

Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Антонова Андрія Сергійовича
(ПІБ)
академічної групи 123-20зск-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)
на тему «Комп'ютерна система ТОВ “Надір” з опрацюванням побудови, налаштування та безпеки корпоративної мережі»
(назва за наказом ректора)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Шедловська Я.І.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В.			

Рецензент				
-----------	--	--	--	--

Нормоконтролер	проф. Цвіркун Л.І.			
----------------	--------------------	--	--	--

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

«__» _____ 2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Антонова А.С. академічної групи 123-20зск-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему «Комп'ютерна система ТОВ “Надір” з опрацюванням побудови, налаштування та безпеки корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 11.04.2023 № 256-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	31.05.2023

Завдання видано _____
(підпис керівника)

доц. Шедловська Я.І.
(прізвище, ініціали)

Дата видачі 25.01.2023

Дата подання до екзаменаційної комісії 12.07.2023

Прийнято до виконання _____
(підпис студента)

Антонов А.С.
(прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 66 с., 33 рис., 8 табл., 1 дод., 9 джерел.

AAA, ACL, LACP, TFTP, TCP/IP, LAN, VLAN, NAT

Об'єкт: комп'ютерна система ТОВ “Надір” з опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета: створення корпоративної мережі транспортної компанії з повним налаштуванням та моделюванням компонентів мережі.

Кваліфікаційна робота містить комп'ютерне моделювання корпоративної мережі на основі віртуальних моделей та їхнього аналізу.

Мережа використовує сучасні мережеві протоколи, має логічну структуровану кабельну систему та відповідає всім стандартам мережі в сучасному світі.

В проєкті використовується діапазон IP-адресації локальних та глобальних мереж. В якості отримання доступу локальних мереж у глобальні мережі використовується протокол NAT.

Деякі мережі мають налаштування локальних підмереж за технологією VLAN. Також, віртуальні мережі використовують списки доступів ACL, для виконання вимог щодо доступності підрозділів.

В мережі забезпечується резервування, шляхом впровадження протоколу агрегування каналів – LACP.

Безпека мережевого обладнання побудована на функціоналі протоколу AAA, а саме – авторизація, аутентифікація та облік.

Кваліфікаційна робота містить повний перелік IP-адрес та представлений у вигляді таблиць.

Моделювання мережі було виконано у додатку Cisco Packet Tracer.

ЗМІСТ

Перелік скорочень, умовних познач, одиниць і термінів	7
Вступ	8
1 Стан питання і постановка завдання	10
1.1 Умови застосування мережі, що проектується	10
1.2 Характеристика та функціонування транспортної компанії ТОВ «Надір»	11
1.3 Складові частини архітектури транспортної компанії	11
1.4 Схема розподілу та локалізації компанії	13
1.5 Дослідження принципів використання ресурсів в мережі	14
1.6 Завдання і мета роботи	15
1.7 Визначення можливих напрямків рішення поставлених завдань	15
2 Розробка апаратної частини комп'ютерної системи	17
2.1 Технічні вимоги до системи	17
2.1.1 Вимоги до системи в цілому	17
2.1.1.1 Вимоги до структури і функціонування системи	17
2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації мережі	17
2.1.1.1.2 Вимоги до способів і засобів зв'язку для обміну інформації між підмережами	18
2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної мережі із суміжними мережами	18
2.1.1.1.4 Вимоги до режимів функціонування мережі	19
2.1.1.1.5 Вимоги до діагностування корпоративної мережі	19
2.1.1.1.6 Перспективи розвитку та модернізації мережі	19
2.1.1.2 Вимоги до показників призначення	20
2.1.1.3 Вимоги до експлуатації	20
2.1.1.3.1 Умови і регламент експлуатації, що повинні забезпечувати використання технічних засобів мережі	20
2.1.1.3.2 Вимоги до параметрів мереж енергопостачання	20

2.1.1.3.3	Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи	21
2.1.1.3.4	Вимоги до регламенту обслуговування мережі	22
2.1.1.4	Вимоги до патентної чистоти	22
2.1.1.5	Додаткові вимоги	22
2.1.1.5.1	Вимоги до активного обладнання	22
2.1.1.5.2	Вимоги до кабель каналів, інформаційним та електричним розеткам	23
2.1.1.5.3	Вимоги до комунікаційного обладнання і його розташування	23
2.1.1.5.4	Вимоги до однорідності	23
2.1.2	Вимоги до задач, які виконуються у комп'ютерній системи	24
2.1.2.1	Вимоги до кожної підмережі та переліку їх функцій	24
2.1.2.2	Вимоги до якості реалізації кожної функції	26
2.1.3	Вимоги до видів забезпечення комп'ютерної системи	27
2.1.3.1	Вимоги до математичного забезпечення	27
2.1.3.2	Вимоги до інформаційного забезпечення	27
2.1.3.3	Вимоги до лінгвістичного забезпечення	27
2.1.3.4	Вимоги до технічного забезпечення	28
2.1.3.5	Вимоги до організаційного забезпечення	28
2.1.3.6	Вимоги до методичного забезпечення	28
2.2	Розробка апаратної частини системи	29
2.2.1	Створення структурної схеми комплексу технічних засобів комп'ютерної мережі	29
2.2.2	Розробка технічних специфікацій комп'ютерного обладнання мережі	30
2.2.3	Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства	36
3	Розробка корпоративної мережі	39
3.1	Конфігурація маршрутних налаштувань комп'ютерної мережі в цифровому значені	39
3.2	Логічне визначення архітектури комп'ютерної мережі	44

3.3	Базова конфігурація параметрів мережевих пристроїв	46
3.4	Налаштування протоколів мережевого керування	47
3.4.1	Конфігурація OSPF-маршрутизації	47
3.4.1.1	Аналіз виконання	48
3.4.2	Конфігурація DHCP-діапазонів	49
3.4.2.1	Аналіз виконання	50
3.4.3	Конфігурація NAT-правил	51
3.4.3.1	Аналіз виконання	51
3.4.4	Конфігурація ACL-параметрів	52
3.4.4.1	Аналіз виконання	53
3.4.5	Конфігурація LACP-груп	53
3.4.5.1	Аналіз виконання	54
3.4.6	Конфігурація VLAN-інтерфейсів	55
3.4.6.1	Аналіз виконання	55
3.4.7	Конфігурація AAA-сервісів	57
3.4.7.1	Аналіз виконання	58
3.4.8	Конфігурація веб-сервера HTTP	59
3.4.8.1	Аналіз виконання	60
3.5	Комплекса оцінка налаштувань	60
4	Розробка компонента системи вентиляції	63
4.1	Розробка системи вентиляції в цілому	63
4.2	Налаштування системи вентиляції	63
4.3	Перевірка працездатності системи	66
	Висновки	67
	Перелік посилань	68
	Додаток А	69

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

DHCP – автоматизована система налаштування конфігурацій пристроїв;

OSPF – протокол маршрутів;

NAT – доступ до мережі Інтернет;

LACP – резервування підключення;

ACL – параметри доступу;

AAA – сервіси безпеки;

HTTP – сервер розгортання веб-сайту;

DNS – протокол співвідношення імені та адреси мережі;

TFTP – сервер збереження файлів;

CIT – додаток cisco packet tracer;

UPS – резервне джерело живлення.

ВСТУП

У наш час інформаційні технології мають великий прогрес порівняно навіть з 10 років тому назад. Корпоративні мережі мають використання сучасних протоколів стеку TCP/IP.

Транспортна компанія зосереджена на глибокому використанні локальної та глобальної мереж. Мета використання мережі для компанії – це мати взаємозв'язок зі всіма співробітниками компанії за короткий час та мати можливість швидкої передачі даних по мережі.

Кваліфікаційна робота має актуальний намір у наш час, для підвищення кваліфікації та підтвердження здобутих навичок в процесі навчання. Практична частина роботи дає змогу відобразити степінь необхідності інформаційних технологій кожній людині та кожній компанії.

Мережа будується та використовує технології локальних та глобальних мереж.

Локальна мережа – це сукупність кінцевих пристроїв в мережі, які мають фізичне підключення один між одним та розміщені на невеликій відстані між собою, наприклад, в межах будинку.

Глобальна мережа – це сукупність локальних мереж, які мають фізичне підключення між собою на великій відстані та застосовують технології інтернет-провайдерів. В залежності від відстані інтернет-провайдери можуть бути магістральні – між континентами та міські – в межах міста.

Корпоративна мережа транспортної компанії використовує технології локальної мережі, для побудови та організації внутрішньої системи зв'язку, та глобальні мережі, для об'єднання своїх підрозділів у єдиний сегмент мережевої інфраструктури.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Умови застосування мережі, що проектується

В якості корпоративної мережі була використана транспортна компанія.

Мережа транспортної компанії призначена для обслуговування та створення задач на перевезення вантажів різної ваги, а також для моніторингу стану перевезення.

Дана мережа дозволяє виконувати ефективну комунікацію між різними відділами транспортної компанії, включаючи взаємодію між логістичним відділом, відділом перевезень, відділом постачання та інформаційним відділом. Вона допомагає швидко обмінюватись інформацією, координувати дії та вирішувати проблеми.

Мережа транспортної компанії забезпечує керування рухом транспортних засобів, відстеження місцезнаходження автомобілів та моніторинг виконання графіків руху. Це дозволяє оптимізувати маршрутизацію, скоротити час доставки та забезпечити ефективне використання ресурсів.

Також, дозволяє інтегрувати різні інформаційні системи, такі як системи управління складом, системи відстеження вантажів, системи обліку та фінансового управління. Це дозволяє компанії миттєво отримувати актуальну інформацію про стан руху вантажів, запаси на складі та фінансову продуктивність.

Вона має важливу роль у забезпеченні безпеки даних та інформації. Застосування захисних механізмів, шифрування даних та контролю доступу допомагає уникнути несанкціонованого доступу до важливої інформації та зберегти конфіденційність даних клієнтів.

Тобто, мережа транспортної компанії – це комплексна система, що включає в себе різні фізичні та інформаційні елементи для забезпечення оптимального функціонування компанії та надання транспортних послуг.

1.2 Характеристика та функціонування транспортної компанії ТОВ «Надір»

ТОВ «Надір» – це транспортна компанія, яка займається доставкою будь-яких матеріалів за допомогою вантажних автомобілів.



Рисунок 1.1 – Вигляд офісу ТОВ «Надір»

Транспортна компанія може здійснювати перевезення вантажів різного типу та обсягу за допомогою автоперевезень. Компанія пропонує послуги доставки вантажів, транспортування контейнерів, спеціалізовані послуги для певних галузей, таких як хімічна промисловість або міжміські перевезення.

1.3 Складові частини архітектури транспортної компанії

Архітектура транспортної компанії складається з різних компонентів, які спільно працюють для забезпечення ефективного та надійного функціонування компанії.

Відповідно до системи управління компанії була створена схема лінійної організації керівництва та мереж.

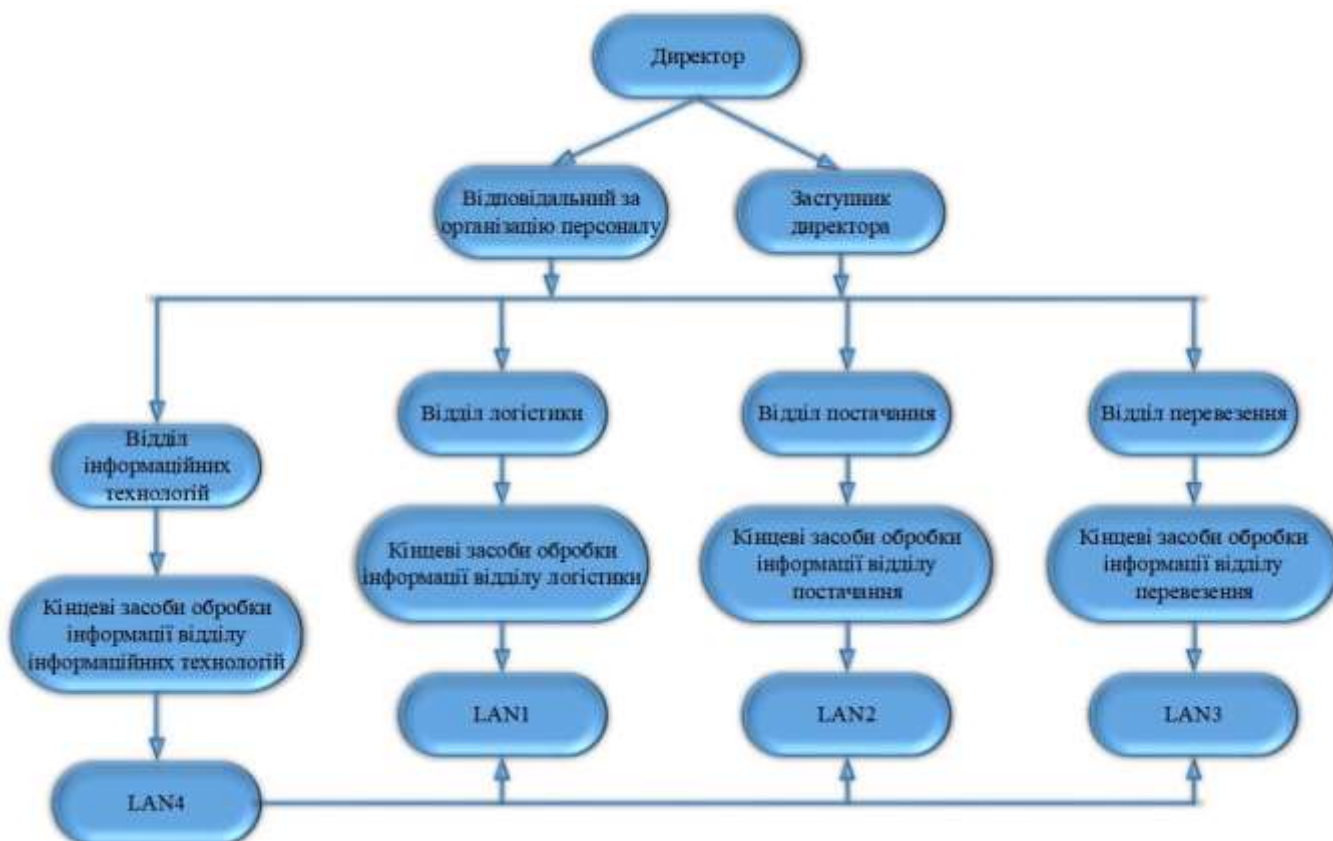


Рисунок 1.2 – Схема лінійної організації керівництва та мереж

Транспортною компанією керує директор, заступник директора та відповідальний за організацію персоналу.

Відділ логістики відповідає за планування та організацію перевезень вантажів, вибір оптимальних маршрутів, управління запасами та облік вантажів.

Відділ перевезень відповідає за здійснення транспортування вантажів, координацію роботи водіїв і транспортних засобів, контроль за виконанням графіків і дотриманням правил безпеки.

Відділ постачання відповідає за закупівлю та облік матеріалів, запасних частин і палива для транспортних засобів, контроль за їхньою якістю і термінами постачання.

Відділ інформаційних технологій відповідає за розробку та підтримку інформаційних систем і програмного забезпечення, забезпечення безпеки даних, підтримку комп'ютерного та мережевого обладнання.

1.4 Схема розподілу та локалізації компанії

Схема розподілу та локалізації підрозділів – це візуальне відображення розташування підрозділів компанії, з яких буде побудована та налаштована корпоративна мережа.

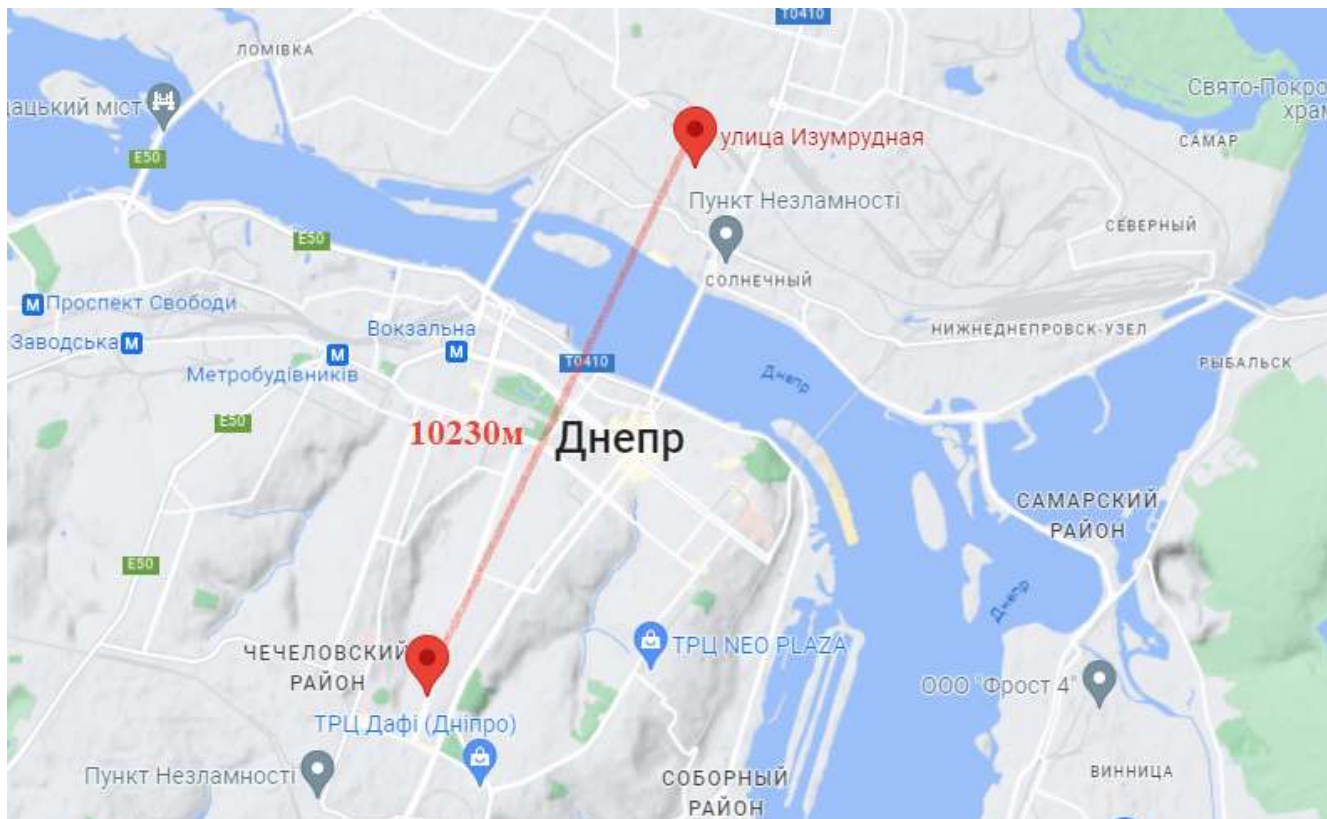


Рисунок 1.3 – Схема розподілу та локалізації компанії

Схема вміщує в собі дві точки які містять 3 будівлі, які знаходяться в Україні, м. Дніпро та мають розташування на різних берегах міста.

Відстань між ними складає – 10 230м, що в розумінні локальних мереж є великою відстанню для самостійного прокладання структурованих кабельних систем.

Тому для об'єднання локальних мереж в єдину корпоративну мережу будемо використовувати спроможності міських інтернет-провайдерів суміжно з налаштуваннями для локальних мереж. При такому застосуванні, відстань між відділам для побудови мережі можна не враховувати.

1.5 Дослідження принципів використання ресурсів в мережі

Архітектура мережі будується на наступних принципах:

- розподілених систем. Цей принцип передбачає, що мережа повинна складатися з розподілених компонентів, що співпрацюють між собою для досягнення спільної мети. Це дозволяє забезпечити високу доступність, масштабованість та надійність системи.
- шаровості. Цей принцип рекомендує розбити мережу на логічні шари або рівні, кожен з яких виконує певні функції. Кожен шар має власну відповідальність і взаємодіє зі шарами вищого і нижчого рівнів. Це сприяє модульності, стандартизації та спрощенню розробки і підтримки мережі.
- скорочення шляхів. Цей принцип використовується в алгоритмах маршрутизації для знаходження найкоротшого шляху між джерелом і призначенням. Використання оптимальних шляхів дозволяє знизити затримки, мінімізувати втрати пакетів і забезпечити ефективне використання ресурсів мережі.
- масштабованості. Цей принцип вказує на необхідність побудови мережі, яка здатна легко розширюватися для врахування зростання обсягу трафіку та кількості вузлів. Застосування масштабованих архітектур та протоколів дозволяє забезпечити продуктивність мережі навіть при збільшенні обсягу даних.
- безпеки. Цей принцип ставить на перший план захист мережі від несанкціонованого доступу, зловживання та збоїв. Використання шифрування, аутентифікації, контролю доступу та інших захисних механізмів допомагає забезпечити конфіденційність, цілісність та доступність даних.
- гнучкості. Цей принцип вказує на необхідність побудови мережі, яка може адаптуватися до змінних потреб користувачів і технологічних вимог. Гнучка мережа здатна швидко реагувати на зміни та впроваджувати нові сервіси та функціональні можливості.

1.6 Завдання і мета роботи

Завдання полягає у проектуванні архітектури мережі, виборі необхідного обладнання, налаштуванні мережевих протоколів та забезпеченням безпеки мережі.

Мета роботи визначає загальний результат, який має бути досягнутий після завершення проекту.

Для продовження проектування мережі, необхідно визначити питання:

- потреб організації;
- з вибору необхідного обладнання;
- з конкретного налаштування обладнання;
- з створення інструкцій налаштування.

Поставлені питання повинні бути вирішені відповідно до загальної топології мережі транспортної компанії.

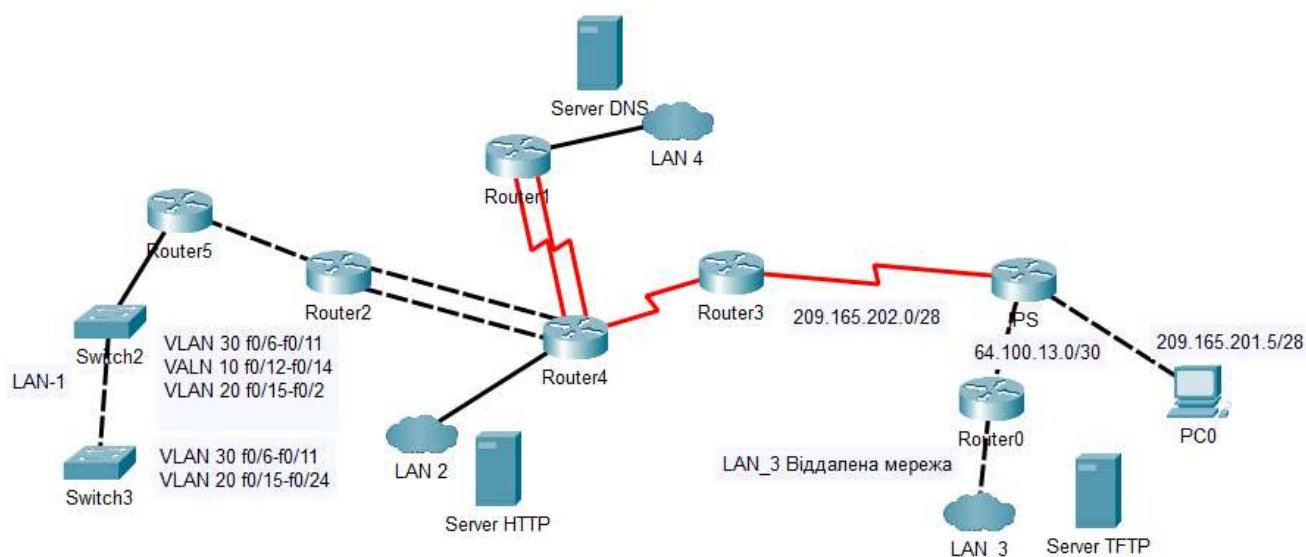


Рисунок 1.4 – Загальна топологія мережі транспортної системи

1.7 Визначення можливих напрямків рішення поставлених завдань

Вирішити поставлені питання можна за допомогою певного алгоритму налаштувань кожного компонента мережі.

В алгоритмі налаштувань необхідно:

- створити структурну схему комплексу технічних засобів;

- розробити технічні специфікації;
- провести розрахунок з пропускної здатності мережі;
- провести конфігурацію маршрутних налаштувань;
- провести логічне визначення архітектури мережі;
- провести базову конфігурацію налаштувань;
- провести конфігурацію OSPF-маршрутизації;
- провести конфігурацію DHCP-діапазонів;
- провести конфігурацію NAT-правил;
- провести конфігурацію ACL-параметрів;
- провести конфігурацію LACP-груп;
- провести конфігурацію VLAN-інтерфейсів;
- провести конфігурацію AAA-сервісів;
- провести конфігурацію веб-сервера HTTP;
- виконати комплексну оцінку налаштувань;
- розробити компонент системи вентиляції.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до системи

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонування системи

2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації мережі

Головною ціллю компанії від мережі є максимальне використання мережевих технологій для забезпечення матеріального капіталу та прискорення швидкості роботи персоналу.

Система мережі транспортної компанії ТОВ «Надір» повинна вміщувати в себе:

- сервер DNS;
- сервер RADIUS;
- сервер HTTP;
- сервер TFTP;
- комп'ютери;
- принтери;
- комутатори;
- маршрутизатори;
- фізичні лінії передач.

Компанія складається з трьох будівель, які розташовані на великій відстані одна від одної, при цьому, мережа повинна мати:

- єдину адресацію для всієї мережі;
- єдиний доступ до ресурсів;
- розподіл адресації для кожної будівлі;
- однакові протоколи доступу.

Схема розподілу та локалізації компанії свідчить про те, що ієрархічні рівні компанії повинні складатися в чотирьох незалежних мереж, однак знаходитися при цьому у складі корпоративної мережі.

Ієрархічні рівні компанії повинні складатися з:

1. рівню логістики;
2. рівню перевезень;
3. рівню постачання;
4. рівню інформаційних технологій.

Задані рівні ієрархії повинні застосовувати корпоративну мережу та забезпечувати безперебійну роботу інфраструктури.

2.1.1.1.2 Вимоги до способів і засобів зв'язку для обміну інформації між підмережами

Засобами передачі інформації є:

1. Маршрутизатори, за якими відбувається передача даних між підмережами та визначається оптимальний шлях доставки пакетів даних від однієї підмережі до іншої;
2. Балансувальник навантаження який дозволяє розподіляти трафік між різними шляхами або каналами зв'язку для покращення продуктивності та доступності мережі.

2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної мережі із суміжними мережами

Для взаємодії з іншими мережами транспортна компанія повинна мати власну IP-адресацію. Це дозволить ідентифікувати та з'єднуватися з іншими мережами за допомогою протоколу IP.

Транспортна компанія повинна приділяти увагу заходам безпеки для взаємодії з іншими мережами з використанням шифрування даних, щоб забезпечити конфіденційність та цілісність інформації, яку обмінюють та використовують мережі.

2.1.1.1.4 Вимоги до режимів функціонування мережі

Вимоги включають поняття щодо спеціалізації кожної частини мережі та відповідальністю.

Відділ логістики повинен відповідати за планування та організацію перевезень вантажів, обирати оптимальні маршрути, управління запасами та облік вантажів.

Відділ перевезень повинен відповідати за здійснення транспортування вантажів, координацію роботи водіїв і транспортних засобів, контролем виконання графіків і дотриманням правил безпеки.

Відділ постачання повинен відповідати за закупівлю та облік матеріалів, запасних частин і палива для транспортних засобів, контролювати за їхньою якістю і термінами постачання.

Відділ інформаційних технологій повинен відповідати за розробку та підтримку інформаційних систем і програмного забезпечення, забезпечення безпеки даних, підтримку комп'ютерного та мережевого обладнання.

2.1.1.1.5 Вимоги до діагностування корпоративної мережі

Діагностика мережі повинна використовувати інструменти аналізу мережевого трафіку для виявлення аномалій:

- велика кількість пакетних втрат;
- висока затримка;
- недостатній пропускний потік.

Це повинно допомогти виявити проблеми зі шляхом маршрутизації, неправильним налаштуванням апаратного забезпечення або атаками на мережу.

2.1.1.1.6 Перспективи розвитку та модернізації мережі

Компанія планує розширити свою діяльність на нові регіони. Це вимагає розгалуженої мережі, яка забезпечить зв'язок між головним офісом та відділеннями в різних містах.

У зв'язку зі зростанням обсягів даних, таких як великі обсяги транспортних відомостей, вантажних документів тощо, потрібно покращити пропускну здатність мережі.

У зв'язку зі зростанням мобільних пристроїв та потреби у доступі до мережі в будь-якому місці, транспортна компанія повинна розглядати розгортання технологій безпроводового зв'язку, таких як Wi-Fi або мережі 4G/5G, для забезпечення бездротового підключення працівників та клієнтів.

2.1.1.2 Вимоги до показників призначення

Транспортна компанія потребує зв'язку з партнерами та клієнтами по всьому світу. Мережа повинна підтримувати міжнародний зв'язок та мовну різноманітність, забезпечуючи ефективну комунікацію та обмін інформацією.

З урахуванням рухомості персоналу та водіїв, транспортна компанія може потребувати мобільних засобів зв'язку, які дозволяють отримувати доступ до мережі та даних з будь-якого місця. Кожен співробітник повинен бути забезпечений планшетом та мати налаштування щодо доступу до корпоративної мережі.

2.1.1.3 Вимоги до експлуатації

2.1.1.3.1 Умови і регламент експлуатації, що повинні забезпечувати використання технічних засобів мережі

Мережа транспортної компанії є критично важливим елементом її інфраструктури, оскільки забезпечує безперебійний обмін інформацією та операційну діяльність протягом усього дня і ночі. Вимога до мережі працювати за графіком – 24/7, без зупинки компонентів мережі.

2.1.1.3.2 Вимоги до параметрів мереж енергопостачання

Відділи транспортної компанії повинні мати резервні джерела живлення, такі як UPS.

UPS забезпечує безперебійне живлення обладнання протягом короткочасних перебоїв у мережі, та не спроможний вести роботу протягом довгого часу, але дозволить зберегти дані клієнтів та належним чином завершити роботу операційних систем.

Потужність UPS повинна бути достатньою, щоб забезпечити живлення всіх критичних компонентів мережі. Середнє значення сумарної споживаної потужності комп'ютерів, маршрутизаторів та комутаторів становить 10 кВт, тоді UPS повинен мати потужність, яка перевищує це значення, наприклад, 12 кВт, для додаткового запасу.

UPS має бути постійно підключений до джерела електромережі. Це забезпечить безперебійне живлення мережевого обладнання протягом тривалого періоду, якщо основне енергопостачання відмовить.

2.1.1.3.3 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи

Згідно з пунктом 2.1.1.3.1 про підтримку цілодобової працездатності компонентів мережі, персонал повинен працювати за цілодобовим графіком, лише керуючу змінами людей.

Для користування мережею транспортної компанії та користування послугами комп'ютера не потрібна особлива освіта.

Для використання комп'ютера і мережі транспортної компанії необхідно володіти базовими навичками роботи з комп'ютером, таких як – уміння запускати програми, вводити текст, переглядати веб-сторінки та надсилати електронні листи іншим компаніям та бути зацікавленим і готовим вивчати основні навички роботи з комп'ютером.

Користувачі можуть навчатися роботи з комп'ютером самостійно, шляхом вивчення посібників або спілкування з іншими користувачами для обміну досвідом та отримання допомоги.

2.1.1.3.4 Вимоги до регламенту обслуговування мережі

Кожного місяця повинна проводитися перевірка стану комутаторів, маршрутизаторів та комп'ютерів. Перевірка повинна виконуватися на наявність фізичних пошкоджень, правильність підключення кабелів, стан вентиляторів та живлення. Також перевіряється наявність оновленого програмного забезпечення та вирішуються поточні проблеми.

Кожну ніч повнино автоматично виконуватися резервне копіювання конфігурацій комутаторів і маршрутизаторів на центральний сервер.

Кожні шість місяців виконується заміна вентиляторів у комутаторах, а раз на рік проводиться оновлення прошивки всього мережевого обладнання.

2.1.1.4 Вимоги до патентної чистоти

Транспортна компанія планує впровадити автоматизовану систему моніторингу та керування вантажними перевезеннями.

Ця система включає в себе розроблене програмне забезпечення, спеціалізовані сенсори та пристрої збору даних.

Транспортна компанія повинна переконатись, що розроблене програмне забезпечення не порушує патенти або авторські права інших компаній.

Якщо в системі використовуються сторонні технології, транспортна компанія повинна мати ліцензійні угоди з власниками патентів або технологій.

2.1.1.5 Додаткові вимоги

2.1.1.5.1 Вимоги до активного обладнання

Кожний маршрутизатор повинен бути оснащений двома інтерфейсними картами HWIC-2T.

HWIC-2T – тип модуля розширення, який використовується для додавання додаткових портів серійної лінії до мережевого обладнання.

Для налаштування корпоративної мережі необхідно використовувати наступні типи кабелів:

- ethernet straight-through;

- ethernet crossover;
- console;
- serial;
- fiber optic.

2.1.1.5.2 Вимоги до кабель каналів, інформаційним та електричним розеткам

Для моделювання фізичної архітектури мережі інформаційні та електричні розетки не потрібні, всі підключення будуть реалізовані безпосередньо від комутатора до комп'ютерів співробітників.

Кабель-канали повинні бути екрановані для забезпечення захисту від електромагнітного впливу та перешкод та використовувати кабелі типу STP (Shielded Twisted Pair).

2.1.1.5.3 Вимоги до комунікаційного обладнання і його розташування

Прилади повинні розташовуватися на зручному місці для компанії, при цьому не використовуючи додаткових місць розташування. Мережеве обладнання не має єдиної системи групування, що не потребує використання шаф або інших компонентів. Кожен пристрій знаходиться приміщенні в залежності від розподілу підмереж.

2.1.1.5.4 Вимоги до однорідності

Транспортна компанія повинна мати один об'єднаний корпоративний бренд, який відображається у її логотипі, графічних елементах, кольорах та комунікаційних матеріалах.

Вимагається застосування корпоративного брендингу на всіх рівнях компанії, включаючи транспортні засоби, приміщення, рекламні матеріали та інші елементи.

2.1.2 Вимоги до задач, які виконуються у комп'ютерній системі

2.1.2.1 Вимоги до кожної підмережі та переліку їх функцій

Робота мережевого обладнання починається з моменту виконання базової конфігурації параметрів:

- мережеві пристрої повинні мати ідентифікатори в мережі та використовувати шаблон їх застосування: *студента_тип-пристрою_номер пристрою*;

- всі засоби мережі повинні мати пароль *cisco* для отримання доступу консольного рядка та ліній *vtu*;

- всі засоби мережі повинні мати пароль *class* до привілейованого режиму;

- всі засоби мережі повинні бути налаштовані на підтримку шифрування паролів;

- засоби мережі повинні мати банери MOTD під час проходження ідентифікації;

- всі засоби мережі повинні мати доступ до ліній *vtu* з використанням протоколу *ssh*;

- всі засоби мережі повинні мати записи користувачів відповідно до шаблону: *група_прізвище* та пароль *admincisco*;

- всі засоби мережі повинні мати відповідність персонального ідентифікатора з доменом;

- дані повинні шифруватися ключем *RSA* з запитом довжини шифрування 1024 біт;

- засоби, в яких інстальовані DCE-інтерфейси повинні мати тактову частоту – 128000;

- засоби мережі повинні мати налаштування повідомлень про роботу процесу *exec*;

Мереже обладнання потребує налаштування маршрутизації мережі:

- необхідно вимкнути поширення маршрутизаційних оновлень в локальній мережі з підключеними безпосередньо мережами в глобальній мережі;

- віртуальні мережі повинні мати єдиний діапазон адрес та маршрут, за яким буде оголошено іншим мережам;
- налаштування OSPF повинно відповідати параметрам пропускної спроможності для розрахунку вартості дозволів гігабітних мережевих інтерфейсів з значенням – 1000;
- serial інтерфейси повинні відповідати пропускній здатності 128 Кб/с та вартості метрики 7500;
- засоби мережі які мають безпосередньо прямі підключення до інтернет-провайдерів повинні оголошувати маршрути до нього за протоколами маршрутизації;
- на даному маршруті потрібно налаштувати ручне підсумовування маршрутів та включити до таблиці приєднання мережі, так як технології маршрутизації підсумовують тільки підмережі загальної корпоративної мережі або організації;
- потрібно додати статичні маршрути, щоб вузли мали доступ за їх допомогою.

Налаштування маршрутизаторів з використанням AAA-сервісів потрібно виконати за вимогами:

- засобами перевірки підключення до ліній VTU слід використовувати локальну базу співробітників;
- ідентифікацію даних співробітників до консолі слід застосовувати на основі RADIUS-серверу, при не отриманні відповіді від нього, можна застосовувати локальну базу;
- RADIUS-сервер повинен мати секретне слово для надання доступу маршрутизаторам – radius123;
- для входу в систему потрібно використовувати ідентифікатори пристроїв та пароль *admin123*.

Відповідний маршрутизатор за постачання інтернету в локальну мережу, має використовувати одне підключення до інтернет-провайдера.

Компоненти мережі або технічні засоби повинні отримувати доступ до мережі Інтернет з використанням протоколу NAT.

Діапазон глобальних адрес повинен бути 209.165.200.5 по 209.165.200.30 з ідентифікатором – AntonovNAT. Для номеру списків доступу необхідно використовувати номер варіанту – 1.

Розробка повинна містити опис налаштувань створеного веб-сайту HTTP, а саме відповідність між <http://123.dnipro.ua> та <http://192.168.5.130> та містити інформацію створення та розробки кваліфікаційної роботи студента, який планує її захищати.

2.1.2.2 Вимоги до якості реалізації кожної функції

Конфігурація маршрутних налаштувань комп'ютерної мережі в цифровому значенні повинна відповідати вимогам:

- діапазони адрес використовувати виключно версії IPv4;
- підключення між маршрутизаторами повинно адресуватися діапазоном адрес 10.0.№.0/24, де № – варіант студента;
- необхідно заздалегідь розрахувати кількість адрес, для того щоб вмістити всіх користувачів в єдину мережу;
- із пулів адрес, перші адреси надавати мережевим інтерфейсам маршрутизаторів;
- із пулів адрес, другі адреси надавати мережевим інтерфейсам комутаторів;
- із пулів адрес, треті адреси надавати мережевим інтерфейсам серверів;
- із пулів адрес, останні адреси надавати мережевим інтерфейсам принтерам та ПК користувачів;
- ПК, принтери та сервери повинні отримувати адресацію з використанням DHCP-діапазонів.

2.1.3 Вимоги до видів забезпечення комп'ютерної системи

2.1.3.1 Вимоги до математичного забезпечення

Для успішного проєктування та створення мережі важливо врахувати вимоги до пропускнуєї спроможності, особливо для найбільшої мережі, яка буде включена в інфраструктуру. Розрахунок пропускнуєї здатності необхідний для визначення можливостей мережі та забезпечення її ефективної роботи.

Найбільша мережа має 45 вузлів, які надсилають інформацію з показником середнього значення інтенсивності трафіку у 157 (кадрів/с).

Необхідно розрахувати пропускну здатність каналів, та урахувати те, що середнє значення даних 650 байт. Також, необхідно виконати вимогу щодо затримки передачі даних до 6 мс.

2.1.3.2 Вимоги до інформаційного забезпечення

Компанія повинна мати систему, яка дозволяє ефективно планувати маршрути транспортних засобів, управляти запасами палива, відстежувати показники споживання палива та здійснювати підтримку водіїв.

Відносно цієї загальної вимоги, отримуємо конкретні вимоги щодо програмного забезпечення:

- transport management systems;
- logistics management systems;
- freight management systems.

2.1.3.3 Вимоги до лінгвістичного забезпечення

Відповідно до вимог у пункті 2.1.1.2 мережа повинна відповідати міжнародному зв'язку та мовній різноманітності.

В компанії повинні бути люди, які будуть знати англійську мову на розмовному рівні.

2.1.3.4 Вимоги до технічного забезпечення

UPS повинен мати достатню потужність для живлення всіх пристроїв, які підключені до мережі, та підтримувати:

- потужність: 1500 вольт-ампер (VA) / 865 ват (W);
- вхідна напруга: 230 вольт змінного струму (V);
- вихідна напруга: 230 вольт змінного струму (V);
- автоматичне регулювання напруги та фільтрації шуму для захисту від

стрибків напруги та перешкод.

2.1.3.5 Вимоги до організаційного забезпечення

Організаційне забезпечення транспортної компанії повинно охоплювати різні аспекти, які допомагають ефективно управляти і контролювати операції компанії.

Воно вміщує в собі використання:

- gps-трекери: повинні бути встановлені на транспортних засобах, для надання змоги відстежувати та контролювати їхнє місце розташування і пересування в реальному часі;
- системи глобального позиціонування (GPS): повинні визначати місце розташування транспортних засобів і оптимізувати маршрути доставки;
- управління транспортними флотами (Fleet Management Systems): для відстежування стану транспортних засобів, контролю витрату палива та планування обслуговування.

2.1.3.6 Вимоги до методичного забезпечення

До методичного забезпечення входить список документів і матеріалів, які допомагають організувати та структурувати роботу в певній підмережі та в певний час. Вони складаються з:

- конфігурацій протоколів мережевого керування;
- логічної частини архітектури комп'ютерної мережі;
- розробки компонента системи вентиляції.

2.2 Розробка апаратної частини системи

2.2.1 Створення структурної схеми комплексу технічних засобів комп'ютерної мережі

Схема представлення взаємозв'язків і взаємодії компонентів у системі являє собою графічне зображення взаємозв'язку та взаємодії різних компонентів і пристроїв у системі. Вона відображає архітектуру і функціональну організацію комплексу, а також дає змогу легко зрозуміти його структуру і взаємозв'язки між елементами.

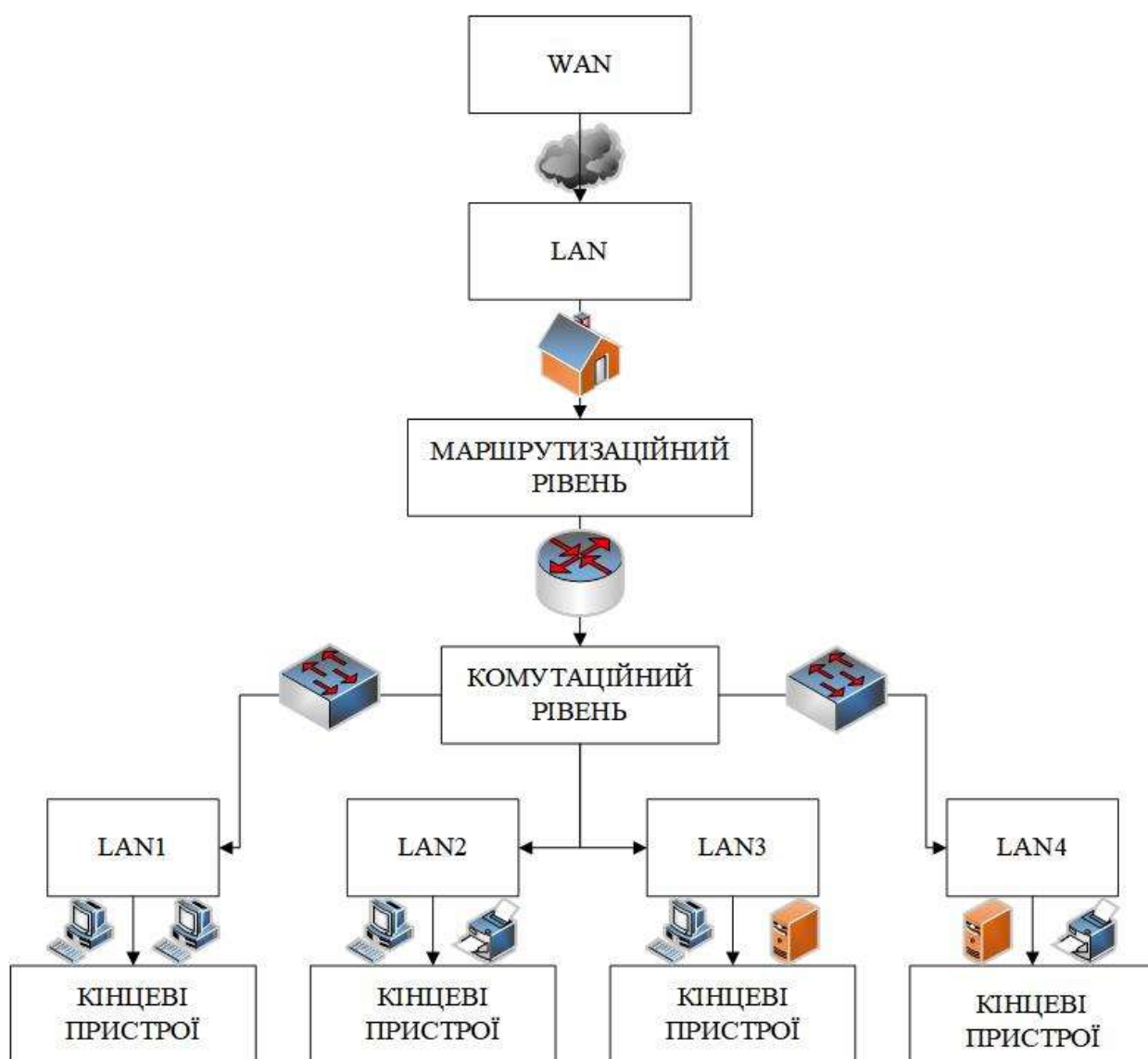


Рисунок 2.1 – Схема представлення взаємозв'язків і взаємодії компонентів у системі

Кожен компонент на схемі представлений у вигляді блоку з відповідними позначеннями та символами. У середині блоків можуть бути вказані додаткові деталі або функції пристроїв. Лінії та стрілки, що з'єднують блоки, показують напрямок потоку інформації або сигналів між компонентами.

Корпоративна мережа має пряме підключення до Інтернет-провайдера за допомогою магістрального маршрутизатора. Він використовує технологію підключення point-to-point.

Point-to-point – це топологія, яка відноситься до мережевої конфігурації, в якій існує пряме з'єднання між двома вузлами (точками) без участі інших вузлів або комутаційних пристроїв. Це означає, що кожен вузол має окреме і пряме з'єднання з іншим вузлом у мережі.

Всі інші вузли підключені за принципом дерева, яке має багато гілок та ділить мережу на підмережі.

Відповідно до схеми представлення взаємозв'язків і взаємодії компонентів у системі була створена таблиця співвідношення мережі та пристроїв.

Таблиця 2.1 – Співвідношення мережі та пристроїв

Назва мережі	Номер мережі	Ідентифікація у додатку	Тип пристрою
Відділ логістики	LAN1	PC18-23	PC
Відділ постачання	LAN2	PC9-14	PC
		Printer0	Printer
		Server HTTP	Server
Відділ перевезень	LAN3	PC_0-8	PC
		Server TFTP	Server
Відділ інформаційних технологій	LAN4	PC15-17	PC
		Printer1	Printer
		Server DNS	Server

2.2.2 Розробка технічних специфікацій комп'ютерного обладнання мережі

При розробці технічних специфікацій комп'ютерного обладнання мережі, приступається до детального аналізу вимог та потреб користувачів. Це включає

визначення функціональних вимог, які мають бути задоволені, таких як швидкість передачі даних, пропускна здатність, надійність, масштабованість та безпека.

Опираючись на ці вимоги, проектується архітектура мережі, включаючи типи комп'ютерів, серверів, комутаторів, маршрутизаторів та інших мережевих пристроїв, які будуть використовуватися.

Для початку, розробимо апаратну конфігурацію мережевого обладнання.

Таблиця 2.2 – Специфікація мережевого обладнання транспортної компанії

Позиція	Назва виробу та технічна характеристика	Тип, марка, позначення	Вимір	Кількість	Підтримка протоколів
1	Комутатор Технології:Fast Ethernet (10/100 Mbps) Gigabit Ethernet (10/100/1000 Mbps) 24 порти Фунції Layer 2 та Layer 3	Cisco Catalyst 2960X	од.	7	IEEE 802.1D STP IEEE 802.1w RSTP IEEE 802.1s MSTP IEEE 802.1Q VLAN IEEE 802.1p CoS IEEE 802.1X IEEE 802.1ab LLDP IEEE 802.3ad LACP Fast Ethernet 802.3u Gigabit Etherne802.3ab
2	Маршрутизатор Процесор 2ядра 1,0 ГГц, 4 ГБ озп Підримка Network Interface Module, Service Module Порти 2x Gigabit Ethernet	Cisco ISR 4321	од.	7	IPv4, IPv6, ICMP, ARP, OSPF, VRRP, DHCP, NAT, ACL, SSH, SSL/TLS, IPsec, MPLS, DNS

Далі, розробимо апаратне забезпечення для кожного співробітника мережі. Кожен компонент, починаючи від процесора і пам'яті, закінчуючи мережевими картами і сховищем даних, ретельно обирається і описується.

Таблиця 2.3 – Специфікація технічних засобів співробітників

Позиція	Назва виробу та технічна характеристика	Тип, марка, позначення	Вимір	Кількість	Примітка
1	Блок – Everest процесор – AMD Athlon II X2 340 (3.2 ГГц) ОЗП – 4 ГБ відеоадаптер – AMD Radeon R7 250, 2 ГБ; SSD 480 ГБ.	Everest s-FM1 AMD	од.	24	Моделювання в програмному забезпечення Cisco Packet Tracer – PC_0-23
2	Монітор Dell діагональ 20.1 частота 60 Гц максимальна роздільна здатність дисплея 1600x1200 інтерфейси DVI/VGA	Dell 2007FPb S-IPS PIVOT	од.	24	Моделювання в програмному забезпечення Cisco Packet Tracer – PC_0-23
3	Принтер Canon	Canon Pixma MG3640S	од.	2	Моделювання в програмному забезпечення Cisco Packet Tracer – Printer0-1

Таблиця 2.3 – це документ, який описує кожен комп'ютер у мережі з усіма його технічними характеристиками, інтерфейсами, протоколами та конфігурацією. Цей документ стає основою для замовлення та налаштування комп'ютерів у мережі.

Для забезпечення надійного резервного джерела живлення виберемо джерело живлення UPS.



Рисунок 2.2 – Резервне джерело живлення UPS

UPS – це електронний пристрій, який призначений для захисту комп'ютерної системи від збоїв в електропостачанні та забезпечення безперервної роботи в разі вимкнення основного джерела живлення.

Занесемо технічні характеристики UPS до таблиці.

Таблиця 2.4 – Специфікація джерела живлення UPS

Позиція	Назва виробу та технічна характеристика	Тип, марка, позначення	Вимір	Кількість	Примітка
1	UPS потужність: 1500 (VA) / 865 (W); вхідна: 230 (В); вихідна: 230 (В); Розміри: 112 мм x 301 мм x 382 мм Вага: 11,8 кг	APC Back-UPS Pro 1500VA	од.	4	Автоматичне регулювання напруги (AVR): Підтримує стабільну напругу живлення в межах безпечних значень.

Розробимо схеми підключення обладнання.

На цих схемах відображаються розташування серверів, комутаторів, маршрутизаторів, сховищ даних і комп'ютерів.

На схемі також показані підключення кабельних систем, а саме маршрути і типи кабелів, що використовуються для з'єднання між обладнанням.

У кінцевому підсумку, схеми розміщення обладнання та підключення кабельними системами є ключовим фактором для фізичної реалізації мережі.

На точках виходу до маршрутизації передбачається оптичний канал, який служить важливою сполучною ниткою між нашою мережею і провайдером послуг. Цей канал забезпечує високошвидкісну передачу даних і надійне з'єднання із зовнішньою мережею.

Це важливий елемент вашої інфраструктури, який забезпечує якісний зв'язок із провайдером послуг і гарантує ефективне передавання даних між вашою мережею та зовнішніми ресурсами.

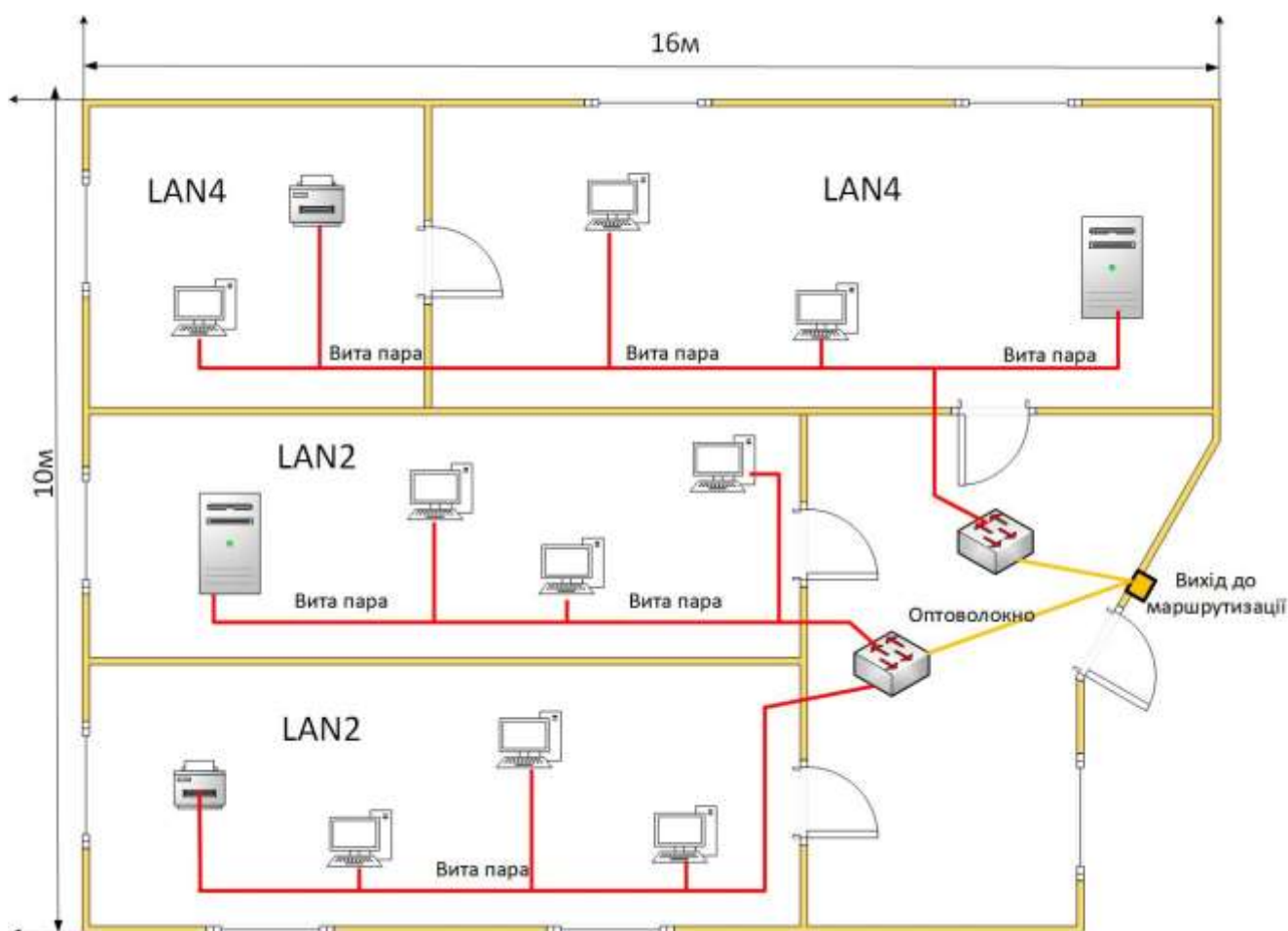


Рисунок 2.3 – Деревоподібне підключення мережі першої будівлі

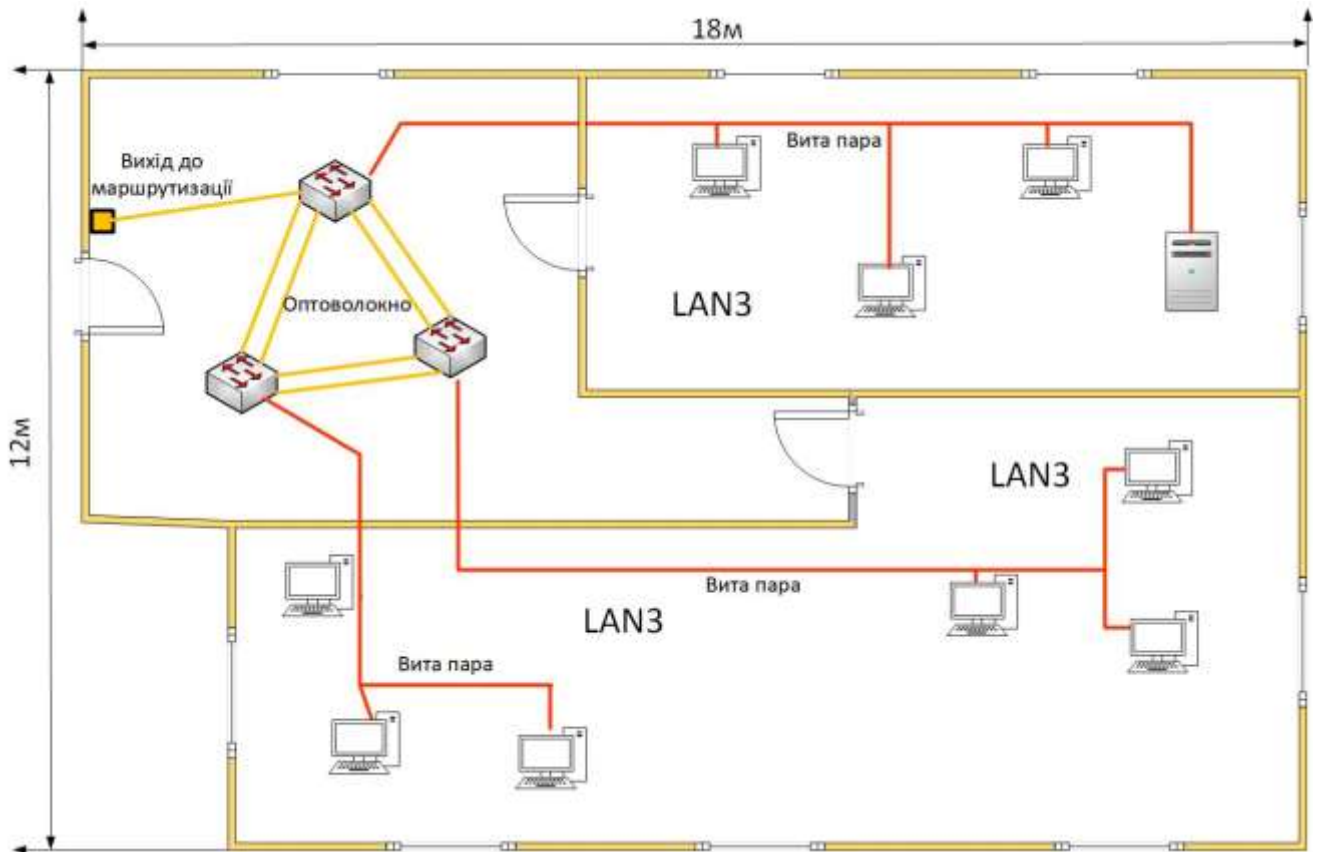


Рисунок 2.4 – Деревоподібне підключення мережі другої будівлі

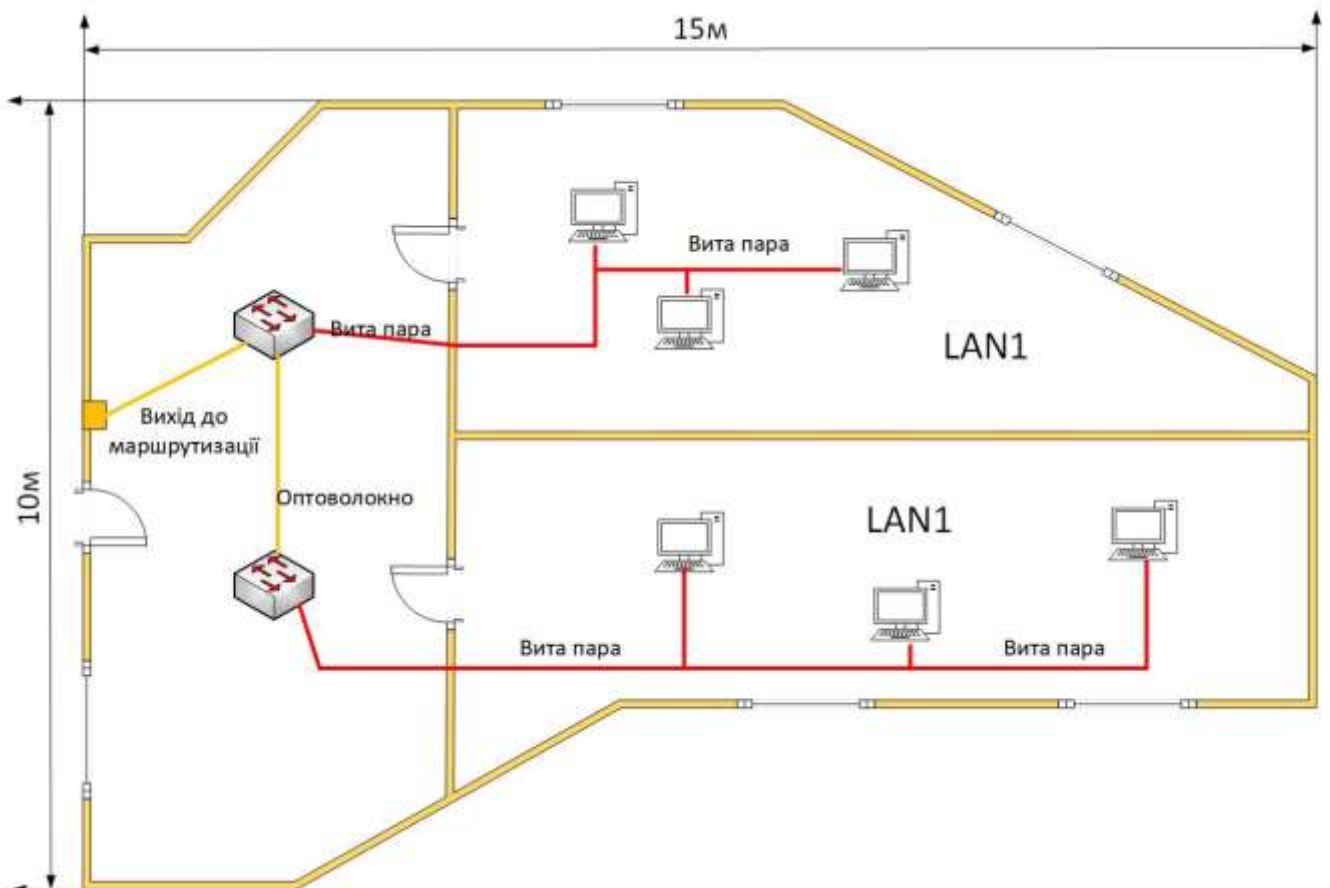


Рисунок 2.5 – Деревоподібне підключення мережі третьої будівлі

Забезпечення транспортної компанії зі сторони програм, було вирішено відповідно до вимог.

Transport management systems – це програмне рішення, яке допомагає управляти транспортними операціями, включаючи планування маршрутів, назначення водіїв і транспортних засобів, відстеження вантажів, контроль запасів, фінансовий облік і звітність.

Logistics management systems – це програма, яка допомагає планувати, виконувати та контролювати логістичні операції, включаючи складський облік, управління запасами, оптимізацію маршрутів, обробку замовлень та відстеження вантажів.

Freight management systems – це програма, яка спеціалізується на управлінні вантажоперевезеннями, включаючи вибір перевізника, тарифи, розрахунок вартості доставки, документообіг і відстеження вантажів.

2.2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

За пунктом 2.1.3.1 вимогам до математичного забезпечення проведемо розрахунок пропускної здатності мережі за заданими значеннями.

Для розрахунку, навантажуюмо мережу на 100% функціоналу та використання.

Максимальне допустиме значення пропускної здатності каналів сягає в межах 1000Мбіт/с.

Після того, як мережею почали користуватися всі співробітники, розрахунок можна розпочинати.

Пропускна здатність мережі комутаторів:

$$P_{p.d} = \mu * 1 * n * 8 = 157 * 650 * 24 * 8 = 19,59 \text{ Мбіт/с}, \quad (2.1)$$

де n – кількість портів комутатора, μ – інтенсивність трафіку.

Найбільша мережа компанії складає 45 вузлів, тому пропускна здатність мережі маршрутизаторів:

$$Pp.p = \mu * l * N * 8 = 157 * 650 * 45 * 8 = 367,38 \text{ Мбіт/с}, \quad (2.2)$$

де N – кількість вузлів в найбільшій мережі.

Пропускна здатність 367,38 Мбіт/с є меншою за максимальну, тому мережеве обладнання не буде працювати в перевантаженому режимі, що дозволить якісну роботу системи.

Розподільчий пристрій направляє трафік на вихідну лінію до маршрутизатора з пропускною здатністю 1000 Мбіт /с:

$$\mu_{\text{вих}} = 1000\,000\,000 / (650 * 8) = 192\,310 \text{ пакетів/с}. \quad (2.3)$$

Кожний пристрій в мережі використовує в середньому 157 пакетів на секунду, тому розрахуємо максимальне значення кількості джерел в корпоративній мережі:

$$N = 192\,310 / 157 = 1224 \text{ джерел}. \quad (2.4)$$

Число повністю забезпечує потрібних 45 вузлів.

Інтенсивність вихідного трафіку найбільшій мережі від всіх користувачів:

$$\lambda = N \cdot \mu = 45 * 157 = 7065 \text{ (пакетів/с)}. \quad (2.5)$$

Визначимо коефіцієнт затримки на маршрутизаторі, поділивши показник навантаження на вихідний канал:

$$\rho = \lambda / \mu_{\text{вих}} = 7065 / 192\,310 = 0,036 \quad (2.6)$$

Коефіцієнт зайнятості комутатора рівня маршрутизатора:

$$r = \rho / (1 - \rho) = 0,036 / (1 - 0,036) = 0,037 \quad (2.7)$$

Середня затримка кадру, пов'язана з чергою М/М/1, становить:

$$T = 1 / ((\mu - \lambda)) = 1 / (192\,310 - 7065) = 5,39 \text{ мкс} \quad (2.8)$$

Середня довжина черги:

$$L_{\text{чер}} = \rho^2 / (1 - \rho) = (0,036)^2 / (1 - 0,036) = 0,0013 \quad (2.9)$$

Середній час пакетів у черзі:

$$T_{\text{оч}} = L_{\text{чер}} / \lambda = 0,0013 / 7065 = 1,22 \text{ мс} \quad (2.10)$$

Затримка в мережі сягає 1,22 мс, а це майже в 6 раз менше ніж задано за вимогами.

Пропускна здатність каналу:

$$\lambda = (\text{пропускна здатність}) / (\text{довжина кадру}) = b/l$$

$$b = \lambda * l = 7065 * 650 * 8 = 36\,738\,000 \text{біт/с} = 36,7 \text{ Мбіт/с} \quad (2.11)$$

Пропускна здатність покриває всі питання, щодо забезпечення максимальної навантаженості в мережі.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Конфігурація маршрутних налаштувань комп'ютерної мережі в цифровому значенні

IP-адресація є важливою складовою мережевої інфраструктури і використовується для ідентифікації та адресації пристроїв у мережі. Вона дозволяє пристроям спілкуватись між собою та передавати дані.

Розрахунок IP-адресації включає декілька кроків. Перш за все, потрібно визначити тип IP-адреси, який може бути IPv4 або IPv6. За вимогами та завдання використовуємо адресу 192.168.5.0.

IPv4 адреси представлені у вигляді чотирьох чисел, розділених крапками, наприклад, 192.168.5.1. Кожне число може приймати значення від 0 до 255.

Після вибору типу IP-адреси потрібно визначити мережу та підмережу. Це здійснюється за допомогою маски підмережі, яка вказує, які біти IP-адреси відповідають мережі і які - хостам. Задана маска мережі – /24.

Маска підмережі представляється так само, як і IP-адреса, у вигляді чотирьох чисел, розділених крапками, наприклад, 255.255.255.0. Ця маска вказує, що перші три числа (24 біти) відповідають мережі, а останнє число (8 біт) - хостам.

Після визначення IP-адреси мережі та маски підмережі можна розрахувати доступні IP-адреси для хостів. Для цього використовується процес підрахунку мережевого ідентифікатора та хостового ідентифікатора.

Мережевий ідентифікатор визначається, застосовуючи операцію побітового І (AND) між IP-адресою та маскою підмережі. Хостовий ідентифікатор визначається, використовуючи операцію побітового НЕ (NOT) з маскою підмережі та мережевим ідентифікатором.

Наприклад:

Адреса – 192.168.5.1, маска – /24, переведемо до двійкового формату:

Адреса – 11000000.10101000.00000101 | 00000001

Маска – 11111111.11111111.11111111 | 00000000

Кожні 8 байт розраховуються проти годинної стрілки, а саме біти 1,2,4,8,16,32,64,128 що в сумі дорівнює 256 адрес. В нашому прикладі частина яка розділена маскою займає перше значення, тобто 1, що і є вузлом мережі.

Таблиця 3.1 – Адресація локальних підмереж

Номер мережі	LAN1	LAN2	LAN3	LAN4
192.168.5.0/24	41	22	45	21

На принципах розрахунку адрес для корпоративної мережі, розрахуємо адреси і для глобальних інтерфейсів, за діапазоном по завданню – 10.0.5.0/30.

В кожному діапазоні нам потрібні лише 2 вузли, а це забезпечить маска 255.255.255.252 або /30.

Таблиця 3.2 – Адресація глобальних підмереж

Назва підмережі	Кількість вузлів	Номер підмережі	Маска підмережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
LAN1	41	192.168.5.0	255.255.255.192	192.168.5.1	192.168.5.62
LAN2	22	192.168.5.128	255.255.255.224	192.168.5.129	192.168.5.158
LAN3	45	192.168.5.64	255.255.255.192	192.168.5.65	192.168.5.126
LAN4	21	192.168.5.160	255.255.255.224	192.168.5.161	192.168.5.190
VLAN11	4	192.168.5.16	255.255.255.240	192.168.5.17	192.168.5.31
VLAN21	4	192.168.5.32	255.255.255.240	192.168.5.33	192.168.5.46
VLAN31	5	192.168.5.48	255.255.255.240	192.168.5.49	192.168.5.62
WAN0	2	64.100.13.0	255.255.255.252	64.100.13.1	64.100.13.2
WAN1	2	10.0.5.0	255.255.255.252	10.0.5.1	10.0.5.2
WAN2	2	10.0.5.4	255.255.255.252	10.0.5.5	10.0.5.6
WAN3	2	10.0.5.8	255.255.255.252	10.0.5.9	10.0.5.10
WAN4	2	10.0.5.12	255.255.255.252	10.0.5.13	10.0.5.14
WAN5	2	10.0.5.16	255.255.255.252	10.0.5.17	10.0.5.18
WAN IPS	2	209.165.202.0	255.255.255.252	209.165.202.1	209.165.202.1

Розрахунок адресації за класами використовується в IPv4 і базується на поділі IP-адрес у мережі на класи: А, В, С, D і Е. Кожен клас має свої особливості та діапазони доступних IP-адрес.

Розберемо опис технічного розрахунку адресації за класами.

Клас А:

- початкова бітова маска: 0xxx.xxxx.xxxx.xxxx;
- діапазон IP-адрес: 1.0.0.0 до 126.0.0.0;
- перший октет використовується для ідентифікації мережі, а три останні – для ідентифікації хостів;
- кількість доступних мереж: 128;
- кількість доступних хостів на мережу: близько 16 мільйонів.

Клас В:

- початкова бітова маска: 10xx.xxxx.xxxx.xxxx;
- діапазон IP-адрес: 128.0.0.0 до 191.255.0.0;
- перші два октети використовуються для ідентифікації мережі, а два останні - для ідентифікації хостів;
- кількість доступних мереж: близько 16 тисяч;
- кількість доступних хостів на мережу: близько 65 тисяч.

Клас С:

- початкова бітова маска: 110x.xxxx.xxxx.xxxx;
- діапазон IP-адрес: 192.0.0.0 до 223.255.255.0;
- перші три октети використовуються для ідентифікації мережі, а останній - для ідентифікації хостів;
- кількість доступних мереж: близько 2 мільйони;
- кількість доступних хостів на мережу: близько 254.

Клас D:

- початкова бітова маска: 1110.xxxx.xxxx.xxxx;
- діапазон IP-адрес: 224.0.0.0 до 239.255.255.255;
- використовується для мультикаст-адресації (передача даних групам пристроїв).

Клас E:

- початкова бітова маска: 1111.xxxx.xxxx.xxxx;
- діапазон IP-адрес: 240.0.0.0 до 255.255.255.255;
- зарезервованій клас, який не використовується для загального

використання.

Наша мережа є локальною та використовує діапазон адрес класу C.

Для прикладу розрахуємо задану адресу на 4 частини, але без урахування кількості вузлів в мережі.

Адреса 192.168.5.0 з маскою /24 вміщує 256 дозволених вузлів. Нам потрібно розділити адресу на мережі, візьмемо вузли 256 розділимо на 4, та отримаємо 64 вузли. Для цього потрібно використовувати /26 маску, тоді мережі будуть виглядати наступним чином:

- 192.168.5.0/26 – 62 вузли;
- 192.168.5.64/26 – 62 вузли;
- 192.168.5.128/26 – 62 вузли;
- 192.168.5.192/26 – 62 вузли.

За таким принцип розбиття за маскою мережі розрахуємо та назначимо адреси всім вузлам мережі, та відобразимо до таблиці відповідно до вимог щодо документації.

Таблиця 3.3 – Адресація індивідуальних засобів мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Мережа IPS						
Antonov_IPS	S0/3/0	209.165.202.2	/30	–	–	S0/3/0
	G0/0	64.100.13.2	/30	–	–	G0/0
	G0/1	209.165.201.1	/28	–	–	G0/1
Antonov_R3	S0/3/0	10.0.5.18	/30	–	–	S0/3/0
	S0/3/1	209.165.202.1	/30	–	–	S0/3/1
Server_AAA	Fa0	209.165.201.5	/28	–	–	Fa0

Продовження таблиці

Мережа LAN1						
Antonov_R5	G0/0	192.168.5.1	/26	–	–	G0/0
	G0/1	10.0.5.1	/30	–	–	G0/1
Antonov_Switch0	Vlan1	192.168.5.2	/26	192.168.5.1	–	G0/1
Antonov_Switch1	Vlan1	192.168.5.3	/26	192.168.5.1	–	G0/1
PC11_18,21	NIC	192.168.5.18- 192.168.5.19	/28	192.168.5.1 7	11	Fa0/12- 0/14
PC21_19,22	NIC	192.168.5.34- 192.168.5.35	/28	192.168.5.3 3	21	Fa0/15- 0/24
PC31_20,23	NIC	192.168.5.50- 192.168.5.51	/28	192.168.5.4 9	31	Fa0/6-0/11
Мережа LAN2						
Antonov_R4	S0/2/0	10.0.5.17	/30	–	–	S0/2/0
	S0/3/0	10.0.5.9	/30	–	–	S0/3/0
	S0/3/1	10.0.5.13	/30	–	–	S0/3/1
	G0/0	10.0.5.6	/30	–	–	G0/0
	G0/1	192.168.5.129	/27	–	–	G0/1
Antonov_Switch3	Vlan1	192.168.5.131	/27	192.168.5.129	–	G0/1
Server_HTTP	NIC	192.168.5.130	/27	192.168.5.129	–	Fa0/7
Printer0	NIC	192.168.5.138	/27	192.168.5.129	–	Fa0/8
PC_9-14	NIC	192.168.5.132- 192.168.5.137	/27	192.168.5.129	–	Fa0/1-6
Мережа LAN3						
Antonov_R0	G0/0	64.100.13.1	/30	–	–	G0/0
	G0/1	192.168.5.65	/26	–	–	G0/1
Antonov_Switch4	Vlan1	192.168.5.66	/26	192.168.5.65	–	Fa0/1- 0/4
Antonov_Switch5	Vlan1	192.168.5.67	/26	192.168.5.65	–	Fa0/1- 0/4
Antonov_Switch6	Vlan1	192.168.5.68	/26	192.168.5.65	–	Fa0/1- 0/4
PC_0-2	NIC	192.168.5.70- 192.168.5.72	/26	192.168.5.65	–	Fa0/5- 0/7_sw4
PC_3-5	NIC	192.168.5.73- 192.168.5.75	/26	192.168.5.65	–	Fa0/5- 0/7_sw5

Кінець таблиці 3.3.

PC_6-8	NIC	192.168.5.76- 192.168.5.78	/26	192.168.5.65	–	Fa0/5- 0/7_sw6
Server_TFTP	NIC	192.168.5.69	/26	192.168.5.65	–	Fa0/8 – sw4
Мережа LAN4						
Antonov_Router2	G0/0	192.168.5.161	/27	–	–	G0/0
	S0/3/0	10.0.5.10	/30	–	–	S0/3/0
	S0/3/1	10.0.5.14	/30	–	–	S0/3/1
PC_15-17	NIC	192.168.5.164- 192.168.5.166	/27	192.168.5.161	–	Fa0/1-3
Antonov_Switch2	Vlan1	192.168.5.163	/27	192.168.5.161	–	G0/1
Printer1	NIC	192.168.5.167	/27	192.168.5.161	–	Fa0/4
Server_DNS	NIC	192.168.5.162	/27	192.168.5.161	–	Fa0/5

3.2 Логічне визначення архітектури комп'ютерної мережі

Логічне визначення архітектури комп'ютерної мережі описує спосіб організації та функціонування мережі на рівні логіки та протоколів. Воно визначає, як дані передаються та обробляються в мережі, а також визначає ролі та взаємозв'язок мережевих компонентів.

Також, вона визначає фізичну та логічну топологію мережі. Фізична топологія описує фізичне розташування пристроїв у мережі за топологією дерево. Логічна топологія визначає логічну структуру мережі та шляхи передачі даних між пристроями.

Маршрутизатори у комп'ютерних мережах підключені за допомогою оптоволоконних з'єднань. Кожен маршрутизатор має вхідні та вихідні порти, які забезпечують підключення до інших пристроїв у мережі. З іншого боку, вузли в мережі підключені за допомогою витих парних кабелів.

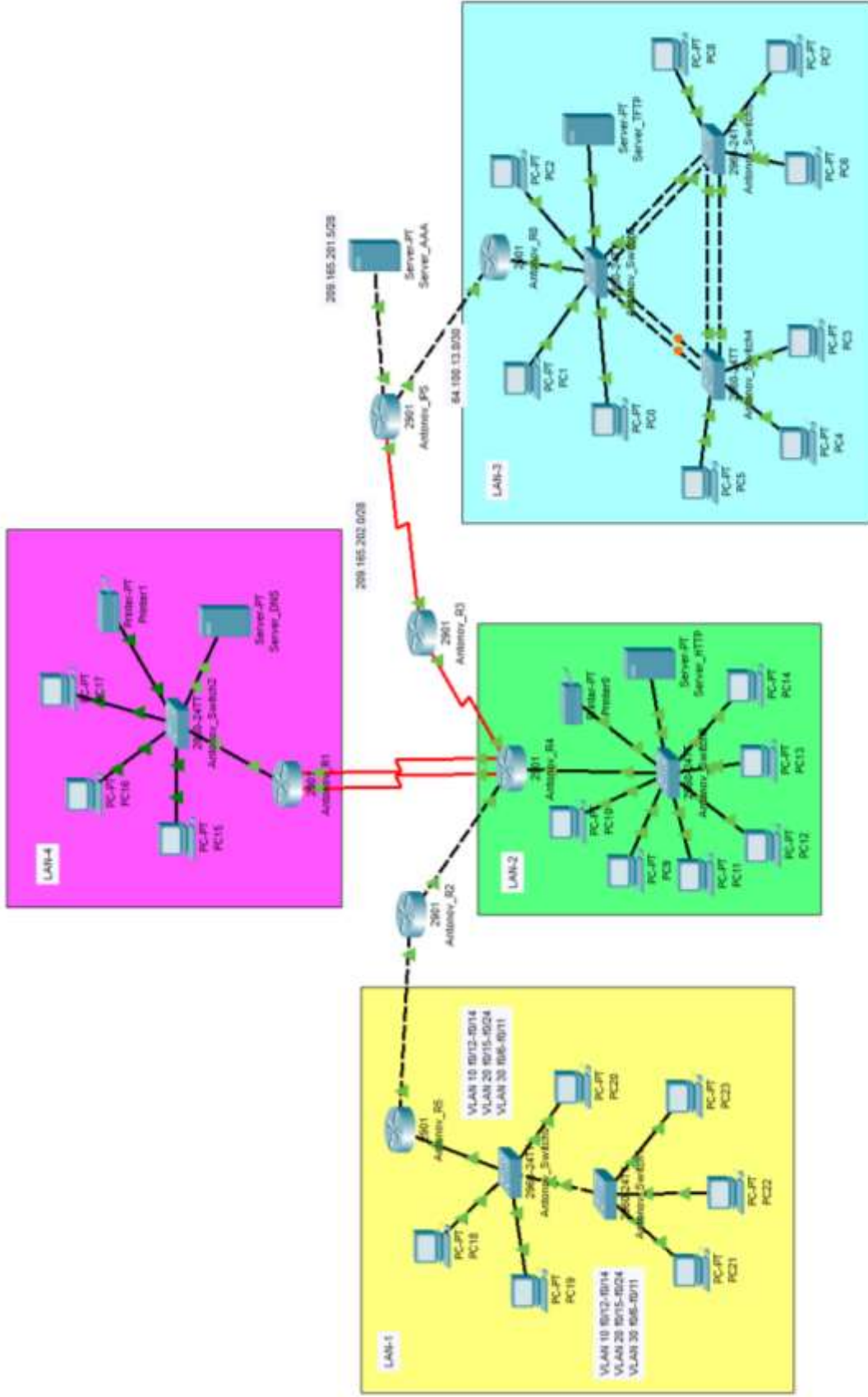


Рисунок 3.1 – Логічне визначення архітектури комп'ютерної мережі транспортної компанії ТОВ «Надір»

3.3 Базова конфігурація параметрів мережевих пристроїв

Корпоративна мережа повністю побудована та має розраховану адресацію. Для подальшого використання мережі необхідно провести налаштування на мережевих пристроях та перевірити роботу системи.

Створимо базову конфігурацію параметрів:

```
enable // отримання доступу режиму EXEC
```

```
configure terminal // режим глобальної конфігурації пристрою
```

```
hostname Antonov_R1 // налаштування імені хоста
```

```
enable secret class // пароль class режиму EXEC
```

```
line console 0 // режим конфігурації лінії консолі
```

```
password cisco // пароль cisco
```

```
login // вмикання аутентифікації для підключень через консольний порт
```

```
service password-encryption // автоматичне шифрування
```

banner motd #123-20zck Antonov authorization PASSWORD# // повідомлення, яке відображається користувачеві під час підключення до пристрою

username 12320zck_Antonov password cisco // використовується для створення інформації про користувача

```
ip domain-name Antonov_R1 // налаштування доменного імені
```

crypto key generate rsa // генерація ключової пари RSA для криптографічних операцій

```
How many bits in the modulus [512]:
```

```
1024
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
line vty 0 4 // налаштування параметрів віртуальних термінальних ліній
```

login local // вмикання аутентифікації для підключень до віртуальних термінальних ліній

transport input ssh // для доступу до віртуальних термінальних ліній дозволено використовувати тільки протокол SSH

Налаштуємо порти комутаторів:

```
interface fa0/4 // перехід в режим конфігурації Fast Ethernet інтерфейсу 4
```

switchport mode access // налаштування режиму порту комутатора (switchport) на режим доступу (access mode)

switchport port-security maximum 1 // налаштування максимальної кількості адрес MAC

switchport port-security mac-address sticky // налаштування порту комутатора (switchport) на використання (sticky) режиму прив'язки адрес MAC для безпеки порту

switchport port-security violation shutdown // налаштування дії при порушенні безпеки порту комутатора (switchport). В даному випадку, при порушенні безпеки порту, порт буде відключений (shutdown).

3.4 Налаштування протоколів мережевого керування

3.4.1 Конфігурація OSPF-маршрутизації

Наведемо один з прикладів налаштування протоколу OSPF (Open Shortest Path First):

router ospf 1 // увімкнення протоколу з унікальним ідентифікатором процесу OSPF

Протокол працює, достатньо лиш написати мережі, які підключаються до маршрутизатору:

network 192.168.5.128 0.0.0.31 area 0 // оголошує мережу 192.168.5.128/27 (з маскою підмережі 255.255.255.224) в області 0 OSPF

network 10.0.5.4 0.0.0.3 area 0 // оголошує мережу 10.0.5.4/30 (з маскою підмережі 255.255.255.252) в області 0 OSPF

network 10.0.5.8 0.0.0.3 area 0 // повтор

network 10.0.5.12 0.0.0.3 area 0 // команд

network 10.0.5.16 0.0.0.3 area 0 // оголошення

Команда "ip route 0.0.0.0 0.0.0.0 209.165.202.2" використовується в пристроях Cisco для налаштування маршруту за замовчуванням (default route). Цей маршрут вказує, що всі пакети, для яких немає більш специфічних маршрутів, повинні бути спрямовані на вказану адресу призначення.

```
ip route 0.0.0.0 0.0.0.0 209.165.202.2
```

Запишемо параметри задані у вимогах:

```
interface s0/3/0 // перехід в режим конфігурації Ethernet інтерфейсу 0/3/0
```

bandwidth 128 // використовується для зміни значень пропускної здатності (bandwidth) на інтерфейсі пристрою. Вона вказує значення пропускної здатності інтерфейсу в кілобітах за секунду (Kbps).

clock rate 128000 // встановлює швидкість передавання даних на серіальному інтерфейсі у 128000 bps

```
ip ospf cost 7500 // налаштування вартості маршруту OSPF
```

3.4.1.1 Аналіз виконання

Проаналізуємо налаштування та підтвердимо налаштування графічною частиною з проекту Cisco Packet Tracer.

```
Antonov_R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O       10.0.5.0/30 [110/66] via 10.0.5.17, 00:33:56, Serial0/3/0
O       10.0.5.4/30 [110/65] via 10.0.5.17, 00:33:56, Serial0/3/0
O       10.0.5.8/30 [110/128] via 10.0.5.17, 00:33:56, Serial0/3/0
O       10.0.5.12/30 [110/128] via 10.0.5.17, 00:33:56, Serial0/3/0
C       10.0.5.16/30 is directly connected, Serial0/3/0
L       10.0.5.18/32 is directly connected, Serial0/3/0
    192.168.5.0/24 is variably subnetted, 6 subnets, 2 masks
O       192.168.5.0/28 [110/67] via 10.0.5.17, 00:33:56, Serial0/3/0
O       192.168.5.16/28 [110/67] via 10.0.5.17, 00:33:56, Serial0/3/0
O       192.168.5.32/28 [110/67] via 10.0.5.17, 00:33:56, Serial0/3/0
O       192.168.5.48/28 [110/67] via 10.0.5.17, 00:33:56, Serial0/3/0
O       192.168.5.128/27 [110/65] via 10.0.5.17, 00:33:56, Serial0/3/0
O       192.168.5.160/27 [110/129] via 10.0.5.17, 00:33:56, Serial0/3/0
    209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/28 is directly connected, Serial0/3/1
L       209.165.202.1/32 is directly connected, Serial0/3/1
S*    0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 3.2 – Налаштовані нами маршрути

```
Antonov_R4#show ip ospf database
      OSPF Router with ID (192.168.5.129) (Process ID 1)

      Router Link States (Area 0)

Link ID        ADV Router    Age          Seq#          Checksum Link count
192.168.5.129  192.168.5.129 1038        0x80000021  0x005717 8
192.168.5.161  192.168.5.161 1070        0x8000001d  0x008622 5
209.165.202.1  209.165.202.1 1068        0x80000019  0x007981 2
10.0.5.5       10.0.5.5       1035        0x8000001c  0x001d9a 2
192.168.5.49   192.168.5.49  1034        0x8000001e  0x003482 5

      Net Link States (Area 0)

Link ID        ADV Router    Age          Seq#          Checksum
10.0.5.6       192.168.5.129 1038        0x80000018  0x0018bf
10.0.5.1       192.168.5.49  1034        0x80000018  0x00dfa0
```

Рисунок 3.3 – База даних протоколу

3.4.2 Конфігурація DHCP-діапазонів

Протокол DHCP-діапазонів дає змогу централізовано керувати й автоматизувати процес виділення IP-адрес, шлюзів за замовчуванням, DNS-серверів та інших мережевих налаштувань для клієнтів.

DHCP дає змогу автоматично призначати IP-адреси клієнтським пристроям під час під'єднання до мережі. Це спрощує процес налаштування мережі, особливо в разі великих мереж або мереж із частим переміщенням клієнтів

Налаштування для прикладу:

```
ip dhcp pool LAN3 // створюємо пул адрес DHCP
```

```
network 192.168.5.64 255.255.255.192 // використовується для налаштування пулу адрес DHCP. Вона вказує діапазон IP-адрес і маску підмережі, які будуть використовуватися для видачі адрес клієнтам DHCP
```

```
default-router 192.168.5.65 // використовується для зазначення адреси основного шлюзу (default gateway) для клієнтів DHCP
```

```
dns-server 192.168.5.162 // використовується для зазначення IP-адреси DNS-сервера, який надаватиме клієнтам DHCP інформацію про доменні імена
```


3.4.2.1 Аналіз виконання

Проаналізуємо налаштування та підтвердимо налаштування графічною частиною з проекту Cisco Packet Tracer.

```
Antonov_R5#show ip dhcp binding
```

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.5.18	00D0.D329.CB7C	--	Automatic
192.168.5.19	0001.43C9.DDAD	--	Automatic
192.168.5.34	0000.0C01.1368	--	Automatic
192.168.5.35	0003.E41C.0D24	--	Automatic
192.168.5.50	0060.5C18.66DD	--	Automatic
192.168.5.51	0009.7C87.1780	--	Automatic

```
Antonov_R5#
```

Рисунок 3.4 – Список DHCP-діапазонів

```
Pool Vlan11 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 14
Leased addresses : 2
Excluded addresses : 0
Pending event : none

1 subnet is currently in the pool
Current index IP address range Leased/Excluded/Total
192.168.5.17 192.168.5.17 - 192.168.5.30 2 / 0 / 14

Pool Vlan21 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 14
Leased addresses : 2
Excluded addresses : 0
Pending event : none

1 subnet is currently in the pool
Current index IP address range Leased/Excluded/Total
192.168.5.33 192.168.5.33 - 192.168.5.46 2 / 0 / 14

Pool Vlan31 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next) : 0 / 0
Total addresses : 14
Leased addresses : 2
Excluded addresses : 0
Pending event : none

1 subnet is currently in the pool
Current index IP address range Leased/Excluded/Total
192.168.5.49 192.168.5.49 - 192.168.5.62 2 / 0 / 14
```

Рисунок 3.5 – Призначені пули адрес

3.4.3 Конфігурація NAT-правил

Конфігурація NAT-правил використовується для перетворення IP-адрес і портів у пакетах даних, що проходять через граничний маршрутизатор перед надсиланням їх у зовнішню мережу провайдера.

Граничний маршрутизатор в мережі – Antonov_R3, який має інтерфейс outside s0/3/1 до інтернет-провайдера.

Налаштування для прикладу:

```
ip nat pool AntonovNAT 209.165.200.5 209.165.200.30 netmask 255.255.255.224
// створюється пул адрес NAT з ім'ям "AntonovNAT", і задається діапазон адрес від
209.165.200.5 до 209.165.200.30 з маскою підмережі 255.255.255.224
```

```
access-list 1 permit 192.168.5.0 0.0.0.255 // створюється access list з номером 1,
і вказується дозвіл (permit) для мережі 192.168.5.0 з маскою підмережі 0.0.0.255
```

```
ip nat inside source list 1 interface s0/3/0 // тут access list з номером 1 (створений
раніше) вказується як умова трансляції
```

```
interface Serial0/3/1
```

```
ip nat outside // інтерфейс s0/3/0 задається як вихідний інтерфейс для
трансльованого трафіку
```

```
interface Serial0/3/0
```

```
ip nat inside інтерфейс s0/3/0 // задається як вхідний інтерфейс для
трансльованого трафіку.
```

3.4.3.1 Аналіз виконання

```
Antonov_R3#show ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: Serial0/3/1
Inside Interfaces: Serial0/3/0
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
Antonov_R3#show ip nat tr
Antonov_R3#show ip nat translations
Pro  Inside global      Inside local          Outside local         Outside global
icmp 209.165.202.1:60     192.168.5.162:60     192.168.5.71:60     192.168.5.71:60
icmp 209.165.202.1:61     192.168.5.162:61     192.168.5.71:61     192.168.5.71:61
icmp 209.165.202.1:62     192.168.5.162:62     192.168.5.71:62     192.168.5.71:62
icmp 209.165.202.1:63     192.168.5.162:63     192.168.5.71:63     192.168.5.71:63
```

Рисунок 3.3 – Встановлені NAT-правила

3.4.4 Конфігурація ACL-параметрів

За допомогою ACL можна визначити, який трафік дозволений або заборонений для проходження через VLAN. Можна вказати, які протоколи, порти або IP-адреси можуть надсилати або отримувати дані всередині VLAN.

ACL дає змогу застосовувати політики безпеки у VLAN. Можна заборонити певні типи трафіку, які можуть становити загрозу або порушувати політику безпеки.

За вимогами, VLAN 11 не повинен мати доступ у підмережі VLAN21 та VLAN31.

Налаштування для прикладу:

```
ip access-list extended 1 // використовується для створення розширеного
списку доступу
```

```
deny ip 192.168.5.16 0.0.0.15 192.168.5.32 0.0.0.15 // правило забороняє трафік
між діапазоном IP-адрес від 192.168.5.16 до 192.168.5.31 і діапазоном IP-адрес від
192.168.5.32 до 192.168.5.47. Параметр "0.0.0.15" задає маску підмережі для
зазначення діапазону адрес
```

```
deny ip 192.168.5.16 0.0.0.15 192.168.5.48 0.0.0.15 // ідентична команда для
іншої мережі
```

```
permit ip any any // використовується для дозволу будь-якого IP-трафіку від
будь-якого джерела до будь-якого призначення. Це правило дає змогу проходити
будь-якому IP-трафіку без будь-яких обмежень
```

```
interface gigabitEthernet 0/0.11 // налаштування інтерфейсу
```

```
ip access-group 1 in // застосовується для прив'язки розширеного списку
доступу (ACL) з ідентифікатором 1 до вхідного трафіку на цьому підінтерфейсі
```

```
interface gigabitEthernet 0/0.21
```

```
ip access-group 1 in
```

```
interface gigabitEthernet 0/0.31
```

```
ip access-group 1 in
```

3.4.4.1 Аналіз виконання

```

C:\>ping 192.168.5.51

Pinging 192.168.5.51 with 32 bytes of data:

Reply from 192.168.5.17: Destination host unreachable.
Reply from 192.168.5.17: Destination host unreachable.
Reply from 192.168.5.17: Destination host unreachable.
Reply from 192.168.5.17: Destination host unreachable.

Ping statistics for 192.168.5.51:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.5.18

Pinging 192.168.5.18 with 32 bytes of data:

Reply from 192.168.5.18: bytes=32 time<1ms TTL=128
Reply from 192.168.5.18: bytes=32 time<1ms TTL=128
Reply from 192.168.5.18: bytes=32 time<1ms TTL=128
Reply from 192.168.5.18: bytes=32 time=25ms TTL=128

Ping statistics for 192.168.5.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 25ms, Average = 6ms

```

Рисунок 3.4 – Працездатність ACL-параметрів

```

Antonov_R5#show access-lists
Extended IP access list lannet
 10 deny ip 192.168.5.16 0.0.0.15 192.168.5.32 0.0.0.15
 20 deny ip 192.168.5.16 0.0.0.15 192.168.5.48 0.0.0.15
 30 permit ip any any (18 match(es))

```

Рисунок 3.5 – Налаштовані ACL-параметрів

3.4.5 Конфігурація LACP-груп

LACP дає змогу комбінувати фізичні мережеві інтерфейси в групу, забезпечуючи збільшення пропускної здатності та підвищення відмовостійкості мережі. Він дає змогу об'єднати кілька фізичних з'єднань між мережевими пристроями (між комутаторами та між комутатором) і використовувати їх як одне логічне з'єднання.

Приклад для налаштування:

int range fa0/1-2 // використовується для переходу в конфігураційний режим інтерфейсу FastEthernet (FastEthernet 0/1-2) на комутаторі

`channel-group 1 mode active` // використовується для налаштування активного режиму агрегації лінків (Link Aggregation) на інтерфейсі

Creating a port-channel interface Port-channel 1

`int port-channel 1` // використовується для переходу в конфігураційний режим віртуального інтерфейсу Port-channel з номером 1 на комутаторі

`switchport mode trunk` // використовується для налаштування режиму роботи інтерфейсу комутатора як транкового (trunk). Транк-порт (trunk port) є типом інтерфейсу, який використовується для передавання даних між комутаторами або між комутатором та іншим мережевим пристроєм із підтримкою віртуальних LAN (VLAN).

Ідентичні налаштування робимо на 3-4 портах, але змінюється одне значення:

`channel-group 2 mode passive` // використовується для налаштування пасивного режиму агрегації лінків (Link Aggregation) на інтерфейсі

3.4.5.1 Аналіз виконання

```
Antonov_Switch6>sh etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)          LACP       Fa0/1(P) Fa0/2(P)
2      Po2(SD)          LACP       Fa0/3(I) Fa0/4(I)
```

Рисунок 3.6 – Налаштовані LACP-групи

```

Group: 1
-----
                        Port-channels in the group:
                        -----

Port-channel: Po1      (Primary Aggregator)
-----

Age of the Port-channel   = 00d:12h:50m:39s
Logical slot/port        = 2/1          Number of ports = 2
GC                       = 0x00000000    HotStandBy port = null
Port state                = Port-channel
Protocol                  = LACP
Port Security              = Disabled

Ports in the Port-channel:

Index  Load  Port      EC state      No of bits
-----+-----+-----+-----+-----
   0    00   Fa0/2     Active        0
   0    00   Fa0/1     Active        0
Time since last port bundled:  00d:12h:50m:39s   Fa0/1
Group: 2
-----
                        Port-channels in the group:
                        -----

Port-channel: Po2      (Primary Aggregator)
-----

Age of the Port-channel   = 00d:12h:50m:39s|
Logical slot/port        = 2/2          Number of ports = 0
GC                       = 0x00000000    HotStandBy port = null
Port state                = Port-channel
Protocol                  = LACP
Port Security              = Disabled

```

Рисунок 3.7 – Відображення інформації про стан агрегованих інтерфейсів

3.4.6 Конфігурація VLAN-інтерфейсів

3.4.6.1 Аналіз виконання

VLAN-інтерфейси дають змогу створювати логічні сегменти мережі, які можуть бути ізольовані один від одного. Це допомагає забезпечити безпеку та запобігає поширенню трафіку між VLAN-ами без потреби.

Таблиця 3.4 – Завдання розподілу

Номер VLAN	Ім'я VLAN	Порт
11	log1	f0/12-f0/14
21	log2	f0/15-f0/24
31	log3	f0/6-f0/11

Налаштування для прикладу:

```
vlan 11 // використовується для створення VLAN з ідентифікатором 11 на комутаторі
```

```
name log1 // використовується для призначення імені або опису VLAN
```

```
interface g0/1
```

```
switchport trunk allowed vlan 11,21,31 // використовується для налаштування списку допустимих VLAN на транковому порту комутатора. Ця команда визначає, які VLAN можуть проходити через транк-порт і брати участь у комунікації.
```

```
switchport mode trunk // використовується для налаштування інтерфейсу комутатора в режимі транка (trunk mode)
```

```
interface range f0/12-14
```

```
switchport mode access // використовується для налаштування інтерфейсу комутатора в режимі доступу (access mode)
```

```
switchport access vlan 11 // використовується для призначення VLAN з ідентифікатором 11 у режимі доступу (access mode) на інтерфейсі комутатора
```

Відповідні налаштування потрібно виконати на інших інтерфейсах:

```
vlan 21
```

```
name log2
```

```
vlan 31
```

```
name log3
```

```
interface range f0/15-24
```

```
switchport mode access
```

```
switchport access vlan 21
```

```
interface range f0/6-11
```

```
switchport mode access
```

```
switchport access vlan 31
```

```
Antonov_Switch0#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5
11 log1	active	Fa0/12, Fa0/13, Fa0/14
21 log2	active	Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
31 log3	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Рисунок 3.8 – Конфігурації VLAN-інтерфейсів

```
Antonov_Switch0#show mac-address-table
Mac Address Table
```

Vlan	Mac Address	Type	Ports
1	0001.6301.9d1a	DYNAMIC	Gig0/2
1	0007.ec34.1301	DYNAMIC	Gig0/1
11	0001.6301.9d1a	DYNAMIC	Gig0/2
11	0007.ec34.1301	DYNAMIC	Gig0/1
21	0001.6301.9d1a	DYNAMIC	Gig0/2
21	0007.ec34.1301	DYNAMIC	Gig0/1
31	0001.6301.9d1a	DYNAMIC	Gig0/2
31	0007.ec34.1301	DYNAMIC	Gig0/1

Рисунок 3.9 – MAC-адреси для всіх віртуальних мереж

3.4.7 Конфігурація AAA-сервісів

AAA-сервіси надають механізми для автентифікації користувачів, авторизації їхніх прав доступу та обліку їхніх дій у мережі.

Налаштування для прикладу:

```
aaa new-model // використовується для активації розширеної моделі AAA
```

```
radius-server host 209.165.201.5 // використовується для налаштування
```

RADIUS-сервера на комутаторі

```
radius-server key radius123 // використовується для налаштування секретного
ключа (shared secret) для RADIUS-сервера
```

```
aaa authentication login default group radius local // "aaa authentication login" -
вказує, що ми налаштуємо метод автентифікації для входу (login), "default" -
```


вказує, що це буде метод аутентифікації, який використовується за замовчуванням для всіх ліній входу, "group radius local" - визначає групу методів аутентифікації, яка буде використана. В даному випадку, використовується комбінація RADIUS і локальної аутентифікації.

3.4.7.1 Аналіз виконання

The screenshot shows the configuration interface for the AAA service on a device named 'Server_AAA'. The interface is divided into several sections:

- Services List:** A sidebar on the left lists various services, with 'AAA' selected and highlighted in blue.
- AAA Service Settings:**
 - Service: On Off
 - Radius Port: 1645
- Network Configuration:**
 - Client Name: Antonov_R2, Client IP: 10.0.5.2
 - Secret: radius123, ServerType: Radius
- Client List Table:**

	Client Name	Client IP	Server Type	Key
1	Antonov_R2	10.0.5.2	Radius	radius123
2	Antonov_R5	10.0.5.1	Radius	radius123
3	Antonov_R4	10.0.5.17	Radius	radius123
4	Antonov_R3	10.0.5.18	Radius	radius123
5	Antonov_R1	10.0.5.10	Radius	radius123
6	Antonov_R0	64.100.13.1	Radius	radius123
- User Setup:**
 - Username: Antonov_R2, Password: admin123
- User List Table:**

	Username	Password
1	Antonov_R2	admin123
2	Antonov_R1	admin123
3	Antonov_R0	admin123
4	Antonov_R3	admin123
5	Antonov_R4	admin123
6	Antonov_R5	admin123

Рисунок 3.10 – Конфігурація AAA-сервісів

3.4.8 Конфігурація веб-сервера HTTP

Налаштуємо код веб-сайту для прикладу:

```
<html> // це відкриваючий тег, який позначає початок HTML-документа
```

```
<body> // є тегом, що визначає основний вміст веб-сторінки, який буде відображатися у вікні браузера
```

```
<center><font size='0' color='light green'> // використовується для вирівнювання вмісту по центру на сторінці, для встановлення розміру шрифту та для встановлення кольору шрифту
```

```
<h1><font face="STENCIL">Веб-сайт Антонова</h1> // використовуються для визначення заголовків і налаштування шрифту відповідно, <h1> - це тег заголовка першого рівня. Він використовується для позначення найважливіших заголовків на веб-сторінці, <font face="STENCIL"> - використовується для встановлення конкретного шрифту для тексту. У даному випадку, значення STENCIL вказує на використання шрифту "STENCIL"
```

Налаштовуємо веб-сайт згідно з поясненням:

```
</font></center>
```

```
<font size='+1' color='grey'>
```

```
</p><font face="STENCIL">Тема - Комп'ютерна система ТОВ "Надір" з опрацюванням побудови, налаштування та безпеки корпоративної мережі</p>
```

```
</p><font face="STENCIL">Антонов А.С.</p>
```

```
</p><font face="STENCIL">Навчальна група - 123-20зск-1</p>
```

```
</p><font face="STENCIL">Інформаційні технології</p>
```

```
</p><font face="STENCIL">Адреса веб-сайту - 123.dnipro.ua</p>
```

```
</font>
```

```
<body>
```

```
<html>
```

3.4.8.1 Аналіз виконання

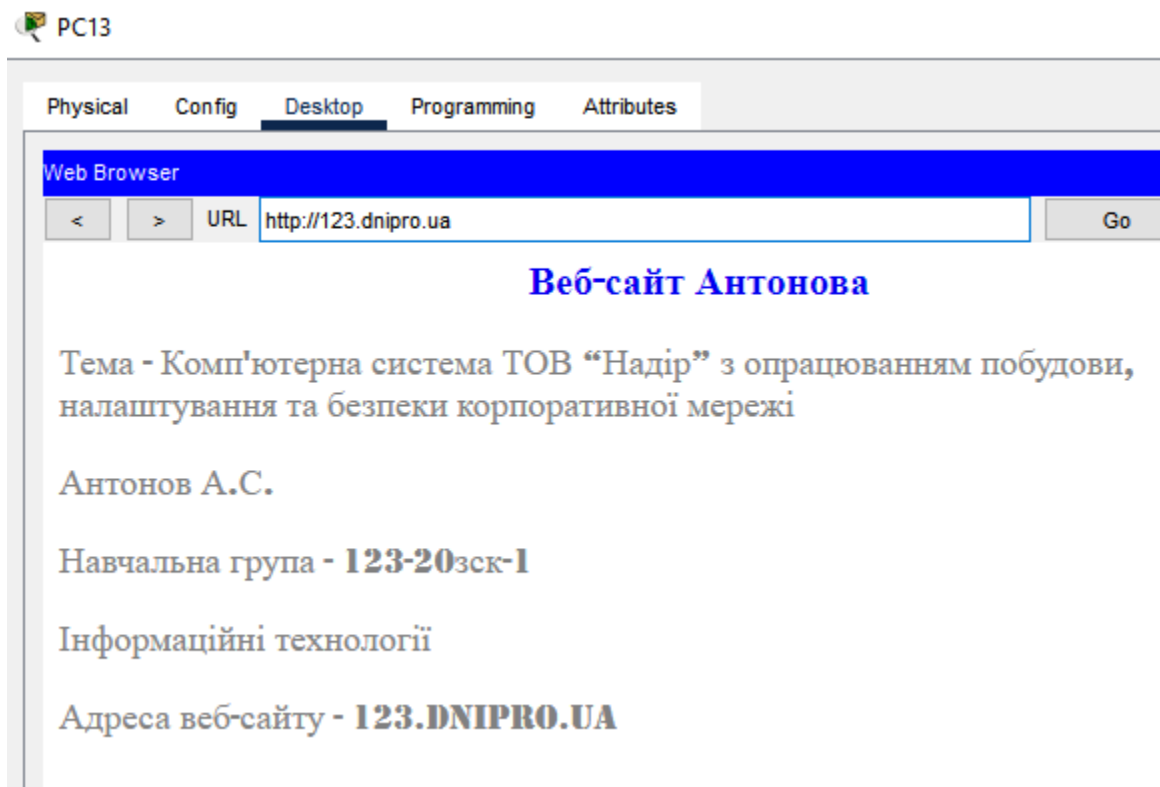


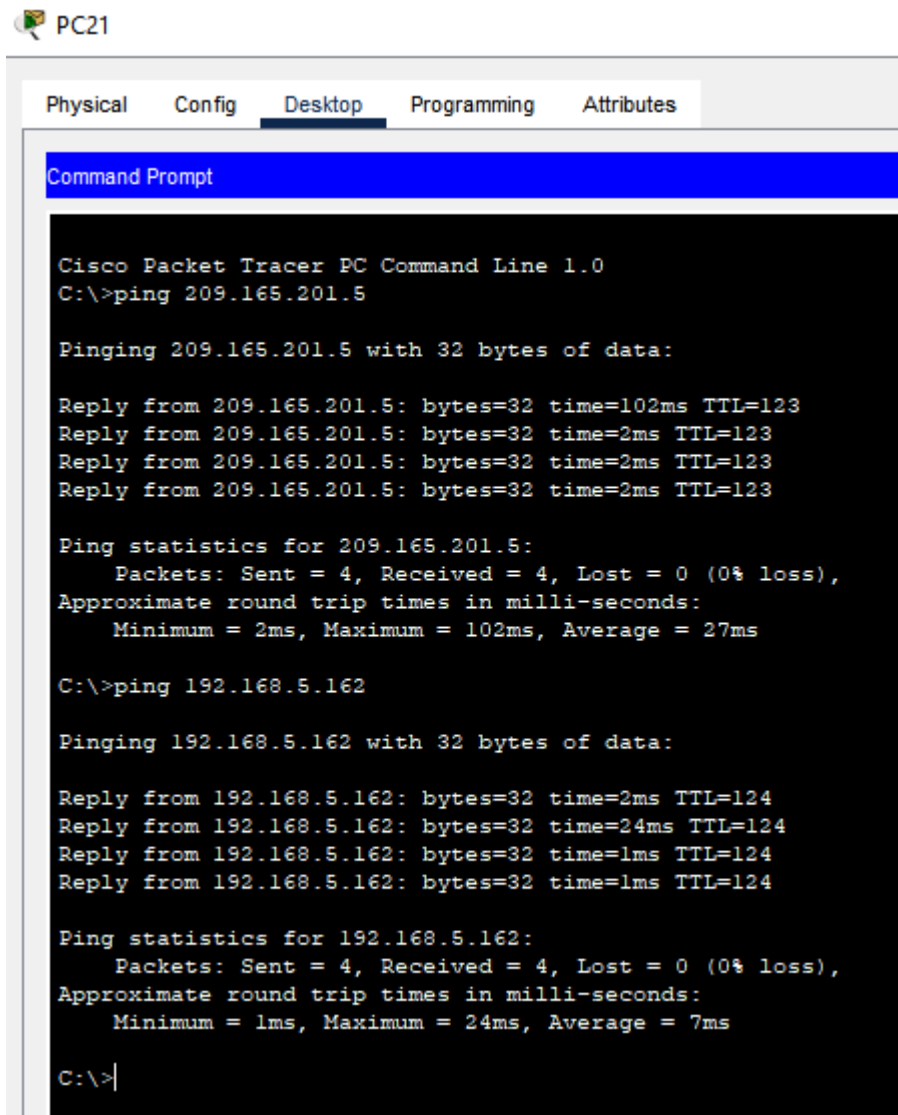
Рисунок 3.11 – Кінцевий вигляд веб-сайту

0	123.dnipro.ua	A Record	192.168.5.130
1	http://123.dnipro.ua	CNAME	123.dnipro.ua

Рисунок 3.12 – Налаштування роботи адреси сайту

3.5 Комплекса оцінка налаштувань

Комплексна оцінка налаштувань мережі складається з останніх перевірок, які не входять в окремі розділи налаштувань, але потребують уваги, для перевірки працездатності мережі.



PC21

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 209.165.201.5

Pinging 209.165.201.5 with 32 bytes of data:

Reply from 209.165.201.5: bytes=32 time=102ms TTL=123
Reply from 209.165.201.5: bytes=32 time=2ms TTL=123
Reply from 209.165.201.5: bytes=32 time=2ms TTL=123
Reply from 209.165.201.5: bytes=32 time=2ms TTL=123

Ping statistics for 209.165.201.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 102ms, Average = 27ms

C:\>ping 192.168.5.162

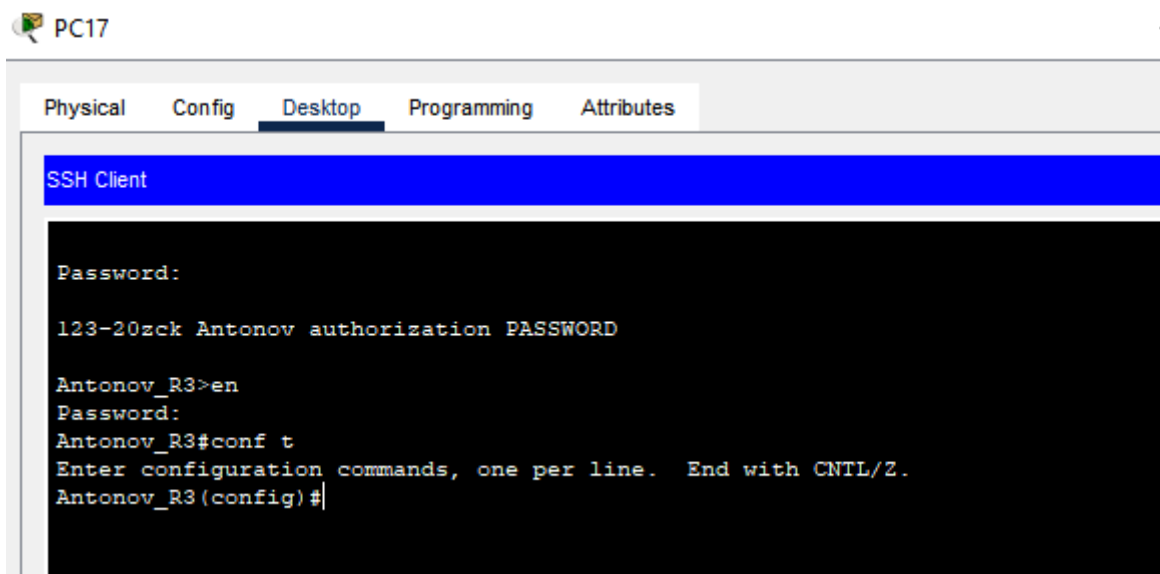
Pinging 192.168.5.162 with 32 bytes of data:

Reply from 192.168.5.162: bytes=32 time=2ms TTL=124
Reply from 192.168.5.162: bytes=32 time=24ms TTL=124
Reply from 192.168.5.162: bytes=32 time=1ms TTL=124
Reply from 192.168.5.162: bytes=32 time=1ms TTL=124

Ping statistics for 192.168.5.162:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 24ms, Average = 7ms

C:\>
```

Рисунок 3.13 – Ехо-запити від мережі LAN4 до серверу AAA



PC17

Physical Config **Desktop** Programming Attributes

SSH Client

```
Password:
123-20zck Antonov authorization PASSWORD

Antonov_R3>en
Password:
Antonov_R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Antonov_R3(config)#
```

Рисунок 3.14 – Застосування протоколу SSH, та демонстрація працездатності налаштування baner MOTD

```

Antonov_R0#copy running-config tftp
Address or name of remote host []? 192.168.5.69
Destination filename [Antonov_R0-config]?

Writing running-config...!!
[OK - 792 bytes]

792 bytes copied in 0.037 secs (21405 bytes/sec)
Antonov_R0#

```

Рисунок 3.15 – Резервне збереження мережевої конфігурації

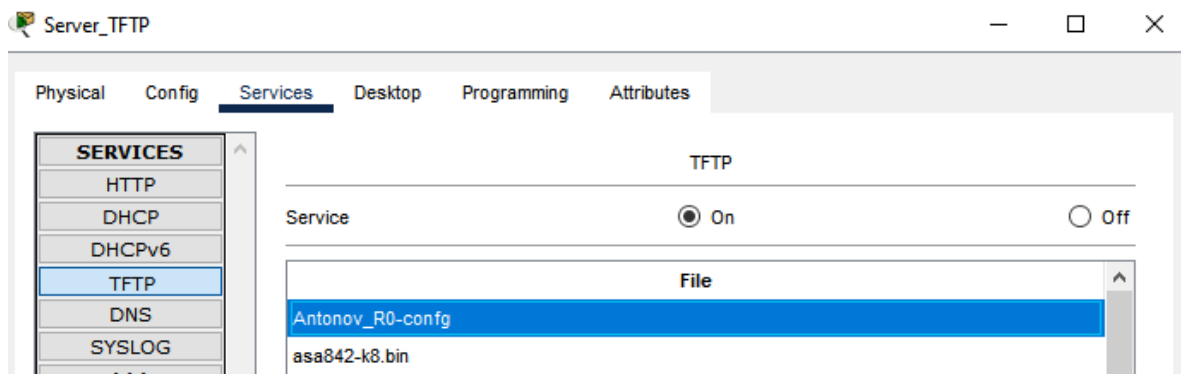


Рисунок 3.16 – Збережена конфігурація у сервері

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ ВЕНТИЛЯЦІЇ

4.1 Розробка системи вентиляції в цілому

За вимогами транспортної компанії ТОВ «Надір» для вантажних відділень було створено систему вентиляції будівель для зниження рівня вуглекислого газу.

Система вентиляції була побудована на технологіях інтернет речей – IoT.

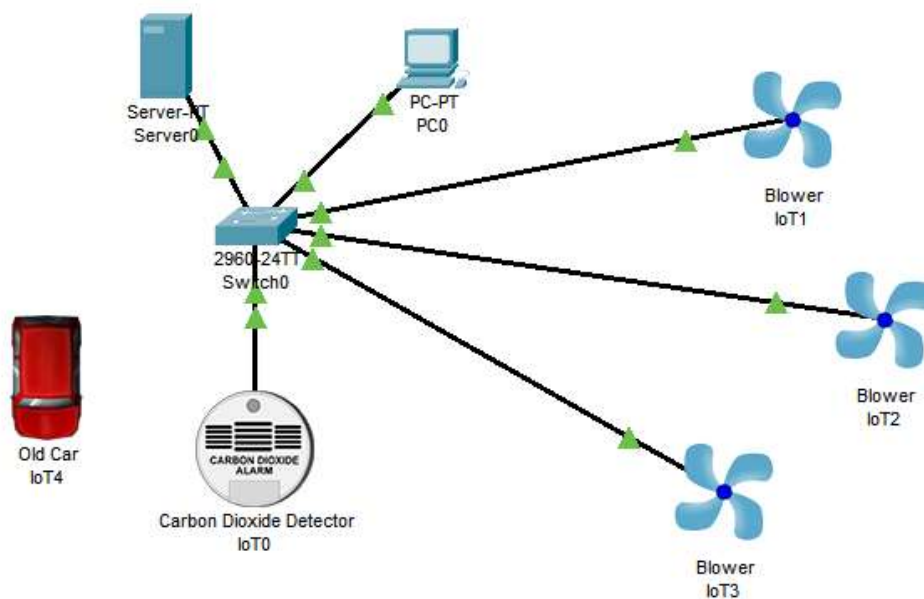


Рисунок 4.1 – Вигляд системи вентиляції

Система вентиляції розрахована на аналізі співвідношення повітря і вуглекислого газу (вихлопні гази машин). Для цього в системі встановлено детектор CO₂.

Система має сервер IoT, ПК – для налаштування та перевірки роботи системи, комутатор – для підключення всіх пристроїв до системи, 3 вентилятори, детектор CO₂ та автомобіль – для перевірки роботи системи.

4.2 Налаштування системи вентиляції

Система вентиляції повинна бути налаштована за конкретними даними показників.

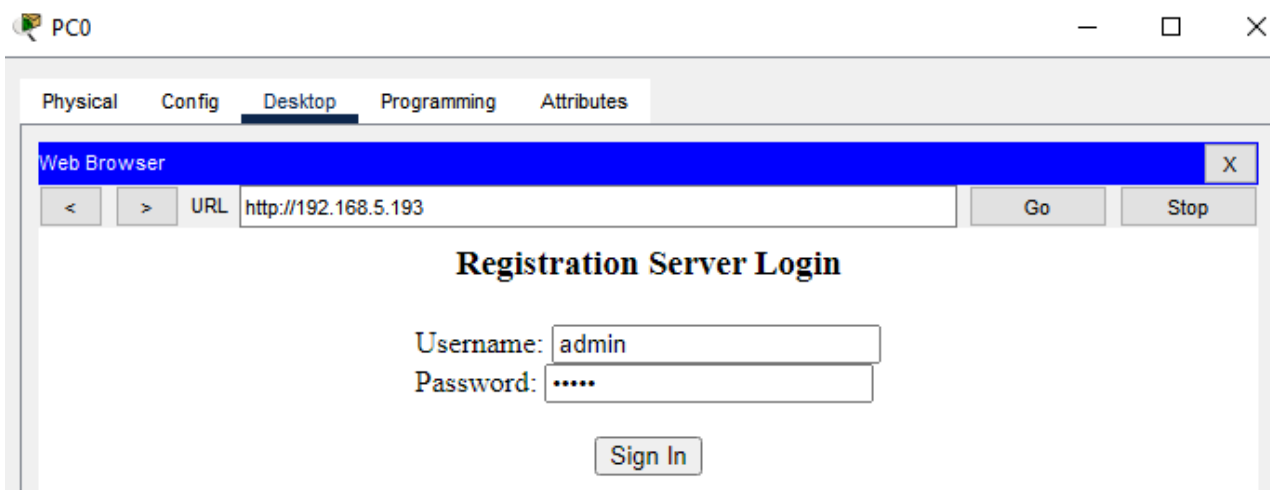


Рисунок 4.2 – Авторизація до серверу IoT

Сервер IoT має IP-адресу – 192.168.5.193 та маску підмережі 255.255.255.240. Для входу до інтерфейсу серверу використовуємо пароль admin/admin.

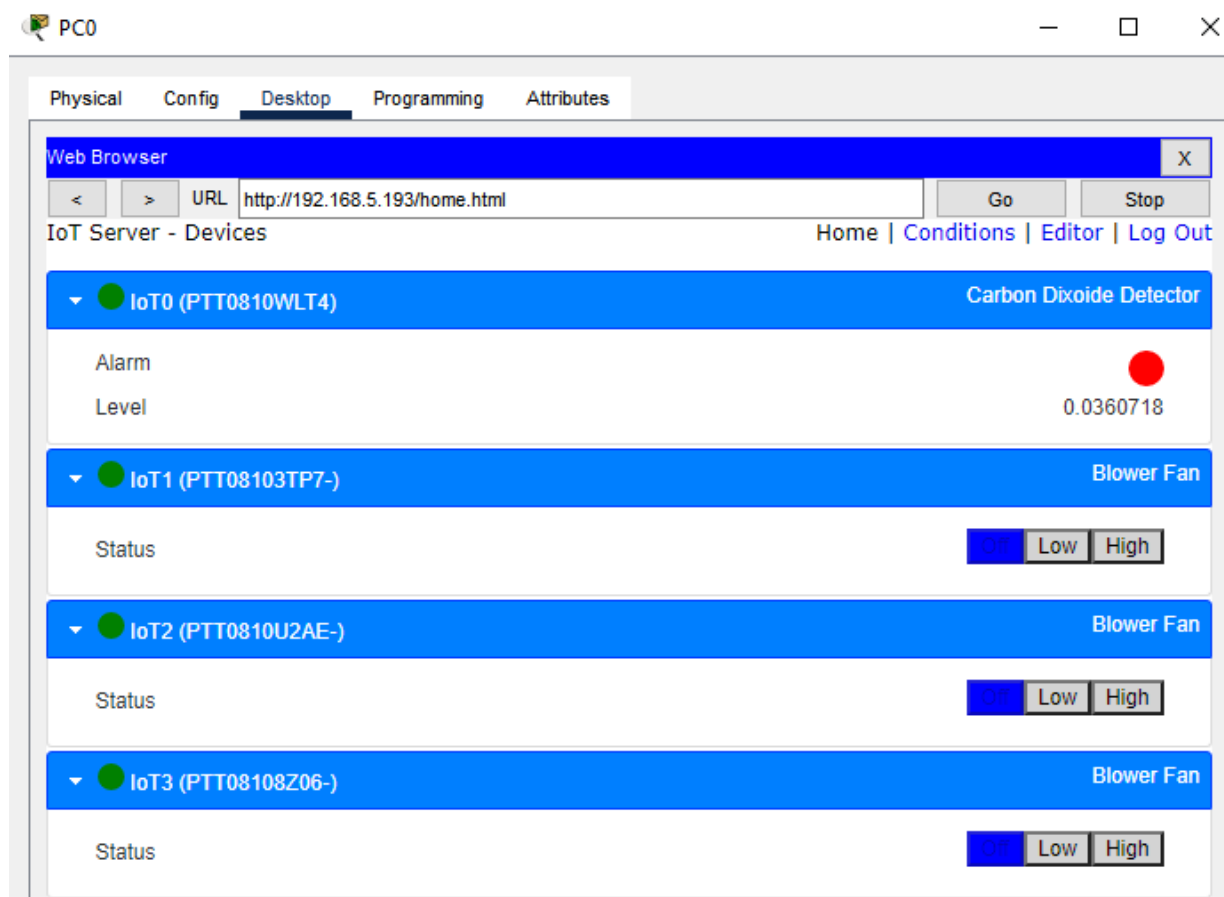


Рисунок 4.3 – Пристрої системи

Після авторизації ми можемо побачити стан пристроїв системи.

Для зчитування інформації від системи вентиляції ми можемо бачити значення детектора повітря та стан кожного вентилятора.

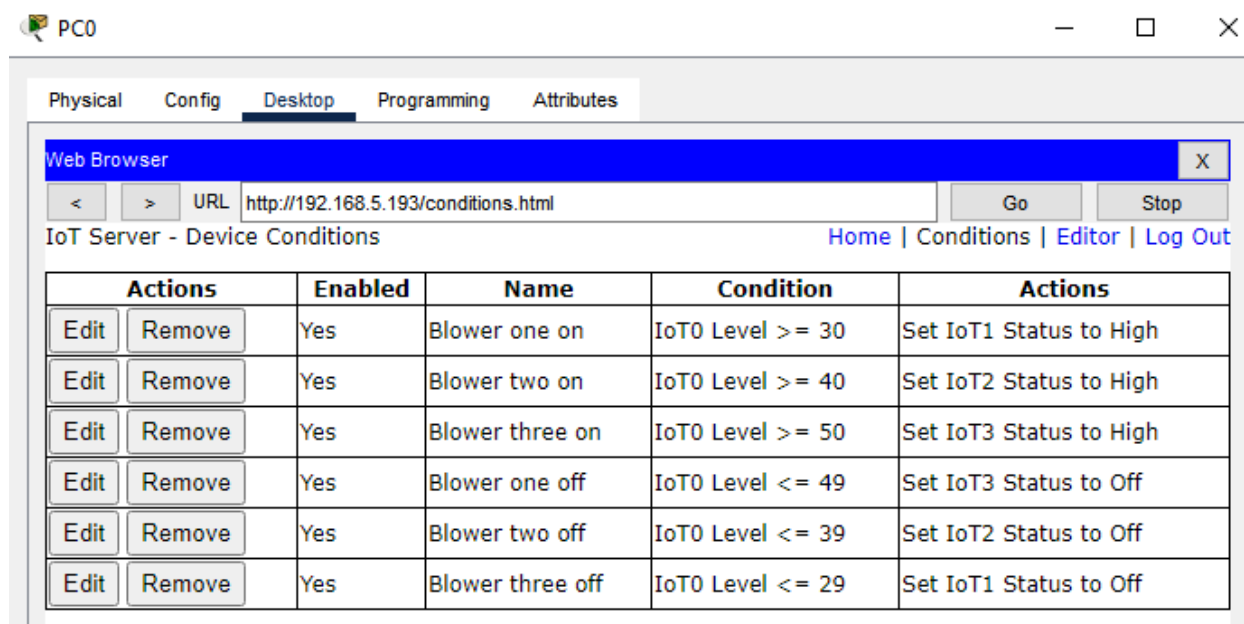


Рисунок 4.4 – Налаштування сценаріїв

Для працездатності системи були створені сценарії спрацювання вентиляторів, а саме:

- якщо вуглекислий газ буде дорівнювати 30%, то увімкнеться перший вентилятор;
- якщо вуглекислий газ буде дорівнювати 40%, то увімкнеться другий вентилятор;
- якщо вуглекислий газ буде дорівнювати 50%, то увімкнеться третій вентилятор;
- якщо вуглекислий газ буде дорівнювати 60%, то увімкнеться сирена на детекторі.

Також, були створені сценарії вимикання вентиляторів:

- якщо вуглекислий газ знизиться до 59% та нижче, то сирена на детекторі вимкнеться;
- якщо вуглекислий газ знизиться до 49% та нижче, то третій вентилятор вимкнеться;
- якщо вуглекислий газ знизиться до 39% та нижче, то другий вентилятор вимкнеться;

– якщо вуглекислий газ знизиться до 29% та нижче, то перший вентилятор вимкнеться.

4.3 Перевірка працездатності системи

Для перевірки працездатності увімкнемо автомобіль для нарахування відсотку вуглекислого газу.

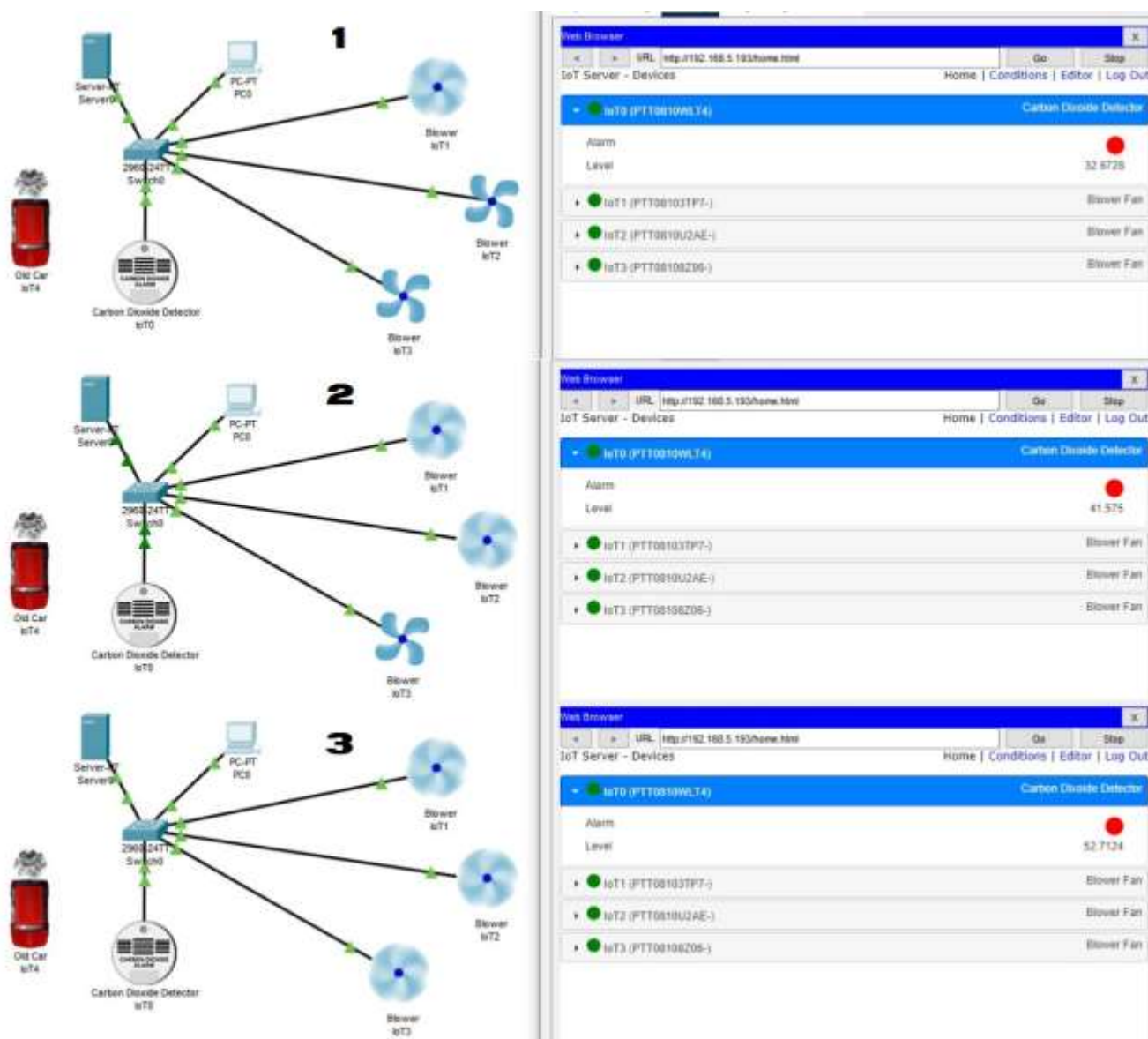


Рисунок 4.5 – Перевірка працездатності системи

Сценарії перевірені та працюють так само і у зворотньому напрямі.

ВИСНОВКИ

У ході написання кваліфікаційної роботи було розроблено апаратну та мережеву частини корпоративної мережі транспортної компанії.

IP-адресація мережі була розподілена відповідно завданню та вимогам компанії та відображена у вигляді таблиць.

Розташування мережевого обладнання та кінцевих пристроїв було графічно зображено у вигляді рисунків та схем. Також, було створена структурована кабельна система, яка має всі елементи для підключення фізичного обладнання мережі.

Мережа використовується для передачі, отримання та обробки інформації.

Для забезпечення якісного функціонування мережі були впроваджені сучасні протоколи стеку TCP/IP.

Мережа використовує технології віртуальних локальних мереж, агрегування каналів зв'язку, технології перетворення локальних мереж в глобальні мережі, системи безпеки мережевого обладнання та резервування конфігурацій мережевого обладнання.

Маршрутизація мережі налаштована за динамічним протоколом OSPF.

Також, в мережі застосовуються технології безпечного віддаленого управління пристроями та списки контролю доступу ACL.

Кваліфікаційна робота має навчальний напрям для майбутнього застосування при створенні або модернізації мереж. Вона може використовуватися як інструкція для проектування та моделювання мережевої інфраструктури будь-якого підприємства або державних установ.

ПЕРЕЛІК ПОСИЛАНЬ

1. ДСТУ «3008-2015». Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – К.: Держстандарт, 1998. – 37 с.
2. Цвіркун Л.І. Комп'ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.
3. ДСТУ «ГОСТ 19.701-90. ЄСПД». Єдина система програмної документації. Схема алгоритмів, програм, даних і систем. Позначення умовні та правила виконання. - М.: Держстандарт, 1990. - 128 с.
4. Цвіркун Л.І. Глобальні комп'ютерні мережі. Програмування мовою PHP: навч. посібник / Л.І. Цвіркун, Р.В. Липовий, під заг. ред. Л.І. Цвіркуна. – Д.: Національний гірничий університет, 2013. – 239 с. – ISBN 978-966-350-417-9.
5. Цвіркун, Л.І. Розробка програмного забезпечення комп'ютерних систем. Програмування: навч. посібник / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова, під заг. ред. Л.І. Цвіркуна. – 3-є вид., випр. – Д.: Національний гірничий університет, 2016. – 223 с. – ISBN 978-966-350-595-4.
6. Реалізація VLAN в пристроях CISCO [Електронний ресурс] – <https://e-server.com.ua/uk/poradi/shho-take-vlan-logika-tehnologija-i-nalashtuvannja-realizacija-vlan-v-pristrojah-cisco>.
7. Що таке NAT, як його налаштувати на роутері [Електронний ресурс] – <http://teg.com.ua/shho-take-nat-yak-jogo-nalashtuvati-na-routeri-zrobiti-vidkritim-abo-zminiti-tip-tehnologiya-loopback-ta-traversal-yak-pratsyuye-network-address-translation/>.
8. ACL (Access Control List): вчимося працювати з доступами у різних системах [Електронний ресурс] – <https://highload.today/uk/acl-access-control-list/>.
9. Топологія типу «Дерево» та її налаштування [Електронний ресурс] – <https://studfile.net/preview/5152835/page:6/>.

Додаток А

Текст програми налаштування мережі комп'ютерної системи

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ

Текст програми
804.02070743.23001-01 12 01

Листів 13

2023

АННОТАЦІЯ

Програма складається з частини програмного коду для налаштування конфігурацій мережевих інтерфейсів мережі. Код призначений для працездатності протоколів DHCP, AAA, NAT, PAgP для налаштування консолей та ліній VTY та для створення комп'ютерних підмереж VLAN, домену та SSH доступу. Також, для налаштування списків доступу ACL та базового налаштування мережевого обладнання.

ЗМІСТ

	Стор.
1.Налаштування маршрутизатора Antonov_R3	4
2.Налаштування маршрутизатора Antonov_R5	6
3.Налаштування комутатора Antonov_Switch0	9

Конфігурація Antonov_R3:

```
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
service password-encryption  
!  
hostname Antonov_R3  
!  
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1  
!  
no ip cef  
no ipv6 cef  
!  
username 12320zck_Antonov password 7 0822455D0A16  
!  
license udi pid CISCO2901/K9 sn FTX1524ZFK5-  
!  
ip domain-name Antonov_R3  
!  
spanning-tree mode pvst  
!  
interface GigabitEthernet0/0  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface GigabitEthernet0/1  
no ip address
```



```
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
ip address 10.0.5.18 255.255.255.252
ip nat inside
!
interface Serial0/3/1
ip address 209.165.202.1 255.255.255.240
ip nat outside
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 10.0.5.16 0.0.0.3 area 0
!
ip nat inside source list 1 interface Serial0/3/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
!
ip flow-export version 9
!
access-list 1 permit 192.168.5.0 0.0.0.255
!
banner motd #123-20zck Antonov authorization PASSWORD#
```

```
!  
line con 0  
  password 7 0822455D0A16  
  login  
!  
line aux 0  
!  
line vty 0 4  
  login local  
  transport input ssh  
!  
end
```

Налаштування маршрутизатора Antonov_R5:

```
!  
version 15.1  
no service timestamps log datetime msec  
no service timestamps debug datetime msec  
no service password-encryption  
!  
hostname Antonov_R5  
!  
ip dhcp pool Vlan11  
  network 192.168.5.16 255.255.255.240  
  default-router 192.168.5.17  
  dns-server 192.168.5.162  
ip dhcp pool Vlan21  
  network 192.168.5.32 255.255.255.240  
  default-router 192.168.5.33  
  dns-server 192.168.5.162
```

```
ip dhcp pool Vlan31
network 192.168.5.48 255.255.255.240
default-router 192.168.5.49
dns-server 192.168.5.162
!
ip cef
no ipv6 cef
!
license udi pid CISCO2901/K9 sn FTX1524C661-
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 192.168.5.1 255.255.255.240
duplex auto
speed auto
!
interface GigabitEthernet0/0.11
description log1
encapsulation dot1Q 11
ip address 192.168.5.17 255.255.255.240
ip access-group lannet in
!
interface GigabitEthernet0/0.21
description log2
encapsulation dot1Q 21
ip address 192.168.5.33 255.255.255.240
ip access-group lannet in
!
interface GigabitEthernet0/0.31
```

```
description log3
encapsulation dot1Q 31
ip address 192.168.5.49 255.255.255.240
ip access-group lannet in
!
interface GigabitEthernet0/1
ip address 10.0.5.1 255.255.255.252
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 10.0.5.0 0.0.0.3 area 0
network 192.168.5.0 0.0.0.15 area 0
network 192.168.5.16 0.0.0.15 area 0
network 192.168.5.32 0.0.0.15 area 0
network 192.168.5.48 0.0.0.15 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
ip route 0.0.0.0 0.0.0.0 10.0.5.2
!
ip flow-export version 9
!
ip access-list extended lannet
deny ip 192.168.5.16 0.0.0.15 192.168.5.32 0.0.0.15
```

```
deny ip 192.168.5.16 0.0.0.15 192.168.5.48 0.0.0.15
permit ip any any
!
line con 0
!
line aux 0
!
line vty 0 4
login
!
end
```

Налаштування комутатора Antonov_Switch0:

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Antonov_Switch0
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
```

```
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/7
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/8
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/9
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/10
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/11
  switchport access vlan 31
  switchport mode access
!
interface FastEthernet0/12
  switchport access vlan 11
```

```
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 11
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 11
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 21
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 21
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 21
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 21
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 21
switchport mode access
!
```

```
interface FastEthernet0/20
  switchport access vlan 21
  switchport mode access
!
interface FastEthernet0/21
  switchport access vlan 21
  switchport mode access
!
interface FastEthernet0/22
  switchport access vlan 21
  switchport mode access
!
interface FastEthernet0/23
  switchport access vlan 21
  switchport mode access
!
interface FastEthernet0/24
  switchport access vlan 21
  switchport mode access
!
interface GigabitEthernet0/1
  switchport trunk allowed vlan 11,21,31
  switchport mode trunk
!
interface GigabitEthernet0/2
  switchport trunk allowed vlan 11,21,31
  switchport mode trunk
!
interface Vlan1
  no ip address
```



```
shutdown
!  
line con 0  
!  
line vty 0 4  
login  
line vty 5 15  
login  
!  
end
```