

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет комп'ютерних наук та технологій

(повне найменування факультету)

Комп'ютерні системи та мереж

(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

бакалавра

(ступінь вищої освіти)

на тему Розробка розподіленої мережі крамниць побутової техніки та
електроніки COMFY

(назва теми)

Виконав: студент 4 курсу, групи КНТ-519

Спеціальності _____

123 – «Комп'ютерна інженерія»

(код і найменування спеціальності)

Освітня програма (спеціалізація) _____

«Комп'ютерні інженерія»

ІВАНОВ О. В.

(ПРИЗВИЩЕ та ініціали)

Керівник _____ КИРИЧЕК Г. Г.

(ПРИЗВИЩЕ та ініціали)

Рецензент _____ САМОЙЛИК С. С.

(ПРИЗВИЩЕ та ініціали)

Міністерство освіти і науки України
Національний університет «Запорізька політехніка»

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

ЗАТВЕРДЖУЮ

Завідувач кафедри КУДЕРМЕТОВ Р. К.

« » 2023 року

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

ІВАНОВА Олега Вадимовича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проекту (роботи) «Розробка розподіленої мережі крамниць побутової техніки та електроніки COMFY»

керівник проекту (роботи) к.т.н. доцент КИРИЧЕК Галина Григорівна

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

затверджені наказом закладу вищої освіти від «24» березня 2023 року № 71

2. Строк подання студентом проекту (роботи) 10 травня 2023 року

3. Вихідні дані до проекту (роботи) Розподілена комп'ютерна мережа крамниць на 100 кінцевих вузлів, 4 віддалених філій, 4 маршрутизаторів та 8 комутатори із використанням технологій Ethernet стандарту 1000BaseFX, VPN із застосуванням протоколу IPsec, технологія передачі даних Frame Relay, списки контролю доступу ACL, використання 4 бездротових точок доступу та технології WiFi стандарту 802.11 ac, динамічної адресації IPv4 та статичної маршрутизації

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

Аналіз технічного завдання

Вибір обладнання та системи моделювання. Налаштування ір адресації

Налаштування додаткових технологій LAN мереж

Налаштування маршрутизації та додаткових технологій WAN мереж

Створення мережевої інфраструктури та прокладання мережі

Варіанти покращення мережі та її робота під час військового стану

Тестування мережі

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Функціональна схема мережі

Структурна схема мережі

Монтажна схема мережі

Карта мережі крамниць

6. Консультанти розділів проекту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-3	КИРИЧЕК Г. Г., к. т. н., доцент		
нормоконтроль	ЩЕРБАК Н.В., ст. викл.		

7. Дата видачі завдання « 23 » лютого 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз технічного завдання	25.03.2023 р.	
2	Вибір обладнання та системи моделювання. Налаштування ір адресації	05.04.2023 р.	
3	Налаштування додаткових технологій LAN мереж	12.04.2023 р.	
4	Налаштування маршрутизації та додаткових технологій WAN мереж	20.04.2023 р.	
5	Створення мережевої інфраструктури та прокладання мережі	26.04.2023 р.	
6	Методи, що до покращення мережі та її робота при військовому стані	2.05.2023 р.	
7	Тестування мережі	08.05.2023 р.	
8	Оформлення графічного матеріалу	12.05.2023 р.	
9	Оформлення пояснювальної записки	17.05.2023 р.	

Студент(ка)


(підпис)

Олег ІВАНОВ

(Ім'я ПРИЗВИЩЕ)

Керівник проекту (роботи)


(підпис)

Галина КИРИЧЕК

(Ім'я ПРИЗВИЩЕ)

РЕФЕРАТ

ПЗ: 66 с., 7 табл., 18 рис., 11 лістингів, 1 додаток, 19 джерел.

IP-АДРЕСАЦІЯ, DHCP, DNS, ACL, FRAMERELAY, VPN (IPsec), КОМП'ЮТЕРНА МЕРЕЖА, ІНТЕРНЕТ ПРИСТРОЇ, ВІДЕОПОСТЕРЕЖЕННЯ, СТАТИЧНА МАРШРУТИЗАЦІЯ, РОБОТА ПРИ ВІЙКОВОМУ СТАНІ

Мета даного проекту – проектування комп'ютерної мережі крамниць побутової техніки та електроніки «COMFY» з віддаленими філіями по місту Запоріжжя, яка б могла працювати в сучасних умовах. Об'єкт розробки – процес проектування комп'ютерної мережі «COMFY» з віддаленими філіями.

Перший розділ присвячено проектуванню мережі зі створенням відповідної топології, де обирається, аналізується та розміщується необхідне обладнання яке використовуватися.

Другий розділ присвячено вибору обладнання, налаштуванню пристроїв, де створюються відповідні підмережі та їх розподіл, налаштовуються інтерфейси на пристроях, а також налаштовується DHCP для динамічного розподілу IP адрес.

Третій розділ визначає додаткові технології з налаштуванням DNS серверу, а також з розробкою ACL списки фільтрації трафіку, для того щоб обмежити доступ демонстраційних моделі до інших пристроїв.

Четвертий розділ присвячений налаштуванню статичної маршрутизації, налаштуванню технологія передачі даних FrameRelay та VPN(IPsec), який дасть можливість передачі даних в зашифрованому режимі .

В п'ятому розділі описані створення мережевої інфраструктури та прокладання мережі.

Шостий розділ присвячений можливостям покращення мережі на майбутнє та як крамниць працюють при військовому стані.

В сьомому розділі представлені результати тестування мережі всіх функцій.

ЗМІСТ

Вступ.....	7
1 Аналіз технічного завдання.....	8
1.1 Опис предметної області	8
1.2 Постановка завдання.....	9
1.3 Завдання до роботи. Розробка функціональної, структурної та монтажної схеми	11
2 Вибір обладнання та системи моделювання. Налаштування ір адресації	14
2.1 Система моделювання	14
2.2 Вибір обладнання	15
2.3 Створення підмереж.....	17
2.4 Налаштування інтерфейсів.....	20
2.5 Налаштування динамічної конфігурації DHCP та статичної конфігурації для керуючих пристроїв та серверів.	23
3 Налаштування додаткових технологій LAN мереж	27
3.1 Налаштування VLAN.....	27
3.2 Налаштування DNS.....	32
3.3 Налаштування ACL.....	34
4 Налаштування маршрутизації та додаткових технологій WAN мереж	37
4.1 Налаштування статичної маршрутизації	37
4.2 Налаштування IPsec VPN	41
4.3 Налаштування Frame-Relay.....	44
5 Створення мережевої інфраструктури та прокладання мережі	48
6 Варіанти покращення мережі та її робота під час військового стану	50
6.1 Робота під час військового стану	52
7 Тестування мережі	54
7.1 Тестування всередині підмереж.	54
7.3 Тестування LAN	55

7.2 Тестування WAN.....	56
Висновки	59
Перелік джерел посилання	61
Додаток А.....	63
Перелік графічних матеріалів:	
Креслення 1 — Функціональна схема мережі	
Креслення 2 — Структурна схема мережі	
Креслення 3 — Монтажна схема мережі	
Плакат 1 — Карта мережі крамниць	

ВСТУП

COMFY є українською мережею магазинів побутової техніки та електроніки, заснованою у 2005 році. Сьогодні це одна з провідних компаній в Україні в галузі роздрібної торгівлі побутовою технікою та електронікою.

З даних на 2021 рік ця мережа налічує в Україні більше ніж 200 магазинами, а також входить до топ-5 найбільших онлайн-магазинів в країні згідно з даними ринкових досліджень. Компанія пропонує широкий асортимент товарів[1].

Крім того, COMFY має розвинуту інфраструктуру доставки товарів та сервісний центр для надання післяпродажного обслуговування своїм клієнтам. Мережа крамниць включає різноманітні формати торговельних точок, такі як гіпермаркети, супермаркети та магазини в ТРЦ. Крім того, є окремі магазини-шоуруми, де клієнти можуть ознайомитися зі свіжим асортиментом та отримати консультацію від фахівців.

В місті Запоріжжя 4 розташувань крамниць «COMFY». Оскільки застосовуватися багато комп'ютерів, ноутбуків, маршрутизаторів та іншого, доцільно створення розподіленої комп'ютерної мережі, яка мати велику актуальність у контексті ефективного функціонування крамниць, тому що вона дозволяє об'єднати їх та підключити до серверів, де зберігається інформація про техніку. Це забезпечує зручний доступ працівникам до інформації про товари, та використовувати спільні ресурси.

Для підвищення безпеки та ефективного використання ресурсів застосовується статична маршрутизація. Крім того, налаштований DNS-сервер для транслявання імені сайту, а не його IP-адреси. Між філіями мережами також налаштований VPN (IPSec), що дозволяє прямо підключатися до потрібної IP-мережі з шифруванням даних. З'єднання філій між собою проходить через інтернет за допомогою Frame Relay.

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Опис предметної області

В Україні завжди були популярні магазини побутової техніки, де люди могли зайти, подивитись, спробувати та отримати консультацію про товар, який їм сподобався. Мережа крамниць COMFY в цій галузі є однією з найбільших. Компанія пропонує широкий асортимент товарів, включаючи в себе бітову техніку для приготування їжі, пральні та посудомийні машини, пилососи, електроніку, таку як комп'ютери, ноутбуки, планшети, смартфони, телевізори, аудіо- та відеотехніку, комплектуючі та периферію для комп'ютерів та ноутбуків, фото- та відеотехніку, кліматичне обладнання, таке як кондиціонери, обігрівачі та вентилятори.

COMFY пропонує своїм клієнтам товари від провідних світових виробників, таких як Apple, Samsung, LG, Sony, Bosch, Electrolux, Philips та інші. Крім того, в магазинах COMFY можна придбати власні брендові товари компанії.

На сьогоднішній день все ж все більше і більше людей переходять на онлайн покупку де також є докладний опис товару та для замовлення треба зробити лише кілька кліків миші. Але ж перевагою крамниць все ще залишається можливість прийти, а побачити на власні очі товар та протестувати його та порівняти, аби точно впевнитись у виборі. Також не доведеться чекати доставку, та можна відразу забрати товар.

Для того щоб ці переваги були зручними потрібно розробити велику мережу. Зараз, компанії будь-якого розміру можуть скористатися можливостями мережі бізнес-класу. Достатньо дослідити наявні можливості, виконати кілька простих кроків і налаштувати мережеву інфраструктуру, яка забезпечить підприємству низку вигод - від підвищення продуктивності до поліпшення рівня обслуговування клієнтів.

Основне завдання, це створення комп'ютерної мережі, в якій знаходитимуться багато різних пристроїв, які виконують різні, або ж спільні функції та взаємодіятимуть між собою та мати доступ один до одного. Це

забезпечить швидкий та зручний доступ, як для працівників мережі, так і для покупців, які користуватимуться пристроями доступних для них.

Створення даної мережі надає працівникам можливість мати доступ до повної інформації про товари такі як: місце розташування по, тип, кількість, марку, назву а також до функціоналу демонстративних моделей.

1.2 Постановка завдання

В даній схемі спроектована мережа для чотирьох супермаркетів, які взаємодіятимуть між собою через мережу інтернет.

Надзвичайні можливості мережі Інтернет щодо обміну інформацією базуються на принципі пакетного передавання. Цей принцип полягає в тому, що дані розділяються на маленькі порції, відомі як пакети, і пересилаються мережею від відправника до одержувача. Мережні пристрої, такі як маршрутизатори та комутатори, відіграють ключову роль у забезпеченні транспортування даних. Вони є основою не лише Інтернету, а й інших комп'ютерних мереж.

Завдяки маршрутизаторам та комутаторам пристрої, наприклад, ПК, можуть обмінюватися даними з іншими пристроями, такими як інші ПК або поштовий сервер, незалежно від того, чи знаходяться вони у тій самій будівлі або на великій відстані один від одного [2]. Для забезпечення швидкого та зручного з'єднання між філіями, навіть при великих відстанях, може використовуватися технологія Frame Relay. Ця технологія дозволяє забезпечити швидке з'єднання навіть по при великі відстані, що представлено на топографічній карті (рис. 1.1).

Таблиця 1.1 – Конфігурація мережі

Пристр роїв	Кількіс ть мереж	Сервер ів	Стандарти локальних мереж	Мережеве обладнанн я	Фізичне середовище	Типи IP адресац ії
100	4	2	1000BaseSX Wi-Fi	Switch	Оптичний кабель, безпроводне	Динаміч на

На робочу область Cisco Packet Tracer, було перенесено:

- 66 PC-PT (кожен з яких був обладнаний модулем PT-HOST-NM-1FGE);
- 32Laptop-PT (кожен з яких був обладнаний модулем WPC300N);
- 2 сервер Server-PT (обладнаний модулем PT-HOST-NM-1FGE);
- 8 комутаторів Switch-PT (3 7 встановлюваними модулями PT-SWITCH-NM-1FGE, та 1 PT-SWITCH-NM-1CGE);
- 4 маршрутизатора 1941 (з встановленим модулем HWIC-2T);
- 4 Wi-Fi маршрутизатора Access Point PT.

1.3 Завдання до роботи. Розробка функціональної, структурної та монтажною схеми

Після проведення аналізу поставленого завдання, визначили необхідні кроки для проектування комп'ютерної мережі. У кожному кранниці необхідно встановити по два комутатору, один з яких застосовується для проведення відеоспостереження, а інший для демонстративних моделей, щоб підключити більше пристроїв до мережі, до другого комутатора також підключена бездротовий Wi-Fi маршрутизатор та по одному маршрутизатору, через який і організовано локальну мережу філії. В середині філії комп'ютери\пристрої з комутатором з'єднуватися за допомогою оптичного кабелю. Пристрої повинні бути розміщені згідно з технічним завданням, з мінімумом 16 пристроїв в на кожному філію (не враховуючи відеокамери). В кожній підмережі до комутатора підключено 7 - 8

пристроїв, деякі з яких розбиті на VLAN та з встановленим ALC режимом аби обмежити небажаний доступ, до комутатора також під'єднана бездротова точка Access Point, до якої теж підключено 8 пристроїв, які всі знаходяться в одній мережі. Дві з філій матимуть встановлені сервери, до якого зможуть звертатись всі підключені пристрої. Структурну, функціональну та монтажну схему представлена на рисунку 1.2, 1.3 та 1.4

Виходячи з обраних технологій, які нам знадобляться для побудови мережі та їх кількість, треба обрати систему моделювання в якій саме ця мережа спроектована та мережеве обладнання, яке задовольнить всі потреби пристроїв в мережі. Після побудови мережі відразу треба зробити її працездатною задавши налаштування LAN конфігурації та WAN маршрутизації, після чого вже налаштовувати інші технології. Після того як мереже вже повністю спроектована, потрібно провести повне її тестування, аби потім уникнути нештатних ситуацій.

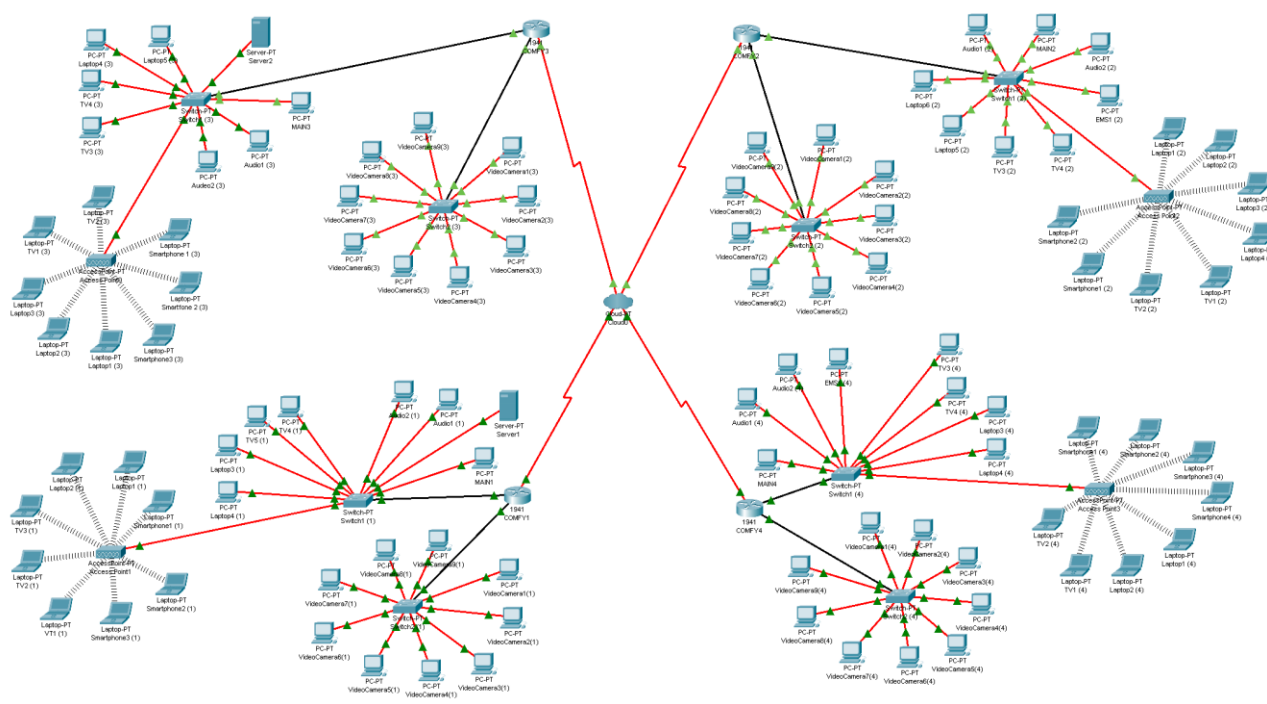


Рисунок 1.2 – Функціональна схема мережі

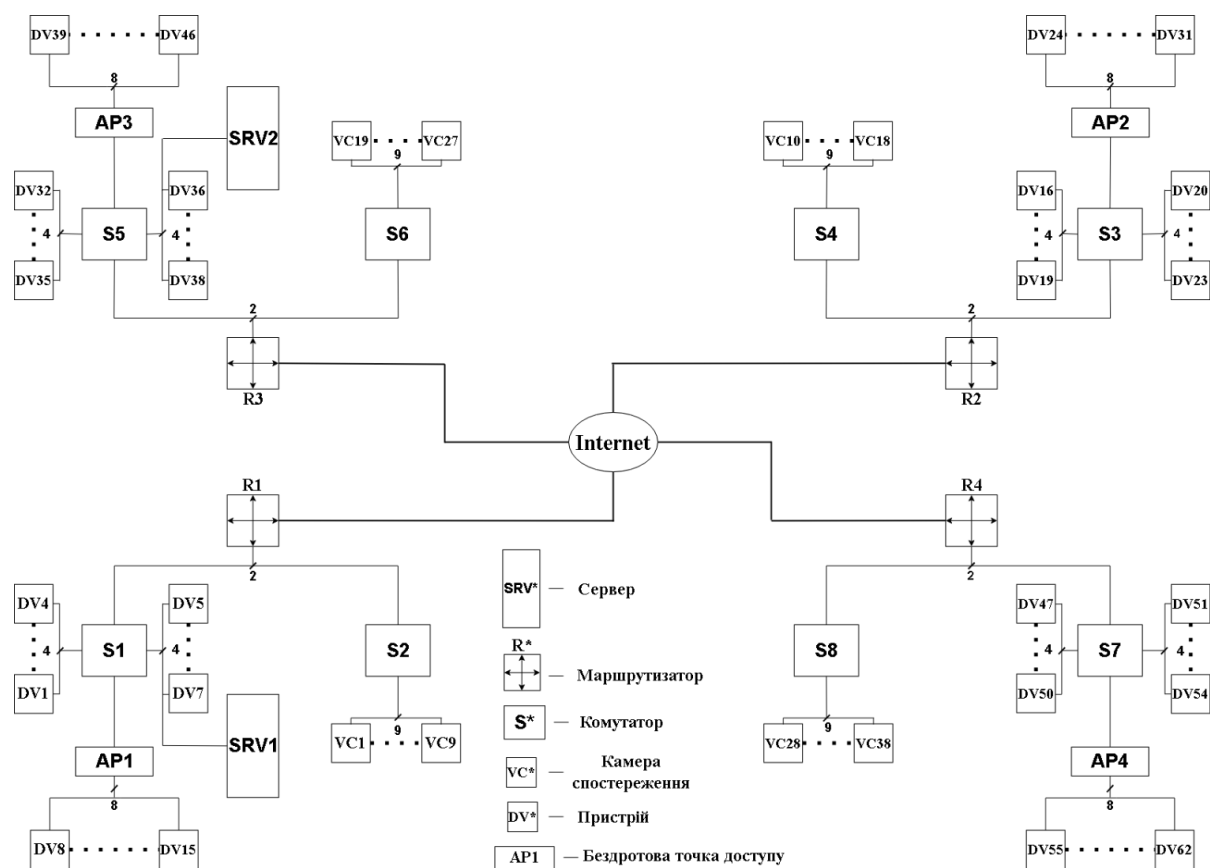


Рисунок 1.3 – Структурна схема мережі

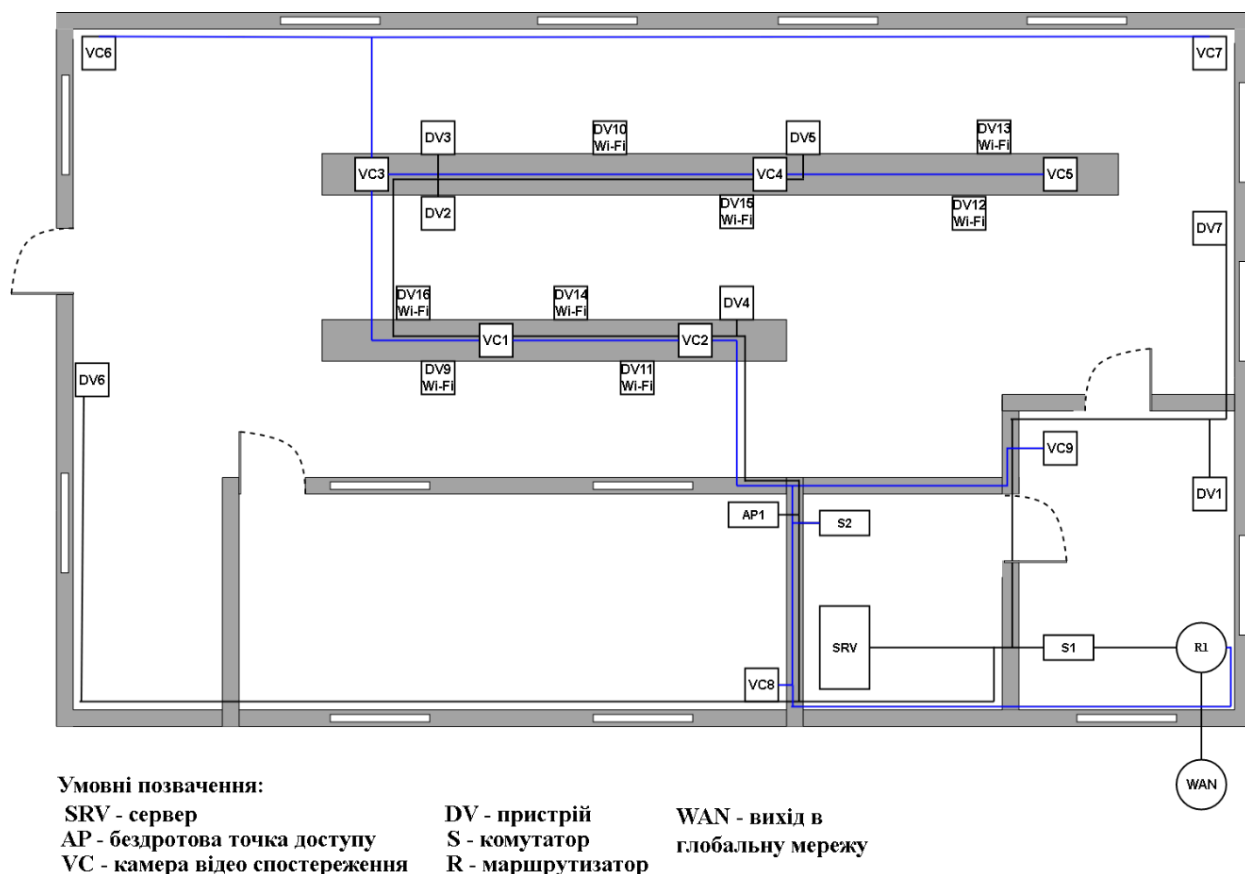


Рисунок 1.4 – Монтажна схема

2 ВИБІР ОБЛАДНАННЯ ТА СИСТЕМИ МОДЕЛЮВАННЯ. НАЛАШТУВАННЯ IP АДРЕСАЦІЇ

2.1 Система моделювання

Щоб спроектувати модель будь якої мережі існують багато систем моделювання як то: Cisco Packet Tracer, GNS3 (Graphical Network Simulator 3), OPNET (Riverbed Modeler), ns-3 (Network Simulator 3), OMNeT++, NetSim, та навіть MATLAB/Simulink. Але дана мережа буде побудована на першій, Cisco Packet Tracer.

Вибір цієї системи зумовлений тим, що по-перше сама компанія Cisco, завдяки своїй широкій продуктивній лінійці та глибокому технічному досвіду, вважається одним з провідних гравців у галузі мережевих технологій, вона спеціалізується на розробці, виробництві та постачанні мережевих обладнань, програмного забезпечення та послуг для комунікаційних та інформаційних технологій. Компанія Cisco також надає послуги консультування, підтримки та навчання, спрямовані на оптимізацію мережевих рішень та підтримку клієнтів у розвитку їхньої інфраструктури. Їхній програмний пристрій фактично теж є таким, маючи в собі великий вибір варіантів побудування мережі.

Cisco Packet Tracer дозволяє створювати віртуальні мережі, підключати різні мережеві пристрої, такі як маршрутизатори, комутатори, сервери, ПК і бездротові пристрої, та налаштовувати їх параметри і взаємодію. Він надає графічний інтерфейс, що спрощує процес створення мережевої топології та налаштування пристроїв. Завдяки графічному інтерфейсу та великому вибору наявних пристроїв, є можливість створювати реалістичні моделі мереж і проводити експерименти з різними сценаріями. Це дозволяє мережевим спеціалістам та студентам перевірити ефективність рішень, виявити можливі проблеми та знайти оптимальні конфігурації для реальних мережевих середовищ.

За його можна виконувати різні завдання, такі як налагодження мережевого з'єднання, налаштування маршрутизації, настройка безпеки мережі, аналіз роботи

мережі та багато іншого. Він також надає можливість створювати сценарії, проводити експерименти та спостерігати за взаємодією пристроїв у віртуальному середовищі.

Cisco Packet Tracer підтримує інтеграцію з іншими платформами та сервісами Cisco, такими як Cisco Networking Academy, що робить його цілком сумісним з освітніми програмами, курсами та матеріалами, розробленими компанією Cisco. Це створює можливості для інтерактивного навчання та розвитку навичок в мережевому середовищі.

Крім того, надає можливість створювати складні сценарії та симулювати реальні умови роботи мережі. Це дозволяє проводити тестування, виявляти уразливості та ризики, а також вивчати реакцію мережі на зміни конфігурацій та обмежень. Все це сприяє підвищенню ефективності, надійності та безпеки мережевих систем.

Маючи в собі всі технології та обладнання для цього проекту, Cisco Packet Tracer є одним за найкращим вибором системи моделювання.

2.2 Вибір обладнання

При виборі обладнання найголовнішим, що вплине на працездатність мережі, це вибір саме мережевого обладнання так як від нього залежить швидкість передачі інформації, можливість становлення додаткових функцій та розширення мережі на майбутнє.

Так, для побудування цієї мережі, найкращим варіантом є маршрутизатор Cisco 1941/K9 від серії 1900 ISR G2 (Integrated Services Router Generation 2). Покращена архітектура ISR G2 забезпечує покращену підтримку мультимедійних капотів та медіа, віртуалізацію, підвищення ефективності та продуктивності за допомогою багатоядерних, 1Gb LAN/WAN гігабітних роз'ємів з покращеним POE та контролем енергоспоживання. Cisco 1900 ISR G2 Router - лінійка інтегрованих

маршрутизаторів послуг (ISR), призначених для малого бізнесу та віддалених відділень. Він пропонує широкий спектр функцій і переваг, включаючи:

- розширена підтримка мультимедійних додатків та медіа;
- підтримка віртуалізації;
- підвищення ефективності та продуктивності завдяки багатоядерним процесорам;
- поліпшення POE і управління живленням;
- віртуальні додатки;
- безпечні операції команд;
- широкий спектр високопродуктивних з'єднань WAN;
- компактний форм-фактор;
- підтримка модулів інтегрованих послуг (ICM);
- зворотна сумісність з модулями попереднього покоління;
- підтримка мереж VPN;
- підтримка бездротових з'єднань.

Cisco 1941/K9 маршрутизатор є потужним і універсальним рішенням для середнього бізнесу і віддалених відділень. Він пропонує широкий спектр функцій та переваг, які можуть допомогти бізнесу підвищити продуктивність мережі, безпеку та продуктивність. Ця модель є не настільки потужна як маршрутизатори серії 2900, та має менше інтерфейсів, але вона і дешевша, та повністю покриває потреби мережі.

Серед комутаторів фактично можна обрати Cisco WS-C2960-8TC-S: Комутатори Cisco Catalyst 2960 мають ряд інтелектуальних функцій, включаючи можливість створення складних списків керування доступом і розширену безпеку. Вони також підтримують комбіновані гігабітні аплінки, що означає, що можна використовувати як мідний Ethernet зі швидкістю 10/100/1000BASE-T, так і SFP-модуль для переходу в інше середовище, наприклад Cisco 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 100BASE-FX, 100BASE-LX, CWDM SFP.

Крім того, пристрої Catalyst 2960 підтримують QoS, можливість обмеження швидкості передачі даних (Rate Limiting), ACL (на базі MAC- або IP-адрес, портів UDP/TCP) і multicast-сервіси. Вони також забезпечують можливість регулювання швидкості передачі на кожному порту з кроком 64 Кбіт, а також можливість створення поєднань (Link Aggregation) для швидкісного з'єднання між комутаторами та серверами.

Цей 8-портовий керований комутатор є хорошим варіантом для невеликих мереж з більшою кількістю пристроїв або пристроїв, які вимагають більшої пропускної здатності. Він пропонує більш широкий спектр функцій та опцій, ніж некерований комутатор, наприклад, можливість налаштування VLAN, QoS та безпеки портів. Для нашої мережі використовується комутатори мінімум на 8 оптичних портів. Це зумовлено тим, що в мережі підключені демонстраційні товари, такі як телефони, ноутбуки та телевізори, щоб забезпечити якісне зображення та передачу всіх можливостей пристрою.

2.3 Створення підмереж

В створенні локальних та глобальних мереж, в даному проекті, використовуються такі IP-адреси, 192.168.1.0/24 – для локальних мереж, 193.169.1.0/24 – для глобальних мереж. Для більш ефективного використання простору адрес IP-мережі за допомогою маски підмережі можуть бути розбиті на більш дрібні підмережі (subnetting) або об'єднані в більш великі мережі (supernetting) [3].

Маска мережі визначає діапазон IP-адрес, які призначені для використання в мережі. Її можна представити у двох форматах: десятковому та бінарному. Для більшої зручності та ефективності мережі маску мережі часто розбивають на підмережі.

Розбивання маски мережі на підмережі дозволяє розділити мережу на менші сегменти, кожен з яких може мати свій власний діапазон IP-адрес. Це дозволяє ефективніше використовувати доступні адреси, зменшує розмір таблиць маршрутизації та полегшує управління мережею.

Також, розбивання мережі на підмережі дозволяє забезпечити кращу безпеку мережі, використовуючи маршрутизатори та брандмауери для контролю доступу до різних сегментів мережі та захисту їх від зовнішніх загроз.

Можна виділити переваги використання підмереж в приватній мережі:

- поділ великої IP-мережі на підмережі дозволяє зменшити обсяг широкомовного трафіку, так як маршрутизатори не передають широкомовні пакети;
- об'єднання невеликих мереж в більші мережі дозволяє збільшити адресний простір за допомогою мереж нижчого класу;
- зміна топології приватної мережі не впливає на таблиці маршрутизації в мережі Інтернет, тому що зберігається тільки маршрут з загальним номером мережі;
- глобальні таблиці маршрутизації в мережі Інтернет не зростають в розмірі;
- адміністратор може створювати нові підмережі без необхідності отримання нових номерів мереж;

Візьмемо спочатку LAN мережу, 192.168.1.0/24, перші три октети адреси (192.168.1) є номером мережі, а октет, що залишився - ідентифікатор хоста. Оскільки на деякі підмережі припадають мінімум по 16 пристроїв доцільно розбити адресу на 8 підмереж, що дасть можливість підключати до 30 хостів, що також в свою чергу надасть можливість збільшення мережі без вручання адміністратора.

Мережа: 192.168.1.0

Маска: /24 (255.255.255.0)

Вихідну маску у двійковому вигляді змістимо на 3 цифри праворуч.

Вихідна маска: 11111111.11111111.11111111.00000000 (/24)

Отримуємо 8 адрес:

– 11111111.11111111.11111111.00000000 (/27);

– 11111111.11111111.11111111.00100000 (/27);

- 11111111.11111111.11111111.01000000 (/27);
- 11111111.11111111.11111111.01100000 (/27);
- 11111111.11111111.11111111.10000000 (/27);
- 11111111.11111111.11111111.10100000 (/27);
- 11111111.11111111.11111111.11000000 (/27);
- 11111111.11111111.11111111.11100000 (/27).

Взявши маску першої підмережі можна дізнатися, що мережа починається з 192.168.1.0/27, закінчується 192.168.1. 31/29, де:

- 192.168.1.0 – адреса підмережі;
- 192.168.1.31/27 – широкомовна адреса;
- 192.168.1.1 - 192.168.1.30 – можливі адреси.

Адресу глобальної мережі WAN, 194.5.81.0 /27 потрібно розбити на 4 підмережі, для цього теж потрібно змістити двійковий вигляд маски також на 3 цифри, аби отримати маску /30. Це обмежить кількість хостів для до 2, що в свою чергу надасть можливість ідентифікувати пристрій фактично за адресую [4].

Інформація про ці підмережі наведена в таблицях 2.1-2.2.

Таблиця 2.1 – Розбиття LAN мережі

Мережа	Маска	Пул адрес	Можливі адреси	Максимальна кількість хостів
192.168.1.0	255.255.255.224 (/27)	192.168.1.0 – 192.168.1.31	192.168.1.1 – 192.168.1.30	30
192.168.1.32	255.255.255.224 (/27)	192.168.1.32 – 192.168.1.63	192.168.1.33 – 192.168.1.62	30
192.168.1.64	255.255.255.224 (/27)	192.168.1.64 – 192.168.1.95	192.168.1.65 – 192.168.1.94	30
192.168.1.96	255.255.255.224 (/27)	192.168.1.96 – 192.168.1.127	192.168.1.97 – 192.168.1.126	30
192.168.1.128	255.255.255.224 (/27)	192.168.1.128 – 192.168.1.159	192.168.1.129 – 192.168.1.158	30
192.168.1.160	255.255.255.224 (/27)	192.168.1.160 – 192.168.1.191	192.168.1.161 – 192.168.1.190	30

Продовження таблиці 2.1

192.168.1.192	255.255.255.224 (/27)	192.168.1.192 – 192.168.1.223	192.168.1.193 – 192.168.1.222	30
192.168.1.224	255.255.255.224 (/27)	192.168.1.224 – 192.168.1.255	192.168.1.225 – 192.168.1.254	30

Таблиця 2.2 – Розбиття WAN мережі

Мережа	Маска	Пул адрес	Можливі адреси	Максимальна кількість хостів
194.5.81.0	255.255.255.252 (/30)	193.169.1.0 – 193.169.1.3	193.169.1.1 – 193.169.1.2	2
194.5.81.4	255.255.255.252 (/30)	193.169.1.4 – 193.169.1.7	193.169.1.5 – 193.169.1.6	2
194.5.81.8	255.255.255.252 (/30)	193.169.1.8 – 193.169.1.11	193.169.1.9 – 193.169.1.10	2
194.5.81.12	255.255.255.252 (/30)	193.169.1.12 – 193.169.1.15	193.169.1.13 – 193.169.1.14	2

2.4 Налаштування інтерфейсів

Щоб налаштувати інтерфейсів існує спеціальний графічний інтерфейс (рис. 2.1), що містить графічні зображення та поля для введення інформації. Це значно полегшує та пришвидшує процес налаштування для адміністратора або людині відповідальній за це діл, але такий підхід обмежує набір доступних функцій в порівнянні з консольним інтерфейсом. Деякі системи можуть не підтримувати графічний інтерфейс взагалі [5].

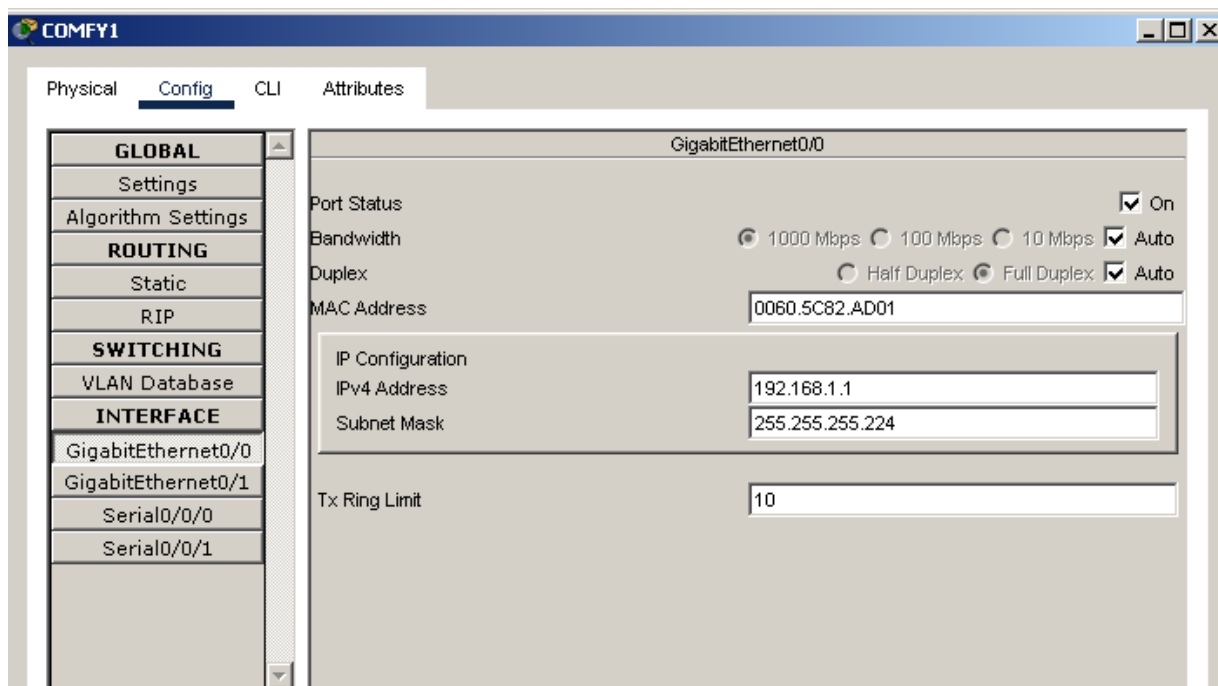


Рисунок 2.1 – Налаштування інтерфейсу через графічний інтерфейс

Для забезпечення роботи локальних та глобальних мереж необхідно налаштувати інтерфейси маршрутизаторів COMFY1 – COMFY4, використовуючи адреси з таблиці 2.3. Налаштування маршрутизаторів наведено в лістинг 2.1.

Таблиця 2.3 – IP адреси інтерфейсів маршрутизаторів

Маршрутизатор	Інтерфейс	IP-address	Маска
COMFY1	Gig0/0	192.168.1.1	255.255.255.224
	Gig0/1	192.168.1.33	255.255.255.224
	S0/0/0	193.169.1.1	255.255.255.252
COMFY2	Gig0/0	192.168.1.65	255.255.255.224
	Gig0/1	192.168.1.97	255.255.255.224
	S0/1/0	193.169.1.5	255.255.255.252
COMFY3	Gig0/0	192.168.1.129	255.255.255.224
	Gig0/1	192.168.1.161	255.255.255.224
	S0/0/1	193.169.1.9	255.255.255.252
COMFY4	Gig0/0	192.168.1.193	255.255.255.224
	Gig0/1	192.168.1.225	255.255.255.224
	S0/1/1	193.169.1.13	255.255.255.252

Лістинг 2.1 – Налаштування інтерфейсів маршрутизаторів

```
COMFY1>ena
COMFY1#conf t
```

Продовження лістингу 2.1

```
COMFY1(config)#interface gig0/0
COMFY1(config-if)#ip address 192.168.1.1 255.255.255.224
COMFY1(config-if)#exit
COMFY1(config)#interface gig0/1
COMFY1(config-if)#ip address 192.168.1.33 255.255.255.224
COMFY1(config-if)#exit
COMFY1(config)#interface s0/0/0
COMFY1(config-if)#ip address 193.169.1.1 255.255.255.252
COMFY1(config-if)#end
COMFY1#wr

COMFY2>ena
COMFY2#conf t
COMFY2(config)#interface gig0/0
COMFY2(config-if)#ip address 192.168.1.65 255.255.255.224
COMFY2(config-if)#exit
COMFY2(config)#interface gig0/1
COMFY2(config-if)#ip address 192.168.1.97 255.255.255.224
COMFY2(config-if)#exit
COMFY2(config)#interface s0/1/0
COMFY2(config-if)#ip address 193.169.1.5 255.255.255.252
COMFY2(config-if)#end
COMFY2#wr

COMFY3>ena
COMFY3#conf t
COMFY3(config)#interface gig0/0
COMFY3(config-if)#ip address 192.168.1.129 255.255.255.224
COMFY3(config-if)#exit
COMFY3(config)#interface gig0/1
COMFY3(config-if)#ip address 192.168.1.161 255.255.255.224
COMFY3(config-if)#exit
COMFY3(config)#interface s0/0/1
COMFY3(config-if)#ip address 193.169.1.9 255.255.255.252
COMFY3(config-if)#end
COMFY3#wr

COMFY4>ena
COMFY4#conf t
COMFY4(config)#interface gig0/0
COMFY4(config-if)#ip address 192.168.1.193 255.255.255.224
COMFY4(config-if)#exit
COMFY4(config)#interface gig0/1
COMFY4(config-if)#ip address 192.168.1.225 255.255.255.224
COMFY4(config-if)#exit
COMFY4(config)#interface s0/1/1
COMFY4(config-if)#ip address 193.169.1.13 255.255.255.252
COMFY4(config-if)#end
COMFY4#wr
```

2.5 Налаштування динамічної конфігурації DHCP та статичної конфігурації для керуючих пристроїв та серверів.

DHCP (англ. Dynamic Host Configuration Protocol – протокол динамічного налаштування вузла) – прикладний протокол, що дозволяє мережевим пристроям автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі. Також існує статична конфігурація[6].

Статичні IP-адреси дозволяють мережевим пристроям постійно зберігати ту саму IP-адресу, Мережевий адміністратор повинен відстежувати кожен статично призначений пристрій, щоб не використовувати цю IP-адресу знову. Оскільки статична IP-адреса вимагає ручного налаштування, це займає більше часу для початкового налаштування мережі та при приєднанні нового комп'ютеру потрібно налаштовувати вручну. Єдиною перевагою такого виду конфігурації є те, що через те що ip-адреса не змінюється – а це добре для веб-серверів, поштових серверів, використовуєте мережні принтери або використовуєте програму віддаленого доступу.

DHCP-сервер призначає вільну IP-адресу всім пристроям, підключеним до мережі. Це спосіб динамічного та автоматичного призначення IP-адрес мережевим пристроям у фізичній мережі. Він усуває завдання, що повторюється, призначення декількох IP-адрес кожному пристрою в мережі. Це може зайняти лише хвилину, але коли ви налаштовуєте сотні мережних пристроїв, це займе набагато більше часу. Точки бездротового доступу також використовують DHCP, тому адміністраторам не потрібно налаштовувати свої пристрої самостійно. Він пропонує автоматизований спосіб розповсюдження та оновлення IP-адрес та іншої інформації про конфігурацію по мережі. При приєднанні нового комп'ютеру до мережі, якщо на ньому включена служба DHCP сконфігується автоматично та можна образу приступати до роботи.

Використання DHCP в цій мережі перед статичною конфігурацією дасть такі переваги:

- автоматичне призначення IP-адрес: DHCP дозволяє автоматично призначати IP-адреси пристроям в мережі. Це усуває необхідність вручному призначенні IP-адрес кожному пристрою, що збільшує ефективність і економить час адміністратора мережі;
- уникнення конфліктів IP-адрес: DHCP виявляє конфлікти IP-адрес та уникає їх, переконуючись, що кожен пристрій отримує унікальну IP-адресу. Це допомагає уникнути можливих проблем з підключенням та забезпечує належну роботу мережі;
- централізоване керування: DHCP надає можливість централізованого керування призначенням IP-адрес та іншою мережевою конфігурацією. Адміністратор мережі може легко керувати і моніторити IP-адреси, призначені пристроям, з одного місця;
- ефективне використання IP-адрес: DHCP дозволяє ефективно використовувати доступні IP-адреси, оскільки вони можуть призначатися пристроям динамічно. Якщо пристрій вимкнено або відключено від мережі, його IP-адреса може бути призначена іншому пристрою, що дозволяє оптимізувати використання доступних адрес;
- легка розширюваність мережі: При додаванні нових пристроїв до мережі, використання DHCP спрощує процес конфігурації, оскільки нові пристрої автоматично отримують IP-адреси та іншу необхідну мережеву конфігурацію.

На лістингу 2.2 приведено список команд, для налаштування DHCP у локальних мережах на маршрутизаторах COMFY1-CONFY4. На рисунку 2.2 зображено автоматично роздані ip-адреси.

Лістинг 2.2 – Налаштування DHCP

```
COMFY1(config)#interface gig0/0
COMFY1(config-if)#service dhcp
COMFY1(config)#ip dhcp excluded-address 192.168.1.2
COMFY1(config)#ip dhcp excluded-address 192.168.1.3
COMFY1(config)#ip dhcp pool Dv1
COMFY1(dhcp-config)#network 192.168.1.0 255.255.255.224
COMFY1(dhcp-config)#default-router 192.168.1.1
COMFY1(dhcp-config)#dns-server 192.168.1.3
```

Продовження лістингу 2.2

```
COMFY1(dhcp-config)#exit
COMFY1(dhcp-config)#interface gig0/1
COMFY1(config-if)#service dhcp
COMFY1(config)#ip dhcp pool VC1
COMFY1(dhcp-config)#network 192.168.1.32 255.255.255.224
COMFY1(dhcp-config)#default-router 192.168.1.33
COMFY1(dhcp-config)#dns-server 192.168.1.3

COMFY2(config)#interface gig0/0
COMFY2(config-if)#service dhcp
COMFY2(config)#ip dhcp excluded-address 192.168.1.70
COMFY2(config)#ip dhcp pool Dv2
COMFY2(dhcp-config)#network 192.168.1.64 255.255.255.224
COMFY2(dhcp-config)#default-router 192.168.1.65
COMFY2(dhcp-config)#dns-server 192.168.1.3
COMFY2(dhcp-config)#exit
COMFY2(dhcp-config)#interface gig0/1
COMFY2(config-if)#service dhcp
COMFY2(config)#ip dhcp pool VC2
COMFY2(dhcp-config)#network 192.168.1.96 255.255.255.224
COMFY2(dhcp-config)#default-router 192.168.1.97
COMFY2(dhcp-config)#dns-server 192.168.1.3

COMFY3(config)#interface gig0/0
COMFY3(config-if)#service dhcp
COMFY3(config)#ip dhcp excluded-address 192.168.1.130
COMFY3(config)#ip dhcp excluded-address 192.168.1.133
COMFY3(config)#ip dhcp pool Dv3
COMFY3(dhcp-config)#network 192.168.1.128 255.255.255.224
COMFY3(dhcp-config)#default-router 192.168.1.129
COMFY3(dhcp-config)#dns-server 192.168.1.130
COMFY3(dhcp-config)#exit
COMFY3(dhcp-config)#interface gig0/1
COMFY3(config-if)#service dhcp
COMFY3(config)#ip dhcp excluded-address 192.168.1.197
COMFY3(config)#ip dhcp pool VC3
COMFY3(dhcp-config)#network 192.168.1.160 255.255.255.224
COMFY3(dhcp-config)#default-router 192.168.1.161
COMFY3(dhcp-config)#dns-server 192.168.1.130
```

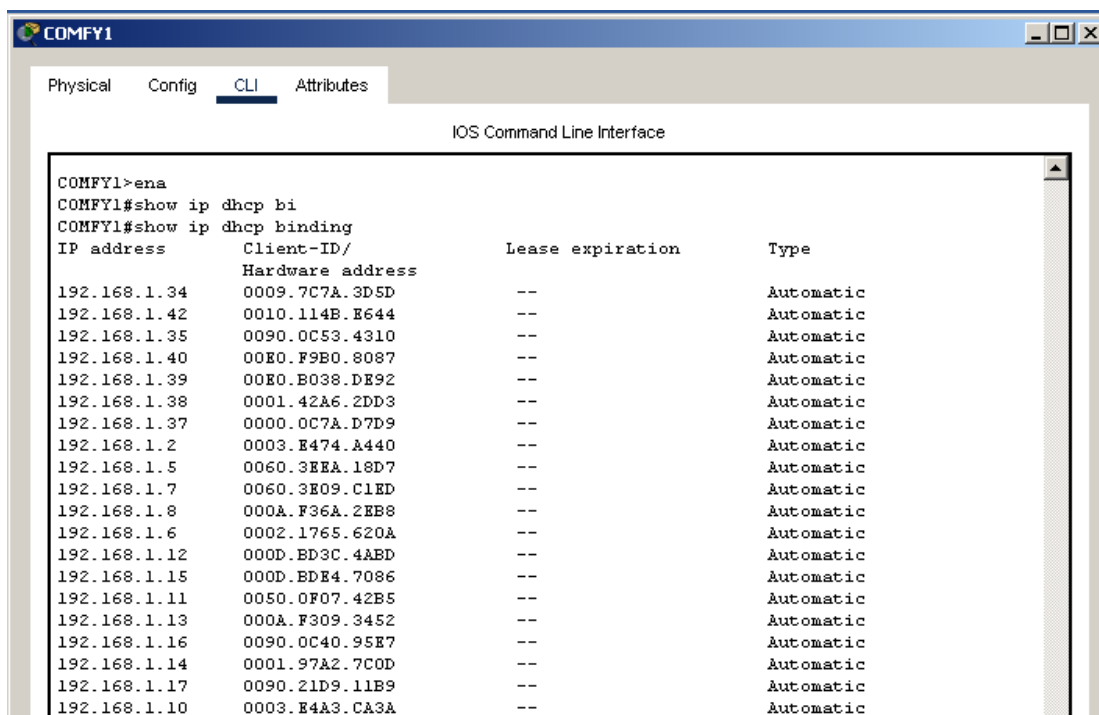


Рисунок 2.2 – Автоматична видачі ip-адрес

Оскільки до керуючих пристроїв відбувається постійне звертання їм потрібно налаштовувати статичну конфігурацію аби IP-адреса не змінювалась та не було конфліктів. Це є дуже важливим налаштуванням особливо для списків доступу ACL які буду встановлені в мережі. В таблиці 2.4 представлені конфігурація статичних IP-адресів.

Таблиця 2.4 – Статична конфігурація

Пристрій	Мережа	IP-адрес	Маска підмережі
Керуючий пристрій MAIN1	COMFY1	192.168.1.2	255.255.255.224
Керуючий пристрій MAIN2	COMFY2	192.168.1.70	255.255.255.224
Керуючий пристрій MAIN3	COMFY3	192.168.1.133	255.255.255.224
Керуючий пристрій MAIN4	COMFY4	192.168.1.197	255.255.255.224
Server1	COMFY1	192.168.1.3	255.255.255.224
Server2	COMFY3	192.168.1.130	255.255.255.224

3 НАЛАШТУВАННЯ ДОДАТКОВИХ ТЕХНОЛОГІЙ LAN МЕРЕЖ

3.1 Налаштування VLAN

VLAN – це мережа віртуального типу, налаштувати її можна на свитчі (сма́рт або керованому) другого рівня. По-іншому вона називається широкомовним доменом [7].

Комутатори, а не робочі станції, мають можливість використовувати VLAN, що означає, що на кожному порту комутатора визначається віртуальна мережа, до якої він належить. Весь трафік, що проходить через порт, позначається міткою - VLAN, і він зможе проходити через інші порти комутатора, які також працюють під цією міткою. Інші порти не зможуть приймати трафік, який проходить через цей порт. Таким чином, створюється окрема підмережа, що не може взаємодіяти з іншими підмережами без використання комутатора або роутера.

Як це працює? Наприклад, якщо є дві віртуальні LAN з ID = 20 і ID = 30, вони можуть бути розділені на дві підмережі на рівні 2, щоб хости в одній мережі не могли бачити хостів в іншій мережі. Щоб забезпечити взаємодію між цими віртуальними підмережами, потрібна маршрутизація трафіку між ними. Це можна здійснити на маршрутизаторі на третьому рівні. Кожному VLAN потрібен власний IP-адреса, який виконує функції шлюзу і необхідний для забезпечення зв'язку між різними підмережами.

Використання VLAN дозволяє:

- створити мережу з незалежною логічною структурою, не залежну від фізичного розташування компонентів мережі;
- розділити один домен на кілька, щоб трафік широкомовного типу, що належить до одного домену, не проходив через інші, тим самим зменшуючи навантаження на мережеве обладнання;
- захистити мережу від стороннього втручання, дозволяючи портам свіча ігнорувати та відкидати кадри, що надходять з інших VLAN, незалежно від їх початкового IP;

- групувати ПК, які входять в одну підмережу, і застосовувати політики на всю групу;

- здійснювати маршрутизацію за допомогою віртуальних портів.

Метою створення таких міток є об'єднання різних пристроїв, що знаходяться на різних свічах, в одну мережу. Застосовуючи VLAN, можна групувати деякі комп'ютери в один віртуальний сегмент, а інші - в інший. Це дозволяє комп'ютерам з різних доменів працювати так, ніби вони знаходяться на одному комутаторі. Навіть якщо пристрої входять до різних VLAN, вони не можуть розпізнати один одного. Це також дозволяє створити гостьову мережу [8].

Зважаючи на все вищевикладене, можна зробити висновок, що використання Virtual LAN має чотири основні переваги:

- дозволяє гнучко угруповувати пристрої та створювати ізольовані підмережі;

- знижує обсяг ширококомовного трафіку за рахунок відсутності трансляції між різними віртуальними підмережами;

- підвищує рівень безпеки та можливості управління, дозволяючи застосовувати різні налаштування безпеки та доступу для кожної віртуальної підмережі;

- знижує кількість мережевих пристроїв і кабелів, що потрібні для створення нової віртуальної підмережі.

В даній мережі VLAN потрібні для того, щоб зробити додаткові ізольовані мережі на які підключатимуться пристрої для тестування та демонстрації, вони матимуть доступ тільки між собою.

Для налаштування VLAN потрібно перейти на комутатор та на якому ми хочемо встановити віртуальні мережі, перейти во вкладку Config – VLAN database, де задаємо ім'я VLAN та його номер, який у нас є від 2 до 1001 тому що це базовий діапазон який нам потрібен (рис. 3.1) (також може бути 1002 - 1005 – це зарезервований для Token Ring та FDDI VLAN, а також розширений в діапазоні 1006 – 4094) [9]

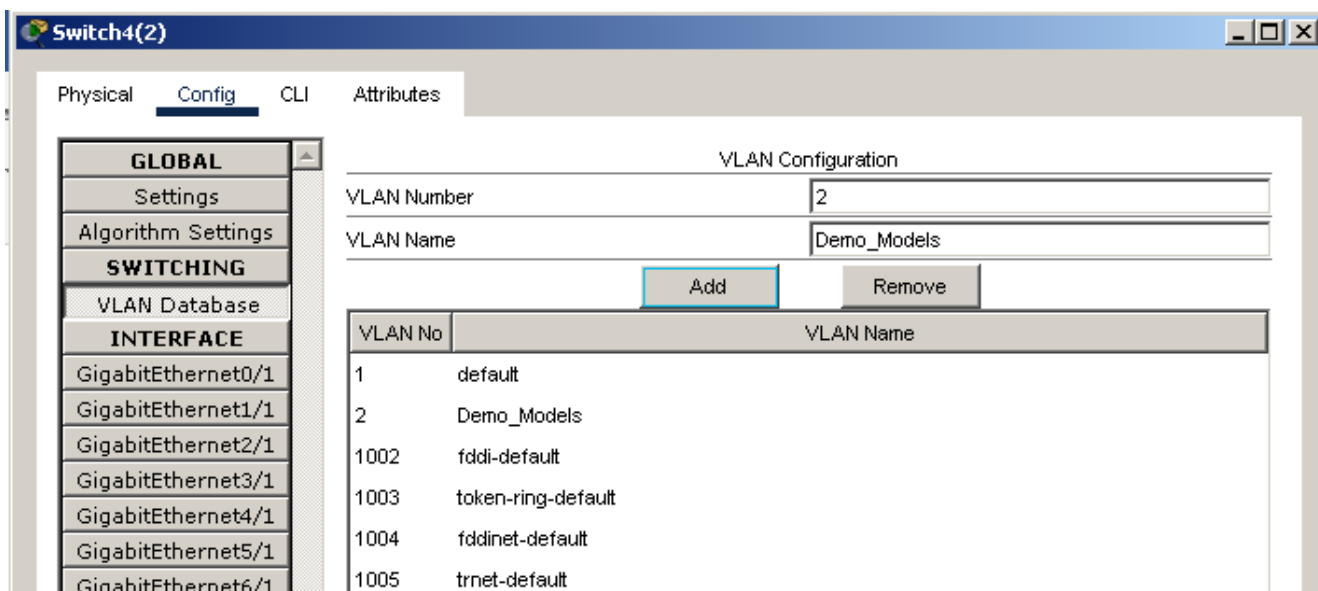


Рисунок 3.1 – Створення VLAN

Тепер, потрібно залишити тільки новостворену VLAN та перемкнути порти потрібних нам девайсів на Access port (рис. 3.2), який призначений для використання одним VLAN і може передавати нетиповий інформаційний трафік.

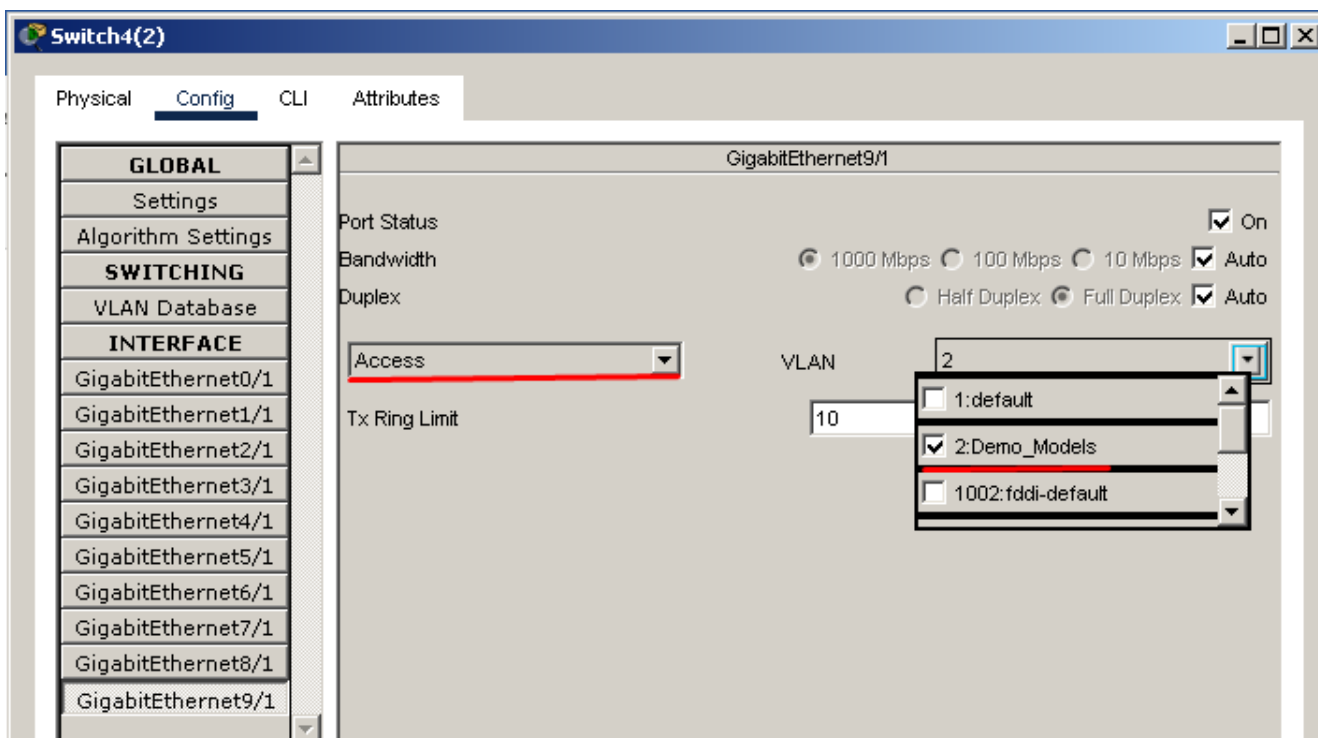


Рисунок 3.2 – Встановлення портів в режим access

Порт який в нас підключений до маршрутизації потрібно ж перевести в режим Trunk port (рис. 3.3), який дозволє передавати трафік з одного або кількох VLAN у вигляді пакетів з тегами.

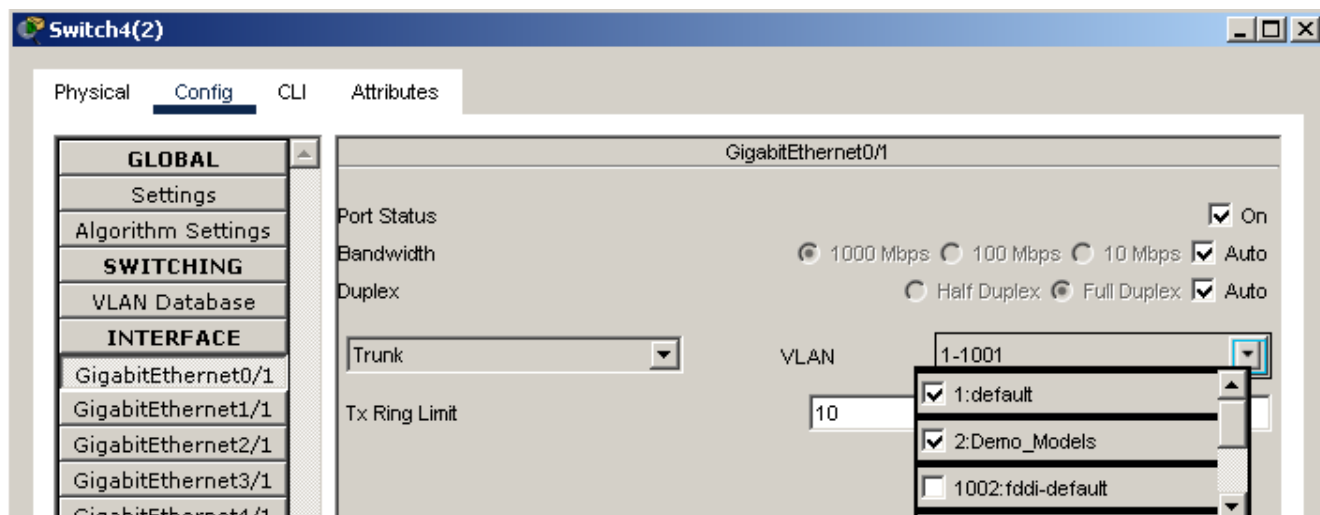


Рисунок 3.3 – Переведення порту підключеного до маршрутизатора в режим Trunk

Такі ж налаштування але зі своїми назвами та номером VLAN треба зробити на комутаторах інших філій.

На маршрутизаторі потрібно перевести порт мережі в режим, який дозволить ідентифікувати та відокремлювати трафік від різних VLAN на одному фізичному мережевому інтерфейсі. Також, оскільки це окрема мережа, для неї також потрібно задати IP адресацію за допомогою DHCP. Налаштування на маршрутизаторах наведені у лістингу 3.1

Лістинг 3.1 – Налаштування інтерфейсів для VLAN

```
COMFY1>ena
COMFY1#conf t
COMFY1(config)#interface gig0/0.2
COMFY1(config-subif)# encapsulation dot1Q 2
COMFY1(config-subif)#ip address 192.168.2.1 255.255.255.224
COMFY1(dhcp-config)#exit
COMFY1(dhcp-config)#interface gig0/0.2
COMFY1(config-if)#service dhcp
COMFY1(config)#ip dhcp pool Demo1
COMFY1(dhcp-config)#network 192.168.2.0 255.255.255.224
```

Продовження лістингу 3.1

```

COMFY1(dhcp-config)#default-router 192.168.2.1
COMFY1(dhcp-config)#dns-server 192.168.1.3
COMFY1(dhcp-config)#end
COMFY1#wr

COMFY2>ena
COMFY2#conf t
COMFY2(config)#interface gig0/0.4
COMFY2(config-subif)#encapsulation dot1Q 4
COMFY2(config-subif)#ip address 192.168.2.33 255.255.255.224
COMFY2(config-subif)#exit
COMFY2(config)#interface gig0/0.4
COMFY2(config-subif)#service dhcp
COMFY2(config)#ip dhcp pool Demo3
COMFY2(dhcp-config)#network 192.168.2.32 255.255.255.224
COMFY2(dhcp-config)#default-router 192.168.2.33
COMFY2(dhcp-config)#dns-server 192.168.1.3
COMFY2(dhcp-config)#end
COMFY2#wr

COMFY3>ena
COMFY3#conf t
COMFY3(config)#int gig0/0.3
COMFY3(config-subif)#encapsulation dot1Q 3
COMFY3(config-subif)#ip address 192.168.2.65 255.255.255.224
COMFY3(config-subif)#exit
COMFY3(config)#int gig0/0.3
COMFY3(config-subif)#service dhcp
COMFY3(config)#ip dhcp pool Demo2
COMFY3(dhcp-config)#network 192.168.2.64 255.255.255.224
COMFY3(dhcp-config)#default-router 192.168.2.65
COMFY3(dhcp-config)#dns-server 192.168.1.130
COMFY3(dhcp-config)#end
COMFY3#wr

COMFY4>ena
COMFY4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
COMFY4(config)#int gig0/0.5
COMFY4(config-subif)#encapsulation dot1Q 5
COMFY4(config-subif)#ip address 192.168.2.129 255.255.255.224
COMFY4(config-subif)#exit
COMFY4(config)#int gig0/0.5
COMFY4(config-subif)#service dhcp
COMFY4(config)#ip dhcp pool Demo4
COMFY4(dhcp-config)#network 192.168.2.128 255.255.255.224
COMFY4(dhcp-config)#default-router 192.168.2.129
COMFY4(dhcp-config)#dns-server 192.168.1.130
COMFY4(dhcp-config)#end
COMFY4#wr

```

3.2 Налаштування DNS

DNS (англ. Domain Name System - система доменних імен) - комп'ютерна розподілена система для отримання інформації про домени. Найчастіше використовується для отримання IP-адреси по імені хоста (комп'ютера або пристрою), отримання інформації про маршрутизацію пошти та про обслуговуючі вузли для протоколів у домену[10].

DNS-сервери взаємодіють за певним протоколом для підтримки розподіленої бази даних DNS, що ґрунтується на ієрархічній структурі доменних імен і зон. Кожен сервер, що відповідає за ім'я, може делегувати відповідальність за піддомен іншому серверу, наділяючи його відповідальністю за збереження актуальної інформації. Це дозволяє розподілити відповідальність за різні частини доменного імені на сервери різних організацій або людей.

Інтернет-провайдери мають свій власний DNS-сервер, який використовують браузері для отримання IP-адреси сервера, де знаходиться потрібний сайт. Це здійснюється за допомогою DNS-клієнта в кожному браузері. Однак, замість DNS-сервера провайдера можна використовувати будь-який інший публічний DNS-сервер, що вказаний в мережевих налаштуваннях. Наприклад, замість DNS-серверів інтернет-провайдера можна використовувати публічні DNS-сервери від Google.

Основне призначення DNS полягає у перетворенні символьних доменних імен на IP-адреси, також може виконувати зворотній процес за допомогою спеціального домена `in-addr.arpa`. В записах DNS можуть бути збережені різні дані, включаючи символьні імена, які можуть бути використані для перетворення IP-адрес на символьні імена. Наприклад, для знаходження DNS-імені для адреси `11.22.33.44` можна звернутися до DNS-сервера із запитом на запис `44.33.22.11.in-addr.arpa`, і сервер поверне відповідне символьне ім'я.

Щоб налаштувати DNS переходимо на сервері в вкладку Services – DNS, де потрібно встановити доменне ім'я, тип запису та адреса сервера (рис. 3.4)

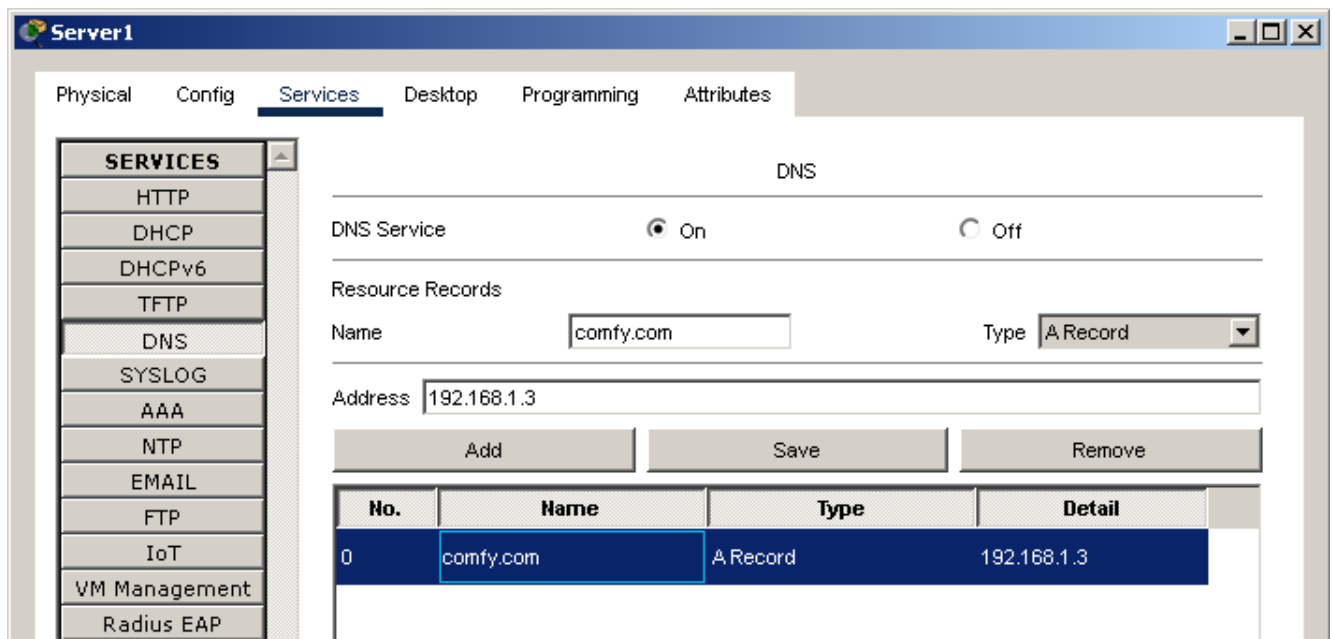


Рисунок 3.4 – Створення DNS

Також треба налаштувати WEB-сторінку, яка з'являється при переході на доменне ім'я серверу. Для цього в вкладці HTTP треба створити файл html (рис. 3.5)

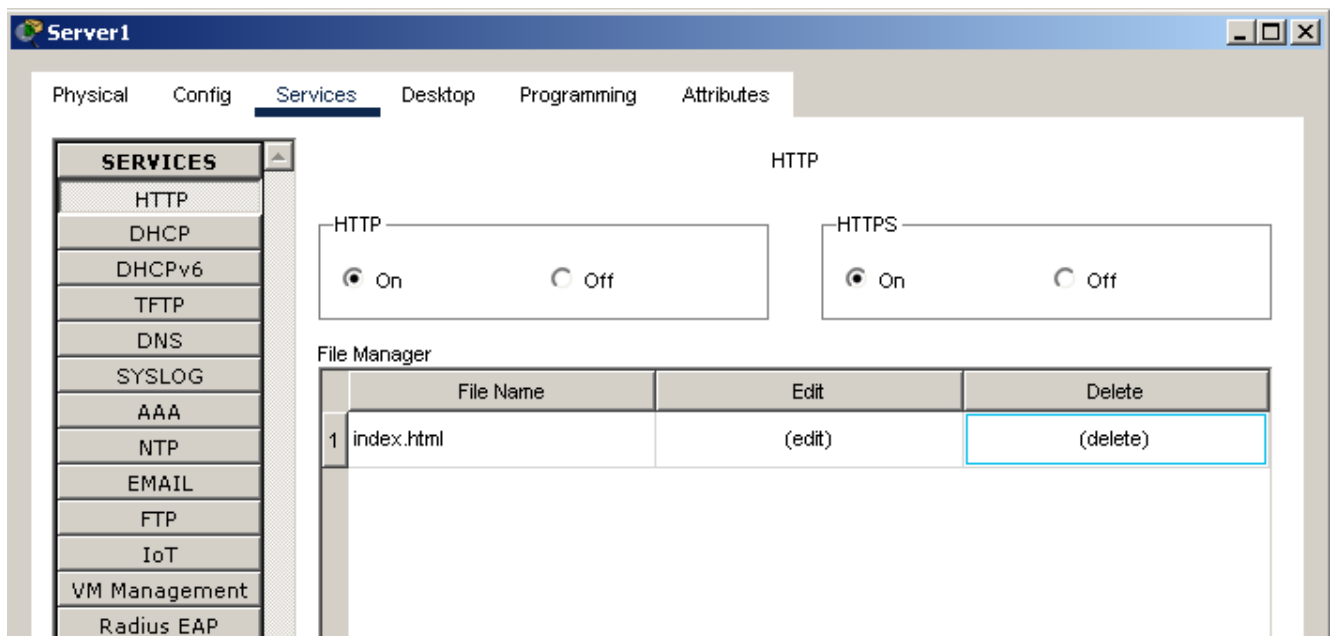


Рисунок 3.5 – Створення WEB-сторінки

3.3 Налаштування ACL

Список контролю доступу (ACL) - це список правил, який визначає, яким користувачам або системам надано або відмовлено в доступі до певного об'єкта або системного ресурсу. Списки контролю доступу також встановлюються в маршрутизаторах або комутаторах, де вони діють як фільтри, керуючи яким трафіком можна отримати доступ до мережі[11].

Кожен системний ресурс має атрибут безпеки, який ідентифікує свій список контролю доступу. Список містить запис для кожного користувача, який може отримати доступ до системи. Найпоширеніші привілеї для файлової системи ACL включають можливість читати файл або всі файли в каталозі, записувати в файл або файли, а також виконувати файл, якщо це виконуваний файл або програма. ACL також вбудовані в мережеві інтерфейси і операційні системи (ОС), включаючи Linux і Windows. У комп'ютерній мережі списки контролю доступу використовуються для заборони або допуску певних видів трафіку до мережі. Вони зазвичай фільтрують трафік на основі його джерела та призначення.

За допомогою розширених ACL можна виконувати фільтрацію трафіку з використанням більшої кількості параметрів, включаючи адреси відправника та одержувача, TCP/UDP порти відправника та одержувача, протоколи та типи трафіку. Розширені ACL мають більші можливості, ніж стандартні ACL, і можуть додатково розширюватися за допомогою нових технологій. Наприклад, Dynamic ACL дозволяє адміністратору створювати рядки, які не працюватимуть до підключення адміністратора до маршрутизатора по telnet, а потім можуть бути активовані, що дозволяє адміністратору зберегти "дірку" в безпеці для налагодження параметрів або при вході в мережу. ACL з відображенням (reflexive ACL) - це списки контролю доступу, які дозволяють запам'ятовувати, які адреси та порти зовнішньої мережі зверталися до ресурсів в мережі і автоматично створювати дзеркальний ACL, який пропускати тільки зворотний трафік з цих адрес та портів всередину мережі, якщо вона вже здійснювала звернення до цих

ресурсів. ACL залежно від часу (time-based ACL) - це списки контролю доступу, в яких деякі правила діють лише в певні періоди часу. Наприклад, легко налаштувати доступ в Інтернет з офісу тільки в робочі години.

Крім стандартних ACL, існують різні розширені варіанти, які надають додаткові можливості для контролю доступу і фільтрації трафіку. Один з них - розширені ACL (Extended ACL) - дозволяє використовувати більше параметрів для фільтрації трафіку, такі як адреси відправника та одержувача, порти TCP/UDP відправника та одержувача, протоколи і типи трафіку.

Ще один вид ACL - динамічні ACL (Dynamic ACL) - дозволяє адміністратору створювати правила, які не застосовуються, поки адміністратор не з'єднаний з пристроєм (наприклад, маршрутизатором) через протокол Telnet. Після підключення адміністратора до пристрою, ці правила можуть бути активовані, що дозволяє адміністратору мати "дірку" у безпеці для відладки або налаштування параметрів перед входом до мережі.

ACL з відображенням (Reflexive ACL) - це список контролю доступу, який дозволяє автоматично створювати "дзеркальний" ACL на основі інформації про адреси та порти зовнішньої мережі, які зверталися до ресурсів у внутрішній мережі. Цей "дзеркальний" ACL пропускати лише зворотний трафік з цих адрес та портів всередину мережі, якщо вона вже здійснювала звернення до цих ресурсів. Це дозволяє автоматично створювати правила для відповідного трафіку і спрощує налаштування ACL.

ACL залежно від часу (Time-based ACL) - це список контролю доступу, в якому деякі правила діють лише в певні періоди часу. Наприкладом може бути обмеження доступу до Інтернету з офісу лише протягом робочих годин. За допомогою ACL залежно від часу можна налаштувати правило, що дозволяє пропускати трафік із мережі офісу до Інтернету тільки в задані години роботи, наприклад з 9:00 ранку до 17:00 вечора. Поза цими годинами, правило відбракуватиме трафік та заборонятиме доступ до Інтернету з офісної мережі.

В даній мережі застосовуватиметься саме іменовані ACL. Іменовані ACL (Named ACL) - це підтип ACL, який дозволяє адміністраторам надавати іменовані

списки прав доступу, які можуть бути застосовані до різних об'єктів у системі. У звичайних ACL, які частіше за все використовуються, права доступу прямо вбудовуються в ресурс або об'єкт. Однак, іменовані ACL зберігаються окремо в системі і можуть бути повторно використані на різних ресурсах.

Застосування іменованих ACL дає більшу гнучкість та керованість при управлінні правами доступу [12]. Наприклад, ви можете створити іменований ACL для групи користувачів "Адміністратори" з встановленими правами доступу, а потім застосувати цей ACL до кількох різних ресурсів у системі. Якщо потрібно змінити права доступу для адміністраторів, можуть змінити іменований ACL один раз, і зміни автоматично відобразяться на всіх ресурсах, до яких він був застосований.

Лістинг 3.2 – Налаштування розширених ACL

```
COMFY1>ena
COMFY1#conf t
COMFY1(config)#ip access-list extended VC1
COMFY1(config-ext-nacl)#permit ip host 192.168.1.3 192.168.1.96
0.0.0.31
COMFY1(config-ext-nacl)#permit ip host 192.168.1.3 192.168.1.32
0.0.0.31
COMFY1(config-ext-nacl)#permit ip any host 255.255.255.255
COMFY1(config-ext-nacl)#permit ip host 192.168.1.2 192.168.1.64
0.0.0.31
COMFY1(config-ext-nacl)#permit ip host 192.168.1.2 192.168.1.128
0.0.0.31
COMFY1(config-ext-nacl)#permit ip host 192.168.1.2 192.168.1.192
0.0.0.31
COMFY1(config-ext-nacl)#permit ip host 192.168.1.3 192.168.1.64
0.0.0.31
COMFY1(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.31 host
192.168.1.70
COMFY1(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.31 host
192.168.1.133
COMFY1(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.31 host
192.168.1.197
COMFY1(config-ext-nacl)#deny ip any any
COMFY1(config-ext-nacl)#exit
COMFY1(config)#int s0/0/0
COMFY1(config-if)#ip access-group VC1 out
COMFY1(config-if)#exit
COMFY1(config)#ip access-list extended VLAN1
COMFY1(config-ext-nacl)#permit ip host 192.168.1.2 192.168.2.0
0.0.0.31
```

Продовження лістингу 3.2

```
COMFY1(config-ext-nacl)#permit ip host 192.168.1.3 192.168.1.96
0.0.0.31
COMFY1(config-ext-nacl)#permit ip host 192.168.1.3 192.168.1.32
0.0.0.31
COMFY1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.31 192.168.1.192
0.0.0.31
COMFY1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.31 192.168.1.128
0.0.0.31
COMFY1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.31 192.168.1.64
0.0.0.31
COMFY1(config-ext-nacl)#permit ip any host 255.255.255.255
COMFY1(config-ext-nacl)#deny ip any any
COMFY1(config-if)#exit
COMFY1(config)#int gig0/0
COMFY1(config-if)#ip access-group VLAN1 in
COMFY1(config-if)#exit
COMFY1(config-if)#end
COMFY1#wr
```

4 НАЛАШТУВАННЯ МАРШРУТИЗАЦІЇ ТА ДОДАТКОВИХ ТЕХНОЛОГІЙ WAN МЕРЕЖ

4.1 Налаштування статичної маршрутизації

Маршрутизація (англ. Routing) — процес визначення маршруту прямування інформації між мережами. Маршрутизатор приймає рішення, що базується на IP-адресі отримувача пакету. Для того, щоб переслати пакет далі, всі пристрої на шляху слідування використовують IP-адресу отримувача. Для прийняття правильного рішення маршрутизатор має знати напрямки і маршрути до віддалених мереж.

Є два типи маршрутизації:

- статична маршрутизація — маршрути задаються вручну адміністратором;
- динамічна маршрутизація — маршрути обчислюються автоматично за допомогою протоколів динамічної маршрутизації — RIP, OSPF, EIGRP, IS-IS, BGP, HSRP та ін, які отримують інформацію про топологію і стан каналів зв'язку від інших маршрутизаторів у мережі.

Протоколи динамічної маршрутизації дозволяють маршрутизаторам обмінюватись інформацією про доступні маршрути, метрики, які вказують на якості шляхів, а також про стан каналів зв'язку. На основі цієї інформації маршрутизатори визначають оптимальні маршрути та оновлюють свої таблиці маршрутизації.

Конфігурація статичних маршрутів вручну вимагає від адміністратора додавання та видалення статичних маршрутів у відповідності до змін мережної топології. У великих мережах це може бути часо- та ресурсоємним процесом, тоді як у невеликих мережах це здійснюється легко. Статична маршрутизація не є масштабованою, у порівнянні з динамічною маршрутизацією, яка потребує додаткового налаштування та втручання адміністратора. Однак, у великих мережах, статична маршрутизація може використовуватися для спеціальних цілей у поєднанні з динамічною маршрутизацією, оскільки вона є більш стабільною та вимагає менше апаратних ресурсів маршрутизатора для обслуговування таблиці маршрутизації.

Хоча статична маршрутизація має свої обмеження, вона також має деякі переваги, зокрема:

- простота налаштування: Статична маршрутизація досить проста для налаштування. Адміністратор може вручну вказати маршрути, що дозволяє більш точно контролювати шляхи, по яких пропускаються дані;
- менша використання ресурсів: Використання статичної маршрутизації не потребує витрат на обчислення маршрутів або обміну маршрутною інформацією між маршрутизаторами. Це дозволяє заощадити ресурси мережі, особливо в малих мережах або в мережах зі стабільною топологією;
- безпека: За використання статичної маршрутизації можна забезпечити високий рівень безпеки. Відсутність автоматичного оновлення маршрутів ускладнює можливість некоректних або зловмисних маршрутизаційних оновлень;
- контроль над маршрутизацією: Статична маршрутизація дозволяє адміністратору повністю контролювати шляхи маршрутизації. Це особливо

важливо в ситуаціях, коли потрібно використовувати специфічні маршрути для взаємодії з певними мережами чи пристроями;

– незмінність маршрутів: Статичні маршрути залишаються стабільними, оскільки не змінюються автоматично під впливом змін у мережі. Це може бути корисним у деяких випадках, коли потрібна стабільність маршрутів для певних послуг або додатків;

Та основна причина чому використана статична маршрутизація в даній мережі, це ізольовані підмережі: У нашому випадку мережа розбита на ізольовані підмережі, які не взаємодіють між собою. Використання статичної маршрутизації дозволяє точно визначити шляхи між цими підмережами та забезпечити їх незалежність.

У таблиці 4.1 приведено основні відмінності статичної та динамічної маршрутизації.

Таблиця 4.1 - порівняння статичної та динамічної маршрутизації

Параметр	Статична маршрутизація	Динамічна маршрутизація
Складність налаштування	Підвищується зі збільшенням розміру мережі	Як правило, не залежить від розміру мережі
Зміна топології мережі	Потрібне втручання мережевого адміністратора	Змінюється автоматично зміні топології мережі
Масштабування	Підходить для простих Топологій	Підходить для простих та складних топологій
Безпека	Вищий рівень Безпеки	Нижчий рівень безпеки
Споживання ресурсів	Не вимагає додаткових Ресурсів	Використовує процесор, пам'ять та смугу пропускання каналу
Передбачуваність маршруту	Маршрут до місця призначення завжди один і той же	Маршрут залежить від поточної топології

Після вручного налаштування статичного маршруту адміністратором, маршрутизатор зберігає його в своїй таблиці маршрутизації (ТМ) та використовує

для пересилання пакетів. Для задання статичного маршруту використовується команда з таким синтаксисом [13]:

```
Rt(config)#ip route prefix mask {ip | int-type int-num}[dist].
```

Де:

prefix та mask - це IP-адреса та маска пункту призначення, відповідно;

ip, int-type та int-num вказують на IP-адресу наступного транзитного переходу (хопа), тип та номер локального інтерфейсу, на який необхідно надіслати пакет, щоб він дістався до вказаного пункту призначення.;

dist, який не є обов'язковим, характеризує надійність маршруту. Чим менша адміністративна відстань (AB), тим надійнішим є маршрут. Маршрути з меншою AB занесені до ТМ.

Налаштування статичної маршрутизації між мережами наведена у лістинг 4.1

Лістинг 4.1 – Статична маршрутизація

```
COMFY1>ena
COMFY1#conf t
COMFY1(config)#ip route 193.169.1.4 255.255.255.252 Serial0/0/0
COMFY1(config)#ip route 193.169.1.8 255.255.255.252 Serial0/0/0
COMFY1(config)#ip route 193.169.1.12 255.255.255.252 Serial0/0/0
COMFY1(config)#ip route 192.168.1.64 255.255.255.224 193.169.1.5
COMFY1(config)#ip route 192.168.1.96 255.255.255.224 193.169.1.5
COMFY1(config)#ip route 192.168.1.128 255.255.255.224 193.169.1.9
COMFY1(config)#ip route 192.168.1.160 255.255.255.224 193.169.1.9
COMFY1(config)#ip route 192.168.1.192 255.255.255.224 193.169.1.13
COMFY1(config)#ip route 192.168.1.224 255.255.255.224 193.169.1.13
COMFY1(config)#end

COMFY2>ena
COMFY2#conf t
COMFY2(config)#ip route 193.169.1.0 255.255.255.252 Serial0/1/0
COMFY2(config)#ip route 193.169.1.8 255.255.255.252 Serial0/1/0
COMFY2(config)#ip route 193.169.1.12 255.255.255.252 Serial0/1/0
COMFY2(config)#ip route 192.168.1.0 255.255.255.224 193.169.1.1
COMFY2(config)#ip route 192.168.1.32 255.255.255.224 193.169.1.1
COMFY2(config)#ip route 192.168.1.128 255.255.255.224 193.169.1.9
COMFY2(config)#ip route 192.168.1.160 255.255.255.224 193.169.1.9
COMFY2(config)#ip route 192.168.1.192 255.255.255.224 193.169.1.13
COMFY2(config)#ip route 192.168.1.224 255.255.255.224 193.169.1.13
COMFY2(config)#end

COMFY3>ena
COMFY3#conf t
```

Продовження лістингу 4.1

```
COMFY3(config)#ip route 193.169.1.0 255.255.255.252 Serial0/0/1
COMFY3(config)#ip route 193.169.1.4 255.255.255.252 Serial0/0/1
COMFY3(config)#ip route 193.169.1.12 255.255.255.252 Serial0/0/1
COMFY3(config)#ip route 192.168.1.0 255.255.255.224 193.169.1.1
COMFY3(config)#ip route 192.168.1.32 255.255.255.224 193.169.1.1
COMFY3(config)#ip route 192.168.1.64 255.255.255.224 193.169.1.5
COMFY3(config)#ip route 192.168.1.96 255.255.255.224 193.169.1.5
COMFY3(config)#ip route 192.168.1.192 255.255.255.224 193.169.1.13
COMFY3(config)#ip route 192.168.1.224 255.255.255.224 193.169.1.13
COMFY3(config)#end
```

```
COMFY4>ena
```

```
COMFY4#conf t
```

```
COMFY4(config)#ip route 193.169.1.0 255.255.255.252 Serial0/1/1
COMFY4(config)#ip route 193.169.1.4 255.255.255.252 Serial0/1/1
COMFY4(config)#ip route 193.169.1.8 255.255.255.252 Serial0/1/1
COMFY4(config)#ip route 192.168.1.0 255.255.255.224 193.169.1.1
COMFY4(config)#ip route 192.168.1.32 255.255.255.224 193.169.1.1
COMFY4(config)#ip route 192.168.1.64 255.255.255.224 193.169.1.5
COMFY4(config)#ip route 192.168.1.96 255.255.255.224 193.169.1.5
COMFY4(config)#ip route 192.168.1.128 255.255.255.224 193.169.1.9
COMFY4(config)#ip route 192.168.1.160 255.255.255.224 193.169.1.9
COMFY4(config)#end
```

4.2 Налаштування IPsec VPN

Віртуальна приватна мережа (VPN) - це зашифроване з'єднання між двома або більше комп'ютерами, яке використовується для безпечного обміну даними через загальнодоступні мережі. Використання VPN дозволяє зберігати приватність і безпеку обміну конфіденційною інформацією, навіть при підключенні до публічного Інтернету. Наприклад, віддалені співробітники можуть використовувати VPN для безпечного доступу до корпоративних файлів і програм.

Багато VPN використовують IPsec (Internet Protocol Security) як набір протоколів для налаштування та забезпечення зашифрованого з'єднання. Однак не всі VPN використовують IPsec. Існує також інший протокол для VPN, відомий як SSL/TLS (Secure Sockets Layer/Transport Layer Security), який працює на іншому рівні моделі OSI (Open Systems Interconnection), ніж IPsec. Модель OSI є

абстрактним представленням процесів, що відбуваються в Інтернеті для забезпечення його правильної роботи.

IPsec - це набір протоколів, які використовуються спільно для створення зашифрованих з'єднань між пристроями з метою забезпечення безпеки передачі даних через публічні мережі. IPsec часто використовується для налаштування віртуальних приватних мереж (VPN) і працює шляхом шифрування IP-пакетів та перевірки автентичності джерела, з якого надходять пакети [14].

Термін «IPsec» походить від "Internet Protocol security" (захист Інтернет-протоколу), де "IP" означає "Internet Protocol" (Інтернет-протокол), а «sec» - «secure» (безпечний). Інтернет-протокол є основним протоколом маршрутизації, використовуваним в Інтернеті, і вказує, куди необхідно направити дані за допомогою IP-адреси. IPsec забезпечує безпеку шляхом додавання шифрування та автентифікації до цього процесу.

Окрім IPsec, існує ще протокол SSL/TLS, який використовується для створення захищених з'єднань на рівні транспортного протоколу. Він широко застосовується для захисту комунікації веб-сайтів, особливо при використанні протоколу HTTPS. SSL/TLS забезпечує шифрування даних та аутентифікацію сторінок, що дозволяє користувачам безпечно взаємодіяти з веб-сайтами і передавати конфіденційну інформацію.

Вибір протоколу VPN залежить від потреб і вимог конкретної ситуації. IPsec забезпечує надійний захист на мережевому рівні, тоді як SSL/TLS забезпечує зручність і захист на рівні транспортного протоколу. При використанні VPN рекомендується також враховувати

Для того щоб почати налаштовувати VPN IPsec на маршрутизаторах, треба впевнитись що на них доступний пакет ліцензії Security Technology Package, без нього, виконати дії які стосуються безпеки трафіку неможливо[15].

Щоб переконатись в наявності, потрібно прописати команду «Show version», після чого опуститись вниз, до ліцензії (рис. 4.1).

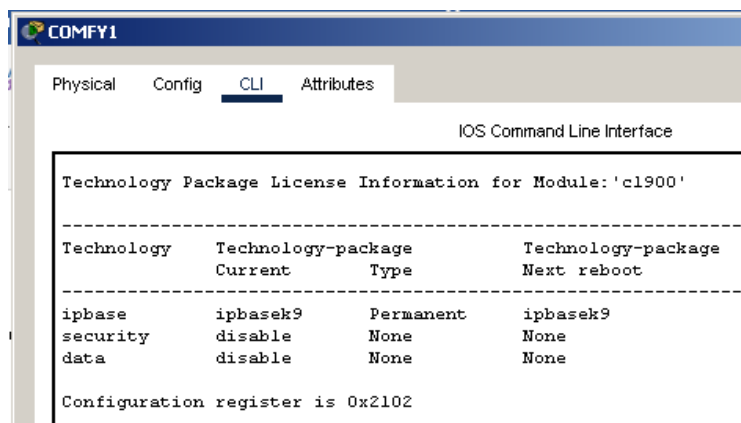


Рисунок 4.1 – Відсутність ліцензії

Для встановлення пакету securityk9 та активації ліцензії потрібно виконати такі дії. В режимі конфігурації прописати наступну команду «> license boot module c1900 technology-package securityk9», після чого нам потрібно бути погодитись на встановлення. Після чого ми зберігаємо встановлені конфігурації командою «copy running-config startup-config» та робимо перезавантаження маршрутизатора, щоб дії вступили в силу командою «reload». Тепер можна побачити, що модуль встановлено (рис. 4.2), та налаштовувати VPN.

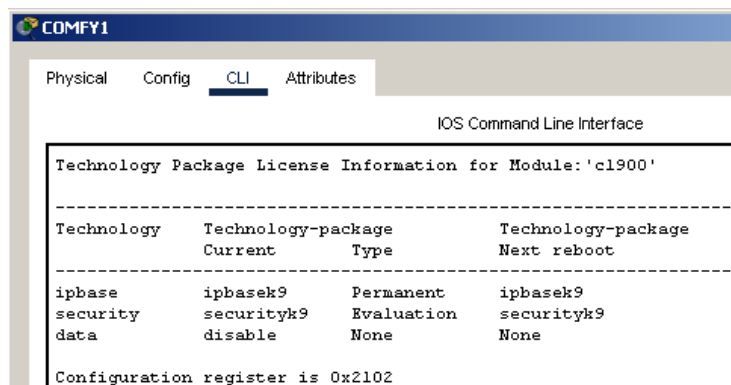


Рисунок 4.2 – Установлений модуль securityk9

Фрагмент налаштування самого модуля VPN IPsec наведено у лістинг 4.2 та у лістингу A.1

Лістинг 4.2 – VPN IPsec між CONFY1 та CONFY2

CONFY1>ena

Продовження лістингу 4.2

```
COMFY1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
COMFY1(config)#crypto isakmp policy 10
COMFY1(config-isakmp)#encryption aes
COMFY1(config-isakmp)#authentication pre-share
COMFY1(config-isakmp)#group 1
COMFY1(config-isakmp)#exit
COMFY1(config)#crypto isakmp key COMFY2 address 193.169.1.5
COMFY1(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
COMFY1(config)#crypto map VPN-MAP 1 ipsec-isakmp
COMFY1(config-crypto-map)#description VPN connection to COMFY2
COMFY1(config-crypto-map)#set peer 193.169.1.5
COMFY1(config-crypto-map)#set transform-set VPN-SET
COMFY1(config-crypto-map)#match address 110
COMFY1(config-crypto-map)#exit
COMFY1(config)#int s0/0/0
COMFY1(config-if)#crypto map VPN-MAP

COMFY2(config)#crypto isakmp policy 10
COMFY2(config-isakmp)#encryption aes
COMFY2(config-isakmp)#authentication pre-share
COMFY2(config-isakmp)#group 1
COMFY2(config-isakmp)#exit
COMFY2(config)#crypto isakmp key COMFY2 address 193.169.1.1
COMFY2(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
COMFY2(config)#crypto map VPN-MAP 1 ipsec-isakmp
COMFY2(config-crypto-map)#description VPN connection to COMFY1
COMFY2(config-crypto-map)#set peer 193.169.1.1
COMFY2(config-crypto-map)#set transform-set VPN-SET
COMFY2(config-crypto-map)#match address 111
COMFY2(config-crypto-map)#exit
COMFY2(config)#int s0/1/0
COMFY2(config-if)#crypto map VPN-MAP
```

4.3 Налаштування Frame-Relay

Frame Relay - це форма телекомунікаційної технології, що дозволяє з'єднувати локальні мережі (LAN) та передавати дані між вузлами в глобальних мережах (WAN)[16].

Frame Relay використовує комутацію пакетів, що означає, що він розділяє дані, наприклад голосові виклики, на менші пакети, відомі як кадри, для їх передачі

через спільну мережу Frame Relay. Після цього кадри даних збираються знову на місці призначення. Frame Relay вже довгий час використовується як частина системи цифрової мережі інтегрованих послуг (ISDN) у багатьох компаній. Він часто розглядається як спрощена версія старішої технології комутації пакетів, відомої як X.25.

Frame Relay зазвичай використовується для передачі даних між віддаленими локальними мережами або через глобальні мережі. В порівнянні з схемами «точка-точка», які використовують виділені лінії між мережами, Frame Relay є економічно ефективним варіантом.

Frame Relay є вигідним з фінансової точки зору, оскільки він використовує спільну мережу з кількома доступами, замість оплати за пропускну здатність окремих виділених ліній. Кожен маршрутизатор у мережі використовує віртуальний канал Frame Relay, що забезпечує ефективне спільне використання ресурсів.

Для отримання доступу до мережі Frame Relay, компанії використовують пристрій доступу Frame Relay (FRAD) на своїй території. Цей пристрій може бути програмним забезпеченням в маршрутизаторі або окремим фізичним пристроєм. FRAD підключається до комутатора frame relay постачальника послуг через інтерфейс користувача до мережі (UNI) і створює канал доступу.

У мережі Frame Relay кожен канал або канал доступу, який підключається до віртуальної мережі, закінчується комутатором Frame Relay. Коли маршрутизатор надсилає пакет даних, він перевіряється комутатором Frame Relay, що шукає ідентифікатор з'єднання каналу передачі даних (DLCI). Це число вказує на віртуальний канал, через який пакет направлятиметься до місця призначення. Потім Frame Relay передає пакет на основі DLCI до призначеного пункту.

Той же процес можна пояснити за допомогою обладнання для передачі даних, такого як обладнання для передачі даних (DCE) і термінальне обладнання для передачі даних (DTE). У мережі Frame Relay, DCE виступає в якості комутатора Frame Relay, оскільки він надає послугу, а DTE відображається на маршрутизаторах, які отримують цю послугу.

Щоб налаштувати Frame-Relay в мережі треба спочатку перевести порт, через який відбувається з'єднання з «Cloud», в режим Frame-Relay (лістинг 4.3)

Лістинг 4.3 – Встановлення портів в режим Frame-relay

```
COMFY1>ena
COMFY1#conf t
COMFY1(config)#int s0/0/0
COMFY1(config)#encapsulation frame-relay
COMFY1(config)#end
COMFY1#wr
```

```
COMFY2>ena
COMFY2#conf t
COMFY2(config)#int s0/1/0
COMFY2(config)#encapsulation frame-relay
COMFY2(config)#end
COMFY2#wr
```

```
COMFY3>ena
COMFY3#conf t
COMFY3(config)#int s0/0/1
COMFY3(config)#encapsulation frame-relay
COMFY3(config)#end
COMFY3#wr
```

```
COMFY4>ena
COMFY4#conf t
COMFY4(config)#int s0/0/0
COMFY4(config)#encapsulation frame-relay
COMFY4(config)#end
COMFY4#wr
```

Тепер потрібно налаштувати ідентифікатор з'єднання каналу передачі даних (DLCI), який вказує на віртуальний канал, котрий направлятиме пакет до місця призначення. Для цього в Cloud перейти в Config – Serial* (рис. 4.3). Потрібно задати DLCI, його назву (краще задавати назву пристрою до якого іде з'єднання), та LMI. LMI дозволяє мережевим пристроям обмінюватися необхідною інформацією для правильної роботи мережі Frame Relay, включаючи виявлення помилок, моніторинг використання ресурсів та керування віртуальними каналами.

В таблиці 4.2 представлені всі DLCI для інтерфейсів.

Таблиця 4.2 – Параметри інтерфейсів для Frame-Relay

Інтерфейс	DLCI	Назва	LMI
Serial0	102	COMFY2	Cisco
Serial0	103	COMFY3	Cisco
Serial0	104	COMFY4	Cisco
Serial1	201	COMFY1	Cisco
Serial1	203	COMFY3	Cisco
Serial1	204	COMFY4	Cisco
Serial2	301	COMFY1	Cisco
Serial2	302	COMFY2	Cisco
Serial2	304	COMFY4	Cisco
Serial3	401	COMFY1	Cisco
Serial3	402	COMFY2	Cisco
Serial3	403	COMFY3	Cisco

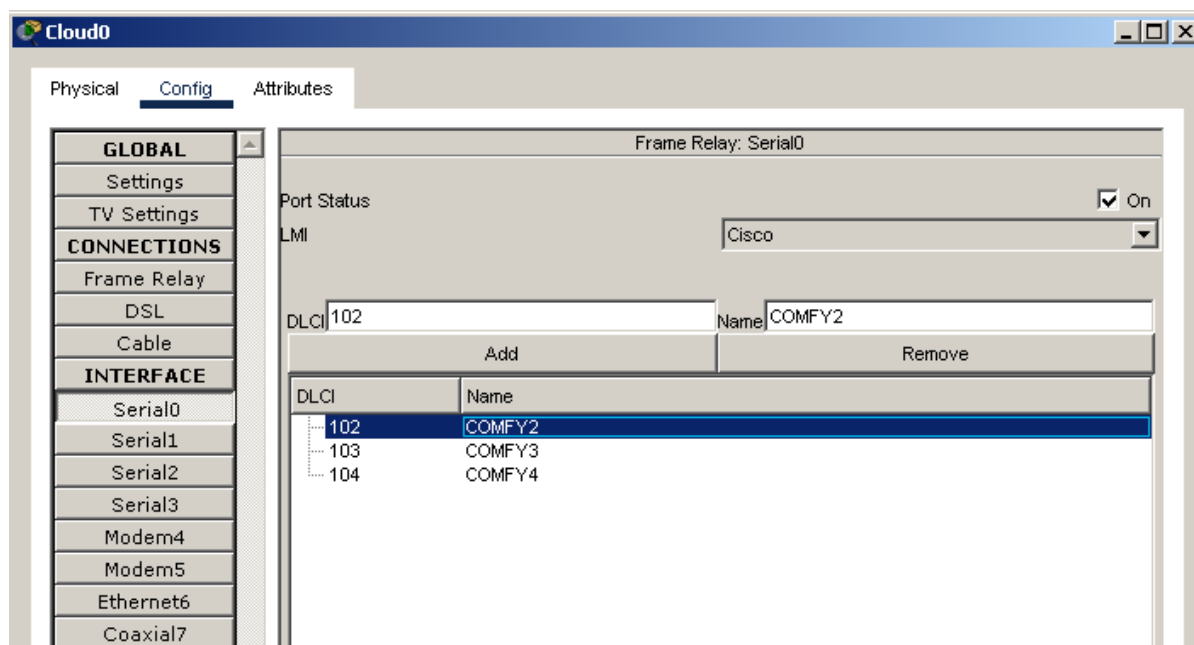


Рисунок 4.3 – Встановлення DLCI

В кінці треба встановити зв'язок між портами, для цього на кладці Frame-Relay обираємо з'єднання між портами. Щоб був доступ філії кожна-к-кожної, достатньо встановити такі з'єднання, які наведені на рисунку 4.4.

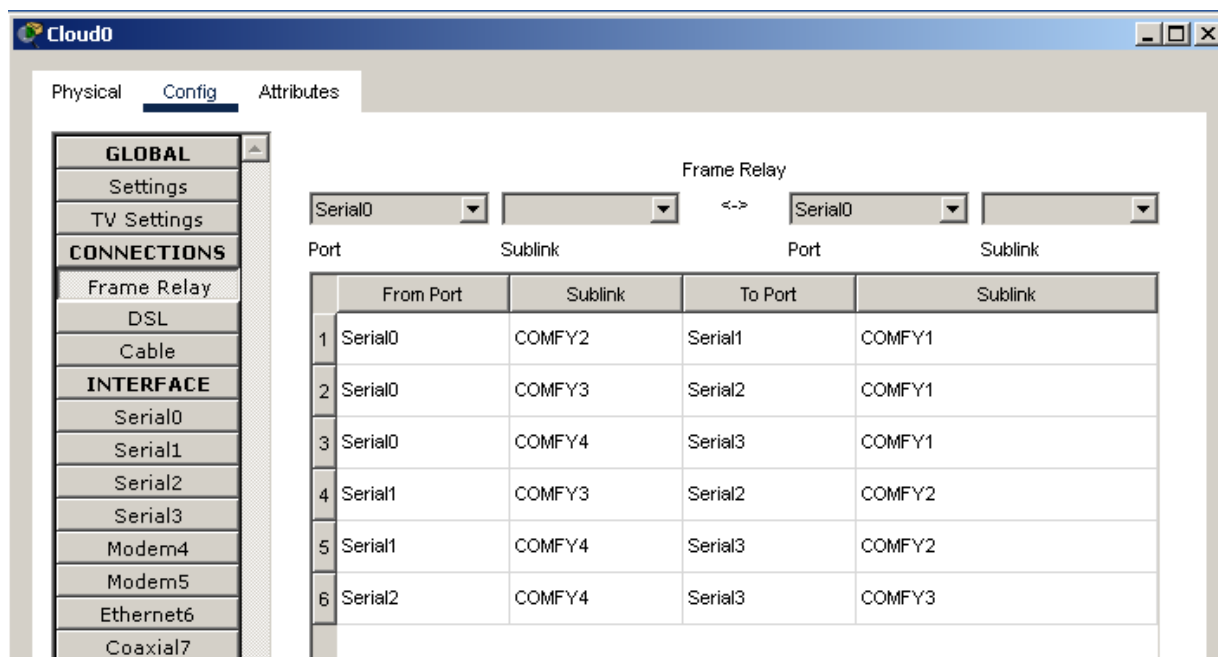


Рисунок 4.4 – Встановлення зв'язків між інтерфейсами

5 СТВОРЕННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА ПРОКЛАДАННЯ МЕРЕЖІ

Щоб побудувати нашу мережу, треба спочатку зробити її мережеву інфраструктуру, тобто сукупність фундаментальних компонентів, які злагоджено працюватимуть.

Проектування мережевої інфраструктури може допомогти спланувати впровадження, моніторинг і керування IT-мережею. Проект може бути створений після визначення експлуатаційних вимог щодо пропускної здатності, якості обслуговування, безпеки та стійкості. Після впровадження проектування мережі це допоможе у вирішенні проблем мережі, допомагаючи легше зрозуміти ролі різних компонентів у мережі та те, як несправний пристрій може вплинути на мережу та інші системи, що використовують мережу [17].

Крім планування дизайну мережевої інфраструктури, мережеві адміністратори можуть використовувати спеціальне програмне забезпечення для отримання огляду мережевої топології, конфігурацій та продуктивності. Такі

програми надають можливість візуалізувати мережеву інфраструктуру, отримати уявлення про її структуру та визначити продуктивність.

Додатково, програмне забезпечення для конфігурації мережі може бути використане для оновлення топологічних карт шляхом сканування змін, що відбуваються в мережі. Це допомагає зрозуміти та відображати мережеву інфраструктуру, виявити зміни в архітектурі мережі та забезпечити більш ефективне масштабування пропускну здатності.

У мережевій інфраструктурі використовуються різноманітні програмні додатки та апаратні компоненти. Основними функціями, які виконуються в будь-якій мережі, є маршрутизація і перемикання. Кожен пристрій та сервер підключаються до комутатора за допомогою власного мережевого кабелю, що дозволяє пряме з'єднання з будь-яким іншим пристроєм. Компонентами мережі є мережеві кабелі, які використовуються для з'єднання серверів, комп'ютерів, принтерів, комутаторів, маршрутизаторів, точок доступу та інших пристроїв. Кожен з цих компонентів відіграє важливу роль у забезпеченні безперебійного зв'язку та обміну даними всередині мережі.

Мережа крамниць побудована та прокладена так, щоб надавати зручні та прості способи для покупки електроніки та побутової техніки своїм клієнтам. Використання телекомунікаційних стійки так прокладання оптоволоконних кабелів через коробки на горі, дає захищеність мережі високого рівня.

Інфраструктура побудована для підтримки зростаючого бізнесу компанії. Вона включає сучасний дистриб'юторський центр, який забезпечує ефективну обробку великих обсягів продукції в усіх філій які з'єднані між собою. Крім того, COMFY має потужну IT-інфраструктуру, яка підтримує їхні онлайн-замовлення та забезпечує якісне обслуговування.

Але прокладання такої мережі має також свої труднощі:

– планування: Компанія COMFY вміло планує маршрути мережі з метою досягнення оптимальної ефективності та економічної вигоди. При цьому враховується також екологічний аспект мережі;

- отримання дозволів: перед тим, як прокласти мережу, потрібно отримати дозволи від місцевих органів влади. Цей процес може бути вимогливим та фінансово затратним;

- координація: COMFY змушений взаємодіяти з іншими комунальними компаніями, щоб уникнути пошкодження їхньої інфраструктури. Це вимагає складних і трудомістких координаційних зусиль;

- вартість: встановлення мережевої інфраструктури є значними інвестиціями для компанії. Тому необхідно ретельно бюджетувати проект, забезпечуючи його економічну ефективність.

Незважаючи на ці проблеми, COMFY віддає перевагу створенню своєї мережевої інфраструктури. Компанія розглядає інвестиції як необхідність для забезпечення майбутнього розвитку свого бізнесу.

6 ВАРІАНТИ ПОКРАЩЕННЯ МЕРЕЖІ ТА ЇЇ РОБОТА ПІД ЧАС ВІЙСЬКОВОГО СТАНУ

Розроблена в даному проекті мережа не є ідеальною та її можна покращувати, як то с точки зору функціоналу так і захисту.

Для досягнення значного покращення продуктивності та забезпечення високого рівня безпеки мережі, рекомендується вживати конкретні заходи. Перш за все, варто інвестувати у більш надійне та ефективне обладнання, таке як оновлені роутери, комутатори та брандмауери. Це дозволить забезпечити більш швидке та стабільне з'єднання, а також підвищить загальну надійність мережі.

Другий важливий крок - впровадження кращих заходів безпеки. Рекомендується використовувати спеціалізовані брандмауери, системи виявлення вторгнень та шифрування. Ці заходи допоможуть захистити вашу мережу від потенційних загроз, забезпечуючи безпеку і конфіденційність даних.

Для ефективного контролю та виявлення проблем з продуктивністю та безпекою мережі, рекомендується використовувати спеціальні інструменти моніторингу мережі. Це дозволить оперативно виявляти потенційні проблеми та здійснювати вчасну реакцію, що збереже час і зусилля в усуненні неполадок та забезпечить ефективну роботу мережі.

Крім того, необхідно мати план відновлення після катастрофи, який включає конкретні кроки для повернення мережі до нормального операційного стану в разі відключень мережі або кібератак. Цей план повинен бути ретельно продуманим і містити інструкції щодо відновлення зв'язку та відновлення даних, щоб забезпечити максимально швидке відновлення нормальної роботи мережі [18].

COMFY може розширити свою мережу, відкривши нові крамниці в різних місцях, що дозволить їй залучити більшу кількість клієнтів. Компанія може розглянути можливість розширення до нових міст або відкриття крамниць у нових районах існуючих міст. Крім того, можуть бути розглянуті альтернативні формати крамниць, такі як невеликі магазини або тимчасові, чи навпаки, зробити велике філію повноцінного магазину.

Зробивши крамниці більш сучасними і привабливими. Компанія може розглянути можливість оновлення дизайну магазинів, встановлення нового освітлення та світильників. Крім того, COMFY може впровадити нові функції, такі як станції самообслуговування та інтерактивні дисплеї. Станції самообслуговування дають змогу клієнтам перевіряти свої покупки без необхідності стояти в черзі до каси. Інтерактивні дисплеї дозволяють клієнтам отримати додаткову інформацію про продукти шляхом дотику або взаємодії з ними.

COMFY може вкладати в технології для поліпшення своєї діяльності. Наприклад, компанія може використовувати системи кас для відстеження запасів і продажів в режимі реального часу або впровадити електронну комерцію для продажу товарів в Інтернеті. Використання систем кас дозволяє магазинам миттєво відстежувати запаси і продажі, забезпечуючи точну інформацію про наявність

товарів. Електронна комерція дозволяє магазинам розширити свій охоплення, продаючи свої товари через Інтернет та привертаючи більш широке коло клієнтів.

Укладання партнерських угод з іншими підприємствами з метою надання клієнтам знижок та акційних пропозицій. Наприклад, магазин може встановити партнерство з фірмою, яка спеціалізується на благоустрої будинків, щоб надавати знижки на послуги монтажу. Також, наприклад співпраця з кредитною компанією, щоб надавати клієнтам знижки на їхні покупки при використанні певних кредитних карт. Ці партнерства допомагають залучити клієнтів та забезпечити їм більш вигідні умови покупок.

Впровадження мобільної торгівлі, що дозволить клієнтам здійснювати покупки зі своїх мобільних пристроїв. Це спрощує процес покупки товарів від, навіть якщо клієнти не знаходяться неподалік від магазину. Мобільна торгівля може бути доступна через веб-сайт або мобільний додаток COMFY.

6.1 Робота під час військового стану

Комп'ютерна мережа COMFY була критичною частиною роботи крамниць під час війни в Україні, дозволяючи продовжувати комунікувати всередині мережі, відстежувати товар і забезпечувати обслуговування клієнтів навіть у розпал хаосу і зриву війни.

Комп'ютерна мережа COMFY є свідченням стійкості українського народу та його здатності адаптуватися та долати навіть найскладніші виклики. Добре спроектована мережа відіграла важливу роль для крамниць продовжуючи працювати під час війни і допомогла забезпечити людям України доступ до необхідних їм товарів і послуг.

Мережа COMFY магазинів використовувалась під час війни для надання підтримки у кількох важливих аспектах:

- забезпечення зв'язку між філіями. Це було критично для координації доставки товарів і послуг, а також для обміну інформацією про війну.

- можливість відстежувати товари у крамницях. Це дозволяло впевнитися, що товари, необхідні людям, були наявні, навіть при обмежених поставках.

- забезпечення обслуговування клієнтів у крамницях. Це було важливо для надання допомоги переселенцям під час війни і надання інформації про ситуацію війни та порад щодо безпеки.

Команда ІТ-фахівців з COMFY та провідна компанія з кібербезпеки спільно розробили мережу, яка використовує різноманітні заходи безпеки для захисту від кібератак. Вона включає в себе використання брандмауерів, систем виявлення вторгнень та шифрування. Крім того, мережа була спроектована з урахуванням стійкості до фізичних пошкоджень, таких як відключення електроенергії або повені. Ця мережа використовується крамницями для обслуговування клієнтів, відстеження інвентаризації та координації доставки товарів і послуг під час війни в Україні. Мережа COMFY є важливою складовою роботи крамниць і відіграє життєво важливу роль у забезпеченні безперебійної роботи компанії під час конфлікту.

Ось додаткові деталі про заходи безпеки, що використовуються в мережі:

- використання брандмауера для блокування несанкціонованого доступу до мережі.

- використання системи виявлення вторгнень для постійного моніторингу мережі на підозрілу активність.

- застосування шифрування для захисту конфіденційних даних.

- розробка мережі з урахуванням стійкості до фізичних пошкоджень, забезпечення енергопостачання від резервного генератора та розташування мережевого обладнання в захищеному місці.

Комп'ютерна мережа COMFY є цінним активом для народу України. Мережа відіграла важливу роль у допомозі магазинам продовжувати працювати під час війни і допомогла забезпечити людям України доступ до необхідних їм товарів і послуг.

7 ТЕСТУВАННЯ МЕРЕЖІ

7.1 Тестування всередині підмереж

Тестування мережі потрібно розбити на декілька пунктів, щоб перевірити працездатність кожної із функцій які були налаштовані в даній мережі. За стандартом, вся мережа налаштована так, щоб у кожний пристрій мав доступ до будь якого іншого пристрою в свої підмережі, чи в іншій, але перевірятися все на готовій мережі з обмеженнями, тільки тих пристроїв до яких є доступ.

Спочатку перевіримо доступ пристроїв всередині філій, Для цього використаємо утиліту ping, що надсилає ICMP запити на вказану адресу. Всередині підмережі всі пристрої можуть взаємодіяти між собою, окрім тестових пристроїв, яким дана інша підмережа. Обравши пристрій Laptop1, якому дана IP-адреса 192.168.1.8, переходимо до вкладці Desktop та обираємо Command Prompt де прописуємо IP-адреси пристроїв MAIN1(192.168.1.2) та Laptop 2 (192.168.1.6) лістинг 7.1. Ці ж самі налаштування допустимі для інших філій.

Лістинг 7.1 – Результати виконання команди на Laptop 1

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=102ms TTL=128
Reply from 192.168.1.2: bytes=32 time=18ms TTL=128
Reply from 192.168.1.2: bytes=32 time=57ms TTL=128
Reply from 192.168.1.2: bytes=32 time=67ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 102ms, Average = 61ms

C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=78ms TTL=128
Reply from 192.168.1.6: bytes=32 time=13ms TTL=128
```

Продовження лістингу 7.1

```
Reply from 192.168.1.6: bytes=32 time=64ms TTL=128  
Reply from 192.168.1.6: bytes=32 time=9ms TTL=128
```

```
Ping statistics for 192.168.1.6:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 9ms, Maximum = 78ms, Average = 41ms
```

7.3 Тестування LAN

DNS працює тільки між філіями COMFY1 – COMFY2 та COMFY3 COMFY4. Для перевірки працездатності перейдемо з пристрою MAIN4 в четвертій філії на WEB-сторінку Server2. В вкладці Desktop обираємо WEB browser та переходимо за посиланням COMFY.com (рис 7.1)

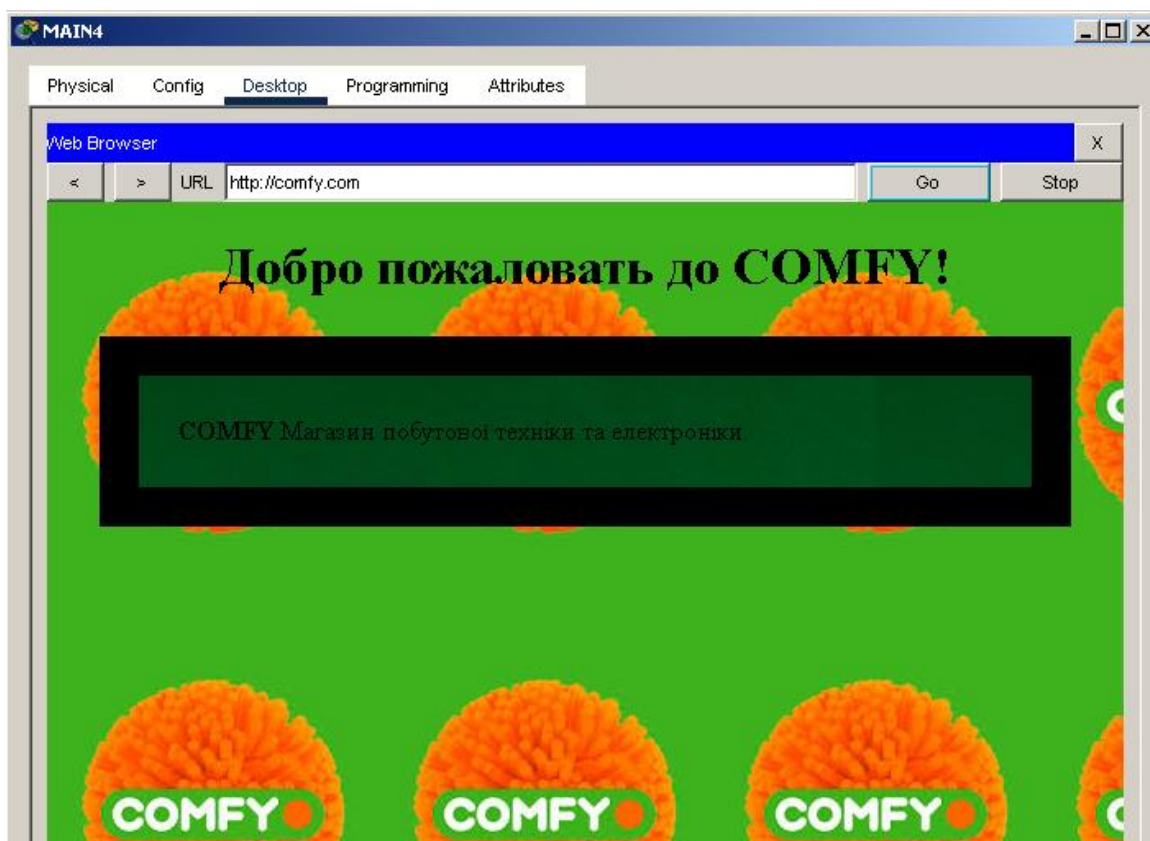


Рисунок 7.1 – Сторінка за посилання comfy.com

VLAN був встановлений, щоб створити внутрішню підмережу, яка застосовується для демонстраційних пристроїв. Він налаштований так що, наприклад, пристрій TV3 в другій філії має доступ лише до MAIN2 (192.168.1.70) та демонстраційних пристроїв, до всіх інших доступ обмежений ,(лістинг 7.2) (192.168.1.68 не демонстраційний пристрій).

Лістинг 7.2 Результати виконання команди TV3

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.70

Pinging 192.168.1.70 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.70: bytes=32 time<1ms TTL=127
Reply from 192.168.1.70: bytes=32 time=1ms TTL=127
Reply from 192.168.1.70: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.1.70:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>ping 192.168.1.68

Pinging 192.168.1.68 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.68:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

7.2 Тестування WAN

Frame-Relay в даній мережі налаштований так, що кожна філія має доступ до будь якої іншої. Для цього з головного пристрою MAIN1перевіримо доступ до

Audio2 (192.168.1.67), який знаходиться в другій філії, та Server2 (192.168.1.130), який знаходиться в третій філії (лістинг 7.2)

Лістинг 7.3 – Результати виконання команди на MAIN1

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.67: bytes=32 time=78ms TTL=126
Reply from 192.168.1.67: bytes=32 time=16ms TTL=126
Reply from 192.168.1.67: bytes=32 time=12ms TTL=126
Reply from 192.168.1.67: bytes=32 time=4ms TTL=126
Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 78ms, Average = 27ms

C:\>ping 192.168.1.130

Pinging 192.168.1.130 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.130: bytes=32 time=33ms TTL=126
Reply from 192.168.1.130: bytes=32 time=32ms TTL=126
Reply from 192.168.1.130: bytes=32 time=32ms TTL=126

Ping statistics for 192.168.1.130:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 32ms, Maximum = 33ms, Average = 32ms
```

Відеокамери налаштовані так, що мають доступ тільки до сервера. Оскільки інформація передається між філіями, то бажано щоб вона була в зашифрованому вигляді. Так між COMFY1 – COMFY2 та COMF3 – COMFY4 було встановлено VPN IPsec. Нижче представлений приклад кількості зашифрованих даних до передачі (рис. 7.2) та після (рис. 7.3) командою `show crypto ipsec sa`.

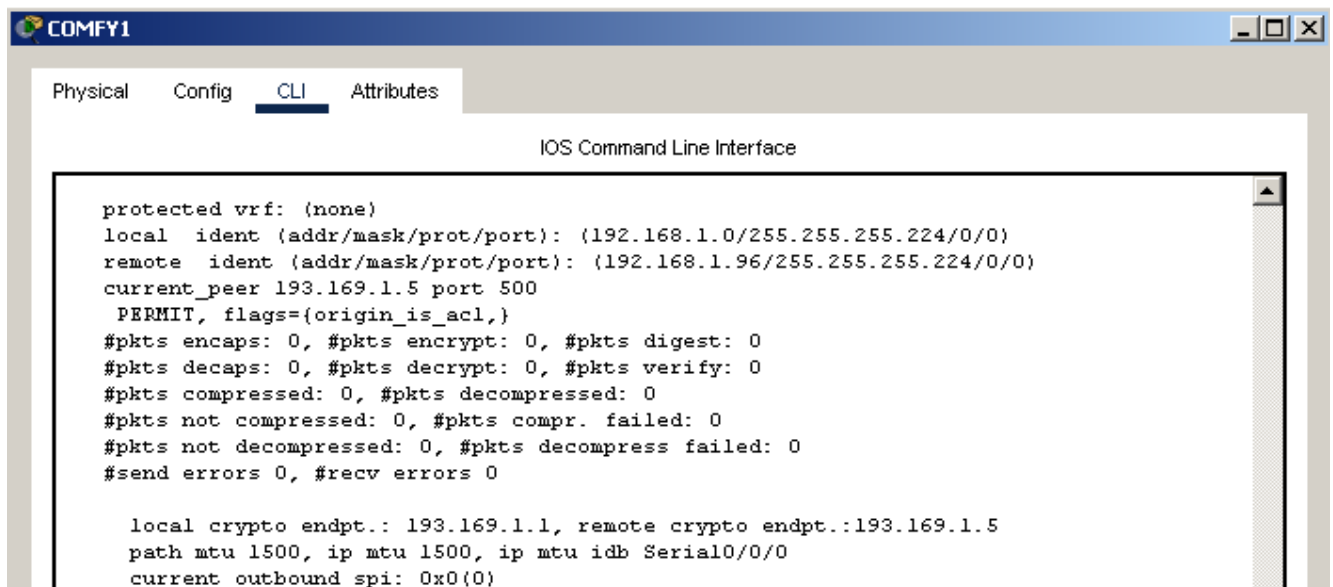


Рисунок 7.2 – Кількість зашифрованих пакетів до передачі

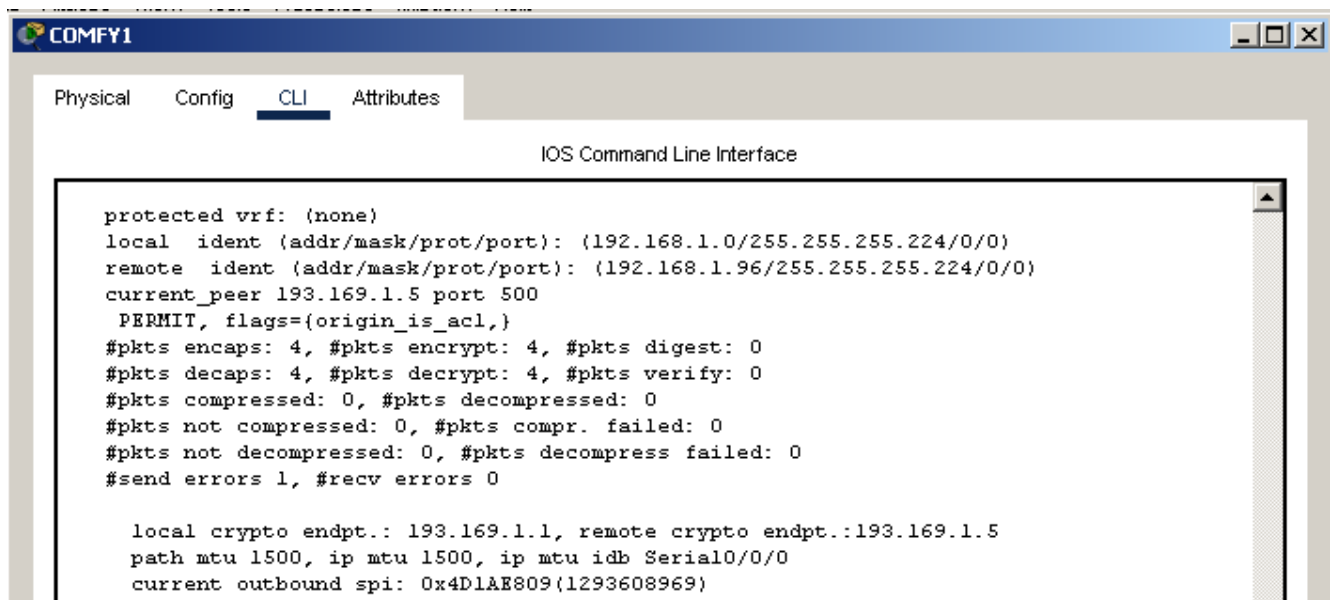


Рисунок 7.3 – Кількість зашифрованих пакетів після передачі

ВИСНОВКИ

Створення даної або подібної розподіленої мережі на декілька філій крамниць побутової техніки та електроніки «COMFY» є дуже необхідним, та надає можливості взаємодіяти між пристроями всередині філій або між ними. Для проектування та створення мережі було проаналізовано поставлене завдання та потреби, розглянуто структуру мережі в цілому та визначено потрібну швидкість каналів зв'язку. Крім того, вибрано необхідне обладнання та розроблено необхідну топологію мережі.

Для того щоб спростити та прискорити підключення нових пристроїв, на кожному пристрої було використано динамічні IP-адреси. Оскільки кожній філії потрібен постійний доступ до інформації складу з товарами, на сервері було організовано DNS. Для того щоб об'єднати декілька демонстративних пристроїв в одну мережу на комутаторі було налаштовано VLAN. А для обмеження доступу до камер встановлено ACL.

Щоб не використовувати додаткові ресурси та підтримувати мережу на безпечному рівні, меж маршрутизаторами філій було організовано статичну маршрутизацію. Між філіями було налаштовано VPN IPsec для передачі відеоінформації меж філіями на сервер в безпечному зашифрованому режимі. Між самими філіями організований інтернет зв'язок на технології Frame-Relay, що дає змогу комунікувати всім філіям навіть якщо в одній з них трапиться нештатна ситуація.

Після завершення проектування була створена повністю налаштована та працездатна комп'ютерна мережа, що значно полегшить та покращить роботу крамниць «COMFY». Це дозволить оптимізувати процеси управління, контролю та обліку товарів, а також покращить якість обслуговування клієнтів. Крім того, створення цієї мережі дозволить вести моніторинг стану обладнання та системи безпеки в реальному часі.

Після завершення проектування була створена повністю налаштована і функціональна комп'ютерна мережа. Це значно полегшить і поліпшить роботу магазинів COMFY. Він дозволить оптимізувати процеси управління, контролю та обліку товарів, а також підвищити якість обслуговування клієнтів. Крім того, створення цієї мережі дозволить контролювати стан обладнання та систем безпеки в режимі реального часу.

Мережа також розрахована на роботу в надзвичайних ситуаціях, таких як воєнний стан, коли може не бути світла, а для людей встановлять спеціальні зарядні станції. Це дозволить людям залишатися на зв'язку і інформуватися під час кризи

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Історія створення та факти мережі крамниць COMFY. URL: <https://comments.ua/ua/dossier/item/company/19-comfy.html> (дата звертання 03.05.2023)

2 Як створити ефективну мережу. // Cisco. URL: https://www.cisco.com/c/dam/global/ru_ua/assets/ingswitchingbrochure_online_ukr_72.pdf (дата звертання 03.05.2023)

3 Розбиття мереж на підмережі за допомогою маски підмережі. URL: http://ni.biz.ua/4/4_16/4_164387_razbienie-setey-na-podseti-s-pomoshchyu-maski-podseti.html (дата звертання 03.05.2023)

4 Приклад розрахунку кількості хостів та підмереж на основі IP-адреси та маски. URL: <https://help.keenetic.com/hc/uk/articles/213965829-Приклад-розрахунку-кількості-хостів-та-підмереж-на-основі-IP-адреси-та-маски> (дата звертання 03.05.2023)

5 В. М. Антонов. Сучасні комп'ютерні системи. «МК-Прес» Київ. 2005 рік – 476 с.

6 Організація комп'ютерних мереж. // Підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с

7 Що таке VLAN: логіка, технологія і налаштування. // Реалізація VLAN в пристроях CISCO. URL: <https://e-server.com.ua/uk/poradi/shho-take-vlan-logika-tehnologija-i-nalashtuvannja-realizacija-vlan-v-pristrojah-cisco> (дата звертання 06.05.2023)

8 Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide // D. Hucaby. – 2nd Edition. – USA: Cisco Press, 2015. – 578 p.

9 VLAN Configuration Commands Step by Step Explained. URL: <https://www.computernetworkingnotes.com/ccna-study-guide/vlan-configuration-commands-step-by-step-explained.html> (дата звертання 06.05.2023)

10 Що таке DNS? URL: <https://2ip.ua/ua/blog/dns> (дата звертання 06.05.2023)

11 access control list (ACL). URL: <https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL> (дата звертання 06.05.2023)

12 Configure and Filter IP Access Lists. URL: <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html> (дата звертання 08.05.2023)

13 Основи статичної маршрутизації URL: https://web.posibnyky.vntu.edu.ua/fiki/3yarovijk_komp_merezhi/4.6.html (дата звертання 08.05.2023)

14 What is IPsec? // How IPsec VPNs work. URL: <https://www.cloudflare.com/learning/network-layer/what-is-ipsec/> (дата звертання 08.05.2023)

15 Configure a LAN-to-LAN IPsec Tunnel Between Two Routers. URL: <https://www.cisco.com/c/en/us/support/docs/routers/1700-series-modular-access-routers/71462-rtr-l2l-ipsec-split.html> (дата звертання 08.05.2023)

16 How does Frame Relay Work? URL: <https://www.geeksforgeeks.org/how-does-frame-relay-work/> (дата звертання 08.05.2023)

17 Мережева інфраструктура: основні відомості, об'єкти та проектування. URL: <https://bigbro.com.ua/merezheva-infrastruktura-osnovni-vidomosti-obyekti-ta-proektuvannya/4/> (дата звертання 11.05.2023)

18 Лекція 3. // Структура комп'ютерної мережі. URL: https://elib.lntu.edu.ua/sites/default/files/elib_upload/Savarin_Pavlo_ENP/teoretic/lec3.html (дата звертання 11.05.2023)

19 Комунікації рітейлу під час війни. // Принципи та кейси Comfy. URL: <https://rau.ua/dosvid/komunikacii-comfy-pid-chas-vijni/> (дата звертання 11.05.2023)

ДОДАТОК А

Лістинг А.1 – Фрагмент коду налаштування DHCP для філії CONFY4.

```
CONFY4(config)#interface gig0/0
CONFY4(config-if)#service dhcp
CONFY4(config)#ip dhcp pool Dv4
CONFY4(dhcp-config)#network 192.168.1.192 255.255.255.224
CONFY4(dhcp-config)#default-router 192.168.1.193
CONFY4(dhcp-config)#dns-server 192.168.1.130
CONFY4(dhcp-config)#exit
CONFY4(dhcp-config)#interface gig0/1
CONFY4(config-if)#service dhcp
CONFY4(config)#ip dhcp pool VC4
CONFY4(dhcp-config)#network 192.168.1.224 255.255.255.224
CONFY4(dhcp-config)#default-router 192.168.1.225
CONFY4(dhcp-config)#dns-server 192.168.1.130
```

Лістинг А.2 – Встановлення розширеного ACL для CONFY2, CONFY3 та CONFY4

```
CONFY2>ena
CONFY2#conf t
CONFY2(config)#ip access-list extended VC2
CONFY2(config-ext-nacl)# permit ip 192.168.1.96 0.0.0.31 host
192.168.1.3
CONFY2(config-ext-nacl)#permit ip 192.168.1.64 0.0.0.31 192.168.1.0
0.0.0.31
CONFY2(config-ext-nacl)#permit ip 192.168.1.64 0.0.0.31 192.168.1.128
0.0.0.31
CONFY2(config-ext-nacl)#permit ip 192.168.1.64 0.0.0.31 192.168.1.192
0.0.0.31
CONFY2(config-ext-nacl)# permit ip any host 255.255.255.255
CONFY2(config-ext-nacl)# permit ip 192.168.1.64 0.0.0.31 host
192.168.1.3
CONFY2(config-ext-nacl)# permit ip 192.168.1.64 0.0.0.31 host
192.168.1.2
CONFY2(config-ext-nacl)#permit ip 192.168.1.64 0.0.0.31 host
192.168.1.133
CONFY2(config-ext-nacl)#permit ip 192.168.1.64 0.0.0.31 host
192.168.1.197
CONFY2(config-ext-nacl)#deny ip any any
CONFY2(config-ext-nacl)#exit
CONFY2(config)#int s0/1/0
CONFY2(config-if)#ip access-group VC2 out
CONFY2(config-if)#exit
CONFY2(config)#ip access-list extended VLAN2
CONFY2(config-ext-nacl)#permit ip host 192.168.1.70 192.168.2.32
0.0.0.31
```

Продовження лістингу А.2

```

COMFY2(config-ext-nacl)#permit ip any host 255.255.255.255

COMFY2(config-ext-nacl)#permit ip 192.168.1.64 0.0.0.31 192.168.1.0
0.0.0.31
COMFY2(config-ext-nacl)#permit ip 192.168.1.64 0.0.0.31 192.168.1.128
0.0.0.31
COMFY2(config-ext-nacl)#permit ip 192.168.1.64 0.0.0.31 192.168.1.192
0.0.0.31
COMFY2(config-ext-nacl)#permit ip any host 255.255.255.255
COMFY2(config-ext-nacl)#deny ip any any
COMFY2(config-ext-nacl)#exit
COMFY2(config)#int gig0/0
COMFY2(config-if)#ip access-group VLAN2 in
COMFY2(config-ext-nacl)#exit
COMFY2(config-if)#end
COMFY2#wr

COMFY3>ena
COMFY3#conf t
COMFY3(config)#ip access-list extended VC3
COMFY3(config-ext-nacl)#permit ip any host 255.255.255.255
COMFY3(config-ext-nacl)#permit ip host 192.168.1.130 192.168.1.224
0.0.0.31
COMFY3(config-ext-nacl)#permit ip host 192.168.1.130 192.168.1.160
0.0.0.31
COMFY3(config-ext-nacl)#permit ip host 192.168.1.133 192.168.1.0
0.0.0.31
COMFY3(config-ext-nacl)#permit ip host 192.168.1.133 192.168.1.64
0.0.0.31
COMFY3(config-ext-nacl)#permit ip host 192.168.1.133 192.168.1.192
0.0.0.31
COMFY3(config-ext-nacl)#permit ip host 192.168.1.130 192.168.1.192
0.0.0.31
COMFY3(config-ext-nacl)#permit ip 192.168.1.128 0.0.0.31 host
192.168.1.2
COMFY3(config-ext-nacl)#permit ip 192.168.1.128 0.0.0.31 host
192.168.1.70
COMFY3(config-ext-nacl)#permit ip 192.168.1.128 0.0.0.31 host
192.168.1.197
COMFY3(config-ext-nacl)#deny ip any any
COMFY3(config-ext-nacl)#exit
COMFY3(config)#int s0/0/1
COMFY3(config-if)#ip access-group VC3 out
COMFY3(config-if)#exit
COMFY3(config)#ip access-list extended VLAN3
COMFY3(config-ext-nacl)#permit ip any host 255.255.255.255
COMFY3(config-ext-nacl)#permit ip host 192.168.1.133 192.168.2.64
0.0.0.31
COMFY3(config-ext-nacl)#permit ip host 192.168.1.130 192.168.1.224
0.0.0.31

```

Продовження лістингу А.2

```

COMFY3(config-ext-nacl)#permit ip host 192.168.1.130 192.168.1.160
0.0.0.31
COMFY3(config-ext-nacl)#permit ip 192.168.1.128 0.0.0.31 192.168.1.0
0.0.0.31
COMFY3(config-ext-nacl)#permit ip 192.168.1.128 0.0.0.31 192.168.1.64
0.0.0.31
COMFY3(config-ext-nacl)#permit ip 192.168.1.128 0.0.0.31
192.168.1.192 0.0.0.31
COMFY3(config-ext-nacl)#deny ip any any
COMFY3(config-ext-nacl)#exit
COMFY3(config)#int gig0/0
COMFY3(config-if)#ip access-group VLAN3 in
COMFY3(config-if)#end
COMFY3#wr

COMFY4>ena
COMFY4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
COMFY4(config)#ip access-list extended VC4
COMFY4(config-ext-nacl)#permit ip 192.168.1.224 0.0.0.31 host
192.168.1.130
COMFY4(config-ext-nacl)#permit ip any host 255.255.255.255
COMFY4(config-ext-nacl)#permit ip host 192.168.1.197 192.168.1.0
0.0.0.31
COMFY4(config-ext-nacl)#permit ip host 192.168.1.197 192.168.1.64
0.0.0.31
COMFY4(config-ext-nacl)#permit ip host 192.168.1.197 192.168.1.128
0.0.0.31
COMFY4(config-ext-nacl)#permit ip 192.168.1.192 0.0.0.31 host
192.168.1.130
COMFY4(config-ext-nacl)#permit ip 192.168.1.192 0.0.0.31 host
192.168.1.2
COMFY4(config-ext-nacl)#permit ip 192.168.1.192 0.0.0.31 host
192.168.1.70
COMFY4(config-ext-nacl)#permit ip 192.168.1.192 0.0.0.31 host
192.168.1.133
COMFY4(config-ext-nacl)#deny ip any any
COMFY4(config-ext-nacl)#exit
COMFY4(config)#int s0/1/1
COMFY4(config-if)#ip access-group VC4 out
COMFY4(config-if)#exit
COMFY4(config)#ip access-list extended VLAN4
COMFY4(config-ext-nacl)#permit ip host 192.168.1.197 192.168.2.128
0.0.0.31
COMFY4(config-ext-nacl)#permit ip any host 255.255.255.255
COMFY4(config-ext-nacl)#permit ip 192.168.1.192 0.0.0.31 192.168.1.0
0.0.0.31
COMFY4(config-ext-nacl)#permit ip 192.168.1.192 0.0.0.31 192.168.1.64
0.0.0.31
COMFY4(config-ext-nacl)#permit ip 192.168.1.192 0.0.0.31
192.168.1.128 0.0.0.31

```

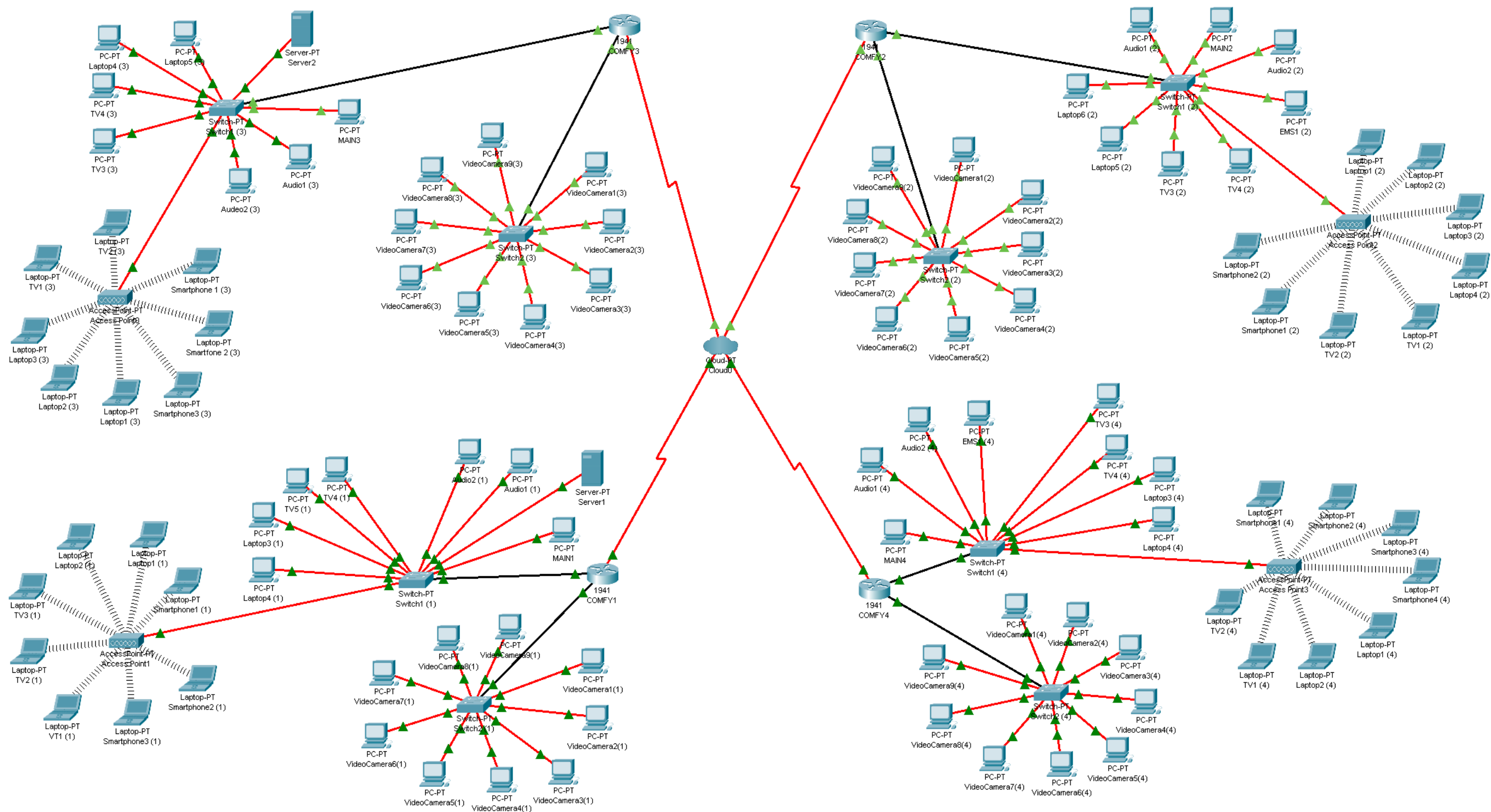
Продовження лістингу А.2

```
COMFY4(config-ext-nacl)#deny ip any any
COMFY4(config-ext-nacl)#exit
COMFY4(config)#int gig0/0
COMFY4(config-if)#ip access-group VLAN4 in
COMFY4(config-if)#end
COMFY4#wr
```

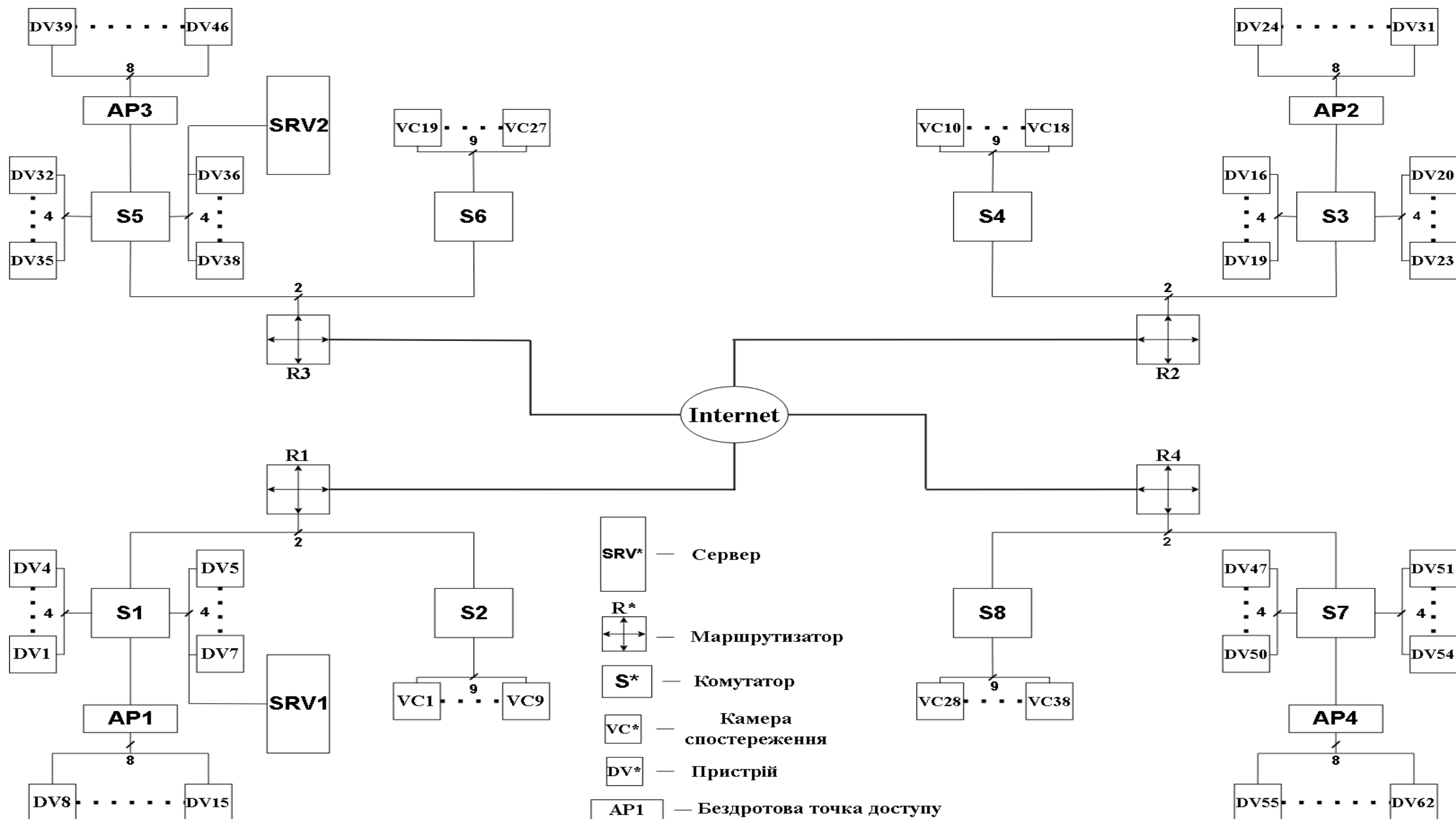
Лістинг А.3 – Фрагмент коду VPN IPsec для філій COMFY3 та COMFY4

```
COMFY3>ena
COMFY3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
COMFY3(config)#crypto isakmp policy 10
COMFY3(config-isakmp)#encryption aes
COMFY3(config-isakmp)#authentication pre-share
COMFY3(config-isakmp)#group 2
COMFY3(config-isakmp)#exit
COMFY3(config)#crypto isakmp key COMFY4 address 193.169.1.13
COMFY3(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
COMFY3(config)#crypto map VPN-MAP 2 ipsec-isakmp
COMFY3(config-crypto-map)#description VPN connection to COMFY4
COMFY3(config-crypto-map)#set peer 193.169.1.13
COMFY3(config-crypto-map)#set transform-set VPN-SET
COMFY3(config-crypto-map)#match address 112
COMFY3(config-crypto-map)#exit
COMFY3(config)#int s0/0/1
COMFY3(config-if)#crypto map VPN-MAP

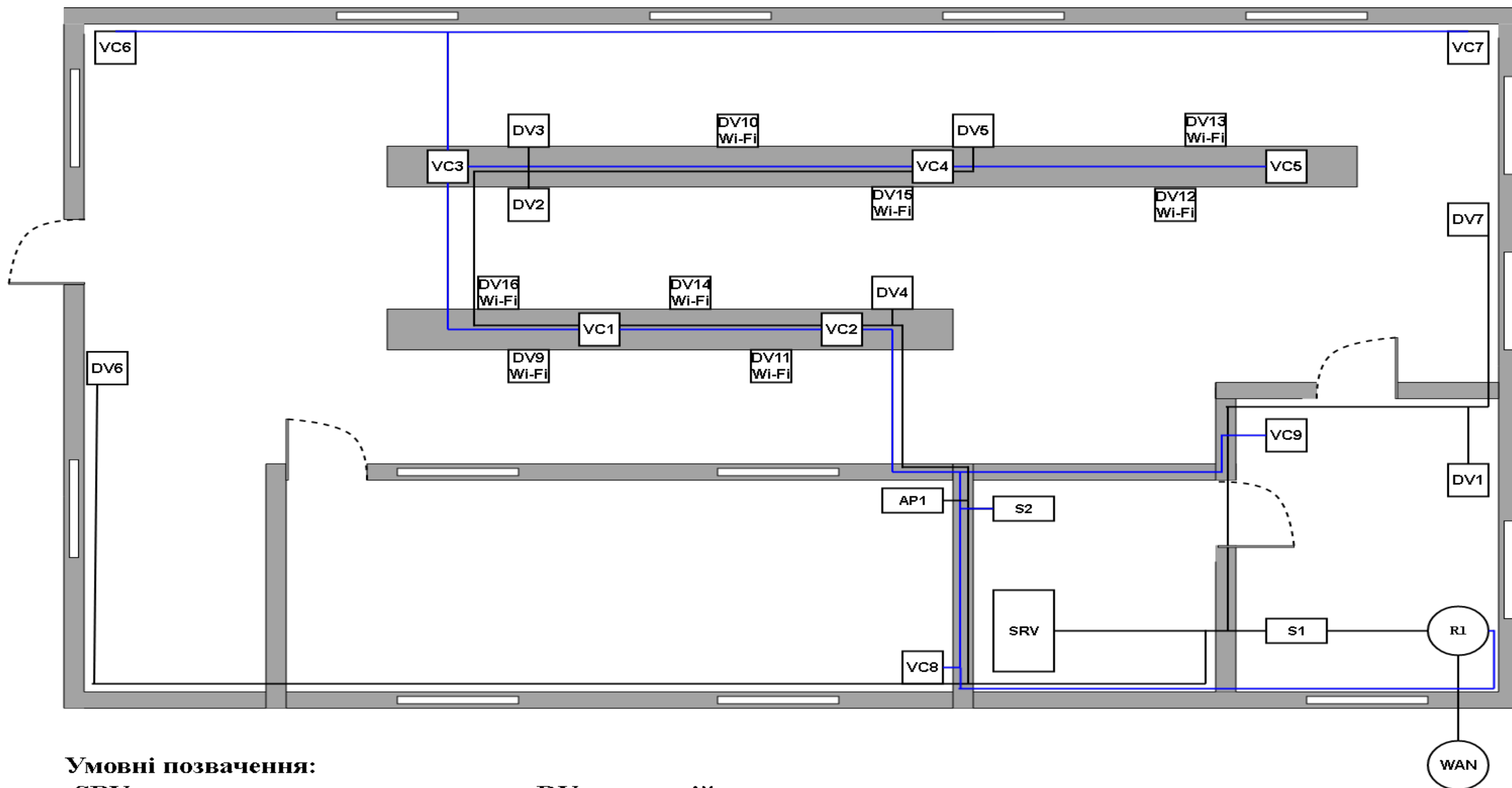
COMFY4>ena
COMFY4#conf t
COMFY4(config)#crypto isakmp policy 10
COMFY4(config-isakmp)#encryption aes
COMFY4(config-isakmp)#authentication pre-share
COMFY4(config-isakmp)#group 2
COMFY4(config-isakmp)#exit
COMFY4(config)#crypto isakmp key COMFY4 address 193.169.1.9
COMFY4(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
COMFY4(config)#crypto map VPN-MAP 2 ipsec-isakmp
COMFY4(config-crypto-map)#description VPN connection to COMFY3
COMFY4(config-crypto-map)#set peer 193.169.1.9
COMFY4(config-crypto-map)#set transform-set VPN-SET
COMFY4(config-crypto-map)#match address 113
COMFY4(config-crypto-map)#exit
COMFY4(config)#int s0/1/1
COMFY4(config-if)#crypto map VPN-MAP
```



					13.02070849.51907 E2					
					Розробка розподіленої мережі крамниць побутової техніки та електроніки COMFY Функціональна схема розподіленої мережі «COMFY»	Літ.		Маса	Масштаб	
Зм	Лист	№ докум.	Підп.	Дата						
	Розроб.	Іванов О.В.								
	Перевір.	Киричек Г.Г.								
	Т. контр.									
	Н. контр.	Щербак Н.В.								
	Затв.	Кудерметов Р.В.								
						НУ «Запорізька політехніка» КНТ-519				



					13.02070849.51907 E1						
					Розробка розподіленої мережі крамниць побутової техніки та електроніки COMFY Структурна схема розподіленої мережі «COMFY»	Літ.			Маса	Масштаб	
Зм	Лист	№ докум.	Підп.	Дата							
Розроб.		Іванов О.В.									
Перевір.		Киричек Г.Г.									
Т. контр.											
						Лист. 1			Листів 1		
Н. контр.		Щербак Н.В.				НУ «Запорізька політехніка» КНТ-519					
Затв.		Кудрметов Р.В.									



Умовні позначення:

SRV - сервер

AP - бездротова точка доступу

VC - камера відео спостереження

DV - пристрій

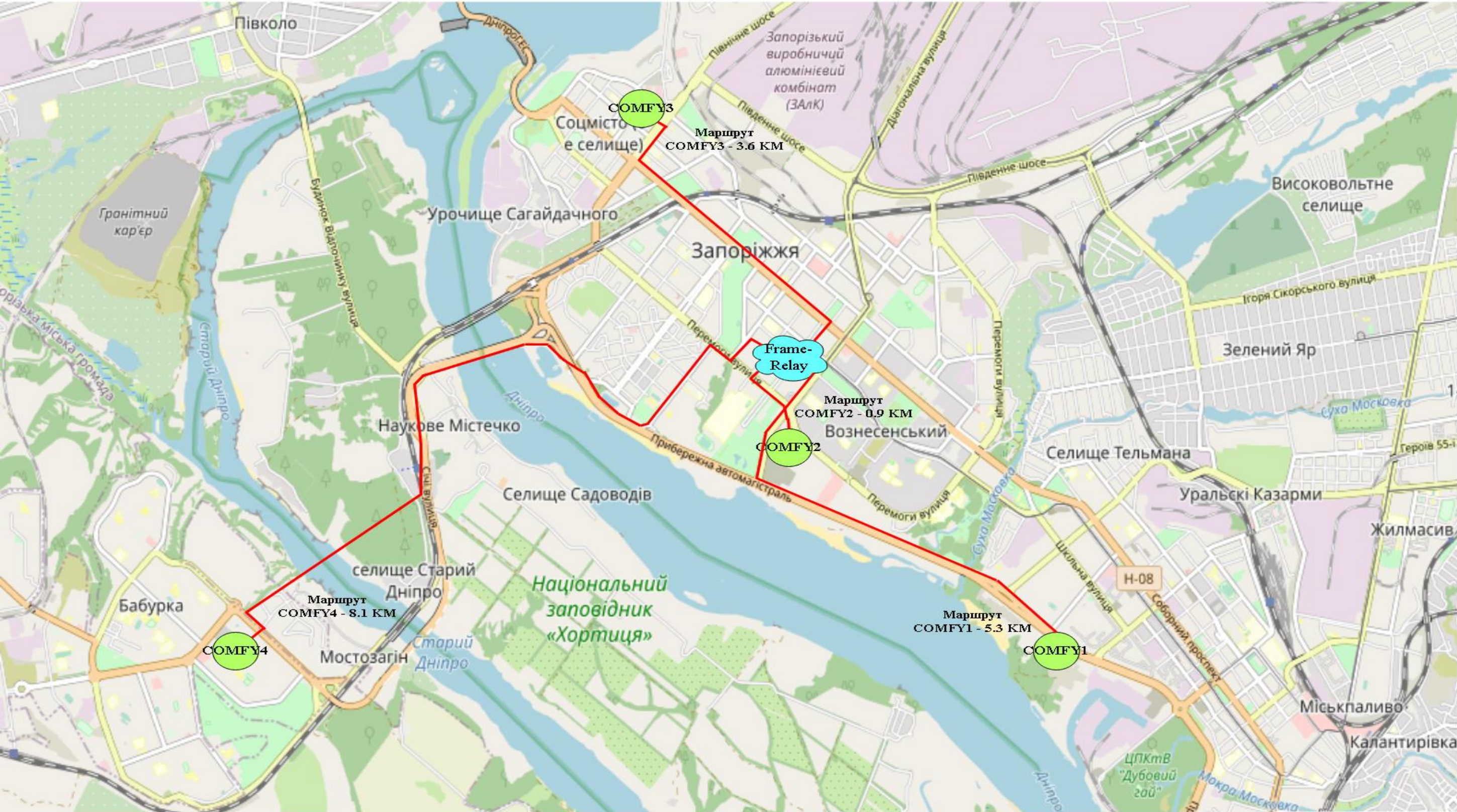
S - комутатор

R - маршрутизатор

WAN - вихід в

глобальну мережу

					13.02070849.51907 E5				
					Розробка розподіленої мережі крамниць побутової техніки та електроніки COMFY	Літ.		Маса	Масштаб
Зм	Лист	№ докум.	Підп.	Дата					
Розроб.		Іванов О.В.							
Перевір.		Киричук Г.Г.							
Т. контр.					Монтажна схема розподіленої мережі «COMFY»	Лист. 1		Листів 1	
Н. контр.		Щербак Н.В.				НУ «Запорізька політехніка» КНТ-519			
Затв.		Кудрметов Р.В.							



					13.02070849.51907 ПЛ1						
					Розробка розподіленої мережі крамниць побутової техніки та електроніки COMFY	Літ.			Маса	Масштаб	
Зм	Лист	№ докум.	Підп.	Дата							
Розроб.		Іванов О.В.									
Перевір.		Киричук Г.Г.									
Т. контр.											
					Карта мережі крамниць розподіленої мережі «COMFY»	Лист. 1			Листів 1		
Н. контр.		Щербак Н.В.				НУ «Запорізька політехніка» КНТ-519					
Затв.		Кудрметов Р.В.									