

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

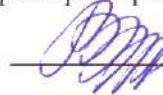
до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми контролю доступу для
захищеної інформаційно-комунікаційної мережі на базі
MPLS VPN»

Виконав: студент 4-го курсу групи КБ-21-2
спеціальності 125 «Кібербезпека»



Дмитро ДАВИДЮК

Керівник: професор кафедри КІ та КБ, д.т.н., доцент,



Володимир ВОРОТНИКОВ

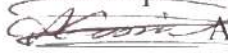
Рецензент: доцент кафедри КІ та КБ, к.т.н., доцент,



Юрій РОССІНСЬКИЙ

Житомир – 2025

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
3 березня 2025 р.

ЗАВДАННЯ
на випускню кваліфікаційну роботу бакалавра

Студент: Давидюк Дмитро Сергійович

Тема роботи: «Проект підсистеми контролю доступу для захищеної інформаційно-комунікаційної мережі на базі MPLS VPN»

затверджена Наказом університету від 3 березня 2025 р. № 80/с

Термін здачі студентом закінченої роботи 20 червня 2025 р.

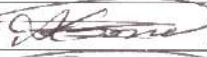
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

Предметом дослідження є методи та засоби реалізації підсистеми контролю доступу в захищеній інформаційно-комунікаційній мережі, побудованій на базі технології MPLS VPN. Об'єктом дослідження є процес проектування та побудови захищеної інформаційно-комунікаційної мережі організації з використанням технології MPLS VPN.

Обладнання та програмне забезпечення:

1. Програмний емулятор GNS3 2.2.42
2. Гіпервізор Oracle Virtual Box 7.1.2
3. ОС Windows 10 Education
4. ОС Microsoft Windows Server 2019 Standard

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Андрій ЄФІМЕНКО	 03.03.25	 03.03.25
2	Андрій ЄФІМЕНКО	 03.03.25	 03.03.25
3	Андрій ЄФІМЕНКО	 03.03.25	 03.03.25

Студент  Дмитро ДАВИДЮК
Керівник  Володимир ВОРОТНІКОВ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	Виконано
2	Аналіз літературних джерел	18.03.2025	Виконано
3	Аналіз об'єкта дослідження	25.03.2025	Виконано
4	Дослідження технології VPN	07.04.2025	Виконано
5	Дослідження технології MPLS	24.04.2025	Виконано
6	Дослідження контролю доступу до мережі	02.05.2025	Виконано
7	Вибір та дослідження технологій та протоколів для захисту КМ	05.05.2025	Виконано
8	Розробка структурної моделі	21.05.2025	Виконано
9	Розрахунок параметрів адресації	23.05.2025	Виконано
10	Оформлення пояснювальної записки	12.06.2025	Виконано
11	Отримання відгуку та рецензій		
12	Захист	24.06.2025	

Студент  Дмитро ДАВИДЮК
Керівник  Володимир ВОРОТНІКОВ

АНОТАЦІЯ

Завданням на кваліфікаційну роботу було дослідити та налаштувати роботу протоколу MPLS VPN та контроль доступу до мережі.

Звіт з кваліфікаційної роботи складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Текстова частина викладена на 64 сторінки друкованого тексту.

Пояснювальна записка має список використаних джерел, який містить 19 найменувань та займає 2 сторінки. В роботі наведено 60 рисунків. Загальний обсяг роботи – 79 сторінки.

В першому розділі було розглянуто теоретичні основи функціонування MPLS VPN та контролю доступу до мережі.

У другому розділі було розроблено топологію та адресацію мережі, розглянуто протокол DHCP та обрано обладнання для побудови мережі.

У третьому розділі було налаштовано адресацію мережі, DHCP, MPLS L3VPN та налаштування AAA та 802.1X за допомогою серверу RADIUS.

Висновок містить результати дослідження та налаштування MPLS VPN та контроль доступу до мережі.

КЛЮЧОВІ СЛОВА: MPLS, VPN, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА МЕРЕЖА, NAS

					KKIK<.KP.B – 125 – 05 – ПЗ			
Змін.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми контролю доступу для захищеної інформаційно-ко- мунікаційної мережі на базі MPLS VPN	Літ.	Арк.	Аркушів
Розроб.		Давидюк Д.С.		24.05.25				
Керівник		Воротников В.В.		24.05.25			4	79
Реценз.		Росієвський Ю.М.		24.05.25				
Н. контр.		Воротников В.В.		24.05.25				
Затверд.		Єфіменко А.А.		24.05.25		ФІКТ, Гр. КБ-21-2		

ANNOTATION

The objective of the qualification work was to research and configure the operation of the MPLS VPN protocol and network access control.

The qualification report consists of an introduction, three chapters, conclusions, a list of references, and appendices. The textual part spans 64 pages of printed text. The explanatory note includes a list of 19 references, occupying 2 pages. The work contains 60 figures. The total volume of the work is 79 pages.

The first chapter examines the theoretical foundations of MPLS VPN operation and network access control.

In the second chapter, the network topology and addressing were developed, the DHCP protocol was reviewed, and the necessary equipment for building the network was selected.

The third chapter includes the configuration of network addressing, DHCP, MPLS L3VPN, and the setup of AAA and 802.1X using a RADIUS server.

The conclusion presents the results of the research and the configuration of MPLS VPN and network access control.

KEYWORDS: MPLS, VPN, INFORMATION AND COMMUNICATION NETWORK, NAC

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ КОНТРОЛЮ ДОСТУПУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ З ВИКОРИСТАННЯМ MPLS VPN	10
1.1 Контроль доступу до мережі	10
1.2 Огляд VPN у комп'ютерних мережах.....	19
1.3 Загальна характеристика технології MPLS та MPLS VPN.....	22
Висновки до першого розділу	30
РОЗДІЛ 2 ПРОЕКТУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ.....	31
2.1 Проектування фізичної топології мережі.....	31
2.2 Розробка схеми адресації мережі	37
2.3 Розробка підсистеми контролю доступу до мережі	39
Висновки до другого розділу.....	40
РОЗДІЛ 3 ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ СПРОЕКТОВАНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ.....	41
3.1 Вибір обладнання Cisco та програмного забезпечення для забезпечення роботи ІКМ	41
3.2 Налаштування IP-адресації на пристроях, налаштування маршрутизації та перевірка зв'язку	44
3.3 Налаштування MPLS VPN.....	45
3.4 Налаштування списків доступу, RADIUS та 802.1X	51
Висновки до третього розділу	61
ВИСНОВКИ.....	62
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	63
ДОДАТКИ.....	65

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

LAN – Local Area Network – Локальна комп'ютерна мережа

VLAN – Virtual Local Area Network – Віртуальна локальна комп'ютерна мережа

WAN – Wide Area Network – Глобальна комп'ютерна мережа

ІКМ – Інформаційно-комунікаційна мережа

IP – Internet Protocol

Fa – Fast Ethernet

Gig – Gigabit Ethernet

DHCP – Dynamic Host Configuration Protocol

VPN – Virtual Private Network

TCP – Transmission Control Protocol – Протокол керування передачею

UDP – User Datagram Protocol – Протокол датаграм користувача

MPLS VPN – Multiprotocol Label Switching VPN

SSH – Secure Shell

ПК – Персональний комп'ютер

NTP – Network Time Protocol

КМ – Комп'ютерна мережа

NAC – Network Access Control – Контроль доступу до мережі

BYOD – Bring Your Own Device – Використання власного пристрою

NAS – Network Access Server – Сервер доступу до мережі

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку інформаційних технологій та зростання обсягів переданої даних захист інформаційно-комунікаційних мереж стає критично важливим завданням для будь-якої організації. Особливого значення набуває питання контролю доступу до мережевих ресурсів, оскільки саме несанкціонований або неконтрольований доступ є одним із головних векторів порушення інформаційної безпеки.

Технологія MPLS VPN широко використовується для побудови масштабованих, ефективних і логічно ізольованих мереж. Проте навіть через умови фізичної або логічної ізоляції трафіку необхідне впровадження додаткових механізмів контролю доступу для обмеження доступу користувачів до певних ресурсів, підвищення рівня безпеки та дотримання внутрішніх політик організації.

Метою кваліфікаційної роботи є проєктування підсистеми контролю доступу для захищеної інформаційно-комунікаційної мережі організації, побудованої на базі технології MPLS VPN, з метою забезпечення безпечного, керованого та ізольованого доступу користувачів до мережевих ресурсів.

Визначена мета обумовлює наступні завдання:

- проаналізувати існуючі підходи до організації контролю доступу в мережах MPLS VPN;
- дослідити можливості використання технологій RADIUS/TACACS+ у контексті контролю доступу;
- розробити логічну структуру підсистеми контролю доступу з урахуванням вимог до безпеки;
- реалізувати модель мережі з підсистемою контролю доступу за допомогою відповідного мережевого обладнання та програмного забезпечення;
- перевірити працездатність проєктного рішення та оцінити його ефективність із погляду забезпечення інформаційної безпеки.

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Об’єктом дослідження є процеси організації та управління контролем доступу в інформаційно-комунікаційних мережах організацій, побудованих з використанням технології MPLS VPN, що забезпечують безпечний обмін даними між віддаленими підрозділами та захист мережевих ресурсів від несанкціонованого доступу.

Предметом дослідження є методи, засоби та технології контролю доступу, зокрема механізми аутентифікації, авторизації та управління доступом у мережах на базі MPLS VPN, що забезпечують захист інформаційних ресурсів і сегментацію мережевого трафіку.

У процесі виконання кваліфікаційної роботи було розроблено проект підсистеми контролю доступу для захищеної інформаційно-комунікаційної мережі на базі MPLS VPN, який забезпечує централізоване управління правами доступу відповідно до політик безпеки організації.

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ КОНТРОЛЮ ДОСТУПУ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ З ВИКОРИСТАННЯМ MPLS VPN

1.1 Контроль доступу до мережі

У сучасному світі комп'ютерні мережі зазнають постійних загроз, що вимагає використання сучасних технологій та протоколів для захисту комп'ютерних мереж. Надійна безпека мережевої інфраструктури є критично важливою для усіх ІКМ.

Традиційний підхід до безпеки корпоративних мереж зосереджується на захисті від зовнішніх атак, наприклад, шляхом розгортання міжмережевих екранів (фаєрволів). Однак, якщо підприємство дозволяє користувачам використовувати термінали, такі як мобільні телефони та комп'ютери, для віддаленого доступу до своєї мережі, дозволяє співробітникам використовувати особисті офісні пристрої для підключення до мережі або класифікує ресурси, доступні для співробітників, йому необхідно впроваджувати заходи контролю доступу для внутрішніх користувачів корпоративної мережі.

Будь-який термінал у корпоративній мережі може вплинути на безпеку всієї мережі. Наприклад, внутрішні користувачі підприємства можуть ненавмисно завантажити шкідливе програмне забезпечення під час перегляду зовнішніх веб-сайтів і поширити його в корпоративній мережі, що створить загрози безпеці. Крім того, надмірна кількість несанкціонованих користувачів, які отримують доступ до корпоративної мережі, може призвести до пошкодження системи обслуговування або розголошення ключових інформаційних активів.

Рішення NAC (контроль доступу до мережі) реалізує контроль безпеки таким чином, що лише авторизовані користувачі та безпечні термінали можуть отримувати доступ до мережі. Воно ізолює неавторизованих та небезпечних користувачів і термінали або надає їм доступ лише до обмежених ресурсів. Такий підхід значно підвищує рівень захисту всієї мережі.

Рішення NAC здійснює аутентифікацію користувачів, які намагаються отримати доступ до мережі, надаючи доступ лише авторизованим користувачам. Це є

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

базовою вимогою для забезпечення безпеки мережі. Аутентифікація терміналів (такі як ПК) у корпоративній мережі повинна відповідати таким вимогам:

- Користувач із безпечним терміналом може отримати доступ до мережі після введення правильного імені користувача та пароля.

- Користувач із небезпечним терміналом не може отримати доступ до мережі та має доступ лише до зони ізоляції мережі.

- Неавторизованим користувачам доступ до мережі заборонений.

НАС надає низку переваг для організацій:

- Контроль за користувачами, які намагаються увійти до корпоративної мережі.

- Контроль доступу до застосунків і ресурсів, до яких прагнуть отримати доступ користувачі.

- Надання доступу до мережі підрядникам, партнерам і гостям за потреби з обмеженням їхніх прав.

- Сегментація працівників за функціональними обов'язками та побудова політик доступу на основі ролей.

- Захист від кібератак шляхом впровадження систем і механізмів, що виявляють незвичну або підозрілу активність.

- Автоматизація реагування на інциденти.

- Генерація звітів і аналітики щодо спроб доступу в межах всієї організації [10].

Щоб задовольнити потреби працівників у новітніх технологіях і персоналізації, а також підвищити їхню ефективність, багато підприємств розглядають можливість дозволити співробітникам підключатися до внутрішньої мережі (інтранету) за допомогою власних смарт-пристроїв (такі як мобільні телефони, планшети та ноутбуки). Це називається BYOD (використання власних пристроїв). Оскільки на таких пристроях зазвичай не встановлено засобів захисту, доступ до корпоративного інтранету через них може створювати загрози безпеці. Рішення НАС використовує технологію ідентифікації типу терміналу для автоматичного визначення типів пристроїв, які працівники використовують для підключення до

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

інтранету. Це дозволяє здійснювати аутентифікацію та авторизацію на основі інформації про користувача, типу пристрою та середовища його функціонування.

Камери відеоспостереження, кіоски для реєстрації та будівельні сенсори – це лише кілька прикладів IoT-пристроїв. Хоча такі пристрої розширюють мережу організації, вони також збільшують площу атаки. Крім того, IoT-пристрої можуть залишатися без нагляду або перебувати в режимі сну протягом тривалого часу. Рішення NAC може зменшити ризики для таких кінцевих точок, застосовуючи визначені методи профілювання та впроваджуючи політики доступу для різних категорій IoT-пристроїв.

Рішення NAC також корисне для надання тимчасового доступу стороннім користувачам, таким як підрядники, консультанти та партнери. NAC може надати таким користувачам доступ до мережі безперешкодно, без необхідності залучати IT-відділ. Звісно, політики доступу для сторонніх користувачів мають відрізнятися від політик для штатних працівників [12].

Важливість керування доступом до мережі:

Покращена безпека. Оскільки NAC забезпечує контроль за всіма пристроями, що використовуються в організації, він підвищує безпеку, аутентифікуючи користувачів і пристрої в момент їх підключення до мережі. Можливість моніторити мережеву активність і негайно вжити заходів проти несанкціонованої або підозрілої поведінки означає, що загрози від шкідливих програм та інших кібератак зменшуються.

Економія коштів. Автоматизований моніторинг і захист пристроїв на великому масштабі призводять до економії коштів для організацій, оскільки потрібно менше IT-ресурсів. Крім того, блокування несанкціонованого доступу або підозри на атаку шкідливого програмного забезпечення запобігає фінансовим втратам, які можуть виникнути, якщо ці дії не будуть зупинені.

Автоматизація. Оскільки кількість та різноманітність пристроїв, які використовують організації, продовжують зростати, організації не можуть вручну перевіряти користувачів та політики безпеки їхніх кінцевих пристроїв під час спроби підключення до мережі. Автоматизовані функції NAC забезпечують вражаючу

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

ефективність процесу аутентифікації користувачів і пристроїв та авторизації доступу.

Легкість контролю. Функції видимості NAC ефективно служать як 24/7 інвентаризація всіх кінцевих пристроїв, авторизованих організацією. Це корисно не лише тоді, коли IT-відділ має визначити, які пристрої чи користувачі отримали доступ до мережі, але й для управління життєвим циклом, коли пристрої потрібно вивести з експлуатації або замінити.

Типи керування доступом до мережі:

Контроль доступу перед допуском. Контроль доступу перед допуском до мережі відбувається до надання доступу. Користувач, який намагається підключитися до мережі, надсилає запит на доступ. Контроль доступу розглядає цей запит і надає доступ, якщо пристрій або користувач можуть аутентифікувати свою особу.

Контроль доступу після допуску. Контроль доступу після допуску до мережі – це процес надання авторизації аутентифікованому пристрою або користувачу, який намагається потрапити до нової або іншої частини мережі, до якої їм ще не було надано доступ. Для отримання авторизації користувач або пристрій повинні знову пройти перевірку своєї особи [11].

802.1X – це протокол контролю доступу до мережі на основі портів. Як і всі види аутентифікації, аутентифікація за допомогою 802.1X полягає в тому, щоб переконатися, що пристрій, який взаємодіє з системою, дійсно є тим, за кого він себе видає. Коли хтось хоче отримати доступ до мережі за допомогою 802.11 та її варіантів, таких як 802.11n, b або g, аутентифікація 802.1X виступає як протокол, який перевіряє, чи є особа, що підключається, тим, ким вона себе називає. Це працює як для бездротових, так і для дротових пристроїв.

802.1X визначає аутентифікацію на основі портів як протокол контролю доступу та аутентифікації, що базується на клієнт-серверній архітектурі та обмежує неавторизованим клієнтам доступ до LAN через публічно доступні порти. Сервер аутентифікації перевіряє кожного запитувача (клієнта), підключеного до порту пристрою доступу (мережевий комутатор доступу), перш ніж надавати будь-які послуги, що пропонуються комутатором або LAN.

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

До того, як клієнт буде аутентифікований, через порт, до якого підключено пристрій, дозволяється лише трафік протоколу розширюваної аутентифікації по LAN (EAPOL). Після успішної аутентифікації нормальний трафік може пройти через порт.

Система аутентифікації 802.1X використовує стандартну клієнт-серверну архітектуру з трьома компонентами: клієнт, пристрій доступу та сервер аутентифікації:

- Клієнт – робоча станція, яка повинна підтримувати протокол EAPoL і мати встановлене програмне забезпечення 802.1X. Клієнти можуть ініціювати аутентифікацію 802.1X, як тільки вони запускають клієнтське програмне забезпечення.

- Пристрій доступу – контролює фізичний доступ до мережі на основі статусу аутентифікації клієнта. Комутатор виступає як посередник між клієнтом та сервером аутентифікації, запитуючи у клієнта інформацію про його ідентифікацію, перевіряючи цю інформацію з сервером аутентифікації та передаючи відповідь клієнту. Комутатор інкапсулює та деінкапсулює кадри протоколу розширюваної аутентифікації (EAP) і взаємодіє з сервером аутентифікації RADIUS.

- Сервер аутентифікації виконує аутентифікацію, авторизацію та облік користувачів. Зазвичай для цього використовують сервер RADIUS (Remote Authentication Dial-In User Service) [14].

Як працює аутентифікація 802.1X:

Ініціація. Під час фази ініціації пристрій доступу надсилає кадри EAP запиту ідентифікації, які використовуються для передачі запиту на ідентифікацію пристрою, що намагається підключитися. Ці кадри надсилаються на адресу 2 рівня в локальній мережі або віртуальній локальній мережі (VLAN). Рівень 2 – це рівень каналу передачі даних, такий як протокол точка-точка (PPP), і він контролює, як дані рухаються через фізичні з'єднання в мережі. Пристрій доступу потім бере ідентифікаційну інформацію, упаковує її та надсилає на сервер аутентифікації.

Аутентифікація. Після того, як досягнуто угоди між клієнтом і сервером аутентифікації на етапі ініціації, відповіді та запити EAP передаються між сервером аутентифікації та клієнтом, і сервер аутентифікації відповідає повідомленням про

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

успіх або невдачу. Якщо процес аутентифікації завершується успішно, пристрій доступу позначає порт як «авторизований». Цей стан дозволяє нормальному трафіку проходити через порт. Якщо процес не вдалося завершити успішно, порт залишається в стані «неавторизований». Це призводить до блокування всього трафіку, окрім EAP.

Авторизація. Після того, як користувач реєструється для отримання сертифіката інфраструктури відкритих ключів (PKI) або підтверджує дійсність своїх облікових даних, йому надається доступ до мережі. RADIUS перевіряє, чи є у нього правильний сертифікат або необхідні облікові дані кожного разу, коли він підключається. Це допомагає запобігти підключенню нелегітимних користувачів до мережі.

Облік та завершення. Облік в системі 802.1X RADIUS реєструє інформацію, що стосується пристроїв, які пройшли аутентифікацію, а також тривалість сесії. Інформація про пристрій надсилається на сервер обліку на початку сесії. Сервер також отримує повідомлення, коли сесія завершується [15].

Протокол Terminal Access Controller Access Control System (TACACS) використовується в Unix-мережах для взаємодії з сервером аутентифікації особистості, який визначає, чи мають користувачі дозвіл на доступ до мережі. Різні виробники розробили розширені версії TACACS. Наприклад, компанія Cisco створила TACACS+, а Huawei – HWTACACS. Обидва – TACACS+ і HWTACACS – є пропрієтарними (власницькими) протоколами. Вони поступово замінили оригінальний TACACS і більше не сумісні з ним.

TACACS – це протокол для управління аутентифікацією, авторизацією та обліком користувачів (AAA), який з'явився у 1980-х роках. Він переважно використовується в Unix-мережах для забезпечення захищеного зв'язку з сервером аутентифікації та перевірки прав доступу користувачів.

У 1984 році протокол TACACS був вперше представлений військовим дослідницьким інститутом США, про що йдеться у RFC 927. Він був розроблений для мережі MILNET з метою спрощення ідентифікації користувачів, дозволяючи їм після входу в один вузол мережі безперешкодно підключатися до інших хостів. З

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

часом компанія Cisco прийняла TACACS і розвинула його у своєму мережевому обладнанні, створивши покращену версію – Extended TACACS (XTACACS), описану у RFC 1492. На відміну від попередника, XTACACS розділяє процеси аутентифікації, авторизації та обліку, що дає можливість керувати цими функціями на окремих серверах для більш гнучкого контролю та адміністрування.

З розвитком мереж з'явилася потреба у більш універсальних варіантах розгортання та кращому контролі над командами користувачів. У відповідь виробники вдосконалили як TACACS, так і XTACACS. Яскравим прикладом таких покращень є TACACS+ від Cisco [19].

Remote Authentication Dial-In User Service (RADIUS) – це розподілений протокол обміну інформацією, що використовує модель клієнт/сервер. Він захищає мережу від несанкціонованого доступу і часто використовується в мережах, які потребують високої безпеки, забезпечуючи при цьому віддалений доступ. RADIUS – це стандартний протокол, який підтримується майже всіма основними пристроями і є найпоширенішим протоколом AAA на живих мережах. Він використовує протокол User Datagram Protocol (UDP) для передачі даних, що забезпечує хорошу продуктивність в реальному часі. Крім того, він має високу надійність завдяки механізмам повторної передачі та резервного сервера. RADIUS легко реалізувати та підтримує багатозадачність на сервері для аутентифікації великої кількості користувачів.

Аутентифікація, Авторизація та Облік (AAA) забезпечують управлінську структуру для налаштування контролю доступу на сервері доступу до мережі (NAS). Він визначає, які користувачі можуть отримати доступ до мережі, які ресурси чи послуги доступні авторизованим користувачам, і як нараховувати оплату користувачам, які використовують мережеві ресурси. AAA може бути реалізований за допомогою різних протоколів, але RADIUS є найбільш поширеним.

RADIUS – це протокол, який використовується для комунікації між сервером доступу до мережі (NAS) та сервером AAA. Спочатку він застосовувався для управління великою кількістю розподілених користувачів, які використовували послідовні порти та модеми, а потім був широко застосований до систем NAS. Для

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

отримання дозволу на доступ до певних мереж або використання мережевих ресурсів, користувач повинен встановити з'єднання з NAS через мережу (наприклад, телефонну мережу). У цьому випадку NAS відповідає за аутентифікацію користувача або з'єднання та надсилає інформацію про користувача та облік на сервер RADIUS. RADIUS визначає, як передавати інформацію про користувача та облікову інформацію між NAS та сервером RADIUS. Після отримання запитів від користувачів, сервер RADIUS аутентифікує користувачів і надсилає необхідну конфігураційну інформацію назад до NAS.

RADIUS має такі характеристики:

- Модель клієнт/сервер
- Захищений механізм обміну повідомленнями
- Хороша масштабованість

Клієнт і сервер RADIUS обмінюються повідомленнями аутентифікації, використовуючи спільний ключ. Спільний ключ – це рядок символів, відомий як клієнту, так і серверу, і його не потрібно передавати окремо по мережі. Крім того, пакет RADIUS має поле Authenticator розміром 16 октетів, яке містить цифровий підпис для всього пакета. Ці дані підпису обчислюються за допомогою алгоритму MD5 і спільного ключа. Після отримання пакета RADIUS пристрій перевіряє підпис і відкидає пакет, якщо підпис неправильний. Цей механізм забезпечує безпеку обміну інформацією між клієнтом і сервером RADIUS [18].

Хоча і TACACS+, і RADIUS є протоколами для управління доступом до мережі, їхні основні сфери застосування суттєво відрізняються. RADIUS переважно призначений для аутентифікації користувачів, які отримують доступ до мережі, тоді як TACACS+ головним чином орієнтований на управління мережевим обладнанням, таким як маршрутизатори та комутатори. Окрім цих ролей, між двома протоколами існує кілька інших ключових відмінностей.

Таблиця 1.1. Порівняння RADIUS та TACACS+

Характеристика	RADIUS (Remote Authentication Dial-In User Service)	TACACS+ (Terminal Access Controller Access-Control System Plus)
Документований	RFC 2865	RFC 1492

Транспортний протокол	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Порти	UDP порт 1812 або 1645 для аутентифікації, 1813 або 1646 для обліку	TCP порт 49 для зв'язку між клієнтом і сервером
Підтримка зовнішньої авторизації команд	Відсутня	Підтримується, забезпечує деталізований контроль
Шифрування	Шифрує тільки паролі, інша інформація передається відкрито	Шифрує всі пакети
Об'єднання аутентифікації та авторизації	Об'єднані, розділити не можна (облік можна використовувати окремо)	Розділені, можливе використання різних протоколів для кожної функції
Підтримка обліку команд	Відсутня	Підтримується
Статус протоколу	Відкритий стандарт	Власницький протокол Cisco
Сумісність	Працює з практично усіма сучасними пристроями	Працює тільки з пристроями Cisco
Рівні привілеїв	Підтримує лише один рівень привілеїв (обмежено привілейованим режимом)	Підтримує кілька рівнів привілеїв
Підтримка 802.1x (контроль доступу на основі портів)	Підтримується	Не підтримується
Основна сфера застосування	Протокол доступу до мережі	Керування пристроями через сервер контролю доступу (ACS)
Підтримка мультипротоколів	Немає (тільки IP)	Підтримує мультипротоколи (IP, Novell, NetBIOS, Apple, X.25)
Аутентифікація мережевого обладнання	Не підтримується	Підтримується

Зважаючи на переваги та недоліки обох протоколів, для реалізації підсистеми контролю доступу було обрано RADIUS. Основною причиною вибору є підтримка протоколом RADIUS стандарту 802.1x, що забезпечує портовий контроль доступу на рівні мережевого обладнання, а також широка сумісність з різноманітними сучасними пристроями різних виробників. Крім того, відкритий стандарт RADIUS сприяє легшій інтеграції та масштабуванню системи контролю доступу в корпоративній мережі. Хоча TACACS+ має розширені можливості для адміністрування мережевого обладнання, його власницький характер і обмежена підтримка поза пристроями Cisco роблять його менш гнучким для реалізації у мультивендорному середовищі. Тому RADIUS є оптимальним вибором для забезпечення безпечного та

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

стандартизованого контролю доступу в захищеній інформаційно-комунікаційній мережі на базі MPLS VPN.

1.2 Огляд VPN у комп'ютерних мережах

У будь-якої організації є потреба передавати інформацію між офісами або забезпечити доступ до корпоративної мережі для працівників, які працюють поза офісом. Для цього можна використати VPN.

Чому важливо використовувати VPN для передачі інформації? У разі підключення працівника до корпоративної мережі віддалено або підключення між офісами трафік проходить через загальнодоступну мережу Інтернет, що робить трафік відкритим для атак.

VPN (віртуальна приватна мережа) – узагальнена назва клієнт-серверних технологій, які дають змогу створити захищений канал поверх загальнодоступних мереж.

VPN вимагає, щоб управління мережею підприємства могло безперешкодно розширюватися від локальних мереж (LAN) до публічних мереж, а також до мереж клієнтів і партнерів. Окрім передачі деяких другорядних завдань управління мережею постачальнику послуг (SP), підприємство також має виконувати багато завдань з управління мережею. Тому необхідна повноцінна система управління VPN. Управління VPN включає в основному управління безпекою, управління пристроями, управління конфігураціями, управління списками контролю доступу (ACL) та управління якістю обслуговування QoS.

VPN створюються на базі публічних мереж. Впровадження VPN є простим, зручним і гнучким. Однак при цьому виникають певні ризики для мережі.

На традиційному IP VPN підприємство повинно гарантувати, що дані VPN не будуть перехоплені або змінені зловмисниками, а також запобігати доступу не-санкціонованих користувачів до внутрішніх ресурсів або приватної інформації підприємства. Екстранет VPN стикаються з ще серйознішими ризиками. Наступні рішення можуть підвищити безпеку VPN:

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

- Тунелювання та шифрування. Протокол тунелювання може реалізувати багатопроTOCOLьну інкапсуляцію, підвищити гнучкість застосування VPN та забезпечити логічні P2P-канали через мережі IP без встановлення з'єднання. Коли користувачі потребують більш безпечної передачі даних, можна застосувати зашифровані тунелі для захисту конфіденційності даних та запобігання їх перехопленню і модифікації.

- Перевірка даних. У небезпечній мережі, такій як публічна мережа, на якій створено VPN, пакети можуть бути незаконно перехоплені та змінені. У результаті отримувач отримує некоректні пакети. Після ввімкнення перевірки даних отримувач зможе розпізнати таку модифікацію, забезпечуючи цілісність даних.

- Аутентифікація користувача. Через аутентифікацію користувачів VPN може дозволити авторизованим користувачам доступ до ресурсів підприємства та заборонити доступ несанкціонованим користувачам. Комутатори можуть аутентифікувати користувачів, авторизувати їх на різних рівнях та генерувати записи доступу через механізм Аутентифікації, Авторизації та Обліку (AAA).

- Брандмауер та засоби виявлення атак. Брандмауери використовуються для фільтрації пакетів і запобігання несанкціонованому доступу. Виявлення атак застосовується для оцінки дійсності пакетів шляхом їх аналізу, застосування політик безпеки в реальному часі, розриву несанкціонованих сеансів та запису випадків несанкціонованого доступу [7].

MPLS VPN створюються на основі міток таблиць пересилання та пакетів на стороні мережі. Якщо MPLS-мережа не підключена до Інтернету, забезпечується безпека внутрішніх ресурсів MPLS-мережі. Тому MPLS VPN можуть забезпечити безпеку VPN певною мірою.

Якщо користувачі MPLS VPN хочуть отримати доступ до Інтернету, можна створити канал з брандмауером, щоб забезпечити безпечне з'єднання для VPN. MPLS VPN легко управляти, оскільки лише одна політика безпеки застосовується на всій мережі VPN.

За класифікацією відповідно до застосування VPN можна поділити на наступні типи:

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

- Intranet VPN. Інтранет VPNs з'єднують усі офіси підприємства через публічні мережі. Інтранет VPNs є розширенням або заміною традиційних приватних мереж чи інших корпоративних мереж.

- Extranet VPN. Екстранет VPN розширюють корпоративні мережі до постачальників, партнерів і клієнтів, використовуючи VPN. VPN встановлюються між різними підприємствами з спільними інтересами через публічні мережі, щоб певні ресурси могли бути спільно використані різними користувачами VPN.

- Access VPN. Через access VPN співробітники у відрядженні, користувачі з малих офісів вдома та віддалених офісів можуть отримувати доступ до внутрішніх серверів підприємств через недорогі засоби дозвону та встановлювати приватні мережеві з'єднання з внутрішніми та зовнішніми мережами підприємств.

За класифікацією на основі режиму роботи VPN можна поділити на наступні типи:

- VPN на основі обладнання замовника (CPE-based VPN), що контролюється користувачами. У режимі VPN на основі обладнання замовника (CPE) користувачі створюють, керують і підтримують VPN. На пристроях користувачів повинен бути налаштований протокол тунелювання VPN, такий як IPsec, GRE, L2TP або PPTP.

- VPN на основі мережі, що контролюються постачальниками інтернет-послуг (ISP). У режимі VPN на основі мережі, постачальники інтернет-послуг (ISP) створюють, керують і підтримують VPN. Постачальники також дозволяють користувачам певною мірою керувати і контролювати послуги. Функції та можливості, пов'язані з VPN, в основному реалізуються на пристроях з боку мережі. На пристроях з боку користувача потрібне лише з'єднання з мережею, і спеціальні функції VPN не потрібні. VPN на основі MPLS, а саме MPLS VPN, належать до VPN на основі мережі. MPLS VPN стає основною технологією IP VPN і широко використовується в мережах телекомунікаційних операторів і підприємств завдяки своїм перевагам у гнучкості, масштабованості та якості обслуговування (QoS). MPLS VPN зазвичай застосовується на агрегатному рівні основної мережі і є важливою технологією для з'єднання філій VIP-клієнтів і ізоляції послуг 3G та NGN. Загалом, VPN

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

на основі MPLS – це надійне, гнучке та ефективне рішення для побудови захищених корпоративних мереж із централізованим контролем і високою якістю сервісу.

1.3 Загальна характеристика технології MPLS та MPLS VPN

У середині 1990-х років апаратні обмеження негативно вплинули на експоненціальне зростання обсягу даних, що передавалися через Інтернет. IP-технології, які базувалися на правилі найдовшого збігу, змушені були покладатися на програмне забезпечення для пошуку маршрутів, що призводило до низької продуктивності пересилання. Це обмежувало розвиток мереж. Для вирішення цих проблем IETF запропонувала протокол MPLS, спрямований на підвищення продуктивності пересилання на маршрутизуючих пристроях у IP-мережах.

Що таке MPLS? MPLS – це протокол, запропонований Internet Engineering Task Force (IETF), який використовує мітки для спрямування передачі пакетів даних на високих швидкостях. Він відображає IP-адреси у короткі мітки фіксованої довжини локального значення, усуваючи потребу в пошуках у таблицях маршрутизації IP. MPLS виконує заміну міток для визначення шляху передачі пакета, що робить пересилання пакетів значно ефективнішим. Крім того, мітки MPLS можуть використовуватися для створення логічних тунелів у IP-мережі. Завдяки сумісності MPLS з різними протоколами мережевого та канального рівня, він може надавати тунелі загальної мережі для широкого спектра послуг, включаючи L2VPN, L3VPN і EVPN.

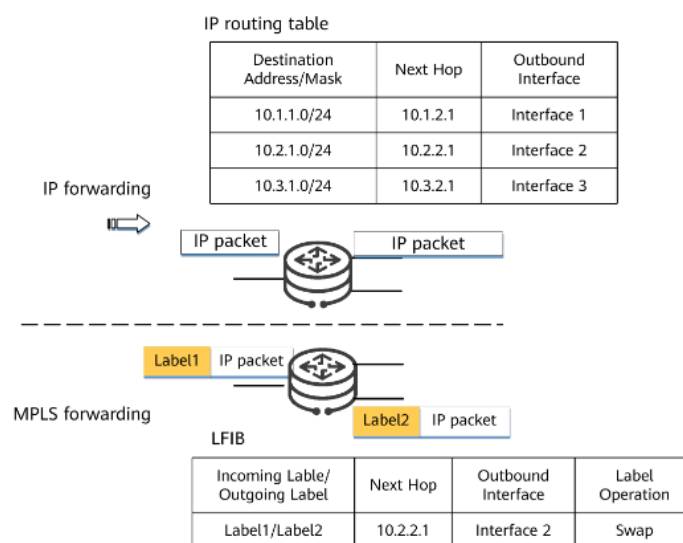


Рисунок 1.1 – Порівняння між IP маршрутизацією та передачею даних MPLS

На рисунку 1.1 можна побачити, що MPLS значно покращує продуктивність передачі даних порівняно з традиційною IP-маршрутизацією в декількох аспектах:

- Усунення ресурсоємного пошуку в таблицях маршрутизації IP: MPLS замінює тривалий процес пошуку в таблицях маршрутизації IP простішим механізмом заміни міток, що значно скорочує час, необхідний для спрямування пакетів.

- Скорочення кількості операцій розбору заголовків і інкапсуляції/декапсуляції міток: після того, як пакет потрапляє в домен MPLS, тільки вхідні та вихідні вузли домену повинні аналізувати заголовок IP-пакета та інкапсулювати або декапсулювати мітки, тоді як транзитні вузли лише замінюють мітки. Це додатково прискорює пересилання пакетів.

З розвитком технології прикладних інтегральних схем (ASIC) і поширенням апаратних засобів як основного способу швидкого пошуку в таблицях маршрутизації IP, MPLS більше не забезпечував значного покращення продуктивності, як раніше.

MPLS отримав нове життя завдяки пересиланню на основі міток, що по суті є технологією тунелювання, яка дозволяє інкапсулювати кілька рівнів міток у пакеті. І оскільки MPLS працює безперебійно з різними протоколами мережевого та канального рівнів, він є ідеальним вибором для створення тунелів загальної мережі для різних VPN-сервісів. Крім того, пересилання пакетів MPLS базується на фіксованих шляхах, що визначаються за допомогою заміни міток, роблячи його технологією пересилання з орієнтацією на з'єднання. Це призвело до його широкого використання в різних сценаріях, таких як інженерія трафіку (TE), QoS та SD-WAN.

Характеристики MPLS. MPLS – це технологія пересилання на основі класів, яка групує схожі пакети даних у єдиний клас, відомий як клас еквівалентності пересилання (FEC). MPLS обробляє пакети, що належать до одного й того ж FEC, однаковою чином. Пакети можуть бути класифіковані в FEC на основі будь-якої комбінації таких елементів, як адреса відправника, адреса одержувача, порт відправника, порт одержувача, тип протоколу, тип послуги тощо. Наприклад, усі

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

пакети, призначені для тієї самої адреси одержувача в IP-маршрутизації, що використовує правило найдовшого збігу, будуть класифіковані в один і той самий FEC.

Мітка MPLS – це короткий ідентифікатор фіксованої довжини, який має лише локальне значення. Він унікально ідентифікує FEC, до якого належить пакет. У деяких випадках (наприклад, коли потрібне балансування навантаження) один FEC може бути відображений на кілька міток MPLS. Однак одна мітка може представляти лише один FEC на пристрої. Мітка MPLS складається з 4 байтів.

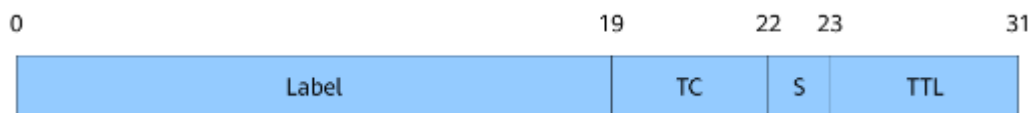


Рисунок. 1.2 – Структура інкапсуляції мітки MPLS

На рисунку 1.2 можна побачити, що Мітка MPLS містить такі чотири поля:

- Мітка: 20-бітне поле, яке визначає значення мітки.
- TC: 3-бітне поле, яке вказує клас трафіку. Це поле також називають Exр. Зазвичай використовується для визначення класу обслуговування (CoS).
- S: 1-бітне поле, яке позначає нижню мітку стека (BoS). MPLS підтримує кілька міток, тобто вкладені мітки. Якщо значення BoS мітки дорівнює 1, це означає, що мітка знаходиться на дні стека міток.
- TTL: 8-бітне поле, яке вказує значення часу життя (TTL). Це поле аналогічне полю TTL у IP-пакетах.

На рисунку 1.3 можна побачити, що Мітка MPLS інкапсулюється між канальним рівнем і мережевим рівнем. Мітки MPLS підтримуються всіма протоколами канального рівня.



Рисунок 1.3 – Позиція інкапсуляції мітки MPLS

Основні операції з мітками MPLS включають додавання мітки (label push), заміну мітки (label swap) і видалення мітки (label pop). Вони є базовими діями пересилання міток і частиною бази інформації про пересилання міток (LFIB).

Основні операції з мітками MPLS такі:

- Додавання мітки (Push): Коли IP-пакет входить у домен MPLS (який складається з серії послідовних LSR), вхідний вузол додає мітку між заголовком рівня 2 і заголовком IP-пакета. Транзитний вузол також може додати мітку до верхньої частини стека міток (вкладення міток) за потреби після отримання пакета.

- "Заміна мітки (Swap): Коли пакет пересилається всередині домену MPLS, транзитний вузол здійснює пошук у LFIB і замінює верхню мітку в стеку міток MPLS-пакета на мітку, призначену наступним вузлом.

- Видалення мітки (Pop): Коли пакет виходить із домену MPLS, вихідний вузол видаляє мітку MPLS; або вузол MPLS на передостанньому кроці видаляє верхню мітку зі стека, щоб зменшити кількість міток у стеку міток.

На рисунку 1.4 зображено шлях перемикавання міток (LSP) – це шлях, уздовж якого пакети, що належать до одного й того ж FEC (тобто пакети, інкапсульовані мітками MPLS), пересилаються в домені MPLS.

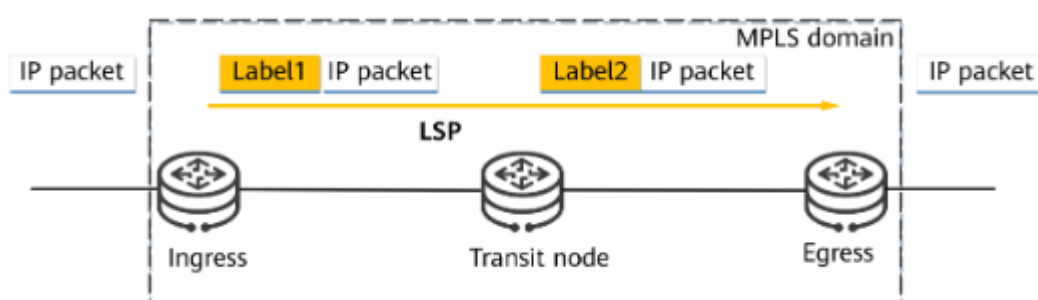


Рисунок 1.4 – Мережа LSP

LSP – це односторонній канал від вхідного до вихідного вузла. LSP виконує такі функції:

- Вхідний вузол (Ingress): початковий вузол LSP. LSP має лише один вхідний вузол. Вхідний вузол додає мітку MPLS до IP-пакета і інкапсулює пакет у MPLS-пакет.

- Транзитний вузол (Transit node): проміжний вузол на LSP. LSP може мати будь-яку кількість транзитних вузлів, включаючи нуль. Транзитний вузол здійснює пошук у LFIB і пересилає MPLS-пакети шляхом заміни міток.

- Вихідний вузол (Egress): останній вузол LSP. LSP має лише один вихідний вузол. Вихідний вузол видаляє певну мітку (якщо вона є) з MPLS-пакета і відновлює оригінальний пакет перед його пересиланням.

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

MPLS широко використовується в IP-мережах і забезпечує такі переваги:

- MPLS повністю сумісний з IP-мережею та є її вдосконаленням, що робить його легким у впровадженні завдяки низькій вартості побудови.
- У MPLS площини управління та пересилання розділені. На площині управління LSP встановлюються на основі IP-маршрутів. MPLS може використовувати гнучкість і механізми надійності IP-маршрутів за потреби. На площині пересилання, орієнтованій на з'єднання, пакети передаються через LSP. Крім того, MPLS ефективно реалізує інженерію трафіку (TE) і забезпечення якості обслуговування (QoS).
- MPLS є незалежним від протоколів канального рівня. Він підтримує такі протоколи, як Frame Relay, ATM, PPP та SDH, забезпечуючи взаємодію різних типів мереж і хорошу сумісність.
- MPLS-мережа підтримує ієрархічну топологію та підходить для розгортання на IP-магістральній мережі.
- Теоретично стек міток MPLS підтримує необмежене вкладення міток, що відповідає вимогам VPN-сервісів до багаторівневої інкапсуляції міток публічної та приватної мереж. Таким чином, MPLS забезпечує потужну підтримку розвитку VPN-сервісів [9].

Як працює MPLS? Основна мета MPLS – це правильне пересилання пакетів, що входять у домен MPLS, до їхнього призначення. Цей процес поділяється на дві частини: встановлення LSP та пересилання пакетів уздовж LSP.

MPLS – це технологія, яка використовує мітки для направлення пересилання пакетів даних. У цій технології встановлення LSP є процесом, у якому LSR уздовж LSP визначають мітки для конкретного FEC.

Мітки MPLS призначаються та розповсюджуються вузлом нижчого рівня до вузла вищого рівня. LSR нижчого рівня класифікує FEC на основі адрес призначення IP-маршрутів і розподіляє мітки для FEC, що відповідають вказаним адресам призначення. Потім LSR нижчого рівня надсилає мітки до LSR вищого рівня, ініціюючи встановлення LFIB на вузлі вищого рівня. Цей процес повторюється, поки серія LSR не утворить LSP (рис. 1.5).

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

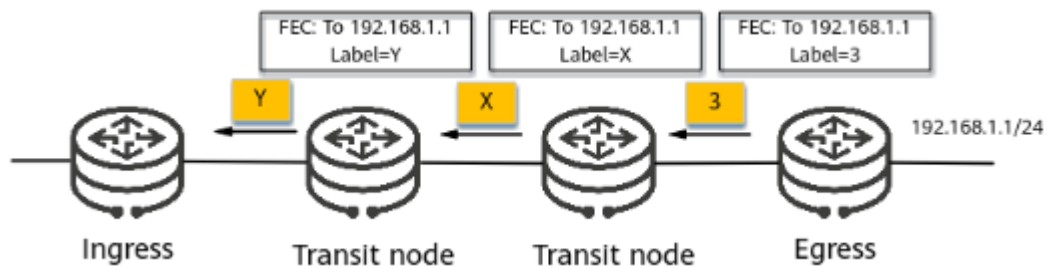


Рисунок 1.5 – Процес утворення LSP

LSP можна класифікувати на статичні та динамічні LSP в залежності від того, як вони встановлюються:

- Статичні LSP встановлюються шляхом ручного призначення міток для FEC. У цьому випадку вихідне значення мітки на LSR вищого рівня повинно збігатися з вхідним значенням мітки на LSR нижчого рівня.

- Динамічний LSP встановлюється, коли LSR використовує протокол розподілу міток для динамічного генерування та розподілу міток. LSR нижчого рівня використовує IP-маршрути для відправки міток до LSR вищого рівня. MPLS підтримує різні протоколи розподілу міток, такі як протокол розподілу міток (LDP), протокол резервування ресурсів для інженерії трафіку (RSVP-TE) та мультипротокове розширення для протоколу прикордонного шлюзу (MP-BGP).

LDP (Протокол розподілу міток) є важливим протоколом керування розподілом міток у системі MPLS. Він відповідає за класифікацію FEC, розподіл міток MPLS та динамічне встановлення і підтримку LSP. LDP визначає різні повідомлення та відповідні процедури для обробки повідомлень під час розподілу міток. Завдяки LDP, LSR можуть безпосередньо відображати маршрутизовану інформацію на мережевому рівні на LSP на каналному рівні, що дозволяє динамічно встановлювати LSP на мережевому рівні [9].

Повідомлення сесії LDP класифікуються на такі типи:

- Повідомлення виявлення (Discovery message): використовується для сповіщення або підтримки присутності LSR.
- Повідомлення сесії (Session message): використовується для встановлення, підтримки та завершення сесій між LDP-сумісними вузлами. Повідомлення

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

ініціалізації та повідомлення про підтримку з'єднання (Keepalive) є типами повідомлень сесії.

- Повідомлення оголошення (Advertisement message): використовується для створення, змінювання або видалення відображення між FEC та мітками.
- Повідомлення сповіщення (Notification message): використовується для надання інформації-консультацій або інформації про помилки.

RSVP був спеціально розроблений для моделі інтегрованих послуг, що дозволяє користувачам запитувати та отримувати різні рівні якості обслуговування (QoS) для Інтернет-додатків. Працюючи як в мережах IPv4, так і IPv6, RSVP не є протоколом маршрутизації. Натомість його основна функція – керувати та рекламувати зарезервовані ресурси в мережі. Отримувач ініціює запит на резервування ресурсів, який потім поширюється вздовж шляху передачі для резервування ресурсів на кожному вузлі, через який проходить запит. Коли отримувач запитує ресурси, він відправляє повідомлення Path для ініціації процесу. Відправник відповідає, надсилаючи повідомлення Resv, що завершує виділення та резервування ресурсів вздовж зворотного шляху повідомлення Path.

RSVP-TE, розширення RSVP, спеціально розроблений для цілей інженерії трафіку. Він вводить нові об'єкти, які допомагають встановлювати MPLS LSP. Об'єкт Label_Request включається в повідомлення Path для ініціації запитів на мітки, а об'єкт Label включається в повідомлення Resv для розподілу міток. Включаючи обмеження шляху, такі як атрибути пропускну здатності та атрибути спорідненості, RSVP-TE оптимізує планування шляхів і управління трафіком у мережі.

Типове застосування MPLS – MPLS VPN. MPLS VPN – це технологія, яка використовує MPLS для побудови VPN на мережі IP. Суть VPN полягає в тому, щоб передавати сервісні дані через публічну мережу так, наче вони перебувають на приватній мережі. Для цього на публічній мережі має бути налаштований тунель, через який дані можуть бути передані безпосередньо до призначення. Зазвичай MPLS VPN використовує LSP, створені за допомогою MPLS, як тунелі публічної мережі для передачі сервісних даних приватної мережі [9].

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

Основна модель MPLS VPN складається з трьох ролей:

- Граничний маршрутизатор клієнта (CE): пристрій на межі мережі користувача. CE безпосередньо підключений до мережі постачальника послуг (SP) через інтерфейси. Веб-сайти VPN користувачів підключені до мережі SP через CE. CE може бути мережею або хостом. Зазвичай CEs не знають про VPN і не потрібно підтримувати MPLS.

- Граничний маршрутизатор провайдера (PE): пристрій на межі мережі SP. PE безпосередньо підключений до CE. У мережі MPLS PEs виконують функції LSR і обробляють усі MPLS та VPN послуги. Це ставить високі вимоги до продуктивності PEs.

- Проміжний маршрутизатор провайдера (P): пристрій у магістральній мережі SP. P не підключений безпосередньо до CE. У мережі MPLS P функціонує як LSR і обробляє лише MPLS послуги. Йому не потрібно зберігати інформацію про VPN.

У MPLS VPN пакет VPN несе зовнішню та внутрішню мітки. Зовнішня мітка замінюється, коли пакет знаходиться в магістральній мережі. Ця мітка ідентифікує LSP від локального PE до партнерського PE, визначаючи шлях пакета до партнерського PE. Внутрішня мітка визначає VPN-екземпляр пакета, коли він передається від партнерського PE до партнерського CE. Пакет пересилається до цільового сайту на основі маршрутизуючої таблиці VPN-екземпляра. Зовнішня мітка виділяється за допомогою LDP та RSVP-TE, а внутрішня мітка – за допомогою LDP.

MPLS VPN повністю використовує технічні переваги MPLS і є найбільш широко використовуваною технологією VPN. Вона надає такі переваги:

- MPLS мітка відповідає потоку даних певної послуги (конкретний FEC), що допомагає ізолювати послуги різних користувачів.

- MPLS забезпечує можливості для управління трафіком (TE) та якості обслуговування (QoS). Користувачі можуть використовувати MPLS для повної оптимізації конфігурації ресурсів VPN.

- MPLS VPN забезпечує гнучкий контроль політик для задоволення особливих вимог різних користувачів та швидкої реалізації додаткових послуг.

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до першого розділу

У даному розділі ми дослідили реалізацію контролю доступу за допомогою протоколу керування доступом до мережі на основі портів 802.1X та протоколу RADIUS у ІКМ. Для реалізації контролю доступу було обрано саме RADIUS зважаючи на його переваги, а саме його підтримку 802.1X та його сумісність з пристроями різних виробників. Було розглянуто функціонування VPN, класифікацію відповідно до застосування VPN та класифікацією на основі режиму роботи VPN. Обрано MPLS VPN зважаючи на переваги та досліджено функціонування MPLS та MPLS VPN.

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1 Проектування фізичної топології мережі

Топологія мережі використовується для опису фізичної та логічної організації мережевих елементів. Вона демонструє, як саме розміщені й з'єднані між собою такі пристрої, як комутатори, маршрутизатори та інші вузли мережі.

Грамотно спроектована мережна топологія сприяє підвищенню ефективності роботи користувачів і спрощує адміністрування, дозволяючи швидко виявляти й усувати несправності, а також забезпечувати ефективний обмін даними та ресурсами.

Топології мережі поділяються на два основні типи:

- Фізична топологія – відображає реальне фізичне розташування пристроїв і їх з'єднання.

- Логічна топологія – показує, яким чином передаються дані між пристроями незалежно від фізичного розміщення.

Базові типи топологій мереж:

- Шина (Bus) – всі пристрої з'єднані одним кабелем. Дані розсилаються всім вузлам, але обробляються лише тим, для якого вони призначені. Ця топологія є простою, але має обмеження щодо масштабу та розширення, тому підходить лише для невеликих мереж.

- Кільцева (Ring) – пристрої з'єднані в замкнене кільце, а дані передаються в одному напрямку через кожен вузол. Вихід з ладу одного вузла призводить до зупинки всієї мережі.

- Зіркоподібна (Star) – усі пристрої підключаються до центрального вузла окремими лініями зв'язку. Відмова центрального вузла призводить до непрацездатності всієї мережі.

Похідні (комплексні) топології:

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

- Сітчаста (Mesh) – кожен вузол має прямі з’єднання з іншими. Це забезпечує високу надійність, швидкість та безпеку, проте така топологія складна в реалізації й дорога.

- Деревоподібна (Tree) – варіант топології зірки з ієрархічною структурою. Вона масштабована та зручна для адміністрування, однак залежить від працездатності центрального вузла та має високу вартість реалізації.

- Гібридна (Hybrid) – поєднує різні типи топологій, що забезпечує гнучкість і масштабованість, але вимагає ретельного проектування і значних витрат.

Для реалізації ІКМ організації обрано гібридну топологію, що базується на трирівневій моделі архітектури мережі, яка включає:

- Рівень ядра
- Рівень розподілу
- Рівень доступу [1]

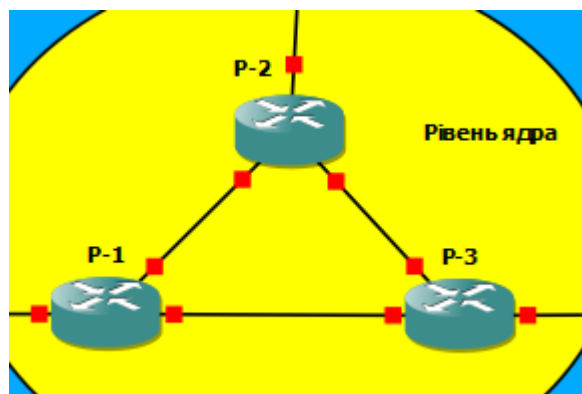


Рисунок 2.1 – Рівень ядра

Рівень ядра виконує роль центральної магістралі мережі, інтегруючи всі пристрої розподільчого рівня. Його основне завдання – забезпечення високошвидкісного передавання даних між різними частинами інфраструктури, а також швидке виявлення та ліквідація потенційних несправностей у мережі.

Рівень ядра у побудованій мережі складається з 3 маршрутизаторів (рис. 2.1). Маршрутизатор Р-1 під’єднаний до маршрутизатора РЕ-1 на рівні розподілу (рис. 2.2). Маршрутизатор Р-2 під’єднаний до маршрутизатора РЕ-2 на рівні розподілу (рис. 2.3). Маршрутизатор Р-3 під’єднаний до маршрутизатора РЕ-3 на рівні розподілу (рис. 2.4).

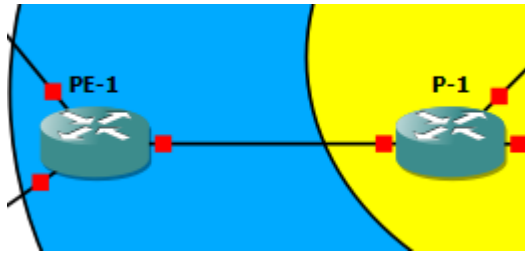


Рисунок 2.2 – Рівень розподілу

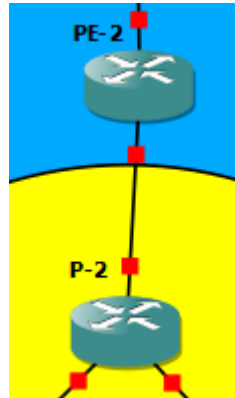


Рисунок 2.3 – Рівень розподілу

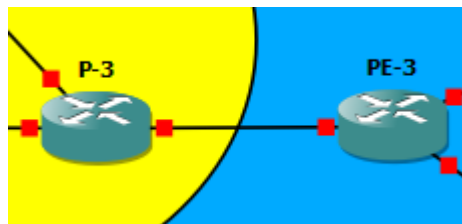


Рисунок 2.4 – Рівень розподілу

Рівень розподілу виконує роль посередника між рівнями доступу та ядра, виконуючи низку критично важливих завдань:

- об'єднує великі комутаційні сегменти мережі,
- з'єднує широкомовні домени другого рівня та визначає межі маршрутизації третього рівня,
- реалізує інтелектуальні функції маршрутизації, комутації та політик контролю доступу,
- підвищує надійність мережі завдяки використанню резервних комутаторів, що забезпечують альтернативні шляхи до ядра,
- забезпечує підтримку різних сервісів відповідно до класу застосунків на межі мережі.

Рівень розподілу у побудованій мережі складається з 3 маршрутизаторів. кожен з яких під'єднаний до маршрутизатора рівня ядра та різних маршрутизаторів на рівні доступу.

Рівень доступу формує крайову частину мережі, через яку здійснюється вхідний та вихідний трафік. Основне завдання комутаторів цього рівня – забезпечити користувачам фізичне підключення до мережі. Вони з'єднуються з маршрутизаторами рівня розподілу, які відповідають за впровадження ключових мережевих функцій, таких як маршрутизація, контроль якості обслуговування та механізми безпеки [2].

Рівень доступу складається з трьох сайтів, де перший сайт має 2 офіси з підмережами А та В. Другий сайт має 2 офіси з підмережами А та В. Третій сайт має 1 офіс, де потрібно забезпечити передачу трафіка між сайтами 1 та 2.

Маршрутизатор PE-1 під'єднаний до CE-1 та CE-2 (рис. 2.5). CE-1 під'єднано до сайту 1 підмережі А (рис. 2.6) та CE-2 під'єднано до сайту 2 підмережі А (рис. 2.7). На PE-1 потрібно забезпечити, щоб трафік між сайтами 1 та 2 не мав змогу передаватися. Підмережа А сайту 1 має містити до 200 пристроїв, тому даній підмережі було виділено маску /24. Підмережа А сайту 2 має містити до 45 пристроїв, тому даній підмережі було виділено маску /26.

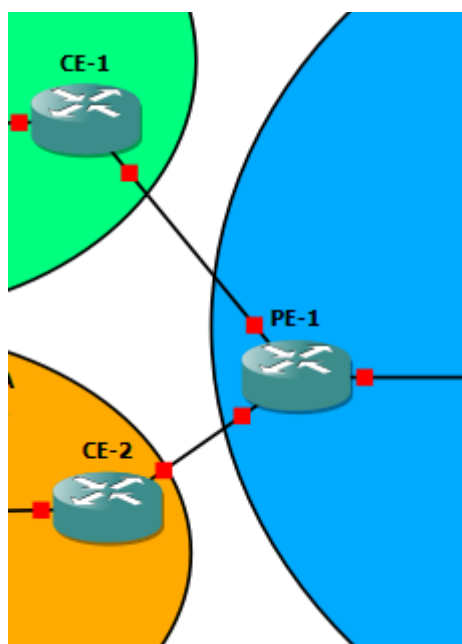


Рисунок 2.5 – Рівень доступу

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

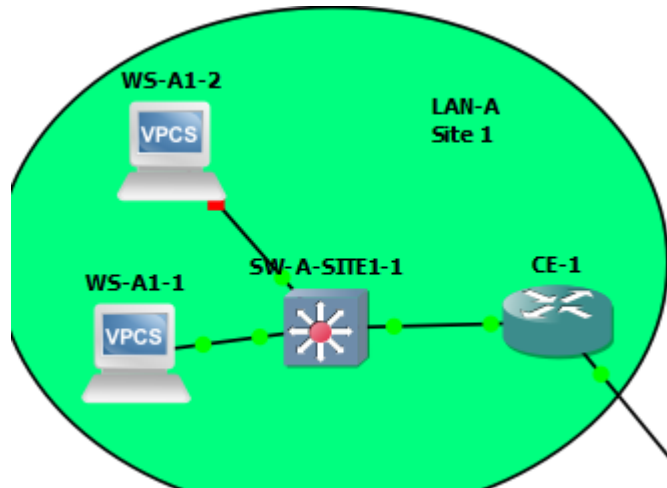


Рисунок 2.6 – LAN A Site 1

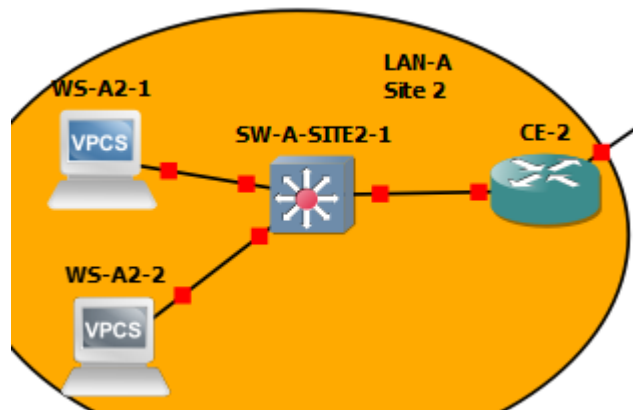


Рисунок 2.7 – LAN A Site 2

Маршрутизатор PE-2 під'єднаний до CE-3 (рис. 2.8). CE-3 під'єднано до сайта 3 підмережі А (рис. 2.9). На PE-2 потрібно забезпечити, щоб сайт 3 мав змогу передавати трафік між усіма сайтами. Підмережа А сайта 3 має містити до 20 пристроїв, тому даній підмережі було виділено маску /27.

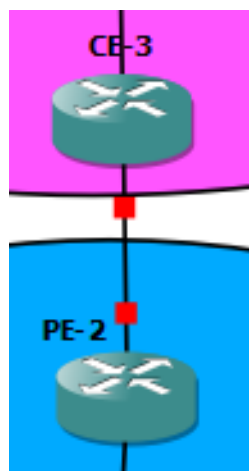


Рисунок 2.8 – Рівень доступу

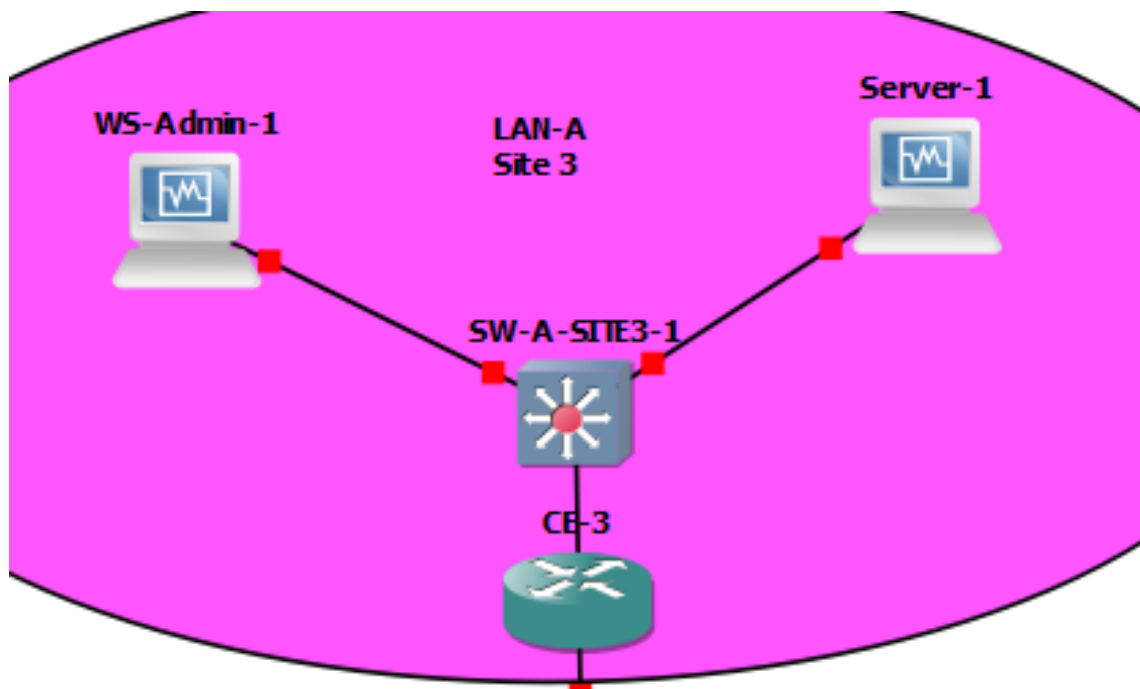


Рисунок 2.9 – LAN A Site 3

Маршрутизатор PE-3 під'єднаний до CE-4 та CE-5 (рис. 2.10). CE-4 під'єднано до сайта 1 підмережі В (рис. 2.11) та CE-2 під'єднано до сайта 2 підмережі В (рис. 2.12). На PE-3 потрібно забезпечити, щоб трафік між сайтами 1 та 2 не мав змогу передаватися. Підмережа В сайта 1 має містити до 100 пристроїв, тому даній підмережі було виділено маску /25. Підмережа В сайта 2 має містити до 220 пристроїв, тому даній підмережі було виділено маску /24.

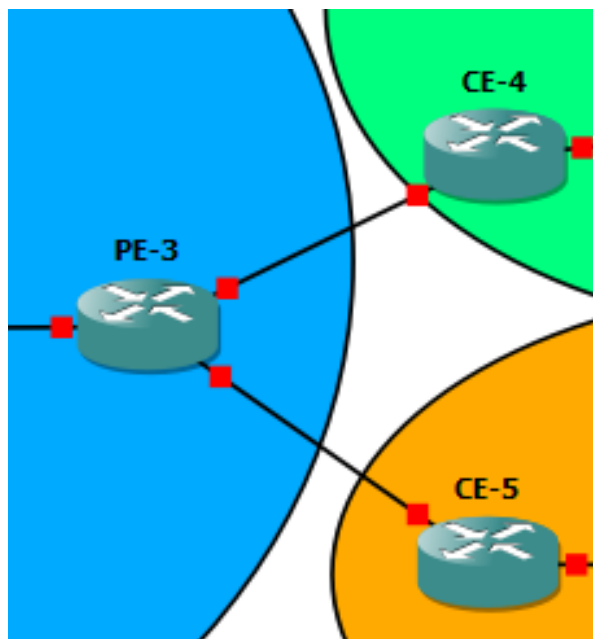


Рисунок 2.10 – Рівень доступу

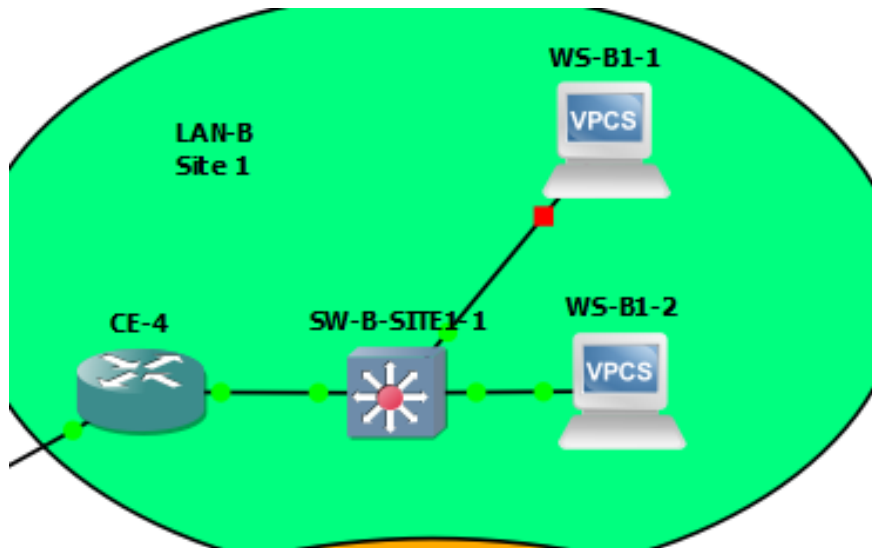


Рисунок 2.11 – LAN B Site 1

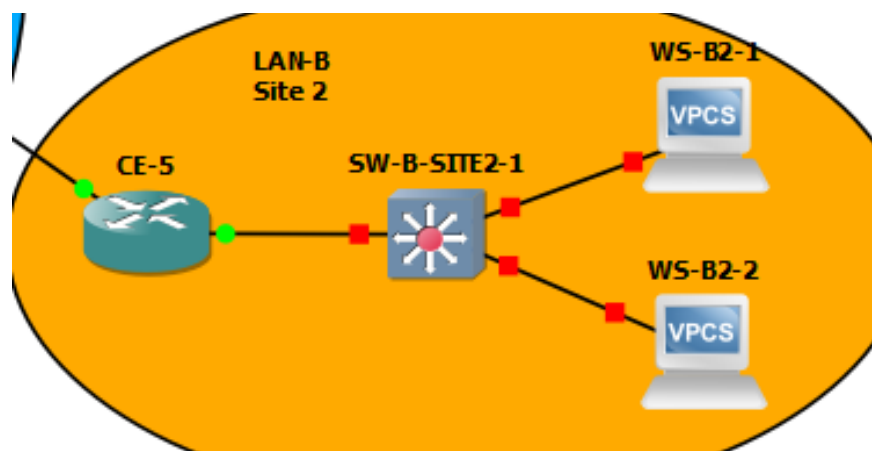


Рисунок 2.12 – LAN B Site 2

2.2 Розробка схеми адресації мережі

Підмережа – це логічно виділений сегмент більшої комп'ютерної мережі. Основна мета її створення – розділення великої мережі на менші, взаємопов'язані частини, що допомагає зменшити обсяг трафіку та запобігти його надмірному поширенню по всій мережі.

IP-адреси розподіляються між підмережами таким чином, щоб кожен пристрій мав унікальну адресу для підключення, а також був забезпечений певний резерв адрес для майбутнього розширення мережі та додавання нових пристроїв.

Таблиця 2.1 – Адресація між рівнем ядра та рівнем розподілу

Канал	Підмережа
P-1 – P-2	200.24.5.0/30
P-1 – P-3	200.24.5.4/30
P-2 – P-3	200.24.5.8/30

Продовження таблиці 2.1

Канал	Підмережа
P-1 – PE-1	200.24.5.12/30
P-2 – PE-2	200.24.5.16/30
P-3 – PE-3	200.24.5.20/30

Таблиця 2.2 – Адресація між рівнем розподілу та рівнем доступу

Канал	Підмережа
PE-1 – CE-1	200.24.5.24/30
PE-1 – CE-2	200.24.5.28/30
PE-2 – CE-3	200.24.5.32/30
PE-3 – CE-4	200.24.5.36/30
PE-3 – CE-5	200.24.5.40/30

Таблиця 2.3 – Адресація підмережі А сайта 1

Призначення	IP-адреса
Адреса мережі	190.24.5.0
Маска мережі	255.255.255.0/24
Мінімальна адреса	190.24.5.1
Максимальна адреса	190.24.5.254
Широкомовна адреса	190.24.5.255

Таблиця 2.4 – Адресація підмережі А сайта 2

Призначення	IP-адреса
Адреса мережі	190.24.6.0
Маска мережі	255.255.255.192/26
Мінімальна адреса	190.24.6.1
Максимальна адреса	190.24.6.62
Широкомовна адреса	190.24.6.63

Таблиця 2.5 – Адресація підмережі А сайта 3

Призначення	IP-адреса
Адреса мережі	199.24.5.0
Маска мережі	255.255.255.224/27
Мінімальна адреса	199.24.5.1
Максимальна адреса	199.24.5.30
Широкомовна адреса	199.24.5.31

Таблиця 2.6 – Адресація підмережі В сайта 1

Призначення	IP-адреса
Адреса мережі	191.24.5.0
Маска мережі	255.255.255.128/25

Призначення	IP-адреса
Мінімальна адреса	191.24.5.1
Максимальна адреса	191.24.5.126
Широкомовна адреса	191.24.5.127

Таблиця 2.7 – Адресація підмережі В сайта 2

Призначення	IP-адреса
Адреса мережі	191.24.6.0
Маска мережі	255.255.255.0/24
Мінімальна адреса	191.24.6.1
Максимальна адреса	191.24.6.254
Широкомовна адреса	191.24.6.255

2.3 Розробка підсистеми контролю доступу до мережі

Підсистема контролю доступу є ключовим елементом забезпечення інформаційної безпеки мережі. Основна мета цієї підсистеми – обмеження несанкціонованого доступу до інформаційних ресурсів організації, як з боку внутрішніх користувачів, так і з боку зовнішніх загроз. У межах проєкту передбачається реалізація контролю доступу на основі технологій 802.1X, RADIUS, а також розмежування трафіку через MPLS VPN з використанням VRF (Virtual Routing and Forwarding).

Першим кроком у розробці стало визначення політик доступу. Користувачі були класифіковані за типами: адміністративний персонал, технічні працівники, віддалені користувачі та гостьовий доступ. Для кожної категорії визначено окремі рівні доступу до ресурсів мережі, з урахуванням принципу мінімальних привілеїв.

Для аутентифікації користувачів обрано протокол 802.1X, який забезпечує контроль доступу на рівні портів комутаторів. Комутатори діють як аутентифікатори, що перенаправляють запити аутентифікації до сервера RADIUS. У ролі RADIUS-сервера виступає Network Policy Server (NPS), розгорнутий на основі Windows Server, що забезпечує централізовану аутентифікацію, авторизацію та ведення журналів доступу.

Для інтеграції з корпоративною системою ідентифікації NPS пов'язано з Active Directory, що дозволяє застосовувати політики доступу на основі груп користувачів. Наприклад, співробітники відділу бухгалтерії можуть мати доступ лише

до обмеженого сегменту мережі, що ізольовано за допомогою окремої VRF у структурі MPLS L3VPN.

Реалізація VRF дозволяє логічно розділити мережу на ізольовані домени маршрутизації, забезпечуючи ефективне розмежування доступу між підрозділами без потреби в додатковому фізичному розділенні. Це особливо актуально для забезпечення безпеки даних, які передаються між віддаленими офісами через MPLS-мережу провайдера.

Додатково застосовано механізми фільтрації трафіку з використанням ACL (Access Control Lists) на маршрутизаторах, що дозволяє обмежити міжмережеву взаємодію навіть у межах однієї VPN. Це гарантує, що навіть у разі компрометації одного вузла, зломисник не зможе отримати доступ до всієї мережі.

У результаті реалізації підсистеми контролю доступу було досягнуто високого рівня безпеки, централізації управління доступом та зниження ризиків внутрішніх загроз. Підхід, що поєднує 802.1X, RADIUS, Active Directory та MPLS VPN, забезпечує гнучкість, масштабованість і надійність інформаційно-комунікаційної мережі організації.

Висновки до другого розділу

У даному розділі ми розробили проект мережі, розглянули рівень ядра, рівень розподілу та рівень доступу у розробленій мережі. Було виконано розподіл IP-адрес між підмережами. Було розроблено підсистему контролю доступу до мережі.

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Cisco 7201 підтримує технології контролю доступу, такі як AAA (Authentication, Authorization, Accounting), 802.1X, RADIUS, TACACS+, що дозволяє інтегрувати його у проєктовану підсистему контролю доступу.

Пристрій має доведену на практиці стабільність у роботі під навантаженням, що робить його доцільним вибором для критично важливих мережевих компонентів, які забезпечують передачу конфіденційних даних.



Рисунок 3.2 – Cisco WS-C3560-24PS-E

В межах проєктування захищеної інформаційно-комунікаційної мережі з використанням технологій MPLS VPN та контролю доступу за допомогою 802.1X було обрано комутатор Cisco Catalyst WS-C3560-24PS-E (рис. 2.13).

Даний пристрій поєднує у собі функціональність рівня 2 (L2) та рівня 3 (L3), забезпечуючи не лише ефективну комутацію, а й базову маршрутизацію, необхідну для сегментації мережі та реалізації інтервлан-маршрутизації.

Однією з ключових причин вибору цієї моделі стала наявність прошивки IP Services IOS, яка відкриває розширені функції маршрутизації. Зокрема, пристрій підтримує статичну маршрутизацію, протоколи RIP, OSPF та EIGRP. Також доступна функція ip routing, яка активує можливість маршрутизації між віртуальними інтерфейсами VLAN (SVI). Завдяки цьому забезпечується логічне розділення мережі, що є основою для реалізації політик доступу та безпеки.

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

У контексті проєкту, де планується використання авторизації на основі RADIUS та 802.1X, даний комутатор підтримує всі необхідні механізми. Зокрема, він дозволяє реалізувати контроль доступу до мережі з аутентифікацією користувачів, фільтрацію трафіку за допомогою списків контролю доступу (ACL), а також перенаправлення запитів до DHCP-сервера (DHCP Relay).

Зважаючи на цілі проєкту – побудова підсистеми контролю доступу у корпоративній мережі з інтеграцією 802.1X та централізованим управлінням доступом – було прийнято рішення використати Windows Server з роллю Network Policy Server (NPS) як RADIUS-сервер. Це обґрунтовано наступними причинами:

- Тісна інтеграція з Active Directory (AD). Windows NPS дозволяє напряду використовувати облікові записи домену, групи безпеки та політики AD для аутентифікації користувачів та пристроїв. Це дає змогу централізовано керувати правами доступу без створення окремих баз даних користувачів.

- Підтримка 802.1X та політик контролю доступу. NPS повністю підтримує аутентифікацію 802.1X для комутаторів і точок доступу, дозволяючи гнучко налаштовувати умови доступу – зокрема, обмеження за MAC-адресою, групою користувачів або типом пристрою.

- Зручність у налаштуванні та GUI. Адміністрування через графічний інтерфейс значно спрощує конфігурацію для адміністраторів, які не мають досвіду роботи з CLI або open-source інструментами, такими як FreeRADIUS.

- Інтеграція з системами аудиту та безпеки Windows. Усі спроби доступу, помилки аутентифікації та політики логуються в Event Viewer, що дозволяє легко здійснювати аудит та моніторинг мережевої активності.

- Відсутність потреби у сторонньому ПЗ. Оскільки Windows Server вже використовується як контролер домену, встановлення NPS не вимагає додаткових ресурсів чи витрат, що є економічно ефективним рішенням.

Попри існування потужних альтернатив, таких як FreeRADIUS або Cisco ISE, Windows NPS виявився найбільш збалансованим варіантом для реалізації централізованої аутентифікації в мережі малого або середнього підприємства. Його інтеграція з Active Directory, підтримка 802.1X, простота налаштування та

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

відповідність вимогам до безпеки зробили його оптимальним вибором для реалізації підсистеми контролю доступу в межах проєкту.

3.2 Налаштування IP-адресації на пристроях, налаштування маршрутизації та перевірка зв'язку

Для реалізації проєкту підсистеми контролю доступу для захищеної інформаційно-комунікаційної мережі з використанням технології MPLS VPN потрібно налаштувати IP-адресацію, маршрутизацію та перевірити зв'язок ключовими вузлами.

```
P-1(config)#int fa0/0
P-1(config-if)#ip add 200.24.5.13 255.255.255.252
P-1(config-if)#no shut
P-1(config-if)#int fal/0
P-1(config-if)#
*Jun 20 06:12:13.231: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Jun 20 06:12:14.231: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
P-1(config-if)#ip add 200.24.5.1 255.255.255.252
P-1(config-if)#no shut
P-1(config-if)#int fal/1
*Jun 20 06:12:26.939: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Jun 20 06:12:27.939: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
P-1(config-if)#int fal/1
P-1(config-if)#ip add 200.24.5.5 255.255.255.252
P-1(config-if)#no shut
P-1(config-if)#
*Jun 20 06:12:45.539: %LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
*Jun 20 06:12:46.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
P-1(config-if)#
```

Рисунок 3.3 – Налаштування адресації на маршрутизаторі P-1

```
P-1#ping 200.24.5.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.24.5.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 16/27/48 ms
P-1#
```

Рисунок 3.4 – Перевірка зв'язку в межах однієї підмережі

```
P-1(config)#router ospf 1
P-1(config-router)#network 200.24.5.0 0.0.0.3 area 0
P-1(config-router)#network 200.24.5.4 0.0.0.3 area 0
P-1(config-router)#network 200.24.5.12 0.0.0.3 area 0
P-1(config-router)#
```

Рисунок 3.5 – Налаштування маршрутизації на маршрутизаторі P-1

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

```

P-1#ping 200.24.5.41
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.24.5.41, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/37/52 ms
P-1#ping 200.24.5.33
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.24.5.33, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/60/80 ms
P-1#ping 200.24.5.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.24.5.21, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/36/48 ms
P-1#

```

Рисунок 3.6 – Перевірка зв'язку між різними підмережами

3.3 Налаштування MPLS VPN

Для забезпечення захищеної передачі даних між сайтами потрібно налаштувати роботу MPLS L3VPN:

```

P-1(config)#int loopback1
P-1(config-if)#ip add 3.3.3.1 255.255.255.255
P-1(config-if)#exit
P-1(config)#mpls ip
P-1(config)#mpls label protocol ldp
P-1(config)#mpls ldp router-id ll force
P-1(config)#int range fa0/0,fa1/0,fa1/1
P-1(config-if-range)#mpls ip
P-1(config-if-range)#exit
P-1(config)#router ospf 1
P-1(config-router)#network 3.3.3.1 0.0.0.0 area 0
P-1(config-router)#

```

Рисунок 3.7 – Налаштування функціонування MPLS на P-1

Команда “mpls ip” у режимі глобальної конфігурації вмикає роботу MPLS глобально. Готує маршрутизатор до використання MPLS-міток для пересилання пакетів. Дозволяє налаштовувати пов'язані з MPLS протоколи, такі як LDP та RSVP. Необхідна для роботи MPLS на інтерфейсах, коли команда “mpls ip” також увімкнена на цих інтерфейсах.

Команда “mpls label protocol ldp” встановлює LDP як протокол розповсюдження міток. Забезпечує призначення та рекламу міток за допомогою LDP для MPLS-пересилання. Потрібна у випадках, коли є кілька варіантів розповсюдження міток.

Команда “mpls ldp router-id loopback1 force” встановлює ідентифікатор маршрутизатора LDP на IP-адресу інтерфейсу Loopback1. Ключове слово force вказує

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

маршрутизатору примусово використати цей ідентифікатор, навіть якщо LDP-сеанси вже були встановлені.

Команда “mpls ip” у режимі конфігурації інтерфейсу вмикає пересилання MPLS на цьому конкретному інтерфейсі. Вказує маршрутизатору використовувати мітки (а не IP-маршрутизацію) для пересилання пакетів, отриманих або надісланих через цей інтерфейс. Дозволяє маршрутизатору надсилати та отримувати мічені пакети через цей інтерфейс. Додає можливість протоколу LDP надсилати сусідам відповідні мітки на цьому інтерфейсі.

```
PE-1(config)#int loopback1
PE-1(config-if)#ip add
*Jun 20 08:08:10.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
PE-1(config-if)#ip add 2.2.2.1 255.255.255.255
PE-1(config-if)#exit
PE-1(config)#mpls ip
PE-1(config)#mpls label protocol ldp
PE-1(config)#mpls ldp router-id ll force
PE-1(config)#int fa0/0
PE-1(config-if)#mpls ip
PE-1(config-if)#exit
PE-1(config)#router ospf 1
PE-1(config-router)#network 2.2.2.1 0.0.0.0 area 0
PE-1(config-router)#
```

Рисунок 3.8 – Налаштування функціонування MPLS на PE-1

```
PE-1(config)#vrf definition S1
PE-1(config-vrf)#address-family ipv4
PE-1(config-vrf-af)#rd 100:1
PE-1(config-vrf)#route-target both 100:1
PE-1(config-vrf)#route-target import 300:1
PE-1(config-vrf)#exit
PE-1(config)#vrf definition S2
PE-1(config-vrf)#address-family ipv4
PE-1(config-vrf-af)#rd 200:1
PE-1(config-vrf)#route-target both 200:1
PE-1(config-vrf)#route-target import 300:1
PE-1(config-vrf)#
```

Рисунок 3.9 – Створення vrf, перехід до адресного простору ipv4, налаштування унікального ідентифікатора RD та налаштування імпорту та експорту маршрутів на PE-1

VRP – це технологія, що дозволяє розділити маршрутизатор на кілька незалежних логічних маршрутизаторів. Кожен VRF має свій власний таблицю маршрутизації, що ізолює трафік між різними мережами або клієнтами.

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Route Distinguisher (RD) – унікальний ідентифікатор, який додається до IPv4-префіксів у VRF.

Route-Target – це розширений атрибут спільноти BGP, який використовується для контролю імпорту та експорту маршрутів у VRF. Він працює як тег, який допомагає визначити, які маршрути VPN обмінюються між різними сайтами.

Команда “route-target export” визначає, які Route-Target будуть додані до маршрутів, що походять із цього VRF. Коли цей VRF рекламує свої маршрути через MP-BGP, ці маршрути несуть цей тег Route-Target для експорту. Цей тег позначає маршрути як такі, що належать до "спільноти" або групи цього VRF.

Команда “route-target import” визначає, які Route-Target цей VRF прийматиме. Маршрутизатор імпортуватиме маршрути до цього VRF лише в тому випадку, якщо рекламований маршрут має один із RT, перелічених в import. Це керує тим, які маршрути з інших VRF або майданчиків будуть додані до таблиці маршрутизації цього VRF.

```
PE-1(config)#router bgp 100
PE-1(config-router)#neighbor 2.2.2.2 remote-as 100
PE-1(config-router)#neighbor 2.2.2.2 update-source 11
PE-1(config-router)#neighbor 2.2.2.3 remote-as 100
PE-1(config-router)#neighbor 2.2.2.3 update-source 11
PE-1(config-router)#address-family vpnv4
PE-1(config-router-af)#neighbor 2.2.2.2 activate
PE-1(config-router-af)#neighbor 2.2.2.3 activate
PE-1(config-router-af)#
```

Рисунок 3.10 – Налаштування BGP 100 на маршрутизаторі PE-1

BGP (Border Gateway Protocol) – це протокол зовнішньої маршрутизації, який використовується для обміну маршрутною інформацією між різними автономними системами в Інтернеті або у великих корпоративних мережах.

Команда “neighbor” вказує IP-адресу або ім'я сусіднього маршрутизатора BGP та налаштовує параметри взаємодії з ним.

Команда “neighbor remote-as” вказує номер автономної системи (AS) сусіда BGP. BGP – це міжавтоматичний протокол маршрутизації, тому кожен пір повинен знати AS іншого.

Команда “neighbor update-source” визначає IP-адресу або інтерфейс джерела, які маршрутизатор використовуватиме при встановленні BGP-сеансу з цим сусідом.

Команда “neighbor activate” активує сусіда BGP у цій адресній сім’ї, щоб можна було обмінюватися маршрутами.

Команда “address-family vpnv4” дозволяє BGP передавати маршрути VPNv4 – це IPv4-маршрути з доданим Route Distinguisher.

```
CE-1(config)#int loopback 1
CE-1(config-if)#ip a
*Jun 20 09:33:02.019: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
CE-1(config-if)#ip add 1.1.1.1 255.255.255.255
CE-1(config-if)#exit
CE-1(config)#router bgp 110
CE-1(config-router)#neighbor 200.24.5.25 remote-as 100
CE-1(config-router)#network 1.1.1.1 mask 255.255.255.255
CE-1(config-router)#address-family ipv4
CE-1(config-router-af)#neighbor 200.24.5.25 activate
CE-1(config-router-af)#redistribute connected
CE-1(config-router-af)#
```

Рисунок 3.11 – Налаштування BGP 110 на маршрутизаторі CE-1

Команда “redistribute connected” додає безпосередньо підключені маршрути до протоколу маршрутизації. Це дозволяє рекламувати ці підключені мережі іншим маршрутизаторам, що беруть участь у цьому протоколі маршрутизації.

```
PE-1(config)#router bgp 100
PE-1(config-router)#address-family ipv4 vrf S1
PE-1(config-router-af)#neighbor 200.24.5.26 remote-as 110
PE-1(config-router-af)#neighbor 200.24.5.26 activate
PE-1(config-router-af)#redistribute connected
PE-1(config-router-af)#exit
PE-1(config-router)#int fal/0
PE-1(config-if)#vrf forwarding S1
PE-1(config-if)#ip add 200.24.5.25 255.255.255.252
PE-1(config-if)#
```

Рисунок 3.12 – Налаштування BGP 100 на маршрутизаторі PE-1

Команда “vrf forwarding” асоціює інтерфейс з певним екземпляром VRF. Таким чином, трафік на цьому інтерфейсі буде ізольований у межах окремого маршрутизувального домену VRF.

```

PE-1(config)#router bgp 100
PE-1(config-router)#address-family ipv4 vrf S1
PE-1(config-router-af)#neighbor 200.24.5.26 remote-as 110
PE-1(config-router-af)#exit
PE-1(config-router)#int fal/0
PE-1(config-if)#vrf forwarding S1
% Interface FastEthernet1/0 IPv4 disabled and address(es) removed due to enabling VRF S1
PE-1(config-if)#
*Jun 20 09:49:58.911: %OSPF-5-ADJCHG: Process 1, Nbr 200.24.5.26 on FastEthernet1/0 from FULL to DOWN, Neighbor Down: Interface down or detached
PE-1(config-if)#ip add 200.24.5.25 255.255.255.252
PE-1(config-if)#
*Jun 20 09:50:14.235: %BGP-5-ADJCHANGE: neighbor 200.24.5.26 vpn vrf S1 Up
PE-1(config-if)#

```

Рисунок 3.12 – Налаштування BGP 100 на маршрутизаторі PE-1

```

PE-1#show ip route vrf S1

Routing Table: S1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

    1.0.0.0/32 is subnetted, 3 subnets
B       1.1.1.1 [20/0] via 200.24.5.26, 00:45:01
B       1.1.1.3 [200/0] via 2.2.2.2, 00:26:57
B       1.1.1.4 [200/0] via 2.2.2.3, 00:08:37
    190.24.0.0/24 is subnetted, 1 subnets
B       190.24.5.0 [20/0] via 200.24.5.26, 00:45:01
    191.24.0.0/25 is subnetted, 1 subnets
B       191.24.5.0 [200/0] via 2.2.2.3, 00:08:37
    199.24.5.0/27 is subnetted, 1 subnets
B       199.24.5.0 [200/0] via 2.2.2.2, 00:26:57
    200.24.5.0/24 is variably subnetted, 4 subnets, 2 masks
C       200.24.5.24/30 is directly connected, FastEthernet1/0
L       200.24.5.25/32 is directly connected, FastEthernet1/0
B       200.24.5.32/30 [200/0] via 2.2.2.2, 00:27:00
B       200.24.5.36/30 [200/0] via 2.2.2.3, 00:08:40
PE-1#

```

Рисунок 3.13 – Виведення таблиці маршрутизації vrf S1 на PE1

```

CE-1#ping 191.24.5.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.24.5.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/77/104 ms
CE-1#

```

Рисунок 3.14 – Перевірка зв'язку між site1 на PE1

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

```

PE-1#show bgp vpnv4 unicast all
BGP table version is 36, local router ID is 2.2.2.1
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: 100:1 (default for vrf S1)
*> 1.1.1.1/32             200.24.5.26              0                0 110 i
*>i 1.1.1.3/32            2.2.2.2                  0          100    0 130 i
*>i 1.1.1.4/32            2.2.2.3                  0          100    0 140 i
*> 190.24.5.0/24          200.24.5.26              0                0 110 ?
*>i 191.24.5.0/25         2.2.2.3                  0          100    0 140 ?
*>i 199.24.5.0/27         2.2.2.2                  0          100    0 130 ?
*> 200.24.5.24/30         0.0.0.0                  0                32768 ?
*                          200.24.5.26              0                0 110 ?
*>i 200.24.5.32/30        2.2.2.2                  0          100    0 ?
*>i 200.24.5.36/30        2.2.2.3                  0          100    0 ?
Route Distinguisher: 200:1 (default for vrf S2)
*> 1.1.1.2/32             200.24.5.30              0                0 120 i
*>i 1.1.1.3/32            2.2.2.2                  0          100    0 130 i
   Network                Next Hop              Metric LocPrf Weight Path
*>i 1.1.1.5/32            2.2.2.3                  0          100    0 150 i
*> 190.24.6.0/26          200.24.5.30              0                0 120 ?
*>i 191.24.6.0/24         2.2.2.3                  0          100    0 150 ?
*>i 199.24.5.0/27         2.2.2.2                  0          100    0 130 ?
* 200.24.5.28/30          200.24.5.30              0                0 120 ?
*>                          0.0.0.0                  0                32768 ?
*>i 200.24.5.32/30        2.2.2.2                  0          100    0 ?
*>i 200.24.5.40/30        2.2.2.3                  0          100    0 ?
Route Distinguisher: 300:1
*>i 1.1.1.3/32            2.2.2.2                  0          100    0 130 i
*>i 199.24.5.0/27         2.2.2.2                  0          100    0 130 ?
*>i 200.24.5.32/30        2.2.2.2                  0          100    0 ?
PE-1#

```

Рисунок 3.15 – Виведення інформації про маршрути bgp у режимі unicast для всіх VRF на PE1

```

PE-1#show mpls forwarding-table
Local   Outgoing Prefix      Bytes Label  Outgoing  Next Hop
Label   Label    or Tunnel Id Switched     interface
16      Pop Label 3.3.3.1/32    0           Fa0/0      200.24.5.13
17      24        3.3.3.2/32    0           Fa0/0      200.24.5.13
18      25        3.3.3.3/32    0           Fa0/0      200.24.5.13
19      Pop Label 200.24.5.0/30 0           Fa0/0      200.24.5.13
20      Pop Label 200.24.5.4/30 0           Fa0/0      200.24.5.13
21      16        200.24.5.8/30 0           Fa0/0      200.24.5.13
22      17        200.24.5.16/30 0          Fa0/0      200.24.5.13
23      18        200.24.5.20/30 0          Fa0/0      200.24.5.13
24      No Label 190.24.6.0/26[V] 980        Fa1/1      200.24.5.30
27      No Label 1.1.1.1/32[V] 0          Fa1/0      200.24.5.26
28      No Label 190.24.5.0/24[V] 4802       Fa1/0      200.24.5.26
29      No Label 200.24.5.24/30[V] \
30      No Label 200.24.5.28/30[V] \
31      No Label 1.1.1.2/32[V] 0          Fa1/1      200.24.5.30
33      19        2.2.2.2/32    0          Fa0/0      200.24.5.13
35      20        2.2.2.3/32    0          Fa0/0      200.24.5.13
PE-1#

```

Рисунок 3.16 – Таблиця пересилання mpls на PE1

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

```

CE-1#ping 190.24.6.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.24.6.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CE-1#

```

Рисунок 3.17 – Спроба перевірки зв'язку між site1 та site2 на PE1

3.4 Налаштування списків доступу, RADIUS та 802.1X

Для початку потрібно встановити роль Active Directory Domain Services на сервері Windows. Це робиться через Server Manager, де вибирається ця роль і запускається процес встановлення. Після інсталяції необхідно налаштувати контролер домену, задавши ім'я домену. Сервер тоді стає центром управління обліковими записами користувачів і комп'ютерів у мережі.

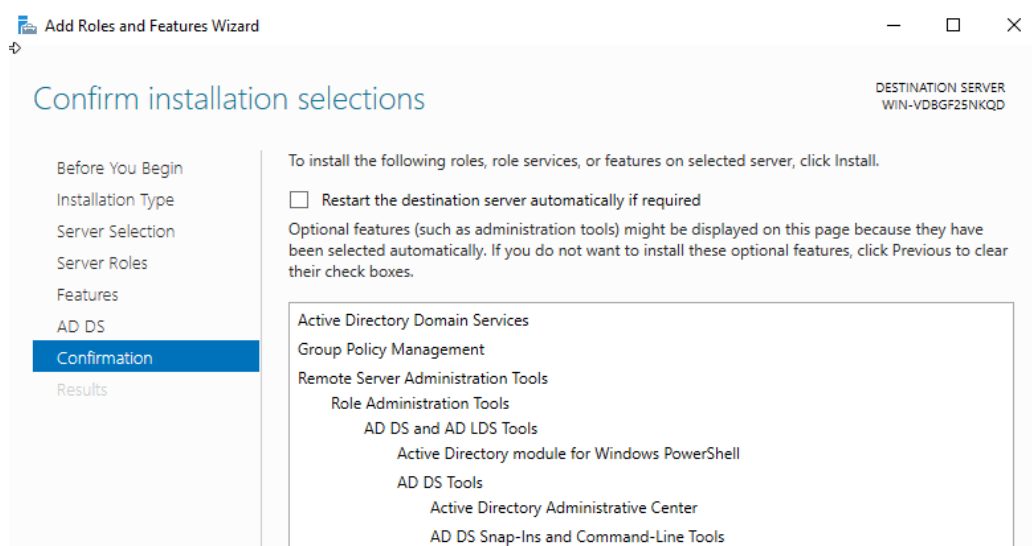


Рисунок 3.18 – Встановлення Active Directory Domain Services

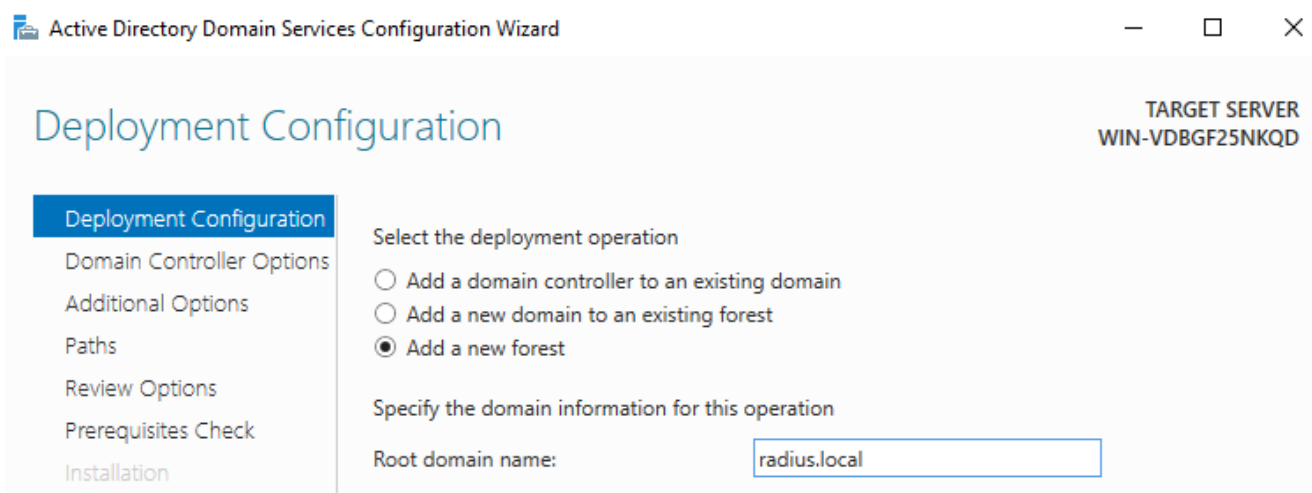


Рисунок 3.19 – Створення лісу в структурі AD

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Після встановлення AD потрібно створити користувачів та встановити роль Network Policy Server (NPS), яка служить RADIUS-сервером. Через Server Manager додається ця роль, після чого в консолі NPS сервер реєструється в Active Directory, що дає йому можливість аутентифікувати доменних користувачів. У самому NPS додаються RADIUS-клієнти – це мережеві пристрої, як-от комутатори чи маршрутизатори, які будуть надсилати запити на аутентифікацію. Для кожного пристрою задається IP-адреса, ім'я та спільний секрет (shared secret), який має збігатися з налаштуваннями на мережевому обладнанні.

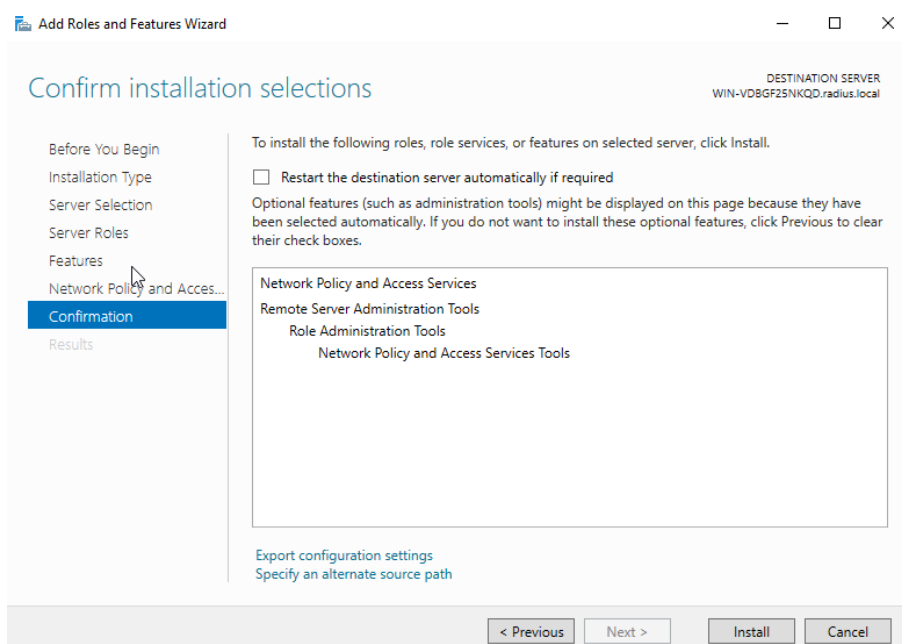


Рисунок 3.20 – Встановлення NPS

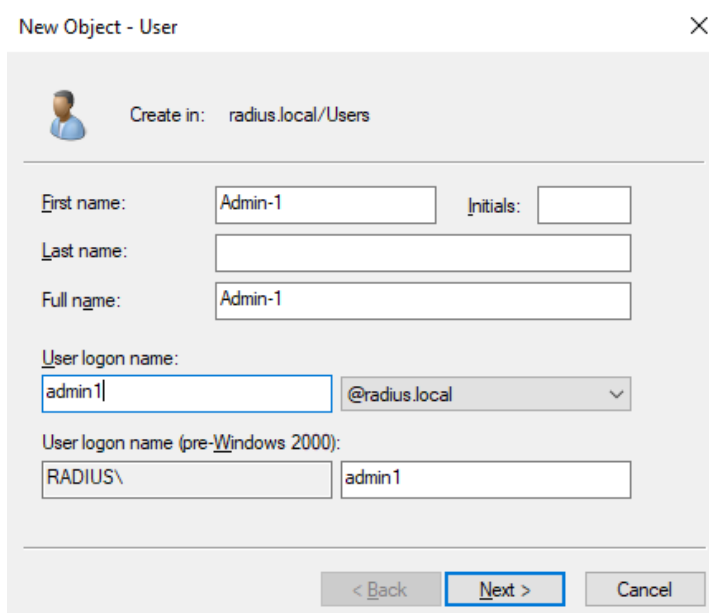


Рисунок 3.21 – Створення користувача admin1

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

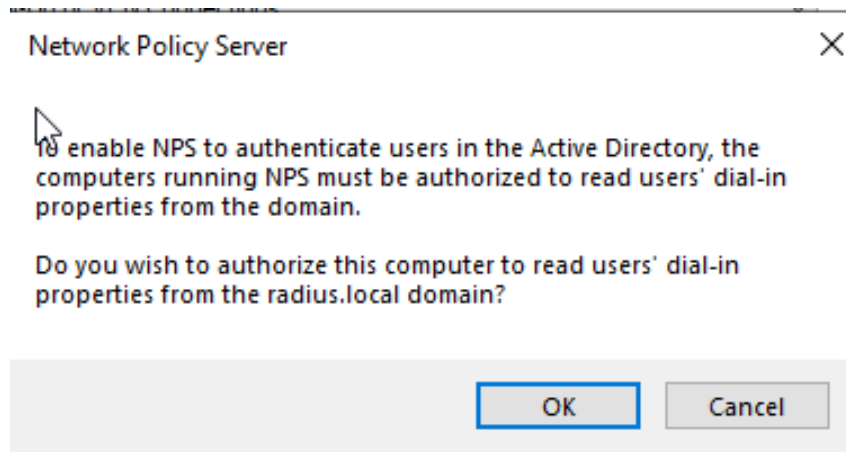


Рисунок 3.22 – Реєстрація сервера у AD

Для коректної роботи NPS створюються Network Policies – правила доступу, які визначають, які користувачі або групи з Active Directory мають право проходити аутентифікацію, і які методи аутентифікації використовуються (наприклад, EAP або PEAP). Також тут можна задати, хто має дозвіл або заборону на доступ до мережі.

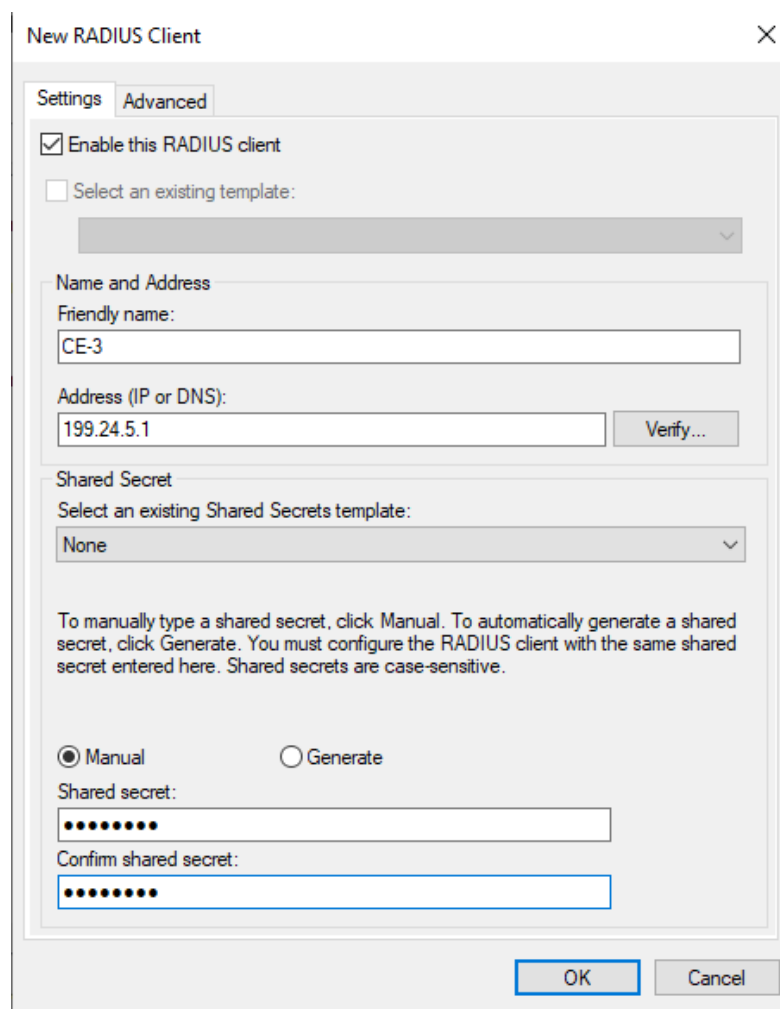


Рисунок 3.23 – Створення клієнта RADIUS

New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

Network connection method
 Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server:

☐ Vendor specific:

Рисунок 3.24 – Створення мережевої політики

New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
NAS Port Type	Ethernet

Рисунок 3.25 – Створення умови для підключення

New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

Network_Policy

Policy conditions:

Condition	Value
NAS Port Type	Ethernet

Policy settings:

Condition	Value
Authentication Method	Unencrypted authentication (PAP, SPAP) OR Encryption authentication (CHAP) OR MS-CHAP v1 ...
Access Permission	Grant Access
Service-Type	Framed
Ignore User Dial-In Properties	False

To close this wizard, click Finish.

Previous Next **Finish** Cancel

Рисунок 3.26 – Створена політика для підключення

Налаштування Cisco маршрутизатора як RADIUS-клієнта полягає в тому, щоб активувати AAA вказати сервер аутентифікації RADIUS та налаштувати SSH.

```
CE-3(config)#aaa new-model
CE-3(config)#aaa authentication login default group radius local
CE-3(config)#aaa authorization exec default group radius local
^
% Invalid input detected at '^' marker.

CE-3(config)#aaa authorization exec default group radius local
CE-3(config)#radius-server host 199.24.5.5 key Cisco123
Warning: The CLI will be deprecated soon
'radius-server host 199.24.5.5 key Cisco123'
Please move to 'radius server <name>' CLI.
CE-3(config)#line vty 0 4
CE-3(config-line)#login authentication default
CE-3(config-line)#transport input ssh
CE-3(config-line)#exit
CE-3(config)#ip domain-name radius.local
CE-3(config)#crypto key generate rsa modulus 1024
The name for the keys will be: CE-3.radius.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

CE-3(config)#ip
*Jun 20 11:22:13.042: %SSH-5-ENABLED: SSH 1.99 has been enabled
CE-3(config)#ip ssh version 2
CE-3(config)#username localuser privilege 15 secret localpassword
CE-3(config)#
```

Рисунок 3.27 – Налаштування маршрутизатора CE-3 як клієнта RADIUS

```
SW-A-SITE3-1#ssh -l admin1 199.24.5.1
Password:
CE-3>
```

Рисунок 3.28 – Підключення до маршрутизатора CE-3 з комутатора SW-A-SITE3-

1

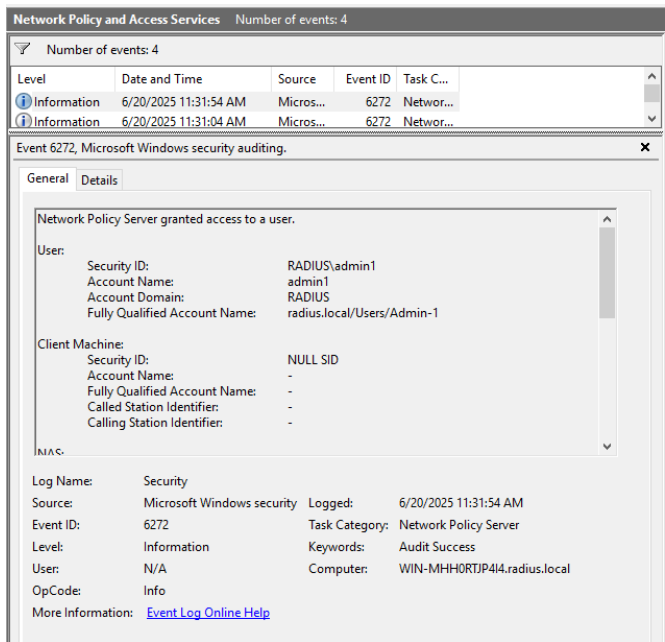


Рисунок 3.29 – Повідомлення про успішне надання доступу на сервері RADIUS

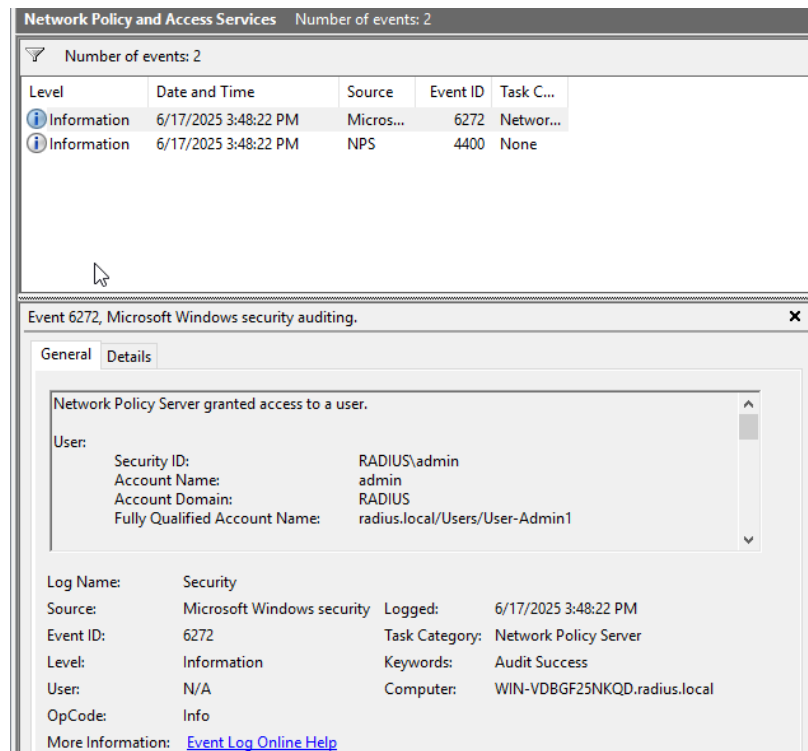


Рисунок 3.30 – Повідомлення про успішне надання доступу на сервері RADIUS

Серверний сертифікат – це цифровий документ, який зазвичай використовується для аутентифікації та захисту інформації в відкритих мережах. Сертифікат надійно пов’язує публічний ключ із суб’єктом, який володіє відповідним приватним ключем. Сертифікати цифрово підписуються органом сертифікації (CA) і можуть видаватися для користувача, комп’ютера або сервісу.

Орган сертифікації (CA) – це структура, відповідальна за встановлення та підтвердження аутентичності публічних ключів, що належать суб’єктам (зазвичай користувачам або комп’ютерам) або іншим органам сертифікації. Діяльність органу сертифікації може включати пов’язання публічних ключів з унікальними іменами за допомогою підписаних сертифікатів, керування серійними номерами сертифікатів та відкликання сертифікатів.

Служби сертифікації Active Directory (AD CS) – це роль сервера, що видає сертифікати як мережевий орган сертифікації. Інфраструктура сертифікації AD CS, також відома як інфраструктура публічних ключів (PKI), надає налаштовані сервіси для видачі та керування сертифікатами в підприємстві.

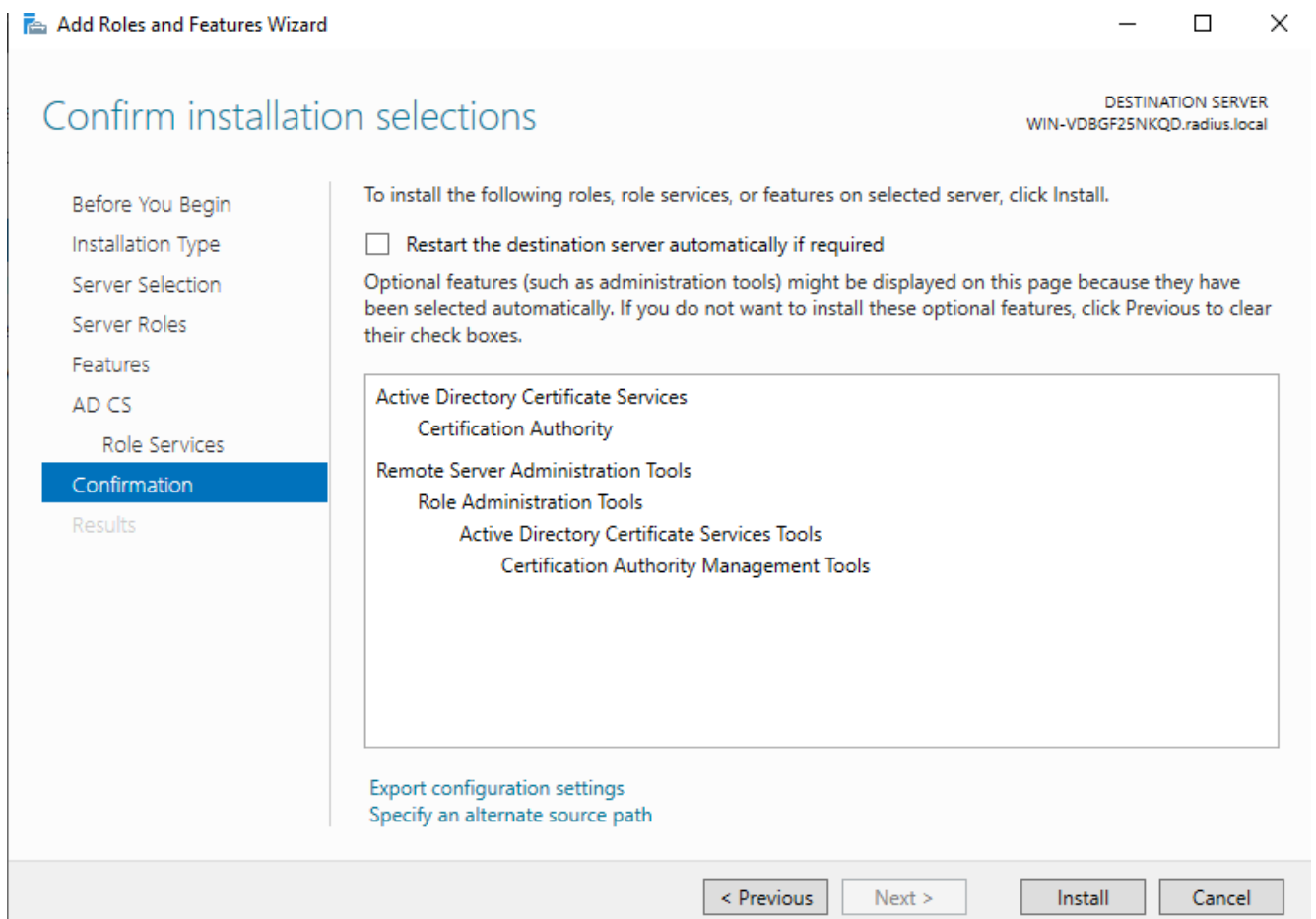


Рисунок 3.31 – Встановлення Active Directory Certificate Services для створення сертифікатів

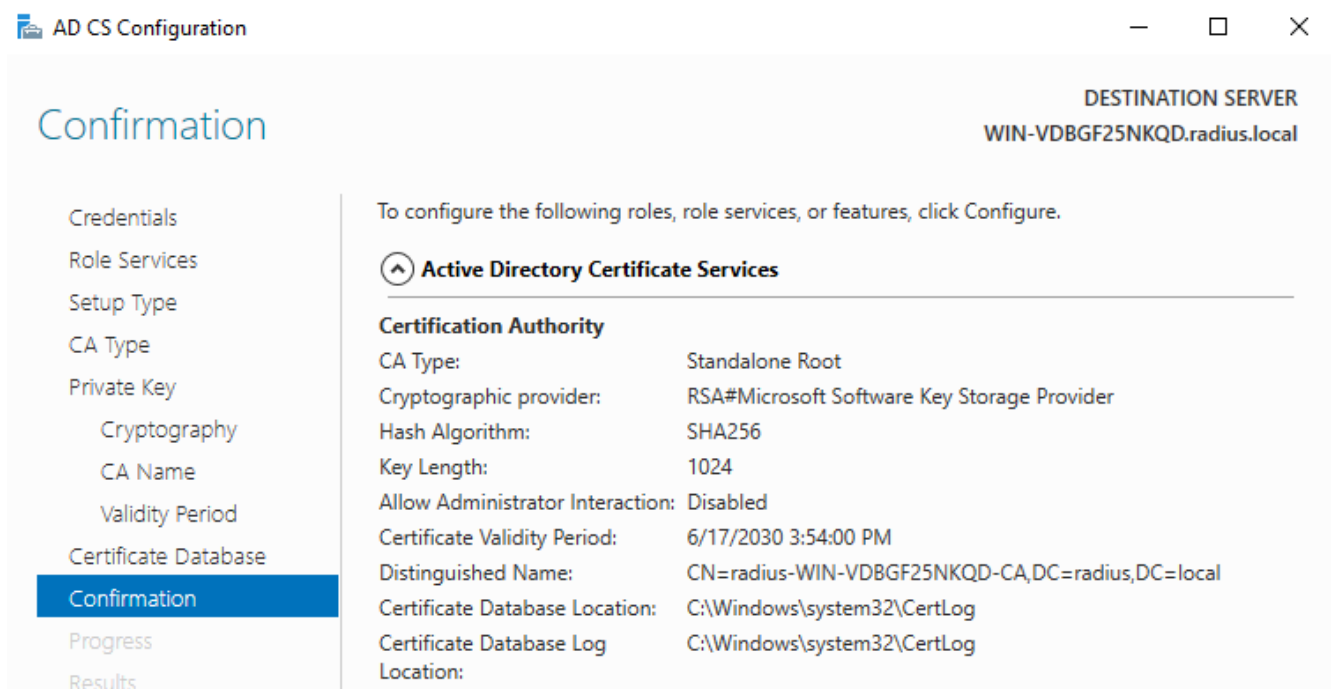


Рисунок 3.32 – Встановлення Active Directory Certificate Services для створення сертифікатів

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

New Object - User

Create in: radius.local/Users

First name: userWindows10 Initials:

Last name:

Full name: userWindows10

User logon name: user1 @radius.local

User logon name (pre-Windows 2000): RADIUS\ user1

< Back Next > Cancel

Рисунок 3.33 – Створення нового користувача для робочої станції Windows10

New RADIUS Client

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name: SW-A-SITE3-1

Address (IP or DNS): 199.24.5.2 Verify...

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual ☐ Generate

Shared secret:

Confirm shared secret:

OK Cancel

Рисунок 3.34 – Додавання комутатора SW-A-SITE3-1 як клієнта RADIUS

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-A-SITE3-1(config)#aaa new-model
SW-A-SITE3-1(config)#aaa authentication dot1x default group radius
SW-A-SITE3-1(config)#aaa authorization network default group radius
SW-A-SITE3-1(config)#aaa authentication login default group radius local
SW-A-SITE3-1(config)#radius-server host 199.24.5.5 key Cisc0123
Warning: The CLI will be deprecated soon
'radius-server host 199.24.5.5 key Cisc0123'
Please move to 'radius server <name>' CLI.
SW-A-SITE3-1(config)#int eth0/1
SW-A-SITE3-1(config-if)#switchport mode access
SW-A-SITE3-1(config-if)#authentication port-control auto
SW-A-SITE3-1(config-if)#dot1x pae authenticator
SW-A-SITE3-1(config-if)#

```

Рисунок 3.35 – Налаштування комутатора SW-A-SITE-3-1 як клієнта RADIUS та налаштування функціонування 802.1X

New Network Policy

×



Completing New Network Policy

You have successfully created the following network policy:

802.1X

Policy conditions:

Condition	Value
NAS Port Type	Ethernet

Policy settings:

Condition	Value
Authentication Method	EAP
Access Permission	Grant Access
Service-Type	Framed
Ignore User Dial-In Properties	False
Extensible Authentication Protocol Method	Microsoft: Smart Card or other certificate OR Microsoft: Protected EAP (PEAP)
Extensible Authentication Protocol Configuration	Configured

To close this wizard, click Finish.

Previous

Next

Finish

Cancel

Рисунок 3.36 – Створення нової політики для 802.1X та налаштування методів аутентифікації

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

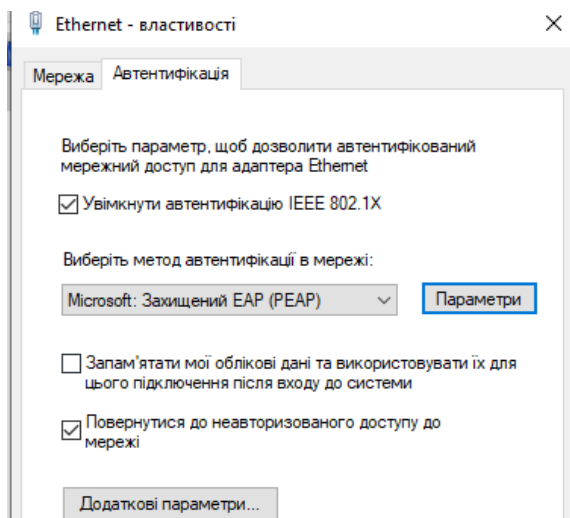


Рисунок 3.37 – Налаштування Аутентифікації за допомогою 802.1X

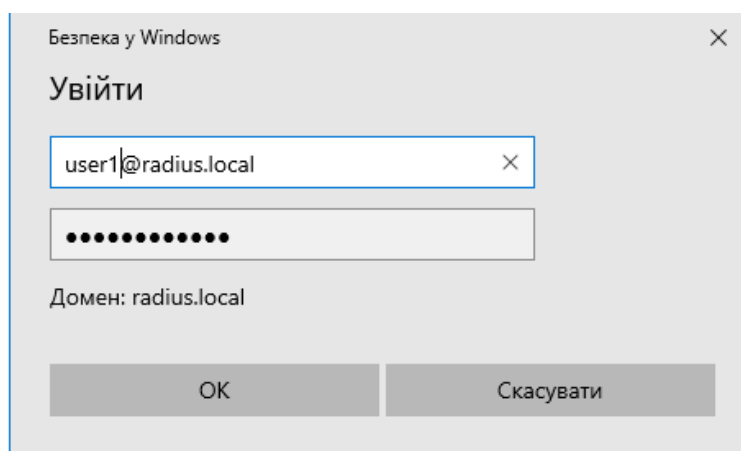


Рисунок 3.38 – Вхід під користувачем user1 на робочій станції Windows 10

```
C:\Users\Student>ping 199.24.5.5

Pinging 199.24.5.5 with 32 bytes of data:
Reply from 199.24.5.5: bytes=32 time=1ms TTL=128
Reply from 199.24.5.5: bytes=32 time<1ms TTL=128
Reply from 199.24.5.5: bytes=32 time<1ms TTL=128
Reply from 199.24.5.5: bytes=32 time<1ms TTL=128

Ping statistics for 199.24.5.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Student>ping 190.24.5.3

Pinging 190.24.5.3 with 32 bytes of data:
Reply from 190.24.5.3: bytes=32 time=3119ms TTL=58
Reply from 190.24.5.3: bytes=32 time=112ms TTL=58
Reply from 190.24.5.3: bytes=32 time=111ms TTL=58
Reply from 190.24.5.3: bytes=32 time=108ms TTL=58

Ping statistics for 190.24.5.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 108ms, Maximum = 3119ms, Average = 862ms

C:\Users\Student>
```

Рисунок 3.39 – Перевірка зв'язку після підключення за допомогою 802.1X

```

CE-3(config)#ip access-list extended INBOUND
CE-3(config-ext-nacl)#permit icmp any 199.24.5.0 0.0.0.31 echo-reply
CE-3(config-ext-nacl)#deny icmp any any
CE-3(config-ext-nacl)#permit ip any any
CE-3(config-ext-nacl)#exit
CE-3(config)#int fa0/0
CE-3(config-if)#ip access-group INBOUND in
CE-3(config-if)#

```

Рисунок 3.40 – Налаштування списку доступу, де пінги з сайта 3 будуть проходити та повертатися, а пінги з сайтів 1 та 2 будуть відкидатися

```

C:\Users\Student>ping 190.24.5.3

Pinging 190.24.5.3 with 32 bytes of data:
Reply from 190.24.5.3: bytes=32 time=3125ms TTL=58
Reply from 190.24.5.3: bytes=32 time=124ms TTL=58
Reply from 190.24.5.3: bytes=32 time=126ms TTL=58
Reply from 190.24.5.3: bytes=32 time=124ms TTL=58

Ping statistics for 190.24.5.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 124ms, Maximum = 3125ms, Average = 874ms

C:\Users\Student>_

```

Рисунок 3.41 – Перевірка зв'язку з робочої станції на сайті 3 з робочою станцією на сайті 1

```

WS-A1-2> ping 199.24.5.6
*200.24.5.34 icmp_seq=1 ttl=250 time=118.127 ms (ICMP type:3, code:13, Communication administratively prohibited)
*200.24.5.34 icmp_seq=2 ttl=250 time=106.976 ms (ICMP type:3, code:13, Communication administratively prohibited)
*200.24.5.34 icmp_seq=3 ttl=250 time=107.553 ms (ICMP type:3, code:13, Communication administratively prohibited)
*200.24.5.34 icmp_seq=4 ttl=250 time=107.819 ms (ICMP type:3, code:13, Communication administratively prohibited)
*200.24.5.34 icmp_seq=5 ttl=250 time=114.247 ms (ICMP type:3, code:13, Communication administratively prohibited)
WS-A1-2>

```

Рисунок 3.42 – Спроба перевірки зв'язку з робочої станції на сайті 1 з робочою станцією на сайті 3

Висновки до третього розділу

У даному розділі було реалізовано побудову, налагодження та тестування спроектованої корпоративної мережі, яка базується на технології MPLS L3VPN і використовує централізовану систему контролю доступу з підтримкою протоколу AAA та RADIUS-сервера, також було налаштовано та протестовано роботу протоколу 802.1X та налаштовано списки доступу.

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

ВИСНОВКИ

В першому розділі ми дослідили реалізацію контролю доступу за допомогою протоколу керування доступом до мережі на основі портів 802.1X та протоколу RADIUS у ІКМ. Для реалізації контролю доступу було обрано саме RADIUS зважаючи на його переваги, а саме його підтримку 802.1X та його сумісність з пристроями різних виробників. Було розглянуто функціонування VPN, класифікацію відповідно до застосування VPN та класифікацією на основі режиму роботи VPN. Обрано MPLS VPN зважаючи на переваги та досліджено функціонування MPLS та MPLS VPN.

У другому розділі ми розробили проект мережі, розглянули рівень ядра, рівень розподілу та рівень доступу у розробленій мережі. Було виконано розподіл IP-адрес між підмережами. Було розроблено підсистему контролю доступу до мережі.

У третьому розділі було реалізовано побудову, налагодження та тестування спроектованої корпоративної мережі, яка базується на технології MPLS L3VPN і використовує централізовану систему контролю доступу з підтримкою протоколу AAA та RADIUS-сервера, також було налаштовано та протестовано роботу протоколу 802.1X та налаштовано списки доступу.

Під час написання кваліфікаційної роботи було створено ІКМ з застосування MPLS VPN у поєднанні з технологіями контролю доступу, що дало змогу побудувати ефективну та захищену мережу. Отже, поставлена мета кваліфікаційної роботи досягнута, а розроблена мережна інфраструктура може бути використана як основа для впровадження реального рішення із високим рівнем захищеності.

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Таненбаум Е., Везеролл Д. Комп'ютерні мережі. – 5-е вид., Київ: Діалектика, 2014. – 960 с.
2. Donahue G. A. Network Warrior. – 2nd ed., Sebastopol: O'Reilly Media, 2011. – 788 p.
3. Davie B., Rekhter Y. MPLS: Technology and Applications. San Francisco: Morgan Kaufmann, 2000. 496 p.
4. Stewart J. M., Kinsey D. Network Security, Firewalls, and VPNs. 3rd ed. Burlington: Jones & Bartlett Learning, 2020. 400 p.
5. Blokdyk G. VPN A Complete Guide - 2023 Edition. [S.l.]: The Art of Service, 2023. 284 p.
6. Configure IP Addresses and Unique Subnets for New Users [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>
7. What Is a VPN? How Does a VPN Work? [Електронний ресурс] – Режим доступу: <https://info.support.huawei.com/info-finder/encyclopedia/en/VPN.html>
8. Multiprotocol BGP MPLS VPN [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_l3_vpns/configuration/15-s/mp-l3-vpns-15-s-book/mp-bgp-mpls-vpn.pdf
9. What Is MPLS? How Does MPLS Work? [Електронний ресурс] – Режим доступу: <https://info.support.huawei.com/info-finder/encyclopedia/en/MPLS.html>
10. What Is Network Access Control (NAC)? [Електронний ресурс] – Режим доступу: <https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-access-control-nac.html>
11. Network Access Control Meaning [Електронний ресурс] – Режим доступу: <https://www.fortinet.com/resources/cyberglossary/what-is-network-access-control>
12. What Is Bring Your Own Device (BYOD)? [Електронний ресурс] – Режим доступу: <https://www.fortinet.com/resources/cyberglossary/byod>

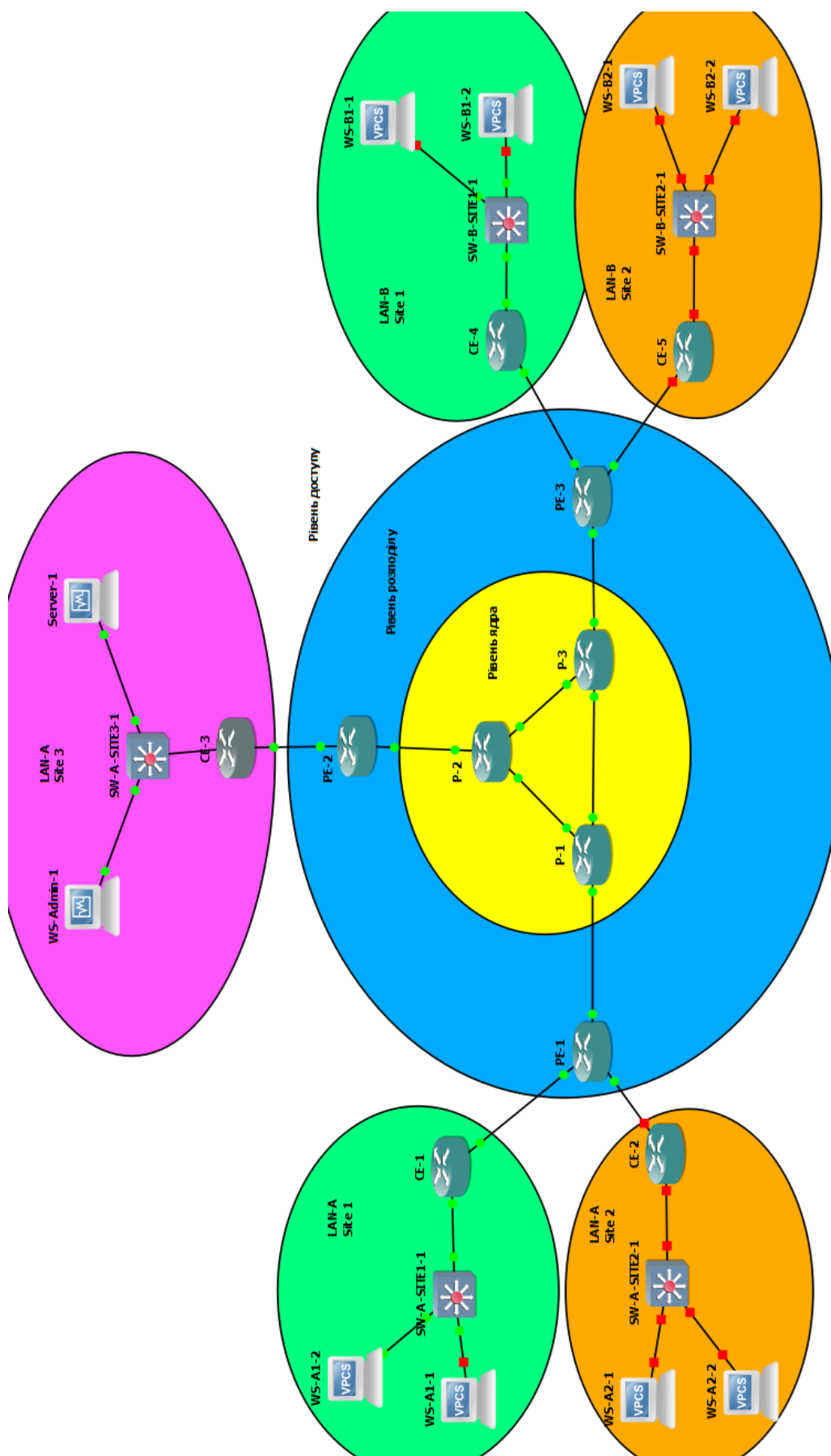
		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

13. Virtual Local Area Networks (VLANs) [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/vlans.pdf
14. What is 802.1X? How Does it Work? [Електронний ресурс] – Режим доступу: <https://www.securew2.com/solutions/802-1x>
15. What is 802.1X? [Електронний ресурс] – Режим доступу: <https://info.support.huawei.com/info-finder/encyclopedia/en/802.1X.html>
16. Understanding and Configuring 802.1X Port-Based Authentication [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dot1x.pdf>
17. Examine how the RADIUS Works [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html>
18. What Is RADIUS? How Does RADIUS Work? [Електронний ресурс] – Режим доступу: <https://info.support.huawei.com/info-finder/encyclopedia/en/RADIUS.html>
19. What Is TACACS? [Електронний ресурс] – Режим доступу: <https://community.fs.com/encyclopedia/tacacs.html>

ДОДАТКИ

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Побудований проект мережі



		Давидюк Д.С.		
		Воротніков В.В.		
Змн.	Арк.	№ докум.	Підпис	Дата


```

line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1

```

```

line vty 0 4
login
!
!
end

```

Конфігураційний файл маршрутизатора P-2

```

Current configuration : 1207 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname P-2
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
mpls label protocol ldp
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
!

```

```

!
!
!
!
interface Loopback1
ip address 3.3.3.2 255.255.255.255
!
interface FastEthernet0/0
ip address 200.24.5.9 255.255.255.252
duplex full
mpls ip
!
interface FastEthernet1/0
ip address 200.24.5.2 255.255.255.252
speed auto
duplex auto
mpls ip
!
interface FastEthernet1/1
ip address 200.24.5.17 255.255.255.252
speed auto
duplex auto
mpls ip
!
router ospf 1
network 3.3.3.2 0.0.0.0 area 0
network 200.24.5.0 0.0.0.3 area 0
network 200.24.5.8 0.0.0.3 area 0
network 200.24.5.16 0.0.0.3 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback1 force
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15

```

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

```

logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous

```

```

stopbits 1
line vty 0 4
login
!
!
end

```

Конфігураційний файл маршрутизатора P-3

```

Current configuration : 1208 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname P-3
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
mpls label protocol ldp
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!

```

```

!
!
!
!
interface Loopback1
ip address 3.3.3.3 255.255.255.255
!
interface FastEthernet0/0
ip address 200.24.5.10 255.255.255.252
duplex full
mpls ip
!
interface FastEthernet1/0
ip address 200.24.5.21 255.255.255.252
speed auto
duplex auto
mpls ip
!
interface FastEthernet1/1
ip address 200.24.5.6 255.255.255.252
speed auto
duplex auto
mpls ip
!
router ospf 1
network 3.3.3.3 0.0.0.0 area 0
network 200.24.5.4 0.0.0.3 area 0
network 200.24.5.8 0.0.0.3 area 0
network 200.24.5.20 0.0.0.3 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
mpls ldp router-id Loopback1 force
!
!
control-plane
!
!
line con 0

```

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```
logging synchronous
stopbits 1
line vty 0 4
login
!
!
end
```

```
no ipv6 cef
```

```
!
!  
mpls label protocol ldp  
multilink bundle-name authenticated
```

!!!

!

!!!

!!!

```
!
ip tcp synwait-time 5
```

!!!

!!!

```
!
interface Loopback1
 ip address 2.2.2.1 255.255.255.255
```

```
!
interface FastEthernet0/0
ip address 200.24.5.14 255.255.255.252
duplex full
mpls ip
```

```
!
interface FastEthernet1/0
 vrf forwarding S1
 ip address 200.24.5.25 255.255.255.252
 speed auto
 duplex auto
```

```
!
interface FastEthernet1/1
 vrf forwarding S2
 ip address 200.24.5.29 255.255.255.252
```

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

```

speed auto
duplex auto
!
router ospf 1
network 2.2.2.1 0.0.0.0 area 0
network 200.24.5.12 0.0.0.3 area 0
network 200.24.5.24 0.0.0.3 area 0
network 200.24.5.28 0.0.0.3 area 0
!
router bgp 100
bgp log-neighbor-changes
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 update-source Loopback1
neighbor 2.2.2.3 remote-as 100
neighbor 2.2.2.3 update-source Loopback1
!
address-family vpnv4
neighbor 2.2.2.2 activate
neighbor 2.2.2.2 send-community extended
neighbor 2.2.2.3 activate
neighbor 2.2.2.3 send-community extended
exit-address-family
!
address-family ipv4 vrf S1
redistribute connected
neighbor 200.24.5.26 remote-as 110
neighbor 200.24.5.26 activate
exit-address-family
!
address-family ipv4 vrf S2
redistribute connected
neighbor 200.24.5.30 remote-as 120
neighbor 200.24.5.30 activate

```

```

exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip access-list extended inbound
!
!
mpls ldp router-id Loopback1 force
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
!
end

```

Конфігураційний файл маршрутизатора PE-2

```

Current configuration : 1897 bytes
!
! Last configuration change at 19:38:44 UTC
Fri Jun 20 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname PE-2
!
boot-start-marker
boot-end-marker
!
!
vrf definition S3
rd 300:1
route-target export 300:1

```

```

route-target import 300:1
route-target import 200:1
route-target import 100:1
!
address-family ipv4
exit-address-family
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
!
!
no ip domain lookup
ip cef

```

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ipv6 cef
!
!
mpls label protocol ldp
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
!
!
!
!
interface Loopback1
 ip address 2.2.2.2 255.255.255.255
!
interface FastEthernet0/0
 ip address 200.24.5.18 255.255.255.252
 duplex full
 mpls ip
!
interface FastEthernet1/0
 vrf forwarding S3
 ip address 200.24.5.33 255.255.255.252
 speed auto
 duplex auto
!
interface FastEthernet1/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
router ospf 1
 network 2.2.2.2 0.0.0.0 area 0
 network 200.24.5.16 0.0.0.3 area 0

```

```

network 200.24.5.32 0.0.0.3 area 0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 2.2.2.1 remote-as 100
 neighbor 2.2.2.1 update-source Loopback1
 neighbor 2.2.2.3 remote-as 100
 neighbor 2.2.2.3 update-source Loopback1
!
 address-family vpnv4
  neighbor 2.2.2.1 activate
  neighbor 2.2.2.1 send-community extended
  neighbor 2.2.2.3 activate
  neighbor 2.2.2.3 send-community extended
 exit-address-family
!
 address-family ipv4 vrf S3
  redistribute connected
  neighbor 200.24.5.34 remote-as 130
  neighbor 200.24.5.34 activate
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end

```

Конфігураційний файл маршрутизатора CE-1

Current configuration : 1224 bytes

!

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

```

version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname CE-1
!
boot-start-marker
boot-end-marker
!
!
!
multilink bundle-name authenticated
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
Biφ
!
!
!
router bgp 110
bgp log-neighbor-changes
neighbor 200.24.5.25 remote-as 100
!
address-family ipv4
network 1.1.1.1 mask 255.255.255.255
redistribute connected
neighbor 200.24.5.25 activate
exit-address-family
!
ip forward-protocol nd
!
!
!
no ip http server
no ip http secure-server
interface Loopback1
ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
ip address 200.24.5.26 255.255.255.252
duplex full
!
interface FastEthernet1/0
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
interface FastEthernet1/1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
!
line vty 0 4
login
router ospf 1
network 200.24.5.24 0.0.0.3 area 0

```

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

<pre> ! Current configuration : 1226 bytes ! version 15.2 service timestamps debug datetime msec service timestamps log datetime msec ! hostname CE-2 ! boot-start-marker boot-end-marker ! ! ! no aaa new-model no ip icmp rate-limit unreachable ! ! ! ! ! no ip domain lookup ip cef no ipv6 cef ! ! multilink bundle-name authenticated ! ! ! ! ! ! ! ! ! ip tcp synwait-time 5 ! ! ! ! ! ! ! ! ! interface Loopback1 </pre>	<pre> end ip address 1.1.1.2 255.255.255.255 ! interface FastEthernet0/0 ip address 200.24.5.30 255.255.255.252 duplex full ! interface FastEthernet1/0 ip address 190.24.6.1 255.255.255.192 speed auto duplex auto ! interface FastEthernet1/1 no ip address shutdown speed auto duplex auto ! router ospf 1 network 200.24.5.28 0.0.0.3 area 0 ! router bgp 120 bgp log-neighbor-changes neighbor 200.24.5.29 remote-as 100 ! address-family ipv4 network 1.1.1.2 mask 255.255.255.255 redistribute connected neighbor 200.24.5.29 activate exit-address-family ! ip forward-protocol nd ! ! no ip http server no ip http secure-server ! ! ! ! control-plane ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous stopbits 1 line aux 0 exec-timeout 0 0 privilege level 15 </pre>
--	--

```

!
!
end

рутизатора CE-3
!
!
!
username localuser privilege 15 secret 5
$1$ghNf$7OuKR18QBqDpX6oIXwb.

```

```
!
!  
!  
!  
!  
!  
ip tcp synwait-time 5  
ip ssh version 2
```

```

!
!
!
!
!
!
!
!
!
interface Loopback1
 ip address 1.1.1.3 255.255.255.255
!
interface FastEthernet0/0
 ip address 200.24.5.34 255.255.255.252
 ip access-group INBOUND in
 duplex full
!
interface FastEthernet1/0
 ip address 199.24.5.1 255.255.255.224
 speed auto
 duplex auto
!
interface FastEthernet1/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
router ospf 1
 network 200.24.5.32 0.0.0.3 area 0
!
router bgp 130
 bgp log-neighbor-changes
 neighbor 200.24.5.33 remote-as 100
!

```

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

```

address-family ipv4
  network 1.1.1.3 mask 255.255.255.255
  redistribute connected
  neighbor 200.24.5.33 activate
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip access-list extended INBOUND
  permit icmp any 199.24.5.0 0.0.0.31 echo-reply
  deny icmp any any
  permit ip any any
!
!
!
!
end

```

```
radius-server host 199.24.5.5 key Cisco123
```

Конфігураційний файл маршрутизатора CE-4

```

Current configuration : 1226 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname CE-4
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
!

```

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface FastEthernet1/1
no ip address
shutdown
speed auto
duplex auto
!
router ospf 1
network 200.24.5.36 0.0.0.3 area 0
!
router bgp 140
bgp log-neighbor-changes
neighbor 200.24.5.37 remote-as 100
!
address-family ipv4
network 1.1.1.4 mask 255.255.255.255
redistribute connected
neighbor 200.24.5.37 activate
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
!
end

```

Конфігураційний файл маршрутизатора CE-5

```

Current configuration : 1224 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname CE-5
!
boot-start-marker
boot-end-marker
!
!
!
ip tcp synwait-time 5
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated

```

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

```

duplex full
!
interface FastEthernet1/0
ip address 191.24.6.1 255.255.255.0
speed auto
duplex auto
!
interface FastEthernet1/1
no ip address
shutdown
speed auto
duplex auto
!
router ospf 1
network 200.24.5.40 0.0.0.3 area 0
!
router bgp 150
bgp log-neighbor-changes
neighbor 200.24.5.41 remote-as 100
!
address-family ipv4
network 1.1.1.5 mask 255.255.255.255
redistribute connected
neighbor 200.24.5.41 activate
exit-address-family
!
ip forward-protocol nd

```

```

!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
!
end

```

Конфігураційний файл комутатора SW-A-SITE3-1

```

Current configuration : 1902 bytes
!
! Last configuration change at 19:14:11 UTC
Fri Jun 20 2025 by admin1
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-A-SITE3-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username localuser privilege 15 secret 5
$1$1bfr$AniASOVgvcg6KE2eJMuz1

```

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

```
!
no ip domain-lookup
ip domain-name radius.local
ip cef
no ipv6 cef
!
!
dot1x system-auth-control
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
!
interface Ethernet0/1
 switchport mode access
 authentication port-control auto
 dot1x pae authenticator
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
```

```

interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 199.24.5.2 255.255.255.224
!
 ip forward-protocol nd
!
 no ip http server
 no ip http secure-server
!
!
!
!
!
!
 radius-server host 199.24.5.5 key Cisco123
!
!
 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
  transport input ssh
!
!
end

```

		Давидюк Д.С.			ККІКБ.КР.Б – 125 – 05 – ПЗ	Арк.
		Воротніков В.В.				79
Змн.	Арк.	№ докум.	Підпис	Дата		