МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
Кафедра комп'ютерної інженерії та кібербезпеки

ТЕХНОЛОГІЧНА ПРАКТИКА
частина 2

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
для студентів спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»

Житомир
2026

УДК 681.324
К63

Рекомендовано до друку науково-методичною радою Державного університету «Житомирська політехніка»
(протокол № 4 від 19 травня 2026 року)

Рецензенти:
М.М. Делембовський – кандидат технічних наук, доцент
А.А. Єфіменко – кандидат технічних наук, доцент

Технологічна практика частина 2: методичні рекомендації для
К63 студентів спеціальності 125 «Кібербезпека та захист інформації» / підг. О.Ю. Дячук, М.С. Колощук, М.О. Хохлов, Б.М. Рудюк. – Житомир: Державний університет «Житомирська політехніка», 2026. – 153 с.

Методичні рекомендації містять теоретичний матеріал, завдання та вказівки для виконання практичних занять технологічної практики (частина 2), пов'язаних із налагодженням агрегації каналів локальних (EtherChannel) і глобальних (Multilink PPP) мереж, віртуальних локальних мереж (VLAN), міжмережевої маршрутизації, динамічних протоколів маршрутизації (RIP, OSPF, EIGRP), редистрибуції маршрутів та протоколів резервування шлюзів (HSRP). Документ включає вісім практичних занять, два тестування (теоретичне в Moodle та практичне з команд CLI), а також вимоги до оформлення звіту, критерії оцінювання та додатки з шаблонами.

Методичні рекомендації призначені для студентів другого курсу, які навчаються за спеціальністю 125 «Кібербезпека та захист інформації».

Підготували: **Дячук О.Ю.**, **Колощук М.С.**, **Хохлов М.О.**, **Рудюк Б.М.**

УДК 681.324

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

Скорочення	Розшифрування
AAA	Authentication, Authorization, Accounting – автентифікація, авторизація, облік
ACL	Access Control List – список контролю доступу
ACK	Acknowledgment – підтвердження (пакет підтвердження доставки)
AD	Administrative Distance – адміністративна відстань (пріоритет джерела маршрутної інформації)
ARP	Address Resolution Protocol – протокол визначення апаратної адреси за IP-адресою (RFC 826)
AS	Autonomous System – автономна система
BDR	Backup Designated Router – резервний призначений маршрутизатор
BGP	Border Gateway Protocol – протокол зовнішньої маршрутизації
BMA	Broadcast Multiple Access – широкомовна мережа з множинним доступом
CLI	Command Line Interface – інтерфейс командного рядка
CHAP	Challenge Handshake Authentication Protocol – протокол автентифікації методом «виклик–відповідь»
DCE	Data Circuit-terminating Equipment – апаратура завершення каналу даних (надає тактову синхронізацію)
DTE	Data Terminal Equipment – термінальне обладнання даних (отримує тактову синхронізацію від DCE)
DTP	Dynamic Trunking Protocol – протокол динамічного узгодження транкового каналу
DUAL	Diffusing Update Algorithm – алгоритм дифузного оновлення (алгоритм збіжності протоколу EIGRP)
DHCP	Dynamic Host Configuration Protocol – протокол динамічного налаштування вузла
DR	Designated Router – призначений маршрутизатор
EIGRP	Enhanced Interior Gateway Routing Protocol – удосконалений протокол внутрішньої маршрутизації
FHRP	First Hop Redundancy Protocol – протокол резервування першого переходу
FD	Feasible Distance – здійсненна відстань (найменша відома метрика від маршрутизатора до мережі у EIGRP)
FS	Feasible Successor – здійсненний наступник (резервний маршрут у таблиці топології EIGRP)
GLBP	Gateway Load Balancing Protocol – протокол балансування навантаження шлюзів
HSRP	Hot Standby Router Protocol – протокол «гарячого» резервування
IOS	Internetwork Operating System – мережева ОС Cisco
ICMP	Internet Control Message Protocol – протокол керуючих повідомлень мережного рівня
IGMP	Internet Group Management Protocol – протокол керування груповою розсилкою

IP	Internet Protocol – міжмережевий протокол
IPv4	Internet Protocol version 4 – версія 4 протоколу IP
IPv6	Internet Protocol version 6 – версія 6 протоколу IP
LACP	Link Aggregation Control Protocol – протокол керування агрегацією каналів (IEEE 802.3ad)
LAG	Link Aggregation Group – група агрегованих каналів
LAN	Local Area Network – локальна обчислювальна мережа
LCP	Link Control Protocol – протокол керування каналом (у складі PPP)
LSA	Link-State Advertisement – оголошення про стан каналу
LSDB	Link-State Database – база даних стану каналів (топологічна база OSPF)
MAC	Media Access Control – управління доступом до середовища
MHSRP	Multiple HSRP – множинний HSRP (кілька груп резервування на одному інтерфейсі для балансування)
MTU	Maximum Transmission Unit – максимальний розмір блока даних, що передається без фрагментації
MLPPP	Multilink PPP – протокол агрегації PPP-каналів (RFC 1990)
NCP	Network Control Protocol – протокол керування мережевим рівнем (у складі PPP)
OSPF	Open Shortest Path First – протокол відкритого найкоротшого шляху
PAP	Password Authentication Protocol – протокол автентифікації за паролем у відкритому вигляді
PAgP	Port Aggregation Protocol – протокол агрегації портів Cisco
PPP	Point-to-Point Protocol – протокол з'єднання «точка-точка» (RFC 1661)
RIP	Routing Information Protocol – протокол маршрутної інформації
SPF	Shortest Path First – алгоритм найкоротшого шляху (Дейкстри)
SSH	Secure Shell – протокол захищеного віддаленого доступу
STP	Spanning Tree Protocol – протокол покривного дерева
SVI	Switched Virtual Interface – віртуальний інтерфейс комутатора
TCP	Transmission Control Protocol – протокол управління передачею
TTL	Time To Live – «час життя» пакета
UDP	User Datagram Protocol – протокол датаграм користувача
VLAN	Virtual Local Area Network – віртуальна локальна мережа
VRRP	Virtual Router Redundancy Protocol – протокол резервування віртуального маршрутизатора
VTP	VLAN Trunking Protocol – протокол тегування VLAN
WAN	Wide Area Network – глобальна обчислювальна мережа

ВСТУП

Технологічна практика (частина 2) є невід'ємною складовою підготовки фахівців за спеціальністю 125 «Кібербезпека та захист інформації» та проводиться на другому курсі навчання. Вона є логічним продовженням технологічної практики (частина 1) та лекційних і лабораторних занять із дисципліни «Комп'ютерні мережі», поглиблюючи практичні навички студентів у сфері проєктування та налагодження комп'ютерних мереж на обладнанні Cisco.

Якщо у першій частині практики студенти оволоділи основами роботи з кабельною інфраструктурою, базовим налагодженням керованих комутаторів і маршрутизаторів Cisco, конфігурацією IPv4/IPv6, DHCP, SSH, Telnet та NAT, то друга частина практики присвячена глибшому вивченню технологій локальних і глобальних мереж: агрегації каналів на рівні комутаторів (EtherChannel з протоколами LACP та PAgP) і маршрутизаторів (Multilink PPP), віртуальних локальних мереж (VLAN), міжмережевої маршрутизації, динамічних протоколів маршрутизації (RIP, OSPF, EIGRP), редистрибуції маршрутів між ними та протоколів резервування шлюзів першого переходу (HSRP).

Базою практики є лабораторії кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка», оснащені реальним мережевим обладнанням провідних виробників:

- комутатори та маршрутизатори Cisco (серії Catalyst 2960, 3400, 3560, 3750, 9300, SOHO91, 851, 891, 901, 1121, 1720, 1721, 1841, 2501, 2514, 2610XM, 2611XM, 2801, 2811, 2821, 2901, 2911, 2921, 4331);
- багаторівневі комутатори Cisco Catalyst 3560, 3560X, 3750X, 9300 та Metro-Ethernet-комутатори серії ME-3400EG (із ліцензіями IP Base, IP Services, LAN Base, Network Advantage, Metro-IP Access);
- комутатори Huawei;
- комутатори ZTE;
- комутатори D-Link;
- комутатори Edge-Core;
- комутатори Hewlett-Packard (H3C);
- кабельна інфраструктура: UTP Cat 5e/Cat 6, конектори RJ-45, крімпери, кабельні тестери, консольні кабелі, SFP-модулі та медіаконвертери.

Тривалість практики – 2 тижні (90 годин), з них 8 практичних занять, 2 тестування, оформлення та захист звіту.

Мета та завдання практики

Метою технологічної практики (частина 2) є закріплення й поглиблення теоретичних знань, отриманих у курсі «Комп'ютерні мережі»; набуття практичних навичок налагодження технологій другого та третього рівнів моделі OSI на обладнанні Cisco; формування вмінь проєктувати, реалізовувати та діагностувати масштабовані комп'ютерні мережі підприємств із забезпеченням резервування та балансування навантаження.

Основними завданнями технологічної практики є:

- набуття практичних навичок налагодження агрегації каналів у локальних мережах (EtherChannel з протоколами LACP, PAgP) на комутаторах Cisco та агрегації каналів у глобальних мережах (Multilink PPP) на маршрутизаторах Cisco;
- набуття практичних навичок проєктування та налагодження віртуальних локальних мереж (VLAN) та міжмережевої маршрутизації (Inter-VLAN Routing);
- оволодіння технологією маршрутизації VLAN на багаторівневому комутаторі з використанням SVI-інтерфейсів;
- набуття практичних навичок налагодження динамічних протоколів маршрутизації RIP, OSPF, EIGRP та їх редистрибуції;
- вивчення особливостей роботи OSPF у широкомовному сегменті мережі (процедури вибору DR/BDR);
- оволодіння технологією балансування навантаження між рівнометричними та нерівнометричними маршрутами (EIGRP Equal/Unequal-Cost Load Balancing);
- набуття практичних навичок налагодження протоколу резервування шлюзів HSRP та ознайомлення з протоколами VRRP і GLBP;
- формування навичок самостійного оформлення технічної документації згідно з ДСТУ.

ОРГАНІЗАЦІЯ ПРАКТИКИ

Практика проводиться протягом 10 робочих днів (2 тижні). Студент отримує завдання на кожне заняття від керівника практики. Щодня студент зобов'язаний:

- з'явитись у лабораторію в призначений час;
- отримати допуск до обладнання (усне опитування за теорією);
- виконати практичне завдання відповідно до свого варіанта;
- занести результати до щоденника практики та отримати підпис керівника.

Керівник практики від кафедри зобов'язаний провести вступний інструктаж, забезпечити доступ до обладнання та контролювати виконання завдань.

ТЕХНІКА БЕЗПЕКИ

Перед початком роботи в лабораторії студент зобов'язаний пройти інструктаж з охорони праці та розписатись у журналі. При роботі з електрообладнанням категорично забороняється:

- підключати або відключати обладнання від мережі живлення без дозволу керівника;
- залишати увімкнене обладнання без нагляду;
- виконувати будь-який ремонт обладнання самостійно;
- торкатись оголених контактів і провідників;
- переміщувати увімкнене обладнання.

При роботі з кабелями та роз'ємами:

- не перегинати кабелі під гострим кутом;
- не застосовувати надмірних зусиль при підключенні роз'ємів.

Консольний кабель підключати лише за вказівкою керівника, дотримуючись правильного напряму вставляння роз'єму RJ-45.

Заходити до лабораторії з відкритими напоями та їжею забороняється. Рідина, що потрапить на обладнання, може спричинити коротке замикання та вихід його з ладу, а також становить небезпеку для здоров'я. Зберігати їжу та напої дозволяється лише у спеціально відведеному місці поза межами робочої зони обладнання. Категорично забороняється:

- вносити у лабораторію відкриті напої (кава, вода, чай тощо) або їжу;
- споживати їжу чи напої безпосередньо за робочим місцем з обладнанням;
- залишати ємності з рідинами поблизу активного мережевого обладнання, кабелів чи розеток.

ЗМІСТ ПРАКТИКИ

Зміст технологічної практики відповідає програмі ОК 32 і охоплює 90 годин роботи. Детальний розподіл часу наведено в таблиці нижче.

№ з/п	Найменування розділів і робіт	Год.	Примітки
	Розділ 1. Техніка безпеки і охорона праці	**1**	
1	Інструктаж з техніки безпеки	1	
	Розділ 2. Ознайомлення з базою практики	**1**	
2	Ознайомлення з лабораторною базою	1	
	Розділ 3. Заняття 1–8 (практичні завдання)	**72**	
3	Заняття 1. Дослідження та налагодження агрегації каналів EtherChannel і Multilink PPP у мережах на базі обладнання Cisco.	9	
4	Заняття 2. Дослідження та налагодження віртуальних локальних мереж на основі групування портів і транкового протоколу 802.1Q у мережах на базі обладнання Cisco	9	
5	Заняття 3. Дослідження та налагодження маршрутизації між віртуальними локальними мережами (Inter-VLAN Routing) у мережі на базі обладнання Cisco	9	
6	Заняття 4. Дослідження та налагодження маршрутизації між віртуальними локальними мережами на базі багаторівневих (L3) комутаторів Cisco	9	
7	Заняття 5. Дослідження та налагодження протоколів динамічної маршрутизації RIPv2 та OSPFv2 і редистрибуції маршрутів у мережі на базі маршрутизаторів Cisco	9	
8	Заняття 6. Дослідження та налагодження протоколу маршрутизації OSPF у широкомовній мережі з множинним доступом на базі маршрутизаторів Cisco	9	
9	Заняття 7. Дослідження та налагодження протоколу маршрутизації EIGRP та балансування навантаження у мережі на базі маршрутизаторів Cisco	9	
10	Заняття 8. Дослідження та налагодження протоколу динамічного резервування шлюзу HSRP у мережі на базі маршрутизаторів Cisco	9	
	Розділ 4. Тестування	**4**	
11	Тестування 1 (теоретичне, ПК, Moodle)	2	
12	Тестування 2 (практичне, команди CLI)	2	
	Розділ 5. Оформлення звіту та щоденника	**12**	
13	Написання та оформлення звіту	10	
14	Захист звіту перед комісією	2	
	Диференційований залік	**–**	
	Всього	**90**	

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ ТА ЩОДЕННИКА

Загальні вимоги

Усі матеріали, зібрані в період технологічної практики (як текстові, так і графічні), розміщуються по розділах, нумеруються та оформлюються у вигляді єдиного звіту. Обсяг звіту – від 20 сторінок.

Документацію оформлюють відповідно до ДСТУ 3008:2015 «Звіти у сфері науки і техніки» на стандартних аркушах паперу формату А4.

Вимоги до форматування тексту

При оформленні звіту необхідно дотримуватися таких вимог:

- шрифт: Times New Roman, 14 пт;
- міжрядковий інтервал: одинарний (1,0);
- поля: верхнє і нижнє – 20 мм, ліве – 30 мм, праве – 10 мм;
- абзацний відступ: 5 знаків (1,25 см);
- вирівнювання тексту: за шириною;
- нумерація сторінок – у правому нижньому куті, починаючи зі змісту (титульний аркуш є першою сторінкою, але номер на ньому не проставляється).

Структура звіту

Звіт повинен містити такі структурні елементи:

1. Титульний аркуш (за зразком у Додатку А).
2. Зміст.
3. Вступ (1–2 сторінки): місце практики в освітній програмі, мета, коротка характеристика лабораторної бази.
4. Основна частина – розділи за кожним виконаним практичним заняттям (Заняття 1–8). Кожен розділ повинен містити: назву та мету заняття; перелік обладнання; короткий опис виконаних дій; схеми з'єднань (якщо передбачено завданням); таблиці з результатами; лістинги команд; аналіз результатів; висновки по занятті.
5. Висновки (1–2 сторінки): узагальнення набутих навичок, оцінка власної роботи.
6. Список використаної літератури (не менше 5 джерел, оформлений відповідно до ДСТУ 8302:2015).
7. Додатки: схеми топологій, таблиці адресації, лістинги конфігурацій (за потреби).

Вимоги до оформлення рисунків

Рисунки (схеми топологій, скриншоти терміналу, фотографії кабелів тощо) розміщуються безпосередньо після тексту, де вони вперше згадуються. Підпис – під рисунком, по центру, наприклад: «Рисунок 1.1 – Схема з'єднань заняття 1».

Вимоги до оформлення таблиць

Таблиці нумеруються послідовно в межах кожного розділу. Над таблицею ліворуч вказують слово «Таблиця» та її номер, а нижче – назву таблиці. Наприклад: «Таблиця 3.1 – Таблиця адресації мережі».

Вимоги до оформлення лістингів команд

Лістинги команд CLI оформлюються шрифтом Courier New, 10–12 пт, міжрядковий інтервал 1, обрамляються рамкою або виділяються сірим фоном. Нумеруються аналогічно рисункам. Підпис – під лістингом.

Вимоги до ведення щоденника практики

Щоденник практики є обов'язковим документом. Студент заповнює його щоденно, вказуючи:

- дату та найменування виконаних робіт;
- короткий опис виконаних дій (3–5 речень);
- результати (що вдалося налаштувати, які виникли труднощі).

Щоденник щодня підписується керівником практики. Наприкінці практики керівник пише підсумковий відгук-характеристику.

Звіт та щоденник здаються на кафедру не пізніше ніж через тиждень після закінчення практики.

Звіт підписується керівником від кафедри та захищається студентом перед спеціально призначеною комісією.

КРИТЕРІЇ ОЦІНЮВАННЯ

Підсумкова оцінка знань, умінь та навичок студента, набутих у ході технологічної практики, встановлюється за 100-бальною шкалою, національною шкалою та шкалою ЄКТС відповідно до програми ОК 32.

Розподіл балів

*Складова оцінки	Балів	Примітки
Виконання 8 практичних занять	64	По 8 балів за кожне заняття: 5 б. – правильне виконання, 2 б. – якість звіту, 1 б. – відповіді на контрольні запитання
Тестування 1 (теоретичне, Moodle)	14	Автоматична перевірка. 50 питань, 60 хв. Одна спроба без перездачі
Тестування 2 (практичні команди CLI)	10	Письмове виконання тестового завдання. Перевірка керівником
Оформлення звіту та своєчасна здача	10	Відповідність ДСТУ, повнота, якість лістингів і схем, дотримання строків
Захист звіту перед комісією	2	Повні й точні відповіді на запитання членів комісії
Разом	**100**	

Критерії виставлення оцінок

Критерії виставлення оцінок при захисті звіту з практики наведено у таблиці нижче, відповідно до вимог програми ОК 32.

ЄКТС	Оцінка	Бали	Вимоги до студента та звіту
A	Відмінно	90–100	Звіт оформлено бездоганно, всі заняття виконано повністю. Студент впевнено відповідає на всі запитання комісії.
B	Добре	82–89	Несуттєві зауваження щодо оформлення. Студент відповідає впевнено, допускає поодинокі неточності.
C	Добре	74–81	Є окремі зауваження до звіту. Студент загалом орієнтується в матеріалі.
D	Задовільно	64–73	Оформлення звіту недбале, частина завдань виконана з помилками. Відповіді неповні.
E	Задовільно	60–63	Більшість вимог виконана мінімально. Студент відповідає невпевнено, допускає значні помилки.
FX	Незадовільно	35–59	Звіт не повний або оформлений неналежно. Студент не може відповісти на більшість запитань. Потрібне повторне виконання.
F	Незадовільно	0–34	Звіт не зданий або містить критичні порушення. Студент не виконав програму практики.

Критерії оцінювання одного практичного заняття (8 балів)

Балів	**Оцінка**	**Опис**
8	Відмінно	Завдання виконано повністю та правильно. Звіт оформлено ретельно. Студент впевнено відповідає на всі контрольні запитання.
5–6	Добре	Незначні помилки при виконанні або в оформленні звіту. На більшість запитань студент відповідає правильно.
3–4	Задовільно	Завдання виконано частково. Звіт має суттєві недоліки. Студент відповідає лише на частину запитань.
0–2	Незадовільно	Завдання не виконано або виконано з грубими помилками. Звіт не зданий. Студент не може відповісти на запитання.

Примітка: Студент, який не виконав програму практики без поважної причини, отримує академічну заборгованість. При наявності поважної причини надається можливість проходження практики в індивідуальному порядку.

ЗАНЯТТЯ № 1

ДОСЛІДЖЕННЯ ТА НАЛАГОДЖЕННЯ АГРЕГАЦІЇ КАНАЛІВ ETHERCHANNEL І MULTILINK PPP У МЕРЕЖАХ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування технологій та протоколів агрегації каналів у локальних (EtherChannel з протоколами LACP і PAgP) та глобальних (Multilink PPP) мережах; отримати практичні навички налагодження, моніторингу та діагностування роботи статичних і динамічних агрегованих каналів на комутаторах і маршрутизаторах Cisco; дослідити процеси передачі кадрів і пакетів через агреговані канали; ознайомитися з методами балансування навантаження між фізичними каналами агрегованого з'єднання та навчитися розраховувати, якими фізичними інтерфейсами проходитиме трафік при різних методах балансування.

Обладнання та програмне забезпечення

Для виконання заняття на робочому місці студента має бути наявним таке обладнання та програмне забезпечення:

1. Керовані комутатори Cisco серії Catalyst 2960 (моделі WS-C2960-24TT-L або WS-C2960-48TT-L або WS-C2960S-F24TS-L або WS-C3560-24TS) – 3 шт.
2. Маршрутизатори Cisco серії 1841/2801/2811/2821/2901/2911/2921 з інтерфейсними слотами для плат розширення – 2 шт.
   - Плати розширення Cisco WIC-2T (або аналогічні) для звичайних послідовних з'єднань – 2 шт.
   - Плата розширення Cisco VWIC2-1MFT-T1/E1 або VWIC1MFT-E1 (або аналогічна) для послідовного з'єднання через RJ-48 – 2 шт.
3. Робочі станції (ПК або ноутбуки) з операційною системою Windows/Linux – не менше 2 шт.
4. Консольний кабель Cisco (rollover) з конектором RJ-45 та перехідником на USB або COM-порт – 1 шт.
5. Ethernet-кабелі прямого типу (T568B) категорії Cat 5e/Cat 6 – не менше 10 шт. (для підключення фізичних каналів агрегованих з'єднань між комутаторами та робочими станціями).
6. Serial-кабелі:
   - нуль-модемні послідовні кабелі (V.35 DTE + V.35 DCE) – 2 шт.
   - кабелі RJ-48 для з'єднання через модуль VWIC – 2 шт.
7. Термінальна програма-емулятор (PuTTY, Tera Term, SecureCRT або аналогічна) – встановлена на робочій станції.

Схема підключення

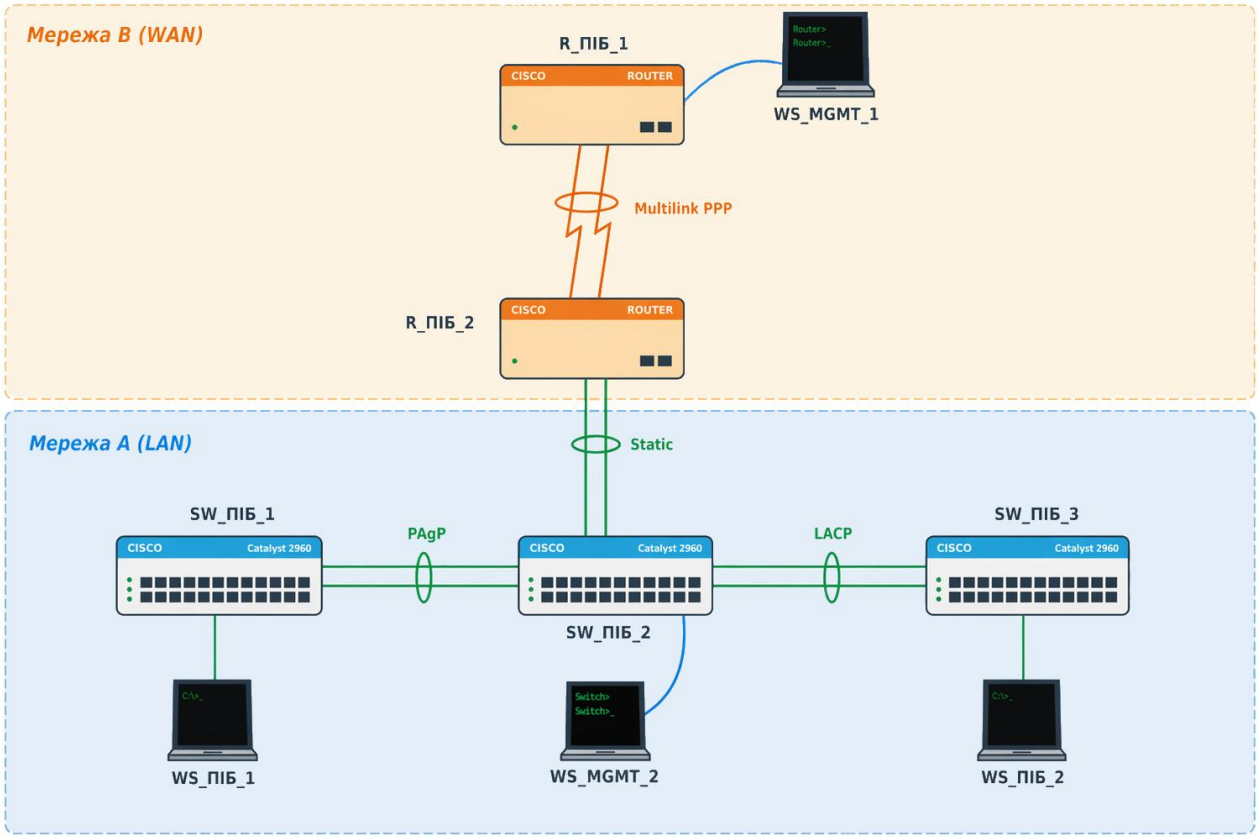

Рис. 1.1. Схема мережі, що будується у межах заняття

Примітка: ПІБ необхідно зазначати у скороченому форматі, який відповідає логіну для входу на платформу learn. Приклад: якщо логін для входу на learn – kb1_kmd, то назва комутатора має бути у форматі SW_kmd_1.

ЗАВДАННЯ

1. Ознайомитися з обладнанням та програмним забезпеченням робочого місця, перевірити наявність консольних, Ethernet- та Serial-кабелів.
2. Створити мережу відповідно до схеми на рис. 1.1. Під час побудови звернути увагу на вибір мережних з'єднань (тип кабелю, тип з'єднання).
3. Провести налагодження іменування всіх 5 пристроїв (R_ПІБ_1, R_ПІБ_2, SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3).
4. Розробити схему IP-адресації пристроїв мережі. Для цього скористатися даними табл. 1.5 згідно з варіантом. Результати заповнити у табл. 1.1.

Таблиця 1.1.

Параметри адресації мережі

Мережа/Пристрій	Інтерфейс	MAC-адреса	IP-адреса	Маска	Префікс
Мережа A	–	–			
Мережа B	–	–			
Маршрутизатор R1	Інтерфейс Multilink 1	–			
Маршрутизатор R2	Інтерфейс Multilink 1	–			
	Port-channel				
Комутатор SW1	Vlan 1				
Комутатор SW2	Vlan 1				
Комутатор SW3	Vlan 1				
WS1					
WS2					

5. Провести налагодження агрегованих каналів. Для цього згідно з варіантом (табл. 1.3) налаштувати:

- Агрегований канал EtherChannel (режим ON) між R_ПІБ_2 та SW_ПІБ_2 на двох фізичних Ethernet-інтерфейсах. На маршрутизаторі створити Port-channel-інтерфейс вручну командою interface port-channel, на комутаторі – автоматично командою channel-group. Призначити IP адресу.
- Агрегований канал на основі протоколу PAgP між SW_ПІБ_1 та SW_ПІБ_2 на двох фізичних Ethernet-інтерфейсах (режими згідно табл. 1.3).
- Агрегований канал на основі протоколу LACP між SW_ПІБ_2 та SW_ПІБ_3 на двох фізичних Ethernet-інтерфейсах (режими згідно табл. 1.3).
- налаштувати метод балансування навантаження для агрегованих каналів EtherChannel згідно з даними табл. 1.4.
- Виконати розрахунок, якими саме фізичними інтерфейсами Port-channel буде передаватися трафік у напрямку від робочої станції WS_ПІБ_1 (підключеної до SW_ПІБ_1) до WS_ПІБ_2 (підключеної до SW_ПІБ_3); Розрахунок здійснити на основі налагодженого методу балансування з урахуванням MAC- та IP-адрес пристроїв мережі. Результати розрахунку порівняти з реальним проходженням трафіку, що спостерігається за командами show etherchannel port-channel (колонка Load) або debug-командами. Оформити у вигляді таблиці 1.2.

Таблиця 1.2.

Розподіл трафіку між фізичними каналами

№	Ділянка EtherChannel	Метод балансу-вання	Значення ключового поля	Молодші біти (дв.)	Біт вибору	Очікуваний інтерфейс	Факт. Load (hex)
1	SW1 → SW2 (PAgP)						
2	SW2 → SW3 (LACP)						
3	SW3 → SW2 (LACP)						
4	SW2 → SW1 (PAgP)						

Примітка: У кожному рядку стовпець «Значення ключового поля» заповнюється фактичним значенням src або dst (залежно від методу балансування) MAC- чи IP-адреси пристрою-джерела або отримувача на поточній ділянці. У стовпці «Молодші біти (дв.)» наводяться 4 молодші біти двійкового подання відповідного поля. У стовпці «Біт вибору» – значення молодшого біта (0 або 1); для методів src-dst-mac / src-dst-ip. Стовпець «Факт. Load» заповнюється на основі виведення команди **show etherchannel port-channel** (колонка «Load») на відповідному комутаторі; дві цифри у шістнадцятковій системі показують, які хеш-значення потрапили на цей фізичний інтерфейс. Якщо очікуваний та фактичний інтерфейси співпадають – розрахунок підтверджено.

6. Налаштувати агрегований канал Multilink PPP між R_ПІБ_1 та R_ПІБ_2, об'єднавши два фізичні канали (Serial DTE/DCE або RJ-48) у групу Multilink відповідно до даних табл. 1.3. Налаштувати автентифікацію PPP за протоколом CHAP/PAP, призначити IP-адресу інтерфейсу Multilink, увімкнути відповідну підтримку multilink на фізичних інтерфейсах.

7. Налаштувати параметри IP-адресації та шлюзів за замовчуванням на робочих станціях. Перевірити наявність зв’язку між усіма пристроями мережі командою **ping**. Використати команду **tracert** (**tracetoute**) для спостереження шляху проходження пакетів.

8. Дослідити результати налагодження агрегованих каналів за допомогою команд **show etherchannel**, **show etherchannel summary**, **show etherchannel port-channel**, **show etherchannel load-balance**, **show lacp / show pagp neighbor**, **show interfaces port-channel**, **show ppp multilink**, **show interfaces multilink**, **show interfaces trunk**.

9. Дослідити відмовостійкість агрегованих каналів: по черзі відключати один з фізичних інтерфейсів кожного агрегованого каналу (команда **shutdown**) і спостерігати за станом каналу за допомогою команд **show etherchannel summary**, **show ppp multilink**. Переконатися, що зв'язність між пристроями зберігається. Поновити інтерфейс командою **no shutdown**.

10. Вивести та проаналізувати файли конфігурацій усіх комунікаційних пристроїв мережі (**show running-config**).

11. У випадку виявлення помилок у налагодженнях – визначити причину та усунути їх.

12. Продемонструвати виконану роботу керівнику практики та оформити звіт за заняттям.

ВАРІАНТИ ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Варіант визначається за номером стійки, за якою працюють студенти, та номером класу, у якому виконуються завдання. Номери груп Port-channel (Po) обираються студентом самостійно з урахуванням обмежень платформи (на Catalyst 2960 – від 1 до 6).

Таблиця 1.3.

Параметри налагодження агрегованих каналів та мультилінку PPP

№ в-та	R2–SW2 (Static)	SW1–SW2 (PAgP)	SW2–SW3 (LACP)	R1–R2 (MLPPP)	Автентифіка-ція MLPPP
1	ON / ON	desirable / desirable	active / active	V.35 DCE/DTE	PAP
2	ON / ON	desirable / auto	active / passive	RJ-48	CHAP
3	ON / ON	auto / desirable	passive / active	V.35 DCE/DTE	PAP
4	ON / ON	desirable / desirable	active / active	RJ-48	CHAP
5	ON / ON	desirable / auto	active / passive	V.35 DCE/DTE	PAP
6	ON / ON	auto / desirable	passive / active	RJ-48	CHAP
7	ON / ON	desirable / desirable	active / active	V.35 DCE/DTE	PAP
8	ON / ON	desirable / auto	active / passive	RJ-48	CHAP
9	ON / ON	auto / desirable	passive / active	V.35 DCE/DTE	PAP
10	ON / ON	desirable / desirable	active / active	RJ-48	CHAP
11	ON / ON	desirable / auto	active / passive	V.35 DCE/DTE	PAP
12	ON / ON	auto / desirable	passive / active	RJ-48	CHAP
13	ON / ON	desirable / desirable	active / active	V.35 DCE/DTE	PAP
14	ON / ON	desirable / auto	active / passive	RJ-48	CHAP
15	ON / ON	auto / desirable	passive / active	V.35 DCE/DTE	PAP
16	ON / ON	desirable / desirable	active / active	RJ-48	CHAP
17	ON / ON	desirable / auto	active / passive	V.35 DCE/DTE	PAP
18	ON / ON	auto / desirable	passive / active	RJ-48	CHAP
19	ON / ON	desirable / desirable	active / active	V.35 DCE/DTE	PAP
20	ON / ON	desirable / auto	active / passive	RJ-48	CHAP

Примітка: Позначення режимів протоколу PAgP: **desirable** – активний режим ініціації агрегації; **auto** – пасивний режим. Позначення режимів протоколу LACP: **active** – активний режим ініціації агрегації; **passive** – пасивний режим. Для автентифікації MLPPP використовуються протоколи **PAP** (Password Authentication Protocol) або **CHAP** (Challenge Handshake Authentication Protocol). Ім'я користувача та пароль автентифікації обираються студентом самостійно.

Таблиця 1.4.

Параметри налагодження методів балансування навантаження

№ варіанта	SW1 (PAgP-канал)	SW2 (усі канали)	SW3 (LACP-канал)
1	dst-mac	src-ip	dst-mac
2	src-mac	dst-mac	dst-ip
3	dst-ip	dst-ip	src-mac
4	src-mac	dst-mac	src-ip
5	dst-mac	src-ip	dst-mac
6	dst-ip	dst-ip	src-mac
7	src-ip	src-mac	dst-mac
8	dst-mac	dst-mac	dst-ip
9	src-ip	src-ip	src-ip
10	dst-mac	dst-ip	dst-ip
11	dst-ip	dst-mac	dst-mac
12	dst-mac	src-mac	src-ip
13	src-mac	dst-ip	src-mac
14	dst-ip	src-ip	dst-mac
15	src-mac	dst-mac	src-mac
16	src-ip	src-mac	dst-ip
17	dst-ip	dst-ip	dst-mac
18	src-mac	src-ip	dst-ip
19	src-ip	dst-mac	src-ip
20	src-mac	src-mac	dst-mac

Таблиця 1.5.

Параметри IP-адресації мережі

№ варіанта	IP-адреса мережі LAN-A	Префікс	IP-адреса шлюзу за замовчуванням/	IP-адреса мережі між B (MLPPP)
1	191.C.S.0	/24	Перша IP-адреса діапазону	172.C.S.0 /30
2	192.C.S.0	/25	Остання IP-адреса діапазону	172.C.S.4 /30
3	193.C.S.0	/26	Перша IP-адреса діапазону	172.C.S.8 /30
4	194.C.S.0	/27	Остання IP-адреса діапазону	172.C.S.12 /30
5	195.C.S.0	/28	Перша IP-адреса діапазону	172.C.S.16 /30
6	196.C.S.0	/24	Остання IP-адреса діапазону	172.C.S.20 /30
7	197.C.S.0	/25	Перша IP-адреса діапазону	172.C.S.24 /30
8	198.C.S.0	/26	Остання IP-адреса діапазону	172.C.S.28 /30
9	199.C.S.0	/27	Перша IP-адреса діапазону	172.C.S.32 /30
10	200.C.S.0	/28	Остання IP-адреса діапазону	172.C.S.36 /30
11	201.C.S.0	/24	Перша IP-адреса діапазону	172.C.S.40 /30
12	202.C.S.0	/25	Остання IP-адреса діапазону	172.C.S.44 /30
13	203.C.S.0	/26	Перша IP-адреса діапазону	172.C.S.48 /30
14	204.C.S.0	/27	Остання IP-адреса діапазону	172.C.S.52 /30
15	205.C.S.0	/28	Перша IP-адреса діапазону	172.C.S.56 /30
16	206.C.S.0	/24	Остання IP-адреса діапазону	172.C.S.60 /30
17	207.C.S.0	/25	Перша IP-адреса діапазону	172.C.S.64 /30
18	208.C.S.0	/26	Остання IP-адреса діапазону	172.C.S.68 /30
19	209.C.S.0	/27	Перша IP-адреса діапазону	172.C.S.72 /30
20	210.C.S.0	/28	Остання IP-адреса діапазону	172.C.S.76 /30

***Примітка*: C** (class) – номер аудиторії: для ауд. **107 – 71**, для ауд. **107a – 72, S** (stand) – номер стійки (зазначено зверху стійки).

УВАГА! В залежності від години проведення практики значення може змінюватись за вимогою керівника.

ЗМІСТ ЗВІТУ З ЗАНЯТТЯ

Звіт з заняття повинен містити:

1. Номер, тему та мету заняття.
2. Короткі теоретичні відомості (за власним конспектом, обсягом 2–3 сторінки) з наступних питань: агрегація каналів у локальних мережах, EtherChannel, протоколи LACP та PAgP, режими налагодження агрегованих каналів, методи балансування навантаження, агрегація каналів у глобальних мережах, протокол Multilink PPP, протоколи автентифікації PPP (PAP, CHAP).
3. Перелік використаного обладнання та програмного забезпечення.
4. Схему (ФОТО) побудованої мережі з позначенням усіх пристроїв (R_ПІБ_1, R_ПІБ_2, SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3) та інтерфейсів, через які виконано з'єднання.
5. Розроблену схему IP-адресації у вигляді табл. 1.1 (з конкретними значеннями IP-адрес, масок та префіксів) та представленими розрахунками.
6. Лістинги команд (або скріншоти термінального вікна) з результатами виконання для кожного з підзавдань 3–7, а саме:
   - налагодження статичного EtherChannel (R2–SW2);
   - налагодження динамічного PAgP-каналу (SW1–SW2);
   - налагодження динамічного LACP-каналу (SW2–SW3);
   - налагодження методу балансування навантаження;
   - таблицю розподілу трафіку між фізичними каналами;
   - налагодження Multilink PPP (R1–R2);
   - налагодження IP-адресації пристроїв;
   - результати перевірки працездатності мережі (вивід команд ping, tracert) між робочими станціями та до маршрутизаторів;
   - вивід та аналіз результатів команд діагностики: show etherchannel summary (для SW1, SW2, SW3), show etherchannel port-channel, show etherchannel load-balance, show lacp neighbor, show pagp neighbor, show ppp multilink, show interfaces multilink, show interfaces trunk.
   - результати дослідження відмовостійкості агрегованих каналів: вивід команд до та після відключення одного з фізичних інтерфейсів кожного каналу.
7. Опис проблем, що виникли під час виконання завдання, та шляхи їх усунення.
8. Висновки по заняттю.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Загальні відомості про агрегацію каналів

Агрегація каналів (англ. *link aggregation*) – технологія об'єднання декількох фізичних мережних інтерфейсів в один логічний канал з метою збільшення пропускної здатності та/або підвищення відмовостійкості з'єднання. Логічний агрегований інтерфейс функціонує як єдиний канал зв'язку, прозоро для протоколів вищих рівнів моделі OSI.

Технологія агрегації каналів стандартизована у документах IEEE 802.1AX (раніше IEEE 802.3ad). На обладнанні Cisco агреговані канали між пристроями прийнято називати **EtherChannel** (10BaseT/F), Fast EtherChannel (FEC, 100BaseTX/FX), Gigabit EtherChannel (GEC, 1000BaseT/FX). Незалежно від технології та методу агрегації, статичні та динамічні канали узагальнено називають **EtherChannel**.

Основними перевагами агрегації каналів порівняно із використанням одного фізичного з'єднання є:

- **збільшення пропускної здатності** – пропускна здатність логічного інтерфейсу дорівнює сумі пропускних здатностей усіх фізичних інтерфейсів, що входять до його складу (до 8 або 16 активних каналів залежно від протоколу);
- **відмовостійкість** – у разі виходу з ладу одного або декількох фізичних каналів, решта продовжують передавати трафік без перерви зв'язку та без перенастройки мережного обладнання;
- **балансування навантаження** – трафік розподіляється між фізичними каналами за одним із кількох алгоритмів, що дозволяє рівномірно завантажувати всі ланки агрегованого з'єднання;
- **прозорість для протоколів STP** – агрегований канал сприймається протоколом STP (Spanning Tree Protocol) як єдиний логічний зв'язок, що запобігає формуванню петель і дозволяє одночасно задіяти всі фізичні лінки.

Статичне агрегування (режим ON)

Статичне агрегування каналів виконується без застосування протоколів узгодження. Обидва кінці каналу налаштовуються у режимі **ON**, що означає безумовне об'єднання зазначених фізичних інтерфейсів у логічний канал EtherChannel незалежно від стану або налаштувань партнера.

Переваги статичного агрегування:

- відсутність додаткової затримки при активації каналу або зміні його налаштувань;
- простота реалізації – не потребує підтримки спеціальних протоколів обома сторонами;
- рекомендується компанією Cisco для з'єднань між комутатором та маршрутизатором (L3-пристроєм).

Недоліки статичного агрегування:

- відсутнє узгодження налаштувань із віддаленою стороною;
- помилки в налаштуванні можуть призвести до утворення петель у мережі;
- відсутня підтримка режиму "гарячого резерву" (standby) для інтерфейсів.

Протокол PAgP (Port Aggregation Protocol)

PAgP (Port Aggregation Protocol) – фірмовий протокол Cisco для динамічного узгодження агрегованих каналів. Протокол обмінюється пакетами

PAgP між сусідніми пристроями для узгодження параметрів та автоматичного формування агрегованого каналу. PAgP підтримується лише на обладнанні Cisco і не може використовуватися для з'єднання з пристроями інших виробників.

Протокол PAgP підтримує два режими роботи:

- **desirable** (активний) – пристрій активно надсилає пакети PAgP до сусіда та ініціює формування агрегованого каналу;
- **auto** (пасивний) – пристрій не надсилає пакети PAgP першим, але відповідає на пакети PAgP від сусіда.

Агрегований канал на базі PAgP сформується лише при таких комбінаціях режимів: **desirable–desirable** або **desirable–auto**. Комбінація **auto–auto** не призводить до формування каналу, оскільки обидві сторони очікують ініціативи від партнера.

Протокол LACP (Link Aggregation Control Protocol)

LACP (Link Aggregation Control Protocol) – відкритий стандартний протокол агрегації каналів, визначений у стандарті IEEE 802.3ad (зараз IEEE 802.1AX). На відміну від PAgP, LACP є міжвендорним і підтримується обладнанням різних виробників, що робить його пріоритетним вибором у гетерогенних мережах.

Протокол LACP підтримує два режими роботи:

- **active** (активний) – пристрій ініціює надсилання LACPDU (LACP Data Unit) та активно формує агрегований канал;
- **passive** (пасивний) – пристрій відповідає на LACPDU від сусіда, але сам їх не ініціює.

Агрегований канал на базі LACP сформується при комбінаціях: **active–active** або **active–passive**. Комбінація **passive–passive** не призводить до формування каналу.

Суттєвою перевагою LACP є підтримка режиму **standby-інтерфейсів**: протокол дозволяє долучати до групи до 16 фізичних портів, з яких 8 будуть активними, а решта – перебувають у режимі гарячого резерву. У разі відмови активного порту один зі standby-портів автоматично переходить в активний режим.

Порівняння комбінацій режимів протоколів PAgP та LACP наведено в таблиці 1.6.

Таблиця 1.6.

Комбінації режимів PAgP і LACP, при яких формується EtherChannel

Протокол PAgP	auto	desirable	Протокол LACP	passive	active
auto	–	+	passive	–	+
desirable	+	+	active	+	+

Вимоги до фізичних інтерфейсів EtherChannel

Для успішного формування агрегованого каналу EtherChannel усі фізичні інтерфейси, що входять до його складу, повинні мати однакові налаштування:

- швидкість (speed) та режим дуплексу (duplex);

- режим доступу або транкінгу (access/trunk) та VLAN, що передаються;
- MTU;
- налаштування native VLAN для транкових портів.

Порушення будь-якої з цих вимог призводить до відмови у формуванні EtherChannel або нестабільної роботи каналу.

Методи балансування навантаження EtherChannel

Механізм балансування навантаження (load balancing) визначає, по якому з фізичних каналів EtherChannel передаватиметься конкретний кадр або пакет. Балансування виконується на рівні потоку (flow-based), тобто всі пакети одного потоку завжди передаються через один і той самий фізичний канал, що гарантує доставку без зміни порядку пакетів у межах потоку.

Вибір фізичного інтерфейсу здійснюється за хеш-функцією від значення обраного ключового поля. Результат хешування дозволяє обчислити індекс (0 або 1 при двох каналах, 0–3 при чотирьох тощо) за формулою: молодші N біт хешу (де $2^N \geq$ кількість фізичних каналів) визначають номер інтерфейсу.

На комутаторах Cisco Catalyst підтримуються методи балансування навантаження наведені в таблиці 1.7.

Таблиця 1.7.

Основні методи балансування навантаження EtherChannel на комутаторах Cisco

Метод	Опис
src-mac	На основі MAC-адреси відправника кадру
dst-mac	На основі MAC-адреси отримувача кадру
src-dst-mac	XOR MAC-адрес відправника та отримувача
src-ip	На основі IP-адреси відправника пакету
dst-ip	На основі IP-адреси отримувача пакету
src-dst-ip	XOR IP-адрес відправника та отримувача
src-port	На основі номера TCP/UDP-порту відправника
dst-port	На основі номера TCP/UDP-порту отримувача
src-dst-port	XOR номерів TCP/UDP-портів відправника та отримувача

Алгоритм розрахунку вибору фізичного інтерфейсу для методів на основі одного поля (src-mac, dst-ip тощо):

- взяти значення ключового поля (MAC або IP-адреса) у двійковому форматі;
- виділити молодші N біт (N = log2(кількість каналів));
- отримане двійкове число є індексом фізичного інтерфейсу.

Для методів з XOR (src-dst-mac, src-dst-ip, src-dst-port) спочатку виконується операція побітового XOR відповідних полів відправника та отримувача, після чого беруться молодші N біти результату.

Налагодження EtherChannel на обладнанні Cisco

Порядок налаштування агрегованих каналів EtherChannel на комутаторах Cisco складається з кількох кроків:

1. Вибрати групу фізичних інтерфейсів, що входитимуть до логічного каналу.
2. Вимкнути вибрані інтерфейси командою **shutdown**.
3. Об'єднати інтерфейси у логічний канал та задати номер групи командою **channel-group [номер] mode [режим]**.
4. Налаштувати метод балансування навантаження командою **port-channel load-balance [метод]** (глобальна команда).
5. Повторити аналогічні кроки на протилежній стороні каналу.
6. Увімкнути інтерфейси командою **no shutdown** та перевірити стан каналу.

Для пристроїв третього рівня (маршрутизаторів або L3-комутаторів) логічний інтерфейс **port-channel** необхідно створювати вручну командою:

…
Router(config)# interface port-channel *number*
Router(config-if)# ip address *IP_address network_mask*
Router(config-if)# no shutdown
…

На комутаторах логічний інтерфейс port-channel створюється автоматично командою **channel-group**. Основний синтаксис команди:

channel-group [номер] mode { on | desirable [non-silent] | auto [non-silent] | active | passive }

де ***group-number*** **–** номер групи портів (номер логічного каналу), що створюється на пристрої, номери груп можуть не збігатися на різних сторонах логічного каналу;

mode – службова конструкція, за допомогою якої встановлюється варіант агрегації;

auto / **desirable** – ввімкнути підтримку протоколу PAgP;

on – ввімкнути статичну агрегацію EtherChannel;

active / **passive** – ввімкнути підтримку протоколу LACP;

non-silent – службова конструкція, яка зазначає активацію у випадку, коли дані отримано з іншого кінця каналу.

Команда **port-channel load-balance** задається у режимі глобального конфігурування і застосовується до всіх агрегованих каналів пристрою:

…
Switch(config)# port-channel load-balance *method*
…

Команди моніторингу та діагностики EtherChannel

Для перегляду стану та параметрів агрегованих каналів EtherChannel використовуються команди діагностики представлені у таблиці 1.8.

Таблиця 1.8.

Команди діагностики EtherChannel, LACP та PAgP

Команда	Призначення
show etherchannel	Загальна інформація про всі агреговані канали пристрою
show etherchannel summary	Зведена таблиця стану агрегованих каналів і їх фізичних складових
show etherchannel port-channel	Детальна інформація про логічні port-channel інтерфейси
show etherchannel load-balance	Метод балансування навантаження, застосований на пристрої
show interfaces port-channel	Інформація про логічний інтерфейс port-channel
show lacp neighbor	Параметри сусіднього пристрою за протоколом LACP
show lacp internal	Параметри LACP локального пристрою
show lacp counters	Лічильники LACP-повідомлень
show pagp neighbor	Параметри сусіднього пристрою за протоколом PAgP
show pagp internal	Параметри PAgP локального пристрою
show interfaces trunk	Параметри транкових з'єднань, у т.ч. агрегованих
show mac-address-table interface port-channel	Таблиця MAC-адрес для порту port-channel

Загальні відомості про протокол Point-to-Point (PPP)

PPP (Point-to-Point Protocol) – стандартний протокол канального рівня для встановлення прямих з'єднань між двома вузлами мережі. Визначений у документах RFC 1661, RFC 1662 та ряді доповнень. PPP широко застосовується на послідовних WAN-каналах (V.35, T1/E1) та замінив застарілий протокол HDLC як більш функціональний і гнучкий аналог.

Архітектура PPP включає такі підпротоколи:

- **LCP** (Link Control Protocol) – відповідає за встановлення, конфігурацію, тестування та завершення PPP-з'єднання. LCP узгоджує параметри з'єднання (MTU, стиснення, автентифікацію) перед передачею даних.
- **NCP** (Network Control Protocol) – сімейство протоколів для передачі через PPP-з'єднання пакетів різних мережних протоколів. Для передачі IP-пакетів використовується IPCP (Internet Protocol Control Protocol).
- **Протоколи автентифікації** – PAP та CHAP, що дозволяють перевірити справжність сторін з'єднання.

Процес встановлення PPP-з'єднання складається з трьох фаз:

- **Фаза LCP** – встановлення та узгодження параметрів каналу;
- **Фаза автентифікації** – перевірка справжності (за наявності конфігурації);
- **Фаза NCP** – узгодження параметрів мережного протоколу та початок передачі даних.

Протокол автентифікації PAP (Password Authentication Protocol)

PAP (Password Authentication Protocol) – простий протокол автентифікації у два кроки, визначений у RFC 1334. При використанні PAP клієнт надсилає своє ім'я та пароль у відкритому (незашифрованому) вигляді, а сервер порівнює ці дані зі своєю базою даних та надсилає у відповідь підтвердження або відмову.

Процес автентифікації за протоколом PAP:

- Клієнт надсилає пакет **Authenticate-Request** з іменем та паролем у відкритому вигляді;
- Сервер перевіряє отримані дані. При збігу надсилає **Authenticate-Ack**, при невідповідності – **Authenticate-Nak**.

Недолік PAP – передача пароля у відкритому вигляді, що робить його вразливим до перехоплення. Проте PAP може використовуватись у разі, коли система аутентифікації партнера не підтримує CHAP.

Протокол автентифікації CHAP (Challenge Handshake Authentication Protocol)

CHAP (Challenge Handshake Authentication Protocol) – більш захищений протокол автентифікації, визначений у RFC 1994. CHAP використовує трьохетапний механізм **challenge-response** та ніколи не передає пароль у явному вигляді. Замість цього пароль використовується лише для обчислення криптографічного хешу.

Процес автентифікації за протоколом CHAP:

- Аутентифікатор надсилає клієнту пакет Challenge з випадковим числом (challenge value) та своїм іменем;
- Клієнт обчислює значення response – MD5-хеш від конкатенації ID пакету, спільного секрету та challenge value;
- Клієнт надсилає пакет Response з обчисленим хешем та своїм іменем;
- Аутентифікатор самостійно обчислює очікуваний хеш та порівнює його з отриманим. При збігу надсилає **Success**, при розбіжності – **Failure**.

Ключові переваги CHAP над PAP:

- Пароль ніколи не передається відкритим текстом;
- Аутентифікація може повторюватися через довільні проміжки часу протягом сесії;
- Використання MD5-хешування забезпечує захист від атак відтворення (replay attack).

Налаштування автентифікації PAP та CHAP на маршрутизаторах Cisco:

Загальні команди для обох протоколів:

…
Router(config)# username *name-string* password *password*
Router(config)# interface *interface-type interface-id*
Router(config-if)# encapsulation ppp
…

Для PAP:

…
Router(config-if)# ppp authentication pap

Router(config-if)# ppp pap sent-username *name-string* password *password*

…

Для CHAP:

…

Router(config-if)# ppp authentication chap

…

Концепція та призначення Multilink PPP

Multilink PPP (MLPPP, RFC 1990) – розширення протоколу PPP, що дозволяє об'єднувати декілька фізичних послідовних каналів в один логічний канал типу **Multilink** з метою збільшення сумарної пропускної здатності WAN-з'єднання та підвищення його відмовостійкості. MLPPP є аналогом EtherChannel для послідовних WAN-з'єднань між маршрутизаторами.

Принцип роботи Multilink PPP полягає у фрагментації вихідних пакетів та їхньому паралельному розподілі між фізичними каналами групи. На стороні отримувача фрагменти збираються у вихідний пакет у правильному порядку. Механізм нумерації фрагментів та порядковий номер у заголовку MLPPP забезпечують коректне складання навіть при різних затримках у фізичних каналах.

На відміну від EtherChannel, де трафік розподіляється на рівні кадрів або пакетів цілком, MLPPP розподіляє фрагменти одного пакета між різними каналами, що забезпечує краще балансування та нижчу затримку навіть при передачі великих пакетів.

Структура кадру Multilink PPP

Кадр Multilink PPP містить стандартний заголовок PPP з додатковим заголовком MLPPP. Заголовок MLPPP включає:

- **Sequence Number** (24 або 12 біт) – порядковий номер фрагмента, що забезпечує правильне складання пакета;
- **Bit B** (Begin) – встановлюється для першого фрагмента пакета;
- **Bit E** (End) – встановлюється для останнього фрагмента пакета;
- **Клас** – ідентифікатор черги для підтримки QoS (у розширених реалізаціях).

Налаштування Multilink PPP на маршрутизаторах Cisco

Для налаштування MLPPP на маршрутизаторі Cisco необхідно виконати такі кроки:

1. Створити логічний інтерфейс **Multilink** та призначити йому IP-адресу;
2. Налаштувати протокол PPP на фізичних послідовних інтерфейсах (encapsulation ppp);
3. Активувати підтримку multilink на фізичних інтерфейсах та включити їх у відповідну групу;
4. Налаштувати автентифікацію PAP або CHAP (за необхідності);
5. На DCE-стороні задати тактову частоту (clock rate).

Типовий сценарій налаштування MLPPP між Router1 (DCE) та Router2 (DTE):

Router1 (DCE-сторона)

```
…
Router1(config)# username Router2 password Cisco123
Router1(config)# interface Multilink 1
Router1(config-if)# ip address 172.16.1.1 255.255.255.252
Router1(config-if)# ppp multilink
Router1(config-if)# ppp multilink group 1
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# interface Serial 0/0/0
Router1(config-if)# clock rate 64000
Router1(config-if)# encapsulation ppp
Router1(config-if)# ppp authentication chap
Router1(config-if)# ppp multilink
Router1(config-if)# ppp multilink group 1
Router1(config-if)# no shutdown
Router1(config-if)# exit
Router1(config)# interface Serial 0/0/1
Router1(config-if)# clock rate 64000
Router1(config-if)# encapsulation ppp
Router1(config-if)# ppp authentication chap
Router1(config-if)# ppp multilink
Router1(config-if)# ppp multilink group 1
Router1(config-if)# no shutdown
…
```

Router2 (DTE-сторона)

```
…
Router2(config)# username Router1 password Cisco123
Router2(config)# interface Multilink 1
Router2(config-if)# ip address 172.16.1.2 255.255.255.252
Router2(config-if)# ppp multilink
Router2(config-if)# ppp multilink group 1
Router2(config-if)# no shutdown
Router2(config-if)# exit
Router2(config)# interface Serial 0/0/0
Router2(config-if)# encapsulation ppp
Router2(config-if)# ppp authentication chap
Router2(config-if)# ppp multilink
Router2(config-if)# ppp multilink group 1
Router2(config-if)# no shutdown
…
```

Команди моніторингу та діагностики Multilink PPP

Для моніторингу та діагностики MLPPP-з'єднань на маршрутизаторах Cisco застосовуються команди наведені у таблиця 1.9.

Таблиця 1.9.

Команди діагностики Multilink PPP

Команда	Призначення
show ppp multilink	Загальна інформація про MLPPP-групи та їх члени
show ppp multilink active	Активні MLPPP-з'єднання
show ppp multilink interface Multilink	Детальна інформація про конкретний Multilink-інтерфейс
show interfaces Multilink	Стан та статистика Multilink-інтерфейсу
show interfaces Serial	Стан та статистика фізичного послідовного інтерфейсу
show controllers Serial	Визначення ролі інтерфейсу (DCE/DTE) та тактова частота
debug ppp negotiation	Відстеження процесу узгодження PPP (LCP/NCP)
debug ppp authentication	Відстеження процесу автентифікації PAP/CHAP

Відмовостійкість Multilink PPP

Multilink PPP забезпечує автоматичну відмовостійкість: при виході з ладу одного або декількох фізичних каналів групи маршрутизатор автоматично продовжує передачу через інтерфейси, що залишились активними. Логічний Multilink-інтерфейс залишається у стані "up" доти, доки принаймні один фізичний канал групи є активним.

На відміну від EtherChannel, в MLPPP немає окремого механізму "standby"-портів, проте будь-який активний послідовний інтерфейс, що входить до групи, рівноправно бере участь у передачі трафіку. При відновленні відключеного інтерфейсу він автоматично повертається у групу та починає брати участь у передачі даних.

Ролі DCE та DTE у послідовних каналах

У послідовних двоточкових каналах кожен з пристроїв виконує одну з двох ролей:

- **DCE** (Data Communication Equipment) – відповідає за синхронізацію каналу. Саме DCE-пристрій задає тактову частоту передачі командою clock rate. У реальній мережі функцію DCE виконує обладнання провайдера або перетворювачі (CSU/DSU).
- **DTE** (Data Terminal Equipment) – кінцевий пристрій, що підключається до каналу. Маршрутизатор-DTE отримує тактові імпульси від DCE-пристрою.

В навчальних стендах роль DCE та DTE визначається типом кабелю (V.35 DCE або DTE). Команда **show controllers *interface-type interface-id*** дозволяє визначити роль інтерфейсу (виводить рядок "DCE" або "DTE").

Стандарти послідовних інтерфейсів

Для з'єднання послідовних каналів між маршрутизаторами Cisco використовуються кабелі наступних стандартів: V.35 (найпоширеніший у лабораторних стендах), X.21, EIA/TIA-232, EIA/TIA-449, EIA-530. У сучасних маршрутизаторах Cisco для WAN-з'єднань через плати розширення типу VWIC використовуються роз'єми RJ-48, що відповідають стандарту T1/E1 (ISDN BRI).

Протокол HDLC та перехід до PPP

За замовчуванням на послідовних інтерфейсах маршрутизаторів Cisco застосовується протокол **Cisco HDLC** – фірмова модифікація стандартного HDLC (High-Level Data Link Control). Cisco HDLC несумісний зі стандартним ISO HDLC та обладнанням інших виробників через додаткове поле типу протоколу в заголовку.

Для взаємодії маршрутизаторів різних виробників, а також для підтримки розширених можливостей (автентифікації, стиснення, multilink) необхідно перейти на протокол PPP командою:

```
…
Router(config-if)# encapsulation ppp
…
```

Відмовостійкість агрегованих каналів та перевірка працездатності

Ключовою практичною перевагою агрегованих каналів є їхня відмовостійкість. Дослідження відмовостійкості виконується у такий спосіб:

- командою **shutdown** на одному з фізичних інтерфейсів агрегованого каналу імітується його відмова;
- за допомогою команд **show etherchannel summary** або **show ppp multilink** спостерігається новий стан каналу;
- командою **ping** перевіряється збереження зв'язності між кінцевими пристроями;
- командою **no shutdown** відновлюється відключений інтерфейс і підтверджується автоматичне повернення його до агрегованого каналу.

Команда **show etherchannel summary** у стовпці *Flags* відображає стан кожного фізичного інтерфейсу агрегованого каналу: **P** – інтерфейс активний (in bundle), **D** – інтерфейс не активний (down), **s** – у режимі standby (лише LACP).

Для перевірки наскрізного зв'язку між пристроями використовуються команди:

- **ping *IP_address*** – перевірка доступності вузла (ICMP Echo Request/Reply);
- **traceroute *IP_address*** – виведення повного маршруту проходження пакетів між вузлами, включно з усіма проміжними маршрутизаторами.

Рекомендована послідовність перевірки роботи EtherChannel і Multilink PPP

Рекомендована послідовність перевірки після завершення налаштування наведена нижче. Для кожної команди показано характерний вивід та пояснення ключових полів.

1. Перевірка стану EtherChannel.

```
Switch# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa0/1(P)   Fa0/2(P)
```

У стовпці Port-channel – стан агрегованого інтерфейсу: **(SU)** – Layer 2, in use (працює); **(SD)** – down. У дужках біля портів-членів: **(P)** – bundled (повноцінно входить у канал); **(I)** – stand-alone (виключений з каналу через несумісні режими); **(s)** – suspended (виключений через розбіжність параметрів). Стовпець Protocol – LACP або PAgP. Якщо колонка порожня – використовується статичний режим (**channel-group ... mode on**).

2. Деталізація переговорів LACP / PAgP.

```
Switch# show etherchannel detail
                Channel-group listing:
                ----------------------
Group: 1
----------
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:    LACP
Ports in the group:
-------------------
Port: Fa0/1
------------
Port state    = Up Mstr Assoc In-Bndl
Channel group = 1     Mode = Active
LACP Pdus sent: 23    LACP Pdus received: 22
```

Рядок «Port state = Up Mstr Assoc In-Bndl» свідчить про коректне включення інтерфейсу у канал. Якщо «Not-In-Bndl» – інтерфейс не зміг увійти. Лічильники LACP Pdus sent/received повинні зростати – якщо received залишається 0, на іншому боці LACP не налагоджено або порти у режимі passive з обох сторін.

3. Перевірка Multilink PPP.

```
Router# show ppp multilink

Multilink1, bundle name is R-2
  Bundle up for 00:15:32, total bandwidth 3072, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x12 received sequence, 0x15 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
```

```
      Se0/0/0, since 00:15:32
      Se0/0/1, since 00:15:30
```

Поле «total bandwidth» дорівнює сумі швидкостей усіх активних членів (для двох T1-каналів: 1536+1536=3072 кбіт/с). Рядок «Member links: 2 active» підтверджує, що обидва канали увійшли в bundle. Якщо одного з них немає у списку – перевірити **ppp multilink** і **ppp multilink group** на цьому інтерфейсі.

4. Перевірка стану і параметрів Multilink-інтерфейсу.

```
Router# show interface Multilink 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Internet address is 10.0.0.1/30
  MTU 1500 bytes, BW 3072 Kbit/sec, DLY 100000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open, multilink Open
  Open: IPCP, CDPCP, loopback not set
```

Стан up/up – multilink-інтерфейс активний. Поля LCP Open та multilink Open означають, що PPP-сесія встановлена і агрегація працює. «IPCP» – IP-протокол узгоджений, отже IP-адреса передається через канал. Якщо стан up/down – фізичні канали є, але PPP-узгодження не завершилося (перевірити **encapsulation ppp** на обох сторонах та збіжність аутентифікації, якщо налагоджена).

5. Перевірка зв'язності.

```
Router# ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/12 ms
```

Успішний **ping** (100%) підтверджує наскрізну зв'язність агрегованого каналу. Часткові втрати (наприклад, 80%) при двох активних членах bundle можуть свідчити про проблему з одним з фізичних каналів – потрібна перевірка лічильників помилок командою show interfaces serial для кожного фізичного інтерфейсу.

Типові помилки при налагодженні EtherChannel і Multilink PPP

1. **Несумісні режими LACP/PAgP на сторонах каналу.** Для успішного формування агрегованого каналу режими інтерфейсів на обох сторонах повинні бути сумісними. Сумісні комбінації для LACP: **active – active**, **active – passive**. Несумісна – **passive – passive** (жодна сторона не ініціює переговори). Для PAgP: **desirable – desirable**, **desirable – auto**. Несумісна – **auto – auto**. Найпоширеніша причина непрацюючого EtherChannel – обидва кінці у пасивному режимі. Перевіряти командою **show etherchannel summary** (стан **SU** – агрегований канал працює).

2. **Розбіжність параметрів інтерфейсів-членів каналу.** Усі фізичні інтерфейси, що включені в один port-channel, повинні мати **ідентичні параметри**: швидкість, дуплекс, режим (access/trunk), дозволені VLAN на trunk, native VLAN. Розбіжність хоча б одного параметра призводить до того, що інтерфейс виключається з каналу зі статусом **err-suspended**. Виправляти – або привести параметри до однакових, або тимчасово вимкнути проблемний інтерфейс командою **shutdown**.

3. **Спроба змішати LACP і PAgP в одному port-channel.** LACP (стандарт IEEE 802.3ad) і PAgP (фірмовий протокол Cisco) **несумісні між собою**. На обох сторонах повинен бути той самий протокол. Помилка часто виникає при підключенні Cisco-обладнання до іншого виробника – там доступний лише LACP, тому з боку Cisco також потрібно встановити LACP-режими (active або passive).

4. **Відсутність clock rate на DCE-стороні Serial-каналу при Multilink PPP.** На послідовних з'єднаннях за технологією V.35 одна сторона є DCE (надає синхронізацію), інша – DTE. Якщо на DCE-стороні не задано команду **clock rate** *rate*, фізичний канал залишається у стані **up/down** (line protocol is down). Перевіряти командою **show controllers serial** ***interface-id*** – відображається «clockrate is unset» для DCE або фактичне значення для DTE.

5. **Невірне налагодження multilink-групи.** Команда **ppp multilink group** ***number*** повинна бути виконана на **кожному** Serial-інтерфейсі, що входить до **multilink-bundle**. Номер групи – однаковий на всіх інтерфейсах одного маршрутизатора, але на іншій стороні каналу він може відрізнятися. Якщо команда не виконана на одному з інтерфейсів, цей канал не агрегується і працює окремо.

6. **Помилкова інкапсуляція PPP.** Multilink PPP працює лише поверх інкапсуляції PPP. Якщо на інтерфейсі залишилася стандартна інкапсуляція HDLC (за замовчуванням для Cisco Serial), агрегація не функціонує. Обов'язково встановити **encapsulation ppp** на обох сторонах кожного фізичного Serial-каналу.

7. **IP-адреса задана на фізичному інтерфейсі замість Multilink-інтерфейсу.** При використанні Multilink PPP IP-адреса повинна бути присвоєна **логічному інтерфейсу Multilink** *number*, а не фізичним Serial-інтерфейсам. На фізичних інтерфейсах IP-адреси НЕ призначаються – вони лише включаються до multilink-групи.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке агрегація каналів? Які переваги вона забезпечує?
2. Чим відрізняється EtherChannel від Multilink PPP?
3. Які три режими налагодження EtherChannel існують?
4. Чим протокол PAgP відрізняється від LACP? Який з них є стандартом IEEE?
5. Які режими має протокол PAgP? Які комбінації дозволяють створення каналу?
6. Які режими має протокол LACP? Які комбінації дозволяють створення каналу?
7. Які вимоги до фізичних портів для об'єднання в EtherChannel?
8. Які методи балансування навантаження підтримуються в EtherChannel? Як обрати оптимальний?
9. Як працює алгоритм хешування при балансуванні навантаження в EtherChannel?
10. Якою командою на комутаторі Cisco створюється EtherChannel? Якою – на маршрутизаторі?
11. Що таке Multilink PPP? Для чого він застосовується?
12. Чим відрізняються протоколи автентифікації PAP та CHAP?
13. Якими командами можна перевірити стан EtherChannel?
14. Якими командами можна перевірити стан Multilink PPP?
15. Як забезпечується відмовостійкість агрегованих каналів?
16. Що відбувається з трафіком при відключенні одного з фізичних інтерфейсів EtherChannel?
17. Чому режим ON (статичний) вважається менш надійним за динамічні режими PAgP/LACP?

ЗАНЯТТЯ № 2

ДОСЛІДЖЕННЯ ТА НАЛАГОДЖЕННЯ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ НА ОСНОВІ ГРУПУВАННЯ ПОРТІВ І ТРАНКОВОГО ПРОТОКОЛУ 802.1Q У МЕРЕЖАХ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження технології VLAN на основі групування портів і транкового протоколу 802.1Q на обладнанні Cisco; отримати практичні навички налагодження, моніторингу та діагностування роботи VLAN, побудованих на базі комутаторів Cisco із застосуванням агрегованих транкових каналів (EtherChannel); дослідити процеси розмежування широкомовних доменів, ізоляції трафіку різних VLAN та забезпечення централізованого керування мережею через виділену VLAN управління; навчитися налаштовувати захищений SSH-доступ до комутаторів з VLAN управління.

Обладнання та програмне забезпечення

Для виконання заняття на робочому місці студента має бути наявним таке обладнання та програмне забезпечення:

1. Керовані комутатори Cisco серії Catalyst 2960 (моделі WS-C2960-24TT-L або WS-C2960-48TT-L або WS-C2960S-F24TS-L або WS-C3560-24TS) – 3 шт.
2. Робочі станції (ПК або ноутбуки) з операційною системою Windows/Linux – не менше 2 шт.
3. Консольний кабель Cisco (rollover) з конектором RJ-45 та перехідником на USB або COM-порт – 1 шт.
4. Ethernet-кабелі прямого типу (T568B) категорії Cat 5e/Cat 6 – не менше 8 шт.
5. Термінальна програма-емулятор (PuTTY, Tera Term, SecureCRT або аналогічна) – встановлена на робочій станції.

Схема підключення

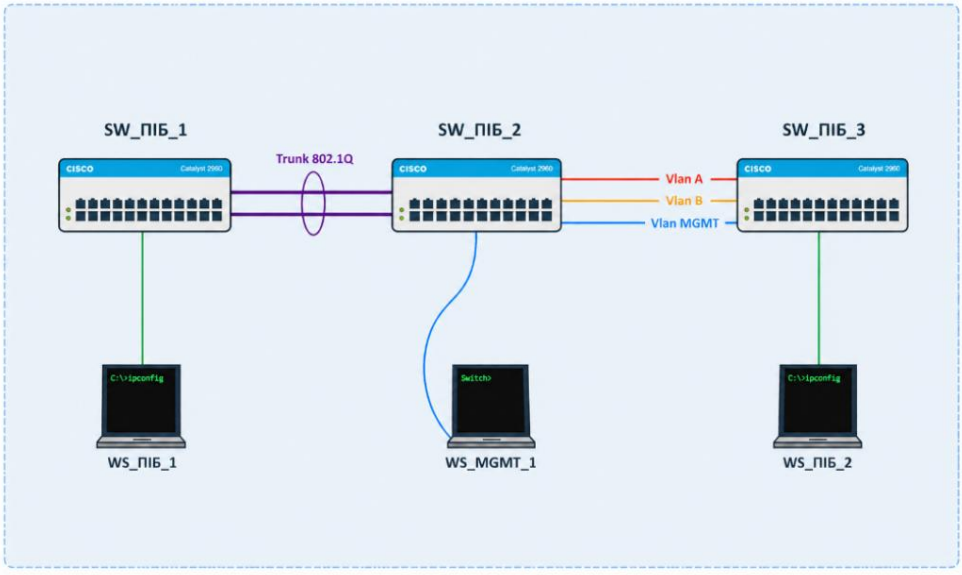

Рис. 2.1. Схема мережі, що будується у межах заняття

Примітка: ПІБ необхідно зазначати у скороченому форматі, який відповідає логіну для входу на платформу learn. Приклад: якщо логін для входу на learn – kb1_kmd, то назва комутатора має бути у форматі SW_kmd_1.

ЗАВДАННЯ

1. Ознайомитися з обладнанням та програмним забезпеченням робочого місця, перевірити наявність консольних та Ethernet-кабелів.
2. Створити мережу відповідно до схеми на рис. 2.1. Під час побудови звернути увагу на вибір типу кабелів та порядок підключення.
3. Провести налагодження іменування всіх 3 пристроїв (SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3) та встановити захищений пароль привілейованого режиму (**enable secret**).
4. Розробити схему IP-адресації пристроїв мережі згідно з варіантом (табл. 2.4). Заповнити таблицю адресації 2.1.

Таблиця 2.1.

Параметри адресації мережі

Мережа/Пристрій	Інтерфейс	MAC-адреса	IP-адреса	Маска	Префікс
VLAN даних A	–	–			
VLAN даних B	–	–			
VLAN керування	–	–			
SW1	Vlan				
SW2	Vlan				
SW3	Vlan				
WS1	NIC				
WS2	NIC				

5. Визначити номери VLAN згідно з варіантом (табл. 2.3). Заповнити таблицю 2.2 параметрів VLAN.

Таблиця 2.2.

Параметри VLAN мережі

Призначення VLAN	Назва VLAN	Номер VLAN
VLAN даних A		
VLAN даних B		
VLAN керування		

6. Виконати налаштування **VLAN** на всіх трьох комутаторах:

- На всіх трьох комутаторах (SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3) створити VLAN згідно з табл. 2.3, задати їм назви.
- Між комутаторами SW_ПІБ_1 та SW_ПІБ_2 налаштувати агрегований канал **EtherChannel** на двох фізичних Ethernet-інтерфейсах (режим згідно з табл. 2.3).
- Між комутаторами SW_ПІБ_1 та SW_ПІБ_2 налаштувати транковий канал який дозволятиме проходження VLAN даних A, B та VLAN управління. Налаштувати **Native VLAN** як VLAN за варіантом табл. 2.3. Вимкнути **DTP** командою **switchport nonegotiate**.
- Між комутаторами SW_ПІБ_2 та SW_ПІБ_3 налаштувати групування портів (окремий канал для кожної Vlan).

- На всіх трьох комутаторах налаштувати різні порти доступу для WS_ПІБ_1 та WS_ПІБ_2 для різних VLAN.

7. Налаштувати VLAN управління на всіх трьох комутаторах, призначити IP-адреси відповідно до табл. 2.1.

8. Налаштувати захищений SSH-доступ на всіх трьох комутаторах:

- Задати доменне ім'я (**ip domain-name**);
- Створити 2 користувачів (**Admin** та **User**) з рівнями привілеїв 15 та 1;
- Згенерувати RSA-ключі (**crypto key generate rsa modulus 2048**);
- Активувати SSHv2 (**ip ssh version 2**);
- Налаштувати лінії VTY на прийом виключно SSH-з'єднань (**transport input ssh**).

9. Налаштувати параметри IP-адресації на робочих станціях WS_ПІБ_1 та WS_ПІБ_2 відповідно до табл. 2.1 для перевірки зв’язку спочатку однакових VLAN а потім різних.

10. Перевірити наявність зв'язку в мережі:

- Командою **ping** підтвердити доступність між WS_ПІБ_1 та WS_ПІБ_2 з однієї VLAN.
- Командою **ping** підтвердити відсутність зв’язку між WS_ПІБ_1 та WS_ПІБ_2 з різних VLAN.
- Командою ping перевірити доступність усіх трьох комутаторів з WS_ПІБ_1 через VLAN керування.
- Підключитися до кожного комутатора по SSH з WS_ПІБ_1 або WS_ПІБ_2 та переконатися у правильності налаштувань доступу через VLAN керування.

11. Дослідити результати налаштувань за допомогою команд: **show vlan brief**, **show vlan**, **show interfaces switchport**, **show interfaces trunk**, **show interfaces port-channel switchport**, **show etherchannel summary**, **show dtp**, **show ip ssh**, **show users**, **show running-config**.

12. Дослідити відмовостійкість агрегованого транкового каналу: відключити один із фізичних інтерфейсів EtherChannel командою **shutdown** та перевірити збереження зв’язку між VLAN командою **ping**. Поновити інтерфейс командою **no shutdown**.

13. Вивести та проаналізувати файли конфігурацій усіх трьох комутаторів (**show running-config**).

14. У випадку виявлення помилок у налагодженнях – визначити причину та усунути їх.

15. Продемонструвати виконану роботу керівнику практики та оформити звіт.

ВАРІАНТИ ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Варіант визначається за номером стійки, за якою працюють студенти.

Таблиця 2.3.

Параметри налаштування VLAN та транкового каналу

№ в-та	VLAN A	VLAN B	VLAN MGMT	SW1–SW2 (EtherChannel)	SW1–SW2 (trunk)	Native VLAN
1	10	20	100	on / on	trunk/on	A
2	11	21	200	desirable / desirable	dynamic desirable	B
3	12	22	300	desirable / auto	trunk/on	A
4	13	23	400	auto / desirable	dynamic desirable	B
5	14	24	500	active / active	trunk/on	A
6	15	25	600	active / passive	trunk/on	B
7	16	26	700	passive / active	dynamic desirable	A
8	17	27	800	on / on	trunk/on	B
9	18	28	900	desirable / desirable	dynamic desirable	A
10	19	29	110	desirable / auto	trunk/on	B
11	30	40	120	auto / desirable	dynamic desirable	A
12	31	41	130	active / active	trunk/on	B
13	32	42	140	active / passive	dynamic desirable	A
14	33	43	150	passive / active	trunk/on	B
15	34	44	160	on / on	dynamic desirable	A
16	35	45	170	desirable / desirable	trunk/on	B
17	36	46	180	desirable / auto	dynamic desirable	A
18	37	47	190	auto / desirable	trunk/on	B
19	38	48	210	active / active	dynamic desirable	A
20	39	49	220	active / passive	trunk/on	B

Таблиця 2.4.

Параметри IP-адресації мережі

№ в-та	IP VLAN A	Prefix	IP VLAN B	Prefix	IP VLAN MGMT	Prefix	IP-адреса шлюзу за замовчуванням/
1	191.C.S.0	/24	192.C.S.0	/25	172.C.S.0	/27	Перша IP-адреса діапазону
2	192.C.S.0	/25	193.C.S.0	/26	172.C.S.0	/28	Остання IP-адреса діапазону
3	193.C.S.0	/26	194.C.S.0	/27	172.C.S.0	/29	Перша IP-адреса діапазону
4	194.C.S.0	/27	195.C.S.0	/28	172.C.S.0	/27	Остання IP-адреса діапазону
5	195.C.S.0	/28	196.C.S.0	/24	172.C.S.0	/28	Перша IP-адреса діапазону
6	196.C.S.0	/24	197.C.S.0	/25	172.C.S.0	/29	Остання IP-адреса діапазону
7	197.C.S.0	/25	198.C.S.0	/26	172.C.S.0	/27	Перша IP-адреса діапазону
8	198.C.S.0	/26	199.C.S.0	/27	172.C.S.0	/28	Остання IP-адреса діапазону
9	199.C.S.0	/27	200.C.S.0	/28	172.C.S.0	/27	Перша IP-адреса діапазону
10	200.C.S.0	/28	201.C.S.0	/24	172.C.S.0	/29	Остання IP-адреса діапазону
11	201.C.S.0	/24	202.C.S.0	/25	172.C.S.0	/27	Перша IP-адреса діапазону
12	202.C.S.0	/25	203.C.S.0	/26	172.C.S.0	/28	Остання IP-адреса діапазону
13	203.C.S.0	/26	204.C.S.0	/27	172.C.S.0	/29	Перша IP-адреса діапазону
14	204.C.S.0	/27	205.C.S.0	/28	172.C.S.0	/27	Остання IP-адреса діапазону
15	205.C.S.0	/28	206.C.S.0	/24	172.C.S.0	/28	Перша IP-адреса діапазону
16	206.C.S.0	/24	207.C.S.0	/25	172.C.S.0	/29	Остання IP-адреса діапазону
17	207.C.S.0	/25	208.C.S.0	/26	172.C.S.0	/27	Перша IP-адреса діапазону
18	208.C.S.0	/26	209.C.S.0	/27	172.C.S.0	/28	Остання IP-адреса діапазону
19	209.C.S.0	/27	210.C.S.0	/28	172.C.S.0	/29	Перша IP-адреса діапазону
20	210.C.S.0	/28	191.C.S.0	/24	172.C.S.0	/27	Остання IP-адреса діапазону

***Примітка*: C** (class) – номер аудиторії: для ауд. **107 – 71**, для ауд. **107a – 72, S** (stand) – номер стійки (зазначено зверху стійки).

УВАГА! В залежності від години проведення практики значення може змінюватись за вимогою керівника.

ЗМІСТ ЗВІТУ З ЗАНЯТТЯ

Звіт з заняття повинен містити:

1. Номер, тему та мету заняття.
2. Короткі теоретичні відомості (за власним конспектом, обсягом 2–3 сторінки) з таких питань: концепція та призначення VLAN, метод групування портів, стандарт IEEE 802.1Q та транкові канали, формат кадру 802.1Q, протокол DTP, SVI-інтерфейс, VLAN управління, протокол SSH (порівняння з Telnet), налаштування SSH на Cisco.
3. Перелік використаного обладнання та програмного забезпечення.
4. Схему (ФОТО) побудованої мережі з позначенням усіх пристроїв (SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3) та інтерфейсів, через які виконано з'єднання.
5. Розроблену схему IP-адресації у вигляді табл. 2.1 та параметри VLAN у вигляді табл. 2.2 з конкретними значеннями та розрахунками.
6. Лістинги команд (або скріншоти термінального вікна) з результатами виконання для кожного підзавдання 3–13, а саме:
   - налаштування VLAN на кожному комутаторі;
   - налаштування агрегованого каналу EtherChannel між SW_ПІБ_1 та SW_ПІБ_2;
   - налаштування транкового каналу між SW_ПІБ_1 та SW_ПІБ_2;
   - налаштування IP адрес та шлюзу за замовчуванням на всіх комутаторах;
   - налаштування SSH на всіх трьох комутаторах;
   - налаштування IP-адресації робочих станцій;
   - результати перевірки зв'язку (**ping** між WS, **ping** до комутаторів);
   - доступ по SSH до кожного комутатора;
   - вивід команд діагностики: **show vlan brief**, **show interfaces trunk**, **show interfaces switchport**, **show etherchannel summary**, **show dtp**, **show ip ssh, show users**;
   - результати дослідження відмовостійкості **EtherChannel**.
7. Опис проблем, що виникли під час виконання завдання, та шляхи їх усунення.
8. Висновки по заняттю.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Загальні відомості про VLAN

VLAN (Virtual Local Area Network, віртуальна локальна мережа) – логічна група вузлів комутованої мережі, що взаємодіють між собою так, ніби вони підключені до одного фізичного комутатора, незалежно від їхнього реального фізичного розташування. Технологія VLAN стандартизована у документі IEEE 802.1Q.

Традиційна комутована мережа без VLAN є єдиним широкомовним доменом: кожен широкомовний кадр (ARP-запит, DHCP-запит тощо) отримує і обробляє кожен хост мережі. Зі збільшенням кількості вузлів це призводить до

зростання широкомовного трафіку та деградації продуктивності. VLAN вирішує цю проблему шляхом поділу єдиного фізичного комутатора на кілька ізольованих логічних сегментів – широкомовних доменів.

Основні переваги використання VLAN:

- **Зменшення широкомовних доменів** – широкомовний трафік обмежений межами VLAN і не поширюється на інші VLAN;
- **Підвищення безпеки** – вузли різних VLAN не можуть безпосередньо взаємодіяти між собою без участі маршрутизатора або L3-комутатора;
- **Гнучка логічна структура** – адміністратор може об'єднувати вузли у логічні групи незалежно від їхнього фізичного розташування;
- **Спрощення адміністрування** – переміщення вузла між VLAN виконується засобами конфігурування комутатора без фізичного перепідключення;
- **Якість обслуговування (QoS)** – різним VLAN можна призначати різні пріоритети передачі трафіку.

Методи ідентифікації VLAN

Існують різні методи визначення приналежності вузла або кадру до тієї чи іншої VLAN:

- **Групування портів (port-based VLAN)** – найпоширеніший метод. Кожному фізичному порту комутатора призначається певний ідентифікатор VLAN (VID). Кадри, що надходять через цей порт, вважаються такими, що належать відповідній VLAN. Метод не вимагає модифікації кінцевих пристроїв.
- **VLAN на основі MAC-адрес** – VLAN визначається на основі MAC-адреси відправника кадру. Таблиця відповідності MAC-адрес та VLAN зберігається в спеціальному сервері VMPS (VLAN Membership Policy Server). Метод гнучкий, але складніший в адмініструванні.
- **VLAN на основі протоколу** – VLAN визначається за типом мережного протоколу (наприклад, IP, IPX, AppleTalk). Зазвичай реалізується у комутаторах рівня 3.
- **VLAN на основі аутентифікації (802.1X)** – VLAN призначається динамічно після успішної аутентифікації користувача за протоколом 802.1X.

Призначення та суть транкових каналів

Порт доступу (access port) підключає кінцевий пристрій до одної конкретної VLAN та передає нетеговані кадри. Проте в комутованій мережі з кількома VLAN постає завдання передачі трафіку різних VLAN між комутаторами через один фізичний канал. Для цього використовуються транкові канали (trunk links).

Транковий канал – це канал між двома комутаторами (або між комутатором і маршрутизатором), через який передаються кадри, що належать

кількох різним VLAN. Щоб отримувач знав, до якої VLAN належить кожен кадр, застосовується механізм тегування.

Формат кадру IEEE 802.1Q

Стандарт IEEE 802.1Q визначає механізм тегування кадрів Ethernet для передачі по транковому каналу. Відповідно до цього стандарту, до стандартного кадру Ethernet між полями Source MAC та Type/Length вставляється 4-байтовий тег 802.1Q (VLAN-тег).

Структура тегу 802.1Q (4 байти):

- **TPID (Tag Protocol Identifier, 2 байти)** – ідентифікатор протоколу тегування, завжди дорівнює 0x8100 для 802.1Q;
- **TCI (Tag Control Information, 2 байти)** – поле управління тегом, що включає:
- **PCP (Priority Code Point, 3 біти)** – пріоритет кадру за стандартом IEEE 802.1p (0–7);
- **DEI (Drop Eligible Indicator, 1 біт)** – індикатор дозволу на відкидання кадру при перевантаженні мережі;
- **VID (VLAN Identifier, 12 біт)** – ідентифікатор VLAN, діапазон значень 0–4095; для мереж Ethernet активно використовується діапазон 2–1001.

Таким чином, 12-бітове поле VID дозволяє ідентифікувати до 4096 різних VLAN (0–4095), з яких VLAN 0 та VLAN 4095 зарезервовані, а VLAN 1 є VLAN за замовчуванням на обладнанні Cisco.

Порівняльна таблиця форматів кадру Ethernet та 802.1Q наведена в табл. 2.5.

Таблиця 2.5.

Порівняння форматів кадру стандартного Ethernet та IEEE 802.1Q

Поле	Звичайний Ethernet	802.1Q кадр	Розмір	Значення/Діапазон
Destination MAC	+	+	6 байт	MAC-адреса отримувача
Source MAC	+	+	6 байт	MAC-адреса відправника
802.1Q Tag (TPID+TCI)	–	+	4 байти	0x8100 + PCP+DEI+VID
Ethertype / Length	+	+	2 байти	Тип протоколу
Payload (Data)	+	+	46–1500 байт	Дані
FCS (CRC)	+	+	4 байти	Контрольна сума

Протокол тегування ISL (Inter-Switch Link)

ISL (Inter-Switch Link) – фірмовий протокол Cisco для тегування кадрів у trunk-каналах, розроблений до появи стандарту IEEE 802.1Q. На відміну від 802.1Q, ISL не вставляє тег всередину кадру, а повністю інкапсулює (обгортає)

оригінальний Ethernet-кадр у новий ISL-заголовок (26 байт) та трейлер (4 байти). Це збільшує максимальний розмір кадру з 1518 до 1548 байт.

Ключові відмінності ISL від IEEE 802.1Q наведені у табл. 2.6.

Таблиця 2.6.

Порівняння ISL та IEEE 802.1Q

Характеристика	ISL	IEEE 802.1Q
Розробник	Cisco (фірмовий)	IEEE (відкритий стандарт)
Метод тегування	Повна інкапсуляція кадру	Вставка 4-байтового тегу
Розмір накладних витрат	30 байт (26 + 4)	4 байти
Native VLAN	Не підтримується	Підтримується
Максимум VLAN	1000	4094
Підтримка на 2960/3650/3850	Відсутня	Є
Підтримка на 3560/3750	Є	Є
Статус	Застарілий (deprecated)	Актуальний, рекомендований

На обладнанні Cisco Catalyst 3560 і 3750, яке присутнє у лабораторії, обидва протоколи підтримуються. Саме тому на цих моделях перед командою **switchport mode trunk** необхідно явно вказати тип інкапсуляції:

```
…
MLS(config-if)# switchport trunk encapsulation dot1q
MLS(config-if)# switchport mode trunk
…
```

Без цього команда **switchport mode trunk** поверне помилку, оскільки комутатор не може визначити, який протокол використовувати. На Catalyst 2960 ця команда не потрібна, бо 2960 підтримує виключно dot1q і визначає тип автоматично.

Перевірити поточний протокол тегування на trunk-порту можна командою **show interfaces trunk** – у стовпці **Encapsulation** відображається **802.1q** або **isl**.

Сьогодні ISL не використовується у нових розгортаннях. Cisco рекомендує виключно IEEE 802.1Q для всіх trunk-з'єднань.

Native VLAN та нетеговані кадри

Для кожного транкового порту визначається так звана **Native VLAN** (рідна VLAN). Кадри, що належать Native VLAN, передаються через транковий канал у нетегованому вигляді (без вставки тегу 802.1Q). Кадри решти VLAN тегуються відповідним VID.

За замовчуванням на комутаторах Cisco Native VLAN – це VLAN 1. З міркувань безпеки рекомендується:

- Змінити Native VLAN з VLAN 1 на будь-яку невикористовувану VLAN (наприклад, VLAN 999);
- Налаштувати тегування кадрів Native VLAN командою **vlan dot1q tag native** (глобально) або **switchport trunk native vlan tag** (на інтерфейсі), щоб запобігти атакам подвійного тегування (double-tagging attack).

Протокол DTP (Dynamic Trunking Protocol)

DTP (Dynamic Trunking Protocol) – фірмовий протокол Cisco для автоматичного узгодження параметрів транкового з'єднання між двома

комутаторами. DTP визначає, чи стане з'єднання транковим, і який протокол тегування буде використовуватись (ISL або 802.1Q).

Режими роботи інтерфейсу щодо DTP:

- **trunk (on)** – примусовий транковий режим; інтерфейс надсилає DTP-кадри та безумовно стає транковим;
- **dynamic desirable** – активно намагається встановити транковий зв'язок, надсилаючи DTP-кадри;
- **dynamic auto** (за замовчуванням) – відповідає на DTP-кадри від сусіда, але сам не ініціює;
- **access** – примусовий режим доступу; DTP-кадри надсилаються, але з'єднання ніколи не стане транковим;
- **nonegotiate** – DTP-кадри не надсилаються і не обробляються; рекомендується поєднувати з режимом **trunk** для підключення до обладнання сторонніх виробників.

Комбінації режимів, за яких формується транковий канал, наведені в таблиці 2.7.

Таблиця 2.7.

Комбінації режимів DTP та результуючий тип з'єднання

Режим	trunk	dynamic desirable	dynamic auto	access
trunk	trunk	trunk	trunk	–
dynamic desirable	trunk	trunk	trunk	access
dynamic auto	trunk	trunk	access	access
access	–	access	access	access

Принцип групування портів (Port-Based VLAN)

При використанні методу групування портів кожен фізичний порт комутатора статично або динамічно прив'язується до певної VLAN. Кадри, отримані на порту доступу, вважаються такими, що належать VLAN, призначеній цьому порту. Порт доступу не додає і не видаляє теги 802.1Q – ця операція виконується виключно всередині комутатора.

Коли комутатор отримує нетегований кадр на порту доступу, він асоціює кадр з VLAN даного порту та пересилає його тільки тим портам, що належать тій самій VLAN (або транковим портам, на яких дана VLAN дозволена). Завдяки цьому трафік різних VLAN є повністю ізольованим на канальному рівні.

Рекомендації Cisco щодо безпеки VLAN

Компанія Cisco розробила перелік базових рекомендацій щодо підвищення рівня захищеності комутованих мереж із VLAN:

1. Відключити всі незадіяні порти та перемістити їх у спеціальну невикористовувану VLAN;
2. Використовувати нестандартну VLAN (відмінну від VLAN 1) як VLAN управління;
3. Не використовувати VLAN 1 для жодного виробничого або адміністративного трафіку;

4. Налаштувати всі порти підключення кінцевих користувачів як порти доступу та вимкнути DTP на цих портах;

5. Явно налаштовувати параметри транкових портів, не покладаючись виключно на DTP;

6. Завжди явно вказувати список дозволених VLAN для транкових каналів;

7. Налаштувати тегування Native VLAN та відкидання нетегованих кадрів на транкових портах;

8. Вимкнути стан порту за замовчуванням – перевести незадіяні порти у shutdown.

Порядок налаштування VLAN на основі групування портів

Порядок налаштування VLAN на основі групування портів на комутаторі Cisco згідно з рекомендаціями виробника:

1. Створити VLAN командою **vlan *vlan-id*** у режимі глобального конфігурування;

2. Вказати текстову назву для VLAN командою **name *text-string*** (необов'язково, але рекомендується для документування);

3. Для інтерфейсу/групи інтерфейсів доступу задати тип access командою **switchport mode access**;

4. Призначити інтерфейс до потрібної VLAN командою **switchport access vlan *vlan-id***;

5. Для транкових інтерфейсів задати тип trunk командою **switchport mode trunk**;

6. Налаштувати параметри транкового каналу (дозволені VLAN, Native VLAN) та вимкнути DTP командою **switchport nonegotiate**;

7. Налаштувати SVI для VLAN управління та призначити IP-адресу комутатору;

8. Вимкнути всі незадіяні порти та перевести їх у спеціальну невикористовувану VLAN.

Основні команди налаштування VLAN

Синтаксис команди **vlan** (режим глобального конфігурування):

vlan *vlan-id*,

де ***vlan-id*** – ідентифікатор (номер) VLAN, може зазначатися в межах від 1 до 4094, для мереж Ethernet типове використання у діапазоні від 2 до 1001.

Синтаксис команди **name** (режим конфігурування VLAN):

name *text-string*,

де ***text-string*** – текстова назва VLAN; якщо текстова назва VLAN явно не зазначається, то система автоматично встановлює назву ви-гляду VLANDDDD, де DDDD – чотирицифровий десятковий номер VLAN.

Синтаксис команди **switchport access vlan** (режим конфігуру-вання інтерфейсу/групи інтерфейсів):

switchport access vlan {*vlan-id* | dynamic},

де ***vlan-id*** – ідентифікатор VLAN;

dynamic – параметр, який зазначає, що належність інтерфей-су/порту до VLAN визначається динамічно (за MAC-адресою), шля-хом запиту до сервера VMPS (VLAN Membership Policy Server).

Синтаксис команди **switchport trunk** (режим конфігурування інтерфейсу/групи):

switchport trunk {allowed vlan *vlan-list* | native vlan *vlan-id* | pruning vlan *vlan-list*},

де **allowed vlan** – службова конструкція, за допомогою якої створюється список дозволених VLAN, для яких транковий інтерфейс може пересилати та отримувати трафік у тегованій формі; за замовчуванням ***vlan-list*** для цієї конструкції дорівнює **all**; ***vlan-list*** у цьому випадку не може дорівнювати **none**;

native vlan – службова конструкція, за допомогою якої створюється список VLAN, для яких транковий інтерфейс може пересилати і отримувати трафік у нетегованій формі;

pruning vlan – службова конструкція, за допомогою якої створюється список VLAN, для яких транковий інтерфейс активований для підтримки режиму VTP-pruning; ***vlan-list*** у цьому випадку не може дорівнювати **all**;

vlan-list – може набувати значень, що наведені нижче; деякі з цих значень доповнюються параметрами ідентифікаторів VLAN IDs:

vlan-atom – список ідентифікаторів VLAN (наприклад, 10-20; 10-30,35-40);

add – додати окрему VLAN або групу VLAN за списком;

all – додати всі VLAN;

except – виключити окрему VLAN або групу VLAN за списком;

none – пустий список;

remove – виключити VLAN зі списку

Синтаксис команди **switchport native** (режим конфігурування інтерфейсу/групи інтерфейсів):

switchport native vlan *vlan-id,*

де ***vlan-id*** – ідентифікатор VLAN.

Налаштування SVI (Switched Virtual Interface) для VLAN управління:

```
…
Switch(config)# interface vlan vlan-id
Switch(config-if)# description text
Switch(config-if)# ip address IP_address network_mask
Switch(config-if)# no shutdown
…
```

Вимкнення DTP на транковому інтерфейсі (рекомендується при підключенні до обладнання сторонніх виробників або при статичному транкуванні):

```
…
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport nonegotiate
…
```

Типовий сценарій налаштування VLAN для навчальної мережі

Нижче наведено типовий сценарій налаштування комутаторів з агрегованим транковим каналом:

Створення VLAN

```
…
Switch(config)# vlan 100
Switch(config-vlan)# name DATA-VLAN-A
Switch(config-vlan)# exit
Switch(config)# vlan 200
Switch(config-vlan)# name DATA-VLAN-B
Switch(config-vlan)# exit
…
```

Агрегований транковий канал

```
Switch(config)# interface range GigabitEthernet0/1-2
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# switchport nonegotiate
Switch(config-if-range)# channel-group 1 mode on
Switch(config-if-range)# exit
Switch(config)# interface port-channel 1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100, 200
Switch(config-if)# switchport trunk native vlan 100
Switch(config-if)# exit
…
```

Порівняння Telnet та SSH

Протокол **Telnet** (Teletype Network, RFC 854) – один із найстаріших протоколів для організації інтерактивного термінального доступу до мережних пристроїв. Telnet передає всі дані, у тому числі ім'я користувача та пароль, у відкритому (незашифрованому) вигляді, що робить його вразливим до перехоплення трафіку.

Протокол **SSH** (Secure Shell, RFC 4251–4256) – захищений протокол для організації термінального доступу з криптографічним захистом каналу. SSH забезпечує шифрування всього трафіку між клієнтом і сервером, аутентифікацію та цілісність даних.

Порівняння протоколів Telnet та SSH наведено в таблиці 2.8.

Таблиця 2.8.

Порівняння протоколів Telnet та SSH

Характеристика	Telnet	SSH
Шифрування трафіку	Відкритий текст	AES, 3DES тощо
Порт	TCP 23	TCP 22
Аутентифікація	Відкритий пароль	Захищений пароль або ключ
Цілісність даних	Перевірка відсутня	HMAC
Підтримка PKI	Відсутня	RSA-ключі
Рекомендація до застосування	У лабораторних умовах	У виробничих мережах

Версії SSH

Існують дві версії протоколу SSH:

- **SSH версії 1 (SSHv1)** – перша реалізація; містить відомі вразливості (Man-in-the-Middle атака) і вважається застарілою. На обладнанні Cisco рекомендується відключити SSHv1.
- **SSH версії 2 (SSHv2)** – сучасна версія з покращеним шифруванням, обміном ключами Diffie-Hellman та строгою перевіркою цілісності. Cisco рекомендує використовувати виключно SSHv2.

Налаштування SSH на комутаторах Cisco

Для налаштування SSH-доступу на комутаторах Cisco необхідно виконати такий порядок дій:

1. Задати доменне ім'я пристрою (обов'язково для генерації RSA-ключа);
2. Задати ім'я хосту (**hostname**) – воно використовується у RSA-ключі;
3. Створити локальних користувачів командою **username**;
4. Згенерувати пару RSA-ключів командою **crypto key generate rsa**;
5. Обмежити версію SSH (рекомендується SSHv2) командою **ip ssh version 2**;
6. Налаштувати лінії VTY для використання SSH командами **transport input ssh** та **login local**.

Для підключення по SSH з робочої станції (що знаходиться у VLAN управління та має IP-адресу з тієї ж підмережі) використовуються такі команди:

З командного рядка Windows:

C:\> ssh -l Admin 192.168.1.2

де **Admin** – ім'я користувача, **192.168.1.2** – IP-адреса VLAN управління комутатора.

З терміналу Linux:

$ ssh Admin@192.168.1.2

З PuTTY:

у полі **Host Name** вказати IP-адресу комутатора, обрати **Connection type** – SSH, **Port** – 22, натиснути Open. У вікні терміналу ввести ім'я користувача та пароль.

З іншого пристрою Cisco (маршрутизатора або комутатора):

Router# ssh -v 2 -l Admin 192.168.1.2

Команди моніторингу та діагностики VLAN на комутаторах Cisco

Для моніторингу та діагностики VLAN на комутаторах Cisco застосовуються спеціалізовані та загальні команди show (таблиця 2.9).

Таблиця 2.9.

Команди діагностики VLAN та SSH на комутаторах Cisco

Команда	Призначення
show vlan	Повна інформація про всі VLAN та їх порти
show vlan brief	Скорочений перегляд: номер, назва, стан, порти
show vlan id *vlan-id*	Детальна інформація про конкретну VLAN за номером

Команда	Призначення
show vlan name *vlan-name*	Інформація про VLAN за її назвою
show vlan summary	Зведена інформація: кількість VLAN, VTP VLAN тощо
show interfaces switchport	Параметри VLAN для всіх інтерфейсів
show interfaces *interface-type interface-id* switchport	Параметри VLAN для конкретного інтерфейсу
show interfaces trunk	Параметри транкових з'єднань та дозволені VLAN
show interfaces vlan *vlan-id*	Стан та статистика SVI-інтерфейсу VLAN
show dtp	Параметри DTP для всього комутатора
show dtp interface *interface-type interface-id*	Параметри DTP для конкретного транкового порту
show running-config	Поточна конфігурація пристрою (містить налаштування VLAN)
show mac-address-table	Таблиця MAC-адрес комутатора з VLAN
show ip ssh	Версія та параметри SSH-сервера
show users	Активні сесії на пристрої (у т.ч. SSH-сесії)

Комбінування VLAN з агрегованим каналом EtherChannel

Перевагами реалізації двох технологій агрегування та транкування каналу 802.1Q:

- Збільшена **пропускна здатність** між комутаторами (2×1 Гбіт/с = 2 Гбіт/с при двох фізичних каналах);
- **Відмовостійкість**: при виході з ладу одного з фізичних каналів EtherChannel логічний канал залишається активним, а трафік усіх VLAN продовжує передаватися;
- **Єдина точка управління**: транкові параметри (дозволені VLAN, Native VLAN) налаштовуються на логічному інтерфейсі port-channel, а не на кожному фізичному інтерфейсі окремо;
- **STP** (Spanning Tree Protocol) сприймає EtherChannel як єдиний логічний канал, що спрощує топологію дерева та прискорює збіжність.

Важливою особливістю є порядок налаштування: параметри інтерфейсу VLAN (**switchport mode trunk**, **switchport trunk allowed vlan**) необхідно задавати саме на логічному інтерфейсі **port-channel**, а не на фізичних інтерфейсах, що входять до групи. Фізичні інтерфейси мають наслідувати параметри логічного port-channel-інтерфейсу автоматично.

Перевірити стан агрегованого транкового каналу можна командами:

- **show etherchannel summary** – стан EtherChannel та фізичних членів групи;
- **show interfaces port-channel *port-channel-id* switchport** – параметри транкування логічного каналу;
- **show interfaces trunk** – відображення port-channel у переліку транкових з'єднань.

Рекомендована послідовність перевірки роботи VLAN і транків 802.1Q

Рекомендована послідовність перевірки після завершення налаштування наведена нижче. Для кожної команди показано характерний вивід та пояснення ключових полів.

1. Перевірка створених VLAN та призначення портів.

```
Switch# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
10   STUDENTS                         active    Fa0/1, Fa0/2
20   TEACHERS                         active    Fa0/3, Fa0/4
100  MANAGEMENT                       active
```

У таблиці повинні бути присутні всі створені VLAN зі статусом **active**. У стовпці Ports перелічені access-порти, призначені до кожної VLAN. Trunk-порти **не відображаються** у виводі цієї команди – для них використовуйте show interfaces trunk. VLAN 100 без портів – нормально для management-VLAN, доступ до якої здійснюється лише через транк.

2. Перевірка стану trunk-каналу.

```
Switch# show interfaces trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/24      on               802.1q         trunking      100
ort        Vlans allowed on trunk
Fa0/24      1,10,20,100
Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,100
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,100
```

Status повинен бути **trunking** – порт активно передає тегований трафік. Encapsulation – **802.1q**. Native VLAN – повинна збігатися на обох сторонах транка (тут – 100). У рядку «Vlans allowed and active» – VLAN, які реально активні на цьому транку. Якщо VLAN не у переліку «allowed» – кадри цієї VLAN через транк не передаються.

3. Перевірка стану конкретного порту.

```
Switch# show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (STUDENTS)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
```

Administrative Mode – те, що задано адміністратором; Operational Mode – фактичний режим. Для access-порту обидва повинні бути «static access». Поле Access Mode VLAN – VLAN, до якої призначений порт. Якщо Operational Mode = «trunk» замість заданого «access» – це означає, що порт перейшов у trunk-режим автоматично через DTP – небезпечна ситуація, потрібна команда **switchport nonegotiate**.

4. Перевірка таблиці MAC-адрес.

```
Switch# show mac address-table
          Mac Address Table

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0050.ab12.3456    DYNAMIC     Fa0/1
  10    0050.ab12.3478    DYNAMIC     Fa0/24
  20    0050.ab12.3490    DYNAMIC     Fa0/3
 100    0050.ab56.7800    DYNAMIC     Fa0/24
```

Таблиця MAC-адрес показує, які пристрої комутатор бачить на кожному порту і у якій VLAN. MAC-адреси, отримані через trunk-порт (Fa0/24), належать кінцевим пристроям з іншого комутатора. Якщо MAC-адреса з'явилася не у тій VLAN – помилка призначення порту. Якщо MAC-адреси з access-порту немає у таблиці – пристрій не передає трафік або відключений.

5. Перевірка зв'язку між пристроями.

```
C:\> ping 192.168.10.20
Reply from 192.168.10.20: bytes=32 time<1ms TTL=128
Reply from 192.168.10.20: bytes=32 time<1ms TTL=128

C:\> ping 192.168.20.20
Request timed out.
```

У межах однієї VLAN (наприклад, VLAN 10) пристрої повинні бачити один одного через ping. У межах різних VLAN ping без маршрутизатора або L3-комутатора **не повинен працювати** – це і є сегментація. Якщо ping між VLAN несподівано працює – VLAN не ізольовані (ймовірно, обидва порти в одній VLAN, або є нелегальний шлюз).

Типові помилки при налагодженні VLAN і транків 802.1Q

1. **VLAN не створений у базі даних комутатора.** Просте призначення команди **switchport access vlan *vlan-id*** без попереднього створення VLAN у глобальній конфігурації призводить до того, що порт залишається у стандартній VLAN 1 або переходить у inactive-стан. Перед призначенням порту до VLAN необхідно створити її командою **vlan *vlan-id*** у режимі глобальної конфігурації. Перевіряти командою **show vlan brief** – VLAN повинна мати статус **active**.

2. **Порт залишений у режимі dynamic auto/desirable у production-мережі.** За замовчуванням Cisco-комутатори увімкнені в режимі **dynamic auto** , що дозволяє порту автоматично перейти у trunk при отриманні DTP-кадрів. Це створює загрозу безпеки (VLAN hopping). У production-мережі обов'язково задавати режим явно: **switchport mode access** для портів кінцевих пристроїв або **switchport mode trunk** для транків. На access-портах додатково вимикати DTP командою **switchport nonegotiate**.

3. **Розбіжність Native VLAN на trunk-каналі.** Native VLAN – це VLAN, кадри якої передаються транком БЕЗ тегування. Якщо на двох сторонах транка налагоджено різні Native VLAN – комутатор Cisco видає попередження «native VLAN mismatch detected» і кадри Native VLAN не доходять до іншого боку. Обов'язково встановлювати однакову Native VLAN на обох сторонах командою **switchport trunk native vlan *vlan-id***. Рекомендується змінити Native VLAN з дефолтної 1 на іншу (наприклад, виділену management-VLAN) – для безпеки.

4. **VLAN не дозволена на транку.** За замовчуванням транк передає всі VLAN (1–4094). Однак якщо адміністратор обмежив список командою **switchport trunk allowed vlan *vlan-list***, то всі інші VLAN автоматично заборонені. Помилка – забути додати нову VLAN до allowed-списку. Перевіряти командою **show interfaces trunk** – у стовпці «Vlans allowed and active in management domain» повинні бути всі необхідні VLAN. Для додавання нової VLAN до існуючого списку використовувати **switchport trunk allowed vlan add *vlan-id***.

5. **Помилкова інкапсуляція на транку.** Деякі моделі Cisco-комутаторів (наприклад, серії 3560) підтримують дві технології транкінгу: 802.1Q і ISL (фірмовий, застарілий). За замовчуванням може бути встановлено dynamic-режим інкапсуляції, що призводить до неузгодженості. Обов'язково задавати явно командою **switchport trunk encapsulation dot1q** перед командою switchport mode trunk. На моделях, що підтримують лише 802.1Q (наприклад, 2960), ця команда недоступна – інкапсуляція встановлюється автоматично.

6. **Management VLAN не налагоджена або без шлюзу.** Для віддаленого керування комутатором використовується SVI (інтерфейс VLAN). Помилки: SVI створено, але не введено в експлуатацію командою **no shutdown**; SVI має IP-адресу, але порт-член Management-VLAN не існує (немає трафіку для активації SVI); не задано шлюз за замовчуванням командою **ip default-gateway**, що унеможливлює керування з іншої підмережі. Перевіряти командою **show ip interface brief** – SVI повинен мати стан up/up.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке VLAN? Яке призначення та основні переваги технології VLAN у комутованих мережах?
2. Поняття широкомовного домену. Яким чином VLAN обмежує розмір широкомовного домену?
3. Які методи ідентифікації VLAN існують? Охарактеризуйте метод групування портів (port-based VLAN).
4. Що таке порт доступу (access port)? Чим він відрізняється від транкового порту (trunk port)?
5. Що таке транковий канал? Яке його призначення у мережі з декількома VLAN?
6. Охарактеризуйте стандарт IEEE 802.1Q. Яка структура тегованого кадру 802.1Q?
7. Скільки VLAN можна ідентифікувати за допомогою поля VID у тегу 802.1Q? Поясніть з урахуванням розміру поля у бітах.
8. Що таке Native VLAN? Як передаються кадри Native VLAN через транковий канал? Яка VLAN є Native за замовчуванням на комутаторах Cisco?
9. Що таке атака подвійного тегування (double-tagging attack)? Яким чином налаштування Native VLAN допомагає її запобігти?
10. Що таке протокол DTP (Dynamic Trunking Protocol)? Які режими роботи він підтримує? При яких комбінаціях режимів формується транковий канал?
11. Що таке VLAN управління (Management VLAN)? Яке її призначення? Чому не рекомендується використовувати VLAN 1 як VLAN управління?
12. Що таке SVI (Switched Virtual Interface)? Яке призначення цього інтерфейсу? Якою командою він налаштовується?
13. Чи можуть хости різних VLAN взаємодіяти між собою без маршрутизатора або L3-комутатора? Поясніть відповідь.
14. Перелічіть основні рекомендації Cisco щодо підвищення рівня захищеності VLAN. Поясніть призначення кожного заходу.
15. Яким чином вимикається протокол DTP на транковому порту? Коли це доцільно застосовувати?
16. Які основні команди налаштування VLAN на основі групування портів та транкових каналів існують на комутаторах Cisco? Поясніть синтаксис кожної команди.
17. Яким чином агрегований канал EtherChannel поєднується з транковим каналом 802.1Q? На якому інтерфейсі (фізичному чи логічному port-channel) налаштовуються параметри VLAN і чому?

ЗАНЯТТЯ № 3

ДОСЛІДЖЕННЯ ТА НАЛАГОДЖЕННЯ МАРШРУТИЗАЦІЇ МІЖ ВІРТУАЛЬНИМИ ЛОКАЛЬНИМИ МЕРЕЖАМИ (INTER-VLAN ROUTING) У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з принципами організації Inter-VLAN Routing; розглянути два основних способи організації Inter-VLAN Routing – Legacy (окремі фізичні інтерфейси маршрутизатора для кожної VLAN) та Router-on-a-Stick (підінтерфейси з протоколом 802.1Q на транковому каналі); отримати практичні навички створення VLAN, налагодження транкових та access-портів, підінтерфейсів маршрутизатора, DHCP-серверів для кожної VLAN, VLAN для керування (Management VLAN) з доступом через SSH; дослідити процеси маршрутизації між VLAN та процеси передачі даних у побудованій мережі.

Обладнання та програмне забезпечення

Для виконання заняття на робочому місці студента має бути наявним таке обладнання та програмне забезпечення:

1. Маршрутизатор Cisco серії 2811/2821/2901/2911/2921 з не менш ніж 3 маршрутизованими (routed) Ethernet-інтерфейсами – 1 шт. (модель 1841 – лише з додатковим routed-модулем, напр. HWIC-1FE/HWIC-2FE; модуль HWIC-4ESW не підходить, оскільки його порти є switchport, а для Legacy потрібні routed-інтерфейси).
2. Керовані комутатори Cisco серії Catalyst 2960 (моделі WS-C2960-24TT-L або WS-C2960-48TT-L або WS-C2960S-F24TS-L) – 2 шт.
3. Робочі станції (ПК або ноутбуки) з операційною системою Windows/Linux – не менше 2 шт.
4. Консольний кабель Cisco (rollover) з конектором RJ-45 та перехідником на USB або COM-порт – 1 шт.
5. Ethernet-кабелі прямого типу (T568B) категорії Cat 5e/Cat 6 – не менше 6 шт. (2 канали Legacy R–SW2, 1 транковий канал R–SW1, 2 канали до робочих станцій).
6. Термінальна програма-емулятор (PuTTY, Tera Term, SecureCRT або аналогічна) – встановлена на робочих станціях.

Схема підключення

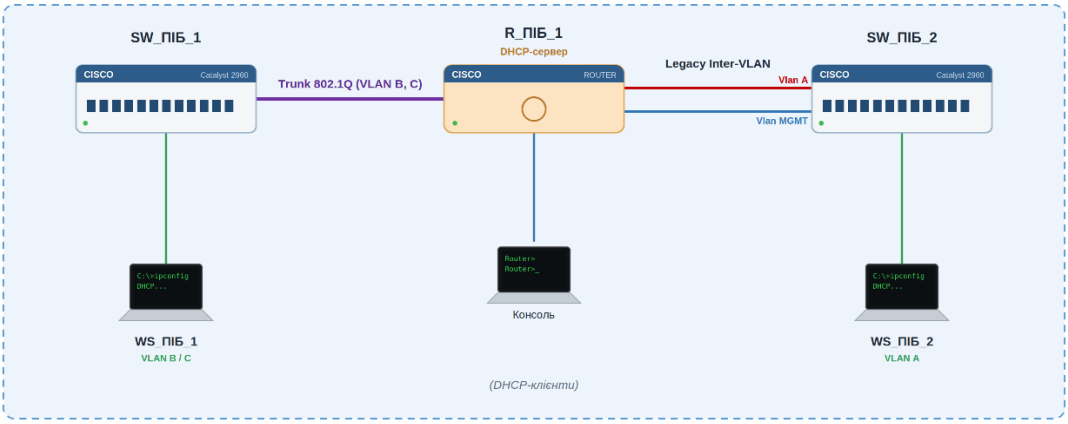

Рис. 3.1. Схема мережі, що будується у межах заняття

Примітка: ПІБ необхідно зазначати у скороченому форматі, який відповідає логіну для входу на платформу learn. Приклад: якщо логін для входу на learn – kb1_kmd, то назва комутатора має бути у форматі SW_kmd_1.

ЗАВДАННЯ

1. Ознайомитися з обладнанням та програмним забезпеченням робочого місця, перевірити наявність консольного та Ethernet-кабелів, термінальної програми.

2. Створити мережу відповідно до схеми на рис. 3.1. Мережа складається з маршрутизатора R_ПІБ_1, двох комутаторів SW_ПІБ_1 та SW_ПІБ_2 і двох робочих станцій WS_ПІБ_1, WS_ПІБ_2. У мережі використовуються чотири VLAN:

- **VLAN A** – робоча VLAN (праворуч, на комутаторі SW2);
- **VLAN B** – робоча VLAN (ліворуч, на комутаторі SW1);
- **VLAN C** – робоча VLAN (ліворуч, на комутаторі SW1);
- **VLAN MGMT** – Management VLAN для керування пристроями через SSH (праворуч, на SW2).

Зліва SW_ПІБ_1 з'єднаний з R_ПІБ_1 через **транковий канал** (Router-on-a-Stick – підінтерфейси для VLAN B і VLAN C). Справа SW_ПІБ_2 з'єднаний з R_ПІБ_1 через **два окремі фізичні канали** (Legacy Inter-VLAN Routing – окремі канали для VLAN A та VLAN MGMT).

3. Провести налагодження іменування всіх пристроїв мережі (R_ПІБ_1, SW_ПІБ_1, SW_ПІБ_2).

4. Розробити схему IP-адресації пристроїв мережі. Для цього скористатися даними табл. 3.2 згідно з варіантом. Результати заповнити у табл. 3.1.

Таблиця 3.1.

Параметри адресації мережі

Мережа / Пристрій	Інтерфейс	MAC-адреса	IP-адреса	Маска	Префікс
Підмережа VLAN A	–	–			
Підмережа VLAN B	–	–			
Підмережа VLAN C	–	–			
Підмережа VLAN MGMT	–	–			
Маршрутизатор R1	(Legacy, VLAN A), до SW2				
	(Legacy, VLAN MGMT), до SW2				
	(підінтерфейс, VLAN B), до SW1				
	(підінтерфейс, VLAN C), до SW1				
Комутатор SW1	SVI VLAN B (керування)				
Комутатор SW2	SVI VLAN MGMT				
Робоча станція WS1	NIC		(DHCP)		
Робоча станція WS2	NIC		(DHCP)		

5. На комутаторі SW_ПІБ_1 створити дві робочі VLAN (B, C) згідно з варіантом (табл. 3.3) і налаштувати:

- порти для підключення робочих станцій – у режимі **access** (VLAN B та VLAN C);
- порт для підключення до маршрутизатора R_ПІБ_1 – у режимі **trunk**;
- IP-адресу на інтерфейсі **VLAN B** для доступу через SSH (керування);
- шлюз за замовчуванням (адресу підінтерфейсу **VLAN B**).

6. На комутаторі SW_ПІБ_2 створити дві VLAN (A, MGMT) і налаштувати:

- порти для підключення робочих станцій – у режимі **access** (лише VLAN A);
- два порти для підключення до маршрутизатора R_ПІБ_1 – у режимі **access** (один – для VLAN A, другий – для VLAN MGMT);
- IP-адресу на інтерфейсі **VLAN MGMT**;
- шлюз за замовчуванням.

7. На маршрутизаторі R_ПІБ_1 налаштувати **Inter-VLAN Routing** двома способами:

a) Router-on-a-Stick (для з'єднання з SW_ПІБ_1):

- активувати фізичний інтерфейс (без IP-адреси);
- створити два підінтерфейси – для VLAN B та для VLAN C;
- на кожному підінтерфейсі налаштувати інкапсуляцію **encapsulation dot1q** з відповідним VLAN-ID (один із підінтерфейсів – native згідно з табл. 3.3);

- призначити IP-адресу кожному підінтерфейсу (шлюз за замовчуванням для відповідної VLAN).

б) Legacy Inter-VLAN Routing (для з'єднання з SW_ПІБ_2):

- на двох фізичних інтерфейсах призначити IP-адреси – для VLAN A та для VLAN MGMT (шлюзи відповідних підмереж);
- активувати інтерфейси командою **no shutdown**.

8. На маршрутизаторі R_ПІБ_1 налаштувати **DHCP-сервер** для VLAN A, VLAN B та VLAN C. Для кожної VLAN створити окремий пул адрес **(ip dhcp pool**), вказати мережу, шлюз за замовчуванням, DNS-сервери (8.8.8.8, 8.8.4.4). Виключити з пулів адреси, призначені для статичного використання (шлюзи, комутатори).

9. Налаштувати **віддалений доступ через SSH** до комутаторів SW_ПІБ_1, SW_ПІБ_2 та маршрутизатора R_ПІБ_1 через VLAN MGMT (комутатор SW1 – через VLAN B, оскільки ліворуч виділеної VLAN MGMT немає). Створити користувачів **Admin** (privilege 15) та **User** (privilege 1) з паролем **1111**. Згенерувати RSA-ключі, увімкнути **SSHv2**.

УВАГА! Усі паролі для користувачів та пароль на привілейований режим повинні бути **1111**.

10. Налаштувати робочі станції WS_ПІБ_1 та WS_ПІБ_2 як DHCP-клієнти. Підключити WS_ПІБ_1 до порту VLAN B на SW_ПІБ_1, перевірити отримання IP-адреси; потім перемкнути цей порт у VLAN C і перевірити отримання іншої адреси. Робочу станцію WS_ПІБ_2 підключити до порту VLAN A на SW_ПІБ_2.

11. Перевірити наявність зв'язку між пристроями різних VLAN:

- з WS_ПІБ_1 (VLAN B на SW1) до WS_ПІБ_2 (VLAN A на SW2) – ping через маршрутизатор;
- з WS_ПІБ_1 (VLAN B на SW1) до вузла у VLAN C (на тому ж SW1, через маршрутизатор) – ping;
- з робочої станції до адрес керування комутаторів (SW2 – **VLAN MGMT, SW1 – VLAN B**);
- виконати **tracert** для спостереження маршруту (через R1).

Зафіксувати результати у звіті.

12. Перевірити доступ через **SSH** з робочої станції до комутаторів та маршрутизатора (через **VLAN MGMT, а до SW1 – через VLAN B**).

13. Дослідити таблиці маршрутизації (**show ip route**), таблиці VLAN (**show vlan brief**), стан транкових каналів (**show interfaces trunk**), стан підінтерфейсів (**show ip interface brief**), прив'язки DHCP (**show ip dhcp binding**).

14. Вивести та проаналізувати файли конфігурацій усіх комунікаційних пристроїв мережі (show running-config).

15. Продемонструвати виконану роботу керівнику практики та оформити звіт за заняттям.

ВАРІАНТИ ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Варіант визначається за номером стійки, за якою працюють студенти.

Таблиця 3.2.

Параметри IP-адресації мережі

№ варіанта	IP-адреса VLAN A	IP-адреса VLAN B	IP-адреса VLAN C	IP-адреса VLAN MGMT	Префікс
1	191.C.S.0	192.C.S.0	193.C.S.0	10.C.S.0	/24
2	192.C.S.0	193.C.S.0	194.C.S.0	10.C.S.0	/24
3	193.C.S.0	194.C.S.0	195.C.S.0	10.C.S.0	/24
4	194.C.S.0	195.C.S.0	196.C.S.0	10.C.S.0	/24
5	195.C.S.0	196.C.S.0	197.C.S.0	10.C.S.0	/24
6	196.C.S.0	197.C.S.0	198.C.S.0	10.C.S.0	/24
7	197.C.S.0	198.C.S.0	199.C.S.0	10.C.S.0	/24
8	198.C.S.0	199.C.S.0	200.C.S.0	10.C.S.0	/24
9	199.C.S.0	200.C.S.0	201.C.S.0	10.C.S.0	/24
10	200.C.S.0	201.C.S.0	202.C.S.0	10.C.S.0	/24
11	201.C.S.0	202.C.S.0	203.C.S.0	10.C.S.0	/24
12	202.C.S.0	203.C.S.0	204.C.S.0	10.C.S.0	/24
13	203.C.S.0	204.C.S.0	205.C.S.0	10.C.S.0	/24
14	204.C.S.0	205.C.S.0	206.C.S.0	10.C.S.0	/24
15	205.C.S.0	206.C.S.0	207.C.S.0	10.C.S.0	/24
16	206.C.S.0	207.C.S.0	208.C.S.0	10.C.S.0	/24
17	207.C.S.0	208.C.S.0	209.C.S.0	10.C.S.0	/24
18	208.C.S.0	209.C.S.0	210.C.S.0	10.C.S.0	/24
19	209.C.S.0	210.C.S.0	211.C.S.0	10.C.S.0	/24
20	210.C.S.0	211.C.S.0	212.C.S.0	10.C.S.0	/24

***Примітка*: C** (class) – номер аудиторії: для ауд. **107 – 71**, для ауд. **107a – 72, S** (stand) – номер стійки (зазначено зверху стійки).

УВАГА! В залежності від години проведення практики значення може змінюватись за вимогою керівника.

Таблиця 3.3.

Параметри VLAN та портів комутаторів

№ варіанта	VLAN A	VLAN B	VLAN C	VLAN MGMT	SW1–R (trunk)	Native VLAN
1	10	20	30	100	trunk	B
2	11	21	31	200	trunk + nonegotiate	C
3	12	22	32	300	trunk	B
4	13	23	33	400	trunk + nonegotiate	C
5	14	24	34	500	trunk	B
6	15	25	35	600	trunk	C
7	16	26	36	700	trunk + nonegotiate	B
8	17	27	37	800	trunk	C
9	18	28	38	900	trunk + nonegotiate	B
10	19	29	39	110	trunk	C
11	30	40	50	120	trunk + nonegotiate	B
12	31	41	51	130	trunk	C
13	32	42	52	140	trunk + nonegotiate	B
14	33	43	53	150	trunk	C
15	34	44	54	160	trunk + nonegotiate	B
16	35	45	55	170	trunk	C
17	36	46	56	180	trunk + nonegotiate	B
18	37	47	57	190	trunk	C
19	38	48	58	210	trunk + nonegotiate	B
20	39	49	59	220	trunk	C

ЗМІСТ ЗВІТУ З ЗАНЯТТЯ

Звіт з заняття повинен містити:

1. Номер, тему та мету заняття.
2. Короткі теоретичні відомості (за власним конспектом, обсягом 2–3 сторінки) з таких питань: віртуальні локальні мережі VLAN, способи організації Inter-VLAN Routing (Legacy та Router-on-a-Stick), транковий протокол 802.1Q, підінтерфейси маршрутизатора, Management VLAN, DHCP у мережі з VLAN.
3. Перелік використаного обладнання та програмного забезпечення.
4. Схему (ФОТО) побудованої мережі з позначенням усіх пристроїв (R_ПІБ_1, SW_ПІБ_1, SW_ПІБ_2, WS_ПІБ_1, WS_ПІБ_2) та інтерфейсів.
5. Розроблену схему IP-адресації у вигляді табл. 3.1 з конкретними значеннями.
6. Лістинги команд (або скріншоти) з результатами виконання, а саме:

- створення VLAN та налагодження **access/trunk-портів** на обох комутаторах;
- налагодження підінтерфейсів (Router-on-a-Stick);
- налагодження фізичних інтерфейсів (Legacy Inter-VLAN);
- налагодження **DHCP-серверів** для VLAN A, B та C;
- налагодження **SSH** та **VLAN MGMT**;

- результати **show vlan brief**, **show interfaces trunk**, **show ip interface brief**;
- результати отримання IP-адрес робочими станціями (**ipconfig /all**);
- результати **show ip dhcp binding**;
- результати перевірки зв'язку між VLAN (**ping**, **tracert**);
- результати підключення через **SSH**;
- вміст **running-config** усіх пристроїв.

7. Опис проблем, що виникли під час виконання завдання, та шляхи їх усунення.
8. Висновки по заняттю.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Загальні відомості про VLAN у контексті маршрутизації

VLAN (Virtual Local Area Network) – це логічне сегментування мережі на рівні комутатора, яке дозволяє об'єднувати порти у групи незалежно від фізичного розташування пристроїв. Кожна VLAN функціонує як окремий широкомовний домен: broadcast-трафік однієї VLAN не проникає в іншу. Для ідентифікації кадрів стандарт IEEE 802.1Q додає до Ethernet-кадру 4-байтовий тег з полем VLAN ID (12 біт, діапазон 1–4094). Детальний опис структури VLAN та формату кадру IEEE 802.1Q наведено у теоретичних відомостях заняття № 2.

Способи організації маршрутизації між VLAN (Inter-VLAN Routing)

Оскільки кожна VLAN утворює окремий широкомовний домен з власною IP-підмережею, зв'язок між пристроями різних VLAN вимагає маршрутизації на третьому (мережному) рівні моделі OSI. Комутатор другого рівня ізолює трафік між VLAN на канальному рівні – маршрутизатор або комутатор третього рівня декапсулює кадр IEEE 802.1Q та приймає рішення про пересилання на підставі IP-адреси призначення у таблиці маршрутизації (перевіряється командою **show ip route**). Існують два основних способи організації **Inter-VLAN Routing**.

1. Legacy Inter-VLAN Routing – маршрутизатор підключається до комутатора окремим фізичним каналом для кожної VLAN. Кожен інтерфейс маршрутизатора має IP-адресу відповідної підмережі та виконує роль шлюзу за замовчуванням для пристроїв цієї VLAN. Порти комутатора, до яких підключений маршрутизатор, налаштовуються у режимі access для відповідних VLAN. Оскільки комутатор другого рівня не має таблиці маршрутизації, для управлінського трафіку Management VLAN на ньому задається команда **ip default-gateway**.

Перевага – простота налаштування (кожен інтерфейс маршрутизатора конфігурується як звичайний Ethernet-інтерфейс без спеціальної інкапсуляції). *Недолік* – потреба у великій кількості фізичних інтерфейсів (по одному на кожну VLAN); метод не масштабується при збільшенні кількості VLAN.

Приклад налаштування Legacy для двох VLAN (VLAN 10 і VLAN 20):

Комутатор – порти у режимі access

```
…
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)#exit
Switch(config)# interface fa0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
…
```

Маршрутизатор – окремий інтерфейс на кожну VLAN

```
…
Router(config)# interface fa0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)#exit
Router(config)# interface fa0/1
Router(config-if)# ip address 192.168.20.1 255.255.255.0
Router(config-if)# no shutdown
…
```

2. Router-on-a-Stick Inter-VLAN Routing – маршрутизатор підключається до комутатора одним фізичним каналом у режимі **trunk**. На фізичному інтерфейсі маршрутизатора створюються логічні підінтерфейси – по одному на кожну VLAN. Підінтерфейс переходить у стан up/up лише після активації батьківського фізичного інтерфейсу командою no shutdown – без цього жоден підінтерфейс не працюватиме. Маршрутизатор у цьому режимі не є учасником STP і не впливає на вибір кореневого моста.

Перевага – один фізичний інтерфейс для будь-якої кількості VLAN. *Недолік* – весь міжVLAN-трафік проходить через один trunk-канал, що може стати вузьким місцем при великих обсягах трафіку.

Приклад налаштування Router-on-a-Stick для VLAN 10, 20 та Management VLAN 100:

Комутатор – trunk до маршрутизатора, access до хостів

```
…
Switch(config)# interface fa0/24
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 100
Switch(config-if)#exit
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)#exit
Switch(config)# interface fa0/2
Switch(config-if)# switchport mode access
```

Switch(config-if)# switchport access vlan 20

…

Маршрутизатор – активація фізичного інтерфейсу (обов'язковий перший крок)

…

Router(config)# interface fa0/0
Router(config-if)# no shutdown

…

Підінтерфейс для VLAN 10

…

Router(config)# interface fa0/0.10
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0

…

Підінтерфейс для VLAN 20

…

Router(config)# interface fa0/0.20
Router(config-subif)# encapsulation dot1q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0

…

Підінтерфейс для Native VLAN 100 (Management)

…

Router(config)# interface fa0/0.100
Router(config-subif)# encapsulation dot1q 100 native
Router(config-subif)# ip address 192.168.100.1 255.255.255.0

…

Порівняльну характеристику обох методів наведено у табл. 3.4.

Таблиця 3.4.

Порівняння методів Inter-VLAN Routing

Критерій	Legacy	Router-on-a-Stick
Фізичних інтерфейсів	По одному на VLAN	Один для всіх VLAN
Масштабованість	Низька	Середня
Пропускна здатність	Окремий канал на VLAN	Спільний trunk-канал
Участь у STP	Ні	Ні
Складність налаштування	Нижча	Середня
Рекомендується при	2–3 VLAN	До 8–10 VLAN

Підінтерфейси маршрутизатора

Підінтерфейс (subinterface) – логічний інтерфейс, створений на базі фізичного Ethernet-інтерфейсу маршрутизатора. Кожен підінтерфейс обслуговує трафік конкретної VLAN і має власну IP-адресу – шлюз за замовчуванням для пристроїв цієї VLAN. Після коректного налаштування підінтерфейс відображається у таблиці маршрутизації як запис типу C (**Connected**) – відсутність такого запису є першою ознакою помилки (перевіряється командою **show ip route**).

Синтаксис створення підінтерфейсу:

…
Router(config)# interface *interface-type interface-id.subinterface-id*
…

де ***subinterface-id*** – числовий ідентифікатор підінтерфейсу (рекомендується використовувати номер VLAN для зручності).

Порядок налаштування є обов'язковим: спочатку задається **encapsulation dot1q**, і лише після – **ip address**. Зворотний порядок на деяких версіях IOS повертає помилку.

…
Router(config-subif)# encapsulation dot1q *vlan-id* native
Router(config-subif)# ip address ip-address subnet-mask
…

де ***vlan-id*** – номер VLAN, необов'язковий параметр **native** вказує, що ця VLAN є Native VLAN – її кадри передаються у trunk-каналі без тегу. **Native VLAN** має збігатися між маршрутизатором і комутатором, інакше виникне петля або втрата трафіку.

Стан підінтерфейсів перевіряється командами **show ip interface brief** та **show interfaces *interface-id.subinterface-id***.

DHCP у мережі з VLAN

При використанні маршрутизатора як DHCP-сервера кожна VLAN вимагає окремого DHCP-пулу, оскільки кожна VLAN є окремою IP-підмережею. Команда **ip dhcp excluded-address** задається до створення пулу та виключає адреси, призначені статично – шлюзу, DNS-сервера тощо. Значення **default-router** має збігатися з IP-адресою підінтерфейсу маршрутизатора для даної VLAN.

Приклад налаштування DHCP для VLAN 10 і VLAN 20:

Виключення статичних адрес

…
Router(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10
Router(config)# ip dhcp excluded-address 192.168.20.1 192.168.20.10
…

Пул для VLAN 10

…
Router(config)# ip dhcp pool VLAN10
Router(dhcp-config)# network 192.168.10.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.10.1
Router(dhcp-config)# dns-server 8.8.8.8
…

Пул для VLAN 20

…
Router(config)# ip dhcp pool VLAN20
Router(dhcp-config)# network 192.168.20.0 255.255.255.0
Router(dhcp-config)# default-router 192.168.20.1
Router(dhcp-config)# dns-server 8.8.8.8
…

Діагностика та верифікація

Основні команди діагностики представлені у табл. 3.5.

Таблиця 3.5.

Основні команди діагностики Inter-VLAN Routing

Команда	Призначення
show vlan brief	Список усіх VLAN та портів, що до них належать
show vlan *vlan-id*	Детальна інформація про конкретну VLAN
show interfaces trunk	Стан транкових каналів та дозволені VLAN
show interfaces *interface-id* switchport	Режим порту (access/trunk), VLAN
show ip interface brief	Короткий статус усіх інтерфейсів та IP-адрес
show ip route	Таблиця маршрутизації
show ip dhcp binding	Видані DHCP-адреси
show ip dhcp pool	Параметри DHCP-пулів
show interfaces *interface-id.subinterface-id*	Стан підінтерфейсу
show ip dhcp conflict	Конфлікти DHCP-адрес (дублювання IP)
show interfaces *interface-id* status	Стан інтерфейсу: up/down, швидкість, дуплекс

Рекомендована послідовність перевірки після завершення налаштувань

Для кожної команди показано характерний вивід та пояснення ключових полів.

1. Перевірка VLAN і портів комутатора.

```
Switch# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
10   STUDENTS                         active    Fa0/1
20   TEACHERS                         active    Fa0/2
100  MANAGEMENT                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Усі налаштовані VLAN (10, 20, 100) присутні у таблиці та мають статус **active**. Порти Fa0/1 і Fa0/2 призначені до VLAN 10 і 20 відповідно. VLAN 100 (Management) не має access-портів – це норма, якщо вона використовується лише для управління комутатором. Якщо потрібна VLAN відсутня у списку – вона не була створена командою **vlan vlan-id** або порт не додано до неї.

2. Перевірка trunk-каналу.

```
Switch# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/24      on           802.1q         trunking      100
Port        Vlans allowed on trunk
Fa0/24      1-4094
Port        Vlans allowed and active in management domain
Fa0/24      1,10,20,100
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/24      1,10,20,100
```

Порт Fa0/24 знаходиться у стані **trunking**, інкапсуляція **802.1q**. Native VLAN – 100, що відповідає налаштуванням маршрутизатора. У рядку **Vlans allowed and active** присутні всі три VLAN (10, 20, 100) – це підтверджує, що вони

створені на комутаторі і пропускаються через trunk. Якщо якоїсь VLAN немає у цьому рядку – вона не була створена на комутаторі, навіть якщо налаштована на маршрутизаторі.

3. Перевірка підінтерфейсів маршрутизатора.

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  up                    up
FastEthernet0/0.10     192.168.10.1    YES manual up                    up
FastEthernet0/0.20     192.168.20.1    YES manual up                    up
FastEthernet0/0.100    192.168.100.1   YES manual up                    up
```

Фізичний інтерфейс Fa0/0 – **up/up** без IP-адреси (норма для Router-on-a-Stick). Усі три підінтерфейси – **up/up** з правильними IP-адресами. Якщо підінтерфейс down/down – батьківський інтерфейс Fa0/0 не активований (**no shutdown**). Якщо **up/down** – проблема на канальному рівні: перевірити encapsulation dot1q на підінтерфейсі та режим **trunk** на комутаторі.

4. Перевірка таблиці маршрутизації.

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, ...
Gateway of last resort is not set
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, FastEthernet0/0.10
L       192.168.10.1/32 is directly connected, FastEthernet0/0.10
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, FastEthernet0/0.20
L       192.168.20.1/32 is directly connected, FastEthernet0/0.20
     192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.100.0/24 is directly connected, FastEthernet0/0.100
L       192.168.100.1/32 is directly connected, FastEthernet0/0.100
```

Для кожного підінтерфейсу присутній запис C (Connected) – підмережа безпосередньо підключена. Запис **L** (Local) – адреса самого інтерфейсу маршрутизатора. Наявність усіх трьох записів C підтверджує коректне налаштування Inter-VLAN Routing. Відсутній запис C для якоїсь VLAN означає, що відповідний підінтерфейс не отримав IP-адресу або перебуває у стані **down**.

5. Перевірка DHCP.

```
Router# show ip dhcp pool

Pool VLAN10 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 2
 Pending event                  : none
 1 subnet is currently in the context :
  subnet : 192.168.10.0   mask : 255.255.255.0
   Leased addresses  : 2
   Excluded addresses: 10
   Pending event     : none
Pool VLAN20 :
 Utilization mark (high/low)    : 100 / 0
 Total addresses                : 254
 Leased addresses               : 1
  subnet : 192.168.20.0   mask : 255.255.255.0
   Leased addresses  : 1
   Excluded addresses: 10
```

Поле **Leased addresses** показує кількість виданих адрес у кожному пулі. Якщо **Leased addresses: 0** при наявності активних клієнтів – DHCP-запити не

доходять до маршрутизатора: перевірити **default-router** у пулі та стан підінтерфейсу.

```
Router# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/            Lease expiration        Type
                    Hardware address/
                    User name
192.168.10.11       0100.50ab.cd12.34      Mar 01 2026 09:15 AM    Automatic
192.168.10.12       0100.50ab.cd56.78      Mar 01 2026 09:22 AM    Automatic
192.168.20.11       0100.50ab.ef34.90      Mar 01 2026 09:18 AM    Automatic
```

Таблиця видач: IP-адреса, MAC-адреса клієнта та час закінчення оренди. Порожня таблиця при наявності клієнтів у мережі – DHCP не працює: перевірити **encapsulation dot1q** на підінтерфейсах та відповідність підмереж у пулах.

```
Router# show ip dhcp conflict

IP address        Detection method   Detection time          VRF
192.168.10.15     Gratuitous ARP     Mar 01 2026 08:45 AM
```

Адреса **192.168.10.15** виявлена як конфліктна (два пристрої мають однакову IP). Маршрутизатор автоматично виключає конфліктні адреси з пулу. Для вирішення конфлікту: усунути статичне призначення адреси на клієнті, потім очистити запис командою **clear ip dhcp conflict 192.168.10.15** або **clear ip dhcp conflict ***.

6. Перевірка стану інтерфейсів

```
Router# show interfaces fastEthernet 0/0.10

FastEthernet0/0.10 is up, line protocol is up
  Hardware is Fast Ethernet, address is 0050.ab12.3456
  Internet address is 192.168.10.1/24
  Encapsulation 802.1Q Virtual LAN, Vlan ID  10.
  ARP type: ARPA, ARP Timeout 04:00:00
  ...
  5 minute input rate 1000 bits/sec, 2 packets/sec
  5 minute output rate 500 bits/sec, 1 packets/sec
     1523 packets input, 182760 bytes
     1204 packets output, 144480 bytes
```

Рядок **Encapsulation 802.1Q Virtual LAN, Vlan ID 10** підтверджує правильну інкапсуляцію. Лічильники **packets input/output** показують наявність трафіку – нулі при активних клієнтах вказують на проблему з доставкою кадрів.

```
Switch# show interfaces fastEthernet 0/24 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/24                       connected    trunk        a-full  a-100 10/100BaseTX
```

Статус **connected**, режим **trunk**, швидкість та дуплекс узгоджені автоматично (**a-full, a-100**). Якщо **notconnect** – фізична проблема з кабелем або SFP. Якщо **err-disabled** – спрацював захист (PortFast, BPDU Guard або port security).

Типові помилки при налагодженні Inter-VLAN Routing

1. **Підінтерфейс створено, але не активований батьківський фізичний інтерфейс.** Підінтерфейси (Fa0/0.10, Fa0/0.20, ...) не можуть мати стан up/up, якщо батьківський фізичний інтерфейс (Fa0/0) – у стані shutdown. Помилка часто виникає при копіюванні конфігурації, коли забувають виконати **no shutdown** на фізичному інтерфейсі. Перевіряти командою **show ip interface brief** – фізичний інтерфейс повинен мати стан up/up без призначеної IP-адреси.

2. **Невірний VLAN-ID у команді encapsulation.** Команда **encapsulation dot1q *vlan-id*** на підінтерфейсі задає, для якої VLAN буде маршрутизуватися трафік. Якщо тут вказано неіснуючий або некоректний VLAN-ID – пакети цієї VLAN не маршрутизуватимуться. VLAN-ID повинен збігатися з тим, що налагоджений на комутаторі.

3. **Native VLAN на підінтерфейсі.** За замовчуванням кадри Native VLAN передаються транком БЕЗ тегу. Тому на підінтерфейсі, що відповідає Native VLAN, потрібно додати ключове слово **native** у команді encapsulation: **encapsulation dot1q *vlan-id* native**. Без цього маршрутизатор очікує тегований трафік, а отримує нетегований – і відкидає його. Якщо Native VLAN не використовується для маршрутизації, цю проблему можна обійти, видаливши Native VLAN з allowed-списку транка.

4. **Trunk на комутаторі, але access на маршрутизаторі (або навпаки).** Для Router-on-a-Stick порт комутатора, до якого підключений маршрутизатор, обов'язково повинен бути у режимі **trunk** (не access). Інакше маршрутизатор отримуватиме тільки кадри однієї VLAN, без тегів. Помилка часто проявляється так: одна VLAN маршрутизується, а інші – ні.

5. **Шлюз за замовчуванням не налагоджений на робочих станціях.** Робочі станції повинні мати шлюзом за замовчуванням IP-адресу свого підінтерфейсу маршрутизатора (наприклад, для VLAN 10 з мережею 192.168.10.0/24 – це 192.168.10.1). Якщо шлюз не задано або задано невірно – пакети не виходять за межі підмережі. Перевіряти на робочій станції командою **ipconfig** (Windows) або **ip route show** (Linux).

6. **Невірне налагодження DHCP-relay при централізованому DHCP-сервері.** Якщо DHCP-сервер знаходиться поза підмережею клієнта (наприклад, у management-VLAN), на підінтерфейсі маршрутизатора у клієнтській VLAN потрібно налаштувати **ip helper-address *server-ip*.** Без цього DHCP-широкомовлення не пересилається через маршрутизатор і клієнти не отримують IP-адресу. Якщо клієнти отримують адресу від «чужого» DHCP – перевірити, чи немає у мережі rogue-DHCP-сервера.

7. **Inter-VLAN не працює через помилки subnet-mask на підінтерфейсі.** Якщо на підінтерфейсі задана IP-адреса з іншою маскою, ніж у клієнтів VLAN – пакети до клієнта формально йдуть у іншу підмережу, маршрутизатор не може їх доставити. Усі IP-адреси в одній VLAN (інтерфейс маршрутизатора + клієнти) повинні бути в одній підмережі з однаковою маскою.

8. **При використанні Legacy Inter-VLAN маршрутизатор не має достатньо фізичних інтерфейсів.** Метод Legacy вимагає по одному фізичному інтерфейсу маршрутизатора на кожну VLAN, що маршрутизується. Якщо VLAN більше, ніж інтерфейсів, частина VLAN не маршрутизується. Це і є основна причина переходу на Router-on-a-Stick. Для масштабних мереж (багато VLAN) Legacy-метод не підходить.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке віртуальна локальна мережа (VLAN)? Які основні переваги надає використання VLAN у комутованій мережі?
2. Чому для забезпечення зв'язку між пристроями різних VLAN необхідний маршрутизатор або комутатор третього рівня?
3. Чим відрізняється режим порту access від режиму trunk? Які команди використовуються для налагодження кожного з режимів?
4. Що таке транковий протокол IEEE 802.1Q? Як він забезпечує передачу трафіку декількох VLAN по одному фізичному каналу?
5. Що таке Native VLAN? Чому з міркувань безпеки рекомендується змінювати Native VLAN з VLAN 1 на іншу?
6. Опишіть спосіб Legacy Inter-VLAN Routing. Які його переваги та недоліки?
7. Опишіть спосіб Router-on-a-Stick Inter-VLAN Routing. Які його переваги та недоліки?
8. Що таке підінтерфейс маршрутизатора? Якими командами він створюється та налагоджується?
9. Яке призначення команди encapsulation dot1q vlan-id? На якому рівні моделі OSI вона працює?
10. Що таке Management VLAN? Чому для керування рекомендується виділяти окрему VLAN?
11. Як налаштувати IP-адресу для керування на комутаторі Cisco за допомогою інтерфейсу Management VLAN?
12. Як налаштувати DHCP-сервер на маршрутизаторі Cisco для декількох VLAN? Чому для кожної VLAN створюється окремий пул?
13. Якими командами show можна перевірити стан VLAN, транкових каналів та підінтерфейсів?
14. Що відбувається з кадром Ethernet при його переході через транковий канал 802.1Q? Як маршрутизатор визначає, до якої VLAN належить кадр?
15. Як забезпечити доступ через SSH до комутатора лише через Management VLAN?
16. Як організувати керування комутатором, на якому немає виділеної Management VLAN (наприклад, лівим комутатором у схемі Router-on-a-Stick)? Через яку VLAN у цьому випадку призначають IP-адресу керування?
17. Чому при використанні Legacy Inter-VLAN Routing для двох VLAN (наприклад, VLAN A та VLAN MGMT) на маршрутизаторі потрібні два окремі фізичні (routed) інтерфейси? Чим це відрізняється від Router-on-a-Stick?

ЗАНЯТТЯ № 4

ДОСЛІДЖЕННЯ ТА НАЛАГОДЖЕННЯ МАРШРУТИЗАЦІЇ МІЖ ВІРТУАЛЬНИМИ ЛОКАЛЬНИМИ МЕРЕЖАМИ НА БАЗІ БАГАТОРІВНЕВИХ (L3) КОМУТАТОРІВ CISCO

Мета заняття: ознайомитися з принципами організації маршрутизації між віртуальними локальними мережами (Inter-VLAN Routing) на базі багаторівневих комутаторів (Layer 3 Switches); розглянути використання інтерфейсів SVI (Switch Virtual Interface) та маршрутизованих портів (routed port); отримати практичні навички налагодження SVI, транкових каналів, маршрутизованих портів та агента ретрансляції DHCP (ip helper-address); засвоїти принципи взаємодії L3-комутатора із зовнішнім DHCP-сервером через механізм DHCP relay.

Обладнання та програмне забезпечення

Для виконання заняття на робочому місці студента має бути наявним таке обладнання та програмне забезпечення:

1. Маршрутизатор Cisco серії 1841/2801/2811/2821/2901/2911/2921 – 1 шт.
2. Багаторівневий комутатор Cisco серії Catalyst 3560/3650/3750/3850 (з підтримкою ip routing та SVI) – 1 шт.
3. Керований комутатор Cisco серії Catalyst 2960 (моделі WS-C2960-24TT-L або WS-C2960-48TT-L) – 2 шт.
4. Робочі станції (ПК або ноутбуки) з операційною системою Windows/Linux – не менше 2 шт.
5. Консольний кабель Cisco (rollover) з конектором RJ-45 та перехідником на USB або COM-порт – 1 шт.
6. Ethernet-кабелі прямого типу (T568B) категорії Cat 5e/Cat 6 – не менше 5 шт.
7. Термінальна програма-емулятор (PuTTY, Tera Term, SecureCRT або аналогічна) – встановлена на робочих станціях.

Схема підключення

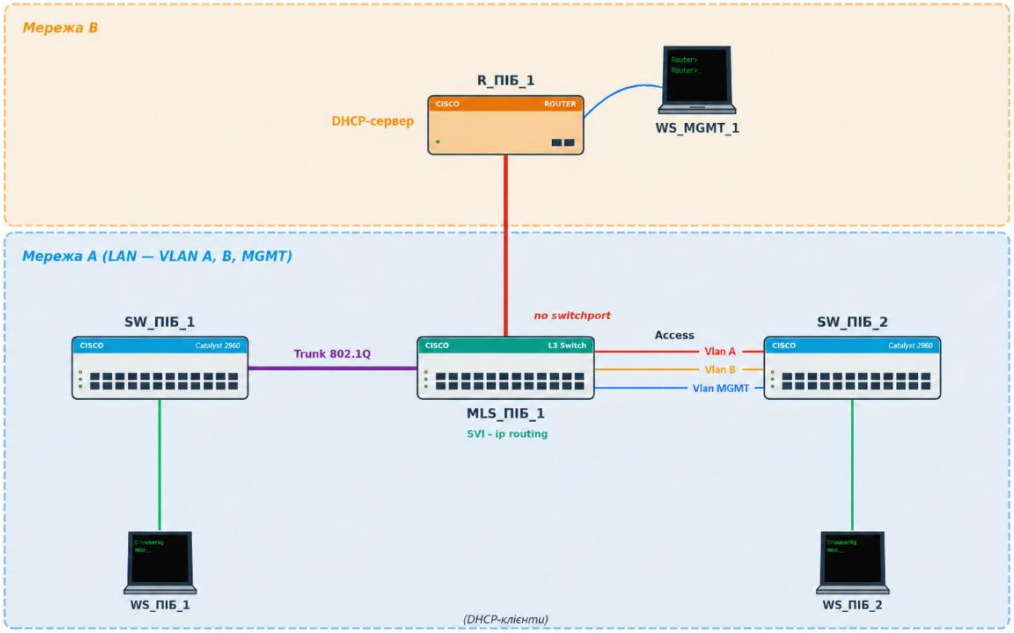

Рис. 4.1. Схема мережі, що будується у межах заняття

Примітка: ПІБ необхідно зазначати у скороченому форматі, який відповідає логіну для входу на платформу learn. Приклад: якщо логін для входу на learn – kb1_kmd, то назва комутатора має бути у форматі SW_kmd_1.

ЗАВДАННЯ

1. Ознайомитися з обладнанням та програмним забезпеченням робочого місця, перевірити наявність консольного та Ethernet-кабелів, термінальної програми. Визначити модель багаторівневого комутатора, переконатися у підтримці **ip routing**.

2. Створити мережу відповідно до схеми на рис. 4.1. Мережа складається з маршрутизатора R_ПІБ_1, багаторівневого комутатора MLS_ПІБ_1 (L3 Switch) та двох комутаторів SW_ПІБ_1 та SW_ПІБ_2 і двох робочих станцій WS_ПІБ_1, WS_ПІБ_2. У мережі використовуються три VLAN:

- **VLAN A** – робоча VLAN для першої групи пристроїв;
- **VLAN B** – робоча VLAN для другої групи пристроїв;
- **VLAN MGMT** – Management VLAN для керування пристроями через SSH.

Зліва MLS_ПІБ_1 з'єднаний з SW_ПІБ_1 через **транковий канал**. Справа MLS_ПІБ_1 з'єднаний з SW_ПІБ_2 через **три окремі фізичні канали**. R_ПІБ_1 – підключеного до багаторівневого комутатора MLS_ПІБ_1 через маршрутизований порт (Мережа B).

3. Провести налагодження іменування всіх пристроїв мережі (R_ПІБ_1, MLS_ПІБ_1, SW_ПІБ_1 та SW_ПІБ_2).

4. Розробити схему IP-адресації пристроїв мережі. Для цього скористатися даними табл. 4.2. Результати занести у табл. 4.1.

Таблиця 4.1.

Параметри адресації мережі

Мережа / Пристрій	Інтерфейс	MAC-адреса	IP-адреса	Маска	Префікс
Підмережа VLAN A	–	–			
Підмережа VLAN B	–	–			
Підмережа VLAN MGMT	–	–			
Підмережа B (R1–MLS1)	–				
Маршрутизатор R1					
MLS1	routed port (до R1)				
MLS1	SVI VLAN A				
MLS1	SVI VLAN B				
MLS1	SVI VLAN MGMT				
Комутатор SW1	Vlan MGMT				
Комутатор SW2	Vlan MGMT				
Робоча станція WS1	NIC		(DHCP)		
Робоча станція WS2	NIC		(DHCP)		

5. На багаторівневому комутаторі MLS_ПІБ_1 створити три VLAN (10, 20, 99) згідно з варіантом (табл. 4.3) та налаштувати:

- увімкнути маршрутизацію командою ip routing.
- порт для підключення до SW_ПІБ_1 у режимі trunk з дозволеними VLAN A, B, MGMT (**switchport trunk encapsulation dot1q** перед **switchport mode trunk**);
- SVI для кожної VLAN (interface vlan A, interface vlan B, interface vlan MGMT) з IP-адресами що будуть шлюзами за замовчуванням для

пристроїв відповідних VLAN;

6. На порту MLS_ПІБ_1, що підключений до маршрутизатора R_ПІБ_1, налаштувати маршрутизований порт командою **no switchport** (перетворити L2-порт на L3-порт) та призначити IP-адресу підмережі B (відповідно до варіанту);

7. На комутаторі SW_ПІБ_1 створити три VLAN (A, B, MGMT) та налаштувати:

- порти для підключення робочих станцій у режимі **access** для VLAN A та VLAN B (за варіантом);
- порт для підключення до MLS_ПІБ_1 у режимі **trunk** з дозволеними VLAN A, B, MGMT;
- IP-адресу на інтерфейсі VLAN MGMT та шлюз за замовчуванням.

8. На комутаторі SW_ПІБ_2 створити три VLAN (A, B, MGMT) та налаштувати:

- порти для підключення робочих станцій у режимі **access** для VLAN A та VLAN B (за варіантом);
- три порти для підключення до MLS_ПІБ_1 у режимі **access** (по одному порту на кожну VLAN – аналогічно **Legacy Inter-VLAN Routing** з заняття № 3);
- IP-адресу на інтерфейсі VLAN MGMT та шлюз за замовчуванням (адресу SVI VLAN MGMT на MLS_ПІБ_1).

9. На маршрутизаторі R_ПІБ_1 налаштувати IP-адресу на інтерфейсі до MLS_ПІБ_1 (підмережа B, відповідно до варіанту) та активувати інтерфейс командою no shutdown.

10. На маршрутизаторі R_ПІБ_1 налаштувати DHCP-сервер для VLAN A та VLAN B. Для кожної VLAN створити окремий пул адрес (**ip dhcp pool**), вказати мережу, шлюз за замовчуванням (адресу SVI відповідної VLAN на MLS_ПІБ_1), DNS-сервери (8.8.8.8, 8.8.4.4). Виключити з пулів адреси SVI та інші статичні адреси. На MLS_ПІБ_1 налаштувати **ip helper-address** на SVI VLAN A та VLAN B (вказати IP-адресу R_ПІБ_1 з підмережі B) для перенаправлення DHCP-запитів.

11. Налаштувати маршрутизацію за замовчуванням

- На MLS_ПІБ_1 додати маршрут за замовчуванням (ip route 0.0.0.0 0.0.0.0 адреса R_ПІБ_1 у підмережі B), що вказує на R_ПІБ_1 як шлюз для досягнення зовнішніх мереж;
- На R_ПІБ_1 додати статичні маршрути до підмереж VLAN A, VLAN B та VLAN MGMT (**ip route** ***network mask*** адреса **routed port** MLS_ПІБ_1 у підмережі B). Без цих маршрутів DHCP **relay** не працюватиме, а відповіді на **ping** до WS не повернуться.

12. Налаштувати віддалений доступ через SSH до MLS_ПІБ_1, SW_ПІБ_1, SW_ПІБ_2 та R_ПІБ_1 через VLAN MGMT. Створити користувачів **Admin** (privilege 15) та **User** (privilege 1) з паролем **1111**. Згенерувати RSA-ключі розміром **2048** біт, увімкнути **SSHv2**. Усі паролі – **1111**.

13. Налаштувати робочі станції WS_ПІБ_1 та WS_ПІБ_2 як DHCP-клієнти. Підключити до портів різних VLAN на SW_ПІБ_1 та SW_ПІБ_2. Перевірити отримання IP-адрес.

14. Перевірити наявність зв'язку між усіма пристроями мережі:

- WS_ПІБ_1 (VLAN A) до WS_ПІБ_2 (VLAN B) – **ping** через MLS_ПІБ_1;
- WS_ПІБ_1 до R_ПІБ_1 – **ping** через MLS_ПІБ_1 та мережу B;
- R_ПІБ_1 до SVI VLAN A, B, MGMT на MLS_ПІБ_1;
- робочих станцій до Management-адрес комутаторів (VLAN MGMT);
- виконати **tracert** для спостереження маршруту.

15. Дослідити таблиці маршрутизації (**show ip route** на R_ПІБ_1 та MLS_ПІБ_1), стан SVI (**show ip interface brief**), таблиці VLAN (**show vlan brief**), стан транкових каналів (**show interfaces trunk**), прив'язки DHCP (**show ip dhcp binding** на R_ПІБ_1).

16. Вивести та проаналізувати файли конфігурацій усіх комунікаційних пристроїв мережі.

17. Продемонструвати виконану роботу керівнику практики та оформити звіт за заняттям.

ВАРІАНТИ ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Варіант визначається за номером стійки, за якою працюють студенти.

Таблиця 4.2.

Параметри IP-адресації мережі

№ варіанта	IP-адреса VLAN A	IP-адреса VLAN B	IP-адреса VLAN MGMT	Префікс підмережі A	IP-адреса підмережі B	Префікс підмережі B
1	191.C.S.0	192.C.S.0	10.C.S.0	/24	172.C.S.0	/30
2	192.C.S.0	193.C.S.0	10.C.S.0	/24	172.C.S.4	/30
3	193.C.S.0	194.C.S.0	10.C.S.0	/24	172.C.S.8	/30
4	194.C.S.0	195.C.S.0	10.C.S.0	/24	172.C.S.12	/30
5	195.C.S.0	196.C.S.0	10.C.S.0	/24	172.C.S.16	/30
6	196.C.S.0	197.C.S.0	10.C.S.0	/24	172.C.S.20	/30
7	197.C.S.0	198.C.S.0	10.C.S.0	/24	172.C.S.24	/30
8	198.C.S.0	199.C.S.0	10.C.S.0	/24	172.C.S.28	/30
9	199.C.S.0	200.C.S.0	10.C.S.0	/24	172.C.S.32	/30
10	200.C.S.0	201.C.S.0	10.C.S.0	/24	172.C.S.36	/30
11	201.C.S.0	202.C.S.0	10.C.S.0	/24	172.C.S.40	/30
12	202.C.S.0	203.C.S.0	10.C.S.0	/24	172.C.S.44	/30
13	203.C.S.0	204.C.S.0	10.C.S.0	/24	172.C.S.48	/30
14	204.C.S.0	205.C.S.0	10.C.S.0	/24	172.C.S.52	/30
15	205.C.S.0	206.C.S.0	10.C.S.0	/24	172.C.S.56	/30
16	206.C.S.0	207.C.S.0	10.C.S.0	/24	172.C.S.60	/30
17	207.C.S.0	208.C.S.0	10.C.S.0	/24	172.C.S.64	/30
18	208.C.S.0	209.C.S.0	10.C.S.0	/24	172.C.S.68	/30
19	209.C.S.0	210.C.S.0	10.C.S.0	/24	172.C.S.72	/30
20	210.C.S.0	211.C.S.0	10.C.S.0	/24	172.C.S.76	/30

***Примітка*: C** (class) – номер аудиторії: для ауд. **107 – 71**, для ауд. **107a – 72, S** (stand) – номер стійки (зазначено зверху стійки).

УВАГА! В залежності від години проведення практики значення може змінюватись за вимогою керівника.

Таблиця 4.3.

Параметри VLAN та портів комутаторів

№ варіанта	VLAN A	VLAN B	VLAN MGMT	SW1–MLS (trunk)	Native VLAN
1	10	20	100	trunk/on	A
2	11	21	200	dynamic desirable	B
3	12	22	300	trunk/on	A
4	13	23	400	dynamic desirable	B
5	14	24	500	trunk/on	A
6	15	25	600	trunk/on	B
7	16	26	700	dynamic desirable	A
8	17	27	800	trunk/on	B
9	18	28	900	dynamic desirable	A
10	19	29	110	trunk/on	B
11	30	40	120	dynamic desirable	A
12	31	41	130	trunk/on	B
13	32	42	140	dynamic desirable	A
14	33	43	150	trunk/on	B
15	34	44	160	dynamic desirable	A
16	35	45	170	trunk/on	B
17	36	46	180	dynamic desirable	A
18	37	47	190	trunk/on	B
19	38	48	210	dynamic desirable	A
20	39	49	220	trunk/on	B

ЗМІСТ ЗВІТУ З ЗАНЯТТЯ

Звіт з заняття повинен містити:

1. Номер, тему та мету заняття.

2. Короткі теоретичні відомості (за власним конспектом, обсягом 2-3 сторінки) з таких питань: багаторівневі комутатори (L3 Switches), інтерфейси SVI, маршрутизовані порти (no switchport), ip routing, DHCP relay (ip helper-address), маршрутизація за замовчуванням, порівняння SVI з Router-on-a-Stick.

3. Перелік використаного обладнання та програмного забезпечення.

4. Схему (ФОТО) побудованої мережі з позначенням усіх пристроїв та інтерфейсів.

5. Розроблену схему IP-адресації у вигляді табл. 4.1 з конкретними значеннями.

6. Лістинги команд (або скріншоти) з результатами виконання, а саме:

- створення VLAN та налагодження **access/trunk**-портів на MLS_ПІБ_1, SW_ПІБ_1 та SW_ПІБ_2;
- налагодження SVI на MLS_ПІБ_1 (interface vlan A, B, MGMT з IP-адресами);

- налагодження маршрутизованого порту (**no switchport**) на MLS_ПІБ_1;
- увімкнення **ip routing** на MLS_ПІБ_1;
- налагодження IP-адреси на R_ПІБ_1;
- налагодження DHCP-серверів на R_ПІБ_1 та **ip helper-address** на MLS_ПІБ_1;
- налагодження статичних маршрутів на R_ПІБ_1 та маршруту за замовчуванням на MLS_ПІБ_1;
- налагодження SSH;
- результати **show vlan brief**, **show interfaces trunk**, **show ip interface brief**, **show ip route** (на обох L3-пристроях);
- результати **show ip dhcp binding** на R_ПІБ_1;
- результати **ipconfig /all** на робочих станціях;
- результати **ping** та **tracert** між пристроями різних VLAN та мережі B;
- результати підключення по SSH;
- вміст **running-config** усіх пристроїв.

7. Опис проблем, що виникли під час виконання завдання, та шляхи їх усунення.

8. Висновки по заняттю.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Детальний опис віртуальних локальних мереж (**VLAN**), транкового протоколу **IEEE 802.1Q**, режимів портів **access** та **trunk** наведено у теоретичних відомостях заняття 2. Основи маршрутизації між VLAN (**Legacy та Router-on-a-Stick**) розглянуті у занятті 3. У цьому розділі описується сучасний метод **Inter-VLAN Routing** на базі багаторівневих комутаторів (**Layer 3 Switches**).

Багаторівневі комутатори (Layer 3 Switches)

Багаторівневий комутатор (Layer 3 Switch, MLS – Multilayer Switch) – мережний пристрій, що поєднує функції комутатора другого рівня та маршрутизатора третього рівня моделі OSI. На відміну від звичайного комутатора L2 (наприклад, Catalyst 2960), багаторівневий комутатор (наприклад, Catalyst 3560, 3650, 3750, 3850) здатний виконувати маршрутизацію IP-пакетів між VLAN апаратно, без пересилання трафіку на зовнішній маршрутизатор.

Переваги використання L3 Switch для Inter-VLAN Routing порівняно з Router-on-a-Stick:

- значно вища швидкість маршрутизації (апаратна комутація замість програмної на маршрутизаторі);
- відсутність вузького місця у вигляді одного транкового каналу до маршрутизатора;
- менша затримка (latency), оскільки перенаправлення пакетів відбувається всередині комутатора;
- спрощення топології – не потрібен зовнішній маршрутизатор для Inter-VLAN Routing.

Інтерфейси SVI (Switch Virtual Interface)

SVI (Switch Virtual Interface) – віртуальний інтерфейс третього рівня, створений на багаторівневому комутаторі для конкретної VLAN. SVI виконує ті ж функції, що й підінтерфейс маршрутизатора або фізичний інтерфейс маршрутизатора: він має IP-адресу, є шлюзом за замовчуванням для пристроїв VLAN і забезпечує маршрутизацію пакетів між VLAN.

Важливо розуміти різницю між SVI на комутаторі другого рівня та на багаторівневому комутаторі. На Catalyst 2960 (L2) **SVI** існує виключно для цілей управління: він має IP-адресу, але не виконує маршрутизацію між VLAN – пакети між різними VLAN через SVI на L2 комутаторі не передаються. На Catalyst 3560/3750 (L3) SVI виконує повноцінну маршрутизацію між VLAN після активації команди **ip routing**: кожен SVI є повноцінним L3-інтерфейсом, аналогічним підінтерфейсу маршрутизатора у **Router-on-a-Stick**.

За замовчуванням на комутаторах Cisco створюється SVI для VLAN 1 (для віддаленого керування). Додаткові SVI необхідно створювати вручну. SVI створюється при першому виконанні команди **interface vlan *vlan-id***.

Умови для переходу SVI у стан **up/up**:

- відповідна VLAN повинна існувати в базі даних VLAN комутатора;
- щонайменше один порт, що належить до цієї VLAN, повинен бути у стані **up**;
- на SVI повинна бути призначена IP-адреса;
- SVI не повинен бути вимкнений командою **shutdown**.

Приклад налаштування SVI:

```
…
MLS(config)# vlan 10
MLS(config-vlan)# name SALES
MLS(config-vlan)# exit
MLS(config)# interface vlan 10
MLS(config-if)# ip address 191.168.1.1 255.255.255.0
MLS(config-if)# no shutdown
…
```

Після створення SVI для всіх потрібних VLAN необхідно увімкнути маршрутизацію **ip routing**.

Команда ip routing

Команда **ip routing** вмикає функцію маршрутизації IP-пакетів між інтерфейсами (**SVI** та **routed port**) безпосередньо на комутаторі. За замовчуванням ця функція відключена навіть на L3 Switch – без неї комутатор передає кадри лише на канальному рівні (як звичайний L2 switch), а IP-адреси SVI використовуються лише для управлінського доступу.

Після виконання цієї команди комутатор починає будувати таблицю маршрутизації (перевіряється командою **show ip route**) і пересилати пакети між підмережами VLAN апаратно через ASIC. Саме апаратна маршрутизація є ключовою перевагою L3 Switch перед **Router-on-a-Stick**, де маршрутизація виконується програмно на CPU маршрутизатора.

Якщо команда **ip routing** не виконана – SVI матимуть IP-адреси, але пінг

між пристроями різних VLAN буде недоступний, а **show ip route** відобразить лише локальні (L) записи без записів типу C (**Connected**) для підмереж VLAN.

Маршрутизовані порти (Routed Ports)

Маршрутизований порт – фізичний порт багаторівневого комутатора, який працює як інтерфейс маршрутизатора (Layer 3 port). На відміну від звичайного порту доступу або транкового порту, маршрутизований порт не належить до жодної VLAN і не бере участі у протоколі **STP**. Він функціонує як звичайний інтерфейс маршрутизатора з IP-адресою.

Для налаштування маршрутизованого порту використовується команда **no switchport**, яка вимикає функціональність другого рівня на цьому порті.

Приклад налаштування Routed Ports:

```
…
MLS(config)# interface GigabitEthernet 1/0/24
MLS(config-if)# no switchport
MLS(config-if)# ip address 172.168.1.2 255.255.255.252
MLS(config-if)# no shutdown
…
```

Для перевірки того, що порт дійсно перейшов у режим **routed port**, використовується команда **show interfaces *interface-id* switchport**. У виводі рядок **Switchport: Disabled** підтверджує, що L2-функціональність відключена і порт працює як L3-інтерфейс:

```
MLS# show interfaces GigabitEthernet1/0/24 switchport
Name: Gi1/0/24
Switchport: Disabled
```

Якщо рядок виводить **Switchport: Enabled** – команда **no switchport** не була виконана або не збереглась у конфігурації.

Після виконання команди **no switchport** порт втрачає можливість належати до VLAN, працювати у режимі **access** або **trunk**. Натомість він отримує можливість мати IP-адресу і бере участь у маршрутизації.

Порівняння SVI та Router-on-a-Stick

Таблиця 4.4.

Порівняння способів Inter-VLAN Routing

Характеристика	Legacy (Заняття 3)	Router-on-a-Stick (Заняття 3)	L3 Switch з SVI (Заняття 4)
Пристрій маршрутизації	Зовнішній маршрутизатор	Зовнішній маршрутизатор	Багаторівневий комутатор
Тип з'єднання	По одному на VLAN	Один trunk-канал	Внутрішньо (SVI)
Швидкість маршрутизації	Програмна (CPU маршрутизатора)	Програмна (CPU маршрутизатора)	Апаратна (ASIC комутатора)
Масштабованість	Низька	Середня	Висока
Затримка	Висока	Середня	Мінімальна
Участь у STP	Ні	Ні	Так (SVI – ні, але порти – так)
Вартість обладнання	Нижча	Нижча	Вища (L3 switch)
Типове застосування	2–3 VLAN, навчальне середовище	До 8–10 VLAN	Середні та великі мережі

DHCP relay (ip helper-address)

Коли DHCP-сервер розташований не на тому ж пристрої, що виконує маршрутизацію між VLAN, а на зовнішньому маршрутизаторі (як у цьому занятті – DHCP-сервер на Router), широкомовні DHCP-запити клієнтів (**DHCP DISCOVER**) не виходять за межі своєї **VLAN**. Для вирішення цієї проблеми на **SVI** багаторівневого комутатора налагоджується команда **ip helper-address**, яка перетворює широкомовні DHCP-запити у спрямовані (**unicast**) і пересилає їх на IP-адресу DHCP-сервера.

Приклад налаштування ip helper-address:

```
…
MLS(config)# interface vlan 10
MLS(config-if)# ip helper-address 172.168.1.1
MLS(config-if)#exit
MLS(config)# interface vlan 20
MLS(config-if)# ip helper-address 172.168.1.1
…
```

де **172.168.1.1** – IP-адреса маршрутизатора Router у мережі B.

Статична маршрутизація та маршрут за замовчуванням

Для забезпечення повної зв'язності між усіма пристроями мережі необхідно налаштувати статичні маршрути на двох пристроях.

На MLS – маршрут за замовчуванням, що вказує на Router як шлюз для досягнення мереж поза VLAN:

```
…
MLS(config)# ip route 0.0.0.0 0.0.0.0 172.168.1.1
…
```

де 172.168.2.1 – IP-адреса інтерфейсу Router у мережі B.

На Router – статичні маршрути до кожної підмережі VLAN через MLS:

```
…
R(config)# ip route 191.168.1.0 255.255.255.0 172.168.1.2
R(config)# ip route 192.168.1.0 255.255.255.0 172.168.1.2
R(config)# ip route 10.168.1.0 255.255.255.0 172.168.1.2
…
```

де 172.168.1.2 – IP-адреса routed port на MLS у мережі B.

Без цих маршрутів пакети від Router до WS у VLAN не матимуть зворотного шляху – **DHCP relay** працюватиме (запит дійде до Router), але відповідь **DHCP OFFER** не повернеться до клієнта.

Команди моніторингу та діагностики

Таблиця 4.5.

Основні команди діагностики Inter-VLAN Routing на L3 Switch

Команда	Призначення
show ip route	Таблиця маршрутизації L3 Switch
show ip interface brief	Короткий статус усіх L3-інтерфейсів (SVI та routed ports)
show vlan brief	Список VLAN та портів
show interfaces trunk	Стан транкових каналів
show interfaces *interface-id* switchport	Режим порту (access/trunk/routed)
show ip dhcp binding	Видані DHCP-адреси
show running-config interface vlan *vlan-id*	Конфігурація SVI
show running-config interface *interface-id*	Конфігурація маршрутизованого порту

Рекомендована послідовність перевірки після завершення налаштування

1. Перевірка стану SVI та routed port.

```
MLS# show ip interface brief

Interface              IP-Address      OK? Method Status    Protocol
GigabitEthernet1/0/24  172.168.1.2      YES manual up        up
Vlan10                 191.168.1.1      YES manual up        up
Vlan20                 192.168.1.1      YES manual up        up
Vlan99                 10.168.1.1       YES manual up        up
```

Порт Gi1/0/24 – **routed port** з IP-адресою. SVI VLAN 10, 20, 99 у стані **up/up** – маршрутизація між VLAN активна. Якщо SVI у стані **down/down** – або VLAN не створена, або немає жодного активного порту в цій VLAN. Якщо **up/down** – SVI вимкнений командою shutdown.

2. Перевірка таблиці маршрутизації на MLS.

```
MLS# show ip route

Codes: C - connected, S - static, L - local

Gateway of last resort is 172.168.1.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.168.1.1
      172.168.1.0/30 is variably subnetted, 2 subnets, 2 masks
C       172.168.1.0/30 is directly connected, GigabitEthernet1/0/24
L       172.168.1.2/32 is directly connected, GigabitEthernet1/0/24
      191.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       191.168.1.0/24 is directly connected, Vlan10
L       191.168.1.1/32 is directly connected, Vlan10
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Vlan20
L       192.168.1.1/32 is directly connected, Vlan20
```

Запис **S* 0.0.0.0/0** – маршрут за замовчуванням до Router. Записи C – підмережі VLAN та підмережа B, безпосередньо підключені. Відсутність **S*** означає, що маршрут за замовчуванням не налаштований – пінг за межі підмереж VLAN не пройде.

3. Перевірка таблиці маршрутизації на Router.

```
Router# show ip route

Gateway of last resort is not set

      172.168.1.0/30 is variably subnetted, 2 subnets, 2 masks
```

```
C       172.168.1.0/30 is directly connected, FastEthernet0/0
L       172.168.1.1/32 is directly connected, FastEthernet0/0
S       191.168.1.0/24 [1/0] via 172.168.1.2
S       192.168.1.0/24 [1/0] via 172.168.1.2
S       10.168.1.0/24  [1/0] via 172.168.1.2
```

Записи **S** – статичні маршрути до підмереж VLAN через MLS. Відсутність статичних маршрутів на Router – найпоширеніша причина того, що **ping** від Router до WS доходить, але відповідь не повертається (**Request timed out**).

4. Перевірка **DHCP relay**.

```
MLS# show running-config interface vlan 10

interface Vlan10
 ip address 191.168.1.1 255.255.255.0
 ip helper-address 172.168.1.1
 no shutdown
```

Рядок ip helper-address 172.168.1.1 підтверджує, що DHCP-запити з VLAN 10 перенаправляються на Router. Якщо цей рядок відсутній – клієнти VLAN 10 не отримають IP-адресу від DHCP-сервера на R_ПІБ_1, навіть якщо маршрутизація між VLAN налаштована правильно.

```
Router# show ip dhcp binding

IP address       Client-ID/Hardware address   Lease expiration    Type
191.168.1.11      0100.50ab.cd12.34            Apr 30 2026 10:00   Automatic
192.168.1.11      0100.50ab.ef56.78            Apr 30 2026 10:05   Automatic
```

Адреси з різних підмереж VLAN (191.168.x і 192.168.x) у таблиці видач підтверджують коректну роботу **DHCP relay**. Якщо таблиця порожня при активних клієнтах – перевірити **ip helper-address** на SVI та статичні маршрути на Router.

Типові помилки при налаштуванні Inter-VLAN на L3 Switch

1. Не увімкнена маршрутизація. Без команди **ip routing** багаторівневий комутатор працює як звичайний L2 switch – SVI мають IP-адреси для керування, але маршрутизація між VLAN не виконується.

2. VLAN не існує. Якщо VLAN не створена командою **vlan vlan-id**, SVI для неї залишиться у стані **down**.

3. Немає активних портів у VLAN. SVI не перейде у стан **up**, якщо жоден порт, що належить до цієї VLAN, не знаходиться у стані **up**.

4. **Switchport trunk encapsulation**. На комутаторах Catalyst 3560/3750 перед **switchport mode trunk** необхідно виконати **switchport trunk encapsulation dot1q** – інакше **trunk** не активується. Причина: ці моделі підтримують два протоколи тегування – **dot1q** та застарілий **ISL** (Inter-Switch Link), тому тип інкапсуляції необхідно вказати явно. Детальний опис **ISL** та відмінностей від **dot1q** наведено у теоретичних відомостях заняття № 2. На Catalyst 2960 ця команда не потрібна, оскільки 2960 підтримує виключно dot1q.

5. Відсутність **ip helper-address**. Якщо DHCP-сервер розташований на іншому пристрої – без **ip helper-address** клієнти не отримають адреси.

6. Відсутність зворотних маршрутів. Якщо на маршрутизаторі не додані маршрути до підмереж VLAN – відповіді на **ping** не повертаються (**Request timed out**).

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке багаторівневий комутатор (Layer 3 Switch)? Чим він відрізняється від звичайного комутатора L2?
2. Що таке інтерфейс SVI (Switch Virtual Interface)? Яке його призначення?
3. Які умови необхідні для переходу SVI у стан up/up?
4. Якою командою увімкнути маршрутизацію на багаторівневому комутаторі Cisco?
5. Що таке маршрутизований порт (routed port)? Якою командою він створюється?
6. Чим маршрутизований порт відрізняється від порту доступу (access) та транкового порту (trunk)?
7. Порівняйте способи Inter-VLAN Routing: Router-on-a-Stick (заняття 3) та L3 Switch з SVI (заняття 4). Які переваги та недоліки кожного?
8. Для чого потрібна команда switchport trunk encapsulation dot1q на L3 Switch? Чому вона не потрібна на комутаторах Catalyst 2960?
9. Що таке DHCP relay? Для чого використовується команда ip helper-address?
10. Чому на SVI кожної VLAN необхідно налагоджувати ip helper-address, якщо DHCP-сервер знаходиться на зовнішньому маршрутизаторі?
11. Як налаштувати маршрутизацію за замовчуванням на L3 Switch? Якою командою?
12. Чому на маршрутизаторі необхідно додавати статичні маршрути до підмереж VLAN?
13. Якими командами show можна перевірити стан SVI, маршрутизацію та VLAN на L3 Switch?
14. Що відбувається, якщо на L3 Switch не виконати команду ip routing, але створити SVI з IP-адресами?
15. Як перевірити, що порт комутатора працює як маршрутизований (routed), а не як L2-порт?

ЗАНЯТТЯ № 5

ДОСЛІДЖЕННЯ ТА НАЛАГОДЖЕННЯ ПРОТОКОЛІВ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ RIPv2 ТА OSPFv2 І РЕДИСТРИБУЦІЇ МАРШРУТІВ У МЕРЕЖІ НА БАЗІ МАРШРУТИЗАТОРІВ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження протоколів динамічної маршрутизації RIPv2 і OSPFv2 на обладнанні Cisco; отримати практичні навички розрахунку метрик і визначення оптимальних маршрутів обох протоколів; ознайомитися з принципами однонаправленої та двосторонньої редистрибуції (перерозподілу) маршрутів між RIPv2 та OSPF; отримати практичні навички налагодження, моніторингу та діагностування роботи комбінованої мережі з двома доменами маршрутизації; налаштувати DHCP-сервер з ретрансляцією запитів (DHCP relay) для робочих станцій з обох доменів; дослідити процеси формування таблиць маршрутизації та порівняти метрики RIP і OSPF на спільному маршруті.

Обладнання та програмне забезпечення

Для виконання заняття на робочому місці студента має бути наявним таке обладнання та програмне забезпечення:

1. Маршрутизатори Cisco серії 1841/2801/2811/2821/2901/2911/2921 з інтерфейсними слотами для плат розширення – 3 шт.
2. Плати розширення Cisco WIC-2T (або аналогічні) для послідовних з'єднань – 2–4 шт. (за варіантом).
3. Плата розширення з оптичним інтерфейсом (HWIC-1GE-SFP, GLC-LH-SMD або аналогічна, для варіантів з оптичним каналом) – 1 шт.
4. Керовані комутатори Cisco серії Catalyst 2960 (моделі WS-C2960-24TT-L або WS-C2960-48TT-L) – 2 шт.
5. Робочі станції (ПК або ноутбуки) з операційною системою Windows/Linux – не менше 2 шт.
6. Консольний кабель Cisco (rollover) з конектором RJ-45 та перехідником на USB або COM-порт – 1 шт.
7. Ethernet-кабелі прямого типу (T568B) категорії Cat 5e/Cat 6 – не менше 6 шт.
8. Нуль-модемні послідовні кабелі (V.35 DTE + V.35 DCE) – 1–2 шт. (за варіантом).
9. Оптичний патч-корд LC/UPC-LC/UPC, одномодовий або багатомодовий (за варіантом) – 1 шт.
10. Термінальна програма-емулятор (PuTTY, Tera Term, SecureCRT або аналогічна) – встановлена на робочих станціях.

Схема підключення

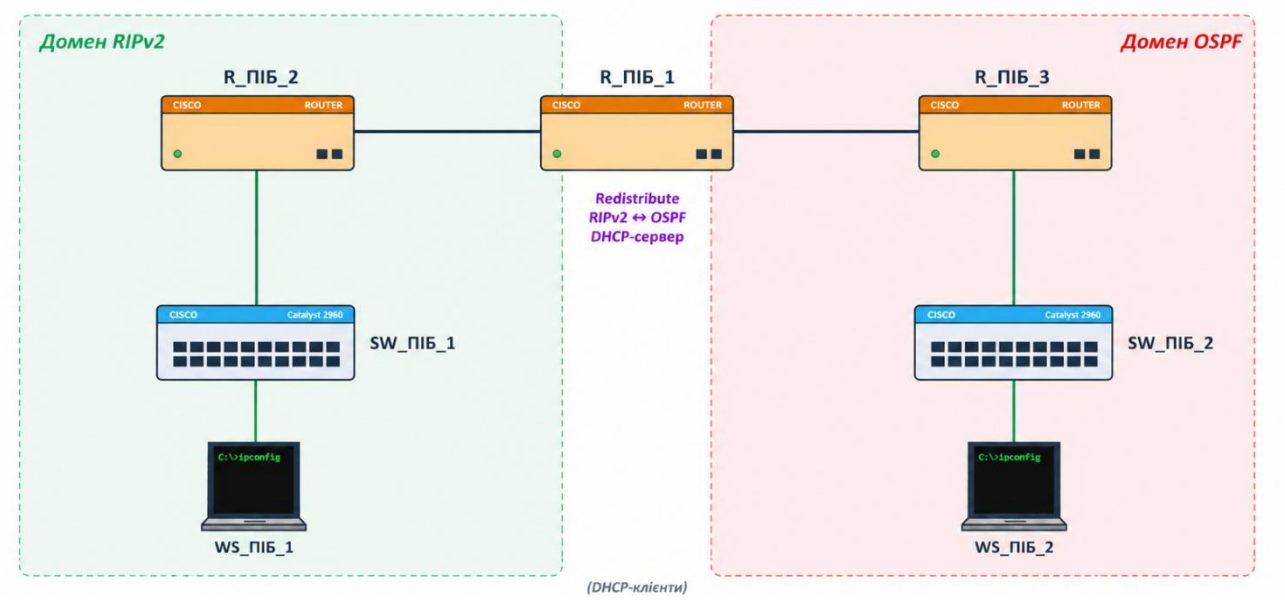

Рис. 5.1. Схема мережі, що будується у межах заняття

Примітка: ПІБ необхідно зазначати у скороченому форматі, який відповідає логіну для входу на платформу learn. Приклад: якщо логін для входу на learn – kb1_kmd, то назва маршрутизатора має бути у форматі R_kmd_1.

ЗАВДАННЯ

1. Ознайомитися з обладнанням та програмним забезпеченням робочого місця, перевірити наявність консольних, **Ethernet**, **Serial** та оптичних кабелів, термінальної програми.
2. Створити мережу відповідно до схеми на рис. 5.1. Тип фізичних каналів між маршрутизаторами обрати згідно з варіантом (табл. 5.3):
   - канал **R_ПІБ_2 – R_ПІБ_1** (домен RIPv2);
   - канал **R_ПІБ_1 – R_ПІБ_3** (домен OSPFv2).

У варіантах з послідовним (Serial) каналом на DCE-стороні встановити синхронізацію командою **clock rate** згідно зі значенням з табл. 5.4. У варіантах з оптичним каналом перевірити стан SFP-модуля та фізичну активність каналу. У варіантах з **Ethernet**-каналом (вита пара) налаштувати швидкість і режим інтерфейсу командами **speed** та **duplex**.

3. Провести налагодження іменування всіх 5 пристроїв мережі (R_ПІБ_1, R_ПІБ_2, R_ПІБ_3, SW_ПІБ_2, SW_ПІБ_3).
4. Розробити схему IP-адресації пристроїв мережі. Для цього скористатися даними табл. 5.2 згідно з варіантом. Результати заповнити у табл. 5.1.

Таблиця 5.1.

Параметри адресації мережі

Мережа / Пристрій	Інтерфейс	MAC-адреса	IP-адреса	Маска	Префікс
Підмережа **A** (LAN to R2, RIP)	–	–			
Підмережа **B** (R2–R1)	–	–			
Підмережа **C** (R1–R3)	–	–			
Підмережа **D** (LAN to R3, OSPF)	–	–			
Маршрутизатор R1 (ASBR)	до R2				
	до R3				
Маршрутизатор R2	до R1				
	до SW2				
Маршрутизатор R3	до R1				
	до SW3				
Комутатор SW2	Vlan 1				
Комутатор SW3	Vlan 1				
Робоча станція WS2	NIC		(DHCP)		
Робоча станція WS3	NIC		(DHCP)		

5. Налаштувати IP-адресацію на всіх інтерфейсах маршрутизаторів та комутаторів згідно з даними табл. 5.1. Перевірити стан інтерфейсів командою **show ip interface brief**. Для оптичних інтерфейсів додатково перевірити стан SFP-модуля командою **show interface *interface-id* transceiver**.

6. На маршрутизаторах R_ПІБ_2 та R_ПІБ_1 (його інтерфейс у бік R_ПІБ_2) налаштувати функціонування протоколу динамічної маршрутизації **RIPv2**:

- активувати протокол командою **router rip**;
- встановити версію 2 командою **version 2**;
- вимкнути автоматичну сумаризацію командою **no auto-summary**;
- оголосити безпосередньо приєднані мережі командою **network** (на R_ПІБ_2 – підмережі A і B; на R_ПІБ_1 – підмережа B);
- для тупикової локальної мережі (підмережа A на R_ПІБ_2, інтерфейс до SW_ПІБ_2) налаштувати пасивний інтерфейс командою **passive-interface**.

7. На маршрутизаторах R_ПІБ_3 та R_ПІБ_1 (його інтерфейс у бік R_ПІБ_3) налаштувати функціонування протоколу динамічної маршрутизації **OSPFv2**:

- сконфігурувати ідентифікатор маршрутизатора (Router ID) командою **router-id** згідно з варіантом (табл. 5.4);
- активувати протокол командою **router ospf** з ідентифікатором процесу, що дорівнює номеру стійки (S);
- оголосити безпосередньо приєднані мережі командою **network** із зазначенням інвертованої маски та номера області (**area 0**);
- встановити еталонну пропускну здатність командою **auto-cost reference-bandwidth 1000**;

- для тупикової локальної мережі (підмережа D на R_ПІБ_3) налаштувати пасивний інтерфейс.

8. Виконати **первинну (однонаправлену) редистрибуцію** маршрутів на R_ПІБ_1 (ASBR):

- у режимі конфігурування протоколу OSPF додати команду **redistribute rip subnets metric *seed-metric* metric-type 2** – для перерозподілу маршрутів RIP у OSPF як зовнішніх типу E2; значення початкової метрики обрати згідно з варіантом (табл. 5.4);
- перевірити появу зовнішніх маршрутів (з міткою **O E2**) у таблиці маршрутизації R_ПІБ_3 командою **show ip route**;
- переконатися, що R_ПІБ_2 поки не має маршрутів до підмереж OSPF-домену (у його таблиці маршрутизації відсутні мережі з RIP-домену в бік R_ПІБ_3).

9. Налаштувати **DHCP-сервер** на **R_ПІБ_1** для робочих станцій WS_ПІБ_2 (підмережа A) та WS_ПІБ_3 (підмережа D):

- створити пул DHCP для підмережі A командою **ip dhcp pool POOL_A**, вказати **network** (адресу та маску підмережі A), **default-router** (адресу інтерфейсу R_ПІБ_2 у підмережі A), **dns-server 8.8.8.8 8.8.4.4**, **lease 0 8 0**);
- аналогічно створити пул DHCP для підмережі D (POOL_D);
- виключити з пулів адреси, призначені для статичного використання, командою **ip dhcp excluded-address**;
- на R_ПІБ_2 (інтерфейс у бік SW_ПІБ_2) налаштувати **DHCP-relay** командою **ip helper-address** з IP-адресою R_ПІБ_1 у підмережі B;
- на R_ПІБ_3 (інтерфейс у бік SW_ПІБ_3) аналогічно налаштувати **ip helper-address** з IP-адресою R_ПІБ_1 у підмережі C;
- перевірити отримання IP-адрес робочими станціями (**ipconfig /renew** у Windows або **dhclient -r && dhclient** у Linux); проаналізувати наявність призначених шлюзів за замовчуванням та DNS-серверів.

10. **Порівняння метрик RIP та OSPF на спільному тестовому маршруті.** На цьому етапі редистрибуція виконується лише в одному напрямку (RIP→OSPF). Мета – порівняти числові значення метрик у двох протоколах та зрозуміти, чому їх не можна співставляти безпосередньо. Для цього:

- на R_ПІБ_3 виконати команду **show ip route** та зафіксувати метрику зовнішнього маршруту до підмережі A (тип **O E2**, метрика дорівнює ***seed-metric***, за замовчуванням 20);
- на R_ПІБ_2 виконати команду **show ip route** – у RIPv2 поки немає маршрутів до підмережі D (бо редистрибуція в RIP ще не виконана);
- заповнити табл. 5.5 з порівнянням метрик; зробити висновок про принципову розбіжність метрик RIP (кількість переходів) та OSPF (вартість на основі пропускної здатності) і про неможливість їх безпосереднього порівняння без редистрибуції з явно заданою початковою метрикою.

11. **Виконати двосторонню редистрибуцію** маршрутів на R_ПІБ_1:

- у режимі конфігурування протоколу RIP додати команду **redistribute ospf *process-id* metric *seed-metric-rip*** – для перерозподілу маршрутів OSPF у RIP; значення початкової метрики обрати згідно з варіантом (табл. 5.4); альтернативно – використати команду **default-metric** у режимі конфігурування RIP;
- перевірити появу зовнішніх маршрутів у таблиці маршрутизації R_ПІБ_2: до підмережі D має з'явитися маршрут типу **R** з метрикою ***seed-metric-rip***;
- перевірити зв'язність **ping** між WS_ПІБ_2 та WS_ПІБ_3, **tracert** з обох сторін.

12. Виконати порівняльне дослідження таблиць маршрутизації на всіх трьох маршрутизаторах. У звіті навести знімки виведення команди **show ip route** з кожного маршрутизатора та проаналізувати:
- типи маршрутів за міткою (**C** – connected, **L** – local, **S** – static, **R** – RIP, **O** – OSPF intra-area, **O E1/O E2** – OSPF external);
- значення адміністративної відстані [AD/metric] у квадратних дужках;
- пояснити, чому на R_ПІБ_3 маршрути типу **O E2** мають однакову метрику для всіх редистрибутованих підмереж (особливість типу E2).

13. Дослідити роботу протоколів за допомогою спеціалізованих команд:
- для RIP – **show ip protocols**, **show ip route rip**, **show ip rip database**, **debug ip rip** (увімкнути на 1–2 інтервали оновлень, потім вимкнути);
- для OSPF – **show ip ospf**, **show ip ospf neighbor**, **show ip ospf interface**, **show ip ospf database** (звернути увагу на наявність LSA Type 5 – External LSA для редистрибутованих маршрутів);
- для DHCP – **show ip dhcp binding**, **show ip dhcp pool**, **show ip dhcp conflict**.

14. Вивести та проаналізувати файли конфігурацій усіх комунікаційних пристроїв мережі (команда **show running-config**). У випадку виявлення помилок у налагодженнях – визначити причину та усунути їх.

15. Продемонструвати виконану роботу керівнику практики та оформити звіт за заняттям.

ВАРІАНТИ ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Варіант визначається за номером стійки, за якою працюють студенти, та номером класу, у якому виконуються завдання.

Таблиця 5.2.

Параметри IP-адресації мережі

№ варіанта	Підмережа A (LAN R2, /24)	Підмережа B (R2–R1, /30)	Підмережа C (R1–R3, /30)	Підмережа D (LAN R3, /24)
1	191.C.S.0	172.C.S.0	172.C.S.80	100.C.S.0
2	192.C.S.0	172.C.S.4	172.C.S.84	101.C.S.0
3	193.C.S.0	172.C.S.8	172.C.S.88	102.C.S.0
4	194.C.S.0	172.C.S.12	172.C.S.92	103.C.S.0
5	195.C.S.0	172.C.S.16	172.C.S.96	104.C.S.0
6	196.C.S.0	172.C.S.20	172.C.S.100	105.C.S.0
7	197.C.S.0	172.C.S.24	172.C.S.104	106.C.S.0
8	198.C.S.0	172.C.S.28	172.C.S.108	107.C.S.0
9	199.C.S.0	172.C.S.32	172.C.S.112	108.C.S.0
10	200.C.S.0	172.C.S.36	172.C.S.116	109.C.S.0
11	201.C.S.0	172.C.S.40	172.C.S.120	110.C.S.0
12	202.C.S.0	172.C.S.44	172.C.S.124	111.C.S.0
13	203.C.S.0	172.C.S.48	172.C.S.128	112.C.S.0
14	204.C.S.0	172.C.S.52	172.C.S.132	113.C.S.0
15	205.C.S.0	172.C.S.56	172.C.S.136	114.C.S.0
16	206.C.S.0	172.C.S.60	172.C.S.140	115.C.S.0
17	207.C.S.0	172.C.S.64	172.C.S.144	116.C.S.0
18	208.C.S.0	172.C.S.68	172.C.S.148	117.C.S.0
19	209.C.S.0	172.C.S.72	172.C.S.152	118.C.S.0
20	210.C.S.0	172.C.S.76	172.C.S.156	119.C.S.0

Примітка: **C** (class) – номер аудиторії: для ауд. **107 – 71**, для ауд. **107a – 72**; **S** (stand) – номер стійки (зазначено зверху стійки).

УВАГА! В залежності від години проведення практики значення може змінюватись за вимогою керівника.

Таблиця 5.3.

Типи фізичних з'єднань між маршрутизаторами

№ варіанта	Канал R_2 – R_1 (домен RIP)	Канал R_1 – R_3 (домен OSPF)
1	Ethernet over Twisted Pair	Ethernet over Twisted Pair
2	Ethernet over Twisted Pair	Serial T1/E1
3	Serial T1/E1	Ethernet over Twisted Pair
4	Serial V.35	Serial V.35
5	Optical Fiber Ethernet	Ethernet over Twisted Pair
6	Ethernet over Twisted Pair	Optical Fiber Ethernet
7	Optical Fiber Ethernet	Serial V.35
8	Serial V.35	Optical Fiber Ethernet
9	Ethernet over Twisted Pair	Ethernet over Twisted Pair
10	Ethernet over Twisted Pair	Serial T1/E1
11	Serial V.35	Ethernet over Twisted Pair
12	Serial V.35	Serial V.35
13	Optical Fiber Ethernet	Ethernet over Twisted Pair
14	Ethernet over Twisted Pair	Optical Fiber Ethernet
15	Optical Fiber Ethernet	Serial V.35
16	Serial V.35	Optical Fiber Ethernet
17	Ethernet over Twisted Pair	Ethernet over Twisted Pair
18	Serial V.35	Serial V.35
19	Ethernet over Twisted Pair	Serial T1/E1
20	Serial V.35	Ethernet over Twisted Pair

Таблиця 5.4.

Параметри налагодження протоколів маршрутизації та редистрибуції

№ варіанта	Clock rate, біт/с	OSPF Process ID	Router ID R_ІПБ_1	Router ID R_ІПБ_3	Seed-metric для RIP (OSPF→RIP)	Seed-metric для OSPF (RIP→OSPF)
1	64000	1	1.1.1.1	11.11.11.11	1	20
2	128000	10	2.2.2.2	12.12.12.12	2	50
3	256000	100	3.3.3.3	13.13.13.13	3	100
4	512000	200	4.4.4.4	14.14.14.14	5	150
5	1024000	1	5.5.5.5	15.15.15.15	7	200
6	2048000	10	6.6.6.6	16.16.16.16	1	20
7	64000	100	7.7.7.7	17.17.17.17	2	50
8	128000	200	8.8.8.8	18.18.18.18	3	100
9	256000	1	9.9.9.9	19.19.19.19	5	150
10	512000	10	10.10.10.10	20.20.20.20	7	200
11	1024000	100	11.11.11.11	21.21.21.21	1	20
12	2048000	200	12.12.12.12	22.12.12.12	2	50
13	64000	1	13.13.13.13	23.23.23.23	3	100
14	128000	10	14.14.14.14	24.24.24.24	5	150

№ варіанта	Clock rate, біт/с	OSPF Process ID	Router ID R_ПІБ_1	Router ID R_ПІБ_3	Seed-metric для RIP (OSPF→RIP)	Seed-metric для OSPF (RIP→OSPF)
15	256000	100	15.15.15.15	25.25.25.25	7	200
16	512000	200	16.16.16.16	26.26.26.26	1	20
17	1024000	1	17.17.17.17	27.27.27.27	2	50
18	2048000	10	18.18.18.18	28.28.28.28	3	100
19	64000	100	19.19.19.19	29.29.29.29	5	150
20	128000	200	20.20.20.20	30.30.30.30	7	200

ЗМІСТ ЗВІТУ З ЗАНЯТТЯ

Звіт з заняття повинен містити:

1. Номер, тему та мету заняття.
2. Короткі теоретичні відомості (за власним конспектом, обсягом 2–3 сторінки) з таких питань: класифікація протоколів динамічної маршрутизації; протокол RIPv2 (метрика, таймери, особливості); протокол OSPFv2 (формула розрахунку метрики, типи LSA, типи зовнішніх маршрутів E1/E2, Router ID); адміністративна відстань; редистрибуція маршрутів між RIP та OSPF; DHCP relay (ip helper-address).
3. Перелік використаного обладнання та програмного забезпечення.
4. Схему (ФОТО) побудованої мережі з позначенням усіх пристроїв та інтерфейсів, типів каналів між маршрутизаторами.
5. Розроблену схему IP-адресації у вигляді табл. 5.1 з конкретними значеннями.
6. Заповнену таблицю порівняння метрик RIP та OSPF (табл. 5.5) за результатами дослідження.
7. Лістинги команд (або скріншоти) з результатами виконання, а саме:

- налагодження IP-адресації та фізичних каналів (включно з параметрами для відповідних варіантів);
- налагодження протоколу RIPv2 на R_ПІБ_2 та R_ПІБ_1 (команди **router rip**, **version 2**, **no auto-summary**, **network**, **passive-interface**);
- налагодження протоколу OSPFv2 на R_ПІБ_1 та R_ПІБ_3 (команди **router ospf**, **router-id**, **network ... area**, **auto-cost reference-bandwidth**);
- налагодження однонаправленої редистрибуції RIP→OSPF та аналіз таблиці маршрутизації R_ПІБ_3 до двосторонньої редистрибуції;
- налагодження DHCP-сервера на R_ПІБ_1 (команди **ip dhcp pool**, **network**, **default-router**, **dns-server**, **ip dhcp excluded-address**) та DHCP-relay на R_ПІБ_2 і R_ПІБ_3 (команда **ip helper-address**);
- результати **ipconfig /all** або **ip addr** на робочих станціях після отримання адрес;
- налагодження двосторонньої редистрибуції на R_ПІБ_1 (команди **redistribute**, **default-metric**);
- результати **show ip protocols** з усіх трьох маршрутизаторів;
- результати **show ip route** з усіх трьох маршрутизаторів з аналізом типів маршрутів та значень метрик;

- результати **show ip rip database**, **debug ip rip** на R_ПІБ_2;
- результати **show ip ospf**, **show ip ospf neighbor**, **show ip ospf database** на R_ПІБ_1 та R_ПІБ_3 (особливо – наявність **LSA Type 5** для зовнішніх маршрутів);
- результати **show ip dhcp binding** та **show ip dhcp pool** на R_ПІБ_1;
- результати **ping** та **tracert** між WS_ПІБ_2 та WS_ПІБ_3 (через ASBR);
- вміст **running-config** усіх пристроїв.

8. Опис проблем, що виникли під час виконання завдання, та шляхи їх усунення.

9. Висновки по заняттю.

Таблиця 5.5.

Порівняння метрик RIP та OSPF на спільному тестовому маршруті

№	Маршрут	Метрика RIP (hops)	Метрика OSPF (cost)	Висновок
1	R2 → підмережа A (пряма, RIP-домен)			
2	R3 → підмережа A (через ASBR, OSPF-домен)	–		
3	R3 → підмережа D (пряма, OSPF-домен)	–		
4	R2 → підмережа D (після двосторонньої редистрибуції)		–	

Примітка: у графах «Метрика RIP» та «Метрика OSPF» наводяться значення, отримані з виведення команди **show ip route** на відповідному маршрутизаторі. Прокоментуйте, чому числові значення метрик RIP та OSPF не можна напряму порівнювати.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Класифікація протоколів динамічної маршрутизації

Динамічна маршрутизація – процес автоматичного формування та оновлення таблиці маршрутизації на основі обміну службовою інформацією між маршрутизаторами. На відміну від статичної маршрутизації (вимагає ручного налаштування), динамічні протоколи забезпечують автоматичну адаптацію мережі до змін топології: відмов каналів, додавання нових мереж, появи нових пристроїв.

За алгоритмом роботи протоколи динамічної маршрутизації поділяють на три класи:

- **дистанційно-векторні** (Distance Vector) – RIPv1, RIPv2, RIPng, IGRP. Маршрутизатори обмінюються повними копіями таблиць маршрутизації з безпосередніми сусідами через регулярні інтервали часу. Метрика – кількість переходів. Алгоритм – Bellman–Ford;
- **протоколи стану каналів** (Link State) – OSPFv2, OSPFv3, IS-IS. Маршрутизатори формують повну топологічну карту мережі (LSDB – Link State Database) на основі обміну повідомленнями про стан каналів (LSA – Link State Advertisement). Метрика – вартість, що залежить від пропускної здатності каналу. Алгоритм – Дейкстри (SPF – Shortest Path First);

- **гібридні** (Advanced Distance Vector) – EIGRP. Поєднують властивості дистанційно-векторних протоколів та протоколів стану каналів. Алгоритм – DUAL.

За областю застосування протоколи поділяють на внутрішні (**IGP** – Interior Gateway Protocol: RIP, OSPF, EIGRP, IS-IS), що працюють у межах однієї автономної системи, та зовнішні (**EGP** – Exterior Gateway Protocol: BGP), що забезпечують маршрутизацію між автономними системами.

Адміністративна відстань (AD – Administrative Distance) – параметр, що визначає пріоритет джерела маршрутної інформації при наявності декількох маршрутів до однієї мережі від різних джерел. Маршрут з меншим значенням AD вважається більш надійним і встановлюється у таблицю маршрутизації. Стандартні значення AD наведені у табл. 5.6.

Таблиця 5.6.

Стандартні значення адміністративної відстані

Джерело маршруту	AD	Джерело маршруту	AD
Connected (безпосередньо приєднана)	0	OSPF	110
Static (статичний)	1	IS-IS	115
EIGRP summary	5	RIP (v1/v2)	120
External BGP	20	ODR	160
Internal EIGRP	90	External EIGRP	170
IGRP	100	Internal BGP	200

Принципово важливо: протоколи з нижчою AD (наприклад, OSPF – 110) витісняють з таблиці маршрутизації маршрути від протоколів з вищою AD (RIP – 120) до тієї самої підмережі. Цю властивість необхідно враховувати при налагодженні редистрибуції маршрутів між RIP та OSPF.

Протокол маршрутизації RIPv2

RIP (Routing Information Protocol) – один з найдавніших протоколів динамічної маршрутизації, що належить до класу дистанційно-векторних. RIPv2 описано у RFC 2453. Метрикою у RIP є **кількість переходів** (hop count) – кількість маршрутизаторів, які пакет повинен пройти на шляху до мережі призначення. Максимальна допустима метрика становить **15**; маршрут з метрикою **16** вважається недосяжним (нескінченним). Це обмеження одночасно є і недоліком (мережі більше ніж з 15 переходами не підтримуються), і способом боротьби з петлями (count-to-infinity).

RIPv2 (на відміну від RIPv1) підтримує безкласову маршрутизацію (CIDR/VLSM) та розсилає оновлення груповим способом (multicast 224.0.0.9). RIP використовує транспортний протокол UDP (порт 520).

Стандартні таймери RIP:

- **Update Timer** – 30 с (інтервал між регулярними оновленнями);
- **Invalid Timer** – 180 с (час, після якого маршрут позначається як недоступний, якщо за нього не надходили оновлення);
- **Holddown Timer** – 180 с (час, протягом якого маршрутизатор ігнорує оновлення з гіршою метрикою для цього маршруту);

- **Flush Timer** – 240 с (час, після якого маршрут вилучається з таблиці маршрутизації).

Приклад налагодження RIPv2 на маршрутизаторі Cisco:

```
…
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# no auto-summary
Router(config-router)# network 192.168.1.0
Router(config-router)# network 10.0.0.0
Router(config-router)# passive-interface FastEthernet 0/0
Router(config-router)# exit
…
```

Параметри основних команд RIP:

- **router rip** – вхід у режим конфігурування протоколу RIP;
- **version {1 | 2}** – встановлення версії протоколу;
- **network *address*** – оголошення безпосередньо приєднаної класової мережі для участі у RIP;
- **no auto-summary** – вимкнення автоматичної сумаризації на межах класових мереж (обов'язково для коректної роботи з підмережами);
- **passive-interface *interface-type interface-id*** – переведення інтерфейсу у пасивний режим (RIP-оновлення не пересилаються через цей інтерфейс).

Команди моніторингу та діагностики роботи протоколу RIP наведено у табл. 5.7.

Таблиця 5.7.

Команди моніторингу та діагностики роботи протоколу RIP

Команда	Призначення
show ip protocols	Інформація про активовані протоколи маршрутизації
show ip route	Повна таблиця маршрутизації
show ip route rip	Таблиця маршрутизації лише з маршрутами RIP
show ip rip database	База даних маршрутів протоколу RIP
debug ip rip	Активація виведення діагностичної інформації
debug ip rip events	Лише події (без вмісту оновлень)
undebug all	Вимкнення всіх дебагів
clear ip route	Очищення таблиці маршрутизації

Протокол маршрутизації OSPFv2

OSPF (Open Shortest Path First) – протокол маршрутизації стану каналів, описаний у RFC 2328 (OSPFv2 для IPv4). На відміну від RIP, OSPF не передає таблиці маршрутизації, а формує у кожного маршрутизатора повну топологічну карту мережі – базу даних стану каналів (LSDB – Link State Database). На основі цієї карти алгоритм Дейкстри (SPF) обчислює оптимальні маршрути до всіх відомих мереж.

Метрика OSPF (вартість, cost) розраховується на основі пропускної здатності каналу:

$$M = \sum_{i=1}^{N} \frac{RefBW}{BWi}, \quad (1)$$

де ***M*** – метрика маршруту; ***N*** – кількість ділянок маршруту; ***RefBW*** (Reference Bandwidth) – еталонна пропускна здатність (за замовчуванням 10^8 біт/с = 100 Мбіт/с); ***BWi*** – пропускна здатність *i*-ї ділянки (біт/с).

За замовчуванням OSPF призначає інтерфейсу Fast Ethernet (100 Мбіт/с) і Gigabit Ethernet (1000 Мбіт/с) однакову вартість 1, що є некоректним. Для усунення цієї проблеми застосовується команда **auto-cost reference-bandwidth** з параметром, який повинен бути не меншим за пропускну здатність найшвидшої технології у мережі. У межах нашого заняття встановлюється значення **1000** (для коректного розрахунку метрик з урахуванням Gigabit Ethernet). Стандартні значення метрик інтерфейсів за різних значень ***RefBW*** наведено у табл. 5.8.

Таблиця 5.8.

Стандартні значення метрик інтерфейсів протоколу OSPF

Технологія	Serial T1	Serial E1	Ethernet	Fast Ethernet	Gigabit Ethernet	10G Ethernet
Пропускна здатність, Мбіт/с	1,544	2,048	10	100	1000	10000
Метрика (RefBW = 100 Мбіт/с)	64	48	10	1	1	1
Метрика (RefBW = 1000 Мбіт/с)	647	488	100	10	1	1

Області OSPF та типи маршрутизаторів. Для масштабованості OSPF підтримує ієрархічний поділ мережі на області (**areas**). Усі області повинні мати з'єднання з магістральною областю – **area 0** (Backbone Area). За розташуванням у ієрархії маршрутизатори OSPF поділяють на:

- **Internal Router (IR)** – всі інтерфейси належать одній області;
- **Backbone Router (BR)** – один або більше інтерфейсів належать **area 0**;
- **ABR** (Area Border Router) – має інтерфейси у двох або більше областях, обов'язково в **area 0**;
- **ASBR** (Autonomous System Boundary Router) – здійснює обмін маршрутами з іншими автономними системами або іншими протоколами маршрутизації.

Типи зовнішніх маршрутів OSPF. Маршрути, отримані через редистрибуцію від інших протоколів, оголошуються через спеціальний тип LSA – **Type 5 (External LSA)**. У таблиці маршрутизації такі маршрути позначаються як **O E1** або **O E2**:

- **E1 (External Type 1)** – підсумкова метрика дорівнює сумі зовнішньої метрики (заданої при редистрибуції) і внутрішньої вартості шляху OSPF до ASBR. Тобто метрика збільшується з кожним переходом всередині OSPF-домену;
- **E2 (External Type 2)** – підсумкова метрика дорівнює лише зовнішній метриці, заданій при редистрибуції (за замовчуванням 20). Внутрішня вартість шляху всередині OSPF не враховується. Цей тип використовується за замовчуванням і є більш стабільним при змінах

внутрішньої топології, але може призводити до неоптимальних маршрутів за наявності кількох ASBR.

Приклад налагодження OSPFv2 на маршрутизаторі Cisco:

```
…
Router(config)# router ospf 10
Router(config-router)# router-id 1.1.1.1
Router(config-router)# auto-cost reference-bandwidth 1000
Router(config-router)# network 10.0.0.0 0.0.0.3 area 0
Router(config-router)# network 192.168.10.0 0.0.0.255 area 0
Router(config-router)# passive-interface FastEthernet 0/1
Router(config-router)# exit
…
```

Команди моніторингу та діагностики роботи протоколу OSPF наведено у табл. 5.9.

Таблиця 5.9.

Команди моніторингу та діагностики роботи протоколу OSPF

Команда	Призначення
show ip protocols	Інформація про активовані протоколи маршрутизації
show ip ospf	Загальна інформація про процес OSPF, RID, кількість областей
show ip ospf interface	Параметри інтерфейсів OSPF (RID, тип мережі, DR/BDR, метрика, таймери)
show ip ospf neighbor	Список сусідніх маршрутизаторів, стан відносин сусідства
show ip ospf database	Вміст бази даних стану каналів (LSDB) – типи LSA
show ip ospf database external	Лише LSA Type 5 (зовнішні маршрути від ASBR)
show ip route ospf	Таблиця маршрутизації лише з маршрутами OSPF
debug ip ospf events	Виведення діагностичної інформації про події
debug ip ospf adj	Виведення діагностичної інформації про відносини сусідства
clear ip ospf process	Перезапуск процесу OSPF

Редистрибуція (перерозподіл) маршрутів

Редистрибуція маршрутів (route redistribution) – процес передачі маршрутної інформації, отриманої одним протоколом маршрутизації, в інший протокол маршрутизації для подальшого розповсюдження. Виконується на **граничному маршрутизаторі** (boundary router; у термінології OSPF – ASBR), який одночасно бере участь у роботі двох (або більше) протоколів маршрутизації.

Необхідність у редистрибуції виникає у таких випадках:

- при злитті компаній, у яких історично використовувалися різні протоколи маршрутизації;
- у мережах, де адміністраторам різних підрозділів надано право самостійно обирати протокол маршрутизації;
- при поетапному переході на новий протокол маршрутизації – на час переходу обидва протоколи функціонують паралельно;

- при підключенні до мереж постачальника послуг (Service Provider), що використовує BGP.

Початкова метрика (seed metric). Метрики кожного протоколу маршрутизації побудовано за різними принципами та відображають різні характеристики маршруту: метрика RIP – кількість переходів (число), метрика OSPF – вартість на основі пропускної здатності (число, але іншого порядку), метрика EIGRP – складова величина (bandwidth, delay, reliability, load, MTU). Тому при редистрибуції з одного протоколу в інший необхідно явно вказати початкову метрику, яку прийматиме редистрибутований маршрут у протоколі-отримувачі. Якщо метрика не задана, маршрут може взагалі не з'явитися у таблиці маршрутизації (значення за замовчуванням для більшості протоколів – нескінченність). Виняток – редистрибуція в OSPF (за замовчуванням метрика 20) та статичних маршрутів і connected-мереж.

Способи задання початкової метрики (у порядку зменшення пріоритету):

- у **route map** за допомогою команди **set metric**;
- безпосередньо у команді **redistribute** параметром **metric**;
- команда **default-metric** у режимі конфігурування протоколу-отримувача (застосовується до всіх редистрибутованих маршрутів).

Таблиця 5.10.

Початкова метрика для редистрибутованих маршрутів за замовчуванням

Протокол-отримувач	Початкова метрика за замовчуванням
RIP	Нескінченність – маршрут не редистрибутується без явного задання metric
OSPF	20 для всіх протоколів, окрім BGP; для BGP – 1
EIGRP	Нескінченність (за винятком редистрибуції з іншого процесу EIGRP)
IS-IS	0
BGP	Метрика IGP-протоколу, з якого виконується редистрибуція

Синтаксис команди **redistribute** у загальному вигляді:

router(config-router)# redistribute protocol [process-id] [metric value] [metric-type *type*] [match route-type] [route-map *map-name*] [subnets]

Найважливіші параметри:

- **subnets** – **обов'язковий параметр при редистрибуції в OSPF** для перерозподілу маршрутів підмереж (без нього OSPF перерозподілить лише класові мережі);
- **metric-type** *type* – для OSPF: тип зовнішнього маршруту (1 – E1, 2 – E2, за замовчуванням E2);
- **route-map** *map-name* – застосування фільтру маршрутів за допомогою карти маршрутів (дозволяє селективно редистрибутувати маршрути, призначати метрики, типи).

Приклад двосторонньої редистрибуції RIP ↔ OSPF на граничному маршрутизаторі:

…

Router(config)# router ospf 10

Router(config-router)# router-id 1.1.1.1

Router(config-router)# redistribute rip subnets metric 100 metric-type 2

```
Router(config-router)# exit
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# no auto-summary
Router(config-router)# redistribute ospf 10 metric 5
Router(config-router)# exit
…
```

Після виконання цих команд на маршрутизаторах протилежних доменів з'являться зовнішні маршрути: на Router з OSPF – маршрути типу **O E2** до підмереж RIP-домену; на Router з RIP – маршрути типу **R** до підмереж OSPF-домену з метрикою, заданою параметром **metric** (або **default-metric**) у режимі конфігурування RIP.

Рекомендована послідовність перевірки роботи протоколів маршрутизації, редистрибуції та DHCP

Рекомендована послідовність перевірки після завершення налаштування наведена нижче. Для кожної команди показано характерний вивід та пояснення ключових полів.

1. Перевірка стану інтерфейсів.

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet0/1        10.0.0.1        YES manual up                    up
Serial0/0/0            172.16.0.1      YES manual up                    up
```

Усі інтерфейси, що задіяні у роботі мережі, повинні мати стан up/up. Стан down/down вказує на фізичну проблему (відсутність кабелю, неактивний інтерфейс – потрібна команда no shutdown). Стан up/down – лінійний протокол не встановлений: для Serial-каналу – відсутність clock rate на DCE-стороні; для Ethernet – узгодження швидкості/дуплексу або помилкова інкапсуляція.

2. Перевірка протоколу RIPv2.

```
Router# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 12 seconds
  Outgoing update filter list for all interfaces is not set
  Default version control: send version 2, receive version 2
  Automatic network summarization is not in effect
  Routing for Networks:
    192.168.1.0
    10.0.0.0
  Passive Interface(s):
    FastEthernet0/0
  Distance: (default is 120)
```

Версія протоколу повинна бути 2 (рядок «send version 2, receive version 2»). Рядок «Automatic network summarization is not in effect» підтверджує виконану команду no auto-summary. У переліку Routing for Networks повинні бути всі оголошені мережі. Distance 120 – стандартна адміністративна відстань RIP.

```
Router# show ip rip database
10.0.0.0/8    auto-summary
10.0.0.0/24
    [1] via 192.168.1.2, 00:00:14, FastEthernet0/0
192.168.1.0/24    auto-summary
192.168.1.0/24    directly connected, FastEthernet0/0
```

База даних RIP містить усі маршрути, отримані від сусідів. Поле [1] – метрика (кількість переходів). Час 00:00:14 – час з моменту останнього оновлення; якщо перевищує 180 с (Invalid Timer), маршрут стає недоступним. Записи directly connected – безпосередньо приєднані мережі.

3. Перевірка протоколу OSPFv2.

```
Router# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:33    10.0.0.1        FastEthernet0/0
```

Стан FULL означає повну синхронізацію баз даних стану каналів (LSDB). Інші стани (INIT, EXSTART, EXCHANGE, LOADING) – проміжні; якщо стан довго залишається не FULL, перевірити збіжність Hello/Dead Interval, ідентифікаторів областей та масок підмереж. Dead Time показує час до закінчення Dead Interval, якщо за нього не надійде Hello.

```
Router# show ip ospf interface FastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 10.0.0.2/24, Area 0
  Process ID 10, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 10.0.0.2
  Backup Designated Router (ID) 2.2.2.2, Interface address 10.0.0.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

Тип мережі BROADCAST встановлений автоматично для Ethernet. Cost 10 розрахований за формулою RefBW/BW = 1000/100 = 10 (з командою auto-cost reference-bandwidth 1000 для Fast Ethernet). Hello 10, Dead 40 – стандартні значення для BMA. State DR / BDR / DROTHER показує роль маршрутизатора у сегменті.

4. Перевірка таблиці маршрутизації та редистрибуції.

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, ...
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, FastEthernet0/0
L       192.168.1.1/32 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:08, FastEthernet0/0
O E2 10.10.30.0/24 [110/100] via 172.16.0.2, 00:01:23, Serial0/0/0
```

Запис R – маршрут отримано від RIP (адміністративна відстань 120, метрика 1 – кількість переходів). Запис O E2 – зовнішній маршрут OSPF типу E2 (адміністративна відстань 110, метрика 100 – це seed-metric, задана командою redistribute rip subnets metric 100, внутрішня вартість шляху OSPF не враховується). Наявність маршрутів обох типів підтверджує коректну роботу двосторонньої редистрибуції на ASBR.

5. Перевірка роботи DHCP-сервера.

```
Router# show ip dhcp pool
Pool POOL_A :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the context :
   Current index    IP address range            Leased addresses
   192.168.1.2      192.168.1.1   - 192.168.1.254     1
```

Поле Leased addresses показує кількість виданих адрес. Якщо при наявності активних клієнтів значення 0 – DHCP-запити не доходять до маршрутизатора: перевірити команду ip helper-address на інтерфейсі найближчого до клієнтів маршрутизатора, а також відповідність підмережі у пулі.

```
Router# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/        Lease expiration       Type
                    Hardware address/
                    User name
192.168.1.10        0100.50ab.cd12.34  Mar 02 2026 14:32 PM   Automatic
```

Таблиця оренд: видана IP-адреса, MAC-адреса клієнта, час закінчення оренди. Порожня таблиця при наявності клієнтів означає, що DHCP не функціонує – необхідно перевірити налагодження ip helper-address на маршрутизаторі-релеї та маршрут від DHCP-сервера до підмережі клієнта.

6. Перевірка наскрізного зв'язку.

```
C:\> tracert 10.10.30.10
Tracing route to 10.10.30.10 over a maximum of 30 hops
  1    1 ms    *      1 ms   192.168.2.1
  2    2 ms    1 ms   2 ms   192.168.1.2
  3    3 ms    2 ms   3 ms   10.10.30.10
Trace complete.
```

Виведення показує шлях від RIP-домену до OSPF-домену. Перший хоп – шлюз за замовчуванням. Другий хоп – ASBR, що виконує редистрибуцію. Останній хоп – кінцева станція. Якщо трасування зупиняється на ASBR, значить редистрибуція з RIP в OSPF (або з OSPF в RIP) працює лише в одному напрямку – потрібна перевірка наявності команд **redistribute** у режимі конфігурування **обох** протоколів та параметра **subnets** при редистрибуції в OSPF.

Типові помилки при налагодженні протоколів маршрутизації та редистрибуції

1. **Не вимкнена автоматична сумаризація у RIP.** За замовчуванням RIPv2 автоматично сумаризує маршрути на межі класових мереж. У мережах з некласовою адресацією це призводить до некоректного формування маршрутів. Обов'язкова команда – **no auto-summary**.
2. **Невірна інвертована маска у команді network OSPF.** Інвертована маска вказує, які біти можуть змінюватися. Для /24 – 0.0.0.255, для /30 – 0.0.0.3, для /16 – 0.0.255.255. Помилка призводить до того, що інтерфейс не активується у потрібній області.
3. **Несумісні параметри для встановлення відносин сусідства OSPF.** Для формування сусідства маршрутизатори OSPF повинні мати: однакові ідентифікатори областей; однакові таймери Hello/Dead; однакові маски підмереж; однакові типи мереж; однакову аутентифікацію (якщо налаштована); унікальні Router ID.
4. **Відсутність ключового слова subnets при редистрибуції в OSPF.** Без параметра **subnets** OSPF перерозподілить лише маршрути класових мереж, ігноруючи всі підмережі. У сучасних мережах це призводить до того, що жоден маршрут не передається.
5. **Не задана початкова метрика при редистрибуції в RIP.** За замовчуванням початкова метрика для редистрибуції в RIP – нескінченність,

тому маршрут не передається. Обов'язково задати **metric** у команді **redistribute** або **default-metric** у режимі конфігурування RIP.

6. **Помилковий port-number для DHCP relay.** Команда **ip helper-address** за замовчуванням пересилає декілька UDP-портів (TFTP, DNS, NTP та інші, не тільки DHCP). У більшості випадків це не створює проблем, але у мережах з власними сервісами на цих портах може спричинити побічні ефекти. Селективну фільтрацію виконують командою **no ip forward-protocol udp** *port*.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке динамічна маршрутизація? У чому її переваги та недоліки порівняно зі статичною?
2. На які класи поділяють протоколи динамічної маршрутизації? До якого класу належать RIP та OSPF?
3. Що таке адміністративна відстань (AD)? Яке її значення для RIP та OSPF?
4. Опишіть принцип роботи дистанційно-векторних протоколів. Який алгоритм лежить в основі RIP?
5. Чим відрізняються RIPv1 та RIPv2? Назвіть три ключові відмінності.
6. Що таке метрика у протоколі RIP? Яке її максимальне значення та чому?
7. Перелічіть та поясніть призначення основних таймерів протоколу RIP.
8. Чому при налагодженні RIPv2 обов'язково використовувати команду no auto-summary?
9. Які механізми боротьби з петлями маршрутизації використовуються у протоколі RIP?
10. Опишіть принцип роботи протоколів стану каналів. Який алгоритм використовує OSPF для розрахунку маршрутів?
11. Як розраховується метрика у протоколі OSPF? Запишіть формулу.
12. Що таке еталонна пропускна здатність (RefBW)? Чому її необхідно змінювати у мережах з Gigabit Ethernet?
13. Що таке Router ID у OSPF? Як він формується за замовчуванням і чому рекомендується задавати його явно?
14. Назвіть основні типи маршрутизаторів у OSPF. Який з них виконує редистрибуцію?
15. Що таке LSDB та LSA? Який тип LSA несе інформацію про зовнішні маршрути?
16. Чим відрізняються типи зовнішніх маршрутів OSPF E1 та E2? Який з них використовується за замовчуванням?
17. Що таке редистрибуція маршрутів? У яких випадках виникає необхідність у її використанні?
18. Що таке seed metric (початкова метрика)? Які три способи її задання Ви знаєте?
19. Чому при редистрибуції в RIP обов'язково задавати початкову метрику явно?
20. Для чого потрібен параметр subnets команди redistribute при редистрибуції в OSPF?

ЗАНЯТТЯ № 6

ДОСЛІДЖЕННЯ ТА НАЛАГОДЖЕННЯ ПРОТОКОЛУ МАРШРУТИЗАЦІЇ OSPF У ШИРОКОМОВНІЙ МЕРЕЖІ З МНОЖИННИМ ДОСТУПОМ НА БАЗІ МАРШРУТИЗАТОРІВ CISCO

Мета заняття: ознайомитися з особливостями функціонування протоколу маршрутизації OSPFv2 у широкомовній мережі з множинним доступом (BMA – Broadcast Multiple-Access); ознайомитися з механізмом виборів виділеного маршрутизатора (DR) та резервного виділеного маршрутизатора (BDR); отримати практичні навички впливу на результат виборів через зміну пріоритетів інтерфейсів та ідентифікаторів маршрутизаторів; дослідити вплив таймерів Hello та Dead на час встановлення відносин сусідства та збіжність мережі; отримати практичні навички налагодження, моніторингу та діагностування роботи протоколу OSPF у комбінованій мережі з широкомовним сегментом.

Обладнання та програмне забезпечення

Для виконання заняття на робочому місці студента має бути наявним таке обладнання та програмне забезпечення:

1. Маршрутизатори Cisco серії 1841/2801/2811/2821/2901/2911/2921 з не менш ніж двома Ethernet-інтерфейсами – 3 шт.
2. Керовані комутатори Cisco серії Catalyst 2960 (моделі WS-C2960-24TT-L або WS-C2960-48TT-L) – 4 шт. (один для широкомовного сегмента, по одному на кожну робочу станцію).
3. Робочі станції (ПК або ноутбуки) з операційною системою Windows/Linux – не менше 3 шт.
4. Консольний кабель Cisco (rollover) з конектором RJ-45 та перехідником на USB або COM-порт – 1 шт.
5. Ethernet-кабелі прямого типу (T568B) категорії Cat 5e/Cat 6 – не менше 9 шт.
6. Термінальна програма-емулятор (PuTTY, Tera Term, SecureCRT або аналогічна) – встановлена на робочих станціях.

Схема підключення

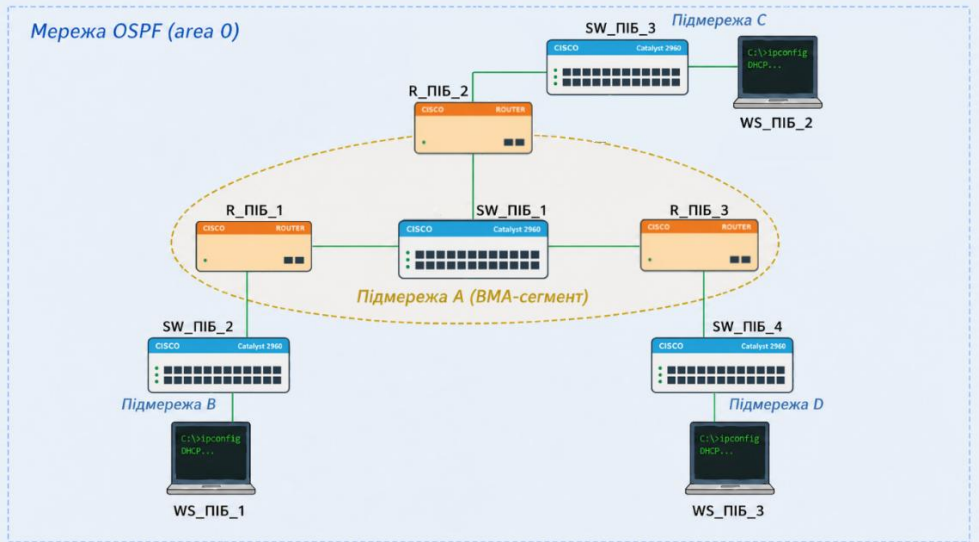

Рис. 6.1. Схема мережі, що будується у межах заняття

Примітка: ПІБ необхідно зазначати у скороченому форматі, який відповідає логіну для входу на платформу learn. Приклад: якщо логін для входу на learn – kb1_kmd, то назва маршрутизатора має бути у форматі R_kmd_1.

ЗАВДАННЯ

1. Ознайомитися з обладнанням та програмним забезпеченням робочого місця, перевірити наявність консольних і Ethernet-кабелів, термінальної програми.

2. Створити мережу відповідно до схеми на рис. 6.1. Усі три маршрутизатори підключити до центрального комутатора SW_ПІБ_1 через інтерфейси таким чином формується широкомовний сегмент з множинним доступом, у якому буде функціонувати OSPF.

3. Провести налагодження іменування всіх пристроїв мережі (R_ПІБ_1, R_ПІБ_2, R_ПІБ_3, SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3, SW_ПІБ_4).

4. Розробити схему IP-адресації пристроїв мережі. Для цього скористатися даними табл. 6.4. Результати заповнити у табл. 6.1.

Таблиця 6.1.

Параметри адресації мережі

Мережа / Пристрій	Інтерфейс	MAC-адреса	IP-адреса	Маска	Префікс
Підмережа A (BMA-сегмент)	–	–			
Підмережа B (LAN R1)	–	–			
Підмережа C (LAN R2)	–	–			
Підмережа D (LAN R3)	–	–			
Маршрутизатор R1	до BMA				
	до LAN B				
Маршрутизатор R2	до BMA				
	до LAN C				
Маршрутизатор R3	до BMA				
	до LAN D				
Комутатор SW1					
Комутатор SW2					
Комутатор SW3					
Комутатор SW4					
Робоча станція WS1	NIC				
Робоча станція WS2	NIC				
Робоча станція WS3	NIC				

5. Налаштувати IP-адресацію на всіх інтерфейсах маршрутизаторів та комутаторів, а також на робочих станціях, згідно з даними табл. 6.1. Перевірити стан інтерфейсів командою **show ip interface brief**. Перевірити зв'язок між парами безпосередньо приєднаних пристроїв командою **ping**.

6. **Базове налагодження OSPF без втручання у вибори DR/BDR.** На всіх трьох маршрутизаторах виконати базове налагодження OSPFv2 із стандартними параметрами:

- активувати протокол командою **router ospf *process-id*** (значення ***process-id*** = номер стійки S);
- оголосити безпосередньо приєднані мережі командою **network** із зазначенням інвертованої маски та **area 0**;

- встановити еталонну пропускну здатність командою **auto-cost reference-bandwidth 1000**;
- для тупикових локальних мереж (LAN R1, LAN R2, LAN R3) налаштувати пасивний інтерфейс командою **passive-interface**.

7. **Аналіз результатів виборів DR/BDR за стандартних умов.** Після того як на всіх трьох маршрутизаторах протокол OSPF активований і відносини сусідства встановлені, виконати дослідження результатів виборів DR/BDR. Для цього:

- на кожному з маршрутизаторів виконати команду **show ip ospf neighbor** – зафіксувати стан відносин сусідства (FULL/DR, FULL/BDR, FULL/DROTHER, 2-WAY/DROTHER) та **Router ID** кожного сусіда;
- виконати команду **show ip ospf interface *interface-id*** на кожному маршрутизаторі – зафіксувати тип мережі (BROADCAST), пріоритет інтерфейсу (Priority), Router ID DR-маршрутизатора (Designated Router) та BDR-маршрутизатора (Backup Designated Router);
- заповнити табл. 6.2 з результатами виборів за стандартних умов;
- пояснити, **чому саме обраний маршрутизатор став DR** (за яким критерієм він переміг – за пріоритетом, за Router ID або найвища IP-адреса серед активних фізичних інтерфейсів).

Таблиця 6.2.

Результати виборів за стандартних умов

Маршрутизатор	Роль (DR, BDR, DROTHER)	Router ID	Priority	Тип мережі	Hello / Dead, с	DR / BDR (Router ID)
R1						
R2						
R3						

***Примітка*:** у графі «Роль» зазначається фактична роль маршрутизатора за результатами **show ip ospf neighbor**. У графі «DR / BDR (Router ID)» – Router ID чинного DR.

8. Перевірити зв'язність між робочими станціями WS_ПІБ_1, WS_ПІБ_2 та WS_ПІБ_3 командою **ping**. Виконати команду **tracert** з WS_ПІБ_1 до WS_ПІБ_3 – переконатися, що пакети проходять через широкомовний сегмент A.

9. **Спостереження станів відносин сусідства через debug.** Між моментом активації OSPF та формуванням повних (FULL) відносин сусідства маршрутизатори проходять послідовність станів: **DOWN → INIT → 2-WAY → EXSTART → EXCHANGE → LOADING → FULL**. Особливість BMA-мережі: між парами маршрутизаторів DR↔DROTHER та BDR↔DROTHER формуються повні (FULL) відносини, але між парами DROTHER↔DROTHER відносини **залишаються у стані 2-WAY** – маршрутизатори «знають» про існування одне одного, але не обмінюються детальною топологічною інформацією напряму. Завдання дослідження:

- на одному з маршрутизаторів сегмента активувати трасування командами **debug ip ospf adj** та **debug ip ospf hello** для виведення інформації про процес встановлення відносин сусідства та про надсилання Hello-повідомлень;

- на цьому ж маршрутизаторі перезапустити процес OSPF командою **clear ip ospf process** (підтвердити дію вводом **yes**); зафіксувати у звіті фрагмент дебаг-виводу з повним списком переходів станів від **DOWN** до **FULL** (або **2-WAY** – якщо сусід є DROTHER);
- звернути увагу на стан **WAITING**, у якому маршрутизатор перебуває до **Wait Timer** секунд (за замовчуванням 40 с – дорівнює Dead Interval) і протягом якого він слухає Hello-повідомлення для виявлення чинних DR/BDR, перш ніж брати участь у виборах. Якщо протягом Wait Timer DR/BDR не виявлено – маршрутизатор сам ініціює вибори;
- після завершення процесу виконати команду **show ip ospf neighbor** та зафіксувати фінальний стан відносин: пари маршрутизатор↔DR і маршрутизатор↔BDR мають бути у стані **FULL/DR** та **FULL/BDR** відповідно, а пара DROTHER↔DROTHER (якщо обидва маршрутизатори – DROTHER) – у стані **2-WAY/DROTHER**;
- вимкнути дебаг командою **undebug all** або **no debug all**.

10. **Налагодження параметрів OSPF для впливу на вибори DR/BDR.** Виконати **три** послідовні сценарії впливу на результат виборів DR/BDR. Перед кожним сценарієм усі попередні налагодження, що впливають на вибори (**loopback**-інтерфейси, **router-id**, **ip ospf priority**), повинні бути скинуті у дефолтний стан, а процес OSPF – перезапущений командою **clear ip ospf process**. Кожен сценарій передбачає досягнення заданого варіантом розподілу ролей DR / BDR / DROTHER одним конкретним методом:

- **Сценарій 1 – вплив через loopback-інтерфейси.** Згідно з даними табл. 6.5 на кожному маршрутизаторі створити loopback-інтерфейс командою **interface Loopback 0** і призначити IP-адресу командою **ip address *A.B.C.D* 255.255.255.255**. Найвища IP-адреса серед активних loopback-інтерфейсів автоматично використовується як Router ID при наступному запуску OSPF; маршрутизатор з найбільшим RID стає DR. Виконати **clear ip ospf process** на всіх трьох маршрутизаторах. Зафіксувати фактичний результат у табл. 6.3;
- **Сценарій 2 – вплив через явне задання Router ID.** Видалити loopback-інтерфейси командою **no interface Loopback 0**. Згідно з даними табл. 6.6 у режимі конфігурування OSPF на кожному маршрутизаторі виконати команду **router-id *A.B.C.D*.** Виконати **clear ip ospf process** на всіх трьох маршрутизаторах. Зафіксувати фактичний результат у табл. 6.3.
- **Сценарій 3 – вплив через пріоритети інтерфейсів.** Скинути значення Router ID у режимі конфігурування OSPF командою **no router-id**. Згідно з даними табл. 6.7 на інтерфейсі кожного маршрутизатора, що дивиться у BMA-сегмент, виконати команду **ip ospf priority** *priority_value*. Маршрутизатор з найбільшим пріоритетом стає DR; пріоритет **0** повністю виключає маршрутизатор з виборів. Виконати **clear ip ospf process** на всіх трьох маршрутизаторах. Зафіксувати фактичний результат у табл. 6.3.

Після кожного сценарію зафіксувати нові результати виборів DR/BDR командами **show ip ospf neighbor** та **show ip ospf interface**. Заповнити окремий блок табл. 6.3 для кожного зі сценаріїв (1, 2, 3). Порівняти отримані результати з

очікуваним розподілом за варіантом, з результатами завдання 7 табл. 6.2 та між сценаріями. Пояснити, чому в усіх трьох сценаріях вдається досягти бажаного розподілу ролей, але різними засобами.

Таблиця 6.3.

Результати виборів DR/BDR (три сценарії)

Сценарій	Маршрутизатор	Параметр (Loopback / RID / Priority)	Router ID	Роль (DR / BDR / DROTHER)	DR / BDR (Router ID)
Сценарій 1 (loopback)	R1				
	R2				
	R3				
Сценарій 2 (router-id)	R1				
	R2				
	R3				
Сценарій 3 (priority)	R1				
	R2				
	R3				

Примітка: у графі «Параметр» для Сценарію 1 зазначається IP-адреса Loopback 0; для Сценарію 2 – значення Router ID; для Сценарію 3 – пріоритет інтерфейсу. У графі «Роль» – фактична роль маршрутизатора.

11. Дослідити роботу протоколу OSPF за допомогою повного набору діагностичних команд:

- **show ip ospf** – загальна інформація про процес OSPF, RID, кількість областей, кількість LSA;
- **show ip ospf interface** – параметри інтерфейсів OSPF (RID, тип мережі, DR/BDR, метрика, таймери Hello/Dead);
- **show ip ospf neighbor** – список сусідніх маршрутизаторів, стан відносин сусідства;
- **show ip ospf neighbor detail** – детальна інформація з зазначенням пріоритету, часу до закінчення Dead Interval та інше;
- **show ip ospf database** – повний вміст LSDB;
- **show ip route ospf** – таблиця маршрутизації з маршрутами OSPF.

12. Виконати порівняльне дослідження таблиць маршрутизації на всіх трьох маршрутизаторах командою **show ip route**. Проаналізувати: типи маршрутів за міткою (**C – connected**, **L – local**, **O – OSPF intra-area**), значення адміністративної відстані [**110/cost**] у квадратних дужках. Пояснити, чому кожен маршрутизатор має маршрути до підмереж A, C, D однаковим способом – через свого сусіда у BMA-сегменті, а не через DR (у термінах SPF-алгоритму DR не є транзитною точкою для трафіку даних, а є лише централізованою точкою обміну топологічною інформацією).

13. Вивести та проаналізувати файли конфігурацій усіх комунікаційних пристроїв мережі (команда **show running-config**). У випадку виявлення помилок у налагодженнях – визначити причину та усунути їх.

14. Продемонструвати виконану роботу керівнику практики та оформити звіт за заняттям.

ВАРІАНТИ ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Варіант визначається за номером стійки, за якою працюють студенти.

Таблиця 6.4.

Параметри IP-адресації мережі

№ варіанта	Підмережа A, /29	Підмережа B, /24	Підмережа C, /24	Підмережа D, /24
1	170.C.S.0 / 29	171.C.S.0 / 24	191.C.S.0 / 24	100.C.S.0 / 24
2	170.C.S.8 / 29	172.C.S.0 / 24	192.C.S.0 / 24	101.C.S.0 / 24
3	170.C.S.16 / 29	173.C.S.0 / 24	193.C.S.0 / 24	102.C.S.0 / 24
4	170.C.S.24 / 29	174.C.S.0 / 24	194.C.S.0 / 24	103.C.S.0 / 24
5	170.C.S.32 / 29	175.C.S.0 / 24	195.C.S.0 / 24	104.C.S.0 / 24
6	170.C.S.40 / 29	176.C.S.0 / 24	196.C.S.0 / 24	105.C.S.0 / 24
7	170.C.S.48 / 29	177.C.S.0 / 24	197.C.S.0 / 24	106.C.S.0 / 24
8	170.C.S.56 / 29	178.C.S.0 / 24	198.C.S.0 / 24	107.C.S.0 / 24
9	170.C.S.64 / 29	179.C.S.0 / 24	199.C.S.0 / 24	108.C.S.0 / 24
10	170.C.S.72 / 29	180.C.S.0 / 24	200.C.S.0 / 24	109.C.S.0 / 24
11	170.C.S.80 / 29	181.C.S.0 / 24	201.C.S.0 / 24	110.C.S.0 / 24
12	170.C.S.88 / 29	182.C.S.0 / 24	202.C.S.0 / 24	111.C.S.0 / 24
13	170.C.S.96 / 29	183.C.S.0 / 24	203.C.S.0 / 24	112.C.S.0 / 24
14	170.C.S.104 / 29	184.C.S.0 / 24	204.C.S.0 / 24	113.C.S.0 / 24
15	170.C.S.112 / 29	185.C.S.0 / 24	205.C.S.0 / 24	114.C.S.0 / 24
16	170.C.S.120 / 29	186.C.S.0 / 24	206.C.S.0 / 24	115.C.S.0 / 24
17	170.C.S.128 / 29	187.C.S.0 / 24	207.C.S.0 / 24	116.C.S.0 / 24
18	170.C.S.136 / 29	188.C.S.0 / 24	208.C.S.0 / 24	117.C.S.0 / 24
19	170.C.S.144 / 29	189.C.S.0 / 24	209.C.S.0 / 24	118.C.S.0 / 24
20	170.C.S.152 / 29	190.C.S.0 / 24	210.C.S.0 / 24	119.C.S.0 / 24

***Примітка*: C** (class) – номер аудиторії: для ауд. **107 – 71**, для ауд. **107a – 72, S** (stand) – номер стійки (зазначено зверху стійки).

УВАГА! В залежності від години проведення практики значення може змінюватись за вимогою керівника.

Таблиця 6.5.

Сценарій 1. IP-адреси Loopback 0 для впливу на вибори DR/BDR

№ вар.	OSPF PID	Loopback 0 R1	Роль R1	Loopback 0 R2	Роль R2	Loopback 0 R3	Роль R3
1	1	3.3.3.3	DR	2.2.2.2	BDR	1.1.1.1	DROTHER
2	10	3.3.3.3	DR	1.1.1.1	DROTHER	2.2.2.2	BDR
3	100	2.2.2.2	BDR	3.3.3.3	DR	1.1.1.1	DROTHER
4	200	1.1.1.1	DROTHER	3.3.3.3	DR	2.2.2.2	BDR
5	2	2.2.2.2	BDR	1.1.1.1	DROTHER	3.3.3.3	DR
6	12	1.1.1.1	DROTHER	2.2.2.2	BDR	3.3.3.3	DR
7	120	6.6.6.6	DR	5.5.5.5	BDR	4.4.4.4	DROTHER
8	220	6.6.6.6	DR	4.4.4.4	DROTHER	5.5.5.5	BDR
9	3	5.5.5.5	BDR	6.6.6.6	DR	4.4.4.4	DROTHER
10	13	4.4.4.4	DROTHER	6.6.6.6	DR	5.5.5.5	BDR
11	130	5.5.5.5	BDR	4.4.4.4	DROTHER	6.6.6.6	DR
12	230	4.4.4.4	DROTHER	5.5.5.5	BDR	6.6.6.6	DR
13	4	9.9.9.9	DR	8.8.8.8	BDR	7.7.7.7	DROTHER
14	14	9.9.9.9	DR	7.7.7.7	DROTHER	8.8.8.8	BDR
15	140	8.8.8.8	BDR	9.9.9.9	DR	7.7.7.7	DROTHER
16	240	7.7.7.7	DROTHER	9.9.9.9	DR	8.8.8.8	BDR
17	5	8.8.8.8	BDR	7.7.7.7	DROTHER	9.9.9.9	DR
18	15	7.7.7.7	DROTHER	8.8.8.8	BDR	9.9.9.9	DR
19	150	6.6.6.6	DR	4.4.4.4	BDR	2.2.2.2	DROTHER
20	250	7.7.7.7	DR	3.3.3.3	DROTHER	5.5.5.5	BDR

Примітка: Маска для всіх loopback-інтерфейсів – **/32** (255.255.255.255). При перезапуску процесу OSPF командою **clear ip ospf process** Router ID кожного маршрутизатора автоматично встановлюється рівним IP-адресі loopback-інтерфейсу. Маршрутизатор з найвищим Router ID стає DR, другий – BDR, третій – DROTHER.

Таблиця 6.6.

Сценарій 2. Значення Router ID для впливу на вибори DR/BDR

№ вар.	OSPF PID	Router ID R1	Роль R1	Router ID R2	Роль R2	Router ID R3	Роль R3
1	1	30.0.0.1	DR	20.0.0.1	BDR	10.0.0.1	DROTHER
2	10	30.0.0.2	DR	10.0.0.2	DROTHER	20.0.0.2	BDR
3	100	20.0.0.3	BDR	30.0.0.3	DR	10.0.0.3	DROTHER
4	200	10.0.0.4	DROTHER	30.0.0.4	DR	20.0.0.4	BDR
5	2	20.0.0.5	BDR	10.0.0.5	DROTHER	30.0.0.5	DR
6	12	10.0.0.6	DROTHER	20.0.0.6	BDR	30.0.0.6	DR
7	120	30.0.0.7	DR	20.0.0.7	BDR	10.0.0.7	DROTHER
8	220	30.0.0.8	DR	10.0.0.8	DROTHER	20.0.0.8	BDR
9	3	20.0.0.9	BDR	30.0.0.9	DR	10.0.0.9	DROTHER
10	13	10.0.0.10	DROTHER	30.0.0.10	DR	20.0.0.10	BDR
11	130	20.0.0.11	BDR	10.0.0.11	DROTHER	30.0.0.11	DR
12	230	10.0.0.12	DROTHER	20.0.0.12	BDR	30.0.0.12	DR
13	4	30.0.0.13	DR	20.0.0.13	BDR	10.0.0.13	DROTHER
14	14	30.0.0.14	DR	10.0.0.14	DROTHER	20.0.0.14	BDR
15	140	20.0.0.15	BDR	30.0.0.15	DR	10.0.0.15	DROTHER
16	240	10.0.0.16	DROTHER	30.0.0.16	DR	20.0.0.16	BDR
17	5	20.0.0.17	BDR	10.0.0.17	DROTHER	30.0.0.17	DR
18	15	10.0.0.18	DROTHER	20.0.0.18	BDR	30.0.0.18	DR
19	150	30.0.0.19	DR	20.0.0.19	BDR	10.0.0.19	DROTHER
20	250	30.0.0.20	DR	10.0.0.20	DROTHER	20.0.0.20	BDR

Примітка: Перед виконанням сценарію 2 видалити loopback-інтерфейси командою **no interface Loopback 0**. Маршрутизатор з найвищим Router ID стає DR.

Таблиця 6.7.

Сценарій 3. Пріоритети інтерфейсів для впливу на вибори DR/BDR

№ вар.	OSPF PID	Priority R1	Роль R1	Priority R2	Роль R2	Priority R3	Роль R3	Hello, с	Dead, с
1	1	200	DR	100	BDR	1	DROTHER	5	20
2	10	200	DR	1	DROTHER	100	BDR	6	24
3	100	100	BDR	200	DR	1	DROTHER	7	28
4	200	1	DROTHER	200	DR	100	BDR	8	32
5	2	100	BDR	1	DROTHER	200	DR	9	36
6	12	1	DROTHER	100	BDR	200	DR	10	40
7	120	200	DR	100	BDR	0	DROTHER	5	20
8	220	100	BDR	200	DR	0	DROTHER	6	24
9	3	200	DR	0	DROTHER	100	BDR	7	28
10	13	0	DROTHER	200	DR	100	BDR	8	32
11	130	200	DR	100	BDR	1	DROTHER	9	36
12	230	200	DR	1	DROTHER	100	BDR	10	40
13	4	100	BDR	200	DR	1	DROTHER	5	20
14	14	1	DROTHER	200	DR	100	BDR	6	24
15	140	100	BDR	1	DROTHER	200	DR	7	28
16	240	1	DROTHER	100	BDR	200	DR	8	32
17	5	200	DR	100	BDR	0	DROTHER	9	36
18	15	100	BDR	200	DR	0	DROTHER	10	40
19	150	200	DR	0	DROTHER	100	BDR	5	20
20	250	0	DROTHER	200	DR	100	BDR	6	24

Примітка: Перед виконанням скинути значення Router ID. Пріоритет задається на інтерфейсі, що дивиться у BMA-сегмент. Значення Hello Interval та Dead Interval застосовуються однаково на всіх трьох маршрутизаторах і **обов'язково** повинні збігатися на всіх сусідах. Пріоритет **0** повністю виключає маршрутизатор з виборів DR/BDR.

ЗМІСТ ЗВІТУ З ЗАНЯТТЯ

Звіт з заняття повинен містити:

1. Номер, тему та мету заняття.
2. Короткі теоретичні відомості (за власним конспектом, обсягом 2–3 сторінки) з таких питань: особливості функціонування OSPF у широкомовних мережах з множинним доступом; призначення DR і BDR; алгоритм та критерії виборів DR/BDR; алгоритм автоматичного вибору Router ID; типи мереж OSPF; LSA Type 1 (Router LSA) та LSA Type 2 (Network LSA) – призначення, генератор, поширення; стани відносин сусідства (DOWN, INIT, 2-WAY, EXSTART, EXCHANGE, LOADING, FULL); таймери Hello, Dead, Wait, Retransmit; команди налагодження та діагностики.
3. Перелік використаного обладнання та програмного забезпечення.

4. Схему (ФОТО) побудованої мережі з позначенням усіх пристроїв та інтерфейсів.

5. Розроблену схему IP-адресації у вигляді табл. 6.1 з конкретними значеннями.

6. Лістинги команд (або скріншоти) з результатами виконання, а саме:

- налагодження IP-адресації на всіх інтерфейсах маршрутизаторів та комутаторів;
- налагодження протоколу OSPFv2 на всіх трьох маршрутизаторах (Етап А – стандартні параметри): команди **router ospf**, **network ... area 0**, **auto-cost reference-bandwidth**, **passive-interface**;
- результати дослідження виборів DR/BDR за стандартних умов – заповнена таблиця 6.2;
- результати дослідження станів відносин сусідства через **debug** – фрагмент дебаг-виводу з **debug ip ospf adj** з повним списком переходів станів від DOWN до FULL/2-WAY;
- налагодження параметрів виборів DR/BDR за трьома сценаріями (згідно з табл. 6.4, 6.5, 6.6 відповідно): команди **interface Loopback 0** + **ip address** (Сценарій 1); **router-id** (Сценарій 2); **ip ospf priority** (Сценарій 3); **clear ip ospf process** після кожного сценарію;
- налагодження таймерів Hello та Dead Interval командами **ip ospf hello-interval** та **ip ospf dead-interval** на всіх інтерфейсах BMA-сегмента (для Сценарію 3);
- результати **show ip ospf neighbor** та **show ip ospf interface** з усіх трьох маршрутизаторів – окремо для кожного зі сценаріїв 1, 2, 3;
- заповнена таблиця 6.7 з результатами трьох сценаріїв;

7. Опис проблем, що виникли під час виконання завдання, та шляхи їх усунення.

8. Висновки по заняттю.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Типи мереж у протоколі OSPF

Протокол OSPF класифікує мережі за кількістю маршрутизаторів, що можуть бути одночасно підключені до одного канального сегмента, та за здатністю середовища передавати широкомовні (broadcast) повідомлення. Виокремлюють чотири основні типи мереж:

- **Point-to-Point** (точка-точка) – двоточкове з'єднання, у якому одночасно може бути не більше двох маршрутизаторів. Прикладом є послідовний канал HDLC або PPP. У такій мережі немає необхідності у виборах DR/BDR, оскільки кожен маршрутизатор має лише одного сусіда. За замовчуванням цей тип встановлюється для послідовних інтерфейсів;
- **Broadcast Multiple-Access (BMA)** – широкомовна мережа з множинним доступом, у якій до одного канального сегмента може бути підключено довільну кількість маршрутизаторів і середовище підтримує широкомовлення. Класичним прикладом є Ethernet-сегмент. У таких

мережах **обов'язково** проводяться вибори DR/BDR. За замовчуванням цей тип встановлюється для Ethernet-інтерфейсів;

- **Non-Broadcast Multiple-Access (NBMA)** – неширокомовна мережа з множинним доступом, до якої може бути підключено довільну кількість маршрутизаторів, але середовище не підтримує широкомовлення. Приклад – Frame Relay у multipoint-режимі. У таких мережах також відбуваються вибори DR/BDR, проте сусіди повинні бути сконфігуровані вручну командою **neighbor**;
- **Point-to-Multipoint** – з'єднання «точка-багато точок», що використовується у спеціальних топологіях. Вибори DR/BDR не проводяться.

Тип мережі OSPF визначається автоматично за типом інтерфейсу, але може бути змінений адміністративно командою **ip ospf network**.

Особливості функціонування OSPF у BMA-мережі. Призначення DR і BDR

Якщо у BMA-сегменті працює n маршрутизаторів і кожен з них формує повні відносини сусідства (full adjacency) з кожним іншим, кількість таких відносин дорівнює $\frac{n\cdot(n-1)}{2}$ – для 3 маршрутизаторів це 3 відносини, для 5 – 10, для 10 – 45. Через кожне таке відношення маршрутизатори обмінюються службовими повідомленнями (Database Description, Link State Update, Link State Acknowledgment), а кожна зміна топології розповсюджується по всіх відносинах. Зі зростанням кількості маршрутизаторів сегмента це призводить до квадратичного зростання обсягу службового трафіка та навантаження на маршрутизатори.

Для усунення цієї проблеми протокол OSPF (RFC 2328) запроваджує концепцію **виділеного маршрутизатора (DR – Designated Router)** та **резервного виділеного маршрутизатора (BDR – Backup Designated Router)**. Принцип роботи:

- DR і BDR обираються між усіма маршрутизаторами сегмента у процесі виборів;
- кожен маршрутизатор сегмента (включно з тими, що залишилися як **DROTHER**) встановлює **повні відносини сусідства тільки з DR і BDR**;
- між DROTHER-маршрутизаторами зберігаються лише двосторонні (2-WAY) відносини сусідства, через які не передається топологічна інформація;
- DROTHER посилають свої LSA на multicast-адресу 224.0.0.6 (AllDRouters), яку слухають лише DR і BDR;
- DR консолідує отриману інформацію та поширює її всім маршрутизаторам сегмента на multicast-адресу 224.0.0.5 (AllSPFRouters);
- BDR також отримує всі повідомлення, але активно ретранслювати починає лише при відмові DR.

Завдяки цьому загальна кількість повних adjacencies на сегменті зменшується з $\frac{n\cdot(n-1)}{2}$ до $2\cdot n-3$ (один DR, один BDR, кожен з решти має 2 повних adjacency – з DR і BDR; разом з відношенням DR↔BDR це і дає $2\cdot n-3$). Для 5 маршрутизаторів: 10 → 7; для 10: 45 → 17. Економія зростає з ростом сегмента.

Алгоритм виборів DR і BDR

Вибори DR і BDR проводяться у такому порядку:

1. При активації OSPF на інтерфейсі маршрутизатор переходить у стан **WAITING** і слухає Hello-повідомлення від інших маршрутизаторів сегмента протягом часу, що дорівнює **Wait Timer** (за замовчуванням дорівнює Dead Interval – 40 с для BMA). Це дозволяє виявити вже наявні DR і BDR, якщо такі є.
2. Маршрутизатор з найвищим значенням **пріоритету інтерфейсу** (OSPF priority – від 0 до 255) обирається як DR. Маршрутизатор з другим найвищим пріоритетом – як BDR. За замовчуванням пріоритет дорівнює **1**.
3. За умови однакових пріоритетів використовується тиебрейкер – найвищий **Router ID** стає DR, другий за величиною – BDR.
4. Маршрутизатор з пріоритетом **0** повністю виключається з процесу виборів – навіть з найвищим Router ID він НЕ може стати ні DR, ні BDR.
5. Маршрутизатор, який не став ні DR, ні BDR, отримує роль **DROTHER**.
6. Після виборів DR починає розсилати Hello-повідомлення для ініціалізації процесу формування повних відносин сусідства з усіма маршрутизаторами сегмента. Розмір LSDB кожного маршрутизатора синхронізується з DR.

«Sticky»-поведінка DR/BDR. Після проведених виборів DR і BDR залишаються у своїх ролях, доки не вийдуть з ладу. Якщо у мережі з'являється новий маршрутизатор з пріоритетом, вищим за пріоритет чинного DR – **перевибори НЕ відбуваються**. Цей новий маршрутизатор просто стає DROTHER. Така поведінка обрана навмисно, оскільки часті перевибори призводили б до постійної ресинхронізації LSDB всього сегмента і зниження стабільності мережі. Перевибори відбуваються лише за такими сценаріями:

- **відмова DR** – BDR автоматично перетворюється на новий DR, після чого проводяться вибори нового BDR серед DROTHER;
- **відмова BDR** – DR залишається DR, проводяться лише вибори нового BDR;
- примусове перезавантаження процесу OSPF командою **clear ip ospf process** на всіх маршрутизаторах сегмента;
- повне відключення усіх маршрутизаторів сегмента (тоді при увімкненні відбуваються нові вибори з нуля).

Алгоритм автоматичного вибору Router ID

Router ID (RID) – 32-бітний ідентифікатор маршрутизатора у форматі IP-адреси (наприклад, *1.1.1.1*), що використовується для однозначної ідентифікації маршрутизатора у домені OSPF, для виборів DR/BDR (як тиебрейкер при рівних пріоритетах) та як Advertising Router у LSA. Алгоритм визначення RID:

1. Якщо у конфігурації OSPF задано команду **router-id *A.B.C.D***, то саме це значення використовується (рекомендований спосіб).
2. Якщо команда **router-id** не задана – RID обирається як **найвища IP-адреса серед активних loopback-інтерфейсів**. Loopback-інтерфейси мають перевагу, бо їх стан не залежить від фізичних з'єднань.

3. Якщо loopback-інтерфейси не налаштовані – RID обирається як **найвища IP-адреса серед активних фізичних інтерфейсів** на момент запуску OSPF.

Після того як RID обрано і процес OSPF активований, **RID не змінюється** навіть якщо з'являється новий інтерфейс з вищою IP-адресою або loopback. Для зміни RID необхідно або задати його явно командою **router-id**, або перезапустити процес OSPF командою **clear ip ospf process**, або перезавантажити маршрутизатор. Тому **на практиці RID завжди задають явно** – це гарантує передбачуваність і стабільність виборів DR/BDR.

Стани відносин сусідства OSPF

При формуванні відносин сусідства маршрутизатори OSPF проходять послідовність станів. Стандартом визначено 8 станів, що відображають прогрес у синхронізації LSDB:

- **DOWN** – початковий стан; Hello-повідомлення від сусіда не отримано;
- **ATTEMPT** – використовується лише для NBMA-мереж; маршрутизатор активно намагається встановити з'єднання з вручну сконфігурованим сусідом;
- **INIT** – отримано Hello-повідомлення від сусіда, але власний RID цього маршрутизатора у списку відомих сусідів цього Hello ще не зазначений; одностороннє з'єднання;
- **2-WAY** – обмін Hello-повідомленнями двосторонній (сусід підтверджує отримання Hello від нашого маршрутизатора). У BMA-мережах **саме на цьому етапі проводяться вибори DR/BDR**. Між парами DROTHER↔DROTHER маршрутизатори зупиняються у стані 2-WAY і далі не просуваються – вони знають про існування одне одного, але не обмінюються детальною топологічною інформацією;
- **EXSTART** – перший етап обміну топологічною інформацією; маршрутизатори домовляються, хто з них буде Master (з вищим RID) і хто Slave у процесі обміну DBD-повідомленнями; встановлюється послідовність повідомлень;
- **EXCHANGE** – обмін Database Description (DBD) повідомленнями, що містять заголовки LSA (без повного вмісту); маршрутизатор будує перелік LSA, які йому ще невідомі;
- **LOADING** – маршрутизатор посилає Link State Request (LSR) повідомлення з переліком невідомих LSA; сусід відповідає Link State Update (LSU); після отримання всіх запитаних LSA маршрутизатор переходить у наступний стан;
- **FULL** – синхронізація LSDB завершена; маршрутизатори мають ідентичні бази даних; повне відношення сусідства встановлено. Саме у цьому стані запускається алгоритм SPF для розрахунку маршрутів.

Wait Timer – важливий допоміжний таймер, що використовується при переході зі стану **INIT** у **2-WAY**. Маршрутизатор очікує до **Wait Timer** секунд (за замовчуванням дорівнює Dead Interval – 40 с для BMA), щоб виявити чинних DR/BDR у сегменті, перш ніж брати участь у виборах. Якщо протягом Wait Timer

DR/BDR не виявлено – маршрутизатор сам ініціює вибори. Це запобігає ситуації, коли перший маршрутизатор, що увімкнувся, відразу ж стає DR, без шансів інших маршрутизаторів вплинути на результат.

Network LSA (LSA Type 2) – особливість BMA-мереж

У BMA-мережах OSPF використовує два типи LSA для опису топології сегмента:

- **LSA Type 1 (Router LSA)** – генерується **кожним маршрутизатором** і описує його власні інтерфейси, стани каналів та сусідів; поширюється тільки в межах однієї області (area);
- **LSA Type 2 (Network LSA)** – генерується **ВИНЯТКОВО DR-маршрутизатором** і описує сам BMA-сегмент: перелік усіх маршрутизаторів, що сформували повні відносини сусідства з DR (тобто DR, BDR і всіх DROTHER). Поле **Link State ID** дорівнює IP-адресі інтерфейсу DR у цьому сегменті; поле **Advertising Router** – Router ID DR.

Чому Network LSA необхідна. Без LSA Type 2 кожен маршрутизатор у Router LSA повинен був би описувати кожного свого сусіда у BMA-сегменті як окреме point-to-point з'єднання, що при n маршрутизаторах у сегменті дало б $n\cdot(n-1)$ описів окремих з'єднань у LSDB. Завдяки LSA Type 2 кожен Router LSA описує BMA-сегмент одним записом «transit network» (тип 2 у Router LSA), що посилається на Network LSA від DR. Це призводить до:

- значного зменшення розміру LSDB у мережах з великою кількістю маршрутизаторів сегмента;
- зменшення обчислювальної складності алгоритму SPF (граф топології спрощується);
- консистентної топологічної моделі: ділянка BMA представляється як «transit network» (один вузол графа топології), до якого приєднані всі маршрутизатори сегмента – це адекватніше відображає реальність, ніж повна mesh-топологія.

LSA Type 2 існує **тільки у BMA та NBMA мережах** – у мережах типу Point-to-Point або Point-to-Multipoint вибори DR/BDR не проводяться, отже, і Network LSA не генерується.

Мультикаст-адреси протоколу OSPF

OSPF використовує дві зарезервовані IPv4 multicast-адреси для розсилки службових повідомлень у BMA-мережах:

- **224.0.0.5 (AllSPFRouters)** – слухається всіма маршрутизаторами OSPF у сегменті. На цю адресу DR і BDR розсилають Hello-повідомлення та Link State Update (LSU) до всіх маршрутизаторів сегмента;
- **224.0.0.6 (AllDRouters)** – слухається лише DR і BDR. На цю адресу DROTHER-маршрутизатори надсилають свої LSU-повідомлення до DR/BDR. Така адресація дозволяє уникнути зайвого навантаження на DROTHER (вони не отримують Hello/LSU від інших DROTHER напряму).

Така асиметрична multicast-схема є частиною оптимізації BMA: інформація концентрується на DR (через 224.0.0.6), а DR одночасно поширює її всім маршрутизаторам сегмента (через 224.0.0.5).

Таймери протоколу OSPF

Стандартні значення таймерів OSPF для різних типів мереж наведено у табл. 6.8.

Таблиця 6.8.

Стандартні значення таймерів протоколу OSPF

Тип мережі	Hello Interval, с	Dead Interval, с (4×Hello)	Wait Timer, с (=Dead)	Retransmit Interval, с
Point-to-Point	10	40	40	5
Broadcast (BMA)	10	40	40	5
Non-Broadcast (NBMA)	30	120	120	5
Point-to-Multipoint	30	120	120	5

Призначення таймерів:

- **Hello Interval** – інтервал між послідовними Hello-повідомленнями. Обов'язково **повинен збігатися** на всіх маршрутизаторах сегмента – інакше відносини сусідства не сформуються;
- **Dead Interval** – час, протягом якого маршрутизатор очікує Hello від сусіда; якщо за цей час Hello не отримано – сусід вважається втраченим. За замовчуванням дорівнює 4×Hello. Також обов'язково повинен збігатися на сусідах;
- **Wait Timer** – час очікування у стані WAITING при формуванні відносин у BMA/NBMA;
- **Retransmit Interval** – інтервал між повторними відправками LSA-оновлень, якщо за них не отримано підтвердження.

Зменшення Hello/Dead Interval (наприклад, до 1/4 с) **прискорює виявлення відмов** і зменшує час збіжності, але **збільшує службовий трафік** і навантаження на CPU маршрутизаторів. Збільшення таймерів – навпаки, зменшує службовий трафік, але збільшує час реакції на відмови.

Команди налагодження OSPF у BMA-мережі

Основні команди налагодження роботи OSPF у BMA-мережі:

- **router ospf *process-id*** – вхід у режим конфігурування OSPF;
- **router-id *A.B.C.D*** – встановлення Router ID у форматі IP-адреси;
- **network *address wildcard area*** – оголошення мережі для участі у OSPF з прив'язкою до області;
- **ip ospf network** {**broadcast** | **non-broadcast** | **point-to-multipoint** | **point-to-point**} (режим інтерфейсу) – встановлення типу мережі OSPF;
- **ip ospf priority *priority_value*** (режим інтерфейсу) – встановлення пріоритету інтерфейсу для виборів DR/BDR; діапазон 0–255; **0 виключає маршрутизатор з виборів**; за замовчуванням 1;
- **ip ospf hello-interval *seconds*** (режим інтерфейсу) – інтервал Hello;
- **ip ospf dead-interval *seconds*** (режим інтерфейсу) – інтервал Dead;

- **ip ospf retransmit-interval *seconds*** (режим інтерфейсу) – інтервал між повторами LSA;
- **clear ip ospf process** – перезапуск процесу OSPF (ініціює нові вибори DR/BDR).

Приклад налагодження OSPF на маршрутизаторі у BMA-мережі (маршрутизатор повинен стати DR):

```
…
Router(config)# router ospf 10
Router(config-router)# router-id 1.1.1.1
Router(config-router)# auto-cost reference-bandwidth 1000
Router(config-router)# network 192.168.1.0 0.0.0.7 area 0
Router(config-router)# network 10.10.1.0 0.0.0.255 area 0
Router(config-router)# passive-interface FastEthernet 0/1
Router(config-router)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip ospf priority 200
Router(config-if)# ip ospf hello-interval 5
Router(config-if)# ip ospf dead-interval 20
Router(config-if)# exit
…
```

Команди моніторингу та діагностики OSPF

Таблиця 6.9.

Команди моніторингу та діагностики роботи OSPF у BMA-мережі

Команда	Призначення
show ip protocols	Інформація про активовані протоколи маршрутизації
show ip ospf	Загальна інформація про процес OSPF, RID, кількість областей
show ip ospf interface	Параметри інтерфейсів OSPF (RID, тип мережі, DR/BDR, пріоритет, таймери)
show ip ospf interface Fa0/0	Параметри конкретного інтерфейсу
show ip ospf neighbor	Список сусідніх маршрутизаторів, стан відносин сусідства, ролі (DR/BDR/DROTHER)
show ip ospf neighbor detail	Детальна інформація про сусідів
show ip ospf database	Повний вміст LSDB (усі типи LSA)
show ip ospf database router	Лише LSA Type 1 (Router LSA)
show ip ospf database network	Лише LSA Type 2 (Network LSA)
show ip route ospf	Таблиця маршрутизації лише з маршрутами OSPF
debug ip ospf adj	Виведення інформації про процес встановлення відносин сусідства
debug ip ospf hello	Виведення інформації про Hello-повідомлення
debug ip ospf events	Загальні події OSPF
clear ip ospf process	Перезапуск процесу OSPF (ініціює нові вибори DR/BDR)
undebug all	Вимкнення всіх дебагів

Рекомендована послідовність перевірки роботи протоколу OSPF у BMA-мережі

Рекомендована послідовність перевірки після завершення налаштування наведена нижче. Для кожної команди показано характерний вивід та пояснення ключових полів.

1. Перевірка стану інтерфейсів.

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        172.16.0.1      YES manual up                    up
FastEthernet0/1        191.71.1.254    YES manual up                    up
Loopback0              3.3.3.3         YES manual up                    up
```

Усі інтерфейси, що задіяні у роботі мережі, повинні мати стан up/up. Для Loopback-інтерфейсу стан завжди up/up незалежно від фізичних з'єднань – це і робить loopback-адресу надійним джерелом для Router ID. Стан down/down фізичного інтерфейсу – потрібна команда no shutdown або перевірка кабелю.

2. Перевірка відносин сусідства OSPF.

```
Router# show ip ospf neighbor
Neighbor ID    Pri  State          Dead Time   Address      Interface
2.2.2.2          1  FULL/BDR       00:00:33    172.16.0.2   FastEthernet0/0
3.3.3.3          1  2-WAY/DROTHER  00:00:35    172.16.0.3   FastEthernet0/0
```

Виведення показує всіх сусідів сегмента BMA. Стан **FULL/DR** або **FULL/BDR** – повна синхронізація LSDB з DR/BDR. Стан **2-WAY/DROTHER** – взаємне розпізнавання між парою DROTHER↔DROTHER без обміну топологічною інформацією напряму (це нормально для BMA-мережі і свідчить про правильну роботу механізму DR/BDR). Якщо стан довго залишається **INIT** або **EXSTART** – перевірити: збіжність Hello/Dead Interval (повинні збігатися на всіх сусідах сегмента); унікальність Router ID; однаковість маски підмережі та area ID. Dead Time показує час до закінчення Dead Interval; повинен бути близько 30–40 с (за замовчуванням Dead 40, Hello 10).

3. Перевірка параметрів інтерфейсу OSPF та результатів виборів DR/BDR.

```
Router# show ip ospf interface FastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 172.16.0.1/29, Area 0
  Process ID 10, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 172.16.0.1
  Backup Designated Router (ID) 2.2.2.2, Interface address 172.16.0.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Neighbor Count is 2, Adjacent neighbor count is 1
```

Тип мережі **BROADCAST** встановлений автоматично для Ethernet-інтерфейсу – це і є умова для проведення виборів DR/BDR. State показує роль маршрутизатора у сегменті: DR / BDR / DROTHER. Поля Designated Router (ID) і Backup Designated Router (ID) повинні бути однаковими на всіх трьох маршрутизаторах сегмента – це підтверджує консистентність виборів. Поле **Adjacent neighbor count** – кількість повних adjacencies (для DR/BDR – дорівнює загальній кількості сусідів; для DROTHER – лише 2: з DR і BDR). Якщо результат виборів не відповідає очікуваному за варіантом – необхідно виконати команду **clear ip ospf process** на всіх трьох маршрутизаторах для повторних виборів.

4. Перевірка бази даних стану каналів (LSDB) та Network LSA.

```
Router# show ip ospf database
            OSPF Router with ID (3.3.3.3) (Process ID 10)
                Router Link States (Area 0)
Link ID         ADV Router      Age   Seq#       Checksum  Link count
1.1.1.1         1.1.1.1         234   0x80000003 0x00A4C2  2
2.2.2.2         2.2.2.2         231   0x80000003 0x008B91  2
3.3.3.3         3.3.3.3         229   0x80000003 0x00721F  2
                Net Link States (Area 0)
Link ID         ADV Router      Age   Seq#       Checksum
172.16.0.1      3.3.3.3         229   0x80000001 0x00C8A3
```

Секція **Router Link States** (LSA Type 1) – кожен маршрутизатор сегмента генерує власне Router LSA з описом своїх інтерфейсів та сусідів. Секція **Net Link States** (LSA Type 2) – особлива для BMA-мережі. Має бути **рівно один запис** для BMA-сегмента, причому поле Advertising Router (ADV Router) повинно дорівнювати **Router ID чинного DR** (у прикладі 3.3.3.3 – DR). Поле Link ID – IP-адреса інтерфейсу DR у BMA-сегменті. Якщо у секції Net Link States кілька записів – це означає неузгодженість виборів DR (різні маршрутизатори вважають себе DR), що є серйозною проблемою.

```
Router# show ip ospf database network 172.16.0.1
            OSPF Router with ID (3.3.3.3) (Process ID 10)
                Net Link States (Area 0)
  Routing Bit Set on this LSA
  LS age: 232
  Options: (No TOS-capability, DC)
  LS Type: Network Links
  Link State ID: 172.16.0.1 (address of Designated Router)
  Advertising Router: 3.3.3.3
  Network Mask: /29
        Attached Router: 3.3.3.3
        Attached Router: 2.2.2.2
 Attached Router: 1.1.1.1
```

Перелік **Attached Router** – це Router ID усіх маршрутизаторів сегмента, що сформували повні відносини сусідства з DR (включно з самим DR і BDR). Має містити **рівно три записи** для нашої мережі. Якщо запис відсутній для одного з маршрутизаторів – він не сформував повне сусідство з DR (наприклад, у нього стан 2-WAY/DROTHER з усіма іншими маршрутизаторами через помилку у конфігурації, або він повністю виключений через **priority 0**).

5. Перевірка таблиці маршрутизації.

```
Router# show ip route
Codes: C – connected, L – local, O – OSPF, IA – OSPF inter area, …
       172.16.0.0/29 is variably subnetted, 2 subnets, 2 masks
C      172.16.0.0/29 is directly connected, FastEthernet0/0
L      172.16.0.1/32 is directly connected, FastEthernet0/0
       191.71.0.0/24 is variably subnetted, 2 subnets, 2 masks
C      191.71.1.0/24 is directly connected, FastEthernet0/1
L      191.71.1.254/32 is directly connected, FastEthernet0/1
O      221.71.1.0/24 [110/11] via 172.16.0.2, 00:05:23, FastEthernet0/0
O      200.71.1.0/24 [110/11] via 172.16.0.3, 00:05:23, FastEthernet0/0
```

Записи **C** і **L** – безпосередньо приєднані мережі та локальні адреси інтерфейсів. Записи **O** – міжвузлові маршрути OSPF (Intra-Area). Адміністративна відстань **110** у квадратних дужках. Метрика **11** – сума cost вихідного інтерфейсу (10 для FastEthernet) та cost інтерфейсу сусіда у LAN (1 для GigabitEthernet 0/1 з RefBW 1000). Зверніть увагу: маршрути проходять **безпосередньо через сусіда у BMA-сегменті**, а не через DR – це підтверджує,

що DR є лише централізованою точкою обміну топологічною інформацією, а не транзитною точкою для трафіку даних.

7. Перевірка наскрізного зв'язку.

```
C:\> tracert 241.71.1.1
Tracing route to 241.71.1.1 over a maximum of 30 hops
  1    1 ms    *      1 ms   191.71.1.254
  2    2 ms    1 ms   2 ms   172.16.0.3
  3    3 ms    2 ms   3 ms   241.71.1.1
Trace complete.
```

Виведення показує шлях до хоста 241.71.1.1. Перший хоп – шлюз за замовчуванням. Другий хоп – інтерфейс Router у BMA-сегменті (172.16.0.3) – пакет передається безпосередньо через BMA-сегмент, **незалежно від того, який маршрутизатор є DR**. Третій хоп – кінцева станція. Якщо **ping** працює, але **tracert** зупиняється – на одному з маршрутизаторів відсутній зворотний маршрут (наприклад, не оголошена якась з підмереж командою **network ... area 0**).

Типові помилки при налагодженні OSPF у BMA-мережі

1. **Розбіжність Hello/Dead Interval на сусідах.** Якщо на двох маршрутизаторах сегмента налагоджено різні значення Hello або Dead Interval, відносини сусідства не сформуються – стан залишиться у INIT. Виявити проблему допомагає команда **show ip ospf interface** (порівняти таймери) або **debug ip ospf hello**.
2. **Невірна інвертована маска у команді network.** Інвертована маска вказує, які біти можуть змінюватися. Для /29 – 0.0.0.7, для /24 – 0.0.0.255, для /30 – 0.0.0.3. Помилка призводить до того, що інтерфейс не активується у потрібній області.
3. **Несумісні Router ID.** Якщо на двох маршрутизаторах задано однаковий Router ID – між ними не сформуються відносини сусідства. Для уникнення цієї помилки рекомендовано задавати RID явно командою **router-id** з унікальним значенням для кожного маршрутизатора.
4. **Неочікуваний результат виборів DR/BDR.** Найпоширеніша причина – забуто виконати **clear ip ospf process** після зміни пріоритетів або Router ID. Через «sticky» властивість, чинні DR/BDR залишаються у своїх ролях навіть після зміни параметрів – нові значення набувають чинності лише після перезапуску процесу.
5. **Маршрутизатор з priority 0 в єдиному сегменті.** Якщо у сегменті всі маршрутизатори мають priority 0 – DR/BDR не обираються, відносини сусідства не формуються, мережа не функціонує. Принаймні один маршрутизатор повинен мати ненульовий пріоритет.
6. **Зміна типу мережі без узгодження.** Якщо на одному з маршрутизаторів сегмента змінити тип мережі OSPF командою **ip ospf network point-to-point** (а на інших залишити broadcast) – відносини сусідства не сформуються, оскільки на сусідах буде розбіжність типів мережі.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Які типи мереж розрізняє протокол OSPF? Назвіть характеристики кожного.
2. Що таке BMA-мережа? Наведіть приклади.
3. Розшифруйте абревіатуру DR. Яке призначення DR у BMA-мережі?
4. Розшифруйте абревіатуру BDR. Чому потрібен BDR, а не лише DR?
5. Опишіть алгоритм виборів DR і BDR. За яким параметром відбувається первинне порівняння маршрутизаторів?
6. Яке значення Priority виключає маршрутизатор з виборів DR/BDR?
7. Що таке Router ID? Опишіть алгоритм його автоматичного вибору.
8. Опишіть «sticky»-поведінку DR/BDR. Що відбувається при появі у мережі нового маршрутизатора з вищим пріоритетом?
9. За яких умов відбуваються перевибори DR/BDR? Що відбувається при відмові DR? При відмові BDR?
10. Перелічіть стани відносин сусідства OSPF у послідовності їх проходження. У якому стані проводяться вибори DR/BDR?
11. Чому у BMA-мережі між парами DROTHER↔DROTHER відносини залишаються у стані 2-WAY, а не переходять у FULL?
12. Що таке Wait Timer? Для чого він потрібен? Чому дорівнює його значення за замовчуванням?
13. Які мультикаст-адреси використовує OSPF? Хто їх слухає, хто на них надсилає?
14. Перелічіть та поясніть призначення основних таймерів OSPF (Hello, Dead, Wait, Retransmit). Які зі стандартних значень для BMA-мереж?
15. Чому Hello Interval та Dead Interval повинні збігатися на всіх маршрутизаторах сегмента?
16. Якими командами Cisco IOS задаються пріоритет інтерфейсу та Router ID?
17. Чому у мережі, де DR і BDR є чітко визначеними ролями, маршрут до іншої підмережі у таблиці маршрутизації НЕ обов'язково проходить через DR? Поясніть різницю між роллю DR на рівні протоколу та маршрутизацією трафіку даних.

ЗАНЯТТЯ 7

ДОСЛІДЖЕННЯ ТА НАЛАГОДЖЕННЯ ПРОТОКОЛУ МАРШРУТИЗАЦІЇ EIGRP ТА БАЛАНСУВАННЯ НАВАНТАЖЕННЯ У МЕРЕЖІ НА БАЗІ МАРШРУТИЗАТОРІВ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження протоколу динамічної маршрутизації EIGRP на обладнанні Cisco; набути практичних навичок розрахунку метрик та визначення оптимальних маршрутів EIGRP; налаштувати протокол EIGRP для IPv4 та IPv6 одночасно (dual-stack); дослідити та налаштувати балансування навантаження між рівнометричними (equal-cost) та нерівнометричними (unequal-cost) маршрутами EIGRP; виконати розрахунок розподілу трафіку між маршрутами; налаштувати пасивні інтерфейси та перевірити відмовостійкість мережі; дослідити механізм DUAL та стани таблиці топології; налаштувати DHCP-сервер і переконатися у наскрізній доступності хостів через обидві версії IP.

Обладнання та програмне забезпечення

Для виконання заняття на робочому місці студента має бути наявним таке обладнання та програмне забезпечення:

1. Маршрутизатори Cisco серії 1841/2801/2811/2821/2901/2911/2921 з інтерфейсними слотами для плат розширення – 3 шт.
2. Плати розширення Cisco WIC-2T (або аналогічні) для послідовних з'єднань – 2–4 шт. (за варіантом).
3. Керовані комутатори Cisco серії Catalyst 2960 (WS-C2960-24TT-L або WS-C2960-48TT-L) – 3 шт.
4. Робочі станції (ПК або ноутбуки) з ОС Windows/Linux – не менше 3 шт.
5. Консольний кабель Cisco (rollover) RJ-45 з перехідником на USB або COM-порт – 1 шт.
6. Ethernet-кабелі прямого типу (T568B) Cat 5e/Cat 6 – не менше 9 шт.
7. Нуль-модемні послідовні кабелі (V.35 DTE + DCE) – 2 шт. (за варіантом).
8. Термінальна програма-емулятор (PuTTY, Tera Term, SecureCRT або аналогічна) – встановлена на робочих станціях.

Схема підключення

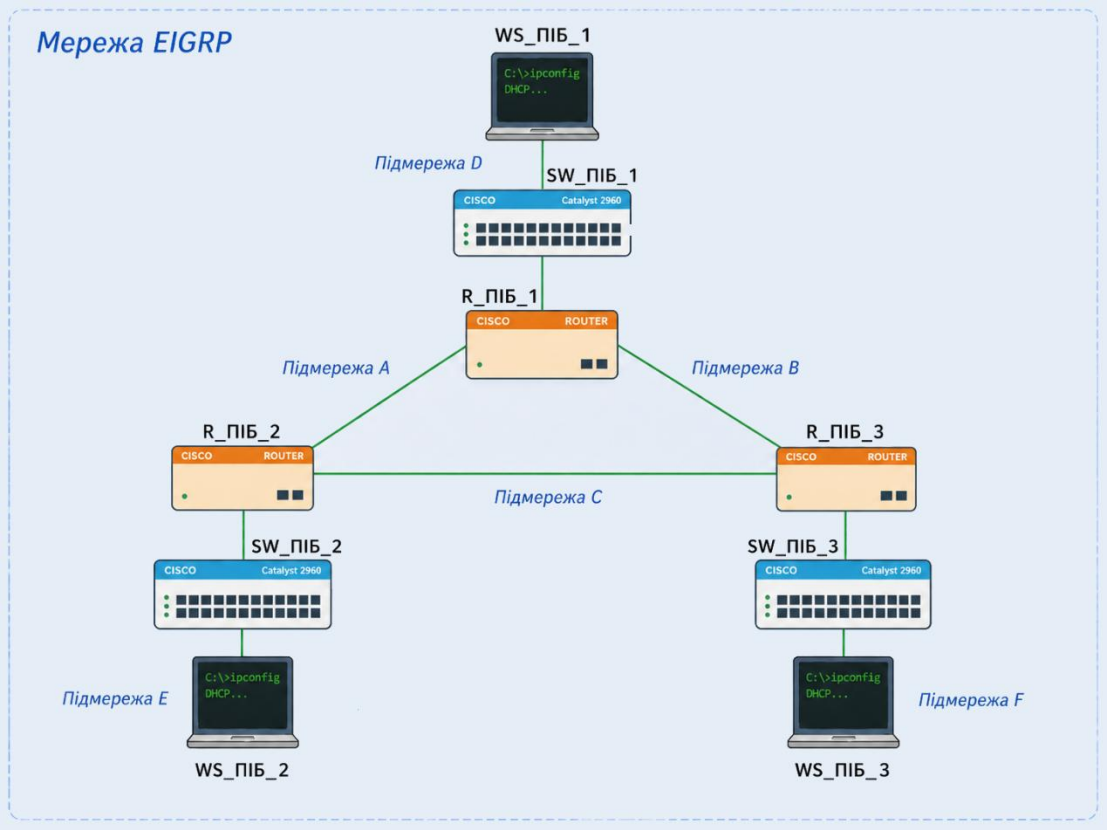

Рис. 7.1. Схема мережі EIGRP, що будується у межах заняття

Примітка: ПІБ необхідно зазначати у скороченому форматі, який відповідає логіну для входу на платформу learn. Приклад: якщо логін для входу на learn – kb1_kmd, то назва комутатора має бути у форматі SW_kmd_1.

ЗАВДАННЯ

1. Ознайомитися з обладнанням та програмним забезпеченням, перевірити наявність консольних, **Ethernet**- та **Serial**-кабелів, термінальної програми.

2. Створити мережу відповідно до схеми (рис. 7.1). Тип фізичних каналів між маршрутизаторами обрати згідно з варіантом (табл. 7.7). У варіантах з Serial-каналом встановити частоту тактових імпульсів командою **clock rate** згідно з табл. 7.8.

3. Провести налагодження іменування всіх пристроїв мережі (R_ПІБ_1, R_ПІБ_2, R_ПІБ_3, SW_ПІБ_1, SW_ПІБ_2, SW_ПІБ_3).

4. Розробити схему IPv4-адресації за даними табл. 7.5 та IPv6-адресації за даними табл. 7.6. Результати заповнити у табл. 7.1. Для кожного інтерфейсу маршрутизатора вказати **обидві адреси**: IPv4, IPv6 **global unicast** та **link-local FE80::**.

Таблиця 7.1.

Параметри адресації мережі

Мережа / Пристрій	Інтерфейс	MAC-адреса	IPv4-адреса / Маска	IPv6 Global Unicast /64	IPv6 Link-Local	Шлюз
Підмережа A (R1–R2)	–	–			–	–
Підмережа B (R1–R3)	–	–			–	–
Підмережа C (R2–R3)	–	–			–	–
Підмережа D (LAN R1)	–	–			–	–
Підмережа E (LAN R2)	–	–			–	–
Підмережа F (LAN R3)	–	–			–	–
R1	до R2					
	до R3					
	до SW1					
R2	до R1					
	до R3					
	до SW2					
R3	до R1					
	до R2					
	до SW3					
SW1					–	
SW2					–	
SW3					–	
WS1	NIC		(DHCP)	(SLAAC)	–	
WS2	NIC		(DHCP)	(SLAAC)	–	
WS3	NIC		(DHCP)	(SLAAC)	–	

5. Налаштувати IPv4-адресацію на всіх інтерфейсах. Налаштувати IPv6-адресацію на маршрутизаторах (команди **ipv6 address**, **ipv6 enable**). Активувати IPv6-маршрутизацію командою **ipv6 unicast-routing**. Перевірити: **show ip interface brief**, **show ipv6 interface brief**.

6. Налаштувати **EIGRP для IPv4** на всіх трьох маршрутизаторах з ASN згідно з варіантом (табл. 7.8):

- активувати командою **router eigrp ASN**;
- оголосити всі підключені мережі командою **network**;
- вимкнути автосумаризацію командою **no auto-summary**;
- для LAN-інтерфейсів (до комутаторів) налаштувати **passive-interface**.

7. Налаштувати **EIGRP для IPv6** на всіх трьох маршрутизаторах:

- активувати командою **ipv6 router eigrp ASN**;
- призначити Router ID командою **eigrp router-id** згідно з варіантом (табл. 7.8);
- активувати процес командою **no shutdown** (процес IPv6 EIGRP за замовчуванням вимкнений);

- на кожному інтерфейсі, що бере участь у маршрутизації, виконати ipv6 eigrp ASN;
- для LAN-інтерфейсів налаштувати **passive-interface**.

8. Перевірити встановлення відносин сусідства командами **show ip eigrp neighbors** та **show ipv6 eigrp neighbors**. Заповнити табл. 7.2.

Таблиця 7.2.

Результати встановлення відносин сусідства EIGRP

Маршрутизатор	Сусід (Router-ID)	Адреса сусіда (IPv4 / Link-Local)	Інтерфейс	Hold (c)	Uptime	IPv4 EIGRP	IPv6 EIGRP
R1 ↔ R2							
R1 ↔ R3							
R2 ↔ R3							

9. Налаштувати **DHCP-сервер** на R_ПІБ_1 для підмереж D, E, F (окремий пул для кожної). На R_ПІБ_2 та R_ПІБ_3 налаштувати DHCP-relay командою **ip helper-address**. Перевірити отримання адрес робочими станціями.

10. Дослідити **рівнометричне балансування навантаження (Equal-Cost LB)**:

- виконати **show ip eigrp topology** – визначити наявність маршрутів з однаковою FD;
- налаштувати однакові параметри **bandwidth** та **delay** на каналах A і B згідно з варіантом (табл. 7.8) для отримання рівнометричних шляхів;
- перевірити наявність обох маршрутів командою **show ip route**;
- виконати розрахунок частки трафіку для кожного маршруту за формулою з теоретичного розділу. Заповнити табл. 7.3.

Таблиця 7.3.

Результати дослідження рівнометричного балансування навантаження (Equal-Cost LB)

Маршрутизатор	Мережа призначення	К-сть шляхів	Наст. вузол 1 (IPv4)	Наст. вузол 2 (IPv4)	FD (метрика)	Розрахунок частки трафіку
R1						
R2						
R3						

11. Дослідити **нерівнометричне балансування навантаження (Unequal-Cost LB)**:

- відновити різні параметри **bandwidth** на каналах A і B (скинути попередні зміни);
- перевірити у таблиці топології наявність Feasible Successor (FS), що задовольняє Feasibility Condition (AD < FD);
- налаштувати команду **variance multiplier** згідно з варіантом (табл. 7.8);
- переконатися, що у таблиці маршрутизації з'явилися обидва маршрути командою **show ip route**;
- виконати розрахунок розподілу трафіку між маршрутами за формулою. Заповнити табл. 7.4.

Таблиця 7.4.

Результати дослідження нерівнометричного балансування навантаження (Unequal-Cost LB)

Мережа призначення	Successor FD	Вузол S	Feas. Succ. AD	Вузол FS	variance	Умова FS (AD<FD?)	Розрахункова частка трафіку (S : FS = FD_fs : FD_s)
Підмережа F від R1							
Підмережа D від R3							

12. Перевірити наскрізний зв'язок між усіма робочими станціями по IPv4 та IPv6 командами **ping** та **tracert** (traceroute).

13. Дослідити відмовостійкість: вимкнути один інтерфейс каналу A або B командою **shutdown**. Зафіксувати час збіжності EIGRP. Переконатися у збереженні зв'язку. Поновити інтерфейс командою **no shutdown**.

14. Дослідити роботу протоколу командами: **show ip eigrp interfaces**, **show ip eigrp topology all-links**, **show ip eigrp traffic**, **show ipv6 eigrp topology**, **show ipv6 route eigrp**, **debug eigrp packets** (короткочасно).

13. Вивести та проаналізувати файли конфігурацій усіх пристроїв мережі (**show running-config**).

14. У випадку виявлення помилок у налагодженнях – визначити причину та усунути їх.

15. Продемонструвати виконану роботу керівнику та оформити звіт.

ВАРІАНТИ ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Варіант визначається за номером стійки, за якою працюють студенти.

Таблиця 7.5.

Параметри IPv4-адресації

№ вар.	Підмережа A /30 (R1–R2)	Підмережа B /30 (R1–R3)	Підмережа C /30 (R2–R3)	Підмережа D /24 (LAN R1)	Підмережа E /24 (LAN R2)	Підмережа F /24 (LAN R3)
1	172.C.S.0	172.C.S.4	172.C.S.8	181.C.S.0	182.C.S.0	183.C.S.0
2	172.C.S.12	172.C.S.16	172.C.S.20	184.C.S.0	185.C.S.0	186.C.S.0
3	172.C.S.24	172.C.S.28	172.C.S.32	187.C.S.0	188.C.S.0	189.C.S.0
4	172.C.S.36	172.C.S.40	172.C.S.44	190.C.S.0	191.C.S.0	192.C.S.0
5	172.C.S.48	172.C.S.52	172.C.S.56	193.C.S.0	194.C.S.0	195.C.S.0
6	172.C.S.60	172.C.S.64	172.C.S.68	196.C.S.0	197.C.S.0	198.C.S.0
7	172.C.S.72	172.C.S.76	172.C.S.80	199.C.S.0	200.C.S.0	201.C.S.0
8	172.C.S.84	172.C.S.88	172.C.S.92	202.C.S.0	203.C.S.0	204.C.S.0
9	172.C.S.96	172.C.S.100	172.C.S.104	205.C.S.0	206.C.S.0	207.C.S.0
10	172.C.S.108	172.C.S.112	172.C.S.116	208.C.S.0	209.C.S.0	210.C.S.0
11	172.C.S.120	172.C.S.124	172.C.S.128	211.C.S.0	212.C.S.0	213.C.S.0
12	172.C.S.132	172.C.S.136	172.C.S.140	214.C.S.0	215.C.S.0	216.C.S.0
13	172.C.S.144	172.C.S.148	172.C.S.152	217.C.S.0	218.C.S.0	219.C.S.0
14	172.C.S.156	172.C.S.160	172.C.S.164	220.C.S.0	221.C.S.0	222.C.S.0
15	172.C.S.168	172.C.S.172	172.C.S.176	100.C.S.0	101.C.S.0	102.C.S.0
16	172.C.S.180	172.C.S.184	172.C.S.188	103.C.S.0	104.C.S.0	105.C.S.0
17	172.C.S.192	172.C.S.196	172.C.S.200	106.C.S.0	107.C.S.0	108.C.S.0
18	172.C.S.204	172.C.S.208	172.C.S.212	109.C.S.0	110.C.S.0	111.C.S.0
19	172.C.S.216	172.C.S.220	172.C.S.224	112.C.S.0	113.C.S.0	114.C.S.0
20	172.C.S.228	172.C.S.232	172.C.S.236	115.C.S.0	116.C.S.0	117.C.S.0

***Примітка*: C** (class) – номер аудиторії: для ауд. **107 – 71**, для ауд. **107a – 72, S** (stand) – номер стійки (зазначено зверху стійки).

УВАГА! В залежності від години проведення практики значення може змінюватись за вимогою керівника.

Таблиця 7.6.

Параметри IPv6-адресації

№ вар.	Підмережа A /64 (R1–R2)	Підмережа B /64 (R1–R3)	Підмережа C /64 (R2–R3)	Підмережа D /64 (LAN R1)	Підмережа E /64 (LAN R2)	Підмережа F /64 (LAN R3)
1	2001:DB8:71C:A::	2001:DB8:71C:B::	2001:DB8:71C:C::	2001:DB8:71C:D::	2001:DB8:71C:E::	2001:DB8:71C:F::
2	2001:DB8:72C:A::	2001:DB8:72C:B::	2001:DB8:72C:C::	2001:DB8:72C:D::	2001:DB8:72C:E::	2001:DB8:72C:F::
3	2001:DB8:73C:A::	2001:DB8:73C:B::	2001:DB8:73C:C::	2001:DB8:73C:D::	2001:DB8:73C:E::	2001:DB8:73C:F::
4	2001:DB8:74C:A::	2001:DB8:74C:B::	2001:DB8:74C:C::	2001:DB8:74C:D::	2001:DB8:74C:E::	2001:DB8:74C:F::
5	2001:DB8:75C:A::	2001:DB8:75C:B::	2001:DB8:75C:C::	2001:DB8:75C:D::	2001:DB8:75C:E::	2001:DB8:75C:F::
6	2001:DB8:76C:A::	2001:DB8:76C:B::	2001:DB8:76C:C::	2001:DB8:76C:D::	2001:DB8:76C:E::	2001:DB8:76C:F::
7	2001:DB8:77C:A::	2001:DB8:77C:B::	2001:DB8:77C:C::	2001:DB8:77C:D::	2001:DB8:77C:E::	2001:DB8:77C:F::
8	2001:DB8:78C:A::	2001:DB8:78C:B::	2001:DB8:78C:C::	2001:DB8:78C:D::	2001:DB8:78C:E::	2001:DB8:78C:F::
9	2001:DB8:79C:A::	2001:DB8:79C:B::	2001:DB8:79C:C::	2001:DB8:79C:D::	2001:DB8:79C:E::	2001:DB8:79C:F::
10	2001:DB8:7AC:A::	2001:DB8:7AC:B::	2001:DB8:7AC:C::	2001:DB8:7AC:D:	2001:DB8:7AC:E::	2001:DB8:7AC:F::

№ вар.	Підмережа A /64 (R1–R2)	Підмережа B /64 (R1–R3)	Підмережа C /64 (R2–R3)	Підмережа D /64 (LAN R1)	Підмережа E /64 (LAN R2)	Підмережа F /64 (LAN R3)
11	2001:DB8:7BC:A::	2001:DB8:7BC:B::	2001:DB8:7BC:C::	2001:DB8:7BC:D:	2001:DB8:7BC:E::	2001:DB8:7BC:F::
12	2001:DB8:7CC:A::	2001:DB8:7CC:B::	2001:DB8:7CC:C::	2001:DB8:7CC:D:	2001:DB8:7CC:E::	2001:DB8:7CC:F::
13	2001:DB8:7DC:A::	2001:DB8:7DC:B::	2001:DB8:7DC:C::	2001:DB8:7DC:D:	2001:DB8:7DC:E::	2001:DB8:7DC:F::
14	2001:DB8:7EC:A::	2001:DB8:7EC:B::	2001:DB8:7EC:C::	2001:DB8:7EC:D:	2001:DB8:7EC:E::	2001:DB8:7EC:F::
15	2001:DB8:7FC:A::	2001:DB8:7FC:B::	2001:DB8:7FC:C::	2001:DB8:7FC:D:	2001:DB8:7FC:E::	2001:DB8:7FC:F::
16	2001:DB8:80C:A::	2001:DB8:80C:B::	2001:DB8:80C:C::	2001:DB8:80C:D:	2001:DB8:80C:E::	2001:DB8:80C:F::
17	2001:DB8:81C:A::	2001:DB8:81C:B::	2001:DB8:81C:C::	2001:DB8:81C:D:	2001:DB8:81C:E::	2001:DB8:81C:F::
18	2001:DB8:82C:A::	2001:DB8:82C:B::	2001:DB8:82C:C::	2001:DB8:82C:D:	2001:DB8:82C:E::	2001:DB8:82C:F::
19	2001:DB8:83C:A::	2001:DB8:83C:B::	2001:DB8:83C:C::	2001:DB8:83C:D:	2001:DB8:83C:E::	2001:DB8:83C:F::
20	2001:DB8:84C:A::	2001:DB8:84C:B::	2001:DB8:84C:C::	2001:DB8:84C:D:	2001:DB8:84C:E::	2001:DB8:84C:F::

Таблиця 7.7.

Типи фізичних з'єднань між маршрутизаторами

№ вар.	Канал A: R1 – R2	Канал B: R1 – R3	Канал C: R2 – R3
1	Ethernet	Ethernet	Ethernet
2	Ethernet	Serial V.35	Ethernet
3	Serial V.35	Ethernet	Ethernet
4	Serial V.35	Serial V.35	Ethernet
5	Ethernet	Ethernet	Serial V.35
6	Serial V.35	Ethernet	Serial V.35
7	Ethernet	Serial V.35	Serial V.35
8	Serial V.35	Ethernet	Serial V.35
9	Ethernet	Ethernet	Ethernet
10	Serial V.35	Ethernet	Serial V.35
11	Ethernet	Serial V.35	Ethernet
12	Serial V.35	Serial V.35	Ethernet
13	Ethernet	Ethernet	Serial V.35
14	Serial V.35	Ethernet	Ethernet
15	Ethernet	Serial V.35	Ethernet
16	Serial V.35	Ethernet	Serial V.35
17	Ethernet	Serial V.35	Serial V.35
18	Serial V.35	Serial V.35	Ethernet
19	Ethernet	Ethernet	Ethernet
20	Ethernet	Serial V.35	Serial V.35

Таблиця 7.8.

Параметри налагодження протоколу EIGRP та балансування навантаження

№ вар.	ASN	Router-ID R1	Router-ID R2	Router-ID R3	Clock rate, біт/с	BW канал A, Кбіт/с	BW канал B, Кбіт/с	Delay канал A, мкс	variance
1	10	1.1.1.1	2.2.2.2	3.3.3.3	64000	1544	512	20000	3
2	20	4.4.4.4	5.5.5.5	6.6.6.6	128000	512	1544	20000	3
3	30	7.7.7.7	8.8.8.8	9.9.9.9	256000	1544	1544	20000	2
4	40	10.10.10.10	11.11.11.11	12.12.12.12	512000	512	512	20000	1
5	50	13.13.13.13	14.14.14.14	15.15.15.15	1024000	1544	512	20000	3
6	60	16.16.16.16	17.17.17.17	18.18.18.18	2048000	512	1544	20000	3
7	70	19.19.19.19	20.20.20.20	21.21.21.21	64000	1544	1544	20000	1
8	80	22.22.22.22	23.23.23.23	24.24.24.24	128000	1544	512	20000	3
9	90	25.25.25.25	26.26.26.26	27.27.27.27	256000	512	1544	20000	3
10	100	28.28.28.28	29.29.29.29	30.30.30.30	512000	1544	1544	20000	1
11	10	31.31.31.31	32.32.32.32	33.33.33.33	1024000	512	512	20000	1
12	20	34.34.34.34	35.35.35.35	36.36.36.36	2048000	1544	512	20000	3
13	30	37.37.37.37	38.38.38.38	39.39.39.39	64000	512	1544	20000	3
14	40	40.40.40.40	41.41.41.41	42.42.42.42	128000	1544	1544	20000	1
15	50	43.43.43.43	44.44.44.44	45.45.45.45	256000	1544	512	20000	3
16	60	46.46.46.46	47.47.47.47	48.48.48.48	512000	512	1544	20000	3
17	70	49.49.49.49	50.50.50.50	51.51.51.51	1024000	1544	1544	20000	1
18	80	52.52.52.52	53.53.53.53	54.54.54.54	2048000	512	512	20000	1
19	90	55.55.55.55	56.56.56.56	57.57.57.57	64000	1544	512	20000	3
20	100	58.58.58.58	59.59.59.59	60.60.60.60	128000	512	1544	20000	3

ЗМІСТ ЗВІТУ З ЗАНЯТТЯ

Звіт з заняття повинен містити:

1. Номер, тему та мету заняття.

2. Короткі теоретичні відомості (2–3 сторінки): гібридні протоколи маршрутизації; EIGRP – алгоритм DUAL, таблиці, метрика; EIGRP для IPv6 та його відмінності; балансування навантаження (equal-cost та unequal-cost), формула розрахунку частки трафіку; DHCP relay; пасивні інтерфейси.

3. Перелік використаного обладнання та програмного забезпечення.

4. Схему (ФОТО) побудованої мережі з позначенням усіх пристроїв та інтерфейсів.

5. Розроблену схему IP-адресації у вигляді табл. 7.1 з конкретними значеннями IPv4 та IPv6.

6. Лістинги команд (скріншоти) з результатами виконання:

- налагодження IPv4 та IPv6-адресації на всіх інтерфейсах маршрутизаторів;
- команди активації **ipv6 unicast-routing** та налагодження EIGRP для IPv4 та IPv6 (включно з **eigrp router-id**, **no shutdown**, **passive-interface**);

- результати **show ip eigrp neighbors** та **show ipv6 eigrp neighbors** – заповнена табл. 7.2;
- результати **show ip eigrp topology** та **show ipv6 eigrp topology** з аналізом successor та feasible successor;
- результати **show ip route eigrp** та **show ipv6 route eigrp** з усіх маршрутизаторів;
- налагодження та результати рівнометричного балансування – заповнена табл. 7.3 з розрахунком;
- налагодження команди **variance** та результати нерівнометричного балансування – заповнена табл. 7.4 з розрахунком;
- налагодження DHCP-сервера та relay – результати **show ip dhcp binding**, ipconfig /all на WS;
- результати ping та tracert по IPv4 та IPv6;
- вміст **running-config** усіх маршрутизаторів.

7. Опис проблем, що виникли під час виконання завдання, та шляхи їх усунення.

8. Висновки по заняттю.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Протокол маршрутизації EIGRP: загальна характеристика та алгоритм DUAL

EIGRP (Enhanced Interior Gateway Routing Protocol) – удосконалений протокол внутрішньої маршрутизації, розроблений компанією Cisco і стандартизований у RFC 7868. Протокол класифікується як гібридний (Advanced Distance-Vector), оскільки поєднує переваги обох класів: обмін маршрутною інформацією лише з безпосередніми сусідами (як дистанційно-векторні протоколи) та зберігання таблиці топології з миттєвими частковими оновленнями (як протоколи стану каналів). Основою EIGRP є алгоритм DUAL (Diffusing Update Algorithm), що гарантує петле-вільну збіжність без тимчасового зберігання маршрутів у петлях. [Odom W. CCNA 200-301 Official Cert Guide. Cisco Press, 2020]

EIGRP підтримує три окремі таблиці даних:

- **Таблиця сусідства (Neighbor Table)** – містить записи про всі маршрутизатори, з якими встановлено відносини сусідства. Для кожного сусіда зберігаються: IP-адреса (або link-local для IPv6), інтерфейс, час до закінчення таймера Hold, SRTT (Smooth Round-Trip Time), RTO (Retransmission Timeout).
- **Таблиця топології (Topology Table)** – містить всі відомі маршрути до кожної мережі: як оптимальний (successor), так і запасні (feasible successor). Алгоритм DUAL обробляє цю таблицю для прийняття маршрутних рішень без ризику петель.
- **Таблиця маршрутизації (Routing Table)** – містить лише оптимальні маршрути (successor-маршрути), що обрані алгоритмом DUAL для пересилання трафіку.

Алгоритм DUAL оперує двома ключовими поняттями метрики:

- **FD (Feasible Distance)** – мінімально відома метрика від поточного маршрутизатора до мережі призначення (відстань найкращого маршруту, що занесений у таблицю маршрутизації);
- **AD або RD (Advertised/Reported Distance)** – метрика, яку сусідній маршрутизатор рекламує для досягнення мережі призначення (відстань маршруту з точки зору сусіда).

Маршрут через вузол з найменшою метрикою отримує статус **Successor (S)** і встановлюється у таблицю маршрутизації. Маршрут через альтернативний вузол, що задовольняє **Feasibility Condition (FC)**, отримує статус **Feasible Successor (FS)** і зберігається у таблиці топології як резерв.

Умова Feasibility Condition (FC): **AD_FS < FD_successor**. Якщо AD маршруту через запасний вузол менше, ніж FD найкращого маршруту, – цей запасний маршрут гарантовано не утворює петлю. При відмові основного маршруту EIGRP миттєво переключається на Feasible Successor без запуску повного обчислення (без DUAL Active State).

Якщо Feasible Successor відсутній, маршрут переходить у стан **Active (A)**, і маршрутизатор розсилає **Query-повідомлення** сусідам у пошуку альтернативного шляху. Час збіжності у цьому випадку більший.

Розрахунок метрики EIGRP

Метрика протоколу EIGRP є комплексною і розраховується за спеціально розробленою фахівцями формулою, яка використовує наступні параметри:

- пропускні здатності інтерфейсів (каналів зв'язку);
- затримки інтерфейсів;
- параметри надійності інтерфейсів;
- завантаження інтерфейсів.

У загальному випадку формула розрахунку метрики протоколу EIGRP має наступний вигляд:

$$M = \left[\left(K_1 \cdot BW + \frac{K_2 \cdot BW}{256 - L} + K_3 \cdot D\right) \cdot \frac{K_5}{K_4 + R}\right] \cdot 256, \qquad (1)$$

де M – метрика певного маршруту;

BW (*BandWidth*) – безрозмірне значення пропускної здатності, яке розраховується за формулою (2);

L (*Load*) – завантаження інтерфейсу (від 1 до 255, 1 – відсутність передачі, 255 – повне завантаження інтерфейсу); визначається для поточного стану інтерфейсу;

D (*Delay*) – безрозмірне значення сумарної затримки для всіх ділянок певного маршруту, яке розраховується за формулою (3);

R (*Reliability*) – надійність інтерфейсу (від 1 до 255, 1 – ненадійний зв'язок, 255 – надійний зв'язок); визначається для поточного стану інтерфейсу;

K_1, K_2, K_3, K_4, K_5 – вагові коефіцієнти для розрахунку метрики, які можуть набувати значень 0 або 1;

Число 256 застосовується у формулі для розширення отриманого значення метрики до 32 бітів.

$$BW = \left[\frac{10^7}{\min(BW_1,\ldots,BW_N)}\right], \quad (2)$$

де BW_i – значення пропускної здатності i-ї ділянки маршруту, Кбіт/с; за замовчуванням дорівнює фізичній пропускній здатності інтерфейсу, може змінюватися адміністративно;

N – кількість ділянок маршруту.

$$D = \sum_{i=1}^{N}\left[\frac{D_i}{10}\right], \quad (3)$$

де D_i – значення затримки для i-ї ділянки маршруту, мкс; для кожного типу інтерфейсу встановлені стандартні значення затримок (див. табл. 7.8), може змінюватися адміністративно;

N – кількість ділянок маршруту.

Таблиця 7.9.

Стандартні значення пропускної здатності та затримок для основних типів інтерфейсів

Тип інтерфейсу	Пропускна здатність, Кбіт/с	Затримка, мкс
Gigabit Ethernet	1 000 000	10
Fast Ethernet	100 000	100
Ethernet 10 Мбіт/с	10 000	1 000
Serial T1	1 544	20 000
Serial E1	2 048	20 000
Serial DS0 (64 Кбіт/с)	64	20 000
Tunnel	9	50 000

За замовчуванням коефіцієнти K у формулі (1) набувають значень: $K_1 = 1$, $K_2 = 0$, $K_3 = 1$, $K_4 = 0$, $K_5 = 0$. Відповідно формула (1) спрощується і виглядає як

$$EIGRP_{Metric} = [BW + D] \cdot 256, \quad (4)$$

Приклад розрахунку: маршрут R1 → R2 → мережа A (дві ділянки: Serial T1 + FastEthernet).

$$BW = \left[\frac{10^7}{\min(1544, 100000)}\right] = \frac{10^7}{1544} \approx 6476;$$

$$D = \frac{(20000 + 100)}{10} = 2010;$$

$$M = 256 \cdot (6476 + 2010) = 2172416;$$

EIGRP для IPv6: архітектура, особливості налагодження та порівняння з IPv4

Протокол EIGRP для IPv6 (EIGRPv6) визначено у RFC 7868. Принцип роботи алгоритму DUAL, структура таблиць (сусідства, топології, маршрутизації) та механізми балансування навантаження повністю ідентичні IPv4-версії. Проте архітектура налагодження принципово відрізняється за кількома аспектами.

Порівняння характеристик EIGRP для IPv4 та IPv6 представлено в табл. 7.10.

Таблиця 7.10.

Порівняльна характеристика EIGRP для IPv4 та IPv6

Параметр	EIGRP для IPv4	EIGRP для IPv6
Активація протоколу	router eigrp ASN (глобальний режим конфігурування)	ipv6 router eigrp ASN (глобальний режим конфігурування)
Оголошення мереж	network address wildcard (у режимі router eigrp)	ipv6 eigrp ASN (безпосередньо на інтерфейсі)
Router ID	Автоматично (найвища IPv4-адреса) або вручну	Обов'язково вручну: eigrp router-id A.B.C.D (у форматі IPv4)
Стан процесу за замовчуванням	Активний після router eigrp	Вимкнений! Потребує no shutdown у режимі ipv6 router eigrp
Адреси для Hello	Multicast 224.0.0.10	Multicast FF02::A (All EIGRP Routers)
Ідентифікація сусідів	IPv4-адреса інтерфейсу	IPv6 Link-Local адреса (FE80::/10)
Пасивний інтерфейс	passive-interface у режимі router eigrp	passive-interface у режимі ipv6 router eigrp
Перевірка сусідства	show ip eigrp neighbors	show ipv6 eigrp neighbors
Таблиця маршрутизації	show ip route eigrp	show ipv6 route eigrp
Таблиця топології	show ip eigrp topology	show ipv6 eigrp topology

Ключова відмінність у налагодженні – активація EIGRP **безпосередньо на інтерфейсі**, а не через оголошення мереж командою **network**. Це пов'язано з тим, що в IPv6 відсутня концепція класових мереж та суміжних підмереж.

Повна послідовність налагодження EIGRP для IPv6:

…
Router(config)# ipv6 unicast-routing
Router(config)# ipv6 router eigrp 10
Router(config-rtr)# eigrp router-id 1.1.1.1
Router(config-rtr)# no shutdown
Router(config-rtr)# passive-interface GigabitEthernet0/1
Router(config-rtr)# exit
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ipv6 eigrp 10
Router(config-if)# interface Serial0/0/0
Router(config-if)# ipv6 eigrp 10
Router(config-if)# interface GigabitEthernet0/1
Router(config-if)# ipv6 eigrp 10
…

Особливість використання link-local адрес: у таблиці сусідства IPv6 EIGRP відображаються link-local адреси сусідів (FE80::X), а не глобальні unicast. Це нормальна поведінка – link-local адреси використовуються для всього EIGRP-трафіку в межах сегмента (Hello, Update, Query, Reply, ACK).

Перевірка стану EIGRP для IPv6:

```
Router# show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(10)
H   Address              Interface    Hold Uptime   SRTT  RTO Q Seq
1   Link-local address:  Se0/0/0      14   00:03:21  12  200 0 11
    FE80::2
0   Link-local address:  Se0/0/1      12   00:03:45   5  200 0  9
    FE80::3
```

```
Router# show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(10)/ID(1.1.1.1)
P 2001:DB8:11C:1::/64, 1 successors, FD is 2172416
  via FE80::2 (2172416/28160), Serial0/0/0
P 2001:DB8:11C:2::/64, 1 successors, FD is 2172416
  via FE80::3 (2172416/28160), Serial0/0/1
```

Балансування навантаження в EIGRP: розрахунок та налагодження

EIGRP підтримує два режими балансування навантаження, що реалізовуються відповідно до принципів:

1. Рівнометричне балансування (Equal-Cost Load Balancing). За замовчуванням EIGRP розподіляє трафік між маршрутами з однаковою метрикою FD. Максимальна кількість рівнометричних шляхів задається командою maximum-paths *N* (за замовчуванням 4, максимум 32). Розподіл трафіку між N рівнометричними шляхами здійснюється рівномірно: кожен шлях отримує 1/*N* загального потоку пакетів.

Розрахункова формула частки трафіку для рівнометричного балансування:

$$Q_i = \frac{Q_{total}}{N}, \tag{5}$$

де Q_i – кількість пакетів через і-й маршрут; Q_{total} – загальна кількість пакетів; N – кількість рівнометричних шляхів.

2. Нерівнометричне балансування (Unequal-Cost Load Balancing). Активується командою **variance multiplier** (діапазон 1–128; за замовчуванням 1 → тільки рівнометричне балансування). Маршрут через Feasible Successor включається до таблиці маршрутизації та балансування, якщо виконуються дві умови:

- Умова 1 – Feasibility Condition: **AD_FS < FD_successor** (запасний маршрут гарантовано без петель);
- Умова 2 – Variance Condition: **FD_FS ≤ FD_successor × variance** (метрика запасного маршруту не більша за FD × множник).

Розподіл трафіку між маршрутами при нерівнометричному балансуванні здійснюється **обернено пропорційно до метрик**:

$$\frac{Q_S}{Q_{FS}} = \frac{FD_{FS}}{FD_S}, \tag{6}$$

де Q_S – частка трафіку через Successor; Q_{FS} – частка трафіку через Feasible Successor; FD_S – метрика Successor; FD_{FS} – метрика Feasible Successor.

Абсолютні значення часток:

$$Q_S = \frac{Q_{total} \cdot FD_{FS}}{(FD_S + FD_{FS})}; \tag{7}$$

$$Q_{FS} = \frac{Q_{total} \cdot FD_S}{(FD_S + FD_{FS})}. \tag{8}$$

Приклад: Router має два маршрути до підмережі.
Маршрут через R2 (Serial T1 + FastEthernet): FD_S = 2 172 416.
Маршрут через R3 (Serial 512 Кбіт/с + FastEthernet):
FD_{FS} = 256 · (19531 + 2010) = 5 514 496.

Перевірка *FC*: $AD_{FS} = 28\,160 < FD_S = 2\,172\,416$ ✓.

Перевірка **variance** = 3: $FD_{FS} = 5\,514\,496 \leq FD_S \cdot 3 = 6\,517\,248$ ✓ → маршрут включається.

Частка S : $FS = \frac{FD_{FS}}{FD_S} = \frac{30720}{2172416} \approx \frac{1}{70}$.

Команди налагодження нерівнометричного балансування:

…

Router(config)# router eigrp 10
Router(config-router)# variance 3
Router(config-router)# maximum-paths 4

…

Команди моніторингу та діагностики EIGRP

Таблиця 7.11.

Команди моніторингу та діагностики протоколу EIGRP

Команда	Призначення
show ip protocols	Активні протоколи, ASN, K-коефіцієнти, maximum-paths, variance, пасивні інтерфейси
show ip route eigrp	Таблиця маршрутизації (лише маршрути EIGRP IPv4)
show ip eigrp interfaces	Інтерфейси EIGRP: кількість сусідів, параметри черги та таймерів
show ip eigrp neighbors	Таблиця сусідства: адреси, інтерфейси, Hold, SRTT, RTO, кількість пакетів у черзі
show ip eigrp topology	Таблиця топології: стан (P/A), successor, FS, FD, AD
show ip eigrp topology all-links	Повна таблиця топології, включно з маршрутами без статусу FS
show ip eigrp topology A.B.C.D/prefix	Детальна інформація про конкретний префікс
show ip eigrp traffic	Статистика: Hello, Update, Query, Reply, ACK
show ipv6 protocols	Активні IPv6-протоколи маршрутизації
show ipv6 route eigrp	Таблиця маршрутизації (маршрути EIGRP IPv6)
show ipv6 eigrp neighbors	Таблиця сусідства IPv6 (link-local адреси)
show ipv6 eigrp topology	Таблиця топології EIGRP IPv6
debug eigrp packets	Пакети EIGRP (Hello, Update, Query, Reply, ACK)
debug eigrp fsm	Події алгоритму DUAL (finite state machine)
debug eigrp neighbors	Зміни відносин сусідства
undebug all	Вимкнення всіх дебагів
clear ip eigrp neighbors	Скидання відносин сусідства (ініціює повторну збіжність)

Рекомендована послідовність перевірки роботи протоколу EIGRP

Рекомендована послідовність перевірки після завершення налаштування наведена нижче. Для кожної команди показано характерний вивід та пояснення ключових полів.

1. Перевірка стану інтерфейсів та адресації.

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status     Protocol
GigabitEthernet0/0     192.168.1.1      YES manual up         up
GigabitEthernet0/1     192.168.2.254    YES manual up         up
Serial0/0/0            192.168.3.5      YES manual up         up
```

```
Router# show ipv6 interface brief
GigabitEthernet0/0     [up/up]
  FE80::1
  2001:DB8:11C:1::1
Serial0/0/0            [up/up]
  FE80::1
  2001:DB8:11C:2::1
```

Усі задіяні інтерфейси мають бути у стані up/up. Наявність IPv6 link-local адреси (FE80::) підтверджує коректне налагодження IPv6. Стан down/down – фізична проблема або **shutdown**; стан up/down на Serial – відсутність **clock rate** на DCE-стороні.

2. Перевірка встановлення відносин сусідства EIGRP (IPv4 та IPv6).

```
Router# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)
H  Address         Interface    Hold Uptime  SRTT  RTO  Q  Seq
1  192.168.1.2      Se0/0/0      13   00:04:21  12  200  0  14
0  192.168.1.6      Gi0/0        11   00:04:45   5  200  0  11
```

```
Router# show ipv6 eigrp neighbors
EIGRP-IPv6 Neighbors for AS(10)
H   Address              Interface    Hold Uptime   SRTT  RTO Q Seq
1   Link-local address:  Se0/0/0      14   00:04:21  12  200 0 11
    FE80::2
0   Link-local address:  Gi0/0        12   00:04:45   5  200 0  9
    FE80::3
```

Hold – час до закінчення таймера (15 с за замовчуванням). SRTT – середній час відповіді. Порожня таблиця IPv4 – різні ASN або відсутня команда **network**. Порожня таблиця IPv6 – відсутня команда **ipv6 eigrp ASN** на інтерфейсі або процес не активований командою **no shutdown**.

3. Аналіз таблиці топології та вибір successor / feasible successor.

```
Router# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(1.1.1.1)
P 192.168.1.0/24, 1 successors, FD is 2172416
    via 192.168.1.2 (2172416/28160), Serial0/0/0  <- Successor
    via 192.168.1.6 (30720/28160), Gi0/0          <- Feasible Successor
```

```
Router# show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(10)/ID(1.1.1.1)
P 2001:DB8:11C:1::/64, 1 successors, FD is 2172416
    via FE80::2 (2172416/28160), Serial0/0/0
```

Стан **P (Passive)** – маршрут стабільний. Стан **A (Active)** – маршрутизатор надіслав Query-повідомлення сусідам у пошуку нового маршруту. У дужках (*FD*/*AD*): перше – *FD* від поточного маршрутизатора, друге – *AD* від сусіда. Наявність Feasible Successor підтверджує виконання умови $AD < FD$, що гарантує миттєве переключення без повного перерахунку.

4. Перевірка таблиці маршрутизації.

```
Router# show ip route eigrp
D  192.168.1.0/24 [90/2172416] via 192.168.1.2, 00:04:21, Serial0/0/0
D  192.168.2.0/24 [90/2172416] via 192.168.1.2, 00:04:21, Serial0/0/0
                  [90/30720]   via 192.168.1.6, 00:04:45, Gi0/0
```

```
Router# show ipv6 route eigrp
D   2001:DB8:11C:1::/64 [90/2172416]
    via FE80::2, Serial0/0/0
D   2001:DB8:11C:2::/64 [90/2172416]
    via FE80::3, Serial0/0/1
```

Мітка *D* – маршрут EIGRP. [90/метрика] – адміністративна відстань 90 / *FD*. Наявність двох рядків **via** для однієї мережі підтверджує активне балансування. Якщо деякі підмережі відсутні – перевірити **network** (IPv4) або **ipv6 eigrp ASN** на відповідних інтерфейсах.

5. Перевірка параметрів балансування навантаження.

```
Router# show ip protocols
Routing Protocol is "eigrp 10"
  EIGRP-IPv4 Protocol for AS(10)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    Maximum path: 4
    Maximum metric variance 3
  Automatic Summarization: disabled
  Routing for Networks:
    192.168.1.0/30   192.168.1.4/30   191.168.2.0/24
  Passive Interface(s): GigabitEthernet0/1
```

Maximum path: 4 – до 4 рівнометричних шляхів. **Maximum metric variance 3** – нерівнометричне балансування активоване: враховуються маршрути з метрикою $\leq FD \cdot 2$. **Passive Interface(s)** – мають бути всі LAN-інтерфейси. **Automatic Summarization: disabled** – підтверджує **no auto-summary**.

6. Перевірка роботи DHCP-сервера та relay.

```
Router# show ip dhcp binding
IP address     Client-ID/HW address    Lease expiration    Type
192.168.1.1     0050.56ab.1234          Apr 30 2026 12:00   Automatic
192.168.2.1     0050.56ab.5678          Apr 30 2026 12:00   Automatic
192.168.3.1     0050.56ab.9abc          Apr 30 2026 12:00   Automatic
```

```
Router# show ip dhcp pool
Pool POOL_D:
  Leased addresses: 1
  Total addresses: 254
```

Наявність трьох записів підтверджує роботу DHCP-relay. Порожня таблиця при активних клієнтах – відсутня команда **ip helper-address** на Router, або DHCP-сервер не має маршруту до підмережі клієнта.

7. Перевірка наскрізного зв'язку по IPv4 та IPv6.

```
C:\> ping 192.168.3.1
Reply from 192.168.3.1: bytes=32 time=2ms TTL=126
C:\> ping -6 2001:DB8:11C:2::1
Reply from 2001:DB8:11C:2::1: bytes=32 time=3ms TTL=125
C:\> tracert 192.168.3.1
  1    1 ms   192.168.1.254
  2    2 ms   192.168.2.2
  3    2 ms   192.168.3.1
```

TTL=126 – пакет пройшов через 2 маршрутизатори (початкове TTL=128). При балансуванні навантаження маршрут **tracert** може відрізнятися між сеансами – це нормально і підтверджує роботу балансування.

8. Перевірка відмовостійкості мережі.

```
Router(config-if)# shutdown
%DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 192.168.2.2 is down: interface down
%DUAL-5-NBRCHANGE: EIGRP-IPv6 10: Neighbor FE80::2 is down: interface down
```

При наявності *FS* – переключення миттєве (<1 с). При відсутності *FS* – маршрут переходить в Active, надсилаються Query.

```
Router# show ip eigrp topology
```

Маршрут через відключений інтерфейс зникає, а зв'язок через резервний канал.

```
Router(config-if)# no shutdown
%DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 192.168.2.2 is up: new adjacency
%DUAL-5-NBRCHANGE: EIGRP-IPv6 10: Neighbor FE80::2 is up: new adjacency
```

Повідомлення **%DUAL-5-NBRCHANGE** інформує про зміну стану сусідства. Команда **debug eigrp packets** дозволяє в реальному часі спостерігати за обміном Update, Query та Reply повідомленнями під час збіжності. Не забути вимкнути командою **undebug all** після завершення спостереження.

Типові помилки при налагодженні EIGRP

1. Розбіжність ASN. Якщо на маршрутизаторах задано різні номери автономної системи, відносини сусідства не встановляться. Виявляється порожньою таблицею show ip eigrp neighbors.

2. Відсутність no auto-summary. У мережах з некласовою адресацією автосумаризація призводить до некоректних записів. Команда no auto-summary є обов'язковою.

3. Відсутність no shutdown для EIGRP IPv6. Процес IPv6 EIGRP за замовчуванням вимкнений. Без no shutdown відносини сусідства по IPv6 не встановляться.

4. Відсутність eigrp router-id для IPv6. Без явного Router ID процес IPv6 EIGRP не запуститься за відсутності IPv4-адрес. Завжди задавати router-id у форматі A.B.C.D.

5. Неправильне значення variance. Якщо маршрут через FS не потрапляє до таблиці маршрутизації – або variance занадто малий, або маршрут не є FS (AD ≥ FD). Перевірити командою show ip eigrp topology all-links.

6. Відсутність ipv6 unicast-routing. За замовчуванням IPv6-маршрутизація на Cisco IOS вимкнена. Без цієї команди пакети IPv6 не пересилаються.

7. Команда ipv6 eigrp не виконана на інтерфейсі. У EIGRP для IPv6 протокол активується безпосередньо на інтерфейсі. Якщо команду пропустити – інтерфейс не бере участі у маршрутизації.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. До якого класу протоколів маршрутизації належить EIGRP? Назвіть три ключові характеристики, що відрізняють його від чисто дистанційно-векторних та протоколів стану каналів.
2. Що таке алгоритм DUAL? У чому полягає принцип «петле-вільної збіжності» та як він пов'язаний з поняттям Feasible Successor?
3. Перелічіть три таблиці EIGRP. Яку інформацію зберігає кожна з них? Що відбувається з таблицею маршрутизації при переході маршруту у стан Active?
4. Що таке Feasible Distance (FD) та Advertised Distance (AD)? Як вони використовуються алгоритмом DUAL для вибору Successor та Feasible Successor?
5. Сформулюйте Feasibility Condition. Чому виконання цієї умови гарантує відсутність петель маршрутизації?
6. Запишіть повну та спрощену формули розрахунку метрики EIGRP. Які параметри інтерфейсу впливають на метрику за замовчуванням?
7. Яка адміністративна відстань внутрішніх та зовнішніх маршрутів EIGRP? Порівняйте зі значеннями OSPF та RIP.
8. Перелічіть чотири принципові відмінності у налагодженні EIGRP для IPv6 порівняно з IPv4. Чому оголошення мереж виконується на інтерфейсі, а не командою network?
9. Навіщо потрібна команда eigrp router-id при налагодженні EIGRP для IPv6? Чому без неї процес може не запуститися?
10. Навіщо потрібна команда no shutdown при налагодженні EIGRP для IPv6? Чому для IPv4 вона не є обов'язковою?
11. Яку адресу використовує EIGRP для IPv6 для ідентифікації сусідів у таблиці сусідства? Яка multicast-адреса використовується для розсилки Hello-повідомлень?
12. Що таке Equal-Cost Load Balancing в EIGRP? Яку команду використовують для збільшення кількості рівнометричних шляхів? Запишіть формулу розрахунку частки трафіку.
13. Поясніть принцип Unequal-Cost Load Balancing. Яку команду слід використати для його активації? Запишіть дві умови, що мають виконуватися для маршруту, який бере участь у нерівнометричному балансуванні.
14. Що таке пасивний інтерфейс в EIGRP? Яка різниця між passive-interface та відсутністю ipv6 eigrp на інтерфейсі (для IPv6)? Чому LAN-інтерфейси рекомендується налагоджувати як пасивні?
16. Що покаже команда show ip eigrp topology all-links на відміну від show ip eigrp topology? У яких випадках необхідно використовувати all-links?
17. Якими командами перевіряють коректність налагодження Unequal-Cost LB? Як інтерпретувати виведення show ip route при наявності двох маршрутів з різними метриками?

ЗАНЯТТЯ 8

ДОСЛІДЖЕННЯ ТА НАЛАГОДЖЕННЯ ПРОТОКОЛУ ДИНАМІЧНОГО РЕЗЕРВУВАННЯ ШЛЮЗУ HSRP У МЕРЕЖІ НА БАЗІ МАРШРУТИЗАТОРІВ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження протоколу динамічного резервування шлюзу HSRP (Hot Standby Router Protocol) на обладнанні Cisco; отримати практичні навички налагодження, моніторингу та діагностування роботи протоколу HSRP у мережі, побудованій на базі маршрутизаторів Cisco; дослідити механізм виборів активного та резервного маршрутизаторів, стани протоколу та таймери; налаштувати функції Interface Tracking і Preempt; дослідити статичне балансування навантаження засобами MHSRP (Multiple HSRP); дослідити аутентифікацію HSRP та налаштувати DHCP-сервер з HSRP-шлюзом.

Обладнання та програмне забезпечення

Для виконання заняття на робочому місці студента має бути наявним таке обладнання та програмне забезпечення:

- Маршрутизатори Cisco серії 1841/2801/2811/2821/2901/2911/2921 з не менш ніж двома Ethernet-інтерфейсами – 3 шт.
- Керований комутатор Cisco серії Catalyst 2960 (WS-C2960-24TT-L або WS-C2960-48TT-L) – 1 шт.
- Робочі станції (ПК або ноутбуки) з операційною системою Windows/Linux – не менше 2 шт.
- Консольний кабель Cisco (rollover) з конектором RJ-45 та перехідником на USB або COM-порт – 1 шт.
- Ethernet-кабелі прямого типу (T568B) категорії Cat 5e/Cat 6 – не менше 7 шт.
- Термінальна програма-емулятор (PuTTY, Tera Term, SecureCRT або аналогічна) – встановлена на робочих станціях.

Схема підключення

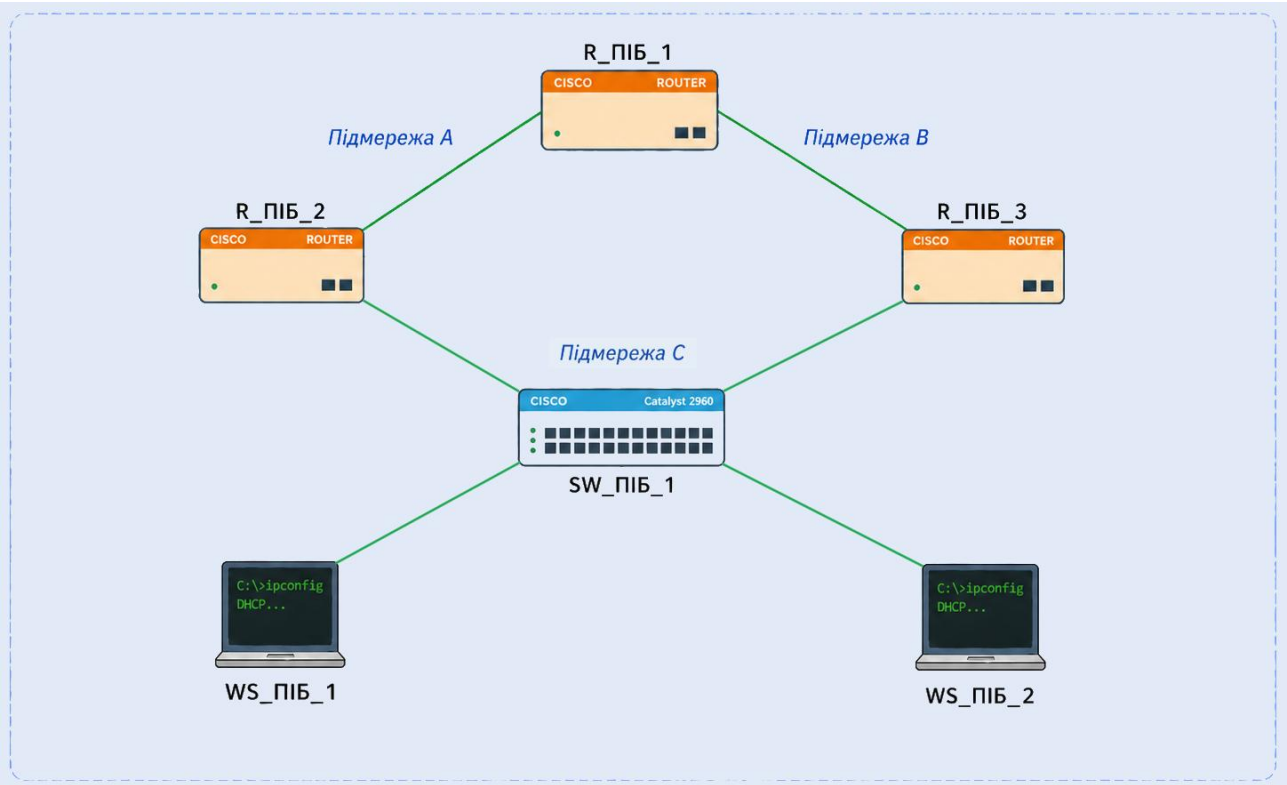

Рис. 8.1. Схема мережі HSRP, що будується у межах заняття

Примітка: ПІБ необхідно зазначати у скороченому форматі, який відповідає логіну для входу на платформу learn. Приклад: якщо логін для входу на learn – kb1_kmd, то назва маршрутизатора має бути у форматі R_kmd_1.

ЗАВДАННЯ

1. Ознайомитися з обладнанням та програмним забезпеченням робочого місця, перевірити наявність консольних і Ethernet-кабелів, термінальної програми.
2. Створити мережу відповідно до схеми на рис. 8.1. Маршрутизатори **R_ПІБ_2** та **R_ПІБ_3** підключити до комутатора **SW_ПІБ_1** – таким чином формується підмережа С (HSRP-сегмент), до якого підключаються також робочі станції WS_ПІБ_1 та WS_ПІБ_2. Маршрутизатор R_ПІБ_1 підключити до R_ПІБ_2 та R_ПІБ_3 через підмережі А та В відповідно; до HSRP-сегмента (підмережа С) маршрутизатор R_ПІБ_1 не підключається.
3. Провести налагодження іменування всіх пристроїв мережі (**R_ПІБ_1**, **R_ПІБ_2**, **R_ПІБ_3**, **SW_ПІБ_1**).
4. Розробити схему IP-адресації пристроїв мережі. Для цього скористатися даними табл. 8.5. Результати заповнити у табл. 8.1.

Таблиця 8.1.

Параметри адресації мережі

Мережа / Пристрій	Інтерфейс	MAC-адреса	IP-адреса	Маска	Префікс	Шлюз за замовчуванням
Підмережа A	–	–				–
Підмережа B	–	–				–
Підмережа C	–	–				–
Віртуальний шлюз HSRP (група 1)	–	(HSRP virtual)				–
Віртуальний шлюз HSRP (група 2)	–	(HSRP virtual)				–
R1	до R2					
	до R3					
R2	до R1					
	до SW1					
R3	до R1					
	до SW1					
SW1	Vlan 1					
WS1	NIC		(DHCP)			
WS2	NIC		(DHCP)			

5. Налаштувати IP-адресацію на всіх інтерфейсах маршрутизаторів та комутатора згідно з табл. 8.1. Перевірити стан інтерфейсів командою **show ip interface brief**. Перевірити зв'язок між безпосередньо приєднаними пристроями командою **ping**.

6. Налаштувати статичну маршрутизацію або протокол динамічної маршрутизації (за табл. 8.6) між підмережами A, B і C для забезпечення повного міжмережного зв'язку.

7. Налаштувати **DHCP-сервер** на R_ПІБ_1 для видачі IP-адрес робочим станціям WS_ПІБ_1 та WS_ПІБ_2. Оскільки R_ПІБ_1 не входить до HSRP-сегмента (підмережа C), на інтерфейсах R_ПІБ_2 та R_ПІБ_3 у підмережі C налаштувати ретрансляцію DHCP-запитів командою ip helper-address (вказати IP-адресу інтерфейсу R_ПІБ_1). Шлюзом за замовчуванням у DHCP-пулі вказати **віртуальну IP-адресу HSRP** (не фізичну адресу маршрутизатора). Перевірити отримання адрес командою **ipconfig /all** на WS.

8. Налаштувати **HSRP версія 2 (дві групи резервування)** на R_ПІБ_2 та R_ПІБ_3 для підмережі C (HSRP-сегмент). Параметри відповідно до варіанту (табл. 8.7):

- задати номер групи HSRP та версію протоколу командою **standby version 2**;
- задати віртуальну IP-адресу командою **standby [group] ip [virtual-ip]**;
- задати пріоритет командою **standby [group] priority [value]** згідно з варіантом;
- увімкнути функцію Preempt командою **standby [group] preempt** на маршрутизаторі з вищим пріоритетом;

- зафіксувати стан HSRP командами **show standby** та **show standby brief**. Визначити, який маршрутизатор став Active, який – Standby. Заповнити табл. 8.2.

Таблиця 8.2.

Результати дослідження стану HSRP (дві групи)

Маршрутизатор	Група HSRP	Роль (Active/Standby)	Пріоритет	Версія	Virtual IP	Virtual MAC	Hello / Hold, с
R2							
R3							

9. Дослідити **функцію Interface Tracking**:

- на маршрутизаторі-Active налаштувати відстеження зовнішнього інтерфейсу командою **standby [group] track [interface] [decrement]** з декрементом пріоритету згідно з варіантом (табл. 8.7);
- вимкнути зовнішній інтерфейс командою **shutdown** – переконатися, що пріоритет Active-маршрутизатора знизився і відбулися перевибори (Preempt). Зафіксувати повідомлення **%HSRP-6-STATECHANGE**;
- відновити інтерфейс командою **no shutdown** – переконатися у зворотньому переключенні. Заповнити табл. 8.3.

Таблиця 8.3.

Результати дослідження Interface Tracking та Preempt

Стан мережі	Active (R)	Standby (R)	Пріоритет Active	Пріоритет Standby	Повідомлення %HSRP-6	Зв'язок WS→WS
До відключення інтерфейсу (базовий стан)						
Після shutdown зовнішнього інтерфейсу на Active						
Після no shutdown (відновлення)						

10. Дослідити **аутентифікацію HSRP (MD5)**:

- на обох маршрутизаторах налаштувати аутентифікацію командою **standby [group] authentication md5 key-string [key]** з ключем згідно з варіантом (табл. 8.7);
- перевірити, що відносини HSRP збереглися (обидва маршрутизатори бачать одне одного);
- на одному з маршрутизаторів змінити ключ – переконатися, що Standby-маршрутизатор втрачає зв'язок з Active та переходить у стан Active самостійно (split-brain). Відновити правильний ключ.

11. Налаштувати **MHSRP (статичне балансування навантаження)** – дві групи резервування на підмережі С:

- Група 1 (за варіантом, табл. 8.7): R_ПІБ_2 – Active (вищий пріоритет), R_ПІБ_3 – Standby;
- Група 2 (за варіантом, табл. 8.7): R_ПІБ_3 – Active (вищий пріоритет), R_ПІБ_2 – Standby;
- На WS_ПІБ_1 задати шлюз = Virtual IP групи 1; на WS_ПІБ_2 задати шлюз = Virtual IP групи 2;

- Перевірити командами **show standby brief** на обох маршрутизаторах – впевнитися, що R_ПІБ_2 є Active для групи 1 і Standby для групи 2, і навпаки для R_ПІБ_3. Заповнити табл. 8.4.

Таблиця 8.4.

Результати налагодження MHSRP (дві групи – статичне балансування)

Група HSRP	Virtual IP	Active маршрутизатор	Пріоритет Active	Standby маршрутизатор	Пріоритет Standby	Шлюз для	show standby brief
1		R2		R3		WS1	
2		R3		R2		WS2	

12. Дослідити **зміну таймерів HSRP**:

- змінити Hello та Hold таймери командою **standby [group] timers [hello] [hold]** згідно з варіантом (табл. 8.7);
- перевірити застосування таймерів командою **show standby** (поле «Hello time»). Зафіксувати нові значення у табл. 8.2.

13. Дослідити **відмовостійкість** HSRP:

- відключити Active-маршрутизатор командою **shutdown** на інтерфейсі підмережі С;
- виконати **ping** з WS_ПІБ_1 – переконатися, що зв'язок відновився через Standby-маршрутизатор;
- зафіксувати час переключення (кількість втрачених ping-пакетів × інтервал). Відновити інтерфейс.

14. Дослідити роботу протоколу HSRP за допомогою діагностичних команд: **show standby**, **show standby brief**, **show standby all**, **debug standby** (короткочасно), **debug standby events**, **debug standby packets**.

15. Вивести та проаналізувати файли конфігурацій усіх пристроїв мережі.

16. Продемонструвати виконану роботу керівнику практики та оформити звіт за заняттям

ВАРІАНТИ ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Варіант визначається за номером стійки, за якою працюють студенти.

Таблиця 8.5.

Параметри IP-адресації мережі (варіанти)

№ вар.	Підмережа A (R1–R2)	Підмережа B (R1–R3)	Підмережа C (HSRP-сегм.)	Вірт. IP група 1	Вірт. IP група 2
1	172.C.S.0/30	172.C.S.4/30	10.C.S.0/24	10.C.S.254	10.C.S.253
2	172.C.S.8/30	172.C.S.12/30	10.C.S.0/24	10.C.S.30	10.C.S.29
3	172.C.S.16/30	172.C.S.20/30	10.C.S.0/24	10.C.S.62	10.C.S.61
4	172.C.S.24/30	172.C.S.28/30	10.C.S.0/24	10.C.S.94	10.C.S.93
5	172.C.S.32/30	172.C.S.36/30	10.C.S.0/24	10.C.S.126	10.C.S.125
6	172.C.S.40/30	172.C.S.44/30	10.C.S.0/24	10.C.S.158	10.C.S.157
7	172.C.S.48/30	172.C.S.52/30	10.C.S.0/24	10.C.S.190	10.C.S.189
8	172.C.S.56/30	172.C.S.60/30	10.C.S.0/24	10.C.S.222	10.C.S.221
9	172.C.S.64/30	172.C.S.68/30	10.C.S.0/24	10.C.S.254	10.C.S.253
10	172.C.S.72/30	172.C.S.76/30	10.C.S.0/24	10.C.S.30	10.C.S.29
11	172.C.S.80/30	172.C.S.84/30	10.C.S.0/24	10.C.S.62	10.C.S.61
12	172.C.S.88/30	172.C.S.92/30	10.C.S.0/24	10.C.S.94	10.C.S.93
13	172.C.S.96/30	172.C.S.100/30	10.C.S.0/24	10.C.S.126	10.C.S.125
14	172.C.S.104/30	172.C.S.108/30	10.C.S.0/24	10.C.S.158	10.C.S.157
15	172.C.S.112/30	172.C.S.116/30	10.C.S.0/24	10.C.S.190	10.C.S.189
16	172.C.S.120/30	172.C.S.124/30	10.C.S.0/24	10.C.S.180	10.C.S.179
17	172.C.S.128/30	172.C.S.132/30	10.C.S.0/24	10.C.S.58	10.C.S.57
18	172.C.S.136/30	172.C.S.140/30	10.C.S.0/24	10.C.S.48	10.C.S.47
19	172.C.S.144/30	172.C.S.148/30	10.C.S.0/24	10.C.S.24	10.C.S.23
20	172.C.S.152/30	172.C.S.156/30	10.C.S.0/24	10.C.S.112	10.C.S.111

***Примітка*: C** (class) – номер аудиторії: ауд. **107 → 71**, ауд. **107a → 72**; **S** (stand) – номер стійки (зазначено зверху стійки).

УВАГА! В залежності від часу проведення практики значення може змінюватись за вимогою керівника.

Таблиця 8.6.

Параметри налагодження протоколу маршрутизації

№ варіанту	1	2	3	4	5	6	7	8	9	10
Протокол маршрутизації	OSPF	EIGRP	RIP	STATIC	EIGRP	RIP	OSPF	STATIC	RIP	OSPF

Продовження табл. 8.6.

№ варіанту	11	12	13	14	15	16	17	18	19	20
Протокол маршрутизації	EIGRP	STATIC	OSPF	EIGRP	RIP	STATIC	EIGRP	RIP	OSPF	STATIC

Таблиця 8.7.

Параметри налагодження протоколу HSRP

№ вар.	HSRP група 1	Пріор. R2 (гр.1)	Пріор. R3 (гр.1)	HSRP група 2	Пріор. R2 (гр.2)	Пріор. R3 (гр.2)	Декр. Tracking	Hello/ Hold, с	MD5 ключ	Затримка Preempt, с
1	10	120	100	20	100	120	30	1/3	cisco8!	5
2	10	130	100	20	100	130	40	1/3	netkey2	5
3	10	120	90	20	90	120	40	2/6	pass123	10
4	10	150	100	20	100	150	60	1/3	hsrpkey	5
5	10	110	100	20	100	110	20	2/6	cisco8!	10
6	10	120	100	20	100	120	30	1/3	netkey2	5
7	10	130	100	20	100	130	40	2/6	pass123	5
8	10	150	90	20	90	150	70	1/3	hsrpkey	10
9	10	120	100	20	100	120	30	1/3	cisco8!	5
10	10	110	100	20	100	110	20	2/6	netkey2	5
11	10	130	100	20	100	130	40	1/3	pass123	10
12	10	120	90	20	90	120	40	2/6	hsrpkey	5
13	10	150	100	20	100	150	60	1/3	cisco8!	5
14	10	110	100	20	100	110	20	2/6	netkey2	10
15	10	130	100	20	100	130	40	1/3	pass123	5
16	10	120	100	20	100	120	30	2/6	hsrpkey	5
17	10	150	90	20	90	150	70	1/3	cisco8!	10
18	10	110	100	20	100	110	20	1/3	netkey2	5
19	10	130	100	20	100	130	40	2/6	pass123	5
20	10	120	90	20	90	120	40	1/3	hsrpkey	10

ЗМІСТ ЗВІТУ З ЗАНЯТТЯ

Звіт з заняття повинен містити:

1. Номер, тему та мету заняття.

2. Короткі теоретичні відомості (за власним конспектом, обсягом 2–3 сторінки): призначення та класифікація FHRP-протоколів; протокол HSRP – принцип роботи, стани, таймери, вибір Active/Standby; функції Interface Tracking та Preempt; MHSRP та статичне балансування навантаження; аутентифікація HSRP.

3. Перелік використаного обладнання та програмного забезпечення.

4. Схему (ФОТО) побудованої мережі з позначенням усіх пристроїв та інтерфейсів.

5. Розроблену схему IP-адресації у вигляді табл. 8.1 з конкретними значеннями.

6. Лістинги команд (або скріншоти) з результатами виконання:

- налагодження HSRP (включно з командами **standby ip**, **standby priority**, **standby preempt**, **standby track**, **standby authentication md5**);

- результати **show standby** та **show standby brief** – заповнена табл. 8.2;
- результати дослідження Interface Tracking – заповнена табл. 8.3;
- результати налагодження MHSRP – заповнена табл. 8.4;
- результати **ping** та **tracert** між WS_ПІБ_1 та WS_ПІБ_2 до та після відмови Active-маршрутизатора;
- фрагмент **debug standby events** під час перевиборів;
- вміст **running-config** усіх маршрутизаторів.

7. Опис проблем, що виникли під час виконання завдання, та шляхи їх усунення.

8. Висновки по заняттю.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Протоколи резервування першого переходу (FHRP)

У сучасних корпоративних мережах критичним компонентом є шлюз за замовчуванням – маршрутизатор, через який кінцеві вузли передають трафік у зовнішні мережі. Вихід з ладу єдиного шлюзу призводить до повної втрати зовнішнього зв'язку для всіх хостів підмережі. Протоколи резервування першого переходу (FHRP – First Hop Redundancy Protocols) вирішують цю проблему шляхом створення групи маршрутизаторів, що разом виступають як єдиний віртуальний шлюз з єдиною IP- та MAC-адресою, прозоро для кінцевих вузлів.

До найпоширеніших FHRP-протоколів належать:

- **HSRP (Hot Standby Router Protocol)** – фірмовий протокол Cisco, RFC 2281 (v1) та RFC 7734 (v2); найбільш поширений у мережах Cisco;
- **VRRP (Virtual Router Redundancy Protocol)** – відкритий стандарт IETF, RFC 5798; аналог HSRP для обладнання різних виробників;
- **GLBP (Gateway Load Balancing Protocol)** – фірмовий протокол Cisco з вбудованим динамічним балансуванням навантаження між усіма учасниками групи одночасно.

Загальна характеристика протоколу HSRP

Протокол HSRP (Hot Standby Router Protocol) розроблений компанією Cisco у 1997 р. для широкомовних мереж з множинним доступом (Ethernet). Основна ідея: група маршрутизаторів обирає один Active-маршрутизатор, який виконує функції шлюзу, та один Standby-маршрутизатор, готовий перебрати функції при відмові Active. Решта маршрутизаторів є запасними (Listen state). Для кінцевих вузлів підмережі вся група виглядає як єдиний віртуальний маршрутизатор з віртуальною IP-адресою та віртуальною MAC-адресою.

Ключові характеристики протоколу:

1. **Транспорт:** UDP, порт 1985 (v1), 1985/2029 (v2); групова адреса 224.0.0.2 (v1) або 224.0.0.102 (v2);
2. **Версії:** HSRPv1 підтримує до 256 груп, HSRPv2 – до 4096 груп і підтримує IPv6;

3. **Пріоритет:** діапазон 0–255, за замовчуванням 100; маршрутизатор з найбільшим пріоритетом стає Active; при рівних пріоритетах – порівнюються IP-адреси (більша стає Active);

4. **Таймери:** Hello Time – 3 с (за замовч.); Hold Time – 10 с (за замовч.); якщо Standby не отримує Hello протягом Hold Time – ініціює перевибори;

5. **Virtual MAC-адреса:** 0000.0C07.ACXX (v1), 0000.0C9F.FXXX (v2), де XX/XXX – номер групи HSRP.

Стани протоколу HSRP

Кожен маршрутизатор у процесі роботи HSRP послідовно проходить такі стани:

1. **Initial** – початковий стан після активації інтерфейсу або зміни параметрів HSRP;

2. **Learn** – маршрутизатор очікує отримання Hello від Active з метою дізнатися Virtual IP та значення таймерів;

3. **Listen** – маршрутизатор знає Virtual IP, але не є ні Active, ні Standby; прослуховує повідомлення Active та Standby;

4. **Speak** – маршрутизатор надсилає власні Hello, беручи участь у виборах Active та Standby;

5. **Standby** – маршрутизатор є резервним (другий за пріоритетом); постійно надсилає Hello для підтвердження своєї готовності;

6. **Active** – маршрутизатор виконує функції шлюзу: відповідає на ARP-запити за Virtual IP, пересилає пакети.

Діаграма переходів: при активації інтерфейсу → Initial → Learn (якщо Virtual IP невідома) → Listen → Speak → Standby або Active. При відмові Active-маршрутизатора: «Standby-маршрутизатор переходить у стан Active після спливання Hold Time (за замовчуванням 10 с) – саме стільки він чекає на Hello-повідомлення, перш ніж констатувати відмову сусіда. Додаткових виборів не потрібно: Standby вже відомий. Час перемикання можна скоротити до мілісекунд, зменшивши таймери командою standby timers msec.»

Функції Interface Tracking та Preempt

Interface Tracking – механізм моніторингу стану зовнішніх (uplink) інтерфейсів маршрутизатора. Якщо відстежуваний інтерфейс виходить з ладу, пріоритет HSRP-маршрутизатора автоматично знижується на задане значення (decrement, за замовч. 10). Це може призвести до зміни ролей, якщо пріоритет став нижчим за пріоритет Standby-маршрутизатора. При відновленні інтерфейсу пріоритет повертається до попереднього значення.

Preempt – функція, що дозволяє маршрутизатору з вищим пріоритетом «відібрати» роль Active у поточного Active-маршрутизатора. За замовчуванням Preempt вимкнений – маршрутизатор, що повернувся у мережу після відмови, навіть маючи вищий пріоритет, залишається у ролі Standby. Preempt обов'язково вмикати разом з Interface Tracking для коректної роботи механізму відновлення.

Команда налагодження:

…

Router(config-if)# standby 1 track GigabitEthernet0/0 30

Router(config-if)# standby 1 preempt delay minimum 5

…

MHSRP – статичне балансування навантаження

MHSRP (Multiple HSRP) – використання двох або більше груп HSRP на одному інтерфейсі для організації статичного балансування навантаження між маршрутизаторами. Кожна група має свою Virtual IP-адресу. Частина хостів підмережі налаштовується на шлюз = Virtual IP групи 1 (де R_ПІБ_2 є Active), інша частина – на шлюз = Virtual IP групи 2 (де R_ПІБ_3 є Active). При цьому обидва маршрутизатори одночасно виконують функції шлюзу для різних груп хостів. Кожна група має власний Standby-маршрутизатор – таким чином досягається і балансування, і резервування.

Приклад налагодження MHSRP:

1. Router1 – Active для групи 1, Standby для групи 2

…

Router1(config-if)# standby 1 ip 10.10.1.254

Router1(config-if)# standby 1 priority 120

Router1(config-if)# standby 1 preempt

Router1(config-if)# standby 2 ip 10.10.1.253

Router1(config-if)# standby 2 priority 100

…

2. Router2 – Active для групи 2, Standby для групи 1

…

Router2(config-if)# standby 1 ip 10.10.1.254

Router2(config-if)# standby 1 priority 100

Router2(config-if)# standby 2 ip 10.10.1.253

Router2(config-if)# standby 2 priority 120

Router2(config-if)# standby 2 preempt

…

Аутентифікація HSRP

HSRP підтримує два механізми аутентифікації для захисту від несанкціонованого підключення маршрутизаторів до групи резервування:

1. **Plaintext (відкритий текст)** – пароль передається у відкритому вигляді у Hello-повідомленнях (не рекомендований для продакшн-мереж);

2. **MD5** – хеш пароля; навіть перехоплення пакетів не дозволяє відновити ключ. Налагоджується командою **standby authentication md5 key-string KEY**. Маршрутизатори з різними ключами не встановлять відносини HSRP між собою. Обидва маршрутизатори повинні мати однаковий ключ.

…

Router1(config-if)# standby 1 authentication md5 key-string cisco8!

Router2(config-if)# standby 1 authentication md5 key-string cisco8!

…

Команди налагодження та моніторингу HSRP

Таблиця 8.8.

Команди налагодження, моніторингу та діагностики протоколу HSRP

Команда	Призначення
standby [gr] ip [vip]	Активація HSRP та задання Virtual IP-адреси групи
standby version {1|2}	Вибір версії протоколу (v2 підтримує більше груп та IPv6)
standby [gr] priority [0-255]	Задання пріоритету маршрутизатора у групі
standby [gr] preempt [delay min N]	Дозвіл на захоплення ролі Active при вищому пріоритеті
standby [gr] track INT [decrement]	Відстеження зовнішнього інтерфейсу; зниження пріоритету при відмові
standby [gr] timers H S	Зміна Hello (H) та Hold (S) таймерів у секундах
standby [gr] authentication md5 key-string KEY	Налагодження MD5-аутентифікації групи HSRP
standby [gr] name NAME	Текстове ім'я групи резервування
show standby	Детальна інформація про всі HSRP-групи: стан, пріоритет, таймери, Virtual IP/MAC
show standby brief	Коротка таблиця HSRP-груп: інтерфейс, група, пріоритет, Active, Standby, VIP
show standby all	Повна інформація з усіх інтерфейсів включно з параметрами аутентифікації
show standby delay	Затримки ініціалізації HSRP на інтерфейсах
debug standby	Увімкнути дебаг усіх подій HSRP
debug standby events	Дебаг подій зміни стану та пріоритету
debug standby packets	Дебаг пакетів Hello, Coup, Resign
debug standby terse	Скорочений дебаг (тільки значущі події)
undebug all	Вимкнути всі дебаги

Рекомендована послідовність перевірки роботи протоколу HSRP

Рекомендована послідовність перевірки після завершення налаштування наведена нижче. Для кожної команди показано характерний вивід та пояснення ключових полів.

1. Перевірка стану інтерфейсів.

```
Router1# show ip interface brief
GigabitEthernet0/0   10.10.1.2   YES manual up   up
GigabitEthernet0/1   192.168.1.2  YES manual up   up
```

Усі інтерфейси мають бути у стані up/up. Стан up/down означає відсутність кабелю або проблему на протилежному кінці.

2. Перевірка стану HSRP (коротка форма).

```
Router1# show standby brief
                     P indicates configured to preempt.
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Gi0/0       1    120 P Active  local           10.10.1.3       10.10.1.254
Gi0/0       2    100   Standby 10.10.1.3       local           10.10.1.253
```

Стовпець State: **Active** – маршрутизатор є активним шлюзом; **Standby** – резервний, готовий перейняти функції. Символ **P** у стовпці Pri – Preempt увімкнений. «local» у стовпці Active/Standby означає, що цей маршрутизатор і є Active або Standby відповідно.

3. Детальна перевірка HSRP.

```
Router1# show standby GigabitEthernet0/0 1
GigabitEthernet0/0 - Group 1 (version 2)
  State is Active
    4 state changes, last state change 00:05:23
  Virtual IP address is 10.10.1.254
  Active virtual MAC address is 0000.0C9F.F001
    Local virtual MAC address is 0000.0C9F.F001 (v2 default)
  Hello time 1 sec, hold time 3 sec
  Next hello sent in 0.608 secs
  Preemption enabled, delay min 5 secs
  Active router is local
  Standby router is 10.10.1.3, priority 100 (expires in 2.848 sec)
  Priority 120 (configured 120)
    Track interface GigabitEthernet0/1 state Up decrement 30
  Authentication MD5, key-string
  Group name is "hsrp-Gi0/0-1" (default)
```

Поле «State is Active» – підтверджує роль. **Virtual IP/MAC** – адреси, на які відповідає Active-маршрутизатор. **Hello time / hold time** – таймери, що мають збігатися на обох маршрутизаторах. **Track interface** – відстежуваний інтерфейс та величина декременту пріоритету.

4. Перевірка відмовостійкості.

```
Router1(config-if)# shutdown
%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 1 state Active -> Speak
%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 1 state Speak -> Standby

На R2:
%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 1 state Standby -> Active
```

Повідомлення **%HSRP-6-STATECHANGE** підтверджує зміну ролей. Час між відключенням інтерфейсу і повідомленням Active на R_ПІБ_3 = Hold Time (за замовч. 10 с). Зменшення таймерів **standby timers msec 200 msec 600** дозволяє скоротити час перемикання до <1 с.

5. Перевірка наскрізного зв'язку через Virtual IP.

```
C:\> ping 10.71.1.254
Reply from 10.71.1.254: bytes=32 time=1ms TTL=255

C:\> arp -a
10.71.1.254    0000-0c9f-f001   dynamic
```

Успішний ping до Virtual IP підтверджує коректну роботу HSRP. ARP-таблиця хоста повинна містити Virtual MAC, а не фізичну MAC-адресу маршрутизатора. При переключенні Active → Standby Virtual MAC залишається незмінною, тому хосту не потрібно оновлювати ARP-кеш.

6. Перевірка MHSRP – обидві групи одночасно.

```
Router1# show standby brief
Interface   Grp  Pri P State   Active      Standby     Virtual IP
Gi0/0       1    120 P Active  local       10.10.1.3   10.10.1.254
Gi0/0       2    100   Standby 10.10.1.3   local       10.10.1.253
```

Router2 є Active для групи 1 і Standby для групи 2 одночасно. Аналогічно Router1 є Active для групи 2 і Standby для групи 1. Таким чином, WS1 (шлюз = 10.10.1.254) використовує R1, а WS2 (шлюз = 10.10.1.253) – R2.

Типові помилки при налагодженні HSRP

1. Розбіжність Virtual IP між маршрутизаторами групи. Якщо на R1 Virtual IP = 10.10.1.254, а на R2 – 10.10.1.253, вони не сформують спільну групу HSRP. Виявляється командою **show standby brief** – обидва маршрутизатори будуть у стані Active для різних адрес.

2. Відсутність Preempt при використанні Interface Tracking. Якщо Preempt вимкнений, маршрутизатор з відновленим зовнішнім інтерфейсом та вищим пріоритетом не поверне собі роль Active автоматично – мережа залишиться на субоптимальному маршруті. Preempt обов'язково вмикати на маршрутизаторі з вищим пріоритетом.

3. Неправильна версія HSRP (v1/v2 розбіжність). HSRPv1 і HSRPv2 використовують різні multicast-адреси (224.0.0.2 vs 224.0.0.102). Маршрутизатори з різними версіями не бачать Hello одне одного і обидва переходять у стан Active (split-brain). Перевірити командою **show standby** – рядок «version».

4. Розбіжність MD5-ключів аутентифікації. Маршрутизатори з різними ключами ігнорують Hello одне одного. Обидва переходять у стан Active для своєї групи. Виявляється через **debug standby packets** – повідомлення «authentication mismatch».

5. Недостатній декремент Interface Tracking. Якщо декремент менший за різницю пріоритетів, пониження пріоритету Active не призведе до перевиборів. Приклад: Active пріоритет 120, Standby – 100, декремент = 10 → після відмови Active стає 110, що більше 100 – перевиборів не відбудеться. Декремент повинен бути достатнім: **decrement > priority_Active - priority_Standby**.

6. Шлюз у DHCP-пулі вказує на фізичну IP замість Virtual IP. Якщо хост отримає фізичну IP-адресу маршрутизатора як шлюз – при відмові цього маршрутизатора хост втратить зв'язок, навіть якщо HSRP коректно переключило роль Active. Завжди вказувати **default-router VIRTUAL_IP** у DHCP-пулі.

7. IGMP Snooping заважає HSRP Hello. На деяких комутаторах IGMP Snooping може блокувати груповий трафік HSRP (224.0.0.102), якщо комутатор не знає, на які порти його пересилати. Рішення: або відключити IGMP Snooping командою **no ip igmp snooping** на комутаторі, або додати статичний маршрут для multicast-групи HSRP.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що таке FHRP? Перелічіть три найбільш поширені протоколи з цієї групи та вкажіть їх ключові відмінності.
2. Поясніть принцип роботи протоколу HSRP. Що таке Virtual IP і Virtual MAC? Навіщо вони потрібні?
3. Перелічіть стани протоколу HSRP та опишіть умови переходу між ними. Який стан є нормальним робочим для Active-маршрутизатора?
4. За яким алгоритмом відбуваються вибори Active та Standby маршрутизаторів у групі HSRP? Що відбувається при рівних пріоритетах?
5. Що таке таймери Hello Time та Hold Time? Які значення є за замовчуванням? Яким чином їх зміна впливає на час перемикання при відмові?
6. Поясніть призначення функції Interface Tracking. Чому недостатнього декременту може бути замало для ініціювання перевиборів?
7. Що таке функція Preempt? Чому її необхідно вмикати разом з Interface Tracking? Що станеться без Preempt після відновлення Active-маршрутизатора?
8. Чим відрізняється HSRP Version 1 від Version 2? Назвіть конкретні технічні відмінності (multicast-адреса, кількість груп, підтримка IPv6).
9. Що таке MHSRP? Як за його допомогою реалізується статичне балансування навантаження? Наведіть приклад з двома групами.
10. Яка різниця між балансуванням у MHSRP та GLBP? У чому обмеженість статичного балансування MHSRP?
11. Які механізми аутентифікації підтримує HSRP? Що відбудеться, якщо на двох маршрутизаторах задано різні MD5-ключі?
12. Якою командою налагоджується HSRP? Перелічіть обов'язкові та необов'язкові команди для базового налагодження.
13. Яку інформацію виводить команда show standby brief? Розшифруйте кожен стовпець у її виводі.
14. Чому у DHCP-пулі шлюз за замовчуванням має вказувати на Virtual IP HSRP, а не на фізичну адресу маршрутизатора?
15. Що таке split-brain у контексті HSRP? Через які помилки він виникає та як його виявити?
16. Яка Virtual MAC-адреса формується для групи HSRP 1 у версії 2? Запишіть формулу.
17. Яким чином HSRP взаємодіє з функцією IGMP Snooping на комутаторі? Яка проблема може виникнути і як її вирішити?
18. Якими командами дебагу можна спостерігати за процесом перевиборів Active/Standby у реальному часі?
19. Порівняйте HSRP та VRRP: спільні риси та відмінності у термінології, таймерах, адресах.
20. Якими способами можна зменшити час переключення HSRP при відмові Active-маршрутизатора нижче 1 секунди?

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про вищу освіту» від 01.07.2014 р. № 1556-VII.
2. Положення «Про проведення практики студентів вищих навчальних закладів України», затвердженого наказом МОН України від 08.04.1993 р. № 93.
3. ДСТУ 3008:2015 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ: ДП «УкрНДНЦ», 2016. – 31 с.
4. ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. – Київ: ДП «УкрНДНЦ», 2016. – 17 с.
5. Odom Wendell. CCNA 200-301 Official Cert Guide. Volume 1. / Wendell Odom. Cisco Press, 2020. – 1095 p.
6. Odom Wendell. CCNA 200-301 Official Cert Guide. Volume 2. / Wendell Odom. Cisco Press, 2020. – 774 p.
7. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 334 с.
8. Буров Є.В. Комп'ютерні мережі. Підручник. Том 2. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 204 с.
9. Єфіменко А.А. Основи побудови локальних комп'ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco: навч. посіб. – Житомир: ДУ «Житомирська політехніка», 2021. – 116 с.
10. Єфіменко А.А. Комп'ютерні мережі: методичні рекомендації для виконання лабораторних робіт. Ч. 1–3. – Житомир: ЖДТУ, 2017–2019.
11. Дячук О.Ю., Єфіменко А.А., Колощук М.С. Глобальні мережі: методичні рекомендації для виконання лабораторних робіт. – Житомир: Житомирська політехніка, 2025. – 192 с.
12. Huawei Technologies Co. S5700 Series Ethernet Switches Configuration Guide. – Shenzhen: Huawei, 2023.
13. Cisco Systems. Cisco IOS Configuration Fundamentals Command Reference. – San Jose: Cisco Press, 2022.
14. Навчальний курс CCNA: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.
15. Навчальний курс CCNA: Switching, Routing, and Wireless Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.
16. Комп’ютерні мережі : навч. посіб. [Електронний ресурс] / А.В.Чепинога, А.А.Єфіменко, К.С.Рудаков, А.О.Лавданський, Є.В.Ланських, Е.В.Фауре. – Житомир : Державний університет «Житомирська політехніка», 2025. – 386 с.

ДОДАТКИ

ДОДАТОК А

Зразок титульного аркуша звіту з технологічної практики

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

Кафедра комп'ютерної інженерії та кібербезпеки

ЗВІТ З ТЕХНОЛОГІЧНОЇ ПРАКТИКИ № 2

Студента (ки) _____ курсу групи _____
спеціальність 125 «Кібербезпека та захист інформації»

_____
(прізвище та ініціали студента)

Керівник практики від кафедри:

_____
(вчений ступінь, звання, прізвище та ініціали)

Житомир – 20ХХ

ДОДАТОК Б

Зразок сторінки щоденника практики

Дата	Найменування виконаних робіт	Підпис студента	Підпис керівника
	Заняття 1. Дослідження та налагодження агрегації каналів EtherChannel і Multilink PPP у мережах на базі обладнання Cisco.		

Відгук керівника практики:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Дата:_____ Підпис керівника: _____

_____