

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет комп'ютерних наук та технологій
(повне найменування факультету)

Кафедра комп'ютерних систем та мереж
(повне найменування кафедри)

Пояснювальна записка
до дипломного проекту (роботи)
бакалавра
(ступінь вищої освіти (освітній ступінь))

на тему **МОДЕРНІЗАЦІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ**
ЗАПОРІЗЬКОГО АВІАЦІЙНОГО ФАХОВОГО КОЛЕДЖУ

Виконав: студент 4 курсу, групи КНТ-511сп
спеціальності _____

123 «Комп'ютерна інженерія»
(код і найменування спеціальності)

Освітня програма (спеціалізація) _____
«Комп'ютерна інженерія»

(ПРИЗВИЩЕ та ініціали)

Керівник ТЯГУНОВА М. Ю.
(ПРИЗВИЩЕ та ініціали)

Рецензент МАЛИЙ О.Ю.
(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування вищого навчального закладу)

Факультет Комп'ютерних наук і технологій
Кафедра «Комп'ютерні системи та мережі»
Ступінь вищої освіти бакалаврський
Спеціальність 123 Комп'ютерна інженерія
(код і найменування)
Освітня програма (спеціалізація) Комп'ютерна інженерія
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри КУДЕРМЕТОВ Р.К.

“ ” 2024 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

КОСЯКА Антона Костянтиновича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Модернізація комп'ютерної мережі Запорізького авіаційного фахового коледжу

керівник проєкту (роботи) к. т. н., доцент, ТЯГУНОВА Марія Юріївна

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом вищого навчального закладу від “01” квітня 2024 року № 105

2. Строк подання студентом проєкту (роботи) 10 травня 2024 року

3. Вихідні дані до проєкту (роботи) 3 маршрутизатори, 8 комутаторів, 42 комп'ютери, 3 сервери (DNS, поштовий сервер, веб сервер), Wi-fi роутер, вита пара, статична маршрутизація.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1) Аналіз предметної області;

2) Апаратне забезпечення комп'ютерної мережі;

3) Програмне забезпечення кінцевих користувачів;

4) Проектування комп'ютерної мережі;

5) Монтаж локальної мережі.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Плакати 1. Структурна схема мережі;

Плакати 2. Схема приєднування мережі;

Плакати 3. Загальна модель мережі;

Плакати 4. Адміністрування (керування) мережею.

6. Консультанти розділів проекту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	ТЯГУНОВА М. Ю., к.т.н., доцент		
нормоконтроль	ЩЕРБАК Н.В., ст. викл.		

7. Дата видачі завдання 01.03.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Отримання завдання	01.03.2024 р.	
2	Збір інформації	15.03.2024 р.	
3	Аналіз технічного завдання та потреби підприємства	20.03.2024 р.	
4	Апаратне забезпечення комп'ютерної мережі	01.04.2024 р.	
5	Програмне забезпечення комп'ютерної мережі	10.04.2024 р.	
6	Проектування комп'ютерної мережі	01.05.2024 р.	
7	Оформлення отриманих результатів у ПЗ	10.05.2024 р.	
8	Оформлення графічного матеріалу	17.05.2023 р.	

Студент (ка)


(підпис)

Антон КОСЯК
(Ім'я ПРІЗВИЩЕ)

Керівник проекту (роботи)


(підпис)

Марія ТЯГУНОВА
(Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

ПЗ: 77 с., 31 рис., 6 табл., 10 джерел.

ETHERNET, LAN, ВИТА ПАРА, КОМП'ЮТЕРНА МЕРЕЖА,
КОМУТАТОР, МАРШРУТИЗАТОР, РОБОЧА СТАНЦІЯ, СЕРВЕР

Об'єкт розробки – структурована локальна мережа Запорізького авіаційного фахового коледжу.

Метою дипломної роботи виступає модернізація комп'ютерної мережі Запорізького фахового авіаційного коледжу.

У першому розділі проведено аналіз існуючої мережі у Запорізькому авіаційному фаховому коледжі, враховуючи її основні характеристики та поточний стан.

У другому розділі надано детальне пояснення використаних мережевих технологій у контексті коледжу та проведено їхній аналіз з урахуванням потреб удосконалення.

У третьому розділі висвітлено апаратну сторону комп'ютерної мережі на підприємстві, описано використане обладнання та представлено перелік програмного забезпечення з метою забезпечення ефективної роботи мережі.

Четвертий розділ присвячено моделюванню локальної мережі в емуляторі Packet Tracer, а також виявленню існуючих недоліків у роботі мережі. Додатково розглянуто рекомендації щодо покращення функціонування мережі та її адаптації до сучасних потреб.

У п'ятому розділі надано практичні кроки та поради щодо монтажу локальної мережі на основі проведених досліджень та аналізу потреб відповідного закладу.

ЗМІСТ

Скорочення та умовні позначки.....	7
Вступ.....	8
1 Аналіз предметної області.....	11
1.1 Аналіз існуючої мережі.....	11
1.2 Призначення та цілі модернізації мережі.....	13
1.3 Постановка задачі.....	17
2 Апаратне забезпечення комп'ютерної мережі.....	18
2.1 Загальні принципи побудови локальних мереж.....	18
2.2 Аналіз наявних LAN технологій.....	20
2.3 Вибір середовища передачі даних	23
2.4 Вибір топології мережі.....	30
2.5 Дослідження та аналіз характеристик, вибір мережевих пристроїв.....	35
3 Програмне забезпечення кінцевих користувачів.....	40
3.1 Вибір програмного забезпечення для робочих станцій в мережі.....	39
3.1.1 Операційна система Microsoft Windows 10 Professional.....	39
3.1.2 Операційна система Microsoft Windows Server 2019.....	41
3.1.3 Антивірус ESET Endpoint Security.....	41
3.1.4 Пакет Microsoft Office 2019.....	43
3.1.5 Системний монітор Sysmon.....	44
3.2 Моделювання комп'ютерної мережі в програмі Cisco Packet Tracer....	46
3.3 Огляд існуючих аналогів для проектування мереж.....	49
4 Проектування комп'ютерної мережі.....	52
4.1 Опис проектування комп'ютерної мережі.....	52
4.2 Адресація комп'ютерної мережі.....	53

4.3 Налаштування динамічної адресації.....	55
4.4 Налаштування VLAN.....	55
4.5 Налаштування протоколу тунелювання.....	57
4.6 Налаштування сервісів.....	59
4.7 Перевірка працездатності мережі.....	68
5 Монтаж локальної мережі.....	69
5.1 Підключення розетки RJ – 45.....	69
5.2 Монтаж оптоволоконних конекторів.....	72
5.3 Підключення мережевого обладнання.....	74
Висновки.....	76
Перелік джерел посилання.....	77
Перелік графічних матеріалів:	
Плакат 1 – Структурна схема мережі	
Плакат 2 – Схема приєднування мережі	
Плакат 3 – Загальна модель мережі	
Плакат 4 – Адміністрування (керування) мережею	

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧКИ

TCP/IP	–	Transmission Control Protocol / Internet Protocol.
IP	–	Internet Protocol
MAC	–	Media Access Control
ПК	–	Персональний комп'ютер
ОС	–	Операційна система
DNS	–	Domain Name System
OSI	–	The Open Systems Interconnection model
HTTP	–	HyperText Transfer Protocol
LAN	–	Локальна обчислювальна мережа
WAN	–	Глобальна комп'ютерна мережа
RIP	–	Протокол маршрутної інформації
CCNA	–	Implementing Cisco IOS Network Security
PPTP	–	Point-to-Point Tunneling Protocol
PPP	–	Point-to-Point Protocol
SSL	–	Secure Sockets Layer
ПЕОМ	–	Персональна електронно-обчислювальна машина

ВСТУП

Теперішній час – століття інформаційних технологій. Інформаційні технології - широкий клас дисциплін та областей діяльності, що належать до технологій управління та обробки даних, у тому числі, із застосуванням обчислювальної техніки. Без перебільшення можна сказати, що ІТ сьогодні охопили майже всі сфери діяльності. Постійно росте об'єм та обіг інформації. Процес накопичення, обробки та використання знань постійно пришвидшується.

У зв'язку з цим виникає необхідність застосування автоматичних засобів, які забезпечують ефективне зберігання, обробку та розподіл накопичених даних. Існування сучасного підприємства великого чи малого, вже неможливо уявити, без використання інформаційних технологій та автоматизації виробництва. Додатково слід відзначити, що успішна діяльність його ґрунтується на технічному забезпеченні компанії інформаційними ресурсами, включаючи комп'ютерні системи. Сучасне управління організацією вимагає постійного моніторингу стану комерційних та фінансових ринків, а також швидкої координації роботи всіх філій та співробітників.

Реалізація названих завдань потребує спільної участі великої кількості різних фахівців, які часто територіально віддалені один від одного. У такій ситуації для організації ефективної взаємодії цих фахівців служать системи розподіленої обробки даних. Локальна обчислювальна мережа – це більше, ніж просто сума об'єднаних нею компонентів. На підключених до мережі комп'ютерах можна спільно використовувати загальне підключення до Інтернету, спільний принтер та інше обладнання та спільні файли.

З'єднання комп'ютерів у мережу значно збільшує їх можливості та дозволяє заощадити гроші. З'єднавши комп'ютери в мережу, можна отримати такі можливості:

- загальний доступ до Інтернету;
- загальний доступ до принтера, сканера та іншого обладнання;
- загальний доступ до файлів та папок;
- економія дискового простору, тобто. не обов'язково зберігати однакові програми на кожній машині.

В даний час будь-яке підприємство, яке має у своєму розпорядженні більше одного комп'ютера прагне об'єднати їх у локальну мережу.

Проектування локальної мережі – це досить складний процес, а також довготривалий, що потребує особливої уваги та високого рівня знань в галузі мережових технологій. Одного лише бажання до розробки локальної мережі буде замало. Потрібно ще й специфічне фахове обладнання. У загальному випадку останнє включає ключові модифікації комунікаційного обладнання, що активно використовується на сьогоднішній день для розробки локальних мереж і об'єднування їх одна із одною через глобальні зв'язки.

Для побудови між комп'ютерами локальних зв'язків активно застосовуються різні варіанти кабельних порядків, мережні адаптери, комутатори, концентратори, мости, повторювачі та маршрутизатори.

Ключова ціль локальної мережі – покрити активним користувачам потенційну перспективу колективного використання інформаційних масивів. Переваги, що набудуться при мережному з'єднанні персональних комп'ютерів у формі обчислювальної внутрішньовиробничої мережі: розподіл інформаційних масивів та ресурсів, диференціювання даних, розподіл програмних зразків, розрахований на багатокористувацький режим роботи.

Для розвитку та вдосконалення організації застосовуються сучасні комп'ютерні технології, що дозволяють підтримувати ступінь інформаційно-технічного забезпечення високому рівні. За допомогою запропонованої системи зв'язку та передачі даних буде можливим задовольняти всім покладеним на неї завданням. А саме: забезпечення безпомилкового інформаційного обміну даними між робочими станціями, зниження навантаження на мережеве обладнання, виключення помилок що виникають

під час роботи з БД. Поряд із цими вимогами система зв'язку та передачі даних буде забезпечувати належний рівень захисту інформації, що не допускає її спотворення, або витоку.

Метою дипломної роботи виступає модернізація комп'ютерної мережі Запорізького фахового авіаційного коледжу.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- проаналізувати існуючу комп'ютерну мережу;
- обрати технології для модернізації мережі;
- спроектувати модернізовану комп'ютерну мережу;
- обрати необхідне програмне та апаратне забезпечення мережі;
- змодельовати роботу мережі в емуляторі Cisco Packet Tracer;
- описати монтаж системи.

Робота складається вступу, п'яти розділів, висновків, списку літературних джерел, графічного матеріалу.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз існуючої мережі

На сьогоднішній день Запорізького авіаційного фахового коледжу ім. О.Г. Івченка об'єднує 51 комп'ютерів, спроектована за стандартом Ethernet 100 Base-T, швидкість передачі даних в мережі – 100 Мбіт/с. Для об'єднання комп'ютерів використовується десять комутаторів із 24-х портів.

Комп'ютери підключаються до відповідного порту switch за допомогою розетки RJ-45, а до розетки за допомогою конектора RJ-45. Мережа будується на основі логічної і фізичної топології «змішаної». Структурна схема існуючої мережі Запорізького авіаційного фахового коледжу (див. рис. 1.1).

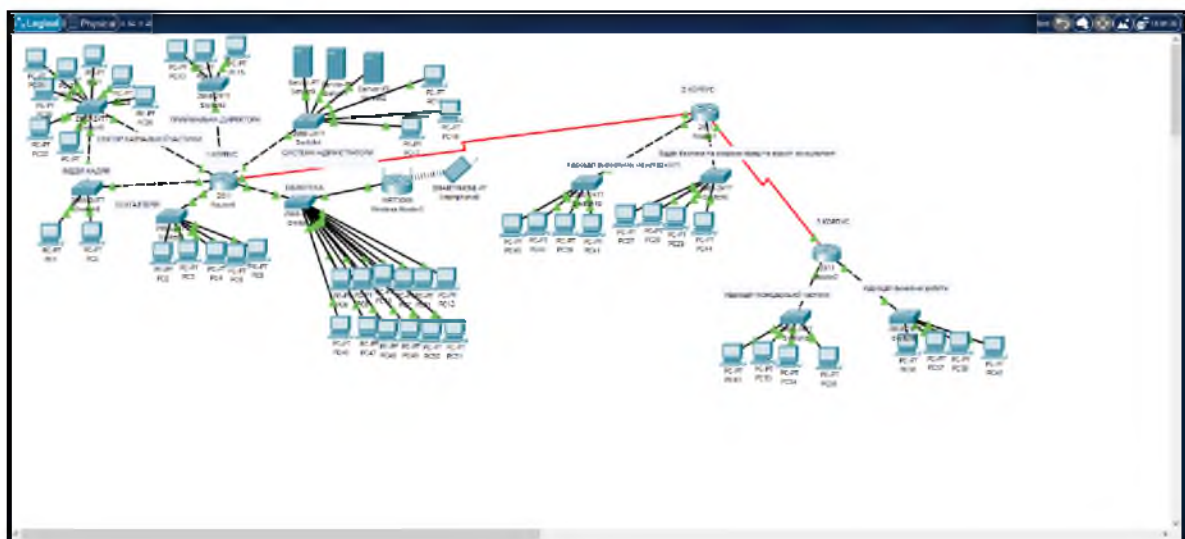


Рисунок 1.1 – Структурна схема існуючої мережі

У зв'язку із збільшенням кількості робочих станцій та із збільшеним навантаженням, так само зросли вимоги до безпеки, існуючої мережі. Знадобилася серйозна модернізація, що включає в себе оновлення мережного обладнання. Особливу увагу необхідно приділити безпеці мережі, що включає в себе не тільки загрози «з зовні» але, так само охоплює такі аспекти як, захист мережі і співробітників від атак, заснованих на використанні соціотехніки і захист від

інсайдерів. Дана задача вирішується шляхом створення на підприємстві комплексної системи захисту.

Мережа, що функціонувала в Запорізькому авіаційному фаховому коледжі ім. О.Г. Івченка мала масу недоліків: відсутність зрозумілої і логічної системи кабелів, ненадійне з'єднання основних комутаторів і вузлів мережі, низька відмовостійкість, неминучість значних фізичних і фінансових витрат при додаванні нових користувачів, скрутність роботи з адміністрування, моніторингу мережі та усунення несправностей, неможливість інтегрування додаткових мережевих служб.

Перераховані недоліки мають наступні причини:

- використання дешевого комутаційного обладнання;
- відсутність сучасних каналів зв'язку;
- недотримання сучасних стандартів при побудові топології;
- неоптимальне використання програмних засобів адміністрування, в т. ч. мережевих протоколів.

Аналіз предметної області показав наступне:

- більшість викладачів, а також студенти використовують в роботі ресурси мережі Інтернет. Необхідно забезпечити швидкий доступ до ресурсів мережі Інтернет (Висока продуктивність мережі), а також гнучку систему управління доступом, із застосуванням різних правил і політик до користувачів;
- необхідно забезпечити недоступність конфіденційної інформації не працюючим з нею користувачам, як всередині установи, так і за його межами;
- запорізький авіаційний фаховий коледж ім. О.Г. Івченка має кілька будівель: головний корпус – чотириповерхова будівля, в якій розташовані всі адміністративні відділи, підрозділи та навчальні аудиторії, з чотирма комп'ютерними класами, будівля майстерень з одним комп'ютерним класом а також двоповерхову будівлю з комп'ютерним класом.

1.2 Призначення та цілі модернізації мережі

Донедавна у державних установах був відсутній принцип автоматизації. Наприклад, карти в медичних установах, облік у податковій службі, ведення щоденників успішності у школах здійснювалось виключно у паперовому вигляді.

Це позначалося на швидкості обробки інформації, якості її зберігання та передачі. Також можна відзначити такі незручності як нестача засобів аналізу та контролю роботи державних установ. Проте, на даний час, відбулася низка змін на шляху до розвитку обміну інформацією з допомогою локально – обчислювальних мереж. Так, наприклад, всередині окремих органів з'являються кошти обліково-розрахункових процесів, електронні способи ведення документа обороту та ін. У державних установах елементи мережної структури можуть бути представлені у вигляді адміністративних та нормативно-методичних зв'язків між організаційними одиницями.

Локально-обчислювальна мережа – це цілий комплекс взаємопов'язаних один з одним програмних та апаратних засобів. Завданням локально - обчислювальної мережі є передача інформації між віддаленими апаратами підприємства. Мережа підприємства зазвичай розробляється змішаною топологією, включаючи кілька локальних мереж. Як правило, всі установи мають схожу структуру, маючи у своєму складі кластер керівників, адміністрацію та підлеглих. При створенні локально – обчислювальних мереж, як правило, поділ відбувається подібним шляхом. Локально – обчислювальна мережа установ має вирішувати такі завдання:

- надання доступу до спільного інформаційного сховища;
- аналітичний контроль ділових процесів;
- електронний обмін бухгалтерськими та податковими документами;
- управління даними локальної системи.

Таким чином, локально - обчислювальна мережа необхідна для створення, розвитку та підтримання працездатності програмно – методичної та технологічної інформаційної структури підприємств, а також адміністративного управління.

Також локальна мережа вирішує питання віддаленого взаємодії у межах певних проєктів. Локальна мережа повинна містити:

- засоби доступу до мережі та передачі даних;
- засоби передачі інформації;
- засоби захисту інформації (міжмережові екрани, програмні засоби фільтрації контенту, ідентифікатор та автентифікатор користувачів);
- засоби комутації (комутатори, маршрутизатори);
- робочі місця з урахуванням персональних комп'ютерів.

При розробці та проєктуванні локальних мереж для держустанов необхідно забезпечити виконання таких вимог:

- розширюваність - простота додавання різних елементів мережі (Додатків, робочих місць та ін.);
- керованість - організація централізованого адміністрування, аналізу та планування розвитку;
- безпека – розмежування даних, заборона несанкціонованого доступу;
- продуктивність - висока продуктивність роботи мереж, швидкість передачі;
- надійність - безупинна робота ліній зв'язку, функціонування робочих місць, забезпечення якісного зберігання даних.

З урахуванням різноманітності діловодства, проєктування локально – обчислювальних мереж держустанов, а особливо державних закладів освіти є досить складним завданням. Саме тому на сьогоднішній день відсутній універсальний механізм розробки.

Функціональні вимоги до мережі, що розробляється:

- мережа має об'єднувати у своєму складі робочі місця співробітників, сервери та комунікаційне обладнання;
- сервер повинен мати максимальне завантаження не більше 65 – 75%;
- активне обладнання мережі повинно мати максимальне завантаження до 65%;
- швидкість передачі основних каналів зв'язку не гірша за 100 Мбіт\с;

- ЛОМ повинна забезпечувати можливість підключення користувачів мережі за допомогою бездротового зв'язку (wi-fi).

Технічні вимоги до мережі, що розробляється:

- ЛОМ повинна забезпечувати доступ до мережевих ресурсів із затримкою менше 2 секунди;
- пропускна здатність мережі повинна бути високою і мати запас, щоб не перевантажити канали зв'язку;
- активне мережне обладнання має: мати максимальне завантаження до 60%, мати швидкість передачі основних каналів зв'язку щонайменше 10 Мбіт/с; відповідати умовам експлуатації: (навколишня температура - $+5^{\circ}\text{C} \div +50^{\circ}\text{C}$; вологість - $20\% \div 90\%$; електроживлення - $220\text{В} \pm 10\text{В}$, 50 Гц від мережі змінного струму).

За виконання цієї дипломної роботи мною були складено основні етапи, необхідні для стандартизації локальних мереж:

- аналіз вимог (розробки в галузі обчислювальних мереж повинні ґрунтуватися на внутрішніх розпорядках навчального закладу, таких як навчальний цикл, довжина навчального дня, періоди звітності та ін.);
- розробка структурної моделі навчального закладу (можна виділити основні виробничі відділи та ієрархічні відносини, які виконують схожу роботу та існують у організації. Так ось всіх організаціях існує керівник та його заступник. Цим двом посадам, як правило, виділяється лідируюча (після адміністратора мережі) позиція, що виражається, наприклад, необмежену швидкість передачі даних, розширені права доступу, пріоритету отримання даних і т.д. Також у кожній організації існує адміністративний відділ (бухгалтерія, нормувальник, секретар, спеціаліст з кадрів). Як правило, до третього розділу користувачів відносять інших співробітників (операторів ПК, диспетчерів, архіваріусів та ін.);
- розробка технічної структури обчислювальної мережі (об'єднавши все галузі в окрему групу за своєю навчальною складовою, можна визначити і перелік апаратних пристроїв та програмних інструментів для прокладання локально – обчислювальної мережі. На даному етапі немає необхідності заглиблюватися в

виробників, моделі та характеристики пристроїв. Тут можна визначитися лише зі списком необхідних пристроїв для подальшої реалізації універсальної структури мережі);

– складання докладного списку необхідних пристроїв. (саме на даному етапі враховується і складається повна параметрична модель майбутньої локально - обчислювальної мережі. Тут потрібно визначитися з маркою та виробником обладнання, його якісних характеристиках, типом кабелю, способом його підключення, протоколами, програмними засобами. Для реалізації ж нашої мети, на даному етапі необхідно визначитися з характеристиками мережі на найменшій ділянці однієї локально – обчислювальної мережі. Саме цю частину згодом можна буде розширювати, дублювати та редагувати для впровадження в абсолютно будь-яку сферу державних установ. При цьому параметри, схема та алгоритми функціонування мережі, як результати даного етапу, будуть використовуватись для подальшого аналізу).

– моделювання та оптимізація локально-обчислювальної мережі (виробляються з метою оцінки характеристик функціонування локальної мережі та їх оптимізації);

– встановлення та обслуговування локальної мережі (мається на увазі контроль відвантаження апаратних засобів, конфігурування, встановлення обладнання, навчання персоналу);

– тестування мережі (виробляються випробування локально – обчислювальної мережі в різних проекціях та ситуаціях);

– супровід та експлуатація (останній етап не має чітких меж, мається на увазі постійне продовження цього етапу).

1.3 Постановка задачі

Потрібно розробити проєкт локальної обчислювальної мережі.

Загалом у роботі навчального задіяно 29 співробітників. Навчальний відділ взаємодіє із усіма відділами. Для потреб організації потрібні принтер, ксерокс, сканер, факс. Також є навчальний зал на 20 осіб, в якому потрібна бездротова мережа.

- потрібно 4 персональних комп'ютерів, кожен з яких повинен мати стабільне підключення до Інтернету;
- крім мережі інтернет, має бути організована внутрішня локальна мережа, розбита кілька частин з використання кількох віртуальних локальних мереж (VLAN);
- потрібна бездротова точка доступу до мережі, кількість користувачів бездротової мережі не більше 20;
- необхідний загальний мережний принтер.

Вимоги до локальної мережі:

- кількість користувачів: необмежена кількість;
- кількість комп'ютерів: 48;
- мережевий принтер: 5;
- підключення до локальної мережі;
- підключення до мережі інтернет;
- бездротове підключення до мережі.

Метою роботи є розробка, налаштування та подальша технічна підтримка локально-обчислювальної мережі навчального закладу Запорізький фаховий коледж. Створена ЛОМ повинна враховувати поступове збільшення парку робочих станцій, і навантаження на мережеві ресурси, що постійно збільшуються.

Для досягнення поставленої мети необхідно буде вирішити наступні завдання:

- Провести аналіз існуючих мережевих технологій і вибрати потрібний- ну для організації мережі;
- вибрати програмне забезпечення (ПЗ) для організації;
- організувати локальну мережу;
- провести встановлення та налаштування програм, необхідних для успішної роботи підприємства та безпеки інформації.

2 АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Загальні принципи побудови локальних мереж

Комп'ютерну мережу можна визначити як з'єднання двох і більше комп'ютерів за допомогою кабелю або телефонної лінії з модемом, що дозволяє їм обмінюватися даними. Комп'ютери, розташовані в одному приміщенні або будівлі та з'єднані між собою, утворюють локальну мережу (LAN - Local Area Network). Кількість комп'ютерів у такій мережі обмежується можливостями кабельної системи та мережевого обладнання. Коли кілька локальних мереж об'єднуються, утворюється кампусна мережа (CAN - Campus Area Network), яка може охоплювати, наприклад, декілька сусідніх будівель або корпусів одного підприємства чи навчального закладу. Міська мережа (MAN - Metropolitan Area Network) з'єднує кілька кампусних або локальних мереж підприємств та організацій, тоді як широка мережа (WAN - Wide Area Network) охоплює кілька міст, область чи навіть регіон. Глобальна мережа (GAN - Global Area Network) включає кілька широких мереж і може охоплювати країну. Нарешті, Інтернет об'єднує всі ці мережі, включаючи Всесвітню павутину (World Wide Web), систему електронної пошти та інші системи зберігання та передачі інформації.

Мережа - це група комп'ютерів, з'єднаних між собою за допомогою спеціального обладнання, що забезпечує обмін інформацією. З'єднання між двома комп'ютерами може бути прямим (двоточковим) або з використанням додаткових

вузлів зв'язку. Комп'ютерні мережі є магістральними інформаційними структурами, що складаються з фізичного та логічного рівнів. Фізичний рівень представлений компонентами мережі, які забезпечують фізичне з'єднання комп'ютерів. Це можуть бути мережеві карти, кабелі (коаксіальні, кручені пари, оптоволокно), а також вузлові елементи (маршрутизатори, концентратори, повторювачі, комутатори) та кінцеві елементи (термінатори, конектори, роз'єми).

Епоха мережевих взаємин між персональними комп'ютерами почалася з простого обміну даними через комунікаційні порти (COM) між двома комп'ютерами з різною архітектурою та операційними системами. Сучасні мережі чітко поділяються на локальні та глобальні, і процес інтеграції перших у другі триває. Локальні мережі можуть налічувати кілька сотень комп'ютерів, тоді як глобальні включають десятки тисяч. Швидкість обміну інформацією досягає 1000 Мбіт/с, а 10 Мбіт/с вважається початковою конфігурацією.

Сучасні комп'ютерні мережі не лише дозволяють передавати та приймати інформацію, але й надають безліч сервісних можливостей, таких як віддалене адміністрування, розподілені файлові системи, віддалене виконання програм, електронна пошта, віддалений друк, розподілені бази даних, системи віддаленого доступу та управління, пошукові системи, телеконференції тощо.

Мережі поділяються на локальні та глобальні, однорангові та багаторангові, однокористувацькі та багатокористувацькі, відкриті та закриті. Більшість класифікацій базується на видах програмного забезпечення. На одній фізичній основі можна створити мережі різних типів і класів.

Комп'ютер у мережі називається робочою станцією (Workstation). Комп'ютери можуть бути також серверами, якщо вони використовуються як керуючі центри або накопичувачі інформації. Локальні мережі об'єднують комп'ютери, розташовані в межах однієї кімнати або будівлі, і зазвичай мають корпоративний характер.

Принципи організації та протоколи локальних та глобальних мереж можуть бути різними або однаковими, тому мережу не можна відносити до локальної або глобальної лише за типом взаємодії чи програмного забезпечення. Мережі можуть

бути комерційними, з платним доступом до послуг, або некомерційними, з умовно безкоштовним доступом, що підтримуються освітніми та інформаційними структурами на добровільних засадах.

2.2 Аналіз наявних LAN технологій

Ethernet - це ціла група технологій, що включає як фірмові, так і стандартні варіанти. Практично всі види технологій Ethernet застосовують один і той самий метод розподілу середовища передачі даних - метод колективного доступу з розпізнаванням і виявленням колізій (CSMA/CD). Цей метод використовується в мережах із логічною загальною шиною. Усі комп'ютери в такій мережі мають прямий доступ до загальної шини, що дозволяє передавати дані між будь-якими двома вузлами мережі. Одночасно всі комп'ютери мережі можуть негайно отримати дані, які будь-який комп'ютер почав передавати на загальну шину. Кабель, до якого підключені всі станції, працює за принципом колективного доступу.

Колізія є важливим явищем у мережах Ethernet - це ситуація, коли дві станції одночасно намагаються передати дані через спільне середовище. Можливість чіткого розпізнавання колізій залежить від правильного вибору параметрів мережі, зокрема від співвідношення між мінімальною довжиною кадру і максимально можливим діаметром мережі. На продуктивність мережі значно впливає коефіцієнт використання, який відображає її завантаженість. За відсутності колізій і очікування доступу цей коефіцієнт залежить від розміру поля даних кадру і має максимальне значення 0,96. Максимально можлива пропускна здатність сегмента Ethernet досягається при передачі кадрів мінімальної довжини і становить 14880 кадрів/с, при цьому корисна пропускна здатність мережі становить лише 5,48 Мбіт/с, що трохи перевищує половину номінальної пропускної здатності - 10 Мбіт/с. Максимально можлива корисна пропускна здатність мережі Ethernet

становить 9,75 Мбіт/с, що відповідає використанню кадрів максимальної довжини 1518 байт, які передаються зі швидкістю 513 кадрів/с.

Залежно від типу фізичного середовища, стандарт IEEE 802.3 визначає різні специфікації: 10Base-5, 10Base-2, 10Base-T, FOIRL, 10Base-FL, 10Base-FB. Кожна специфікація визначає тип кабелю, максимальні довжини безперервних відрізків кабелю, а також правила використання повторювачів для збільшення діаметра мережі: правило "5-4-3" для коаксіальних варіантів мереж, і правило "4-х хабів" для крученої пари та оптоволокна.

Технологія Token Ring (802.5), розроблена компанією IBM, має статус стандарту IEEE 802.5. У мережах Token Ring використовується маркерний метод доступу, що гарантує кожній станції отримання доступу до кільця протягом часу обороту маркера. Метод доступу ґрунтується на пріоритетах: від 0 (нижчий) до 7 (вищий). Станція визначає пріоритет поточного кадру і може захопити кільце, якщо в ньому немає пріоритетних кадрів. Мережі Token Ring працюють на швидкостях 4 і 16 Мбіт/с і можуть використовувати як фізичне середовище UTP, STP, а також волоконно-оптичний кабель. Станції об'єднують кільце за допомогою концентраторів MSAU. Пасивний концентратор MSAU виконує роль кросової панелі, що з'єднує вихід попередньої станції в кільці з наступним входом. Максимальна відстань від станції до MSAU становить 100 м для STP і 45 м для UTP. Максимальна кількість станцій у кільці - 260, а максимальна довжина кільця - 4 км.

Технологія Token Ring має елементи відмовостійкості. За рахунок зворотного зв'язку кільця одна зі станцій - активний монітор - постійно контролює наявність маркера, а також час обороту маркера та кадрів даних. У разі некоректної роботи кільця запускається процедура повторної ініціалізації. Максимальний розмір поля даних кадру Token Ring залежить від швидкості кільця. Для швидкості 4 Мбіт/с він дорівнює близько 5000 байт, а для швидкості 16 Мбіт/с - близько 16 Кбайт. Мінімальний розмір поля даних кадру не визначено. Активний монітор виконує в кільці роль повторювача - він ресинхронізує сигнали, що проходять кільцем. Кільце

може бути побудоване на основі активного концентратора MSAU, який у цьому випадку називають повторювачем.

Fast Ethernet та 100 VG-AnyLan. Потреба у високошвидкісній і водночас недорогій технології для підключення до мережі потужних робочих станцій призвела на початку 90-х років до створення ініціативної групи, яка займалася пошуками нового Ethernet - такої ж простої та ефективної технології, але яка працює на швидкості 100 Мбіт/с. Фахівці поділилися на два табори, і в результаті восени 1995 року комітет 802.3 затвердив стандарт Fast Ethernet, що майже повністю повторює технологію Ethernet 10 Мбіт/с, а комітет 802.12 затвердив стандарт технології 100VG-AnyLAN, яка зберігала формат кадру Ethernet. Технологія Fast Ethernet зберегла спосіб доступу CSMA/CD. Усі відмінності Fast Ethernet від Ethernet виявляються на фізичному рівні. У стандарті Fast Ethernet визначено три специфікації фізичного рівня: 100Base-TX для 2-х пар UTP категорії 5 або 2-х пар STP Type 1 (метод кодування 4B/5B), 100Base-FX для волоконно-оптичного кабелю з двома оптичними волокнами (метод кодування 4B/5B) та 100Base-T4, що працює на 4-х парах UTP категорії 3, але використовує одночасно лише три пари для передачі, а решту - для виявлення колізії (метод кодування 8B/6T). Стандарти 100Base-TX/FX можуть працювати у повнодуплексному режимі.

Технологія Fast Ethernet, працюючи на кручений парі, дозволяє завдяки процедурі автопереговорів двом портам вибирати найбільш ефективний режим роботи - швидкість 10 Мбіт/с або 100 Мбіт/с, а також напівдуплексний або повнодуплексний режим. Максимальний діаметр мережі Fast Ethernet становить приблизно 200 метрів. У домені колізій Fast Ethernet допускається не більше одного повторювача класу 1 (що дозволяє транслювати коди 4B/5B коди 8B/6T і назад) і не більше двох повторювачів класу II (що не дозволяють виконувати трансляцію кодів).

У технології 100VG-AnyLAN арбітром, що вирішує питання про надання станціям доступу до середовища, є концентратор, що підтримує метод Demand Priority - пріоритетні вимоги. Цей метод оперує з двома рівнями пріоритетів, які

виставляють станції, причому пріоритет станції, яка довго не отримує обслуговування, підвищується динамічно. Технологія 100VG-AnyLAN підтримує кабель UTP категорії 3, і для забезпечення швидкості 100 Мбіт/с передає дані одночасно по 4 парам.

Високошвидкісна технологія Gigabit Ethernet додає новий, 1000 Мбіт/с, рівень у ієрархії швидкостей сімейства Ethernet. Цей рівень дозволяє ефективно будувати великі локальні мережі, у яких потужні сервери та магістралі нижніх рівнів

2.3 Вибір середовища передачі даних

Сьогодні існування сучасного навчального закладу неможливо уявити без локальної мережі – основи створення автоматизованих робочих місць.

Локальна мережа являє собою кабельну систему будівлі або групи будівель, розділену на структурні підсистеми у відповідність необхідним стандартам. Структурована кабельна система (СКС) є ієрархічною кабельною системою будівлі або групи будівель, розділену на структурні підсистеми. Вона складається з набору мідних та оптичних кабелів, крос-панелей, сполучних шнурів, кабельних роз'ємів, модульних гнізд, інформаційних розеток та допоміжного обладнання. Всі перелічені елементи інтегруються в єдину систему та експлуатуються згідно з певними правилами. Правильна організація кабельної системи будівлі є одним із ключових завдань створення інтелектуальних систем та визначає надійність функціонування всіх служб та підрозділів компанії. Саме тому при створенні кабельної системи будівлі необхідно, щоб вона була такою ж капітальною, як і сама будівля. У той самий час зміни у технологіях передачі, мережевих і комунікаційних стандартах насамперед зачіпають саме кабельні системи. Через це доводиться постійно модернізувати або навіть повністю замінювати всю слабкострумову проводку.

Структурована кабельна система – основа інформаційної інфраструктури будь-якого підприємства, що дозволяє звести в єдину систему безліч інформаційних сервісів різного призначення: локальні обчислювальні та телефонні мережі, системи безпеки, відеоспостереження тощо. Саме тому така велика роль СКС при побудові інформаційної системи: від того, наскільки коректно виконано СКС, залежать надійність та безпека різних операцій, без яких неможлива діяльність сучасного підприємства.

Під таким терміном розуміється кабельна частина телекомунікаційної інфраструктури будівлі або, іншим словом, середовище передачі будь-яких слаботочних сигналів у межі (комплексу) житлової, офісної та промислової будівель.

СКС є основою локальної комп'ютерної та офісної телефонної мережі і завоює все найбільше визнання внаслідок низки переваг – універсальності, зручність в експлуатації та надійності. Визнання даної технології залежить переважно від організацій, які розвивають, впроваджують та використовують СКС, а також від органів стандартизації.

Універсальність структурованої кабельної системи мається на увазі в використанні її для різного виду систем: комп'ютерних мережах; телефонних мереж; охоронних системах; пожежних сигналізацій; - Інші. Такі кабельні системи незалежні від кінцевого обладнання, це дозволяє створити гнучкі комунікаційні інфраструктури підприємств.

Структурні кабельні мережі – охоплюють весь простір будівель, з'єднують усі точки засобів передачі даних, такі як комп'ютер, телефон, датчики пожежних та охоронних сигналізацій, системи відеоспостереження та контролю доступу. Кожен із цих засобів забезпечується індивідуальними точками входу до загальних систем будівель.

Мережа, яка окрема для кожної інформаційної розетки, що зв'язує точки входу з комутаційними центрами поверхів утворюючи горизонтальні кабельні підсистеми. На кожному з поверхів усі комутаційні вузли спеціальною магістраллю поєднуються в комутаційних центрах будівель. Крім того, сюди ж підбиваються

зовнішні кабельні магістралі для підключення будівлі до глобальної інформаційної мережі, телефонії, інтернету. Конкретна топологія дає надійне управління всією системою будівель, забезпечуючи гнучкість та зменшуючи складність системи, а також робить її уніфікованою.

Головними структурами при побудові СКС є:

- робоче місце – область, де відбувається встановлення технічних засобів користувачів, підключених до кабельної мережі будівель. Робочі місця оснащуються не менш ніж двома інфо-розетками, виходячи з того, що звичайні офісні робочі місця містять як мінімум один комп'ютер користувачів та телефон. Для підключення комп'ютера та телефону використовується розетка зі стандартизованими роз'ємами RJ-45 та комутаційний шнур довжиною від 1 метри;

- горизонтальна кабельна проводка – кабельна лінія, що з'єднує робочі місця із комутаційним вузлом поверху. Горизонтальні кабельні проводки, на основі мідних провідників, використовують чотирипарні одножильні кабелі у різних виконаннях. У стандартних умовах застосовується неекранований, а за більш високих вимог до електромагнітного випромінювання, сумісності або конфіденційності – екранований кабель. У рідкісному та особливому випадку як горизонтальні кабельних систем можливе застосування оптоволоконних кабелів, що забезпечує підвищений захист від електромагнітних випромінювань та захист від несанкціонованих доступів;

- комутаційний вузол поверху – області, в яких сходяться лінії горизонтальних кабельних проводок, розміщуються комутаційні засоби та обладнання, що здійснюється адміністрування кабельних системи поверху. Під адмініструванням СКС розуміється внесення змін та доповнення існуючих конфігурацій. Базою такого центру є патчі та кроспанелі. Для простоти встановлення та зручності роботи, комутаційні засоби та обладнання розміщується у спеціальній шафі, до якої підводяться всі кабельні мережі. Шафа також виконує функцію обмеження доступу до комутаційним засобам;

- вертикальні кабельні проводки - кабельні лінії, які з'єднують комутаційний вузол поверхів із комутаційними центрами будівель;

- магістральні підсистеми - підсистеми комплексу будівель, які можуть складатися з мідних та/або оптоволоконних типів кабелів, та які об'єднують усі кабельні системи будівель;

Проектування структурованої кабельної мережі є складним процесом та вимагає відповідності наступним загальним вимогам:

- СКС мають бути спроектовані з надмірністю за кількістю підключень;
- структуровані кабельні системи мають бути виконані відповідно до стандартів – міжнародними, європейськими, американськими та українським. Такими є приміром EIA/ANSI/TIA 568 та EIA/ANSI/TIA 569;
- робочі місця повинні мати, як мінімум, роз'єм для підключення до локальної обчислювальної мережі та роз'єм для підключення телефону;
- максимальні відстані горизонтальних проводок не повинні бути понад 90 метрів;
- устаткування, яке використовується для структурних побудов кабельних систем повинно відповідати мінімум четвертої категорії;
- кожна з ліній зв'язку СКС від точок підключень обладнання до точок підключень до комутаційних панелей повинні пройти тестування на приналежність мінімум до четвертої категорії;
- структуровані кабельні системи мають забезпечувати швидкі перекомутації ліній горизонтальних проводок та магістралей будівлі;
- прокладки кабелів у коридорах повинні здійснюватися за укриттями, якщо такі є, а за їх відсутності – у спеціальних кабельних каналах; в робочому приміщенні підведення кабелів до робочого місця провадиться в кабель-каналах.

Комп'ютери в локальній мережі з'єднуються за допомогою кабелів, які передають сигнали. Кабель, що з'єднує два компоненти мережі (наприклад, два комп'ютери), називається сегментом. Кабелі класифікуються залежно від можливих значень швидкості передачі та частоти виникнення збоїв і помилок. Найчастіше використовуються кабелі трьох основних категорій:

- вита пара;
- коаксіальний кабель;

– оптоволоконний кабель.

Для побудови локальних мереж зараз найширше використовується вита пара (див. рис. 2.1).

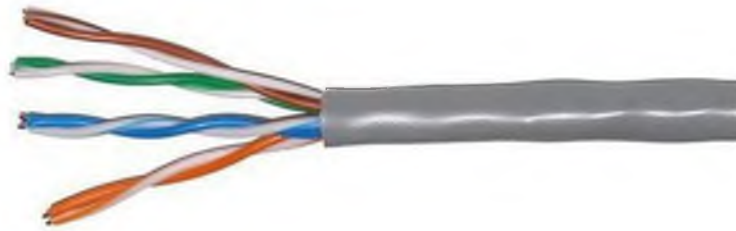


Рисунок 2.1 – Вита пара

Вита пара (англ. Twisted pair) - це тип мережевого кабелю, який складається з однієї або декількох пар ізольованих провідників, скручених між собою з певною кількістю витків на одиницю довжини. Це зменшує взаємні наведення під час передачі сигналу. Провідники покриті пластиковою оболонкою. Цей тип кабелю використовується в багатьох технологіях, таких як Ethernet, ARCNet та Token Ring, і завдяки своїй дешевизні та простоті установки, є найпоширенішим для побудови локальних мереж.

Залежно від наявності захисного екрану, виділяють різні типи витної пари: неекранована (UTP - Unshielded Twisted Pair), екранована (STP - Shielded Twisted Pair), фольгована (FTP - Foiled Twisted Pair) та екранована фольгована (S/FTP - Shielded Foiled Twisted Pair). У деяких типах екранованого кабелю захисний шар може бути присутній навколо кожної окремої пари. Екранування забезпечує найкращий захист від електромагнітних наведень, як зовнішніх, так і внутрішніх.

Існує кілька категорій кабелю вита пара, що нумеруються від CAT1 до CAT7. Кабель вищої категорії зазвичай містить більше пар дротів, і кожна пара має більше витків на одиницю довжини. Категорії неекранованої витої пари описуються в стандарті EIA/TIA 568.

- CAT1 – це телефонний кабель, що складається з однієї пари провідників. Використовувався раніше для передачі голосу або даних за допомогою модему.

- CAT2 - старий тип кабелю, що містить дві пари провідників. Підтримував передачу даних на швидкостях до 4 Мбіт/с, використовувався в мережах Token Ring та ARCNet.

- CAT3 – двопарний кабель, використовуваний у локальних мережах 10BASE-T та Token Ring, підтримує швидкість передачі даних до 10 Мбіт/с. Відповідає вимогам стандарту IEEE 802.3.

- CAT4 – кабель, що складається з чотирьох пар провідників, використовувався в мережах Token Ring, 10BASE-T та 10BASE-T4, з максимальною швидкістю передачі даних до 16 Мбіт/с.

- CAT5 – чотирипарний кабель, широко відомий як стандартна витопара, підтримує швидкість передачі до 100 Мбіт/с при використанні двох пар і до 1000 Мбіт/с при використанні чотирьох пар. Сьогодні використовується покращений варіант CAT5e, який краще пропускає високочастотні сигнали.

- CAT6 – кабель, що застосовується в мережах Fast Ethernet та Gigabit Ethernet, складається з чотирьох пар провідників і здатний передавати дані на швидкості до 10000 Мбіт/с. Доданий до стандарту у червні 2002 року, підтримує сигнали частотою до 200 МГц.

- CAT7 – специфікація цього кабелю затверджена міжнародним стандартом ISO 11801, швидкість передачі даних до 10000 Мбіт/с, частота сигналу до 600-700 МГц. Кабель цієї категорії має загальний екран і екрани навколо кожної пари провідників.

Вита пара широко застосовується у мережевих технологіях та комунікаціях, сьогодні кабель категорії 6 часто замінює коаксіальний кабель. Незважаючи на більшу захищеність екранованої витої пари, її не так часто використовують через

складність установки та потребу в заземленні. Коаксіальний кабель, у свою чергу, складається з мідного дроту, покритого ізоляцією, екрануючою металевою обплетенням і зовнішньою оболонкою. Сигнали передаються по центральному дроту, який може бути як цілісним, так і багатожильним (див. рис. 2.2).



Рисунок 2.2 – Коаксіальний кабель

Для створення локальної мережі використовують два види коаксіального кабелю: тонкий ThinNet та товстий ThickNet. Сьогодні локальні мережі, засновані на коаксіальному кабелі, майже не зустрічаються. Максимальна швидкість передачі даних у такій мережі не перевищує 10 Мбіт/с. Обидва типи кабелів, ThinNet і ThickNet, підключаються до роз'єму BNC, і на обох кінцях кабелю необхідно встановити термінатори.

Оптоволоконний кабель (див. рис. 2.3) складається з оптичних волокон (світловодів), по яких дані передаються у вигляді світлових імпульсів. Через оптоволоконний кабель не передаються електричні сигнали, тому перехопити сигнал неможливо, що практично виключає несанкціонований доступ до даних.



Рисунок 2.3 – Оптоволоконний кабель

Оптоволоконний кабель використовують для транспортування великих обсягів інформації на максимально доступних швидкостях. Головним недоліком такого кабелю є його крихкість: його легко пошкодити, а монтувати та з'єднувати можна лише за допомогою спеціального обладнання.

2.4 Вибір топології мережі

Топологія мережі визначається геометричною фігурою, утвореною лініями зв'язку між комп'ютерами, або фізичним розташуванням по відношенню один до одного комп'ютерів, пов'язаних між собою. Топологія мережі може бути однією з показників порівняння і класифікації різних комп'ютерних мереж. Виділяють кілька видів топології мережі:

- загальна шина;
- зірка;
- кільце;
- змішана.

У разі використання загальної шини, всі комп'ютери підключаються до одного кабелю, який називається шиною даних. При цьому пакет прийматиметься всіма комп'ютерами, які підключені до цього сегменту мережі. Швидкодія мережі багато в чому визначається кількістю підключених до загальної шини комп'ютерів. Що більше таких комп'ютерів, то повільніше працює мережа. Крім того, подібна топологія може стати причиною різноманітних колізій, що виникають, коли кілька комп'ютерів одночасно намагаються передати інформацію до мережі. Колізія - нормальне явище, що з'являється під час роботи мережі. Щоб проаналізувати та усунути колізію, всі комп'ютери одночасно вивчають сигнали, що виникають на кабелі. Якщо сигнали, що передаються і реально спостерігаються, не збігаються, то є присутність колізії. Ті комп'ютери, які помітили колізію, відправляють до мережі

32-бітову послідовність, яка називається jam-послідовністю. Імовірність появи колізії зростає із збільшенням кількості підключених до шини комп'ютерів. Щоб запобігти відображенню електричних сигналів, на кожному кінці кабелю встановлюють термінатори (terminators), що поглинають ці сигнали. Всі кінці мережного кабелю повинні бути до чогось підключені, наприклад до комп'ютера або баррел-коннектор - для збільшення довжини кабелю. До будь-якого вільного - непідключеного - кінця кабелю повинен бути приєднаний термінатор, щоб запобігти відображенню електричних сигналів. Топологія "Загальна шина" представлена на рис. 2.4.

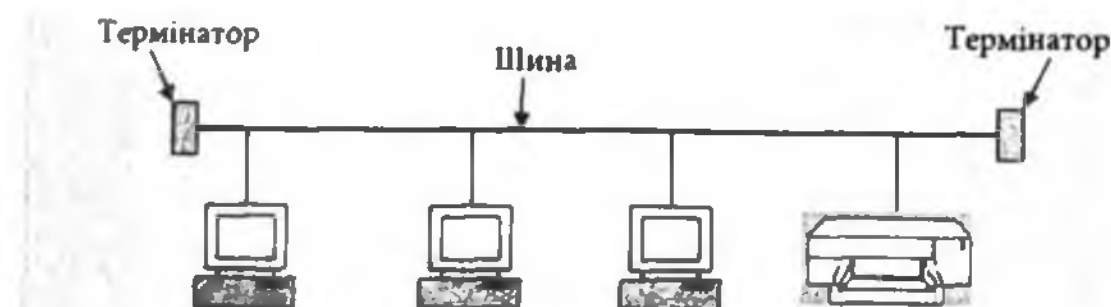


Рисунок 2.4 – Топологія "Загальна шина"

Переваги використання мереж з топологією «загальна шина» включають значну економію кабелю, простоту створення та управління. Проте маютьс я й недоліки, такі як ймовірність колізій зі збільшенням числа комп'ютерів у мережі, можливість обриву кабелю, що може призвести до відключення багатьох комп'ютерів, а також низький рівень захисту передачі інформації, оскільки будь-який комп'ютер може отримати дані, що передаються.

У той час як при використанні зіркоподібної топології кожен комп'ютер підключається до центрального комутатора або концентратора, що забезпечує більш високий рівень надійності. Всі пакети даних транспортуються через центральний пристрій, що спрощує керування мережею. Також можна використовувати як активні, так і пасивні концентратори. У разі розриву з'єднання між комп'ютером і концентратором решта мережі продовжує працювати. Однак у

випадку виходу з ладу центрального концентратора мережа може припинити роботу.

За допомогою зіркоподібної структури можна легко підключати до мережі навіть інші локальні мережі(див. рис. 2.5).



Рисунок 2.5 – Топологія "Зірка"

Використання топології «зірка» є дуже зручним при пошуку пошкоджених елементів, таких як кабелі, мережеві адаптери чи роз'єми. У порівнянні з топологією «загальна шина», «зірка» виявляється набагато зручнішою при додаванні нових пристроїв до мережі. Мережі з швидкістю передачі 100 та 1000 Мбіт/с часто побудовані саме за топологією «зірка».

Якщо розмістити концентратор у самому центрі «зірки», то логічна топологія зміниться на «загальну шину», проте це зазвичай не використовується через потенційні проблеми з колізіями даних.

Перевагами топології «зірка» є:

- Простота створення та управління мережею.
- Високий рівень надійності, оскільки поломка одного з'єднання не призводить до зупинки решти мережі.

– Висока захищеність передачі інформації, особливо якщо у центрі «зірки» розташований комутатор, що забезпечує виключення несанкціонованого доступу.

Основним недоліком є те, що поломка концентратора (або комутатора у разі, якщо він використовується) може призвести до припинення роботи всієї мережі, якщо не застосовується резервування (див. рис. 2.6).

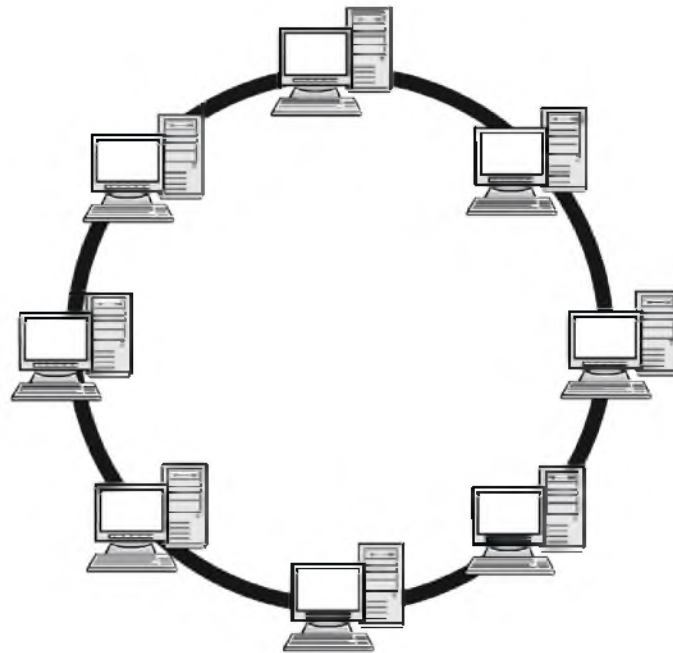


Рисунок 2.6 – Топологія "Кільце"

У випадку застосування кільцевої топології абсолютно усі комп'ютери мережі конектяться із одним кабелем кільця. Пакети рухаються по кільцю в єдиному напрямку через усі мережеві плати які завчасно під'єднані до мережі комп'ютерів. Комп'ютер впотужнюватиме сигнал, і направлятиме його далі по кільцю. Мережа з такою топологією зображена на малюнку.

Плюси кільцевої топології понижають у тому, що більші об'єми потоків даних обслуговуються результативніше, аніж у інциденті із загальною шиною. Кожен комп'ютерний пристрій виступає повторювачем: він впотужнює сигнал перед посилом наступній машині, що дає можливість збільшити розмір мережі значною мірою, потенцію установити різні верхи доступу до мережі; при цьому

комп'ютер, у якого перевага більша, зможе більшу тривалість часу утримувати маркер та доклатати більше потоку інформації.

До суттєвих вад можна пов'язати той факт, що обрив мережного кабелю у результаті призводить усю мережу до непрацездатності, довільний комп'ютер має змогу одержати дані, що ширяться мережею. Дана топологія окреслює під'єднання кожного комп'ютера через індивідуальний провід до останку комп'ютерів, що у мережі. Використання даного методу надає можливість зужитковувати додаткові напрями транспортування потоків даних. У випадку бескеду будь-якого кабелю масив інформаційних даних подається іншим курсом, а мережа зможе адекватно функціонувати далі.

Змішані топології суміщають у собі дві або більше топології, формуючи тим самим довершену мережеву конструкцію. При застосовуванні топології "зірка-шина" декілька мереж, яким властива зіркоподібна топологію, під'єднані до однієї шини (див. рис. 2.7).

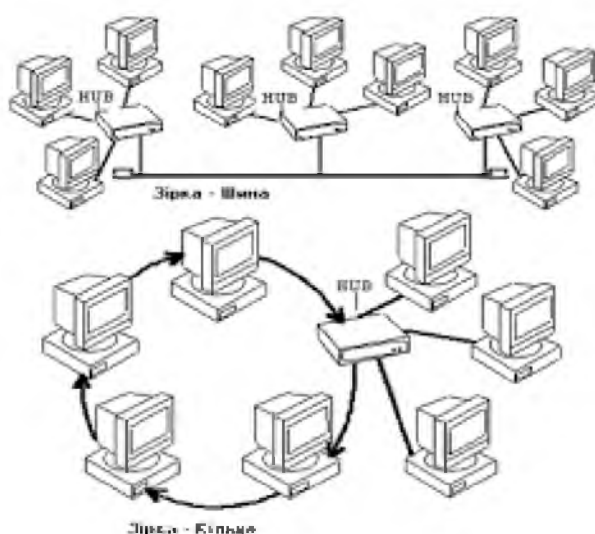


Рисунок 2.7 – Топологія "зірка-шина"

У даній топології збій коректного функціонування на одному з комп'ютерів не віддзеркалиться на роботі мережі в цілому. Якщо ж аберація генерального концентратора, до якого під'єднуються комп'ютери «зірки», всі вони будуть позбавлені можливості підтримувати зв'язок у подальшому. У топології «зірка-

кільце» комп'ютери конектяться до ключового компоненту, як і зіркоподібної мережі. При цьому самі компоненти поєднані мережею з кільцевою топологією.

Порівняльний аналіз топологій локально-обчислювальних мереж наведено (Таблиця 2.1)

Таблиця 2.1 – Порівняльний аналіз топологій локально-обчислювальних мереж

Характеристики	Топології обчислювальних мереж		
	Зірка	Кільце	Шина
Вартість розширення	Незначна	Середня	Середня
Приєднання абонентів	Пасивне	Активне	Пасивне
Захист від відмов	Незначна	Незначна	Висока
Розміри системи	Будь-які	Будь-які	Обмежені
Обслуговування	Гарна	Хороша	Незначна
Вартість підключення	Незначна	Незначна	Висока
Поведінка системи при високих навантаженнях	Хороша	Задовільна	Погана
Можливість роботи в режимі реального часу	Дуже хороша	Хороша	Погана
Розведення кабелю	Хороша	Задовільна	Хороша
Обслуговування	Хороше	Середнє	Середнє

2.5 Дослідження та аналіз характеристик, вибір мережевих пристроїв

Для виконання поставленого завдання вирішено використовувати наступне мережеве обладнання:

- маршрутизатор Cisco 2811;
- маршрутизатор Cisco 2960;
- комутатор Cisco 2960;
- фаєрвол ASA5506;
- персональний комп'ютер.

– лазерний принтер HP LaserJet Pro M203dn

Далі у роботі доцільно розглянути короткі технічні характеристики засобів, що використовувались у процесі розгортання мережі.

Таблиця 2.2 – Технічні характеристики Cisco 2811

Виробник	Cisco
Опис продукту	Модульний маршрутизатор
Тип продукту	Маршрутизатор
Апаратні характеристики:	
Процесор:	NPE-G1
Продуктивність	1018000 пакетів/с
Пам'ять процесора: -	За замовчуванням: 256 МБ - Максимум: 1 ГБ
Флеш-пам'ять PCMCIA (опціонально, доступно 2 слоти)	За замовчуванням: 64 МБ; Максимум: 128 МБ (для контролера I/O)
Додаткова флеш-пам'ять (опціонально):	Флеш-пам'ять PCMCIA:- За замовчуванням: 64 МБ- Максимум: 256 МБ Флеш-пам'ять Compact Flash:- За замовчуванням: 64 МБ- Максимум: 256 МБ
Розширення вводу/виводу	
Інтерфейсні порти	3 x RJ-45 GigE/FE/E
Слоти карт розширення	1
Слоти РА (Порт-адаптер)	6
Карти розширення, порти, слоти:	• Настроювані слоти без Port Adapter Jacket Card - 6• - Настроювані слоти з Port Adapter Jacket Card - 7• - Порти Ethernet (10BASE-T) - 48• - Порти Ethernet (10BASE-FL) - 30• - Порти Fast Ethernet (TX) - до 6• - Порти Fast Ethernet (FX) – до 6• - Порт-адаптери EtherSwitch – 4• - Порти 100VG-AnyLAN – до 6• - Порти ATM (T3, OC-3) – до 6, 4• - Packet over SONET – 6• - Порт-адаптери ATM-CES (Data, Voice, Video), Dual-Wide – 1• - Порти Token Ring (FDX, HDX) – 24• - Синхронні послідовні порти – 48• - Порти ISDN BRI (U, S/T) – 24, 48• - Порти ISDN PRI, багатоканальна T1/E1 - 48• - Порти багатоканальної T3 – до 6• - Порти HSSI – до 12• - Порти Packet over T3/E3 (вбудований DSU) – до 14• - Інтерфейсні порти IBM Channel (ESCON та Parallel) – 6• - Модуль прискорення VPN - 1
Тип слоту розширення	AIM
Мережеві технології	10 / 100Base-TX
Технологія Ethernet	Fast Ethernet
Управління та протоколи	

Продовження таблиці 2.2

Управління	• Element Manager Software (EMS) for the Cisco 7200 VXR Series • Cisco Secure Policy Manager • Cisco VPN Device Manager (VDM) • Cisco QoS Device Manager (QDM) • Cisco Info Center • CiscoWorks • Security Device Manager • MPLS Diagnostics Expert • Безпечний інтерфейс командного рядка з використанням протоколу Secure Shell (SSH) Protocol • Веб-інтерфейс
Протоколи маршрутизації	EIGRP, IGRP, IS-IS, OSPF, BGP, PIM, RIP
Протоколи, що підтримуються	ARP, IPCP, IP forwarding, IP host, IP Multicast, PPP-over-ATM, TCP, Telnet, TFTP, UDP, transparent bridging, VLAN, MPLS, IPv6, GRE, L2TP, UTI, L2TPv3, 6to4, ACLs, NAT, NetFlow, Firewall, Flexible Packet Matching, IPsec VPN, Secure Multicast, AAA, CHAP, FTP, RADIUS, SNMP, PAP, TACACS, RARP, SLIP, SNMP, DHCP, HSRP
QoS:	• Low-Latency Queuing (LLQ) • Class-Based Weighted Fair Queuing (CBWFQ) • Class-Based Weighted Random Early Detection (CBWRED) • Policing • Marking • Shaping • Committed Access Rate (CAR) • Generic Traffic Shaping (GTS) • Frame Relay Traffic Shaping (FRTS) • Modular QoS command-line interface (MQC) support • Network-Based Application Recognition

Таблиця 2.3 – Технічні характеристики Cisco 2960

Виробник	Cisco
Ідентифікаційний номер	WS-C2960-24TT
Опис продукту	Catalyst 2960 24 10/100 + 2 базовий образ LAN 1000BT
Тип продукту	Комутатор Ethernet
Інтерфейси / Порти	
Загальна к-ть портів	24
Порт висхідного каналу	Да
К-ть мережевих портів (RJ-45)	24
Деталі порта	24 x мережа Fast Ethernet 2 висхідних канали Gigabit Ethernet
Медіа та продуктивність	
Тип носія що підтримується	Вита пара
Стандарт кабелю виті пари	Категорія 5
Технологія Ethernet	Fast Ethernet
Мережеві технології	10Base-T 10/100 / 1000Base-T
Мережа та зв'язок	

Продовження таблиці 2.3

Слой що підтримується	
Управління та протоколи	
Управління	Мережевий помічник Cisco Підтримка CiscoWorks Налаштування Cisco Express Додаток CiscoView ПЗ Cisco Network Assistant

Таблиця 2.4 – Технічні характеристики Cisco ASA 5506

Виробник	Cisco ASA 5506
Пропускна здатність з контролем стану (багатопротокольна)	300 Mbit/c
Пропускна здатність VPN (Потрійний стандарт шифрування даних DES / Розширений стандарт шифрування даних (3DES/AES))	100 Mbit/c
Однорангові підключення IPsec VPN	10; 50
Користувачі Cisco Cloud Web Security	275
Однорангові підключення Cisco AnyConnect Premium / Apex VPN (включено; максимум)	2; 50
Віртуальні інтерфейси (VLAN)	5; 30
Контексти захисту (включено / максимум)	Недоступно
Висока доступність	необхідна ліцензія Security Plus активно / в режимі очікування

Користувачський слот флеш-пам'яті	-
Порти USB 2.0	
Інтегрований введення-виведення	8 x 1GE
Виділений порт управління	Так (разом з сервісами FirePOWER), 10/100/1000
Серійні порти	
Твердотільний жорсткий диск	50 ГБ mSata
Пам'ять	4 Гбайт
Мінімальний об'єм флеш-пам'яті системи	8 Гбайт
Системна шина	Багатошинна архітектура

3 ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ КІНЦЕВИХ КОРИСТУВАЧІВ

3.1 Вибір програмного забезпечення для робочих станцій в мережі

3.1.1 Операційна система Microsoft Windows 10 Professional

Операційна система – це набір програм, що керують ресурсами комп'ютера і сприяють взаємодії з користувачем. У структурі комп'ютерної системи операційна система знаходиться між апаратним обладнанням та прикладними програмами. Вона відповідає за ефективне використання ресурсів, управління процесами, файлами та мережею, а також надає зручний інтерфейс для користувачів.

Операційні системи можуть відрізнятися особливостями реалізації внутрішніх алгоритмів керування основними ресурсами комп'ютера (процесорами, пам'яттю, пристроями), особливостями використаних методів проектування, типами апаратних платформ, областями використання та багатьма іншими властивостями.

Основні функції операційної системи:

- реалізація запитів програм (виведення та введення потоків даних, старт та зупинка інших платформ, акцентування та звільнення додаткової пам'яті та ін.);
- завантаження програм на оперативну пам'ять;
- уодноманітнюваний доступ до периферійних приладів (програмні засоби вводу-виводу);
- керування оперативної пам'яттю (диференціювання між процесами, упорядкування віртуальної пам'яті);
- керування доступом до потоків даних на незалежних носіях, впорядкованим у тій чи іншій файлової системі;
- формування інтерфейсу активного користувача;
- завантаження даних щодо помилок системи;
- багатозадачність;
- продуктивне диференціювання ресурсів між процесами обчислювальної системи;

- розподіл доступу багатоманітних процесів до ресурсів;
- взаємодіяння між активними процесами: взаємообмін інформаційними даними, обопільна синхронізація;
- безпеку самої системи, а також даних активного користувача і програм від дій додатків або користувачів;
- передбачений на велику кількість активних користувачів користувачів і диференціювання прав доступу.

Windows 10 — операційна система персональних комп'ютерів, розроблена корпорацією Microsoft у межах сімейства Windows NT. Після Windows 8 система одержала номер 10, минаючи 9. Система має стати єдиною для різних пристроїв, таких як персональні комп'ютери, планшети, смартфони, консолі Xbox One та ін. Доступна єдина платформа розробки та єдиний магазин універсальних програм, сумісних з усіма підтримуваними пристроями.

Windows 10 постачається як послуга з випуском оновлень протягом усього циклу підтримки. Для операційної системи існують такі жорсткі системні вимоги проти Windows 8.1.

Мінімальні системні вимоги, опубліковані на офіційному сайті Microsoft, наведено у таблиці 3.1.

Таблиця 3.1 – Мінімальні апаратні вимоги Windows 10

Архітектура	32 біт	64 біт
Процесор	1 ГГц і більше тактової частоти з підтримкою PAE, NX та SSE2 (x86-64 процесори повинні також підтримувати CMPXCHG16B, PrefetchW та LAHF/SAHF інструкції).	
Оперативна пам'ять	1 Гб (для системи, що постачається як оновлення). 2 Гб (для системи, що постачається окремо)	2 Гб (для системи, що постачається як оновлення, так і окремо)
Відеокарта	Відеоадаптер з підтримкою DirectX 9 та WDDM версії 1.0	

Продовження таблиці 3.1

Архітектура	32 біт	64 біт
Вільне місце на жорсткому диску	16 Гб вільного місця	20 Гб вільного місця
Дисплей	800*600	
Пристрій введення	Клавіатура та миша	

3.1.2 Операційна система Microsoft Windows Server 2019

Microsoft Windows Server Standard 2019 – серверна операційна система, розроблена на платформі Windows Server 2019. Рішення консультує дійсно новий рівень безпеки та нововведень для програм та системи компаній.

ОС Microsoft Windows Server Standard 2019 започаткована для осередків із мінімізованою щільністю та не розрахована на віртуалізовані системи.

Зашифровані мережі можна домірювати, що надасть можливість адміністраторам шифрувати компоненти мережі для надійного захисту рівня мережі між серверами. Разом з тим, вбудований захист від загроз Windows Defender (ATP) підтримує превентивний захист, ідентифікуючи будь-які атаки, залучаючи атаки з нульовим днем.

Windows Server 2019 відрекомендовує вагомі покращення для обрахунку, зберігання та результативної роботи мережевих компонентів кластера Kubernetes. Більш того, Windows Server 2019 консультує вдосконалений WSL, зараджуючи користувачам Linux втілювати свої сценарії у Windows під час застосовування галузевих стандартів, таких як OpenSSH, Curl & Tar.

Hyper-конвергентна інфраструктура (HCI) Microsoft активно співробітничав з генеральними галузевими постачальниками обладнання для якісного надання надійного і водночас надзвичайно доступного рішення HCI із вивіреним дизайном.

3.1.3 Антивірус ESET Endpoint Security

ESET Endpoint Security – це хмарна пропозиція для захисту фінальних точок, спроектовано для надійного захисту організації будь-якого масштабу.

Рішення дораджує багаторівневий захист, яким адміністратори мають змогу управляти за сприянням послідньої централізованої консолі керування. ESET

Endpoint Security вберігає комп'ютери, мобільні пристрої, файлові сервери та віртуальні середовища. ESET масовий як індивідуальний продукт і як фрагмент більш грандіозного пакета корпоративної кібербезпеки, ESET PROTECT Enterprise, який також залучає безпеку файлового сервера, шифрування диска та EDR(див. рис. 3.1).

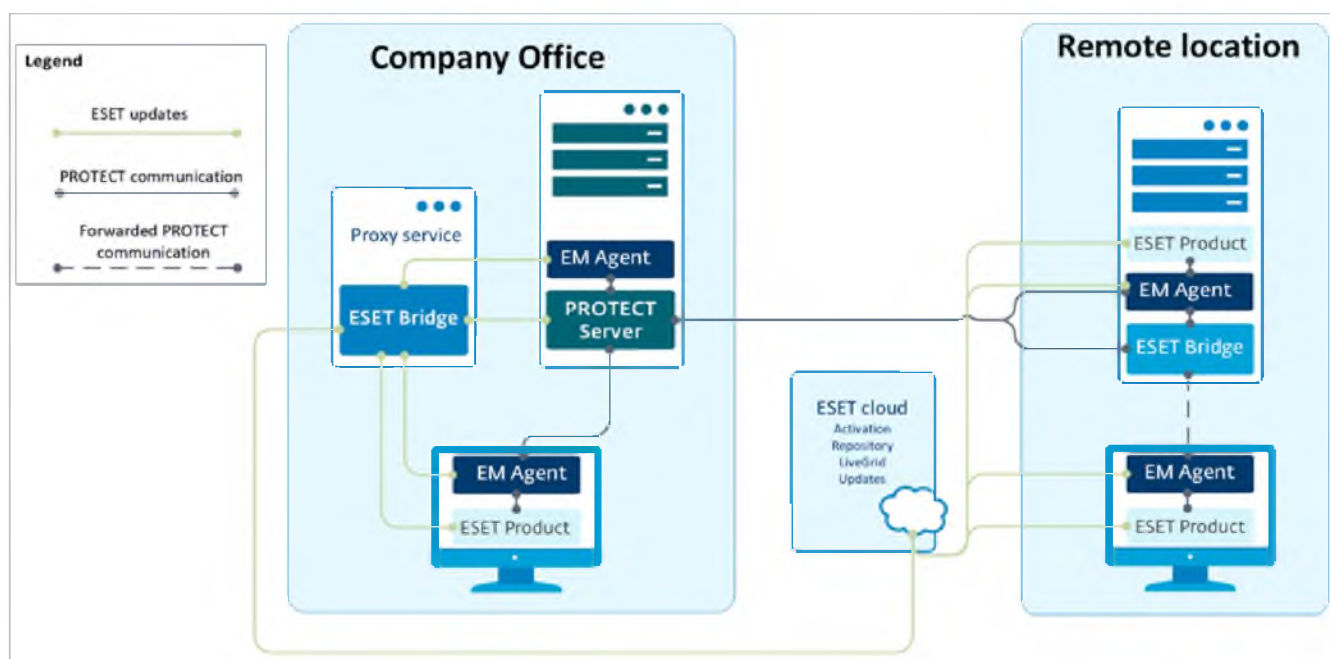


Рисунок 3.1 – Структура програмного рішення ESET Endpoint Security

ESET Endpoint Security вважається модерним підходом до формування дійсно багаторівневої системи безпеки комп'ютера. Модерна версія модуля сканування у дуєті із фаховими модулями фаєрвола та безпеки від спаму покриває точність та швидкість, які так необхідні для безпеки комп'ютера. Подібним чином, даний програмний продукт виступає інтелектуальною системою неперервного захисту від шкідливих програм та атак, які перспективно можуть нести загрозу безпеці комп'ютера.

ESET Endpoint Security – це багаторівневе рішення для формування рівня безпеки, яке є наслідком довгострокових зусиль, цілеспрямованих на звершення оптимального поєднання високого рівня захисту з мінімальним діянням на продуктивність комп'ютера.

Модерні технології, базовані на використанні штучного інтелекту, спроможні превентивно протистояти зараженням вірусами, а також іншими атаками з Інтернету без прямого впливу на результативність комп'ютера та інтервалів у роботі.

Рішення ESET Endpoint Security в першу чергу призначене для діючих станцій поміж невеликих підприємств. Для коректної роботи ESET Endpoint Security рішення має насамперед відповідати вказаним у роботі нижче програмним та апаратним вимогам. Підтримувані процесори: 32-розрядний (x86) процесор із набором інструкцій SSE2 або 64-розрядний (x64) процесор, 1 ГГц і вище, Операційні системи з останніми оновленнями Windows (принаймні KB4474419 та KB4490628), Операційна система та інше програмне забезпечення, встановлене на комп'ютері, повинні відповідати системним вимогам, 0,3 ГБ вільної системної пам'яті та 1 ГБ вільного місця на диску (див. примітку 2), Мінімальна роздільна здатність дисплея повинна становити 1024 x 768, Підключення через Інтернет або локальну мережу до джерела оновлення продукту.

Хоча існує можливість встановити та запустити продукт у системах, які не відповідають цим вимогам, рекомендується спочатку провести тестування можливостей використання на підставі вимог до продуктивності.

3.1.4 Пакет Microsoft Office 2019

Microsoft Office 2019 фаховий пакет офісних програм, що забезпечує найвищу продуктивність та продуктивну спільну роботу. Microsoft Office 2019 поглиблює функціональні потенції редакції Professional та розміщує знаряддя для розробки професійної документації та легку інтеграцію.

У пакет включені програми Office 2019, Word 2019, Excel 2019, PowerPoint 2019, OneNote 2016, Outlook 2019, Publisher 2019, Access 2019.

Переваги Microsoft Office для організацій:

- відповідність та архівування;
- бізнес-аналітика;
- корпоративний голос;
- керування правами доступу до інформації та можливості політики;

- захист цифрових даних від несанкціонованого використання шляхом інтеграції зі службами керування правами Windows для Windows Server;
- уніфікований обмін повідомленнями, присутність і голос.

3.1.5 Системний монітор Sysmon

При організації системи управління ІБ у компанії безліч завдань пов'язані із забезпеченням безпеки кінцевих точок (робочих станцій та серверів) під управлінням ОС Windows та Linux. Вибір засобів захисту великий, проте певні обмеження накладають і бюджети, що виділяються на ІБ, і питання сумісності аналізованих СЗІ з конкретними ОС. При цьому часто від захисних рішень потрібна реалізація функцій безпеки, які присутні або в самих ОС у вигляді вбудованого функціоналу, або у ПЗ, що вільно розповсюджується.

Прикладом такого функціоналу є ведення детальних журналів подій безпеки та передача їх у SIEM-системи, з урахуванням того, що ІБ-аналітиків зазвичай цікавить запуск та зупинка процесів та сервісів, мережеві з'єднання, зміна конфігурацій кінцевих пристроїв, а також специфічні події, що вказують на шкідливу активність. Аналіз таких подій може сприяти виявленню кіберінцидентів, а в рамках розслідування кібератаки журнали аудиту можуть стати джерелом цінних відомостей.

Одним із найкорисніших інструментів аналітика SOC-центру є рішення для захисту кінцевих точок (EDR, Endpoint Detection and Response), які поєднують у собі функціонал ведення детальних журналів безпеки, моніторинг та блокування небезпечних дій, централізоване управління. Однак СЗІ такого типу недешеві, тому в деяких випадках доцільно розглянути деякі безкоштовні утиліти, що хоча б частково реалізують необхідний функціонал.

Однією з таких програм є утиліта Sysmon (скорочення від System Monitor) з офіційного пакету Microsoft Sysinternals Suite, яка встановлюється на Windows та Linux та дозволяє вести глибокий аудит роботи ОС з метою виявлення кібератак. Ця утиліта добре зарекомендувала себе як серед дослідників кібербезпеки, так і серед аналітиків SOC-центрів. У цій статті ми докладно розповімо про Sysmon, дамо рекомендації щодо її налаштування та використання.

Відповідно до опису на офіційній сторінці Sysmon, дана утиліта призначена для моніторингу та запису системних дій, вона встановлюється у вигляді сервісу та драйвера, а також має функціонал запобігання несанкціонованим змінам її роботи за допомогою технології захисту процесів Protected Process Light (PPL).

Ця технологія застосовується в ОС старше Windows 8.1 і дозволяє захистити критичні системні процеси, підписані цифровим підписом, від впливу ВПЗ чи зловмисних дій користувачів. Встановлення драйвера утиліти Sysmon дозволяє отримувати більш глибокий доступ до даних про роботу ОС і розпочинати збір подій відразу після включення пристрою, що допомагає виявляти потайливе ВПЗ, яке запускається до старту основних компонентів ОС.

Спрощує централізований збір подій аудиту в SIEM-систему те, що події Sysmon записуються в стандартний журнал Windows (Applications and Services Logs – Microsoft – Windows – Sysmon/Operational). Принцип збору даних утилітою Sysmon полягає у виконанні зворотних викликів до ядра Windows (kernel callbacks), використанні трасування подій Windows (Event Tracing for Windows, скорочено ETW), а також виконанні API-дзвінків постачальників телеметрії Windows.

У ОС Linux робота Sysmon заснована на використанні бібліотеки sysinternalsEBPF, яка використовує технологію eBPF для збору інформації про роботу процесів, системних викликів та сокетів. Події Sysmon в ОС Linux записуються у стандартний файл /var/log/syslog.

Актуальна версія утиліти Sysmon для Windows має наступний функціонал:

- реєструє події створення процесу з командним рядком запуску та даними батьківського процесу;
- фіксує значення хеш-суми виконуваного файлу процесу з використанням алгоритмів SHA1, MD5, SHA256, IMPHASH;
- реєструє завантаження драйверів та DLL із зазначенням їх цифрових підписів та значень хеш-сум;
- реєструє прямий доступ (raw access) до дисків і томів;
- реєструє мережеві з'єднання із зазначенням імені процесу-ініціатора, IP-адреси призначення, імені хоста та номера порту;

- виявляє зміни у даті створення файлів;
- дозволяє заблокувати створення файлів форматів EXE, DLL, SYS у певних каталогах, з певними хеш-сумами, створювані певними батьківськими процесами;
- дозволяє створювати гнучкі XML-конфігурації із зазначенням об'єктів контролю для врахування всіх особливостей середовища функціонування.

3.2 Моделювання комп'ютерної мережі в програмі Cisco Packet Tracer

Cisco Packet Tracer рекомендовано використовувати для вивчення телекомунікаційних мереж та мережевого обладнання, а також для проведення уроків з лабораторних робіт у вищих закладах.

Основні можливості Cisco Packet Tracer:

- дружній графічний інтерфейс (GUI) сприяє кращому розумінню організації мережі, принципів роботи пристрою;
- можливість змоделювати логічну топологію для того, щоб створити мережі будь-якого розміру на рівні CCNA складності;
- моделювання як реального часу;
- режим симуляції;
- багатомовність інтерфейсу програми дозволяє вивчати програму своєю рідною мовою;
- удосконалене зображення мережного обладнання зі здатністю додавати/видаляти різні компоненти;
- наявність Activity Wizard дозволяє мережевим інженерам, студентам та викладачам створювати шаблони мереж та використовувати їх надалі;
- проєктування фізичної топології.

Емулятор мережі надає змогу мережевим інженерам будувати мережі будь-якої складності, формуючи та відправляючи різні пакети даних, зберігати та коментувати свою роботу. Професіоналісти мають змогу вивчати і надалі

використовувати такі мережеві пристрої, як комутатори другого та третього рівнів, робочі станції, визначати типи зв'язків між ними та з'єднувати їх. рядки (див. рис. 3.2).

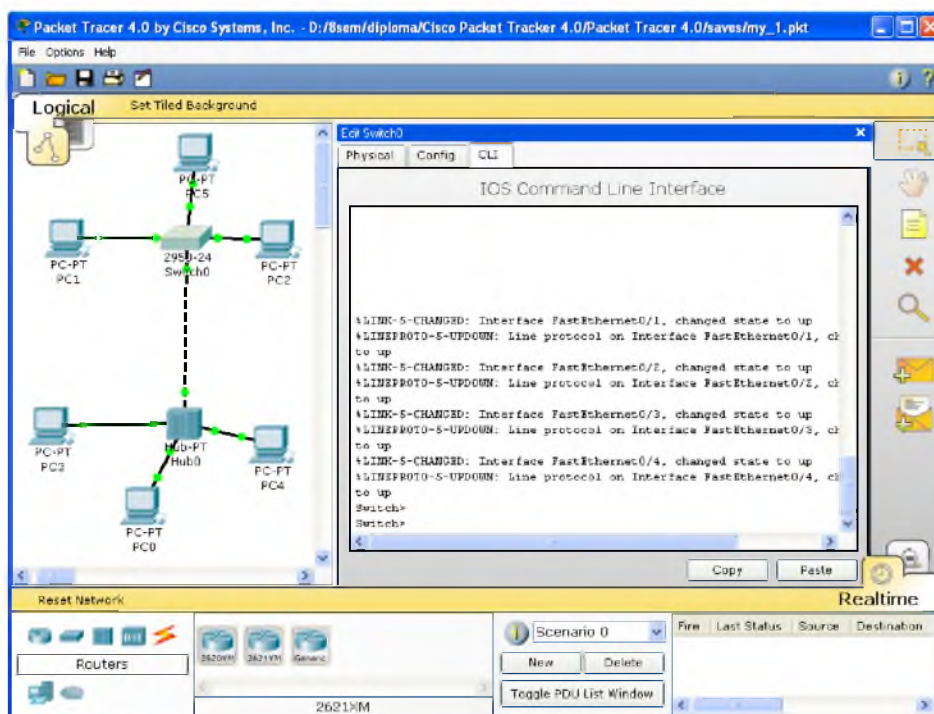


Рисунок 3.2 – Cisco Packet Tracer

Однією з найважливіших особливостей даного симулятора є у ньому «Режиму симуляції» (див. рис. 3.3). У цьому режимі всі пакети, що пересилаються всередині мережі, відображаються у графічному вигляді. Ця можливість дозволяє мережевим фахівцям наочно продемонструвати, за яким інтерфейсом зараз переміщається пакет, який протокол використовується і т.д.

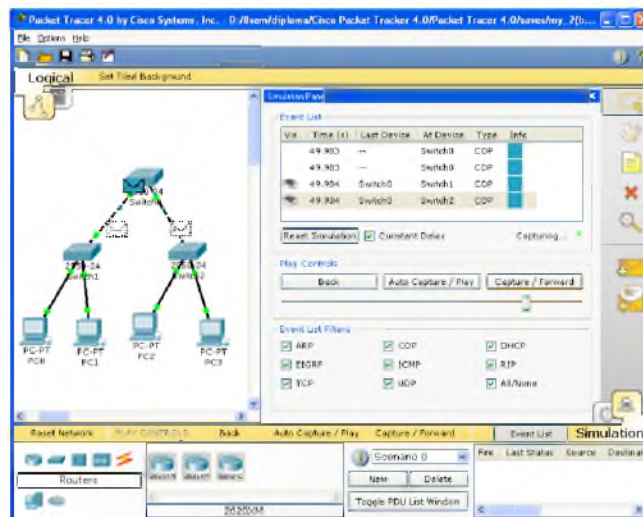


Рисунок 3.3 – Режим «Симуляції» в Cisco Packet Tracer

У «Режимі симуляції» мережеві інженери можуть лише відстежувати використовувані протоколи, а й бачити, якому з семи рівнів моделі OSI даний протокол задіяний (див. рис. 3.4). Це дозволяє з легкістю визначити, на якому із семи рівнів моделі OSI була допущена помилка і, відповідно, своєчасно її усунути.

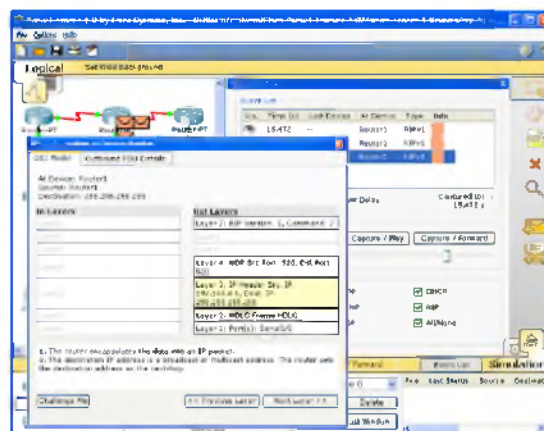


Рисунок 3.4 – Аналіз семирівневої моделі OSI у Cisco Packet Tracer

Cisco Packet Tracer здатний моделювати велику кількість пристроїв різного призначення, а також багато різних типів зв'язків, що дозволяє проєктувати мережі будь-якого розміру на високому рівні складності.

Моделювані пристрої: комутатори другого та третього рівнів, мережні концентратори, кінцеві пристрої, бездротові пристрої.

Типи зв'язків: консоль, прямий кабель, крос-кабель, волоконно-оптичний кабель, телефонна лінія, SerialDCE, SerialDTE.

У Packet Tracer можна відстежувати різні протоколи: ARP, CDP, DHCP, EIGRP, ICMP, RIP, TCP, UDP.

3.3 Огляд існуючих аналогів для проєктування мереж

Розглянемо найпопулярніші емулятори, що дозволяють створити віртуальні копії мережного обладнання.

Найбільш відомим емулятором мережного обладнання є Cisco Packet Tracer, це програмний продукт, розроблений самою компанією Cisco Systems.

Packet Tracer здобув значне розповсюдження за рахунок доцільності його використання для проходження навчання в межах програм Cisco Network Academy, мережевої академії, якої кожного року здобувають велика кількість фахівців-початківців. Розроблення мережної інфраструктури та наступна видозмінювана відбуваються крізь призму графічного інтерфейсу, який є інстинктивно популярним та найбільш комфортабельних з графічних інтерфейсів керівництва, наданих програмними засобами емуляції, що аналізуються стосовно мережевого обладнання.

Інтерфейс вкрай позитивно акліматизований для дебютантів фахівців і дуже полегшує процедуру розроблення нових мережевих інфраструктур або старт та конфігурування потрібних для здійснення практичних занять сервісів.

Ключове призначення емулятора Packet Tracer у розробленні віртуальних мереж для здійснення практичних робіт для виучки до сертифікаційних іспитів CCNA (Cisco Certified Network Associate) та CCNA Security (Cisco Certified Network Associate Security).

Окрім уніфікованих маршрутизаторів та комутаторів Packet Tracer затверджує емуляцію IP-телефонів, бездротових точок доступу та серверів з переліком стереотипних служб.

У Packet Tracer конфігуровано велику кількість засобів, що облегшують досліджування роботи мережної інфраструктури, таких як сніфери, що надають можливість дістати деталізовану інформацію щодо всіх потовів даних, що ширяться тому чи іншому пристрої, динамо-машини мережевого трафіку, що надають змогу ненатурально формувати навантаження, та засоби відбиття потоків даних, що надають можливість відслідкувати маршрут проходження мережі будь-яким пакетом або процедуру видозміни пакету при проходження різних пристроїв.

Ключова прерогатива Cisco Packet Tracer – безкоштовність даного продуктного рішення.

Тобто, емулятор Cisco Packet Tracer виступає щонайліпшим інструментом для здійснення практичних занять у процесі вишкілу за опорними курсів компанії Cisco та при виучці до іспитів рівня фахівця. Але для розв'язання складніших задач моделювання обчислювальних мереж це ПЗ не підходить, так як є симулятором і не надає всіх можливостей реального обладнання, і далі не розглядатиметься.

GNS3 GNS3 (Graphical Network Simulator 3) – це самостійний безкоштовний емулятор маршрутизаторів Cisco. GNS3 підтримується в масовості операційних систем Linux, Windows та Mac OS X, при тому цей емулятор надає змогу емулювати апаратну частину маршрутизаторів Cisco, для цього він загрузає та зужитковує реальний образ операційної системи Cisco IOS.

GNS3 – це графічна оболонка, що суміщає в собі перелік різноманітних програмних модусів емуляції. Графічний інтерфейс осередку емуляції, не призвичаюваний для фахівців-початківців, він більше розрахований на тих, хто вже має практику діяльності із засобами емуляції, мережевим обладнанням та проінформований з ключовими принципами діяння мережевих пристроїв. Але присутність графічних прийомів керівництва безкінечно спрощує процедуру розробки мережної інфраструктури та формує роботу з нею більш комфортабельною.

GNS3 залучає три ізольованих програмних емулятора.

Перший це Dynamips. Незліченно спеціалістів, що досліджують мережеві технології, використовують у роботі Dynamips тільки у середовищі GNS3, тому що відвалюється доцільність роботи з конфігураційними файлами та командним рядком.

Другим виступає Qemu, який надає змогу емулювати міжмережеві екрани. Cisco PIX і ASA та системи відвертання вторгненням Cisco IPS, присутність сприяння даних пристроїв у великій мірі збільшує коло можливостей імплементування GNS3 у навчанні за лініями, пов'язаними із забезпеченням безпеки мережевих інфраструктур.

Третім компонентом виступає систематичність віртуалізації VirtualBox, яка дає можливість об'єднувати в мережеву інфраструктуру з емульованих пристроїв віртуальні сервери або комп'ютери, які дають змогу абсолютно відбудувати достеменну інформаційну інфраструктуру, а значить вивчити більшу низку технологій.

GNS3 є дуже прискіпливою до ресурсів систематичністю емуляції. Так як включаються кілька незалежних систем емуляції одночасно, а зверху над ними їх інспектує середовище, що забезпечує ще й графічний інтерфейс, що безперестанку віддзеркалює зміни в стані інфраструктури, доконечні розважливі обчислювальні потужності.

EVE-NG – мережевий емулятор, котрий маніфестує собою платформу, розраховану на велику кількість активних користувачів, для розробки і формування віртуальних мереж, багатоманітних лабораторій, що затверджує ваговитий список телекомунікаційного обладнання. Отже, концептуальною новизною продукту EVE-NG виступає здатність запускання та застосовування програми між багатоманітними платформами та багатоманітними продуцентами пристроїв.

Разом з тим, EVE-NG активно застосовується в мережевому інженерингу, у тому числі для комплексного підходу у ідентифікуванні та елімінації причин питання неполадки мереж (troubleshooting).

З переваг даоного рішення доцільно також запримітити перспективу запуску необмеженої кількості примірників обладнання (роутерів, комутаторів, пристроїв безпеки тощо), кількість обмежена тільки апаратними можливостями робочого місця. Підтримка обладнання в EVE-NG є дуже широкою.

EVE-NG дає можливість запуску образів з VIRT (vIOS-L2 та vIOS-L3), образів ASA, Cisco IOL-образів, образів Cisco IPS, образів XRv і CSR1000v, образів dynamips з емулятора GNS, образів Cisco vWLC та vWSA. Крім перерахованих образів підтримується значний список з обладнання інших вендорів: Aruba ClearPass, Alcatel 7750 SR, Arista vEOS, Brocade Virtual ADX, Citrix Netscaler VPX virtual, Checkpoint Firewall, HP VSR1000, Juniper Olive (porting), Juniper Networks vMX router, Juniper vSRX, S-Terra Firewall, MS Windows та ін.

4 ПРОЄКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ

4.1 Опис проєктування комп'ютерної мережі

При проєктуванні комп'ютерної мережі було використано:

- 2 маршрутизатора CISCO 2911;
- 3 маршрутизатора CISCO 2811;
- 12 комутаторів CISCO 2960-24;
- 7 серверів;
- 1 міжмережевий екран;
- 5 принтерів;
- 48 персональних комп'ютерів.

В даній локальній мережі фізичним середовищем був оптичний кабель. З'єднання маршрутизатора дозволяє виконувати передачу даних на швидкості до 10 Гбіт/сек. Для інших елементів комп'ютерної мережі було використано провід кручена пара (див. рис. 4.1).

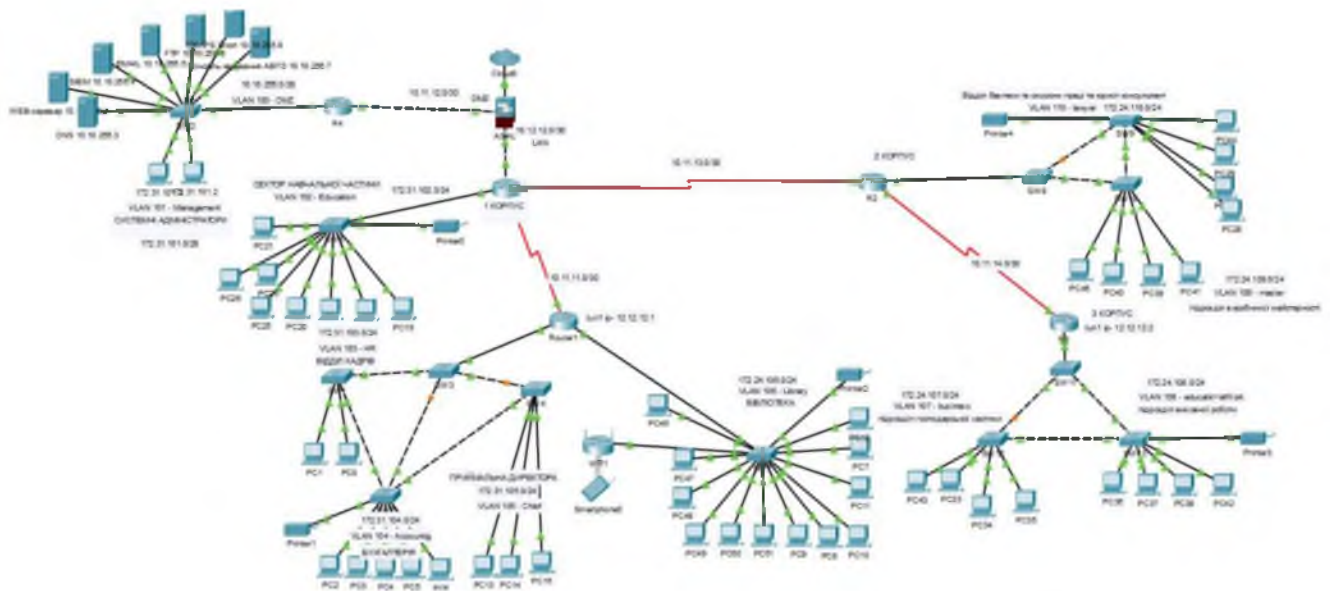


Рисунок 4.1 – Структурна схема після модернізації

4.2 Адресація комп'ютерної мережі

Адресація комп'ютерної мережі є важливим аспектом, що визначає унікальність кожного пристрою в мережі та дозволяє їм ефективно комунікувати один з одним. Унікальність тексту може бути досягнута шляхом використання індивідуальних IP-адрес для кожного пристрою.

IP-адреса (Internet Protocol Address) – це унікальний числовий ідентифікатор, призначений кожному пристрою в комп'ютерній мережі, який дозволяє їм здійснювати комунікацію в мережі Інтернет.

Існують дві версії IP-адрес: IPv4 і IPv6. IPv4 використовує 32-бітні адреси, в той час як IPv6 використовує 128-бітні адреси, що забезпечує значно більшу кількість унікальних адрес.

Кожен пристрій в мережі отримує свою власну IP-адресу, що може бути статичною (постійною) або динамічною (періодично змінюється). Статичні IP-адреси призначаються вручну адміністратором мережі, тоді як динамічні адреси

можуть бути автоматично призначені пристрою через протокол DHCP (Dynamic Host Configuration Protocol).

Унікальність IP-адрес забезпечується тим, що кожен пристрій в мережі отримує відмінну IP-адресу, яка ідентифікує його в мережі. Це дозволяє передавати дані точно до конкретного пристрою, що покращує ефективність комунікації в мережі.

В моєму випадку адресація вузлів динамічна, у цьому випадку адреси налаштовуються на кожному персональному комп'ютері автоматично.

Логічна адресація в LAN представлена в таблиці 4.1.

Таблиця 4.1 – Логічна адресація в LAN

Приналежність мережі	Мережа
мережа системних адміністраторів	172.31.101.0/28
мережа для сервісів (DMZ- демілітаризована зона)	10.10.255.0/28
мережа сектору навчальної частини	172.31.102.0/24
мережа відділу кадрів	172.31.103.0/24
мережа відділу бухгалтерії	172.31.104.0/24
приймальна директора	172.31.105.0/24
бібліотека	172.24.106.0/24
підрозділ господарської частини	172.24.107.0/24
підрозділ виховної роботи	172.24.108.0/24
підрозділ виробничої майстерні	172.24.109.0/24
відділ безпеки та охорони праці та юрист консультант	172.24.110.0/24
мережа, яка використовується для побудови GRE-тунелю	12.12.12.0/24
Службова мережа	10.11.12.0/30
	10.12.12.0/30
	10.11.11.0/30
	10.11.13.0/30
	10.11.14.0/30

4.3 Налаштування динамічної адресації

Налаштування динамічної адресації маршрутизатора R7 (див. рис. 4.2).

```

interface GigabitEthernet0/0.103
encapsulation dot1Q 103
ip address 172.31.103.1 255.255.255.0

interface GigabitEthernet0/0.104
encapsulation dot1Q 104
ip address 172.31.104.1 255.255.255.0

interface GigabitEthernet0/0.105
encapsulation dot1Q 105
ip address 172.31.105.1 255.255.255.0

interface GigabitEthernet0/1.106
encapsulation dot1Q 106
ip address 172.24.106.1 255.255.255.0

interface Serial0/3/0
ip address 10.11.11.2 255.255.255.252

ip dhcp pool HR
network 172.31.103.0 255.255.255.0
default-router 172.31.103.1
dns-server 10.10.255.3
ip dhcp pool Accounting
network 172.31.104.0 255.255.255.0
default-router 172.31.104.1
dns-server 10.10.255.3
ip dhcp pool Chief
network 172.31.105.0 255.255.255.0
default-router 172.31.105.1
dns-server 10.10.255.3
ip dhcp pool Library
network 172.24.106.0 255.255.255.0
default-router 172.24.106.1
dns-server 10.10.255.3

```

Рисунок 4.2 – Налаштування динамічної адресації маршрутизатора R7

Після налаштувань маршрутизаторів перейшли до налаштувань динамічної адресації персональних комп'ютерів на серверів (див. рис. 4.3).

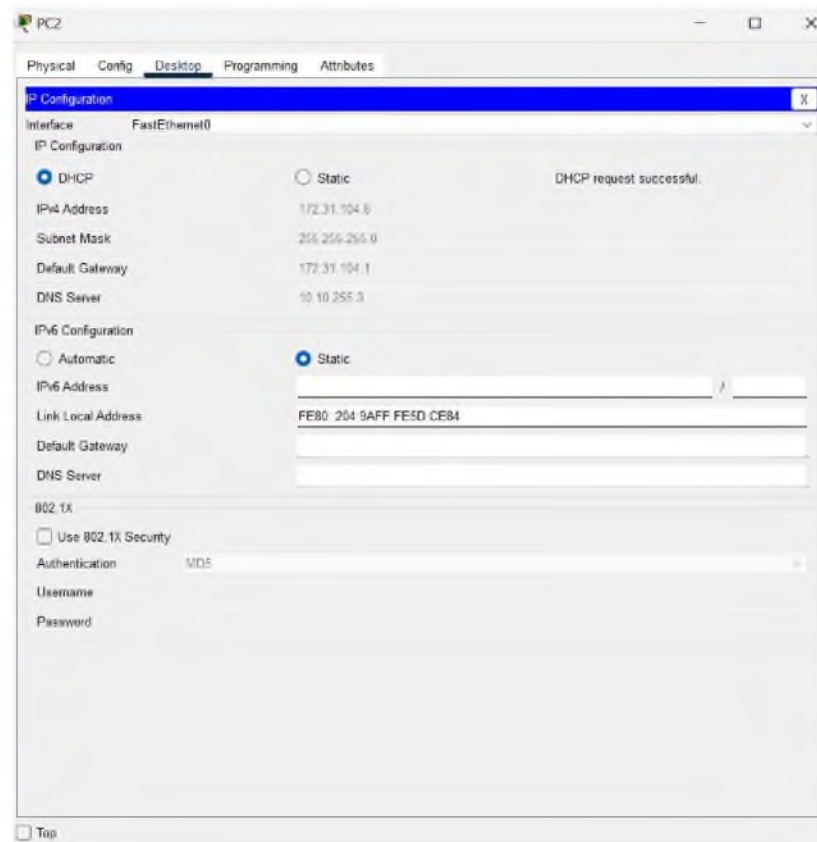


Рисунок 4.3 – Налаштування адресації на PC2

4.4 Налаштування VLAN

Сегментація мережі зроблена за допомогою VLAN. Налаштовуються вони за допомогою наступних команд (див. рис. 4.4).

```

vlan 106
name Education
int fa0/1
switchport mode trunk
switchport trunk allowed vlan 106
int range fa0/2-6, fa0/9
switchport mode access
switchport access vlan 106
switch port-security mac-address sticky

```

Рисунок 4.4 – Сегментація мережі за допомогою VLAN 106

4.5 Налаштування протоколу тунелювання

Протоколи тунелювання є важливими інструментами для забезпечення безпеки, конфіденційності та доступності мережевого трафіку, особливо в ситуаціях, коли мережі пов'язані через непевні або ненадійні мережі, такі як Інтернет.

У нашій мережі було обрано протокол GRE(Generic Routing Encapsulation), він володіє деякими особливостями, що роблять його корисним:

Простота реалізації: GRE дуже простий у реалізації, що робить його популярним в різних сценаріях мережевого тунелювання.

Підтримка багатьох протоколів: GRE може тунелювати різні мережеві протоколи, включаючи IPv4, IPv6 та IPX.

Гнучкість маршрутизації: GRE не має власної механіки маршрутизації і може тунелювати будь-які мережеві пакети, що робить його відмінним вибором для різних сценаріїв.

У нашій мережі тунель налаштований між маршрутизатором R7 та R5 за допомогою наступних команд(див. рис. 4.5).

Для маршрутизатора R7:

```
interface Tunnel1
ip-address 12.12.12.1 255.255.255.0
mtu 1476
tunnel source Serial0/3/0
tunnel destination 10.11.14.2
router ospf 1
log-adjacency-changes
network 12.12.12.0 0.0.0.255 area 0
network 172.31.103.0 0.0.0.255 area 0
network 172.31.104.0 0.0.0.255 area 0
network 172.31.105.0 0.0.0.255 area 0
network 172.24.106.0 0.0.0.255 area 0
network 10.11.11.0 0.0.0.3 area 0
```

Для маршрутизатора R5:

```
interface Tunnel1
ip-address 12.12.12.2 255.255.255.0
mtu 1476
tunnel source Serial0/1/0
tunnel destination 10.11.11.2
router ospf 1
log-adjacency-changes
network 12.12.12.0 0.0.0.255 area 0
network 10.11.14.0 0.0.0.3 area 0
network 172.24.107.0 0.0.0.255 area 0
network 172.24.108.0 0.0.0.255 area 0
```

Рисунок 4.5 – Налаштування тунелі між маршрутизатором R7 та R5

4.6 Налаштування сервісів

В даній роботі було налаштовано такі сервери:

- DNS-сервер;
- вебсервер;
- поштовий сервер;
- FTP-сервер;
- SIEM сервер.

Налаштування вебсервера зображено на рисунках 4.6, 4.7.

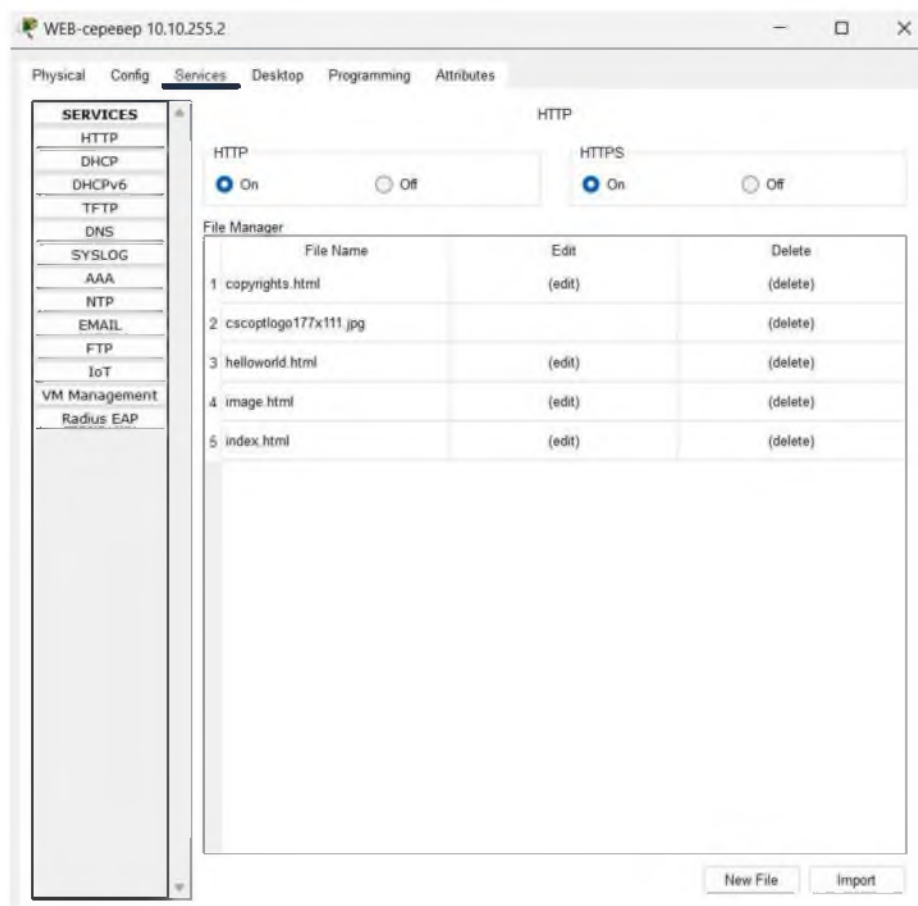


Рисунок 4.6 – Конфігурація вебсервера

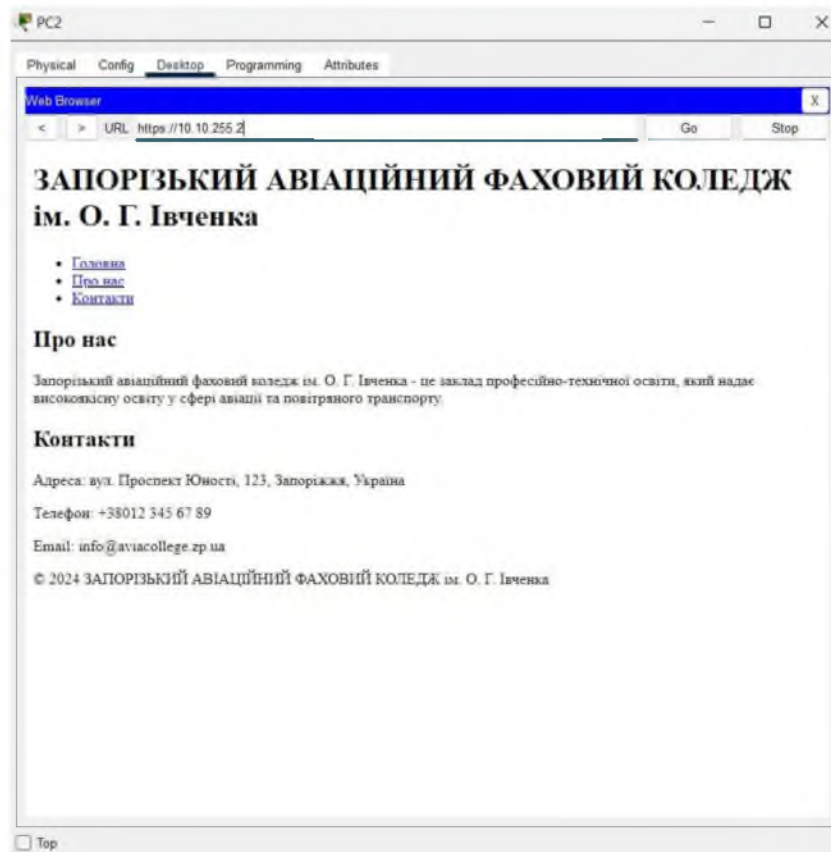


Рисунок 4.7 – Приклад вебсторінки

Після адресації комп'ютерів було налаштовано адресація сервера DNS (див. рис. 4.8). Було здійснено налаштування сервера DNS для комфортної роботи особового складу. DNS-сервер – це сервер, який містить базу даних публічних IP-адрес та пов'язаних з ними імен хостів. Як правило, DNS-сервер виконує роль перекладача, дозволяючи або переводячи імена хостів в IP-адреси. В результаті виходить ряд чисел, що стає зрозумілим людині URL. DNS-сервери використовують спеціальне програмне забезпечення та взаємодіють один з одним окремими протоколами. У процесі обробки запитів вони призначають правильну IP-адресу URL-адресою або правильну URL-адресу IP-адреси.

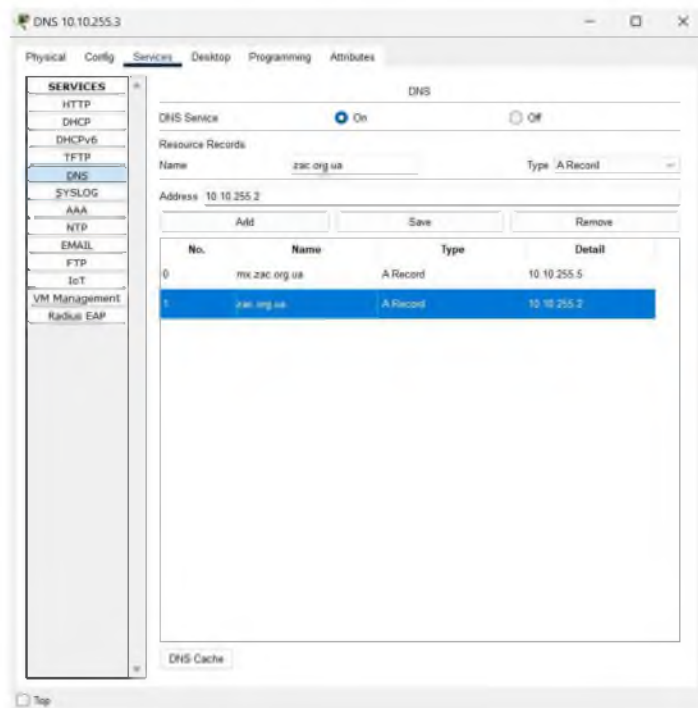


Рисунок 4.8 – DNS-сервер

Поштовий сервер налаштований для зручної роботи всіх працівників цієї організації. Розгорнуто поштовий сервер, а також створено поштові скриньки для користувачів. Для налаштування поштової скриньки необхідно вказати доменне ім'я, ім'я користувача та пароль (див. рис. 4.9).

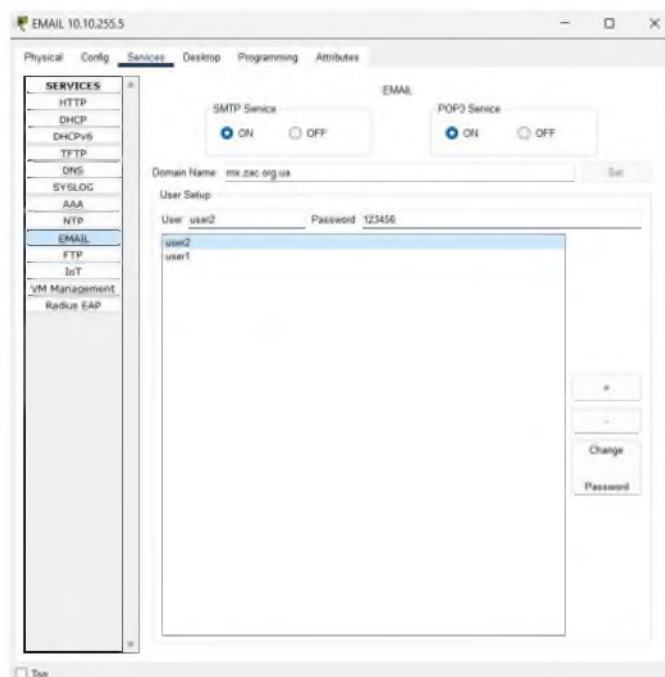


Рисунок 4.9 – Налаштування поштового сервера

Для налаштування сервера документообігу, мережного емулятора Cisco Packet Tracer недостатньо. Для компенсації цього було розгорнуто FTP-сервер, обмінюватись файлами (див. рис. 4.10). FTP-сервер, який буде використовуватися для розміщення навчальних матеріалів, а також резервних копій налаштувань телекомунікаційного обладнання.

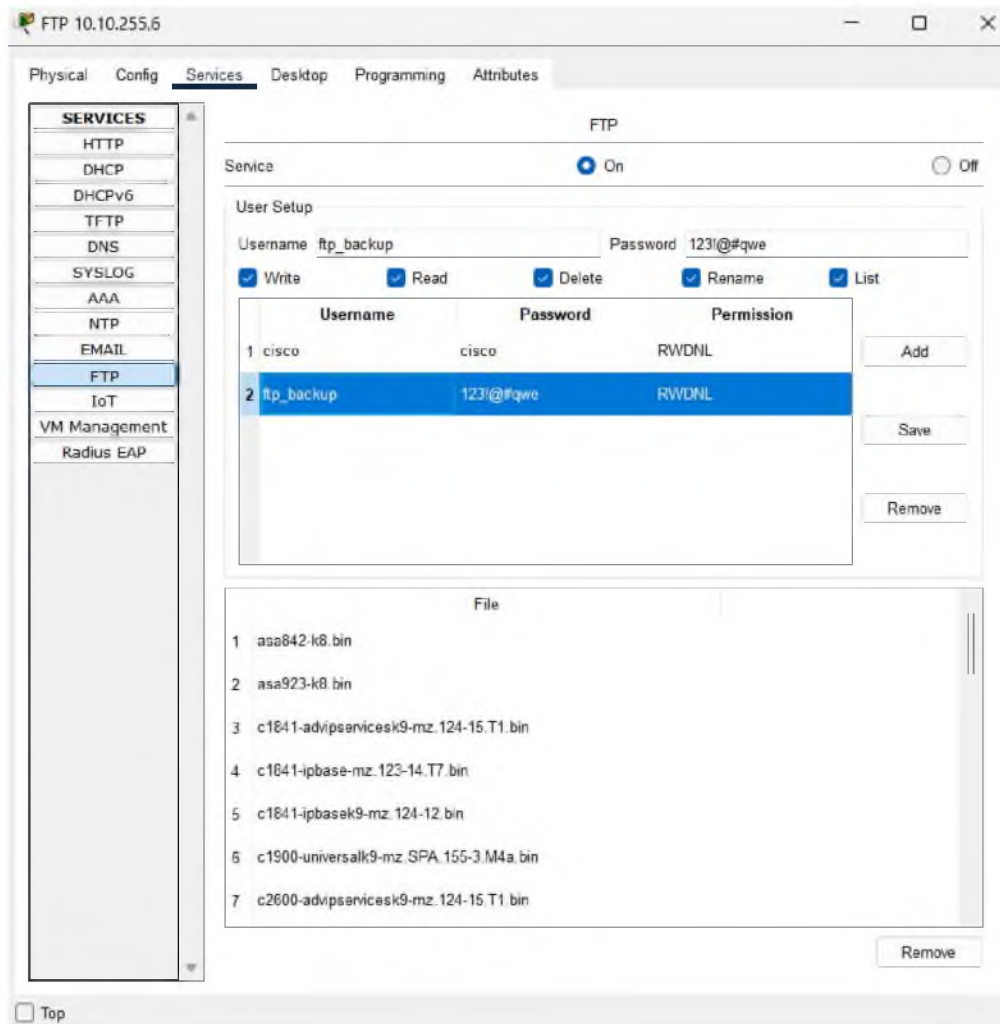


Рисунок 4.10 – Налаштування FTP-серверу

SIEM - це програмне забезпечення, яке об'єднує в собі функціонал реєстрації, аналізу та відслідковування подій з різних джерел у реальному часі з метою виявлення інцидентів безпеки, управління потенційними загрозами та забезпечення відповідності нормативно-правовим вимогам.

Основні функції SIEM:

- моніторинг подій: збір, агрегація та аналіз подій з різних джерел, таких як лог-файли, системні журнали, мережеві протоколи тощо;
- детекція загроз: виявлення потенційно небезпечних або аномальних активностей, які можуть вказувати на атаку або порушення безпеки;
- відгук на інциденти: автоматизоване або ручне управління відповідями на виявлені загрози з метою мінімізації ризиків та наслідків;

Переваги використання SIEM:

- підвищення рівня безпеки: реагування на потенційні загрози швидше та ефективніше;
- відповідність вимогам: можливість вести журнали подій та забезпечувати відповідність з регуляторними вимогами;
- зниження ризиків: попередження втрат даних, порушень безпеки та інших інцидентів.

В якості SIEM було обрано рішення Splunk (див. рис. 4.11).

Роль Splunk в SIEM:

- Splunk є однією з провідних платформ SIEM, яка надає розширені можливості аналізу та візуалізації даних;
- вона дозволяє збирати, аналізувати та використовувати дані з різних джерел для виявлення загроз та аномальних активностей;
- Splunk також надає інструменти для автоматизації реагування на інциденти та управління їх наслідками.

Приклади використання SIEM та Splunk:

- великі корпоративні компанії: для моніторингу та захисту великих мереж та інфраструктури в реальному часі;
- організації з високими вимогами до безпеки: для виявлення та реагування на загрози та інциденти безпеки даних;
- постачальники послуг з обробки даних: для забезпечення безпеки та відповідності вимогам щодо захисту персональних даних.

Splunk – це спеціалізована SIEM платформа для збору, зберігання, аналізу, моніторингу та аналітики інформації. Особливість платформи полягає в роботі з різними джерелами даних, на кшталт віртуального і фізичного хоста, різних IoT-пристроїв, хмари, CRM системи і іншого.

У продукті є великий набір операцій з даними з безпеки, включаючи оцінку рівня безпеки системи, моніторинг, попередження та обробку інцидентів, CSIRT, аналіз порушень і реакція на них, кореляцію подій.

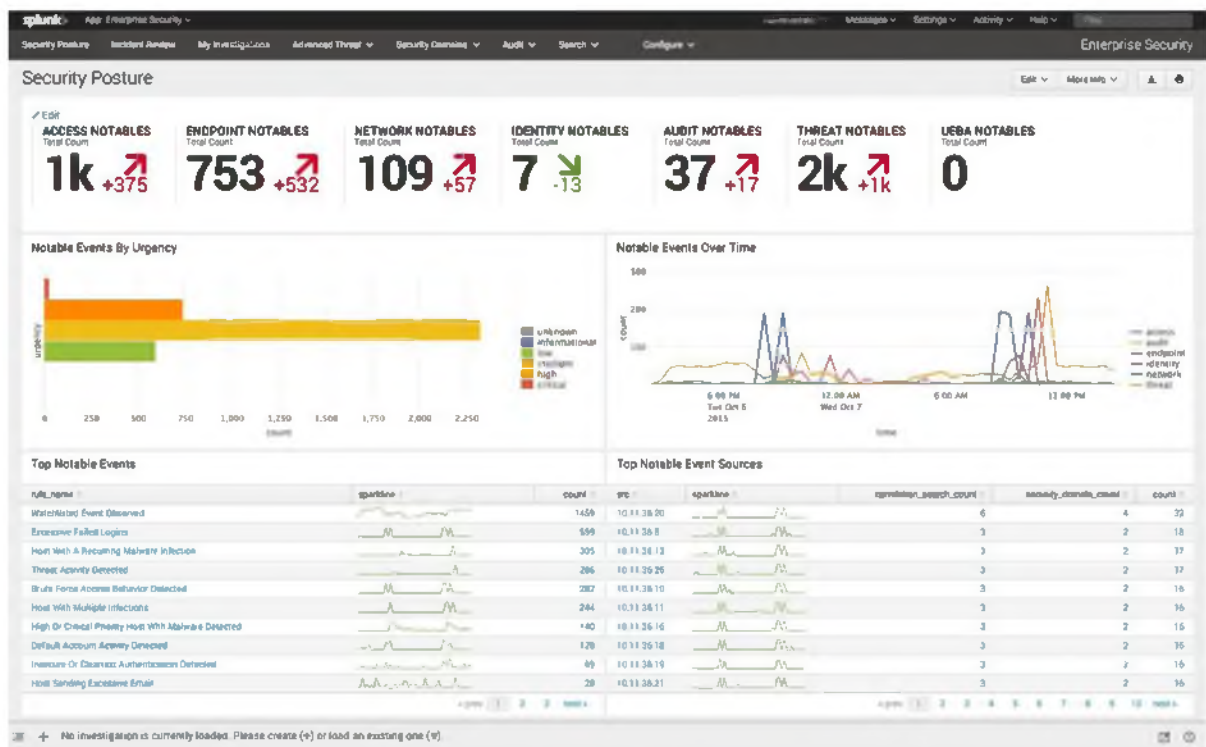


Рисунок 4.11 – SIEM Splunk

В якості консолі віддаленого керування антивірусним програмним забезпечення було обрано ESET PROTECT дозволяє керувати продуктами ESET на робочих станціях, серверах і мобільних пристроях, які працюють у мережі, з єдиного центру.

Веб-консоль ESET PROTECT дозволяє розгортати рішення ESET, керувати задачами, примусово застосовувати політики безпеки, відстежувати статус системи й швидко реагувати на проблеми чи загрози на віддалених комп'ютерах.

До складу ESET PROTECT входять такі компоненти:

- ESET PROTECT сервер – Цей сервер керує обміном даними з агентами, а також збирає та зберігає дані програми в базі даних. ESET PROTECT Сервер можна інсталиювати на серверах Windows і Linux; він також надається як віртуальний пристрій;
- веб-консоль ESET PROTECT. Веб-консоль є основним інтерфейсом, який дозволяє керувати клієнтськими комп'ютерами у вашому середовищі. У цій консолі відображається стан клієнтів у вашій мережі; вона дає змогу вам розгорнути рішення ESET на некерованих комп'ютерах віддалено.
- ESET Management Agent: забезпечує обмін даними між ESET PROTECT Server і клієнтськими комп'ютерами. Для встановлення зв'язку між комп'ютером і ESET PROTECT Server агент має бути інстальований на клієнтському комп'ютері.
- Rogue Detection Sensor. Rogue Detection Sensor виявляє у вашій мережі комп'ютери, які ще не контролюються, та надсилає їх дані на сервер ESET PROTECT. Це дає змогу керувати новими клієнтськими комп'ютерами в ESET PROTECT без потреби вручну шукати й додавати їх.
- консоль віддаленого керування антивірусним програмним забезпеченням, яке встановлено на комп'ютері.

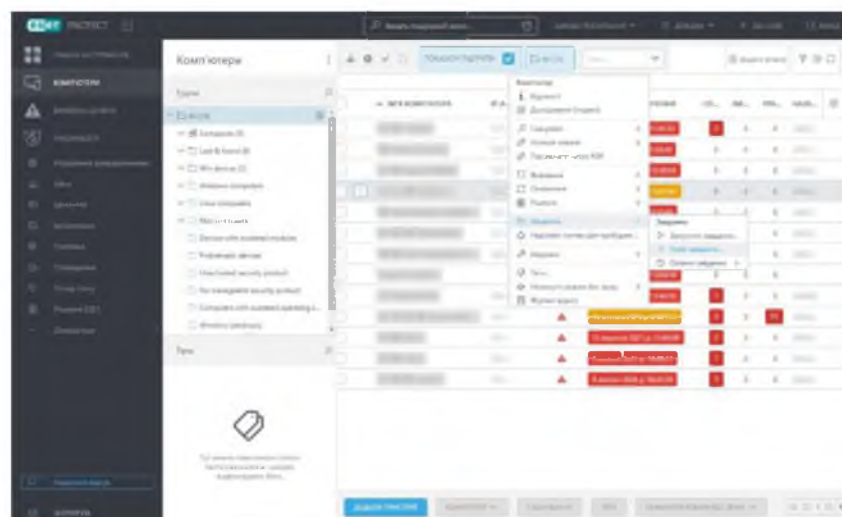


Рисунок 4.12 – Консоль віддаленого керування антивірусним програмним забезпеченням

Кібербезпека є важливим питанням як для науковців, так і для практиків, оскільки успішні кібератаки можуть призвести до астрономічних витрат через втрату конфіденційності, цілісності або доступності. Для виявлення кібератак були запропоновані різні підходи до забезпечення безпеки, серед яких найпоширенішими є системи виявлення вторгнень (IDS) та системи виявлення мережових вторгнень (NIDS).

Багато розроблених методів і підходів до виявлення NIDS часто класифікують як засновані на аномаліях (ANIDS) або засновані на сигнатурах (SNIDS). Системи на основі аномалій оцінюють типову поведінку системи і видають попередження, коли відхилення від нормальної поведінки досягає певного порогу. Методи на основі сигнатур перевіряють дані на наявність шаблонів (сигнатур) у досліджуваних даних і видають попередження, якщо вони відповідають відомим загрозам.

Однією з провідних систем виявлення та запобігання вторгнень на основі сигнатур у світі кібербезпеки є Snort. Snort – це система запобігання вторгненням з відкритим вихідним кодом, яка може аналізувати та реєструвати пакети в режимі реального часу. Snort є найпоширенішим у світі рішенням IDS/IPS, що поєднує в собі переваги перевірки на основі підписів, протоколів та аномалій. Завдяки мільйонам завантажень і приблизно 400 000 зареєстрованих користувачів, Snort став галузевим стандартом для систем запобігання вторгненням (IPS).

У нашій мережі Snort буде відслідковувати аномальну та нетипову поведінку в мережі де знаходяться всі сервіси. І буде відслідковувати за допомогою наступних налаштувань:

- виявлення спроб використання відомих вразливостей (alert tcp any any -> 10.10.255.0/28 any (msg:"Attempted Use of Known Vulnerability"; content:"|90 02 9E B6|"; sid:100006;));
- виявлення можливих атак на веб-додатки (alert tcp any any -> 10.10.255.0/28 80 (msg:"Web Application Attack"; uricontent:"/phpmyadmin"; nocase; sid:100007));
- виявлення SQL-ін'єкцій(alert tcp any any -> 10.10.255.0/28 1433 (msg:"SQL Injection Attempt"; content:"select"; nocase; content:"from"; nocase; sid:100008));

- виявлення атак на DNS(alert udp any any -> 10.10.255.0/28 53 (msg:"DNS Attack"; content:"|00 20|"; sid:100009));
- виявлення спроб експлуатації слабких паролів (alert tcp any any -> 10.10.255.0/28 22 (msg:"SSH Weak Password Attempt"; content:"password"; nocase; sid:100010));
- виявлення спроб атаки на FTP(alert tcp any any -> 10.10.255.0/28 21 (msg:"FTP Attack"; content:"USER "; nocase; sid:100011))
- виявлення небезпечних скриптів в HTTP-трафіку (alert tcp any any -> 10.10.255.0/28 80 (msg:"Malicious HTTP Script"; content:"<script>"; nocase; sid:100012));
- виявлення спроб атак на веб-сервер Apache (alert tcp any any -> 10.10.255.0/28 80 (msg:"Apache Web Server Attack"; content:"GET /cgi-bin/"; nocase; sid:100013));
- виявлення можливих атак на SSL/TLS(alert tcp any any -> 10.10.255.0/28 443 (msg:"SSL/TLS Attack"; content:"|16 03|"; sid:100014));
- виявлення спроб перехоплення сесій (Session Hijacking) (alert tcp any any -> 10.10.255.0/28 any (msg:"Session Hijacking Attempt"; flags:A+; sid:100015));
- виявлення спроб сканування портів з високою швидкістю (alert tcp any any -> 10.10.255.0/28 any (msg:"High Speed Port Scan Detected"; threshold: type limit, track by_src, seconds 1, count 10; sid:100016));
- виявлення спроб атаки типу Denial of Service (DoS)(alert udp any any -> 10.10.255.0/28 53 (msg:"DNS DoS Attack"; content:"|00 20|"; threshold: type limit, track by_src, seconds 10, count 5; sid:100017));

Якщо пакети будуть співпадати згідно написаних правил, то Snort буде відправляти сповіщення на SIEM Splunk і адміністратор матиме змогу оперативно реагувати на кіберінцидент.

4.7 Перевірка працездатності мережі

Для перевірки працездатності мережі можна виконати передачу пакетів між різними пристроями мережі або перейти на сервери.

На рисунку 4.13 показано, що у користувачів є доступ до користувацького серверу.

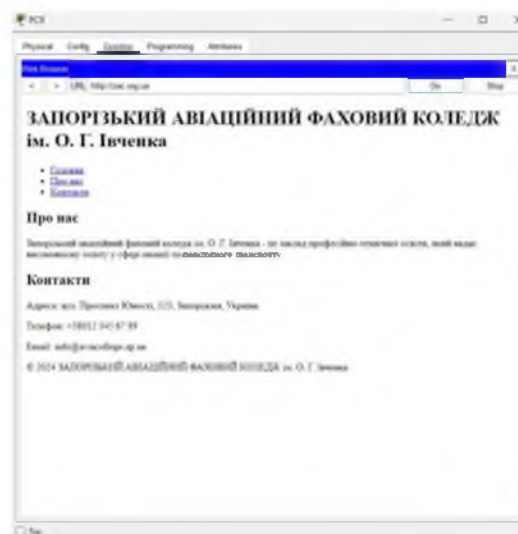


Рисунок 4.13 – Перевірка доступу до серверів

Перевірити коректно налаштовану мережу можна також за допомогою використання команди `tracert` та `ping` у командній строці (див. рис. 4.14).

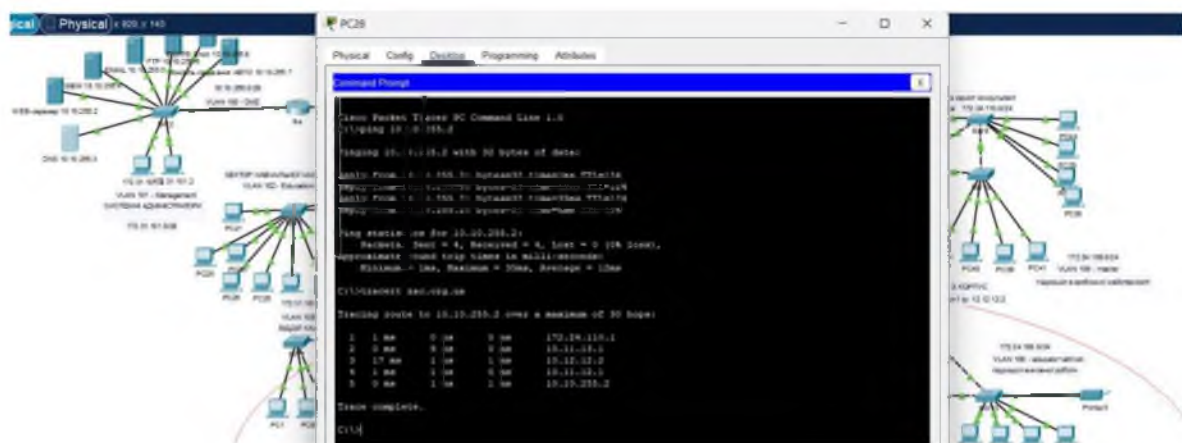


Рисунок 4.14 – Результат використання команди `tracert` та `ping`

5 МОНТАЖ ЛОКАЛЬНОЇ МЕРЕЖІ

5.1 Підключення розетки RJ – 45

Для монтажу знадобиться зовнішня розетка RJ-45 категорії 5е, пристрій для зачистки кручений пари, ударний інструмент для закладення в модуль Keystone, кабель кручена пара.

Крок 1. Встановлення зовнішньої розетки RJ-45 (див. рис. 5.1) на стіну монтаж розетки RJ-45 Зніміть кришку розетки, виберіть місце встановлення та закріпіть основу корпусу розетки на стіні за допомогою шурупів. Залежно від типу поверхні стіни можна використовувати дюбелі чи інші елементи кріплення. Для проходу кабелю зробіть вирізи кабельного каналу за допомогою кусачок або іншого інструменту.



Рисунок 5.1 – Встановлення зовнішньої розетки RJ-45

Крок 2. Зняття верхньої оболонки кабелю (див. рис. 5.2). Інструмент для зачищення та обрізання кабелю кручена пара має бути правильно відрегульований під встановлюваний тип кабелю. Розташуйте кабель в інструменті, акуратно

поверніть інструмент на 360 градусів та зніміть верхню ізоляцію. Після зняття зовнішньої оболонки перевірте ізоляцію провідників, вона не повинна бути пошкоджена.



Рисунок 5.2 - Зняття верхньої оболонки кабелю

Крок 3. Розкладка та закладення кабелю в модулі Keystone (див. рис. 5.3) . У процесі монтажу локальної мережі необхідно дотримуватись єдиного стандарту T568A або T568B в межах всієї структурованої кабельної системи. Розкладіть кручені пари на контакти модуля відповідно до зазначеної нумерації та кольорового маркування. Зріз зовнішньої оболонки кабелю повинен бути якомога ближче до контактів модуля зменшення розвитку пар. Також для скорочення розвитку пар рекомендується розкласти кручені пари без їх розплетення. Перед забиванням провідників у контакти модуля оберіть відповідний ударний інструмент під цей тип контактів – Krone або IDC 110. Встановіть інструмент у контакт модуля над провідником і переконайтеся, що ніж інструмента для обрізки знаходиться із зовнішнього боку модуля. Натисніть різко на інструмент до натискання, при цьому провідник забивається в контакт і обрізається. Забийте за таким же принципом провідники, що залишилися.



Рисунок 5.3 – Розкладка та закладення кабелю в модулі Keystone

Крок 4. Встановлення модулів у розетку та закриття кришки Вставте модуль RJ-45 в основу розетки і приєднайте лицьову кришку. Нанесіть маркування розеток відповідно до проекту. Підключіть всі розетки, що залишилися, і перевірку СКС проведіть на відповідність вимогам стандартів.

5.2 Монтаж оптоволоконних конекторів

При будівництві будь-якої волоконно-оптичної лінії необхідно проводити монтаж сполучних муфт та кінцевих пристроїв. При підключенні кінцевих пристроїв на кінці ОВ має бути конектор, тобто завдання монтажника - обтиснути оптоволоконний кабель, встановити конектор.

Крім підключення до обладнання, оптичний конектор використовується для вимірювальних приладів та здійснення перемикань.

Способи монтажу оптичних конекторів:

- виготовлення конектора на місці (клейова технологія);

- приварювання пігтейлу (оптичного шнура з конектором);
- монтаж неполірованого конектора (з використанням механічного з'єднання) або Fast-конектора;
- монтаж конектора, що приварюється (технологія Splice-On).

Перший спосіб існує досить давно, для монтажу необхідно підготувати ВВ у ферул конектора, за допомогою шприца залити клей і вставити туди підготовлене ВВ. Потім почекати поки висохне клей, за допомогою ручки-скальвателя зколоти ОВ, що виходить за межі ферула. За допомогою спецнабору абразивів зробити полірування. При цьому лише полірування класу SPC.

Приварювання пігтейлу - найпростіший, тому що використовується заводський оптичний шнур з конектором. Може бути будь-який вид конектора, з будь-яким поліруванням. Для монтажу необхідно мати зварювальний апарат та набір інструменту для підготовки ОВ.

Монтаж неполірованого конектора передбачає використання з'єднувача з торцем, що відполірується, з волокном. З'єднання з ВВ здійснюється механічним з'єднувачем, усередині якого знаходиться імерсійний гель, який у свою чергу прибирає похибку юстування та встановлення ВВ. До цього способу можна віднести так звані FAST-конектори. У них також використовується імерсійний гель, тільки спосіб монтажу трохи відрізняється.

Монтаж за технологією Splice-On передбачає приварювання конектора, в якому ВВ вже встановлене і відполіроване у ферулі, при цьому є необхідна довжина ВВ для здійснення зварювання волокна. Деякі з виробників апаратів є виробниками таких конекторів Splice-On, при цьому конектори не універсальні - вони виробляються лише під конкретні апарати та притискні майданчики. Тому не рекомендується монтувати конектори одного виробника на апаратах інших виробників – можуть не підійти за розмірами.

Кожен із способів монтажу конекторів має свої переваги та недоліки, тому можна визначати їх місце застосування. Клейовий спосіб досить специфічний, оскільки потрібен час для висихання клею. Відповідно, критичний до температури

навколишнього середовища та чистоти повітря. Це досить незручно у польових умовах і більше підходить для лабораторних умов чи виробництв.

Монтаж пігтейлів - найпростіший, дешевий і надійний спосіб монтажу конектора. Цей спосіб застосовується при монтажі кросів різної густини, при підключенні абонентських ліній на мережах FTTH. При цьому до недоліків можна віднести лише необхідність застосування зварювального апарату, сколювальної ОВ, які потрібно придбати, а це досить затратно.

Менш витратний спосіб - монтаж Fast-конекторів і неполіровані конекторів. Для їх встановлення не потрібне використання зварювального апарату, достатньо наявності сколювача та стриперів для зачистки ОВ. Даний вид конекторів розроблений для використання на мережах FTTH, для монтажу абонента в квартирі або підключення до вуличної крос-муфти, яка, як правило, встановлюється на опорі. Якщо використовувати конектори низької якості, то з часом якість з'єднання погіршується, зростають втрати, а потім взагалі втрачається сигнал. Зварні конектори, як і Fast-конектори, передбачається використовувати на мережах FTTH або там, де немає можливості розташувати КДЗС та запас волокна та пігтейлу. Даний варіант досить зручний і надійний, але має кілька особливостей: монтажник повинен мати певні навички монтажу таких конекторів, оскільки можливість повторного монтажу у них відсутня. При цьому потрібно вибирати конектор того ж виробника, що і зварювальний апарат, щоб виконати монтаж без проблем.

Для підготовки до монтажу конекторів зазвичай використовується стандартний набір інструментів. До них відноситься інструмент для оброблення оптичного кабелю та шнурів - стрипери для видалення буферного та акрилового покриття, ножиці для видалення арамідних ниток, плоскогубці, бокорізи, сколювач, серветки, пропанол. Для монтажу пігтейлу потрібний зварювальний апарат. Для монтажу конекторів, що не поліруються, додається монтажний столик або стрипер для оброблення дроп-кабелю. При монтажі зварних конекторів Splice-On необхідний набір спеціальних притискних майданчиків для зварювального апарату.

5.3 Підключення мережевого обладнання

Комутатори і концентратори підключаються до локальної мережі однаково. Якщо використовується кілька комутаторів, то вони об'єднуються між собою кабелем UTP з «перевернутої» розводкою (T568A - T568B). Довжина кабелю повинна бути не менше 0,5 м (див. рис. 5.4).

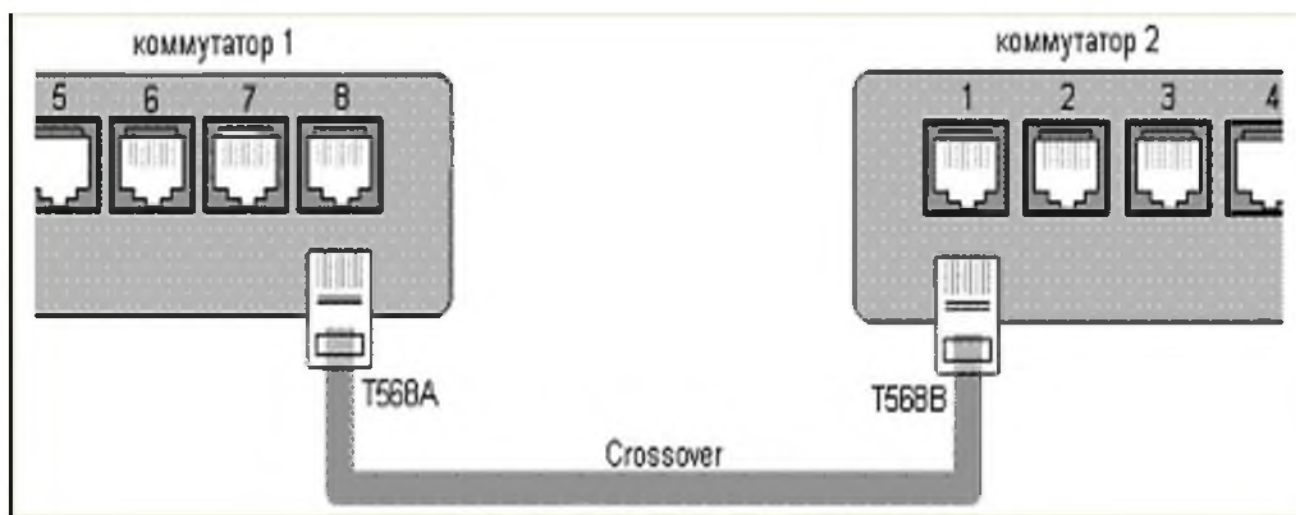


Рисунок 5.4 -З'єднання комутаторів кабелем з розводкою по стандарту T568A – T568B

У багатьох моделях комутаторів поряд з простими портами використовується додатковий порт “Uplink”. Він сполучений з одним із простих портів і має «перевернуту» розводку відповідно до стандарту T568A.

Використовуючи цей порт можна підключати другий комутатор простим кабелем (T568B - T568B) (див. рис. 5.5).



Рисунок 5.5 - Використання порту "Uplink" для підключення кабелю з розводкою по стандарту T568B - T568B

В сучасних комутаторах реалізована функція автоматичного визначення типу кабелю. Кожен порт комутатора може самостійно визначити стандарт підключеного до нього кабелю. В результаті порт сам визначає в якому режимі йому працювати. Функція автоматичного визначення типу кабелю значно полегшує роботу адміністратора мережі.

Адміністратори можуть підключати пристрої до комутатора без потреби у визначенні типу кабелю, що зменшує час на налаштування мережі і дозволяє швидше вводити її в експлуатацію. Завдяки автоматичному визначенню типу кабелю, мережа стає більш адаптивною до змін. Підключення нових пристроїв або зміна конфігурацій стають простішими, оскільки не потрібно враховувати тип кабелю. Також, оскільки функція автоматичного визначення типу кабелю зменшує кількість необхідних спеціалізованих кабелів, організації можуть зекономити на закупівлі та зберіганні різних типів кабелів.

ВИСНОВКИ

У ході виконання кваліфікаційної дипломної роботи було модернізовано локальну комп'ютерну мережу для Запорізького авіаційного фахового коледжу.

У ході модернізації локально-обчислювальної мережі Запорізького авіаційного фахового коледжу було ідентифіковано ключові вимоги та функціональні обов'язки локально-обчислювальної мережі: доступ до Інтернету, доступ до мережного принтера, реалізація бездротової мережі. Для прокладання каналів потрібно виконання ряду монтажних робіт, для виконання яких потрібно додаткове обладнання.

Було зроблено вибір активного мережного обладнання та складено схему комунікацій з умовними позначеннями.

В процесі аналізу мережі було розглянуто обладнання компанії CISCO. В мережі вже застосовується обладнання цієї фірми; відповідне співвідношення "ціна / якість", що є значущою першопричиною з урахуванням обсягу виділених коштів. Обладнання компаній CISCO задовольняє всім вимогам.

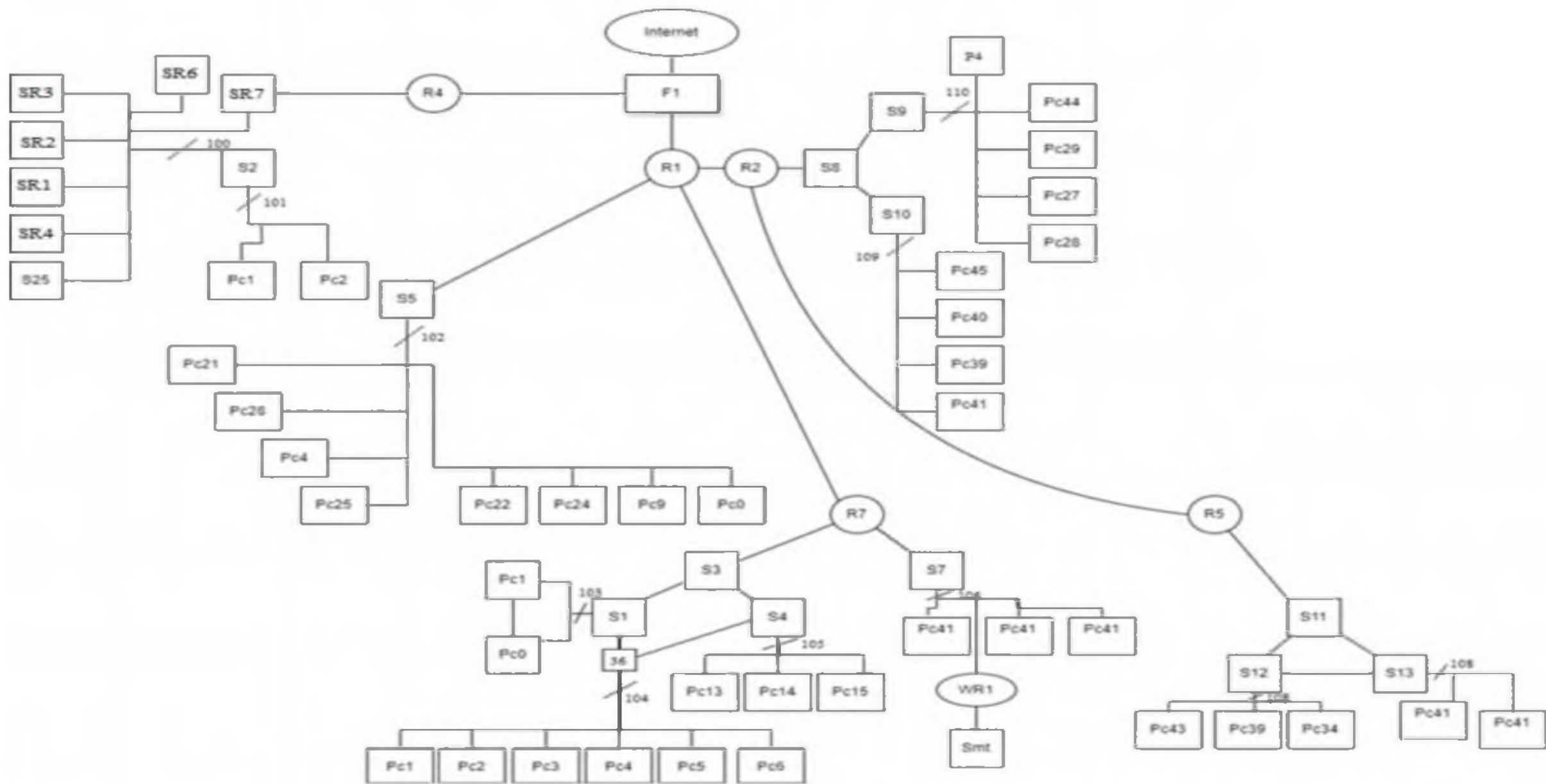
У ході виконання даної кваліфікаційної роботи було досягнуто наступних результатів:

- розглянуто та проаналізовано ключові аспекти побудови локальних мереж.
- модернізовано локально-обчислювальну мережу для запорізького авіаційного фахового коледжу.
- обрано програмне забезпечення та обґрунтовано його доцільність використання.
- виконано проєктування мережі, а саме виконано адресацію комп'ютерної мережі, налаштовано динамічну адресацію та VLAN, зроблено налаштування сервісів.
- описано процедуру виконання монтажу локальної мережі запорізького авіаційного фахового коледжу.
- підготовлено робочу документацію.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

- 1 Базові поняття мережевих технологій. URL: <https://mobiz.com.ua/bazovi-poniattiamerezhevykh-tekhnologij.html> (дата звернення: 06.05.2024).
- 2 Василенко М.М. Комп'ютерні мережі: навчальний посібник. Київ: Ліра-К, 2018. 304 с.
- 3 Городянин А.В., Слюсарь І.І. Організація віддаленого доступу в корпоративних інформаційних системах. *Матеріали щорічної студентської наукової конференції Полтавської державної аграрної академії*, 17 листопада 2020 р. Полтава: ПП «АСТРАЯ», 2020. С. 15-17.
- 4 Грищенко В. В. Бездротові мережі передачі даних: навчальний посібник. Київ: Видавничий дім "Слово", 2019. 256 с.
- 5 Карпенко М.Ю., Макогон Н.В. Конспект лекцій з курсу «Комп'ютерні мережі». Харків: ХНУМГ, 2019. 45 с.
- 6 Слюсарь І.І., Поліщук Ю.В. Реалізація MultiWAN та його маршрутизація за допомогою Mikrotik RouterOS. URL: <http://dSPACE.pdaa.edu.ua:8080/handle/123456789/8772> (дата звернення 05.05.2024).
- 7 Клименко О. О. Основи цифрової обробки сигналів: навчальний посібник. Київ: Видавничий дім "Києво-Могилянська академія", 2018. 336 с.
- 8 Курочкін, О. В. Мережі зв'язку: теорія та практика. Київ: Видавничий дім "ІНЖЕНЕР", 2019. 496 с.
- 9 Чернега В., Платнер Б. Безпроводні комп'ютерні мережі: навч. посібн. Київ: Кондор, 2018. 236 с.
- 10 Офіційний сайт компанії Cisco Packet Tracer. URL: <https://www.cisco.com/> (дата звернення: 20.05.2024).

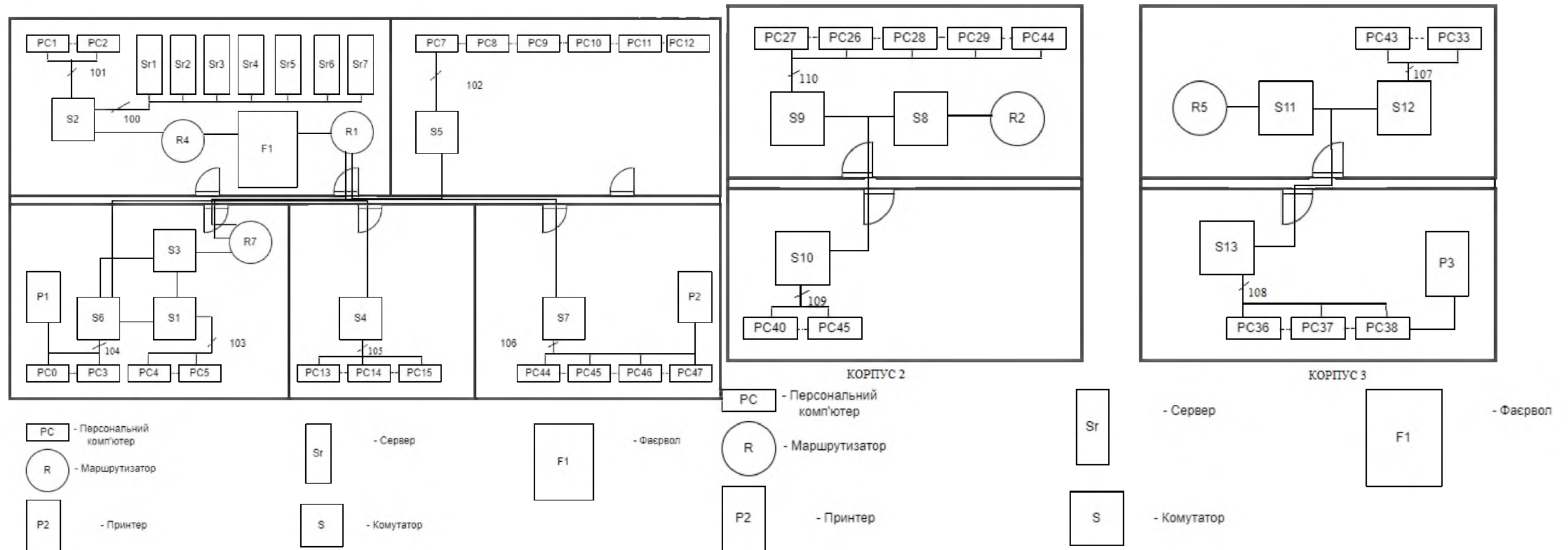
Структурна схема мережі



- PC - Персональний комп'ютер
- R - Маршрутизатор
- P2 - Принтер
- Sr - Сервер
- S - Комутатор

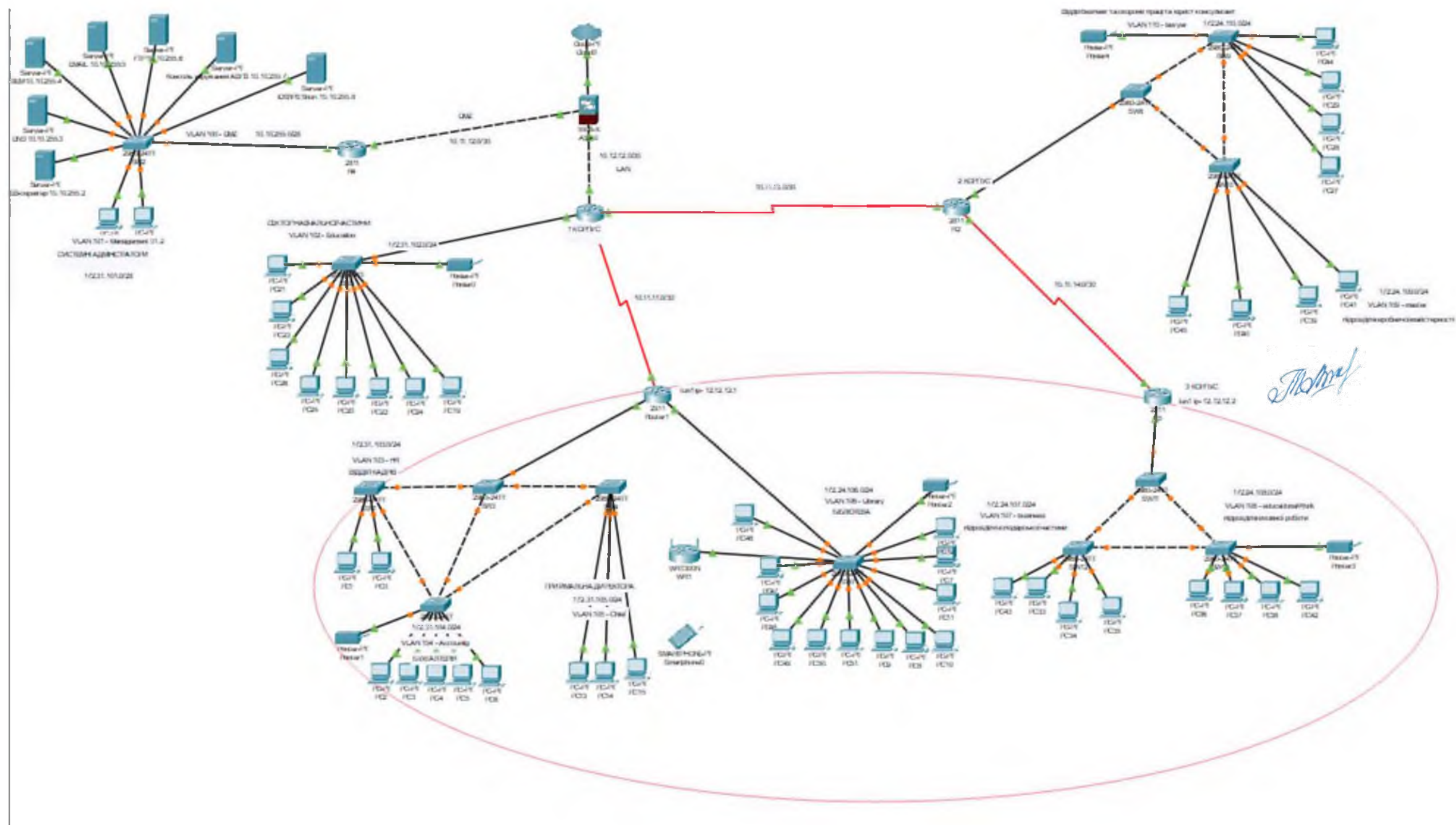
					13.02070849.51126 ПЛ1						
					Модернізація комп'ютерної мережі Запорізького авіаційного фахового коледжу	Літ.		Маса	Масштаб		
Зм	Лист	№ докум.	Підп.	Дата							
Розроб.		Косяк А.К.									
Перевір.		Тягунова М.Ю.									
Т. контр.					Структурна схема мережі	Лист. 1		Листів 1			
						НУ «Запорізька політехніка» КНТ-511сп					
Н. контр.		Щербак Н.В.									
Затв.		Кудерметов Р.К.									

Схема приєднування мережі



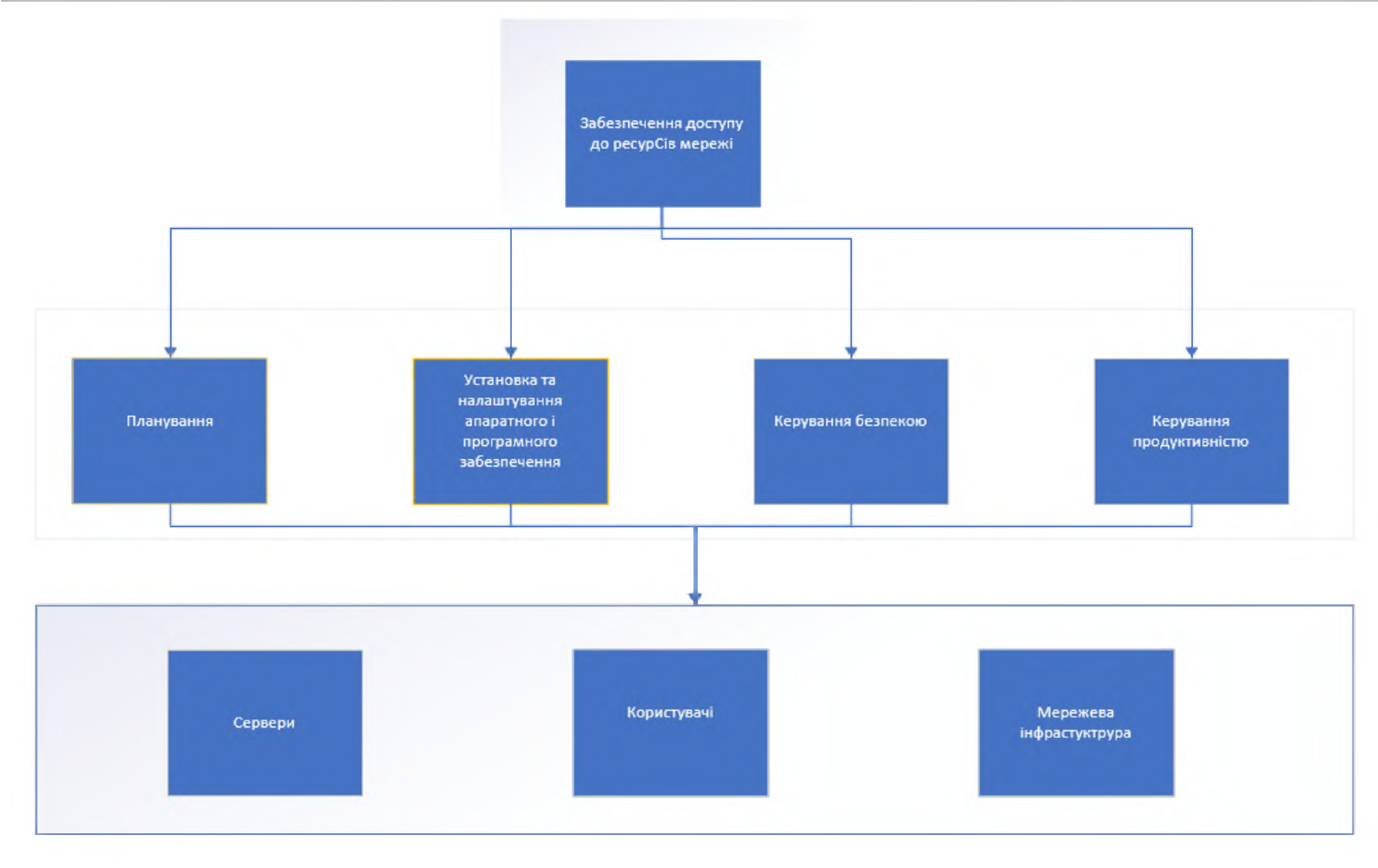
					13.02070849.51126 ПЛ2				
					Модернізація комп'ютерної мережі Запорізького авіаційного фахового коледжу	Літ.	Маса	Масштаб	
Зм	Лист	№ докум.	Підп.	Дата					
Розроб.		Косяк А.К.							
Перевір.		Тягунова М.Ю.							
Т. контр.									
					Схема приєднування мережі	Лист. 1	Листів 1		
						НУ «Запорізька політехніка» КНТ-511сп			
Н. контр.		Щербак Н.В.							
Затв.		Кудерметов Р.К.							

Загальна модель мережі



					13.02070849.51126 ПЛЗ				
					Модернізація комп'ютерної мережі Запорізького авіаційного фахового коледжу	Літ.	Маса	Масштаб	
Зм	Лист	№ докум.	Підп.	Дата					
Розроб.		Косяк А.К.							
Перевір.		Тягунова М.Ю.							
Т. контр.									
					Загальна модель мережі	Лист. 1	Листів 1		
Н. контр.		Щербак Н.В.				НУ «Запорізька політехніка» КНТ-511сп			
Затв.		Кудерметов Р.К.							

Адміністрування(керування) мережею



					13.02070849.51126 ПЛ4			
					Модернізація комп'ютерної мережі Запорізького авіаційного фахового коледжу Адміністрування (керування) мережею	Літ.	Маса	Масштаб
Зм	Лист	№ докум.	Підп.	Дата				
Розроб.		Косяк А.К.						
Перевір.		Тягунова М.Ю.						
Т. контр.						Лист. 1		Листів 1
Н. контр.		Щербак Н.В.				НУ «Запорізька політехніка» КНТ-511сп		
Затв.		Кудерметов Р.К.						