

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»



ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра інформаційних технологій та комп'ютерної інженерії

В.Ю. Каштан, Я.В. Панферова, Л.В. Бешта

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання лабораторних робіт
для здобувачів ступеня бакалавра
спеціальності F7 Комп'ютерна інженерія

У 2 частинах

Частина 2

Дніпро
НТУ «ДП»
2026

Комп'ютерні мережі [Електронний ресурс] : методичні рекомендації до виконання лабораторних робіт з дисципліни «Комп'ютерні мережі» для здобувачів ступеня бакалавра спеціальності F7 Комп'ютерна інженерія : у 2 ч. / уклад.: В.Ю. Каштан, Я.В. Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2026. – Ч. 2. – 50 с.

Укладачі:

В.Ю. Каштан, канд. техн. наук, доц.;

Я.В. Панферова, асист.;

Л.В. Бешта, асист.

Затверджено науково-методичною комісією зі спеціальності F7 Комп'ютерна інженерія (протокол № 6 від 09.06.2026 р.) за поданням кафедри інформаційних технологій та комп'ютерної інженерії (протокол № 21 від 09.06.2026 р.).

Методичні рекомендації містять опис методики виконання лабораторних робіт з дисципліни «Комп'ютерні мережі» студентами спеціальності F7 Комп'ютерна інженерія.

Орієнтовано на активізацію навчальної діяльності бакалаврів та закріплення практичних навичок з даної дисципліни.

Відповідальний за випуск завідувач кафедри інформаційних технологій та комп'ютерної інженерії В.В. Гнатушенко, д-р техн. наук, проф.

ЗМІСТ

1 Лабораторна робота №1. Налаштування статичних маршрутів і маршрутів за умовчанням для IPv4.....	7
1.1 Мета лабораторної роботи.....	7
1.2 Організація виконання лабораторної роботи	7
1.3 Зміст звіту.....	10
1.4 Питання для підготовки до захисту лабораторної роботи.....	10
2 Лабораторна робота № 2. Налаштування динамічного протоколу маршрутизації EIGRP	11
2.1 Мета лабораторної роботи.....	11
2.2 Організація виконання лабораторної роботи	11
2.3 Зміст звіту.....	14
2.4 Питання для підготовки до захисту лабораторної роботи.....	14
3 Лабораторна робота №3. Централізовані алгоритми маршрутизації. Алгоритм Дейкстри.	15
3.1 Мета лабораторної роботи.....	15
3.2 Організація виконання лабораторної роботи	15
3.3 Зміст звіту.....	16
3.4 Питання для підготовки до захисту лабораторної роботи.....	16
4 Лабораторна робота №4. Налаштування мереж VLAN, протоколів DTP та VTP, та маршрутизації між VLAN	17
4.2 Мета лабораторної роботи.....	17
4.3 Організація виконання лабораторної роботи	17
4.4 Зміст звіту.....	22
4.5 Питання для підготовки до захисту лабораторної роботи.....	23
5 Лабораторна робота №5. Налаштування маршрутизатора як сервера DHCP	24
5.1 Мета роботи	24
5.2 Організація виконання лабораторної роботи	24
5.3 Зміст звіту.....	25
5.4 Питання для підготовки до захисту лабораторної роботи.....	25
6 Лабораторна робота №6. Налаштування бездротової мережі Meraki	27
5.1 Мета роботи	27
5.2 Організація виконання лабораторної роботи	27
6.3 Зміст звіту.....	33
6.4 Питання для підготовки до захисту лабораторної роботи.....	33
7 Лабораторна робота №7. Налаштування статичного, динамічного NAT та PAT.....	34
7.1 Мета роботи	34
7.2 Організація виконання лабораторної роботи	34
7.3 Зміст звіту.....	37
7.4 Питання для підготовки до захисту лабораторної роботи.....	38
8 Лабораторна робота №8. Дослідження керування мережею на основі командного рядка та контролера SDN	39

8.1 Мета роботи	39
8.2 Організація виконання лабораторної роботи	39
8.3 Зміст звіту.....	46
8.4 Питання для підготовки до захисту лабораторної роботи.....	46
Додаток А. Скрип на мові Python для збору інформації по мережні пристрої.....	48
Список рекомендованих джерел.....	49

ВСТУП

Методичні рекомендації призначені для студентів спеціальності F7 Комп'ютерна інженерія, що вивчають дисципліну «Комп'ютерні мережі».

Методичні вказівки включають низку частково взаємопов'язаних робіт, після виконання яких студенти можуть вміти:

- налаштовувати і перевіряти статичну маршрутизацію і маршрутизацію за замовчуванням;

- налаштовувати і перевіряти роботу протоколу RIPv2, EIGRP, OSPF та усувати неполадки, пов'язані з ними;

- впроваджувати на комутаторах функцію Switch Port Security;

- створювати логічно розділені мережі VLAN та налаштовувати маршрутизацію між ними;

- розуміти принципи роботи та налаштування різних типів списків контролю доступу (ACL) для мереж IPv4;

- налаштовувати маршрутизатори Cisco в якості DHCP-серверів для мереж IPv4;

- розуміти принципи роботи та налаштування перетворення мережних адрес (NAT) для мереж IPv4;

- керувати мережею через централізований SDN-контролер.

Перед виконання лабораторної роботи студенти повинні:

- ознайомитися з методичними вказівками;

- повторити лекційний матеріал, пов'язаний з лабораторною роботою;

- підготувати відповіді на питання, які наведені у методичних вказівках наприкінці кожної лабораторної роботи.

Виконавши ці завдання, студент повинен продемонструвати викладачеві роботу на комп'ютері або в зошиті, оформити звіт за результатами даної лабораторної роботи, захистити його та здати викладачеві.

Загальні вимоги до виконання лабораторної роботи, що мають забезпечити максимальну оцінку:

- повна відповідність звіту про виконання лабораторної роботи методичним рекомендаціям;

- володіння теоретичним матеріалом про предмет досліджень;

- загальна та професійна грамотність, лаконізм та логічна послідовність викладу матеріалу;

- відповідність оформлення звіту чинним стандартам.

При своєчасному (протягом двох тижнів від дати проведення заняття) та вірному виконанні завдання здобувач отримує оцінку 10. з яких:

- 8 балів: виконання та оформлення лабораторної роботи;

- 2 бали: захист лабораторної роботи.

При несвоєчасному виконанні завдання -1 бал за кожен прострочений тиждень.

Критерії оцінювання лабораторних робіт:

Бали за виконання та оформлення	
8	роботу виконано повністю, налаштування правильні, результати перевірено, звіт оформлено належним чином;
6-7	роботу виконано переважно правильно, але наявні окремі неточності, які не впливають істотно на загальний результат;
4-5	роботу виконано частково, наявні помилки в налаштуваннях або недостатньо представлено результати перевірки;
1-3	виконано лише окремі етапи, мережа працює частково, звіт неповний;
0	роботу не виконано або поданий результат не відповідає завданню.
Бали за захист	
2	здобувач упевнено пояснює виконані налаштування й отримані результати та правильно відповідає на запитання;
1	здобувач розуміє основний зміст роботи, але допускає неточності у відповідях;
0	здобувач не може пояснити виконання роботи та не відповідає на основні запитання.

1 ЛАБОРАТОРНА РОБОТА №1.

НАЛАШТУВАННЯ СТАТИЧНИХ МАРШРУТІВ І МАРШРУТІВ ЗА УМОВЧАННЯМ ДЛЯ IPV4

1.1 Мета лабораторної роботи

Налаштування статичних маршрутів і маршрутів за умовчанням на маршрутизаторах мережі організації з метою забезпечення взаємодії між всіма ПК.

1.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки, такі питання:

- принцип дії та конфігурація статичних маршрутів;
- принцип дії та конфігурація маршрутів за умовчанням;
- принцип дії та налаштування плаваючого статичного маршруту;
- перевірка маршрутної інформації.

Вихідні дані: налаштована мережа з лабораторної роботи «Впровадження і налаштування сервісів веб-серверу, серверу електронної пошти, DHCP, DNS та FTP» відповідно до методичних рекомендацій [8].

Для обміну даними між підмережами організації потрібно визначити маршрути для їх досягнення і ввести їх в таблиці маршрутизації. Для цього необхідно вручну налаштувати статичні маршрути. Для доступу в Інтернет необхідно налаштувати маршрути за замовчуванням. У цьому завданні використовуються три різних статичних маршрути: рекурсивний статичний маршрут, безпосередньо підключений статичний маршрут і маршрут за замовчуванням.

Для додавання надмірності в випадку втрати зв'язку між Filial1 та Central необхідно додати резервний канал по Serial і налаштувати плаваючі статичні маршрути.

Далі виконати наведені кроки.

Крок 1. Перевірка конфігурацій

1. Перевірте досяжність мереж, відправивши echo-запити по табл. 1.1, та дайте пояснення. На даний момент ПК не можуть відправляти echo-запити на ПК в віддалені підмережі.

Таблиця 1.1 – Результат перевірки досяжності мереж командою «ping»

Від ПК в мережі	До ПК в мережі	Так/ні	Пояснення
LAN1	LAN2		
LAN3	LAN4		
LAN5	LAN6		
LAN1	LAN3		
LAN1	LAN5		
LAN3	LAN5		
LAN1	Internet Server		

2. Використовуйте команду «show ip route» щоб переглянути таблицю маршрутизації на кожному маршрутизаторі. Кожен маршрутизатор покаже тільки свої мережі, безпосередньо з'єднані з ним. Занотуйте їх у звіт з лабораторної роботи.

Крок 2. Налаштування та перевірка статичних маршрутів на маршрутизаторах організації

1. На Filial1 налаштуйте рекурсивні статичні маршрути до всіх віддалених підмереж організації, вказавши в якості наступного переходу IP-адресу інтерфейсу маршрутизатора Central на протилежному кінці. Синтаксис команди:

```
Router(config)# ip route <NETWORK-ADDRESS> <SUBNET-MASK> <IP-ADDRESS>
```

2. На Central налаштуйте безпосередньо підключені статичні маршрути до всіх віддалених підмереж організації, вказавши відповідний Ethernet-інтерфейс в якості вихідного. Синтаксис команди:

```
Router(config)# ip route <NETWORK-ADDRESS> <SUBNET-MASK> <EXIT-INTF>
```

Примітка: не звертайте увагу на попереджувальне повідомлення «%Default route without gateway, if not a point-to-point interface, may impact performance». Це означає, що маршрутизатор кожного разу буде застосовувати ARP для кінцевого пункту призначення замість IP-адреси наступного переходу. Це може призвести до надмірного ARP-трафіку на цьому інтерфейсі, уповільнюючи продуктивність вашої мережі на вихідних даних до Інтернету.

3. Перевірте досяжність мереж, відправивши echo-запити по табл. 1.1. Обґрунтуйте зміни в новій таблиці.

4. На Filial2 налаштуйте статичні маршрути до всіх віддалених підмереж організації будь-яким пропонованим раніше способом.

5. Перевірте досяжність мереж, відправивши echo-запити по табл. 1.1. Обґрунтуйте зміни в новій таблиці.

6. Виберіть кожен маршрутизатор організації і перегляньте таблицю маршрутизації. Переконайтеся, що таблиці маршрутизації мають відомості про всі підмережі організації та занотуйте їх у звіт.

Крок 3. Налаштування та перевірка маршрутів за замовчуванням та доступу в Інтернет

У таблицях маршрутизації не може бути маршрутів для всіх можливих вузлів мережі Інтернет. В корпоративних середовищах маршрути за замовчуванням виводять Інтернет-трафік з мережі до ISP.

Маршрут за замовчуванням, вказує який шлюз використовувати, якщо в таблиці маршрутизації немає шляху до адреси призначення. Маршрути за замовчуванням вказують наступний маршрутизатор на шляху до ISP. У команді використовується або IP-адреса наступного переходу, або вихідний інтерфейс.

Синтаксис команд налаштування маршруту за замовчуванням:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 {IP-ADDRESS | EXIT-INTF}
```

LAN1 та LAN2, LAN3 та LAN4 – це ще тупикові мережі. Тупикова мережа – це сценарій, коли маршрутизатор має лише одне пряме фізичне з'єднання з іншим маршрутизатором. Оскільки вони мають лише одне з'єднання, то можна спростити конфігурацію та управління мережею, задавши тільки один запис маршруту за замовчуванням.

1. Виберіть Filial1. Видаліть всі статичні маршрути. Налаштуйте маршрут за замовчуванням з відповідним IP-адресом наступного переходу. Синтаксис команди:

2. Виберіть Filial2, видаліть всі статичні маршрути. Налаштуйте маршрут за замовчуванням використовуючи вихідний інтерфейс для передачі пакетів.

3. Виберіть Central. Оголосіть маршрут за замовчуванням до постачальника Internet-послуг ISP.

4. Оголосіть на маршрутизаторі ISP маршрут до загальної IP-адреси мережі організації будь-яким застосованим раніше способом.

5. Перевірте досяжність мереж, відправивши echo-запити по табл. 1.1. Обґрунтуйте зміни в новій таблиці.

6. На кожному маршрутизаторі перегляньте таблиці маршрутизації та занотуйте їх у звіт.

Крок 4. Налаштування плаваючого статичного маршруту

На випадок, якщо розірветься канал GigabitEthernet між Filial1 та Central, виконайте між ними резервне підключення по Serial, додавши модуль HWIC-2T на вкладці *Physical*, та налаштуйте резервний плаваючий статичний маршрут.

1. Виконайте резервне підключення через Serial-кабель (Serial DCE або Serial DTE) між Filial1 та Central. Для підключення через даний кабель, необхідно додати інтерфейсну панель HWIC-2T на вкладці *Physical* у вікні властивостей кінцевого пристрою.

2. Надайте підключенню адреси з діапазону наступної WAN-мережі з префіксом /30.

3. З будь-якого вузла в Filial1 виконайте трасування маршруту до Internet Server.

```
PC> tracert 123.123.0.10
```

4. На Filial1 налаштуйте безпосередньо підключений плаваючий статичний маршрут за замовчуванням, адміністративна дистанція якого дорівнює AD=5. Маршрут повинен мати напрямок до Central.

```
Router(config)# ip route network-address subnet-mask {IP-ADDRESS | EXIT-INTF} [DISTANCE]
```

5. Перегляньте поточну конфігурацію «show running-config» і переконайтеся, що в цій конфігурації міститься плаваючий статичний маршрут за замовчуванням, а також статичний маршрут за замовчуванням.

6. Перегляньте і занотуйте у звіт таблицю маршрутизації. Чи видно плаваючий статичний маршрут в таблиці маршрутизації? Обґрунтуйте відповідь.

7. На Central налаштуйте плаваючі статичні маршрути до мереж LAN1 та LAN2 для формування резервних шляхів до них в разі обриву основного маршруту між Filial1 та Central.

8. Виконайте обрив основного маршруту між Filial1 та Central, відключивши на Filial1 вихідний GigabitEthernet-інтерфейс.

Filial1(config-if)# shutdown

9. Переконайтеся в тому, що маршрут за замовчуванням міститься в таблиці маршрутизації.

10. Від будь-якого вузла в Filial1 виконайте трасування маршруту до вузла до Internet Server. Чи був виконаний перехід на резервний маршрут? Занотуйте у звіт таблиці маршрутизації на Filial1 та Central.

11. Відновіть підключення до основного маршруту на Filial1.

Filial1(config-if) # no shutdown

12. Виконайте трасування маршруту від вузла будь-якого вузла в Filial1 до Internet Server, щоб переконатися в успішному відновленні основного маршруту.

1.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- схему логічної топології мережі;
- команди налаштування маршрутів на кожному кроці з поясненнями;
- перевірки досяжності мереж у вигляді таблиці 1.1;
- таблиці маршрутизації після кожного кроку виконання лабораторної роботи;
- відповіді на поставлені питання;
- проект мережі з назвою за правилом *Surname_Group_lab1_KM.pkt* (наприклад, *Ivanov_KI-25-1_lab1_KM.pkt*).

1.4 Питання для підготовки до захисту лабораторної роботи

1. Яке значення адміністративної дистанції має статичний маршрут?
2. У чому різниця між кодами C, S і S*, зазначеними поруч з маршрутами в таблиці маршрутизації?
3. Як налаштовується плаваючий статичний маршрут для забезпечення резервного підключення?
4. Поясніть процес обробки маршрутизатором пакетів при використанні рекурсивного статичного маршруту.
5. Які параметри наступного переходу можуть бути зазначені в синтаксисі команди налаштування статичного маршруту?

2 ЛАБОРАТОРНА РОБОТА № 2.

НАЛАШТУВАННЯ ДИНАМІЧНОГО ПРОТОКОЛУ МАРШРУТИЗАЦІЇ EIGRP

2.1 Мета лабораторної роботи

Налаштувати та дослідити роботу протоколу EIGRP з метою забезпечення взаємодії між всіма ПК та доступу до Інтернет.

2.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки, такі питання:

- порядок роботи протоколу EIGRP;
- типи і формат повідомлень EIGRP;
- налаштування EIGRP на маршрутизаторах Cisco;
- перевірка маршрутної інформації.

Вихідні дані: налаштована мережа з лабораторної роботи «Впровадження і налаштування сервісів веб-серверу, серверу електронної пошти, DHCP, DNS та FTP» відповідно до методичних рекомендацій [8].

Для обміну даними між підмережами організації та для забезпечення доступу в Інтернет внутрішнім користувачам, потрібно визначити маршрути для їх досягнення і внести їх в таблиці маршрутизації. Для цього було прийнято рішення застосувати протокол динамічної маршрутизації EIGRP. При такому рішенні маршрути обчислюються автоматично.

Налаштуйте протокол EIGRP. Також врахуйте, що:

- маршрутизатори Filial1, Filial2 та Central повинні анонсувати лише безпосередньо підключені мережі організації;
- номер автономної системи EIGRP = 100;
- на маршрутизаторі Central повинен бути прописаний маршрут за замовчуванням до маршрутизатора ISP (в Інтернет);
- Central повинен поширити маршрут за замовчуванням на інші маршрутизатори EIGRP, щоб вузли могли отримати доступ до Internet;
- на ISP оголосити статичний маршрут до загальної IP-адреси мережі організації;
- для додавання надмірності в випадку втрати зв'язку між Filial1 та Central необхідно додати резервний канал по *Serial* і анонсувати його по EIGRP.

У разі успішного налаштування відповідно до вимог, всі вузли повинні мати можливість пінгувати один одного та Internet Server.

Далі виконати наведені кроки.

Крок 1. Перевірка конфігурацій

1. Перевірте досяжність мереж, відправивши echo-запити по табл. 1.1 з лабораторної роботи №1, та дайте пояснення.

2. Використовуйте команду «show ip route» щоб переглянути таблицю

маршрутизації на кожному маршрутизаторі. На даному кроці кожен маршрутизатор покаже тільки свої мережі, з'єднані безпосередньо з ним. Занотуйте їх у звіт з лабораторної роботи.

Крок 2. Налаштування та перевірка EIGRP

1. Виберіть маршрутизатор Filial1, увійдіть в режим глобальної конфігурації та увімкніть маршрутизацію EIGRP

```
Router(config)# router eigrp 100
```

2. Оголосіть напряму підключені мережі на маршрутизаторі Filial1 (LAN1, LAN2, WAN1) з інвертованою маскою. Синтаксис команди:

```
Router(config-router)#network <LAN> <WILDCARD_MASK>
```

3. Вимкніть на Filial1 поширення оновлень на всі локальні мережі. Синтаксис команди:

```
Router(config-router)#passive-interface <INTERFACE>
```

4. Виконайте аналогічні налаштування на Central, оголосивши безпосередньо підключені його мережі (LAN5, LAN6, WAN1, WAN2). Вимкніть поширення оновлень на всі локальні мережі.

Примітка. Після додавання інтерфейсу WAN1 у процес маршрутизації EIGRP з'явиться повідомлення відносин суміжності із сусідніми пристроєм Filial1.

```
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor .... is up: new adjacency
```

5. Після обміну повідомленнями між Filial1 та Central використовуйте команду «show ip route» для відображення таблиці маршрутизації на кожному маршрутизаторі. Чому на Filial1 та Central не відображаються підмережі Filial2 (LAN3 та LAN4)?

6. Оголосіть на Filial2 безпосередньо підключені його мережі з інвертованими масками та вимкніть поширення оновлень в локальні мережі.

7. Перевірте досяжність мереж, відправивши ехо-запити по табл. 1.1. Обґрунтуйте зміни в новій таблиці. Якщо EIGRP налаштований правильно, ехо-запити між усіма пристроями в підмережах організації мають бути успішними, але без доступу в Інтернет.

8. Відобразіть таблиці маршрутизації на даному кроці на кожному маршрутизаторі організації та занотуйте їх у звіт.

Крок 3. Налаштування та перевірка доступу до Інтернет

1. Виберіть маршрутизатор Central. Оголосіть маршрут за замовчуванням з відповідною IP-адресою наступного переходу Це викличе трафік до будь-якого невідомого адресу призначення до ISP, що імітує доступ в Інтернет.

```
Central(config)#ip route 0.0.0.0 0.0.0.0 <IP-ISP>
```

2. Маршрутизатор Central оголосить цей маршрут іншим маршрутизаторам в домені, якщо додати команду «redistribute static» в конфігурацію EIGRP.

```
Central(config-router)# redistribute static
```

3. Подивіться таблицю маршрутизації на Filial1 та Filial2. Чи забезпечується магістраль для Інтернет-трафіку в їх таблицях маршрутизації?

4. Оголосіть на маршрутизаторі ISP маршрут до загальної IP-адреси мережі організації.

5. Перевірте досяжність мереж, відправивши echo-запити по табл. 1.1. Обґрунтуйте зміни в новій таблиці.

6. Виберіть кожен маршрутизатор організації і перегляньте таблицю маршрутизації. Переконайтеся, що таблиці маршрутизації мають відомості про всі мережі та магістраль для Інтернет-трафіку. Занотуйте їх у звіт.

Додатково. В режим *Simulation Mode* натисніть на кнопку *Auto Capture Play* та поспостерігайте за розсилкою в мережі періодичних EIGRP-оновлень. Зверніть увагу на їх тип та середній інтервал, через який генеруються. Наприклад, вимкніть мережу LAN2. Поспостерігайте за тим, як відбувається конвергенція в мережі. За якою адресою відбувається розсилка EIGRP-повідомлень? Яка метрика присвоєна мережі LAN2 в таблицях маршрутизації? Простежте, через який час записи з даною мережею будуть віддалені з таблиць на інших маршрутизаторах? Щоб не очищався буфер повідомлень, встановіть поведінку буфера (рис.2.1). Потім відновіть підключення до мережі LAN2.

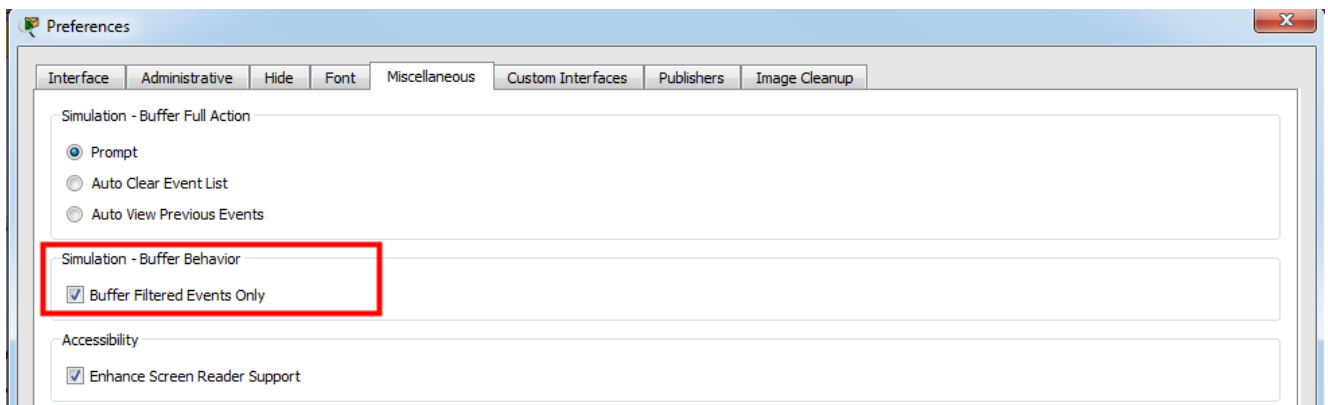


Рисунок 2.1 – Options->Preference

Крок 4. Налаштування резервного підключення між Filial1 та Central

1. Виконайте резервне підключення по оптоволоконному кабелю по Serial між Filial1 та Central. Пам'ятайте, що перед вимкненням живлення треба зберегти поточну конфігурацію.

1. Надайте підключенню адреси з діапазону наступної WAN-мережі з префіксом /30.

2. З будь-якого вузла в Filial1 виконайте трасування маршруту до вузла до Internet Server.

3. На Filial1 та Central в налаштуванні EIGRP оголосіть нову мережу.

4. Відобразіть таблицю маршрутизації на Central та занотуйте шлях та метрику до мереж LAN1 та LAN2.

5. Виконайте обрив основного маршруту між Filial1 та Central, відключивши на Filial1 вихідний GigabitEthernet-інтерфейс.

6. Відобразіть таблицю маршрутизації на Central та занотуйте зміни записів до мереж LAN1 та LAN2. Зверніть увагу на значення метрики.

7. Від будь-якого вузла в Filial1 виконайте трасування маршруту до вузла до Internet Server. Чи був виконаний перехід на резервний маршрут?

8. Відновіть підключення до основного маршруту на Filial1.

9. Виконайте трасування маршруту від вузла будь-якого вузла в Filial1 до Internet Server, щоб переконатися в успішному відновленні основного маршруту. Подивіться зміни в таблиці маршрутизації на Central.

Крок 5. Перевірка налаштувань EIGRP

1. На одному з маршрутизаторів організації введіть команди і вивчіть їх результати.

Router#show ip eigrp {interfaces | topology | neighbors | traffic}

Команда «show ip eigrp topology» дозволяє переглядати інформацію про маршрути, отримані від сусідів EIGRP.

Команда «show ip eigrp neighbors» дозволяє переглядати відносини суміжності, встановлених із сусідніми маршрутизаторами, які беруть участь у роботі протоколу EIGRP.

Команда «show ip eigrp interfaces» надає інформацію про інтерфейси, які беруть участь у роботі протоколу EIGRP та параметри їх взаємодії.

Командою «show ip protocols» перевіряється інформація про активовані протоколи маршрутизації та параметри їх функціонування та оголошені мережі.

2.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- схему логічної топології мережі;
- команди налаштування маршрутів на кожному кроці з поясненнями;
- перевірки досяжності мереж у вигляді табл. 1.1 після виконання кроків 1-4;
- таблиці маршрутизації після кожного кроку виконання лабораторної роботи;
- проект мережі з назвою за правилом *Surname_Group_lab2_KM.pkt*.

2.4 Питання для підготовки до захисту лабораторної роботи

1. Як розраховується метрика в протоколі EIGRP та змінити її значення?
2. Які існують типи пакетів EIGRP?
3. За яким IP-адресом розсилаються EIGRP-пакети HELLO?
4. Як EIGRP забезпечує відсутність виникнення петель маршрутизації?
5. В яких випадках маршрутизатори не зможуть встановити сусідство?

3 ЛАБОРАТОРНА РОБОТА №3.

ЦЕНТРАЛІЗОВАНІ АЛГОРИТМИ МАРШРУТИЗАЦІЇ. АЛГОРИТМ ДЕЙКСТРИ.

3.1 Мета лабораторної роботи

Вивчення алгоритму Дейкстри, що використовується в протоколі OSPF.

3.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки, такі питання:

- централізовані та децентралізовані алгоритми маршрутизації;
- маршрутизація в комп'ютерних мережах;
- алгоритм Дейкстри.

Комп'ютерна мережа представлена графом на рис. 3.1. Вершинам графа відповідають маршрутизатори, ребрам – канали зв'язку, а ваги ребер – метрики. У таблиці 3.1 представлені ваги ребер. Визначити найкоротший шлях від вузла А до всіх інших вузлів за алгоритмом Дейкстри.

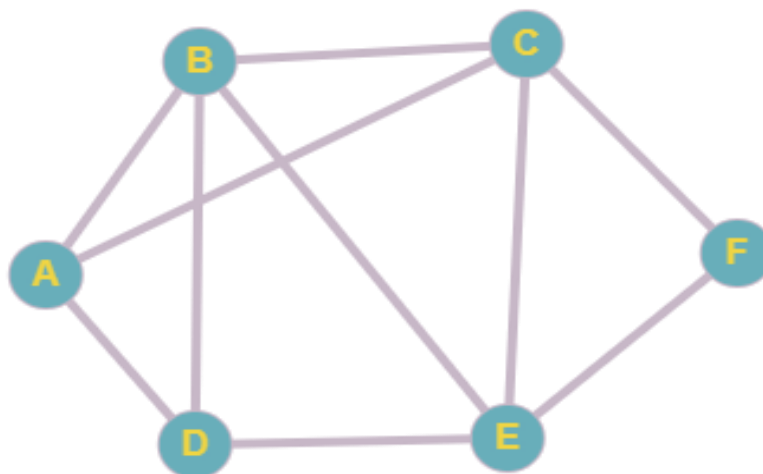


Рисунок 3.1 – Топологія мережі

Таблиця 3.1 – Варіанти завдань

№	AB	AD	AC	BC	BD	BE	CE	CF	DE	EF
1	5	12	3	5	6	4	13	7	14	5
2	3	6	10	13	2	11	6	7	10	9
3	7	2	2	7	2	14	9	9	14	6
4	2	3	5	7	12	2	8	12	11	9
5	14	3	6	7	7	13	6	7	3	13
6	10	4	14	8	5	13	8	11	6	6
7	7	3	9	6	6	14	5	4	2	2
8	11	2	8	6	5	4	14	4	10	3
9	6	9	6	11	4	5	4	8	5	2
10	12	14	7	9	2	9	7	8	11	7
11	10	12	7	2	12	4	12	7	10	4

Продовження табл. 3.1

№	AB	AD	AC	BC	BD	BE	CE	CF	DE	EF
12	14	12	9	13	14	9	7	11	4	12
13	6	7	7	10	13	11	8	8	2	13
14	13	8	7	7	7	13	13	8	7	7
15	5	13	12	5	5	10	11	2	9	5
16	12	13	4	10	4	10	8	3	13	14
17	3	10	9	12	4	6	5	11	9	11
18	4	6	14	7	12	7	8	5	6	11
19	8	8	3	11	7	13	2	5	10	13
20	6	14	3	4	3	6	11	13	6	14
21	6	8	5	12	13	4	5	4	12	12
22	4	8	9	3	14	14	11	5	13	3
23	2	7	7	12	2	4	3	10	2	3
24	13	10	10	4	13	7	10	13	11	14
25	14	12	10	3	3	7	6	14	10	4

3.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- вихідний граф мережі;
- покрокове отримання найкоротшого шляху від вузла А до всіх інших вузлів у вигляді графів;
- покрокове отримання найкоротшого шляху від вузла А до всіх інших вузлів у вигляді таблиці;
- дерево найкоротших шляхів від вузла А до інших вузлів.

3.4 Питання для підготовки до захисту лабораторної роботи

1. В чому полягає задача алгоритму маршрутизації?
2. Які алгоритми маршрутизації використовуються в сучасних мережах?
3. Як централізовані та децентралізовані алгоритми маршрутизації обчислюють шляхи з найменшою вартістю?
4. Який фізичний зміст нульової метрики ребра?
5. За яку кількість ітерацій алгоритм Дейкстри визначить шлях до всіх N-вузлів?

4 ЛАБОРАТОРНА РОБОТА №4. НАЛАШТУВАННЯ МЕРЕЖ VLAN, ПРОТОКОЛІВ DTP ТА VTP, ТА МАРШРУТИЗАЦІЇ МІЖ VLAN

4.2 Мета лабораторної роботи

Поділ в різні підмережі комп'ютерів, підключених до існуючих комутаторів та налаштування маршрутизації між створеними VLAN з використанням конфігурації router-on-a-stick.

4.3 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки до даної роботи, наступні питання:

- сегментування віртуальних локальних мереж;
- типи VLAN;
- стандарт IEEE 802.1Q ;
- налаштування VLAN на комутаторах Cisco;
- налаштування VTP та DTP на комутаторах Cisco;
- налаштування маршрутизації між VLAN з використанням методу router-on-a-stick.

Вихідними даними є побудована мережа в Packet Tracer з лабораторної роботи № 2 «Налаштування динамічного протоколу маршрутизації EIGRP».

Виникла необхідність розділити користувачів в мережі LAN3 на три групи по виконуваних ними функціях, незалежно від їх фізичного розташування (рис.4.1). Таким чином потрібно сегментувати мережу LAN3 на три однакові за розміром підмережі для наступних груп користувачів: Гості, Бухгалтерія, Співробітники. В організації немає ресурсів на придбання додаткового обладнання. Вами біло прийнято рішення реалізувати поставлену задачу за допомогою віртуальних локальних мереж (VLAN) на існуючих комутаторах. Вами була розроблена таблиця VLAN і призначень портів (таблиця 4.1).

З метою безпеки було прийнято не застосовувати VLAN1 за замовчуванням і тому передбачена також окрема мережа VLAN 80 для управління комутаторами, а для нетегованих кадрів мережа native VLAN 90 . При поділі мережі LAN3 на підмережі маски підмереж змінної довжини використовуватися не будуть. Всі адреси підмереж матимуть однакову маску.

Необхідно створити та присвоїти назви мережам VLAN, а також призначити порти доступу конкретним мережам VLAN. Створити транкові порти і призначити їх мережі native VLAN 90. Налаштувати маршрутизацію між VLAN з використанням конфігурації router-on-a-stick.

Додаткове завдання на підвищену оцінку. З розширенням мережі і встановленням додаткових комутаторів було прийнято рішення автоматизувати та спростити конфігурацію VLAN та транкінгу між комутаторами, налаштувавши протоколи VTP та DTP.

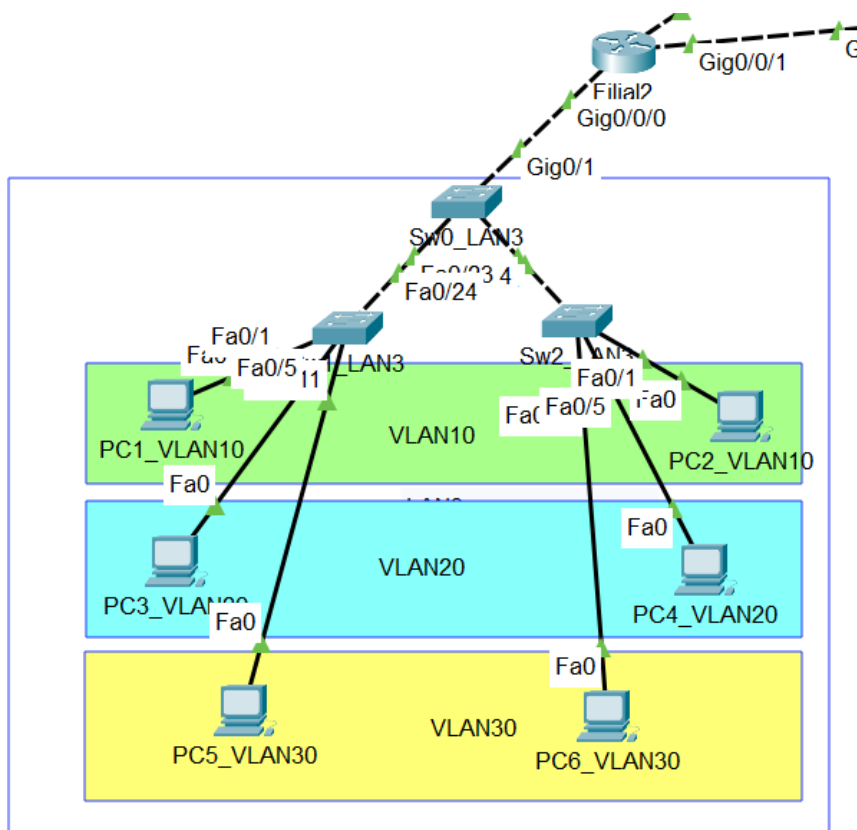


Рисунок 4.1 – Топологія з VLAN

Таблиця 4.1 – Мережі VLAN и призначень портів

VLAN ID	Ім'я VLAN	Порт	Режим роботи	Примітка
1	Default			Не використ.
10	Accounting	Sw1_LAN3 f0/1-4 Sw2_LAN3 f0/1-4	access	«Бухгалтерія»
20	Colleague	Sw1_LAN3 f0/5-19 Sw2_LAN3 f0/5-19	access	«Співробітники»
30	Guest	Sw1_LAN3 f0/20-22 Sw2_LAN3 f0/20-22	access	«Гості»
80	Management	SVI		Для керування пристроями
90	Native	На всіх комутаторах: f0/23-24, gig0/1-2	trunk	Транковий канал 802.1Q

Далі виконати наведені кроки.

Крок 1. Сегментування мережі LAN3

1. Визначити кількість сегментів в мережі, виходячи з вимог таблиці 4.1. Розрахувати маску підмереж і визначити діапазон адресів підмереж, що входять в об'єднану мережу LAN3. Інформацію о підмережах необхідно надати у вигляді табл. 4.2.

Таблиця 4.2 – Підмережі LAN3

Ім'я VLAN	Номер VLAN	Адреса підмережі	Маска підмережі у десятковому форматі	Префікс	Діапазон допустимих IP-адресів вузлів	Широкомовна адреса

2. Розробити схему адресації для ПК та мережних пристроїв та задокументувати у вигляді таблиць 4.3 и 4.4, враховуючи наступні вимоги:

– перші допустимі для використання IP-адреси будуть назначатися підінтерфейсам маршрутизатора в LAN3;

– останні з використовуваних IP-адрес призначаються вузлам в підмережах.

Таблиця 4.3 – Таблиця адресації для ПК

Пристрій	IP-адреса	Маска	Шлюз	Порт комутатора, до якого під'єднаний	VLAN ID
PC1					
PC2					
PC3					
PC4					
PC5					
PC6					

Таблиця 4.4 – Таблиця адресації для пристроїв в LAN3

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN ID
Sw0 LAN3	SVI 80				
Sw1 LAN3	SVI 80				
Sw2 LAN3	SVI 80				
Filial2	GigEthernet 0/0/0.10				
	GigEthernet 0/0/0.20				
	GigEthernet 0/0/0.30				
	GigEthernet 0/0/0.80				

3. По табл. 4.3 призначити ПК IP-адреси, маски підмереж і шлюзи за замовчуванням

4. По табл. 4.4 призначити комутаторам IP-адреси і шлюз за замовчуванням.

Крок 2. Перевірка конфігурації VLAN, встановленої за замовчуванням

1. На кожному комутаторі відобразити всі налаштовані мережі VLAN командою «show vlan» або «show vlan brief».

2. Перевірити підключення між комп'ютерами в однакових VLAN. Чи успішно виконані echo-запити?

3. Перевірити підключення між комп'ютерами в різних VLAN. Чи успішно виконані echo-запити?

4. Перейти в режим *Simulation*, сформувати широкомовні пакети в кожній підмережі і простежити, як вони поширюються. Чому echo-запити до вузлів з інших мереж виконані невдало?

Крок 3. Створення мереж VLAN

1. Відповідно до табл. 4.1 створити на комутаторах мережі VLAN і надати їм імена.

```
Switch(config)#vlan <VLAN ID>
```

```
Switch(config-vlan)#name <NAME VLAN>
```

2. Виконайте команду «show vlan» на кожному комутаторі, щоб переглянути список мереж VLAN.

Якою є VLAN за замовчуванням? _____

За замовчуванням до якої мережі VLAN належать порти комутаторів? _____

Крок 4. Налаштування портів доступу

1. Відповідно до таблиці 4.1 на комутаторах Sw1_LAN3 і Sw2_LAN3 налаштувати відповідні інтерфейси в якості портів доступу і призначити їм мережі VLAN.

```
Switch(config)#interface range <INTERFACE RANGE>
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan <VLAN ID>
```

2. Виконати команду «show vlan brief» на кожному комутаторі і переконатися, що мережі VLAN призначені правильним інтерфейсам. Занотувати їх у звіт.

Крок 5. Налаштування транкових каналів

1. Відповідно до таблиці 4.1 на комутаторах налаштувати інтерфейси між комутаторами та маршрутизатором для створення транкових каналів.

```
Switch(config)#interface range <INTERFACE RANGE>
```

```
Switch(config-if-range)#switchport mode trunk
```

2. Налаштувати мережу VLAN 90 як native VLAN на відповідних інтерфейсах комутаторів.

```
Switch(config-if-range)#switchport trunk native vlan <VLAN ID>
```

3. Виконати команду «show interface trunk», щоб переконатися в налаштуванні транкових каналів.

4. Відправити echo-запити між комп'ютерами в однакових VLAN. Чи успішно виконуються echo-запити?

5. Відправити echo-запити між комп'ютерами в різних VLAN. Чи успішно виконуються echo-запити?

6. Перейти в режим *Simulation*, сформувати широкомовні пакети в кожній підмережі і спостерігати, як вони поширюються. Порівняти з поширенням пакетів на кроці 2.

Крок 6. Налаштування на Filial2 маршрутизації між VLAN за допомогою інкапсуляції 802.1Q

1. Перед тим, як створювати та налаштовувати підінтерфейси для кожної VLAN, слід видалити адресу на інтерфейсі в LAN3.

```
Filial2(config)# interface g0/0/0
```

```
Filial2(config-if)#no ip address
```

2. На інтерфейсі в LAN3 створити підінтерфейси для кожної VLAN за допомогою інкапсуляції 802.1Q:

```
Filial2(config)# int g0/0/0.<SUB-INTERFACE>
```

```
Filial2(config-subif)# encapsulation dot1Q <VLAN ID>
```

```
Filial2(config-subif)# ip address <IP-ADDRESS> <MASK>
```

3. Спробувати відправити echo-запити між комп'ютерами в різних VLAN. Чи успішно виконуються echo-запити?

4. Перевірити конфігурацію підінтерфейсів командою «show ip interface brief» та занотувати в звіт її результат.

Додаткове завдання

В зв'язку з розширенням мережі виникла необхідність підключити нових співробітників в віддаленій мережі. Це розширення потребує встановлення додаткового комутатора для підключення нових робочих станцій співробітників. Було прийнято рішення встановити робочу VTP-середу на віддаленому комутаторі. Це дозволить більш ефективно підтримувати віртуальні локальні мережі з головного комутатора Sw0_LAN3.

Крок 1. Підключення нового комутатора до мережі

1. Додати в мережу LAN3 ще один комутатор серії Cisco Catalyst 2960 (Sw3_LAN3). Під'єднайте до нього декілька робочих станцій, які будуть належати до VLAN 20 співробітників, призначення портів аналогічно до табл. 4.1.

2. Під'єднати порт g0/2 Sw0_LAN3 з портом f0/24 доданого комутатора.

Крок 2. Використання протоколу DTP (Dynamic Trunking Protocol) для створення магістральних каналів

Було прийнято рішення для створення і узгодження магістральних каналів між Sw0_LAN3 і Sw3_LAN3 використовувати протокол DTP.

3. Перевірити командою «show interface *interface* switchport», що порти g0/2 Sw0_LAN3 та f0/24 Sw3_LAN3 налаштовані на автоматичне використання протоколу DTP (налаштування за замовчуванням).

Яка вказана конфігурація DTP для порту g0/2 Sw0_LAN3? _____

Яка вказана конфігурація DTP для порту f0/24 Sw3_LAN3? _____

Який вказано поточний стан порту g0/2 Sw0_LAN3? _____

Який вказано поточний стан порту f0/24 Sw3_LAN3? _____

4. Налаштувати порт g0/2 Sw0_LAN3 як рекомендований для протоколу DTP:

```
Switch(config)# interface <INTERFACE>
```

```
Switch(config-if)# switchport mode dynamic desirable
```

5. Перевірити знов поточний стан портів комутаторів.

Яка вказана конфігурація DTP для порту g0/2 Sw0_LAN3? _____

Яка вказана конфігурація DTP для порту f0/24 Sw3_LAN3? _____

Який вказано поточний стан порту g0/2 Sw0_LAN3? _____

Який вказано поточний стан порту f0/24 Sw3_LAN3? _____

Крок 3. Налаштування протоколу VTP (VLAN Trunking Protocol)

Протокол VTP служить для поширення відомостей про мережі VLAN на комутатори, що входять в домен VTP.

1. Щоб створити новий домен VTP, налаштувати комутатор Sw0_LAN3 як сервер VTP, присвоївши йому доменне ім'я *Cisco_VTP* і задавши пароль *cisco12345*.

Примітка. Назви доменів VTP слід вводити з урахуванням регістра. Пароль вказувати необов'язково, однак це дозволяє підвищити рівень безпеки.

```
Switch(config)#vtp mode server
```

```
Switch(config)#vtp domain <DOMAIN>
```

```
Switch(config)#vtp password <PASSWORD>
```

2. Додайте в домен комутатор Sw3_LAN3 в якості клієнта VTP і виконати відповідні налаштування.

```
Switch(config)#vtp mode client
```

```
Switch(config)#vtp domain <DOMAIN>
```

```
Switch(config)#vtp password <PASSWORD>
```

Крок 4. Перевірка роботи VTP

1. Перевірити на Sw0_LAN3, чи був створений домен *Cisco_VTP* та режимом VTP є Server. Переконайтеся, що встановлено пароль VTP *cisco12345*.

```
Switch#show vtp status
```

```
Switch#show vtp password
```

2. Перевірити на Sw3_LAN3 режим VTP, домен, пароль.

3. Переконайтеся, що комутатор Sw3_LAN3 отримав дані про мережі VLAN.

```
Switch#show vlan brief
```

4. Занотувати в звіт результати перевірок.

5. Перевірити підключення до комп'ютерів в VLAN 20, під'єднаних до інших комутаторів, відправивши echo-запити. При невдалій перевірці виконайте пошук і усунення несправностей.

4.4 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- таблиці 4.2-4.4 з вихідними даними для VLAN;
- команди налаштувань в ході виконання лабораторної роботи з коментарями;
- результат команди «show vlan brief» на всіх комутаторах в LAN3 на кроці 3;
- результат команди «show interface trunk» на всіх комутаторах в LAN3 на кроці 4;

- результат команди «show vtp status» та «show vtp password» на комутаторах Sw0_LAN3 та Sw3_LAN3 при виконанні додаткового завдання;
- відповіді на поставлені питання;
- проект мережі з назвою за правилом *Surname_Group_lab4_KM*.

4.5 Питання для підготовки до захисту лабораторної роботи

1. Призначення та переваги використання мереж?
2. Який тип мережі VLAN використовується адміністратором для доступу до комутатора і його налаштування?
3. Для чого служить ідентифікатор кадру (tag) і де він розміщується?
4. Что такое транк?
5. Як забезпечується взаємодія між вузлами в різних VLAN?

5 ЛАБОРАТОРНА РОБОТА №5. НАЛАШТУВАННЯ МАРШРУТИЗАТОРА ЯК СЕРВЕРА ДНСП

5.1 Мета роботи

Ознайомитися з особливостями функціонування та налагодження роботи протоколу динамічного конфігурування вузлів ДНСП на обладнанні Cisco.

5.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій, методичні вказівки до даної роботи наступні питання:

- логічна адресація в IP-мережах;
- налаштування ДНСП-сервера на базі маршрутизатора Cisco.

Вихідними даними є налаштована мережа з лабораторної роботи №4 «Налаштування мереж VLAN, протоколів DTP та VTP, та маршрутизації між VLAN».

З метою швидкого призначення хостам мережні налаштування (IP-адреса, адресу шлюза та DNS-сервера) в підмережах LAN3-LAN6 організації було прийнято рішення застосовувати маршрутизатор Central для забезпечення служб ДНСП без необхідності виділеного сервера.

Перед вами стоїть завдання створити на Central пули ДНСП з урахуванням наступних вимог:

- забезпечити динамічний розподіл адрес для клієнтів усередині мереж LAN3-LAN6, враховуючи, що мережа LAN3 розділена на VLAN;
- для імені пула застосовувати назву підмережі;
- в кожному пулі ДНСП оголосити домен за правилом *Surname.Group.com*, наприклад *Ivanov.KI-25-1.com*;
- в кожному пулі задати адресу DNS-сервера з підмережі LAN2;
- в кожному пулі ДНСП виключити IP-адреси LAN-інтерфейсів та ще дев'ять інших адрес для статичного призначення іншим пристроям, таким як комутатори, сервери, принтери та інтерфейси керування пристроями;

Хости в LAN3 та LAN4 також будуть отримувати адреси по ДНСП, тому необхідно налаштувати маршрутизатор Filial2 як агента ретрансляції ДНСП.

Далі виконати такі дії.

Крок 1. Налаштування пулів ДНСП на Central

Увійти в режим конфігурації термінала маршрутизатора і виконайте наступні кроки для кожної підмережі з завданням вимогами:

1. Виключити з роздачі перші 10 адрес з діапазону допустимих адрес
Router(config)#ip dhcp excluded-address <початкова адреса> <кінцева адреса>
2. Створити ДНСП пул командою:
Router(config)# ip dhcp pool <POOL_NAME>

3. Налаштувати параметри DHCP пулу, такі як адресу мережі, з якої будуть роздаватися IP-адреси, назва домену, шлюз за замовчуванням, DNS-сервер:

```
Router(dhcp-config)# network <NETWORK_ADDRESS> <SUBNET_MASK>
```

```
Router(dhcp-config)# default-router <DEFAULT_GATEWAY>
```

```
Router(dhcp-config)# domain-name <DOMAIN-NAME>
```

```
Router(dhcp-config)# dns-server <DNS_SERVER_IP>
```

4. Завершити налаштування DHCP пулу:

```
Router(dhcp-config)# exit
```

5. По завершенні налаштування пулу DHCP для мереж LAN3-LAN6 зберегти зміни:

```
Router(config)#do copy running-config startup-config
```

Крок 2. Налаштування маршрутизатора Filial2 як агента ретрансляції DHCP

1. Активувати DHCP на відповідних інтерфейсах, вказавши IP-адресу інтерфейса маршрутизатора Central, яка під'єднана до Filial2:

```
Router(config)# interface <INTERFACE>
```

```
Router(config-if)# ip helper-address <DHCP_SERVER_IP>
```

```
Router(config-if)# exit
```

2. Зберегти зміни:

```
Router# copy running-config startup-config
```

Після виконання цього кроку маршрутизатор Central буде надавати IP-адреси через DHCP на вказаному інтерфейсі.

Крок 3. Перевірка роботи DHCP

1. Налаштуйте вузли в мережах LAN3-LAN6 таким чином, щоб вони отримували IP-адреси через DHCP.

2. Перевірте, чи отримали вузли адреси з правильних пулів DHCP.

3. Відобразіть на Central список орендованих DHCP адрес командою «show ip dhcp binding».

4. Виконайте команду «show ip dhcp pool», щоб переглянути налаштування пулів DHCP.

5.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- команди налаштувань DHCP з коментарями;
- результати перевірки роботи DHCP;
- проект мережі з назвою за правилом *Surname_Group_lab5_KM.pkt*.

5.4 Питання для підготовки до захисту лабораторної роботи

1. У чому полягає перевага використання агентів DHCP-ретрансляції замість використання кількох маршрутизаторів, які працюють як сервери DHCP?

2. Які переваги використання DHCP?

3. У чому призначення DHCP у клієнтській мережі?
4. Яка IP-адреса призначається робочій станції після оновлення її IP-адреси?
5. Які інші параметри DHCP, які не описані в даній роботі, можна встановити на маршрутизаторах?

6 ЛАБОРАТОРНА РОБОТА №6. НАЛАШТУВАННЯ БЕЗДРОТОВОЇ МЕРЕЖІ MERAKI

6.1 Мета роботи

Ознайомитися з міжмережевим екраном Meraki Security Appliance та доступом до налаштувань через хмарний веб-сервіс.

6.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій, методичні вказівки до даної роботи і довідку в Packet Tracer (*Help->Content->Configuring Devices->Meraki Devices*), наступні питання:

- мережні пристрої Meraki;
- налаштування пристроїв Meraki в Packet Tracer;
- нова архітектура мереж Cisco SD-WAN.

Вихідними даними є налаштована мережа з лабораторної роботи №5 «Налаштування маршрутизатора як сервера DHCP»

У цій лабораторній роботі ви додасте до підмереж LAN4 та LAN6 міжмережевий екран Meraki Security Appliance (SA) та налаштуєте бездротове підключення для користувачів через хмарний веб-сервер Meraki. Для бездротових мереж Meraki буде використовуватися адресний блок 192.168.0.0/24.

Cisco Meraki – це набір керованих через Інтернет мережевих рішень, що забезпечують єдине джерело управління місцями розташування, інфраструктурою і пристроями.

Meraki SA – це керовані з хмари пристрої Unified Threat Management (UTM) з підтримкою програмно-конфігурованих глобальних мереж (Software Defined Wide Area Networking - SD-WAN) і бездротовими можливостями.

Cisco Packet Tracer версії 7.2 і вище підтримує спрощену версію Meraki SA модель MX65W та хмарний веб-сервер Meraki.

Далі виконати такі дії.

Крок 1. Додавання пристроїв Meraki і побудова мережі

1. Додайте в мережу LAN4 з блоку *Wireless Devises* пристрій Meraki-MX65W. З'єднайте через кабель *Straight-Throuhg* порт *Internet 1* на Meraki SA з вільним портом на комутаторі (рис. 6.1).

2. Додайте в топологію нового користувача та під'єднайте до *GigabitEthernet3* на Meraki SA (рис. 6.1).

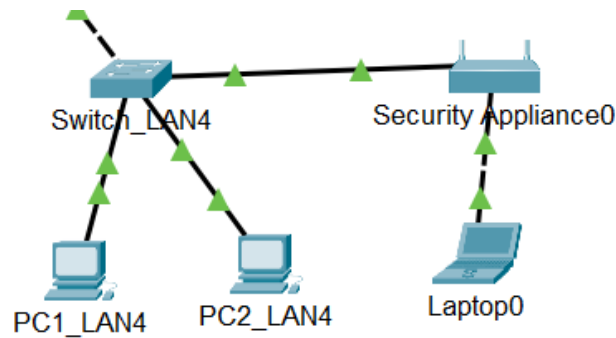


Рисунок 6.1 – Побудова мережі з Meraki-MX65W

3. На вкладці *Physical* Meraki SA під'єднайте до нього блок живлення.

4. Для демонстрації керування Meraki SA з будь-якої точки локації, додайте до віддаленої мережі веб-сервер Meraki та ПК для керування через веб-інтерфейс (рис. 6.2). В табл. 6.1 наведені відомості для адресації пристроїв в цій мережі.

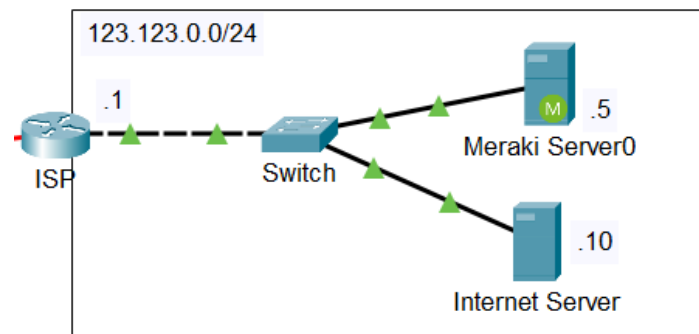


Рисунок 6.2 – Мережа з веб-сервером Meraki

Таблиця 6.1 – IP-адресація пристроїв в мережі з веб-сервером Meraki

Пристрій	Мережа	IPv4 Address	Default Gaeway	DNS Server
Meraki Server	123.123.0.0/24	123.123.0.5	123.123.0.1	
Internet Server		123.123.0.10	123.123.0.1	123.123.0.5

Крок 2. Налаштування базових початкових параметрів Meraki SA

1. Щоб підключитися до Meraki SA локально через веб-інтерфейс, надайте доданому ПК в LAN4 статичну IP-адресу з мережі 192.168.0.0/24 (не забудьте вказати шлюз та адресу DNS-сервера в організації, що знаходиться в LAN2).

2. Увімкнений Meraki SA можна налаштувати локально через HTTP-сеанс від ПК до SA з URL-адресою <http://setup.meraki.com> або <http://192.168.0.1>. Ім'я користувача - це серійний номер Meraki SA без пароля (рис. 6.3).

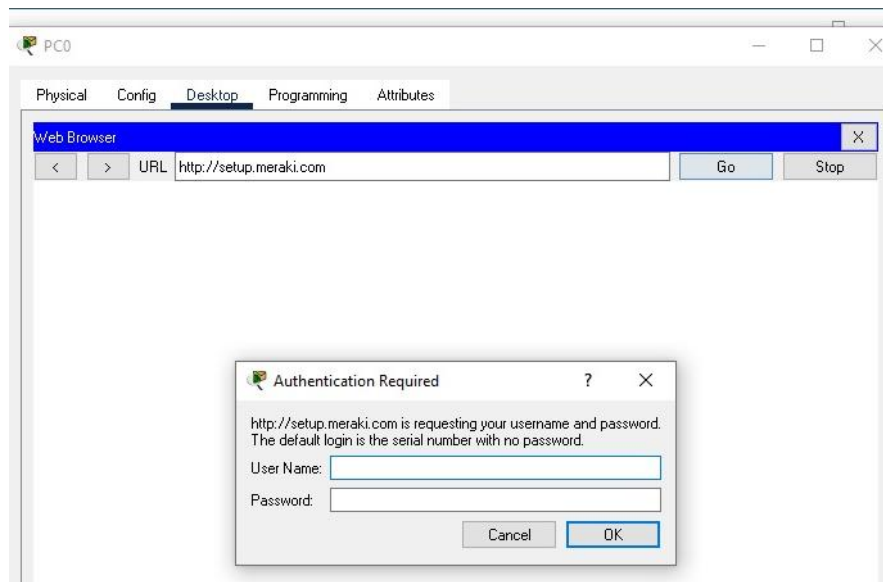


Рисунок 6.3 – Встановлення HTTP-сеансу від ПК до Meraki SA

Серійний номер можна знайти на вкладці *Config* в розділі *Settings* пристрою Meraki SA (рис. 6.4). Задокументуйте його для подальшого використання.

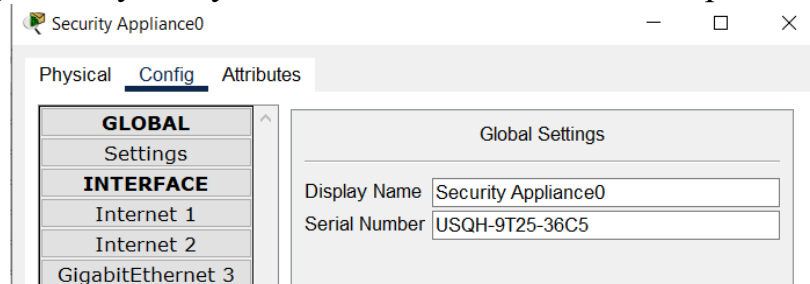


Рисунок 6.4 – Серійний номер SA Meraki SA

3. Після входу відображатиметься поточний статус Meraki SA.

4. На вкладці *Configure* в розділі *Internet 1* налаштуйте:

- Connection type: Direct;
- IP assignment: DHCP.

ВАЖЛИВО! Важливо, щоб Meraki SA отримав адресу на інтерфейсі *Internet 1* динамічно. При статичному налаштуванні IP-адреси взаємодії між сервером та SA не має (баг програми).

5. Збережіть налаштування на Meraki SA. Він повинен отримати адресу на інтерфейсі *Internet 1* динамічно.

6. На вкладці *Connection* в розділі *Security Appliance details* задокументуйте MAC-адресу пристрою для подальшого використання.

Крок 3. Налаштування DNS-сервера для доступу до сервера Meraki за URL-адресою

Базова мережева конфігурація Meraki SA може бути досягнута через HTTP-сеанс з ПК локально, безпосередньо підключеного до пристрою безпеки за URL-адресою <http://setup.meraki.com> або <http://192.168.0.1>. Однак функції бездротового зв'язку і безпеки можна налаштовувати віддалено через хмарний сервер Meraki за URL-адресою <https://dashboard.meraki.com> після підключення пристрою безпеки до сервера Meraki.

1. Внесіть в розділ *DNS* на ServerDNS організації адресу хмарного сервера Meraki (рис. 6.5).

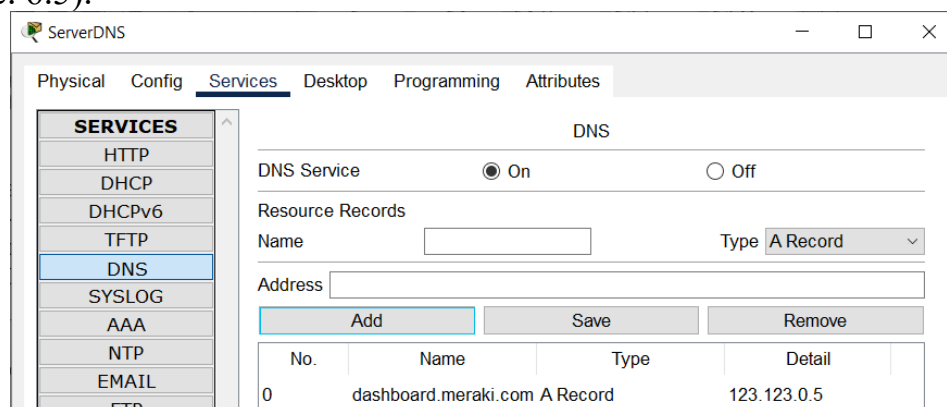


Рисунок 6.5 – DNS-запис URL-адреси сервера Meraki

2. З будь-якого ПК в організації підключиться до веб-сервера Meraki для налаштування бездротової мережі і Meraki SA (<https://dashboard.meraki.com>). Зверніть увагу, що підключення тільки по протоколу HTTPS.

3. Створіть нового користувача (рис. 6.6):

– email: admin_meraki@cisco.com;

– password: 12345678.

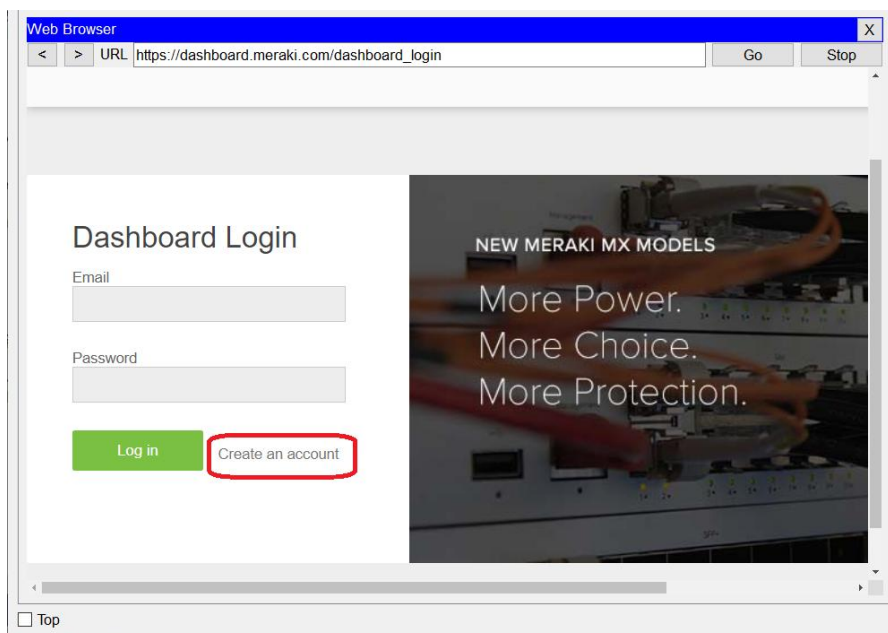


Рисунок 6.6 – Додавання нового користувача до веб-сервера Meraki

4. Використовуйте зареєстровану адресу електронної пошти та пароль для входу в панель керування.

5. Якщо це перший вхід в систему або в обліковий запис не додано ніякі мережі або пристрої, панель управління і навігація зліва обмежені. Якщо додані мережі і пристрої, на панелі керування з'явиться список мереж і пристроїв, а на лівій панелі навігації буде більше параметрів.

Крок 4. Створення мереж та реєстрація пристроїв

В *Meraki Dashboard* доступ до сторінки створення мереж та реєстрації пристроїв можна отримати, натиснувши посилання *Create a network* на лівій навігаційній панелі або в меню *Organization > Create a network*.

6. Створіть нову мережу LAN4 (рис. 6.7).

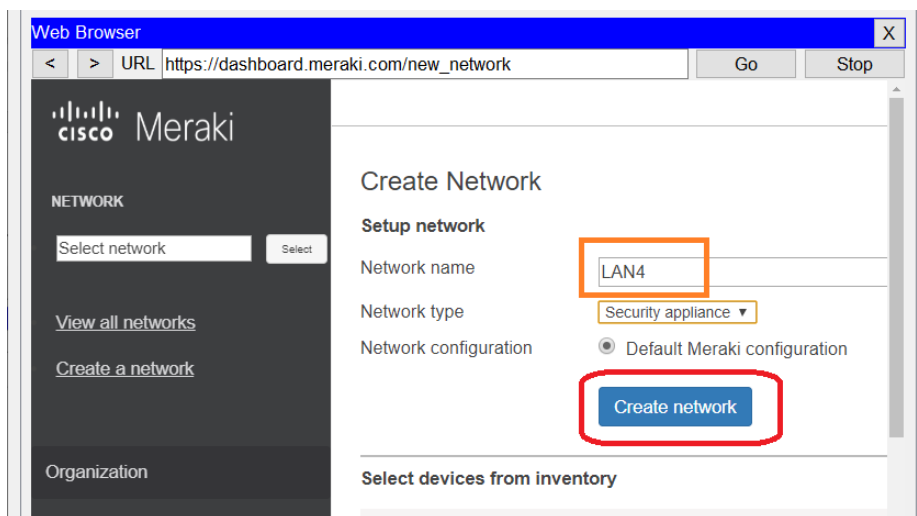


Рисунок 6.7 – Додавання нової мережі в Meraki Dashboard

7. Додайте в мережу LAN4 пристрій Meraki-MX65W з задокументованими його параметрами (рис. 6.8).

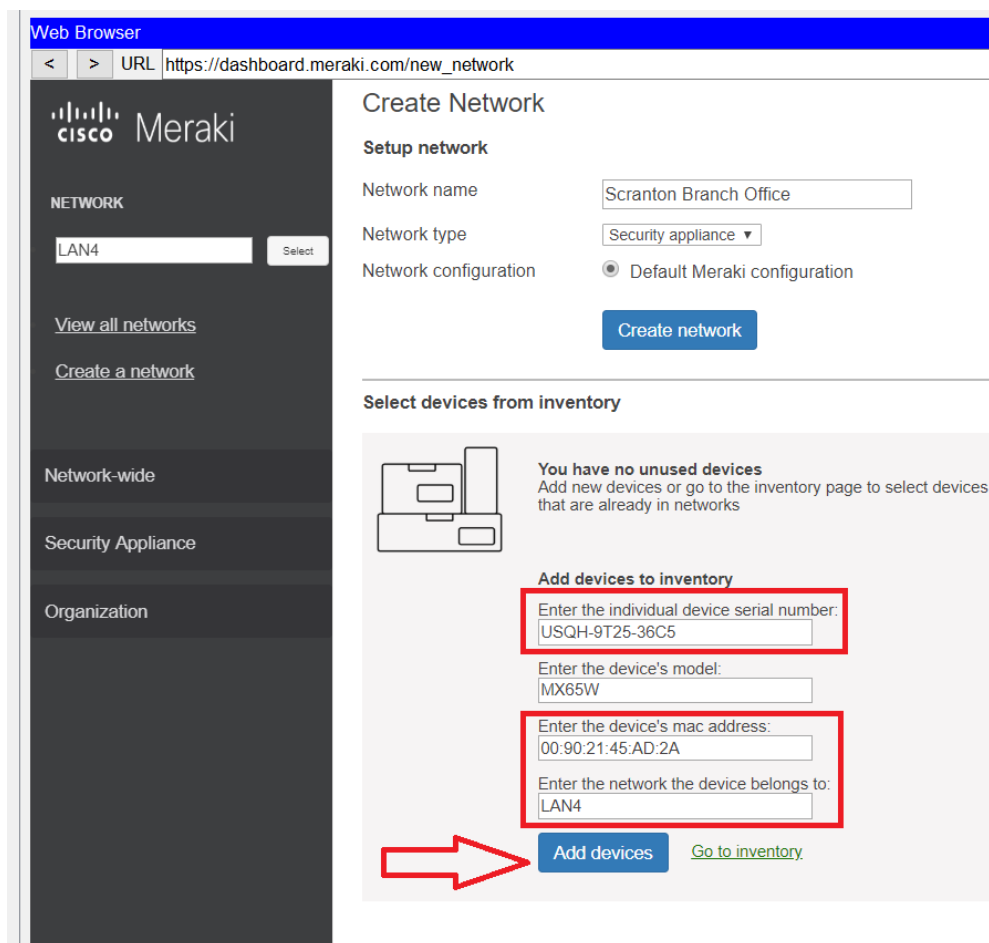


Рисунок 6.8 – Додавання пристрою Meraki-MX65W до Meraki Dashboard

8. Якщо пристрій буде успішно додано, на сторінці *Security Appliance > Appliance Status* відображатимуться поточні дані про стан портів (рис.6.9). Посилання *Uplink* показуватиме конфігурацію WAN Інтернет-порту.

Примітка. Якщо по повторному відкритті проекту не буде відображатися актуальний стан портів, підключитися до нього локально та збережіть налаштування на веб-сторінці цього пристрою (<http://setup.meraki.com>), натиснувши кнопку *Save* на вкладці *Configure*, та почекайте, поки оновиться інформація.

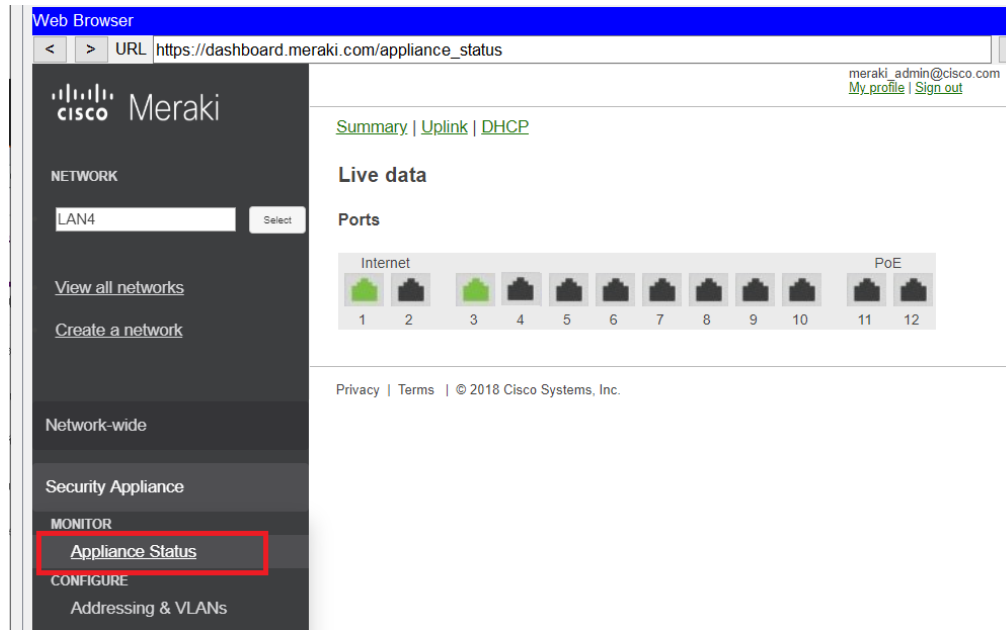


Рисунок 6.9 – Стан портів пристрою

9. На сторінці *Security Appliance->Wireless Settings* налаштуйте параметри Wi-Fi мережі для бездротового під'єднання користувачів в LAN4 згідно рис. 5.10.

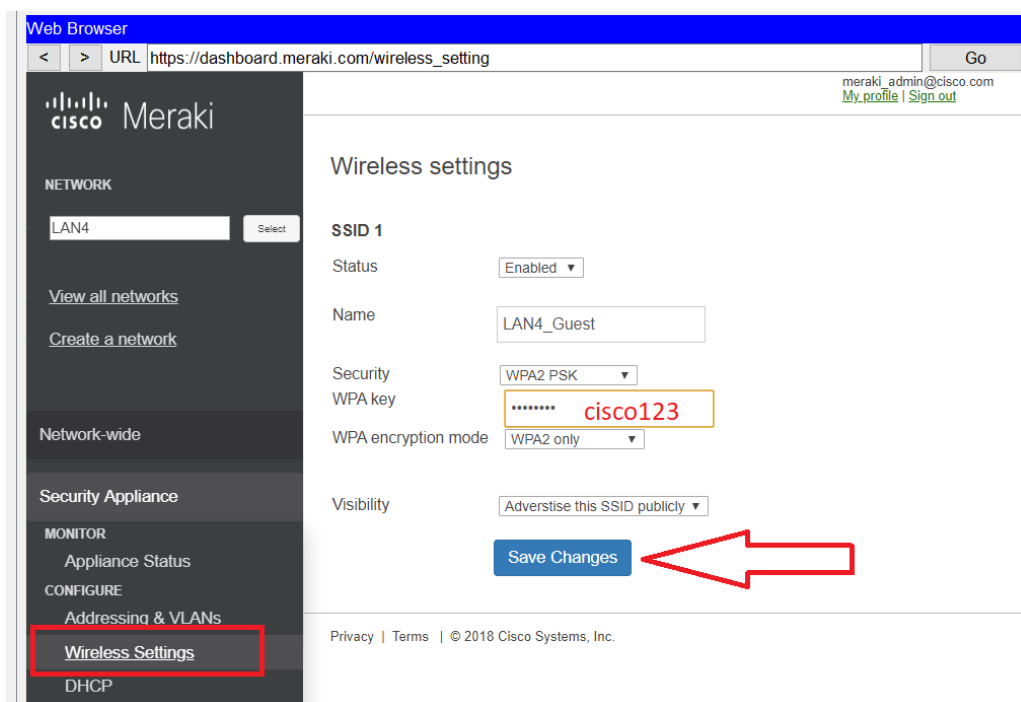


Рисунок 6.10 – Налаштування параметрів мережі Wi-Fi

10. Додайте в LAN4 бездротових клієнтів (наприклад ноутбук з доданим бездротовим інтерфейсом WPC300N) та зробіть на них налаштування відповідно до зроблених налаштувань бездротової мережі.

Крок 5. Додавання до підмережі LAN6 Meraki SA та налаштування бездротового підключення для користувачів.

1. Аналогічним чином додайте до підмережі LAN6 міжмережевий екран Meraki SA та налаштуєте відповідне бездротове підключення для користувачів через хмарний веб-сервер Meraki.

6.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

– проект мережі з назвою за правилом *Surname_Group_lab6_KM.pkt*.

6.4 Питання для підготовки до захисту лабораторної роботи

1. Що включає в себе рішення Cisco Meraki?
2. Які переваги має використання Cisco Meraki для підприємств?
3. Яка роль Meraki SA (Security Appliance) у розгалуженій мережі?
4. Які основні функції і можливості Meraki SA?
5. Як Meraki сприяє забезпеченню безпеки мережі в офісних приміщеннях та віддалених робочих місцях?

7 ЛАБОРАТОРНА РОБОТА №7.

НАЛАШТУВАННЯ СТАТИЧНОГО, ДИНАМІЧНОГО NAT ТА PAT

7.1 Мета роботи

Налаштування, застосування та перевірка різних типів перетворення мережних адрес (NAT) на граничному маршрутизаторі мережі організації з внутрішніх IP-адрес в зовнішні публічні адреси.

7.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки до даної роботи, наступні питання:

- типи NAT;
- принцип роботи статичного NAT;
- принцип роботи динамічного NAT;
- налаштування NAT на маршрутизаторах Cisco.

Вихідними даними є побудована мережа в Packet Tracer з лабораторної роботи №6 «Налаштування бездротової мережі Meraki».

В організації зараз використовується адресація із приватної мережі, яка не може бути використовуватися для комунікації в глобальній мережі Інтернет. Для обміну даними в Інтернеті використовуються публічні IP-адреси. Для забезпечення зв'язку між локальною мережею з приватними IP-адресами та глобальною мережею Інтернет використовується технологія Network Address Translation (NAT), яка дозволяє перетворювати приватні IP-адреси на публічні при виході в інтернет

Постачальник послуг Інтернету ISP виділив для організації діапазон публічних IP-адрес 209.165.202.128/27. Цей діапазон надає організації 30 публічних IP-адрес. IT-відділ надав наступну інформацію для перетворення наданих IP-адрес (табл. 7.1):

Таблиця 7.1 – Вихідні дані для NAT

Inside local	Inside global	Тип NAT
MultiServer	209.165.202.129	статичний
ServerDNS	209.165.202.130	статичний
LAN3	209.165.202.131-209.165.202.157	NAT
LAN1-2, LAN4-LAN6	209.165.202.158	PAT

Необхідно налаштувати граничний маршрутизатор Central відповідно до наданих даних по табл. 7.1.

Далі виконати наведені кроки.

Крок 1. Налаштування статичної маршрутизації

Статичний маршрут використовується на ділянці від ISP до Central, тоді як маршрут за замовчуванням використовується на ділянці від Central до ISP.

1. Видаліть статичний маршрут на ISP до мережі організації, яка приналежить приватній мережі.

2. Створіть статичний маршрут на маршрутизаторі ISP до діапазону виділених публічних IP-адрес 209.165.202.128/27 організації.

```
ISP(config) # ip route 209.165.202.128 255.255.255.224 {IP_Central || out_interface}
```

Крок 2. Налаштування статичного NAT

Статичний NAT задає однозначну відповідність однієї адреси іншій. Іншими словами, при проходженні через маршрутизатор, адреса(и) змінюються на строго задану адресу, один-до-одного. Запис такої трансляції зберігається необмежено довго, поки є рядок в конфігурації.

Згідно табл. 7.1 виконайте статичне перетворення, завдяки чому користувачі зможуть отримати доступ до серверів з Інтернету.

3. Виберіть граничний маршрутизатор Central. Введіть

```
Central(config)#ip nat inside source static <IP_MultiServer> 209.165.202.129
```

```
Central(config)#ip nat inside source static <IP_ServerDNS> 209.165.202.130
```

4. Налаштуйте всі інтерфейси, підключені до підмереж організації, як внутрішні інтерфейси NAT. Наприклад:

```
Central (config-if)#ip nat inside
```

5. Налаштуйте інтерфейс підключення до ISP як зовнішній інтерфейс NAT.

```
Central(config-if)#ip nat outside
```

Крок 3. Перевірка роботи статичного NAT

1. Відобразіть таблицю статичних перетворень NAT за допомогою команди «show ip nat translations» за заповніть ними табл. 7.2.

Таблиця 7.2 – Перетворення NAT на Central

Protocol	Inside global	Inside local	Outside local	Outside global	Пояснення

2. З командного рядка MultiServer відправте echo-запит на Internet Server.

```
> ping 123.123.0.10
```

3. Перегляньте таблицю NAT та додайте результат в табл. 7.2.

4. Оскільки статичний NAT налаштований для MultiServer, переконайтеся в успішному проходженні echo-запиту від Internet Server до серверу через публічну адресу 209.165.202.129.

```
cmd > ping 209.165.202.129
```

5. Перегляньте таблицю NAT та додайте результат в табл. 7.2.

6. Переконайтеся в успішному проходженні echo-запиту від Internet Server до ServerDNS через публічну адресу 209.165.202.130.

cmd > ping 209.165.202.130

7. Перегляньте таблицю NAT та додайте результат в табл. 7.2.

8. Спробуйте echo-запити від Internet Server до ServerDNS та MultiServer через внутрішню IP-адресу. Чи успішно виконані запити і чому?

9. Спробуйте echo-запити з командного рядка ПК в мережі LAN1 та інших ПК в підмережах організації на від Internet Server. Чи успішно виконані запити і чому?

10. Перевірте статистику NAT, виконавши на Central команду «show ip nat statistics».

Скільки активних перетворень виконано? Скільки адрес мається в пулі? Скільки адрес вже виділено?

Крок 4. Налаштування динамічного NAT

В динамічному NAT при проходженні через маршрутизатор нова адреса вибирається динамічно з деякого пулу адрес. Запис про трансляцію зберігається деякий час, щоб відповідні пакети могли бути доставлені адресату. Якщо протягом деякого часу трафік по цій трансляції відсутній, трансляція видаляється і адреса повертається в пул. Якщо потрібно створити трансляцію, а вільних адрес в пулі немає, то пакет відкидається.

Налаштуємо трансляцію внутрішніх адрес вузлів в підмережі LAN3 в зовнішні при проходженні трафіку через маршрутизатор Central.

1. Очистіть дані NAT перед додаванням динамічних перетворень.

Central# clear ip nat translation *

Central# clear ip nat statistics (в PT не підтримується)

2. Створіть іменований стандартний список контролю доступом ACL назвою ACL_LAN1, який дозволяє весь трафік від мережі LAN3.

Примітка. ACL керують трафіком, порівнюючи адресу джерела IP-пакетів з адресами, заданими в списку. Маски, використовувані для списків доступу, є зворотними (wildcard-mask) (наприклад, зворотна маска для 255.255.255.0 буде 0.0.0.255).

Central(config)# ip access-list standard ACL_LAN3

Central(config-std-nacl)#permit <LAN3> <WILDCARD-MASK>

3. Створіть пул з назвою NAT_LAN3, вказавши початкову і кінцеву придатних до використання публічних IP-адрес.

Central(config)# ip nat pool NAT_LAN3 209.165.202.131 209.165.202.157
netmask 255.255.255.224

4. Створіть трансляцію NAT, зіставши ACL-список ACL_LAN3 зі пулом зовнішніх адрес NAT_LAN3.

Central (config)#ip nat inside source list ACL_LAN3 pool NAT_LAN3

Крок 5. Перевірка роботи динамічного NAT

1. З командного рядка **всіх** ПК в мережі LAN3 відправте echo-запити на IP-адресу Internet Server. Проекспериментуйте з більшою кількістю протоколів, таких як HTTP, HTTPS, telnet. Відобразіть перетворення NAT на маршрутизаторі Central

за допомогою команди «show ip nat translations». Додайте результати в табл. 7.2.

2. Перевірте статистику NAT, виконавши на Central команду «show ip nat statistics».

Скільки активних перетворень виконано? Скільки адрес мається в пулі? Скільки адрес вже виділено?

Крок 6. Налаштування NAT з перевантаженням (PAT)

Динамічний NAT з перевантаженням (PAT) працює майже також, як динамічний NAT, але при цьому відбувається трансляція багато-в-один, задіюючи при цьому можливості транспортного рівня

1. Очистіть дані NAT перед додаванням динамічних перетворень.

2. Створіть іменований ACL-список з назвою *ACL_PAT*, відповідний IP-адресам мереж LAN1-2, LAN4-LAN6.

```
Central(config)# ip access-list standard ACL_PAT  
Central(config-std-nacl)#permit <LAN1> <WILDCARD-MASK>  
Central(config-std-nacl)#permit <LAN2> <WILDCARD-MASK>  
Central(config-std-nacl)#permit <LAN4> <WILDCARD-MASK>  
Central(config-std-nacl)#permit <LAN5> <WILDCARD-MASK>  
Central(config-std-nacl)#permit <LAN6> <WILDCARD-MASK>  
Central(config-std-nacl)#exit
```

3. Визначте пул *PUBLIC_PAT* придатних до використання публічних IP-адрес.

```
Central(config)# ip nat pool PUBLIC_PAT 209.165.202.158 209.165.202.158  
netmask 255.255.255.224
```

4. Визначте NAT з внутрішнього списку адрес *ACL_PAT* в пул зовнішніх адрес *PUBLIC_PAT* з параметром *overload*.

```
Central (config)#ip nat inside source list ACL_PAT pool PUBLIC_PAT overload
```

Крок 7. Перевірка роботи PAT

1. З командного рядка ПК в кожній із мереж LAN1-2, LAN4-LAN6 відправте echo-запити на IP-адресу Internet Server. Проекспериментуйте з більшою кількістю протоколів, таких як HTTP, HTTPS, telnet.

2. Відобразіть перетворення NAT на маршрутизаторі Central за допомогою команди «show ip nat translations». Додайте результати в табл. 7.2.

3. Перевірте статистику PAT, виконавши на Central команду «show ip nat statistics».

Скільки активних перетворень виконано? Скільки адрес мається в пулі? Скільки адрес вже виділено?

7.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- табл. 7.1 з вихідними даними для NAT;
- табл. 7.2 з перетвореннями NAT та поясненнями;

ми;

- команди налаштувань в ході виконання лабораторної роботи з коментарями;

- статистика роботи кожного типу NAT з відповідями на запитання;

- звіт та проект мережі з назвою за правилом *Surname_Group_lab7_KM.pkt*.

7.4 Питання для підготовки до захисту лабораторної роботи

1. У чому полягає перевага статичного NAT?

2. Навіщо потрібно використовувати NAT в мережі?

3. Які обмеження динамічного NAT?

4. Коли вузол повертає зовнішній глобальний адрес назад в пул для використання іншим вузлом?

5. У чому полягає перевага PAT?

8 ЛАБОРАТОРНА РОБОТА №8. ДОСЛІДЖЕННЯ КЕРУВАННЯ МЕРЕЖЕЮ НА ОСНОВІ КОМАНДНОГО РЯДКА ТА КОНТРОЛЕРА SDN

8.1 Мета роботи

Порівняти керування мережними пристроями через командний рядок CLI, мережний контролер SDN та запити API.

8.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій, методичні рекомендації до даної роботи і довідку в Packet Tracer (*Help->Content->Configuring Devices-> Network Controllers*), наступні питання:

- призначення Network Controllers (NC);
- конфігурація та керування NC за допомогою веб-інтерфейсу;
- документація API.

Вам поставлена задача зібрати інформацію про версію програмного забезпечення мережних пристроїв в організації та інші дані у вигляді таблиці 8.1.

Таблиця 8.1 – Інформація про мережні пристрої

Hostname	Type	Product ID	Software Version	MAC Address	Serial Number

У цій лабораторній роботі ви додасте Network Controller (NC) та порівняєте відмінності між керуванням мережею:

- за допомогою інтерфейсу командного рядка (CLI);
- за допомогою можливостей мереж SDN через графічний web-інтерфейс NC;
- за допомогою можливостей мереж SDN з використанням API (Application Programming Interface) та програми на мові Python.

SDN (Software-Defined Networking, програмно-конфігуровані мережі) – це набір керованих через Інтернет мережеских рішень, що забезпечують єдине джерело управління місцями розташування, інфраструктурою і пристроями. Основна ідея SDN – відділення функцій передачі трафіку від функцій управління, включаючи контроль як самого трафіку, так і здійснюють його передачу пристроїв. Згідно з концепцією SDN, вся логіка управління виноситься в контролери, які здатні відслідковувати роботу всієї мережі. SDN надає адміністраторам можливість управління та надання мережеских послуг з централізованого місця.

Доступ до різних функцій та стану інформації, доступних на пристроях мережевого контролера, можна отримати програмно через API REST через HTTP. Доступ до документації API можна отримати через довідку в Packet Tracer (*Help->Content->Network Controller API*). API Network Controller – це програмний інтерфейс, який надається Cisco для взаємодії з їхніми мережескими контролерами.

За допомогою API Network Controller розробники можуть автоматизувати конфігурацію, моніторинг та управління мережею, що дозволяє підвищити продуктивність та ефективність управління мережею.

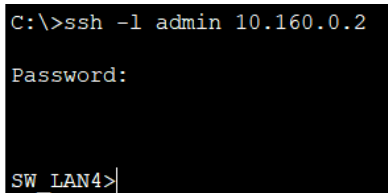
Далі виконати такі дії.

Частина 1. Використання CLI для збору інформації

В цій частині ви вручну отримуєте доступ до кожного пристрою, щоб отримати інформацію про версію програмного забезпечення.

Примітка: для віддаленого підключення до мережних пристроїв на них повинні бути виконані базові налаштування: назва пристрою, доступ до vty-ліній та пароль до привілейованого режиму, а на комутаторі ще IP-адреса та шлюз. Перевірте, щоб були відповідні налаштування на всіх маршрутизаторах та комутаторах.

1. На будь-якому ПК відкрити командний рядок *Desktop->Command Promt* та ввести команду «ssh -l», де -l — це літера «L», а не цифра один, та вказати IP-адресу найближчого комутатора (рис. 8.1).



```
C:\>ssh -l admin 10.160.0.2
Password:
SW_LAN4>
```

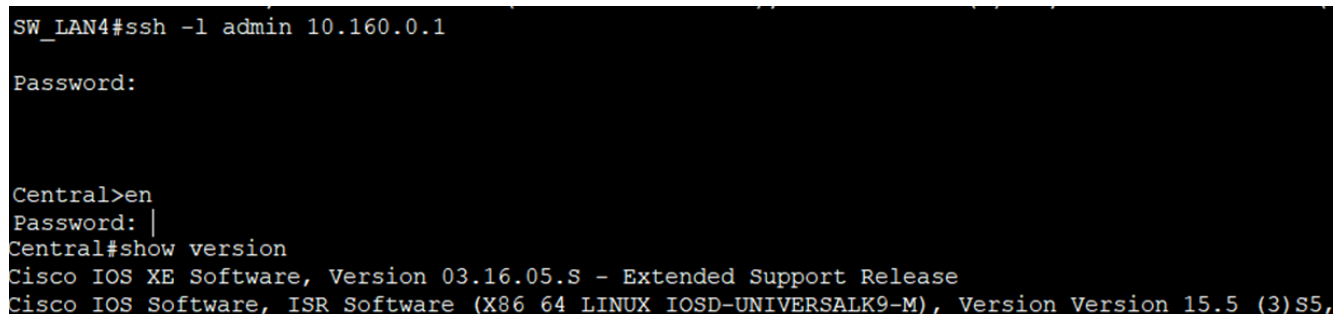
Рисунок 8.1 – Віддалене під'єднання до пристрою з ПК

2. Ввести пароль до vty (*cisco123*) та підключитись до пристрою.

3. Перейти в привілейований режим та отримати інформацію про програмне забезпечення пристрою IOS та інші дані (*show version*, *show license udi*).

4. Задokumentуйте у вигляді таблиці 8.1 для зберігання відомостей про цей мережний пристрій.

5. Спробуйте зібрати інформацію з решти мережевих пристроїв. Це можна зробити і з CLI поточного пристрою (рис.8.2).



```
SW_LAN4#ssh -l admin 10.160.0.1
Password:

Central>en
Password: |
Central#show version
Cisco IOS XE Software, Version 03.16.05.S - Extended Support Release
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5 (3)S5,
```

Рисунок 8.2 – Під'єднання до іншого пристрою з CLI

Частина 2. Використання web-інтерфейсу NC для збору інформації

Крок 1. Додавання та налаштування Network Controller

1. Додати в будь-яку мережу з блоку *End Devices* пристрій *Network Controller* (рис. 8.3). З'єднати через кабель *Straight-Throuhg* порт *Gig0* на NC з вільним портом на комутаторі.

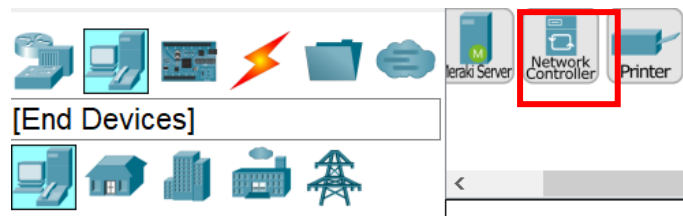


Рисунок 8.3 – Network Controller

2. Надати NC статичну незайняту IP-адресу з діапазону допустимих адрес в цій мережі, шлюз та адресу DNS-сервера.

Крок 2. Налаштування під'єднання до Network Controller

Доступ до NC можна отримати з реальної мережі та запрограмувати через його веб-API за допомогою Python від Visual Studio Code (VS Code).

1. В налаштуваннях програми *Options->Preferences* для зовнішнього доступу встановити відповідні прапорці (рис 8.4).

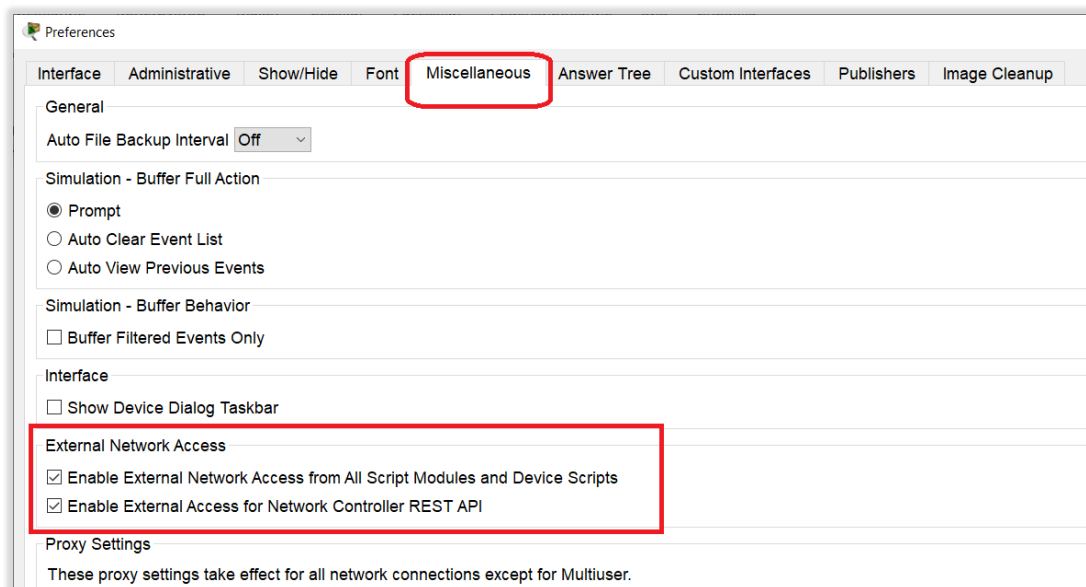


Рисунок 8.4 – Налаштування зовнішнього доступу в Packet Tracer

2. В налаштуваннях NC дозволити заданий номер порту, зазвичай 58000 (рис.8.5).

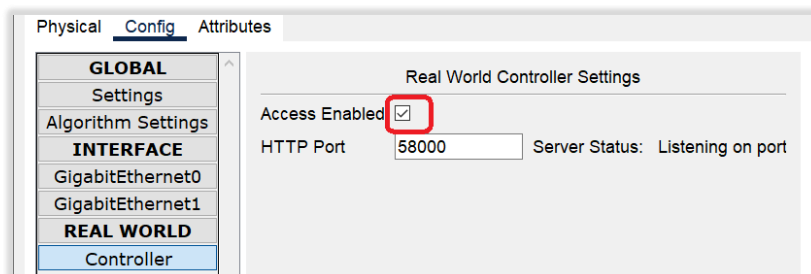


Рисунок 8.5 – Налаштування зовнішнього доступу на Network Controller

Примітка. Цей номер порту знадобиться при зовнішньому доступі до Packet Tracer з Web-браузера, VS Code і т.п.

Крок 3. Початкова конфігурація Network Controller

Щоб отримати доступ і керувати NC за допомогою веб-інтерфейсу, користувач повинен мати обліковий запис користувача рівня «administrator». Під час першого доступу до веб-інтерфейсу NC буде запропоновано виконати початкове налаштування, створивши такий обліковий запис, як показано нижче.

1. Перейти до будь-якого ПК та на вкладці *Desktop* обрати *Web Browser*. В полі URL вказати IP-адресу NC та натиснути *Go* (рис. 8.6). Або в веб-браузері введіть <http://127.0.0.1:58000> (рис. 8.7).

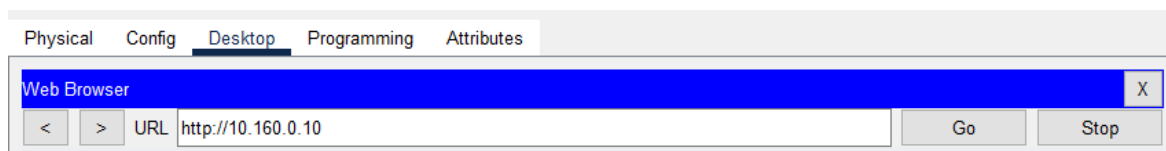


Рисунок 8.6 – Веб-сайт Network Controller з Packet Tracer



Рисунок 8.7 – Веб-сайт Network Controller з браузера

2. Використовуйте *Username*, *Password*, *Confirm Password* щоб ввести атрибути свого облікового запису та натисніть *Setup*, щоб створити новий обліковий запис (рис. 8.8).

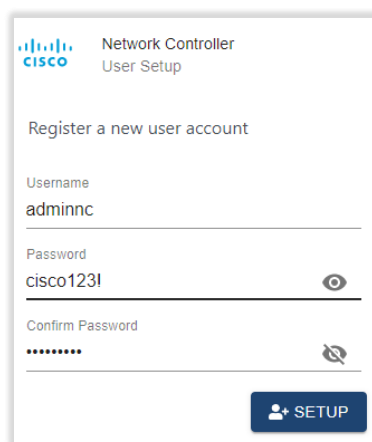


Рисунок 8.8 – Вікно створення облікового запису NC

Крок 4. Додавання облікових даних для доступу до всіх мережевих пристроїв у топології

Після входу у контролер тепер доступні усі дані про стан мережі, її топологія, адреси, проходження адрес, та здатність конфігурувати пристрої у мережі. Це так званий *Dashboard* (рис. 8.9).

На даному кроці відомості відсутні, тому налаштуємо NC для автоматичного виявлення пристроїв з використанням протоколу Cisco Discover Protocol (CDP).

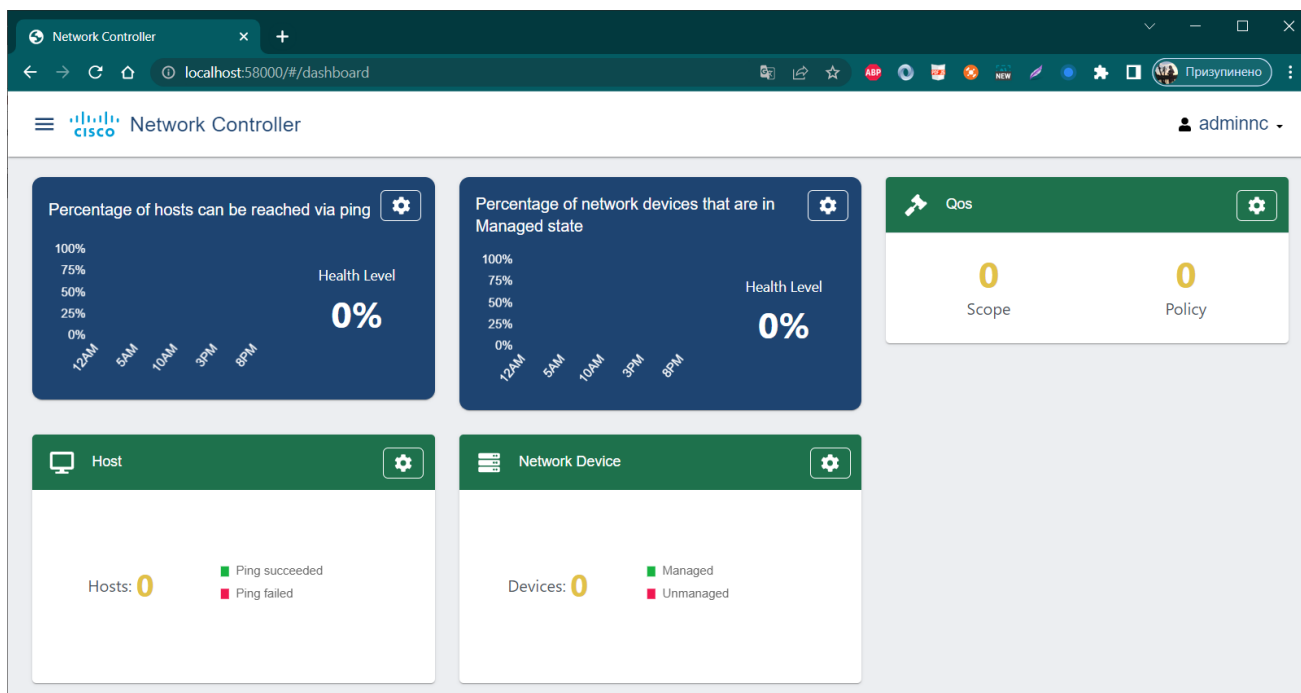


Рисунок 8.9 – Dashboard NC

3. Натиснути на 3 полоси зверху зліва та вибрати розділ *Provisioning* (рис. 8.10).

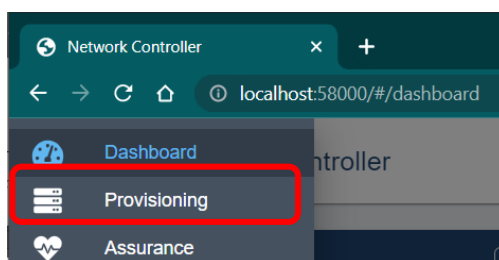


Рисунок 8.10 – Розділ Provisioning

4. Натиснути *CREDENTIAL*, а потім *+CREDENTIAL*, щоб додати нові облікові дані.

5. Додати дані користувача, які задавались в базовій конфігурації пристроїв (username *admin* password *cisco123*). Залишити *Enable Password* порожнім, ввести опис та натиснути *OKAY* (рис. 8.11).

The screenshot shows a 'New Credential' dialog box with the following fields and values:

- Username:** admin
- Password:** cisco123 (masked with dots)
- Enable Password:** (empty field)
- Description:** admin credential

At the bottom of the dialog, there are two buttons: 'CANCEL' and 'OKAY'.

Рисунок 8.11 – Додавання облікових даних

6. Нові облікові дані CLI тепер зберігаються на NC для використання в завданнях автоматизації (рис.8.12).

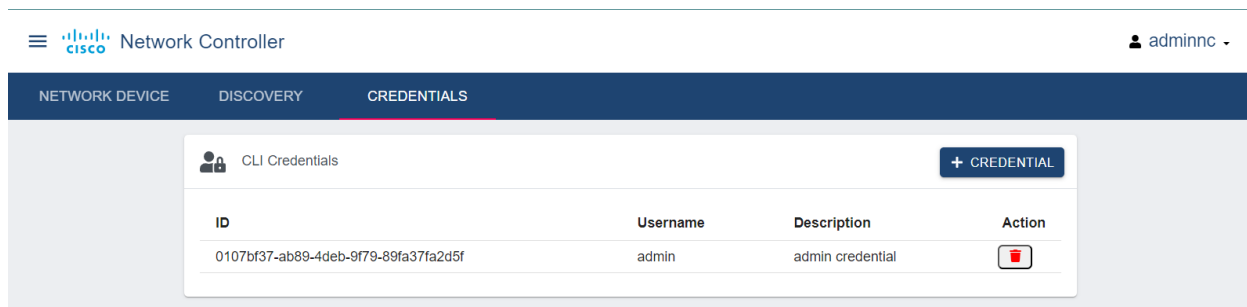


Рисунок 8.12 – Відомості про облікові дані CLI

Крок 5. Використання CDP для виявлення пристрої в мережі

7. Натиснути *DISCOVERY* а потім *+DISCOVERY*, щоб додати нове виявлення (рис. 8.13).

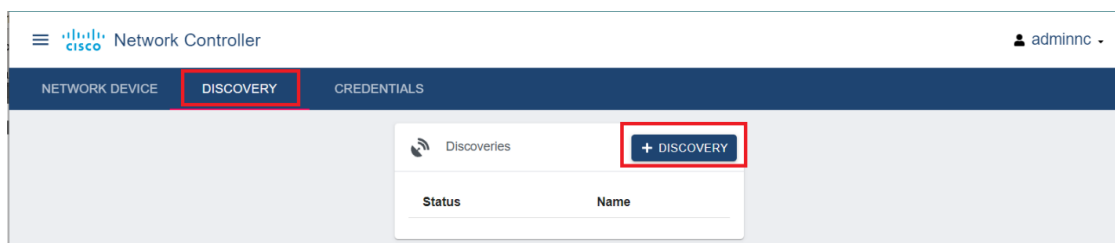


Рисунок 8.13 – Вкладка DISCOVERY

8. Надати назву пошуку, вказати IP-адресу шукаючого пристрою. Розкрити список і обрати створений *Credential*, натиснути *ADD* (рис. 8.14).

New Discovery

Discovery Type: CDP

Name: SW_LAN4

IP Address: 10.160.0.2

Timeout: 5

Retry: 3

CDP Level: 16

Credential: admin - admin credential

CANCEL ADD

Рисунок 8.14 – Створення *DISCOVERY* для виявлення пристрої в мережі

9. Тепер ви повинні побачити *Status as In Progress*. Зачекати, поки Packet Tracer завершить моделювання цього процесу.

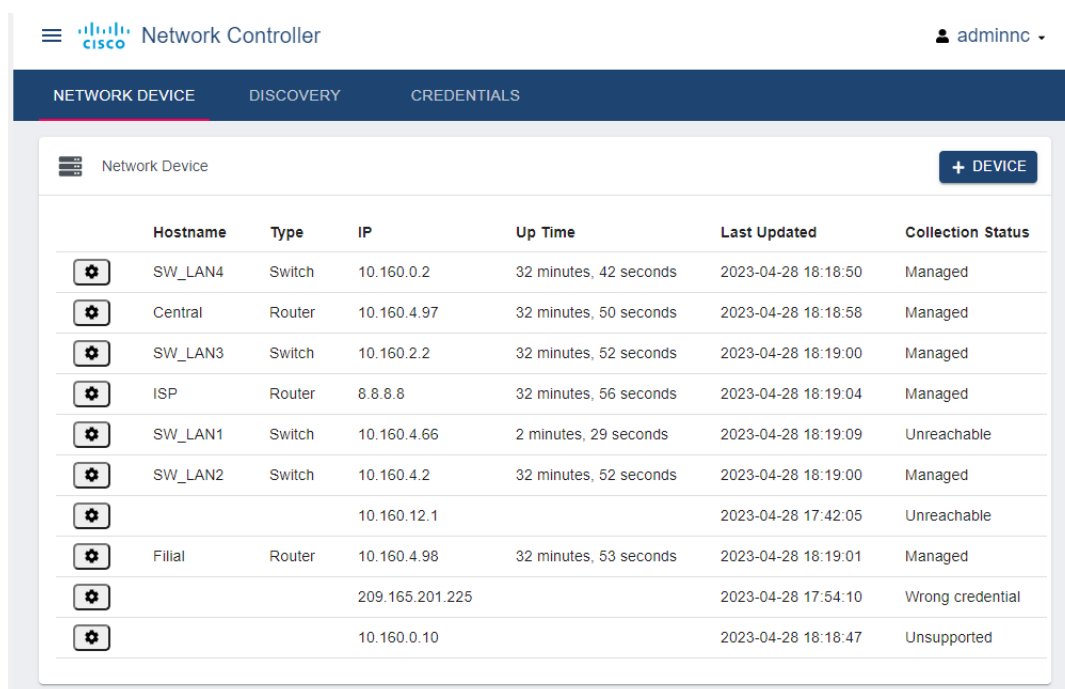
Крок 6. Використання графічного web-інтерфейсу NC для збору інформації

На цьому кроці буде використовуватися графічний web-інтерфейс NC для перегляду інформації про мережеві пристрої та хост-пристрої в топології.

1. Щоб переглянути список виявлених мережових пристроїв натиснути *NETWORK DEVICE*. Тепер ви повинні побачити всі мережові пристрої у списку (рис. 8.15).

2. Натиснути значок шестірні біля імені будь-якого пристрою, щоб переглянути інформацію, зібрану під час процесу виявлення. Зверніть увагу, що вказано версію програмного забезпечення, а також низку іншої детальної інформації про пристрій.

3. Доповніть табл. 8.1 інформацією про решту мережних пристроїв, яку ви не отримали через CLI.



	Hostname	Type	IP	Up Time	Last Updated	Collection Status
	SW_LAN4	Switch	10.160.0.2	32 minutes, 42 seconds	2023-04-28 18:18:50	Managed
	Central	Router	10.160.4.97	32 minutes, 50 seconds	2023-04-28 18:18:58	Managed
	SW_LAN3	Switch	10.160.2.2	32 minutes, 52 seconds	2023-04-28 18:19:00	Managed
	ISP	Router	8.8.8.8	32 minutes, 56 seconds	2023-04-28 18:19:04	Managed
	SW_LAN1	Switch	10.160.4.66	2 minutes, 29 seconds	2023-04-28 18:19:09	Unreachable
	SW_LAN2	Switch	10.160.4.2	32 minutes, 52 seconds	2023-04-28 18:19:00	Managed
			10.160.12.1		2023-04-28 17:42:05	Unreachable
	Filial	Router	10.160.4.98	32 minutes, 53 seconds	2023-04-28 18:19:01	Managed
			209.165.201.225		2023-04-28 17:54:10	Wrong credential
			10.160.0.10		2023-04-28 18:18:47	Unsupported

Рисунок 8.15 – Список пристроїв на NC

Частина 3. Використання API для збору інформації

Після налаштування всіх апаратних конфігурацій слід перейти до написання програми, яка буде збирати дані про мережеве обладнання. Реалізувати таку програму можна на скриптовій мові Python, яка є однією з найпопулярніших при роботі з даними. Бібліотека *requests* надає змогу працювати з мережевою інформацією за допомогою запитів *GET*, *POST*, *DELETE* та інших.

Програмний код реалізує наступну послідовність дій: запит для отримання сервісного токена для доступу до мережевого контролера за його IP-адресою. Після цього формується запит на отримання інформації про мережові прилади у вигляді JSON-файлу.

JSON – це текстовий формат обміну даними між комп'ютерами. JSON базується на тексті, може бути прочитаним людиною. Формат дає змогу описувати об'єкти та інші структури даних. Цей формат використовується переважно для передачі структурованої інформації через мережу завдяки процесу, що називають серіалізацією. Структура JSON-документу подібна до словника (*dictionary*) у мові Python, бо доступ до певного елемента можна отримати через відповідний ключ, або індекс.

1. На будь-якому ПК на вкладці *Programming* створіть пустий проект на мові Python та вставте в файл **main.py** скрипт з Додатку А. Дослідить та запустіть його. Програма виведить відомості про версії IOS мережних пристроїв (рис. 8.17) та додатково перелік користувачів на NC та їх роль.

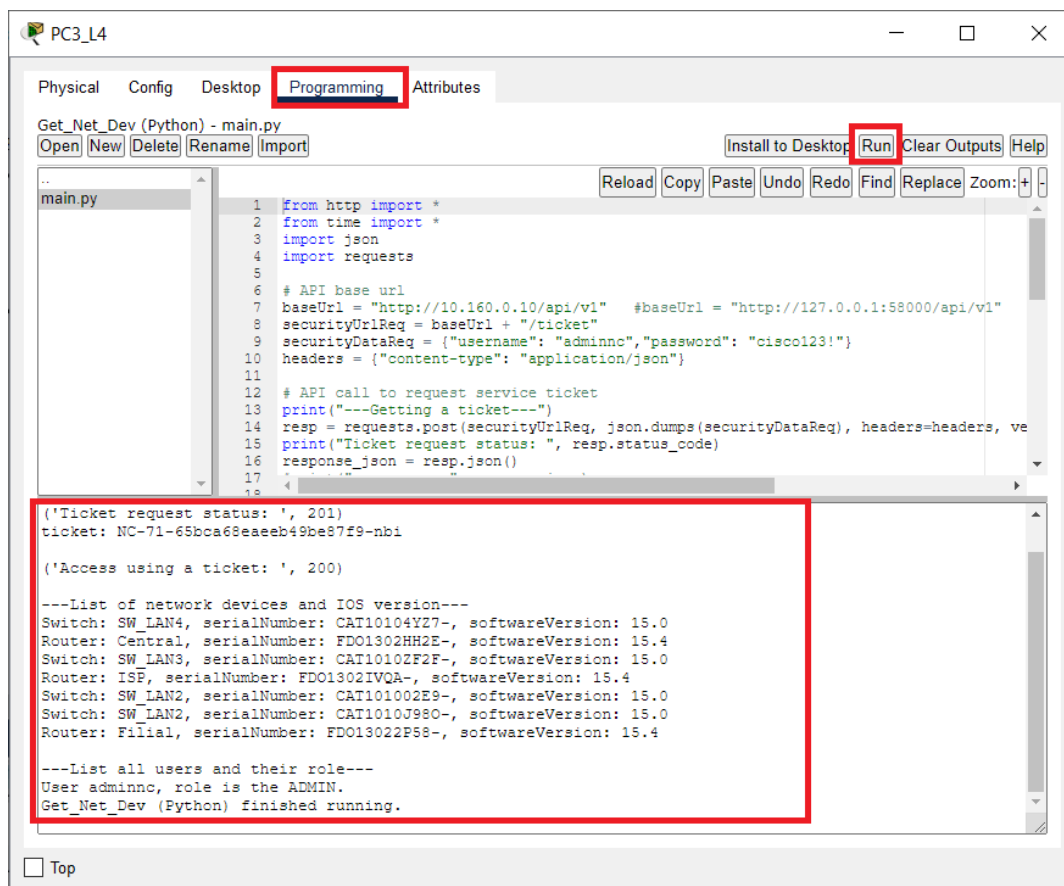


Рисунок 8.16 – Скрипт Python

Примітка. Код можна скопіювати і запустити і в будь-якому середовищі для розробки ПЗ (Visual Studio, Python IDE ...). В цьому випадку замініть baseUrl на адресу localhost:58000/api/v1

baseUrl = <http://127.0.0.1:58000/api/v1>

8.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- відомості про пристрої у вигляді табл. 8.1;
- список виявлених мережних пристроїв через графічний web-інтерфейс NC (вкладка *NETWORK DEVICE*);
- відомості про пристрої, отримані через API;
- проект мережі з назвою за правилом *Surname_Group_lab08.pkt*.

8.4 Питання для підготовки до захисту лабораторної роботи

1. Який метод отримання інформації про IOS мережних пристроїв був найшвидшим?
2. Які основні функції мережевого контролера в системі комп'ютерних мереж і як API взаємодіє з цими функціями?

3. Які переваги використання API для взаємодії з мережевим контролером порівняно із традиційними методами комунікації?

4. Як API мережевого контролера може бути застосовано в розробці додатків для моніторингу і керування мережевими ресурсами? Наведіть приклади використання.

5. Які основні аспекти безпеки повинні бути враховані при розробці API для мережевого контролера? Які заходи можна вжити для захисту від атак інших систем?

ДОДАТОК А.

Скрип на мові Python для збору інформації по мережні пристрої

```
from http import *
from time import *
import json
import requests

# API base url
baseUrl = http://10.50.4.10/api/v1
# baseUrl= «http://127.0.0.1:58000/api/v1»
securityUrlReq = baseUrl + «/ticket»
securityDataReq = {«username»: «adminnc», «password»: «cisco123!»}
headers = {«content-type»: «application/json»}

# API call to request service ticket
print(«---Getting a ticket---»)
resp = requests.post(securityUrlReq, json.dumps(securityDataReq),
headers=headers, verify=False)
print(«Ticket request status: », resp.status_code)
response_json = resp.json()
print(«response = », response_json)
ticket = response_json[«response»][«serviceTicket»]
print(«ticket: » + ticket+«\n»)

# Access using a ticket ...
headers = {«X-Auth-Token»: ticket }# X-Auth-Token header
resp = requests.get(baseUrl+«/network-device», headers=headers)# API
call to request list of network devices
print(«Access using a ticket: », resp.status_code)# This is the http
request status
result = resp.json()# Get the json-encoded content from response
print (json.dumps(result, indent=4))# Convert «response_json» object
to a JSON formatted string and print it out

# Parsing raw response to list network devices
(hostname+serialNumn=ber+version IOS)
print(«\n---List of network devices and IOS version---»)
print(«Hostname \t Type \t\t Product ID \t Software Ver. \t MAC
Address \t serialNumber»)

for i in result[«response»]:
    if(i[«type»]==»Switch» or i[«type»]==»Router»):
        print(i[«hostname»] + «\t\t» + i[«type»]+»\t\t» +i[«productId»]+»
\t\t» +i[«softwareVersion»]+ «\t\t» +i[«macAddress»]+»\t»
+i[«serialNumber»])

# Parsing raw response to list all users and their role
print(«\n---List all users and their role---»)
resp = requests.get(baseUrl+«/user», headers=headers)
result = resp.json()# Get the json-encoded content from response
for i in result[«response»]:
    for j in i[«authorization»]:
        print (User %s, role is
the %s.»%(i[«username»], (j[«role»])[5:])))
```

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Cisco Networking Academy: Learn Cybersecurity, Python & More. *Networking Academy*. URL: <https://www.netacad.com> (date of access: 15.01.2024).
2. Комп'ютерні мережі : підручник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.]. – Вінниця : ВНТУ, 2020. – 378 с.
3. Жураковський Б. Ю. Комп'ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковський, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 336 с. – Режим доступу до ресурсу: <https://ela.kpi.ua/handle/123456789/36615>.
4. Жураковський Б. Ю. Комп'ютерні мережі. Частина 2 Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковський, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 372 с. – Режим доступу до ресурсу: <https://ela.kpi.ua/handle/123456789/36641>
5. Wireshark · Go Deep. *Wireshark*. URL: <https://www.wireshark.org/> (date of access: 15.01.2024).
6. CIDR/VLSM Calculator – subnettingpractice.com. *subnettingpractice.com*. URL: <https://subnettingpractice.com/vlsm.html> (date of access: 15.01.2024).
7. VLSM Calculator. *VLSM Calculator*. URL: <https://vlsmcalc.vercel.app/> (date of access: 15.04.2024).
8. Каштан В.Ю. Комп'ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності F7 Комп'ютерна інженерія: у 2 ч. / В.Ю. Каштан, Я.В. Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. Техн. Ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2024. – Ч. 1. – 60 с.
9. Ramon Nastase. Cisco CCNA Command Guide: An Introductory Guide for CCNA & Computer Networking Beginners.– Independently published, 2018. – 74 p. ISBN-10: 1731124279, ISBN-13: 978-1731124272.
10. Ramon Nastase. IP Subnetting for Beginners: Your Complete Guide to Master IP Subnetting in 4 Simple Steps. – Independently published, 2018. – 67 p. ISBN-10: 1791770088, ISBN-13: 978-1791770082.
11. Natalia Olifer, Victor Olifer. Computer Networks: Principles, Technologies and Protocols for Network Design . – Wiley; 1st edition, 2016. – 992 p. - ISBN-10: 0470869828

Навчальне видання

Каштан Віта Юріївна
Панферова Яна Володимирівна
Бешта Лілія Валеріївна

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання лабораторних робіт
для здобувачів ступеня бакалавра
спеціальності F7 Комп'ютерна інженерія

У 2 частинах

Частина 2

Видано в авторській редакції.

Електронний ресурс.
Підписано до видання 16.07.2026. Авт. арк. 1,8.

Національний технічний університет «Дніпровська політехніка»
49005, м. Дніпро, просп. Дмитра Яворницького, 19