

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем

Кафедра телекомунікацій та радіотехніки

КВАЛІФІКАЦІЙНИЙ ПРОЄКТ

Бакалавр

Освітній рівень

Спеціальність 172 Телекомунікації та радіотехніка

Шифр і назва спеціальності

на тему: **ПРОЕКТУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ НА БАЗІ
МАРШРУТИЗИРУЮЩИХ КОМУТАТОРІВ**

КПТР. 2017017.01.07 ПЗ

Виконав:

студент 4 курсу, група ТР-17-1


підпис

Роженюк Р.В.

Ініціали, прізвище

Керівник:

д-р техн. наук, проф.


підпис


Мясіщев О.А.

Ініціали, прізвище

До захисту допускаю:

Зав. кафедри ТР

д-р техн. наук, проф.


підпис

Бойко Ю.М.

Ініціали, прізвище

«20» травня 2021р.

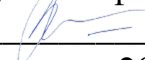
Хмельницький, 2021

Хмельницький національний університет

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра телекомунікацій та радіотехніки
Спеціальність 172 – Телекомунікації та радіотехніка

ЗАТВЕРДЖУЮ

Завідувач кафедри ТР


Юлій БОЙКО
«10» лютого 2021 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНИЙ ПРОЄКТ**

дипломнику Роженюк Роман Васильович

(Прізвище, ім'я, по батькові студента)

1 Тема проекту Проектування телекомунікаційної мережі на базі маршрутизуючих комутаторів

Затверджено наказом ректора університету від 5 02 2021 р. № 11

2 Строк подання студентом проекту на кафедру «1» 06 2021 р. 3 Вихідні дані до проекту. Провести моделювання в середовищі Cisco Packet Tracer; Розглянути Протокол STP для усунення петель і резервування зв'язків; Використання маршрутизаторів в мережевих технологіях; Зробити загальний огляд побудови сучасних телекомунікаційних мереж на базі комутаторів, маршрутизаторів та проаналізувати основні функції та призначення комутаторів; Зробити аналіз типів та протоколів, які використовуються у коммутаторах при побудові телекомунікаційних мереж 4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):

1 Аналітичний огляд літературних джерел по темі кваліфікаційної роботи;

2 Аналіз побудови телекомунікаційних мереж;


3 Моделювання телекомунікаційної мережі

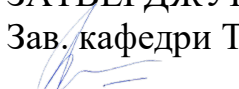
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень): Структура пакету на вхідному комутаторі; Результат моделювання телекомунікаційної мережі в реальному часі; Модель корпоративної телекомунікаційної мережі, яка побудована з використанням технології VLAN.

6 Термін подання роботи до захисту 20 травня 2021 року

7 Дата видачі завдання 10 лютого 2020 року

Науковий керівник 

Завдання отримав 

ЗАТВЕРДЖУЮ
Зав. кафедри ТР
 Юлій БОЙКО
«10» лютого 2021 р.


ПЛАН ІНДИВІДУАЛЬНОЇ РОБОТИ

№ п/п	Найменування виду роботи	Форма звітності, термін виконання	Відмітка наукового керівника
1.	Огляд літератури	Вступ 11.02	Виконано
2.	Ознайомлення з комутаторами та маршрутизаторами	Розділ 1 17.02	Виконано
3.	Аналіз принципу побудови мереж	Розділ 2 10.03	Виконано
4.	Моделювання мережі в середовищі СРТ	Розділ 3 24.03	Виконано
5.	Плакат. Модель спроектованої телекомунікаційної мережі	Плакат 7.04	Виконано
6.	Структурна схема	Креслення 19.04	Виконано
7.	Висновки по роботі	Висновки 23.04	Виконано

Примітки:

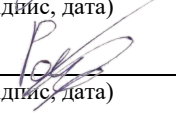
1. _____
2. _____

Науковий керівник



(підпис, дата)

Студент






(підпис, дата)

ЗМІСТ

Стор

1 ВСТУП.....	6
1 АНАЛІТИЧНИЙ ОГЛЯД ЛІТЕРАТУРНИХ ДЖЕРЕЛ ПО ТЕМІ КВАЛІФІКАЦІЙНОЇ РОБОТИ.....	7
1.1. Основні принципи побудови сучасних локальних мереж	7
1.2. Комутатори в локальних мережах	10
1.3. Рівні комутації	13
1.4. Режими комутації	15
1.5. Класифікація комутаторів	16
1.6. Використання маршрутизаторів в мережевих технологіях	18
1.7. Постановка задачі	20
2 АНАЛІЗ ПОБУДОВИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ	21
2.1. Аналіз віртуальних локальних мереж	21
2.2. Протокол STP для усунення петель і резервування зв'язків	23
2.3. Використання протоколу динамічної маршрутизації RIP для організації резервних зв'язків між маршрутизаторами	26
2.4. Протокол маршрутизації OSPF	29
2.5. Використання списків керування доступом ACL	32
3 МОДЕЛЮВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ.....	35
3.1. Результати моделювання в середовищі Cisco Packet Tracer	35
3.2. Тестування побудованої телекомунікаційної мережі.....	50
ВИСНОВКИ.....	54
СПИСОК ЛІТЕРАТУРИ.....	55

					КПТР2017017.01.07 ПЗ				
Зм.	Арк.	№докум.	Підпис	Дата	Проектування телекомунікаційної мережі на базі маршрутизуючих комутаторів Пояснювальна записка	Літера	Аркуш	Аркушів	
Виконав	Роженик Р.В.					у		4	
Перевір.	Мясищев О.А.								
Т.Контр									
Н.контр.									
Затвер.	Бойко Ю.М.							ТР-17-1, ФПКТС, VUV	

РЕФЕРАТ

Записка: 55 сторінок, 47 рисунків, 10 джерел.

Мета роботи – проектування телекомунікаційної мережі на базі маршрутизаторів та маршрутизуючих комутаторів, вибір технологій мережі.

Об'єкт дослідження - створенні за допомогою комутаторів віртуальні мережі в телекомунікаційній мережі.

Предмет дослідження – рух та маршрутизація трафіку між віртуальними мережами у телекомунікаційній мережі.

Метод дослідження – метод комп'ютерного моделювання.

Для розробленої телекомунікаційної мережі здійснено обґрунтування використання технологій локальної мережі Ethernet/FastEthernet, VLAN. Спроектвана телекомунікаційна мережа у середовищі Cisco Packet Tracer перевірена на працездатність на основі тестування мережі в реальному часі та перехопленні пакетів в режимі симуляції.

ТЕЛЕКОМУНІКАЦІЙНА МЕРЕЖА, STP, ACL, МАРШРУТИЗАТОР, МАРШРУТИЗИРУЮЩИЙ КОМУТАТОР, КОМУТАЦІЯ, МАРШРУТИЗАЦІЯ, VLAN.

					КПТР 2017017.01.07 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		5

ВСТУП

В наш час Інтернет є глобальною мережею передачі інформації на землі, яка створила єдиний інформаційний простір. Мережа Інтернет складається з безлічі великих і малих мереж, а також індивідуальних комп'ютерів, які пов'язані між собою. Основу Інтернету складають IP-технології. Сучасні тенденції розвитку телекомунікаційних мереж і систем передачі інформації передбачають надання різноманітних послуг, таких як: обмін даними між користувачами, передача аудіо-та відеоінформації по єдиній мультисервісній мережі зв'язку. Для цієї мети створюються мережі нового покоління Next Generation Network - NGN. Передача даних по мережі Інтернет реалізується, в основному, на базі протоколу TCP / IP (Transmission Control Protocol / Internet Protocol - Протокол управління передачею даних / Міжмережевий протокол). Протокол TCP / IP - це набір протоколів або правил, які були створені, щоб надати можливість комп'ютерам спільно використовувати ресурси мережі. В сучасному суспільстві досить важко знайти офіс компанії, яка не має своєї локальної мережі. Локальна комп'ютерна мережа є основою для взаємодії працівників у робочих групах, відділах і між ними, через мережу здійснюється взаємодія між головним офісом компанії і філіями, працівниками та клієнтами. Останні кілька років стрімке зростання отримали домашні локальні мережі, провайдери Ethernet To Home, які надають практично будь-які можливі сервіси, які звично отримувати в іншому вигляді, наприклад, цифрове телебачення або практично безкоштовна IP-телефонія, за допомогою якої стало можливим спілкуватися без обмежень з усім світом. Крім клієнтського обладнання, такого, як стаціонарні комп'ютери та ноутбуки мережа включає в себе досить велику кількість різних службових пристроїв. Службові пристрої створюють мережеву інфраструктуру і управляють потоками даних, надають різні додаткові сервіси, задають різні правила і політики роботи мережі. Найбільш поширеним обладнанням в мережах TCP / IP є комутатори і маршрутизатори.

					<i>КПТР 2017017.01.07 ПЗ</i>	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		6

1 АНАЛІТИЧНИЙ ОГЛЯД ЛІТЕРАТУРНИХ ДЖЕРЕЛ ПО ТЕМІ КВАЛІФІКАЦІЙНОЇ РОБОТИ

1.1. Основні принципи побудови сучасних локальних мереж

Телекомунікаційні мережі являють собою сукупність апаратних і програмних засобів, які разом забезпечують передачу даних і інформаційних повідомлень між користувачами[1]. При побудові телекомунікаційних мереж неможливо всіх абонентів мережі з'єднати окремими лініями зв'язку. Тому з'єднання користувачів телекомунікаційних послуг мережі (абонентів) (А), що знаходяться в різних частинах земної кулі, здійснюється через транзитні вузли (ТВ) зв'язку (рис.1.1).

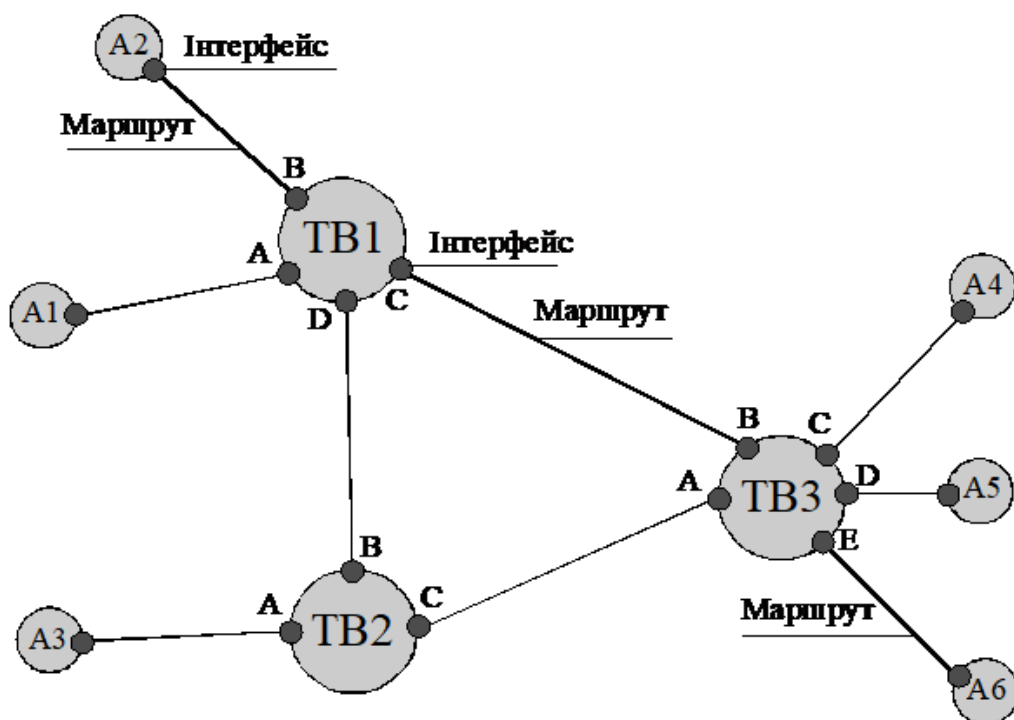


Рисунок 1.1 – Телекомунікаційна мережа

Телекомунікаційна мережа складається із користувачів мережі - абонентів (А) і вузлів зв'язку, з'єднаних телекомунікаційними лініями зв'язку.

Вузли ТВ здійснюють комутацію повідомлення, яке надійшло з вхідного інтерфейсу на вихідний інтерфейс . Наприклад, в мережі рис.1.1 при передачі даних від абонента А2 абоненту А6 транзитний вузол ТВ1 виробляє комутацію повідомлення з вхідного інтерфейсу В на вихідний С, транзитний вузол ТВ3 - з вхідного інтерфейсу В на вихідний Е.

При передачі даних формується маршрут, по якому передаються повідомлення. Комутація – це процес формування маршруту. Комутацією ще називають передачу (просування) повідомлення з вхідного на вихідний інтерфейс. Функцію комутатора виконують транзитні телекомунікаційні вузли у мережах де всі можливі маршрути вже створені і необхідно тільки вибрати найбільш оптимальний маршрут. Процес вибору оптимального маршруту для передачі повідомлень по мережі отримав назву маршрутизація, а пристрій який реалізує цей процес – маршрутизатор(router). Існують таблиці маршрутизації(комутації) з використанням певного критерію - метрики для вибору оптимального маршруту вузлом. Тому, мережі поділяють на: мережі з комутацією каналів, коли ТВ виконують функції комутаторів, і з комутацією пакетів (повідомлень), коли ТВ виконують функції маршрутизаторів. Дані види телекомунікаційних мереж використовуються для передачі різних видів трафіку. Мережі з комутацією каналів в основному використовують для передачі рівномірного трафіку, наприклад, мережі зв'язку. У мережах передачі даних з змінним трафіком застосовується комутація пакетів, наприклад, в локальних комп'ютерних мережах. Різниця між комутацією пакетів та комутацією повідомлень полягає в тому, що повідомлення може мати дуже великий об'єм. Тому, коли в повідомленні виникає помилка, тоді повторно потрібно передавати все повідомлення великого обсягу. У мережах з комутацією пакетів повідомлення поділяється на невеликі пакети (сегменти), тому при втраті або спотворенні частини даних повторно потрібно передати тільки втрачений пакет. В наш час створюються мережі нового покоління (Next Generation Network - NGN), в яких всі види трафіку передаються по єдиній

						<i>КПТР 2017017.01.07 ПЗ</i>	Арк.
Зм.	Арк.	№докум.	Підпис	Дата			8

мультисервісній телекомунікаційній мережі (Internet Multi Service - IMS) на відміну існуючих моносервісних мереж.

Мультисервісна телекомунікаційна мережа надає великий набір телекомунікаційних послуг з гнучкими можливостями їх керування. Телекомунікаційні мережі NGN використовуються для передачі різних видів інформації: аудіо, відеоінформації та дискретних даних. Передача голосу, даних, і відео по мережі NGN отримала назву Triple Play. На рис.1.2 наведено приклад телекомунікаційної мережі, в якій користувачі через мережі доступу підключаються до магістральної мережі, що забезпечує транспорт повідомлень. Користувачі об'єднуються в локальні комп'ютерні мережі, що функціонують в межах обмеженого простору (приміщення, корпус, будинок, офіс)[3, 7].



Рисунок 1.2. – Структурна схема телекомунікаційної мережі

Для створення маршрутів передачі даних у телекомунікаційних мережах необхідно задавати адреси джерел і отримувачів повідомлень. Ці адреси бувають двох типів: фізичні і логічні. Фізичні адреси адресують відповідні інтерфейси телекомунікаційних вузлів і абонентських пристроїв, а логічні адреси належать користувачам.

Зм.	Арк.	№докум.	Підпис	Дата

колізій при мікросегментації не виникає. При одночасній передачі даних від двох джерел одному адресату буферизація кадрів дозволяє запам'ятати і передати кадри по черзі, що дозволяє уникнути їх втрати. Відсутність колізій дозволяє застосовувати топології мережі з індивідуальним підключенням вузлів до портів комутатора. Комутатор є пристроєм другого (канального) рівня семирівневої моделі OSI, в якому для адресації використовуються MAC-адреси. Адресація відбувається на основі MAC-адрес мережевих адаптерів вузлів (рис.1.3)[1, 3].

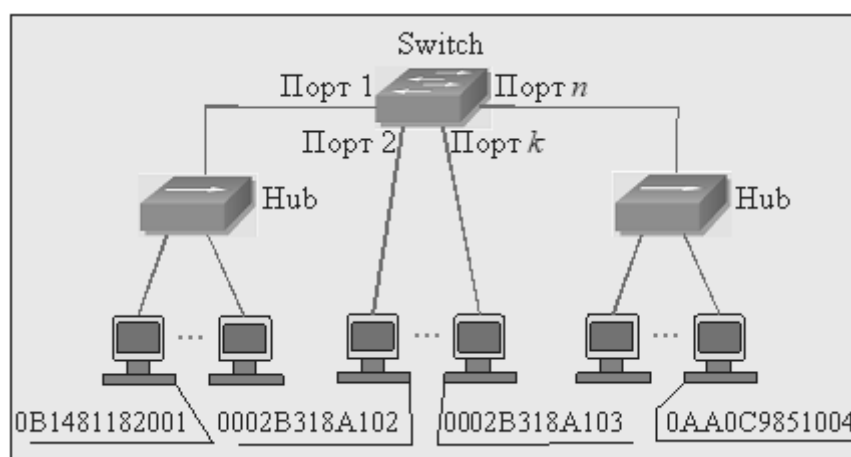


Рисунок 1.3 – Мережа на базі комутатора

Для передачі кадрів в локальних мережах використовується алгоритм прозорого моста, який визначається стандартом 802.1D. Реалізація алгоритму прозорого моста здійснюється за рахунок створення статичних або динамічних записів адресної таблиці комутації. Статичні записи адресної таблиці створюються адміністратором цієї мережі. В динамічному режимі комутатор можна й не конфігурувати, він буде працювати за замовчуванням, створюючи записи адресної таблиці. При цьому в буферній пам'яті порту запам'ятовуються всі поступивші на порт кадри. Спочатку інформація про те, які MAC-адреси мають підключення до конкретного порту вузла, в комутаторі відсутня. Комутатор, отримавши кадр, передає його на всі свої порти, за винятком того,

на який кадр був отриманий, і одночасно аналізує MAC-адресу джерела і запам'ятовує його в адресній таблиці. Наприклад, якщо вузол з MAC-адресою 0B1481182001 передає кадр даних вузлу 0AA0C9851004 (рис.1.3), то в таблиці (табл. 1.1) з'явиться перший запис. При передачі даних від вузла 0AA0C9851004 вузлу 0002B318A102 в табл. 1.1 з'явиться другий запис і т.д. Таким чином, число записів в адресній таблиці може дорівнювати числу вузлів в мережі, побудованої на основі комутатора.

Таблиця 1.1 – Таблиця комутації

№ запису	MAC-адреса	№ порта
1	0B1481182001	1
2	0AA0C9851004	<i>n</i>
3		
4		

Коли адресна таблиця комутації сформована, на підставі записів в адресній таблиці відбувається передача кадрів. При отриманні кадру комутатор перевіряє, чи існує MAC-адреса вузла призначення в таблиці комутації. При виявленні адресата в таблиці комутатор робить перевірку: чи знаходяться адресат і джерело в одному сегменті. Якщо адресат і джерело в різних сегментах, то комутатор виробляє просування (forwarding) кадру в порт, до якого підключений вузол призначення. Якщо вони знаходяться в одному сегменті, то передавати кадр на інший порт нетреба. В данному випадку кадр повинен бути вилучений з буфера порту, що називається фільтрацією (filtering) кадрів. З появою в мережі нових вузлів адресна таблиця поповнюється. Якщо протягом певного часу (зазвичай близько 300 сек.) вузол не передає дані, то вважається, що він в мережі відсутній, тому відповідний запис з таблиці видаляється[1, 3, 9].

При отриманні кадрів з ширококомовними адресами комутатор передає їх на всі свої порти. Але комутатор не фільтрує кадри з ширококомовними адресами, тому якщо будь-якої вузол через збій починає помилково генерувати кадри з

широкомовними адресами, то мережа перевантажується, настає широкомовний шторм (broadcast storm), і мережа "падає". Цим широко користуються хакери, які бажають порушити нормальне функціонування мережі. Вони «наповнюють» мережу широкомовними повідомленнями з помилковими адресами джерела, адресна таблиця комутації коммутатора переповнюється і комутатор починає працювати, як концентратор. При цьому зловмисник отримує можливість аналізувати всю інформацію, передану по локальній мережі. З широкомовним штормом може боротися тільки маршрутизатор (рис.1.4), який ділить мережу на широкомовні домени.

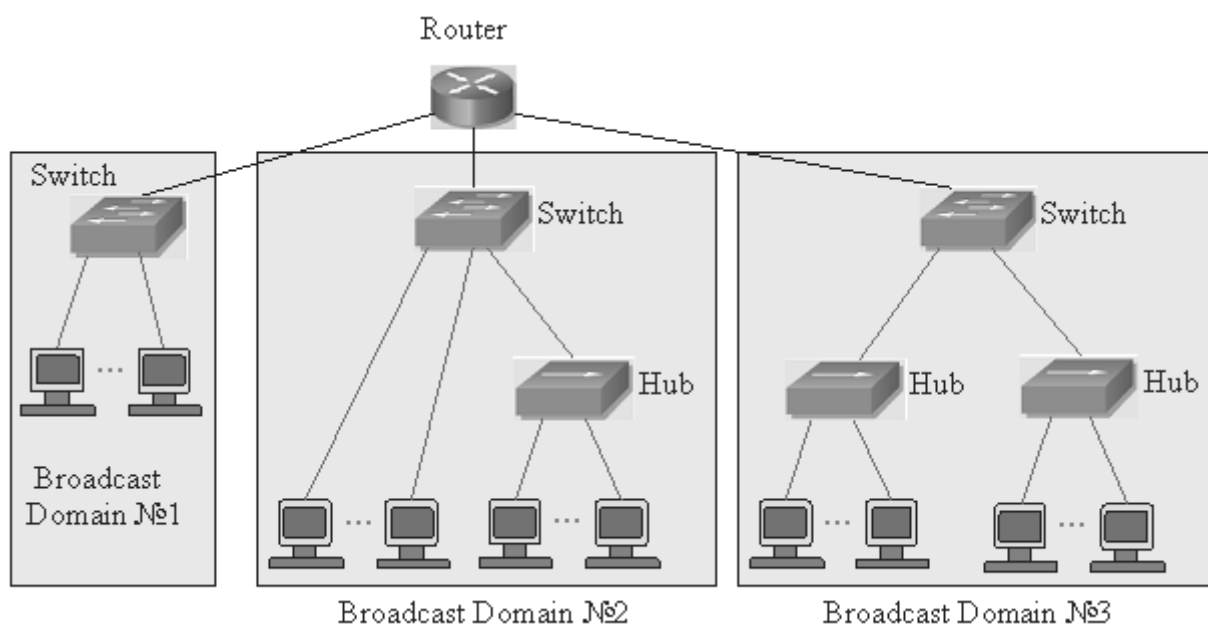


Рисунок 1.4 – Поділ мережі на широкомовні домени

Швидкодія будь-якого комутатора визначаються швидкістю просування кадрів, тривалістю затримки передачі кадру, швидкістю фільтрації кадрів і пропускною спроможністю[7].

1.3. Рівні комутації

Існує декілька рівнів комутації. Комутація другого рівня – є апаратною. За допомогою спеціалізованого контролера Application-Specific Integrated Circuits (ASIC) обробляється передача кадру в комутаторі. Дана технологія

комутації дозволяє комутаторам підтримувати гігабітні швидкості з невеликою часовою затримкою. Основними причинами використання комутаторів другого рівня є об'єднання робочих груп і поділ мережі на сегменти. Комутація другого рівня, незважаючи на значні переваги все ж таки має певні обмеження. Наявність комутаторів в мережі не запобігає поширенню ширококомовних кадрів (broadcast) по всіх сегментах мережі, зберігаючи її прозорість. Отже, телекомунікаційній мережі необхідна функціональність третього рівня моделі OSI. Комутація третього рівня – це апаратна маршрутизація, де передача пакетів обробляється контролерами ASICs. Комутатори третього рівня приймають рішення не на основі MAC – адрес, а на основі інформації мережевого рівня. Комутація третього рівня застосовується для отримання високої швидкості комутації, яка властива коммутаторам другого рівня і для отримання масштабованості маршрутизації. Обробку пакетів комутатором третього рівня така сама, як і обробка пакетів маршрутизатором. В основі комутації третього рівня лежить апаратна реалізація, що є основною відмінністю між маршрутизаторами і L3 комутаторами. У маршрутизаторах загального призначення комутація пакетів здійснюється програмно. Оскільки комутатори третього рівня зазвичай швидше і дешевше маршрутизаторів, то їх використання в локальних мережах дуже вигідно. В якості прикладів комутаторів третього рівня можна відзначити D-Link DES-3326S і DES-3326SR, DES-3350SR[4, 5].

Комутація четвертого рівня ґрунтується на апаратній маршрутизації мережевого рівня OSI, яка відповідає за управляючу інформацію четвертого рівня. Застосування комутації четвертого рівня дає можливість приймати рішення про передачу пакета, спираючись не лише на MAC або IP адреси, а й на параметри четвертого рівня такі, як номер порту. Маршрутизатори вміють керувати трафіком, ґрунтуючись на інформації транспортного рівня. Одним з методів є створення розширених списків доступу (extended access lists). Коли комутатори виконують функції четвертого рівня, вони читають поля TCP і UDP

всередині заголовка і визначають, який тип інформації передається в цьому пакеті. Адміністратор комп'ютерної мережі може запрограмувати комутатор обробляти трафік відповідно до пріоритету додатків. Ця функція дозволяє визначити якість сервісу для кінцевих користувачів. Комутація четвертого рівня необхідна, якщо обрана політика передбачає поділ управління трафіком за додатками або потрібний облік кількості трафіку, що виробляється кожним додатком. Однак слід зауважити, що комутаторам, які виконують комутацію четвертого рівня, потрібна можливість визначати і зберігати велику кількість таблиць комутації, особливо якщо комутатор використовується всередині ядра корпоративної мережі[4].

Маршрутизуючі комутатори мають в своєму складі RISC-процесори, які допомагають обробляти програми статичної та динамічної маршрутизації. Комутатори побудовані за однією з наступних архітектур: з розділяємою багатовходовою пам'яттю (shared memory), на основі загальної високошвидкісної шини, на основі комутаційної матриці.

В даний час комутатори використовують в якості базової одну з трьох схем взаємодії своїх блоків або модулів: комутаційна матриця; розділяема багатовходовою пам'ять; загальна шина. Часто ці три способи взаємодії комбінуються в одному комутаторі.

1.4. Режими комутації

Комутатори можуть працювати в декількох режимах, при переході між якими змінюються надійність і затримка. Для забезпечення максимальної швидкодії передачі інформації комутатор може починати передачу кадру відразу, як тільки отримає MAC-адресу вузла призначення. Такий режим отримав назву наскрізної комутації або (cut-through switching). Режим комутації "на льоту" забезпечує найменшу затримку при проходженні кадрів через комутатор. Проте, в цьому режимі неможливий контроль помилок, оскільки поле контрольної суми знаходиться в кінці кадру. У другому режимі комутатор

отримує кадр цілком, поміщає його в буфер, перевіряє поле контрольної суми (FCS) і потім пересилає адресату. Якщо отриманий кадр прийшов з помилками, то він відкидається (discarded) комутатором. Оскільки кадр перед відправкою адресата призначення запам'ятовується в буферній пам'яті, то такий режим комутації отримав назву комутації з проміжним зберіганням (store-and-forward switching). В режимі буферизації забезпечується висока надійність, але низька швидкість комутації. Проміжне положення між наскрізною комутацією на льоту і буферизацією займає режим комутації вільного фрагмента (fragment-free mode). В цьому режимі читаються перші 64 байта, які включають заголовок кадру і поле даних мінімальної довжини. Після цього починається передача кадру до того, як буде отримано і прочитаний весь кадр цілком. При цьому проводиться верифікація адресації та інформації LLC протоколу, щоб переконатися, що дані будуть правильно оброблені і доставлені адресату. Коли використовується режим наскрізної комутації на льоту, порти пристроїв джерела і призначення повинні мати однакову швидкість передачі (bit rate). Такий режим називається симетричною комутацією (symmetric switching). Якщо швидкості не однакові, то кадр повинен запам'ятовуватися (буферизуватися) перед тим, як буде передаватися з іншою швидкістю. Такий режим називається асиметричною комутацією (asymmetric switching), при цьому повинен використовуватися режим з буферизацією. Асиметрична комутація забезпечує зв'язок між портами з різною пропускнуою здатністю (bandwidths). Даний режим є характерним, наприклад, для потоку даних між багатьма клієнтами і сервером, при якому багато клієнтів можуть одночасно з'єднуватися з сервером. Тому на це з'єднання повинна бути виділена широка смуга пропускання[4, 8].

1.5. Класифікація комутаторів

Комутатори можливо класифікувати за різними ознаками, зокрема по керуванню. Існують керовані комутатори, які мають широкий функціонал

					КПТР 2017017.01.07 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		16

забезпечують зв'язок між мережами і визначають найкращий шлях пакета даних до мережі адресата. Причому, технології локальних мереж, які об'єднуються можуть бути різними.

1.7. Постановка задачі

Як вже було сказано раніше, найбільш поширеним обладнанням в мережах TCP / IP є комутатори і маршрутизатори. Комутація третього рівня – це апаратна маршрутизація, де передача пакетів обробляється контролерами ASICs. Комутатори третього рівня приймають рішення не на основі MAC – адрес, а на основі інформації мережевого рівня. Комутація третього рівня застосовується для отримання високої швидкості комутації, яка властива коммутаторам другого рівня і для отримання масштабованості маршрутизації. Обробка пакетів комутатором третього рівня така сама, як і обробка пакетів маршрутизатором. В основі комутації третього рівня лежить апаратна реалізація, що є основною відмінністю між маршрутизаторами і L3 комутаторами. Оскільки комутатори третього рівня зазвичай швидше і дешевше маршрутизаторів, то їх використання в локальних мережах дуже привабливо.

Проаналізувавши існуючі рішення, щодо застосування комутаторів і маршрутизаторів в телекомунікаційних мережах необхідно виконати наступні завдання:

- зробити загальний огляд побудови сучасних телекомунікаційних мереж на базі комутаторів, маршрутизаторів та проаналізувати основні функції та призначення комутаторів;
- зробити аналіз типів та протоколів, які використовуються у коммутаторах при побудові телекомунікаційних мереж;
- змодельовати телекомунікаційну мережу в середовищі Cisco Packet Tracer та протестувати на предмет розподілу трафіку в даній мережі.

					<i>КПТР 2017017.01.07 ПЗ</i>	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		20

2 АНАЛІЗ ПОБУДОВИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

2.1. Аналіз віртуальних локальних мереж

Virtual Local Area Network(VLAN) – це віртуальна локальна мережа. VLAN можна порівняти з комутатором всередині комутатора. VLAN дозволяє об'єднати комп'ютери в одну мережу на каналному рівні (2-й рівень моделі OSI). Навіть, якщо вони фізично під'єднанні до різних комутаторів. VLAN дозволяє ізолювати весь трафік групи вузлів від основної мережі.

VLAN допомагає структурувати мережу – можна виділити в одну мережу групу комп'ютерів підключену до загального комутатора певного відділу фірми. Всі користувачі підключені до одного комутатора, але наприклад користувачі бухгалтерії повинні мати окрему мережу, яка відділена від звичайних користувачів, студентів, інших працівників[4].

Точно так само можна виконувати розділення сегментів серверів, звичайних користувачів, IP телефонів, IP відеокамер і.т.д. VLAN - це основа побудови будь-якої мережі, яка має декілька інформаційних ресурсів. VLAN вибудовує логічну структуру вашої мережі. Таку структуру набагато легше аналізувати ніж звичайну фізичну схему де зображені тільки підключення рис.2.1:

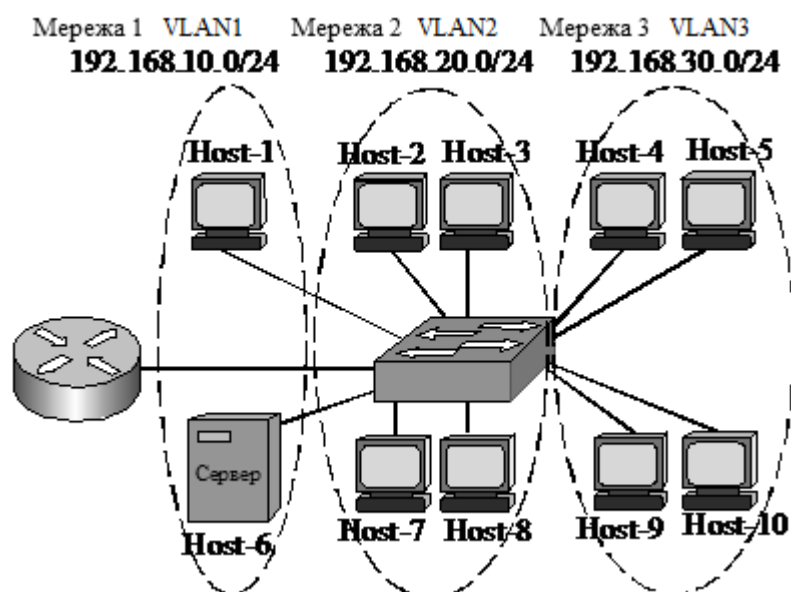


Рисунок 2.1 – Побудова віртуальної локальної мережі

Зм.	Арк.	№докум.	Підпис	Дата

КПТР 2017017.01.07 ПЗ

Арк.

21

VLAN використовується для забезпечення безпеки, наприклад нам потрібно розділити мережу гостей-користувачів від мережі серверів. Розділення мереж значно підвищує безпеку. Так, як можливий зловмисник просто не буде мати доступу в інший сегмент мережі. Користувачі різних сегментів можуть взаємодіяти лише на мережевому рівні моделі(3-му рівні) OSI. А для цього вже потрібно спеціалізований маршрутизуючий пристрій, який функціонує на 3-му рівні OSI, тобто маршрутизатор або маршрутизуючий комутатор.

Наприклад, якщо ми створили три сегмента мережі: сегмент бухгалтерії, сегмент серверів та сегмент звичайних користувачів (рис.2.1). То для зв'язку між цими сегментами нам потрібен буде маршрутизатор, який маршрутизує ці дві мережі, без маршрутизатора ці користувачі взаємодіяти не зможуть.

Також VLAN використовують для об'єднання користувачів - це дає можливість об'єднання користувачів на канальному рівні, навіть якщо вони підключені до різних фізичних комутаторів. Немає необхідності протягувати кабель від користувачів до потрібного комутатора, достатньо лише linka між самими комутаторами (рис.2.2). Користувачі можуть знаходитись на різних поверхах, але завдяки VLAN будуть об'єднанні в одну віртуальну мережу.

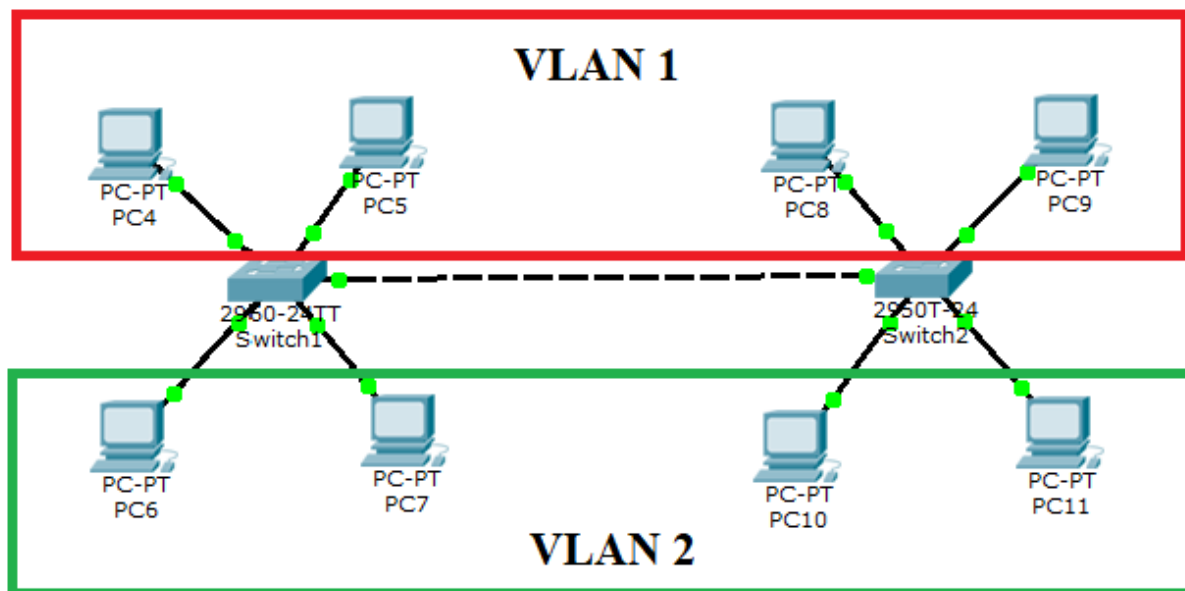


Рисунок 2.2 – Побудова віртуальної мережі фірми

VLAN зменшує кількість ширококомовного трафіка - кожен VLAN це окремий ширококомовний домен.

Звичайний комутатор це пристрій другого рівня моделі осі. За замовчуванням всі порти в комутаторі знаходяться в одному VLANі, а значить в одному ширококомовному домені. Широкомовний домен - це сегмент в якому передаються ширококомовні кадри, тобто кадри які передаються на всю мережу даного сегмента, тобто в кожен порт комутатора. Ці кадри необхідні для роботи багатьох протоколів, таких як: DHCP і інших. В великій мережі ширококомовний трафік може привести до не раціонального використання полоси пропускання. Створення додаткових VLAN на комутаторі означає розбиття комутатора на декілька ширококомовних доменів. Комп'ютери VLAN 1 незважаючи на те, що вони підключені до різних комутаторів знаходяться в одному ширококомовному домені. Якщо користувач буде генерувати ширококомовний запит, то всі комп'ютери даного сегмента його побачать. Користувачі, які знаходяться в іншому сегменті VLAN 2 цей трафік не побачать (рис.2.2). Налаштувати VLAN можна лише на керованих комутаторах до яких можна підключитись по консолі або віддалено з використанням протоколів TELNET або SSH, або за допомогою веб-інтерфейса чи спеціалізованого ПО.

2.2. Протокол STP для усунення петель і резервування зв'язків

Для захисту телекомунікаційної мережі використовують наступні методи організації відказостійких каналів. Перший метод – це метод резервування з'єднань, традиційна надлишкова топологія рис.2.3.

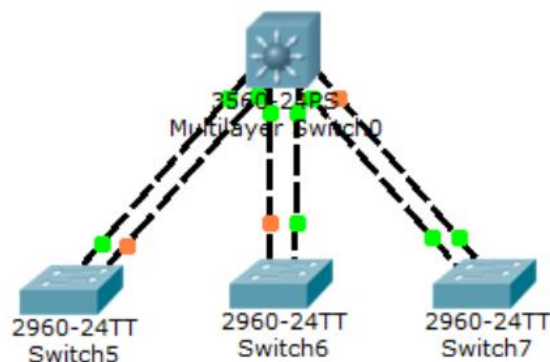


Рисунок 2.3 – Резервування з'єднань на комутаторах

Алгоритм роботи протоколу STP

1) Вибираємо кореневий комутатор. Порти данного комутатора знаходяться в стані передачі даних (призначені порти), вони можуть обмінюватись пакетами рис.2.5:

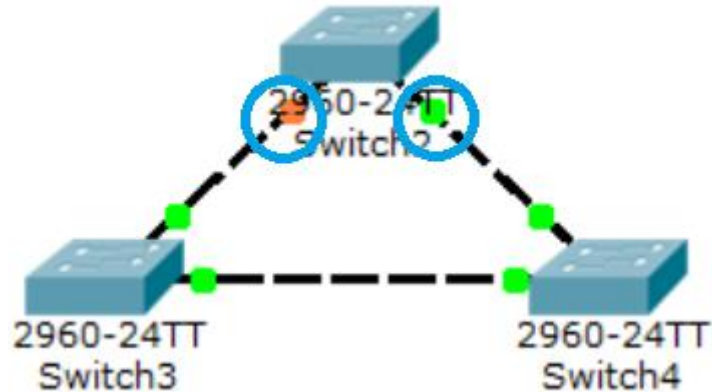


Рисунок 2.5 – Порти кореневого Switch 2(призначені)

2) На некореновому комутаторі необхідно обрати кореневі порти. В залежності від ціни шляху через канал від некоренового комутатора до кореневого коммутатора ми можемо обрати кореневі порти. Ціна шляху (Path Cost) розраховується виходячи із пропускної здатності каналу. Пропускна здатність більша – вартість менша.

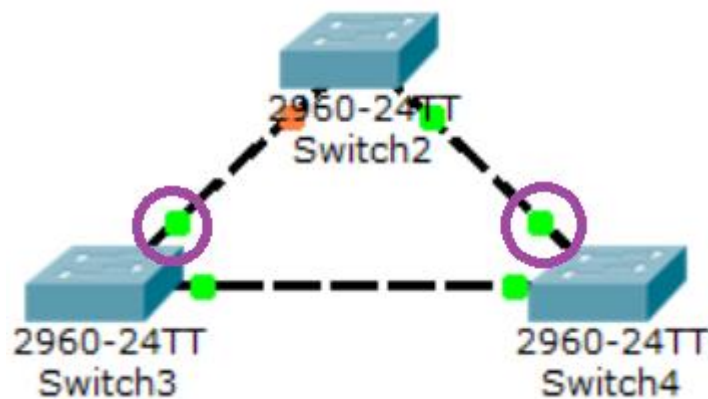


Рисунок 2.6 – Кореневі порти Switch 3 та Switch 4

3) Необхідно здійснити вибір призначеного інтерфейсу(порта). Його вибір залежить від ціни шляху, тобто його обирають на некореновому комутаторі, шлях від якого до кореневого коммутатора має найменшу ціну.

маршруту до такої мережі, він встановлює значення лічильника рівним 1. Отримавши анонс від R2, маршрутизатор R1 заносить маршрут до мережі 172.30.22.0 в свою таблицю маршрутизації і вважає, що цей маршрут є оптимальним, оскільки інших маршрутів у нього немає. У якості вихідного інтерфейсу для нового маршруту R1 використовує S0/0, оскільки анонс був отриманий через нього. В якості адреси наступного транзитного пристрою на маршруті використовує адресу 172.30.1.2, оскільки анонс маршрутизації був отриманий від відправника з цією IP-адресою. З анонсів маршрутів виключаються деякі маршрути для того, щоб виключити кільцеві маршрути і зациклення пакетів. Кільцевий маршрут утворюється коли два або більше маршрутизаторів пересилають один одному пакети по замкнутому шляху при якому пакети не досягають потрібного одержувача. Кільцевий маршрут діятиме до тих пір, поки маршрутизатори в мережі не оновлять свої таблиці маршрутизації. Для уникнення кільцевих маршрутів, маршрутизатори розсилають інформацію про відмови у маршруті зі спеціальною метрикою, рівною нескінченності (для протоколу RIP це значення дорівнює 16). Така розсилка називається коригуванням маршруту. Ще один механізм запобігання кільцевих маршрутів - таймер зберігання інформації. Якщо отримано відкоригований маршрут (з максимальною метрикою), який свідчить про те, що цей маршрут недоступний, запускається таймер для такого маршруту. Стандартне значення таймера зберігання інформації дорівнює 3 хв. До тих пір поки не закінчиться таймер, нова інформація про маршрут не береться пристроєм, але інформація від сусіднього маршрутизатора, який раніше анонсував зниклий маршрут, приймається і обробляється до закінчення таймера зберігання інформації. Приклад мережі і її налаштування з використанням протоколу RIP на рис.2.8:

					<i>КПТР 2017017.01.07 ПЗ</i>	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		27

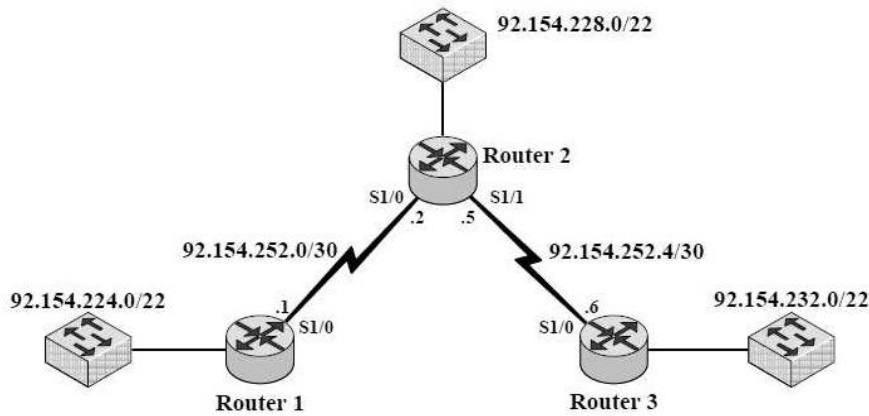


Рисунок 2.8 – Мережа з використанням протоколу RIP

Для налаштування RIP використовується команда `router rip` та команда `network`, яка містить № мережі, підключеної до маршрутизатора та інформацію, яка анонсується у мережу рис. 2.9[4,7]:

```

Physical Config CLI
IOS Command Line Interface

Router1(config)# router rip
Router1(config-router)# network 92.154.224.0
Router1(config-router)# network 92.154.252.0
Router1(config-router)# version 2
Router2(config)# router rip
Router2(config-router)# network 92.154.252.0
Router2(config-router)# network 92.154.252.4
Router2(config-router)# network 92.154.228.0
Router2(config-router)# version 2
Router3(config)# router rip
Router3(config-router)# network 92.154.252.4
Router3(config-router)# network 92.154.232.0
Router3(config-router)# version 2
Router1# show ip route rip
92.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
R 92.154.228.0/22 [120/1] via 92.154.252.2, 00:00:20, Serial1/0
R 92.154.232.0/22 [120/2] via 92.154.252.2, 00:00:20, Serial1/0
R 92.154.252.4/30 [120/1] via 92.154.252.2, 00:00:20, Serial1/0

```

Рисунок 2.9 –Налаштування протоколу RIP на маршрутизаторах

2.4. Протокол маршрутизації OSPF

Протокол OSPF є протоколом маршрутизації, який враховує стан каналів. В цьому класі протоколів в якості метрики використовується вартість маршруту, яка розраховується на основі пропускної здатності кожного каналу на шляху від маршрутизатора до необхідної мережі. Тому процес роботи протоколу OSPF умовно можна розділити на три етапи: виявлення сусідніх маршрутизаторів, обмін базами маршрутів і розрахунок оптимальних маршрутів. Пристрої, підключені до одного каналу і беруть участь в процесі обміну інформацією протоколу OSPF називаються сусідніми маршрутизаторами. Для виявлення OSPF-пристроїв маршрутизатори розсилають багатоадресні Hello-пакети через всі інтерфейси, на яких налаштований протокол OSPF. У запиті міститься наступна інформація: ідентифікатор маршрутизатора-відправника Router ID - RID, ідентифікатор зони OSPF Area ID, Hello-інтервал, інтервал виявлення не працездатності пристрою (dead interval), пріоритет маршрутизатора (router priority), ідентифікатор RID виділеного маршрутизатора (designated router DR), ідентифікатор RID резервного виділеного маршрутизатора (backup designated router BDR) список сусідніх пристроїв, виявлених маршрутизатором-відправником. Кожному маршрутизатору присвоюється унікальний номер - ідентифікатор маршрутизатора RID. Він являє собою 32-бітове число, тому для зручності в якості ідентифікатора використовують IP-адресу. Протоколом автоматично вибирається найстарша IP-адреса з усіх адрес на інтерфейсах пристроїв (в т.ч. віртуальних). Наприклад, маршрутизатор «А» отримує Hello-повідомлення від маршрутизатора «Б». Пристрою «А» потрібно повідомити маршрутизатор «Б» про те, що повідомлення було отримано, тому маршрутизатор «А» додає ідентифікатор RID маршрутизатора «Б» в своє наступне (і всі наступні) Hello-повідомлення. Аналогічно, коли маршрутизатор «Б» отримує Hello-повідомлення, він додасть ідентифікатор RID пристрою «А» в свої наступні Hello-повідомлення. Коли маршрутизатор

					<i>КПТР 2017017.01.07 ПЗ</i>	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		29

виявляє свій ідентифікатор RID у вхідному Hello-повідомленні, він вважає, що з суміжним пристроєм був встановлений двосторонній канал. Після цього маршрутизатори перевіряють базові настройки протоколу один у одного, що містяться в Hello-повідомленнях: IP-адресу, маску підмережі, інтервал розсилки Hello-повідомлень, інтервал виявлення непрацездатності сусіднього пристрою (dead interval), ідентифікатор зони OSPF (area ID) і ін. налаштування повинні збігатися, інакше протокол працювати не буде. Після перевірки, якщо настройки збігаються, маршрутизатори можуть обмінюватися анонсами стану каналів (Link-State Advertisements - LSA). Після встановлення двостороннього каналу маршрутизатори продовжують періодично обмінюватися Hello-повідомленнями. Якщо зв'язок відсутній протягом часу, який визначається dead-інтервалом, то вважається, що зв'язок з сусіднім пристроєм втрачено. Стандартно в протоколі OSPF інтервал розсилки Hello-повідомлень дорівнює 10 с, dead-інтервал - 40 с. В анонсах LSA міститься докладна інформація про топологію мережі. Процес розсилки цих анонсів називається лавинною розсилкою (flooding), при якій маршрутизатори пересилають анонси LSA своїм сусідам, які, в свою чергу, розсилають їх своїм сусідам, і так до тих пір, поки всі пристрої в мережі не отримають інформацію з анонсу. Анонси LSA розсилаються періодично (за замовчуванням один раз в 30 хв). Після закінчення процесу розсилки у всіх маршрутизаторів в домені маршрутизації з'явиться загальна однакова інформація про мережу. Інформація зберігається у вигляді структури, званої базою даних стану каналів link-state database - LSDB. Коли у кожного маршрутизатора в домені маршрутизації є ідентична копія бази LSDB, то використовується технологія протоколів маршрутизації з урахуванням стану каналів. Встановлюються маршрути в таблицю IP-маршрутизації: створюються записи, що містять адресу підмережі, маску, вихідний інтерфейс і адресу наступного транзитного пристрої (next-hop). Для виконання даного завдання використовується алгоритм пошуку першого найкоротшого шляху. Протокол OSPF вибирає маршрут між

					<i>КПТР 2017017.01.07 ПЗ</i>	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		30

маршрутизатором і будь-якої мережею з найменшою вартістю. З кожним інтерфейсом на маршруті пов'язано деяке значення вартості. Вартість всіх інтерфейсів (каналів), через які пролягає шлях до мережі, підсумовується і вибирається шлях, вартість якого мінімальна. Таким чином, кожен маршрутизатор будує маршрути подібно структурі дерева, в корені якої ставить себе. Для настройки протоколу OSPF використовуються команда `router ospf`, яка містить 16-розрядний ідентифікатор процесу від 1 до 65535 і команда `network`, що містить номер мережі, інверсну маску (wildcard mask) і ідентифікатор зони. Розглянемо приклад налаштування протоколу для мережі рис.2.10:

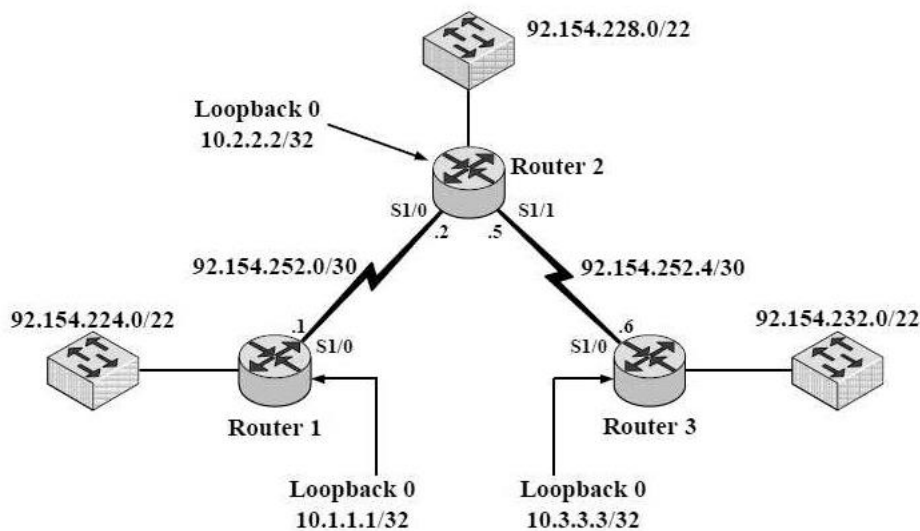


Рисунок 2.10 – Мережа з використанням протоколу OSPF

```

Physical Config CLI
IOS Command Line Interface
Router1(config)# router ospf 1
Router1(config-router)# network 92.154.252.0 0.0.0.3 area 0
Router1(config-router)# network 92.154.224.0 0.0.3.255 area 0
Router2(config)# router ospf 1
Router2(config-router)# network 92.154.252.0 0.0.0.3 area 0
Router2(config-router)# network 92.154.252.4 0.0.0.3 area 0
Router2(config-router)# network 92.154.228.0 0.0.3.255 area 0
Router3(config)# router ospf 1
Router3(config-router)# network 92.154.252.4 0.0.0.3 area 0
Router3(config-router)# network 92.154.232.0 0.0.3.255 area 0
  
```

Рисунок 2.11 – Налаштування протоколу OSPF на маршрутизаторах

Для перегляду списку сусідніх маршрутизаторів на яких налаштований протокол OSPF, використовуємо команду «show ip ospf neighbor».

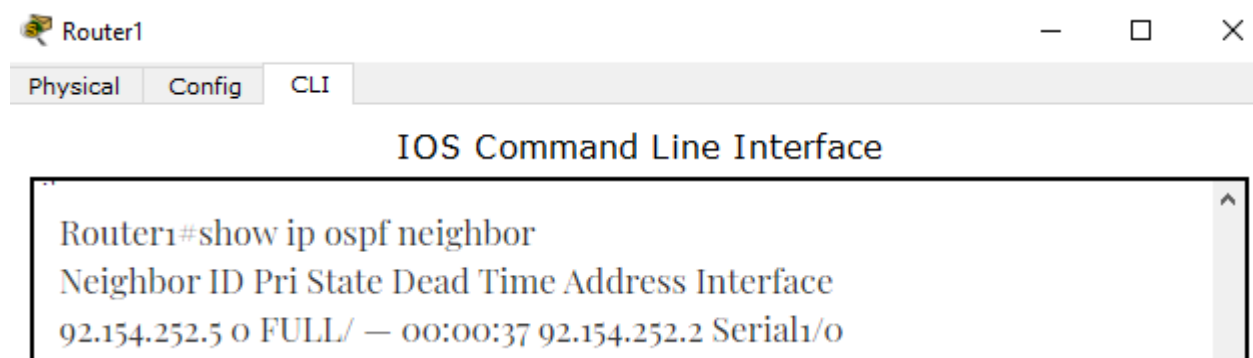


Рисунок 2.11 –Перегляд списку маршрутизаторів

Для функціонування протоколу OSPF важливо, щоб хоча б один інтерфейс маршрутизатора, включений в таблицю маршрутизації протоколу OSPF, повинен перебувати в піднятому (up) стані. В іншому випадку OSPF відключиться і подальше включення можливо буде тільки вручну. Для уникнення такої проблеми в мережі необхідно налаштувати і включити в протокол OSPF віртуальний інтерфейс loopback.

Для настройки інтерфейсу loopback використовується команда interface loopback, після вказується номер віртуального інтерфейсу.

2.5. Використання списків керування доступом ACL

При побудові великої комп'ютерної мережі часто виникає необхідність в фільтрації даних, які рухаються мережею. Зазвичай між будівлями, підрозділами підприємства встановлюють керуючі комутатори, як правило, підвищеної продуктивності. Як приклад розглянемо комутатор фірми D-Link DES-3326SR третього рівня для виконання завдання фільтрації пакетів між портами[4, 5].

Комутатори для обмеження проходження трафіку дозволяють створювати профілі доступу, які вказують йому, які види пакетів приймати, а які відкидати. Прийом пакетів або відмова в прийомі ґрунтується на певних ознаках, таких як адреса джерела, адреса приймача, адреса порту джерела і приймача. За допомогою сформованих списків управління доступом (ACL -

Access Control Lists) профіль управління доступом дає можливість переглядати певні пакети, зазначені в списках ACL.

У комутаторах D-Link існує два основних типи профілів управління доступом: Ethernet і IP. Фільтрація в цих типах профілів може виконуватися на основі MAC-адрес джерела і приймача, VLAN, IP-адрес, номерів портів.

Профілі доступу працюють послідовно, в порядку зростання їх номерів (Profile ID). Пакет перевіряється на відповідність умовам, зазначеним в профілях доступу, починаючи з першого профілю. Якщо профіль підходить, пакет або приймається або відкидається і далі не перевіряється. Якщо ні один профіль не підходить, застосовується політика за замовчуванням, яка дозволяє проходження всього трафіку.

Процес створення профілів доступу ділиться на два етапи:

1. Створення маски профілю доступу: вказується, яку частину або частини кадру перевірятиме комутатор, наприклад IP-адреса призначення або IP-адреса призначення і IP-адреса джерела.

2. Створення правил профілю доступу: вводиться умова, яку комутатор буде використовувати для визначення дій над кадром (прийняти кадр або відкинути).

Розглянемо приклад налаштування списків керування доступом на комутаторі фірми D-Link DES-3326SR третього рівня рис. 2.12:

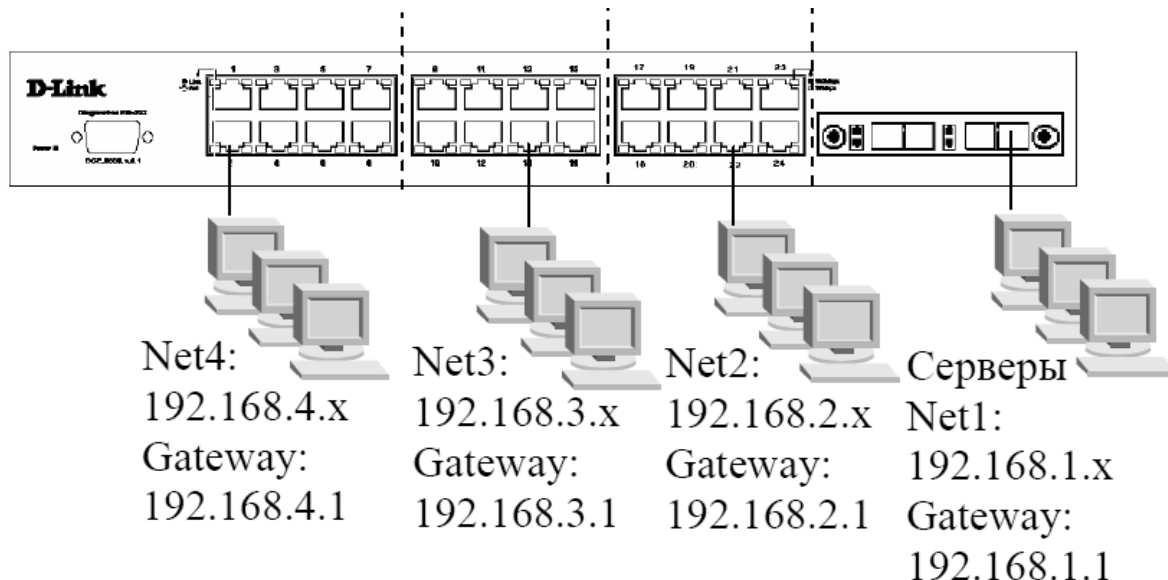


Рисунок 2.12 – Налаштування ALC на DES-3326SR

Дозволити доступ тільки в одну мережу з інших підмереж: підмережа 1 (192.168.1.x) може бути доступною з підмережі 2, підмережі 3, підмережі 4. Підмережа 2, підмережа 3, підмережа 4 не мають доступ один до одного:

Правила:

1. Якщо Dest. IP = 192.168.1.x, то дозволити доступ.
2. Якщо Src. IP = 192.168.1.x, то дозволити доступ.
3. Якщо DestIP = 192.168.2.x і SrcIP = 192.168.2.x, то дозволити доступ.
4. Якщо DestIP = 192.168.3.x і SrcIP = 192.168.3.x, то дозволити доступ.
5. Якщо DestIP = 192.168.4.x і SrcIP = 192.168.4.x, то дозволити доступ.
6. Заборонити все інше, команди:

Дозволити доступ лише до підмережі 192.168.1.x з інших підмереж

```
# create access_profile ip destination_ip_mask 255.255.255.0 permit profile_id 10
# config access_profile profile_id 10 add access_id 11 ip destination_ip 192.168.1.0
```

Дозволити доступ лише з підмережі 192.168.1.x в інші підмережі

```
# create access_profile ip source_ip_mask 255.255.255.0 permit profile_id 20
# config access_profile profile_id 20 add access_id 21 ip source_ip 192.168.1.0
```

Дозволити доступ всередині підмереж 192.168.2.x, 192.168.3.x і 192.168.4.x.

```
# create access_profile ip source_ip_mask 255.255.255.0 destination_ip_mask 255.255.255.0 permit profile_id 30
```

```
# config access_profile profile_id 30 add access_id 31 ip source_ip 192.168.2.0 destination_ip 192.168.2.0
```

```
# config access_profile profile_id 30 add access_id 32 ip source_ip 192.168.3.0 destination_ip 192.168.3.0
```

```
# config access_profile profile_id 30 add access_id 33 ip source_ip 192.168.4.0 destination_ip 192.168.4.0
```

Заборонити все інше.

```
# create access_profile ip source_ip_mask 0.0.0.0 deny profile_id 40
```

```
# config access_profile profile_id 40 add access_id 41 ip source_ip 0.0.0.0
```

Рисунок 2.13 – Налаштування ALC на DES-3326SR

					КПТР 2017017.01.07 ПЗ	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		34

3 МОДЕЛЮВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

3.1. Результати моделювання телекомунікаційної мережі в середовищі Cisco Packet Tracer

Побудуємо модель телекомунікаційної мережі, яка з'єднує за допомогою мережі інтернет два філіали однієї компанії. Фірма має два офіси. В першому офісі знаходиться декілька комп'ютерів і один коммутатор рис. 3.1

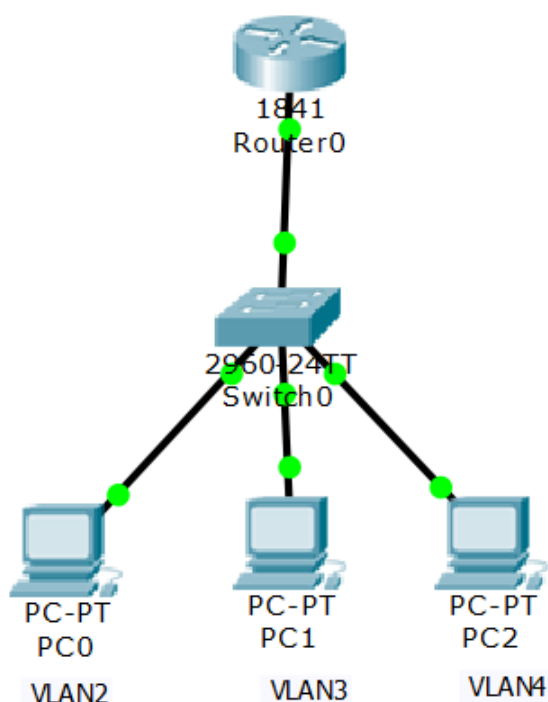


Рисунок 3.1 – Локальна мережа офісу 1

В офісі першої фірми локальний трафік є невеликим і немає виділених серверів, тому немає необхідності в установці коммутатора 3-го рівня. Це буде не рентабельно для такої схеми локальної мережі і її навантаження. Оскільки L3 комутатори досить дорогі. В данному випадку нам вистачить одного маршрутизатора для надання співробітникам фірми доступу у мережу інтернет.

Перейдемо до налаштування мережі офісу 1. Спочатку налаштуємо VLAN. Для цього зайдемо в інтерфейс командної стрічки (CLI) комутатора і зробимо необхідні налаштування. Спочатку створимо віртуальні комп'ютерні мережі і дамо їм імена від VLAN2 до VLAN 4 рис.3.2:

```

Switch0
Physical Config CLI
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name VLAN2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name VLAN3
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name VLAN4
Switch(config-vlan)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
Switch#

```

Рисунок 3.2 – Налаштування VLAN на комутаторі 2960-24TT

Далі необхідно визначити і помістити наші ПК в потрібний сегмент відповідної віртуальної мережі. Комп'ютер ПК0 підключений до інтерфейсу Fa0/1, комп'ютер ПК1 до інтерфейсу Fa0/2, комп'ютер ПК2 до інтерфейсу Fa0/3. Після чого нам необхідно налаштувати trunk-порт, який йде до маршрутизатора 1841, який підключений до порту коммутатора Fa0/4 рис. 3.3.:

```

Switch0
Physical Config CLI
IOS Command Line Interface
Switch(config-if)#int fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#int fastEthernet 0/4
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 2,3,4
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

```

Рисунок 3.3 – Налаштування комутатора для визначення ПК

0/0.4 для яких присвоєні ір-адреси. Для перевірки на ПК0, ПК1, ПК2 пропишемо відповідні ір-адреси для кожної віртуальної мережі. Наприклад для ПК0 це буде адреса, яка відноситься до мережі VLAN2 і.т.д. рис.3.7:

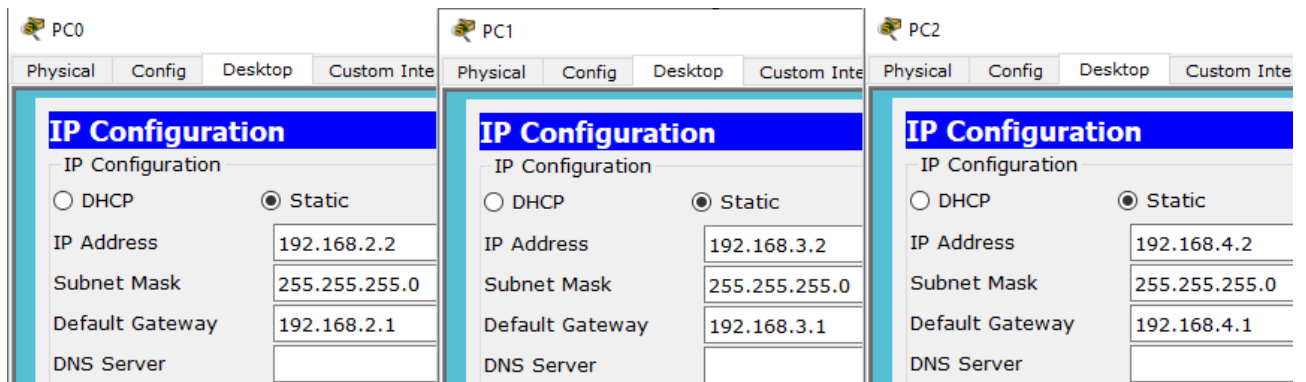


Рисунок 3.7 – Налаштування ПК офісу 1

Для перевірки працездатності мережі перевіримо ping до шлюзу, який знаходиться в його VLAN та сусідні сегменти мережі рис.3.8:

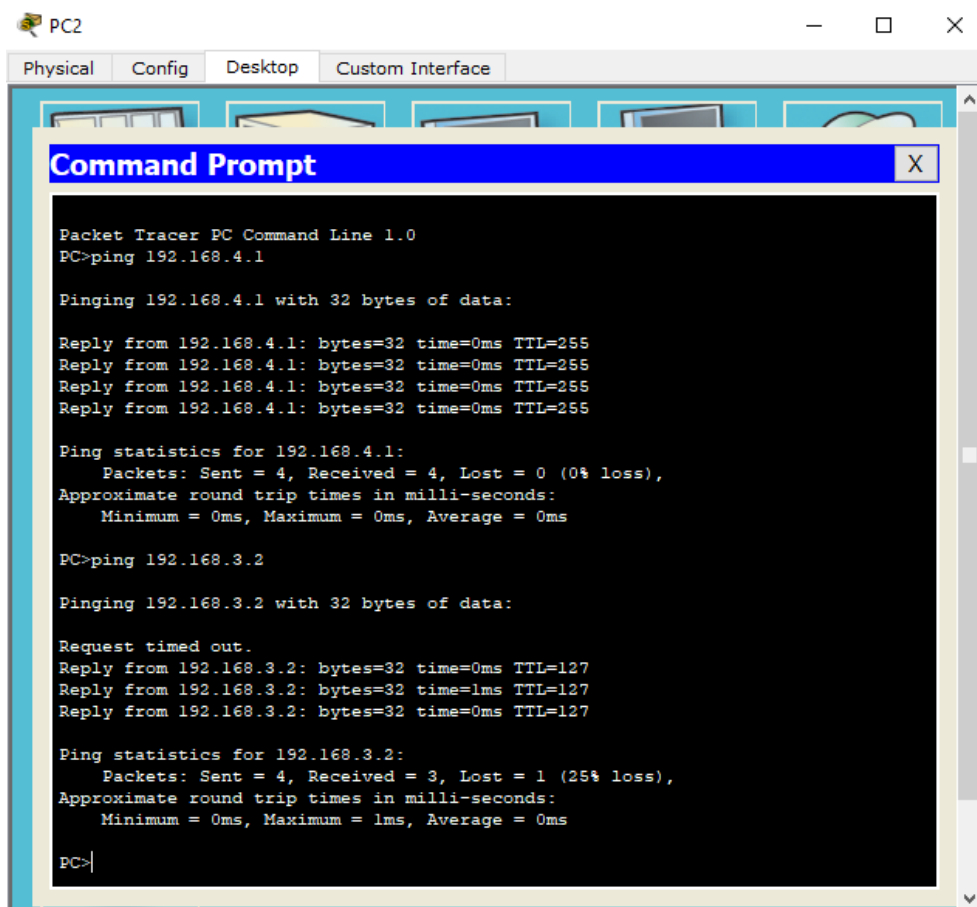


Рисунок 3.8 – Перевірка локальної мережі офісу 1

Таким чином за допомогою маршрутизатора ми організували маршрутизацію трафіка між трьома сегментами мережі без застосування маршрутизуючого коммутатора третього рівня. Даний маршрутизатор також може використовуватись для маршрутизації локального трафіку в мережу інтернет за допомогою технології NAT або звичайної маршрутизації.

Другий офіс фірми має декілька комутаторів рівня доступу до яких підключені до сотні ПК. Крім того в другому офісі знаходяться виділені сервери. Для такої структури мережі локальний трафік є досить великим і потрібна висока пропускна здатність мережі для доступу до локальних серверів. Звичайний маршрутизатор з таким навантаженням не впорається. Для такої структури мережі необхідно використання коммутатора третього рівня, в данному випадку це Cisco 3560-24PS рис. 3.9.:

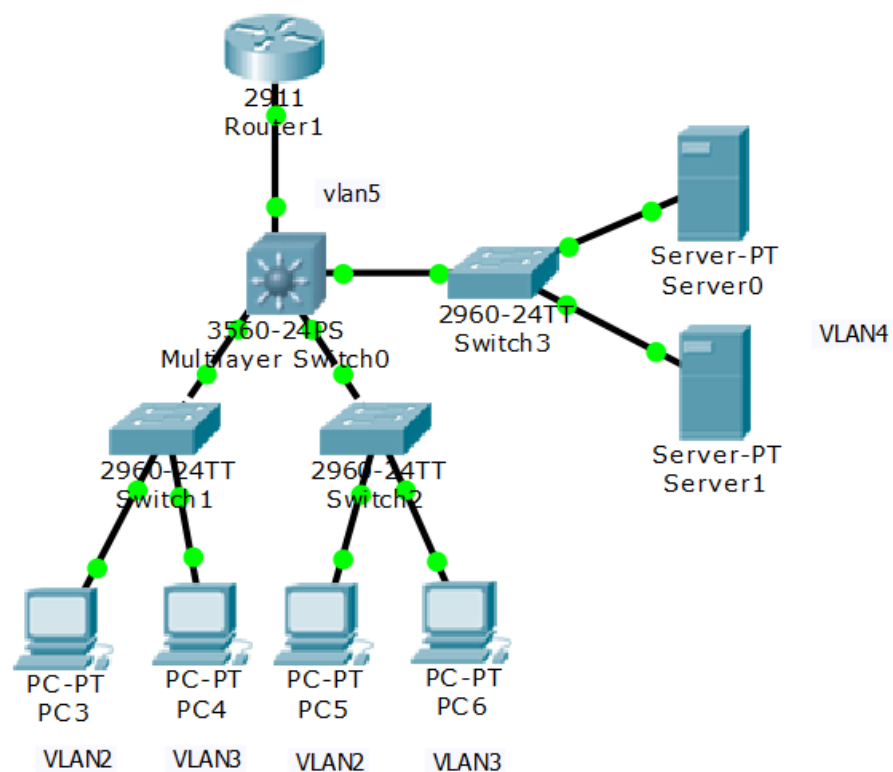


Рисунок 3.9 – Локальна мережа офісу 2

Нехай персональні компютери ПК3 та ПК5 знаходяться в віртуальній мережі №2, а персональні компютери ПК4 та ПК6 знаходяться в віртуальній

Після виконання команди show run ми побачимо , що порт Fa0/1 trunk-порт налаштований на VLAN 2 та VLAN 3 , Fa0/2 trunk-порт налаштований на VLAN 2 та VLAN 3, порт Fa0/3 trunk-порт для підключення виділених серверів VLAN 4. Також на данному комутаторі працюють віртуальні інтерфейси, яким присвоєнні відповідні ір-адреси.

Для перевірки працездатності мережі перевіримо ping до сусідніх сегментів мережі. З комп'ютера ПК3 пропінгуємо компютер ПК5, який знаходиться в тому ж сегменті, також перевіримо сусідній сегмент це компютери ПК4 та ПК6, які знаходяться в VLAN 3 та перевіримо зеднання із серверами рис.3.14:

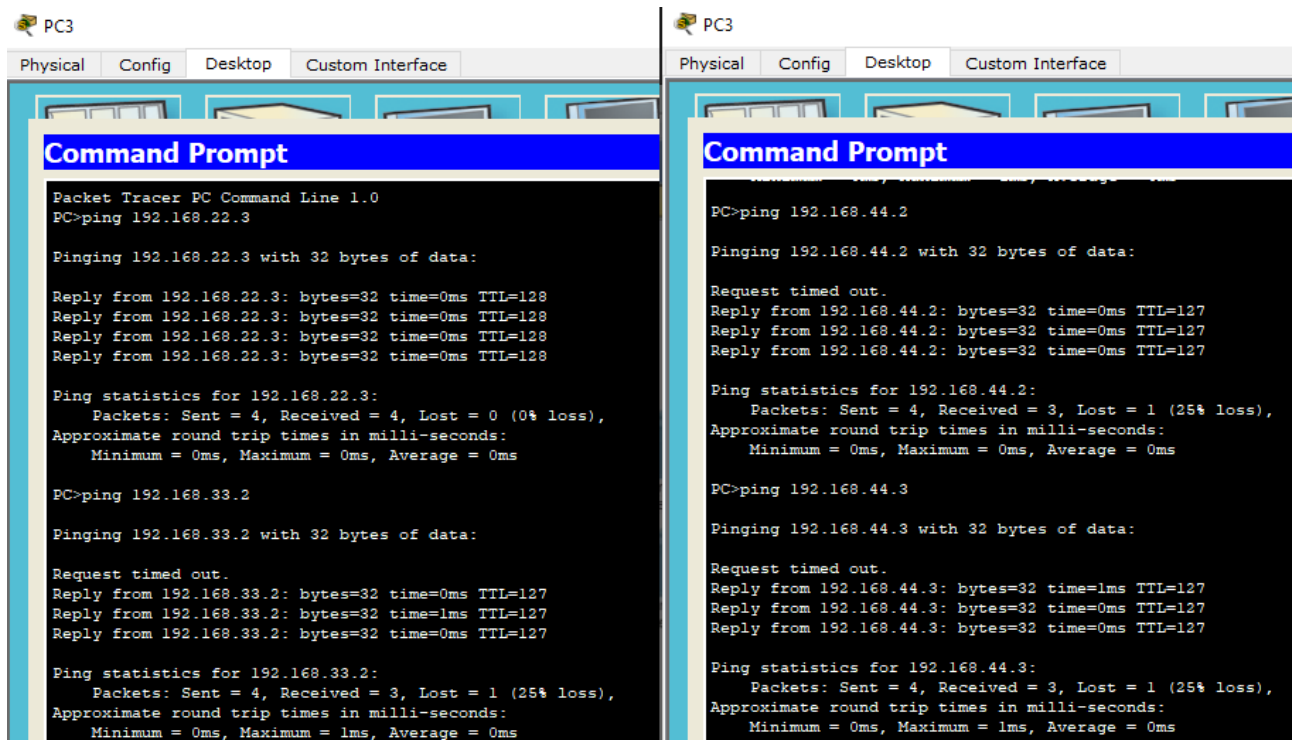


Рисунок 3.14 – Перевірка локальної мережі офісу 2

Як ми бачимо, вся міжмережева взаємодія всередині локальної мережі реалізована на комутаторі Cisco 3560-24PS. Це високопродуктивний коммутатор, його продуктивності цілком вистачить для комфортної роботи користувачів всередині локальної мережі. Але для маршрутизації локального трафіку в мережу Internet потрібен маршрутизатор на якому можна

налаштувати функції мережевого екрану, NAT, VPN і ін. Приступимо до налаштування виходу в мережу Internet. Для цього створимо віртуальну мережу VLAN 5. Для початку налаштуємо комутатор Cisco 3560-24PS створимо на ньому ще одну мережу VLAN 5, аналогічно, як ми робили в попередніх прикладах. Створимо інтерфейс VLAN 5 присвоємо йому ім'я VLAN 5. Підніmemo віртуальний інтерфейс і присвоємо ір-адресу. Порт коммутатора gi0/1 визначимо, як access-порт. Перевіримо налаштування Cisco 3560-24PS.

```

!
interface GigabitEthernet0/1
 switchport access vlan 5
 switchport mode access
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 192.168.22.1 255.255.255.0
!
interface Vlan3
 ip address 192.168.33.1 255.255.255.0
!
interface Vlan4
 ip address 192.168.44.1 255.255.255.0
!
interface Vlan5
 ip address 192.168.55.2 255.255.255.0
!
ip classless
!
ip flow-export version 9

```

Рисунок 3.15 – Створення і налаштування VLAN 5 на Cisco 3560-24PS

Інтерфейс gi0/1 у нас налаштований, як access-порт в VLAN 5, віртуальний інтерфейс VLAN 5 піднятий. Зберігаем дану конфігурацію і переходимо до налаштувань маршрутизатора. Для цього фізичний інтерфейс маршрутизатора gi0/0 піднімаємо, і на нього вішаємо ір-адресу. У нас немає необхідності тут створювати підінтерфейси, оскільки немає додаткових віртуальних мереж. Перевіримо чи пінгується Cisco 3560-24PS з

Для перевірки працездатності мережі перевіримо ping до сусідніх сегментів мережі.

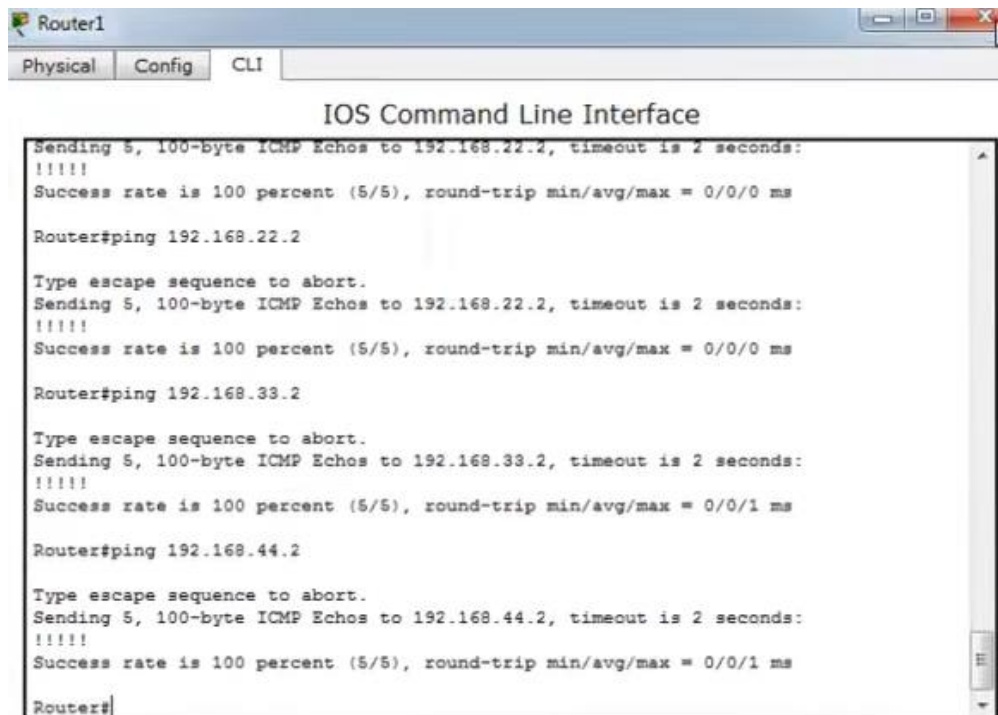


Рисунок 3.18 – Перевірка з'єднання між сегментами офісу 2

Тепер нам необхідно об'єднати два офіси в одну мережу, для цього ми використаємо, ще один маршрутизатор 1841. Ми отримаємо модель корпоративної мережі, яка побудована з використанням технології VLAN рис.3.19

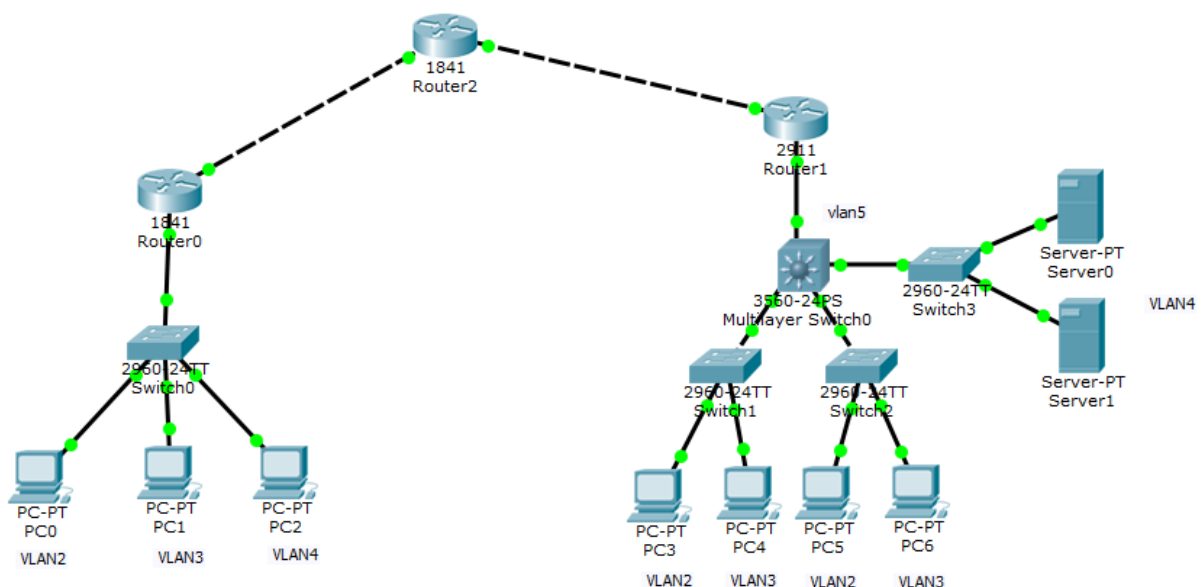
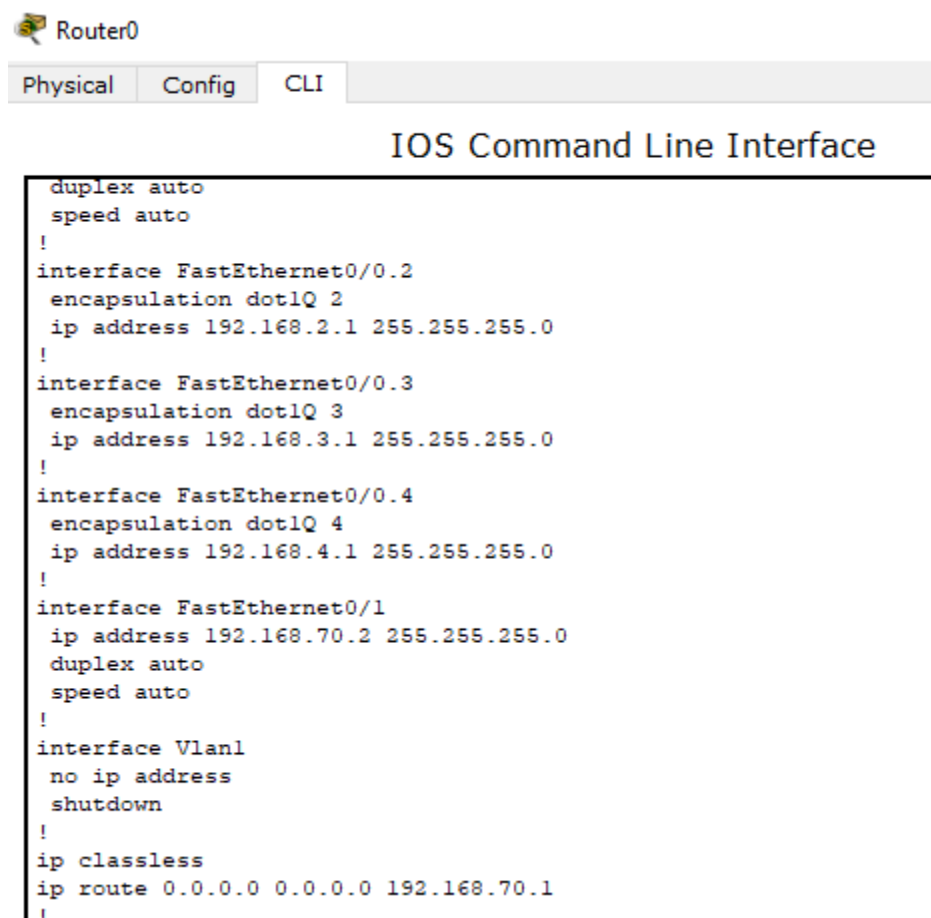


Рисунок 3.19 – Модель телекомунікаційної мережі

Щоб усі пристрої даної мережі могли бачити один одного і обмінюватись даними необхідно налаштувати статичні маршрути на маршрутизаторі 1841 офісу 1, маршрутизаторі 2911 офісу 2, маршрутизаторі 1841, який з'єднає мережі двох офісів та на комутаторі Cisco 3560-24PS. На початку налаштовуються фізичні інтерфейси на маршрутизаторах 0, 1, 2 після з'єднання двох мереж за допомогою маршрутизатора 1841. Налаштування аналогічні тим, що ми виконували вище. Подивимось налаштування маршрутизатора 1841 офісу 1 зайшовши в інтерфейс CLI рис. 3.20:



```
Router0
Physical Config CLI
IOS Command Line Interface

duplex auto
speed auto
!
interface FastEthernet0/0.2
encapsulation dot1Q 2
ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/0.3
encapsulation dot1Q 3
ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/0.4
encapsulation dot1Q 4
ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/1
ip address 192.168.70.2 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.70.1
!
```

Рисунок 3.20 – Налаштування маршрутизатора 0

Як ми бачимо із налаштувань маршрутизатора в ньому прописані статичні маршрути до трьох віртуальних мереж офісу 1 та шлюзом по замовчуванню в мережу офісу 2 є маршрутизатор 2. Далі нам необхідно подивитись налаштування маршрутизатора 2911. Для цього скористаємось командою show run в CLI рис 3.21:

```
Router1
Physical Config CLI
IOS Command Line Interface
!
interface GigabitEthernet0/0
ip address 192.168.55.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.80.2 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.22.0 255.255.255.0 192.168.55.2
ip route 192.168.33.0 255.255.255.0 192.168.55.2
ip route 192.168.44.0 255.255.255.0 192.168.55.2
ip route 0.0.0.0 0.0.0.0 192.168.80.1
!
```

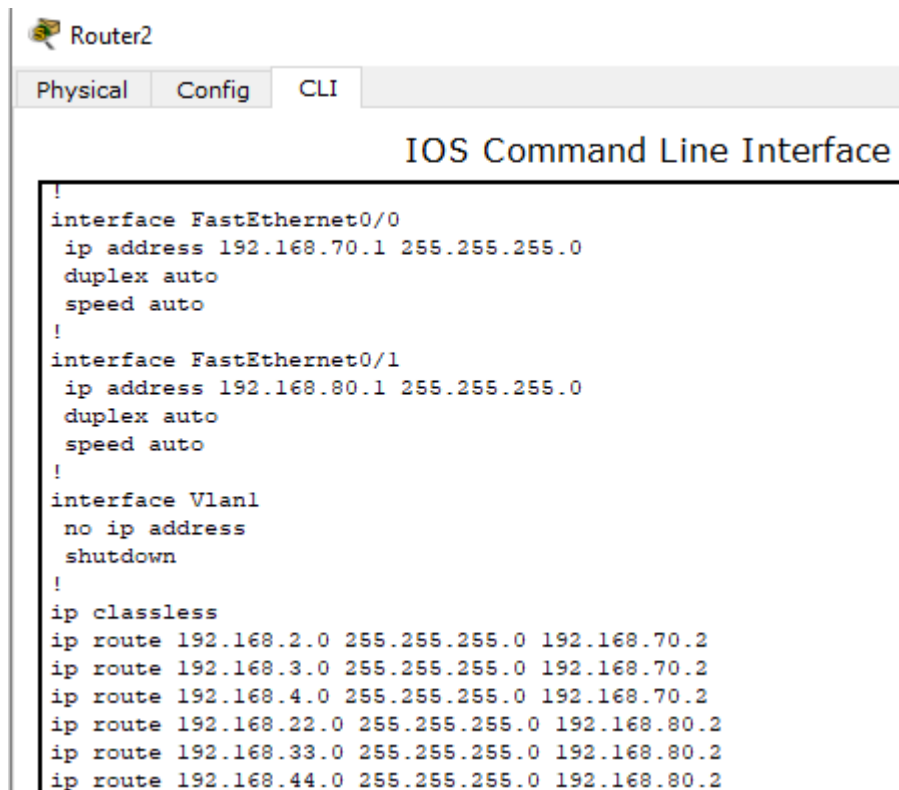
Рисунок 3.21 – Налаштування маршрутизатора 1

Як ми бачимо із налаштувань маршрутизатора в ньому прописані статичні маршрути до трьох віртуальних мереж офісу 2 та шлюзом по замовчуванню в мережу офісу 1 є маршрутизатор 2. А вихід в мережу офісу 2 здійснюється через комутатор Cisco 3560-24PS. Далі нам необхідно подивитись налаштування комутатора Cisco 3560-24PS. Для цього скористаємось командою show run в CLI рис 3.22:

```
Multilayer Switch0
Physical Config CLI
IOS Command Line Interface
shutdown
!
interface Vlan2
ip address 192.168.22.1 255.255.255.0
!
interface Vlan3
ip address 192.168.33.1 255.255.255.0
!
interface Vlan4
ip address 192.168.44.1 255.255.255.0
!
interface Vlan5
ip address 192.168.55.2 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.55.1
!
```

Рисунок 3.22 – Налаштування комутатора Cisco 3560-24PS

Шлюз по замовчуванню для комутатора Cisco 3560-24PS є маршрутизатор 2911. І останній це маршрутизатор 1841, який з'єднує локальні мережі двох офісів рис. 3.23:



```
Router2
Physical Config CLI
IOS Command Line Interface
!
interface FastEthernet0/0
ip address 192.168.70.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.80.1 255.255.255.0
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip classless
ip route 192.168.2.0 255.255.255.0 192.168.70.2
ip route 192.168.3.0 255.255.255.0 192.168.70.2
ip route 192.168.4.0 255.255.255.0 192.168.70.2
ip route 192.168.22.0 255.255.255.0 192.168.80.2
ip route 192.168.33.0 255.255.255.0 192.168.80.2
ip route 192.168.44.0 255.255.255.0 192.168.80.2
```

Рисунок 3.23 – Налаштування маршрутизатора 2

Як ми бачимо в маршрутизатора 1841 підключені два інтерфейси, і в його таблиці маршрутизації прописані статичні маршрути до всіх пристроїв локальних мереж офісу 1 та офісу 2. В результаті перевірки побудованої мережі, всі пристрої бачать один одного і можуть зв'язуватись між собою.

Отже, ми побудували телекомунікаційну мережу фірми рис. 3.19, яка має два офіси використавши в якості обладнання три маршрутизатори на один комутатор третього рівня Cisco 3560-24PS. Пропускної здатності побудованої телекомунікаційної мережі вистачить для підключення великої кількості персональних комп'ютерів, що повністю задовільняє потреби працівників данного підприємства.

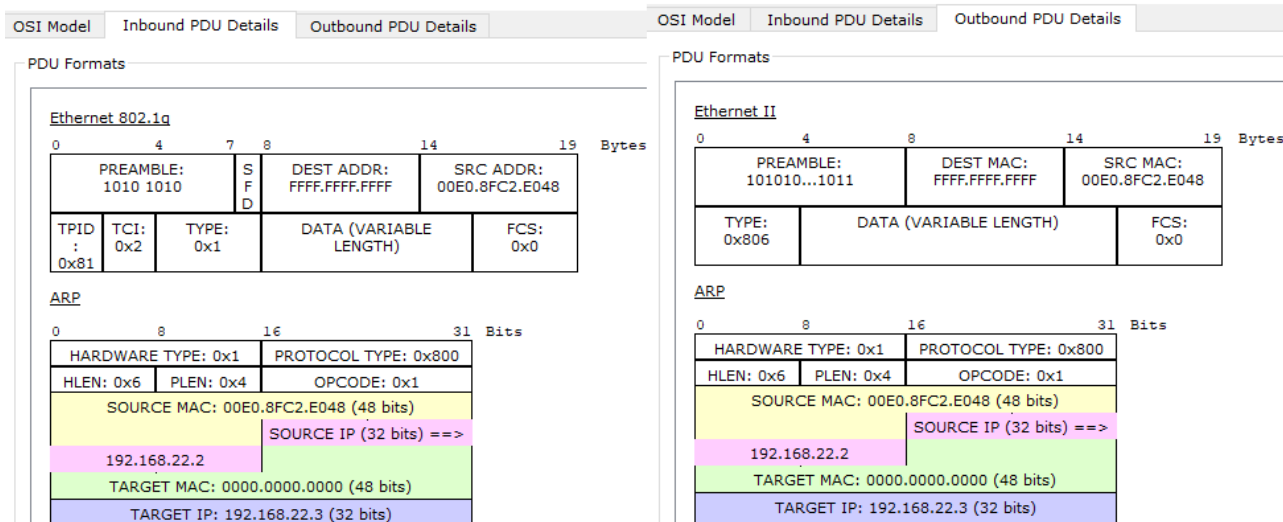


Рисунок 3.26 – Структура пакету на вхідному комутаторі

Можемо зробити висновок – побудована телекомунікаційна мережа працює правильно, згідно теоретичних засад.

Тепер протестуємо просування пакету з однієї віртуальної мережі офісу 1 до іншої. При цьому будуть використовуватись магістральні канали комутаторів. Отже перешлемо пакет з ПК0 VLAN 2 до ПК1 VLAN 3.

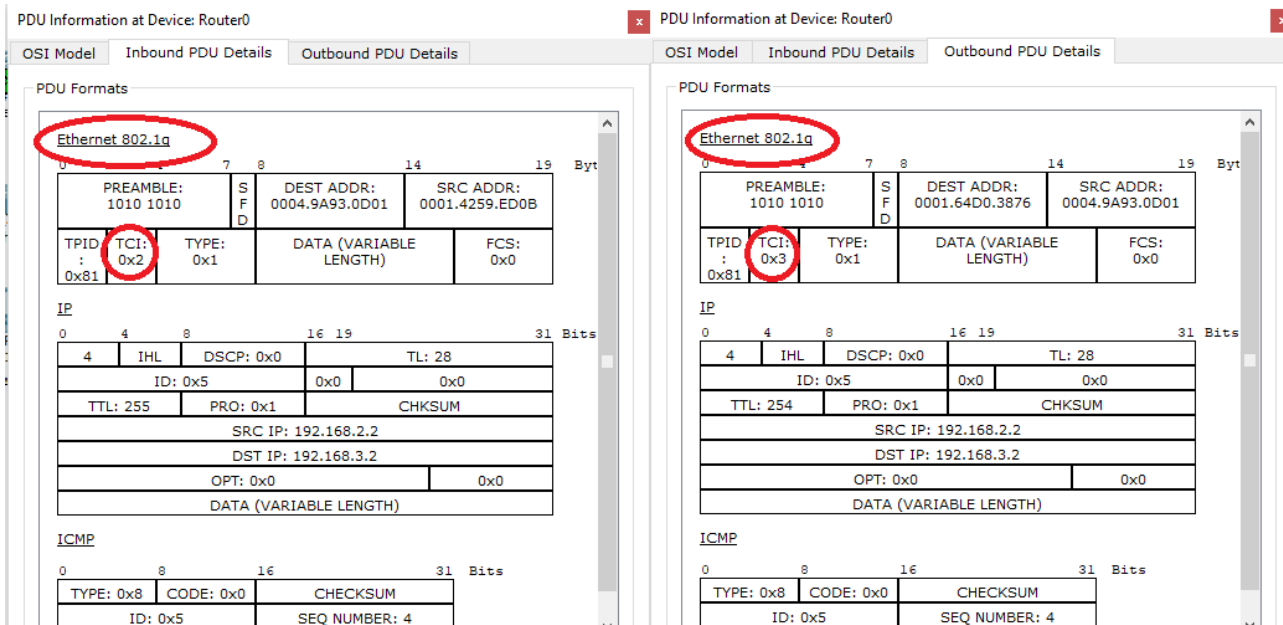


Рисунок 3.27 – Структура пакету на проміжному маршрутизаторі 1841

Дослідимо структуру пакету на проміжному вузлі мережі – на

маршрутизаторі 1841 між двома trunk-каналами. Згідно з теорією на обох вкладках Outbound PDU Details та Inbound PDU Details ми маємо побачити інкапсульований пакет із мітками віртуальних мереж рис.3.26. Так і є ми бачимо інкапсульований пакет Ethernet 802.1Q, але мітки віртуальних мереж будуть різними на Inbound PDU Details мітка VLAN 2 (0x2), а на Outbound PDU Details мітка VLAN 3 (0x3).

Отже, побудована телекомунікаційна мережа повністю робоча, функціонує і сконфігурована правильно.

					<i>КПТР 2017017.01.07 ПЗ</i>	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		53

ВИСНОВКИ

У результаті виконання роботи вирішено інженерно технічне завдання, яке полягало у проектуванні телекомунікаційної мережі з застосуванням маршрутизаторів та маршрутизуючих комутаторів. Для вирішення даного завдання ми розглянули структуру побудови телекомунікаційних мереж та встановили, що найбільш поширеним обладнанням в мережах ТСП / ІР є комутатори і маршрутизатори.

Проаналізувавши існуючі рішення, щодо застосування комутаторів і маршрутизаторів в телекомунікаційних мережах ми виконали наступні завдання:

1. Зробити загальний огляд побудови сучасних телекомунікаційних мереж на базі комутаторів, маршрутизаторів та проаналізувати основні функції та призначення комутаторів. В результаті огляду встановили, що комутатори третього рівня зазвичай швидше і дешевше маршрутизаторів, тому їх використання в локальних мережах дуже привабливо.

2. Зробити аналіз основних типів та протоколів, які використовуються у коммутаторах при побудові телекомунікаційних мереж.

3. Змоделювати спроектовану телекомунікаційну мережу в середовищі Cisco Packet Tracer та протестувати її на предмет розподілу трафіку в даній мережі. Перевірили працездатність мережі на основі тестування мережі в реальному часі та перехопленні пакетів в режимі симуляції.

СПИСОК ЛІТЕРАТУРИ

1. Альтман Е.А. Компьютерные сети на базе оборудования фирмы Cisco./Е.А. Альтман//Омский гос. ун-т путей сообщения. Омск, 2007. 32 с.
2. Альваро Ретана Принципы проектирования корпоративных IP сетей/ Альваро Ретана, Дон Слайс //. Издательство "Вильямс", 2002 г. 368 с.
3. Васин Н.Н. Сети и системы передачи информации на базе коммутаторов и маршрутизаторов. / Н.Н. Васин // Конспект лекций. – Самара: ГОУВПО ПГУТИ, 2010. – 283 с.
4. Учебное пособие: Коммутаторы локальных сетей D-Link. Москва, 2006 – 156 с.
5. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство. М.: Издательский дом «Вильямс», 2005. – 1168 с.
6. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство. М.: Издательский дом «Вильямс», 2006. – 1000 с.
7. Пакет К. Создание масштабируемых сетей CISCO / К. Пакет, Д. Тир// : [пер. с англ.] – М.: Изд. дом “Вильямс”, 2002. – 792 с.
8. Хилл Б. Полный справочник по CISCO / Хилл Б. //: [пер. с англ.] – М. : изд. дом “Вильямс”, 2004. – 1088 с.
9. Тодд Леммл CCNP. Настройка коммутаторов Cisco. Учебное руководство/ Тодд Леммл, Кевин Хейзл// Издано: 2002, М., Лори, 464 стр.
Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNT/CCNA/ICND1/ Одом, Уэнделл, 3-е изд. – Москва, Вильямс, 2015– 668 с.
10. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNT/CCNA/ICND1/ Одом, Уэнделл, 3-е изд. – Москва, Вильямс, 2015– 668 с.

					<i>КПТР 2017017.01.07 ПЗ</i>	Арк.
Зм.	Арк.	№докум.	Підпис	Дата		55

Завідувачу кафедри телекомунікацій
та радіотехніки
д.т.н., професору БОЙКУ Юлію
здобувача вищої освіти
РОЖЕНЮК Роман
ФПКТС, гр. ТР-17-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

25 травня 2021 р.
дата


підпис

Ім'я користувача:
Kafedra telekom_radiotechniki

ID перевірки:
1008314711

Дата перевірки:
16.06.2021 20:03:33 EEST

Тип перевірки:
Doc vs Internet

Дата звіту:
16.06.2021 20:06:41 EEST

ID користувача:
100005656

Назва документа: Бакалаврська робота Роженюк Роман 2021

Кількість сторінок: 53 Кількість слів: 8745 Кількість символів: 66113 Розмір файлу: 1.73 MB ID файлу: 1008381939

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

2.38%
Схожість

Найбільша схожість: 0.38% з Інтернет-джерелом (<https://ua-referat.com/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D>

2.38% Джерела з Інтернету

110

Сторінка 55

Пошук збігів з Бібліотекою не проводився

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи

11

Підозріле форматування

20
сторінок

РІШЕННЯ КАФЕДРИ ТЕЛЕКОМУНІКАЦІЙ ТА РАДІОТЕХНІКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Проектування телекомунікаційної мережі на базі маршрутизуючих комутаторів

Автор: Роженюк Роман Васильович

Спеціальність: 172 Телекомунікації та радіотехніка

Науковий керівник: д.т.н., професор Мясіщев Олександр Анатолійович

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	-
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	-
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	-
5	Інше:	-

Підтвердження: Виявленні запозичення не є плагіатом так як розміщені в розділах, які не описують безпосередньо авторське дослідження (є власні терміни, визначення тощо), складають 2,38% та мають посилання на приведений список літературних джерел.

«16» червня 2021 р.

Науковий керівник

Завідувач кафедрою ТР




Олександр МЯСІЩЕВ

Юлій БОЙКО

РЕЦЕНЗІЯ

на кваліфікаційний проєкт Роженюка Романа Васильовича “Проектування телекомунікаційної мережі на базі маршрутизуючих комутаторів”, за спеціальністю 172 Телекомунікації та радіотехніка

Тема бакалаврської роботи є доволі актуальною. Сучасні тенденції розвитку телекомунікаційних мереж і систем передачі інформації передбачають надання різноманітних послуг, таких як: обмін даними між користувачами, передача аудіо-та відеоінформації по єдиній мультисервісній мережі зв'язку. Для цієї мети створюються мережі нового покоління Next Generation Network - NGN. Передача даних по мережі Інтернет реалізується, в основному, на базі протоколу TCP / IP (Transmission Control Protocol / Internet Protocol - Протокол управління передачею даних / Міжмережєвий протокол). Протокол TCP / IP - це набір протоколів або правил, які були створені, щоб надати можливість комп'ютерам спільно використовувати ресурси мережі. Крім клієнтського обладнання, такого, як стаціонарні комп'ютери та ноутбуки мережа включає в себе досить велику кількість різних службових пристроїв. Службові пристрої створюють мережеву інфраструктуру і управляють потоками даних, надають різні додаткові сервіси, задають різні правила і політики роботи мережі. Найбільш поширеним обладнанням в мережах TCP / IP є комутатори і маршрутизатори.

У представленій бакалаврській роботі викладені результати, що пов'язані застосуванням мережевих протоколів при побудові телекомунікаційних мереж. Показано приклад застосування протоколу STP для вирішення проблем із появою комутаційних петель. Показано використання протоколу динамічної маршрутизації RIP для створення резервних каналів між маршрутизаторами. Також показано використання списків керування доступом ACL для фільтрації даних в локальних мережах. Застосовано технологію VLAN, яка дозволила структурувати мережу. Автором запропоновано використовувати комутатори третього рівня доступу тому, що зазвичай вони швидше і дешевше маршрутизаторів, тому їх використання в локальних мережах дуже привабливо.

До недоліків роботи слід віднести такі зауваження:

1. В роботі не має математичних моделей та розрахунків.
2. Розглянута в третьому розділі спроектована телекомунікаційна мережа є дещо абстрактною, без конкретного впровадження.
3. В роботі містяться помилки стилістичного характеру.

Незважаючи на зазначені вище зауваження та недоліки, робота Роженюка Романа Васильовича є закінченим дослідженням, яке за предметом досліджень, метою, вирішеним завданням, висновками відповідає вимогам до бакалаврських кваліфікаційних робіт за спеціальністю 172 Телекомунікації та радіотехніка.

Результати роботи мають практичну цінність для задач з побудови сучасних телекомунікаційних мереж.

Автор роботи, Роженюк Роман Васильович, заслуговує на оцінку «добре».

к.т.н., доц. кафедри ТМІТ



Мішан В.В.