МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни
"**Технології проектування телекомунікаційних мереж**"
для магістрів спеціальності 123 "Комп'ютерна інженерія", освітні програми «Комп'ютерні системи та мережі» та «Спеціалізовані комп'ютерні системи», усіх форм навчання.
Graphical Network Simulator-3

2020

Методичні вказівки до виконання лабораторних робіт з дисципліни "Технології проектування телекомунікаційних мереж" для магістрів спеціальності 123 "Комп'ютерна інженерія", освітні програми «Комп'ютерні системи та мережі» та «Спеціалізовані комп'ютерні системи», усіх форм навчання. Graphical Network Simulator-3 / Укл. Г.Г.Киричек, С.Ю.Скрупський. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 38 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.
С.Ю. Скрупський, доцент, к.т.н.

Рецензент: М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 2 від 04.09.2020

Рекомендовано до видання
НМК КНТ
Протокол № 2/1 від 15.09.2020

ЗМІСТ

1 ЛАБОРАТОРНА РОБОТА.
Graphical Network Simulator-3

Мета роботи: ознайомитися з основними можливостями програми емулятора GNS3 при проектуванні та моделюванні комп'ютерних мереж.

1.1 Теоретичні відомості

GNS3 – графічний емулятор, який дозволяє моделювати складні мережі. Для забезпечення повної емуляції, gns3 тісно пов'язаний з наступними компонентами:

- Dynamips – ядро програми, що дозволяє емулювати CiscoIOS;
- Dynagen – текстовий інтерфейс для Dynamips;
- PEM емулятор брандмауера CiscoPIX на основі Qemu.

GNS3 є відмінним додатковим інструментом для реалізації лабораторних робіт Cisco для мережевих інженерів, адміністраторів і людей, які бажають пройти сертифікацію CCNA, CCNP, CCIP і CCIE. Він також може бути використаний для експериментів над Cisco IOS або для перевірки налаштувань, які треба розгорнути на реальних маршрутизаторах. GNS3 є проектом з відкритим вихідним кодом, безкоштовна програма, яку можна використовувати на багатьох операційних системах, включаючи Linux, MacOS і Windows.

Емулятор дозволяє створити модель комп'ютера або іншого пристрою і запускати всередині оригінальне програмне забезпечення. Емулюються всі основні компоненти пристрою, в тому числі процесор, пам'ять і пристрої вводу/виводу.

У випадку з Cisco, емулятор створює модель маршрутизатора і запускає всередині реальну операційну систему Cisco IOS. Таким чином ми отримуємо повнофункціональний маршрутизатор. Тобто запустивши маршрутизатор Cisco, ми отримаємо у доступі практично всі функції, які працюють на реальному маршрутизаторі (у Cisco Packet Tracer значна частина функціоналу недоступна, тому що це лише симулятор).

Також у GNS3 можна додати повноцінний комп'ютер з Windows або Ubuntu. При цьому Windows Server або RedHat можна використовувати в схемі за допомогою технологій віртуалізації

(VirtualBox або VMWare) або підключивши GNS3 до реальної мережі. Таким чином можна перевірити встановлений VPN, аутентифікацію користувачів через сервер та використовувати справжній браузер при підключенні до Інтернету.

Недоліком даного програмного забезпечення є відсутність можливості повноцінної симуляції комутаторів Cisco другого рівня. У такому для виконання лабораторних робіт з використанням комутаторів другого рівня застосовують вже відомий вам симулятор Cisco Packet Tracer.

До складу GNS3 не входять образи Ios/ips/pix/asa/junos, оскільки вони є частиною комерційних продуктів відповідних компаній та не мають жодного прямого відношення до проекту GNS3. На даний момент це вже не є проблемою, оскільки знайти необхідний образ вже не складає труднощів.

Ще один важливий недолік - дуже високі вимоги до системних ресурсів. Однак це не проблема GNS3, а проблема пристроїв, що запускаються в ньому та потребують дуже багато ресурсів. GNS3 на відміну від Cisco Packet Tracer працює з реальними прошивками пристроїв. Наприклад, для запуску Cisco ASA потрібен 1Гб оперативної пам'яті. А якщо ви хочете зібрати кластер? А якщо в схемі присутній Cisco IPS, якому потрібен ще 1Гб? А якщо в топологію необхідно додати ще пару серверів?

Тому на сьогоднішній день, мінімальні системні вимоги для GNS3 це 4Гб оперативної пам'яті. Але краще мати 8Гб, якщо ви плануєте збирати схеми корпоративних мереж.

Не зважаючи на недоліки, однією з найцікавіших особливостей GNS3 є можливість з'єднання топології мережі, що проектується з реальною мережею. Це надає унікальну можливість перевірити на практиці будь-який проект, без використання реального устаткування. Використання Wireshark дозволяє провести моніторинг трафіку усередині топології мережі, що проектується. Це дає додаткову інформацію для розуміння технологій, які вивчаються у даному курсі.

1.2 Установка емулятора GNS3

Для встановлення програми емулятора GNS3 треба отримати його дистрибутив. Це можна зробити двома способами: або скористатися тим, що є на комп’ютері в аудиторії, або загрузити з

офіціального сайту gns3.com (при цьому згідно з політикою сайту вам треба буде зареєструватися). У зв'язку з тим, що версії постійно оновлюються, в етапах установки наводиться тільки абревіатура GNS3 без надання версії програмного продукту.

Далі виконаємо наступні дії:

– запускаємо программу-встановлювач – GNS3 – win32-all-in-one.exe;

– у вікні GNS3 Setup Welcome to the GNS3 Setup Wizard натискаємо на кнопку "Next";

– у вікні GNS3 Setup License Agreement читаємо ліцензійну угоду та погоджуємося з нею. Далі натискаємо на кнопку "I Agree";

– у вікні GNS3 Setup Choose Start Menu Folder натискаємо на кнопку "Next";

– у вікні GNS3 Setup Choose Components залишаємо все за замовчуванням та натискаємо на кнопку "Next";

– у вікні GNS3 Setup Choose Install Location залишаємо за замовчуванням та натискаємо на кнопку "Install";

– у вікні WinPcap 4.1.x Setup WinPcap 4.1.x Installer натискаємо на кнопку "Next";

– у вікні WinPcap 4.1.x Setup Welcome to the WinPcap 4.1.x Setup Wizard натискаємо на кнопку "Next";

– у вікні WinPcap 4.1.x Setup License Agreement читаємо ліцензійну угоду та натискаємо на кнопку "I Agree";

– у вікні WinPcap 4.1.x Setup Installation options залишаємо відміченим Automatically start the WinPcap driver at boot time та натискаємо на кнопку "Install";

– у вікні WinPcap 4.1.x Setup Completing the Win Pcap 4.1.x Setup Wizard натискаємо на кнопку "Finish";

– у вікні Setup – GNS3 Virtual Box Edition Completing the GNS3 Virtual Box Edition Setup Wizard натискаємо на кнопку "Finish";

– перезавантажуємо комп'ютер.

1.3 Конфігурувння емулятора GNS3

Після перезавантаження комп'ютера, виконаємо конфігурування встановленого програмного продукту GNS3.

Для цього необхідні наступні дії:

– при першому запуску GNS3 з'явився setup wizard. Він складається з двох кроків (рис. 1.1);

– тиснемо "Step 1";

– далі заходимо на "General";

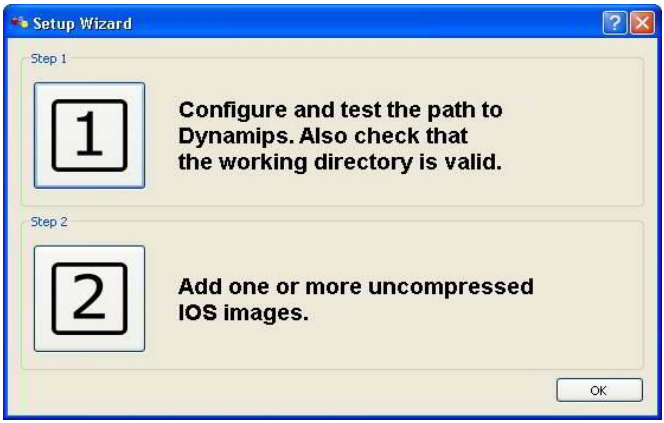

Рисунок 1.1 – GNS3 setup wizard

– на вкладці Terminal Settings зі списку Preconfigurated terminal commands обираємо Putty (Windows, included with GNS3) та натискаємо кнопку "Use";

– натискаємо кнопку "Apply";

– далі заходимо на "Dynamips";

– на вкладці Dynamips в Executable path вказуємо шлях до виконавчого файлу dynamips-wxp.exe (знаходиться по тому шляху куди встановлена програма);

– вказуємо шлях до робочої директорії;

– натиснемо кнопку "Test", якщо видало: "Dynamips successfully started", то все зроблено правильно, якщо ні, то перевіряємо налаштування;

– натиснемо кнопку "Apply";

– переходимо до "Capture";

– обираємо робочу директорію для capture files;

– натиснемо "Apply";

– переходимо на "Qemu";

– обираємо шлях до виконавчих файлів qemuwrapper.exe, qemu, qemu-img та до робочої теки;

– натиснемо "Test";

– якщо видало позитивне повідомлення, то налаштування вірні і тиснемо "Apply";

– повертаємось до SetupWizards і обираємо "Step 2";

– на вкладці IOS Images в полі Image file обираємо образ необхідного пристрою (образ ми копіюємо в теку з образами, яку вибирали в Step 1);

– натиснемо Save.

1.4 Створення найпростішої технології в GNS3

На наступному етапі створемо найпростійшу технологію в GNS3 з використанням маршрутизатору.

Для цього виконаємо такі дії:

– перетягнемо Router c7200 з Nodes Types на головне поле;

– натиснемо праву клавішу миші на вибраному маршрутизаторі і виберемо зі списку команду Start;

– тепер знову натиснемо праву клавішу миші на маршрутизаторі та виберемо команду Console;

– щоб зменшити навантаження на процесор треба присвоїти йому значення "Idle PC";

– не виходячи з консолі тиснемо праву клавішу миші на маршрутизаторі та вибираємо команду "Idle PC";

– зі списку вибираємо значення "Idle PC" з позначкою *;

– повертаємося до консолі, набираємо: "enable", потім "configurate terminal", або "config t";

– далі можна робити різні маніпуляції, які дозволяють налаштування (змінювати хост-ім’я пристрою, IPадресу та інші);

– натиснемо праву кнопку миші на маршрутизаторі та виберемо команду "Stop", після цього консоль зникне.

1.5 Рекомендації по запуску GNS3 на ПК з малим об’ємом ОП

У даному розділі надаються рекомендації щодо запуску та роботи GNS3 на комп’ютерах з малим об’ємом оперативної пам’яті.

Загальні налаштування GNS3 та поради:

– "Edit" > "Preferences" > "Dynamips" > "Hypervisor Manager", зняти пташку з пункту "Allocate a new hypervisor per IOS image" та встановити "Memory usage limit per hypervisor" 128 MB;

– перед початком і у процесі роботи не відкривати жодних сторонніх програм та не поспішати виконувати дії у GNS3, бо через малий об’єм ОЗП програма буде працювати повільно.

Налаштування образів роутерів для віртуальної машини виконати з урахуванням того, що у лабораторних роботах GNS3 використовуються два образи роутерів, а саме c7200-adventerprisek9_sna-mz.150-1.M.bin та c3640-jk9s-mz.124-16.bin.

Для c7200-adventerprisek9_sna-mz.150-1.M.bin:

– "Edit" > "IOS images and hypervisors" > "Default RAM" > " 512 MB;

– виконати підбор значення "IDLE PC" із * згідно методичних вказівок.

Для c3640-jk9s-mz.124-16.bin:

– "Edit" > "IOS images and hypervisors" > "Default RAM" > " 128 MB;

– виконати підбор значення "IDLE PC" із * згідно методичних вказівок.

Якщо не вдається запустити образи чи не працює симуляція (за умови, що вона правильна), спробуйте збільшити об’єм оперативної пам’яті, виділений під роутери та гипервізор.

Примітка. Наголошуємо, що коректна робота GNS3 на конфігурації, що не відповідає мінімальним системним вимогам (табл.1.1) не гарантується, и будь-яка створена симуляція може працювати не коректно не зважаючи на її правильність.

Таблиця 1.1 – Системні вимоги до GNS3

Предмет	**Вимоги**
Операційна система	Windows 7 (64 bit) або новіша
Процесор	2 або більше логічних ядер
Віртуалізація	Підтримка AMD-V чи INTEL VT-X
Пам'ять	4 Гб ОЗП
Сховище	1 Гб вільного місця

1.6 Зміст звіту

– хід роботи;
– результати отримані в процесі виконання загальних етапів;
– переваги та недоліки емулятора GNS3 в порівнянні із симулятором Cisco Packet Tracer.
– короткий опис усіх команд контекстного меню маршрутизатору.

1.7 Контрольні питання

1. Для чого використовується GNS3?
2. Призначення Dynamips?
3. Для чого використовуються образи IOS?
4. Опишіть процес налаштування простої мережі в GNS3.

2 ЛАБОРАТОРНА РОБОТА.
VoIP на базі Graphical Network Simulator-3

Мета роботи: ознайомитися з технологією VoIP та навчитися її емулювати в програмному забезпеченні GNS3.

2.1 Теоретичні відомості

VoIP (voice over IP) – технологія передачі медіа даних в реальному часі за допомогою сімейства протоколів TCP/IP. IP-телефонія – система зв'язку, в якій аналоговий звуковий сигнал від одного абонента дискретизується (кодується в цифровий вигляд),

стискається і пересилається по цифрових каналах зв'язку до іншого абонента, де проводиться зворотна операція – декомпресія, декодування і відтворення аналогового сигналу.

Основу технології VoIP складають протокол RTP (real time protocol), побудований поверх протоколів UDP/IP, а також протоколи кодування медіа даних. Існують розширення (профілі) протоколу RTP, такі як SRTP (secure RTP) та інші.

Протоколи забезпечують реєстрацію IP пристрою (шлюз, термінал або IP-телефон) на сервері або гейткіпері провайдера, виклик і/або переадресацію виклику, встановлення голосового з'єднання, передачу імені і/або номера абоненту.

В даний час широкого поширення набули наступні протоколи VoIP:

– SIP – забезпечує передачу голосу (для сигналізації зазвичай використовує порт 5060 UDP);
– H.323 – протокол, більш прив'язаний до систем традиційної телефонії, чим SIP (сигналізація по порту 1720 TCP);
– IAX2 – сигналізація і медіа використовують порт 4569 UDP;
– MGCP;
– SIGTRAN;
– SCTP;
– SGCP;
– Skinny/SCCP;
– Unistim – закритий протокол передачі сигнального трафіку в продуктах компанії Nortel.

Джерелом інформаційних даних є мовний сигнал, можливою моделлю якого є нестаціонарний випадковий процес. У першому наближенні можна виділити такі типи сигнальних фрагментів: вокалізування, невокалізування, перехідні і паузи. При передачі мови в цифровій формі кожен тип сигналу при одній і тій же тривалості і однаковій якості вимагає різного числа біт для кодування і передачі.

Отже, швидкість передачі різних типів сигналу також може бути різною, що обумовлює застосування кодеків із змінною швидкістю. В результаті передача мовних даних в кожному напрямі дуплексного каналу розглядається як передача асинхронних логічно самостійних фрагментів цифрових послідовностей (транзакцій) з датаграмною синхронізацією усередині транзакції, наповненої блоками різної довжини.

У основі кодека мови зі змінною швидкістю лежить класифікатор вхідного сигналу, що визначає ступінь його інформативності і, таким чином, задає метод кодування і швидкість передачі мовних даних. Найбільш простим класифікатором мовного сигналу є VAD (Voice Activity Detector, детектор мовної активності), який виділяє у вхідному мовному сигналі активну мову і паузи. Фрагменти сигналу, що класифікуються як активна мова, кодуються якимось з відомих алгоритмів (як правило, на базі методу Code Excited Linear Prediction – CELP) з базовою швидкістю 4 – 8 Кбіт/с. Фрагменти, класифіковані як паузи, кодуються і передаються з низькою швидкістю 0.1 – 0.2 Кбіт/с, або не передаються взагалі.

Коли спрацьовує VAD, на приймальній стороні може автоматично генеруватися так званий "комфортний шум" щоб у співбесідника не виникало відчуття пропажі зв'язку. При цьому передачі мінімальної інформації про фрагменти пауз надається перевага. Дана стратегія дозволяє оптимізувати швидкість кодування 2 – 4 Кбіт/с при достатній якості мови, що синтезується. Для особливо критичних фрагментів мовного сигналу виділяється велика швидкість передачі, для менш відповідальних – менша.

Вокодер вносить додаткову затримку 15 – 45 мс, яка виникає з наступних причин:

– використання буфера для накопичення сигналу і обліку статистики подальших відліків (алгоритмічна затримка);

– математичні перетворення, що виконуються над мовним сигналом, вимагають процесорного часу (обчислювальна затримка).

Проведений в різних дослідницьких групах аналіз якості передачі мовних даних через мережу Інтернет показує, що основним джерелом виникнення спотворень, зниження якості і розбірливості синтезованої мови є переривання потоку мовних даних, викликане втратами пакетів при передачі по мережі зв'язку та перевищенням допустимого часу доставки пакету з мовними даними.

Це вимагає рішення задачі оптимізації затримок в мережі і створення алгоритмів компресії мови, стійких до втрат пакетів (відновлення втрачених пакетів).

З урахуванням можливих втрат пакетів в мережі для відновлення мовного потоку на приймальній стороні використовується протокол реального часу – Real Time Protocol (RTP). У заголовку даного протоколу, зокрема, передаються тимчасова мітка і номер пакету. Ці

параметри дозволяють при мінімальних затримках визначити порядок і момент декодування кожного пакету, а також інтерполювати втрачені пакети. Відновлена послідовність, з можливими пропусками як одиночних пакетів, так і груп пакетів, поступає на декодер. Декодер має забезпечити відновлення мовної інформації, заповнення пауз фоновим шумом, а також ехо-компенсацію кодованого сигналу, виявлення і детектування телефонної сигналізації.

Основними перевагами технології VoIP є скорочення необхідної смуги пропускання, що забезпечується обліком статистичних характеристик мовного трафіку:

– блокуванням передачі пауз (діалогових, складових, смислових і ін.), які можуть складати до 40–50 % часу зайнятості каналу передачі;

– високою надмірністю мовного сигналу і його стисненням (без втрати якості при відновленні) до рівня 20–40 % початкового сигналу.

З іншого боку, трафік VoIP критичний до затримок пакетів в мережі, але толерантний (стійкий) щодо втрат окремих пакетів. Так втрата до 5 % пакетів не призводить до погіршення розбірливості мови.

2.2 Установка Cisco IP Communicator

Cisco IP Communicator – додаток для робочого столу, що перетворює комп'ютер в повнофункціональний IP-телефон Cisco Unified, який дозволяє здійснювати і отримувати дзвінки, а також виконувати інші операції обробки викликів.

При установці програми Cisco IP Communicator на портативний комп'ютер можна використовувати Cisco IP Communicator (з усіма телефонними системами параметрами налаштування) в будь-якому місці, в якому можна установити з'єднання зі своєю корпоративною мережею.

Наприклад, підключившись до мережі, Cisco IP Communicator можна використовувати для прийому викликів та прослуховування голосових повідомлень. Cisco IP Communicator працює з Cisco Unified Video Advantage, іншим настільним додатком, що додає до можливостей зв'язку передачу відео.

Для установки Cisco IP Communicator виконаємо наступні дії:

– виділяємо Cisco IP Communicator Setup.exe та тиснемо "Enter";

– у вікні Cisco IP Communicator – InstallShield Wizard натиснемо "Next";

– далі читаємо ліцензійну угоду, вибираємо "I accept the terms in the license agreement" та натиснемо "Next";

– вибираємо шлях до теки, куди треба встановити програму та натиснемо "Next";

– натиснемо "Install";

– натиснемо "Finish";

– перезавантажуємо комп’ютер.

2.3 Створення loopback інтерфейсу (Windows)

Для початку створимо loopback інтерфейс в Windows, на якому ми збираємося емулювати маршрутизатор. Для цього виконаємо наступні дії:

– натиснемо "Пуск", "Панель Управления", "Принтеры и другое оборудование", "Установка оборудования", "Далее";

– вибираємо "Да, устройство уже подсоединено", натиснемо "Далее";

– вибираємо "Добавление нового устройства", "Далее";

– вибираємо "Установка оборудования, выбранного из списка вручну", "Далее";

– вибираємо "Сетевые платы", "Далее";

– вибираємо ім’я виробника "Microsoft", а справа – "Адаптер Microsoft замыкания на себя", "Далее", "Далее", "Готово".

– вже на цьому етапі ми можемо взаємодіяти з віртуальною мережею, але лише з одного комп'ютера. А наша мета – відкрити доступ до неї зі всіх машин реальної мережі;

– заходимо в розділ "Сетевые подключения", виділяємо обидва адаптери – реальний, за допомогою якого ми виходимо в реальну мережу та віртуальний "loopback", який ми створили. Далі натискаємо "Створити міст". В результаті отримаємо з'єднання типа "міст", яке дозволяє обмінюватися трафіком віртуальному інтерфейсу та реальному;

– при створенні моста система сама призначає йому IP адреу і її нам треба знати;

– дізнатися IP-адресу, яку Windows присвоїв мосту ми зможемо, наприклад, за допомогою команди "ipconfig /all" і запам’ятати, або записати її;

– перезавантажити комп’ютер.

2.4 Емуляція VoIP в GNS3

Тепер почнемо створення маршрутизатора в GNS3 і налаштування Cisco Communication Manager Express (CME).

Для цього необхідні наступні дії:

– запускаємо GNS3;

– створюємо новий проект (в проекті будемо використовувати Router c7200);

– на головне поле переносимо Router c7200 (образ якого ми додали раніше в л.р. № 1), натискаємо праву клавішу миші на Router c7200 та обираємо "Configure", переходимо на вкладку "Slots" та обираємо зі списку C7200-IO-2FE, далі натиснемо "OK";

– на головне поле переносимо "Cloud";

– натискаємо правою клавішею миші на "Cloud" та обираємо команду "Configure", натиснемо на "C1";

– в NIO Ethernet вибираємо наш "MSLoopBack", натиснемо "ADD" (рис. 2.1);

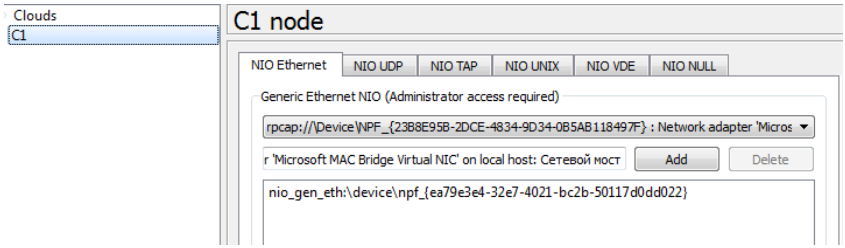

Рисунок 2.1 – Конфігурування "C1 node"

– натиснемо "Apply";

– зв’язуємо маршрутизатор та "Cloud" натиснувши на "Addlink – FastEthernet" (рис. 2.2);

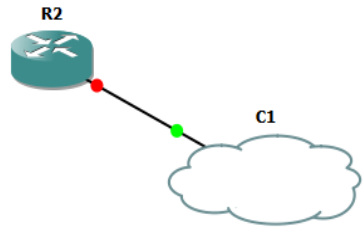

Рисунок 2.2 – З’єднання маршрутизатора та "Cloud"

– натискаємо правою клавішею миші на маршрутизаторі та обираємо команду "Start";

– натискаємо правою клавішею миші на маршрутизаторі та обираємо команду "Console";

– коли маршрутизатор готовий вводимо наступні команди:

```
enable
config t
interface FastEthernet0/0
ip address 192.168.1.50 255.255.255.0
```

(інтерфейсу потрібно привласнити IP адресу, яка входить в створену мережу, але не використовується іншими пристроями, включаючи створений міст)

```
no shutdown
```

– перевіряємо правильність налаштувань, для цього заходимо в консоль та перевіряємо зв'язок з віртуальним маршрутизатором (ping 192.168.1.50), в консолі маршрутизатора перевіряємо зв'язок з пристроями нашої мережі, наприклад:

```
ping 192.168.1.1
```

– далі переходимо знову до консолі роутера та вводимо такі команди:

```
telephony-service
max-ephones 10
```

(команда max-ephones встановлює максимальну кількість IP телефонів, які обслуговуватиме даний маршрутизатор)

```
max-dn 10
```

(max-dn, відповідно, максимальна кількість ліній)

```
ip source-address 192.168.1.50 port 2000
```

(команда ipsource-address вказує з якого інтерфейсу CME повинен приймати запити на підключення до нього телефонів)

```
auto assign 1 to 10
```

(команда auto assign 1 to 10 вказує маршрутизатору що треба, щоб він автоматично призначав лінії з номерами від 1 до 10, підключеним телефонам);

– налаштовуємо лінії – вводимо в консоль роутера:

```
exit
ephone-dn 1
number 101
ephone-dn 2
number 102
```

(командою ephone-dn ми створюємо лінію, а number привласнює цій лінії телефонний номер).

Системні повідомлення, які спливають в командному рядку, допоможуть нам зрозуміти, що лінії активовані і включені.

2.5 Тестування отриманих результатів

Наступний етап - встановлення та налаштування Cisco IP Communicator.

Для цього виконаємо такі дії:

– запускаємо Cisco IP Communicator, який встановили раніше. В результаті з’явиться телефон, що зображений на рисунку 2.3;

– натискаємо правою клавішею миші на ньому та заходимо в налаштування;

– на вкладці "Network" в "Network Adapter" вибираємо адаптер, через який є підключення до мережі (в нашому випадку – це міст), а в "Use these TFTP servers" вводимо адресу нашого віртуального роутера;

– після цього телефон перезавантажиться, знайде CME, авторизується там і виглядатиме як показано на рисунку 2.4;

Рисунок 2.3 – Cisco IP Communicator

– виконавши такі ж маніпуляції на другому комп'ютері у мережі, ви отримаєте другий телефон з відповідним номером, і так далі. Таким чином, нарощуючи віртуальну мережу, і піднімаючи все нові і нові софтфони на комп'ютерах, ми можемо створити досить складну інфраструктуру.

Рисунок 2.4 – Підключений телефон VoIP

Примітка. Комунікатор та GNS3 мають працювати одночасно. При налаштуванні "Cloud" підключаємо мережевий адаптер

"MSLoopBack". При налаштуванні комунікатора – в налаштуванні Інтернету вказуємо міст.

2.6 Зміст звіту

- хід роботи;
- результати отримані в процесі виконання загальних етапів;
- опис переваг та недоліків технології VoIP;
- основні етапи моделювання VoIP в GNS3.

2.7 Контрольні питання

1. Які протоколи використовує технологія VoIP?
2. Опишіть передачу мови в цифровій формі.
3. Що лежить у основі кодека мови зі змінною швидкістю?
4. Опишіть фрагменти сигналу, які класифікуються як активна мова або як пауза.
5. Для чого використовується Cisco IP Communicator?
6. Опишіть створення loopback інтерфейсу в Windows.

3 ЛАБОРАТОРНА РОБОТА. Протокол MPLS

Мета роботи: ознайомитися з протоколом MPLS та навчитися його емулювати в програмному забезпеченні GNS3.

3.1 Теоретичні відомості

MPLS (Multiprotocol Label Switching) – багатопротокольна комутація по мітках. Вона частково замінює IP-маршрутизацію – рішення про пересилку пакету (вихідний інтерфейс і наступний хоп маршруту) приймається не на основі полів IP-заголовку (зазвичай адреса призначення) і таблиці маршрутизації, а на основі міток, які прикріплені до пакету. Такий підхід прискорює процес пересилки, тому що пошук наступного хопа стає значно простішим в порівнянні з пошуком маршруту.

Ефективність пересилки – не основна перевага MPLS. MPLS вносить до мережевих технологій якісно нові можливості, наприклад маршрутизація за адресою джерела. MPLS-пересилки відключають обробку заголовків мережевого рівня (наприклад, IP), тому дії, засновані на мережевому рівні, такі як NAT і фільтрації не можуть бути застосовані до тих пакетів, що пересилаються з використанням MPLS пакетів. Будь-які дії, засновані на мережевому рівні, повинні виконуватись на вході або виході з хмари MPLS.

У простій формі MPLS можна розглядати як поліпшення маршрутизації: мітки розподіляються за допомогою протоколу LDP для маршрутів, які є активними і помічений пакет проходить той же шлях, який він би пройшов, навіть якщо б не був маркований. Шлях комутації по міткам забезпечує передачу даних на вихід з хмари MPLS. Використання MPLS ґрунтуються на базовій концепції шляху комутації по міткам LSP (label switching path).

Коли мітка присвоюється пакету, вона збільшує його довжину на 32 біти (4 байти). Ці 32 біта розподіляються таким чином:

– мітка (20 біт) - вибір відповідного шляху комутації по мітках;

– час життя (TTL) (8 біт) – аналог поля IP- пакету. Потрібно, щоб LSR могли відкидати пакети, тільки на підставі інформації, яка міститься в заголовку MPLS, не звертаючись до заголовку IP;

– клас послуги (Class of Service). Поле CoS (3 біти), спочатку зарезервовано для розвитку технології, використовується в основному для вказівки класу трафіку, що вимагає певного рівня QoS;

– ознака дна стека міток (S), займає 1 біт.

MPLS працює з класами еквівалентності при пересилці (forwarding equivalence class – FEC). Приклади класів FEC: пакети з однаковою мережею призначення; пакети з однаковою мережею призначення і однаковою мережею джерелом; пакети з однаковими портами призначення і т.п.

Для пакетів з кожного класу FEC MPLS призначає свою систему міток, що дозволяє їх однаково обробляти. Де б пакет не знаходився в MPLS-мережі, мітка визначає до якого FEC пакет відноситься і може бути оброблений залежно від FEC. Саме цією властивістю MPLS вносить принципово нову якість до сучасних мережевих технологій.

3.2 Конфігурація та моделювання мережі з MPLS в GNS3

Виконаємо конфігурування та моделювання мережі з протоколом MPLS в GNS3. Для цього зробимо наступне:

– запускаємо програму GNS3;

– створюємо новий проект;

– в лабораторній роботі використовуємо Router c3600 та відповідно c3640-jk9s-mz.124-16.bin;

– розташуємо на головному полі три екземпляри Router c3600;

– кожен маршрутизатор має такі характеристики (натиснемо на праву кнопку миші та обираємо команду "Configure"):

```
R1:    slot0=NM-4E
R2:    slot0=NM-4E
R3:    slot0=NM-4E
```

– з’єднуємо їх як показано на рисунку 3.1;

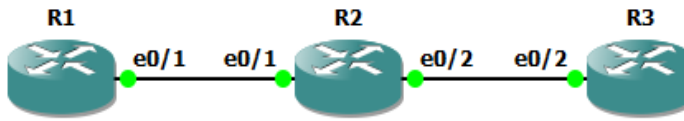

Рисунок 3.1 – Схема з’єднання роутерів 3600

– починаємо конфігурувати маршрутизатори: на панелі інструментів тиснемо на  , далі тиснемо  , переходимо до консолі роутера R1 та вводимо команди:

```
enable
conf t
 hostname R1
 ip cef
 mpls ip
 mpls traffic-eng tunnel
interface Loopback0
 ip address 10.10.10.1 255.255.255.255
 exit
interface Ethernet0/1
 ip address 10.0.1.2 255.255.255.0
```

```
 mpls ip
 mpls traffic-eng tunnel
 no shutdown
 exit
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 exit
interface Tunnel1
 ip unnumbered Loopback0
 tunnel destination 10.10.10.3
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 dynamic
end
```

– переходимо до консолі роутера R2 та вводимо команди:

```
enable
conf t
 hostname R2
 ip cef
 mpls ip
 mpls traffic-eng tunnel
interface Loopback0
 ip address 10.10.10.2 255.255.255.255
 exit
interface Ethernet0/1
 ip address 10.0.1.1 255.255.255.0
 mpls ip
 mpls traffic-eng tunnel
 no shutdown
 exit
interface Ethernet0/2
 ip address 10.0.2.1 255.255.255.0
 mpls ip
 mpls traffic-eng tunnel
 no shutdown
 exit
```

```
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
end
```

– переходимо до консолі роутера R3 та вводимо команди:

```
enable
conf t
 hostname R3
 ip cef
 mpls ip
 mpls traffic-eng tunnel
interface Loopback0
 ip address 10.10.10.3 255.255.255.255
 exit
interface Ethernet0/2
 ip address 10.0.2.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnel
 no shutdown
 exit
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
end
```

– перевіряємо налаштування MPLS. Для цього треба натиснути правою кнопкою на з'єднання між роутерами R1 та R2, обрати пункт "Start capture". У вікні обрати порт Ethernet0/1 R2 та натиснути OK;

– відкриється вікно аналізатору пакетів Wireshark. В ньому у полі "Filter" вказуємо фільтр icmp та натискаємо Enter;

– в консолі роутера R1 виконуємо команду "ping 10.10.10.3";

– у вікні Wireshark знаходимо будь-який пакет exo-запиту "Echo (ping) request", в нижній частині вікна має бути заголовок MPLS "MultiProtocol Label Switching Header" (рис. 3.2);

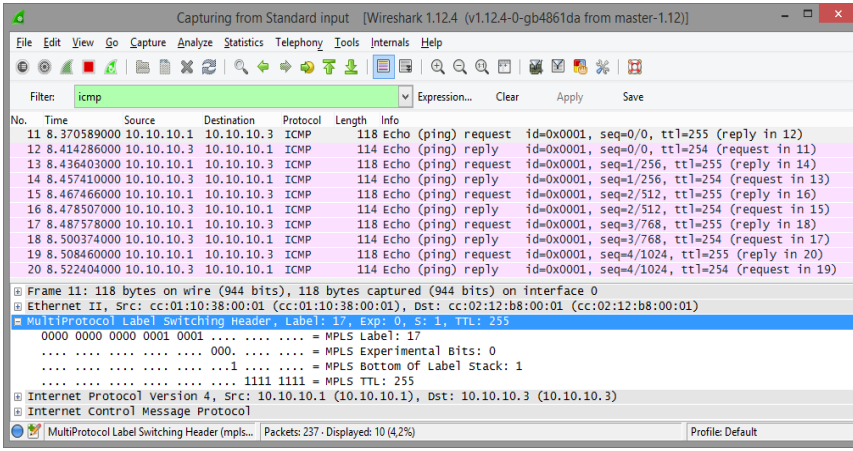

Рисунок 3.2 – Перевірка наявності заголовка MPLS

3.3 Зміст звіту

– хід роботи;
– результати отримані в процесі виконання загальних етапів;
– статистика з маршрутизатора R1, зібрана за допомогою наступних команд:

```
show ip interface brief
show ip route
show ip cef
show ip vrf
show ip rsvp listeners
show mpls forwarding-table
show mpls forwarding-table detail
show mpls interfaces
show mpls interfaces detail
show mpls ip binding
show mpls ip binding detail
show mpls ip binding local
show mpls ip binding summary
show mpls label range
show mpls ldp backoff
show mpls ldp bindings
show mpls ldp bindings detail
```

```
show mpls ldp discovery
show mpls ldp graceful-restart
show mpls ldp igp sync all
show mpls ldp neighbor
show mpls ldp neighbor detail
show mpls ldp parameters
show mpls static binding
show mpls static crossconnect
show mpls traffic-eng autoroute
show mpls traffic-eng link-management admission-
control
show mpls traffic-eng link-management
advertisements
show mpls traffic-eng link-management bandwidth-
alloc
show mpls traffic-eng link-management igp-neighbors
show mpls traffic-eng link-management interfaces
show mpls traffic-eng link-management statistics
show mpls traffic-eng topology
show mpls traffic-eng topology brief
show tag-switching forwarding-table
show tag-switching forwarding-table detail
show tag-switching interfaces detail
```

– статистика з маршрутизаторів R2 та R3, зібрана за допомогою наступних команд:

```
show ip interface brief
show ip route
show mpls forwarding-table
```

3.4 Контрольні питання

1. Переваги технології MPLS.
2. Які протоколи входять у MPLS?
3. Основні команди налаштування MPLS-маршрутизаторів.
4. Чи використовуються таблиці маршрутизації в MPLS-маршрутизаторах?

4 ЛАБОРАТОРНА РОБОТА.
Конфігурування IP-телефонії

Мета роботи: виконання моделювання і конфігурування мережі, а також налаштування IP-телефонії.

4.1 Побудова моделі мережі

Запустіть Packet Tracer. Зберіть мережу за схемою, представленою на рисунку 4.1, з основними параметрами комутаційного обладнання та інтерфейсів (табл. 4.1).

Для цього виконайте наступні дії.

З панелі приладів в робочу область перенесіть 3 комутатори 2950-24 та 3 роутери 2811 (для цього на панелі приладів необхідно вибрати перший елемент – Switches, потім елемент 2811 на панелі Routers (рис. 4.2).

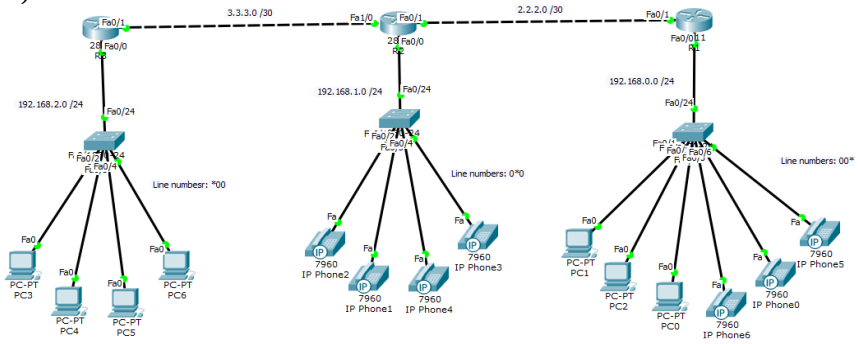

Рисунок 4.1 – Модель мережі

Додайте 7 комп'ютерів та 7 ip-телефонів і з'єднайте їх з комутатором 2950-24, а комутатори з'єднайте з відповідними роутерами згідно з рисунком 4.1 (комп'ютери та телефони знаходяться в розділі End Devices). Для маршрутизатора R2 необхідно встановити NM-2FE2W модуль як показано на рисунку 4.3.

Таблиця 4.1 – Параметри інтерфейсів

Device (Hostname)	IP address
R1(fa0/0)	192.168.0.24/24
R1(fa0/1)	2.2.2.1/30
R2(fa0/0)	192.168.1.254/24
R2(fa0/1)	2.2.2.2/30
R2(fa1/0)	3.3.3.1/30
R3(fa0/0)	192.168.2.254/24
R1(fa0/1)	3.3.3.2/30

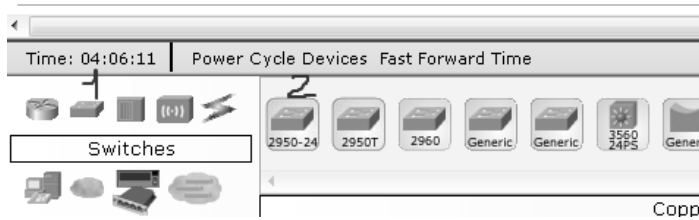

Рисунок 4.2 – Панель обладнання

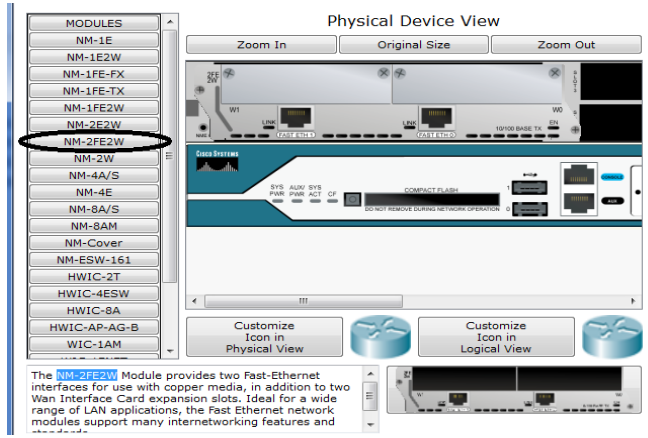

Рисунок 4.3 – Встановлення модулю на R2

4.2 Налаштування коммутаторів та маршрутизаторів

Всі комутатори необхідно конфігурувати через CLI інтерфейс:

```
S1>ena
S1#conf t
S1(config)#interface range fastEthernet0/1-24
S1(config-if-range)#switchport voice vlan 1
```

Перед налаштуванням маршрутизаторів спочатку зконфігуруємо DHCP:

```
R1(config)#ip dhcp pool pool_R1
R1(dhcp-config)#network 192.168.0.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.0.254
R1(dhcp-config)#option 150 ip 192.168.0.254
R1(dhcp-config)#exit
R1(config)#
```

Встановлюємо робочі станції в режим DHCP отримання адрес (рис. 4.4) та підключаємо живлення до IP-телефонів (рис. 4.5). Після цього всі робочі станції та IP-телефони повинні отримати IP-адреси.

Конфігурація для R2:

```
R2(config)#ip dhcp pool pool_R2
R2(dhcp-config)#network 192.168.1.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.254
R2(dhcp-config)#option 150 ip 192.168.1.254
R2(dhcp-config)#exit
R2(config)#
```

Конфігурація для R3:

```
R3(config)#ip dhcp pool pool_R3
R3(dhcp-config)#network 192.168.2.0 255.255.255.0
R3(dhcp-config)#default-router 192.168.2.254
R3(dhcp-config)#option 150 ip 192.168.2.254
R3(dhcp-config)#exit
R3(config)#
```

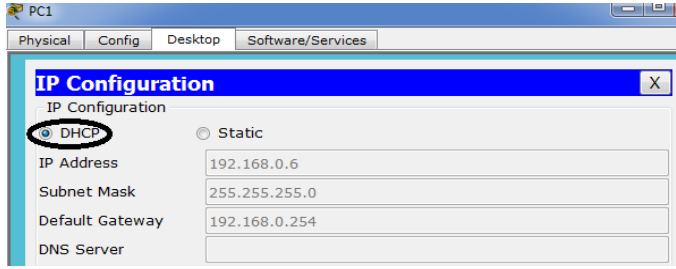

Рисунок 4.4 – Встановлення режиму DHCP

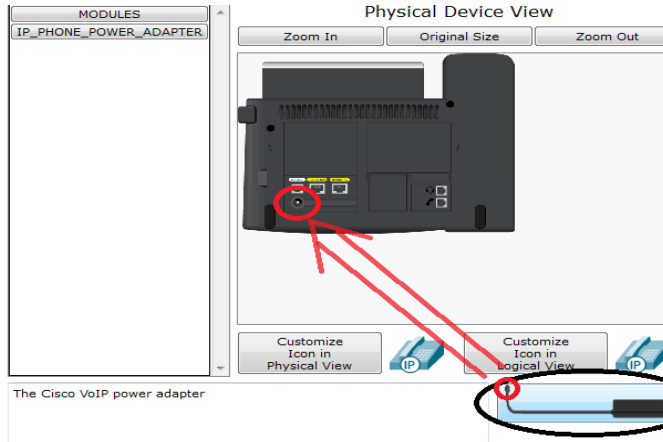

Рисунок 4.5 – Підключення живлення до телефону

Переходимо до конфігурування IP телефонії на R1:

```
R1(config)#telephony-service
R1(config-telephony)#max-dn 10
R1 (config-telephony)#max-ephones 10
R1 (config-telephony)#auto-reg-ephone
R1 (config-telephony)#auto assign 1 to 10
R1 (config-telephony)#ip source-address
192.168.0.254 port 2000
R1 (config-telephony)#exit
R1(config-telephony)#ephone-dn 1
R1(config-ephone-dn)#number 001
R1(config-ephone-dn)#exit
```

```
R1(config)#ephone-dn 2
R1(config-ephone-dn)#number 002
R1(config-ephone-dn)#exit
R1(config)#ephone-dn 3
R1(config-ephone-dn)#number 003
R1(config-ephone-dn)#exit
R1(config)#ephone-dn 4
R1(config-ephone-dn)#number 004
R1(config-ephone-dn)#exit
R1(config)#ephone-dn 5
R1(config-ephone-dn)#number 005
R1(config-ephone-dn)#exit
R1(config)#ephone-dn 6
R1(config-ephone-dn)#number 006
R1(config-ephone-dn)#exit
R1(config)#
```

Після цього кожен телефон та Cisco IP Communicator повинен отримати відповідний нормер (рис. 4.6 та рис. 4.7).

Рисунок 4.6 – Отримання номеру лінії на IP-телефоні

Рисунок 4.7 – Отримання номеру лінії на Cisco IP Communicator

Конфігурація для R2:

```
R2(config)#telephony-service
R2(config-telephony)#max-dn 10
R2 (config-telephony)#max-ephones 10
R2 (config-telephony)#auto-reg-ephone
R2 (config-telephony)#auto assign 1 to 10
R2 (config-telephony)#ip source-address
192.168.1.254 port 2000
R2 (config-telephony)#exit
R2(config-telephony)#ephone-dn 1
R2(config-ephone-dn)#number 010
R2(config-ephone-dn)#exit
R2(config)#ephone-dn 2
R2(config-ephone-dn)#number 020
R2(config-ephone-dn)#exit
R2(config)#ephone-dn 3
R2(config-ephone-dn)#number 030
R2(config-ephone-dn)#exit
R2(config)#ephone-dn 4
R2(config-ephone-dn)#number 040
R2(config-ephone-dn)#exit
R2(config)#
```

Конфігурація для R3:

```
R3(config)#telephony-service
R3(config-telephony)#max-dn 10
R3 (config-telephony)#max-ephones 10
R3 (config-telephony)#auto-reg-ephone
R3 (config-telephony)#auto assign 1 to 10
R3       (config-telephony)#ip       source-address
192.168.2.254 port 2000
R3 (config-telephony)#exit
R3(config-telephony)#ephone-dn 1
R3(config-ephone-dn)#number 100
R3(config-ephone-dn)#exit
R3(config)#ephone-dn 2
R3(config-ephone-dn)#number 200
R3(config-ephone-dn)#exit
R3(config)#ephone-dn 3
R3(config-ephone-dn)#number 300
R3(config-ephone-dn)#exit
R3(config)#ephone-dn 4
R3(config-ephone-dn)#number 400
R3(config-ephone-dn)#exit
R3(config)#
```

Далі необхідно налаштувати маршрутизацію на кожному роутері.

```
R1(config)#router ospf 1
R1  (config-router)#network  192.168.0.0  0.0.0.255
area 0
R1 (config-router)#network 2.2.2.0 0.0.0.3 area 0
R1 (config-router)#exit
```

Конфігурація відповідно для R2 та R3:

```
R2(config)#router ospf 1
R2  (config-router)#network  192.168.1.0  0.0.0.255
area 0
R2 (config-router)#network 2.2.2.0 0.0.0.3 area 0
R2 (config-router)#network 3.3.3.0 0.0.0.3 area 0
R2 (config-router)#exit

R3(config)#router ospf 1
R3  (config-router)#network  192.168.1.0  0.0.0.255
area 0
```

```
R3 (config-router)#network 3.3.3.0 0.0.0.3 area 0
R3 (config-router)#exit
```

Після налаштування маршрутизації необхідно перевірити надходження пакетів між мережами. Далі необхідно налаштувати зв'язок між телефонами та коммунікаторми з різних мереж. Для цього виконаємо наступні команди на роутерах.

Для встановлення звязку між мережами роутерів R1 та R2:

```
R1(config)#dial-peer voice 1 voip
R1(config-dial-peer)#destination-pattern 0.0
R1(config-dial-peer)#session target ipv4:2.2.2.2
R1(config-dial-peer)#exit

R2(config)#dial-peer voice 1 voip
R2(config-dial-peer)#destination-pattern 00.
R2(config-dial-peer)#session target ipv4:2.2.2.1
R2(config-dial-peer)#exit
```

Примітка. Необхідно приділити увагу параметру *destination-pattern*. Для R1 ми вказали його рівним "0.0". Це тому, що номера лінії на роутері R2 дорівнюють 010, 020, 030 і т.п. Відповідно для роутера R2 цей параметр дорівнює "00.", бо номера лінії з мережі R1 дорівнюють 001, 002, 003, 004 і т.д.

Зв'язок між роутером R3 та R2:

```
R3(config)#dial-peer voice 2 voip
R3(config-dial-peer)#destination-pattern 0.0
R3(config-dial-peer)#session target ipv4:3.3.3.1
R3(config-dial-peer)#exit

R2(config)#dial-peer voice 2 voip
R2(config-dial-peer)#destination-pattern .00
R2(config-dial-peer)#session target ipv4:3.3.3.2
R2(config-dial-peer)#exit
Зв'язок між роутером R1 та R3:

R1(config)#dial-peer voice 3 voip
R1(config-dial-peer)#destination-pattern .00
R1(config-dial-peer)#session target ipv4:3.3.3.2
```

```
R1(config-dial-peer)#exit

R3(config)#dial-peer voice 3 voip
R3(config-dial-peer)#destination-pattern 00.
R3(config-dial-peer)#session target ipv4:2.2.2.1
R3(config-dial-peer)#exit
```

Після цього необхідно зателефонувати з кожної мережі в кожну (рис. 4.8 та рис. 4.9).

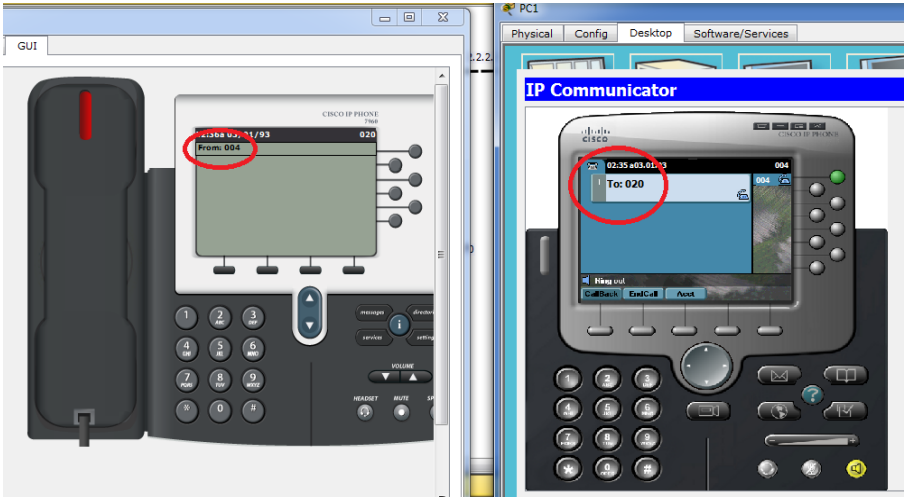

Рисунок 4.8 – Перевірка коректності налаштування

4.3 Моделювання передачі пакетів

Після перевірки зв’язку, для перегляду структури пакетів, що курсують між телефонами, необхідно провести симуляцію та відфільтрувати діючи протоколи та залишити тільки протокол RTP (рис. 4.10).

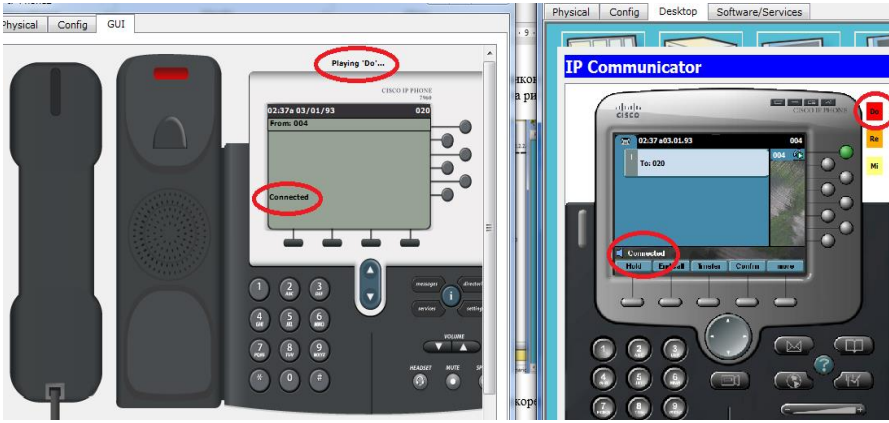

Рисунок 4.9 – Перевірка коректності налаштування

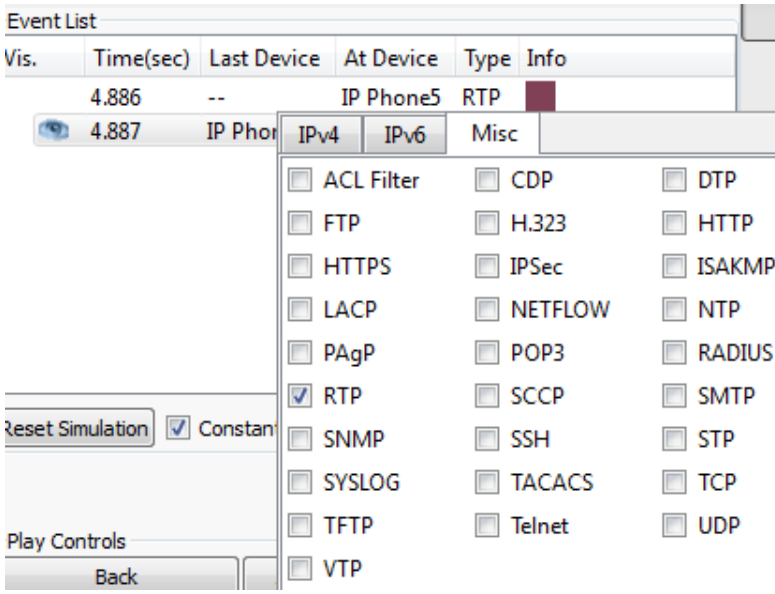

Рисунок 4.10 – Вікно симуляції передачі пакету

Натискаючи на кнопку caption forward ми почнемо пересування пакету по мережі. Вміст пакету, що сформований протоколом RTP, наведено на рис. 4.11.

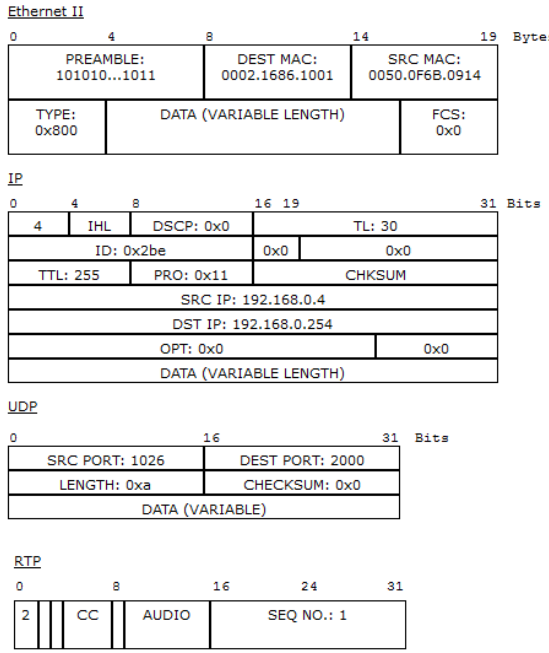

Рисунок 4.11 – Вміст пакету, сформований протоколом RTP

4.4 Індивідуальне завдання

Завдання для першого варіанту: під’єднати до маршрутизатора R1 ще один маршрутизатор з комутатором та двома IP-телефонами. Провести всі відповідні налаштування, щоб можна було телефонувати зі створеної нової мережі в інші, та з інших мереж в нову.

Завдання для другого варіанту: під’єднати до маршрутизатора R3 ще один маршрутизатор з комутатором та двома робочими станціями. Провести всі відповідні налаштування, щоб можна було телефонувати зі створеної нової мережі в інші, та з інших мереж в нову.

4.5 Зміст звіту

– хід роботи;
– результати отримані в процесі виконання загальних етапів роботи;
– структура створеної мережі;
– структура пакетів, сформованих протоколом RTP.

4.6 Контрольні питання

1. Визначення та характеристики VoIP.
2. Приклади застосування VoIP.
3. Архітектура VoIP.
4. Протоколи VoIP та їх функції.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101 / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 912 с. – ISBN 978-5-8459-1906-9.

2. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 736 с. – ISBN 978-5-8459-1907-6.

3. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. – 5-е изд. – СПб.: Питер, 2016. – 992с.: ил.

4. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д.Уэзеролл. – 5-е изд. – СПб.: Питер, 2012. – 960 с.

5. Бакланов И.Г. NGN: принципы построения и организации. – М. : Эко–Трендз, 2008. – 400 с.

6. Гольдштейн А.Б. Технология и протоколы MPLS / А.Б.Гольдштейн, Б.С.Гольдштейн. – СПб.: БХВ, 2005. – 304 с. Глотиков К. IMS (IP multimedia Subsystem). М. : Эко-трендз. 2009. – 100 с.

7. Гольдштейн Б.С. Сети связи. Учебник для вузов / Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский. – СПБ. : БХВ, 2009. – 400 с.

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