

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 модернізації корпоративної

IPv4-мережі організації»

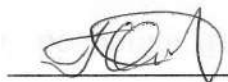
Виконав студент 4-го курсу групи КІ-4

спеціальності 123 «Комп'ютерна інженерія»



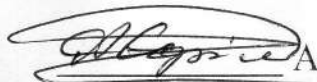
Акім Балан

Керівник доцент кафедри КІ та КБ, к.пед.н.,



Олена Головня

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



Андрій Єфіменко

Державний університет «Житомирська політехніка»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

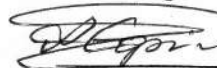
Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Балан Акім Олегович

Тема роботи: «Проект модернізації корпоративної IPv4-мережі організації»

затверджена Наказом університету від 1 березня 2022 р. № 127/с

Термін здачі студентом закінченої роботи 10 червня 2022 р.

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

Об'єктом дослідження є дослідження процесу розробки та налаштування комп'ютерної мережі; предметом дослідження є розробка та налаштування корпоративної комп'ютерної мережі на основі IPv6, EIGRPv6, DHCPv6 та VLAN.

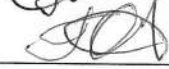
Обладнання та програмне забезпечення:

1. Virtual Box
2. Cisco Packet Tracer
3. Обладнання серії Cisco Catalyst

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Головня О.С.		
2	Головня О.С.		
3	Головня О.С.		

Студент  Акім Балан

Керівник  Олена Головня

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз літературних джерел	07.03.2022 р.	
2	Аналіз об'єкта дослідження	15.03.2022 р.	
3	Постановка задачі дослідження	22.03.2022 р.	
4	Розробка структурної моделі	29.03.2022 р.	
5	Розрахунок параметрів адресації	05.05.2022 р.	
6	Вибір технології для реалізації	12.05.2022 р.	
7	Розробка захищеної КМ	19.05.2022 р.	
8	Налаштування мережі	03.06.2022 р.	
9	Перевірка працездатності	11.06.2022 р.	
10	Оформлення пояснювальної записки	17.06.2022 р.	
11	Оформлення презентації	21.06.2022 р.	
	Захист	Згідно з розкладом	

Студент  Акім Балан

Керівник  Олена Головня

АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи на тему “Проект модернізації корпоративної IPv4-мережі організації” складається з вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Текстова частина викладена на 45 сторінках друкованого тексту.

Пояснювальна записка має 12 сторінок додатків. Список використаних джерел містить 19 найменувань і займає 2 сторінки. В роботі наведено 36 рисунків. Загальний обсяг роботи - 59 сторінок.

У першому розділі було визначено мету кваліфікаційної роботи - розробка проекту модернізації корпоративної IPv4 мережі організації. Визначено теоретичні основи побудови та адміністрування корпоративних комп'ютерних мереж на базі IPv6. Обґрунтовано вибір засобів та технологій для корпоративної комп'ютерної мережі.

У другому розділі виконано проектування топології комп'ютерної мережі та розроблено схему адресації.

У третьому розділі обґрунтовано вибір мережевого обладнання. Встановлено та налаштовано мережеве обладнання, організовано моніторинг роботи системи, а також оптимізовано функціонування спроектованої мережі. Організовано систему захисту даних (ACL), реалізована система розмежування прав доступу (VLAN), налаштований віддалений доступ. Реалізована динамічна система адресації (DHCP), агрегація каналів, маршрутизація. Перевірено роботу усієї мережі у звичайному та стресовому режимах.

Висновки містять результати виконаної роботи, а саме результат проектування вдосконаленої корпоративної IPv4 мережі. У додатку представлені налаштування обладнання для адміністрування мережі, а також топологія спроектованої мережі.

Ключові слова: VLAN, PVST+, PAGP, DHCPV6, IPV6, NAT, IPV4, ACL, SLAAC, SWITCH, CISCO, ROUTER, CATALYST, NDP, FASTETHERNET.

					KIK.KP.B – 123 – 03 – ПЗ				
Вик.	Арк.	№ докум.	Підпис	Дата	Проект модернізації корпоративної IPv4-мережі організації	Літ.	Арк.	Аркушів	
Розроб.		Балан А.О.		20.06					
Модерніз.		Головня О.С.		20.06			4	59	
Реценз.		Сфіменко А.А.		20.06		ФІКТ, Гр. КІ-4			
Ін. контр.		Головня О.С.		20.06					
Затверд.		Сфіменко А.А.		20.06					

ANNOTATION

The explanatory note to the qualification work on the topic "Project of modernization of the corporate IPv4-network of the organization" consists of an introduction, three sections, conclusions, list of references, and appendices.

The text is set out on 45 pages of printed text. The explanatory note has 12 pages of appendices. The list of references contains 19 names and occupies 2 pages. The paper presents 36 figures. The total volume of work is 59 pages.

The first section identified the purpose of the qualification work - the development of a project to modernize the corporate IPv4 network of the organization. Theoretical bases of construction and administration of corporate computer networks on the basis of IPv6 are defined. The choice of tools and technologies for the corporate computer network is justified.

In the second section, the design of the computer network topology is performed and the addressing scheme is developed.

The third section substantiates the choice of network equipment. We managed to install and configure network equipment, organize monitoring of the system, as well as optimize the operation of the designed network. The data protection system (ACL) has been organized, the system of delimitation of access rights (VLAN) has been implemented, remote access has been configured. Dynamic addressing system (DHCP), channel aggregation, routing had been implemented. The operation of the entire network in normal and stress modes was tested.

The conclusions include the results of the work done, namely the result of developed an advanced corporate IPv4 network.

The appendix presents the settings of the equipment for network administration, as well as the topology of the designed network.

Keywords: VLAN, PVST+, PAGP, DHCPV6, IPV6, NAT, IPV4, ACL, SLAAC, SWITCH, CISCO, ROUTER, CATALYST, NDP, FASTETHERNET.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ НА IPv6	10
1.1 Технологія VLAN	10
1.2 Технологія NAT	11
1.3 Технологія PVST+	12
1.4 Протокол PAgP	13
1.5 SLAAC	13
1.6 Протокол DHCPv6	14
1.7 Списки контролю доступу	15
1.8 Агрегація каналів	17
1.9 EIGRPv6	19
1.10 Протоколи IPv4 та IPv6	20
РОЗДІЛ 2 ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СХЕМИ АДРЕСАЦІЇ	22
2.1 Розробка топології комп'ютерної мережі	22
2.2 Розробка схеми адресації мережі	27
РОЗДІЛ 3 ВИБІР ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ	30
3.1 Вибір обладнання для організації роботи мережі	30
3.2 Налаштування обладнання мережі	33
ВИСНОВКИ	43
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	45
ДОДАТКИ	48

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КМ - комп'ютерні мережі

FE - Fast Ethernet

GbE - Gigabit Ethernet

STP - Spanning Tree Protocol

VLAN – Virtual local area network – Віртуальна локальна мережа

RID – Router Identifier – Ідентифікатор маршрутизатора

SW – Switch – Комутатор

DHCP – Dynamic Host Configuration Protocol – Протокол динамічного налаштування вузла

ACL – Список контролю доступу – Список управління доступом

VPN – Virtual private network – Приватна захищена мережа

NAT – Network Address Translation – перетворення мережеских адрес

SLAAC – Stateless Address Autoconfiguration – Автоналаштування адреси без стану

NDP – Neighbor Discovery Protocol – Протокол пошуку сусідів

RAgP – Протокол агрегації портів

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність обраної теми обумовлена необхідністю створення нових мереж та супроводу наявних. На сьогодні більшість компаній, що мають комп'ютерне устаткування, потребують доступу до інтернету. Індивідуальний підхід до кожного пристрою не є раціональним способом витрачання коштів, тому створення спільної мережі, яка задовольняла би ці потреби є гарним рішенням. Проблемою може стати застарілість такої мережі, якщо реалізовані протоколи не є актуальними. Їх оновлення дає змогу підвищити життєспроможність та надійність мережі. Завдяки такому підходу, масштабування та менеджмент значно полегшуються, що дозволяє вкладати ресурси компанії ефективно. До того ж, якість створеної мережі в плані захисту даних та надійності роботи не створить проблем. Враховуючи усе вищесказане, навички адміністрування комп'ютерних мереж є важливими для майбутнього спеціаліста, а самі такі кадри є цінними на ринку праці. Отже, обрана тема проекту є актуальною.

Метою кваліфікаційної роботи є розробка проекту модернізації корпоративної IPv4 мережі організації.

Завданням на кваліфікаційну роботу є:

1. Аналіз теоретичних засад та ринку обладнання для адміністрування комп'ютерної мережі;
2. Проектування топології корпоративної мережі;
3. Підбір та налаштування відповідного обладнання;
4. Перевірка відповідності мережі вимогам замовника;
5. Тестування працездатності мережі та перевірка на стресостійкість.

Об'єктом дослідження є процес розробки та налаштування комп'ютерної мережі.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Предметом є розробка та налаштування корпоративної комп'ютерної мережі на основі IPv6, EIGRPv6, DHCPv6 та VLAN.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ НА БАЗІ IPv6

1.1 Технологія VLAN

Коли йдеться про локальні мережі, ми частіше всього маємо на увазі деякий набір пристроїв, що під'єднанні до одного маршрутизатора та мають спільну “білу” адресу. Але на сьогоднішній день технології проектування комп’ютерних мереж надають нам можливість логічно (частіше за все програмно) розділити одну мережу на декілька.

Подібна практика активно використовується на підприємствах як складова політики безпеки та ефективного адміністрування. На рисунку 1.1 Можливо наочно побачити принцип логічного розмежування мереж. Таким чином, VLAN1 може відповідати за одну внутрішню ділянку обладнання компанії, зі своїми налаштування безпеки (наприклад, внутрішня мережа із необхідністю ідентифікації по ID), а VLAN2 за публічні машини робітників у яких не буде доступу до внутрішніх або зовнішніх ресурсів.

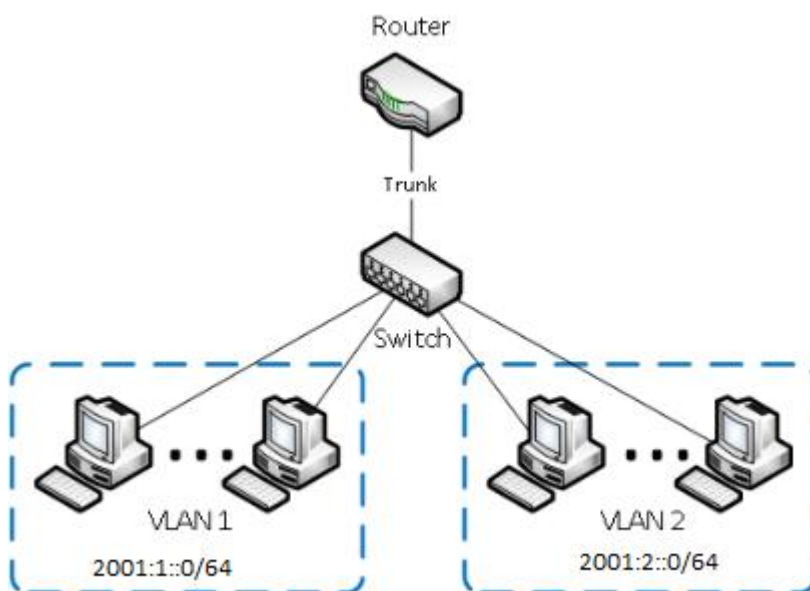


Рисунок 1.1 - Схема приклад VLAN

VLAN якісно відрізняються від їх фізичних аналогів тим, що не потребують додаткового обладнання для впровадження. Подібна технологія, завдяки своїй доступності, дозволяє покращити загальний рівень мережевої грамотності та являє собою сучасний стандарт організації мереж.

Як наслідок, під час проектування майбутньої мережі буде необхідно виділити всередині неї логічні блоки підмереж за допомогою VLAN. Подібне розмежування, крім фактичного розділення також буде однією із складових політик безпеки^[18].

1.2 Технологія NAT

Вільне використання IPv4 обмежується “білими” адресами. Їх кількість обмежена та вже розподілена. Для Реалізації можливості доступу до мережі усім пристроям було реалізовано технологію перекладу адрес. Суть технології у тому, що одній "білій", або публічній, адресі може відповідати декілька "сірих", або приватних, адрес.

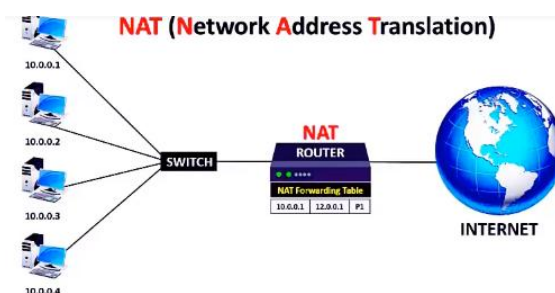


Рисунок 1.2 - Схема роботи NAT

NAT означає трансляцію мережевих адрес. Це спосіб зіставити кілька локальних приватних адрес із загальнодоступними перед передачею інформації. Організації, які хочуть, щоб кілька пристроїв використовували одну IP-адресу, використовують NAT, як і більшість домашніх маршрутизаторів^[16].

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

Дана технологія дозволяє зменшити потребу в унікальних IP-адресах, та допомагає провайдеру або компанії з менеджментом власної мережі. Більшості користувачів надається “сіра” адреса, яка за необхідності транслюється та спілкується з глобальною мережею. NAT буває декількох типів: статичний та динамічний. Статичний NAT створює таблицю відповідності адрес, що дозволяє отримати фіксовану публічну адресу, а динамічний формує список адрес, та видає їх за необхідністю (принцип видачі - first-in-first-out). Крім того можливо за необхідністю присвоїти великій кількості “сірих” адрес 1 публічну, що дозволяє ще більше оптимізувати видачу адрес.

1.3 Технологія PVST+

Rapid per VLAN Spanning Tree (Rapid PVST+) — це оновлена реалізація STP, яка дозволяє створити одну топологію опорного дерева для кожної VLAN. Rapid PVST+ — це режим протоколу Spanning Tree Protocol (STP) за замовчуванням на комутаторі^[14].

Протокол Rapid PVST+ — це стандарт IEEE 802.1w, протокол швидкого зв’язного дерева (RSTP), реалізований на основі кожної VLAN. Rapid PVST+ взаємодіє зі стандартом IEEE 802.1D, який передбачає використання одного екземпляра STP для всіх VLAN, а не для кожної VLAN. Швидкий PVST+ увімкнено за замовчуванням у всіх мережах на основі VLAN (обладнання CISCO).

Коли йде створення відмовостійких мереж, необхідно мати шлях без петель між усіма вузлами мережі. Алгоритм STP обчислює найкращий шлях без петель у комутованій мережі. Порти LAN через регулярні проміжки часу надсилають та отримують кадри STP, які називаються одиницями даних протоколу мосту (BPDU - Bridge Protocol Data Unit, одиниця даних протоколу управління мережевими мостами). Перемикачі не пересилають ці кадри, а використовують кадри для побудови шляху без петель.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

1.4 Протокол PAgP

Протокол агрегації портів (PAgP) — це власний мережевий протокол Cisco Systems, який використовується для автоматизованого логічного об'єднання портів комутатора Ethernet, відомого як EtherChannel. PAgP є власністю Cisco Systems.

Більшість комутаторів Cisco використовують хеш MAC-адреси src/dst як метод розподілу, що означає, що один сеанс використовуватиме пропускну здатність одного інтерфейсу. Інші комутатори Cisco використовують власний метод розповсюдження, що дозволяє максимальній швидкості каналу бути такою ж, як сумарна швидкість інтерфейсів, що складають групу агрегації^[15].

На жаль, жоден логічний потік не може перевищувати швидкість фізичного порту. Однак деякі комутатори з підтримкою PAgP можуть узгоджувати при зв'язку «максимальне балансування навантаження» та «збереження порядку»: перше забезпечує максимальну сукупну пропускну здатність за рахунок упорядкування пакетів, тимчасом як останнє забезпечує відсутність переупорядкування пакетів, але обмежує одну передачу до пропускну здатності одного інтерфейсу.

1.5 SLAAC

Автоналаштування адреси без стану (з англ. Stateless Address Autoconfiguration) — це частина стандарту IPv6, призначена для того, щоб дозволити хостам самостійно налаштовувати себе ("авто" означає "самостійне"; отже, "самостійне налаштування") в мережі IPv6. Він був розроблений як простіший і зрозуміліший підхід до автоматичної адресації IPv6. У своїй поточній реалізації, як визначено в RFC 4862, SLAAC не надає хостам адреси DNS-серверів, і тому на даний момент він не є широко розповсюдженим^[3].

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Це механізм, який дозволяє кожному хосту в мережі автоматично налаштовувати унікальну адресу IPv6 без жодного пристрою, який відстежує, яка адреса призначена якому вузлу. Без стану та без статусу в контексті призначення адреси означають наступне. Призначення адреси з урахуванням стану включає сервер або інший пристрій, який відстежує стан кожного призначення. Він відстежує доступність пулу адрес і вирішує конфлікти дубльованих адрес. Він також реєструє кожне призначення та відстежує час закінчення. Призначення адреси без стану означає, що жоден сервер не відстежує, які адреси були призначені та які адреси все ще доступні для призначення.

Також у сценарії призначення без стану вузли відповідають за вирішення будь-яких конфліктів дубльованих адрес, дотримуючись логіки: згенеруйте адресу IPv6, запустіть виявлення дублікатів адреси (DAD), якщо адреса використовується, згенеруйте іншу та знову запустіть DAD і так далі.

По суті, коли пристрій підключається до мережі, він надсилає пакет на маршрутизатор із запитом параметрів конфігурації для з'єднання. Після отримання параметрів підключення пристрій створює свою власну адресу, поєднуючи свою апаратну MAC-адресу та 64-бітний префікс, надісланий маршрутизатором.

1.6 Протокол DHCPv6

На відміну від SLAAC, DHCPv6 — це повноцінний мережевий протокол для конфігурації вузлів версії 6 (IPv6), потрібний для роботи з IP-адресами, префіксами IP та іншими даними конфігурацій, які в свою чергу необхідні для роботи в мережі IPv6. Це нова версія протоколу DHCP. За допомогою IPv6 можна автоматично генерувати IP-адресу (використовуючи автоналаштування). Крім того, протокол DHCPv6 може генерувати їх використовуючи задані заздалегідь конфігурації.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

За допомогою серверів на IPv6, які використовують DHCP, користувачі також можуть отримати додаткову інформацію (домен, DNS сервер). Також DHCPv6 може використовуватися для отримання подібної інформації, навіть якщо він не використовується для отримання самої IP-адреси (допоміжний DHCP сервер). Однак, DHCPv6 не потрібен для конфігурації з адресами серверів систем доменного імені (DNS), тому що вони можуть бути налаштовані за допомогою протоколу сусідніх пристроїв (NDP), який також є механізмом автоналаштування.

Сервер DHCPv6 використовується лише для призначення інформації, яку не дає автоконфігурація (наприклад, ім'я домену), кілька DNS-серверів та всі інші параметри, які може запропонувати DHCP.

Комунікація у мережі на DHCP зазвичай відбувається за допомогою 4х повідомлень, які називаються вимогою, пропозицією, запитом та відповіддю (solicit, advertise, request, reply). Можливий також “швидкий” тип спілкування: 2 повідомлення (лише запит і відповідь). За замовчуванням використовується звичайний режим, якщо компанія хоче швидкий режим, його потрібно ввімкнути як на сервері DHCPv6, так і на клієнті^[2].

Звичайний і швидкий режими мають різну спеціалізацію використання: за RFC 4039, швидкий режим корисний у мережах «високої мобільності», де клієнти часто приходять і відходять. Накладні витрати на 4 повідомлення можуть не знадобитися, тому 2 повідомлення достатньо для виконання роботи. Якщо у мережі є кілька серверів DHCPv6 (для резервування), компанії потрібно використовувати звичайний режим (4 повідомлення).

1.7 Списки контролю доступу

Перш за все, ACL (Access Control List) — це список керування доступом, який визначає, які пристрої або користувач може отримувати доступ до об'єкта (у нашому випадку мережі або ресурсу мережі), і які саме операції можна або

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

заборонено виконувати суб'єкту (у нашому випадку, який стек протоколів можливо використати).

Кожен ACL має один або кілька записів контролю доступу (ACE), які складаються з імені користувача або групи користувачів. Користувач також може бути ім'ям ролі, наприклад, програміст або тестувальник. Для кожного з цих користувачів, груп або ролей права доступу вказані в рядку бітів, які називають маскою доступу. Як правило, системний адміністратор або власник об'єкта створює список контролю доступу для об'єкта^[1].

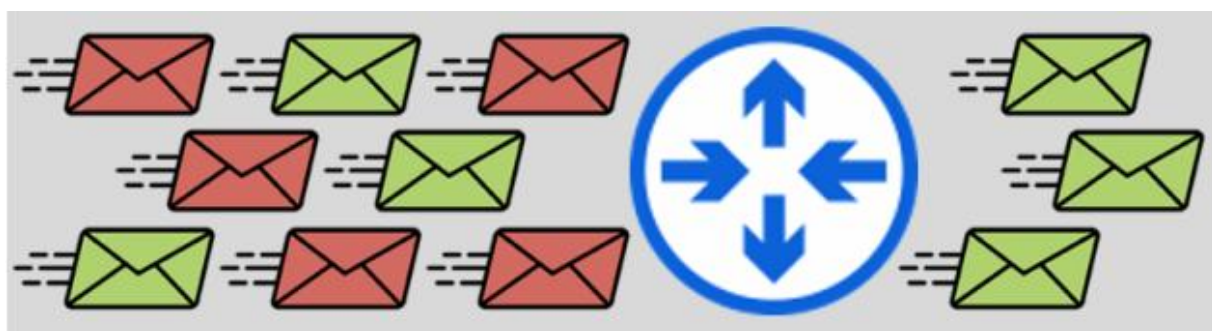


Рис 1.3 Списки контролю доступу

Одна з основних переваг ACL це - продуктивність. ACL забезпечують переваги в продуктивності перед іншими технологіями, які виконують ту ж функцію. Вони налаштовуються безпосередньо на апаратному забезпеченні пересилання пристрою маршрутизації, тому списки контролю доступу не мають негативного впливу на продуктивність пристроїв маршрутизації. Порівняйте це з брандмауером перевірки стану, який є окремою програмою, яка може спричинити погіршення продуктивності. Крім того, контроль мережевого трафіку дозволяє мережам бути більш ефективними.

ACL у мережі на IPv6 відрізняється від четвертої версії протоколу. На відміну від попереднього розділення на звичайні (номер списку від 1 до 99) та розширені (номер від 100) ACL, тепер вони усі є розширеними. Подібні обмеження були зумовлені мінімальною інформацією, що могла передаватись в

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

мережі. З останньою версією протоколу кількість даних значно більша, тому за допомогою ACL можливо контролювати протоколи, які будуть проходити фільтрацію. Обмеженням ACL на IPv6 є неможливість фільтрації за MAC-адресами, що зумовлена специфікою самого протоколу.

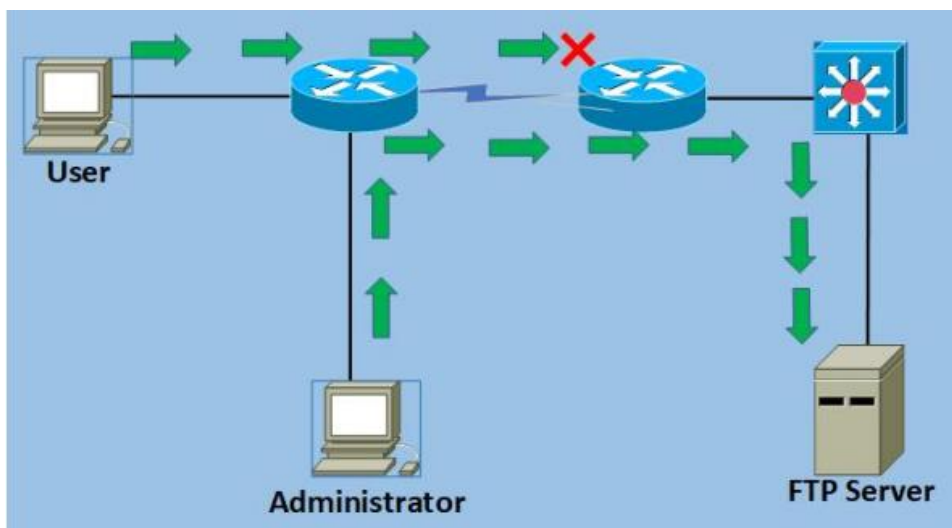


Рис 1.4 Схематичне зображення роботи ACL

Адміністратори мережі можуть розмістити список контролю доступу в різних точках мережі залежно від архітектури мережі. ACL часто розміщуються на граничних маршрутизаторах мережі, оскільки вони межують із загальнодоступним Інтернетом. Це дає ACL можливість фільтрувати трафік, перш ніж він досягне решти мережі.

1.8 Агрегація каналів

Для підвищення пропускної здатності між обладнанням в мережі, необхідно виконати агрегацію відповідних портів. Агрегування каналів (англ. link aggregation) - технології об'єднання декількох паралельних каналів передачі даних в мережах Ethernet в один логічний, що дозволяють збільшити пропускну здатність та підвищити надійність. У різних конкретних реалізаціях агрегування застосовуються інші назви: транкінг портів (англ. port trunking),

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

зв'язування каналів (link bundling), склеювання адаптерів (NIC bonding), сполучення адаптерів (NIC teaming).

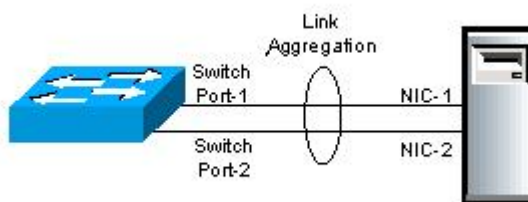


Рисунок 1.5 - Агрегація каналів

Головна перевага налаштування каналів таким чином у тому, що потенційно підвищується смуга пропускання: в ідеальних умовах смуга може досягти суми смуг пропускання об'єднаних каналів. Інша перевага — «гаряче» резервування ліній зв'язку: у разі відмови одного з агрегованих каналів трафік без переривання сервісу надсилається через решту, а після відновлення каналу, що відмовив, він автоматично включається в роботу.

Мережевий стандарт IEEE 802.3ad у складі групи для локальних обчислювальних мереж IEEE 802 прийнятий у 2000 році. У загальному випадку, агрегування восьми стандартних каналів за допомогою 802.3ad виявляється дешевшим, ніж один пристрій, що підтримує на порядок більшу пропускну здатність, і дозволяє поступово збільшувати швидкість каналів у системі без необхідності купувати дорогі швидші адаптери.

Однак агрегування має обмеження: розподіл трафіку каналами може бути нерівномірним, аж до того, що весь трафік йде по одному каналу, а інші простоюють, що в крайніх випадках означає відсутність виграшу у пропускну здатності порівняно з єдиним каналом^{[10][11]}. Крім того, об'єднувати можна не більше 8 каналів, що у разі гігабітних каналів дає теоретичну сумарну пропускну здатність лише в 8 Гбіт/сек замість 10 Гбіт/сек, які може забезпечити один швидкодіючий адаптер.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

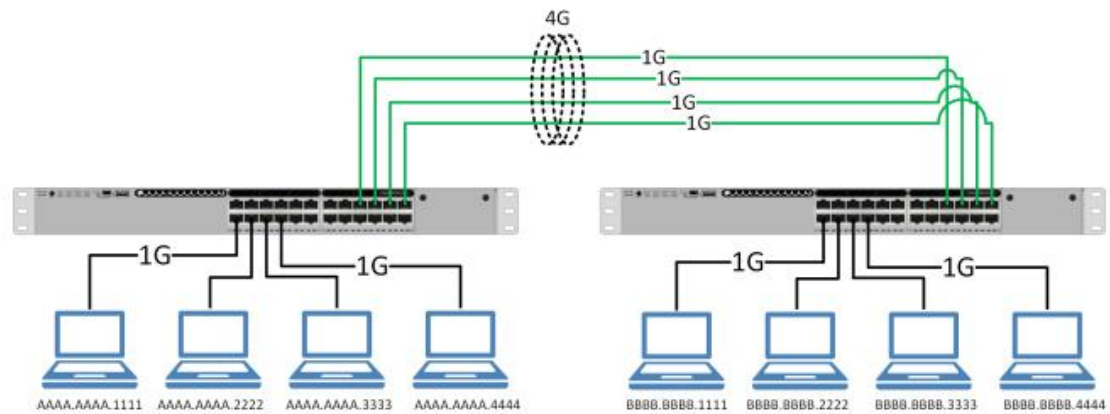


Рисунок 1.6 - Схематичне зображення агрегації портів

Варто зазначити, що, як правило, усі порти при агрегуванні повинні бути одного типу. Об'єднані порти повинні бути налаштовані на одну швидкість передачі (хоча за стандартом 802.3ad змішувати порти з різною швидкістю допустимо, на практиці такі конфігурації найчастіше виявляються непрацездатними).

1.9 EIGRPv6

Enhanced Interior Gateway Routing Protocol (EIGRP) — це вдосконалений протокол векторної маршрутизації, який використовується в комп'ютерній мережі для автоматизації рішень щодо маршрутизації та налаштування. Протокол був розроблений Cisco Systems як власний протокол, доступний лише на маршрутизаторах Cisco. EIGRP використовується на маршрутизаторі для спільного використання маршрутів з іншими маршрутизаторами в одній автономній системі.

На відміну від інших добре відомих протоколів маршрутизації, таких як RIP, EIGRP надсилає лише інкрементні оновлення, зменшуючи навантаження на маршрутизатор і кількість даних, які необхідно передати. EIGRP замінив протокол внутрішньої маршрутизації шлюзу (IGRP) у 1993 році. Однією з

		Балан А.О.			KIK.KP.B – 123 – 03 – ПЗ	Арк.
		Головня О.С.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

основних причин цього була зміна на безкласові адреси IPv4 в Інтернет-протоколі, який IGRP не міг підтримувати. EIGRPv6^{[2][4][7]} відрізняється тим, що у першу чергу налаштовується для шостої версії IP протоколу. Через це, процес налаштування також відрізняється (налаштування в першу чергу на інтерфейсі). В плані авторизацій EIGRPv6, порівняно з EIGRP підтримує лише авторизацію за допомогою MD5. У налаштуванні параметрів маршрутизації за замовчуванням (широта та затримка) не відрізняються від свого попередника. Додаткові параметри для налаштування, як навантаження або надійність, є спільними для обох.

1.10 Протоколи IPv4 та IPv6

Протокол IPv4 (англ. Internet Protocol version 4) - четверта версія інтернет-протоколу (IP). Перша версія, що широко використовується у світі. Далеко у минулому, коли інтернет лише створювався, його сучасний об'єм був неправильно оцінений, тому 32-бітні адреси (IP-адреси) вважались добрим рішенням. Однак на сьогодні кількості унікальних IP-адрес, що може надати IPv4 вже недостатньо для задоволення потреб людства (32-бітні адреси це потенційно 2^{32} унікальних). Вважається, що станом на 2022 рік кількість пристроїв у мережі більше 12,2 мрд штук^[19]. Рішенням нестачі унікальних адрес мала слугувати NAT, однак ця технологія не є єдиним рішенням.

Протокол IPv6 є логічним розвитком четвертої версії. Протокол розроблений у 1996 році та мав слугувати заміщенням недосконалого попередника. На той період часу вже було зрозуміло, що з IPv4 унікальних адрес буде недостатньо для всіх користувачів. Разом із поступовим впровадженням IPv6, було прийнято рішення зберегти зворотню сумісність цих протоколів, тому більшість приладів, маючи доступ до інтернету, працюють у режимі “дуал стек”, підтримуючи обидві технології одразу.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 1.1

Порівняння версій протоколу IP

	IPv4	IPv6
Розроблений	1981	1999
Розмір адреси	32-бітна	128-бітна
Позначення адреси	Розмежована точками десятькова: 192.162.25.10/24	Шістнадцяткова система числення 3FFE:F2001:0324::ABDD/48
Кількість адрес	$2^{32} = 4,294,967,296$	$2^{128} = 5 \cdot 10^{28}$

IPv6 базується на IP та використовує 128-бітні адреси. Іноді стверджується, новий протокол може забезпечити до $5 \cdot 10^{28}$ унікальних адрес на кожного жителя Землі. Такий великий адресний простір було запроваджено заради ієрархічності адрес (це полегшує маршрутизацію). Проте збільшений простір адрес зробить NAT необов'язковим. Класичне застосування IPv6 (по мережі /64 на абонента; використовується тільки unicast-адресація) забезпечить можливість використання понад 300 млн. IP-адрес на кожного жителя Землі. Крім того, більшість суміжних протоколів також отримали оновлення, що сприяє загальній якості мережі. Більш детально порівняння протоколів можна подивитись у таблиці 1.1.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СХЕМИ АДРЕСАЦІЇ

2.1 Розробка топології комп'ютерної мережі

Корпоративна мережа повинна мати декілька відділів (за аналогією з реальним розмежуванням поверхів, наприклад). Для кращого адміністрування та масштабування, вона буде спроектована з урахуванням ієрархії (а саме розділення на рівні):

- *Ядро (Core);
- *Розподіл (Distribution);
- *Рівень доступу (Access layer).

Загальна топологія спроектованої мережі представлена на рисунку 2.1. Збільшене подання загальної топології наведене у додатку А.

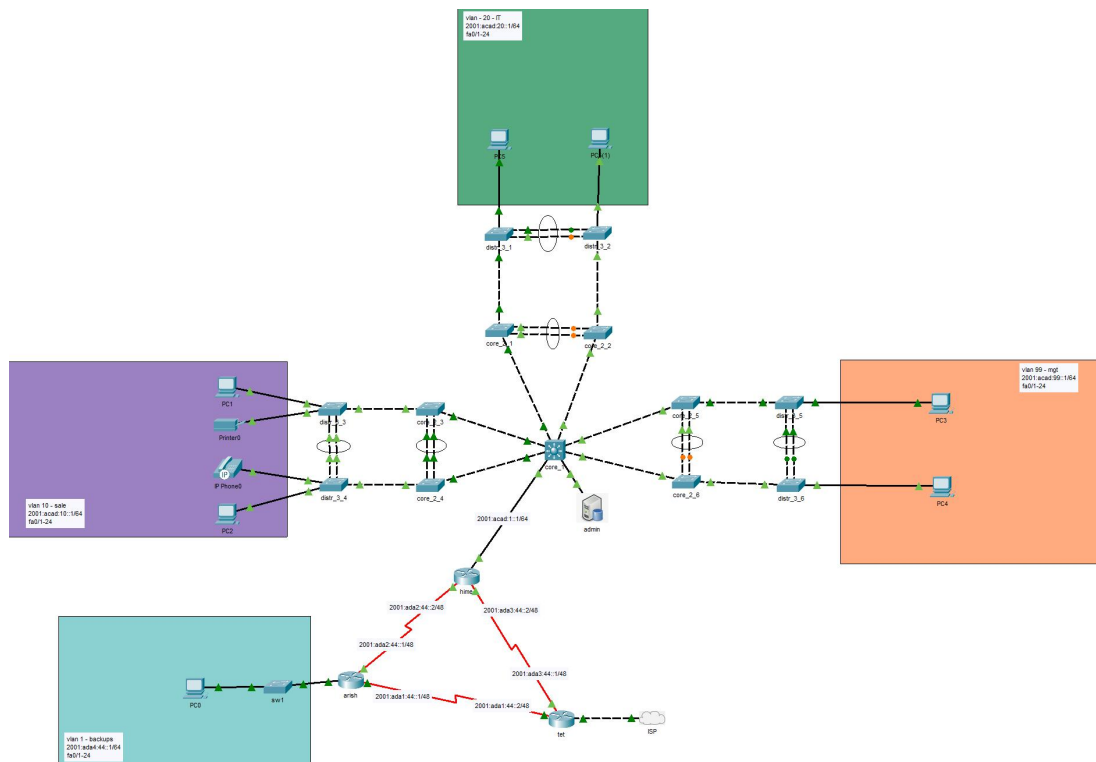


Рисунок 2.1 - Загальна топологія спроектованої мережі

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

Ядро:

*6 комутаторів 2950-24, 3 пари агрегованих між собою для більшої надійності та розподілу навантаження.

*1 L2 комутатор 3650-24IPS, об'єднує філіали організації між собою, та надає доступ до корпоративної ланки мережі.

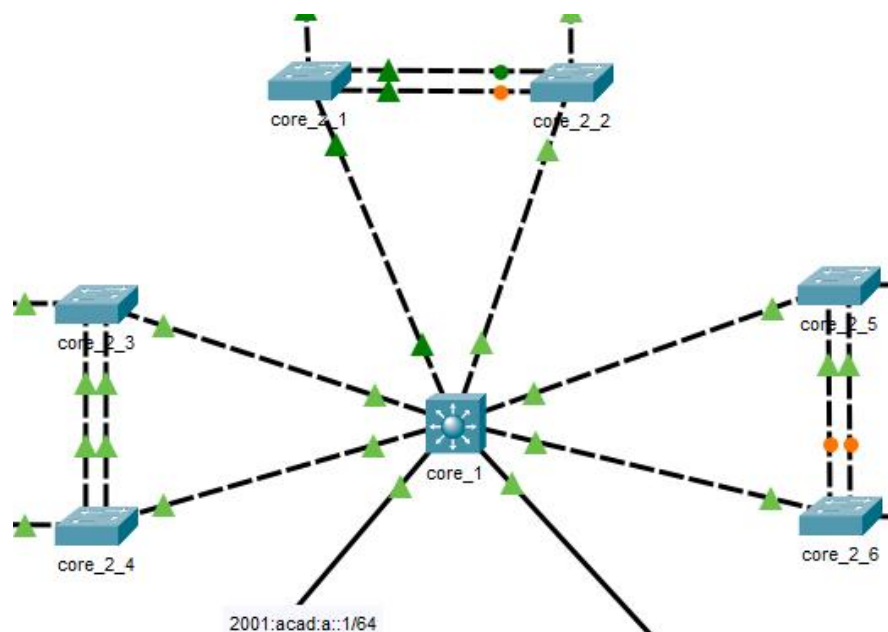


Рис 2.2 Ядро мережі

Розподіл:

*6 комутаторів 2950-24, розділених по 2 на кожну гілку корпорації, кількість обладнання рівномірно розподіляється між 2 комутаторами.



Рис 2.3 Рівень розподілу мережі

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

Доступ:

- *6 робочих станцій, що мають прямий доступ до комутатора розподілу
- *1 Сервер адміністрування
- *2 одиниці розумної техніки (принтер, IP телефон)

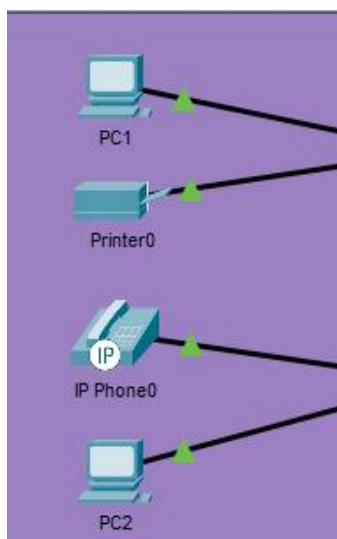


Рис 2.4 Рівень доступу мережі

Ядром мережі являє собою комутатор 2 рівня (layer 2), що виконує роль брандмауера (мережевого екрану) для внутрішньої мережі. Через ядро мережі проходить весь трафік компанії. Доступ до внутрішньої мережі відбувається через граничний маршрутизатор.

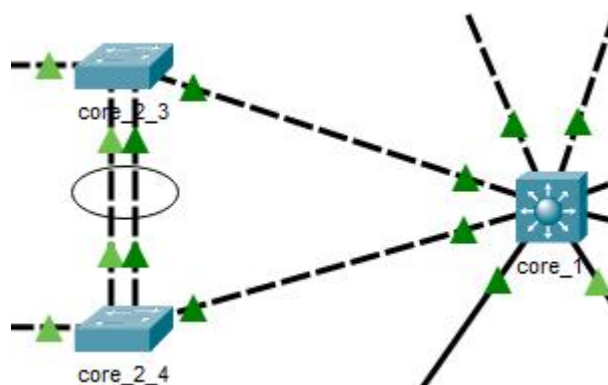


Рис 2.5 Ядро мережі та мережева ланка корпорації

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

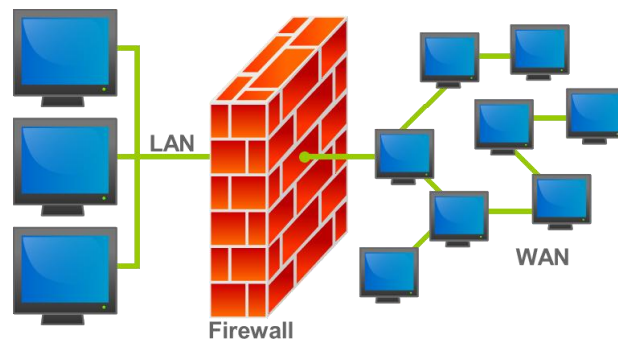


Рис 2.6 Схематичне зображення брандмауера

Корпоративна мережа з'єднує між собою офіси компанії. Ці офіси в силу розташування знаходяться далеко один від одного, тому з'єднання відбувається за рахунок виділених каналів зв'язку із використанням власного обладнання.

Варто зазначити, що можливий варіант оренди каналів зв'язку у самого провайдера інтернету, що може бути вдалим рішенням при обмеженому бюджеті. Власні канали надають можливість кращого адміністрування та супроводження. Вкупі з контролем протоколів всередині мережі, це створює кращі умови для розширення корпоративної мережі.

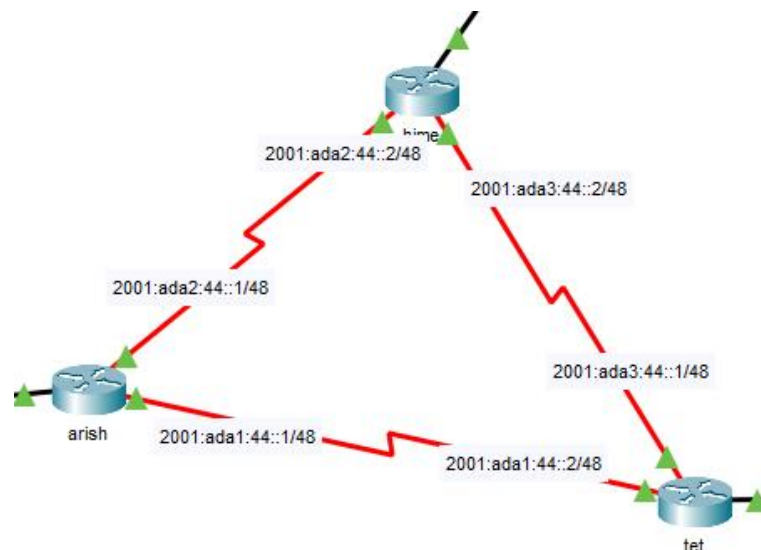


Рис 2.7 Виділені канали зв'язку

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

Важливо зазначити необхідність використання оптоволоконних кабелів. Враховуючи об'єм трафіку та відстань передачі без використання ретрансляторів, передача мідним кабелем неможлива. Оптика, хоча і має більшу собівартість (встановлення та обслуговування) надає більші потужності проєктованій мережі.

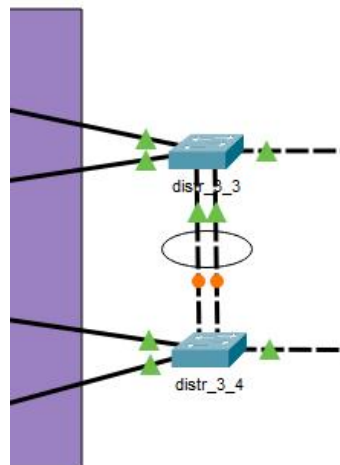


Рис 2.8 Рівень розподілу

Рівень розподілу має надавати можливість підключення робочим станціям. Це локальні комутатори, що знаходяться у прямій близькості до користувачів. Це можуть бути робочі кабінети або ділянка приміщення, користувачам на якій потрібний доступ в інтернет. Користувачі будуть розділені між собою технологією VLAN для більшої зручності адміністрування та в якості однієї з політик захисту мережі.

Рівень доступу - це звичайні користувачі, що мають доступ до мережі. Залежно від кількості кінцевих вузлів, необхідно лише збільшити кількість комутаторів. Змінювати налаштування самої мережі не потрібно, звичайно, якщо мова не йде про збільшення кількості віртуальних мереж. Доступ до ресурсів корпорації може бути обмежений за допомогою ACL, що встановлений локально, або на ключових вузлах мережі (наприклад, ядрі). Усі

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

користувачі отримують адреси через заздалегідь налаштований DHCP-пул.

Варто зазначити, що можлива також і роздільна видача адрес. Для цього можливо налаштувати виділений сервер. Час оренди по замовчуванню - 1 доба. Усі зміни у адресному пулі фіксуються у таблиці адресації.

2.2 Розробка схеми адресації мережі

Для планування адресації мережі був використане правило, що власному обладнанню буде надана статична адреса, поза пулом DHCP. Усім користувачам, адреси видаються довільним чином зі стеку. Розподілення адрес відбувається за відділами залежно від логічного розмежування за VLAN.

Таблиця 2.1

Таблиця маршрутизації відділів компанії

№	Назва відділу	Номер Vlan	Префікс	Довжина префіксу
1	Відділ продажів	10	2001:acad:10::	/64
2	Технічний відділ (IT)	20	2001:acad:20::	/64
3	Менеджмент	99	2001:acad:99::	/64

Для планування адресацій виділених каналів прийнято рішення виділити окрему підмережу для пари маршрутизаторів.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.2

Таблиця маршрутизації виділених каналів

№	Назва обладнання	Інтерфейс	Префікс	Довжина префіксу
1	Маршрутизатор hime	Serial1/0	2001:ada2:44::2	/48
		Serial1/1	2001:ada3:44::2	
		Fa0/0	2001:acad:a::1	/64
2	Маршрутизатор arish	Serial1/0	2001:ada2:44::1	/48
		Serial1/1	2001:ada1:44::1	
		Fa0/0	2001:ada4:44::1	/64
3	Маршрутизатор tet	Serial1/0	2001:ada3:44::1	/48
		Serial1/1	2001:ada1:44::2	
		Fa0/0	2001:ada6:44::1	/64

Адресація всередині мережі для користувачів відбувається динамічно, але для власного обладнання (комутаторів) з міркувань безпеки, а також зручності було прийнято рішення використовувати статистику.

Таблиця 2.3

Таблиця маршрутизації пристроїв мережі

№	Назва обладнання (Комутатор)	Адреса	Маска	Префікс	Інтерфейс
1	core_2_1	192.168.25.21	255.255.255.0	/24	Vlan1
2	core_2_2	192.168.25.22			

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

Продовження таблиці 2.3

№	Назва обладнання (Комутатор)	Адреса	Маска	Префікс	Інтерфейс
3	core_2_3	192.168.25.23	255.255.255.0	/24	Vlan1
4	core_2_4	192.168.25.24			
5	core_2_5	192.168.25.25			
6	core_2_6	192.168.25.26			
7	distr_3_1	192.168.25.31			
8	distr_3_2	192.168.25.32			
9	distr_3_3	192.168.25.33			
10	distr_3_4	192.168.25.34			
11	distr_3_5	192.168.25.35			
12	distr_3_6	192.168.25.36			

Таблиця 2.4

Таблиця маршрутизації пристроїв ядра

№	Назва обладнання	Інтерфейс	Префікс	Довжина префіксу
1	Core_1	Vlan1	2001:acad:a::2	/64

РОЗДІЛ 3 ВИБІР ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Вибір обладнання для організації роботи мережі

При виборі моделі комутатора основними критеріями виступають:

- *Можливість налаштування;
- *Кількість входів/виходів;
- *Швидкодія;
- *Модульність;
- *Собівартість.

У даній мережі використовуються комутатори декількох напрямленостей: ключові та вторинні. Залежно від потреб та логічного розташування обладнання, будуть підібрані потужності приладу. Якщо мова йде про вузли мережі, будуть використані потужні рішення, якщо про підключення звичайних користувачів - оптимальні.



Рис 3.1 Cisco 2960 IOS15 (схематичне зображення у PacketTracer та реальний вигляд)

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

У даній мережі використовуються комутатори 2960 та 2950 на двадцять чотири/шість портів відповідно Fast Ethernet. Так як об'єм трафіку, що планується на передачу, досить великий, необхідно використовувати обладнання, що може працювати без перебоїв з великими масивами даних.



Рис 3.2 Cisco 2950-24 (схематичне зображення у PacketTracer та реальний вигляд)

У якості вузлових комутаторів, будуть використовуватись моделі Cisco 3560 24 PS. Catalyst — це бренд для різноманітних мережевих комутаторів, бездротових контролерів і бездротових точок доступу, що продаються Cisco Systems. Хоча вони зазвичай асоціюються з комутаторами Ethernet, протягом історії бренду було доступно кілька різних типів мережевих інтерфейсів.



Рис 3.3 Cisco 3650-24PS (схематичне зображення у PacketTracer та реальний вигляд)

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Залежно від рівня використання було підібрано 3 моделі комутаторів: для розподілення трафіку ядра (3650-24PS), для рівня розподілу (2950-24) та для рівня доступу (2960 IOS15).



Рис 3.4 Cisco 2811 (схематичне зображення у PacketTracer та реальний вигляд)

В якості моделі маршрутизаторів була вибрана модель 2811 так як вона підтримує інтерфейс типу Serial та стек необхідних протоколів. У якості економних рішень, буде використовуватись Cisco 1941 через свою модульність, підтримку потрібних протоколів та ціну.



Рис 3.5 Cisco 1941 (схематичне зображення у PacketTracer та реальний вигляд)

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

Платформи Integrated Services Routers Generation 2 мають багатоядерні процесори, комутацію Gigabit Ethernet. з розширеним POE та новими можливостями моніторингу та контролю енергії, одночасно покращуючи загальну продуктивність системи.

Крім того, новий модуль програмного забезпечення Cisco IOS® Software Universal Image and Services Ready Engine дає змогу відокремити розгортання апаратного та програмного забезпечення, забезпечуючи стабільну технологічну основу, яка може швидко адаптуватися до зростаючих вимог мережі. Загалом, Cisco серії 1900 пропонує безпрецедентну загальну економію вартості володіння та гнучкість мережі завдяки інтелектуальній інтеграції провідних на ринку систем безпеки, уніфікованих комунікацій, бездротового зв'язку та послуг прикладних програм.

Варто зазначити, що усе підібране обладнання відповідає світовим стандартам якості та надійності. За особистим досвідом, обладнання фірми Cisco та, особливо, Catalyst є надійним та призводить до мінімуму можливих ризиків для мережі.

3.2 Налагодження обладнання мережі

Перш за все, відокремлено 3 підмережі: VLAN 10, 20, 99. Присвоєно відповідним інтерфейсам адреси IPv6. Ввімкнено інкапсуляцію dot1Q на віртуальних інтерфейсах. Ввімкнено DHCP сервіси на цих інтерфейсах (відповідно до попереднього розподілення). Ввімкнено multicast-routing для коректної роботи пристрою та присвоєно 32-бітний ідентифікатор маршрутизатора для подальшого налаштування EIGRPv6. Додано асоціації DHCP пулів до віртуальних інтерфейсів, налаштовано додаткові параметри маршрутизації.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface FastEthernet0/0.10
 encapsulation dot1Q 10
 no ip address
 ipv6 address 2001:ACAD:10::1/64
 ipv6 dhcp server dhcp-pool-vlan-10
!
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 no ip address
 ipv6 address 2001:ACAD:20::1/64
 ipv6 dhcp server dhcp-pool-vlan-20
!
interface FastEthernet0/0.99
 encapsulation dot1Q 99
 no ip address
 ipv6 address 2001:ACAD:99::1/64
 ipv6 dhcp server dhcp-pool-vlan-99
!

```

Рис 3.6 Налаштування інтерфейсів на маршрутизаторі h1me

```

interface Serial1/0
 no ip address
 ipv6 address 2001:ADA2:44::2/48
 ipv6 eigrp 1
!
interface Serial1/1
 no ip address
 ipv6 address 2001:ADA3:44::2/48
 ipv6 eigrp 1
!

```

Рис 3.7 Налаштування Serial інтерфейсів на маршрутизаторі h1me

```

ipv6 router eigrp 1
 eigrp router-id 1.1.1.1
 no shutdown
!

```

Рис 3.8 Налаштування EIGRPv6 на маршрутизаторі h1me

```

ipv6 dhcp pool dhcp-pool-vlan-10
 address prefix 2001:acad:10::/64 lifetime 172800 86400
 domain-name SERV1.main
!
ipv6 dhcp pool dhcp-pool-vlan-20
 address prefix 2001:acad:20::/64 lifetime 172800 86400
 domain-name SERV1.main
!
ipv6 dhcp pool dhcp-pool-vlan-99
 address prefix 2001:acad:99::/64 lifetime 172800 86400
 domain-name SERV1.main
!

```

Рис 3.9 Налаштування DHCP серверу на маршрутизаторі h1me

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Vlan1
  no ip address
  ipv6 address 2001:ACAD:A::2/64

```

Рис 3.10 Ввімкнено та налагоджено Vlan1 та присвоєно йому адресу IPv6 на комутаторі Core_1

```

!
interface GigabitEthernet1/0/2
  switchport mode trunk
!
interface GigabitEthernet1/0/3
  switchport mode trunk
!
interface GigabitEthernet1/0/4
  switchport mode trunk
!
interface GigabitEthernet1/0/5
  switchport mode trunk
!
interface GigabitEthernet1/0/6
  switchport mode trunk
!
interface GigabitEthernet1/0/7
  switchport mode trunk
!

```

Рис 3.10 Налагоджено режим передачі інтерфейсів на комутаторі Core_1

```

line vty 0 4
  login local
  transport input telnet
!

username admin privilege 15 password 0 pass
!

```

Рис 3.11 Налаштована можливість віддаленого доступу до обладнання та створена необхідність авторизації

Для оптимізації роботи комутаторів розподілу та доступу, щоб уникнути можливої відмови мережі, кількість комутаторів подвоєна та створено агреговані канали для балансування навантаження. В теорії це має збільшити пропускну здатність комутатора вдвічі. У якості протоколу агрегації використано PAgP у режимі desirable.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface FastEthernet0/3
  switchport mode trunk
  channel-group 1 mode desirable
!
interface FastEthernet0/4
  switchport mode trunk
  channel-group 1 mode desirable

core_2_4#show etherchannel
      Channel-group listing:
      -----

Group: 1
-----
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Portchannels = 1
Protocol:   PAgP
core_2_4#show etherchannel summ
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)        PAgP       Fa0/3(P) Fa0/4(P)
core_2_4#

```

Рис 3.12 Агрегація каналів у режимі PAgP

```

!
interface FastEthernet0/2
  switchport access vlan 10
!

```

Рис 3.13 Розмежовано користувачів по Vlan за попереднім розподілом

```

IPv6 access list server-acl
deny ipv6 2001:ADA4:44::/64 host 2001:ACAD:A::3
IPv6 access list main-acl
deny ipv6 2001:ADA4:44::/64 host 2001:ACAD:A::3

core_1#

```

Рис 3.14 Налаштування ACL на комутаторі Core_1

Для налагодження EIGRP було налаштовано відповідний ідентифікатор на самому маршрутизаторі та закріплено інтерфейси до вибраної групи. Для налаштування додаткових параметрів, а саме затримку та надійність були використані параметри за замовчуванням.

```

show ipv6 eigrp interfaces
IPv6-EIGRP interfaces for process 1

Interface      Peers    Xmit Queue Mean    Pacing Time Multicast    Pending
                Un/Reliable SRTT    Un/Reliable Flow Timer  Routes
-----
Ser1/0          1         0/0     1236    0/10         0           0
Ser1/1          1         0/0     1236    0/10         0           0
Fa0/0           0         0/0     1236    0/10         0           0

hime#show ipv6 pro
hime#show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Interfaces:
    Serial1/0
    Serial1/1
    FastEthernet0/0
  Redistributing: eigrp 1
    Maximum path: 16
    Distance: internal 90 external 170

hime#

```

Рис 3.15 Перевірка роботи EIGRP на маршрутизаторі hime

3.3 Перевірка працездатності мережі

Далі необхідно перевірити коректність розмежування користувачів по VLAN, а також правильну видачу IP-адрес DHCP сервером, а саме видачу IPv6 префіксів залежно від віртуальної мережі в якій знаходиться кінцевий пристрій.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

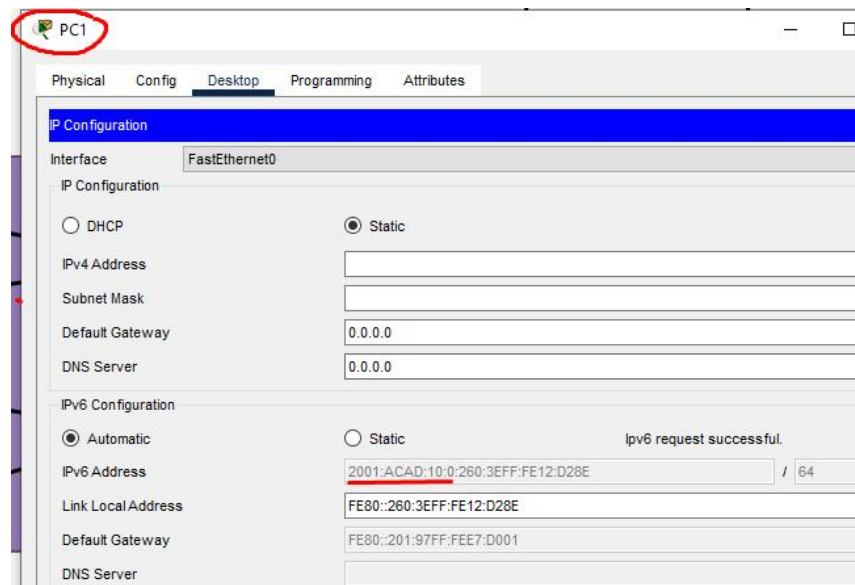


Рис 3.16 Видача адреси PC1 з DHCP-пулу (VLAN 10)

```
C:\>ping 2001:acad:a::1

Pinging 2001:acad:a::1 with 32 bytes of data:

Reply from 2001:ACAD:A::1: bytes=32 time=263ms TTL=255
Request timed out.
Reply from 2001:ACAD:A::1: bytes=32 time=33ms TTL=255
Reply from 2001:ACAD:A::1: bytes=32 time=526ms TTL=255

Ping statistics for 2001:ACAD:A::1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 526ms, Average = 274ms
```

```
C:\>ping 2001:ACAD:10:0:260:3EFF:FE12:D28E

Pinging 2001:ACAD:10:0:260:3EFF:FE12:D28E with 32 bytes of data:

Reply from 2001:ACAD:10:0:260:3EFF:FE12:D28E: bytes=32 time=241ms TTL=128

Ping statistics for 2001:ACAD:10:0:260:3EFF:FE12:D28E:
    Packets: Sent = 2, Received = 1, Lost = 1 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 241ms, Maximum = 241ms, Average = 241ms

Control-C
^C
C:\>
```

Рис 3.17 Перевірка зв'язку між станціями

Налаштуємо захист мережі за допомогою ACL. Налаштування брандмауера буде захищати внутрішній сервер від контактів ззовні. Доступ всередині мережі вільний. Подібна політика повинна захистити конфіденційні данні від несанкційованого доступу.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

```
hime#show ipv6 access-list
IPv6 access list MAIN-ACL
deny icmp any host 2001:ACAD:A::3 (4 match(es))
```

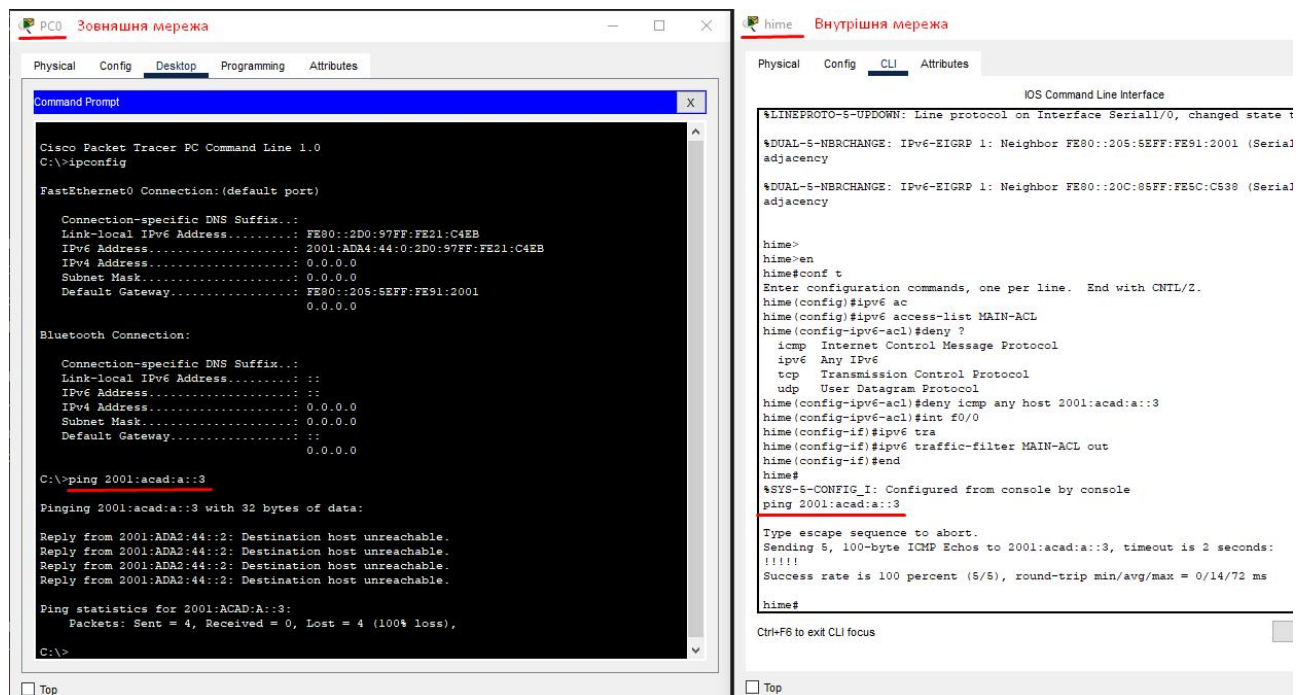


Рис 3.18 Перевірка роботи ACL

Перевірено можливість підключення віддалено до обладнання. Подібне налаштування потрібно для можливості налаштувати комутатор/маршрутизатор без фізичного знаходження біля нього. Для налаштувань необхідно авторизуватись та залежно від користувача (його привілеїв) будуть доступні ті чи інші команди. Для перевірки підключення буде створений користувач з ім'ям Admin та паролем pass та привілеєм рівним 15 (найвищий рівень доступу).



Рис 3.19 Підключення до обладнання

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

Для стенду на Packet Tracer та демонстрації процедури віддалених сесій були використані попередні дані для входу. При введенні неправильного користувача, обладнання має видати повідомлення про некоректний ввід даних. При неправильному паролі обладнання має перервати активну сесію підключення:



Рис 3.20 Помилки віддаленого підключення



Рис 3.21 Помилки віддаленого підключення (неправильний пароль)

Доступ до консольного порту вирішено залишити, через необхідність прямого налаштування обладнання у разі потреби. Усі вузли (комутатори та маршрутизатори) фізично захищені від зовнішнього втручання (знаходять у пластикових/залізних стендах або у приміщеннях ключі від яких є у керівництва та відповідного персоналу).

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

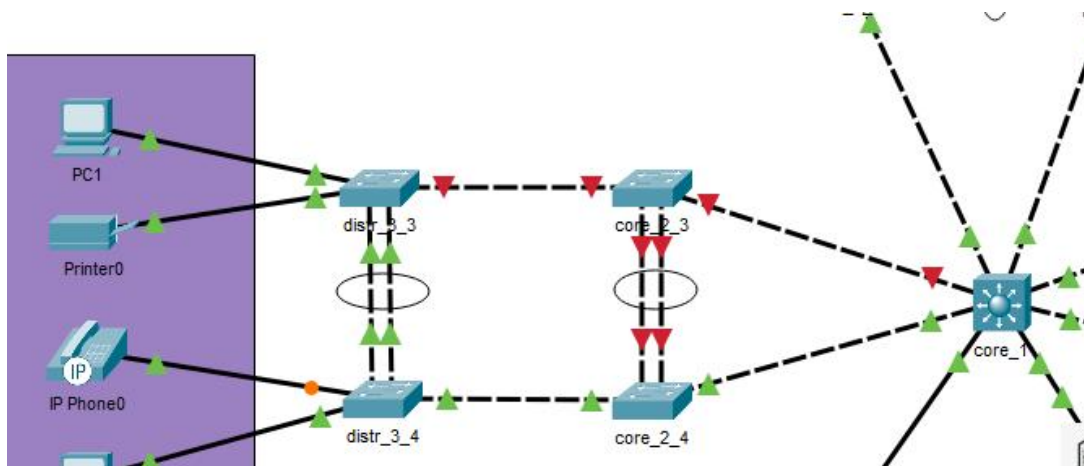


Рисунок 3.22 Перевірка роботи мережі за умови відмови живлення одного з вузлів ядра

В ході тестування мережі на стресостійкість було виявлено збільшений об'єм трафіку, що проходить на другий комутатор з пари ядра. Проблем зі зв'язком всередині мережі не виявлено. Збільшився час реагування до серверу у вузлів що були під'єднані до вимкненого комутатора. Було спрогнозовано орієнтовний час реагування для усунення проблем із маршрутизатором див таб. 3.1.

Таблиця 3.1

Усунення несправності у мережі

№п/п	Проблема	Час на усунення	Примітка
1	Аналіз масштабів аварії	до 5 хвилин	Необхідно перевірити кількість проблемного обладнання у всій мережі
2	Підготовка обладнання на заміну (комплектція) та призначення відповідальної особи	від 5 до 7 хвилин	Залежно від кількості уражених вузлів чи каналів час може відрізнятись, комплектція відбувається паралельно із аналізом мережі

Продовження таблиці 3.1

Усунення несправності у мережі

№п/п	Проблема	Час на усунення	Примітка
3	Аналіз каналів зв'язку та обладнання спеціалістом на місці, заміна обладнання	від 30 хвилин до декількох годин	Перевірка каналів зв'язку та обладнання відбуваються перед потенційною заміною, при ураженні перших, можлива затримка у зв'язку з перевіркою місця розриву.
4	Повторний аналіз мережі	до 5 хвилин	Необхідно перевірити кількість проблемного обладнання після заміни
	Всього	від 45 хвилин	

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було розроблено проект модернізації корпоративної IPv4 мережі організації. Проаналізовано теоретичні засади та ринок мережевого обладнання для адміністрування комп'ютерної мережі. Було спроектовано топологію корпоративної мережі, з урахуванням потреб замовника. Підібрано та налаштовано відповідне обладнання. Перевірено відповідність побудованої мережі вимогам замовника. Фізично реалізовано розроблену корпоративну мережу на обладнанні Cisco. Протестовано її роботу у звичайних та стресових умовах.

У першому розділі, виконуючи завдання кваліфікаційної роботи було опрацьовано та проаналізовано особливості побудови корпоративних мереж, структуру мереж інтернет провайдерів та локальних мереж на основі сучасних протоколів. Досліджено специфікації, особливості мережевих технологій у тому числі структуру витої пари (Fast/Gigabit та Ethernet). Досліджено особливості функціонування та структуру технологій IP шостої та четвертої версій, оптимізації топології PVST, організацію DHCP-сервісів у різних варіаціях (із фіксацією стану та без нього) тощо. Здійснено аналіз ринку, вибрано рішення, що задовольняють поставлені потреби та адаптовано їх за необхідності. Було проаналізовано їх недоліки та переваги, що дало розуміння, можливості виконання поставленого завдання.

У другому розділі розроблено проект модернізації корпоративної IPv4-мережі організації. Розроблено схему побудови даної мережі. Відокремлено рівень ядра, транспортний рівень та рівень доступу. Проаналізовано ринок мережевого обладнання та впроваджено знайдені рішення у проект залежно від розташування даних елементів у мережі. Розроблено схему адресації обладнання, користувачів та віртуальних мереж. Попередньо розподілено обладнання у різні точки будівлі та розмежовано за необхідністю різними VLAN. Закріплено практичні навички налагодження маршрутизації між мережами, організації віртуальних локальних мереж.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

У третьому розділі було перевірено відповідність розробленої мережі поставленим вимогам. Протестовано основні якості мережі: швидкодію, стресостійкість та захищеність. Перевірено можливість віддаленого під'єднання до обладнання. Змодельовано спроектовану мережу у Cisco Packet Tracer та GNS3. Перевірено роботу змодельованої мережі, зв'язок між користувачами, зв'язок користувачів та глобальної мережі а також стресостійкість шляхом вимикання одного з ключових елементів - комутатора ядра. Зроблено відповідні висновки за проведеною роботою.

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is Access Control List (ACL)? - SearchSoftwareQuality (techtarget.com) [Електронний ресурс] – Режим доступу до ресурсу: <https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL>
2. Cisco DHCPv6 Server Configuration (networklessons.com) [Електронний ресурс] – Режим доступу до ресурсу: <https://networklessons.com/ipv6/cisco-dhcpv6-server-configuration>
3. IPv6 Stateless Address Auto-configuration (SLAAC) | NetworkAcademy.io [Електронний ресурс] – Режим доступу до ресурсу: <https://www.networkacademy.io/ccna/ipv6/stateless-address-autoconfiguration-slaac>
4. 13-4 EIGRP for IPv6 - Free CCNA Study Guide [Електронний ресурс] – Режим доступу до ресурсу: <https://www.freecnastudyguide.com/study-guides/ccna/ch13/13-4-eigrp-ipv6/>
5. Мережевий екран — Вікіпедія (wikipedia.org) [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D0%B5%D0%BA%D1%80%D0%B0%D0%BD
6. Брандмауер — Вікіпедія (wikipedia.org) [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/%D0%91%D1%80%D0%B0%D0%BD%D0%B4%D0%BC%D0%B0%D1%83%D0%B5%D1%80>
7. 7.4.1.2 Comparing EIGRP for IPv4 and IPv6 (num.edu.mn) [Електронний ресурс] – Режим доступу до ресурсу: http://cisco.num.edu.mn/CCNA_R&S4/course/module7/7.4.1.2/7.4.1.2.html
8. Інтернет речей — Вікіпедія (wikipedia.org) [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1>

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

%80%D0%BD%D0%B5%D1%82_%D1%80%D0%B5%D1%87%D0%B5%D0%B9

9. Networking Basics: How to Configure Standard ACLs on Cisco Routers | CBT Nuggets [Электронный ресурс] – Режим доступа до ресурсу: <https://www.cbtnuggets.com/blog/certifications/cisco/networking-basics-how-to-configure-standard-acls-on-cisco-routers>
10. Solved: How to put router in trunk mode and link to switch [Solved] - Cisco Community [Электронный ресурс] – Режим доступа до ресурсу: <https://community.cisco.com/t5/switching/how-to-put-router-in-trunk-mode-and-link-to-switch-solved/td-p/2381000>
11. VLAN Trunks (3.2.2) > Cisco Networking Academy's Introduction to VLANs | Cisco Press [Электронный ресурс] – Режим доступа до ресурсу: <https://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=7>
12. Client Mode Vs Transparent Mode - Cisco Community [Электронный ресурс] – Режим доступа до ресурсу: <https://community.cisco.com/t5/switching/client-mode-vs-transparent-mode/td-p/815804>
13. IPv6 Subnet Calculator - subnettingpractice.com [Электронный ресурс] – Режим доступа до ресурсу: <https://subnettingpractice.com/ipv6-subnet-calculator.html>
14. Spanning Tree from PVST+ to Rapid-PVST Migration Configuration Example - Cisco [Электронный ресурс] – Режим доступа до ресурсу: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/72836-rapidpvst-mig-config.html>
15. PAgP configuration (Cisco) - Grandmetric [Электронный ресурс] – Режим доступа до ресурсу: https://www.grandmetric.com/knowledge-base/design_and_configure/how-to-configure-cisco-pagp/
16. IP Addressing: NAT Configuration Guide, Cisco IOS Release 15M&T - Configuring NAT for IP Address Conservation [Support] - Cisco [Электронный ресурс] – Режим доступа до ресурсу:

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/iadnat-addr-consv.html

17. Configure Telnet, Console and AUX Port Passwords on Routers - Cisco [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/45843-configpasswords.html>

18. Как настроить VLAN'ы на коммутаторах Cisco Catalyst - Cisco Community [Електронний ресурс] – Режим доступу до ресурсу: <https://community.cisco.com/t5/%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F-%D0%B8-%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%86%D0%B8%D1%8F/%D0%BA%D0%B0%D0%BA-%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B8%D1%82%D1%8C-vlan-%D1%8B-%D0%BD%D0%B0-%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%82%D0%BE%D1%80%D0%B0%D1%85-cisco-catalyst/ta-p/3145627>

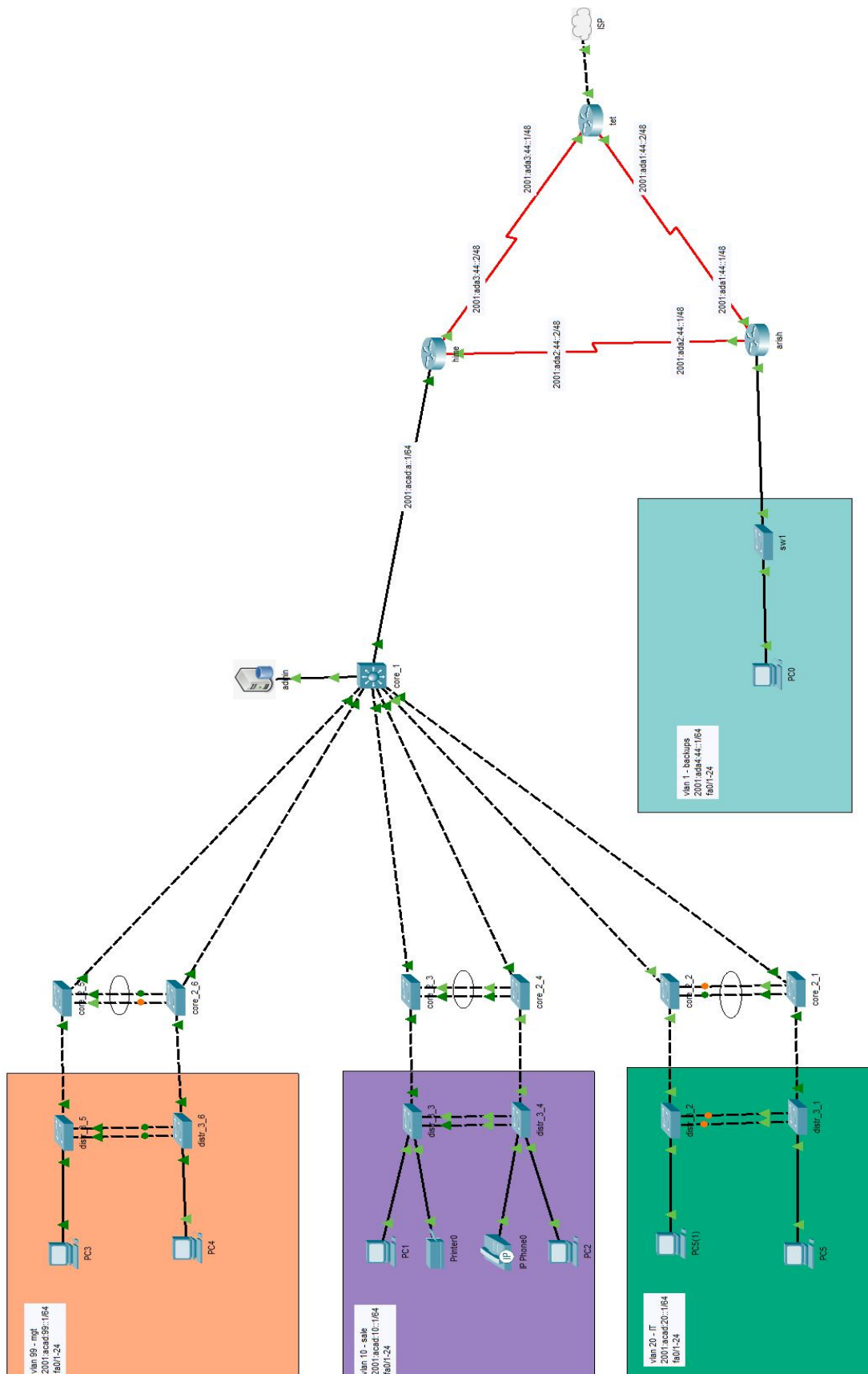
19. Звіт: кількість підключених пристроїв IoT зросла на 18% до 14,4 мільярдів по всьому світу (internetua.com) [Електронний ресурс] – Режим доступу до ресурсу: <https://internetua.com/zvit-kilkist-pidkluacsenih-pristroyiv-iot-zrosla-na-18-do-14-4-milyardiv-po-vsomu-svitu>

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток А – Топологія мережі



		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрутизатор hime

```

Current configuration : 1822 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname hime
!
!
!
!
!
!
!
!
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
ipv6 dhcp pool dhcp-pool-vlan-10
address prefix 2001:acad:10::/64 lifetime
172800 86400
domain-name SERV1.main
!
ipv6 dhcp pool dhcp-pool-vlan-20
address prefix 2001:acad:20::/64 lifetime
172800 86400
domain-name SERV1.main
!
ipv6 dhcp pool dhcp-pool-vlan-99
address prefix 2001:acad:99::/64 lifetime
172800 86400
domain-name SERV1.main
!
!
!
!
license udi pid CISCO2811/K9 sn
FTX1017Q15A-
!
!
!
!

```

Маршрутизатор arish

```
Current configuration : 1069 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname arish
!
!
!
!
!
!
!
!
!
no ip cef
ipv6 unicast-routing
!
no ipv6 cef
!
!
!
!
license udi pid CISCO2811/K9 sn
FTX1017WU00-
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
```

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

<pre> ! ! ! ! ! no ip domain-lookup ! ! spanning-tree mode pvst ! ! ! ! ! ! interface FastEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:ACAD:A::1/64 ipv6 eigrp 1 ! interface FastEthernet0/0.10 encapsulation dot1Q 10 no ip address ipv6 address 2001:ACAD:10::1/64 ipv6 dhcp server dhcp-pool-vlan-10 ! interface FastEthernet0/0.20 encapsulation dot1Q 20 no ip address ipv6 address 2001:ACAD:20::1/64 ipv6 dhcp server dhcp-pool-vlan-20 ! interface FastEthernet0/0.99 encapsulation dot1Q 99 no ip address ipv6 address 2001:ACAD:99::1/64 ipv6 dhcp server dhcp-pool-vlan-99 ! interface FastEthernet0/1 no ip address duplex auto speed auto shutdown ! interface Serial1/0 no ip address </pre>	<pre> no ip address duplex auto speed auto ipv6 address 2001:ADA4:44::1/64 ipv6 eigrp 1 ! interface FastEthernet0/1 no ip address duplex auto speed auto shutdown ! interface Serial1/0 no ip address ipv6 address 2001:ADA2:44::1/48 ipv6 eigrp 1 clock rate 2000000 ! interface Serial1/1 no ip address ipv6 address 2001:ADA1:44::1/48 ipv6 eigrp 1 clock rate 2000000 ! interface Serial1/2 no ip address clock rate 2000000 shutdown ! interface Serial1/3 no ip address clock rate 2000000 shutdown ! interface Vlan1 no ip address shutdown ! ipv6 router eigrp 1 eigrp router-id 2.2.2.2 no shutdown ! ip classless ! ip flow-export version 9 ! ! ! </pre>
--	---

<pre> ipv6 address 2001:ADA2:44::2/48 ipv6 eigrp 1 ! interface Serial1/1 no ip address ipv6 address 2001:ADA3:44::2/48 ipv6 eigrp 1 ! interface Serial1/2 no ip address clock rate 2000000 shutdown ! interface Serial1/3 no ip address clock rate 2000000 shutdown ! interface Vlan1 no ip address shutdown ! router rip ! ipv6 router eigrp 1 eigrp router-id 1.1.1.1 no shutdown ! ip classless ! ip flow-export version 9 ! ! ! ! ! ! ! ! ! line con 0 ! line aux 0 ! line vty 0 4 login ! ! ! ! ! </pre>	<pre> ! ! ! ! ! line con 0 ! line aux 0 ! line vty 0 4 login ! ! ! end Маршрутизатор tet Current configuration : 1033 bytes ! version 15.1 no service timestamps log datetime msec no service timestamps debug datetime msec no service password-encryption ! hostname tet ! ! ! ! ! ! ! ! ! ! no ip cef ipv6 unicast-routing ! no ipv6 cef ! ! ! ! ! license udi pid CISCO2811/K9 sn FTX10171H8V- ! ! ! ! ! ! ! </pre>
---	---

no ip address

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

```
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
!
interface GigabitEthernet1/0/4
switchport mode trunk
!
interface GigabitEthernet1/0/5
switchport mode trunk
!
interface GigabitEthernet1/0/6
switchport mode trunk
!
interface GigabitEthernet1/0/7
switchport mode trunk
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
```

```

shutdown
!
ipv6 router eigrp 1
eigrp router-id 3.3.3.3
no shutdown
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
!
!
End
Комутатор core_2_3
Current configuration : 1317 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname core_2_3
!
!
!
!
!
username admin privilege 15 password 0 pass
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1

```

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address
ipv6 address 2001:ACAD:A::2/64
!
ip classless
!
ip flow-export version 9
!
!
ipv6 access-list server-acl
permit ipv6 2001:ADA4:44::/64 host
2001:ACAD:A::3
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
login local
transport input telnet
!
!
!
!
End
Комутатор core_2_4
Current configuration : 1248 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec

```

```

switchport mode trunk
!
interface FastEthernet0/1
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
switchport mode trunk
channel-group 1 mode desirable
!
interface FastEthernet0/4
switchport mode trunk
channel-group 1 mode desirable
!
interface FastEthernet0/5
switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!

```

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no service password-encryption
!
hostname core_2_4
!
!
!
!
username admin privilege 15 password 0 pass
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
!
interface FastEthernet0/1
!
interface FastEthernet0/2
switchport mode trunk
!
interface FastEthernet0/3
channel-group 1 mode desirable
!
interface FastEthernet0/4
channel-group 1 mode desirable
!
interface FastEthernet0/5
switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!

```

```

interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface Vlan1
ip address 192.168.25.23 255.255.255.0
!
!
!
!
line con 0
!
line vty 0 4
login local
transport input telnet
line vty 5 15
login
!
!
!
End
Комутатор distr_3_3
Current configuration : 1387 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname distr_3_3
!
!
!
!
username admin privilege 15 password 0 pass
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
switchport mode trunk

```

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface Vlan1
ip address 192.168.25.24 255.255.255.0
!
!
!
!
line con 0
!
line vty 0 4
login local
transport input telnet
line vty 5 15
login
!
!
!
!
end
Комутатор distr_3_4
Current configuration : 1410 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname distr_3_4
!

```

```

!
interface FastEthernet0/1
!
interface FastEthernet0/2
switchport access vlan 10
!
interface FastEthernet0/3
switchport mode trunk
channel-group 1 mode desirable
!
interface FastEthernet0/4
switchport mode trunk
channel-group 1 mode desirable
!
interface FastEthernet0/5
switchport access vlan 10
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21

```

		Балан А.О.			КИК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
username admin privilege 15 password 0 pass
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
switchport mode trunk
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
switchport access vlan 10
!
interface FastEthernet0/3
switchport mode trunk
channel-group 1 mode desirable
!
interface FastEthernet0/4
switchport mode trunk
channel-group 1 mode desirable
!
interface FastEthernet0/5
switchport access vlan 10
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!

```

```

!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.25.33 255.255.255.0
!
!
!
line con 0
!
line vty 0 4
login local
transport input telnet
line vty 5 15
login
!
!
!
end

```

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.25.34 255.255.255.0
!
!
!
!
line con 0
!
line vty 0 4
login local
transport input telnet
line vty 5 15
login
!
!
!
!
end

```

		Балан А.О.			КІК.КР.Б – 123 – 03 – ПЗ	Арк.
		Головня О.С.				59
Змн.	Арк.	№ докум.	Підпис	Дата		