ЗАТВЕРДЖЕНО
Науково-методичною радою
Державного університету
«Житомирська політехніка»
протокол від 19 травня 2026 р.
№ 4

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
для проведення лабораторних занять
з навчальної дисципліни
«Основи мережевих інформаційних технологій, телемедицина»
Частина 1. Основи мережевих ІТ

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності G22 «Біомедична інженерія»
освітньо-професійна програма «Біомедична інженерія»
факультет інформаційно-комп’ютерних технологій
кафедра комп’ютерних технологій у медицині та телекомунікаціях

Рекомендовано на засіданні кафедри комп’ютерних технологій у медицині та телекомунікаціях
8 квітня 2026 р., протокол № 3

Розробник: старший викладач кафедри комп’ютерних технологій у медицині та телекомунікаціях МОРОЗОВ Дмитро
к.т.н., доцент кафедри комп’ютерних технологій у медицині та телекомунікаціях КОРЕНІВСЬКА Оксана,

Житомир
2026

ЗМІСТ

ВСТУП..... 3

Лабораторна робота №1. IP-адресація в сучасних мережах..... 4

Лабораторна робота №2. Базове налаштування мережевого обладнання Cisco (IOS CLI)..... 14

Лабораторна робота №3. Побудова локальної мережі. Протоколи канального рівня..... 27

Лабораторна робота №4. Налаштування статичної маршрутизації на обладнанні Cisco. 38

Лабораторна робота №5. Налаштування протоколу динамічної маршрутизації OSPF..... 51

Лабораторна робота №6. DHCP та DNS у мережі медичного закладу..... 65

Лабораторна робота №7. VLAN та міжмережева комунікація (Inter-VLAN Routing)..... 76

Лабораторна робота №8. NAT, списки контролю доступу (ACL) та основи мережевої безпеки..... 87

ВСТУП

Стрімкий розвиток ІКТ докорінно змінює сучасну медицину. Електронні медичні картки, системи підтримки клінічних рішень, медичні інформаційні системи, системи архівування та передачі зображень, дистанційний моніторинг пацієнтів — все це неможливе без надійної мережевої інфраструктури. Мережа стала таким самим критично важливим ресурсом медичного закладу, як електропостачання чи водопостачання.

Особливе місце серед напрямів цифровізації медицини посідає телемедицина — галузь, що використовує телекомунікаційні технології для надання медичної допомоги на відстані. Телеконсультації, дистанційна діагностика, передача медичних зображень між закладами, моніторинг хронічних хворих удома, системи екстреного оповіщення — реалії сучасної практики.

Для майбутнього інженера з біомедичної інженерії розуміння принципів роботи комп'ютерних мереж є фундаментальною компетентністю. Мережевий або біомедичний інженер відповідає за проектування і підтримку інфраструктури, по якій передаються дані ЕКГ, знімки МРТ, сигнали моніторів пацієнта та відеопотоки телемедичних консультацій. Помилка в налаштуванні мережі може призвести не лише до затримки даних, а й до реальної загрози безпеці пацієнта.

Цей посібник є першою частиною курсу з дисципліни «Основи мережевих інформаційних технологій, телемедицина» і охоплює базові мережеві технології. Друга частина містить 10 лабораторних робіт присвячених телемедицині. Засвоєння першої частини є необхідною передумовою для другої.

Перша частина містить вісім лабораторних робіт, що послідовно охоплюють такі теми:

– ЛР №1. IP-адресація та знайомство з Cisco Packet Tracer. IPv4, маски, CIDR, розрахунок підмереж, перші кроки в CPT.
– ЛР №2. Базове налаштування Cisco IOS CLI. Режими IOS, паролі, облікові записи, рівні привілеїв, команди show.
– ЛР №3. Побудова LAN. Протоколи канального рівня. MAC-адреси, таблиця комутатора, широкомовні домени, STP.
– ЛР №4. Статична маршрутизація. Таблиця маршрутизації, ip route, default route, плаваючий та підсумовуючий маршрути.
– ЛР №5. Динамічна маршрутизація OSPF. Link-state, алгоритм Дейкстри, LSDB, метрика cost, DR/BDR, single-area.
– ЛР №6. DHCP та DNS у мережі медичного закладу. DORA, DHCP-пули, Relay Agent, DNS-записи, nslookup.
– ЛР №7. VLAN та Inter-VLAN Routing. Сегментація мережі лікарні, 802.1Q, trunk, VTP, Router-on-a-Stick.
– ЛР №8. NAT, ACL та основи мережевої безпеки. PAT, Static NAT, стандартні та розширені ACL для захисту медичних даних.

Кожна лабораторна робота виконується у Cisco Packet Tracer і включає детальні пояснення команд Cisco IOS, приклади реального виводу та окремий розділ з діагностики мережевих проблем.

Лабораторна робота №1.

IP-адресація в сучасних мережах.

Мета роботи: Засвоїти основи IP-адресації. Навчитися самостійно розраховувати параметри підмереж. Отримати початкові навички роботи із симулятором Cisco Packet Tracer.

ТЕОРЕТИЧНІ ВІДОМОСТІ:

Що таке IP-адреса і навіщо вона потрібна?

Мережа – це сукупність пристроїв, що обмінюються даними. Щоб дані потрапили саме до потрібного пристрою, кожен вузол мережі повинен мати унікальну адресу. Протокол IP (Internet Protocol) є основою сучасних мереж і визначає правила адресації та маршрутизації пакетів даних.

IPv4-адреса – це 32-бітне двійкове число, що записується у вигляді чотирьох десяткових чисел (октетів), розділених крапками. Кожен октет може приймати значення від 0 до 255.

Октет 1	Октет 2	Октет 3	Октет 4
192	168	10	5
11000000	10101000	00001010	00000101

Таблиця 1.1 – Приклад IPv4-адреси 192.168.10.5 у десятковому та двійковому форматах

Важливо розуміти: ***IP-адреса складається з двох частин*** *– ідентифікатора мережі (network ID) та ідентифікатора хоста (host ID). Межа між ними визначається маскою підмережі.*

Маска підмережі – це також 32-бітне число, в якому одиниці позначають частину мережі, а нулі – частину хоста. Маска записується або у вигляді чотирьох октетів (наприклад, 255.255.255.0), або у форматі CIDR (Classless Inter-Domain Routing) – числом одиниць після символу «/» (наприклад, /24).

Маска (десяткова)	CIDR	Двійкова	Кількість хостів
255.0.0.0	/8	11111111.00000000.00000000.00000000	16 777 214
255.255.0.0	/16	11111111.11111111.00000000.00000000	65 534
255.255.255.0	/24	11111111.11111111.11111111.00000000	254
255.255.255.128	/25	11111111.11111111.11111111.10000000	126
255.255.255.192	/26	11111111.11111111.11111111.11000000	62
255.255.255.224	/27	11111111.11111111.11111111.11100000	30
255.255.255.240	/28	11111111.11111111.11111111.11110000	14
255.255.255.248	/29	11111111.11111111.11111111.11111000	6
255.255.255.252	/30	11111111.11111111.11111111.11111100	2

Таблиця 1.2 – Найпоширеніші маски підмереж

Формула розрахунку кількості хостів: *кількість хостів = 2^n – 2, де n – кількість нульових біт у масці (бітів, відведених під хост-частину).*

Від загального числа вираховуються 2, тому що перша адреса (всі нулі в хост-частині) є адресою самої мережі, а остання (всі одиниці) – broadcast-адресою, яка використовується для широкомовного розсилання на всі вузли підмережі.

Розрахунок параметрів підмережі – покроковий алгоритм

Розглянемо детальний алгоритм визначення параметрів підмережі на конкретному прикладі.
Приклад: Дана адреса хоста 192.168.1.70 з маскою /26 (255.255.255.192). Знайти: адресу мережі, broadcast-адресу, діапазон хост-адрес, кількість хостів.

Крок 1. Визначте розмір блоку підмережі. Маска /26 означає 26 одиниць і 6 нулів. Розмір блоку = $2^6 = 64$. Це означає, що адресний простір четвертого октету ділиться на блоки по 64: 0-63, 64-127, 128-191, 192-255.

Крок 2. Знайдіть, до якого блоку належить адреса. Адреса хоста: 192.168.1.70. Четвертий октет = 70. Шукаємо блок: $64 \leq 70 < 128$. Отже, хост належить до блоку, що починається з 64.

Крок 3. Визначте адресу мережі. Адреса мережі – це початок блоку, де хост-частина дорівнює нулю: 192.168.1.64

Крок 4. Визначте broadcast-адресу. Broadcast-адреса – це остання адреса блоку (64 + 64 – 1 = 127): 192.168.1.127

Крок 5. Визначте діапазон хост-адрес. Перша хост-адреса: 192.168.1.65 (адреса мережі + 1)
Остання хост-адреса: 192.168.1.126 (broadcast – 1)

Крок 6. Порахуйте кількість хостів. Кількість хостів = $2^6 – 2 = 62$ хости.

Параметр	Значення
Адреса хоста / маска	192.168.1.70 / 26
Адреса мережі	192.168.1.64
Перша хост-адреса	192.168.1.65
Остання хост-адреса	192.168.1.126
Broadcast-адреса	192.168.1.127
Кількість хостів	62

Таблиця 1.3 – Результати розрахунку параметрів підмережі

Зверніть увагу!
Адреса мережі та broadcast-адреса НЕ можуть бути призначені жодному хосту. Спроба налаштувати мережевий інтерфейс з такою адресою призведе до помилки або некоректної роботи мережі.

Класи IP-адрес та приватні адресні простори

Первісно адреси IPv4 ділилися на класи залежно від першого октету. Хоча сьогодні класова адресація витіснена CIDR, розуміння класів залишається важливим для роботи з мережами.

Клас	Діапазон першого октету	Стандартна маска	Кількість мереж	Хостів у мережі
A	1 – 126	255.0.0.0 (/8)	126	16 777 214
B	128 – 191	255.255.0.0 (/16)	16 384	65 534
C	192 – 223	255.255.255.0 (/24)	2 097 152	254
D	224 – 239	–	Multicast	–
E	240 – 255	–	Зарезервовано	–

Таблиця 1.4 – Класи IP-адрес

Приватні (RFC 1918) адресні простори – діапазони адрес, які не маршрутизуються в Інтернеті і використовуються у внутрішніх мережах організацій (у тому числі медичних закладів):

- 10.0.0.0 – 10.255.255.255 (маска /8, клас A)
- 172.16.0.0 – 172.31.255.255 (маски /12, клас B)
- 192.168.0.0 – 192.168.255.255 (маска /16, клас C)

Застосування в медицині.
У мережах лікарень та медичних центрів для внутрішньої адресації зазвичай застосовують приватні діапазони 192.168.x.x або 10.x.x.x. Вихід у зовнішні мережі (Інтернет) здійснюється через NAT (Network Address Translation). Поділ на підмережі (subnetting) дозволяє відокремити, наприклад, мережу медичних приладів від адміністративної або гостьової мережі.

CIDR та поділ на підмережі (Subnetting)

CIDR (Classless Inter-Domain Routing) – сучасний метод адресації, що дозволяє використовувати маску довільної довжини, а не лише «класові» /8, /16, /24. Це дає змогу ефективніше розподіляти адресний простір.

Практичний приклад subnetting: Необхідно розбити мережу 192.168.5.0/24 на 4 рівні підмережі.
Для 4 підмереж потрібно 2 біти ($2^2 = 4$). Запозичуємо 2 біти з хост-частини, маска стає /26.

Підмережа	Адреса мережі	Broadcast	Перший хост	Останній хост
1	192.168.5.0/26	192.168.5.63	192.168.5.1	192.168.5.62
2	192.168.5.64/26	192.168.5.127	192.168.5.65	192.168.5.126
3	192.168.5.128/26	192.168.5.191	192.168.5.129	192.168.5.190
4	192.168.5.192/26	192.168.5.255	192.168.5.193	192.168.5.254

Таблиця 1.5 – Результат поділу 192.168.5.0/24 на чотири підмережі /26

Спеціальні адреси

Loopback (127.0.0.1) – адреса зворотної петлі, призначена для тестування мережевого стеку на самому пристрої. Пакети, надіслані на цю адресу, не виходять у мережу.
APIPA (169.254.x.x) – автоматично призначається ОС, якщо DHCP-сервер недоступний. Поява такої адреси на інтерфейсі свідчить про проблему з отриманням IP-адреси від сервера.
Broadcast 255.255.255.255 – обмежений broadcast, що адресований усім вузлам у локальному сегменті мережі (не маршрутизується між мережами).

Знайомство з Cisco Packet Tracer

Cisco Packet Tracer (CPT) – безкоштовний мережевий симулятор від компанії Cisco, що дозволяє проектувати та тестувати мережі без використання реального обладнання. Він є стандартним інструментом для навчання мережевих технологій у всьому світі.

Інтерфейс програми

Після запуску Cisco Packet Tracer відкривається головне вікно, що складається з кількох функціональних зон:

- **Робоча область (Workspace)** – центральна частина екрану, де розміщуються мережеві пристрої та з'єднання між ними.
- **Панель пристроїв (Device-Type Selection Box)** – розташована у нижній частині вікна зліва. Містить категорії обладнання: маршрутизатори (Routers), комутатори (Switches), концентратори (Hubs), бездротові пристрої (Wireless Devices), кінцеві пристрої (End Devices), WAN-емуляція тощо.
- **Панель конкретних пристроїв (Specific Device Selection)** – відображається праворуч від категорій і показує конкретні моделі обладнання вибраної категорії.
- **Панель з'єднань (Connections)** – секція з типами кабелів. Зображена значком блискавки.
- **Панель інструментів (Toolbar)** – у верхній частині вікна, містить інструменти виділення, переміщення, видалення, додавання нотаток тощо.
- **Режими симуляції** – у правому нижньому куті перемикач між Realtime (реальний час) та Simulation (покрокова симуляція пакетів).

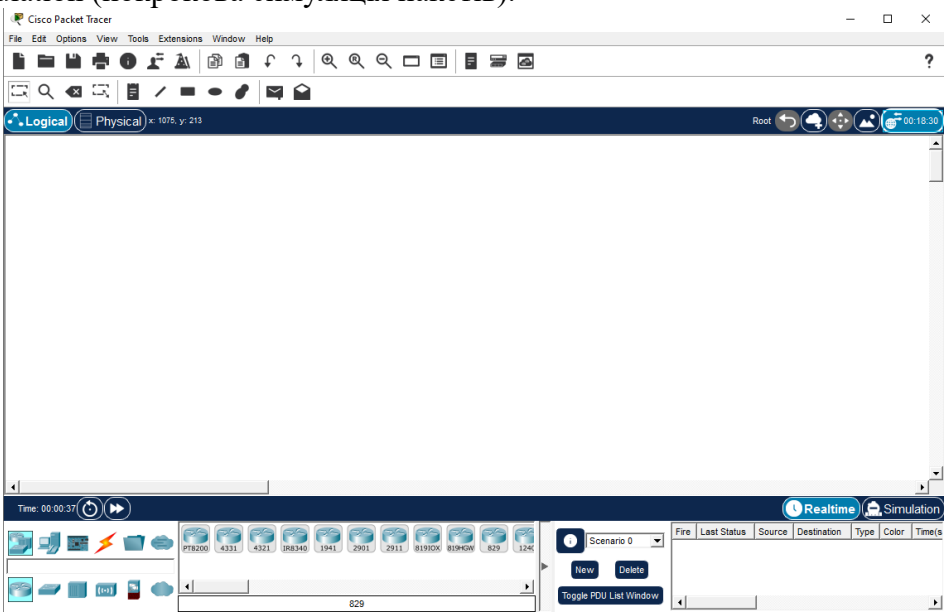

Рисунок 1.1 – Інтерфейс Cisco Packet Tracer

Розміщення пристроїв на робочому полі

Для додавання пристрою на робоче поле необхідно:

1. Клацнути на потрібну категорію в нижньому лівому куті (наприклад, End Devices для комп'ютерів).
2. У панелі конкретних пристроїв знайти потрібну модель (наприклад, PC або Laptop).
3. Перетягнути значок пристрою (drag-and-drop) на робочу область або просто клацнути на ньому, а потім клацнути у потрібному місці робочої області.
4. Для перейменування пристрою слід двічі клацнути на його назві під значком і ввести нове ім'я.

З'єднання пристроїв кабелями

Cisco Packet Tracer підтримує різні типи кабелів. Для вибору кабелю слід клацнути на категорію з'єднань (значок блискавки) у нижній панелі.

Найважливіші типи кабелів:

Тип кабелю	Коли використовувати	Піктограма у CPT
Straight-through (прямий)	PC/сервер ↔ комутатор, маршрутизатор ↔ комутатор	
Crossover (перехресний)	PC ↔ PC, комутатор ↔ комутатор, маршрутизатор ↔ маршрутизатор (без Auto-MDIX)	
Serial DCE/DTE	З'єднання маршрутизаторів через WAN-інтерфейс	
Автоматично (Auto)	CPT сам визначає тип – рекомендується новачкам	

Таблиця 1.6 – Типи кабелів у Cisco Packet Tracer

Щоб з'єднати два пристрої: клацніть на обраний тип кабелю, потім клацніть на першому пристрої (CPT запропонує вибрати порт), оберіть порт і клацніть на другому пристрої. Якщо з'єднання успішне, на кінцях кабелю з'являться кружечки: зелений – порт активний, помаранчевий – ініціалізація (STP), червоний – проблема.

Налаштування IP-адреси на комп'ютері (PC)

Для налаштування мережевого інтерфейсу кінцевого пристрою (PC) в Cisco Packet Tracer:

1. Двічі клацніть на значку PC, щоб відкрити вікно налаштувань пристрою.
2. Перейдіть на вкладку Desktop.
3. Виберіть IP Configuration.
4. Оберіть Static (статична адреса).
5. Введіть IP Address, Subnet Mask та (за потреби) Default Gateway.
6. Закрийте вікно – налаштування застосовуються автоматично.

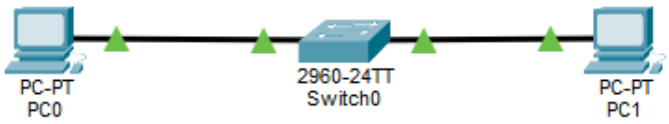

Рисунок 1.2 – Проста мережа з двох PC через комутатор

Перевірка зв'язку командою `ping`. Зберіть схему на Нисунку 1.2. Налаштуйте IP-адреси і маски підмережі на комп'ютерах. Для PC0 встановіть IP-адресу 192.168.1.1 і маску 255.255.255.0. Для PC1 встановіть IP-адресу 192.168.1.2 і маску 255.255.255.0.
Після налаштування IP-адрес необхідно перевірити, чи можуть вузли обмінюватися даними. Для цього:

1. Двічі клацніть на PC → вкладка Desktop → Command Prompt.
2. Введіть команду: `ping 192.168.1.2`
3. Якщо зв'язок є, ви побачите повідомлення:

```
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

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

4. Якщо зв'язку немає:

```
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Корисна порада
Якщо перший ping видає timeout – це нормально! CPT надсилає ARP-запит для з'ясування MAC-адреси, що займає час. Повторний ping, як правило, вже проходить успішно.

Діагностика проблем з IP-адресацією

Вміння знаходити і виправляти помилки в мережі – одна з ключових компетенцій мережевого інженера. Нижче наведено типові проблеми та методику їх усунення.

Основний алгоритм діагностики

При виникненні проблеми зі зв'язком рекомендується дотримуватися такого порядку перевірок:

1. Перевірте фізичний рівень – стан індикаторів портів (зелений/червоний у CPT).
2. Перевірте правильність IP-адреси та маски на кожному пристрої.
3. Переконайтеся, що адреси належать до однієї підмережі (або вказано шлюз за замовчуванням).
4. Виконайте `ping` до шлюзу (Default Gateway) – якщо шлюз не відповідає, перевіряйте маршрутизатор.
5. Виконайте `ping` до цільового хоста.
6. Використайте traceroute для визначення, де саме пакет губиться.

Типові помилки та їх симптоми

Симптом	Ймовірна причина	Спосіб перевірки
ping не проходить між двома PC	Різні підмережі або неправильна маска	Перевірити адреси обох PC
Червоний індикатор на порту в CPT	Неправильний тип кабелю або порт вимкнено	Замінити кабель на Auto
APIPA-адреса (169.254.x.x)	DHCP-сервер недоступний	Перевірити DHCP або призначити static IP
Перший ping – timeout, другий – OK	ARP-ресолюція (нормальна поведінка)	Повторити ping – проблема зникне
Destination host unreachable	Немає маршруту до мережі призначення	Перевірити шлюз за замовчуванням

Таблиця 1.7 – Типові проблеми з IP-адресацією та методи їх усунення

Корисні команди для діагностики в CPT

На пристроях PC (через Desktop → Command Prompt) доступні такі команди:

Команда	Що показує
`ipconfig`	Поточні IP-адреса, маска, шлюз на всіх інтерфейсах
`ping <IP>`	Перевірка досяжності вузла (ICMP Echo)
`tracert <IP>`	Маршрут пакету до вузла та затримки на кожному переході
`arp -a`	Таблиця ARP (відповідність IP та MAC-адрес)

Таблиця 1.8 – Команди діагностики на кінцевих пристроях у Cisco Packet Tracer

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

Завдання складається з двох частин. Перша частина – розрахункова (студент має привести в звіті всі розрахунки і результат), друга – практична (виконується в Cisco Packet Tracer).

Частина 1. Розрахунок параметрів підмережі
Для адреси хоста та маски підмережі, наведених у таблиці варіантів, визначте:

- Адресу мережі
- Broadcast-адресу
- Першу та останню хост-адресу
- Кількість можливих хостів у підмережі
- Маску підмережі у форматі 255.x.x.x та у CIDR-нотації (/xx)

Оформіть результати у вигляді таблиці (аналогічно Таблиці 1.3 у теоретичних відомостях). Покажіть покрокові обчислення.

Частина 2. Побудова мережі в Cisco Packet Tracer
Відповідно до вашого варіанту побудуйте та налаштуйте мережу з наступної топологією:

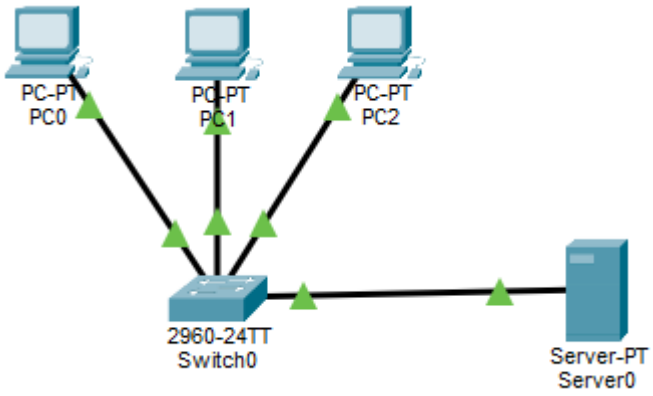

Рисунок 1.3 – Топологія мережі для завдання

Мережа має складатись із таких пристроїв:

- Три комп'ютери (PC0, PC1, PC2)
- Один комутатор Cisco Catalyst 2960
- Один сервер (Server0)

Всі пристрої підключаються до комутатора прямим (straight-through) кабелем або через Auto-з'єднання.
Адреси для кожного пристрою обираються зі стовпця «Адреси хостів» таблиці варіантів – послідовно (PC0 отримує першу адресу, PC1 – другу і т.д.).

Порядок виконання:

1. Запустіть Cisco Packet Tracer та створіть новий проект (File → New).
2. Розмістіть на робочому полі: 3 PC (End Devices → PC), 1 Сервер (End Devices → Server), 1 Комутатор (Switches → 2960).
3. З'єднайте всі пристрої з комутатором кабелем Auto (або Straight-through).
4. Налаштуйте IP-адреси відповідно до вашого варіанту (Desktop → IP Configuration → Static).
5. Заповніть таблицю адресації (Таблиця 1.9) у звіті.

6. Перевірте зв'язок командою `ping` з кожного PC до всіх інших пристроїв.
7. Зробіть скріншот топології мережі та результатів `ping`.
8. Збережіть файл проекту (.pkt).

Таблиця адресації (заповнити у звіті)

Пристрій	IP-адреса	Маска підмережі	Broadcast
PC0			
PC1			
PC2			
Server0			

Таблиця 1.9 – Таблиця адресації

Варіанти завдань

Знайдіть свій варіант за вказівкою викладача. У кожному варіанті задано адресу мережі та маску. Послідовно призначте адреси хостам (починаючи з першої доступної хост-адреси).

Вар.	Адреса мережі / Маска	IP_1 (PC0)	IP_2 (PC1)	IP_3 (PC2)	IP_S (Server)
1	192.168.1.0 /24	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.10
2	192.168.2.0 /24	192.168.2.1	192.168.2.2	192.168.2.3	192.168.2.10
3	172.16.0.0 /24	172.16.0.1	172.16.0.2	172.16.0.3	172.16.0.10
4	10.10.1.0 /24	10.10.1.1	10.10.1.2	10.10.1.3	10.10.1.10
5	192.168.10.0 /25	192.168.10.1	192.168.10.2	192.168.10.3	192.168.10.10
6	192.168.10.128 /25	192.168.10.129	192.168.10.130	192.168.10.131	192.168.10.140
7	10.0.0.0 /26	10.0.0.1	10.0.0.2	10.0.0.3	10.0.0.10
8	10.0.0.64 /26	10.0.0.65	10.0.0.66	10.0.0.67	10.0.0.70
9	172.16.5.0 /26	172.16.5.1	172.16.5.2	172.16.5.3	172.16.5.10
10	172.16.5.64 /26	172.16.5.65	172.16.5.66	172.16.5.67	172.16.5.70
11	192.168.100.0 /27	192.168.100.1	192.168.100.2	192.168.100.3	192.168.100.10
12	192.168.100.32 /27	192.168.100.33	192.168.100.34	192.168.100.35	192.168.100.40
13	10.5.0.0 /27	10.5.0.1	10.5.0.2	10.5.0.3	10.5.0.10
14	172.20.1.0 /28	172.20.1.1	172.20.1.2	172.20.1.3	172.20.1.5
15	192.168.50.32 /28	192.168.50.33	192.168.50.34	192.168.50.35	192.168.50.40

Таблиця 1.10 – Варіанти завдань для лабораторної роботи № 1

Вимоги до звіту

Звіт має містити:
1) Розрахункову частину з покроковим визначенням параметрів підмережі.
2) Заповнену таблицю адресації (Приклад - Таблиця 1.9).
3) Скріншот топології мережі в CPT.
4) Скріншоти результатів `ping` між усіма вузлами.
5) Відповіді на контрольні запитання.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке IP-адреса і яку функцію вона виконує в комп'ютерній мережі? Скільки бітів вона містить і в якому форматі записується?
2. Що таке маска підмережі? Як пов'язані між собою десятковий запис маски (наприклад, 255.255.255.0) та CIDR-нотація (/24)?
3. За якою формулою розраховується максимальна кількість хостів у підмережі? Чому від загальної кількості адрес віднімають 2?
4. Що таке адреса мережі та broadcast-адреса? Чому їх не можна призначати хостам?
5. Дано адресу хоста 10.20.30.150/27. Визначте адресу мережі, broadcast-адресу, кількість хостів та діапазон допустимих хост-адрес.
6. Які діапазони IP-адрес відносяться до приватних (RFC 1918)? Чому їх називають «приватними» і де вони застосовуються?
7. Що означає адреса 169.254.x.x на мережевому інтерфейсі? Що необхідно перевірити у разі її появи?
8. Що означають різні кольори індикаторів на кінцях кабелів у Cisco Packet Tracer (зелений, помаранчевий, червоний)?
9. Чому перший ping між двома PC у Cisco Packet Tracer може завершитись timeout, а повторний – успішно? Який протокол відповідає за цю поведінку?
10. Яка різниця між командами `ping` та `tracert`? В якій ситуації доцільно використовувати кожну з них при діагностиці мережевих проблем?

Лабораторна робота №2.

Базове налаштування мережевого обладнання Cisco (IOS CLI).

Мета роботи: Ознайомитися з операційною системою Cisco IOS та принципами роботи з інтерфейсом командного рядка (CLI). Вивчити ієрархію режимів доступу та рівні привілеїв. Отримати практичні навички початкового налаштування маршрутизатора та комутатора: встановлення імені пристрою, банера, паролів та облікових записів користувачів з різними рівнями доступу, налаштування мережевих інтерфейсів. Навчитися перевіряти результати налаштування за допомогою команд групи show та зберігати конфігурацію.

ТЕОРЕТИЧНІ ВІДОМОСТІ:

Cisco IOS – операційна система мережевого обладнання

Cisco IOS (Internetwork Operating System) – це спеціалізована операційна система, що використовується на маршрутизаторах і комутаторах Cisco. На відміну від звичних настільних ОС, IOS оптимізована для виконання мережевих функцій: маршрутизації, комутації, управління трафіком і забезпечення безпеки.

Основним інструментом взаємодії з Cisco IOS є CLI (Command Line Interface) – інтерфейс командного рядка. Саме через нього мережевий інженер вводить команди налаштування, перевіряє стан пристрою та усуває несправності. Розуміння CLI є фундаментальною навичкою для будь-якого спеціаліста, що працює з мережевою інфраструктурою медичного закладу.

Доступ до CLI можна отримати кількома способами:

- **Console (Консоль)** – пряме підключення через спеціальний консольний кабель (RJ-45 або USB). Використовується для початкового налаштування або коли мережевий доступ недоступний. У Cisco Packet Tracer – вкладка CLI у вікні пристрою.
- **Telnet** – підключення по мережі через порт 23. Незашифроване, тому небажане у виробничих середовищах.
- **SSH (Secure Shell)** – зашифроване мережеве підключення через порт 22. Рекомендований спосіб віддаленого управління.

Ієрархія режимів Cisco IOS

Cisco IOS побудована на принципі ієрархічних режимів доступу. Кожен режим надає певний набір дозволених команд і позначається характерним запрошенням (prompt) у рядку вводу.

Режим	Запрошення (prompt)	Як увійти	Що дозволено
`User EXEC`	`Router>`	Початковий режим після підключення	Базові команди моніторингу (`ping`, `show version`)
`Privileged EXEC`	`Router#`	`enable` (з `User EXEC`)	Всі команди перегляду, `debug`, `copy`, `reload`
`Global Configuration`	`Router(config)#`	`configure terminal` (з режиму `Privileged`)	Глобальні налаштування пристрою
`Interface Configuration`	`Router(config-if)#`	`interface <тип> <номер>`	Налаштування конкретного

			інтерфейсу

`Line Configuration`	`Router(config-line)#`	`line console 0`
		або
		`line vty 0 4`
			Налаштування ліній доступу (`console`, `telnet/SSH`)

Таблиця 2.1 – Ієрархія режимів Cisco IOS

```
Підключення до пристрою
      |
      v
[ User EXEC: Router> ]        <--- logout / exit
      | enable
      v                disable
[ Privileged EXEC: Router# ]  <----------+
      | configure terminal               |
      v                        end / Ctrl+Z  |
[ Global Config: Router(config)# ]  -----+
      |                    |
interface Fa0/0          line console 0
      |                    |
[Router(config-if)#]   [Router(config-line)#]
```

Рисунок 2.1 – Ієрархія та переходи між режимами Cisco IOS

Для повернення з будь-якого режиму конфігурації одразу до Privileged EXEC достатньо натиснути Ctrl+Z або ввести команду end. Команда exit повертає на один рівень вище.

Підказка щодо роботи з CLI. Cisco IOS підтримує автодоповнення команд клавішею **Tab** та скорочення: достатньо ввести стільки символів команди, щоб вона стала унікальною. Наприклад, `conf t` замість `configure terminal`, або `sh ip int br` замість `show ip interface brief`. Знак `?` після команди або пробілу покаже список доступних варіантів.

Початкове налаштування пристрою

Після першого ввімкнення пристрій Cisco не має жодної конфігурації (або містить заводські значення). Перше, що необхідно зробити – виконати базове налаштування, яке забезпечить ідентифікацію пристрою в мережі та захист від несанкціонованого доступу.

Встановлення імені пристрою (hostname)

Ім'я пристрою відображається у рядку запрошення CLI і є важливим ідентифікатором у великих мережах.

```
Router> enable
Router# configure terminal
Router(config)# hostname MedRouter-1
MedRouter-1(config)#
```

Приклад 2.1 – Встановлення імені пристрою

Налаштування банера (banner)

Банер – це повідомлення, що відображається при підключенні до пристрою. Юридично важливий елемент: попереджає неавторизованих користувачів про недопустимість несанкціонованого доступу. Особливо важливо у медичних закладах, де обладнання може

оброблювати персональні дані пацієнтів.

```
MedRouter-1(config)# banner motd #
Enter TEXT message.  End with the character '#'.
================================================
  УВАГА! Доступ лише для авторизованих осіб.
  Несанкціонований доступ заборонений.
  Медичний центр. Мережеве обладнання.
================================================
#
MedRouter-1(config)#
```

Приклад 2.2 – Налаштування банера MOTD

Символ # є роздільником (delimiter) – він позначає початок і кінець тексту банера. Можна використати будь-який символ, якого немає в тексті банера.

Захист пристрою паролями

Cisco IOS надає кілька незалежних механізмів захисту доступу. Важливо налаштувати всі з них, оскільки кожен захищає окремий вектор доступу.

Пароль на Privileged EXEC (`enable secret`)

Це найважливіший пароль: він захищає перехід до привілейованого режиму, де можна змінювати будь-які налаштування.

```
MedRouter-1(config)# enable secret P@ssw0rd_Med
```

Приклад 2.3 – Встановлення захищеного пароля `enable secret`

`enable secret` *vs* `enable password`

Cisco IOS має дві команди: `enable password` *(застаріла, зберігає пароль відкритим текстом) та* `enable secret` *(сучасна, зберігає MD5-хеш пароля). Завжди використовуйте* enable secret*. Якщо налаштовані обидві –* `enable secret` *має пріоритет.*

Шифрування всіх паролів у конфігурації

За замовчуванням деякі паролі в Cisco IOS зберігаються відкритим текстом у файлі конфігурації. Команда `service password-encryption` вмикає базове шифрування для всіх паролів (тип 7 – оборотне шифрування).

```
MedRouter-1(config)# service password-encryption
```

Приклад 2.4 – Увімкнення шифрування паролів

Захист консольної лінії (console)

Консольна лінія – фізичне підключення через консольний порт. Навіть якщо пристрій розміщений у захищеній серверній кімнаті, консоль слід захистити паролем.

```
MedRouter-1(config)# line console 0
MedRouter-1(config-line)# password C0ns0le_Pwd
MedRouter-1(config-line)# login
MedRouter-1(config-line)# exec-timeout 5 0
MedRouter-1(config-line)# exit
```

Приклад 2.5 – Захист консольної лінії

Команда `exec-timeout 5 0` встановлює тайм-аут сесії: 5 хвилин 0 секунд бездіяльності – після цього сесія автоматично завершується. Перший параметр – хвилини, другий – секунди.

Захист ліній VTY (Telnet / SSH)

Лінії VTY (Virtual TeleType) – це віртуальні лінії для віддаленого підключення. Більшість пристроїв Cisco має 16 ліній VTY (0–15). Необхідно захистити всі.

```
MedRouter-1(config)# line vty 0 15
MedRouter-1(config-line)# password VTY_P@ss
MedRouter-1(config-line)# login
MedRouter-1(config-line)# exec-timeout 10 0
MedRouter-1(config-line)# transport input ssh
MedRouter-1(config-line)# exit
```

Приклад 2.6 – Захист VTY ліній (тільки SSH)

Команда `transport input ssh` дозволяє підключення лише через SSH, забороняючи Telnet. Для медичних мереж, де може передаватися конфіденційна інформація, це обов'язкова вимога.

Облікові записи користувачів і рівні привілеїв

Cisco IOS підтримує гнучку систему управління доступом на основі облікових записів користувачів та рівнів привілеїв. Це особливо важливо у середовищах з кількома адміністраторами різного рівня відповідальності – типова ситуація у великих медичних закладах.

Рівні привілеїв Cisco IOS

Cisco IOS підтримує 16 рівнів привілеїв (0–15). Кожному рівню можна призначити певний набір команд.

Рівень	Назва	Доступні команди за замовчуванням	Типове використання
0	Мінімальний	`disable, enable, exit, help, logout`	Немає фактичного доступу
1	`User EXEC`	Базові команди `ping, show version` тощо	Читання базових даних
2–14	Користувацькі	Визначаються адміністратором	Спеціалізовані ролі
15	`Privileged EXEC`	Усі команди IOS без обмежень	Повний адміністративний доступ

Таблиця 2.2 – Рівні привілеїв Cisco IOS

Створення локальних облікових записів

Команда `username` дозволяє створювати локальні облікові записи безпосередньо на пристрої. Кожному запису призначається ім'я, пароль та рівень привілеїв.

```
! Адміністратор мережі – повний доступ (рівень 15)
MedRouter-1(config)# username admin privilege 15 secret Adm1n_Str0ng!

! Технік – обмежений доступ (рівень 5), лише перегляд
MedRouter-1(config)# username technik privilege 5 secret T3chn1k_Med

! Гостьовий обліковий запис (рівень 1) – лише базові команди
MedRouter-1(config)# username guest privilege 1 secret Guest_View
```

Приклад 2.7 – Створення облікових записів з різними рівнями привілеїв

Ключове слово `secret` (замість застарілого `password`) забезпечує збереження пароля у вигляді MD5-хешу. Якщо використати `password` – пароль зберігається відкритим текстом (навіть якщо увімкнено `service password-encryption`, захист буде слабшим).

Налаштування аутентифікації через локальну базу

Щоб пристрій використовував локальні облікові записи для авторизації (а не прості паролі на лініях), необхідно вказати `login local` на відповідних лініях:

```
! Консольна лінія – аутентифікація через локальну базу
MedRouter-1(config)# line console 0
MedRouter-1(config-line)# login local
MedRouter-1(config-line)# exit

! VTY лінії – аутентифікація через локальну базу
MedRouter-1(config)# line vty 0 15
MedRouter-1(config-line)# login local
MedRouter-1(config-line)# transport input ssh
MedRouter-1(config-line)# exit
```

Приклад 2.8 – Увімкнення аутентифікації через локальну базу користувачів

`login` ***vs*** `login local`

Команда `login` *(без* `local`*) вимагає пароль, налаштований командою* `password` *на лінії. Команда* `login local` *вимагає ввести ім'я користувача та пароль з локальної бази (username).* `login local` *є кращим варіантом, оскільки дозволяє персоналізувати доступ і вести облік дій кожного адміністратора.*

Призначення команд до рівнів привілеїв

Рівні 2–14 порожні за замовчуванням. Адміністратор може самостійно вирішити, які команди доступні на кожному рівні:

```
! Дозволити команду 'show running-config' на рівні 5
MedRouter-1(config)# privilege exec level 5 show running-config

! Дозволити команду 'show interface' на рівні 5
MedRouter-1(config)# privilege exec level 5 show interface
```

Приклад 2.9 – Призначення команд до рівня привілеїв

Налаштування мережевих інтерфейсів маршрутизатора

На відміну від комутаторів, де порти активні за замовчуванням, інтерфейси маршрутизатора Cisco завжди вимкнені після першого увімкнення. Їх необхідно сконфігурувати та ввімкнути вручну.

Типи інтерфейсів маршрутизатора:

- FastEthernet (Fa0/0, Fa0/1...) – 100 Мбіт/с Ethernet-порти. Найпоширеніші на навчальних моделях (1841, 2811).
- GigabitEthernet (Gi0/0, Gi0/1...) – 1 Гбіт/с. Сучасні маршрутизатори (ISR 4000, серія 2900/3900).
- Serial (Se0/0/0, Se0/0/1...) – послідовні інтерфейси для WAN-з'єднань. Для роботи потрібен Serial-кабель (DCE/DTE).

Налаштування Ethernet-інтерфейсу

```
MedRouter-1(config)# interface FastEthernet 0/0
MedRouter-1(config-if)# description === LAN: Merezha Kardiology ===
MedRouter-1(config-if)# ip address 192.168.1.1 255.255.255.0
MedRouter-1(config-if)# no shutdown
MedRouter-1(config-if)# exit

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
```

Приклад 2.10 – Налаштування FastEthernet інтерфейсу

Команда `no shutdown` є обов'язковою – саме вона фізично вмикає інтерфейс. Без неї він залишається в стані `administratively down`. Якщо з'єднання фізично встановлено, після no shutdown з'являться повідомлення про зміну стану інтерфейсу на up.

Команда `description` є необов'язковою, але надзвичайно корисною: вона дозволяє залишати коментарі щодо призначення інтерфейсу. Особливо важливо в мережах медичних закладів, де кожен порт може вести до конкретного відділення або обладнання.

Налаштування інтерфейсу керування комутатором (SVI)

Комутатор Cisco – це рівень 2 (канальний рівень), тому він не має звичайних IP-інтерфейсів. Для отримання IP-адреси (потрібна для віддаленого управління) використовується SVI (Switch Virtual Interface) – логічний інтерфейс VLAN 1.

```
Switch(config)# hostname MedSwitch-1
MedSwitch-1(config)# interface vlan 1
MedSwitch-1(config-if)# ip address 192.168.1.2 255.255.255.0
MedSwitch-1(config-if)# no shutdown
MedSwitch-1(config-if)# exit

! Вказуємо шлюз за замовчуванням для виходу за межі підмережі
MedSwitch-1(config)# ip default-gateway 192.168.1.1
```

Приклад 2.11 – Налаштування IP-адреси для управління комутатором

Збереження конфігурації

Cisco IOS зберігає поточну конфігурацію в оперативній пам'яті (RAM) у файлі running-config. При вимкненні живлення ця конфігурація втрачається. Щоб зберегти налаштування, їх необхідно записати у постійну пам'ять (NVRAM) у файл startup-config.

```
MedRouter-1# copy running-config startup-config
Destination filename [startup-config]?
[Enter]
Building configuration...
[OK]

! Скорочений варіант тієї ж команди:
MedRouter-1# wr
```

Приклад 2.12 – Збереження конфігурації

Важливо!

Якщо не виконати `copy running-config startup-config`*, після перезавантаження пристрою всі ваші налаштування будуть втрачені! Завжди зберігайте конфігурацію після внесення змін. Команда* `reload` *перезавантажує пристрій – перед її виконанням обов'язково зберігайте конфіг.*

Команди перевірки конфігурації (show-команди)

Команди групи `show` – основний інструмент перевірки результатів налаштування та діагностики проблем. Всі вони виконуються в режимі Privileged EXEC (або деякі – в User EXEC).

Перегляд конфігурації

```
! Поточна (активна) конфігурація в RAM:
MedRouter-1# show running-config

! Збережена конфігурація в NVRAM (завантажиться при перезапуску):
MedRouter-1# show startup-config

! Переглянути лише секцію інтерфейсів у running-config:
MedRouter-1# show running-config | section interface

! Переглянути лише рядки, що містять слово 'username':
MedRouter-1# show running-config | include username
```

Приклад 2.13 – Команди перегляду конфігурації

Перегляд стану інтерфейсів

```
! Коротка таблиця всіх інтерфейсів (IP, статус, протокол):
MedRouter-1# show ip interface brief

Interface        IP-Address      OK? Method Status                Protocol
FastEthernet0/0  192.168.1.1     YES manual up                    up
FastEthernet0/1  unassigned      YES unset  administratively down  down

! Детальна інформація про конкретний інтерфейс:
MedRouter-1# show interface FastEthernet 0/0

! Стан інтерфейсів з IP-налаштуваннями:
MedRouter-1# show ip interface FastEthernet 0/0
```

Приклад 2.14 – Команди перегляду стану інтерфейсів

Стовпці `Status` та `Protocol` у виводі `show ip interface brief` дають чітке розуміння стану інтерфейсу:

Status	Protocol	Значення
`up`	`up`	Інтерфейс працює нормально
`up`	`down`	Фізичний рівень OK, є проблема на канальному рівні
`administratively down`	`down`	Вимкнений командою `shutdown` (потрібна `no shutdown`)
`down`	`down`	Фізична проблема: немає кабелю, пристрій вимкнений

Таблиця 2.3 – Стани інтерфейсів у виводі `show ip interface brief`

Перегляд системної інформації та версії IOS

```
! Версія IOS, час роботи, модель пристрою, обсяг пам'яті:
MedRouter-1# show version

! Список усіх флеш-файлів (образ IOS тощо):
MedRouter-1# show flash
```

```
! Використання пам'яті:
MedRouter-1# show processes memory
```

Приклад 2.15 – Перегляд системної інформації

Перегляд облікових записів та ліній доступу

```
! Переглянути всі рядки з 'username' у конфігурації:
MedRouter-1# show running-config | include username
username admin privilege 15 secret 5 $1$mERr$ILh...
username technik privilege 5 secret 5 $1$xYzP$...

! Переглянути налаштування консолі та VTY:
MedRouter-1# show running-config | section line

! Показати поточні підключення до пристрою:
MedRouter-1# show users

! Показати рівень привілеїв поточного сеансу:
MedRouter-1# show privilege
Current privilege level is 15
```

Приклад 2.16 – Перегляд облікових записів та поточних сесій

Зведена таблиця найважливіших show-команд

Команда	Що перевіряє
`show running-config`	Вся поточна конфігурація пристрою
`show startup-config`	Збережена конфігурація (NVRAM)
`show ip interface brief`	Короткий стан всіх інтерфейсів (IP + статус)
`show interface <ім'я>`	Детальна статистика конкретного інтерфейсу
`show version`	Версія IOS, модель, час роботи, пам'ять
`show users`	Список активних сеансів на пристрої
`show privilege`	Рівень привілеїв поточного сеансу
`show flash`	Файли у флеш-пам'яті (образ IOS)
`show running-config | include <слово>`	Фільтрація конфігурації за ключовим словом
`show running-config | section <розділ>`	Виведення конкретного розділу конфігурації

Таблиця 2.4 – Основні команди перевірки конфігурації Cisco IOS

Діагностика проблем конфігурації пристрою

Помилки при первинному налаштуванні обладнання трапляються навіть у досвідчених інженерів. Важливо вміти їх швидко виявити та виправити.

Алгоритм перевірки базового налаштування

1. Перевірте `hostname`: запрошення CLI має відповідати встановленому імені.

2. Виконайте `show ip interface brief` – перевірте, що потрібні інтерфейси мають статус `up/up` та правильні IP-адреси.
3. Виконайте `show running-config` – переконайтеся, що всі команди присутні у конфігурації.
4. Перевірте збережену конфігурацію: `show startup-config` повинна збігатися з `running-config` (якщо ви зберігали).
5. Спробуйте ping до шлюзу та сусідніх пристроїв з відповідного інтерфейсу.

Типові помилки та їх вирішення

Симптом	Причина	Вирішення
Інтерфейс у стані `admin down`	Не введена команда `no shutdown`	Зайти в `interface config`, ввести `no shutdown`
`% Login invalid` після введення пароля	Неправильний пароль або `login local` без `username`	Перевірити `username` командою `show run | include username`
Після `reload` налаштування зникли	Не збережено: `running ≠ startup`	`copy running-config startup-config` перед `reload`
`enable secret` не приймає пароль	Введено неправильно або скинуто	Ввести новий: `enable secret <новий_пароль>`
Пінг між PC та Router не проходить	Маска або IP налаштовані неправильно	`show ip interface brief` – перевірити адресу та маску
`% Ambiguous command`	Введено скорочення, що підходить до кількох команд	Дописати команду або натиснути `?` для підказки

Таблиця 2.5 – Типові помилки при базовому налаштуванні та їх усунення

Скасування команд (`no`)

Будь-яку команду конфігурації Cisco IOS можна скасувати, додавши перед нею ключове слово `no`:

```
! Видалити IP-адресу з інтерфейсу:
MedRouter-1(config-if)# no ip address

! Вимкнути (адміністративно вимкнути) інтерфейс:
MedRouter-1(config-if)# shutdown

! Видалити обліковий запис користувача:
MedRouter-1(config)# no username technik

! Видалити банер:
MedRouter-1(config)# no banner motd
```

Приклад 2.17 – Скасування команд конфігурації

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

Завдання полягає у побудові мережі відповідно до схеми та виконанні повного базового налаштування маршрутизатора і комутатора в Cisco Packet Tracer. Кожен студент виконує свій варіант із таблиці варіантів.

Топологія мережі

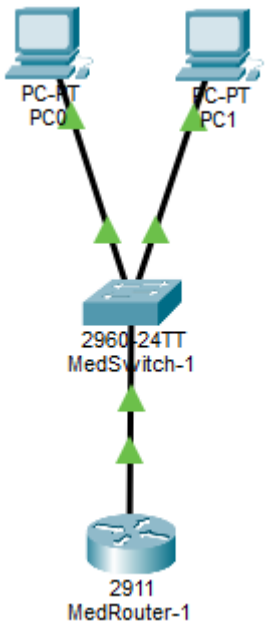

Рисунок 2.1 – Топологія мережі для лабораторної роботи № 2

Порядок виконання

Частина 1. Побудова топології

1. Запустіть Cisco Packet Tracer, створіть новий проект (File → New).
2. Розмістіть пристрої: маршрутизатор (Routers → 1941 або 2911), комутатор (Switches → 2960), два комп'ютери (End Devices → PC).
3. З'єднайте PC0 та PC1 з комутатором кабелем Straight-through (або Auto).
4. З'єднайте комутатор (порт Fa0/24) з маршрутизатором (Gig/0) кабелем Straight-through.
5. Налаштуйте IP-адреси на PC0 та PC1 відповідно до вашого варіанту (Desktop → IP Configuration → Static). Шлюзом вказати IP_GW (IP-адреса інтерфейсу маршрутизатора).

Частина 2. Налаштування маршрутизатора

1. Двічі клацніть на маршрутизаторі, перейдіть на вкладку CLI.
2. Встановіть ім'я пристрою: MedRouter-XX (де XX – ваш номер варіанту).
3. Налаштуйте банер MOTD з попередженням про авторизований доступ.
4. Встановіть `enable secret` (пароль за варіантом).
5. Захистіть консольну лінію паролем та командою `exec-timeout 5 0`.
6. Захистіть лінії `VTY (0 15)` паролем та командою `login`.

7. Увімкніть шифрування паролів: `service password-encryption`.
8. Створіть два облікові записи: `admin (privilege 15)` та `monitor (privilege 5)` – паролі за варіантом.
9. Налаштуйте інтерфейс Gig0/0: IP-адреса IP_GW, маска за варіантом, опис «`LAN Interface`», `no shutdown`.
10. Збережіть конфігурацію: `copy running-config startup-config`.

Частина 3. Налаштування комутатора

1. Відкрийте CLI комутатора.
2. Встановіть ім'я: `MedSwitch-XX`.
3. Налаштуйте банер MOTD.
4. Встановіть `enable secret` (пароль за варіантом).
5. Налаштуйте SVI (interface vlan 1): IP_SW, маска за варіантом, `no shutdown`.
6. Вкажіть шлюз за замовчуванням: `ip default-gateway IP_GW`.
7. Захистіть консольну та VTY лінії.
8. Збережіть конфігурацію.

Частина 4. Перевірка результатів

1. На маршрутизаторі виконайте `show ip interface brief` – зробіть скріншот.
2. Виконайте `show running-config` – зробіть скріншот (або переконайтеся, що всі налаштування присутні).
3. Виконайте `show running-config | include username` – перевірте наявність облікових записів.
4. Виконайте `show privilege` – зафіксуйте рівень доступу.
5. З PC0 виконайте ping до PC1, до IP_GW (маршрутизатора) та до IP_SW (комутатора) – зробіть скріншоти результатів.
6. Перевірте роботу пароля: вийдіть з privileged EXEC командою `disable` та знову увійдіть через `enable` – система має запитати пароль.

Таблиця адресації (заповнити у звіті)

Пристрій	IP-адреса	Маска підмережі	Шлюз (Gateway)
PC0			
PC1			
MedRouter-1 Gig0/0 (IP_GW)			–
MedSwitch-1 VLAN1 (IP_SW)			IP_GW

Таблиця 2.6 – Таблиця адресації

Варіанти завдань

Адреси мереж, паролі та імена облікових записів наведені для кожного варіанту. Налаштовуйте паролі точно як вказано у таблиці.

В.	Мережа / Маска	IP_GW	IP_SW	Enable secret	Пароль admin	Пароль monitor
1	192.168.1.0/24	192.168.1.1	192.168.1.2	En@ble_01	Adm1n_01	Mon1tor_01
2	192.168.2.0/24	192.168.2.1	192.168.2.2	En@ble_02	Adm1n_02	Mon1tor_02
3	192.168.3.0/24	192.168.3.1	192.168.3.2	En@ble_03	Adm1n_03	Mon1tor_03
4	172.16.1.0/24	172.16.1.1	172.16.1.2	En@ble_04	Adm1n_04	Mon1tor_04
5	172.16.5.0/24	172.16.5.1	172.16.5.2	En@ble_05	Adm1n_05	Mon1tor_05
6	10.0.1.0/24	10.0.1.1	10.0.1.2	En@ble_06	Adm1n_06	Mon1tor_06
7	10.10.0.0/24	10.10.0.1	10.10.0.2	En@ble_07	Adm1n_07	Mon1tor_07
8	192.168.10.0/25	192.168.10.1	192.168.10.2	En@ble_08	Adm1n_08	Mon1tor_08
9	192.168.20.0/25	192.168.20.1	192.168.20.2	En@ble_09	Adm1n_09	Mon1tor_09
10	10.5.0.0/25	10.5.0.1	10.5.0.2	En@ble_10	Adm1n_10	Mon1tor_10
11	172.16.10.0/25	172.16.10.1	172.16.10.2	En@ble_11	Adm1n_11	Mon1tor_11
12	192.168.30.0/26	192.168.30.1	192.168.30.2	En@ble_12	Adm1n_12	Mon1tor_12
13	192.168.40.64/26	192.168.40.65	192.168.40.66	En@ble_13	Adm1n_13	Mon1tor_13
14	10.20.0.0/26	10.20.0.1	10.20.0.2	En@ble_14	Adm1n_14	Mon1tor_14
15	172.20.5.0/26	172.20.5.1	172.20.5.2	En@ble_15	Adm1n_15	Mon1tor_15

Таблиця 2.7 – Варіанти завдань для лабораторної роботи № 2

Адреси PC: PC0 отримує третю хост-адресу мережі, PC1 – четверту. Наприклад, для варіанту 1 (192.168.1.0/24): PC0 = 192.168.1.3, PC1 = 192.168.1.4.

Вимоги до звіту

Звіт має містити:
1) Заповнену таблицю адресації;
2) Скріншот топології мережі в CPT;
3) Скріншоти виводу команд `show ip interface brief` та `show running-config | include username`;
4) Скріншоти результатів ping між усіма вузлами;
5) Скріншот, що підтверджує запит пароля при вході через `enable`;
6) Відповіді на контрольні запитання.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Які режими роботи існують у Cisco IOS? Опишіть характерне запрошення (prompt) кожного режиму та команди переходу між ними.
2. У чому різниця між командами `enable secret` та `enable password`? Яку з них рекомендується використовувати і чому?
3. Що таке `running-config` та `startup-config`? Де кожен з них зберігається? Що станеться з налаштуваннями, якщо не зберегти конфігурацію перед вимкненням пристрою?
4. Що таке рівні привілеїв у Cisco IOS? Яке значення мають рівні 1 та 15? Навіщо використовуються рівні 2–14?
5. У чому різниця між командами `login` та `login local` при налаштуванні ліній `console` та `VTY`?
6. Чому інтерфейси маршрутизатора Cisco після ввімкнення знаходяться в стані `administratively down`? Яка команда їх активує?
7. Що таке SVI (Switch Virtual Interface) і навіщо вона потрібна на комутаторі? Якій VLAN вона відповідає за замовчуванням?
8. Яка команда дозволяє переглянути лише рядки конфігурації, що містять слово `'username'`? Запишіть повний синтаксис.
9. Що означають стани `up/up`, `administratively down/down` та `down/down` у виводі команди `show ip interface brief`?
10. Навіщо в мережах медичних закладів важливо використовувати окремі облікові записи для різних адміністраторів замість спільного пароля? Які ризики усуває такий підхід?

Лабораторна робота №3.

Побудова локальної мережі. Протоколи канального рівня.

Мета роботи: Вивчити принципи роботи мереж на канальному рівні моделі OSI: механізм комутації кадрів на основі MAC-адрес, процес навчання комутатора та побудову таблиці MAC-адрес. Зрозуміти поняття широкомовного домену та проблему петель комутації. Ознайомитися з принципами роботи протоколу Spanning Tree Protocol (STP). Набути практичних навичок побудови локальної мережі з кількох комутаторів у Cisco Packet Tracer, перевірки таблиці MAC-адрес та стану STP-портів

Теоретичні відомості:

Канальний рівень моделі OSI та його роль у локальній мережі

Модель OSI (Open Systems Interconnection) описує роботу мережевих протоколів як набір із семи рівнів. Кожен рівень виконує конкретну функцію і взаємодіє лише з сусідніми рівнями.
Канальний рівень (Data Link Layer, рівень 2) відповідає за передачу даних між пристроями в межах однієї фізичної мережі. Основна одиниця даних на цьому рівні – кадр (frame). Канальний рівень забезпечує:

- адресацію в межах локальної мережі (MAC-адреси);
- виявлення та виправлення помилок передачі (FCS – Frame Check Sequence);
- управління доступом до середовища передачі (у бездротових мережах – CSMA/CA);
- комутацію кадрів між портами комутатора.

Пристрої канального рівня – це комутатори (switches) та мости (bridges). Вони передають кадри між своїми портами, орієнтуючись виключно на MAC-адреси, і не «бачать» IP-адрес.

MAC-адреса: структура та призначення

MAC-адреса (Media Access Control address) – унікальний ідентифікатор мережевого інтерфейсу, що присвоюється виробником обладнання і зберігається у постійній пам'яті мережевої карти (NIC). MAC-адреса є 48-бітним числом і записується у шістнадцятковому форматі.

```
MAC-адреса:  AA:BB:CC:DD:EE:FF
             |           |
         OUI (3 байти)   NIC (3 байти)
       (ідентифікатор    (унікальний номер
        виробника)        пристрою)
```

Рисунок 3.1 – Структура MAC-адреси

OUI (Organizationally Unique Identifier) – перші три байти, що ідентифікують виробника мережевого обладнання. Наприклад, префікс 00:50:56 належить VMware, а 00:1A:2B – Cisco Systems.
Спеціальна MAC-адреса **FF:FF:FF:FF:FF:FF** – це широкомовна (broadcast) адреса. Кадр з такою адресою призначення надсилається всім пристроям у межах одного широкомовного домену.

Принцип роботи комутатора. Таблиця MAC-адрес

Комутатор (switch) – основний пристрій локальної мережі. Він з'єднує кілька пристроїв і передає кадри між ними вибірково: лише на той порт, до якого підключений пристрій-отримувач. Це принципово відрізняє комутатор від концентратора (hub), який передавав кадри одразу на всі порти.

Для вибіркової передачі комутатор підтримує таблицю MAC-адрес (CAM-таблицю або MAC address table) – базу даних відповідностей MAC-адрес та номерів портів.

Процес навчання комутатора (MAC Learning)

Комутатор не знає MAC-адрес з самого початку – він навчається динамічно:

1. Коли на порт надходить кадр, комутатор зчитує MAC-адресу відправника та записує її в таблицю разом із номером порту.
2. Комутатор шукає MAC-адресу отримувача в таблиці.
3. Якщо адреса знайдена – кадр надсилається лише на відповідний порт (unicast forwarding).
4. Якщо адреса не знайдена – кадр надсилається на всі порти, крім порту-відправника (flooding). Це схоже на поведінку концентратора, але лише для невідомих адрес.
5. Широкомовний кадр (`broadcast FF:FF:FF:FF:FF:FF`) завжди надсилається на всі порти (flooding).

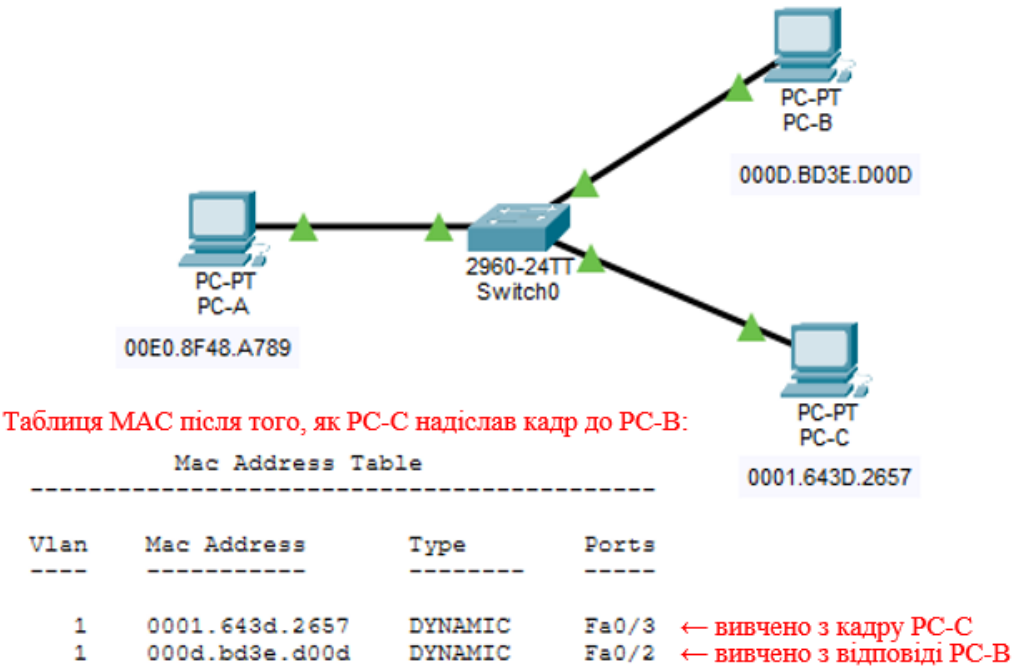

Рисунок 3.2 – Процес навчання комутатора та таблиця MAC-адрес

Широкомовний домен та його розмір

Широкомовний домен (broadcast domain) – це сукупність усіх пристроїв, які отримують широкомовний кадр, надісланий будь-яким із них. У мережі з одним або кількома комутаторами (без маршрутизаторів) всі пристрої належать до одного широкомовного

домену.
Маршрутизатор розділяє широкомовні домени: широкомовний трафік не перетинає межі маршрутизатора. Саме тому у великих мережах (наприклад, лікарняних) мережу ділять на підмережі за допомогою маршрутизатора або VLAN – щоб широкомовний трафік одного відділення не перевантажував мережу іншого.

Чому розмір широкомовного домену важливий для медичних мереж
У мережі лікарні можуть працювати сотні пристроїв: комп'ютери лікарів, медичні монітори, УЗД-апарати, IP-телефони. Якщо всі вони перебувають в одному великому широкомовному домені, широкомовний трафік (ARP-запити, DHCP-запити тощо) може суттєво навантажити мережу та сповільнити роботу критично важливого обладнання. Поділ на підмережі та VLAN вирішує цю проблему (докладніше – у ЛР №7).

Проблема петель комутації та протокол STP

При побудові мережі з кількох комутаторів виникає спокуса додати резервні з'єднання між ними – щоб мережа продовжувала працювати при обриві одного кабелю. Проте без додаткового механізму це призводить до катастрофічної проблеми – петлі комутації (switching loop).

Що таке петля комутації

Петля комутації виникає, коли між комутаторами існує більше одного шляху. Широкомовний кадр (наприклад, ARP-запит) починає безкінечно циркулювати між комутаторами, копіюючись та розмножуючись з кожним проходженням. За лічені секунди це повністю блокує мережу – явище відоме як broadcast storm (широкомовний шторм). Саме для вирішення цієї проблеми був розроблений протокол STP.

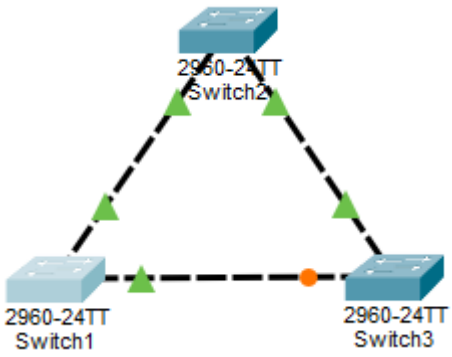

Рисунок 3.3 – Топологія з потенційною петлею комутації

На рисунку 3.3 комутатори, з'єднані у трикутник: без STP – broadcast storm! з STP – один порт заблокований (резерв)

Spanning Tree Protocol (STP, IEEE 802.1D)

STP (Spanning Tree Protocol) – протокол канального рівня, що автоматично визначає та блокує надлишкові з'єднання між комутаторами, залишаючи активними лише ті, що утворюють дерево без петель (spanning tree). При відмові активного з'єднання STP автоматично активує резервне.

Ключові поняття STP

Термін	Опис
Root Bridge	Кореневий комутатор – центр дерева STP. Обирається за найменшим Bridge ID (пріоритет + MAC). Всі шляхи будуються відносно нього.
Bridge ID	Унікальний ідентифікатор комутатора = Пріоритет (за замовч. 32768) + MAC-адреса комутатора.
Root Port	Порт не-кореневого комутатора, що знаходиться найближче до Root Bridge (з найменшою вартістю шляху).
Designated Port	Призначений порт – кращий порт на кожному сегменті мережі для досягнення Root Bridge. Завжди активний.
Blocked Port	Заблокований порт – надлишкове з'єднання, заблоковане STP для запобігання петлям. Не передає трафік, але слухає BPDU.
BPDU	Bridge Protocol Data Unit – службові кадри STP, якими обмінюються комутатори для узгодження топології.
PortFast	Функція Cisco: порт одразу переходить у стан Forwarding, минаючи затримки STP. Використовується на портах з кінцевими пристроями.

Таблиця 3.1 – Ключові поняття Spanning Tree Protocol

Стани портів STP

Стан порту	Тривалість	Що відбувається
Blocking	до 20 сек	Слухає BPDU, не передає кадри даних, не навчається MAC
Listening	15 сек	Обробляє BPDU, бере участь у виборі ролей, не передає дані
Learning	15 сек	Навчається MAC-адресам, не передає дані користувача
Forwarding	постійно	Повноцінна передача кадрів – нормальний робочий стан
Disabled	–	Адміністративно вимкнений (shutdown)

Таблиця 3.2 – Стани портів STP (класичний IEEE 802.1D)

Чому CPT показує помаранчевий колір на портах при підключенні?
Коли ви з'єднуєте два комутатори, порти спочатку показуються помаранчевим кольором – це нормально! Порт проходить через стани Listening і Learning (разом ~30 секунд), перш ніж стати зеленим (Forwarding). Натисніть кнопку швидкого переходу (>>\|) у CPT, щоб прискорити симуляцію, або просто зачекайте.

Сучасні версії STP

RSTP (Rapid STP, IEEE 802.1w) – прискорена версія STP. Час збіжності скорочено з ~50 секунд до 1–2 секунд. Замінила класичний STP у більшості сучасних мереж.
PVST+ (Per-VLAN Spanning Tree Plus) – реалізація Cisco, що підтримує окремий екземпляр STP для кожного VLAN. Це дозволяє балансувати навантаження між резервними каналами.
MSTP (Multiple STP, IEEE 802.1s) – стандарт IEEE для групування VLAN з єдиним екземпляром STP.

На комутаторах Cisco Catalyst за замовчуванням увімкнено PVST+ (або Rapid PVST+ на новіших моделях), тому у Cisco Packet Tracer ви побачите саме цей варіант.

Команди налаштування та перевірки комутатора

Перегляд таблиці MAC-адрес

```
! Повна таблиця MAC-адрес комутатора:
Switch# show mac address-table

          Mac Address Table
-------------------------------------------
Vlan  Mac Address       Type        Ports
----  -----------       --------    -----
   1  00d0.bca2.1234    DYNAMIC     Fa0/1
   1  00e0.f7c3.5678    DYNAMIC     Fa0/2
   1  00a0.1122.3344    DYNAMIC     Fa0/3

! Таблиця MAC для конкретного VLAN:
Switch# show mac address-table vlan 1

! Таблиця MAC для конкретного порту:
Switch# show mac address-table interface FastEthernet0/1

! Кількість записів у таблиці:
Switch# show mac address-table count
```

Приклад 3.1 – Перегляд таблиці MAC-адрес комутатора

Перегляд стану STP

```
! Стан STP для VLAN 1 (хто Root Bridge, стан портів):
Switch# show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.4298.ABCD
             This bridge is the root

  Bridge ID  Priority    32769
             Address     0001.4298.ABCD

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- ----
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/24           Root FWD 19        128.24   P2p

! Короткий підсумок STP по всіх VLAN:
Switch# show spanning-tree summary

! Деталі STP для конкретного інтерфейсу:
Switch# show spanning-tree interface FastEthernet0/1
```

Приклад 3.2 – Перегляд стану Spanning Tree Protocol

Налаштування пріоритету Root Bridge

За замовчуванням Root Bridge обирається автоматично – це комутатор із найменшим Bridge ID. Щоб гарантовано зробити певний комутатор кореневим, адміністратор знижує його пріоритет:

```
! Встановити пріоритет STP вручну (менше = більший пріоритет, крок 4096):
Switch(config)# spanning-tree vlan 1 priority 4096

! Або використати зручну команду Cisco (автоматично встановлює 24576):
Switch(config)# spanning-tree vlan 1 root primary

! Зробити комутатор резервним Root Bridge:
Switch(config)# spanning-tree vlan 1 root secondary
```

Приклад 3.3 – Налаштування пріоритету Root Bridge

PortFast та BPDU Guard

Порти, підключені до кінцевих пристроїв (PC, принтерів, медичного обладнання), не потребують проходження через стани STP – це лише затримує їх ввімкнення. Функція PortFast дозволяє таким портам одразу переходити у стан Forwarding.

```
! Увімкнути PortFast на конкретному порту:
Switch(config)# interface FastEthernet0/1
Switch(config-if)# spanning-tree portfast
Switch(config-if)# exit

! Увімкнути BPDU Guard (захист: якщо на PortFast-порт прийде BPDU
! від іншого комутатора – порт автоматично вимкнеться):
Switch(config)# interface FastEthernet0/1
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)# exit

! Увімкнути PortFast та BPDU Guard глобально на всіх access-портах:
Switch(config)# spanning-tree portfast default
Switch(config)# spanning-tree portfast bpduguard default
```

Приклад 3.4 – Налаштування PortFast та BPDU Guard

Увага: PortFast тільки для кінцевих пристроїв!

Ніколи не вмикайте PortFast на портах, до яких підключені інші комутатори! Якщо між комутаторами є петля, PortFast-порт одразу перейде у Forwarding і не дасть STP усунути петлю. BPDU Guard є додатковим захистом: він автоматично вимикає порт (переводить в err-disabled), якщо на нього приходить BPDU від комутатора.

Корисні команди перевірки комутатора

Команда	Що показує
`show mac address-table`	Вся таблиця MAC-адрес
`show mac address-table count`	Кількість записів у MAC-таблиці
`show spanning-tree vlan 1`	Стан STP для VLAN 1: Root Bridge, ролі та стани портів
`show spanning-tree summary`	Загальний підсумок STP по всіх VLAN
`show spanning-tree interface Fa0/1`	Роль та стан STP для конкретного порту
`show interfaces status`	Стан усіх портів: connected/notconnect, speed, duplex
`show interfaces FastEthernet0/1`	Детальна статистика порту: помилки, CRC, лічильники
`show ip interface brief`	IP-адреса SVI (VLAN-інтерфейсу) та її стан

`clear mac address-table dynamic`	Очистити динамічну MAC-таблицю (для тестування)

Таблиця 3.3 – Команди перевірки стану комутатора Cisco

Діагностика проблем локальної мережі

Алгоритм усунення несправностей

1. Перевірте фізичний рівень: індикатори портів у CPT (зелений = active, помаранчевий = STP converging, червоний = проблема). У реальній мережі – стан LED на комутаторі.
2. Виконайте `show interfaces status` – переконайтесь, що потрібні порти мають статус `connected`.
3. Перевірте MAC-таблицю: `show mac address-table`. Якщо MAC-адреса певного PC відсутня – пакети від нього ще не надходили або таблиця вже очищена.
4. Перевірте стан STP: `show spanning-tree vlan 1`. Переконайтесь, що порти перебувають у стані FWD, а не BLK.
5. Виконайте `ping` між пристроями. Якщо перший `ping – timeout` (ARP-resolution) – це нормально. Повторний має пройти.
6. Якщо `ping` не проходить навіть після кількох спроб – перевірте IP-адреси та маски на обох хостах командою ipconfig.

Типові проблеми та їх вирішення

Симптом	Причина	Вирішення
Порт помаранчевий довгий час	STP: порт у стані Listening/Learning	Зачекати ~30 сек або натиснути >> в CPT
Порт залишається помаранчевим завжди	STP заблокував порт (BLK) – петля в топології	`show spanning-tree` – порт BLK є нормою при надлишкових зв'язках
ping між PC не проходить (інтерфейси зелені)	Різні підмережі або неправильний шлюз	Перевірити IP-адреси та маски на обох PC
MAC-адреса відсутня у таблиці	PC ще не генерував трафік	Виконати `ping` – після цього MAC з'явиться
Мережа повністю зависає (CPT гальмує)	Broadcast storm через петлю без STP	Переконатись, що STP увімкнено; прибрати надлишкові зв'язки
Порт перейшов в err-disabled	Спрацював BPDU Guard (BPDU на PortFast-порту)	`shutdown + no shutdown` на порту; перевірити, що підключено

Таблиця 3.4 – Типові проблеми локальної мережі та методи їх усунення

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

Завдання складається з двох частин. У першій частині будується проста мережа з одним комутатором і досліджується таблиця MAC-адрес. У другій частині будується мережа з трьома комутаторами у топології трикутника з резервними з'єднаннями та вивчається робота STP.

Порядок виконання

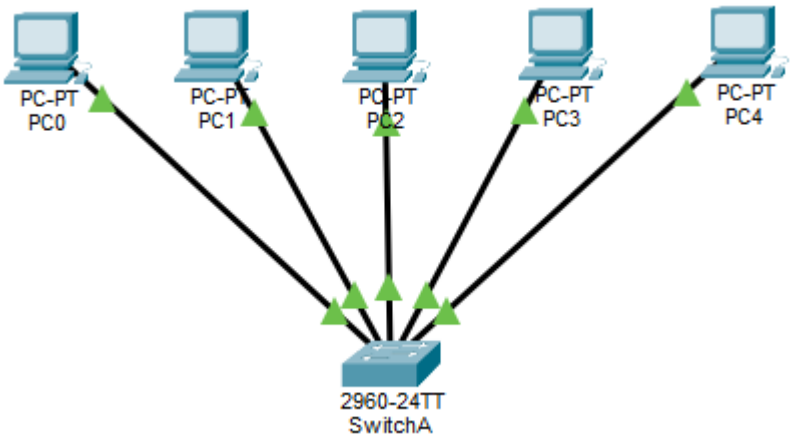

Рисунок 3.4 – Топологія мережі для першої частини лабораторної роботи № 3

Частина 1. Дослідження таблиці MAC-адрес

1. Створіть новий проект у Cisco Packet Tracer.
2. Розмістіть один комутатор Catalyst 2960 та п'ять PC.
3. З'єднайте PC0–PC4 з портами Fa0/1–Fa0/5 комутатора (Straight-through або Auto).
4. Налаштуйте IP-адреси на всіх PC відповідно до вашого варіанту (одна підмережа /24).
5. Відкрийте CLI комутатора та виконайте: `show mac address-table`. Зробіть скріншот. Таблиця має бути порожньою або містити лише статичні записи.
6. Виконайте `ping` з PC0 до PC1. Потім знову `show mac address-table`. Зафіксуйте, які MAC-адреси з'явилися та на яких портах.
7. Виконайте `ping` з PC2 до PC4. Знову `show mac address-table`. Порівняйте з попереднім результатом.
8. Виконайте `show interfaces status` – зробіть скріншот.
9. Налаштуйте PortFast на всіх портах Fa0/1–Fa0/5: `interface range Fa0/1-5` → `spanning-tree portfast`.
10. Збережіть конфігурацію комутатора.

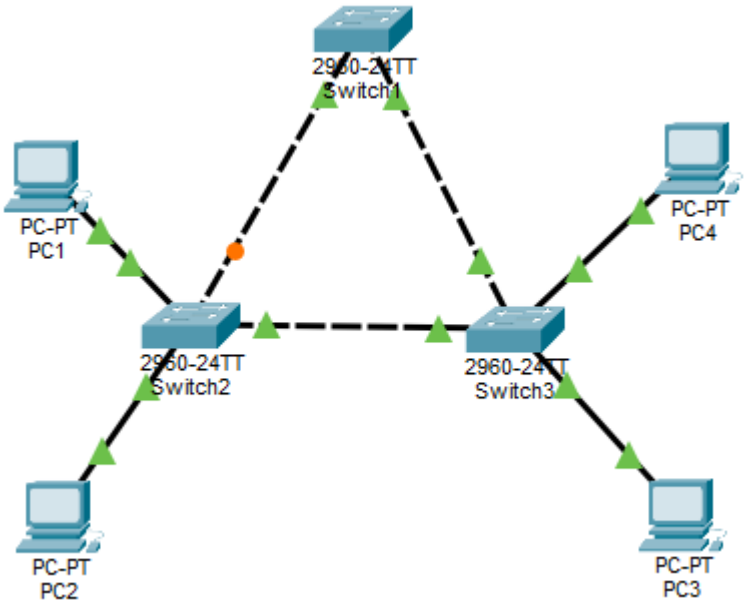

Рисунок 3.5 – Топологія мережі для першої частини лабораторної роботи № 3

Частина 2. Дослідження STP у топології з трьома комутаторами

11. Додайте до проекту ще два комутатори Catalyst 2960 (Switch2, Switch3) та три PC (по одному до кожного комутатора).
12. З'єднайте комутатори між собою Straight-through кабелями у трикутник: Switch-1↔Switch2 (Fa0/23), Switch2↔Switch3 (Fa0/23), Switch1↔Switch3 (Fa0/24). Це створює надлишкові з'єднання.
13. Підключіть PC1 до Switch2 (Fa0/1), PC2 до Switch2 (Fa0/2), PC3 до Switch3 (Fa0/1), PC4 до Switch3 (Fa0/2).
14. Налаштуйте IP-адреси на PC1, PC2, PC3, PC4 відповідно до варіанту (та сама підмережа).
15. Зачекайте, поки всі індикатори стануть зеленими або помаранчевими. Зробіть скріншот топології.
16. На кожному комутаторі виконайте `show spanning-tree vlan 1` та зафіксуйте: хто є Root Bridge, які порти Forwarding, який порт Blocked.
17. Зробіть `show spanning-tree summary` на всіх трьох комутаторах.
18. Зробіть Switch-1 гарантованим Root Bridge: `spanning-tree vlan 1 root primary`. Повторіть `show spanning-tree vlan 1`.
19. Виконайте ping з PC1 до PC4 – переконайтесь, що зв'язок є незважаючи на заблокований порт.
20. Збережіть конфігурацію всіх комутаторів.

Таблиця адресації (заповнити у звіті)

Пристрій	IP-адреса	Маска підмережі	Підключений до
PC0			SwitchA Fa0/1
PC1			SwitchA Fa0/2
PC2			SwitchA Fa0/3
PC3			SwitchA Fa0/4
PC4			SwitchA Fa0/5

PC1			Switch2 Fa0/1
PC2			Switch2 Fa0/2
PC3			Switch3 Fa0/1
PC4			Switch3 Fa0/2

Таблиця 3.5 – Таблиця адресації

Варіанти завдань

Усі пристрої одного варіанту знаходяться в одній підмережі /24. Адреси PC призначаються послідовно починаючи з першої хост-адреси мережі.

Вар.	Мережа /24	Адреси PC0–PC4 (Частина 1)	Адреси PC1–PC4 (Частина 2)
1	192.168.1.0/24	192.168.1.1 – 192.168.1.5	192.168.1.10 – 192.168.1.13
2	192.168.2.0/24	192.168.2.1 – 192.168.2.5	192.168.2.10 – 192.168.2.13
3	192.168.3.0/24	192.168.3.1 – 192.168.3.5	192.168.3.10 – 192.168.3.13
4	192.168.4.0/24	192.168.4.1 – 192.168.4.5	192.168.4.10 – 192.168.4.13
5	192.168.5.0/24	192.168.5.1 – 192.168.5.5	192.168.5.10 – 192.168.5.13
6	10.10.1.0/24	10.10.1.1 – 10.10.1.5	10.10.1.10 – 10.10.1.13
7	10.10.2.0/24	10.10.2.1 – 10.10.2.5	10.10.2.10 – 10.10.2.13
8	10.20.1.0/24	10.20.1.1 – 10.20.1.5	10.20.1.10 – 10.20.1.13
9	172.16.1.0/24	172.16.1.1 – 172.16.1.5	172.16.1.10 – 172.16.1.13
10	172.16.2.0/24	172.16.2.1 – 172.16.2.5	172.16.2.10 – 172.16.2.13
11	172.16.3.0/24	172.16.3.1 – 172.16.3.5	172.16.3.10 – 172.16.3.13
12	172.16.4.0/24	172.16.4.1 – 172.16.4.5	172.16.4.10 – 172.16.4.13
13	10.30.1.0/24	10.30.1.1 – 10.30.1.5	10.30.1.10 – 10.30.1.13
14	10.30.2.0/24	10.30.2.1 – 10.30.2.5	10.30.2.10 – 10.30.2.13
15	10.30.3.0/24	10.30.3.1 – 10.30.3.5	10.30.3.10 – 10.30.3.13

Таблиця 3.6 – Варіанти завдань для лабораторної роботи № 3

Вимоги до звіту

Звіт має містити:

1) Заповнену таблицю адресації;
2) Скріншот порожньої MAC-таблиці та після виконання ping;
3) Скріншот `show spanning-tree vlan 1` на всіх трьох комутаторах Частини 2;
4) Скріншот топології з позначенням заблокованого порту STP;
5) Скріншот результатів `ping` між PC1 та PC4;
6) Відповіді на контрольні запитання.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке MAC-адреса? З яких частин вона складається та яку довжину має? Яка MAC-адреса є широкомовною?
2. Опишіть алгоритм роботи комутатора при отриманні кадру: що відбувається, якщо MAC-адреса отримувача відома і невідома в таблиці?
3. Що таке широкомовний домен? Чим комутатор відрізняється від маршрутизатора з точки зору обробки широкомовного трафіку?
4. Що таке петля комутації і чому вона небезпечна? Що таке broadcast storm?
5. Що таке Spanning Tree Protocol (STP)? Яку проблему він вирішує і яким чином?
6. Що таке Root Bridge? За яким критерієм він обирається? Як адміністратор може вплинути на вибір Root Bridge?
7. Перелічіть стани портів у класичному STP (IEEE 802.1D) та вкажіть їх тривалість. Чому між з'єднанням кабелю і початком передачі трафіку проходить ~30 секунд?
8. Що таке PortFast? На яких портах його слід вмикати, а на яких – категорично не можна? Чому?
9. Яка команда дозволяє переглянути поточний стан STP: хто є Root Bridge, які порти Forwarding і Blocked?
10. Яка команда дозволяє переглянути таблицю MAC-адрес комутатора? Що означає тип запису DYNAMIC і що означало б STATIC?

Лабораторна робота №4.

Налаштування статичної маршрутизації на обладнанні Cisco.

Мета роботи: Вивчити принципи роботи маршрутизації на мережевому рівні та будову таблиці маршрутизації Cisco IOS. Зрозуміти різницю між безпосередньо підключеними, статичними та динамічними маршрутами. Отримати практичні навички налаштування статичних маршрутів між кількома мережами в Cisco Packet Tracer, включаючи налаштування маршруту за замовчуванням. Навчитися перевіряти коректність маршрутизації командами show ip route, ping та traceroute.

ТЕОРЕТИЧНІ ВІДОМОСТІ:

Що таке маршрутизація і навіщо вона потрібна

У попередніх лабораторних роботах ми будували мережі, де всі пристрої знаходилися в одній підмережі та з'єднувалися через комутатор. Комутатор працює на канальному рівні (рівень 2 моделі OSI) і передає кадри в межах однієї підмережі, орієнтуючись на MAC-адреси.

Проте реальні мережі – і мережі медичних закладів не є винятком – складаються з багатьох підмереж: окрема підмережа для відділення реанімації, для адміністрації, для медичних приладів, для гостьового Wi-Fi тощо. Щоб пакети могли переміщатися між різними підмережами, потрібен пристрій рівня 3 – маршрутизатор (router).

Маршрутизація (routing) – це процес визначення оптимального шляху для передачі пакетів між різними мережами. Маршрутизатор аналізує IP-адресу призначення у кожному пакеті та вирішує, через який інтерфейс (і до якого наступного пристрою) його відправити.

Таблиця маршрутизації (Routing Table)

Основний інструмент маршрутизатора – таблиця маршрутизації. Це база даних, що зберігається в оперативній пам'яті і містить інформацію про всі відомі мережі та шляхи до них. Для перегляду таблиці маршрутизації використовується команда:

```
Router# show ip route
```

Приклад виводу команди `show ip route`:

```
Codes: C - connected, S - static, R - RIP, O - OSPF,
       * - candidate default, ... (скорочено)

Gateway of last resort is 10.0.0.2 to network 0.0.0.0

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    10.0.0.0/30    is directly connected, Serial0/0/0
S    192.168.2.0/24 [1/0] via 10.0.0.2
S    192.168.3.0/24 [1/0] via 10.0.0.2
S*   0.0.0.0/0      [1/0] via 10.0.0.2
```

Приклад 4.1 – Вивід команди `show ip route`

Розберемо значення кожного елементу:

Позначка	Приклад	Значення
C	C 192.168.1.0/24	Directly connected – мережа безпосередньо підключена до інтерфейсу маршрутизатора
S	S 192.168.2.0/24	Static – статичний маршрут, доданий адміністратором вручну
R	R 192.168.5.0/24	RIP – маршрут, отриманий від протоколу динамічної маршрутизації RIP
O	O 10.5.0.0/24	OSPF – маршрут, отриманий від протоколу OSPF
S*	S* 0.0.0.0/0	Static default route – статичний маршрут за замовчуванням
[1/0]	[1/0] via ...	[Адміністративна відстань / Метрика] – пріоритет маршруту

Таблиця 4.1 – Позначки у таблиці маршрутизації Cisco IOS

Адміністративна відстань (AD) – показник довіри до джерела маршруту. Чим менше значення – тим вищий пріоритет:

Джерело маршруту	Адміністративна відстань (AD)
Безпосередньо підключена мережа (Connected)	0
Статичний маршрут (Static)	1
OSPF	110
RIP	120

Таблиця 4.2 – Адміністративна відстань різних джерел маршрутів

Статична маршрутизація

Статична маршрутизація – це спосіб, при якому маршрути до мереж вводяться адміністратором вручну. Маршрутизатор не «дізнається» про мережі автоматично – він знає лише те, що йому сказали.

Переваги статичної маршрутизації:

- Простота і передбачуваність – маршрути незмінні, якщо не втрутиться адміністратор.
- Відсутність трафіку маршрутизаційних протоколів – не навантажує мережу.
- Висока безпека – неможливо підробити маршрути через протокол.
- Ідеально підходить для невеликих мереж або мереж зі стабільною топологією.

Недоліки статичної маршрутизації:

- Масштабування: у великій мережі кількість маршрутів стає некерованою.
- Відсутність автоматичного відновлення при відмові каналу – потрібне втручання адміністратора.

Де застосовується у медичних мережах

Статична маршрутизація ідеально підходить для невеликих медичних закладів (амбулаторія, невелика клініка) з постійною топологією мережі. Великі лікарні з розгалуженою інфраструктурою використовують динамічну маршрутизацію (OSPF), але навіть там статичні маршрути часто застосовуються для окремих сегментів або маршруту за замовчуванням до провайдера.

Синтаксис команди `ip route`

Для додавання статичного маршруту використовується команда `ip route` у режимі Global Configuration:

```
Router(config)# ip route <мережа-призначення> <маска> <next-hop або вихідний інтерфейс> [AD]
```

Параметри команди:

Параметр	Опис
`<мережа-призначення>`	IP-адреса мережі, до якої потрібно прокласти маршрут
`<маска>`	Маска підмережі призначення (у форматі 255.x.x.x, не CIDR)
`<next-hop>`	IP-адреса наступного маршрутизатора (Next-Hop Router)
`<вихідний інтерфейс>`	Альтернатива next-hop: назва інтерфейсу, через який відправляти пакети
`[AD]`	Необов'язково: адміністративна відстань (за замовчуванням 1)

Таблиця 4.3 – Параметри команди ip route

Статичний маршрут через адресу next-hop

Найпоширеніший варіант: вказується IP-адреса наступного маршрутизатора, через який потрібно передати пакет.

```
! Маршрут до мережі 192.168.2.0/24 через маршрутизатор з адресою 10.0.0.2
Router1(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2

! Маршрут до мережі 192.168.3.0/24 через той самий next-hop
Router1(config)# ip route 192.168.3.0 255.255.255.0 10.0.0.2
```

Приклад 4.2 – Статичні маршрути через адресу next-hop

Статичний маршрут через вихідний інтерфейс

Альтернативний варіант: замість IP-адреси наступного маршрутизатора вказується локальний інтерфейс, через який виходить трафік. Частіше застосовується на Serial-з'єднаннях типу точка-точка.

```
! Маршрут через вихідний Serial-інтерфейс

Router1(config)# ip route 192.168.2.0 255.255.255.0 Serial0/0/0
```

Приклад 4.3 – Статичний маршрут через вихідний інтерфейс

Маршрут за замовчуванням (Default Route)

Маршрут за замовчуванням (default route) – це особливий маршрут, що відповідає будь-якій мережі призначення, для якої немає більш конкретного запису в таблиці. Він позначається як 0.0.0.0/0 і часто називається «маршрутом останньої надії» (gateway of last resort).

Маршрут за замовчуванням використовується для виходу в Інтернет: замість того, щоб зберігати мільйони маршрутів до всіх мереж Інтернету, маршрутизатор просто «не знає куди» – надсилає пакет до провайдера.

```
! Маршрут за замовчуванням: всі невідомі пакети – до 10.0.0.2 (провайдер або прикордонний роутер)

Router1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

Приклад 4.4 – Налаштування маршруту за замовчуванням

Маска 0.0.0.0 для default route

Маска 0.0.0.0 означає, що жоден біт не перевіряється при порівнянні адреси призначення з цим маршрутом. Тому він підходить до будь-якої адреси. Cisco IOS показує такий маршрут з позначкою S та рядком 'Gateway of last resort is X.X.X.X to network 0.0.0.0' у виводі show ip route.*

Типова топологія зі статичною маршрутизацією

Розглянемо мережу з трьох підмереж, що з'єднані двома маршрутизаторами. Це типова схема для медичного закладу, де окремі підмережі виділені для різних відділень.

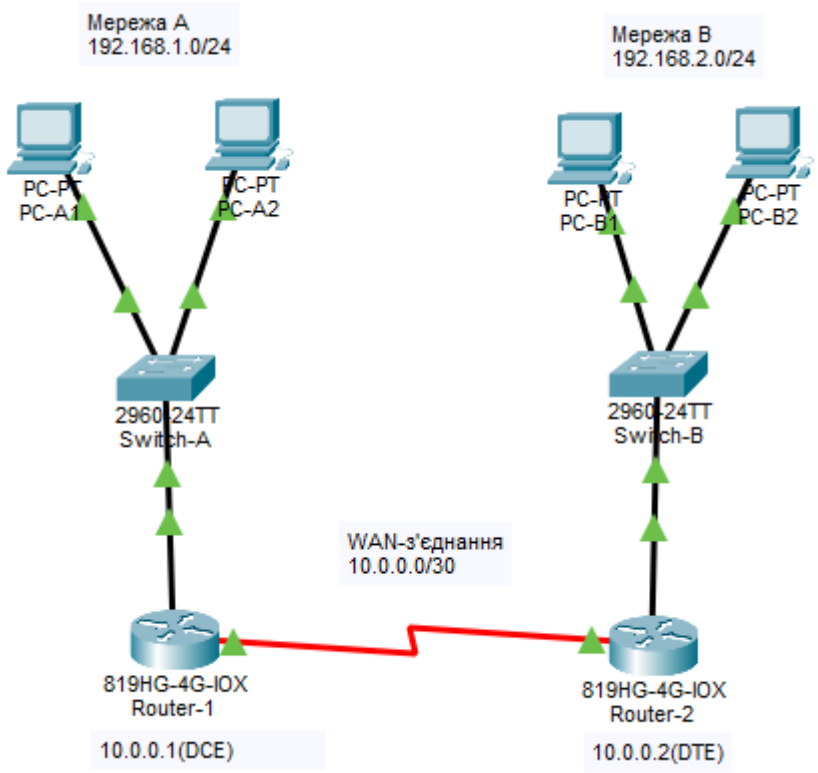

Рисунок 4.1 – Топологія з двома маршрутизаторами та трьома мережами

Налаштування Router-1

```
Router(config)# hostname Router-1

! Інтерфейс до LAN (мережа A)
Router-1(config)# interface FastEthernet0/0
Router-1(config-if)# ip address 192.168.1.1 255.255.255.0
Router-1(config-if)# description === LAN: Viddilennya A ===
Router-1(config-if)# no shutdown
Router-1(config-if)# exit
```

```
! WAN-інтерфейс (Serial – сторона DCE, потрібен clock rate)
Router-1(config)# interface Serial0/0/0
Router-1(config-if)# ip address 10.0.0.1 255.255.255.252
Router-1(config-if)# clock rate 64000
Router-1(config-if)# no shutdown
Router-1(config-if)# exit

! Статичний маршрут до мережі B через Router-2
Router-1(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2
```

Приклад 4.5 – Повне налаштування Router-1

Налаштування Router-2

```
Router(config)# hostname Router-2

! Інтерфейс до LAN (мережа B)
Router-2(config)# interface FastEthernet0/0
Router-2(config-if)# ip address 192.168.2.1 255.255.255.0
Router-2(config-if)# description === LAN: Viddilennya B ===
Router-2(config-if)# no shutdown
Router-2(config-if)# exit

! WAN-інтерфейс (Serial – сторона DTE, clock rate не потрібен)
Router-2(config)# interface Serial0/0/0
Router-2(config-if)# ip address 10.0.0.2 255.255.255.252
Router-2(config-if)# no shutdown
Router-2(config-if)# exit

! Статичний маршрут до мережі A через Router-1
Router-2(config)# ip route 192.168.1.0 255.255.255.0 10.0.0.1
```

Приклад 4.6 – Повне налаштування Router-2

DCE та DTE на Serial-інтерфейсах

У Cisco Packet Tracer при з'єднанні двох маршрутизаторів Serial-кабелем один кінець є DCE (Data Circuit-terminating Equipment), інший – DTE (Data Terminal Equipment). Сторона DCE задає тактову частоту командою clock rate. Визначити, який інтерфейс є DCE, можна командою: show controllers Serial0/0/0. У CPT зазвичай символом годинника позначена DCE-сторона кабелю.

Перевірка маршрутизації – команди `show` та діагностика

Перегляд таблиці маршрутизації

```
! Повна таблиця маршрутизації:
Router-1# show ip route

! Лише статичні маршрути:
Router-1# show ip route static

! Лише безпосередньо підключені мережі:
Router-1# show ip route connected

! Детальна інформація про конкретний маршрут:
Router-1# show ip route 192.168.2.0
```

Приклад 4.7 – Команди перегляду таблиці маршрутизації

Перевірка зв'язку між мережами

```
! Ping з маршрутизатора до вузлів різних мереж:
Router-1# ping 192.168.2.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms

! Якщо маршруту немає:
Router-1# ping 192.168.2.1
.....
Success rate is 0 percent (0/5)
```

Приклад 4.8 – Перевірка зв'язку командою `ping`

У виводі `ping` символ **!** означає успішну відповідь, **.** – тайм-аут (пакет загублений або маршруту немає).

Трасування маршруту

```
! Traceroute – показує кожен маршрутизатор на шляху до мережі призначення:
Router-1# traceroute 192.168.2.10

Type escape sequence to abort.
Tracing the route to 192.168.2.10

  1   10.0.0.2     2 msec   1 msec   2 msec
  2   192.168.2.10 3 msec   3 msec   3 msec
```

Приклад 4.9 – Трасування маршруту командою `traceroute`

Кожен рядок виводу traceroute відповідає одному маршрутизатору (hop) на шляху пакету. Якщо на якомусь переході з'являються зірочки (***) – там пакет губиться або маршрутизатор блокує ICMP.

Перевірка стану Serial-інтерфейсу

```
! Перевірити стан та налаштування Serial-інтерфейсу:
Router-1# show interface Serial0/0/0

! Перевірити, хто є DCE (шукати 'DCE' у виводі):
Router-1# show controllers Serial0/0/0

! Коротка таблиця всіх інтерфейсів:
Router-1# show ip interface brief
```

Приклад 4.10 – Перевірка Serial-інтерфейсу

Зведена таблиця команд лабораторної роботи

Команда	Призначення
`ip route <мережа> <маска> <next-hop>`	Додати статичний маршрут через next-hop
`ip route 0.0.0.0 0.0.0.0 <next-hop>`	Маршрут за замовчуванням
`no ip route <мережа> <маска> <next-hop>`	Видалити статичний маршрут
`show ip route`	Вся таблиця маршрутизації
`show ip route static`	Лише статичні маршрути
`show ip route connected`	Лише підключені мережі
`show ip interface brief`	Стан всіх інтерфейсів
`ping <IP>`	Перевірка досяжності вузла
`traceroute <IP>`	Трасування маршруту до вузла

`show controllers Serial0/0/0`	Визначення DCE/DTE на Serial-інтерфейсі
`clock rate 64000`	Встановлення тактової частоти на DCE-інтерфейсі

Таблиця 4.4 – Команди налаштування та перевірки статичної маршрутизації

Плаваючий статичний маршрут (Floating Static Route)

Плаваючий статичний маршрут – це статичний маршрут з підвищеним значенням адміністративної дистанції (AD > 1). Він використовується як резервний: поки основний маршрут активний – плаваючий у таблиці маршрутизації не відображається і не використовується. Якщо основний маршрут зникає (наприклад, через обрив каналу) – плаваючий автоматично стає активним.

```
! Основний маршрут через оптоволокно (AD=1, стандартний):
Router1(config)# ip route 192.168.3.0 255.255.255.0 10.0.0.2

! Резервний (плаваючий) маршрут через 4G-маршрутизатор (AD=5):
! З'явиться в таблиці лише якщо основний маршрут зникне
Router1(config)# ip route 192.168.3.0 255.255.255.0 10.0.1.2 5

! Перевірка: поки обидва канали активні – видно лише основний (AD=1):
Router1# show ip route 192.168.3.0
Routing entry for 192.168.3.0/24
  Known via 'static', distance 1, metric 0
  * 10.0.0.2
```

Приклад 4.11 – Плаваючий статичний маршрут як резервний канал

Застосування у медичних мережах

Плаваючий статичний маршрут – простий спосіб організувати резервування каналу без динамічних протоколів. Наприклад: основне з'єднання між корпусами лікарні – оптоволокно (AD=1), резервне – 4G/LTE-маршрутизатор (AD=5). При обриві оптики трафік автоматично перейде на мобільний канал без жодного втручання адміністратора.

Підсумовуючий маршрут (Summary Static Route)

Якщо маршрутизатор має кілька статичних маршрутів до суміжних підмереж однієї великої мережі, їх можна об'єднати в один підсумовуючий маршрут. Це скорочує таблицю маршрутизації та спрощує управління – особливо актуально при великій кількості підмереж.

Приклад: замість чотирьох маршрутів до 192.168.0.0/24 – 192.168.3.0/24 використовуємо один /22, що охоплює всі чотири підмережі:

```
! Чотири окремі маршрути (неоптимально):
! ip route 192.168.0.0 255.255.255.0 10.0.0.2
! ip route 192.168.1.0 255.255.255.0 10.0.0.2
! ip route 192.168.2.0 255.255.255.0 10.0.0.2
! ip route 192.168.3.0 255.255.255.0 10.0.0.2

! Один підсумовуючий маршрут /22 замінює всі чотири /24:
Router1(config)# ip route 192.168.0.0 255.255.252.0 10.0.0.2

! Перевірка – в таблиці тепер один запис замість чотирьох:
Router1# show ip route static
S    192.168.0.0/22 [1/0] via 10.0.0.2
```

Приклад 4.12 – Підсумовуючий статичний маршрут

Розширений ping для перевірки маршрутизації

Окрім стандартного ping, Cisco IOS підтримує розширений ping (extended ping) – він запускається командою ping без аргументів у режимі Privileged EXEC і дає додаткові можливості для діагностики.

```
Router1# ping
Protocol [ip]:
Target IP address: 192.168.2.10
Repeat count [5]: 20
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 20, 1500-byte ICMP Echos to 192.168.2.10, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (20/20), round-trip min/avg/max = 1/2/4 ms
```

Приклад 4.13 – Розширений ping із зазначенням адреси джерела

Параметр **Source address** дозволяє вказати конкретний інтерфейс як джерело пакетів. Це перевіряє симетричність маршрутів: чи проходить трафік в обох напрямках через правильні інтерфейси. Якщо звичайний `ping` проходить, а з конкретного джерела – ні, це вказує на асиметрію маршрутизації.

Діагностика проблем маршрутизації

Помилки в статичній маршрутизації є одними з найпоширеніших у мережевій практиці. Нижче наведено систематичний підхід до їх виявлення та усунення.

Алгоритм діагностики

1. Виконайте `show ip interface brief` на обох маршрутизаторах. Всі задіяні інтерфейси мають бути `up/up`.
2. Перевірте `ping` між безпосередньо підключеними інтерфейсами (наприклад, з Router-1 до 10.0.0.2). Якщо WAN-з'єднання не працює – маршрутизація між мережами неможлива.
3. Виконайте `show ip route` і переконайтеся, що в таблиці є записи `S` для всіх потрібних мереж.
4. Перевірте симетричність маршрутів: якщо Router-1 знає про мережу B, то Router-2 обов'язково має знати про мережу A. Відсутність зворотного маршруту – найпоширеніша помилка.
5. Виконайте `ping` з кінцевого хоста і traceroute для визначення, де саме пакет зупиняється.

Типові помилки та їх симптоми

Симптом	Причина	Вирішення
`Ping` між мережами не проходить, але WAN `ping` OK	Відсутній статичний маршрут або є помилка в адресі мережі	`show ip route` – перевірити наявність та правильність маршрутів
`Ping` йде в одну сторону, назад – ні	Відсутній зворотний маршрут на іншому роутері	Додати маршрут на Router-2 до мережі відправника
Serial-інтерфейс у стані `down/down`	Немає `clock rate` на DCE або кабель не підключено	`show controllers` – перевірити DCE/DTE, додати `clock rate`
Маршрут є в таблиці, але `ping` не проходить	Неправильна IP-адреса або маска на хості	Перевірити налаштування PC: шлюз та маску підмережі
`traceroute` зупиняється на першому hop	Маршрут до наступної мережі відсутній на проміжному роутері	Додати відповідний статичний маршрут
`U (unreachable)` у виводі `traceroute`	`ICMP unreachable` – маршрут є, але хост недоступний	Перевірити IP та шлюз на кінцевому хості

Таблиця 4.5 – Типові помилки статичної маршрутизації та їх усунення

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

Завдання складається з двох частин. У першій частині будується мережа з двох маршрутизаторів та налаштовується базова статична маршрутизація. У другій – додається третій маршрутизатор і студент самостійно прокладає маршрути для зв'язку між трьома мережами.

Топологія мережі

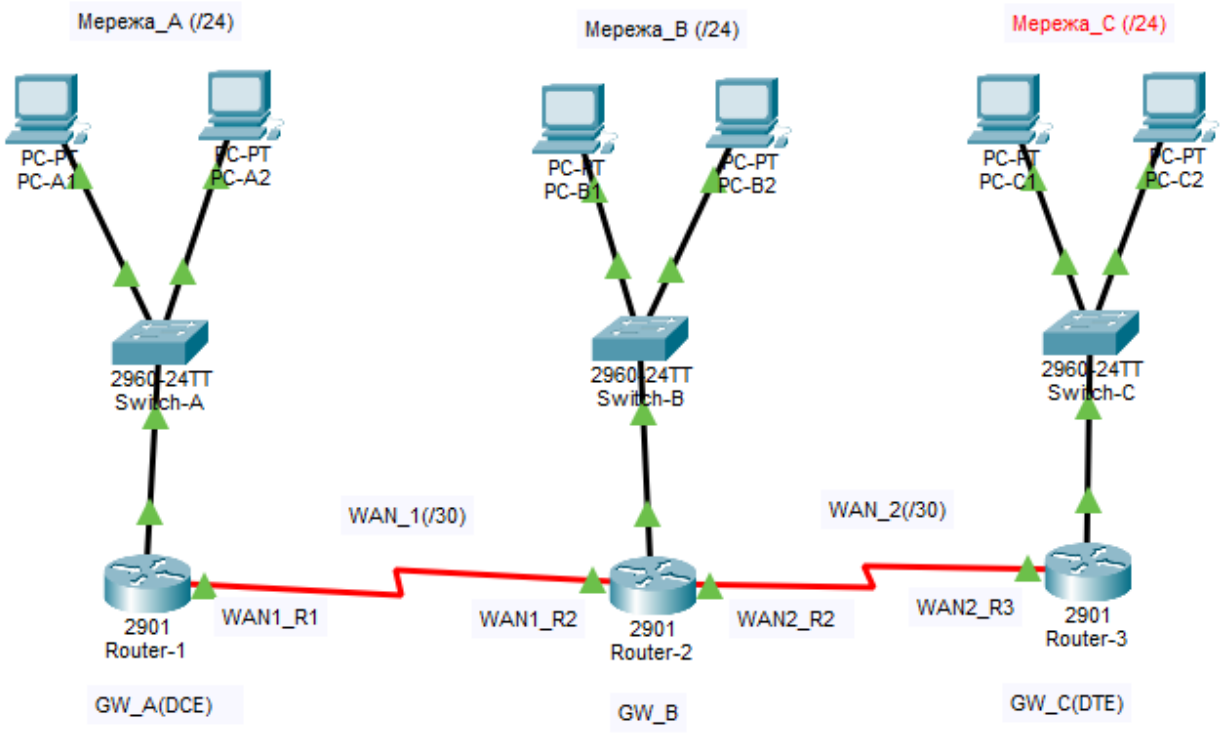

Рисунок 4.2 – Топологія мережі для лабораторної роботи № 4

Порядок виконання

Частина 1. Два маршрутизатори – базова статична маршрутизація

1. Створіть новий проект у Cisco Packet Tracer.
2. Розмістіть два маршрутизатори (1941 або 2901), два комутатори (2960), чотири PC.
3. З'єднайте PC-A1, PC-A2 зі Switch-A; PC-B1, PC-B2 зі Switch-B (Straight-through).
4. Switch-A підключіть до Router-1 (Gig0/0); Switch-B – до Router-2 (Gig0/0).
5. Додайте модулі HWIC-2T в маршрутизатори 1941 або 2901 щоб отримати можливість використовувати Serial-інтерфейси. Алгоритм додавання модуля в CPT:
   - двічі клацніть на маршрутизаторі
   - перейдіть на вкладку Physical
   - вимкніть живлення (кнопка живлення)
   - перетягніть модуль HWIC-2T у вільний слот
   - увімкніть живлення знову
6. З'єднайте Router-1 і Router-2 Serial-кабелем DCE. Починайте кабель з Router-1 (він стане DCE).

7. Налаштуйте Router-1: hostname, Gig0/0 (IP = GW_A, /24, no shutdown), Se0/0/0 (IP = WAN1_R1, /30, clock rate 64000, no shutdown), статичний маршрут до Мережі_B.
8. Налаштуйте Router-2: hostname, Gig0/0 (IP = GW_B, /24, no shutdown), Se0/0/0 (IP = WAN1_R2, /30, no shutdown), статичний маршрут до Мережі_A.
9. Налаштуйте IP-адреси на PC-A1, PC-A2 (шлюз = GW_A) та PC-B1, PC-B2 (шлюз = GW_B).
10. Перевірте: `show ip route` на обох роутерах – мають бути рядки C та S. Скріншот.
11. Ping з PC-A1 до PC-B1, PC-B2. Ping з Router-1 до GW_B. Скріншоти.
12. Tracert з PC-A1 до PC-B2 – зафіксуйте кількість переходів та їх адреси. Скріншот.

Частина 2. Третій маршрутизатор – самостійне налаштування

1. Додайте до проекту Router-3, Switch-C, PC-C1, PC-C2.
2. З'єднайте Switch-C з Router-3 (Gig0/0). З'єднайте Router-2 (Se0/0/1) з Router-3 (Se0/0/0) Serial-кабелем – DCE на стороні Router-2.
3. Самостійно налаштуйте всі інтерфейси Router-3 та Router-2 (Se0/0/1) відповідно до таблиці варіантів.
4. Додайте статичні маршрути на ВСІХ трьох маршрутизаторах так, щоб будь-який PC міг досягти будь-якого іншого PC. Врахуйте, що Router-1 тепер потребує маршруту і до Мережі_C, а Router-3 – до Мережі_A та Мережі_B.
5. Додайте маршрут за замовчуванням на Router-1 та Router-3 через Router-2 (умовний вихід в Інтернет).
6. Перевірте `show ip route` на всіх трьох маршрутизаторах. Скріншоти.
7. `Ping` з PC-A1 до PC-C2 та `tracert` – скріншоти. Переконайтесь, що пакет проходить через два маршрутизатори.
8. Збережіть конфігурацію всіх пристроїв.

Таблиця адресації (заповнити у звіті)

Пристрій / Інтерфейс	IP-адреса	Маска підмережі	Шлюз
Router-1 Gig0/0 (GW_A)		255.255.255.0	–
Router-1 Se0/0/0 (WAN1_R1)		255.255.255.252	–
Router-2 Gig0/0 (GW_B)		255.255.255.0	–
Router-2 Se0/0/0 (WAN1_R2)		255.255.255.252	–
Router-2 Se0/0/1 (WAN2_R2)		255.255.255.252	–
Router-3 Gig0/0 (GW_C)		255.255.255.0	–
Router-3 Se0/0/0 (WAN2_R3)		255.255.255.252	–
PC-A1		255.255.255.0	
PC-A2		255.255.255.0	
PC-B1		255.255.255.0	
PC-B2		255.255.255.0	
PC-C1		255.255.255.0	
PC-C2		255.255.255.0	

Таблиця 4.6 – Таблиця адресації

Варіанти завдань

Кожен варіант містить три LAN-мережі та два WAN-з'єднання. GW_A, GW_B, GW_C – перші хост-адреси відповідних мереж. Адреси PC призначаються студентом самостійно (наступні хост-адреси).

В.	**Мережа_A /24**	**Мережа_B /24**	**Мережа_C /24**	**WAN_1 /30**	**WAN1_R1**	**WAN1_R2**	**WAN_2 /30**
1	192.168.1.0	192.168.2.0	192.168.3.0	10.0.0.0	10.0.0.1	10.0.0.2	10.0.1.0
2	192.168.4.0	192.168.5.0	192.168.6.0	10.0.2.0	10.0.2.1	10.0.2.2	10.0.3.0
3	172.16.1.0	172.16.2.0	172.16.3.0	10.1.0.0	10.1.0.1	10.1.0.2	10.1.1.0
4	172.16.4.0	172.16.5.0	172.16.6.0	10.1.2.0	10.1.2.1	10.1.2.2	10.1.3.0
5	10.10.1.0	10.10.2.0	10.10.3.0	172.31.0.0	172.31.0.1	172.31.0.2	172.31.0.4
6	10.10.4.0	10.10.5.0	10.10.6.0	172.31.0.8	172.31.0.9	172.31.0.10	172.31.0.12
7	192.168.10.0	192.168.20.0	192.168.30.0	10.2.0.0	10.2.0.1	10.2.0.2	10.2.0.4
8	192.168.40.0	192.168.50.0	192.168.60.0	10.3.0.0	10.3.0.1	10.3.0.2	10.3.0.4
9	10.20.1.0	10.20.2.0	10.20.3.0	172.31.1.0	172.31.1.1	172.31.1.2	172.31.1.4
10	10.30.1.0	10.30.2.0	10.30.3.0	172.31.2.0	172.31.2.1	172.31.2.2	172.31.2.4
11	172.20.1.0	172.20.2.0	172.20.3.0	10.4.0.0	10.4.0.1	10.4.0.2	10.4.0.4
12	172.20.4.0	172.20.5.0	172.20.6.0	10.5.0.0	10.5.0.1	10.5.0.2	10.5.0.4
13	192.168.70.0	192.168.80.0	192.168.90.0	10.6.0.0	10.6.0.1	10.6.0.2	10.6.0.4
14	10.40.1.0	10.40.2.0	10.40.3.0	172.31.3.0	172.31.3.1	172.31.3.2	172.31.3.4
15	10.50.1.0	10.50.2.0	10.50.3.0	172.31.4.0	172.31.4.1	172.31.4.2	172.31.4.4

Таблиця 4.7 – Варіанти завдань для лабораторної роботи № 4

WAN2_R2 = WAN_2 + .1 (наприклад, для варіанту 1: 10.0.1.1), **WAN2_R3** = WAN_2 + .2 (10.0.1.2).

Вимоги до звіту

Звіт має містити:

1) Заповнену таблицю адресації;
2) Скріншот топології;
3) Скріншоти `show ip route` на всіх трьох маршрутизаторах (з рядками C та S);
4) Скріншот `ping` та `tracert` з PC-A1 до PC-C2 (має бути 2 переходи через маршрутизатори);
5) Перелік усіх налаштованих статичних маршрутів з поясненням кожного;
6) Відповіді на контрольні запитання.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке маршрутизація? Яка відмінність між комутатором та маршрутизатором з точки зору рівнів моделі OSI?
2. Що таке таблиця маршрутизації? Які типи записів вона може містити? Що означають позначки C та S у виводі show ip route?
3. Що таке адміністративна відстань (AD)? Яке значення AD має статичний маршрут і чому це важливо при одночасному використанні статичної та динамічної маршрутизації?
4. Запишіть команду для додавання статичного маршруту до мережі 10.5.0.0/24 через next-hop 192.168.1.1. Поясніть кожен параметр.
5. Що таке маршрут за замовчуванням (default route)? Яка адреса та маска використовується для його запису? Для чого він застосовується?
6. Чому при налаштуванні статичної маршрутизації між двома маршрутизаторами необхідно налаштовувати маршрути на ОБОХ пристроях? Що відбудеться, якщо маршрут є лише на одному?
7. Що таке DCE та DTE на Serial-інтерфейсах? Яка команда налаштовується лише на DCE-стороні і навіщо вона потрібна?
8. Що означають символи ! та . у виводі команди ping на Cisco IOS? Який відсоток успішності вважається прийнятним?
9. Чим відрізняється команда ping від traceroute (tracert)? Коли доцільно використовувати кожну з них?
10. Назвіть три типових причини, чому ping між двома мережами не проходить, хоча обидва маршрутизатори увімкнені та мають правильні IP-адреси на інтерфейсах.

Лабораторна робота №5.

Налаштування протоколу динамічної маршрутизації OSPF.

Мета роботи: Зрозуміти відмінність між статичною та динамічною маршрутизацією та переваги протоколів стану каналів (link-state). Вивчити принципи роботи OSPF: процес встановлення сусідства, побудову топологічної бази даних (LSDB), розрахунок найкоротших шляхів за алгоритмом Дейкстри та механізм вибору DR/BDR. Отримати практичні навички налаштування OSPF single-area на маршрутизаторах Cisco в Cisco Packet Tracer, перевірки стану протоколу та усунення типових помилок конфігурації.

ТЕОРЕТИЧНІ ВІДОМОСТІ:

Динамічна маршрутизація: навіщо вона потрібна

У попередній лабораторній роботі ми налаштовували статичну маршрутизацію – кожен маршрут вводився адміністратором вручну. Такий підхід добре працює у невеликих стабільних мережах. Однак із зростанням мережі виникають серйозні проблеми: кількість маршрутів стає некерованою, а при будь-якій зміні топології (обрив кабелю, додавання нового сегменту) адміністратор змушений вручну оновлювати конфігурацію на кожному маршрутизаторі.

Динамічна маршрутизація вирішує ці проблеми: маршрутизатори самостійно обмінюються інформацією про мережу, автоматично будують таблиці маршрутизації та реагують на зміни топології без втручання адміністратора.

Критерій	Статична маршрутизація	OSPF (динамічна)
Налаштування	Вручну кожен маршрут	Одноразово – протокол решту робить сам
Реакція на відмову каналу	Немає (вручну)	Автоматично за секунди
Масштабованість	Погана (>10 роутерів – складно)	Відмінна (тисячі маршрутизаторів)
Навантаження на CPU/канал	Немає	Незначне (OSPF оптимізований)
Де застосовується	Дрібні мережі, stub-мережі	Корпоративні мережі, ISP, лікарні

Таблиця 5.1 – Порівняння статичної маршрутизації та OSPF

OSPF – протокол стану каналів

OSPF (Open Shortest Path First) – протокол динамічної маршрутизації класу link-state (стан каналів), стандартизований у RFC 2328 (OSPFv2 для IPv4). Це найпоширеніший протокол внутрішньої маршрутизації (IGP) у корпоративних мережах будь-якого масштабу.

Ключові характеристики OSPF

- Використовує алгоритм Дейкстри (SPF – Shortest Path First) для розрахунку найкоротших шляхів.
- Метрика – cost (вартість), що обчислюється на основі пропускної здатності інтерфейсу.

- Швидка збіжність: реагує на зміни топології протягом секунд.
- Підтримує VLSM (Variable Length Subnet Masking) та CIDR – передає маску разом з адресою.
- Не обмежений кількістю переходів (на відміну від RIP з його лімітом 15 hop).
- Підтримує ієрархічну структуру через розбиття на зони (areas).
- Адміністративна відстань (AD) = 110.

Принцип роботи OSPF

Топологічна база даних (LSDB)

На відміну від протоколів дистанційно-векторного типу (де кожен маршрутизатор знає лише про своїх сусідів), OSPF будує повну карту мережі – топологічну базу даних (Link State Database, LSDB). Всі маршрутизатори в одній OSPF-зоні мають однакову LSDB.
Для обміну інформацією OSPF використовує спеціальні пакети – **LSA (Link State Advertisement)**. Кожен маршрутизатор генерує LSA із описом своїх інтерфейсів і сусідів та розсилає їх по всій зоні. Отримавши повну LSDB, кожен маршрутизатор самостійно запускає алгоритм Дейкстри і розраховує найкоротший шлях до кожної мережі.

Процес встановлення сусідства (Adjacency)

Перш ніж обмінюватися маршрутною інформацією, маршрутизатори OSPF мають встановити сусідські відносини (adjacency). Цей процес відбувається поетапно через кілька станів:

Стан	Опис
Down	Початковий стан – OSPF-пакети ще не отримані від сусіда
Init	Отримано Hello від сусіда, але сусід ще не підтвердив отримання наших Hello
2-Way	Двостороннє Hello-обміно підтверджено. На ethernet-мережах тут обирають DR/BDR
ExStart	Визначення Master/Slave для обміну базами даних
Exchange	Обмін DBD-пакетами (Database Description) – заголовки LSA
Loading	Запит та отримання відсутніх LSA
Full	Бази даних синхронізовані. Сусідство встановлено – нормальний робочий стан

Таблиця 5.2 – Стани сусідства OSPF

Hello-пакети та таймери OSPF

OSPF використовує Hello-пакети для виявлення та підтримки сусідів. Hello interval – як часто надсилається Hello (за замовчуванням 10 сек на Ethernet, 30 сек на Serial). Dead interval – через який час сусід вважається недоступним (зазвичай 4 × Hello interval). Щоб сусідство встановилося, обидва маршрутизатори ПОВИННІ мати однакові Hello та Dead interval!

Метрика OSPF – Cost

Cost (вартість) – метрика OSPF, що визначає «ціну» використання певного інтерфейсу. Маршрут з меншим сумарним cost вважається кращим. Cost розраховується за формулою:

```
Cost = Reference Bandwidth / Interface Bandwidth

де Reference Bandwidth = 100 Мбіт/с (за замовчуванням у Cisco IOS)

Приклади:
FastEthernet (100 Мбіт/с):    Cost = 100 / 100  = 1
GigabitEthernet (1000 Мбіт/с): Cost = 100 / 1000 = 1 (мінімум 1!)
Serial (1.544 Мбіт/с):         Cost = 100 / 1.544 ≈ 64
Serial (64 кбіт/с):             Cost = 100 / 0.064 ≈ 1562
```

Формула розрахунку Cost OSPF

Проблема з Reference Bandwidth

За замовчуванням Reference Bandwidth = 100 Мбіт/с. Це означає, що FastEthernet і GigabitEthernet отримують однаковий cost = 1. OSPF не розрізняє їх швидкість! У реальних мережах Reference Bandwidth збільшують: для гігабітних мереж – 1000, для 10G – 10000. Команда: `Router(config-router)# auto-cost reference-bandwidth 1000`

Зони OSPF (Areas)

OSPF підтримує ієрархічну структуру через поділ на зони (areas). Зони дозволяють масштабувати мережу: маршрутизатори в різних зонах не обмінюються детальною топологічною інформацією, що зменшує навантаження на CPU та обсяг LSDB.

Area 0 (Backbone Area) – обов'язкова центральна зона, до якої мають бути підключені всі інші зони. У простих мережах (single-area OSPF) використовується лише Area 0.

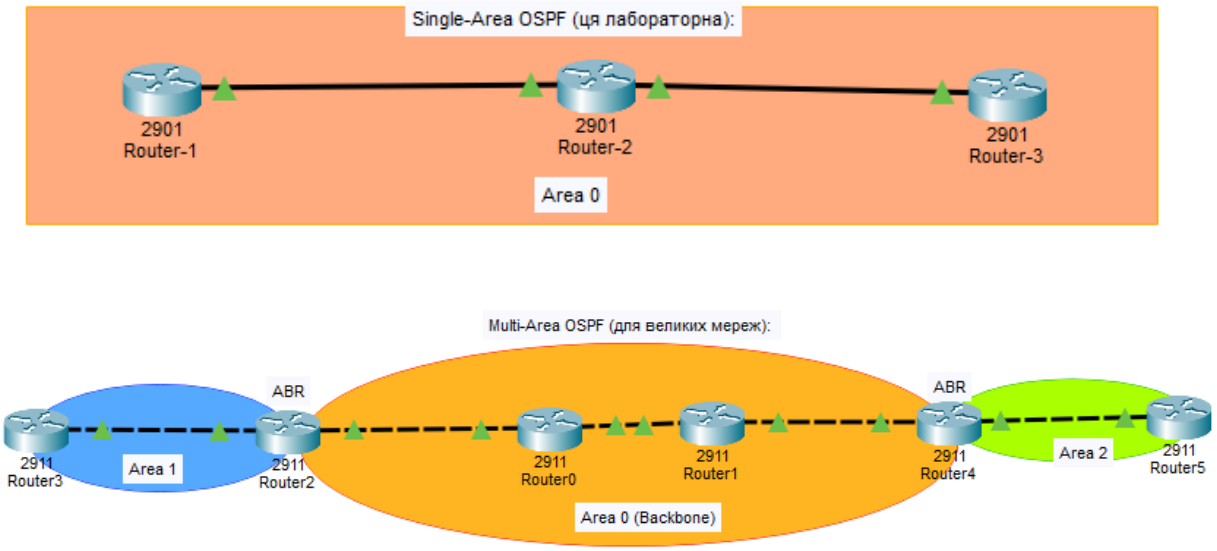

Рисунок 5.1 – Single-area та Multi-area OSPF

Вибір DR та BDR на broadcast-мережах

На Ethernet-мережах (broadcast multi-access) кілька маршрутизаторів можуть бути підключені до одного комутатора. Якщо кожен OSPF-маршрутизатор встановлював би сусідство з кожним – кількість adjacency зростала б як n(n-1)/2. Для оптимізації OSPF обирає двох спеціальних маршрутизаторів:

DR (Designated Router) – головний маршрутизатор сегменту. Всі інші маршрутизатори встановлюють повне сусідство (Full adjacency) лише з DR та BDR. LSA розсилаються через

DR.

BDR (Backup Designated Router) – резервний. Якщо DR виходить з ладу – BDR автоматично стає DR.

DROther – всі інші маршрутизатори сегменту. Вони встановлюють стан 2-Way між собою (не Full).

Критерії вибору DR/BDR

1. Найвищий OSPF Priority (за замовчуванням 1; діапазон 0–255; priority 0 означає, що маршрутизатор не може стати DR/BDR).
2. При рівному priority – найвищий Router ID.

Router ID – унікальний ідентифікатор маршрутизатора в OSPF. Визначається за правилом: 1) вручну задане Router ID; 2) найвища IP-адреса loopback-інтерфейсу; 3) найвища IP-адреса активного фізичного інтерфейсу.

```
! Встановити Router ID вручну (рекомендується):
Router1(config-router)# router-id 1.1.1.1

! Або створити loopback з потрібною адресою:
Router1(config)# interface Loopback0
Router1(config-if)# ip address 1.1.1.1 255.255.255.255
Router1(config-if)# exit
```

Приклад 5.1 – Встановлення Router ID

Налаштування OSPF на Cisco IOS

Увімкнення OSPF та оголошення мереж

Налаштування OSPF починається з активації процесу та оголошення мереж, що беруть участь у маршрутизації. OSPF-процес ідентифікується номером (Process ID), що є локальним для маршрутизатора і може відрізнятися на різних пристроях.

```
! Крок 1: Увійти в режим налаштування OSPF (process-id = 1)
Router1(config)# router ospf 1

! Крок 2: Встановити Router ID (рекомендується зробити першим)
Router1(config-router)# router-id 1.1.1.1

! Крок 3: Оголосити мережі командою network
! Синтаксис: network <IP-адреса> <wildcard-маска> area <номер-зони>
Router1(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router1(config-router)# network 10.0.0.0 0.0.0.3 area 0
Router1(config-router)# exit
```

Приклад 5.2 – Базове налаштування OSPF

Wildcard-маска – що це таке

Wildcard-маска – інверсована маска підмережі, що використовується в OSPF (і ACL). Вона вказує, які біти адреси перевіряються (0 = перевіряти, 1 = ігнорувати).

Маска підмережі	Wildcard-маска	Мережа	Що охоплює
255.255.255.0	0.0.0.255	192.168.1.0	Всі адреси 192.168.1.x
255.255.255.252	0.0.0.3	10.0.0.0	10.0.0.0 – 10.0.0.3
255.255.0.0	0.0.255.255	172.16.0.0	Всі адреси 172.16.x.x
255.255.255.255	0.0.0.0	1.1.1.1	Лише одна адреса 1.1.1.1

Таблиця 5.3 – Маски підмереж та відповідні wildcard-маски

Простий спосіб розрахунку wildcard: відніміть маску від 255.255.255.255. Наприклад: 255.255.255.255 – 255.255.255.0 = 0.0.0.255.

Пасивні інтерфейси (passive-interface)

Інтерфейси, підключені до кінцевих пристроїв (PC, сервери, медичне обладнання), не потребують відправки OSPF Hello-пакетів – там немає інших маршрутизаторів. Відправка Hello на такі інтерфейси – зайве навантаження та потенційна загроза безпеці. Команда passive-interface вимикає відправку Hello на вказаному інтерфейсі, залишаючи мережу оголошеною в OSPF.

```
! Зробити LAN-інтерфейс пасивним (не надсилати Hello до кінцевих пристроїв):
Router1(config)# router ospf 1
Router1(config-router)# passive-interface GigabitEthernet0/0

! Або зробити всі інтерфейси пасивними за замовчуванням,
! а потім активувати лише потрібні (до інших роутерів):
Router1(config-router)# passive-interface default
Router1(config-router)# no passive-interface Serial0/0/0
Router1(config-router)# exit
```

Приклад 5.3 – Налаштування passive-interface

Зміна пріоритету DR/BDR та cost інтерфейсу

```
! Змінити OSPF priority на інтерфейсі (0 = ніколи не стане DR/BDR):
Router1(config)# interface GigabitEthernet0/0
Router1(config-if)# ip ospf priority 100
Router1(config-if)# exit

! Змінити cost вручну на інтерфейсі:
Router1(config)# interface GigabitEthernet0/0
Router1(config-if)# ip ospf cost 10
Router1(config-if)# exit

! Змінити Reference Bandwidth глобально для всіх інтерфейсів:
Router1(config)# router ospf 1
Router1(config-router)# auto-cost reference-bandwidth 1000
Router1(config-router)# exit
```

Приклад 5.4 – Налаштування priority та cost

Повний приклад налаштування OSPF для трьох маршрутизаторів

Розглянемо налаштування OSPF для типової топології медичної мережі з трьома маршрутизаторами та трьома підмережами.

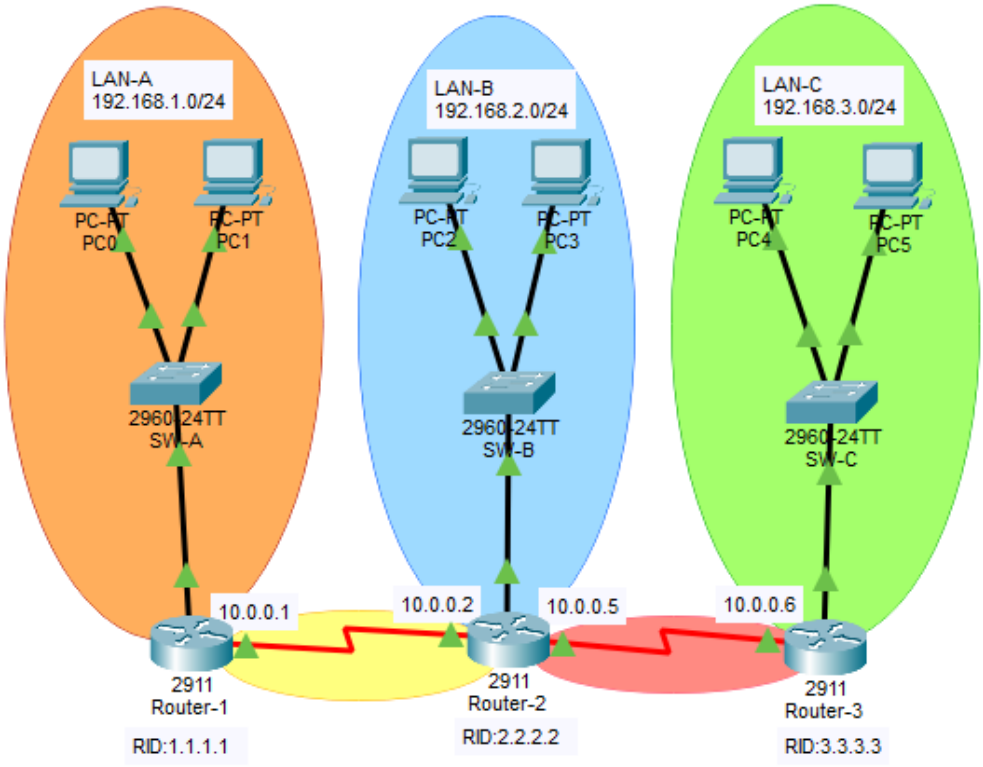

Рисунок 5.2 – Топологія для прикладу OSPF

Налаштування Router-1

```
Router(config)# hostname Router-1
Router-1(config)# interface Loopback0
Router-1(config-if)# ip address 1.1.1.1 255.255.255.255
Router-1(config-if)# exit

Router-1(config)# interface GigabitEthernet0/0
Router-1(config-if)# ip address 192.168.1.1 255.255.255.0
Router-1(config-if)# no shutdown
Router-1(config-if)# exit

Router-1(config)# interface Serial0/0/0
Router-1(config-if)# ip address 10.0.0.1 255.255.255.252
Router-1(config-if)# clock rate 64000
Router-1(config-if)# no shutdown
Router-1(config-if)# exit

Router-1(config)# router ospf 1
Router-1(config-router)# router-id 1.1.1.1
Router-1(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router-1(config-router)# network 10.0.0.0 0.0.0.3 area 0
Router-1(config-router)# passive-interface GigabitEthernet0/0
Router-1(config-router)# exit
Router-1(config)# end
Router-1# copy running-config startup-config
```

Приклад 5.5 – Повне налаштування Router-1 з OSPF

Налаштування Router-2

```
Router(config)# hostname Router-2
Router-2(config)# interface Loopback0
Router-2(config-if)# ip address 2.2.2.2 255.255.255.255
Router-2(config-if)# exit

Router-2(config)# interface GigabitEthernet0/0
Router-2(config-if)# ip address 192.168.2.1 255.255.255.0
Router-2(config-if)# no shutdown
Router-2(config-if)# exit

Router-2(config)# interface Serial0/0/0
Router-2(config-if)# ip address 10.0.0.2 255.255.255.252
Router-2(config-if)# no shutdown
Router-2(config-if)# exit

Router-2(config)# interface Serial0/0/1
Router-2(config-if)# ip address 10.0.0.5 255.255.255.252
Router-2(config-if)# clock rate 64000
Router-2(config-if)# no shutdown
Router-2(config-if)# exit

Router-2(config)# router ospf 1
Router-2(config-router)# router-id 2.2.2.2
Router-2(config-router)# network 192.168.2.0 0.0.0.255 area 0
Router-2(config-router)# network 10.0.0.0 0.0.0.3 area 0
Router-2(config-router)# network 10.0.0.4 0.0.0.3 area 0
Router-2(config-router)# passive-interface GigabitEthernet0/0
Router-2(config-router)# exit
```

Приклад 5.6 – Повне налаштування Router-2 з OSPF

Налаштування Router-3

```
Router(config)# hostname Router-3
Router-3(config)# interface Loopback0
Router-3(config-if)# ip address 3.3.3.3 255.255.255.255
Router-3(config-if)# exit

Router-3(config)# interface GigabitEthernet0/0
Router-3(config-if)# ip address 192.168.3.1 255.255.255.0
Router-3(config-if)# no shutdown
Router-3(config-if)# exit

Router-3(config)# interface Serial0/0/0
Router-3(config-if)# ip address 10.0.0.6 255.255.255.252
Router-3(config-if)# no shutdown
Router-3(config-if)# exit

Router-3(config)# router ospf 1
Router-3(config-router)# router-id 3.3.3.3
Router-3(config-router)# network 192.168.3.0 0.0.0.255 area 0
Router-3(config-router)# network 10.0.0.4 0.0.0.3 area 0
Router-3(config-router)# passive-interface GigabitEthernet0/0
Router-3(config-router)# exit
```

Приклад 5.7 – Повне налаштування Router-3 з OSPF

Команди перевірки OSPF

Перевірка сусідства

```
! Список OSPF-сусідів та їх стан (має бути FULL):
Router-1# show ip ospf neighbor
```

```
Neighbor ID   Pri   State      Dead Time   Address     Interface
2.2.2.2         1   FULL/DR    00:00:36    10.0.0.2    Serial0/0/0

! Детальна інформація про конкретного сусіда:
Router-1# show ip ospf neighbor detail
```

Приклад 5.8 – Перевірка сусідів OSPF

У стовпці **State** нормальний стан – **FULL**. На Serial-з'єднаннях пишеться **FULL/-** (DR/BDR не обираються на point-to-point). На Ethernet – **FULL/DR** або **FULL/BDR**.

Перевірка маршрутів OSPF у таблиці маршрутизації

```
! Вся таблиця маршрутизації (OSPF-маршрути позначені 'O'):
Router-1# show ip route

O    192.168.2.0/24 [110/65] via 10.0.0.2, 00:01:23, Serial0/0/0
O    192.168.3.0/24 [110/129] via 10.0.0.2, 00:01:10, Serial0/0/0
O    10.0.0.4/30    [110/128] via 10.0.0.2, 00:01:10, Serial0/0/0

! Лише OSPF-маршрути:
Router-1# show ip route ospf
```

Приклад 5.9 – OSPF-маршрути у таблиці маршрутизації

Значення **[110/65]**: 110 – адміністративна відстань OSPF, 65 – сумарний cost шляху (cost Serial = 64 + cost до наступної мережі 1).

Перевірка бази даних OSPF (LSDB)

```
! Топологічна база даних OSPF:
Router-1# show ip ospf database

! Детальна інформація про OSPF-процес:
Router-1# show ip ospf

! Стан OSPF на конкретному інтерфейсі:
Router-1# show ip ospf interface Serial0/0/0
Router-1# show ip ospf interface GigabitEthernet0/0

! Короткий стан всіх OSPF-інтерфейсів:
Router-1# show ip ospf interface brief
```

Приклад 5.10 – Перевірка бази даних та інтерфейсів OSPF

Зведена таблиця команд OSPF

Команда	Що перевіряє
`show ip ospf neighbor`	Список сусідів та стан (має бути FULL)
`show ip ospf neighbor detail`	Детальна інформація про кожного сусіда
`show ip route ospf`	Тільки OSPF-маршрути в таблиці
`show ip ospf`	Параметри OSPF-процесу: RID, area, timer
`show ip ospf database`	Топологічна база даних (LSDB)
`show ip ospf interface <ім'я>`	Стан OSPF на інтерфейсі: cost, DR/BDR, таймери
`show ip ospf interface brief`	Короткий список всіх OSPF-інтерфейсів
`clear ip ospf process`	Перезапустити OSPF-процес (скидає сусідство)

`debug ip ospf events`	Відлагодження OSPF-подій в реальному часі
`no debug all`	Вимкнути всі debug-виводи

Таблиця 5.4 – Команди перевірки та діагностики OSPF

Діагностика проблем OSPF

Більшість проблем OSPF пов'язані з тим, що сусідство між маршрутизаторами не встановлюється або встановлюється некоректно. Нижче наведено систематичний підхід до усунення таких проблем.

Алгоритм діагностики: від фізичного до логічного

1. Перевірте фізичний рівень: `show ip interface brief` – всі задіяні інтерфейси мають бути up/up.
2. Перевірте IP-адреси та маски на інтерфейсах обох маршрутизаторів – вони мають належати до однієї підмережі.
3. Виконайте `ping` між безпосередньо підключеними інтерфейсами (наприклад, з 10.0.0.1 до 10.0.0.2). Якщо ping не проходить – OSPF не запрацює.
4. Перевірте `show ip ospf neighbor` – якщо сусіда немає взагалі, проблема у фізиці або параметрах OSPF.
5. Якщо сусід є, але стан не FULL – перевірте таймери, area, network-команди.
6. Перевірте `show ip route ospf` – чи з'явилися маршрути від сусідів.
7. Виконайте ping між кінцевими хостами різних мереж.

Умови встановлення сусідства OSPF

OSPF-сусідство НЕ встановиться, якщо хоча б одна з наступних умов не виконана:

Умова	Симптом при порушенні	Команда перевірки
Інтерфейси в одній підмережі	Сусіда немає в show ip ospf neighbor	`show ip interface brief`
Однакові Hello/Dead interval	Сусід з'являється, але зникає	`show ip ospf interface <ім'я>`
Однаковий Area ID	Сусіда немає або стан Init	`show ip ospf neighbor`
Однаковий MTU (на Ethernet)	Стан зупиняється на ExStart/Exchange	`show interface` – MTU має збігатися
Мережа оголошена командою network	Маршрути не з'являються у сусідів	`show ip ospf database`
Router ID унікальний	Непередбачувана поведінка маршрутизації	`show ip ospf` – перевірити `RID`

Таблиця 5.5 – Умови встановлення OSPF-сусідства та діагностика

Типові помилки та їх вирішення

Симптом	Причина	Вирішення
`show ip ospf neighbor` – порожній вивід	Мережу не оголошено командою network або інтерфейс down	Перевірити network-команди та стан інтерфейсів

Сусід є, але стан INIT (не FULL)	Hello-пакети надходять, але є розбіжність у параметрах	Перевірити area, таймери на обох роутерах
Маршрут є, але ping не проходить	passive-interface встановлено на WAN-інтерфейс	Перевірити passive-interface – лише LAN-порти!
Wildcard-маска некоректна	Мережа не оголошується або охоплює зайве	Перерахувати: wildcard = 255.255.255.255 – маска
Після зміни Router ID сусідство не оновлюється	Router ID кешується до перезапуску OSPF	clear ip ospf process – підтвердити Yes
O-маршрути є, але деякі мережі відсутні	Мережу не оголошено на одному з роутерів	`show ip ospf database` – перевірити LSA всіх роутерів

Таблиця 5.6 – Типові помилки OSPF та методи їх усунення

Корисний debug для OSPF

```
! Відстежити обмін Hello-пакетами (перевірка сусідства):
Router-1# debug ip ospf hello

! Відстежити всі OSPF-події (зміни стану, LSA):
Router-1# debug ip ospf events

! ОБОВ'ЯЗКОВО вимкнути debug після завершення перевірки!
Router-1# no debug all
! або
Router-1# undebug all
```

Приклад 5.11 – Використання debug для діагностики OSPF

Увага при використанні debug!

Команди debug можуть генерувати величезний обсяг виводу і суттєво навантажувати CPU маршрутизатора. У виробничих мережах (наприклад, у лікарні під час роботи) використовуйте debug лише у крайньому разі і ЗАВЖДИ вимикайте його командою no debug all після завершення діагностики!

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

Завдання полягає у побудові мережі з трьох маршрутизаторів та налаштуванні протоколу OSPF (single-area, Area 0) для автоматичного обміну маршрутною інформацією. На відміну від ЛР №4, жодного статичного маршруту налаштовувати не потрібно – всю роботу виконає OSPF.

Топологія мережі

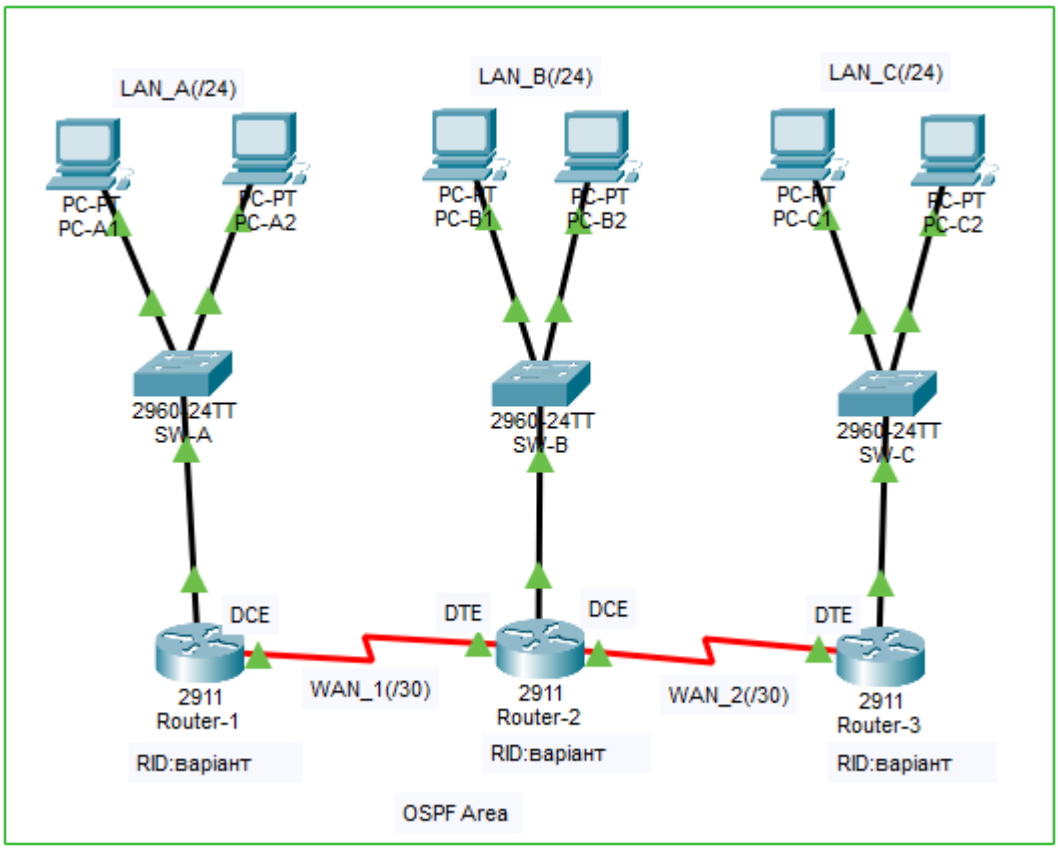

Рисунок 5.3 – Топологія мережі для лабораторної роботи № 5

Порядок виконання

Частина 1. Побудова топології та налаштування інтерфейсів

1. Створіть новий проект у Cisco Packet Tracer.
2. Розмістіть три маршрутизатори (1941 або 2911), три комутатори (2960), шість PC (по два на кожну мережу).
3. З'єднайте PC зі своїми комутаторами, комутатори – з маршрутизаторами (Gig0/0, Straight-through).
4. З'єднайте Router-1 ↔ Router -2 Serial-кабелем DCE (починайте з Router -1). З'єднайте Router -2 ↔ Router -3 Serial-кабелем DCE (починайте з Router -2).
5. Налаштуйте IP-адреси на всіх інтерфейсах маршрутизаторів відповідно до вашого варіанту. Не забудьте `clock rate 64000` на DCE-інтерфейсах та `no shutdown` на всіх.

6. Налаштуйте IP-адреси та шлюзи на всіх шести PC.
7. Перевірте `ping` між безпосередньо підключеними інтерфейсами маршрутизаторів – має проходити.

Частина 2. Налаштування OSPF

1. На кожному маршрутизаторі створіть loopback-інтерфейс з адресою з таблиці варіантів (RID).
2. Запустіть `OSPF process 1` на кожному маршрутизаторі: `router ospf 1`.
3. Встановіть Router ID: `router-id X.X.X.X` (відповідно до варіанту).
4. Оголосіть усі мережі (LAN та WAN) командою network з правильною wildcard-маскою та `area 0`.
5. Встановіть passive-interface на всіх LAN-інтерфейсах (Gig0/0) кожного маршрутизатора.
6. Збережіть конфігурацію на всіх маршрутизаторах.

Частина 3. Перевірка та аналіз

1. Виконайте `show ip ospf neighbor` на всіх маршрутизаторах. Стан сусідів має бути FULL. Зробіть скріншоти.
2. Виконайте `show ip route ospf` – переконайтесь, що кожен маршрутизатор бачить усі три LAN-мережі. Зробіть скріншоти.
3. Виконайте `show ip ospf interface brief` – зафіксуйте cost кожного інтерфейсу. Скріншот.
4. Виконайте `show ip ospf` – знайдіть рядок з Router ID та інформацією про Area 0. Скріншот.
5. Ping з PC-A1 до PC-B1, PC-C1, PC-C2. Ping з PC-C1 до PC-A2. Всі мають відповідати. Скріншоти.
6. Tracert з PC-A1 до PC-C1 – зафіксуйте шлях через два маршрутизатори. Скріншот.
7. Симуляція відмови каналу: відключіть кабель між Router -1 та Router -2 (клацніть ПКМ → Delete connection або просто видаліть з'єднання). Зачекайте 30–60 секунд. Виконайте `show ip ospf neighbor` та `show ip route ospf` на Router -1 – зафіксуйте зміни. (Примітка: при топології ланцюжка зв'язок буде втрачено – це нормальний результат, що демонструє роботу OSPF).
8. Відновіть з'єднання та переконайтесь, що OSPF відновив маршрути.

Таблиця адресації (заповнити у звіті)

Пристрій / Інтерфейс	IP-адреса	Маска підмережі	Шлюз / RID
Router -1 Loopback0 (RID)		255.255.255.255	–
Router-1 Gig0/0 (GW_A)		255.255.255.0	–
Router-1 Se0/0/0 (WAN1_R1)		255.255.255.252	–
Router-2 Loopback0 (RID)		255.255.255.255	–
Router-2 Gig0/0 (GW_B)		255.255.255.0	–
Router-2 Se0/0/0 (WAN1_R2)		255.255.255.252	–
Router-2 Se0/0/1 (WAN2_R2)		255.255.255.252	–

Router-3 Loopback0 (RID)		255.255.255.255	–
Router-3 Gig0/0 (GW_C)		255.255.255.0	–
Router-3 Se0/0/0 (WAN2_R3)		255.255.255.252	–
PC-A1 / PC-A2		255.255.255.0	GW_A
PC-B1 / PC-B2		255.255.255.0	GW_B
PC-C1 / PC-C2		255.255.255.0	GW_C

Таблиця 5.7 – Таблиця адресації (заповнюється студентом)

Варіанти завдань

Кожен варіант містить три LAN-мережі, два WAN-з'єднання та Router ID для кожного маршрутизатора. GW_A, GW_B, GW_C – перші хост-адреси відповідних LAN. WAN1_R1 та WAN1_R2 – перша та друга адреси першого WAN /30. WAN2_R2 та WAN2_R3 – першого /30 другого WAN.

В.	**LAN_A /24**	**LAN_B /24**	**LAN_C /24**	**WAN1 /30**	**WAN2 /30**	**RID Router-1**	**RID Router-2 / Router-3**
1	192.168.1.0	192.168.2.0	192.168.3.0	10.0.0.0	10.0.0.4	1.1.1.1	2.2.2.2 / 3.3.3.3
2	192.168.4.0	192.168.5.0	192.168.6.0	10.0.1.0	10.0.1.4	1.1.1.2	2.2.2.2 / 3.3.3.2
3	172.16.1.0	172.16.2.0	172.16.3.0	10.1.0.0	10.1.0.4	1.1.1.3	2.2.2.3 / 3.3.3.3
4	172.16.4.0	172.16.5.0	172.16.6.0	10.1.1.0	10.1.1.4	1.1.1.4	2.2.2.4 / 3.3.3.4
5	10.10.1.0	10.10.2.0	10.10.3.0	172.31.0.0	172.31.0.4	1.1.1.5	2.2.2.5 / 3.3.3.5
6	10.10.4.0	10.10.5.0	10.10.6.0	172.31.0.8	172.31.0.12	1.1.1.6	2.2.2.6 / 3.3.3.6
7	192.168.10.0	192.168.20.0	192.168.30.0	10.2.0.0	10.2.0.4	1.1.1.7	2.2.2.7 / 3.3.3.7
8	192.168.40.0	192.168.50.0	192.168.60.0	10.3.0.0	10.3.0.4	1.1.1.8	2.2.2.8 / 3.3.3.8
9	10.20.1.0	10.20.2.0	10.20.3.0	172.31.1.0	172.31.1.4	1.1.1.9	2.2.2.9 / 3.3.3.9
10	10.30.1.0	10.30.2.0	10.30.3.0	172.31.2.0	172.31.2.4	1.1.1.10	2.2.2.10 / 3.3.3.10
11	172.20.1.0	172.20.2.0	172.20.3.0	10.4.0.0	10.4.0.4	1.1.1.11	2.2.2.11 / 3.3.3.11
12	172.20.4.0	172.20.5.0	172.20.6.0	10.5.0.0	10.5.0.4	1.1.1.12	2.2.2.12 / 3.3.3.12
13	192.168.70.0	192.168.80.0	192.168.90.0	10.6.0.0	10.6.0.4	1.1.1.13	2.2.2.13 / 3.3.3.13
14	10.40.1.0	10.40.2.0	10.40.3.0	172.31.3.0	172.31.3.4	1.1.1.14	2.2.2.14 / 3.3.3.14
15	10.50.1.0	10.50.2.0	10.50.3.0	172.31.4.0	172.31.4.4	1.1.1.15	2.2.2.15 / 3.3.3.15

Таблиця 5.8 – Варіанти завдань для лабораторної роботи № 5

Вимоги до звіту

Звіт має містити:
1) Заповнену таблицю адресації;
2) Скріншот топології;
3) Скріншоти `show ip ospf neighbor` на всіх трьох маршрутизаторах (стан FULL);
4) Скріншоти `show ip route ospf` на всіх трьох (мають бути O-маршрути до всіх LAN);
5) Скріншот `show ip ospf interface brief` (з cost-значеннями);
6) Скріншоти `ping` та `tracert` між крайніми мережами;
7) Скріншоти `show ip ospf neighbor` після відключення кабелю (симуляція відмови);
8) Відповіді на контрольні запитання.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке динамічна маршрутизація і яка її головна перевага перед статичною у великих мережах?
2. Що таке OSPF і до якого класу протоколів він належить? Поясніть поняття 'link-state' та чим цей підхід відрізняється від дистанційно-векторного.
3. Що таке LSDB (Link State Database)? Чи однакова вона на всіх маршрутизаторах однієї OSPF-зони?
4. Що таке Router ID в OSPF? За яким правилом він визначається автоматично і як його задати вручну?
5. Що таке метрика cost у OSPF? За якою формулою вона розраховується? Чому FastEthernet і GigabitEthernet можуть мати однаковий cost і як це виправити?
6. Що таке DR та BDR у OSPF? Для чого вони потрібні і за якими критеріями обираються?
7. Що таке wildcard-маска? Як вона пов'язана зі звичайною маскою підмережі? Розрахуйте wildcard для маски 255.255.255.252.
8. Що означає команда passive-interface у OSPF-конфігурації? На яких інтерфейсах її слід застосовувати і чому?
9. Яка команда дозволяє перевірити стан OSPF-сусідства? Який стан є нормальним (робочим)? Що означає стан INIT?
10. Перелічіть три найбільш поширені причини, через які OSPF-сусідство не встановлюється між двома маршрутизаторами.

Лабораторна робота №6.

DHCP та DNS у мережі медичного закладу.

Мета роботи: Вивчити принципи роботи протоколу DHCP, процес отримання IP-адреси (DORA), структуру DHCP-пулу, параметри, що передаються клієнту. Зрозуміти особливості роботи DHCP у багатосегментних мережах та призначення DHCP Relay Agent. Ознайомитися з принципами роботи DNS, ієрархію доменних імен, типи DNS-записів, процес розв'язання імен. Отримати практичні навички налаштування DHCP-сервера (на базі Cisco IOS та сервера CPT), DHCP Relay, DNS-сервера в Cisco Packet Tracer та перевірки їх роботи.

Теоретичні відомості:

Протокол DHCP – автоматичне призначення адрес

У попередніх лабораторних роботах IP-адреси на кожному комп'ютері налаштовувалися вручну (статично). У реальних мережах, особливо у медичних закладах з десятками та сотнями пристроїв, ручне налаштування є непрактичним та схильним до помилок. Протокол DHCP вирішує цю проблему.

DHCP (Dynamic Host Configuration Protocol) – протокол прикладного рівня (порти UDP 67/68), що дозволяє мережевим пристроям автоматично отримувати IP-адресу та інші мережеві параметри від централізованого DHCP-сервера.

Параметри, що передаються DHCP-сервером клієнту:

- IP-адреса та маска підмережі
- Шлюз за замовчуванням (Default Gateway)
- Адреса DNS-сервера
- Час оренди адреси (Lease Time)
- Ім'я домену (Domain Name) – необов'язково
- Адреса WINS-сервера, NTP-сервера тощо – за потреби

Процес отримання адреси – DORA

Процес отримання IP-адреси від DHCP-сервера складається з чотирьох повідомлень, що утворюють абревіатуру DORA:

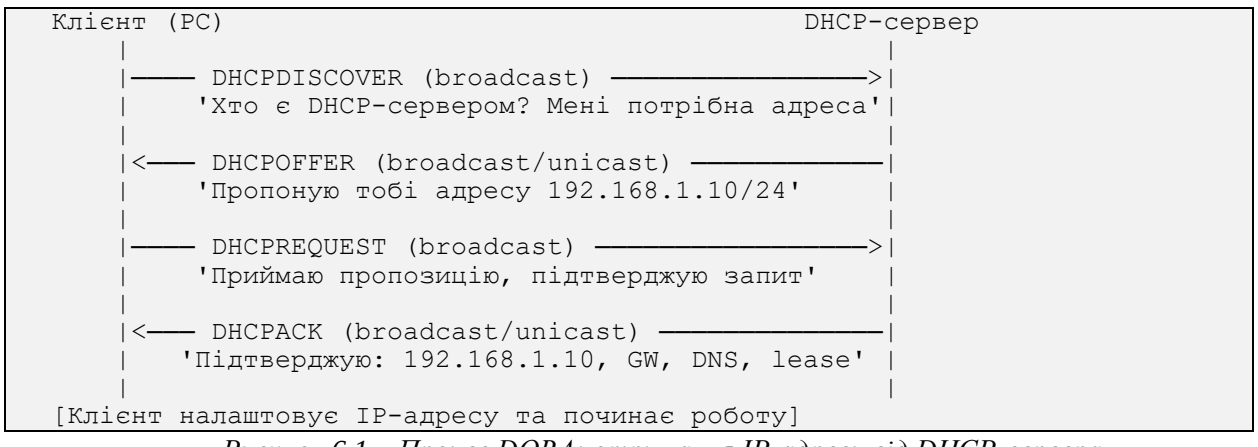

Рисунок 6.1 – Процес DORA: отримання IP-адреси від DHCP-сервера

D – Discover: клієнт надсилає широкомовний пакет у пошуках DHCP-сервера (адреса

джерела 0.0.0.0, призначення 255.255.255.255).
O – Offer: сервер пропонує вільну адресу з пулу разом із мережевими параметрами.
R – Request: клієнт формально запитує запропоновану адресу (широкомовно – щоб інші сервери знали про вибір).
A – Acknowledge: сервер підтверджує надання адреси та встановлює час оренди (lease time).

Оренда адреси (Lease) та її поновлення

DHCP-адреса надається клієнту не назавжди, а на певний час – lease time. Після закінчення 50% часу оренди клієнт намагається поновити адресу у того самого сервера (unicast DHCPREQUEST). Після 87.5% – надсилає широкомовний запит до будь-якого DHCP-сервера. Якщо поновлення не вдалося – клієнт припиняє використання адреси.
Типові значення lease time: **8 годин** – для офісів і лікарень (збалансовано); **1 доба** – для стабільних мереж; **30 хвилин** – для гостьових мереж з великою ротацією пристроїв.

Налаштування DHCP-сервера на маршрутизаторі Cisco IOS

Маршрутизатор Cisco може виступати DHCP-сервером для підключених до нього підмереж. Це зручно для невеликих мереж – не потрібен окремий сервер.

Створення DHCP-пулу

```
! Крок 1: Виключити з пулу адреси, що призначені статично
! (шлюз, сервери, принтери - всі статичні пристрої)
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.20

! Крок 2: Створити DHCP-пул з іменем
Router(config)# ip dhcp pool LAN-KARDIOLOGY

! Крок 3: Налаштувати параметри пулу
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 192.168.1.100
Router(dhcp-config)# domain-name med-center.local
Router(dhcp-config)# lease 0 8 0
Router(dhcp-config)# exit
```

Приклад 6.1 – Налаштування DHCP-пулу на маршрутизаторі Cisco

Команда	Опис
`ip dhcp excluded-address`	Виключити одну адресу або діапазон з пулу – для статичних пристроїв
`network <мережа> <маска>`	Адресний простір пулу DHCP
`default-router <IP>`	Шлюз за замовчуванням для клієнтів
`dns-server <IP>`	Адреса DNS-сервера (можна вказати до 8)
`domain-name <ім'я>`	Ім'я домену (необов'язково)
`lease <дні> <год> <хв>`	Час оренди. lease 0 8 0 = 8 годин. lease infinite = безстроково

Таблиця 6.1 – Команди налаштування DHCP-пулу Cisco IOS

Кілька пулів для різних підмереж

Маршрутизатор може обслуговувати кілька підмереж одночасно – для кожної створюється окремий пул. Це типова ситуація у медичному закладі, де різні відділення мають свої підмережі.

```
! Пул для підмережі адміністрації
Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.20
Router(config)# ip dhcp pool ADMIN
Router(dhcp-config)# network 192.168.1.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.1.1
Router(dhcp-config)# dns-server 192.168.1.100
Router(dhcp-config)# lease 1 0 0
Router(dhcp-config)# exit

! Пул для підмережі медичного обладнання
Router(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.30
Router(config)# ip dhcp pool MED-DEVICES
Router(dhcp-config)# network 192.168.2.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.2.1
Router(dhcp-config)# dns-server 192.168.1.100
Router(dhcp-config)# lease 0 8 0
Router(dhcp-config)# exit
```

Приклад 6.2 – Два DHCP-пули для різних підмереж медичного закладу

DHCP Relay Agent – робота в багатосегментних мережах

DHCPDISCOVER – це широкомовний пакет. Широкомовний трафік не перетинає маршрутизатор. Це означає, що якщо DHCP-сервер знаходиться в одній підмережі, а клієнт – в іншій, клієнт ніколи не отримає адресу!

DHCP Relay Agent (ip helper-address) – функція маршрутизатора, що вирішує цю проблему. Маршрутизатор «перехоплює» широкомовний DHCPDISCOVER від клієнта та пересилає його unicast-пакетом безпосередньо до DHCP-сервера. Відповідь сервера також передається назад через маршрутизатор до клієнта.

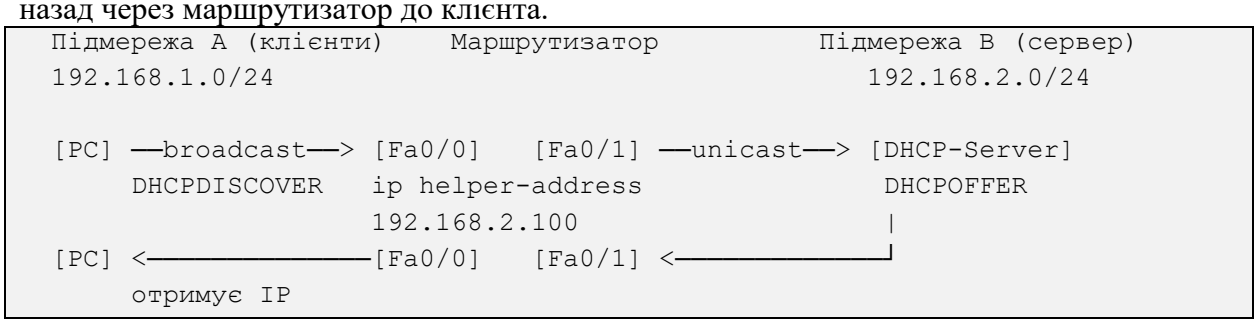

Рисунок 6.2 – Принцип роботи DHCP Relay Agent (ip helper-address)

```
! Налаштовується на інтерфейсі, ЩО ДИВИТЬСЯ НА КЛІЄНТІВ:
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip helper-address 192.168.2.100
Router(config-if)# exit

! Якщо клієнти в кількох підмережах – налаштовується
! на кожному відповідному інтерфейсі окремо:
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip helper-address 192.168.2.100
Router(config-if)# exit
```

Приклад 6.3 – Налаштування DHCP Relay на маршрутизаторі

DHCP у мережі лікарні

У великій лікарні зазвичай є один центральний DHCP-сервер (або два – основний і резервний)

у серверній кімнаті. Кожен маршрутизатор (або L3-комутатор) у відділеннях налаштований з ip helper-address, що вказує на цей центральний сервер. Завдяки цьому всі пристрої лікарні – від комп'ютерів лікарів до медичних моніторів – автоматично отримують адреси з відповідних пулів.

Перевірка та моніторинг DHCP на Cisco IOS

```
! Переглянути всі видані оренди (lease):
Router# show ip dhcp binding

IP address      Client-ID/          Lease expiration    Type
                Hardware address
192.168.1.21    0100.5056.ab12.34   Mar 01 2025 08:00   Automatic
192.168.1.22    0100.1234.5678.9a   Mar 01 2025 08:10   Automatic

! Переглянути статистику DHCP-сервера:
Router# show ip dhcp server statistics

! Переглянути налаштовані пули:
Router# show ip dhcp pool

! Переглянути виключені адреси:
Router# show running-config | section dhcp

! Очистити всі оренди (корисно при налагодженні):
Router# clear ip dhcp binding *
```

Приклад 6.4 – Команди перевірки DHCP на маршрутизаторі

Перевірка на клієнті (PC в CPT)

```
! На PC (Desktop → Command Prompt):

! Переглянути отримані параметри DHCP:
PC> ipconfig

FastEthernet0 Connection:(default port)
   Link-local IPv6 Address: fe80::...
   IP Address.............: 192.168.1.21
   Subnet Mask............: 255.255.255.0
   Default Gateway........: 192.168.1.1

! Примусово оновити DHCP-оренду:
PC> ipconfig /release
PC> ipconfig /renew
```

Приклад 6.5 – Перевірка DHCP-параметрів на клієнті

DNS – система доменних імен

DNS (Domain Name System) – розподілена ієрархічна система, що перетворює зрозумілі людині доменні імена (наприклад, med-center.local або www.google.com) на IP-адреси, і навпаки. Без DNS користувачі змушені були б пам'ятати числові IP-адреси всіх ресурсів.

Ієрархія DNS

DNS організована як ієрархічне дерево доменів:

- Кореневий домен (Root): . – вершина ієрархії, керується IANA
- Домени верхнього рівня (TLD): .com, .org, .net, .ua, .local тощо
- Домени другого рівня: google.com, med-center.local, hospital.ua
- Піддомени: mail.med-center.local, ris.hospital.ua

Типи DNS-записів

Тип запису	Назва	Призначення
A	Address	Ім'я → IPv4-адреса (основний тип запису)
AAAA	IPv6 Address	Ім'я → IPv6-адреса
PTR	Pointer	IP-адреса → ім'я (зворотне розв'язання)
CNAME	Canonical Name	Псевдонім для іншого запису (alias)
MX	Mail Exchanger	Адреса поштового сервера домену
NS	Name Server	Авторитетний DNS-сервер для домену
SOA	Start of Authority	Початковий запис зони з параметрами

Таблиця 6.2 – Основні типи DNS-записів

Процес розв'язання DNS-імені

Коли користувач вводить адресу в браузері, відбувається такий процес:

1. Комп'ютер перевіряє локальний кеш DNS та файл hosts – чи не відома вже ця адреса.
2. Якщо ні – надсилає запит до налаштованого DNS-сервера (зазвичай отриманого від DHCP).
3. DNS-сервер перевіряє свою базу даних. Якщо запис є – повертає відповідь.
4. Якщо DNS-сервер не знає відповіді – він або пересилає запит на інший DNS-сервер (рекурсивний запит), або повертає посилання на авторитетний сервер (ітеративний запит).
5. Клієнт отримує IP-адресу, кешує її на TTL (Time To Live) та встановлює з'єднання.

Налаштування DNS-сервера в Cisco Packet Tracer

У Cisco Packet Tracer роль DNS-сервера виконує пристрій Server. Для налаштування DNS:

1. Двічі клацніть на сервері → вкладка Services → DNS.
2. Увімкніть службу: перемикач DNS Service → On.
3. Додайте записи типу A: у поле Name введіть ім'я хоста, у поле Address – IP-адресу, натисніть Add.
4. Можна додати записи типу CNAME (псевдоніми) та інші.

```
Приклад записів DNS для медичного закладу:

Тип   Ім'я                          Адреса
──────────────────────────────────────────────────
A     server.med-center.local      192.168.1.100
A     ris.med-center.local         192.168.1.101
A     pacs.med-center.local        192.168.1.102
A     router.med-center.local      192.168.1.1
CNAME www.med-center.local         server.med-center.local
```

Приклад 6.6 – DNS-записи для мережі медичного закладу в CPT

Перевірка DNS на клієнті

```
! На PC (Desktop → Command Prompt):

! Перевірити розв'язання імені:
PC> nslookup server.med-center.local
Server:  [192.168.1.100]
Address: 192.168.1.100

Name:    server.med-center.local
Address: 192.168.1.100

! Або просто ping за іменем:
PC> ping server.med-center.local
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time<1ms TTL=128
```

Приклад 6.7 – Перевірка DNS-розв'язання на клієнті

Налаштування DHCP на сервері в Cisco Packet Tracer

Окрім маршрутизатора Cisco IOS, роль DHCP-сервера може виконувати пристрій Server у CPT. Це корисно коли потрібен виділений сервер, а не функція маршрутизатора.

1. Двічі клацніть на сервері → вкладка Services → DHCP.
2. Увімкніть службу: DHCP Service → On.
3. Заповніть параметри пулу: Pool Name, Default Gateway, DNS Server, Start IP Address, Subnet Mask, Max number of users.
4. Натисніть Add та Save.

```
Приклад налаштування DHCP-пулу на сервері CPT:

Pool Name:          LAN-KARDIOLOGY
Default Gateway:    192.168.1.1
DNS Server:         192.168.1.100
Start IP Address:   192.168.1.21
Subnet Mask:        255.255.255.0
Max users:          50
TFTP Server:        0.0.0.0  (не використовується)
Lease Time:         86400    (секунди = 24 години)
```

Приклад 6.8 – Параметри DHCP-пулу на Server у CPT

Діагностика проблем DHCP та DNS

Алгоритм діагностики DHCP

1. Перевірте, чи отримав клієнт адресу: `ipconfig` на PC. Якщо адреса 0.0.0.0 або 169.254.x.x – клієнт не отримав відповідь від DHCP-сервера.
2. Перевірте, чи активний DHCP-сервер: `show ip dhcp pool` та `show ip dhcp binding` на маршрутизаторі.
3. Перевірте ping між клієнтом та DHCP-сервером – якщо не проходить, проблема в маршрутизації.
4. Якщо клієнт і сервер у різних підмережах – перевірте наявність `ip helper-address` на інтерфейсі маршрутизатора, що дивиться на клієнтів.
5. Перевірте, чи не вичерпаний пул адрес: `show ip dhcp binding` – порахуйте кількість оренд.
6. Перевірте `excluded-address` – можливо, виключено занадто багато адрес і пул порожній.

Алгоритм діагностики DNS

1. Перевірте, чи правильна адреса DNS-сервера на клієнті: `ipconfig`.
2. Ping до DNS-сервера за IP-адресою – якщо не проходить, проблема в мережевому зв'язку, а не в DNS.
3. Виконайте `nslookup <ім'я>` – якщо повертає помилку `'DNS request timed out'` – сервер недоступний або запис відсутній.
4. Перевірте наявність запису на DNS-сервері: Services → DNS → переглянути список записів.
5. Перевірте, чи увімкнена служба DNS на сервері (перемикач On).

Типові помилки та їх вирішення

Симптом	Причина	Вирішення
PC отримує 169.254.x.x (APIPA)	DHCP-сервер недоступний (немає зв'язку або relay)	Перевірити маршрутизацію та `ip helper-address`
PC отримує 0.0.0.0	DHCP-служба вимкнена або пул не налаштований	Перевірити `show ip dhcp pool` на маршрутизаторі
Пул вичерпаний – нові клієнти не отримують адресу	Забагато пристроїв або малий пул	Збільшити пул або зменшити lease time
Клієнт отримав адресу, але не пінгує шлюз	Неправильний `default-router` в пулі	Перевірити командою `show ip dhcp pool`
`nslookup` повертає помилку	Неправильна IP DNS-сервера або служба вимкнена	Перевірити ipconfig та доступність сервера
`ping` за іменем не працює, за IP – так	DNS не налаштований або запис відсутній	Додати A-запис на DNS-сервері
`ip helper-address` є, але `relay` не працює	Маршрут до DHCP-сервера відсутній	Перевірити таблицю маршрутизації на роутері

Таблиця 6.3 – Типові проблеми DHCP/DNS та методи їх усунення

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

Завдання моделює мережу невеликого медичного закладу з двома підмережами: адміністративною та медичного обладнання. DHCP-сервер і DNS-сервер розташовані в адміністративній підмережі. Пристрої медичної підмережі отримують адреси через DHCP Relay.

Топологія мережі

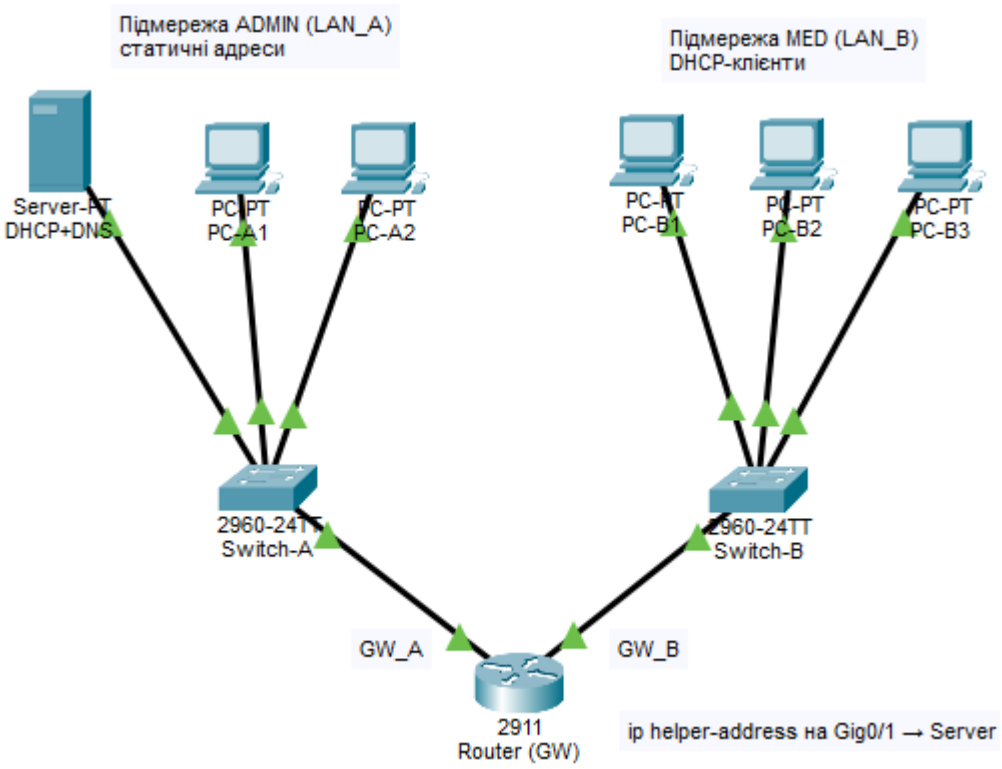

Рисунок 6.3 – Топологія мережі медичного закладу для ЛР №6

Порядок виконання

Частина 1. Побудова топології та статичне налаштування

1. Створіть новий проект у Cisco Packet Tracer.
2. Розмістіть: 1 маршрутизатор (1941 або 2911), 2 комутатори (2960), 1 сервер (End Devices → Server), 5 PC.
3. З'єднайте Server, PC-A1 та PC-A2 зі Switch-A (Straight-through).
4. З'єднайте PC-B1, PC-B2, PC-B3 зі Switch-B (Straight-through).
5. З'єднайте Switch-A з маршрутизатором (Gig0/0) та Switch-B з маршрутизатором (Gig0/1).
6. Налаштуйте маршрутизатор: hostname, Gig0/0 (IP = GW_A, /24, no shutdown), Gig0/1 (IP = GW_B, /24, no shutdown). Збережіть конфігурацію.
7. Налаштуйте Server статичною адресою: IP = IP_SERVER, маска /24, шлюз = GW_A.
8. Налаштуйте PC-A1 статичною адресою: IP = IP_A1, маска /24, шлюз = GW_A.

Частина 2. Налаштування DHCP

1. На маршрутизаторі налаштуйте два DHCP-пули відповідно до вашого варіанту:
2. Пул ADMIN для LAN_A: excluded-address (перші 20 адрес), network, default-router = GW_A, dns-server = IP_SERVER, lease 1 0 0.
3. Пул MED для LAN_B: excluded-address (перші 10 адрес), network, default-router = GW_B, dns-server = IP_SERVER, lease 0 8 0.
4. Налаштуйте PC-A2 на автоматичне отримання адреси (DHCP): Desktop → IP Configuration → DHCP. Зачекайте та перевірте отриману адресу командою ipconfig.
5. Налаштуйте PC-B1, PC-B2, PC-B3 на автоматичне отримання адреси (DHCP).
6. На маршрутизаторі на інтерфейсі Fa0/1 (що дивиться на LAN_B) налаштуйте ip helper-address IP_SERVER.
7. Перевірте, що PC-B1–PC-B3 отримали адреси командою `ipconfig` на кожному. Скріншоти.
8. Виконайте `show ip dhcp binding` на маршрутизаторі – мають відображатися всі видані оренди. Скріншот.
9. Виконайте `show ip dhcp pool` – перевірте використання пулів. Скріншот.

Частина 3. Налаштування DNS

1. Відкрийте сервер → Services → DNS → увімкніть DNS Service.
2. Додайте DNS-записи типу A відповідно до вашого варіанту (мінімум 4 записи: сервер, маршрутизатор та два довільні хости).
3. На PC-A2 виконайте `nslookup server.med-center.local` – перевірте розв'язання імені. Скріншот.
4. Виконайте `ping server.med-center.local` з PC-A2 та PC-B1. Скріншоти.
5. Виконайте `nslookup router.med-center.local` з PC-B2. Скріншот.

Частина 4. Перевірка наскрізного зв'язку

1. Ping з PC-B1 (DHCP-клієнт) до Server (статична адреса). Скріншот.
2. Ping з PC-A1 (статична) до PC-B3 (DHCP). Скріншот.
3. Виконайте `ipconfig /release` та `ipconfig /renew` на PC-A2 – переконайтесь, що адреса оновлюється. Скріншот до та після.
4. Збережіть конфігурацію маршрутизатора.

Таблиця адресації (заповнити у звіті)

Пристрій	IP-адреса	Маска підмережі	Шлюз / Примітка
Router Gig0/0 (GW_A)		255.255.255.0	–
Router Gig0/1 (GW_B)		255.255.255.0	–
Server (DHCP+DNS)		255.255.255.0	GW_A (статично)
PC-A1		255.255.255.0	GW_A (статично)
PC-A2	отримано від DHCP	255.255.255.0	GW_A (DHCP)
PC-B1	отримано від DHCP	255.255.255.0	GW_B (DHCP)
PC-B2	отримано від DHCP	255.255.255.0	GW_B (DHCP)
PC-B3	отримано від DHCP	255.255.255.0	GW_B (DHCP)

Таблиця 6.4 – Таблиця адресації

Варіанти завдань

Кожен варіант містить дві підмережі (LAN_A – адміністративна, LAN_B – медична), адресу сервера та адреси статичних хостів. Ім'я домену для всіх варіантів: med-center.local.

В.	LAN_A /24	LAN_B /24	GW_A	GW_B	IP_SERVER / IP_A1
1	192.168.1.0	192.168.2.0	192.168.1.1	192.168.2.1	192.168.1.100 / .101
2	192.168.3.0	192.168.4.0	192.168.3.1	192.168.4.1	192.168.3.100 / .101
3	192.168.5.0	192.168.6.0	192.168.5.1	192.168.6.1	192.168.5.100 / .101
4	172.16.1.0	172.16.2.0	172.16.1.1	172.16.2.1	172.16.1.100 / .101
5	172.16.3.0	172.16.4.0	172.16.3.1	172.16.4.1	172.16.3.100 / .101
6	10.10.1.0	10.10.2.0	10.10.1.1	10.10.2.1	10.10.1.100 / .101
7	10.10.3.0	10.10.4.0	10.10.3.1	10.10.4.1	10.10.3.100 / .101
8	10.20.1.0	10.20.2.0	10.20.1.1	10.20.2.1	10.20.1.100 / .101
9	172.20.1.0	172.20.2.0	172.20.1.1	172.20.2.1	172.20.1.100 / .101
10	172.20.3.0	172.20.4.0	172.20.3.1	172.20.4.1	172.20.3.100 / .101
11	192.168.10.0	192.168.20.0	192.168.10.1	192.168.20.1	192.168.10.100 / .101
12	192.168.30.0	192.168.40.0	192.168.30.1	192.168.40.1	192.168.30.100 / .101
13	10.30.1.0	10.30.2.0	10.30.1.1	10.30.2.1	10.30.1.100 / .101
14	10.40.1.0	10.40.2.0	10.40.1.1	10.40.2.1	10.40.1.100 / .101
15	10.50.1.0	10.50.2.0	10.50.1.1	10.50.2.1	10.50.1.100 / .101

Таблиця 6.5 – Варіанти завдань для лабораторної роботи № 6

DNS-записи (однакові для всіх варіантів, з адресами свого варіанту):

Тип	Ім'я	Значення (адреса свого варіанту)
A	`server.med-center.local`	`IP_SERVER`
A	`router.med-center.local`	`GW_A`
A	`gw-med.med-center.local`	`GW_B`
A	`workstation1.med-center.local`	`IP_A1`

Таблиця 6.5 – DNS-записи для налаштування

Вимоги до звіту

Звіт має містити:

1) Заповнену таблицю адресації з фактично отриманими DHCP-адресами;
2) Скріншот топології;
3) Скріншоти `ipconfig` на PC-A2, PC-B1, PC-B2, PC-B3 (отримані DHCP-адреси);
4) Скріншот `show ip dhcp binding` на маршрутизаторі;
5) Скріншот `show ip dhcp pool`;
6) Скріншоти `nslookup` та `ping` за DNS-іменем з PC-A2 та PC-B1;
7) Скріншот результату `ipconfig /release` та `/renew`;
8) Відповіді на контрольні запитання.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке DHCP і яку проблему він вирішує? Які параметри, крім IP-адреси, може передавати DHCP-сервер клієнту?
2. Розшифруйте абревіатуру DORA та опишіть кожне з чотирьох повідомлень процесу отримання DHCP-адреси. Чому перший пакет є широкомовним?
3. Що таке Lease Time (час оренди) в DHCP? Коли клієнт намагається поновити оренду вперше і вдруге?
4. Що таке DHCP Relay Agent? Навіщо він потрібен і на якому інтерфейсі маршрутизатора налаштовується команда `ip helper-address`?
5. Що станеться, якщо не налаштувати `ip helper-address`, а DHCP-сервер знаходиться в іншій підмережі ніж клієнти?
6. Що означає адреса `169.254.x.x` на мережевому інтерфейсі комп'ютера? Яка служба її призначає і що це означає для діагностики?
7. Що таке DNS і яку функцію він виконує? Чим відрізняється A-запис від CNAME-запису?
8. Опишіть послідовність кроків, які виконує операційна система при спробі відкрити сайт за доменним іменем.
9. Яка команда на PC дозволяє перевірити розв'язання DNS-імені? Яка команда примусово оновлює DHCP-оренду?
10. Клієнт отримав IP-адресу від DHCP, але `ping` за іменем (наприклад, `ping server.local`) не працює, тоді як `ping` за IP-адресою – працює. Яка найімовірніша причина і як її усунути?

Лабораторна робота №7.

VLAN та міжмережева комунікація (Inter-VLAN Routing).

Мета роботи: Зрозуміти концепцію VLAN як засобу логічного поділу фізичної мережі на ізольовані широкомовні домени. Вивчити типи портів комутатора (access, trunk) та протокол тегування 802.1Q. Ознайомитися з протоколом VTP для централізованого управління VLAN. Отримати практичні навички створення та налаштування VLAN на комутаторах Cisco, налаштування trunk-портів, організації Inter-VLAN Routing методом Router-on-a-Stick в Cisco Packet Tracer, перевірки ізоляції трафіку між VLAN та зв'язку через маршрутизатор.

Теоретичні відомості:

Що таке VLAN і навіщо він потрібен

У лабораторній роботі №3 ми розглядали локальну мережу як єдиний широкомовний домен: всі пристрої на одному або кількох комутаторах отримують широкомовні пакети від будь-якого іншого пристрою. У невеликій мережі це прийнятно, але у великій лікарні така організація призводить до серйозних проблем.

VLAN (Virtual Local Area Network) – технологія логічного поділу однієї фізичної мережі (комутаторів) на кілька незалежних широкомовних доменів. Пристрої в різних VLAN не «бачать» один одного на канальному рівні, навіть якщо підключені до одного фізичного комутатора.

Переваги VLAN у мережі медичного закладу

Перевага	Опис для медичної мережі
Безпека	Медичні прилади, ЕМК-сервери та гостьовий Wi-Fi ізольовані. Пацієнт не може «бачити» медичне обладнання
Зменшення broadcast	Широкомовний шторм від несправного пристрою не впливає на інші VLAN
Гнучкість	Лікар може перейти в інший кабінет і залишитися у своєму VLAN незалежно від фізичного порту
Економія обладнання	Один комутатор замість кількох фізичних – менше витрат
QoS	Пріоритизація трафіку: VoIP та медичне обладнання важливіші за гостьовий Wi-Fi

Таблиця 7.1 – Переваги VLAN у мережі медичного закладу

Типова схема VLAN для лікарні

VLAN ID	Назва	Підмережа	Призначення
10	ADMIN	192.168.10.0/24	Адміністрація, бухгалтерія
20	DOCTORS	192.168.20.0/24	Робочі станції лікарів, ЕМК
30	MED-DEVICES	192.168.30.0/24	Медичні монітори, УЗД, МРТ
40	VOIP	192.168.40.0/24	IP-телефони
50	GUEST	192.168.50.0/24	Гостьовий Wi-Fi для пацієнтів
99	MGMT	192.168.99.0/24	Управління мережевим обладнанням

Таблиця 7.2 – Приклад схеми VLAN для мережі лікарні

Типи портів комутатора: Access та Trunk

Access-порт

Access-порт – порт комутатора, що належить до одного конкретного VLAN. До access-порту підключаються кінцеві пристрої (PC, принтери, IP-телефони, медичне обладнання). Кадри, що надходять через access-порт, не містять VLAN-тегу – комутатор сам знає, якому VLAN цей порт належить.

Trunk-порт та протокол 802.1Q

Trunk-порт – порт комутатора, що передає трафік кількох VLAN одночасно. Використовується для з'єднання комутаторів між собою або комутатора з маршрутизатором. Щоб розрізнити, якому VLAN належить кожен кадр, використовується тегування.

IEEE 802.1Q – стандартний протокол тегування VLAN. До кожного Ethernet-кадру на trunk-порту додається 4-байтовий тег, що містить VLAN ID (12 біт, значення 1–4094).

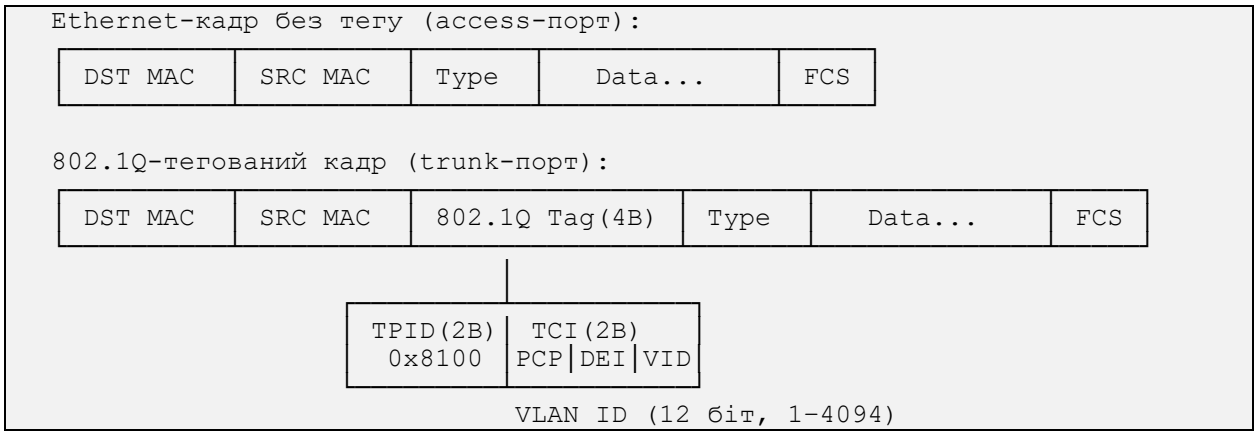

Рисунок 7.1 – Структура Ethernet-кадру з тегом 802.1Q

Native VLAN – VLAN, кадри якого передаються через trunk без тегу. За замовчуванням це VLAN 1. Native VLAN на обох кінцях trunk-з'єднання повинен збігатися, інакше виникнуть проблеми з комунікацією.

Налаштування VLAN на комутаторі Cisco

Створення VLAN

```
! Спосіб 1: через режим VLAN database
Switch(config)# vlan 10
Switch(config-vlan)# name ADMIN
Switch(config-vlan)# exit

Switch(config)# vlan 20
Switch(config-vlan)# name DOCTORS
Switch(config-vlan)# exit

Switch(config)# vlan 30
Switch(config-vlan)# name MED-DEVICES
Switch(config-vlan)# exit

! Перевірка: переглянути всі VLAN
Switch# show vlan brief
```

Приклад 7.1 – Створення VLAN на комутаторі Cisco

Налаштування access-порту

```
! Призначити порт до VLAN 10 (режим access):
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# spanning-tree portfast
Switch(config-if)# exit

! Призначити діапазон портів до одного VLAN (зручно для кількох PC):
Switch(config)# interface range FastEthernet0/2 - 5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 20
Switch(config-if-range)# spanning-tree portfast
Switch(config-if-range)# exit
```

Приклад 7.2 – Налаштування access-портів

Налаштування trunk-порту

```
! Налаштувати trunk-порт (для з'єднання з іншим комутатором або роутером):
Switch(config)# interface FastEthernet0/24
Switch(config-if)# switchport mode trunk

! Дозволити лише конкретні VLAN через trunk (рекомендується):
Switch(config-if)# switchport trunk allowed vlan 10,20,30,99

! Встановити Native VLAN (за замовчуванням VLAN 1):
Switch(config-if)# switchport trunk native vlan 99
Switch(config-if)# exit

! Перевірка trunk-портів:
Switch# show interfaces trunk
```

Приклад 7.3 – Налаштування trunk-порту

Увага: Native VLAN

За замовчуванням Native VLAN = 1, і через нього проходить нетегований трафік. З міркувань безпеки рекомендується змінити Native VLAN на невикористовуваний VLAN (наприклад, 99) та вилучити VLAN 1 з усіх trunk-з'єднань. Це захищає від атаки VLAN hopping.

Протокол VTP (VLAN Trunking Protocol)

VTP (VLAN Trunking Protocol) – пропрієтарний протокол Cisco для централізованого управління базою VLAN у групі комутаторів (VTP-домені). Замість того щоб створювати VLAN на кожному комутаторі окремо, адміністратор налаштовує їх на одному – VTP Server, а решта комутаторів (VTP Client) автоматично отримують оновлення.

Режим VTP	Де налаштовується	Можливості
Server	Центральний комутатор	Створює, змінює, видаляє VLAN; поширює інформацію
Client	Всі інші комутатори	Отримує VLAN-інформацію від сервера; не може змінювати VLAN
Transparent	Ізольований комутатор	Не отримує і не поширює VTP; VLAN налаштовуються локально
Off (VTPv3)	Повне вимкнення	VTP повністю вимкнено

Таблиця 7.3 – Режими роботи VTP

```
! Налаштування VTP на Server-комутаторі:
Switch(config)# vtp mode server
Switch(config)# vtp domain MED-CENTER
Switch(config)# vtp password Med@2024
Switch(config)# vtp version 2

! Налаштування VTP на Client-комутаторі:
Switch(config)# vtp mode client
Switch(config)# vtp domain MED-CENTER
Switch(config)# vtp password Med@2024

! Перевірка VTP:
Switch# show vtp status
```

Приклад 7.4 – Налаштування VTP Server та Client

Міжмережева комунікація між VLAN (Inter-VLAN Routing)

VLAN ізолюють трафік на канальному рівні – пристрої з різних VLAN не можуть спілкуватися безпосередньо. Для організації зв'язку між VLAN потрібна маршрутизація (рівень 3). Існує два основних методи:

- Router-on-a-Stick – маршрутизатор із підінтерфейсами (один фізичний порт, кілька логічних)
- Layer 3 Switch (MLS) – комутатор з підтримкою маршрутизації (SVI-інтерфейси)

Метод Router-on-a-Stick

Router-on-a-Stick («маршрутизатор на паличці») – метод, при якому один фізичний інтерфейс маршрутизатора підключається до trunk-порту комутатора і розділяється на кілька підінтерфейсів – по одному для кожного VLAN. Кожен підінтерфейс отримує IP-адресу, що стає шлюзом для відповідного VLAN.

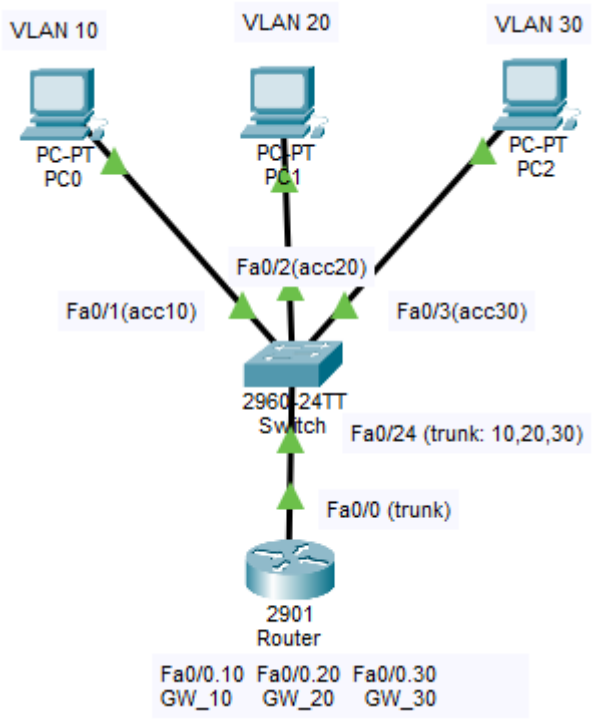

Рисунок 7.2 – Схема Router-on-a-Stick

Налаштування підінтерфейсів Router-on-a-Stick

```
! Увімкнути фізичний інтерфейс (БЕЗ IP-адреси на ньому!):
Router(config)# interface GigabitEthernet0/0
Router(config-if)# no shutdown
Router(config-if)# exit

! Підінтерфейс для VLAN 10:
Router(config)# interface GigabitEthernet0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit

! Підінтерфейс для VLAN 20:
Router(config)# interface GigabitEthernet0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit

! Підінтерфейс для VLAN 30:
Router(config)# interface GigabitEthernet0/0.30
Router(config-subif)# encapsulation dot1Q 30
Router(config-subif)# ip address 192.168.30.1 255.255.255.0
Router(config-subif)# exit

! Підінтерфейс для Native VLAN 99 (управління):
Router(config)# interface GigabitEthernet0/0.99
Router(config-subif)# encapsulation dot1Q 99 native
Router(config-subif)# ip address 192.168.99.1 255.255.255.0
Router(config-subif)# exit
```

Приклад 7.5 – Налаштування підінтерфейсів Router-on-a-Stick

`encapsulation dot1Q` – обов'язкова команда

Команда `encapsulation dot1Q <vlan-id>` є обов'язковою для кожного підінтерфейсу – вона вказує, трафік якого VLAN (за тегом 802.1Q) має оброблятися на цьому підінтерфейсі. Без цієї команди підінтерфейс не знатиме, які кадри йому «призначені». Ключове слово `native` вказується лише для `Native VLAN`

Inter-VLAN Routing на Layer 3 комутаторі (SVI)

Більш сучасний підхід – використання комутатора рівня 3 (наприклад, Cisco Catalyst 3560 або 3650). Такий комутатор підтримує маршрутизацію без окремого маршрутизатора. Для кожного VLAN створюється SVI (Switched Virtual Interface) – логічний інтерфейс, що стає шлюзом для цього VLAN.

```
! Увімкнути IP-маршрутизацію на L3-комутаторі:
Switch(config)# ip routing

! Створити SVI для VLAN 10:
Switch(config)# interface vlan 10
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit

! Створити SVI для VLAN 20:
Switch(config)# interface vlan 20
Switch(config-if)# ip address 192.168.20.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit

! Створити SVI для VLAN 30:
Switch(config)# interface vlan 30
```

```
Switch(config-if)# ip address 192.168.30.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit

! Перевірка маршрутизації між VLAN:
Switch# show ip route
```

Приклад 7.6 – Inter-VLAN Routing на L3-комутаторі через SVI

Команди перевірки налаштування VLAN

```
! Переглянути всі VLAN та їх порти (коротко):
Switch# show vlan brief

VLAN Name                 Status    Ports
---- ———————————————————— ———————— ——————————————————————————
1    default              active    Fa0/6, Fa0/7...
10   ADMIN                active    Fa0/1
20   DOCTORS              active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
30   MED-DEVICES          active    (none)

! Детальна інформація про конкретний VLAN:
Switch# show vlan id 10

! Переглянути trunk-порти:
Switch# show interfaces trunk

Port      Mode       Encapsulation  Status        Native vlan
Fa0/24    on         802.1q         trunking      99

Port      Vlans allowed on trunk
Fa0/24    10,20,30,99

! Перевірити режим конкретного порту:
Switch# show interfaces FastEthernet0/1 switchport

! Переглянути стан VTP:
Switch# show vtp status

! Переглянути підінтерфейси маршрутизатора:
Router# show ip interface brief

! Перевірити таблицю маршрутизації (між VLAN):
Router# show ip route
```

Приклад 7.7 – Команди перевірки VLAN та Inter-VLAN Routing

Зведена таблиця команд

Команда	Призначення
`vlan <id>`	Увійти в режим конфігурації VLAN
`name <назва>`	Задати ім'я VLAN
`switchport mode access`	Встановити порт у режим access
`switchport access vlan <id>`	Призначити access-порт до VLAN
`switchport mode trunk`	Встановити порт у режим trunk
`switchport trunk allowed vlan <список>`	Дозволити конкретні VLAN на trunk
`switchport trunk native vlan <id>`	Встановити Native VLAN на trunk

`encapsulation dot1Q <id>`	Тегування 802.1Q на підінтерфейсі
`ip routing`	Увімкнути маршрутизацію на L3-комутаторі
`show vlan brief`	Список всіх VLAN та їх портів
`show interfaces trunk`	Стан і параметри trunk-портів
`show interfaces <порт> switchport`	Режим порту та VLAN-налаштування
`show vtp status`	Стан і режим VTP

Таблиця 7.4 – Основні команди налаштування та перевірки VLAN

Діагностика проблем VLAN

Алгоритм діагностики

1. Перевірте `show vlan brief` – чи існує потрібний VLAN і чи призначені до нього потрібні порти.
2. Перевірте `show interfaces trunk` – чи є trunk між комутаторами і чи дозволені потрібні VLAN.
3. Перевірте `show interfaces <порт> switchport` – переконайтесь у правильному режимі (`access/trunk`) та VLAN.
4. Якщо ping у межах одного VLAN не проходить – перевірте IP-адреси та маски. Вони мають бути в одній підмережі.
5. Якщо `ping` між різними VLAN не проходить – перевірте конфігурацію Router-on-a-Stick: чи є підінтерфейс, чи виконана `encapsulation dot1Q`, чи піднятий фізичний інтерфейс (`no shutdown`).
6. Перевірте `show ip route` на маршрутизаторі – має бути маршрут `C` (`connected`) для кожного підінтерфейсу.

Типові помилки та їх вирішення

Симптом	Причина	Вирішення
`Ping` між PC одного VLAN не проходить	VLAN не створений або порт не призначений	`show vlan brief` – перевірити VLAN та порти
`Trunk` не пропускає трафік VLAN	VLAN не дозволений на trunk	`switchport trunk allowed vlan add <id>`
`Ping` між різними VLAN не проходить	Відсутній підінтерфейс або немає `encapsulation`	Перевірити `show ip interface brief` та конфіг субінтерфейсів
Підінтерфейс є, але не піднімається	Фізичний інтерфейс у стані `shutdown`	`no shutdown` на фізичному `Fa0/0`
Неправильний VLAN отримується через `trunk`	Native VLAN не збігається на обох кінцях	Встановити однаковий native vlan на обох портах
VTP не поширює VLAN	Різний VTP domain або password	`show vtp status` – перевірити `domain` та `revision`
Після VTP Client втратив VLAN	VTP revision number скинувся	Перевірити `revision`; у критичних мережах – Transparent

Таблиця 7.5 – Типові помилки VLAN та методи їх усунення

Небезпека VTP у виробничих мережах

VTP має відомий ризик: якщо підключити до мережі новий комутатор з вищим VTP Revision Number та режимом Server, він може перезаписати всю базу VLAN на всіх комутаторах домену – навіть видалити всі існуючі VLAN! У мережах медичних закладів, де надійність критична, рекомендується або використовувати VTP Transparent, або VTPv3 з захистом від цієї проблеми.

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

Завдання моделює мережу медичного закладу з трьома відділами: адміністрація, лікарі та медичне обладнання. Кожен відділ отримує окремий VLAN. Зв'язок між VLAN організується методом Router-on-a-Stick через один маршрутизатор. Додатково налаштовується VTP для управління VLAN через два комутатори.

Топологія мережі

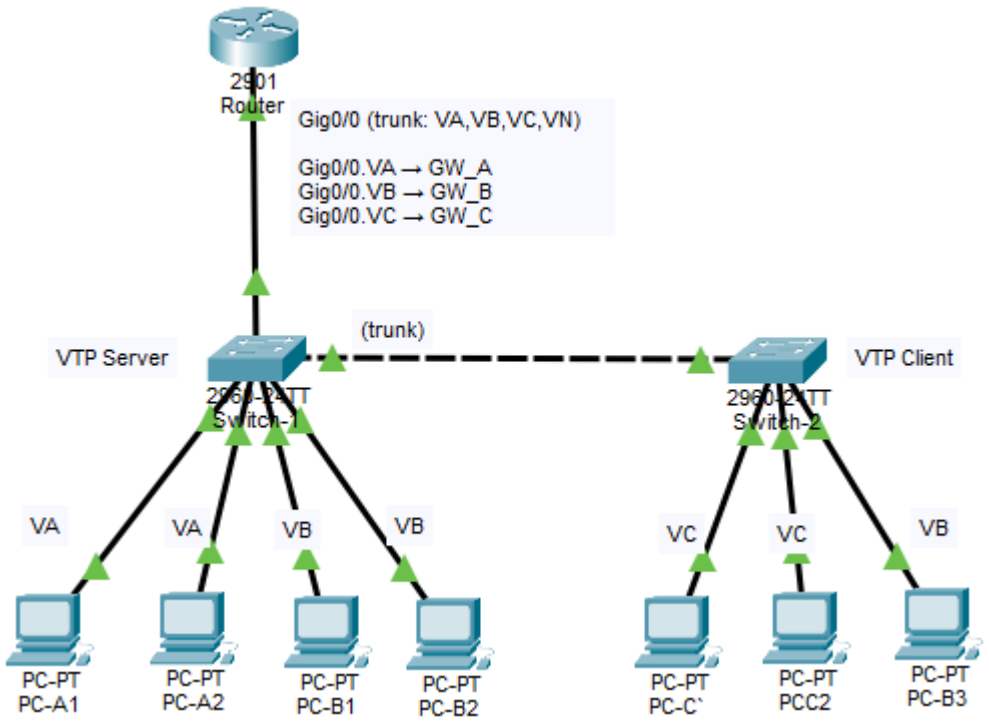

Рисунок 7.3 – Топологія мережі для ЛР №7 (VA, VB, VC – номери VLAN за варіантом)

Порядок виконання

Частина 1. Побудова топології

1. Створіть новий проект у Cisco Packet Tracer.
2. Розмістіть: 1 маршрутизатор (1941 або 2911), 2 комутатори Catalyst 2960, 7 PC.
3. З'єднайте Switch-1 з маршрутизатором (Fa0/24 → Gig0/0, Straight-through).
4. З'єднайте Switch-1 з Switch-2 (Fa0/23 → Fa0/24, Cross-over).

5. Підключіть PC-A1, PC-A2 до Fa0/1, Fa0/2 на Switch-1; PC-B1, PC-B2 до Fa0/3, Fa0/4 на Switch-1.
6. Підключіть PC-C1, PC-C2 до Fa0/1, Fa0/2 на Switch-2; PC-B3 до Fa0/3 на Switch-2.

Частина 2. Налаштування Switch-1 (VTP Server)

1. Відкрийте CLI Switch-1.
2. Встановіть ім'я: `hostname SW1-MedCenter`.
3. Налаштуйте VTP: `mode server`, `domain` та `password` відповідно до варіанту.
4. Створіть три VLAN відповідно до варіанту (VA, VB, VC) з іменами ADMIN, DOCTORS, MED-DEVICES.
5. Налаштуйте access-порти: Fa0/1, Fa0/2 → VA; Fa0/3, Fa0/4 → VB.
6. Налаштуйте trunk Fa0/24 (до маршрутизатора): allowed vlan VA,VB,VC; native vlan VN.
7. Налаштуйте trunk Fa0/23 (до Switch-2): allowed vlan VA,VB,VC; native vlan VN.
8. Збережіть конфігурацію.

Частина 3. Налаштування Switch-2 (VTP Client)

1. Відкрийте CLI Switch-2.
2. Встановіть ім'я: `hostname SW2-MedCenter`.
3. Налаштуйте VTP: `mode client`, `domain` та `password` – однакові з Switch-1.
4. Налаштуйте trunk Fa0/24 (до Switch-1): allowed vlan VA,VB,VC; native vlan VN.
5. Налаштуйте access-порти: Fa0/1, Fa0/2 → VC; Fa0/3 → VB.
6. Виконайте `show vlan brief` – VLAN мають з'явитися автоматично від VTP Server. Скріншот.
7. Збережіть конфігурацію.

Частина 4. Налаштування маршрутизатора (Router-on-a-Stick)

1. Відкрийте CLI маршрутизатора.
2. Встановіть ім'я: `hostname GW-MedCenter`.
3. Увімкніть фізичний інтерфейс Gig0/0 командою `no shutdown` (БЕЗ IP-адреси).
4. Створіть підінтерфейс для кожного VLAN відповідно до варіанту: `encapsulation dot1Q <VA/VB/VC>`, `ip address GW_A/GW_B/GW_C`.
5. Збережіть конфігурацію.

Частина 5. Налаштування PC та перевірка

1. Налаштуйте IP-адреси на всіх PC відповідно до варіанту та таблиці адресації. Шлюз для VLAN A = GW_A, для B = GW_B, для C = GW_C.
2. Перевірте `show vlan brief` на обох комутаторах – порти мають бути у правильних VLAN. Скріншоти.
3. Перевірте `show interfaces trunk` – trunk-порти мають бути активними та пропускати потрібні VLAN. Скріншоти.
4. Перевірте `show ip interface brief` на маршрутизаторі – підінтерфейси мають бути up/up. Скріншот.
5. Ping в межах одного VLAN: PC-A1 → PC-A2 (мають спілкуватися). Скріншот.
6. Ping між різними VLAN: PC-A1 → PC-B1, PC-A1 → PC-C1 (мають спілкуватися через маршрутизатор). Скріншоти.

7. Ping PC-B3 (Switch-2) → PC-A1 (Switch-1) – пакет проходить через міжкомутаторний trunk. Скріншот.
8. Перевірте ізоляцію: тимчасово відключіть підінтерфейс маршрутизатора командою `shutdown` і переконайтесь, що `ping` між різними VLAN більше не проходить. Відновіть (no shutdown).

Таблиця адресації (заповнити у звіті)

Пристрій / Інтерфейс	IP-адреса	Маска підмережі	Шлюз / VLAN
Router Gig0/0.VA (GW_A)		255.255.255.0	VLAN VA
Router Gig0/0.VB (GW_B)		255.255.255.0	VLAN VB
Router Gig0/0.VC (GW_C)		255.255.255.0	VLAN VC
PC-A1 (VLAN VA, SW1)		255.255.255.0	GW_A
PC-A2 (VLAN VA, SW1)		255.255.255.0	GW_A
PC-B1 (VLAN VB, SW1)		255.255.255.0	GW_B
PC-B2 (VLAN VB, SW1)		255.255.255.0	GW_B
PC-B3 (VLAN VB, SW2)		255.255.255.0	GW_B
PC-C1 (VLAN VC, SW2)		255.255.255.0	GW_C
PC-C2 (VLAN VC, SW2)		255.255.255.0	GW_C

Таблиця 7.6 – Таблиця адресації

Варіанти завдань

Кожен варіант містить номери трьох VLAN (VA, VB, VC), Native VLAN (VN), підмережі для кожного VLAN та VTP-параметри. Адреси GW є першими хост-адресами підмереж. Адреси PC призначаються студентом самостійно (наступні хост-адреси).

B.	VA	VB	VC	VN	Підмережа A	Підмережа B	Підмережа C	VTP Domain	VTP Pass
1	10	20	30	99	192.168.10.0	192.168.20.0	192.168.30.0	MED-CTR-01	Med@01
2	11	21	31	99	192.168.11.0	192.168.21.0	192.168.31.0	MED-CTR-02	Med@02
3	12	22	32	99	192.168.12.0	192.168.22.0	192.168.32.0	MED-CTR-03	Med@03
4	13	23	33	99	192.168.13.0	192.168.23.0	192.168.33.0	MED-CTR-04	Med@04
5	14	24	34	98	10.10.14.0	10.10.24.0	10.10.34.0	MED-CTR-05	Med@05
6	15	25	35	98	10.10.15.0	10.10.25.0	10.10.35.0	MED-CTR-06	Med@06
7	16	26	36	98	172.16.16.0	172.16.26.0	172.16.36.0	MED-CTR-07	Med@07
8	17	27	37	98	172.16.17.0	172.16.27.0	172.16.37.0	MED-CTR-08	Med@08
9	18	28	38	97	192.168.18.0	192.168.28.0	192.168.38.0	MED-CTR-09	Med@09
10	19	29	39	97	192.168.19.0	192.168.29.0	192.168.39.0	MED-CTR-10	Med@10
11	40	50	60	99	10.20.40.0	10.20.50.0	10.20.60.0	MED-CTR-11	Med@11
12	41	51	61	99	10.20.41.0	10.20.51.0	10.20.61.0	MED-CTR-12	Med@12
13	42	52	62	98	172.20.42.0	172.20.52.0	172.20.62.0	MED-CTR-13	Med@13

14	43	53	63	98	172.20.43.0	172.20.53.0	172.20.63.0	MED-CTR-14	Med@14
15	44	54	64	97	10.30.44.0	10.30.54.0	10.30.64.0	MED-CTR-15	Med@15

Таблиця 7.7 – Варіанти завдань для лабораторної роботи № 7

Вимоги до звіту

Звіт має містити:
1) Заповнену таблицю адресації;
2) Скріншот топології;
3) Скріншоти `show vlan brief` на обох комутаторах;
4) Скріншот `show interfaces trunk` на Switch-1;
5) Скріншот `show ip interface brief` на маршрутизаторі;
6) Скріншоти `ping` у межах одного VLAN та між різними VLAN;
7) Скріншот `show vtp status` на Switch-2 (підтвердження отримання VLAN від Server);
8) Відповіді на контрольні запитання.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке VLAN? Яку проблему він вирішує порівняно зі звичайною фізичною мережею? Як VLAN впливає на широкомовний домен?
2. Чим відрізняються access-порт і trunk-порт комутатора? У яких ситуаціях використовується кожен?
3. Що таке протокол 802.1Q? Опишіть структуру тегу, що він додає до Ethernet-кадру. Що таке Native VLAN?
4. Що таке VTP? Які режими роботи він підтримує? Чим відрізняються Server, Client та Transparent?
5. Яка небезпека пов'язана з VTP Revision Number і як захиститись від неї у виробничих мережах?
6. Що таке Inter-VLAN Routing? Чому пристрої з різних VLAN не можуть спілкуватися без маршрутизації?
7. Опишіть метод Router-on-a-Stick. Скільки фізичних інтерфейсів маршрутизатора потрібно? Яка команда є обов'язковою для кожного підінтерфейсу?
8. Яка різниця між Router-on-a-Stick та Inter-VLAN Routing на L3-комутаторі через SVI? Які переваги кожного методу?
9. Назвіть три можливі причини, через які ping між PC з різних VLAN не проходить, хоча VLAN створені і порти правильно налаштовані.
10. Поясніть, навіщо у мережі лікарні доцільно розміщувати медичне обладнання, комп'ютери лікарів та гостьовий Wi-Fi у різних VLAN. Які загрози це усуває?

Лабораторна робота №8.

NAT, списки контролю доступу (ACL) та основи мережевої безпеки.

Мета роботи: Вивчити принципи та типи NAT. Зрозуміти концепцію списків контролю доступу (ACL). Отримати практичні навички налаштування PAT та ACL на маршрутизаторах Cisco в Cisco Packet Tracer, застосування ACL для обмеження доступу між підмережами медичного закладу та перевірки роботи засобами `show` та `debug`

Теоретичні відомості:

NAT – трансляція мережевих адрес

У ЛР №1 було розглянуто приватні IP-адреси (RFC 1918): 10.x.x.x, 172.16–31.x.x, 192.168.x.x. Ці адреси не маршрутизуються в Інтернеті – маршрутизатори провайдерів їх ігнорують. Щоб внутрішні пристрої мережі могли виходити в Інтернет, використовується NAT.

NAT (Network Address Translation) – технологія заміни IP-адрес у заголовках пакетів при їх проходженні через маршрутизатор. Внутрішні приватні адреси замінюються зовнішньою публічною адресою, і навпаки.

Термінологія NAT

Термін	Значення
Inside Local	Приватна IP-адреса внутрішнього пристрою (наприклад, 192.168.1.10)
Inside Global	Публічна IP-адреса, яку «бачить» Інтернет (наприклад, 203.0.113.5)
Outside Global	IP-адреса зовнішнього (інтернет) сервера
Inside interface	Інтерфейс маршрутизатора, що дивиться на внутрішню мережу (ip nat inside)
Outside interface	Інтерфейс маршрутизатора, що дивиться назовні – до провайдера (ip nat outside)

Таблиця 8.1 – Термінологія NAT

Типи NAT

Тип	Відповідність	Використання
Static NAT	1 приватна ↔ 1 публічна (постійно)	Публікація внутрішніх серверів (веб, пошта)
Dynamic NAT	1 приватна → 1 з пулу публічних	Рідко. Пул публічних адрес > 1
PAT / NAT Overload	Багато приватних → 1 публічна (через порти)	Найпоширеніший. Весь офіс через одну IP

Таблиця 8.2 – Типи NAT

PAT – Port Address Translation (NAT Overload)

PAT (Port Address Translation), також відомий як NAT Overload – найпоширеніший тип NAT. Тисячі внутрішніх пристроїв використовують одну публічну IP-адресу, розрізняючись за номерами портів TCP/UDP. Саме так працює домашній роутер та більшість корпоративних мереж.

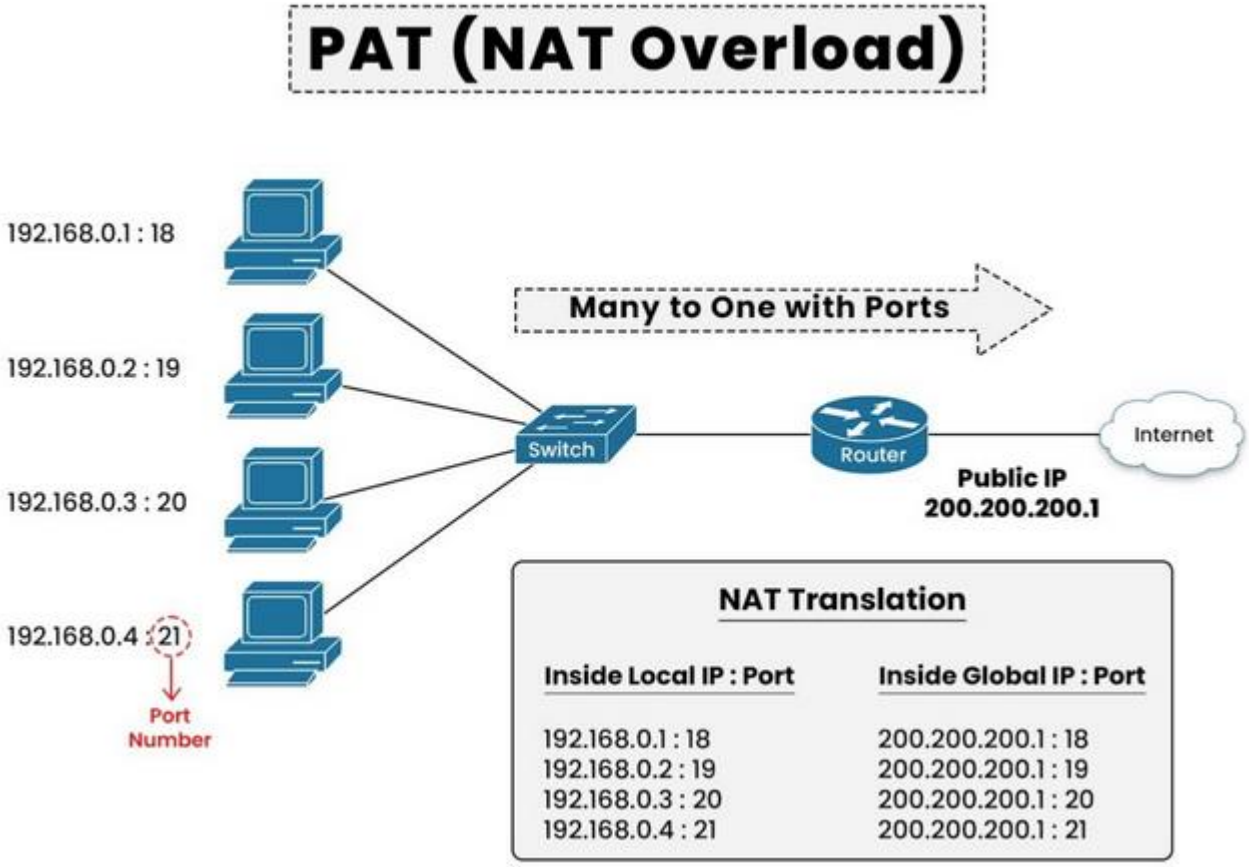

Рисунок 8.1 – Принцип роботи PAT: багато внутрішніх адрес – одна зовнішня

Налаштування PAT на Cisco IOS

```
! Крок 1: Визначити внутрішній (inside) та зовнішній (outside) інтерфейси
Router(config)# interface FastEthernet0/0
Router(config-if)# ip nat inside
Router(config-if)# exit

Router(config)# interface FastEthernet0/1
Router(config-if)# ip nat outside
Router(config-if)# exit

! Крок 2: Створити ACL, що визначає які адреси підлягають трансляції
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255

! Крок 3: Налаштувати PAT (overload) – трансляція на зовнішній інтерфейс
Router(config)# ip nat inside source list 1 interface FastEthernet0/1
overload
```

Приклад 8.1 – Налаштування PAT на маршрутизаторі Cisco

Ключове слово `overload`

Слово `overload` в команді `ip nat inside source list` робить її PAT (а не Dynamic NAT). Без `overload` – це Dynamic NAT: кожній внутрішній адресі призначається окрема публічна. З `overload` – усі внутрішні адреси використовують одну публічну IP, розрізняючись за портами.

Static NAT – публікація сервера

Static NAT використовується коли внутрішній сервер (наприклад, веб-сервер лікарні або PACS-сервер) має бути доступний ззовні за постійною публічною адресою.

```
! Налаштування static NAT: внутрішній сервер 192.168.1.100
! отримує постійну публічну адресу 203.0.113.10
Router(config)# ip nat inside source static 192.168.1.100 203.0.113.10

! Перевірка NAT-трансляцій:
Router# show ip nat translations

Pro  Inside global     Inside local      Outside local    Outside global
---  203.0.113.10      192.168.1.100     ---              ---
tcp  203.0.113.5:10001 192.168.1.10:1025 8.8.8.8:80      8.8.8.8:80

! Статистика NAT:
Router# show ip nat statistics

! Очистити таблицю динамічних трансляцій:
Router# clear ip nat translation *
```

Приклад 8.2 – Static NAT та команди перевірки

ACL – списки контролю доступу

ACL (Access Control List) – набір правил (записів), що дозволяють або забороняють проходження пакетів через інтерфейс маршрутизатора на основі критеріїв: IP-адреса джерела/призначення, протокол, порт. ACL виконують роль простого міжмережевого екрану (firewall) на рівні маршрутизатора.

Важливо розуміти принцип роботи ACL:

- Правила перевіряються послідовно, зверху донизу.
- Застосовується ПЕРШЕ правило, що збігається з пакетом – решта не перевіряються.
- В кінці кожного ACL є неявне правило deny any – якщо жодне явне правило не спрацювало, пакет відкидається.
- Через неявний deny – в ACL завжди потрібно явно дозволити те, що не має бути заблоковано.

Стандартні ACL (Standard ACL)

Стандартні ACL фільтрують пакети лише за IP-адресою ДЖЕРЕЛА. Номери: 1–99 та 1300–1999.

Правило розміщення: стандартні ACL розміщують якомога БЛИЖЧЕ до призначення (destination), оскільки вони фільтрують лише за джерелом і можуть ненавмисно заблокувати трафік до інших мереж.

```
! Синтаксис стандартного ACL:
Router(config)# access-list <1-99> {permit|deny} <адреса-джерела> <wildcard>

! Приклад: дозволити мережу 192.168.1.0/24, заборонити решту
Router(config)# access-list 10 permit 192.168.1.0 0.0.0.255
! (неявний deny all в кінці – блокує все інше)

! Дозволити конкретний хост:
Router(config)# access-list 10 permit host 192.168.1.50

! Заборонити конкретну мережу, решту дозволити:
Router(config)# access-list 11 deny 10.0.0.0 0.255.255.255
Router(config)# access-list 11 permit any
```

```
! Застосувати ACL до інтерфейсу:
Router(config)# interface FastEthernet0/1
Router(config-if)# ip access-group 10 out
Router(config-if)# exit
```

Приклад 8.3 – Стандартний ACL

Розширені ACL (Extended ACL)

Розширені ACL фільтрують пакети за: IP-адресою джерела і призначення, протоколом (IP, TCP, UDP, ICMP), портом джерела і призначення. Номери: 100–199 та 2000–2699.

Правило розміщення: розширені ACL розміщують якомога БЛИЖЧЕ до ДЖЕРЕЛА трафіку – щоб небажаний трафік відкидався одразу, не навантажуючи мережу.

```
! Синтаксис розширеного ACL:
! access-list <100-199> {permit|deny} <протокол>
!   <src-IP> <src-wild> <dst-IP> <dst-wild> [eq <порт>]

! Дозволити HTTP (порт 80) з мережі 192.168.1.0 до будь-якого сервера:
Router(config)# access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80

! Дозволити HTTPS (порт 443):
Router(config)# access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 443

! Дозволити DNS (порт 53, UDP):
Router(config)# access-list 100 permit udp 192.168.1.0 0.0.0.255 any eq 53

! Дозволити ICMP (ping):
Router(config)# access-list 100 permit icmp 192.168.1.0 0.0.0.255 any

! Заборонити доступ з гостьової мережі до медичного сервера:
Router(config)#  access-list  101  deny  ip  192.168.50.0  0.0.0.255  host
192.168.1.100
Router(config)# access-list 101 permit ip any any
```

Приклад 8.4 – Розширений ACL

Іменовані ACL (Named ACL)

Замість числових номерів ACL можна задавати імена. Це значно зручніше у великих мережах – одразу зрозуміло призначення ACL. Крім того, іменовані ACL дозволяють видаляти окремі рядки, що неможливо у числових.

```
! Створення стандартного іменованого ACL:
Router(config)# ip access-list standard BLOCK-GUEST
Router(config-std-nacl)# deny 192.168.50.0 0.0.0.255
Router(config-std-nacl)# permit any
Router(config-std-nacl)# exit

! Створення розширеного іменованого ACL:
Router(config)# ip access-list extended PROTECT-MED-SERVER
Router(config-ext-nacl)#   permit   tcp   192.168.20.0   0.0.0.255   host
192.168.1.100 eq 80
Router(config-ext-nacl)#   permit   tcp   192.168.10.0   0.0.0.255   host
192.168.1.100 eq 80
Router(config-ext-nacl)# deny ip any host 192.168.1.100
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# exit

! Застосувати іменований ACL до інтерфейсу:
Router(config)# interface FastEthernet0/0
Router(config-if)# ip access-group PROTECT-MED-SERVER in
Router(config-if)# exit
```

Приклад 8.5 – Іменований розширений ACL для захисту медичного сервера

Напрям застосування ACL: in та out

ACL застосовується до інтерфейсу у певному напрямку відносно маршрутизатора:

Напрям	Що фільтрується	Коли використовувати
in	Трафік, що ВХОДИТЬ в інтерфейс (від мережі до роутера)	Блокувати трафік від конкретної мережі на вході
out	Трафік, що ВИХОДИТЬ з інтерфейсу (від роутера до мережі)	Обмежити що отримує певна мережа

Таблиця 8.3 – Напрями застосування ACL

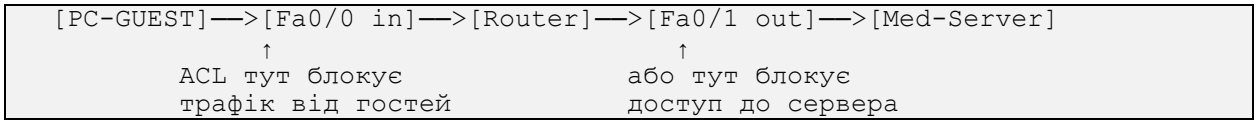

Рисунок 8.2 – Напрями in та out відносно маршрутизатора

Команди перевірки ACL та NAT

```
! ── ACL ──────────────────────────────────────────────────────

! Переглянути всі ACL та їх правила (з лічильниками спрацювань):
Router# show access-lists

Standard IP access list 10
    10 permit 192.168.1.0, wildcard bits 0.0.0.255 (15 matches)

Extended IP access list PROTECT-MED-SERVER
    10 permit tcp 192.168.20.0 0.0.0.255 host 192.168.1.100 eq 80 (8
matches)
    20 deny ip any host 192.168.1.100 (3 matches)
    30 permit ip any any (42 matches)

! Переглянути конкретний ACL:
Router# show access-lists 100
Router# show ip access-lists PROTECT-MED-SERVER

! Переглянути ACL, застосовані до інтерфейсів:
Router# show ip interface FastEthernet0/0

! Скинути лічильники спрацювань ACL:
Router# clear ip access-list counters

! ── NAT ──────────────────────────────────────────────────────

! Таблиця поточних NAT-трансляцій:
Router# show ip nat translations

! Статистика NAT (кількість трансляцій, hits, misses):
Router# show ip nat statistics

! Очистити динамічні трансляції:
Router# clear ip nat translation *

! Debug NAT (для детального відстеження в реальному часі):
Router# debug ip nat
Router# no debug all
```

Приклад 8.6 – Команди перевірки ACL та NAT

Зведена таблиця команд

Команда	Призначення
`ip nat inside / ip nat outside`	Позначити інтерфейс як inside або outside
`ip nat inside source list <ACL> int <if> overload`	Налаштувати PAT
`ip nat inside source static <in> <out>`	Статична трансляція (Static NAT)
`show ip nat translations`	Таблиця поточних NAT-трансляцій
`show ip nat statistics`	Статистика NAT
`clear ip nat translation *`	Очистити динамічні NAT-трансляції
`access-list <1-99> permit/deny <src> <wild>`	Стандартний ACL (за джерелом)
`access-list <100-199> permit/deny <proto> ...`	Розширений ACL (джерело+призначення+порт)
`ip access-list standard/extended <ім'я>`	Іменований ACL
`ip access-group <ACL> in/out`	Застосувати ACL до інтерфейсу
`show access-lists`	Всі ACL з лічильниками спрацювань
`show ip interface <if>`	ACL, застосовані до інтерфейсу

Таблиця 8.4 – Основні команди NAT та ACL

Діагностика проблем NAT та ACL

Алгоритм діагностики NAT

1. Перевірте `show ip nat statistics` – переконайтесь, що є активні трансляції (hits > 0).
2. Перевірте `show ip nat translations` – таблиця має бути непорожньою при активному трафіку.
3. Перевірте, чи правильно позначені інтерфейси: `show ip interface` – шукайте рядки `'Inbound/Outbound access list'`, а також `NAT inside/outside`.
4. Перевірте ACL, що використовується для NAT: `show access-lists` – адреса клієнта має потрапляти під правило `permit`.
5. Перевірте маршрут за замовчуванням: `show ip route` – має бути маршрут до мережі Інтернет (або симульованого ISP).
6. `Ping` від клієнта до зовнішньої адреси – якщо не проходить, але таблиця NAT порожня, перевірте ACL для NAT.

Алгоритм діагностики ACL

1. Перевірте `show access-lists` – лічильники `matches`. Якщо лічильник на `deny` збільшується – ACL блокує трафік.
2. Перевірте напрям ACL: `show ip interface <ім'я>` – ACL може бути застосовано в неправильному напрямку (`in` замість `out` або навпаки).
3. Перевірте порядок правил – більш специфічні правила мають бути ВИЩЕ більш загальних.

4. Пам'ятайте про неявний `deny`: якщо в ACL немає `permit any` – весь незазначений трафік буде заблокований.
5. Для тимчасового тестування можна видалити ACL з інтерфейсу: `no ip access-group`, перевірити зв'язок, потім повернути.

Типові помилки та їх вирішення

Симптом	Причина	Вирішення
PAT не працює, трансляцій немає	Немає маршруту за замовчуванням або ACL не охоплює адресу	`show ip route`; перевірити `access-list` для NAT
`Ping` проходить, але HTTP не працює	ACL блокує TCP порт 80/443	Додати `permit tcp ... eq 80` та `eq 443`
ACL блокує весь трафік	Відсутній `permit any` в кінці ACL	Додати `permit ip any any` або `permit any`
Static NAT не працює	Немає `ip nat inside/outside` на інтерфейсах	Перевірити `show ip interface`
ACL застосовано, але трафік не блокується	Неправильний напрям in/out	Перевірити та виправити напрям `ip access-group`
Після зміни ACL не вступають в силу	Числовий ACL – не можна редагувати рядки	Видалити весь ACL (`no access-list N`) і створити заново
NAT не транслює трафік певної мережі	Мережу не включено в ACL для NAT	Додати `permit` для цієї мережі в ACL

Таблиця 8.5 – Типові помилки NAT та ACL та методи їх усунення

ACL у мережі медичного закладу: важливі сценарії

1. Заборонити гостьовому Wi-Fi (VLAN 50) доступ до серверів ЕМК та медичного обладнання.

2. Дозволити лише адміністраторам (VLAN 10) підключатися до мережевого обладнання через SSH.

3. Обмежити доступ до PACS-серверу лише з підмережі радіологічного відділення.

4. Дозволити лікарям (VLAN 20) доступ до ЕМК-сервера лише по HTTPS (порт 443).

Правильно налаштовані ACL разом з VLAN утворюють ефективний захист персональних даних пацієнтів.

ЗАВДАННЯ НА ЛАБОРАТОРНУ РОБОТУ

Завдання моделює мережу медичного закладу з виходом в Інтернет (симульований ISP-маршрутизатор). Необхідно налаштувати PAT для забезпечення доступу внутрішніх мереж до зовнішньої мережі, Static NAT для публікації медичного сервера, а також ACL для обмеження доступу між підмережами відповідно до політики безпеки.

Топологія мережі

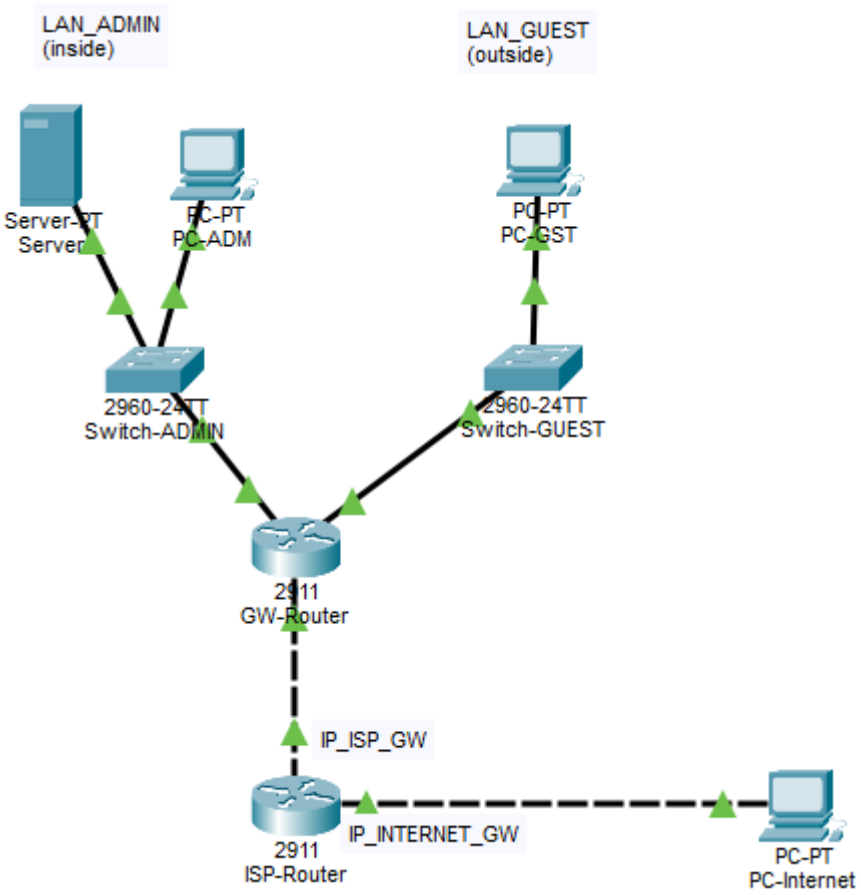

Рисунок 8.2 – Топологія мережі для ЛР №8

Порядок виконання

Частина 1. Побудова топології та базове налаштування

1. Створіть новий проект у Cisco Packet Tracer.
2. Розмістіть: 2 маршрутизатори (GW-Router та ISP-Router, моделі 1941/2911), 2 комутатори (2960), 1 сервер, 3 PC.
3. З'єднайте Server та PC-ADM зі Switch-ADMIN; PC-GST зі Switch-GUEST.
4. Switch-ADMIN підключіть до GW-Router (Gig0/0); Switch-GUEST до GW-Router (Gig0/1).
5. З'єднайте GW-Router (Gig0/2) з ISP-Router (Gig0/0) – це WAN-з'єднання.
6. Підключіть PC-Internet до ISP-Router (Gig0/1).

7. Налаштуйте GW-Router: ім'я, інтерфейси Gig0/0, Gig0/1 (адреси з варіанту), Gig0/2 (публічна IP), маршрут за замовчуванням до ISP.
8. Налаштуйте ISP-Router: ім'я, Gig0/0 (IP_ISP_GW), Gig0/1 (IP_INTERNET_GW), маршрут до публічної IP (Static NAT адреса) через GW-Router.
9. Налаштуйте Server та PC статичними адресами відповідно до варіанту.

Частина 2. Налаштування PAT

1. На GW-Router позначте інтерфейси: Gig0/0 та Gig0/1 як `ip nat inside`; Gig0/2 як `ip nat outside`.
2. Створіть стандартний ACL 1 що охоплює обидві внутрішні підмережі (LAN_ADMIN та LAN_GUEST).
3. Налаштуйте PAT: `ip nat inside source list 1 interface Fa0/2 overload`.
4. Налаштуйте маршрут за замовчуванням на GW-Router: `ip route 0.0.0.0 0.0.0.0 IP_ISP_GW`.
5. Перевірте `ping` з PC-ADM до PC-Internet. Скріншот.
6. Виконайте `show ip nat translations` на GW-Router – мають з'явитися трансляції. Скріншот.
7. Виконайте `show ip nat statistics`. Скріншот.

Частина 3. Налаштування Static NAT для сервера

1. Налаштуйте Static NAT: внутрішня адреса Server → публічна адреса IP_STATIC_NAT (за варіантом).
2. Перевірте `show ip nat translations` – має з'явитися статичний запис. Скріншот.
3. `Ping` з PC-Internet до IP_STATIC_NAT – має відповісти Server. Скріншот.

Частина 4. Налаштування ACL

Налаштуйте такі правила безпеки відповідно до варіанту:

- **Правило 1:** Заборонити PC-GST (LAN_GUEST) доступ до Server. Решту трафіку від гостей – дозволити.
- **Правило 2:** Дозволити PC-ADM (LAN_ADMIN) доступ до Server лише по HTTP (порт 80). Решту трафіку між ADMIN та Server – заборонити.
- **Правило 3:** Дозволити ICMP (`ping`) з обох мереж у будь-якому напрямку.

1. Створіть іменований розширений ACL GUEST-POLICY: заборонити ip від LAN_GUEST до Server; дозволити ip від LAN_GUEST будь-куди.
2. Застосуйте GUEST-POLICY до Fa0/1 у напрямку in.
3. Перевірте: ping з PC-GST до Server – не має проходити. Скріншот.
4. Перевірте: ping з PC-GST до PC-ADM – має проходити (якщо немає іншого правила). Скріншот.
5. Перевірте: ping з PC-GST до PC-Internet – має проходити (через PAT). Скріншот.
6. Виконайте `show access-lists` – перевірте лічильники `matches`. Скріншот.
7. Збережіть конфігурацію.

Таблиця адресації (заповнити у звіті)

Пристрій / Інтерфейс	IP-адреса	Маска підмережі	Шлюз / Примітка
GW-Router Fa0/0		255.255.255.0	inside
GW-Router Fa0/1		255.255.255.0	inside
GW-Router Fa0/2 (публічна)		255.255.255.252	outside
ISP-Router Fa0/0		255.255.255.252	–
ISP-Router Fa0/1		255.255.255.0	–
Server (статично)		255.255.255.0	GW Fa0/0
PC-ADM (статично)		255.255.255.0	GW Fa0/0
PC-GST (статично)		255.255.255.0	GW Fa0/1
PC-Internet (статично)		255.255.255.0	ISP Fa0/1
Static NAT (публічна для Server)	IP_STATIC_NAT	–	Публічна адреса сервера

Таблиця 8.6 – Таблиця адресації

Варіанти завдань

Кожен варіант містить адреси внутрішніх мереж (LAN_ADMIN та LAN_GUEST), WAN-з'єднання між GW-Router та ISP, зовнішню мережу Інтернет та публічну адресу для Static NAT. IP_STATIC_NAT – додаткова публічна адреса для публікації сервера (наступна за WAN-адресою GW).

B.	LAN_ADMIN /24	LAN_GUEST /24	WAN /30 GW	WAN ISP	Інтернет /24	PC-Internet	IP_STATIC_NAT
1	192.168.1.0	192.168.2.0	203.0.113.1	203.0.113.2	8.8.8.0	8.8.8.100	203.0.113.10
2	192.168.3.0	192.168.4.0	203.0.114.1	203.0.114.2	8.8.8.0	8.8.8.100	203.0.114.10
3	172.16.1.0	172.16.2.0	203.0.115.1	203.0.115.2	8.8.8.0	8.8.8.100	203.0.115.10
4	172.16.3.0	172.16.4.0	203.0.116.1	203.0.116.2	8.8.8.0	8.8.8.100	203.0.116.10
5	10.10.1.0	10.10.2.0	203.0.117.1	203.0.117.2	8.8.8.0	8.8.8.100	203.0.117.10
6	10.10.3.0	10.10.4.0	203.0.118.1	203.0.118.2	8.8.8.0	8.8.8.100	203.0.118.10
7	10.20.1.0	10.20.2.0	203.0.119.1	203.0.119.2	8.8.8.0	8.8.8.100	203.0.119.10
8	10.20.3.0	10.20.4.0	203.0.120.1	203.0.120.2	8.8.8.0	8.8.8.100	203.0.120.10
9	172.20.1.0	172.20.2.0	203.0.121.1	203.0.121.2	8.8.8.0	8.8.8.100	203.0.121.10
10	172.20.3.0	172.20.4.0	203.0.122.1	203.0.122.2	8.8.8.0	8.8.8.100	203.0.122.10
11	192.168.10.0	192.168.20.0	203.0.123.1	203.0.123.2	8.8.8.0	8.8.8.100	203.0.123.10
12	192.168.30.0	192.168.40.0	203.0.124.1	203.0.124.2	8.8.8.0	8.8.8.100	203.0.124.10
13	10.30.1.0	10.30.2.0	203.0.125.1	203.0.125.2	8.8.8.0	8.8.8.100	203.0.125.10
14	10.40.1.0	10.40.2.0	203.0.126.1	203.0.126.2	8.8.8.0	8.8.8.100	203.0.126.10
15	10.50.1.0	10.50.2.0	203.0.127.1	203.0.127.2	8.8.8.0	8.8.8.100	203.0.127.10

Таблиця 8.7– Варіанти завдань для лабораторної роботи № 8

GW-Router Gig0/0 (шлюз LAN_ADMIN) = LAN_ADMIN перша хост-адреса. GW-Router Gig0/1 (шлюз LAN_GUEST) = LAN_GUEST перша хост-адреса. **Server** = LAN_ADMIN + .100, **PC-ADM** = LAN_ADMIN + .101, **PC-GST** = LAN_GUEST + .10.

Вимоги до звіту

Звіт має містити:
1) Заповнену таблицю адресації;
2) Скріншот топології;
3) Скріншот `show ip nat translations` (з PAT-трансляціями та Static NAT-записом);
4) Скріншот `show ip nat statistics`;
5) Скріншот `ping` з PC-ADM до PC-Internet (PAT працює);
6) Скріншот `ping` з PC-Internet до IP_STATIC_NAT (Static NAT);
7) Скріншот `ping` з PC-GST до Server (заблокований ACL);
8) Скріншот `ping` з PC-GST до PC-Internet (дозволений PAT+ACL);
9) Скріншот `show access-lists` з лічильниками `matches`;
10) Відповіді на контрольні запитання.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке NAT і яку проблему він вирішує? Чому приватні IP-адреси не маршрутизуються в Інтернеті?

2. Поясніть різницю між Static NAT, Dynamic NAT та PAT (NAT Overload). Наведіть приклад практичного застосування кожного типу.

3. Що таке Inside Local та Inside Global адреси? Наведіть приклад для мережі лікарні, де внутрішній сервер публікується назовні через Static NAT.

4. Що таке ACL? Опишіть принцип роботи: послідовність перевірки правил та що відбувається якщо жодне правило не збіглося.

5. Чим відрізняється стандартний ACL від розширеного? За якими критеріями фільтрує кожен? Які номери їм відповідають?

6. Що означають напрями in та out при застосуванні ACL до інтерфейсу? У якому напрямку рекомендується розміщувати стандартні та розширені ACL і чому?

7. Що таке неявний deny any в кінці ACL? Яку практичну проблему він може спричинити і як її вирішити?

8. Яка команда дозволяє переглянути поточні NAT-трансляції? Що означає запис з порожнім полем Outside у таблиці трансляцій?

9. Яка команда дозволяє перевірити, скільки разів спрацювало кожне правило ACL? Як цю інформацію використовувати для діагностики?

10. Опишіть три сценарії застосування ACL у мережі медичного закладу для захисту персональних даних пацієнтів та медичних інформаційних систем.