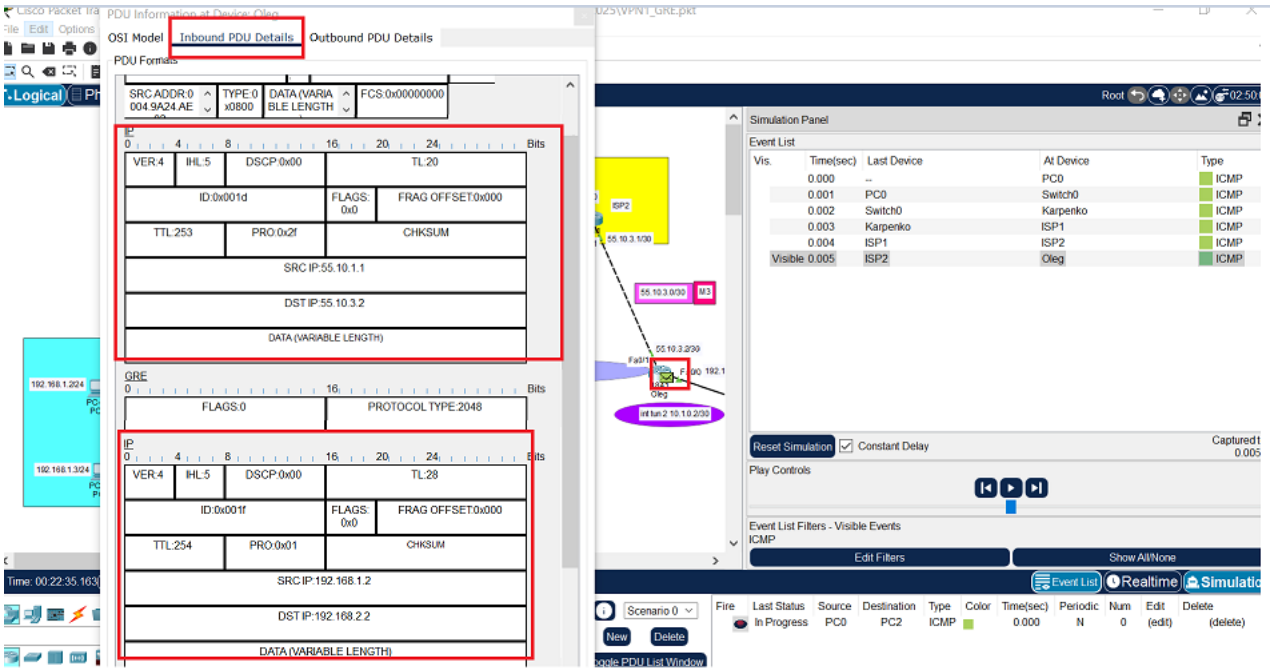


Рисунок 19 – Вхідний пакет з мережі на маршрутизаторі філіалу

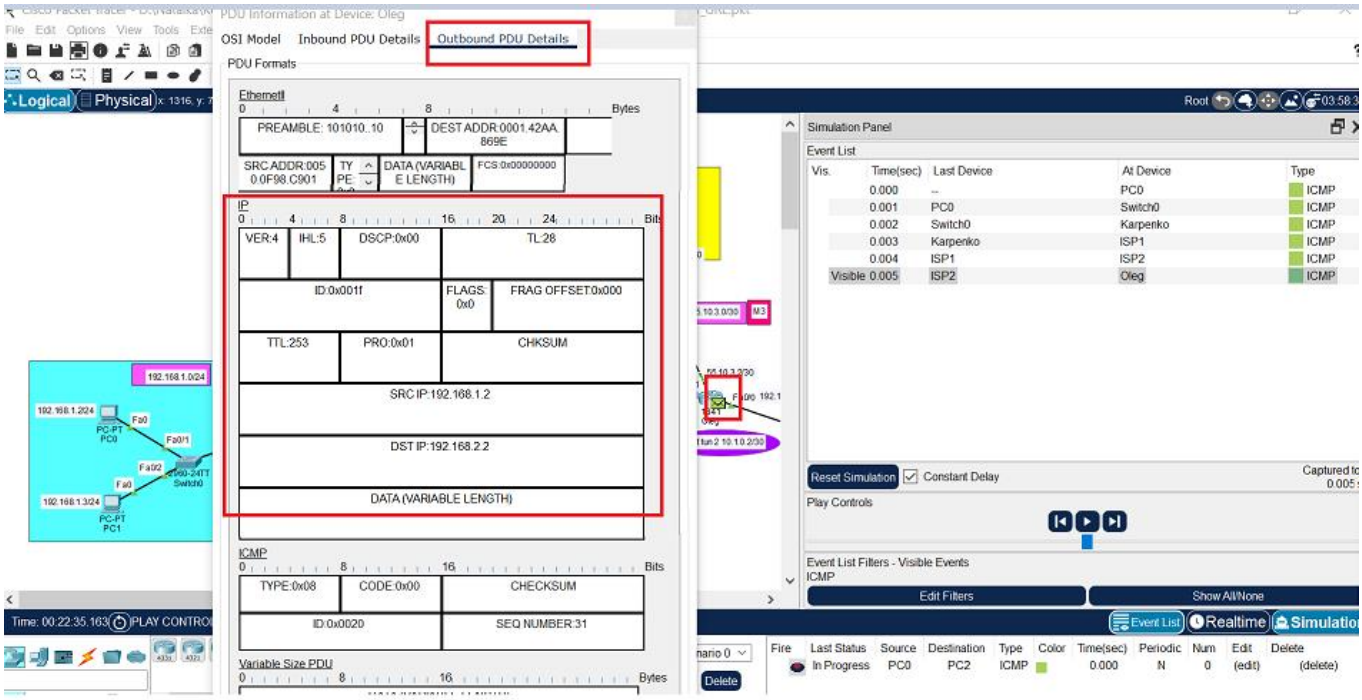


Рисунок 20 – Вихідний пакет з мережі на маршрутизаторі філіалу

Натиснути ще два рази кнопку (Capture) і пакет переміститься на комутатор, а тоді на PC2 (рис. 21).

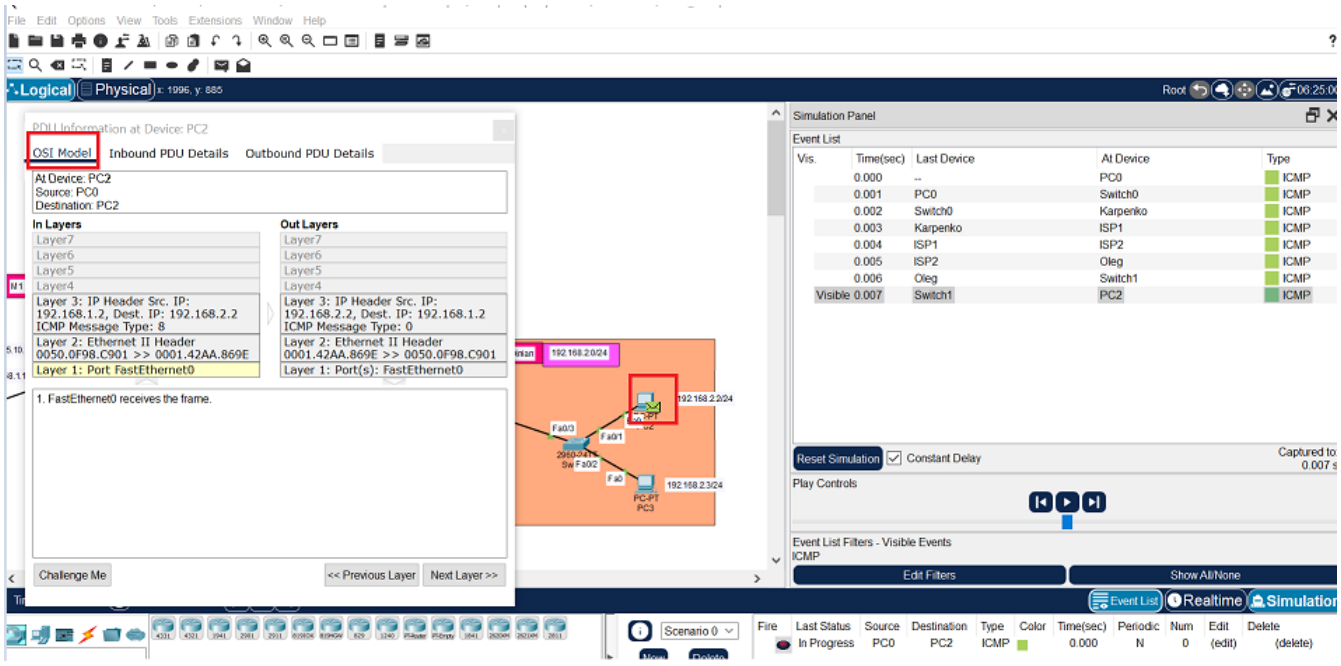


Рисунок 21 –Переміщення пакету на PC2

На рисунках 22 та 23 зображено вигляд вихідного та вхідного пакету, який знаходиться на PC2.

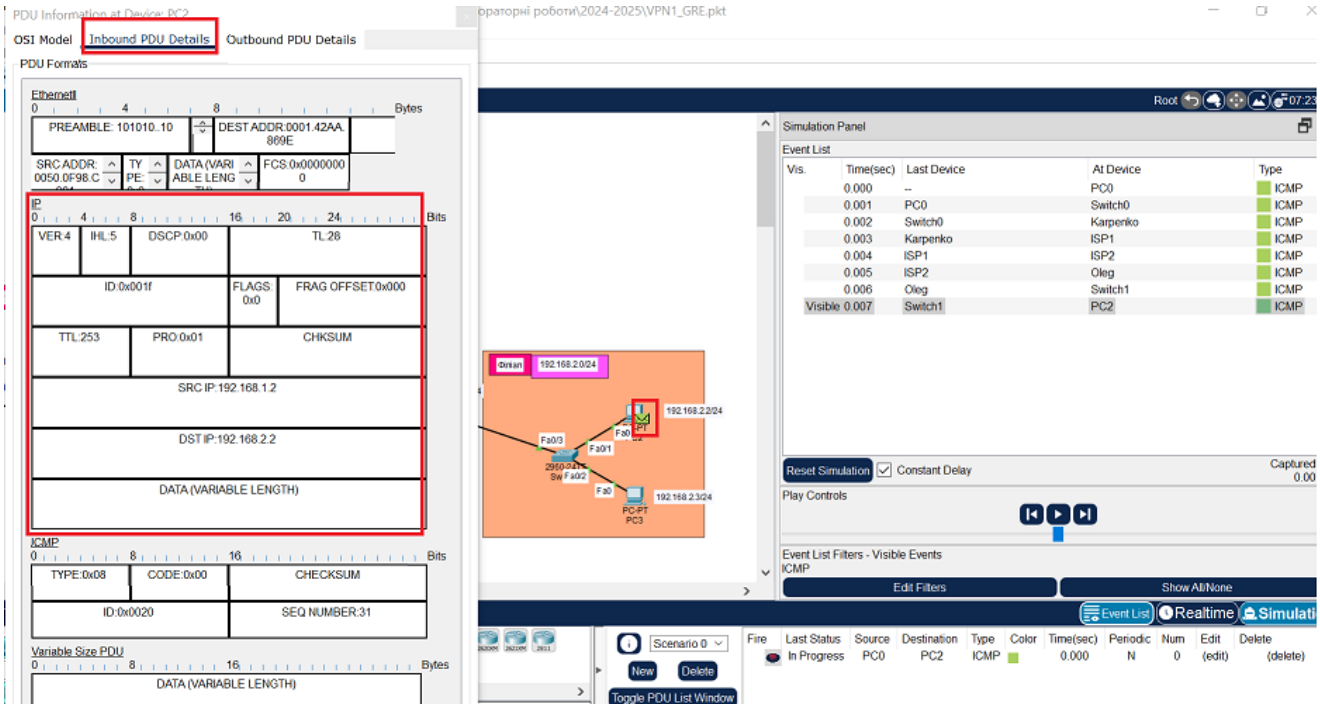


Рисунок 22 – Вхідний пакет на PC2

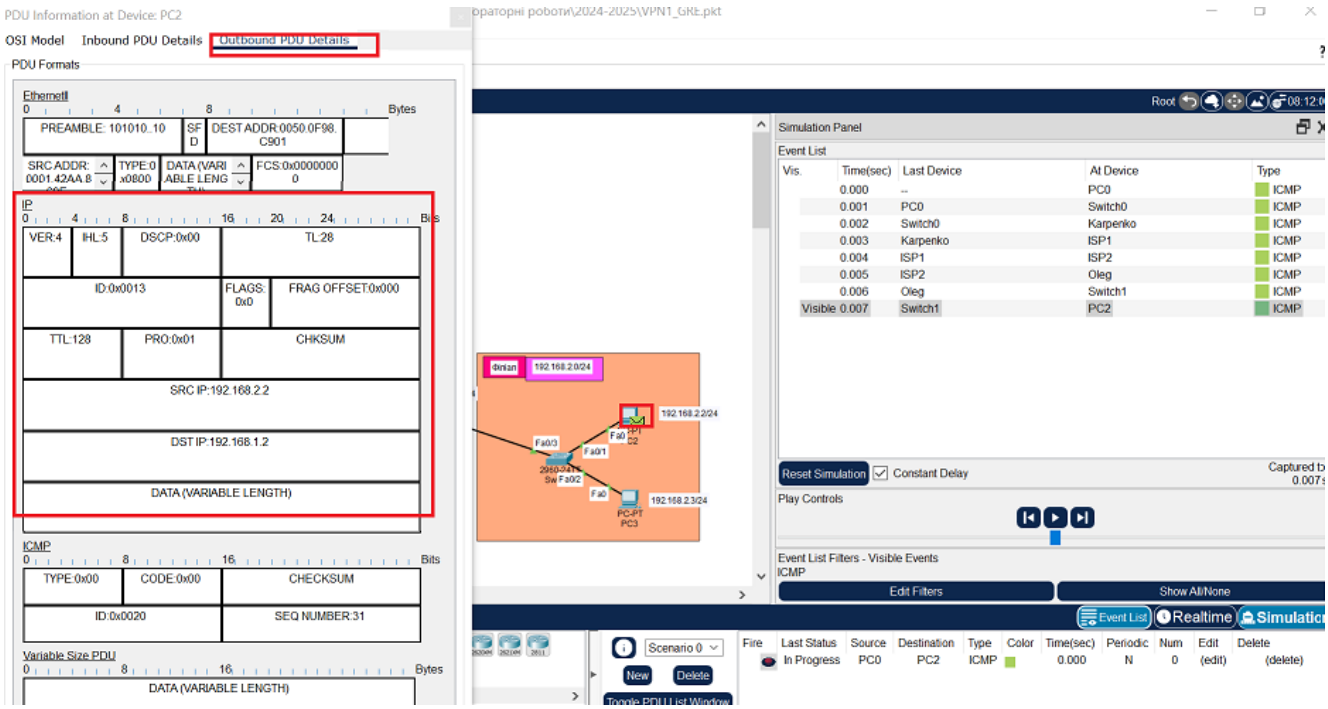


Рисунок 23 – Вихідний пакет на PC2

Коли відбудеться надсилання пакета-відповіді з PC2, явище інкапсуляції та деінкапсуляції відбувається аналогічно, як описано вище.

Натиснути два рази кнопку  (Capture). Пакет переміститься спочатку на комутатор, а тоді на машрутизатор філіалу (рис. 24-26). Спочатку на машрутизаторі філіалу вхідний пакет буде в початковому стані (рис. 25), а на виході він вже буде інкапсульований (рис. 26).

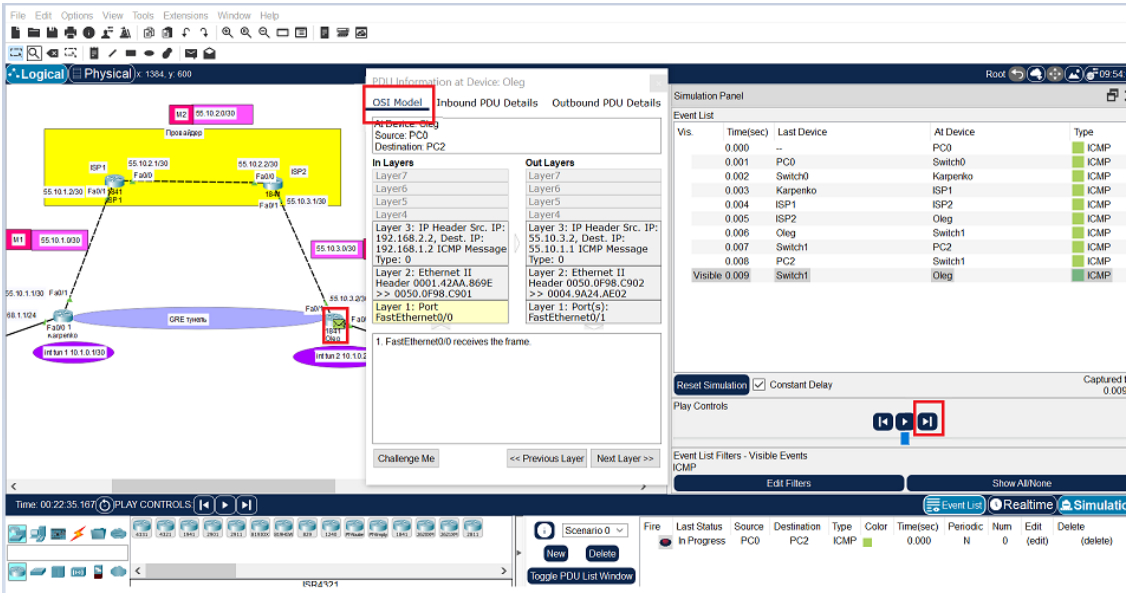


Рисунок 24 – Вкладка Модель OSI

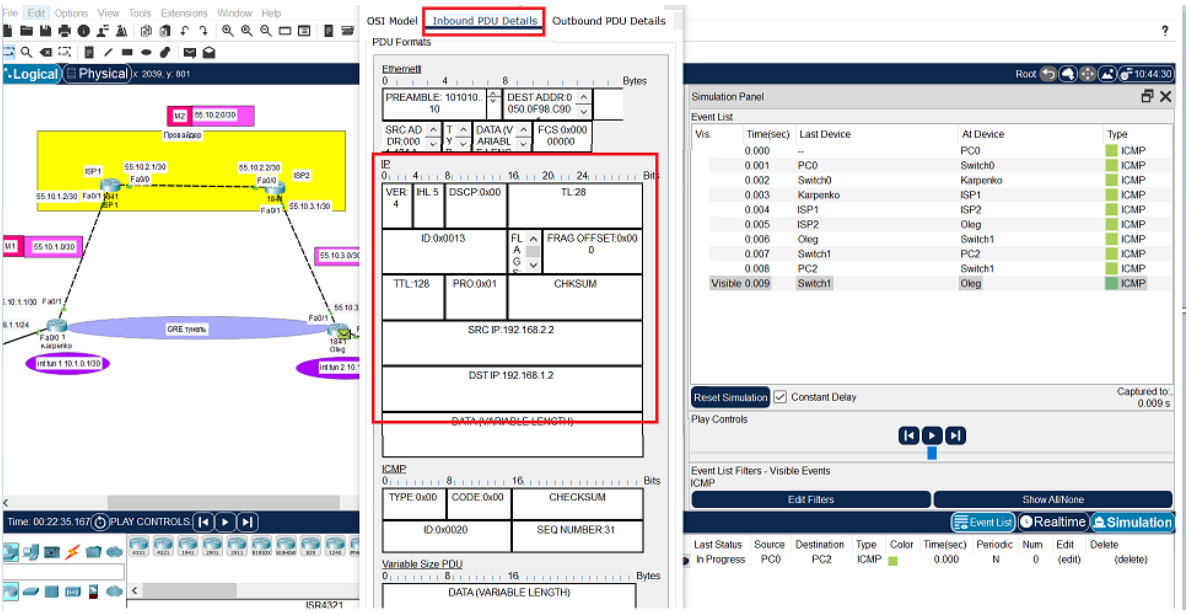


Рисунок 25 – Вхідний пакет на машрутизаторі філіалу

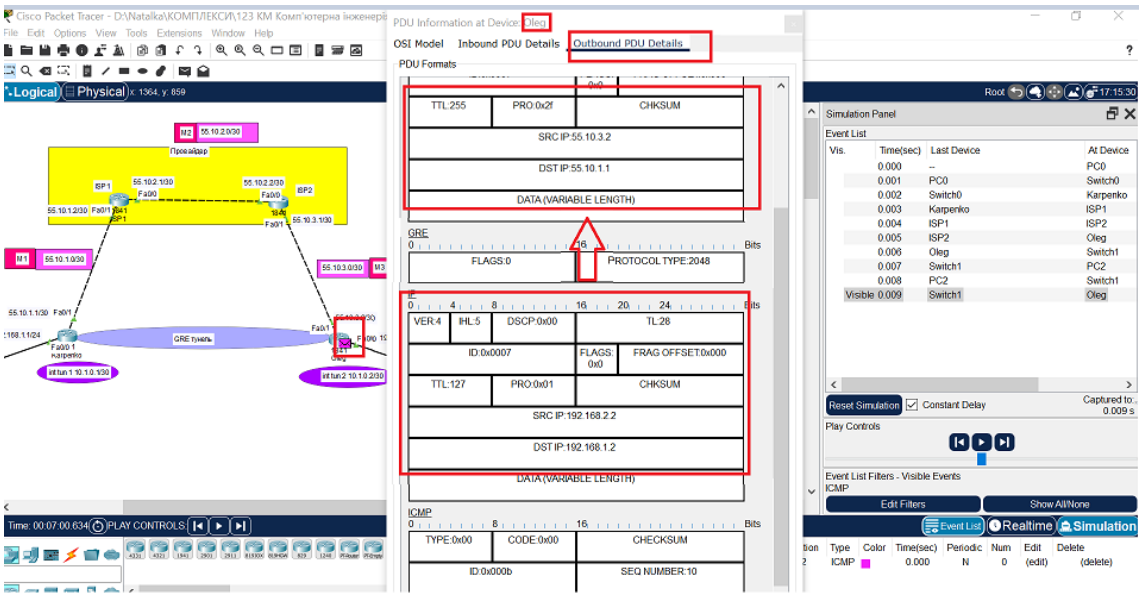


Рисунок 26 – Вихідний пакет на машрутизаторі філіалу (інкапсульований)

Натиснути ще три рази кнопку (Capture) (за ці три переходи поля IP-пакетів будуть не змінними, так як машрутизатори їх тільки пересилають). Але коли пакет переміститься на маршрутизатор головного офісу, то на вході пакет буде ще інкапсульований (рис. 27), а на виході відбудеться деінкапсуляція (рис. 28).

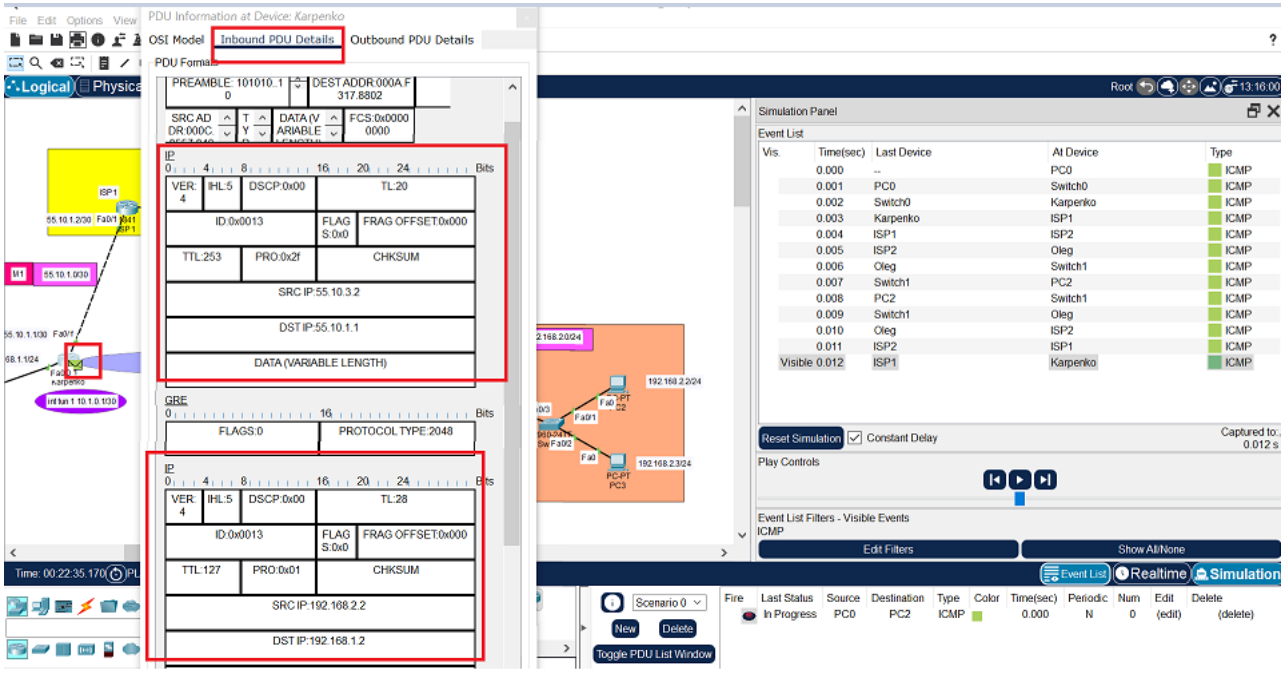


Рисунок 27 – Вхідний пакет на маршрутизаторі головного офісу

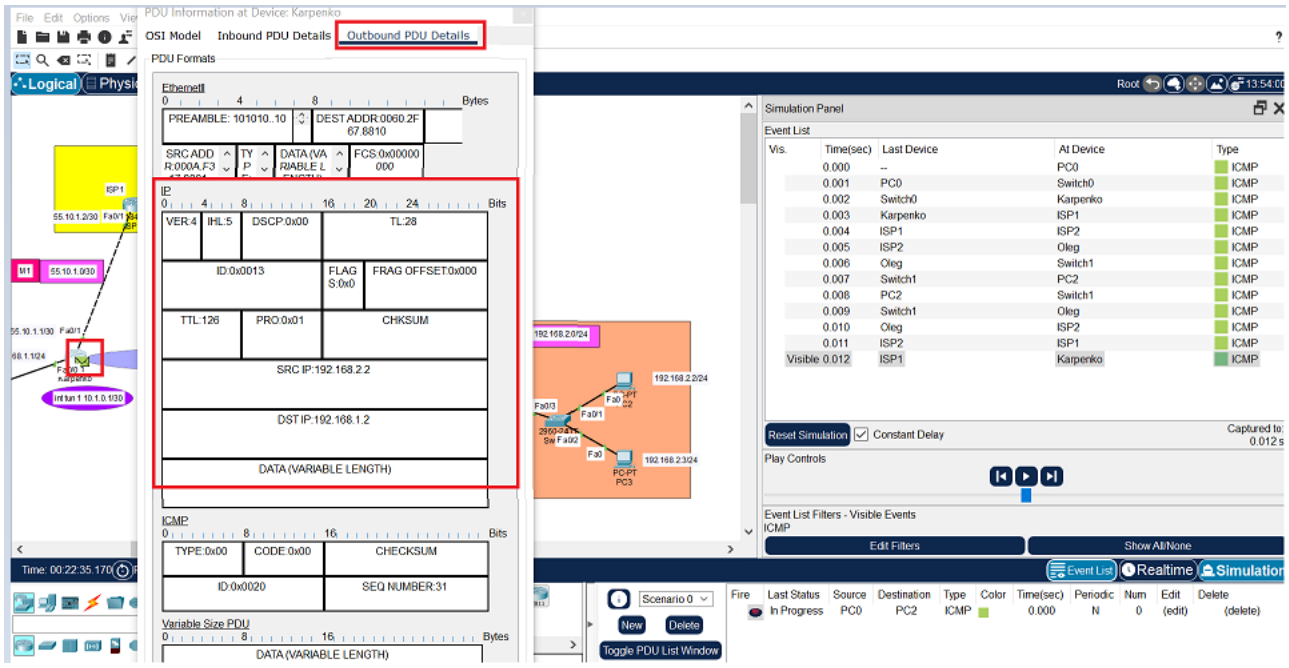


Рисунок 28 – Вихідний пакет на маршрутизаторі головного офісу

Натиснути ще два рази кнопку (Capture) і пакет з відповіддю досягне комп’ютера PC0 (рис. 29).

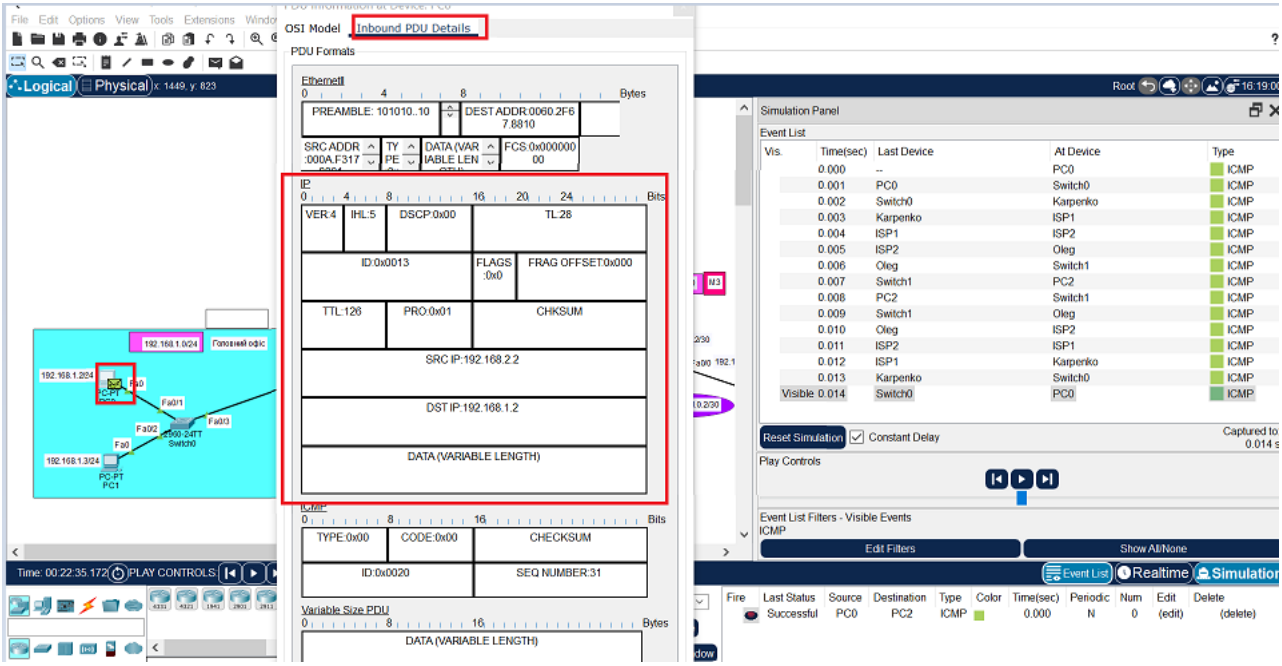


Рисунок 29 – Пакет з відповіддю досягнув комп’ютер PC0

Якщо спробувати відправити пакет в мережу, наприклад, філіалу з маршрутизатора ISP1 (натиснути кнопку , тоді спочатку клацтути по маршрутизатору ISP1, далі клацнути по комп’ютеру PC2 філіалу і натиснути кнопку (Capture) , то цей пакет навіть не буде надісланий (рис. 30-31). Тобто, для інших вузлів мережі хости мереж головного офісу та філіалу недоступні. Це відбувається тому, що, наприклад, на маршрутизаторі ISP1, немає маршруту в дані мережі. Перевірити це можна , ввівши на маршрутизаторі ISP1 та ISP2 команду для перегляду таблиці маршрутизації **show ip route** (рис. 32-33).

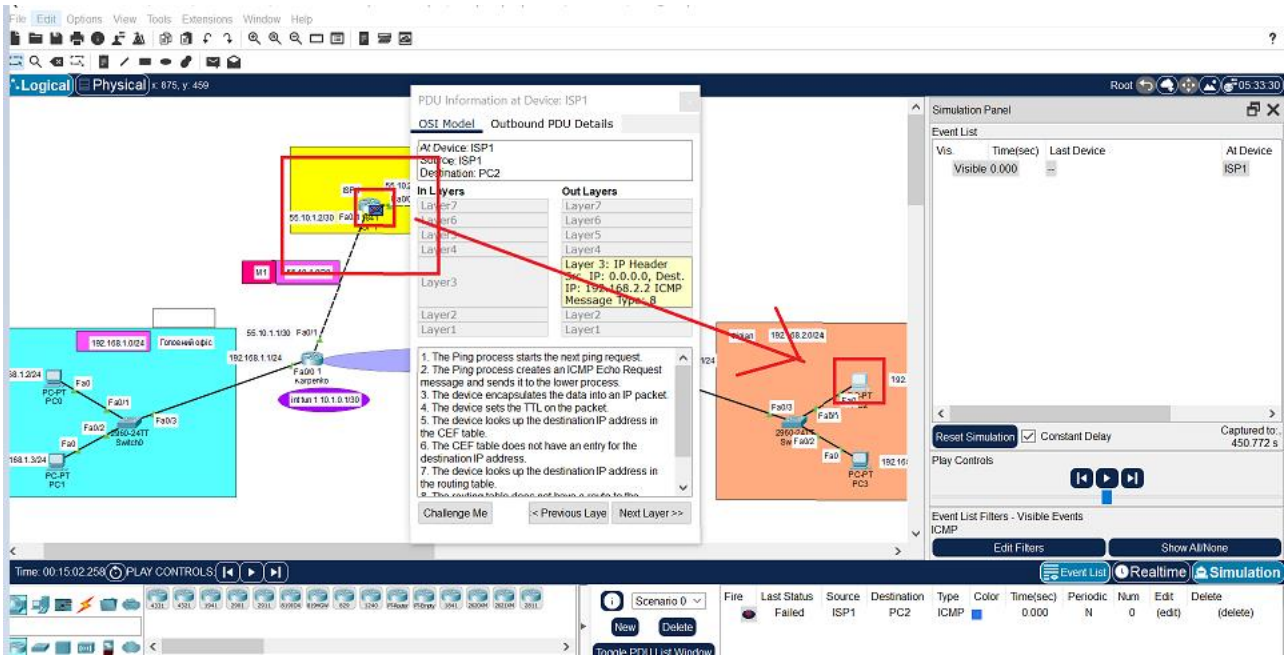


Рисунок 30 – Відправка пакету в мережу філіалу з маршрутизатора ISP1

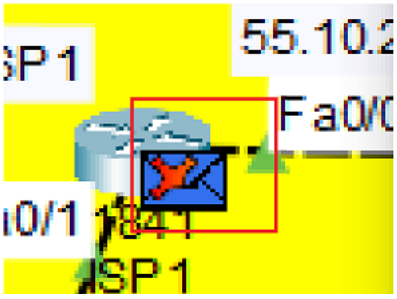


Рисунок 31 – На схемі отримаємо відображення пакету з перекресленим червоним хрестиком (тобто, що пакет не надсилається)

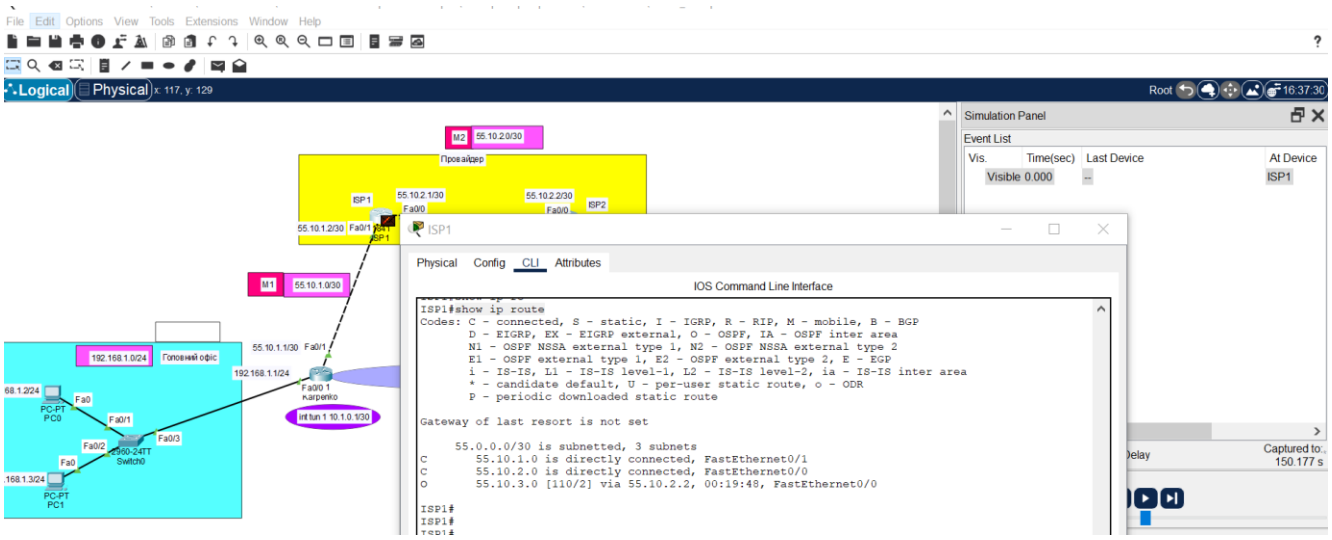


Рисунок 32 – Перегляд таблиці маршрутизації на маршрутизаторі ISP1

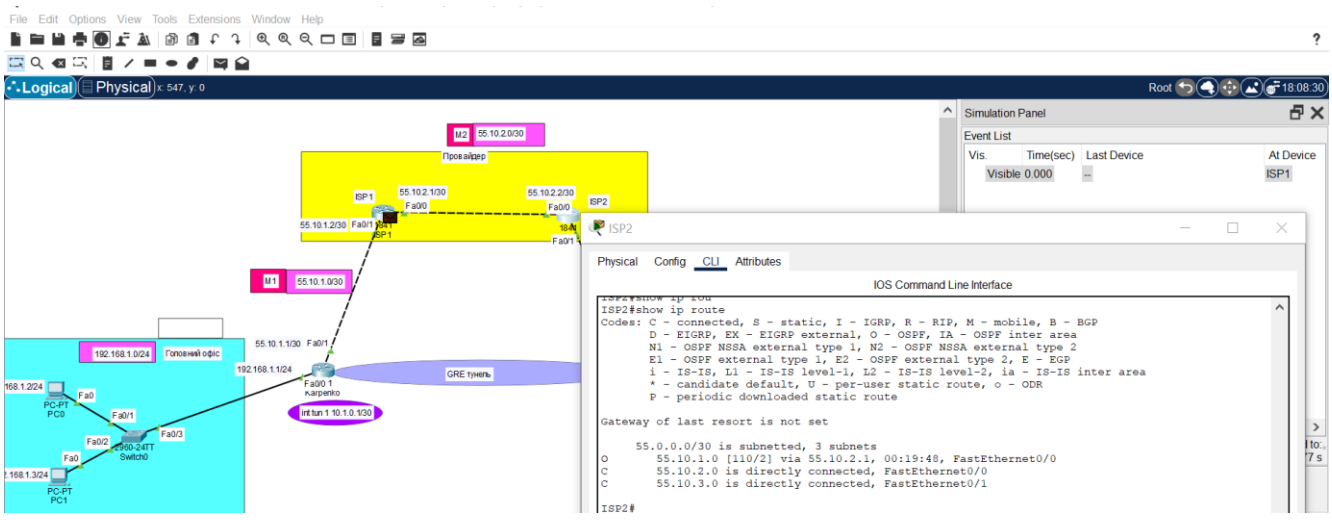


Рисунок 33 – Перегляд таблиці маршрутизації на маршрутизаторі ISP2

Варіант завдання

Таблиця 1 – Варіанти завдань

Варіант	Головний офіс, маска /24	Філіал, маска /24	M1	M2	M3	tunnel 1, маска /30	tunnel 2, маска /30
1	192.168.3.0	192.168.4.0	будь-яка публічна	будь-яка публічна	будь-яка публічна	10.1.1.1	10.1.1.2
2	192.168.5.0	192.168.6.0				10.1.2.1	10.1.2.2
3	192.168.7.0	192.168.8.0				10.1.3.1	10.1.3.2
4	192.168.9.0	192.168.10.0				10.1.4.1	10.1.4.2
5	192.168.11.0	192.168.12.0				10.1.5.1	10.1.5.2

Продовження таблиці 1

Варіант	Головний офіс, маска /24	Філіал, маска /24	M1	M2	M3	tunnel 1, маска /30	tunnel 2, маска /30
6	192.168.13.0	192.168.14.0	будь-яка публічна адреса класу A, маска 255.255.255.252 (/30)	будь-яка публічна адреса класу B, маска 255.255.255.252 (/30)	будь-яка публічна адреса класу C, маска 255.255.255.252 (/30)	10.1.6.1	10.1.6.2
7	192.168.15.0	192.168.16.0				10.1.7.1	10.1.7.2
8	192.168.17.0	192.168.18.0				10.1.8.1	10.1.8.2
9	192.168.19.0	192.168.20.0				10.1.9.1	10.1.9.2
10	192.168.21.0	192.168.22.0				10.1.10.1	10.1.10.2
11	192.168.23.0	192.168.24.0				10.1.11.1	10.1.11.2
12	192.168.25.0	192.168.26.0				10.1.12.1	10.1.12.2
13	192.168.27.0	192.168.28.0				10.1.13.1	10.1.13.2
14	192.168.29.0	192.168.30.0				10.1.14.1	10.1.14.2
15	192.168.31.0	192.168.32.0				10.1.15.1	10.1.15.2
16	192.168.33.0	192.168.34.0				10.1.16.1	10.1.16.2
17	192.168.35.0	192.168.36.0				10.1.17.1	10.1.17.2
18	192.168.37.0	192.168.38.0				10.1.18.1	10.1.18.2
19	192.168.39.0	192.168.40.0				10.1.19.1	10.1.19.2
20	192.168.41.0	192.168.42.0				10.1.20.1	10.1.20.2
21	192.168.43.0	192.168.44.0				10.1.21.1	10.1.21.2
22	192.168.45.0	192.168.46.0				10.1.22.1	10.1.22.2
23	192.168.47.0	192.168.48.0				10.1.23.1	10.1.23.2
24	192.168.49.0	192.168.50.0				10.1.24.1	10.1.24.2
25	192.168.51.0	192.168.52.0				10.1.25.1	10.1.25.2
26	192.168.53.0	192.168.54.0				10.1.26.1	10.1.26.2
27	192.168.55.0	192.168.56.0				10.1.27.1	10.1.27.2
28	192.168.57.0	192.168.58.0				10.1.28.1	10.1.28.2
29	192.168.59.0	192.168.60.0				10.1.29.1	10.1.29.2
30	192.168.61.0	192.168.62.0				10.1.30.1	10.1.30.2
31	192.168.63.0	192.168.64.0				10.1.31.1	10.1.31.2
32	192.168.65.0	192.168.66.0				10.1.32.1	10.1.32.2

Примітка. Комбінація клавіш **Ctrl Shift 6** − дозволяє користувачеві перервати процес IOS, наприклад, ping або traceroute.

ПЕРЕЛІК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Курс мережевої академії Cisco Packet Tracer (Курс-інструкція до симулятору мереж та IoT). Доступний з URL: http://surl.li/mimft (дата звернення: 14.10.2024).
2. Курс Мережевої академії Cisco CCNAv7: Introduction to Networks URL: https://www.netacad.com/courses/networking/ccna-introduction-networks (дата звернення: 18.11.2024).
3. Курс Мережевої академії Cisco CCNAv7: Switching, Routing, and Wireless Essentials URL: https://www.netacad.com/courses/networking/ccna-switching-routing-wireless-essentials (дата звернення: 29.11.2024).
4. NetAcademy - Networking101Lite Перша сесія «Модель OSI/Мережі/Базові налаштування обладнання». URL: http://surl.li/eoiux (дата звернення: 02.12.2024)
5. Networking101Lite Сесія №4 «Динамічне назначення IP адрес. DHCP». URL: http://surl.li/eoivc (дата звернення: 10.12.2025)
6. Networking101Lite Друга сесія «Другий (канальний) рівень OSI моделі. Ethernet. Комутація. VLAN». URL: http://surl.li/eoiuy (дата звернення: 15.12.2024).
7. Admin. What is the Secure Shell (SSH) Protocol? | SSH Academy. PAM solutions, Key Management Systems, Secure File Transfers | SSH. URL: https://www.ssh.com/academy/ssh/protocol (date of access: 24.12.2024).
8. Богдан Комп'ютерний. SSH: як підключитися до іншого пристрою через командний рядок? | IT довідник, 2024. YouTube. URL: https://www.youtube.com/watch?v=LNG5bfg6Bc0 (дата звернення: 14.01.2025).
9. Networking101Lite Третя сесія «Третій (мережевий) рівень OSI моделі. IP. Маршрутизація». URL: http://surl.li/eoiuz (дата звернення: 17.01.2025)
10. Networking101Lite Сесія №9 «Динамічна маршрутизація/OSPF URL: http://surl.li/eoivq (дата звернення: 22.02.2025)
11. Курс Мережевої академії Cisco CCNAv7: CCNA: Enterprise Networking, Security, and Automation https://www.netacad.com/courses/ccna-enterprise-networking-security-automation?courseLang=en-US (дата звернення: 18.03.2025).
12. Networking101Lite Сесія №5 «Мережева взаємодія. Сокети. Утиліти для мережевого інженера». URL: http://surl.li/eoive (дата звернення: 12.04.2025)
13. Networking101Lite Сесія №6 «Контроль трафіку. Списки доступу. Налаштування контролю». URL: http://surl.li/eoivg (дата звернення: 15.04.2025)
14. Networking101Lite Сесія №7 « Трансляція IP адрес. Доступ в Інтернет. NAT». URL: http://surl.li/eoivi (дата звернення: 18.04.2025).
15. Основи мереж та IoT. Основи NAT у Cisco Packet Tracer, 2023. YouTube. URL: https://www.youtube.com/watch?v=Y3iQWpqYXj4 (дата звернення: 11.05.2025).
16. Networking101Lite Сесія №8 « VPN/Захист даних при передачі/IPSec». URL: http://surl.li/eoivm (дата звернення: 20.04.2025).
17. Networking101Lite Сесія №10 «Динамічна маршрутизація/bgp». URL: http://surl.li/eoivr (дата звернення: 23.04.2025)
18. Задерейко О. В., Багнюк Н.В., Толокнов А. А. Комп'ютерні мережі : навчально-методичний посібник для підготовки здобувачів вищої освіти галузі

знань 12 «Інформаційні технології». URL: http://hdl.handle.net/11300/25951 (дата звернення: 20.05.2025).

К17 Комп’ютерні мережі: методичні вказівки до лабораторних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Комп’ютерна інженерія» галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія денної та заочної форм навчання / уклад. Н. В. Багнюк, К. Я. Бортник. Луцьк: ЛНТУ, 2025. 118 с.

Методичне видання до до лабораторних занять з дисципліни «Комп’ютерні мережі» складене відповідно до діючої програми курсу.

Призначене для здобувачів вищої освіти спеціальності 123 Комп’ютерна інженерія освітньої програми «Комп’ютерна інженерія».

Комп’ютерний набір Н. В. Багнюк

Редактор Н. В. Багнюк

Підп. до друку «___» _____ 2025р.

Формат 60х84/16. Папір офс. Гарнітура Таймс.

Ум. друк. арк. ____. Тираж 10 прим. Зам. ____

Відділ іміджу та промоцій

Луцького національного технічного університету

43018, м. Луцьк, вул. Львівська, 75