МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

ГЛОБАЛЬНІ МЕРЕЖІ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
ДЛЯ ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

Житомир
2025

УДК 681.324
К63

Рекомендовано до друку науково-методичною радою
Державного університету «Житомирська політехніка»
(протокол № 4 від 12 червня 2025 року)

Рецензенти:
В.В. Воротніков – доктор технічних наук, доцент
В. В. Чухов – кандидат технічних наук, доцент

К63 **Глобальні мережі** : методичні рекомендації для виконання лабораторних робіт. / підг. О.Ю. Дячук, А. А. Єфіменко, М.С. Колощук. – Житомир : Житомирська політехніка, 2025. – 192 с.

Методичні рекомендації містять теоретичний матеріал, приклади та вказівки для виконання лабораторних робіт, пов'язаних із вивченням питань адресації кінцевих вузлів.

Методичні рекомендації призначені для студентів, які навчаються за спеціальностями галузі знань 12 „Інформаційні технології".

Підготували: **О.Ю. Дячук,** кандидат технічних наук, доцент **А. А. Єфіменко, М.С. Колощук**.

УДК 681.324

ЗМІСТ

ВСТУП

Дані методичні рекомендації розроблені для студентів, які навчаються за спеціальностями галузі знань 12 „Інформаційні технології", для вивчення відповідного змістового модуля навчальної дисципліни „Глобальні мережі". Зазначена дисципліна згідно з освітньою програмою та навчальними планами підготовки бакалаврів належить до нормативної частини циклу дисциплін професійної і практичної підготовки.

Основним призначенням даного видання є: поглиблення теоретичних знань, отриманих студентами під час вивчення змістового модуля; набуття практичних навичок із налагодження, моніторингу та діагностики роботи кінцевих вузлів та комунікаційних пристроїв; набуття навичок дослідження процесів передачі даних у глобальних мережах під час використання різних мережних технологій, а також набуття навичок усунення проблем у ході роботи мережних пристроїв.

Для проведення лабораторних робіт, залежно від можливостей навчальних лабораторій, передбачається два альтернативних варіанти. Перший варіант – використання реального обладнання, другий – використання спеціалізованих програмних комплексів із комп'ютерної симуляції/емуляції роботи мережних вузлів і пристроїв та мереж у цілому. Вибір варіанта, обладнання та програмних комплексів покладається на викладача. Не виключається поєднання двох варіантів.

Особливістю даних методичних рекомендацій є: наявність у кожній лабораторній роботі необхідних теоретичних відомостей, пов'язаних із вивченням певної технології чи протоколу; наявність достатньо деталізованої довідкової інформації з питань налагодження та діагностики роботи мережних пристроїв, технологій та протоколів, а також наявність готових прикладів налагоджень пристроїв. Слід зазначити, що роботи виконуються індивідуально за варіантами. Вибір номера варіанта проводиться за списком групи. Під час іменування комунікаційних пристроїв, кінцевих вузлів, розрахунку параметрів та розподілу IP-адрес також використовується індивідуалізований підхід. Він полягає у тому, що у назвах пристроїв, IP-адресах мереж використовуються дві останні цифри номера групи (G) та дві цифри номера варіанта (N). Наприклад, IP-адреса мережі 192.G.N.0/24 для 12-ї групи та 25-го номера варіанта вигля-

датиме як 192.12.25.0/24. Додаткові параметри налагоджень також обираються відповідно до варіанта.

Повне виконання лабораторної роботи передбачає виконання таких етапів: ознайомлення з теоретичними відомостями; аналіз прикладу (сценарію) розрахунків та налагоджень; аналіз індивідуального варіанта завдання; підготовка інформації для налагодження пристроїв та з'єднань; виконання, за потреби, теоретичних розрахунків; проведення налагоджень мережних пристроїв та кінцевих вузлів; діагностика роботи побудованої мережі; визначення проблем у взаємодії вузлів та їх усунення; дослідження процесів передачі даних у побудованій мережі; формування висновків по роботі; оформлення та захист звіту; підготовка до подальших контрольних заходів.

Звіт із лабораторної роботи оформлюється згідно з вимогами Державного стандарту України ДСТУ 3008-95 „Документація. Звіти у сфері науки і техніки. Структура і правила оформлення", міжнародних стандартів ISO 5966:1982, ГОСТ 19.404 ЕСПД „Пояснительная записка. Требования к содержанию и оформлению" і повинен містити такі складові: номер роботи; тема роботи; мета роботи; розділ, у якому описано хід виконання роботи відповідно до пунктів завдання; висновки; додаток із лістингами налагоджень усіх комунікаційних пристроїв (за необхідності), рукописні відповіді на контрольні питання. Звіт виконується в електронному вигляді, роздруковується, доповнюється відповідями на контрольні питання і здається на кафедру для перевірки та захисту.

Під час оформлення звіту необхідно дотримуватися таких вимог: звіт оформлюється на аркушах формату А4 з рамками (перша сторінка – з кутовим штампом форми 2, решта сторінок – форми 2а за ГОСТ 2.104-68 ЕСКД. „Основные надписи"). Штампи заповнюються згідно з вимогами. Нумерація сторінок наскрізна в межах роботи. Поля для тексту: ліве – 25 мм, праве – 10 мм, верхнє – 20 мм від краю аркуша, нижнє – 10 мм від верхнього краю штампа. Текст роботи оформлюється шрифтом Times New Roman 14-го розміру, міжрядковий інтервал 1 – 1,5. Абзацний відступ 5 символів. Тексти сценаріїв налагоджень, лістингів конфігураційних файлів та інших елементів рекомендується оформлювати шрифтом Curier New, 10–12-го розміру, міжрядковий інтервал 1. Рекомендується у текстах сценаріїв та лістингів видаляти інформацію, яка не є значущою для виконання завдання або роботи. Ілюстрації та таблиці повинні роз-

міщуватися безпосередньо після тексту, де вони зустрічаються.

Ілюстрації (креслення, рисунки, схеми тощо) позначаються таким чином: „Рисунок № – Назва рисунка” (вирівнювання по центру, без абзацного відступу). Позначення ілюстрації виконується під ілюстрацією. Якщо кількість ілюстрацій значна і вони однотипні та невеликі за розміром, то їх рекомендується групувати в одну ілюстрацію, позначати літерами *а*), *б*) ... і підписувати їх як одну ілюстрацію.

Таблиці позначаються таким чином: „Таблиця № – Назва таблиці” (вирівнювання по лівому краю, без абзацного відступу). Їх нумерація здійснюється окремо і наскрізно у межах роботи. Позначення таблиці виконується над таблицею. Текст таблиць рекомендується оформлювати шрифтом New Roman 12-го розміру, міжрядковий інтервал 1. Якщо таблиця займає понад одну сторінку, то на другій і наступних сторінках ставиться позначення „Продовження табл. №”. Шапка таблиці повторюється в усіх її частинах.

У тексті звіту можна використовувати переліки (списки в термінології текстових редакторів). Перед перерахуванням ставиться двокрапка. Перед кожною позицією списку можна ставити тире, малу літеру українського алвафіту з дужкою, арабські цифри з дужкою. Елементи переліку пишуться з маленької літери, наприкінці ставиться крапка з комою, для останнього елемента – крапка.

Для оформлення додатка до роботи, який містить лістинги налагоджень комунікаційних пристроїв, допускається подання інформації у колонки. Слід звернути увагу на те, що лістинги налагоджень окремих пристроїв повинні бути підписані і відокремлені один від одного. Відповіді на контрольні питання оформлюються акуратно, чітким почерком, літерами достатнього для нормального сприйняття розміру. Їх оформлення слід починати з нового аркуша.

Важливо, щоб контрольні питання, які наводяться після кожної лабораторної роботи, були ретельно відпрацьованими студентом самостійно з метою підготовки до контрольних заходів, таких як тестування та вирішення практичних завдань.

Лабораторна робота № 1
ОСНОВИ РОБОТИ З МЕРЕЖНИМИ ПРИСТРОЯМИ CISCO З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ АДРЕСАЦІЇ IPv4 ТА IPv6

Мета заняття: Ознайомитися з основами роботи з мережними пристроями Cisco, вивчити принципи налаштування та діагностики інтерфейсів маршрутизаторів і комутаторів Cisco із використанням технологій адресації IPv4 та IPv6. Освоїти базові команди Cisco IOS для налаштування мережних інтерфейсів, перевірки їх працездатності та усунення можливих проблем у мережевій інфраструктурі.

Теоретичні відомості

Мережні інтерфейси та кабельні з'єднання Ethernet

Мережний інтерфейс (Network Interface) – фізичний (або віртуальний) пристрій, призначений для передавання даних у мережу та приймання даних із мережі. Мережний інтерфейс Ethernet – це фізичний пристрій, який є складовою кінцевого або проміжного вузла мережі. Цей інтерфейс забезпечує фізичне підключення вузла до середовища передачі даних та проводить інформаційний обмін з іншими вузлами мережі. Мережний інтерфейс Ethernet є пристроєм, що виконує фунції фізичного і канального (MAC-підрівень) рівнів моделі OSI. Стосовно стеку TCP/IP мережний інтерфейс Ethernet є пристроєм, що виконує фунції рівня мережних інтерфейсів. Прикладами мережних інтерфесів Ethernet є мережні адаптери/плати робочих станцій та серверів, порти комутаторів або точок доступу, мережні інтерфейси, плати та модулі маршрутизаторів тощо.

Відповідно до функцій рівнів моделі OSI мережний інтерфейс Ethernet фактично розглядається як сукупність фізичного і логічного інтерфейсів. Фізичний інтерфейс забезпечує фізичне підключення до середовища передачі даних та вирішує питання передавання/приймання сигналів. Логічний інтерфейс забезпечує опрацювання сукупності сигналів як повідомлень певного формату.

Згідно зі стандартом (ISO/IEC/IEEE 8802-3:2014 „Standard for Ethernet") для побудови кабельних з'єднань мереж Ethernet можуть застосовуватися такі фізичні середовища передачі даних, як коаксіальний кабель, вита пара, волоконно-оптичний кабель. У сучасній практиці побудови мереж коаксіальний кабель є застарілим середо-

вищем і майже не застосовується. Вита пара є основним середовищем, що застосовується для підключень пристроїв, які знаходяться на невеликих відстанях (до 100 м) один від одного. У сучасних мережах застосовується вита пара категорії 5е і вище. Волоконно-оптичний кабель є основним середовищем, що застосовується для підключень на великі відстані (сотні метрів і більше). У сучасних мережах застосовується як одномодовий, так і багатомодовий волоконно-оптичний кабель.

Для технологій Ethernet, які як середовище передачі даних застосовують 8-провідникову виту пару (Ethernet 10Base-T, Fast Ethernet 100Base-TX, Gigabit Ethernet 1000Base-T тощо) основним фізичним рознімом є 8-контактний рознім, відомий під назвою RJ-45 (Registered Jack). У деяких джерелах замість позначення RJ-45 рекомендується застосовувати більш коректне позначення 8P8C (8 Position 8 Contact). Зовнішній вигляд 8-позиційних модульної вилки та гнізда рознім RJ–45 наведено на рис. 1.

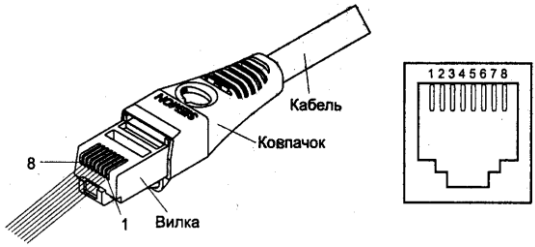


Рис. 1. Модульна вилка та гніздо рознім RJ–45

Слід зазначити, що гнізда рознім RJ–45 мережних адаптерів та комунікаційних пристроїв для забезпечення коректного використання полярності сигналів поділяються на два види:

– гнізда RJ–45 MDI (Media Dependent Interface);

– гнізда RJ–45 MDIX (Media Dependent Interface Xover= Crossover).

Призначення контактів та сигналів рознім RJ–45 технологій Ethernet 10Base-T, Fast Ethernet 100Base-TX та Gigabit Ethernet 1000Base-T для гнізд MDI/MDIX наведено у табл. 1. Типові гнізда рознім RJ–45 найпоширеніших мережних пристроїв Ethernet наведені у табл. 2.

Таблиця 1

Контакти та сигнали розніму RJ–45

Кон-	Технології 10Base-T/100Base-TX		Технологія 1000Base-T	
такт	MDI	MDIX	MDI	MDIX
1	Tx+ (Передавання+)	Rx+ (Приймання+)	BI_DA+	BI_DB+
2	Tx– (Передавання–)	Rx– (Приймання–)	BI_DA–	BI_DB–
3	Rx+ (Приймання+)	Tx+ (Передавання+)	BI_DB+	BI_DA+
4	Не задіяний	Не задіяний	BI_DC+	BI_DD+
5	Не задіяний	Не задіяний	BI_DC–	BI_DD–
6	Rx– (Приймання–)	Tx– (Передавання–)	BI_DB–	BI_DA–
7	Не задіяний	Не задіяний	BI_DD+	BI_DC+
8	Не задіяний	Не задіяний	BI_DD–	BI_DC–

Таблиця 2

Типові гнізда пристроїв технологій Ethernet для розніму RJ-45

Пристрій	Гніздо	Пристрій	Гніздо
Мережний адаптер (NIC)	MDI	Повторювач (Repeater)	MDIX
Маршрутизатор (Router)	MDI	Концентратор (Hub)	MDIX
Точка доступу (Access Point)	MDI	Міст (Bridge)	MDIX
IP-Телефон (IP-Phone)	MDI	Комутатор (Switch)	MDIX
VoIP шлюз (VoIP Gateway)	MDI	DSL-модем (DSL-Modem)	MDIX
Мережний принтер (Network Printer)	MDI	Кабельний модем (TV Cable Modem)	MDIX

У багатьох моделях концентраторів та комутаторів наявні додаткові порти RJ-45 „Up-Link”, що призначені для з’єднання пристроїв між собою, підключення концентратора чи комутатора до маршрутизатора тощо. Порти „Up-Link” типово є портами MDI. У деяких старих моделях концентраторів та комутаторів один із звичайних портів RJ-45 (зазвичай перший або останній) також може бути портом „Up-Link”, у цьому разі переключення між MDI/MDIX для порту здійснюється фізично за допомогою перемикача.

У варіантах технології Ethernet 10Base-T та Fast Ethernet 100Base-TX для забезпечення передачі даних застосовуються дві з наявних чотирьох пар провідників. Кожна з пар є окремим симплексним каналом передачі. По одній із пар передача здійснюється в одному напрямку, по іншій – у протилежному. Разом вони формують дуплексний канал передачі. У технології Gigabit Ethernet 1000Base-T застосовуються всі чотири пари провідників. По кожній парі передача здійснюється у двох напрямках одночасно.

З метою з'єднання порту MDI одного пристрою з портом MDIX іншого пристрою застосовується прямий кабель Ethernet (Ethernet Straight-Through Cable). З метою з'єднання двох пристроїв, які мають однакові порти (MDI–MDI чи MDIX–MDIX), застосовується перехресний кабель Ethernet (Ethernet Crossover Cable). Схеми з'єднання контактів розніму RJ-45 прямого та перехресного кабелів для технологій Ethernet 10Base-T та Fast Ethernet 100Base-TX наведені на рис. 2, а та рис. 2, б відповідно. Мінімальна рекомендована стандартом довжина кабелю Ethernet – 0,5 м. Максимальна можлива довжина – 100 м. Допускається використання кабелів більшої довжини (на 10–15%), при цьому необхідно контролювати якість та втрати сигналу. Для зручності підключення до пристроїв із метою адміністрування розроблено модульний адаптер-перехідник (Ethernet Crossover Adapter), який дає змогу „перетворити" прямий кабель Ethernet у перехресний.

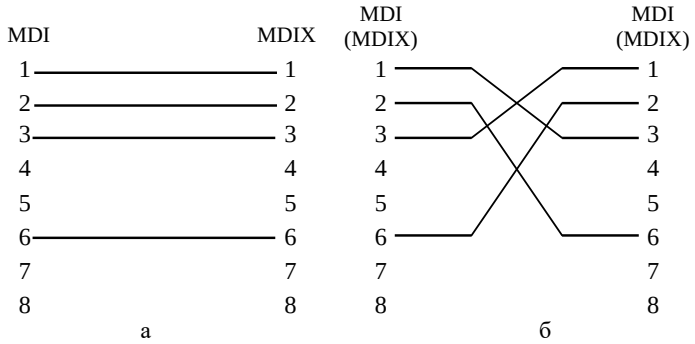


Рис. 2. Схеми кабелів Ethernet 10BaseT/ Fast Ethernet 100Base-TX:
а – прямий кабель; б – перехресний кабель

Вибір провідника витої пари за кольором для відповідного контакту вилки RJ-45 прямого чи перехресного кабелю Ethernet визначається вимогами стандарту побудови структурованих кабельних мереж у комерційних будівлях TIA-568 „Commercial Building Telecommunications Cabling Standard Set". У цьому стандарті описано два варіанти використання кольорів – так звані монтажні схеми (таблиці, „розкладки") T568A та T568B. Параметри цих схем наведені у табл. 3. Найпоширенішою сьогодні є монтажна схема T568B.

Таблиця 3

Параметри монтажних схем T568A та T568B

Контакт	Монтажна схема T568A		Монтажна схема T568B	
	Колір: основний/смужки	Номер пари	Колір: основний/смужки	Номер пари
1	Білий/зелений	3 (Tip – прямий)	Білий/помаранчевий	2 (Tip – прямий)
2	Зелений	3 (Ring – зворотний)	Помаранчевий	2 (Ring – зворотний)
3	Білий/помаранчевий	2 (Tip)	Білий/зелений	3 (Tip)
4	Помаранчевий	1 (Ring)	Синій	1 (Ring)
5	Білий/синій	1 (Tip)	Білий/синій	1 (Tip)
6	Синій	2 (Ring)	Зелений	3 (Ring)
7	Білий/коричневий	4 (Tip)	Білий/коричневий	4 (Tip)
8	Коричневий	4 (Ring)	Коричневий	4 (Ring)

У багатьох сучасних мережних адаптерах, комутаторах та маршрутизаторах Ethernet на інтерфейсах RJ-45 підтримується функція автоматичного визначення полярності сигналів, що передаються по витій парі, відома як Auto-MDI. Функція Auto-MDI, залежно від того, прямий чи перехресний кабель Ethernet використано для підключення пристрою до комутатора, забезпечує автоматичне переведення інтерфейсу з MDI у MDIX і навпаки. У деяких моделях комутаторів реалізація функції Auto-MDI є ще більш інтелектуальною – дає змогу коректно передавати дані через кабелі, які мають некоректне з'єднання контактів.

Необхідно зазначити, що мережні інтерфейси технологій Ethernet 10Base-T, Fast Ethernet 100Base-TX, Gigabit Ethernet 1000Base-T, окрім підтримки автоматичного визначення полярності сигналів за допомогою функції Auto-MDI, також забезпечують автоматичне узгодження швидкостей і режимів передачі за допомогою функції Auto-Negotiation.

Основні команди налагодження параметрів інтерфейсів/портів комутатора Cisco

Інтерфейси комутатора Cisco з погляду адміністрування можна розділити на дві групи: фізичні інтерфейси та логічні (віртуальні) інтерфейси. Фізичні інтерфейси – це інтерфейси/порти відповідних технологій Ethernet. Логічні інтерфейси – це інтерфейси, які автоматично створені операційною системою Cisco IOS для виконання певних функцій, або інтерфейси, які створюються адміністратором із певною метою. Позначення і, в багатьох аспектах, налагодження фізичних інтерфейсів не залежить від того, чи є вони електричними, чи оптичними. Слід зазначити, що фізичні інтерфейси комутатора Cisco за замовчуванням є активними. Позначення інтерфейсів комутатора Cisco наведені у табл. 4.

Таблиця 4

Інтерфейси (порти) комутаторів Cisco

Назва інтерфейсу	Опис інтерфейсу
Фізичні інтерфейси	
Ethernet	Класичний Ethernet, 10 Мбіт/с
FastEthernet	Fast Ethernet, 100 Мбіт/с
GigabitEthernet	Gigabit Ethernet, 1 Гбіт/с
TenGigabitEthernet	10 Gigabit Ethernet, 10 Гбіт/с
Логічні інтерфейси	
Vlan, SVI (Switched Virtual Interface)	Інтерфейс VLAN (Virtual LAN), на комутаторах автоматично створено vlan 1. До цієї VLAN за замовчуванням входять усі фізичні інтерфейси.
PortChannel	Інтерфейс агрегованого каналу зв'язку EtherChannel

Вибір інтерфейсу для налагодження здійснюється командою **interface**. Налагодження інтерфейсу комутатора передбачає зміну як фізичних параметрів роботи інтерфейсу (середовища, типу кабелю, швидкості, режиму), так і зміну параметрів фунціонування певних мережних протоколів. Основними командами налагодження параметрів інтерфейсу є **description**, **media-type**, **mdix auto**, **duplex**, **speed**, **mac-address**, **shutdown** та деякі інші.

Команда **description** застосовується для зазначення текстового опису інтерфейсу. Цей опис полегшує аналіз конфігураційного файла пристрою та аналіз результатів виведення діагностичної інформації певного інтерфейсу. За допомогою команди **media-type** здійснюється вибір типу середовища передачі. Команда **mdix auto** активує режим автоматичного визначення типу (прямий чи перех-

ресний) Ethernet-кабелю, що застосовується для підключення пристрою, та переключення у відповідний режим. За замовчуванням ця команда активована. Для того, щоб команда **mdix auto** працювала коректно, необхідно також, щоб швидкість і режим інтерфейсу визначалися автоматично. За допомогою команд **duplex** та **speed** можна змінити режим та швидкість передачі даних інтерфейсу. За замовчуванням встановлено автоматичне визначення цих параметрів. Команда **mac-address** застосовується для примусового призначення MAC-адреси інтерфейсу комутатора. Відключення інтерфейсу здійснюється за допомогою команди **shutdown**. Відміна дії вищезгаданих команд – використання форми **no**. Синтаксис розглянутих команд та режими їх застосування наведено нижче.

Можливе одночасне налагодження групи інтерфейсів. Для цього застосовується команда **interface range**. Для зручності роботи із групами інтерфейсів можливе застосування макросів. Створення макросу виконується командою **define interface-range.** Видалення – командою **no define interface-range**.

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

interface *interface_type interface_id*,

де ***interface_type*** – тип інтерфейсу (порту), може набувати значень **Ethernet**, **FastEthernet**, **GigabitEthernet**, **Port-channel**, **Vlan** та ін.;

interface_id – ідентифікатор інтерфейсу (порту), може мати одночислове позначення ***number*** (номер порту), або двочислове позначення ***module/number*** (номер модуля/номер порту).

Синтаксис команди **interface range** (режим глобального конфігурування):

interface range { *port_range* | macro *macro_name* },

де ***port_range*** – діапазон ідентифікаторів інтерфейсів (портів), що може формуватися як і з неперервної послідовності ідентифікаторів інтерфейсів, так і з окремих ідентифікаторів. Наприклад, FastEthernet 0/1 – 0/10, FastEthernet 1/1, FastEthernet 2/1;

macro – службова конструкція, за допомогою якої зазначається необхідність використання макросу;

macro_name – текстова назва макросу.

Синтаксис команди **define interface-range** (режим глобального конфігурування):

define interface-range *macro_name port_range*,

де ***macro_name*** – текстова назва макросу;

port_range – діапазон ідентифікаторів інтерфейсів (портів).

Синтаксис команди **description** (режим конфігурування інтерфейсу):

description *text_line*,

де ***text_line*** – тестовий рядок опису інтерфейсу (до 240 символів).

Синтаксис команди **duplex** (режим конфігурування інтерфейсу):

duplex { auto | full | half },

де **auto** – службова конструкція, за допомогою якої встановлюється автоматичний вибір режиму передачі;

full – службова конструкція, за допомогою якої встановлюється повнодуплексний режим передачі;

half – службова конструкція, за допомогою якої встановлюється напівдуплексний режим передачі.

Синтаксис команди **speed** (режим конфігурування інтерфейсу):

speed { 10 | 100 | 1000 | auto [10 | 100 | 1000] | nonegotiate },

де **10**, **100**, **1000** – фіксовані значення швидкості (Мбіт/с);

auto – службова конструкція, за допомогою якої встановлюється автоматичний вибір швидкості; якщо використовується форма **auto 10** (**auto 100, auto 1000**), порт веде переговори лише на цій швидкості;

nonegotiate – службова конструкція, за допомогою якої відключається режим автопереговорів про швидкість передачі.

Синтаксис команди **media-type** (режим конфігурування інтерфейсу):

media-type {**auto-select** | **rj45** | **sfp**},

де **auto-select** – службова конструкція, за допомогою якої активується вибір середовища передачі (змінного інтерфейсного модуля); автоматичний вибір встановлений за замовчуванням;

rj45 – службова конструкція, за допомогою якої зазначається застосування змінного інтерфейсного модуля RJ-45;

sfp – службова конструкція, за допомогою якої зазначається застосування змінного інтерфейсного модуля SFP.

Синтаксис команди **mdix** (режим конфігурування інтерфейсу):

mdix auto.

Команда не має параметрів.

Синтаксис команди **mac-address** (режим конфігурування інтерфейсу):

mac-address *hw_address*,

де ***hw_address*** – MAC-адреса інтерфейсу у вигляді HHHH.HHHH.HHHH; кожне число HHHH має довжину 2 байти і записується у шістнадцятковій формі.

Основні команди діагностики параметрів інтерфейсів, параметрів адресації та процесу роботи комутатора Cisco

Для виведення діагностичної інформації про параметри фізичних та логічних інтерфейсів, результати налагоджень, уміст службових таблиць, процес роботи комутатора використовуються різні варіанти команд **show**. Перелік команд та їх призначення наведено у табл. 5.

Таблиця 5

Перелік команд show, необхідних для діагностики процесу роботи комутатора Cisco

Команда	Призначення
show interfaces	Виведення деталізованої інформації про всі фізичні і логічні інтерфейси комутатора
show interface ***interface-type interface-id***	Виведення деталізованої інформації про конкретний інтерфейс комутатора
show controllers ethernet-controller ***interface-type interface-id***	Виведення деталізованої інформації про стан контролера конкретного інтерфейсу Ethernet
show controllers utilization	Виведення інформації про завантаження комутатора в цілому або окремого його порту
show version	Виведення інформації про фізичні параметри пристрою та параметри IOS

Основні команди налагодження параметрів інтерфейсів маршрутизатора Cisco

Вибір інтерфейсу маршрутизатора для налагодження виконується командою **interface**. Можливе одночасне налагодження групи інтерфейсів. Для цього використовується команда **interface range**. Слід нагадати, що за замовчуванням фізичні інтерфейси маршрутизатора знаходяться у відключеному стані, а логічні інтерфейси залежно від типу можуть знаходитися як у відключеному, так і включеному станах. Відключення інтерфейсу виконується командою **shutdown**, включення – командою **no shutdown**. Для налагодження параметрів інтерфейсів маршрутизатора, залежно від їх типу використовується достатньо великий набір команд. Більшість команд є загальними для всіх інтерфейсів, частина – характерними лише для інтерфейсів певних технологій.

Основними командами налаштування параметрів фізичного і канального рівня для інтерфейсів маршрутизатора є команди: **arp**,

bandwidth, **clock rate, delay**, **description**, **duplex**, **encapsulation**, **keepalive**, **ip**, **mac-address**, **mtu**, **speed.** Відміна дії команд – використання форми **no**, або команда **default**.

Команда **arp** та її модифікації служать для обробки ARP-запитів та їх параметрів на інтерфейсі. Команда **bandwidth** служить для встановлення значення пропускної здатності, що використовується при обчисленні метрик маршрутів у протоколах маршрутизації, не встановлює швидкість передачі даних інтерфейсу і не впливає на фактичну швидкість передачі даних по каналу зв'язку. Команда **clock rate** служить для налаштування частоти тактових імпульсів на одному з пари інтерфейсів (типу DCE), що формують прямий двоточковий послідовний канал між двама маршрутизаторами (з'єднання типу нуль-модем). При підключенні маршрутизатора через DCE-пристрій (наприклад, CSU/DSU) команда не задається, оскільки синхронізація здійснюється провайдером послуг. Команда **delay** служить для встановлення значення затримки на інтерфейсі, це значення використовується при обчисленні метрик у деяких протоколах маршрутизації, команда не визначає параметрів інтерфейса. Команда **description** служить для опису інтерфейсу, використовується з метою полегшення аналізу результатів виводу команд при адмініструванні. Команда **duplex** (та її модифікації **duplex-full, duplex-half**) служать для зазначення режиму передачі даних на інтерфейсі. Команда **encapsulation** служить для налаштування типу інкапсуляції на інтерфейсі. Часто використовується на послідовних інтерфейсах для зазначення протоколу або технології канального рівня, на інтерфейсах Ethernet використовується для тегування VLAN (як 802.1Q, так і ISL). Команда **keepalive** служить для зазначення інтервалу, протягом якого маршрутизатор буде очікувати перед тим, як відправити через інтерфейс повідомлення про перевірку зв'язку для визначення чи працює інтерфейс на іншому кінці послідовного каналу. На Ethernet-інтерфейсах маршрутизатор пересилає повідомлення самому собі. Команда **mtu** служить для зазначення MTU інтерфейса, це значення варто змінювати для оптимізації продуктивності мережі, наприклад, для каналів з великими втратами його варто зменшувати.

Синтаксис команди **interface** (режим глобального конфігурування).

interface ***interface-type interface-id.subinterface-id*** **[{point-to-point | multipoint}]**

де ***interface-type*** – тип інтерфейса, може приймати значення **Ethernet**, **FastEthernet**, **Serial**, **ATM**, **Loopback**, **Tunnel**, **Vlan** та ін.;

interface-id – ідентифікатор інтерфейса, може мати одночислове позначення ***number*** (номер інтерфейса), двочислове позначення ***module/number*** (номер модуля (адаптера)/номер інтерфейса), тричислове позначення ***slot/module/number*** (номер слота/номер модуля(адаптера)/ номер інтерфейса);

subinterface-id **–** ідентифікатор підінтерфейса, може приймати значення від 0 до 4294967295, за замовчуванням інтерфейс не містить підінтерфейсів, вони створюються у процесі виконання команди **interface**; підінтерфейси використовуються дла забезпечення роботи протоколу 802.1Q та технологій Frame Relay і ATM;

point-to-point – службова конструкція, яка зазначає, що підінтерфейс логічно з'єднаний з одним віддаленим вузлом;

multipoint – службова конструкція, яка зазначає, що підінтерфейс логічно з'єднаний з кількома віддаленими вузлами;

Параметри **point-to-point** та **multipoint**, як правило, зазначаються при роботі з інтерфейсами Frame Relay і ATM.

Синтаксис команди **arp** (режим конфігурування інтерфейсу).

arp {arpa | frame-relay | probe | snap }

де **arpa** – інкапсуляція для мереж Ethernet, встановлюється за замовчуванням;

frame-relay – інкапсуляція для мереж Frame Relay;

probe – інкапсуляція для протоколу HP Probe;

snap – інкапсуляція для SNAP (згідно RFC 1042);

Синтаксис команди **arp timeout** (режим конфігурування інтерфейсу).

arp timeout ***seconds***

де ***seconds*** – час життя ARP-запису в ARP-таблиці (с), за замовчуванням дорівнює 14400.

Синтаксис команди **bandwidth** (режим конфігурування інтерфейсу).

bandwidth ***value***

де ***value*** – значення пропускної здатності в Кбіт/с, за замовчуванням залежить від типу інтерфейсу.

Синтаксис команди **clock rate** (режим конфігурування інтерфейсу).

clock rate *bps*

де ***bps*** – значення частоти тактових імпульсів (біт/с), може приймати значення 1200, 2400, 4800, 9600, 19 200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, 4000000; за замовчуванням не зазначається.

Синтаксис команди **delay** (режим конфігурування інтерфейсу).

delay *value*

де ***value*** – значення затримки на інтерфейсі в десятках мілісекунд, за замовчуванням залежить від типу інтерфейсу.

Синтаксис команди **description** (режим конфігурування інтерфейсу).

description *text-line*

де ***text-line*** – тестовий рядок опису інтерфейсу (до 240 символів).

Синтаксис команди **duplex** (режим конфігурування інтерфейсу).

duplex {auto | full | half}

де **auto** – автоматичний вибір режиму;

full – повнодуплексний режим;

half – напівдуплексний режим.

Синтаксис команди **encapsulation** (режим конфігурування інтерфейсу/підінтерфейсу).

encapsulation { ppp | hdlc | frame-relay [cisco | ietf] | dotlq *vlan-id* … }

ppp – службова конструкція, яка вказує, що інкапсуляцію здійснювати згідно стандартів протоколу PPP;

hdlc – службова конструкція, яка вказує, що інкапсуляцію здійснювати згідно стандартів протоколу HDLC;

frame-relay – службова конструкція, яка вказує, що інкапсуляцію здійснювати згідно стандартів технології Frame Relay;

cisco – фірмовий спосіб інкапсуляції Cisco для Frame Relay;

ietf – стандартний спосіб інкапсуляції IETF;

dotlq – інкапсуляція по протоколу 802.1Q;

vlan-id – номер VLAN в діапазоні від 1 до 1005 при використанні стандартного образу IOS, при використанні образу з розширеними можливостями – в діапазоні від 1 до 4094.

Синтаксис команди **keepalive** (режим конфігурування інтерфейсу).

keepalive *seconds*

де ***seconds*** – значення інтервалу часу очікування, яке задається в секундах, за замовчуванням становить 10 с.

Синтаксис команди **ip** (режим конфігурування інтерфейса/підінтерфейса).

Синтаксис команди **ip address** (режим конфігурування інтерфейса)**.**

ip address {*address network_mask*} | dhcp

де ***address*** – IP-адреса в десятковому записі;

network_mask – маска мережі, записана у звичайній формі;

dhcp – службова конструкція, яка вказує, що IP-адресу необхідно отримати автоматично по протоколу DHCP.

Синтаксис команди **mac-address** (режим конфігурування інтерфейсу).

mac-address *hw-address*

де ***hw-address*** – MAC-адреса інтерфейсу у вигляді HHHH.HHHH.HHHH, кожне число HHHH має довжину 2 байти і записується в шістнадцятковій формі.

Синтаксис команди **mtu** (режим конфігурування інтерфейсу).

mtu *value*

де ***value*** – значення MTU в байтах, значення за замовчуванням залежить від технології або протоколу канального рівня.

Синтаксис команди **speed** (режим конфігурування інтерфейсу).

speed {10 | 100 | 1000 | auto [10 | 100 | 1000] | nonegotiate}

де **10**, **100**, **1000** – значення швидкості в Мбіт/с,

auto – службова конструкція, яка вказує автоматичний вибір швидкості; якщо використовується форма **auto 10** (**auto 100, auto 1000**) інтерфейс веде переговори лише на цій швидкості;

nonegotiate – службова конструкція, яка відключає режим автопереговорів про швидкість.

Синтаксис команди **config-register** (режим глобального конфігурування):

config-register *conf_reg_value*

де ***conf_reg_value*** – значення конфігураційного регістру, число з діапазону 0x0000 ... 0xFFFF; за замовчуванням становить 0x2102.

Основні команди Cisco IOS для базової діагностики роботи маршрутизатора Cisco

Для виведення діагностичної інформації про фізичні параметри маршрутизатора чи його інтерфейсів, стан маршрутизатора, результати налагоджень або результати роботи маршрутизатора тощо використовується команда **show**. Вона є доступною як із режиму користувача, так і з привілейованого режиму. Залежно від режиму дана команда може мати різні параметри. Частина параметрів є однаковими і доступними в обох режимах. Часто команда **show** із певним параметром уважається окремою командою. Перелік основних команд **show** та їх призначення наведені у табл. 6.

Таблиця 6

Перелік основних параметрів команди show

Команда	Призначення
show version	Виведення поточної інформації про апаратне і програмне забезпечення
show tech-support	Виведення системної інформації для технічної підтримки
show flash	Перегляд вмісту флеш-пам'яті
show file systems	Виведення про файлову систему
show memory	Виведення інформації про використання пам'яті
show processes	Виведення інформації про процеси, запущені на пристрої
show processes cpu	Виведення деталізованої інформації про завантаження процесора
show processes memory	Виведення інформації про завантаження процесами оперативної пам'яті
show controllers	Виведення деталізованої інформації про роботу контролера інтерфейса
show interfaces	Виведення деталізованої інформації про інтерфейси маршрутизатора та їх стан
show ip interface	Виведення інформації про функціонування протоколу IP версії 4 та суміжних протоколів
show ip interface brief	Виведення інформації про функціонування протоколу IP версії 4 на інтерфейсі у скороченеому вигляді
show ipv6 interface	Виведення інформації про функціонування протоколу IP версії 6 та суміжних протоколів
show ipv6 interface brief	Виведення інформації про функціонування протоколу IP версії 6 на інтерфейсі у скороченеому вигляді
show route	Виведення таблиці маршрутизації протоколу IP версії 4
Show ipv6 route	Виведення таблиці маршрутизації протоколу IP версії 6
show protocols	Виведення глобальної та інтерфейсно-залежної інформації про протоколи 3-го рівня, що функціонують на маршрутизаторі
show startup-config	Перегляд стартової конфігурації пристрою
show running-config	Перегляд поточної конфігурації пристрою
show history	Перегляд списку останніх виконаних команд (за замовчуванням 10 рядків)
show clock	Виведення часу, встановленого на маршрутизаторі

Статичне налаштування глобальної унікальної адреси (GUA) та локальної адреси каналу (LLA)

Більшість команд налаштування та перевірки мережі IPv6 в операційній системі Cisco IOS схожі на свої аналоги для мережі IPv4. У багатьох випадках єдиною відмінністю між ними є використання в командах **ipv6** замість **ip**. Наприклад, команда Cisco IOS для налаштування адреси IPv4 на інтерфейсі: **ip address *ip-address subnet-mask***. Для налаштування GUA IPv6 на інтерфейсі використовується команда: **ipv6 address *ipv6-adress/prefix-length***.

Зверніть увагу, що між ipv6-address і prefix-length немає пробілу.

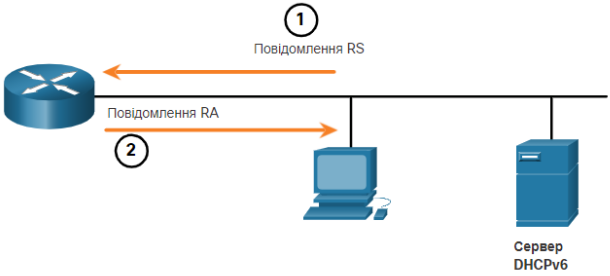
Статичне налаштування локальної адреси каналу дозволяє створити адресу, яку легше розпізнати та запам'ятати. Як правило, достатньо створити локальні адреси на маршрутизаторах, які розпізнаються. Це зручно тому, що локальні адреси маршрутизаторів використовуються як адреси шлюзу за замовчуванням і в повідомленнях анонсування маршрутизатора.

Локальні адреси каналів можна налаштувати вручну за допомогою команди **ipv6 address *ipv6-link-local-address* link-local**. Якщо адреса починається з гекстету в межах від fe80 до febf link-local то параметри локального каналу повинні слідувати за адресою.

Динамічна адресація для глобальних унікальних адрес (GUA) IPv6

Якщо ви не хочете статично налаштовувати глобальні унікальні адреси (GUA) IPv6, не потрібно турбуватися. Більшість пристроїв отримують свої глобальні унікальні адреси (GUA) IPv6 динамічно. Цей процес здійснюється за допомогою повідомлень: Анонсування маршрутизатора (Router Advertisement, RA) та Запит маршрутизатора (Router Solicitation, RS).

Для глобальної унікальної адреси пристрій динамічно отримує адресу за допомогою міжмережного протоколу керуючих повідомлень версії 6 (ICMPv6). Маршрутизатори IPv6 періодично розсилають повідомлення RA ICMPv6 кожні 200 секунд для усіх пристроїв з підтримкою IPv6. Повідомлення RA також буде надіслане у відповідь на вузол, який відправив повідомлення RS ICMPv6, що є запитом на повідомлення RA. Обидва повідомлення показано на рис.3.



1. Повідомлення RS надсилаються усім маршрутизаторам IPv6 від вузлів, які запитують адресну інформацію.
2. Повідомлення RA надсилаються усім вузлам IPv6. Якщо використовується Метод 1 (лише для SLAAC), RA включає в себе мережний префікс, довжину префікса та інформацію про шлюз за замовчуванням.

Рис.3. RS та RA повідомлення ICMPv6

Повідомлення RA є на інтерфейсах Ethernet маршрутизатора IPv6. Маршрутизатор повинен бути увімкнений для маршрутизації IPv6, яку за замовчуванням не увімкнено. Щоб маршрутизатор запрацював як IPv6-маршрутизатор, необхідно використовувати команду режиму глобальної конфігурації – **ipv6 unicast-routing**.

Повідомлення RA ICMPv6 вказує пристрою як отримати глобальну унікальну адресу (GUA) IPv6. Остаточне рішення залежить від операційної системи пристрою. Повідомлення RA ICMPv6 включає в себе наступне:

1. Префікс мережі та довжину префікса (повідомляють пристрою, до якої мережі він належить).

2. Адреса шлюзу за замовчуванням (локальна IPv6-адреса каналу, IPv6-адреса джерела повідомлення RA).

3. DNS-адреса та доменне ім'я (адреси DNS-серверів і доменне ім'я).

Існує три методи для повідомлень RA:

Метод 1: SLAAC – «У мене є все, що вам потрібно, включаючи префікс, довжину префікса та адресу шлюзу за замовчуванням».

Метод 2: SLAAC і сервер DHCPv6 без відстеження стану – «Ось моя інформація, але вам потрібно отримати іншу інформацію, таку як DNS-адреси від сервера DHCPv6 без відстеження стану».

Метод 3: DHCPv6 з відстеженням стану (немає SLAAC) - «Я можу надати вам вашу адресу шлюзу за замовчуванням. Вам потрібно звернутися до сервера DHCPv6 з відстеженням стану за вашою іншою інформацією».

Модельний приклад налагодження IPv4-адресації та параметрів каналу зв'язку технології Fast Ethernet побудованого між маршрутизатором та комутатором Cisco

Розглянемо специфіку налагодження параметрів каналу зв'язку технології Fast Ethernet між маршрутизатором та комутатором Cisco для з'єднання, схема якої наведена на рис. 4.

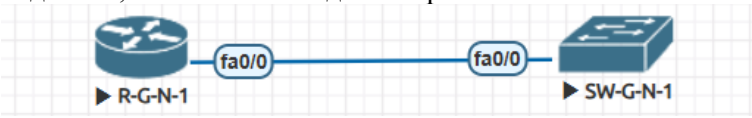


Рис. 4. Приклад мережі

Під час побудови каналу зв'язку для з'єднання пристроїв використано дані табл. 7. Для налагодження параметрів адресації інтерфейсів пристроїв використано дані табл. 8.

Таблиця 7

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Fa0/0	Комутатор SW-1	Fa0/1
Комутатор SW-1	Fa0/1	Маршрутизатор R-1	Fa0/0

Таблиця 8

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/ Мережний адаптер/ Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	–	195.1.1.0	255.255.255.0	/24
Маршрутизатор R-1	Інтерфейс Fa0/0	195.1.1.1	255.255.255.0	/24
Комутатор SW-1	Інтерфейс Fa0/1	195.1.1.2	255.255.255.0	/24

Сценарії налагодження параметрів інтерфейсів технології Fast Ethernet (швидкість, режим роботи) та параметрів IPv4-адресації для маршрутизатора R-1 та SW-1 наведені нижче.

```
…
Router>enable
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#interface FastEthernet 0/0
R-1(config-if)#description LINK-TO-SW-1
```

R-1(config-if)#speed 100
R-1(config-if)#duplex full
R-1(config-if)#ip address 195.1.1.1 255.255.255.0
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#exit
R-1# copy running-config startup-config
R-1#
…

…
Switch >enable
SW-1#configure terminal
SW-1(config)#interface FastEthernet 0/1
SW-1(config-if)#description LINK-TO-R-1
SW-1(config-if)#duplex full
SW-1(config-if)#speed 100
SW-1(config-if)#exit
SW-1(config)#interface vlan 1
SW-1(config-if)#ip address 195.1.1.2 255.255.255.0
SW-1(config-if)#no shutdown
SW-1(config-if)#exit
SW-1(config)#ip default-gateway 195.1.1.1
SW-1(config)#exit
SW-1#copy running-config startup-config
SW-1#
…

Сценарій налагодження локальних відповідностей між назвами кінцевих вузлів та комунікаційних пристроїв та їх IPv4-адресами для маршрутизатора R-1 наведено нижче.

…
R-1>enable
R-1#configure terminal
R-1(config)#ip host R-2 195.1.1.2
R-1(config)#exit
R-1#
…

Результати виконання команд моніторингу та діагностики роботи інтерфейсів пристроїв для розглянутого прикладу

З метою перегляду інформації про функціонування інтерфейсів пристроїв для розглянутого прикладу використано команди **show interfaces, show ip interface brief**. Перевірка зв'язку між пристроями здійснена за допомогою команди **ping**. Результати роботи цих команд для пристроїв R-1 та SW-1 наведено відповідно на рис. 5–11.

```
R-1#show interfaces FastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 00aa.00ad.0001 (bia c403.0755.0000)
  Description: LINK-TO-R-2
  Internet address is 195.1.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:30, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     24 packets input, 4536 bytes
     Received 13 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     66 packets output, 7056 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R-1#
```

Рис. 5. Результат виконання команди **show interfaces FastEthernet 0/0** на маршрутизаторі R-1

```
SW-1#show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0002.1632.c760 (bia 0002.1632.c760)
  Internet address is 195.1.1.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
```

```
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Рис. 6. Результат виконання команди **show interfaces Vlan 1** на комутаторі **SW-1**

```
R-1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Proto-
col
FastEthernet0/0            195.1.1.1       YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
```

Рис. 7. Результат виконання команди **show ip interface brief** на маршрутизаторі R-1

```
SW-1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual down down
Vlan1 195.1.1.2 YES manual up down
SW-1#
```

Рис. 8. Результат виконання команди **show ip interface brief** на комутаторі **SW-1**

```
SW-1#ping 195.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/19 ms
```

Рис. 9. Результат виконання команди **ping** на комутаторі **SW-1**

```
R-1#show hosts
Default Domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255
Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined
Host Port Flags Age Type Address(es)
R-2 None (perm, OK) 0 IP 195.1.1.2
R-1#
```

Рис. 10. Результат виконання команди **show hosts** на комутаторі **R-1**

```
R-1#ping R-2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Рис. 11. Результат виконання команди **ping** за встановленими локальними віідповідностями на комутаторі **R-1**

Модельний приклад налагодження IPv6-адресації та параметрів каналу зв'язку технології Fast Ethernet побудованого між маршрутизатором та комутатором Cisco

Розглянемо специфіку налагодження параметрів каналу зв'язку технології Fast Ethernet між маршрутизатором та комутатором Cisco для з'єднання, схема якої наведена на рис. 4.

Під час побудови каналу зв'язку для з'єднання пристроїв використано дані табл. 9. Для налагодження параметрів адресації інтерфейсів пристроїв використано дані табл. 10.

Таблиця 9

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Fa0/0	Комутатор SW-1	Fa0/1
Комутатор SW-1	Fa0/1	Маршрутизатор R-1	Fa0/0

Таблиця 10

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Префікс
Підмережа A	–	2001:195:1:1::0	/64
Маршрутизатор R-1	Інтерфейс Fa0/0	2001:195:1:1::1	/64
Комутатор SW-1	Інтерфейс Fa0/1	2001:195:1:1::2	/64

Сценарії налагодження параметрів IPv6-адресації для маршрутизаторів R-1, R-2 наведені нижче.

```
Router>enable
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#interface FastEthernet 0/0
R-1(config-if)#description LINK-TO-SW-1
R-1(config-if)#ipv6 address 2001:195:1:1::1/64
R-1(config-if)#no shutdown
R-1(config-if)#end
R-1#copy running-config startup-config
R-1#
…
…
```

Switch>enable
Switch#configure terminal
Switch (config)#hostname SW-1
SW-1(config)#interface vlan 1
SW-1(config-if)#ipv6 address 2001:195:1:1::2/64
SW-1(config-if)#no shutdown
SW-1(config-if)#exit
SW-1(config)#ipv6 route ::/0 2001:195:1:1::1
SW-1(config)#exit
SW-1#copy running-config startup-config
SW-1#

Сценарій налагодження локальних відповідностей між назвами кінцевих вузлів та комунікаційних пристроїв та їх IPv6-адресами для маршрутизатора R-1 наведено нижче.

R-1>enable
R-1#configure terminal
R-1(config)#ipv6 host R-2 2001:195:1:1::2
R-1(config)#exit
R-1#

Результати виконання команд моніторингу та діагностики роботи інтерфейсів пристроїв для розглянутого прикладу

З метою перегляду інформації про функціонування інтерфейсів пристроїв для розглянутого прикладу використано команди **show ipv6 interface brief, show ipv6 route**. Перевірка зв'язку між пристроями здійснена за допомогою команди **ping** та **traceroute**. Результати роботи цих команд для пристроїв R-1 та SW-1 наведено відповідно на рис. 12–19.

```
R-1#show ipv6 interface brief
FastEthernet0/0 [up/up]
     FE80::202:16FF:FED7:2401
     2001:195:1:1::1
FastEthernet0/1 [administratively down/down]
     unassigned
Vlan1 [administratively down/down]
     unassigned
```

Рис. 12. Результат виконання команди **show ipv6 interface brief** на маршрутизаторі **R-1**

```
R-1#show ipv6 route
IPv6 Routing Table - 3 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C 2001:195:1:1::/64 [0/0]
   via ::, FastEthernet0/0
L 2001:195:1:1::1/128 [0/0]
   via ::, FastEthernet0/0
L FF00::/8 [0/0]
   via ::, Null0
R-1#
```

Рис. 13. Результат виконання команди **show ipv6 route** на маршрутизаторі **R-1**

```
SW-1#show ipv6 interface brief
FastEthernet0/1 [up/up]
FastEthernet0/2 [down/down]
FastEthernet0/3 [down/down]
…]
FastEthernet0/23 [down/down]
FastEthernet0/24 [down/down]
GigabitEthernet0/1 [down/down]
GigabitEthernet0/2 [down/down]
Vlan1 [up/up]
FE80::202:16FF:FE32:C760
2001:195:1:1::2
SW-1#
```

Рис. 14. Результат виконання команди **show ipv6 interface brief** на комутаторі **SW-1**

```
SW-1#show ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
S ::/0 [1/0]
   via 2001:195:1:1::1
C 2001:195:1:1::/64 [0/0]
   via ::, Vlan1
L 2001:195:1:1::2/128 [0/0]
   via ::, Vlan1
L FF00::/8 [0/0]
   via ::, Null0
SW-1#
```

Рис. 15. Результат виконання команди **show ipv6 route** на комутаторі **SW-1**

```
R-1#ping 2001:195:1:1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:195:1:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
R-1#
```

Рис. 16. Результат виконання команди **ping** на комутаторі **R-1**

```
R-1#traceroute 2001:195:1:1::2
Type escape sequence to abort.
Tracing the route to 2001:195:1:1::2
  1 2001:195:1:1::2 0 msec 0 msec 0 msec
R-1#
```

Рис. 17. Результат виконання команди **traceroute** на комутаторі **R-1**

```
R-1#show hosts
Default Domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255
Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined
Host Port Flags Age Type Address(es)
R-2 None (perm, OK) 0 IPV 2001:195:1:1::2
R-1#
```

Рис. 18. Результат виконання команди **show hosts** на комутаторі **R-1**

```
R-1#ping R-2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:195:1:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Рис. 19. Результат виконання команди **ping** за встановленими локальними віідповідностями на комутаторі **R-1**

Модельний приклад налагодження IPv4-адресації та параметрів каналу зв'язку технології Fast Ethernet побудованого між маршрутизаторами Cisco

Розглянемо специфіку налагодження параметрів каналу зв'язку технології Fast Ethernet між маршрутизаторами Cisco для з'єднання, схема якої наведена на рис. 20.

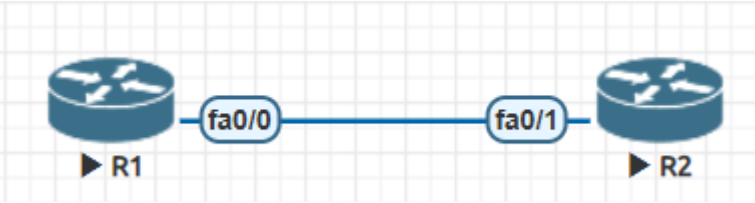


Рис. 20. Приклад мережі

Під час побудови каналу зв'язку для з'єднання пристроїв використано дані табл. 11. Для налагодження параметрів адресації інтерфейсів пристроїв використано дані табл. 12.

Таблиця 11

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Fa0/0	Маршрутизатор R-2	Fa0/1
Маршрутизатор R-2	Fa0/1	Маршрутизатор R-1	Fa0/0

Таблиця 12

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	–	195.1.1.0	255.255.255.252	/30
Маршрутизатор R-1	Інтерфейс Fa0/0	195.1.1.1	255.255.255.252	/30
Маршрутизатор R-2	Інтерфейс Fa0/1	195.1.1.2	255.255.255.252	/30

Сценарії налагодження параметрів інтерфейсів технології Fast Ethernet (швидкість, режим роботи) та параметрів IPv4-адресації для маршрутизаторів R-1 та R-2 наведені нижче.

```
…
Router>enable
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#interface FastEthernet 0/0
R-1(config-if)#description LINK-TO-R-2
R-1(config-if)#speed 100
R-1(config-if)#duplex full
R-1(config-if)#ip address 195.1.1.1 255.255.255.252
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#exit
R-1# copy running-config startup-config
R-1#
…
Router>enable
Router#configure terminal
Router(config)#hostname R-2
R-2(config)#interface FastEthernet 0/1
R-2(config-if)#description LINK-TO-R-1
R-2(config-if)#speed 100
R-2(config-if)#duplex full
R-2(config-if)#ip address 195.1.1.2 255.255.255.252
R-2(config-if)#no shutdown
R-2(config-if)#exit
R-2(config)#exit
R-2(config)#ip route 0.0.0.0 0.0.0.0 195.1.1.1
R-2(config)# exit
R-2# copy running-config startup-config
R-2#
```

Результати виконання команд моніторингу та діагностики роботи інтерфейсів маршрутизаторів для розглянутого прикладу

З метою перегляду інформації про функціонування інтерфейсів маршрутизаторів для розглянутого прикладу використано команди **show interfaces, show ip interface brief**. Перевірка зв'язку між маршрутизаторами здійснена за допомогою команди **ping**. Результати роботи цих команд для маршрутизаторів R-1 та R-2 наведено відповідно на рис. 21–25.

```
R-1#show interfaces FastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 00aa.00ad.0001 (bia c403.0755.0000)
  Description: LINK-TO-R-2
  Internet address is 195.1.1.1/30
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:30, output 00:00:03, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     24 packets input, 4536 bytes
     Received 13 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     66 packets output, 7056 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Рис. 21. Результат виконання команди **show interfaces FastEthernet 0/0** на маршрутизаторі **R-1**

```
R-2#show interfaces FastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Gt96k FE, address is 00aa.00ad.0002 (bia c404.0764.0001)
  Description: LINK-TO-R-1
  Internet address is 195.1.1.2/30
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:36, output 00:00:06, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     20 packets input, 3716 bytes
     Received 8 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     69 packets output, 7526 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Рис. 22. Результат виконання команди **show interfaces FastEthernet 0/1** на маршрутизаторі **R-2**

```
R-1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Proto-
col
FastEthernet0/0            195.1.1.1       YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
R-1#
```

Рис. 23. Результат виконання команди **show ip interface brief** на маршрутизаторі **R-1**

```
R-2#show ip interface brief
Interface                  IP-Address      OK? Method Status                Proto-
col
FastEthernet0/0            unassigned      YES NVRAM  administratively down down
FastEthernet0/1            195.1.1.2       YES NVRAM  up                    up
FastEthernet1/0            unassigned      YES NVRAM  administratively down down
R-2#
```

Рис. 24. Результат виконання команди **show ip interface brief** на маршрутизаторі **R-2**

```
R-1#ping 195.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 195.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/36/84 ms
R-1#
```

Рис. 25. Результат виконання команди **ping** на маршрутизаторі R-1

Модельний приклад налагодження IPv6-адресації та параметрів каналу зв'язку технології Fast Ethernet побудованого між маршрутизаторами Cisco

Розглянемо специфіку налагодження параметрів каналу зв'язку технології Fast Ethernet між маршрутизаторами Cisco для з'єднання, схема якої наведена на рис. 20.

Під час побудови каналу зв'язку для з'єднання пристроїв використано дані табл. 13. Для налагодження параметрів адресації інтерфейсів пристроїв використано дані табл. 14.

Таблиця 13

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Fa0/0	Маршрутизатор R-2	Fa0/1
Маршрутизатор R-2	Fa0/1	Маршрутизатор R-1	Fa0/0

Таблиця 14

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Префікс
Підмережа А	–	2001:195:1:1::0	/64
Маршрутизатор R-1	Інтерфейс Fa0/0	2001:195:1:1::1	/64
Маршрутизатор R-2	Інтерфейс Fa0/1	2001:195:1:1::2	/64

Сценарії налагодження параметрів IPv6-адресації для маршрутизаторів R-1, R-2 наведені нижче.

```
Router>enable
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#interface FastEthernet 0/0
R-1(config-if)#description LINK-TO-SW-1
R-1(config-if)#ipv6 address 2001:195:1:1::1/64
R-1(config-if)#no shutdown
R-1(config-if)#end
R-1#copy running-config startup-config
R-1#
```

```
Router>enable
Router#configure terminal
Router(config)#hostname R-2
R-2(config)#interface FastEthernet 0/1
R-2(config-if)#description LINK-TO-R-1
R-2(config-if)#ipv6 address 2001:195:1:1::2/64
R-2(config-if)#no shutdown
R-2(config-if)#exit
R-2(config)#ipv6 route ::/0 2001:195:1:1::1
R-2(config)#exit
R-2#copy running-config startup-config
R-2#
```

Результати виконання команд моніторингу та діагностики роботи інтерфейсів пристроїв для розглянутого прикладу

З метою перегляду інформації про функціонування інтерфейсів маршрутизаторів для розглянутого прикладу використано команди **show ipv6 interface brief, show ipv6 route**. Перевірка зв'язку між маршрутизаторами здійснена за допомогою команди **ping** та **traceroute**. Результати роботи цих команд для пристроїв R-1 та SW-1 наведено відповідно на рис. 26–31.

```
R-1#show ipv6 interface brief
FastEthernet0/0 [up/up]
     FE80::202:16FF:FED7:2401
     2001:195:1:1::1
FastEthernet0/1 [administratively down/down]
     unassigned
Vlan1 [administratively down/down]
     unassigned
```

Рис. 26. Результат виконання команди **show ipv6 interface brief** на маршрутизаторі **R-1**

```
R-1#show ipv6 route
IPv6 Routing Table - 3 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C 2001:195:1:1::/64 [0/0]
   via ::, FastEthernet0/0
L 2001:195:1:1::1/128 [0/0]
   via ::, FastEthernet0/0
L FF00::/8 [0/0]
   via ::, Null0
```

Рис. 27. Результат виконання команди **show ipv6 route** на маршрутизаторі **R-1**

```
R-2#show ipv6 interface brief
FastEthernet0/0 [administratively down/down]
     unassigned
FastEthernet0/1 [up/up]
     FE80::290:21FF:FE77:702
     2001:195:1:1::2
Vlan1 [administratively down/down]
     unassigned
```

Рис. 28. Результат виконання команди **show ipv6 interface brief** на маршрутизаторі **R-2**

```
R-2#show ipv6 route
IPv6 Routing Table - 4 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S ::/0 [1/0]
   via 2001:195:1:1::1
C 2001:195:1:1::/64 [0/0]
   via ::, FastEthernet0/1
L 2001:195:1:1::2/128 [0/0]
   via ::, FastEthernet0/1
L FF00::/8 [0/0]
   via ::, Null0
```

Рис. 29. Результат виконання команди **show ipv6 route** на маршрутизаторі **R-2**

```
R-2#ping 2001:195:1:1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:195:1:1::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
R-2#
```

Рис. 30. Результат виконання команди **ping** на маршрутизаторі R-2

```
R-1#ping R-2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:195:1:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms
R-1#
```

Рис. 31. Результат виконання команди **ping** за встановленною локальною відповідністю на маршрутизаторі R-1

Завдання на лабораторну роботу

1. У середовищі віртуальної мережевої лабораторія eve.ztu.edu.ua створити проєкт мережі (рис. 32), або завантажити готовий проєкт прикріплений під методичними рекомендаціями.

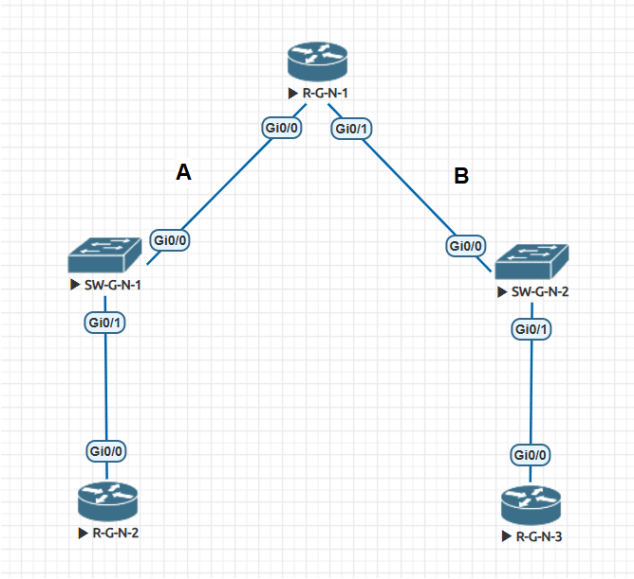


Рис. 32. Проєкт мережі

2. Розробити схему адресації пристроїв мережі. Для цього скористатися даними табл. 16. Результати навести у вигляді таблиці, яка аналогічна табл. 8.

3. Провести налагодження параметрів мережних адаптерів/інтерфейсів маршрутизаторів та комутаторів. Для цього скористатися даними табл. 15.

Таблиця 15

Вихідні дані для налагодження параметрів інтерфейсів пристроїв

№ варіанта	Канал R-G-N-1 – SW-G-N-1		Канал R-G-N-1 – SW-G-N-2		Канал SW-G-N-1 – R-G-N-2		Канал SW-G-N-2 – R-G-N-3	
	Швидкість, Мбіт/с	Режим	Швидкість, Мбіт/с	Режим	Швидкість, Мбіт/с	Режим	Швидкість, Мбіт/с	Режим
Парний	1000	Full	100	Full	100	Full	1000	Full
Не парний	100	Full	1000	Full	1000	Full	100	Full

Таблиця 16

Параметри IP-адресації підмереж

Мережа	Адреса мережі та префікс (ipv4)	Адреса мережі та префікс (ipv6)
A	193.G.N.0 /24	2001:193:G:N::0 /64
B	194.G.N.0 /24	2001:194:G:N::0 /64

*Примітка: **G** – унікальний номер групи, **N** – номер варіанту.*

4. Провести налагодження параметрів IP-адресації пристроїв мережі згідно з даними п. 2. На кожному комутаторі та на маршрутизаторі для всіх вузлів встановити локальні відповідності між текстовими іменами та IP-адресами (обох версій) вузлів мережі.

5. Провести обмін даними між пристроями. Перевірити наявність зв’язку між всіма пристроями мережі.

6. Дослідити особливості отримання службової та діагностичної інформації.

Контрольні питання

1. Які основні типи мережних пристроїв використовуються в сучасних мережах?
2. Які функції виконує маршрутизатор у комп'ютерних мережах?
3. Які особливості має комутатор у порівнянні з маршрутизатором?
4. Яка роль мережної операційної системи Cisco IOS у керуванні мережевими пристроями?
5. Які основні команди використовуються для входу в режим конфігурації пристрою Cisco?
6. Як виконується базове налаштування інтерфейсів маршрутизатора Cisco?
7. Які команди використовуються для призначення IPv4-адреси інтерфейсу маршрутизатора?
8. Як налаштовується IPv6-адресація на інтерфейсах маршрутизатора?
9. Чим відрізняється глобальна унікальна адреса (GUA) від локальної адреси каналу (LLA) в IPv6?
10. Як за допомогою команди **show interfaces** можна перевірити стан мережного інтерфейсу?
11. Які команди використовуються для діагностики мережного з'єднання на пристроях Cisco?
12. Як працює команда **ping**, і як вона допомагає у тестуванні мережевих з'єднань?
13. У чому відмінність між командами **show ip interface brief** та **show ipv6 interface brief**?
14. Яке призначення команди **no shutdown**?
15. Як зберегти конфігурацію маршрутизатора після внесення змін?
16. Чому важливо використовувати команду **description** при налаштуванні інтерфейсів?
17. Які функції виконує команда **show ip route**, і як вона використовується в діагностиці мережі?
18. Як правильно визначати та усувати можливі помилки при налаштуванні мережевих пристроїв Cisco?

Лабораторна робота № 2
НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ АГРЕГУВАННЯ КАНАЛІВ У КОМУТОВАНИХ МЕРЕЖАХ ETHERNET

Мета заняття: ознайомитися з особливостями функціонування технологій та протоколів агрегування каналів мереж Ethernet; отримати практичні навички налагодження, моніторингу та діагностування роботи агрегованих каналів на обладнанні Cisco; дослідити процеси передачі кадрів через агреговані канали.

Теоретичні відомості

Агрегування каналів у комутаторах Cisco

Агрегування каналів на обладнанні Cisco може здійснюватися як статично, так і динамічно, як із використанням засобів 2-го, так і 3-го рівнів моделі OSI. Залежно від швидкості технології Ethernet агреговані канали між пристроями Cisco прийнято називати Etherchannel (10BaseT/F), Fast Etherchannel (FEC, 100BaseTX/FX), Gigabit Etherchannel (GEC, 1000BaseT/FX). Статичні та динамічні агреговані канали часто називають каналами Etherchannel незалежно від технології і методу агрегації.

Статичне агрегування має перевагу в тому, що не вносить додаткової затримки при активації агрегованого каналу або зміни його налагоджень. Недоліки статичного агрегування: відсутнє узгодження налагоджень із віддаленою стороною; помилки в налагодженні можуть призвести до утворення петель. Cisco рекомендує використовувати статичне агрегування каналів.

Для динамічного агрегування каналів можуть використовуватися два протоколи: стандартний протокол LACP (Link Aggregation Control Protocol); фірмовий протокол Cisco PAgP (Port Aggregation Protocol). Ці протоколи виконують одні і ті ж завдання (з невеликими розбіжностями щодо можливостей), тому рекомендується використовувати стандартний протокол LACP. Перевагами агрегування з використанням протоколу LACP є: узгодження налагоджень із віддаленою стороною, яке дозволяє уникнути помилок і петель у мережі; підтримка standby-інтерфейсів дозволяє агрегувати до 16 портів, 8 портів будуть активними, а решта – в режимі гарячого резерву. Недоліком агрегування з використанням протоколу LACP є внесення додаткової затримки при активації агрегованого каналу або при зміні його налагоджень.

Порядок налагодження агрегованих каналів на обладнанні Cisco

Налагодження агрегування каналів на обладнанні Cisco складається із кількох етапів. Порядок їх виконання є таким:

1. Вибрати групу інтерфейсів на першому пристрої.
2. Вимкнути вибрані інтерфейси.
3. Об'єднати вибрані інтерфейси у логічний інтерфейс (Cisco також називає цей інтерфейс port-channel) та присвоїти йому номер.
4. Залежно від виду агрегації каналів та типу протоколу налагодити відповідний режим роботи каналу.
5. Налагодити метод балансування трафіка (необов'язково).
6. Перейти на другий пристрій та виконати на ньому дії п. 1 – 5.
7. Увімкнути інтерфейси на обох пристроях та перевірити працездатність налаштованого каналу.

Команди налагодження агрегованих каналів на комутаторах Cisco

Для створення логічних каналів та налагодження всіх варіантів їх агрегації на комутаторах Cisco використовується команда **channel-group**. За її допомогою зазначається, якому логічному каналу (логічному інтерфейсу) належить фізичний інтерфейс і який варіант агрегування застосовується. Для прямого зазначення протоколу агрегування використовується команда **channel-protocol**. Для вибору методу розподілу кадрів між фізичними каналами одного логічного каналу застосовується команда **port-channel load-balance**. Особливістю налагодження агрегування на пристроях третього рівня є те, що логічний інтерфейс необхідно створювати вручну, а не автоматично командою **channel-group**. Для цього застосовується команда **interface port-channel.**

Синтаксис команд та режими їх застосування наведено нижче.

Синтаксис команди **channel-group** (режим конфігурування інтерфейсу/групи інтерфейсів):

channel-group [*group-number*] mode { **auto [non-silent] | desirable [non-silent] | on} | {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 – ввімкнути підтримку протоколу PAgP, тільки якщо прийде повідомлення PagP;

desirable – ввімкнути підтримку протоколу PAgP;

on – ввімкнути статичну агрегацію EtherChannel;

active – ввімкнути підтримку протоколу LACP;

passive – ввімкнути підтримку протоколу LACP, тільки якщо прийде повідомлення LACP;

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

Комбінації режимів за яких увімкнеться агрегування каналів для протоколів PAgP та LACP наведені на рис. 1.

Режим LACP	**passive**	**active**
passive	**–**	**+**
active	**+**	**+**

Режим PAgP	**auto**	**desirable**
auto	**–**	**+**
desirable	**+**	**+**

Рис. 1. Комбінації режимів для протоколів PAgP та LACP

Синтаксис команди **channel-protocol** (режим конфігурування інтерфейсу/групи інтерфейсів):

channel-protocol *protocol*,

де ***protocol*** – параметр, який може набувати значень **lacp**, **pagp**.

Синтаксис команди **port-channel load-balance** (режим глобального конфігурування):

port-channel load-balance *method*,

де ***method*** – метод балансування навантаження між фізичними каналами логічного каналу, може набувати значень:

dst-mac – на основі MAC-адреси отримувача;

src-mac – на основі MAC-адреси відправника;

dst-ip – на основі IP-адреси отримувача;

src-ip – на основі IP-адреси відправника;

dst-port – на основі номера порту отримувача;

src-port – на основі номера порту відправника;

src-dst-mac – за результатами операції XOR MAC-адрес відправника та отримувача;

src-dst-ip – за результатами операції XOR IP-адрес відправника та отримувача;

src-dst-port – за результатами операції XOR номерів портів відправника та отримувача.

Синтаксис команди **interface port-channel** (режим глобального конфігурування):

interface port-channel *number*,

де ***number*** –номер логічного каналу, що створюється на пристрої.

Команди моніторингу та діагностики роботи агрегованих каналів Etherchannel

Для перегляду параметрів налагоджень окремих агрегованих каналів та їх складових використовуються як команди загального призначення, так і спеціалізовані команди. Серед команд загального призначення можна виділити такі команди: **show interfaces**, **show interface *interface-type interface-id***, **show running-config, show startup-config**. До спеціалізованих команд належать команди **show etherchannel**, **show lacp**, **show pagp**. Зазначені спеціалізовані команди мають певний набір модифікацій, які формують інші команди, їх перелік наведений у табл. 1. Для діагностики роботи та усунення проблем з налагодженням також використовуються команди обнулення лічильників **clear lacp, clear pagp**.

Таблиця 1

Перелік команд *show* діагностики роботи агрегованих каналів на комутаторах Cisco

Команда	Призначення
Команди діагностики роботи агрегованих каналів	
show etherchannel	Виведення загальної інформації про агреговані канали на пристрої
show etherchannel summary	Виведення сумарної інформації про агреговані канали пристрою
show etherchannel port-channel	Виведення детальної інформації про логічні інтерфейси
show etherchannel load-balance	Виведення інформації про метод балансування навантаження на поточному комутаторі
show interface etherchannel	Виведення повної інформації про інтерфейси, які використовуються в агрегованому каналі
show mac-address-table interfaces port-channel	Виведення таблиці комутації комутатора для задіяних для передачі кадрів агрегованих каналів
Команди діагностики роботи протоколу LACP	
show lacp counters	Виведення інформації про лічильники LACP
show lacp internal	Виведення інформації LACP локального комутатора
show lacp neighbor	Виведення інформації LACP із сусіднього комутатора
show lacp sys-id	Виведення інформації про системний ідентифікатор LACP
Команди діагностики роботи протоколу PAgP	
show pagp internal	Виведення інформації PAgP локального комутатора
show pagp neighbor	Виведення інформації PAgP із сусіднього комутатора
show pagp counters	Виведення інформації про лічильники PAgP

Модельний приклад налагодження параметрів агрегованого каналу технології Gigabit Ethernet, побудованого між маршрутизаторами Cisco

Розглянемо специфіку налагодження параметрів агрегованого каналу зв'язку технології Gigabit Ethernet між маршрутизаторами Cisco для з'єднання, схема якої наведена на рис. 2.

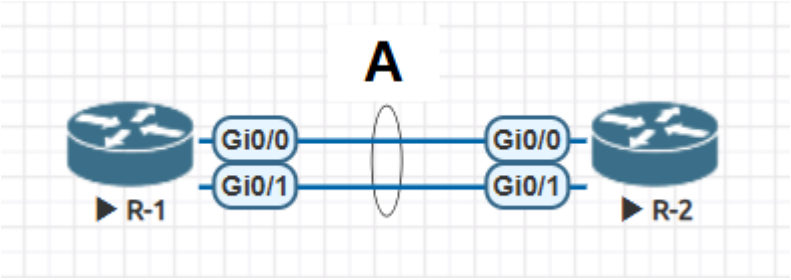


Рис. 2. Приклад мережі

Під час побудови каналу зв'язку для з'єднання пристроїв використано дані табл. 2. Для налагодження параметрів адресації інтерфейсів пристроїв використано дані табл. 3.

Таблиця 2

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Gi0/0	Маршрутизатор R-2	Gi0/0
	Gi0/1		Gi0/1
Маршрутизатор R-2	Gi0/0	Маршрутизатор R-1	Gi0/0
	Gi0/1		Gi0/1

Таблиця 3

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	–	197.1.1.0	255.255.255.252	/30
Маршрутизатор R-1	Інтерфейс Port-Channel 1	197.1.1.1	255.255.255.252	/30
Маршрутизатор R-2	Інтерфейс Port-Channel 1	197.1.1.2	255.255.255.252	/30

Сценарії налагодження параметрів агрегованого каналу технології Gigabit Ethernet та параметрів адресації для маршрутизаторів R-1, R-2 наведені нижче.

```
Router>enable
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#interface port-channel 1
R-1(config-if)#description AGGREGATED_LINK-TO-R-2
R-1(config-if)#ip address 197.1.1.1 255.255.255.0
R-1(config-if)#exit
R-1(config)#interface GigabitEthernet 0/0
R-1(config-if)#channel-group 1
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#interface GigabitEthernet 0/1
R-1(config-if)#channel-group 1
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#exit
R-1#
…
Router>enable
Router#configure terminal
Router(config)#hostname R-2
R-2(config)#interface Port-Channel 1
R-2(config-if)#description AGGREGATED_LINK-TO-R-1
R-2(config-if)#ip address 197.1.1.2 255.255.255.0
R-2(config-if)#exit
R-2(config)#interface GigabitEthernet 0/0
R-2(config-if)#channel-group 1
R-2(config-if)#no shutdown
R-2(config-if)#exit
R-2(config)#interface GigabitEthernet 0/1
R-2(config-if)#channel-group 1
R-2(config-if)#no shutdown
R-2(config-if)#exit
R-2#
…
```

Результати виконання команд моніторингу та діагностики роботи інтерфейсів маршрутизаторів для розглянутого прикладу

З метою перегляду інформації про функціонування інтерфейсів маршрутизаторів для розглянутого прикладу використано команди **show interfaces**. Перевірка зв'язку між маршрутизаторами здійснена за допомогою команди **ping**. Результати роботи цих команд для маршрутизаторів R-1 та R-2 наведено відповідно на рис. 3–5.

```
R-1#show interfaces port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is GEChannel, address is ca01.0645.0008 (bia ca01.0645.0006)
  Description: AGGREGATED_LINK-TO-R-2
  Internet address is 197.1.1.1/30
  MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Unknown duplex, Unknown Speed, media type is unknown media type
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 2
        Member 0 : GigabitEthernet0/0 , Full-duplex, 1000Mb/s
        Member 1 : GigabitEthernet1/0 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
    No. of PF_JUMBO supported members in this channel : 0
  Last input 00:01:54, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/150/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/80 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 516 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     6 packets output, 576 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
R-1#
```

Рис. 3. Результати виконання команди **show interface port-channel 1** на маршрутизаторі R-1

```
R-2#show interfaces port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is GEChannel, address is ca02.0720.0008 (bia ca02.0720.0006)
  Description: AGGREGATED_LINK-TO-R-1
  Internet address is 197.1.1.2/30
  MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Unknown duplex, Unknown Speed, media type is unknown media type
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 2
        Member 0 : GigabitEthernet0/0 , Full-duplex, 1000Mb/s
        Member 1 : GigabitEthernet1/0 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
    No. of PF_JUMBO supported members in this channel : 0
  Last input 00:02:59, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/150/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/80 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

R-2#
```

Рис. 4. Результати виконання команди **show interface port-channel 1** на маршрутизаторі R-2

```
R-1#ping 197.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 197.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/28/60 ms
R-1#
```

Рис. 5. Результати виконання команди **ping** на маршрутизаторі R-1

Модельний приклад налагодження функціонування агрегованого каналу Gigabit Ethernet між комутатором і маршрутизатором Cisco

Розглянемо специфіку налагодження параметрів агрегованого каналу зв'язку технології Gigabit Ethernet між комутатором і маршрутизатором Cisco для з'єднання, схема якої наведена на рис. 6.

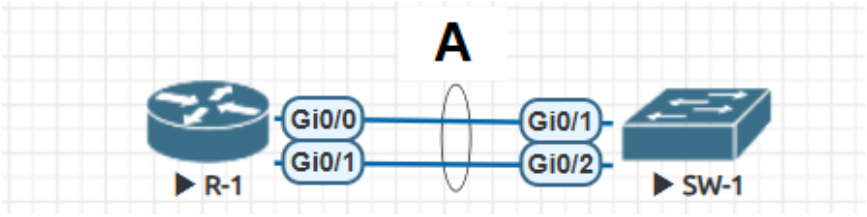


Рис. 6. Приклад мережі

Під час побудови каналу зв'язку для з'єднання пристроїв використано дані табл. 4. Для налагодження параметрів адресації інтерфейсів пристроїв використано дані табл. 5.

Таблиця 4

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Канал/ Метод агрегування	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Маршрутизатор R-1	Агрегований канал А/ статичне агрегування	Gi0/0	Комутатор SW-1	Gi0/1
		Gi0/1		Gi0/2
Комутатор SW-1	Агрегований канал А/ статичне агрегування	Gi0/1	Маршрутизатор R-1	Gi0/0
		Gi0/2		Gi0/1

Таблиця 5

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Мережа	–	195.10.1.0	255.255.255.0	/24
Маршрутизатор R-1	Інтерфейс Port-Channel 1	195.10.1.254	255.255.255.0	
Комутатор SW-1	Інтерфейс vlan 1	195.10.1.252	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–

Сценарії налагодження параметрів агрегованого каналу технології Gigabit Ethernet та параметрів адресації для маршрутизатора R-1 та коммутатора SW-1 наведені нижче.

…
Router>enable
Router#configure terminal
Router(config)#hostname R-1
R-1(config)#interface port-channel 1
R-1(config-if)#description AGGREGATED-LINK-TO-SW-1
R-1(config-if)#ip address 195.10.1.254 255.255.255.0
R-1(config-if)#exit
R-1(config)#interface range GigabitEthernet 0/0, GigabitEthernet 0/1
R-1(config-if-range)#description LINK-TO-SW-1
R-1(config-if-range)#channel-group 1
R-1(config-if-range)#no shutdown
R-1(config-if-range)#exit
R-1(config-if)#
…
Switch>enable
Switch #configure terminal
Switch (config)#hostname SW-1
SW-1(config)#interface Port-Channel 1
SW-1(config-if)#description AGGREGATED-LINK-TO-R-1
SW-1(config-if)#exit
SW-1(config)#interface range GigabitEthernet 0/0-1
SW-1(config-if)#description LINK-TO-R-1
SW-1(config-if)#channel-group 1 mode on
SW-1(config-if)#exit
SW-1(config)#port-channel load-balance src-dst-mac
SW-1(config)#interface vlan 1
SW-1(config-if)#ip address 195.10.1.252 255.255.255.0
SW-1(config-if)#no shutdown
SW-1(config-if)#exit
SW-1(config)#ip default-gateway 195.10.1.254
SW-1(config)#ip name-server 195.10.1.254
SW-1(config)#
…

Результати виконання команд моніторингу та діагностикироботи агрегованних каналів для розглянутого модельного прикладу

Для перегляду інформації про налагодження EtherChannel для розглянутого прикладу використано команду **show interfaces port-channel** для маршрутизатора та команди **show etherchannel, show etherchannel summary, show etherchannel port-channel**, **show etherchannel load-balance** для комутатора. Результат роботи цих команд для для маршрутизатора R-1 та комутатора SW-1 наведено відповідно на рис. 7 – 12.

```
R-1#show interfaces port-channel 1
Port-channel1 is up, line protocol is up
  Hardware is GEChannel, address is ca01.06f2.0008 (bia ca01.06f2.0006)
  Description: AGGREGATED-LINK-TO-SW-1
  Internet address is 195.10.1.254/24
  MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Unknown duplex, Unknown Speed, media type is unknown media type
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 2
        Member 0 : GigabitEthernet0/0 , Full-duplex, 1000Mb/s
        Member 1 : GigabitEthernet0/1 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
    No. of PF-JUMBO supported members in this channel : 0
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/150/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/80 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
R-1#
```

Рис. 7. Результат роботи команди **show interfaces port-channel 1** для маршрутизатора R-1

```
SW-1#show etherchannel
                Channel-group listing:
                ----------------------
Group: 1
----------
Group state = L2
Ports: 2   Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol:    -
Minimum Links: 0
SW-1#
```

Рис. 8. Результат роботи команди **show etherchannel** для комутатора SW-1

```
SW-1#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
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)          -        Fa0/1(P)    Fa0/2(P)
SW-1#
```

Рис. 9. Результат роботи команди **show etherchannel summary** для комутатора SW-1

```
SW-1#show etherchannel port-channel
                Channel-group listing:
                ----------------------
Group: 1
----------
                Port-channels in the group:
                ---------------------------
Port-channel: Po1
------------
Age of the Port-channel   = 0d:00h:04m:22s
Logical slot/port   = 2/1          Number of ports = 2
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =    -
Port security       = Disabled
Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/1    On                 0
  0     00     Fa0/2    On                 0
Time since last port bundled:    0d:00h:03m:27s    Fa0/2
SW-1#
```

Рис. 10. Результат роботи команди **show etherchannel port-channel** для комутатора SW-1

```
SW-1#show interfaces etherchannel
----
FastEthernet0/1:
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = On              Gcchange = -
Port-channel  = Po1         GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =    -

Age of the port in the current state: 0d:00h:05m:15s

----
FastEthernet0/2:
Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = On              Gcchange = -
Port-channel  = Po1         GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =    -

Age of the port in the current state: 0d:00h:05m:15s

----
Port-channel1:
Age of the Port-channel   = 0d:00h:06m:11s
Logical slot/port   = 2/1          Number of ports = 2
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =    -
Port security       = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/1    On                 0
  0     00     Fa0/2    On                 0

Time since last port bundled:    0d:00h:05m:15s    Fa0/2
```

Рис. 11. Результат роботи команди **show interfaces etherchannel** для комутатора SW-1

```
SW-1#show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-mac

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination MAC address
  IPv6: Source XOR Destination MAC address

SW-1#
```

Рис. 12. Результат роботи команди **show etherchannel load-balance** для комутатора SW-1

Завдання на лабораторну роботу

1. У середовищі віртуальної мережевої лабораторія eve.ztu.edu.ua створити проєкт мережі (рис. 13), або завантажити готовий проєкт прикріплений під методичними рекомендаціями.

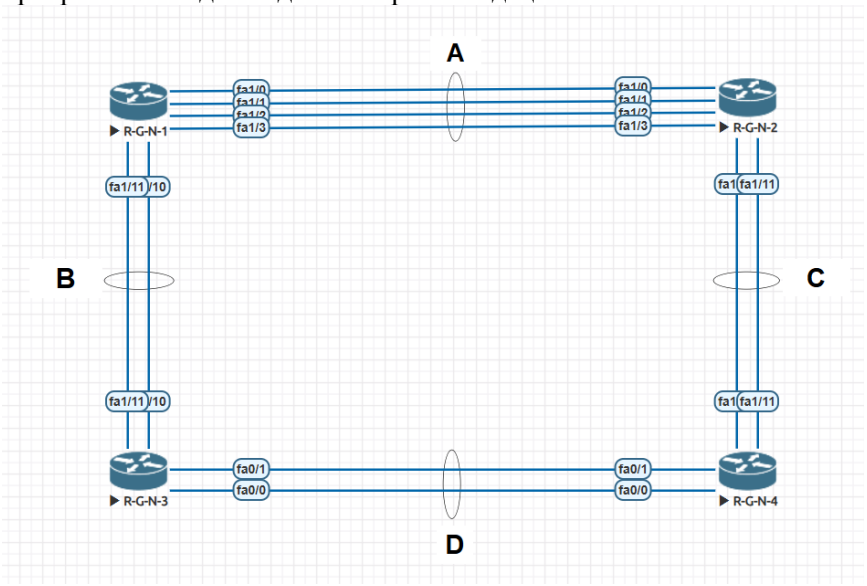


Рис. 13. Проект мережі

2. Розробити схему адресації пристроїв мережі на основі даних, які наведені у табл. 7. Результати навести у вигляді аналогічної таблиці.

3. Провести налагодження статичних агрегованих каналів.

4. Провести налагодження параметрів IP-адресації пристроїв мережі відповідно до даних п. 2. Перевірити наявність зв'язку між пристроями мережі.

5. Дослідити особливості передачі трафіка та отримання службової та діагностичної інформації про налагодження агрегованих каналів за допомогою відповідних команд.

6. Налагодити балансування навантаження на основі статичної маршрутизації та плаваючих статичних маршрутів.

7. Згенерувати трафік між двома маршрутизаторами:

– використовуючи команду **ping** між пристроями для перевірки балансування на основі IP-адрес.

– використовуючи команду **iperf** створіть TCP або UDP трафік між пристроями.

8. Налаштувати MPLS Traffic Engineering (TE) на базі EtherChannel каналу за табл. 8, перевірити роль EtherChannel у магістральних MPLS мережах та протестувати балансування трафіку і резервування каналів.

Таблиця 7

Параметри IP-адресації мережі

№ варіанта	IP-адреса мережі A	IP-адреси мереж
1	Мережа A	191.G.N.0 /30
2	Мережа B	192.G.N.0 /30
3	Мережа C	193.G.N.0 /30
4	Мережа D	194.G.N.0 /30

Таблиця 8

Параметри налаштування MPLS TE

№ варіанта	Канал для налаштування MPLS	Інтерфейс для тунелю MPLS TE	Параметри **iperf**	
			Тривалість тесту, хв	Інтервал виводу статистики, с
Не парні	B	Tunel **N**	1	1
Парні	C	Tunel **N**	2	2

** Примітка: N – номер варіанту*

Контрольні питання

1. Поняття агрегування каналів. Основні завдання агрегування каналів.
2. Статичне агрегування каналів Ethernet. Переваги та недоліки.
3. Динамічне агрегування каналів Ethernet. Переваги та недоліки.
4. Протоколи динамічного агрегування каналів Ethernet.
5. Порядок налагодження агрегованого каналу на пристроях Cisco.
6. Нумерація агрегованих каналів на пристроях Cisco. Обмеження та особливості використання.
7. Команди налагодження статичного агрегування каналів на комутаторах Cisco.
8. Команди налагодження динамічного агрегування каналів за допомогою протоколу LACP на комутаторах Cisco.
9. Команди налагодження динамічного агрегування каналів за допомогою протоколу PAgP на комутаторах Cisco.
10. Методи балансування навантаження агрегованих каналів на комутаторах Cisco.
11. Команди діагностики налагоджень агрегованого каналу між комутаторами Cisco.
12. Команди діагностики роботи агрегованого каналу між комутаторами Cisco.
13. Команди діагностики роботи методу балансування навантаження на пристроях Cisco.
14. Команди діагностики роботи протоколів динамічного агрегування на комутутаторах Cisco.
15. Різниця у налагодженні агрегованих каналів 2-го та 3-го рівнів на пристроях Cisco.
16. Методи балансування трафіку в агрегованих каналах Cisco.
17. Різниця балансування трафіку за MAC-адресами та за IP-адресами.
18. Команда налаштування методу балансування трафіку в EtherChannel.
19. Роль EtherChannel у магістральних MPLS-мережах.
20. Команди налаштування MPLS TE тунелів.

Лабораторна робота № 3
НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПОСЛІДОВНИХ КАНАЛІВ ЗВ'ЯЗКУ У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження послідовних каналів зв'язку глобальних мереж; налагодити функціонування послідовних з'єднань глобальних мереж із використанням протоколів HDLC та PPP на базі обладнання Cisco; дослідити процеси передачі даних та особливості функціонування обладнання у побудованій мережі.

Теоретичні відомості

Загальні відомості про застосування послідовних каналів зв'язку у мережах, побудованих на базі обладнання Cisco

Послідовний двоточковий канал зв'язку між маршрутизаторами Cisco будується за типовою схемою, що наведена на рис. 1, *а*. В лабораторних умовах для побудових тестових та навчальних стендів використовується спрощена схема, наведена на рис. 1, *б*. Кабельні з'єднання між DTE та DCE-пристроями є з'єднаннями стандартів V.35, X.21, EIA/TIA-232, EIA/TIA-449, EIA-530 (TIA-530-A), EIA-612/613 (HSSI, High-Speed Serial Interface). Вибір з'єднувальних кабелів здійснюється за даними технічної документації залежно від стандартів та ролей (DTE чи DCE) відповідних послідовних інтерфейсів пристроїв. Як протоколи канального рівня, як правило, використовуються загальновживані протоколи HDLC та PPP.

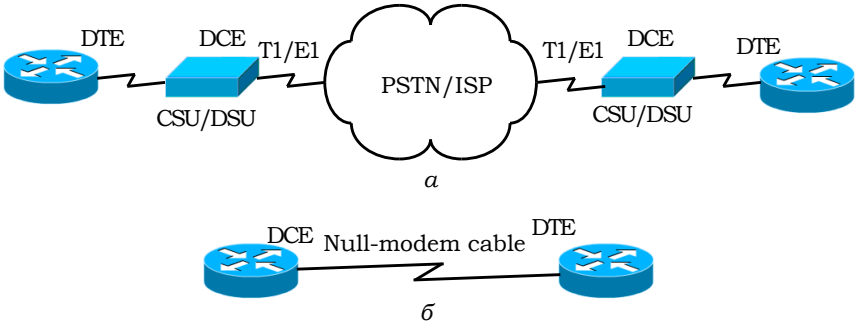


Рис. 1. Схеми побудови послідовного двоточкового каналу зв'язку

Порядок налагодження інтерфейсів послідовних каналів зв'язку у мережах, побудованих на базі обладнання Cisco

Налагодження функціонування послідовного інтерфейсу маршрутизатора Cisco для формування каналу зв'язку за рекомендаціями виробника передбачає такі етапи:

1. Вибрати та активувати послідовний інтерфейс (обов'язково).
2. Встановити тип інтерфейсу (DCE чи DTE). Для інтерфейсу DCE встановити параметри синхронізації (обов'язково).
3. Налагодити додаткові параметри функціонування каналу (необов'язково).
4. Налагодити протокол інкапсуляції канального рівня та додаткові параметри його функціонування (необов'язково).
5. Присвоїти інтерфейсу IP-адресу та маску підмережі (обов'язково).

Команди налагодження послідовних каналів зв'язку у мережах, побудованих на базі обладнання Cisco

Оскільки послідовні інтерфейси маршрутизаторів Cisco використовуються у багатьох технологіях та протоколах фізичного і канального рівнів моделі OSI, то для їх налагодження використовується достатньо великий набір команд, пов'язаних із різними аспектами функціонування того чи іншого протоколу або технології. Частина команд також використовується для налагодження певних параметрів, що належать до мережного рівня моделі OSI. Найбільш уживаними є команди: **interface, clock rate, description, ip address**, **shutdown**. Частовживаними є команди, що стосуються налагодження параметрів протоколів канального рівня інтерфейсів, зокрема команда вибору протоколу **encapsulation** та команди, які стосуються певних протоколів, – наприклад, похідні команди від команди **ppp**. Серед команд, які досить часто використовуються, слід згадати команди, що стосуються налагодження параметрів інтерфейсів: **keepalive**, **serial restart-delay**, **compress**, **crc**, **mtu**. Команди, які можуть використовуватися для впливу на розрахунок метрик протоколів маршрутизації: **bandwidth, delay**.

Для вибору інтерфейсу використовується команда **interface**. Команда **clock rate** призначена для налаштування частоти тактових імпульсів на одному (типу DCE) з пари інтерфейсів, що формують

прямий двоточковий послідовний канал між двома пристроями (з'єднання типу „нуль-модем"). У разі підключення маршрутизатора через DCE-пристрій (наприклад, CSU/DSU) команда не виконується, оскільки синхронізація здійснюється провайдером послуг. Команда **description** призначена для опису інтерфейсу, використовується з метою полегшення аналізу результатів виведення команд при адмініструванні. Команда **ip address** призначена для присвоєння IP-адреси інтерфейсові.

Команда **encapsulation** призначена для налагодження протоколу канального рівня на інтерфейсі. За замовчуванням на послідовних інтерфейсах налагоджено використання протоколу HDLC. Команда **ppp** та похідні від неї команди призначені для налагодження додаткових параметрів функціонування протоколу PPP (аутентифікація, шифрування, багатоканальність та ін.).

За допомогою команди **keepalive** зазначають інтервал, протягом якого маршрутизатор буде очікувати перед тим, як відправити через інтерфейс повідомлення про перевірку зв'язку для визначення, чи працює інтерфейс на іншому кінці послідовного каналу. Командою **serial restart-delay** встановлюють інтервал перезапуску інтерфейсу. Команда **compress** призначена для налагодження стиснення трафіка, який передається через інтерфейс. За допомогою команди **crc** змінюють довжину поля, що містить контрольну суму кадру. Командою **mtu** вказуються MTU інтерфейсу, це значення слід змінювати для оптимізації продуктивності мережі, наприклад, для каналів із великими втратами його необхідно зменшувати.

Команда **bandwidth** призначена для встановлення значення пропускної здатності, що використовується при обчисленні метрик маршрутів у протоколах маршрутизації, команда не встановлює швидкість передачі даних інтерфейсу і не впливає на фактичну швидкість передачі даних по каналу зв'язку. Команда **delay** призначена для встановлення значення затримки на інтерфейсі, це значення використовується при обчисленні метрик у деяких протоколах маршрутизації, команда не встановлює фізичних параметрів затримки на інтерфейсі.

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

interface *interface-type interface-id*,

де ***interface-type*** – тип інтерфейсу, для послідовних з'єднань набуває значення **Serial**;

interface-id – ідентифікатор інтерфейсу, може мати одночислове позначення ***number*** (номер інтерфейсу), двочислове позначення ***module/number*** (номер модуля (адаптера)/номер інтерфейсу), тричислове позначення ***slot/module/number*** (номер слоту/номер модуля (адаптера)/ номер інтерфейсу);

Синтаксис команди **bandwidth** (режим конфігурування інтерфейсу):

bandwidth *bw_value*,

де ***bw_value*** – значення пропускної здатності в Кбіт/с, за замовчуванням залежить від типу інтерфейсу.

Синтаксис команди **clock rate** (режим конфігурування інтерфейсу):

clock rate *bps_value*,

де ***bps_value*** – значення частоти тактових імпульсів (біт/с), може набувати значень 1200, 2400, 4800, 9600, 19 200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, 4000000; за замовчуванням не зазначається.

Синтаксис команди **delay** (режим конфігурування інтерфейсу):

delay *delay_value*,

де ***delay_value*** – значення затримки на інтерфейсі в десятках мілісекунд, за замовчуванням залежить від типу інтерфейсу.

Синтаксис команди **description** (режим конфігурування інтерфейсу):

description *text-line*,

де ***text-line*** – тестовий рядок опису інтерфейсу (до 240 символів).

Синтаксис команди **encapsulation** (режим конфігурування інтерфейсу):

encapsulation *type* { *commands* ... },

де ***type*** – параметр, який зазначає протокол або технологію інкапсуляції канального рівня, може набувати значень **atm-dxi**, **bstun**, **frame-relay**, **hdlc**, **lapb**, **ppp**, **sdlc**, **sdlc-primary**, **sdlc-secondary**, **smds**, **stun**, **x25**;

commands – додаткові параметри, залежно від протоколу або технології.

Синтаксис команди **ip address** (режим конфігурування інтерфейсу):

ip address *IP-address network_mask*,

де ***IP-address*** – IP-адреса у десятковому записі;

network_mask – маска мережі, записана у звичайній формі.

Синтаксис команди **mtu** (режим конфігурування інтерфейсу):

mtu *mtu_value*,

де ***mtu_value*** – значення MTU у байтах, число з діапазону 64 ... 17940; значення за замовчуванням залежить від технології або протоколу канального рівня.

Синтаксис команди **compress** (режим конфігурування інтерфейсу):

compress { stac | predictor | lzs | mppc },

де **stac** – тип стиснення, який використовує більше пропускної здатності, але менше процесорного часу і пам'яті маршрутизатора (використовується для з'єднань як протоколу PPP, так і HDLC);

predictor – тип стиснення, який використовує більше процесорного часу і пам'яті маршрутизатора, але менше пропускної здатності (використовується для з'єднань протоколу PPP);

lzs – тип стистення, який базується на алгоритмі LZS (використовується для з'єднань протоколу PPP);

mppc – тип стистення, який базується на алгоритмі MPPC (Microsoft Point-to-Point Compression) (використовується для з'єднань протоколу PPP).

Синтаксис команди **crc** (режим конфігурування інтерфейсу):

crc *crc_value*,

де ***crc_value*** – параметр, який вказує довжину поля контрольної суми в кадрі (у бітах), може набувати значень 16 або 32; за замовчуванням дорівнює 16 бітів.

Синтаксис команди **keepalive** (режим конфігурування інтерфейсу):

keepalive *seconds*,

де ***seconds*** – значення інтервалу часу очікування, яке задається у секундах, за замовчуванням становить 10 с.

Синтаксис команди **serial restart-delay** (режим конфігурування інтерфейсу):

serial restart-delay *seconds*,

де ***seconds*** – значення інтервалу часу рестарту, яке задається у секундах у діапазоні від 0 до 900, за замовчуванням становить 0 с.

Команди налагодження функціонування протоколу PPP для послідовних каналів зв'язку мереж, побудованих на базі маршрутизаторів Cisco

Для налагодження функціонування протоколу PPP на послідовних інтерфейсах маршрутизатора використовується досить велика кількість підкоманд команди **ppp**, пов'язаних із різними аспектами функціонування протоколу, зокрема це команди: **ppp accm**, **ppp accounting**, **ppp acfc**, **ppp authentication**, **ppp authorization**, **ppp bcp**, **ppp bridge**, **ppp caller**, **ppp chap**, **ppp direction**, **ppp disconnect-cause**, **ppp dnis**, **ppp eap**, **ppp encrypt**, **ppp ipcp**, **ppp iphc**, **ppp lcp**, **ppp link**, **ppp loopback**, **ppp max-bad-auth**, **ppp max-configure**, **ppp max-failure**, **ppp max-terminate**, **ppp ms-chap**, **ppp ms-chap-v2**, **ppp mtu**, **ppp multilink**, **ppp ncp**, **ppp pap**, **ppp pfc**, **ppp quality**, **ppp reliable-link**, **ppp timeout.** Призначення основних команд **ppp** наведено нижче.

Команда **ppp authentication** призначена для налагодження протоколу аутентифікації. Основними протоколами аутентифікації є протоколи CHAP та PAP, можливе використання й інших протоколів: EAP, MS-CHAP тощо. Додаткові параметри аутентифікації налагоджуються за допомогою команд **ppp chap**, **ppp pap**, **ppp eap**, **ppp ms-chap**, **ppp ms-chap-v2**. Для встановлення шифрування даних за протоколом MPPE (Microsoft Point-to-Point Encryption) використовується команда **ppp encrypt mppe**. Для встановлення контролю надійності каналу на одному з його інтерфейсів використовується команда **ppp quality**. Якщо значення надійності стає меншим, ніж вказане значення, канал перезавантажується. Для активації перевірки помилок канального рівня використовується команда **ppp reliable-link**. Ця процедура допомагає при пересилці UDP-датаграм. Для налаштування значення MTU використовується команда **ppp mtu**. Для налагодження багатоканальних послідовних PPP-з'єднань використовуються команди **interface multilink, ppp multilink**, **ppp multilink group**.

Синтаксис основних команд налагодження протоколу PPP та режими їх застосування наведено нижче.

Синтаксис команди **ppp authentication** (режим конфігурування інтерфейсу):

ppp authentication {chap | chap pap | pap chap | pap} [if-needed ...],

де **chap** – параметр, який використовується для встановлення протоколу аутентифікації CHAP;

chap pap – параметри, які використовуються для встановлення початкового протоколу аутентифікації CHAP, наступного – PAP; у випадку неможливості аутентифікації за протоколом CHAP проводиться аутентифікація за протоколом PAP;

pap chap – аналогічно попередньому пункту;

pap – параметр, який використовується для встановлення протоколу аутентифікації PAP;

if-needed – службова конструкція для активації додаткових параметрів аутентифікації.

Синтаксис команди **ppp chap** (режим конфігурування інтерфейсу):

ppp chap {{hostname *name-string* } | { password { *password-level password-string* | *password-string* } } | { refuse [callin] } | wait },

де **hostname** – службова конструкція, яка вказує на необхідність використання як параметра аутентифікації альтернативної текстової назви пристрою;

name-string – альтернативна текстова назва пристрою;

password – службова конструкція, яка вказує на необхідність використання паролю;

password-level – рівень шифрування паролю, може набувати значень від 0 до 7; якщо використовується значення 0, то пароль не зашифровується;

password-string – текстовий рядок паролю;

refuse – службова конструкція, яка призначена для встановлення відмови від аутентифікації з використанням протоколу CHAP;

callin – службова конструкція, яка призначена для встановлення відмови від аутентифікації з використанням протоколу CHAP для вхідних з'єднань;

wait – службова конструкція, яка призначена для активації очікування спроби аутентифікації від іншого кінця каналу.

Синтаксис команди **ppp pap** (режим конфігурування інтерфейсу):

ppp pap { refuse [callin] | { sent-username *name-string* password { *password-level password-string* | *password-string* } } | wait },

де **refuse** – службова конструкція, яка призначена для встановлення відмови від аутентифікації з використанням протоколу PAP;

callin – службова конструкція, яка призначена для встановлення відмови від аутентифікації з використанням протоколу PAP для вхідних з'єднань;

sent-username – службова конструкція, яка вказує на необхідність використання як параметра аутентифікації імені і паролю;

password-level – рівень шифрування паролю, може набувати значень від 0 до 7; якщо використовується значення 0, то пароль не шифрується;

password-string – текстовий рядок паролю;

wait – службова конструкція, яка призначена для активації очікування спроби аутентифікації від іншого кінця каналу.

Синтаксис команди **ppp encrypt mppe** (режим конфігурування інтерфейсу):

ppp encrypt mppe {40 | 128 | auto },

де **40** – шифрування з використанням тільки 40-бітних ключів;

128 – шифрування з використанням тільки 128-бітних ключів;

auto – конструкція, використання якої дозволяє пропонувати як 40- так і 128-бітні ключі.

Синтаксис команди **ppp quality** (режим конфігурування інтерфейсу):

ppp quality *percentage_value*,

де ***percentage_value*** – значення надійності у відсотках.

Синтаксис команди **ppp reliable-link** (режим конфігурування інтерфейсу):

ppp reliable-link.

Команда не має параметрів.

Синтаксис команди **ppp mtu adaptive** (режим конфігурування інтерфейсу):

ppp mtu adaptive.

Команда не має параметрів.

Синтаксис команди **interface multilink** (режим глобального конфігурування):

interface multilink *group-number*,

де ***group_value*** – значення номера групи, число з діапазону 1 ... 2147483647.

Синтаксис команди **ppp multilink** (режим конфігурування інтерфейсу):

ppp multilink [{ group *group_value*} | { endpoint ... } | ...] ,

де **group** – службова конструкція, яка використовується для створення групи;

group_value – значення номера групи, число з діапазону 1 ... 2147483647.

Команди моніторингу та діагностики роботи послідовних каналів на маршрутизаторах Cisco

Для визначення параметрів послідовних інтерфейсів та параметрів налагоджених протоколів інкапсуляції канального рівня, а також для моніторингу і діагностики роботи послідовних каналів використовуються команди **show controllers** та **show interfaces**. Для отримання більш детальної інформації стосовно протоколу PPP використовуються команди, похідні від команди **show ppp**. Для відстеження роботи послідовних інтерфейсів використовуються команди **debug serial**. Для відстеження повідомлень протоколу PPP призначені команди **debug ppp**. Узагальнений перелік команд моніторингу та діагностики наведений у табл. 1.

Таблиця 1

Перелік команд моніторингу та діагностики послідовних каналів та протоколів HDLC і PPP на маршрутизаторах Cisco

Команда	Призначення
show controllers ***interface-type interface-id***	Виведення деталізованої інформації про стан контролера конкретного послідовного інтерфейсу
show interfaces	Виведення деталізованої інформації про всі фізичні і логічні інтерфейси пристрою
show interface ***interface-type interface-id***	Виведення деталізованої інформації про конкретний інтерфейс пристрою
show compress	Виведення інформації про використання алгоритмів стистення
show compress details	Виведення деталізованої інформації про використання алгоритмів стистення
show ppp bap counter	Виведення інформації про лічильники протоколу BAP
show ppp bap group	Виведення інформації про групу протоколу BAP
show ppp bap queues	Виведення інформації про черги протоколу BAP
show ppp multilink	Виведення узагальненої інформації про функціонування багатоканальних послідовних PPP-з'єднань
show ppp multilink active	Виведення інформації про активні багатоканальні послідовні PPP-з'єднання
show ppp multilink endpoint	Виведення інформації лише про багатоканальні послідовні PPP-з'єднання, дескриптори яких збігаються з указаним значенням
show ppp multilink inactive	Виведення інформації про неактивні багатоканальні послідовні PPP-з'єднання
show ppp multilink interface	Виведення інформації про конкретний багатокальний інтерфейс пристрою
show ppp multilink username	Виведення інформації лише про багатоканальні послідовні PPP-з'єднання, які збігаються з указаним значенням імені

Модельний приклад налагодження параметрів послідовного каналу, побудованого між маршрутизаторами Cisco

Розглянемо специфіку налагодження послідовних інтерфейсів маршрутизаторів Cisco у ході організації двоточкового послідовного каналу, що зображений на рис. 2.

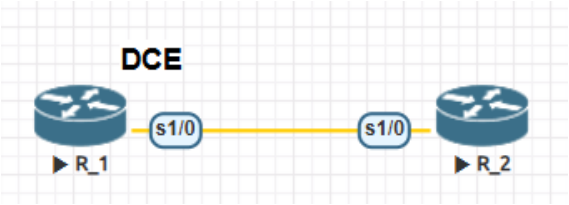


Рис. 2. Приклад мережі

Під час побудови даного каналу для з'єднання пристроїв використано дані табл. 2. Для налаштування параметрів адресації пристроїв використано дані табл. 3.

Таблиця 2

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R_1	Se1/0 (DCE)	Маршрутизатор R_2	Se1/0 (DTE)
Маршрутизатор R_2	Se1/0 (DTE)	Маршрутизатор R_1	Se1/0 (DCE)

Таблиця 3

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	–	196.1.1.0	255.255.255.252	/30
Маршрутизатор R_1	Інтерфейс Se1/0	196.1.1.1	255.255.255.252	/30
Маршрутизатор R_2	Інтерфейс Se1/0	196.1.1.2	255.255.255.252	/30

Сценарії налагодження параметрів послідовних інтерфейсів та параметрів адресації для маршрутизаторів R_1 та R_2 за умови використання встановленого за замовчуванням канального протоколу HDLC наведені нижче.

...
R_1>enable
R_1#configure terminal
R_1(config)#interface Serial 1/0
R_1(config-if)#description LINK_TO_R_2
R_1(config-if)#keepalive 5
R_1(config-if)#serial restart-delay 3
R_1(config-if)#clock rate 64000
R_1(config-if)#mtu 1492
R_1(config-if)#crc 32
R_1(config-if)#ip address 196.1.1.1 255.255.255.252
R_1(config-if)#no shutdown
R_1(config-if)#exit
...
R_2>enable
R_2#configure terminal
R_2(config)#interface Serial 1/0
R_2(config-if)#description LINK_TO_R_1
R_2(config-if)#keepalive 5
R_2(config-if)#serial restart-delay 3
R_2(config-if)#crc 32
R_2(config-if)#mtu 1492
R_2(config-if)#ip address 196.1.1.2 255.255.255.252
R_2(config-if)#no shutdown
R_2(config-if)#exit
...

Результати виконання основних команд діагностики на маршрутизаторах R_1 та R_2 для даних сценаріїв наведено на рис. 3–6.

```
R_1#show controllers serial 1/0
Interface Serial1/0
Hardware is GT96K
DCE 530, clock rate 64000
idb at 0x6570905C, driver data structure at 0x65710780
wic_info 0x65710D84
Physical Port 1, SCC Num 1
...
```

Рис. 3. Результати виконання команди **show controllers Serial 1/0** на маршрутизаторі R_1

```
R_2#show controllers serial 1/0
Interface Serial1/0
Hardware is GT96K
DTE 530 serial cable attached
idb at 0x6570905C, driver data structure at 0x65710780
wic_info 0x65710D84
Physical Port 1, SCC Num 1
...
```

Рис. 4. Результати виконання команди **show controllers Serial 1/0** на маршрутизаторі R_2

```
R_1#show interfaces Serial 1/0
Serial1/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: LINK_TO_R_2
  Internet address is 196.1.1.1/30
  MTU 1492 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (5 sec)
  Restart-Delay is 3 secs
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/1/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 1/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6 packets input, 1038 bytes, 0 no buffer
     Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     56 packets output, 3123 bytes, 0 underruns
     0 output errors, 0 collisions, 78 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
R_1#
```

Рис. 5. Результати виконання команди **show interface Serial 1/0** на маршрутизаторі R_1

```
R_2#show interfaces Serial 1/0
Serial1/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: LINK_TO_R_1
  Internet address is 196.1.1.2/30
  MTU 1492 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (5 sec)
  Restart-Delay is 3 secs
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/1/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 1/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     100 packets input, 5073 bytes, 0 no buffer
     Received 100 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     50 packets output, 2988 bytes, 0 underruns
     0 output errors, 0 collisions, 6 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
R_2#
```

Рис. 6. Результати виконання команди **show interface Serial 1/0** на маршрутизаторі R_2

Сценарії налагодження параметрів інтерфейсів та параметрів адресації для маршрутизаторів R_1, R_2 за умови використання протоколу PPP та стиснення даних за протоколом MPCC наведені нижче.

```
...
R_1>enable
R_1#configure terminal
R_1(config)#interface Serial 1/0
R_1(config-if)#description LINK_TO_R_2
R_1(config-if)#keepalive 5
R_1(config-if)#serial restart-delay 3
R_1(config-if)#clock rate 64000
R_1(config-if)#mtu 1492
R_1(config-if)#encapsulation ppp
R_1(config-if)#compress mppc
R_1(config-if)#ip address 196.1.1.1 255.255.255.252
R_1(config-if)#no shutdown
R_1(config-if)#exit
...
R_2>enable
R_2#configure terminal
R_2(config)#interface Serial 1/0
R_2(config-if)#description LINK_TO_R_1
R_2(config-if)#keepalive 5
R_2(config-if)#serial restart-delay 3
R_2(config-if)#mtu 1492
R_2(config-if)#encapsulation ppp
R_2(config-if)#compress mppc
R_2(config-if)#ip address 196.1.1.2 255.255.255.252
R_2(config-if)#no shutdown
R_2(config-if)#exit
...
```

Результати виконання основних команд діагностики на маршрутизаторах R_1 та R_2 для даних сценаріїв наведено на рис. 7, 8.

```
R_1#show interfaces serial 1/0
Serial1/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: LINK_TO_R2
  Internet address is 196.1.1.1/30
  MTU 1492 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CCP, CDPCP, loopback not set
  Keepalive set (5 sec)
  Restart-Delay is 3 secs
  Last input 00:00:11, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:00:54
  Input queue: 0/75/1/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 1/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     31 packets input, 1429 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     36 packets output, 1492 bytes, 0 underruns
     0 output errors, 0 collisions, 7 interface resets
     5 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
R_1#
```

Рис. 7. Результати виконання команди **show interface Serial 1/0** на маршрутизаторі R_1

```
R_2#show interfaces serial 1/0
Serial1/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: LINK_TO_R_1
  Internet address is 196.1.1.2/30
  MTU 1492 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CCP, CDPCP, loopback not set
  Keepalive set (5 sec)
  Restart-Delay is 3 secs
  Last input 00:00:25, output 00:00:03, output hang never
  Last clearing of "show interface" counters 00:02:27
  Input queue: 0/75/1/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 1/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     72 packets input, 2318 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     72 packets output, 2326 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
R_2#
```

Рис. 8. Результати виконання команди **show interface Serial 1/0** на маршрутизаторі R_2

Сценарії налагодження протоколу аутентифікації CHAP для маршрутизаторів R_1, R_2 наведені нижче.

```
...
R_1>enable
R_1#configure terminal
R_1(config)#username R_2 password mypass
R_1(config)#interface Serial 1/0
R_1(config-if)#ppp authentication chap
...
...
R_2>enable
R_2#configure terminal
R_2(config)#username R_1 password mypass
R_2(config)#interface Serial 1/0
R_2(config-if)#ppp authentication chap
...
```

Сценарії налагодження протоколу аутентифікації PAP для маршрутизаторів R_1, R_2 наведені нижче.

```
...
R_1>enable
R_1#configure terminal
R_1(config)#username R_2 password mypass
R_1(config)#interface Serial 1/0
R_1(config-if)#encapsulation ppp
R_1(config-if)#ppp authentication PAP
R_1(config-if)#ppp pap sent-username R_1 password mypass
...
...
R_2>enable
R_2#configure terminal
R_2(config)#username R_1 password mypass
R_2(config)#interface Serial 1/0
R_2(config-if)#encapsulation ppp
R_2(config-if)#ppp authentication PAP
R_2(config-if)#ppp pap sent-username R_2 password mypass
...
```

Завдання на лабораторну роботу

1. У середовищі віртуальної мережевої лабораторія eve.ztu.edu.ua створити проєкт мережі (рис. 9), або завантажити готовий проєкт прикріплений під методичними рекомендаціями.

2. Розробити схему адресації пристроїв мережі. Для цього скористатися даними табл. 4. Результати навести у вигляді таблиці, яка аналогічна табл. 3.

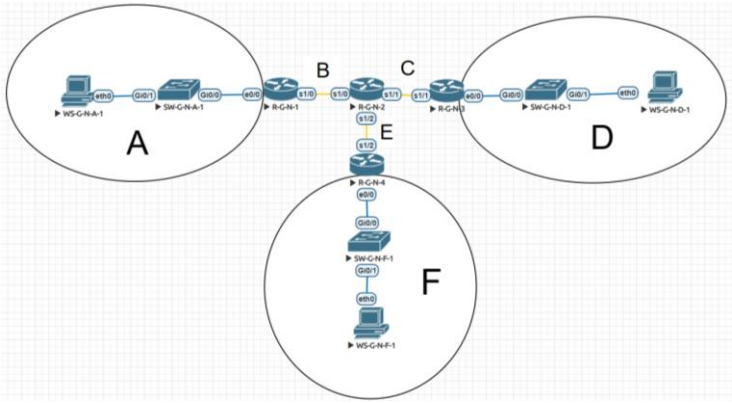


Рис. 9. Проект мережі

3. Провести базове налагодження пристроїв, інтерфейсів та каналів зв'язку (для каналів B, C, E для вибору параметрів каналів та протоколів канального рівня скористатися даними табл. 5, 6). Провести налагодження параметрів IP-адресації пристроїв мережі відповідно до даних, які отримані у п. 2. Перевірити наявність зв'язку між сусідніми парами пристроїв мережі.

4. Дослідити процеси функціонування налагоджених послідовних каналів зв'язку та реакцію маршрутизаторів на відключення або зміни параметрів інтерфейсів, що використовуються для формування послідовних каналів зв'язку. Дослідження виконувати за допомогою відповідних службових та діагностичних команд.

5. Налагодити функціонування засобів маршрутизації у побудованій мережі (для вибору методу/протоколу маршрутизації скористатися даними табл. 7) та перевірити доступність ресурсів мереж.

6. Дослідити процеси передачі даних між вузлами віддалених підмереж. За відсутності зв'язку визначити проблеми та усунути їх.

Таблиця 4

Дані для адресації підмереж

№ варіанта	Підмережа A		Підмережа B		Підмережа C		Підмережа D		Підмережа E		Підмережа F	
	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс
Не парні	193.G.N.0	/25	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/27	197.G.N.8	/30	198.G.N.0	/24
Парні	193.G.N.0	/26	194.G.N.4	/30	195.G.N.20	/30	196.G.N.64	/27	197.G.N.28	/30	198.G.N.0	/25

Т аблиця 5

Параметри каналів зв'язку

№ варіанта	Канал B					Канал C					Канал E				
	Serial restart-delay, с	Keepalive, с	CRC, біт	MTU, байт	Стиснення	Serial restart-delay, с	Keepalive, с	CRC, біт	MTU, байт	Стиснення	Serial restart-delay, с	Keepalive, с	CRC, біт	MTU, байт	Стиснення
Не парні	0	5	16	1500	S	1	2	32	1424	L	1	2	16	1512	M
Парні	1	10	32	1496	S	1	4	16	1432	L	2	2	32	1524	P

Примітка: S – стиснення Stac, M – стиснення MPCC;
P – стиснення Predictor; L – стиснення LZS.

Т аблиця 6

Дані для налагодження протоколів канального рівня

№ варіанта	Канал B			Канал C			Канал E		
	Протокол канального рівня	Протокол аутентифікації	Тип шифрування	Протокол канального рівня	Протокол аутентифікації	Тип шифрування	Протокол канального рівня	Протокол аутентифікації	Тип шифрування
Не парні	HDLC	–	–	PPP	CHAP	40	PPP	PAP	40
Парні	HDLC	–	–	PPP	PAP	128	PPP	CHAP	128

Т аблиця 7

Дані для вибору методу/протоколу маршрутизації

№ варіанта	Не парні	Парні
Метод/протокол маршрутизації	OSPF	RIPv2

Контрольні питання

1. Інтерфейси послідовних каналів маршрутизаторів Cisco.
2. Загальна характеристика протоколу HDLC. Протоколи, похідні від протоколу HDLC.
3. Ролі вузлів та режими передачі протоколу HDLC.
4. Формат кадру HDLC. Типи кадрів протоколу HDLC.
5. Команди протоколу HDLC та їх застосування.
6. Загальна характеристика протоколу PPP.
7. Структура стеку протоколів PPP.
8. Формат кадру PPP. Типи кадрів протоколу PPP.
9. Команди протоколу PPP. Машина станів протоколу PPP.
10. Порівняльна характеристика протоколів HDLC та PPP.
11. Команди налагодження послідовних інтерфейсів на маршрутизаторах Cisco.
12. Команди налагодження протоколів інкапсуляції канального рівня послідовних інтерфейсів на маршрутизаторах Cisco.
13. Команди налагодження аутентифікації з використанням протоколів PAP/CHAP на маршрутизаторах Cisco.
14. Команди створення та налагодження послідовного багатоканального з'єднання з використанням протоколу PPP на маршрутизаторах Cisco.
15. Команди діагностики роботи послідовних інтерфейсів та протоколів канального рівня HDLC та PPP на маршрутизаторах Cisco.

Лабораторна робота № 4
НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПОСЛІДОВНИХ КАНАЛІВ ЗВ'ЯЗКУ У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження послідовних каналів зв'язку глобальних мереж; налагодити функціонування послідовних з'єднань глобальних мереж із використанням протоколів HDLC та PPP на базі обладнання Cisco; дослідити процеси передачі даних та особливості функціонування обладнання у побудованій мережі.

Теоретичні відомості

Загальні відомості про застосування послідовних каналів зв'язку у мережах, побудованих на базі обладнання Cisco

Послідовний двоточковий канал зв'язку між маршрутизаторами Cisco будується за типовою схемою, що наведена на рис. 1, *а*. В лабораторних умовах для побудових тестових та навчальних стендів використовується спрощена схема, наведена на рис. 1, *б*. Кабельні з'єднання між DTE та DCE-пристроями є з'єднаннями стандартів V.35, X.21, EIA/TIA-232, EIA/TIA-449, EIA-530 (TIA-530-A), EIA-612/613 (HSSI, High-Speed Serial Interface). Вибір з'єднувальних кабелів здійснюється за даними технічної документації залежно від стандартів та ролей (DTE чи DCE) відповідних послідовних інтерфейсів пристроїв. Як протоколи канального рівня, як правило, використовуються загальновживані протоколи HDLC та PPP.

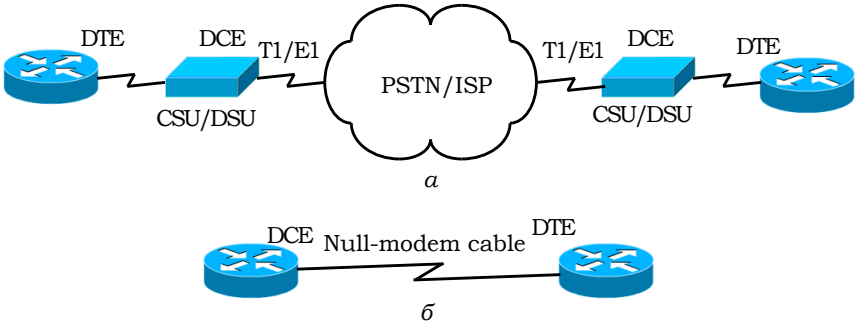


Рис. 1. Схеми побудови послідовного двоточкового каналу зв'язку

Порядок налагодження інтерфейсів послідовних каналів зв'язку у мережах, побудованих на базі обладнання Cisco

Налагодження функціонування послідовного інтерфейсу маршрутизатора Cisco для формування каналу зв'язку за рекомендаціями виробника передбачає такі етапи:

1. Вибрати та активувати послідовний інтерфейс (обов'язково).
2. Встановити тип інтерфейсу (DCE чи DTE). Для інтерфейсу DCE встановити параметри синхронізації (обов'язково).
3. Налагодити додаткові параметри функціонування каналу (необов'язково).
4. Налагодити протокол інкапсуляції канального рівня та додаткові параметри його функціонування (необов'язково).
5. Присвоїти інтерфейсу IP-адресу та маску підмережі (обов'язково).

Команди налагодження послідовних каналів зв'язку у мережах, побудованих на базі обладнання Cisco

Оскільки послідовні інтерфейси маршрутизаторів Cisco використовуються у багатьох технологіях та протоколах фізичного і канального рівнів моделі OSI, то для їх налагодження використовується достатньо великий набір команд, пов'язаних із різними аспектами функціонування того чи іншого протоколу або технології. Частина команд також використовується для налагодження певних параметрів, що належать до мережного рівня моделі OSI. Найбільш уживаними є команди: **interface, clock rate, description, ip address**, **shutdown**. Частовживаними є команди, що стосуються налагодження параметрів протоколів канального рівня інтерфейсів, зокрема команда вибору протоколу **encapsulation** та команди, які стосуються певних протоколів, – наприклад, похідні команди від команди **ppp**. Серед команд, які досить часто використовуються, слід згадати команди, що стосуються налагодження параметрів інтерфейсів: **keepalive**, **serial restart-delay**, **compress**, **crc**, **mtu**. Команди, які можуть використовуватися для впливу на розрахунок метрик протоколів маршрутизації: **bandwidth, delay**.

Для вибору інтерфейсу використовується команда **interface**. Команда **clock rate** призначена для налаштування частоти тактових імпульсів на одному (типу DCE) з пари інтерфейсів, що формують

прямий двоточковий послідовний канал між двома пристроями (з'єднання типу „нуль-модем"). У разі підключення маршрутизатора через DCE-пристрій (наприклад, CSU/DSU) команда не виконується, оскільки синхронізація здійснюється провайдером послуг. Команда **description** призначена для опису інтерфейсу, використовується з метою полегшення аналізу результатів виведення команд при адмініструванні. Команда **ip address** призначена для присвоєння IP-адреси інтерфейсові.

Команда **encapsulation** призначена для налагодження протоколу канального рівня на інтерфейсі. За замовчуванням на послідовних інтерфейсах налагоджено використання протоколу HDLC. Команда **ppp** та похідні від неї команди призначені для налагодження додаткових параметрів функціонування протоколу PPP (аутентифікація, шифрування, багатоканальність та ін.).

За допомогою команди **keepalive** зазначають інтервал, протягом якого маршрутизатор буде очікувати перед тим, як відправити через інтерфейс повідомлення про перевірку зв'язку для визначення, чи працює інтерфейс на іншому кінці послідовного каналу. Командою **serial restart-delay** встановлюють інтервал перезапуску інтерфейсу. Команда **compress** призначена для налагодження стиснення трафіка, який передається через інтерфейс. За допомогою команди **crc** змінюють довжину поля, що містить контрольну суму кадру. Командою **mtu** вказуються MTU інтерфейсу, це значення слід змінювати для оптимізації продуктивності мережі, наприклад, для каналів із великими втратами його необхідно зменшувати.

Команда **bandwidth** призначена для встановлення значення пропускної здатності, що використовується при обчисленні метрик маршрутів у протоколах маршрутизації, команда не встановлює швидкість передачі даних інтерфейсу і не впливає на фактичну швидкість передачі даних по каналу зв'язку. Команда **delay** призначена для встановлення значення затримки на інтерфейсі, це значення використовується при обчисленні метрик у деяких протоколах маршрутизації, команда не встановлює фізичних параметрів затримки на інтерфейсі.

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

interface *interface-type interface-id*,

де ***interface-type*** – тип інтерфейсу, для послідовних з'єднань набуває значення **Serial**;

interface-id – ідентифікатор інтерфейсу, може мати одночислове позначення ***number*** (номер інтерфейсу), двочислове позначення ***module/number*** (номер модуля (адаптера)/номер інтерфейсу), тричислове позначення ***slot/module/number*** (номер слоту/номер модуля (адаптера)/ номер інтерфейсу);

Синтаксис команди **bandwidth** (режим конфігурування інтерфейсу):

bandwidth *bw_value*,

де ***bw_value*** – значення пропускної здатності в Кбіт/с, за замовчуванням залежить від типу інтерфейсу.

Синтаксис команди **clock rate** (режим конфігурування інтерфейсу):

clock rate *bps_value*,

де ***bps_value*** – значення частоти тактових імпульсів (біт/с), може набувати значень 1200, 2400, 4800, 9600, 19 200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, 4000000; за замовчуванням не зазначається.

Синтаксис команди **delay** (режим конфігурування інтерфейсу):

delay *delay_value*,

де ***delay_value*** – значення затримки на інтерфейсі в десятках мілісекунд, за замовчуванням залежить від типу інтерфейсу.

Синтаксис команди **description** (режим конфігурування інтерфейсу):

description *text-line*,

де ***text-line*** – тестовий рядок опису інтерфейсу (до 240 символів).

Синтаксис команди **encapsulation** (режим конфігурування інтерфейсу):

encapsulation *type* { *commands* ... },

де ***type*** – параметр, який зазначає протокол або технологію інкапсуляції канального рівня, може набувати значень **atm-dxi**, **bstun**, **frame-relay**, **hdlc**, **lapb**, **ppp**, **sdlc**, **sdlc-primary**, **sdlc-secondary**, **smds**, **stun**, **x25**;

commands – додаткові параметри, залежно від протоколу або технології.

Синтаксис команди **ip address** (режим конфігурування інтерфейсу):

ip address *IP-address network_mask*,

де ***IP-address*** – IP-адреса у десятковому записі;

network_mask – маска мережі, записана у звичайній формі.

Синтаксис команди **mtu** (режим конфігурування інтерфейсу):

mtu *mtu_value*,

де ***mtu_value*** – значення MTU у байтах, число з діапазону 64 ... 17940; значення за замовчуванням залежить від технології або протоколу канального рівня.

Синтаксис команди **compress** (режим конфігурування інтерфейсу):

compress { stac | predictor | lzs | mppc },

де **stac** – тип стиснення, який використовує більше пропускної здатності, але менше процесорного часу і пам'яті маршрутизатора (використовується для з'єднань як протоколу PPP, так і HDLC);

predictor – тип стиснення, який використовує більше процесорного часу і пам'яті маршрутизатора, але менше пропускної здатності (використовується для з'єднань протоколу PPP);

lzs – тип стистення, який базується на алгоритмі LZS (використовується для з'єднань протоколу PPP);

mppc – тип стистення, який базується на алгоритмі MPPC (Microsoft Point-to-Point Compression) (використовується для з'єднань протоколу PPP).

Синтаксис команди **crc** (режим конфігурування інтерфейсу):

crc *crc_value*,

де ***crc_value*** – параметр, який вказує довжину поля контрольної суми в кадрі (у бітах), може набувати значень 16 або 32; за замовчуванням дорівнює 16 бітів.

Синтаксис команди **keepalive** (режим конфігурування інтерфейсу):

keepalive *seconds*,

де ***seconds*** – значення інтервалу часу очікування, яке задається у секундах, за замовчуванням становить 10 с.

Синтаксис команди **serial restart-delay** (режим конфігурування інтерфейсу):

serial restart-delay *seconds*,

де ***seconds*** – значення інтервалу часу рестарту, яке задається у секундах у діапазоні від 0 до 900, за замовчуванням становить 0 с.

Команди налагодження функціонування протоколу PPP для послідовних каналів зв'язку мереж, побудованих на базі маршрутизаторів Cisco

Для налагодження функціонування протоколу PPP на послідовних інтерфейсах маршрутизатора використовується досить велика кількість підкоманд команди **ppp**, пов'язаних із різними аспектами функціонування протоколу, зокрема це команди: **ppp accm**, **ppp accounting**, **ppp acfc**, **ppp authentication**, **ppp authorization**, **ppp bcp**, **ppp bridge**, **ppp caller**, **ppp chap**, **ppp direction**, **ppp disconnect-cause**, **ppp dnis**, **ppp eap**, **ppp encrypt**, **ppp ipcp**, **ppp iphc**, **ppp lcp**, **ppp link**, **ppp loopback**, **ppp max-bad-auth**, **ppp max-configure**, **ppp max-failure**, **ppp max-terminate**, **ppp ms-chap**, **ppp ms-chap-v2**, **ppp mtu**, **ppp multilink**, **ppp ncp**, **ppp pap**, **ppp pfc**, **ppp quality**, **ppp reliable-link**, **ppp timeout.** Призначення основних команд **ppp** наведено нижче.

Команда **ppp authentication** призначена для налагодження протоколу аутентифікації. Основними протоколами аутентифікації є протоколи CHAP та PAP, можливе використання й інших протоколів: EAP, MS-CHAP тощо. Додаткові параметри аутентифікації налагоджуються за допомогою команд **ppp chap**, **ppp pap**, **ppp eap**, **ppp ms-chap**, **ppp ms-chap-v2**. Для встановлення шифрування даних за протоколом MPPE (Microsoft Point-to-Point Encryption) використовується команда **ppp encrypt mppe**. Для встановлення контролю надійності каналу на одному з його інтерфейсів використовується команда **ppp quality**. Якщо значення надійності стає меншим, ніж вказане значення, канал перезавантажується. Для активації перевірки помилок канального рівня використовується команда **ppp reliable-link**. Ця процедура допомагає при пересилці UDP-датаграм. Для налаштування значення MTU використовується команда **ppp mtu**. Для налагодження багатоканальних послідовних PPP-з'єднань використовуються команди **interface multilink, ppp multilink**, **ppp multilink group**.

Синтаксис основних команд налагодження протоколу PPP та режими їх застосування наведено нижче.

Синтаксис команди **ppp authentication** (режим конфігурування інтерфейсу):

ppp authentication {chap | chap pap | pap chap | pap} [if-needed ...],

де **chap** – параметр, який використовується для встановлення протоколу аутентифікації CHAP;

chap pap – параметри, які використовуються для встановлення початкового протоколу аутентифікації CHAP, наступного – PAP; у випадку неможливості аутентифікації за протоколом CHAP проводиться аутентифікація за протоколом PAP;

pap chap – аналогічно попередньому пункту;

pap – параметр, який використовується для встановлення протоколу аутентифікації PAP;

if-needed – службова конструкція для активації додаткових параметрів аутентифікації.

Синтаксис команди **ppp chap** (режим конфігурування інтерфейсу):

ppp chap {{hostname *name-string* } | { password { *password-level password-string* | *password-string* } } | { refuse [callin] } | wait },

де **hostname** – службова конструкція, яка вказує на необхідність використання як параметра аутентифікації альтернативної текстової назви пристрою;

name-string – альтернативна текстова назва пристрою;

password – службова конструкція, яка вказує на необхідність використання паролю;

password-level – рівень шифрування паролю, може набувати значень від 0 до 7; якщо використовується значення 0, то пароль не зашифровується;

password-string – текстовий рядок паролю;

refuse – службова конструкція, яка призначена для встановлення відмови від аутентифікації з використанням протоколу CHAP;

callin – службова конструкція, яка призначена для встановлення відмови від аутентифікації з використанням протоколу CHAP для вхідних з'єднань;

wait – службова конструкція, яка призначена для активації очікування спроби аутентифікації від іншого кінця каналу.

Синтаксис команди **ppp pap** (режим конфігурування інтерфейсу):

ppp pap { refuse [callin] | { sent-username *name-string* password { *password-level password-string* | *password-string* } } | wait },

де **refuse** – службова конструкція, яка призначена для встановлення відмови від аутентифікації з використанням протоколу PAP;

callin – службова конструкція, яка призначена для встановлення відмови від аутентифікації з використанням протоколу PAP для вхідних з'єднань;

sent-username – службова конструкція, яка вказує на необхідність використання як параметра аутентифікації імені і паролю;

password-level – рівень шифрування паролю, може набувати значень від 0 до 7; якщо використовується значення 0, то пароль не шифрується;

password-string – текстовий рядок паролю;

wait – службова конструкція, яка призначена для активації очікування спроби аутентифікації від іншого кінця каналу.

Синтаксис команди **ppp encrypt mppe** (режим конфігурування інтерфейсу):

ppp encrypt mppe {40 | 128 | auto },

де **40** – шифрування з використанням тільки 40-бітних ключів;

128 – шифрування з використанням тільки 128-бітних ключів;

auto – конструкція, використання якої дозволяє пропонувати як 40- так і 128-бітні ключі.

Синтаксис команди **ppp quality** (режим конфігурування інтерфейсу):

ppp quality *percentage_value*,

де ***percentage_value*** – значення надійності у відсотках.

Синтаксис команди **ppp reliable-link** (режим конфігурування інтерфейсу):

ppp reliable-link.

Команда не має параметрів.

Синтаксис команди **ppp mtu adaptive** (режим конфігурування інтерфейсу):

ppp mtu adaptive.

Команда не має параметрів.

Синтаксис команди **interface multilink** (режим глобального конфігурування):

interface multilink *group-number*,

де ***group_value*** – значення номера групи, число з діапазону 1 ... 2147483647.

Синтаксис команди **ppp multilink** (режим конфігурування інтерфейсу):

ppp multilink [{ group *group_value*} | { endpoint ... } | ...] ,

де **group** – службова конструкція, яка використовується для створення групи;

group_value – значення номера групи, число з діапазону 1 ... 2147483647.

Команди моніторингу та діагностики роботи послідовних каналів на маршрутизаторах Cisco

Для визначення параметрів послідовних інтерфейсів та параметрів налагоджених протоколів інкапсуляції канального рівня, а також для моніторингу і діагностики роботи послідовних каналів використовуються команди **show controllers** та **show interfaces**. Для отримання більш детальної інформації стосовно протоколу PPP використовуються команди, похідні від команди **show ppp**. Для відстеження роботи послідовних інтерфейсів використовуються команди **debug serial**. Для відстеження повідомлень протоколу PPP призначені команди **debug ppp**. Узагальнений перелік команд моніторингу та діагностики наведений у табл. 1.

Таблиця 1

Перелік команд моніторингу та діагностики послідовних каналів та протоколів HDLC і PPP на маршрутизаторах Cisco

Команда	Призначення
show controllers ***interface-type interface-id***	Виведення деталізованої інформації про стан контролера конкретного послідовного інтерфейсу
show interfaces	Виведення деталізованої інформації про всі фізичні і логічні інтерфейси пристрою
show interface ***interface-type interface-id***	Виведення деталізованої інформації про конкретний інтерфейс пристрою
show compress	Виведення інформації про використання алгоритмів стистення
show compress details	Виведення деталізованої інформації про використання алгоритмів стистення
show ppp bap counter	Виведення інформації про лічильники протоколу BAP
show ppp bap group	Виведення інформації про групу протоколу BAP
show ppp bap queues	Виведення інформації про черги протоколу BAP
show ppp multilink	Виведення узагальненої інформації про функціонування багатоканальних послідовних PPP-з'єднань
show ppp multilink active	Виведення інформації про активні багатоканальні послідовні PPP-з'єднання
show ppp multilink endpoint	Виведення інформації лише про багатоканальні послідовні PPP-з'єднання, дескриптори яких збігаються з указаним значенням
show ppp multilink inactive	Виведення інформації про неактивні багатоканальні послідовні PPP-з'єднання
show ppp multilink interface	Виведення інформації про конкретний багатокальний інтерфейс пристрою
show ppp multilink username	Виведення інформації лише про багатоканальні послідовні PPP-з'єднання, які збігаються з указаним значенням імені

Модельний приклад налагодження агрегованого послідовного каналу, побудованого між маршрутизаторами Cisco

Розглянемо специфіку налагодження послідовних інтерфейсів маршрутизаторів Cisco у ході організації агрегованого послідовного каналу, що зображений на рис. 2. Як протокол канального рівня використовується протокол PPP.

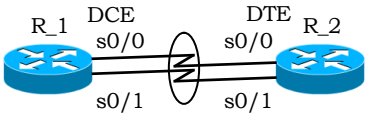


Рис. 2. Приклад мережі

Під час побудови даного каналу для з'єднання пристроїв використано дані табл. 4. Для налаштування параметрів адресації пристроїв використано дані табл. 5.

Таблиця 2

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс		Підключення до пристрою	Підключення до інтерфейсу	
Маршрутизатор R_1	Multilink 1	Se1/0 (DCE)	Маршрутизатор R_2	Multilink 1	Se1/0 (DTE)
		Se1/1 (DCE)			Se1/1 (DTE)
Маршрутизатор R_2	Multilink 1	Se1/0 (DTE)	Маршрутизатор R_1	Multilink 1	Se1/0 (DCE)
		Se1/1 (DTE)			Se1/1 (DCE)

Таблиця 3

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа А	–	196.1.1.0	255.255.255.252	/30
Маршрутизатор R_1	Інтерфейс Multilink 1	196.1.1.1	255.255.255.252	/30
Маршрутизатор R_2	Інтерфейс Multilink 1	196.1.1.2	255.255.255.252	/30

Сценарії налагодження параметрів інтерфейсів агрегованого каналу та параметрів адресації для маршрутизаторів R_1, R_2 за умови використання протоколу PPP та стиснення даних за протоколом LZS наведені нижче.

```
...
R_1(config)# interface Multilink 1
R_1(config-if)#description AGGREGATED_LINK_TO_R_2
R_1(config-if)#ip address 196.1.1.1 255.255.255.252
R_1(config-if)#ppp multilink
R_1(config-if)#ppp multilink group 1
R_1(config-if)#compress lzs
R_1(config-if)#exit
R_1(config)#interface Serial 0/0
R_1(config-if)#encapsulation ppp
R_1(config-if)#ppp multilink
R_1(config-if)#ppp multilink group 1
R_1(config-if)#no shutdown
R_1(config-if)#exit
R_1(config)#interface Serial 0/1
R_1(config-if)#encapsulation ppp
R_1(config-if)#ppp multilink
R_1(config-if)#ppp multilink group 1
R_1(config-if)#no shutdown
R_1(config-if)#exit
R_1(config)#
...
R_2(config)#interface Multilink 1
R_2(config-if)# description AGGREGATED_LINK_TO_R_1
R_2(config-if)# ip address 196.1.1.2 255.255.255.252
R_2(config-if)# ppp multilink
R_2(config-if)# ppp multilink group 1
R_2(config-if)#compress lzs
R_2(config-if)#exit
R_2(config)#interface Serial 0/0
R_2(config-if)#encapsulation ppp
R_2(config-if)#ppp multilink
R_2(config-if)#ppp multilink group 1
R_2(config-if)#no shutdown
R_2(config-if)#exit
R_2(config)#interface Serial 0/1
R_2(config-if)#encapsulation ppp
R_2(config-if)#ppp multilink
R_2(config-if)#ppp multilink group 1
R_2(config-if)#no shutdown
R_2(config-if)#exit
R_2(config)#
...
```

Результати виконання основних команд діагностики на маршрутизаторах R_1 та R_2 для даних сценаріїв наведено на рис. 10–13.

```
R_1#show interfaces multilink 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Description: AGGREGATED_LINK_TO_R_2
  Internet address is 196.1.1.1/30
  MTU 1500 bytes, BW 3088 Kbit/sec, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open, multilink Open
  Open: IPCP, CCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 2 seconds on reset
  Last input 00:00:40, output never, output hang never
  Last clearing of "show interface" counters 00:05:20
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     8 packets input, 393 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     8 packets output, 393 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Рис. 3. Результати виконання команди **show interface multilink 1** на маршрутизаторі R_1

```
R_2#show interfaces multilink 1
Multilink1 is up, line protocol is up
  Hardware is multilink group interface
  Description: AGGREGATED_LINK_TO_R_1
  Internet address is 196.1.1.2/30
  MTU 1500 bytes, BW 3088 Kbit/sec, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open, multilink Open
  Open: IPCP, CCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 2 seconds on reset
  Last input 00:00:47, output never, output hang never
  Last clearing of "show interface" counters 00:03:17
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6 packets input, 377 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     9 packets output, 418 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

Рис. 4. Результати виконання команди **show interface multilink 1** на маршрутизаторі R_2

```
R_1#show ppp multilink

Multilink1, bundle name is R_2
  Endpoint discriminator is R_2
  Bundle up for 00:07:08, total bandwidth 3088, 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
    0x7 received sequence, 0x7 sent sequence
  Member links: 2 active, 0 inactive (max not set, min not set)
    Se0/0, since 00:07:08
    Se0/1, since 00:06:41
No inactive multilink interfaces
R_1#
```

Рис. 5 Результати виконання команди **show ppp multilink** на маршрутизаторі R_1

```
R_2#show ppp multilink

Multilink1, bundle name is R_1
  Endpoint discriminator is R_1
  Bundle up for 00:07:42, total bandwidth 3088, 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
    0x7 received sequence, 0x7 sent sequence
  Member links: 2 active, 0 inactive (max not set, min not set)
    Se0/0, since 00:07:42
    Se0/1, since 00:07:15
No inactive multilink interfaces
R_2#
```

Рис. 6. Результати виконання команди **show ppp multilink** на маршрутизаторі R_2

Завдання на лабораторну роботу

1. У середовищі віртуальної мережевої лабораторія eve.ztu.edu.ua створити проєкт мережі (рис. 7), або завантажити готовий проєкт прикріплений під методичними рекомендаціями. Для мережі заповнити описову таблицю, яка аналогічна табл. 2.

2. Розробити схему адресації пристроїв мережі. Для цього скористатися даними табл. 4. Результати навести у вигляді таблиці, яка аналогічна табл. 3.

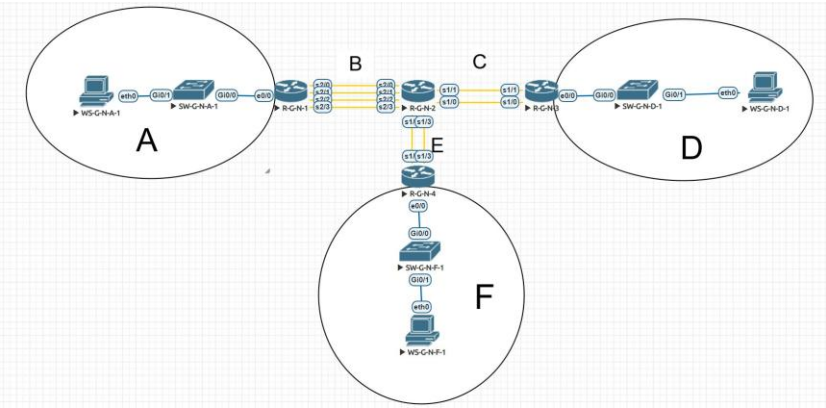


Рис. 7. Проект мережі

3. Провести базове налагодження пристроїв, інтерфейсів та каналів зв'язку (для каналів B, C, E для вибору параметрів каналів та протоколів канального рівня скористатися даними табл. 5 та 6). Провести налагодження параметрів IP-адресації пристроїв мережі відповідно до даних, які отримані у п. 2. Перевірити наявність зв'язку між сусідніми парами пристроїв мережі.

4. Дослідити процеси функціонування налагоджених послідовних каналів зв'язку та реакцію маршрутизаторів на відключення або зміни параметрів інтерфейсів, що використовуються для формування послідовних каналів зв'язку. Дослідження виконувати за допомогою відповідних службових та діагностичних команд.

5. Налагодити функціонування засобів маршрутизації у побудованій мережі (для вибору методу/протоколу маршрутизації

скористатися даними табл. 7) та перевірити доступність ресурсів мереж.

6. Дослідити процеси передачі даних між вузлами віддалених підмереж. За відсутності зв'язку визначити проблеми та усунути їх.

Таблиця 4

Дані для адресації підмереж

№ варіанта	Підмережа A		Підмережа B		Підмережа C		Підмережа D		Підмережа E		Підмережа F	
	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс
Непарні	193.G.N.0	/25	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/27	197.G.N.8	/30	198.G.N.0	/24
Парні	193.G.N.0	/26	194.G.N.4	/30	195.G.N.20	/30	196.G.N.64	/27	197.G.N.28	/30	198.G.N.0	/25

Таблиця 5

Параметри каналів зв'язку

№ варіанта	Канал B					Канал C					Канал E				
	Serial restart-delay, c	Keepalive, c	CRC, біт	MTU, байт	Стиснення	Serial restart-delay, c	Keepalive, c	CRC, біт	MTU, байт	Стиснення	Serial restart-delay, c	Keepalive, c	CRC, біт	MTU, байт	Стиснення
Непарні	0	5	16	1500	S	1	2	32	1424	L	1	2	16	1512	M
Парні	3	5	32	1488	M	2	8	16	1448	P	1	4	32	1548	S

Примітка: S – стиснення Stac, M – стиснення MPCC; P – стиснення Predictor; L – стиснення LZS.

Таблиця 6

Дані для налагодження протоколів канального рівня

№ варіанта	Канал B			Канал C			Канал E		
	Протокол канального рівня	Протокол аутентифікації	Тип шифрування	Протокол канального рівня	Протокол аутентифікації	Тип шифрування	Протокол канального рівня	Протокол аутентифікації	Тип шифрування
Непарні	HDLC	–	–	PPP	CHAP	40	PPP	PAP	40
Парні	PPP	CHAP	40	HDLC	–	–	PPP	PAP	auto

Таблиця 7

Дані для вибору методу/протоколу маршрутизації

№ варіанта	Метод/протокол маршрутизації
Не парні	Static
Парні	RIP

Контрольні питання

1. Інтерфейси послідовних каналів маршрутизаторів Cisco.
2. Загальна характеристика протоколу HDLC. Протоколи, похідні від протоколу HDLC.
3. Ролі вузлів та режими передачі протоколу HDLC.
4. Формат кадру HDLC. Типи кадрів протоколу HDLC.
5. Команди протоколу HDLC та їх застосування.
6. Загальна характеристика протоколу PPP.
7. Структура стеку протоколів PPP.
8. Формат кадру PPP. Типи кадрів протоколу PPP.
9. Команди протоколу PPP. Машина станів протоколу PPP.
10. Порівняльна характеристика протоколів HDLC та PPP.
11. Команди налагодження послідовних інтерфейсів на маршрутизаторах Cisco.
12. Команди налагодження протоколів інкапсуляції канального рівня послідовних інтерфейсів на маршрутизаторах Cisco.
13. Команди налагодження аутентифікації з використанням протоколів PAP/CHAP на маршрутизаторах Cisco.
14. Команди створення та налагодження послідовного багатоканального з'єднання з використанням протоколу PPP на маршрутизаторах Cisco.
15. Команди діагностики роботи послідовних інтерфейсів та протоколів канального рівня HDLC та PPP на маршрутизаторах Cisco.

Лабораторна робота № 5
НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ ДИНАМІЧНОГО РЕЗЕРВУВАННЯ ШЛЮЗУ VRRP У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження роботи протоколу динамічного резервування шлюзу VRRP на обладнанні Cisco; отримати практичні навички налагодження, моніторингу та діагностування роботи протоколу VRRP у мережі, побудованій на базі обладнання Cisco; дослідити процес роботи протоколу VRRP та процеси передачі даних у побудованій мережі.

Теоретичні відомості

Загальні відомості про протокол динамічного резервування шлюзу VRRP

Протокол VRRP (Virtual Router Redundancy Protocol) був розроблений як альтернатива закритим протоколам (у першу чергу фірмовому протоколу Cisco HSRP) і є єдиним на сьогодні стандартним відкритим протоколом динамічного резервування шлюзу. Окрім динамічного резервування шлюзу у протоколі VRRP існує можливість використання статичного балансування (розподілу) навантаження.

У розробці стандартів даного протоколу брали участь провідні фахівці багатьох світових розробників та виробників мережного обладнання та програмного забезпечення, зокрема, Ascend Communications Inc., Microsoft Inc., Nokia, Digital Equipment Corp., IBM Corporation, Ericsson. Основною організацією, яка координує розробку стандартів протоколу VRRP, є IETF. Відповідно цей протокол описаний у таких стандартах IETF: RFC-2338 „Virtual Router Redundancy Protocol", RFC-2787 „Definitions of Managed Objects for the Virtual Router Redundancy Protocol", RFC-3768 „Virtual Router Redundancy Protocol (VRRP)", RFC-5798 „Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", RFC-6527 „Definitions of Managed Objects for the Virtual Router Redundancy Protocol Version 3 (VRRPv3)". Питання застосування протоколу VRRP розглянуті і в деяких інших стандартах IETF, зокрема, RFC-5342 „IANA

Considerations and IETF Protocol Usage for IEEE 802 Parameters", RFC-7042 ,,IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters", які належать до категорії ,,Best Current Practice".

На базі протоколу VRRP провідні виробники мережного обладнання (зокрема, фірми Brocade Communications Systems, Inc та Hewlett-Packard Company) розробили тестову версію нового відкритого промислового протоколу VRRPE (VRRP Extended), у якому реалізували динамічне балансування навантаження.

Існують три версії протоколу VRRP. Сьогодні широко використовуються дві з них: VRRP Version 2, описана у RFC-3768 та орієнтована на функціонування в IP-мережах версії 4, і VRRP Version 3, описана у RFC-5798 та орієнтована на функціонування в IP-мережах версій 4 та 6.

Стосовно моделі OSI протокол VRRP є протоколом мережного рівня. Відповідно, стосовно стеку TCP/IP даний протокол є протоколом рівня міжмережної взаємодії. Повідомлення протоколу VRRP напряму інкапсулюються в IP-пакети, які у свою чергу інкапсулюються у кадри канального рівня відповідної мережної технології. Як адреси призначення в IP-пакетах використовуються IP-адреси групової розсилки, зарезервовані за протоколом VRRP. Групові MAC-адреси призначення у кадрах формуються за правилами перетворення групових IP-адрес.

Для забезпечення функціонування протоколу VRRP уведено поняття маршрутизатор VRRP (VRRP Router) та група резервування VRRP. Маршрутизатором VRRP є будь-який маршрутизатор, на якому активовано використання протоколу VRRP. До групи резервування протоколу VRRP входять активний маршрутизатор VRRP (VRRP Master Router, VRRP Virtual Router Master) та резервні маршрутизатори VRRP (VRRP Backup Routers, VRRP Virtual Router Backups). Оскільки одна група резервування VRRP передбачає підтримку функціонування одного віртуального маршрутизатора (VRRP Virtual Router), то для її позначення використовується ідентифікатор віртуального маршрутизатора VRID (VRRP Virtual Router IDentifier). Цій групі відповідають одна віртуальна адреса мережного рівня (VRRP Virtual IP-Address) та одна віртуальна адреса канального рівня (VRRP Virtual MAC-Address). Virtual IP-Address – це адреса шлюзу за замовчуванням для кінцевих вуз-

лів мережі. У протоколі VRRP наявне поняття власника IP-адреси (VRRP IP-Address Owner) – це маршрутизатор VRRP, що використовує IP-адресу, призначену віртуальному маршрутизатору, як реальну IP-адресу, призначену інтерфейсу. Оскільки функції віртуального маршрутизатора VRRP фактично виконує активний маршрутизатор VRRP, то саме через нього здійснюється фізична пересилка IP-пакетів до інших мереж. Слід зазначити, що один реальний маршрутизатор може бути членом кількох груп резервування VRRP, в одних групах він може бути активним, в інших – резервним. За рахунок цієї властивості реалізовуються схеми підключення локальних мереж, у яких необхідне статичне балансування навантаження.

Вибори активного маршрутизатора VRRP здійснюються на основі механізму пріоритетів (Priority). Пріоритет може набувати значень у діапазоні від 0 до 255. Маршрутизатор із найбільшим пріоритетом вибирається як активний маршрутизатор VRRP, йому призначаються віртуальні IP-адреса і MAC-адреса, і на нього покладаються функції маршрутизації. Решта маршрутизаторів групи резервування є резервними маршрутизаторами. Якщо пріоритети маршрутизаторів, які претендують на роль активного, однакові, то виконується порівняння їх IP-адрес і маршрутизатор із найбільшою адресою стає активним маршрутизатором VRRP.

Правила протоколу VRRP передбачають, що активний маршрутизатор групи резервування періодично (через інтервал Advertisement Interval) розсилає службові повідомлення для підтвердження свого статусу, відомі як VRRP-оголошення (VRRP Advertisement). Структури повідомлення протоколу VRRP версій 2 та 3 наведені у додатку Б. Якщо VRRP-оголошення відсутні протягом певного проміжку часу (Master Down Interval), то вважається, що активний маршрутизатор вийшов із ладу (або вимкнений примусово) і активним стає той з резервних маршрутизаторів, пріоритет якого є найбільшим. Значення інтервалу Advertisement Interval встановлюється за замовчуванням і може змінюватися адміністратором мережі.

Значення інтервалу Master Down Interval розраховується за спеціальною формулою:

$$Master\_Down\_Interval = 3 \times Advertisement\_Interval + Scew\_Time,$$

де *Master_Down_Interval* – інтервал Master Down Interval, с;
Advertisement_Interval – інтервал Advertisement Interval, с;
Scew_Time – час відхилення, с.

Значення часу відхилення розраховується за формулою:

$$Scew\_Time = (256 - Priority)/256,$$

де *Priority* – значення пріоритету VRRP-маршрутизатора.

У роботі протоколу VRRP використовуються два службові таймери: Adver Timer та Master Down Timer. Таймер Adver Timer – це таймер, який спрацьовує для ініціалізації відправлення VRRP-оголошень, він формується за допомогою значення інтервалу Advertisement Interval. Таймер Master Down Timer – це таймер, який спрацьовує у тому разі, коли VRRP-оголошення не приходило протягом інтервалу Master Down Interval.

У ході виконання операцій протоколу маршрутизатор VRRP групи резервування може знаходитися в одному з таких станів:

– початковий стан (*Initialize State*);

– стан активного маршрутизатора (*Master State/Master Router*);

– стан резервного маршрутизатора (*Backup State/Backup Router*).

Діаграма змін станів маршрутизатора VRRP наведена на рис. 1. Ця діаграма використовується в усіх версіях протоколу VRRP. Відмітності стосуються лише умов переходів між станами. Для VRRP версії 2 ці умови описано нижче.

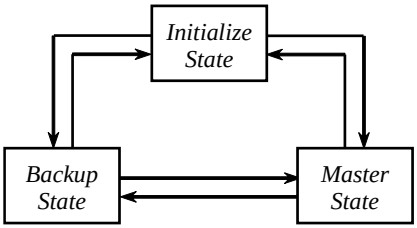


Рис. 1. Діаграма змін станів маршрутизатора VRRP

Початково VRRP-маршрутизатор знаходиться у стані *Initialize State*. У цьому стані він очікує на подію, яка сигналізує про

початок роботи протоколу (Startup Event). Після того, як використання протоколу VRRP на маршрутизаторі активовано, виконується перевірка, чи дорівнює пріоритет пристрою 255 (тобто чи є маршрутизатор власником IP-адреси, призначеної віртуальному маршрутизатору).

Якщо пріоритет дійсно дорівнює 255, то маршрутизатор повинен виконувати такі дії:

– розсилати повідомлення-оголошення VRRP Advertisement;

– надіслати запит Gratuitous ARP (містить MAC-адресу віртуального маршрутизатора для кожної IP-адреси, що асоційована з віртуальним маршрутизатором);

– встановити значення таймера Adver Timer таким, що дорівнює значенню інтервалу Advertisement Interval;

– перейти до стану *Master State*.

Якщо ж пріоритет пристрою не дорівнює 255, то маршрутизатор повинен перейти до стану *Backup State*.

У стані *Backup State* маршрутизатор здійснює моніторинг доступності і стану активного маршрутизатора. У цьому стані маршрутизатор повинен виконувати такі дії:

– не відповідати на ARP-запити, що стосуються IP-адреси, асоційованої з віртуальним маршрутизатором;

– відкидати повідомлення з MAC-адресою отримувача, яка дорівнює MAC-адресі віртуального маршрутизатора;

– не повинен приймати повідомлення, що відправлені на IP-адресу, яка асоційована з віртуальним маршрутизатором;

– якщо на маршрутизаторі відключається функціонування протоколу VRPR (Shutdown Event), то маршрутизатор повинен обнулити таймер Master Down Timer та перейти до стану *Initialize State*;

– якщо спрацює таймер Master Down Timer, то маршрутизатор повинен: надіслати VRRP-оголошення, розіслати запит Gratuitous ARP (що містить MAC-адресу віртуального маршрутизатора для кожної IP-адреси, яка асоційована з віртуальним маршрутизатором), встановити значення таймера Adver Timer таким, що дорівнює Advertisement Interval, та перейти у стан *Master State*;

– якщо отримано VRRP-оголошення, то машрутизатор повинен виконати перевірку, чи дорівнює пріоритет в отриманому повідомленні 0; якщо ж пріоритет дорівнює 0, то встановити значення таймера Master Down Timer таким, що дорівнює Skew Time, у противному разі виконати такі дії: якщо значення Preempt дорівнює False або якщо пріоритет в отриманому повідомленні більший чи дорівнює локальному пріоритету, то встановити Master Down Timer таким, що дорівнює Master Down Interval; інакше – відкинути отримане VRRP-оголошення.

У стані *Master State* маршрутизатор відповідає за пересилку IP-пакетів, що спрямовуються на IP-адресу, яка асоційована з віртуальним маршрутизатором. У цьому стані маршрутизатор повинен виконувати такі дії:

– відповідати на ARP-запити, що спрямовані на IP-адресу, яка асоційована з віртуальним маршрутизатором;

– повинен опрацьовувати повідомлення з MAC-адресою отримувача, яка дорівнює MAC-адресі віртуального маршрутизатора;

– не повинен приймати повідомлення, що відправлені на IP-адресу, яка асоційована з віртуальним маршрутизатором, якщо він не є власником IP-адреси;

– повинен приймати повідомлення, що відправлені на IP-адресу, яка асоційована з віртуальним маршрутизатором, якщо він є власником IP-адреси;

– якщо на маршрутизаторі відключається функціонування протоколу VRPR (Shutdown Event), то маршрутизатор повинен обнулити таймер Adver Timer, надіслати VRRP-оголошення, у якому пріоритет дорівнює нулеві та перейти до стану *Initialize State*;

– якщо спрацює таймер Adver Timer, то маршрутизатор повинен: надіслати VRRP-оголошення, встановити значення Adver Timer таким, що дорівнює значенню Advertisement Interval;

– якщо отримано VRRP-оголошення, то машрутизатор повинен перевірити значення пріоритету у цьому оголошенні і якщо значення пріоритету дорівнює нулеві, то маршрутизатор повинен: надіслати VRRP-оголошення, встановити значення Adver Timer таким, що дорівнює значенню Advertisement Interval, якщо ж зна-

чення пріоритету в отриманому VRRP-оголошенні більше за значення локального пріоритету або якщо значення пріоритету в отриманому VRRP-оголошенні дорівнює локальному пріоритету й основна IP-адреса відправника більша від локальної основної IP-адреси, то маршрутизатор повинен: обнулити таймер Adver Timer, встановити значення Master Down Timer таким, що дорівнює значенню Master Down Interval, перейти до стану *Backup State,* інакше маршрутизатор повинен відкинути VRRP-оголошення.

Недоліком протоколу VRRP, у порівнянні з протоколом HSRP, є відсутність корисної функції контролю стану зовнішніх щодо VRRP інтерфейсів та канальних сегментів. Неможливість враховувати стан зовнішніх інтерфейсів та підключених каналів зв'язку робить процедуру вибору активного маршрутизатора досить формальною. Для усунення цього недоліку виробники обладнання вимушені реалізовувати спеціальні механізми контролю зовнішніх інтерфейсів, каналів та мереж, відомі як EOT (Enhanced Object Tracking). Функція перевиборів Preemt у протоколі VRRP наявна і діє подібно до аналогічної функції протоколу HSRP.

Параметри протоколу VRRP версії 2 за замовчуванням наведені у табл. 1.

Таблиця 1

Параметри протоколу VRRP версії 2 за замовчуванням

Характеристика/параметр	Значення
Функціонування протоколу за замовчуванням	неактивований
Групова IP-адреса призначення	224.0.0.18
Номер протоколу в IP-пакеті	112
Кількість груп резервування	до 256
Віртуальна MAC-адреса	00-00-5E-00-01-XX
Пріоритет інтерфейсу за замовчуванням	100
Інтервал Advertise Interval за замовчуванням, с	1
Інтервал Master Down Interval за замовчуванням, с	розраховується за формулою
Крок зміни пріоритету інтерфейсу пристрою при виконанні операції механізму EOT (Enhanced Object Tracking).	10

Примітка: XX – номер групи резервування VRRP.

Порядок налагодження функціонування протоколу VRRP на маршрутизаторі Cisco

Налагодження функціонування протоколу динамічного резервування шлюзу VRRP версії 2 на маршрутизаторі Cisco згідно з рекомендаціями виробника складається із певних обов'язкових та необов'язкових етапів. Порядок виконання згаданих етапів є таким:

1. Вибрати та активувати фізичний (Ethernet) інтерфейс маршрутизатора, налагодити параметри IP-адресації для обраного інтерфейсу (обов'язково).
2. Активувати функціонування протоколу на обраному інтерфейсі (обов'язково).
3. Зазначити текстовий опис групи резервування протоколу VRRP (необов'язково).
4. Налагодити параметри вибору (пріоритет) VRRP-маршрутизатора (необов'язково).
5. Налагодити часові параметри розсилки та опрацювання повідомлень протоколу (необов'язково).
6. Створити логічні об'єкти, пов'язані з контролем функціонування певних елементів мережі (фізичного каналу, маршруту у таблиці маршрутизації тощо), і налагодити параметри їх функціонування (необов'язково).
7. Налагодити параметри відстеження (контролю) стану зовнішніх щодо VRRP логічних об'єктів, пов'язаних із контролем функціонування певних фізичних і логічних елементів мережі, та параметри впливу на роботу протоколу в разі виникнення певних подій, пов'язаних із цими об'єктами (необов'язково).
8. Налагодити параметри активації протоколу VRRP після відновлення функціонування зовнішніх щодо VRRP елементів мережі (необов'язково).
9. Відключити функціонування не потрібних на момент налагодження груп резервування протоколу (необов'язково).
10. Налагодити параметри аутентифікації протоколу (необов'язково).

Порядок налагодження функціонування протоколу VRRP версії 3 має певні відмітності. Тому для отримання детальнішої інформації рекомендується користуватися технічною документацією.

Команди налагодження функціонування протоколу динамічного резервування шлюзу VRRP на маршрутизаторах Cisco

Налагодження функціонування протоколу динамічного резервування шлюзу VRRP може здійснюватися як на маршрутизаторах, так і на комутаторах 3-го рівня, виготовлених фірмою Cisco. Деякі відмітності у процесі налагодження можуть виникати через особливості синтаксису команд та версій Cisco IOS. Слід пам'ятати, що налагодження виконується не на маршрутизаторі у цілому, а лише на певному його інтерфейсі. За замовчуванням функціонування протоколу VRRP на інтерфейсі вимкнено. Основною командою, від якої походить решта команд для налагодження засобів протоколу VRRP у Cisco IOS, є команда **vrrp**. До переліку похідних команд входять такі команди як: **vrrp authentication**, **vrrp description**, **vrrp ip**, **vrrp preempt**, **vrrp priority**, **vrrp shutdown**, **vrrp timers, vrrp track**. Призначення та синтаксис вищезгаданих команд наведено нижче.

Для активації функціонування протоколу VRRP використовується команда **vrrp ip**. Для зазначення текстового опису групи резервування протоколу VRRP застосовується команда **vrrp description**. Зміна пріоритету VRRP-маршрутизатора здійснюється за допомогою команди **vrrp priority**. Часові параметри розсилки та опрацювання повідомлень протоколу VRRP можна змінити за допомогою команди **vrrp timers**. За допомогою команди **vrrp shutdown** на інтерфейсі здійснюється відключення функціонування певної групи резервування VRRP.

Команда **vrrp track** дає змогу відстежувати стан зовнішніх щодо VRRP логічних об'єктів, пов'язаних з функціонуванням певних елементів мережі (інтерфейсів, каналів, протоколів), і впливати на роботу протоколу в разі виходу їх з ладу. Із застосуванням цієї команди тісно пов'язане застосування команди **vrrp preempt**, яка дає змогу маршрутизатору з більш високим пріоритетом перехопити роль активного маршрутизатора, як правило, після відновлення функціонування після виходу з ладу.

Команда **vrrp track** також передбачає використання спеціалізованих команд, похідних від команди **track**, що забезпечують функціонування механізму EOT на маршрутизаторах Cisco як для протоколу VRRP, так і для іншого фірмового протоколу Cisco – GLBP. Серед команд **track** варто згадати команди **track interface**,

track ip route, **track list**, **track rtr**. Після виконання цих команд здійснюється перехід до спеціального режиму config-track, у якому доступний набір інших спеціалізованих команд, зокрема команда налаштування затримок **delay**. Команда **track interface** застосовується для створення логічного об'єкта, що буде відстежувати або стан протоколу фізичної лінії (каналу) для певного інтерфейсу, або наявність маршруту у таблиці маршрутизації і можливість інтерфейсу маршрутизувати IP-пакети. За допомогою команди **track ip route** можна налагодити логічний об'єкт відстеження доступності певної віддаленої мережі. Команда **track list** дає змогу об'єднувати створені окремі логічні об'єкти в один об'єкт і надалі відстежувати його стан.

У протоколі VRRP наявні засоби підвищення рівня захищеності при обміні службовими повідомленнями – засоби взаємної аутентифікації пристроїв, що входять до групи резервування VRRP. Налагодження аутентифікації здійснюється за допомогою команди **vrrp authentication**.

Синтаксис команди **vrrp authentication** (режим конфігурування інтерфейсу):

vrrp *group_number* authentication md5 { { key-string [0 | 7] *key_string* [timeout *timeout_value*]} | { key-chain *key_chain* } } | text *string*,

де ***group_number*** – номер групи резервування протоколу VRRP; може набувати значень від 0 до 255; за замовчуванням дорівнює 0;

md5 – службова конструкція, за допомогою якої зазначається, що для аутентифікації буде використовуватися функція хешування MD;

key-string – службова конструкція, за допомогою якої зазначається, що буде використовуватися ключ key_*string*, який може бути незашифрований (0) або зашифрований за алгоритмом Віженера (7);

key_string – текстовий ключ довжиною до 64 символів;

timeout – службова конструкція, за допомогою якої зазначається інтервал перед прийняттям нового ключа;

timeout_value – значення інтервалу (с) перед прийняттям нового ключа; може набувати значень від 0 до 32767; за замовчуванням дорівнює 0;

key-chain – службова конструкція, за допомогою якої зазначається, що буде використовуватися попередньо згенерований ключ;

key_chain –попередньо згенерований ключ;

text – службова конструкція, за допомогою якої зазначається, що буде застосовуватися аутентифікація з використанням звичайного відкритого пароля;

string – текстовий рядок пароля.

Синтаксис команди **vrrp description** (режим конфігурування інтерфейсу):

vrrp *group_number* description *text*,

де ***group_number*** – номер групи резервування протоколу VRRP; може набувати значень від 0 до 255; за замовчуванням дорівнює 0;

text – текстовий рядок опису (довжиною до 80 символів) групи резервування протоколу VRRP.

Синтаксис команди **vrrp ip** (режим конфігурування інтерфейсу):

vrrp *group_number* ip *IP_address* [secondary],

де ***group_number*** – номер групи резервування протоколу VRRP; може набувати значень від 1 до 255;

IP_address – IP-адреса для групи резервування протоколу VRRP (IP-адреса шлюзу за замовчуванням для кінцевих вузлів) у десятковому записі;

secondary – службова конструкція, за допомогою якої зазначається, що вказана IP-адреса є вторинною VRRP -адресою.

Синтаксис команди **vrrp preempt** (режим конфігурування інтерфейсу):

vrrp *group_number* preempt [delay minimum *delay_value*],

де ***group_number*** – номер групи резервування протоколу VRRP; може набувати значень від 1 до 255;

delay minimum – службова конструкція, за допомогою якої зазначається інтервал затримки перед тим, як маршрутизатор виконає спробу стати активним маршрутизатором після відновлення роботи каналу/інтерфейсу;

delay_value – значення інтервалу затримки (с), може набувати значень від 0 до 3600; за замовчуванням дорівнює 0 с.

Синтаксис команди **vrrp priority** (режим конфігурування інтерфейсу):

vrrp ***group_number*** **priority** ***priority_level***,

де ***group_number*** – номер групи резервування протоколу VRRP; може набувати значень від 1 до 255;

priority_level – значення пріоритету маршрутизатора VRRP; може набувати значень від 1 до 254; значення 0 та 255 зарезервовано для спеціальних цілей; за замовчуванням значення пріоритету дорівнює 100; більше значення свідчить про вищий рівень пріоритету пристрою.

Синтаксис команди **vrrp shutdown** (режим конфігурування інтерфейсу):

vrrp ***group_number*** **shutdown**,

де ***group_number*** – номер групи резервування протоколу VRRP; може набувати значень від 1 до 255;

Синтаксис команди **vrrp timers** (режим конфігурування інтерфейсу):

vrrp ***group_number*** **timers { advertise [msec]** ***advertisement_value*** **} | learn**,

де ***group_number*** – номер групи резервування протоколу VRRP; може набувати значень від 1 до 255;

advertise – службова конструкція, за допомогою якої змінюється значення інтервалу розсилки оповіщень протоколу VRRP;

msec – службова конструкція, за допомогою якої вказується на те, що значення інтервалу розсилки буде зазначено в мілісекундах;

advertisement_value – значення інтервалу розсилки оповіщення протоколу VRRP (с); може змінюватися у межах від 1 до 255; за замовчуванням дорівнює 1 с;

learn – службова конструкція, за допомогою якої вказується, що значення інтервалу розсилки необхідно встановити таким же, як на активному (Master Router) маршрутизаторі групи.

Синтаксис команди **vrrp track** (режим конфігурування інтерфейсу):

vrrp ***group_number*** **track** ***object_number*** **[decrement** ***priority_value*** **]**,

де ***group_number*** – номер групи резервування протоколу VRRP; може набувати значень від 1 до 255;

object_number – номер об'єкта для відстеження; число, яке може набувати значень від 1 до 500;

decrement – службова конструкція, за допомогою якої зазначається зменшення пріоритету інтерфейсу при виникненні певної події;

priority_value – значення, на яке пріоритет інтерфейсу зменшується у випадку, коли інтерфейс деактивується; за замовчуванням дорівнює 10.

Синтаксис команди **track interface** (режим конфігурування інтерфейсу):

track *object_number* interface *interface_type interface_id* { line-protocol | ip routing},

де ***object_number*** – номер об'єкта для відстеження; число, яке може набувати значень від 1 до 500;

interface_type – тип інтерфейсу, може набувати значень **Ethernet**, **FastEthernet**, **GigabitEthernet, Serial** тощо;

interface_id* –** ідентифікатор інтерфейсу (порту), може мати одночислове позначення ***number (номер порту), двочислове позначення ***module/number*** (номер модуля/номер порту), тричислове позначення ***slot/module/number*** (номер слоту/номер модуля (адаптера)/номер інтерфейсу);

line-protocol – службова конструкція, за допомогою якої зазначається ознака того, що буде контролюватися функціонування протоколу фізичної лінії (каналу);

ip routing – службова конструкція, за допомогою якої зазначається те, що буде контролюватися наявність маршруту у таблиці маршрутизації і можливість інтерфейсу маршрутизувати IP-пакети;

Синтаксис команди **track ip route** (режим конфігурування інтерфейсу):

track *object_number* ip route *network_IP-address network_mask* { metric threshold | reachability },

де ***object_number*** – номер об'єкта для відстеження; число, яке може набувати значень від 1 до 500;

***network_IP-address* –** IP-адреса мережі (у десятковому записі),

network_mask – маска мережі, записана у звичайній формі;

metric threshold – службова конструкція, яка призначена для перевірки перевищення метрики маршруту до відповідної IP-мережі;

reachability – службова конструкція, яка призначена для активації перевірки досяжності відповідної IP-мережі.

Синтаксис команди **track list** (режим конфігурування інтерфейсу):

track *object_number* list boolean { and | or } | threshold { percentage | weight },

де ***object_number*** – номер об'єкта для відстеження; число, яке може набувати значень від 1 до 500;

boolean – службова конструкція, за допомогою якої обирається логічна операція (**and** чи **or)**, яка буде виконуватися над об'єктами відстеження;

and – службова конструкція, за допомогою якої зазначається, що буде використовуватися операція логічного "ТА";

or – службова конструкція, за допомогою якої зазначається, що буде використовуватися операція логічного "АБО";

threshold – службова конструкція, за допомогою якої вказується варіант перевищення одного з параметрів **percentage** чи **weight**;

percentage – службова конструкція, за допомогою якої зазначається, що буде використовуватися параметр **percentage**;

percentage – службова конструкція, за допомогою якої зазначається, що буде використовуватися параметр **weight**.

Синтаксис команди **delay** (режим конфігурування параметрів відстеження об'єкта config-track):

delay up | down *delay_value*,

де **up** – службова конструкція, за допомогою якої вказується затримка інформування після активації об'єкта відстеження;

down – службова конструкція, за допомогою якої вказується затримка інформування після деактивації об'єкта відстеження;

***delay_value* –** значення інтервалу затримки (с); може змінюватися у межах від 1 до 180 с.

Команди моніторингу та діагностики роботи протоколу динамічного резервування шлюзу VRRP на маршрутизаторах Cisco

Для моніторингу та діагностики функціонування протоколу VRRP на маршрутизаторах Cisco використовуються як команди загального призначення, так і спеціалізовані команди. Перелік спеціалізо-

ваних команд є відносно невеликим і містить такі команди, як: **show vrrp**, **show vrrp all**, **show vrrp brief**, **show vrrp interface**. Додатково використовуються команди **show track**, **show track brief**, **show track interface**, **show track ip**, **show track resolution**, **show track timers**.

Важливими командами, які допомагають зрозуміти процеси передачі повідомлень протоколу VRRP, є команди трасування такі, як: **debug vrrp**, **debug vrrp all**, **debug vrrp auth**, **debug vrrp errors**, **debug vrrp events**, **debug vrrp packets**, **debug vrrp state**, **debug vrrp track**, **debug track**.

Узагальнений перелік команд моніторингу та діагностики роботи протоколу VRRP на маршрутизаторі Cisco наведений у табл. 2.

Таблиця 2

Перелік команд моніторингу та діагностики роботи протоколу VRRP на маршрутизаторі Cisco

Команда	Призначення
Команди **show vrrp**	
show vrrp	Виведення інформації про роботу протоколу VRRP
show vrrp all	Виведення повної інформації про функціонування протоколу VRRP (зокрема, неактивні групи резервування)
show vrrp brief	Виведення інформації про функціонування протоколу VRRP у скороченому вигляді
show vrrp interface ***interface_type interface_id***	Виведення інформації про функціонування протоколу VRRP на певному інтерфейсі
Команди **show track**	
show track	Виведення інформації про об’єкти відстеження подій
show track brief	Виведення інформації про об’єкти відстеження подій у скороченому вигляді
show track interface	Виведення інформації про інтерфейси, на яких відбувається відстеження подій
show track ip	Виведення інформації про параметри протоколу IP, які відстежуються
show track resolution	Виведення інформації про відображення об’єктів відстеження
show track timers	Виведення інформації про таймери відстеження
Команди **debug vrrp**	
debug vrrp	Активувати виведення узагальненої інформації про функціонування протоколу VRRP
debug vrrp all	Активувати виведення всієї інформації про функціонування протоколу VRRP
debug vrrp auth	Активувати виведення інформації про аутентифікацію протоколу VRRP
debug vrrp errors	Активувати виведення інформації про помилки протоколу VRRP

debug vrrp events	Активувати виведення інформації про події протоколу VRRP
debug vrrp packets	Активувати виведення інформації про передачу повідомлень протоколу VRRP
debug vrrp state	Активувати виведення інформації про стан пристрою VRRP
debug vrrp track	Активувати виведення інформації про відстеження протоколу VRRP
debug track	Активувати виведення інформації про відстеження подій

Модельний приклад налагодження функціонування протоколу динамічного резервування шлюзу VRRP у мережі на базі обладнання Cisco

Розглянемо специфіку налагодження роботи протоколу резервування шлюзу VRRP для мережі, схема якої наведена на рис. 2. Для забезпечення функціонування мережі використано протокол маршрутизації EIGRP.

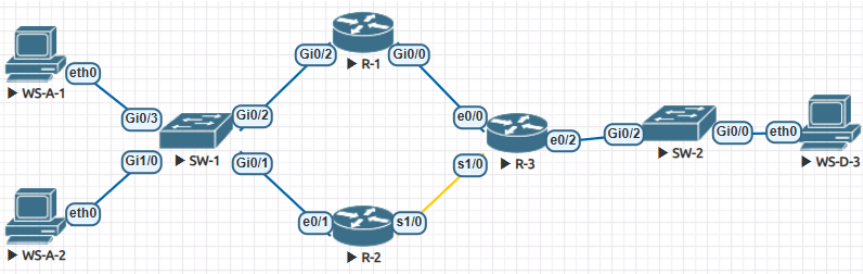


Рис. 2. Приклад мережі

Під час побудови даної мережі для з'єднання пристроїв використано дані табл. 3. Для налагодження параметрів адресації пристроїв використано дані табл. 4.

Таблиця 3

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R_1	Gig0/2	Комутатор SW_1	Gig0/2
	Gig0/0	Маршрутизатор R_3	Eth0/0
Маршрутизатор R_2	Eth0/1	Комутатор SW_1	Gig0/1
	Se1/0 (DCE)	Маршрутизатор R_3	Se1/0 (DTE)
Маршрутизатор R_3	Eth0/0	Маршрутизатор R_1	Fa0/1
	Eth0/2	Комутатор SW_2	Gig0/2
	Se1/0 (DTE)	Маршрутизатор R_2	Se1/0 (DCE)
Комутатор SW_1	Gig0/2	Маршрутизатор R_1	Gig0/2
	Gig0/1	Маршрутизатор R_2	Eth0/1
	Fa0/3	Робоча станція WS_A_1	Fa0/0
	Fa0/4	Робоча станція WS_A_2	Fa0/0
Комутатор SW_2	Gig0/2	Маршрутизатор R_3	Eth0/2
	Gig0/0	Робоча станція WS_D_1	Eth0
Робоча станція WS_A_1	Eth0	Комутатор SW_1	Gig0/3
Робоча станція WS_A_2	Eth0		Gig1/0
Робоча станція WS_D_1	Eth0	Комутатор SW_2	Gig0/0

Таблиця 4

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	–	195.10.1.0	255.255.255.0	/24
Підмережа B	–	195.20.1.0	255.255.255.252	/30
Підмережа C	–	195.30.1.0	255.255.255.252	/30
Підмережа D	–	195.40.1.0	255.255.255.128	/25
Маршрутизатор R_1	Інтерфейс Gig0/2	195.10.1.252	255.255.255.0	/24
	Інтерфейс Gig0/0	195.20.1.1	255.255.255.252	/30
Маршрутизатор R_2	Інтерфейс Eth0/1	195.10.1.253	255.255.255.0	/24
	Інтерфейс Se1/0	195.30.1.1	255.255.255.252	/30
Маршрутизатор R_3	Інтерфейс Gig0/2	195.20.1.2	255.255.255.252	/30
	Інтерфейс Eth0/2	195.40.1.126	255.255.255.128	/25
	Інтерфейс Se1/0	195.30.1.2	255.255.255.252	/30
Віртуальний маршрутизатор	Група резервування VRRP	195.10.1.254	255.255.255.0	/24
Комутатор SW_1	Інтерфейс Vlan 1	195.10.1.250	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
Комутатор SW_2	Інтерфейс Vlan 1	195.40.1.120	255.255.255.128	/25
	Шлюз за замовчуванням	195.40.1.126	–	–
Робоча станція WS_A_1 (Linux)	Мережний адаптер	195.10.1.1	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
Робоча станція WS_A_2(Windows)	Мережний адаптер	195.10.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
Робоча станція WS_D_1 (Linux)	Мережний адаптер	195.40.1.1	255.255.255.128	/25
	Шлюз за замовчуванням	195.40.1.126	–	–

Параметри налагодження протоколу VRRP для пристроїв підмережі A наведені у табл. 5.

Таблиця 5

Параметри налагодження протоколу VRRP для пристроїв підмережі A

Параметр	Значення параметра
Версія протоколу	2 (встановлена автоматично)
Номер групи резервування	1
Опис групи резервування	LAN-A
Віртуальна IP-адреса	195.10.1.254
Віртуальна MAC-адреса	00-00-5E-00-01-01
Маршрутизатор Master	R_1
Пріоритет маршрутизатора Master	50
Маршрутизатор Backup	R_2
Пріоритет маршрутизатора Backup	45
Інтервал розсилки оновлень протоколу, с	5
Затримка перед спробою стати активним маршрутизатором після перезавантаження, с	3

Сценарії налагодження параметрів адресації інтерфейсів та протоколу маршрутизації EIGRP для маршрутизаторів мережі наведені нижче.

```
…
R_1>enable
R_1#configure terminal
R_1(config)#interface GigabitEthernet 0/2
R_1(config-if)#description LINK_TO_LAN_A
R_1(config-if)#ip address 195.10.1.252 255.255.255.0
R_1(config-if)#no shutdown
R_1(config-if)#exit
R_1(config)#interface GigabitEthernet 0/0
R_1(config-if)#description LINK_TO_R_3
R_1(config-if)#ip address 195.20.1.1 255.255.255.252
R_1(config-if)#no shutdown
R_1(config-if)#exit
R_1(config)#router eigrp 1
R_1(config-router)#network 195.10.1.0 0.0.0.255
R_1(config-router)#network 195.20.1.0 0.0.0.3
R_1(config-router)#exit
R_1(config)#exit
R_1#
…
R_2>enable
R_2#configure terminal
R_2(config)#interface Ethernet 0/1
R_2(config-if)#description LINK_TO_LAN_A
R_2(config-if)#ip address 195.10.1.253 255.255.255.0
R_2(config-if)#no shutdown
R_2(config-if)#exit
R_2(config)#interface Serial 1/0
R_2(config-if)#description LINK_TO_R_3
R_2(config-if)#ip address 195.30.1.1 255.255.255.252
R_2(config-if)#clock rate 64000
R_2(config-if)#no shutdown
R_2(config-if)#exit
R_2(config)#router eigrp 1
```

R_2(config-router)#network 195.10.1.0 0.0.0.255
R_2(config-router)#network 195.30.1.0 0.0.0.3
R_2(config-router)#exit
R_2(config)# exit
R_2#

…

R_3>enable
R_3#configure terminal
R_3(config)#interface Ethernet 0/0
R_3(config-if)#description LINK_TO_R_1
R_3(config-if)#ip address 195.20.1.2 255.255.255.252
R_3(config-if)#no shutdown
R_3(config-if)#exit
R_3(config)#interface Ethernet 0/2
R_3(config-if)#description LINK_TO_LAN_D
R_3(config-if)#ip address 195.40.1.254 255.255.255.128
R_3(config-if)#no shutdown
R_3(config-if)#exit
R_3(config)#interface Serial 1/0
R_3(config-if)#description LINK_TO_R_2
R_3(config-if)#ip address 195.30.1.2 255.255.255.252
R_3(config-if)#no shutdown
R_3(config-if)#exit
R_3(config)#router eigrp 1
R_3(config-router)#network 195.20.1.0 0.0.0.3
R_3(config-router)#network 195.30.1.0 0.0.0.3
R_3(config-router)#network 195.40.1.0 0.0.0.127
R_3(config-router)#exit
R_3(config)# exit
R_3#
…

Сценарій налагодження параметрів адресації комутатора SW_1 та відключення функції **ip igmp snooping** наведений нижче.

```
…
SW_1>enable
SW_1#configure terminal
SW_1(config)#interface vlan 1
SW_1(config-if)#ip address 195.10.1.250 255.255.255.0
SW_1(config-if)#no shutdown
SW_1(config-if)#exit
SW_1(config)#no ip igmp snooping
SW_1(config)#exit
SW_1#
…
```

Сценарії налагодження функціонування протоколу резервування шлюзу VRRP на маршрутизаторах R_1 та R_2 наведені нижче.

```
…
R_1>enable
R_1#configure terminal
R_1(config)#interface GigabitEthernet 0/2
R_1(config-if)#vrrp 1 ip 195.10.1.254
R_1(config-if)#vrrp 1 priority 50
R_1(config-if)#vrrp 1 description LAN-A
R_1(config-if)#vrrp 1 timers advertise 5
R_1(config-if)#vrrp 1 timers learn
R_1(config-if)#vrrp 1 track 100 decrement 10
R_1(config-if)#vrrp 1 preempt delay minimum 3
R_1(config-if)#exit
R_1(config)#track 11 interface GigabitEthernet 0/0 line-protocol
R_1(config-track)#delay up 1
R_1(config-track)#delay down 1
R_1(config-track)#exit
R_1(config)#track 12 interface GigabitEthernet 0/0 ip routing
R_1(config-track)#delay up 1
R_1(config-track)#delay down 1
R_1(config-track)#exit
```

R_1(config)#track 100 list boolean or
R_1(config-track)#object 11
R_1(config-track)#object 12
R_1(config-track)#exit
R_1(config)#exit
R_1#
…

R_2>enable
R_2#configure terminal
R_2(config)#interface Ethernet 0/1
R_2(config-if)#vrrp 1 ip 195.10.1.254
R_2(config-if)#vrrp 1 priority 45
R_2(config-if)#vrrp 1 description LAN-A
R_2(config-if)#vrrp 1 timers advertise 5
R_2(config-if)#vrrp 1 timers learn
R_2(config-if)#vrrp 1 track 200 decrement 10
R_2(config-if)#vrrp 1 preempt delay minimum 3
R_2(config-if)#exit
R_2(config)#track 21 interface Serial 1/0 line-protocol
R_2(config-track)#delay up 1
R_2(config-track)#delay down 1
R_2(config-track)#exit
R_2(config)#track 22 interface Serial 1/0 ip routing
R_2(config-track)#delay up 1
R_2(config-track)#delay down 1
R_2(config-track)#exit
R_2(config)#track 200 list boolean or
R_2(config-track)#object 21
R_2(config-track)#object 22
R_2(config-track)#exit
R_2(config)#exit
R_2#
…

Результати виконання команд моніторингу та діагностики роботи протоколу VRRP для розглянутого прикладу

З метою перегляду інформації про роботу протоколу VRRP для розглянутого прикладу використано команди **show vrrp** (команди **show vrrp interface FastEthernet 0/0** та **show vrrp all** для даного прикладу покажуть аналогічні результати**)**, **show vrrp brief**, **show track**, **show track brief**. Результати роботи цих команд для маршрутизаторів R_1 та R_2 наведено відповідно на рис. 3 – 10.

```
R_1#show vrrp
FastEthernet0/0 - Group 1
LAN-A
  State is Master
  Virtual IP address is 195.10.1.254
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 5.000 sec
  Preemption enabled, delay min 3 secs
  Priority is 50
    Track object 100 state Up decrement 10
  Master Router is 195.10.1.252 (local), priority is 50
  Master Advertisement interval is 5.000 sec
  Master Down interval is 15.804 sec
R_1#
```

Рис. 3. Результати виконання команди **show vrrp** на маршрутизаторі R_1

```
R_2#show vrrp
FastEthernet0/0 - Group 1
LAN-A
  State is Backup
  Virtual IP address is 195.10.1.254
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 5.000 sec
  Preemption enabled, delay min 3 secs
  Priority is 45
    Track object 200 state Up decrement 10
  Master Router is 195.10.1.252, priority is 50
  Master Advertisement interval is 5.000 sec
  Master Down interval is 15.824 sec (expires in 15.708 sec) Learning
```

Рис. 4. Результати виконання команди **show vrrp** на маршрутизаторі R_2

```
R_1#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Gig0/2             1   50  15804      Y  Master  195.10.1.252    195.10.1.254
R_1#
```

Рис. 5. Результати виконання команди **show vrrp brief** на маршрутизаторі R_1

```
R_2#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Eth0/0             1   45  15824      Y  Backup  195.10.1.252    195.10.1.254
R_2#
```

Рис. 6. Результати виконання команди **show vrrp brief** на маршрутизаторі R_2

```
R_1#show track
Track 11
  Interface GigabitEthernet 0/0 line-protocol
  Line protocol is Up
    1 change, last change 00:01:25
  Delay up 1 sec, down 1 sec
Track 12
  Interface GigabitEthernet 0/0 ip routing
  IP routing is Up
    1 change, last change 00:00:50
  Delay up 1 sec, down 1 sec
Track 100
  List boolean or
  Boolean OR is Up
    4 changes, last change 00:01:24
    object 11 Up
    object 12 Up
  Tracked by:
    VRRP GigabitEthernet 0/2 1
R_1#
```

Рис. 7. Результати виконання команди **show track** на маршрутизаторі R_1

```
R_2#show track
Track 21
  Interface Serial1/0 line-protocol
  Line protocol is Up
    1 change, last change 00:03:24
  Delay up 1 sec, down 1 sec
Track 22
  Interface Serial1/0 ip routing
  IP routing is Up
    1 change, last change 00:03:02
  Delay up 1 sec, down 1 sec
Track 200
  List boolean or
  Boolean OR is Up
    2 changes, last change 00:03:23
    object 21 Up
    object 22 Up
  Tracked by:
    VRRP Ethernet 0/1 1
R_2#
```

Рис. 8. Результати виконання команди **show track** на маршрутизаторі R_2

```
R_1#show track brief
Track   Object                              Parameter        Value
11      interface GigabitEthernet 0/0       line-protocol    Up
12      interface GigabitEthernet 0/0       ip routing       Up
100     list                                boolean          Up
R_1#
```

Рис. 9. Результати виконання команди **show track brief** на маршрутизаторі R_1

```
R_2#show track brief
Track   Object                          Parameter         Value
21      interface Serial1/0             line-protocol     Up
22      interface Serial1/0             ip routing        Up
200     list                            boolean           Up
R_2#
```

Рис. 10. Результати виконання команди **show track brief** на маршрутизаторі R_2

З метою перевірки досяжності шлюзу за замовчуванням мережі A з робочих станцій WS_A_1 та WS_A_2 використано команду **ping**. З метою перевірки досяжності мережі D (зокрема, робочої станції WS_D_1) використано команду **tracert** (**traceroute).** Побічним результатом використання цих команд є додавання записів в ARP-таблиці відповідних вузлів. Результати виконання команд діагностики **ping**, **traceroute** (**tracert**), **arp** на робочих станціях WS_A_1 та WS_A_2 наведені відповідно на рис. 11 – 16.

```
root@WS_A_1~#ping 195.10.1.254
PING 195.10.1.254 (195.10.1.254): 56 data bytes
64 bytes from 195.10.1.254: seq=0 ttl=255 time=10.769 ms
64 bytes from 195.10.1.254: seq=1 ttl=255 time=6.331 ms
64 bytes from 195.10.1.254: seq=2 ttl=255 time=14.258 ms
64 bytes from 195.10.1.254: seq=3 ttl=255 time=9.333 ms
^C
--- 195.10.1.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 6.331/10.172/14.258 ms
root@WS_A_1~#
```

Рис. 11. Результат виконання команди **ping** на робочій станції WS_A_1

```
root@WS_A_1~#traceroute 195.40.1.1
traceroute to 195.40.1.1 (195.40.1.1), 30 hops max, 38 byte packets
 1  195.10.1.252 (195.10.1.252)  10.459 ms  10.886 ms  7.863 ms
 2  195.20.1.2 (195.20.1.2)  30.877 ms  31.386 ms  30.417 ms
 3  195.40.1.1 (195.40.1.1)  50.499 ms  42.296 ms  43.536 ms
root@WS_A_1~#
```

Рис. 12. Результат виконання команди **traceroute** на робочій станції WS_A_1

```
root@WS_A_1~#arp -a
? (195.10.1.254) at 00:00:5e:00:01:01 [ether]  on eth0
root@WS_A_1~#
```

Рис. 13. Результат виконання команди **arp** на робочій станції WS_A_1

```
C:\>ping 195.10.1.254
Обмен пакетами с 195.10.1.254 по 32 байт:
Ответ от 195.10.1.254: число байт=32 время 23мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 4мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 6мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 11мс TTL=125
Статистика Ping для 195.10.1.254:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 <0% потерь>,
Приблизительное время приема-передачи в мс:
    Минимальное = 4 мсек, Максимальное 23 мсек, Среднее = 11 мсек
C:\>
```

Рис. 14. Результат виконання команди **ping** на робочій станції WS_A_2

```
C:\>tracert 195.40.1.1
Трассировка маршрута к 195.4.1.2 с максимальным числом прыжков 30
  1   11 ms    10 ms    10 ms  195.10.1.252
  2   18 ms    31 ms    20 ms  195.20.1.2
  3   59 ms    43 ms    41 ms  195.40.1.1
Трассировка завершена.
C:\>
```

Рис. 15. Результат виконання команди **tracert** на робочій станції WS_A_2

```
c:\>arp -a
Интерфес: 195.10.1.2 -- 0x2
  Адрес IP            Физический адрес      Тип
  195.10.1.254        00:00:5e:00:01:01     динамический
c:\>
```

Рис. 16. Результат виконання команди **arp** на робочій станції WS_A_2

Необхідно зазначити, що команда **traceroute** (**tracert**) першою точкою маршруту виводить не IP-адресу шлюзу за замовчуванням мережі (віртуальну IP-адресу групи резервування VRRP), а IP-адресу інтерфейса маршрутизатора, через який відбуватиметься фактична передача трафіка. У нашому випадку – це маршрутизатор R_1.

З метою перевірки роботи протоколу VRRP змоделюємо ситуацію виходу з ладу каналу зв'язку між маршрутизаторами R_1 та R_2 за рахунок відключення інтерфейсу **FastEthernet 0/1** маршрутизатора R_1. Для відстеження інформаційного обміну між маршрутизаторами активуємо режим відлагодження на маршрутизаторі R_2. Зміни у роботі протоколу на маршрутизаторах R_1 та R_2 відстежимо за допомогою команд **show vrrp** та **show track brief**. Результати виконання цих команд наведені на рис. 17 – 20. Результати інформаційного обміну між маршрутизаторами наведені на рис. 21.

```
R_1#show vrrp
GigabitEthernet 0/2 - Group 1
LAN-A
  State is Backup
  Virtual IP address is 195.10.1.254
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 5.000 sec
  Preemption enabled, delay min 3 secs
  Priority is 40  (cfgd 50)
    Track object 100 state Down decrement 10
  Master Router is 195.10.1.253, priority is 45
  Master Advertisement interval is 5.000 sec
  Master Down interval is 15.804 sec (expires in 12.740 sec) Learning
R_1#
```

Рис. 17. Результати виконання команди **show vrrp** на маршрутизаторі R_1

```
R_1#show track brief
Track   Object                          Parameter        Value
11      interface GigabitEthernet 0/0 line-protocol    Down (hw admin-down)
12      interface GigabitEthernet 0/0 ip routing       Down (hw admin-down)
100     list                          boolean          Down
R_1#
```

Рис. 18. Результати виконання команди **show track brief** на маршрутизаторі R_1

```
R_2#show vrrp
FastEthernet0/0 - Group 1
LAN-A
  State is Master
  Virtual IP address is 195.10.1.254
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 5.000 sec
  Preemption enabled, delay min 3 secs
  Priority is 45
    Track object 200 state Up decrement 10
  Master Router is 195.10.1.253 (local), priority is 45
  Master Advertisement interval is 5.000 sec
  Master Down interval is 15.824 sec
R_2#
```

Рис. 19. Результати виконання команди **show vrrp** на маршрутизаторі R_2

```
R_2#show track brief
Track   Object                          Parameter        Value
21      interface Serial1/0             line-protocol    Up
22      interface Serial1/0             ip routing       Up
200     list                            boolean          Up
R_2#
```

Рис. 20. Результати виконання команди **show track brief** на маршрутизаторі R_2

```
R_2#debug vrrp all
VRRP debugging is on
R_2#
*Mar  1 00:01:18.595: VRRP: Grp 1 Advertisement priority 50, ipaddr 195.10.1.252
*Mar  1 00:01:18.595: VRRP: Grp 1 Event - Advert higher or equal priority
R_2#
*Mar  1 00:01:22.011: VRRP: Grp 1 Advertisement priority 50, ipaddr 195.10.1.252
*Mar  1 00:01:22.015: VRRP: Grp 1 Event - Advert higher or equal priority
R_2#
*Mar  1 00:01:26.083: VRRP: Grp 1 Advertisement priority 40, ipaddr 195.10.1.252
R_2#
*Mar  1 00:01:29.083: VRRP: Grp 1 Event - Master down timer expired
*Mar  1 00:01:29.083: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Backup -> Master
R_2#
*Mar  1 00:01:29.083: VRRP: tbridge_smf_update failed
*Mar  1 00:01:29.087: VRRP: Grp 1 sending Advertisement checksum ECEF
R_2#
*Mar  1 00:01:33.847: VRRP: Grp 1 sending Advertisement checksum ECEF
R_2#
*Mar  1 00:01:38.399: VRRP: Grp 1 sending Advertisement checksum ECEF
R_2#
*Mar  1 00:01:42.447: VRRP: Grp 1 sending Advertisement checksum ECEF
R_2#
*Mar  1 00:01:46.615: VRRP: Grp 1 sending Advertisement checksum ECEF
R_2#
```

Рис. 21. Результати інформаційного обміну протоколу VRRP на маршрутизаторі R_2

Також виконаємо перевірку досяжності шлюзу за замовчуванням мережі A та перевірку досяжності мережі D. Для цього також використаємо команди діагностики **ping, tracert** (**traceroute**), **arp**. Результати виконання цих команд на робочих станціях WS_A_1 та WS_A_2 наведені відповідно на рис. 22 – 27.

```
root@WS_A_1~#ping 195.10.1.254
PING 195.10.1.254 (195.10.1.254): 56 data bytes
64 bytes from 195.10.1.254: seq=0 ttl=255 time=12.064 ms
64 bytes from 195.10.1.254: seq=1 ttl=255 time=5.239 ms
64 bytes from 195.10.1.254: seq=2 ttl=255 time=13.561 ms
64 bytes from 195.10.1.254: seq=3 ttl=255 time=10.502 ms
^C
--- 195.10.1.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 5.239/10.341/13.561 ms
root@WS_A_1~#
```

Рис. 22. Результат виконання команди **ping** на робочій станції WS_A_1

```
root@WS_A_1~#traceroute 195.40.1.1
traceroute to 195.40.1.1 (195.40.1.1), 30 hops max, 38 byte packets
 1  195.10.1.253 (195.10.1.253)  7.648 ms  8.826 ms  10.220 ms
 2  195.30.1.2 (195.30.1.2)  9.594 ms  10.748 ms  9.548 ms
 3  195.40.1.1 (195.40.1.1)  30.128 ms  19.790 ms  20.697 ms
root@WS_A_1~#
```

Рис. 23. Результат виконання команди **traceroute** на робочій станції WS_A_1

```
root@WS_A_1~#arp -a
? (195.10.1.254) at 00:00:5e:00:01:01 [ether]  on eth0
root@WS_A_1~#
```

Рис. 24. Результат виконання команди **arp** на робочій станції WS_A_1

```
C:\>ping 195.10.1.254
Обмен пакетами с 195.10.1.254 по 32 байт:
Ответ от 195.10.1.254: число байт=32 время 21мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 4мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 2мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 6мс TTL=125
Статистика Ping для 195.10.1.254:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 <0% потерь>,
Приблизительное время приема-передачи в мс:
    Минимальное = 2 мсек, Максимальное 21 мсек, Среднее = 8 мсек
C:\>
```

Рис. 25. Результат виконання команди **ping** на робочій станції WS_A_2

```
C:\>tracert 195.40.1.1
Трассировка маршрута к 195.4.1.2 с максимальным числом прыжков 30
  1    8 ms    10 ms    32 ms  195.10.1.253
  2    9 ms    10 ms    10 ms  195.30.1.2
  3   27 ms    22 ms    19 ms  195.40.1.1
Трассировка завершена.
C:\>
```

Рис. 26. Результат виконання команди **tracert** на робочій станції WS_A_2

```
c:\>arp -a
Интерфес: 195.10.1.2 -- 0x2
  Адрес IP            Физический адрес      Тип
  195.10.1.254        00:00:5e:00:01:01     динамический
c:\>
```

Рис. 27. Результат виконання команди **arp** на робочій станції WS_A_2

Результат виконання команди **tracert** (**traceroute)** також підтверджує той факт, що маршрут передачі трафіка змінився –весь мережний трафік із підмережі A до зовнішніх мереж фізично проходитиме через маршрутизатор R_2.

Завдання на лабораторну роботу

1. У середовищі віртуальної мережевої лабораторія eve.ztu.edu.ua створити проєкт мережі (рис. 28). Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 3.

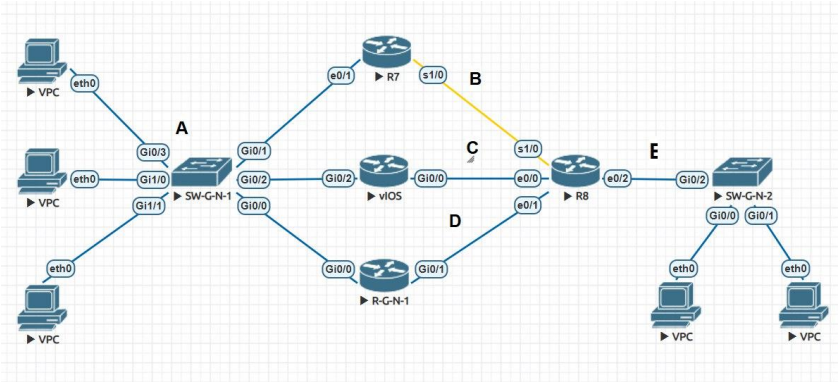


Рис. 28. Проект мережі

2. Розробити схему адресації пристроїв мережі. Для цього скористатися даними табл. 6. Результати навести у вигляді таблиці, яка аналогічна табл. 4. При виконанні розрахунків врахувати такі особливості адресації:

– у мережі А будуть використовуватися дві групи резервування VRRP, кожна з яких матиме власну віртуальну IP-адресу;

– перша половина робочих станцій та серверів мережі буде мати IP-адресу шлюзу за замовчуванням першої групи резервування, а друга половина – другої групи резервування.

3. Визначити основні параметри для налагодження протоколу VRRP для пристроїв підмережі А. Для визначення параметрів скористатися даними табл. 7. При виборі ролей маршрутизаторів VRRP враховувати пропускні здатності зовнішніх каналів зв'язку. Результати навести у вигляді таблиці, яка аналогічна табл. 5.

4. Провести базове налагодження пристроїв, інтерфейсів та каналів зв'язку. Провести налагодження параметрів IP-адресації пристроїв мережі відповідно до даних, які отримані у п. 2. Перевi-

рити наявність зв'язку між сусідніми парами пристроїв мережі. Налагодити функціонування засобів маршрутизації у побудованій мережі (для вибору методу/протоколу маршрутизації скористатися даними табл. 7).

5. Налагодити основні параметри функціонування протоколу VRRP на пристроях мережі A відповідно до даних, які отримані у п. 3.

6. Налагодити додаткові параметри функціонування протоколу VRRP на пристроях мережі:

– відслідковування стану зовнішніх щодо VRRP інтерфейсів маршрутизаторів (обов'язково);

– відслідковування стану зовнішніх щодо VRRP мереж (необов'язково);

7. Дослідити функціонування протоколу VRRP на пристроях мережі та поведінку VRRP-пристроїв у разі:

– виходу з ладу (відключення) одного з маршрутизаторів – членів групи резервування VRRP;

– виходу з ладу (відключення) одного або кількох інтерфейсів, які використовуються для формування каналів B, C, D між маршрутизаторами мережі;

– відновлення функціонування маршрутизатора – члена групи резервування VRRP, який виходив із ладу;

– відновлення функціонування інтерфейсу/інтерфейсів, які виходили з ладу.

8. Дослідити процеси передачі даних між вузлами віддалених підмереж A та E при виконанні дій, які аналогічні діям п. 7.

Таблиця 6

Дані для адресації підмереж (каналів)

№ варіанта	Підмережа A		Підмережа B		Підмережа C		Підмережа D		Підмережа E		Протокол маршрутизації
	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	
Не парні	193.G.N.0	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/30	197.G.N.0	/24	OSPF
Парні	193.G.N.64	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/30	197.G.N.0	/25	EIGRP

Таблиця 7

Параметри для налагодження функціонування протоколу VRRP

№ варіанта	Номер групи резервування		Пріоритети маршрутизаторів						Інтервал протоколу Advertisement Interval, с
			Група резервування 1			Група резервування 2			
	Група 1	Група 2	Master Router	Backup Router 1	Backup Router 2	Master Router	Backup Router 1	Backup Router 2	
Не парні	101	201	200	195	190	150	145	140	3
Парні	102	202	195	190	185	145	140	135	4

Контрольні питання

1. Передумови розробки протоколу VRRP.
2. Загальна характеристика протоколу VRRP.
3. Порівняльна характеристика протоколів VRRP та HSRP.
4. Стандартизація протоколу VRRP.
5. Характеристики протоколу VRRP стосовно моделі OSI та стеку TCP/IP.
6. Версії протоколу VRRP.
7. Ролі пристроїв у протоколі VRRP. Група резервування протоколу VRRP.
8. Стани пристроїв у протоколі VRRP.
9. Адресація у протоколі VRRP.
10. Часові інтервали та таймери протоколу VRRP.
11. Структура повідомлення протоколу VRRP. Типи повідомлень протоколу VRRP.
12. Балансування навантаження у протоколі VRRP.
13. Механізми (елементи) захисту даних протоколу VRRP.
14. Наведіть перелік та поясніть призначення основних команд для налагодження протоколу VRRP на маршрутизаторі Cisco.
15. Наведіть перелік та поясніть призначення основних команд моніторингу роботи протоколу VRRP на маршрутизаторі Cisco.

Лабораторна робота № 6
НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ ДИНАМІЧНОГО РЕЗЕРВУВАННЯ ШЛЮЗУ ТА БАЛАНСУВАННЯ НАВАНТАЖЕННЯ GLBP У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

Мета заняття: ознайомитися з особливостями функціонування та налагодження роботи протоколу динамічного резервування шлюзу та балансування навантаження GLBP на обладнанні Cisco; отримати практичні навички налагодження, моніторингу та діагностування роботи протоколу GLBP у мережі, побудованій на базі обладнання Cisco; дослідити процес роботи протоколу GLBP та процеси передачі даних у побудованій мережі.

Теоретичні відомості

Загальні відомості про протокол динамічного резервування шлюзу та балансування навантаження GLBP

Досвід упровадження та експлуатації у великих мережах фірмового протоколу резервування шлюзу Cisco Systems Inc. HSRP та відкритого протоколу IETF VRRP показав, що, з одного боку, ці протоколи повністю забезпечували виконання своєї головної функції – резервування шлюзу, а з іншого боку, мали значні проблеми при реалізації допоміжної функції – балансування (розподілу) навантаження. Розподіл навантаження як у протоколі HSRP, так і у протоколі VRRP можна організувати лише за статичною схемою, яка передбачає ручне налагодження пристроїв на основі виміряних або передбачуваних об’ємів трафіка. Але відомо, що інформаційні потоки у будь-якій комп’ютерній мережі змінюються динамічно, без певних закономірностей. Це означає, що статичне балансування навантаження не відповідає реальному стану передачі трафіка між вузлами. Тому виникла необхідність у розробці спеціалізованого протоколу, який повинен:

– виконувати балансування навантаження без попередніх ручних змін конфігурацій кінцевих вузлів мережі;

– виконувати балансування навантаження за алгоритмом, який обрано адміністратором, з урахуванням можливостей резервуючого пристрою та його поточного завантаження запитами від кінцевих вузлів мережі;

– забезпечувати розподіл навантаження тільки між тими з резервуючих пристроїв, які мають достатній пріоритет і своєчасно підтверджують свою працездатність.

Перерахованим вище вимогам відповідає розроблений і реалізований у 2005 році фірмовий протокол Cisco Systems Inc. GLBP (Gateway Loading Balancing Protocol). Головна відмітність протоколу GLBP від протоколів HSRP та VRRP полягає в тому, що функції шлюзу можуть виконувати не один, а кілька маршрутизаторів групи резервування одночасно. Це забезпечується за рахунок застосування для доступу до шлюзу групи адрес канального рівня замість однієї адреси, як це передбачено правилами протоколів HSRP та VRRP. У такий спосіб досягається можливість одночасного використання кількох пристроїв групи резервування для обслуговування запитів, які надходять від вузлів локальної мережі. Слід зазначити, що провідні виробники мережного обладнання (зокрема, фірми Brocade та HP) на базі протоколу VRRP розробили та проводять процес тестування відкритого промислового протоколу VRRPE (VRRP Extended), який аналогічний за функціями протоколу GLBP.

Протокол GLBP описується у внутрішніх стандартизуючих документах фірми Cisco Systems Inc. Стосовно моделі OSI цей протокол є протоколом канального рівня. Для передачі своїх повідомлень протокол GLBP використовує можливості протоколу UDP у режимі групової розсилки. Поточна версія протоколу орієнтована на функціонування в IP-мережах версій 4 та 6.

Для забезпечення функціонування протоколу GLBP уведено поняття маршрутизатор/шлюз GLBP (GLBP Router / GLBP Gateway) та група резервування GLBP. Маршрутизатором/шлюзом GLBP є будь-який маршрутизатор, на якому активовано використання протоколу GLBP. Як правило, такий маршрутизатор носить назву віртуального шлюзу GLBP (GLBP VG, GLBP Virtual Gateway). Групі резервування GLBP відповідають одна віртуальна адреса мережного рівня (GLBP vIP, GLBP Virtual IP-Address) та група віртуальних адрес канального рівня (GLBP vMACs, GLBP Virtual MAC-Addresses). Virtual IP-Address – це IP-адреса шлюзу за замовчуванням для кінцевих вузлів мережі. Virtual MAC-Addresses – це віртуальні MAC-адреси пристроїв, що входять до групи резервування GLBP. Теоретично кількість віртуальних MAC-адрес становить 255, нато-

мість реалізовано можливість використання лише до чотирьох віртуальних MAC-адрес.

До групи резервування протоколу GLBP входять такі віртуальні шлюзи: активний віртуальний шлюз-диспетчер GLBP (GLBP AVG, GLBP Active Virtual Gateway), резервний віртуальний шлюз-диспетчер GLBP (GLBP SVG, GLBP Standby Virtual Gateway) та запасні віртуальні шлюзи (шлюзи-диспетчери) GLBP. Всі маршрутизатори – члени групи резервування є віртуальними шлюзами-відправниками GLBP (GLBP VFs, GLBP Virtual Forwarders). Для забезпечення передачі трафіка у протоколі GLBP використовуються лише чотири віртуальних шлюзи-відправники, відомі як активні віртуальні шлюзи-відправники (GLBP Active Virtual Forwarders), причому один з них обирається як первинний активний віртуальний шлюз-відправник (GLBP Primary AVF, GLBP Primary Active Virtual Forwarder). Решта пристроїв стають вторинними віртуальними шлюзами-відправниками (GLBP Secondary VFs, GLBP Secondary Virtual Forwarders) і знаходяться у резерві. Вторинний шлюз-відправник може стати активним шлюзом-відправником після виходу з ладу одного з активних шлюзів-відправників.

Основними завданнями шлюзу-диспетчера є:

– вибір активних компонентів групи резервування та розподіл між ними віртуальних MAC-адрес шлюзу;

– розподіл зовнішніх запитів між активними членами групи резервування (за рахунок видачі ARP-відповідей із різними віртуальними MAC-адресами на запити до віртуальної IP-адреси).

Вибори активного та резервного віртуальних шлюзів-диспетчерів GLBP здійснюються на основі механізму пріоритетів (Priority). Пріоритет може набувати значень у діапазоні від 0 до 255. Маршрутизатор із найбільшим пріоритетом вибирається як активний віртуальний шлюз-диспетчер GLBP. Маршрутизатор із наступним пріоритетом вибирається як резервний віртуальний шлюз-диспетчер GLBP. Решта маршрутизаторів уважаються запасними віртуальними шлюзами-диспетчерами GLBP.

Якщо пріоритети маршрутизаторів, які претендують на роль активного шлюза-диспетчера GLBP, однакові, то виконується порівняння їх IP-адрес, і маршрутизатор із найбільшою адресою стає активним віртуальним шлюзом-диспетчером GLBP. Якщо пріоритети маршрутизаторів, які претендують на роль резервного, однакові, також

виконується порівняння їх IP-адрес, і маршрутизатор із найбільшою адресою стає резервним віртуальним шлюзом-диспетчером GLBP.

Для підтвердження свого статусу активний віртуальний шлюз-диспетчер групи резервування GLBP періодично (через інтервал Hello Time) розсилає решті шлюзів-диспетчерів повідомлення свого існування GLBP Hello. Якщо резервний і запасні віртуальні шлюзи-диспетчери не отримують повідомлення GLBP Hello через певний проміжок часу (інтервал Hold Time), то вони констатують, що активний віртуальний шлюз-диспетчер вийшов із ладу (або вимкнений примусово), відповідно резервний віртуальний шлюз-диспетчер стає активним, і серед запасних віртуальних шлюзів-диспетчерів обирається новий резервний віртуальний шлюз-диспетчер. Для обміну адресною інформацією між активним віртуальним шлюзом-диспетчером і рештою пристроїв групи резервування GLBP використовуються повідомлення GLBP Request та GLBP Reply (GLBP Response). Структура повідомлення протоколу GLBP наведена у додатку В.

Важливими часовими параметрами протоколу GLBP також є інтервали Redirect Time та Secondary Hold Time. Інтервал Redirect Time – це інтервал, протягом якого активний віртуальний шлюз-диспетчер переспрямовує запити клієнтів до активних віртуальних шлюзів-відправників. Використовується з метою продовження пересилки нових ARP-запитів у відповідності до поточної схеми балансування навантаження до моменту, поки непрацездатний віртуальний шлюз-відправник не відновить свою роботу. Якщо така ситуація виникне протягом інтервалу Redirect Time, то відновлений віртуальний шлюз-відправник повернеться до стану свого попереднього завантаження. Як правило, інтервал Redirect Time отримується від активного віртуального шлюзу-диспетчера.

Інтервал Secondary Hold Time – це інтервал, протягом якого вторинний віртуальний шлюз-відправиник залишається коректним при виході з ладу первинного шлюзу-відправника. Вторинний віртуальний шлюз-відправник видаляється, якщо цей інтервал спливає. Якщо вторинний віртуальний шлюз-відправиник видалений, то навантаження перерозподіляється між рештою віртуальних шлюзів-відправників. Цей інтервал повинен бути більшим, ніж час існування записів в ARP-таблицях кінцевих вузлів. Як правило, цей інтервал отримується від активного віртуального шлюзу-диспетчера.

У ході виконання операцій протоколу маршрутизатор групи резервування GLBP може знаходитися в одному з таких станів:

– вимкнений стан (*Disabled State*);

– початковий стан (*Initial State*);

– стан прослуховування мережі (*Listen State*);

– стан передачі повідомлень (*Speak State*);

– стан резервного шлюзу-диспетчера (*Standby State/ Standby Virtual Gateway*);

– стан активного шлюзу-диспетчера (*Active State/ Active Virtual Gateway*).

Діаграма змін станів маршрутизатора GLBP наведена на рис. 1, а.

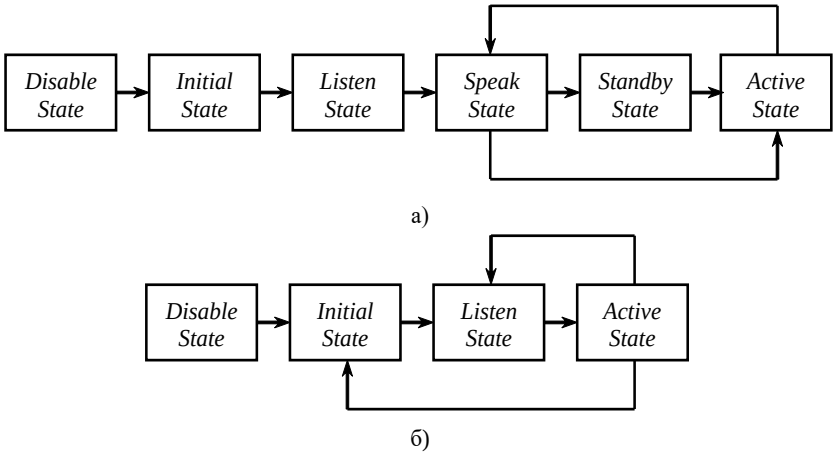


Рис. 1. Діаграма змін станів: а – маршрутизатора GLBP;
б – віртуального шлюзу-відправника GLBP

У стані *Disabled State* маршрутизатор не володіє інформацією про віртуальну IP-адресу (адреса або не налагоджена, або ще не отримана від інших пристроїв), але інші параметри протоколу GLBP наявні. У стані *Initial State* інформація про віртуальну IP-адресу наявна, але процедура налагодження віртуального шлюзу-диспетчера ще не закінчена (повинен бути активованим і налагодженим фізичний інтерфейс для маршрутизації IP-пакетів, інтерфейсу повинна бути призначена IP-адреса). У стані *Listen State* віртуальний шлюз отримує повідомлення GLBP Hello і готовий зміни-

ти свій стан на стан *Speak State*, якщо активний віртуальний шлюз-диспетчер або резервний віртуальний шлюз-диспетчер стануть недоступними. У стані *Speak State* пристрій виконує спробу перейти або до стану *Standby State*, або до стану *Active State*. Стан *Standby State* свідчить про те, що пристрій виконує функції резервного віртуального шлюзу-диспетчера. Відповідно стан *Active State* свідчить про те, що пристрій виконує функції активного віртуального шлюзу-диспетчера, тобто надсилає відповіді на ARP-запити для віртуальної IP-адреси.

Після виборів активного та резервного віртуальних шлюзів-диспетчерів проводиться визначення первинного активного віртуального шлюзу-відправника, решта віртуальних шлюзів стають вторинними віртуальними шлюзами-відправниками.

У ході виконанні операцій вибору віртуального шлюзу-відправника маршрутизатор групи резервування GLBP може знаходитися в одному з таких станів:

– вимкнений стан (*Disabled State*);

– початковий стан (*Initial State*);

– стан прослуховування мережі (*Listen State*);

– стан активного шлюзу-відправника (*Active State/ Active Virtual Forwarder*).

Діаграма змін станів віртуального шлюзу-відправника GLBP наведена на рис. 1, б.

У стані *Disabled State* маршрутизатор не володіє інформацією про віртуальну MAC-адресу (адреса або не налагоджена, або ще не отримана від інших пристроїв). У стані *Initial State* інформація про віртуальну MAC-адресу наявна, але процедура налагодження віртуального шлюзу-відправника ще не закінчена (повинен бути активованим і налагодженим фізичний інтерфейс для маршрутизації IP-пакетів, інтерфейсу повинна бути призначена IP-адреса, а також повинна бути відома віртуальна IP-адреса). У стані *Listen State* віртуальний шлюз-відправник отримує повідомлення GLBP Hello і готовий змінити свій стан на стан *Active State*, якщо активний віртуальний шлюз-відправник стане недоступним. Стан *Active State* свідчить про те, що пристрій виконує функції активного віртуального шлюзу-відправника і готовий пересилати кадри, які будуть надсилатися за його віртуальною MAC-адресою.

У протоколі GLBP підтримуються такі режими балансування (розподілу) навантаження:

– монопольний режим балансування (None Load-Balancing);

– циклічний режим балансування (Round-Robin Load-Balancing;

– режим балансування за адресою вузла (Host-Dependent Load-Balancing);

– зважений режим балансування (Weighted Load-Balancing);

У монопольному режимі не підтримується балансування навантаження. Всі запити, які надходять до AVG, на ньому ж і опрацьовуються. При використанні даного режиму правила роботи протоколу GLBP майже повністю відповідають правилам роботи протоколу HSRP.

Циклічний режим балансування передбачає почергове використання всіх активних віртуальних шлюзів-відправників для обслуговування запитів, які надходять від вузлів локальної мережі.

Режим балансування за адресою вузла застосовується у тих випадках, коли бажано, щоб один і той же вузол локальної мережі отримував у відповідь на свої ARP-запити до AVG одну і ту ж віртуальну MAC-адресу. Особливо це актуально у разі, якщо є необхідність використовувати технологію NAT. Даний режим використовується за замовчуванням.

Використання зваженого режиму балансування передбачає наявність вагових коефіцієнтів для кожного з маршрутизаторів – членів групи резервування GLBP. Потік трафіка, який надходить від вузлів локальної мережі AVG розподіляється між AVF пропорційно значенням їх вагових коефіцієнтів. Вагові коефіцієнти протоколу GLBP призначені для керування станами маршрутизаторів групи резервування. Активний статус, як правило, отримує той пристрій, ваговий коефіцієнт якого перевищує встановлене граничне значення. Значення вагових коефіцієнтів можуть встановлюватися як статично (визначаються на основі експлуатаційних характеристик шлюзів), так і динамічно (змінюються відповідно до змін станів їх зовнішніх інтерфейсів). Механізм відстеження станів зовнішніх інтерфейсів у протоколі GLBP багато у чому схожий на відповідний механізм протоколу HSRP. Відмітність полягає у тому, що механізм протоколу GLBP забезпечує можливість зміни вагового коефіцієнта шлюзу залежно від стану протоколу мережного рівня на контрольованому інтерфейсі.

Контроль працездатності активного віртуального шлюзу-диспетчера та активних шлюзів-відправників із використанням механізму розсилки повідомлень GLBP Hello не завжди є ефективним. Часто виникає ситуація, коли інтерфейс маршрутизатора, що бере участь у роботі протоколу GLBP, функціонує нормально, а зовнішній інтерфейс або канал зв'язку до сусіднього комунікаційного пристрою вийшов із ладу. У такому разі для вузлів локальної мережі стосовно доступності шлюзу за замовчуванням проблеми немає, а стосовно забезпечення пересилки IP-пакетів до зовнішних мереж проблема існує. Тому з метою підвищення надійності роботи у протоколі GLBP використовуються: спеціальний механізм контролю зовнішніх об'єктів (EOT, Enhanced Object Tracking) та функція Preemt. EOT забезпечує контроль стану зовнішніх (щодо інтерфейсу GLBP) інтерфейсів маршрутизатора, канальних сегментів та IP-мереж і динамічну зміну пріоритету маршрутизатора. Функція Preempt забезпечує швидкі перевибори після змін пріоритетів пристроїв. Дана функція для активного віртуального шлюзу-диспетчера за замовчуванням вимкнена, для активних віртуальних шлюзів-відправників увімкнена із затримкою 30 с. Слід зауважити, що механізм EOT та функція Preemt використовуються одночасно.

Основні параметри протоколу GLBP за замовчуванням наведені у табл. 1.

Таблиця 1

Параметри протоколу GLBP за замовчуванням

Характеристика/параметр	Значення
Функціонування протоколу за замовчуванням	неактивований
Групова IP-адреса призначення	224.0.0.102
UDP-порт (як відправника, так і отримувача)	3222
Кількість груп резервування	до 1024
Кількість активних шлюзів-відправників	до 255 (фактично обмежена 4-ма)
Віртуальна MAC-адреса	00-07-B4-YY-YY-YY
Пріоритет (вага) інтерфейсу за замовчуванням	100
Інтервал Hello Time за замовчуванням, с	3
Інтервал Hold Time за замовчуванням, с	10
Інтервал Redirect Time за замовчуванням, с	300
Інтервал Secondary Hold Time за замовчуванням, с	3600
Крок зміни пріоритету інтерфейсу при виконанні операції EOT	10

Примітка: YY-YY-YY – містить: 6 бітів, які дорівнюють 0; 10 бітів – номер групи резервування протоколу GLBP, 8 бітів – номер активного шлюзу-відправника

Порядок налагодження функціонування протоколу GLBP на маршрутизаторі Cisco

Налагодження функціонування протоколу динамічного резервування шлюзу та балансування навантаження GLBP на маршрутизаторі Cisco згідно з рекомендаціями виробника складається із певних обов'язкових та необов'язкових етапів. Порядок виконання згаданих етапів є таким:

1. Вибрати та активувати фізичний (Ethernet) інтерфейс маршрутизатора, налагодити параметри IP-адресації для обраного інтерфейсу (обов'язково).
2. Активувати функціонування протоколу на обраному інтерфейсі (обов'язково).
3. Налагодити параметри іменування групи резервування GLBP (необов'язково).
4. Налагодити параметри вибору (пріоритет) GLBP-маршрутизатора (необов'язково).
5. Налагодити часові та кількісні параметри опрацювання записів у кеш-таблиці протоколу (необов'язково).
6. Налагодити основні часові параметри відправки та утримання повідомлень протоколу (необов'язково).
7. Налагодити додаткові часові параметри протоколу (необов'язково).
8. Налагодити метод (та у разі необхідності параметри) балансування навантаження протоколу (необов'язково).
9. Налагодити параметри відстеження (контролю) стану зовнішніх щодо GLBP логічних об'єктів і параметри впливу на роботу протоколу при змінах у станах згаданих об'єктів (необов'язково).
10. Налагодити параметри активації протоколу GLBP після відновлення функціонування зовнішніх щодо GLBP логічних об'єктів (необов'язково).
11. Налагодити параметри аутентифікації протоколу GLBP (необов'язково).

Команди налагодження функціонування протоколу динамічного резервування шлюзу та балансування навантаження GLBP на маршрутизаторах Cisco

Налагодження функціонування протоколу динамічного резервування шлюзу та балансування навантаження GLBP може здійснюватися як на маршрутизаторах, так і на комутаторах 3-го рівня, виготовлених фірмою Cisco. Деякі відмітності у процесі налагодження можуть виникати через особливості синтаксису команд та версій Cisco IOS. Слід пам'ятати, що налагодження виконується не на маршрутизаторі у цілому, а лише на певному його інтерфейсі. За замовчуванням функціонування протоколу GLBP на інтерфейсі вимкнено.

Основною командою, від якої походить решта команд для налагодження засобів протоколу GLBP у Cisco IOS, є команда **glbp**. До переліку похідних команд входять такі команди, як: **glbp authentication**, **glbp client-cache**, **glbp forwarder preempt**, **glbp ip**, **glbp load-balancing**, **glbp name**, **glbp preempt**, **glbp priority**, **glbp timers**, **glbp weighting, glbp weighting track.** Важливими командами для налагодження також є команда **track** та похідні від неї команди **track interface**, **track ip route**, **track list**, **track rtr**. Призначення та синтаксис вищезгаданих команд наведено нижче.

Для активації функціонування протоколу GLBP використовується команда **glbp ip**. Ця ж команда використовується для призначення віртуальної IP-адреси групі резервування GLBP. Для зазначення текстової назви групи резервування протоколу GLBP застосовується команда **glbp name**. Зміна пріоритету GLBP-маршрутизатора здійснюється за допомогою команди **glbp priority**. Основні часові параметри розсилки та опрацювання повідомлень протоколу GLBP можна змінити за допомогою команди **glbp timers**. Додаткові часові параметри змінюються модифікацією попередньої команди – командою **glbp timers redirect**. Кількісні та часові параметри збереження та опрацювання записів у кеш-таблиці протоколу можна змінити за допомогою команди **glbp client-cache**.

Для вибору режиму балансування навантаження призначена команда **glbp load-balancing**. Для встановлення вагових коефіцієнтів при використанні зваженого режиму балансування застосовуєть-

ся команда **glbp weighting**. Модифікація команди **glbp weighting** – команда **glbp weighting track** дає змогу відстежувати стан зовнішніх щодо GLBP логічних об'єктів, пов'язаних із функціонуванням певних елементів мережі (інтерфейсів, каналів, протоколів), і впливати на роботу протоколу в разі виходу їх з ладу. Із застосуванням цієї команди тісно пов'язане застосування команд **glbp preempt** та **glbp forwarder preempt**. Активація функції перевиборів активного шлюзу-диспетчера після відновлення роботи попереднього активного шлюзу-диспетчера здійснюється за допомогою команди **glbp preempt**. Активація можливості для поточного пристрою взяти на себе функції активного віртуального шлюзу-відправника у випадку, якщо поточний активний віртуальний шлюз-відправник опустився нижче від порогового значення, здійснюється за допомогою команди **glbp forwarder preempt**.

Команда **glbp weighting track** також передбачає використання спеціалізованих команд, похідних від команди **track**, що забезпечують функціонування механізму EOT на маршрутизаторах Cisco як для протоколу GLBP, так і для протоколу VRRP. Серед команд **track** слід згадати команди **track interface**, **track ip route**, **track list**, **track rtr**. Після виконання цих команд здійснюється перехід у спеціальний режим config-track, у якому доступний набір інших спеціалізованих команд, зокрема команда налаштування затримок **delay**. Команда **track interface** застосовується для створення логічного об'єкта, що буде відстежувати або стан протоколу фізичної лінії (каналу) для певного інтерфейсу, або наявність маршруту у таблиці маршрутизації і можливість інтерфейсу маршрутизувати IP-пакети. За допомогою команди **track ip route** можна налагодити логічний об'єкт відстеження доступності певної віддаленої мережі. Команда **track list** дає змогу об'єднувати створені логічні об'єкти в один об'єкт і надалі відстежувати його стан.

У протоколі GLBP наявні засоби підвищення рівня захищеності при обміні службовими повідомленнями – засоби взаємної аутентифікації пристроїв, що входять у групу резервування GLBP. Налагодження аутентифікації здійснюється за допомогою команди **glbp authentication**.

Синтаксис команди **glbp authentication** (режим конфігурування інтерфейсу):

glbp *group_number* authentication md5 { { key-string [0 | 7] *key_string* } | { key-chain *key_chain* } } | text *string*,

де ***group_number*** – номер групи резервування протоколу GLBP; може набувати значень від 0 до 1023;

md5 – службова конструкція, за допомогою якої зазначається, що для аутентифікації пристроїв буде використовуватися функція хешування MD;

key-string – службова конструкція, за допомогою якої зазначається, що буде використовуватися ключ *key_string*, який може бути незашифрованим текстовим ключем (0) або зашифрованим за алгоритмом Віженера ключем (7);

key_string – текстовий ключ довжиною до 100 символів;

key-chain – службова конструкція, за допомогою якої зазначається, що буде використовуватися попередньо згенерований ключ;

key_chain – попередньо згенерований ключ;

text – службова конструкція, за допомогою якої зазначається, що буде застосовуватися аутентифікація з використанням звичайного відкритого пароля;

string – текстовий рядок пароля.

Синтаксис команди **glbp client-cache** (режим конфігурування інтерфейсу):

glbp *group_number* client-cache maximum *number_value* [timeout *timeout_value*],

де ***group_number*** – номер групи резервування протоколу GLBP; може набувати значень від 0 до 1023;

maximum – службова конструкція, за допомогою якої зазначається, яка кількість клієнтів буде збережена у кеш-таблиці протоколу;

number_value – максимальна кількість клієнтів у кеш-таблиці протоколу; може набувати значень від 8 до 2000;

timeout – службова конструкція, за допомогою якої зазначається інтервал часу збереження записів у кеш-таблиці протоколу;

timeout_value – значення інтервалу часу (хв); може набувати значень від 1 до 1440; рекомендується встановлювати значення,

дещо більше, ніж значення інтервалу часу збереження запису в ARP-таблиці (ARP-кеші).

Синтаксис команди **glbp forwarder preempt** (режим конфігурування інтерфейсу):

glbp *group_number* forwarder preempt [**delay minimum *delay_value***],

де ***group_number*** – номер групи резервування протоколу GLBP; може набувати значень від 0 до 1023;

delay minimum – службова конструкція, за допомогою якої зазначається мінімальна затримка перед тим, як пристрій візьме на себе фукнції віртуального шлюзу-відправника;

delay_value – значення інтервалу затримки (с), може набувати значень від 0 до 3600; за замовчуванням дорівнює 30 с.

Синтаксис команди **glbp ip** (режим конфігурування інтерфейсу):

glbp *group_number* ip [*IP_address* [secondary]],

де ***group_number*** – номер групи резервування протоколу GLBP; може набувати значень від 0 до 1023;

IP_address – IP-адреса для групи резервування протоколу GLBP (IP-адреса шлюзу за замовчуванням для кінцевих вузлів) у десятковому записі;

secondary – службова конструкція, за допомогою якої зазначається, що вказана IP-адреса є вторинною GLBP-адресою.

Синтаксис команди **glbp load-balancing** (режим конфігурування інтерфейсу):

glbp *group_number* load-balancing [**host-dependent** | **round-robin** | **weighted**],

де ***group_number*** – номер групи резервування протоколу GLBP; може набувати значень від 0 до 1023;

host-dependent – службова конструкція, за допомогою якої зазначається, що використовується режим балансування навантаження за адресою вузла;

round-robin – службова конструкція, за допомогою якої зазначається, що використовується циклічний режим балансування навантаження; даний режим балансування навантаження використовується за замовчуванням;

weighted – службова конструкція, за допомогою якої зазначається, що використовується зважений режим балансування навантаження.

Синтаксис команди **glbp name** (режим конфігурування інтерфейсу):

glbp *group_number* name *text*,

де ***group_number*** – номер групи резервування протоколу GLBP; може набувати значень від 0 до 1023;

text – текстовий рядок опису групи резервування протоколу GLBP.

Синтаксис команди **glbp preempt** (режим конфігурування інтерфейсу):

glbp *group_number* preempt [delay minimum *delay_value*],

де ***group_number*** – номер групи резервування протоколу GLBP; може набувати значень від 0 до 1023;

delay minimum – службова конструкція, за допомогою якої зазначається інтервал затримки перед тим, як маршрутизатор виконає спробу стати активним маршрутизатором після відновлення роботи каналу/інтерфейсу;

delay_value – значення інтервалу затримки (с), може набувати значень від 0 до 3600; за замовчуванням дорівнює 0 с.

Синтаксис команди **glbp priority** (режим конфігурування інтерфейсу):

glbp *group_number* priority *priority_level,*

де ***group_number*** – номер групи резервування протоколу GLBP; може набувати значень від 0 до 1023;

priority_level – значення пріоритету GLBP-маршрутизатора; може набувати значень від 1 до 255; значення 0 зарезервовано для спеціальних цілей; за замовчуванням значення пріоритету дорівнює 100; більше значення свідчить про вищий рівень пріоритету пристрою.

Синтаксис команди **glbp timers** (режим конфігурування інтерфейсу):

glbp *group_number* timers { [msec] *hellotime_value* [msec] *holdtime_value* } | { redirect *redirect_value timeout_value* },

де ***group_number*** – номер групи резервування протоколу GLBP; може набувати значень від 0 до 1023;

msec – службова конструкція, за допомогою якої вказується на те, що значення інтервалу розсилки буде зазначено в мілісекундах;

hellotime_value – значення інтервалу розсилки оновлення протоколу GLBP (с), може змінюватися у межах від 1 до 60; за замовчуванням дорівнює 3 с; якщо використовується конструкція **msec**, значення може змінюватися від 50 до 60000 мс;

holdtime_value – значення інтервалу утримання під час виконання функцій AVF та/або AVG протоколу GLBP (с), може змінюватися у межах від 1 до 180 с; за замовчуванням дорівнює 10 с; якщо використовується конструкція **msec**, значення може змінюватися від 1400 до 180000 мс; рекомендується, щоб даний інтервал був більший за інтервал розсилки оновлення протоколу у три і більше разів;

redirect – службова конструкція, за допомогою якої вказується інтервал Redirect Time, протягом якого AVG переспрямовує запити клієнтів до AVF та інтервал Secondary Hold Time, протягом якого Secondary AVF залишається дійсним, коли Primary AVF став недоступним;

redirect_value – значення інтервалу переспрямування запитів Redirect Time (с); може змінюватися у межах від 1 до 3600 с; за замовчуванням дорівнює 300 с;

timeout_value – значення вторинного інтервалу утримання Secondary Hold Time (с); може змінюватися у межах від ***redirect_value*** **+** 1 до 64800 с; за замовчуванням дорівнює 3600 с.

Синтаксис команди **glbp weighting** (режим конфігурування інтерфейсу):

glbp ***group_number*** **weighting** ***maximum_value*** **[lower** ***lower_value*** **] [upper** ***upper_value*****],**

де ***group_number*** – номер групи резервування протоколу GLBP; може набувати значень від 0 до 1023;

maximum_value – максимальне вагове значення; може змінюватися у межах від 1 до 254;

lower – службова конструкція, за допомогою якої налагоджується нижня межа вагового значення;

lower_value – значення нижньої межі вагового значення; може змінюватися у межах від 1 до ***maximum_value*** **– 1**;

upper – службова конструкція, за допомогою якої налагоджується верхня межа вагового значення;

upper_value – значення верхньої межі вагового значення; може змінюватися у межах від ***lower_value*** до ***maximum_value***.

Синтаксис команди **glbp weighting track** (режим конфігурування інтерфейсу):

glbp ***group_number*** **weighting track** ***object_number*** **[decrement** ***weight_value*****]**,

де ***group_number*** – номер групи резервування протоколу GLBP; може набувати значень від 0 до 1023;

object_number – номер об'єкта для відстеження; число, яке може набувати значень від 1 до 500;

decrement – службова конструкція, за допомогою якої зазначається зменшення вагового коефіцієнта інтерфейсу в разі виникнення певної події;

weight _value – значення, на яке ваговий коефіцієнт інтерфейсу зменшується у випадку, коли зовнішній об'єкт змінює свій стан (відключається); може змінюватися у межах від 1 до 254; за замовчуванням дорівнює 10.

Синтаксис команди **track interface** (режим конфігурування інтерфейсу):

track ***object_number*** **interface** ***interface_type interface_id*** **{ line-protocol | ip routing}**,

де ***object_number*** – номер об'єкта для відстеження; число, яке може набувати значень від 1 до 500;

interface_type – тип інтерфейсу, може набувати значень **Ethernet**, **FastEthernet**, **GigabitEthernet, Serial** тощо;

interface_id – ідентифікатор інтерфейсу (порту), може мати одночислове позначення ***number*** (номер порту), двочислове позначення ***module/number*** (номер модуля/номер порту), тричислове позначення ***slot/module/number*** (номер слоту/номер модуля (адаптера)/номер інтерфейсу);

line-protocol – службова конструкція, за допомогою якої зазначається ознака того, що буде контролюватися функціонування протоколу фізичної лінії (каналу);

ip routing – службова конструкція, за допомогою якої зазначається те, що буде контролюватися наявність маршруту у таблиці маршрутизації і можливість інтерфейсу маршрутизувати IP-пакети;

Синтаксис команди **track ip route** (режим конфігурування інтерфейсу):

track ***object_number*** **ip route** ***network_IP-address network_mask*** **{ metric threshold | reachability }**,

де ***object_number*** – номер об'єкта для відстеження; число, яке може набувати значень від 1 до 500;

network_IP-address – IP-адреса мережі (у десятковому записі),

network_mask – маска мережі, записана у звичайній формі;

metric threshold – службова конструкція, яка призначена для перевірки перевищення метрики маршруту до відповідної IP-мережі;

reachability – службова конструкція, яка призначена для активації перевірки досяжності відповідної IP-мережі.

Синтаксис команди **track list** (режим конфігурування інтерфейсу):

track ***object_number*** **list boolean {and | or } | threshold { percentage | weight }**,

де ***object_number*** – номер об'єкта для відстеження; число, яке може набувати значень від 1 до 500;

boolean – службова конструкція, за допомогою якої обирається логічна операція (**and** чи **or)**, яка буде виконуватися над об'єктами відстеження;

and – службова конструкція, за допомогою якої зазначається, що буде використовуватися операція логічного „ТА";

or – службова конструкція, за допомогою якої зазначається, що буде використовуватися операція логічного „АБО";

threshold – службова конструкція, за допомогою якої вказується варіант перевищення одного з параметрів **percentage** чи **weight**;

percentage – службова конструкція, за допомогою якої зазначається, що буде використовуватися параметр **percentage**;

percentage – службова конструкція, за допомогою якої зазначається, що буде використовуватися параметр **weight**.

Синтаксис команди **delay** (режим конфігурування параметрів відстеження об'єкта config-track):

delay up | down ***delay_value***,

де **up** – службова конструкція, за допомогою якої вказується затримка інформування після активації об'єкта відстеження;

down – службова конструкція, за допомогою якої вказується затримка інформування після деактивації об'єкта відстеження;

delay_value **–** значення інтервалу затримки (с); може змінюватися у межах від 1 до 180 с.

Команди моніторингу та діагностики роботи протоколу динамічного резервування шлюзу та балансування навантаження GLBP на маршрутизаторах Cisco

Для моніторингу та діагностики функціонування протоколу GLBP на маршрутизаторах Cisco використовуються як команди загального призначення, так і спеціалізовані команди. Перелік спеціалізованих команд є відносно невеликим і містить такі команди, як: **show glbp**, **show glbp *interface_type interface_id***, **show glbp active**, **show glbp brief**, **show glbp capability**, **show glbp disabled**, **show glbp init**, **show glbp listen**, **show glbp standby**. Важливими командами, які допомагають зрозуміти процеси передачі повідомлень протоколу GLBP, є команди відлагодження такі, як: **debug glbp**, **debug glbp errors**, **debug glbp events**, **debug glbp packets**, **debug glbp terse**. Узагальнений перелік команд моніторингу та діагностики роботи протоколу GLBP на маршрутизаторах Cisco наведений у табл. 2.

Таблиця 2

Перелік команд моніторингу та діагностики роботи протоколу GLBP на маршрутизаторах Cisco

Команда	Призначення
Команди **show glbp**	
show glbp	Виведення інформації про роботу протоколу GLBP
show glbp *interface_type interface_id*	Виведення інформації про функціонування протоколу GLBP на певному інтерфейсі
show glbp active	Виведення інформації про групи резервування протоколу GLBP, які знаходяться у стані *Active*
show glbp brief	Виведення інформації про функціонування протоколу GLBP у скороченому вигляді
show glbp capability	Виведення інформації про можливості протоколу GLBP
show glbp disabled	Виведення інформації про відключені групи резервування протоколу GLBP
show glbp init	Виведення інформації про групи резервування протоколу GLBP, які знаходяться у стані *Initial*
show glbp listen	Виведення інформації про групи резервування протоколу GLBP, які знаходяться у стані *Listen*
show glbp standby	Виведення інформації про групи резервування протоколу GLBP, які знаходяться у станах *Standby* або *Speak*
Команди **debug glbp**	
debug glbp	Активувати виведення узагальненої інформації про функціонування протоколу GLBP
debug glbp errors	Активувати виведення інформації про помилки протоколу GLBP
debug glbp events	Активувати виведення інформації про події протоколу GLBP
debug glbp packets	Активувати виведення інформації про передачу повідомлень протоколу GLBP
debug glbp terse	Активувати виведення інформації про обмежений набір помилок, подій, передачу повідомлень протоколу GLBP

Модельний приклад налагодження функціонування протоколу динамічного резервування шлюзу та балансування навантаження GLBP у мережі на базі обладнання Cisco

Розглянемо специфіку налагодження роботи протоколу резервування шлюзу та балансування навантаження GLBP для мережі, схема якої наведена на рис. 2. Для забезпечення функціонування мережі використано протокол маршрутизації EIGRP.

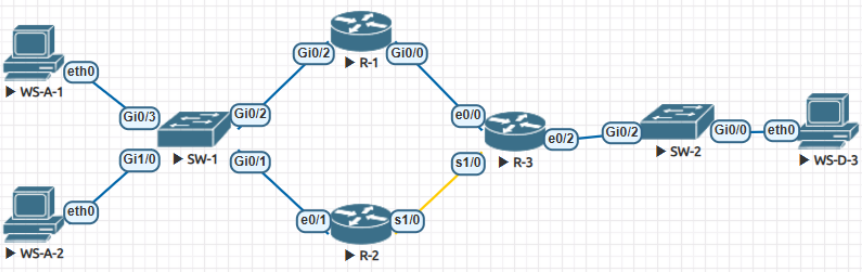


Рис. 2. Приклад мережі

Під час побудови даної мережі для з'єднання пристроїв використано дані табл. 3. Для налагодження параметрів адресації пристроїв використано дані табл. 4.

Таблиця 3

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R_1	Gig0/2	Комутатор SW_1	Gig0/2
	Gig0/0	Маршрутизатор R_3	Eth0/0
Маршрутизатор R_2	Eth0/1	Комутатор SW_1	Gig0/1
	Se1/0 (DCE)	Маршрутизатор R_3	Se1/0 (DTE)
Маршрутизатор R_3	Eth0/0	Маршрутизатор R_1	Fa0/1
	Eth0/2	Комутатор SW_2	Gig0/2
	Se1/0 (DTE)	Маршрутизатор R_2	Se1/0 (DCE)
Комутатор SW_1	Gig0/2	Маршрутизатор R_1	Gig0/2
	Gig0/1	Маршрутизатор R_2	Eth0/1
	Fa0/3	Робоча станція WS_A_1	Fa0/0
	Fa0/4	Робоча станція WS_A_2	Fa0/0
Комутатор SW_2	Gig0/2	Маршрутизатор R_3	Eth0/2
	Gig0/0	Робоча станція WS_D_1	Eth0
Робоча станція WS_A_1	Eth0	Комутатор SW_1	Gig0/3
Робоча станція WS_A_2	Eth0		Gig1/0
Робоча станція WS_D_1	Eth0	Комутатор SW_2	Gig0/0

Таблиця 4

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	–	195.10.1.0	255.255.255.0	/24
Підмережа B	–	195.20.1.0	255.255.255.252	/30
Підмережа C	–	195.30.1.0	255.255.255.252	/30
Підмережа D	–	195.40.1.0	255.255.255.128	/25
Маршрутизатор R_1	Інтерфейс Gig0/2	195.10.1.252	255.255.255.0	/24
	Інтерфейс Gig0/0	195.20.1.1	255.255.255.252	/30
Маршрутизатор R_2	Інтерфейс Eth0/1	195.10.1.253	255.255.255.0	/24
	Інтерфейс Se1/0	195.30.1.1	255.255.255.252	/30
Маршрутизатор R_3	Інтерфейс Gig0/2	195.20.1.2	255.255.255.252	/30
	Інтерфейс Eth0/2	195.40.1.126	255.255.255.128	/25
	Інтерфейс Se1/0	195.30.1.2	255.255.255.252	/30
Віртуальний маршрутизатор	Група резервування GLBP	195.10.1.254	255.255.255.0	/24
Комутатор SW_1	Інтерфейс Vlan 1	195.10.1.250	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
Комутатор SW_2	Інтерфейс Vlan 1	195.40.1.120	255.255.255.128	/25
	Шлюз за замовчуванням	195.40.1.126	–	–
Робоча станція WS_A_1 (Linux)	Мережний адаптер	195.10.1.1	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
Робоча станція WS_A_2(Windows)	Мережний адаптер	195.10.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	195.10.1.254	–	–
Робоча станція WS_D_1 (Linux)	Мережний адаптер	195.40.1.1	255.255.255.128	/25
	Шлюз за замовчуванням	195.40.1.126	–	–

Параметри налагодження протоколу GLBP для пристроїв підмережі A наведені у табл. 5.

Таблиця 5

Параметри налагодження протоколу GLBP для пристроїв підмережі A

Параметр	Значення параметра
Номер групи резервування	1
Опис групи резервування	LAN-A
Віртуальна IP-адреса	195.10.1.254
Віртуальна MAC-адреса 1	00-07-b4-00-01-01
Віртуальна MAC-адреса 2	00-07-b4-00-01-02
Активний віртуальний шлюз-диспетчер (AVG)	R_1
Пріоритет AVG	50
Резервний віртуальний шлюз-диспетчер (SVG)	R_2
Пріоритет SVG	45
Інтервал розсилки оновлень протоколу Hello Time, с	5
Інтервал утримання протоколу Hold Time, с	10
Затримка перед спробою стати AVG після перезавантаження, с	3

Сценарії налагодження параметрів адресації інтерфейсів та протоколу маршрутизації EIGRP для маршрутизаторів мережі наведені нижче.

```
…
R_1>enable
R_1#configure terminal
R_1(config)#interface GigabitEthernet 0/2
R_1(config-if)#description LINK_TO_LAN_A
R_1(config-if)#ip address 195.10.1.252 255.255.255.0
R_1(config-if)#no shutdown
R_1(config-if)#exit
R_1(config)#interface GigabitEthernet 0/0
R_1(config-if)#description LINK_TO_R_3
R_1(config-if)#ip address 195.20.1.1 255.255.255.252
R_1(config-if)#no shutdown
R_1(config-if)#exit
R_1(config)#router eigrp 1
R_1(config-router)#network 195.10.1.0 0.0.0.255
R_1(config-router)#network 195.20.1.0 0.0.0.3
R_1(config-router)#exit
R_1(config)#exit
R_1#
…
R_2>enable
R_2#configure terminal
R_2(config)#interface Ethernet 0/1
R_2(config-if)#description LINK_TO_LAN_A
R_2(config-if)#ip address 195.10.1.253 255.255.255.0
R_2(config-if)#no shutdown
R_2(config-if)#exit
R_2(config)#interface Serial 1/0
R_2(config-if)#description LINK_TO_R_3
R_2(config-if)#ip address 195.30.1.1 255.255.255.252
R_2(config-if)#clock rate 64000
R_2(config-if)#no shutdown
R_2(config-if)#exit
R_2(config)#router eigrp 1
```

R_2(config-router)#network 195.10.1.0 0.0.0.255
R_2(config-router)#network 195.30.1.0 0.0.0.3
R_2(config-router)#exit
R_2(config)# exit
R_2#
…
R_3>enable
R_3#configure terminal
R_3(config)#interface Ethernet 0/0
R_3(config-if)#description LINK_TO_R_1
R_3(config-if)#ip address 195.20.1.2 255.255.255.252
R_3(config-if)#no shutdown
R_3(config-if)#exit
R_3(config)#interface Ethernet 0/2
R_3(config-if)#description LINK_TO_LAN_D
R_3(config-if)#ip address 195.40.1.254 255.255.255.128
R_3(config-if)#no shutdown
R_3(config-if)#exit
R_3(config)#interface Serial 1/0
R_3(config-if)#description LINK_TO_R_2
R_3(config-if)#ip address 195.30.1.2 255.255.255.252
R_3(config-if)#no shutdown
R_3(config-if)#exit
R_3(config)#router eigrp 1
R_3(config-router)#network 195.20.1.0 0.0.0.3
R_3(config-router)#network 195.30.1.0 0.0.0.3
R_3(config-router)#network 195.40.1.0 0.0.0.127
R_3(config-router)#exit
R_3(config)# exit
R_3#
…

Сценарій налагодження параметрів адресації комутатора SW_1 та відключення функції **ip igmp snooping** наведений нижче.

```
…
SW_1>enable
SW_1#configure terminal
SW_1(config)#interface vlan 1
SW_1(config-if)#ip address 195.10.1.250 255.255.255.0
SW_1(config-if)#no shutdown
SW_1(config-if)#exit
SW_1(config)#no ip igmp snooping
SW_1(config)#exit
SW_1#
…
```

Сценарії налагодження функціонування протоколу резервування шлюзу та балансування навантаження GLBP на маршрутизаторах R_1 та R_2 наведені нижче.

```
…
R_1>enable
R_1#configure terminal
R_1(config)#interface GigabitEthernet 0/2
R_1(config-if)#glbp 1 ip 195.10.1.254
R_1(config-if)#glbp 1 priority 50
R_1(config-if)#glbp 1 name LAN-A
R_1(config-if)#glbp 1 timers 5 10
R_1(config-if)#glbp 1 preempt delay minimum 3
R_1(config-if)#glbp 1 load-balancing weighted
R_1(config-if)#glbp 1 weighting 95
R_1(config-if)#glbp 1 weighting track 100 decrement 95
R_1(config-if)#exit
R_1(config)#track 11 interface GigabitEthernet 0/0 line-protocol
R_1(config-track)#delay up 1
R_1(config-track)#delay down 1
R_1(config-track)#exit
R_1(config)#track 12 interface GigabitEthernet 0/0 ip routing
R_1(config-track)#delay up 1
R_1(config-track)#delay down 1
```

R_1(config-track)#exit
R_1(config)#track 100 list boolean or
R_1(config-track)#object 11
R_1(config-track)#object 12
R_1(config-track)#exit
R_1(config)#exit
R_1#
…

R_2>enable
R_2#configure terminal
R_2(config)#interface Ethernet 0/1
R_2(config-if)#glbp 1 ip 195.10.1.254
R_2(config-if)#glbp 1 priority 45
R_2(config-if)#glbp 1 name LAN-A
R_2(config-if)#glbp 1 timers 5 10
R_2(config-if)#glbp 1 preempt delay minimum 3
R_2(config-if)#glbp 1 load-balancing weighted
R_2(config-if)#glbp 1 weighting 5
R_2(config-if)#glbp 1 weighting track 200 decrement 5
R_2(config-if)#exit
R_2(config)#track 21 interface Serial 1/0 line-protocol
R_2(config-track)#delay up 1
R_2(config-track)#delay down 1
R_2(config-track)#exit
R_2(config)#track 22 interface Serial 1/0 ip routing
R_2(config-track)#delay up 1
R_2(config-track)#delay down 1
R_2(config-track)#exit
R_2(config)#track 200 list boolean or
R_2(config-track)#object 21
R_2(config-track)#object 22
R_2(config-track)#exit
R_2(config)#exit
R_2#
…

Результати виконання команд моніторингу та діагностики роботи протоколу GLBP для розглянутого прикладу

З метою перегляду інформації про роботу протоколу GLBP для розглянутого прикладу використано команди **show glbp** (команди **show glbp interface FastEthernet 0/0** для даного прикладу покажуть аналогічні результати**)**, **show glbp brief**, **show track, show track brief.** Результати роботи цих команд для маршрутизаторів R_1 та R_2 наведено відповідно на рис. 3 – 10.

```
R_1#show glbp
GigabitEthernet 0/0 - Group 1
  State is Active
    2 state changes, last state change 01:29:13
  Virtual IP address is 195.10.1.254
  Hello time 5 sec, hold time 10 sec
    Next hello sent in 2.296 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 3 sec
  Active is local
  Standby is 195.10.1.253, priority 45 (expires in 7.720 sec)
  Priority 50 (configured)
  Weighting 95 (configured 95), thresholds: lower 1, upper 95
    Track object 100 state Up decrement 95
  Load balancing: weighted
  IP redundancy name is "LAN-A"
  Group members:
    c401.077c.0000 (195.10.1.252) local
    c402.078b.0000 (195.10.1.253)
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 01:29:03
    MAC address is 0007.b400.0101 (default)
    Owner ID is c401.077c.0000
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 95
  Forwarder 2
    State is Listen
      608 state changes, last state change 00:00:34
    MAC address is 0007.b400.0102 (learnt)
    Owner ID is c402.078b.0000
    Redirection enabled, 595.144 sec remaining (maximum 600 sec)
    Time to live: 14395.144 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 195.10.1.253 (primary), weighting 5 (expires in 5.140 sec)
```

Рис. 3. Результати виконання команди **show glbp** на маршрутизаторі R_1

```
R_2#show glbp
Ethernet 0/1 - Group 1
  State is Standby
    4 state changes, last state change 00:01:40
  Virtual IP address is 195.10.1.254
  Hello time 5 sec, hold time 10 sec
    Next hello sent in 4.104 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 3 sec
  Active is 195.10.1.252, priority 50 (expires in 9.004 sec)
  Standby is local
  Priority 45 (configured)
  Weighting 5 (configured 5), thresholds: lower 1, upper 5
    Track object 200 state Up decrement 5
  Load balancing: weighted
  IP redundancy name is "LAN-A"
  Group members:
    c401.077c.0000 (195.10.1.252)
    c402.078b.0000 (195.10.1.253) local
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Listen
      2 state changes, last state change 00:01:50
    MAC address is 0007.b400.0101 (learnt)
    Owner ID is c401.077c.0000
    Time to live: 14396.868 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 195.10.1.252 (primary), weighting 95 (expires in 6.864 sec)
  Forwarder 2
    State is Active
      3 state changes, last state change 00:02:15
    MAC address is 0007.b400.0102 (default)
    Owner ID is c402.078b.0000
    Preemption enabled, min delay 30 sec
    Active is local, weighting 5
R_2#
```

Рис. 4. Результати виконання команди **show glbp** на маршрутизаторі R_2

```
R_1#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Gig0/2       1    -   50  Active   195.10.1.254    local           195.10.1.253
Gig0/2       1    1   -   Active   0007.b400.0101  local           -
Gig0/2       1    2   -   Listen   0007.b400.0102  195.10.1.253    -
R_1#
```

Рис. 5. Результати виконання команди **show glbp brief** на маршрутизаторі R_1

```
R_2#show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Eth0/1       1    -   45  Standby  195.10.1.254    195.10.1.252    local
Eth0/1       1    1   -   Listen   0007.b400.0101  195.10.1.252    -
Eth0/1       1    2   -   Active   0007.b400.0102  local           -
R_2#
```

Рис. 6. Результати виконання команди **show glbp brief** на маршрутизаторі R_2

```
R_1#show track
Track 11
  Interface GigabitEthernet 0/0 line-protocol
  Line protocol is Up
    1 change, last change 00:34:19
  Delay up 1 sec, down 1 sec
  Tracked by:
    Track-list 100
Track 12
  Interface GigabitEthernet 0/0 ip routing
  IP routing is Up
    1 change, last change 00:33:39
  Delay up 1 sec, down 1 sec
  Tracked by:
    Track-list 100
Track 100
  List boolean or
  Boolean OR is Up
    2 changes, last change 00:32:43
    object 11 Up
    object 12 Up
  Tracked by:
    GLBP GigabitEthernet 0/2
R_1#
```

Рис. 7. Результати виконання команди **show track** на маршрутизаторі R_1

```
R_2#show track
Track 21
  Interface Serial1/0 line-protocol
  Line protocol is Up
    2 changes, last change 00:05:21
  Delay up 1 sec, down 1 sec
  Tracked by:
    Track-list 200
Track 22
  Interface Serial1/0 ip routing
  IP routing is Up
    2 changes, last change 00:05:21
  Delay up 1 sec, down 1 sec
  Tracked by:
    Track-list 200
Track 200
  List boolean or
  Boolean OR is Up
    2 changes, last change 00:05:20
    object 21 Up
    object 22 Up
  Tracked by:
    GLBP Ethernet0/1 1
R_2#
```

Рис. 8. Результати виконання команди **show track** на маршрутизаторі R_2

```
R_1#show track brief
Track   Object                          Parameter        Value
11      interface GigabitEthernet 0/0   line-protocol    Up
12      interface GigabitEthernet 0/0   ip routing       Up
100     list                            boolean          Up
R_1#
```

Рис. 9. Результати виконання команди **show track brief** на маршрутизаторі R_1

```
R_2#show track brief
Track   Object                          Parameter        Value
21      interface Serial1/0             line-protocol    Up
22      interface Serial1/0             ip routing       Up
200     list                            boolean          Up
R_2#
```

Рис. 10. Результати виконання команди **show track brief** на маршрутизаторі R_2

З метою перевірки досяжності шлюзу за замовчуванням мережі A з робочих станцій WS_A_1 та WS_A_2 використано команду **ping**. З метою перевірки досяжності мережі D (зокрема, робочої станції WS_D_1) використано команду **tracert** (**traceroute).** Побічним результатом використання цих команд є додавання записів в ARP-таблиці відповідних вузлів. Результати виконання команд діагностики **ping**, **traceroute** (**tracert**), **arp** на робочих станціях WS_A_1 та WS_A_2 наведені відповідно на рис. 11 – 16.

```
root@WS_A_1~#ping 195.10.1.254
PING 195.10.1.254 (195.10.1.254): 56 data bytes
64 bytes from 195.10.1.254: seq=0 ttl=255 time=10.769 ms
64 bytes from 195.10.1.254: seq=1 ttl=255 time=6.331 ms
64 bytes from 195.10.1.254: seq=2 ttl=255 time=14.258 ms
64 bytes from 195.10.1.254: seq=3 ttl=255 time=9.333 ms
^C
--- 195.10.1.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 6.331/10.172/14.258 ms
root@WS_A_1~#
```

Рис. 11. Результати виконання команди **ping** на робочій станції WS_A_1

```
root@WS_A_1~#traceroute 195.40.1.1
traceroute to 195.40.1.1 (195.40.1.1), 30 hops max, 38 byte packets
 1  195.10.1.252 (195.10.1.252)  10.459 ms  10.886 ms  7.863 ms
 2  195.20.1.2 (195.20.1.2)  30.877 ms  31.386 ms  30.417 ms
 3  195.40.1.1 (195.40.1.1)  50.499 ms  42.296 ms  43.536 ms
root@WS_A_1~#
```

Рис. 12. Результати виконання команди **traceroute** на робочій станції WS_A_1

```
root@WS_A_1~#arp -a
? (195.10.1.254) at 00:07:b4:00:01:01 [ether]  on eth0
root@WS_A_1~#
```

Рис. 13. Результати виконання команди **arp** на робочій станції WS_A_1

```
C:\>ping 195.10.1.254
Обмен пакетами с 195.10.1.254 по 32 байт:
Ответ от 195.10.1.254: число байт=32 время 23мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 4мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 6мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 11мс TTL=125
Статистика Ping для 195.10.1.254:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 <0% потерь>,
Приблизительное время приема-передачи в мс:
    Минимальное = 4 мсек, Максимальное 23 мсек, Среднее = 11 мсек
C:\>
```

Рис. 14. Результати виконання команди **ping** на робочій станції WS_A_2

```
C:\>tracert 195.40.1.1
Трассировка маршрута к 195.4.1.2 с максимальным числом прыжков 30
  1    4 ms    10 ms    21 ms  195.10.1.253
  2   11 ms    10 ms    10 ms  195.10.1.252
  3   18 ms    31 ms    20 ms  195.20.1.2
  4   59 ms    43 ms    41 ms  195.40.1.1
Трассировка завершена.
C:\>
```

Рис. 15. Результати виконання команди **tracert** на робочій станції WS_A_2

```
c:\>arp -a
Интерфес: 195.10.1.2 -- 0x2
  Адрес IP            Физический адрес      Тип
  195.10.1.254        00:07:b4:00:01:01     динамический
c:\>
```

Рис. 16. Результати виконання команди **arp** на робочій станції WS_A_2

Необхідно зазначити, що команда **traceroute** (**tracert**) першими точками маршруту виводить не одну IP-адресу шлюзу за замовчуванням мережі (віртуальну IP-адресу групи резервування GLBP), а дві IP-адреси з однієї IP-мережі – адреси маршрутизаторів – членів групи резервування GLBP. Конкретний інтерфейс, через який відбуватиметься фактична передача трафіка, обирається відповідно до налагодженого режиму балансування навантаження. У нашому випадку – це маршрутизатор R_1.

З метою перевірки роботи протоколу GBRP змоделюємо ситуацію виходу з ладу каналу зв'язку між маршрутизаторами R_1 та R_2 за рахунок відключення інтерфейсу **FastEthernet 0/1** маршрутизатора R_1. Для відстеження інформаційного обміну між маршрутизаторами активуємо режим відлагодження на маршрутизаторі R_2. Зміни у роботі протоколу на маршрутизаторах R_1 та R_2 відстежимо за допомогою команд **show glbp** та **show track brief**. Результати виконання цих команд наведені на рис. 17 – 20. Результати інформаційного обміну між маршрутизаторами наведені на рис. 21.

```
R_1#show glbp
GigabitEthernet 0/2 - Group 1
  State is Active
    2 state changes, last state change 00:14:13
  Virtual IP address is 195.10.1.254
  Hello time 5 sec, hold time 10 sec
    Next hello sent in 1.640 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 3 sec
  Active is local
  Standby is 195.10.1.253, priority 45 (expires in 6.384 sec)
  Priority 50 (configured)
  Weighting 0, low (configured 95), thresholds: lower 1, upper 95
    Track object 100 state Down decrement 95
  Load balancing: weighted
  IP redundancy name is "LAN-A"
  Group members:
    c401.077c.0000 (195.10.1.252) local
    c402.078b.0000 (195.10.1.253)
  There are 2 forwarders (0 active)
  Forwarder 1
    State is Listen
      2 state changes, last state change 00:01:03
    MAC address is 0007.b400.0101 (default)
    Owner ID is c401.077c.0000
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is 195.10.1.253 (secondary), weighting 5 (expires in 8.012 sec)
  Forwarder 2
    State is Listen
      2 state changes, last state change 00:13:12
    MAC address is 0007.b400.0102 (learnt)
    Owner ID is c402.078b.0000
    Redirection enabled, 598.008 sec remaining (maximum 600 sec)
    Time to live: 14398.004 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is 195.10.1.253 (primary), weighting 5 (expires in 8.000 sec)
```

Рис. 17. Результати виконання команди **show glbp** на маршрутизаторі R_1

```
R_1#show track brief
Track   Object                          Parameter        Value
11      interface GigabitEthernet 0/2   line-protocol    Down (hw admin-down)
12      interface GigabitEthernet 0/2   ip routing       Down (hw admin-down)
100     list                            boolean          Down
```

Рис. 18. Результати виконання команди **show track brief** на маршрутизаторі R_1

```
R_2#show track brief
Track   Object                          Parameter        Value
21      interface Serial1/0             line-protocol    Up
22      interface Serial1/0             ip routing       Up
200     list                            boolean          Up
```

Рис. 19. Результати виконання команди **show track brief** на маршрутизаторі R_2

```
R_2#show glbp
Ethernet0/1 - Group 1
  State is Standby
    1 state change, last state change 00:14:57
  Virtual IP address is 195.10.1.254
  Hello time 5 sec, hold time 10 sec
    Next hello sent in 2.900 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 3 sec
  Active is 195.10.1.252, priority 50 (expires in 6.688 sec)
  Standby is local
  Priority 45 (configured)
  Weighting 5 (configured 5), thresholds: lower 1, upper 5
    Track object 200 state Up decrement 5
  Load balancing: weighted
  IP redundancy name is "LAN-A"
  Group members:
    c401.077c.0000 (195.10.1.252)
    c402.078b.0000 (195.10.1.253) local
  There are 2 forwarders (2 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:02:40
    MAC address is 0007.b400.0101 (learnt)
    Owner ID is c401.077c.0000
    Time to live: 14397.824 sec (maximum 14400 sec)
    Preemption enabled, min delay 30 sec
    Active is local, weighting 5
  Forwarder 2
    State is Active
      1 state change, last state change 00:14:39
    MAC address is 0007.b400.0102 (default)
    Owner ID is c402.078b.0000
    Preemption enabled, min delay 30 sec
    Active is local, weighting 5
```

Рис. 20. Результати виконання команди **show glbp** на маршрутизаторі R_2

```
R_2#
*Mar  1 00:41:11.703: GLBP: Fa0/0 1.1 Listen: k/Hello rcvd from lower pri Active
router (39/195.10.1.252)
*Mar    1  00:41:11.707:  GLBP  IPRAPI:  Group  "LAN-A"  (IDB:  656EDD8C),  event
FORWARDER_ACTIVE_CHANGE
*Mar  1 00:41:11.707: GLBP: Fa0/0 1.1 Listen -> Active
*Mar   1 00:41:11.707: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 1 state
Listen -> Active
R_2#
*Mar  1 00:41:11.707: GLBP: Fa0/0 1.1 Redundancy "LAN-A" state Backup -> Active
*Mar    1  00:41:11.707:  GLBP  IPRAPI:  Group  "LAN-A"  (IDB:  656EDD8C),  event
FORWARDER_STATE_CHANGE
R_2#
*Mar   1 00:41:32.307: GLBP: Fa0/0 API ARP active virtual address 195.10.1.254
found
```

Рис. 21. Результати інформаційного обміну протоколу GLBP на маршрутизаторі R_2

Також виконаємо перевірку досяжності шлюзу за замовчуванням мережі A та перевірку досяжності мережі D. Для цього також використаємо команди діагностики **ping, tracert** (**traceroute)**, **arp**. Результати виконання цих команд на робочих станціях WS_A_1 та WS_A_2 наведені відповідно на рис. 22 – 27.

```
root@WS_A_1~#ping 195.10.1.254
PING 195.10.1.254 (195.10.1.254): 56 data bytes
64 bytes from 195.10.1.254: seq=0 ttl=255 time=12.064 ms
64 bytes from 195.10.1.254: seq=1 ttl=255 time=5.239 ms
64 bytes from 195.10.1.254: seq=2 ttl=255 time=13.561 ms
64 bytes from 195.10.1.254: seq=3 ttl=255 time=10.502 ms
^C
--- 195.10.1.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 5.239/10.341/13.561 ms
root@WS_A_1~#
```

Рис. 22. Результати виконання команди **ping** на робочій станції WS_A_1

```
root@WS_A_1~#traceroute 195.40.1.1
traceroute to 195.40.1.1 (195.40.1.1), 30 hops max, 38 byte packets
 1  195.10.1.253 (195.10.1.253)  7.648 ms  8.826 ms  10.220 ms
 2  195.30.1.2 (195.30.1.2)  9.594 ms  10.748 ms  9.548 ms
 3  195.40.1.1 (195.40.1.1)  30.128 ms  19.790 ms  20.697 ms
root@WS_A_1~#
```

Рис. 23. Результати виконання команди **traceroute** на робочій станції WS_A_1

```
root@WS_A_1~#arp -a
? (195.10.1.254) at 00:07:b4:00:01:01 [ether]  on eth0
root@WS_A_1~#
```

Рис. 24. Результати виконання команди **arp** на робочій станції WS_A_1

```
C:\>ping 195.10.1.254
Обмен пакетами с 195.10.1.254 по 32 байт:
Ответ от 195.10.1.254: число байт=32 время 21мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 4мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 2мс TTL=125
Ответ от 195.10.1.254: число байт=32 время 6мс TTL=125
Статистика Ping для 195.10.1.254:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 <0% потерь>,
Приблизительное время приема-передачи в мс:
    Минимальное = 2 мсек, Максимальное 21 мсек, Среднее = 8 мсек
C:\>
```

Рис. 25. Результати виконання команди **ping** на робочій станції WS_A_2

```
C:\>tracert 195.40.1.1
Трассировка маршрута к 195.4.1.2 с максимальным числом прыжков 30
  2    8 ms    10 ms    32 ms  195.10.1.252
  3    9 ms    10 ms    10 ms  195.30.1.2
  4   27 ms    22 ms    19 ms  195.40.1.1
Трассировка завершена.
C:\>
```

Рис. 26. Результати виконання команди **tracert** на робочій станції WS_A_2

```
c:\>arp -a
Интерфес: 195.10.1.2 -- 0x2
  Адрес IP            Физический адрес      Тип
  195.10.1.254        00:07:b4:00:01:01     динамический
c:\>
```

Рис. 27. Результати виконання команди **arp** на робочій станції WS_A_2

Результат виконання команди **tracert** (**traceroute**) також підтверджує той факт, що маршрут передачі трафіку змінився – увесь мережний трафік із підмережі A до зовнішніх мереж фізично проходитиме через маршрутизатор R_2.

Завдання на лабораторну роботу

1. У середовищі віртуальної мережевої лабораторія eve.ztu.edu.ua створити проєкт мережі (рис. 28). Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 3.

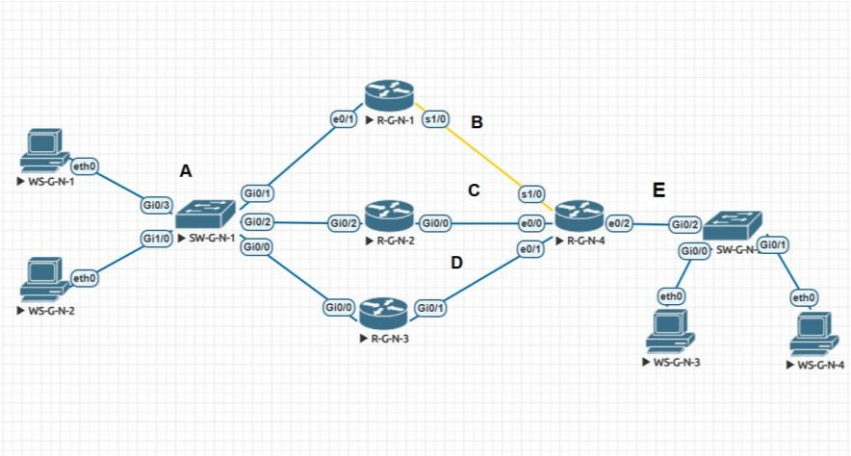


Рис. 28. Проект мережі

2. Розробити схему адресації пристроїв мережі. Для цього скористатися даними табл. 7. Результати навести у вигляді таблиці, яка аналогічна табл. 4.

3. Визначити основні параметри для налагодження протоколу GLBP для пристроїв підмережі A. Для визначення параметрів скористатися даними табл. 8. При виборі ролей GLBP-маршрутизаторів враховувати пропускні здатності зовнішніх каналів зв'язку. Результати навести у вигляді таблиці, яка аналогічна табл. 5.

4. Провести базове налагодження пристроїв, інтерфейсів та каналів зв'язку. Провести налагодження параметрів IP-адресації пристроїв мережі відповідно до даних, які отримані у п. 2. Перевірити наявність зв'язку між сусідніми парами пристроїв мережі. Налагодити функціонування засобів маршрутизації у побудованій ме-

режі (для вибору методу/протоколу маршрутизації скористатися даними табл. 8).

5. Налагодити основні параметри функціонування протоколу GLBP на пристроях мережі A відповідно до даних, які отримані у п. 3. При налагодженні комутатора/комутаторів мережі врахувати особливості використання протоколу GLBP у поєднанні з функцією ip igmp snooping.

6. Дослідити функціонування протоколу GLBP на пристроях мережі та маршрути передачі трафіка між вузлами віддалених підмереж A та E за встановленого за замовчуванням циклічного режиму балансування навантаження.

7. Налагодити додаткові параметри функціонування протоколу GLBP на пристроях мережі:

– циклічний режим балансування навантаження;

– відслідковування стану зовнішніх щодо GLBP інтерфейсів маршрутизаторів (обов'язково);

– відслідковування стану зовнішніх щодо GLBP мереж (необов'язково).

8. Дослідити функціонування протоколу GLBP на пристроях мережі та поведінку GLBP-пристроїв за умови:

– виходу з ладу (відключення) одного з маршрутизаторів – членів групи резервування GLBP;

– виходу з ладу (відключення) одного або кількох інтерфейсів, які використовуються для формування каналів B, C, D між маршрутизаторами мережі;

– відновлення функціонування маршрутизатора – члена групи резервування GLBP, який виходив із ладу;

– відновлення функціонування інтерфейсу/інтерфейсів, які виходили з ладу.

9. Дослідити процеси передачі даних між вузлами віддалених підмереж A та E в разі виконання дій, які аналогічні діям п. 9. Звернути увагу на зміни маршрутів передачі трафіка.

Таблиця 6

Варіанти технологій для побудови каналів (мереж)

№ варіанта	Канали підключення мережі A	Канал (мережа) B	Канал (мережа) C	Канал (мережа) D	Канал підключення мережі E
Не парні	1000BaseT	1000BaseT	1000BaseT	100BaseTX	1000BaseT
Парні	1000BaseFX	100BaseTX	1000BaseT	1000BaseT	1000BaseT

Таблиця 7

Дані для адресації підмереж (каналів)

№ варіанта	Підмережа A		Підмережа B		Підмережа C		Підмережа D		Підмережа E		Протокол маршрутизації
	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс	
Не парні	193.G.N.0	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/30	197.G.N.0	/24	OSPF
Парні	193.G.N.64	/27	194.G.N.0	/30	195.G.N.0	/30	196.G.N.0	/30	197.G.N.0	/25	EIGRP

Таблиця 8

Параметри для налагодження функціонування протоколу GLBP

№ варіанта	Номер групи резервування	Пріоритети маршрутизаторів			Інтервали протоколу	
		Active Virtual Gateway	Standby Virtual Gateway	Virtual Gateway	Hello-time, c	Holdtime, c
Не парні	101	200	195	190	3	10
Парні	102	195	190	185	4	11

Контрольні питання

1. Передумови розробки протоколу GLBP.
2. Загальна характеристика протоколу GLBP.
3. Порівняльна характеристика протоколів VRRP, HSRP, GLBP.
4. Стандартизація протоколу GLBP.
5. Характеристика протоколу GLBP стосовно моделі OSI.
6. Характеристика протоколу GLBP стосовно стеку TCP/IP.
7. Ролі пристроїв у протоколі GLBP. Група резервування протоколу VRRP.
8. Стани пристроїв у протоколі GLBP.
9. Адресація у протоколі GLBP.
10. Часові інтервали та таймери протоколу GLBP.
11. Структура повідомлення протоколу GLBP. Типи повідомлень протоколу GLBP.
12. Балансування навантаження у протоколі GLBP.

Лабораторна робота № 7
НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ МАРШРУТИЗАЦІЇ BGP У МЕРЕЖІ НА БАЗІ МАРШРУТИЗАТОРІВ CISCO

Мета заняття: налагодити функціонування протоколу маршрутизації BGP у мережі на базі маршрутизаторів Cisco; дослідити особливості функціонування даного протоколу маршрутизації**.**

Теоретичні відомості

Прикордонний (зовнішній) шлюзовий протокол (Border Gateway Protocol, BGP) версії 4 на сьогодні є основним протоколом обміну маршрутною інформацією між автономними системами в Інтернеті. Протокол BGP прийшов на зміну EGP (Exterior Gateway Protocol), який використовувався в ті часи, коли Інтернет мав єдину магістраль. Ця магістраль була центральною автономною системою, до якої приєднувалися, у відповідності до деревовидної технології, всі інші автономні системи.

Маршрутизатори, які використовують протокол BGP, обмінюються інформацією про доступність мереж. Разом з інформацією про мережі передаються різні атрибути цих мереж, за допомогою яких BGP обирає кращий маршрут та налаштовуються політики маршрутизації.

Один з основних атрибутів, котрі передаються разом з інформацією про маршрут - це список автономних систем, через які ця інформація пройшла. Ця інформація дозволяє BGP визначити, де знаходиться мережа відносно автономних систем, виключати петлі маршрутизації, а також може бути використана при налаштуванні політик.

Маршрутизація здійснюється покроково від однієї автономної системи до іншої. Всі політики BGP налаштовуються, в основному, по відношенню до зовнішніх (сусідніх) автономних систем, тобто описуються правила взаємодії з ними.

BGP обирає кращі маршрути не на основі технічних характеристик шляху (пропускної здатності, затримки, тощо), а на основі політик. В локальних мережах найбільше значення має швидкість сходження мережі, час реагування на зміни. І маршрутизатори, котрі використовують внутрішні протоколи

динамічної маршрутизації, при виборі маршруту, як правило, порівнюють якісь технічні характеристики шляху, наприклад, пропускну здатність інтерфейсів.

Якщо існує декілька шляхів до отримувача, то маршрутизатор буде анонсувати сусідам не всі можливі варіанти, а тільки кращий з таблиці BGP.

Таймери протоколу маршрутизації BGP

Keepalive Interval - Інтервал часу в секундах між відправкою повідомлень keepalive. За замовчуванням 60 секунд.

Hold Time - Інтервал часу в секундах, по закінченні якого сусід буде вважатися недоступним.

Порядок налаштування функціонування протоколу маршрутизації BGP на маршрутизаторі Cisco

У загальному випадку налагодження функціонування протоколу BGP складається з кількох обов'язкових, деяких необов'язкових, але рекомендованих та великої кількості необов'язкових етапів. Порядок виконання налагодження є наступним:

1. Створення процесу BGP (обов'язково).
2. Вибір ідентифікатора маршрутизатора (необов'язково).
3. Створення сусідів BGP (обов'язково).
4. Вказати підключені мережі, параметри яких відповідають налаштуванню інтерфейсів, або налагодити редистрибуцію маршрутів (обов'язково).
5. Відключити сумаризацію маршрутів (необов'язково).
6. Налагодити сумарну агреговану адресу (необов'язково).

Команди базового налагодження фунціонування протоколу маршрутизації BGP на маршрутизаторі Cisco

Основними командами, які є необхідними і достатніми для мінімально ефективного налагодження роботи протоколу BGP, є команди **neighbor, network, auto-summary, aggregate-address, redistribute**. Решта команд використовується у специфічних складних ситуаціях.

Команда **network** призначена для прямого інформування протоколу про безпосередньо підключені мережі.

Команда **auto-summary** по-різному поводиться при використанні її з командами **redistribute** і **network**.

При включеній команді **auto-summary**:

- команда **redistribute** додає лише відповідну класову мережу до BGP-таблиці,
- команда **network** додає відповідну класову мережу та підмережі (якщо вони є в таблиці маршрутизації) до BGP-таблиці.

При вимкненій команді **no auto-summary**:

- команда **redistribute** додає відповідні підмережі до BGP-таблиці,
- команда **network** додає підмережі до BGP-таблиці, якщо вони є в таблиці маршрутизації.

Команда ***aggregate-address*** дозволяє створити сумарні маршрути вручну.

Синтаксис основних команд налагодження протоколу BGP та режими їх застосування наведено нижче.

Синтаксис команди ***router*** (привілейований режим):

router bgp *[as_number]*,

де ***as_number*** - номер автономної системи BGP, який може набувати значень від 1 до 65535;

Синтаксис команди ***neighbor*** (режим налагодження протоколу маршрутизації):

neighbor *[ip-address | peer-group-name]* remote-as *[as_number],*

де ***ip-address*** - ідентифікатор сусіднього маршрутизатора, тобто та адреса, яка буде вказана в ролі отримувача в BGP-пакетах. У локального маршрутизатора обов'язково має бути маршрут до цього сусіда для того, щоб успішно встановити відношення сусідства з ним.

peer-group-name - група маршрутизаторів BGP, які використовують однакову політику оновлень.

as_number - номер автономної системи сусіда.

Синтаксис команди network (режим налагодження протоколу маршрутизації):

network *[address]* mask *[network-mask],*

де address - адреса мережі в десятковому вигляді,

mask *[network-mask]* - маска мережі (може не вказуватися).

Синтаксис команди **auto-summary** (режим налагодження протоколу маршрутизації):

auto-summary. Команда не має параметрів.

Синтаксис команди **redistribute** (режим налагодження протоколу маршрутизації):

redistribute *[protocol] [metrics],*

де ***protocol*** - протокол маршрутизації,

metrics - значення метрики.

Команди налагодження таймерів протоколу маршрутизації BGP на маршрутизаторах Cisco

Серед додаткових параметрів протоколу BGP, які доводиться налагоджувати адміністратору мережі, основними є таймери протоколу. Для налагодження таймерів протоколу застосовуються команда **timers bgp**. Синтаксис даної команди та режим її застосування наведено нижче.

Синтаксис команди **timers bgp** (режим конфігурування протоколу маршрутизації):

timers bgp *[keepalive] [holdtime]*,

де ***keepalive*** - значення інтервалу між відправкою повідомлень keepalive в секундах, за замовчуванням становить 60 секунд.

holdtime - інтервал часу, після закінчення якого сусід буде вважатися недоступним, задається в секундах, за замовчуванням становить 180 секунд.

Команди моніторингу та діагностики роботи протоколу маршрутизації BGP на маршрутизаторі Cisco

Для моніторингу та діагностики роботи протоколу BGP на маршрутизаторах Cisco використовуються як команди загального призначення, так і спеціалізовані команди. Серед команд загального призначення можна виділити такі команди: **show interfaces, show interface *interface-type interface-id,* show running-config, show startup-config.**

До спеціалізованих команд належать команди: **show ip protocols, show ip route, show ip bgp neighbors, show ip bgp all, show ip bgp replication, debug bgp ipv4, debug bgp all, undebug all.**

Зазначені спеціалізовані команди мають певний набір модифікацій, які формують інші команди, їх перелік наведений у табл. 1.

Таблиця 1

Перелік команд моніторингу та діагностики роботи протоколу маршрутизації BGP на маршрутизаторах Cisco

Команда	Призначення
show ip protocols	Виведення інформації про активовані протоколи маршрутизації та параметри їх функціонування
show ip protocols summary	Виведення сумарної інфомації про функціонування IP-протоколів
show ip route	Виведення повної таблиці маршрутизації
show ip route eigrp	Виведення таблиці маршрутизації протоколу BGP
show ip route A.B.C.D	Виведення детальної маршрутної інформації певної мережі
show ip route hostname	Виведення детальної маршрутної інформації певного вузла
show ip bgp neighbors	Виведення інформації про сусідні маршрутизатори, які беруть участь у роботі протоколу BGP
show ip bgp all	Виведення інформації про всі мережі протоколу.
show ip bgp replication	Виведення інформації про статус реплікації.
debug bgp ipv4	Активація виведення діагностичної інформації про мережі протоколу IP версії 4.
debug bgp all	Активація виведення діагностичної інформації про всі мережі протоколу.
undebug bgp ipv4	Деактивація виведення діагностичної інформації про мережі протоколу IP версії 4.
undebug bgp all	Деактивація виведення діагностичної інформації про всі мережі протоколу.

Приклад налагодження функціонування мережі з використанням протоколу маршрутизації BGP та маршрутизаторів Cisco

Розглянемо специфіку налагодження роботи протоколу BGP для мережі, зображеної на рис. 1.

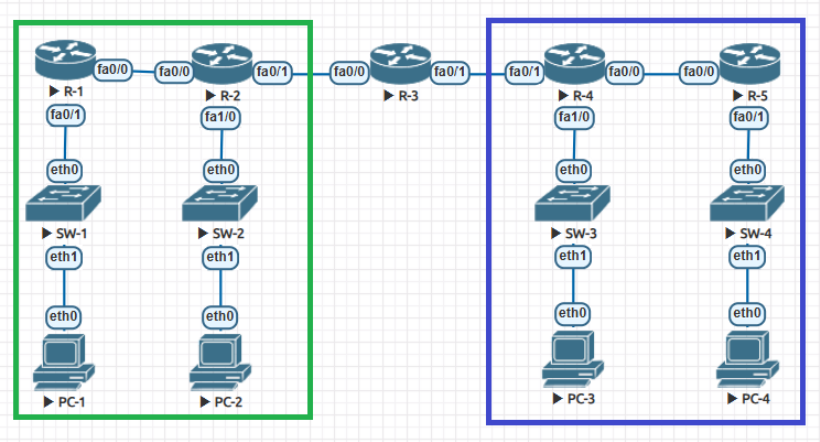


Рис. 1. Приклад мережі

При побудові даної мережі для з'єднання пристроїв використано дані табл. 1. Для налагодження параметрів адресації пристроїв використано дані табл. 2.

Таблиця 1

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R-1	Fa0/0	R-2	Fa0/0
	Fa0/1	SW-1	Eth0
Маршрутизатор R-2	Fa0/0	R-1	Fa0/0
	Fa0/1	R-3	Fa0/0
	Fa1/0	SW-2	Eth0
Маршрутизатор R-3	Fa0/0	R-2	Fa0/1
	Fa0/1	R-4	Fa0/1
Маршрутизатор R-4	Fa0/0	R-5	Fa0/0
	Fa0/1	R-3	Fa0/1
	Fa1/0	SW-3	Eth0
Маршрутизатор R-5	Fa0/0	R-4	Fa0/0
	Fa0/1	SW-4	Eth0
Комутатор SW-1	Eth0	R-1	Fa0/0
	Eth1	PC-1	Eth0

Продовження таблиці 1

Комутатор SW-2	Eth0	R-2	Fa0/0
	Eth1	PC-2	Eth0
Комутатор SW-3	Eth0	R-4	Fa1/0
	Eth1	PC-3	Eth0
Комутатор SW-4	Eth0	R-5	Fa0/1
	Eth1	PC-4	Eth0
Робоча станція PC-1	Eth0	SW-1	Eth1
Робоча станція PC-2	Eth0	SW-2	Eth1
Робоча станція PC-3	Eth0	SW-3	Eth1
Робоча станція PC-4	Eth0	SW-4	Eth1

Таблиця 2

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Підмережа A	–	192.168.1.0	255.255.255.0	/24
Підмережа B	–	192.168.2.0	255.255.255.0	/24
Підмережа C	–	192.168.3.0	255.255.255.0	/24
Підмережа D	–	192.168.4.0	255.255.255.0	/24
Підмережа E	–	10.10.10.0	255.255.255.252	/30
Підмережа F	–	11.11.11.0	255.255.255.252	/30
Підмережа G	–	21.21.21.0	255.255.255.252	/30
Підмережа H	–	20.20.20.0	255.255.255.252	/30
Маршрутизатор R-1	Інтерфейс Fa0/0	10.10.10.1	255.255.255.252	/30
	Інтерфейс Fa0/1	192.168.1.1	255.255.255.0	/24
Маршрутизатор R-2	Інтерфейс Fa0/0	10.10.10.2	255.255.255.252	/30
	Інтерфейс Fa0/1	11.11.11.1	255.255.255.252	/30
	Інтерфейс Fa1/0	192.168.2.1	255.255.255.0	/24
Маршрутизатор R-3	Інтерфейс Fa0/0	11.11.11.2	255.255.255.252	/30
	Інтерфейс Fa0/1	21.21.21.2	255.255.255.252	/30
Маршрутизатор R-4	Інтерфейс Fa0/0	20.20.20.1	255.255.255.252	/30
	Інтерфейс Fa0/1	21.21.21.1	255.255.255.252	/30
	Інтерфейс Fa1/0	192.168.3.1	255.255.255.0	/24
Маршрутизатор R-5	Інтерфейс Fa0/0	20.20.20.2	255.255.255.252	/30
	Інтерфейс Fa0/1	192.168.4.1	255.255.255.0	/24
Робоча станція PC-1	Мережний адаптер	192.168.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.1	–	–
Робоча станція PC-2	Мережний адаптер	192.168.2.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.2.1	–	–
Робоча станція PC-3	Мережний адаптер	192.168.3.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.3.1	–	–
Робоча станція PC-4	Мережний адаптер	192.168.4.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.4.1	–	–

Сценарії налагодження параметрів адресації інтерфейсів та протоколу маршрутизації для маршрутизаторів мережі наведені нижче.

R-1#configure terminal
R-1(config)#interface FastEthernet0/1
R-1(config-if)#ip address 192.168.1.1 255.255.255.0
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#interface FastEthernet0/0
R-1(config-if)#ip address 10.10.10.1 255.255.255.252
R-1(config-if)#no shutdown
R-1(config-if)#exit
R-1(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
R-1(config)#router ospf 1
R-1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R-1(config-router)#network 10.10.10.0 0.0.0.3 area 0
R-1(config-router)#passive-interface FastEthernet 0/1
…
R-2(config-if)#no shutdown
R-2(config-if)#exit
R-2(config)#interface FastEthernet0/1
R-2(config-if)#ip address 11.11.11.1 255.255.255.252
R-2(config-if)#no shutdown
R-2(config-if)#exit
R-2(config)#interface FastEthernet1/0
R-2(config-if)#ip address 192.168.2.1 255.255.255.252
R-2(config-if)#no shutdown
R-2(config-if)#exit
R-2(config)#router ospf 1
R-2(config-router)#network 192.168.2.0 0.0.0.255 area 0
R-2(config-router)#network 10.10.10.0 0.0.0.3 area 0
R-2(config-router)#passive-interface FastEthernet 1/0
…
R-3#configure terminal
R-3(config)#interface FastEthernet0/0
R-3(config-if)#ip address 11.11.11.2 255.255.255.252
R-3(config-if)#no shutdown
R-3(config-if)#exit

R-3(config)#interface FastEthernet0/1
R-3(config-if)#ip address 21.21.21.2 255.255.255.252
R-3(config-if)#no shutdown
R-3(config-if)#exit
…
R-4(config)#interface FastEthernet0/0
R-4(config-if)#ip address 20.20.20.1 255.255.255.252
R-4(config-if)#ip address 20.20.20.1 255.255.255.252
R-4(config-if)#no shutdown
R-4(config-if)#exit
R-4(config)#interface FastEthernet1/0
R-4(config-if)#ip address 192.168.3.1 255.255.255.0
R-4(config-if)#no shutdown
R-4(config-if)#exit
R-4(config)#router eigrp 1
R-4(config-router)#network 20.20.20.0 0.0.0.3
R-4(config-router)#network 192.168.3.0 0.0.0.255
R-4(config-router)#passive-interface fa1/0
R-4(config-router)#passive-interface fa0/1
…
R-5#configure terminal
R-5(config)#interface FastEthernet0/0
R-5(config-if)#ip address 20.20.20.2 255.255.255.252
R-5(config-if)#no shutdown
R-5(config-if)#exit
R-5(config)#interface FastEthernet0/1
R-5(config-if)#ip address 192.168.4.1 255.255.255.0
R-5(config-if)#no shutdown
R-5(config-if)#exit
R-5(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
…

Сценарії налагодження протоколу маршрутизації BGP для маршрутизаторів мережі наведені нижче.

…
R-2(config)#router bgp 100
R-2(config-router)#neighbor 11.11.11.2 remote-as 1
R-2(config-router)#redistribute ospf 1
…

R-3(config)#router bgp 1
R-3(config-router)#network 11.11.11.0 mask 255.255.255.252
R-3(config-router)#network 21.21.21.0 mask 255.255.255.252
R-3(config-router)#neighbor 11.11.11.1 remote-as 100
R-3(config-router)#neighbor 21.21.21.1 remote-as 200
…
R-4(config)#router bgp 200
R-4(config-router)#neighbor 21.21.21.2 remote-as 1
R-4(config-router)#redistribute eigrp 1
…

Результати виконання команд моніторингу та діагностики роботи протоколу маршрутизації BGP для розглянутого прикладу

З метою перегляду інформації про параметри інтерфейсів та роботу протоколу маршрутизації OSPF для розглянутого прикладу використано команди моніторингу та діагностики роботи **show ip route, show ip bgp, show ip bgp summary**. Результати роботи цих команд для маршрутизаторів наведено відповідно на рис. 2–10.

```
R-2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     21.0.0.0/30 is subnetted, 1 subnets
B       21.21.21.0 [20/0] via 11.11.11.2, 00:06:34
     20.0.0.0/30 is subnetted, 1 subnets
B       20.20.20.0 [20/0] via 11.11.11.2, 00:06:34
B    192.168.4.0/24 [20/0] via 11.11.11.2, 00:06:34
     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, FastEthernet0/0
     11.0.0.0/30 is subnetted, 1 subnets
C       11.11.11.0 is directly connected, FastEthernet0/1
O    192.168.1.0/24 [110/20] via 10.10.10.1, 00:16:46, FastEthernet0/0
     192.168.2.0/30 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, FastEthernet1/0
B    192.168.3.0/24 [20/0] via 11.11.11.2, 00:06:39
R-2#
```

Рис. 2. Результат роботи команди **show ip route** для маршрутизатора R-2

```
R-3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     21.0.0.0/30 is subnetted, 1 subnets
C       21.21.21.0 is directly connected, FastEthernet0/1
     20.0.0.0/30 is subnetted, 1 subnets
B       20.20.20.0 [20/0] via 21.21.21.1, 00:00:03
B    192.168.4.0/24 [20/307200] via 21.21.21.1, 00:00:03
     10.0.0.0/30 is subnetted, 1 subnets
B       10.10.10.0 [20/0] via 11.11.11.1, 00:00:03
     11.0.0.0/30 is subnetted, 1 subnets
C       11.11.11.0 is directly connected, FastEthernet0/0
B    192.168.1.0/24 [20/20] via 11.11.11.1, 00:00:03
     192.168.2.0/30 is subnetted, 1 subnets
B       192.168.2.0 [20/0] via 11.11.11.1, 00:00:07
B    192.168.3.0/24 [20/0] via 21.21.21.1, 00:00:07
R-3#
```

Рис. 3. Результат роботи команди **show ip route** для маршрутизатора R-3

```
R-4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
     21.0.0.0/30 is subnetted, 1 subnets
C       21.21.21.0 is directly connected, FastEthernet0/1
     20.0.0.0/30 is subnetted, 1 subnets
C       20.20.20.0 is directly connected, FastEthernet0/0
D    192.168.4.0/24 [90/307200] via 20.20.20.2, 00:11:09, FastEthernet0/0
     10.0.0.0/30 is subnetted, 1 subnets
B       10.10.10.0 [20/0] via 21.21.21.2, 00:07:38
     11.0.0.0/30 is subnetted, 1 subnets
B       11.11.11.0 [20/0] via 21.21.21.2, 00:07:38
B    192.168.1.0/24 [20/0] via 21.21.21.2, 00:07:43
     192.168.2.0/30 is subnetted, 1 subnets
B       192.168.2.0 [20/0] via 21.21.21.2, 00:07:43
C    192.168.3.0/24 is directly connected, FastEthernet1/0
R-4#
```

Рис. 4. Результат роботи команди **show ip route** для маршрутизатора R-4

```
R-2#show ip bgp
BGP table version is 16, local router ID is 192.168.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/30    0.0.0.0                  0         32768 ?
r> 11.11.11.0/30    11.11.11.2               0             0 1 i
*> 20.20.20.0/30    11.11.11.2                             0 1 200 ?
*> 21.21.21.0/30    11.11.11.2               0             0 1 i
*> 192.168.1.0      10.10.10.1              20         32768 ?
*> 192.168.2.0/30   0.0.0.0                  0         32768 ?
*> 192.168.3.0      11.11.11.2                             0 1 200 ?
*> 192.168.4.0      11.11.11.2                             0 1 200 ?
```

Рис. 5. Результат роботи команди **show ip bgp** для маршрутизатора R-2

```
R-3#show ip bgp
BGP table version is 9, local router ID is 21.21.21.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/30    11.11.11.1               0             0 100 ?
*> 11.11.11.0/30    0.0.0.0                  0         32768 i
*> 20.20.20.0/30    21.21.21.1               0             0 200 ?
*> 21.21.21.0/30    0.0.0.0                  0         32768 i
*> 192.168.1.0      11.11.11.1              20             0 100 ?
*> 192.168.2.0/30   11.11.11.1               0             0 100 ?
*> 192.168.3.0      21.21.21.1               0             0 200 ?
*> 192.168.4.0      21.21.21.1          307200             0 200 ?
```

Рис. 6. Результат роботи команди **show ip bgp** для маршрутизатора R-3

```
R-4#show ip bgp
BGP table version is 10, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/30    21.21.21.2                             0 1 100 ?
*> 11.11.11.0/30    21.21.21.2               0             0 1 i
*> 20.20.20.0/30    0.0.0.0                  0         32768 ?
r> 21.21.21.0/30    21.21.21.2               0             0 1 i
*> 192.168.1.0      21.21.21.2                             0 1 100 ?
*> 192.168.2.0/30   21.21.21.2                             0 1 100 ?
*> 192.168.3.0      0.0.0.0                  0         32768 ?
*> 192.168.4.0      20.20.20.2          307200         32768 ?
```

Рис. 7. Результат роботи команди **show ip bgp** для маршрутизатора R-4

```
R-2#show ip bgp summary
BGP router identifier 192.168.2.1, local AS number 100
BGP table version is 16, main routing table version 16
8 network entries using 960 bytes of memory
8 path entries using 416 bytes of memory
5/4 BGP path/bestpath attribute entries using 620 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 2076 total bytes of memory
BGP activity 11/3 prefixes, 11/3 paths, scan interval 60 secs
Neighbor            V      AS  MsgRcvd  MsgSent     TblVer   InQ  OutQ  Up/Down
State/PfxRcd
11.11.11.2      4     1      27      26       16    0    0 00:11:00        5
```

Рис. 8. Результат роботи команди **show ip bgp summary** для маршрутизатора R-2

```
R-3#show ip bgp summary
BGP router identifier 21.21.21.2, local AS number 1
BGP table version is 9, main routing table version 9
8 network entries using 960 bytes of memory
8 path entries using 416 bytes of memory
6/5 BGP path/bestpath attribute entries using 744 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 2200 total bytes of memory
BGP activity 8/0 prefixes, 8/0 paths, scan interval 60 secs
Neighbor            V      AS  MsgRcvd  MsgSent     TblVer   InQ  OutQ  Up/Down
State/PfxRcd
11.11.11.1      4   100      17      20        9    0    0 00:11:34        3
21.21.21.1      4   200      16      19        9    0    0 00:11:22        3
```

Рис. 9. Результат роботи команди **show ip bgp summary** для маршрутизатора R-3

```
R-4#show ip bgp summary
BGP router identifier 192.168.3.1, local AS number 200
BGP table version is 10, main routing table version 10
8 network entries using 960 bytes of memory
8 path entries using 416 bytes of memory
5/4 BGP path/bestpath attribute entries using 620 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 2076 total bytes of memory
BGP activity 8/0 prefixes, 8/0 paths, scan interval 60 secs
Neighbor            V      AS  MsgRcvd  MsgSent     TblVer   InQ  OutQ  Up/Down
State/PfxRcd
21.21.21.2      4     1      20      17       10    0    0 00:12:26        5
```

Рис. 10. Результат роботи команди **show ip bgp summary** для маршрутизатора R-4

Завдання на лабораторну роботу

1. У середовищі віртуальної мережевої лабораторія eve.ztu.edu.ua створити проєкт мережі (рис. 11). Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 1

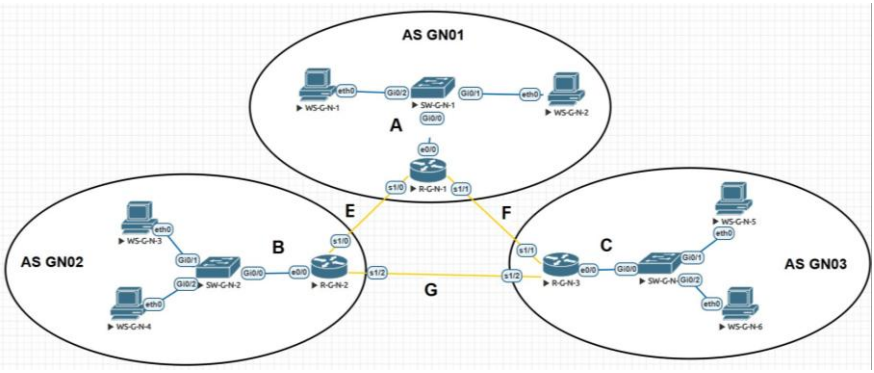


Рис. 11. Проект мережі

2. Розробити схему адресації пристроїв мережі. Для цього використовувати дані табл. 4. Результати навести у вигляді таблиці, яка аналогічна табл. 2.

3. На маршрутизаторах мережі налагодити функціонування протоколу BGP. Маршрутизацію всередині автономних систем налаштувати відповідно до даних табл. 5. Налаштувати редистрибуцію маршрутів.

4. Дослідити особливості отримання службової та діагностичної інформації протоколу за допомогою відповідних команд.

5. Дослідити процеси передачі даних між вузлами віддалених підмереж. У разі відсутності зв’язку визначити проблеми та усунути їх.

Таблиця 3

Параметри підмереж (каналів зв'язку)

№ варіанта	Канал E			Канал F			Канал G		
	DCE	Clock rate, біт/с	Bandwidth, Кбіт\с	DCE	Clock rate, біт/с	Bandwidth, Кбіт\с	DCE	Clock rate, біт/с	Bandwidth, Кбіт\с
Не парні	R_G_N_1	9600	64	R_G_N_3	500000	128	R_G_N_3	72000	192
Парні	R_G_N_1	1000000	128	R_G_N_3	800000	192	R_G_N_2	500000	256

Таблиця 4

Дані для адресації підмереж

№ варіанта	Підмережа A		ПідмережаB		Підмережа C	
	IP-адреса	Префікс	IP-адреса	Префікс	IP-адреса	Префікс
Не парні	193.G.N.0	/25	193.G.N.128	/25	194.G.N.0	/29
Парні	193.G.N.0	/26	193.G.N.64	/26	194.G.N.8	/29

Таблиця 5

Протоколи маршрутизації для автономних систем

№ варіанту	**AS GN01**	**AS GN02**	**AS GN03**
Не парні	OSPF	RIP	EIGRP
Парні	RIP	EIGRP	OSPF

Контрольні питання

1. Що таке BGP і для чого він використовується в комп'ютерних мережах?
2. Чим відрізняється внутрішній протокол маршрутизації від зовнішнього, на прикладі BGP?
3. Яка основна роль атрибуту AS-path у BGP?
4. Які кроки є обов'язковими при налаштуванні BGP на маршрутизаторі Cisco?
5. Для чого використовується команда neighbor у конфігурації BGP?
6. Що виконує команда network у налаштуванні BGP?
7. У чому різниця між командами auto-summary та no auto-summary у BGP?
8. Для чого використовується команда aggregate-address?
9. Яке призначення команди redistribute у BGP?
10. Які параметри визначають роботу таймерів BGP, та для чого використовується команда timers bgp?
11. Яке призначення команди show ip bgp summary?
12. Що означає символ *> у виведенні команди show ip bgp?
13. Як перевірити стан сусідства між BGP-маршрутизаторами?
14. У чому полягає різниця між LocPrf, Weight та Metric у таблиці BGP?

Лабораторна робота № 8
НАГОДЖЕННЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ L2/L3 MPLS VPN У МЕРЕЖІ НА БАЗІ МАРШРУТИЗАТОРІВ CISCO

Мета заняття: налагодити функціонування технологій L2/L3 MPLS VPN у мережі на базі маршрутизаторів Cisco; дослідити особливості побудови, маршрутизації та передачі даних у мережі MPLS з використанням механізмів VRF.

Теоретичні відомості

MPLS (англ. Multiprotocol Label Switching — багатопротокольна комутація за мітками) — механізм передачі даних, який емулює різні властивості мереж з комутацією каналів через мережі з комутацією пакетів.

MPLS є масштабуємим та незалежним від будь-яких протоколів (L2TP, PPTP, PPPoE) механізмом передачі даних. В мережі, заснованій на MPLS, пакетам даних присвоюються мітки. Рішення про подальшу передачу пакету даних іншому вузлу здійснюється лише на основі значення присвоєної мітки без необхідності вивчення самого пакета даних.

За рахунок того, що проводиться лише аналіз міток можливе створення наскрізного віртуального каналу, незалежно від середовища передачі та використовуючи будь-який протокол передачі.

MPLS було розроблено з метою забезпечення універсальної служби передавання даних як для клієнтів мереж з комутацією каналів, так і мереж із комутацією пакетів. За допомогою MPLS можна передавати трафік найрізноманітнішої природи, такий як IP-пакети, ATM, Frame Relay, SONET і кадри Ethernet.

Багатопротокольною (MultiProtocol) комутацією MPLS називається, тому що її засоби можуть застосовуватись до будь-якого протоколу мережевого рівня, тобто MPLS - це свого роду інкапсулюючий протокол, здатний транспортувати інформацію багатьох протоколів нижчих рівнів моделі OSI.

Робочі групи, що займалися розробкою технології MPLS визначили 3 основних її елементи:

- FEC (Forwarding Equivalency Class) – Клас еквівалентності пересилки;

- LSR (Label Switching Router) – маршрутизатори комутації міток;
- LSP (Label Switched Path) – маршрут по мітках.

Серед LSR можна виділити такі компоненти як:

- Граничні маршрутизатори провайдера (LER (E-LSR) – Label Edge Router – граничний маршрутизатор міток) – на вході в домен дані маршрутизатори додають MPLS-мітку до пакету даних, а на виході видаляють MPLS-мітку з пакету. Також мають назву PE (Provide Edge).
- Маршрутизатори MPLS домену (LSR – Label Switching Router - маршрутизатор, що комутує мітки) – це маршрутизатори, що виконують маршрутизацію спираючись лише на значення мітки. Інша назва – P (Provide).

Окрему групу становлть маршрутизатори призначені для підключення користувачів – CE маршрутизатори.

У заголовку пакета міститься набагато більше інформації, ніж потрібно для того, щоб вибрати наступний маршрутизатор при передачі даних. Цей вибір можна організувати простіше - шляхом виконання двох функцій. Одна з них полягає в поділі всієї безлічі пакетів, що надходять на класи, які називаються класами еквівалентності пересилки FECs (Forwarding Equivalence Classes). Друга ставить у відповідність кожному FEC певний «напрямок» пересилки (в мережі використовується режим hop-by-hop, і різні пакети одного і того ж FEC можуть пересилатися до різних маршрутизаторів, тобто фізичні напрямки пересилання можуть бути різними). З точки зору вибору наступного маршрутизатора всі пакети, що належать одному FEC, не відрізняються.

LSR маршрутизатори для обміну інформацією про мітки використовують протокол LDP (Label Distribution Protocol). За допомогою даного протоколу маршрутизатори можуть виявити один одного та встановити взаємодію.

Послідовність LSR маршрутизаторів, які комутують пакет з міткою через MPLS мережу утворюють маршрут просування пакетів через MPLS мережу – LSP (Label Switch Path).

Головна задача розподілу міток - це організація і обслуговування трактів LSP, в тому числі, визначення кожної прив'язки «FEC-мітка» у кожному LSR тракті LSP.

Для комутації пакетів VPN між пристроями LSR використовується дві мітки, що утворюють стек.

Загалом технологія MPLS заснована на обробці заголовку MPLS, що додається до кожного пакета даних. Цей заголовок може складатись з 1 чи декількох міток (стеку міток). Кожен запис стеку містить 4 поля. Заголовок MPLD зображений на рисунку 1.

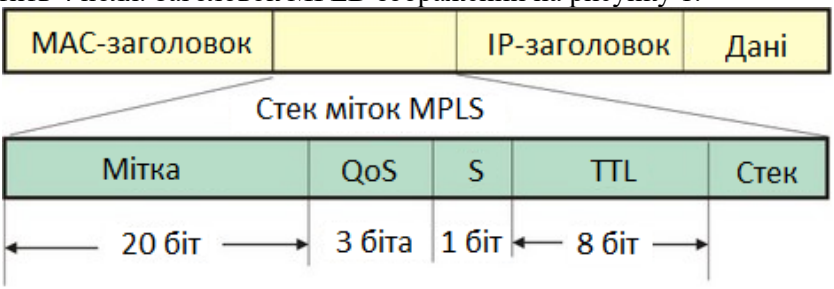


Рис 1. Заголовок MPLS

Поле значення мітки в MPLS заголовку займає 20 біт, таким чином максимально можливе значення мітки одно 1048576.

За допомогою міток визначаються і маршрути, і атрибути послуг. На периферії мережі, в точці входу, відбувається обробка вхідних пакетів. Тут же вибираються і привласнюються мітки . Опорна мережа зчитує мітки, відповідним чином обробляє пакети і передає їх далі згідно з мітками. Дії, що вимагають великих процесорних потужностей (аналіз, класифікація і фільтрація), виконуються тільки один раз, в точці входу. Після цього пакети з мітками передаються по опорній мережі. Пристрої опорної мережі сервіспровайдера передають пакети тільки на основі міток і не аналізують заголовки IP- пакетів. У точці виходу мітки видаляються, і пакети передаються в пункт призначення.

Особливості технології L2 MPLS VPN

Для створення VPN Layer 2 за схемою точка-точка (point-to-point) розроблена технологія Any Transport Over MPLS (AToM), що забезпечує передачу Layer 2 фреймів через MPLS мережу.

AToM - це інтегральна технологія, що включає Frame Relay over MPLS, ATM over MPLS, Ethernet over MPLS.

EoMPLS інкапсулює Ethernet фрейми в MPLS пакети і використовує стек міток для просування через MPLS мережу.

Канал, побудований на технології EoMPLS, для споживача послуг провайдера виглядає як віртуальний патчкорд.

Перевагою використання технології L2VPN MPLS є те, що L2 VPN не прив'язаний до конкретних IP-мереж і працює на рівні Ethernet.

Послуга дозволяє зв'язати два локальних мережевих сегмента. Реалізація здійснюється на базі AToM - Any Transport over MPLS. Призначається для забезпечення прозорої передачі через MPLS-мережу будь-яких транспортних протоколів 2-го рівня.

Особливості технології L3 MPLS VPN

L3 MPLS VPN полягає у використання сумісно технологій VRF та MPLS VPN.

За великим рахунком, технологія VRF близька до поняття VPN. Але VPN - це принцип об'єднання вузлів клієнта, що знаходяться під єдиним адміністративним підпорядкуванням, через публічну мережу оператора, а VRF - це більше опис VPN в прибудовах одного пристрою, який включає атрибути і правила розповсюдження маршрутної інформації, окрему таблицю маршрутизації і так далі.

Іншими словами, VRF-и ділять один фізичний роутер, на певну кількість віртуальних роутерів, які працюють незалежно один від одного. Таким чином виходить, що скільки у нас буде заплановано VPN-ів, стільки VRF-ів нам необхідно буде створити на пристрої.

VRF (virtual routing and forwarding instance) – це об’єкт, до складу якого входять компоненти, що відносяться до конкретної VPN на конкретному вузлі доступу до мережі MPLS:

- Множина інтерфейсів LSR, до яких підключається маршрутизатор зі сторони клієнта із одного VPN;
- VRF-таблиця;
- Атрибути і правила розповсюдження маршрутної інформації.

VRF є локальним для кожного LSR пристрою.

Виділяють два параметри у VRF:

- RD (Route Distinguisher) – унікальний для кожного VRF ідентифікатор (може бути лише один), який перетворює маршрут IPv4 в унікальний для всієї мережі провайдера

маршрут VPNv4. Фактично саме він дозволяє використовувати перетин адресації у клієнтів.

- RT (Route Target) – параметр, який додається в спеціальне поле при розсилці маршрутів всередині мережі оператора по MP-BGP (MultiProtocol BGP – розширення для BGP, що дає можливість роботи і з VPNv4 маршрутами), який і визначає в таблицю маршрутизації якого чи яких VRF попаде даний маршрут.

Щоб зв'язати територіально рознесені сайти замовника в єдину мережу, необхідно, по-перше, створити для них загальний простір поширення маршрутної інформації, по-друге, прокласти у внутрішній мережі шляхи, по яких належать різним сайтам вузли однієї і тієї ж мережі VPN могли б вести захищений обмін даними.

Механізмом, за допомогою якого сайти, що належать одній і тій же мережі VPN, обмінюються маршрутною інформацією, є багатопротокольне розширення для протоколу BGP (MultiProtocol extensions for BGP, MP-BGP). З його допомогою прикордонні маршрутизатори організовують сеанси зв'язку, в рамках яких обмінюються маршрутною інформацією зі своїх таблиць VRF.

Особливість протоколу BGP і його розширень полягає в тому, що він отримує і передає свої маршрутні оголошення не всім безпосередньо пов'язаним з ним маршрутизаторам, як протоколи IGP, а тільки тим, які зазначені в його конфігураційних параметрах як сусідів. Причому сусідами можуть бути « призначені» маршрутизатори, що знаходяться на відстані багатьох хопів. Маршрутизатор PE сконфігурований так, що всі одержувані від клієнтських сайтів маршрутні оголошення він за допомогою MP-BGP пересилає тільки певним прикордонним маршрутизаторам PE. Цілеспрямоване поширення маршрутів між маршрутизаторами PE забезпечується належним вибором атрибутів протоколу MP-BGP.

Питання про те, кому відправляти маршрутні оголошення, а кому ні, цілком залежить від топології віртуальних приватних мереж, підтримуваних даним постачальником послуг.

Отже, крім маршрутів , що надходять від безпосередньо приєднаних до пристрою PE сайтів, кожна таблиця VRF доповнюється маршрутами, одержуваними від інших сайтів даної мережі VPN по протоколу MP-BGP. Таким шляхом створюються таблиці , що описують маршрути в рамках окремої мережі VPN.

Основними перевагами організації VPN на базі MPLS можна назвати:

- Можливість масштабування;
- Можливість перетину адресних просторів, вузлів, що підключені до різних VPN;
- Ізолювання трафіку VPN один від одного на другому рівні моделі OSI.

Порядок налаштування функціонування протоколу MPLS на маршрутизаторі Cisco

1. Увімкнути MPLS на пристрої.
2. Увімкнути MPLS на відповідних інтерфейсах.
3. Визначити Router ID для LDP.
4. Перевірити, що IGP забезпечує повну IP-зв'язність між маршрутизаторами.
5. Переконатися, що LDP-сусідство встановлено.

Команди базового налагодження фунціонування протоколу маршрутизації MPLS на маршрутизаторі Cisco

Основними командами, які є необхідними і достатніми для мінімально ефективного налагодження роботи протоколу MPLS, є команди **mpls ip, mpls label protocol, mpls ldp router-id, mpls mtu**. Решта команд використовується у специфічних або розширених сценаріях налаштування MPLS VPN, TE тощо.

Команда **mpls ip** активує підтримку протоколу MPLS на пристрої або інтерфейсі.

Команда **mpls label protocol** дозволяє вказати протокол для обміну мітками (найчастіше використовується LDP).

Команда **mpls ldp router-id** використовується для встановлення ідентифікатора маршрутизатора для LDP.

Команда **mpls mtu** використовується для задання розміру MTU, необхідного для інкапсуляції MPLS.

Синтаксис основних команд налагодження протоколу MPLS та режими їх застосування наведено нижче.

Синтаксис команди активації MPLS (глобальний режим конфігурації):

mpls ip

– активує MPLS глобально на маршрутизаторі.

Синтаксис команди визначення протоколу обміну мітками (глобальний режим конфігурації):

mpls label protocol ldp

– задає LDP як протокол обміну мітками.

Синтаксис команди вказання router-id для LDP (глобальний режим конфігурації):

mpls ldp router-id *[інтерфейс]* force

де інтерфейс – зазвичай loopback-інтерфейс, що стабільно працює незалежно від фізичних з'єднань.

Синтаксис команди активації MPLS на інтерфейсі (режим конфігурації інтерфейсу):

interface *[інтерфейс]*

mpls ip

Синтаксис команди встановлення MTU для MPLS (режим конфігурації інтерфейсу):

mpls mtu *[значення]* де значення, як правило, не менше 1512.

Команди моніторингу та діагностики роботи протоколу маршрутизації MPLS на маршрутизаторі Cisco

Для моніторингу та діагностики роботи протоколу MPLS на маршрутизаторах Cisco використовуються як команди загального призначення, так і спеціалізовані команди. Серед команд загального призначення можна виділити такі команди: **show interfaces, show interface *[тип] [номер],* show running-config, show startup-config**.

До спеціалізованих команд належать команди: **show mpls interfaces, show mpls ldp neighbors, show mpls forwarding-table, show mpls ldp bindings, debug mpls ldp, undebug all.** Зазначені спеціалізовані команди мають певний набір модифікацій, які формують інші команди, їх перелік наведений у таблиці 1.

Таблиця 1

Команди моніторингу та діагностики протоколу MPLS на маршрутизаторі Cisco

Команда	**Призначення**
show mpls interfaces	Перевірка активних інтерфейсів з підтримкою MPLS
show mpls ldp neighbors	Відображення інформації про LDP-сусідів
show mpls forwarding-table	Таблиця пересилки MPLS-пакетів
show mpls ldp bindings	Перевірка зіставлення міток до префіксів
debug mpls ldp	Отримання діагностичної інформації по LDP
undebug all	Виведення детальної маршрутної інформації певного вузла

Приклад налагодження функціонування мережі з використанням протоколу маршрутизації MPLS та маршрутизаторів Cisco

Розглянемо специфіку налагодження роботи протоколу BGP для мережі, зображеної на рис. 2.

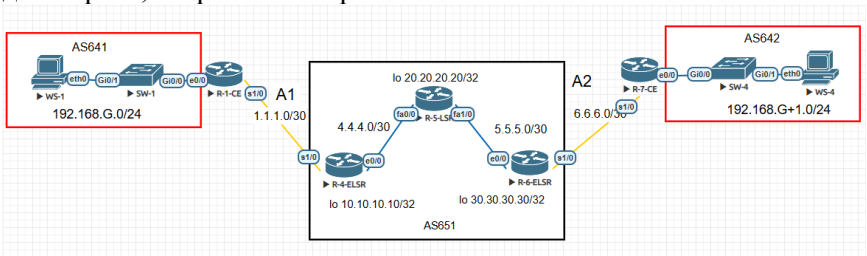


Рис. 2. Приклад мережі

При побудові даної мережі для з'єднання пристроїв використано дані табл. 2. Для налагодження параметрів адресації пристроїв використано дані табл. 3.

Таблиця 2

Параметри інтерфейсів пристроїв для прикладу

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R1-CE	Se1/0	R-4-ELSR	Se1/0
	Eth0/0	SW-1	Gig0/0
Маршрутизатор R-4-ELSR	Se1/0	R1-CE	Se1/0
	Fa0/1	R-3	Fa0/0
Маршрутизатор R-5-LSR	Fa0/0	R-4-ELSR	Eth0/0
	Fa1/0	R-6-ELSR	Eth0/0
Маршрутизатор R-6-ELSR	Eth0/0	R-5-LSR	Fa1/0
	Se1/0	R7-CE	Se1/0
Маршрутизатор R7-CE	Se1/0	R-6-ELSR	Se1/0
	Eth0/0	SW-4	Gig0/0
Комутатор SW-1	Gig0/0	R1-CE	Eth0/0
	Gig0/1	WS-1	Eth0
Комутатор SW-4	Gig0/0	R7-CE	Eth0/0
	Gig0/1	WS-4	Eth0
Робоча станція WS-1	Eth0	SW-1	Gig0/1
Робоча станція WS-4	Eth0	SW-2	Gig0/1

Таблиця 3

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підмережі	Пре-фікс
Підмережа A	–	192.168.1.0	255.255.255.0	/24
Підмережа B	–	192.168.2.0	255.255.255.0	/24
Підмережа C	–	192.168.3.0	255.255.255.0	/24
Підмережа D	–	192.168.4.0	255.255.255.0	/24
Підмережа E	–	10.10.10.0	255.255.255.252	/30
Підмережа F	–	11.11.11.0	255.255.255.252	/30
Підмережа G	–	21.21.21.0	255.255.255.252	/30
Підмережа H	–	20.20.20.0	255.255.255.252	/30
Маршрутизатор R-G-N-1-CE	Інтерфейс Fa0/0	10.10.10.1	255.255.255.252	/30
	Інтерфейс Fa0/1	192.168.1.1	255.255.255.0	/24
Маршрутизатор R-G-N-4-ELSR	Інтерфейс Fa0/0	10.10.10.2	255.255.255.252	/30
	Інтерфейс Fa0/1	11.11.11.1	255.255.255.252	/30
	Інтерфейс Fa1/0	192.168.2.1	255.255.255.0	/24
Маршрутизатор R-G-N-6-ELSR	Інтерфейс Fa0/0	11.11.11.2	255.255.255.252	/30
	Інтерфейс Fa0/1	21.21.21.2	255.255.255.252	/30
Маршрутизатор R-G-N-5-LSR	Інтерфейс Fa0/0	20.20.20.1	255.255.255.252	/30
	Інтерфейс Fa0/1	21.21.21.1	255.255.255.252	/30
	Інтерфейс Fa1/0	192.168.3.1	255.255.255.0	/24
Маршрутизатор R-G-N-7-CE	Інтерфейс Fa0/0	20.20.20.2	255.255.255.252	/30
	Інтерфейс Fa0/1	192.168.4.1	255.255.255.0	/24
Комутатор SW-1	Мережний адаптер	192.168.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.1	–	–
Комутатор SW-4	Мережний адаптер	192.168.2.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.2.1	–	–
Робоча станція WS-1	Мережний адаптер	192.168.3.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.3.1	–	–
Робоча станція WS-4	Мережний адаптер	192.168.4.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.4.1	–	–

Сценарії налагодження параметрів адресації інтерфейсів, протоколів маршрутизації та налаштування протоколу MPLS для маршрутизаторів мережі наведені нижче.

…

R-G-N-1-CE#configure terminal
R-G-N-1-CE(config)#interface Ethernet0/0.5
R-G-N-1-CE(config-subif)#encapsulation dot1Q 5
R-G-N-1-CE(config-subif)#ip address 192.168.45.254 255.255.255.0
R-G-N-1-CE(config-subif)#exit

R-G-N-1-CE(config)#interface Ethernet0/0
R-G-N-1-CE(config-if)#no shutdown
R-G-N-1-CE(config-if)#exit
R-G-N-1-CE(config)#interface Serial1/0
R-G-N-1-CE(config-if)#ip address 1.1.1.2 255.255.255.252
R-G-N-1-CE(config-if)#exit
R-G-N-1-CE(config)#ip route 0.0.0.0 0.0.0.0 Serial1/0
R-G-N-1-CE(config)#router bgp 64561
R-G-N-1-CE(config-router)#network 192.168.45.0
R-G-N-1-CE(config-router)#neighbor 1.1.1.1 remote-as 65561
…
R-G-N-4-ELSR#configure terminal
R-G-N-4-ELSR(config)#interface Loopback0
R-G-N-4-ELSR(config-if)#ip address 10.10.10.10 255.255.255.255
R-G-N-4-ELSR(config-if)#exit
R-G-N-4-ELSR(config)#interface Ethernet0/0
R-G-N-4-ELSR(config-if)#ip address 4.4.4.2 255.255.255.252
R-G-N-4-ELSR(config-if)#mpls ip
R-G-N-4-ELSR(config-if)#no shutdown
R-G-N-4-ELSR(config-if)#exit
R-G-N-4-ELSR(config)#router eigrp 1
R-G-N-4-ELSR(config-router)#network 4.4.4.0 0.0.0.3
R-G-N-4-ELSR(config-router)#network 10.10.10.10 0.0.0.0
R-G-N-4-ELSR(config-router)#exit
R-G-N-4-ELSR(config)#router bgp 65561
R-G-N-4-ELSR(config-router)#neighbor 30.30.30.30 remote-as 65561
R-G-N-4-ELSR(config-router)#neighbor 30.30.30.30 update-source Loopback0
R-G-N-4-ELSR(config-router)#address-family vpnv4
R-G-N-4-ELSR(config-router-af)#neighbor 30.30.30.30 activate
R-G-N-4-ELSR(config-router-af)#exit
R-G-N-4-ELSR(config)#ip vrf A1
R-G-N-4-ELSR(config-vrf)#rd 2:1
R-G-N-4-ELSR(config-vrf)#route-target both 2:1
R-G-N-4-ELSR(config-vrf)#exit
R-G-N-4-ELSR(config)#interface Serial1/0
R-G-N-4-ELSR(config-if)#ip vrf forwarding A1
R-G-N-4-ELSR(config-if)#ip address 1.1.1.1 255.255.255.252
R-G-N-4-ELSR(config-if)#exit
R-G-N-4-ELSR(config)#router bgp 65561
R-G-N-4-ELSR(config-router)#address-family ipv4 vrf A1

R-G-N-4-ELSR(config-router-af)#neighbor 1.1.1.2 remote-as 64561
…
R-G-N-6-ELSR#configure terminal
R-G-N-6-ELSR(config)#interface Loopback0
R-G-N-6-ELSR(config-if)#ip address 30.30.30.30 255.255.255.255
R-G-N-6-ELSR(config-if)#exit
R-G-N-6-ELSR(config)#interface Ethernet0/0
R-G-N-6-ELSR(config-if)#ip address 5.5.5.2 255.255.255.252
R-G-N-6-ELSR(config-if)#mpls ip
R-G-N-6-ELSR(config-if)#no shutdown
R-G-N-6-ELSR(config-if)#exit
R-G-N-6-ELSR(config)#router eigrp 1
R-G-N-6-ELSR(config-router)#network 5.5.5.0 0.0.0.3
R-G-N-6-ELSR(config-router)#network 30.30.30.30 0.0.0.0
R-G-N-6-ELSR(config-router)#exit
R-G-N-6-ELSR(config)#router bgp 65561
R-G-N-6-ELSR(config-router)#neighbor 10.10.10.10 remote-as 65561
R-G-N-6-ELSR(config-router)#neighbor 10.10.10.10 update-source Loopback0
R-G-N-6-ELSR(config-router)#address-family vpnv4
R-G-N-6-ELSR(config-router-af)#neighbor 10.10.10.10 activate
R-G-N-6-ELSR(config-router-af)#exit
R-G-N-6-ELSR(config)#ip vrf A2
R-G-N-6-ELSR(config-vrf)#rd 2:1
R-G-N-6-ELSR(config-vrf)#route-target both 2:1
R-G-N-6-ELSR(config-vrf)#exit
R-G-N-6-ELSR(config)#interface Serial1/0
R-G-N-6-ELSR(config-if)#ip vrf forwarding A2
R-G-N-6-ELSR(config-if)#ip address 6.6.6.1 255.255.255.252
R-G-N-6-ELSR(config-if)#exit
R-G-N-6-ELSR(config)#router bgp 65561
R-G-N-6-ELSR(config-router)#address-family ipv4 vrf A2
R-G-N-6-ELSR(config-router-af)#neighbor 6.6.6.2 remote-as 64562
…
R-G-N-5-LSR#configure terminal
R-G-N-5-LSR(config)#interface Loopback0
R-G-N-5-LSR(config-if)#ip address 20.20.20.20 255.255.255.255
R-G-N-5-LSR(config-if)#exit
R-G-N-5-LSR(config)#interface Ethernet0/0
R-G-N-5-LSR(config-if)#ip address 4.4.4.1 255.255.255.252
R-G-N-5-LSR(config-if)#mpls ip

```
R-G-N-5-LSR(config-if)#no shutdown
R-G-N-5-LSR(config-if)#exit
R-G-N-5-LSR(config)#interface Ethernet1/0
R-G-N-5-LSR(config-if)#ip address 5.5.5.1 255.255.255.252
R-G-N-5-LSR(config-if)#mpls ip
R-G-N-5-LSR(config-if)#no shutdown
R-G-N-5-LSR(config-if)#exit
R-G-N-5-LSR(config)#router eigrp 1
R-G-N-5-LSR(config-router)#network 4.4.4.0 0.0.0.3
R-G-N-5-LSR(config-router)#network 5.5.5.0 0.0.0.3
R-G-N-5-LSR(config-router)#network 20.20.20.20 0.0.0.0
…
R-G-N-7-CE#configure terminal
R-G-N-7-CE(config)#interface Ethernet0/0.7
R-G-N-7-CE(config-subif)#encapsulation dot1Q 7
R-G-N-7-CE(config-subif)#ip address 192.168.46.254 255.255.255.0
R-G-N-7-CE(config-subif)#exit
R-G-N-7-CE(config)#interface Ethernet0/0
R-G-N-7-CE(config-if)#no shutdown
R-G-N-7-CE(config-if)#exit
R-G-N-7-CE(config)#interface Serial1/0
R-G-N-7-CE(config-if)#ip address 6.6.6.2 255.255.255.252
R-G-N-7-CE(config-if)#exit
R-G-N-7-CE(config)#ip route 0.0.0.0 0.0.0.0 Serial1/0
R-G-N-7-CE(config)#router bgp 64562
R-G-N-7-CE(config-router)#network 192.168.46.0
R-G-N-7-CE(config-router)#neighbor 6.6.6.1 remote-as 65561
…
```

Результати виконання команд моніторингу та діагностики роботи протоколу маршрутизації MPLS для розглянутого прикладу

З метою перегляду інформації про параметри інтерфейсів та роботу протоколу маршрутизації OSPF для розглянутого прикладу використано команди моніторингу та діагностики роботи **show mpls forwarding-table**. Результати роботи цих команд для маршрутизаторів наведено відповідно на рис. 3–6.

```
R-45-6-4-ELSR#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  5.5.5.0/30       0             Et0/0      4.4.4.1
17         Pop Label  20.20.20.20/32   0             Et0/0      4.4.4.1
18         No Label   192.168.45.0/24[V]   \
                                       0             Se1/0      point2point
R-45-6-4-ELSR#
```

Рис. 3. Результат роботи команди show mpls forwarding-table
на маршрутизаторі R-G-N-4-ELSR

```
R-45-6-4-ELSR#ping vrf A1 192.168.45.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.45.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/9 ms
R-45-6-4-ELSR#
```

Рис. 4. Результат виконання команди ping на маршрутизаторі R-G-N-4-ELSR

```
WS-1> ping 192.168.46.1

84 bytes from 192.168.46.1 icmp_seq=1 ttl=59 time=37.921 ms
84 bytes from 192.168.46.1 icmp_seq=2 ttl=59 time=24.991 ms
84 bytes from 192.168.46.1 icmp_seq=3 ttl=59 time=28.922 ms
84 bytes from 192.168.46.1 icmp_seq=4 ttl=59 time=19.748 ms
84 bytes from 192.168.46.1 icmp_seq=5 ttl=59 time=28.058 ms

WS-1>
```

Рис. 5. Результат виконання команди ping на робочій станції WS-1

```
WS-1> trace 192.168.46.1
trace to 192.168.46.1, 8 hops max, press Ctrl+C to stop
 1   192.168.45.254   1.389 ms  1.226 ms  1.083 ms
 2   1.1.1.1   9.321 ms  9.455 ms  8.653 ms
 3   4.4.4.1   24.396 ms  19.780 ms  29.473 ms
 4   6.6.6.1   20.039 ms  19.751 ms  19.589 ms
 5   6.6.6.2   19.867 ms  19.717 ms  19.444 ms
 6   *192.168.46.1   19.759 ms (ICMP type:3, code:3, Destination port unrea

WS-1>
```

Рис. 6. Результати виконання команди **tracert** на робочій станції WS-1

Завдання на лабораторну роботу

1. У середовищі віртуальної мережевої лабораторія eve.ztu.edu.ua створити проєкт мережі (рис. 11). Для побудованої мережі заповнити описову таблицю, яка аналогічна табл. 2

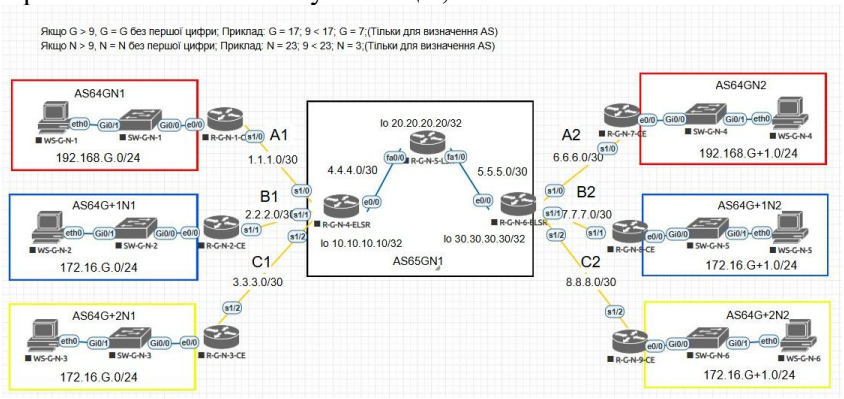


Рис. 7. Схема мережі

2. Розробити схему адресації пристроїв мережі. Для цього використовувати дані, що вказані в проєкті. Результати навести у вигляді таблиці, яка аналогічна табл. 3.

3. На маршрутизаторах мережі налагодити функціонування технології MPLS. Провести налаштування VRF-екземплярів та організувати сегментацію мережі відповідно до індивідуального варіанта.

4. Налаштувати протокол BGP для взаємодії між автономними системами відповідно до топології мережі. Забезпечити обмін маршрутами та коректну маршрутизацію між VRF через MPLS-домен.

5. Дослідити особливості отримання службової та діагностичної інформації протоколу MPLS та VRF за допомогою відповідних команд моніторингу та відлагодження.

6. Дослідити процеси передачі даних між вузлами різних VRF та автономних систем. У разі відсутності зв’язку визначити причини порушення та усунути їх.

Таблиця 4

Варіанти завдань для налаштування MPLS VPN з параметрами протоколів маршрутизації та RD для VRF

№ варіанту	Протокол маршрутизації	RD RF_A	RD RF_B	RD RF_C
Не парні	RIP	2:1	3:1	4:1
Парні	OSPF	4:1	5:1	6:1

Контрольні питання

1. Що таке MPLS VPN?
2. Основні елементи MPLS.
3. Що таке LSR, їх поділ.
4. Що таке FEC?
5. Що таке LDP?
6. Що таке LSP?
7. Заголовок MPLS.
8. Переваги використання MPLS.
9. Особливості технології L2 MPLS VPN.
10. Що таке VRF, його складові.
11. Параметри VRF.
12. Призначення протоколу BGP.
13. Які таблиці формуються при використанні технології MPLS?
14. Для чого призначена команда show mpls l2transport vc
15. Для чого призначена команда show mpls forwarding-table
16. Для чого призначена команда show ip route vrf, її синтаксис.

СПИСОК ЛІТЕРАТУРИ

1. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 334 с.

2. Буров Є.В. Комп'ютерні мережі. Підручник. Том 2. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 204 с.

3. Микитишин А.Г. Комп'ютерні мережі. Книга 1. Навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник – Львів, «Магнолія 2006», 2013. – 256 с.

4. Микитишин А.Г. Комп'ютерні мережі. Книга 2. Навчальний посібник. / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2013. – 328 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. – 1444 p.

7. Одом Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICNDl 100-101; акад. изд. / пер. с англ. Уэнделл Одом. – М. : ООО „И.Д. Вильямс", 2015. – 896 с.

8. Одом Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация, акад. изд. / пер. с англ. Уэнделл Одом. – М. : ООО „И.Д. Вильямс", 2015. – 736 с.

9. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. – 6-е изд. / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2020. – 1008 с.

10.Навчальний курс CCNAv7: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

11.Навчальний курс CCNAv7: Switching, Routing, and Wireless Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.

12.Навчальний курс CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс] – Режим доступу: www.netacad.com.

13.Навчальний курс CCNA Routing and Switching: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

14.Навчальний курс CCNA Routing and Switching: Routing and Switching Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.

15.Навчальний курс CCNA Routing and Switching: Scaling Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

16.Навчальний курс CCNA Routing and Switching: Connecting Networks [Електронний ресурс] – Режим доступу: www.netacad.com.

Навчально-методичне видання

ГЛОБАЛЬНІ МЕРЕЖІ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
ДЛЯ ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

Підготували
Дячук Ольга Юріївна
Єфіменко Андрій Анатолійович
Колощук Марія Сергіївна

Редактор
Комп'ютерне верстання – **А. А. Єфіменко**

Свідоцтво про реєстрацію № 4 від 12 червня 2025 року
Підписано до друку 12.06.25 Формат 60×84/16.
Ум. друк. арк. 192. Зам. __ офс.

Безкоштовно

Друкарня Державного університету «Житомирська політехніка»