МИКОЛАЇВСЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МЕНЕДЖМЕНТУ
КАФЕДРА ЕКОНОМІЧНОЇ КІБЕРНЕТИКИ,
КОМП'ЮТЕРНИХ НАУК ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Адміністрування комп'ютерних систем та мереж

Методичні рекомендації
для практичних занять та самостійної роботи
здобувачів першого (бакалаврського) рівня вищої освіти
ОПП «Комп'ютерні науки»
за спеціальністю F3(122) «Комп'ютерні науки»
денної форми здобуття вищої освіти

Миколаїв
2026

УДК 004.7
А28

Друкується за рішенням науково-методичної комісії факультету менеджменту Миколаївського національного аграрного університету (протокол № 6 від 05 лютого 2026 р)

Укладачі:

С. І. Ємельянов – PhD, старший викладач кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

С. І. Тищенко – к.п.н., доцент, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

О. Ю. Пархоменко – к.ф.-м.н., доцент, доцент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

О. О. Жебко – асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету;

О. Є. Богатєнкова – асистент кафедри економічної кібернетики, комп'ютерних наук та інформаційних технологій Миколаївського національного аграрного університету

Рецензенти:

Махровська Н. А. – кандидат фізико-математичних наук, доцент кафедри теорії й методики природничо-математичної освіти та інформаційних технологій Миколаївський обласний інститут післядипломної педагогічної освіти

Полянський П. М. – кандидат економічних наук, доцент, доцент кафедри загальнотехнічних дисциплін Миколаївського національного аграрного університету

Адміністрування комп'ютерних систем та мереж : методичні рекомендації для А28 практичних занять та самостійної роботи здобувачів першого (бакалаврського) рівня вищої освіти ОПП «Комп'ютерні науки» за спеціальністю F3(122) «Комп'ютерні науки» денної форми здобуття вищої освіти / уклад. С. І. Ємельянов, С. І. Тищенко, О. Ю. Пархоменко, О. О. Жебко, О. Є. Богатєнкова. Миколаїв : МНАУ, 2026. 106 с.

УДК 004.7

ЗМІСТ

ПЕРЕДМОВА

Методичні рекомендації до практичних та самостійних занять призначені для формування у студентів цілісного розуміння принципів побудови, функціонування та підтримки сучасних інформаційних інфраструктур. У межах курсу увага зосереджується на вивченні архітектури комп'ютерних систем, основ мережевої взаємодії, принципів маршрутизації, протоколів передачі даних, бездротових технологій, мережевих служб та хмарних рішень. Практична складова дисципліни спрямована на розвиток навичок конфігурації обладнання, розгортання мережевих сервісів, забезпечення стабільності та безпеки мереж, а також моніторингу та оптимізації їхньої роботи.

Самостійна робота студентів відіграє важливу роль у закріпленні знань, отриманих під час занять, та сприяє розвитку відповідальності, аналітичного мислення й здатності до пошуку рішень у нестандартних ситуаціях. Методичні рекомендації містять орієнтири для практичної діяльності та рекомендації щодо виконання індивідуальних завдань, допомагаючи студентам поступово освоювати професійні компетентності у сфері адміністрування комп'ютерних систем та мереж.

Дані рекомендації створені для підтримки ефективного навчального процесу, формування практичних умінь та підготовки студентів до реальних умов роботи системного чи мережевого адміністратора, де важливими є не лише технічні знання, а й уміння працювати з інформацією, приймати рішення, забезпечувати надійність, продуктивність та безпеку мережевих інфраструктур.

ПРАКТИЧНА РОБОТА №1
Створення локальної мережі

Мета роботи: сформувати уміння проєктувати, налаштовувати та тестувати локальну комп’ютерну мережу відповідно до базових принципів мережевої інженерії. Навчитись аналізувати вимоги до мережі, обирати відповідну топологію, здійснювати підключення обладнання, налаштовувати параметри мережевих інтерфейсів та перевіряти працездатність мережевих з’єднань.

Матеріали та ресурси: комп’ютери або ноутбуки, мережеві кабелі (патч-корди), маршрутизатор або комутатор, а також доступ до мережевого симулятора (Cisco Packet Tracer).

Завдання для роботи під час заняття

1. Створення локальної мережі

1. Додайте на робочу область програми 5 комутаторів Switch 2960-24TT. За замовчуванням вони називаються Switch0 – Switch4.

2. Додайте на робоче поле 8 комп'ютерів з іменами за замовчуванням PC0 – PC7.

3. Об’єднайте пристрої до мережі Ethernet, як показано на рис. 1.1. Комп'ютер з комутатором об’єднуються витою парою, а комутатори між собою – крос-кабелем. Всі пристрої для підключення використовують порти FastEthernet.

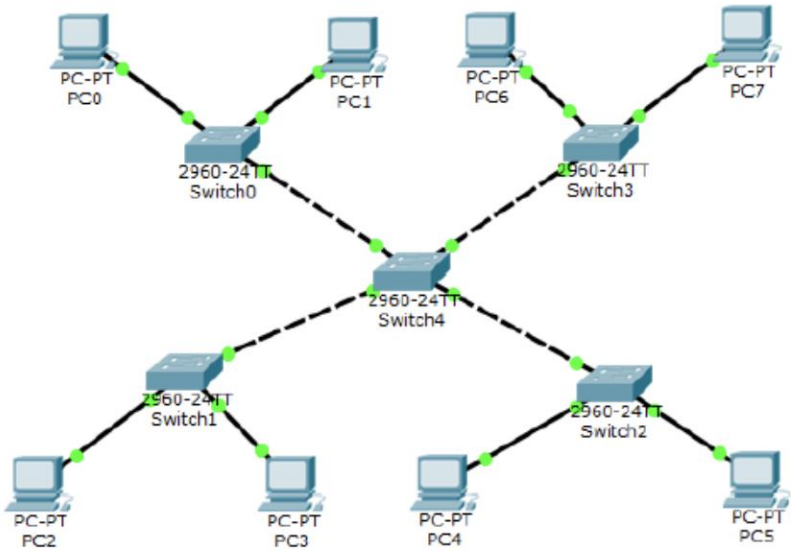


Рис. 1.1. Модель мережі Ethernet

4. Збережіть створену топологію за допомогою команди *Save* в меню *File*.

5. Відкрийте вікно властивостей пристрою PC0, клацнувши лівою кнопкою миші на його зображення. Перейдіть на вкладку *Desktop*і відкрийте

командний рядок, натиснувши на *Command Prompt*.

6. Для виведення списку доступних команд в командний рядок внесіть *?* та натисніть *Enter*.

7. Налаштування комп'ютера здійснюється за допомогою команди *ipconfig*. Наприклад, для того, щоб задати PC0 мережеву адресу *192.168.1.2* і маску *255.255.255*.0 в командному рядку потрібно внести:

```
ipconfig 192.168.1.2 255.255.255.0
```

8. Для перевірки присвоєних значень мережевої адреси і маски в командний рядок потрібно повторно ввести ipconfig. З'явиться повідомлення про задані мережні параметри пристрою:

```
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.........: FE80:230:A3FF:FEAA:BD12
IP Address.....................: 192.168.1.2
Subnet Mask....................: 255.255.255.0
Default Gateway................: 0.0.0.0
```

9. IP-адресу та мережеву маску мережі також можна встановити використовуючи графічний інтерфейс пристрою. Для цього у вікні *Desktop* необхідно набрати *IP Configuration.* Відкриється вікно, що зображено на рис. 1.2. Мережева адреса вводиться в поле *IP Adress*, а маска – в поле *Subnet Mask*. Перемикач способу присвоєння IP-адреси повинен бути в положенні *Static*.

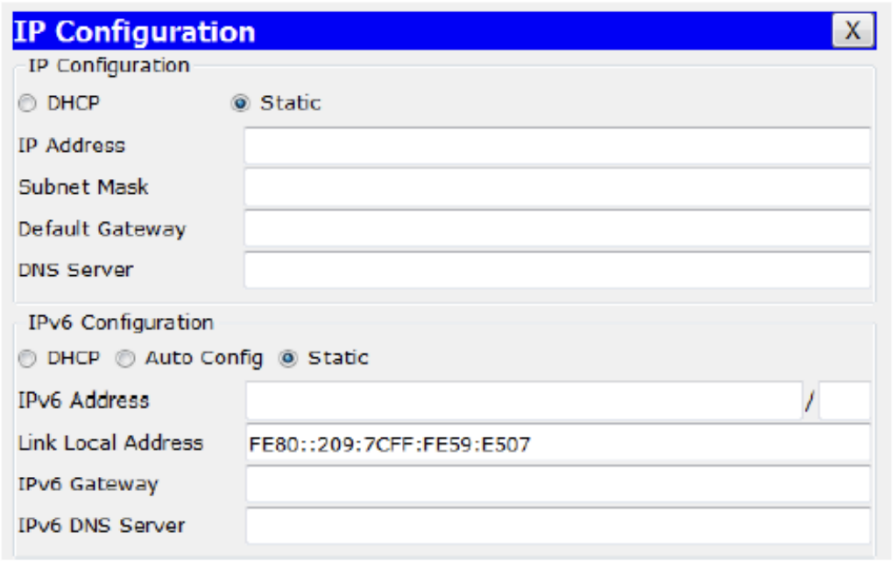


Рис. 1.2. Вікно налаштувань IP Configuration

10. Аналогічно для решти комп’ютерів призначте адреси використовуючи один з перерахованих вище способів. Мережні адреси та маска підмережі пристроїв наведені в таблиці. 1.1.

Таблиця 1.1. Налаштування комп'ютерної мережі

Ім’я компютера	IP-адреса	Маска підмережі
ПК0	192.168.1.2	255.255.255.0
ПК1	192.168.1.3	255.255.255.0
ПК2	192.168.1.4	255.255.255.0
ПК3	192.168.1.5	255.255.255.0
ПК4	192.168.1.6	255.255.255.0
ПК5	192.168.1.7	255.255.255.0
ПК6	192.168.1.8	255.255.255.0
ПК7	192.168.1.9	255.255.255.0

11. Перевірте правильність мережевих налаштувань пристроїв та роботоздатність мережі за допомогою команди *ping*. Для цього, потрібно відкрити командний рядок пристрою, ввести *ping* і IP-адресу іншого мережевого пристрою. Наприклад, зайдемо на комп'ютер PC0 і «пропінгуємо» комп'ютер PC1. Нижче наведені результати виконаної команди *ping:*

```
PC>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 4, Lost =0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Таким чином, якщо пристрої мережі сконфігуровані правильно, можна пропінгувати з кожного комп’ютера будь-який інший.

12. У середовищі Packet Tracer можна простежити рух пакетів різних мережевих протоколів з допомогою режиму симуляції. Щоб перейти до режиму

симуляції, натисніть кнопку *Simulation Mode* у правому нижньому куті робочої області або комбінацію клавіш *Shift+S*.

Справа від робочої області відкриється вікно *Simulation Panel* (див. рис. 1.3), в верхній частині якого знаходиться область подій *Event List* та кнопка очистки списку подій *Reset Simulation*. Управління відтворенням здійснюється з допомогою кнопок *Play Controls*. Так для переходу до наступнеої події потрібно натиснути кнопку *Capture / Forward.* В нижній частині вікна знаходиться фільтр потоків.

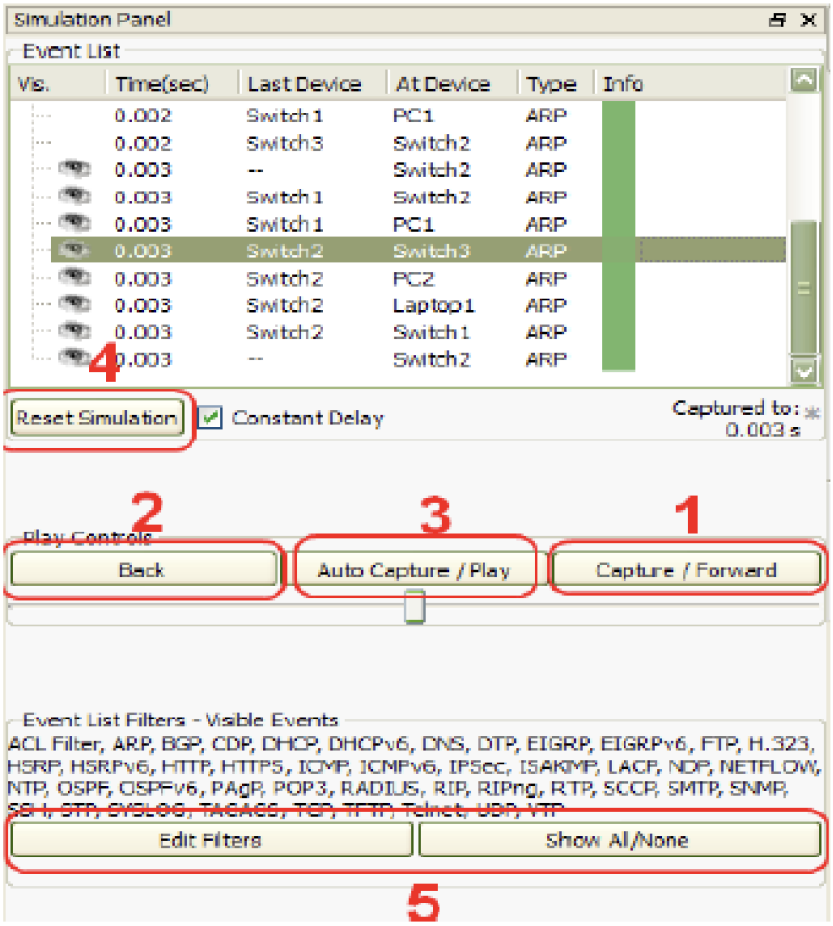


Рис. 1.3. Вікно Simulation Panel

13. З вузла PC1 пропінгуйте вузол PC3. Для того щоб виключити випадковий трафік між вузлами із запропонованого для дослідження списку протоколів виберіть тільки протокол ICMP. Відкрийте командний рядок пристрою PC1, введіть *ping* та IP-адресу мережевого пристрою PC3. В результаті таких дій на вузлі PC1 утвориться пакет («конверт») (рисунок 1.4).

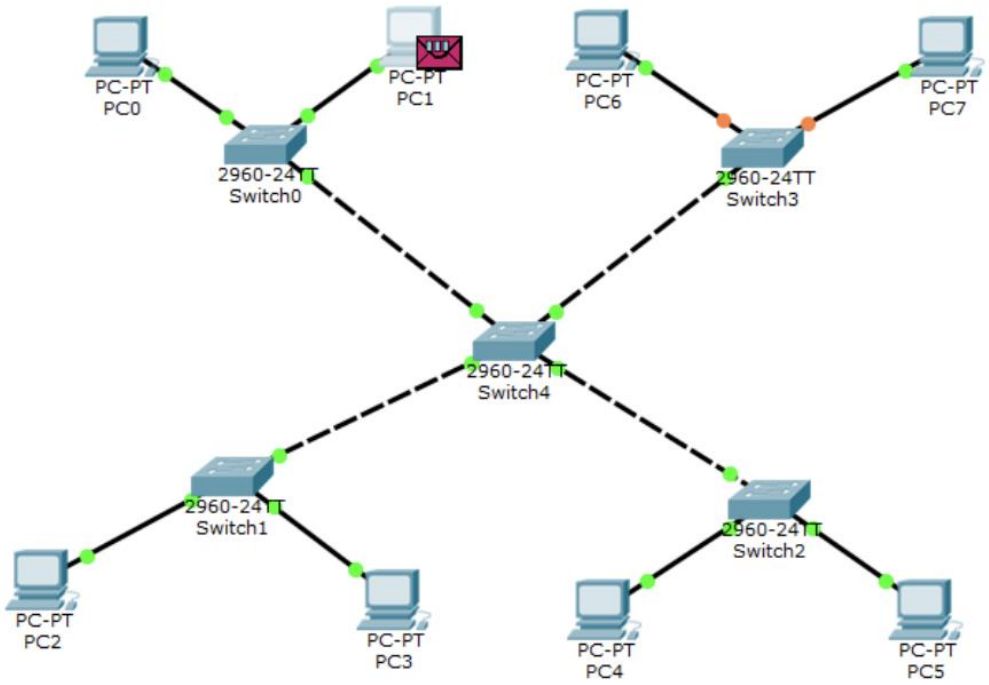


Рис. 1.4. Створення запиту в режимі симуляції

При цьому в полі *Event List* з'явиться даний пакет з зазначенням його типу (рис.1.5.).

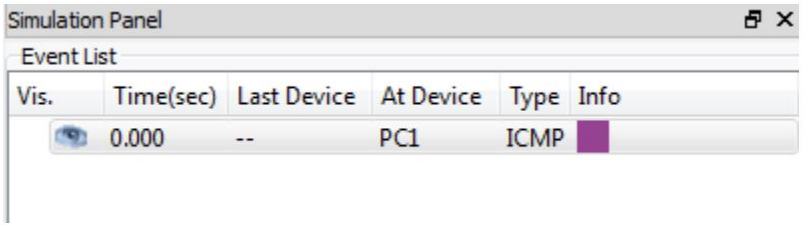
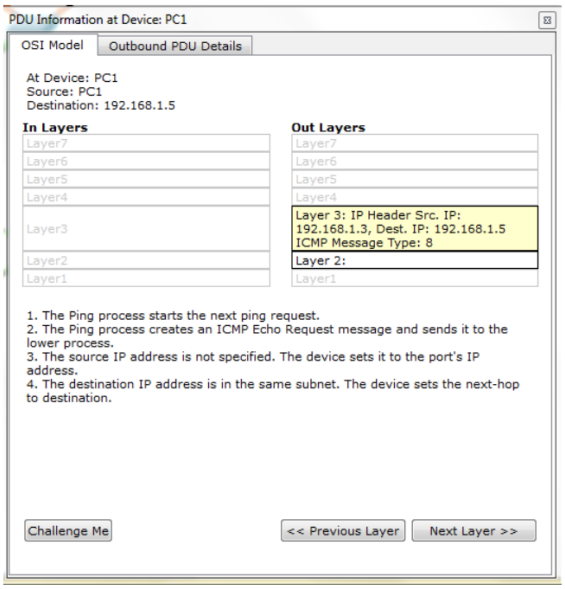


Рис. 1.5. Контроль роботи протоколів

Для отримання більш детальної інформації про пакет, натисніть на нього лівою кнопкою миші. На вкладці *OSI Model* можна побачити, на якій мережевій моделі OSI був сформований пакет та які рівні він пройде для переходу на наступний вузол (рис. 1.6). На вкладці *Outbound PDU Details* відображається структура пакету (рис. 1.7)



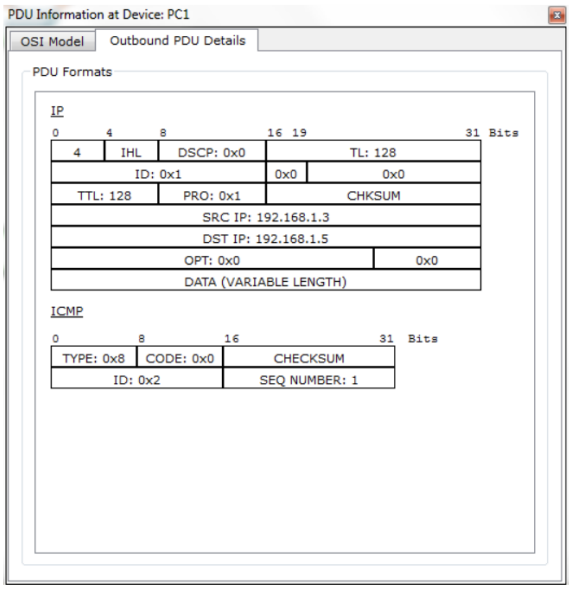


Рис. 1.5. Пакет на рівнях моделі OSI **Рис. 1.6.** Структура пакету

14. Щоб запустити пакет в мережу, потрібно натиснути кнопку *Capture / Forward* у вікні *Simulation Panel*. Пакет перейде на комутатор Switch0, оскільки це єдине мережеве підключення вузла PC1. Комутатор Switch0 пересилає пакет на комутатор Switch4. У свою чергу, комутатор Switch4 пересилає пакет на Switch1, а потім Switch1 надсилає той пакет на вузол PC3., PC3, після отримання пакета, визначає, що він призначений для нього, і, сформувавши відповідь, відправляє пакет на PC1.

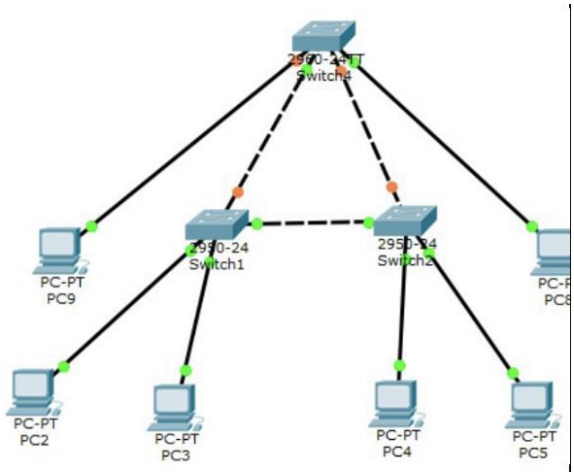
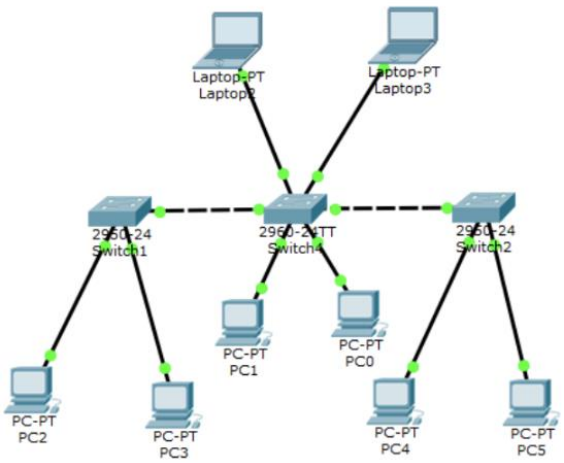
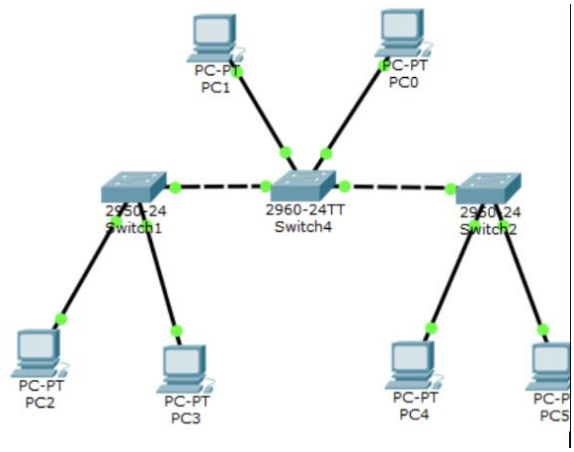
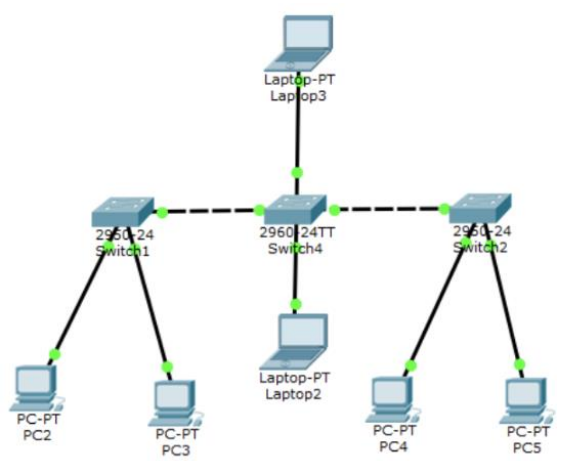
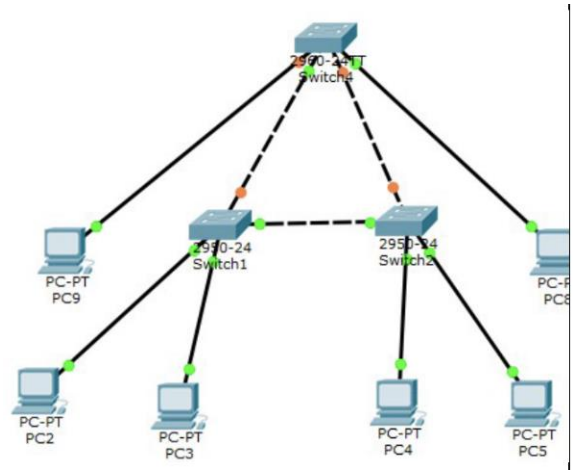
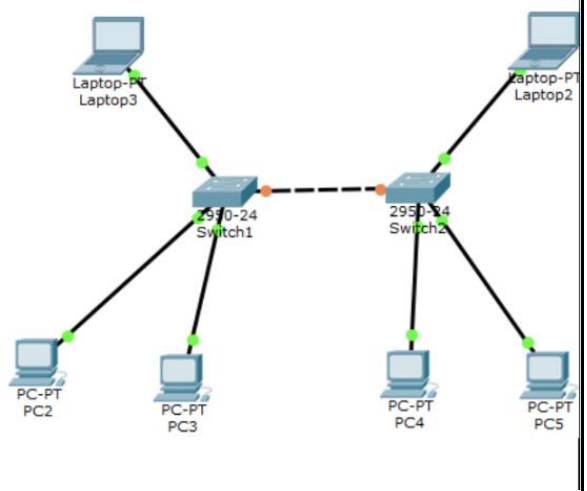
Після того, як PC1 отримав відповідь від PC3, у вікні командного рядка з’явиться запис, що повідомляє про проходження ехо-запиту:

```
PC>ping 192.168.1.5
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time=7ms TTL=128
```

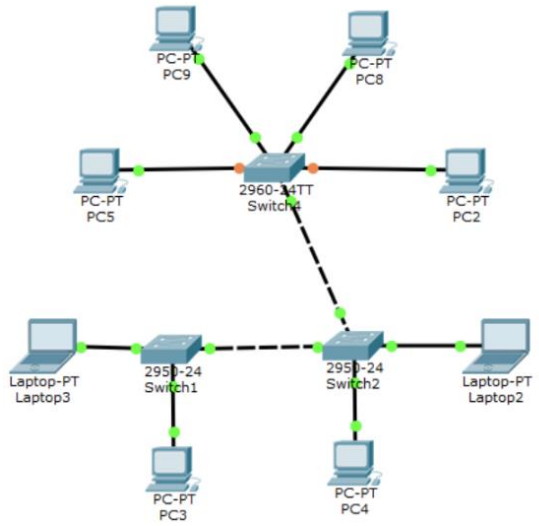
Завдання для самостійної роботи

1. Створіть топологію мережі відповідно до варіанту (табл. 1.2). У всіх варіантах в якості комутаторів використайте Switch 2960.
2. Призначте комп’ютерам IP-адреси відповідно до вказаного діапазону адрес (Таблиця 1.3). Мережева маска для всіх пристроїв 255.255.255.0.
3. Дайте всім кінцевим вузлам різні імена.
4. Перевірте налаштування кожного кінцевого вузла (команда *ipconfig*).
5. Перевірте всі з'єднання між комп'ютерами (команда *ping*).
6. У режимі симуляції надішліть запит (команда *ping*) з PC3 до PC5. Відстежуйте рух пакета ICMP.

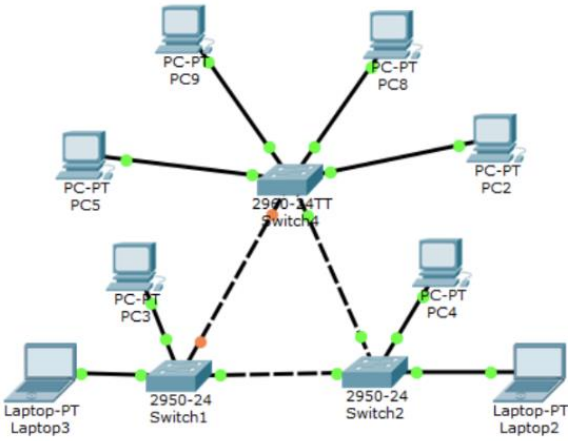
Таблиця 1.2. Параметри завдання топології мережі

Варіант 1	Варіант 2
	
Варіант 3	Варіант 4
	
Варіант 5	Варіант 6
	

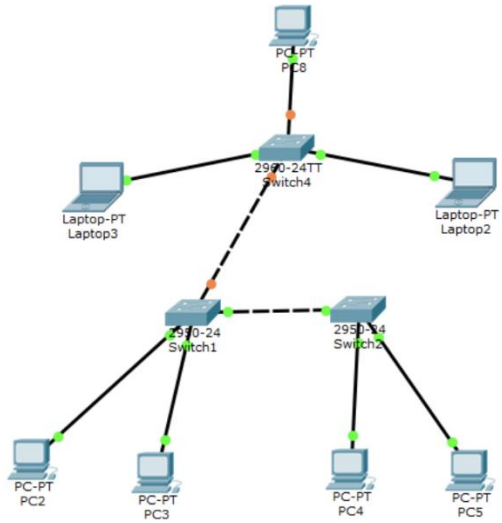
Варіант 7



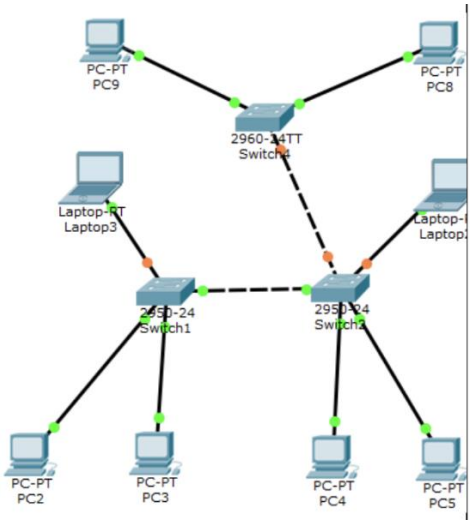
Варіант 8



Варіант 9



Варіант 10



Таблиця 1.3. Варіанти діапазонів адрес

№ варіанта	**1**	**2**	**3**	**4**	**5**
Діапазон адрес	112.168.5.15 112.168.5.25	12.208.6.15 12.208.6.25	144.18.9.15 144.18.9.25	133.73.9.60 133.73.9.69	12.208.6.15 12.208.6.25
№ варіанта	**6**	**7**	**8**	**9**	**10**
Діапазон адрес	13.18.0.45 13.18.0.55	152.164.8.75 152.164.8.85	122.8.85.45 122.8.85.55	155.38.0.0 155.38.0.9	212.28.68.15 212.28.68.25

Питання для обговорення на занятті

1. Які фактори потрібно враховувати під час проєктування локальної мережі в організації?
2. Чим відрізняються основні типи топологій мережі та коли доцільно використовувати кожну з них?
3. Чому IP-адресація є критично важливою для коректної роботи мережі?
4. Які переваги та недоліки має використання комутаторів у порівнянні з концентраторами?
5. Яким чином вибір мережевих кабелів (UTP, STP, оптоволокно) впливає на роботу мережі?
6. Чому важливо розуміти різницю між приватними та публічними IP-адресами?
7. Які типові проблеми можуть виникати під час налаштування локальної мережі та як їх швидко діагностувати?
8. Яку роль відіграють мережеві протоколи (ARP, DHCP, ICMP) у функціонуванні локальної мережі?
9. Чим мережеві симулятори корисні для навчання побудові локальних мереж?
10. Як масштабованість мережі впливає на вибір обладнання та топології?

Тестові запитання

1. Який пристрій використовується для з’єднання комп’ютерів у локальній мережі?

A. Маршрутизатор;
B. Комутатор;
C. Модем;
D. Межмережевий екран.

2. Що визначає маска підмережі?

A. Швидкість мережі;
B. Довжину кабелю;
C. Межі мережі та кількість доступних адрес;
D. Тип операційної системи.

3. Який протокол використовується для перевірки доступності вузлів у мережі?

A. ICMP (ping);
B. HTTP;

C. FTP;
D. DNS.

4. Який тип топології є найпоширенішим у сучасних локальних мережах?
A. Кільце;
B. Шина;
C. Зірка;
D. Дерево без розгалужень.

5. Який тип кабелю зазвичай застосовується для Ethernet-підключень?
A. HDMI;
B. UTP;
C. USB-C;
D. VGA.

6. Який елемент мережі відповідає за розподіл IP-адрес, якщо використовується автоматична конфігурація?
A. DNS-сервер;
B. DHCP-сервер;
C. FTP-сервер;
D. SSH-сервер.

7. Яка адреса є приватною?
A. 8.8.8.8;
B. 172.16.0.5;
C. 203.0.113.10;
D. 150.10.0.1.

8. Яка команда використовується для перегляду параметрів мережевого інтерфейсу у Windows?
A. ls;
B. ipconfig;
C. netstat;
D. ifconfig.

9. Що є ключовою ознакою працездатності мережі після налаштування?
A. Можливість запуску браузера;
B. Наявність відповіді на ping від інших вузлів;
C. Робота антивіруса;

D. Підключення USB-пристрою.

10. Яка роль ARP у локальній мережі?
A. Визначає маршрут пакетів між мережами;
B. Перетворює IP-адреси на MAC-адреси;
C. Забезпечує шифрування трафіку;
D. Надає доменні імена.

ПРАКТИЧНА РОБОТА №2
Налаштування Proxmox VE та створення віртуальної машини

Мета роботи: сформувати практичні навички встановлення, первинного налаштування та використання платформи Proxmox Virtual Environment (Proxmox VE) для створення та керування віртуальними машинами. Навчитися працювати з веб-інтерфейсом Proxmox, правильно конфігурувати апаратні параметри віртуальних машин, обирати образи операційних систем, керувати ресурсами, а також розуміти принципи роботи гіпервізора та віртуалізаційних технологій.

Матеріали та ресурси: комп'ютери або сервер із встановленим Proxmox VE, доступ до веб-інтерфейсу Proxmox через браузер, інсталяційні ISO-образи операційних систем (наприклад, Ubuntu Server, Windows Server або інші), а також мережеве підключення для взаємодії з гіпервізором.

Завдання для роботи під час заняття

0. Завантажте та встановіть необхідне ПЗ (у VirtualBox необхідно створити віртуальну машину та встановити на неї Proxmox):

- VirtualBox - https://www.virtualbox.org/wiki/Downloads
- Proxmox VE 8.4 ISO Installer - https://www.proxmox.com/en/downloads/proxmox-virtual-environment

1. Ознайомлення з інтерфейсом Proxmox VE та підготовка до роботи

1. Увійдіть до веб-інтерфейсу Proxmox через браузер, використовуючи адресу на кшталт: https://IP-адреса-сервера:8006
2. Уведіть логін і пароль адміністратора.
3. Після входу уважно ознайомтесь з основними розділами лівої панелі:
    - Datacenter — загальні налаштування всього кластера;
    - Node (вузол) — сервер, на якому розташовані ВМ;
    - Disks — сховища й типи дисків;
    - Shell — термінал вузла;
    - System / Network / Updates — системні параметри.
4. Натисніть на вузол (наприклад, pve) і перегляньте, які ресурси доступні: кількість ядер процесора, обсяг оперативної пам'яті, розмір дисків, використання ресурсів у реальному часі.
5. Ознайомтесь з вкладкою Storage, де зберігаються ISO-образи, диски ВМ та резервні копії.

2. Додавання ISO-образу та аналіз параметрів майбутньої ВМ

1. Знайдіть в лівій панелі сховище, яке містить тип ISO Image (зазвичай це local або local-lvm).

2. Виберіть вкладку ISO Images → Upload та завантажте образ операційної системи (наприклад, Ubuntu Server або Windows).

3. Після завантаження образ з'явиться у списку — перевірте, що файл коректний.

4. Визначте параметри майбутньої віртуальної машини:
   - скільки CPU-ядр їй потрібно;
   - скільки оперативної пам'яті потрібно (наприклад, 1–4 ГБ для Linux);
   - який розмір диска буде достатнім (20–40 ГБ);
   - чи потрібний швидкий тип диска (VirtIO);
   - тип мережевого адаптера (VirtIO або e1000).

3. Створення віртуальної машини в Proxmox VE

1. Натисніть кнопку Create VM у правому верхньому куті.
2. У вкладці *General* задайте ID ВМ (автоматично генерується) та напишіть коротку назву, наприклад Ubuntu-Server-Test.
3. У вкладці *OS* виберіть раніше доданий ISO-образ, визначте тип ОС (Linux/Windows).
4. У вкладці *System* встановіть тип BIOS (OVMF або SeaBIOS), залиште інші параметри за замовчуванням.
5. У вкладці *Hard Disk* виберіть тип диска (VirtIO — найшвидший), задайте розмір диска (наприклад, 20 ГБ).
6. У вкладці *CPU* встановіть кількість ядер (наприклад, 2).
7. У вкладці *Memory* встановіть RAM (наприклад, 2048 МБ).
8. У вкладці *Network* виберіть VirtIO NIC, підключіть до bridge vmbr0.
9. Натисніть Finish.

4. Установка ОС всередині віртуальної машини

1. Виберіть створену VM та натисніть Start.
2. Перейдіть у вкладку Console.
3. Дочекайтеся завантаження інсталятора ОС.
4. Виконайте стандартний процес інсталяції: виберіть мову, налаштуйте диск (звичайна розмітка), створіть адміністратора, налаштуйте мережу (DHCP або статично).
5. Дочекайтеся завершення встановлення.
6. Перезавантажте ВМ.
7. Увійдіть в систему і перевірте її працездатність командами:

```
uname -a
ip a
```

```
ping 8.8.8.8
```

5. Створення snapshot і керування параметрами ВМ

1. Зупиніть або поставте на паузу ВМ.
2. Перейдіть у вкладку Snapshots.
3. Натисніть Take Snapshot та дайте йому назву, наприклад clean-install.
4. Змініть параметри ВМ: додайте 1 ядро CPU; збільшіть RAM (наприклад, до 3 ГБ).
5. Перезапустіть ВМ та оцініть, чи зміни вплинули на швидкість роботи.
6. За бажанням протестуйте функції Stop, Reset, Suspend, Backup.

Завдання для самостійної роботи

Оберіть будь-яку операційну систему, яку ви плануєте встановити у віртуальне середовище (наприклад, Ubuntu Server або Windows). На основі цього коротко опишіть вимоги до ресурсів обраної ОС, після чого сформуйте план створення віртуальної машини: вкажіть, який обсяг оперативної пам’яті, кількість ядер процесора, тип мережевого адаптера та розмір віртуального диска ви оберете й чому. Далі опишіть послідовність дій зі сторони користувача в Proxmox VE: як знайти та завантажити ISO-образ, у якому розділі створюється VM, які параметри необхідно налаштувати під час проходження майстра створення.

Питання для обговорення на занятті

1. Які переваги використання Proxmox VE у порівнянні з традиційною фізичною інфраструктурою?
2. Чому важливо правильно планувати ресурси (CPU, RAM, Storage) перед створенням віртуальної машини?
3. Які можливості та функції веб-інтерфейсу Proxmox є найбільш корисними для адміністратора?
4. Чим відрізняється локальне сховище (local, local-lvm) від мережевих сховищ (NFS, ZFS, Ceph)?
5. Навіщо використовувати ISO-образи і які вимоги до них під час створення VM?
6. Які фактори впливають на вибір параметрів віртуальної машини (кількість ядер CPU, обсяг пам’яті, тип диска)?
7. Чим відрізняються типи BIOS/UEFI у Proxmox і коли кожен із них потрібен?
8. Яку роль відіграє мережевий інтерфейс VirtIO, і чому його рекомендують використовувати?

9. Чому важливо створювати snapshot перед внесенням змін у віртуальну машину?

10. Які основні відмінності між snapshot, backup та шаблоном (template) у Proxmox VE?

Тестові запитання

1. Що таке Proxmox VE?

A. Хмарна CRM-система;

B. Платформа для віртуалізації та контейнеризації;

C. Брандмауер для захисту мережі;

D. Інструмент для розробки програм.

2. Через який порт за замовчуванням здійснюється доступ до веб-інтерфейсу Proxmox?

A. 22;

B. 8080;

C. 443;

D. 8006.

3. Для чого використовується ISO-образ у Proxmox VE?

A. Для збереження snapshot;

B. Для керування мережевими адаптерами;

C. Для встановлення операційної системи у віртуальну машину;

D. Для резервного копіювання.

4. Який тип віртуального диска вважається найшвидшим у Proxmox?

A. IDE;

B. SATA;

C. VirtIO;

D. USB.

5. Який тип віртуального мережевого інтерфейсу рекомендується використовувати для кращої продуктивності?

A. e1000;

B. Realtek;

C. VirtIO;

D. vHost-off.

6. Що робить функція Snapshot?

A. Видаляє старі резервні копії;

B. Створює повний шаблон ВМ;

C. Зберігає поточний стан ВМ для можливого повернення;

D. Перезавантажує вузол Proxmox.

7. Який тип BIOS зазвичай обирають для сучасних операційних систем?

A. SeaBIOS;

B. Basic BIOS;

C. UEFI (OVMF);

D. Legacy Boot.

8. У якому розділі Proxmox можна переглянути параметри CPU, RAM та використання ресурсів вузла?

A. Datacenter → Permissions;

B. Node → Summary;

C. Storage → ISO Images;

D. VM → Snapshots.

9. Яка команда перевіряє мережеву доступність у консольному режимі VM?

A. uname -a;

B. ls;

C. ping;

D. top.

10. Що є перевагою Proxmox VE?

A. Підтримка лише однієї операційної системи;

B. Відсутність веб-інтерфейсу;

C. Підтримка кластерів, високої доступності та контейнерів;

D. Неможливість створювати резервні копії.

ПРАКТИЧНА РОБОТА №3
Обчислення підмереж IPv4

Мета роботи: сформувати практичні навички поділу мережі на підмережі, розуміння структури IPv4-адреси, роботи з масками підмереж та визначення діапазонів адрес. Навчитися аналізувати вимоги до мережі, обирати оптимальну кількість підмереж, розраховувати маску для кожної з них і правильно визначати мережеву адресу, адресу першого та останнього хоста, а також широкомовну адресу.

Матеріали та ресурси: комп'ютери та доступ до калькулятора підмереж, таблиці бінарних чисел і CIDR-нотацій, симулятор мережі (Packet Tracer), текстовий редактор.

Завдання для роботи під час заняття

1. **Визначення адреси мережі, якщо відомі IP-адреса хоста і підмережа**

➢ **Приклад 1**

Визначте адресу мережі, якщо IP-адреса хоста *192.168.10.10 і* маска підмережі *255.255.255.0.*

Розв'язання:

- переводимо IP-адресу з десяткової системи числення в двійкову: *192.168.10.10 = 110000000.10101000.00001010.0000101010* ;
- перетворюємо маску мережі з десяткової системи числення на двійкову: *255.255.255.0 = 11111111.11111111.11111111.00000000* ;
- додаємо IP-адресу з маскою за допомогою логічної операції «І». *1100000000.10101000.00001010.00001010 (IP-адреса)*
  І
  111111111.11111111.11111111.00000000 (маска)
  =
  1100000000.10101000.00001010.00000000 (мережева адреса) ;
- переводимо адресу мережі з двійкової системи в десяткову та отримуємо 192.168.10.0 адреса мережі в десятковій формі з маскою 255.255.255.0. Одиниці в масці вказують на частину мережевої адреси (1100000000.10101000.00001010), а нулі на частину адреси хоста (00001010).

➢ **Приклад 2**

Визначте мережеву адресу, якщо IP-адреса хоста 172.30.239.145, а маска підмережі 255.255.192.0.

Розв'язання:

- переводимо IP-адресу з десяткової системи числення в двійкову: *172.30.239.145 = 10110100.00100010.11101111.111011111* ;

- перетворюємо маску мережі з десяткової системи числення на двійкову: *255.255.192.0 = 11111111.11111111.11000000.00000000* ;
- складаємо IP-адресу з маскою за допомогою логічної операції «І». *10110100.00100010.11101111.11101111 (IP-адреса)*
  І
  11111111.11111111.11000000.00000000 (маска)
  =
  10110100.00100010.11000000.000000000 (мережева адреса)
- переводимо адресу мережі з двійкової системи числення в десяткову і отримуємо *172.30.192.0* адресу мережі в десятковій формі з маскою *255.255.192.0* ;
- проаналізувавши ці два приклади, можна побачити, що якщо маска підмережі має в октеті десяткове значення 255, результатом завжди буде вихідне значення цього октету. Якщо маска підмережі має в октеті десяткове значення 0, результат для цього октету завжди буде 0.

➢ **Приклад 3**

Визначте максимальну кількість вузлів у мережі за допомогою маски *255.255.192.0.*

Розв'язання:

Оскільки маска підмережі становить *255.255.192.0,* префікс буде */18* (тобто 18 біт для мережевої адреси). IPv4-адреса містить 32 біти. Отже, для вузлової частини залишається *32 – 18 = 14 біт.* Виходячи з цього, максимальна кількість вузлів у даній мережі

$2^{14} - 2 = 16384 - 2 = 16382$ *вузли.*

➢ **Приклад 4**

Визначте яку кількість підмереж із маскою *255.255.240.0* можна створити в мережі з маскою *255.255.0.0.*

Розв'язання:

Маска мережі 255.255.0.0 або /16

Маска підмережі 255.255.240.0 або /20

Кількість бітів у маски мережі – 16, а маски підмережі – 20. Різниця складає 4 біти. Таким чином, можна створити $2^4 = 16$ підмереж.

Завдання для самостійної роботи

1. Відповідно до варіанту (табл. 3.1.) за вказаною адресою IPv4 та маскою підмережі визначте такі параметри:
   - адреси мереж А і Б;
   - широкомовні адреси мереж А і Б;
   - максимальну кількість вузлів у мережах А та Б;
   - діапазон доступних адрес вузлів в мережах А і Б.

- кількість можливих підмереж Б в мережі А.

Таблиця 3.1. Параметри завдання

Номер варіанту	IP-адреса	Маска мережі А	Маска мережі Б
1	128.107.0.55	255.255.0.0	255.255.255.0
2	192.135.250.180	255.255.255.0	255.255.255.248
3	10.101.99.228	255.0.0.0	255.255.128.0
4	91.19.35.13	255.255.224.0	255.255.255.224
5	190.15.157.6	255.0.0.0	255.255.192.0
6	65.16.16.182	255.255.0.0	255.255.224.0
7	81.16.190.64	255.255.128.0	255.255.255.0
8	125.18.19.16	255.255.240.0	255.255.255.0
9	196.168.26	255.255.248.0	255.255.255.248
10	156.56.3.64	255.192.0.0	255.255.0.0

2. Заповніть таблицю 3.2.

Таблиця 3.2. Результати розрахунків

Параметри	Мережа А	Мережа Б
Маска мережі		
Мережева адреса		
Адреса трансляції мережі		
IPv4-адреса першого вузла в мережі		
IPv4-адреса останнього вузла в мережі		

Кількість вузлів в мережі		
Кількість можливих підмереж B у мережі A		

3. Створіть в середовищі Packet Tracer мережу A що складається з трьох стаціонарних ПК, ноутбуку та одного комутатора Switch 2960 25TT (див. рис. 3.1).

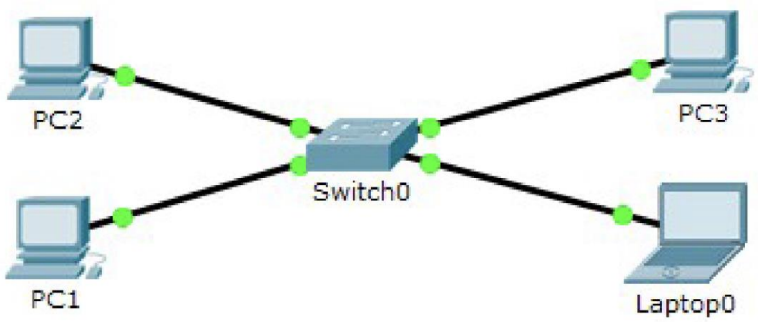


Рис. 3.1. Топологія мережі

4. Всім кінцевим вузлам мережі A задайте IP-адреси:
   - PC1 – третя адреса мережі A;
   - PC2 – четверта адреса мережі A;
   - PC3 – п’ята адреса мережі A;
   - leptop1 – остання адреса мережі A.
5. Встановіть відповідні мережеві маски для всіх кінцевих вузлів.
6. Перевірте параметри кожного кінцевого вузла за допомогою команди *ipconfig.*
7. Перевірте роботоздатність мережі за допомогою команди *ping.*

Питання для обговорення на занятті

1. Чому у сучасних мережах необхідно використовувати підмережі, замість того щоб залишати одну велику мережу?
2. Як впливає довжина маски підмережі на кількість доступних хостів?
3. Чому важливо вміти працювати з бінарним представленням IPv4-адреси?
4. У яких ситуаціях доцільно використовувати VLSM (маску змінної довжини)?
5. Як неправильний вибір маски підмережі може вплинути на роботу мережі?
6. Чим відрізняється мережа від широкомовної адреси та як їх визначити?

7. Чому необхідно враховувати адресу першого та останнього хоста?

8. Яким чином сабнетинг сприяє підвищенню безпеки та оптимізації трафіку?

9. Як різні топології мережі можуть впливати на вибір кількості підмереж?

10. Які типові помилки студенти допускають під час обчислення підмереж і як їх уникнути?

Тестові запитання

1. Яку кількість хостів можна розмістити в мережі /26?

A. 30

B. 62

C. 14

D. 126

2. Яка маска відповідає префіксу /24?

A. 255.255.0.0

B. 255.255.255.0

C. 255.255.255.128

D. 255.255.224.0

3. Який діапазон хостів можливий у підмережі 192.168.10.0/25?

A. 192.168.10.0 – 192.168.10.63

B. 192.168.10.1 – 192.168.10.126

C. 192.168.10.1 – 192.168.10.62

D. 192.168.10.128 – 192.168.10.254

4. Яка кількість підмереж утвориться при поділі мережі /24 на підмережі /26?

A. 2

B. 4

C. 8

D. 16

5. Яка адреса є широкомовною (broadcast) для підмережі 10.0.4.0/22?

A. 10.0.4.255

B. 10.0.7.255

C. 10.0.5.255

D. 10.0.4.1

6. Який префікс відповідає масці 255.255.255.240?
A. /26
B. /27
C. /28
D. /29

7. Яка мережа є наступною після 172.16.0.0/20?
A. 172.16.20.0/20
B. 172.16.16.0/20
C. 172.16.10.0/20
D. 172.16.32.0/20

8. Адреса 192.168.1.255 у мережі /24 — це:
A. Перша адреса хоста
B. Мережева адреса
C. Broadcast
D. Адреса шлюзу

9. Скільки хостів можна розмістити у мережі /30?
A. 4
B. 2
C. 6
D. 1

10. Яка мережа містить IP-адресу 192.168.15.78 при масці /20?
A. 192.168.0.0/20
B. 192.168.16.0/20
C. 192.168.15.0/20
D. 192.168.8.0/20

ПРАКТИЧНА РОБОТА №4
Розділення мережі на підмережі однакової довжини

Мета роботи: сформувати уміння виконувати поділ IPv4-мережі на підмережі однакової довжини, використовуючи механізм фіксованої маски підмережі. Навчитися визначати кількість необхідних підмереж, обчислювати нову маску, будувати логічну структуру мережі.

Матеріали та ресурси: ПК, таблиці CIDR-нотацій, онлайн-калькулятор підмереж, а також мережевий симулятори (Cisco Packet Tracer).

Завдання для роботи під час заняття

1. **Поділ мережі на підмережі**

➢ **Приклад 1**

Нехай задана мережа *74.126.205.0* з маскою мережі *255.255.255.0*. Потрібно створити 4 підмережі.

Розв'язання:

Обраховуємо кількість бітів у основній масці, необхідних для створення підмереж. Оскільки потрібно створити 4 підмережі, тобто 2^2, то це означає, що буде запозичено 2 біти в основної маски мережі:

74.126.205.0 - 01001010.01111110.11001101.00000000

*255.255.255.192 - 11111111.11111111.11111111.**11000000***

Розширення маски до значення 255.255.255.192 відбулося за рахунок двох бітів вихідної частини вузла в адресі, які були використані для створення підмереж. Ідентифікатор вузла тепер містить шість бітів, що залишилися, тому кожна підмережа може містити 64 (2^6) адрес вузлів, 62 з яких фактично можуть бути віднесені до пристроїв, оскільки ідентифікатори вузлів не можуть складатися лише з одиниць або нулів. З урахуванням всіх перерахованих вище факторів створені підмережі представлені в таблиці. 4.1.

Таблиця 4.1. Представлення мережі в десяткових та двійкових системах числення

Підмережа (10)	Підмережа (2)
74.126.205.0	01001010.01111110.11001101. **00**000000
74.126.205.64	01001010.01111110.11001101. **01**000000
74.126.205.192	01001010.01111110.11001101. **11**000000

74.126.205.128	01001010.01111110.11001101. **10**000000
Маска підмережі (10)	**Маска підмережі (2)**
255.255.255.192	11111111.11111111.11111111.11000000

Технологія розподілу на підмережі в цьому прикладі дозволяє створити чотири підмережі. Кожна підмережа може підтримувати до 62 адрес вузлів. З цього можна зробити висновок, що чим більше бітів використовується для маски підмережі, тим більше підмереж доступно. Однак чим більше доступно підмереж, тим менше хост-адрес, доступних у кожній підмережі.

Перевірте працездатність цієї мережі. Для цього:

1. Створіть в середовищі Packet Tracer топологію, що містить один роутер Generic Router-PT-Empty (Router1), чотири комутатори Switch 2960-24TT (Switch0 – Switch3) и 8 ПК (PC0 – PC7).
2. Додайте до маршрутизатора чотири Gigabit Ethernet-модулі PT-ROUTER NM-1CGE в роутер. Для цього відкрийте властивості Router1, на вкладці Physical на моделі роутера натисніть кнопку живлення для вимкнення, виберіть вказаний модуль підключення, встановіть чотири таких модулі у вільні слоти та включіть роутер.
3. Комп'ютери з комутаторами об’єднайте крученою парою. Порти підключення – FastEthernet. Комутатори з роутером також об’єднайте крученою парою. Порти з'єднання – GigabitEthernet. Топологія моделі мережі представлена на рис. 4.1.
4. Збережіть створену топологію.

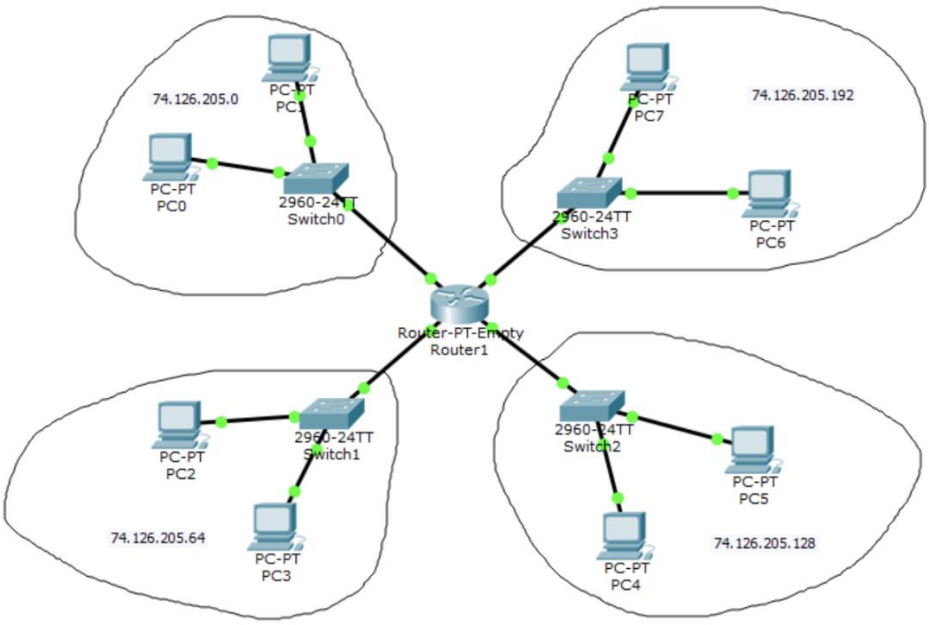


Рис. 4.1. Топологія мережі

5. Налаштуйте елементи мережі. У кожній підмережі зарезервуйте для маршрутизатора першу доступну IP-адресу, а комп’ютерам присвойте другу та наступні адреси. Маска мережі для всіх пристроїв – *255.255.255.192*.

6. Щоб налаштувати PC0, який належить до першої підмережі, відкрийте його властивості. На вкладці *Desktop* виберіть пункт *IP Config* і для режиму отримання IP-адрес *Static* у полі *IP Address* введіть другу доступну адресу підмережі – *74.126.205.2*, в поле *Subnet Mask* – маску мережі *255.255.255.192*, а в полі *Default Gateway* (шлюз за замовчуванням) вкажіть першу доступну IP адресу підмережі, зарезервовану для роутера – *74.126.205.1*. Комутатор PC1 налаштовується аналогічно, але в *IP Address* введіть останню доступну адресу підмережі – *74.126.205.62*.

7. Задайте IP-адресу для другої підмережі: комп’ютер PC2 – *74.126.205.66*, комп’ютер PC3 – *74.126.205.126*, шлюз – *74.126.205.65*; для третьої підмережі: комп'ютер PC4 – *74.126.205.130*, комп'ютер PC5 – *74.126.205.190*, шлюз – *74.126.205.129*; комп'ютер PC6 – *74.126.205.194*, комп’ютер PC7 – *74.126.205.254*, шлюз – *74.126.205.193*.

8. Виконайте настройку роутера, яка буде заключатись в окремому мережевому налаштуванні кожного з Gigabit Ethernet-модулів, до яких підключені комутатори підмереж. Відкрийте властивості маршрутизатора та перейдіть до вкладки *Config* та в підменю *INTERFACE* виберіть модуль GigabitEthernet0/0, до якого підключено перший комутатор підмережі *74.126.205.0*. У поле *IP Address* введіть першу зарезервовану IP-адресу підмережі – *74.126.205.1*, а в поле *Subnet Mask* – маску мережі *255.255.255.192*. Потім увімкніть даний модуль – для *Port Status* встановіть значення On. Інші

три модулі налаштуйте аналогічно – в полі *IP Address* вкажіть першу зарезервовану IP-адресу підмережі, комутатор якої підключений до модуля.

9. Перевірте роботоздатність мережі. Наприклад, зайдіть на комп'ютер PC0 і пропінгуйте комп'ютер PC7. Для цього відкрийте властивості комп'ютера PC0, на вкладці *Desktop* виберіть *Command Promt* і у вікні, що відкриється в командному рядку введіть команду ping та IP-адресу комп'ютера PC7. Нижче наведено результати команди *ping:*

```
PC>ping 74.126.205.254
Pinging 74.126.205.254 with 32 bytes of data:
Reply from 74.126.205.254: bytes=32 time=0ms TTL=127
Reply from 74.126.205.254: bytes=32 time=0ms TTL=127
Reply from 74.126.205.254: bytes=32 time=0ms TTL=127
Reply from 74.126.205.254: bytes=32 time=0ms TTL=127
Ping statistics for 74.126.205.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Це підтверджує правильність мережевих налаштувань пристроїв та загальну роботоздатність мережі.

Завдання для самостійної роботи

1. Відповідно до варіанту (табл. 4.2) за вказаною IP-адресою та маскою розділіть задану мережу на чотири рівні підмережі.

Таблиця 4.2. Параметри завдання

Номер варіанта	**Адреса мережі**	**Маска мережі**
1	129.138.60.0	255.255.252.0
2	191.197.206.0	255.255.254.0
3	17.53.208.0	255.255.248.0
4	144.29.236.0	255.255.252.0
5	48.185.104.0	255.255.248.0
6	109.88.38.0	255.255.254.0

7	13.140.208.0	255.255.240.0
8	78.97.205.0	255.255.255.0
9	192.199.140.0	255.255.252.0
10	87.247.176.0	255.255.240.0

2. Виконайте розрахунки та заповніть таблицю 4.3.

Таблиця 4.3. Результати розрахунків

Ім'я підмережі	**А**	**Б**	**В**	**Г**
Мережева адреса підмережі				
Маска підмережі				
Префікс маски підмережі				
Широкомовна адреса підмережі				
Доступний діапазон адрес вузлів в підмережі				
Кількість вузлів у підмережі				

3. В середовищі Packet Tracer створіть топологію, аналогічну тій, що описана в прикладі (рис. 3.2).

4. Всім кінцевим вузлам задайте IP-адреси та маски із описаних раніше підмереж (А, Б, В, Г):

- всім інтерфейсам маршрутизатора задайте перші допустимі IП-адреси підмережі;
- першим вузлам в підмережі задайте другі допустимі IP-адреси;
- другим вузлам задайте останні допустимі IP-адреси.

5. Перевірте параметри кожного цільового вузла за допомогою

команди ipconfig.

6. Перевірте стан здоров'я мережі за допомогою команди ping.

Питання для обговорення на занятті

1. Навіщо виконувати розділення мережі на підмережі однакової довжини? Які переваги це дає?
2. Як визначити, скільки біт необхідно позичити для створення певної кількості підмереж?
3. Чому в підмережах однакового розміру важливий принцип кратності?
4. Як зміна маски підмережі впливає на кількість доступних хостів?
5. Яким чином визначається приріст (step) між підмережами і чому він важливий?
6. Чому під час сабнетингу важливо знати бінарну форму маски та мережевої адреси?
7. У яких ситуаціях фіксований сабнетинг кращий за VLSM (Variable-Length Subnet Mask)?
8. Які наслідки може мати неправильне визначення broadcast-адреси?
9. Як підмережування однакової довжини впливає на логіку маршрутизації?
10. Які типові помилки виникають при розрахунку підмереж з фіксованою довжиною і як їх уникнути?

Тестові запитання

1. Який префікс утвориться при поділі мережі /24 на 4 однакові підмережі?

A. /25;
B. /26;
C. /27;
D. /28.

2. Скільки підмереж можна отримати при позиченні 3 біт із хостової частини?

A. 4;
B. 6;
C. 8;
D. 16.

3. Який буде приріст (step) для мережі /26?

A. 32;
B. 256;

C. 64;
D. 16.

4. Яка з наведених адрес є broadcast-адресою для мережі 192.168.10.0/26?
A. 192.168.10.63;
B. 192.168.10.64;
C. 192.168.10.62;
D. 192.168.10.1.

5. Кількість доступних хостів у мережі /27 становить:
A. 62;
B. 30;
C. 14;
D. 6.

6. Яка маска відповідає префіксу /28?
A. 255.255.255.224;
B. 255.255.255.240;
C. 255.255.255.192;
D. 255.255.255.248.

7. Яка буде другою підмережею для базової мережі 10.0.0.0/26?
A. 10.0.0.32;
B. 10.0.0.64;
C. 10.0.0.128;
D. 10.0.0.16.

8. Яка мережева адреса належить до підмережі /25?
A. 192.168.1.128;
B. 192.168.1.200;
C. 192.168.1.63;
D. 192.168.1.255.

9. Яка формула використовується для визначення кількості хостів у підмережі?
A. $2^n - 1$;
B. $2^n - 2$;
C. 2^n;
D. $2^n \times 2$.

10. Яка характеристика обов’язково однакова при сабнетингу фіксованої довжини?

A. Кількість хостів у підмережах;

B. Величини VLAN;

C. Розташування хостів у топології;

D. Типи маршрутизаторів.

ПРАКТИЧНА РОБОТА №5
Розділення мережі на підмережі змінної довжини

Мета роботи: сформувати уміння виконувати поділ IPv4-мережі на підмережі змінної довжини, використовуючи технологію VLSM. Навчитися аналізувати вимоги до кількості хостів у різних мережевих сегментах, визначати відповідні маски підмереж, виконувати розрахунок префіксів, діапазонів адрес, мережевих і широкомовних адрес, а також складати ієрархічну структуру підмереж із мінімальними втратами адрес.

Матеріали та ресурси: ПК, доступ до онлайн-калькулятору підмереж, таблиці CIDR-нотацій, симулятор мережі (Cisco Packet Tracer).

Завдання для роботи під час заняття

1. Поділ мережі на підмережі

Нехай задана мережа 74.126.205.0 з мережевою маскою 255.255.255.0. Розробіть схему поділу цієї мережі на 4 підмережі за допомогою VLSM: підмережа А повинна містити 14 вузлів, підмережа Б – 28 вузлів, підмережа В – 15 вузлів, підмережа Г – 5 вузлів.

1. Визначіть, яку маску підмережі варто використати щоб отримати потрібну кількість вузлів.

Мережа А: має вмістити 14 вузлів. Найбільше підходить значення $2^n = 16$, це означає що кількість бітів вузлової частини $n=4$, кількість бітів для ідентифікатора підмережі становитимуть $8 – 4 = 4$ біти. Отже, маска цієї підмережі буде *255.255.255.240* або */28.*

Мережа Б: повинна вмістити 28 вузлів. Найбільше підходить значення $2^n = 32$, значить кількість бітів вузлової частини $n = 5$, а кількість бітів для ідентифікатора підмережі становитимуть $8 – 5 = 3$ *біти*. Отже, маска цієї підмережі буде *255.255.255.224* або */27.*

Мережа В: повинна мати 15 вузлів. Найбільше підходить значення $2^n = 16$, але тому, що кожна мережа повинна мати широкомовний адрес та адресу підмережі, то 16 для цієї підмережі буде недостатньо. Тому вибираємо $2^n = 32$. Кількість бітів частини вузла n = 5, а кількість бітів для ідентифікатора підмережі становитиме 8 – 5 = 3 біти. Таким чином, маска цієї підмережі буде 255.255.255.224 або /27.

Мережа Г: має містити 5 вузлів. Найбільше підходить значення $2^n = 8$, значить кількість бітів частини вузла n = 3, а кількість бітів для ідентифікатора підмережі становитиме 8 – 3 = 5 біт. Тому маска цієї підмережі буде 255.255.255.248 або /29.

VLSM-розбиття на підмережі схоже на традиційне в тому, що в ньому, для створення підмережі, запозичаються біти. Формули обчислення кількості

можливих підмереж та кількості вузлів в кожній підмережі також можуть застосовуватись. Різниця лише в тому, що розбиття на підмережі виконується в декілька етапів. При використанні VLSM мережа спочатку розбивається на підмережі, які, в свою чергу, знову діляться на підмережі. Цей процес може повторитися багато разів для створення підмереж різних розмірів. Для початку відсортуємо підмережі, які потрібно створити, за кількістю доступних вузлів:

- мережа Б: 32 вузли;
- мережа В: 32 вузли;
- мережа А: 16 вузлів;
- мережа Г: 8 вузлів.

2. Далі розібийте задану мережу (в якій доступно 256 адрес) по 32 адреси (найбільша підмережа, яку ви шукаєте). У отриманих підмережах кількість бітів ідентифікатора підмережі – 3, тому нові підмережі будуть виглядати так:

*01001010.01111110.11001101.**000**00000*
*01001010.01111110.11001101.**001**00000*
*01001010.01111110.11001101.**010**00000*
*01001010.01111110.11001101.**011**00000*
*01001010.01111110.11001101.**100**00000*
*01001010.01111110.11001101.**101**00000*
*01001010.01111110.11001101.**110**00000*
*01001010.01111110.11001101.**111**00000*

Нам потрібні тільки перші дві підмережі (для Б і В). Маска у цих підмереж буде *255.255.255.224* або */27*.

Щоб визначити наступні підмережі, розділіть мережу 01001010.01111110.11001101.**010**00000 навпіл (тобто запозичимо ще один біт для ідентифікатора підмережі).

Ми отримуємо дві мережі:

*01001010.01111110.11001101.**0100**0000*
*01001010.01111110.11001101.**0101**0000*

Перша з цих підмереж призначена для мережі А маскою /28. Другу – ще раз ділимо навпіл, тобто запозичимо ще один біт у ідентифікатора підмережі. Отримаємо ще дві мережі:

*01001010.01111110.11001101.**01010**000*
*01001010.01111110.11001101.**01011**000*

Перший з них відповідає мережі Г з маскою /29.

Результат переведення значень знайдених підмереж в десяткову форму представлений в таблиці. 5.1.

Таблиця 5.1. Параметри підмережі

Ім'я	Підмережа (2)	Підмережа (10)	Маска (10)
Б	01001010.01111110.11001101. **000**00000	74.126.205.0	255.255.255.224
В	01001010.01111110.11001101. **001**00000	74.126.205.32	255.255.255.224
А	01001010.01111110.11001101. **0100**0000	74.126.205.6	255.255.255.240
Г	01001010.01111110.11001101. **01010**000	74.126.205.80	255.255.255.248

3. Для визначення діапазону доступних у підмережі вузлів необхідно спочатку додати номера підмережі додати одиницю (це буде адреса першого вузла), а потім до номера підмережі додати кількість доступних адрес (це буде адреса останнього вузла). Результати представлені в таблиці. 5.2.

Таблиця 5.2. Діапазон доступних вузлів

Ім'я	Підмережа	Маска	Діапазон доступних адрес
Б	74.126.205.0	255.255.255.224	74.126.205.1 - 74.126.205.30
В	126.205.32	255.255.255.224	74.126.205.33 - 74.126.205.62
А	74.126.205.64	255.255.255.240	74.126.205.65 - 74.126.205.78
Г	74.126.205.80	255.255.255.248	126.205.81 - 74.126.205.86

Метод VLSM розподілу на підмережі в цьому прикладі дозволяє створити чотири підмережі з заданою кількістю вузлів у кожній. Створення мережі з чотирьох підмереж і настроювання мережевих компонент в Packet Tracer описаний в попередній роботі.

Завдання для самостійної роботи

1. Відповідно до варіанту (табл. 5.3) за вказаною IP-адресою та маскою підмережі розділіть задану мережу на чотири підмережі враховуючи

кількість вузлів в кожній з допомогою методу VLSM.

Таблиця 5.3.

			Кількість вузлів в підмережі			
Номер варіанту	**Адреса мережі**	**Маска мережі**	**А**	**Б**	**В**	**Г**
1	126.198.0.0	255.254.0.0	155	255	86	161
2	192.200.0.0	255.248.0.0	72	104	130	109
3	10.192.0.0	255.252.0.0	73	55	133	106
4	156.168.0.0	255.248.0.0	92	180	105	102
5	81.176.0.0	255.248.0.0	89	158	171	60
6	91.184.0.0	255.252.0.0	80	100	64	150
7	190.128.0.0	255.254.0.0	09	65	155	62
8	65.48.0.0	255.248.0.0	120	132	90	146
9	125.192.0.0	255.240.0.0	64	95	59	181
10	14.160.0.0	255.224.0.0	50	258	140	107

2. Виконайте розрахунки та заповніть таблицю 5.4.

Таблиця 5.4. Результати розрахунку

Ім'я підмережі				
Мережева адреса підмережі				
Маска підмережі				
Префікс маски підмережі				

Широкомовна адреса підмережі				
Діапазон доступних адрес вузлів в підмережі				
Кількість вузлів у підмережі				

3. Створіть топологію мережі в середовищі Packet Tracer.
4. Для всіх кінцевих вузлів задайте IP-адреси та маски із обчислених раніше підмереж (A, B, C, D):
    - для всіх інтерфейсів маршрутизатора задайте перші допустимі IP-адреси підмережі;
    - першим вузлам в підмережі присвойте другі допустимі IP-адреси;
    - другим вузлам присвойте останні допустимі IP-адреси.
5. Перевірте параметри кожного вузла за допомогою команди ipconfig.
6. Перевірте роботоздатність мережі за допомогою команди ping.

Питання для обговорення на занятті

1. У чому полягає принципова різниця між фіксованим сабнетингом (FLSM) та VLSM?
2. Чому VLSM дозволяє ефективніше використовувати IPv4-адресний простір?
3. Як визначити, яку маску підмережі потрібно застосувати для сегмента з конкретною кількістю хостів?
4. Чому під час VLSM важливо починати розрахунки з найбільшої підмережі?
5. Які ризики можуть виникнути, якщо підмережі при VLSM перекриваються?
6. Як VLSM впливає на маршрутизацію і чому вона стає більш гнучкою?
7. У яких типових сценаріях мережевого планування застосування VLSM є обов’язковим?
8. Чому важливо вести структурований запис підмереж під час використання VLSM?

9. Як за допомогою VLSM можна мінімізувати втрати IP-адрес у великих корпоративних мережах?

10. Які типові помилки допускають студенти при роботі з VLSM і як їх уникнути?

Тестові запитання

1. Що означає абревіатура VLSM?

A. Very Large Subnet Map;

B. Variable Length Subnet Mask;

C. Virtual Logical Subnet Method;

D. Variable Local Segment Mapping.

2. Який принцип є ключовим у VLSM?

A. Усі підмережі повинні бути однакового розміру;

B. Кожна підмережа отримує випадкову маску;

C. Підмережам призначаються різні маски залежно від потреб у хостах;

D. Маска підмережі змінюється автоматично.

3. Яку маску потрібно використати для сегмента, що вимагає 30 хостів?

A. /25;

B. /26;

C. /27;

D. /28.

4. Скільки хостів допускає підмережа /29?

A. 6;

B. 14;

C. 30;

D. 2.

5. Яка підмережа буде першою, якщо базова мережа 10.0.0.0/24, а перший сегмент потребує /26?

A. 10.0.0.0/26;

B. 10.0.0.64/26;

C. 10.0.0.128/26;

D. 10.0.0.192/26.

6. Який префікс забезпечує приблизно 14 хостів?

A. /26;

B. /27;

C. /28;

D. /29.

7. Яка проблема виникає, якщо діапазони підмереж VLSM перекриваються?

A. Зменшується ширина каналу;

B. Виникає конфлікт маршрутизації;

C. Підвищується швидкість роботи мережі;

D. Підмережі автоматично об’єднуються.

8. Яку підмережу отримаємо наступною після 192.168.1.0/26?

A. 192.168.1.64/26;

B. 192.168.1.32/26;

C. 192.168.1.128/26;

D. 192.168.1.96/26.

9. Яка формула використовується для підрахунку хостів у підмережі?

A. $2^n – 1$;

B. $2^n – 2$;

C. 2^n;

D. n^2.

10. Чому під час VLSM потрібно починати з найбільшої підмережі?

A. Щоб зменшити час розрахунків;

B. Щоб уникнути перевищення глибини маски;

C. Щоб великі сегменти не були розбиті на дрібні блоки через нестачу місця;

D. Щоб зробити схему більш симетричною.

ПРАКТИЧНА РОБОТА №6
Об’єднання підмереж

Мета роботи: сформувати уміння виконувати об’єднання кількох підмереж у більшу узагальнену мережу шляхом застосування принципів супернетингу та агрегування маршрутів. Навчитися аналізувати діапазони IPv4-адрес, визначати спільні бітові префікси, знаходити найменший можливий агрегований блок адрес.

Матеріали та ресурси: ПК, калькулятор підмереж, таблиці бінарних значень, симулятор мережі (Cisco Packet Tracer) для демонстрації застосування агрегованих маршрутів.

Завдання для роботи під час заняття

1. Об’єднання підмереж

Нехай задані мережа «А» 192.168.1.0 з маскою мережі 255.255.255.0 і мережа «Б» 172.16.0.0 з мережевою маскою 255.255.0.0. Їх потрібно об'єднати.

1. Створіть в середовищі Packet Tracer топологію, що містить один маршрутизатор Generic Router-PT-Empty (Router0), один комутатор Generic Switch-PTEmpty (Switch0), одну бездротову точку доступу Generic Access-Point PT (Access Point0), 2 ПК (PC0 – PC1) и 2 планшети (Tablet PC0 и Tablet PC1).

2. Додайте один оптичний Gigabit Ethernet-модуль PT-ROUTER-NM-1FGE до маршрутизатора для підключення мережі А та один Gigabit Ethernet-модуль PTROUTER-NM-1CGE в роутер для підключення мережі В. Для цього відкрийте властивості Router0, на вкладці *Physical* на моделі роутера натисніть кнопку живлення, щоб його вимкнути, виберіть зазначені модулі з'єднання, встановіть їх у вільні слоти і включіть роутер.

3. Додайте один Gigabit Ethernet-модуль PT-SWITCH-NM-1FGE в комутатор. Відкрийте властивості Switch0 на вкладці *Physical* на моделі комутатора натисніть кнопку живлення, щоб вимкнути її, виберіть вказаний модуль з'єднання, встановіть його у слот. Щоб підключити комп'ютери, виберіть і встановіть у вільні слоти два модулі PT-SWITCH-NM-1CFE і включіть комутатор.

4. Комп'ютери з комутатором з’єднайте витою парою – порти підключення FastEthernet. Роутер з комутатором з’єднаємо оптичним кабелем – порти підключення GigabitEthernet. Планшети з’єднайте з точкою доступу по відкритому бездротовому з’єднанню. Точку доступу з роутером з’єднайте витою парою – порти, відповідно, Port0 та GigabitEthernet. Топологія мережевої моделі показана на рис. 6.1.

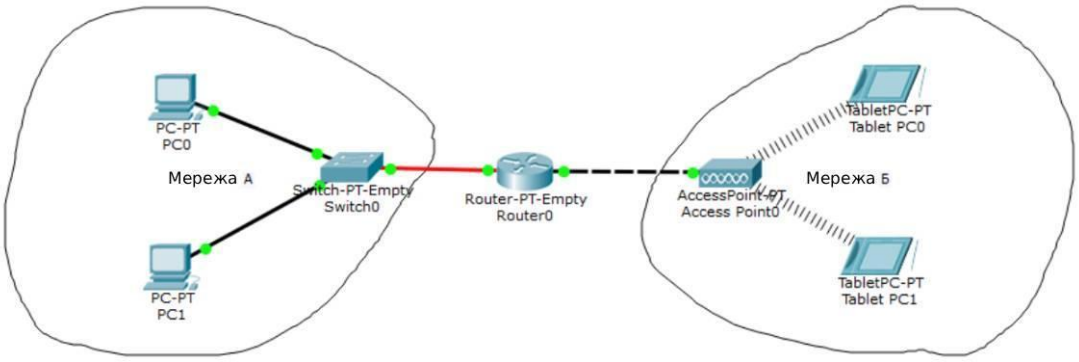


Рис. 6.1 Приклад мережевого зв'язування

5. Налаштуйте елементи мережі. У кожній мережі зарезервуйте для роутера першу доступну IP-адресу, а вузлам терміналів задайте другу та наступну доступні адреси.

6. Щоб налаштувати комп'ютер PC0, який належить до мережі А, відкрийте його властивості. На вкладці *Desktop* виберіть пункт *IP Config* і для режиму отримання IP-адреси *Static*, в поле *IP Address* введіть другу доступну адресу підмережі – 192.168.1.2, в полі *Subnet Mask* – маску мережі 255.255.255.0, а *Default Gateway* – першу доступну IP-адресу підмережі, зарезервовану для роутера: 192.168.1.254. Компютер PC1 налаштовується аналогічно, але в поле *IP Address* введіть останню доступну адресу підмережі – 192.168.1.254.

7. Задайте IP-адреси для пристроїв мережі В: планшетний ПК0 – 172.16.0.2 маска 255.255.0.0, шлюз – 172.16.0.1; - планшет PC1 – 172.16.255.254 маска 255.255.0.0, шлюз – 172.16.0.1.

8. Виконайте налаштування роутера, що буде заключатися в окремому мережному налаштуванні кожного з модулів, до яких підключені комутатор та точка доступу. Відкрийте властивості роутера, перейдіть на вкладку *Config* і в підменю *INTERFACE* та оберіть модуль GigabitEthernet0/0, до якого підключено комутатор першої мережі А 192.168.1.0. У полі IP Address введіть першу зарезервовану IP-адресу підмережі – 192.168.1.1, а в поле *Subnet Mask* – маску мережі 255.255.255.0. Після цього ввімкніть цей модуль – *Port Status* встановіть на *On*. Другий модуль налаштуйте аналогічно – в поле *IP Address* внесіть першу зарезервовану IP-адресу мережі В, тобто 172.16.0.1, а в полі *Subnet Mask* – 255.255.0.0.

9. Перевірте роботоздатність мережі. Наприклад, зайдіть на комп'ютер PC0 та пропінгуйте планшетний PC1. Для цього відкрийте властивості PC0, на вкладці *Desktop* виберіть пункт *Command Promt* і в вікні, що відкриється в командному рядку, введіть команду *ping* та IP-адресу комп’ютера *Tablet PC1*. Нижче наведені результати виконання команди *ping:*

```
PC>ping 172.16.0.254
```

```
Pinging 172.16.0.254 with 32 bytes of data:
Reply from 172.16.0.254: bytes=32 time=1ms TTL=127
Reply from 172.16.0.254: bytes=32 time=18ms TTL=127
Reply from 172.16.0.254: bytes=32 time=20ms TTL=127
Reply from 172.16.0.254: bytes=32 time=11ms TTL=127
Ping statistics for 172.16.0.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 20ms, Average = 12ms
```

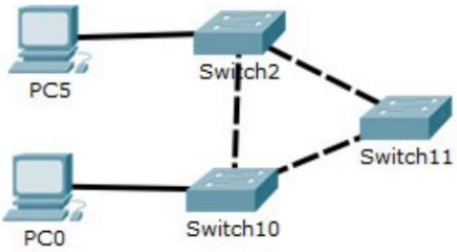
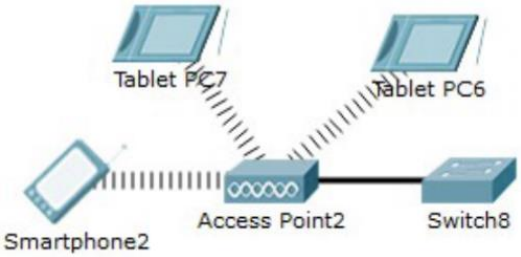
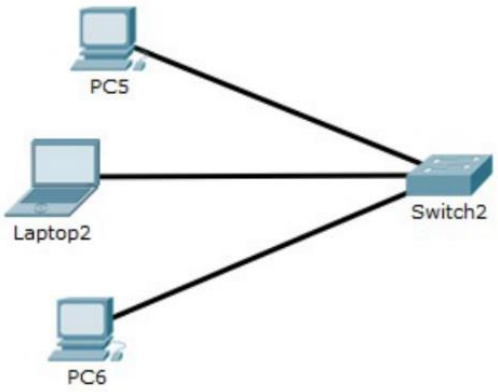
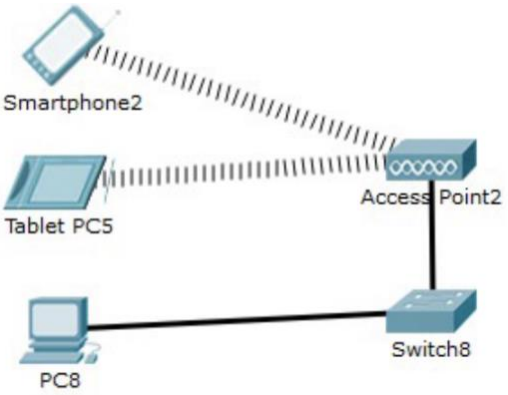
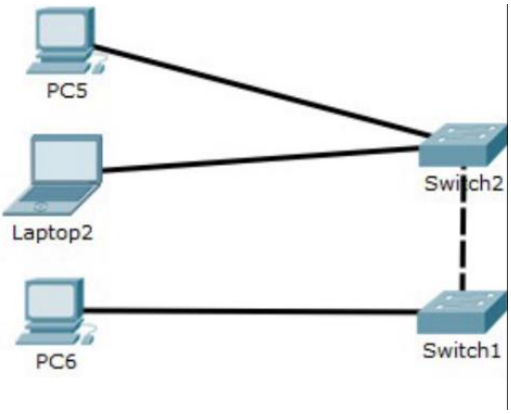
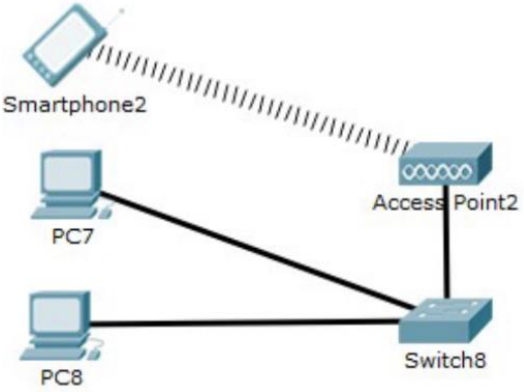
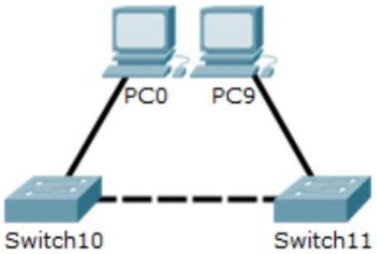
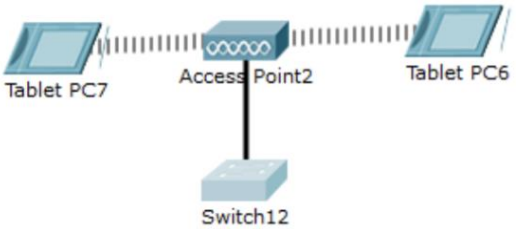
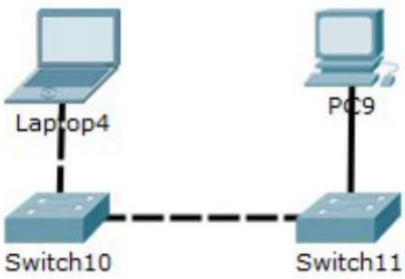
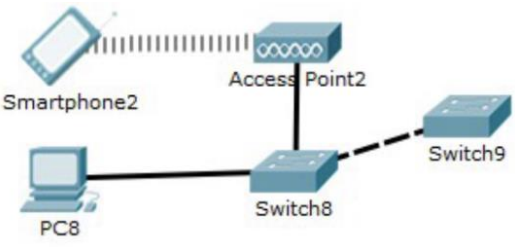
Це підтверджує правильність мережевих налаштувань пристроїв та загальну роботоздатність мережі.

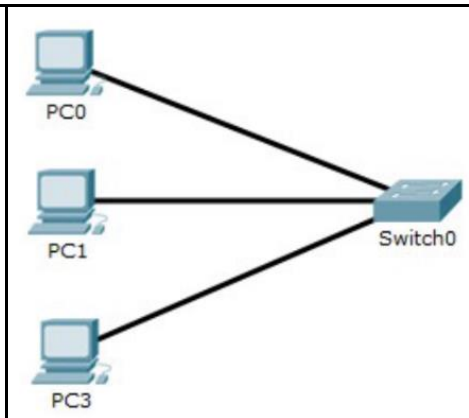
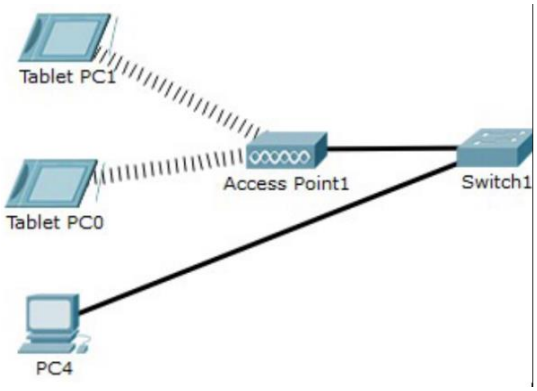
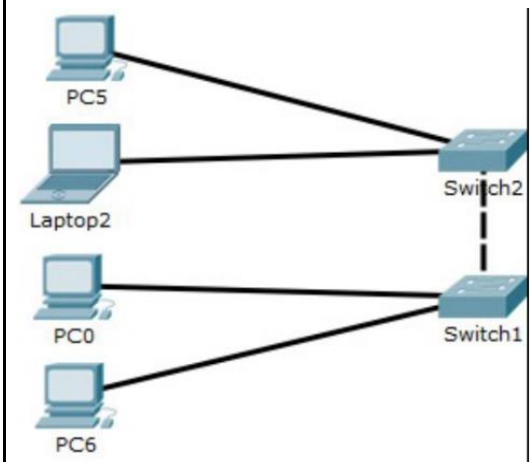
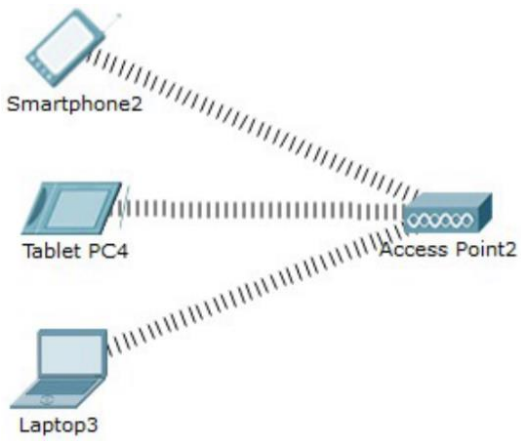
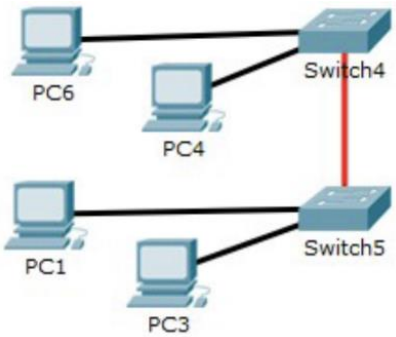
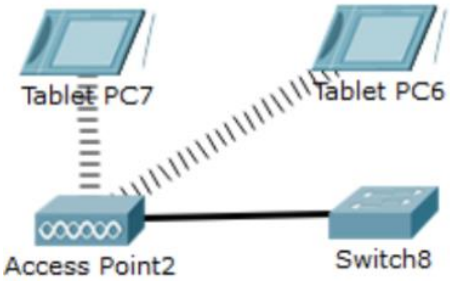
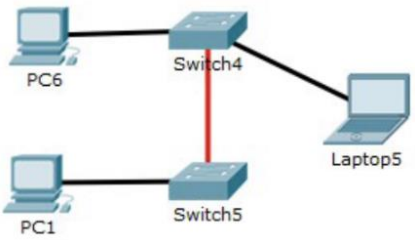
Завдання для самостійної роботи

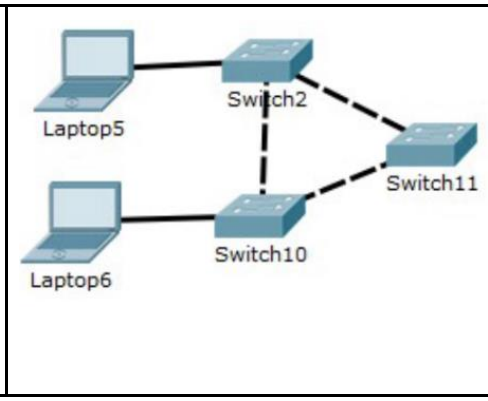
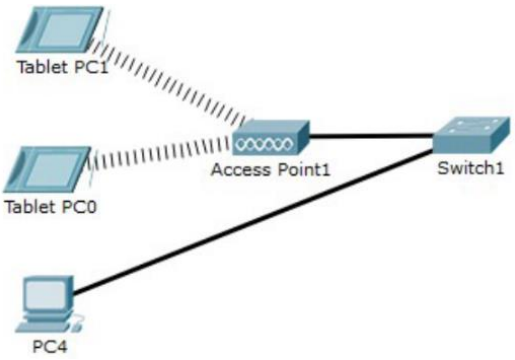
1. Відповідно до зазначеного варіанту (табл. 6.1) об'єднайте мережі «А» та «В». В якості пристрою об’єднання використайте роутер Generic Router-PT Empty. В якості комутатора – Generic Switch-PTEmpty, в якості точки доступу – Generic Access-Point-PT. Спосіб підключення мережі до роутера вказаний в таблиці. 6.2.
2. Додайте до маршрутизатора і комутатора необхідні модулі для об'єднання мереж.
3. Встановіть IP-адреси та маски для всіх вузлів відповідно до таблиці 6.3.
    - всім інтерфейсам маршрутизатора задайте останнє допустиме значення IP адреси мережі;
    - встановіть дійсні IP-адреси для всіх цільових вузлів у мережах, починаючи з першого.
4. Перевірте параметри кожного цільового вузла за допомогою команди *ipconfig*.
5. Перевірте роботоспроможність мережі за допомогою команди *ping*.

Таблиця 6.1. Варіанти завдань топології мережі

№ вар.	**Мережа А**	**Мережа Б**

1	 PC5 Switch2 Switch11 PC0 Switch10	 Tablet PC7 Tablet PC6 Smartphone2 Access Point2 Switch8
2	 PC5 Laptop2 Switch2 PC6	 Smartphone2 Access Point2 Tablet PC5 Switch8 PC8
3	 PC5 Switch2 Laptop2 PC6 Switch1	 Smartphone2 Access Point2 PC7 PC8 Switch8
4	 PC0 PC9 Switch10 Switch11	 Tablet PC7 Access Point2 Tablet PC6 Switch12
5	 Laptop4 PC9 Switch10 Switch11	 Smartphone2 Access Point2 Switch9 Switch8 PC8

6	 PC0 PC1 PC3 Switch0	 Tablet PC1 Access Point1 Switch1 Tablet PC0 PC4
7	 PC5 Switch2 Laptop2 PC0 Switch1 PC6	 Smartphone2 Tablet PC4 Access Point2 Laptop3
8	 PC6 Switch4 PC4 PC1 Switch5 PC3	 Tablet PC7 Tablet PC6 Access Point2 Switch8
9	 PC6 Switch4 Laptop5 PC1 Switch5	 Tablet PC7 Access Point2 Tablet PC6

10		

Таблиця 6.2. Параметри перемикання мережі

№ варіанту	**Мережа А**	**Мережа Б**
1	Switch10 витою парою	Switch8 оптичним кабелем
2	Switch2 оптичним кабелем	Switch8 витою парою
3	Switch2 витою парою	Switch8 оптичним кабелем
4	Switch10 оптичним кабелем	Switch12 витою парою
5	Switch11 витою парою	Switch9 оптичним кабелем
6	Switch0 оптичним кабелем	Switch1 витою парою
7	Switch1 витою парою	AccessPoint2 витою парою
8	Switch5 оптичним кабелем	Switch8 витою парою
9	Switch5 витою парою	AccessPoint2 витою парою
10	Switch11 оптичним кабелем	Switch1 витою парою

Таблиця 6.3. IP-адреси та маски для всіх вузлів

№ вар.	**Адреса мережі А**	**Маска мережі А**	**Адреса мережі Б**	**Маска мережі Б**

1	155.54.14.128	255.255.255.128	16.58.25.32	255.255.255.224
2	182.167.19.64	255.255.255.192	11.16.16.192	255.255.255.224
3	194.151.156.192	255.255.255.192	47.58.69.64	255.255.255.224
4	189.178.15.32	255.255.255.224	13.161.19.64	255.255.255.192
5	65.5.54.128	255.255.255.128	49.46.43.192	255.255.255.192
6	18.15.54.64	255.255.255.192	52.14.16.0	255.255.255.128
7	165.55.18.192	255.255.255.192	13.19.49.32	255.255.255.224
8	168.98.46.32	255.255.255.224	82.84.86.192	255.255.255.192
9	65.49.18.128	255.255.255.128	15.8.66.0	255.255.255.192
10	54.12.18.64	255.255.255.192	19.19.46.192	255.255.255.224

Питання для обговорення на занятті

1. У чому полягає основна ідея супернетингу і чим він відрізняється від звичайного підмережування?
2. Які умови повинні виконуватись, щоб кілька підмереж можна було об’єднати в одну супермережу?
3. Чому важливо аналізувати бінарні представлення адрес перед об’єднанням підмереж?
4. Як визначити найдовший спільний префікс для набору підмереж?
5. Чому важливо, щоб підмережі були суміжними та утворювали безперервний блок адрес?
6. Як супернетинг впливає на таблиці маршрутизації та продуктивність мережі?
7. У яких сценаріях провайдери активно використовують агрегування маршрутів?
8. Які ризики можуть виникнути при неправильному обчисленні супермережі?
9. Чому при супернетингу потрібно переконатися, що новий діапазон повністю покриває всі вихідні підмережі?

10. Які практичні переваги дає агрегування маршрутів для адміністраторів великих мереж?

Тестові запитання

1. Як називається процес об’єднання кількох суміжних підмереж в одну більшу?

A. Сабнетинг;

B. Супернетинг;

C. NAT;

D. VLAN.

2. Яка умова є обов’язковою для супернетингу?

A. Підмережі мають бути різних класів;

B. Підмережі повинні бути суміжними та кратними;

C. Підмережі повинні мати однакову кількість хостів;

D. Підмережі повинні мати однакові broadcast-адреси.

3. Який результат отримаємо при об’єднанні мереж 192.168.4.0/24 і 192.168.5.0/24?

A. 192.168.4.0/24;

B. 192.168.4.0/23;

C. 192.168.0.0/22;

D. Об’єднання неможливе.

4. Яка маска відповідає префіксу /22?

A. 255.255.255.0;

B. 255.255.254.0;

C. 255.255.252.0;

D. 255.255.240.0.

5. Який із варіантів НЕ можна об’єднати у супермережу?

A. 10.0.0.0/24 і 10.0.1.0/24;

B. 172.16.8.0/24 і 172.16.9.0/24;

C. 192.168.10.0/24 і 192.168.12.0/24;

D. 192.168.20.0/23 і 192.168.22.0/23.

6. Який спільний префікс мають мережі 172.16.0.0/23 і 172.16.2.0/23?

A. /24;

B. /22;

C. /21;

D. /20.

7. Що відбувається з кількістю маршрутів у таблиці маршрутизатора під час супернетингу?

A. Збільшується;

B. Не змінюється;

C. Зменшується;

D. Стає випадковою.

8. Яка адреса буде broadcast-адресою для супермережі 192.168.4.0/22?

A. 192.168.4.255;

B. 192.168.5.255;

C. 192.168.7.255;

D. 192.168.3.255.

9. Який інструмент найчастіше використовують для визначення спільного префікса підмереж?

A. ASCII-таблиці;

B. Бінарне порівняння адрес;

C. DHCP-сервер;

D. SNMP.

10. Який діапазон покриває супермережа 10.0.0.0/21?

A. 10.0.0.0 – 10.0.0.255;

B. 10.0.0.0 – 10.0.1.255;

C. 10.0.0.0 – 10.0.7.255;

D. 10.0.0.0 – 10.0.15.255.

ПРАКТИЧНА РОБОТА №7
Статична та динамічна маршрутизація

Мета роботи: сформувати уміння розрізняти принципи роботи статичної та динамічної маршрутизації, розуміти їхні переваги та обмеження, навчитися створювати базові конфігурації для обох типів маршрутизації у простих мережевих топологіях.

Матеріали та ресурси: ПК з мережевими симуляторами (Cisco Packet Tracer, GNS3 або EVE-NG), таблиці команд для маршрутизаторів.

Завдання для роботи під час заняття

1. Використання статичної маршрутизації

У найпростішому випадку при об'єднанні мереж, між якими є кілька роутерів, використовується статична маршрутизація. Наприклад, візьмемо дві мережі: 192.168.1.0 з маскою 255.255.255.0 та 172.16.0.0 з маскою 255.255.255.0, між якими буде два роутери з мережею між ними 10.10.10.0 з маскою 255.255.255.252.

1. На робоче поле програми Packet Tracer додайте два комутатори 2950-24 (Switch0 і Switch1), два роутери Router 1841 (Router0 и Router1), два стаціонарних комп'ютери (PC0 і PC1).

2. Підключіть всі пристрої з комутатором за допомогою витої пари, а роутери між собою – крос-кабелем. Порти підключення для всіх пристроїв – FastEthernet. Топологія мережевої моделі показана на рис. 7.1.

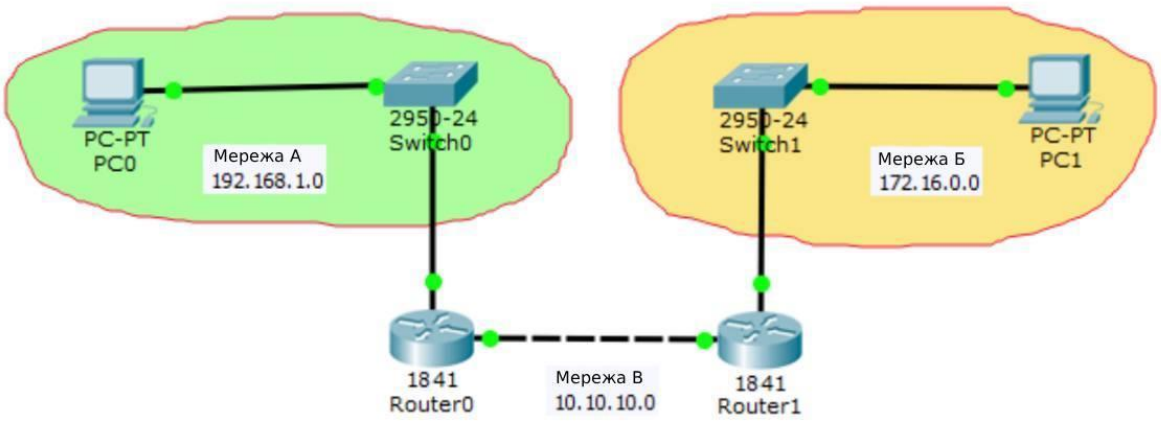


Рис. 7.1. Топологія мережевої моделі

3. Збережіть створену топологію.

4. Налаштуйте елементи мережі. Зарезервуйте для роутера Router0 першу доступну IP-адресу в мережі А – 192.168.1.1, а для роутера Router1 – першу доступну IP-адресу в мережі В – 172.16.0.1.

5. Щоб налаштувати PC0, відкрийте його властивості. На вкладці *Desktop* виберіть пункт *IP Config* і для режиму отримання IP-адреси *Static* в поле *IP Address* введіть другу доступну мережеву адресу – 192.168.1.2, в поле *Subnet*

Mask – маску мережі 255.255.255.0, а в полі *Default Gateway* вкажіть першу доступну IP-адресу мережі А, зарезервовану для роутера тобто 192.168.1.1. Комп'ютер PC1 мережі Б налаштовуйте аналогічно, але в поле *IP Address* введіть адресу – 172.16.0.2, а в поле *Default Gateway* – 172.16.0.1.

6. Налаштуйте роутер Router0. Щоб відкрити властивості роутера, перейдіть на вкладку *Config* та в підменю *INTERFACE* виберіть модуль FastEthernet0/0, до якого підключена мережа А. У поле IP Address введіть першу зарезервовану IP-адресу підмережі – 192.168.1.1, а в поле *Subnet Mask* – мережну маску 255.255.255.0. Після цього включіть цей модуль – *Port Status* встановіть в *On*. В інтерфейсі FastEthernet0/1 встановіть адресу 10.10.10.1 та мережну маску 255.255.255.252 мережі Б.

7. Аналогічно, налаштуйте Router1. На інтерфейсі FastEthernet0/0 вкажіть адресу 172.16.0.1 та маску мережі 255.255.255.0 мережі В, а на інтерфейсі FastEthernet0/1 задайте адресу 10.10.10.2 та мережеву маску 255.255.255.252 мережі В.

8. Оскільки Router0 не знає про мережу В, а Router1 – про мережу А, додайте відповідні статичні маршрути до маршрутизаторів. Відкрийте властивості Router0, перейдіть на вкладку *Config* та в підменю *ROUTING* виберіть *Static*. У полі *Network* введіть адресу мережі Б – 172.16.0.0, в *Mask – її маску* 255.255.255.0, а в якості наступного переходу в полі *Next Hop* вкажіть Router1, до якого підключено Router0, – 10.10.10.2 (рис. 7.2). Для додавання цих відомостей до списку адрес натисніть кнопку *Add*.

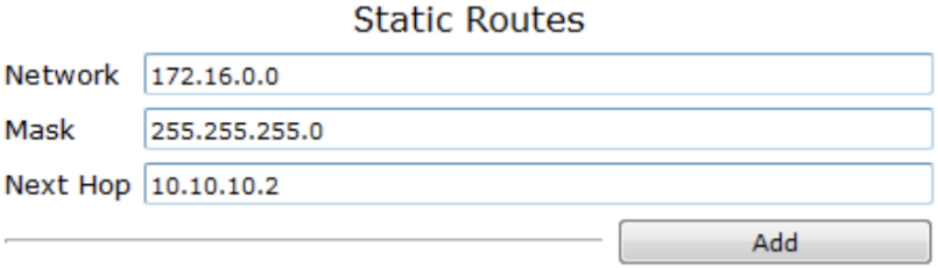


Рис. 7.2. Додавання статичного запису в Router0

Router1 налаштовується аналогічно. У полі *Network* введіть адресу мережі А – 192.168.1.0, в *Mask* – її маску 255.255.255.0, а в якості наступного переходу, у полі *Next Hop* вкажіть інтерфейс Router0, до якого підключено Router1, – 10.10.10.1.

9. Перевірте правильність налаштувань мережевих пристроїв і працездатність мережі. Пропінгуйте з компютера PC0 комп'ютер PC. Для цього відкрийте властивості комп'ютера PC0 на вкладці *Desktop* виберіть пункт *Command* P*romt* і у вікні, що відкриється, в командному рядку, введемо команду *ping* та IP-адресу комп'ютера PC1. Нижче наведені результати виконання команди *ping:*

```
PC>ping 172.16.0.2
Pinging 172.16.0.2 with 32 bytes of data:
Reply from 172.16.0.2: bytes=32 time=13ms TTL=126
Reply from 172.16.0.2: bytes=32 time=11ms TTL=126
Reply from 172.16.0.2: bytes=32 time=11ms TTL=126
Reply from 172.16.0.2: bytes=32 time=14ms TTL=126
Ping statistics for 172.16.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 14ms, Average = 12ms
```

10. Перевірте шлях пакетів з мережі А в мережу Б. У командний рядок комп'ютера PC0 введіть команду *tracert* та IP-адресу комп'ютера PC1. Нижче наведено результати команди *tracert:*

```
PC>tracert 172.16.0.2
Tracing route to 172.16.0.2 over a maximum of 30 hops:
1 0 ms 0 ms 0 ms 192.168.1.1
2 0 ms 0 ms 0 ms 10.10.10.2
3 12 ms 12 ms 12 ms 172.16.0.2
Trace complete.
```

Такий результат підтверджує, що всі мережні пристрої настроєно належним чином.

2. Використання динамічної маршрутизації

Для об'єднання мереж, між якими є якась кількість роутерів, використовується динамічна маршрутизація. Розглянемо динамічну маршрутизацію на топології мережі з попереднього прикладу.

1. Залишіть всі мережеві налаштування пристроїв без змін, за винятком статичних маршрутів – видаліть усі налаштовані статичні маршрути на Router0 і Router1. Для цього відкрийте властивості роутера, перейдіть на вкладку *Config*, у підменю *ROUTING* виберіть *Static*, у полі *Network Address* виділіть запис та натисніть кнопку *Remove*.

2. Тепер, після видалення маршрутів, Router0 не знає про мережу Б, а Router1 про мережу А. Налаштуйте динамічну маршрутизацію за протоколом RIP на обох маршрутизаторах. Для цього кожному роутеру потрібно визначити, які мережі до нього підключені. Відкрийте властивості Router0, перейдіть на вкладку *Config*, в підменю *ROUTING* виберіть пункт RIP. У полі *Network* введіть адреси підключених мереж 10.10.10.0 та 192.168.1.0 і додайте їх до списку за допомогою кнопки Add (рис. 7.3).

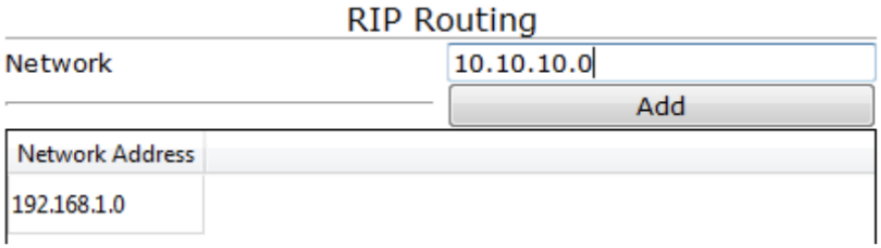


Рис. 7.3. Оголошення мереж в маршрутизаторі0

3. Аналогічно для Router1 оголосіть мережі 10.10.10.0 та 172.16.0.0.

4. Перевірте правильність мережевих налаштувань пристроїв і працездатність мережі. Пропінгуйте з комп'ютера PC0 комп'ютер PC1. Нижче наведені результати команди *ping:*

```
PC>ping 172.16.0.2
Pinging 172.16.0.2 with 32 bytes of data:
Reply from 172.16.0.2: bytes=32 time=11ms TTL=126
Reply from 172.16.0.2: bytes=32 time=12ms TTL=126
Reply from 172.16.0.2: bytes=32 time=12ms TTL=126
Reply from 172.16.0.2: bytes=32 time=12ms TTL=126
Ping statistics for 172.16.0.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 12ms, Average = 11ms
```

5. Перевірте шлях пакетів з мережі А в мережу Б. Нижче представлені результат команди *tracert:*

```
PC>tracert 172.16.0.2
Tracing route to 172.16.0.2 over a maximum of 30 hops:
1 0 ms 0 ms 0 ms 192.168.1.1
2 0 ms 0 ms 0 ms 10.10.10.2
3 11 ms 12 ms 11 ms 172.16.0.2
Trace complete.
```

З цього випливає, що всі пристрої в мережі налаштовані правильно.

Завдання для самостійної роботи

1. Додайте на робоче поле програми Packet Tracer три комутатори Switch 2950-24 (Switch0 – Switch2), три загальні роутери Generic Router-PT-Empty (Router0 – Router2), шість стаціонарних комп'ютерів (PC1 – PC6).

2. Додайте до кожного роутери по три Gigabit Ethernet-модуля PT ROUTERNM-1CGE і створіть мережу відповідно до рис. 7.4.

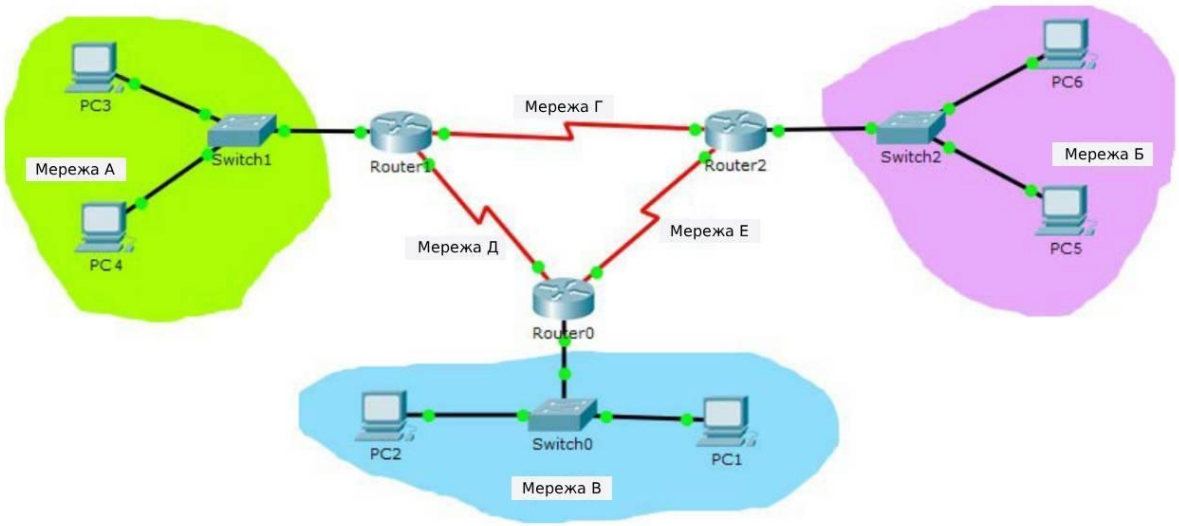


Рис. 7.4. Топологія мережі

3. Призначте всім вузлам статичні IP-адреси відповідно до варіанту (табл. 7.1). Для мереж А, Б, В використайте мережеву маску 255.255.255.0, а для мереж Г, Д, Е – 255.255.255.252.

Таблиця 7.1. Варіанти завдань

№ вар.	Мережа А	Мережа Б	Мережа В	Мережа Г	Мережа Д	Мережа Е
1	92.16.0.0	45.44.47.0	72.28.200.0	223.16.166.8	22.16.0.4	78.4.4.16
2	90.15.128.0	7.27.37.0	45.228.25.0	223.166.18.8	20.15.128.4	42.45.15.16
3	92.135.0.0	57.27.25.0	27.42.27.0	232.16.13.8	22.135.0.4	55.13.13.16
4	10.101.64.0	41.77.123.0	77.77.7.0	94.45.41.8	223.16.166.4	11.11.11.16
5	25.98.0.0	123.16.166.0	31.169.1.0	42.42.7.8	223.166.18.4	22.22.22.16
6	56.6.128.0	123.166.18.0	169.1.196.0	75.28.72.8	202.16.13.4	25.165.16.16
7	81.16.0.0	192.16.13.0	16.163.1.0	49.4.4.8	61.49.48.4	3.16.166.16
8	91.29.192.0	123.99.81.0	106.49.19.0	19.196.16.8	65.46.98.4	3.166.18.16
9	90.155.0.0	192.16.19.0	158.89.1.0	19.16.18.8	18.156.5.4	3.16.13.16
10	65.16.128.0	77.88.2.0	198.19.169.0	41.84.65.8	4.46.46.4	15.15.15.16

4. Інтерфейсам роутерів призначте першу та другу доступні адреси

мережі. Цільовим пристроям слід надавати адреси, починаючи з третьої доступної адреси.

5. Створіть на роутерах статичні маршрути до невідомих їм мереж:
    - для Router0 додайте статичні маршрути в мережу А, Д, Е.
    - для Router1 додайте статичні маршрути в мережі Б, В, Е.
    - для Router2 додайте статичні маршрути в мережу А, В, Д.
6. Перевірте роботу мережі за допомогою команди *ping.*
7. Виконайте трасування між вузлами PC3 і PC6, PC5 і PC1.
8. Перевірте таблицю маршрутизації роутерів за допомогою інструменту «Inspect/Routing Table
9. Видаліть всі статичні маршрути на роутерах.
10. Оголосіть на роутерах безпосередньо підключені до них мережі для роботи протоколу динамічної маршрутизації RIP:
    - для маршрутизатора0 оголосіть маршрути в мережі В, Д, Е.
    - для маршрутизатора1 оголосіть маршрути в мережі А, Д, Г.
    - для маршрутизатора2 оголосіть маршрути в мережі В, Е, Г.
11. Перевірте роботу мережі за допомогою команди *ping.*
12. У режимі симуляції відправте запит з PC1 на PC3. Прослідкуйте за рухом пакетів по протоколу ICMP.
13. Виконайте трасування між вузлами PC3 і PC6, PC5 і PC1. Видаліть під’єднання мережі Г. Повторіть трасування.
14. Перевірте таблицю маршрутизації роутерів за допомогою інструменту *Inspect/Routing Table*.

Питання для обговорення на занятті

1. У чому полягає принципова різниця між статичною та динамічною маршрутизацією?
2. Які переваги статичних маршрутів у невеликих мережах?
3. Які недоліки статичної маршрутизації стають критичними у великих мережах?
4. Чому динамічна маршрутизація вважається гнучкішою та масштабованішою?
5. Чим відрізняється робота протоколів RIP та OSPF?
6. Як маршрутизатор вибирає найкращий маршрут у протоколах динамічної маршрутизації?
7. Які типові ситуації вимагають використання статичних резервних маршрутів?
8. Як петлі маршрутизації можуть виникати в динамічних протоколах і як їх уникнути?
9. Чому OSPF вважається швидшим і надійнішим у порівнянні з RIP?

10. Які фактори потрібно враховувати при виборі протоколу маршрутизації для конкретної мережі?

Тестові запитання

1. Що таке статичний маршрут?

A. Маршрут, який автоматично оновлюється мережею;

B. Маршрут, який задається адміністратором вручну;

C. Маршрут, що виникає через NAT;

D. Маршрут, який генерує DNS.

2. Який протокол належить до динамічної маршрутизації?

A. ARP;

B. RSTP;

C. OSPF;

D. VLAN.

3. Який недолік притаманний статичним маршрутам?

A. Потребують менше ресурсів;

B. Автоматично адаптуються до змін у мережі;

C. Потрібно вручну оновлювати при зміні топології;

D. Працюють тільки у LAN.

4. Який алгоритм використовує OSPF?

A. Bellman-Ford;

B. Dijkstra (Shortest Path First);

C. Random Forwarding;

D. Flooding.

5. Який максимальний хоп-каунт у протоколу RIP?

A. 5;

B. 10;

C. 15;

D. 255.

6. Який тип маршрутизації зазвичай використовують у великих корпоративних мережах?

A. Лише статичну;

B. Лише динамічну;

C. Комбіновану (гібридну);

D. Маршрутизацію без таблиць.

7. Який параметр OSPF використовує для вибору найкращого маршруту?

A. Пропускну здатність інтерфейсу (cost);

B. IP-адресу;

C. MAC-адресу;

D. RTT.

8. Який тип маршрутизації вимагає менше трафіку службових повідомлень?

A. RIP;

B. OSPF;

C. Статична маршрутизація;

D. EIGRP;

9. Як називається таблиця, де маршрутизатор зберігає маршрути?

A. ARP-таблиця;

B. Routing table;

C. Forwarding table;

D. MAC-таблиця.

10. У якій ситуації динамічна маршрутизація буде ефективнішою?

A. Мережа має 3–4 пристрої;

B. Топологія мережі часто змінюється;

C. Мережа працює лише з IPv6;

D. Комутатори працюють у режимі L2.

ПРАКТИЧНА РОБОТА №8
Налаштування бездротової мережі в Cisco Packet Tracer

Мета роботи: сформувати уміння створювати та налаштовувати бездротову мережу Wi-Fi у Cisco Packet Tracer, розуміти принципи роботи точок доступу, параметри безпеки, режими шифрування та зв’язок між бездротовими й дротовими сегментами мережі. Навчитися створювати базову WLAN, налаштовувати SSID, типи автентифікації, параметри радіоканалу, інтервал маяків, шифрування WPA2, а також забезпечувати коректне підключення клієнтів та перевірку якості зв’язку й маршрутизації між сегментами мережі.

Матеріали та ресурси: ПК з установленим Cisco Packet Tracer, документація Cisco щодо Wireless Devices, інструкції для налаштування безпеки WLAN.

Завдання для роботи під час заняття

1. Налаштування бездротової мережі

1. Додайте на робочу область програми Packet Tracer стаціонарний комп’ютер та Wi-Fi роутер WRT300N. Комп’ютер з роутером об’єднайте витою парою. Порт підключення комп'ютера FastEthernet, роутера – Ethernet.

2. Стандартна IP-адреса сучасних бездротових маршрутизаторів – *192.168.0.1* з маскою – *255.255.255.0*. Призначені адресу та маску роутера можна перевірити у вікні властивостей пристрою на вкладці *Config* в підменю *LAN*.

3. Для того щоб підключити комп'ютер до маршрутизатора у вікні властивостей комп'ютера на вкладці *Desktop* виберіть *IP Configuration.* Для автоматичного отримання IP-адреси перемикач способу призначення адреси встановіть в положення DHCP. Через деякий час у відповідних полях з'явиться IP-адреса комп'ютера, маска мережі та IP-адреса шлюзу.

4. Щоб відобразити налаштування мережі, відкрийте на комп’ютері командний рядок (*Desktop/Command Promt*) і введіть команду *ipconfig /all*. Результат виконання команди буде мати вигляд:

```
PC>ipconfig /all
FastEthernet0 Connection:(default port)
Physical Address.................: 00D0.9739.B139
Link-local IPv6 Address......: FE80::2D0:97FF:FE39:B139
IP Address.......................: 192.168.0.100
Subnet Mask.....................: 255.255.255.0
Default Gateway.................: 192.168.0.1
```

```
DNS Servers.....................: 0.0.0.0
DHCP Servers....................: 192.168.0.1
DHCPv6 Client DUID........: 00-01-00-01-29-8D-D2-19-00-D0-97-
39-B1-39
```

5. Щоб перевірити зв’язок комп'ютера з роутером, потрібно надіслати запит з комп'ютера за допомогою команди *ping:*

```
PC>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=2ms TTL=255
Reply from 192.168.0.1: bytes=32 time=0ms TTL=255
Reply from 192.168.0.1: bytes=32 time=0ms TTL=255
Reply from 192.168.0.1: bytes=32 time=0ms TTL=255
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

6. Відкрийте Web Browser, в рядок введення URL введіть IP-адресу роутера. Відкриється вікно запиту на введення імені користувача та пароля. За замовчуванням на всіх маршрутизаторах Wi-Fi встановлено ім'я «admin» і пароль «admin». Після їх входу перейдемо до сторінки налаштування роутера. Цю сторінку також можна відкривати через властивості роутера на вкладці GUI. Але в реальних умовах доступ до налаштувань Wi-Fi-роутера можна отримати лише через браузер підключеного до нього комп’ютера.

На сторінці налаштування маршрутизатора є кілька вкладок:

- На вкладці *Setup* налаштовується вхідне Інтернет-з’єднання (Internet Setup), яке можна налаштувати на отримання динамічних налаштувань (DHCP), статичних налаштувань PPPoe. Усі ці параметри повідомляє інтернет-провайдер. Також на вкладці Setup можна налаштувати IP-адресу маршрутизатора всередині локальної мережі (Network Setup) та встановити DHCP-сервер (сервер автоматичної роздачі IP-адрес в мережі), в ролі якого також може виступати в якості Wi-Fi-роутер.
- На вкладці *Wireless* підменю *Basic Wireless Setting* можна сконфігурувати установки безпровідної мережі:
    - *Network Mode (Режим роботи)* – керування режимами швидкості передачі даних;
    - *Network Name (SSID) (*Ідентифікатор мережі) – ім'я бездротової мережі, відображення якого можна приховати (SSID Broadcast – Disable);

- Standard Channel – встановлює канал передачі даних;
- в підменю *Wireless Security* налаштовується режим безпеки (Security Mode) бездротової мережі – вибирається метод шифрування (WEP, WPA, WPA2) і встановлюється пароль на підключення до мережі;
- в підменю *Wireless MAC Filter* налаштовується фільтрація за MAC адресою – дозвіл на підключення до бездротової мережі тільки певних вже відомих пристроїв.

- На вкладці *Access Restrictions* можна заборонити доступ до мережі тому чи іншому пристрою або протоколу.
- На вкладці *Application and Gaming* пункт Port Forwarding використовується для налаштування так званого «пробросу» портів (технологія трансляції мережевої адреси залежно від TCP/UDP-порта отримувача).
- На вкладці *Administration* можна налаштувати доступ до роутера (ім'я, пароль, доступ до мережі, доступ до Web-інтерфейсу).
- На вкладці *Wireless* в підменю *Basic Wireless Setting* в полі ідентифікатора мережі вводимо ім'я мережі LabRab. Режим безпеки у підменю *Wireless Security* встановіть WPA2 Personal. Алгоритм шифрування – AES. Пароль (Passphrase) повинен містити не менше 8 символів, в це поле введіть, наприклад, 11111111.

7. Підключіть ноутбук до бездротової мережі. До робочої області програми додайте пристрій Laptop. За замовчуванням ноутбук не містить Wi-Fi модуль. Щоб встановити його, необхідно відкрити властивості Laptop, вибрати вкладку *Physical*, на моделі ноутбука натисніть кнопку живлення для вимкнення, вийміти модуль підключення до локальної мережі, та на його місце встановіть модуль Wi-Fi WPC300N і увімкніть ноутбук. Потім перейдіть на вкладку *Config* в підменю *Wireless0*. Перемикач IP Configuration повинен бути в положенні DHCP для автоматичного отримання IP-адреси. У полі SSID введіть назву мережі – LabRab. Перемикач аутентифікації встановіть в положення WPA2-PSK і в поле PSK Pass Phrase введіть заданий раніше пароль 11111111. Ноутбук підключиться до вказаної бездротової мережі. Перевірити підключення можна за допомогою меню *PC Wireless* на вкладці *Desktop* властивостей ноутбука. На вкладці *Connect* відображається список бездротових мереж і основна інформація про них (рис. 8.1). За допомогою цього інтерфейсу також можна підключитись до бездротової мережі. Для цього потрібно вибрати мережу, натиснути кнопку *Connect* та вказати тип шифрування та пароль. На вкладці *Link information* ідентифікаторами відображається потужність сигналу якість зв’язку. Отримати більш детальну інформацію про мережу можна

натиснувши кнопку *More information*.

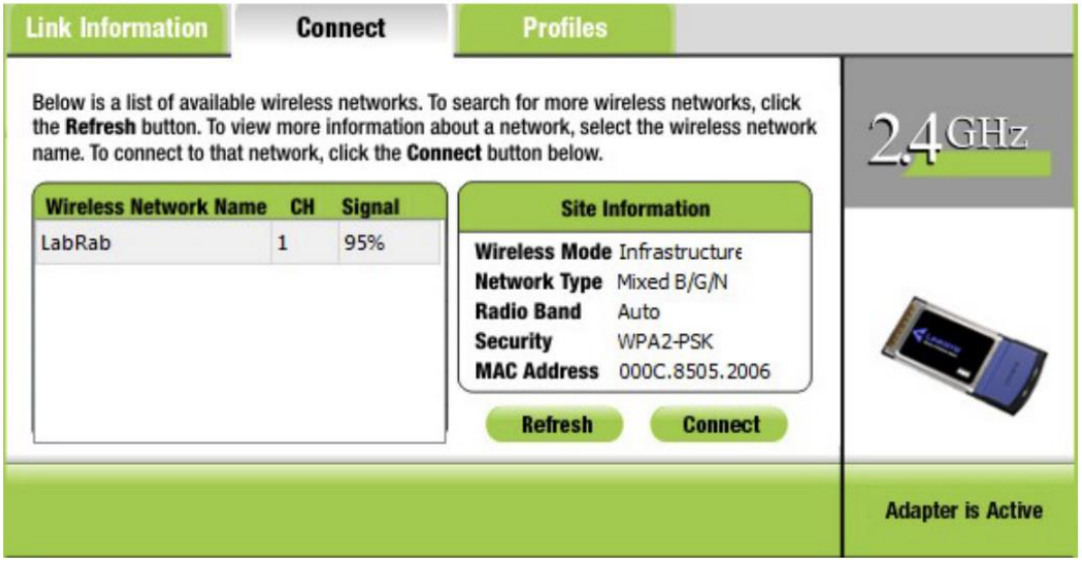


Рис. 8.1. Вікно підключення до бездротової мережі

8. Інші пристрої до мережі Wi-Fi без широкомовлення SSID підключаються аналогічно: у властивостях пристрою на вкладці *Config* в підменю *Wireless0* потрібно, як описано вище, заповнити поля SSID, Authentication, IP Configuration.

Завдання для самостійної роботи

1. Додайте в робочу область Packet Tracer настільний комп'ютер (PCPT PC1) та Wi-Fi роутер (WRT300N) і підключіть їх прямим кабелем типу вита пара.

2. Через Web-інтерфейс комп’ютера PC1 виконайте налаштування Wi-Fi роутера відповідно до зазначеного варіанту (табл. 8.1).

3. Змініть внутрішню IP-адресу роутера відповідно до таблиці. 8.2. (При зміні локальної IP-адреси роутера з'єднання з ПК переривається, тому що IP адреси цих пристроїв будуть в різних мережах. Для відновлення підключення необхідно на PC зайти в пункт *IP Configuration* вибрати *Static*, а потім *DHCP*. В результаті PC отримає нову IP-адресу з новим номером мережі.

Таблиця 8.1. Параметри завдання перемикання WAN

№ вар.	**Тип комутації провайдера**	**Налаштування провайдера для роутера**
1	Автоматичні налаштування	-

2	Статичні налаштування	IP-адреса Інтернету – 45.45.42.42 Маска підмережі – 255.255.0.0 Шлюз за промовчанням – 45.45.0.1 DNS-сервер – 58.255.0.1
3	Параметри PPPoe	Username – a87svfk Password – dsfjhDFS921
4	Автоматичні налаштування	-
5	Статичні налаштування	Internet IP Address – 19.52.132.22 Subnet Mask – 255.255.255.0 Default-Gateway – 19.52.132.1 DNS Server – 158.55.30.41
6	Параметри PPPoe	Username – ADSo23473 Password – sdgkj56hg
7	Автоматичні налаштування	-
8	Параметри PPPoe	Username – BVB44556 Password – htrbYJJYfg676
9	Статичні налаштування	Internet IP Address – 88.45.42.42 Subnet Mask – 255.255.0.0 Default-Gateway – 88.45.0.1 DNS Server – 88.45.0.1
10	Автоматичні налаштування	-

4. Збережіть поточну конфігурацію.

5. Увімкніть сервер «Отримання автоматичних налаштувань» (DHCP) для клієнтів. Діапазон видачі IP-адрес задайте відповідно до табл. 8.2.

Таблиця 8.2. Параметри визначення діапазону адрес для DHCP-сервера

№ вар.	IP-адреса роутера	Перша адреса діапазону	Остання адреса діапазону	Маска мережі
1	192.168.2.254	192.168.2.20	192.168.2.200	255.255.255.0
2	192.168.7.254	192.168.7.50	192.168.7.100	255.255.255.0
3	192.168.50.254	192.168.50.100	192.168.50.130	255.255.255.0
4	192.168.8.254	192.168.8.140	192.168.8.200	255.255.255.0
5	192.168.5.254	192.168.5.200	192.168.5.220	255.255.255.0
6	192.168.22.254	192.168.22.60	192.168.22.90	255.255.255.0
7	192.168.70.254	192.168.70.90	192.168.70.120	255.255.255.0
8	192.168.150.254	192.168.150.120	192.168.150.160	255.255.255.0
9	192.168.12.254	192.168.12.180	192.168.12.210	255.255.255.0
10	1192.168.90.254	192.168.90.70	192.168.90.90	255.255.255.0

6. Налаштуйте бездротову мережу відповідно до таблиці 8.3.

Таблиця 8.3. Параметри завдання бездротового налаштування

№ вар.	Швидкість передачі сигналу, (Мбит/с)	Канал передачі даних	Ширина каналу, (МГц)	Режим захисту	Шифрування
1	11	2	20	WEP	40/64-біт
2	300	4	40	WPA Pers.	TKIP
3	54	6	20	WPA2 Pers. AES	

4	11	8	20	WEP	40/64-біт
5	300	10	40	WPA Pers.	TKIP
6	54	9	20	WPA2 Pers. AES	
7	11	7	20	WEP	40/64-біт
8	300	5	40	WPA Pers.	TKIP
9	54	3	20	WPA2 Pers. AES	
10	11	1	20	WEP	40/64-біт

7. В якості ідентифікатора використайте ідентифікатор (SSID) бездротової мережі використайте «власне ім'я + номер варіанту».

8. Дозвольте трансляцію SSID.

9. Змініть пароль для входу на роутер.

10. Збережіть поточну конфігурацію.

11. Підключіть маршрутизатор до інтернету (елемент Cloud-PT).

12. Додайте другий комп'ютер PC2 до мережі та підключіть його до маршрутизатора з допомогою витої пари. Призначте інтерфейсу PC2 другу доступну адресу в мережі з маскою 255.255.255.0. Як шлюз за замовчуванням використовуйте IP-адресу маршрутизатора.

13. Додайте в мережу ноутбук, планшет і смартфон. Ці пристрої повинні підключатися до мережі по бездротовому зв'язку з динамічним налаштування мережі (рис. 8.2).

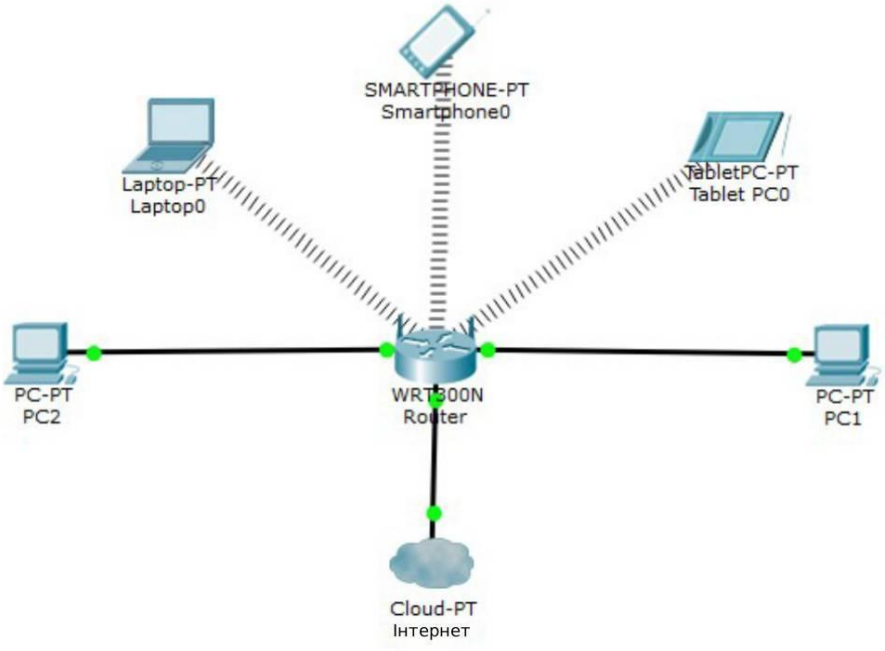


Рис. 8.2. Топологія мережі

14. Перевірте налаштування всіх цільових вузлів в мережі за допомогою команди *ipconfig /all.*

15. Переконайтеся, що мережа працює за допомогою команди *ping.*

Питання для обговорення на занятті

1. Які основні відмінності між дротовою та бездротовою мережею з точки зору архітектури та безпеки?
2. Що таке SSID і для чого він використовується?
3. Чому важливо змінювати за замовчуванням заданий SSID і пароль на точці доступу?
4. У чому різниця між відкритою мережею, WEP, WPA та WPA2?
5. Як вибір радіоканалу впливає на швидкість і стабільність Wi-Fi?
6. Чим відрізняється точка доступу від домашнього Wi-Fi-маршрутизатора?
7. Чому в Packet Tracer правильна IP-адресація важлива навіть у бездротовому сегменті?
8. Які типи пристроїв найчастіше використовуються для підключення до WLAN?
9. Як перевірити працездатність бездротового підключення в Packet Tracer?
10. Які ризики виникають при неправильному налаштуванні безпеки Wi-Fi?

Тестові запитання

1. Що таке SSID?

А. MAC-адреса точки доступу;

B. Ім’я бездротової мережі;

C. Тип шифрування;

D. Канал передачі даних.

2. Який тип шифрування вважається найбезпечнішим для WLAN у Packet Tracer?

A. Open;

B. WEP;

C. WPA;

D. WPA2.

3. Який інструмент використовують у Packet Tracer для тестування доступності пристроїв?

A. Trace Tool;

B. Ping;

C. Packet Filter;

D. Simulation Graph.

4. Яка частота найчастіше використовується стандартними точками доступу в Packet Tracer?

A. 1.2 GHz;

B. 2.4 GHz;

C. 5 MHz;

D. 900 MHz.

5. Що робить точка доступу?

A. Роздає IP-адреси;

B. Маршрутизує пакети між VLAN;

C. Забезпечує бездротове підключення клієнтів;

D. Виконує NAT.

6. Який канал у діапазоні 2.4 GHz найменше схильний до перешкод у більшості регіонів?

A. 1;

B. 3;

C. 6;

D. 12.

7. Який параметр обов’язково потрібно вказати під час підключення клієнта до Wi-Fi?

A. VLAN ID;

B. Gateway MAC;

C. SSID;

D. DNS-сервер.

8. Який параметр відповідає за фільтрацію доступу за фізичною адресою?

A. WPA-ключ;

B. MAC-фільтрація;

C. DNS-фільтрація;

D. ARP-таблиця.

9. Який інтерфейс клієнта потрібно активувати для підключення до бездротової мережі?

A. Ethernet;

B. FastEthernet;

C. Serial;

D. Wireless0.

10. Яке твердження є правильним?

A. Wi-Fi працює швидше за дротову мережу;

B. Відкриті мережі завжди безпечні;

C. WPA2 забезпечує сильніше шифрування, ніж WEP;

D. Підключення до WLAN не потребує IP-адресації.

ПРАКТИЧНА РОБОТА №9

Налаштування та використання служби DHCP

Мета роботи: сформувати практичні навички налаштування та використання служби DHCP у комп’ютерних мережах, розуміння принципів автоматичного розподілу IP-адрес, параметрів DHCP-пула, механізмів оренди адрес та взаємодії між DHCP-сервером, маршрутизатором і клієнтськими пристроями.

Матеріали та ресурси: ПК з установленим Cisco Packet Tracer чи іншим мережевим симулятором, довідкові матеріали з DHCP, таблиці IP-адресації, приклади конфігурацій для маршрутизаторів Cisco.

Завдання для роботи під час заняття

1. **Налаштування служби DHCP**

Нехай є мережа 192.168.1.0 з маскою 255.255.255.0, що складається з трьох настільних комп'ютерів, трьох ноутбуків, комутатора, роутера і сервера. Необхідно настроїти DHCP-сервер і встановити автоматичне присвоєння IP адрес ноутбукам.

1. Додайте робоче поле програми Packet Tracer три стаціонарних комп’ютери (PC0 – PC2), три ноутбуки (Laptop0 – Laptop2), комутатор 2960-24TT (Switch0), роутер Generic Router-PT-Empty (Router0) і сервер Generic Server-PT (Server0).

2. Додайте один Gigabit Ethernet-модуль PT-ROUTER-NM-1CGE в роутер для підключення до мережі. Для цього відкрийте властивості Router0, на вкладці *Physical* на моделі роутера натисніть кнопку живлення для завершення роботи, виберіть вказаний модуль з'єднання та встановіть його у вільний слот.

3. Підключіть всі пристрої за допомогою витої пари. Порти підключення роутера і комутатора – GigabitEthernet, інших пристроїв та комутатора – FastEthernet. Топологія мережевої моделі представлена на рис. 9.1.

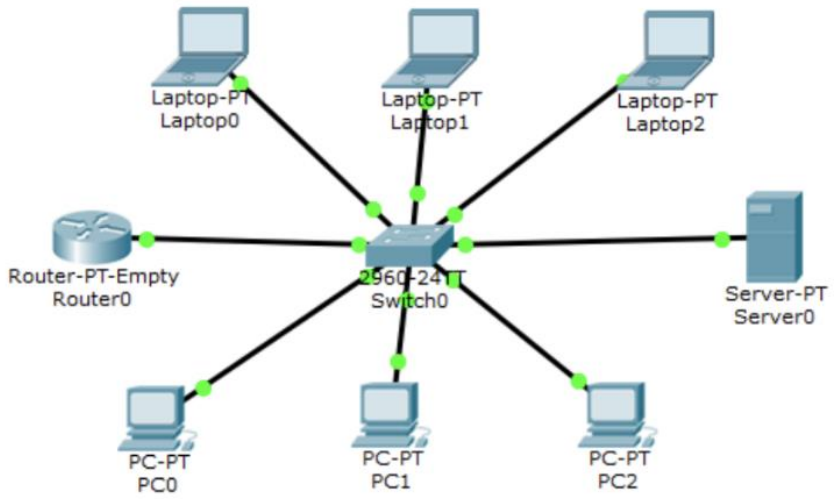


Рис. 9.1. Топологія мережі

4. Збережіть створену топологію.

5. Налаштуйте елементи мережі. Зарезервуйте для маршрутизатора першу доступну IP-адресу, для сервера - другу, а стаціонарні комп'ютери будуть отримувати адреси послідовно починаючи з третьої доступної. Маска мережі для всіх пристроїв – 255.255.255.0.

6. Щоб налаштувати PC0, відкрийте його властивості. На вкладці *Desktop* виберіть параметр *IP Config* і для режиму отримання IP-адреси Static в поле IP адреса введіть третю доступну мережеву адресу – 192.168.1.3, в поле *Subnet Mask* –255.255.255.192, а в поле за *Default Gateway* – першу доступну IP-адресу мережі, зарезервовану для роутера – 192.168.1.1. Інші настільні комп'ютери налаштуйте аналогічно.

7. Налаштуйте роутер. Для цього відкрийте його властивості, перейдіть до вкладки *Config* та в підменю *INTERFACE* виберіть модуль *GigabitEthernet0/0*, до якого підключено комутатор. У поле *IP Address* – введіть першу зарезервовану IP-адресу підмережі – 192.168.1.1, а в поле *Subnet Mask* – 255.255.0 та включіть цей модуль – *Port Status* встановіть на значення On.

8. Щоб налаштувати сервер, відкрийте його властивості, перейдіть на вкладку *Config* та в підменю *INTERFACE* виберіть модуль *FastEthernet0*. У поле *IP Address* – введіть другу зарезервовану IP-адресу мережі – 192.168.1.2, в *Subnet Mask* – 255.255.255.0 та включіть даний модуль.

9. Налаштуйте сервіс DHCP. Для цього відкрийте вкладку *Services* виберіть підменю *DHCP*. Для включення перемикач *Service* встановіть в положення *On*. Призначте ім'я пулу для роздачі адрес – у поле *Pool Name* введіть *APP_Pool;* в поле *Default Gateway* – IP-адресу роутера 192.168.1.1. Для автоматичного розподілу виділіть адреси починаючи з шостої доступної адреси мережі: в поле *Start IP Address* введіть 192.168.1.6; в поле *Subnet Mask* – маску мережі 255.255.255.0; натисніть кнопку *Add* і в DHCP-таблиці з'явиться відповідний запис.

10. Налаштуйте ноутбуки для автоматичного отримання IP-адреси. Для laptop0, у його властивостях на вкладці *Desktop* виберіть пункт *IP Config* та активуйте режим отримання IP-адреси DHCP. Через деякий час в полях *IP Address* та *Subnet Mask* з'являться мережеві параметри. У нашому випадку це перша IP-адреса, доступна для автоматичне призначення – 192.168.1.6 та маска мережі – 255.255.255.0.

Решта ноутбуків налаштуйте аналогічно. Перевірити призначені адреси можна використавши засіб Inspect/Port Status Summary Table.

11. Перевірте працездатність мережі. Зайдіть на PC0 і пропінгуйте Laptop0. Результати виконання команди *ping*:

```
PC>ping 192.168.1.6
Pinging 192.168.1.6 with 32 bytes of data:
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Reply from 192.168.1.6: bytes=32 time=0ms TTL=128
Ping statistics for 192.168.1.6:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Такий результат роботи вказує на те, що параметри мережевих пристроїв є правильними.

Завдання для самостійної роботи

1. Створіть мережу відповідно до топології, показаної на рис. 9.1.
2. Призначте статичні IP-адреси цільовим вузлам відповідно до варіанту (табл. 9.1):
   - призначте першу доступну адресу інтерфейсу роутера;
   - призначте другу доступну адресу інтерфейсу сервера;
   - призначте PC0 третю доступну адресу;
   - призначте PC1 четверту доступну адресу;
   - призначте PC2 п'яту доступну адресу.

Таблиця 9.1. Параметри завдання

№ варіанту	Адреса мережі	Маска мережі
1	44.16.105.0	255.255.255.128
2	45.16.115.0	255.255.255.192
3	46.16.125.0	255.255.255.224
4	47.16.135.0	255.255.255.128
5	48.16.145.0	255.255.255.192
6	49.16.155.0	255.255.255.224

7	50.16.165.0	255.255.255.128
8	51.16.175.0	255.255.255.192
9	52.16.185.0	255.255.255.224
10	53.16.195.0	255.255.255.128

3. Налаштуйте Server0 сервіс DHCP.

4. У режимі симуляції налаштуйте Laptop0 на динамічне отримання IP адреси. Відстежте рух пакетів за допомогою протоколу DHCP. Налаштуйте решту ноутбуків в мережі для динамічного отримання IP-адрес.

5. Перевірте налаштування комп'ютера за допомогою команди *ipconfig /all.*

6. Перевірте працездатність мережі – пропінгуйте з першого стаціонарного комп’ютера всі вузли.

Питання для обговорення на занятті

1. Які основні функції виконує DHCP у мережі?
2. Чим DHCP відрізняється від статичної адресації?
3. Чому важливо визначати коректний діапазон адрес у DHCP-пулі?
4. Які параметри, окрім IP-адреси, клієнт може отримати через DHCP?
5. Що таке оренда IP-адреси і як працює її оновлення?
6. Які можливі проблеми виникають, якщо два DHCP-сервери працюють у одній мережі без узгодження?
7. У чому різниця між relay-агентом (IP helper) і DHCP-сервером?
8. Чому DHCP важливий для великих корпоративних мереж?
9. Як перевірити у Packet Tracer, що клієнт отримав адресу автоматично?
10. Які заходи можуть підвищити безпеку використання DHCP у мережі?

Тестові запитання

1. Яка основна функція DHCP?

A. Розподіляти MAC-адреси;

B. Автоматично надавати IP-адреси клієнтам;

C. Маршрутизувати трафік між VLAN;

D. Шифрувати мережеві дані.

2. Який параметр клієнт НЕ отримує від DHCP?

A. DNS-сервер;
B. Шлюз за замовчуванням;
C. Маска підмережі;
D. MAC-адреса.

3. Яка команда на маршрутизаторі Cisco створює DHCP-пул?
A. ip dhcp helper;
B. ip dhcp pool;
C. dhcp enable;
D. config-dhcp start.

4. Що робить команда ip dhcp excluded-address?
A. Вимикає DHCP-сервер;
B. Видаляє всі адреси з пулу;
C. Забороняє видачу певних адрес клієнтам;
D. Встановлює час оренди.

5. Який стандартний порт використовує DHCP?
A. 21;
B. 53;
C. 67/68;
D. 443.

6. Який протокол використовується DHCP для роботи?
A. UDP;
B. TCP;
C. ICMP;
D. SMTP.

7. Як клієнт у Packet Tracer отримує нову адресу?
A. Через вручну доданий ARP-запис;
B. Після команди renew у Desktop → IPConfiguration;
C. Через перезавантаження комутатора;
D. Автоматично після ping.

8. Який етап DHCP відбувається першим?
A. DHCPREQUEST;
B. DHCPACK;

C. DHCPDISCOVER;
D. DHCPOFFER.

9. Чому важливо виключати адреси перед створенням DHCP-пулу?
A. Щоб уникнути конфліктів з ручними статичними адресами;
B. Щоб пришвидшити роботу DHCP;
C. Щоб збільшити кількість доступних адрес;
D. Щоб DHCP працював у VLAN.

10. Що станеться, якщо DHCP-сервер недоступний?
A. Клієнти автоматично генерують приватні адреси APIPA;
B. Маршрутизація припиниться;
C. DNS перестане працювати;
D. Клієнти отримають адреси з попереднього VLAN.

ПРАКТИЧНА РОБОТА №10
Налаштування та використання служби DNS

Мета роботи: сформувати практичні навички роботи зі службою DNS: розуміння принципів перетворення доменних імен у IP-адреси, налаштування локального DNS-сервера, створення основних записів зон, перевірки роботи служби та діагностики можливих помилок. Навчитися визначати роль DNS у комп'ютерних мережах, конфігурувати прості зони імен, забезпечувати роботу іменування у внутрішній мережі та використовувати інструменти перевірки резолюції доменів.

Матеріали та ресурси: ПК із встановленим Cisco Packet Tracer або іншим мережевим симулятором, документація з DNS, довідкові таблиці записів зон, інструкції з налаштування DNS на маршрутизаторах Cisco.

Завдання для роботи під час заняття

1. Налаштування служби DNS

Нехай існує мережа 192.168.1.0 з мережевою маскою 255.255.255.0, що складається з двох настільних комп'ютерів, двох ноутбуків, комутатора та сервера. Потрібно налаштувати DNS-сервер.

1. Додайте на робочу область програми Packet Tracer два стаціонарних комп'ютера (PC0 і PC1), два ноутбуки (Laptop0 і Laptop1), комутатор 2960-24TT (Switch0) і сервер Generic Server-PT (Server0)

2. Всі пристрої підключіть до комутатора витою парою. Порти підключення – FastEthernet. Топологія мережевої моделі представлена на рис. 10.1.

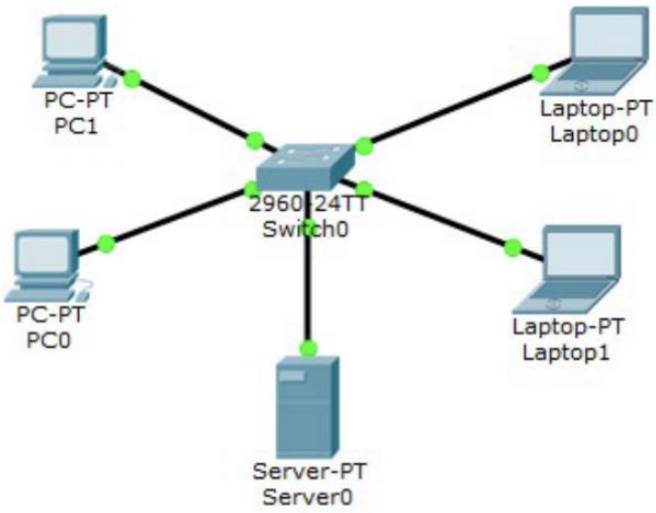


Рис. 10.1. Топологія мережі

3. Збережіть створену топологію.

4. Налаштуйте елементи мережі. Зарезервуйте для сервера першу доступну IP-адресу, а комп'ютерам надайте адреси послідовно починаючи з

другої доступної. Мережева маска для всіх пристроїв – 255.255.255.0. Дайте комп’ютерам імена, які будете використовувати в запитах замість IP-адрес: PC0 – APP1, PC1 – APP2, Laptop0 – APP3, Laptop1 – APP4.

5. Щоб налаштувати PC0, відкрийте його властивості та на вкладці *Desktop* виберіть пункт *IP Config* та для режиму отримання IP-адреси *Static* в поле *IP Address* введіть другу доступну мережеву адресу – 192.168.1.2, в поле *Subnet Mask* – маску мережі 255.255.255.192, а в поле DNS-сервер вкажіть першу доступну IP-адресу мережі, зарезервовану для сервера – 192.168.1.1. Ім'я комп'ютера можна змінити на вкладці *Config* в підменю *Global Setting* – у полі *Display Name* введіть APP1. Аналогічно налаштуйте решту комп’ютерів.

6. Налаштуйте сервер. Для цього відкрийте його властивості, перейдіть на вкладку *Config* та в підменю *INTERFACE* виберіть модуль *FastEthernet0*. У поле *IP Address* введіть першу зарезервовану IP-адресу мережі – 192.168.1.1, в поле *Subnet Mask* – маску мережі 255.255.255.0 та включіть даний модуль (*Port Status* встановіть в *On*).

7. Налаштуйте службу DNS. Перейдіть на вкладку *Services* та виберіть підменю *DNS*. Щоб увімкнути сервіс перемикач *DNS Service* встановіть в положення *On*. Щоб додати перший комп'ютер в DNS-таблицю у поле *Name* внесіть APP1, а в поле *Address* його IP-адресу – 192.168.1.2 та натисніть кнопку *Add*. В таблиці DNS з’явиться відповідний запис. Інші пристрої додайте аналогічно.

8. Перевірте працездатність мережі. Для цього перейдіть до комп'ютера APP1 та пропінгуйте ноутбук APP4. Для цього відкрийте властивості APP1, та на вкладці *Desktop* виберіть пункт *Command Promt* і у командний рядок, що відкриється, введіть команду *ping* і символьне ім'я ноутбука (APP4). Нижче наведено результати виконання команди *ping:*

```
PC>ping APP4
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Ping statistics for 192.168.1.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Такий результат роботи вказує на те, що параметри мережевих пристроїв є правильними.

Завдання для самостійної роботи

1. Створіть мережу відповідно до топології, показаної на рис. 10.1.
2. Встановіть на всі ПК та ноутбуки довільні імена за типом: "ім'я-ПК" (наприклад, «Алекс-ПК»).
3. Призначте адреси цільовим вузлам відповідно до вказаного варіанту (таблиця 10.1):
   - призначте першу доступну адресу в мережі інтерфейсу DNS-сервера;
   - призначте PC0 другу доступну адресу;
   - призначте PC1 третю доступну адресу;
   - призначте останню доступну адресу laptop0;
   - призначте передостанню доступну адресу laptop1.

Таблиця 10.1. Параметри завдання

№ варіанту	Адреса мережі	Маска мережі
1	100.10.15.0	255.255.255.240
2	100.11.15.0	255.255.255.128
3	100.12.15.0	255.255.255.0
4	100.13.15.0	255.255.255.240
5	100.14.15.0	255.255.255.128
6	100.15.15.0	255.255.255.0
7	100.16.15.0	255.255.255.240
8	100.17.15.0	255.255.255.128
9	100.18.15.0	255.255.255.0
10	100.19.15.0	255.255.255.240

4. Налаштуйте на Server0 службу DNS.
5. Перевірте працездатність мережі та DNS-сервера пропінгувавши з першого компютера решту вузлів. В якості аргумента команди ping

використовуйте символьні імена.

6. У режимі симуляції надішліть запит з символьним іменем з PC0 на Laptop0. Відстежте рух пакетів по протоколах DNS і ICMP.

Питання для обговорення на занятті

1. Для чого потрібна служба DNS і яку проблему вона вирішує?
2. Як працює процес резолюції доменного імені?
3. Що таке DNS-зона і як вона пов’язана з доменом?
4. Чим відрізняються записи A, CNAME, MX та PTR?
5. Чому DNS використовує ієрархічну модель з кореневими серверами?
6. Яку роль відіграє кешування DNS-запитів?
7. Чим відрізняється локальний DNS-сервер від публічного?
8. Які інструменти можна використовувати для діагностики роботи DNS?
9. Чому неправильні DNS-записи можуть порушити роботу веб-сайтів або додатків?
10. Які заходи підвищують надійність DNS у великих мережах?

Тестові запитання

1. Яка основна функція DNS?

A. Розподіл MAC-адрес;

B. Шифрування трафіку;

C. Перетворення доменних імен у IP-адреси;

D. Керування VLANами.

2. Який тип DNS-запису використовується для IPv4-адрес?

A. AAAA;

B. MX;

C. A;

D. CNAME.

3. Який інструмент у Packet Tracer застосовується для перевірки резолюції DNS?

A. Traceroute;

B. Nslookup;

C. DHCP Probe;

D. MAC Checker.

4. Який запис визначає псевдонім для іншого домену?

A. MX;

B. PTR;
C. CNAME;
D. SOA.

5. Що означає запис MX?
A. Сервер пошти домену;
B. Головний сервер зони;
C. Аліас доменного імені;
D. IPv6-адреса.

6. Який порт найчастіше використовує DNS?
A. 443;
B. 80;
C. 53;
D. 21.

7. Яка відповідь DNS клієнту означає, що доменного імені не існує?
A. NXDOMAIN;
B. REFUSED;
C. SERVFAIL;
D. TIMEOUT.

8. Який запис потрібен для забезпечення зворотного DNS-запиту?
A. A;
B. CNAME;
C. PTR;
D. NS.

9. Який компонент DNS є найвищим у ієрархії?
A. Secondary servers
B. Root servers
C. TLD servers
D. Authoritative servers

10. Який параметр необхідно вказати на клієнті, щоб використовувати DNS?
A. Домашню папку;
B. DHCP-option;
C. IP-адресу DNS-сервера;

D. MAC-фільтр.

ПРАКТИЧНА РОБОТА №11
Налаштування електронної пошти

Мета роботи: сформувати навички налаштування та використання служб електронної пошти у мережевому середовищі. Навчитися відправляти та отримувати електронні листи, розуміти різницю між протоколами для доставки та отримання пошти, а також використовувати інструменти перевірки працездатності поштового сервісу.

Матеріали та ресурси: ПК з установленим Cisco Packet Tracer або будь-яким іншим симулятором мереж, довідкові матеріали з поштових протоколів SMTP/POP3/IMAP, документація поштових серверів, робочі схеми мережі, таблиці портів та налаштувань безпеки.

Завдання для роботи під час заняття

1. Налаштування поштового серверу

Нехай задана мережа 192.168.1.0 з маскою 255.255.255.0, що складається з двох настільних ПК, комутатора та сервера. Необхідно налаштувати поштовий сервер і настроїти обидва ПК для отримання та надсилання електронних листів.

1. Додайте на робоче поле програми Packet Tracer два стаціонарних комп'ютери (PC0 і PC1), комутатор 2960-24TT (Switch0) і сервер Generic Server PT (Server0).

2. Підключіть всі пристрої до комутатора за допомогою витої пари. Порти підключення всіх пристроїв і комутатора – FastEthernet. Топологія моделі мережі представлена на рис. 11.1.

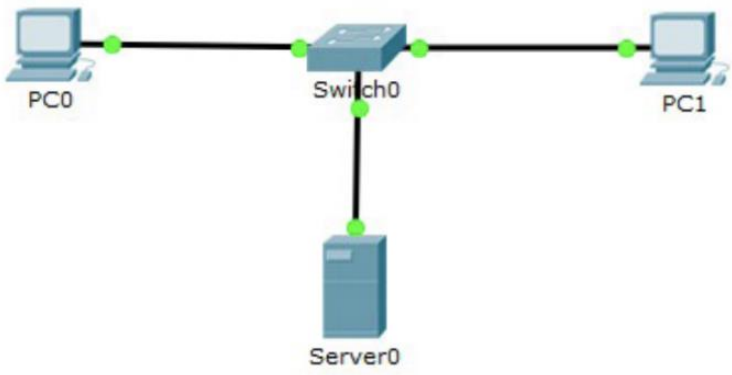


Рис. 11.1. Топологія мережі

3. Збережіть створену топологію.

4. Налаштуйте елементи мережі. Зарезервуйте для сервера – другу доступну IP-адресу, а стаціонарним комп'ютерам задайте адреси послідовно з третьої доступної. Мережева маска для всіх пристроїв – 255.255.255.0.

5. Щоб налаштувати PC0, відкрийте його властивості. На вкладці *Desktop* виберіть пункт *IP Config* і для режиму отримання IP-адреси *Static* в поле *IP Address* введіть третю доступну мережеву адресу – 192.168.1.3, в поле *Subnet*

Mask– маску мережі 255.255.255.0, а поле *Default Gateway* за замовчуванням можна залишити порожнім, тому що у нас немає виходу за межі нашої мережі. Другий стаціонарний комп'ютер налаштуйте аналогічно.

6. Щоб налаштувати сервер, відкрийте його властивості, перейдіть на вкладку *Config* і в підменю *INTERFACE* виберіть модуль *FastEthernet0*. У поле *IP Address* введіть другу зарезервовану IP-адресу мережі – 192.168.1.2, а в поле *Subnet Mask* – маску мережі 255.255.0. Після цього включіть цей модуль – *Port Status* встановіть в *On*.

7. Далі налаштуйте сервіс *EMAIL*. Перейдіть на вкладку *Services* та виберіть підменю *EMAIL*. Для ввімкнення перемикачі *SMTP Service* і *POP3 Service* встановіть в положення *On*. Призначте доменне ім'я поштовому серверу - в поле *Domain Name* введіть, наприклад, *mnau.edu.ua.* Натисніть кнопку *Set,* щоб зберегти ім'я домену. Далі створіть два облікові записи користувачів. Для цього потрібно в поле *User* ввести ім'я облікового запису, а в поле *Password* – *пароль.* Для додавання запису до бази даних, натисніть кнопку "+". Таким чином, створіть ще два записи: user1 з паролем user1 і user2 з паролем user2.

8. Налаштуйте поштові скриньки на ПК0 і ПК1. На вкладці *Desktop* виберіть елемент *Email.* З'явиться вікно для налаштування поштової скриньки. У полі *Your Name* вкажіть довільне ім'я поштової скриньки, яке зберігатиметься тільки на локальному ПК (наприклад, для PC0 – U1, а для PC2 – U2). В полі *Email Address* вкажіть повне ім'я поштової скриньки *email = і'мя облікового запису на сервері* + @ + *доменне і'мя сервера (*для PC0 це user1@*mnau*.edu.com, а для PC1 це user2@*mnau*.edu.com). В розділі *Server Information* вкажіть IP-адресу для серверів вхідної і вихідної пошти – в нашому випадку *Incoming Mail Server* и *Outgoing Mail Server* адреса буде однакова для обох ПК – 192.168.1.2. У розділі *Logon Information* вкажіть ім'я та пароль облікового запису, раніше записаного на сервері (для PC0 – user1 з паролем user1, а для PC1 – user2 з паролем user2). Щоб зберегти конфігурацію, натисніть кнопку *Save*.

9. Перевірте працездатність поштових скриньок. Наприклад, зайдіть на комп'ютер PC0 до розділу *Desktop / Email.* Відкриється вікно *Mail Browser.* Для відправки листа натисніть кнопку *Compose.* У полі *To* вкажіть e-mail адресу отримувача – user2@*mnau*.edu.com, в поле *Subject* введіть тему листа (наприклад, «тест»), а в нижнє поле – текст листа (наприклад, «Мій перший текст!!!»). Щоб надіслати повідомлення, натисніть кнопку *Send.* Після відправки листа в нижній частині вікна з'явиться запис про те, що повідомлення було відправлено.

Щоб прочитати отриманий лист, перейдіть до розділу *Desktop / Email* на комп'ютері PC1 та натисніть кнопку *Receive*. Відобразиться список усіх отриманих листів (див. Рис. 11.2). Відкрити лист можна подвійним натисканням

лівої кнопки миші.

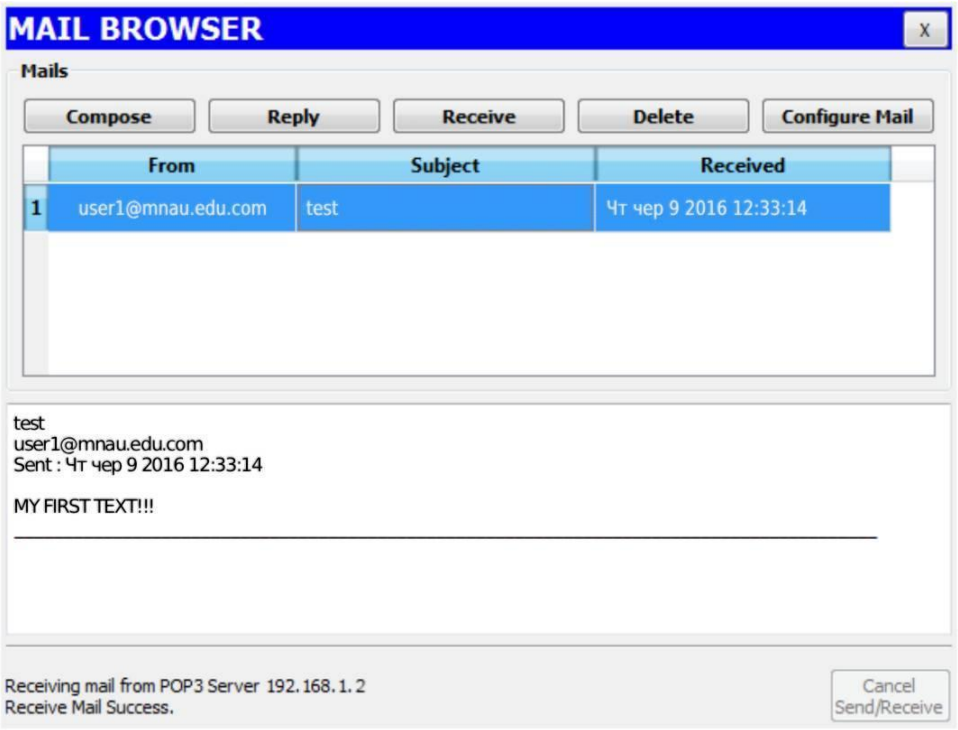


Рис. 11.2. Перелік отриманих повідомлень

Завдання для самостійної роботи

1. Додайте до робочого поля програми Packet Tracer два стаціонарні комп'ютери (PC0, PC1), два ноутбуки (Laptop0, Laptop1), два комутатори 2960-24TT (Switch0, Switch1), роутер Generic Router-PT-Empty (Router0) та два сервери Generic Server-PT (email_A, email_Б).

2. Додайте два Gigabit Ethernet-модуля PT-ROUTER-NM-1CGE до роутера для підключення мережі.

3. Об’єднайте всі пристрої за допомогою витої пари. Порти підключення роутера та комутаторів – GigabitEthernet, решти пристроїв з комутаторами – FastEthernet. Топологія мережевої моделі показана на рис. 11.3.

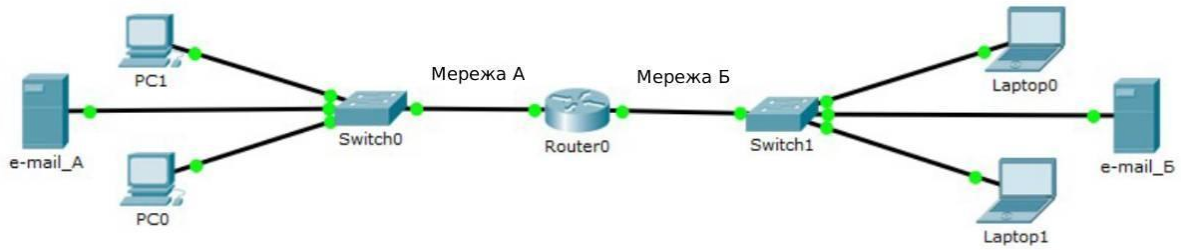


Рис. 11.3. Задання топологія мережі

4. Призначте статичні IP-адреси цільовим вузлам у мережах А та Б відповідно до зазначеного варіанту (табл. 11.1):

- призначте першу доступну адресу інтерфейсу роутера в мережах А і Б.
- призначте останні доступні адреси серверам у мережах А та

Б.

- призначте другу доступну адресу в мережі А.
- комп’ютеру PC1 призначте третю доступну адресу в мережі А.
- призначте другу доступну адресу в мережі В для Laptop0.
- призначте третю доступну адресу в мережі В для Laptop1.

Таблиця 11.1. Параметри завдання мережної адреси

№ вар.	Адреса мережі А	Маска мережі А	Адреса мережі Б	Маска мережі Б
1	14.67.11.128	255.255.255.192	51.18.41.160	255.255.255.224
2	14.67.12.128	255.255.255.224	51.18.42.160	255.255.255.240
3	14.67.13.128	255.255.255.128	51.18.43.160	255.255.255.248
4	14.67.14.128	255.255.255.192	51.18.44.160	255.255.255.224
5	14.67.15.128	255.255.255.224	51.18.45.160	255.255.255.240
6	14.67.16.128	255.255.255.128	51.18.46.160	255.255.255.248
7	14.67.17.128	255.255.255.192	51.18.47.160	255.255.255.224
8	14.67.18.128	255.255.255.224	51.18.48.160	255.255.255.240
9	14.67.19.128	255.255.255.128	51.18.49.160	255.255.255.248
10	14.67.20.128	255.255.255.192	51.18.50.160	255.255.255.224

5. Перевірте працездатність мережі – пропінгуйте з PC0 решту вузлів мережі.

6. Згідно з таблицею 11.2 створіть на серверах email_A та email_B поштові сервера з доменними іменами і додайте до них по два облікові записи. Для кожного запису придумайте свій пароль.

7. Налаштуйте поштові скриньки на всіх цільових вузлах відповідно до таблиці 11.2.

8. Перевірте відправку пошти:

- відправте тестові листи з PC0 на всі інші поштові скриньки;
- відправте тестові листи з Laptop0 на всі інші поштові скриньки.

9. Перевірте прийом листів на всіх пристроях.

10. У режимі моделювання надішліть тестовий електронний лист з PC1 на Laptop1. Відстежуйте рух пакетів за протоколами SMTP та POP3 під час надсилання і отримання листа.

Таблиця 11.2. Параметри завдання імені домену

№ вар.	Домен сервера email_А	Обліковий запис PC0	Обліковий запис PC1	Домен сервера email_Б	Обліковий запис Laptop0	Обліковий запис Laptop1
1	Albania.com	Tirana	Durres	Chad.net	Koumra	Mongo
2	Algeria.com	Algiers	Oran	Pakistan.net	Islamabad	Karachi
3	Chad.com	Bangor	Fada	Peru.net	Lima	Arequipa
4	Angola.com	Luanda	Huambo	Cyprus.net	Nicosia	paphos
5	Ecuador.com	Quito	Loja	Sudan.net	Khartoum	Omdurma
6	Iran.com	Ahar	Kilan	Taiwan.net	Kaohsiung	Taipei
7	India.com	Mumbai	Delhi	Fiji.net	Suva	Lami
8	Cameroon.com	Douala	Yaounde	Vietnam.net	Hanoi	Haiphong
9	Chile.com	Santiago	Arica	Yemen.net	Aden	Sana
10	Cuba.com	Havana	Holguin	Zimbabwe.net Harare		Bulaway

Питання для обговорення на занятті

1. Яку роль виконує електронна пошта у мережевій інфраструктурі?
2. Чим відрізняється SMTP від POP3 та IMAP?
3. Які стандартні порти використовують SMTP, POP3 та IMAP?
4. Як працює процес включення повідомлення в SMTP-пакет?
5. Чому важливо правильно налаштувати аутентифікацію на поштовому сервері?

6. Які ризики можуть виникнути при неправильному налаштуванні поштового сервера?

7. Чим відрізняється зберігання пошти у POP3 та IMAP?

8. Які обмеження мають поштові клієнти у Packet Tracer?

9. Як перевірити, що поштовий сервер правильно обробляє вихідні та вхідні повідомлення?

10. Чому безпека електронної пошти є важливою у корпоративному середовищі?

Тестові запитання

1. Який протокол відповідає за надсилання електронної пошти?

A. IMAP;

B. POP3;

C. SMTP;

D. FTP.

2. Який порт за замовчуванням використовує SMTP?

A. 80;

B. 25;

C. 53;

D. 143.

3. Який протокол призначений для отримання пошти з сервера?

A. DHCP;

B. IMAP;

C. SSH;

D. ARP.

4. Чим POP3 відрізняється від IMAP?

A. POP3 дозволяє працювати з поштою на сервері без завантаження;

B. POP3 зазвичай забирає листи з сервера на пристрій;

C. POP3 використовує порт 1100;

D. POP3 не потребує аутентифікації.

5. Який параметр необхідно вказати у налаштуваннях поштового клієнта?

A. MAC-адресу сервера;

B. IP-адресу SMTP і POP3/IMAP сервера;

C. DNS-імена всіх VLAN;

D. Тип комутатора.

6. Який тип серверів відповідає за зберігання поштових скриньок?
A. DNS-сервер;
B. Web-сервер;
C. SMTP/POP3/IMAP сервер;
D. FTP-сервер.

7. Яка команда у Packet Tracer дозволяє перевірити надсилання листа?
A. ping;
B. send;
C. mail test;
D. test message.

8. Що означає термін “аутентифікація SMTP”?
A. Дозвіл серверу змінювати пакети;
B. Процес підтвердження користувача перед відправкою пошти;
C. Перевірка MAC-адрес;
D. Створення резервної копії листів.

9. Яку функцію виконує поле “From” у листі?
A. Вказує IP-адресу відправника;
B. Визначає тему повідомлення;
C. Показує електронну адресу відправника;
D. Показує адресу SMTP-сервера.

10. Чому електронна пошта вважається важливою службою мережі?
A. Вона не потребує серверів;
B. Її безпечно використовувати без шифрування;
C. Вона забезпечує швидкий обмін інформацією між користувачами;
D. Її використовують лише у лабораторних роботах.

ПРАКТИЧНА РОБОТА №12
Налаштування веб-сервера (NGINX, Apache) на Proxmox

Мета роботи: сформувати практичні навички розгортання веб-сервера в середовищі віртуалізації Proxmox VE. Навчитися готувати серверне середовище, працювати з файловою структурою веб-сервера, вносити зміни у конфігураційні файли, керувати станом служби, переглядати журнали подій та діагностувати потенційні помилки.

Матеріали та ресурси: ПК із доступом до встановленого Proxmox VE (локально або через браузер), дистрибутив Linux (Ubuntu, Debian або CentOS) для розгортання віртуальної машини чи LXC-контейнера, базові HTML-файли для тестування роботи сервера та блокнот для фіксації результатів.

Завдання для роботи під час заняття

1. Створення віртуального середовища в Proxmox

Створіть нову віртуальну машину або LXC-контейнер для подальшої роботи веб-сервера.

1. Виберіть шаблон або ISO-образ Linux-дистрибутива.
2. Встановіть параметри: кількість ядер CPU, обсяг оперативної пам’яті, розмір диску, тип мережевого інтерфейсу.
3. Налаштуйте мережу (DHCP або статичну IP-адресу).

2. Підготовка операційної системи

1. Оновіть пакунки (apt update && apt upgrade).
2. Встановіть базові утиліти (nano, curl, net-tools).
3. Перевірте коректність підключення до інтернету.
4. Дізнайтеся IP-адресу сервера (ip a).

3. Встановлення веб-сервера (NGINX або Apache)

Виберіть один із серверів або встановіть обидва для порівняння.

Варіант 1: установка **NGINX**:

```
sudo apt install nginx -y
```

Варіант 2: установка **Apache**:

```
sudo apt install apache2 -y
```

Після встановлення:

- перевірте статус служби (systemctl status nginx або systemctl status apache2),
- відкрийте веб-сервер через браузер, використавши IP-адресу віртуальної машини,
- поясніть, як працює дефолтна сторінка веб-сервера.

4. Налаштування власної веб-сторінки

Створіть власну просту HTML-сторінку (файл *index.html*) та розмістіть її у каталозі веб-сервера.

NGINX: */var/www/html/*

Apache: */var/www/html/*

Завдання 5. Базове конфігурування веб-сервера

Виконайте одне із базових налаштувань, наприклад:

- змінити порт прослуховування веб-сервера;
- налаштувати новий віртуальний хост (server block / VirtualHost);
- змінити кореневу директорію сайту;
- увімкнути логування доступів і помилок.

Опишіть який файл конфігурації змінювався, що саме було змінено, як перезапустити сервер (systemctl restart nginx або apache2), як вплинули зміни на доступність сайту.

Завдання 6. Діагностика та тестування

Протестуйте роботу сервера:

- перевірте відкриті порти (ss -tulnp),
- перегляньте журнали (journalctl -u nginx або apache2),
- перевірте відповідь сервера командою curl.

Завдання для самостійної роботи

Створіть тестове серверне середовище на локальній віртуальній машині або в контейнері (наприклад, під керуванням Ubuntu або Debian) та встановіть один із веб-серверів — NGINX або Apache. Після встановлення підготуйте власну HTML-сторінку та розмістіть її у стандартному каталозі веб-сервера, замінивши дефолтну сторінку. Далі створіть окремий віртуальний хост (VirtualHost у Apache або server block у NGINX), який працюватиме з іншою кореневою директорією сайту та відповідатиме на запити для вигаданого доменного імені, наприклад mytest.local. Переконайтеся, що налаштування працюють: додайте запис у локальний hosts-файл своєї системи та відкрийте сайт у браузері. Завершіть роботу коротким висновком про те, на які параметри конфігурації потрібно звертати особливу увагу під час роботи з веб-сервером та які труднощі виникли під час налаштування.

Питання для обговорення на занятті

1. Які переваги дає розгортання веб-сервера у віртуальному середовищі Proxmox порівняно з фізичним сервером?
2. У чому полягає різниця між встановленням веб-сервера у VM та LXC-контейнері?
3. Які основні відмінності між NGINX та Apache з точки зору архітектури та продуктивності?

4. Чому важливо оновлювати операційну систему перед встановленням веб-сервера?

5. Які конфігураційні файли є ключовими для налаштування NGINX та Apache?

6. Що таке віртуальні хости (server blocks) і для чого вони використовуються?

7. Як зміна порту прослуховування може вплинути на доступність сайту?

8. Які типові помилки виникають при налаштуванні веб-сервера та як їх діагностувати?

9. Чому важливо правильно налаштувати права доступу до веб-каталогів?

10. Як можна поєднати роботу веб-сервера з іншими сервісами у Proxmox (наприклад, базами даних)?

Тестові запитання

1. Який пакет встановлює NGINX у Debian/Ubuntu?

A. nginx;

B. install-nginx;

C. httpd;

D. webserver-ng.

2. Який веб-сервер за замовчуванням використовує конфігураційний файл /etc/apache2/apache2.conf?

A. NGINX;

B. Apache;

C. Lighttpd;

D. Tomcat.

3. Де знаходиться коренева директорія за замовчуванням для NGINX на Ubuntu?

A. /srv/www;

B. /var/www/html;

C. /etc/nginx/www;

D. /var/nginx/www.

4. Яка команда перевіряє статус NGINX?

A. service nginx status;

B. nginx status;

C. sysctl nginx;

D. nginx-check.

5. Який порт слухає веб-сервер за замовчуванням?
A. 80;
B. 21;
C. 110;
D. 53.

6. Яка команда перезапускає Apache?
A. apachectl reload;
B. systemctl restart apache2;
C. reload apache;
D. sudo fix-apache.

7. Що таке server block в NGINX?
A. Модуль шифрування;
B. Віртуальний хост;
C. Тип кешування;
D. Засіб моніторингу.

8. Який файл містить основну конфігурацію для NGINX?
A. /etc/nginx/main.cnf;
B. /etc/nginx/nginx.conf;
C. /etc/nginx/index.conf;
D. /etc/nginx/server.conf.

9. Який інструмент дозволяє перевірити відповідь веб-сервера з CLI?
A. traceroute;
B. curl;
C. nslookup;
D. dig.

10. Який з варіантів НЕ є перевагою використання Proxmox для веб-сервера?
A. Можливість швидкого створення резервних копій;
B. Гнучке масштабування ресурсів;
C. Відсутність потреби у конфігурації мережі;
D. Можливість запускати кілька серверів на одній фізичній машині.

ПРАКТИЧНА РОБОТА №13
Налаштування Zabbix для моніторингу Proxmox

Мета роботи: сформувати уміння встановлювати та налаштовувати систему моніторингу Zabbix для отримання даних про стан інфраструктури на платформі Proxmox VE, включаючи збір метрик з вузла віртуалізації, віртуальних машин та контейнерів. Навчитися встановлювати Zabbix Server та Zabbix Agent, виконувати базову конфігурацію моніторингу, додавати Proxmox-хости в систему, застосовувати шаблони, аналізувати отримані дані, працювати з тригерами та графіками, а також розуміти принципи виявлення проблем і попереджень у серверній інфраструктурі.

Матеріали та ресурси: ПК із доступом до встановленого Proxmox VE, сервер або віртуальна машина з Linux для розгортання Zabbix Server, доступ до консольних утиліт Linux (SSH, Nano, systemctl), документація Zabbix та офіційні шаблони для моніторингу Proxmox, мережевий доступ між Zabbix і вузлом Proxmox, а також браузер для доступу до веб-інтерфейсу Zabbix.

Завдання для роботи під час заняття

1. Підготовка середовища для встановлення Zabbix Server

Створіть окрему віртуальну машину на Proxmox (або використайте наявну), яка буде виконувати роль Zabbix Server.

1. Встановіть Linux-дистрибутив (наприклад, Debian або Ubuntu LTS).
2. Оновіть систему (apt update && apt upgrade).
3. Встановіть базові інструменти (curl, wget, nano, net-tools).
4. Перевірте мережеву доступність та IP-адресу сервера.

2. Встановлення Zabbix Server та веб-інтерфейсу

Встановіть Zabbix Server і веб-інтерфейс за офіційною інструкцією. Основні кроки:

- додайте офіційний Zabbix репозиторій;
- встановіть пакети zabbix-server, zabbix-frontend-php, zabbix-sql-schema, zabbix-agent;
- налаштуйте базу даних (MariaDB або PostgreSQL);
- виконайте імпорт схеми;
- налаштуйте PHP для роботи UI-застосунку;
- запустіть служби Zabbix.

3. Встановлення Zabbix Agent на хост Proxmox

Встановіть Zabbix Agent безпосередньо на Proxmox-ноду.

1. Додайте репозиторій Zabbix у систему Proxmox.
2. Встановіть пакет *zabbix-agent*.

3. Відкрийте та відредагуйте конфігураційний файл */etc/zabbix/zabbix_agentd.conf*.

4. Вкажіть адресу Zabbix Server (*Server*= та *ServerActive*=).

5. Задайте ім’я хоста (HostName=proxmox-node).

6. Перезапустіть агента (systemctl restart zabbix-agent).

4. Додавання вузла Proxmox у Zabbix та застосування шаблонів

Перейдіть у веб-інтерфейс Zabbix і виконайте наступне:

- додай те нов ий хост (Host → Create new h ost);
- прив’яжіть до групи (наприклад, “Proxmox Nodes”);
- вкажіть IP-адреси агента;
- виберіть шаблон моніторингу “Template Proxmox VE” або сторонній готовий шаблон;
- збережіть конфігурації.

5. Перевірка отримання даних, робота з графіками та тригерами

Перейдіть на вкладку Latest Data для перевірки, що Proxmox-нода успішно відправляє метрики:

- знайдіть CPU load, RAM usage, disk I/O;
- відкрийте графіки та перевірте, чи спрацювали будь-які тригери (Warning, High Load тощо).

6. Діагностика та робота з журналами

Виконайте базову діагностику:

- перевірте статус агента Zabbix на Proxmox (*systemctl status zabbix-agent*);
- перегляньте журнал */var/log/zabbix/zabbix_agentd.log*;
- перевірте наявність мережевої доступності між вузлами (*ping, telnet <zabbix_ip> 10050*).

Опишіть найчастіші помилки під час моніторингу.

Завдання для самостійної роботи

Створіть тестове середовище для моніторингу, використовуючи наявний сервер Proxmox та окрему віртуальну машину з Linux, на якій потрібно встановити Zabbix Server. Після встановлення сервера налаштуйте веб-інтерфейс Zabbix та створіть у ньому нового хоста, що відповідатиме вашому вузлу Proxmox. На самому вузлі встановіть Zabbix Agent, пропишіть у конфігураційному файлі адресу сервера та унікальне ім’я хоста, перезапустіть службу агента і переконайтеся, що з’єднання встановлено. Потім застосуйте до хоста шаблон моніторингу Proxmox, перегляньте перші отримані метрики у розділі «Latest Data» та відкрийте кілька графіків, щоб проаналізувати завантаження процесора та використання пам’яті. Завершіть роботу коротким висновком про те, які параметри моніторингу є найбільш критичними для

контролю стану Proxmox і з якими труднощами ви зіткнулися під час налаштування Zabbix.

Питання для обговорення на занятті

1. Чому моніторинг є обов'язковим елементом адміністрування інфраструктури Proxmox?
2. Які компоненти складають систему Zabbix і яку роль виконує кожен з них?
3. Чим відрізняється Zabbix Server від Zabbix Agent?
4. Які переваги дає встановлення агента безпосередньо на вузол Proxmox?
5. Чому важливо правильно налаштувати параметр HostName у конфігурації агента?
6. Які метрики є найважливішими для моніторингу вузла Proxmox і чому?
7. Що дають шаблони моніторингу та як вони спрощують роботу адміністратора?
8. Які типові помилки виникають при додаванні нового Proxmox-хоста в Zabbix?
9. Для чого потрібні тригери і як вони впливають на сповіщення про проблеми?
10. Як моніторинг Proxmox може допомогти в оптимізації ресурсів віртуальних машин?

Тестові запитання

1. Який порт за замовчуванням використовує Zabbix Agent?

A. 80;
B. 22;
C. 10050;
D. 443.

2. Яка служба відповідає за збір і передачу метрик з Proxmox у Zabbix?

A. Zabbix Frontend;
B. Zabbix Sender;
C. Zabbix Proxy;
D. Zabbix Agent.

3. У якому файлі встановлюються параметри агента Zabbix?

A. /etc/zabbix/zabbix.conf;
B. /etc/zabbix/zabbix_agentd.conf;
C. /etc/proxmox/agent.conf;

D. /etc/agent/zbx.conf.

4. Який компонент забезпечує веб-інтерфейс Zabbix?
A. Zabbix UI;
B. Zabbix Proxy;
C. Zabbix Dashboard;
D. Zabbix Frontend.

5. Який тип Zabbix-елемента відповідає за графічне відображення метрик?
A. Trigger;
B. Graph;
C. Item;
D. Action.

6. Що необхідно зробити після внесення змін у конфігураційний файл агента?
A. Встановити оновлення Proxmox;
B. Очистити кеш веб-браузера;
C. Перезапустити службу zabbix-agent;
D. Перевстановити Zabbix Server.

7. Який елемент Zabbix використовується для автоматичного реагування на перевищення порогу?
A. Action;
B. Template;
C. Widget;
D. Map.

8. Яка умова необхідна для появи даних від агента у Zabbix?
A. Однакові MAC-адреси клієнта і сервера;
B. Відповідність HostName між агентом і хостом у Zabbix;
C. Наявність DHCP-сервера;
D. Відкритий порт 3000.

9. Який шаблон найчастіше застосовують для моніторингу Proxmox?
A. Template OS Windows;
B. Template Linux by SNMP;
C. Template Proxmox VE;
D. Template Database MySQL.

10. Яка команда дозволяє перевірити роботу агента на стороні Proxmox?
A. systemctl status zabbix-agent;
B. zabbix agent check;
C. proxmox-monitor --agent;
D. agentctl status.

ПРАКТИЧНА РОБОТА №14
Використання Docker у Proxmox для розгортання

Мета роботи: сформувати практичні навички розгортання контейнеризованих сервісів у середовищі Proxmox за допомогою Docker. Навчитися створювати віртуальну машину для роботи Docker, інсталювати Docker Engine, запускати окремі контейнери, працювати з Docker Hub, використовувати команди керування контейнерами, а також створювати власні docker-compose конфігурації для запуску багатокомпонентних сервісів.

Матеріали та ресурси: ПК, встановлений Proxmox VE з можливістю створення віртуальних машин або контейнерів, дистрибутив Linux (рекомендовано — Debian або Ubuntu), доступ до інтернету для завантаження Docker-пакетів і образів, базові інструкції з Docker Engine і Docker Compose, доступ до Docker Hub, термінальні інструменти (SSH, bash).

Завдання для роботи під час заняття

1. Підготовка середовища для запуску Docker

Створіть окрему віртуальну машину в Proxmox (або LXC-контейнер з увімкненою підтримкою Docker) для встановлення Docker:

- створіть VM із 2 ГБ RAM, 2 vCPU та 10–20 ГБ диску;
- встановіть Linux (Ubuntu/Debian);
- виконайте оновлення системи (apt update && apt upgrade);
- встановіть додаткові утиліти (curl, vim, net-tools).

2. Встановлення Docker Engine

Встановлює Docker за офіційною інструкцією Docker:

- додайте репозиторій Docker;
- встановіть пакети docker-ce, docker-ce-cli, containerd.io;
- перевірте роботу Docker (docker --version, docker run hello-world).

3. Запуск першого контейнера

Завантажте та запустіть простий контейнер. Наприклад:

```
docker run -d -p 8080:80 nginx
```

Після запуску необхідно перевірте список контейнерів (docker ps), протестуйте доступ до сервера за IP та портом 8080.

4. Робота з Docker Hub і образами

Виконайте пошук і завантажте новий образ:

```
docker search mysql
docker pull mysql
```

5. Створення та управління контейнерами

1. Запустіть контейнер з MySQL,

2. Створіть змінні середовища (root-пароль),
3. Зупиніть контейнер (*docker stop*),
4. Видаліть контейнер (*docker rm*).

6. Створення docker-compose.yml для багатокомпонентного сервісу

Створіть новий файл *docker-compose.yml*, який запускає два сервіси: веб-сервер (наприклад, NGINX), базу даних (наприклад, MySQL або MariaDB).

1. Опишіть сервіс, мережу, томи даних;
2. Запустіть проєкт (*docker compose up -d*);
3. Перевірте роботу сервісів;
4. Поясніть, як *compose* спрощує керування складною структурою контейнерів.

7. Діагностика контейнерів

1. Перегляньте логи (*docker logs <container>*),
2. Перевірте використання ресурсів (*docker stats*),
3. Пошукайте типові помилки (конфігурація, порти, залежності),
4. Зніміть резервні копії томів або експортуйте образи.

Завдання для самостійної роботи

Створіть у Proxmox окрему віртуальну машину з Linux-дистрибутивом (наприклад, Ubuntu Server) та встановіть на неї Docker Engine, дотримуючись офіційних інструкцій. Після встановлення запустіть тестовий контейнер NGINX з пробросом порту та переконайтеся, що веб-сервер доступний із робочої станції через браузер. Потім завантажте другий образ, наприклад MySQL або Redis, та створіть контейнер із необхідними змінними середовища. Створіть простий файл docker-compose.yml, який запускає обидва сервіси одночасно, об’єднані у спільну мережу Docker. Запустіть проект за допомогою docker compose up -d і перевірте, що обидва контейнери працюють. Завершіть роботу коротким висновком про те, які переваги дає Docker у порівнянні зі звичайними програмами, і які труднощі виникли у процесі роботи з контейнерами в середовищі Proxmox.

Питання для обговорення на занятті

1. У чому полягає різниця між віртуалізацією Proxmox та контейнеризацією Docker?
2. Чому Docker зазвичай рекомендують запускати у віртуальній машині Proxmox, а не в LXC-контейнері?
3. Які переваги використання Docker для розгортання сервісів у порівнянні з традиційним встановленням програм?
4. Що таке Docker-образ і як він пов’язаний з контейнером?
5. Чому Docker Hub відіграє важливу роль у роботі з Docker?

6. Як працює проброс портів (-p) і чому він важливий при розгортанні сервісів у Proxmox?

7. Які плюси й мінуси має використання docker-compose у порівнянні з ручним керуванням контейнерами?

8. Як Docker допомагає оптимізувати використання ресурсів у Proxmox-кластері?

9. Чому важливо правильно працювати з томами (volumes) у Docker, особливо для баз даних?

10. Які типові проблеми можуть виникнути при розгортанні контейнерів і як їх діагностувати?

Тестові запитання

1. Яка команда використовується для запуску контейнера NGINX у Docker?

A. docker run nginx start;
B. run docker nginx;
C. docker run -d nginx;
D. docker start nginx.

2. Де зазвичай зберігаються локальні Docker-образи?

A. /etc/docker/images;
B. На Docker Hub;
C. /var/lib/docker;
D. /usr/docker/storage.

3. Яка команда показує список запущених контейнерів?

A. docker show;
B. docker ps;
C. docker list;
D. docker active.

4. Яка команда завантажує образ із Docker Hub?

A. docker load image;
B. docker get;
C. docker pull;
D. docker fetch hub.

5. Для чого використовується команда docker logs <container>?

A. Для запуску контейнера;
B. Для перегляду журналу подій контейнера;

C. Для видалення контейнера;
D. Для завантаження образу.

6. Який файл використовується для опису багатоконтейнерних сервісів?
A. dockerfile.yml;
B. docker-config.xml;
C. docker-compose.yml;
D. container-setup.json.

7. На якому рівні працює Docker у порівнянні з VM у Proxmox?
A. Docker віртуалізує обладнання;
B. Docker працює на рівні ядра/операційної системи;
C. Docker працює на рівні BIOS;
D. Docker працює на рівні гіпервізора.

8. Яка команда зупиняє працюючий контейнер?
A. docker stop;
B. docker pause;
C. docker shutdown;
D. docker off.

9. Який сервіс обов’язково має бути встановлений для роботи Docker Engine?
A. SSH;
B. Containerd;
C. Cron;
D. Proxmox Tools.

10. Для чого використовуються volumes (томи) у Docker?
A. Для прискорення мережевих запитів;
B. Для зберігання даних контейнера поза межами образу;
C. Для створення резервних копій у Proxmox;
D. Для запуску контейнерів без інтернету.

ПРАКТИЧНА РОБОТА №15
Розгортання віртуальної машини в хмарі (AWS, Azure, Google Cloud)

Мета роботи: сформувати уміння створювати та налаштовувати віртуальні машини у провідних хмарних платформах. Навчитися орієнтуватися в інтерфейсі хмарних сервісів, створювати екземпляри віртуальних машин, працювати з ключами доступу, правилами брандмауера, типами інстансів, а також усвідомити відмінності між платформами та моделі оплати за використання ресурсів.

Матеріали та ресурси: ПК з доступом до інтернету, акаунти в одній із хмарних платформ (AWS Free Tier, Google Cloud Free Tier), доступ до документації відповідних сервісів, SSH-клієнт або термінал для підключення до віртуальної машини.

Завдання для роботи під час заняття

1. Створення акаунта та підготовка хмарного середовища

Оберіть одну з хмарних платформ: AWS EC2 або Google Compute Engine:

1. увійдіть в акаунт або створіть його;
2. перейдіть в консоль управління;
3. знайдіть розділ керування віртуальними машинами;
4. ознайомтеся з доступними регіонами та зонами доступності.

2. Створення нової віртуальної машини

1. Виберіть образ операційної системи (AMI/Image): Ubuntu, Debian, Windows Server тощо.
2. Виберіть тип інстанса (t2.micro / B1s / e2-micro) залежно від платформи та Free Tier.
3. Виконайте конфігурацію диску (SSD/HDD, розмір).
4. Налаштуйте мережу:
    - VPC/Virtual Network,
    - Subnet,
    - Auto-assign public IP.

3. Налаштування доступу та безпеки

1. Створіть або завантажте SSH-ключі для Linux.
2. Задайте пароль для Windows.
3. Додайте правила брандмауера (Security Group / Firewall Rule):
    - дозвольте SSH (порт 22),
    - або RDP (порт 3389) для Windows,
    - дозвольте HTTP/HTTPS, якщо потрібно.

4. Запуск віртуальної машини та підключення

Запустіть VM та підключіться до неї через SSH-клієнт (Linux/Unix/Windows PowerShell) або через RDP-клієнт для Windows.

Після підключення необхідно перевірити систему, виконати оновлення (*sudo apt update && sudo apt upgrade*), встановити базові утиліти.

5. Розгортання простого сервісу на VM

1. Встановіть тестовий веб-сервер, наприклад NGINX або Apache:

```
sudo apt install nginx -y
```

2. Перевірте доступність сервера через зовнішню IP-адресу.

3. Перевірте, що сторінка завантажується у браузері.

6. Зміна параметрів VM та тестування масштабування

1. У консолі хмарної платформи тимчасово змініть тип віртуальної машини (наприклад, збільшіть CPU/RAM);

2. Перезапустіть інстанс;

3. Перевірте, як зміни вплинули на роботу сервісу.

Завдання для самостійної роботи

Створіть у вибраній хмарній платформі (AWS або Google Cloud) тестову віртуальну машину, використовуючи безкоштовний тариф або навчальний доступ. Виберіть Linux-дистрибутив (наприклад, Ubuntu) та налаштуйте мінімальні параметри інстанса. Після запуску віртуальної машини створіть SSH-ключ або використайте наявний, підключіться до сервера через термінал та виконайте оновлення системи. Далі встановіть простий веб-сервер, наприклад NGINX, і перевірте його доступність через браузер за допомогою зовнішньої IP-адреси інстанса. За потреби відкрийте відповідні порти у Security Group або Firewall Rules. Завершіть роботу коротким висновком про те, які кроки були найбільш критичними для успішного розгортання VM, які налаштування безпеки стали необхідними та як хмарна інфраструктура спрощує розгортання сервісів у порівнянні з локальними рішеннями.

Питання для обговорення на занятті

1. Чим відрізняється віртуалізація у хмарі від локальної віртуалізації на фізичному сервері?

2. Які ключові відмінності між платформами AWS, Azure та Google Cloud з точки зору розгортання віртуальних машин?

3. Що таке регіони та зони доступності, і чому важливо правильно їх обирати?

4. Як вибір типу інстанса (t2.micro, B1s, e2-micro тощо) впливає на продуктивність та вартість?

5. Які ризики можуть виникнути при неправильному налаштуванні Security Group або Firewall Rule?

6. Чим SSH-доступ відрізняється від RDP та коли краще використовувати кожен з них?

7. Чому важливо виконувати оновлення операційної системи після першого запуску віртуальної машини?

8. Які кроки потрібні для розгортання простого сервісу (наприклад, веб-сервера) на хмарній VM?

9. Як працює масштабування ресурсів (CPU, RAM, диск) у хмарних інстансах і чому це зручно?

10. Чому важливо видаляти або вимикати невикористовувані ресурси в хмарі?

Тестові запитання

1. Яка служба відповідає за віртуальні машини в AWS?

A. EC2;

B. S3;

C. RDS;

D. CloudFront.

2. У якій службі Azure створюють віртуальні машини?

A. Azure Functions;

B. Azure VM;

C. Azure Blob;

D. Azure Active Directory.

3. Яка хмарна служба відповідає за VM у Google Cloud?

A. GKE;

B. Compute Engine;

C. App Engine;

D. Cloud Run.

4. Який протокол використовується для віддаленого доступу до Linux-серверів?

A. FTP;

B. SSH;

C. RDP;

D. HTTP.

5. Який порт необхідно відкрити для RDP-доступу до Windows-сервера?

A. 22;

B. 80;

C. 3389;
D. 5432.

6. Який компонент відповідає за контроль доступу до віртуальної машини в AWS?
A. Storage Class;
B. Availability Zone;
C. Security Group;
D. IAM Group.

7. Який інструмент необхідний для підключення до Linux-VM через SSH?
A. Веб-браузер;
B. Текстовий редактор;
C. Термінал або SSH-клієнт;
D. SQL-клієнт.

8. Що таке AMI в AWS?
A. Тип віртуальної мережі;
B. Образ операційної системи;
C. Вид сховища;
D. Сервіс для керування контейнерами.

9. Яка оплачувальна модель найчастіше використовується для VM у хмарі?
A. Pay-as-you-Go;
B. Monthly Unlimited;
C. Flat Rate VM;
D. Lifetime Hosting.

10. Який компонент найчастіше визначає публічну IP-адресу в хмарних VM?
A. Virtual Disk;
B. Subnet;
C. Key Pair;
D. Network Interface.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Основна

1. Адміністрування комп'ютерних систем та мереж : методичні рекомендації для практичних занять та самостійної роботи здобувачів першого (бакалаврського) рівня вищої освіти ОПП «Комп'ютерні науки» спеціальності 122 «Комп'ютерні науки» денної форми здобуття вищої освіти / уклад. : С. І. Тищенко, О. Ю. Пархоменко, Р. С. Мірошник, І. І. Хилько. Миколаїв : МНАУ, 2024. 77 с. URL: https://dspace.mnau.edu.ua/jspui/handle/123456789/19244
2. Буров Є. В., Митник М. М. Комп'ютерні мережі : навчальний посібник. Т. 1. Львів : Магнолія 2006, 2026. 340 с.
3. Буров Є. В., Митник М. М. Комп'ютерні мережі : навчальний посібник. Т. 2. Львів : Магнолія 2006, 2026. 400 с.
4. Комп'ютерні мережі. Частина 1. Моделювання комп'ютерних мереж : лабораторний практикум / уклад.: О. С. Яценко, О. І. Яценко. Житомир : Вид-во ЖДУ ім. І. Франка, 2022. 76 с. URL : http://eprints.zu.edu.ua/33991/1/km.pdf
5. Комп'ютерні мережі: контроль та прогнозування перевантажень :навчальний посібник / О. М. Ткаченко та ін. Київ : ДУТ, 2021. 77 с.URL : https://duikt.edu.ua/uploads/l_2227_38365572.pdf
6. Комплексна безпека інформаційних мережевих систем: навчальний посібник / уклад.: А. Г. Микитишин, М. М. Митник, О. С. Голотенко, В. В. Карташов. Тернопіль : ФОП Паляниця В.А., 2023. 324 с.
7. Коробейнікова Т. І., Захарченко С. М. Комп'ютерні мережі : навчальний посібник. Львів : Львівська політехніка, 2025. 228 с.
8. Матвій О. В., Мельник В. С., Черевко І. М. Основи комп'ютерних мереж : навчальний посібник. Чернівці : Чернівецький національний університет ім. Юрія Федьковича, 2024. 158 с.
9. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі : навчальний посібник. Кн. 1. Львів : Магнолія 2006, 2025. 256 с.
10. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі : навчальний посібник. Кн. 2. Львів : Магнолія 2006, 2025. 328 с.
11. Проектування бездротових комп'ютерних мереж: навч. посібник / А. В. Лемешко та ін. Київ : ДУТ, 2021. 147 с. URL : https://duikt.edu.ua/uploads/l_2224_69488065.pdf

12. Хомуляк М. О. Адміністрування комп'ютерних систем і мереж : навч. посіб. Львів : "Магнолія 2006", 2024. 153 с.

Додаткова

1. Блозва А. І., Матус Ю. В., Касаткін Д. Ю. Комп’ютерні мережі. Том 1 : підручник. Київ : Компрінт, 2019. 483 с. URL : https://nubip.edu.ua/sites/default/files/u34/pidruchnik_tom.1_-_kompyuterni_merezhi.pdf
2. Жураковський Б. Ю., Зенів І. О. Комп’ютерні мережі. Частина 1 : навч. посіб. / КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/c4ecfaa7-73d5-498c-a63a-513137ee0aba/content
3. Технології забезпечення безпеки мережевої інфраструктури : підручник / В. Л. Бурячок та ін. Київ : КУБГ, 2019. 218 с. URL : https://elibrary.kubg.edu.ua/id/eprint/27191/1/VL_Buriachok_TZBMI.pdf

Навчальне видання

Адміністрування комп'ютерних систем та мереж

Методичні рекомендації

Укладачі: **Ємельянов** Святослав Ігорович
Тищенко Світлана Іванівна
Пархоменко Олександр Юрійович
Жебко Олександр Олегович
Богатєнкова Олександра Євгенівна

Формат 60х84 1/16. Ум. друк. арк. 9,00.
Наклад 50 прим. Зам. № _____

Надруковано у видавничому відділі
Миколаївського національного аграрного університету
54020, м. Миколаїв, вул. Георгія Гонгадзе, 9

Свідоцтво суб'єкта видавничої справи
ДК № 4490 від 20.02.2013 р.