

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту корпоративної
IPv4/IPv6 мережі побудованої на базі MPLS VPN»

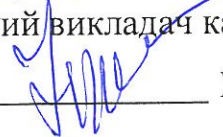
Виконав студент 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»

 Владислав ФОМІН

Керівник: старший викладач кафедри КІ та КБ

 Олександра ПОКОТИЛО

Рецензент: старший викладач кафедри КІ та КБ

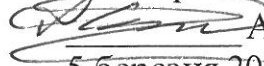
 Ігор ФАЛЬКОВСЬКИЙ

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Фомін Владислав Васильович

Тема роботи: «Проект підсистеми захисту корпоративної IPv4/IPv6 мережі
побудованої на базі MPLS VPN»

затверджена Наказом університету від 5 березня 2024 р. № 98

Термін здачі студентом закінченої роботи 9 червня 2024 р.

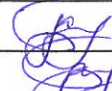
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Топологія мережі; підсистема захисту корпоративної IPv4/IPv6 мережі;
налагоджена технологія MPLS VPN

Обладнання та програмне забезпечення:

1. Маршрутизатори Cisco 7200 Series та Cisco 3745 Series
2. Комутатор Cisco Catalyst 2960
3. Операційні системи Windows 7, Kali Linux
4. Мережевий емулятор GNS3
5. Програмне забезпечення TFTPД32

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О.А.	05.03.2024 	05.03.2024 
2	Покотило О.А.	26.04.2024 	26.04.2024 
3	Покотило О.А.	13.05.2024 	13.05.2024 

Студент  Владислав ФОМІН

Керівник  Олександра ПОКОТИЛО

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	05.03.2024 – 10.03.2024	
2	Аналіз літературних джерел	12.03.2024 – 15.03.2024	
3	Аналіз об'єкта дослідження	16.03.2024 – 22.03.2024	
4	Постановка задачі дослідження	24.03.2024 – 26.03.2024	
5	Розробка структурної моделі	27.03.2024 – 31.03.2024	
6	Розрахунок параметрів адресації	01.04.2024 – 05.04.2024	
7	Вибір технології для реалізації	06.04.2024 – 11.04.2024	
8	Розробка КМ	13.04.2024 – 26.04.2024	
9	Налаштування мережі	29.04.2024 – 17.04.2024	
10	Адміністрування мережі	20.05.2024 – 31.05.2024	
11	Перевірка працездатності	03.06.2024 – 07.06.2024	
12	Оформлення пояснювальної записки	05.06.2024 – 09.06.2024	
13	Оформлення презентації	09.06.2024 – 10.06.2024	
14	Захист		

Студент  Владислав ФОМІН

Керівник  Олександра ПОКОТИЛО

АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи на тему «Проект підсистеми захисту корпоративної IPv4/IPv6 мережі побудованої на базі MPLS VPN» складається зі вступу, трьох розділів, висновку та списку використаної літератури.

Текстова частина викладена на 68 сторінках друкованого тексту. Пояснювальна записка має 70 сторінку та додаток на 37 сторінок. Список використаних джерел містить 13 найменувань і займає 2 сторінки. В роботі наведено 46 рисунків та 7 таблиць. Загальний обсяг роботи 107 сторінок.

У першому розділі визначено теоретичні аспекти функціонування технологій та протоколів побудови захищених корпоративних мереж. А саме таких технологій: MPLS, VRF, BGP, VPN та IPv4/IPv6.

У другому розділі проведено проектування захищеної корпоративної мережі та розробка параметрів IP-адресації, а також проведено вибір прикладних служб та сервісів, і спроектовано підсистеми захисту.

У третьому розділі проведено вибір обладнання, здійснено побудову, налагодження та тестування проєктованої корпоративної мережі.

Висновок містить в собі результати про виконану роботу при дослідженні та проєктуванні захищеної корпоративної IPv4/IPv6 мережі побудованої на базі MPLS VPN.

Ключові слова: CISCO, КОРПОРАТИВНА МЕРЕЖА, ЗАХИСТ, MPLS VPN, IPV6.

					ККІКБ.КР.Б – 125 – 20 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Фомін В.В.		14.06	Проект підсистеми захисту корпоративної IPv4/IPv6 мережі побудованої на базі MPLS VPN	Літ.	Арк.	Аркуші
Керівник		Покотило О.А.		17.06			4	61
Реценз.		Фальковський І.Г.						
Н. контр.		Покотило О.А.		17.06		ФІКТ Гр. КБ-20-1		
Затверд.		Сфіменко А.А.		17.06				

ANNOTATION

The explanatory note to the qualification work on the topic ‘Project of the corporate IPv4/IPv6 network security subsystem using MPLS VPN technology’ consists of an introduction, three chapters, a conclusion and a list of references.

The text part is set out on 68 pages of printed text. The explanatory note has 70 pages and an appendix of 37 pages. The list of references includes 13 titles and occupies 2 pages. The paper contains 46 figures and 7 tables. The total volume of the paper is 107 pages.

The first chapter defines the theoretical aspects of the functioning of technologies and protocols for building secure corporate networks. Namely, the following technologies: MPLS, VRF, BGP, VPN, and IPv4/IPv6.

The second section describes the design of a secure corporate network and the development of IP addressing parameters, as well as the selection of application services and services, and the design of security subsystems.

In the third section, we selected the equipment, built, configured, and tested the designed corporate network.

The conclusion contains the results of the work performed in the research and design of a secure corporate IPv4/IPv6 network using MPLS VPN.

Keywords: CISCO, CORPORATE NETWORK, SECURITY, MPLS VPN, IPV6.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ (ПРИНЦИПИ ПОБУДОВИ ТА) ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЙ ТА ПРОКОЛІВ ПОБУДОВИ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ.....	10
1.1. Корпоративна мережа. Її особливості та відмінності від інших типів мереж	10
1.2. Особливості IPv6	12
1.3. Мультипротокольна комутація міток (MPLS).....	15
1.4. Віртуальна маршрутизація та переадресація (VRF)	21
1.5. Протокол граничного шлюзу (BGP).....	23
1.6. Відмінності MPLS від інших альтернатив.....	25
РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ....	31
2.1. Проєктування фізичної та логічної (L2) топології мережі	31
2.2. Проєктування логічної (L3) топології мережі та розробка системи IP-адресації.....	33
2.3. Проєктування служб та сервісів прикладного рівня.....	35
2.4. Проєктування підсистеми мережного захисту	37
РОЗДІЛ 3. ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ ПРОЄКТОВАНОЇ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ.....	39
3.1. Вибір обладнання та ОС пристроїв для розробленого проєкту мережі....	39
3.2. Побудова та налагодження спроєктованої мережі	45
3.3. Тестування роботи побудованої локальної мережі	56
ВИСНОВКИ.....	68
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	69
ДОДАТКИ.....	71

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MPLS – Мультипротокольна комутація міток

VPN – Віртуальна приватна мережа

CE – Маршрутизатор користувача, що підключається до PE.

PE – Маршрутизатор провайдера, що з'єднує маршрутизатор користувача з ядром MPLS.

P – Маршрутизатор ядра MPLS.

LSR – Маршрутизатор з комутацією міток

LDP – Протокол розподілу міток

LSP – Пакет стану зв'язку

VRF – Віртуальна маршрутизація та переадресація

LAN – Локальна мережа

VLAN – Віртуальна локальна мережа

BGP – Протокол прикордонного шлюзу

MP-BGP – Багатопротокольний BGP

IP – Інтернет-протокол; IPv4/IPv6 – версії, 4 та 6 відповідно

RD – Розпізнавачі маршрутів

AS – Автономна система

CIDR – Безкласова міждоменна маршрутизація

QoS – Якість обслуговування

LFIB – Інформаційна база переадресації міток

VLSM – Маска підмережі змінної довжини.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми. У сучасних умовах постійного розвитку інформаційних технологій і зростання кількості інформаційних систем у підприємствах виникає досить важлива проблема: “Як забезпечити захист на надійсність цієї інформаційною системи?”. Ця проблема є ще більш актуальною для корпоративних мереж, адже вони використовуються для пересилання конфіденційної інформації.

На сьогоднішній день існує багато методів і технологій за допомогою яких можна реалізовувати ефективний та надійний захист корпоративної мережі, але однією з найбільш багатообіцяючих технологій є багато протокольна комутація міток з використанням віртуальних приватних мереж (MPLS VPN). MPLS VPN дозволяє нам створювати приватні мережі, які встановлюють захищений та надійний канал зв'язку між корпоративними ресурсами, незалежно від їхнього фізичного розташування. Завдяки своїм перевагам MPLS VPN широко використовується у реалізації корпоративних комп'ютерних мереж.

Також однією з актуальних проблем є використання IPv4. При розробці IPv4 вважалося, що ці IP-адреси ніколи не закінчатся, але з розвитком технологій та Інтернету ми зіштовхнулися з проблемою нестачі IP-адрес.

Вирішити цю проблему покликана наступна ітерація Інтернет-протоколу – IPv6. На відміну від IPv4, що використовує 32-бітні адреси, IPv6 використовує 128-бітові адреси, що мають набагато більший адресний простір. Це покликано вирішити проблему виснаження IP-адрес, яка стає все більш гострою зі зростанням кількості підключених до інтернету пристроїв. Також IPv6 є більш захищеним протоколом, адже він має вбудовану підтримку IPsec, протоколу безпеки, що забезпечує шифрування та автентифікацію даних. IPv6 розроблявся з урахуванням майбутніх технологій, таких як Інтернет речей та мобільний широкосмуговий доступ, що робить його більш гнучким та масштабованим, якщо порівнювати з IPv4. IPv6 пропонує значні переваги над IPv4, що робить його необхідним для майбутнього розвитку Інтернету. Зростаюча потреба в

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

більшій кількості IP-адрес, покращеній безпеці та ефективності мережі робить перехід на IPv6 неминучим.

Мета дослідження. Метою даної роботи є дослідження та проектування підсистеми захисту корпоративної IPv4/IPv6 мережі побудованої на базі MPLS VPN для можливості її використання у реальному житті.

Завдання роботи. Для того щоб досягти поставленої мети необхідно виконати такі завдання як:

- Провести аналіз існуючих методів та технологій захисту корпоративних мереж.
- Дослідити та вивчити принципи роботи технології MPLS VPN.
- Зпроектувати архітектуру підсистеми захисту корпоративної мережі.
- Виконати вибір апаратури та програмного забезпечення для реалізації даної мережі.
- Провести тестування та перевірити правильність налаштувань реалізованої корпоративної мережі.

Об'єкт дослідження. У даній кваліфікаційній роботі об'єктом дослідження є корпоративна IPv4/IPv6 мережа, методи її проектування та реалізації.

Предмет дослідження. Предметом дослідження є використання технології MPLS VPN у процесі розробки підсистеми захисту корпоративної IPv4/IPv6 мережі.

Методи дослідження. У даній кваліфікаційній роботі будуть використані такі методи дослідження як: аналіз літературних джерел, моделювання корпоративної мережі, експериментальні дослідження та реалізації змодельованої мережі.

Практичне значення. Результати даної кваліфікаційної роботи можуть бути використані як приклад налаштування MPLS VPN та реалізації підсистеми захисту корпоративної IPv4/IPv6 мережі на підприємствах різних галузей.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

**РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ (ПРИНЦИПИ ПОБУДОВИ
ТА) ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЙ ТА ПРОКОЛІВ
ПОБУДОВИ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ**

1.1. Корпоративна мережа. Її особливості та відмінності від інших типів мереж

Будучи цифровою основою великої організації, корпоративна мережа об'єднує людей, пристрої та ресурси на великій географічній території. Це не просто комп'ютерна мережа, а складна екосистема, розроблена для забезпечення ефективності, масштабованості, надійності та безпеки.

Корпоративна мережа є більш географічно розподіленою і включає в себе ряд інших типів мереж і інші технологічні рівні, ніж локальна мережа (LAN), яка обслуговує лише одну будівлю.

На рисунку 1.1 показано можливу структуру корпоративної мережі.

Enterprise WAN Network

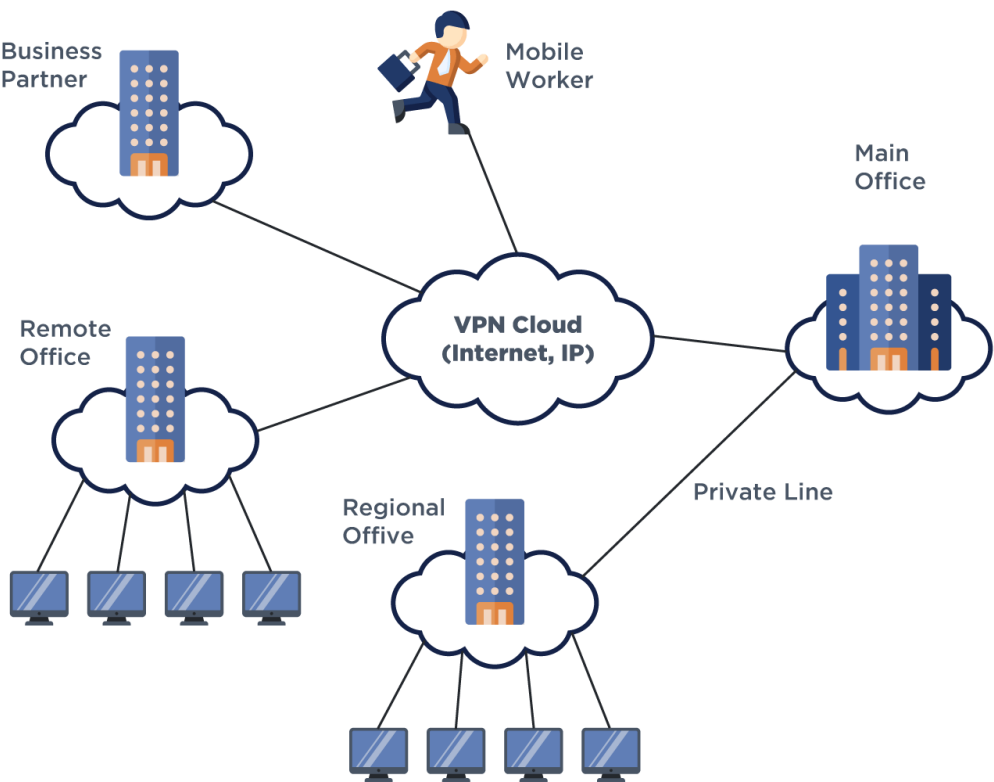


Рис. 1.1. Приклад корпоративної мережі

Це масштабна мережа, яка може з'єднувати навіть віддалені офіси між континентами, охоплюючи при цьому всі внутрішні мережі та пристрої. Вона складається з взаємопов'язаних локальних мереж (LAN), глобальних мереж (WAN), бездротових мереж (WLAN) та хмарних мереж.

Основними відмінностями від інших типів мереж можна назвати її розмір та складність, більший акцент на безпеку, прискіпливіші вимоги до управління та продуктивності, та масштабованість.

На відміну від базових домашніх мереж, безпека тут має особливе значення, адже необхідно забезпечити захист внутрішніх даних і ресурсів. Для реалізації захисту корпоративної мережі застосовуються суворі заходи безпеки, наприклад: брандмауери, контроль доступу та шифрування конфіденційних даних.

Для цієї масштабної мережі необхідно забезпечити високу продуктивність і мінімізувати будь які затримки, адже нею передаються дуже великі обсяги даних, а також вона може мати вимогливі застосунки. Найбільш важливою характеристикою для безперервності бізнесу є висока продуктивність і надійність, адже його потреби значно перевищують задачі звичайної локальної мережі, таких як наприклад перегляд веб-сторінок або обмін файлами.

Ще на етапі планування даної мережі необхідно взяти до уваги її масштабованість і зарання пристосувати її до можливого розширення та потреб бізнесу, за допомогою легкого додавання нових користувачів, пристроїв або додатків. Така мережа повинна адаптуватися до зростаючої організації, на відміну від статичних мереж у менших середовищах.

Також корпоративна мережа повинна мати централізоване керування – це уніфіковані інструменти управління, що контролюють всю мережу для ефективного її моніторингу, усунення несправностей та обслуговування. На відміну від менших мереж, якими легко керувати на локальному рівні, централізоване управління має вирішальне значення для підтримки складної мережі.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Отже, корпоративна мережа - це джерело сучасного бізнесу, що забезпечує безперебійну роботу, зв'язок і потік даних в усій організації. Її унікальні характеристики і складність відрізняють її від інших типів мереж, вимагаючи спеціалізованого дизайну, технологій і управління для оптимальної продуктивності і безпеки.

1.2. Особливості IPv6

У мережі, що складається з мільярдів цифрових пристроїв, підключених до Інтернету, саме ваша IP-адреса повідомляє нам, хто ви і де ви знаходитесь.

Мережеву комунікацію забезпечують саме протоколи мережевого рівня, такі як IPv6, або Інтернет-протокол версії 6. Робоча група з розробки інтернету (IETF) створила IPv6 у грудні 1998 року на заміну IPv4 у зв'язку з експоненціальним зростанням глобальної бази користувачів інтернету.

IPv6 – це стандарт адрес Інтернет-протоколу (IP) наступного покоління, що покликаний співіснувати з IPv4 і з часом замінити його. Комп'ютер, смартфон, датчик Інтернету речей, компонент домашньої автоматизації або будь-який інший пристрій підключений до Інтернету, потребує цифрової IP-адреси для зв'язку з іншими пристроями. Оригінальна схема IP-адресації, відома як IPv4, вичерпується через величезну кількість підключених пристроїв [1].

Найпоширенішим типом IP-адрес є IPv4, або "Інтернет протокол версії 4". Приклад IPv4-адреси виглядає наступним чином: 192.168.50.1.

IPv4-адреса складається з чотирьох чисел, кожне з яких містить від однієї до трьох цифр, кожне число відокремлюється однією крапкою (.). Всі адреси, які використовуються для надсилання та отримання даних через Інтернет, створюються за допомогою цього набору розділених чисел. Оскільки IPv4 використовує 32-бітну схему адресації, цей адресний простір може зберігати лише понад 4 мільярди адрес, що хоча і здається великим числом, але є недостатнім на сьогодні. Він вважається основним Інтернет-протоколом і забезпечує 94% від всього Інтернет-трафіку [1]. Спочатку передбачалося, що ці адреси ніколи не вичерпаються, але нинішня ситуація змушує звертатися до IPv6.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

Наступна ітерація стандарту IP відома як Інтернет-протокол версії 6 (IPv6).

IPv6 адреса складається з восьми груп по чотири шістнадцяткові цифри. Ось приклад IPv6-адреси: 2001:0db8:8a2e:0270:5221 3001:0da5:72a5

Ця нова версія IP-адрес вводиться саме для того щоб задовільнити зростаючий попит на IP-адреси. Він пропонує 2^{128} унікальних адрес зі 128-бітним адресним простором [1]. Це дуже велике число, можна навіть сказати, що ці IP-адреси ніколи не закінчатся, або принаймні їх вистачить на дуже довгий час.

Нам потрібно впровадити IPv6, щоб продовжувати розвиватися і додавати нові пристрої та послуги в Інтернеті.

Є такі типи IPv6-адрес [2]:

- Одноадресні (Unicast addresses) – вказує лише на один інтерфейс. Пакет рухається від одного хоста до хоста призначення, коли він надсилається на одноадресну адресу призначення.
- Багатоадресні адреси (Multicast addresses) – представляють групу IP-пристроїв і можуть використовуватися лише як адресат дейтаграми.
- Адреса будь-якої трансляції (Anycast addresses) – це особливий тип адрес. Це одна IPv6-адреса призначення до декількох інтерфейсів на різних пристроях по усій мережі. Будь який пристрій з цією адресою може отримувати відправлений на неї трафік.

Є такі переваги IPv6:

- IPv6 підтримує багатоадресну передачу замість широкомовної передачі в IPv4. Ця функція дозволяє надсилати потоки пакетів з високою пропускнуою здатністю (наприклад, мультимедійні потоки) на декілька пунктів призначення одночасно.
- В IPv6 вбудована функція IPSecurity, яка забезпечує конфіденційність і цілісність даних.
- Ефективність маршрутизації.
- Надійність.
- Найголовніше - це остаточне рішення для зростаючої кількості вузлів у глобальній мережі.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

- Пристрій самостійно розподіляє адреси.
- Можливість увімкнення простої агрегації префіксів, виділених для IP-мереж; це економить пропускну здатність, дозволяючи одночасну передачу великих пакетів даних.

Але є і такі недоліки:

- Через широке використання IPv4 в даний час знадобиться тривалий період для повного переходу на IPv6.
- Пристрої з IPv4 та IPv6 не можуть безпосередньо взаємодіяти один з одним, оскільки міжпротокольний зв'язок заборонений.
- IPv6 не може виконуватися на комп'ютерах, що підтримують лише IPv4, оскільки він недоступний в системах IPv4.

Також у таблиці 1.1. наведено приклад відмінностей між IPv6 та IPv4

Таблиця 1.1.

Відмінності між IPv6 та IPv4

IPv6	IPv4
IPv6 має довжину адреси 128 біт	IPv4 має 32-бітну довжину адреси
Підтримує автоматичну та перенумеровану конфігурацію адрес	Підтримує ручну та DHCP конфігурацію адреси
Адресний простір IPv6 досить великий, він може створювати 2^{128} адрес	Він може генерувати 2^{32} адрес
Представлення адреси IPv6 у шістнадцятковому форматі	Представлення адреси IPv4 у десятковій системі числення
В IPv6 поле контрольної суми недоступне	Для IPv4 доступне поле контрольної суми
IPv6 має фіксований заголовок довжиною 40 байт	IPv4 має заголовок довжиною 20-60 байт.
IPv6 не підтримує VLSM (маску підмережі змінної довжини).	IPv4 підтримує VLSM.

1.3. Мультипротокольна комутація міток (MPLS)

Мультипротокольна комутація міток (MPLS) - це технологія маршрутизації IP-пакетів. Завдяки цій технології IP-пакети маршрутизуються за допомогою міток, а не складних таблиць маршрутизації на маршрутизаторах, що, в свою чергу, прискорює доставку IP-пакетів.

Вона була розроблена у 1990-х роках і дозволила корпоративним мережам встановлювати високошвидкісні мережеві з'єднання. До того, як у 2001 році Робоча група з розробки інтернету (IETF) стандартизувала його як RFC 3031, протокол був приватною власністю [3].

Зазвичай, поки пакет не досягне місця призначення, він пересилається від одного маршрутизатора до іншого через загальнодоступний Інтернет. Однак MPLS надсилає пакети за вже визначеним мережевим маршрутом. Це означає, що пакети повторюють один і той самий маршрут, і через це маршрутизатору потрібно менше часу, щоб визначити, куди переслати кожен пакет. У мережевій моделі OSI MPLS функціонує між рівнями 2 і 3, або мережевим і канальним рівнями, відповідно [4]. Тому він також вважається протоколом рівня 2.5 [5].

MPLS функціонує дещо подібно до VPN: трафік від різних клієнтів відокремлюється один від одного. Хоч при цьому MPLS і не шифрує дані, як стандартна VPN, вона гарантує, що пакет, надісланий одним клієнтом, не може бути отриманий чужим клієнтом.

Заголовок MPLS, також відомий як протокол рівня 2.5 або shim-протокол, розташовується між заголовками рівня 2 і 3. Він зберігає масштабованість і динамічні можливості протоколів 3-го рівня, пересилаючи пакети зі швидкістю протоколів 2-го рівня. Цей протокол дозволяє економити час і ресурси, оскільки маршрутизаторам не потрібно відкривати заголовки пакетів 3-го рівня. Заголовок MPLS має довжину 32 біти і розділений на чотири частини [3]:

1. Перші 20 біт – мітка, яка визначає, куди пересилається пакет.
2. Наступні 3 біти використовуються для пріоритету якості обслуговування (QoS) і явного сповіщення про перевантаження (ECN), розширення

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

протоколу IP, яке дозволяє мережам справлятися з перевантаженням без втрати пакетів.

3. Наступний 1 біт – це поле "дно стека". Коли воно встановлене, це означає, що пакет досягнув кінця мережевого маршруту MPLS.
4. Останні 8 біт – це час життя пакету (TTL). Його значення зменшується на одиницю при кожному переході, щоб запобігти застряганню пакета в мережі.

Більш наглядно структуру заголовку MPLS наведено на рисунку 1.2.

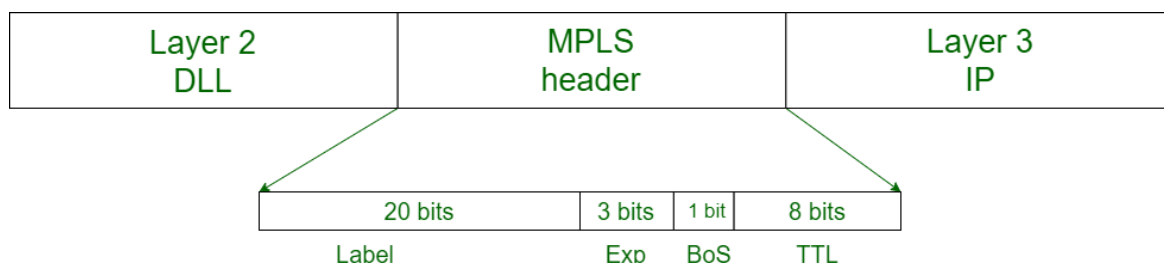


Рис. 1.2. Заголовок MPLS

Основною метою впровадження MPLS підвищення продуктивності та надійності мережевого трафіку. Також є і переваги з точки зору безпеки: незважаючи на те, що за замовчуванням посилення MPLS не шифруються, вони зазвичай ізольовані від решти мережі, утворюючи окремий віртуальний тунель, який функціонує подібно до віртуальної приватної мережі (VPN).

У MPLS переадресація виглядає наступним чином: після отримання IP-пакетів від CE-маршрутизатора, LSR інкапсулюють кадри 2-го рівня, додаючи заголовок MPLS між 3-м і 2-м рівнями. Ця функція, яка називається "багатопротоальною", дозволяє LSR підтримувати прийом пакетів, що містять кадри різних протоколів, включаючи Frame Relay, Metro Ethernet тощо.

Основою переадресації MPLS є мітка IP-пакета. Протокол розподілу міток (Label Distribution Protocol, LDP) - це протокол, який керує цією міткою. Як і будь-який інший маршрутизатор, кожен LSR повинен спочатку вивчити свої маршрути. Це вивчення маршруту починається на PE-маршрутизаторах [5]. PE-маршрутизатор отримує інформацію про маршрути до інших підмереж від CE-маршрутизаторів. Для наочності уявимо, що CE-маршрутизатор показує PE-

маршрутизатору PE1 шлях до підмережі підмережі 1. Тепер PE1 ставить мітку на пакет, пересилає його до найближчого LSR і дає йому вказівку переслати його мені, якщо він прийде з адресою призначення в підмережі 1.

Потім LSR проходить цю процедуру ще раз. Інформаційна база переадресації міток (Label Forwarding Information Base, LFIB) отримує цю інформацію від LSR, оскільки саме таким чином він вивчає маршрути [5]. Тепер, вивчивши мітки і LFIB, LSR може просто переслати IP-пакет на будь-який PE-маршрутизатор, який отримує пакет з адресою призначення в підмережі 1.

Приклад як виглядає MPLS-мережа наведено у рисунку 1.3.

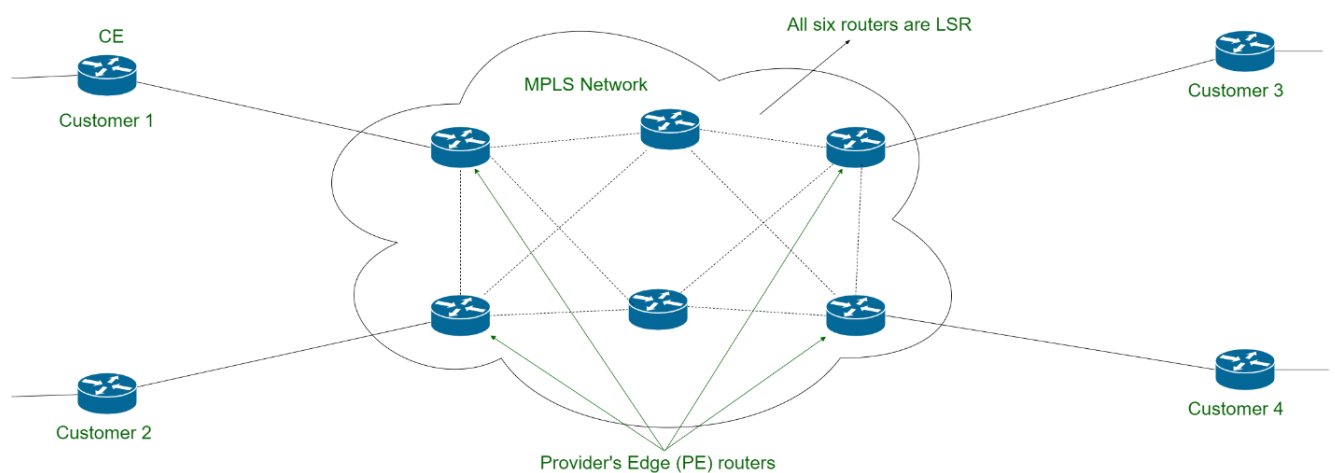


Рис. 1.3. MPLS-мережа

Механізм маршрутизації MPLS працює майже з усіма типами мережевих протоколів і каналів передачі, такими як IP (Internet Protocol), ATM (Asynchronous Transport Mode), Ethernet.

У телекомунікаційній мережі маршрутизатори називаються шляхами комутаторів з мітками (LSP) і використовуються для маршрутизації пакетів дейтаграм шляхом маркування кожного пакета при проходженні через них [6]. У мережі-приймачі кожен попередньо визначений шлях має мітку, прикріплену до нього. Приймач дейтаграми динамічно маркує пакет дейтаграми, щоб його можна було передати іншим приймачам. Це означає, що, на відміну від мереж з комутацією пакетів, контрольна мітка є вищою.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Мітки, що використовуються для комутації, у мережі MPLS слугують шляхами передачі, які створюються протоколами сигналізації. Ці шляхи спрямовують пакети даних і голосу до потрібного призначення у мережі.

Розглянемо наступний сценарій: якщо листоноша використовує автоматизовану конвеєрну сортувальну систему для пошуку і сортування посилок, скануючи штрих-код на верхній частині посилки, автоматизована обробка системи значно збільшить швидкість обробки і сортування посилок, завдяки чому вони будуть зберігатися довше і більш ефективно [5]. З іншої сторони, якщо пошта призначає листоношу для пошуку, сортування та перевірки кожної посилки, щоб з'ясувати адресу її одержувача, ручна робота тільки сповільнить процес. Саме тут LSP покращують швидкість і оптимізують процес передачі пакетів даних, дозволяючи кожному маршрутизатору швидко визначити, куди прямує пакет.

У мережі MPLS маршрутизатори обмінюються мітками пакетів даних, коли вони проходять через неї. Пакет перевіряється, класифікується і отримує мітку, коли він перетинає кордон магістралі MPLS. Після цього ці пакети направляються по заздалегідь встановленому шляху з комутацією міток (Label Switched Path, LSP) до наступного кроку [6]. Кожен маршрутизатор на цьому шляху використовує мітку, щоб визначити, куди переслати дейтаграму, коли пакет проходить через нього.

На рисунку 1.4. можна більш наочно побачити принцип роботи MPLS-мережі.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

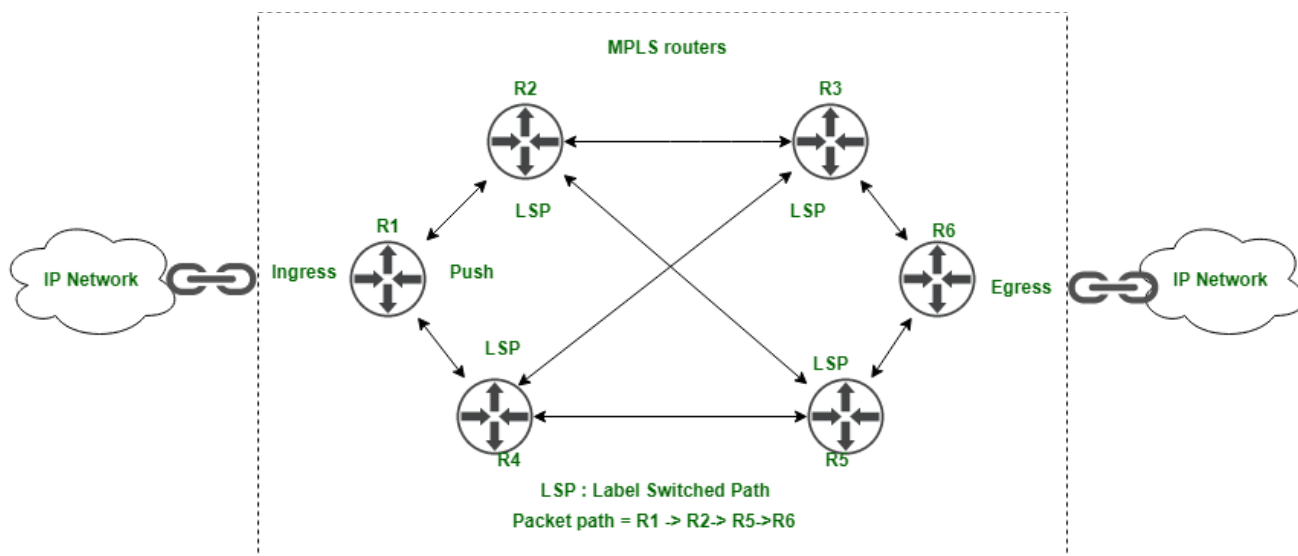


Рис. 1.4. Принцип роботи MPLS-мережі

Для розгортання MPLS VPN, необхідно здійснити конфігурацію VRF, RD, LDP і MP BGP.

Віртуальна маршрутизація і переадресація (Virtual Routing and Forwarding, скорочено VRF) – це технологія, яка дозволяє маршрутизатору мати кілька екземплярів таблиці маршрутизації одночасно [7]. Ці таблиці маршрутизації співіснують на маршрутизаторі, але при цьому є сегментованими і незалежними одна від одної.

Розпізнавач маршрутів (Route Distinguisher, RD) – це спосіб визначення VPN маршруту в мережі MPLS. Він додає 8-байтне значення до префікса IPv4 для створення префікса VPNv4, який зазвичай називають адресою VPN-IPv4. Оскільки кожному клієнту присвоюється унікальний RD, їхні адреси гарантовано будуть унікальними. Отже, якщо у вас є клієнт А, який має адресний простір 10.0.0.0/24, і клієнт В, який також має адресний простір 10.0.0.0/24, додавання RD надає унікальність кожному з них. Номінально RD виглядає як 1:100.

BGP може бути дуже потужним протоколом і у реалізації MPLS VPN використовують цю перевагу. Цитата з RFC4577: “Багато постачальників послуг пропонують своїм клієнтам послуги віртуальної приватної мережі (VPN), використовуючи техніку, в якій прикордонні маршрутизатори клієнта (CE-

маршрутизатори) є маршрутизаторами прикордонних маршрутизаторів постачальника (PE-маршрутизаторів). Протокол прикордонного шлюзу (BGP) використовується для розподілу маршрутів клієнтів через магістральну IP-мережу провайдера, а багатопрокольна комутація міток (MPLS) використовується для тунелювання клієнтських пакетів через магістральну мережу провайдера.” Це відоме як "IP VPN на базі BGP/MPLS". Тут використовується VRF частина BGP, оскільки вона забезпечує можливість перерозподілу між BGP і визначеним клієнтським VRF. Зв'язок між PE і CE-маршрутизаторами може бути будь-яким обраним протоколом маршрутизації - RIP, OSPF, EIGRP, Static, BGP тощо, і – на основі визначеного RD – є можливість перерозподіляти маршрути між обраним протоколом і BGP VRF.

На рисунку 1.5. наведено наглядний приклад реалізації MPLS-мережі з використанням BGP VRF.

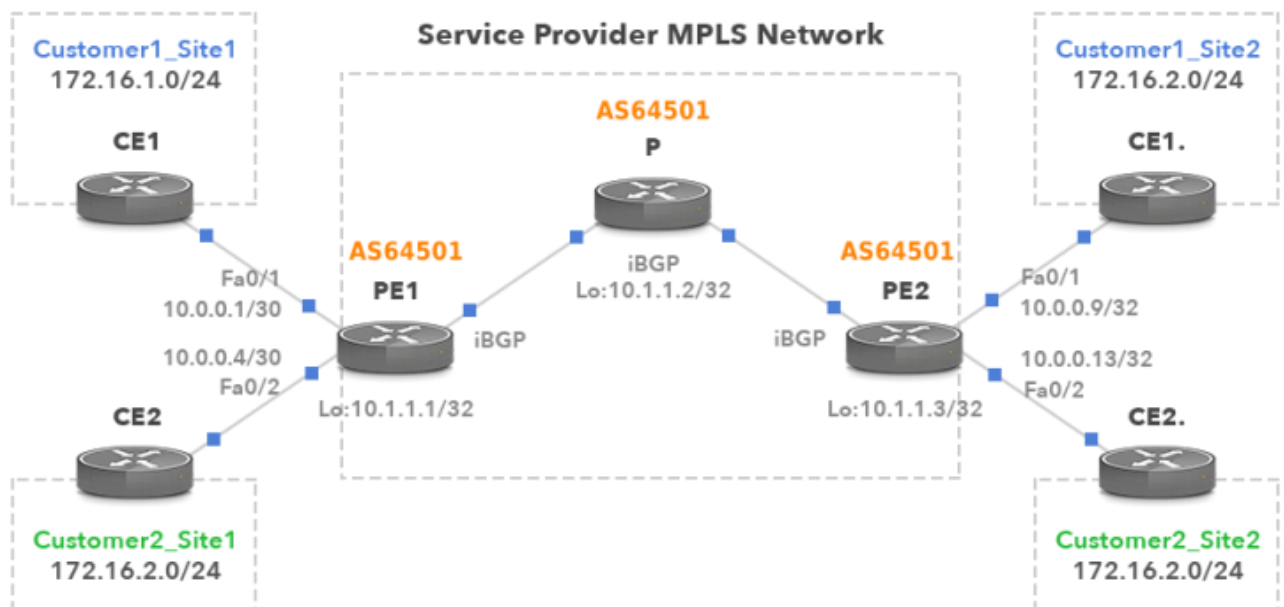


Рис. 1.5. Приклад реалізації MPLS-мережі

Хоча MPLS все ще широко використовується в корпоративних мережах, її використання як єдиного варіанту мережевого підключення йде на спад. Крім того, що інфраструктура MPLS є дорогою і складною в налаштуванні, вона є негнучкою, що ускладнює адаптацію до змін в організаційній структурі та додавання нових периферійних точок. У майбутньому MPLS все ще буде

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

використовуватися разом з іншими варіантами підключення, такими як широкосмуговий Інтернет і SD-WAN.

1.4. Віртуальна маршрутизація та переадресація (VRF)

Віртуальна маршрутизація і переадресація (VRF) - це технологія, яка використовується в мережевих маршрутизаторах Інтернет-протоколу (IP) і дозволяє декільком екземплярам таблиці маршрутизації існувати у віртуальному маршрутизаторі і працювати одночасно [7].

Завдяки розділенню мережевих шляхів без необхідності використання декількох пристроїв покращується зв'язок. VRF підвищує безпеку мережі, автоматично розділяючи трафік і усуваючи необхідність автентифікації та шифрування.

VRF часто використовуються інтернет-провайдерами для створення окремих віртуальних приватних мереж (VPN) для своїх клієнтів. Коли вона завершена, це називається маршрутизацією та переадресацією VPN.

VRF працює так як і логічний маршрутизатор. Однак VRF використовує лише одну таблицю VRF, тоді як логічний маршрутизатор може мати декілька таблиць маршрутизації.

VRF також потребує списку пристроїв, які можна використовувати для пересилання пакетів, таблиці пересилання, яка визначає наступну дію кожного пакета даних, і набору правил і протоколів маршрутизації, які визначають метод пересилання пакета. Ці таблиці зупиняють пересилання трафіку, який не повинен потрапляти за межі VRF-шляху.

Різницю між використанням VRF та його відсутністю наведено на рисунку 1.6.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

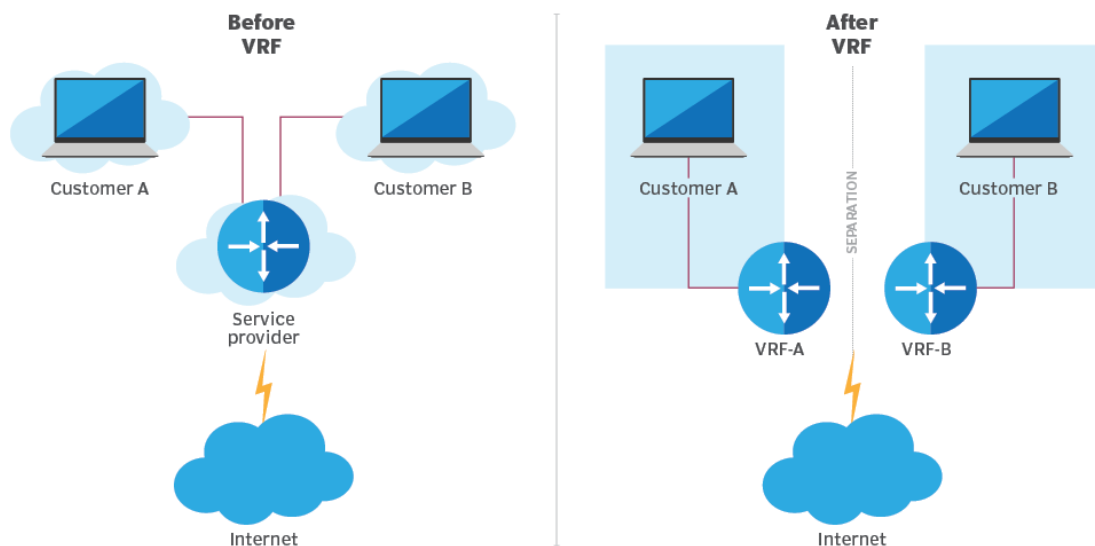


Рис. 1.6. Принцип роботи VRF

Використовуючи віртуальну маршрутизацію і переадресацію, на маршрутизаторі або комутаторі 3-го рівня можна налаштувати кілька екземплярів маршрутизації. Мета цього полягає в тому, щоб розділити клієнтський трафік і маршрутизацію, використовуючи одне і те ж обладнання.

Клієнтський трафік маршрутизується через фізичні інтерфейси або підінтерфейси з фільтрацією списків контролю доступу, щоб розділити трафік в ситуаціях, коли VRF не може бути використаний.

VRF стає все більш поширеним в центрах обробки даних, сервіс-провайдерах і корпоративних локальних мережах (LAN), які використовують багатопроколову комутацію міток (MPLS) і багатопроколовий прикордонний шлюзовий протокол (MP-BGP) [7].

Віртуальні локальні мережі (VLAN) і функції віртуального маршрутизатора (VRF) по суті однакові з точки зору віртуалізації. Їх можна порівняти з IP-рівнем протоколу управління передачею VLAN версії 3-го рівня [7]. Обидва екземпляри маршрутизації можуть мирно співіснувати один з одним, оскільки вони працюють незалежно один від одного.

Крім того, завдяки сегментації мережових шляхів без необхідності використання декількох маршрутизаторів покращується функціональність

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

мережі. Використовуючи VRF, один маршрутизатор може виглядати як кілька маршрутизаторів. Таким же чином, використовуючи VLAN, один комутатор може виглядати як кілька комутаторів.

BGP VRF пропонує додатковий контроль маршрутів трафіку, а також підтримку умовних оголошень з урахуванням BGP VRF для цих сімейств протоколів IP-адрес [8]:

- IPv4 Unicast
- IPv4 одноадресний VRF
- IPv6 одноадресний
- IPv6 одноадресний VRF

Зв'язок BGP між VRF та VRF на одному маршрутизаторі вмикається шляхом призначення ідентифікатора маршрутизатора BGP. Його можна призначити автоматично за допомогою режиму конфігурації сімейства адрес або вручну для кожного унікального VRF.

Організації можуть повторно використовувати простір IP-адрес між ізольованими доменами маршрутизації, використовуючи імена VRF. Оскільки кожен клієнт має унікальну IP-адресу VRF, підмережі, що перетинаються, ізольовані. Кожен маршрут за замовчуванням відрізняється від інших маршрутів, якщо використовувати вирішувач маршрутів, також відомий як RD.

1.5. Протокол граничного шлюзу (BGP)

Протокол граничного шлюзу (BGP) - це протокол, який використовується між провайдерами в різних мережах для обміну інформацією про маршрутизацію через Інтернет.

Будь-яка мережа в автономній системі може бути з'єднана за допомогою цього протоколу з використанням будь-якої топології. Все, що необхідно – це щоб в кожній автономній системі був мінімум один маршрутизатор з підтримкою BGP, який пов'язаний з мінімум одним BGP-маршрутизатором в іншій автономній системі. Обмін інформацією про доступність мережі між системами BGP є основною метою цього протоколу. BGP-маршрутизатори обмінюються

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

інформацією, а протокол прикордонного шлюзу використовує цю інформацію для створення графа автономних систем [8].

Характеристики протоколу прикордонного шлюзу (BGP):

- Основна роль BGP полягає в забезпеченні зв'язку між двома автономними системами.
- BGP підтримує парадигму Next-Хор.
- Координація між декількома BGP-спікерами в межах автономної системи.
- Оголошення BGP також включають інформацію про шлях, разом з досяжним пунктом призначення і наступною парою пунктів призначення.
- BGP може реалізовувати політики налаштовані адміністратором. Наприклад: маршрутизатор, на якому запущено BGP, можна налаштувати так, щоб він розрізняв маршрути, відомі в межах AS, і маршрути, відомі ззовні AS.
- Працює поверх TCP.
- BGP економить пропускну здатність мережі.
- BGP підтримує CIDR.
- BGP також підтримує налаштування безпеки.

BGP виконує 3 функції, які наведені нижче.

Перша функція полягає в початковому визначенні та автентифікації однорангового вузла. Обидва вузли встановлюють TCP-з'єднання і виконують обмін повідомленнями, що гарантує, що обидві сторони погодилися на зв'язок.

Друга функція в основному зосереджена на надсиланні негативної або позитивної інформації про доступність.

Третя функція перевіряє, чи правильно функціонують однорангові вузли та мережеве з'єднання між ними.

Функції управління маршрутною інформацією BGP:

- Кожен BGP зберігає інформацію про те, як досягти інших мереж.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

- Оновлення маршрутів: У цьому завданні використовуються спеціальні методи, щоб визначити, коли і як використовувати інформацію, отриману від однорангових маршрутизаторів, для належного оновлення маршрутів.
- Кожен BGP використовує інформацію в своїх базах даних маршрутів для вибору найкращих маршрутів до кожної мережі в загальній Інтернет-мережі.
- Кожен BGP-спікер регулярно ділиться інформацією з іншими BGP-маршрутизаторами про те, що йому відомо про різні мережі і способи зв'язку з ними.

1.6. Відмінності MPLS від інших альтернатив

MPLS та VPN:

Віртуальна приватна мережа, або VPN, - це різновид приватної мережі, яка існує лише віртуально. Віртуальна приватна мережа забезпечує підключення з віддалених місць до мережі організації за допомогою зашифрованої передачі даних. Деякі з найпоширеніших причин, чому люди використовують VPN – це захист від шпигунства через громадський Wi-Fi, обхід Інтернет-цензури або підключення до внутрішньої мережі підприємства з метою віддаленої роботи [9].

VPN використовують декілька стандартів шифрування, включаючи TripleDES, EAS і RSA. У VPN для маскуванню публічної IP-адреси користувача використовується приватна IP-адреса. Завдяки автентифікації відправника та криптографічному протоколу тунелювання вони гарантують конфіденційність і цілісність. VPN використовують ряд протоколів безпеки, включаючи LT2P, PPTP і Ipsec [10].

Переваги VPN:

- VPN, як правило, дешевша за MPLS, оскільки використовує вже існуючі Інтернет-з'єднання.
- VPN є гнучкою і може використовуватися з різними пристроями та операційними системами.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

- VPN можна масштабувати для підтримки великої кількості користувачів та пристроїв.
- VPN забезпечує віддалений доступ до мережі компанії, що дозволяє співробітникам працювати з будь-якого місця.
- VPN легко встановити та налаштувати, що робить її доступною для малого бізнесу та приватних осіб.

Недоліки VPN:

- Якщо VPN не налаштована належним чином, вона може бути вразливою до ризиків безпеки, залишаючи дані та мережі вразливими для хакерів.
- VPN може мати нижчу надійність, ніж MPLS, через залежність від загальнодоступного Інтернету, який схильний до перебоїв та інших проблем.
- VPN може мати нижчу продуктивність, ніж MPLS.

Переваги MPLS:

- MPLS забезпечує високу надійність і якість обслуговування, оскільки використовує виділені з'єднання, а не загальнодоступний Інтернет.
- MPLS забезпечує високу продуктивність і низьку затримку, оскільки використовує виділені з'єднання і не вимагає шифрування і дешифрування даних.
- MPLS можна масштабувати для підтримки великої кількості користувачів і трафіку.
- MPLS підтримує якість обслуговування (QoS), що дозволяє визначати пріоритети трафіку і управляти ним, щоб гарантувати, що критичні додатки отримують необхідну пропускну здатність і найнижчу затримку.
- MPLS забезпечує кращу безпеку, ніж VPN, оскільки він не схильна до тих же вразливостей, що і загальнодоступний Інтернет.

Недоліки MPLS:

- MPLS, як правило, дорожчий за VPN, оскільки вимагає виділених з'єднань.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

- MPLS менш гнучкий, ніж VPN, і може вимагати спеціалізованого обладнання або програмного забезпечення.
- MPLS може вимагати більше часу на впровадження, ніж VPN, через необхідність виділених з'єднань і спеціалізованого апаратного або програмного забезпечення.

Схожість:

- Обидві технології можна використовувати для створення захищених приватних мереж.
- Обидві технології можна використовувати для підключення географічно розподілених сайтів і віддалених працівників до центральної мережі.
- Обидві технології використовують шифрування для захисту даних під час передачі.
- Обидві технології можуть визначати пріоритети трафіку і забезпечувати якість обслуговування (QoS), щоб гарантувати, що критичні додатки отримують необхідну пропускну здатність і низьку затримку.
- Обидві технології можна використовувати для створення безпечного з'єднання через публічну мережу.

Для встановлення безпечних і приватних з'єднань між пристроями або мережами використовуються дві різні технології: MPLS і VPN. При встановленні безпечного з'єднання через Інтернет, VPN використовує шифрування і тунелювання, тоді як MPLS встановлює приватну мережу через загальну інфраструктуру. У той час як MPLS використовується для приватних мережевих з'єднань між двома або більше сайтами, VPN зазвичай використовується для віддаленого доступу [11].

Хоча технології MPLS і VPN часто розглядаються як конкуренти, вони також можуть доповнювати одна одну. Наприклад, гібридний хмарний бізнес може використовувати VPN для безпечного підключення своїх хмарних дата-центрів, а MPLS - для надійного з'єднання своїх фізичних локацій [3]. У такому випадку кожен ресурс пов'язаний з найкращою технологією. Недоліками є неузгодженість та підвищена складність інфраструктури.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

MPLS та підключення через публічний Інтернет:

І загальнодоступний Інтернет, і MPLS є основними варіантами підключення для підприємств. Інтернет є дешевшим варіантом, але має свої недоліки, тоді як MPLS пропонує більш надійне з'єднання за додаткову плату. І MPLS, і Інтернет-мережі підтримують повномасштабний міжсайтовий зв'язок і різні середовища 1-го рівня (наприклад, T1, DSL, Ethernet) [3].

Основні відмінності між MPLS і підключенням до Інтернету полягають у наступному:

- Підключення MPLS залежить від одного оператора, в той час як Інтернет є необмеженим і може передавати дані через різних операторів.
- Провайдери MPLS гарантують пріоритетність і доставку пакетів, а Інтернет – ні.
- MPLS є кращим варіантом для голосового та відеозв'язку, оскільки він надає пріоритет доставці пакетів.
- MPLS має визначену угоду про рівень обслуговування з високим рівнем сервісу, в той час як Інтернет SLA варіюються.
- MPLS є дорожчим, ніж підключення до Інтернету.
- MPLS вважається приватним і більш безпечним, ніж загальнодоступний Інтернет.

MPLS та IPsec:

Група протоколів під назвою IPsec використовується для створення захищених з'єднань між пристроями. Це сприяє безпеці даних, що передаються через загальнодоступні мережі. IPsec часто використовується для створення VPN-мереж. Він функціонує шляхом шифрування IP-пакетів і підтвердження їх походження [3].

Назва IPsec означає "безпека Інтернет-протоколу (IP)". Основний протокол маршрутизації, який використовується в Інтернеті, називається Інтернет-протокол. IPsec посилює цю процедуру за допомогою автентифікації та шифрування.

Порівняння між технологіями MPLS та IPsec наведено у таблиці 1.2.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

MPLS та SD-WAN:

Програмована глобальна мережа (SD-WAN) – це технологія, яка використовує концепцію програмно-визначених мереж для розподілу мережевого трафіку в глобальній мережі (WAN). SD-WAN автоматично визначає найефективніший спосіб маршрутизації трафіку додатків між філіями та центрами обробки даних на основі налаштованих політик [3].

Багато в чому SD-WAN можна розглядати як програмну абстракцію технології MPLS, яка може бути застосована до більш широких сценаріїв: Вона забезпечує безпечне приватне з'єднання, яке є агностичним до всіх видів зв'язку і провайдерів, а також враховує хмарні технології.

Порівняння між технологіями MPLS та SD-WAN наведено у таблиці 1.3.

Таблиця 1.2.

Порівняння MPLS та IPsec

	MPLS	IPsec
Вартість	MPLS вважається приватною мережею, яка не потребує шифрування.	IPsec вимагає наявності зашифрованого тунелю між кожними двома границями мережі, що збільшує вартість обладнання
Безпека	MPLS вважається безпечною, навіть якщо дані, що передаються через мережу MPLS, не зашифровані, оскільки вона базується на приватному каналі.	Дані IPsec VPN завжди зашифровані. Однак, через загальнодоступний Інтернет вони піддаються більшому ризику перехоплення та підслуховування.
Надійність	Лінії MPLS - це приватні мережі, які постачаються з чітким SLA, що фокусується на надійності та доступності як основній цінності послуги.	З'єднання IPsec залежать від інтернет-інфраструктури, а тому менш надійні і схильні до нестабільності.
Якість обслуговування (QoS)	MPLS дозволяє користувачам визначати пріоритетність певного трафіку в мережі.	IPsec також забезпечує QoS, але оскільки базовою інфраструктурою є Інтернет, розриви з'єднань є поширеною проблемою.

Таблиця 1.3.

Порівняння MPLS та SD-WAN

	MPLS	SD-WAN
Використання пропускної здатності (Bandwidth Use)	MPLS вимагає дорогих приватних каналів для масштабування доступної пропускної здатності.	Підключені до SD-WAN сайти можна легко модернізувати, додаючи нові посилення.
Зворотний зв'язок (Backhauling)	Кожна віддалена точка підключається через одне MPLS-з'єднання, що збільшує затримку і споживає цінну пропускну здатність MPLS.	SD-WAN може створювати динамічні прямі з'єднання між філіями, хмарними дата-центрами та Інтернетом.
Вартість	MPLS має високу вартість, оскільки покладається на приватну та виділену інфраструктуру.	SD-WAN знижує витрати, поєднуючи використання MPLS та Інтернету для побудови глобальної мережі.
Безпека	Мережі MPLS вважаються безпечними, оскільки вони базуються на інфраструктурі приватних каналів зв'язку.	SD-WAN використовує зашифрований зв'язок, оскільки дані передаються через публічний Інтернет.

Висновок до першого розділу: Протягом цього розділу було досліджено принципи роботи MPLS, порівняно MPLS з технологіями-аналогами, визначено різницю між використанням MPLS та звичайного VPN, досліджено технології, що застосовуються для реалізації MPLS VPN, а саме віртуальну маршрутизацію та переадресацію (VRF) та протокол граничного шлюзу (BGP).

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1. Проєктування фізичної та логічної (L2) топології мережі

Здійснимо проєктування за допомогою трирівневої структури, що включає в себе:

- Рівень ядра
- Рівень розподілу
- Рівень доступу

Спроектовану мережу представлено на рисунку 2.1.

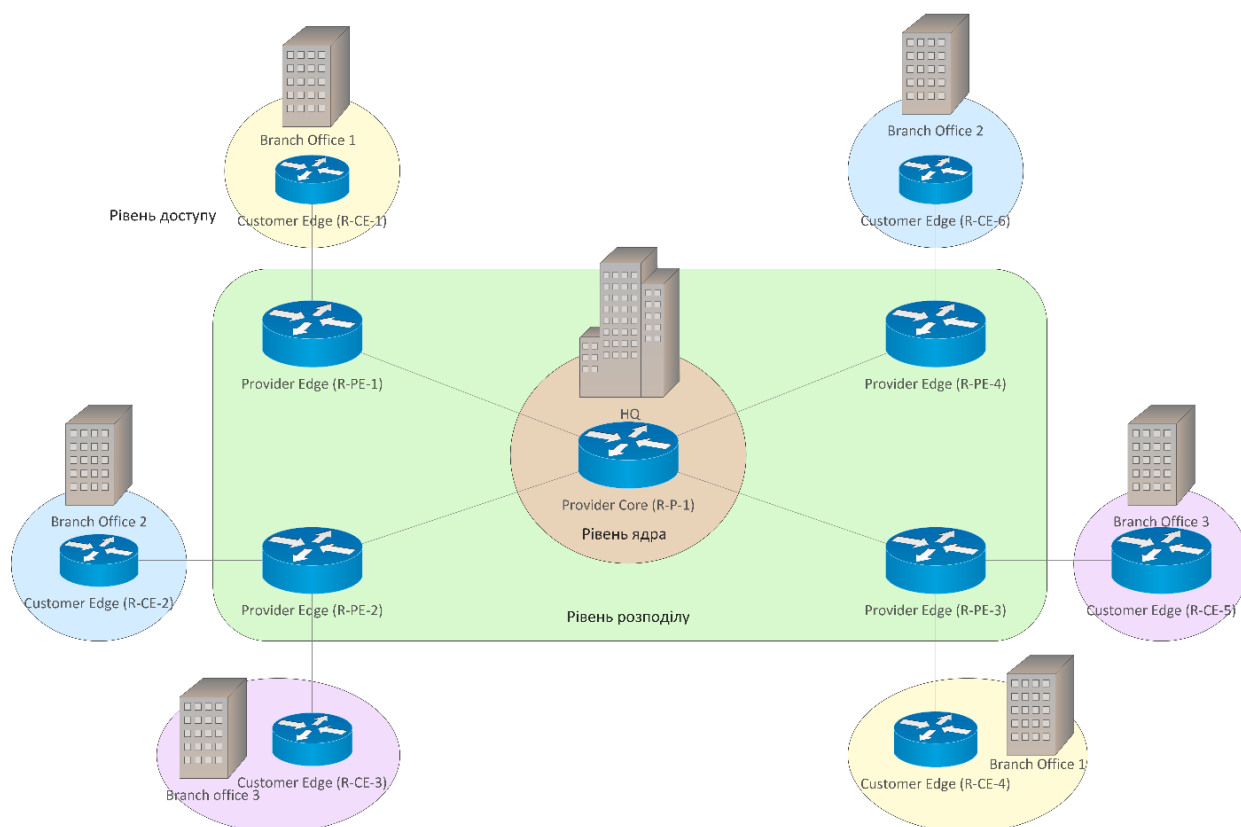


Рис. 2.1. Проєкт фізичної топології корпоративної мережі

Рівень ядра складатиметься з одного Р-маршрутизатора який з'єднуватиметься з іншими РЕ-маршрутизаторами за допомогою Gigabit Ethernet.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Рівень розподілу в свою чергу складатиметься з 4 маршрутизаторів, які за необхідності підтримуватимуть розширення мережі. Підключення до маршрутизаторів кінцевих клієнтів здійснюватиметься за допомогою Gigabit Ethernet.

Рівень доступу – це кінцеве устаткування користувачів, у даному випадку це наші віддалені філіали. Цей рівень також передбачає розширення мережі. Для підключення локальних пристроїв підмережі використовуватиметься Gigabit Ethernet.

Загальна корпоративна мережа складатиметься із сумарно 6 підмереж-філіалів. Усього є 3 гілки, кожна з яких складатиметься із 2 віддалених філіалів, що також матимуть однаковий адресний простір.

Кожна підмережа розрахована на 1 комутатор з 24 портами для підключень робочих станцій, серверів, та з'єднання з іншими комутаторами, та 1 маршрутизатор, який з'єднуватиме кінцевих користувачів з внутрішньою локальною мережею та матиме вихід в глобальну мережу Інтернет.

Кожен комутатор має такі призначені порти:

- Перший порт для підключення до маршрутизатора
- Другий порт для підключення до сервера
- 4 резервні порти для розширення мережі, або налагодження комутатора
- Решті портів призначаються VLAN та підключаються робочі станції.

У кожній мережі присутній сервер на якому будуть налаштовані усі необхідні служби та сервіси прикладного рівня.

Приклад спроектованої підмережі філіалу наведено на рисунку 2.2. Важливо зазначити, що сервер буде присутній лише у першій підмережі філіалу.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

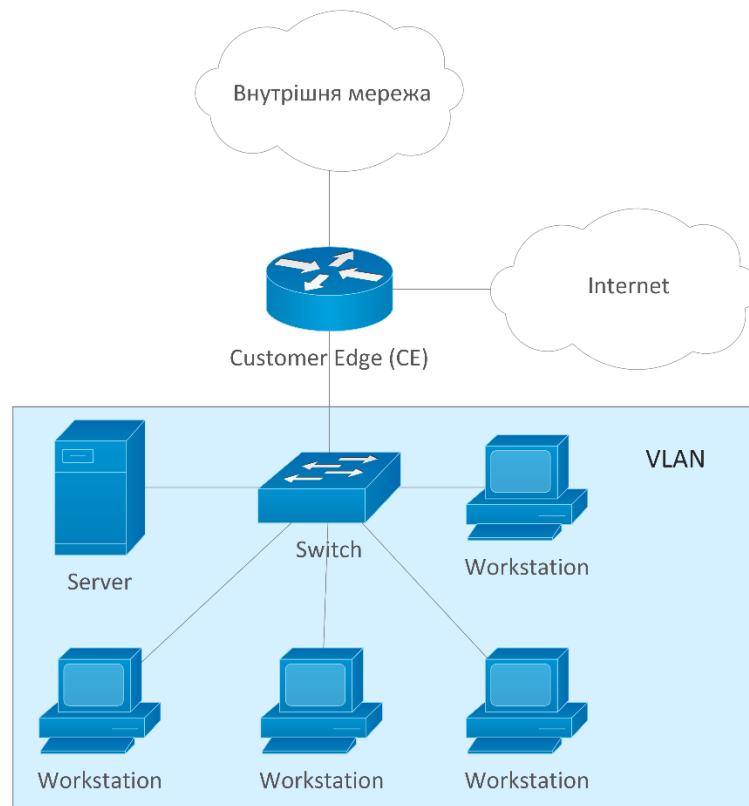


Рис. 2.2. Проєкт фізичної топології підмережі (філіалу)

2.2. Проєктування логічної (L3) топології мережі та розробка системи IP-адресації

Для роботи мережі були розраховані параметри IP-адресації, результати наведені в таблиці 2.1. При розрахунку також враховувалася економія IP-адрес, тому мережі були розділені на підмережі з оптимальними масками відповідно до кількості вузлів у кожній підмережі. Враховувалася також можливість розширення підмереж.

Маршрутизаторам, комутаторам і серверам присвоюється статична IP-адреса, в той час як робочі станції отримують IP-адресу від DHCP-сервера відповідної підмережі.

Для з'єднань між рівнями ядра, розподілу та доступу адресація створювалася таким чином, щоб використовувати мінімальну кількість IP-адрес, задовольняючи при цьому потреби підключених вузлів. Розрахунок показано у таблицях 2.1 – 2.3.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Таблиця 2.1.

Параметри IP-адресації для Loopback інтерфейсу

Пристрій	IP-адреса	
R-P-1	1.0.0.1/32	
R-PE-1	2.0.0.1/32	
R-PE-2	2.0.0.2/32	
R-PE-3	2.0.0.3/32	
R-PE-4	2.0.0.4/32	
R-CE-1	ABCD::1/128	3.0.0.1/32
R-CE-2	ABCD::2/128	3.0.0.1/32
R-CE-3	ABCD::3/128	3.0.0.3/32
R-CE-4	ABCD::4/128	3.0.0.4/32

Таблиця 2.2.

Параметри IP-адресації для підключень між рівнями ядра та розподілу

Пристрої	IP-адреса мережі
R-P-1 до R-PE-1	1.1.1.0/31
R-P-1 до R-PE-2	1.1.2.0/31
R-P-1 до R-PE-3	1.1.3.0/31
R-P-1 до R-PE-4	1.1.4.0/31

Таблиця 2.3.

Параметри IP-адресації для підключень між рівнями розподілу та доступу:

Пристрої	IP-адреса мережі
R-PE-1 до R-CE-1	2001:db8:A:1::0/126
R-PE-2 до R-CE-2	2001:db8:A:2::0/126
R-PE-2 до R-CE-3	2001:db8:A:3::0/126
R-PE-3 до R-CE-4	2001:db8:A:4::0/126
R-PE-3 до R-CE-5	2001:db8:A:5::0/126
R-PE-4 до R-CE-6	2001:db8:A:6::0/126

Завдяки особливостям технології MPLS VPN, а саме тому що параметри IP-адресації можуть повторюватися між підмережами, усі підмережи матимуть однакові параметри IP-адресації. Параметри IP-адресації для філіалів наведено у таблиці 2.4.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Таблиця 2.4.

Параметри IP-адресації філіалів

Призначення	IP-адреса	
Адреса мережі	2001:db8:bd:1::0/120	2001:db8:bd:2::0/120
Мінімальна адреса	2001:db8:bd:1::1	2001:db8:bd:2::1
Максимальна адреса	2001:db8:bd:1::ff	2001:db8:bd:2::ff
Шлюз за замовчуванням	2001:db8:bd:1::1	2001:db8:bd:2::1
Діапазон адрес комутаторів	2001:db8:bd:1::2	2001:db8:bd:2::2
	2001:db8:bd:1::10	2001:db8:bd:2::10
Діапазон статичних адрес	2001:db8:bd:1::11	2001:db8:bd:2::11
	2001:db8:bd:1::30	2001:db8:bd:2::30
Діапазон адрес майбутніх ПК	2001:db8:bd:1::31	2001:db8:bd:2::31
	2001:db8:bd:1::fe	2001:db8:bd:2::fe

2.3. Проектування служб та сервісів прикладного рівня

Кожна мережа матиме свій DHCP-сервер із вказаними діапазонами видаваних IP-адрес робочим станціям мережі. Роль DHCP-сервера виконуватиме маршрутизатор підмережі. Так як усі підмережі працюють на IPv6, відповідно використовуватиметься саме DHCPv6.

DHCPv6, скорочення від Dynamic Host Configuration Protocol версії 6, є важливим мережевим протоколом, призначеним для полегшення конфігурації хостів Інтернет-протоколу версії 6 (IPv6). Його основна функція полягає у призначенні IP-адрес, IP-префіксів, маршрутів за замовчуванням, MTU локального сегмента та інших параметрів конфігурації, необхідних для безперебійної роботи пристроїв у мережі IPv6. Важливо зазначити, що DHCPv6 не є просто прямим аналогом IPv4; скоріше, він виконує окремі функції, адаптовані до середовища IPv6.

У середовищі IPv6 хости мають можливість автономно генерувати свої IP-адреси за допомогою автоконфігурації адрес без статусу (SLAAC). Крім того, вони можуть покладатися на DHCPv6 для отримання даних конфігурації. У

багатьох випадках хости можуть використовувати комбінацію обох методів для оптимального налаштування мережі.

Для синхронізації часу між пристроями мережі, використовуватиметься технологія NTP. Роль NTP-сервера належатиме маршрутизатору підмережі, який слугуватиме еталонним джерелом часу та синхронізуватиме час з пристроями підмережі. Своє ж джерело часу маршрутизатор отримуватиме з глобального серверу з Інтернету.

Протокол мережевого часу (Network Time Protocol, NTP) - це важливий протокол, призначений для синхронізації годинників комп'ютерів у мережі. Працюючи як прикладний протокол, NTP відповідає за забезпечення синхронізації хостів у мережі TCP/IP.

Функціонуючи на прикладному рівні, NTP використовує ієрархічну структуру часових ресурсів для полегшення синхронізації між серверами різних рівнів. На самому верхньому рівні знаходяться високоточні часові ресурси, такі як атомні або GPS-годинники, які відносяться до серверів нульового рівня. Ці сервери з'єднані з серверами NTP на нижчих рівнях, позначених як рівень 1, рівень 2 і так далі. Згодом ці сервери надають точну інформацію про дату і час, що дозволяє хостам, які спілкуються, узгоджувати свої годинники один з одним.

Також важливо забезпечити журналювання усіх подій у підмережі для забезпечення коректної роботи усіх служб та сервісів, та підтримки безпеки, за допомогою виявлення всіх аномальних подій. Для цієї задачі використовуватиметься протокол Syslog. Служба протоколу Syslog буде виконуватися на сервері підмережі.

Syslog - це стандартний протокол реєстрації повідомлень, який комп'ютерні системи використовують для надсилання журналів подій на сервер Syslog для зберігання. На мережевих пристроях Syslog може використовуватися для реєстрації таких подій, як зміна стану інтерфейсу, перезавантаження системи тощо. Можна реєструвати багато різних типів подій. Журнали мають важливе значення при усуненні несправностей, вивченні причин інцидентів і т.д.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Сервер Syslog дозволяє нам надсилати інформацію журналу всіх наших мережевих пристроїв в одне централізоване місце. Повідомлення журналу надсилаються через UDP-порт 514 на сервер Syslog. Звідси ми можемо шукати, керувати та архівувати всю інформацію журналу.

2.4. Проектування підсистеми мережного захисту

Кожен маршрутизатор та комутатор підмережі матиме встановлені 2 користувачі:

- Користувач Admin з найвищим рівнем доступу (15) – доступ на рівні привілеїв дозволяє увійти в режим привілейованого виконання і забезпечує повний контроль над маршрутизатором.
- Користувач User з низьким рівнем доступу (1) – доступ на рівні користувача дозволяє увійти в режим User Exec, який надає дуже обмежений доступ до маршрутизатора тільки для читання.

Привілейований режим у комутаторах та маршрутизаторах буде захищено паролем.

Доступ до маршрутизаторів рівню ядра та розподілу буде можливий лише по прямому консольному підключенню та буде захищений паролем.

Створені паролі будуть 5 типу, тобто шифруватимуться за допомогою хешування MD5.

MD5 (Message-Digest Algorithm 5) – це криптографічна хеш-функція, яка обробляє вхідні повідомлення різної довжини і перетворює їх у 16-байтні повідомлення фіксованої довжини. Спочатку задуманий як вдосконалення MD4, MD5 був розроблений з урахуванням підвищених вимог до безпеки.

Також буде налаштовано можливість отримання віддаленого доступу за допомогою SSHv2.

Транспортний протокол SSHv2 забезпечує надійний, безпечний, двонаправлений потік даних між вузлами з SSH. Безпека забезпечується за допомогою шифрування і надійних перевірок цілісності.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Наразі підтримуються такі методи шифрування: 3des-cbc; blowfish-cbc; twofish-cbc, aes-cbc, serpent-cbc з ключами 128, 192 і 256 біт. idea-cbc; cast-cbc з ключами 128 біт; і RC4. Серед них 3des-cbc є обов'язковим, 128-бітний aes-cbc рекомендований, а решта – дискретні.

Можливість підключення надаватиметься лише пристроям з однієї підмережі, підключення по SSH з пристроїв інших підмереж блокуватиметься за допомогою списків доступу (ACL).

У сфері комп'ютерної безпеки список контролю доступу (ACL) – це перелік дозволів, пов'язаних із системним ресурсом. Він визначає, які користувачі або системні процеси мають дозвіл на доступ до ресурсів, а також конкретні операції, дозволені на цих ресурсах. У стандартному списку ACL кожен запис розмежовує об'єкт та операцію.

У певному пропрієтарному комп'ютерному обладнанні, зокрема маршрутизаторах і комутаторах, список контролю доступу містить правила, що застосовуються до номерів портів або IP-адрес, доступних на хості або на іншому рівні 3-го рівня. Кожне правило містить список авторизованих хостів та/або мереж, яким дозволено використовувати послугу.

Для більш надійного зв'язку та відмовостійкості на всіх маршрутизаторах і комутаторах варто налагодити резервні лінії зв'язку, такі як агреговані канали, але через обмеження GNS3 лише комутатори підмережі матимуть агреговані канали. Кожен окремий комутатор матиме свій окремий VLAN, а при розширенні мережі створюватимуться нові. Також для підвищення безпеки мережі, на портах комутатора буде налаштовано Port-Security.

Висновки до другого розділу: Протягом виконання даного розділу було виконано проєктування загальної корпоративної мережі та її підмереж-філіалів, також було визначено які технології використовувати для підключення між маршрутизаторами та іншими пристроями, розроблено систему IP-адресації для пристроїв мережі, спроектовано підсистеми мережного захисту, такі як: доступ за користувачами та базовий захист, віддалений доступ.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

РОЗДІЛ 3. ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ ПРОЄКТОВАНОЇ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1. Вибір обладнання та ОС пристроїв для розробленого проєкту мережі

Для реалізації MPLS VPN необхідно приділити увагу саме до вибору обладнання, адже не всі маршрутизатори підтримують функціонал, який необхідно забезпечити для реалізації MPLS.

У даній мережі використовуватимуться 4 різних типи маршрутизаторів, а саме Р, РЕ, СЕ і С:

- Р - основний маршрутизатор провайдера. Будь-який маршрутизатор Cisco серії 7200 або вище може функціонувати як Р-маршрутизатор.
- РЕ - прикордонний маршрутизатор провайдера. Маршрутизатор Cisco 2600, а також будь-який маршрутизатор серії 3600 або вище може функціонувати як РЕ-маршрутизатор.
- СЕ - прикордонний маршрутизатор клієнта. Можна використовувати будь-який маршрутизатор, який може обмінюватися інформацією про маршрутизацію зі своїм РЕ-маршрутизатором.
- С - маршрутизатор клієнта. Так само як і СЕ, можна використовувати будь-який маршрутизатор.

Через обмеження GNS3, а саме через неможливість налаштування VPNv6 на Cisco серії 3745, для Р та РЕ маршрутизаторів використовуватиметься Cisco серії 7200. Для СЕ та С маршрутизаторів також використовуватимуться маршрутизатори Cisco серії 7200, через неможливість налаштування прикладних сервісів на IPv6. Зовнішній вигляд маршрутизатора Cisco 7200 Series наведено на рисунку 3.1.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39



Рис. 3.1. Маршрутизатор Cisco 7200 Series

Завдяки адаптерам портів і сервісів від NxDS0 до Gigabit Ethernet і OC-3, швидкості обробки до 2 мільйонів пакетів в секунду і неперевершеній кількості високотехнологічних IP-сервісів, серія Cisco 7200 VXR є ідеальним периферійним пристроєм для агрегації послуг WAN/MAN для підприємств і постачальників послуг, які впроваджують будь-яке з наступних рішень:

- Якість обслуговування (QoS) на межі глобальної мережі, відзначена багатьма нагородами.
- Завдяки широкосмуговій агрегації можлива підтримка до 16 000 сеансів протоколу Point-to-Point (PPP) на одне шасі.
- Найпопулярнішим варіантом розгортання прикордонної мережі провайдера на сьогоднішній день є багатопроTOCOLна комутація з комутацією по мітках (Multiprotocol Label Switching Provider Edge, MPLS PE).
- Віртуальна приватна мережа (VPN) для захисту IP, яка може масштабуватися до 5 000 тунелів на шасі.

- Високотехнологічне обладнання в приміщеннях клієнтів (CPE): Це зменшує витрати на обладнання, транспортування та адміністративні витрати для керованих глобальних мереж.

У філіях підприємств маршрутизатори Cisco 3700 забезпечують значно вищий рівень інтеграції додатків і сервісів. Маршрутизатори Cisco 3700 забезпечують щільність обслуговування філій у невеликому форм-факторі завдяки підтримці декількох модулів розширеної інтеграції (AIM), нових сервісних модулів високої щільності і вбудованого підключення до локальної/глобальної мережі. Приклад маршрутизатора Cisco 3700 Series наведено на рисунку 3.2.

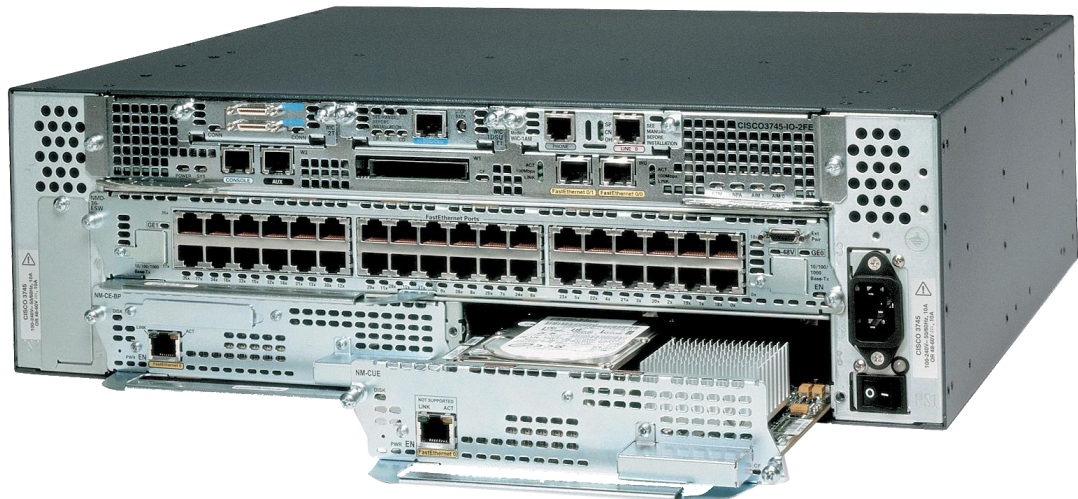


Рис. 3.2. Маршрутизатор Cisco 3745 Series

Серія Cisco 3700 - це потужне рішення для доступу до віддалених офісів для клієнтів, які готуються до перенесення сервісів зі старої інфраструктури та розповсюдження нових додатків від ядра до периферії підприємства. Впровадження Cisco 3700 Series знижує загальну вартість володіння інфраструктурою клієнтів, збільшує конкурентні переваги мережі і прискорює отримання клієнтами переваг від економії витрат на додатки для електронного бізнесу.

У ролі комутатора мережі можна використати старіший Cisco Catalyst 2960 Series Switch, який підтримує весь необхідний функціонал для раніше спроектованих систем захисту підмережі, або нову модель Cisco Catalyst 9200 Series Switches. Побачити комутатор Cisco Catalyst 2960 можна на рисунку 3.3.



Рис. 3.3. Комутатор Cisco Catalyst 2960 Series Switch

Cisco Catalyst 2960 є частиною лінійки автономних пристроїв з фіксованою конфігурацією, які забезпечують підключення настільних комп'ютерів за технологіями Fast Ethernet і Gigabit Ethernet для мереж підприємств початкового рівня, середнього бізнесу і філій для надання розширених послуг локальної мережі.

Cisco Catalyst 2960 – це серія мережевих комутаторів, призначених для розгортання на рівні доступу, як правило, для малого та середнього бізнесу, але також може використовуватися і у великих організаціях. Вони представлені моделями зі швидкістю Fast Ethernet (100 Мбіт/с) або Gigabit Ethernet (1 Гбіт/с).

Ключові особливості комутаторів Cisco Catalyst 2960:

- Працює на 2-му рівні моделі OSI, тобто пересилає пакети даних на основі MAC-адрес.
- Пропонує такі функції, як списки контролю доступу (ACL) для обмеження доступу до мережі та контроль доступу до мережі (NAC) для посилення безпеки.
- Визначає пріоритети трафіку для критично важливих додатків, таких як голос і відео (QoS).
- Деякі моделі можна об'єднувати в стек, щоб збільшити кількість доступних портів.
- Підтримує різні варіанти управління для конфігурації та моніторингу.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

В цілому, комутатори Cisco Catalyst 2960 є надійним і безпечним рішенням для підключення пристроїв рівню доступу до мережі.

Кількість портів на комутаторі Cisco Catalyst 2960 залежить від конкретної моделі. Зазвичай вони становлять від 24 до 48 портів:

- Cisco Catalyst 2960-24TT: 24 x 10/100 Мбіт/с порти Fast Ethernet
- Cisco Catalyst 2960-48TC-S: 48 x 10/100 Мбіт/с портів Fast Ethernet і 2 x Gigabit Ethernet SFP порти
- Cisco Catalyst 2960-C: 24 x порти Gigabit Ethernet

Комутатори Cisco Catalyst серії 9200 є наступником серії 2960 і призначені для створення модульних і масштабованих мереж для підприємств будь-якого розміру. Цей комутатор можна побачити на рисунку 3.4.



Рис. 3.4. Комутатор Cisco Catalyst 9200 Series Switch

Ось короткий огляд їх ключових особливостей:

- Ці комутатори поставляються в різних конфігураціях з різними типами портів, що дозволяє налаштувати їх під конкретні потреби.
- Гігабітні порти Ethernet (1 Гбіт/с)
- Мультигігабітні порти (2,5 Гбіт/с, 5 Гбіт/с і 10 Гбіт/с) для високошвидкісних додатків Power over Ethernet (PoE+) для забезпечення живлення таких пристроїв, як VoIP-телефони та IP-камери, безпосередньо через комутатор.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

- Об'єднання в мережу на основі намірів - ця функція спрощує керування комутатором, автоматизуючи завдання на основі загальних цілей (намірів) вашої мережі.
- Catalyst 9200 надає пріоритет безпеці завдяки функціям, які захищають обладнання, програмне забезпечення та всі дані, що проходять через комутатор.
- Ці комутатори розроблені для забезпечення надійності та безперебійної роботи, підтримуючи безперебійну роботу вашої мережі.
- Вони також пропонують такі функції, як: Якість обслуговування (QoS) для пріоритизації критично важливого трафіку; Віртуальна маршрутизація і переадресація (VRF) для створення ізольованих сегментів мережі

Сервер у підмережах повинен забезпечувати роботу служби Syslog. У ролі сервера мережі використовуватиметься робоча станція з операційною системою Windows. Я вибрав саме Windows 7, через її низькі вимоги до ресурсів комп'ютера та підтримку усіх необхідних серверу програмних засобів. Логотип даної операційної системи наведено у рисунку 3.5.



Рис. 3.5. Логотип Windows 7

Windows 7 від Microsoft є значним оновленням операційної системи Windows NT, що 22 жовтня 2009 року стала загальнодоступною. Це заміна Windows Vista, яка була випущена майже трьома роками раніше. Windows 7 все ще є життєздатною операційною системою для використання на персональних комп'ютерах, таких як настільні та портативні комп'ютери, що використовуються для бізнесу та дому, планшетні комп'ютери та комп'ютери-медіацентри.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Для реалізації зазначених раніше служб використовується програмне забезпечення TFTPД. Інтерфейс програми наведено на рисунку 3.6.

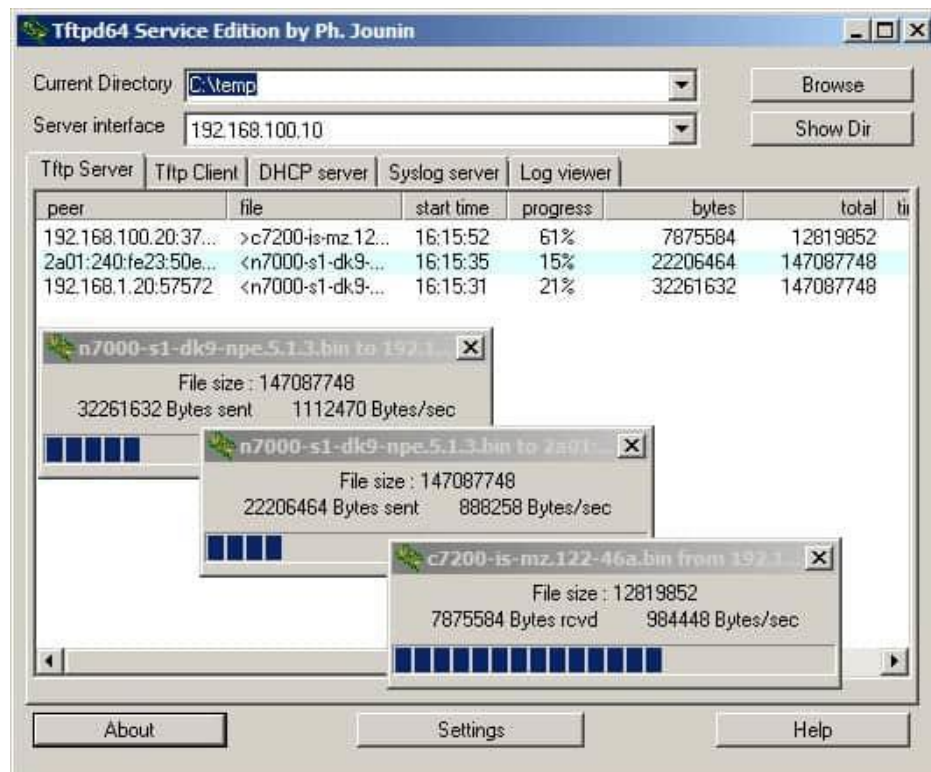


Рис. 3.6. Інтерфейс програми TFTPД

TFTPД 32/64 - це безкоштовна, легка програма з відкритим вихідним кодом, яка підтримує роботу з IPv6, а також включає як серверні служби серверу DHCP, TFTP, DNS, SNTP і Syslog, а також TFTP клієнт.

3.2. Побудова та налагодження спроектованої мережі

Всі налаштування пристроїв мережі починаються з призначення хостнеймів та IP-адрес до відповідних інтерфесів. Як було визначено раніше, маршрутизатори, комутатори та сервери мають статичні параметри адресації, а робочі станції отримуватимуть свої IP-адреси з DHCP-сервера. Приклад налаштування наведено на рисунках 3.7. та 3.8.

```

R-CE-1(config)#hostname R-CE-1
R-CE-1(config)#no ip domain lookup
R-CE-1(config)#ipv6 unicast-routing
R-CE-1(config)#ipv6 cef
R-CE-1(config)#interface Loopback0
R-CE-1(config-if)#ipv6 addr ABCD::1/128
R-CE-1(config-if)#ip addr 3.0.0.1 255.255.255.255
R-CE-1(config-if)#exit
R-CE-1(config)#interface g0/0
R-CE-1(config-if)#ipv6 address 2001:db8:a:1::2/126
R-CE-1(config-if)#no shut
R-CE-1(config-if)#exit
R-CE-1(config)#interface g1/0
R-CE-1(config-if)#ipv6 address 2001:db8:bd:1::1/120
R-CE-1(config-if)#no shut
R-CE-1(config-if)#exit
R-CE-1(config)#router bgp 200

```

Рис. 3.7. Налаштування хостнейму та призначення IP-адрес

```

R-CE-2(config)#ipv6 dhcp pool Site2LanA
R-CE-2(config-dhcpv6)#address prefix 2001:db8:bd:1::0/120
R-CE-2(config-dhcpv6)#dns-server 2001:db8:bd:1::1
R-CE-2(config-dhcpv6)#domain-name Site2LanA.net
R-CE-2(config-dhcpv6)#exit
R-CE-2(config)#in f1/0
R-CE-2(config-if)#ipv6 dhcp server Site2LanA
R-CE-2(config-if)#ipv6 nd managed-config-flag
R-CE-2(config-if)#exit
R-CE-2(config)#

```

Рис. 3.8. Налаштування DHCPv6 на маршрутизаторі R-CE-2

Налаштувавши всі статичні адреси та забезпечивши роботу DHCP-сервера переходимо до налаштування MPLS VPN на Р та РЕ-маршрутизаторах.

Першим кроком буде налаштування Р-маршрутизатора, який і слугуватиме ядром MPLS-мережі. Приклад налаштування наведено на рисунку 3.9. Після призначення усіх статичних параметрів IP-адресації налаштування здійснюється так:

1. Командою “ip cef” вмикаємо Cisco Express Forwarding для маршрутизації IP пакетів.
2. Командами “mpls ip”, “mpls label protocol ldp”, “mpls ldp router-id loop0” вмикаємо і налаштовуємо MPLS, вказуємо використовуваний протокол LDP і призначаємо щоб ідентифікатором маршрутизатора стала його Loopback адреса.

3. Після цього на усіх портах, що ведуть до інших маршрутизаторів, які забезпечують роботу MPLS-мережі, виконується команда “mpls ip”.
4. Далі для забезпечення зв’язку і маршрутизації між маршрутизаторами рівню ядра та розподілу необхідно виконати налаштування OSPF. Команда “mpls ldp autoconfig” дозволяє автоконфігурацію MPLS LDP для інтерфейсів, що належать до процесу маршрутизації OSPF.

```

R-P-1(config)#ip cef
R-P-1(config)#mpls ip
R-P-1(config)#mpls label protocol ldp
R-P-1(config)#mpls ldp router-id loop0
R-P-1(config)#in loop0
R-P-1(config-if)#ip addr 1.0.0.1 255.255.255.255
R-P-1(config-if)#exit
R-P-1(config)#in g1/0
R-P-1(config-if)#ip addr 1.1.1.1 255.255.255.252
R-P-1(config-if)#mpls ip
R-P-1(config-if)#no shut
R-P-1(config-if)#exit
R-P-1(config)#in g2/0
R-P-1(config-if)#ip addr 1.1.2.1 255.255.255.252
R-P-1(config-if)#mpls ip
R-P-1(config-if)#no shut
R-P-1(config-if)#exit
R-P-1(config)#in g3/0
R-P-1(config-if)#ip addr 1.1.3.1 255.255.255.252
R-P-1(config-if)#mpls ip
R-P-1(config-if)#no shut
R-P-1(config-if)#exit
R-P-1(config)#in g4/0
R-P-1(config-if)#ip addr 1.1.4.1 255.255.255.252
R-P-1(config-if)#mpls ip
R-P-1(config-if)#no shut
R-P-1(config-if)#exit
R-P-1(config)#router ospf 1
R-P-1(config-router)#mpls ldp autoconfig
R-P-1(config-router)#network 1.0.0.1 0.0.0.0 area 0
R-P-1(config-router)#network 1.1.1.0 0.0.0.3 area 0
R-P-1(config-router)#network 1.1.2.0 0.0.0.3 area 0
R-P-1(config-router)#network 1.1.3.0 0.0.0.3 area 0
R-P-1(config-router)#network 1.1.4.0 0.0.0.3 area 0
R-P-1(config-router)#exit
R-P-1(config)#exit

```

Рис. 3.9. Налаштування маршрутизатора R-P-1

На цьому налаштування маршрутизатора-ядра MPLS завершено. Переходимо до налаштування маршрутизаторів рівня розподілу. Ці налаштування вже більш комплексні, ніж у R-маршрутизатора, хоч деякі

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

налаштування і повторюються. Приклад налаштування наведено на рисунках 3.10 та 3.11.

Налаштування відбувається так:

1. Так само як і у Р-маршрутизаторах, використовуючи команду “ip cef” вмикаємо Cisco Express Forwarding, далі вмикаємо і налаштовуємо MPLS за допомогою команд “mpls ip”, “mpls label protocol ldp”, “mpls ldp router-id loop0” після чого виконуємо команду “mpls ip” на порті, який веде до Р-маршрутизатора.
2. Далі з’являється відмінність у налаштуваннях. Використовуємо команду “ipv6 cef” у режимі глобального конфігурування для увімкнення Cisco Express Forwarding для IPv6. Маршрутизація IPv6 не ввімкнена за замовчуванням і має бути ввімкнена за допомогою команди “ipv6 unicast-routing”.
3. Тепер налаштовуємо VRF відповідно до кожної підключеної підмережі. Створення VRF здійснюється за допомогою команди “vrf definition Site1”. За допомогою команди “rd 200:1” створюємо VRF-таблицю, вказуючи розпізнавач маршрутів [12]. Команда “address-family ipv6” вказує сімейство адрес IPv6 і переходить у режим їхньої конфігурації [13]. Тут за допомогою команд “route-target export | import 200:1 ” створюємо список цільових спільнот імпорту, експорту маршрутів для вказаного VRF. Потім на інтерфейсах маршрутизатора, які ведуть до маршрутизатора клієнта виконується команда “vrf forwarding Site1”. На цьому етапі створення і налаштування VRF закінчено.
4. Після чого забезпечуємо зв’язок з іншими маршрутизаторами за допомогою BGP. Переходимо до налаштування BGP за допомогою команди “router bgp 100”. Спочатку додаємо усі сусідні маршрутизатори рівню розподілу як сусідні за допомогою команди “neighbor 2.0.0.2 remote-as 100”. Далі переходимо у налаштування сімейства адрес IPv6 командою “address-family ipv6”, активуємо вказані сусідні маршрутизатори командами “neighbor 2.0.0.2 activate” [12].

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

5. Тепер необхідно налаштувати сімейство адрес VPNv6, яке необхідно для функціонування MPLS VPN. Командою “address-family vpnv6” переходимо до налаштування сімейства адрес, далі за допомогою команд “neighbor 2.0.0.2 activate” та “neighbor 2.0.0.2 send-community extended” активуємо VPNv6 [13].
6. Останнім кроком в налаштуванні BGP стане налаштування сімейства адрес для створених VRF. Перехід до налаштування виконується командою “address-family ipv6 vrf Site1”, далі додаємо і активуємо сусідній маршрутизатор клієнта командами “neighbor 2001:DB8:A:1::2 remote as 200” та “neighbor 2001:DB8:A:1::2 activate” [13].
7. Залишається лише налаштувати OSPF і на цьому реалізація функціонування PE-маршрутизатора завершена. Налаштування здійснюється так само як і для P-маршрутизатора.

```

R-PE-1(config)#vrf def Site1
R-PE-1(config-vrf)#rd 200:1
R-PE-1(config-vrf)#address-family ipv6
R-PE-1(config-vrf-af)#route-target export 200:1
R-PE-1(config-vrf-af)#route-target import 200:1
R-PE-1(config-vrf-af)#exit
R-PE-1(config-vrf)#exit
R-PE-1(config)#no ip domain lookup
R-PE-1(config)#ip cef
R-PE-1(config)#ipv6 unicast-routing
R-PE-1(config)#ipv6 cef
R-PE-1(config)#mpls label protocol ldp
R-PE-1(config)#mpls ldp router-id Loopback0 force
R-PE-1(config)#interface Loopback0
R-PE-1(config-if)#ip addr 2.0.0.1 255.255.255.255
R-PE-1(config-if)#no shut
R-PE-1(config-if)#exit
R-PE-1(config)#interface g0/0
R-PE-1(config-if)#ip address 1.1.1.2 255.255.255.252
R-PE-1(config-if)#mpls ip
R-PE-1(config-if)#no shut
R-PE-1(config-if)#exit
R-PE-1(config)#interface g1/0
R-PE-1(config-if)#vrf forwarding Site1
R-PE-1(config-if)#no ip addr
R-PE-1(config-if)#ipv6 address 2001:db8:a:1::1/126
R-PE-1(config-if)#no shut
R-PE-1(config-if)#exit

```

Рис. 3.10. Налаштування маршрутизатора R-PE-1

```

R-PE-1(config)#router ospf 1
R-PE-1(config-router)#network 1.1.1.0 0.0.0.3 area 0
R-PE-1(config-router)#network 2.0.0.1 0.0.0.0 area 0
R-PE-1(config-router)#exit
R-PE-1(config)#router bgp 100
R-PE-1(config-router)#bgp log-neighbor-changes
R-PE-1(config-router)#no bgp default ipv4-unicast
R-PE-1(config-router)#neighbor 2.0.0.2 remote-as 100
R-PE-1(config-router)#neighbor 2.0.0.2 update-source Loopback0
R-PE-1(config-router)#neighbor 2.0.0.3 remote-as 100
R-PE-1(config-router)#neighbor 2.0.0.3 update-source Loopback0
R-PE-1(config-router)#neighbor 2.0.0.4 remote-as 100
R-PE-1(config-router)#neighbor 2.0.0.4 update-source Loopback0
R-PE-1(config-router)#address-family ipv6
R-PE-1(config-router-af)#neighbor 2.0.0.2 activate
R-PE-1(config-router-af)#neighbor 2.0.0.2 send-label
R-PE-1(config-router-af)#neighbor 2.0.0.3 activate
R-PE-1(config-router-af)#neighbor 2.0.0.3 send-label
R-PE-1(config-router-af)#neighbor 2.0.0.4 activate
R-PE-1(config-router-af)#neighbor 2.0.0.4 send-label
R-PE-1(config-router-af)#exit
R-PE-1(config-router)#address-family vpnv6
R-PE-1(config-router-af)#neighbor 2.0.0.2 activate
R-PE-1(config-router-af)#neighbor 2.0.0.2 send-community extended
R-PE-1(config-router-af)#neighbor 2.0.0.4 activate
R-PE-1(config-router-af)#neighbor 2.0.0.4 send-community extended
R-PE-1(config-router-af)#neighbor 2.0.0.3 activate
R-PE-1(config-router-af)#neighbor 2.0.0.3 send-community extended
R-PE-1(config-router-af)#neighbor 2.0.0.4 activate
R-PE-1(config-router-af)#neighbor 2.0.0.4 send-community extended
R-PE-1(config-router-af)#exit
R-PE-1(config-router)#address-family ipv6 vrf Site1
R-PE-1(config-router-af)#neighbor 2001:db8:a:1::2 remote-as 200
R-PE-1(config-router-af)#neighbor 2001:db8:a:1::2 activate
R-PE-1(config-router-af)#neighbor 2001:db8:a:1::2 as-override
R-PE-1(config-router-af)#redistribute connected
R-PE-1(config-router-af)#exit
R-PE-1(config-router)#exit
R-PE-1(config)#

```

Рис. 3.11. Налаштування маршрутизатора R-PE-1

Останньою ланкою у даній мережі є маршрутизатори клієнтів, або CE маршрутизатори. Приклад налаштування наведено на рисунку 3.12. Налаштування у них найпростіші:

1. Виконуємо команди “ipv6 unicast-routing” та “ipv6 cef” для увімкнення маршрутизації IPv6.
2. Переходимо до налаштування BGP за допомогою команди “router bgp 200”, додаємо сусідній маршрутизатор з рівню доступу – “neighbor 2001:db8:1:3::1 remote-as 100”, заходимо в налаштування сімейства адрес

- “address-family ipv6” та активуємо сусідній маршрутизатор – “neighbor 2001:db8:a:3::1 activate”.

3. Останнім кроком налаштовуємо маршрутизацію за допомогою команди “ipv6 route ::/0 2001:db8:a:4::1”.

```
R-CE-4(config)#hostname R-CE-4
R-CE-4(config)#ip domain lookup
R-CE-4(config)#ipv6 unicast-routing
R-CE-4(config)#ipv6 cef
R-CE-4(config)#interface Loopback0
R-CE-4(config-if)#ipv6 addr ABCD::4/128
R-CE-4(config-if)#ip addr 3.0.0.4 255.255.255.255
R-CE-4(config-if)#exit
R-CE-4(config)#interface g0/0
R-CE-4(config-if)#ipv6 address 2001:db8:a:4::2/126
R-CE-4(config-if)#no shut
R-CE-4(config-if)#exit
R-CE-4(config)#interface g1/0
R-CE-4(config-if)#ipv6 address 2001:db8:bd:4::1/120
R-CE-4(config-if)#no shut
R-CE-4(config-if)#exit
R-CE-4(config)#router bgp 200
R-CE-4(config-router)#no synchronization
R-CE-4(config-router)#bgp log-neighbor-changes
R-CE-4(config-router)#redistribute connected
R-CE-4(config-router)#neighbor 2001:db
*Jun  4 06:51:46.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up8:a:4::1 remote-as 100
R-CE-4(config-router)#no auto-summary
R-CE-4(config-router)#address-family ipv6
R-CE-4(config-router-af)#neighbor 2001:db8:a:4::1 activate
R-CE-4(config-router-af)#network ABCD::4/128
R-CE-4(config-router-af)#redistribute connected
R-CE-4(config-router-af)#no synchronization
R-CE-4(config-router-af)#exit
R-CE-4(config-router)#exit
R-CE-4(config)#ipv6 route ::/0 2001:db8:a:4::1
```

Рис. 3.12. Налаштування маршрутизатора R-CE-4

На цьому етапі базове налаштування мережі та реалізацію MPLS VPN завершено, тому перейдемо до налаштування засобів захисту та прикладних сервісів.

Для початку виконаємо налаштування наших комутаторів у підмережі, налаштувавши відношення портів до відповідних VLAN та налагодивши Port-Security. Приклад налаштування комутатора наведено на рисунку 3.13.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

```

SW-3B-1(config)#in vlan 4
SW-3B-1(config-if)#ipv6 addr 2001:db8:bd:2::2/120
SW-3B-1(config-if)#no shut
SW-3B-1(config-if)#exit
SW-3B-1(config)#vlan 4
SW-3B-1(config-vlan)#name Site-3-Lan-B
SW-3B-1(config-vlan)#exit
SW-3B-1(config)#
SW-3B-1(config)#in range e0/0 - 3
SW-3B-1(config-if-range)#switchport
SW-3B-1(config-if-range)#switchport mode access
SW-3B-1(config-if-range)#switchport access vlan 4
SW-3B-1(config-if-range)#exit
SW-3B-1(config)#in range e1/0 - 3, e2/0 - 2, e3/0 - 3
SW-3B-1(config-if-range)#switchport
SW-3B-1(config-if-range)#switchport mode access
SW-3B-1(config-if-range)#switchport access vlan 4
SW-3B-1(config-if-range)#switchport port-security
SW-3B-1(config-if-range)#switchport port-security violation restrict
SW-3B-1(config-if-range)#exit
SW-3B-1(config)#

```

Рис. 3.13. Налаштування комутатора SW-3B-1

Тепер налаштуємо наш сервер, а саме встановимо параметри IP-адресації та налаштуємо програмний застосунок Tftpd32. Приклад налаштування серверу наведено на рисунках 3.14. та 3.15.

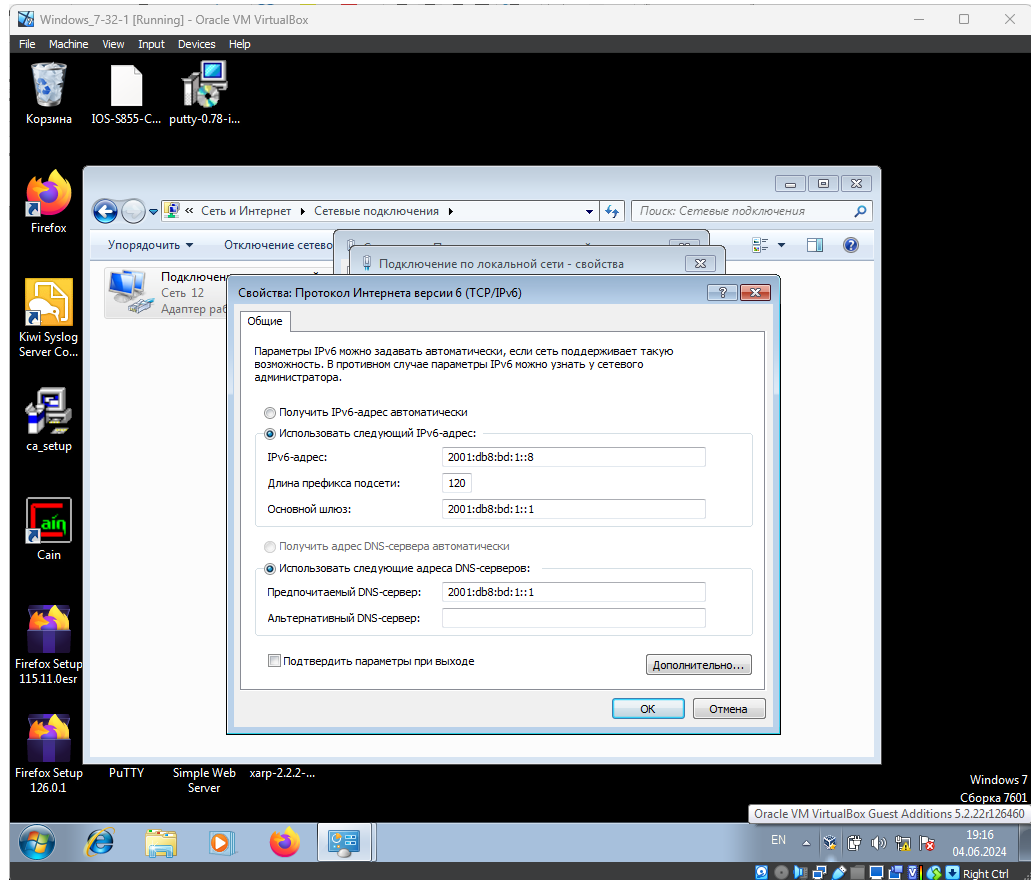


Рис. 3.14. Встановлення параметрів IP-адресації на Serv-1A

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

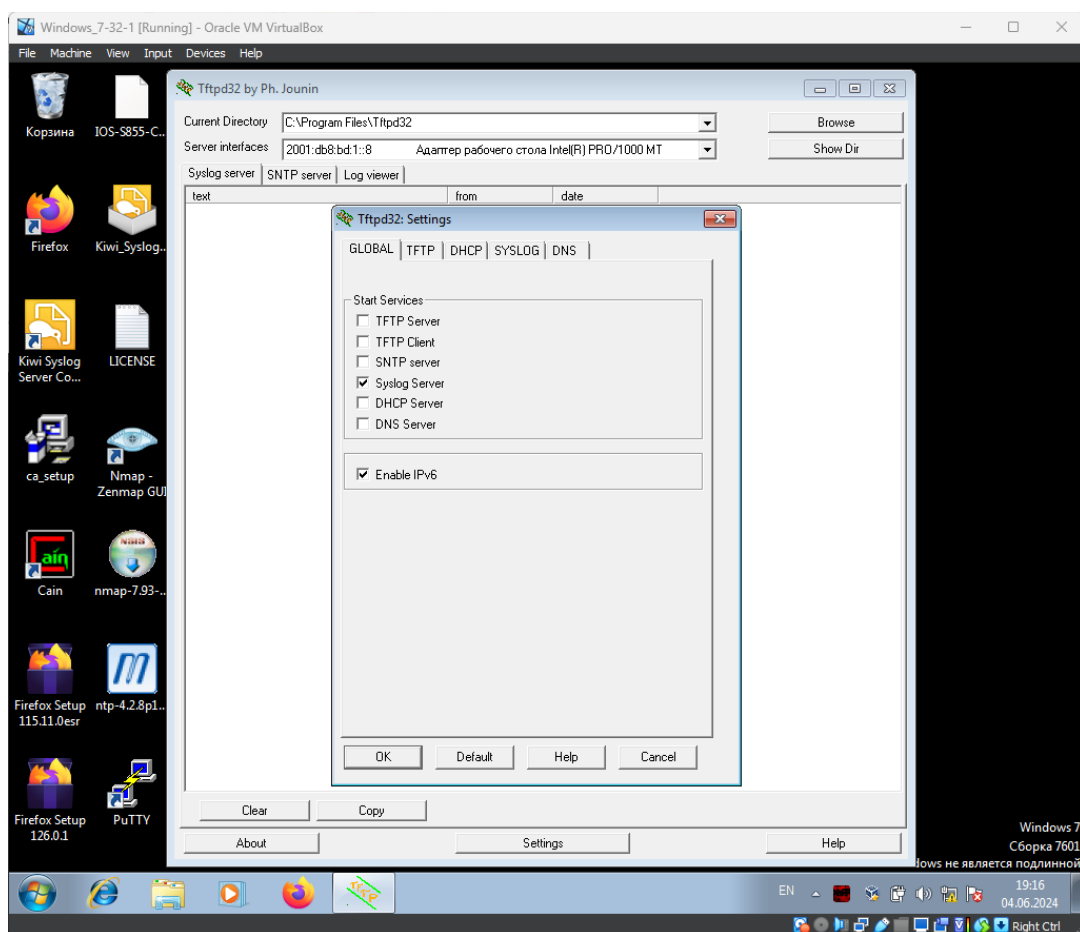


Рис. 3.15. Налаштування Tftpd32 на Serv-1A

Необхідно забезпечити маршрутизатору доступ в Інтернет для того щоб він міг синхронізуватися з онлайн NTP-сервером. Для цього необхідно підключити GNS3 Cloud до порта маршрутизатора і призначити йому IPv4 адресу за допомогою DHCP. Приклад налаштувань показано на рисунку 3.16.

```
R-CE-2(config)#ip domain lookup
R-CE-2(config)#ip name-server 192.168.50.1
R-CE-2(config)#in g2/0
R-CE-2(config-if)#ip addr dhcp
R-CE-2(config-if)#ipv6 nat
R-CE-2(config-if)#no shut
R-CE-2(config-if)#exit
R-CE-2(config)#in g1/0
R-CE-2(config-if)#ipv6 nat
R-CE-2(config-if)#exit
R-CE-2(config)#ipv6 access-list IPv6toIPv4
R-CE-2(config-ipv6-acl)#permit any any
R-CE-2(config-ipv6-acl)#exit
R-CE-2(config)#
R-CE-2(config)#ipv6 nat v6v4 source list IPv6toIPv4 interface g2/0 overload
R-CE-2(config)#ipv6 nat translation timeout never
R-CE-2(config)#
```

Рис. 3.16. Налаштування доступу в Інтернет на маршрутизаторі R-CE-2

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Тепер після налаштування виходу в Інтернет перейдемо до налаштування NTP та Syslog на наших пристроях мережі, а саме маршрутизаторі та комутаторі. Приклад налаштування маршрутизатора продемонстровано на рисунку 3.16, а комутатора – на рисунку 3.17.

```
R-CE-1(config)#logging host ipv6 2001:db8:bd:1::8
R-CE-1(config)#clock timezone GMT 2
R-CE-1(config)#clock summer-time DST recurring
R-CE-1(config)#ntp server 0.ua.pool.ntp.org
Translating "0.ua.pool.ntp.org"...domain server (192.168.50.1) [OK]

R-CE-1(config)#ntp source g2/0
R-CE-1(config)#ntp update-calendar
R-CE-1(config)#in g1/0
R-CE-1(config-if)#ntp broadcast
R-CE-1(config-if)#exit
R-CE-1(config)#exit
R-CE-1#
```

Рис. 3.16. Налаштування NTP-сервера та syslog-клієнта на маршрутизаторі R-CE-1

```
SW-3A-1(config)#logging host ipv6 2001:db8:bd:1::8
SW-3A-1(config)#clock timezone EEST 2
SW-3A-1(config)#clock summer-time EEST recurring
SW-3A-1(config)#in vlan 4
SW-3A-1(config-if)#ntp broadcast client
SW-3A-1(config-if)#exit
SW-3A-1(config)#ntp server 2001:db8:bd:1::1 source vlan 4 prefer
SW-3A-1(config)#ntp update-calendar
SW-3A-1(config)#
```

Рис.3.17. Налаштування NTP та syslog-клієнта на комутаторі SW-3A-1

Останнім кроком буде налаштування засобів безпеки, а саме: створення користувачів з різними рівнями доступу, встановлення пароля для входу в привілейований режим, налаштування віддаленого підключення за допомогою SSHv2 та обмеження доступу до нього за допомогою списків контролів доступу. Приклад налаштування засобів безпеки та віддаленого доступу для маршрутизатора наведено на рисунку 3.18, а комутатора – на рисунку 3.19.

```

R-CE-2(config)#ip domain-name Site2LanA.net
R-CE-2(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R-CE-2.Site2LanA.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
*Jun  7 02:20:01.287: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jun  7 02:20:01.767: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Jun  7 02:20:02.291: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
*Jun  7 02:20:02.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
[OK] (elapsed time was 4 seconds)

R-CE-2(config)#ip ssh ver 2
R-CE-2(config)#username Admin-Site2-LanA priv 15 secret admin
R-CE-2(config)#username User-Site2-LanA priv 1 secret user
R-CE-2(config)#ipv6 access-list SSH-BLOCK
R-CE-2(config-ipv6-acl)#permit 2001:db8:bd:1::0/120 any
R-CE-2(config-ipv6-acl)#exit
R-CE-2(config)#line vty 0 15
R-CE-2(config-line)#transport input ssh
R-CE-2(config-line)#login local
R-CE-2(config-line)#ipv6 access-class SSH-BLOCK in
R-CE-2(config-line)#exit
R-CE-2(config)#enable secret admin-cisco
R-CE-2(config)#

```

Рис.3.18. Налаштування засобів безпеки та віддаленого доступу на маршрутизаторі R-CE-2

```

SW-3A-1(config)#ip ssh ver 2
SW-3A-1(config)#username Admin-Site3-LanA priv 15 secret admin-sw
SW-3A-1(config)#username User-Site3-LanA priv 1 secret user-sw
SW-3A-1(config)#ipv6 access-list SSH-BLOCK
SW-3A-1(config-ipv6-acl)#permit 2001:db8:bd:1::0/120 any
SW-3A-1(config-ipv6-acl)#exit
SW-3A-1(config)#line vty 0 4
SW-3A-1(config-line)#transport input ssh
SW-3A-1(config-line)#login local
SW-3A-1(config-line)#ipv6 access-class SSH-BLOCK in
SW-3A-1(config-line)#exit
SW-3A-1(config)#enable secret admin-cisco
SW-3A-1(config)#

```

Рис. 3.19. Налаштування засобів безпеки на комутаторі SW-3A-1

Як зазначалося на етапі проектування, Р та РЕ-маршрутизатори матимуть лише локальний доступ при прямому консольному підключенні для більшої безпеки. Налаштування наведені на рисунку 3.20.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

```

R-P-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-P-1(config)#enable secret admin-cisco
R-P-1(config)#username Admin-P-1 priv 15 secret admin-p
R-P-1(config)#username User-P-1 priv 1 secret user
R-P-1(config)#exit

```

Рис. 3.20. Налаштування маршрутизатора R-P-1

3.3. Тестування роботи побудованої локальної мережі

Підемо по порядку налаштування наших пристроїв, а отже починаємо з перевірки роботи DHCPv6. На жаль, VPCs у GNS3 не підтримують Stateful DHCPv6, тому перевірка відбуватиметься на робочій станції з встановленим Kali Linux. Перевірку продемонстровано на рисунку 3.21.

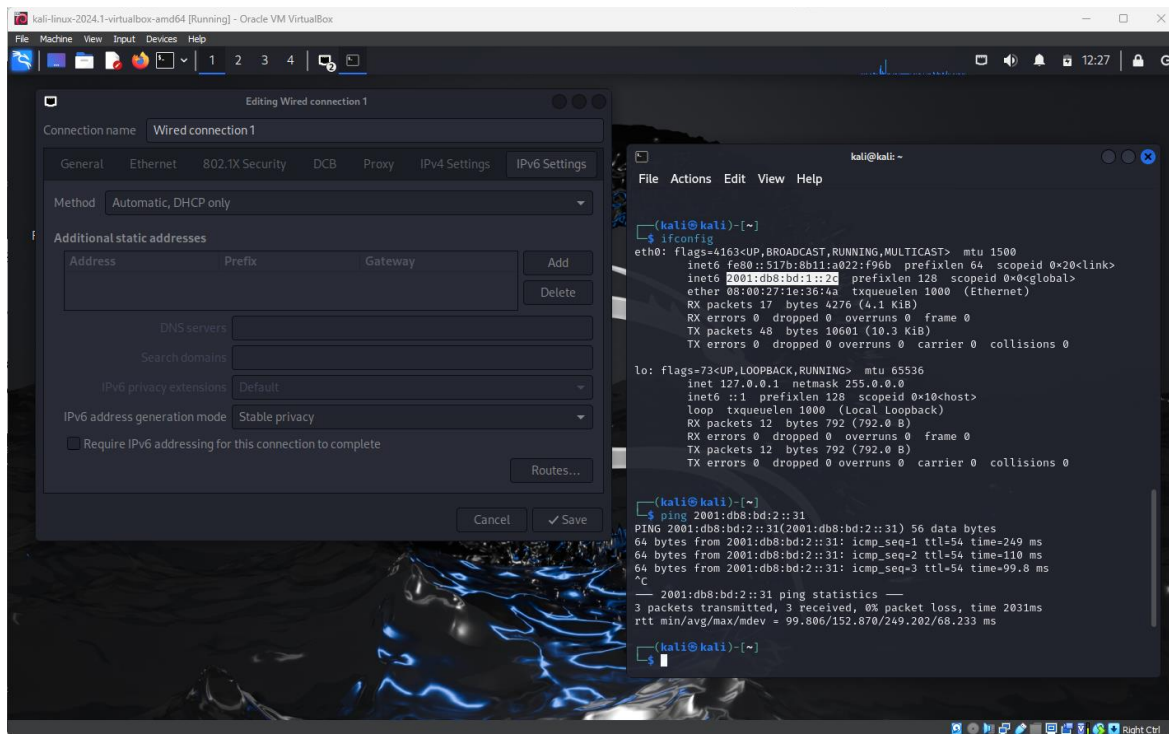


Рис. 3.21. Перевірка роботи DHCPv6 на робочій станції WS-1A-2

Як можна побачити, все працює коректно і робоча станція успішно встановлює зв'язок з іншими робочими станціями.

Переглянемо інформацію про DHCPv6 на нашому маршрутизаторі. Команди для перегляду та саму інформацію про протокол наведено на рисунку 3.22.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

```

R-CE-1#show ipv6 dhcp interface
GigabitEthernet1/0 is in server mode
  Using pool: SitellanA
  Preference value: 0
  Hint from client: ignored
  Rapid-Commit: disabled
R-CE-1#show ipv6 dhcp pool
DHCPv6 pool: SitellanA
  Address allocation prefix: 2001:DB8:BD:1::/120 valid 172800 preferred 86400 (2
in use, 0 conflicts)
  DNS server: 2001:DB8:BD:1::1
  Domain name: SitellanA.net
  Active clients: 2
R-CE-1#show ipv6 dhcp binding
Client: FE80::4D43:B0D4:6DB1:D209
  DUID: 00010001240EF2CC0800279E2740
  Username : unassigned
  IA NA: IA ID 0x0E080027, T1 43200, T2 69120
    Address: 2001:DB8:BD:1::33
              preferred lifetime 86400, valid lifetime 172800
              expires at Jun 06 2024 07:24 PM (172462 seconds)
Client: FE80::517B:8B11:A022:F96B
  DUID: 0004F7ADC9317C208D5F8A42E0F27A7A2328
  Username : unassigned
  IA NA: IA ID 0x2B506735, T1 43200, T2 69120
    Address: 2001:DB8:BD:1::2C
              preferred lifetime 86400, valid lifetime 172800
              expires at Jun 06 2024 07:24 PM (172463 seconds)
R-CE-1#

```

Рис. 3.22. Перегляд інформації про DHCPv6 на маршрутизаторі R-CE-1

Наступним кроком буде перевірка роботи MPLS VPN. Для цього спочатку перевіримо чи є зв'язок до віддаленої підмережі, а потім переглянемо чи до коректної підмережі встановлюється цей зв'язок, адже усі параметри IP-адресації повністю однакові на усіх підмережах, ця можливість є однією з особливостей MPLS VPN.

Для більшої наочності здійсимо перевірку з робочої станції, на якій встановлено Kali Linux. Деталі перевірки зв'язку та дослідження маршруту наведено на рисунку 3.23.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

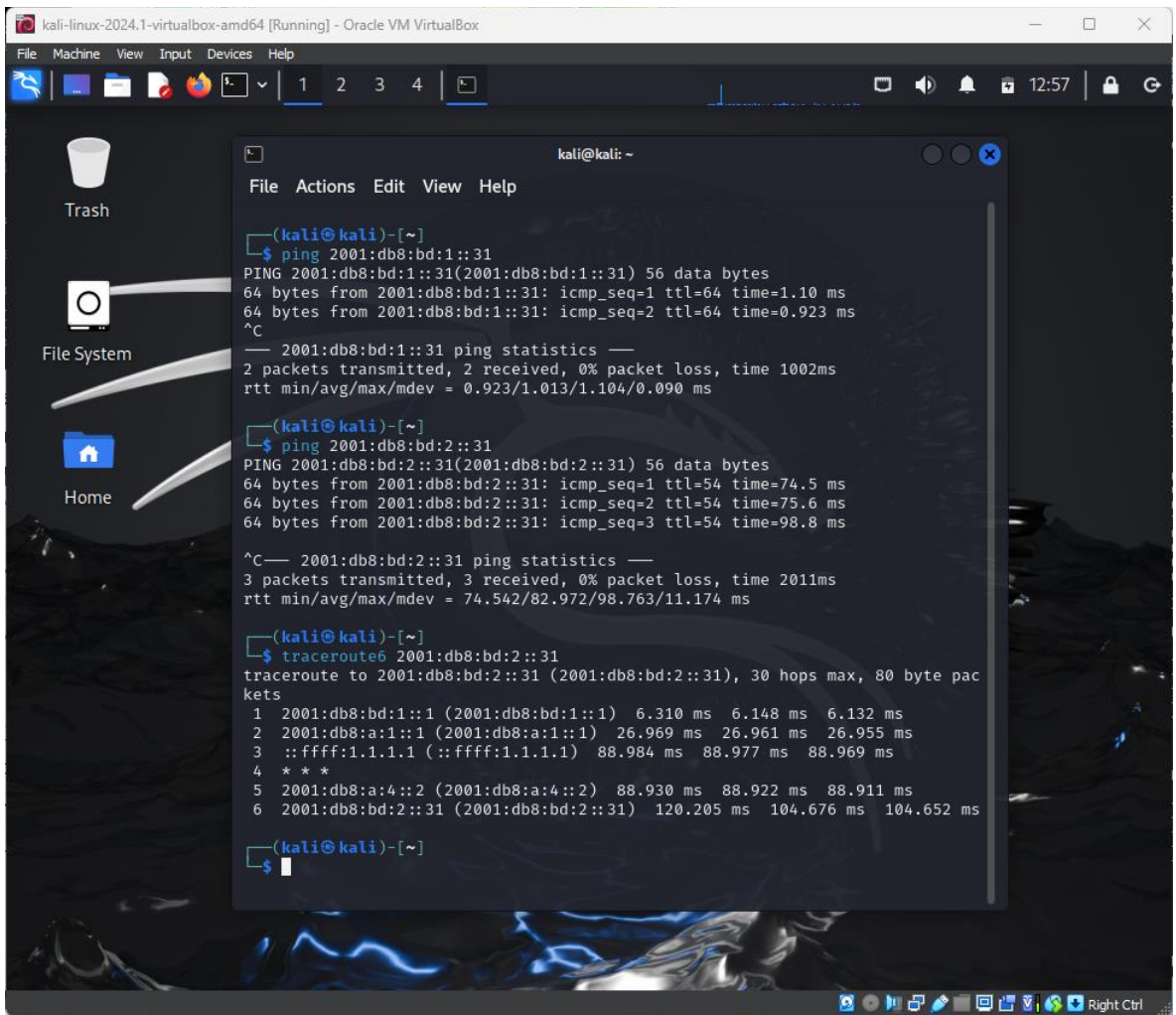


Рис. 3.23. Перевірка зв'язку та дослідження маршруту на робочій станції WS-1A-2

Так ми можемо побачити, що зв'язок між віддаленими підмережами працює коректно. А також дослідивши маршрут пакету, можна побачити що пакет дійшов до маршрутизатора R-CE-4 з адресою 2001:db8:a:4::2 і потім до нашої іншої робочої станції з адресою 2001:db8:bd:2::31.

Звернемося до Р та РЕ-маршрутизаторів та переглянемо інформацію про протоколи MPLS та BGP. Команди для перевірки роботи протоколу та результат їх виконання наведено на рисунках 3.24 та 3.25.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

```

R-PE-3#show bgp all
For address family: IPv4 Unicast

For address family: IPv6 Unicast

For address family: VPNv6 Unicast

BGP table version is 13, local router ID is 2.0.0.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

      Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 200:1 (default for vrf Sitel)
*>i 2001:DB8:A:1::/126
               ::FFFF:2.0.0.1             0      100      0 ?
*   2001:DB8:A:4::/126
               2001:DB8:A:4::2             0                   0 200 ?
*>
               ::                          0          32768 ?
*>i 2001:DB8:BD:1::/120
      Network          Next Hop          Metric LocPrf Weight Path
               ::FFFF:2.0.0.1             0      100      0 200 ?
*> 2001:DB8:BD:2::/120
               2001:DB8:A:4::2             0                   0 200 ?
*>i ABCD::1/128       ::FFFF:2.0.0.1             0      100      0 200 i
*> ABCD::4/128       2001:DB8:A:4::2             0                   0 200 i
Route Distinguisher: 400:1 (default for vrf Site3)
*   2001:DB8:A:5::/126
               2001:DB8:A:5::2             0                   0 400 ?
*>
               ::                          0          32768 ?
*> 2001:DB8:BD:2::/120
               2001:DB8:A:5::2             0                   0 400 ?
*> ABCD::5/128       2001:DB8:A:5::2             0                   0 400 i

For address family: IPv4 Multicast

R-PE-3#show mpls ldp neighbor
Peer LDP Ident: 1.0.0.1:0; Local LDP Ident 2.0.0.3:0
TCP connection: 1.0.0.1.646 - 2.0.0.3.57254
State: Oper; Msgs sent/rcvd: 48/49; Downstream
Up time: 00:32:00
LDP discovery sources:
  GigabitEthernet0/0, Src IP addr: 1.1.3.1
Addresses bound to peer LDP Ident:
  1.1.1.1          1.0.0.1          1.1.2.1          1.1.3.1
  1.1.4.1
R-PE-3#

```

Рис. 3.24. Перегляд інформації про роботу MPLS та BGP на маршрутизаторі R-PE-1

```

R-P-1#show mpls ip binding
 1.0.0.1/32
   in label:      imp-null
   out label:     16      lsr: 2.0.0.4:0
   out label:     19      lsr: 2.0.0.3:0
   out label:     18      lsr: 2.0.0.1:0
 1.1.1.0/30
   in label:      imp-null
   out label:     19      lsr: 2.0.0.4:0
   out label:     21      lsr: 2.0.0.3:0
   out label:     imp-null lsr: 2.0.0.1:0
 1.1.2.0/30
   in label:      imp-null
   out label:     18      lsr: 2.0.0.4:0
   out label:     20      lsr: 2.0.0.3:0
   out label:     19      lsr: 2.0.0.1:0
 1.1.3.0/30
   in label:      imp-null
   out label:     17      lsr: 2.0.0.4:0
   out label:     imp-null lsr: 2.0.0.3:0
   out label:     20      lsr: 2.0.0.1:0
 1.1.4.0/30
   in label:      imp-null
   out label:     imp-null lsr: 2.0.0.4:0
   out label:     22      lsr: 2.0.0.3:0
   out label:     21      lsr: 2.0.0.1:0
 2.0.0.1/32
   in label:      22
   out label:     18      lsr: 2.0.0.3:0
   out label:     imp-null lsr: 2.0.0.1:0      inuse
   out label:     21      lsr: 2.0.0.4:0
 2.0.0.3/32
   in label:      21
   out label:     imp-null lsr: 2.0.0.3:0      inuse
   out label:     22      lsr: 2.0.0.1:0
   out label:     20      lsr: 2.0.0.4:0
 2.0.0.4/32
   in label:      20
   out label:     imp-null lsr: 2.0.0.4:0      inuse
   out label:     17      lsr: 2.0.0.3:0
   out label:     17      lsr: 2.0.0.1:0
R-P-1#show mpls ldp neighbor
Peer LDP Ident: 2.0.0.4:0; Local LDP Ident 1.0.0.1:0
TCP connection: 2.0.0.4.15091 - 1.0.0.1.646
State: Oper; Msgs sent/rcvd: 48/46; Downstream
Up time: 00:32:23
LDP discovery sources:
  GigabitEthernet4/0, Src IP addr: 1.1.4.2
Addresses bound to peer LDP Ident:
  1.1.4.2      2.0.0.4
Peer LDP Ident: 2.0.0.3:0; Local LDP Ident 1.0.0.1:0
TCP connection: 2.0.0.3.57254 - 1.0.0.1.646
State: Oper; Msgs sent/rcvd: 48/46; Downstream
Up time: 00:32:12
LDP discovery sources:
  GigabitEthernet3/0, Src IP addr: 1.1.3.2
Addresses bound to peer LDP Ident:
  1.1.3.2      2.0.0.3
Peer LDP Ident: 2.0.0.1:0; Local LDP Ident 1.0.0.1:0
TCP connection: 2.0.0.1.43660 - 1.0.0.1.646
State: Oper; Msgs sent/rcvd: 46/73; Downstream
Up time: 00:32:11
LDP discovery sources:
  GigabitEthernet1/0, Src IP addr: 1.1.1.2
Addresses bound to peer LDP Ident:
  1.1.1.2      2.0.0.1
R-P-1#

```

Рис. 3.25. Перегляд інформації про MPLS на маршрутизаторі R-P-1

		Фомін В.В.		
		Покотило О.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

ККІКБ.КР.Б – 125 – 20 – ПЗ

Арк.

60

Після реалізації MPLS VPN, ми перейшли до налаштування комутаторів, а саме VLAN та Port-Security. Перевіримо як комутатор відреагує на порушення безпеки. Для цього підмінимо нашу робочу станцію у мережі Site 3 Lan-A іншою. Весь процес перевірки наведено на рисунках 3.26 – 3.29.

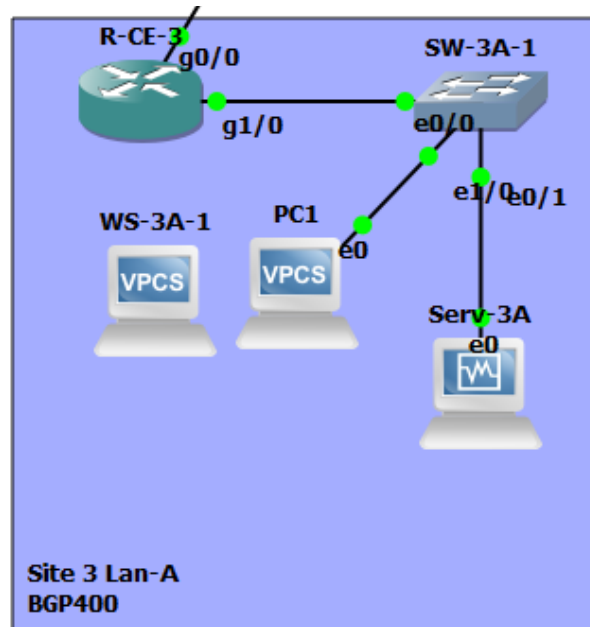


Рис. 3.26. Підміна робочої станції

```
*Jun  4 17:15:54.158: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0050.7966.6804 on port Ethernet1/0.
SW-3A-1#
*Jun  4 17:15:59.596: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0050.7966.6804 on port Ethernet1/0.
SW-3A-1#
```

Рис. 3.27. Реакція комутатора на порушення безпеки

```
PC1>
PC1> ip 2001:db8:bd:1::31/120 2001:db8:bd:1::1
PC1 : 2001:db8:bd:1::31/120

PC1> ping 2001:db8:bd:1::1

host (2001:db8:bd:1::1) not reachable

PC1>
```

Рис. 3.28. Підмінена робоча станція не має доступу до мережі

Як можна побачити, усі налаштування успішно спрацювали і підмінена робоча станція не змогла отримати доступ до мережі.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

```
WS-3C-1> ping 2001:db8:bd:1::1

2001:db8:bd:1::1 icmp6_seq=1 ttl=64 time=5.715 ms
2001:db8:bd:1::1 icmp6_seq=2 ttl=64 time=9.504 ms
2001:db8:bd:1::1 icmp6_seq=3 ttl=64 time=10.055 ms
2001:db8:bd:1::1 icmp6_seq=4 ttl=64 time=9.300 ms
2001:db8:bd:1::1 icmp6_seq=5 ttl=64 time=10.540 ms

WS-3C-1> █
```

Рис. 3.29. Коректна робоча станція має доступ до мережі

Після перепідключення коректної робочої станції вона одразу отримала доступ до мережі, отже усе працює правильно.

Переглянемо які повідомлення зв'явилися на нашому налаштованому Syslog-сервері. Приклад повідомлень Syslog наведено на рисунку 3.30.

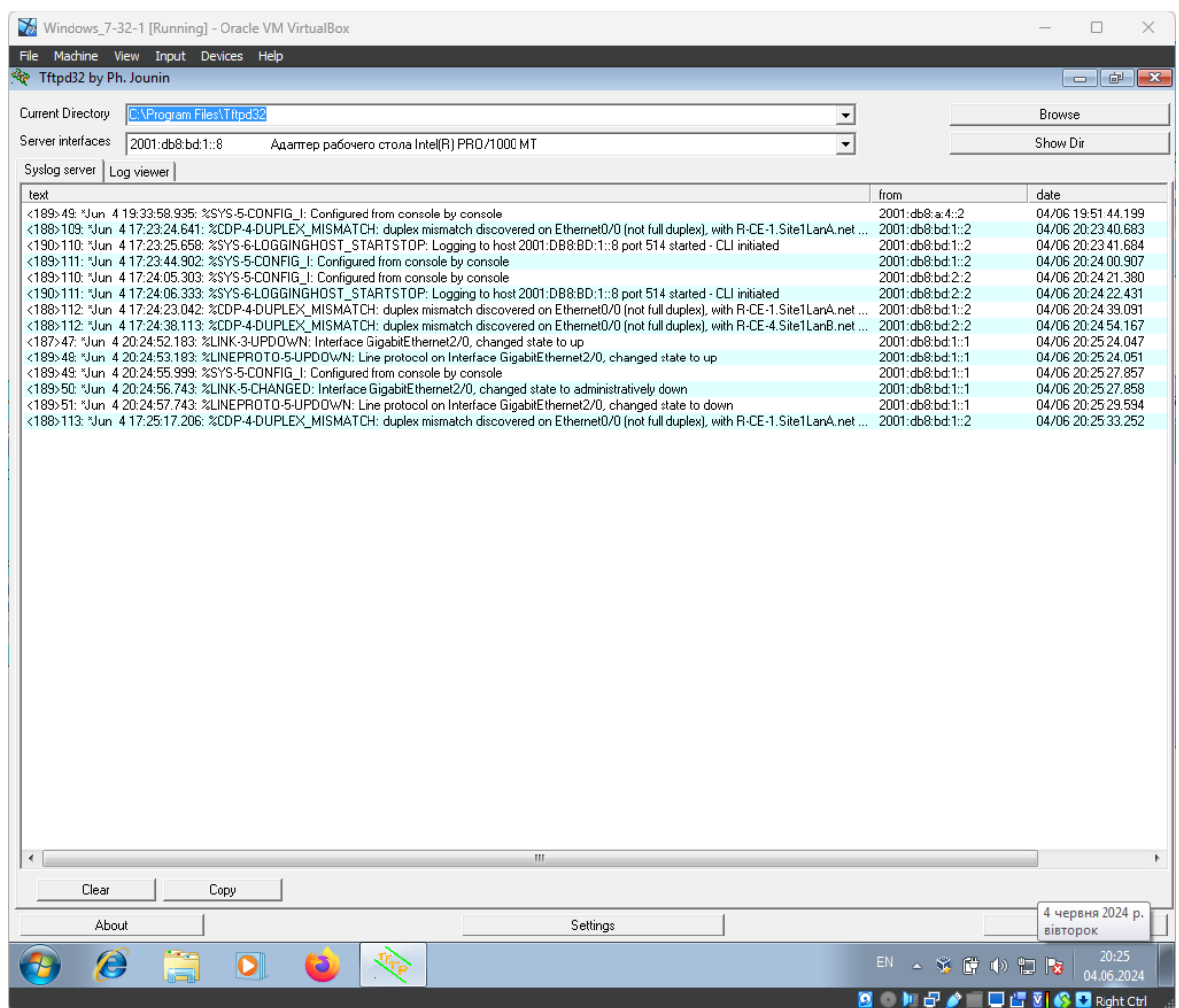


Рис. 3.30. Перегляд повідомлень на сервері Serv-1А

Повідомлення надходять як від маршрутизаторів та комутаторів власної підмережі так і від віддаленої підмережі, а отже все працює коректно. Переглянемо також чи працює NTP на маршрутизаторах та комутаторах. Команди для перевірки на результати їх виконання наведено на рисунках 3.31 та 3.32.

```
R-CE-1#show ntp status
Clock is synchronized, stratum 3, reference is 194.54.80.29
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**21
ntp uptime is 113600 (1/100 of seconds), resolution is 4000
reference time is EA0CCB1A.9858EFF5 (02:56:10.595 DST Fri Jun 7 2024)
clock offset is -13.3895 msec, root delay is 28.23 msec
root dispersion is 963.01 msec, peer dispersion is 439.13 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 64, last update was 69 sec ago.
R-CE-1#
```

Рис. 3.31. Перевірка роботи NTP на маршрутизаторі R-CE-1

```
SW-1A-1#show ntp status
Clock is synchronized, stratum 4, reference is 151.39.166.44
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**10
ntp uptime is 123900 (1/100 of seconds), resolution is 4000
reference time is EA0CCB6F.9A5E36E8 (02:57:35.603 EEST Fri Jun 7 2024)
clock offset is 20.3691 msec, root delay is 38.87 msec
root dispersion is 2429.60 msec, peer dispersion is 940.12 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000000 s/s
system poll interval is 64, last update was 75 sec ago.
SW-1A-1#
```

Рис. 3.32. Перевірка роботи NTP на маршрутизаторі SW-1A-1

NTP працює коректно, а отже можна йти далі. Останнім кроком перевіримо наші налаштовані засоби захисту, а саме: створених користувачів, доступ до привілейованого режиму за паролем, віддаленого підключення по SSH, яке повинно бути доступне лише з локальної підмережі. Перевірки створених користувачів наведено на рисунках 3.31 – 3.33. Перевірку підключення по SSH для маршрутизаторів та комутаторів наведено на рисунках 3.34 – 3.37.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

```

R-CE-4>en
Password:
R-CE-4#show run
Building configuration...

Current configuration : 2589 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

```

Рис. 3.31. Вхід у привілейований режим потребує пароль

```

R-CE-4>login
Username: Admin-Sitel-LanB
Password:
R-CE-4#?
Exec commands:
  access-enable      Create a temporary Access-List entry
  access-profile     Apply user-profile to interface
  access-template    Create a temporary Access-List entry
  alps               ALPS exec commands
  archive            manage archive files
  audio-prompt       load ivr prompt
  auto               Exec level Automation
  beep               Blocks Extensible Exchange Protocol commands
  bfe                For manual emergency modes setting
  calendar            Manage the hardware calendar
  call               Voice call
  call-home           Call-Home commands
  cd                  Change current directory
  clear              Reset functions
  clock              Manage the system clock
  cns                CNS agents
  configure           Enter configuration mode
  connect             Open a terminal connection
  copy                Copy from one file to another
  crypto              Encryption related commands.
  dcm                Data Collection Manager
--More--

```

Рис. 3.32. Перевірка рівню доступу користувача Admin

```
R-CE-4>login
Username: User-Sitel-LanB
Password:
R-CE-4>?
Exec commands:
  access-enable      Create a temporary Access-List entry
  access-profile     Apply user-profile to interface
  clear              Reset functions
  connect            Open a terminal connection
  crypto             Encryption related commands.
  disable            Turn off privileged commands
  disconnect         Disconnect an existing network connection
  do-exec            Mode-independent "do-exec" prefix support
  emm                Run a configured Menu System
  enable             Turn on privileged commands
  ethernet           Ethernet parameters
  exit              Exit from the EXEC
  help              Description of the interactive help system
  ips                Intrusion Prevention System
  lat                Open a lat connection
  lig                LISP Internet Groper
  lock               Lock the terminal
  login              Log in as a particular user
  logout            Exit from the EXEC
  mrinfo             Request neighbor and version information from a multicast router
  mstat             Show statistics after multiple multicast traceroutes
  mtrace            Trace reverse multicast path from destination to source
  name-connection   Name an existing network connection
--More--
```

Рис. 3.33. Перевірка рівню доступу користувача User

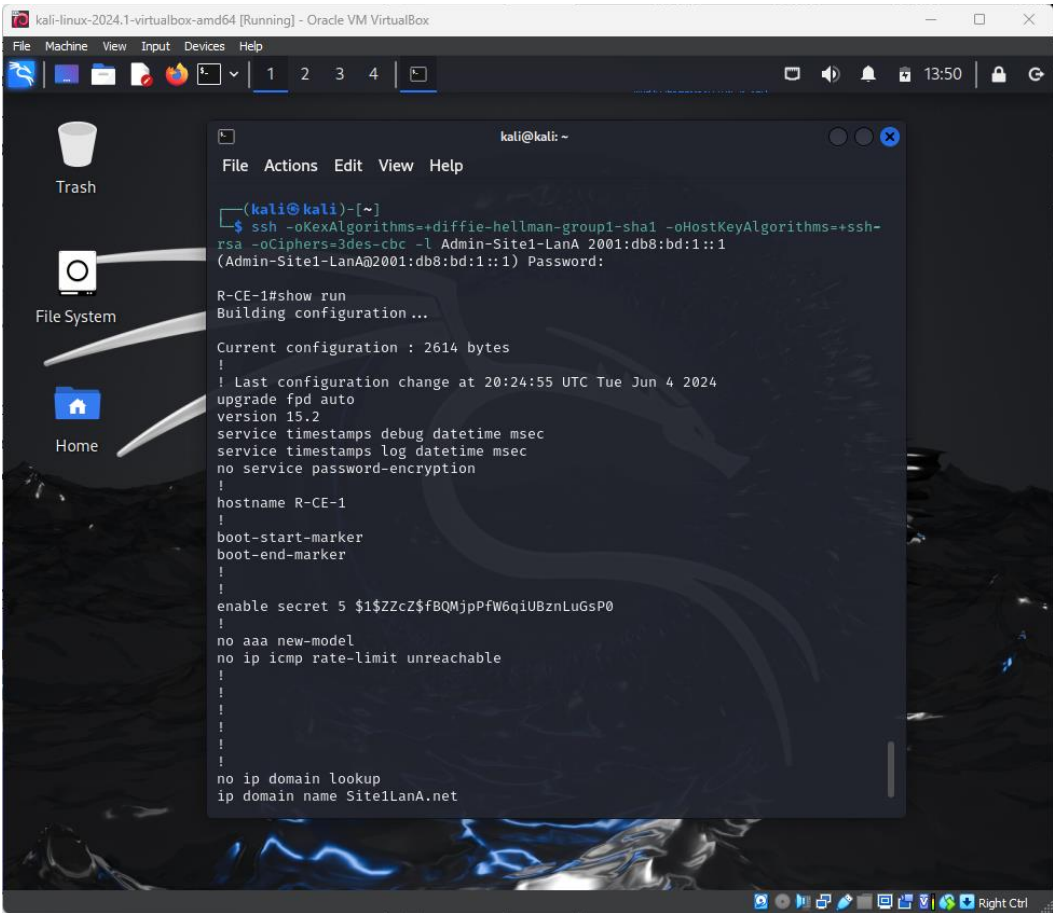


Рис. 3.34. Підключення до R-CE-1 по SSH з робочої станції власної підмережі

```
(kali㉿kali)-[~]  
$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa -oCiphers=3des-cbc -l Admin-Site1-LanB 2001:db8:bd:2::1  
ssh: connect to host 2001:db8:bd:2::1 port 22: Connection refused
```

Рис. 3.35. Підключення по SSH до віддаленої мережі заблоковано

Після виконання даних перевірок можна дійти висновку, що усі підключення по SSH до маршрутизаторів працює коректно.

Варто також перевірити підключення до комутаторів мережі.

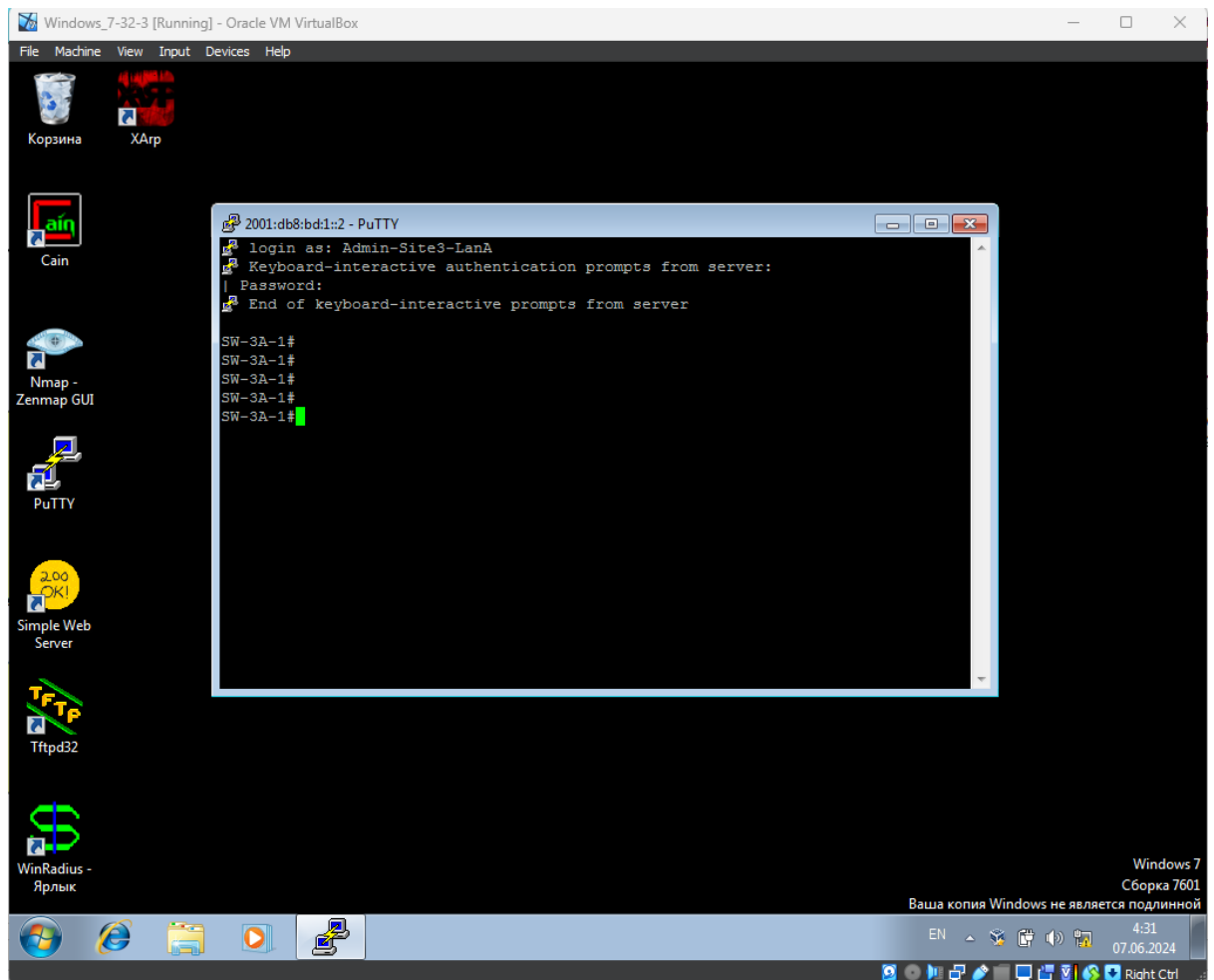


Рис. 3.36. Підключення до комутатора власної підмережі працює

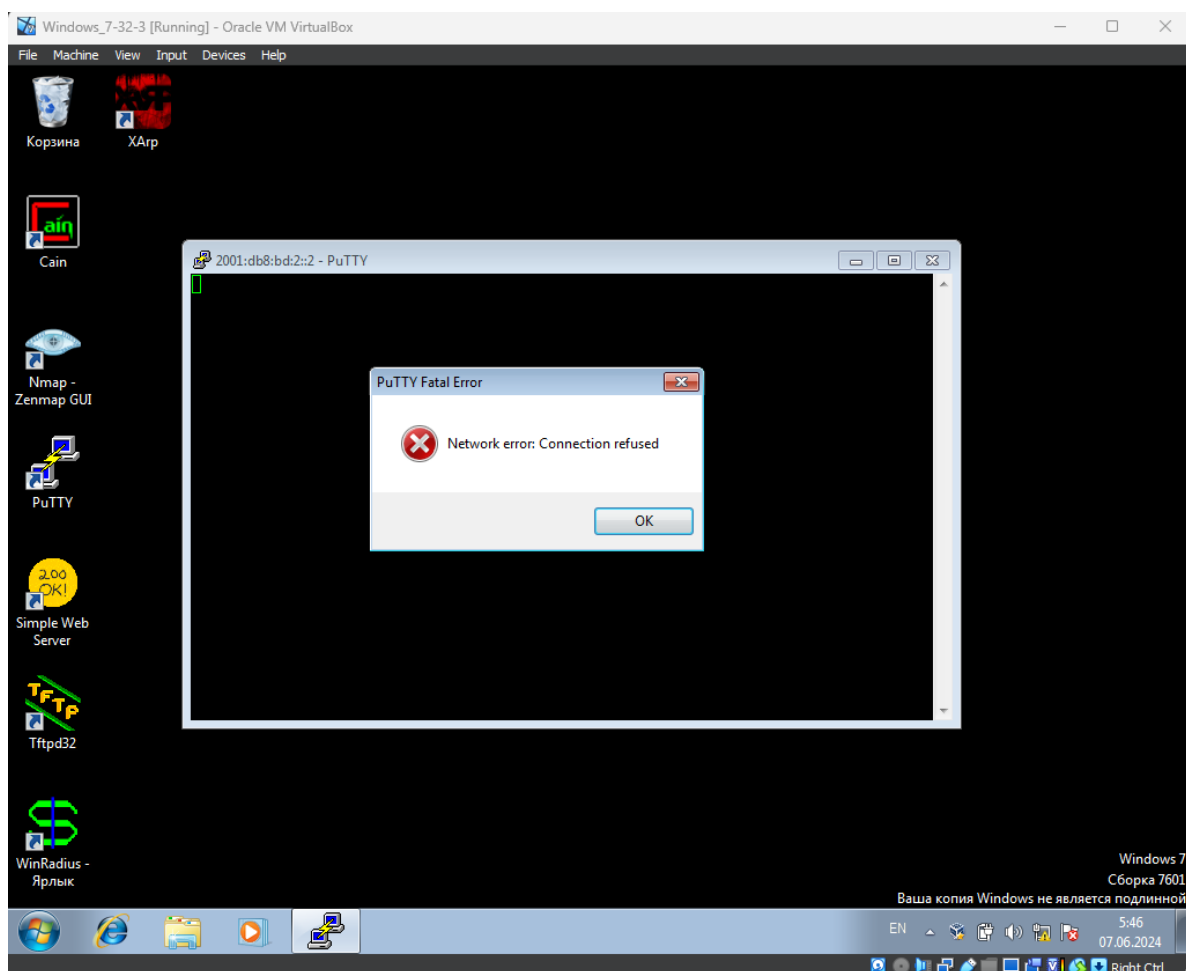


Рис. 3.37. Підключення до комутатора віддаленої мережі блокується

Отже, усі перевірки пройшли успішно: пристрої потребують вводу паролю для входу в привілейований режим, користувачі мають різні рівні доступу, доступ по SSH доступний лише для власних підмереж, а усі віддалені підключення блокуються за допомогою списків контролів доступу. Отже можна дійти висновку, що все працює успішно.

Висновки до третього розділу: Протягом даного розділу було виконано вибір обладнання для мережі, визначено ОС та програмне забезпечення для серверу підмережі. Після вибору обладнання, ОС та ПЗ було налаштовано усі раніше спроектовані протоколи та прикладні сервіси. Також була здійснена перевірка роботи усіх налаштувань та пристроїв.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

ВИСНОВКИ

Під час розробки даної кваліфікаційної роботи було досліджено роботу MPLS VPN, а також спроектовано захищену корпоративну IPv4/IPv6 мережу з використанням даної технології.

Створена мережа має 11 маршрутизаторів та 6 комутаторів з можливістю розширення, а також щонайменше 3 сервери та 24 робочі станції.

Протягом першого розділу було досліджено принципи побудови та функціонування MPLS VPN, визначено відмінності між MPLS його альтернативами; досліджено технології необхідні для реалізації MPLS VPN: протокол граничного шлюзу (BGP) та віртуальну маршрутизацію та переадресацію (VRF).

Другий розділ складається з проєктування загальної корпоративної мережі та її підмереж-філіалів, її параметрів IP-адресації, а також технологій що використовуватимуться для підключення усіх пристроїв мережі. Було виконано вибір служб та сервісів прикладного рівня, що використовуватиметься у мережі. Забезпечено проєктування підсистеми мережного захисту.

У третьому розділі кваліфікаційної роботи було проведено вибір обладнання, здійснено побудову, налагодження та тестування проєктованої корпоративної мережі. В якості маршрутизаторів використовувалися Cisco 7200 Series, комутаторів – Cisco Catalyst 2960, операційна система сервера – Windows 7, а в якості програмного забезпечення для налаштування Syslog-серверу було вибрано TFTP32.

Результатом виконання даної кваліфікаційної роботи стали поглиблені теоретичні знання про використання IPv6, MPLS VPN та всі пов'язані технології, а також здобуто навички проєктування та реалізації захищених корпоративних мереж. Спроектована підсистема захисту корпоративної IPv4/IPv6 мережі, може буде використана у житті.

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is IPv6 [Електронний ресурс] / GeeksForGeeks – 2024. – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/what-is-ipv6/>
2. Internet Protocol version 6 (IPv6) [Електронний ресурс] / GeeksForGeeks – 2024. – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/internet-protocol-version-6-ipv6/>
3. What is MPLS? [Електронний ресурс] / CATO Networks – 2024 – Режим доступу до ресурсу: <https://www.catonetworks.com/what-is-mpls/>
4. What is MPLS? [Електронний ресурс] / Cloudflare – 2024 - Режим доступу до ресурсу: <https://www.cloudflare.com/learning/network-layer/what-is-mpls/>
5. Multi Protocol Label Switching (MPLS) [Електронний ресурс] / GeeksForGeeks – 2024. – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/multi-protocol-label-switching-mpls/>
6. How does Multiprotocol Label Switching (MPLS) Routing work ? [Електронний ресурс] / GeeksForGeeks – 2024. – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/how-does-multiprotocol-label-switching-mpls-routing-work/>
7. Курси CCNAv7: Switching, Routing, and Wireless Essentials та CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс] / Cisco – 2024. – Режим доступу до ресурсу: <https://www.netacad.com/portal/learning>
8. Border Gateway Protocol (BGP) [Електронний ресурс] / GeeksForGeeks – 2024. – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/border-gateway-protocol-bgp/>
9. What is VPN? [Електронний ресурс] / Cloudflare – 2024 - Режим доступу до ресурсу: <https://www.cloudflare.com/learning/access-management/what-is-a-vpn/>

		Фомін В.В.			ККІКБ.КР.Б – 125 – 20 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

10. Configure a Basic MPLS VPN / Cisco – 2024. – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/13733-mpls-vpn-basic.html>
11. Difference between Virtual Private Network (VPN) and Multi-Protocol Label Switching (MPLS) [Електронний ресурс] / GeeksForGeeks – 2024. – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/difference-between-virtual-private-network-vpn-and-multi-protocol-label-switching-mpls/>
12. MPLS: Layer 3 VPNs Configuration Guide, Cisco IOS Release 15M&T Chapter: Multiprotocol BGP MPLS VPN [Електронний ресурс] / Cisco – 2024. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/mp-bgp-mpls-vpn.html
13. MPLS: Layer 3 VPNs Configuration Guide, Cisco IOS Release 15M&T Chapter: IPv6 VPN over MPLS [Електронний ресурс] / Cisco – 2024. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-mt/mp-l3-vpns-15-mt-book/ip6-mpls-6vpn.html

ДОДАТКИ

					ККІКБ.КР.Б – 125 – 21 – ПЗ					
Змн.	Арк.	№ докум.	Підпис	Дата	Проект захищеної корпоративної мережі			Літ.	Арк.	Аркушів
Розроб.		Фомін В.В.								
Керівник		Покотило О.А.							4	61
Реценз.								ФІКТ Гр. КБ-20-1[2]		
Н. контр.										
Затверд.		Єфіменко А.А.								

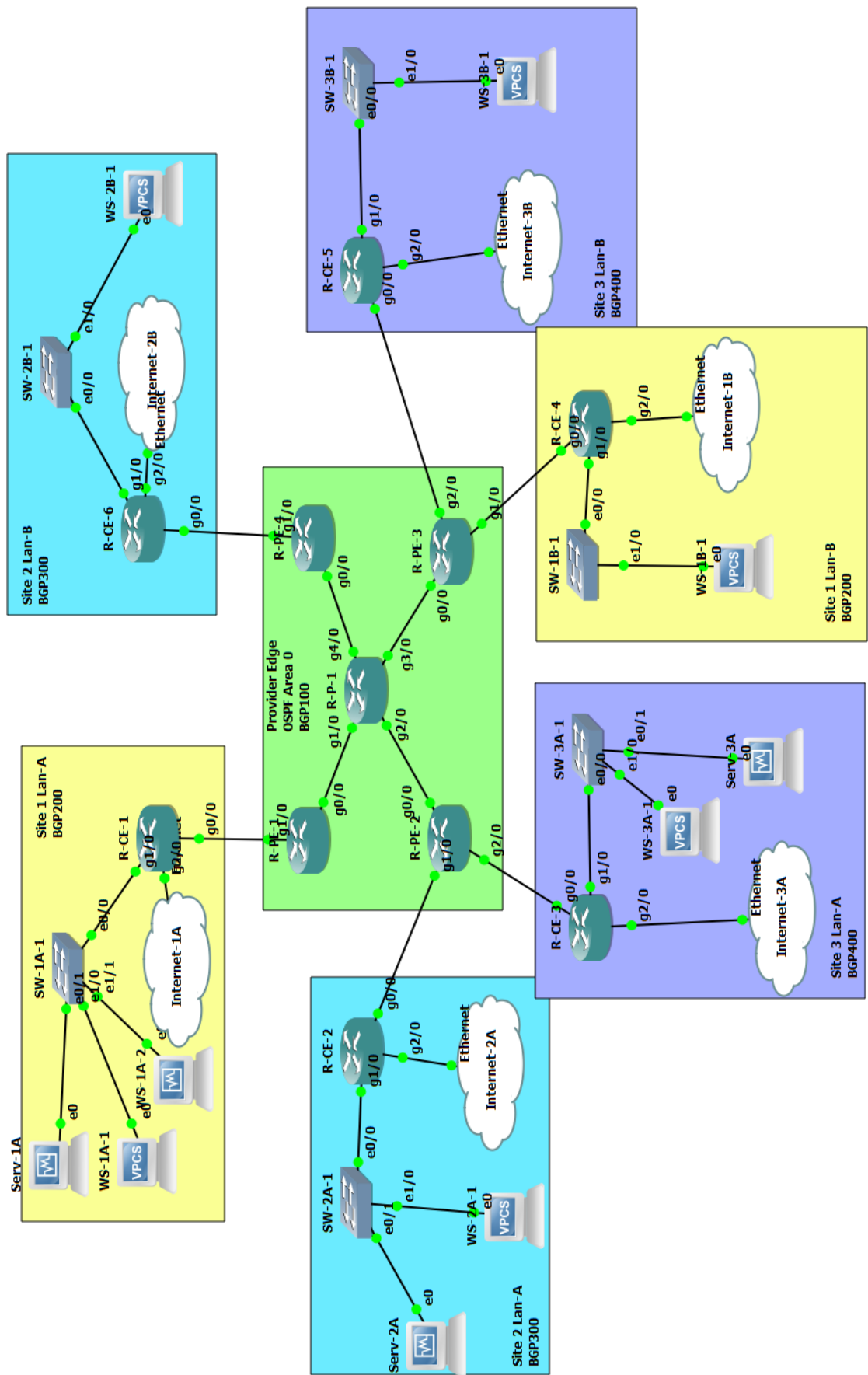


Рис. А.1. Проєкт мережі

ДОДАТОК В

Нижче представлені конфігураційні файли пристроїв мережі

R-P-1	!	ip address 1.0.0.1
!	no ip domain lookup	255.255.255.255
!	ip cef	!
!	no ipv6 cef	interface FastEthernet0/0
!	!	no ip address
!	multilink bundle-name	shutdown
!	authenticated	duplex half
!	mpls label protocol ldp	!
	!	interface GigabitEthernet1/0
!	!	ip address 1.1.1.1
	!	255.255.255.252
! Last configuration change at	!	negotiation auto
02:56:01 UTC Tue Jun 4 2024	!	mpls ip
upgrade fpd auto	!	!
version 15.2	!	interface GigabitEthernet2/0
service timestamps debug	!	ip address 1.1.2.1
datetime msec	!	255.255.255.252
service timestamps log datetime	!	negotiation auto
msec	!	mpls ip
no service password-encryption	!	!
!	redundancy	interface GigabitEthernet3/0
hostname R-P-1	!	ip address 1.1.3.1
!	ip tcp synwait-time 5	255.255.255.252
boot-start-marker	!	negotiation auto
boot-end-marker	!	mpls ip
!	!	!
!	!	interface GigabitEthernet4/0
!	!	ip address 1.1.4.1
no aaa new-model	!	255.255.255.252
no ip icmp rate-limit unreachable	!	negotiation auto
!	!	mpls ip
!	!	!
!	!	router ospf 1
!	!	mpls ldp autoconfig
!	interface Loopback0	network 1.0.0.1 0.0.0.0 area 0

network 1.1.1.0 0.0.0.3 area 0	privilege level 15	address-family ipv6
network 1.1.2.0 0.0.0.3 area 0	logging synchronous	route-target export 200:1
network 1.1.3.0 0.0.0.3 area 0	stopbits 1	route-target import 200:1
network 1.1.4.0 0.0.0.3 area 0	line vty 0 4	exit-address-family
!	login	!
ip forward-protocol nd	transport input all	enable secret 5
no ip http server	!	\$1\$v5Bw\$n.iV0qrpNNJLW9K.5r
no ip http secure-server	!	xKB1
!	end	!
!		no aaa new-model
!	R-PE-1	no ip icmp rate-limit unreachable
no cdp log mismatch duplex	!	!
!	!	!
!	!	!
mpls ldp router-id Loopback0	!	!
!		!
control-plane	!	no ip domain lookup
!	! Last configuration change at	ip cef
!	00:46:01 UTC Fri Jun 7 2024	ipv6 unicast-routing
!	upgrade fpd auto	ipv6 cef
mgcp profile default	version 15.2	!
!	service timestamps debug	
!	datetime msec	multilink bundle-name
!	service timestamps log datetime	authenticated
!	msec	mpls label protocol ldp
gatekeeper	no service password-encryption	!
shutdown	!	!
!	hostname R-PE-1	!
!	!	!
line con 0	boot-start-marker	!
exec-timeout 0 0	boot-end-marker	!
privilege level 15	!	!
logging synchronous	!	!
stopbits 1	vrf definition Site1	!
line aux 0	rd 200:1	username Admin-PE-1 privilege
exec-timeout 0 0	!	15 secret 5
		\$1\$soZ2\$B0DwSyrrIaQu59dbvy
		PQE1

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		74

username User-PE-1 secret 5
\$1\$Rr2Q\$uqx8G2wnw4QVoteZ
yGDU1

!

redundancy

!

!

ip tcp synwait-time 5

!

!

!

!

!

!

!

!

!

!

interface Loopback0

ip address 2.0.0.1
255.255.255.255

!

interface Ethernet0/0

no ip address

shutdown

duplex auto

!

interface GigabitEthernet0/0

ip address 1.1.1.2
255.255.255.252

duplex full

speed 1000

media-type gbic

negotiation auto

mpls ip

!

interface GigabitEthernet1/0

vrf forwarding Site1

no ip address

negotiation auto

ipv6 address
2001:DB8:A:1::1/126

!

interface GigabitEthernet2/0

no ip address

shutdown

negotiation auto

!

interface GigabitEthernet3/0

no ip address

shutdown

negotiation auto

!

interface GigabitEthernet4/0

no ip address

shutdown

negotiation auto

!

interface GigabitEthernet5/0

no ip address

shutdown

negotiation auto

!

interface GigabitEthernet6/0

no ip address

shutdown

negotiation auto

!

router ospf 1

network 1.1.1.0 0.0.0.3 area 0

network 2.0.0.1 0.0.0.0 area 0

!

router bgp 100

bgp log-neighbor-changes

no bgp default ipv4-unicast

neighbor 2.0.0.2 remote-as 100

neighbor 2.0.0.2 update-source
Loopback0

neighbor 2.0.0.3 remote-as 100

neighbor 2.0.0.3 update-source
Loopback0

neighbor 2.0.0.4 remote-as 100

neighbor 2.0.0.4 update-source
Loopback0

!

address-family ipv4

exit-address-family

!

address-family ipv6

neighbor 2.0.0.2 activate

neighbor 2.0.0.2 send-label

neighbor 2.0.0.3 activate

neighbor 2.0.0.3 send-label

neighbor 2.0.0.4 activate

neighbor 2.0.0.4 send-label

exit-address-family

!

address-family vpnv6

neighbor 2.0.0.2 activate

neighbor 2.0.0.2 send-
community extended

neighbor 2.0.0.3 activate

neighbor 2.0.0.3 send-
community extended

neighbor 2.0.0.4 activate

neighbor 2.0.0.4 send-
community extended

exit-address-family

!

address-family ipv6 vrf Site1

redistribute connected

Фомін В.В.

Покотило О.А.

№ докум.

Підпис

Дата

ККІКБ.КР.Б – 125 – 21 – ПЗ

Арк.

75

neighbor 2001:DB8:A:1::2 remote-as 200	line aux 0	route-target export 300:1
	exec-timeout 0 0	route-target import 300:1
neighbor 2001:DB8:A:1::2 activate	privilege level 15	exit-address-family
neighbor 2001:DB8:A:1::2 as- override	logging synchronous	!
	stopbits 1	vrf definition Site3
exit-address-family	line vty 0 4	rd 400:1
!	login	!
ip forward-protocol nd	transport input all	address-family ipv6
no ip http server	!	route-target export 400:1
no ip http secure-server	!	route-target import 400:1
!	end	exit-address-family
!	R-PE-2	!
!	!	enable secret 5
no cdp log mismatch duplex	!	\$1\$eB/J\$aLD7baZpF7QoCemigoJ p/0
!		!
!	!	no aaa new-model
mpls ldp router-id Loopback0 force	! Last configuration change at 05:44:11 UTC Fri Jun 7 2024	no ip icmp rate-limit unreachable
!	upgrade fpd auto	!
control-plane	version 15.2	!
!	service timestamps debug	!
!	datetime msec	!
!	service timestamps log datetime msec	!
mgcp profile default	no service password-encryption	!
!	!	no ip domain lookup
!	hostname R-PE-2	ip cef
!	!	ipv6 unicast-routing
gatekeeper	boot-start-marker	ipv6 cef
shutdown	boot-end-marker	!
!	!	multilink bundle-name authenticated
!	!	mpls label protocol ldp
line con 0	vrf definition Site2	!
exec-timeout 0 0	rd 300:1	!
privilege level 15	!	!
logging synchronous	address-family ipv6	!
stopbits 1		

!	ip address 1.1.2.2	!
!	255.255.255.252	interfa ce GigabitEthernet6/0
!	duplex full	no ip address
!	speed 1000	shutdown
!	media-type gbic	negotiation auto
username Admin-PE-2 privilege	negotiation auto	!
15 secret 5	mpls ip	router ospf 1
\$1\$F/0i\$iDK3cQi0eKdItG4lcwu	!	network 1.1.2.0 0.0.0.3 area 0
8p0	interfa ce GigabitEthernet1/0	network 2.0.0.2 0.0.0.0 area 0
username User-PE-2 secret 5	vrf forwarding Site2	!
\$1\$mXQq\$QR.UDV9TP8AhgkU	no ip address	router bgp 100
AuxmDv.	negotiation auto	bgp log-neighbor-changes
!	ipv6 address	no bgp default ipv4-unicast
redundancy	2001:DB8:A:2::1/126	neighbor 2.0.0.1 remote-as 100
!	!	neighbor 2.0.0.1 update-source
ip tcp synwait-time 5	interfa ce GigabitEthernet2/0	Loopback0
!	vrf forwarding Site3	neighbor 2.0.0.3 remote-as 100
!	no ip address	neighbor 2.0.0.3 update-source
!	negotiation auto	Loopback0
!	ipv6 address	neighbor 2.0.0.4 remote-as 100
!	2001:DB8:A:3::1/126	neighbor 2.0.0.4 update-source
!	!	Loopback0
!	interfa ce GigabitEthernet3/0	!
!	no ip address	address-family ipv4
!	shutdown	exit-address-family
!	negotiation auto	!
!	!	address-family ipv6
interfa ce Loopback0	interfa ce GigabitEthernet4/0	neighbor 2.0.0.1 activate
ip address 2.0.0.2	no ip address	neighbor 2.0.0.1 send-label
255.255.255.255	shutdown	neighbor 2.0.0.3 activate
!	negotiation auto	neighbor 2.0.0.3 send-label
interfa ce Ethernet0/0	!	neighbor 2.0.0.4 activate
no ip address	interfa ce GigabitEthernet5/0	neighbor 2.0.0.4 send-label
shutdown	no ip address	exit-address-family
duplex auto	shutdown	!
!	negotiation auto	address-family vpnv6
interfa ce GigabitEthernet0/0		

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

```

neighbor 2.0.0.1 activate                !                !
neighbor 2.0.0.1 send-community extended mpls ldp router-id Loopback0 force !
neighbor 2.0.0.3 activate                !                !
neighbor 2.0.0.3 send-community extended control-plane                ! Last configuration change at
                                         !                00:33:38 UTC Fri Jun 7 2024
neighbor 2.0.0.4 activate                !                upgrade fpd auto
neighbor 2.0.0.4 send-community extended !                version 15.2
exit-address-family                      mgcp profile default        service timestamps debug
!                                         !                datetime msec
address-family ipv6 vrf Site2            !                service timestamps log datetime
redistribute connected                  !                msec
neighbor 2001:DB8:A:2::2                 gatekeeper                no service password-encryption
remote-as 300                           shutdown                   !
neighbor 2001:DB8:A:2::2                 !                          hostname R-PE-3
activate                               !                          !
neighbor 2001:DB8:A:2::2 as-override    !                          boot-start-marker
exit-address-family                     line con 0                boot-end-marker
!                                       exec-timeout 0 0         !
address-family ipv6 vrf Site3            privilege level 15        !
redistribute connected                  logging synchronous      vrf definition Site1
neighbor 2001:DB8:A:3::2                 stopbits 1              rd 200:1
remote-as 400                           line aux 0                !
neighbor 2001:DB8:A:3::2                 exec-timeout 0 0        address-family ipv6
activate                               privilege level 15        route-target export 200:1
neighbor 2001:DB8:A:3::2 as-override    logging synchronous      route-target import 200:1
exit-address-family                     stopbits 1              exit-address-family
!                                       line vty 0 4            !
ip forward-protocol nd                  login                    vrf definition Site3
no ip http server                       transport input all      rd 400:1
no ip http secure-server                !                          !
!                                       !                          address-family ipv6
!                                       !                          route-target export 400:1
!                                       !                          route-target import 400:1
no cdp log mismatch duplex              end                      exit-address-family
!                                       R-PE-3                  !
                                         !                          !

```

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		78

enable secret 5	!	ipv6 address
\$1\$0k4d\$eqDnHLbCZrDAj8gq8	!	2001:DB8:A:4::1/126
2vqH0	!	
!	ip tcp synwait-time 5	!
no aaa new-model	!	interface GigabitEthernet2/0
no ip icmp rate-limit unreachable	!	vrf forwarding Site3
!	!	no ip address
!	!	negotiation auto
!	!	ipv6 address
!	!	2001:DB8:A:5::1/126
!	!	!
!	!	interface GigabitEthernet3/0
!	!	no ip address
no ip domain lookup	!	shutdown
ip cef	!	negotiation auto
ipv6 unicast-routing	interface Loopback0	!
ipv6 cef	ip address 2.0.0.3	interface GigabitEthernet4/0
!	255.255.255.255	no ip address
	!	shutdown
multilink bundle-name	interface Ethernet0/0	negotiation auto
authenticated	no ip address	!
mpls label protocol ldp	shutdown	interface GigabitEthernet5/0
!	duplex auto	no ip address
!	!	shutdown
!	interface GigabitEthernet0/0	negotiation auto
!	ip address 1.1.3.2	!
!	255.255.255.252	interface GigabitEthernet6/0
!	duplex full	no ip address
!	speed 1000	shutdown
!	media-type gbic	negotiation auto
!	negotiation auto	!
username Admin-PE-3 privilege	mpls ip	router ospf 1
15 secret 5	!	network 1.1.3.0 0.0.0.3 area 0
\$1\$DXpz\$GwgXf9ZmR85E1lbD		network 2.0.0.3 0.0.0.0 area 0
wqtYE1	interface GigabitEthernet1/0	!
username User-PE-3 secret 5	vrf forwarding Site1	router bgp 100
\$1\$ff/H\$lwHz8AmSknQ2U7PPE	no ip address	bgp log-neighbor-changes
JhBw/	negotiation auto	
!		
redundancy		

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

no bgp default ipv4-unicast	neighbor 2001:DB8:A:4::2 remote-as 200	gatekeeper shutdown
neighbor 2.0.0.1 remote-as 100	neighbor 2001:DB8:A:4::2 activate	!
neighbor 2.0.0.1 update-source Loopback0	neighbor 2001:DB8:A:4::2 as- override	!
neighbor 2.0.0.2 remote-as 100	exit-address-family	line con 0
neighbor 2.0.0.2 update-source Loopback0	!	exec-timeout 0 0
neighbor 2.0.0.4 remote-as 100	address-family ipv6 vrf Site3	privilege level 15
neighbor 2.0.0.4 update-source Loopback0	redistribute connected	logging synchronous
!	neighbor 2001:DB8:A:5::2 remote-as 400	stopbits 1
address-family ipv4	neighbor 2001:DB8:A:5::2 activate	line aux 0
exit-address-family	neighbor 2001:DB8:A:5::2 activate	exec-timeout 0 0
!	neighbor 2001:DB8:A:5::2 as- override	privilege level 15
address-family ipv6	exit-address-family	logging synchronous
neighbor 2.0.0.1 activate	!	stopbits 1
neighbor 2.0.0.1 send-label	ip forward-protocol nd	line vty 0 4
neighbor 2.0.0.2 activate	no ip http server	login
neighbor 2.0.0.2 send-label	no ip http secure-server	transport input all
neighbor 2.0.0.4 activate	!	!
neighbor 2.0.0.4 send-label	!	end
exit-address-family	!	
!	!	R-PE-4
address-family vpnv6	no cdp log mismatch duplex	!
neighbor 2.0.0.1 activate	!	!
neighbor 2.0.0.1 send- community extended	!	!
neighbor 2.0.0.2 activate	mpls ldp router-id Loopback0 force	!
neighbor 2.0.0.2 send- community extended	!	!
neighbor 2.0.0.4 activate	control-plane	!
neighbor 2.0.0.4 send- community extended	!	! Last configuration change at 00:25:03 UTC Fri Jun 7 2024
exit-address-family	!	upgrade fpd auto
!	mgcp profile default	version 15.2
address-family ipv6 vrf Site1	!	service timestamps debug datetime msec
redistribute connected	!	service timestamps log datetime msec
	!	

no service password-encryption	!	duplex auto
!	!	!
hostname R-PE-4	!	interface GigabitEthernet0/0
!	!	ip address 1.1.4.2
boot-start-marker	!	255.255.255.252
boot-end-marker	!	duplex full
!	!	speed 1000
!	!	media-type gbic
vrf definition Site2	!	negotiation auto
rd 300:1	username Admin-PE-4 privilege	mpls ip
!	15 secret 5	!
address-family ipv6	\$1\$7Gph\$HhjYKsE8x3T64XPN	interface GigabitEthernet1/0
	99ooR/	vrf forwarding Site2
route-target export 300:1	username User-PE-4 secret 5	no ip address
route-target import 300:1	\$1\$KnHF\$DK8Mv88XcZOSjPR	negotiation auto
exit-address-family	LjYbQX/	ipv6 address
!	!	2001:DB8:A:6::1/126
enable secret 5	!	!
\$1\$../n\$deqmXRS8ylorXUiXBG	!	interface GigabitEthernet2/0
cFn/	!	no ip address
!	ip tcp synwait-time 5	shutdown
no aaa new-model	!	negotiation auto
no ip icmp rate-limit unreachable	!	!
!	!	interface GigabitEthernet3/0
!	!	no ip address
!	!	shutdown
!	!	negotiation auto
!	!	!
no ip domain lookup	!	interface GigabitEthernet4/0
ip cef	!	no ip address
ipv6 unicast-routing	interface Loopback0	shutdown
ipv6 cef	ip address 2.0.0.4	negotiation auto
!	255.255.255.255	!
	!	
multilink bundle-name	interface Ethernet0/0	interface GigabitEthernet5/0
authenticated		no ip address
mpls label protocol ldp	no ip address	shutdown
	shutdown	

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

negotiation auto	address-family vpnv6	mgcp profile default
!	neighbor 2.0.0.1 activate	!
interface GigabitEthernet6/0	neighbor 2.0.0.1 send-community extended	!
no ip address	neighbor 2.0.0.2 activate	!
shutdown	neighbor 2.0.0.2 send-community extended	gatekeeper
negotiation auto	neighbor 2.0.0.3 activate	shutdown
!	neighbor 2.0.0.3 send-community extended	!
router ospf 1	exit-address-family	!
network 1.1.4.0 0.0.0.3 area 0	!	line con 0
network 2.0.0.4 0.0.0.0 area 0	address-family ipv6 vrf Site2	exec-timeout 0 0
!	redistribute connected	privilege level 15
router bgp 100	neighbor 2001:DB8:A:6::2 remote-as 300	logging synchronous
bgp log-neighbor-changes	neighbor 2001:DB8:A:6::2 activate	stopbits 1
no bgp default ipv4-unicast	neighbor 2001:DB8:A:6::2 as-override	line aux 0
neighbor 2.0.0.1 remote-as 100	exit-address-family	exec-timeout 0 0
neighbor 2.0.0.1 update-source Loopback0	!	privilege level 15
neighbor 2.0.0.2 remote-as 100	ip forward-protocol nd	logging synchronous
neighbor 2.0.0.2 update-source Loopback0	no ip http server	stopbits 1
neighbor 2.0.0.3 remote-as 100	no ip http secure-server	line vty 0 4
neighbor 2.0.0.3 update-source Loopback0	!	login
!	!	transport input all
address-family ipv4	!	!
exit-address-family	!	end
!	no cdp log mismatch duplex	R-CE-1
address-family ipv6	!	!
neighbor 2.0.0.1 activate	!	!
neighbor 2.0.0.1 send-label	mpls ldp router-id Loopback0 force	!
neighbor 2.0.0.2 activate	!	! Last configuration change at 08:20:10 EEST Fri Jun 7 2024
neighbor 2.0.0.2 send-label	control-plane	upgrade fpd auto
neighbor 2.0.0.3 activate	!	version 15.2
neighbor 2.0.0.3 send-label	!	service timestamps debug
exit-address-family	!	datetime msec
!	!	

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

service timestamps log datetime msec	multilink bundle-name authenticated	ipv6 address ABCD::1/128
no service password-encryption	!	!
!	!	interface Ethernet0/0
hostname R-CE-1	!	no ip address
!	!	shutdown
boot-start-marker	!	duplex auto
boot-end-marker	!	!
!	!	interface GigabitEthernet0/0
!	!	no ip address
enable secret 5	!	duplex full
\$1\$C5Xw\$uL34KRnaL0o/NoUoYKX9K/	username Admin-Site1-LanA	speed 1000
!	privilege 15 secret 5	media-type gbic
no aaa new-model	\$1\$Ld.n\$83WermrcebNUhpGA6Vh1H/	negotiation auto
clock timezone EEST 2 0	username User-Site1-LanA secret 5	ipv6 address 2001:DB8:A:1::2/126
clock summer-time EEST recurring	\$1\$6I2T\$fd76BEiRhC7EltIC3iz/f0	!
no ip icmp rate-limit unreachable	!	interface GigabitEthernet1/0
!	redundancy	no ip address
!	!	negotiation auto
!	!	ipv6 address 2001:DB8:BD:1::1/120
!	ip tcp synwait-time 5	ipv6 nd managed-config-flag
!	ip ssh version 2	ipv6 nat
!	!	ipv6 dhcp server Site1LanA
ip domain name Site1LanA.net	!	ntp broadcast
ip name-server 192.168.50.1	!	!
ip cef	!	interface GigabitEthernet2/0
ipv6 unicast-routing	!	ip address dhcp
ipv6 cef	!	negotiation auto
ipv6 dhcp pool Site1LanA	!	ipv6 enable
address prefix 2001:DB8:BD:1::/120	!	ipv6 nat
	!	!
dns-server 2001:DB8:BD:1::1	!	interface GigabitEthernet3/0
domain-name Site1LanA.net	interface Loopback0	no ip address
!	ip address 3.0.0.1	shutdown
!	255.255.255.255	negotiation auto

!	no ip http secure-server	logging synchronous
interface GigabitEthernet4/0	!	stopbits 1
no ip address	!	line aux 0
shutdown	!	exec-timeout 0 0
negotiation auto	logging host ipv6 2001:DB8:BD:1::8	privilege level 15
!		logging synchronous
interface GigabitEthernet5/0	no cdp log mismatch duplex	stopbits 1
no ip address	ipv6 route ::/0 2001:DB8:A:1::1	line vty 0 4
shutdown	ipv6 nat translation timeout never	ipv6 access-class SSH-BLOCK in
negotiation auto	ipv6 nat v6v4 source list IPv6toIPv4 interface GigabitEthernet2/0 overload	login
!		transport input ssh
interface GigabitEthernet6/0	!	line vty 5 15
no ip address	!	ipv6 access-class SSH-BLOCK in
shutdown	!	
negotiation auto	ipv6 access-list IPv6toIPv4	login
!	permit ipv6 any any	transport input ssh
router bgp 200	!	!
bgp log-neighbor-changes	ipv6 access-list SSH-BLOCK	ntp master 2
neighbor 2001:DB8:A:1::1 remote-as 100	permit ipv6 2001:DB8:BD:1::/120 any	ntp update-calendar
!	!	ntp server 0.ua.pool.ntp.org prefer source GigabitEthernet2/0
address-family ipv4	control-plane	!
redistribute connected	!	end
no neighbor 2001:DB8:A:1::1 activate	!	
exit-address-family	mgcp profile default	R-CE-2
!	!	!
address-family ipv6	!	!
redistribute connected	!	!
network ABCD::1/128	gatekeeper	!
neighbor 2001:DB8:A:1::1 activate	shutdown	! Last configuration change at 08:21:24 DST Fri Jun 7 2024
exit-address-family	!	upgrade fpd auto
!	!	version 15.2
ip forward-protocol nd	line con 0	service timestamps debug datetime msec
no ip http server	exec-timeout 0 0	
	privilege level 15	service timestamps log datetime msec

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

no service password-encryption	!	interface Ethernet0/0
!	!	no ip address
hostname R-CE-2	!	shutdown
!	!	duplex auto
boot-start-marker	!	!
boot-end-marker	!	interface GigabitEthernet0/0
!	!	no ip address
!	!	duplex full
enable secret 5	!	speed 1000
\$1\$t.vj\$XkC0Qn3IIYkAvrVuRdg		
wR1	username Admin-Site2-LanA	media-type gbic
!	privilege 15 secret 5	negotiation auto
	\$1\$AIQP\$QJxEZDLAgdlMoR/X	
	o3OGA1	ipv6 address
no aaa new-model		2001:DB8:A:2::2/126
clock timezone DST 2 0	username User-Site2-LanA secret	!
	5	
clock summer-time DST	\$1\$51CK\$h4Pr4Hg6LMs7OseG	interface GigabitEthernet1/0
recurring	RenQq/	
no ip icmp rate-limit unreachable	!	no ip address
!	redundancy	negotiation auto
!	!	
!	!	ipv6 address
!	!	2001:DB8:BD:1::1/120
!	ip tcp synwait-time 5	ipv6 nd managed-config-flag
!	ip ssh version 2	ipv6 nat
!	!	ipv6 dhcp server Site2LanA
ip domain name Site2LanA.net	!	ntp broadcast
ip name-server 192.168.50.1	!	!
ip cef	!	interface GigabitEthernet2/0
ipv6 unicast-routing	!	ip address dhcp
ipv6 cef	!	negotiation auto
ipv6 dhcp pool Site2LanA	!	ipv6 enable
address prefix	!	ipv6 nat
2001:DB8:BD:1::/120	!	!
dns-server 2001:DB8:BD:1::1	!	interface GigabitEthernet3/0
domain-name Site2LanA.net	interface Loopback0	no ip address
!	ip address 3.0.0.2	shutdown
!	255.255.255.255	negotiation auto
multilink bundle-name	ipv6 address ABCD::2/128	!
authenticated	!	interface GigabitEthernet4/0

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

no ip address	!	line aux 0
shutdown	!	exec-timeout 0 0
negotiation auto	logging host ipv6	privilege level 15
!	2001:DB8:BD:1::8	logging synchronous
interface GigabitEthernet5/0	no cdp log mismatch duplex	stopbits 1
no ip address	ipv6 route ::/0 2001:DB8:A:2::1	line vty 0 4
shutdown	ipv6 nat translation timeout never	ipv6 access-class SSH-BLOCK
negotiation auto	ipv6 nat v6v4 source list	in
!	IPv6toIPv4 interface	login local
	GigabitEthernet2/0 overload	transport input ssh
interfa ce GigabitEthernet6/0	!	line vty 5 15
no ip address	!	ipv6 access-class SSH-BLOCK
shutdown	!	in
negotiation auto	ipv6 access-list IPv6toIPv4	login local
!	permit ipv6 any any	transport input ssh
router bgp 300	!	!
bgp log-neighbor-changes	ipv6 access-list SSH-BLOCK	ntp master 6
neighbor 2001:DB8:A:2::1	permit ipv6	ntp update-calendar
remote-as 100	2001:DB8:BD:1::/120 any	ntp server 0.ua.pool.ntp.org prefer
!	!	source GigabitEthernet2/0
address-family ipv4	control-plane	!
redistribute connected	!	end
no neighbor 2001:DB8:A:2::1	!	
activate	!	R-CE-3
exit-address-family	mgcp profile default	!
!	!	!
address-family ipv6	!	
redistribute connected	!	!
network ABCD::2/128	gatekeeper	! Last configuration change at
neighbor 2001:DB8:A:2::1	shutdown	08:22:32 DST Fri Jun 7 2024
activate	!	upgrade fpd auto
exit-address-family	!	version 15.2
!	line con 0	service timestamps debug
ip forward-protocol nd	exec-timeout 0 0	datetime msec
no ip http server	privilege level 15	service timestamps log datetime
no ip http secure-server	logging synchronous	msec
!	stopbits 1	no service password-encryption
		!

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

hostname R-CE-3	!	shutdown
!	!	duplex auto
boot-start-marker	!	!
boot-end-marker	!	interface GigabitEthernet0/0
!	!	no ip address
!	!	duplex full
enable secret 5	!	speed 1000
\$1\$LTdY\$TtZ6eyoLiwQCiDmO		
Z3IJA/	username Admin-Site3-LanA	media-type gbic
!	privilege 15 secret 5	negotiation auto
	\$1\$a1NF\$JtuWfsVy85WerZxc5g	
no aaa new-model	4nL.	ipv6 address
clock timezone DST 2 0	username User-Site3-LanA secret	2001:DB8:A:3::2/126
clock summer-time DST	5	!
recurring	\$1\$gi5y\$J.O0Su1xj1krDTD8Vm	interface GigabitEthernet1/0
	16o0	
no ip icmp rate-limit unreachable	!	no ip address
!	redundancy	negotiation auto
!	!	ipv6 address
!	!	2001:DB8:BD:1::1/120
!	!	ipv6 nd managed-config-flag
!	ip tcp synwait-time 5	ipv6 nat
!	ip ssh version 2	ipv6 dhcp server Site3LanA
!	!	ntp broadcast
ip domain name Site3LanA.net	!	!
ip name-server 192.168.50.1	!	interface GigabitEthernet2/0
ip cef	!	ip address dhcp
ipv6 unicast-routing	!	negotiation auto
ipv6 cef	!	ipv6 enable
ipv6 dhcp pool Site3LanA	!	ipv6 nat
address prefix	!	!
2001:DB8:BD:1::/120	!	
dns-server 2001:DB8:BD:1::1	!	interface GigabitEthernet3/0
domain-name Site3LanA.net	interface Loopback0	no ip address
!		shutdown
!	ip address 3.0.0.3	negotiation auto
	255.255.255.255	
multilink bundle-name	ipv6 address ABCD::3/128	!
authenticated	!	interface GigabitEthernet4/0
!	interface Ethernet0/0	no ip address
!	no ip address	shutdown

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

negotiation auto	logging host ipv6	privilege level 15
!	2001:DB8:BD:1::8	logging synchronous
interface GigabitEthernet5/0	no cdp log mismatch duplex	stopbits 1
no ip address	ipv6 route ::/0 2001:DB8:A:3::1	line vty 0 4
shutdown	ipv6 nat translation timeout never	ipv6 access-class SSH-BLOCK
negotiation auto	ipv6 nat v6v4 source list	in
!	IPv6toIPv4 interface	login local
interface GigabitEthernet6/0	GigabitEthernet2/0 overload	transport input ssh
no ip address	!	line vty 5 15
shutdown	!	ipv6 access-class SSH-BLOCK
negotiation auto	ipv6 access-list IPv6toIPv4	in
!	permit ipv6 any any	login local
router bgp 400	!	transport input ssh
bgp log-neighbor-changes	ipv6 access-list SSH-BLOCK	!
neighbor 2001:DB8:A:3::1	permit ipv6	ntp master 6
remote-as 100	2001:DB8:BD:1::/120 any	ntp update-calendar
!	!	ntp server 0.ua.pool.ntp.org prefer
address-family ipv4	control-plane	source GigabitEthernet2/0
redistribute connected	!	!
no neighbor 2001:DB8:A:3::1	!	end
activate	!	R-CE-4
exit-address-family	mgcp profile default	!
!	!	!
address-family ipv6	!	!
redistribute connected	!	!
network ABCD::3/128	gatekeeper	!
neighbor 2001:DB8:A:3::1	shutdown	! Last configuration change at
activate	!	08:29:41 DST Fri Jun 7 2024
exit-address-family	!	upgrade fpd auto
!	!	version 15.2
ip forward-protocol nd	line con 0	service timestamps debug
no ip http server	exec-timeout 0 0	datetime msec
no ip http secure-server	privilege level 15	service timestamps log datetime
!	logging synchronous	msec
!	stopbits 1	no service password-encryption
!	line aux 0	!
	exec-timeout 0 0	hostname R-CE-4
		!

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		88

boot-start-marker	!	!
boot-end-marker	!	interface GigabitEthernet0/0
!	!	no ip address
!	!	duplex full
enable secret 5	!	speed 1000
\$1\$JfqU\$rHEVahghMyNXjwTja	username Admin-Site1-LanB	media-type gbic
Rb6K.	privilege 15 secret 5	negotiation auto
!	\$1\$H4O7\$TNsdfcajp0O9tuZcWS	ipv6 address
no aaa new-model	yiM/	2001:DB8:A:4::2/126
clock timezone DST 2 0	username User-Site1-LanB secret	!
clock summer-time DST	5	interface GigabitEthernet1/0
recurring	\$1\$qRC3\$WUldFRVUZIfvQmY	
	3XXgNF0	
no ip icmp rate-limit unreachable	!	no ip address
!	redundancy	negotiation auto
!	!	ipv6 address
!	!	2001:DB8:BD:2::1/120
!	ip tcp synwait-time 5	ipv6 nd managed-config-flag
!	ip ssh version 2	ipv6 nat
!	!	ipv6 dhcp server Site1LanB
ip domain name Site1LanB.net	!	ntp broadcast
ip name-server 192.168.50.1	!	!
ip cef	!	interface GigabitEthernet2/0
ipv6 unicast-routing	!	ip address dhcp
ipv6 cef	!	negotiation auto
ipv6 dhcp pool Site1LanB	!	ipv6 enable
address prefix	!	ipv6 nat
2001:DB8:BD:2::/120	!	!
dns-server 2001:DB8:BD:2::1	!	interface GigabitEthernet3/0
domain-name Site1LanB.net	interface Loopback0	no ip address
!	ip address 3.0.0.4	shutdown
!	255.255.255.255	negotiation auto
multilink bundle-name	ipv6 address ABCD::4/128	!
authenticated	!	interface GigabitEthernet4/0
!	interface Ethernet0/0	no ip address
!	no ip address	shutdown
!	shutdown	negotiation auto
!	duplex auto	!

interfa ce Giga bitEthernet5/0	ipv6 route ::/0 2001:DB8:A:4::1	stopbits 1
no ip address	ipv6 nat translation timeout never	line vty 0 4
shutdown	ipv6 nat v6v4 source list	ipv6 access-class SSH-BLOCK
negotiation auto	IPv6toIPv4 interface	in
!	Giga bitEthernet2/0 overload	login local
interfa ce Giga bitEthernet6/0	!	transport input ssh
no ip address	!	line vty 5 15
shutdown	!	ipv6 access-class SSH-BLOCK
negotiation auto	ipv6 access-list IPv6toIPv4	in
!	permit ipv6 any any	login local
router bgp 200	!	transport input ssh
bgp log-neighbor-changes	ipv6 access-list SSH-BLOCK	!
neighbor 2001:DB8:A:4::1	permit ipv6	ntp master 6
remote-as 100	2001:DB8:BD:2::/120 any	ntp update-calendar
!	!	ntp server 0.ua.pool.ntp.org prefer
address-family ipv4	control-plane	source Giga bitEthernet2/0
redistribute connected	!	!
no neighbor 2001:DB8:A:4::1	!	end
activate	!	
exit-address-family	mgcp profile default	R-CE-5
!	!	!
address-family ipv6	!	!
redistribute connected	!	
network ABCD::4/128	gatekeeper	!
neighbor 2001:DB8:A:4::1	shutdown	! Last configuration change at
activate	!	08:30:30 DST Fri Jun 7 2024
exit-address-family	!	upgrade fpd auto
!	line con 0	version 15.2
ip forward-protocol nd	exec-timeout 0 0	service timestamps debug
no ip http server	privilege level 15	datetime msec
no ip http secure-server	logging synchronous	service timestamps log datetime
!	stopbits 1	msec
!	line aux 0	no service password-encryption
!	exec-timeout 0 0	!
logging host ipv6	privilege level 15	hostname R-CE-5
2001:DB8:BD:1::8	logging synchronous	!
no cdp log mismatch duplex		boot-start-marker
		boot-end-marker

!	!	no ip address
!	!	duplex full
enable secret 5	!	speed 1000
\$1\$Oxmc\$rNkf03jJ6XCH5dai6dMSX1	username Admin-Site3-LanB	media-type gbic
!	privilege 15 secret 5	negotiation auto
no aaa new-model	\$1\$g8lM\$LSt.s5fzneWo2mkkgI4EA0	ipv6 address
clock timezone DST 2 0	username User-Site3-LanB secret 5	2001:DB8:A:5::2/126
clock summer-time DST recurring	\$1\$cS3r\$W7LvsADzuheFqFq/UynGa0	!
no ip icmp rate-limit unreachable	!	interfa ce GigabitEthernet1/0
!	redundancy	no ip address
!	!	negotiation auto
!	!	ipv6 address
!	ip tcp synwait-time 5	2001:DB8:BD:2::1/120
!	ip ssh version 2	ipv6 nd managed-config-flag
!	!	ipv6 nat
ip domain name Site3LanB.net	!	ipv6 dhcp server Site3LanB
ip name-server 192.168.50.1	!	ntp broadcast
ip cef	!	!
ipv6 unicast-routing	!	interfa ce GigabitEthernet2/0
ipv6 cef	!	ip address dhcp
ipv6 dhcp pool Site3LanB	!	negotiation auto
address prefix	!	ipv6 enable
2001:DB8:BD:2::/120	!	ipv6 nat
dns-server 2001:DB8:BD:2::1	!	!
domain-name Site3LanB.net	!	interfa ce GigabitEthernet3/0
!	interface Loopback0	no ip address
!	ip address 3.0.0.5	shutdown
	255.255.255.255	negotiation auto
multilink bundle-name authenticated	ipv6 address ABCD::5/128	!
!	!	interfa ce GigabitEthernet4/0
!	interface Ethernet0/0	no ip address
!	no ip address	shutdown
!	shutdown	negotiation auto
!	duplex auto	!
!	!	interfa ce GigabitEthernet5/0
!	interfa ce GigabitEthernet0/0	no ip address

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		91

shutdown	ipv6 nat v6v4 source list	ipv6 access-class SSH-BLOCK
negotiation auto	IPv6toIPv4 interface	in
!	GigabitEthernet2/0 overload	login local
interface GigabitEthernet6/0	!	transport input ssh
no ip address	!	line vty 5 15
shutdown	ipv6 access-list IPv6toIPv4	ipv6 access-class SSH-BLOCK
negotiation auto	permit ipv6 any any	in
!	!	login local
router bgp 400	!	transport input ssh
bgp log-neighbor-changes	ipv6 access-list SSH-BLOCK	!
neighbor 2001:DB8:A:5::1	permit ipv6	ntp master 6
remote-as 100	2001:DB8:BD:2::/120 any	ntp update-calendar
!	!	ntp server 0.ua.pool.ntp.org prefer
address-family ipv4	control-plane	source GigabitEthernet2/0
redistribute connected	!	!
no neighbor 2001:DB8:A:5::1	!	end
activate	mgcp profile default	R-CE-6
exit-address-family	!	!
!	!	!
address-family ipv6	!	!
redistribute connected	gatekeeper	!
network ABCD::5/128	shutdown	! Last configuration change at
neighbor 2001:DB8:A:5::1	!	08:31:08 DST Fri Jun 7 2024
activate	!	upgrade fpd auto
exit-address-family	!	version 15.2
!	line con 0	service timestamps debug
ip forward-protocol nd	exec-timeout 0 0	datetime msec
no ip http server	privilege level 15	service timestamps log datetime
no ip http secure-server	logging synchronous	msec
!	stopbits 1	no service password-encryption
!	line aux 0	!
!	exec-timeout 0 0	hostname R-CE-6
logging host ipv6	privilege level 15	!
2001:DB8:BD:1::8	logging synchronous	boot-start-marker
no cdp log mismatch duplex	stopbits 1	boot-end-marker
ipv6 route ::/0 2001:DB8:A:5::1	line vty 0 4	!
ipv6 nat translation timeout never	!	!

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		92

enable secret 5	!	speed 1000
\$1\$aAk4\$O7gcSE0c9Jnu8fLenO	username Admin-Site2-LanB	media-type gbic
LoB/	privilege 15 secret 5	negotiation auto
!	\$1\$12da\$klIjEXrgbWtunPzmQt	ipv6 address
no aaa new-model	Dqu/	2001:DB8:A:6::2/126
clock timezone DST 2 0	username User-Site2-LanB secret	!
clock summer-time DST	5	interfa ce GigabitEthernet1/0
recurring	\$1\$g1hv\$ceweusehqKAj3Xl5.a5	
	xa0	
no ip icmp rate-limit unreachable	!	no ip address
!	redundancy	negotiation auto
!	!	ipv6 address
!	!	2001:DB8:BD:2::1/120
!	ip tcp synwait-time 5	ipv6 nd managed-config-flag
!	ip ssh version 2	ipv6 nat
!	!	ipv6 dhcp server Site2LanB
!	!	ntp broadcast
ip domain name Site2LanB.net	!	!
ip name-server 192.168.50.1	!	interfa ce GigabitEthernet2/0
ip cef	!	ip address dhcp
ipv6 unicast-routing	!	negotiation auto
ipv6 cef	!	ipv6 enable
ipv6 dhcp pool Site2LanB	!	ipv6 nat
address prefix	!	!
2001:DB8:BD:2::/120	!	interfa ce GigabitEthernet3/0
dns-server 2001:DB8:BD:2::1	!	no ip address
domain-name Site2LanB.net	interface Loopback0	shutdown
!	ip address 3.0.0.6	negotiation auto
!	255.255.255.255	!
multilink bundle-name	ipv6 address ABCD::6/128	interfa ce GigabitEthernet4/0
authenticated	!	no ip address
!	interface Ethernet0/0	shutdown
!	no ip address	negotiation auto
!	shutdown	!
!	duplex auto	interfa ce GigabitEthernet5/0
!	!	no ip address
!	interface GigabitEthernet0/0	shutdown
!	no ip address	negotiation auto
!	duplex full	

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		93

!	!	transport input ssh
interface GigabitEthernet6/0	!	line vty 5 15
no ip address	!	ipv6 access-class SSH-BLOCK
shutdown	ipv6 access-list IPv6toIPv4	in
negotiation auto	permit ipv6 any any	login local
!	!	transport input ssh
router bgp 300	ipv6 access-list SSH-BLOCK	!
bgp log-neighbor-changes	permit ipv6	ntp master 6
neighbor 2001:DB8:A:6::1	2001:DB8:BD:2::/120 any	ntp update-calendar
remote-as 100	!	ntp server 0.ua.pool.ntp.org prefer
!	control-plane	source GigabitEthernet2/0
address-family ipv4	!	!
redistribute connected	!	end
no neighbor 2001:DB8:A:6::1	!	
activate	mgcp profile default	SW-1A-1
exit-address-family	!	
!	!	!
address-family ipv6	!	! Last configuration change at
redistribute connected		02:16:18 EEST Fri Jun 7 2024
network ABCD::6/128	gatekeeper	
neighbor 2001:DB8:A:6::1	shutdown	! NVRAM config last updated at
activate	!	02:18:14 EEST Fri Jun 7 2024
exit-address-family	!	!
!	line con 0	version 15.1
ip forward-protocol nd	exec-timeout 0 0	service timestamps debug
no ip http server	privilege level 15	datetime msec
no ip http secure-server	logging synchronous	service timestamps log datetime
!	stopbits 1	msec
!	line aux 0	no service password-encryption
!	exec-timeout 0 0	service compress-config
logging host ipv6	privilege level 15	!
2001:DB8:BD:1::8	logging synchronous	boot-start-marker
no cdp log mismatch duplex	stopbits 1	boot-end-marker
ipv6 route ::0 2001:DB8:A:6::1	line vty 0 4	!
ipv6 nat translation timeout never	ipv6 access-class SSH-BLOCK	!
ipv6 nat v6v4 source list	in	
IPv6toIPv4 interface	login local	
GigabitEthernet2/0 overload		

Гігабіт Інтернет 2/0 Overload					ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Фомін В.В.				94
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		

logging discriminator EXCESS
severity drops 6 msg-body drops
EXCESSCOLL

logging buffered 50000

logging console discriminator
EXCESS

enable secret 4
w6SU2qPDvI3Ej0oRbRap1NLG
c1ayP3FfFKetRKoR5Xs

!

username Admin-Site1-LanA
privilege 15 secret 4
izGO6v0T6B4dt/8P5Cgmh5kDw
pMe92WEeeiPJ9Sq/UM

username User-Site1-LanA secret
4
XgRFn7gKUXI.7.FPlsHaby5uIrb
89dSC4Yx4i3Dz6So

no aaa new-model

clock timezone EEST 2 0

clock summer-time EEST
recurring

no ipv6 cef

ipv6 multicast rpf use-bgp

no ip icmp rate-limit unreachable

!

no ip domain-lookup

ip domain-name Site1LanA.net

ip cef

!

!

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

!

!

!

vlan internal allocation policy
ascending

!

ip tcp synwait-time 5

ip ssh version 2

!

!

!

!

!

!

!

!

!

interface Ethernet0/0

switchport access vlan 2

switchport mode access

duplex auto

!

interface Ethernet0/1

switchport access vlan 2

switchport mode access

duplex auto

!

interface Ethernet0/2

switchport access vlan 2

switchport mode access

duplex auto

!

interface Ethernet0/3

switchport access vlan 2

switchport mode access

duplex auto

!

interface Ethernet1/0

switchport access vlan 2

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet1/1

switchport access vlan 2

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet1/2

switchport access vlan 2

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet1/3

switchport access vlan 2

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet2/0

switchport access vlan 2

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		95

```

!
interface Ethernet2/1
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security violation
 restrict
 duplex auto
!
interface Ethernet2/2
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security violation
 restrict
 duplex auto
!
interface Ethernet2/3
 duplex auto
!
interface Ethernet3/0
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security violation
 restrict
 duplex auto
!
interface Ethernet3/1
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security violation
 restrict
 duplex auto
!
interface Ethernet3/2
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security violation
 restrict
 duplex auto
!
interface Ethernet3/3
 switchport access vlan 2
 switchport mode access
 switchport port-security
 switchport port-security violation
 restrict
 duplex auto
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 no ip address
 ipv6 address
 2001:DB8:BD:1::2/120
 ntp broadcast client
!
!
 no ip http server
!
!
!
 logging host ipv6
 2001:DB8:BD:1::8
!
!
!
 ipv6 access-list SSH-BLOCK
 permit ipv6
 2001:DB8:BD:1::/120 any
!
!
 control-plane
!
 line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 line vty 0 4
 ipv6 access-class SSH-BLOCK
 in
 login local
 transport input ssh
!
 ntp update-calendar
 ntp server 2001:DB8:BD:1::1
 prefer source Vlan2
end
SW-1B-1
!
! Last configuration change at
04:21:55 EEST Fri Jun 7 2024
!
version 15.1
service timestamps debug
datetime msec
service timestamps log datetime
msec
no service password-encryption
service compress-config
!

```

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

hostname SW-1B-1	spanning-tree extend system-id	switchport mode access
!	!	duplex auto
boot-start-marker	!	!
boot-end-marker	!	interface Ethernet1/0
!	!	switchport access vlan 2
!	vlan internal allocation policy ascending	switchport mode access
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL	!	switchport port-security
logging buffered 50000	ip tcp synwait-time 5	switchport port-security violation restrict
logging console discriminator EXCESS	ip ssh version 2	duplex auto
enable secret 4	!	!
w6SU2qPDvI3Ej0oRbRap1NLGc1ayP3FfFKEtRKoR5Xs	!	interface Ethernet1/1
!	!	switchport access vlan 2
username Admin-Site1-LanB privilege 15 secret 4 X4ZqtPJ///KxuEWxHSsJrv3beQ Vnz2ise/xj8fF6eFU	!	switchport mode access
username User-Site1-LanB secret 4	!	switchport port-security
/DWNPORXhuZdgE8Csk/pOSfn dXJ6PRem2RIGm3iRyDg	!	switchport port-security violation restrict
no aaa new-model	!	duplex auto
clock timezone EEST 2 0	interface Ethernet0/0	!
clock summer-time EEST recurring	switchport access vlan 2	interface Ethernet1/2
no ipv6 cef	switchport mode access	switchport access vlan 2
ipv6 multicast rpf use-bgp	duplex auto	switchport mode access
no ip icmp rate-limit unreachable	!	switchport port-security
!	interface Ethernet0/1	switchport port-security violation restrict
no ip domain-lookup	switchport access vlan 2	duplex auto
ip domain-name Site1LanB.net	switchport mode access	!
ip cef	duplex auto	interface Ethernet1/3
!	!	switchport access vlan 2
!	interface Ethernet0/2	switchport mode access
!	switchport access vlan 2	switchport port-security
!	switchport mode access	switchport port-security violation restrict
!	duplex auto	duplex auto
!	!	!
spanning-tree mode pvst	interface Ethernet0/3	interface Ethernet2/0
	switchport access vlan 2	switchport access vlan 2

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		97

switchport mode access	switchport port-security violation restrict	!
switchport port-security		!
switchport port-security violation restrict	duplex auto	ipv6 access-list SSH-BLOCK
	!	permit ipv6
duplex auto	interface Ethernet3/2	2001:DB8:BD:2::/120 any
!	switchport access vlan 2	!
interface Ethernet2/1	switchport mode access	control-plane
switchport access vlan 2	switchport port-security	!
switchport mode access	switchport port-security violation restrict	!
switchport port-security	duplex auto	line con 0
switchport port-security violation restrict	!	exec-timeout 0 0
duplex auto	interface Ethernet3/3	privilege level 15
!	switchport access vlan 2	logging synchronous
interface Ethernet2/2	switchport mode access	line aux 0
switchport access vlan 2	switchport port-security	exec-timeout 0 0
switchport mode access	switchport port-security violation restrict	privilege level 15
switchport port-security	duplex auto	logging synchronous
switchport port-security violation restrict	!	line vty 0 4
duplex auto	interface Vlan1	ipv6 access-class SSH-BLOCK in
!	no ip address	login local
interface Ethernet2/3	shutdown	transport input ssh
duplex auto	!	!
!	interface Vlan2	ntp update-calendar
interface Ethernet3/0	no ip address	ntp server 2001:DB8:BD:2::1
switchport access vlan 2	ipv6 address	prefer source Vlan2
switchport mode access	2001:DB8:BD:2::2/120	end
switchport port-security	ntp broadcast client	
switchport port-security violation restrict	!	SW-2A-1
duplex auto	!	!
!	no ip http server	!
interface Ethernet3/1	!	! Last configuration change at 03:06:04 EEST Fri Jun 7 2024
switchport access vlan 2	logging host ipv6	! NVRAM config last updated at 03:41:36 EEST Fri Jun 7 2024
switchport mode access	2001:DB8:BD:1::8	!
switchport port-security	!	version 15.1

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				98
Змн.	Арк.	№ докум.	Підпис	Дата		

service timestamps debug	ip cef	switchport access vlan 3
datetime msec	!	switchport mode access
service timestamps log datetime msec	!	duplex auto
no service password-encryption	!	!
service compress-config	!	interface Ethernet0/3
!	spanning-tree mode pvst	switchport access vlan 3
hostname SW-2A-1	spanning-tree extend system-id	switchport mode access
!	!	duplex auto
boot-start-marker	!	!
boot-end-marker	!	interface Ethernet1/0
!	!	switchport access vlan 3
!	vlan internal allocation policy ascending	switchport mode access
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL	!	switchport port-security
logging buffered 50000	ip tcp synwait-time 5	switchport port-security violation restrict
logging console discriminator EXCESS	ip ssh version 2	duplex auto
enable secret 4	!	!
w6SU2qPDvI3Ej0oRbRap1NLG	!	interface Ethernet1/1
c1ayP3FfFKEtRKoR5Xs	!	switchport access vlan 3
!	!	switchport mode access
username Admin-Site2-LanA	!	switchport port-security
privilege 15 secret 4	!	switchport port-security violation restrict
izGO6v0T6B4dt/8P5Cgmh5kDw	!	duplex auto
pMe92WEeeiPJ9Sq/UM	!	!
username User-Site2-LanA secret 4	!	interface Ethernet1/2
XgRFn7gKUXI.7.FPlsHaby5uIrb	interface Ethernet0/0	switchport access vlan 3
89dSC4Yx4i3Dz6So	switchport access vlan 3	switchport mode access
no aaa new-model	switchport mode access	switchport port-security
clock timezone EEST 2 0	duplex auto	switchport port-security violation restrict
clock summer-time EEST recurring	!	!
no ipv6 cef	interface Ethernet0/1	duplex auto
ipv6 multicast rpf use-bgp	switchport access vlan 3	!
no ip icmp rate-limit unreachable	switchport mode access	interface Ethernet1/3
!	duplex auto	switchport access vlan 3
no ip domain-lookup	!	switchport mode access
ip domain-name Site2LanA.net	interface Ethernet0/2	

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		99

```

switchport port-security          switchport port-security violation
restrict                          !
switchport port-security violation
restrict                          !
duplex auto                      !
!                                !
interface Ethernet2/0            interface Ethernet3/1
switchport access vlan 3         !
switchport mode access           logging host ipv6
switchport port-security         2001:DB8:BD:1::8
switchport port-security violation
restrict                          !
duplex auto                      !
!                                !
interface Ethernet2/1            interface Ethernet3/2
switchport access vlan 3         !
switchport mode access           control-plane
switchport port-security         !
switchport port-security violation
restrict                          !
duplex auto                      line con 0
!                                exec-timeout 0 0
interface Ethernet2/2            privilege level 15
switchport access vlan 3         logging synchronous
switchport mode access           line aux 0
switchport port-security         exec-timeout 0 0
switchport port-security violation
restrict                          privilege level 15
duplex auto                      logging synchronous
!                                line vty 0 4
interface Ethernet2/3            ipv6 access-class SSH-BLOCK
duplex auto                      in
!                                login local
interface Ethernet3/0            transport input ssh
switchport access vlan 3         !
switchport mode access           ntp update-calendar
switchport port-security         ntp server 2001:DB8:BD:1::1
                                prefer source Vlan3
                                end
                                SW-2B-1
                                ntp broadcast client

```

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				100
Змн.	Арк.	№ докум.	Підпис	Дата		

	no ipv6 cef	interface Ethernet0/1
!	ipv6 multicast rpf use-bgp	switchport access vlan 3
! Last configuration change at 04:27:32 EEST Fri Jun 7 2024	no ip icmp rate-limit unreachable	switchport mode access
!	!	duplex auto
version 15.1	no ip domain-lookup	!
service timestamps debug datetime msec	ip domain-name Site2LanB.net	interface Ethernet0/2
service timestamps log datetime msec	ip cef	switchport access vlan 3
no service password-encryption	!	switchport mode access
service compress-config	!	duplex auto
!	!	!
hostname SW-2B-1	spanning-tree mode pvst	interface Ethernet0/3
!	spanning-tree extend system-id	switchport access vlan 3
boot-start-marker	!	switchport mode access
boot-end-marker	!	duplex auto
!	!	!
!	!	interface Ethernet1/0
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL	vlan internal allocation policy ascending	switchport access vlan 3
logging buffered 50000	!	switchport mode access
logging console discriminator EXCESS	ip tcp synwait-time 5	switchport port-security
enable secret 4	ip ssh version 2	switchport port-security violation restrict
w6SU2qPDvI3Ej0oRbRap1NLG c1ayP3FfFKEtRKoR5Xs	!	duplex auto
!	!	!
username Admin-SiteB-LanA privilege 15 secret 4 X4ZqtPJ///KxuEWxHSsJrv3beQ Vnz2ise/xj8fF6eFU	!	interface Ethernet1/1
username User-SiteB-LanA secret 4 /DWNPORXhuZdgE8Csk/pOSfn dXJ6PRem2RIGm3iRyDg	!	switchport access vlan 3
no aaa new-model	!	switchport mode access
clock timezone EEST 2 0	!	switchport port-security
clock summer-time EEST recurring	interface Ethernet0/0	switchport port-security violation restrict
	switchport access vlan 3	duplex auto
	switchport mode access	!
	duplex auto	interface Ethernet1/2
	!	switchport access vlan 3
		switchport mode access
		switchport port-security

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		101

switchport port-security violation restrict	duplex auto	!
duplex auto	!	interface Vlan3
!	interface Ethernet3/0	no ip address
interface Ethernet1/3	switchport access vlan 3	ipv6 address 2001:DB8:BD:2::2/120
switchport access vlan 3	switchport mode access	ntp broadcast client
switchport mode access	switchport port-security	!
switchport port-security	switchport port-security violation restrict	!
switchport port-security violation restrict	duplex auto	no ip http server
duplex auto	!	!
!	interface Ethernet3/1	!
interface Ethernet2/0	switchport access vlan 3	logging host ipv6 2001:DB8:BD:1::8
switchport access vlan 3	switchport mode access	!
switchport mode access	switchport port-security	!
switchport port-security	switchport port-security violation restrict	!
switchport port-security violation restrict	duplex auto	ipv6 access-list SSH-BLOCK
duplex auto	!	permit ipv6 2001:DB8:BD:2::/120 any
!	interface Ethernet3/2	!
interface Ethernet2/1	switchport access vlan 3	control-plane
switchport access vlan 3	switchport mode access	!
switchport mode access	switchport port-security	!
switchport port-security	switchport port-security violation restrict	line con 0
switchport port-security violation restrict	duplex auto	exec-timeout 0 0
duplex auto	!	privilege level 15
!	interface Ethernet3/3	logging synchronous
interface Ethernet2/2	switchport access vlan 3	line aux 0
switchport access vlan 3	switchport mode access	exec-timeout 0 0
switchport mode access	switchport port-security	privilege level 15
switchport port-security	switchport port-security violation restrict	logging synchronous
switchport port-security violation restrict	duplex auto	line vty 0 4
duplex auto	!	ipv6 access-class SSH-BLOCK in
!	interface Vlan1	login local
interface Ethernet2/3	no ip address	transport input ssh
	shutdown	!

ntp update-calendar	izGO6v0T6B4dt/8P5Cgmh5kDw	!
ntp server 2001:DB8:BD:2::1	pMe92WEeeiPJ9Sq/UM	!
prefer source Vlan3	username User-Site3-LanA secret	!
end	4	
	XgRFn7gKUXI.7.FPlsHaby5uIrb	interface Ethernet0/0
	89dSC4Yx4i3Dz6So	
SW-3A-1	no aaa new-model	switchport access vlan 4
	clock timezone EEST 2 0	switchport mode access
!	clock summer-time EEST	duplex auto
	recurring	!
! Last configuration change at	no ipv6 cef	interface Ethernet0/1
04:12:54 EEST Fri Jun 7 2024	ipv6 multicast rpf use-bgp	switchport access vlan 4
! NVRAM config last updated at	no ip icmp rate-limit unreachable	switchport mode access
04:12:57 EEST Fri Jun 7 2024	!	duplex auto
!	no ip domain-lookup	!
version 15.1	ip domain-name Site3LanA.net	interface Ethernet0/2
service timestamps debug	ip cef	switchport access vlan 4
datetime msec	!	switchport mode access
service timestamps log datetime	!	duplex auto
msec	!	!
no service password-encryption	!	interface Ethernet0/3
service compress-config	spanning-tree mode pvst	switchport access vlan 4
!	spanning-tree extend system-id	switchport mode access
hostname SW-3A-1	!	duplex auto
!	!	!
boot-start-marker	!	interface Ethernet1/0
boot-end-marker	!	switchport access vlan 4
!	!	switchport mode access
!	!	switchport port-security
logging discriminator EXCESS	vlan internal allocation policy	switchport port-security violation
severity drops 6 msg-body drops	ascending	restrict
EXCESSCOLL	!	duplex auto
logging buffered 50000	ip tcp synwait-time 5	!
logging console discriminator	ip ssh version 2	interface Ethernet1/1
EXCESS	!	switchport access vlan 4
enable secret 4	!	switchport mode access
w6SU2qPDvI3Ej0oRbRap1NLG	!	switchport port-security
c1ayP3FfFKEtRKoR5Xs	!	
!	!	
username Admin-Site3-LanA	!	
privilege 15 secret 4	!	
	!	

```

switchport port-security violation
restrict

duplex auto

!

interface Ethernet1/2

switchport access vlan 4

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet1/3

switchport access vlan 4

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet2/0

switchport access vlan 4

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet2/1

switchport access vlan 4

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet2/2

```

```

switchport access vlan 4

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet2/3

duplex auto

!

interface Ethernet3/0

switchport access vlan 4

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet3/1

switchport access vlan 4

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet3/2

switchport access vlan 4

switchport mode access

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Ethernet3/3

switchport access vlan 4

switchport mode access

```

```

switchport port-security

switchport port-security violation
restrict

duplex auto

!

interface Vlan1

no ip address

shutdown

!

interface Vlan4

no ip address

ipv6 address
2001:DB8:BD:1::2/120

ntp broadcast client

!

!

no ip http server

!

!

logging host ipv6
2001:DB8:BD:1::8

!

!

!

ipv6 access-list SSH-BLOCK

permit ipv6
2001:DB8:BD:1::/120 any

!

control-plane

!

!

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

line aux 0

exec-timeout 0 0

```

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		104

privilege level 15	logging console discriminator EXCESS	!
logging synchronous		!
line vty 0 4	enable secret 4 w6SU2qPDvI3Ej0oRbRap1NLG	!
ipv6 access-class SSH-BLOCK	c1ayP3FfFKEtRKoR5Xs	!
in	!	!
login local	username Admin-Site3-LanB	!
transport input ssh	privilege 15 secret 4 X4ZqtPJ///KxuEWxHSsJrv3beQ	!
!	Vnz2ise/xj8fF6eFU	!
ntp update-calendar	username User-Site3-LanB secret 4	!
ntp server 2001:DB8:BD:1::1	/DWNPORXhuZdgE8Csk/pOSfn	interface Ethernet0/0
prefer source Vlan4	dXJ6PRem2RIGm3iRyDg	switchport access vlan 4
end	no aaa new-model	switchport mode access
	clock timezone EEST 2 0	duplex auto
SW-3B-1	clock summer-time EEST recurring	!
!	no ipv6 cef	interface Ethernet0/1
! Last configuration change at 04:27:46 EEST Fri Jun 7 2024	ipv6 multicast rpf use-bgp	switchport access vlan 4
!	no ip icmp rate-limit unreachable	switchport mode access
	!	duplex auto
version 15.1	no ip domain-lookup	!
service timestamps debug datetime msec	ip domain-name Site3LanB.net	interface Ethernet0/2
service timestamps log datetime msec	ip cef	switchport access vlan 4
no service password-encryption	!	switchport mode access
service compress-config	!	duplex auto
!	!	!
hostname SW-3B-1	spanning-tree mode pvst	interface Ethernet0/3
!	spanning-tree extend system-id	switchport access vlan 4
boot-start-marker	!	switchport mode access
boot-end-marker	!	duplex auto
!	!	!
!	!	interface Ethernet1/0
	!	switchport access vlan 4
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL	vlan internal allocation policy ascending	switchport mode access
	!	switchport port-security
logging buffered 50000	ip tcp synwait-time 5	switchport port-security violation restrict
	ip ssh version 2	duplex auto

!	switchport port-security violation restrict	duplex auto
interface Ethernet1/1		!
switchport access vlan 4	duplex auto	interface Ethernet3/3
switchport mode access	!	switchport access vlan 4
switchport port-security	interface Ethernet2/2	switchport mode access
switchport port-security violation restrict	switchport access vlan 4	switchport port-security
duplex auto	switchport mode access	switchport port-security violation restrict
!	switchport port-security violation restrict	duplex auto
interface Ethernet1/2	duplex auto	!
switchport access vlan 4	!	interface Vlan1
switchport mode access	interface Ethernet2/3	no ip address
switchport port-security	duplex auto	shutdown
switchport port-security violation restrict	!	!
duplex auto	interface Ethernet3/0	interface Vlan4
!	switchport access vlan 4	no ip address
interface Ethernet1/3	switchport mode access	ipv6 address 2001:DB8:BD:2::2/120
switchport access vlan 4	switchport port-security	ntp broadcast client
switchport mode access	switchport port-security violation restrict	!
switchport port-security	duplex auto	!
switchport port-security violation restrict	!	no ip http server
duplex auto	interface Ethernet3/1	!
!	switchport access vlan 4	!
interface Ethernet2/0	switchport mode access	logging host ipv6 2001:DB8:BD:1::8
switchport access vlan 4	switchport port-security	!
switchport mode access	switchport port-security violation restrict	!
switchport port-security	duplex auto	!
switchport port-security violation restrict	!	ipv6 access-list SSH-BLOCK
duplex auto	interface Ethernet3/2	permit ipv6 2001:DB8:BD:2::/120 any
!	switchport access vlan 4	!
interface Ethernet2/1	switchport mode access	control-plane
switchport access vlan 4	switchport port-security	!
switchport mode access	switchport port-security violation restrict	!
switchport port-security		line con 0

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		106

```

exec-timeout 0 0

privilege level 15

logging synchronous

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

line vty 0 4

ipv6 access-class SSH-BLOCK
in

login local

transport input ssh

!

ntp update-calendar

ntp server 2001:DB8:BD:2::1
prefer source Vlan4

end

```

		Фомін В.В.			ККІКБ.КР.Б – 125 – 21 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		107