МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Факультет електроніки та інформаційних технологій
Кафедра комп’ютерних наук

Кваліфікаційна робота магістра

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА ТЕХНОЛОГІЯ ПРОЄКТУВАННЯ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ETHERNET З ІНТЕГРАЦІЄЮ РЕАЛЬНОГО ТА ВІРТУАЛЬНОГО ОБЛАДНАННЯ CISCO

Здобувач освіти гр. ІК.мз-11с Дмитро ВЕЛИКОДНИЙ

Науковий керівник,
к.т.н., доцент Наталія БАРЧЕНКО

В.о. завідувача кафедри
к.т.н., доцент Ігор ШЕЛЕХОВ

Суми 2022

Сумський державний університет
(назва вузу)

Факультет *ЕлІТ* Кафедра *Комп'ютерних наук*
Спеціальність *«122 - Комп'ютерні науки»*

Затверджую:
зав.кафедрою _____
_____
"_____" _____ 20___р.

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТОВІ

Великодному Дмитру Володимировичу
(прізвище, ім'я, по батькові)

1. Тема проєкту (роботи) *Інформаційно-комунікаційна технологія проєктування мультисервісної мережі Ethernet з інтеграцією реального та віртуального обладнання Cisco*

затверджую наказом по інституту від "____" _____ 20 ___ р. № _____

2. Термін здачі студентом закінченого проєкту (роботи)_____

3. Вхідні данні до проєкту (роботи) _____
_____
_____
_____

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

1) Аналіз предметної області; 2) Постановка задачі та формування завдання дослідження; 3) Аналіз апаратно-програмного мережевого забезпечення, що використовуються для побудови мультисервісних мереж Ethernet; 4)Моделювання мультисервісної мережі з використанням обладнання Cisco та емулятора GNS3; 5) Розробка описової моделі предметної області; 6) Програмна реалізація; 7) Аналіз результатів.

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

6. Консультанти до проєкту (роботи), із значенням розділів проєкту, що стосується їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проєкту (роботи)	Термін виконання проєкту (роботи)	Примітка
1.	Огляд наявних рішень		
2.	Постановка задачі та формування завдань дослідження		
3.	Проєктування та моделювання		
4.	Програмна реалізація		
5.	Оформлення пояснювальної записки до кваліфікаційної магістерської роботи		

Студент – дипломник _____
(підпис)

Керівник проєкту _____
(підпис)

РЕФЕРАТ

Записка: 90 стор., 47 рис., 1 додаток, 16 літературних джерел.

Об'єкт дослідження — мультисервісна мережа Ethernet, побудована на базі віртуальних та реальних роутерів Cisco з підтримкою сервісів VoIP та IPTV.

Мета роботи — розробка інформаційно-комунікаційної технології проєктування мультисервісної мережі Ethernet з інтеграцією реального та віртуального обладнання Cisco, складовою частиною якої є програма для автоконфігурування мережевого обладнання.

Результати — проведено аналіз предметної області в напрямі розробки інформаційно-комунікаційної технології проєктування мультисервісної мережі Ethernet. За результатами дослідження розроблено описову модель предметної області. З метою автоматизації налаштування мультисервісних мереж у середовищі графічного програмування LabVIEW створено програмний додаток, за допомогою якого можна здійснити автоконфігурування мережевого обладнання, що надало можливість значно комфортніше, надійніше та швидше здійснювати автоконфігурування основних компонентів сучасних комп'ютерних мереж з підтримкою сервісів IPTV та VoIP. Підтримка функції дзеркалізації портів на L3 комутаторах Catalist 3560 дозволила перехоплювати мережевий трафік та здійснювати його аналіз.

ETHERNET, VoIP, IPTV, GNS3, CISCO, ROUTER, SWITCH, LABVIEW, ГРАФІЧНИЙ ІНТЕРФЕЙС, КОНФІГУРУВАННЯ

ЗМІСТ

ВСТУП

Значне зростання кількості комп'ютерів та мобільних гаджетів спонукає до активного розвитку мережевих технологій, що значно розширюють функціональні можливості комп'ютерів та надають клієнтам доступ до всесвітньої мережі Internet. Обчислювальна мережа несе у собі величезні можливості, а також новий потенційний підйом та значне прискорення виробничого процесу. Все це вимагає вирішення питання організації комп'ютерної мережі, яка повинна відповідати сучасним вимогам і тенденціям та одночасно враховувати сумісність із вже існуючим мережевим обладнанням та перспективи подальшого розширення функціоналу та продуктивності мережі з огляду на появу нових апаратних та програмних рішень.

VoIP (Voice-over-IP або IP-телефонія) – це технологія, яка, завдяки поєднанню набору протоколів передачі голосу та обміну даними, дозволила для організації традиційних функцій спілкування залучити апаратно-програмне забезпечення мереж передачі даних. Такий підхід надав клієнтам можливість значно знизити витрати у порівнянні з традиційною телефонією, при цьому підвищивши якість зв'язку та додавши ряд інтерактивних сервісів.

Сучасним трендом у сфері цифрового телебачення стало інтерактивне IPTV телебачення. IPTV надає клієнтам можливість керувати переглядом мультимедійного контенту, налаштовуючи телевізійний контент під свої бажання та потреби і при цьому надаючи сервіси високої якості та у зручному форматі.

Метою даної роботи є теоретичний огляд інфо-комунікаційної мережі з підтримкою сервісів VoIP та IPTV, а також моделювання такої мережі з використанням симулятора GNS3 та «реального» мережевого обладнання Cisco.

РОЗДІЛ 1. ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ ОГЛЯД

1.1 Маршрутизація у комп'ютерних мережах

Маршрутизація є необхідною складовою частиною функціонування комп'ютерної мережі. Загальними словами маршрутизацію можна описати як процес передачі пакетів між з'єднаними мережами. Маршрутизація у TCP/IP мережах – це частина протоколу IP (Internet Protocol), що використовується у поєднанні з іншими службами мережевих протоколів для забезпечення передачі даних між вузлами [1-2].

Маршрут – це шлях, по якому пакети пересилають від відправника до одержувача. Маршрут визначає тільки сегмент шляху від хосту до шлюзу, або від шлюзу до шлюзу, а не повний шлях, який може пересилати пакети цільовому хосту.

Існує три типи маршрутів:

- маршрут до хосту – визначає шлюз, який може пересилати пакети вказаному хосту в іншій мережі;
- маршрут до мережі – визначає шлюз, який може пересилати пакети іншому хосту вказаної мережі;
- маршрут за замовчуванням – у разі коли не було наведено маршрут до цільового хосту або маршрут до мережі цільового хосту.

Маршрути у мережах можуть створюватися адміністраторами вручну або обчислюватися з використанням протоколів маршрутизації, беручи за основу інформацію про топологію мережі та стан роботи мережевого обладнання. Сформовані маршрути зберігаються в таблиці маршрутизації.

Трафік у мережах поділяють на:

- вхідний (інформація, що надходить в мережу);
- вихідний (інформація, що виходить за межі мережі);

- внутрішній (як правило, обмежений розміром локальної мережі);
- зовнішній (як правило, трафік, що передається у публічній Internet мережі).

Функцію побудови маршрутизації у комп'ютерних мережах виконують спеціалізовані програмно-апаратні засоби – маршрутизатори (роутери). Історично першими роутерами були комп'ютери зі встановленим відповідним програмним забезпеченням. Наразі це спеціалізоване мережеве обладнання заточене під високопродуктивну передачу інформації з додаванням мережевих сервісів автоналаштування, безпеки, а також з наявними широкими можливостями адміністративного контролю.

У TCP/IP мережах передбачено два типи маршрутизації: статична і динамічна. Розглянемо їх нижче.

Статична маршрутизація.

Статична маршрутизація – це різновид маршрутизації, при якій оптимальні маршрути в мережі вказуються у явному вигляді адміністратором маршрутизатора під час його конфігурації. При налаштуванні статичної маршрутизації протоколи динамічної маршрутизації не використовуються, а якщо і присутні, то мають нижчий за неї пріоритет [3].

Статична маршрутизація передбачає ручне додавання IP-маршрутів у системну таблицю маршрутизації і, зазвичай, це робиться через зміну таблиці маршрутизації командою route. Статична маршрутизація надає багато переваг у порівнянні з динамічною маршрутизацією, такі як простота реалізації на невеликих мережах, передбачуваність (таблиця маршрутизації завжди складена завчасно і тому завжди використовується маршрут, який повторюється щоразу з точністю) і низьке навантаження на інші маршрутизатори та мережеві з'єднання. Однак у статичної маршрутизації є й слабкі місця.

При завданні статичного маршруту вказують:

- адресу мережі та маску мережі;

- адресу шлюзу (вузла), який відповідає за подальшу маршрутизацію;
- метрику маршруту.

За наявністю декількох маршрутів до однієї й тієї ж мережі маршрутизатори обирають маршрут, що має мінімальне значення метрики.

За необхідності на маршрутизаторах можна вказати вихідний інтерфейс, через який необхідно надсилати трафік до віддаленої мережі. Окрім цього можна сформувати додаткові умови, згідно з якими буде визначатися маршрут (наприклад, протокол SLA на маршрутизаторах CISCO).

Переваги використання статичної маршрутизації:

- низьке значення навантаження на центральний процесор маршрутизатора;
- простота налаштування, особливо у невеликих мережах;
- передбачуваність у кожен момент часу;
- миттєва готовність, при якій не вимагається інтервал для конфігурування або підлаштування;
- відсутність часових витрат на оброку інформації від протоколів маршрутизації.

Недоліки при використанні статичної маршрутизації:

- відсутність динамічного балансування навантаження;
- незадовільна можливість масштабування мережі. Під'єднання до мережі будь-якого нового сегменту мережі або роутера потребує оновлення записів про маршрути на всіх маршрутизаторах мережі, що при великих масштабах мережі створює значне навантаження на роботу адміністраторів;
- необхідність вести окрему документацію до маршрутів, тому що є проблема синхронізації документації і реальних маршрутів;
- низька стійкість до пошкоджень ліній зв'язку. Особливо, якщо пошкодження відбулося між пристроями другого рівня й порт маршрутизатора не отримує статус down.

У реальних умовах статична маршрутизація використовується в умовах наявності шлюзу за замовчуванням. Окрім того, статична маршрутизація використовується для, так званого, «вирівнювання» роботи маршрутизуючих протоколів в умовах наявності тунелю, щоб маршрутизація трафіку, який створюється тунелем, не проводився через сам тунель [4].

Статична маршрутизація обмежена невеликими мережами і не може масштабуватися. Коли мережа взаємодіє з великим числом мереж, то число шлюзів різко зростає, тому для обслуговування таблиць вручну потрібен значний час. Тому цей тип маршрутизації рекомендується застосовувати тоді, коли ваша мережа взаємодіє з однією або двома іншими мережами.

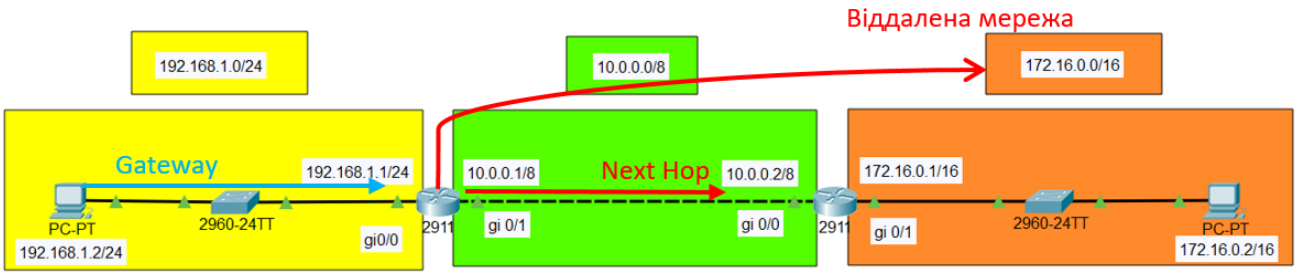


Рисунок 1.1 – Приклад статичної маршрутизації

Динамічна маршрутизація.

Динамічна маршрутизація – вид маршрутизації, у якому таблиця маршрутизації обчислюється автоматично за допомогою протоколів динамічної маршрутизації [4-5].

Динамічна маршрутизація застосовується у великих мережах з декількома можливими IP-маршрутами від джерела до приймача й використовує для цього спеціальні протоколи маршрутизації, такі як RIP, який управляє автоматичним регулюванням таблиць маршрутизації, що і робить динамічну маршрутизацію можливою. Динамічна маршрутизація має ряд переваг над статичною, таких як високий рівень масштабованості і можливість адаптації до збоїв і обривів в мережевих з'єднаннях. Крім того, вона вимагає менше ручного адміністрування

таблиць маршрутизації, оскільки маршрутизатори самі дізнаються один від іншого про своє існування та про доступні маршрути. Ця особливість також виключає можливість внесення помилок в таблицю маршрутів через людський фактор. Динамічна маршрутизація не досконала, оскільки у неї існують слабкі місця, такі як підвищена складність і додаткове навантаження від взаємодії маршрутизаторів, які не дають негайного ефекту кінцевим користувачам, а тільки використовують смугу пропускання мережі [6].

За алгоритмами виділяють:

- дистанційно-векторні протоколи (Distance-vector Routing Protocols):
  - RIP.
- протоколи стану каналів зв'язку (Link-state Routing Protocols):
  - OSPF;
  - IS-IS.
- іноді виділяють третій клас, вдосконалені дистанційно-векторні протоколи (advanced distance-vector), для того, щоб підкреслити суттєві відмінності протоколів від класичних дистанційно-векторних:
  - EIGRP.

Компанія CISCO раніше називала протокол EIGRP змішаним протоколом, однак, за своїми принципами роботи EIGRP дистанційно-векторний протокол.

По області застосування:

- міждоменна маршрутизація:
  - BGP;
- внутрішньодоменна маршрутизації:
  - OSPF;
  - RIP;
  - EIGRP;
  - IS-IS.

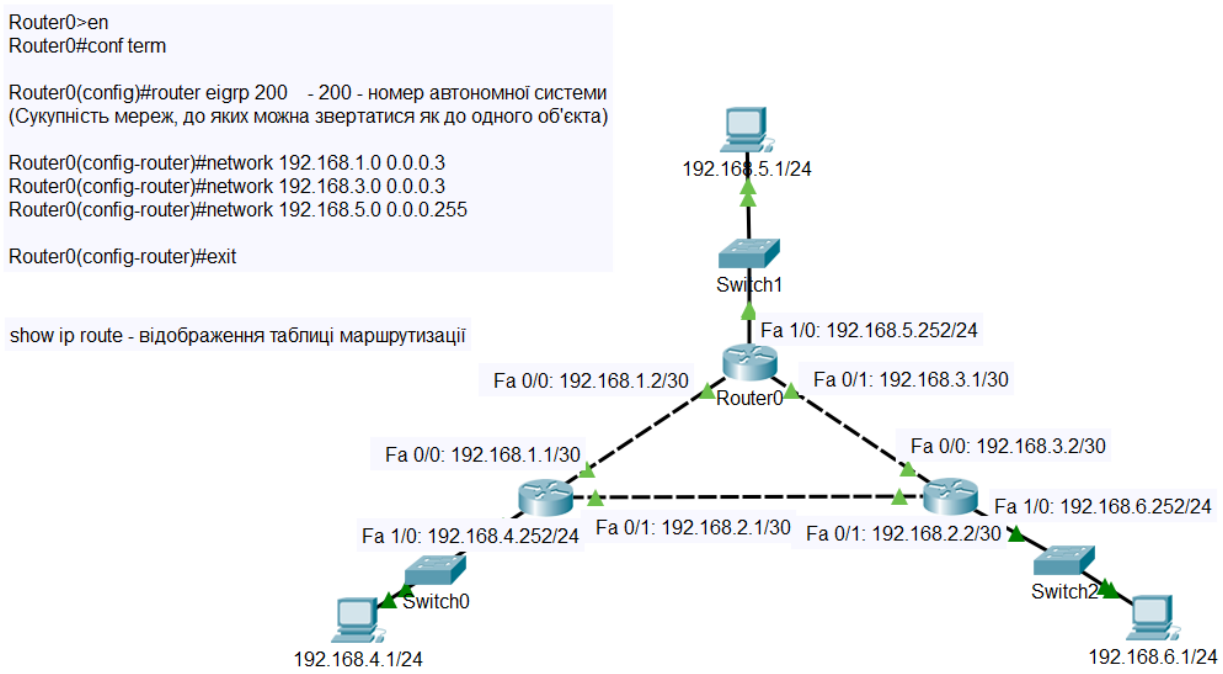


Рисунок 1.2 – Приклад динамічної маршрутизації за протоколом EIGRP

При активації динамічної маршрутизації маршрутизатор формує таблицю оптимальних шляхів передачі до віддаленої мережі, базуючи свій вибір на підставі мінімальної кількості проміжних вузлів (хопів), у тому числі аналізуючи пропускну здатність каналів зв’язку, часові затримки при передачі трафіку тощо. Параметри, що визначають оптимальний маршрут передачі даних, як правило, залежать від типу протоколу маршрутизації та задаються під час конфігурації маршрутизатора. Динамічна маршрутизація автоматично підтримує таблицю маршрутизації роутера в актуальному стані, здійснюючи постійний моніторинг стану оптимальних маршрутів та зміни в топології мережі. У той же час динамічна маршрутизація створює додаткове навантаження на мережеві пристрої, а часті збої у роботі обладнання можуть призводити до ситуацій, коли маршрутизатори мережі не встигають оновити та синхронізувати таблиці маршрутизації, що створює прецеденти з невизначеністю маршрутів або наявністю суперечливої

маршрутної інформації, що у свою чергу, призводить до перевантаження мережі та часткової втрати інформації.

При побудові локальних та корпоративних мереж і подальшому їх під'єднанні до мереж провайдерів, як правило, використовуються протоколи внутрішньої динамічної маршрутизації. Зазвичай, зовнішні протоколи динамічної маршрутизації слід використовувати лише при побудові закритої масштабної за розмірами системи, яка свій зв’язок із зовнішнім світом забезпечує обмеженою кількістю захищених каналів з’єднання [4].

Прикладом сучасного протоколу зовнішньої динамічної маршрутизації можна вважати протокол BGP. Він дозволяє поєднувати мережі (автономні системи AS) з несумісними між собою протоколами внутрішньої динамічної маршрутизації, наприклад, RIP з EIGRP, OSPF з EIGRP тощо. У своїх системних повідомленнях при поєднанні різних автономних систем BGP дозволяє зазначити різні величини метрик для інформаційних маршрутів, що, відповідно, сприяє вибору оптимального маршруту передачі даних. У той же час, значення величин метрик не визначається незалежними параметрами, як то, час доступу до ресурсу, швидкість ліній зв’язку або кількість транзитних хопів на шляху до віддаленої мережі. Пріоритет та значення метрик встановлюється адміністратором, і тому таку маршрутизацію іноді називають політично вмотивованою маршрутизацією, оскільки вона відображає політику адміністрації автономної системи при отриманні доступу до інших автономних систем та їх інформаційних ресурсів.

1.2 Сервіси VoIP у сучасних інфо-комунікаційних мережах

Клієнти IP-телефонії не тільки зберігають переваги традиційної телефонної мережі, що включають широкий діапазон послуг та зручність у використанні, стабільність та якість голосового сигналу, але і отримують наступні ключові переваги [7]:

- значно нижча ціна на послуги телефонного зв'язку;
- VoIP-телефонія одночасно забезпечує передачу голосу та даних, відповідаючи вимогам конвергенції мереж. Клієнти отримують значні переваги від економії мережевих ресурсів за рахунок використання єдиної інфраструктури та незначних об’ємів трафіку, що необхідний для передачі голосу, а також підвищену ступінь захисту голосової інформації у комп’ютерній мережі;
- значна ступінь мобільності користувачів VoIP-телефонії: дзвінки автоматично маршрутизуються в мережі Internet, а відповідно користувачі матимуть доступ до сервісів незалежно від того, де і на якому обладнанні вони підключаються до мережі. Така розподілена мережева архітектура надає можливість клієнтам працювати без прив'язки до робочого місця та навіть країни;
- широкий спектр обладнання доступу – від традиційних телефонів до смартфонів та комп'ютерів;
- нові послуги зв’язку (голосова пошта, конференц- та відеозв’язок тощо). Відкрита архітектура на базі IP забезпечує сумісність з широким спектром програмних додатків;
- можливість налаштування набору послуг зв’язку;
- зручність оплати послуг IP-телефонії;
- простота контролю за станом абонентського рахунку.

Інтернет-провайдери з легкістю можуть зайняти нішу на ринку послуг VoIP, оскільки IP-інфраструктура їх мереж відкриває широкі перспективи для організації послуг голосового зв'язку, а необхідні для VoIP апаратно-програмні засоби можна встановити у декілька етапів. Також Інтернет-провайдери вже мають точки з’єднання з комутаційним обладнанням інших міських провайдерів і операторів зв’язку загального користування [8].

Для Інтернет-провайдерів нова послуга VoIP забезпечує такі переваги [9]:

- зниження витрат за рахунок використання стандартних відкритих платформ;
- зменшення експлуатаційних витрат у результаті надання різноманітності послуг на основі єдиної мережевої інфраструктури;
- відкрита архітектура створює більш конкурентне середовище, а отже менші витрати на розробку нових послуг;
- усі послуги можуть бути доступні через єдиний канал з'єднання з користувачем.

Показник якості VoIP.

Традиційні телефонні мережі при передачі голосових повідомлень гарантують стабільність смуги пропускання, значення якої достатнє для якісної передачі сигналів голосового спектру. Так, завдяки фіксованій пропускній здатності каналів, ціна секунди голосового зв'язку залежить від відстані між абонентами [7].

VoIP-телефонія є однією з тих ніш телекому, де важлива мінімальна затримка при передачі сигналу. Цей параметр забезпечується сучасними технологіями кодування та передачі інформації, а також зростанням пропускної здатності каналів, що дозволяє VoIP успішно конкурувати з традиційними мережами телефонного зв'язку.

Основними параметрами якості зв'язку в IP-телефонії є:

– якість мови, що включає:

- діалог – можливість абонентів встановлювати з'єднання і вести розмову у реальному часі і в повнодуплексному режимі зв'язку;
- розбірливість – чистота та тональність голосових сигналів;
- відлуння – фактор чутності в телефоні власних голосових повідомлень;
- рівень – величина гучності голосових сигналів.

– якість сигналізації, що включає:

- швидкість встановлення виклику – час на встановлення з'єднання;
- завершення виклику – час необхідний на роз'єднання голосового з’єднання;
- DTMF – можливість функції багаточастотного набору номера.

Проблеми технології VoIP.

Якість передачі голосу в VoIP визначають дві групи параметрів: характеристики устаткування і характеристики IP-мережі. До характеристик обладнання претензій немає, всі вони використовують максимум своїх ресурсів, щоб забезпечити якість зв'язку. Тому всі проблеми, які виникають у VoIP, пов'язані з характеристиками IP-мережі і проблем, які їй притаманні [9].

Проблеми IP-мереж:

- затримка і час очікування;
- джиттер;
- втрата пакетів;
- недостатня захищеність.

Затримка і час очікування.

Затримка в VoIP – це час, за який голос проходить шлях від одного користувача до іншого. Сучасні телефонні мережі мають три типи затримки – затримку на поширення, затримку на серіалізацію і затримку на обробку. Найбільший вклад вносить затримка на поширення і на обробку. Перша викликана довжиною маршруту, по якому проходить сигнал від одного пристрою VoIP до іншого. Друга обумовлена процесом кодування та формуванням голосових сигналів у IP пакети для їх подальшої передачі через мережу.

Затримка на обробку.

Значення часу затримки кодування або обробки голосових повідомлень залежить від швидкодії процесора та алгоритму обробки голосових сигналів, що використовують пристрої, які передають IP пакети по мережі. Даний тип затримок

властивий так само і телефонним мережам, що стало великою проблемою для пакетних систем.

Одним із способів боротьби із затримкою на обробку є Цифровий процесор сигналів (Digital Signal Processor – DSP) – продукт Cisco IOS для VoIP, який створює вибірки голосу кожні 10 мс. У такий пакет вміщуються 2 вибірки голосу, відповідно затримка буде дорівнювати 20 мс. Відповідно до стандарту G.729., загальна затримка на передачу фрейму становитиме 25 мс, так як він враховує 5 мс попередньої початкової затримки. Тому, щоб зменшити навантаження на маршрутизатори і шлюзи, в Cisco відповідальність за кадрування і формування пакетів поклали на процесор DSP.

Затримка черги.

Дана затримка відбувається в результаті потрапляння пакетів у чергу на перевантаженому вихідному інтерфейсі. Це відбувається тоді, коли випущено більше пакетів, ніж інтерфейс може обробити за даний інтервал. Так само існує фактична затримка черги виводу, оптимальне значення якої має становити менше 10 мс [8].

Відповідно до стандарту, для хорошої якості голосу, наскрізна затримка не повинна перевищувати 150 мс. У реалізації VoIP від Cisco два маршрутизатора, з'єднаних між собою, використовують наскрізну затримку близько 60 мс. Таким чином, на переміщення IP-пакета від відправника до одержувача, залишається ще 90 мс мережевої затримки.

Джиттер.

Джиттер – це нерівномірність періодів часу на доставку пакетів. Даний вид проблем виникає внаслідок передачі голосу по IP-мережі. У голосових мережах очікується, що інтервал переданих пакетів не зміниться по приходу у вузол призначення, однак в реальних умовах, через проблеми, що виникають в IP-мережах, пакет може не досягти приймаючої станції за звичайний інтервал

(рисунок 1.3). Різниця між очікуваним часом отримання пакету і фактичним часом називається джиттером.

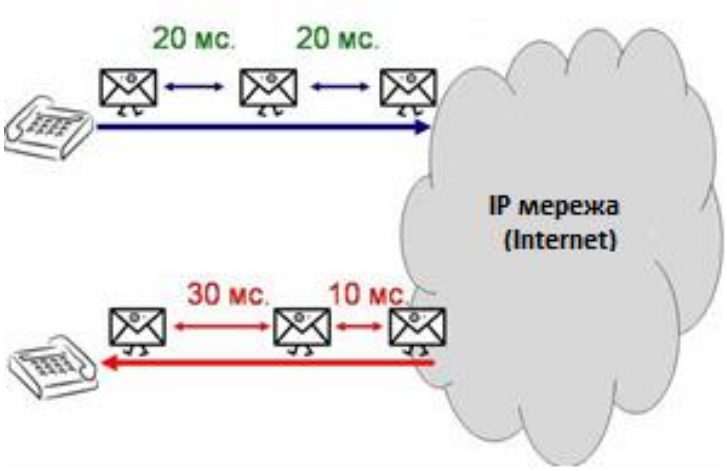


Рисунок 1.3 – Джитер у VoIP мережі

Для того щоб компенсувати вплив джитера, в абонентських терміналах використовують джиттер-буфер (рисунок 1.4), який накопичує пакети, що приходять з різною затримкою, і видає їх назовні вже з фіксованими затримками. Тобто він вирівнює інтервал між пакетами до того значення, яким він був при відправці.

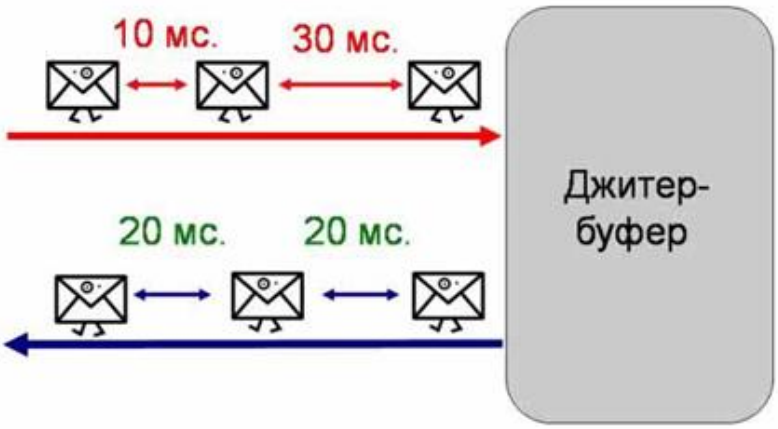


Рисунок 1.4 – Вирівнювання інтервалу за допомогою джитер-буфера

Проте, при великих затримках в мережі джиттер-буфер не допомагає, так як він безпосередньо впливає на затримку між співрозмовниками. Тобто, щоб вносити мінімальну затримку, джиттер-буфер повинен бути коротким, але для ефективної роботи він повинен бути довгим. Це протиріччя вирішується динамічною зміною довжини джиттер-буфера в залежності від якості мережі.

Втрата пакетів.

Втрата пакетів в мережах передачі даних – явище звичайне й очікуване.

Як правило, втрата пакетів відбувається при високому навантаженні на маршрутизатор, коли його вхідний буфер переповнюється. У такому випадку будь-які пакети, що надійшли в цей момент втрачаються. Якби для передачі голосового трафіку використовувався протокол TCP, то втрат пакетів не відбулося б, тому що вони запитувалися б повторно. Однак у VoIP-мережах немає часу на повторний запит пакетів, тому використовується інший транспортний протокол UDP. Він набагато швидше доставляє дані, яким потрібен малий час доставки, навіть якщо і надає доставку пакетів «по можливості».

Фактично, багато протоколів даних використовують втрату пакетів для отримання інформації про стан мережі і можуть зменшувати кількість посилок пакетів.

Реалізація VoIP від Cisco Systems дозволяє маршрутизатору реагувати на періодичну втрату пакетів. Якщо голосовий пакет не отримано за очікуваний час, він вважається втраченим, а останній отриманий пакет повторно відтворюється. Оскільки втрачений пакет містить всього 20 мс мови, то, як правило, слухач не звертає уваги на зміну якості.

Безсумнівною перевагою VoIP є її стійка робота в сильно завантажених мережах, де втрата пакетів становить до 5%. Втрачені пакети зазвичай легко компенсуються різними методами інтерполяції мови.

Недостатня захищеність.

При створенні протоколу IP в нього не були закладені вимоги з безпеки, що призвело до початкової вразливості реалізації цього протоколу [9]. На даний момент IP-мережа відкрита для безлічі видів несанкціонованого доступу в процес обміну даними. Так як дані передаються через зовнішню мережу Інтернет у відкритому вигляді, існує ймовірність перехоплення, аналізу та підміни цих даних на шляху від одного користувача до іншого. Надання загального доступу до внутрішніх ресурсів тягне за собою загрозу зовнішніх вторгнень, метою яких є отримання конфіденційної інформації. На сьогоднішній день дуже популярні атаки виду Відмова обслуговування (DDoS), метою яких є перевантаження вузла або мережі та втрата доступу до даних. Крім того, всі комп'ютери в мережі схильні до атак на програмне забезпечення, вразливості якого дозволяють виконувати на віддаленому комп'ютері довільний код, що відкриває доступ до управління програмним забезпеченням від особи адміністратора, права якого дозволяють виконувати будь-які дії на віддаленому комп'ютері.

1.3 Сервіси та архітектура IPTV

Для реалізації IPTV або multicast необхідна головна станція (Head-End) – це серверний програмно-апаратний комплекс, який приймає, зберігає та записує контент, керує послугами та абонентами [10]. Також потрібне клієнтське обладнання Set-Top-Box приставки для телевізорів, які є клієнтами для головної станції.

Використовувати всі можливості двостороннього телебачення дозволяють локальні IP-мережі. Зараз мережеві технології дуже поширені. Вони використовуються для підключення до Інтернету, IP-телефонії і, в тому числі, для IP-телебачення. Технологія IPTV дозволяє транслювати цифрове телебачення через IP-мережі з 4K якістю та багатоканальним звуком. Для цього необхідна

локальна IP-мережа з підтримкою multicast-трафіку, головна станція, що приймає зовнішні цифрові телесигнали і керує всім IPTV комплексом, а також кінцеві приставки для телевізорів користувачів.

Рисунок 1.5 – Архітектура IPTV комплексу

Протокол IP дозволяє організувати двосторонній зв'язок між головною станцією та абонентськими приставками. Це дозволяє абонентам користуватися інтерактивними послугами телебачення та іншими медіа послугами, недоступними користувачам звичайного телебачення.

Головною перевагою IPTV технології є її інтерактивність та можливість надання абонентам широкого набору додаткових послуг, пов'язаних трансляцією медіаконтенту [11]. Крім звичайних ТВ-каналів, IPTV надає користувачеві такі інтерактивні послуги:

- Video on Demand (VoD) – відео за запитом. Це система індивідуальної доставки абоненту відеофільмів. Сервіс дозволяє абоненту замовити для перегляду будь-

який фільм із бібліотеки VoD сервера за одноразову оплату. Під час перегляду фільму абонент може користуватися функціями паузи та перемотування.

- Near Video on Demand (nVoD) – «майже» відео за запитом. Іноді такий вид сервісу називають "віртуальний кінозал" або "карусельне відео". Цей сервіс схожий на VoD, але орієнтований відразу на значну кількість користувачів, підключених до цієї послуги. Попередньо складається програма мовлення відеоконтенту за розкладом. Користувач може переглянути цю програму та спланувати перегляд цікавого для нього контенту.
- Time Shifted TV – телебачення зі зсувом у часі. Цей сервіс додає інтерактивні можливості перегляду телепередач. Користувач у будь-який момент може поставити передачу на паузу та повернутися до перегляду пізніше. Також існує можливість перемотування ТВ-передач. Для цього використовуються записані на TVoD-сервері відео потоки.
- TV on Demand (TVoD) – телебачення на запит. Це система відкладеного перегляду телепередач. Користувач може заздалегідь вибрати потрібні телеканали для запису та пізніше переглянути записані на TVoD-сервері передачі.

Для функціонування IPTV комплексу також потрібна локальна IP-мережа, яка підтримує такі режими передачі IP-пакетів у мережі:

- Unicast. Використовується для надання користувачам персональних послуг: такий метод дозволяє передавати інформацію від сервера до конкретної адреси IP клієнта. Абонент замовляє персональний контент і тільки він отримує замовлений спектр медіапослуг. У випадку одночасного перегляду замовлень декількома абонентами їхній медіатрафік сумується на ділянці від сервера, на якому знаходиться необхідний контент, до абонентської лінії, наприклад, фізичного порту на мережевому обладнанні.
- Broadcast. Використовується при передачі даних з одного джерела до всіх клієнтів та вузлів підмережі. Для розсилки подібного типу трафіку

використовуються спеціальні адреси, у яких вузлова частина IP-адреси складається з усіх двійкових одиниць, або у десятковому вигляді закінчується на 255, наприклад, 192.168.1.255/24. Якщо транслювати медіаконтент у режимі broadcast, то усі користувачі, що знаходяться у даній підмережі, будуть отримувати даний контент. Тому такий режим застосовується лише для передачі службових повідомлень.

- Multicast. Призначений для розсилки даних групі абонентів та використовується для організації медіатрансляцій та інших послуг групового користування. Для ідентифікації multicast груп використовується спеціальний діапазон IP-адрес (клас D), що приймає значення від 224.0.0.0 до 239.255.255.255. При трансляції multicast трафіку медіатрафік від джерела до абонентських комутаторів йде одним інформаційним потоком, але обробляють його лише ті вузи, які цю інформацію замовляли. Multicast дозволяє значно економити смугу пропускання транспортної мережі, оскільки не вимагається окремого потоку даних для кожного глядача.

Технологія IPTV для multicast трансляції та керування сервісами використовує наступні типи протоколів:

- UDP – передача потокового відео та аудіо з мінімальними затримками;
- HTTP – організація інтерактивних сервісів (меню користувача), передача потокового відео та аудіо;
- RTSP – керування потоками мовлення;
- RTP – розсилка потокового відео в мережі;
- IGMP – керування multicast-потоками.

Клієнтське обладнання.

Для перегляду IPTV медіаконтенту за допомогою персонального комп'ютера існує спеціальний програмний клієнт. Завдяки йому абонент має змогу

переглядати телеканали та користуватись усіма сервісами, що надає технологія IPTV, на своєму персональному комп'ютері.

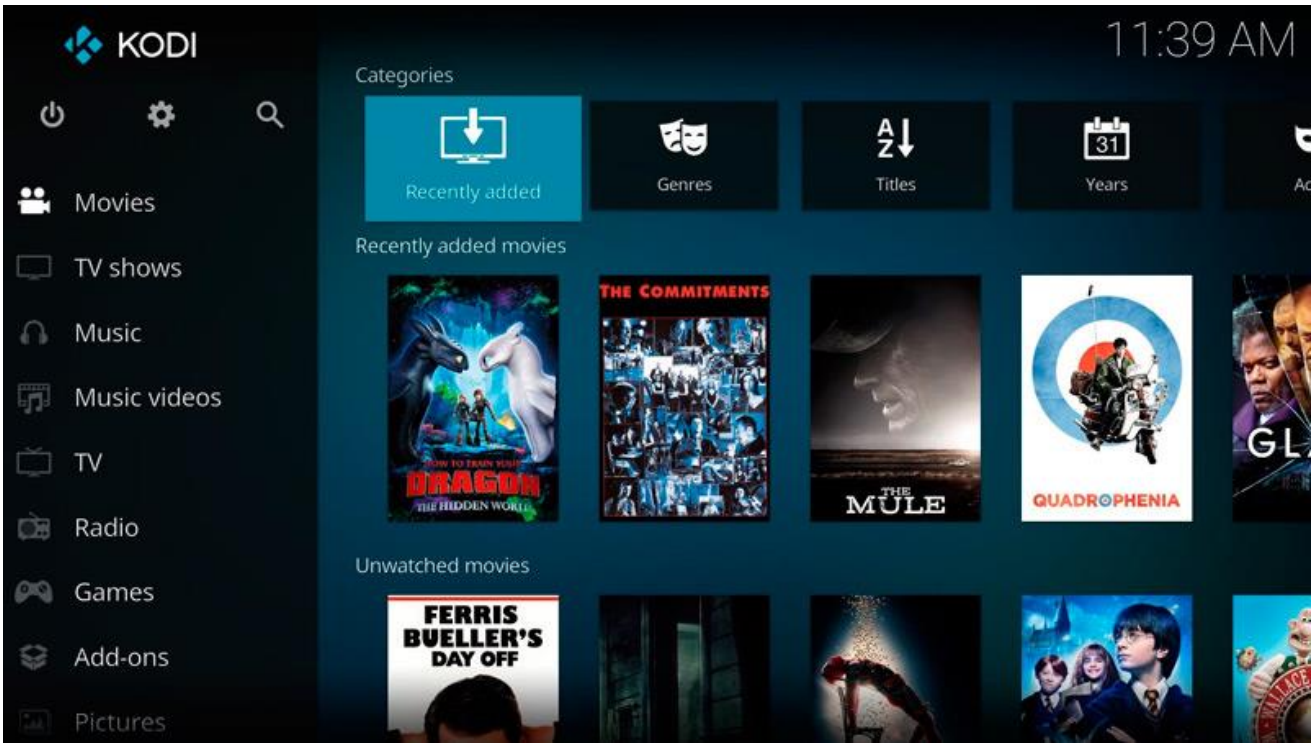


Рисунок 1.6 – Приклад інтерфейсу IPTV PC клієнта

Абонентські термінали.

Для ефективного доступу абонентів до сервісів IPTV телевізор має підтримувати функціонал Smart-TV або до нього має бути під'єднана спеціальна приставка Set-Top-Box (STB) або ж, як актуально в останній час, Android smart tv box. Вони є засобом з'єднання між операційною системою Middleware мережі IPTV оператора та телевізором абонента. Приставка приймає сигнал по протоколу IP і перетворює його у внутрішній формат, що підтримує телевізор абонента, таким чином виступаючи у ролі декодера на стороні клієнта. Для кожного телевізора в оселі клієнта потрібна окрема приставка Android smart tv box.

Рисунок 1.6 – Приклад абонентської приставка Android smart tv box

Для ознайомлення надано основні характеристики Android smart tv box приставки.

Об’єм оперативної пам'яті:

- 4 GB.

Стандарти підключення до мережі:

- Bluetooth 5.0;
- Ethernet;
- Wi-Fi.

Працює під управлінням операційної системи:

- Android 9.0.

Підтримка мультимедійного контенту:

- Підтримка IPTV;
- Підтримка OTT;
- Підтримка інтернет-сервісів.

Максимальна роздільна здатність зображення:

- 4K Ultra HD (3840x2160).

Порти входів та виходів:

- HDMI 2.1; 3 x USB 2.0; 1 x USB 3.0; Ethernet.

Жорсткий диск:

- 64 GB eMMC.

Процесор: Amlogic S922X:

- Кількість ядер і частота: 4 x Cortex A73 до 1.8 ГГц + 2 x Cortex A53 1.9 ГГц;
- Графіка: Arm Mali-G52 MP6.

Підтримка медіакодеків:

- MPEG1; MPEG2; MPEG4 (1Mbps-1000Mbps); HD Video decode support (MPEG2-MP@HL/H.264 MPEG-4 part10 MP@L4); WAV; WMV/VC1; MP3; WMA; AAC/AAC+.

Контент для IPTV.

Медіаконтент для трансляції через технологію IPTV ділиться на потоковий та контент, що надається абоненту за запитом (Video on Demand) [12]. Записаний медіаконтент зберігається на серверах VoD та nVoD. Ззовні контент надходить безпосередньо з супутникових антен, волоконно-оптичних та мідних кабелів або радіоефіру. Потоковий медіаконтент буває двох типів:

- FTA (free-to-air) – телеканали, які відкрито транслюються. Кількість таких відкритих каналів, які приймаються з одного транспондера або мультиплексу, обмежена смугою пропускання каналів зв’язку.

- PayTV – закодовані телеканали. Для такого виду контенту необхідне попереднє декодування за допомогою апаратних або програмних CAM-модулів – спеціальних пристроїв, що здійснюють розкодування зашифрованих телесигналів. Кількість каналів, що може транслюватися стрімером з одного окремого транспондера, залежить від продуктивності CAM-модуля, оскільки кожен CAM-модуль здатний здійснити декодування обмеженої кількості телевізійних каналів.

1.4 Постановка задачі

На основі зібраних та проаналізованих літературних джерел можна сформулювати ключові етапи кваліфікаційної магістерської роботи.

1. Провести аналіз предметної області за напрямом розробки інформаційно-комунікаційної технології проєктування мультисервісної мережі Ethernet з інтеграцією реального та віртуального обладнання Cisco, складовою частиною якої є програма для автоконфігурування мережевого обладнання. За результатами дослідження розробити описову модель предметної області.

2. Використовуючи симулятор GNS3 та «живе» телекомунікаційне обладнання фірми Cisco, побудувати мультисервісну мережу Ethernet з підтримкою сервісів VoIP та IPTV.

3. Проаналізувати потоки даних за допомогою сніферу Wireshark, визначивши закономірності у транспортуванні мережевого трафіку.

4. З метою оптимізації налаштування подібних схем у майбутньому в середовищі графічного програмування LabVIEW створити програмний додаток, графічний інтерфейс якого допоможе генерувати програмний код для налаштування мультисервісних мереж.

5. Перевірити працездатність та конфігурацію «живого» та віртуального телекомунікаційного обладнання, налаштування якого було здійснено за допомогою розробленого програмного додатку.

РОЗДІЛ 2. МОДЕЛЮВАННЯ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ETHERNET З ІНТЕГРАЦІЄЮ РЕАЛЬНОГО ТА ВІРТУАЛЬНОГО ОБЛАДНАННЯ CISCO

2.1 Моделювання комп'ютерних мереж з використанням емулятора GNS3

GNS3 (Graphical Network Simulator) – середовище графічного моделювання локальних та глобальних телекомунікаційних мереж. В GNS3 використовується мережеве обладнання, що функціонує під керуванням процесорів з MIPS архітектурою. До такого типу мережевих пристроїв відносяться більшість мережевих комутаторів та маршрутизаторів всесвітньо відомої компанії CISCO.

Середовище GNS3 було створено у 2007 році Джеремі Гроссманом як середовище для моделювання та тестування комп'ютерних мереж. В основу середовища лягла розробка емулятора MIPS для пристроїв Dynamips та графічного інтерфейсу Dynagen.

На теперішній час середовище GNS3 набуло широкої популярності серед студентів та адміністраторів комп’ютерних мереж і, на ряду з симулятором Cisco Packet Tracer, є одним з найбільш популярних середовищ для вивчення сучасних комп'ютерних мереж, налаштування та тестування мережевого обладнання перед впровадженням на реальних об’єктах [13].

У останніх версіях емулятора GNS3 для забезпечення сервісів моделювання мереж використовується наступне програмне забезпечення:

- WinPCAP – системний драйвер і бібліотека функцій, дозволяє отримати доступ до мережевих інтерфейсів фізичного комп'ютера та переданої через них інформації. Може бути використаний для аналізу мережевого трафіку;
- Wireshark – популярний графічний аналізатор трафіку. Дозволяє графічно відобразити інформацію про мережевий трафік, що передається через інтерфейси

комп’ютера. Використовується як складова частина емулятора GNS3, так і окрема програма, що дозволяє аналізувати трафік реальної комп'ютерної мережі;

- Dynamips – середовище для моделювання мережевого обладнання, реалізованого з урахуванням MIPS архітектури процесорів. Для функціонування необхідно завантажити образи операційних систем IOS для необхідних моделей роутерів CISCO. Окрім цього GNS3 також допускає роботу з іншими операційними системами;
- VCPS, VirtualBox, QEMU – середовища моделювання операційних систем комп’ютера. Використовуються для емуляції клієнтських комп’ютерів або проміжних пристроїв, реалізація яких здійснена на комп’ютерах з IBM/PC архітектурою;
- SolarWinds Response – середовище аналізу мережевого трафіку. Допомагає провести зручний графічний аналіз та відображення інформації, перехопленої сніфером Wireshark;
- SuperPUTTY – консольний доступ до реального та віртуального мережевого обладнання. Використовуючи популярні протоколи та стандарти, дозволяє здійснити пряме або віддалене підключення до мережевих пристроїв та отримати доступ до керування ними;
- Cpulimit – дозволяє оптимізувати роботу GNS3 та віртуального обладання для запобігання перевантаження CPU комп’ютера.

GNS3 – це емулятор комп’ютерних мереж з відкритим вихідним кодом, функціональні можливості якого дозволяють здійснювати моделювання та експериментальні дослідження у складних комп'ютерних мережах як масштабу офісу так і масштабу мережі оператора зв’язку на прикладі мереж MPLS та Carrier Ethernet. Він дає можливість створити макет мережі максимально наближений до реального аналогу, не вимагаючи при цьому наявності специфічного обладнання, такого як комутатори і маршрутизатори [14]. Програма володіє гнучким і

інтуїтивно зрозумілим інтерфейсом. З метою забезпечення повного і точного моделювання, додаток фактично використовує відповідні емулятори для роботи таких же операційних систем, як в реальній мережі (Dynamips, VirtualBox, Juniper і Qemu), кожен з яких виконує свій набір завдань. У рамках кваліфікаційної магістерської роботи емулятор GNS3 був успішно застосований для створення та тестування моделі мультисервісної мережі з підтримкою сервісів VoIP та IPTV.

Також важливо відмітити надзвичайну перевагу емулятора GNS3 – можливість реалізувати підключення віртуальної мережі до реальної через мережеву карту комп'ютера та перехоплення пакетів за допомогою сніферу Wireshark. А завдяки підтримці програмних сервісів VirtualBox, студенти та адміністратори мереж можуть використовувати GNS3 як зручне та функціональне середовище для створення телеком-лабораторій та тестування функціональності мереж перед їх впровадженням в реальних проєктах.

Однією з головних особливостей GNS3 є можливість створити будь-яку топологію і підключити її до реальної мережі, що дає можливість на практиці протестувати будь-який проєкт, при цьому не використовуючи самого обладнання. Для цього досить додати в робочу область зовнішній інтерфейс комп'ютера і підключити його до віртуальної топології мережі, як це зображено на рисунку 2.1

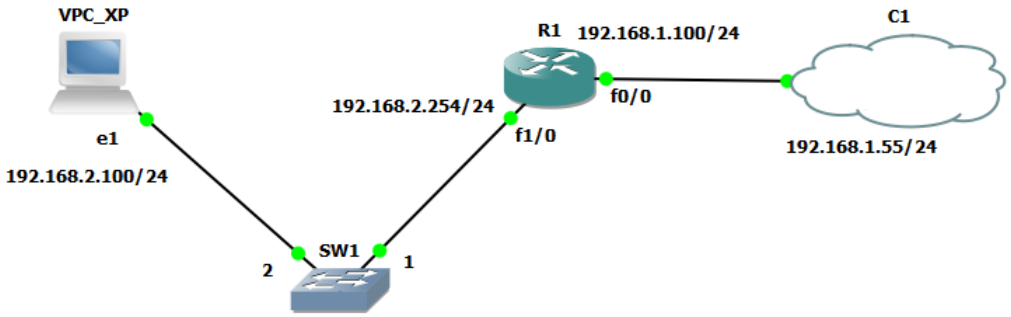


Рисунок 2.1 – Елемент Cloud (C1) реалізує зв'язок віртуальної топології з зовнішньою мережею Інтернет

Завдяки використанню реальних образів маршрутизаторів Cisco, топологія, створена у цій програмі, відповідає можливостям реальних комп'ютерних мереж та дозволяє здійснити експорт налаштувань з віртуального обладнання на реальне, попередньо виконавши безпечне тестування роботи телекомунікаційних сервісів.

2.2 Моделювання мережі з використанням обладнання Cisco та емулятора GNS3

Моделювання комп'ютерних мереж відіграє важливу роль при розробці та дослідженні телекомунікаційних технологій. Наразі існує велика кількість емуляторів, що дозволяють будувати, налаштовувати, досліджувати та тестувати мережі. Серед них найбільш популярними є Cisco Packet Tracer та GNS3 [13-14]. Такі емулятори допомагають будувати не лише невеликі локальні мережі, а й великі мережі для компаній операторів телекомунікаційного зв'язку MPLS та Carrier Ethernet. Але особливістю схеми, дослідженої у даній кваліфікаційній магістерській роботі та наведеної на рисунку 2.2, є поєднання симулятора GNS3 та «живого» телекомунікаційне обладнання фірми Cisco.

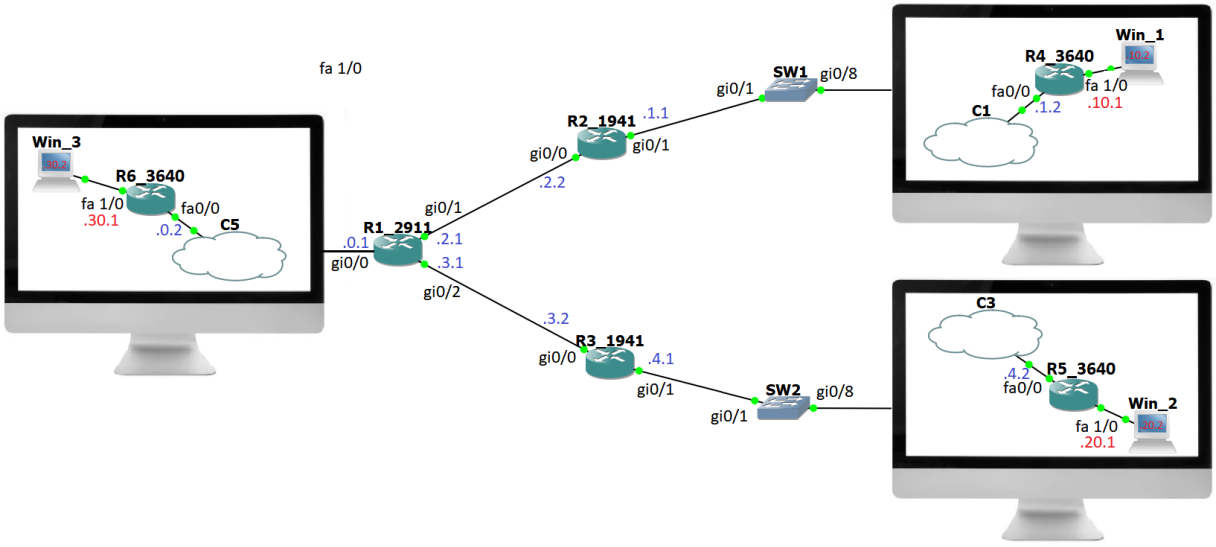


Рисунок 2.2 – Поєднання віртуального та «живого» телекомунікаційного обладнання фірми Cisco для побудови мультисервісної мережі

Це надало нам змогу здійснити моделювання та подальше дослідження мультисервісної мережі Ethernet з підтримкою сервісів VoIP та IPTV.

Побудову схеми та налаштування мережевого обладнання можна розбити на наступні ключові етапи.

Етап 1. Для початкового підключення до обладнання використовувався консольний порт роутерів Cisco, а також кабель USB-miniUSB. Після встановлення з'єднання на роутерах для зручності віддаленого адміністрування піднімався протокол Telnet.

Приклад типових команд конфігурації протоколу Telnet на віддаленому комутаторі:

Switch>enable

Switch#configure terminal – *вхід до режиму конфігурації.*

Switch(config)#interface vlan 1 – *вхід до режиму конфігурації інтерфейсу vlan 1 (за замовчуванням усі порти комутатора знаходяться у vlan 1).*

Switch(config-if)#ip address 192.168.255.254 255.255.255.0 – *налаштування IP-адреси та маски мережі.*

Switch(config-if)#no shutdown – *увімкнення інтерфейсу vlan 1.*

Switch(config-if)#exit – *вихід із режиму налаштування інтерфейсу.*

Switch(config)#line vty 0 15 – *вхід у режим налаштування віртуальних ліній (призначені для віддаленого підключення та адміністрування через telnet, ssh)*.

Switch(config-line)#password cisco – *встановлення пароля «cisco» для підключення telnet.*

Switch(config-line)#login – *встановлення способу аутентифікації за допомогою пароля.*

Switch(config-line)#transport input telnet – *встановлення протоколу підключення telnet.*

Switch(config-line)#exit – *повернення до конфігураційного режиму.*
Switch(config)#enable secret cisco – *встановлення пароля на доступ до привілейованого режиму конфігурації обладнання.*

Налаштування DHCP серверу

Switch(config)#ip dhcp pool vlan1 – *створення dhcp пулу з ім'ям Vlan1.*
Switch(dhcp-config)#network 192.168.255.0 255.255.255.0 – *зазначається номер мережі, з діапазону IP-адрес якої будуть видаватися IP-адреси клієнтам.*
Switch(dhcp-config)#default-router 192.168.255.254
Switch(dhcp-config)#dns-server 8.8.8.8

Налаштування з'єднання віртуального та реального обладнання

Для під'єднання віртуальної складової мережі до «живого» обладнання використовувався емулятор GNS3, в якому за допомогою елементу Cloud організовувався зв'язок віртуальних роутерів з мережевою картою «живого» комп'ютера. Після чого через мережеву карту та кабель вита пара здійснювалося підключення до «живого» мережевого обладнання Cisco.

Етап 2. Налаштування IP-адрес на інтерфейсах роутерів. Для прикладу у кваліфікаційній магістерській роботі описано налаштування роутера Cisco 2911. Конфігурація інших роутерів здійснювалася аналогічним чином.

Router>en
Router#conf t
Router(config)#int gi 0/0 – *конфігурація інтерфейсу gigabitEthernet 0/0.*

Router(config-if)#ip add 192.168.0.1 255.255.255.0 – *вказується IP-адреса та маска IP-адреси для вибраного інтерфейсу.*

Router(config-if)#no sh – *включення інтерфейсу роутера*.

Router(config-if)#exit

Router(config)#int gi 0/1 – *конфігурація інтерфейсу gigabitEthernet 0/1*.

Router(config-if)#ip add 192.168.2.1 255.255.255.0

Router(config-if)#no sh

Router(config-if)#exit

Router(config)#int gi 0/2 – *конфігурація інтерфейсу gigabitEthernet 0/2.*

Router(config-if)#ip add 192.168.2.1 255.255.255.0

Router(config-if)#no sh

Router(config-if)#exit

Етап 3. Налаштування динамічної маршрутизації. Оптимальним варіантом протоколу динамічної маршрутизації для нашої схеми можна вважати проприєтарний протокол EIGRP від фірми Cisco, оскільки в ній використано обладнання лише даного виробника.

Router(config)#router eigrp 100 – *активація протоколу EIGRP та зазначення номеру автономної системи.*

Router(config-router)#network 192.168.0.0 – *перераховуються мережі безпосередньо під'єднані до даного роутера.*

Router(config-router)#network 192.168.2.0

Router(config-router)#network 192.168.3.0

Router(config-router)#exit

Етап 4. Налаштування VoIP сервісів на роутерах та переадресації дзвінків між різними VoIP шлюзами.

Router(config)#telephony-service – *активація сервісу IP-телефонії.*
Router(config-telephony)#max-dn 144 – *максимальна кількість номерів у мережі.*
Router(config-telephony)#max-ephones 42 – *максимальна кількість телефонів.*

Router(config-telephony)# keepalive 15
Router(config-telephony)# system message VoIP-C2911– *системне повідомлення.*
Router(config-telephony)#ip source-address 192.168.0.1 port 2000 – *адреса сервера IP-телефонії.*
Router(config-telephony)# create cnf-files
Router(config-telephony)# auto assign 1 to 144 – *підтримка автореєстрації телефонів та призначення їм номерів із пулу допустимих значень.*
Router(config-telephony)# exit
Router(config)#ephone-dn 1 – *перший логічний цифровий номер.*
Router(config-ephone-dn)#number 2001 – *номер абонента.*
Router(config-ephone-dn)#name VASYA – *ім'я абонента*
Router(config)#ephone-dn 2
Router(config-ephone-dn)#number 2002
Router(config-ephone-dn)#name VOVA
Router(config)#ephone-dn 3
Router(config-ephone-dn)#number 2003
Router(config-ephone-dn)#name KOLYA
Router(config-ephone-dn)#exit

Для отримання телефонного номеру на Cisco IP Phone необхіно вказати IP-адресу TFTP серверу.

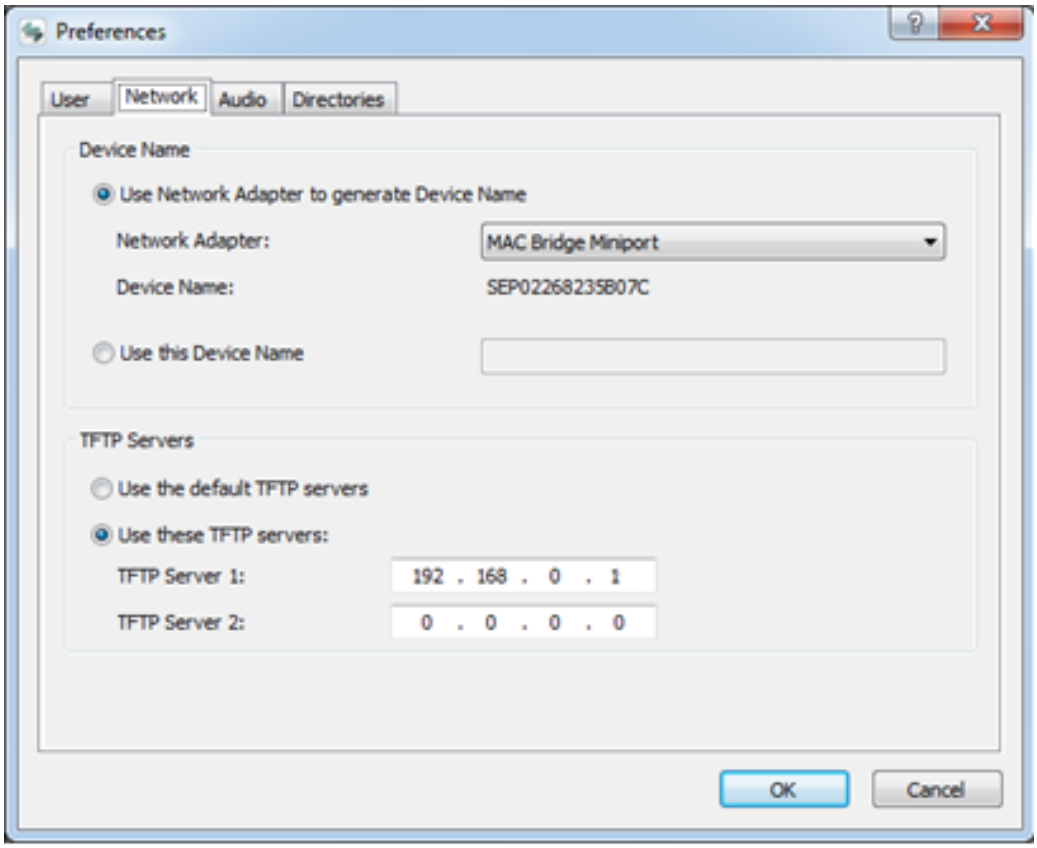


Рисунок 2.3 – Налаштування TFTP серверу

Рисунок 2.4 – Результат коректного налаштування IP-телефонії

Для організації переадресування дзвінків між VoIP шлюзами на роутері необхідно налаштувати наступні команди VOIP маршрутизації.

Router(config)#dial-peer voice 1 voip – *створюється перше правило переадресації.*

Router(config-dial-peer)# destination-pattern 10.. – *вказується формат номерів на віддаленому VoIP шлюзі, на який здійснюється переадресація дзвінків.*

Router(config-dial-peer)# session target ipv4:192.168.10.1 – *вказується IP-адреса віддаленого VoIP шлюзу.*

Router(config-dial-peer)#exit

Router(config)#dial-peer voice 2 voip

Router(config-dial-peer)# destination-pattern 20..

Router(config-dial-peer)# session target ipv4:192.168.20.1

Router(config-dial-peer)#exit

Результатом правильного виконання описаних вище команд є можливість успішно здійснювати IP-телефонійні дзвінки між мережами.

Етап 5. Налаштування підтримки multicast мовлення з метою подальшої трансляції відеопотоків у мультисервісній мережі Ethernet. Для цього на всіх роутерах нашої мережі необхідно налаштувати наступні команди.

Router(config)#ip multicast-routing – *активація підтримки multicast трафіку в мережі.*
Router(config)#int gi 0/0
Router(config-if)#ip pim dense-mode – *активація підтримки протоколу pim на інтерфейсах роутера.*
Router(config-if)#exit
Router(config)#int gi 0/1
Router(config-if)#ip pim dense-mode
Router(config-if)#exit
Router(config)#int gi 0/2
Router(config-if)#ip pim dense-mode
Router(config-if)#exit

Етап 6. Для успішної трансляції потокового відео в мережі необхідно здійснити відповідні налаштування серверної та клієнтської частини VLC медіаплеєру. Покрокові інструкції налаштування серверу наведено на рисунках 2.5-2.12. Налаштування клієнтської частини наведено на рисунках 2.13-2.15.

Налаштування серверної частини VLC медіаплеєру.

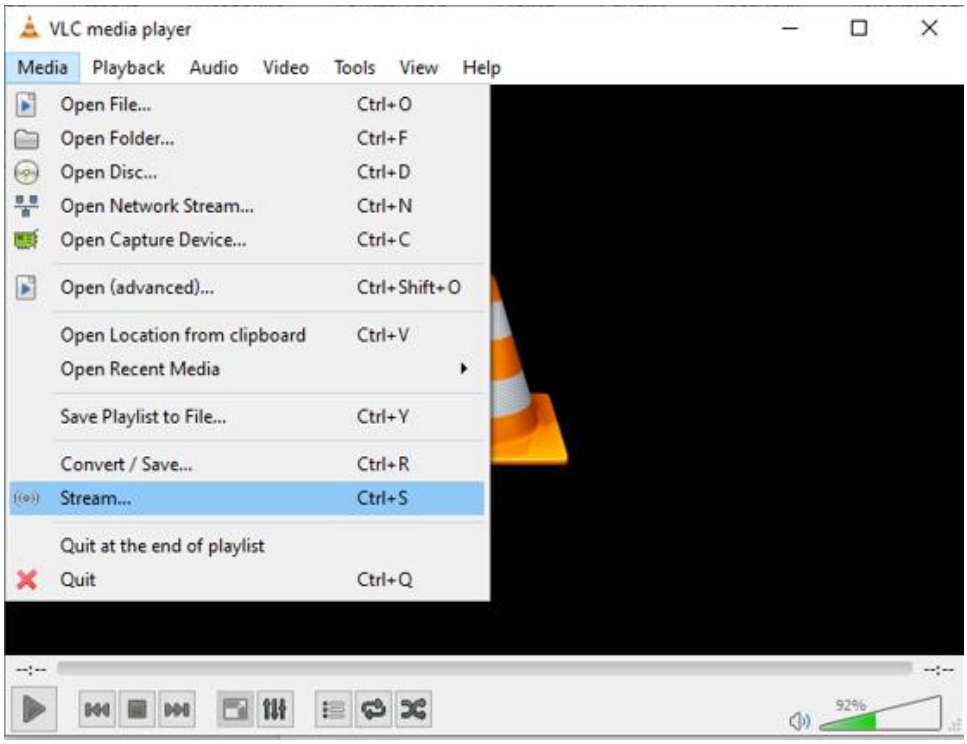


Рисунок 2.5 – Налаштування серверу трансляції відеопотоків. Крок 1

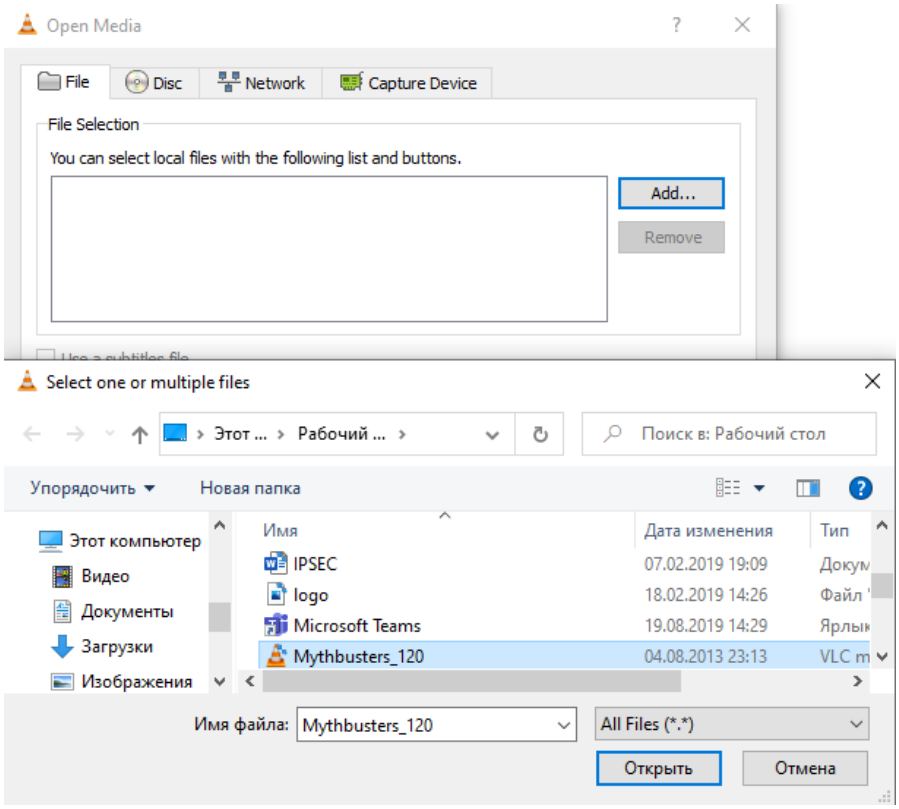


Рисунок 2.6 – Налаштування серверу трансляції відеопотоків. Крок 2

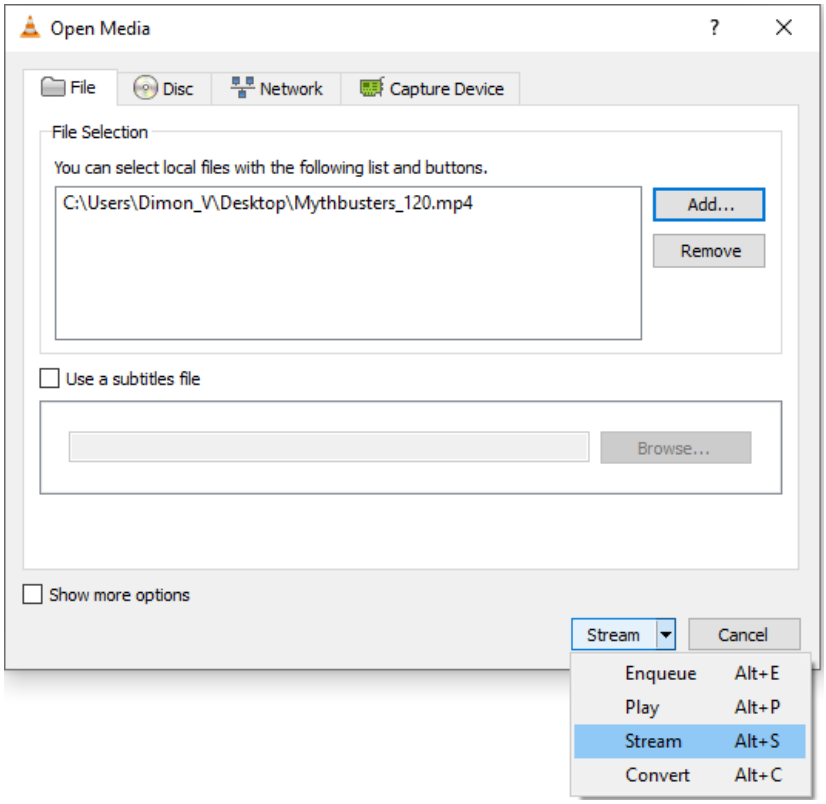


Рисунок 2.7 – Налаштування серверу трансляції відеопотоків. Крок 3

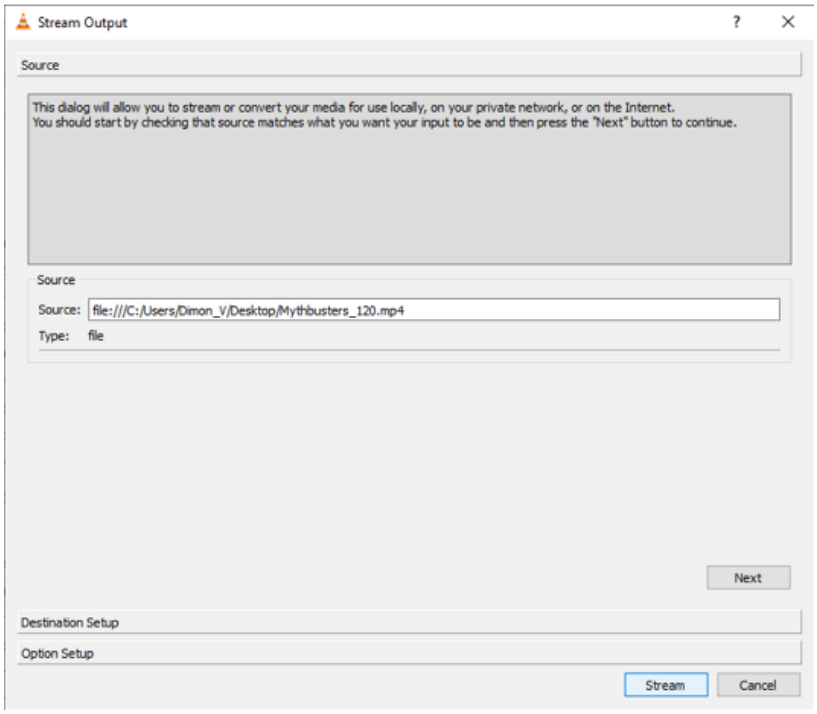


Рисунок 2.8 – Налаштування серверу трансляції відеопотоків. Крок 4

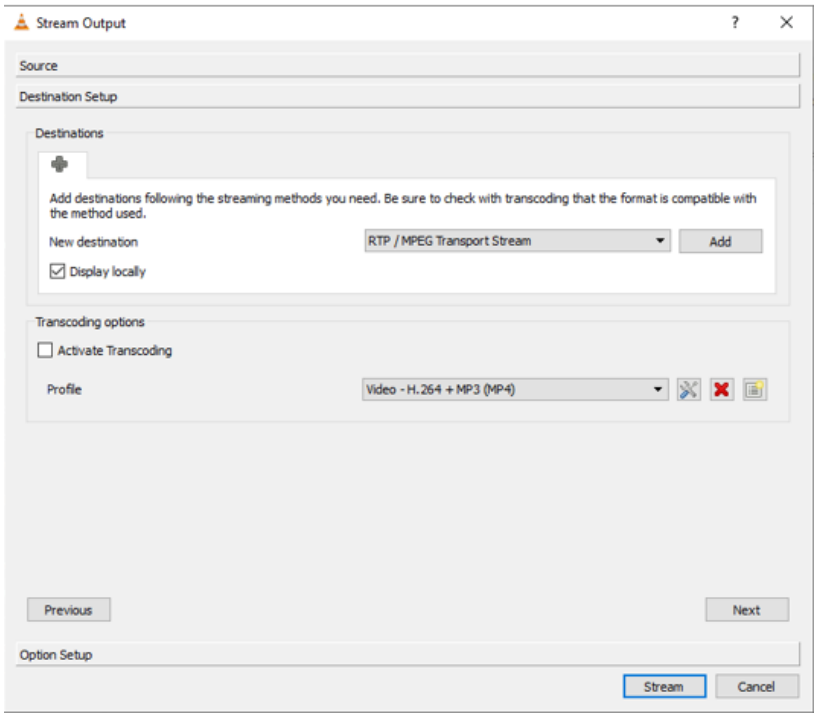


Рисунок 2.9 – Налаштування серверу трансляції відеопотоків. Крок 5

В налаштуваннях «Новий шлях призначення» рекомендовано вказати протокол RTP/MPEG Transport Stream.

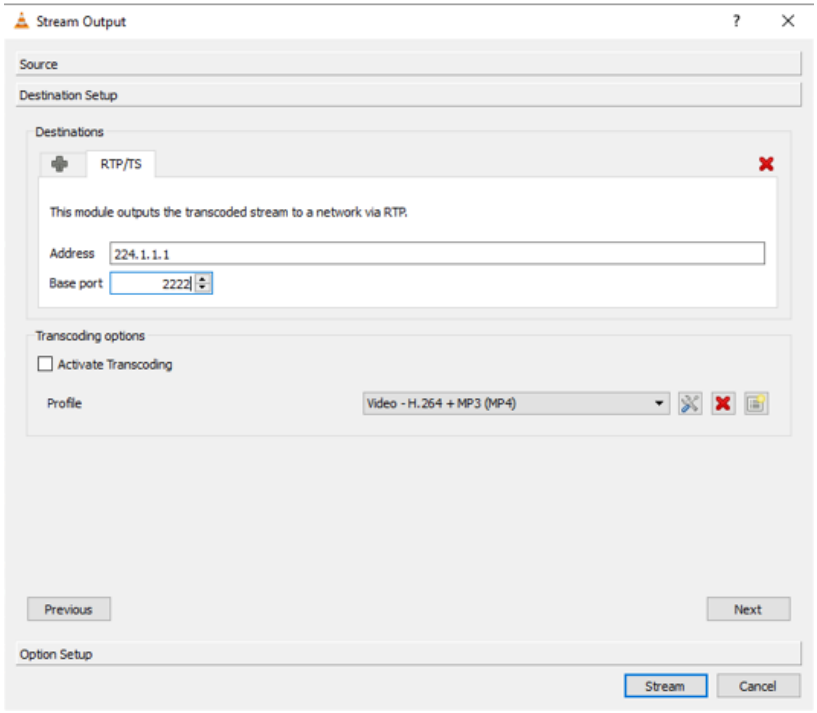


Рисунок 2.10 – Налаштування серверу трансляції відеопотоків. Крок 6

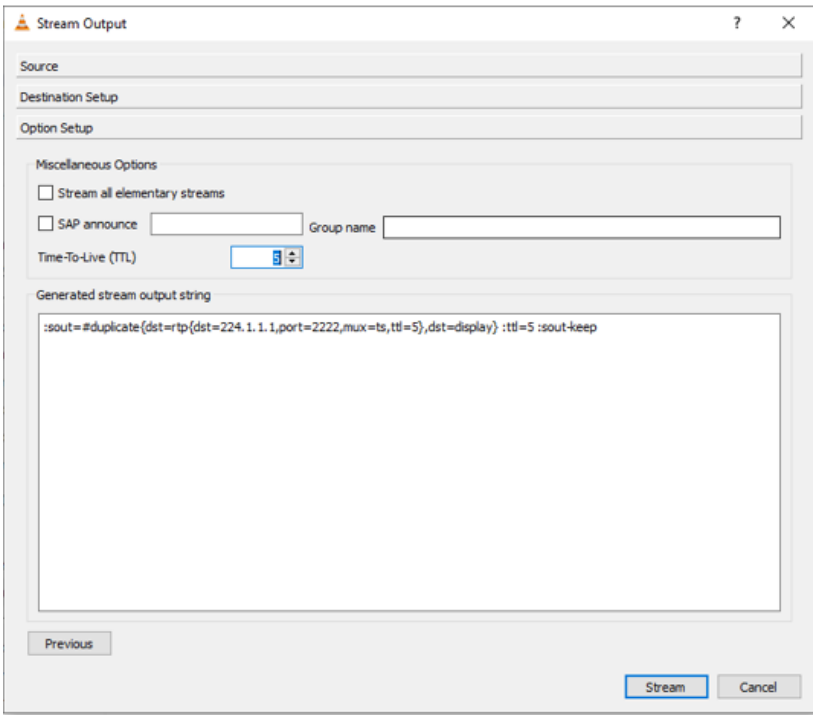


Рисунок 2.11 – Налаштування серверу трансляції відеопотоків. Крок 7

На цій сторінці нас цікавить параметр TTL («Час життя»). Оскільки у нас в мережі найбільш тривалий маршрут включає 5 транзитних роутерів і враховуючи, що кожен роутер зменшить значення TTL на одиницю, то рекомендовано встановити радіус трансляції відеопотоку за параметром TTL не менше 6. Натиснувши кнопку "Потік" запускаємо відеотрансляцію. Її можна спостерігати у вікні VLC програвача або в інформації про медіа-файл («Інструменти» – «Інформація про медіа-файл» – «Статистика»).

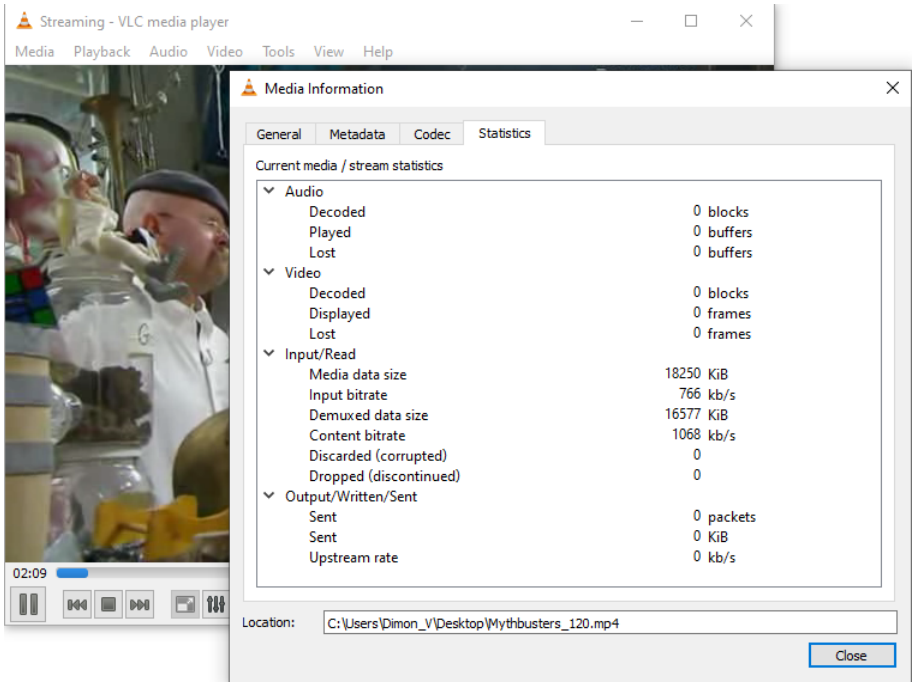


Рисунок 2.12 – Налаштування серверу трансляції відеопотоків. Крок 8

Налаштування клієнтської частини VLC медіаплеєру.

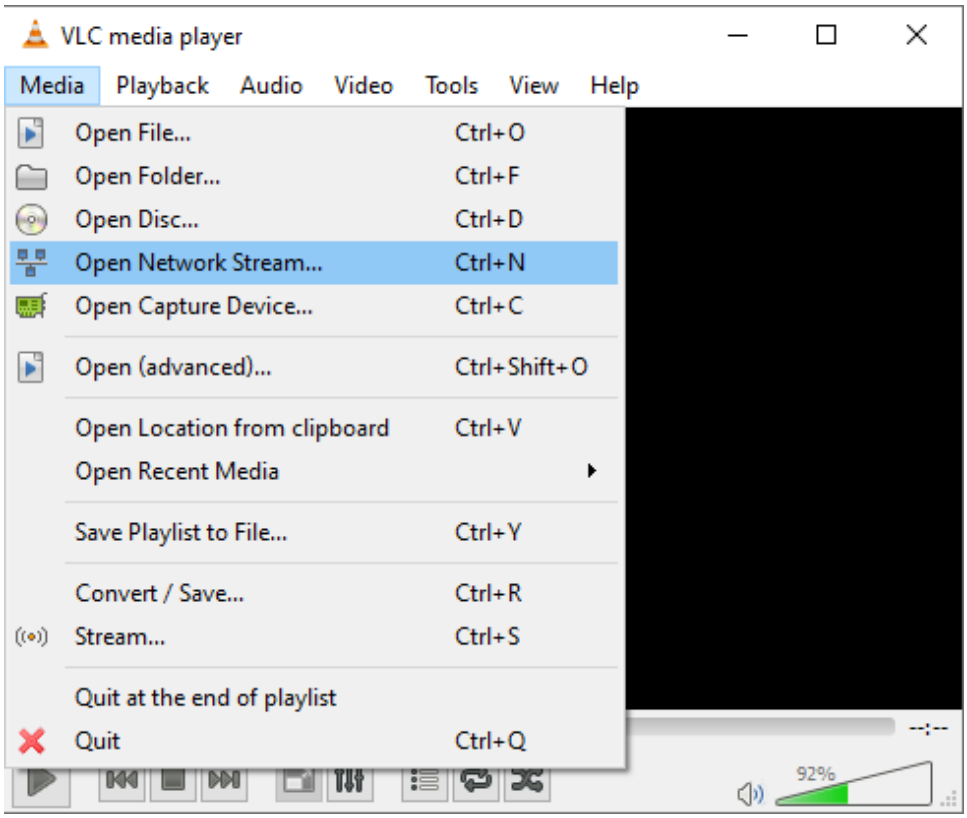


Рисунок 2.13 – Налаштування клієнта для відображення відеопотоків. Крок 1

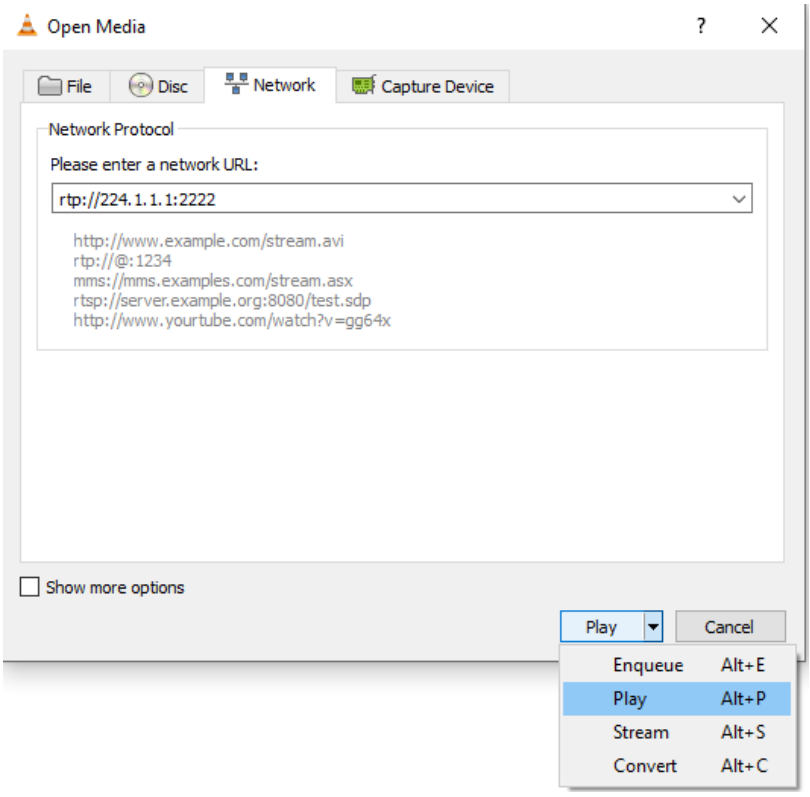


Рисунок 2.14 – Налаштування клієнта для відображення відеопотоків. Крок 2

Вводимо адресу multicast потоку та порт **rtp://224.1.1.1:1234** та запускаємо відображення трансляції.

Рисунок 2.15 – Налаштування клієнта для відображення відеопотоків. Крок 3

Як можна зазначити, у нас немає можливості прокручувати відеопотік вперед чи назад, а адреса потоку відповідає адресі серверу трансляції. Переглянути інформацію про multicast трафік на роутерах можна за допомогою команд:

Router#sh ip mroute

Router#sh ip igmp group

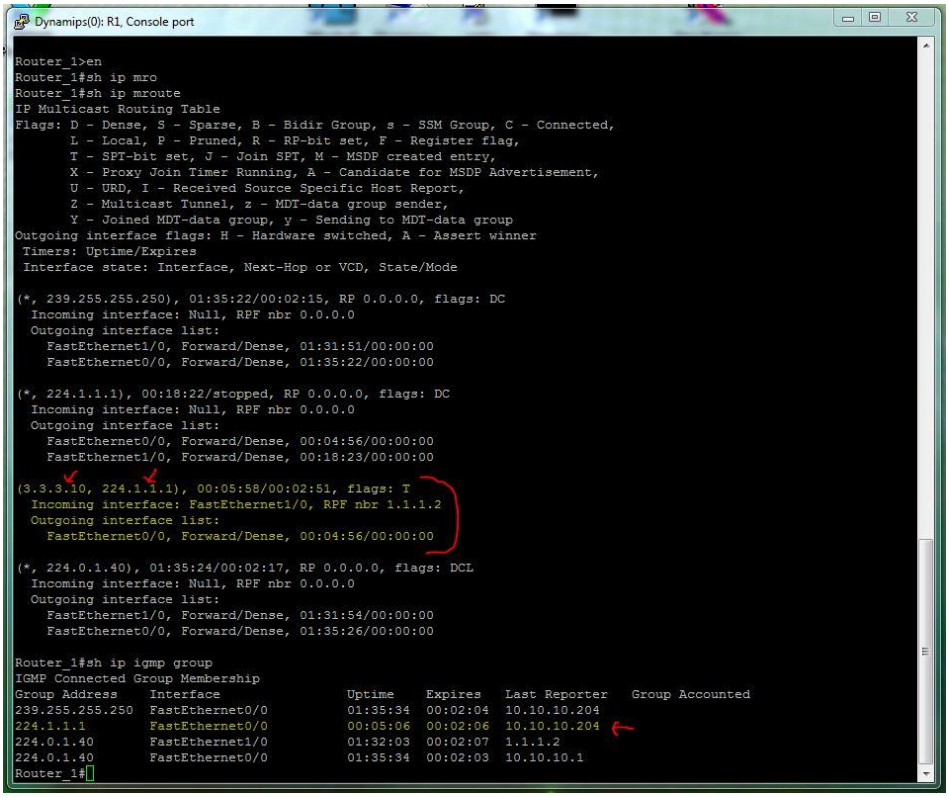


Рисунок 2.15 – Інформація про multicast трафік на роутерах мережі

Таким чином, у практичній частині кваліфікаційної магістерської роботи нам вдалося, використовуючи симулятор GNS3 та «живе» телекомунікаційне обладнання фірми Cisco, побудувати мультисервісну мережу Ethernet з підтримкою найбільш популярних мережевих сервісів VoIP та IPTV.

2.3 Графічне середовище програмування LabVIEW

LabVIEW – це головний програмний продукт компанії National Instruments. LabVIEW – це скорочення від назви Laboratory Virtual Instrumentation Engineering Workbench [15]. Навіть у назві цього програмного продукту відзначається його орієнтація на лабораторні та наукові дослідження, вимірювання та аналіз даних. Реалізувати SCADA–систему в LabVIEW значно простіше, ніж використовуючи «традиційні» засоби розробки. LabVIEW – це принципово інша мова програмування або навіть ціла "філософія" розробки програмних додатків. Функціональність мови LabVIEW змушує програміста мислити іншими образами і згодом надає унікальні можливості для реалізації проєктів. Чи можна LabVIEW вважати мовою програмування? В цьому питанні думки розходяться, оскільки в LabVIEW немає стандарту, як, наприклад, в мові «C». Розробники на LabVIEW часто говорять, що пишуть свої програмні додатки мовою «G». Формально така мова не існує, але це є навіть перевагою такого середовища розробки: оскільки в кожній новій версії в мову вводяться нові програмні конструкції. Гадаю, важко уявити, що у наступній версії «C» з'явиться нова структура, наприклад, для циклу For. А от в LabVIEW таке нововведення цілком можливе. Слід зауважити, що LabVIEW входить до популярного рейтингу мов програмування TIOBE, займаючи в ньому тридцяте місце між Прологом і Фортраном.

Компанія National Instruments створена у 1976 році трьома засновниками Джеффом Кодоски, Джеймсом Тручардом та Біллом Новліним в американському місті Остін, штаті Техас. Головною спеціалізацією компанії є апаратно-програмні засоби для вимірювань та автоматизація виробництва.

Перша версія LabVIEW вийшла у світ через десять років після заснування компанії – у 1986 році (версія для Apple Mac). Інженери National Instruments вирішили кинути виклик «традиційним» мовам програмування і створили виключно графічне середовище розробки. Основним ідеологом такого підходу

став Джефф Кодоски. Перша версія LabVIEW під операційну систему Windows з’явилася у 1993 році. Актуальною на цей час є версія 2022 Q3. В Остіні і по сьогоднішній день розташовується головний офіс компанії. Сьогодні в компанії працюють майже чотири тисячі людей, офіси розташовані майже у сорока країнах світу.

LabVIEW – кросплатформове графічне середовище розробки програмних додатків. LabVIEW можна вважати універсальною мовою програмування. Незважаючи на те, що цей програмний продукт тісно пов'язаний з апаратним забезпеченням National Instruments, він не пов'язаний з конкретною апаратною архітектурою. У LabVIEW наявні версії для Windows, Linux та MacOS. Вихідні коди можуть переноситись, а програми, написані на LabVIEW, виглядають однаково на всіх операційних системах. Згенерований у LabVIEW код може бути виконаний на Windows Mobile або PalmOS. Графічне середовище LabVIEW може успішно використовуватися для створення великих програмних проєктів, для обробки текстів, графіки та роботи з базами даних [16].

LabVIEW можна вважати високорівневою мовою, але за потреби до неї можна під’єднати «низькорівневі» модулі. Навіть можливо використання вставок написаних на асемблері – це цілком можливо, потрібно лише згенерувати DLL та вставити виклик в програмний код. Окрім цього, високорівневість мови дозволяє доволі легко робити дуже складні операції з даними, на подібні операції у звичайній мові програмування могли бути витрачені сотні рядків коду.

Але все-таки деякі операції низькорівневих мов (робота з вказівниками) не легко реалізувати в LabVIEW через його «високорівневість».

Мова LabVIEW містить у собі основні конструкції, що мають аналоги у традиційних мовах програмування:

- змінні (локальні та глобальні);
- розгалуження (case structure);

- For – цикли з перевіркою умови на завершення та без;
- While – цикли;
- об’єднання операцій.

LabVIEW – програма та можливості мови

У мові LabVIEW програмні модулі мають назву Virtual Instruments (віртуальні інструменти) або VI. Такі модулі мають розширення *.vi. VIs – це елементи конструкції, з якої складається програма написана на LabVIEW. Будь-яка LabVIEW програма містить мінімум один програмний модуль VI. У термінах мови «С» можна провести аналогію з функцією, але лише з тією різницею, що в LabVIEW одна функція міститься в одному файлі (на основі такого принципу можна створювати бібліотеки найбільш часто затребуваних інструментів). У результаті один програмний модуль VI може бути викликаний з іншого програмного модуля. Як наведено нижче, кожен VI складається з двох частин: Блок-Діаграми (Block Diagram) та Передньої Панелі (Front Panel). Блок-діаграма – це аналог програмного коду (візуальне графічне уявлення коду), а Передня панель – це графічний інтерфейс. Стандартний класичний приклад Hello, World! у мові LabVIEW буде виглядати наступним чином (рисунок 2.16).

В основі програмування на LabVIEW лежить парадигма послідовності потоків даних. У наведеному прикладі константа та термінал індикатору поєднані лінією один з одним. Така лінія називається Wire (кабель або дріт). По дротах відбувається передача потоків даних від одних елементів до інших. Концепція подібних зв’язків називається Data Flow. Блок-Діаграма – це вузли (ноди), при цьому виходи одних вузлів (як правило праві виходи) приєднані до входів інших вузлів (ліві входи вузлів).

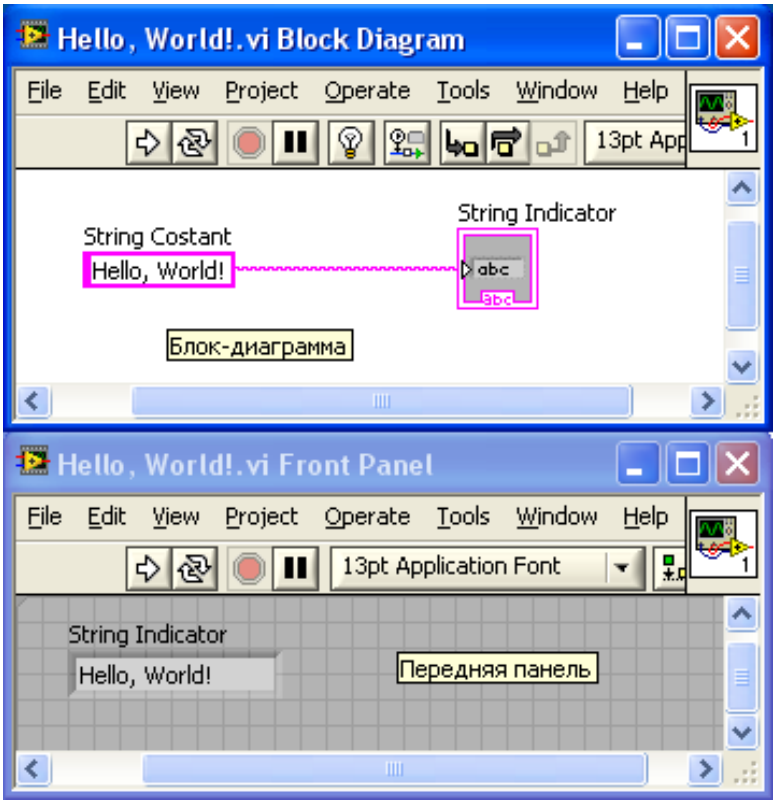


Рисунок 2.16 – Графічний інтерфейс та блок-діаграма підпрограми написаної на LabVIEW

Вузли у програмі розпочинають виконання лише тоді, коли на них приходять усі необхідні для обробки вхідні дані. У наведеному прикладі на блок-діаграмі зображено два ноди, при чому один з них є константою. Оскільки цей вузол є самодостатнім – він виконується одразу ж при запуску програми. Другий вузол виконує функцію індикатора. Він відображає у графічний інтерфейс дані, що передала на нього константа.

Варіантом трохи складнішого прикладу може бути додавання та множення двох чисел. У традиційних мовах ми напишемо щось на зразок:

```
int a, b, sum, mul;
//...
sum = a + b;
mul = a * b;
```

Програмна реалізація подібного прикладу у LabVIEW буде виглядати наступним чином:

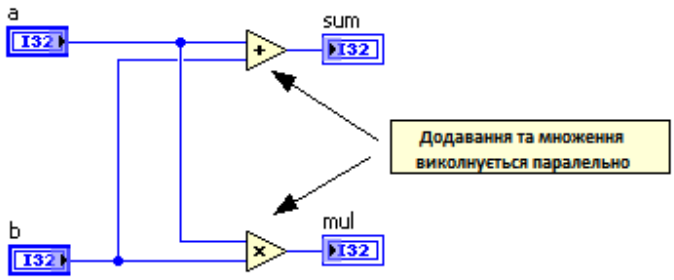


Рисунок 2.17 – Приклад написання арифметичних операцій в LabVIEW

Зверніть увагу на те, що операції додавання та множення у цьому випадку будуть виконуватись паралельно. На багатопроцесорній машині автоматично будуть задіяні два процесори.

Структури циклів while / for та if / then / else у LabVIEW мають наступний вигляд:

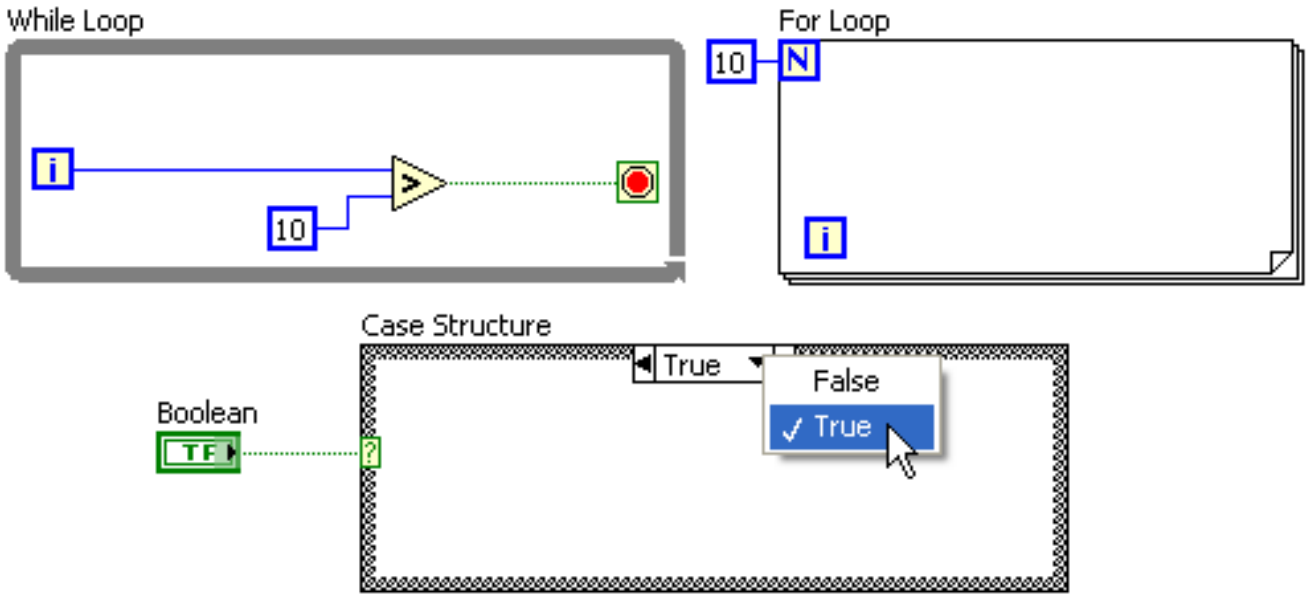


Рисунок 2.18 – Приклад організації циклів в LabVIEW

Як вже згадувалося, всі елементи виконуватимуться паралельно, то ж необов’язково контролювати процес розпаралелювання завдання на декілька окремих потоків, що можна було б виконати паралельно на декількох окремих процесорах. Але в останніх версіях з’явилась можливість у явному вигляді вказати, на якому з процесорів необхідно запускати виконання того чи іншого циклу While. У сучасних текстових мовах теж існують надбудови, що дозволяють просто досягти підтримки багатопроцесорних систем, але так легко та зручно, як на LabVIEW, це ніде не вдалося реалізувати. Щодо багатопотокової обробки даних, то слід зазначити, що в арсеналі розробника LabVIEW наявний багатий вибір інструментів, що дозволять синхронізувати потоки: семафори, черги, рандеву тощо.

Стандартна версія LabVIEW містить у собі блоки для роботи з файлами ini, реєстром, функції для обробки двійкових та тестових файлів, математичні функції, розвинений функціонал інструментів для побудови графіків (оскільки акцент LabVIEW на лабораторних дослідженнях). А на додаток до раніше зазначеної можливості викликів DLL, мова LabVIEW дозволяє успішно працювати з ActiveX компонентами та .NET. Починаючи з версії 8.0 у LabVIEW було реалізовано підтримку класів, таким чином мова LabVIEW стала об'єктноорієнтованою. На даний час реалізовану підтримку не можна назвати абсолютною, але основні риси об'єктноорієнтованих мов, такі як успадкування та поліморфізм, вже присутні. Важливо, що функціональність мови LabVIEW можна розширити додатковими модулями, як, наприклад, модуль NI Vision Toolkit, що застосовується для обробки зображень та машинного зору. Використовуючи модуль Application Builder можна генерувати exe-файли. За допомогою модуля Internet Toolkit є можливість працювати з FTP-серверами, а за допомогою Database Connectivity Toolkit – з базами даних.

Нерідко можна почути зауваження, що графічний код вкрай важко читається. Без звички велика кількість іконок та провідників дійсно дещо шокує недосвідченого користувача. На початку знайомства з мовою програмування LabVIEW розробники-початківці іноді створюють програми-«простирадла» та програми-«спагетті». Однак більш досвідчений LabVIEW-розробник ніколи не стане створювати панель діаграм, що перевищує розмір його екрану, навіть якщо програма буде складатися із сотень окремих модулів. Правильно розроблена програма фактично «самодокументується», оскільки в її основі лежить зручне для розуміння графічне уявлення програмних процесів.

Для прикладу можна навести фрагмент коду програми, що був використаний у даній кваліфікаційній магістерській роботі під час розробки інтерактивного графічного інтерфейсу конфігурування мережевого «живого» та віртуального обладнання.

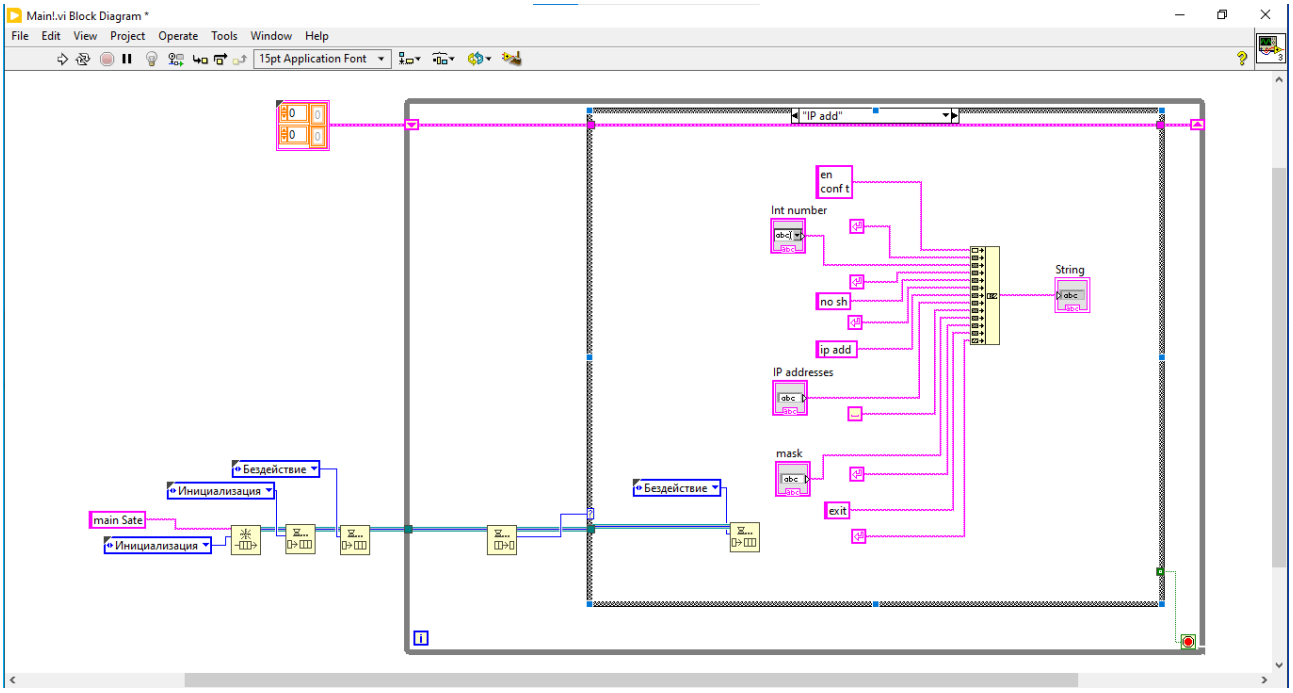


Рисунок 2.19 – Блок-діаграма (графічне уявлення коду) програми конфігурування роутера Cisco

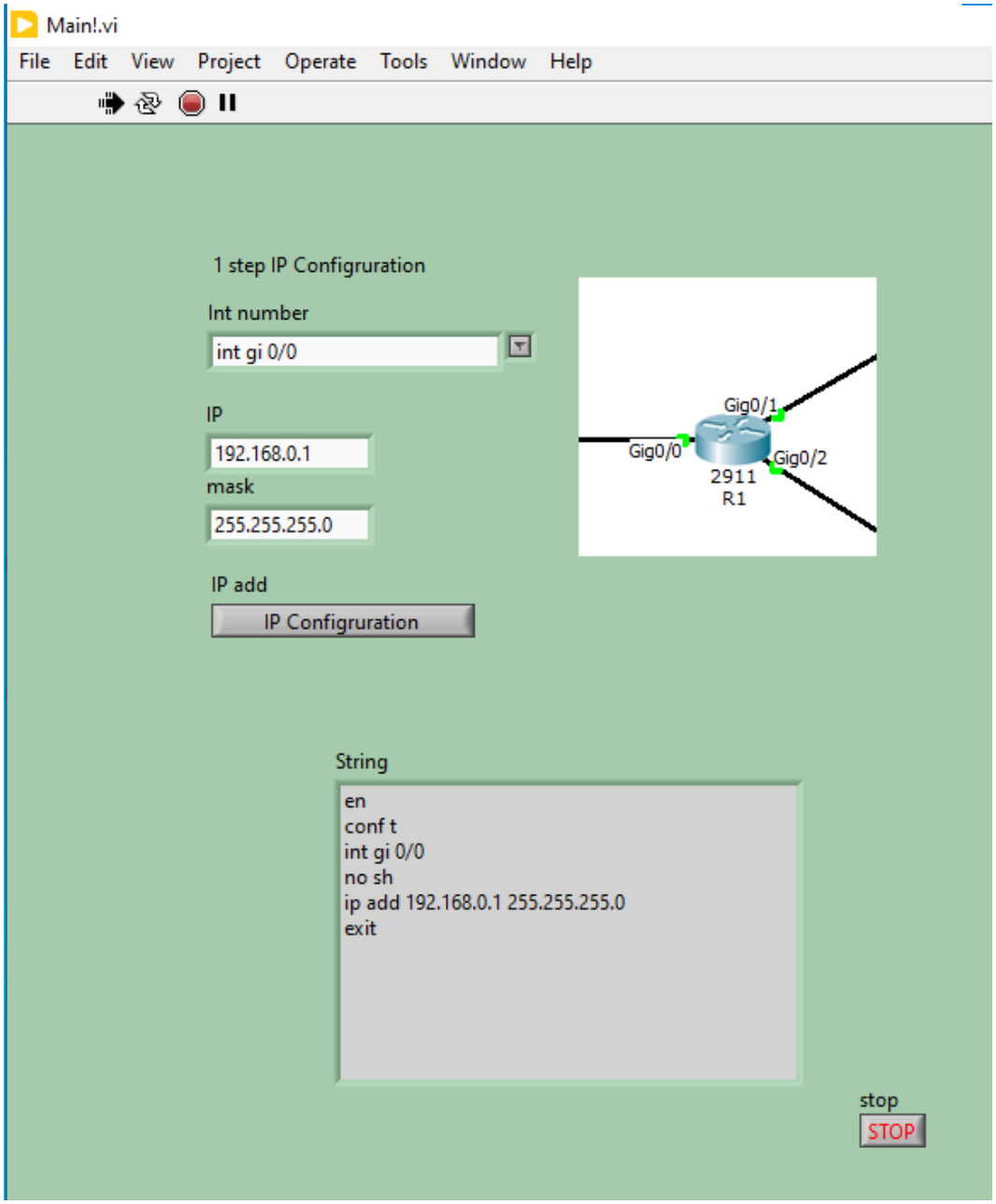


Рисунок 2.20 – Передня панель (інтерфейс) програми конфігурування роутера Cisco

На наведених рисунках зображено роботу із символьними рядками (string), завдяки яким з графічних елементів формувався код конфігурації роутерів Cisco. Сформований код можна скопіювати на мережеве обладнання, тим самим значно скоротивши час на рутинні та повторювані операції, а також уникнувши зайвих синтаксичних помилок.

РОЗДІЛ 3. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА ТЕХНОЛОГІЯ ПРОЄКТУВАННЯ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ETHERNET

3.1 Описова модель предметної області мультисервісної мережі Ethernet

Аналіз наведеної на рисунку 2.2 комп'ютерної мережі надав можливість описати предметну область у вигляді структурної формули W:

$$W =< Routers,\ Switches,\ PC,\ IPPhones\ ,\ IPTV\_Players >, \quad (3.1)$$

де *Routers* – множина роутерів мультисервісної мережі;

Switches – множина комутаторів мережі;

PC – множина комп'ютерів мережі;

IPPhones – множина VoIP телефонів;

IPTV_Players – множина VLC Media Players для трансляції та перегляду multicast контенту у мережі.

$$Routers =< Real\_Routers,\ Virtual\_Routers >, \quad (3.2)$$

де *Real_Routers* – множина реальних роутерів Cisco;

Virtual_Routers – множина віртуальних роутерів, реалізованих на ПК за допомогою емулятора GNS3.

$$Real\_Routers =< \text{Interface},\ \#AS,\ Allow\_\text{Multicast},\ Allow\_VoIP > \quad (3.3)$$

У кожного роутера мережі обов'язково є кілька мережевих інтерфейсів, тип даних інтерфейсів залежить від конкретної моделі роутера. Так, наприклад, роутер C2911 має інтерфейси gi0/0, gi0/1, gi0/2, роутер C1941 – інтерфейси gi0/0, gi0/1, а роутер C3640 – інтерфейси fa0/0, fa0/1, fa1/0.

У загальному вигляді інтерфейси роутера можна описати:

$$Interface =< type\_interface_i,\ \{ip\_parametr_{ij}\} \mid i \in \overline{(1,n)},\ j \in \overline{(1,2)} >, \quad (3.4)$$

де $typeinterface_i$ – типи інтерфейсів роутера;

$ip\_parametr_{ij}$ – параметри роутера (IP-адреса та маска інтерфейсу);
n – кількість інтерфейсів роутера.

Аналогічним чином можна описати складові параметри конфігурації віртуальних роутерів.

#AS – номер автономної системи, унікальний ідентифікатор оператора, якому належать роутери даної мережі і може приймати значення від 1 до 2^{16}=65536. Параметри номерів мереж підключених до роутера, які застосовуються при побудові динамічної маршрутизації визначаються структурною формулою 3.4

Allow_multicast – активація користувачем підтримки multicast трафіку у мережі Ethernet, може приймати значення «так» або «ні».

Allow_VoIP – активація користувачем підтримки IP-телефонії, також може приймати значення так або ні.

За умови якщо *Allow_VoIP* має значення «так» налаштування підтримки сервісу VoIP у загальному вигляді можна описати наступним чином:

$$Allow\_VoIP =< \ IPPhones_i, \ \{voip\_parametr_{ij}\} \mid i \in \overline{(1,n)}, \ j \in \overline{(1,2)} >, \qquad (3.5)$$

де $IPPhones_i$ – множина VoIP телефонів;
$voip\_parametr_{ij}$ – параметри VoIP телефонів (номер телефону та ім’я абонента);
n – кількість VoIP телефонів у мультисервісній мережі.

3.2 Розробка програмного забезпечення для автоматизованого налаштування мережевого обладнання

Використовуючи графічне середовище розробки програмних додатків LabVIEW у ході виконання кваліфікаційної магістерської роботи було розроблено програмне забезпечення, що дозволяє здійснити автоконфігурування мережевого обладнання (такого як маршрутизаторів та комутаторів) з використанням графічного інтерфейсу.

Приклад фронтальної панелі розробленого програмного забезпечення наведено на рисунку 3.1.

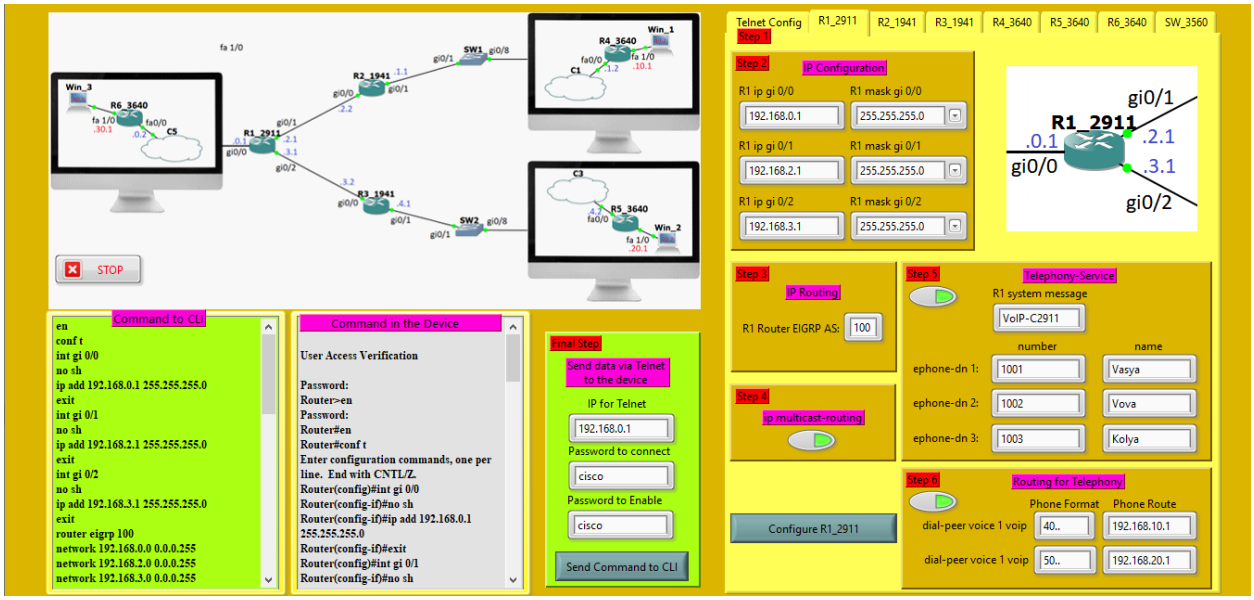


Рисунок 3.1 – Інтерфейс програмного забезпечення для автоконфігурування мережевого обладнання мультисервісної мережі Ethernet

Як було зазначено вище, розробники-початківці створюють програми-«простирадла» і програми-«спагетті», у той час як досвідчені LabVIEW-розробники ніколи не створять діаграм, що перевищують розмір екрану, навіть якщо програма складається із сотень модулів. Саме тому, при розробці програмного забезпечення, нами було використано парадигму програмування на

основі «подія-керованого кінцевого автомату на базі черги». Кінцевий автомат є одним із найпоширеніших і дуже зручних зразків проєктування для LabVIEW. Його можна використовувати для реалізації будь-якого алгоритму, що явно описується діаграмою станів або блок-схемою. Кінцеві автомати зазвичай реалізують алгоритми прийняття рішень помірної складності, наприклад, для діагностики або управління процесами.

В розробленій нами програмі створено ряд екранних форм, через які користувач заносить ключові параметри, необхідні для конфігурації мережевого обладнання, а по натиску на конопку «Configure…» запускається процес автоматичного формування конфігураційних команд роутерів та комутаторів у відповідності до вимог синтаксису, що висувається до обладнання Cisco.

За ключову ідею побудови програми було взято висновок, що сформувався на підставі багаторічного досвіду роботи з мережевим обладнанням Cisco. Його можна сформувати наступним чином. У більшості випадків під час конфігурування стандартних мережевих функцій в консоль доводиться вводити велику кількість однотипних команд, час від часу змінюючи в них лише ключові параметри, такі як: номери інтерфейсів, їх IP-адреси та маски, параметри пулів адрес, IP-адреси роутера за замовчуванням і DNS-сервера при конфігурації DHCP серверів, зазначення IP-адреси сервера при налаштуванні IP-телефонії та номерів телефонів. Це, звичайно, вкрай важливі параметри, але необхідність слідкувати за дотриманням чіткого синтаксису вводу команд відволікає увагу початківця від головного: розуміння ключових параметрів налаштування мережевих сервісів та логіки роботи мережевого обладнання. Тому наша програма взяла на себе рутинну задачу: автоматичне формування команд конфігурації та дотримання синтаксису, а користувач формує ключові параметри конфігурації та виконує загальний контроль за процесом формування та внесення команд конфігурації в налаштування мережевого обладнання. На рисунку 3.2 наведено частину блок-

діаграми (графічне уявлення коду) програми автоконфігурування мережевого обладнання мультисервісної мережі Ethernet, що відповідає за відстежування дій користувача з графічним інтерфейсом програми.

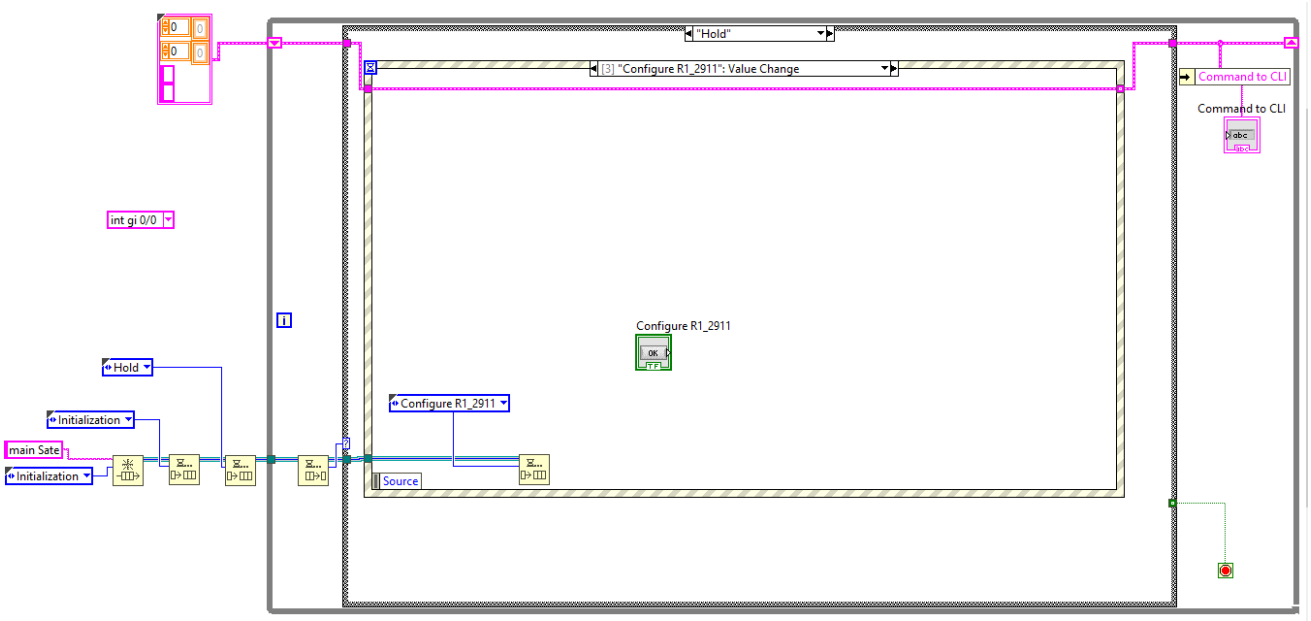
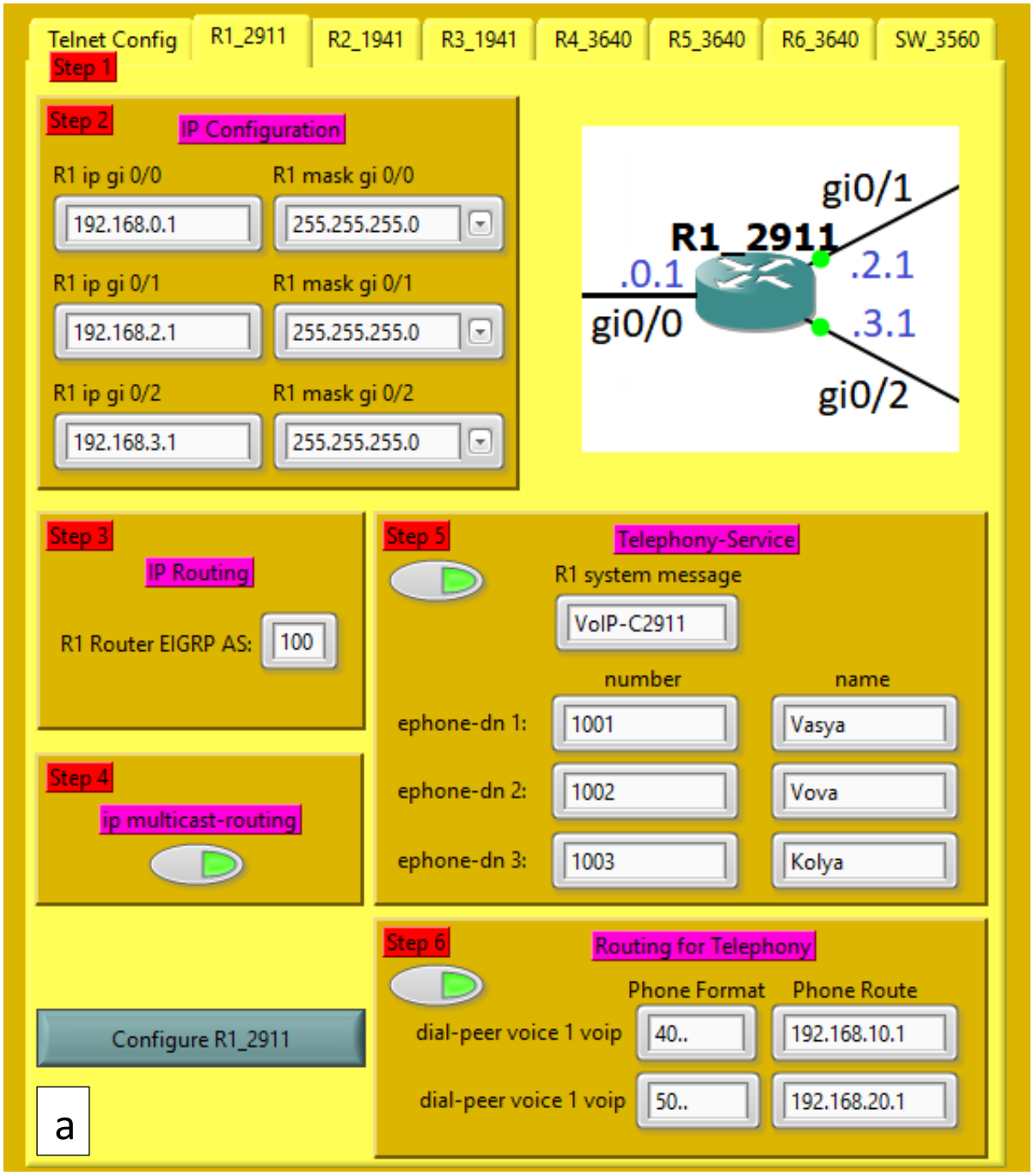


Рисунок 3.2 – Блок-діаграма програми відповідальна за відстежування дій користувача з графічним інтерфейсом програми

У даному випадку в кейсі «Hold» виконується безперервне відслідковування за діями користувача і при натисканні на ключові кнопки графічного інтерфейсу (такі як «Configure…», «Send Command to CLI» та інші) запускається чітка послідовність (черга) операцій конфігурування мережевого обладнання, конфігурацію якого у даний час здійснює користувач програми.

На рисунку 3.3 наведено частину передньої панелі (інтерфейсу) програми (рис 3.3 а) та відповідну блок-діаграму (рис 3.3 б) формування конфігурації команд для роутера Cisco 2911, що був обраний як типовий зразок мережевого обладнання нашої мультисервісної мережі, та за прикладом якого були створені подальші кейси роботи з іншим мережевим обладнанням нашої схеми.


Telnet Config
R1_2911
R2_1941
R3_1941
R4_3640
R5_3640
R6_3640
SW_3560
Step 1
Step 2
IP Configuration
R1 ip gi 0/0
192.168.0.1
R1 mask gi 0/0
255.255.255.0
R1 ip gi 0/1
192.168.2.1
R1 mask gi 0/1
255.255.255.0
R1 ip gi 0/2
192.168.3.1
R1 mask gi 0/2
255.255.255.0
gi0/1
R1_2911
.0.1
.2.1
gi0/0
.3.1
gi0/2
Step 3
IP Routing
R1 Router EIGRP AS:
100
Step 4
ip multicast-routing
Step 5
Telephony-Service
R1 system message
VoIP-C2911
number
name
ephone-dn 1:
1001
Vasya
ephone-dn 2:
1002
Vova
ephone-dn 3:
1003
Kolya
Step 6
Routing for Telephony
Phone Format
Phone Route
dial-peer voice 1 voip
40..
192.168.10.1
dial-peer voice 1 voip
50..
192.168.20.1
Configure R1_2911
a

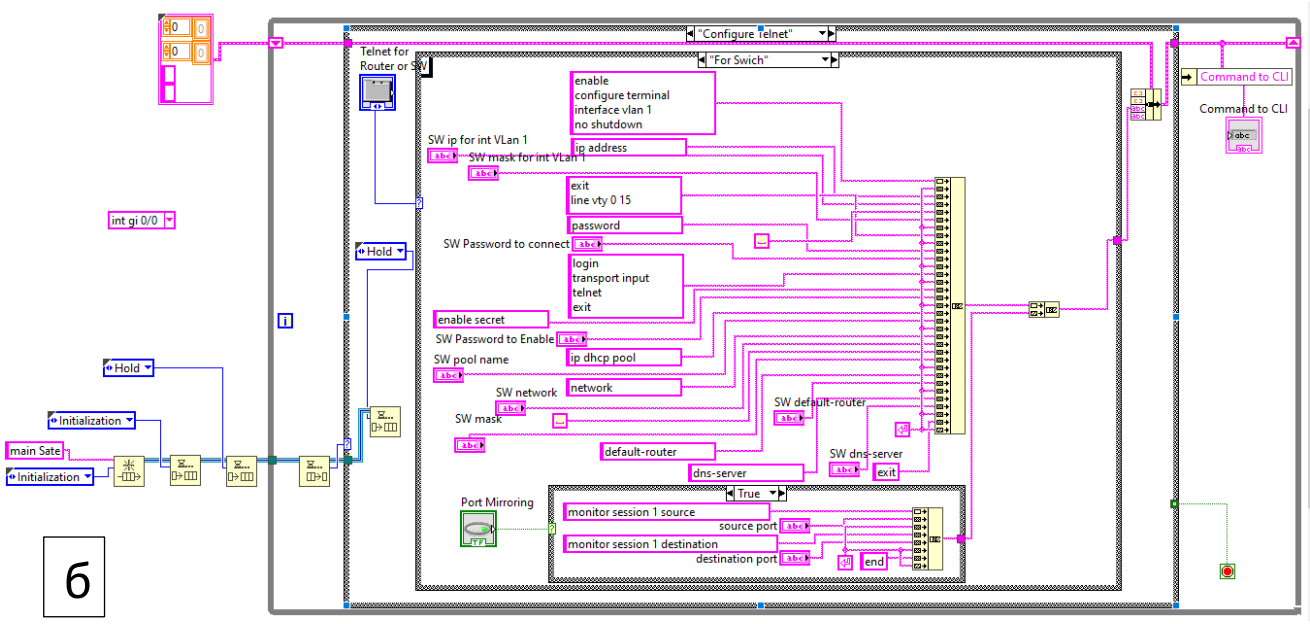


Рисунок 3.3 – Частина інтерфейсу програми (а)
та блок-діаграма (б) формування конфігурації роутера Cisco 2911

На рисунку 3.3 (а) можна спостерігати послідовність етапів (step1 - step6) конфігурації роутера R1_2911 (Cisco 2911) за допомогою графічного інтерфейсу користувача. Далі наведено детальних опис даних етапів.

Step 1. Вибір необхідної моделі мережевого обладнання. Серед наведених варіантів можна вибрати роутери Cisco моделі: C2911, C1941 та C3640, а також L3 комутатор Cisco серії Catalist 3560, що відповідають пристроям нашої мультисервісної мережі, зображеним на рисунку 2.2 Розділу 2 пояснювальної записки до кваліфікаційної магістерської роботи. Також на даному етапі можливо вибрати меню конфігурації протоколу Telnet (Telnet Config) де можна, з урахуванням ключових параметрів заданих користувачем, згенерувати команди налаштування протоколу Telnet на роутерах або комутаторах Cisco.

Step 2. Налаштування IP-адреси та маски на інтерфейсах роутера. У даної моделі роутера наявні 3 мережевих інтерфейси gigabitEthernet 0/0, gigabitEthernet 0/1 та gigabitEthernet 0/2. Попередніми налаштуваннями кожному з цих інтерфейсів роутера задано значення за замовчуванням, що відповідають

базовій схемі конфігурації наведеній у Розділі 2 на рисунку 2.2, але користувач тут і надалі в графічному інтерфейсі має змогу за необхідності змінити чи підкорегувати ключові параметри конфігурації обладнання відповідно до власних потреб або поставлених задач.

Step 3. Налаштування динамічної маршрутизації. В нашій програмі реалізовано налаштування динамічної маршрутизації за протоколом EIGRP. Даний протокол є найбільш сучасним протоколом динамічної маршрутизації та оптимальним варіантом при налаштуванні мережевого обладнання Cisco, оскільки є пропрієтарним протоколом фірми Cisco та оптимізований для роботи з мережевим обладнанням даного виробника. В налаштуваннях динамічної маршрутизації клієнту залишається лише вказати номер автономної системи (умовний номер власника мережі), а інші параметри IP-адрес мереж та масок, що під'єднані до роутера, будуть взяті автоматично з конфігураційних параметрів вказаних на етапі Step 2.

Step 4. З метою підтримки мережею multicast трансляції (за замовчуванням ця функція на роутерах вимкнена) та активації протоколу PIM (необхідного для забезпечення трансляції IPTV трафіку у мережі) на інтерфейсах роутерів клієнт може активувати функцію автоконфігурування необхідних параметрів, натиснувши на відповідну кнопку у даному меню графічного інтерфейсу. У разі, якщо цей функціонал не є необхідним, відповідну кнопку меню слід вимкнути (оскільки вона активована за замовчуванням відповідно до прогнозованих параметрів налаштування схеми наведеної у Розділі 2 на рисунку 2.2).

Step 5. Налаштування сервісу IP-телефонії. В нашій програмі підтримка даного сервісу реалізована лише для роутерів C2911 та C3640. Для роутерів C1941 такі конфігураційні можливості відсутні, оскільки роутери цієї серії не підтримують функціонал «telephony-service». У зазначеному екранному меню користувачу надано можливість ввести параметри «system message»

(повідомлення, що буде відображатися на екранах телефонів, які у якості VoIP шлюзу вибрали даний роутер) та номери для трьох телефонів і відповідні імена осіб, що є користувачами цих телефонів. Інші конфігураційні параметри налаштування «telephony-service» здебільшого є стандартними та конфігуруються у коді автоматично відповідно до параметрів заданих на попередніх етапах.

Step 6. В нашій мережі передбачено одночасне функціонування декількох незалежних VoIP шлюзів. Тож для організації переадресування дзвінків між VoIP шлюзами на роутері необхідно налаштувати наступні команди VoIP маршрутизації. Користувачу у даному меню необхідно ввести «префікс» телефонних номерів віддаленого VoIP шлюзу та його IP-адресу, після чого програма сама сформує відповідні конфігураційні команди для роутера.

По завершенню налаштування роутера користувач має натиснути на кнопку «Configure R1_2911» і «подія-керований кінцевий автомат на базі черги» запустить алгоритм формування конфігураційних команд для роутера. Результат роботи даного етапу можна спостерігати на рисунку 3.3, де відображено вікно програми, команди у якому були сформовані автоматично у відповідності з вимогами користувача.

Аналогічним чином користувач за допомогою екранних форм, розробленого нами програмного забезпечення може здійснити автоконфігурування роутерів C1941 та C3640, а також L3 комутатора Cisco серії Catalist 3560. Приклади відповідних частин графічного інтерфейсу наведено на рисунку 3.4 та рисунку 3.5.

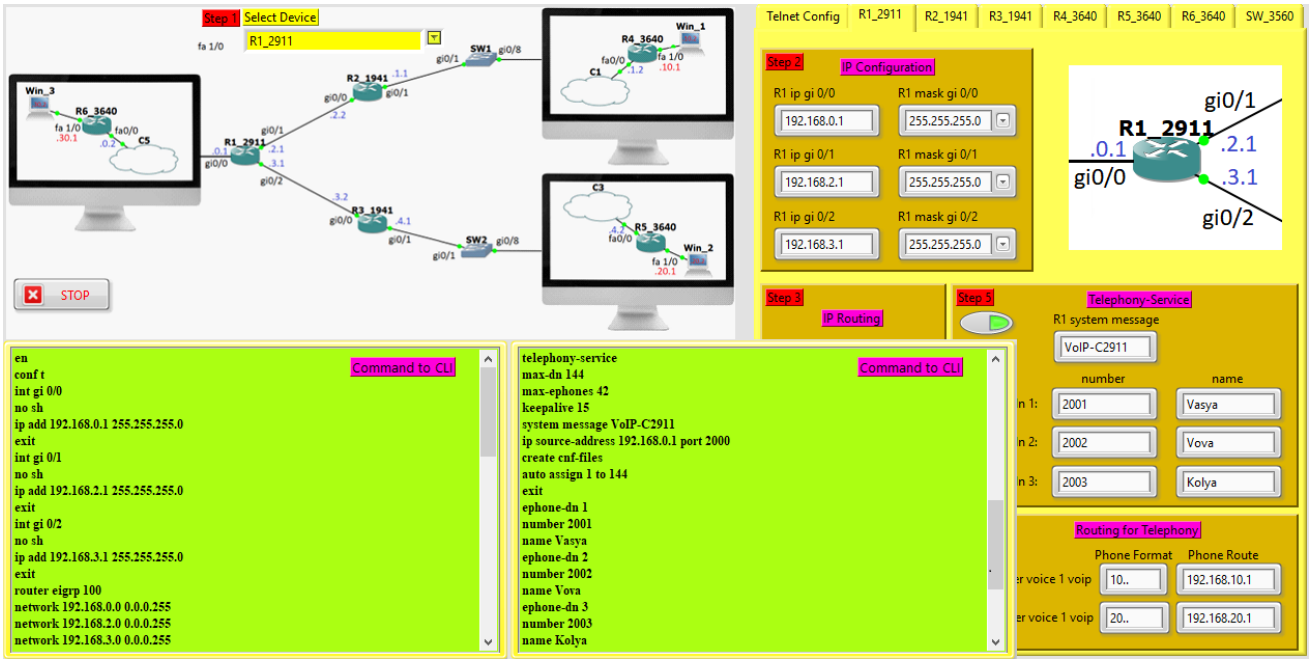


Рисунок 3.3 – Автоконфігурування мережевого обладнання відповідно до налаштувань вказаних на етапах step1 - step6

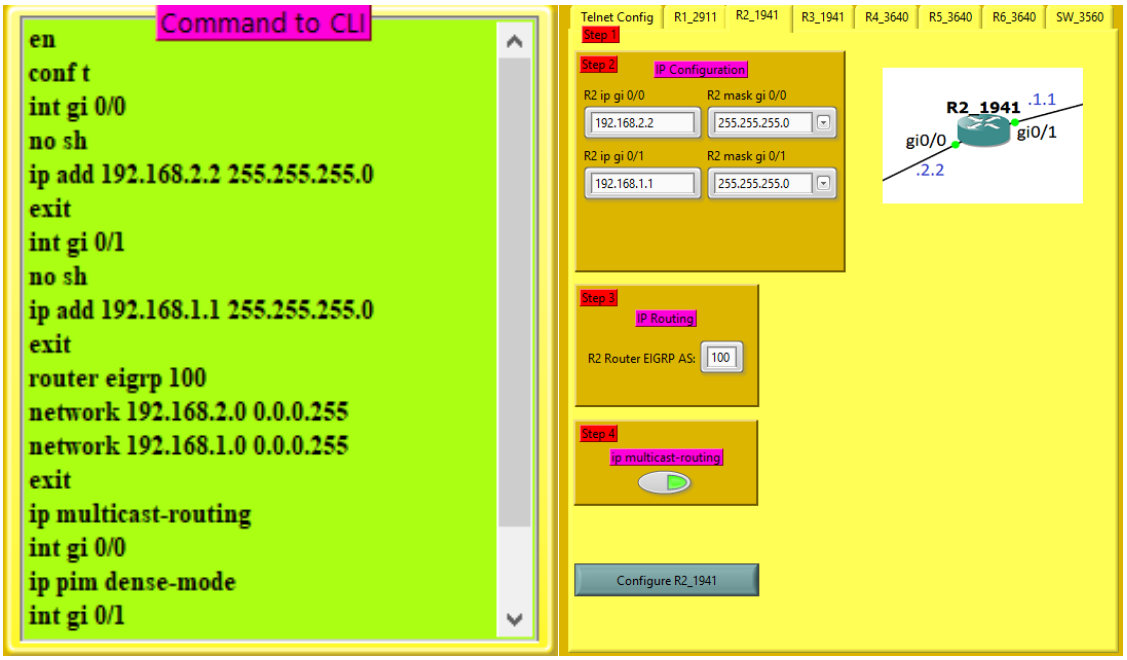


Рисунок 3.4 – Графічний інтерфейс та результат автоконфігурування роутера Cisco 1941

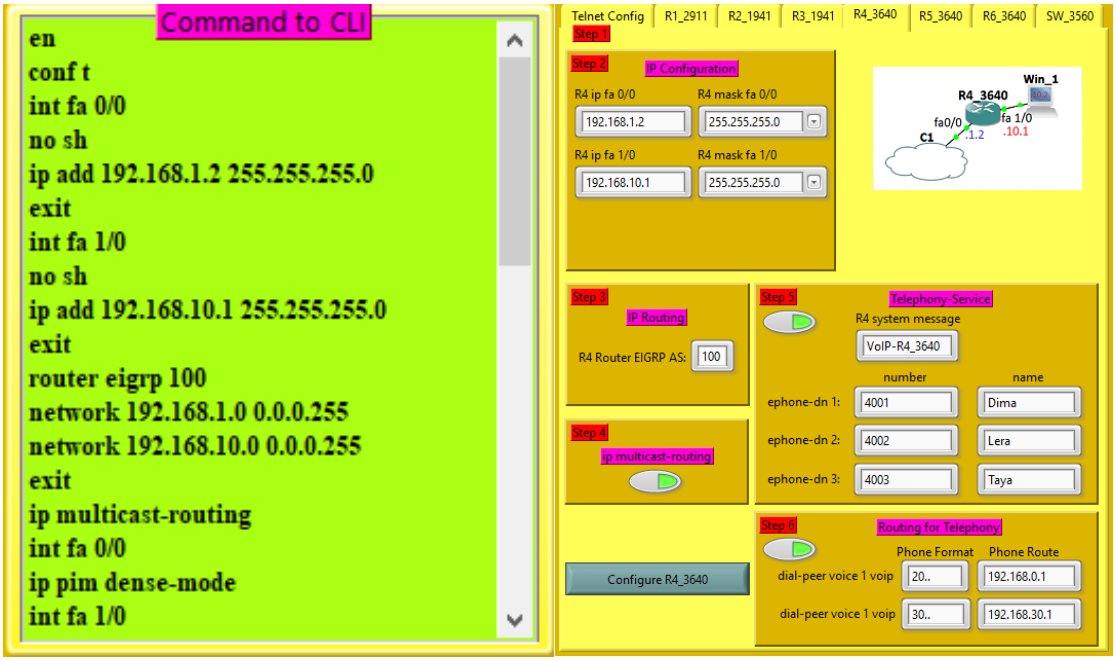


Рисунок 3.5 – Графічний інтерфейс та результат автоконфігурування роутера Cisco 3640

Також окремо слід звернути увагу на важливий функціонал у конфігурації мережевого обладнання, що користувач може обрати на етапі Step 1. Обравши у верхньому меню конфігурації вкладку «Telnet Config», користувач має змогу з урахуванням заданих ним ключових параметрів згенерувати команди налаштування протоколу Telnet на роутерах або комутаторах Cisco. Вбудований у нашу програму механізм активації протоколу Telnet дозволив у автоматичному режимі через локальну мережі одразу ж після автоконфігурування роутерів на етапах step1 - step6 занести дані конфігураційні параметри безпосередньо на віддалені роутери та комутатори мережі. Це безперечно можна вважати однією зі значних переваг роботи нашої програми, що здійснює конфігурування мультисервісної мережі Ethernet з інтеграцією реального та віртуального обладнання Cisco.

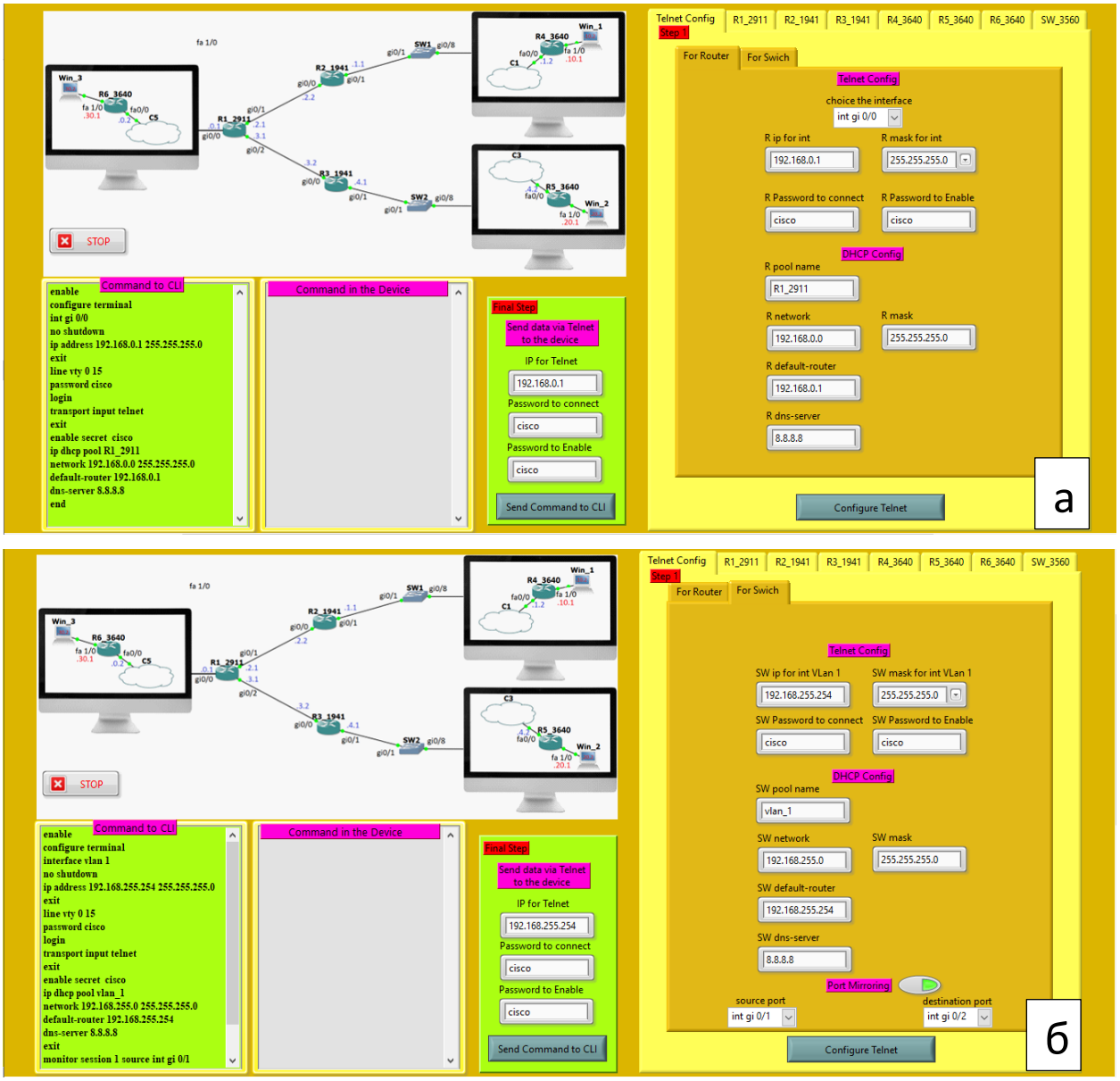


Рисунок 3.6 – Графічний інтерфейс автоконфігурування протоколу Telnet на роутерах Cisco (а) та L3 комутаторі Cisco Catalist 3560 (б)

На рисунку 3.6 наведено графічні інтерфейси, за допомогою яких користувач може згенерувати базові команди налаштування протоколу Telnet для роутерів Cisco (а) та L3 комутатора Catalist 3560 (б) відповідно до вказаних ним ключових параметрів конфігурації. До таких параметрів відноситься активація та

присвоєння IP-адреси для мережевого інтерфейсу роутера, або віртуального інтерфейсу (VLan 1 для комутатора), а також зазначення паролів на доступ до віддаленого пристрою. Окрім цього передбачено налаштування DHCP серверу на мережевих пристроях, що дозволить уникнути необхідності вручну налаштовувати параметри роботи з мережею на ПК, з якого надалі за допомогою нашого програмного забезпечення буде здійснюватися автоконфігурування роутерів та комутаторів мережі. На рисунку 3.7 наведено графічний інтерфейс та блок-діаграму підпрограми налаштування протоколу Telnet, що є невід'ємною складовою нашої загальної програми.

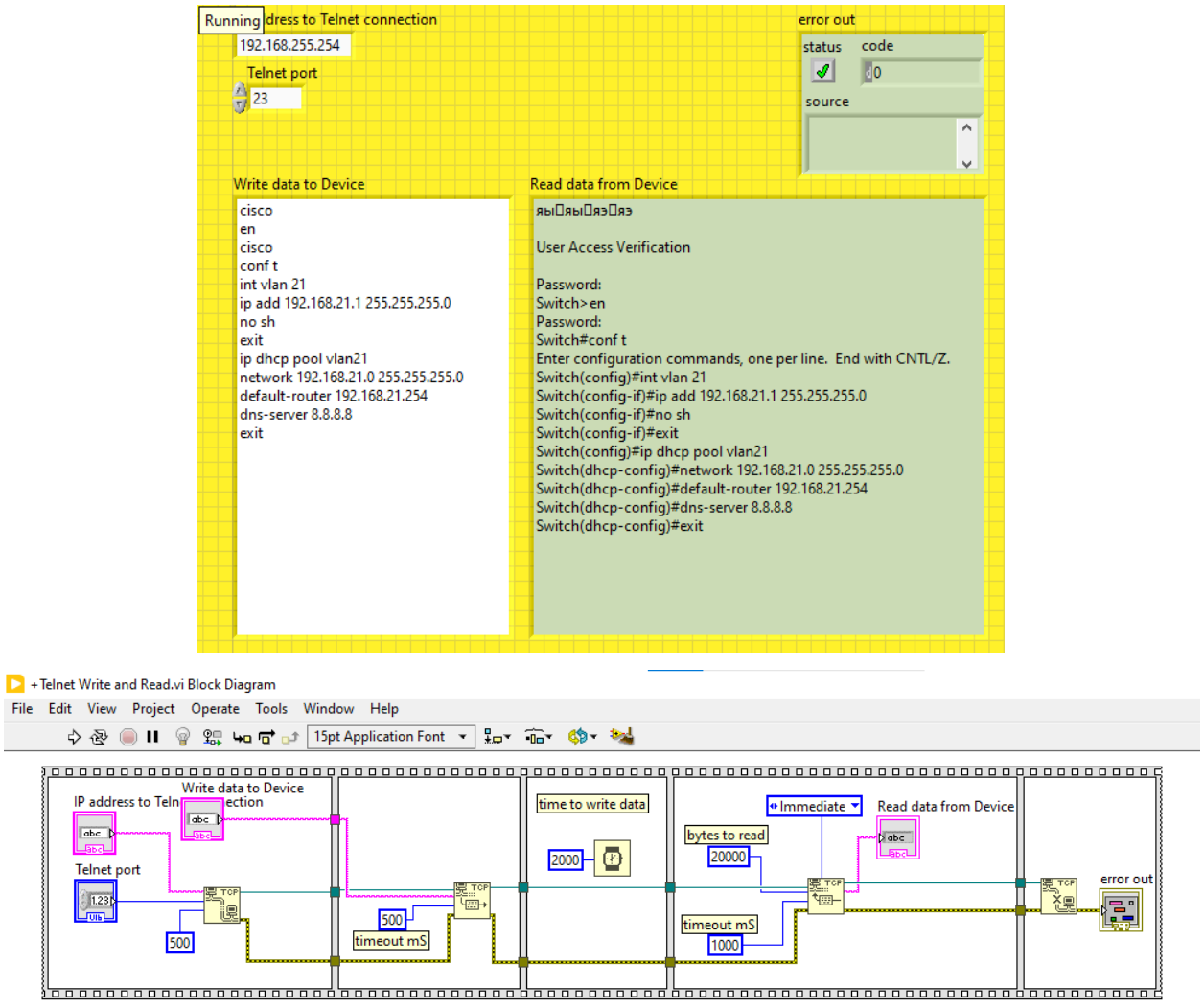


Рисунок 3.7 – Графічний інтерфейс та блок-діаграма підпрограми налаштування протоколу Telnet

3.3 Тестування розробленого програмного забезпечення на віртуальному та «живому» обладнанні Cisco

Тестування програмного забезпечення для автоконфігурування мережевого обладнання мультисервісної мережі Ethernet, розробленого під час виконання кваліфікаційної магістерської роботи, здійснювалося як з використанням симуляторів мереж Cisco Packet Tracer та GNS3, так і з використанням «живого» телекомунікаційного обладнання Cisco. У даному розділі роботи буде наведено опис ключових етапів тестування програмного забезпечення та відповідні результати перевірки роботи сформованих конфігураційних параметрів на «живому» мережевому обладнанні.

Тестування програмного забезпечення для автоконфігурування роутера Cisco 2911.

На першому підготовчому кроці у меню конфігурації протоколу Telnet (вкладка Telnet Config) здійснювалось автоконфігурування команд налаштування протоколу Telnet для маршрутизатора Cisco (рисунок 3.8). Дані команди є типовими для будь-якого маршрутизатора нашої мультисервісної мережі Ethernet і користувачу слід лише обрати мережевий інтерфейс роутера, задати йому IP-адресу та маску, а також вибрати пароль на доступ до консолі та до привілейованого режиму конфігурації роутера. Також для зручності передбачено налаштувати DHCP сервер, що позбавить користувача необхідності в ручному режимі налаштовувати мережеві конфігураційні параметри на ПК, з якого надалі буде здійснюватися автоконфігурування роутера через локальну мережу Ethernet.

Визначивши у диспетчері пристроїв ПК номер віртуального послідовного COM порту (рисунок 3.9), що використовується для підключення до Console порту роутера, використовуючи кабель USB-miniUSB та програму Putty (рисунок 3.10), було встановлено консольне з’єднання з маршрутизатором.

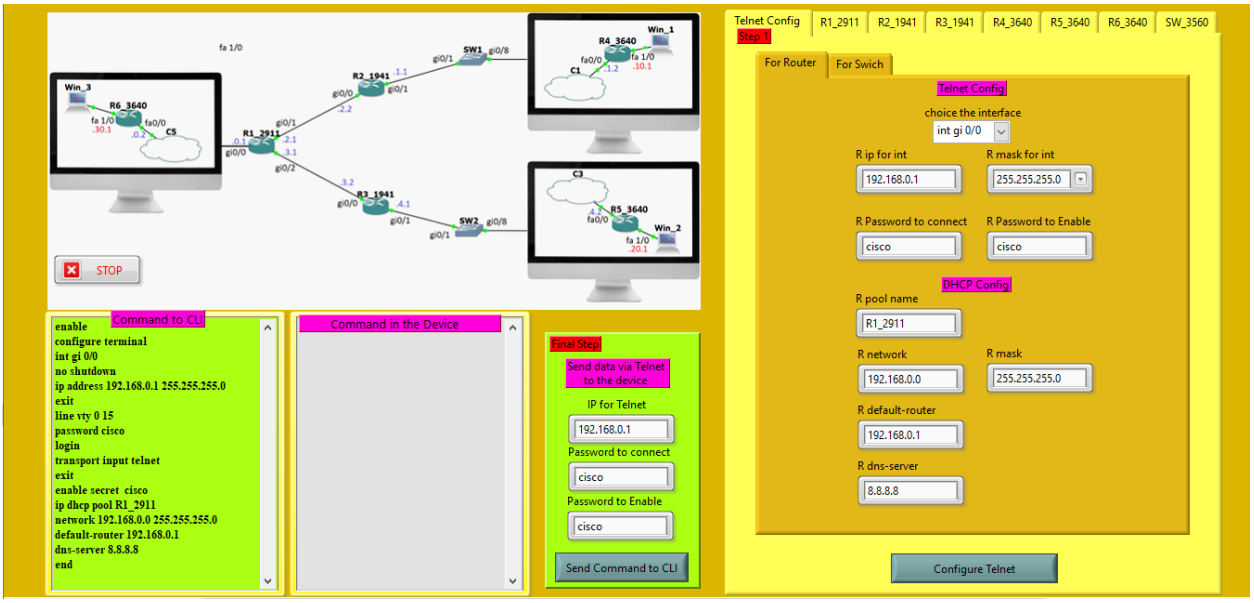


Рисунок 3.8 – Графічний інтерфейс автоконфігурування протоколу Telnet. Крок 1

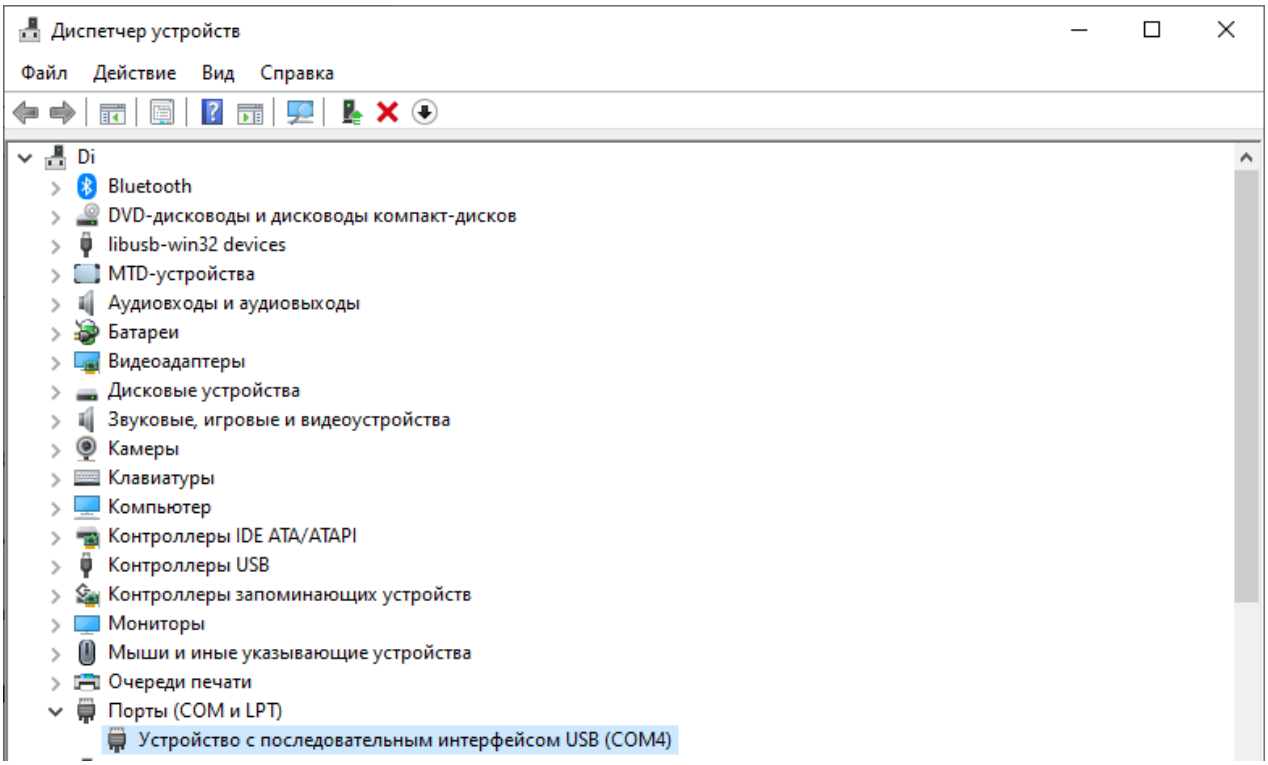


Рисунок 3.9 – Визначення активного віртуального послідовного COM порту для підключення до Console порту комутатора. Крок 2

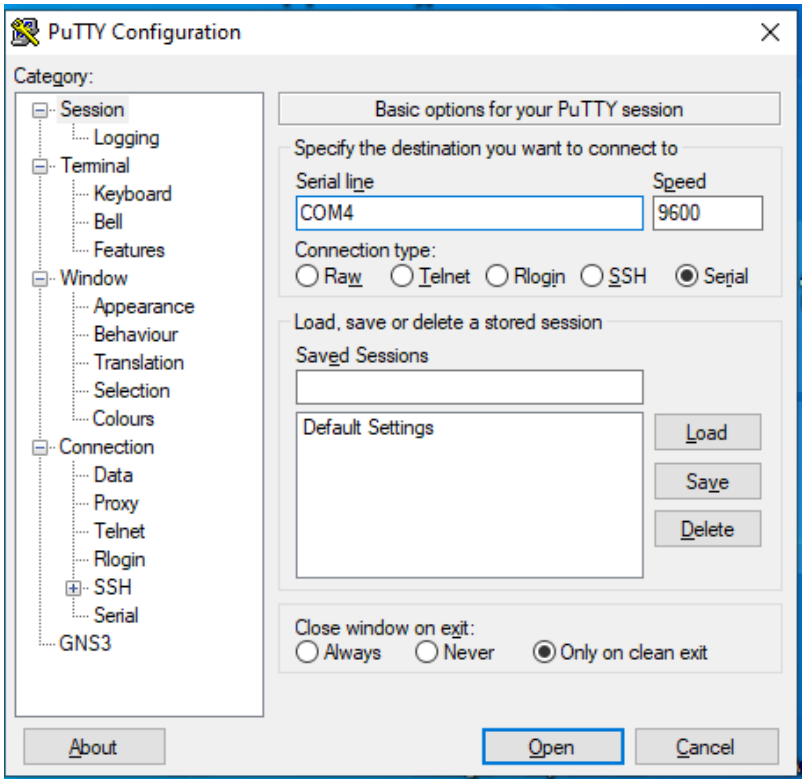


Рисунок 3.10 – Налатування програми Putty
для підключення через порт Console до роутера C2911. Крок 3

Після цього команди конфігурації протоколу Telnet через буфер обміну даними були скопійовані з вікна нашої програми через консоль putty у пам'ять комутатора (рисунок 3.11).

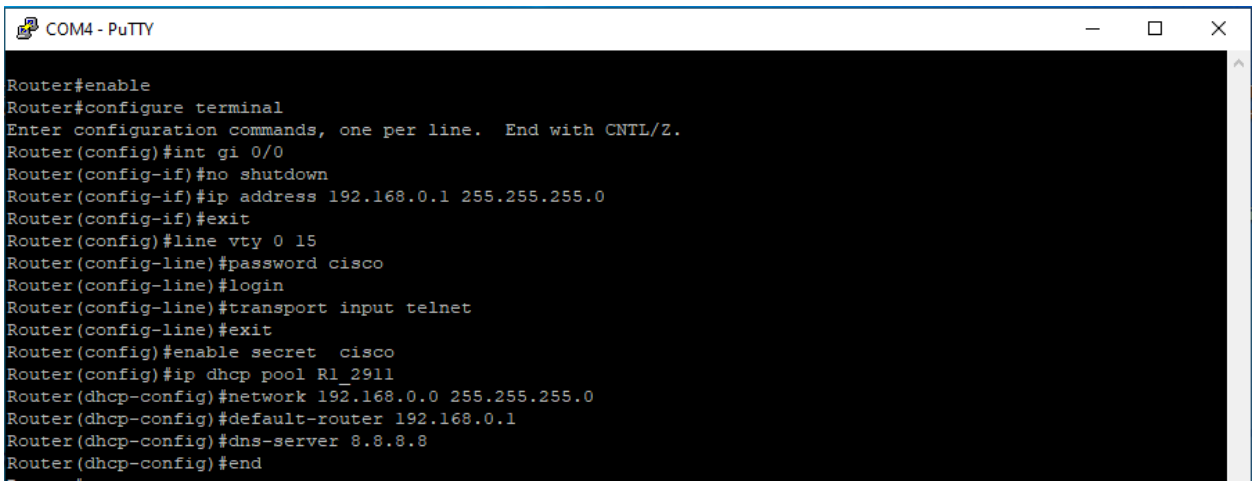


Рисунок 3.11 – Попереднє конфігурування протоколу Telnet
через консоль програми Putty. Крок 4

Підключившись за допомогою кабелю вита пара до порту gigabitEthernet 0/0 маршрутизатора здійснено перевірку Ethernet з'єднання та коректності роботи протоколу DHCP (рисунок 3.12).

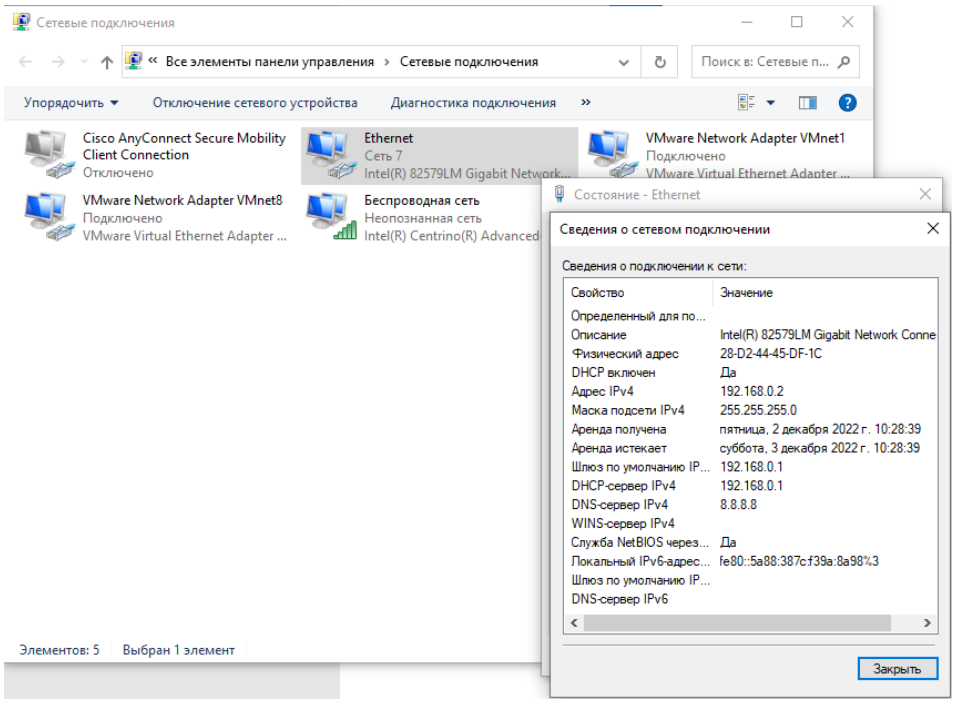


Рисунок 3.12 – Перевірка Ethernet з'єднання
та коректності роботи протоколу DHCP на ПК. Крок 5

Впевнившись у можливості віддаленого підключення та конфігурування маршрутизатора через локальну мережу на наступному етапі здійснено автоконфігурування інтерфейсів роутера, протоколу динамічної маршрутизації, підтримки мережею multicast трафіку та сервісів IP-телефонії відповідно до детально описаних у попередньому підрозділі кроків step1- step6 (рисунок 3.13).

Надалі команди автоконфігурації роутера з використанням меню «Send Command to CLI», вказавши параметри аутентифікації користувача, через мережу Ethernet та з використанням протоколу Telnet автоматично переносяться на роутер Cisco 2911. Успішне виконання даного етапу можна спостерігати у вікні інтерфейсу нашої програми у блоці «Command in the Device». Як можна

спостерігати, даний етап у нас пройшов успішно та автоматично сконфігуровані нашою програмою команди були коректно записані у Command line interface (CLI) роутера (рисунок 3.14).

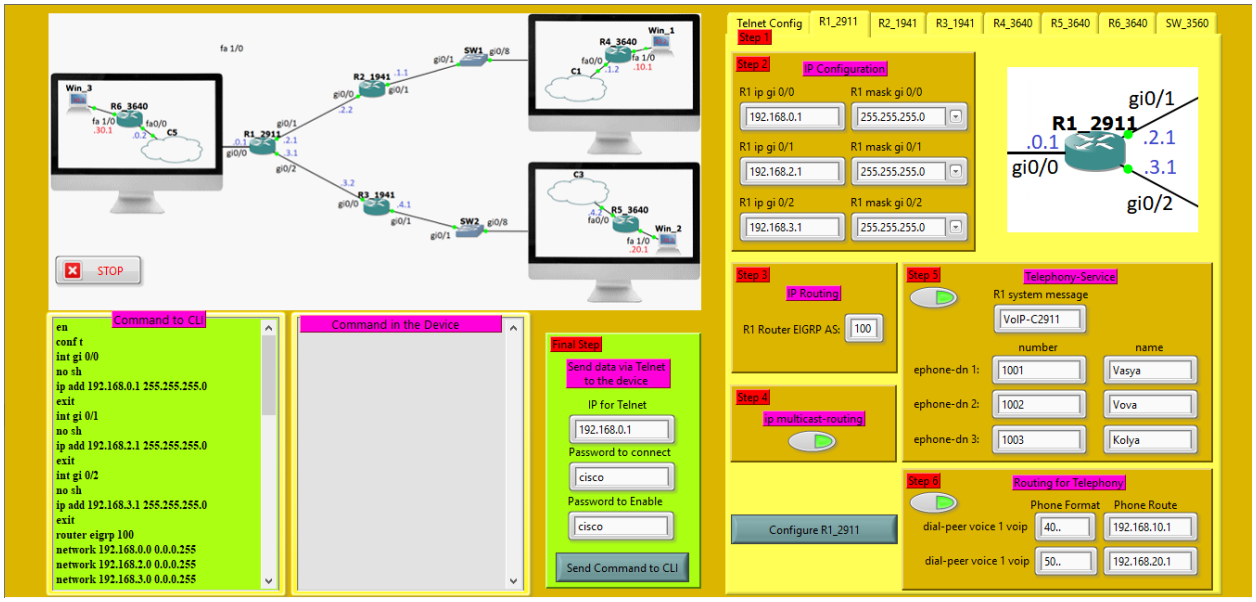


Рисунок 3.13 – Автоконфігурування роутера Cisco 2911. Крок 6

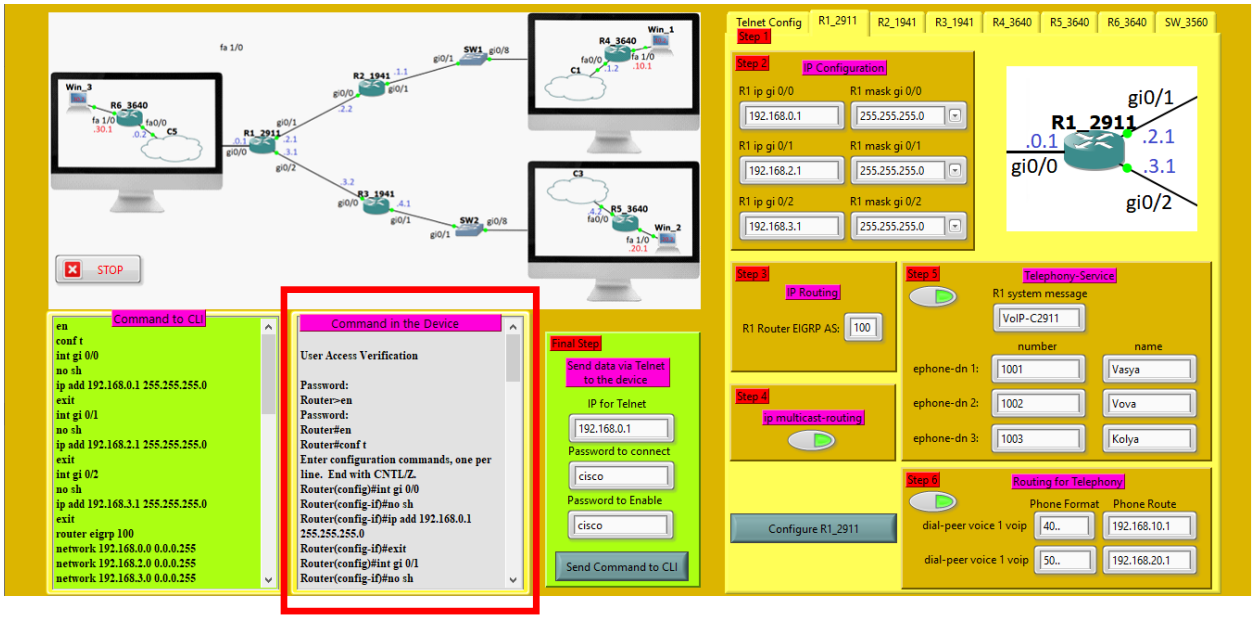


Рисунок 3.14 – Запис команд автоконфігурування через мережу Ethernet по протоколу Telnet на роутер Cisco 2911. Крок 7

Перевірку коректності запису команд автоконфігурування додатково було здійснено з використанням консольного з’єднання через програму Putty. Результат команди Router#sh running-config наведено на рисунку 3.15.

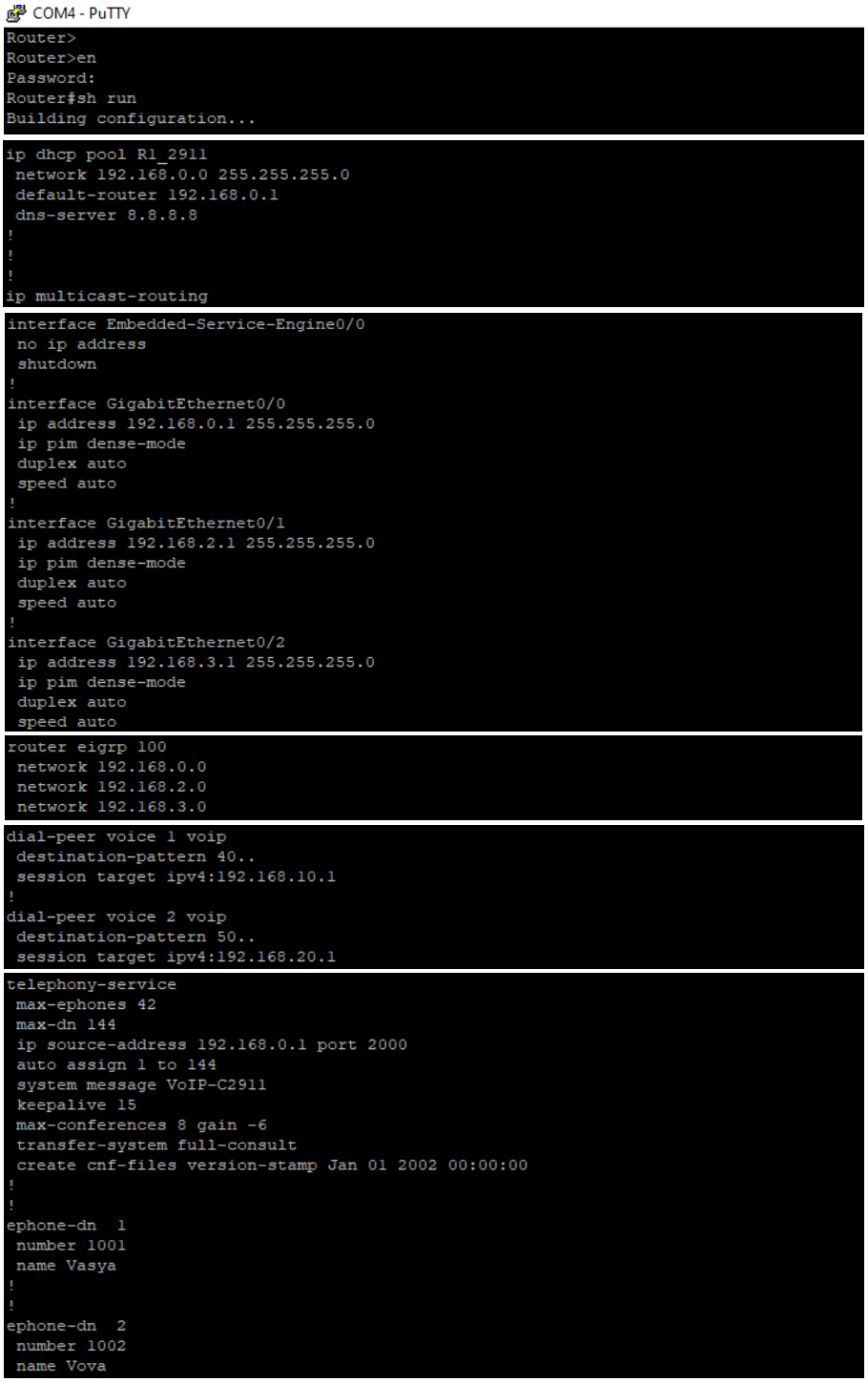


Рисунок 3.15 – Перевірка коректності запису команд автоконфігурування з використанням консольного з’єднання через програму Putty. Крок 8

Аналогічні етапи тестування програмного забезпечення були здійснені на всіх роутерах нашої мультисервісної мережі. У результаті тестування було налаштовано мережеві інтерфейси обладнання. Завдяки протоколу динамічної маршрутизації EIGRP роутери успішно визначили номери віддалених мереж та побудували до них найкоротші маршрути. Активація підтримки multicast трафіку дозволила здійснити трансляцію IPTV трафіку у мережі, а налаштування сервісів IP-телефонії дозволила успішно здійснювати телефонні дзвінки між Cisco IP Communicator-ами (IP Phone), встановленими на ПК, та VirtualBox. Результати успішного тестування розробленого нами програмного забезпечення та налаштованої за допомогою нього мережі зображено на рисунках 3.16-3.17.

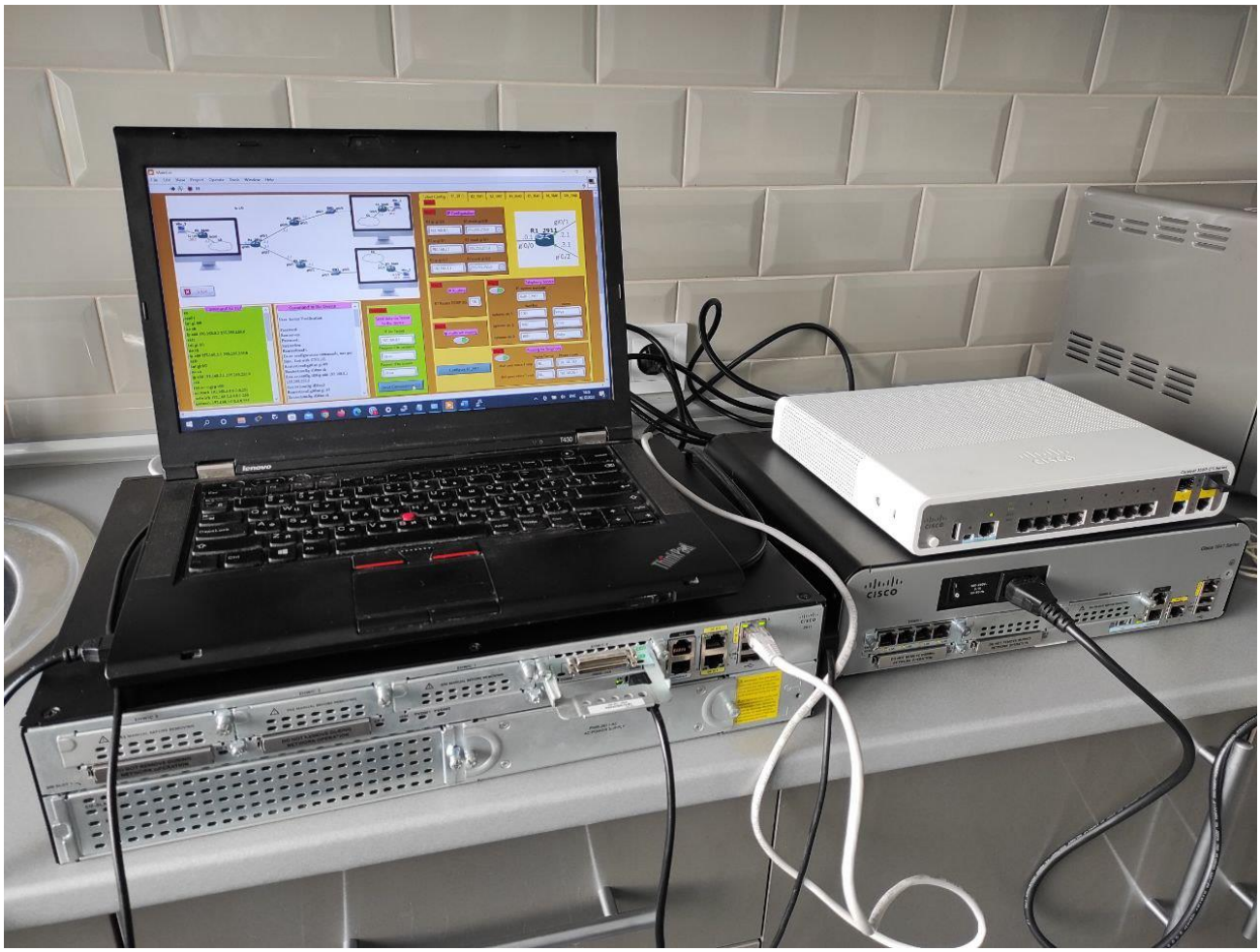


Рисунок 3.16 – Автоконфігурування роутерів мультисервісної мережі Ethernet

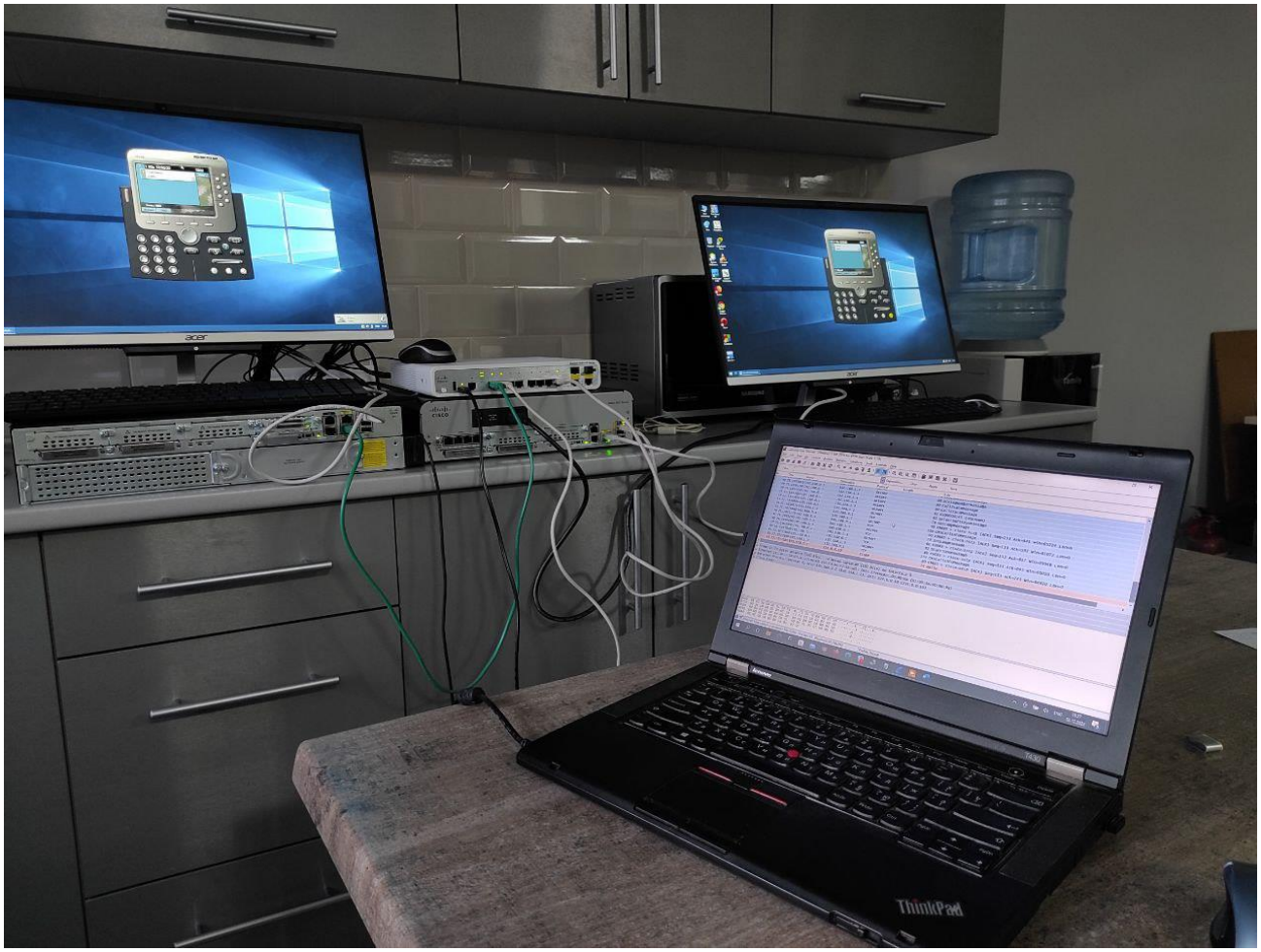


Рисунок 3.17 – Тестування сервісу VoIP у сконфігурованій
в автоматичному режимі мережі Ethernet

Розроблена нами інформаційно-комунікаційна технологія проєктування мультисервісної мережі Ethernet з інтеграцією реального та віртуального обладнання Cisco має значну практичну цінність, оскільки, завдяки інтуїтивно зрозумілим екранним формам, дає можливість значно комфортніше, надійніше та швидше здійснювати автоконфігурування основних компонентів сучасних комп’ютерних мереж з підтримкою сервісів IPTV та VoIP.

Однак, крім практичної цінності, наша технологія також дозволяє відкрити перспективу науковому дослідженню особливостей роботи сучасних комп'ютерних мереж. З цією метою у нашій програмі передбачено підтримку автоконфігурування функції дзеркалізації портів на L3 комутаторах Catalist 3560 (рисунок 3.18).

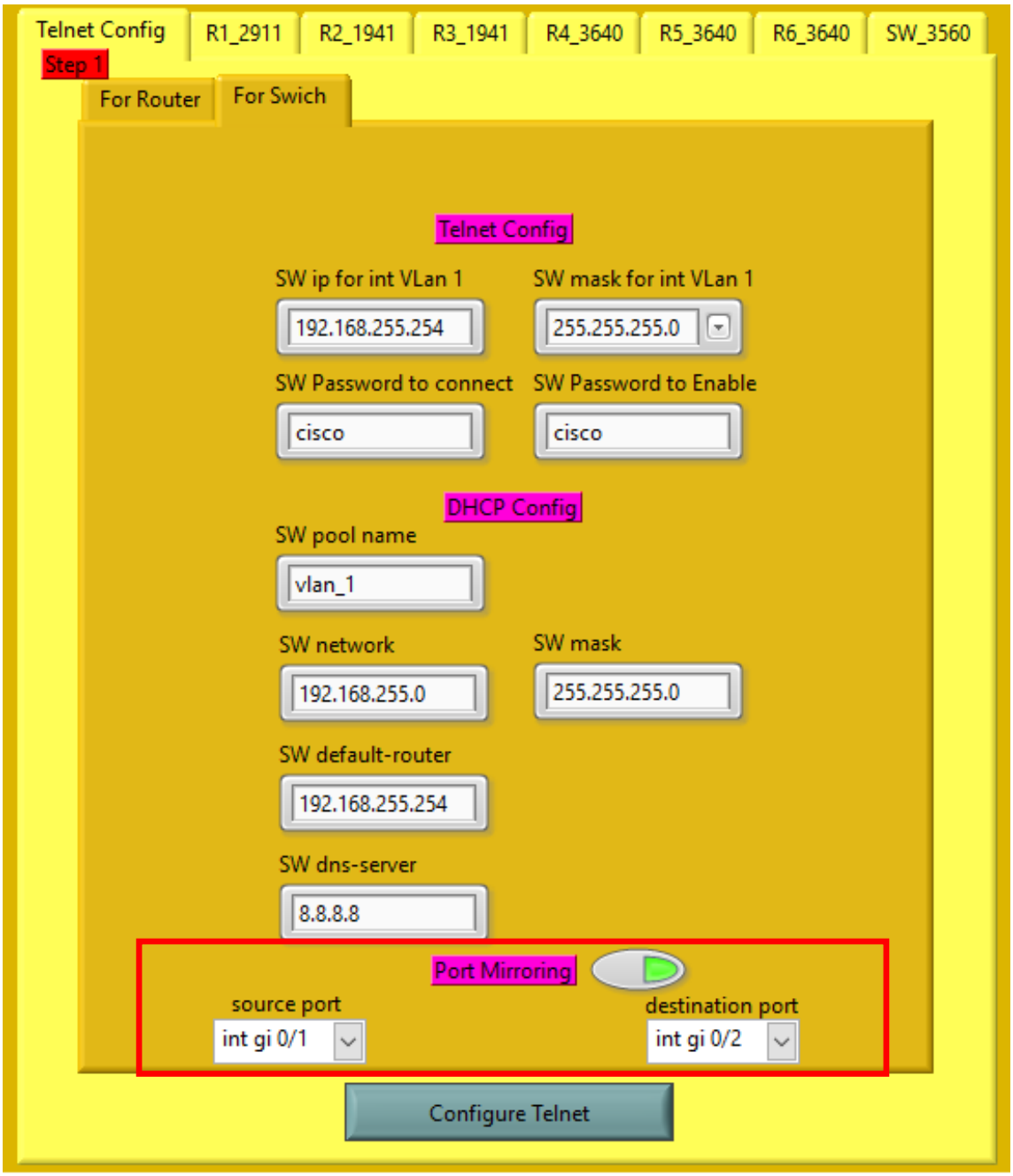


Рисунок 3.18 – Налаштування дзеркалізації портів
на L3 комутаторах Cisco Catalist 3560

Завдяки підтримці даного функціоналу, вказавши sourse port (порт захвату пакетів) та destination port (порт, на який буде надсилатися перехоплений трафік) та з використанням програми сніферу Wireshark нам вдалося перехопити мережевий трафік та здійснити його аналіз. На рисунку 3.19 наведено знімок екрану програми Wireshark, на якому можна спостерігати трафік пакетів протоколу Telnet, що були надіслані від ПК через мережу Ethernet на віддалений роутер Cisco 2911 та були перехоплені L3 комутатором Catalist 3560 у проміжній точці мережі.

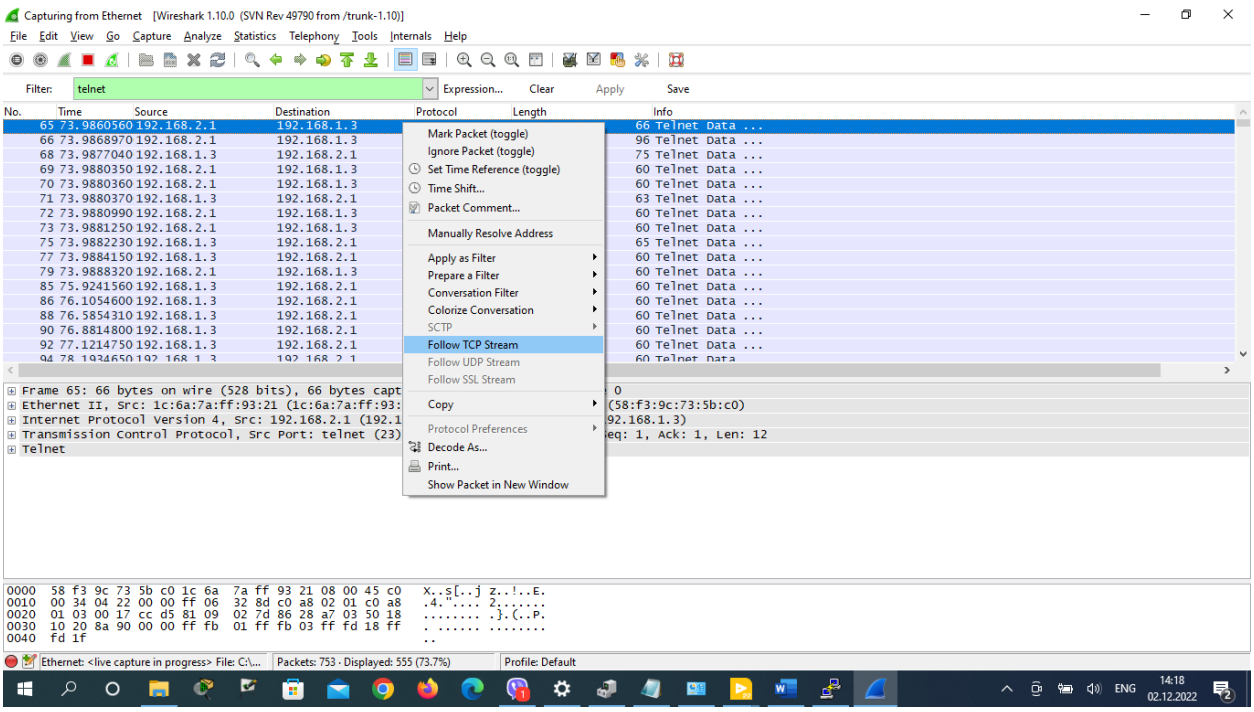


Рисунок 3.19 – Аналіз пакетів протоколу Telnet перехоплених комутатором

Провівши аналіз перехоплених пакетів протоколу Telnet, можна стверджувати про можливість застосування цього протоколу лише в межах безпечних відокремлених мереж, оскільки у протоколі Telnet всі дані надсилаються у відкритому вигляді (у тому числі паролі), що можна спостерігати на рисунку 3.20.

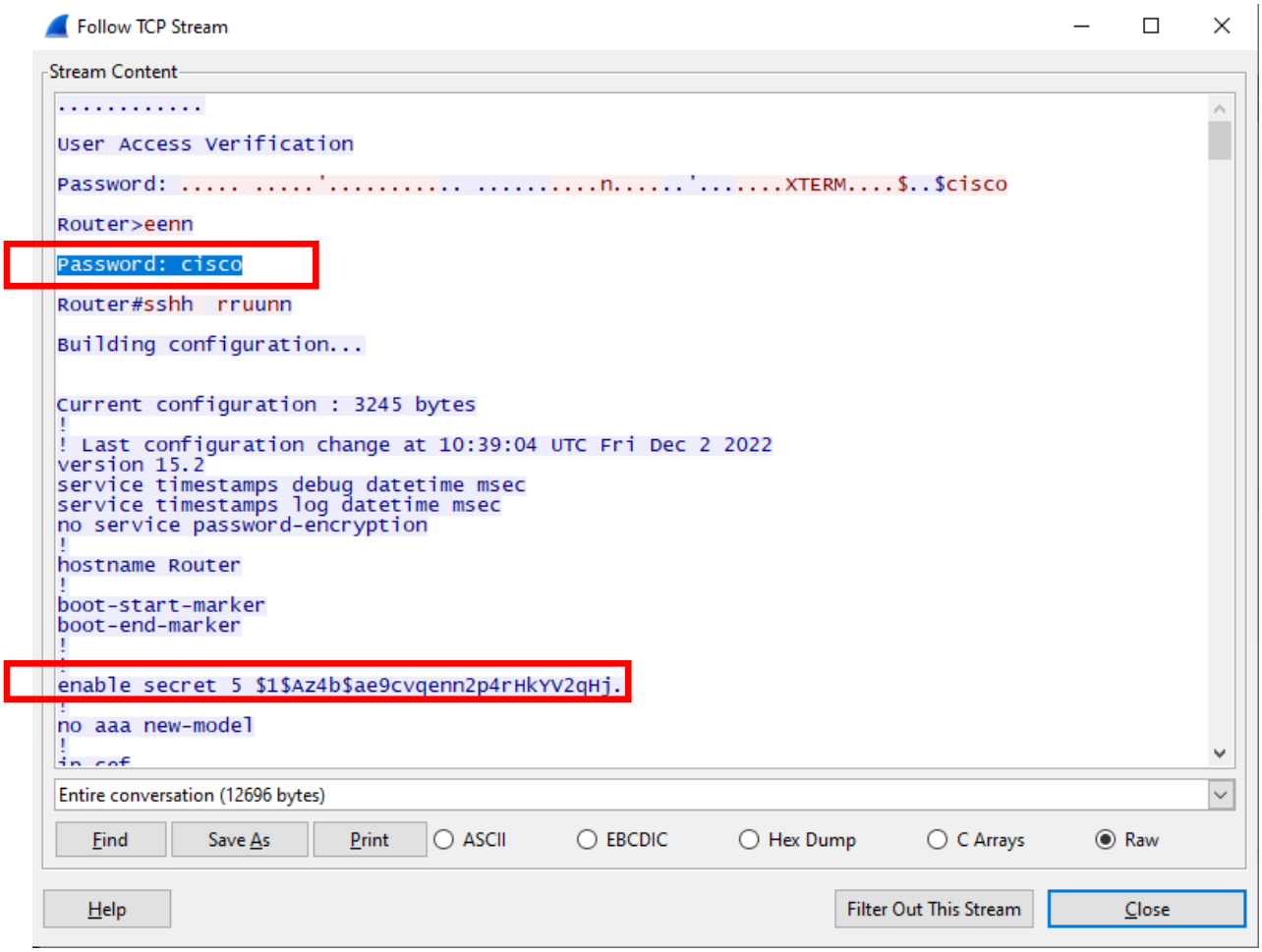


Рисунок 3.20 – Аналіз конфіденційних даних перехолених у мережі

Тож, для подальшого вдосконалення подібного програмного забезпечення, можна рекомендувати для віддаленого конфігурування пристроїв мережі задіяти захищений протокол SSH, що підвищить функціональні можливості та надасть змогу проводити подібні автоконфігурації віддалено через публічну мережу Internet, а не лише в рамках лабораторних досліджень у навчальній аудиторії чи ізольованому сегменті мережі. У рамках кваліфікаційної магістерської роботи аналогічні задачі з перехоплення трафіку були здійснені для протоколів ICMP, EIGRP та трафіку VoIP, що наведено на рисунках 3.21 та 3.22.

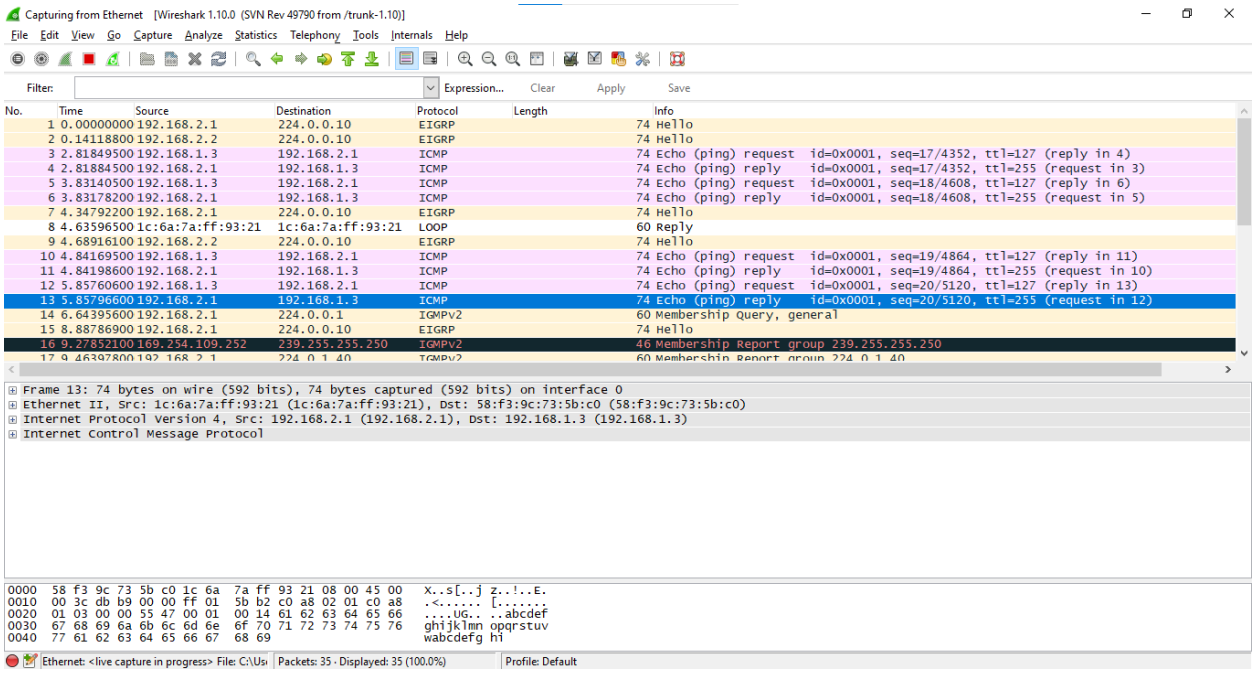


Рисунок 3.20 – Аналіз пакетів протоколів ICMP та EIGRP перехоплених комутатором

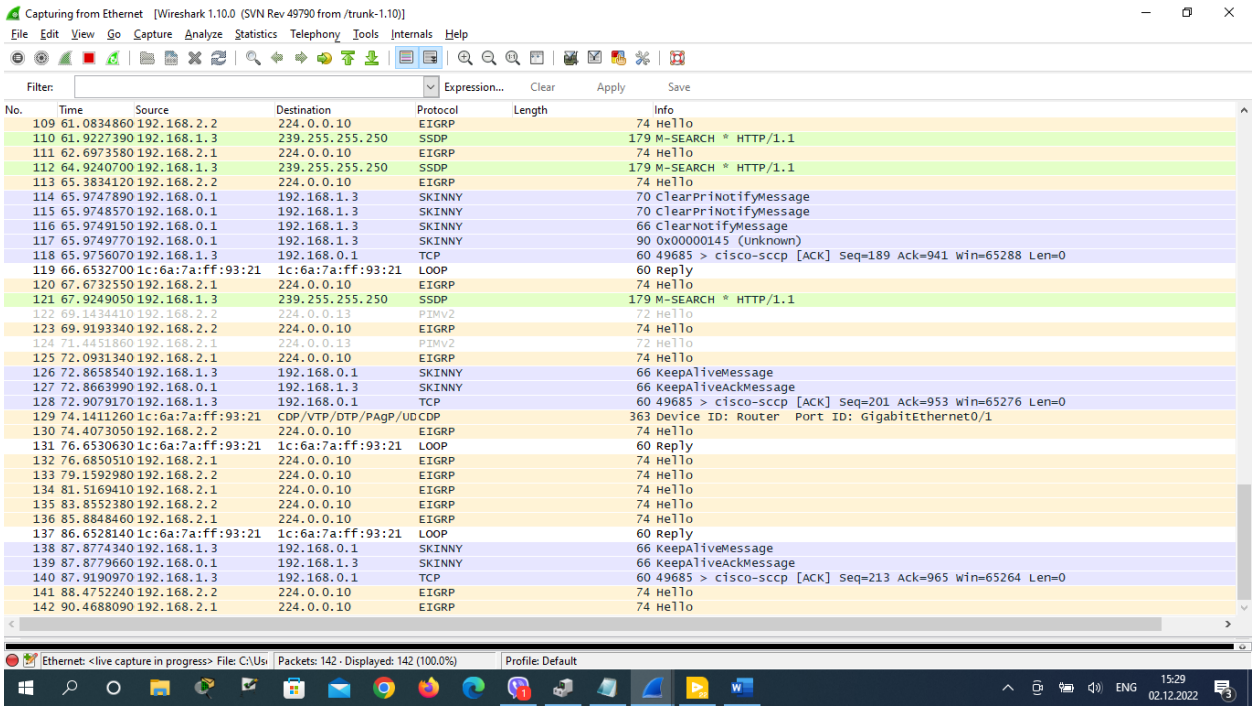


Рисунок 3.21 – Аналіз пакетів протоколу SKINNY під час сеансу IP-телефонії

Таким чином, під час виконання кваліфікаційної магістерської роботи було створено інформаційно-комунікаційну технологію проєктування мультисервісної мережі Ethernet з інтеграцією реального та віртуального обладнання Cisco, складовою частиною якої є програма для автоконфігурування мережевого обладнання. Дане програмне забезпечення зробило інтуїтивно зрозумілим та швидким процес конфігурування роутерів та комутаторів, а також налаштування на них підтримки сервісів IPTV та VoIP.

Дану програму можуть використовувати студенти під час виконання лабораторних робіт з дисциплін «Інформаційні та телекомунікаційні технології» та «Інтелектуальні функції апаратного забезпечення мереж Ethernet» як інструмент для конфігурування та перевірки працездатності роботи комп’ютерних мереж та мережевого обладнання. Окрім того, дана програма стане у нагоді досвідченим адміністраторам, які бажають здійснити автоматизацію операцій налаштування мережевого обладнання мультисервісних мереж, а також як конструктор для створення нових алгоритмів автоматизації при конфігуруванні мережевого обладнання. Закладені у програмі принципи є універсальними та підійдуть для автоматизації практично всіх конфігурацій сучасних комп’ютерних мереж.

ВИСНОВКИ

У кваліфікаційній магістерській роботі проведено аналіз предметної області за напрямом розробки інформаційно-комунікаційної технології проєктування мультисервісної мережі Ethernet. За результатами дослідження розроблено описову модель предметної області.

Використовуючи симулятор GNS3 та «живе» телекомунікаційне обладнання фірми Cisco, була побудована мультисервісна мережа Ethernet з підтримкою сервісів VoIP та IPTV.

З метою оптимізації налаштування подібних мереж створено інформаційно-комунікаційну технологію проєктування мультисервісної мережі Ethernet з інтеграцією реального та віртуального обладнання Cisco, складовою частиною якої є розроблена у середовищі графічного програмування LabVIEW програма, за допомогою якої можна здійснити автоконфігурування мережевого обладнання. Дане програмне забезпечення має значну практичну цінність, оскільки, завдяки інтуїтивно зрозумілим екранним формам, дає можливість значно комфортніше, надійніше та швидше здійснювати автоконфігурування основних компонентів сучасних комп’ютерних мереж з підтримкою сервісів IPTV та VoIP. Завдяки функціоналу автоконфігурування функції дзеркалізації портів на L3 комутаторах Catalist 3560 розроблена технологія дозволила відкрити перспективу наукових досліджень сучасних комп’ютерних мереж шляхом перехоплення мережевого трафіку та його детального аналізу.

СПИСОК ЛІТЕРАТУРИ

1. Організація комп’ютерних мереж: підручник: для студ. спеціальності 122 / Ю. А. Тарнавський, І. М. Кузьменко. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.
2. Карпенко М. Ю. Конспект лекцій з курсу «Комп’ютерні мережі» (для студентів усіх форм навчання спеціальностей 122 – Комп’ютерні науки, 151 – Автоматизація та комп’ютерно-інтегровані технології, 126 – Інформаційні системи та технології) / М. Ю. Карпенко, Н. В. Макогон; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2019. – 99 с.
3. Комп’ютерні мережі : курс лекцій / Ю. В. Волосюк. – Миколаїв: МНАУ, 2019. – 203 с.
4. Комп’ютерні мережі. Протоколи, технології, обладнання : навч. посіб. для студ. спец. 125 «Кібербезпека» / В. М. Базилевич, Д. Б. Мехед, Ю. М. Ткач. – Ніжин: ФОП Лук’яненко В.В. ТПК «Орхідея», 2018. – 108 с.
5. П784 Івашко В.В. Конспект лекцій з навчальної дисципліни «Програмне забезпечення інформаційно-вимірювальних систем». Чернівці : Чернівецький національний університет імені Юрія Федьковича, 2021. – 80 с.
6. Телекомунікаційні системи та мережі : навчальний посібник / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. – Тернопіль : ТНТУ ім. І.Пулюя, 2017.
7. Технологія VoIP. Навч. посібник, підготовлено для студентів вищих навчальних закладів / Сторчак К.П., Ткаленко О.М., Маркіна О.А. – Київ: ДУТ, 2018. – 120с.
8. Evaluating QoE in VoIP networks with QoS mapping and machine learning algorithms. ZhiGuo Hu,HongRen Yan,Tao Yan,HaiJun Geng,GuoQing Liu, Neurocomputing, Volume 386, 21 April 2020. - Pages 63-83.

9. On the deployment of VoIP in Ethernet networks: methodology and case study. KhaledSalah, Computer Communications, Volume 29, Issue 8, 15 May 2006. - Pages 1039-1054.

10. Що таке IPTV (телебачення через Інтернет) [Електронний ресурс] — Режим доступу до ресурсу: https://uk.myservername.com/10-best-free-video-converter-software-2021

11. Customer acceptance of IPTV service quality. Hyeong Yu Jang, Mi Jin Noh. International Journal of Information Management, Volume 31, Issue 6, December 2011. - Pages 582-592.

12. A Hybrid QoS-QoE Estimation System for IPTV Service. Jaroslav Frnda, Jan Nedoma, Jan Vanus, Radek Martinek. Electronics (Multidisciplinary Digital Publishing Institute), Vol. 8, Iss: 5, 27 May 2019. - pp 585.

13. Cisco Packet Tracer [Електронний ресурс] — Режим доступу до ресурсу: https://www.netacad.com/

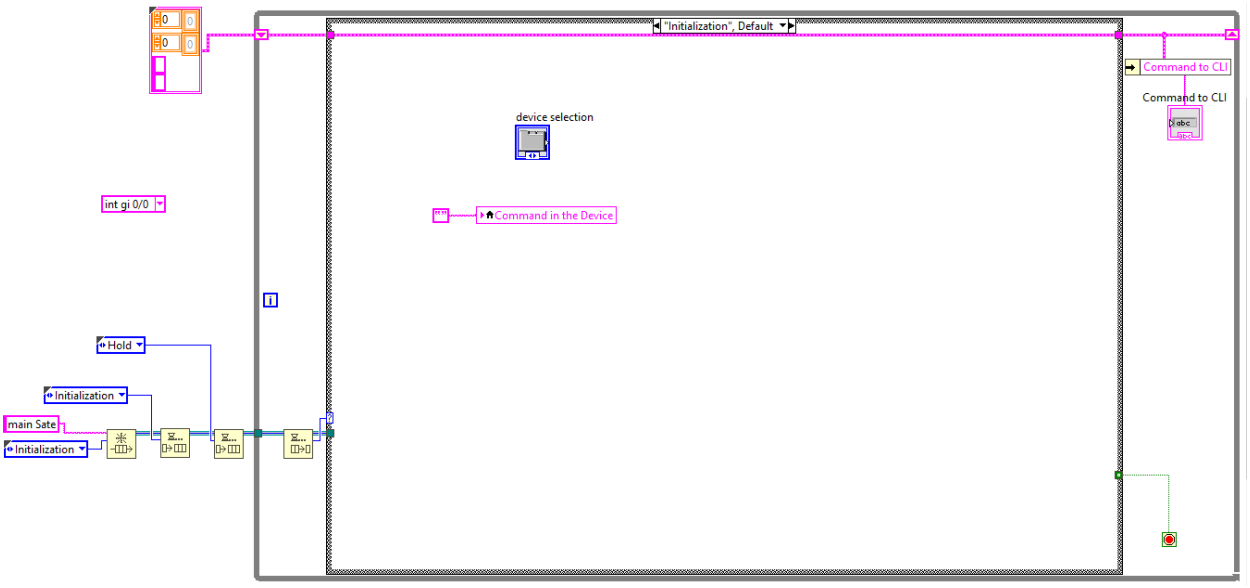
14. Getting Started with GNS3 [Електронний ресурс] — Режим доступу до ресурсу: https://docs.gns3.com/docs/

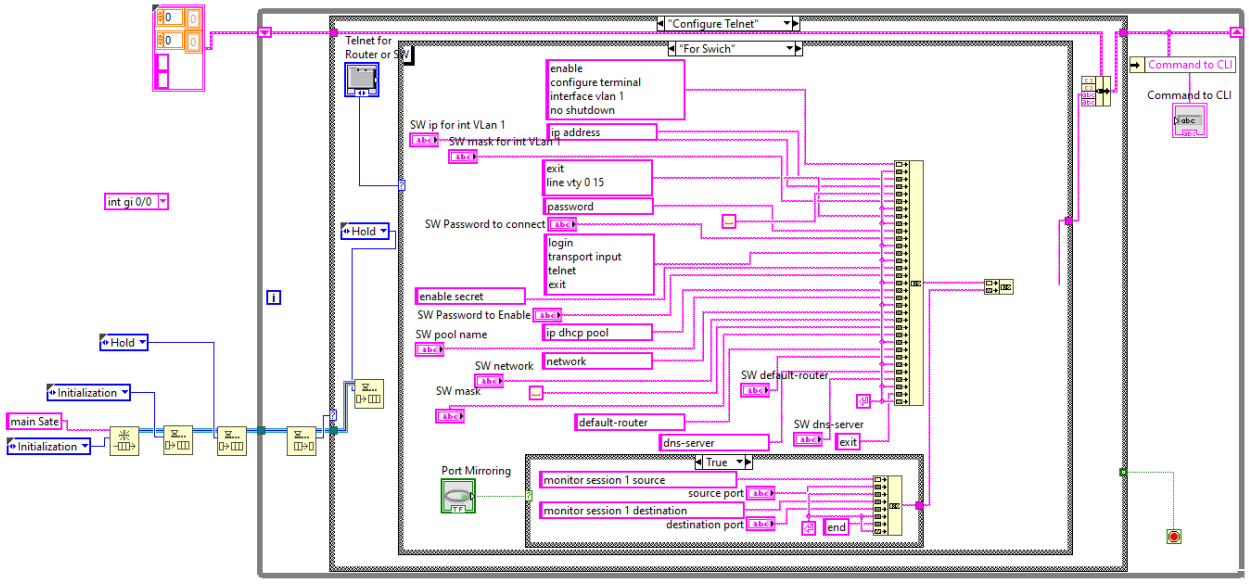
15. LabVIEW Graphical Programming, Fifth Edition 5th Edition, Richard Jennings, Fabiola De la Cueva, McGraw Hill, 2019. - 640 pages.

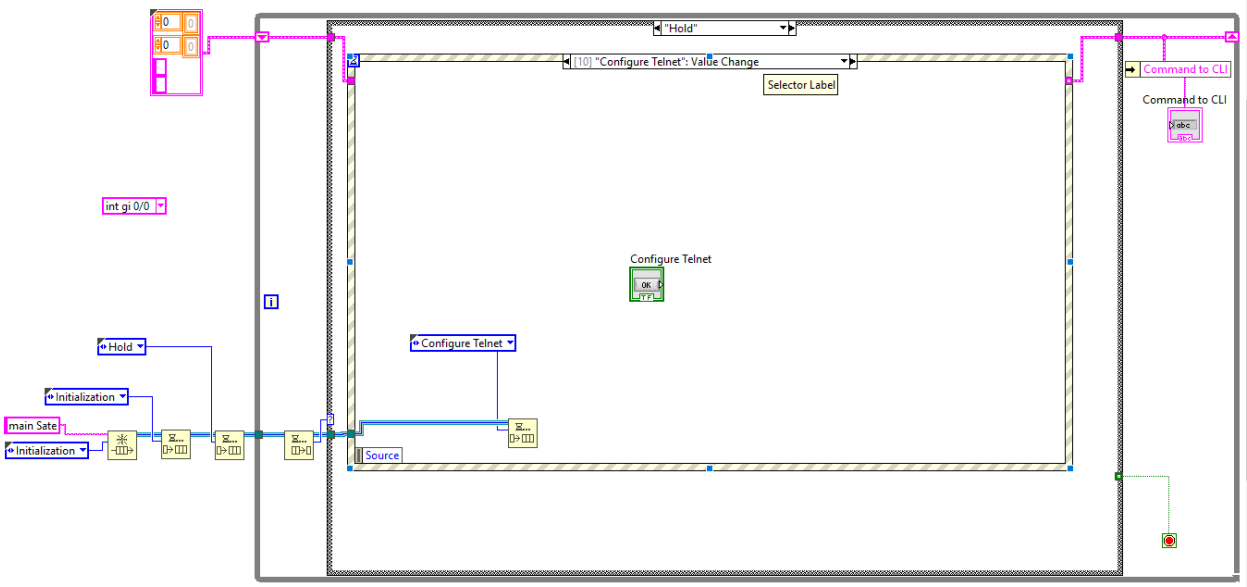
16. Hands-On Introduction to LabVIEW for Scientists and Engineers 4th Edition, John Essick, Oxford University Press, 2018. - 720 pages.

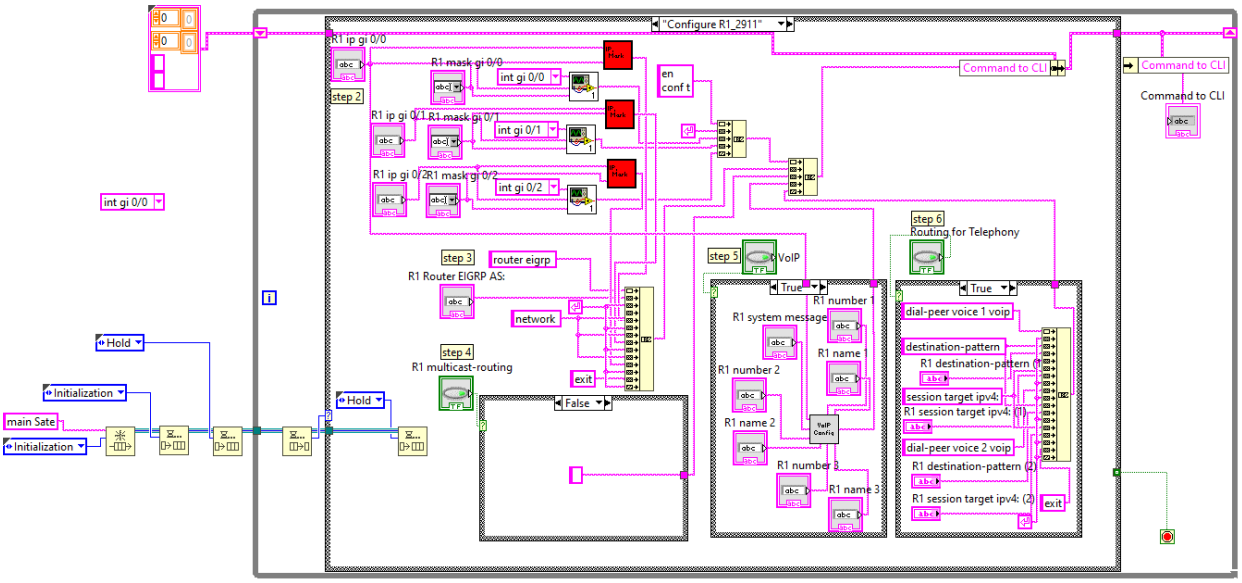
ДОДАТОК

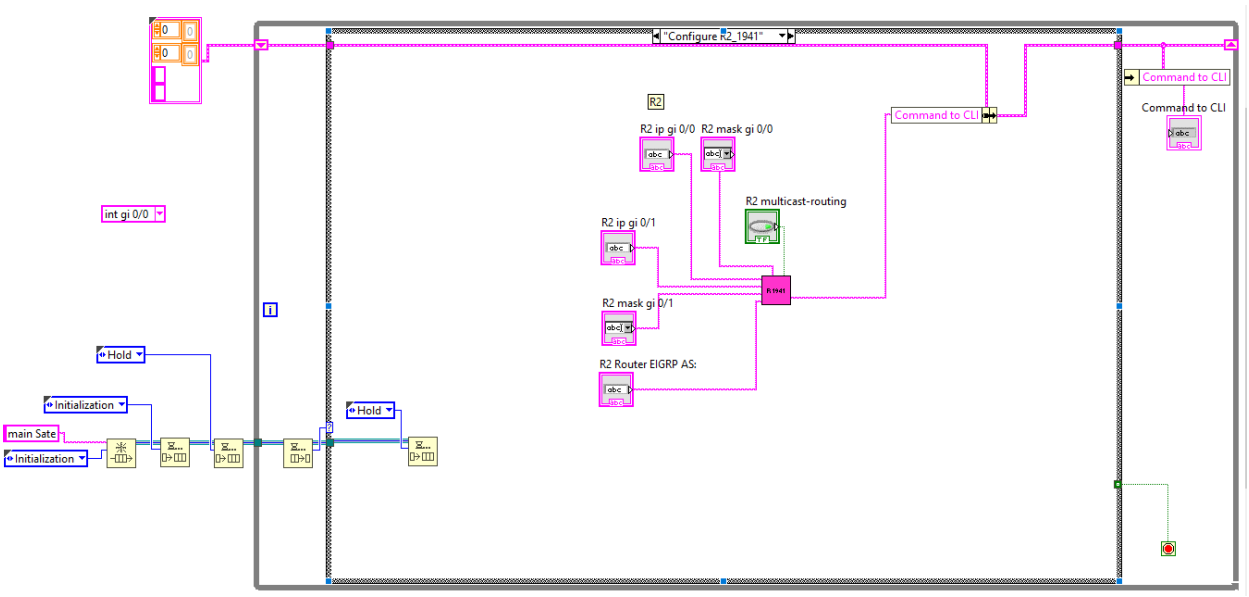
Розроблена у середовищі графічного програмування LabVIEW програма для автоконфігурування мережевого обладнання мультисервісної мережі Ethernet з підтримкою сервісів VoIP та IPTV.

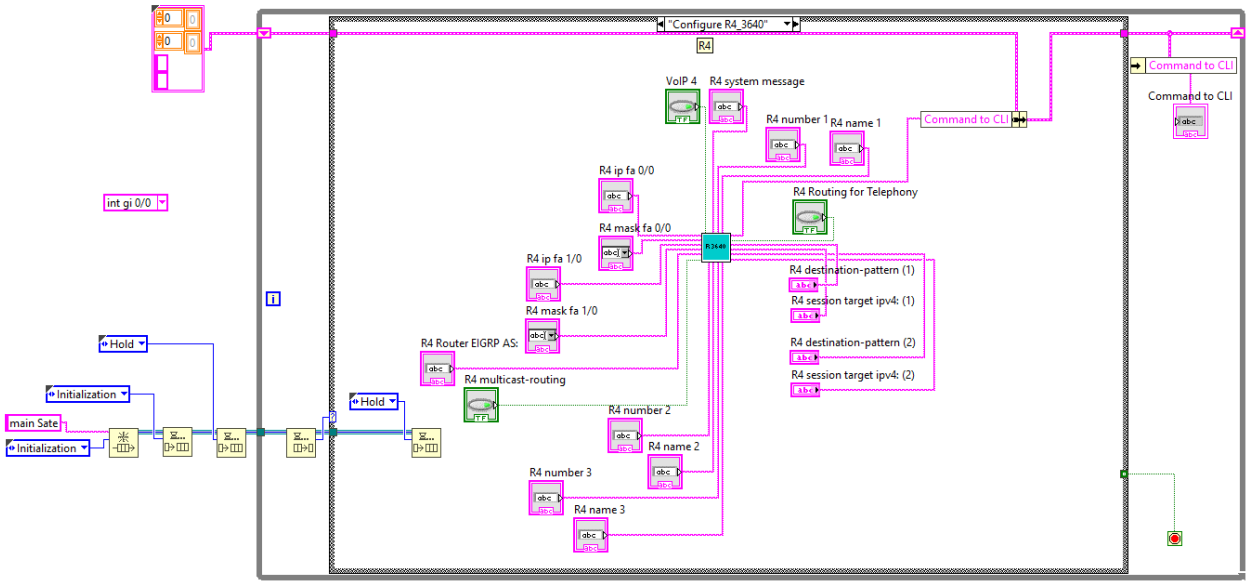


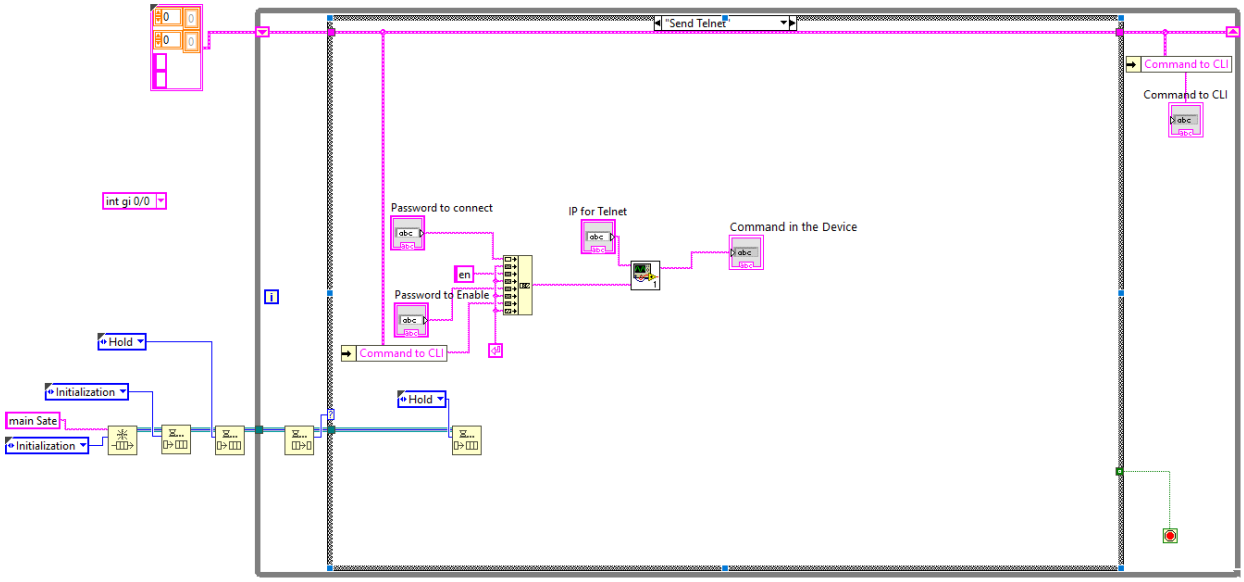


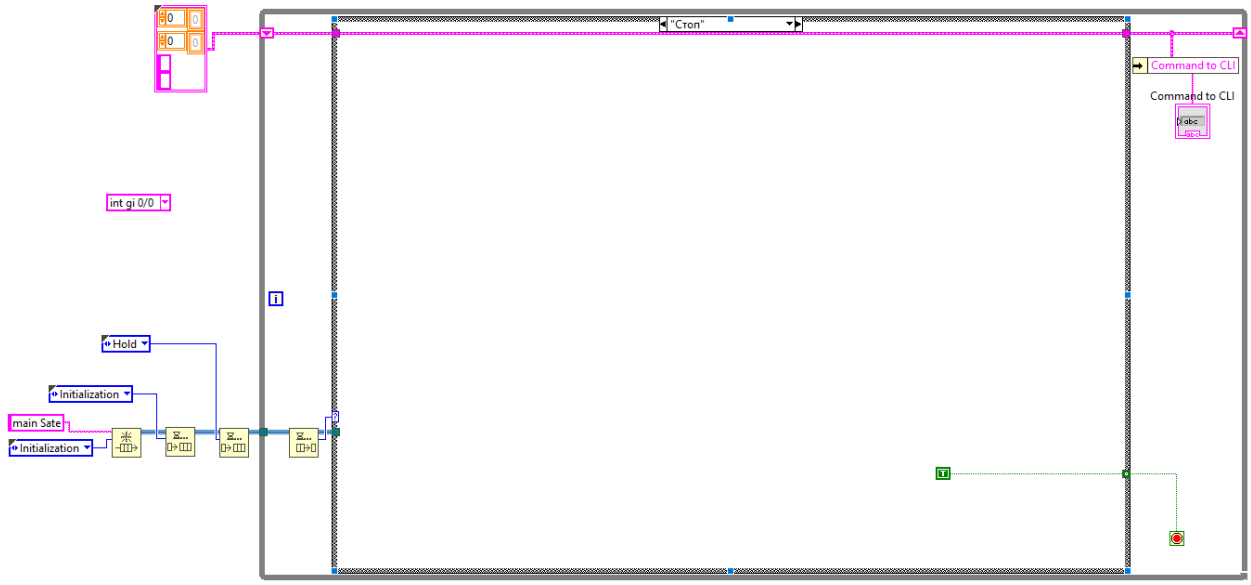

"Hold"
[10] "Configure Telnet": Value Change
Selector Label
Command to CLI
Command to CLI
int gi 0/0
Configure Telnet
Hold
Configure Telnet
Initialization
main Sate
Initialization
Source

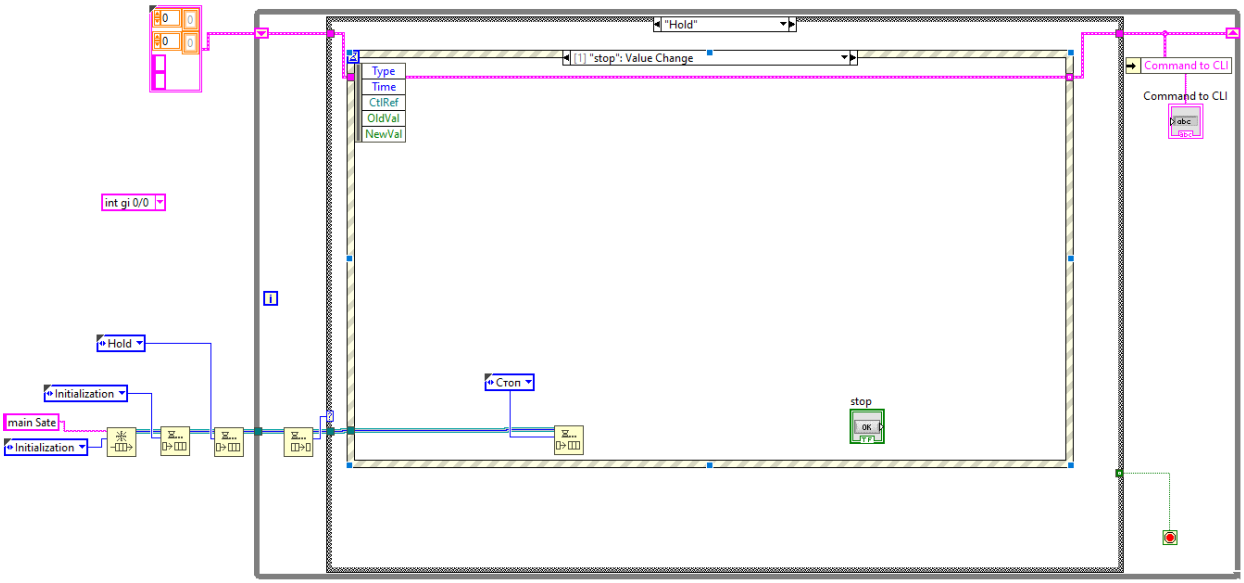

"Configure R1_2911"
R1 ip gi 0/0
R1 mask gi 0/0
int gi 0/0
step 2
en
conf t
R1 ip gi 0/1
R1 mask gi 0/1
int gi 0/1
R1 ip gi 0/2
R1 mask gi 0/2
int gi 0/2
Command to CLI
Command to CLI
Command to CLI
int gi 0/0
step 3
router eigrp
R1 Router EIGRP AS:
network
step 4
R1 multicast-routing
exit
step 5
VoIP
True
R1 number 1
R1 system message
R1 name 1
R1 number 2
R1 name 2
R1 number 3
R1 name 3
step 6
Routing for Telephony
True
dial-peer voice 1 voip
destination-pattern
R1 destination-pattern (1)
session target ipv4:
R1 session target ipv4: (1)
dial-peer voice 2 voip
R1 destination-pattern (2)
R1 session target ipv4: (2)
exit
Hold
False
Hold
Initialization
main Sate
Initialization

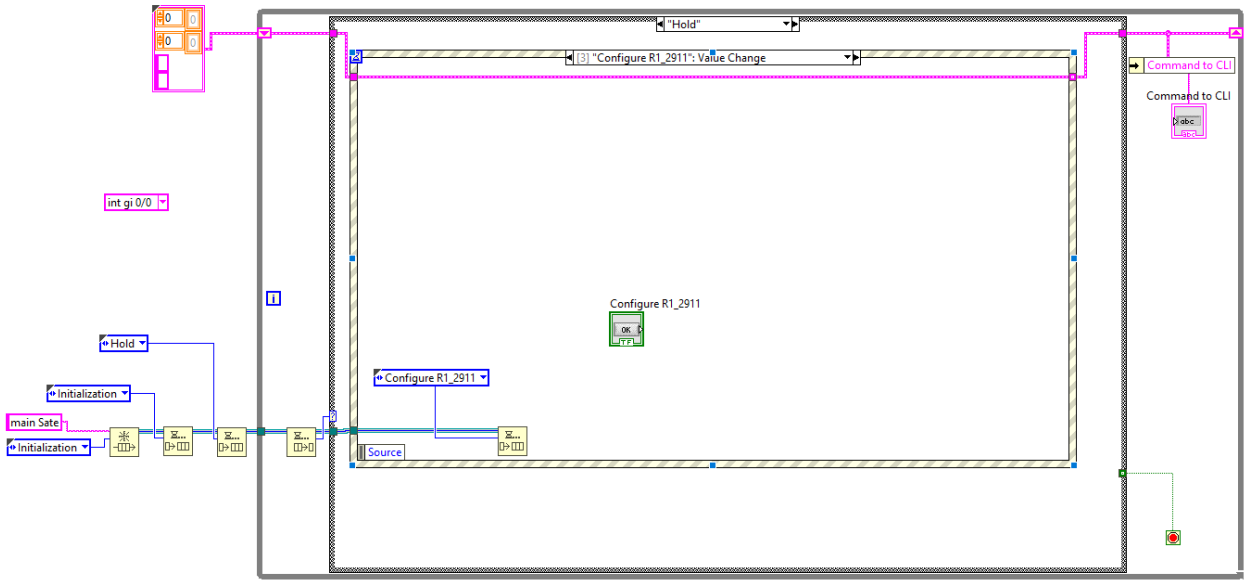

"Configure R2_1941"
R2
Command to CLI
Command to CLI
Command to CLI
R2 ip gi 0/0
R2 mask gi 0/0
R2 multicast-routing
R2 ip gi 0/1
R2 mask gi 0/1
R2 Router EIGRP AS:
int gi 0/0
Hold
Initialization
main Sate
Initialization
Hold

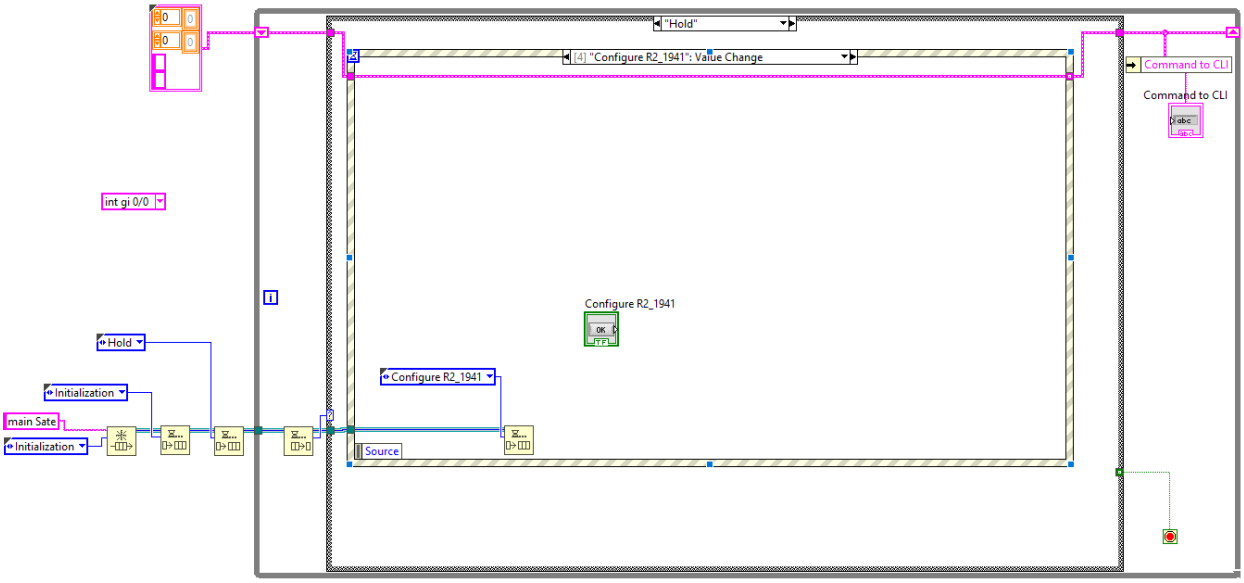

"Configure R4_3640"
R4
Command to CLI
Command to CLI
Command to CLI
VoIP 4
R4 system message
R4 number 1
R4 name 1
R4 Routing for Telephony
R4 ip fa 0/0
R4 mask fa 0/0
R4 ip fa 1/0
R4 mask fa 1/0
R4 Router EIGRP AS:
R4 multicast-routing
R4 destination-pattern (1)
R4 session target ipv4: (1)
R4 destination-pattern (2)
R4 session target ipv4: (2)
R4 number 2
R4 name 2
R4 number 3
R4 name 3
int gi 0/0
Hold
Initialization
main Sate
Initialization
Hold

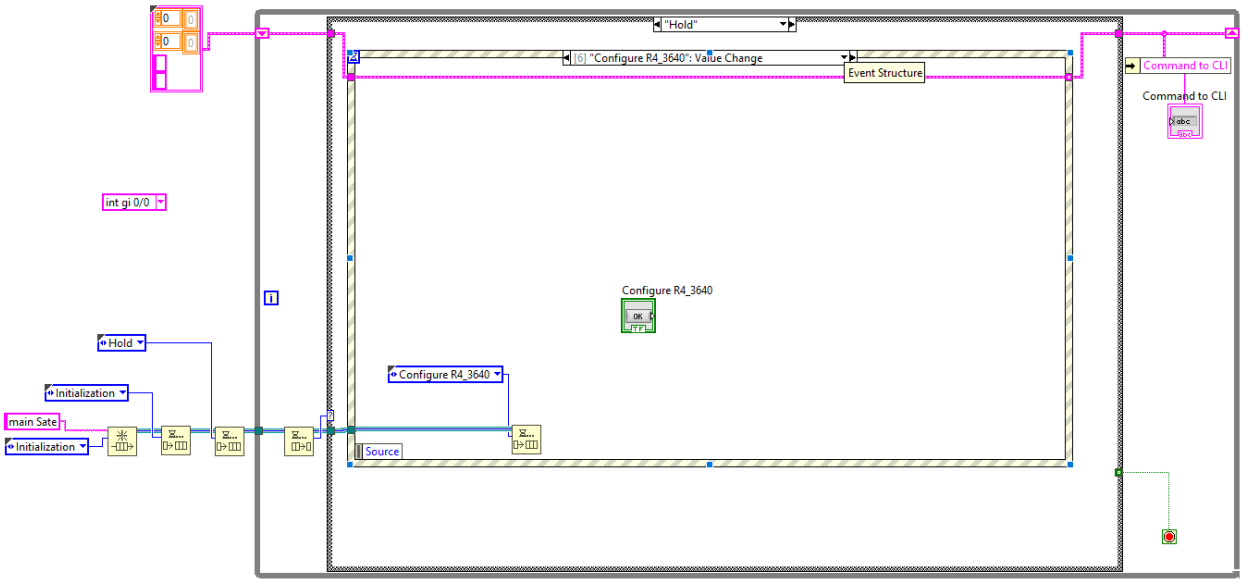

"Send Telnet"
Command to CLI
Command to CLI
int gi 0/0
Password to connect
IP for Telnet
Command in the Device
en
Password to Enable
Command to CLI
Hold
Initialization
main Sate
Initialization
Hold


"Cron"
Command to CLI
Command to CLI
int gi 0/0
Hold
Initialization
main Sate
Initialization

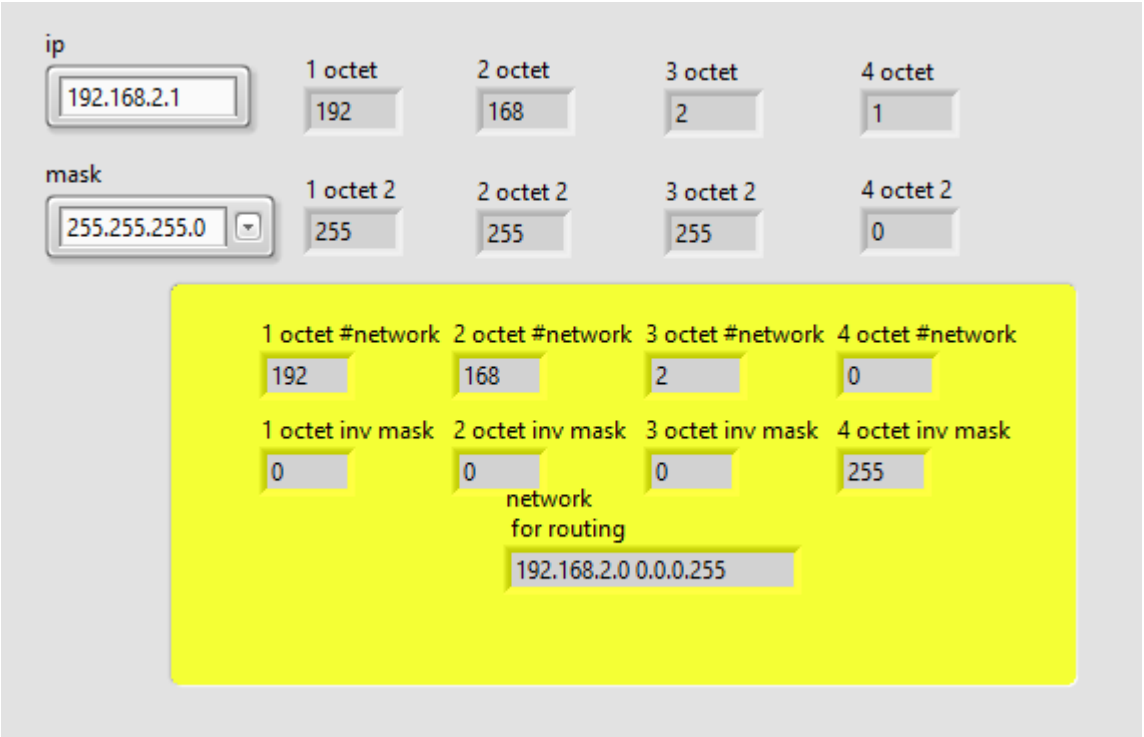

"Hold"
[1] "stop": Value Change
Type
Time
CtlRef
OldVal
NewVal
Command to CLI
Command to CLI
int gi 0/0
Hold
Initialization
main Sate
Initialization
Cron
stop

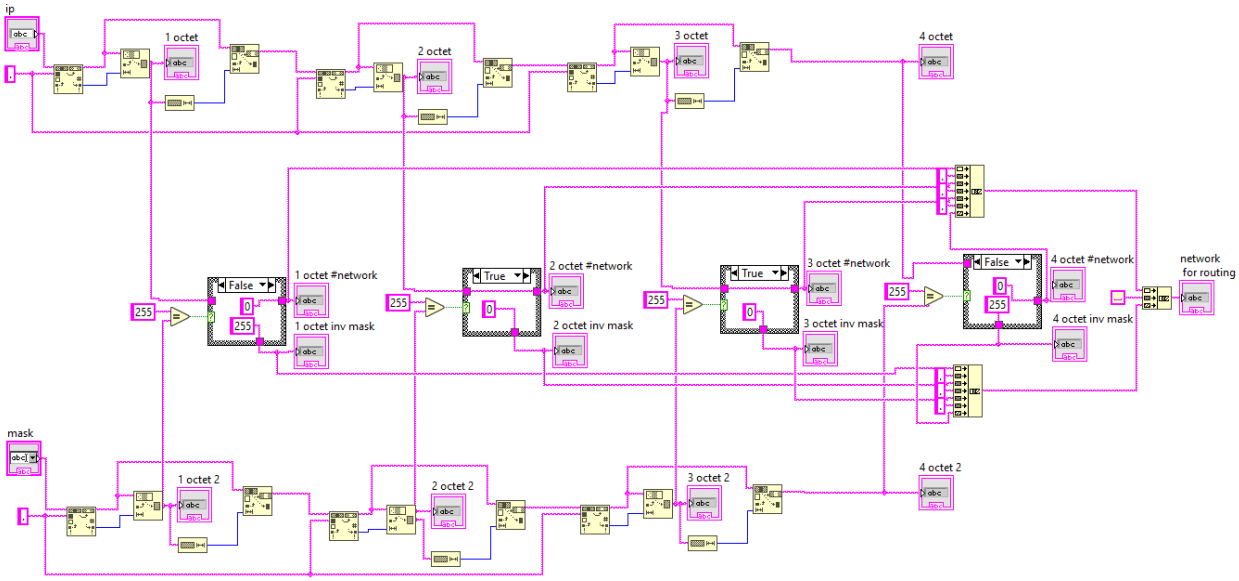

"Hold"
[3] "Configure R1_2911": Value Change
Command to CLI
Command to CLI
int gi 0/0
Configure R1_2911
Hold
Initialization
main Sate
Initialization
Configure R1_2911
Source


"Hold"
[4] "Configure R2_1941": Value Change
Command to CLI
Command to CLI
int gi 0/0
Configure R2_1941
Hold
Initialization
main Sate
Initialization
Configure R2_1941
Source


"Hold"
[6] "Configure R4_3640": Value Change
Event Structure
Command to CLI
Command to CLI
int gi 0/0
Configure R4_3640
Hold
Initialization
main Sate
Initialization
Configure R4_3640
Source

Підпрограма перетворення IP-адрес інтерфейсу роутера у формат номеру мережі.





Підпрограма автоконфігурації роутерів.