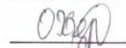


Міністерство освіти і науки України
Державний Університет «Житомирська Політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

До випускної кваліфікаційної роботи бакалавра на тему:
“Проект захищеної корпоративної мережі компанії на основі
комутаторів 3 рівня”

Виконав студент 4-го курсу групи КБ-21-2
спеціальності 125 “Кібербезпека”

 Єгор ОХРЕМЧУК

Керівник завідувач кафедри
комп'ютерної інженерії та кібербезпеки,
кандидат технічних наук, доцент

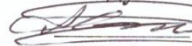
 Андрій ЄФІМЕНКО

Рецензент професор кафедри
комп'ютерної інженерії та кібербезпеки,
доктор технічних наук, доцент

 Володимир ВОРОТНИКОВ

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 КІ та КБ
 Андрій ЄФІМЕНКО
"3" березня 2025р.

ЗАВДАННЯ

На випускню кваліфікаційну роботу бакалавра
Охремчуку Єгору Максимовичу

Тема роботи: "Проект захищеної корпоративної мережі компанії на основі комутаторів 3 рівня"

Затверджена Наказом університету від 3 березня 2025 року №80с

Термін здачі студентом закінченої роботи

Вихідні дані роботи:

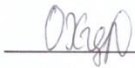
- корпоративна мережа організації
- протоколи та методи для захисту від загроз та атак

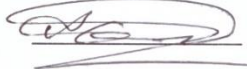
Обладнання та програмне забезпечення:

1. Симулятор Cisco Packet tracer

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

Розділ	Прізвище, ініціали та посади консультанта	Підпис, дата	
		завдання видав	завдання прийняв

Студент  Єгор ОХРЕМЧУК

Керівник роботи  Андрій ЄФІМЕНКО

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	03.03.2025	Виконано
2	Аналіз літературних джерел	30.03.2025	Виконано
3	Аналіз об'єкта дослідження	01.04.2025	Виконано
4	Постановка задачі дослідження	05.04.2025	Виконано
5	Розробка структурної моделі	07.04.2025	Виконано
6	Розрахунок параметрів адресації	09.04.2025	Виконано
7	Вибір технології для реалізації	15.04.2025	Виконано
8	Розробка захищеної КМ	22.04.2025	Виконано
9	Налаштування мережі	16.05.2025	Виконано
10	Адміністрування мережі	26.06.2025	Виконано
11	Перевірка працездатності	01.06.2025	Виконано
12	Оформлення пояснювальної записки	26.06.2025	Виконано
13	Оформлення презентації	26.06.2025	Виконано
14	Захист	Згідно розкладу	

Студент Охремчук Єгор Єгор ОХРЕМЧУК

Керівник роботи Єфіменко Андрій Андрій ЄФІМЕНКО

АНОТАЦІЯ

Кваліфікаційна робота на тему “Проект захищеної корпоративної мережі компанії на основі комутаторів 3 рівня” складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Пояснювальна записка містить 38 рисунків та займає 103 сторінки. Список використаних джерел містить 24 найменувань.

Метою даної роботи є розробка проекту захищеної корпоративної мережі компанії на основі комутаторів 3 рівня.

У додатках наведені конфігураційні файли маршрутизатора та комутаторів.

Ключові слова: локальна мережа, Cisco, комутатор третього рівня, LACP, VLAN, PVST+, VTP, RADIUS, мережна безпека, SSH, NTP, Syslog, DHCP Snooping, Dynamic ARP Inspection, автентифікація, агрегація каналів, топологія мережі, інформаційна безпека, інфраструктура підприємства.

					ККІК.КР.Б - 125 - 14 - ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект захищеної корпоративної мережі компанії на основі комутаторів 3 рівня	Літ.	Арк.	Аркушів
Розроб.		Охремчук С.М.		26.06.25				
Керівник		Єфіменко А.А.		26.06.25			1	103
Реценз.		Воротніков В.В.		26.06.25		ФІКТ Гр. КБ-21-2		
Н. контр.		Трокоз С.М.		26.06.25				
Затверд.		Єфіменко А.А.		26.06.25				

ABSTRACT

The qualification work on the topic ‘Project of a secure corporate network of a company based on Layer 3 switches’ consists of a list of abbreviations, introduction, three chapters, conclusions, a list of references and appendices.

The explanatory note contains 38 figures and runs to 103 pages. The list of references includes 24 titles.

The purpose of this paper is to develop a project of a secure corporate network based on Layer 3 switches.

The appendices contain configuration files for the router and switches.

Keywords: local area network, Cisco, Layer 3 switch, LACP, VLAN, PVST+, VTP, RADIUS, network security, SSH, NTP, Syslog, DHCP Snooping, Dynamic ARP Inspection, authentication, link aggregation, network topology, information security, enterprise infrastructure.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				2
Змн.	Арк.	№ док.ум.	Підпис	Дата		

Зміст

ВСТУП.....	5
РОЗДІЛ 1 ПРИНЦИПИ ПОБУДОВИ КОРПОРАТИВНИХ КАМПУСНИХ МЕРЕЖ	6
1.1 Підходи до побудови корпоративних кампусних комп'ютерних мереж організацій на базі L3-комутаторів	6
1.2 Технології та протоколи побудови кампусної корпоративної мережі	13
1.3 Технології та протоколи захисту кампусної корпоративної мережі	25
1.4 Сервіси та протоколи забезпечення підтримки роботи користувачів кампусної корпоративної мережі	33
РОЗДІЛ 2 ПРОЕКТУВАННЯ МЕРЕЖІ ОРГАНІЗАЦІЇ.....	42
2.1 Проектування топології мережі.....	42
2.2 Розробка системи IP-адресації.....	44
2.3 Проектування служб та сервісів прикладного рівня	47
2.4 Проектування підсистеми мережного захисту	50
РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ СПРОЕКТОВАНОЇ ЛОКАЛЬНОЇ IPV4-МЕРЕЖІ ОРГАНІЗАЦІЇ.....	53
3.1 Вибір обладнання для розробленого проекту мережі	53
3.2 Налаштування спроектованої мережі.....	57
3.3 Тестування роботи побудованої мережі	64
ВИСНОВКИ	79
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	80
ДОДАТКИ	83

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				3
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

VLAN – Virtual Local Area Network

PAgP – Port Aggregation Protocol

PVST+ – Per-VLAN Spanning Tree+

LAN – Local Area Network

DR – Designated Bridge

BDR – Backup Designated Bridge

SSH – Secure SHell

DHCP – Dynamic Host Configuration Protocol

NTP – Network Time Protocol

VTP – VLAN Trunking Protocol

RSPAN – Remote SPAN

SPAN – Switched Port Analyzer

ARP – Address Resolution Protocol

DAI – Dynamic ARP Inspection

STP – Spanning Tree Protocol

BPDU – Bridge Protocol Data Unit

QoS – Quality of service

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				4
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасних умовах стрімкого розвитку цифрових технологій та збільшення кіберзагроз зростає потреба у створенні надійних, масштабованих і безпечних мережевих інфраструктур. Особливої уваги потребують корпоративні мережі, які є основою інформаційної взаємодії у компаніях. Застосування комутаторів третього рівня дозволяє поєднати високі швидкості передачі даних із можливостями маршрутизації та безпеки. Тема проектування захищеної корпоративної мережі з використанням комутаторів 3 рівня є актуальною в контексті захисту інформаційних ресурсів підприємств і підвищення ефективності мережевої інфраструктури.

Мета кваліфікаційної роботи: розробити проект захищеної корпоративної кампусної мережі компанії з використанням комутаторів третього рівня, що забезпечує ефективну маршрутизацію, сегментацію мережі та впровадження сучасних механізмів інформаційної безпеки.

Об’єкт дослідження: процес проектування та побудови захищеної корпоративної мережі компанії на основі комутаторів 3 рівня.

Предмет дослідження: сучасні методи проектування, маршрутизації та захисту корпоративних кампусних мереж, на базі комутаторів третього рівня з використанням технологій: VLAN, EIGRP, RADIUS, DHCP Snooping, DAI, PVST+, LACP, а також інтеграція сервісів (DHCP, NTP, Syslog) для підвищення безпеки та ефективності інфраструктури.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ПРИНЦИПИ ПОБУДОВИ КОРПОРАТИВНИХ КАМПУСНИХ МЕРЕЖ

1.1 Підходи до побудови корпоративних кампусних комп'ютерних мереж організацій на базі L3-комутаторів

Кампусна мережа є критичною інфраструктурою підприємства, що забезпечує надійне та безпечне з'єднання користувачів, доступ до додатків, спільну роботу та підтримку різноманітних пристроїв. Її роль трансформувалася від базової зв'язності до стратегічного активу, що безпосередньо впливає на продуктивність, інновації та користувацький досвід, підтримуючи цифрову трансформацію, гібридну роботу, хмарні сервіси.

Базовими моделями побудови корпоративних кампусних мереж є наступні моделі :

1. Ієрархічна (трирівнева) модель.
2. Модель зі згорнутим ядром (collapsed core, дворівнева).
3. Модель Spine-Leaf (кампусна фабрика, листкова).

Ієрархічна трирівнева модель лежить в основі сучасних мереж, її використовують для проектування мереж з високою надійністю та масштабованістю. Модель логічно розділяє мережу на окремі рівні, як правило – це рівень доступу, розподілу і ядро. Кожен рівень виконує свої функції, що сприяє створенню структури, полегшене керування та передбачуваний потік інформації.

Рівень доступу відповідає за під'єднання кінцевих пристроїв, пристроїв IoT, бездротові точки доступу. Основними функціями є забезпечення L2-з'єднання, безпека портів, передача живлення на підключені пристрої, реалізація QoS і початкове опрацювання трафіку.

Рівень розподілу працює як точка агрегації трафіку, від декількох комутаторів нижчого рівня. Слугує важливою межею контролю, що забезпечує дотримання мережевих політик за допомогою списків контролю доступу, механізмів QoS та іншого. Цей рівень також маршрутизує трафік між VLAN, консолідує отриману інформацію, забезпечує резервування шляхів у разі відмови.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

Рівень ядра: основний рівень, може мати назву: “Магістраль мережі”. Призначений для забезпечення високошвидкісного та надійного передавання даних через мережу кампусу. З’єднує різні блоки розподільчого рівня і потенційно може підключатися до центру обробки даних або межі глобальної мережі.

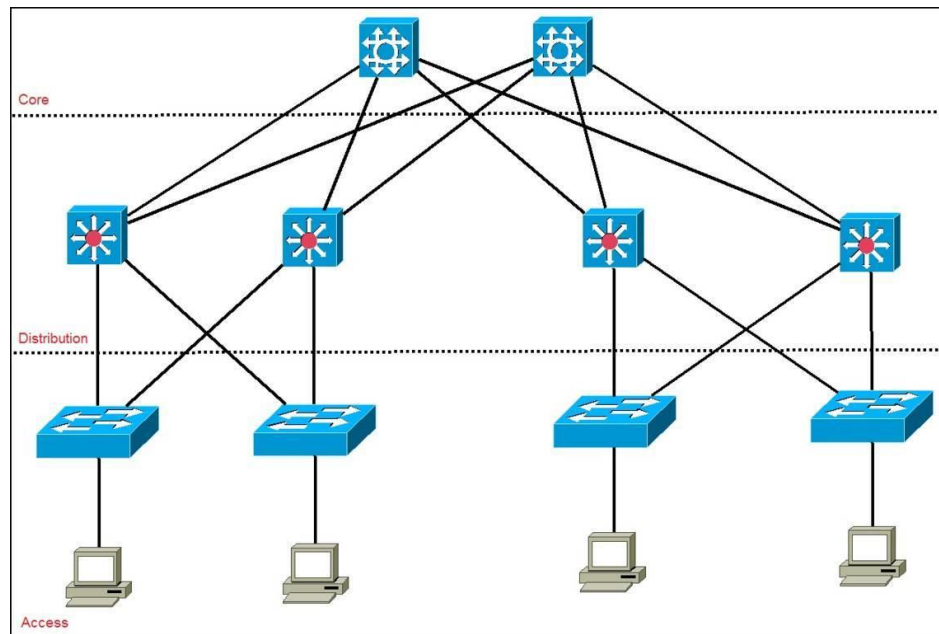


Рисунок 1.1 – Приклад ієрархічної моделі

Модель зі згорнутим ядром використовується в менших кампусах, де обслуговується приблизно 1000-1500 користувачів, для економії витрат, або без планів значного розширення мережі. Сутність цієї моделі полягає у об’єднанні функціональності рівня ядра та розподілу в один фізичний та логічний рівень. Комутатори, що виконують комбіновану роль зобов’язані бути потужними та високонадійними, оскільки на них покладаються критично важливі завдання: виконують маршрутизацію між VLAN, застосовують мережеві політики, забезпечують резервування шляхів до рівня доступу, а також відповідають за швидкісний транспорт агрегованого трафіку між різними мережевими сегментами, чи блоками, та мають підключення до критичних ресурсів (сервери, центри обробки даних, шлюзи, WAN).

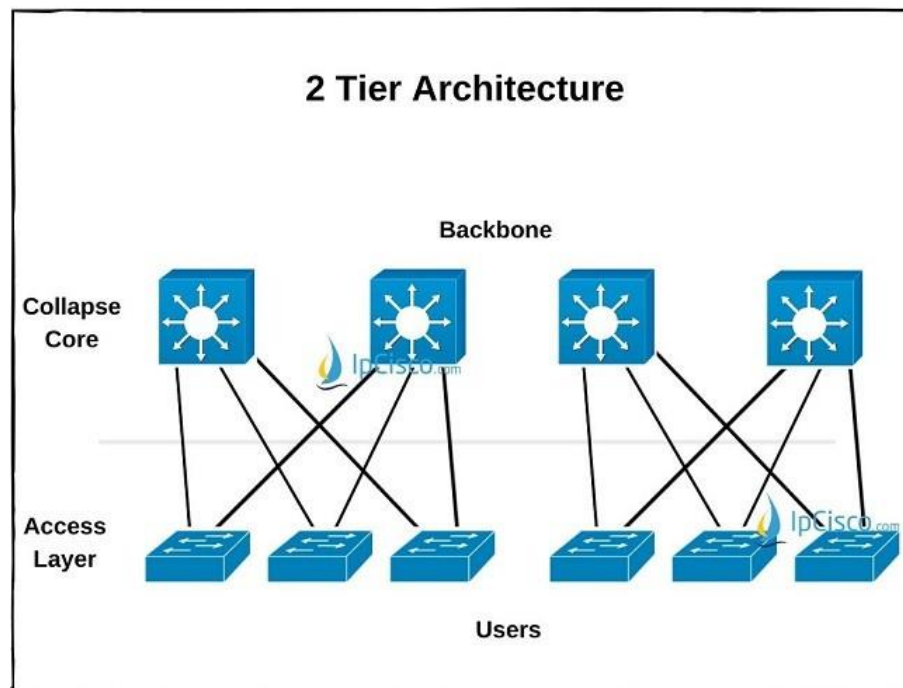


Рисунок 1.2 – Приклад дворівневої моделі

Модель Spine-Leaf застосовується у великих кампусах, або середовищах з високими вимогами до гнучкості, автоматизації та сегментації. Вона запозичує принципи архітектури дата-центрів, адаптуючи їх до специфіки кампусу. При її описі визначають два основні рівні, а саме – Leaf та Spine.

Leaf-рівень містить в собі комутатори, до яких безпосередньо підключаються кінцеві пристрої, виконують роль розширеного рівня доступу. Кожен Leaf-комутатор має високошвидкісні з'єднання до кожного комутатора Spine-рівня.

Spine-рівень складається з високопродуктивних комутаторів ядра, які виключно з'єднують Leaf-комутатори між собою. Spine-комутатори не з'єднуються безпосередньо між собою, їхня єдина функція – забезпечити надійний та високошвидкісний транспорт трафіку. Кожен Leaf підключений до кожного Spine.

2-Tier Spine-Leaf Architecture

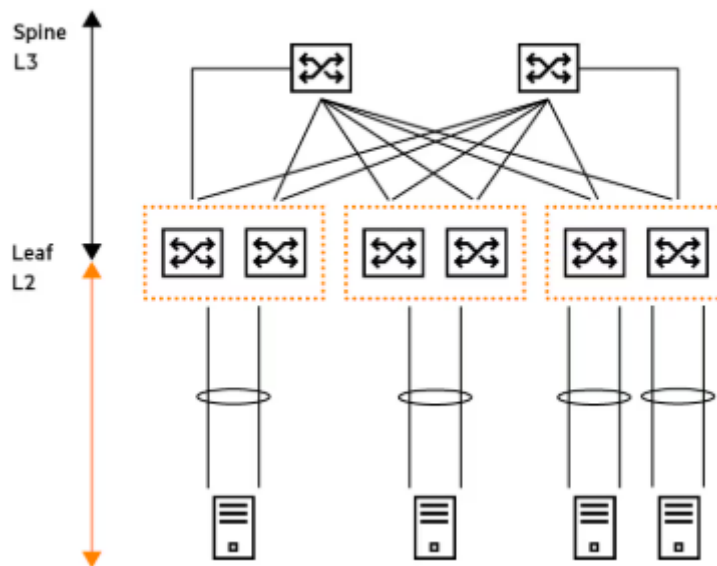


Рисунок 1.3 – Приклад листкової моделі

Таблиця 1.1

Переваги та недоліки різних методів побудови

	Ієрархічна модель	Модель зі згорнутим ядром	Модель Spine-Leaf
1	2	3	4
Переваги	Чітка сегментація функцій (доступ, розподіл, ядро). Ефективна ізоляція збоїв. Оптимальна для середніх/великих кампусів з прогнозованим зростанням. Перевірена надійність та широка підтримка обладнання.	Значна економія вартості. Спрощена фізична топологія та менша кількість пристроїв. Зменшення OPEX (спрощене управління, менше вузлів). Зберігає базові переваги ієрархії. Ідеальна для малих статичних середовищ.	Найвища продуктивність. Мінімальна та передбачувана затримка. Лінійна масштабованість (легке додавання Leaf/Spine). Відсутність єдиних точок відмови. Гнучка сегментація. Висока автоматизація (політико-орієнтоване керування). Оптимальна для великих/динамічних середовищ та хмарних робочих навантажень.

1	2	3	4
Недоліки	Вища вартість, складніша топологія . Потенційні вузькі місця на ядрі при значному зростанні трафіку. Обмежена підтримка сучасних автоматизованих середовищ. Повільніша збіжність при збоях порівняно з ESMR.	Більша область впливу збою. Жорсткі обмеження масштабування. Вищі вимоги до комутаторів. Складність модернізації при необхідності переходу до 3-рівневої. Обмежена продуктивність для інтенсивного міжсегментного трафіку.	Найвища початкова вартість. Значна складність кабельної інфраструктури. Високі вимоги до обладнання Leaf. Складність реалізації в розподілених кампусах. Низька ефективність для дуже малих мереж. Складність управління без спеціалізованих SDN-інструментів.

Під час побудови корпоративних кампусних мереж виникає низка завдань, для ефективного вирішення яких використовуються наступні принципи:

1. Масштабованість.
2. Відмовостійкість.
3. Безпека.
4. Продуктивність.

Масштабованість: здатність інфраструктури до безперервного зростання та адаптації до нових вимог, без потреби у великій перебудові мережевої архітектури. Масштабованість реалізується завдяки використанню ієрархічної модульної архітектури, яка забезпечує логічну та фізичну ізоляцію функцій, спрощує впровадження змін і дає змогу локалізувати модернізацію окремих ділянок мережі. Завчасне резервування пропускної здатності каналів, портів і обчислювальних ресурсів на ключових вузлах дозволяє уникати перевантажень при зростанні навантаження. Динамічні протоколи маршрутизації, автоматично адаптуються до змін у топології мережі, спрощуючи інтеграцію нових сегментів. Технології віртуалізації надають гнучкість у логічному розділенні інфраструктури, а засоби

автоматизації й центрального керування дозволяють віддалено масштабувати конфігурації та розгортати сервіси. В умовах сучасних ІТ-реалій усе більшого значення набуває інтеграція з хмарними середовищами, що забезпечують еластичне масштабування ресурсів у гібридних моделях.

Відмовостійкість передбачає збереження працездатності інфраструктури навіть у разі виходу з ладу окремих її компонентів або появи збоїв. Досягається за рахунок надлишковості критичних елементів — резервування маршрутизаторів, комутаторів, серверів, каналів зв'язку із дотриманням архітектурних підходів. Протоколи високої доступності, такі як HSRP, VRRP чи GLBP, дозволяють автоматично й майже миттєво перемикаєти шлюзи без порушення з'єднань. Для агрегації каналів і балансування навантаження використовуються в більшості протоколи LACP і PAgP, а у високодоступних рішеннях з двома активними контролерами — технології MC-LAG. Для запобігання мережевим петлям та пришвидшеного відновлення мережі в разі зміни топології застосовуються протоколи RSTP, MSTP, а в більш динамічних мережах — TRILL або SPB, які забезпечують паралельне використання кількох маршрутів. Сучасне обладнання підтримує функції безперервної передачі трафіку навіть під час внутрішніх збоїв або перезавантаження завдяки технологіям Non-Stop Forwarding і Stateful Switchover. Відмовостійкість неможлива без системного підходу до планування аварійного відновлення — Disaster Recovery Planning, що передбачає регулярне тестування сценаріїв аварійної роботи.

Безпека охоплює захист як фізичних ресурсів, так і логічної інфраструктури, даних, сервісів та користувачів. Сучасний підхід до побудови безпечної мережі базується на концепції багаторівневого захисту, де кожен рівень: фізичний, мережевий, прикладний — має власні механізми виявлення та протидії загрозам. На фізичному рівні важливо забезпечити контроль доступу до серверних приміщень і телекомунікаційних вузлів. На логічному рівні реалізується сегментація мережі за допомогою VLAN, DMZ, VPN або мікросегментації, що дозволяє ізолювати різні типи трафіку та обмежити поширення потенційної

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				11
Змн.	Арк.	№ докum.	Підпис	Дата		

загрози. Доступ до мережевих ресурсів контролюється через автентифікацію 802.1X, механізми AAA, списки контролю доступу, а також фаєрволи. Шифрування трафіку із застосуванням IPSec, SSL/TLS або MACsec забезпечує конфіденційність і цілісність переданих даних. Особлива увага приділяється протидії атакам через використання IDS/IPS-систем, DHCP Snooping, Dynamic ARP Inspection і IP Source Guard. В основі новітніх підходів до безпеки лежить концепція нульової довіри (Zero Trust), яка передбачає перевірку кожного елементу доступу незалежно від його розташування в мережі. Підкріпленням безпеки на організаційному рівні є впровадження політик інформаційної безпеки відповідно до стандартів, системи управління безпекою (ISMS) і моніторинг подій через SIEM-платформи.

Продуктивність - це здатність інфраструктури ефективно обробляти, передавати та доставляти трафік відповідно до вимог. Продуктивність залежить від вибору фізичних технологій доступу та магістральних каналів, з урахуванням майбутнього зростання обсягу трафіку. Сучасні мережі використовують 10G/25G/40G/100G Ethernet і оптичні інтерфейси, здатні обробляти великі обсяги даних із мінімальними затримками. Ключовим механізмом забезпечення продуктивності є система якості обслуговування, яка дозволяє класифікувати трафік, маркувати пакети за пріоритетом, керувати чергами та пріоритетами. Топологія мережі має бути оптимізована з урахуванням мінімізації кількості хопів і затримок, а балансування навантаження як на рівні серверів, так і маршрутів дозволяє рівномірно розподіляти трафік та уникати перевантаження окремих вузлів. Важливу роль відіграє використання високопродуктивного обладнання, з підтримкою лінійної швидкості обробки трафіку на всіх портах. Продуктивність мережі контролюється за допомогою систем моніторингу (SNMP, NetFlow, sFlow, IPFIX, telemetry), що дозволяють своєчасно виявляти вузькі місця, аналізувати поведінку трафіку та здійснювати проактивне планування модернізації інфраструктури.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2 Технології та протоколи побудови кампусної корпоративної мережі

1.2.1 Організація та використання VLAN. Протокол VTP.

Віртуальна локальна мережа – це логічно виділена область трансляції на каналному рівні моделі OSI. VLAN забезпечує розділення фізичної мережі на кілька віртуальних сегментів, ізольованих один від одного, цим дозволяє групувати пристрої в єдину віртуальну мережу незалежно від їхнього фізичного розташування. Також спрощують проектування мережі, зокрема, часто використовують для поділу великих мереж на автономні сегменти та зменшення широкомовного шуму.

Класифікація VLAN здійснюється за такими ознаками:

1. Функціональне призначення.
2. За методом конфігурації.
3. По способу формування VLAN.

За функціональним призначенням виділяють такі VLAN:

- VLAN даних (Data VLAN);
- Голосові VLAN (Voice VLAN);
- VLAN керування (Management VLAN);
- VLAN за замовчуванням (Default VLAN);
- Нативна VLAN (Native VLAN).

Data VLAN призначені для передачі даних користувачів, Voice VLAN призначені для передавання трафіку VoIP телефонії та відео; Management VLAN призначені для мережевого адміністрування. Voice VLAN конфігурується з пріоритетом передачі для покращення якості голосу. Management VLAN використовується виключно для керування мережевим обладнанням, ізольовуючи його від звичайного трафіку. Крім того, Default VLAN (за замовчуванням VLAN 1) і Native VLAN (потрапляє нетегований трафік)

За методом конфігурації розрізняють:

- Статичні

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

- Динамічні

Статичні VLAN (портово-базовані) налаштовуються вручну, кожен порт комутатора призначається до певного VLAN. Динамічні VLAN формуються автоматично за заданими критеріями: на основі MAC-адреси пристрою, IP-підмережі чи мережевого протоколу.

По способу формування VLAN описують:

- На основі групування портів
- На основі групування MAC-адрес
- На основі інформації 3-го рівня
- На основі стандарту IEEE 802.1.Q
- На основі стандарту IEEE 802.1ad
- На основі портів та протоколів IEEE 802.1v
- Комбіновані

У практиці VLAN реалізуються в більшості на комутаторах. Кожен порт комутатора налаштовують як access або trunk. Access-порт асоціюється з одним VLAN і приймає трафік лише цього VLAN. Натомість trunk-порт може нести трафік декількох VLAN одночасно – для цього кадрам додається 802.1Q-тег з ідентифікатором VLAN. Теги розміщуються між MAC-адресами і полем типу Ethernet-кадру, що дозволяє кожному кадру знати, якому VLAN він належить. У мережі з VLAN комутатори будують власну таблицю VLAN, в якій зберігаються імена та ID віртуальних мереж. При отриманні кадру комутатор дивиться на VLAN ID і передає його тільки по тому сегменту, який відповідає цьому VLAN. Таким чином, трафік різних VLAN, хоч і проходить одним фізичним каналом, залишається логічно розділеним.

Переваги використання VLAN:

1. Ізоляція трафіку і сегментація мережі.
2. Підвищена безпека.
3. Гнучкість управління.
4. Ефективність і економія ресурсів.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

Ізоляція трафіку і сегментація мережі полягають у наступному – VLAN обмежують широкомовний трафік у межах окремої доменної трансляції, що значно зменшує надмірні широкомовні кадри в мережі.

Підвищена безпека будується на тому, що VLAN дозволяють логічно ізолювати мережеві групи на рівні канального рівня. Користувачі з різних VLAN не можуть спілкуватися між собою без маршрутизації, що ускладнює несанкціонований доступ.

Оскільки налаштування здійснюється програмно, адміністратори можуть формувати віртуальні «робочі групи» незалежно від фізичного розташування пристроїв і створюють гнучкість управління..

Використання VLAN зменшує потребу в додатковому обладнанні та кабелях: один фізичний комутатор може обслуговувати кілька сегментів VLAN, а транкові з'єднання дозволяють спільно використовувати канали зв'язку. Це також оптимізує передачу трафіку – комутатори можуть застосовувати пріоритезацію кадрів (802.1p) залежно від VLAN і забезпечувати кращу пропускну здатність для критичного трафіку, що дозволяє ефективно та економно використовувати ресурси.

У великих мережах створення та підтримка VLAN вручну на кожному комутаторі є трудомістким процесом, що збільшує ризик помилок і ускладнює адміністрування. Щоб спростити керування та забезпечити узгодженість конфігурації, використовуються протоколи автоматизації. Один із таких протоколів – VTP. VLAN Trunking Protocol – це фірмовий протокол Cisco для централізованого управління конфігурацією VLAN у межах одного домену.

VTP дозволяє створювати, змінювати та видаляти VLAN на одному центральному комутаторі, а потім автоматично поширювати ці зміни на всі комутатори домену. Коли адміністратор додає або змінює VLAN на VTP-сервері, внутрішній лічильник ревізії конфігурації збільшується. Сервер надсилає VTP-рекламації (advertisements) через канали, які проходять між комутаторами. У цих повідомленнях міститься повний опис усіх VLAN. VTP-клієнти – отримують

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

інформацію та автоматично синхронізують свої таблиці VLAN зі змінами. Таким чином забезпечується єдина узгоджена конфігурація VLAN по всій мережі.

Режими роботи VTP:

- Server (серверний режим)
- Client (клієнтський режим)
- Transparent (прозорий режим)

Серверний режим : у цьому режимі комутатор може створювати, змінювати і видаляти VLAN, а також задавати параметри VTP. Всі зміни, внесені на VTP-сервері, автоматично анонсуються іншим комутаторам домену. Сервер є режимом за замовчуванням.

Клієнтський режим: комутатори-клієнти приймають і синхронізують інформацію про VLAN, але не дозволяють локально створювати чи змінювати VLAN.

Прозорий режим: transparent-комутатор не бере активної участі у протоколі VTP. Він не приймає і не змінює свою базу VLAN за отриманими VTP-повідомленнями, але за умов VTPv2 пересилає отримані VTP-рекламації далі. У цьому режимі VLAN конфігуруються локально на самому комутаторі і не впливають на інші пристрої в домені VTP.

1.2.2 Протоколи та технології агрегування каналів

У сучасних корпоративних мережах часто виникає потреба в підвищенні пропускної здатності між ключовими вузлами, забезпеченні відмовостійкості та балансуванні навантаження. Для досягнення цих цілей використовуються технології агрегування каналів, які дозволяють об'єднувати декілька фізичних з'єднань в один логічний канал. Одним із найпоширеніших рішень у цій сфері є технологія EtherChannel, яка підтримується обладнанням Cisco та низкою інших виробників. Налаштування EtherChannel можуть бути здійснені як статично, так і динамічно, за допомогою протоколів. Агрегація каналів дозволяє розподілити трафік між фізичними портами в залежності від конфігурації.

Обмеження для агрегації каналів:

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

- Не можна об'єднувати різні типи інтерфейсів
- Кожен EtherChannel може складатися з максимум восьми сумісно налаштованих портів Ethernet.

- Конфігурація окремого порту члена групи EtherChannel повинна бути узгоджена на обох пристроях.

Що перевіряють пристрої один в одного для створення логічного каналу:

- Швидкість
- Дуплексний режим
- Стан портів (всі мають бути або в режимі транку, або доступу)
- Якщо порти в режимі доступу, то VLAN доступу
- Якщо порти в режимі транку, то список дозволених VLAN

Наразі, використовуються різні протоколи та технології, що визначають спосіб узгодження портів, метод формування логічного каналу та рівень сумісності між обладнанням. Залежно від виробника обладнання та вимог до гнучкості чи автоматизації конфігурації, застосовуються як пропрієтарні, так і відкриті рішення, найпопулярнішими є:

- PAgP (Port Aggregation Protocol).
- LACP (Link Aggregation Control Protocol).
- LAG (статичне з'єднання, Manual Link Aggregation Group).
- vPC (Virtual Port-Channel).
- Linux Bonding

PAgP: пропрієтарний протокол компанії Cisco, призначений для автоматичного формування EtherChannel шляхом обміну спеціальними пакетами між портами комутаторів. Під час роботи PAgP активні порти групуються у загальний логічний канал, а у випадку виходу з ладу одного із них автоматично активується резервний порт. Протокол узгоджує параметри кожного порту та динамічно об'єднує сумісні порти в єдиний агрегований канал. Працює тільки на пристроях Cisco або на обладнанні з ліцензією Cisco.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

LACP: відкритий протокол динамічного агрегування, визначений у стандарті IEEE 802.3ad (нині IEEE 802.1AX). Він дозволяє об'єднувати кілька фізичних портів у єдиний логічний канал за рахунок обміну LACP-кадрами між пристроями. Кожен вузол в групі LACP регулярно обмінюється інформацією про порт (priority, статус) і автоматично формує агрегат лише з однаково налаштованих та активних портів. При відмові одного лінку LACP групи, інші лінки приймають на себе навантаження без втрати зв'язку. Підтримується майже всіма виробниками мережевого обладнання.

LAG: ручне об'єднання кількох фізичних лінків в один логічний канал без використання протоколу переговорів. Адміністратор вручну створює порт-канал і додає до нього інтерфейси на обох сторонах з'єднання. У такому режимі комутатори вважають всі члени LAG активними і розподіляють між ними трафік на основі обраного алгоритму (зазвичай хешування за MAC, IP тощо). У разі відмови одного з лінків трафік автоматично переходить на інші активні лінки цього LAG. Статичне LAG є частиною стандарту IEEE 802.3ad (802.1AX) як «no-negotiate» режим, воно сумісне з будь-якими комутаторами, що підтримують Link Aggregation.

vPC: пропрієтарна технологія Cisco для комутаторів серій Nexus, що реалізує мультишасі-агрегування (Multi-Chassis EtherChannel). Вона дозволяє створювати порт-канал, фізично розподілений між двома незалежними комутаторами/ У конфігурації vPC два Nexus-комутатори незалежно керуються, проте узгоджують між собою стан портів через спеціальний «peer-link». Різнцевий пристрій бачить обидва комутатори як один логічний порт-канал, а spanning-tree вважає його одним комутатором.

Linux Bonding: у Linux-ядрі існує драйвер „bonding“, що дозволяє об'єднувати кілька мережевих інтерфейсів у єдиний віртуальний інтерфейс. Режим роботи бонду задається параметром mode, який визначає політику передачі та резервування. У режимі active-backup (mode 1) активним є тільки один інтерфейс – інші чекають у резерві. Якщо активний лінк відключається, один із резервних

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арх.
		Єфіменко А.А.				18
Змн.	Арх.	№ докум.	Підпис	Дата		

набуває статусу активного. У режимі 802.3ad (mode 4) драйвер реалізує динамічний LACP відповідно до стандарту IEEE 802.3ad (802.1AX), агрегуючи всі лінки із однаковими швидкістю та дуплексом. Існують також інші режими (round-robin, balance-xor, broadcast, balance-tlb, balance-alb) з різною логікою розподілу трафіку та резервування.

1.2.3 Маршрутизація в мережі

Маршрутизація — ключовий процес у корпоративних кампусних мережах, що забезпечує передачу даних між різними сегментами: VLAN, підмережами або віддаленими філіями. Її ефективність визначає продуктивність усієї інфраструктури. Inter-VLAN Routing є фундаментом для зв'язку між віртуальними мережами. Без нього пристрої в різних VLAN, навіть знаючи IP-адреси, не зможуть обмінюватися трафіком. Ця функція реалізується виключно пристроями третього рівня.

Найбільш використовувані технології та протоколи для маршрутизації в корпоративних кампусних мережах:

- Статична маршрутизація.
- OSPF (Open Shortest Path First).
- EIGRP (Enhanced Interior Gateway Routing Protocol).
- Маршрутизатор-на-палиці (Router-on-a-Stick)
- Маршрутизація на L3 комутаторах.

Статична маршрутизація: полягає у ручному заданні маршрутів адміністратором без використання динамічних протоколів. Для кожної підмережі в таблиці маршрутизації вказується конкретний наступний хоп чи інтерфейс. Цей підхід простий у реалізації та потребує мінімальних ресурсів, що робить його придатним для малих або стабільних мереж. Також статичні маршрути забезпечують точний контроль за шляхами передачі і меншу вразливість до зовнішніх атак.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Переваги: не створює додаткового трафіку для обміну маршрутами і практично не навантажує CPU/пам'ять пристроїв, проста конфігурація для невеликих топологій, висока безпека

Недоліки: відсутність динамічної адаптації – при зміні топології маршрути доводиться міняти вручну, що може призводити до простоїв, низька масштабованість – у великих мереж обслуговування статичних маршрутів стає громіздким і схильним до помилок.

OSPF: внутрішній протокол маршрутизації типу Link-State, що використовує алгоритм найкоротшого шляху. Кожен пристрій OSPF збирає інформацію про стан з'єднань суміжних вузлів і будує глобальну карту топології області. На основі цієї карти виконується алгоритм Дейкстри для обчислення найкращих шляхів до всіх підмереж усередині автономної системи. Мережа може бути розбита на кілька областей (areas) з метою зменшення обсягу обміну даними і прискорення конвергенції.

Переваги: швидка конвергенція і детальна відомість про топологію; добре масштабується на великі мережі завдяки ієрархічній схемі областей; підтримка ESMR (рівноцінного балансування трафіку) за однакової вартості маршрутів, відкритий стандарт, що забезпечує широке вендорне покриття.

Недоліки: вища складність налаштування і підтримки порівняно зі статичними рішеннями, значніше використання CPU та пам'яті, на малих мережах може бути надмірно громіздким і непотрібним; обмін станом посилянь під час ініціалізації чи збоїв може створювати пікове навантаження.

EIGRP: це «гібридний» протокол маршрутизації Cisco, що поєднує переваги векторного і станового підходів. Він використовує алгоритм DUAL (Diffused Update Algorithm) для швидкого пошуку альтернативних безпетельних маршрутів при збоях. Маршрутизатори EIGRP обмінюються лише необхідними оновленнями замість періодичних повних таблиць, що знижує мережеве навантаження. EIGRP використовує складну метрику, що включає пропускну здатність і затримку лінків

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

(за замовчуванням), а також підтримує балансування із різною вартістю (variance) між кількома маршрутами.

Переваги: дуже швидка конвергенція і мінімальні оновлення – оновлення надсилаються тільки при зміні мережі, крім регулярних hello-пакетів, висока масштабованість у добре спроектованих мережах, можливість мультипוטного балансування з нерівною.

Недоліки: підтримка є обмеженою на не-Cisco обладнанні. На відміну від OSPF, EIGRP не має стандартних областей, що ускладнює проектування надвеликих мереж без додаткової агрегації.

Маршрутизатор-на-палиці: спосіб організації маршрутизації між VLAN за допомогою одного фізичного інтерфейсу роутера з кількома логічними підінтерфейсами. Кожен підінтерфейс налаштований на певний VLAN і отримує IP-адресу цієї підмережі. З'єднання між комутатором і роутером налаштовується як транковий порт із VLAN-тегуванням (802.1Q), тому весь трафік від різних VLAN надходить на один фізичний інтерфейс, а роутер розрізняє пакети за їх тегом і маршрутизує між VLAN.

Переваги: спрощує організацію інтер-VLAN маршрутизації на малих мережах, бо достатньо одного роутера та одного кабеля, економія обладнання, простота конфігурації, доцільний в малих мережах.

Недоліки: вся маршрутизація між VLAN відбувається через один фізичний канал, тому при великому обсязі трафіку цей інтерфейс може стати вузьким місцем, технологія мало придатна для великих мереж з багатьма VLAN – вона не забезпечує високу масштабованість.

Маршрутизація на L3 комутаторах є сучасним методом реалізації апаратного рівня 3 у комутаторах, що дозволяє їм виконувати функції маршрутизації на швидкості лінії без залучення зовнішніх маршрутизаторів. Замість програмної обробки, спеціалізовані мікросхеми швидко обробляють IP-пакети між підмережами. Ключовим інструментом є SVI (Switched Virtual Interfaces) –

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

віртуальні інтерфейси для кожного VLAN, які виступають шлюзом для пристроїв у своїй мережі.

Переваги: найвища продуктивність та низькі затримки завдяки апаратному прискоренню маршрутизації, що критично для трафікоємних середовищ.

Недоліки: L3-комутатори з апаратним прискоренням дорожчі за звичайні L2-моделі. Складніше налаштування та супровід порівняно з базовою комутацією. У дуже великих мережах може вимагати додаткового планування для оптимізації таблиць маршрутизації.

1.2.4. Принципи та протоколи резервування зв'язків у мережах ethernet.

У мережах Ethernet критично важливим є забезпечення надійності та відмовостійкості через резервування фізичних зв'язків, однак надлишкові шляхи створюють ризик виникнення небезпечних петель, що призводить до широкомовних штормів, деградації продуктивності або повного колапсу мережі. Для вирішення цієї суттєвої проблеми було розроблено сімейство протоколів Spanning Tree, які динамічно блокують надлишкові зв'язки, формуючи безпетельну топологію, але зберігають їх у резерві для миттєвого відновлення при збоях. Цей механізм став фундаментом для побудови стійких корпоративних інфраструктур, що поєднують надійність з ефективним використанням ресурсів.

Spanning Tree Protocol – мережний протокол запобігання петлям, який підтримує резервування при створенні топології другого рівня без зациклення. Протокол STP досягає своєї основної мети шляхом моніторингу мережі для відстеження всіх зв'язків і вимикає надлишкові з них. STP використовує алгоритм основного дерева (STA), щоб спочатку створити бази даних топології, а потім для пошуку і відключення надлишкових каналів. Коли STP працює, кадри пересилатимуться лише за найкращими, обраними STP каналами.

Для створення топології без зациклення проводяться наступні дії:

1. Обрання кореневого моста.
2. Обрання кореневих портів.
3. Обрання призначених портів.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Обрання альтернативних портів.

Порти комутатора з підтримкою IEEE 802.1d STP можуть переходити через п'ять різних станів:

- Вимкнений.
- Заблокований.
- Прослуховування.
- Навчання.
- Переадресація.

Вимкнений порт в адміністративно вимкненому стані не бере участі у пересиланні кадрів або STP. Порт у відключеному стані практично не працює.

Заблокований порт не буде пересилати кадри. Мета блокування - запобігти створенню петель. Всі порти перебувають у стані блокування за замовчуванням, коли комутатор увімкнено.

Порт в стані прослуховування вивчає BPDU, щоб переконатися, що в мережі немає петель, перш ніж передати кадри даних, готується до пересилання кадрів даних не заповнюючи таблицю MAC-адрес.

Порт в режимі навчання вивчає BPDU і всі шляхи в комутованій мережі. Заповнює таблицю MAC-адрес, але все ще не пересилає кадри даних.

Стан переадресації: надсилає і приймає всі кадри даних на мостовому порту. Якщо порт залишається призначеним або кореневим портом наприкінці стану навчання, він перейде у стан переадресації. Порт переадресації, як правило, є тим, який має найнижчу вартість для кореневого мосту.

Після того, як комутатор визначає найкращий шлях до кореневого моста для свого кореневого порту і всіх призначених портів, всі інші, резервні порти переходять в режим блокування. Якщо комутатор визначає, що заблокований порт повинен стати призначеним або кореневим портом через зміну топології, він перейде в режим прослуховування і перевірить всі отримані BPDU щоб переконатися, що після переходу порту в режим переадресації не виникне петля.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				23
Змн.	Арк.	№ докum.	Підпис	Дата		

Різновиди протоколів єднального дерева

Протокол	Опис
STP	Це оригінальна версія IEEE 802.1D, яка створює топологію без петель у мережі з надлишковими з'єднаннями. Також має назву Common Spanning Tree (CST), оскільки передбачає створення єдиного спільного екземпляру єднального дерева для всієї комутованої мережі, незалежно від кількості VLAN.
PVST+	Єднальне дерево на основі VLAN (Per-VLAN Spanning Tree)— це створена Cisco вдосконалена версія STP, яка визначає окремий екземпляр єднального дерева 802.1D для кожної VLAN, налаштованої у мережі. PVST+ підтримує PortFast, UplinkFast, BackboneFast, захист BPDU, фільтр BPDU, захист кореня і захист від петель.
802.1D-2004	Це оновлена версія стандарту STP, що містить IEEE 802.1w.
RSTP	Протокол швидкого єднального дерева (Rapid Spanning Tree Protocol) або IEEE 802.1w є вдосконаленою версією STP, що забезпечує швидшу збіжність.
Rapid PVST+	Це покращена система RSTP, запропонована Cisco, яка використовує PVST+ і забезпечує окремий екземпляр 802.1w для кожної VLAN. Кожен окремий екземпляр підтримує PortFast, захист BPDU, фільтр BPDU, захист кореня і захист від петель.
MSTP	Протокол множинного єднального дерева (Multiple Spanning Tree Protocol) - це стандарт IEEE, натхненний ранньою фірмовою версією протоколу, Multiple Instance STP (MISTP), розробленого Cisco. MSTP поєднує декілька VLAN у одному екземплярі єднального дерева.
MST	Множинне єднальне дерево (Multiple Spanning Tree) — це реалізація MSTP компанії Cisco, яка надає до 16 екземплярів RSTP і поєднує декілька VLAN з однаковою фізичною і логічною топологією у спільному екземплярі RSTP. Кожен екземпляр підтримує PortFast, захист BPDU, фільтр BPDU, захист кореня і захист від петель.

1.3 Технології та протоколи захисту кампусної корпоративної мережі

З розвитком цифрових технологій та ускладненням мережевої інфраструктури, корпоративні мережі стали об'єктом постійної уваги з боку кіберзлочинців. Відкритість до Інтернету, велика кількість підключених пристроїв, мобільних користувачів і хмарних сервісів створюють численні вектори атак. Надійний захист потребує комплексного підходу, що включає як превентивні, так і реактивні заходи безпеки. Для цього застосовуються різноманітні технології, від класичних міжмережевих екранів до розподілених систем виявлення загроз, контролю доступу, шифрування та моніторингу подій..

1.3.1 Міжмережеві екрани

Міжмережеві екрани (Firewalls): це апаратний або програмний засіб, що фільтрує трафік між різними сегментами мережі відповідно до заданих правил безпеки. Його призначення – блокувати несанкціонований доступ і захищати внутрішню мережу від потенційних загроз, пропускаючи тільки безпечні з'єднання. Фаєрволі зазвичай працюють на мережевому (3-му) і транспортному (4-му) рівнях моделі OSI, аналізуючи IP-адреси, порти та інші поля заголовків пакетів. Більш просунуті рішення здійснюють детальний аналіз трафіку до 7-го рівня, контролюючи сам вміст протоколів HTTP, DNS тощо. Принцип роботи фаєрволу базується на наборі правил. Кожен вхідний або вихідний пакет послідовно порівнюється з цими правилами: якщо він задовольняє умову, то пропускається, інакше – блокується. Існують два основні підходи до обробки трафіку: «default allow», або «default deny». Більшість фаєрволів також забезпечує функції трансляції адрес (NAT) та аудиту подій.

За способом роботи виокремлюють наступні міжмережеві екрани:

- Пакетні (статичні).
- Стейтфул (динамічні).
- Проксі-фаєрволи (застосункові шлюзи).
- Next-Generation Firewall (NGFW).

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				25
Змн.	Арк.	№ докum.	Підпис	Дата		

Пакетний фаєрвол на рівні IP-фільтрації аналізує кожен пакет за адресами та портами без урахування стану з'єднання.

Стейтфул фаєрвол зберігає стан кожного з'єднання, він аналізує не тільки заголовки, а й логіку протоколі.

Проксі-фаєрволи: пакети від клієнтів обробляє проміжний сервер, який розгортає з'єднання з зовнішніми серверами від свого імені. Завдяки глибокій перевірці трафіку вони розуміють контент протоколів і можуть блокувати небажані команди чи зловмисні дані всередині пакету. Головний недолік – затримки й високе навантаження на ресурс пристрою.

Next-Generation Firewall поєднують класичну перевірку на мережевому рівні зі вбудованим системами виявлення вразливостей і фільтрацією контенту. Вони використовують бази загроз і поведінковий аналіз, аби коректно інтерпретувати трафік на рівні додатків.

Переваги міжмережевих екранів: здійснюють гнучкий контроль і фільтрацію трафіку за IP, портами та протоколами. Стейтфул-аналіз дозволяє допускати лише легітимні потоки даних і блокувати небезпечні. Прості у розгортанні та управлінні; широковідомі та надійні технології.

Обмеження: вразливі для зашифрованого трафіку, а також не бачать поведінку атак, що відбуваються всередині довірчої зони. Можуть стати вузьким місцем за великих обсягів трафіку або комплексних правил, потребують ретельної настройки політик безпеки. Статичні фільтри (stateless) не відстежують зв'язок пакетів, тому більш вразливі до деяких видів атак.

1.3.2 IDS/IPS системи

Системи виявлення та запобігання вторгненням призначені для виявлення аномальної або шкідливої активності в мережі чи на окремих пристроях. IDS аналізує мережевий трафік або системні логи і повідомляє про підозрілі події. IPS за потреби може самостійно блокувати або розривати небезпечні з'єднання та запобігати атакам в режимі реального часу. У сучасних рішеннях часто об'єднують функції IDS і IPS в одному комплексі (IDPS). Методи виявлення бувають

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

сигнатурними та евристичними. Сигнатурний аналіз порівнює фрагменти трафіку з базою відомих шаблонів. Він ефективний для відомих атак і має відносно низький рівень хибних спрацювань, але не може розпізнати нові або модифіковані загрози без оновлення бази. Евристичний аналіз використовує статистичні моделі чи машинне навчання, щоб визначати відхилення від звичайної поведінки мережі чи системи. Це дозволяє знаходити невідомі атаки, проте збільшує кількість хибнопозитивних спрацювань та вимагає складної настройки. Системи IDS/IPS поділяються за місцем розташування на:

- Мережеві IDS/IPS (NIDS/NIPS)
- Хостові IDS/IPS (HIDS/HIPS)

Мережеві встановлюються на ключових вузлах мережі і аналізують весь трафік, що через нього проходить.

Хостові працюють на окремому сервері або робочій станції. Вони перевіряють внутрішній стан системи (журнали подій, цілісність файлів, системні виклики тощо) і виявляють локальні вторгнення.

Переваги: допомагають виявити відомі загрози та аномальні дії, що можуть пройти крізь звичайні фаєрволи. Сигнатурна перевірка точна для відомих шаблонів атак, а поведінковий аналіз здатен розпізнавати нові варіанти атак. IDS забезпечують раннє сповіщення про проникнення, а IPS, у свою чергу, дозволяють негайно реагувати, блокуючи атаки.

Обмеження: чутливі до хибних спрацювань, особливо при недостатній адаптації під конкретну мережу. Сигнатурні методи не виявлять нові або модифіковані атаки без своєчасного оновлення баз. IPS вимагає, щоб трафік проходив через нього всередині – через це система може стати точкою відмови, а також існує ризик помилкового блокування легітимного трафіку. Не аналізують зашифрований трафік без його попереднього розшифрування.

1.3.3 Захист від DDoS-атак

У сучасних умовах, небезпеку для корпоративних мереж становлять DDoS-атаки. Цей тип атаки спрямований на виведення з ладу критичних сервісів шляхом

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

перевантаження систем надмірним трафіком із численних джерел. Подібні атаки можуть призвести до повної недоступності ресурсів, фінансових втрат і порушення бізнес-процесів.

Оборона від такого типу атак використовує комбінацію виявлення аномалій і заходів пом'якшення атак.

Методи виявлення атак: системи мережевого моніторингу встановлюють порогові значення нормального трафіку, якщо спостерігається раптовий сплеск вхідних з'єднань або величезний обсяг пакетів, може спрацювати сигнал тривоги. Використовують також методи аналізу патернів та співставлення з відомими шаблонами DDoS. Сучасні рішення можуть використовувати машинне навчання, щоб розрізнити легітимний піковий трафік від атаки.

Методи пом'якшення: при виявленні DDoS-атаки є декілька практичних підходів:

- Rate limiting (обмеження швидкості).
- Чорна діра (blackholing).

При використанні rate limiting, мережеві пристрої накладають ліміти на нові з'єднання, або пакети з одного джерела/групи пакетів.

При застосуванні методу blackholing, у екстремальному випадку вся підозріла атака перенаправляється в «чорну діру», тобто вона не доходить до сервера. Цей метод зрізує і легітимний, і зловмисний трафік, але зберігає працездатність внутрішньої мережі.

1.3.4 DHCP snooping

У корпоративних мережах, особливо з великою кількістю кінцевих пристроїв, критично важливо забезпечити захист від атак, пов'язаних із піддробкою мережевих служб. Одним із поширених векторів таких атак є несанкціоноване розгортання зловмисного DHCP-сервера, який може роздавати фальшиві IP-адреси та перенаправляти трафік через шкідливі вузли. DHCP snooping – це функція безпеки, що призначена для запобігання піддробленим DHCP-серверам у мережі. Коли вона увімкнена, пристрій відслідковує DHCP-повідомлення між клієнтами й

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

серверами. Адміністратор позначає певні порти як довірені. Усі інші порти вважаються недовіреними. Якщо комутатор отримує DHCP-відповідь на невідповідному порту, він її просто ігнорує. Таким чином, зловмисний DHCP-сервер, підключений до непозначеного порту, не зможе роздавати IP-адреси клієнтам, при цьому будується таблиця зв'язків, куди заносить інформацію про IP-адресу, MAC-адресу, VLAN і номер порту кожного клієнта на основі успішних DHCP-угод. Цю таблицю потім використовують для інших механізмів захисту.

1.3.5 Dynamic ARP inspection

Dynamic ARP Inspection (DAI) – це механізм на комутаторах, який перевіряє коректність ARP-повідомлень у мережі для захисту від спуфінгу ARP. Його завдання упевнитися, що ARP-відповіді містять правильне поєднання IP- і MAC-адрес. Коли DAI активовано, комутатор інтерцептує всі ARP-запити й відповіді на недовірених портах. Він порівнює отриману пару IP–MAC з binding table, створеною за допомогою DHCP snooping. Якщо вхідний ARP-пакет не співпадає з відомою відповідністю з таблиці, комутатор викидає цей пакет. Комбінація DHCP snooping + DAI є ключовою: перший створює авторитетну таблицю зв'язків, а другий використовує її для перевірки ARP.

1.3.6 Port Security

Одним із ефективних засобів запобігання несанкціонованим підключенням до мережі через комутатори є використання механізму Port Security. Функція Port Security на комутаторі дозволяє контролювати доступ до конкретного порту за MAC-адресами кінцевих пристроїв. Якщо на порті виявляється кадр з незареєстрованою або надлишком адрес, комутатор виконує попередньо визначену дію:

- Protect (захист).
- Restrict (обмеження).
- Shutdown (відключення).

Protect – просто відкидає кадр з незнайомою MAC-адресою без додаткових наслідків.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

Restrict – відкидає кадр та фіксує це як подію в логах (може генерувати сповіщення).

Shutdown – перемикає порт у неактивний стан (errdisable). Щоб відновити роботу порту, потрібне втручання адміністратора або таймаут.

Цей механізм ефективно обмежує кількість пристроїв, що можуть підключатися до одного фізичного порту. З його допомогою можна припинити несанкціоноване підключення стороннього обладнання, а також захиститися від атаки MAC flooding. У разі переповнення перемикання портів за заданими правилами запобігає широку трансляцію кадрів по всій мережі.

1.3.7 Контроль доступу на рівні мережі

Контроль доступу на рівні мережі (802.1X, NAC) – це підхід до безпеки, який вимагає автентифікації пристроїв і користувачів перед наданням їм повного мережевого доступу. 802.1X – стандарт IEEE для портової автентифікації: коли комп'ютер підключається до порту комутатора, або до бездротової точки доступу, порт блокується і не пропускає звичайний трафік, поки пристрій не пройде аутентифікацію за допомогою протоколу EAP.

Механізм роботи: клієнт надсилає свої облікові дані на пристрій, той передає інформацію на сервер. Якщо сервер підтверджує авторизацію, порт «відмикається» і користувач отримує мережевий доступ у відповідну VLAN. Якщо аутентифікацію не пройдено, порт залишається заблокованим або переводиться до ізольованої VLAN з обмеженим доступом. NAC-рішення можуть також включати перевірку конфігурації пристрою – чи оновлено антивірус, чи є необхідні патчі ОС. При невідповідності політикам пристрій ізолюється або взагалі не підключається.

1.3.8 MACsec

MACsec (802.1AE) – технологія захисту канального рівня Ethernet. Вона забезпечує шифрування та автентифікацію кадрів безпосередньо на рівні канального з'єднання між двома пристроями. Портам MACsec-пристроїв призначаються симетричні ключі шифрування за допомогою протоколу MACsec Key Agreement. Потім кожен Ethernet-кадр, що передається між цими пристроями,

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

шифрується з використанням AES та матиме на собі теги аутентифікації і цілісності.

1.3.9 Контроль доступу на основі політик/списків/контролю доступу

Контроль доступу є системою керівних принципів, що визначає взаємодії користувачів, пристроїв та сервісів з мережними ресурсами. У сучасних інфраструктурах цей механізм перетворюється на бар'єр проти несанкціонованих операцій, забезпечуючи відповідність політикам безпеки та регуляторним вимогам.

Контроль доступу на основі списків (ACL) – це набір правил, що визначають, які пакети мережевого трафіку слід пропускати або блокувати. Правила ACL використовуються у мережевому обладнанні і на серверах, ОС. Кожне правило містить умови та дію. Пакети перевіряються за списком зверху вниз, і діє правило, яке спрацювало першим. ACL дозволяє реалізувати базові політики безпеки.

RBAC (Role-Based Access Control, контроль доступу за ролями) – модель доступу, де кожному користувачу присвоєно одну або кілька ролей, а роль у свою чергу визначає набір прав і дозволів.

1.3.10 Zero trust architecture

Архітектура з нульовою довірою – концепція побудови безпеки мережі на принципі «нікому і нічому не довіряй за замовчуванням». На відміну від традиційної моделі з чітким периметром, ZTA вимагає автентифікації й авторизації для кожного запиту, незалежно від того, де перебуває користувач або пристрій.

Основні принципи ZTA:

- Мінімальні привілеї.
- Мікросегментація.
- Безперервна автентифікація.
- Моніторинг та логування.

Мінімальні привілеї полягають в тому, що кожному об'єкту дається тільки необхідний мінімум прав доступу до ресурсів.

Принцип мікросегментації: мережа поділена на дрібні контрольовані зони, між якими трафік проходить через фаєрволи або політики безпеки.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Безперервна автентифікація досягається тим, що доступ перевіряється не одноразово, а динамічно, наприклад із використанням багатофакторної автентифікації, аналізу контексту та поведінки користувача.

Постійний аналіз подій безпеки для виявлення відхилень чи потенційно компрометованих пристроїв забезпечують моніторинг та логування.

1.3.11 SIEM

SIEM (Security Information and Event Management) – це система, яка централізовано збирає та аналізує логи й події безпеки з усіх компонентів ІТ-інфраструктури. Метою SIEM є кореляція розрізнених подій для своєчасного виявлення складних атак і підтримка процесу реагування на інциденти. SIEM-консоль підключається до різних джерел подій та отримує їх у реальному часі або пакетами, потім вона нормалізує формати і застосовує аналітичні правила. При виявленні патерна, що відповідає відомим загрозам, система генерує оповіщення для адміністратора.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

1.4 Сервіси та протоколи забезпечення підтримки роботи користувачів кампусної корпоративної мережі

Ефективне функціонування кампусної корпоративної мережі неможливе без надійного сервісного забезпечення, яке дозволяє користувачам безперешкодно виконувати повсякденні задачі. Побудова мережі лише на фізичному рівні та рівні безпеки не гарантує її придатності для реального використання в умовах багатокористувацького середовища. Для стабільної та зручної роботи необхідне впровадження мережових сервісів, що забезпечують автентифікацію користувачів, доступ до електронної пошти, обмін файлами, роботу з вебресурсами, тощо. Такі сервіси відіграють ключову роль у забезпеченні доступності, зручності, безпеки та надійності інформаційної взаємодії в межах організації, сприяючи ефективній роботі користувачів незалежно від їхнього розташування в мережі.

1.4.1. AAA

Модель AAA («Authentication, Authorization, Accounting») описує три основні функції контролю доступу в ІТ: автентифікацію, авторизацію та облік. Вона використовується для централізованого керування мережею та іншими ресурсами, а також для реєстрації дій користувачів. AAA-сервери зазвичай реалізовані за клієнт-серверною схемою: клієнт приймає запит від користувача, а сервер перевіряє облікові дані, видає права доступу і фіксує діяльність. Такий підхід забезпечує масштабованість і централізоване адміністрування користувачів та політик доступу у великих мережах.

Основні складові AAA:

- Аутентифікація (Authentication).
- Авторизація (Authorization).
- Облік (Accounting).

Аутентифікація здійснюється у перевірці особи користувача або пристрою, що намагається підключитися до мережі. На цьому етапі система порівнює надані облікові дані з інформацією у базі AAA-сервера. У разі успішної автентифікації встановлюється особа користувача.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

Авторизація після автентифікації визначає, які саме ресурси та сервіси мережі доступні користувачу. Наприклад, перевіряються його права та налаштовуються VLAN, групи доступу, діапазони IP, привілеї на обладнанні тощо.

Облік полягає у фіксації та моніторингу діяльності користувача в мережі. Під час обліку записуються різні події: час підключення/відключення, обсяг переданих даних, використані сервіси та команди. Ці дані використовуються для аудитів безпеки, розрахунку трафіку чи оплати послуг і допомагають відстежувати витрати мережевих ресурсів.

Кампусні мережі часто використовують AAA для управління доступом до Wi-Fi (через WPA2/WPA3-Enterprise і RADIUS-сервер) та дротового комутованого доступу (802.1X/EAP з RADIUS). В цілому, AAA дозволяє зробити політику безпеки динамічною, замість статичного налаштування доступу, адміністратори можуть централізовано змінювати облікові дані й права у сервері, а не оновлювати кожен пристрій локально.

Поширені протоколи та технології AAA:

- RADIUS (Remote Authentication Dial-In User Service)
- TACACS+ (Terminal Access Controller Access-Control System Plus)

RADIUS – це відкритий стандартний протокол AAA, який підтримується багатьма виробниками мережевого обладнання. RADIUS реалізовано за клієнт-серверною моделлю: пристрій виступає AAA-клієнтом, а спеціальний сервер виконує аутентифікацію, авторизацію та облік. RADIUS визначено у RFC 2865/2866, і він поєднує процедури аутентифікації й авторизації в одному потоці, тоді як інформація обліку передається окремими повідомленнями. RADIUS використовує UDP, що спрощує реалізацію та дозволяє широке використання, але вимагає додаткових заходів надійності для передачі даних.

TACACS+ – це пропрієтарний протокол AAA, розроблений компанією Cisco, який використовують переважно для аутентифікації та авторизації доступу до мережевого обладнання. На відміну від RADIUS, TACACS+ передбачає використання TCP для більш надійного з'єднання та шифрує вміст усіх

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

повідомлень. TACACS+ дозволяє розділяти процеси автентифікації, авторизації та обліку, він підтримує гнучке керування привілеями на командному рівні. Наразі TACACS+ використовується переважно в обладнанні Cisco, хоча є сумісні варіанти від інших вендорів.

Порівняння RADIUS та TACACS+:

Архітектура: TACACS+ чітко розділяє функції автентифікації, авторизації й обліку, що надає більшу гнучкість і модульність реалізації сервера захисту. RADIUS об'єднує автентифікацію та авторизацію в одному процесі, а облік виконується окремо.

Транспортування: RADIUS передає повідомлення через UDP, що забезпечує простішу імплементацію, але потребує механізмів повторної передачі для надійності. TACACS+ працює поверх TCP, що забезпечує надійніший зв'язок та управління помилками.

Шифрування і безпека: TACACS+ шифрує весь вміст пакетів AAA, а не лише пароль як у RADIUS. Це робить TACACS+ більш стійким до прослуховування і маніпуляцій. Окрім того, TACACS+ передбачає розширену підтримку для аутентифікації команд адміністраторів.

Сфера застосування: RADIUS є відкритим стандартом, підтримується широким колом виробників і тому добре підходить для загального доступу користувачів до мережі. TACACS+ оптимізований для управління доступом до мережевого обладнання та надання гнучких привілеїв адміністраторським діям. Вибір протоколу залежить від конкретних вимог мережевої інфраструктури та політик безпеки.

1.4.2. DHCP

DHCP (Dynamic Host Configuration Protocol) – це протокол мережевого рівня, призначений для автоматичного призначення IP-адрес та інших конфігураційних параметрів пристроям, при їх підключенні до мережі. Він працює за клієнт-серверною моделлю, використовуючи UDP. Основне призначення – спрощення адміністрування мережі шляхом усунення необхідності ручного налаштування IP-

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				35
Змн.	Арк.	№ докum.	Підпис	Дата		

адрес на кожному клієнті. Процес отримання адреси (лізинг) складається з чотирьох етапів (DORA): широкомовний запит клієнта на пошук сервера (DHCPDISCOVER), пропозиція параметрів від сервера (DHCPOFFER), запит клієнта на використання запропонованої адреси (DHCPREQUEST) та підтвердження від сервера (DHCPACK). Адреса видається на обмежений час, який можна продовжити.

1.4.3. DNS

DNS (Domain Name System) - це глобальна, розподілена, ієрархічна система, її основне завдання – перетворення зручних для людини доменних імен на відповідні числові IP-адреси, необхідні для маршрутизації трафіку між пристроями. Система працює за принципом розподіленої бази даних, організованої у вигляді дерева доменів. Запити обробляються рекурсивно або ітеративно через ланцюжок серверів. Результати кешуються на певний час для зменшення навантаження та прискорення подальших запитів. DNS є фундаментом для зручного доступу користувачів кампусу до внутрішніх та зовнішніх мережевих ресурсів.

1.4.4. Поштові протоколи

Електронна пошта залишається одним із засобів ділової комунікації в корпоративному середовищі. Для забезпечення її стабільної роботи, доставки повідомлень, доступу до поштових скриньок і синхронізації листування використовуються спеціалізовані мережеві протоколи прикладного рівня. Вони визначають, яким чином повідомлення передаються від відправника до одержувача, як зберігаються на поштових серверах і як до них отримується доступ з клієнтських пристроїв.

Серед основних протоколів, що забезпечують роботу поштової системи, можна виділити:

- SMTP (Simple Mail Transfer Protocol).
- IMAP (Internet Message Access Protocol).
- POP3 (Post Office Protocol version 3).

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

SMTP: основний протокол для відправлення електронної пошти. Він визначає правила передачі повідомлень між поштовими клієнтами та поштовими серверами, а також між самими серверами МТА. SMTP працює поверх TCP. Процес відправки включає встановлення з'єднання, аутентифікацію, вказівку відправника, одержувача та передачу самого повідомлення. Для знаходження сервера отримувача використовуються записи типу MX у DNS. SMTP відповідає лише за доставку повідомлення на поштовий сервер отримувача, але не за доступ користувача до його скриньки.

IMAP: протокол для доступу та управління електронною поштою, що зберігається на сервері. Основна перевага IMAP – синхронізація стану скриньки між усіма пристроями клієнта. Клієнт завантажує заголовки повідомлень при підключенні, а самі тіла листів – лише за вимогою. Усі операції відбуваються безпосередньо на сервері. IMAP працює з TCP. Він ідеально підходить для користувачів, які працюють з поштою з кількох пристроїв.

POP3: протокол для завантаження електронної пошти з сервера на локальний пристрій клієнта. Типова поведінка – повідомлення видаляються з сервера після успішного завантаження. Налаштування дозволяють залишати копії на сервері, але POP3 не підтримує синхронізацію стану скриньки між різними клієнтами. Працює на TCP. POP3 простіший у реалізації та менш навантажує сервер, але менш зручний для багатопристроєвого доступу порівняно з IMAP.

Таблиця 1.3

Порівняння поштових протоколів для отримання/відправлення

Критерій	SMTP	IMAP	POP3
1	2	3	4
Призначення	Відправлення пошти між серверами/клієнтом та сервером	Доступ до пошти на сервері, синхронізація	Завантаження пошти з сервера на локальний пристрій
Робота зі скринькою	-	Повна синхронізація стану	Локальне керування

Продовження табл. 1.3

1	2	3	4
Зберігання	-	Пошта залишається на сервері	Пошта зазвичай видаляється з сервера після завантаження
Підхід для кілької пристроїв	-	+	-
Порти за замовчуванням	25,587,465	143, 993	110, 995
Безпека	Вимагає TLS для захисту даних	Вимагає TLS для захисту даних	Вимагає TLS для захисту даних
Переваги	Стандарт для відправки, сумісність	Синхронізація, централізоване зберігання, доступ з будь-якого пристрою	Простота, менше навантаження на сервер, підходить для одного пристрою
Недоліки	Лише для відправки	Вище навантаження на сервер, складніше налаштування	Не підходить для кількох пристроїв, ризик втрати даних при локальних збоях

1.4.5. HTTP/HTTPS

У сучасних комп'ютерних мережах протоколи HTTP та HTTPS відіграють фундаментальну роль у доступі до веб-ресурсів і взаємодії між клієнтами та серверами. Саме через ці протоколи здійснюється переважна більшість обміну інформацією в Інтернеті, перегляд вебсторінок, обробка форм, передача API-запитів, тощо.

HTTP – це основний протокол прикладного рівня для передачі даних у всесвітній павутині. Він визначає формат та обмін повідомленнями між клієнтами та серверами для отримання веб-ресурсів. HTTP є безстановним протоколом, що працює поверх TCP. Клієнт формує HTTP-запит і відправляє його на сервер, той обробляє запит і повертає HTTP-відповідь, що містить код статусу, заголовки та тіло відповіді. HTTP/1.1 ввів механізм постійних з'єднань, HTTP/2 додав

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арх.
		Єфіменко А.А.				38
Змн.	Арх.	№ док.м.	Підпис	Дата		

мультиплексування, а HTTP/3 використовує QUIC поверх UDP для покращення продуктивності.

HTTPS – безпечна версія HTTP, що реалізує шифрування та аутентифікацію за допомогою протоколу TLS. Весь обмін даними між клієнтом і сервером шифрується, що захищає конфіденційність та цілісність даних, а також дозволяє клієнту перевірити справжність сервера за допомогою цифрового сертифіката. HTTPS працює також з TCP, на порту 443. Процес починається з TLS-рукопотискання, під час якого узгоджуються криптографічні параметри та аутентифікується сервер, перш ніж починається передача зашифрованих HTTP-даних.

1.4.6. Протоколи файлового обміну

У корпоративному середовищі, користувачі постійно працюють із файлами, документами, звітами та іншими цифровими ресурсами, які часто зберігаються централізовано на серверних платформах. Для ефективного, безпечного та зручного доступу до цих даних необхідно використовувати протоколи файлового обміну. Вони забезпечують можливість перегляду, передачі, збереження та синхронізації файлів між пристроями користувачів і мережевими сховищами. Різні протоколи орієнтовані на конкретні операційні системи, рівень безпеки, продуктивність та зручність використання.

Найпопулярніші рішення для файлового обміну:

- SMB/CIFS (Server Message Block / Common Internet File System).
- NFS (Network File System).
- FTP (File Transfer Protocol).
- SFTP (SSH File Transfer Protocol).
- FTPS (FTP Secure).

SMB/CIFS: основний протокол для спільного доступу до файлів, принтерів та інших ресурсів у середовищах Windows. SMB забезпечує прозорий доступ до

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

віддалених файлів і папок, з підтримкою аутентифікації, списків контролю доступу та шифрування. CIFS – це застаріла реалізація/діалект SMB.

NFS: стандартний протокол для спільного доступу до файлів у середовищах Unix/Linux. Дозволяє серверам "експортувати" директорії, а клієнтам – "монтувати" їх у свою локальну файлову систему. NFSv4 працює поверх підтримує станність та кращу інтеграцію з фаєрволами та безпекою. Забезпечує високу продуктивність у однорідному Unix/Linux середовищі.

FTP: використовується для передачі файлів між клієнтом та сервером. Застосовує окремі з'єднання для керування та даних. Головні недоліки – передача даних у відкритому вигляді та складність налаштування через використання динамічних портів для даних.

SFTP: не є розширенням FTP. Окремий протокол, який використовує захищений канал SSH для безпечної передачі файлів та виконання файлових операцій. Усі дані шифруються.

FTPS: розширення FTP, що додає підтримку шифрування за допомогою TLS/SSL. Може працювати у явному або неявному режимі. Усюди шифрує керуюче з'єднання та з'єднання даних. Успадковує складність FTP з динамічними портами даних.

Таблиця 1.4

Порівняння протоколів файлового обміну

Критерій	SMB/CIFS	NFS	FTP	SFTP	FTPS
1	2	3	4	5	6
Призначення	Спільний доступ до файлів/принтерів у середовищах Windows	Спільний доступ у Unix/Linux - середовищах	Передача файлів між клієнтом і сервером	Безпечна передача файлів через SSH	FTP із шифруванням через TLS/SSL
Безпека	Аутентифікація через Active Directory, шифрування (SMB3)	Аутентифікація Kerberos (NFSv4), ACL	Дані та паролі у відкритому вигляді	Шифрування трафіку (SSH), перевірка сертифікатів	Шифрування TLS/SSL, сертифікати X.509

1	2	3	4	5	6
Швидкість	Висока у локальних мережах; чутлива до затримок	Висока для дрібних файлів у Unix-середовищі	Середня; обмежена TCP-накладними витратами	Середня	Середня; високі накладні витрати TLS
Платформи	Підтримка Windows; Samba для Linux	Підтримка Unix/Linux ; клієнти для Windows	Крос-платформний	Крос-платформний	Крос-платформний
Типове застосування	Корпоративні файлові сервери, мережеві диски	Домашні каталоги в комп'ютерних класах, наукові дані	Публічні сховища	Адміністративні задачі, передача конфіденційних даних	Бізнес-обмін із вимогами шифрування

Висновок до 1 розділу: проаналізовано принципи побудови корпоративних мереж, технології сегментації, агрегації каналів, маршрутизації, механізми безпеки та сервіси підтримки. Встановлено, що комбінація ієрархічної моделі з технологіями Cisco забезпечує масштабованість, відмовостійкість і захист від сучасних загроз.

РОЗДІЛ 2 ПРОЕКТУВАННЯ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1 Проектування топології мережі

Спроектована мережа буде реалізована відповідно до трирівневої ієрархічної моделі Cisco, яка передбачає розділення інфраструктури на рівні доступу, розподілу та ядра. Такий підхід дозволяє досягти високої масштабованості, керованості та відмовостійкості. Архітектура мережі враховує критично важливі аспекти корпоративної інфраструктури: резервування каналів, балансування трафіку, ізоляцію сегментів.

– Core Layer (MLS1, MLS2, MLS3) – забезпечує швидке транзитне з'єднання між розподільчими вузлами та шлюзами до Інтернету (R1, R2), що гарантує високу швидкодію і надійність.

– Distribution Layer (MLS4–MLS7) – здійснює маршрутизацію між VLAN, застосовує фільтрацію доступу (ACL), реалізує політики безпеки та якості обслуговування (QoS).

– Access Layer (SW1–SW7) – підключає кінцеві пристрої (робочі станції, принтери, сервери, точки доступу).

Для підвищення надійності застосовано агрегування каналів (LACP), що збільшує пропускну здатність і виключає єдині точки відмови.

Також передбачено логічну сегментацію трафіку за допомогою VLAN:

- VLAN 10
- VLAN 20
- VLAN 30
- VLAN 40
- VLAN 50
- VLAN 60
- VLAN 77 – мережне адміністрування

Це дозволяє ізолювати трафік між підрозділами, зменшити широкомовне навантаження, підвищити безпеку, а також застосовувати політики доступу на рівні IP-адресації.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Для кожної VLAN реалізовано окрему підмережу на базі IPv4 та IPv6, що забезпечує гнучкість у подальшому масштабуванні інфраструктури. Використання обох протоколів дає змогу забезпечити сумісність з поточними сервісами й підтримку сучасних пристроїв, включаючи IoT.

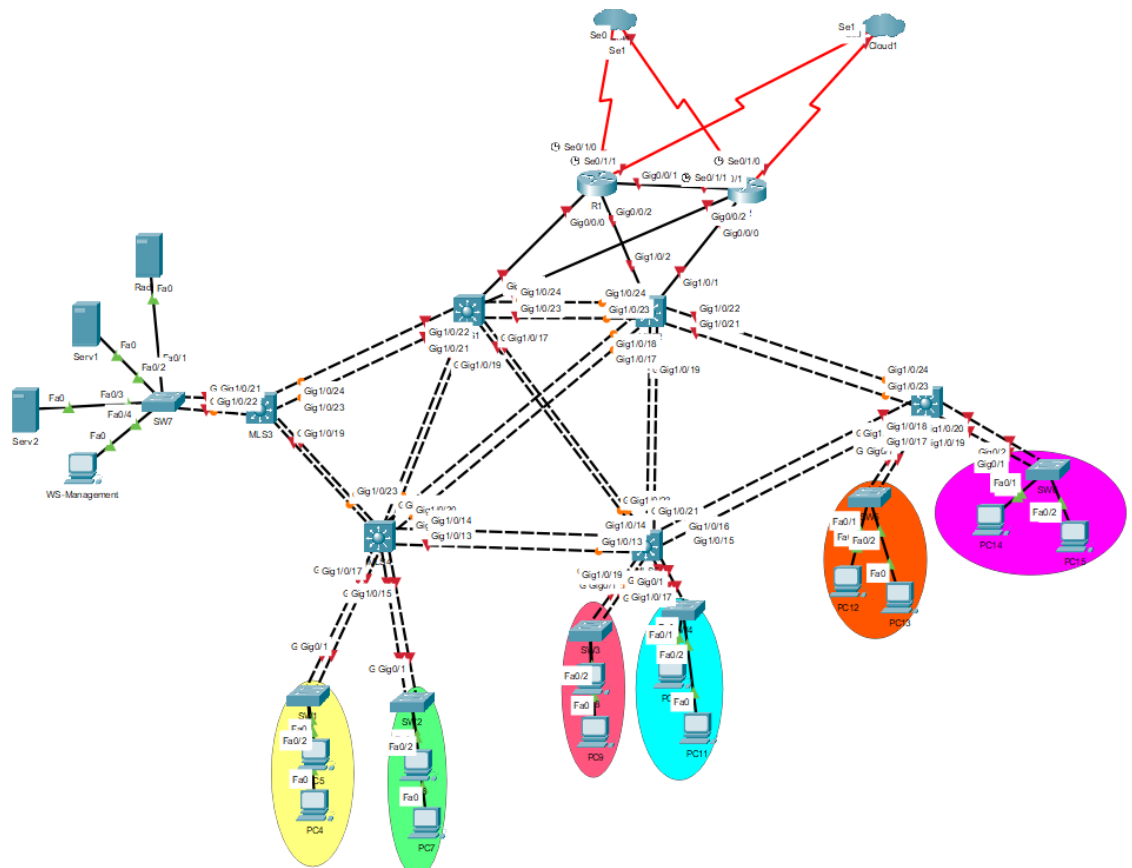


Рисунок 2.1 – Топологія мережі

Уникнення петель на другому рівні, та забезпечення резервування шляхів, окремо для кожної VLAN, було реалізовано за допомогою PVST+, EIGRP було обрано як внутрішній протокол маршрутизації завдяки швидкій конвергенції, підтримці балансування між кількома маршрутами та гнучкому налаштуванню. Його гібридна складова дозволяє оптимізувати маршрутизацію без перевантаження процесора.

2.2 Розробка системи IP-адресації

На сьогодні взаємозв'язок пристроїв є критично важливим для функціонування будь-якої організації чи сервісу, і система IP-адресації виступає її фундаментальним компонентом. Продумана, логічна та масштабована адресна схема є одним із першочергових завдань при побудові або модернізації мережі. Вона забезпечує ефективну маршрутизацію, унікальну ідентифікацію пристроїв і коректну доставку даних у межах всієї мережі. Без впорядкованої адресації маршрутизатори не зможуть визначати оптимальні шляхи для трафіку, що призведе до затримок, неефективного використання ресурсів або навіть до втрати зв'язку між сегментами. Також, IP-адресація тісно пов'язана з адмініструванням мережі та усуненням несправностей: чітка структура підмереж спрощує діагностику проблем, локалізацію збоїв і застосування політик безпеки. Адресна організація без логіки ускладнює моніторинг і контроль доступу. Ще, вона визначає здатність мережі масштабуватися: адресний простір має враховувати можливість зростання кількості пристроїв і появу нових підрозділів, що особливо актуально в умовах обмежень IPv4, без резерву адрес або поділу на логічні підмережі будь-яке розширення призводить до складних і затратних змін. У контексті стрімкого розвитку IoT, хмарних сервісів і переходу на IPv6, значення грамотно спроектованої адресної структури лише посилюється. На основі вищезазначених принципів було сформовано таблиці, в яких представлено детальну IP-адресацію майбутньої мережі.

Таблиця 2.1

IP-адресація v4 в мережі

Мережа/Прис трій	Інтерфейс/Ме режний адаптер	IP-адреса	Маска	Пре фікс
1	2	3	4	5
VLAN 10	-	200.24.0.0	255.255.255.128	/25
VLAN 20	-	200.24.0.128	255.255.255.128	/25
VLAN 30	-	200.24.1.0	255.255.255.192	/26
VLAN 40	-	200.24.1.64	255.255.255.192	/26
VLAN 50	-	200.24.1.128	255.255.255.192	/26

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

Продовження табл. 2.1

1	2	3	4	5
VLAN 60	-	200.24.1.192	255.255.255.192	/26
VLAN 77	-	200.24.2.0	255.255.255.192	/26
R1	Gig0/0/0	200.24.2.1	255.255.255.192	/26
	Gig0/0/1	192.169.1.1	255.255.255.252	/30
	Se0/1/1	192.168.0.1	255.255.0.0	/16
	Se0/1/0	192.167.0.1	255.255.0.0	/16
R2	Gig0/0/0	200.24.2.17	255.255.255.192	/26
	Gig0/0/1	192.169.1.2	255.255.255.252	/30
	Se0/1/1	192.168.0.2	255.255.0.0	/16
	Se0/1/0	192.167.0.2	255.255.0.0	/16
MLS1	Vlan77	200.24.2.2	255.255.255.192	/26
MLS2	Vlan77	200.24.2.3	255.255.255.192	/26
MLS3	Vlan77	200.24.2.4	255.255.255.192	/26
MLS4	Vlan77	200.24.2.5	255.255.255.192	/26
MLS5	Vlan77	200.24.2.6	255.255.255.192	/26
MLS6	Vlan77	200.24.2.7	255.255.255.192	/26
SW1	Vlan77	200.24.2.9	255.255.255.192	/26
SW2	Vlan77	200.24.2.10	255.255.255.192	/26
SW3	Vlan77	200.24.2.11	255.255.255.192	/26
SW4	Vlan77	200.24.2.12	255.255.255.192	/26
SW5	Vlan77	200.24.2.13	255.255.255.192	/26
SW6	Vlan77	200.24.2.14	255.255.255.192	/26
SW7	Vlan77	200.24.2.15	255.255.255.192	/26
Serv1	Vlan77	200.24.2.21	255.255.255.192	/26
Serv2	Vlan77	200.24.2.22	255.255.255.192	/26
Radius	Vlan77	200.24.2.23	255.255.255.192	/26
WS- Management1	Vlan77	200.24.2.16	255.255.255.192	/26
Хости VLAN 10	Eth0/0	DHCP		
Хости VLAN 20	Eth0/0	DHCP		
Хости VLAN 30	Eth0/0	DHCP		
Хости VLAN 40	Eth0/0	DHCP		
Хости VLAN 50	Eth0/0	DHCP		
Хости VLAN 60	Eth0/0	DHCP		

IP-адресація v6 в мережі

Мережа/Прис трій	Інтерфейс/Ме режний адаптер	IP-адреса	Префік с
VLAN 10	-	2001:db8:0:10::	/121
VLAN 20	-	2001:db8:0:20::	/121
VLAN 30	-	2001:db8:0:30::	/121
VLAN 40	-	2001:db8:0:40::	/121
VLAN 50	-	2001:db8:0:50::	/121
VLAN 60	-	2001:db8:0:60::	/121
VLAN 77	-	2001:db8:0:77::	/121
MLS1	Vlan77	2001:db8:0:77::2	/121
MLS2	Vlan77	2001:db8:0:77::3	/121
MLS3	Vlan77	2001:db8:0:77::4	/121
MLS4	Vlan77	2001:db8:0:77::5	/121
MLS5	Vlan77	2001:db8:0:77::6	/121
MLS6	Vlan77	2001:db8:0:77::7	/121
SW1	Vlan77	2001:db8:0:77::9	/121
SW2	Vlan77	2001:db8:0:77::10	/121
SW3	Vlan77	2001:db8:0:77::11	/121
SW4	Vlan77	2001:db8:0:77::12	/121
SW5	Vlan77	2001:db8:0:77::13	/121
SW6	Vlan77	2001:db8:0:77::14	/121
SW7	Vlan77	2001:db8:0:77::15	/121
Serv1	Vlan77	2001:db8:0:77::21	/121
Serv2	Vlan77	2001:db8:0:77::22	/121
Radius	Vlan77	2001:db8:0:77::23	/121
WS- Management1	Vlan77	2001:db8:0:77::16	/121
Хости VLAN 10	DHCP		
Хости VLAN 20	DHCP		
Хости VLAN 30	DHCP		
Хости VLAN 40	DHCP		
Хости VLAN 50	DHCP		
Хости VLAN 60	DHCP		

2.3 Проектування служб та сервісів прикладного рівня

Служби прикладного рівня відіграють ключову роль у забезпеченні повноцінного функціонування корпоративної мережі, перетворюючи технічну інфраструктуру на зручний та ефективний інструмент для виконання повсякденних задач користувачів і підтримки бізнес-процесів організації. Ефективність служб прикладного рівня значною мірою залежить від їх узгодженості з системою адресації, маршрутизацією, механізмами безпеки та політиками доступу. Правильне проектування цих сервісів гарантує не лише надійність і продуктивність, але й масштабованість та зручність усієї мережевої інфраструктури.

Серед служб прикладного рівня існують критично важливі для базового функціонування мережі, як DHCP для автоматичної видачі адрес, DNS для доменної трансляції імен, а також засоби мережевого моніторингу. Існують сервіси, впровадження яких залежить від специфіки роботи організації: системи електронної пошти, обміну файлами. Їх вибір і налаштування мають враховувати індивідуальні вимоги, політики безпеки та очікувані навантаження.

2.3.1 DHCP

Для забезпечення автоматичної видачі IP-адрес користувацьким пристроям було спроектовано окремі DHCP-пули для відповідних VLAN. Це дозволяє спростити процес конфігурації хостів, забезпечити унікальність IP-адрес та полегшити управління адресним простором. Кожен пул має визначений діапазон доступних адрес та виключає з розподілу зарезервовані адреси для шлюзів або інших критичних служб. Окремо реалізовано підтримку як для IPv4, так і для IPv6. В таблицях нижче наведено структуру DHCP-пулів для обох версій IP.

Таблиця 2.3

IP-адреси v4 які включені в пули

DHCP-pool	Діапазон адрес	Виключені адреси
1	2	3
POOL10	200.24.0.1 – 200.24.0.126	200.24.0.1
POOL20	200.24.0.129 – 200.24.0.254	200.24.0.129

1	2	3
POOL30	200.24.1.1 – 200.24.1.62	200.24.1.1
POOL40	200.24.1.65 – 200.24.1.126	200.24.1.65
POOL50	200.24.1.129 – 200.24.1.190	200.24.1.129
POOL60	200.24.1.193 – 200.24.1.254	200.24.1.193

Таблиця 2.4

IP-адреси v6 які включені в пули

DHCP-pool	Діапазон адрес	Виключені адреси
Vlan10v6	2001:db8:0:10::1 – 2001:db8:0:10::7E	2001:db8:0:10::1
Vlan20v6	2001:db8:0:20::1 – 2001:db8:0:20::7E	2001:db8:0:20::1
Vlan30v6	2001:db8:0:30::1 – 2001:db8:0:30::7E	2001:db8:0:30::1
Vlan40v6	2001:db8:0:40::1 – 2001:db8:0:40::7E	2001:db8:0:40::1
Vlan50v6	2001:db8:0:50::1 – 2001:db8:0:50::7E	2001:db8:0:50::1
Vlan60v6	2001:db8:0:60::1 – 2001:db8:0:60::7E	2001:db8:0:60::1

2.3.2. NTP

Точна синхронізація часу між усіма пристроями один із ключових моментів найдійної мережі. Для цього використовується протокол мережевого часу (Network Time Protocol), який забезпечує координацію годинників мережевих пристроїв шляхом отримання еталонного часу через мережі з комутацією пакетів і змінною затримкою. Синхронізація часу має критичне значення для ряду аспектів функціонування інформаційних систем, зокрема:

- забезпечує правильну послідовність записів у журналах подій, що є важливим для моніторингу, аналізу інцидентів та усунення несправностей;
- дозволяє коректно обробляти цифрові сертифікати та інші механізми безпеки, які мають часові обмеження дії;

– є необхідною умовою для функціонування деяких мережових протоколів, що залежать від точного часу.

У межах проєктованої мережі, в ролі еталонного джерела часу буде використовуватись сервер Serv1, який працюватиме як NTP-сервер. Усі інші мережові пристрої будуть налаштовані як NTP-клієнти. Це рішення забезпечує цілісність хронології подій у мережі, підвищує ефективність адміністрування та сприяє дотриманню вимог інформаційної безпеки.

2.3.3. Syslog

Для забезпечення централізованого моніторингу стану мережевої інфраструктури використовується служба журналювання Syslog. Вона дозволяє реєструвати системні повідомлення, попередження, помилки та інші події, що генеруються мережевими пристроями. Це дає змогу отримувати поточний стан мережі, своєчасно виявляти відхилення в роботі обладнання та оперативно реагувати на потенційні інциденти.

У даному проєкту передбачається використання серверів Serv1 та Serv2 як основного та резервного Syslog-серверів відповідно. Маршрутизатори і комутатори в мережі будуть налаштовані як Syslog-клієнти.

2.3.4 DNS

Служба доменних імен є ключовим елементом мережевої інфраструктури, що забезпечує перетворення символьних імен у відповідні IP-адреси, необхідні для маршрутизації трафіку. Її використання значно спрощує доступ до ресурсів як у внутрішньому середовищі організації, так і в Інтернеті.

DNS-сервер розгортається на сервері Serv1, із реалізацією механізму резервування на сервері Serv2. Цей підхід гарантує безперервність і стійкість до відмов у роботі системи імен, що є критично важливим для забезпечення стабільного доступу користувачів до інформаційних ресурсів.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

2.3.5 Система електронної пошти

Для забезпечення внутрішнього та зовнішнього електронного листування в межах корпоративної мережі впроваджується система електронної пошти, розгорнута на сервері Serv1.

Відправлення листів та взаємодія з поштовими серверами інших доменів здійснюється за допомогою SMTP-протоколу з підтримкою TLS-шифрування, що гарантує конфіденційність переданих повідомлень.

Для отримання пошти користувачами на локальні пристрої використовується POP3, який забезпечує завантаження електронних листів із сервера та їх збереження на клієнтській стороні. Така конфігурація дозволяє ефективно організувати поштову взаємодію в межах корпоративної інфраструктури.

2.3.6 Протокол передачі файлів (FTP)

Для організації централізованого обміну файлами між підрозділами компанії у проєктованій мережі передбачено розгортання служби FTP на сервері Serv1. Доступ до ресурсу здійснюватиметься з використанням механізмів автентифікації, що дозволить контролювати доступ користувачів до файлів відповідно до встановлених політик безпеки.

2.4 Проектування підсистеми мережного захисту

Проектування підсистеми мережевого захисту становить критичний етап розробки інфраструктури, оскільки безпека мережі є фундаментальною умовою стабільної роботи всіх сервісів та збереження цілісності даних. Підсистема не обмежується технічними засобами блокування загроз, вона формує комплексний механізм управління ризиками, що охоплює проактивний захист ресурсів, контроль доступу, моніторинг інцидентів та забезпечення відмовостійкості. Ефективна реалізація вимагає глибокої інтеграції з усіма компонентами архітектури.

2.4.1 Користувачі та базовий захист пристроїв

У проєкті передбачено створення локальних облікових записів для адміністрування мережевих пристроїв з різними рівнями привілеїв. Це дозволяє

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

забезпечити диференційований доступ залежно від функціональних обов'язків персоналу. Будуть створені облікові записи на основі розподілу прав доступу: адміністративні користувачі з різними рівнями привілеїв для керування мережевими пристроями, а також облікові записи для користувачів у відповідних службах для кожної VLAN відповідно до їхніх функцій та службового призначення.

Адміністративні користувачі для мережних пристроїв:

- Користувач: admin15; рівень привілеїв: 15; пароль admin;
- Користувач: admin13; рівень привілеїв: 13; пароль admin;
- Користувач: admin10; рівень привілеїв: 10; пароль admin;
- Користувач: admin8; рівень привілеїв: 8; пароль admin;
- Користувач: technic; рівень привілеїв: 5; пароль tech;

Використана генерація RSA-ключів довжиною 2048 бітів для шифрування.

2.4.2 Віддалений доступ

Забезпечення безпечного віддаленого доступу до мережних пристроїв є критично важливим завданням в кожній компанії. Одним із найпоширеніших і найбільш захищених методів є використання протоколу SSH (Secure Shell), який дозволяє здійснювати шифроване підключення до пристроїв для адміністрування та обслуговування. У проекті буде налаштовано SSH з обмеженням параметрів доступу відповідно до вимог безпеки:

- Версія протоколу: 2
- Час тайм-аут сесії: 60 секунд
- Кількість спроб аутентифікації: 3
- Кількість одночасних SSH з'єднань: 2
- Максимальний інтервал інактиву: 20
- Таймер-попередження: 10

2.4.3 Інші питання безпеки

Для забезпечення комплексного захисту мережевої інфраструктури необхідно впроваджувати додаткові функції мережевої безпеки, що працюють на

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

різних рівнях моделі OSI. Такі механізми дозволяють виявляти та запобігати типових векторах атак, контролювати поведінку трафіку, а також забезпечувати стабільність і надійність функціонування мережі навіть у випадках несанкціонованих або аномальних дій.

Будуть налаштовані наступні функції безпеки:

- BPDU Guard.
- DHCP Snooping.
- DAI.
- Storm Control.
- Port Security.
- RADIUS.

Висновки до 2 розділу: розроблено архітектуру мережі з трирівневою ієрархією (ядро-розподіл-доступ), логічною сегментацією на 7 VLAN, системою IPv4/IPv6-адресації. Спроектовано підсистему безпеки на базі BPDUGuard, DHCP Snooping, DAI, Port Security та AAA. Впроваджено критичні сервіси: DHCP для автоматизації, NTP для синхронізації, Syslog для моніторингу, DNS для перетворення імен, SMTP, POP3 для корпоративної пошти та FTP для захищеного обміну файлами.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ, ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ СПРОЕКТОВАНОЇ ЛОКАЛЬНОЇ IPV4-МЕРЕЖІ ОРГАНІЗАЦІЇ

3.1 Вибір обладнання для розробленого проекту мережі

Проектування потребує ретельного добору мережевого обладнання відповідно до функціональних ролей, які повинні виконувати пристрої в межах архітектури. Для забезпечення стабільної, масштабованої, керованої та захищеної мережевої інфраструктури в даному проєкті було використано обладнання Cisco Catalyst трьох серій, кожне з яких виконує специфічну роль у трирівневій моделі мережі (core, distribution, access).

3.1.1 Вибір маршрутизаторів

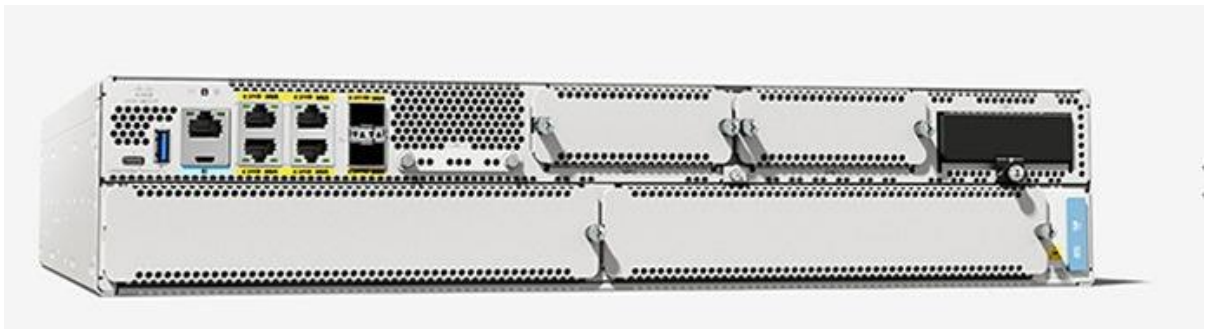


Рисунок 3.1 – Cisco Catalyst 8300 Series

Обраний для реалізації функцій шлюзів до Інтернету та зовнішніх WAN-з'єднань. Розташовані на рівні ядра та забезпечують:

- Агрегацію підмереж.
- Захищене з'єднання з Інтернетом через VPN (IPsec, DMVPN).
- Високу пропускну здатність (до 9.3 Гбіт/с) для обробки великого обсягу трафіку.
- Модульність, що дозволяє гнучко розширювати функціонал (порти, VPN, маршрути).
- Інтегровані засоби безпеки, включно з Zone-Based Firewall та MACSec.
- Підтримку маршрутизуючих протоколів (OSPF, EIGRP, BGP) та керування через IOS XE, RESTCONF.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

3.1.2 Вибір комутаторів



Рисунок 3.2 – Cisco Catalyst 9300 Series

Ця серія пристроїв обрана для розподільчого рівня, де відбувається:

- Маршрутизація між VLAN із високою швидкістю.
- Обробка великого обсягу трафіку – пропускна здатність до 1.76 Тбіт/с або 14 Тбіт/с у стеку.
- Сегментація мережі через підтримку VRF-lite.
- Безпечна фільтрація доступу через ACL, MACSec.
- Підтримка стекування StackWise, що забезпечує високу відмовостійкість та спрощує адміністрування.
- Інтеграція з Cisco DNA Center для централізованого управління, автоматизації та аналітики.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				54
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.3 – Cisco Catalyst 9200L Series

Комутатори цієї серії встановлені на рівні доступу, де відбувається підключення кінцевих пристроїв користувачів:

- Порти 48×1 Гб + 4×uplink, із можливістю підтримки PoE+ для живлення IP-телефонів чи точок доступу.
- Базові функції безпеки: DHCP Snooping, Port Security, Dynamic ARP Inspection.
- Підтримка стекування до 8 пристроїв для підвищення гнучкості та відмовостійкості.
- Підтримка VLAN, STP, RSTP, що дозволяє побудувати стійку топологію без петель.

Обрані пристрої Cisco доповнюють один одного і реалізують трирівневу модель, що забезпечує: продуктивність на кожному рівні мережі відповідно до навантаження, безпеку за рахунок розподілу функцій захисту на всіх рівнях, масштабованість завдяки стекуванню, модульності, VRF та централізованому

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

управлінню, відмовостійкість і керованість як на рівні інтерфейсів, так і через Cisco DNA Center.

У результаті такий підхід дозволяє побудувати надійну, збільшувану та захищену корпоративну мережу, яка відповідає сучасним вимогам до інформаційної інфраструктури підприємства.

У зв'язку з обмеженнями Cisco Packet Tracer, у середовищі моделювання неможливо використовувати реальні пристрої Cisco Catalyst 8300, 9300 та 9200L. Тому для відображення їх функціональності були застосовані спрощені аналоги, Cisco ISR4331, Cisco Catalyst 3650-24PS, Cisco Catalyst 2960 відповідно. Налаштування пристроїв є також обмеженими, тому повноцінно розгорнути спроектовану мережу не вдається.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Налаштування спроектованої мережі

Конфігурація управлінського доступу є першочерговим завданням, оскільки забезпечує контроль над пристроєм під час подальшого налаштування.

Базова конфігурація пристроїв:

```
Switch(config)#username admin15 privilege 15 secret admin15
Switch(config)#username admin13 privilege 13 secret admin13
Switch(config)#username admin10 privilege 10 secret admin10
Switch(config)#username admin8 privilege 8 secret admin8
Switch(config)#username technic privilege 5 secret tech5
Switch(config)#enable secret pass
Switch(config)#ip domain-name mynet.net
Switch(config)#crypto key generate rsa general-keys modulus 2048
Switch(config)#ip ssh version 2
Switch(config)#line vty 0 4
Switch(config-line)#login local
Switch(config-line)#transport input ssh
Switch(config-line)#transport output ssh
Switch(config-line)#logging synchronous
Switch(config-line)#exit
Switch(config)#ip ssh authentication-retries 3
Switch(config)#ip ssh time-out 60
```

Визначення VLAN і VTP створює логічну основу для сегментації мережі перед налаштуванням інтерфейсів.

Налаштування VTP та VLAN:

```
Switch#vlan database
Switch(vlan)#vlan 10 name
Switch(vlan)#vlan 20 name
Switch(vlan)#vlan 30 name
Switch(vlan)#vlan 40 name
```

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				57
Змн.	Арк.	№ докum.	Підпис	Дата		

Switch(vlan)#vlan 50 name

Switch(vlan)#vlan 60 name

Switch(vlan)#vlan 77 name VLAN-Management

Switch(vlan)#vtp server

Switch(vlan)#vtp domain mynet

Switch(vlan)#vtp password pass

Switch(config)#vtp mode client

Switch(config)#vtp domain mynet

Switch(config)#vtp password pass

Агрегація каналів, що гарантує коректне застосування параметрів до фізичних та логічних інтерфейсів.

Налаштування EtherChannel:

Switch(config)#interface range gig0/1-2

Switch(config-if-range)#channel-group 1 mode active

Switch(config)#interface port-channel 1

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50,60,77

Switch(config)#interface range gig0/1-2

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 10

Налаштування SVI (VLAN інтерфейсів):

MLS4(config)#interface Vlan10

MLS4(config)#ip address 200.24.0.1 255.255.255.128

MLS4(config)#ipv6 address 2001:DB8:0:10::1/121

MLS4(config)#ipv6 nd managed-config-flag

MLS4(config)#ipv6 enable

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				58
Змн.	Арк.	№ докum.	Підпис	Дата		

```

MLS4(config)#ipv6 dhcp server POOL10v6
MLS4(config)#interface Vlan20
MLS4(config)#ip address 200.24.0.129 255.255.255.128
MLS4(config)#ipv6 address 2001:DB8:0:20::1/121
MLS4(config)#ipv6 nd managed-config-flag
MLS4(config)#ipv6 enable
MLS4(config)#ipv6 dhcp server POOL20v6
MLS4(config)#interface Vlan77
MLS4(config)#ip address 200.24.2.5 255.255.255.192
MLS4(config)#ipv6 address 2001:DB8:0:77::2/121

```

DHCP-сервер конфігурується після визначення шлюзів, оскільки пули адрес посилаються на SVI інтерфейси як default-router:

```

MLS4(config)#ip dhcp excluded-address 200.24.0.1
MLS4(config)#ip dhcp excluded-address 200.24.0.129
MLS4(config)#ip dhcp pool POOL10
MLS4(config)#network 200.24.0.0 255.255.255.128
MLS4(config)#default-router 200.24.0.1
MLS4(config)#dns-server 200.24.2.21
MLS4(config)#domain-name my.net
MLS4(config)#ip dhcp pool POOL20
MLS4(config)#network 200.24.0.128 255.255.255.128
MLS4(config)#default-router 200.24.0.129
MLS4(config)#dns-server 200.24.2.21
MLS4(config)#domain-name my.net
MLS4(config)#ipv6 dhcp pool POOL10v6
MLS4(config)#address prefix 2001:db8:0:10::/121 lifetime 172800 86400
MLS4(config)#dns-server 2001:DB8:0:77::21
MLS4(config)#domain-name my.net
MLS4(config)#ipv6 dhcp pool POOL20v6

```

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

MLS4(config)#address prefix 2001:db8:0:20::/121 lifetime 172800 86400

MLS4(config)#dns-server 2001:DB8:0:77::21

MLS4(config)#domain-name my.net

Налаштування STP виконується після створення VLAN, але до впровадження безпекових механізмів, що використовують топологію:

MLS4(config)#spanning-tree mode pvst

MLS4 (config)#spanning-tree vlan 10 priority 4096

MLS4 (config)#spanning-tree vlan 20 priority 4096

Конфігурація NTP/Syslog розгортається після базової мережевої інтеграції:

MLS4(config)#service timestamps log datetime msec

MLS4(config)#service timestamps debug datetime msec

MLS4(config)#clock timezone GMT 3

MLS4(config)#ntp server 200.24.2.21 key 2506

MLS4(config)#ntp authenticate

MLS4(config)#ntp authentication-key 2506 md5 pass

MLS4(config)#ntp trusted-key 2506

MLS4(config)#ntp update-calendar

MLS4(config)#logging on

MLS4(config)#logging 200.24.2.21

MLS4(config)#logging 200.24.2.22

MLS4(config)#logging userinfo

MLS4(config)#logging trap debugging

MLS4(config)#logging buffered 64000

Налаштування безпеки:

Switch(config)#interface range fa0/15-24

Switch(config-if-range)#spanning-tree portfast

Switch(config-if-range)#spanning-tree bpduguard enable

Switch(config)#errdisable recovery cause bpduguard

Switch(config)#errdisable recovery interval 360

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				60
Змн.	Арк.	№ докum.	Підпис	Дата		

```
Switch(config)#ip dhcp snooping vlan 10,20,30,40,50,77,999
```

```
Switch(config)#interface range gig1/0/1-8
```

```
Switch(config-if-range)#ip dhcp snooping trust
```

```
Switch(config-if-range)#ip dhcp snooping limit rate 256
```

```
Switch(config)#ip arp inspection vlan 10,20,30,40,50,77,999
```

```
Switch(config)#interface range gig1/0/1-8
```

```
Switch(config-if-range)#ip arp inspection trust
```

```
Switch(config-if-range)#exit
```

```
Switch(config)#errdisable recovery cause arp-inspection
```

```
Switch(config)#errdisable recovery interval 120
```

```
MLS1(config)#aaa new-model
```

```
MLS1(config)#aaa authentication login default group radius local
```

```
MLS1(config)#aaa authentication enable default group radius local
```

```
MLS1(config)#radius server Radius
```

```
MLS1(config-radius-server)#address ipv4 200.24.2.23 auth-port 1645
```

```
MLS1(config-radius-server)#key 7 pass
```

Маршрутизація та NAT конфігуруються останніми, оскільки вимагають повної готовності внутрішньої інфраструктури:

```
MLS5(config)#router eigrp 100
```

```
MLS5(config-router)#network 200.24.1.0 0.0.0.63
```

```
MLS5(config-router)#network 200.24.1.64 0.0.0.63
```

```
R1(config)#int gig0/0/1
```

```
R1(config-if)#ip address 192.169.1.1 255.255.255.252
```

```
R1(config-if)#no shut
```

```
R1(config)#int se0/1/1
```

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

R1(config-if)#ip address 192.168.0.1 255.255.0.0

R1(config-if)#no shut

R1(config-if)#ex

R1(config)#int se 0/1/0

R1(config-if)#ip address 192.167.0.1 255.255.0.0

R1(config-if)#no shut

R1(config-if)#ex

R1(config)#int se0/1/1

R1(config-if)#ip nat outside

R1(config-if)#ex

R1(config)#int se0/1/0

R1(config-if)#ip nat outside

R1(config-if)#ex

R1(config)#int gig0/0/0

R1(config-if)#ip nat inside

R1(config)#p nat inside source static 200.24.2.1 192.168.0.1

Всі налаштування на інших пристроях були налаштовані відповідно.

Надалі була налаштована працездатність серверів:

The screenshot shows the RADIUS configuration window with the 'Services' tab selected. The 'AAA' service is configured with 'On' selected and 'Radius Port' set to 1645. Under 'Network Configuration', a table lists clients SW2 through SW7 with their IP addresses and Radius keys. Below this, the 'User Setup' section shows a table of users including admin10, admin13, admin15, admin8, and tech with their respective passwords.

	Client Name	Client IP	Server Type	Key
1	SW2	200.24.2.10	Radius	pass
2	SW3	200.24.2.11	Radius	pass
3	SW4	200.24.2.12	Radius	pass
4	SW5	200.24.2.13	Radius	pass
5	SW6	200.24.2.14	Radius	pass
6	SW7	200.24.2.15	Radius	pass

	Username	Password
1	admin10	admin10
2	admin13	admin13
3	admin15	admin15
4	admin8	admin8
5	tech	tech

Рисунок 3.4 – Налаштований сервер RADIUS

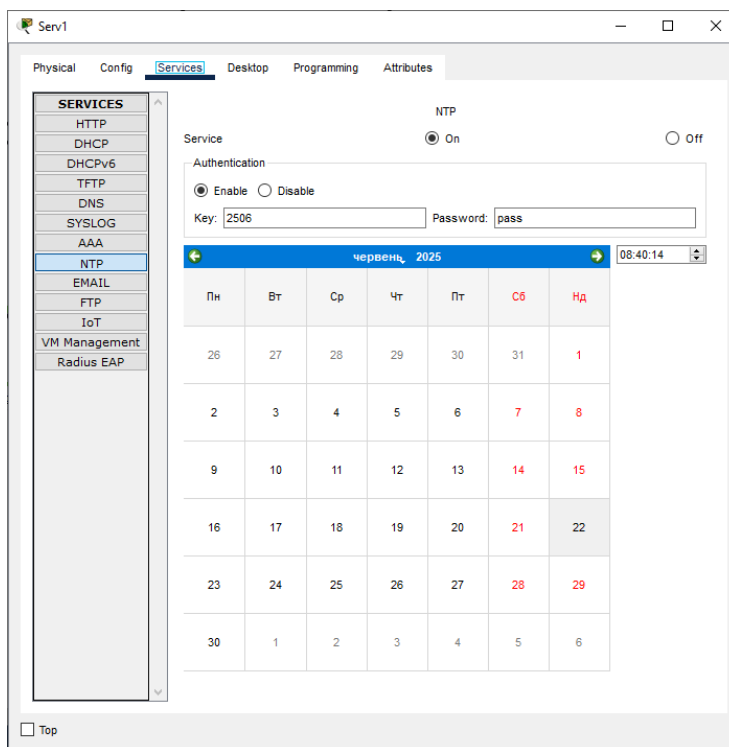


Рисунок 3.5 – Налаштування NTP сервера

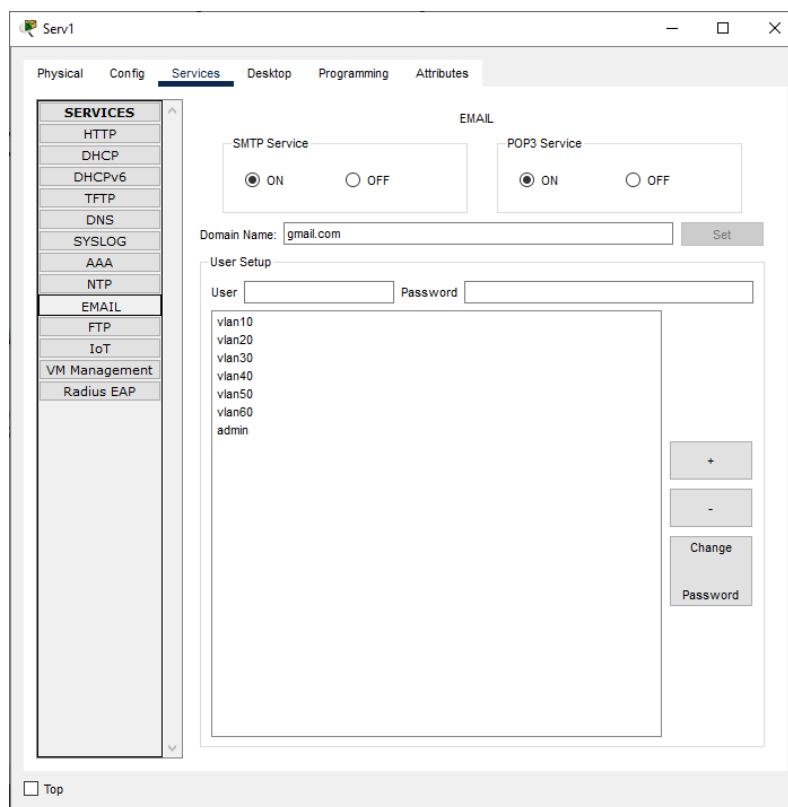


Рисунок 3.6 – Налаштування пошти на сервері

Конфігураційні файли мережних пристроїв наведені у додатках.

3.3 Тестування роботи побудованої мережі

Після завершення проєктування та налаштування корпоративної мережі важливим етапом є тестування її працездатності, яке дозволяє переконатися в коректності реалізації закладеної логіки, виявити можливі помилки в конфігурації та підтвердити відповідність проєкту технічним вимогам. Мета тестування полягає в перевірці функціонування основних мережевих сервісів, протоколів маршрутизації, безпеки та доступу, а також у забезпеченні взаємодії між усіма вузлами мережі відповідно до заданої структури.

Основні етапи тестування включають:

- Перевірка доступності хостів.
- Тестування VLAN і міжвланової маршрутизації.
- Перевірка DHCP.
- Тестування роботи DNS.
- Аналіз функціонування електронної пошти.
- Перевірка захищеного віддаленого доступу (SSH).
- Тестування механізмів безпеки.
- Моніторинг через Syslog та NTP.

Перевірка за допомогою пінгів у мережі:

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

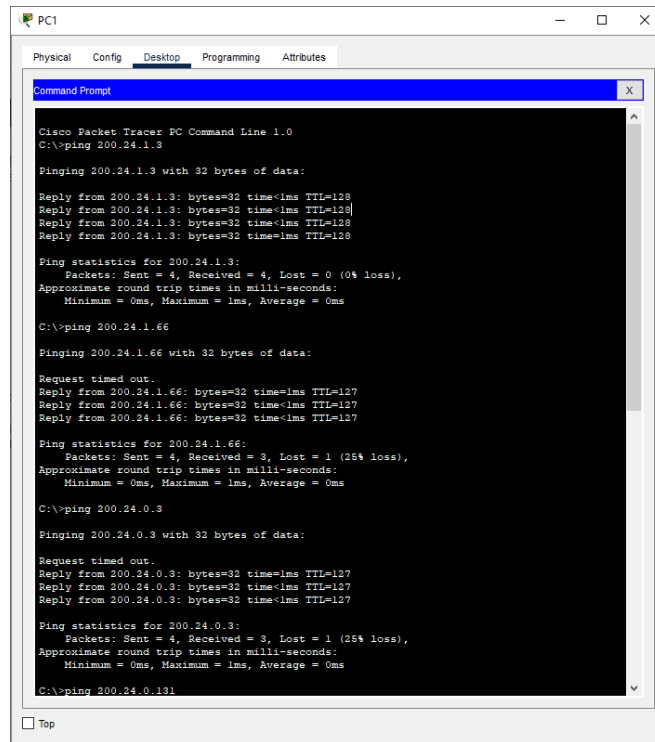


Рисунок 3.7 – Перевірка зв'язку в мережі та маршрутизації між VLAN

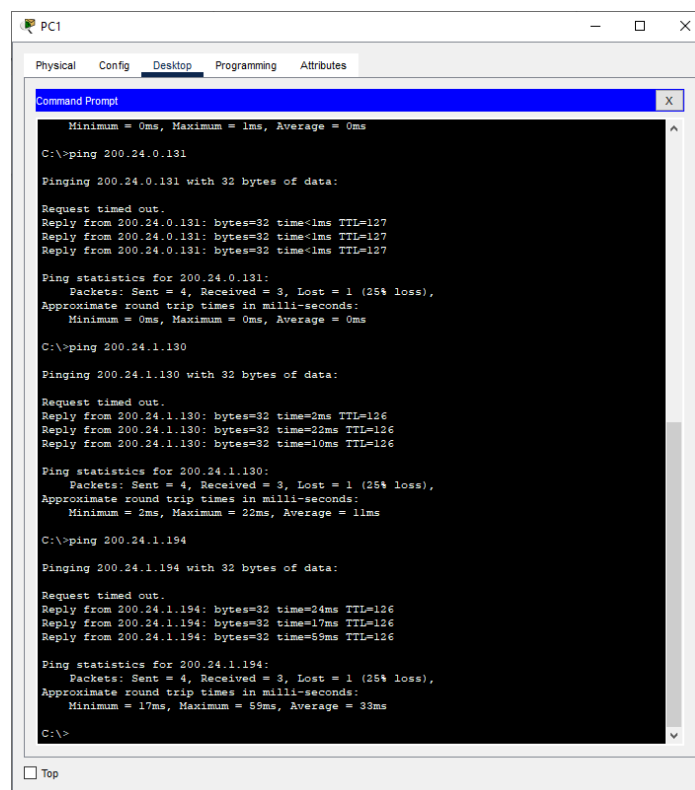


Рисунок 3.8 – Перевірка зв'язку в мережі та маршрутизації між VLAN

Перевірка DHCPv4 та DHCPv6 були зроблені в кожній VLAN.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				65
Змн.	Арк.	№ докum.	Підпис	Дата		

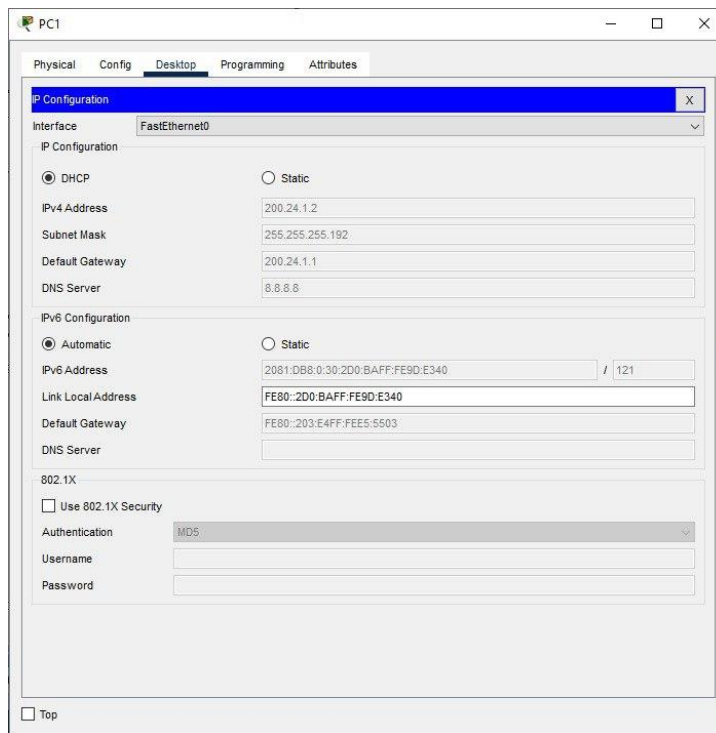


Рисунок 3.9 – Приклад роботи DHCP у VLAN 30

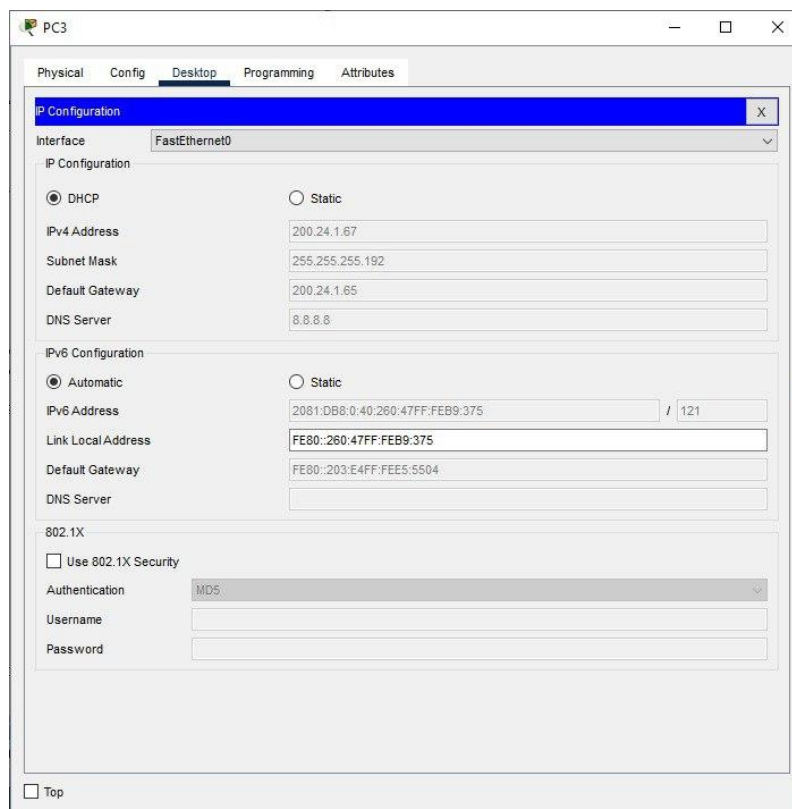


Рисунок 3.10 – Приклад роботи DHCP у VLAN 40

PC5

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 200.24.0.6

Subnet Mask: 255.255.255.128

Default Gateway: 200.24.0.1

DNS Server: 8.8.8.8

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address: 2081:DB8:0:10:2D0:58FF:FE88:240A / 121

Link Local Address: FE80::2D0:58FF:FE88:240A

Default Gateway: FE80::2D0:BDFF:FECC:3701

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Рисунок 3.11 – Приклад роботи DHCP у VLAN 10

PC8

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 200.24.0.134

Subnet Mask: 255.255.255.128

Default Gateway: 200.24.0.129

DNS Server: 8.8.8.8

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address: 2081:DB8:0:20:260:47FF:FE23:8383 / 121

Link Local Address: FE80::260:47FF:FE23:8383

Default Gateway: FE80::203:E4FF:FEE5:5502

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Рисунок 3.12 – Приклад роботи DHCP у VLAN 20

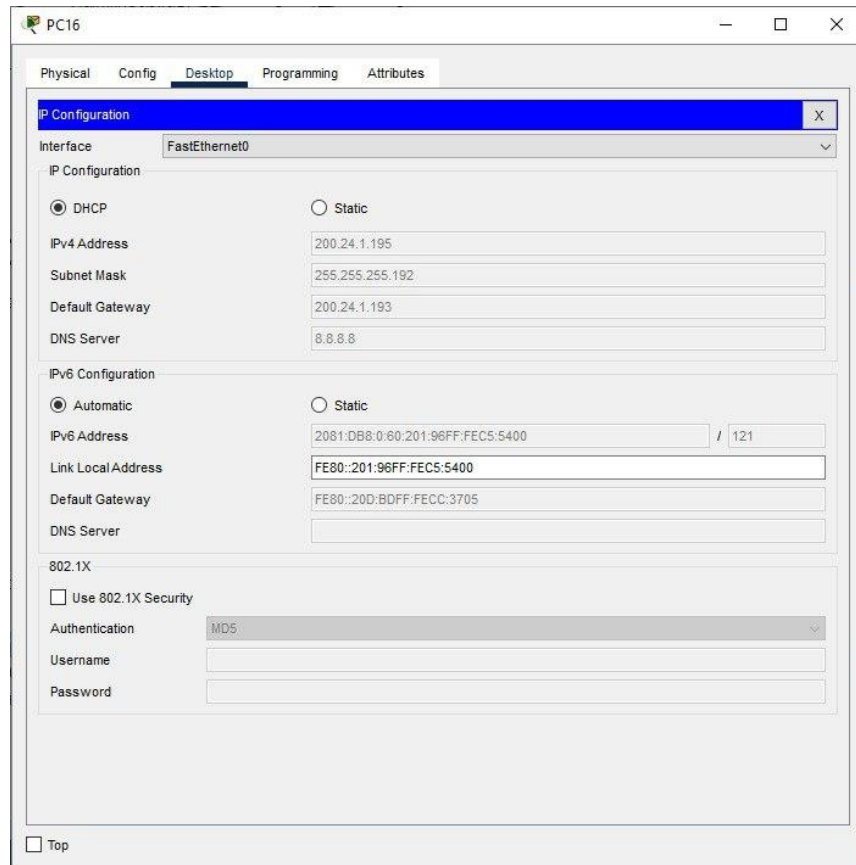


Рисунок 3.13 – Приклад роботи DHCP у VLAN 60

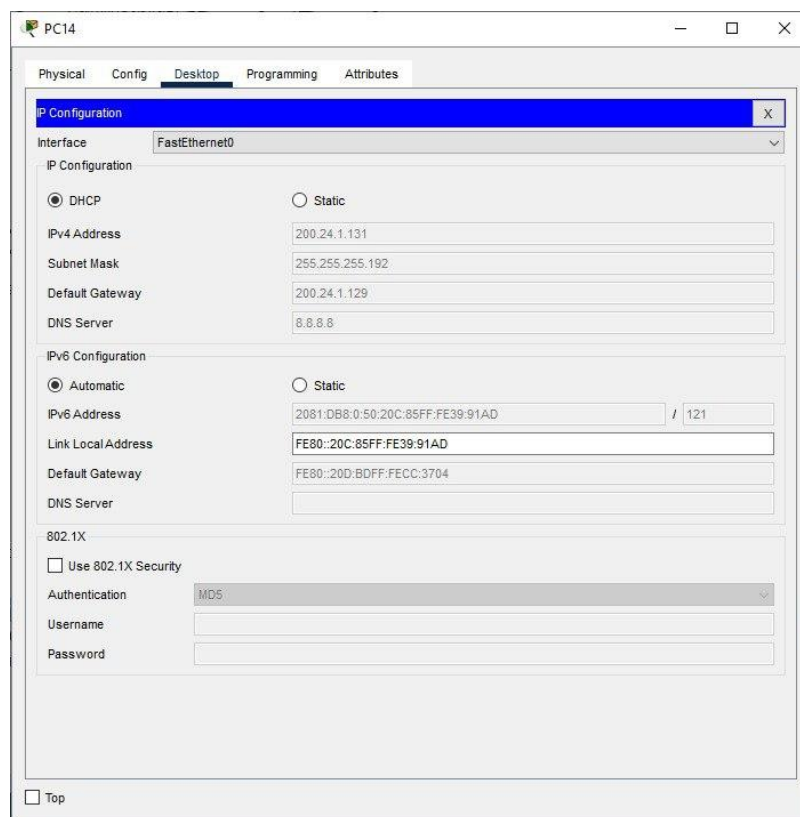


Рисунок 3.14 – Приклад роботи DHCP у VLAN 50

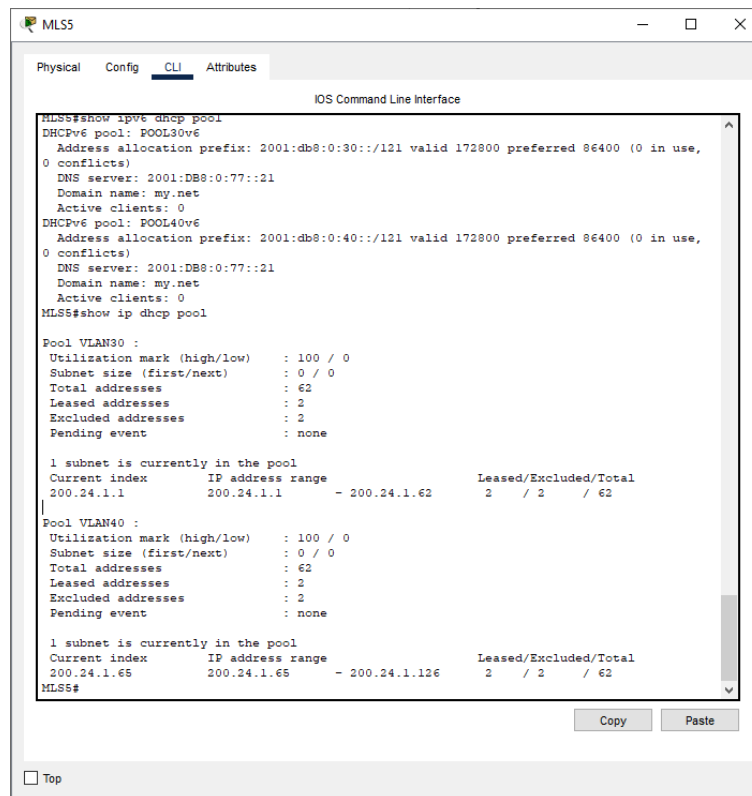


Рисунок 3.15 – Команди діагностики DHCP на MLS5

Наступними критичними службами для перевірки стали DNS, HTTP:

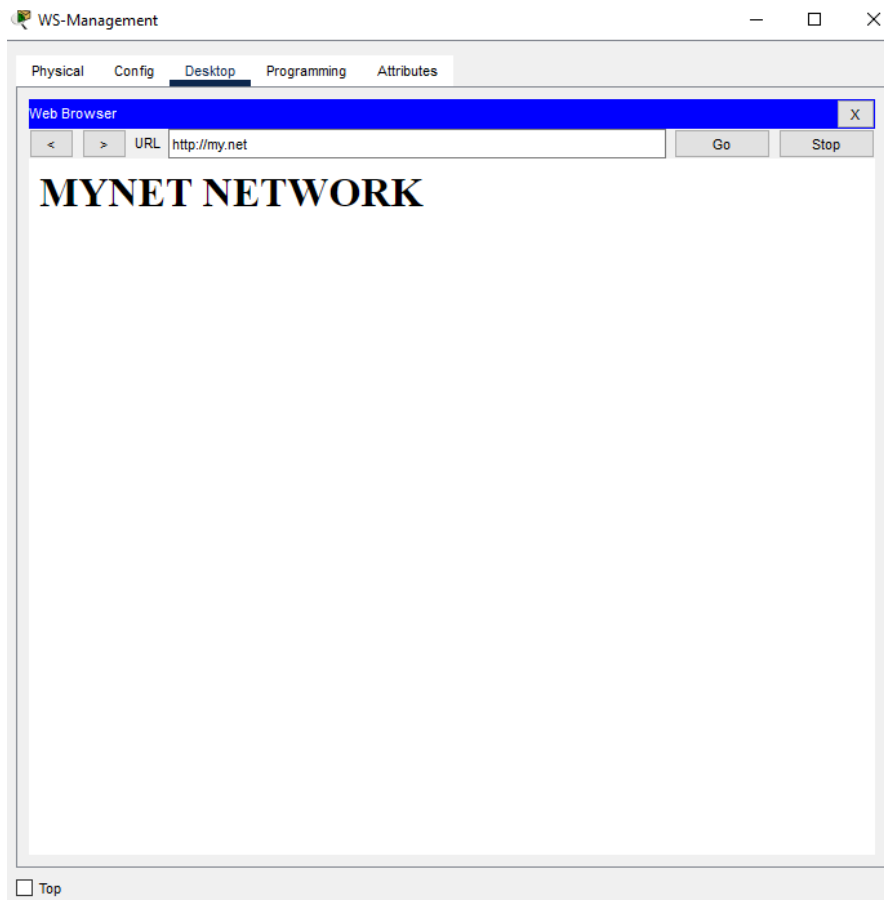


Рисунок 3.16 – Перевірка роботи HTTP та DNS

Перевірка роботи поштових служб:

WS-Management

Physical Config **Desktop** Programming Attributes

Configure Mail X

User Information

Your Name: Yehor

Email Address: 123@gmail.com

Server Information

Incoming Mail Server: 200.24.2.21

Outgoing Mail Server: 200.24.2.21

Logon Information

User Name: vlan10

Password:

Save Remove Clear Reset

☐ Top

Рисунок 3.17 – Перевірка роботи пошти

Serv2

Physical Config Services **Desktop** Programming Attributes

Configure Mail X

User Information

Your Name: Yehor2

Email Address: 321@gmail.com

Server Information

Incoming Mail Server: 200.24.2.21

Outgoing Mail Server: 200.24.2.21

Logon Information

User Name: vlan20

Password:

Save Remove Clear Reset

☐ Top

Рисунок 3.18 – Перевірка роботи пошти

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				70
Змн.	Арк.	№ док.ум.	Підпис	Дата		

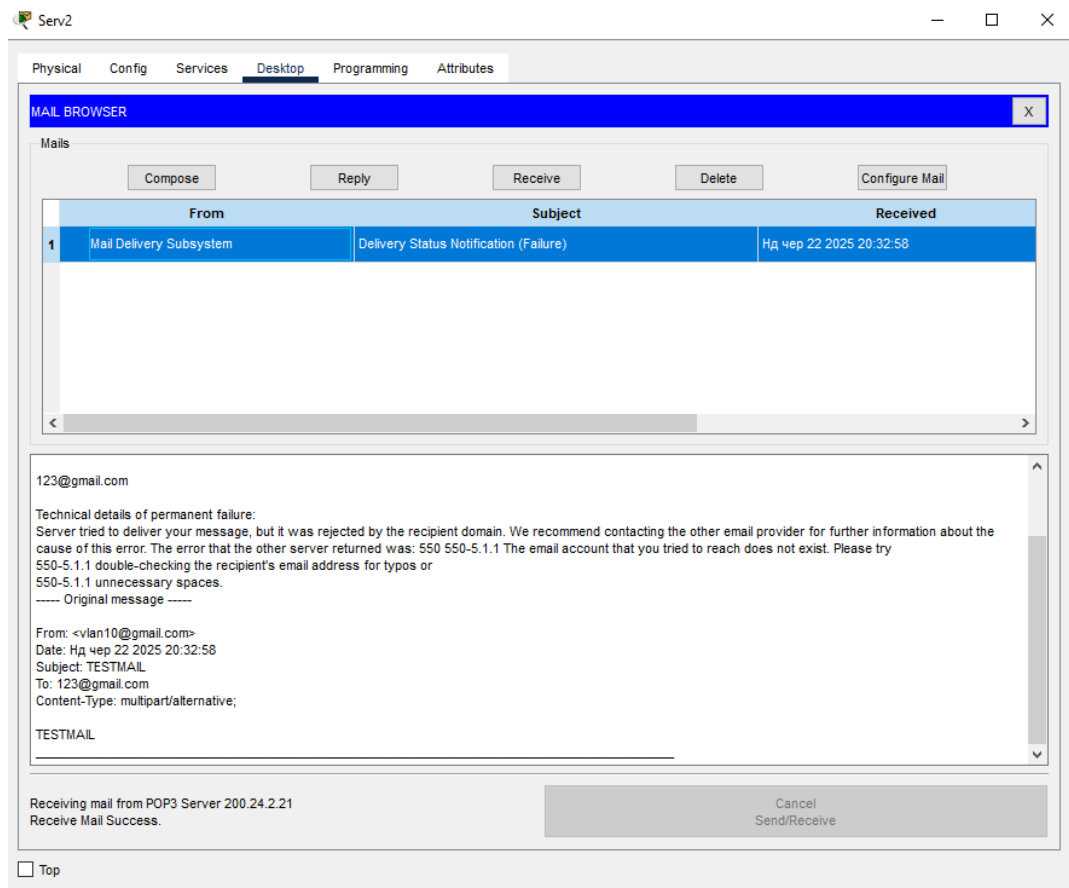


Рисунок 3.19 – Результат роботи пошти

Перевірка роботи файлового обміну:

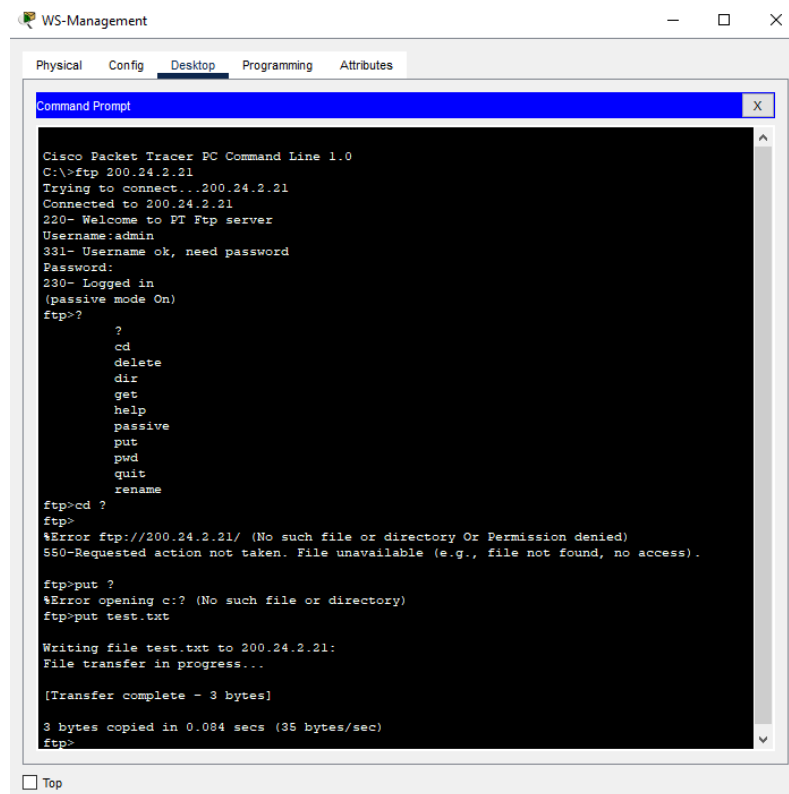


Рисунок 3.20 – Перевірка роботи FTP

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

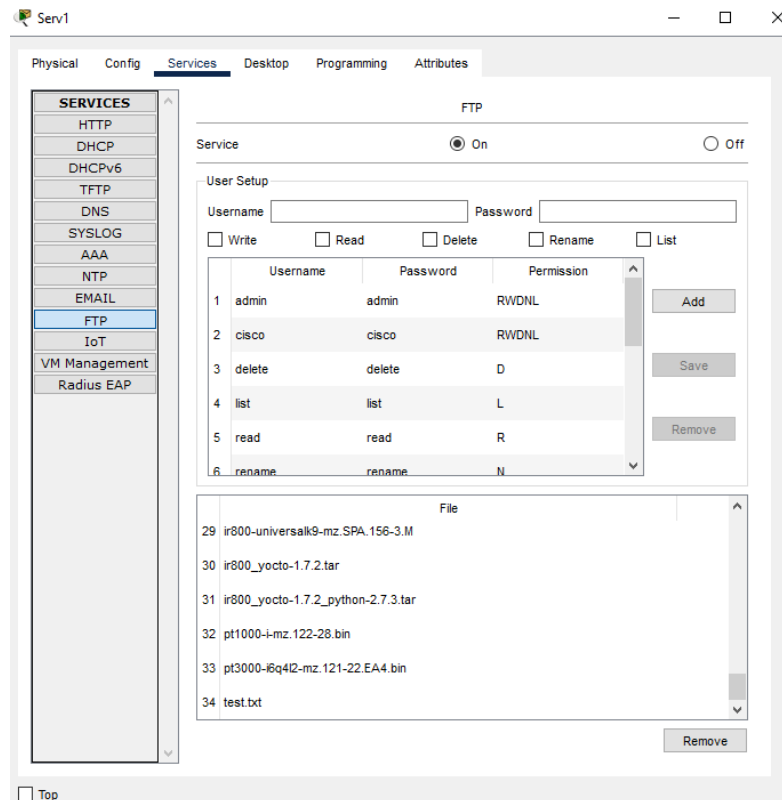


Рисунок 3.21 – Результат перевірки FTP

Перевірка підключення за допомогою SSH:

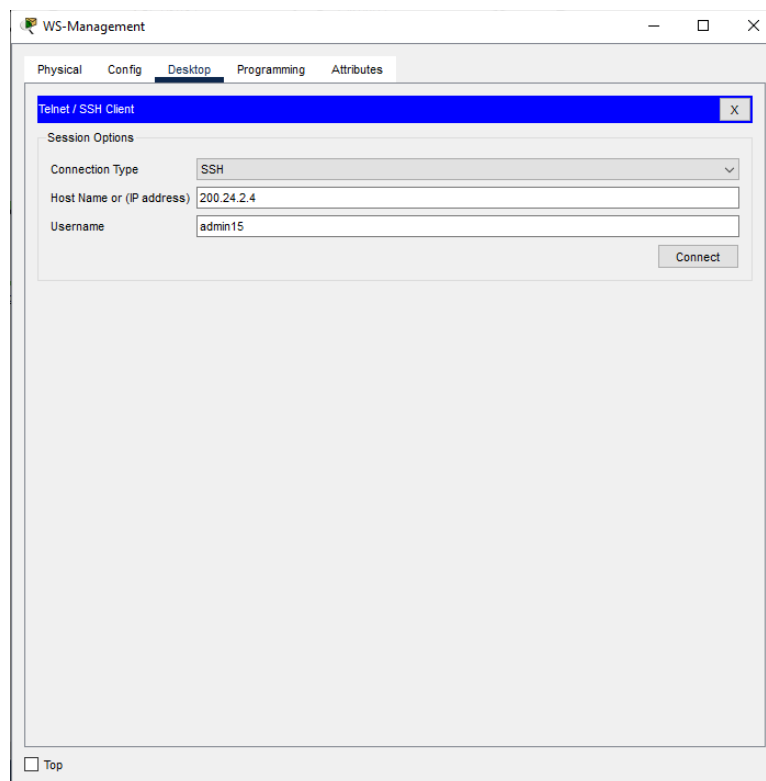


Рисунок 3.22 – Перевірка віддаленого підключення

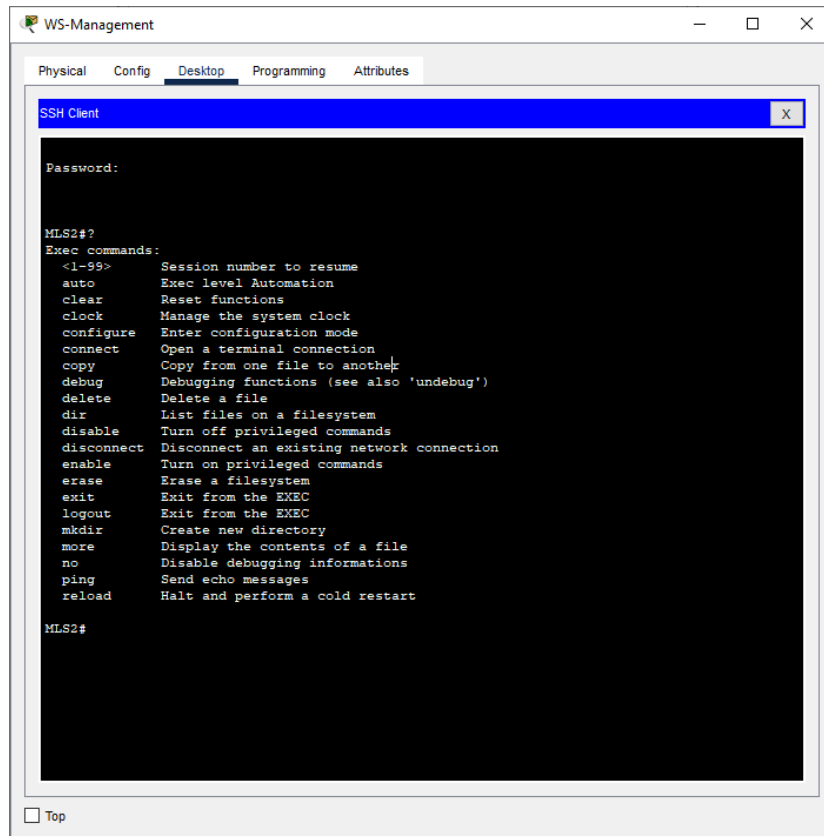


Рисунок 3.23 – Перевірка віддаленого підключення
Під'єднання комутатора до інтерфейсу з захистом BPDUGuard:

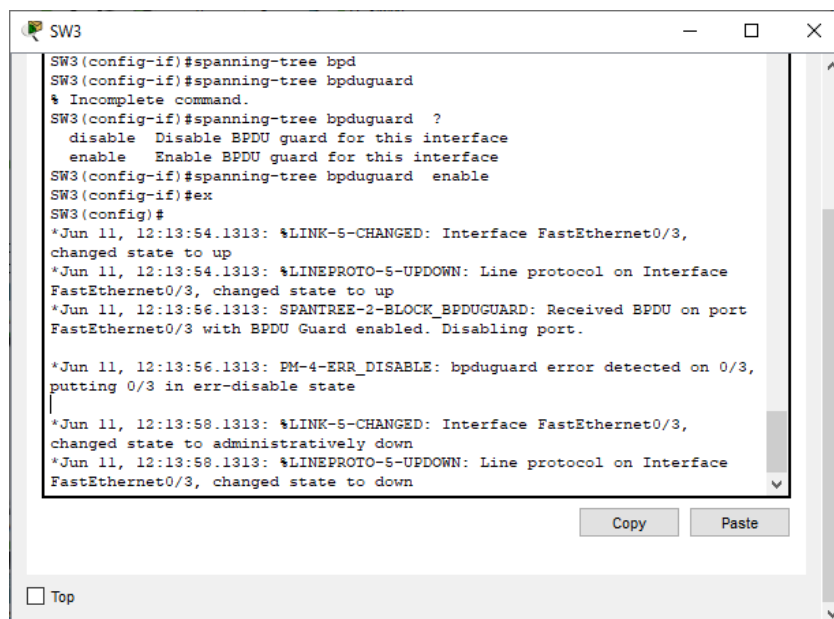


Рисунок 3.24 – Перевірка роботи BPDUGuard
Перевірка SYSLOG та NTP:

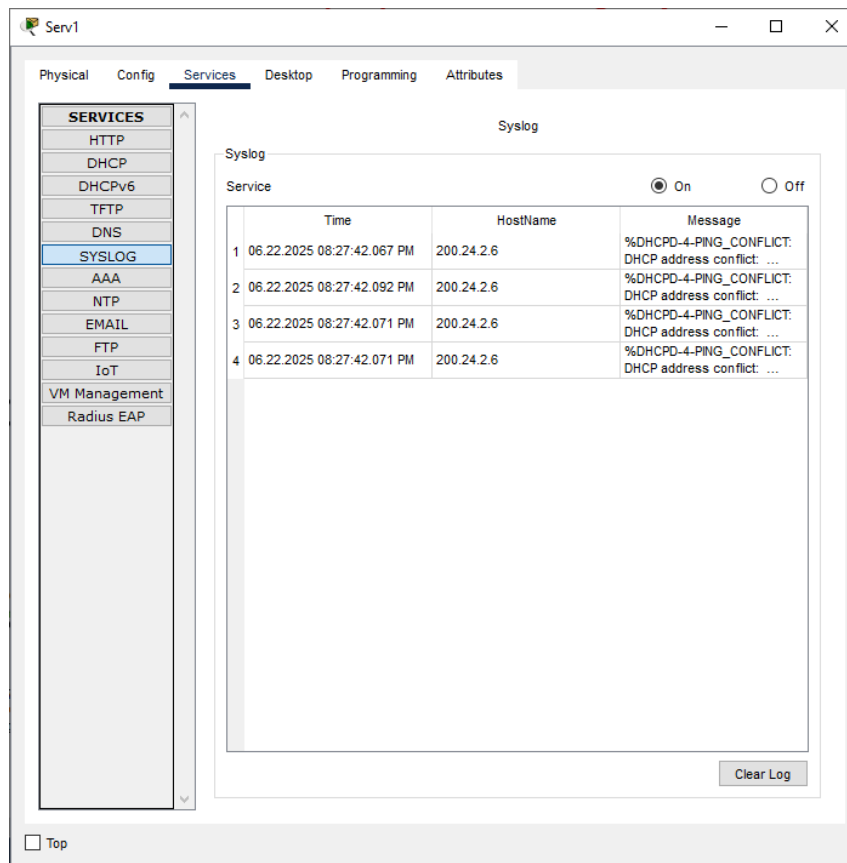


Рисунок 3.25 – Робота сервера з журналювання подій

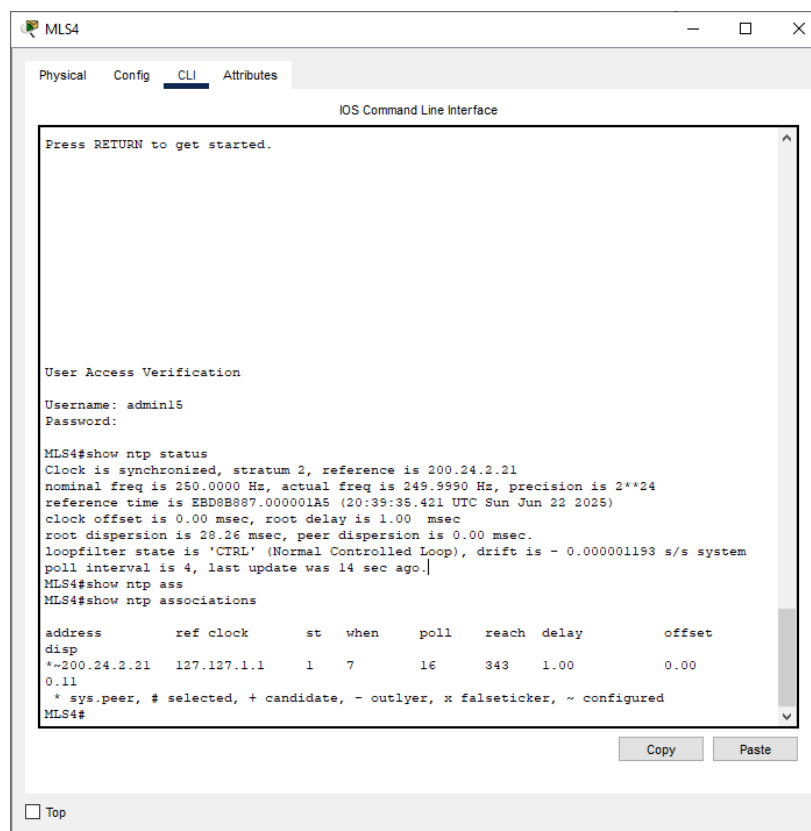


Рисунок 3.26 – Команди діагностики NTP на MLS4

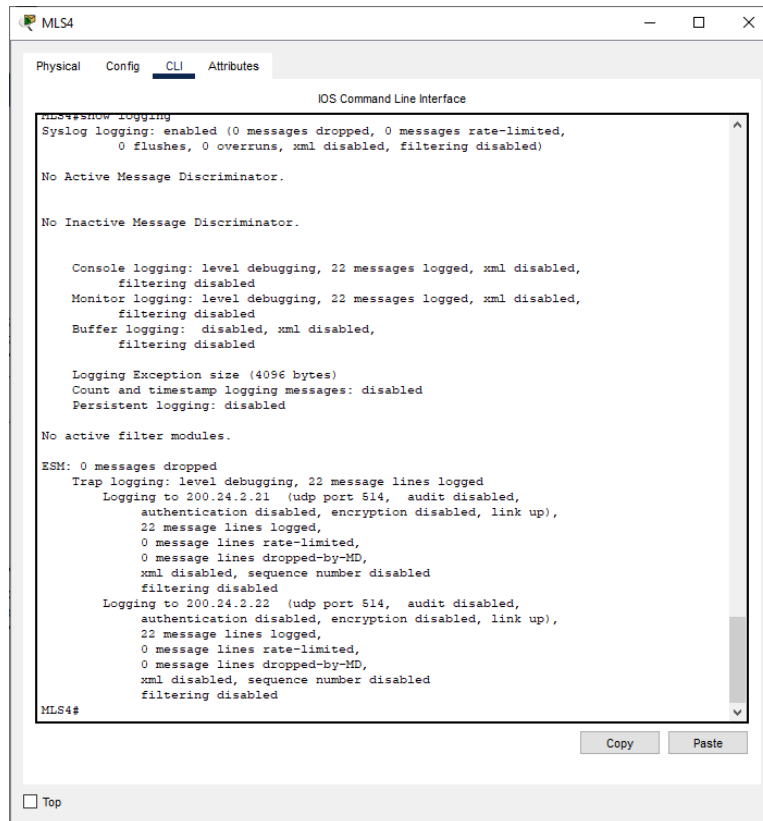


Рисунок 3.27 – Команди діагностики журналювання на MLS4

Перевірка роботи PVST+:

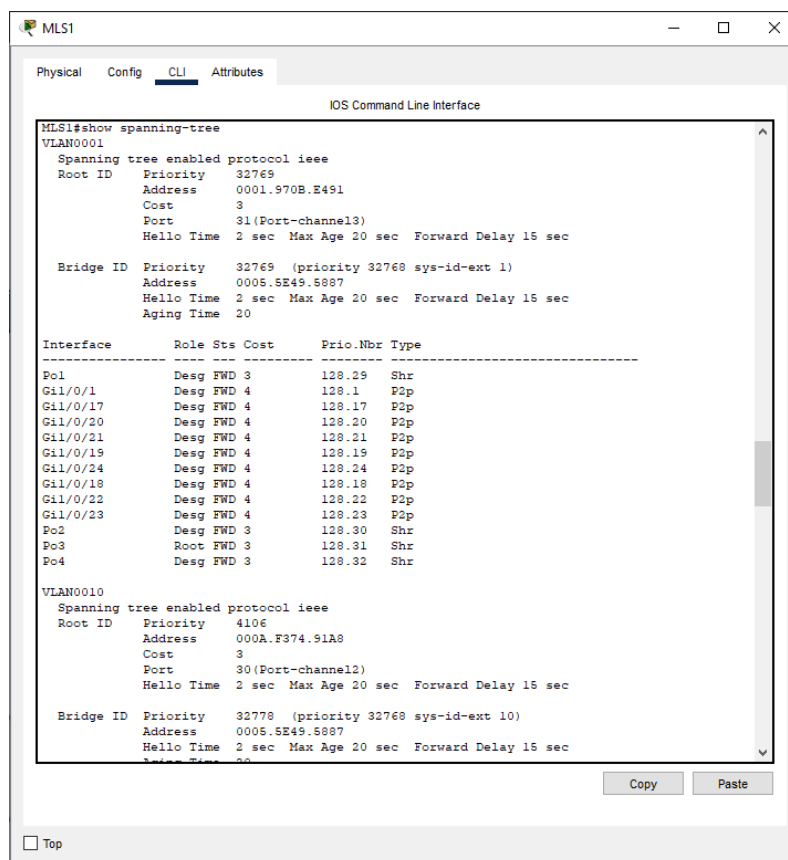


Рисунок 3.28 – Вивід команди show spanning tree на MLS1

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арх.
		Єфіменко А.А.				75
Змн.	Арх.	№ докум.	Підпис	Дата		

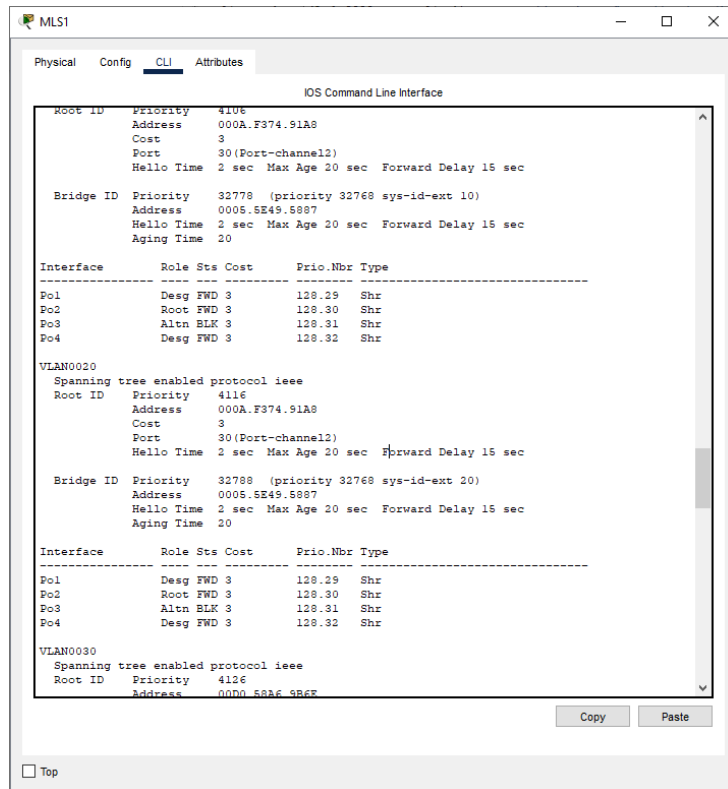


Рисунок 3.29 – Вивід команди show spanning tree на MLS1

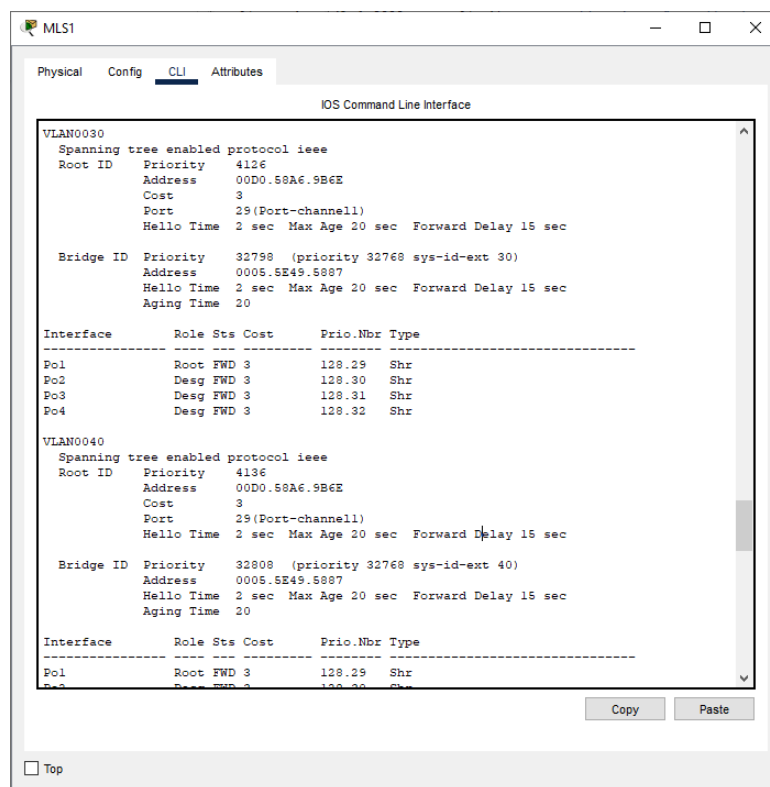


Рисунок 3.30 – Вивід команди show spanning tree на MLS1

Перевірка EtherChannel:

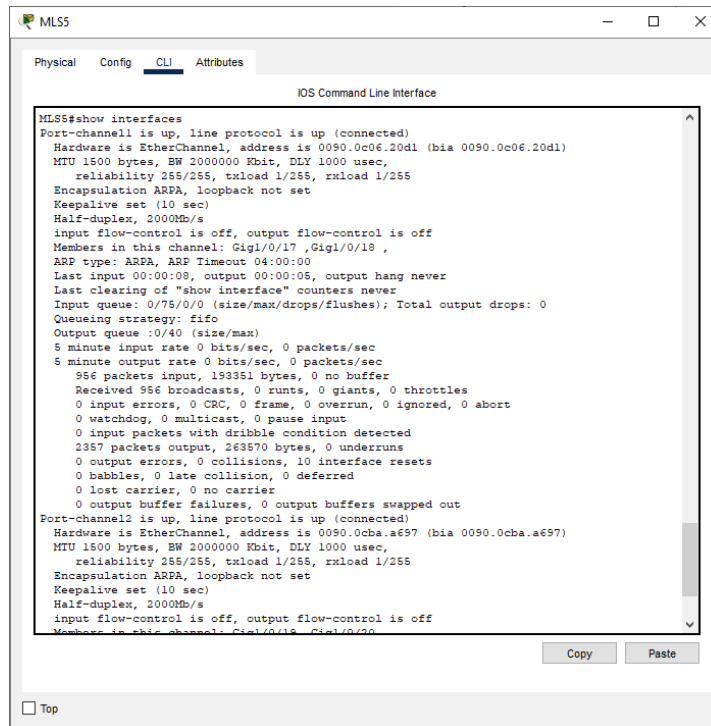


Рисунок 3.31 – Вивід команди show interfaces на MLS5

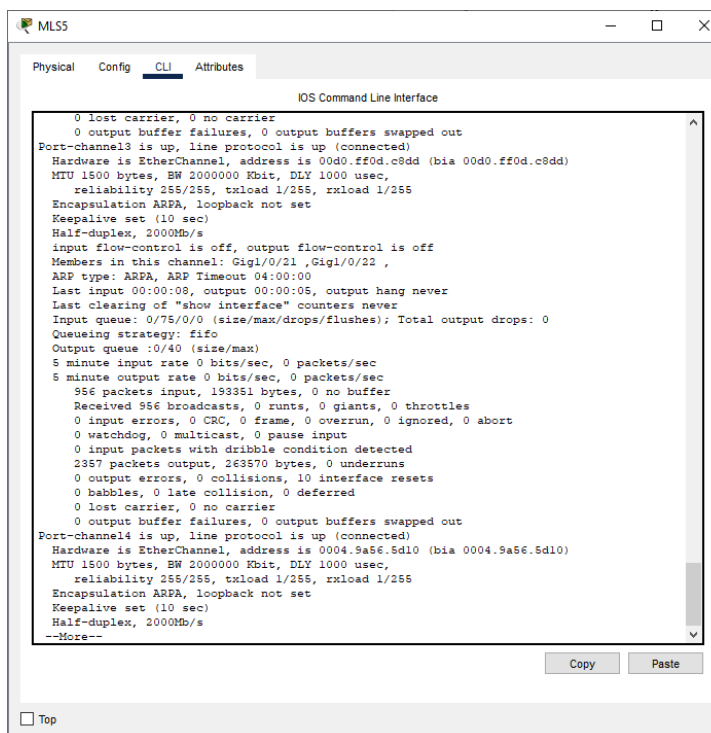


Рисунок 3.32 – Вивід команди show interfaces на MLS5

		Охремчук Є.М.					Арк.
		Єфіменко А.А.				ККІК.КР.Б – 125 – 14 - ПЗ	77
Змн.	Арк.	№ докум.	Підпис	Дата			

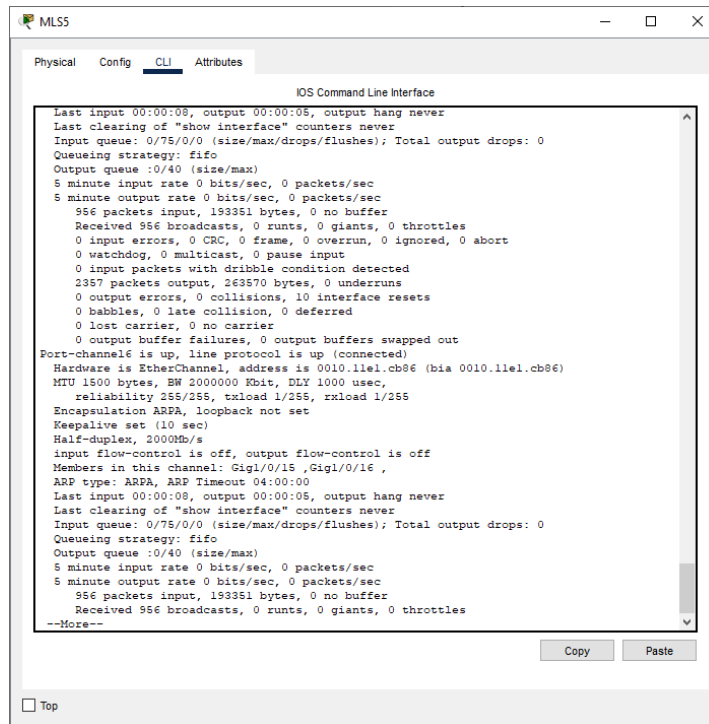


Рисунок 3.33 – Вивід команди show interfaces на MLS5

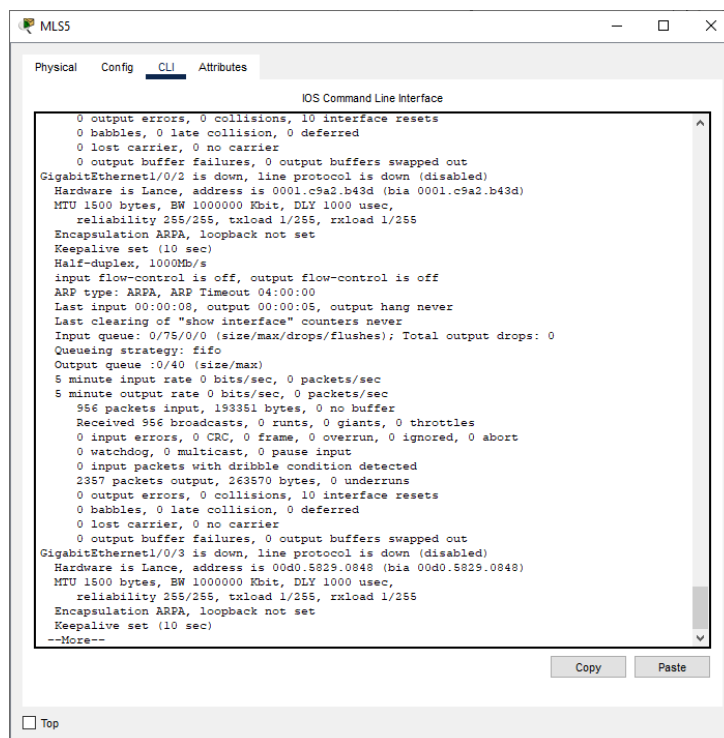


Рисунок 3.34 – Вивід команди show interfaces на MLS5

Висновок до 3 розділу: обрано обладнання Cisco Catalyst (8300, 9300, 9200L), налаштовано мережу в Cisco Packet Tracer. Тестування підтвердило працездатність коректної роботи DHCP, VLAN, NTP, Syslog, віддаленого доступу через SSH, захисту від атак, тощо.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У кваліфікаційній роботі розроблено комплексний проект захищеної корпоративної кампусної мережі з використанням комутаторів третього рівня Cisco, орієнтований на виконання сучасних вимог до продуктивності, масштабованості, безпеки, та керованості мережевої інфраструктури. Основою архітектури стала трирівнева ієрархічна модель Cisco, яка дозволяє чітко розмежовувати функції в мережі, полегшує адміністрування та забезпечує високу відмовостійкість.

Застосовано логічну сегментацію трафіку за допомогою VLAN, що підвищує рівень безпеки та дозволяє ефективно структурувати мережевий простір. Розгорнута система IPv4/IPv6-адресації забезпечує універсальність та готовність до сучасних вимог з боку прикладних сервісів. Впроваджено критично важливі служби підтримки роботи користувачів і адміністрування — DHCP, DNS, NTP, Syslog, FTP, поштові сервіси, що гарантують стабільність функціонування.

Особливу увагу приділено питанням інформаційної безпеки. Інтегровано захисні механізми другого рівня — DHCP Snooping, Dynamic ARP Inspection, Port Security, BPDU Guard, Storm Control — а також реалізовано централізовану автентифікацію користувачів на основі моделі AAA з використанням RADIUS. Забезпечено захист доступу до мережевих пристроїв через протокол SSH із використанням шифрування RSA та обмеженням кількості підключень.

Результатом виконання роботи є масштабований та безпечний шаблон інфраструктури, адаптований до середніх компаній. Запропоноване рішення здатне підтримувати підвищене навантаження, гнучко масштабуватися залежно від потреб бізнесу і ефективно протидіяти актуальним кіберзагрозам, забезпечуючи стійку та керовану мережу підприємства.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Буров Є.В. М.М. Митник. Комп'ютерні мережі : підручник. Том 1. Львів: «Магнолія 2006», 2021. 334 с.
2. Буров Є.В. М.М. Митник. Комп'ютерні мережі : підручник. Том 2. Львів: «Магнолія 2006», 2021. 204 с.
3. Lammle T. CCNA Routing and Switching Complete Study Guide. 2nd ed. – Indianapolis, IN : Sybex, 2016. 1136 с.
4. Odom W. CCNA 200-301 Official Cert Guide: Vol. 1. Indianapolis, IN : Cisco Press, 2020. 1095 с.
5. Odom W. CCNA 200-301 Official Cert Guide: Vol. 2. Indianapolis, IN : Cisco Press, 2020. 717 с.
6. Cisco Networking Academy. Switching, Routing, and Wireless Essentials: Companion Guide. Indianapolis, IN : Cisco Press, 2020. 640 с.
7. Cisco Networking Academy. Network Security Companion Guide. Indianapolis, IN : Cisco Press, 2021.
8. Gillis A. S., Loshin P., Cobb M. What is SSH (secure shell) and how does it work? *SearchSecurity*. URL: <https://www.techtarget.com/searchsecurity/definition/Secure-Shell> (дата звернення: 25.04.2025).
9. Implement AAA with TACACS server: for enterprise networks. miniOrange Security Software: Unified IAM, SSO, MFA, PAM, and CASB Solution. URL: <https://www.miniorange.com/blog/aaa-tacacs-authentication/> (дата звернення: 25.04.2025).
10. What Is VLAN (Virtual LAN)? - IT Glossary | SolarWinds. Observability, Database, and IT Service Management. SolarWinds. URL: <https://www.solarwinds.com/resources/it-glossary/vlan> (дата звернення: 25.04.2025).
11. Design zone - High availability campus network design-Routed access layer using EIGRP or OSPF. *Cisco*. URL:

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				80
Змн.	Арк.	№ док.м.	Підпис	Дата		

<https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/routed-ex.html> (дата звернення: 25.04.2025)

12. Campus Network Design: Routed Access // Cisco Validated Design. – Cisco, 2023.

URL: <https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/routed-ex.html> (дата звернення: 24.04.2025)

13. Design Zone - Enterprise Campus 3.0 Architecture: Overview and Framework. *Cisco*. URL:

<https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html> (дата звернення: 24.04.2025)

14. AI Infrastructure, Secure Networking, and Software Solutions - Cisco.

URL:

https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Small_Enterprise_Design_Profile/chap2sba.pdf (дата звернення: 25.04.2025).

15. IEEE - The world's largest technical professional organization dedicated to advancing technology for the benefit of humanity: <https://www.ieee.org/> (дата звернення: 25.04.2025).

16. Modern Campus Network Design: Scalability & Resilience Guide. *Enterprise IT Solutions & Co-Managed Services Intelligent Visibility*.

URL: <https://intelligentvisibility.com/campus-networking/resilient-design-architecture> (дата звернення: 25.04.2025).

17. IPv6 - Traditional Campus (Cisco SD-WAN and Cisco Firepower) Integration Guide. *Cisco*. URL: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/catalyst-center/cisco-validated-solution-profiles/b_cisco_validated_profile_ipv6_traditional_campus.html (дата звернення: 25.04.2025).

18. CCNP Enterprise Design ENSLD 300 - 420 Official Cert Guide: Designing Cisco Enterprise Networks. Cisco Press, 2022. 1227 с.

19. Clark K., Hamilton K. Cisco LAN Switching. Cisco Press, 1999. 960 с.

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				81
Змн.	Арк.	№ док.ум.	Підпис	Дата		

20. High-Quality 10 Gbps Campus Network Solution - Huawei Enterprise. *Huawei Enterprise*. URL: <https://e.huawei.com/ua/solutions/enterprise-network/campus-network/medium-and-large-sized-campus-network> (дата звернення: 25.04.2025).

21. Campus Network ScienceDirect. Elsevier. URL: <https://www.sciencedirect.com/topics/computer-science/campus-network> (дата звернення: 25.06.2025).

22. Cisco Catalyst 8300 Series Edge Platforms Data Sheet. *Cisco*. URL: <https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-8300-series-edge-platforms/datasheet-c78-744088.html> (дата звернення: 25.04.2025).

23. Cisco Catalyst 9300 Series Switches. *Cisco*. URL: <https://www.cisco.com/site/us/en/products/networking/switches/catalyst-9300-series-switches/index.html> (дата звернення: 25.04.2025).

24. Cisco Catalyst 9200 Series Switches Data Sheet. *Cisco*. URL: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html> (дата звернення: 25.04.2025).

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				83
Змн.	Арк.	№ док.ум.	Підпис	Дата		

Конфігураційні файли пристроїв

MLS1

Building configuration...

Current configuration : 5013 bytes

version 16.3.2

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname MLS1

logging userinfo

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

clock timezone GMT 3

no ip cef

ip routing

ipv6 unicast-routing

no ipv6 cef

username admin10 privilege 10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 privilege 13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 privilege 15 secret 5

\$1\$mERr\$Cmr5Jcu2UQ4pbE4V6OOIu1

username admin8 privilege 8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZaI1

username technic privilege 5 secret 5

\$1\$mERr\$g9HiLncvsENDvCAP1qyJx0

ip arp inspection vlan 10,20,30,40,50,77,999

ip dhcp snooping vlan 10,20,30,40,50,77,999

ip ssh version 2

ip domain-name my.net

spanning-tree mode pvst

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel3

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel4

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel5

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel6

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface GigabitEthernet1/0/1

interface GigabitEthernet1/0/2

interface GigabitEthernet1/0/3

interface GigabitEthernet1/0/4

interface GigabitEthernet1/0/5

interface GigabitEthernet1/0/6

interface GigabitEthernet1/0/7

interface GigabitEthernet1/0/8

interface GigabitEthernet1/0/9

interface GigabitEthernet1/0/10

interface GigabitEthernet1/0/11

interface GigabitEthernet1/0/12

interface GigabitEthernet1/0/13

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/14

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/15

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/16

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/17

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet1/0/18

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet1/0/19

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				84
Змн.	Арк.	№ док.ум.	Підпис	Дата		

```

ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 2 mode active
interface GigabitEthernet1/0/20
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 2 mode active
interface GigabitEthernet1/0/21
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/22
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/23
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/0/24
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/1/1
interface GigabitEthernet1/1/2
interface GigabitEthernet1/1/3
interface GigabitEthernet1/1/4
interface Vlan1
no ip address
shutdown
interface Vlan10
mac-address 0005.5e49.5801

```

```

no ip address
interface Vlan77
mac-address 0005.5e49.5802
ip address 200.24.2.2 255.255.255.192
ipv6 address 2001:DB8:0:77::2/121
interface Vlan999
mac-address 0005.5e49.5803
no ip address
shutdown
ip classless
ip flow-export version 9
logging trap debugging
logging 200.24.2.21
logging 200.24.2.22
line con 0
login local
line aux 0
line vty 0 4
logging synchronous
login local
ntp authentication-key 2506 md5 08314D5D1A 7
ntp authenticate
ntp trusted-key 2506
ntp server 200.24.2.21 key 2506
ntp update-calendar
End

```

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				85
Змн.	Арк.	№ док.ум.	Підпис	Дата		

MLS2

Building configuration...

Current configuration : 4986 bytes

version 16.3.2

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname MLS2

logging userinfo

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

clock timezone GMT 3

no ip cef

ip routing

ipv6 unicast-routing

no ipv6 cef

username admin10 privilege 10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 privilege 13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 privilege 15 secret 5

\$1\$mERr\$cMr5Jcu2UQ4pbE4V6OOIu1

username admin8 privilege 8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZa11

username technic privilege 5 secret 5

\$1\$mERr\$g9HiLncvsENDvCAP1qyJx0

ip arp inspection vlan 10,20,30,40,50,77,999

ip dhcp snooping vlan 10,20,30,40,50,77,999

ip ssh version 2

ip domain-name my.net

spanning-tree mode pvst

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel3

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel4

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel5

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel6

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface GigabitEthernet1/0/1

interface GigabitEthernet1/0/2

interface GigabitEthernet1/0/3

interface GigabitEthernet1/0/4

interface GigabitEthernet1/0/5

interface GigabitEthernet1/0/6

interface GigabitEthernet1/0/7

interface GigabitEthernet1/0/8

interface GigabitEthernet1/0/9

interface GigabitEthernet1/0/10

interface GigabitEthernet1/0/11

interface GigabitEthernet1/0/12

interface GigabitEthernet1/0/13

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/14

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/15

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/16

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/17

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet1/0/18

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet1/0/19

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 2 mode active

interface GigabitEthernet1/0/20

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				86
Змн.	Арк.	№ док.ум.	Підпис	Дата		

```

ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 2 mode active
interface GigabitEthernet1/0/21
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/22
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/23
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/0/24
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/1/1
interface GigabitEthernet1/1/2
interface GigabitEthernet1/1/3
interface GigabitEthernet1/1/4
interface Vlan1
no ip address
shutdown
interface Vlan77
mac-address 00e0.f9b1.0501
ip address 200.24.2.3 255.255.255.192
ipv6 address 2001:DB8:0:77::2/121
ipv6 address 2001:DB8:0:77::3/121
interface Vlan999
mac-address 00e0.f9b1.0502
no ip address
shutdown
ip classless

```

```

ip flow-export version 9
logging trap debugging
logging 200.24.2.21
logging 200.24.2.22
line con 0
login local
line aux 0
line vty 0 4
logging synchronous
login local
ntp authentication-key 2506 md5 08314D5D1A 7
ntp authenticate
ntp trusted-key 2506
ntp server 200.24.2.21 key 2506
ntp update-calendar
End

```

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				87
Змн.	Арк.	№ док.ум.	Підпис	Дата		

MLS3

Building configuration...

Current configuration : 5019 bytes

version 16.3.2

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname MLS3

logging userinfo

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

clock timezone GMT 3

no ip cef

ip routing

ipv6 unicast-routing

no ipv6 cef

username admin10 privilege 10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 privilege 13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 privilege 15 secret 5

\$1\$mERr\$cMr5Jcu2UQ4pbE4V6OOIu1

username admin8 privilege 8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZa11

username technic privilege 5 secret 5

\$1\$mERr\$g9HiLncvsENDvCAP1qyJx0

ip arp inspection vlan 10,20,30,40,50,77,999

ip dhcp snooping vlan 10,20,30,40,50,77,999

ip ssh version 2

ip domain-name my.net

spanning-tree mode pvst

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel3

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel4

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel5

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel6

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface GigabitEthernet1/0/1

interface GigabitEthernet1/0/2

interface GigabitEthernet1/0/3

interface GigabitEthernet1/0/4

interface GigabitEthernet1/0/5

interface GigabitEthernet1/0/6

interface GigabitEthernet1/0/7

interface GigabitEthernet1/0/8

interface GigabitEthernet1/0/9

interface GigabitEthernet1/0/10

interface GigabitEthernet1/0/11

interface GigabitEthernet1/0/12

interface GigabitEthernet1/0/13

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/14

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/15

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/16

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/17

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet1/0/18

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet1/0/19

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 2 mode active

interface GigabitEthernet1/0/20

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				88
Змн.	Арк.	№ докum.	Підпис	Дата		

```

ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 2 mode active
interface GigabitEthernet1/0/21
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/22
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/23
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/0/24
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/1/1
interface GigabitEthernet1/1/2
interface GigabitEthernet1/1/3
interface GigabitEthernet1/1/4
interface Vlan1
no ip address
shutdown
interface Vlan77
mac-address 0001.970b.e401
ip address 200.24.2.4 255.255.255.192
ipv6 address 2001:DB8:0:77::2/121
ipv6 address 2001:DB8:0:77::4/121
interface Vlan999
mac-address 0001.970b.e402
no ip address
shutdown
router eigrp 100

```

```

auto-summary
ip classless
ip flow-export version 9

logging trap debugging
logging 200.24.2.21
logging 200.24.2.22
line con 0
login local
line aux 0
line vty 0 4
logging synchronous
login local
ntp authentication-key 2506 md5 08314D5D1A 7
ntp authenticate
ntp trusted-key 2506
ntp server 200.24.2.21 key 2506
ntp update-calendar
End

```

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				89
Змн.	Арк.	№ док.ум.	Підпис	Дата		

MLS4

Building configuration...

Current configuration : 6102 bytes

version 16.3.2

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname MLS4

logging userinfo

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

ip dhcp excluded-address 200.24.0.1

ip dhcp excluded-address 200.24.0.129

ip dhcp pool POOL10

network 200.24.0.0 255.255.255.128

default-router 200.24.0.1

dns-server 200.24.2.21

domain-name my.net

ip dhcp pool POOL20

network 200.24.0.128 255.255.255.128

default-router 200.24.0.129

dns-server 200.24.2.21

domain-name my.net

clock timezone GMT 3

no ip cef

ip routing

ipv6 unicast-routing

no ipv6 cef

ipv6 dhcp pool POOL10v6

address prefix 2001:db8:0:10::/121 lifetime 172800
86400

dns-server 2001:DB8:0:77::21

domain-name my.net

ipv6 dhcp pool POOL20v6

address prefix 2001:db8:0:20::/121 lifetime 172800
86400

dns-server 2001:DB8:0:77::21

domain-name my.net

username admin10 privilege 10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 privilege 13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 privilege 15 secret 5

\$1\$mERr\$Cmr5Jcu2UQ4pbE4V6OOIu1

username admin8 privilege 8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZaI1

username technic privilege 5 secret 5

\$1\$mERr\$g9HiLncvsENDvCAP1qyJx0

ip arp inspection vlan 10,20,30,40,50,77,999

ip dhcp snooping vlan 10,20,30,40,50,77,999

ip ssh version 2

ip domain-name my.net

spanning-tree mode pvst

spanning-tree vlan 10,20 priority 4096

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel3

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel4

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel5

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel6

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface GigabitEthernet1/0/1

...

interface GigabitEthernet1/0/13

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/14

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/15

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/16

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/17

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet1/0/18

ip arp inspection trust

ip dhcp snooping trust

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				90
Змн.	Арк.	№ докum.	Підпис	Дата		

```

ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 1 mode active
interface GigabitEthernet1/0/19
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 2 mode active
interface GigabitEthernet1/0/20
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 2 mode active
interface GigabitEthernet1/0/21
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/22
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/23
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/0/24
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/1/1
interface GigabitEthernet1/1/2
interface GigabitEthernet1/1/3

```

```

interface GigabitEthernet1/1/4
interface Vlan1
no ip address
shutdown
interface Vlan10
mac-address 000a.f374.9101
ip address 200.24.0.1 255.255.255.128
ipv6 address 2001:DB8:0:10::1/121
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server POOL10v6
interface Vlan20
mac-address 000a.f374.9102
ip address 200.24.0.129 255.255.255.128
ipv6 address 2001:DB8:0:20::1/121
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server POOL20v6
interface Vlan77
mac-address 000a.f374.9103
ip address 200.24.2.5 255.255.255.192
ipv6 address 2001:DB8:0:77::2/121
ipv6 address 2001:DB8:0:77::5/121
interface Vlan999
mac-address 000a.f374.9104
no ip address
shutdown
router eigrp 100
network 200.24.0.0 0.0.0.127
network 200.24.0.128 0.0.0.127
auto-summary
ip classless
ip flow-export version 9
logging trap debugging
logging 200.24.2.21
logging 200.24.2.22
line con 0
login local
line aux 0
line vty 0 4
logging synchronous
login local
ntp authentication-key 2506 md5 08314D5D1A 7
ntp authenticate
ntp trusted-key 2506
ntp server 200.24.2.21 key 2506
ntp update-calendar
End

```

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				91
Змн.	Арк.	№ док.ум.	Підпис	Дата		

MLS5

Building configuration...

Current configuration : 6071 bytes

version 16.3.2

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname MLS5

logging userinfo

enable secret 5

\$1\$mERr\$WWYFDFfled5FpJh6NNHr41

ip dhcp excluded-address 200.24.1.1

ip dhcp excluded-address 200.24.1.65

ip dhcp pool VLAN30

network 200.24.1.0 255.255.255.192

default-router 200.24.1.1

dns-server 200.24.2.21

domain-name my.net

ip dhcp pool VLAN40

network 200.24.1.64 255.255.255.192

default-router 200.24.1.65

domain-name my.net

clock timezone GMT 3

no ip cef

ip routing

ipv6 unicast-routing

no ipv6 cef

ipv6 dhcp pool POOL30v6

address prefix 2001:db8:0:30::/121 lifetime 172800
86400

dns-server 2001:DB8:0:77::21

domain-name my.net

ipv6 dhcp pool POOL40v6

address prefix 2001:db8:0:40::/121 lifetime 172800
86400

dns-server 2001:DB8:0:77::21

domain-name my.net

username admin10 privilege 10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 privilege 13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 privilege 15 secret 5

\$1\$mERr\$Cmr5Jcu2UQ4pbE4V6OOIu1

username admin8 privilege 8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZa11

username technic privilege 5 secret 5

\$1\$mERr\$g9HiLncvsENDvCAP1qyJx0

ip arp inspection vlan 10,20,30,40,50,77,999

ip dhcp snooping vlan 10,20,30,40,50,77,999

ip ssh version 2

ip domain-name my.net

spanning-tree mode pvst

spanning-tree vlan 30,40 priority 4096

interface Port-channel1

switchport trunk allowed vlan
10,20,30,40,50,60,77,999

switchport mode trunk
interface Port-channel2

switchport trunk allowed vlan
10,20,30,40,50,60,77,999

switchport mode trunk
interface Port-channel3

switchport trunk allowed vlan
10,20,30,40,50,60,77,999

switchport mode trunk
interface Port-channel4

switchport trunk allowed vlan
10,20,30,40,50,60,77,999

switchport mode trunk
interface Port-channel5

switchport trunk allowed vlan
10,20,30,40,50,60,77,999

switchport mode trunk
interface Port-channel6

switchport trunk allowed vlan
10,20,30,40,50,60,77,999

switchport mode trunk
interface GigabitEthernet1/0/1

...

interface GigabitEthernet1/0/13

switchport trunk allowed vlan
10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/14

switchport trunk allowed vlan
10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/15

switchport trunk allowed vlan
10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/16

switchport trunk allowed vlan
10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/17

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport trunk allowed vlan
10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet1/0/18

ip arp inspection trust

ip dhcp snooping trust

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				92
Змн.	Арк.	№ докum.	Підпис	Дата		

```

ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 1 mode active
interface GigabitEthernet1/0/19
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 2 mode active
interface GigabitEthernet1/0/20
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 2 mode active
interface GigabitEthernet1/0/21
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/22
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/23
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/0/24
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/1/1
interface GigabitEthernet1/1/2
interface GigabitEthernet1/1/3

```

```

interface GigabitEthernet1/1/4
interface Vlan1
no ip address
shutdown
interface Vlan30
mac-address 00d0.58a6.9b01
ip address 200.24.1.1 255.255.255.192
ipv6 address 2001:DB8:0:30::1/121
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server POOL30v6
interface Vlan40
mac-address 00d0.58a6.9b02
ip address 200.24.1.65 255.255.255.192
ipv6 address 2001:DB8:0:40::1/121
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server POOL40v6
interface Vlan77
mac-address 00d0.58a6.9b03
ip address 200.24.2.6 255.255.255.192
ipv6 address 2001:DB8:0:77::2/121
ipv6 address 2001:DB8:0:77::6/121
interface Vlan999
mac-address 00d0.58a6.9b04
no ip address
shutdown
router eigrp 100
network 200.24.1.0 0.0.0.63
network 200.24.1.64 0.0.0.63
auto-summary
ip classless
ip flow-export version 9

```

```

logging trap debugging
logging 200.24.2.21
logging 200.24.2.22
line con 0
login local
line aux 0
line vty 0 4
logging synchronous
login local

```

```

ntp authentication-key 2506 md5 08314D5D1A 7
ntp authenticate
ntp trusted-key 2506
ntp server 200.24.2.21 key 2506
ntp update-calendar
End

```

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				93
Змн.	Арк.	№ докum.	Підпис	Дата		

MLS6

Building configuration...

Current configuration : 6110 bytes

version 16.3.2

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname MLS6

logging userinfo

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

ip dhcp excluded-address 200.24.1.129

ip dhcp excluded-address 200.24.1.193

ip dhcp pool VLAN50

network 200.24.1.128 255.255.255.192

default-router 200.24.1.129

dns-server 200.24.2.21

domain-name my.net

ip dhcp pool VLAN60

network 200.24.1.192 255.255.255.192

default-router 200.24.1.193

dns-server 200.24.2.21

domain-name my.net

clock timezone GMT 3

no ip cef

ip routing

ipv6 unicast-routing

no ipv6 cef

ipv6 dhcp pool POOL50v6

address prefix 2001:db8:0:50::/121 lifetime 172800
86400

dns-server 2001:DB8:0:77::21

domain-name my.net

ipv6 dhcp pool POOL60v6

address prefix 2001:db8:0:60::/121 lifetime 172800
86400

dns-server 2001:DB8:0:77::21

domain-name my.net

username admin10 privilege 10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 privilege 13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 privilege 15 secret 5

\$1\$mERr\$Cmr5Jcu2UQ4pbE4V6OOIu1

username admin8 privilege 8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZaI1

username technic privilege 5 secret 5

\$1\$mERr\$g9HiLncvsENDvCAP1qyJx0

ip arp inspection vlan 10,20,30,40,50,77,999

ip dhcp snooping vlan 10,20,30,40,50,77,999

ip ssh version 2

ip domain-name my.net

spanning-tree mode pvst

spanning-tree vlan 50,60 priority 4096

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel3

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel4

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel5

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface Port-channel6

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface GigabitEthernet1/0/1

...

interface GigabitEthernet1/0/13

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/14

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 5 mode active

interface GigabitEthernet1/0/15

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/16

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 6 mode active

interface GigabitEthernet1/0/17

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet1/0/18

ip arp inspection trust

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				94
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 1 mode active
interface GigabitEthernet1/0/19
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 2 mode active
interface GigabitEthernet1/0/20
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 2 mode active
interface GigabitEthernet1/0/21
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/22
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 3 mode active
interface GigabitEthernet1/0/23
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/0/24
ip arp inspection trust
ip dhcp snooping trust
ip dhcp snooping limit rate 256
switchport trunk allowed vlan
10,20,30,40,50,60,77,999
switchport mode trunk
channel-group 4 mode active
interface GigabitEthernet1/1/1
interface GigabitEthernet1/1/2

```

```

interface GigabitEthernet1/1/3
interface GigabitEthernet1/1/4
interface Vlan1
no ip address
shutdown
interface Vlan50
mac-address 0010.11ee.1b01
ip address 200.24.1.129 255.255.255.192
ipv6 address 2001:DB8:0:50::1/121
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server POOL50v6
interface Vlan60
mac-address 0010.11ee.1b02
ip address 200.24.1.193 255.255.255.192
ipv6 address 2001:DB8:0:60::1/121
ipv6 nd managed-config-flag
ipv6 enable
ipv6 dhcp server POOL60v6
interface Vlan77
mac-address 0010.11ee.1b03
ip address 200.24.2.7 255.255.255.192
ipv6 address 2001:DB8:0:77::2/121
ipv6 address 2001:DB8:0:77::7/121
interface Vlan999
mac-address 0010.11ee.1b04
no ip address
shutdown
router eigrp 100
network 200.24.1.128 0.0.0.63
network 200.24.1.192 0.0.0.63
auto-summary
ip classless
ip flow-export version 9
logging trap debugging
logging 200.24.2.21
logging 200.24.2.22
line con 0
login local
line aux 0
line vty 0 4
logging synchronous
login local
ntp authentication-key 2506 md5 08314D5D1A 7
ntp authenticate
ntp trusted-key 2506
ntp server 200.24.2.21 key 2506
ntp update-calendar
End

```

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

SW7

Building configuration...

Current configuration : 3048 bytes

version 15.0

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname SW7

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

aaa new-model

clock timezone GMT 3

mls qos

ip ssh version 2

ip domain-name mynet.net

username admin10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 secret 5

\$1\$mERr\$cMr5Jcu2UQ4pbE4V6OOIu1

username admin8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZa11

username technic secret 5

\$1\$mERr\$H8ID5fTpWRo6mb13JWuF6/

ip arp inspection vlan 10,20,30,40,50,60,77,999

ip dhcp snooping vlan 10,20,30,40,50,60,77,999

spanning-tree mode pvst

spanning-tree extend system-id

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface FastEthernet0/1

switchport access vlan 77

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/2

switchport access vlan 77

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/3

switchport access vlan 77

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/4

switchport access vlan 77

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/5

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

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet0/1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet0/2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface Vlan1

no ip address

shutdown

interface Vlan77

ip address 200.24.2.15 255.255.255.192

no cdp run

logging trap debugging

logging 200.24.2.21

logging 200.24.2.22

line con 0

login

line vty 0 4

logging synchronous

login authentication switchlogin

line vty 5 15

ntp authenticate

ntp trusted-key 2506

ntp server 200.24.2.21 key 2506

end

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				96
Змн.	Арк.	№ док.ум.	Підпис	Дата		

SW1

Building configuration...

Current configuration : 2823 bytes

version 15.0

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname SW1

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

aaa new-model

clock timezone GMT 3

ip ssh version 2

ip domain-name mynet.net

username admin10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 secret 5

\$1\$mERr\$cMr5Jcu2UQ4pbE4V6OOIu1

username admin8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZa11

username technic secret 5

\$1\$mERr\$H8ID5fTpWRo6mb13JWuF6/

ip arp inspection vlan 10,20,30,40,50,60,77,999

ip dhcp snooping vlan 10,20,30,40,50,60,77,999

spanning-tree mode pvst

spanning-tree extend system-id

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface FastEthernet0/1

switchport access vlan 10

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/2

switchport access vlan 10

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

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

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet0/1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet0/2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface Vlan1

no ip address

shutdown

interface Vlan77

ip address 200.24.2.9 255.255.255.192

no cdp run

logging trap debugging

logging 200.24.2.21

logging 200.24.2.22

line con 0

login

line vty 0 4

logging synchronous

login authentication switchlogin

line vty 5 15

ntp authenticate

ntp trusted-key 2506

ntp server 200.24.2.21 key 2506

End

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				97
Змн.	Арк.	№ докум.	Підпис	Дата		

SW2

Building configuration...

Current configuration : 2824 bytes

version 15.0

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname SW2

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

aaa new-model

clock timezone GMT 3

ip ssh version 2

ip domain-name mynet.net

username admin10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 secret 5

\$1\$mERr\$cMr5Jcu2UQ4pbE4V6OOIu1

username admin8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZa11

username technic secret 5

\$1\$mERr\$H8ID5fTpWRo6mb13JWuF6/

ip arp inspection vlan 10,20,30,40,50,60,77,999

ip dhcp snooping vlan 10,20,30,40,50,60,77,999

spanning-tree mode pvst

spanning-tree extend system-id

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface FastEthernet0/1

switchport access vlan 20

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/2

switchport access vlan 20

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

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

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet0/1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet0/2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface Vlan1

no ip address

shutdown

interface Vlan77

ip address 200.24.2.10 255.255.255.192

no cdp run

logging trap debugging

logging 200.24.2.21

logging 200.24.2.22

line con 0

login

line vty 0 4

logging synchronous

login authentication switchlogin

line vty 5 15

ntp authenticate

ntp trusted-key 2506

ntp server 200.24.2.21 key 2506

End

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				98
Змн.	Арк.	№ докум.	Підпис	Дата		

SW3

Building configuration...

Current configuration : 2824 bytes

version 15.0

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname SW3

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

aaa new-model

clock timezone GMT 3

ip ssh version 2

ip domain-name mynet.net

username admin10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 secret 5

\$1\$mERr\$cMr5Jcu2UQ4pbE4V6OOIu1

username admin8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZa11

username technic secret 5

\$1\$mERr\$H8ID5fTpWRo6mb13JWuF6/

ip arp inspection vlan 10,20,30,40,50,60,77,999

ip dhcp snooping vlan 10,20,30,40,50,60,77,999

spanning-tree mode pvst

spanning-tree extend system-id

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface FastEthernet0/1

switchport access vlan 30

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/2

switchport access vlan 30

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

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

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet0/1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet0/2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface Vlan1

no ip address

shutdown

interface Vlan77

ip address 200.24.2.11 255.255.255.192

no cdp run

logging trap debugging

logging 200.24.2.21

logging 200.24.2.22

line con 0

login

line vty 0 4

logging synchronous

login authentication switchlogin

line vty 5 15

ntp authenticate

ntp trusted-key 2506

ntp server 200.24.2.21 key 2506

End

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				99
Змн.	Арк.	№ докум.	Підпис	Дата		

SW6

Building configuration...

Current configuration : 2824 bytes

version 15.0

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname SW6

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

aaa new-model

clock timezone GMT 3

ip ssh version 2

ip domain-name mynet.net

username admin10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 secret 5

\$1\$mERr\$cMr5Jcu2UQ4pbE4V6OOIu1

username admin8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZa11

username technic secret 5

\$1\$mERr\$H8ID5fTpWRo6mb13JWuF6/

ip arp inspection vlan 10,20,30,40,50,60,77,999

ip dhcp snooping vlan 10,20,30,40,50,60,77,999

spanning-tree mode pvst

spanning-tree extend system-id

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface FastEthernet0/1

switchport access vlan 60

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/2

switchport access vlan 60

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

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

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet0/1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet0/2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface Vlan1

no ip address

shutdown

interface Vlan77

ip address 200.24.2.14 255.255.255.192

no cdp run

logging trap debugging

logging 200.24.2.21

logging 200.24.2.22

line con 0

login

line vty 0 4

logging synchronous

login authentication switchlogin

line vty 5 15

ntp authenticate

ntp trusted-key 2506

ntp server 200.24.2.21 key 2506

end

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				100
Змн.	Арк.	№ докум.	Підпис	Дата		

SW4

Building configuration...

Current configuration : 2824 bytes

version 15.0

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname SW4

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

aaa new-model

clock timezone GMT 3

ip ssh version 2

ip domain-name mynet.net

username admin10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 secret 5

\$1\$mERr\$cMr5Jcu2UQ4pbE4V6OOIu1

username admin8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZa11

username technic secret 5

\$1\$mERr\$H8ID5fTpWRo6mb13JWuF6/

ip arp inspection vlan 10,20,30,40,50,60,77,999

ip dhcp snooping vlan 10,20,30,40,50,60,77,999

spanning-tree mode pvst

spanning-tree extend system-id

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface FastEthernet0/1

switchport access vlan 40

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/2

switchport access vlan 40

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

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

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet0/1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet0/2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface Vlan1

no ip address

shutdown

interface Vlan77

ip address 200.24.2.12 255.255.255.192

no cdp run

logging trap debugging

logging 200.24.2.21

logging 200.24.2.22

line con 0

login

line vty 0 4

logging synchronous

login authentication switchlogin

line vty 5 15

ntp authenticate

ntp trusted-key 2506

ntp server 200.24.2.21 key 2506

End

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				101
Змн.	Арк.	№ докум.	Підпис	Дата		

R1

Building configuration...

Current configuration : 931 bytes

version 15.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname R1

no ip cef

no ipv6 cef

spanning-tree mode pvst

interface GigabitEthernet0/0/0

ip address 200.24.2.1 255.255.255.192

ip nat inside

duplex auto

speed auto

interface GigabitEthernet0/0/1

ip address 192.169.1.1 255.255.255.252

duplex auto

speed auto

interface GigabitEthernet0/0/2

no ip address

duplex auto

speed auto

shutdown

interface Serial0/1/0

ip address 192.167.0.1 255.255.0.0

ip nat outside

clock rate 2000000

interface Serial0/1/1

ip address 192.168.0.1 255.255.0.0

ip nat outside

clock rate 2000000

interface Vlan1

no ip address

shutdown

ip nat inside source static 200.24.2.1 192.168.0.1

ip classless

ip flow-export version 9

line con 0

line aux 0

line vty 0 4

login

end

R2#show run

Building configuration...

Current configuration : 933 bytes

version 15.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname R2

no ip cef

no ipv6 cef

spanning-tree mode pvst

interface GigabitEthernet0/0/0

ip address 200.24.2.17 255.255.255.192

ip nat inside

duplex auto

speed auto

interface GigabitEthernet0/0/1

ip address 192.169.1.2 255.255.255.252

duplex auto

speed auto

interface GigabitEthernet0/0/2

no ip address

duplex auto

speed auto

shutdown

interface Serial0/1/0

ip address 192.167.0.2 255.255.0.0

ip nat outside

clock rate 2000000

interface Serial0/1/1

ip address 192.168.0.2 255.255.0.0

ip nat outside

clock rate 2000000

interface Vlan1

no ip address

shutdown

ip nat inside source static 200.24.2.17 192.168.0.1

ip classless

ip flow-export version 9

line con 0

line aux 0

line vty 0 4

login

End

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				102
Змн.	Арк.	№ докum.	Підпис	Дата		

SW5

Building configuration...

Current configuration : 2824 bytes

version 15.0

service timestamps log datetime msec

service timestamps debug datetime msec

no service password-encryption

hostname SW5

enable secret 5

\$1\$mERr\$WWYFDFfcd5FpJh6NNHr41

aaa new-model

clock timezone GMT 3

ip ssh version 2

ip domain-name mynet.net

username admin10 secret 5

\$1\$mERr\$iwKHMfY4StAVIS45.UiGP0

username admin13 secret 5

\$1\$mERr\$gldpGvrPKHTng/vsetUcP.

username admin15 secret 5

\$1\$mERr\$cMr5Jcu2UQ4pbE4V6OOIu1

username admin8 secret 5

\$1\$mERr\$YDQwEjMa.4d9OwXR2rZa11

username technic secret 5

\$1\$mERr\$H8ID5fTpWRo6mb13JWuF6/

ip arp inspection vlan 10,20,30,40,50,60,77,999

ip dhcp snooping vlan 10,20,30,40,50,60,77,999

spanning-tree mode pvst

spanning-tree extend system-id

interface Port-channel1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

switchport mode trunk

interface FastEthernet0/1

switchport access vlan 50

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/2

switchport access vlan 50

switchport mode access

spanning-tree portfast

spanning-tree bpduguard enable

interface FastEthernet0/3

interface FastEthernet0/4

interface FastEthernet0/5

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

interface FastEthernet0/22

interface FastEthernet0/23

interface FastEthernet0/24

interface GigabitEthernet0/1

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface GigabitEthernet0/2

switchport trunk allowed vlan

10,20,30,40,50,60,77,999

ip arp inspection trust

ip dhcp snooping trust

ip dhcp snooping limit rate 256

switchport mode trunk

channel-group 1 mode active

interface Vlan1

no ip address

shutdown

interface Vlan77

ip address 200.24.2.13 255.255.255.192

no cdp run

logging trap debugging

logging 200.24.2.21

logging 200.24.2.22

line con 0

login

line vty 0 4

logging synchronous

login authentication switchlogin

line vty 5 15

ntp authenticate

ntp trusted-key 2506

ntp server 200.24.2.21 key 2506

end

		Охремчук Є.М.			ККІК.КР.Б – 125 – 14 - ПЗ	Арк.
		Єфіменко А.А.				103
Змн.	Арк.	№ докум.	Підпис	Дата		