Міністерство освіти і науки України

ІНФОРМАЦІЙНІ МЕРЕЖІ ТА АДМІНІСТРУВАННЯ

Методичні вказівки до практичних занять
для здобувачів першого (бакалаврського) рівня вищої освіти
освітньої програми
«Інформаційні системи та технології охорони і безпеки»
галузь знані 12 (F) Інформаційні технології
спеціальності 126 (F6) Інформаційні системи та технології
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: _____ Роман ГРУДЕЦЬКИЙ, сарший викладач кафедри автоматизації та комп'ютерно-інтегрованих технологій, проректор з НПР та цифрової трансформації ЛНТУ

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

І-74 Інформаційні мережі та адміністрування: методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спеціальності 126 (F6) Інформаційні системи та технології денної та заочної форм навчання / уклад. Н. В. Багнюк, К. Я. Бортник. Луцьк: ЛНТУ, 2025.132 с.

Методичне видання до практичних занять з дисципліни «Інформаційні мережі та адміністрування» складено відповідно до діючої програми курсу.

Призначене для здобувачів вищої освіти спеціальності 126 (F6) Інформаційні системи та технології освітньої програми «Інформаційні системи та технології охорони і безпеки».

ЗМІСТ

ВСТУП

Методичні вказівки призначені для практичних занять з дисципліни «Інформаційні мережі та адміністрування». Їх метою є формування та розвиток у здобувачів вищої освіти практичних умінь і професійних компетентностей, пов’язаних із побудовою, налаштуванням, адмініструванням та тестуванням мережевої інфраструктури. Робота з мережевими пристроями, програмними симуляторами та серверними службами сприяє закріпленню теоретичних знань, отриманих під час вивчення дисципліни, та їх застосуванню для вирішення реальних інженерних завдань.

У процесі виконання завдань студенти опановують сучасні інструменти і технології, працюють з офіційною документацією та технічними інструкціями, аналізують конфігураційні сценарії, навчаються застосовувати алгоритми налаштування мережевих протоколів, сервісів і серверних ролей. Практична діяльність включає роботу з мережевою адресацією IPv4/IPv6, конфігурування комутаторів і маршрутизаторів, реалізацію VLAN, статичної та динамічної маршрутизації, налаштування служб DHCP, NAT, VPN, а також адміністрування мережевих сервісів Windows Server і Linux.

Виконання практичних робіт сприяє розвитку навичок роботи з інтерфейсом командного рядка, аналізу таблиць маршрутизації, діагностики мережевих подій і несправностей, документування конфігурацій та прийняття обґрунтованих інженерних рішень. Також приділяється увага аспектам інформаційної безпеки: моніторингу мережевої активності, застосуванню політик доступу, аудитів та протидії мережевим загрозам.

Всі студенти обов’язково авторизуються на платформі https://www.netacad.com та реєструються на курси CCNA. Курс «Вступ до мереж» на платформі https://www.netacad.com імплементований в робочу програму дисципліни «Інформаційні мережі та адміністрування». В основному цей курс виноситься на самостійне опрацювання студентів, але окремі практичні завдання винесені на практичні заняття та лабораторні роботи (відповідно вказано запозичення даного матеріалу з цих ресурсів згідно вимог до оформлення посилання на літературні джерела), що зазначено в робочій програмі дисципліни. Також вивчаються окремі розділи курсів «Основи комутації, маршрутизації та бездротових мереж» та «Побудова, безпека і автоматизація корпоративних мереж».

Таким чином, дані методичні вказівки забезпечують практичну підготовку здобувачів вищої освіти у сфері інформаційні системи та технології, сприяють формуванню цілісних знань і компетентностей з побудови та адміністрування комп’ютерних мереж і систем та є важливим елементом професійної підготовки майбутніх фахівців.

Практичне заняття 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 аудиторіїї з використанням мережевого обладнання).

Завдання 2. У даному завданні необхідно з'єднати обладнання, як показано на схемі топології (рис. 1.1) та налаштувати, використовувати адресацію з таблиці 1.1 або таблиці 1.2 для другої групи (варіант обирається згідно порядкового номеру в журналі групи, якщо груп дві, то для другої групи варіант обирається з таблиці 1.2).

Хід роботи

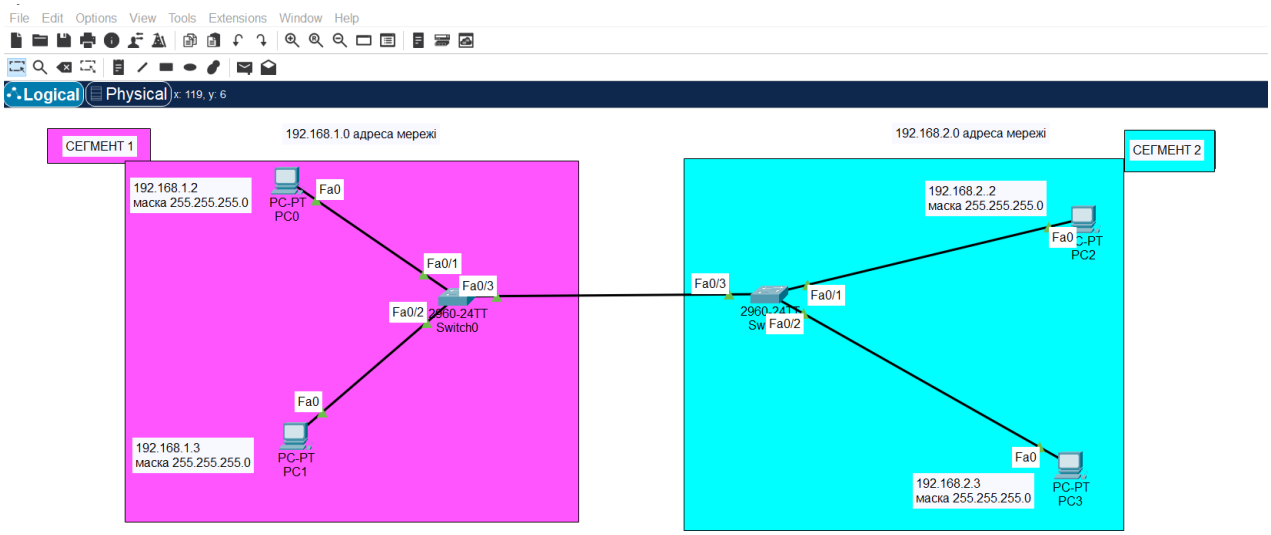


Рисунок 1.1 – Топологія мережі

Таблиця 1.1 – Варіанти завдання для першої групи

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
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

Продовження таблиці 1.1

Номер варіанту	Мережева адреса сегменту 1, маска /24	Мережева адреса сегменту 2, маска /24
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

Таблиця 1.2 – Варіанти завдання для другої групи

Номер варіанту	Мережева адреса сегменту 1, маска /24	Мережева адреса сегменту 2, маска /24
1.	192.168.67.0	192.168.68.0
2.	192.168.69.0	192.168.70.0
3.	192.168.71.0	192.168.72.0
4.	192.168.73.0	192.168.74.0
5.	192.168.75.0	192.168.76.0
6.	192.168.77.0	192.168.78.0
7.	192.168.79.0	192.168.80.0
8.	192.168.81.0	192.168.82.0
9.	192.168.83.0	192.168.84.0
10.	192.168.85.0	192.168.86.0
11.	192.168.87.0	192.168.88.0
12.	192.168.89.0	192.168.90.0
13.	192.168.91.0	192.168.92.0
14.	192.168.93.0	192.168.94.0
15.	192.168.95.0	192.168.96.0
16.	192.168.97.0	192.168.98.0
17.	192.168.99.0	192.168.100.0
18.	192.168.101.0	192.168.102.0
19.	192.168.103.0	192.168.104.0
20.	192.168.105.0	192.168.106.0
21.	192.168.107.0	192.168.108.0
22.	192.168.109.0	192.168.110.0
23.	192.168.111.0	192.168.112.0
24.	192.168.113.0	192.168.114.0
25.	192.168.115.0	192.168.116.0
26.	192.168.117.0	192.168.118.0
27.	192.168.119.0	192.168.120.0
28.	192.168.121.0	192.168.122.0

Продовження таблиці 1.2

Номер варіанту	Мережева адреса сегменту 1, маска /24	Мережева адреса сегменту 2, маска /24
29.	192.168.123.0	192.168.124.0
30.	192.168.125.0	192.168.126.0
31.	192.168.127.0	192.168.128.0
32.	192.168.129.0	192.168.130.0
33.		

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 практичних робіт в курсі [1-2].

Для позначення підмереж на схемі в Packet Tracer різними кольорами (рис. 1.2), використати піктограму  або  .

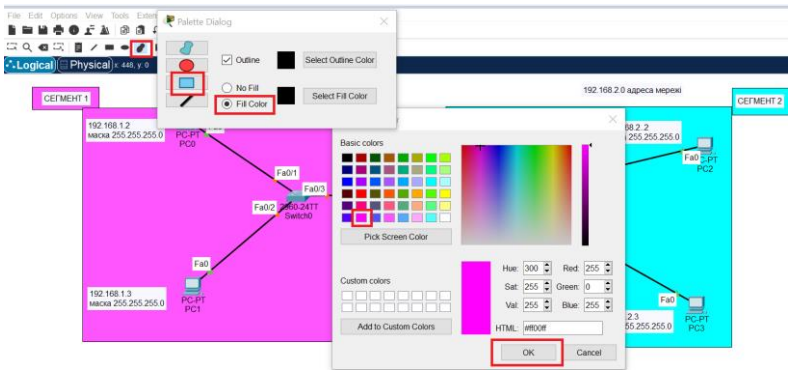


Рисунок 1.2 – Створення кольорових областей

IP-адреси на комп'ютері налаштувати статично (рис. 1.3).

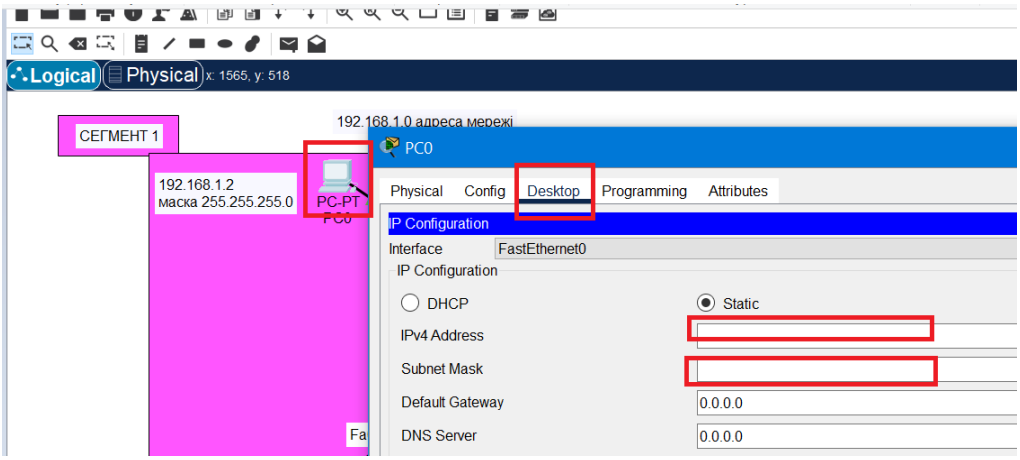


Рисунок 1.3 – Налаштування статичної IP-адреси на комп'ютері

1. Завдання виконати згідно варіанту (обрати IP-адреси підмереж згідно варіанту), поданому в таблиці 1.1. Маска підмереж 255.255.255.0 (/24). 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-0 192.168.1.2, 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;

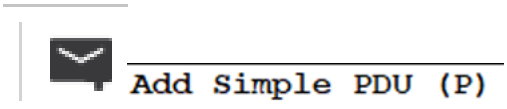
– налаштуйте IP-адресу та маску підмережі на PC-3 192.168.2.3, маска підмережі 255.255.255.0.

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. 1.4).

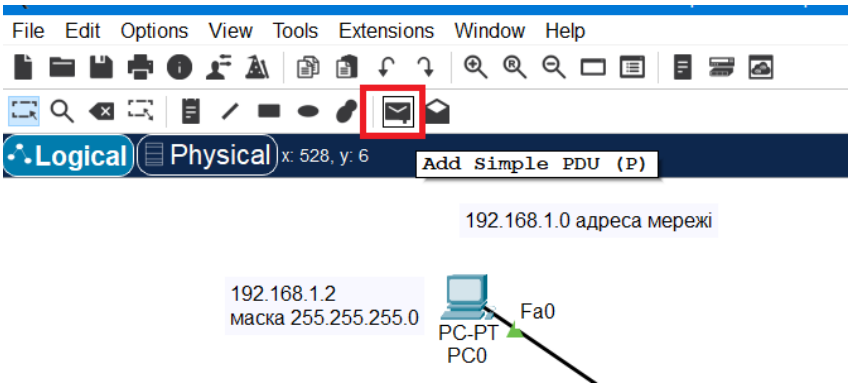


Рисунок 1.4 – Команда ping

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.

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

Практичне заняття 2
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 2.1. 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.

Хід роботи

1. Виконати адресацію мережі згідно виданого варіанту в таблиці 2.1 (варіант – порядковий номер в списку групи студентів) та внести дані в таблицю 2.2.

Варіанти завдання

Таблиця 2.1 – 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
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

Таблиця 2.2 – Адресація мережі

Вихідна маска підмережі в десятковому форматі	255.255.255.0
Вихідна маска підмережі в десятковому форматі	/24
Написати варіант згідно таблиці 2.2	Написати IP-адресу та кількість підмереж згідно завдання в таблиці 2.2
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. 2.1).

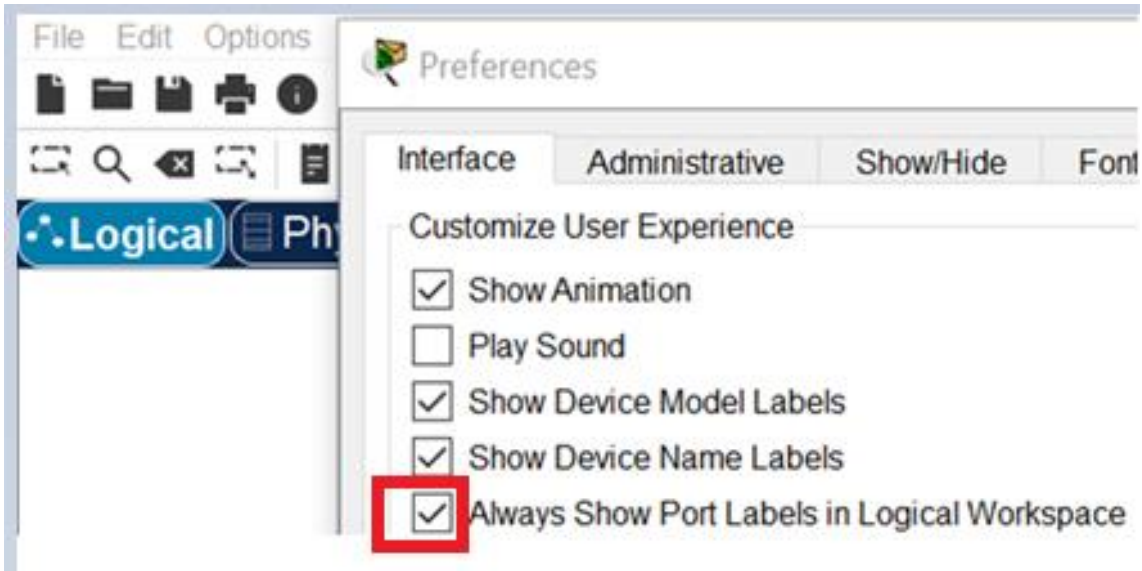


Рисунок 2.1 – Відображення назви інтерфейсів

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 2.2 та 2.3.

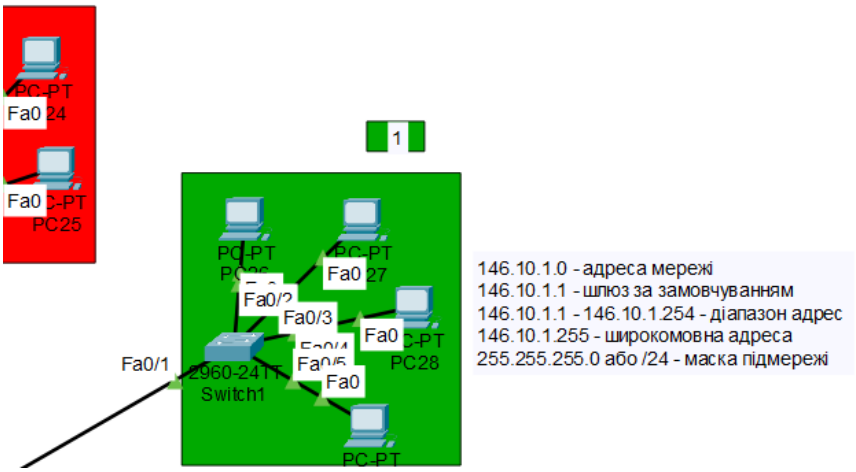


Рисунок 2.2 – Вигляд схеми підмережі в Packet Tracer (в текстовому полі зазначити адресу мережі, діапазон хостових адрес, шлюз за замовчування, широкомовну адресу та маску мережі)

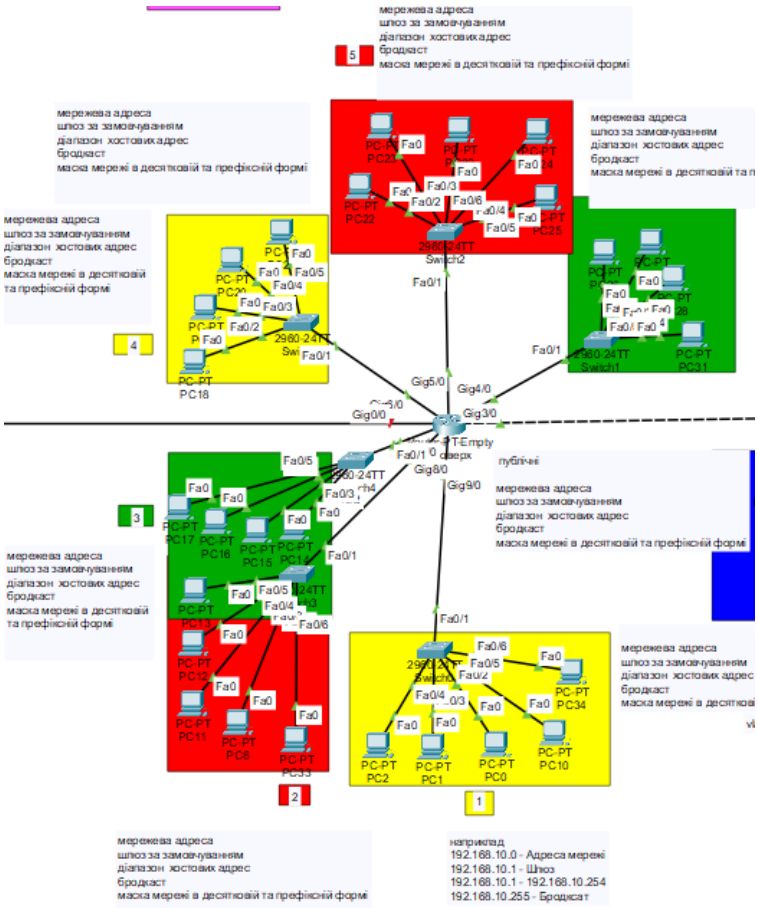


Рисунок 2.3 – Загальний вигляд схеми підмережі в Packet Tracer (в текстовому полі зазначити адресу мережі, діапазон адрес, шлюз за замовчування, широкомовну адресу та маску мережі)

4. Всі підмережі позначити на схемі в Packet Tracer різними кольорами (рисунок 2.2, 2.3, 2.4), використавши для цього піктограму (рис. 2.4) та назвати в текстовому полі (М1 – мережа 1, М2 – мережа 2 і т.д.).

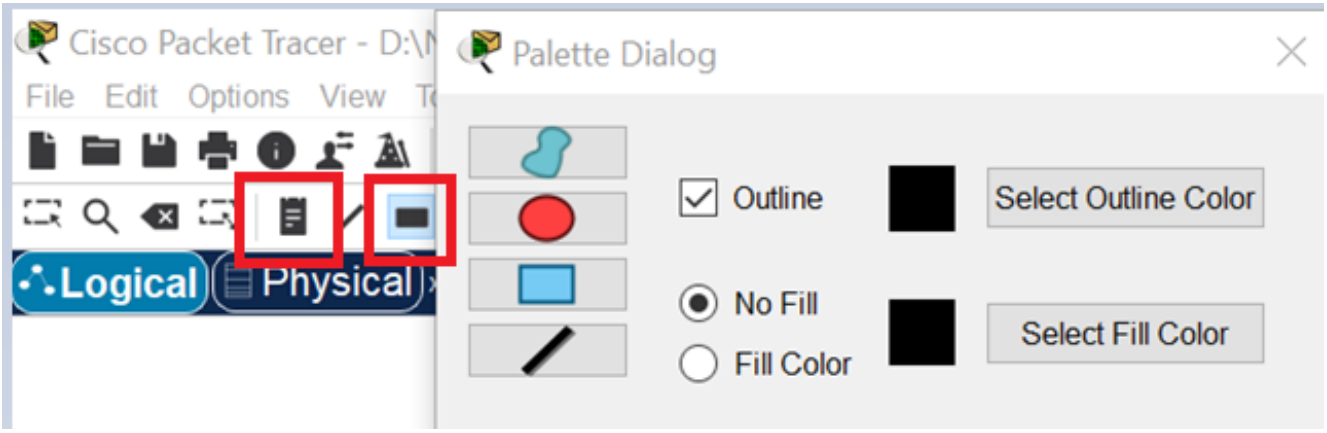


Рисунок 2.4 – Створення кольорових областей

5. Налаштувати IP-адреси на інтерфейсах маршрутизатора та ввімкнути їх (рис. 2.5). 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 2.5 – 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 практичних робіт в курсі.

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

Практична робота 3
Побудова мережі з комутатором і маршрутизатором на базі обладнання Cisco

Мета роботи: навчити студентів налаштовувати мережу на прикладі обладнання Cisco

Завдання: налаштувати топології згідно рисунка 3.1, провести адресацію пристроїв (табл. 3.1) та перевірити з'єднання [2].

Хід роботи

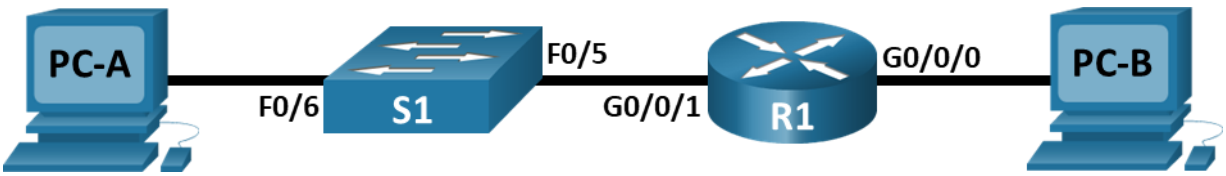


Рисунок 3.1 – Топологія мережі

Таблиця 3.1 − 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 (рис. 3.1). Потім потрібно налаштувати пристрої у відповідності до таблиці адресації (табл. 3.1). 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

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 практичної 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 потрібно використати для його активації?

Практична робота 4
Налаштування IPv6-адресації

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

Завдання: налаштувати адресацію IPv6 на маршрутизаторі, серверах, клієнтських вузлах згідно таблиці 4.1, протестувати мережу та перевірити зв'язок в мережі (рис. 4.1) [2].

Хід роботи

Таблиця 4.1 – Адресація

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

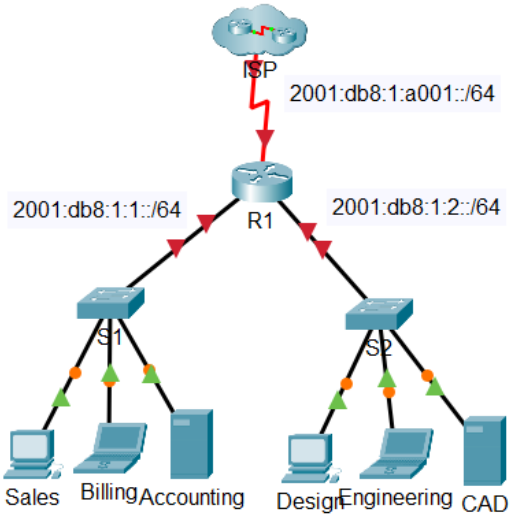


Рисунок 4.1 – Топологія мережі

1. Налаштування адресації IPv6 на маршрутизаторі [2-3]. 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.

Практичне заняття 5
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 згідно завдання в таблиці 5.1. Для сервера DHCP підібрати довільну IP-адресу з пулу приватних IPv4-адрес і щоб вона не повторювала видані для vlan. Перевірити отримання мережевих параметрів автоматично (рис. 5.1).

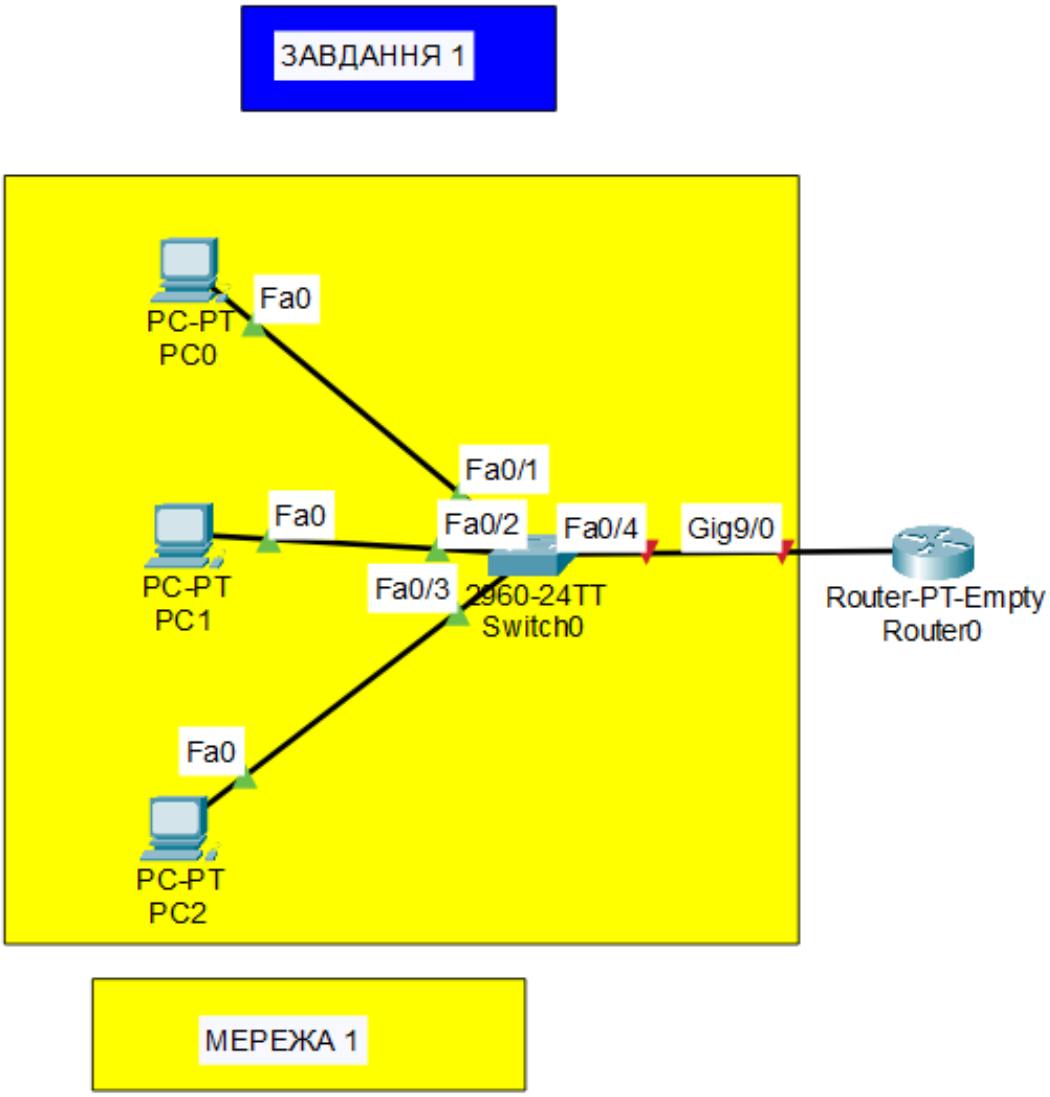


Рисунок 5.1 – Топологія мережі

Варіант роботи

Таблиця 5.1 – 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

Хід роботи

1. Опрацювати матеріа [4]. Завдання виконати згідно варіанту, поданому в таблиці 5.1. Створити схему мережі та з’єднати обладнання, як показано на схемі топології (рис. 5.1) . Комутатор, що використовуються в практичній роботі Catalyst 2960 та маршрутизатор PT-Empty (вимкнути живлення, додати до даного маршрутизатора порт PT-ROUTER-NM-1CGE, ввімкнути живлення, (рис. 5.2). Назвати маршрутизатор Вашим прізвищем.

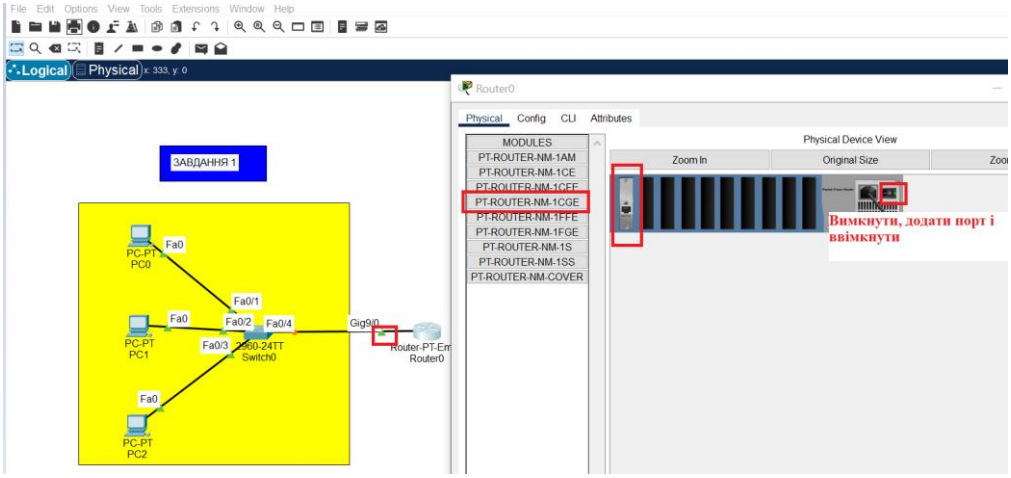


Рисунок 5.2 – Додавання порту на маршрутизаторі

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. 5.3).

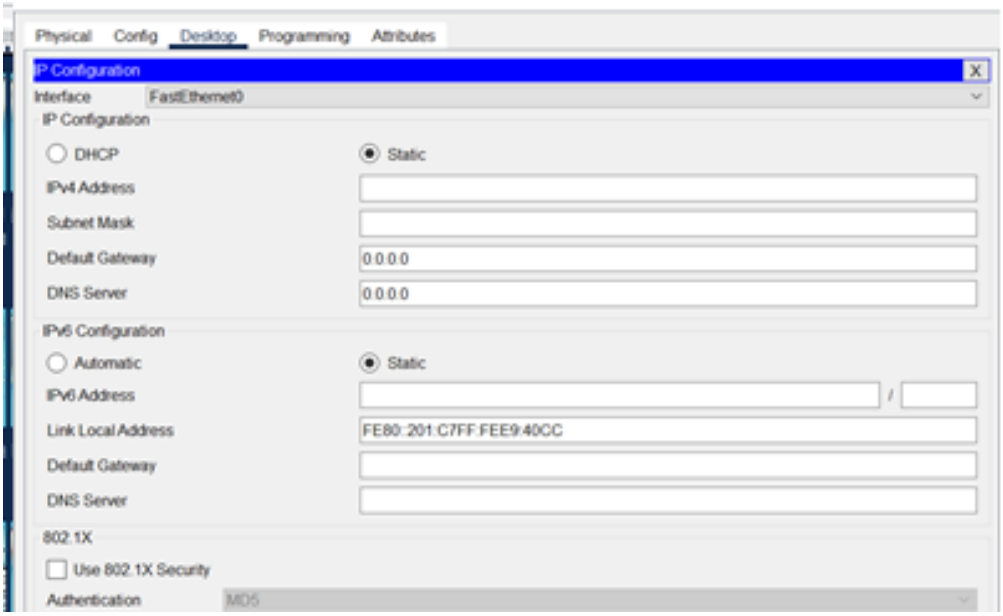


Рисунок 5.3 – Вкладку IP configuration

Як бачимо, за замовчуванням виставлено параметр Static (рис. 5.4), хоча насправді на реальних комп'ютерах завжди за замовчуванням встановлено параметер DHCP. Перемикаємо на параметр DHCP і комп'ютері повинен отримав ip-адресу з відповідного пулу.

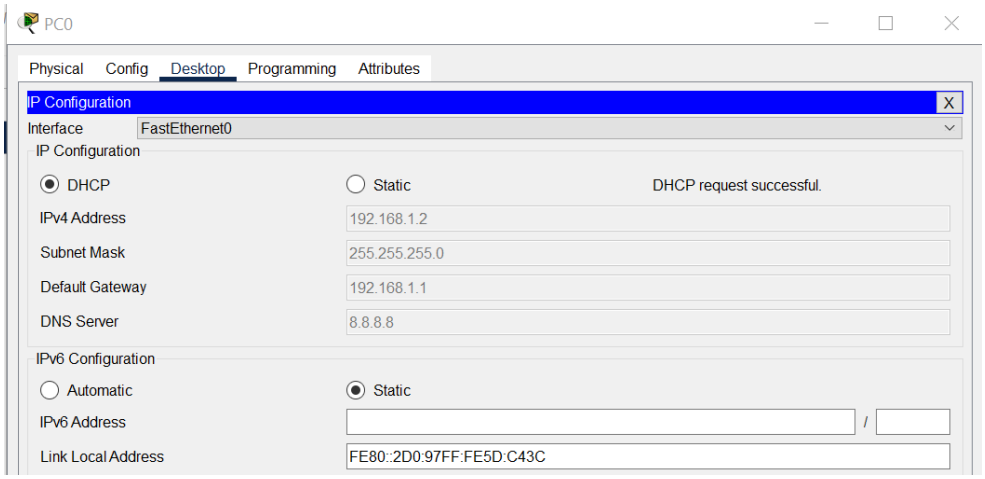


Рисунок 5.4 – Комп'ютері повинен отримав ip-адресу з відповідного пулу

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

Завдання 2. IPv4-адреси для мереж 1, 2, 3 підібрати з різних класів приватних IPv4-адрес.

У даному завданні необхідно з'єднати обладнання, як показано на схемі топології (рис. 5.5) та налаштувати пристрої у відповідності до схеми. Після збереження налаштувань, потрібно перевірити виконані конфігурації, протестувавши під'єднання до мережі. Всі мережі повинні обмінюватися між собою інформацією, роздачу IPv4-адрес для комп'ютерів налаштувати динамічно за допомого протоколу DHCP.

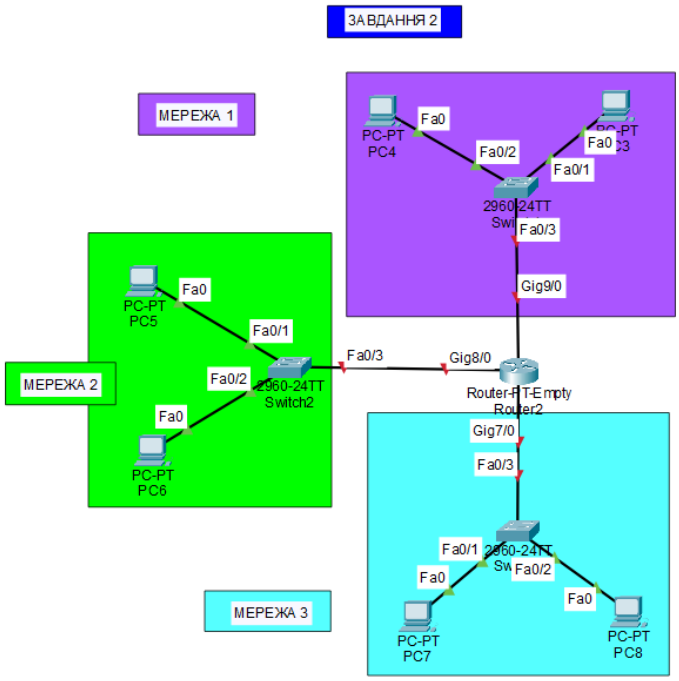


Рисунок 5.5 – Топологія мережі

Завдання 3. 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. 5.6): 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).

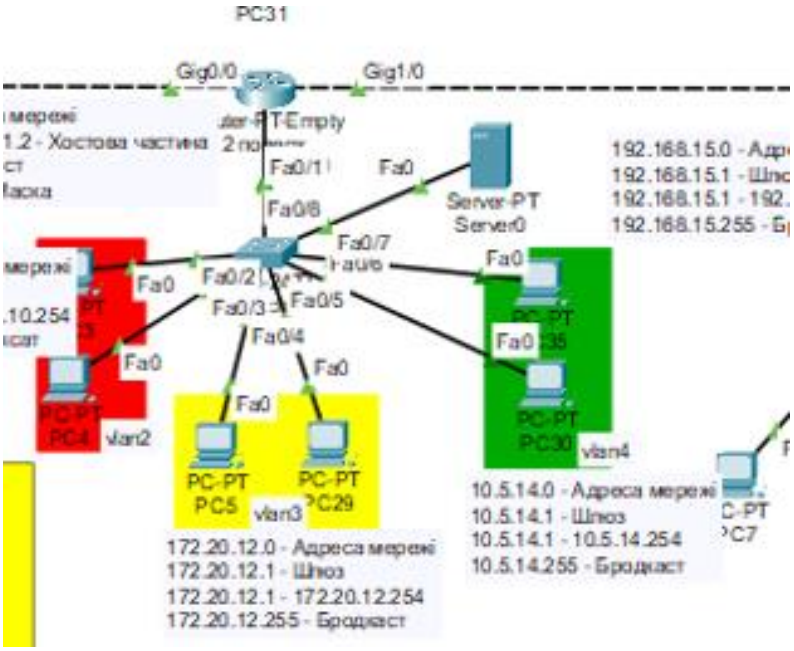


Рисунок 5.6 – Орієнтовна схема другого поверху

1. Налаштуємо комутатор, щоб сегментувати нашу мережу. Створимо vlan (табл. 5.2, рис. 5.7, 5.8).

Таблиця 5.2 – 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`

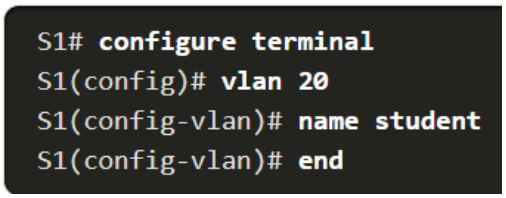


Рисунок 5.7 – Приклад створення VLAN [2]

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 [2].

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

У таблиці наведено синтаксис команд (табл. 5.3), 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 5.3 – Команди налаштування належності портів до VLAN [2]

Завдання	Команда IOS
Увійдіть до режиму глобальної конфігурації	`Switch# configure terminal`

Продовження таблиці 5.3

Завдання	Команда IOS
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].

```
S1# configure terminal
S1(config)# interface fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
```

Рисунок 5.8 – 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. 5.9-5.11) необхідно налаштувати взаємопов’язані порти за допомогою команд конфігурації інтерфейсу, перелік яких наведений у таблиці 5.4 [2].

Таблиця 5.4 – 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`

Продовження таблиці 5.4 [2]

Завдання	Команда IOS
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 5.9 – 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 5.10 – Приклад налаштування належності порту до vlan 2 та налаштування транкового каналу vlan 2-5

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 [2].

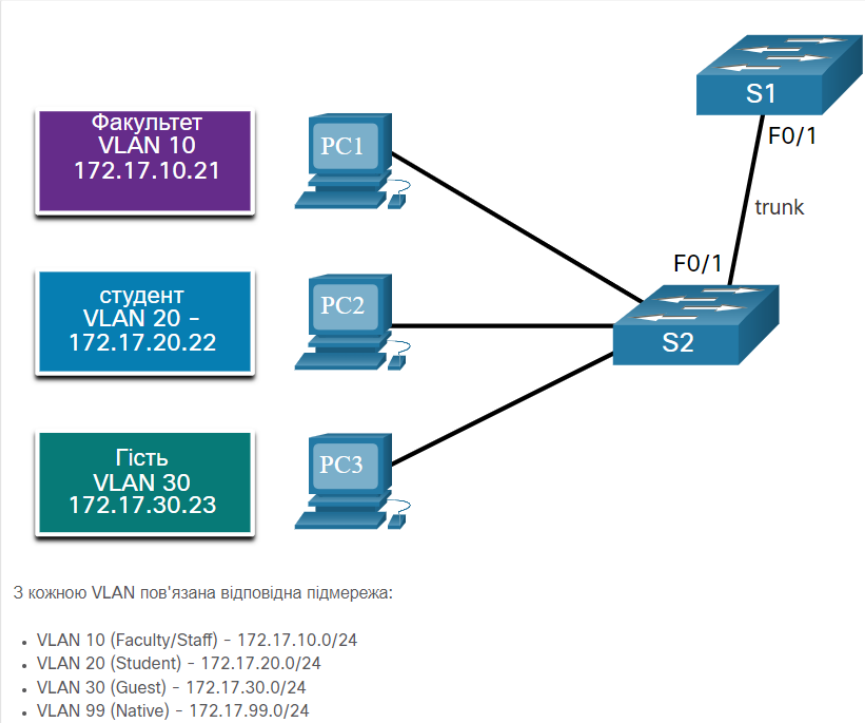


Рисунок 5.11 – Приклад схеми відображення транкового каналу [2]

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) [2].

2. На маршрутизаторі налаштуємо саб-інтерфейси (саб-інтерфейси дозволяють розділити один фізичний інтерфейс на декілька віртуальних інтерфейсів, кожний зі своєю конфігурацією) (рис. 5.12).

```
!
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 5.12 – 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 5.13), маску та шлюз за замовчуванням (перша адреса в діапазоні адрес, рисунок 5.13).

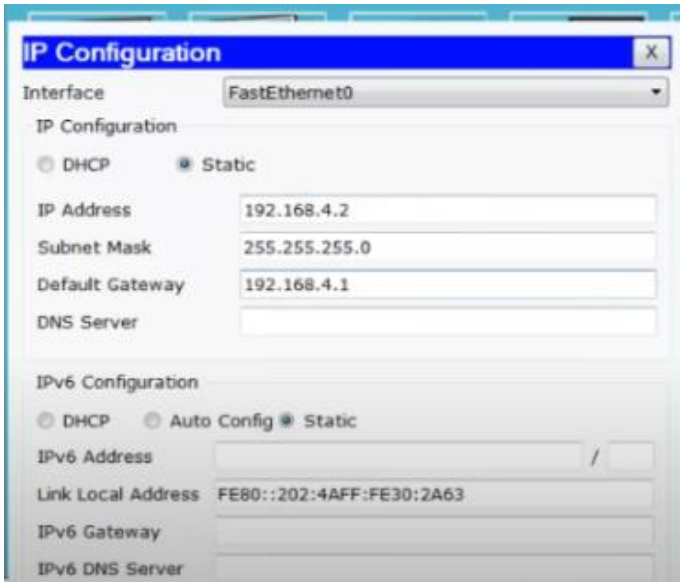


Рисунок 5.13 – Налаштування адресації на сервері

3. Перейти на сервері у вкладку налаштування DHCP (рис. 5.14).

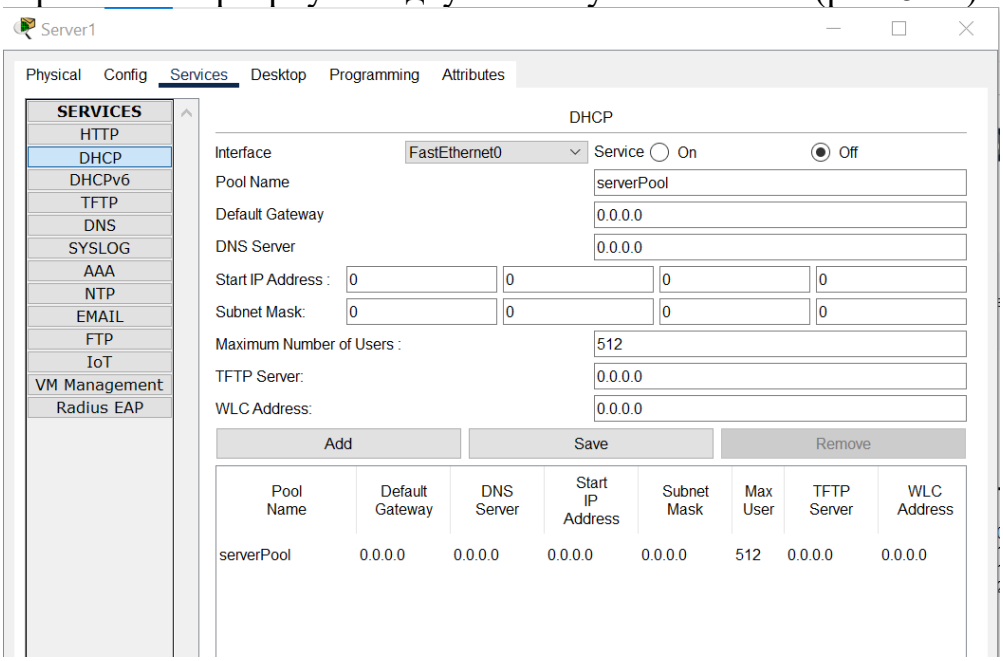


Рисунок 15.4 – Вкладка налаштування DHCP

На початку є створений один дефолтний сервер-пул. Цей пул залишається і далі створити нові, тобто, VLAN2, VLAN3, VLAN4 (рис. 5.15) та

кнопкою Add їх додаємо (адресація обираєть студентом самостійно з приватного пулу IPv4 адрес, див. вище).

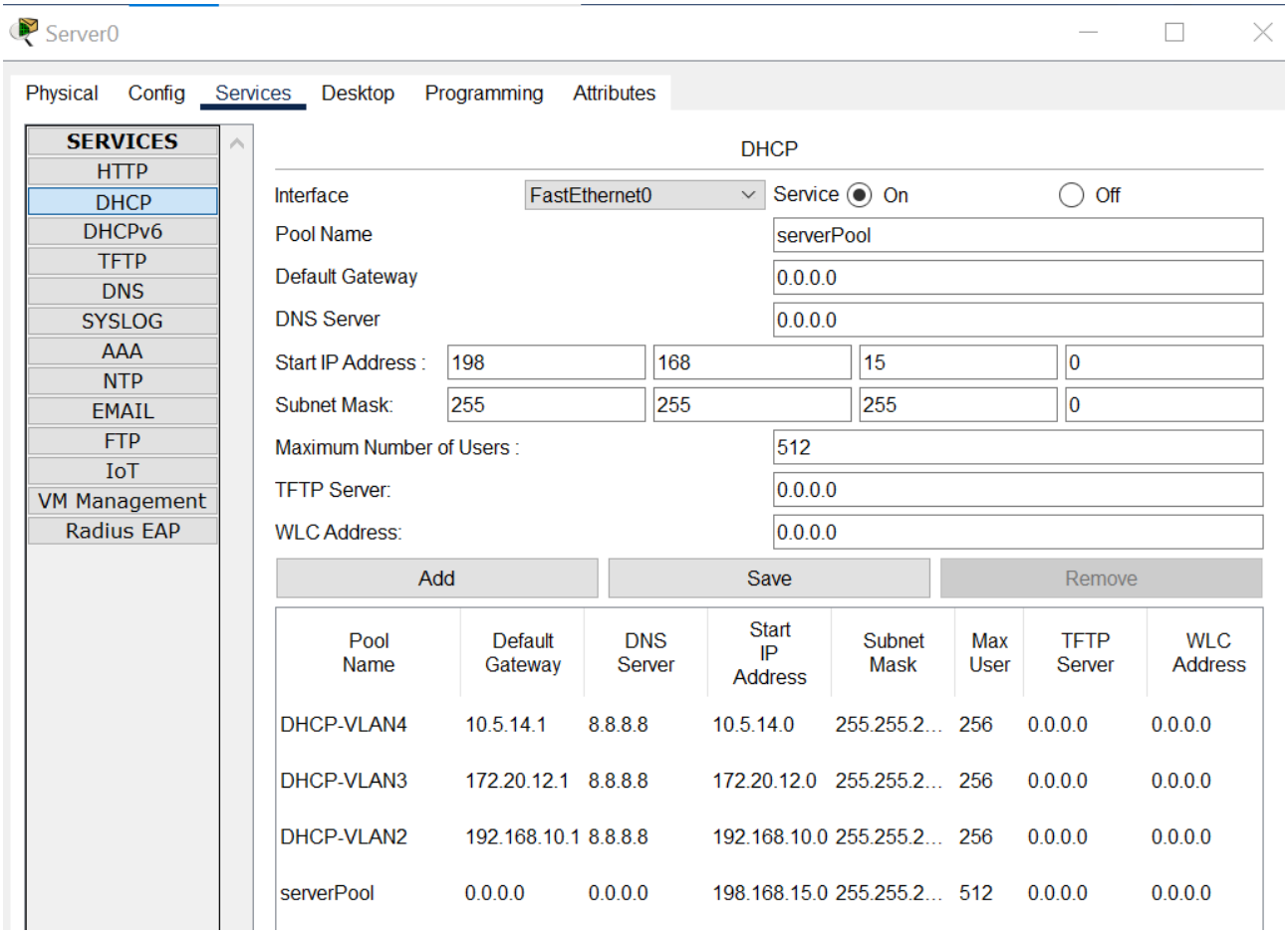


Рисунок 5.15 – Вкладка налаштування DHCP

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 5.12).

Практичне заняття 6
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. Завдання виконати згідно варіанту в таблиці 6.1.

Хід роботи

І. Налаштування маршрутизатора:

Завдання1:

Таблиця 6.1 – 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

1. Опрацювати матеріал [7, 8]; з’єднати обладнання, як показано на схемі топології (рис. 6.1);

Топологія

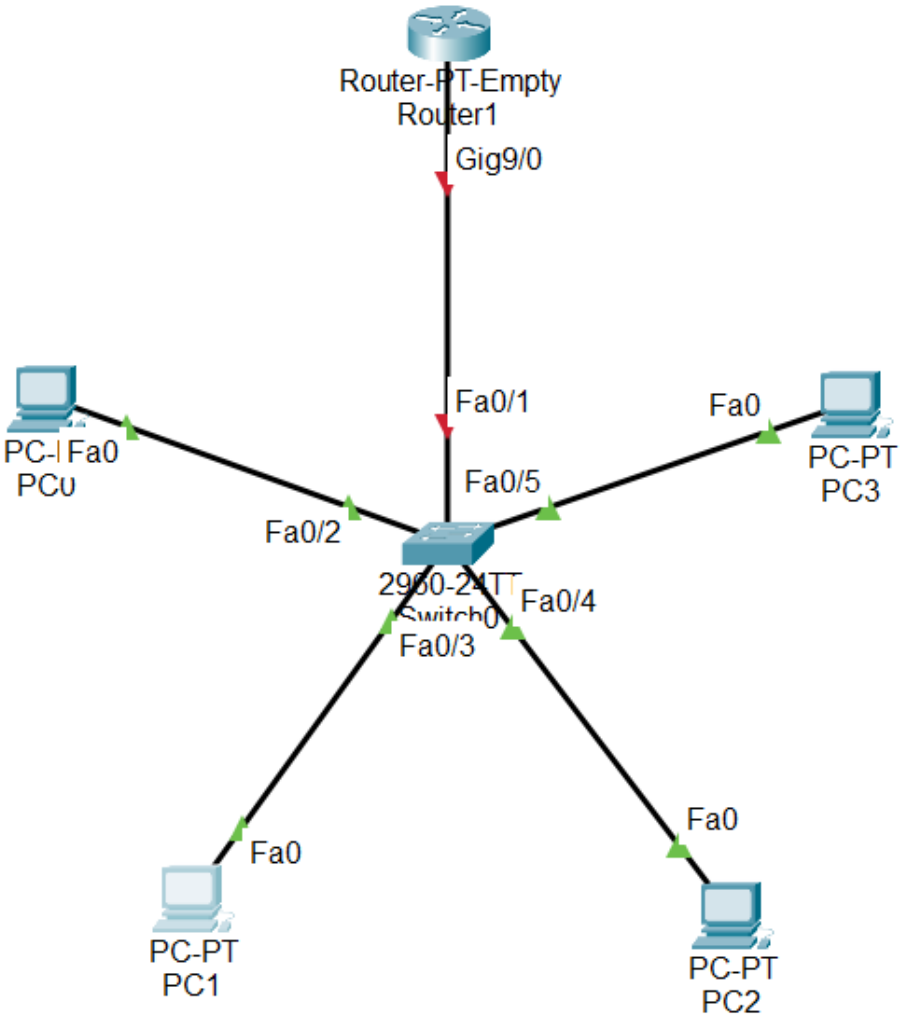


Рисунок 6.1 – Топологія мережі

2. комп’ютерам задати IP-адреси статично, адресу мережі обрати згідно варіанту в таблиці 6.1, 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 6.1. 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 AdminПрізвищеСтудента;
   Karpenko(config)#ip domain-name AdminKarpenko
7. створити логін і пароль, які будемо використовувати для авторизації на маршрутизаторі (в даній практичній 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 практичній 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. 6.2);

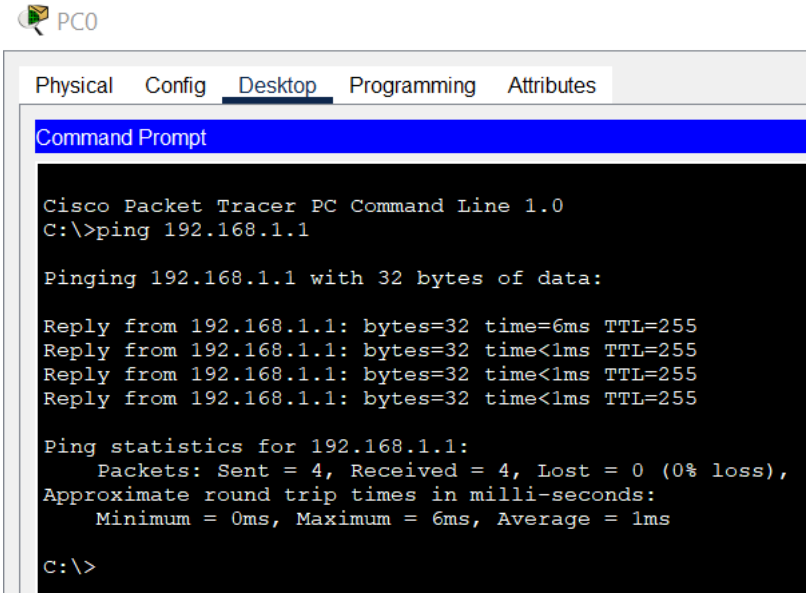


Рисунок 6.2 – Перевірка досяжності маршрутизатора з PC0

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. 6.3-6.4) та переглянути налаштування з використанням команди show startup-config (рис. 6.5), ввести пароль 123 для входу по ssh на маршрутизатор та пароль 123456 для входу в превілейований режим;

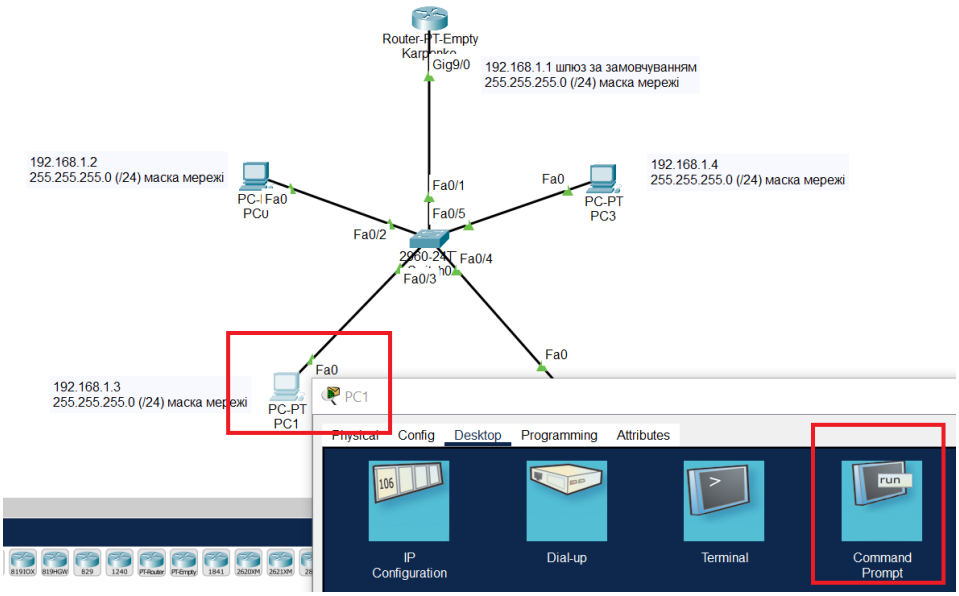


Рисунок 6.3 – Перевірка досяжності маршрутизатора з PC0

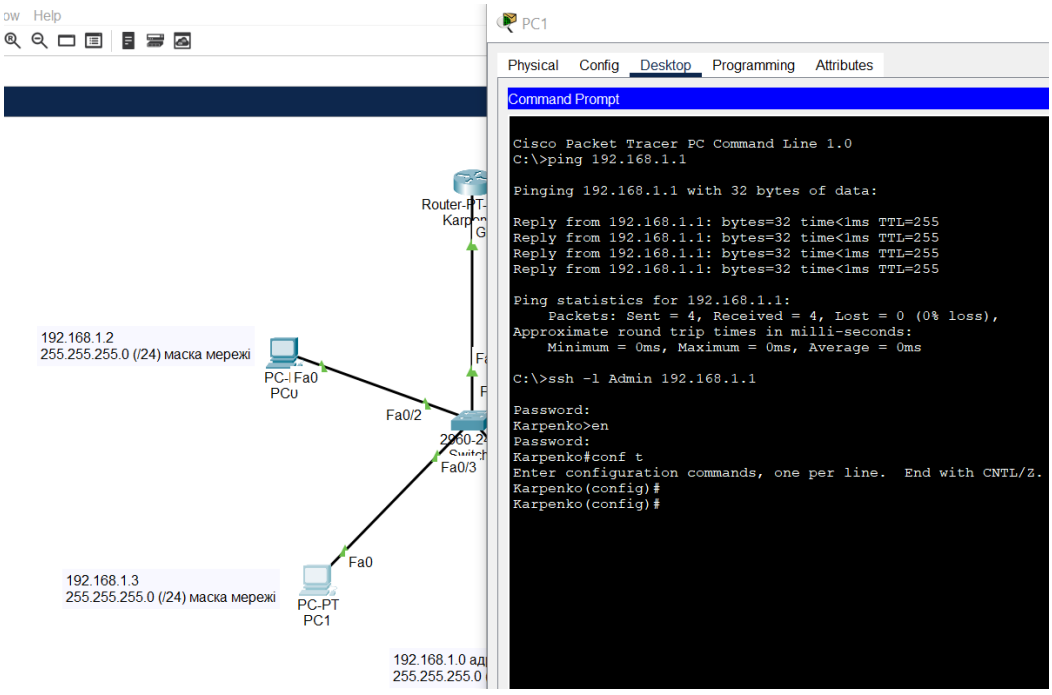


Рисунок 6.4 – Вхід на маршрутизатор з використанням команди ssh

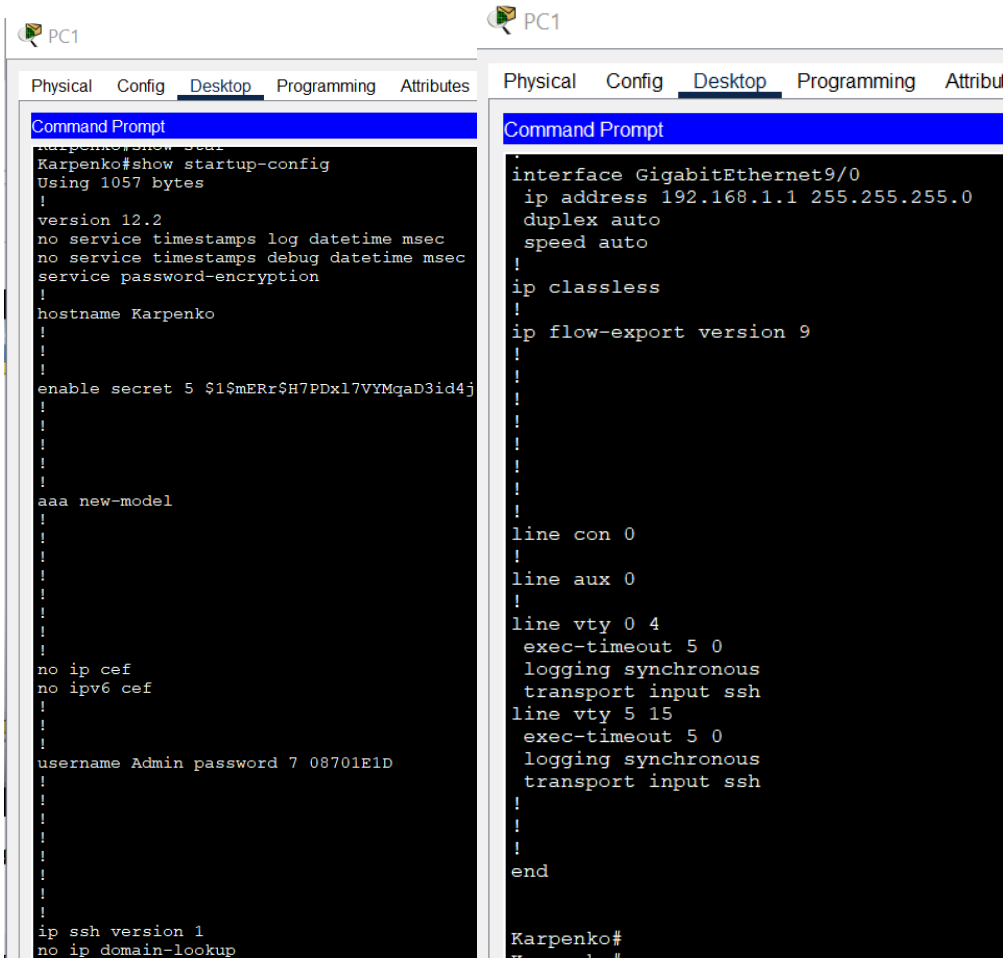


Рисунок 6.5 – Перегляд налаштувань

Завдання 2.

1. З’єднати маршрутизатор та будь який комп’ютер консольним кабелем (рис. 6.6);

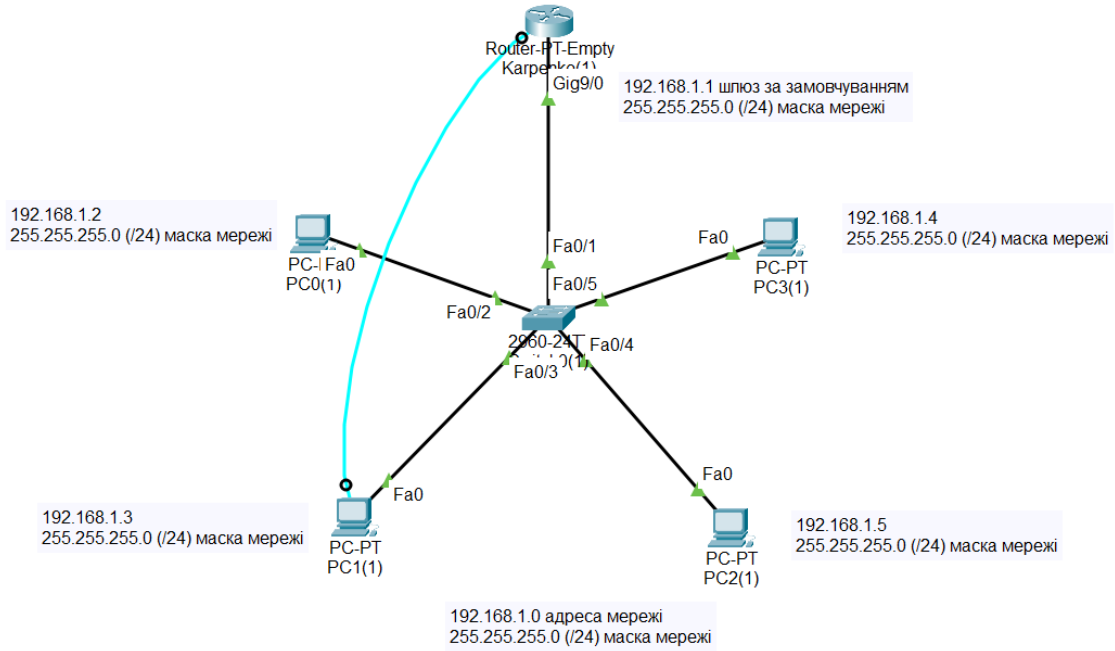


Рисунок 6.6 – Топологія мережі з консольним з’єднанням

2. ввійти в режим симуляції терміналу (рис. 6.7);

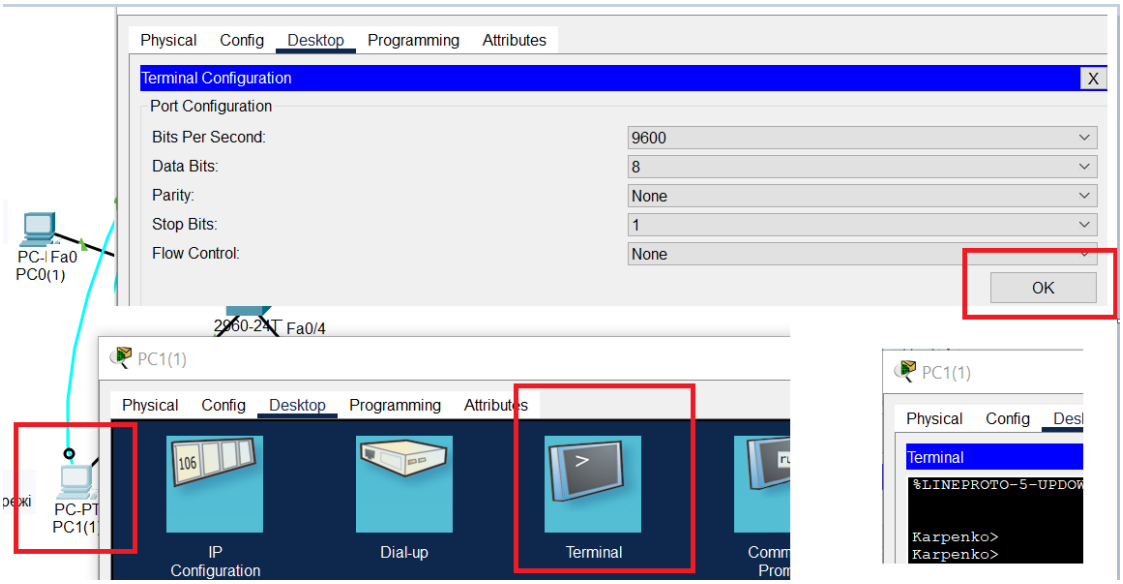


Рисунок 6.7 – Режим симуляції терміналу

3. захистити паролем вхід на пристрій по консолі (так як ввімкнено ааа, 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. 6.8).

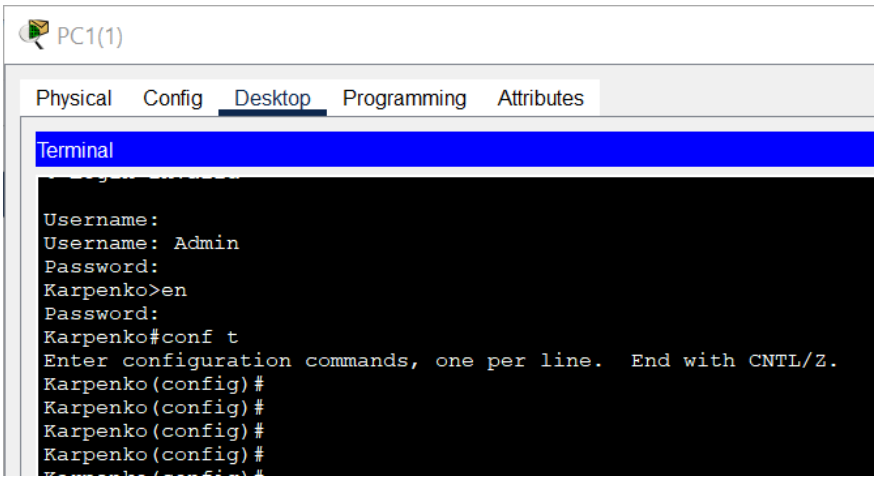


Рисунок 6.8 – Перевірка налаштувань пристрою

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. 6.9);

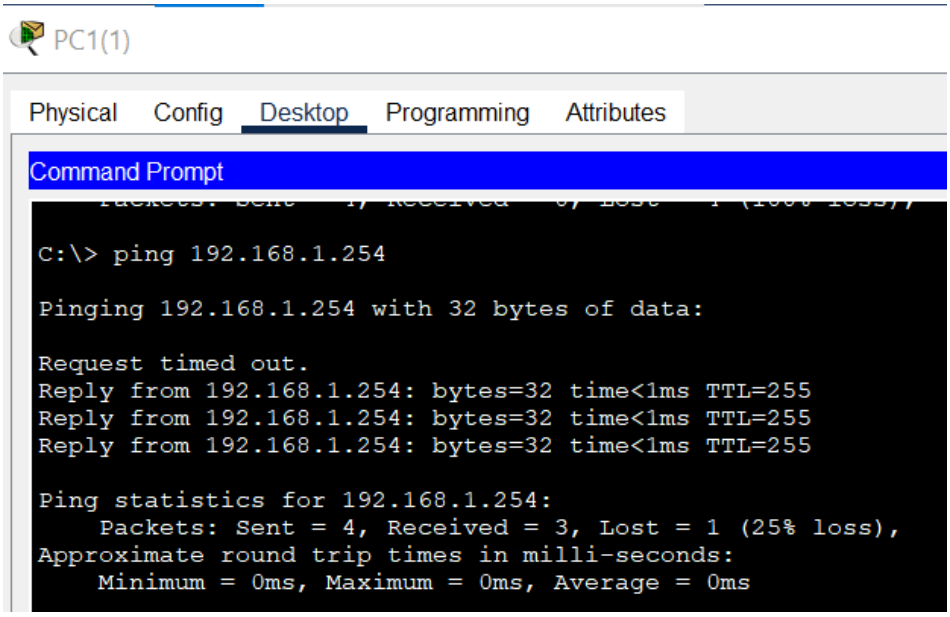


Рисунок 6.9 – Перевірка з’єднання між комп’ютерами та vlan 1

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. 6.10):

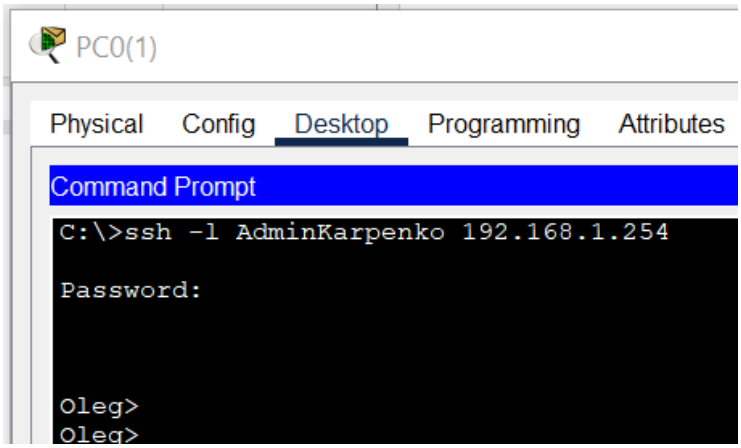


Рисунок 6.10 – Перевірка підключення до комутатора за допомогою ssh

Практичне заняття 7
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. 7.1, табл. 7.1).

Хід роботи

Опрацюйте матеріал [9, 10, 11]. 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. 7.1, табл. 7.1).

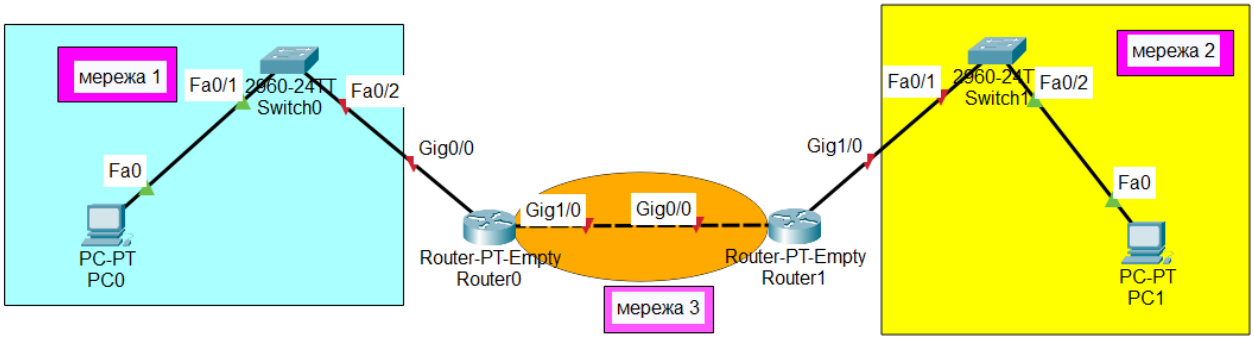


Рисунок 7.1 – Топологія мережі

Налаштувати функціонування протоколу маршрутизації OSPF згідно варіанту, наведеному в таблиці 7.1.

Таблиця 7.1 – Варіант завдання

№	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

Продовження таблиця 7.1

№	Мережева адреса мережі 1, маска /24	Мережева адреса мережі 2, маска /24	Мережева адреса мережі 3, маска /30
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

…

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.

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. 7.2).

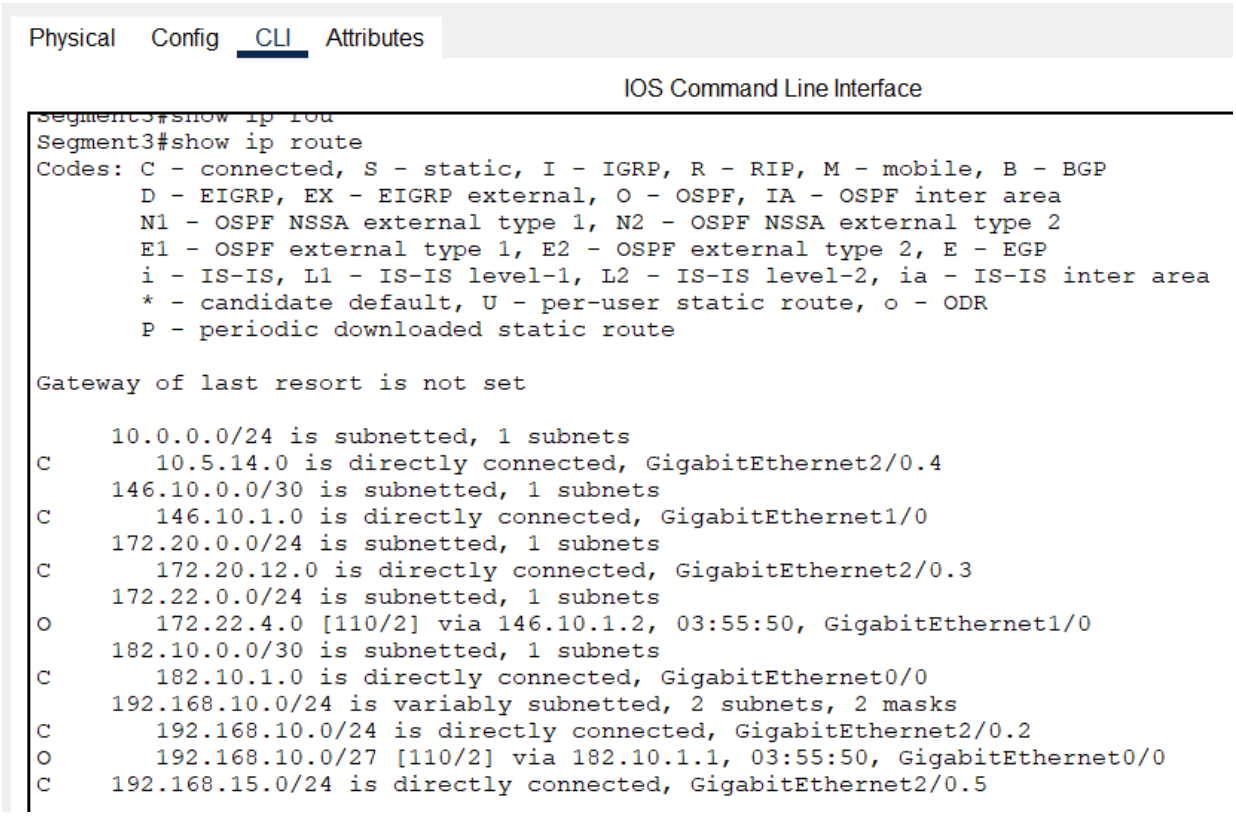


Рисунок 7.2 – Таблиця маршрутизації

В звіті до роботи вивести результат виконання команди на кожному маршрутизаторі, як показвно на рисунку 7.2.

Практичне заняття 8
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. 8.1) [2] використовуючи для адресації таблицю 8.1 [2].

Хід роботи

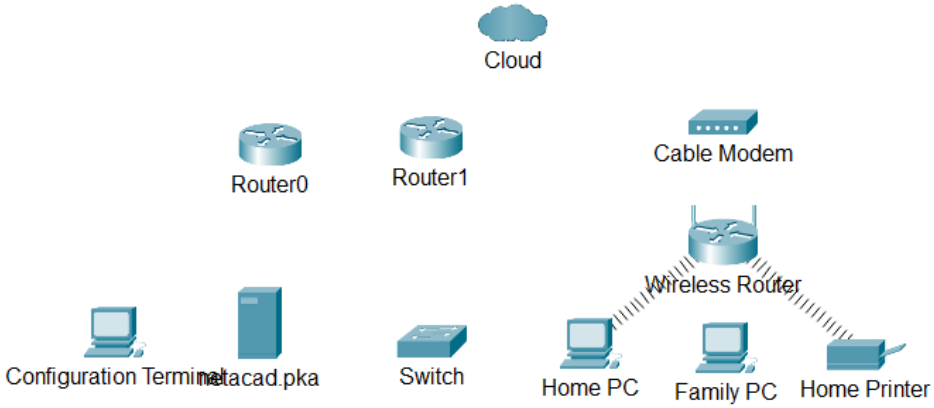


Рисунок 8.1 – Топологія мережі

Таблиця 8.1 – 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.

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.

Практичне заняття 9
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). Завдання виконати за описаним прикладом згідно варіанту, поданому в таблиці 9.1. Варіант завдання обирається згідно порядкового номеру в списку журналу групи.

Хід роботи

Таблиця 9.1 – Варіанти завдань

Порядковий номер в списку групи	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
1.	10.196.178.0	10.118.210.0	10.38.26.0	10.121.116.0	23.86.76.0	120.2.133.0
2.	172.26.242.0	192.168.69.0	10.157.113.0	172.17.227.0	100.185.112.0	187.132.140.0
3.	10.219.183.0	192.168.143.0	172.21.79.0	192.168.240.0	47.142.203.0	143.163.191.0
4.	10.178.230.0	10.59.73.0	10.39.10.0	192.168.224.0	43.190.249.0	41.250.34.0
5.	172.19.115.0	192.168.16.0	172.21.114.0	172.21.99.0	194.150.33.0	185.51.18.0
6.	10.117.69.0	10.39.166.0	172.19.197.0	172.16.60.0	4.92.197.0	209.187.156.0
7.	10.52.61.0	10.94.8.0	10.37.225.0	172.24.91.0	184.196.10.0	113.41.188.0
8.	192.168.174.0	192.168.117.0	172.19.167.0	172.26.189.0	182.45.44.0	54.24.104.0
9.	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.	10.173.120.0	172.29.162.0	10.246.110.0	172.23.252.0	83.176.51.0	163.161.223.0
11.	10.89.12.0	10.34.114.0	10.191.203.0	10.24.164.0	131.149.23.0	128.121.2.0
12.	10.135.24.0	192.168.108.0	172.31.99.0	10.212.54.0	84.173.40.0	166.186.13.0
13.	10.224.89.0	10.60.161.0	10.55.171.0	192.168.247.0	85.215.43.0	128.164.187.0
14.	10.87.84.0	10.235.178.0	10.145.104.0	192.168.235.0	119.174.77.0	138.204.152.0
15.	192.168.97.0	172.19.158.0	172.18.103.0	192.168.9.0	78.205.106.0	151.151.107.0
16.	192.168.197.0	10.93.24.0	192.168.124.0	172.26.177.0	90.170.23.0	198.83.86.0
17.	172.29.186.0	192.168.88.0	172.23.61.0	10.135.11.0	108.20.22.0	3.142.121.0
18.	192.168.24.0	192.168.62.0	10.2.210.0	192.168.135.0	26.35.194.0	31.217.156.0
19.	192.168.94.0	192.168.127.0	172.21.10.0	10.84.116.0	29.94.160.0	69.61.11.0
20.	192.168.142.0	192.168.241.0	10.207.155.0	172.29.201.0	77.23.87.0	45.121.228.0
21.	172.20.37.0	192.168.54.0	10.52.114.0	172.17.139.0	109.122.107.0	157.188.209.0
22.	172.25.38.0	172.24.83.0	192.168.163.0	192.168.51.0	186.121.73.0	57.53.42.0

Продовження таблиці 9.1

Порядковий номер в списку групи	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
23.	192.168.223.0	172.23.223.0	172.28.175.0	192.168.191.0	107.35.148.0	64.196.8.0
24.	10.108.53.0	192.168.220.0	172.18.194.0	192.168.34.0	62.132.246.0	158.234.64.0
25.	192.168.208.0	10.95.211.0	172.29.13.0	10.237.217.0	118.241.176.0	128.89.191.0
26.	192.168.52.0	10.151.198.0	10.24.177.0	172.29.86.0	215.49.224.0	113.23.168.0
27.	192.168.137.0	172.23.182.0	10.234.165.0	10.115.158.0	221.80.91.0	176.242.49.0
28.	192.168.70.0	172.18.234.0	172.27.33.0	192.168.227.0	14.145.242.0	67.214.22.0
29.	192.168.199.0	172.20.194.0	192.168.53.0	172.23.247.0	104.160.55.0	168.253.16.0
30.	192.168.56.0	192.168.123.0	10.245.12.0	172.26.69.0	137.118.255.0	180.129.106.0
31.	10.184.154.0	172.19.78.0	10.227.186.0	172.22.102.0	171.230.124.0	16.209.180.0
32.	192.168.120.0	172.26.162.0	10.209.155.0	192.168.148.0	186.134.61.0	185.32.74.0

Опрацюйте матеріал [12-15].

Виконати налаштування топології згідно варіанту, поданому в таблиці 9.1.

Створити мережу, топологія якої зображена на рисунку 9.1.

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.

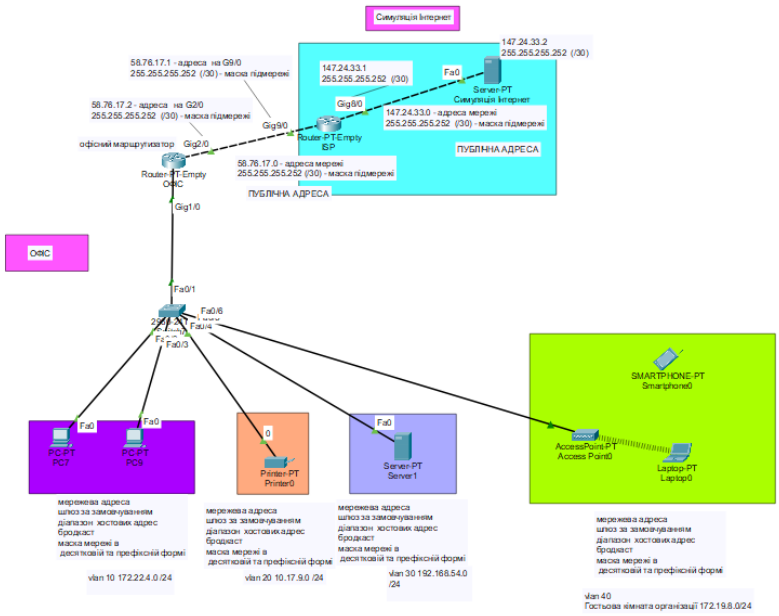


Рисунок 9.1 – Приклад топології Офісу

Створимо гостьову кімнату у вже існуючій мережі організації з використанням точок доступу. Для цього перейдіть у вкладку Wirelless Devices та розмістіть точку доступу (рис. 9.2). Далі потрібно з'єднати точку доступу з комутатором.

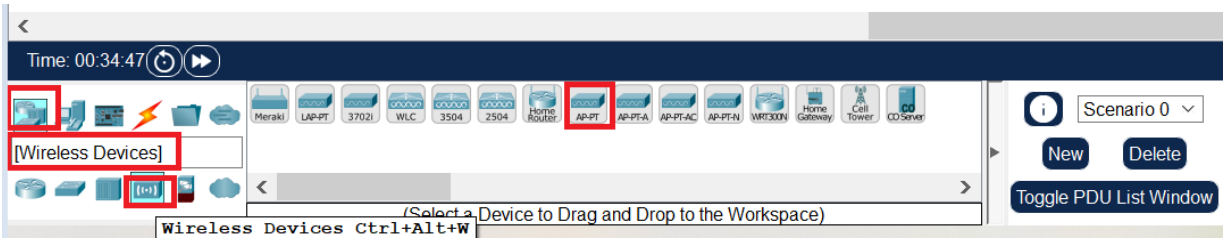


Рисунок 9.2 – Приклад додавання точки доступу

Встановити гігабітний порт на точці доступу (рис. 9.3)

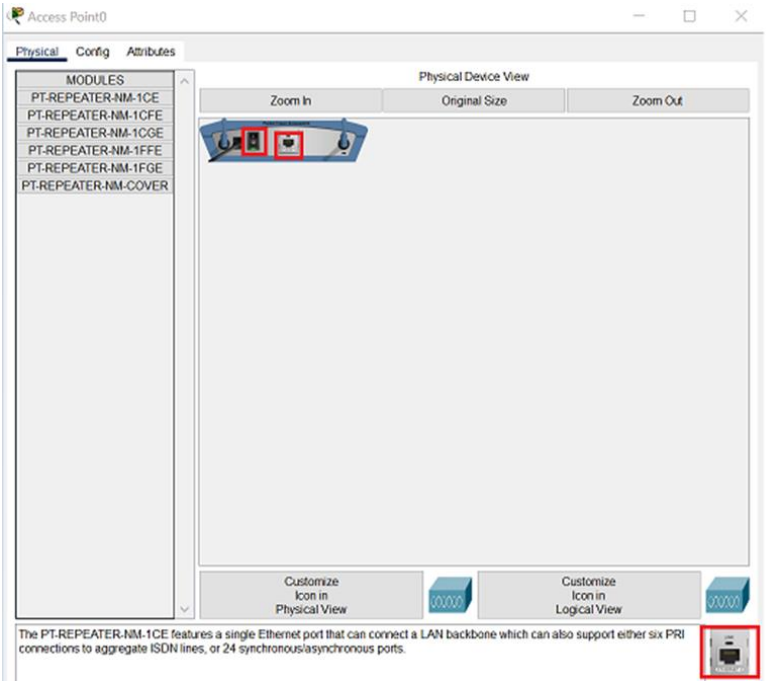


Рисунок 9.3 – Приклад встановлення гігабітного порту на точці доступу

Налаштувати точку доступу (рис. 9.4): ім'я мережі – VLAN40, шифрування – WPA2-PSK, PSK Pass Phrase – network123.

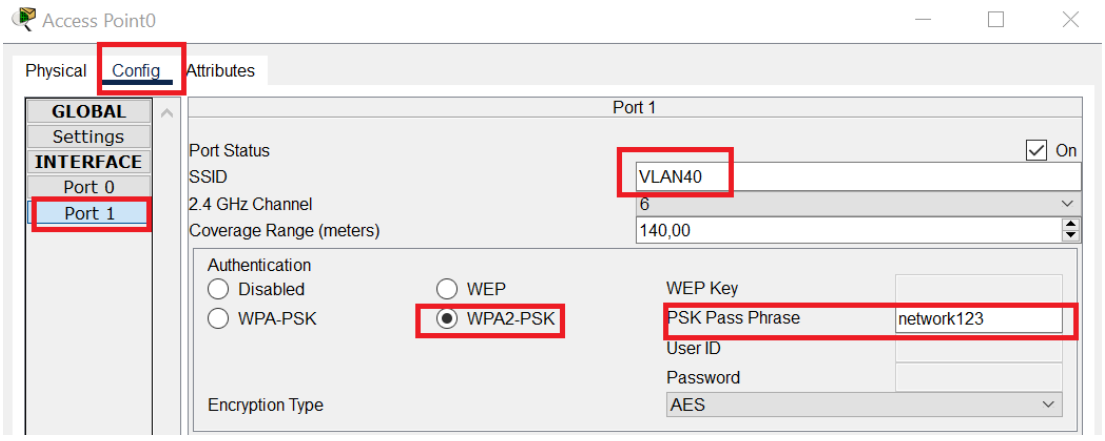


Рисунок 9.4 – Налаштування точки доступу

Налаштувати ноутбук (рис. 9.5): вимкнути ноутбук, замінити модуль Ehternet на модуль радіоканалу, включити ноутбук, зробити підключення до існуючої мережі.

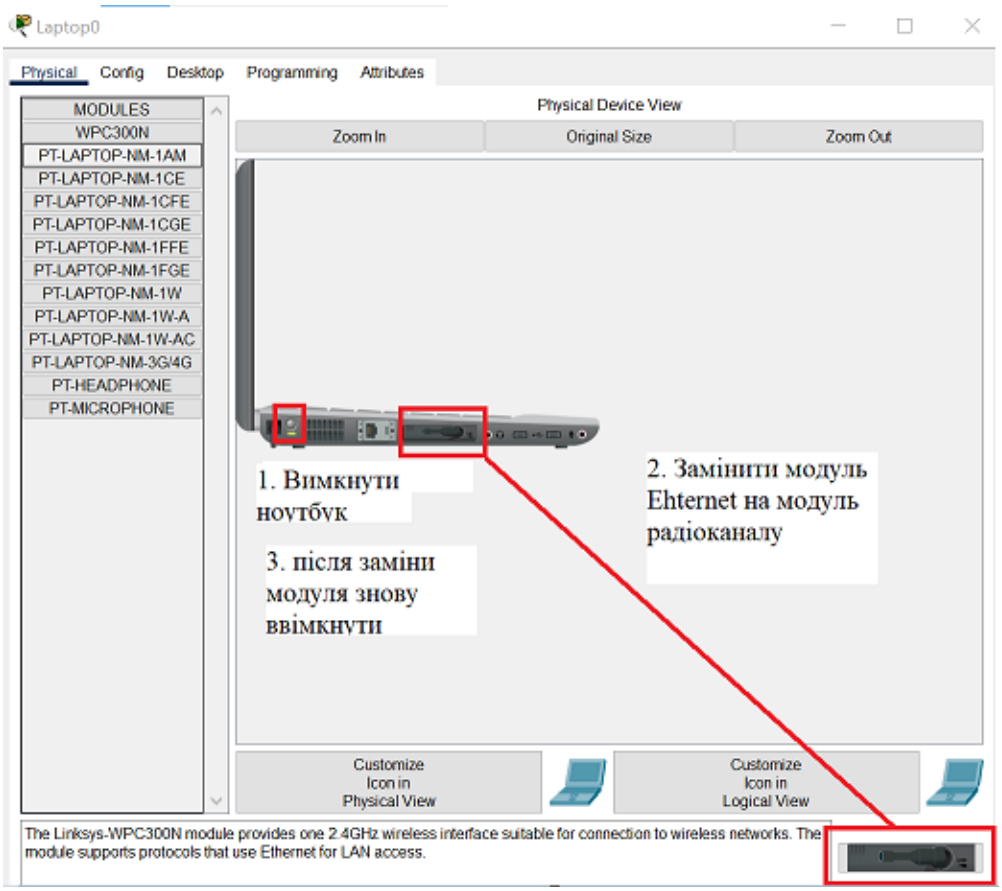


Рисунок 9.5 – Налаштування ноутбука

Під’єднаємо до існуючої мережі (рис. 9.6-9.8)

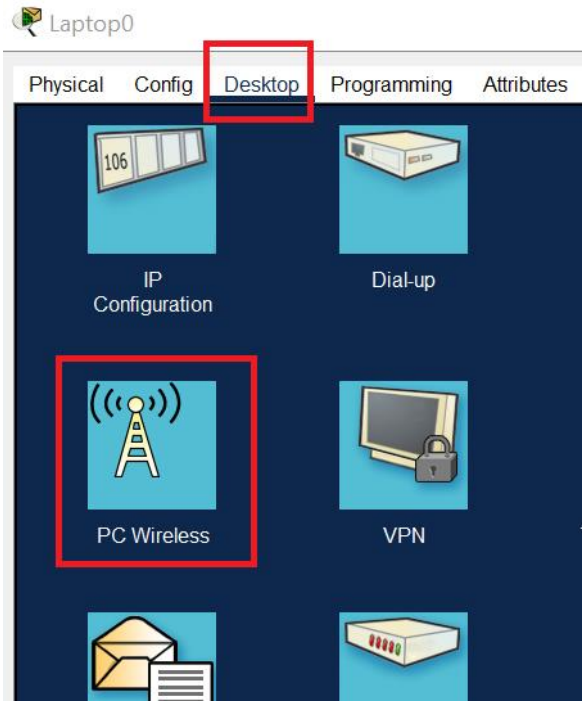


Рисунок 9.6 – Під’єднання до існуючої мережі

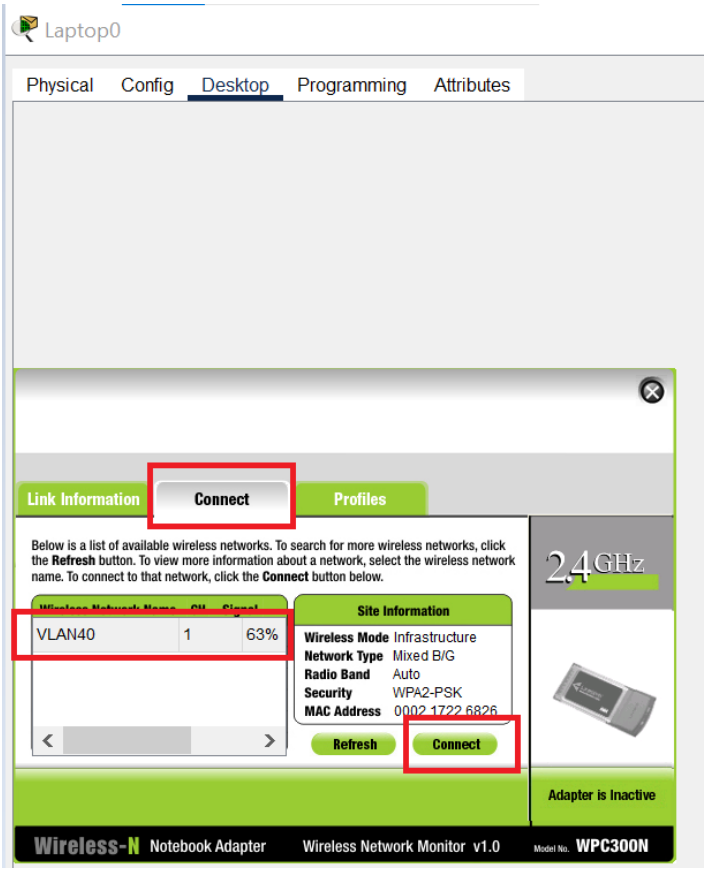


Рисунок 9.7 – Під’єднання до існуючої мережі

Вводимо ключове слово network123.

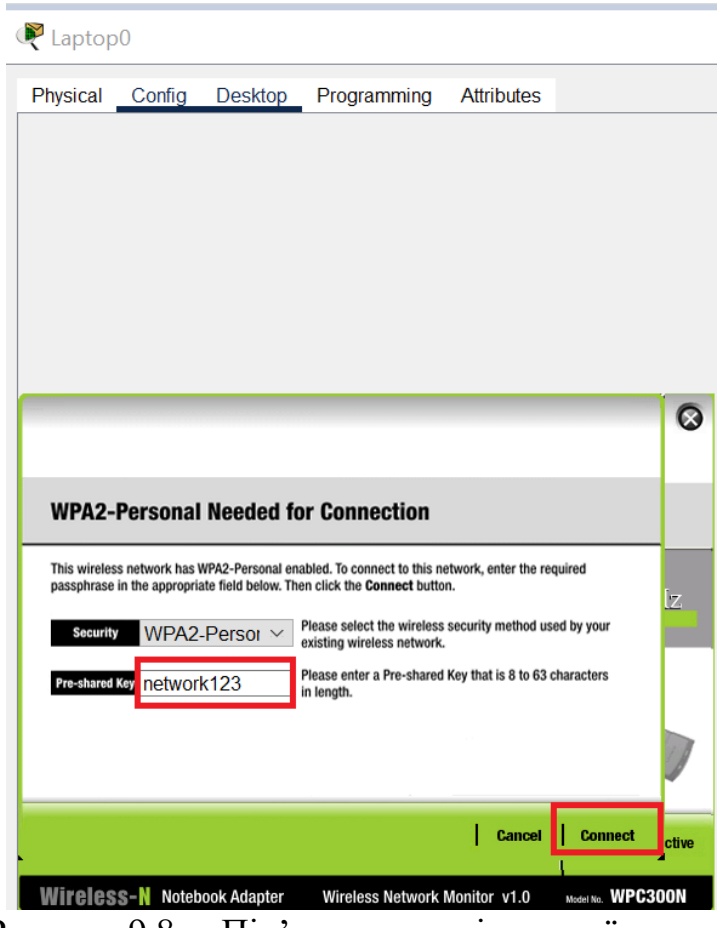


Рисунок 9.8 – Під’єднання до існуючої мережі

Як бачимо на схемі, підключення успішне (рис. 9.9).

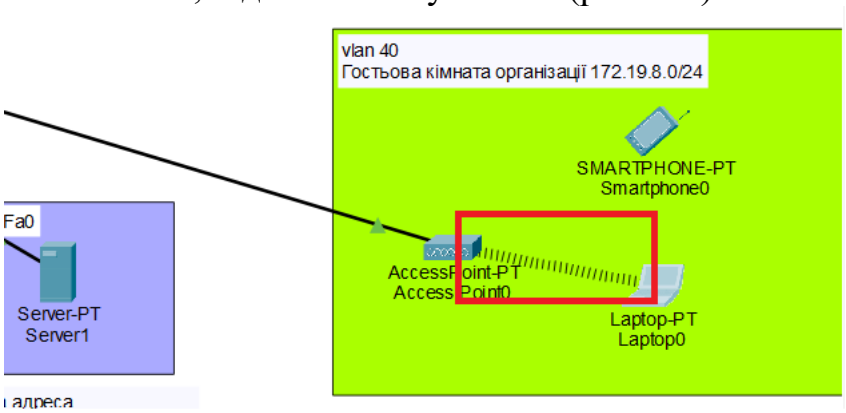


Рисунок 9.9 – З'єднання між ноутбуком та віддаленим сервером

Після налаштування точки доступу та ноутбука, з'єднання між ноутбуком та віддаленим сервером має бути успішним (рис. 9.9-9.10). Дане з'єднання буде успішним після того, коли буде налаштовано NAT (описано нижче по тексту)

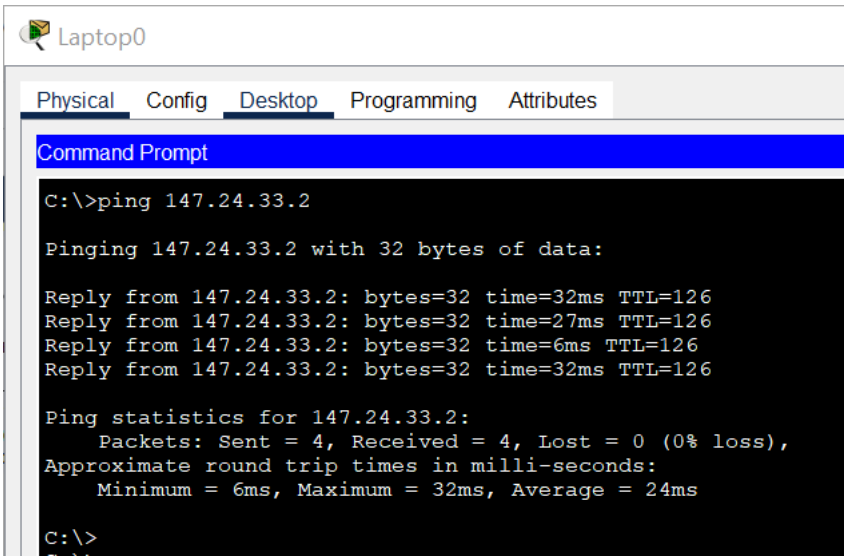


Рисунок 9.10 – З'єднання між ноутбуком та віддаленим сервером

Далі налаштувати на маршрутизаторі протокол DHCP (вивчено в попередніх практичних 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. 9.11) провайдер присвоїв IP-адресу 58.76.17.1, маска підмережі 255.255.255.252 (/30).

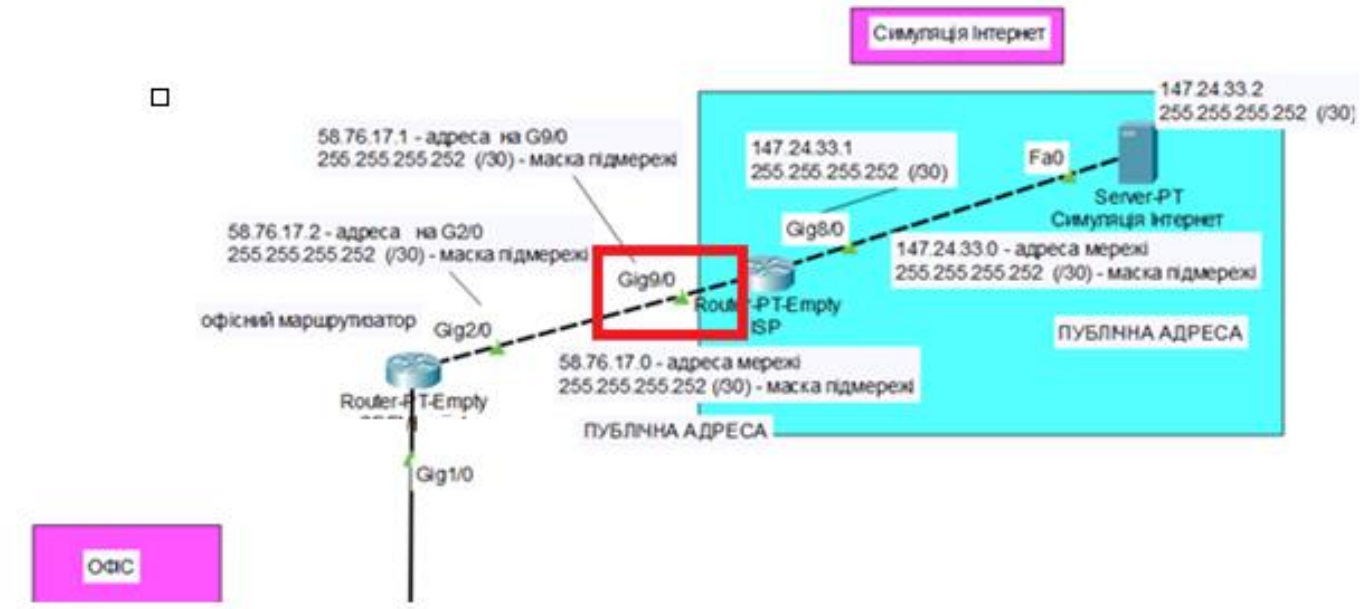


Рисунок 9.11 – Налаштування інтерфейсу G9/0

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).

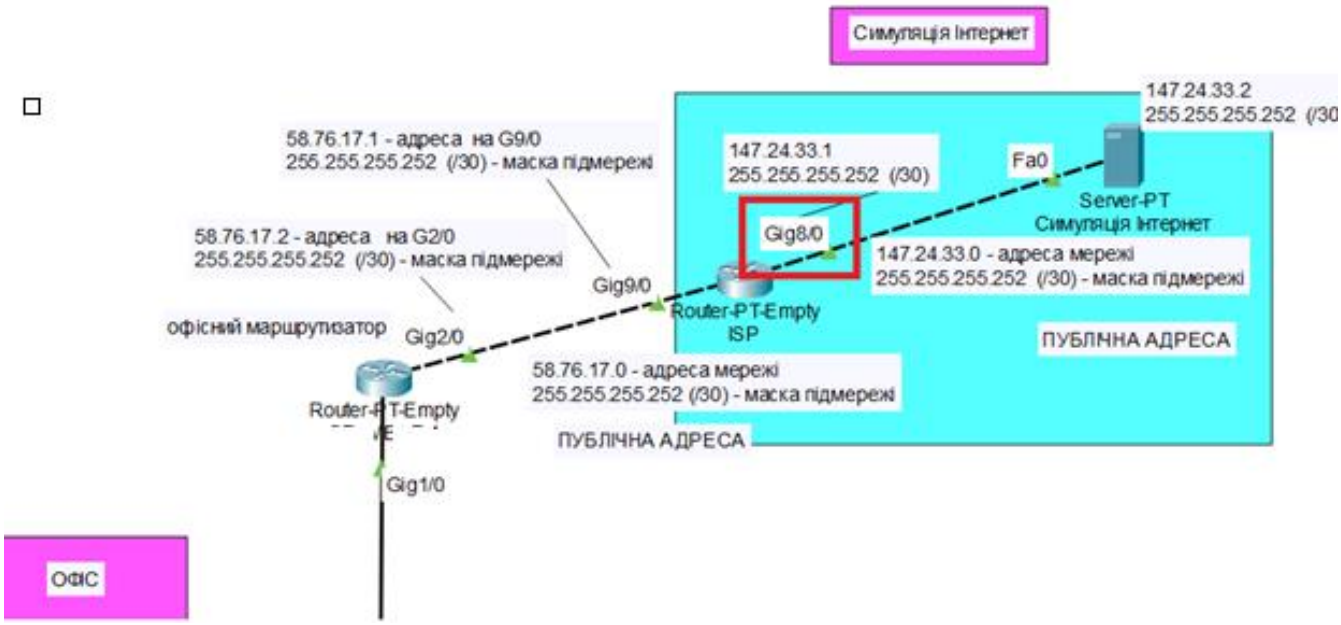


Рисунок 9.12 – Налаштування інтерфейсу G8/0

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).

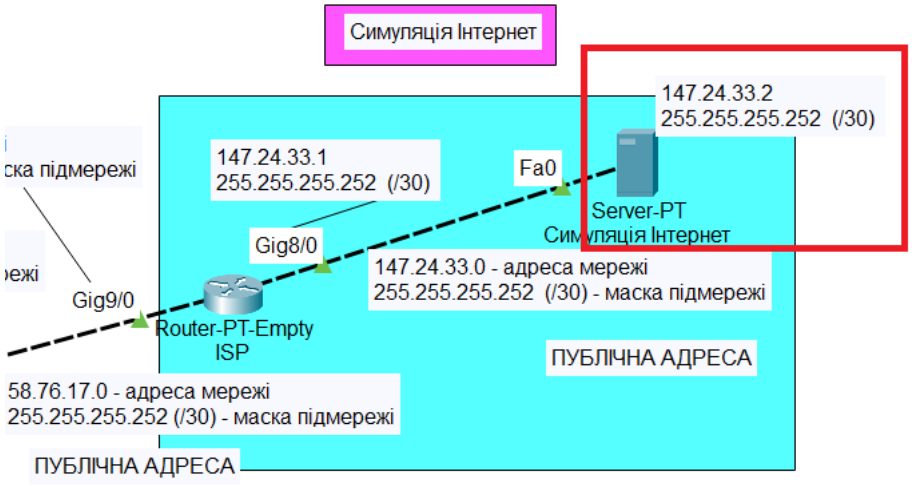


Рисунок 9.13 – Віддалений сервер

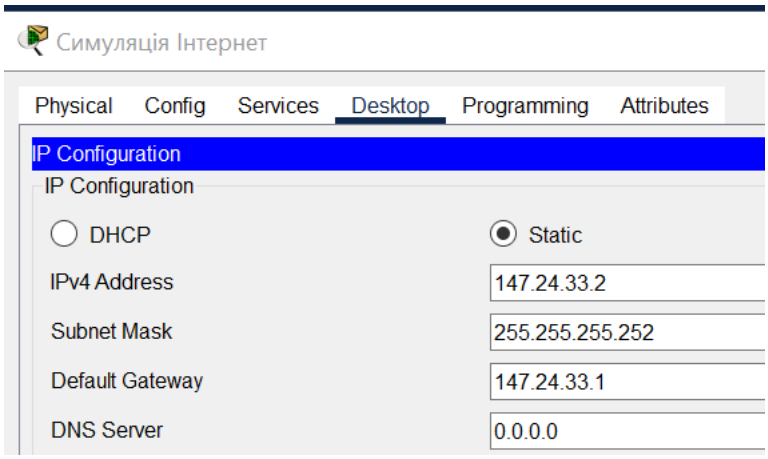


Рисунок 9.14 – Призначення серверу статичної IP-адреси

Перейти на маршрутизатор мережі (рис. 9.15) та налаштувати на порті G2/0 IP-адресу 58.76.17.2 та маску 255.255.255.252 (/30).

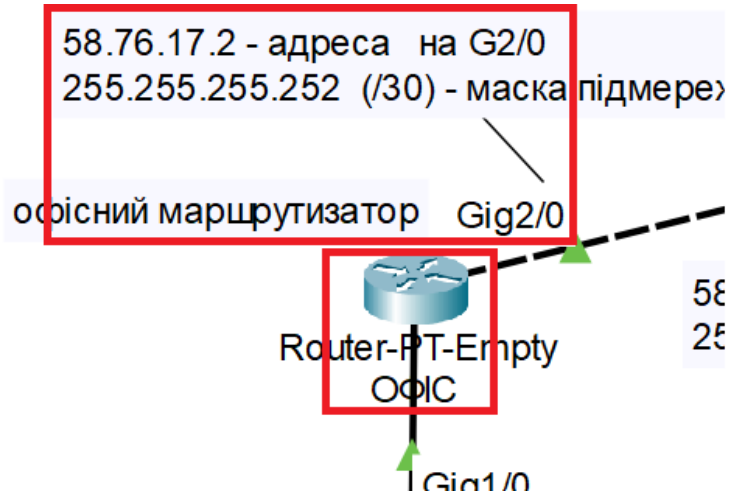


Рисунок 9.15 – Налаштування інтерфейсу G2/0

Також налаштуємо шлюз за замовчуванням на маршрутизаторі мережі (рис. 9.16), 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).

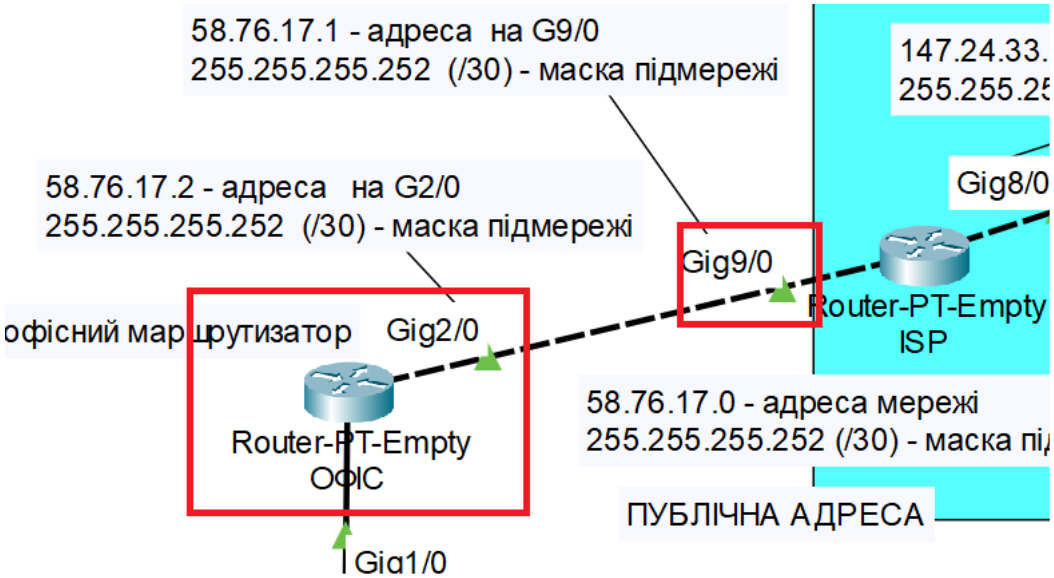


Рисунок 9.16 – Налаштування шлюзу за замовчуванням на маршрутизаторі мережі

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. 9.17), який інтерфейс буде зовнішнім, а який внутрішнім для NAT.

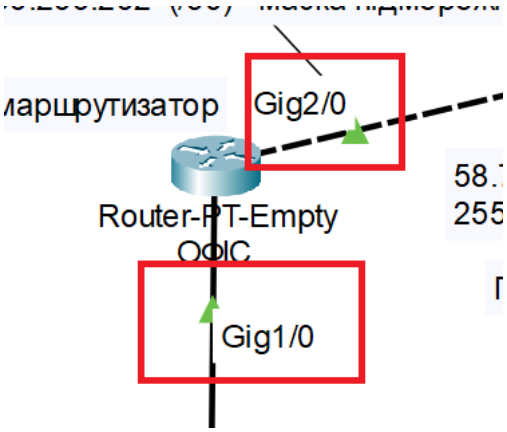


Рисунок 9.17 – Визначення внутрішніх та зовнішніх інтерфейсів

Інтерфейс G2/0 – налаштувати як office(config-if)#ip nat outside (рис. 9.18).

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

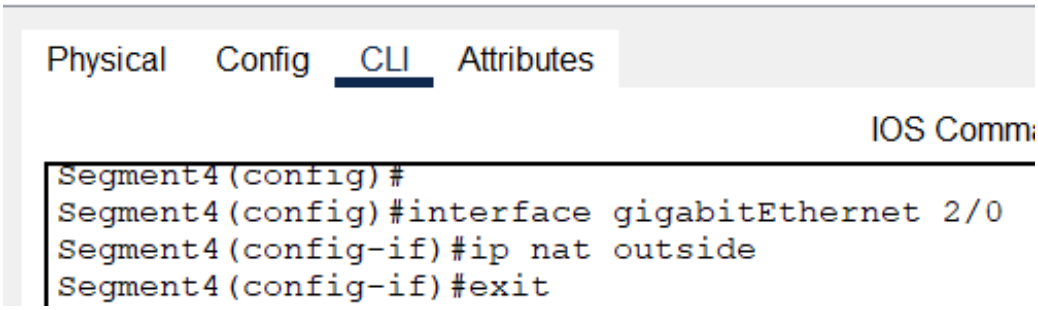


Рисунок 9.18 – Налаштування інтерфейсу G2/0

Підінтерфейси G1/0.10, G1/0.20, G1/0.30, G1/0.40 (рис. 9.19) – налаштувати як office(config-subif)#ip nat inside.

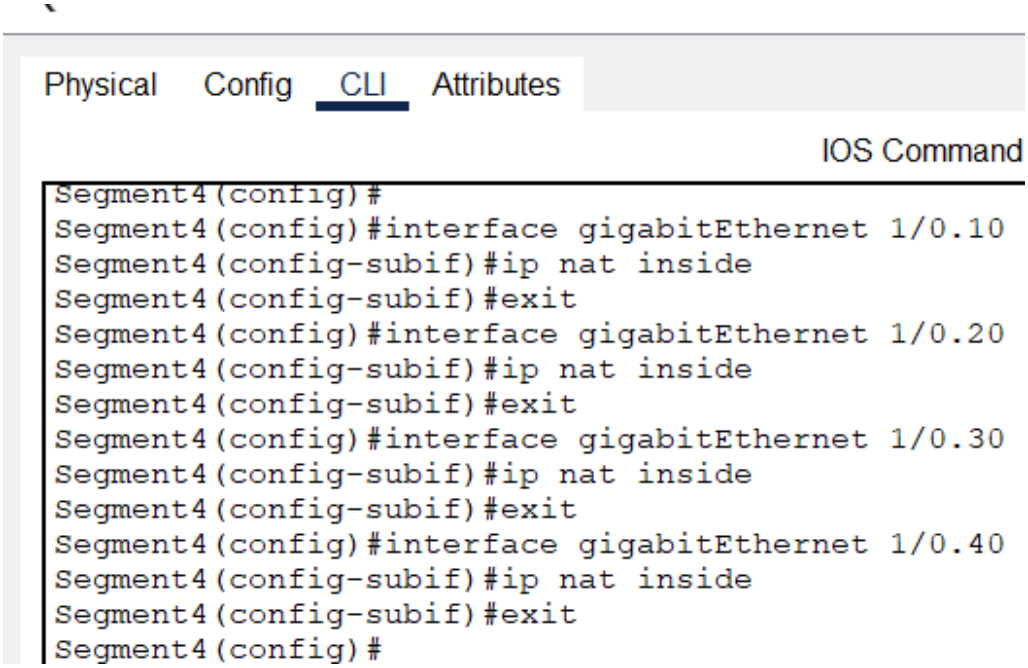


Рисунок 9.19 – Налаштування підінтерфейсів G1/0.10, G1/0.20, G1/0.30, G1/0.40

Тепер потрібно створити access-list, який буде характеризувати, який саме трафік будемо «натити» (рис. 9.20-9.21).

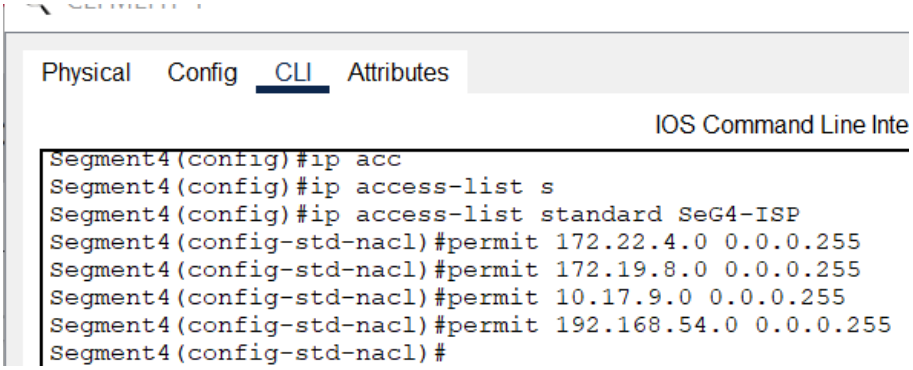


Рисунок 9.20 – Створення access-list

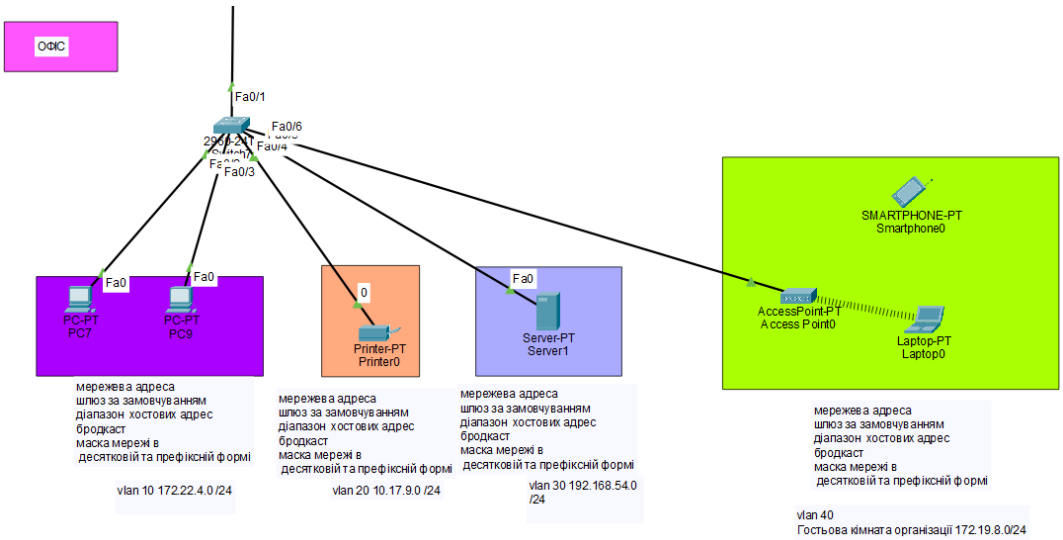


Рисунок 9.21 – Схема для створення access-list

Та прописати наступну команду (рис. 9.22):
office(config)#ip nat inside source list SeG4-ISP interface gigabitEthernet 2/0 overload

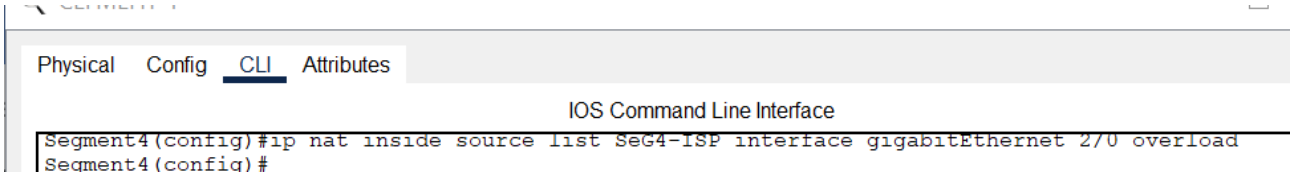


Рисунок 9.22 – Команда ip nat inside source list SeG4-ISP interface gigabitEthernet 2/0 overload

Якщо налаштування виконані вірно, то при перевірці з'єднання пінг між елементами мережі, позначеними на рис. 9.23, буде вдалим, наприклад, як на рис. 9.24.

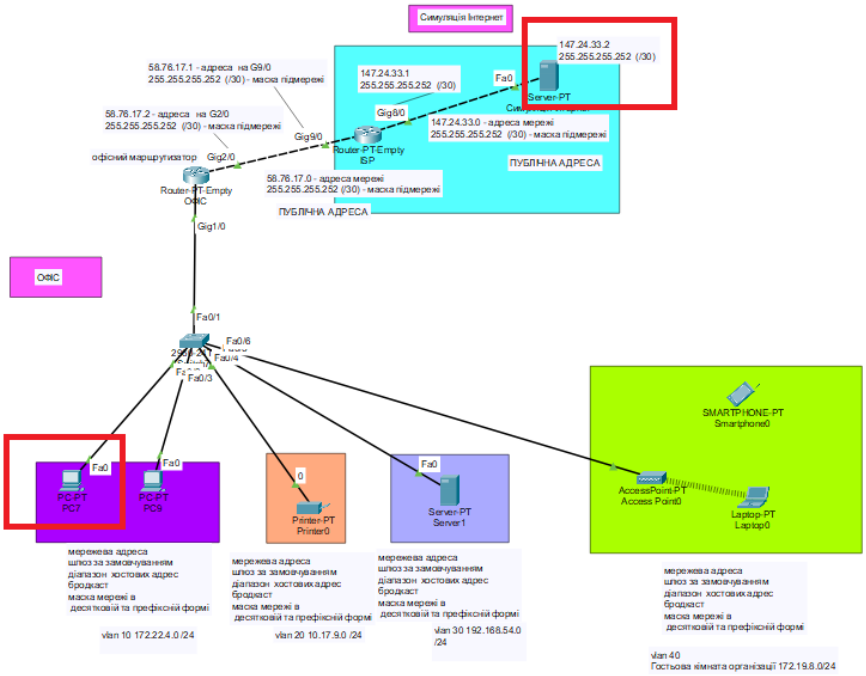


Рисунок 9.23 – Перевірка зв'язку з локальної мережі до віддаленого сервера

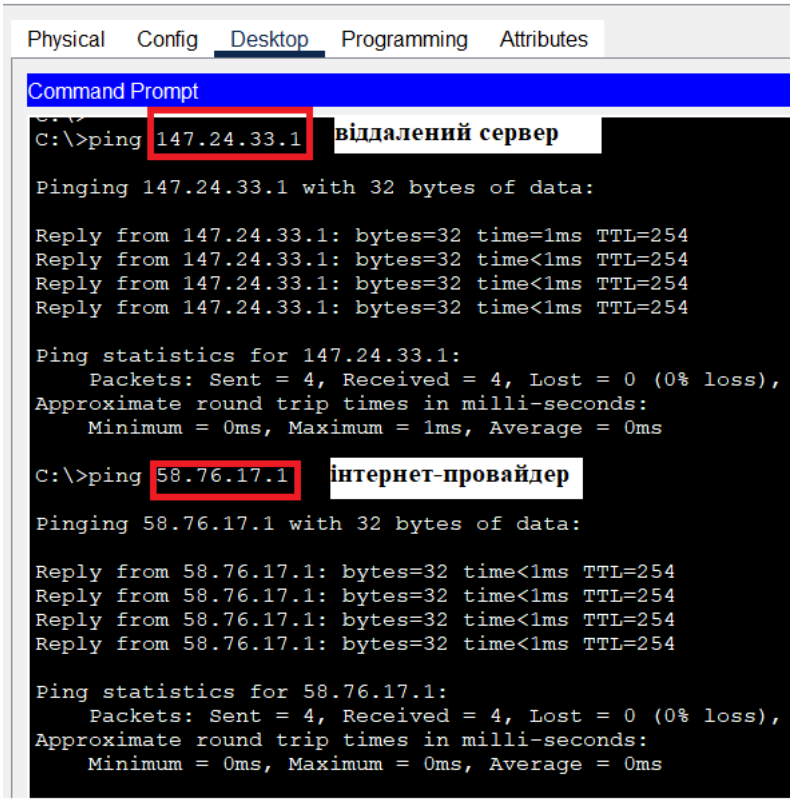


Рисунок 9.24 – Перевірка зв’язку з локальної мережі до віддаленого сервера

Застосуємо на маршрутизаторі ОФІС команду office#show ip nat translations і побачимо трансляцію NAT (рис. 9.25).

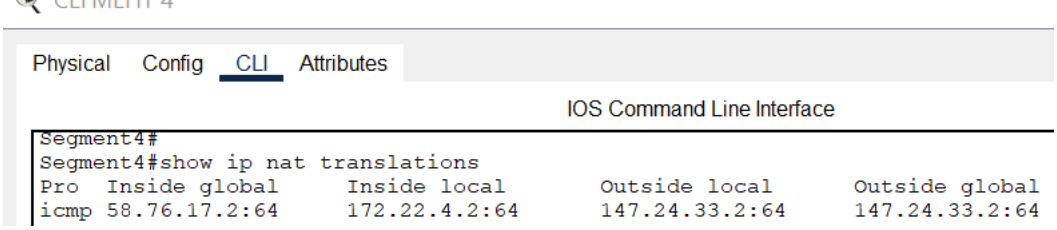


Рисунок 9.25 – Трансляція NAT

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 смартфона з віддаленим сервером.

Практичне заняття 10
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.

Теоретичні відомості

Опрацюйте матеріал [11, 16, 17].

«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 [11].

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. 10.1) [11].

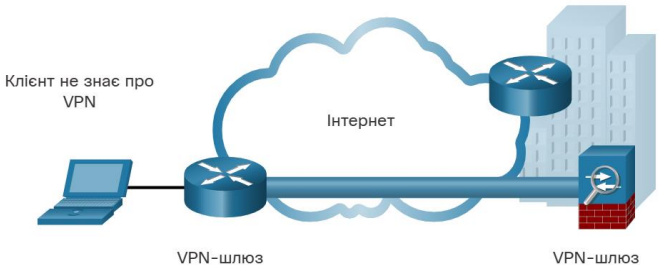


Рисунок 10.1 – Site-to-Site VPN [11]

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.

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

Завдання виконати згідно варіанту, поданому в таблиці 10.1. Номер варіанту – порядковий номер в списку групи.

Таблиця 10.1 – 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
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

1. Створити топологію мережі, зображену на рис. 10.2;

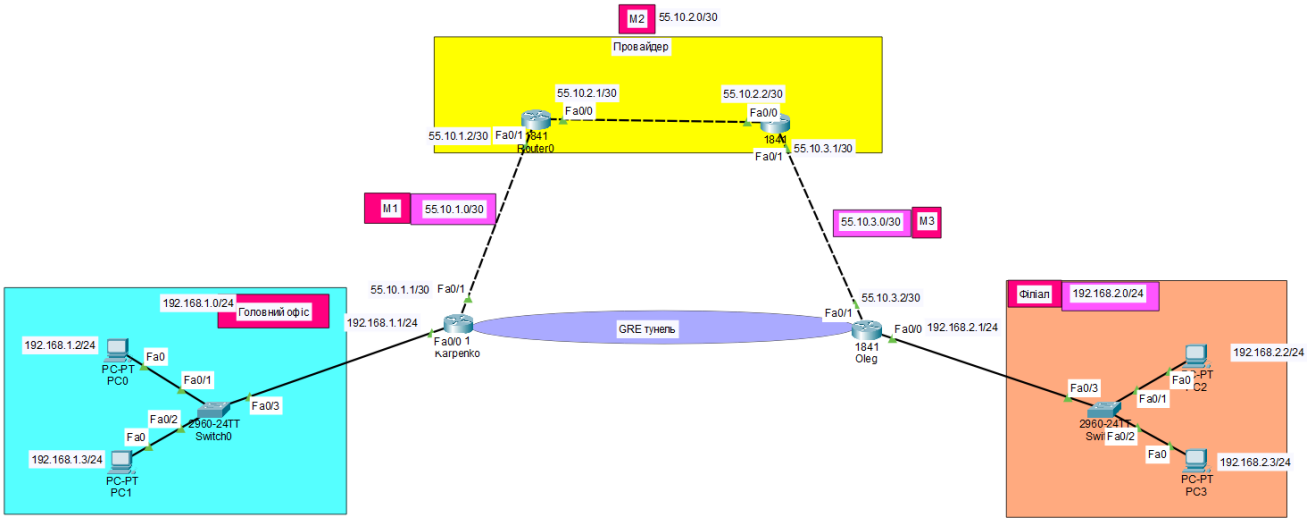


Рисунок 10.2 – Топологія мережі

2. адресацію використати згідно варіанту, поданому в таблиці 10.1;
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 відвовідно – ISP1 та ISP2;
7. призначити IP-адреси на інтерфейсах маршрутизаторів згідно варіанту, поданому в таблиці 10.1, 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. 10.3), застосувавши команду ping з маршрутизатора офісу (Karpenko) до IP-адресу інтерфейсу fastEthernet 0/1 маршрутизатора ISP2.

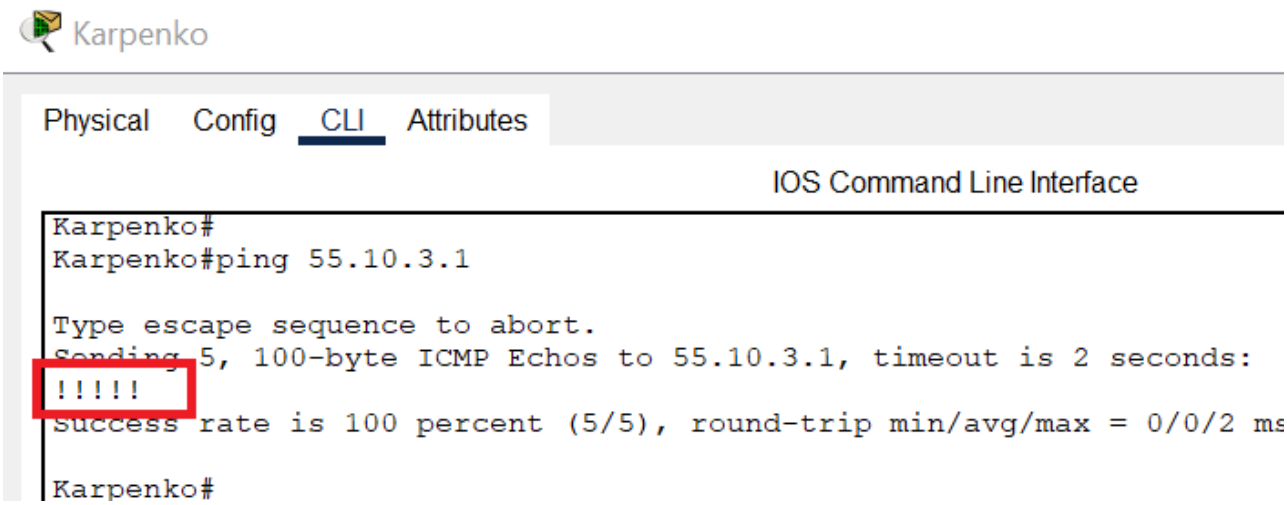


Рисунок 10.3 – Тестування роботоздатності мережі

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. 10.4), так як маршрутизатор головного офісу не знає шлях в мережу віддаленого офісу.

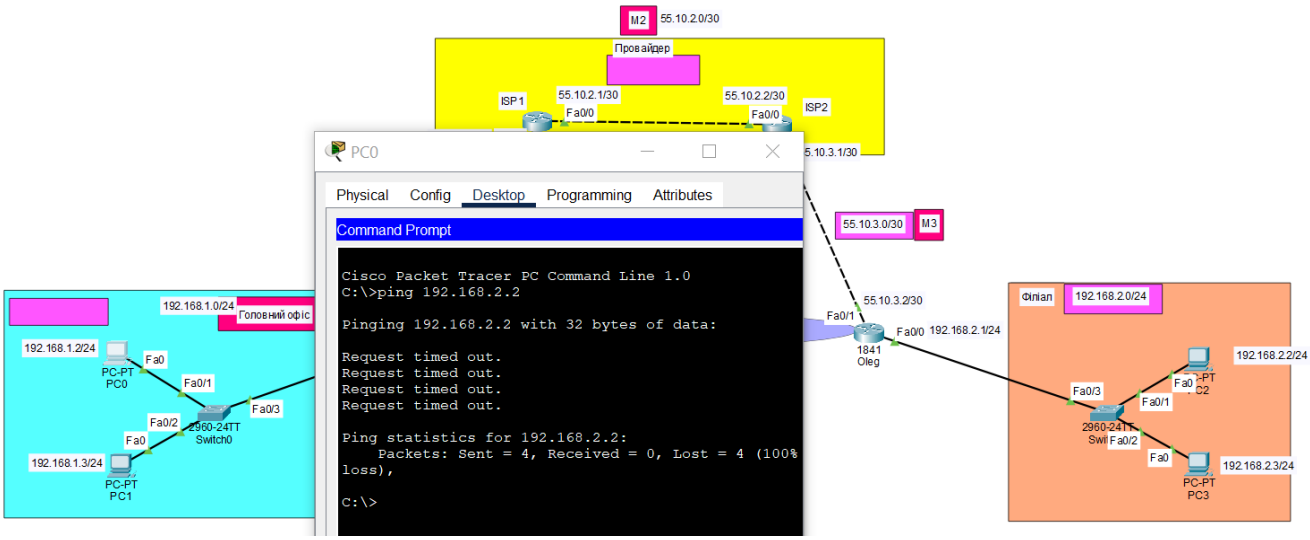


Рисунок 10.4 – Перевірка з'єднання між головним офісом та філіалом

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. 10.5).

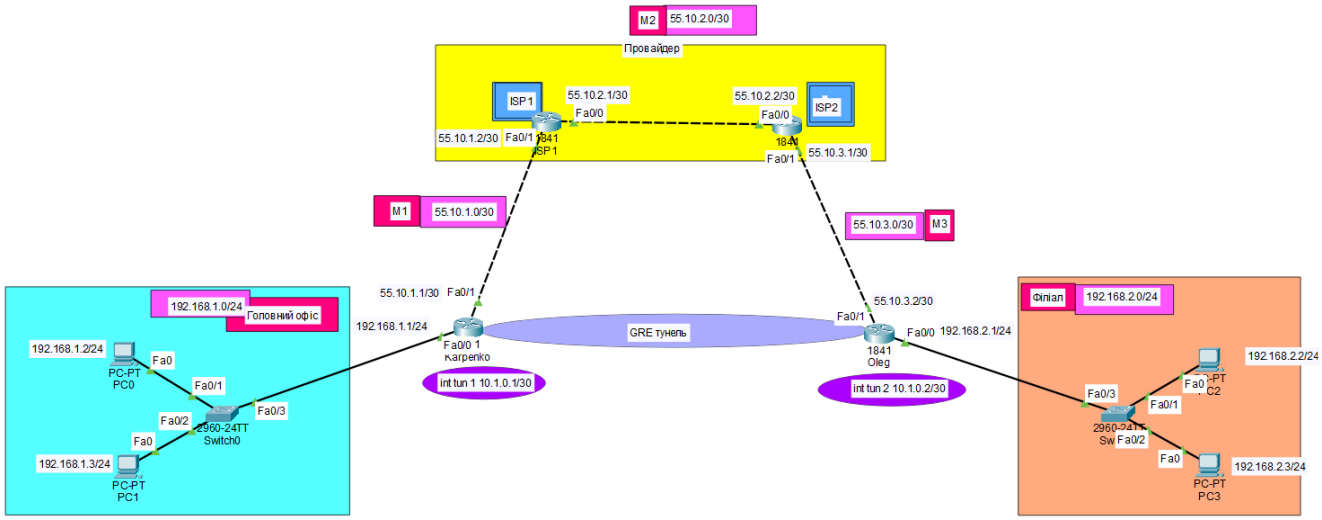


Рисунок 10.5 – Створення GRE-тунелю

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. 10.6). Результати виконання даної перевірки мають бути в звіті до роботи.

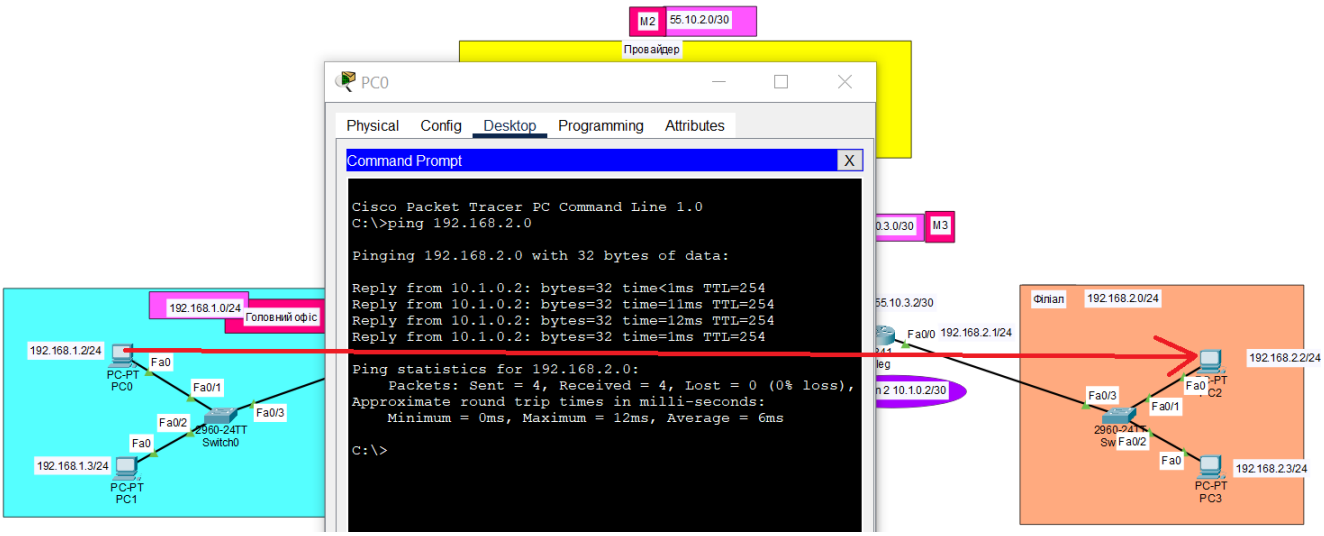


Рисунок 10.6 – Перевірка з'єднання між головним офісом та філіалом

Також переглянемо трасування командою tracert 192.168.2.2 (адреса PC2 філіалу) для того, щоб подивитись, через які маршрутизатори буде проходити пакет (рис. 10.7).

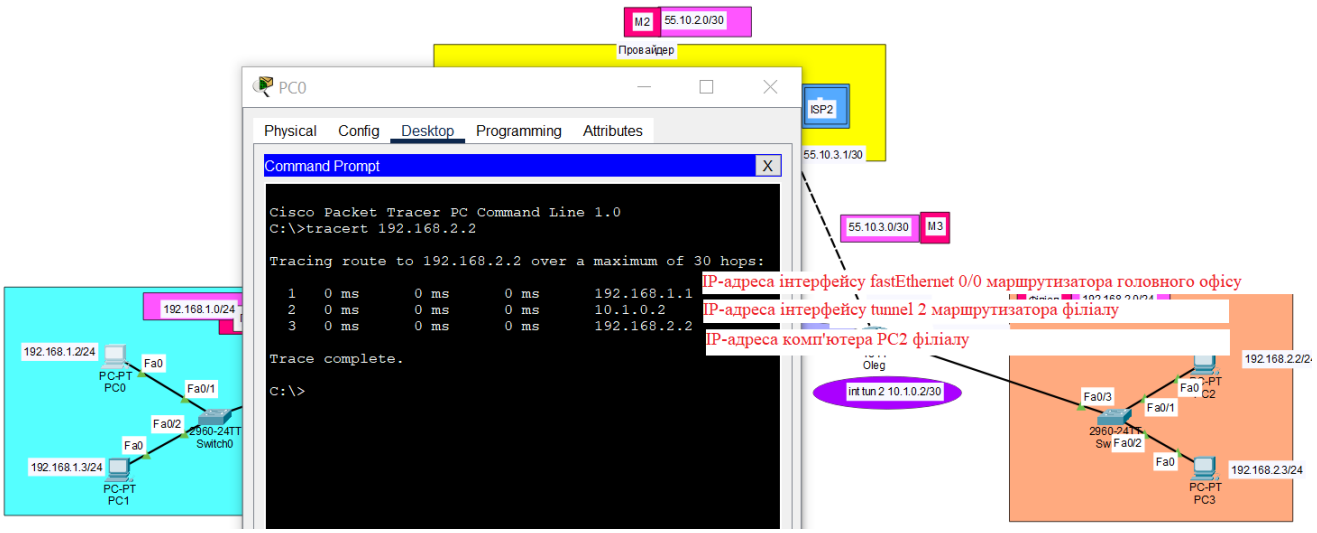


Рисунок 10.7 – Трасування командою tracert

Як бачимо з рис. 10.7, в трасуванні не відображені маршрутизатори провайдера.

Перегляд налаштувань в режимі симуляції

1. Перейти в режим симуляції (рис. 10.8) та відобразити в звіті в вигляді скрінів, що відбувається з пакетами при їх переміщенні по мережі.

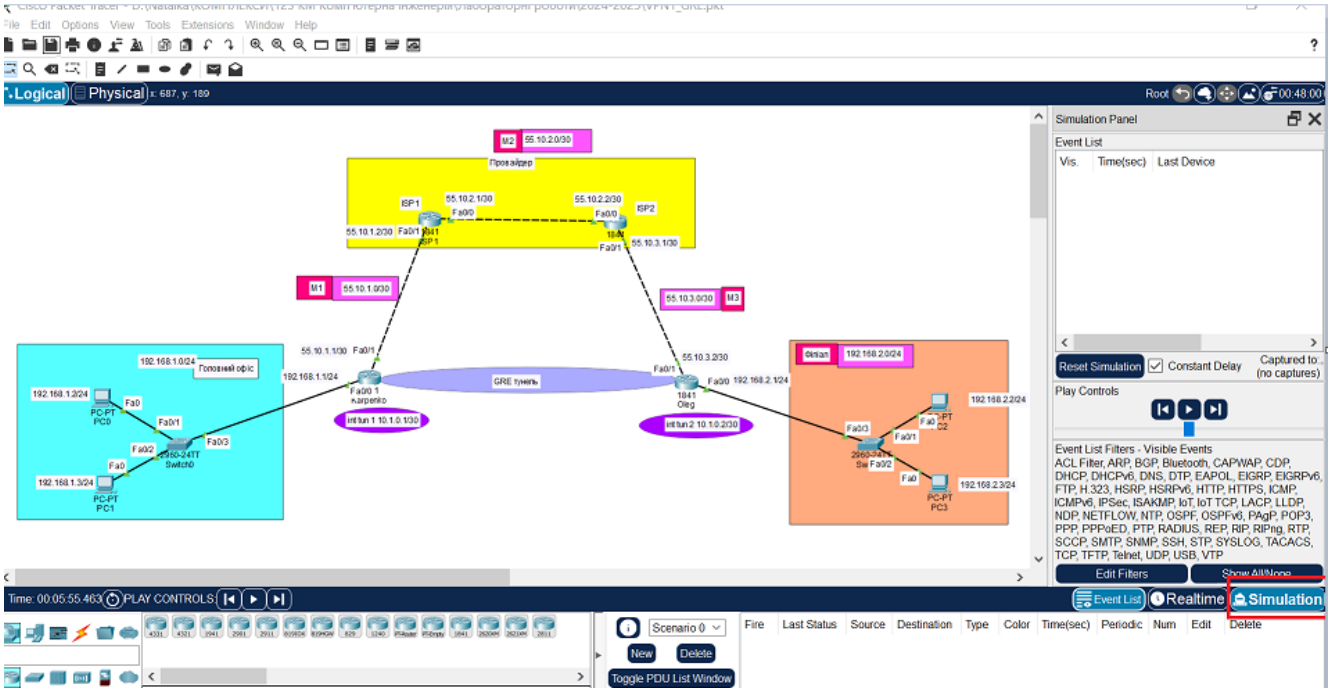


Рисунок 10.8 – Режим симуляції

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. 10.9). Пропінгувати PC0 та PC2 (рис. 10.10), використавши кнопку .

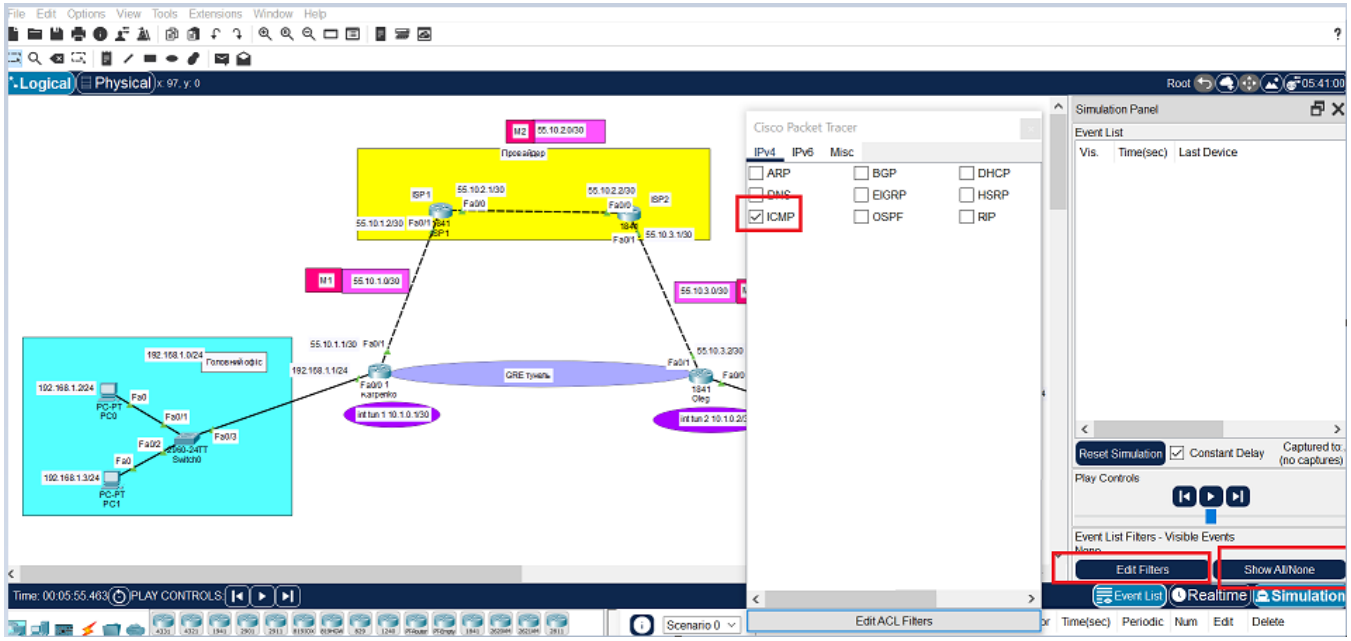


Рисунок 10.9 – В фільтрах відображати тільки пакети протоколу ICMP

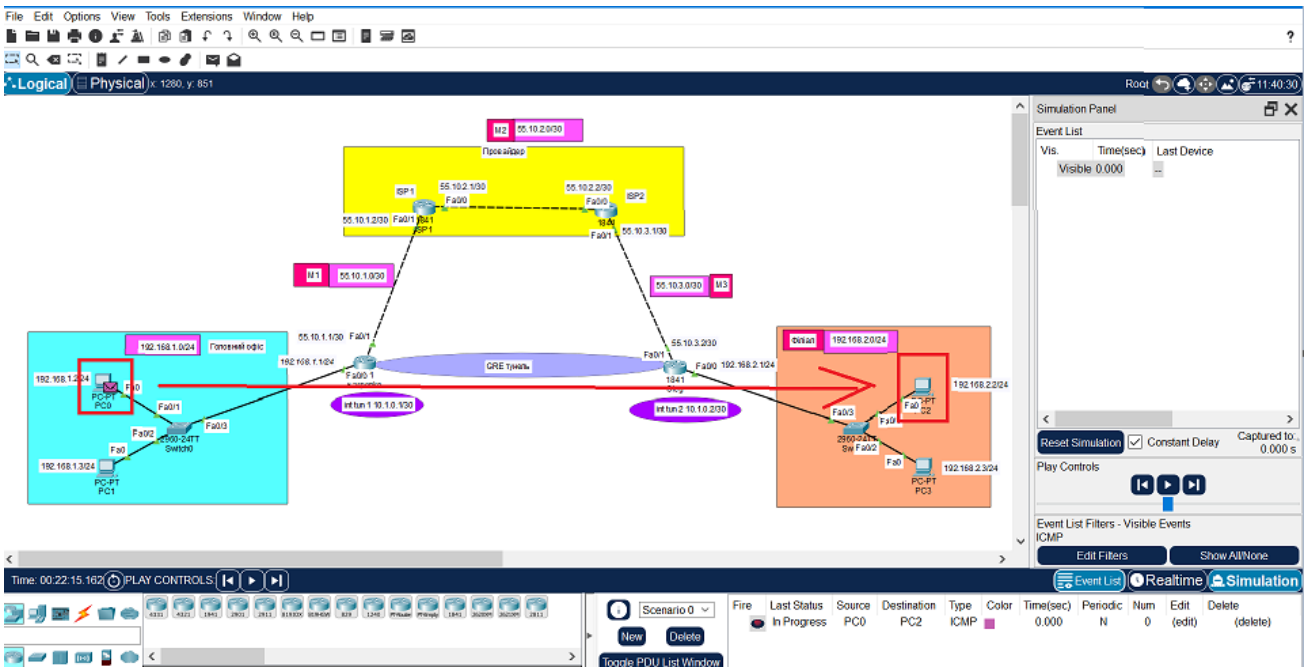


Рисунок 10.10 – Пропінгувати PC0 та PC2

Натиснути кнопку  (Capture) два рази (рис. 10.11), 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. 10.12).

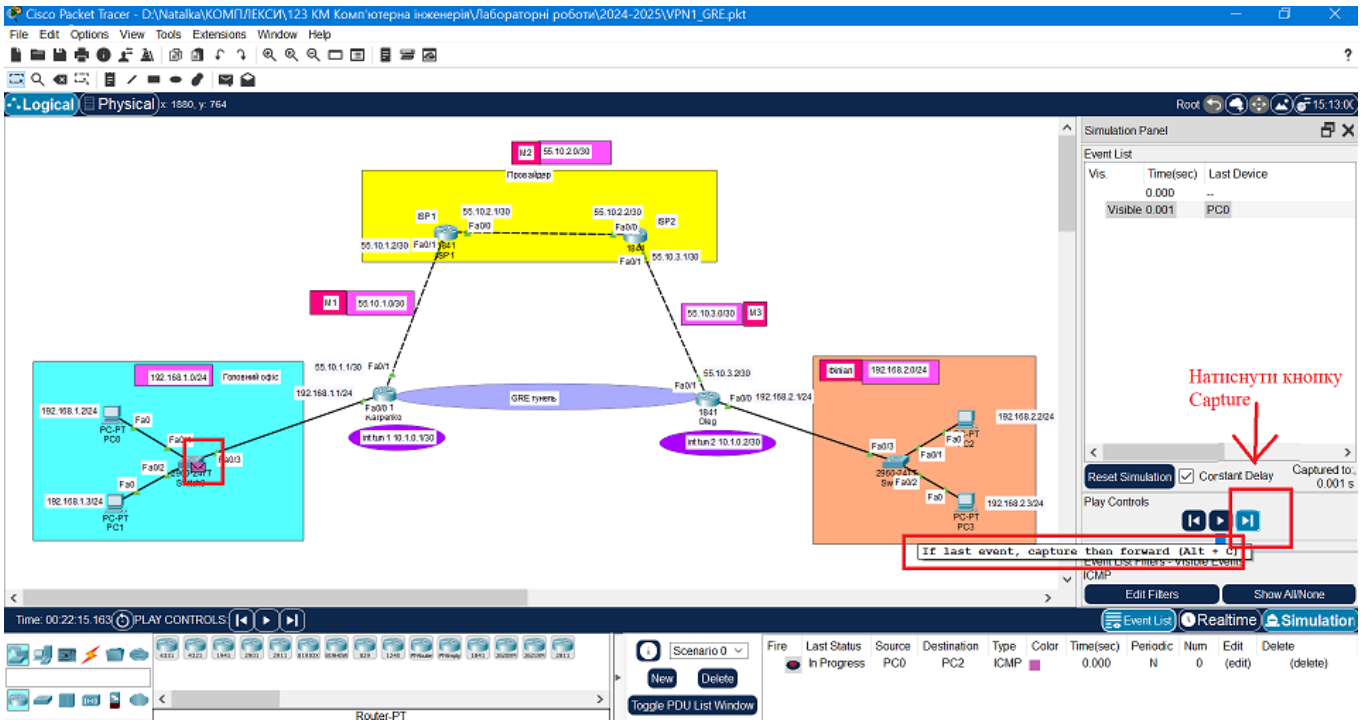


Рисунок 10.11 – Перегляд переміщення пакету з комп’ютера на комутатор

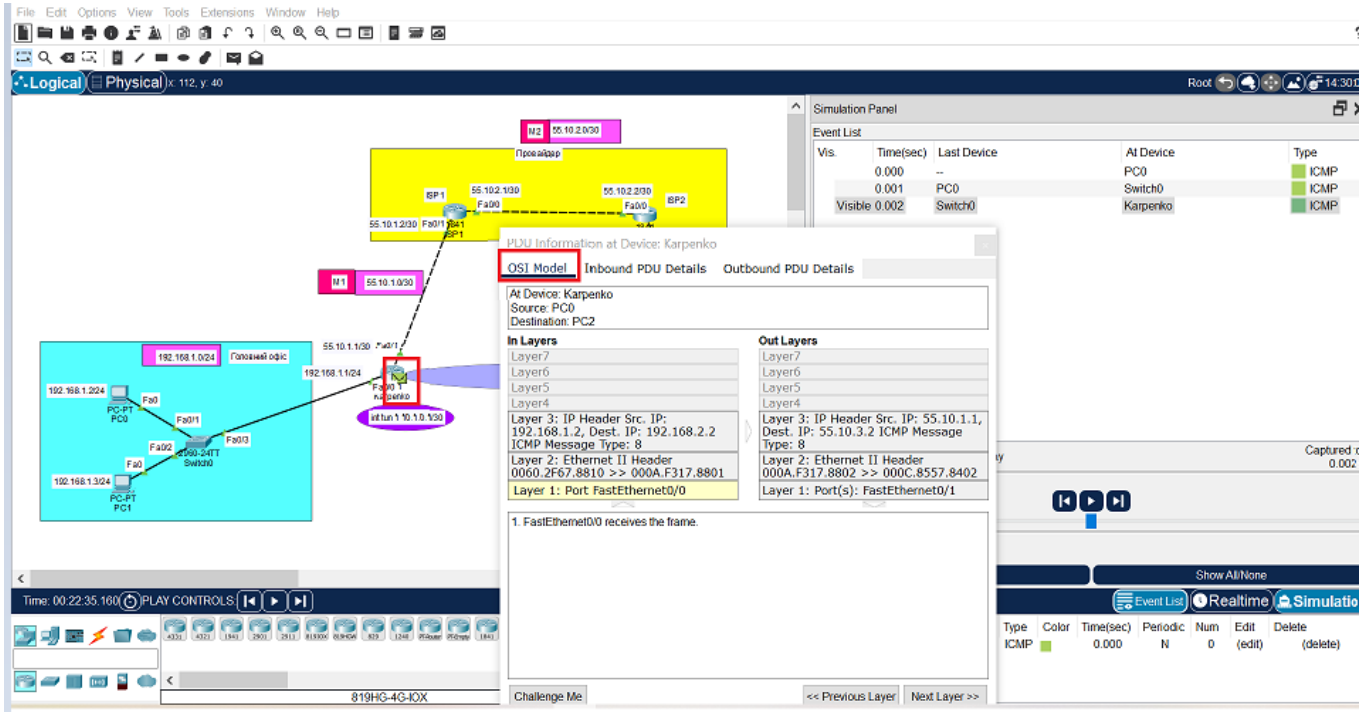


Рисунок 10.12 – Перегляд вмісту пакету на маршрутизаторі головного офісу

Розглядаючи вміст даного пакету (рис. 10.13), 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.

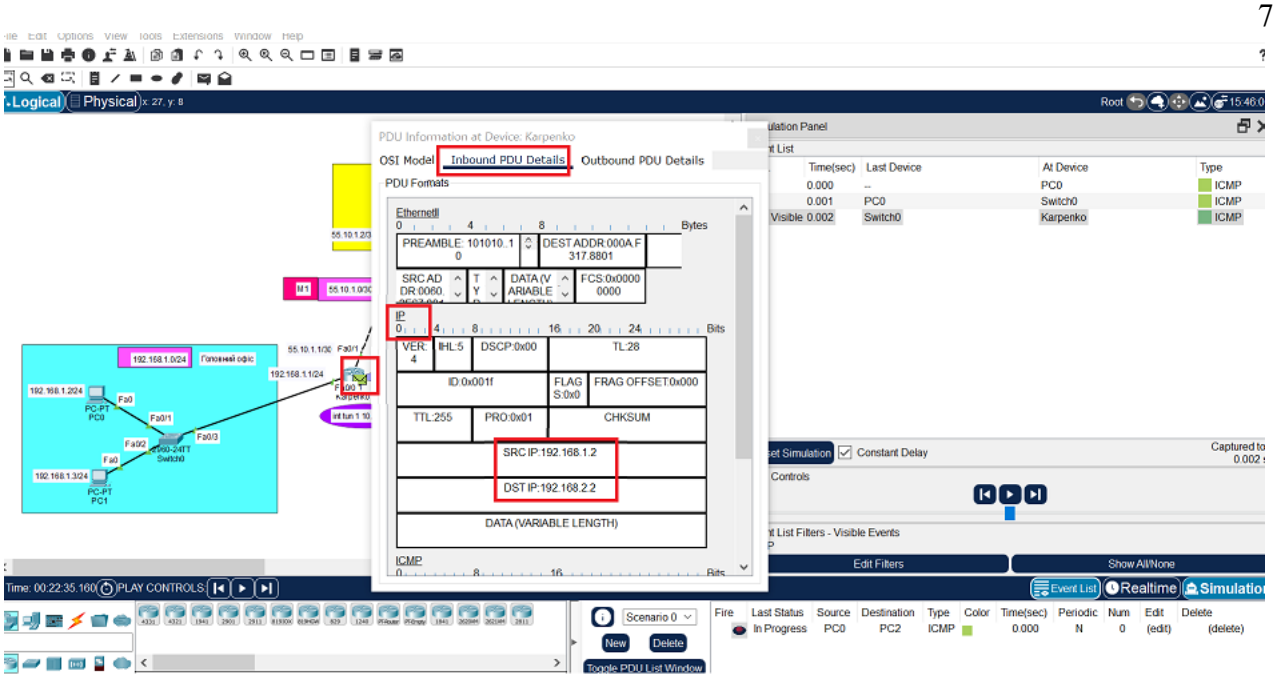


Рисунок 13.13 – Вхідний пакет з мережі на маршрутизатор

На виході пакета з маршрутизатора (рис. 10.14) 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.

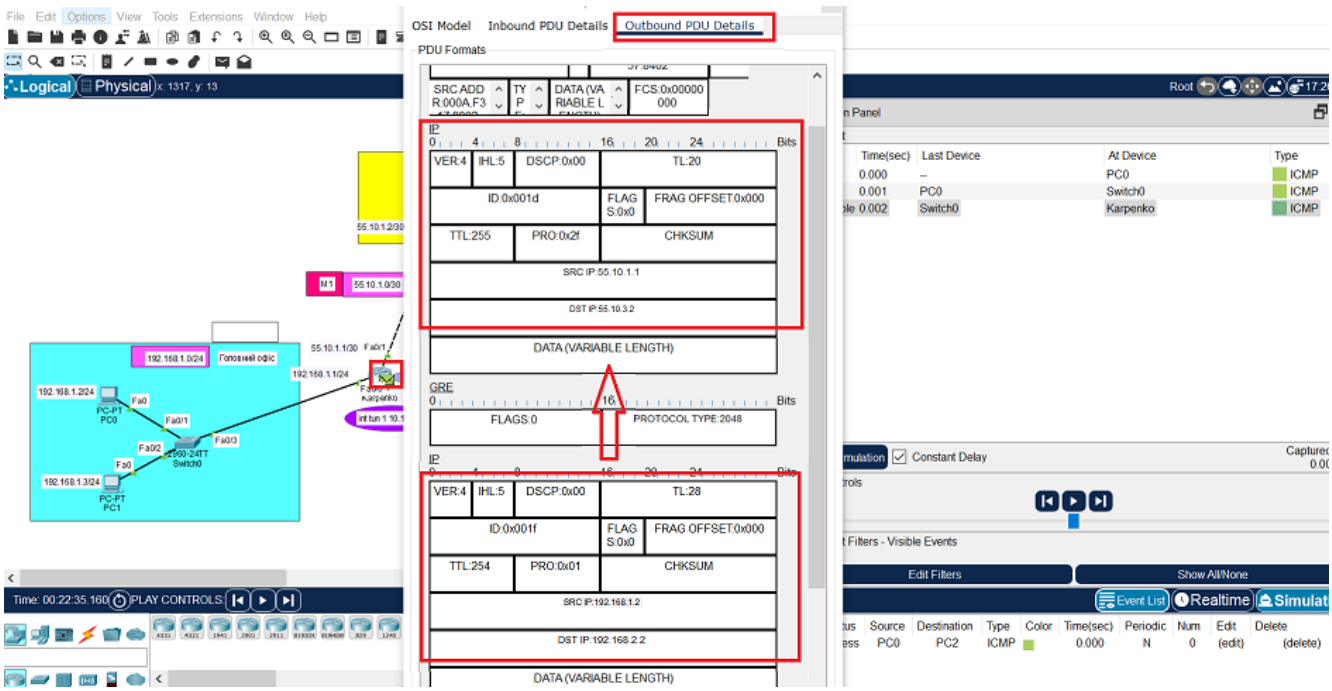


Рисунок 10.14 – Інформація про вихідний пакет з маршрутизатора головного офісу

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. 10.15-10.17).

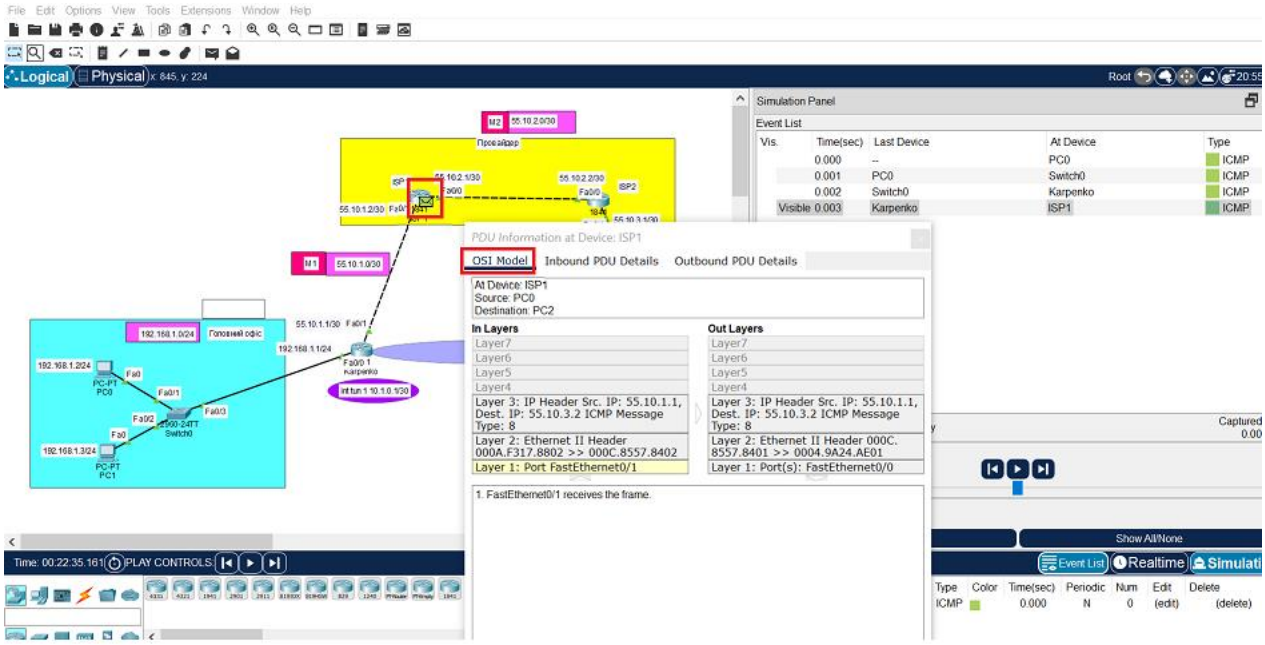


Рисунок 10.15 – Інформація про пакет на маршрутизаторі ISP1

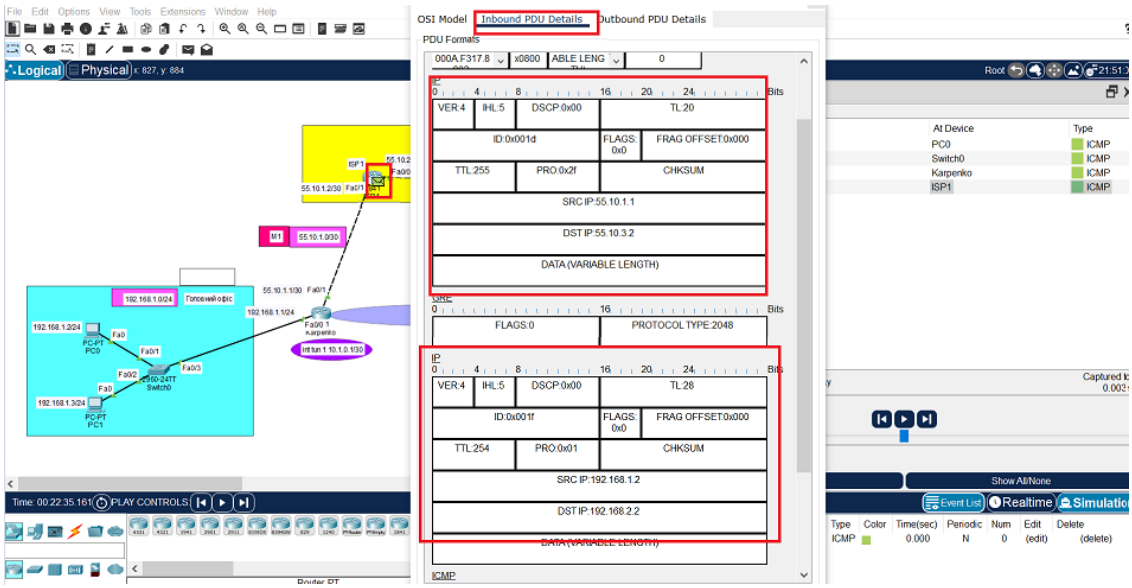


Рисунок 10.16 – Вхідний пакет з мережі на маршрутизаторі ISP1

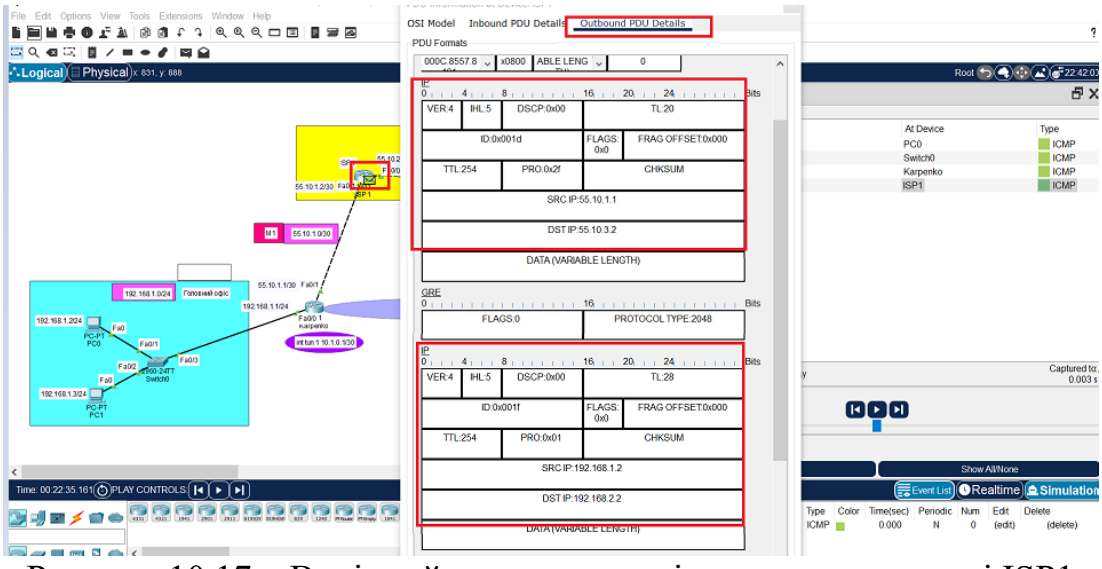


Рисунок 10.17 – Вихідний пакет з мережі на маршрутизаторі ISP1

Натиснути ще два рази кнопку  (Capture). Пакет перемістився з маршрутизатора ISP1 на маршрутизатор філіалу (рис. 10.18).

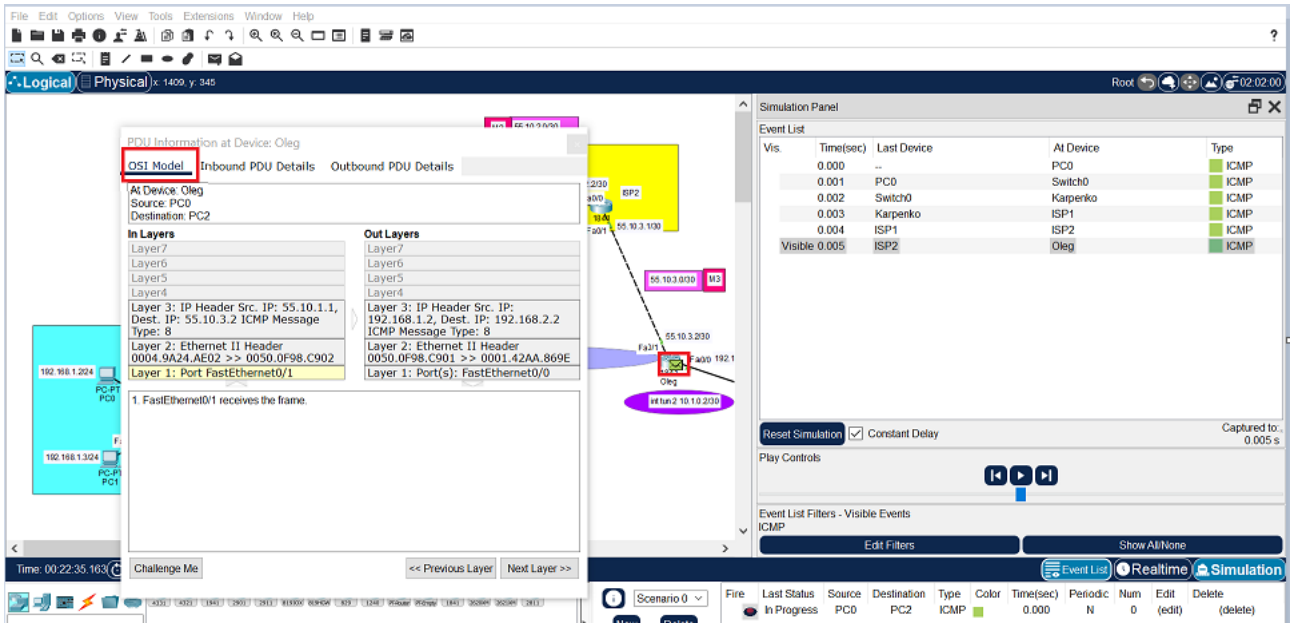


Рисунок 10.18 – Інформація про пакет на маршрутизаторі філіалу

На вході в маршрутизатор філіалу пакет все ще інкапсульований (рис. 10.19), а на виході (рис. 10.20) 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.

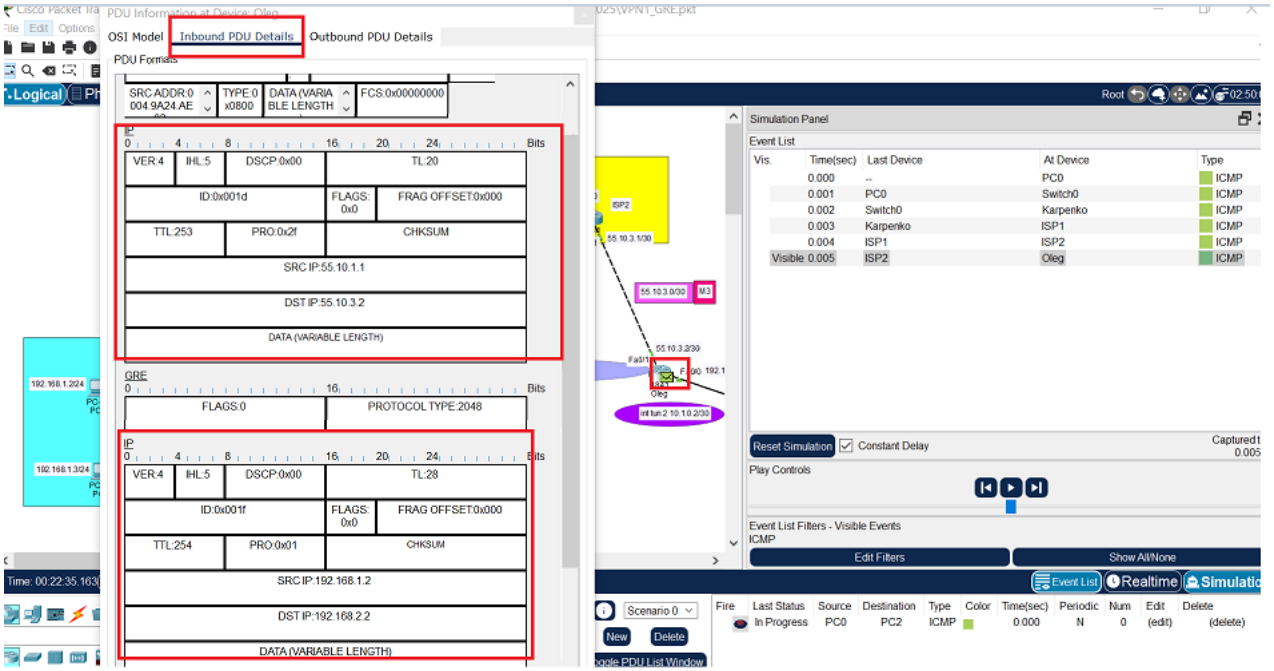


Рисунок10.19 – Вхідний пакет з мережі на маршрутизаторі філіалу

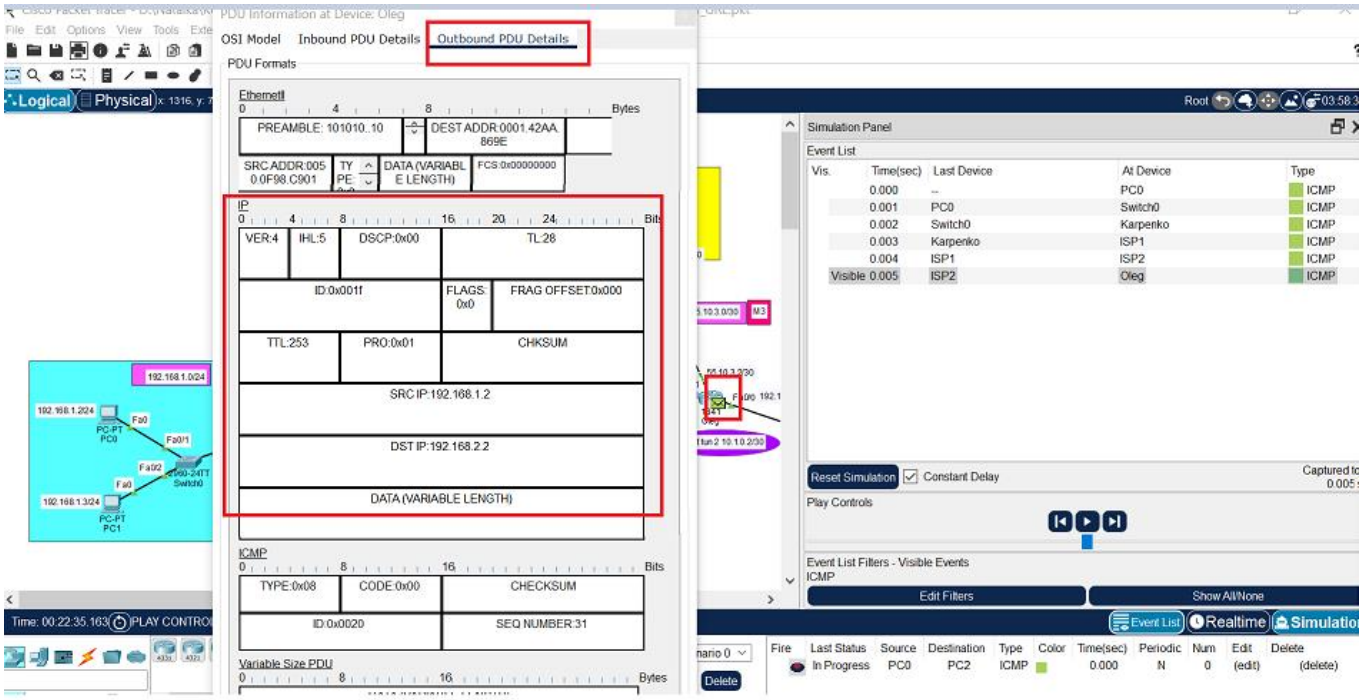


Рисунок 10.20 – Вихідний пакет з мережі на маршрутизаторі філіалу

Натиснути ще два рази кнопку (Capture) і пакет переміститься на комутатор, а тоді на PC2 (рис. 10.21).

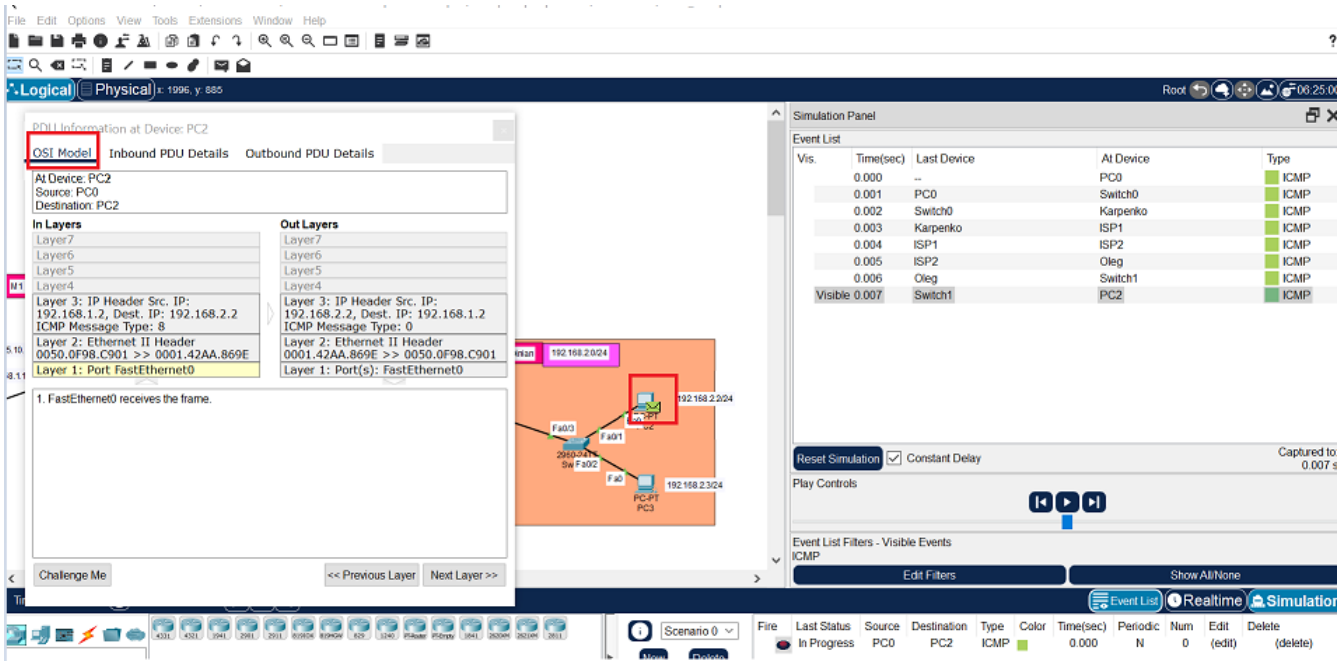


Рисунок 10.21 –Переміщення пакету на PC2

На рисунках 10.22 та 10.23 зображено вигляд вихідного та вхідного пакету, який знаходиться на PC2.

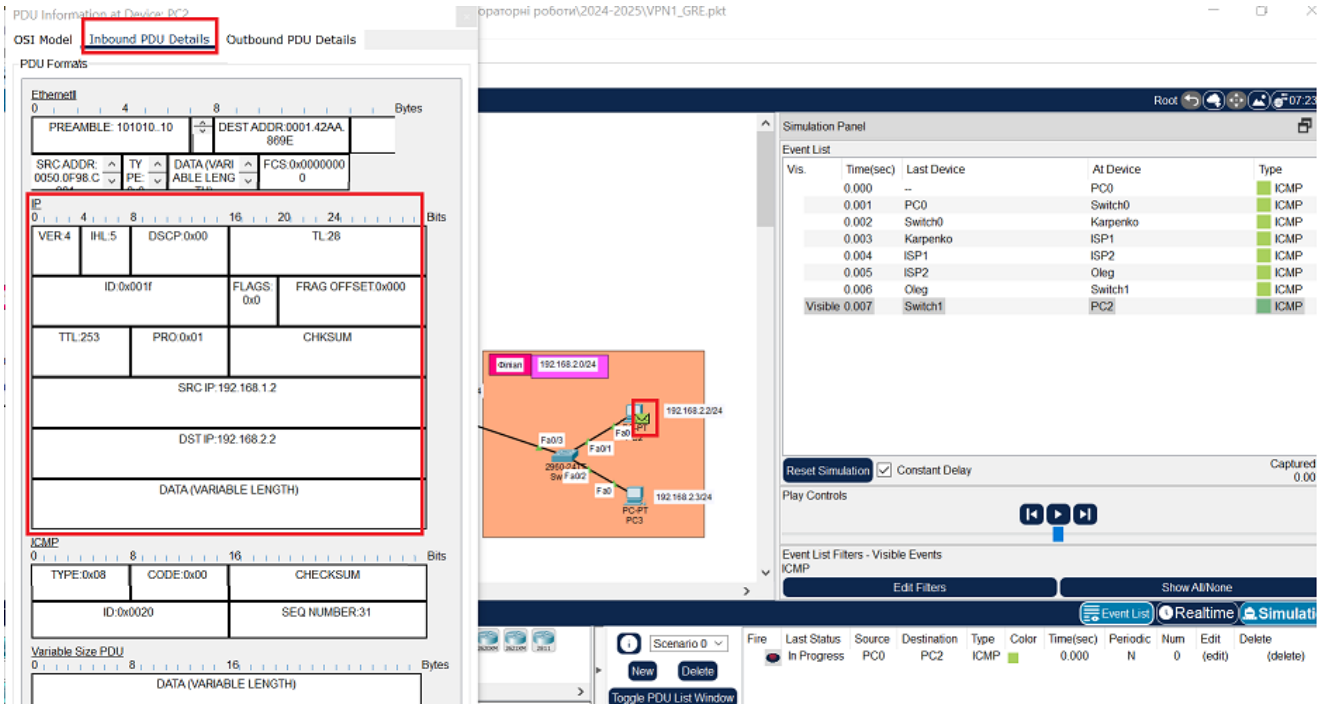


Рисунок 10.22 – Вхідний пакет на PC2

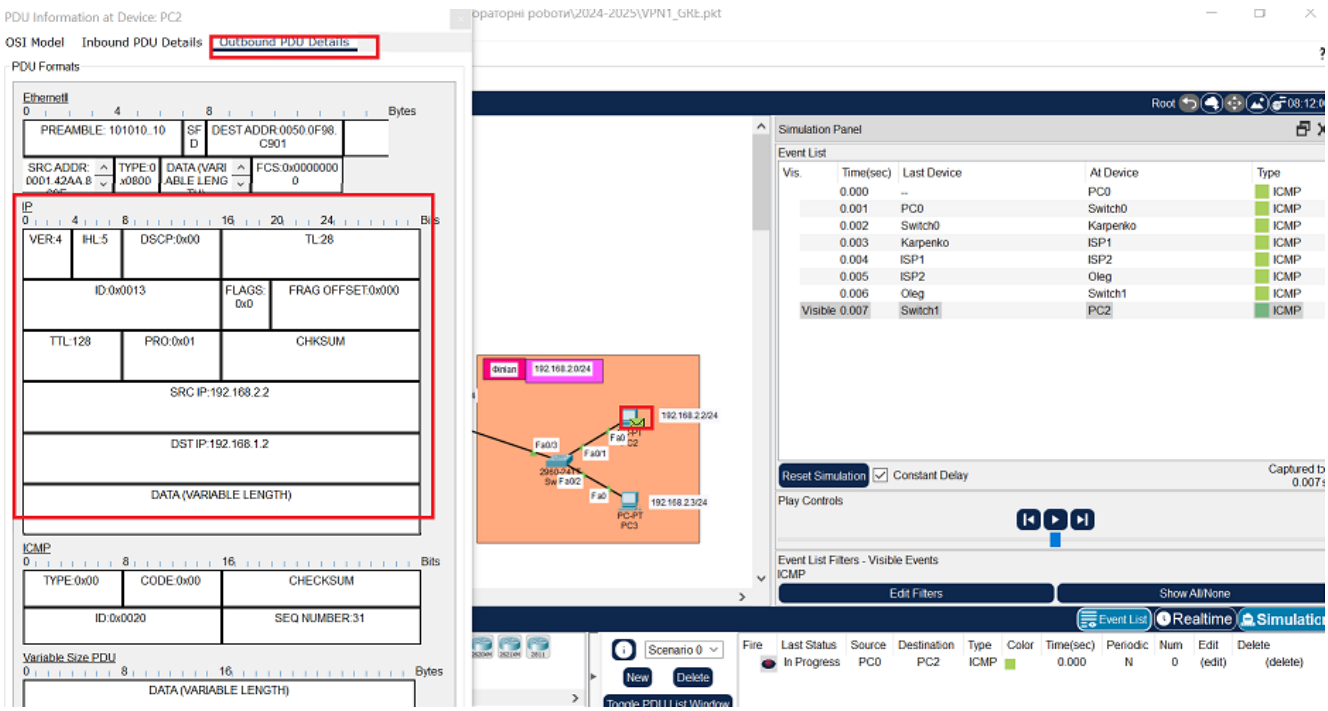


Рисунок 10.23 – Вихідний пакет на PC2

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. 10.24-10.26). Спочатку на машрутизаторі філіалу вхідний пакет буде в початковому стані (рис. 10.25), а на виході він вже буде інкапсульований (рис. 10.26).

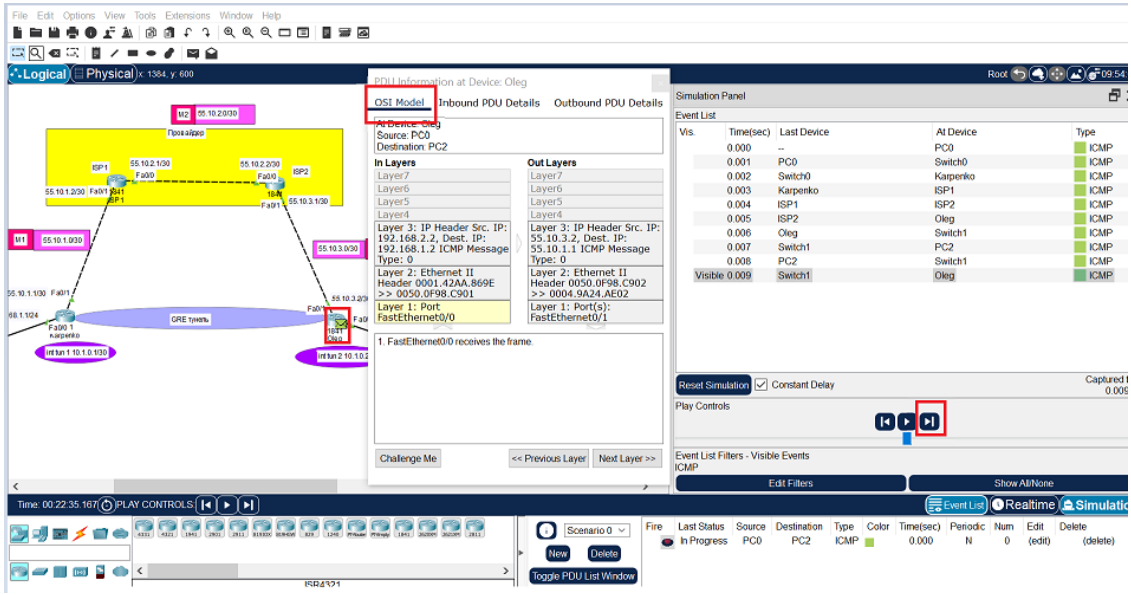


Рисунок 10.24 – Вкладка Модель OSI

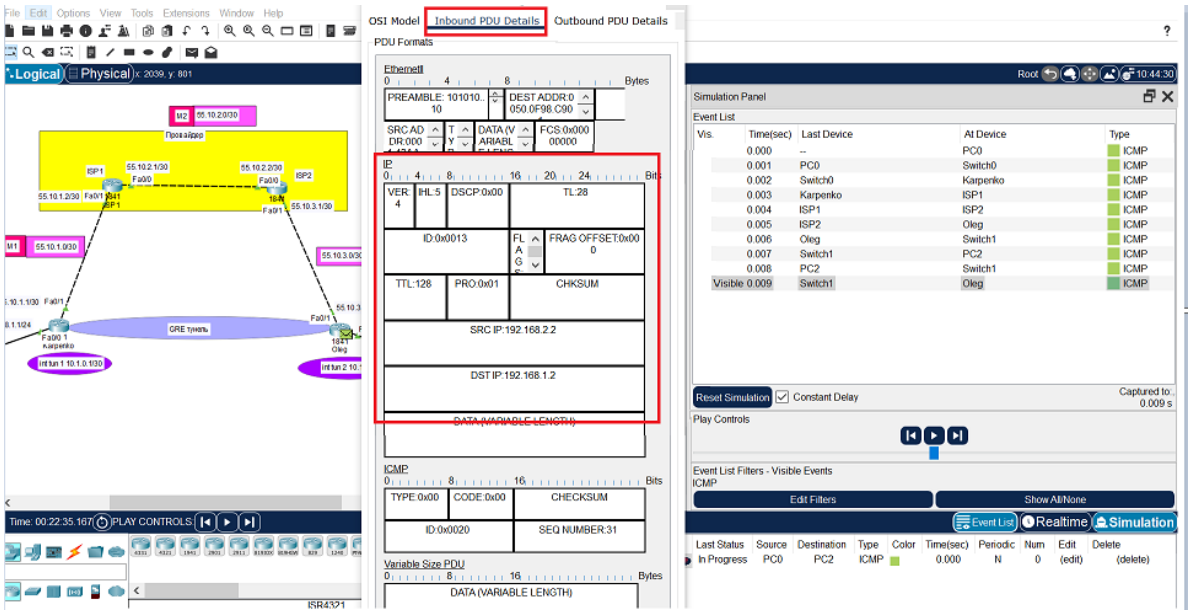


Рисунок 10.25 – Вхідний пакет на машрутизаторі філіалу

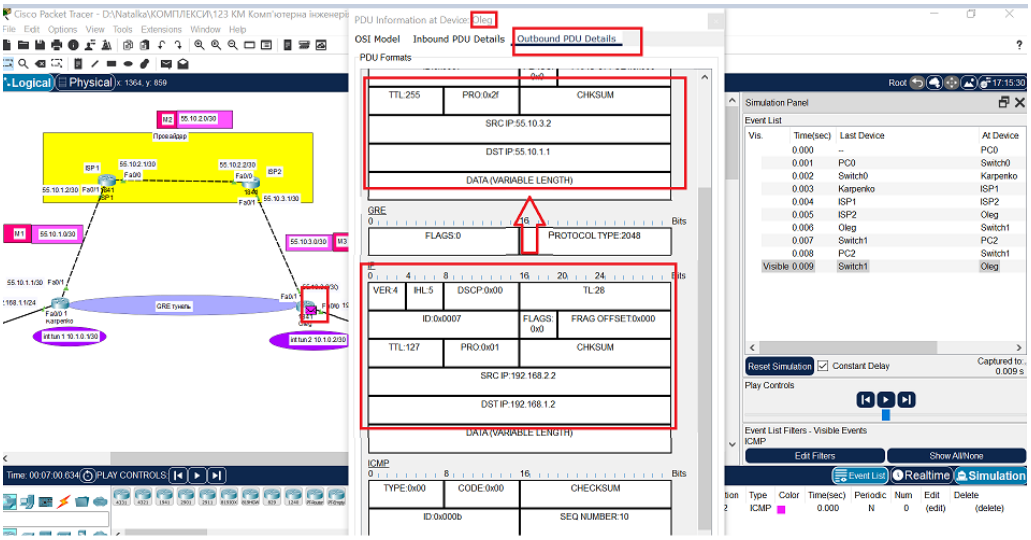


Рисунок 10.26 – Вихідний пакет на машрутизаторі філіалу (інкапсульований)

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. 10.27), а на виході відбудеться деінкапсуляція (рис. 10.28).

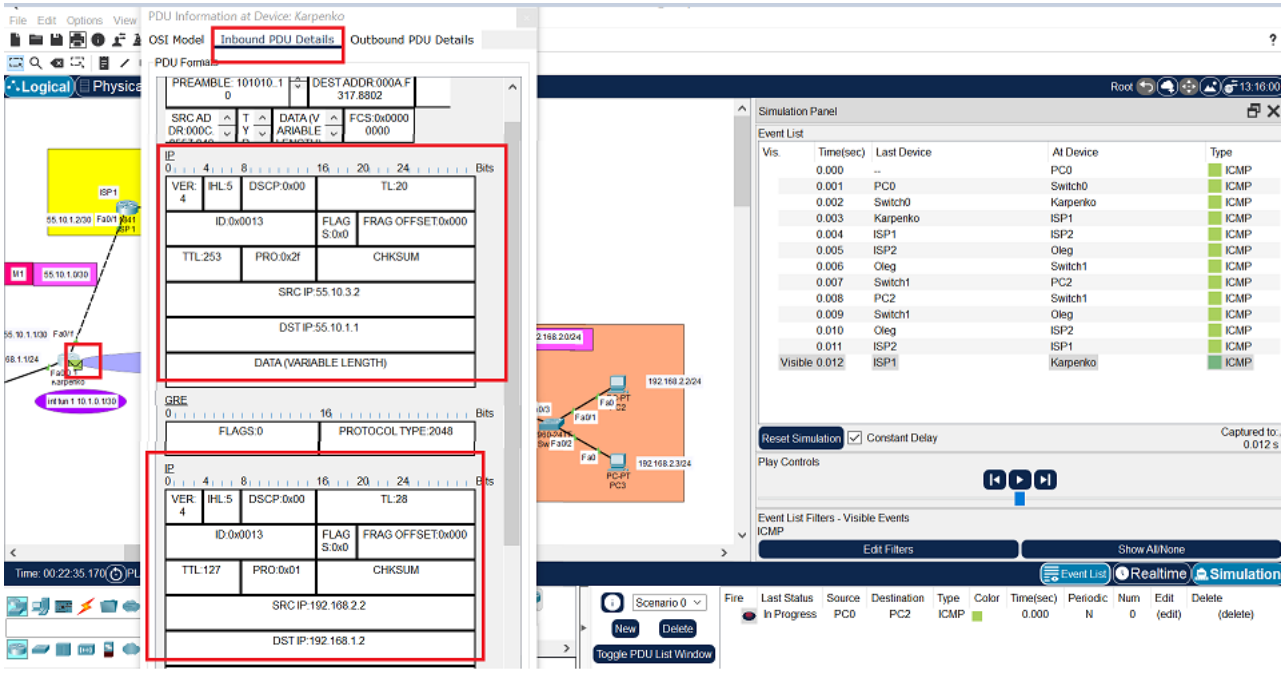


Рисунок 10.27 – Вхідний пакет на маршрутизаторі головного офісу

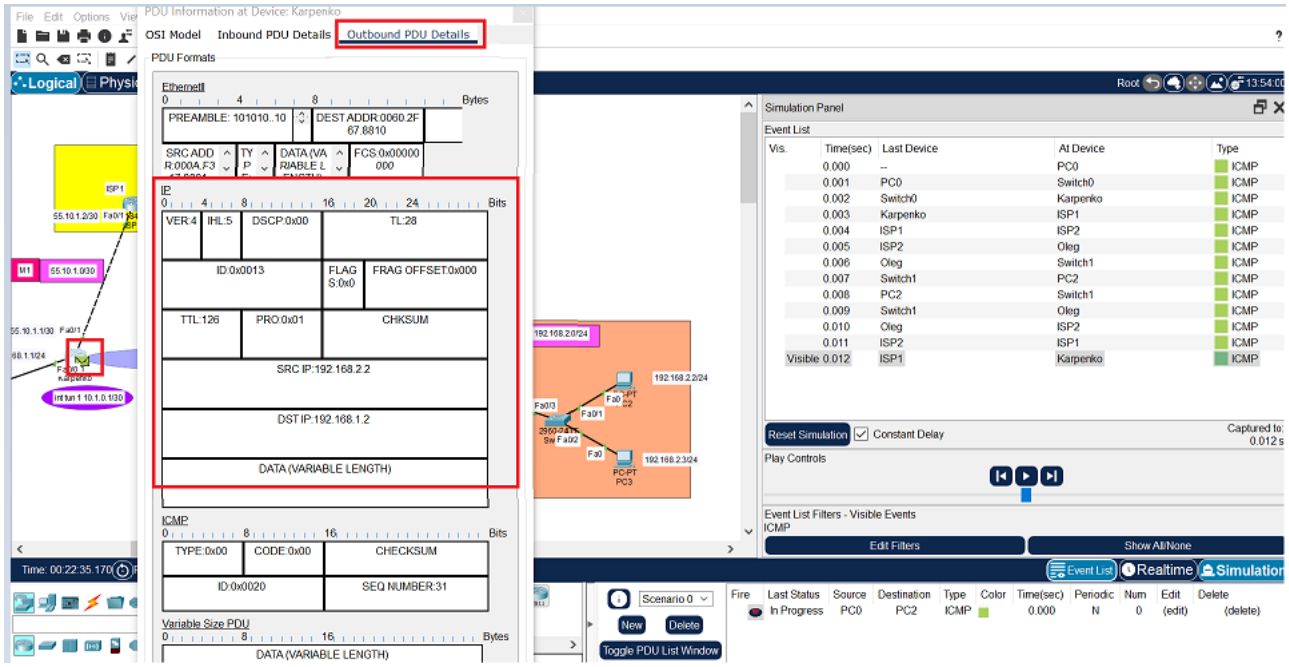


Рисунок 10.28 – Вихідний пакет на маршрутизаторі головного офісу

Натиснути ще два рази кнопку (Capture) і пакет з відповіддю досягне комп’ютера PC0 (рис. 10.29).

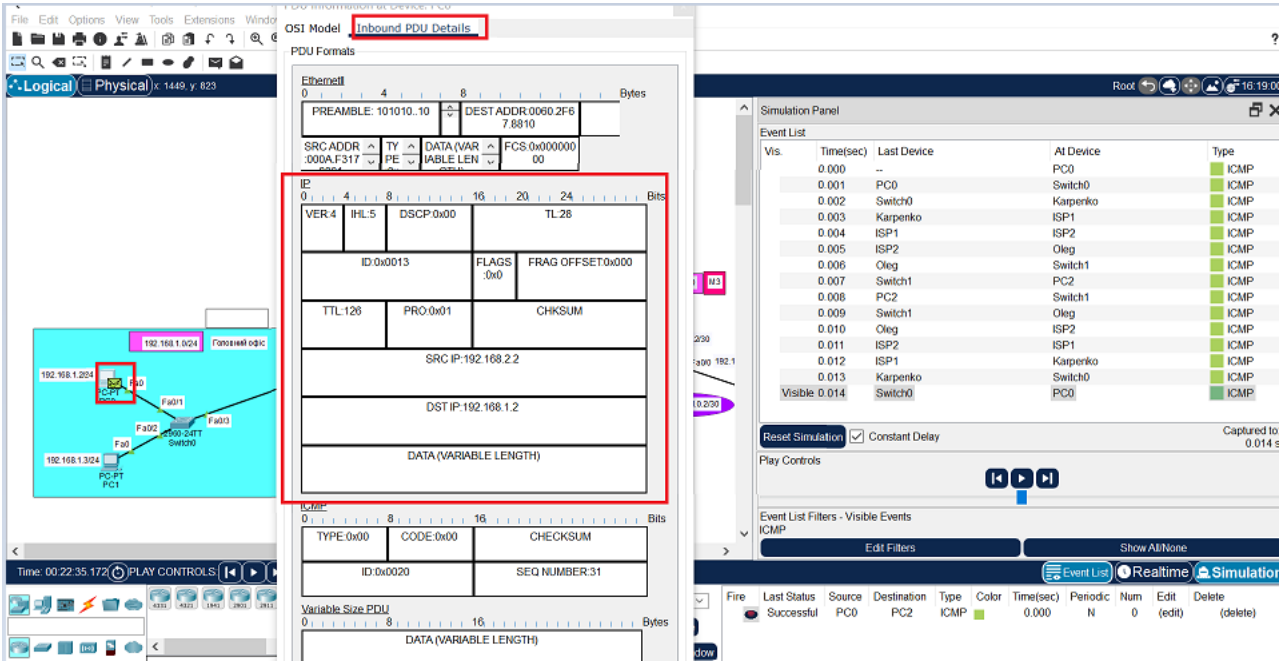


Рисунок 10.29 – Пакет з відповіддю досягнув комп'ютер PC0

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. 10.30-10.31). 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. 10.32-10.33).

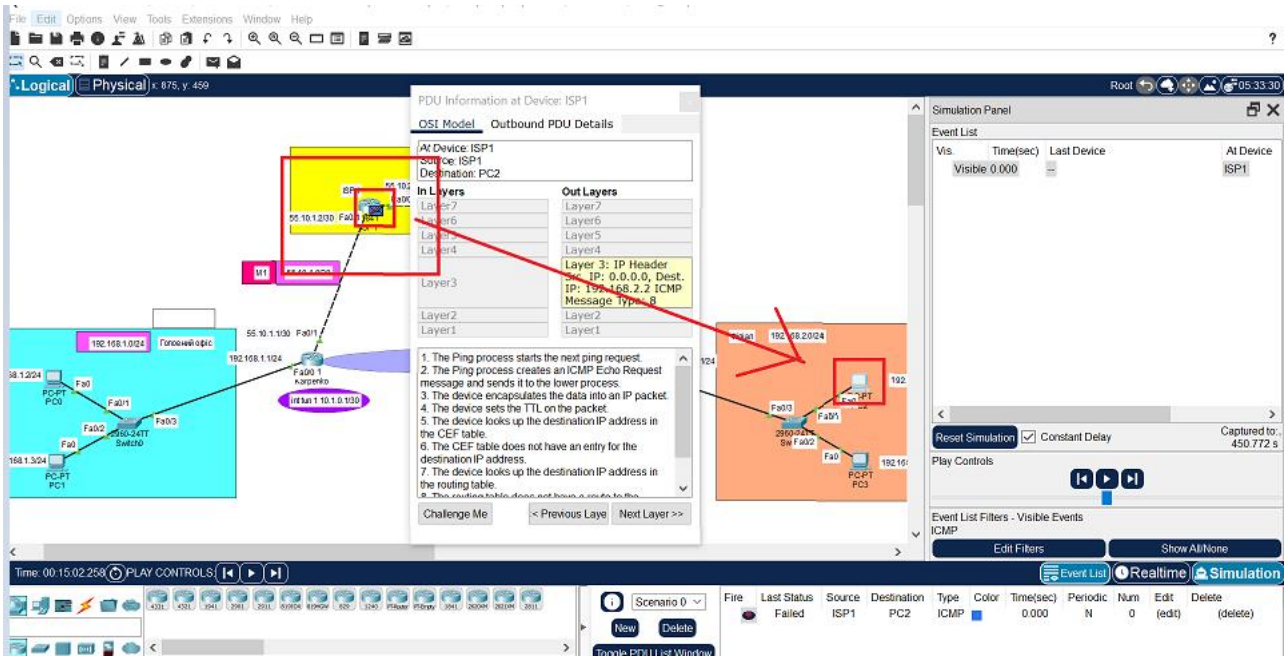


Рисунок 10.30 – Відправка пакету в мережу філіалу з маршрутизатора ISP1

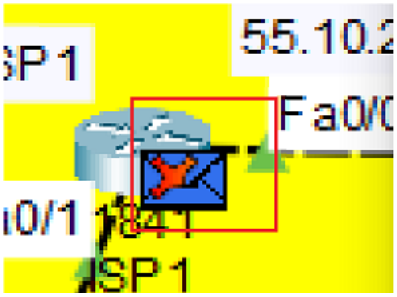


Рисунок 10.31 – На схемі отримаємо відображення пакету з перекресленим червоним хрестиком (тобто, що пакет не надсилається)

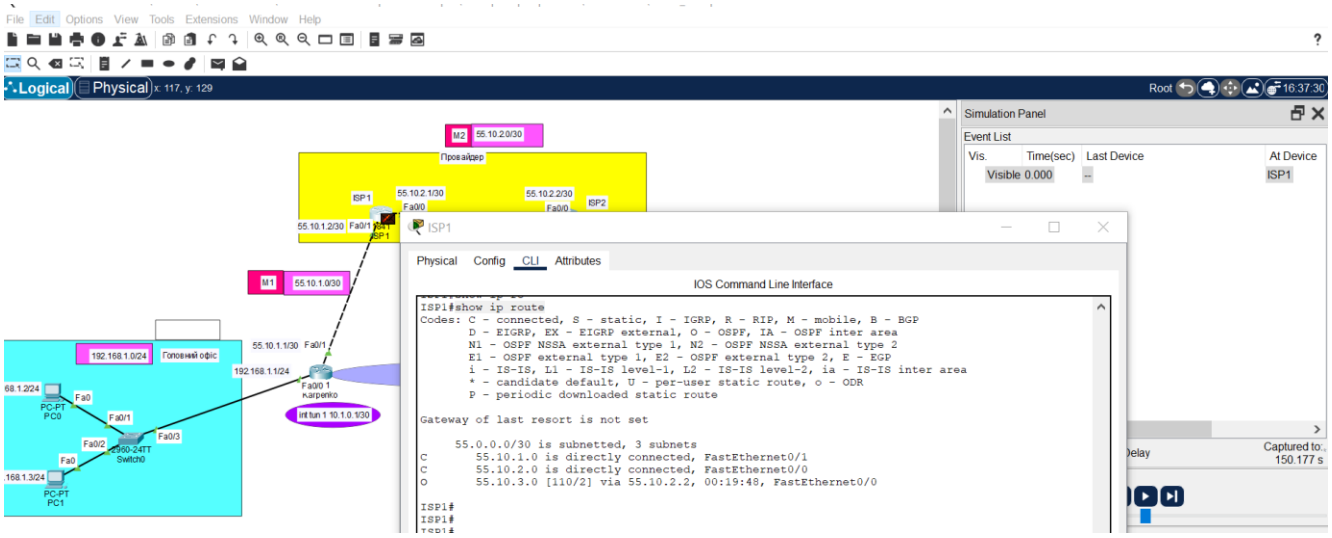


Рисунок 10.32 – Перегляд таблиці маршрутизації на маршрутизаторі ISP1

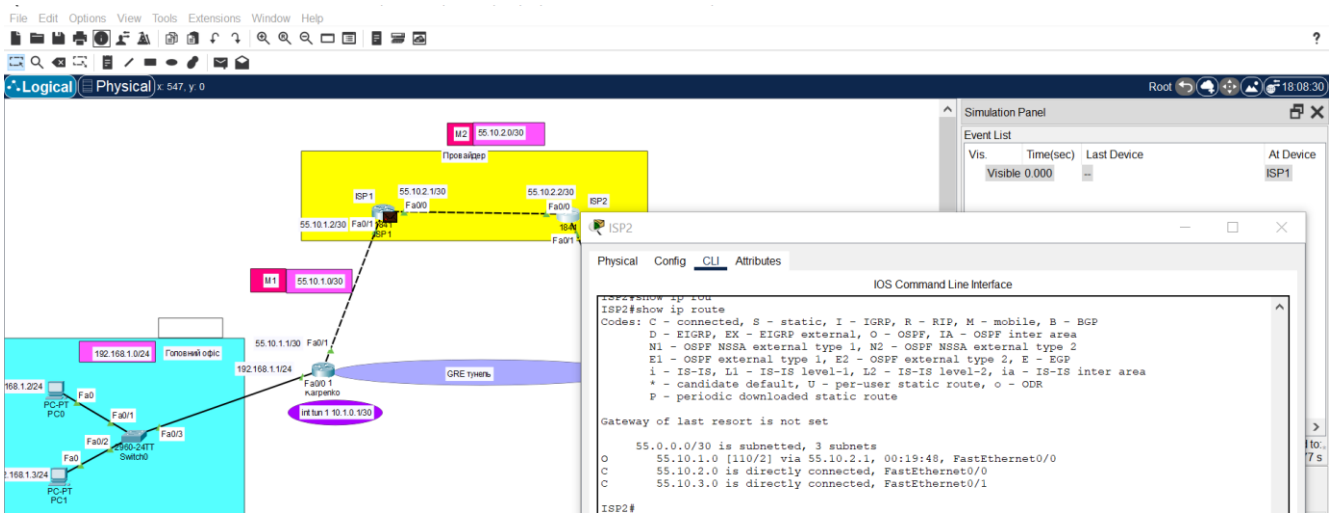


Рисунок 10.33 – Перегляд таблиці маршрутизації на маршрутизаторі ISP2

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

Практична робота 11
Active Directory у Windows Server 2025

Мета роботи: закріпити практичні навички встановлення та налаштування ролі «Доменні служби Active Directory» у середовищі Windows Server 2025, навчитися створювати та конфігурувати домен, додавати облікові записи користувачів і груп, а також здійснювати аналіз процесів реплікації між контролерами домену для забезпечення надійного функціонування корпоративної мережевої інфраструктури [18-21].

Хід роботи

Завдання 1. Створення та налаштування домену

Перед початком виконання завдань даної практичної роботи запустимо розгорнуту віртуальну машину Windows Server 2025 в середовищі Hyper-V, яка була створена в результаті виконання одного із завдань попередньої практичної роботи.

Після успішного запуску відкриваємо «Диспетчер серверів». Для того, щоб створити та налаштувати домен, встановимо нову роль для цього сервера. Тому натискаємо «Управління» – «Додати ролі та компоненти». І за допомогою майстра додавання ролей та компонентів встановлюємо нову роль – «Доменні служби Active Directory». Алгоритм додавання простий та зрозумілий і опрацьований нами детально в попередній практичній роботі (рис. 11.1).

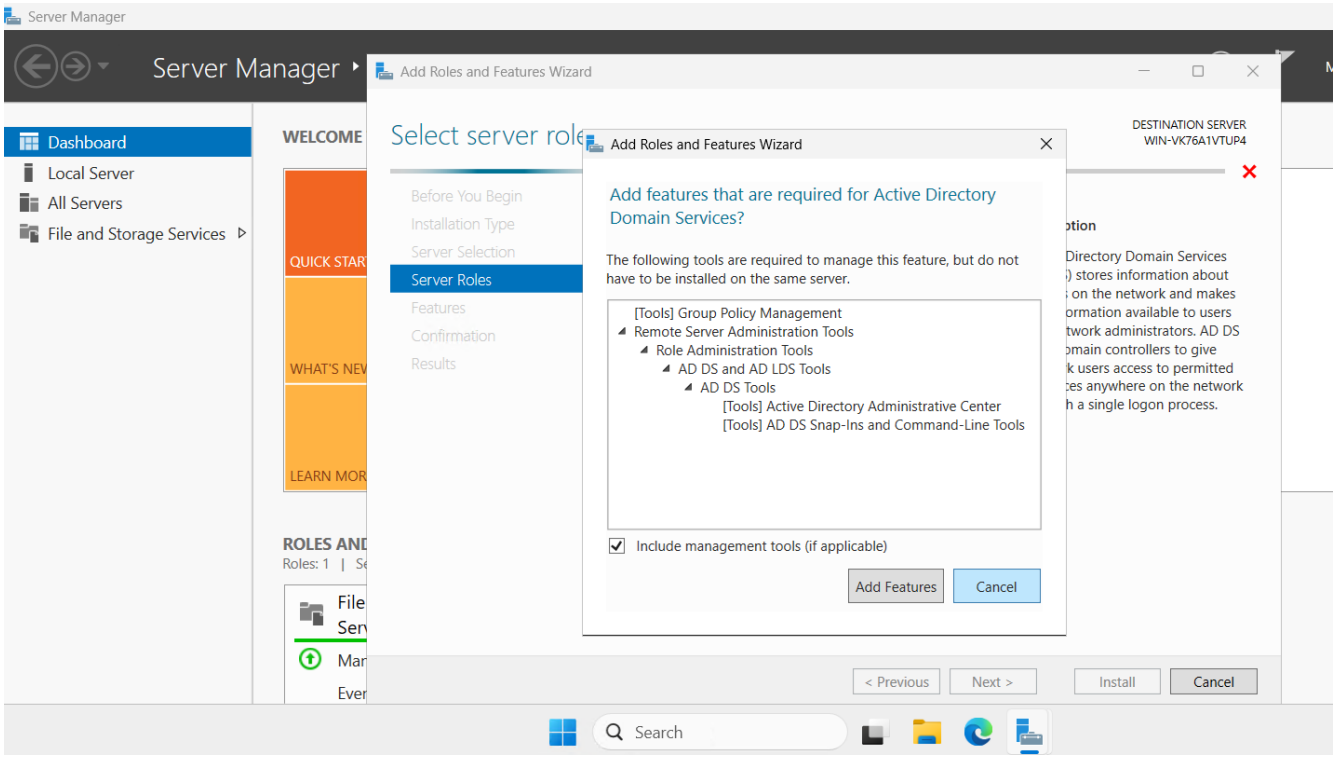


Рисунок 11.1 – Встановлення ролі «Доменні служби Active Directory»

Після вибору потрібної ролі, натискаємо «Далі» і так переключаємося до вікна підтвердження, де підтверджуємо встановлення вибраної ролі та чекаємо завершення цього процесу (рис. 11.2).

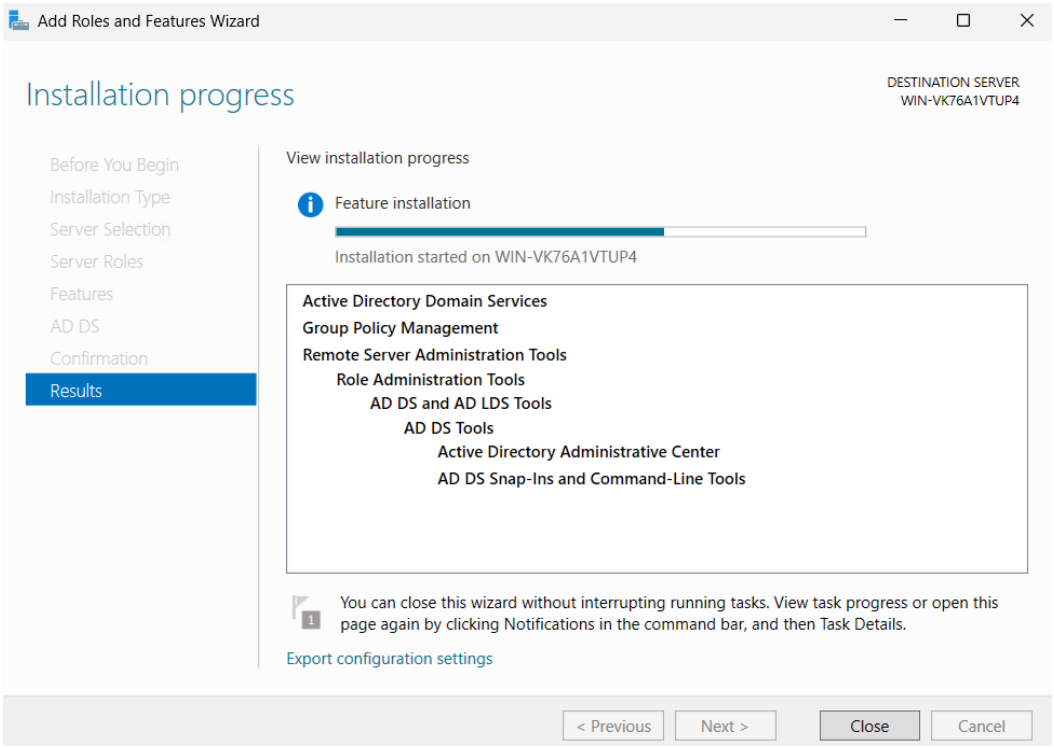


Рисунок 11.2 – Процес встановлення вибраних ролей та компонентів (ролі «Доменні служби Active Directory»)

Коли завершився процес встановлення вибраної ролі та компонентів, то з’явиться повідомлення «Підвищити роль цього сервера до рівня контролера домена» – натискаємо на нього (рис. 11.3).

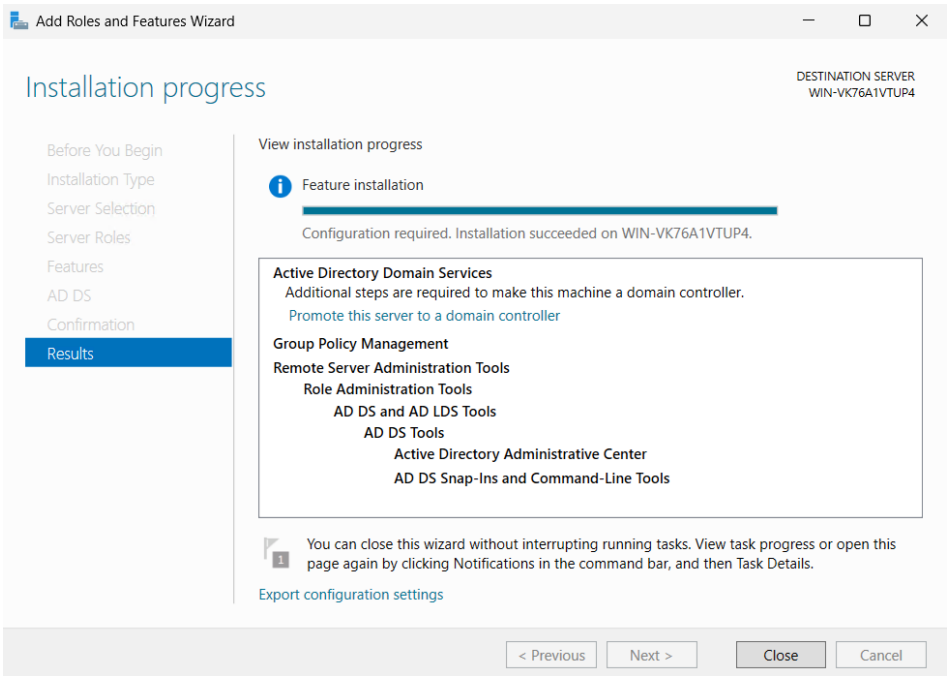


Рисунок 11.3 – Повідомлення «Підвищити роль цього сервера до рівня контролера домена»

Після натиснення відкривається «Майстер налаштування доменних служб Active Directory» (рис. 11.4).

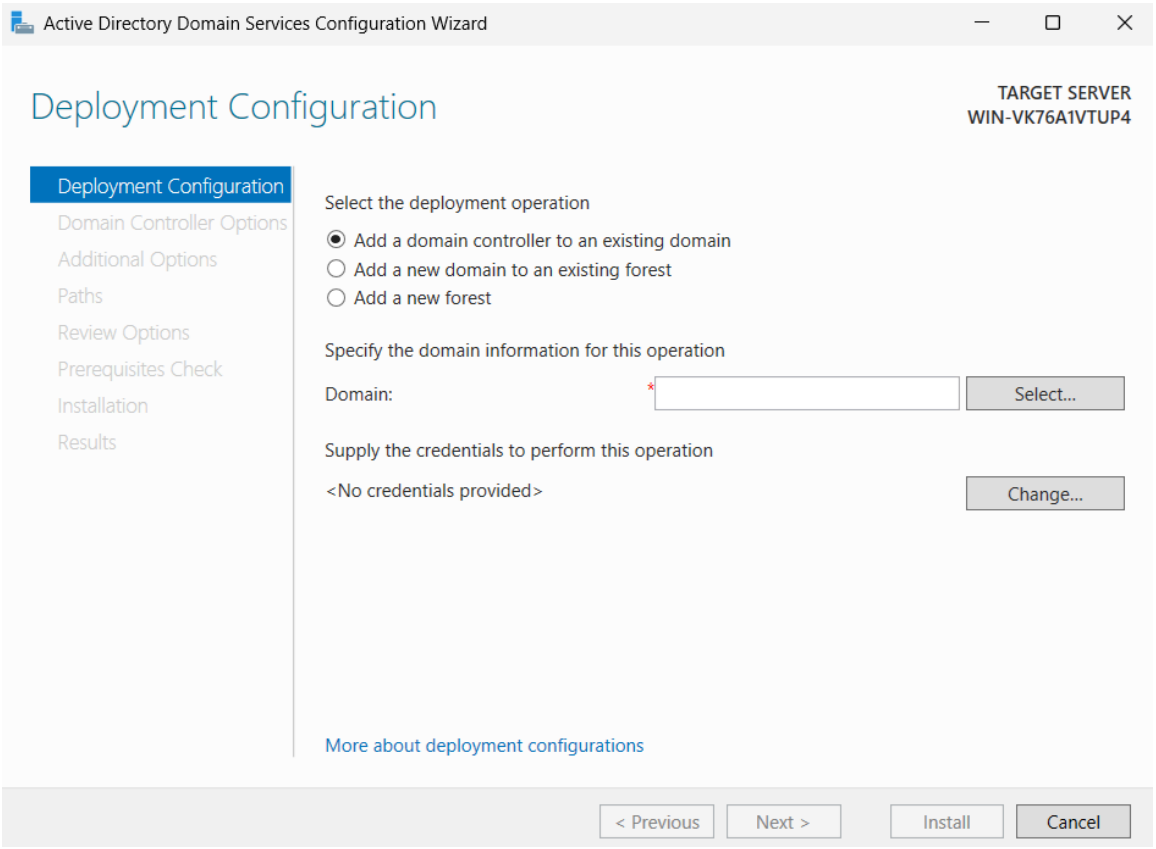


Рисунок 11.4 – «Майстер налаштування доменних служб Active Directory»

В цьому вікні є можливість обрати один з трьох варіантів:

«Додати контролер домена в існуючий домен» – використовується, якщо домен уже існує, і ви хочете додати ще один контролер.

«Додати новий домен в існуючий ліс» – якщо у нас уже є «ліс» (forest), і ми хочемо створити в ньому новий домен.

«Додати новий ліс» – використовується, коли створюється домен уперше, тобто ще немає ні «лісу», ні домену.

Оскільки, ми створюємо домен уперше, то натискаємо «Додати новий ліс» та вводимо назву домену. Потім натискаємо «Далі» (рис. 11.5).

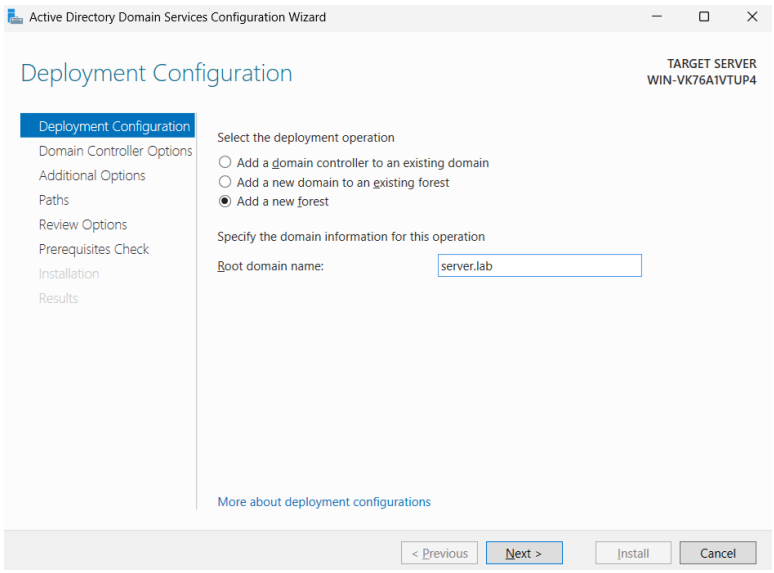


Рисунок 11.5 – Вибір «Додати новий ліс» та введення назви домену

В наступній вкладці вікна все залишаємо без змін, тільки вписуємо пароль для режиму відновлення служб каталогів (DSRM) (рис. 11.6).

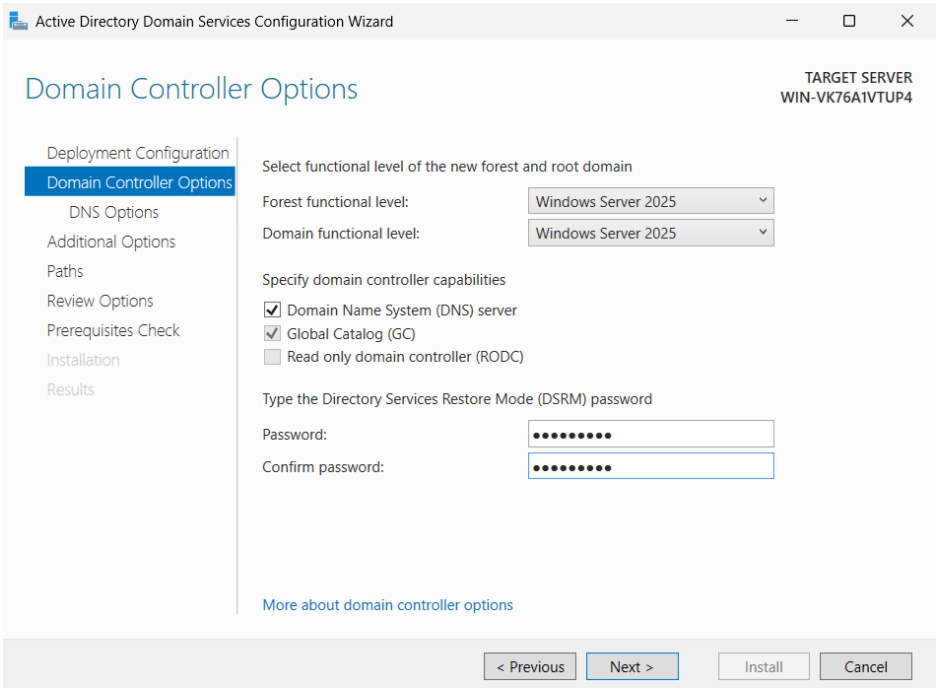


Рисунок 11.6 – «Параметри контролера домена»

У наступних вікнах «Параметри DNS» та «Додаткові параметри» просто натискаємо «Далі». На вкладці «Шляхи» теж залишаємо все без змін і з параметрами за-замовчуванням (рис. 11.7).

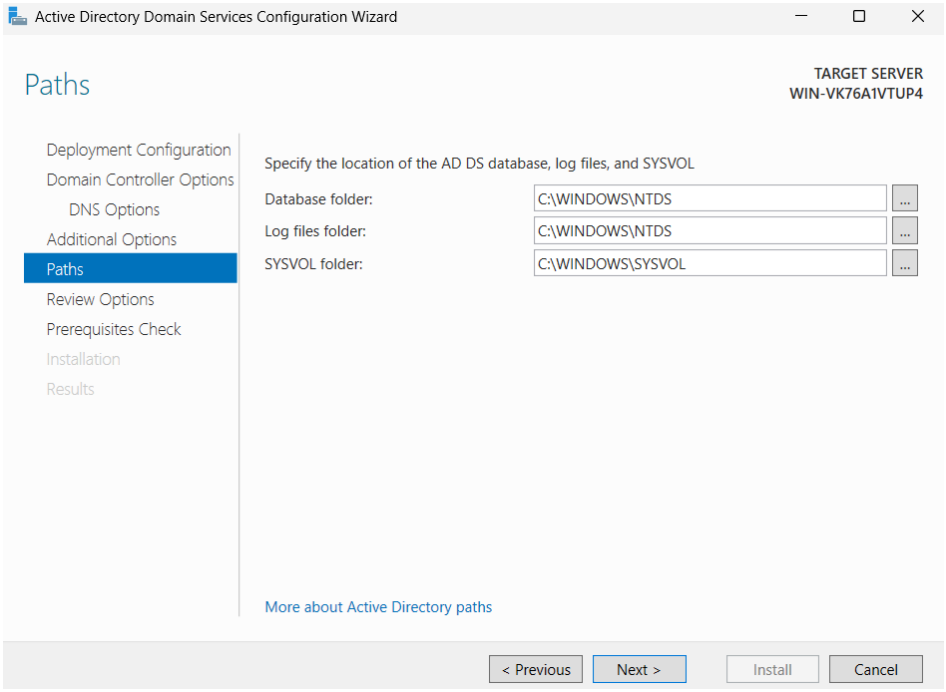


Рисунок 11.7 – Вкладка «Шляхи»

Після цього на вкладці «Переглянути параметри» перевіряємо введені дані. Якщо все вірно натискаємо «Далі». Після цього, якщо все відповідає

вимогам, відбувається встановлення. За успішним встановленням слідує перезавантаження сервера (рис. 11.8).

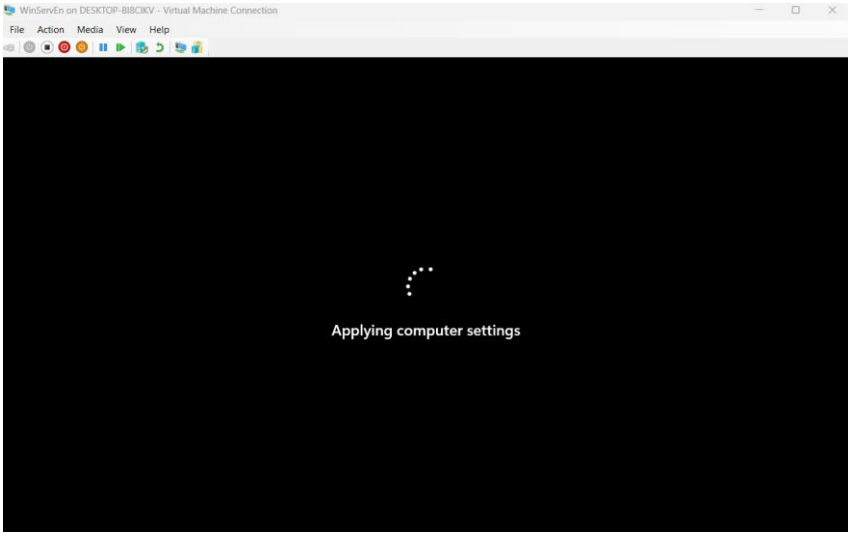


Рисунок 11.8 – Перезавантаження сервера

Після перезавантаження сервера, можемо зайти в «Диспетчер серверів», далі – «Інструменти», знайти там «Користувачі і комп'ютери Active Directory».

Якщо вікно відкривається і ми бачимо наш домен (наприклад, server.lab) з контейнерами – значить домен створений і сервер став контролером. Отже, створення та налаштування домену завершено.

Завдання 2. Додавання користувачів і груп

Для цього натискаємо «Диспетчер серверів» – «Інструменти» – «Користувачі та комп'ютери Active Directory» (рис. 11.9).

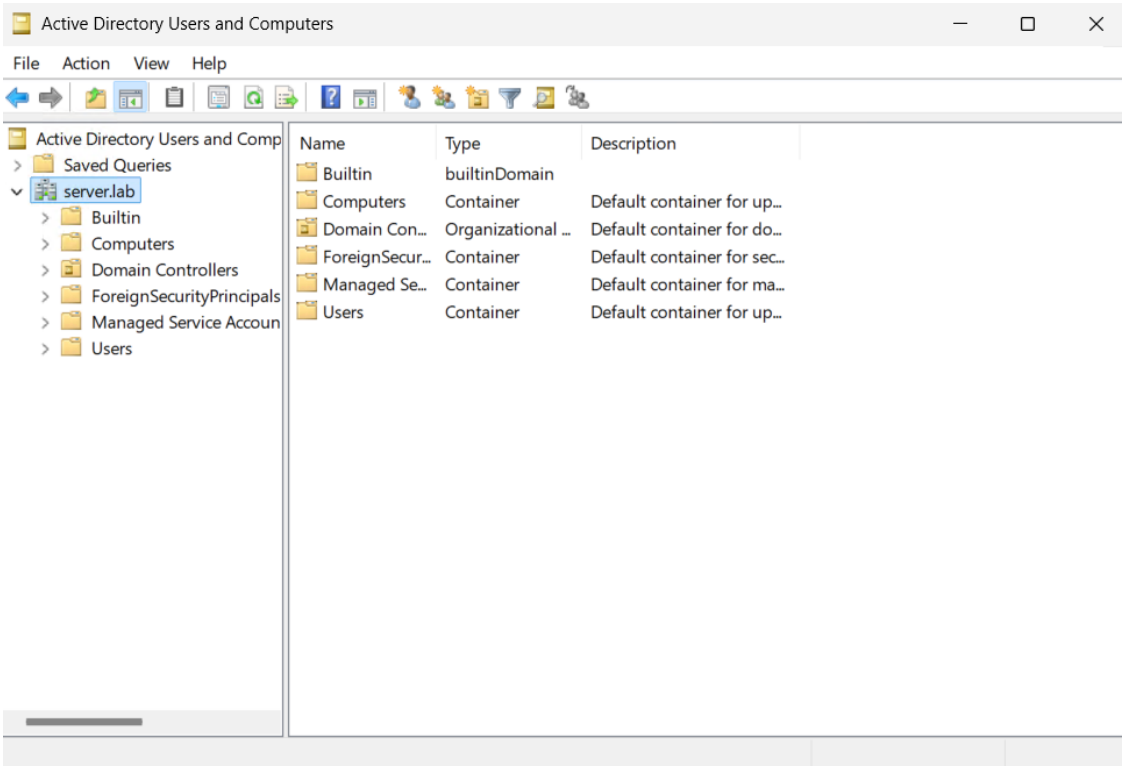


Рисунок 11.9 – Вікно «Користувачі та комп'ютери Active Directory»

Коли відкриється вікно, ми бачимо наш домен (server.lab) і стандартні контейнери:

Users (Користувачі) – тут знаходяться стандартні облікові записи та групи.

Computers (Комп'ютери) – сюди за замовчуванням потрапляють комп'ютери, приєднані до домену.

Domain Controllers (Контролери домена) – тут відображаються сервери з роллю контролера домену.

Щоб створити нового користувача можемо натиснути на піктограму «Створення нового користувача» або ж натиснути ПКМ по контейнеру «Users» – «Створити» – «Користувач» (рис. 11.10).

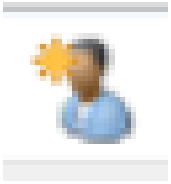


Рисунок 11.10 – Піктограма «Створення нового користувача»

Відкривається «Майстер створення нового користувача». Тут заповнюємо всі необхідні поля, такі, як «Ім'я», «Прізвище», «Ініціали» та найважливіше – «Ім'я входу користувача», коли це зроблено натискаємо «Далі» (рис. 11.11).

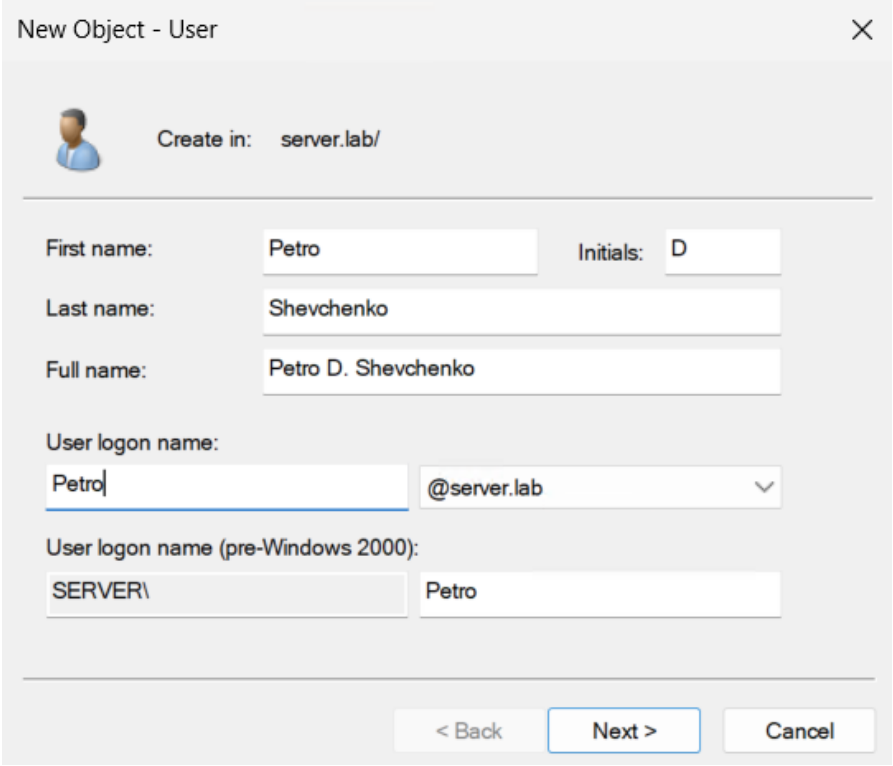


Рисунок 11.11 – Майстер створення нового користувача

На наступній вкладці відбувається налаштування пароля. Створюємо і записуємо новий пароль, повторюємо його та встановлюємо прапорець «Вимагати зміни пароля при наступному вході в систему» – це зумовлено

налаштуваннями безпеки. Інші прапорці залишаємо без змін в цьому випадку (рис. 11.12).

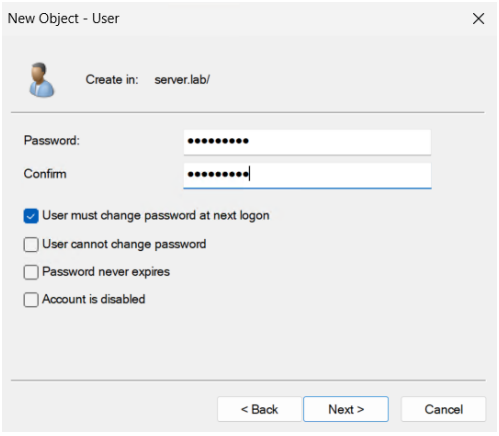


Рисунок 11.12 – Налаштування пароля для створюваного користувача

Далі натискаємо «Готово» – новий користувач створений.

Для створення групи користувачів алгоритм дій подібний – натискаємо відповідну піктограму або ПКМ по контейнеру «Users» – «Створити» – «Група» (рис. 11.13).

Рисунок 11.13 – Піктограма «Створення нової групи»

Відкривається «Майстер створення нової групи». Тут заповнюємо всі необхідні поля, такі, як «Ім’я групи», вибираємо область дій групи – «Локальна в домені» та тип групи – «Безпеки», коли це зроблено натискаємо «ОК» – нова група користувачів створена (рис. 11.14).

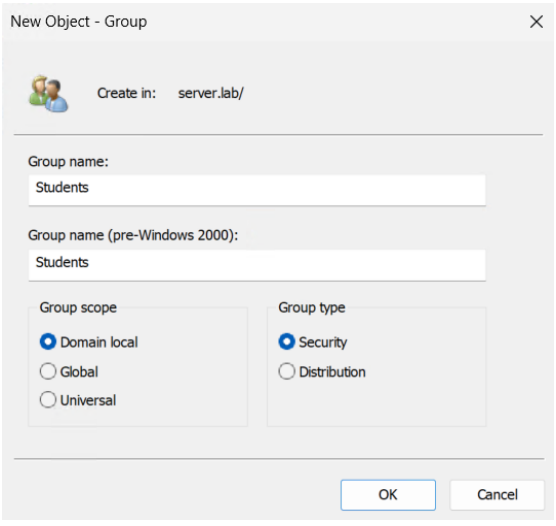


Рисунок 11.14 – Створення нової групи

Для того, щоб додати користувача до групи можна скористатися двома способами. Перший – натиснути на групу ПКМ, далі вибрати «Додати в групу» і у вікні, що відкрилося ввести ім'я користувача, що потрібно додати в цю групу і натиснути «ОК». Другий спосіб – зайти в контейнер «Користувачі», там знайти користувача, якого слід додати до групи, натиснути на нього ПКМ, вибрати «Властивості». У вікні властивостей, що відкрилося обрати «Член груп» – «Додати». Далі ввести назву групи і натиснути «ОК» (рис. 11.15).

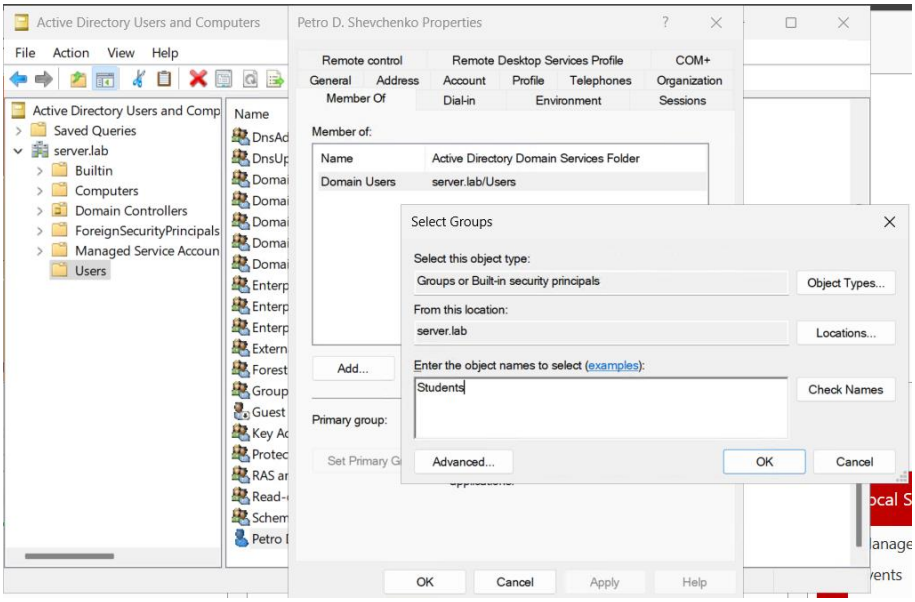


Рисунок 11.15 – Додавання користувача до групи

Після цього у вікні властивостей потрібно натиснути «Застосувати» і «ОК». В результаті цих дій користувач буде доданий до вказаної групи.

Завдання 3. Аналіз реплікації між контролерами домену

Для виконання цього завдання створюємо другу віртуальну машину Windows Server 2025, процес описаний в першій практичній роботі, додаємо роль Active Directory. Приєднуємо її до існуючого домену як додатковий контролер (опція Add a domain controller to an existing domain).

Після цього на основній (першій) машині відкриваємо «Диспетчер серверів», переходимо до «Інструменти» – «Сайти і служби Active Directory».

У дереві бачимо наш сайт за замовчуванням: Default-First-Site-Name (рис. 11.16).

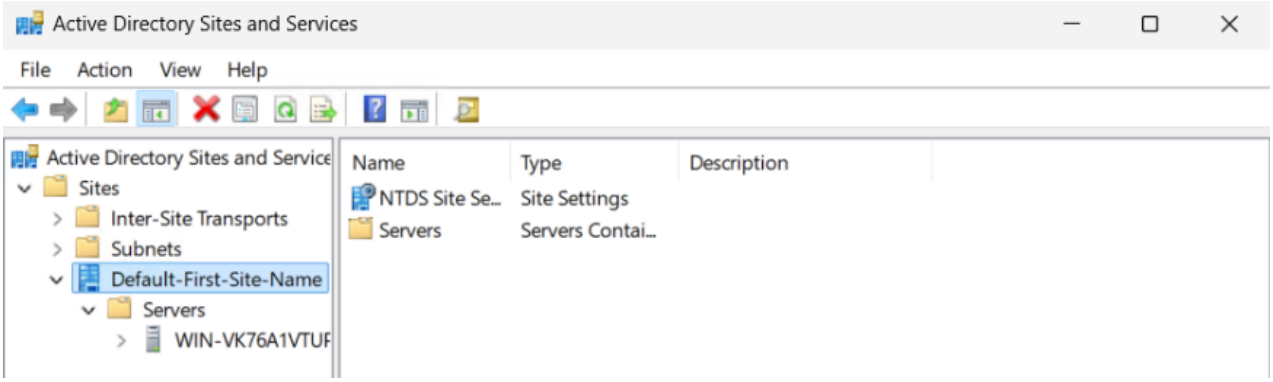


Рисунок 11.16 – Сайти і служби Active Directory

Розгортаємо вузол – «Servers» – бачимо список наших контролерів домену (DC1, DC2). Після цього для перегляду з’єднання реплікації розгортаємо сервер – «NTDS Settings». У правій частині бачимо автоматично створені з’єднання (зв’язки реплікації), це вказує, з ким контролер обмінюється даними.

Для детального аналізу виконуємо примусову реплікацію. Для цього натискаємо ПКМ на з’єднанні, потім «Виконати реплікацію зараз», підтверджуємо дію.

Якщо реплікація успішна, отримуємо повідомлення «Active Directory Domain Services has replicated the connections».

Практична робота 12
Групові політики у Windows Server 2025

Мета роботи: ознайомитися з принципами функціонування та адміністрування групових політик у середовищі Windows Server 2025, набути практичних навичок налаштування політик безпеки, зокрема параметрів паролів та обмеження доступу до зовнішніх носіїв, а також опанувати методи діагностики і усунення помилок при застосуванні групових політик у доменній інфраструктурі [22-27].

Хід роботи

Завдання 1. Налаштування політик паролів

Перед початком виконання завдань даної практичної роботи запустимо розгорнуту віртуальну машину Windows Server 2025 в середовищі Hyper-V, яка була створена.

Далі відкриваємо «Диспетчер серверів». Натискаємо «Інструменти» – «Керування груповою політикою» – таким чином відкриваємо інструмент управління політиками (рис. 12.1).

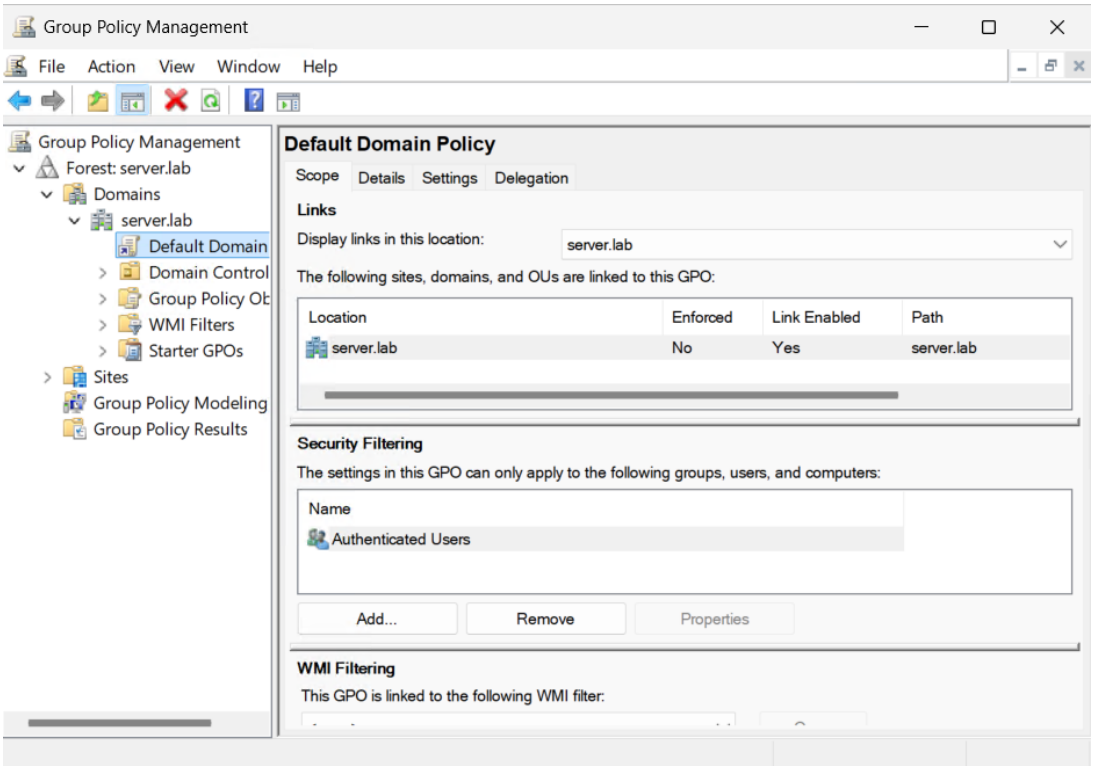


Рисунок 12.1 – Відкрите вікно «Керування груповою політикою»

Після цього відкриваємо дерево зліва: розгортаємо наш домен, вибираємо об’єкт Default Domain Policy (Політика за-замовчуванням для домена). Це саме та політика, яка застосовується для всіх користувачів домену, якщо ми її змінюємо. І далі, щоб налаштувати політику паролів клацаємо правою кнопкою миші по «Default Domain Policy» – «Змінити». Внаслідок цього відкривається редактор групових політик (рис. 12.2).

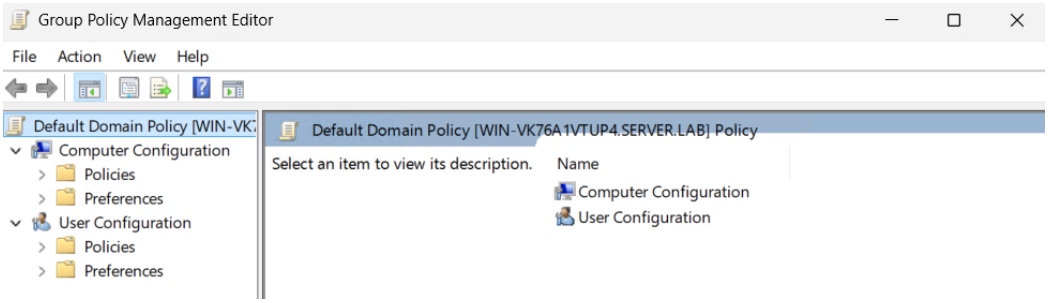


Рисунок 12.2 – Відкрите вікно «Редактор управління груповими політиками»

Далі у редакторі вибираємо «Конфігурація комп'ютера», в наступній вкладці редактора обираємо пункт «Політики» (рис. 12.3).

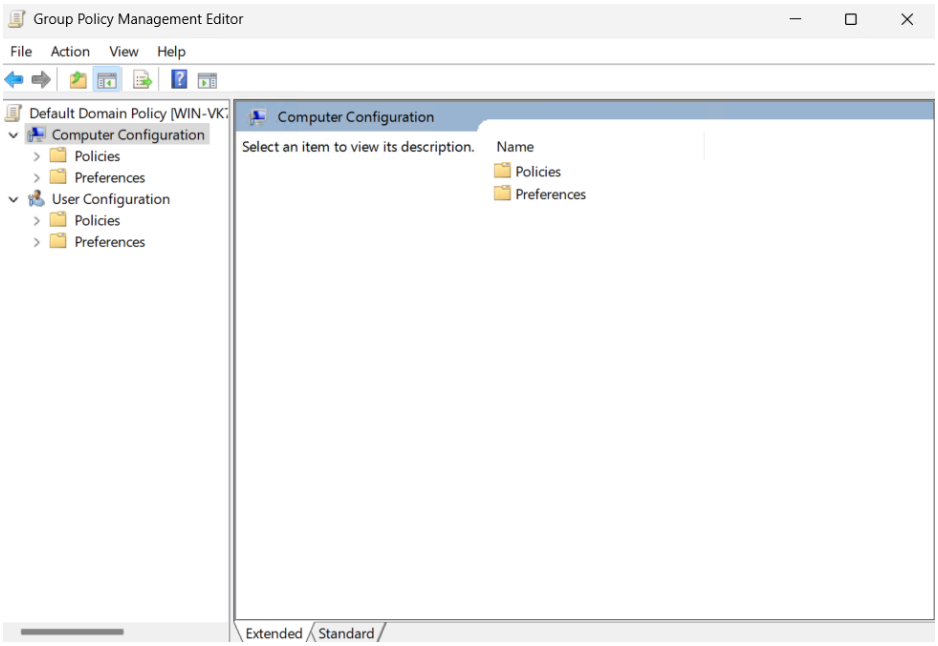


Рисунок 12.3 – Вибір пункту меню «Політики»

Згодом, у новій вкладці обираємо «Конфігурація Windows» (рис. 12.4).

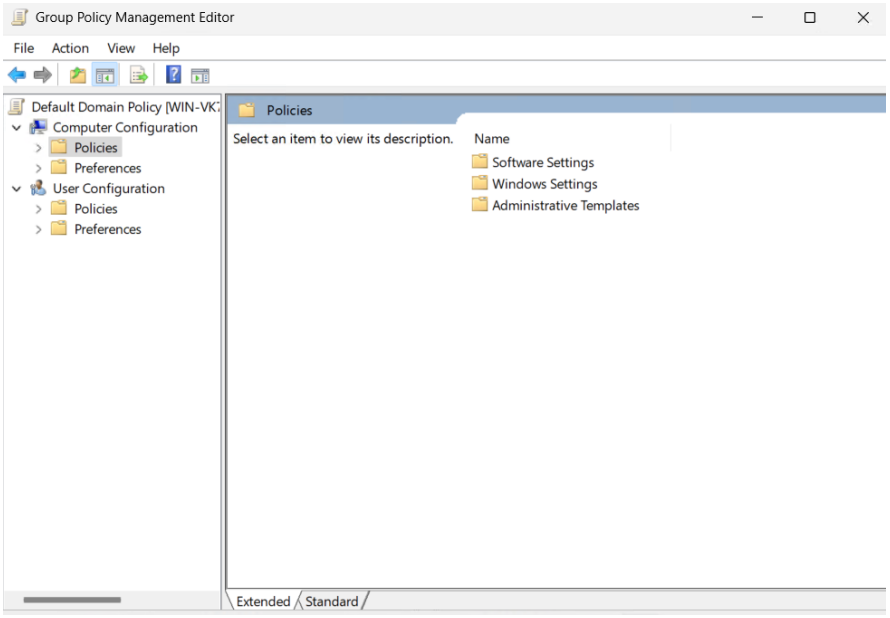


Рисунок 12.4 – Вибір пункту меню «Конфігурація Windows»

Після цього, у вкладці, що відрилася обираємо «Параметри безпеки» (рис. 12.5).

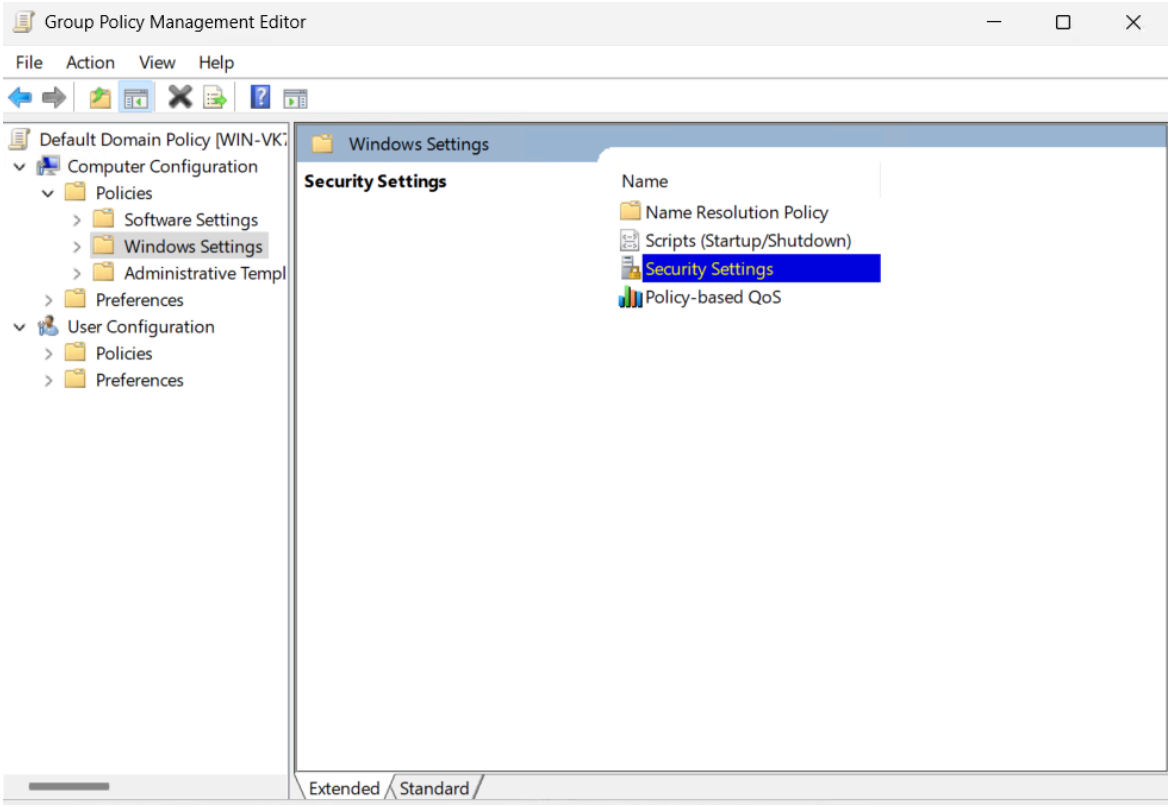


Рисунок 12.5 – Вибір пункту меню «Параметри безпеки»

Далі вибираємо пункт «Політики облікових записів» (рис. 12.6).

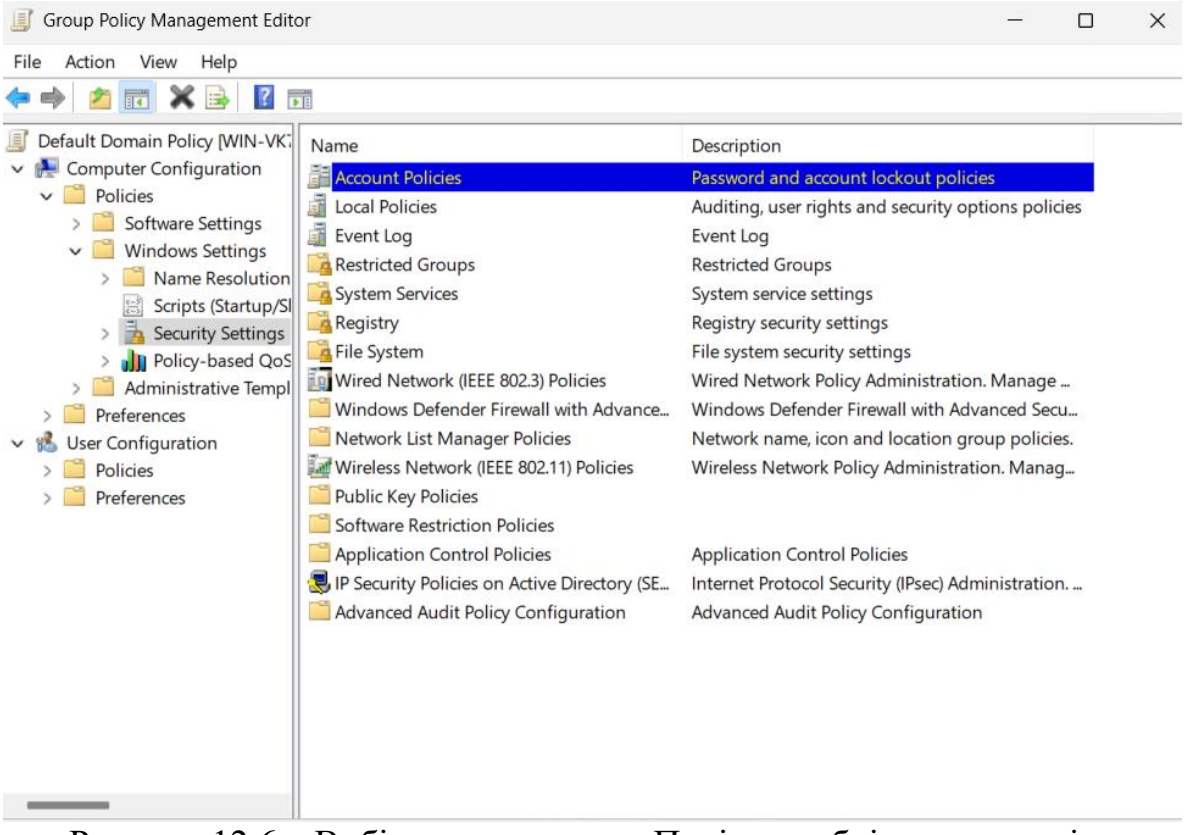


Рисунок 12.6 – Вибір пункту меню «Політики облікових записів»

Після цього відкривається вкладка з потрібним нам для налаштування пунктом меню і видом політик – «Політика паролів» (рис. 12.7-12.8).

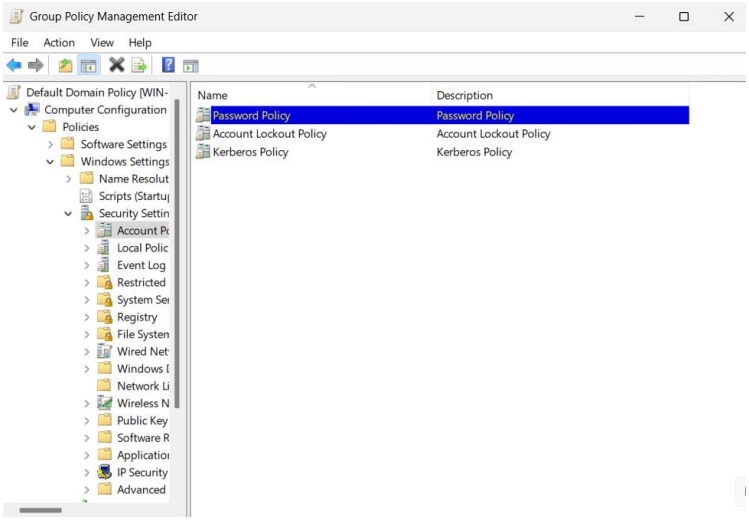


Рисунок 12.7 – Вибір пункту меню «Політика паролів»

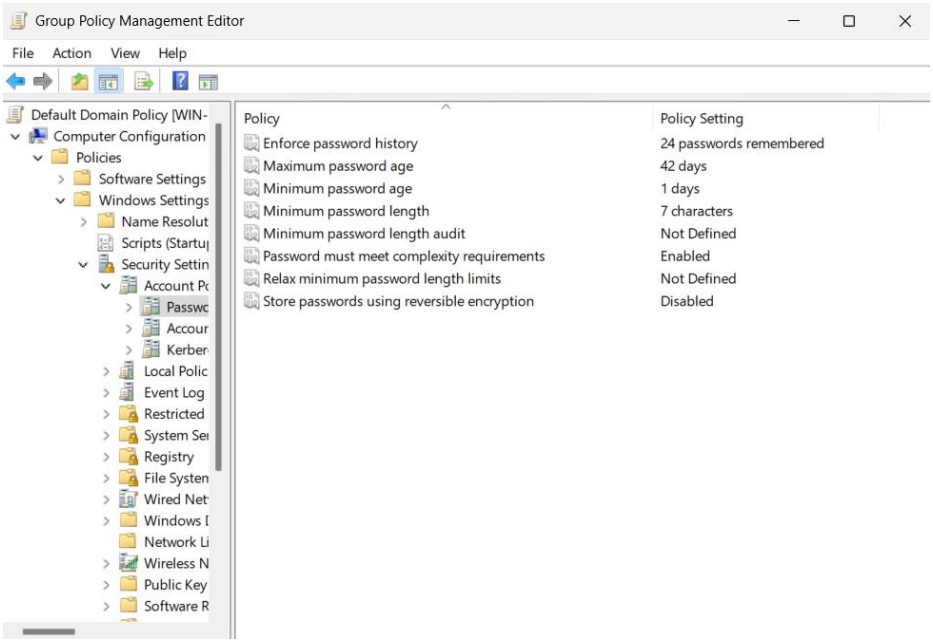


Рисунок 12.8 – Вікно налаштування політики паролів

Тут ми бачимо кілька ключових параметрів:

Вести журнал паролів – скільки паролів зберігається.

Максимальний термін дії пароля – як часто потрібно міняти пароль.

Мінімальний термін дії пароля – через який час після зміни пароль можна змінити знову.

Мінімальна довжина пароля – мінімальна кількість символів.

Пароль повинен відповідати вимогам – вимагає використання великих, малих літер, цифр та символів.

Зберігати паролі використовуючи реверсивне шифрування – даний параметр стосується безпеки та типу шифрування паролів.

Налаштування політики паролів, наприклад, здійснюємо наступним чином: мінімальна довжина пароля – 8 символів; термін дії пароля – 30 днів; вести журнал паролів – 5 останніх; складність пароля – Вимкнено.

Для налаштування певного пункту політики два рази натискаємо на нього лівою кнопкою миші (рис. 12.9-12.10).

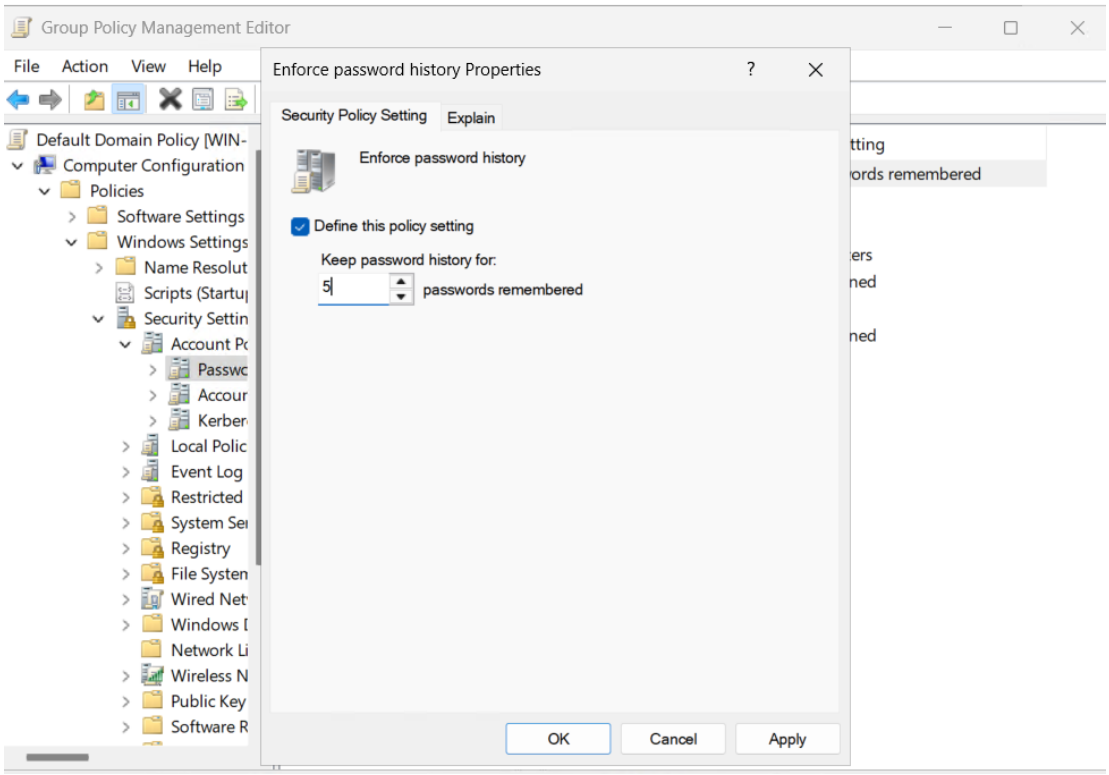


Рисунок 12.9 – Редагування значення пункту «Вести журнал паролів» в редакторі політик

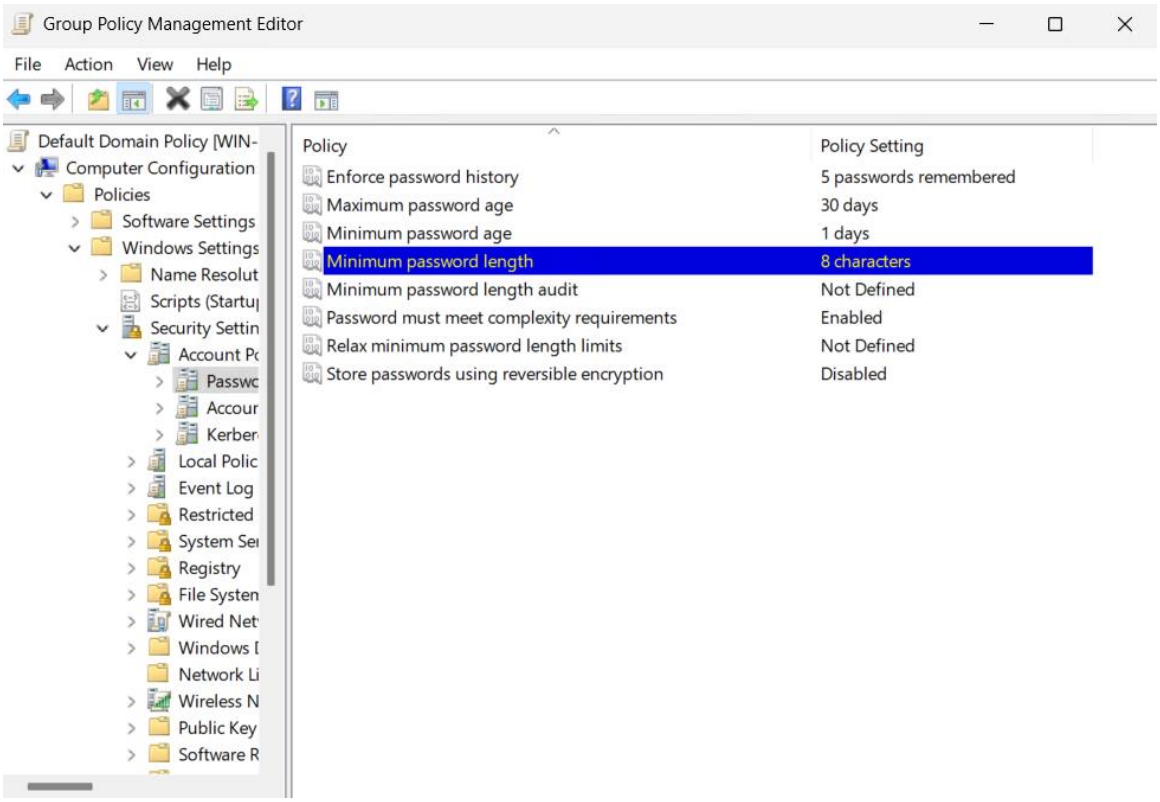


Рисунок 12.10 – Налаштована згідно завдання політика паролів

Коли налаштування проведено закриваємо «Редактор управління груповими політиками». Далі у середовищі Windows PowerShell запускаємо gpupdate /force, щоб зміни вступили в силу (рис. 12.11).

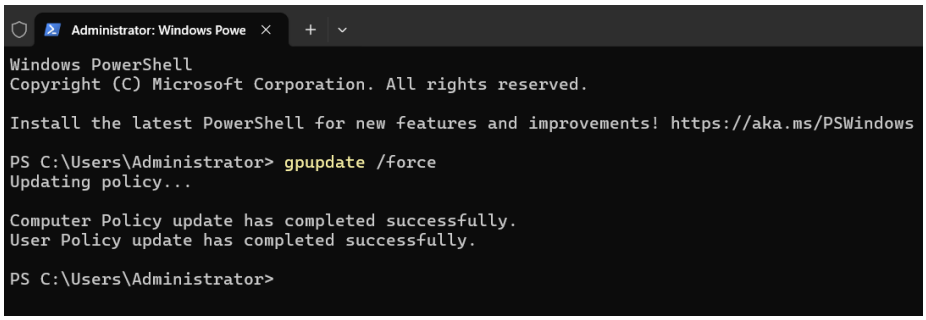


Рисунок 12.11 – Застосування gpupdate /force в середовищі Windows PowerShell

Для того, щоб переконатися в тому, що зміни вступили в силу знову відкриваємо налаштування політики паролів та перевіряємо значення відповідних параметрів. В результаті перевірки переконуємось у правильності здійснених налаштувань.

Завдання 2. Обмеження доступу до USB-носіїв

Для налаштування цієї опції також слід скористатися редактором групових політик. Для цього, як і в попередньому завдання заходимо в нього.

Якщо ми хочемо застосувати обмеження для всіх користувачів домену – редагуємо Default Domain Policy.

Якщо для певної групи або OU (організаційного підрозділу) – створюємо нову політику (натискаємо на назву домену ПКМ та вибираємо «Створити об’єкт групової політики в цьому домені та зв’язати його…») та прив’язуємо її до OU та дотримуємося подальших інструкцій майстра.

У редакторі політик йдемо шляхом: «Конфігурація комп’ютера» – «Політики» – «Адміністративні шаблони» – «Система» – «Доступ до знімних запам’ятовуючих пристроїв» (рис. 12.12-12.13).

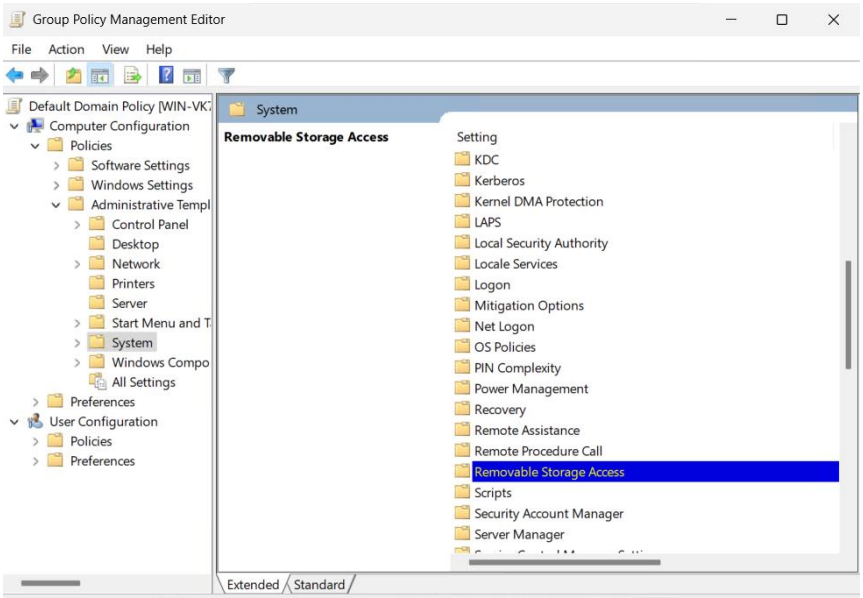


Рисунок 12.12 – Вибір пункту меню «Доступ до знімних запам’ятовуючих пристроїв»

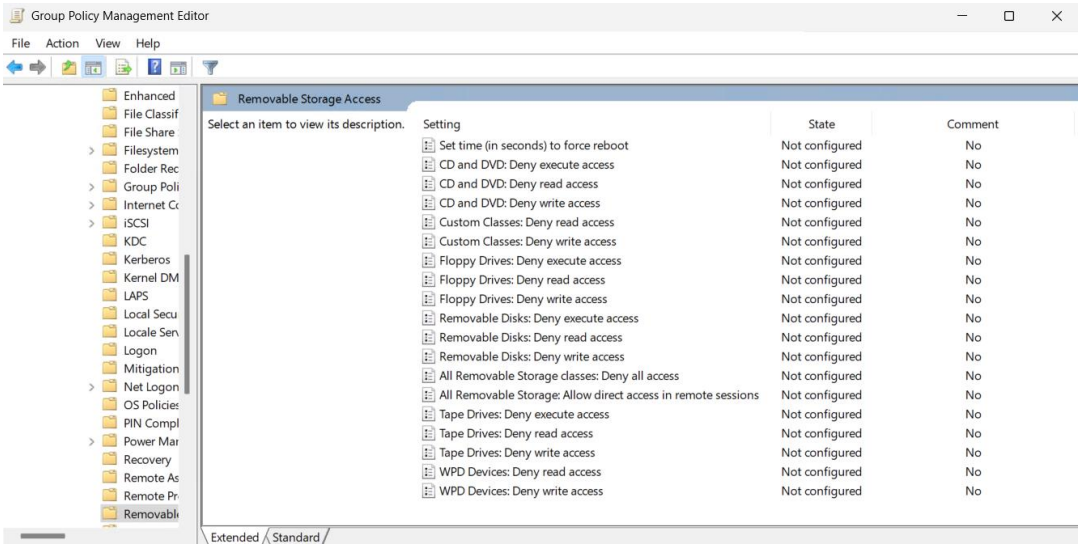


Рисунок 12.13 – Вікно налаштування політик щодо знімних запам’ятовуючих пристроїв

У вікні налаштування політик щодо знімних запам’ятовуючих пристроїв бачимо список параметрів для різних типів пристроїв: CD/DVD, USB-носії, зовнішні диски та інші подібні пристрої.

Ми можемо керувати як читанням, так і записом, вмикаючи та вимикаючи ці параметри для конкретного типу знімних пристроїв.

Для обмеження доступу до USB-носіїв вмикаємо політику «Знімні диски: заборонити читання» – «Увімкнути», а також вмикаємо політику «Знімні диски: заборонити запис» – «Увімкнути». Це означає, що користувачі не зможуть ані читати, ані записувати дані з USB-носіїв (рис. 12.14-12.15).

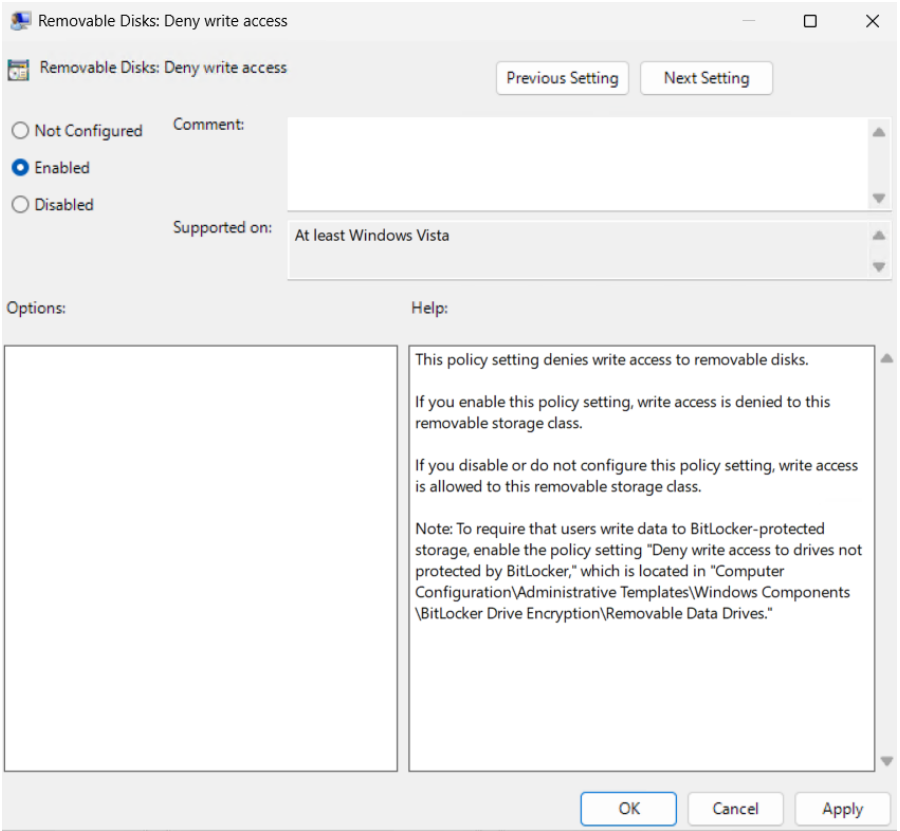


Рисунок 12.14 – Ввімкнення політики «Знімні диски: заборонити запис»

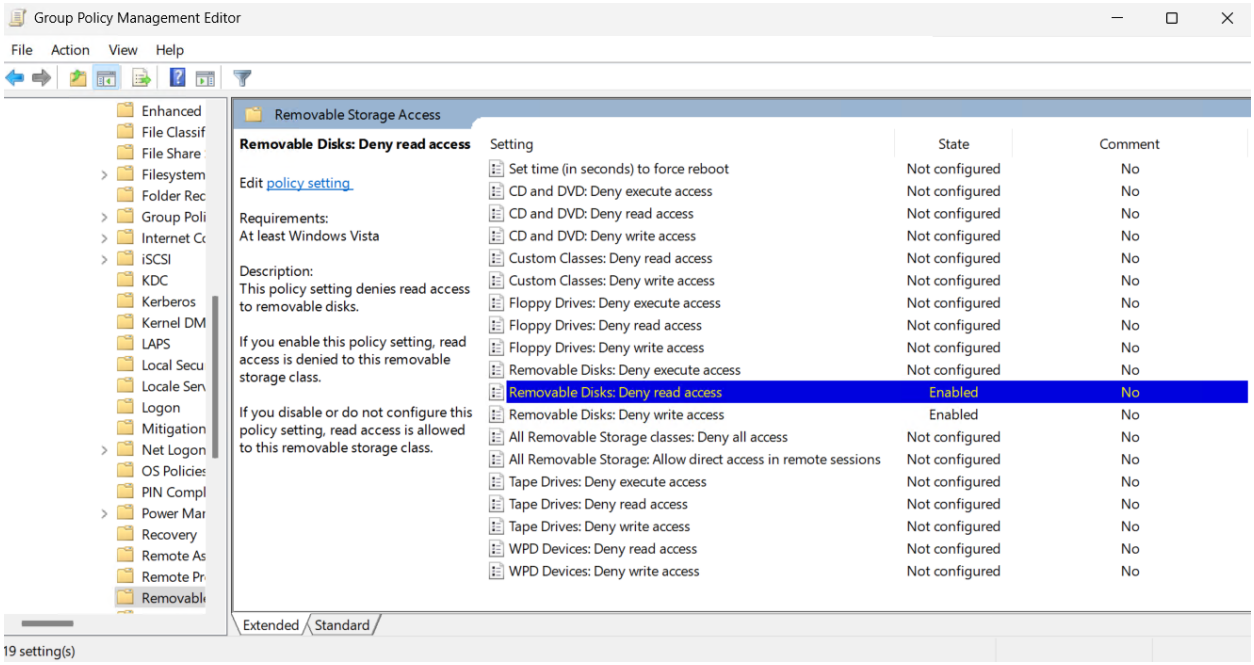


Рисунок 12.15 – Налаштована політика щодо знімних пристроїв для обмеження доступу до USB-носіїв

Коли налаштування проведено закриваємо «Редактор управління груповими політиками». Далі у середовищі Windows PowerShell запускаємо gpupdate /force, щоб зміни вступили в силу.

Для того, щоб переконатися в тому, що зміни вступили в силу знову відкриваємо налаштування політики знімних запам'ятовуючих пристроїв та перевіряємо значення відповідних параметрів політики. В результаті перевірки переконуємось у виконанні здійснених налаштувань.

Завдання 3. Діагностика помилок групових політик

Для діагностики, аналізу та перевірки групових політик є кілька інструментів, які можна застосувати.

Перше – це використання оснастки RSoP (Resultant Set of Policy). Для того, щоб застосувати її натискаємо Win + R та вводимо rsop.msc, натискаємо Enter. В результаті відкривається вікно Resultant Set of Policy (рис. 12.16).

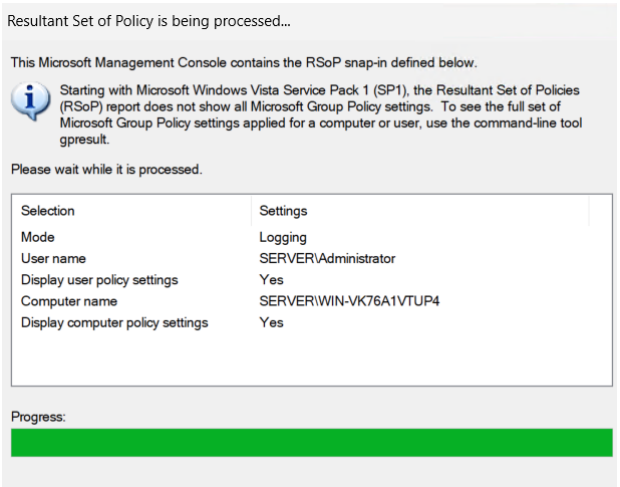


Рисунок 12.16 – Вікно «Resultant Set of Policy»

Система проводить збір інформації та показує нам, які саме політики застосувалися до користувача та комп'ютера та які параметри політик активні. Якщо політика не застосувалася, біля неї буде відображено помилку або попередження.

Наступний інструмент – «Результати групових політик» у «Менеджері управління груповими політиками». Ми відкриваємо «Керування груповими політиками» у «Менеджері серверів». Далі у дереві ліворуч розгортаємо вузол нашого домену. Клацаємо правою кнопкою миші на «Результати групової політики», вибираємо «Майстер результатів групових політик». Запускається майстер, де ми обираємо комп'ютер і користувача, для яких хочемо перевірити застосування політик.

Після завершення майстер формує звіт, про те, які політики застосовані, які були заблоковані та, що найважливіше чи виникли конфлікти між політиками (рис. 12.17-12.19).

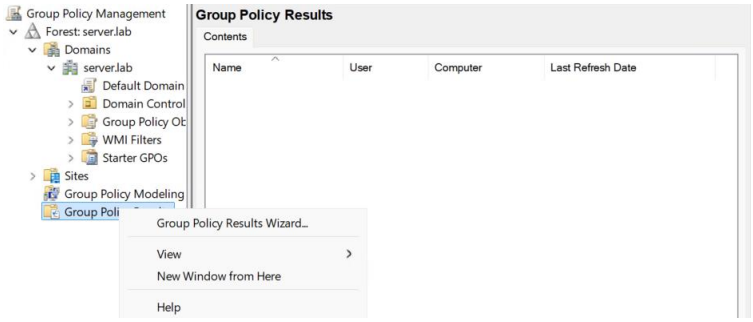


Рисунок 12.17 – Відкриття «Майстра результатів групових політик»

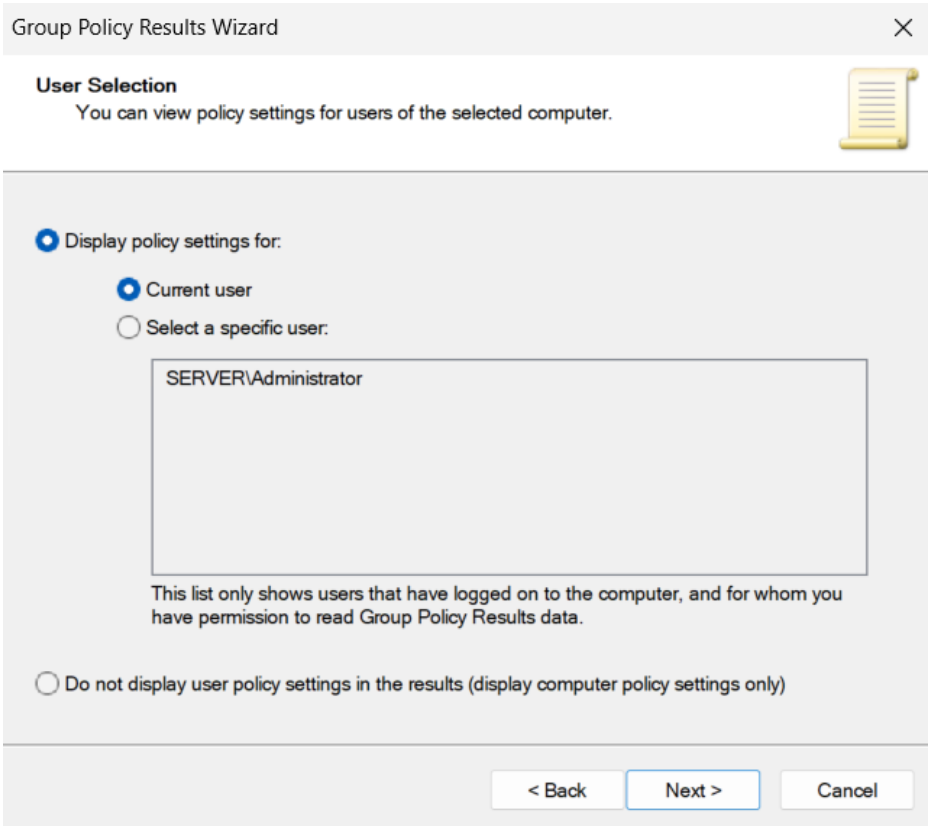


Рисунок 12.18 – Вибір користувача, щодо якого буде створено звіт використання групових політик

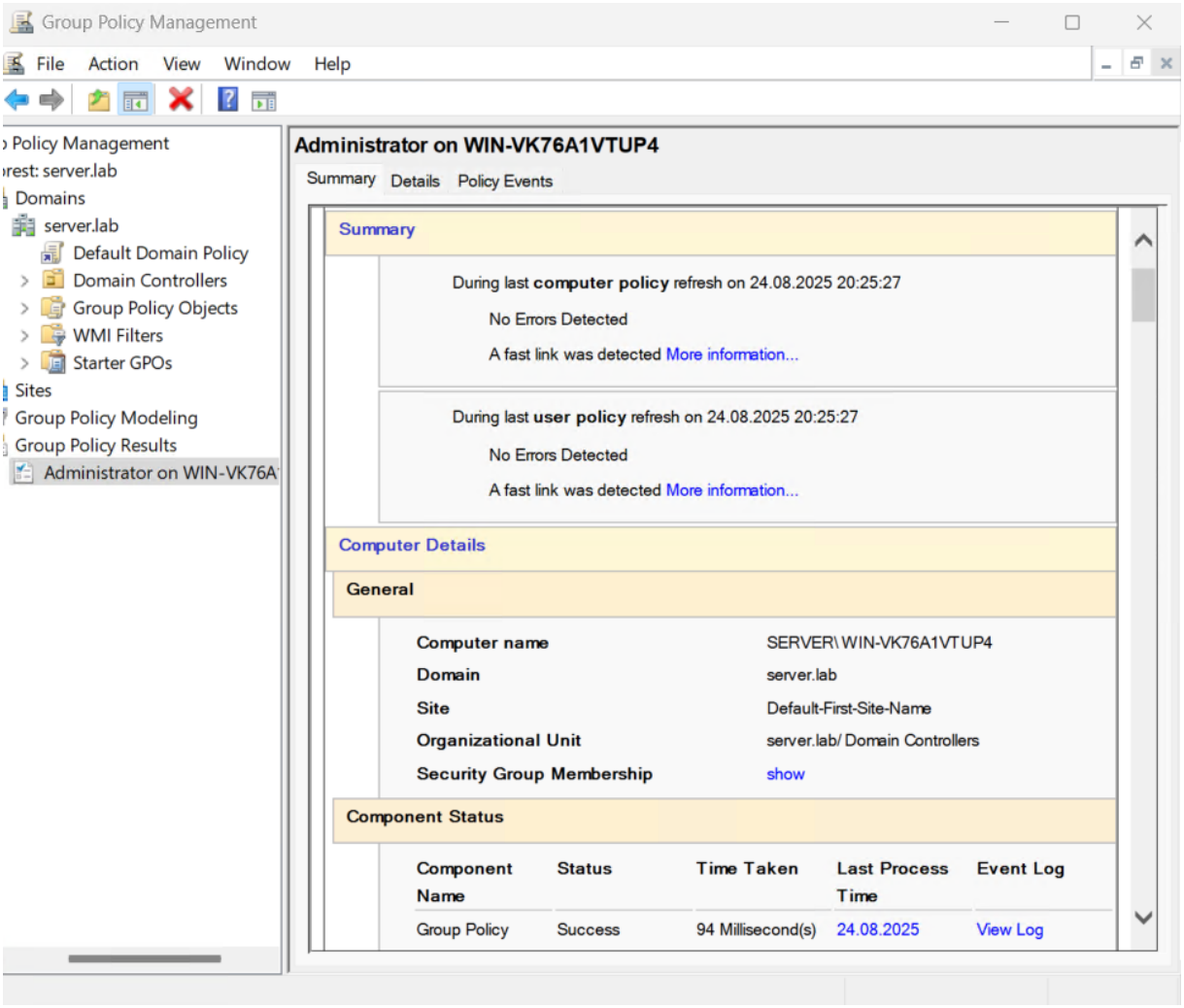


Рисунок 12.19 – Створений звіт використання групових політик

Також можна застосувати «Журнал подій» («Event Viewer») для діагностики роботи та помилок групових політик. Ми відкриваємо «Пуск» – «Адміністративні інструменти» – «Журнал подій» (рис. 12.20).

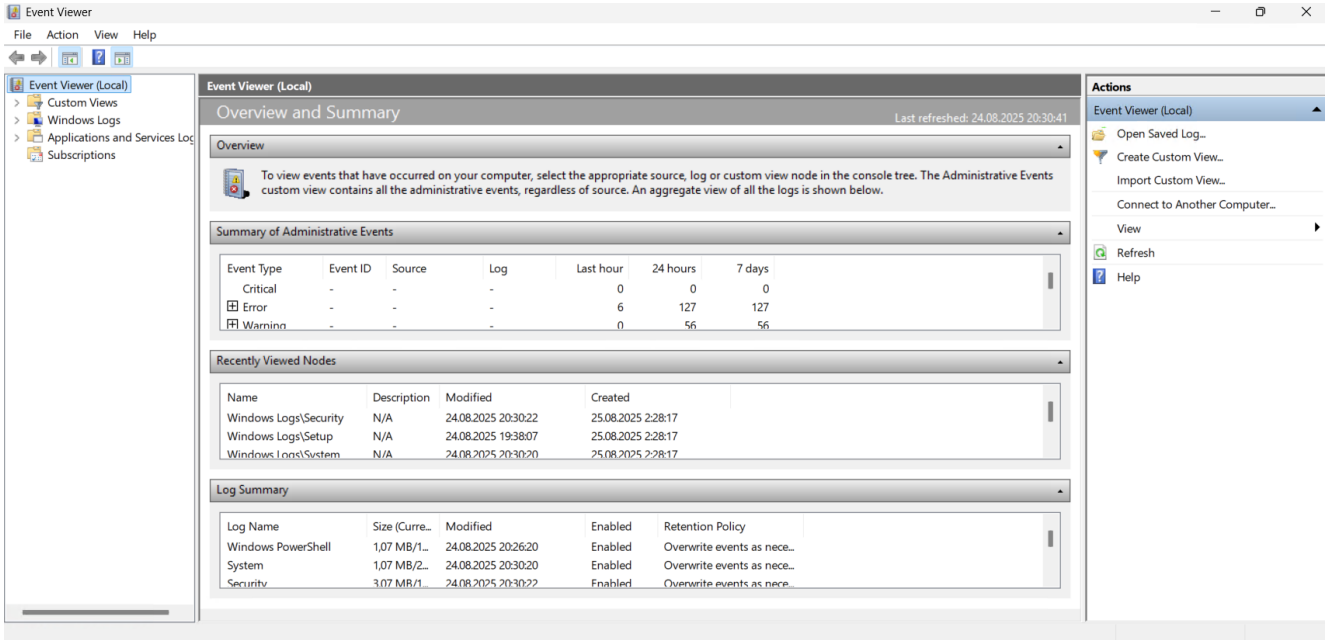


Рисунок 12.20 – Відкритий «Журнал подій»

У дереві ліворуч йдемо шляхом: «Журнали додатків та сервісів» – «Microsoft» – «Windows» – «GroupPolicy» – «Operational» (рис. 12.21).

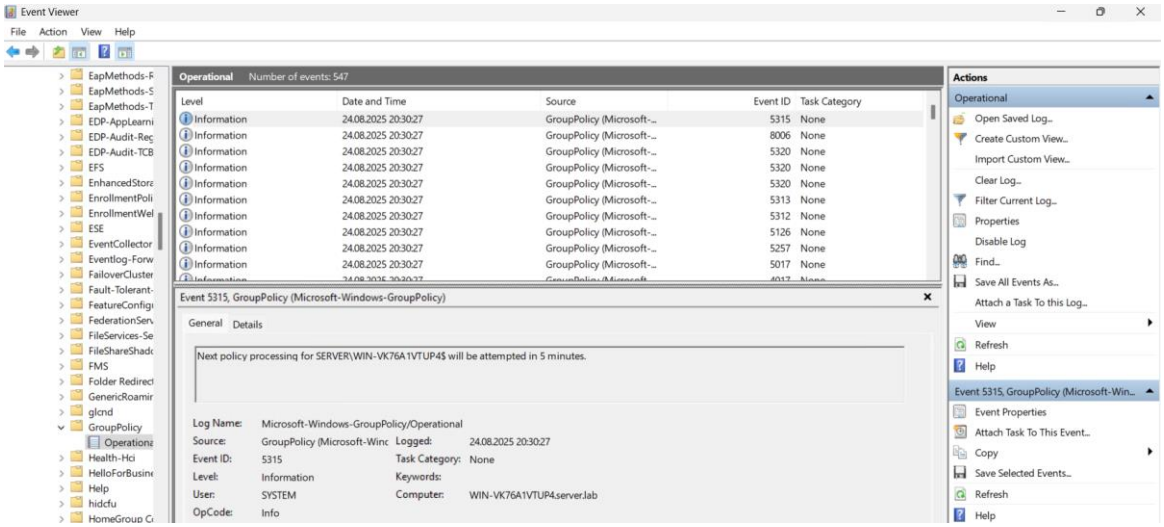


Рисунок 12.21 – Відкритий «Журнал подій» – «Operational»

У цьому журналі бачимо: час і спроби застосування політик, чи успішно вони застосувалися, а також точні повідомлення про помилки (наприклад, «немає доступу до контролера домену» або «політика не знайдена») чи попередження (рис. 12.22).

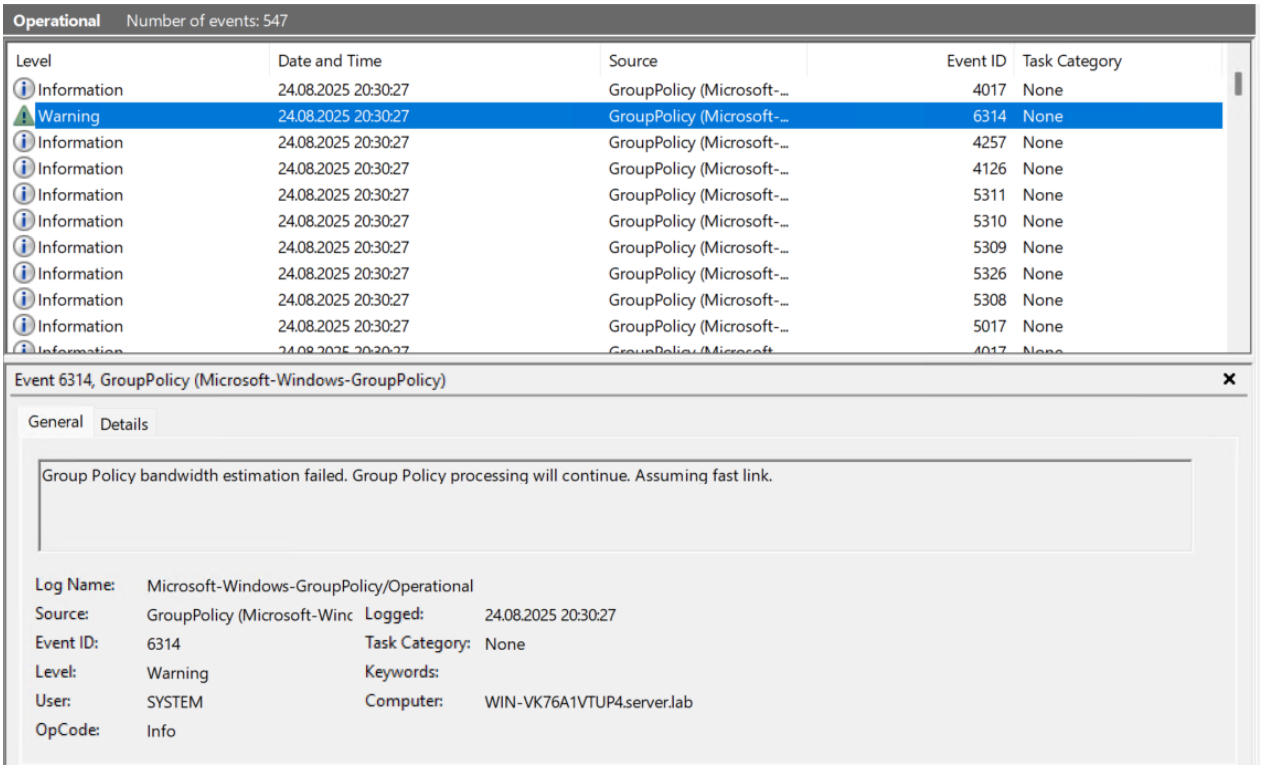


Рисунок 12.22 – Приклад попередження в журналі «Operational» щодо застосування групових політик

Для того, щоб точно знайти помилки, варто скористатися фільтром поточного журналу, вибравши відповідні категорії подій – «Помилка» та «Критичне» (рис. 12.23).

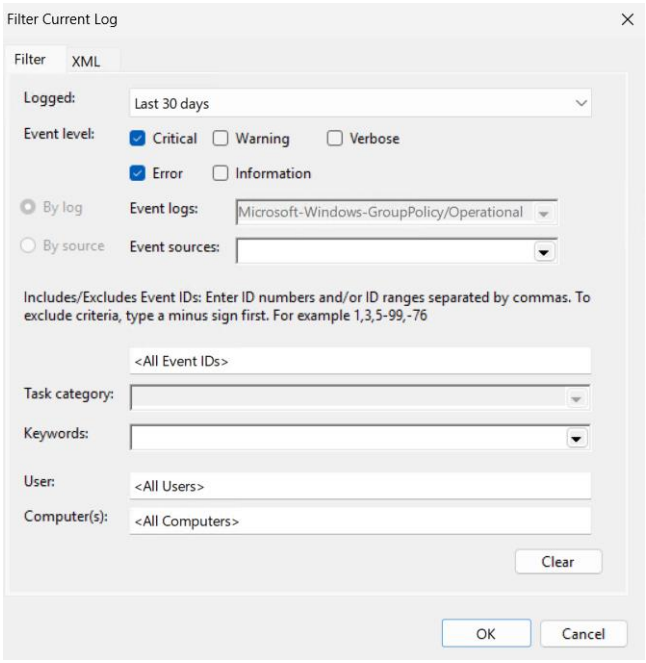


Рисунок 12.23 – Створення фільтру для пошуку та діагностики помилок політик

Якщо в результаті журнал буде пустий, це означає, що помилок немає. В іншому випадку будуть показані помилки та їхні властивості, які і слід детально проаналізувати та виправити.

Також для діагностики та перевірки помилок групових політик можна виконати перевірку послідовності застосування політик. Для цього переходимо в «Управління груповою політикою», там можемо відкрити потрібний OU (організаційний підрозділ). Далі вибираємо вкладку «Наслідування групових політик» (рис. 12.24).

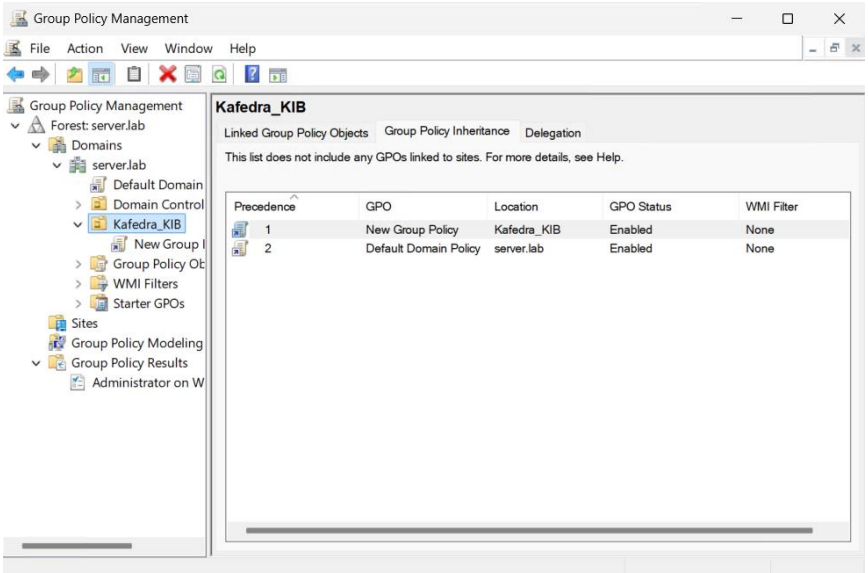


Рисунок 12.24 – Вкладка «Наслідування групових політик»

Тут бачимо порядок застосування політик: яка з них має вищий пріоритет і яка може перекривати інші. Якщо політика не працює – перевіряємо, чи не перекривається вона іншою, адже це може бути однією з причин помилки групової політики.

Практична робота 13
Налаштування DNS у Windows Server 2025

Мета роботи: ознайомитися з принципами роботи служби доменних імен (DNS) у середовищі Windows Server 2025, набути практичних навичок зі створення та налаштування прямої та зворотної зони DNS, дослідити механізми кешування DNS-запитів, а також виконати діагностику та усунення можливих помилок у функціонуванні служби [28, 29].

Хідроботи

Завдання 1. Створення прямої та зворотної зони DNS

Перед початком виконання завдань даної практичної роботи запустимо розгорнуту віртуальну машину Windows Server 2025 в середовищі Hyper-V, яка була створена в результаті виконання одного із завдань першої практичної роботи.

Для роботи з DNS та створення прямої та зворотної зони DNS відкриваємо «Диспетчер DNS», який попередньо встановлюємо через «Додавання ролей та компонентів» – додавання ролі «DNS-сервер». Вікдриття робиться наступним чином: відкриваємо «Диспетчер серверів», переходимо до пункту меню «Інструменти» і там шукаємо та вибираємо «DNS» (рис. 13.1).

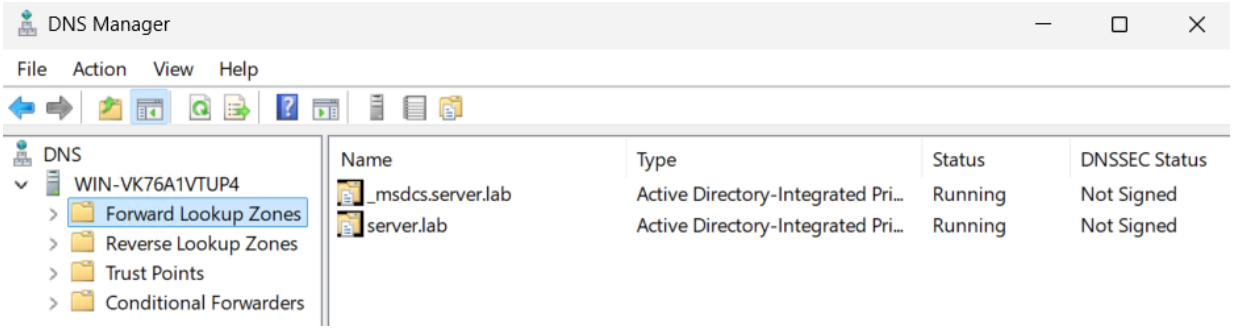


Рисунок 13.1 – Відкритий «Диспетчер DNS»

Після цього створюємо пряму зону DNS. Для цього у дереві зліва розгортаємо наш сервер DNS. Клацаємо правою кнопкою миші на «Прямі зони пошуку» – обираємо «Створити нову зону…» (рис. 13.2).

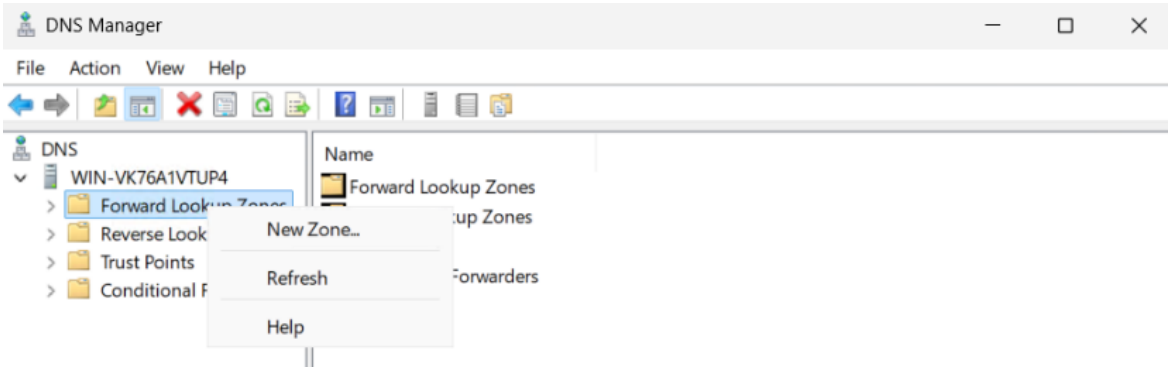


Рисунок 13.2 – Початок створення прямої зони DNS

Внаслідок цих дій запускається «Майстер створення нової зони», у вікні, що відкрилося натискаємо «Далі» (рис. 13.3).

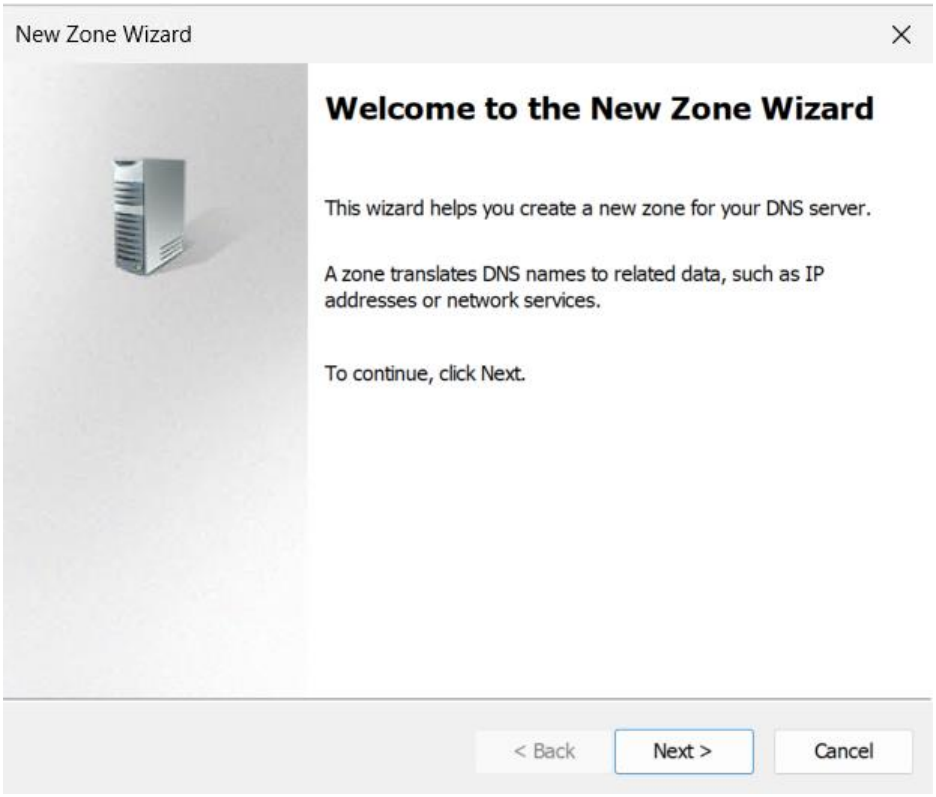


Рисунок 13.3 – «Майстер створення нової зони»

В наступній вкладці «Майстра створення нової зони» обираємо тип зони – «Основна зона». Якщо сервер є частиною домену, залишаємо галочку «Зберігати зону в Active Directory» (а в нашому випадку це так і є) і тиснемо «Далі» (рис. 13.4).

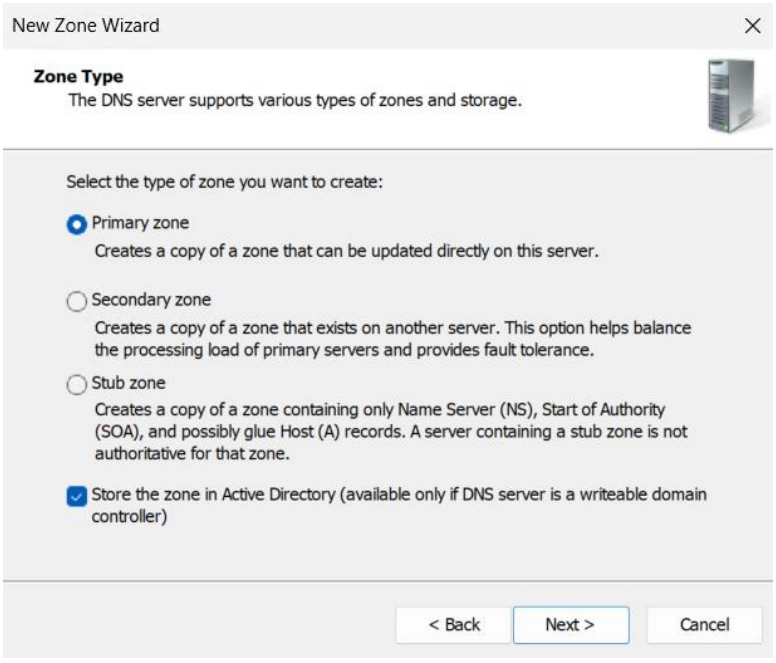


Рисунок 13.4 – Вибір типу зони DNS

Після цього, в іншій вкладці обираємо область реплікації – «Для всіх серверів DNS у домені» і тиснемо «Далі» (рис. 13.5).

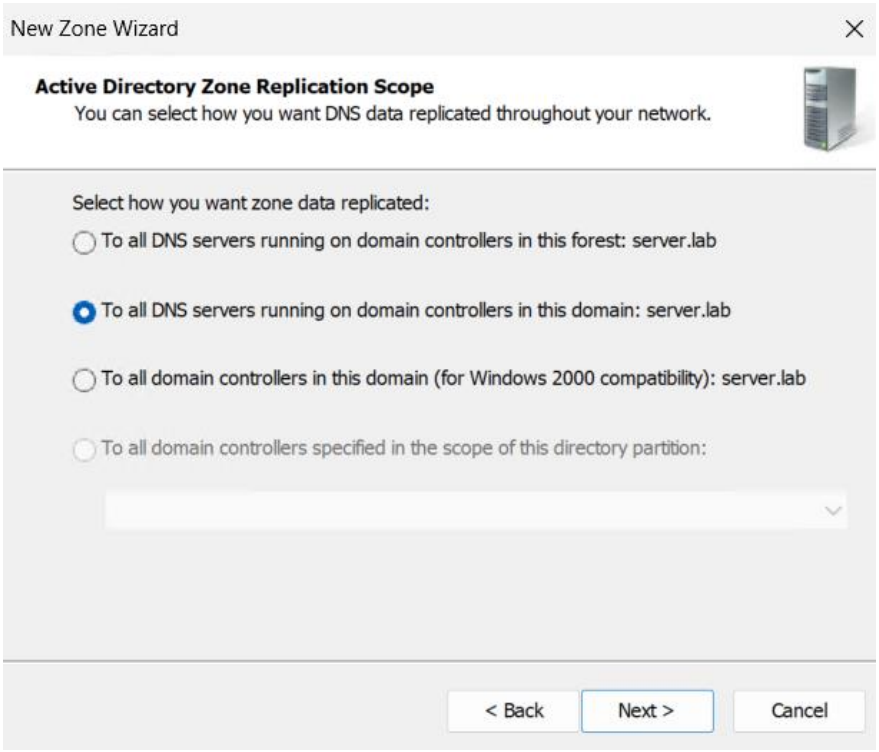


Рисунок 13.5 – Вибір області реплікації зони DNS

Коли вибір області реплікації виконано, вводимо ім’я зони, наприклад, «server_dns_forward_zone» і натискаємо «Далі» (рис. 13.6).

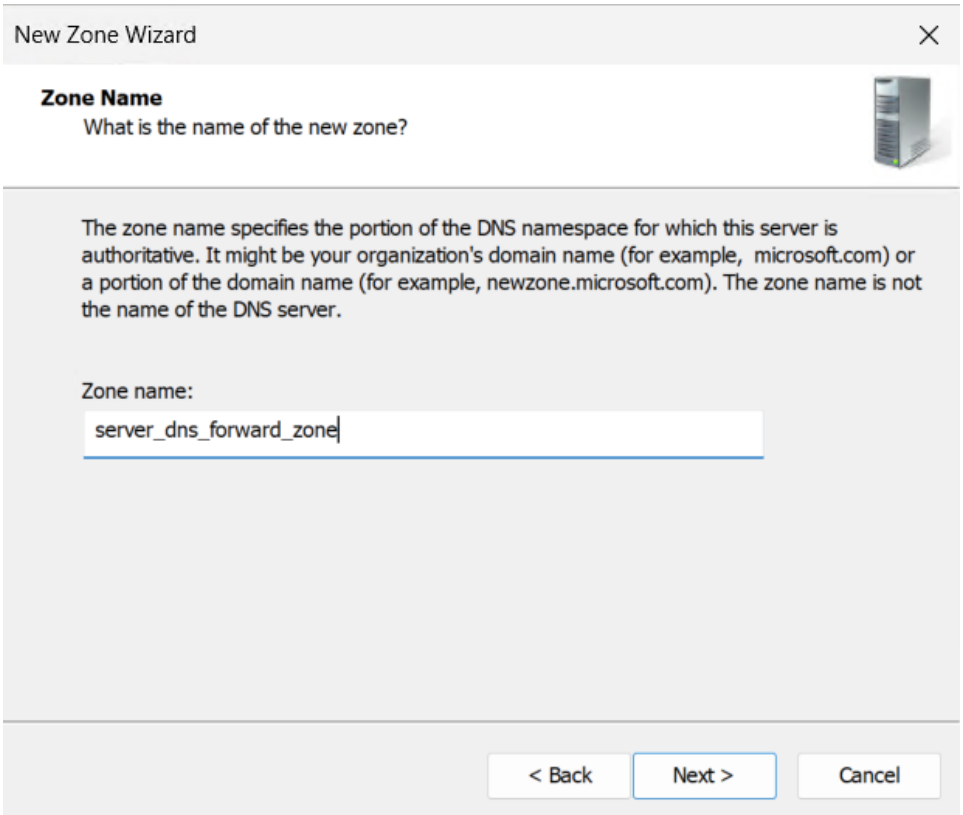


Рисунок 13.6 – Надання імені прямій зоні DNS

Коли надано ім’я, вибираємо спосіб оновлення зони DNS – «Дозволити лише захищені динамічні оновлення» – це оптимальний вибір з точки зору безпеки та функціональності і натискаємо «Далі» (рис. 13.7).

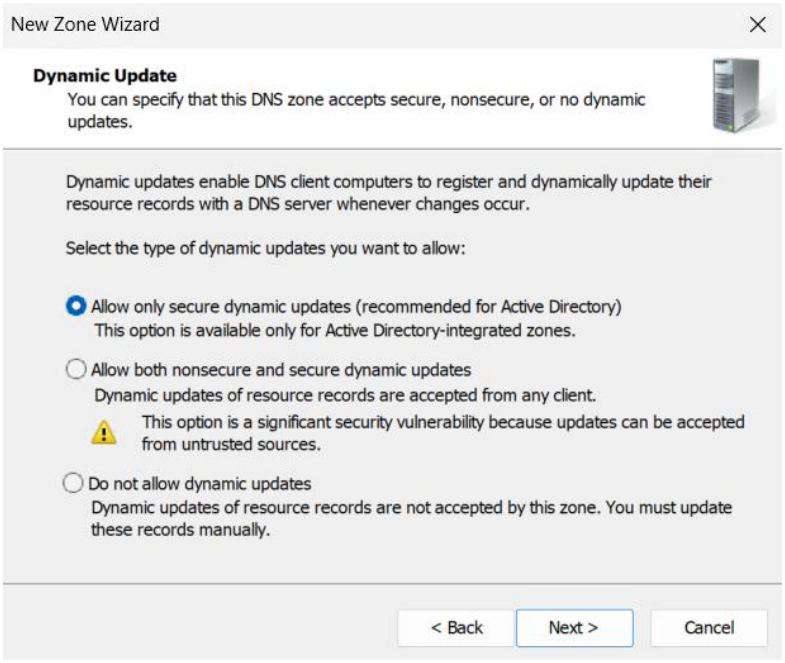


Рисунок 13.7 – Вибір способу оновлення прямої зони DNS

Далі на останній вкладці «Майстра створення нової зони» натискаємо «Готово» і в результаті цього пряма зона DNS створена (рис. 13.8).

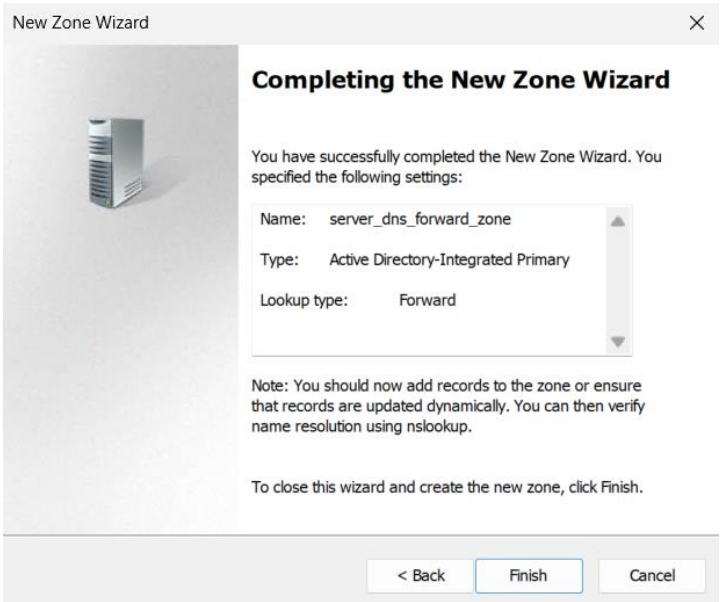


Рисунок 13.8 – Завершення створення прямої зони DNS

Щоб створити зворотну зону DNS здійснюємо подібні дії. У дереві зліва розгортаємо наш сервер DNS. Клацаємо правою кнопкою миші на «Зворотні зони пошуку», далі обираємо «Створити нову зону». Відкривається «Майстер створення нової зони», в першій вкладці натискаємо «Далі». Потім обираємо тип зони – «Основна зона» – «Далі». Далі обираємо реплікацію (як у прямій зоні). Після цього починаються деякі відмінності від прямої зони DNS, оскільки у наступній вкладці з’являється вибір «Зона зворотного пошуку IPv4» або «Зона зворотного пошуку IPv6». Ми обираємо IPv4 та натискаємо «Далі» (рис. 13.9).

Рисунок 13.9 – Вибір типу IP-адрес для створюваної зворотної зони DNS

Після цього, вводимо ідентифікатор мережі. Наприклад, якщо мережа, в якій працює сервер – 172.30.243.0 /24, то вводимо «172.30.243.» і тиснемо «Далі» (рис. 13.10).

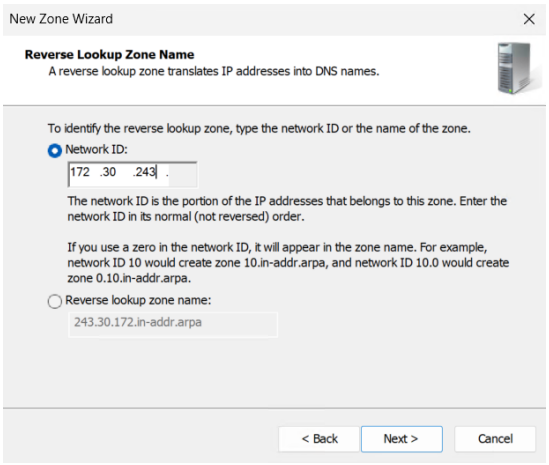


Рисунок 13.10 – Надання ідентифікатора мережі для зворотної зони DNS

Після цього вибираємо тип оновлень. Залишаємо «Дозволити лише захищені динамічні оновлення» (рис. 13.11).

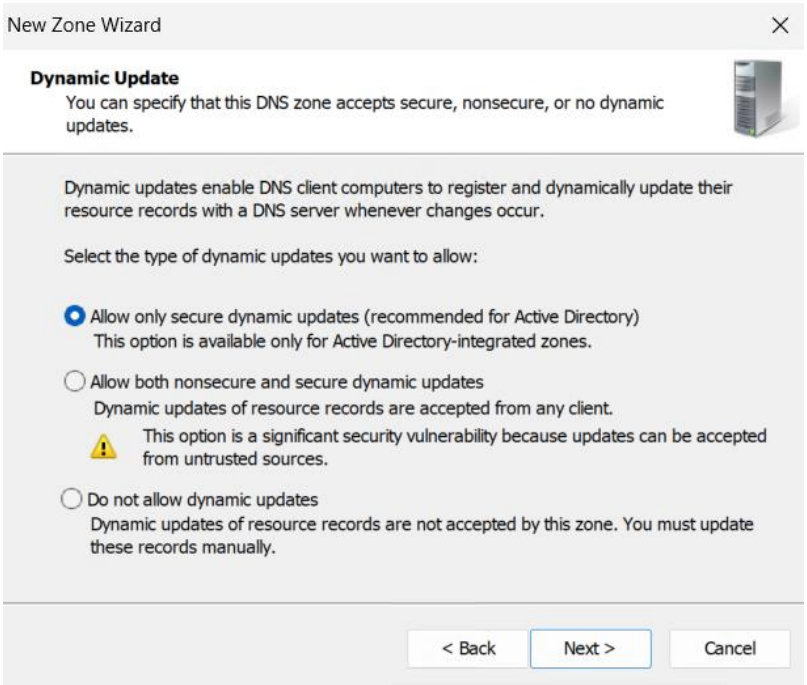


Рисунок 13.11 – Вибір типу оновлень для зворотної зони DNS

В останній вкладці тиснемо «Готово» і як наслідок зворотна зона DNS створена (рис. 13.12).

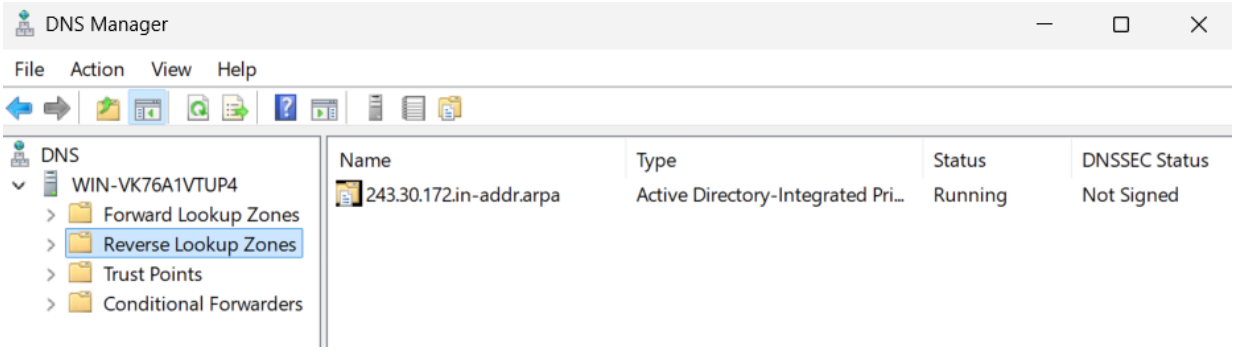


Рисунок 13.12 – Створена зворотна зона DNS

Завдання 2. Аналіз роботи кешування DNS

Для аналізу кешування DNS на сервері запускаємо «Диспетчер DNS». У лівій панелі обираємо наш сервер. Розгортаємо вузол «Кеш-пам'ять DNS». Тут бачимо записи, які сервер тимчасово зберіг після звернення до зовнішніх ресурсів. Кеш дозволяє швидше відповідати на повторні запити, не звертаючись щоразу до зовнішніх DNS-серверів.

Для перевірки кешування на сервері відкриваємо «Командний рядок» і виконуємо команду: «nslookup google.com». В результаті цього DNS-сервер отримає IP-адресу від зовнішнього DNS і збереже її у кеші. Далі виконуємо ту саму команду ще раз і тепер відповідь прийде значно швидше, бо сервер бере дані з кешу. Повертаємось у «Диспетчер DNS» – «Кеш-пам'ять DNS». Тут має з'явитися домен google.com та його підзаписи. Щоб не заходити в «Командний рядок» можна в «Диспетчер DNS» натиснути «Дії» – «Запустити NSLOOKUP» (рис. 13.13).

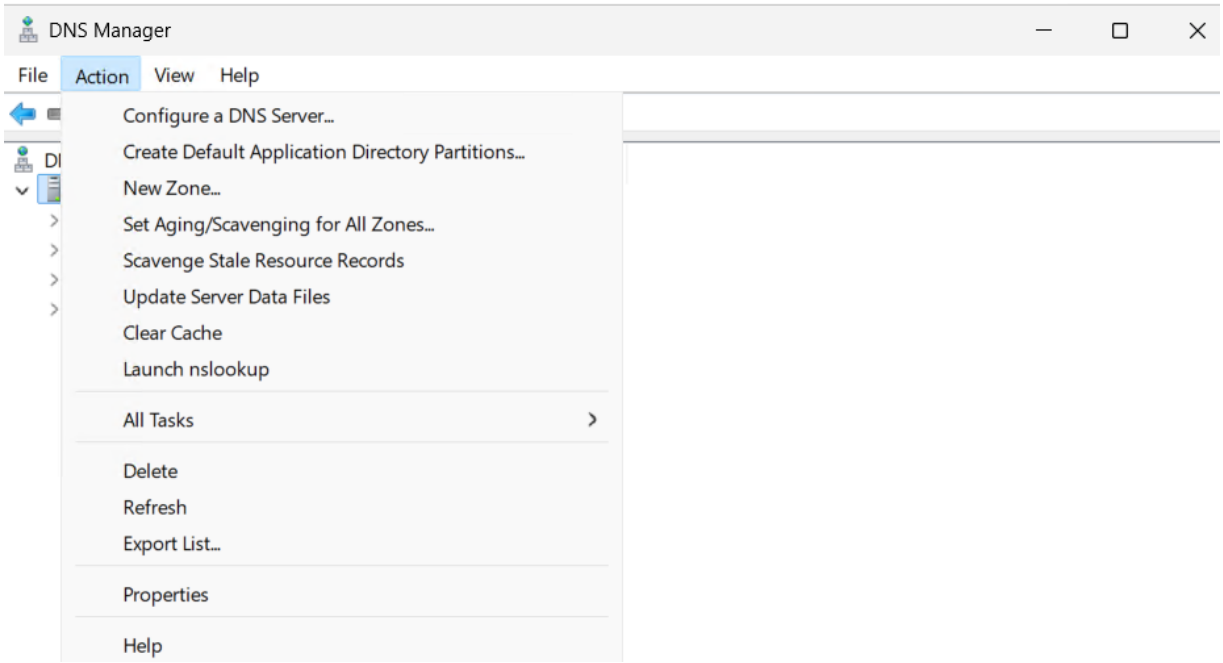


Рисунок 13.13 – «Запустити NSLOOKUP»

Після цього проводимо очищення кешу DNS. Щоб це виконати у DNS-менеджері натискаємо правою кнопкою миші на сервер та обираємо «Очистити кеш». Після цього кеш у вікні «Кеш-пам'ять DNS» очиститься (рис. 13.14).

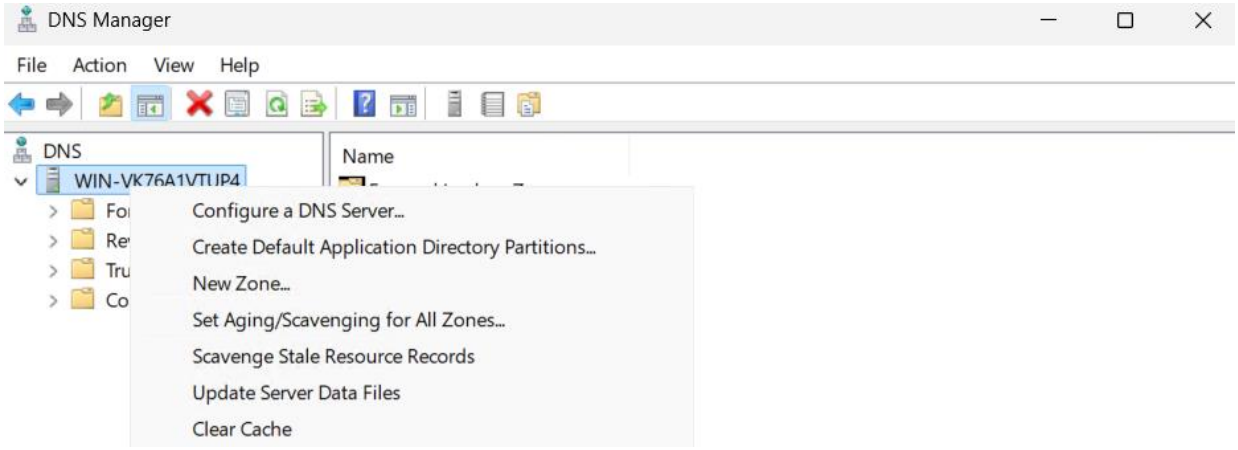


Рисунок 13.14 – «Очистити кеш»

Варто зазначити, що в кожного запису кешу DNS є параметр TTL (Time To Live) – це час, протягом якого він зберігається в кеші. Коли TTL закінчується, запис автоматично видаляється і при наступному запиті оновлюється.

Завдання 3. Діагностика та усунення помилок DNS

Для початку перевіряємо стан служби DNS. Відкриваємо «Диспетчер серверів». Переходимо у розділ «Служби». Переконуємось, що служба «DNS» має стан «Запущено». Якщо служба не працює – запускаємо її через натиснення на «Пуск».

Наступне, що варто виконати – це перевірка резолюції імен. Для цього відкриваємо «Командний рядок», виконуємо команду «nslookup google.com» Якщо бачимо IP-адресу, то резолюція працює. Якщо отримуємо помилку «Server failed» або «Request timed out», потрібно перевіряти далі та змінювати налаштування (рис. 13.15).

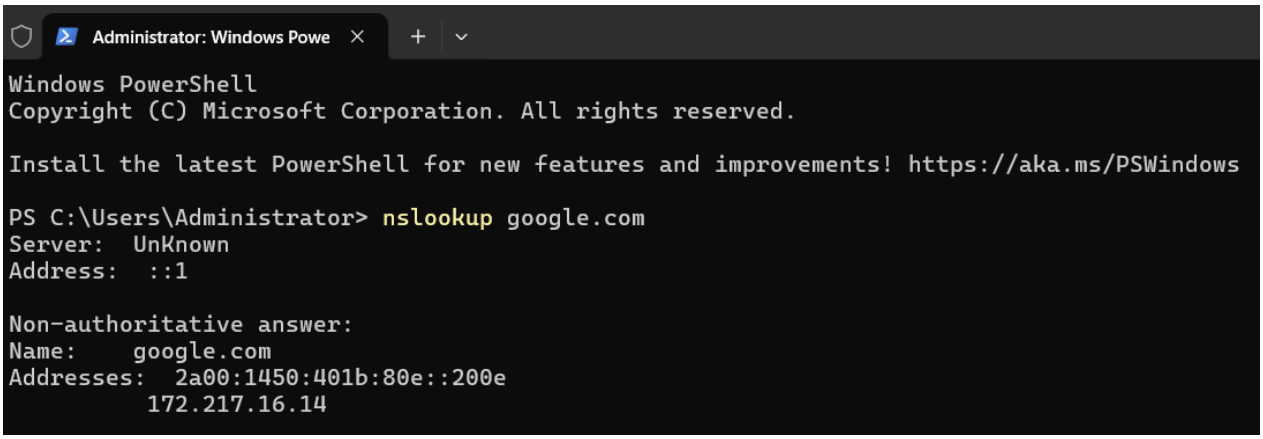


Рисунок 13.15 – Приклад успішного виконання команди «nslookup google.com»

Для діагностики налаштувань DNS виконуємо також перевірку клієнтських налаштувань. Відкриваємо «Центр управління мережами і спільним доступом» (рис. 13.16).

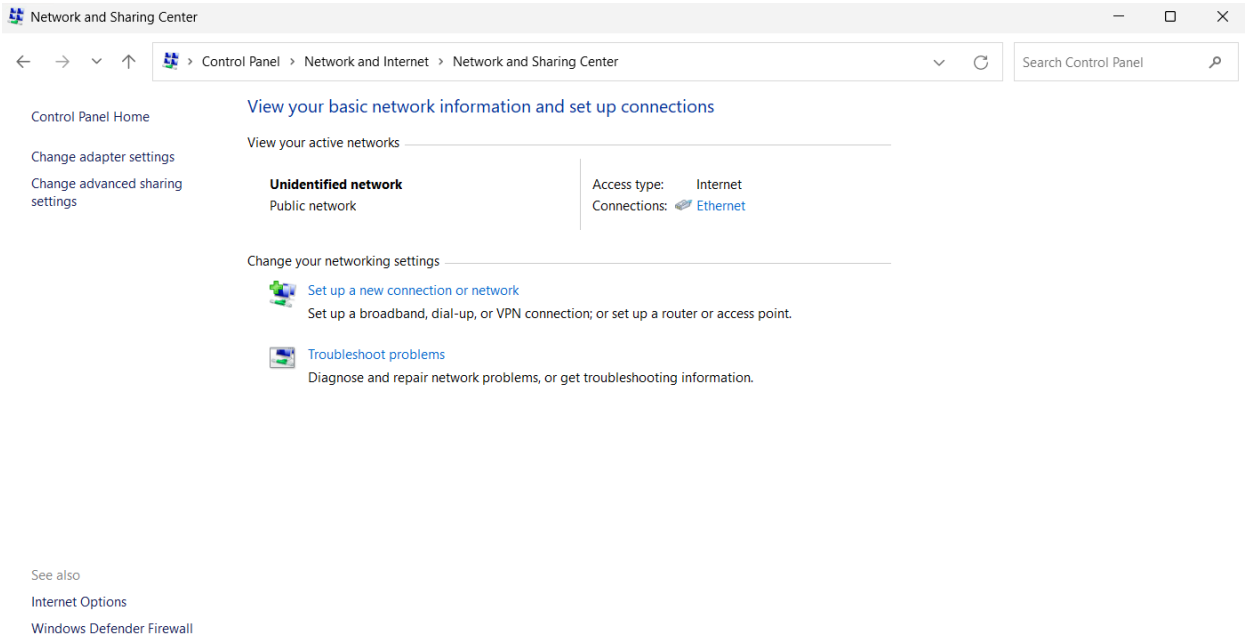


Рисунок 13.16 – «Центр управління мережами і спільним доступом»

Натискаємо на «Ethernet» та у вікні, що відкрилося заходимо у «Властивості». Вибираємо «Протокол TCP/IPv4» та натискаємо «Властивості». Переконуємось, що у полі «DNS-сервер» вказана IP-адреса нашого DNS-сервера (рис. 13.17).

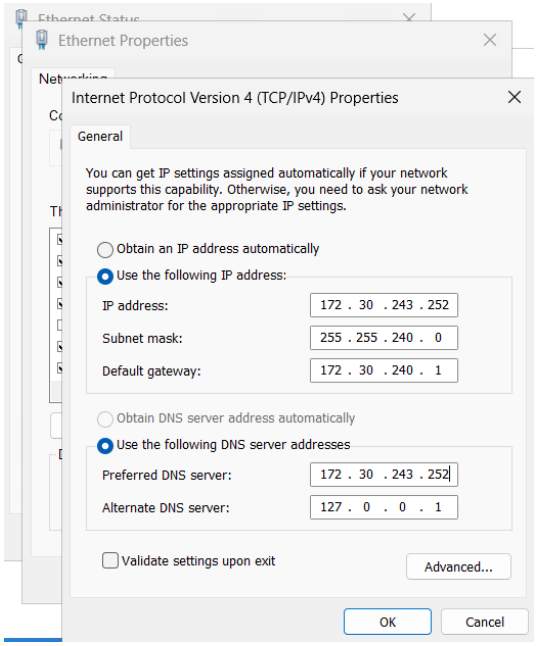


Рисунок 13.17 – Властивості IPv4 сервера та значення параметрів DNS-сервера

Також для діагностики проводиться перевірка зон DNS. Відкриваємо «Диспетчер DNS». Переглядаємо «Зони прямого перегляду» та «Зони зворотного перегляду».

Переконуємось, що: існує зона для домену (наприклад, server.lab). Є записи A (хост) для серверів і клієнтів. У зворотній зоні створені записи PTR. Якщо записи відсутні – створюємо їх вручну (натискаємо ПКМ по назві типу

зони та вибираємо «Новий вузол (A або AAAA)», «Новий вказівник (PTR)») (рис. 13.18).

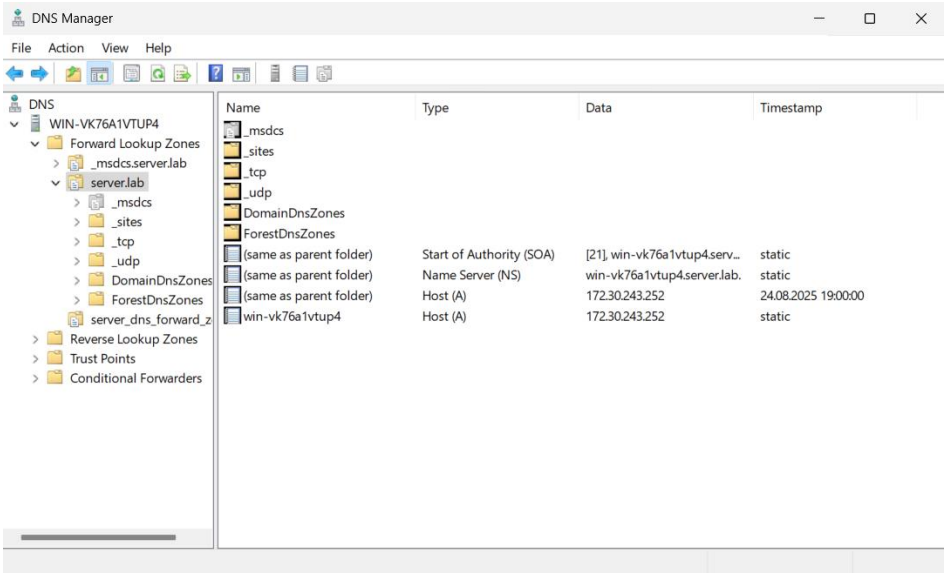


Рисунок 13.18 – Перевірка зон DNS

Також для діагностики роботи DNS та перевірки на наявність помилок застосовується утиліта «nslookup». Для її застосування у командному рядку вводимо «nslookup» – з'явиться консоль утиліти. Далі перевіряємо наш конкретний DNS-сервер – вводимо команду «server <ip address DNS-server>», в даному випадку «server 172.30.247.252». Після цього запитуємо будь-який домен, наприклад, google.com. Якщо є відповідь, то сервер працює. Якщо помилка, то проблема у зоні або маршруті (рис. 13.19).

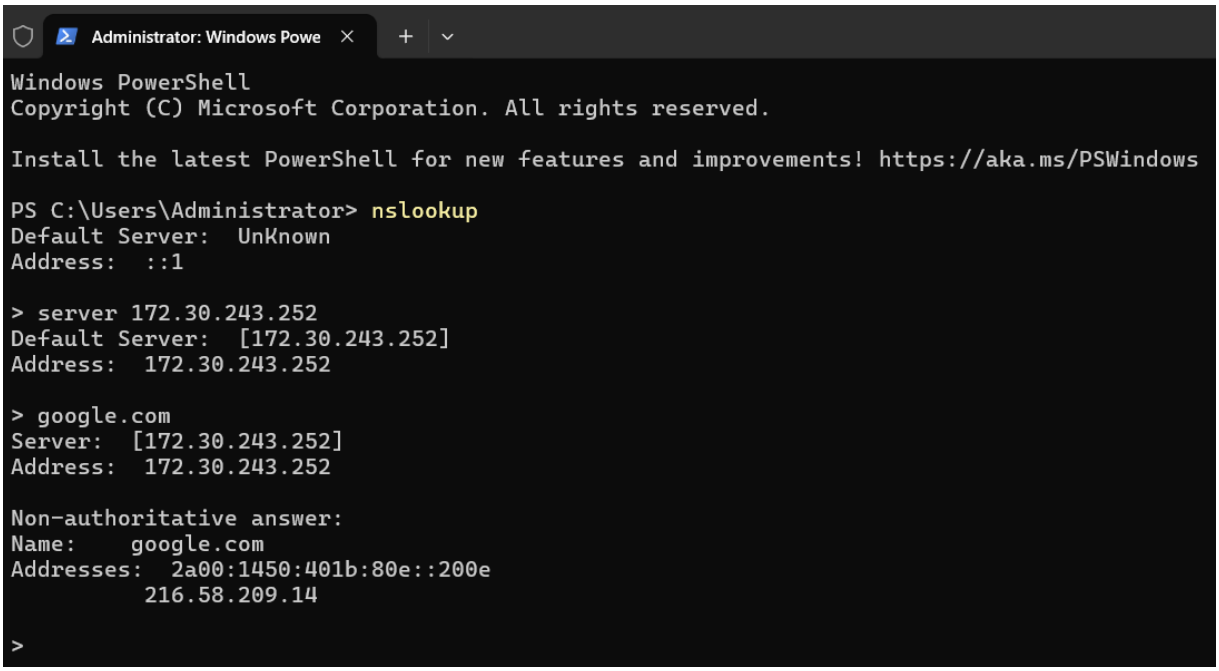


Рисунок 13.19 – Використання утиліти «nslookup» для діагностики роботи DNS

Практична робота 14
DHCP у Windows Server 2025

Мета роботи: ознайомитися з принципами функціонування служби DHCP у середовищі Windows Server 2025, набути практичних навичок з інсталяції та конфігурації DHCP-сервера, створення та налаштування діапазонів IP-адрес, перевірки автоматичної видачі мережевих параметрів клієнтам, а також аналізу журналів роботи служби та усунення типових помилок [30-33].

Хідроботи

Завдання 1. Розгортання DHCP-сервера

Перед початком виконання завдань даної практичної роботи запустимо розгорнуту віртуальну машину Windows Server 2025 в середовищі Hyper-V, яка була створена в результаті виконання одного із завдань першої практичної роботи.

Для розгортання DHCP-сервера, потрібно встановити для цього локального сервера роль «DHCP-сервер». Як, додавати ролі та компоненти опрацьовано в попередніх практичних роботах. Тому, відкриваємо «Диспетчер серверів». У верхньому правому меню обираємо «Керування» – «Додати ролі та компоненти». У майстрі додаємо роль «Ролі серверів» – «Сервер DHCP» (рис. 14.1).

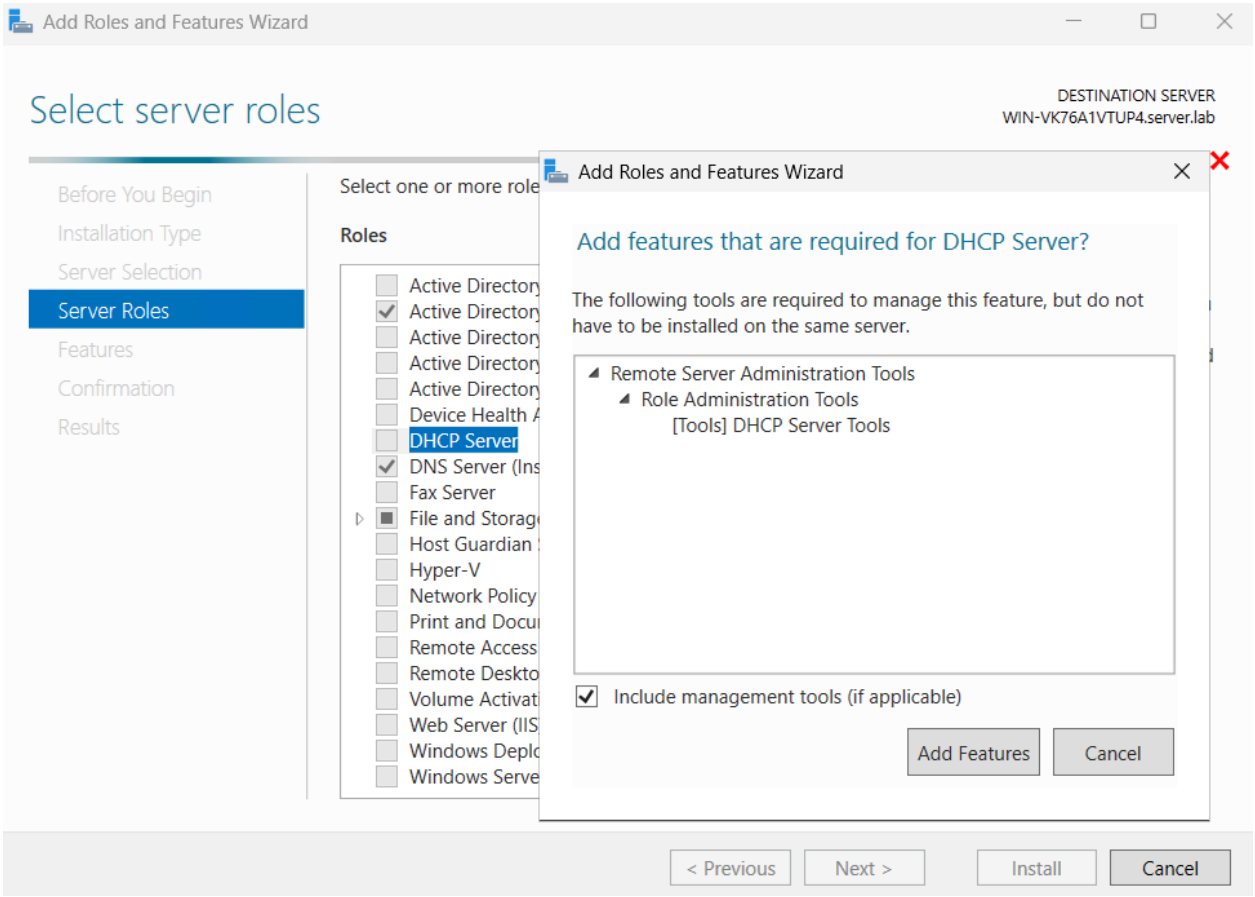


Рисунок 14.1 – Додавання ролі «Сервер DHCP»

Після вибору ролі, підтверджуємо вибір та чекаємо завершення інсталяції. Після завершення – натискаємо «Закрити» (рис. 14.2).

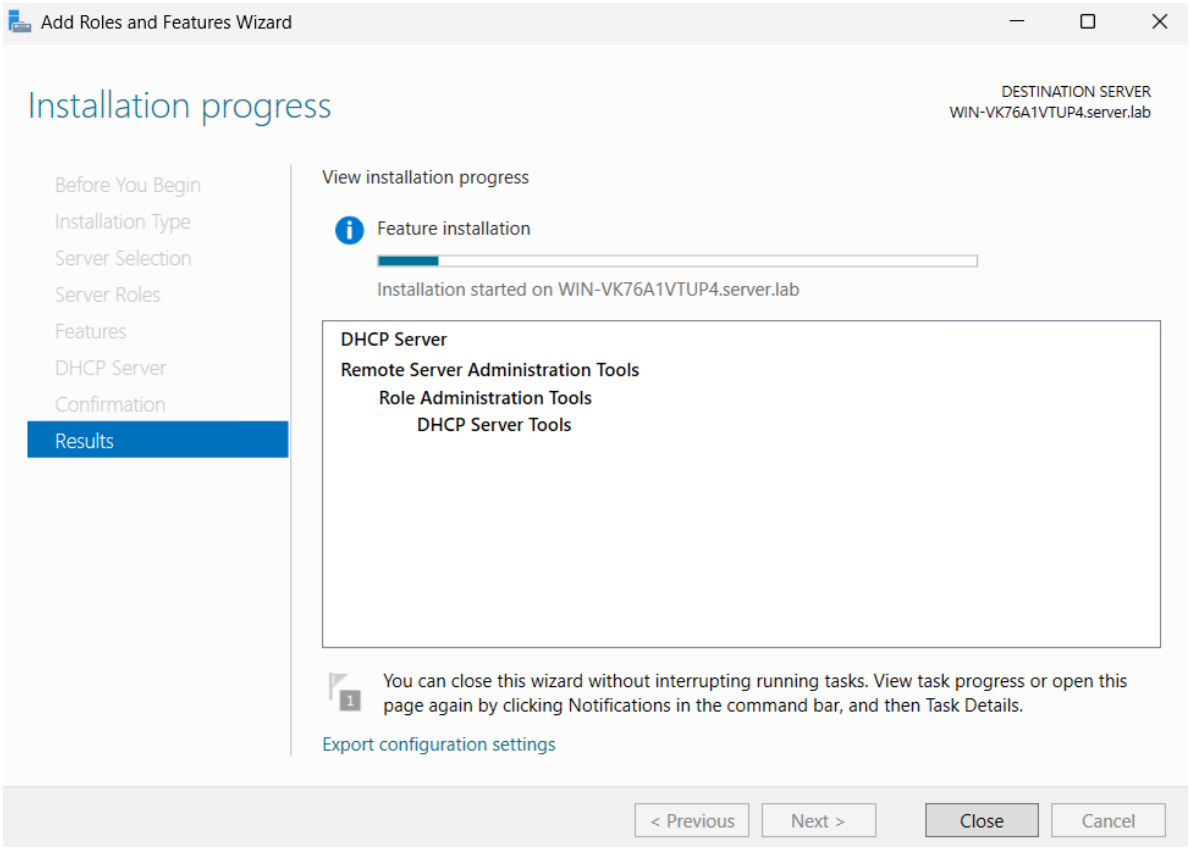


Рисунок 14.2 – Встановлення ролі «Сервер DHCP»

Після інсталяції у «Диспетчері серверів» з’явиться повідомлення про необхідність виконати початкову конфігурацію DHCP(рис. 14.3).

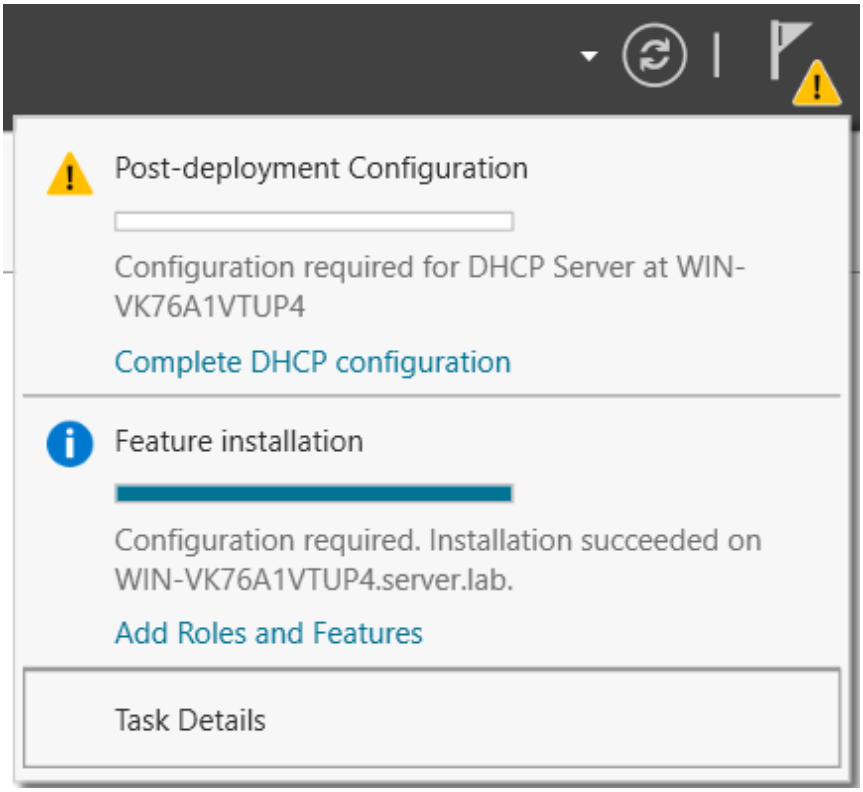


Рисунок 14.3 – Повідомлення про необхідність виконати конфігурацію DHCP

Натискаємо «Завершити конфігурацію DHCP», відкривається «Майстер налаштування DHCP після встановлення», на першій вкладці натискаємо «Далі» (рис. 14.4).

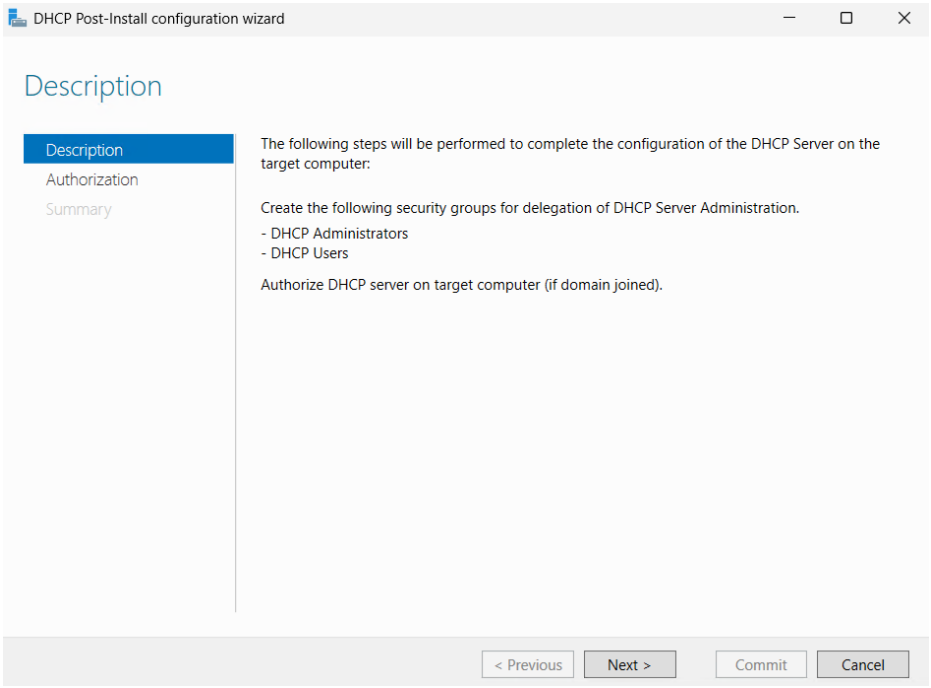


Рисунок 14.4 – Перша вкладка «Майстра налаштування DHCP після встановлення»

У наступному вікні майстра підтверджуємо використання облікового запису адміністратора для авторизації. Завершуємо налаштування та натискаємо «Закрити» (рис. 14.5-14.6).

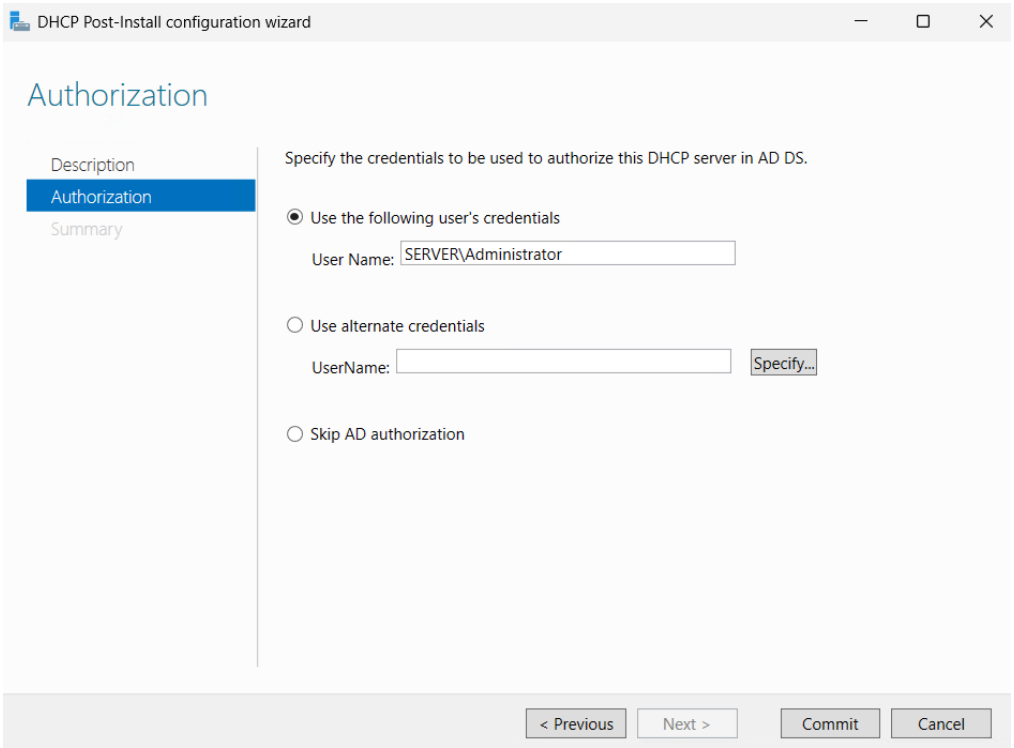


Рисунок 14.5 – Підтвердження використання облікового запису адміністратора

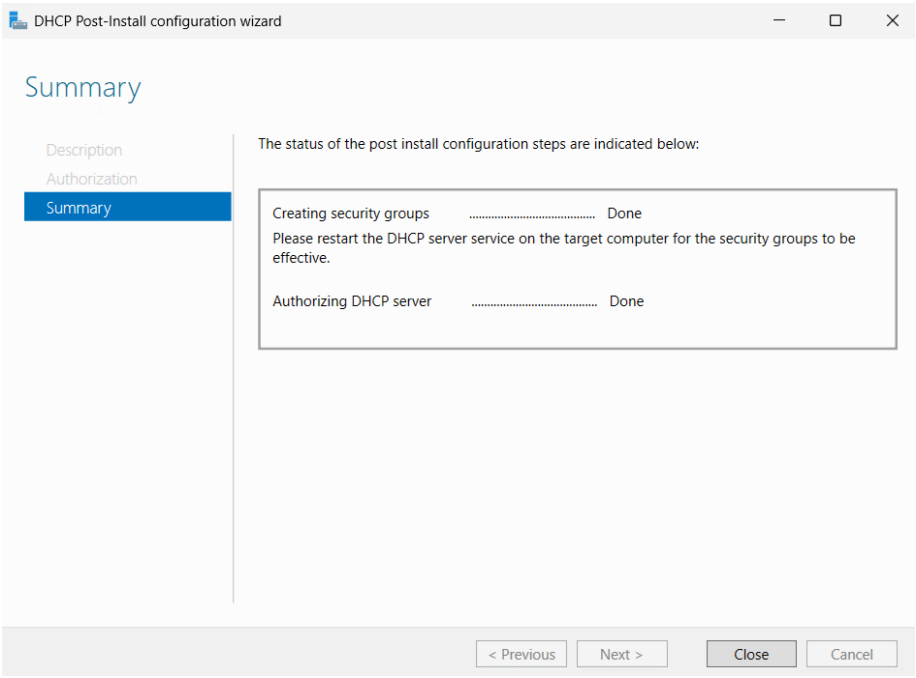


Рисунок 14.6 – Завершення початкового налаштування DHCP

Завдання 2. Налаштування діапазону IP-адрес

Подальшим етапом налаштування DHCP-сервера є налаштування діапазону IP-адрес, який цей сервер використовуватиме та видаватиме клієнтським пристроям. Для створення нового діапазону IP-адрес відкриваємо «DHCP», щоб це виконати «Диспетчері серверів» переходимо до «Інструменти» – «DHCP». Відкривається вікно «Менеджера DHCP» (рис. 14.7).

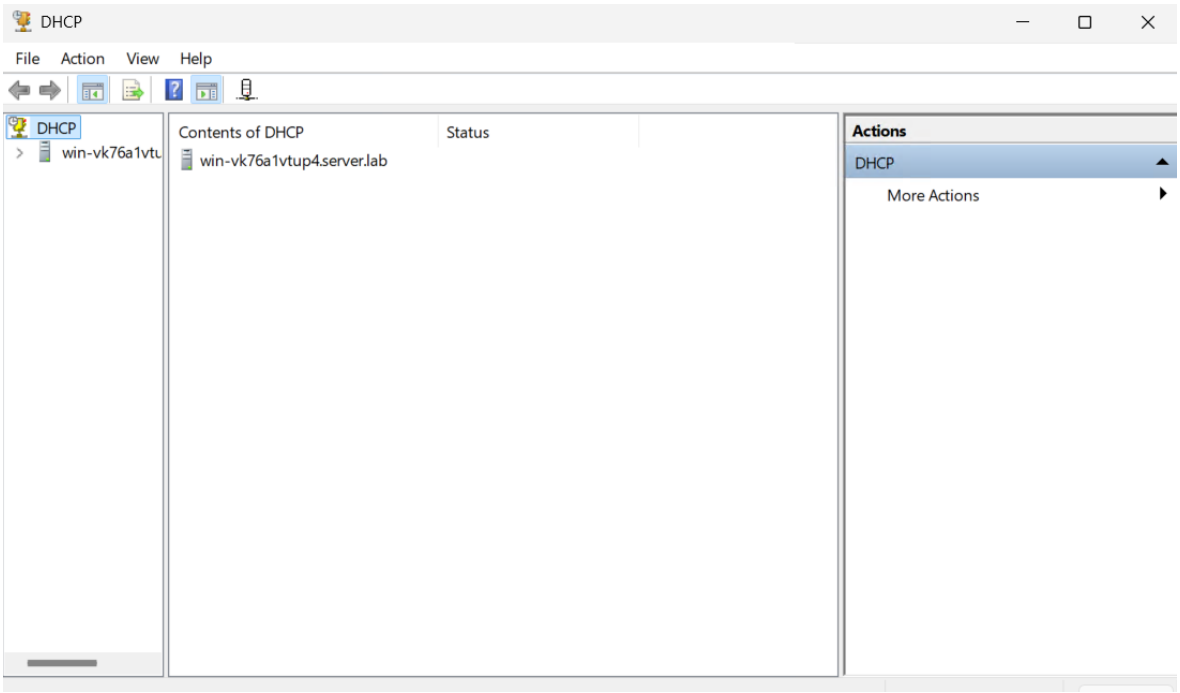


Рисунок 14.7 – Вікно «Менеджера DHCP»

У дереві зліва обираємо свій сервер, натискаємо на нього. Далі клацаємо правою кнопкою миші на «IPv4» та вибираємо «Створити область». В результаті цих дій відкривається «Майстер створення області» (рис. 14.8).

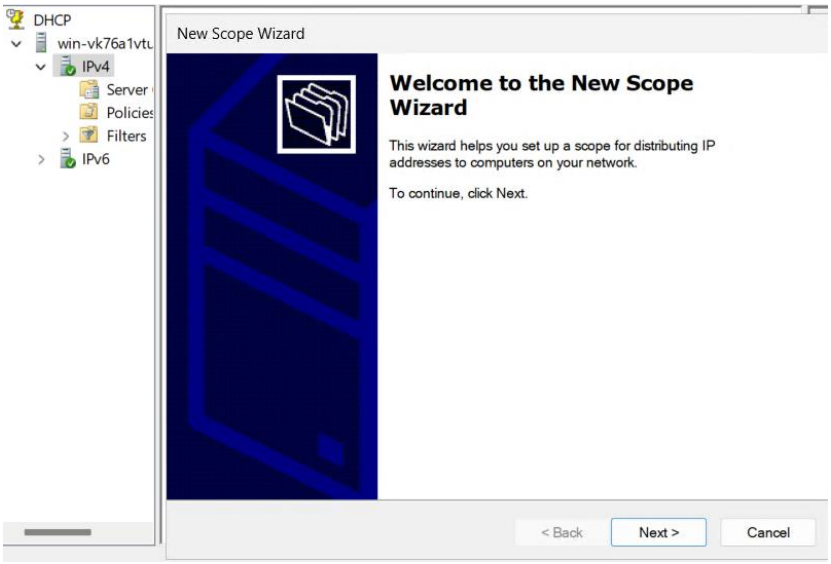


Рисунок 14.8 – Вікно «Майстер створення області»

На першій вкладці даного «Майстра…» натискаємо «Далі». Після цього починаються власне налаштування створюваного діапазону IP-адрес. Спочатку налаштовуємо ім'я діапазону (вводимо наприклад «DHCP-M1»). За необхідності можна додати опис, це корисно, якщо існує кілька DHCP-пулів для різних мереж і пристроїв(рис. 14.9).

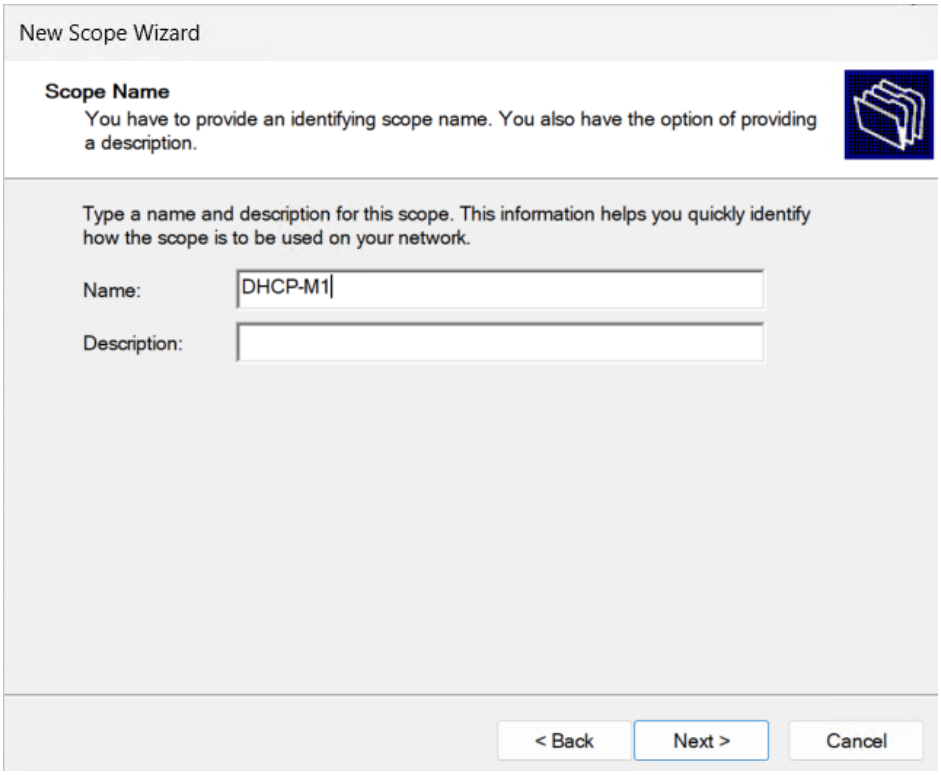


Рисунок 14.9 – Надання імені DHCP-діапазону

В наступній вкладці налаштовуємо найважливіші параметри: початкова IP-адреса (наприклад: 172.30.243.80); кінцева IP-адреса (наприклад: 172.30.243.160). Маска підмережі (наприклад: 255.255.240.0). Після заповнення всіх полів натискаємо «Далі» (рис. 14.10).

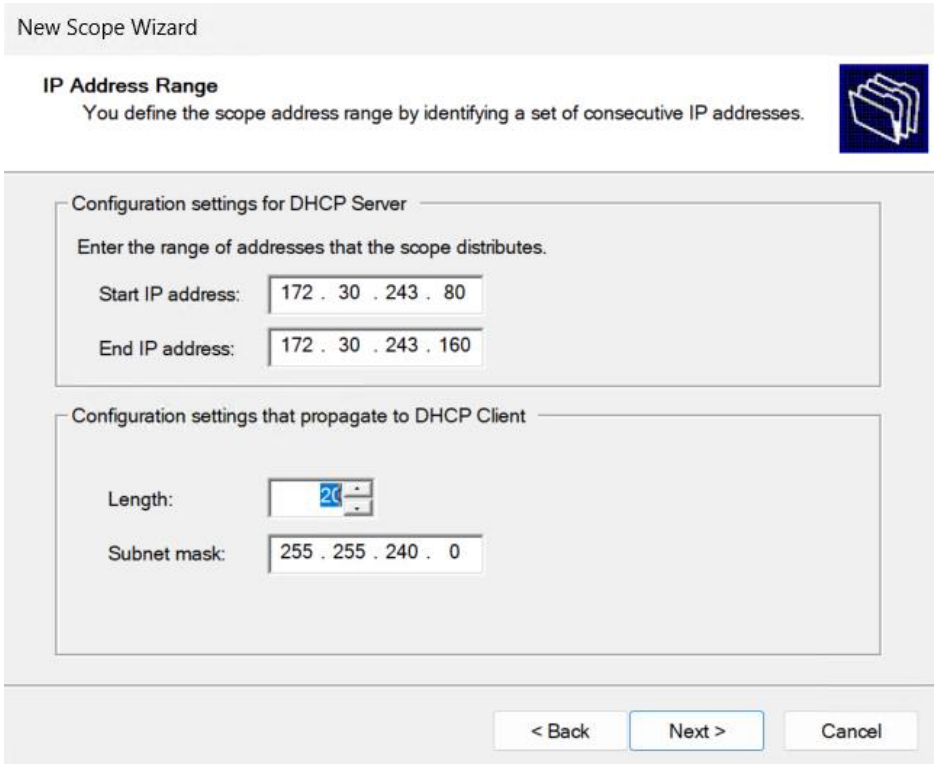


Рисунок 14.10 – Налаштування IP-параметрів DHCP-діапазону

В наступній вкладці, якщо є IP-адреси, які не повинні видаватися клієнтам, додаємо їх у «Виключення» та знову тиснемо «Далі» (рис. 14.11).

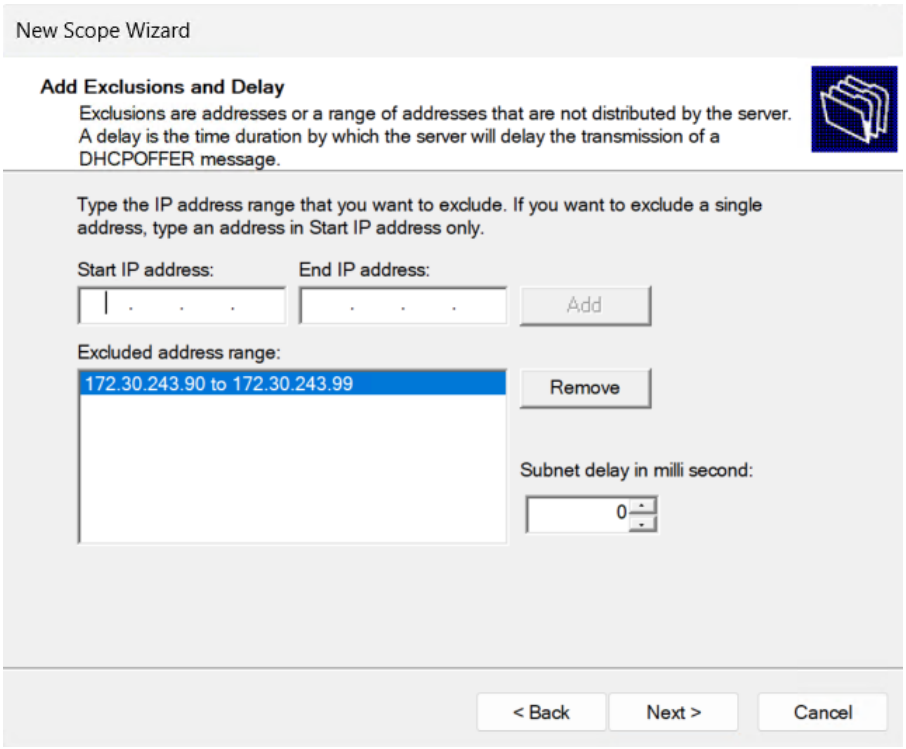


Рисунок 14.11 – Налаштування IP-адрес, які будуть виключені з DHCP-діапазону

Після цього налаштовуємо час оренди (наприклад, 30 днів) і натискаємо «Далі» (рис. 14.12).

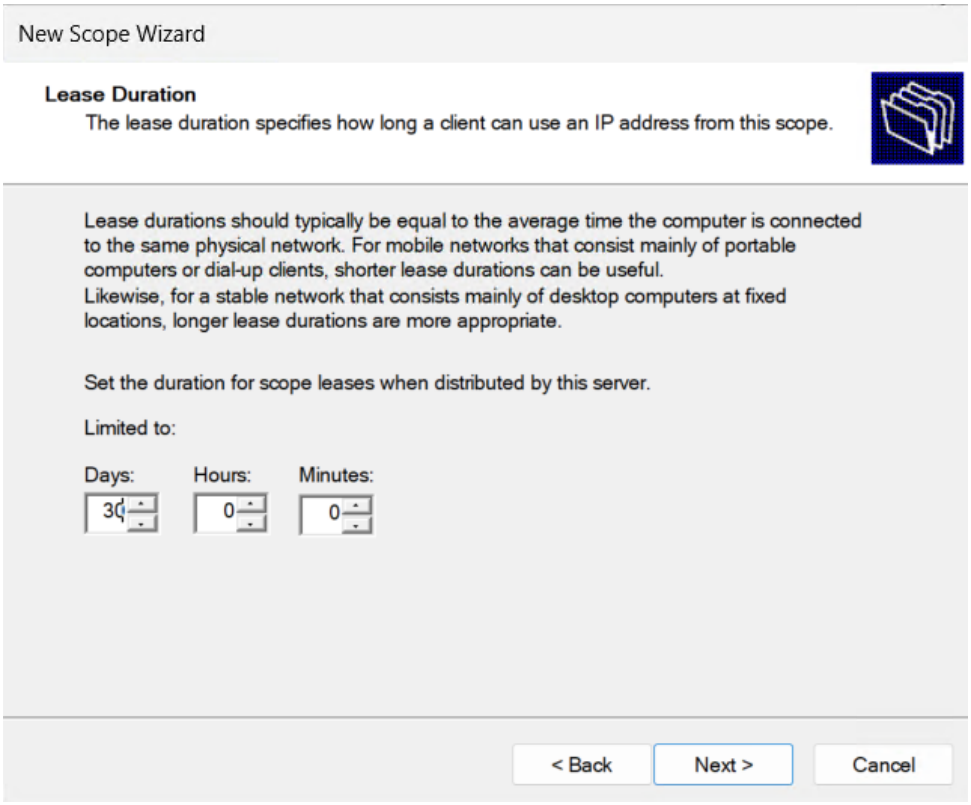


Рисунок 14.12 – Налаштування часу оренди для DHCP-діапазону

Далі, в наступній вкладці, вибираємо «Так, налаштувати ці параметри зараз». тиснемо «Далі». Потім вказуємо шлюз за замовчуванням (IP-адреса порту маршрутизатора) – наприклад: 172.30.240.1 (рис. 14.13).

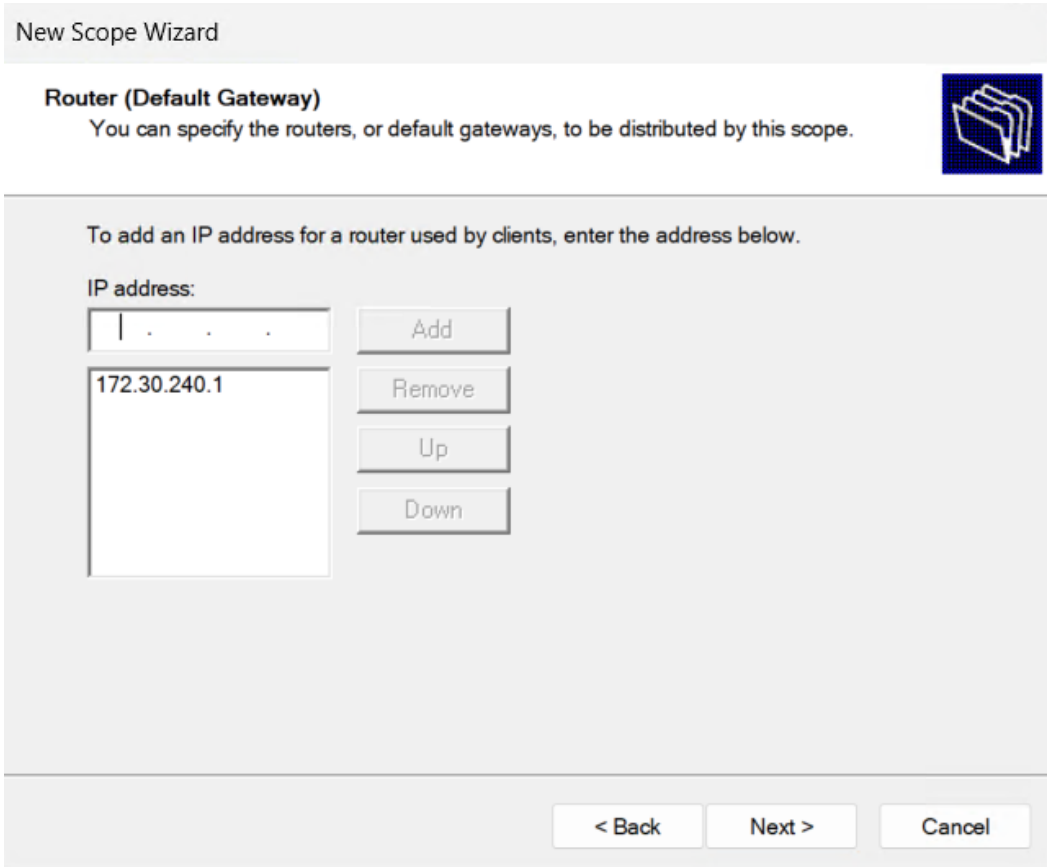


Рисунок 14.13 – Налаштування шлюзу за замовчуванням для DHCP-діапазону

Після цього виконуємо налаштування DNS-сервера для створюваного DHCP-діапазону, вказуємо IP-адресу нашого DNS (наприклад: 172.30.243.252). Якщо налаштування DNS, вже було виконано, то IP-адреса DNS-сервера буде записана автоматично і додаткового введення на цьому етапі не потребуватиме (рис. 14.14).

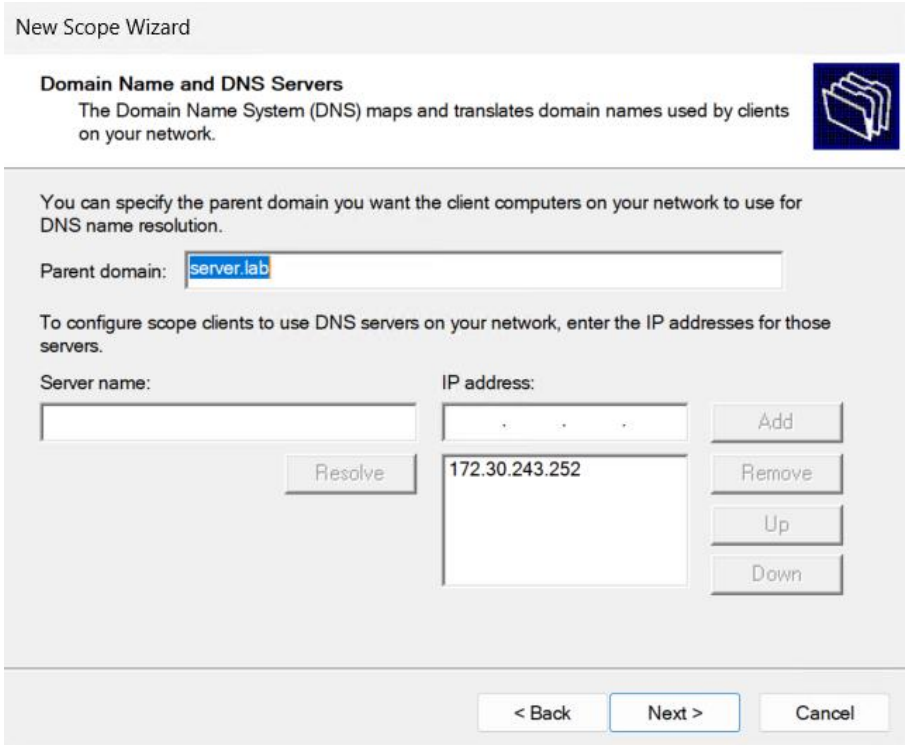


Рисунок 14.14 – Налаштування DNS-сервера для DHCP-діапазону

Згодом натискаємо «Далі» в цій вкладці і у наступній також. При виборі часу активації DHCP-області обираємо варіант «Так, я хочу активувати цю область зараз» і тиснемо «Далі» (рис. 14.15).

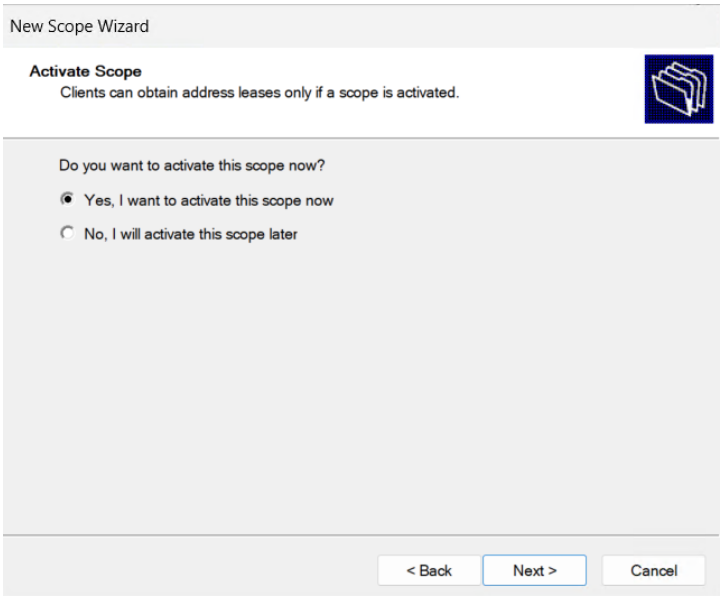


Рисунок 14.15 – Вибір часу активації DHCP-області

Далі натискаємо «Готово» і завершуємо створення та налаштування DHCP-діапазону (рис. 14.16).

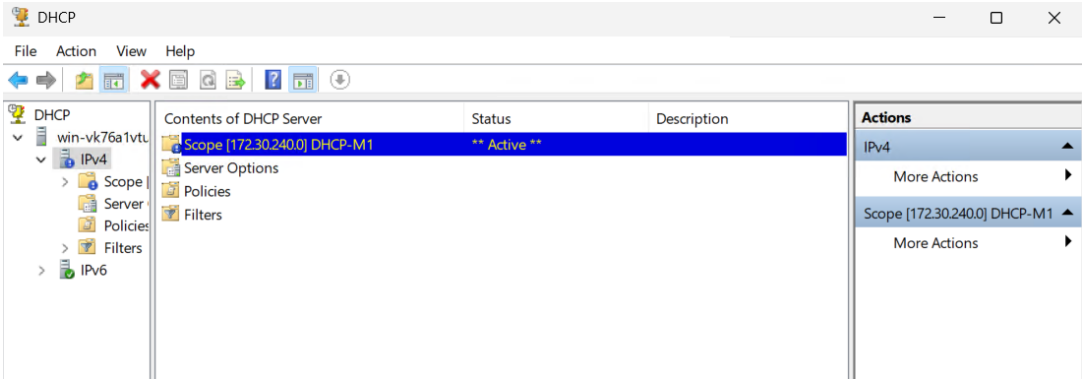


Рисунок 14.16 – Створена та активована DHCP-область

Щоб перевірити функціонування DHCP-сервера запускаємо іншу віртуальну машину у Hyper-V (наприклад, клієнт з Windows 10/11). Налаштовуємо мережеву карту цієї ВМ так, щоб вона отримувала IP-адресу автоматично.

У командному рядку клієнтської ВМ вводимо команди «ipconfig /renew» (оновлення IP) та «ipconfig /all» (перегляд виданої IP-адреси). Переконуємось, що клієнт отримав адресу з діапазону, який ми створили.

Завдання 3. Аналіз логів DHCP-сервера

Аналіз логів DHCP-сервера передбачає використання журналів Windows для аналізу функціонування DHCP. Для цього відкриваємо «Переглядач подій» (Event Viewer). У дереві ліворуч переходимо: «Журнали програм та служб» – «Microsoft» – «Windows» – «DHCP-Server» та аналізуємо журнали, що присутні для цього DHCP-сервера (рис. 14.17).

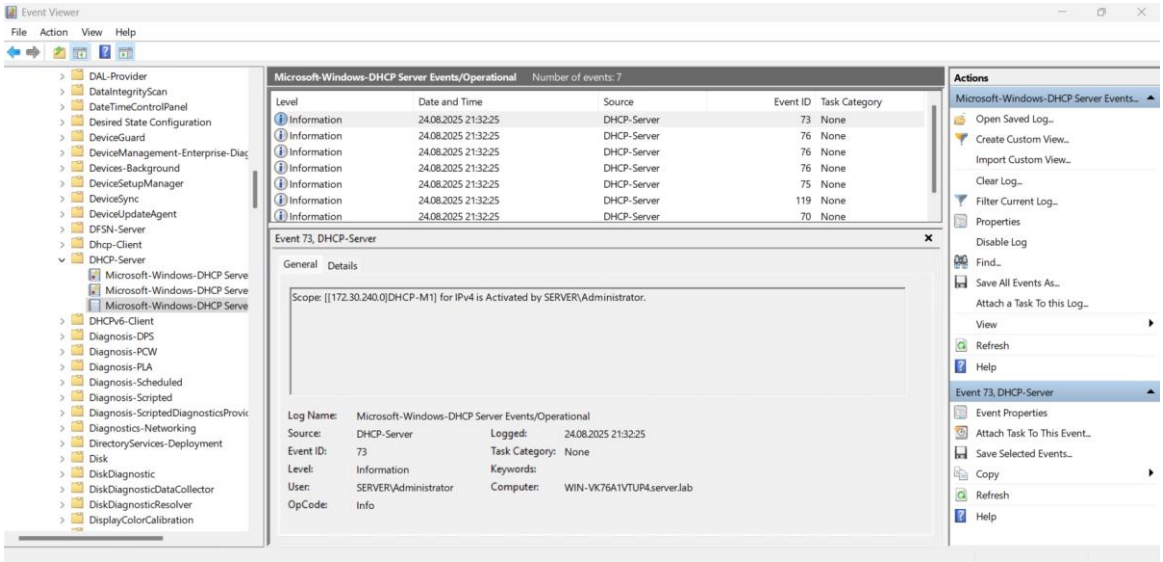


Рисунок 14.17 – Аналіз журналів DHCP-сервера

Аналізуємо записи в журналі за кодом події. Успішна видача IP-адреси – Event ID 10. Відмова через відсутність вільних IP-адрес – Event ID 20. Конфлікт

IP-адрес – Event ID 30. Можна профільтрувати журнал для знаходження помилок для їх подальшого виправлення.

Логи DHCP також зберігаються у файлах на диску за адресою «C:\Windows\System32\dhcp». Файли мають назви DhcpSrvLog-XXX.log, де XXX – це день тижня написаний англійською мовою (Mon, Tue, Wed…). Відкриваємо файл за допомогою Блокнота (Блокнот / Notepad) або іншого текстового редактора (рис. 14.18).

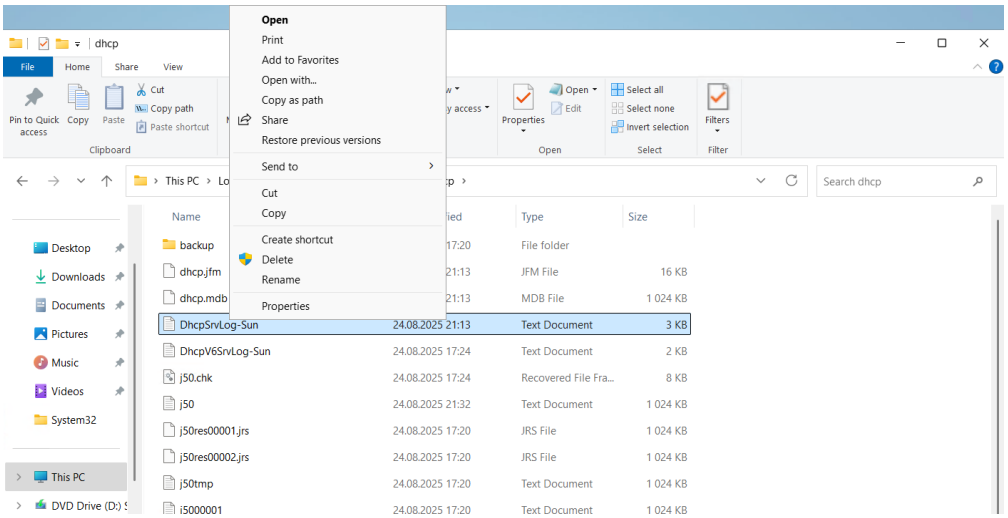


Рисунок 14.18 – Приклад текстового журналу DHCP-сервера на диску

У цих логах можна знайти записи: DHCPDISCOVER – клієнт шукає сервер, DHCPOFFER – сервер пропонує IP, DHCPREQUEST – клієнт запитує IP, DHCPACK – сервер підтверджує видачу, DHCPNACK – відмова у видачі адреси.

Щодо виправлення помилок, то типові помилки – це якщо клієнти не отримують IP-адреси – перевіряємо чи є вільні адреси у діапазоні; якщо є конфлікти – перевіряємо Event ID 30 (конфлікт) та уточнюємо, чи немає статичних IP в межах діапазону; якщо DHCP не запускається – перевіряємо службу у Службах (Services.msc).

Практична робота 15
Налаштування мережевих служб у Linux

Мета роботи: закріпити практичні навички налаштування мережевих служб у Linux, зокрема конфігурації статичних IP-адрес, встановлення та адміністрування SSH-сервера, а також опанувати інструменти моніторингу мережевої активності. Виконання роботи спрямоване на формування компетентностей із забезпечення стабільного мережевого підключення, віддаленого управління сервером та контролю використання мережевих ресурсів у серверному середовищі Linux [34-37].

Хід роботи

Завдання 1. Налаштування статичної IP

Запускаємо Linux Server розгорнутий. Входимо в систему під своїм користувачем. Відкриваємо «Параметри» (Settings), далі розділ «Мережа» (Network). У списку інтерфейсів «Wired» (провідне з'єднання) натискаємо на піктограму шестерні (рис. 15.1).

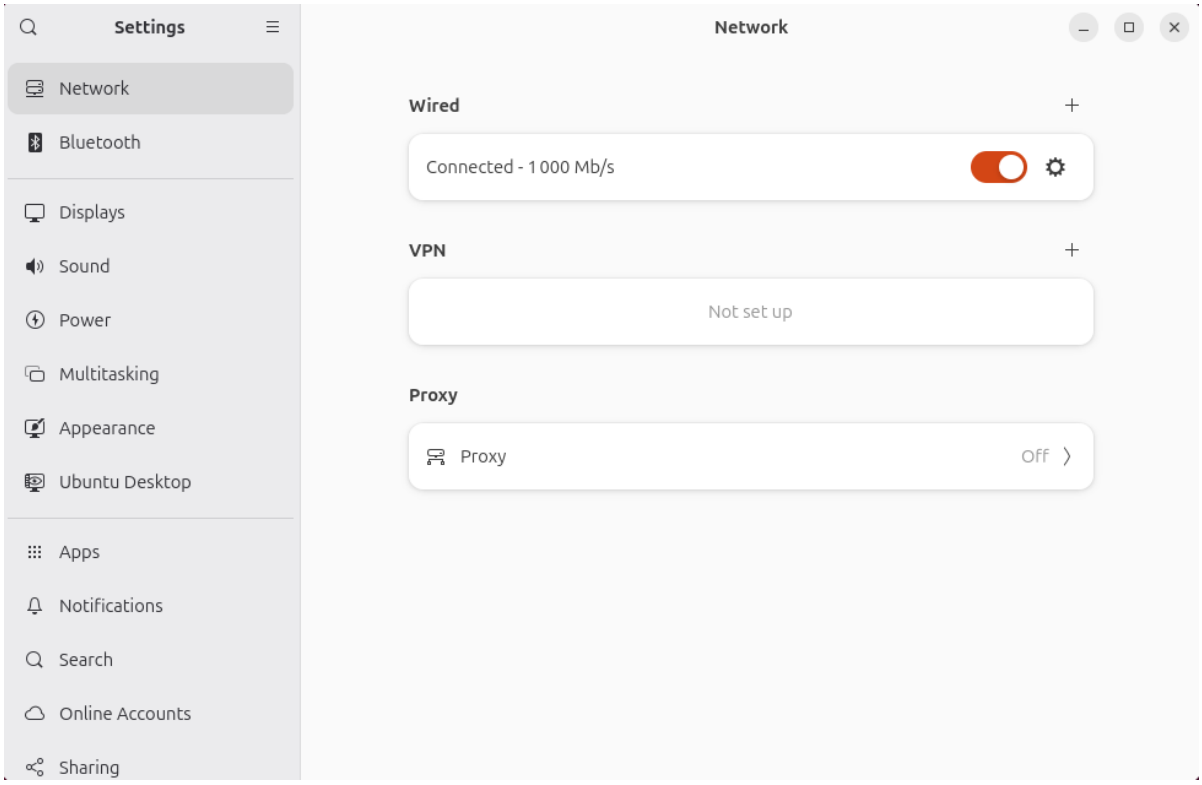


Рисунок 15.1 – Вікно «Налаштування мережі»

В результаті цього відкривається вікно налаштувань підключення. Переходимо у вкладку «IPv4», у вікні, що відкрилося (рис. 15.2).

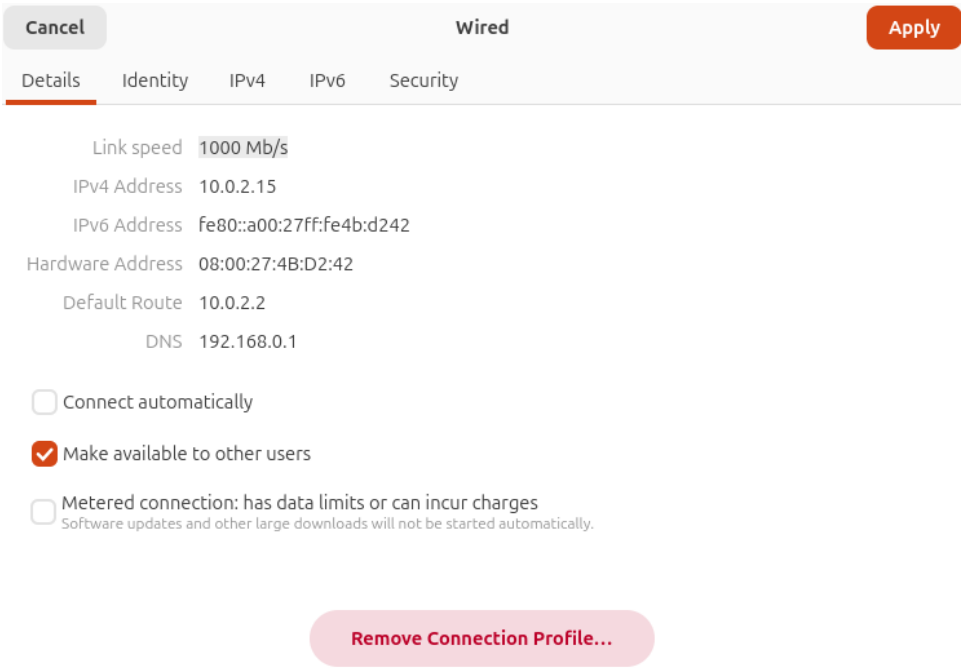


Рисунок 15.2 – Вікно «Налаштування провідного з’єднання мережі»

Відкривши вкладку «IPv4» у полі «Метод» обираємо «Manual» (Ручний). У полі «Addresses» додаємо: Address: 192.168.56.10; Netmask: 255.255.255.0; Gateway: 192.168.56.1. Зберігаємо налаштування натиснувши «Apply», вимикаємо/вмикаємо інтерфейс (або просто відключаємо і підключаємо мережу) (рис. 15.3).

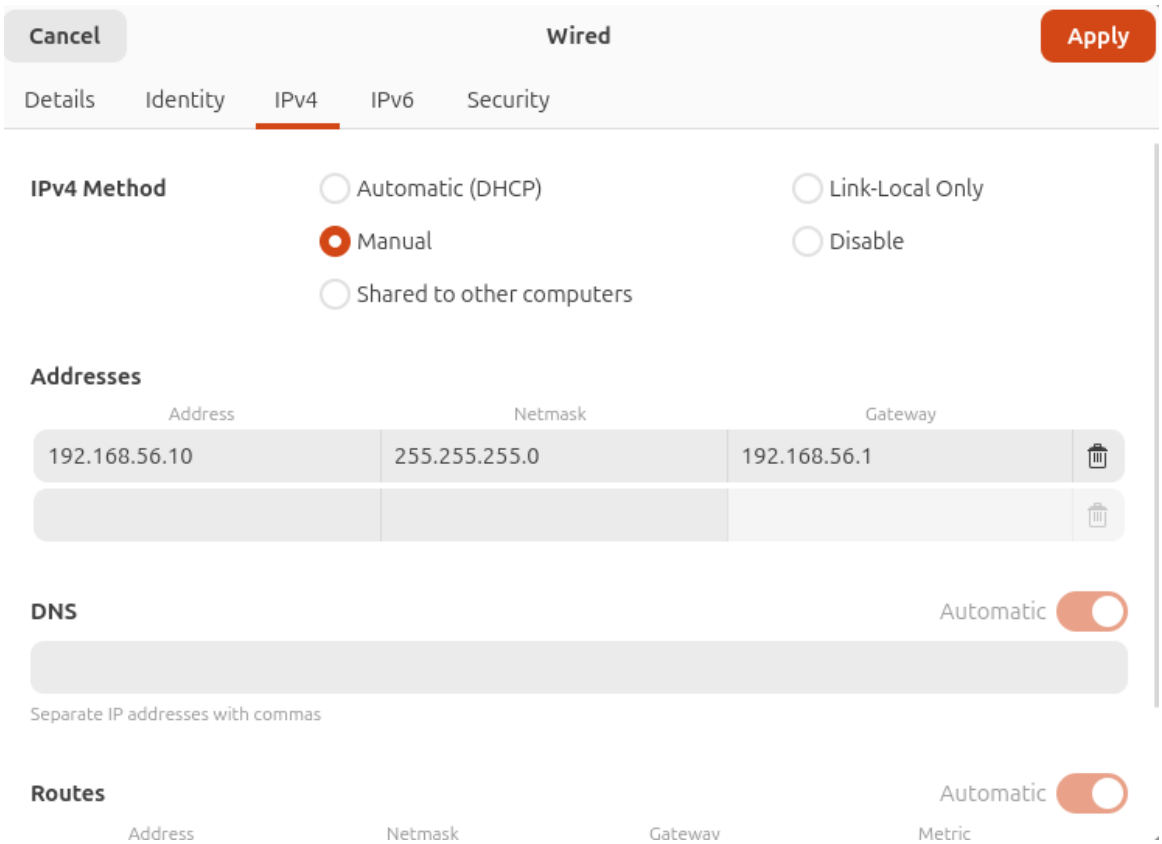


Рисунок 15.3 – Налаштування статичної IP-адресації для сервера

Після цього перевіряємо підключення та налаштування статичних IP-адрес. Для цього у терміналі виконуємо «ip addr show», «ping -c 4 192.168.56.1», «ping -c 4 8.8.8.8». Якщо команди виконалися коректно, відповідно налаштування статичної IP застосовано.

Завдання 2. Встановлення та налаштування SSH-сервера

Для встановлення SSH-сервера в терміналі застосовуємо команди «sudo apt update» та після неї команду «sudo apt install openssh-server –y» (рис. 15.4-15.5).

```
administrator@adminserv:~$ sudo apt install openssh-server -y
Наступні пакунки були встановлені автоматично і більше не потрібні:
  linux-headers-6.14.0-15          linux-modules-extra-6.14.0-15-generic
  linux-headers-6.14.0-15-generic  linux-tools-6.14.0-15
  linux-modules-6.14.0-15-generic  linux-tools-6.14.0-15-generic
Використовуйте 'sudo apt autoremove' щоб видалити їх.

Installing:
  openssh-server
```

Рисунок 15.4 – Введення команд для встановлення SSH-сервера

```
administrator@adminserv: ~
(Reading database ... 198120 files and directories currently installed.)
Preparing to unpack .../openssh-sftp-server_1%3a9.9p1-3ubuntu3.1_amd64.deb ...
Unpacking openssh-sftp-server (1:9.9p1-3ubuntu3.1) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a9.9p1-3ubuntu3.1_amd64.deb ...
Unpacking openssh-server (1:9.9p1-3ubuntu3.1) ...
Selecting previously unselected package ncurses-term.
Preparing to unpack .../ncurses-term_6.5+20250216-2_all.deb ...
Unpacking ncurses-term (6.5+20250216-2) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_5.11-0ubuntu3_all.deb ...
Unpacking ssh-import-id (5.11-0ubuntu3) ...
Setting up openssh-sftp-server (1:9.9p1-3ubuntu3.1) ...
Setting up openssh-server (1:9.9p1-3ubuntu3.1) ...
Creating config file /etc/ssh/sshd_config with new version
Created symlink '/etc/systemd/system/sockets.target.wants/ssh.socket' → '/usr/lib/system
d/system/ssh.socket'.
Created symlink '/etc/systemd/system/ssh.service.requires/ssh.socket' → '/usr/lib/system
d/system/ssh.socket'.
Setting up ssh-import-id (5.11-0ubuntu3) ...
Setting up ncurses-term (6.5+20250216-2) ...
Processing triggers for man-db (2.13.0-1) ...

Progress: [ 94%] [                                                    ]
```

Рисунок 15.5 – Процес встановлення SSH-сервера

Після встановлення перевіряємо роботу служби SSH-сервера. Для цього використовуємо команду «sudo systemctl status ssh» в терміналі. Також після цього перевіряємо, чи «слухає» сервер порт 22 командою «ss -tlnp | grep 22» (рис. 15.6).

```
administrator@adminserv:~$ sudo systemctl status ssh
○ ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
     Active: inactive (dead)
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
administrator@adminserv:~$
administrator@adminserv:~$
administrator@adminserv:~$ ss -tlnp | grep 22
LISTEN 0      4096         0.0.0.0:22        0.0.0.0:*
LISTEN 0      4096            [::]:22           [::]:*
administrator@adminserv:~$
```

Рисунок 15.6 – Перевірка встановлення та роботи SSH-сервера

Для змінення налаштувань SSH слід відкрити конфігураційний файл, що міститься за адресою «/etc/ssh/ssh_config». Там знайшовши потрібне поле провести зміни. Після зміни виконуємо перезапуск SSH-сервера командою «sudo systemctl restart ssh» (рис. 15.7).

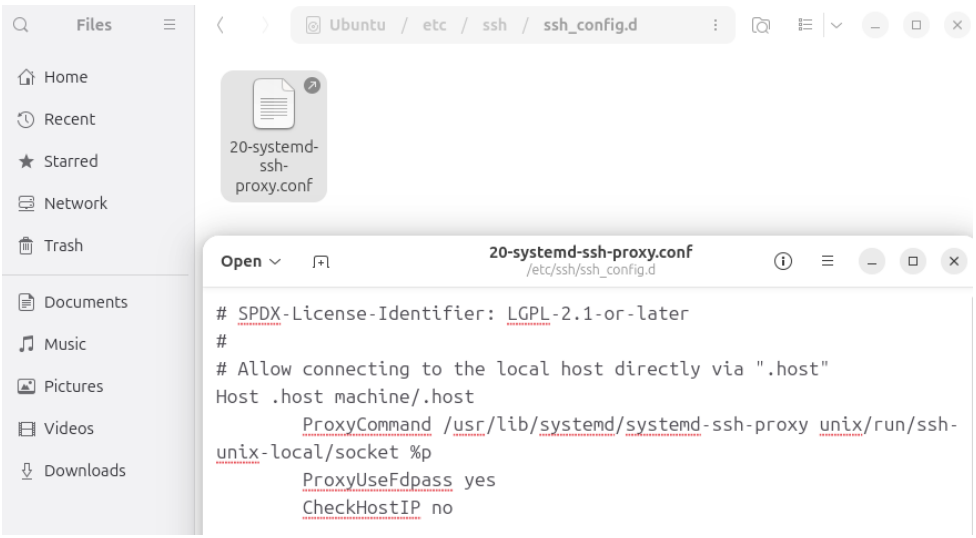


Рисунок 15.7 – Файл конфігурації SSH-сервера

Для подальшого правильного функціонування SSH-сервера проводимо налаштування відповідних параметрів брандмауера. Для цього в терміналі «вводимо команду «sudo ufw allow 22/tcp» та наступну команду «sudo ufw enable». Коли ці дії зроблено, то SSH-сервер має коректно працювати (рис. 15.8).

```
administrator@adminserv: ~
administrator@adminserv:~$ sudo ufw allow 22/tcp
[sudo] password for administrator:
Rules updated
Rules updated (v6)
administrator@adminserv:~$
administrator@adminserv:~$ sudo ufw enable
Firewall is active and enabled on system startup
administrator@adminserv:~$
```

Рисунок 15.8 – Налаштування брендмауера для роботи SSH-сервера

Завдання 3. Моніторинг мережевої активності у Linux

Для моніторингу мережевої активності у Linux відкриваємо «Додатки», там шукаємо групу додатків «Система», тиснемо на неї і там обираємо «System Monitor» (Системний монітор). У вікні «Системного монітора» переходимо у вкладку «Resources» (Ресурси). У розділі «Мережа» відображаються: швидкість прийому/передачі даних на сервері (RX/TX) та загальний обсяг переданих даних (рис. 15.9).

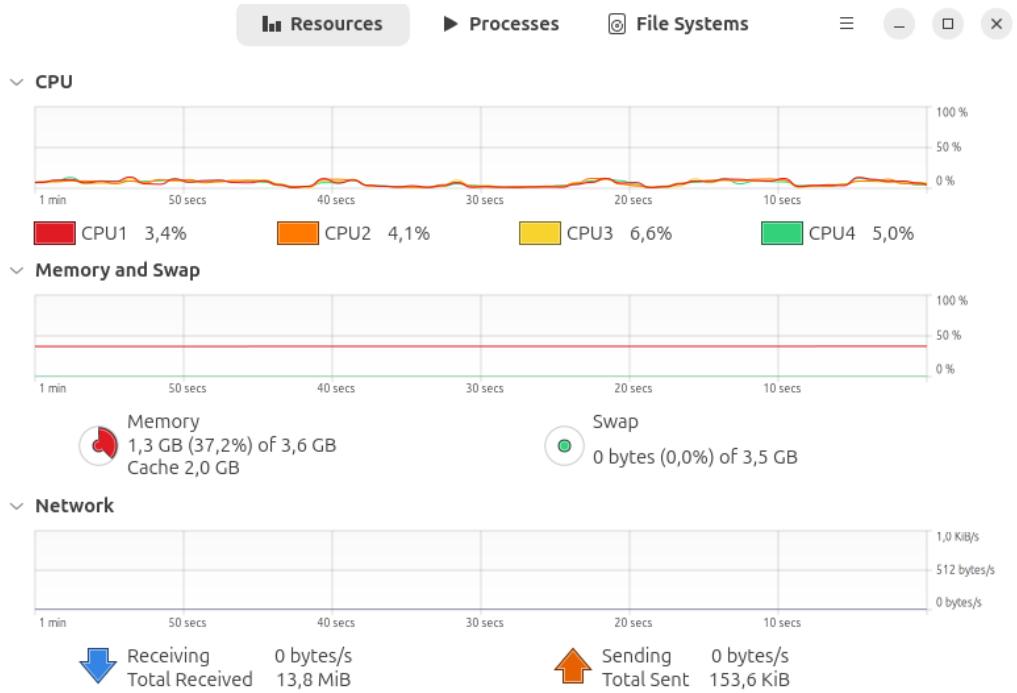


Рисунок 15.9 – Моніторинг мережевої активності у вікні «Системного монітора»

Також у вкладці «Processes» (Процеси) можна відсортувати процеси та подивитися, які програми активно використовують мережу.

Моніторинг мережевої активності можна також здійснювати у терміналі. Активні з’єднання переглядаємо командою «ss –tulpn». Дана команда показує активні сокети, протоколи, порти й процеси (рис. 15.10).

Рисунок 15.10 – Моніторинг активних сокетів, протоколів, портів й процесів

Для моніторингу трафіку інтерфейсу встановлюємо в терміналі інструмент «iftop». Це виконується командою «sudo apt install iftop –y». Після цього запускаємо даний інструмент – «sudo iftop -i enp0s3». Замість «enp0s3» використовується назву інтерфейсу (рис. 15.11-15.12)

```
administrator@adminserv:~$ sudo apt install iftop -y
Наступні пакунки були встановлені автоматично і більше не потрібні:
  linux-headers-6.14.0-15          linux-modules-extra-6.14.0-15-generic
  linux-headers-6.14.0-15-generic  linux-tools-6.14.0-15
  linux-modules-6.14.0-15-generic  linux-tools-6.14.0-15-generic
Використовуйте 'sudo apt autoremove' щоб видалити їх.

Installing:
  iftop

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 18
  Download size: 33,5 kB
  Space needed: 87,0 kB / 5 297 MB available

Отр:1 http://ua.archive.ubuntu.com/ubuntu plucky/universe amd64 iftop amd64 1.0
pre4-9build2 [33,5 kB]
Отримано 33,5 kB за 0cB (205 kB/s)
```

Рисунок 15.11 – Встановлення інструменту моніторингу трафіку «iftop»

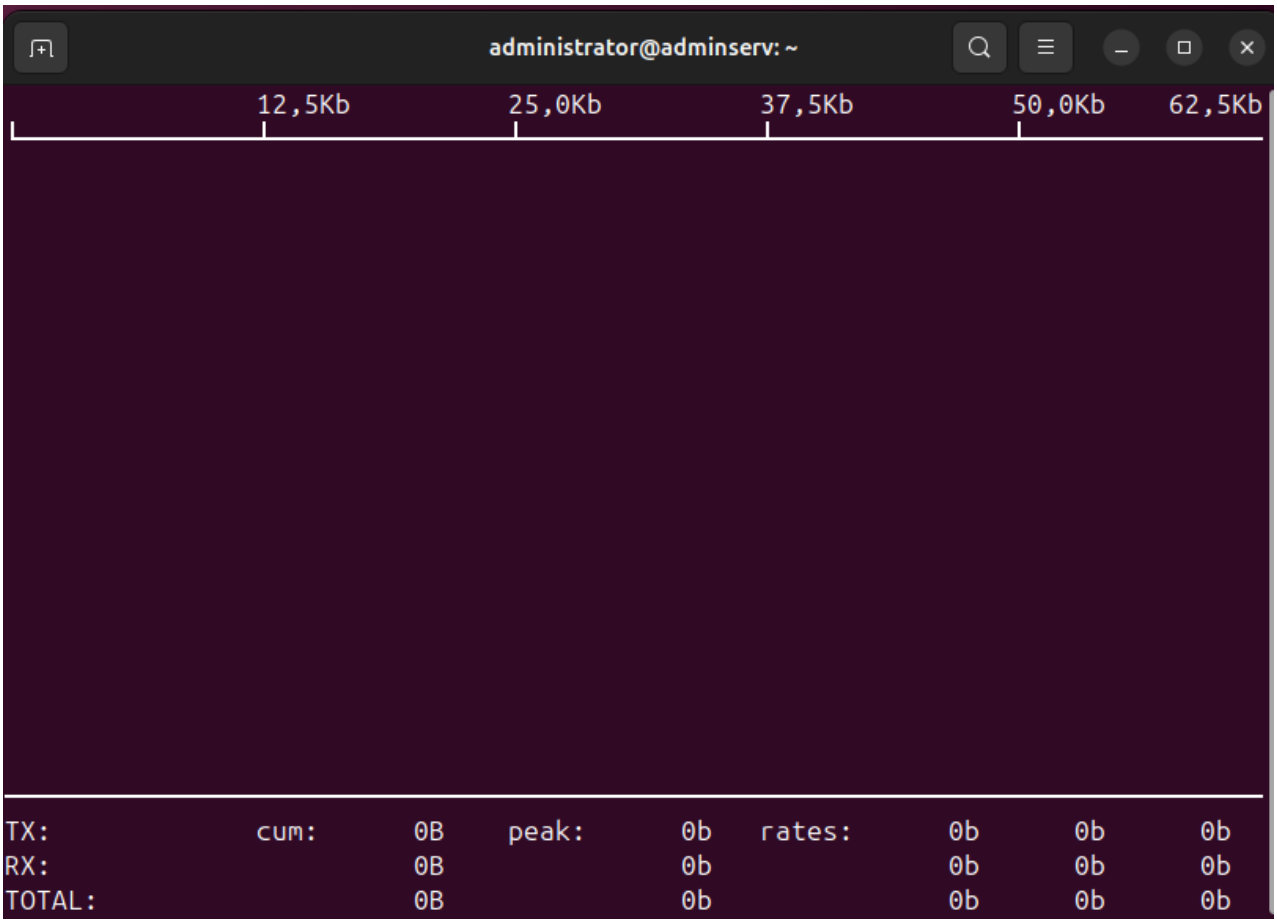


Рисунок 15.12 – Вікно роботи інструменту моніторингу трафіку «iftop»

Для моніторингу трафіку по процесах виконуємо встановлення «nethogs». Для цього вписуємо команду «sudo apt install nethogs –y» і встановлюємо даний інструмент. Після цього запускаємо – «sudo nethogs». Ця утиліта показує, які процеси створюють навантаження на мережу (рис. 15.13-15.14).

```
administrator@adminserv:~$ sudo apt install nethogs -y
Наступні пакунки були встановлені автоматично і більше не потрібні:
  linux-headers-6.14.0-15          linux-modules-extra-6.14.0-15-generic
  linux-headers-6.14.0-15-generic  linux-tools-6.14.0-15
  linux-modules-6.14.0-15-generic  linux-tools-6.14.0-15-generic
Використовуйте 'sudo apt autoremove' щоб видалити їх.

Installing:
  nethogs

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 18
  Download size: 37,0 kB
  Space needed: 99,3 kB / 5 297 MB available

Отр:1 http://ua.archive.ubuntu.com/ubuntu plucky/universe amd64 nethogs amd64 0.
8.8-1 [37,0 kB]
Отримано 37,0 kB за 0cB (166 kB/s)
```

Рисунок 15.13 – Встановлення інструменту моніторингу трафіку по процесах «nethogs»

```
administrator@adminserv: ~
NetHogs version 0.8.8-1

    PID USER     PROGRAM                  DEV        SENT      RECEIVED
      ? root     unknown TCP                         0.000      0.000 kB/s

  TOTAL                                              0.000      0.000 kB/s
```

Рисунок 15.14 – Вікно роботи інструменту моніторингу трафіку по процесах «nethogs»

Для моніторингу статистики інтерфейсів та помилок в передачі мережевого трафіку застосовується команда «ip -s link». Дана команда виведе статистику по кожному мережевому інтерфейсу (пакети, помилки тощо) (рис. 15.15).

```
administrator@adminserv:~$ ip -s link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
 group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    RX:  bytes packets errors dropped  missed   mcast
         92770    1114      0       0       0       0
    TX:  bytes packets errors dropped carrier collsns
         92770    1114      0       0       0       0
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:4b:d2:42 brd ff:ff:ff:ff:ff:ff
    RX:  bytes packets errors dropped  missed   mcast
      14535503    9793      0       0       0       0
    TX:  bytes packets errors dropped carrier collsns
        161671    1853      0       0       0       0
    altname enx0800274bd242
administrator@adminserv:~$
```

Рисунок 15.15 – Моніторинг статистики інтерфейсів, пакетів та помилок в терміналі Linux Server

Моніторинг мережевої активності у Linux дозволяє контролювати використання мережевих ресурсів, виявляти аномалії та потенційні загрози, а також оптимізувати продуктивність системи. Використовуючи інструменти як ss, iftop, nethogs та графічні утиліти в GNOME, адміністратор може отримувати детальну інформацію про з’єднання, трафік та активні процеси. Регулярний моніторинг підвищує безпеку та стабільність серверного середовища.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Курс мережевої академії Cisco Packet Tracer (Курс-інструкція до симулятору мереж та IoT). Доступний з URL: http://surl.li/mimft (дата звернення: 11.10.2024).

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: 10.12.2024)

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: 20.05.2025).

17. Networking101Lite Сесія №10 «Динамічна маршрутизація/bgp». URL: http://surl.li/eoivr (дата звернення: 23.05.2025)

18. Active Directory overview - Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-

us/troubleshoot/windows-server/active-directory/active-directory-overview?utm_source=chatgpt.com (date of access: 23.05.2025).

19. Install Active Directory Domain Services on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-?utm_source=chatgpt.com (date of access: 23.05.2025).
20. Install Active Directory Domain Services on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-?utm_source=chatgpt.com (date of access: 02.06.2025).
21. Active Directory Domain Services overview. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview?utm_source=chatgpt.com (date of access: 05.06.2025).
22. Group Policy overview for Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview (date of access: 07.06.2025).
23. Group Policy preferences in Windows. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-preferences (date of access: 07.06.2025).
24. Group Policy Management Console in Windows. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-management-console (date of access: 07.06.2025).
25. The Admin's Guide to Group Policy Best Practices | Netwrix. Data Security that Starts with Identity| Netwrix. URL: https://netwrix.com/en/resources/guides/group-policy-best-practices/ (date of access: 10.06.2025).
26. Group Policy Management Guide. Active Directory Pro. URL: https://activedirectorypro.com/group-policy-guide/ (date of access: 10.06.2025).
27. Group Policies and Group Policies Preferences (2025). Hybrid Infrastructure and Cloud Architecture. URL: https://hartiga.de/windows-server/group-policies-foundation/ (date of access: 10.06.2025).
28. Install and Configure DNS Server on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/dns/quickstart-install-configure-dns-server?utm_source=chatgpt.com&tabs=powershell (date of access: 10.06.2025).
29. Manage DNS zones using DNS server in Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/dns/manage-dns-zones?utm_source=chatgpt.com&tabs=powershell (date of access: 10.06.2025).

30. What is DHCP Server in Windows Server?. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top (date of access: 10.06.2025).
31. Install and configure DHCP Server on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/quickstart-install-configure-dhcp-server?tabs=powershell (date of access: 10.06.2025).
32. Guidance for troubleshooting DHCP - Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/troubleshoot-dhcp-guidance (date of access: 10.06.2025).
33. Migrate existing DHCP failover deployment on Windows Server. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/migrate-existing-dhcp-failover?tabs=powershell (date of access: 10.06.2025).
34. Configuring IIS for Web Hosting on Windows: A Step-by-Step Guide. Kamatera. URL: https://www.kamatera.com/knowledgebase/configuring-iis-for-web-hosting-on-windows/ (date of access: 15.06.2025).
35. Ubuntu Server documentation. Ubuntu Server. URL: https://documentation.ubuntu.com/server/ (date of access: 15.06.2025).
36. Munna R. Linux DNS Server Configuration: Detailed Guide [2025]. MailServerGuru. URL: https://mailserverguru.com/linux-dns-server/?utm_source=chatgpt.com#Master-Update-the-System (date of access: 15.06.2025).
37. Imron M. Guide to Creating a Simple Web Server Using Nginx and Apache2. Medium. URL: https://medium.com/@muhammadimron1410/guide-to-creating-a-simple-web-server-using-nginx-and-apache2-ae7d27b421c6 (date of access: 15.06.2025).

Для нотаток

І-74 Інформаційні мережі та адміністрування: методичні вказівки до практичних занять для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 (F) Інформаційні технології спеціальності 126 (F6) Інформаційні системи та технології денної та заочної форм навчання / уклад. Н. В. Багнюк, К. Я. Бортник. Луцьк: ЛНТУ, 2025. 132 с.

Методичне видання до практичних занять з дисципліни «Інформаційні мережі та адміністрування» складене відповідно до діючої програми курсу.

Призначене для здобувачів вищої освіти спеціальності 126 (F6) Інформаційні системи та технології освітньої програми «Інформаційні системи та технології охорони і безпеки».

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