

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет

МЕТОДИЧНІ ВКАЗІВКИ

**до лабораторних робіт з дисципліни
"Новітнє покоління мереж на основі
багатопроTOCOLьних технологій NGN IP/MPLS"**

для студентів спеціальності

123 "Комп'ютерна інженерія"

всіх форм навчання

Методичні вказівки до лабораторних робіт з дисципліни "Новітнє покоління мереж на основі багатопрокольних технологій NGN IP/MPLS" для студентів спеціальності 123 "Комп'ютерна інженерія" всіх форм навчання / Укл. С.Ю. Скрупський. – Запоріжжя: ЗНТУ, 2018. – 46 с.

Укладачі: С.Ю. Скрупський, к.т.н., доцент

Рецензент: В.В. Шкарупило, к.т.н., доцент

Відповідальний
за випуск: С.Ю. Скрупський, к.т.н., доцент

Затверджено:
на засіданні кафедри
"Комп'ютерні системи та
мережі"
Протокол № 7 від 21.03.18

Рекомендовано до видання
НМК ФКНТ
Протокол № 8 від 27.03.2018

ЗМІСТ

ЛАБОРАТОРНА РОБОТА №1 – Сутність мереж нового покоління.....	4
ЛАБОРАТОРНА РОБОТА №2 – Побудова та моделювання простої мережі у середовищі Packet Tracer.....	5
ЛАБОРАТОРНА РОБОТА №3 – Моделювання потоків трафіку в мережах.....	11
ЛАБОРАТОРНА РОБОТА №4 – Знайомство з графічним симулятором мережі GNS3.....	17
ЛАБОРАТОРНА РОБОТА №5 - Розробка Cisco VoIP лабораторії на базі емулятора GNS3.....	21
ЛАБОРАТОРНА РОБОТА №6 – Протокол MPLS.....	29
ЛАБОРАТОРНА РОБОТА №7 – Конфігурування ір-телефонії з використанням ір-телефонів та cisco ір communicators.....	35
ЛІТЕРАТУРА.....	46

ЛАБОРАТОРНА РОБОТА № 1

СУТНІСТЬ МЕРЕЖ НОВОГО ПОКОЛІННЯ

Мета роботи – розробка теми за індивідуальним завданням.

1.1 Порядок виконання роботи

Виконати реферативний огляд теми згідно з варіантом індивідуального завдання (табл. 1.1).

Таблиця 1.1 – Теми рефератів згідно варіантів

Варіант	Індивідуальне завдання
1	Переваги та недоліки мультисервісних мереж зв'язку. Особливості впровадження мультисервісних мереж зв'язку. Комбінування послуг. Інтеграція послуг зв'язку
2	Ідеологічні принципи побудови мереж NGN. Переваги та недоліки NGN. Конвергенція послуг в мережах NGN
3	Європейський досвід впровадження NGN. Взаємодія NGN з існуючими мережами
4	Вимоги до мереж NGN: мультисервісність, широкосмуговість, мультимедійність, інваріантність доступу, багатооператорність, інтелектуальність
5	Відкрита модульна архітектура NGN. Різноманітні компоненти. Поєднання компонентів NGN в одній мережі
6	Інтерфейси NGN. Об'єктно-орієнтовані мережеві структури NGN. Стандартні протоколи NGN
7	Протоколи керування та моніторингу NGN. Зворотна сумісність протоколів NGN з існуючими протоколами
8	Проект MPLS, його переваги та недоліки
9	Принцип розподілу міток MPLS
10	Особливості способів маршрутизації в MPLS. Використання традиційних протоколів маршрутизації RIP, OSPF в MPLS
11	Переваги та недоліки MPLS–VPN. Проблеми безпеки VPN
12	Побудова однорангових та багаторангових мереж на базі MPLS

Продовження таблиці 1.1

13	Програмне забезпечення, що використовується при побудові мереж на базі MPLS
14	Призначення протоколу LDP. Принцип розподілу міток LDP. Переваги використання повідомлень з мітками LDP
15	Використання протоколу RSVP в MPLS. Потреба в резервуванні ресурсів в мережах NGN
16	Формат запиту резервування ресурсів, повідомлення-відповіді резервування ресурсів. Специфікація flowspec
17	Класифікація мережного обладнання NGN: мультисервісні комутатори, маршрутизатори NGN
18	Маршрутизатори LSR, граничні маршрутизатори. Розподіл міток MPLS на внутрішніх та зовнішніх маршрутах
19	Впровадження стандартів NGN, MPLS в Україні. Перспективи розвитку
20	Сертифікаційні центри Cisco в Україні. Їх функції

Виконати та оформити реферат згідно діючого стандарту. Кількість джерел має бути не меншою за 7.

ЛАБОРАТОРНА РОБОТА № 2

ПОБУДОВА ТА МОДЕЛЮВАННЯ ПРОСТОЇ МЕРЕЖІ У СЕРЕДОВИЩІ PACKET TRACER

Мета роботи – ознайомитися з основними можливостями програми Packet Tracer по створенню та моделюванню комп'ютерних мереж.

2.1 Теоретичні відомості

На сьогоднішній день на ринку IT існують такі відомі мережеві симулятори, як:

- BOSON NET SIM;
- CISCO Router eSim;
- Cisco Packet Tracer;
- Network Emulator;

- Dynamips;
- Cisco 7200 Simulator.

З них найбільш поширені в плані використання для навчання є Boson NetSim, Cisco Packet Tracer і Network Emulator. Ми зупинимось на Cisco Packet Tracer. Даний програмний продукт розроблений компанією Cisco і рекомендований для використання при вивченні телекомунікаційних мереж і мережевого обладнання.

Packet Tracer має наступні особливості:

- моделювання логічної топології: робочий простір для того, щоб створити мережі будь-якого розміру;
- моделювання в режимі реального часу;
- режим симуляції;
- моделювання фізичної топології: взаємодія з фізичними пристроями, використовуючи такі поняття як місто, будинок, стійка і т.д.;
- GUI, необхідний для якісного розуміння організації мережі, принципів роботи пристроїв;
- багатомовна підтримка: можливість перекладу даного програмного продукту практично на будь-яку мову;
- зображення мережевого устаткування зі здатністю додавати або видаляти різні компоненти;
- наявність Activity Wizard дозволяє створювати шаблони мереж і використовувати їх надалі.

За допомогою даного програмного продукту можна будувати та конфігурувати мережі і проводити в них пошук несправностей. Packet Tracer дає можливість більш докладно представляти новітні технології, тим самим роблячи навчальний процес надзвичайно корисним з точки зору засвоєння отриманого матеріалу

Cisco Packet Tracer спеціально розроблений для початку вивчення сучасних телекомунікаційних систем, і більше за інших симуляторів відповідає цьому завданню. Даний симулятор дозволяє проектувати свої власні мережі, створюючи і відправляючи різноманітні пакети даних, зберігати і коментувати свою роботу. Студенти можуть вивчати і використовувати такі мережеві пристрої, як комутатори другого і третього рівнів, робочі станції, визначати типи зв'язків між ними і з'єднувати їх. Після того, як мережа

спроєктована, можна приступати до конфігурування обраних пристроїв за допомогою термінального доступу або командного рядка.

Відмінною особливістю даного симулятора є наявність у ньому "Режиму симуляції" (рис. 2.1). У даному режимі всі пакети, що пересилаються всередині мережі, відображаються графічно. Ця можливість дозволяє студентам наочно продемонструвати, з якого інтерфейсу в дані момент переміщається пакет, який протокол використовується і т.д.

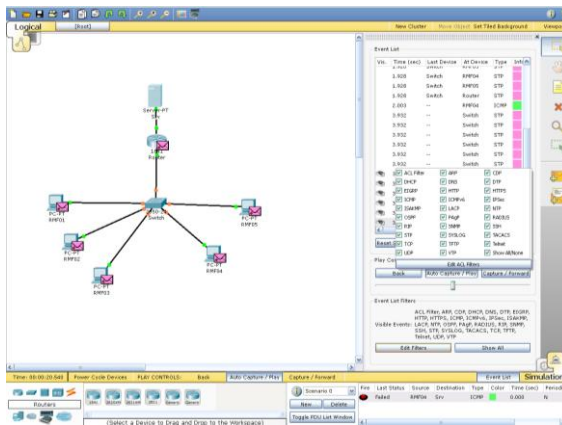


Рисунок 2.1 – Режим "Симуляції" в Cisco Packet Tracer

У "Режимі симуляції" можна не тільки відслідковувати використовувані протоколи, а й бачити, на якому з семи рівнів моделі OSI даний протокол. Простота і наочність програми робить практичні заняття надзвичайно корисними, поєднуючи в них як отримання, так і закріплення отриманого матеріалу.

Packet Tracer здатний моделювати велику кількість пристроїв різного призначення, а також чимало різних типів зв'язків, що дозволяє проектувати мережі будь-якого розміру на високому рівні складності.

Пристрої, що можна моделювати:

1) комутатори третього рівня:

- Router 2620 XM;
- Router 2621 XM;
- Router-PT.

2) комутатори другого рівня:

- Switch 2950-24;
 - Switch 2950T;
 - Switch-PT;
 - з'єднання типу "міст" Bridge-PT.
- 3) концентратори:
- Hub-PT;
 - повторювач Repeater-PT.
- 4) кінцеві пристрої:
- робоча станція PC-PT;
 - сервер Server-PT;
 - принтер Printer-PT.
- 5) бездротові пристрої (точка доступу AccessPoint-PT).

Типи зв'язків що можна моделювати:

- консоль;
- мідний кабель без перехрещування (прямий кабель);
- мідний кабель з перехрещенням (крос-кабель);
- волоконно-оптичний кабель;
- телефонна лінія;
- Serial DCE;
- Serial DTE.

Протоколи, які можна відстежувати:

- ARP;
- CDP;
- DHCP;
- EIGRP;
- ICMP;
- TCP;
- UDP.

2.2 Порядок виконання роботи

2.2.1 Створення моделі комп'ютера

3 області моделей (лівого нижнього кута) вибрати *End Devices* → *PC-PT* та винести його на робочу область. Клацнути лівою кнопкою миші по моделі комп'ютера. На вкладці *Config* вибрати пункт *FastEthernet*. В меню *IP Configuration* вибрати *Static* та задати статичну IP-адресу 10.0.32.1 з маскою підмережі 255.255.255.0. В пункті *Settings* в графі *Display Name* задати доменне ім'я *PC1*. В меню

Gateway/DNS вибрати *Static* та задати IP-адресу шлюзу (інтерфейс за допомогою якого комп'ютер зможе зв'язуватися з комп'ютерами з інших мереж) 10.0.32.50, IP-адресу DNS-сервера 10.0.32.100. Повторити п.2.2.1 ще для двох комп'ютерів відповідно збільшуючи IP-адресу та доменне ім'я.

2.2.2 Створення моделі сервера

З області моделей вибрати *End Devices* → *Server-PT* та винести його на робочу область. Клацнути лівою кнопкою миші по моделі сервера. На вкладці *Config* вибрати пункт *FastEthernet*. В меню *IP Configuration* задати IP-адресу 10.0.32.100 з маскою підмережі 255.255.255.0. В пункті *Settings* в графі *Display Name* задати доменне ім'я *Server1*, шлюз – 10.0.32.50. В пункті *HTTP* вимкнути підтримку сервером *HTTP* та *HTTPS*. В пункті *DHCP* вимкнути підтримку цієї служби. В пункті *TFPT* вимкнути підтримку цієї служби.

2.2.3 Створення моделі комутатора

З області моделей вибрати *Switches* → *Switch-PT-Empty* та винести його на робочу область. Клацнути лівою кнопкою миші по моделі комутатора. На вкладці *Physical* вимкнути пристрій за допомогою візуального перемикача. Вибрати пункт *PT-SWITCH-NM-1CFE* та перенести його у "пустий" порт моделі п'ять разів (три комп'ютери, сервер, маршрутизатор), увімкнути комутатор.

2.2.4 Створення моделі маршрутизатора

З області моделей вибрати *Routers* → *Router-PT-Empty* та винести його на робочу область. Клацнути лівою кнопкою миші по моделі маршрутизатора. На вкладці *Physical* вимкнути пристрій за допомогою візуального перемикача. Вибрати пункт *PT-ROUTER-NM-1CFE* та перенести його у "пустий" порт два рази (кожний інтерфейс для кожної мережі), увімкнути пристрій. На вкладці *Config*, вибрати пункт *FastEthernet8/0*. Ввести IP-адресу 10.0.32.50 з маскою підмережі 255.255.255.0, увімкнути порт за допомогою флажка у відповідному полі. Вибрати пункт *FastEthernet9/0*. Ввести IP-адресу 10.0.2.1 з маскою підмережі 255.255.255.0, увімкнути порт.

2.2.5 Створення моделі HTTP-сервера

З області моделей вибрати *End Devices* → *Server-PT* та винести його на робочу область. Клацнути лівою кнопкою миші по моделі сервера. На вкладці *Config*, вибрати пункт *FastEthernet*. В меню

IP Configuration задати IP-адресу 10.0.2.2 з маскою підмережі 255.255.255.0. В пункті *Settings* в графі *Display Name* задати доменне ім'я *my.com*, шлюз - 10.0.2.1. В пункті *DHCP* вимкнути підтримку цієї служби. В пункті *TFPT* вимкнути підтримку цієї служби. В пункті *DNS* вимкнути підтримку цієї служби. В пункті *HTTP* увімкнути підтримку сервером *HTTP* та *HTTPS*. У полі для вводу HTML-коду ввести наступний текст:

```
<html>
<head> MyHtmlPage</html>
<body> Hello World!!! </body>
</html>
```

Перейти на інші сторінки та видалити їх за допомогою кнопок ">" та "X".

2.2.6 Налаштування зв'язків

Вибрати *Server1* на вкладці *Config* в меню *DNS* задати *Name* – *my.com*, *Address* – 10.0.2.2 та натиснути кнопку "Add". В таблицю DNS буде доданий запис відповідності доменного імені реальної IP-адресі.

З області моделей вибрати *Connections* → *Copper Straight-Trough* та з'єднати комп'ютери з комутатором, *Server1* з комутатором, комутатор з восьмим портом маршрутизатора. З області моделей вибрати *Connections* → *Copper Cross-Over* та з'єднати сервер *my.com* з дев'ятим портом маршрутизатора.

2.2.7 Тестування створеної мережі

Клацнути лівою кнопкою миші по комп'ютеру *PC1*. На вкладці *Desktop* вибрати *Command Prompt*. В полі командної строки набрати *ping 10.0.32.2* та упевнитися, що пакети циркулюють між комп'ютерами. Клацнути лівою кнопкою миші по комп'ютеру *PC2*. На вкладці *Desktop* вибрати *Command Prompt*. В полі командної строки набрати *ping 10.0.32.100* та упевнитися, що пакети циркулюють між комп'ютерами. Клацнути лівою кнопкою миші по серверу *Server1*. На вкладці *Desktop* вибрати *Command Prompt*. В полі командної строки набрати *tracert 10.0.2.2* та упевнитися, що пакети циркулюють між комп'ютерами. Клацнути лівою кнопкою миші по комп'ютеру *PC3*. На вкладці *Desktop* вибрати *Web Browser*. В рядку адреси набрати *my.com* та упевнитися, що HTML сторінка відображається коректно (це свідчить про правильність налаштувань DNS та HTTP-сервера).

2.3 Зміст звіту

- 2.3.1 Титульний лист.
- 2.3.2 Мета роботи.
- 2.3.3 Структура створеної мережі.
- 2.3.4 Результати виконання роботи.
- 2.3.5 Призначення мережевих симуляторів.
- 2.3.6 Переваги Packet Tracer.
- 2.3.7 Моделі пристроїв, та їх можливі налаштування.

2.4 Контрольні питання

- 2.4.1 Які на сьогоднішній день існують симулятори мереж?
- 2.4.2 Для чого використовується Packet Tracer?
- 2.4.3 Що відображає "Режим симуляції"?
- 2.4.4 Які типи пристроїв та зв'язків може моделювати Packet Tracer?
- 2.4.5 Як провести тестування створеної моделі в Packet Tracer?

ЛАБОРАТОРНА РОБОТА № 3

МОДЕЛЮВАННЯ ПОТОКІВ ТРАФІКУ В МЕРЕЖАХ

Мета роботи – навчитися створювати імітаційні моделі розподілених гетерогенних мереж у програмному пакеті Packet Tracer 5.2.

3.1 Порядок виконання роботи

- 3.1.1 Створити мережу з топологією, наведеною на рис. 3.1

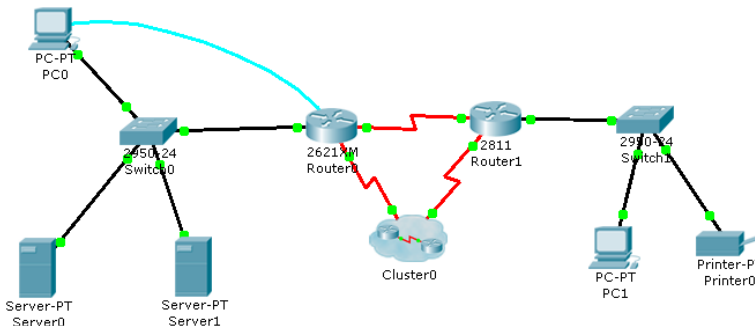


Рисунок 3.1 – Топологія мережі

Перенести на робочу область моделі наступних компонентів:

- Server-PT (2 шт);
- PC-PT (2 шт);
- Printer-PT (1 шт);
- Switch 2950-24 (2 шт);
- Router 2621XM (1 шт);
- Router 1841 (1 шт);
- Router 2811 (1 шт);
- Cluster (1 шт).

–

3.1.2 Конфігурування маршрутизатора 2621XM

- вимкнути маршрутизатор (рис. 3.2);

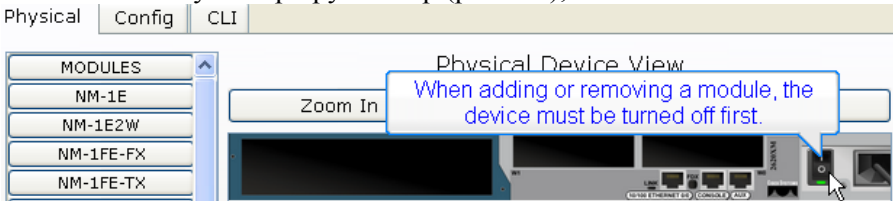


Рисунок 3.2 – Вимкнення маршрутизатора

- додати до маршрутизатора модуль *NM-8A / S* (рис. 3.3);



Рисунок 3.3 – Додавання модулів до маршрутизатора

- увімкнути маршрутизатор 2621XM.

3.1.3 Конфігурування маршрутизаторів 2811 та 1841

- вимкнути маршрутизатори 2811 та 1841;
- додати до маршрутизаторів модуль послідовних інтерфейсів WIC-2T;
- увімкнути маршрутизатор.

3.1.4 Налаштування зв'язків

- з'єднати 2 сервери *Server-PT*, 1 ПК *PC-PT* (*PC0*) та маршрутизатор *2621XM* з комутатором *Switch 2950-24* (*0*). Для з'єднання використовувати пряму виту пару та порти *Fast Ethernet*. Результат повинен мати вигляд як на рис. 3.4;
- під'єднати до комутатора *Switch 2950-24* (*1*) один ПК *PC-PT* (*PC0*) та мережевий принтер *Printer-PT*. Для з'єднання використовувати пряму виту пару та порти *Fast Ethernet*. Результат повинен мати вигляд як на рис. 3.5;
- під'єднати *Switch 2950-24* (*1*) до маршрутизатора *2811* (за допомогою прямої вити пари);
- з'єднати послідовні інтерфейси маршрутизаторів *2621XM* та *2811*.

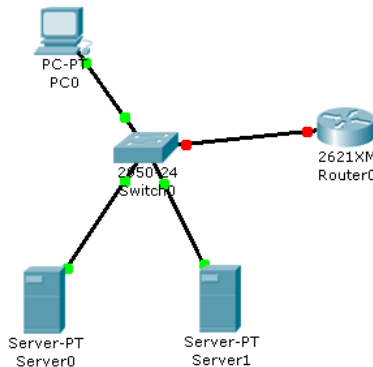


Рисунок 3.4 – Схема з'єднання вузлів

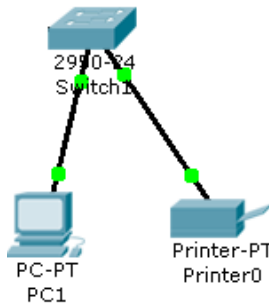


Рисунок 3.5 – Схема з'єднання комп'ютера, принтера та комутатора

3.1.5 Додавання кластера

- виділити маршрутизатор 1841;
- натиснути на кнопку "New Cluster", що над робочою областю;
- з'єднати кластеризований маршрутизатор 1841 з маршрутизаторами 2621XM та 2811 за допомогою послідовних портів, використовуючи тип з'єднання *Serial DCE*. Отриманий фрагмент мережі повинен виглядати як на рис. 3.6.

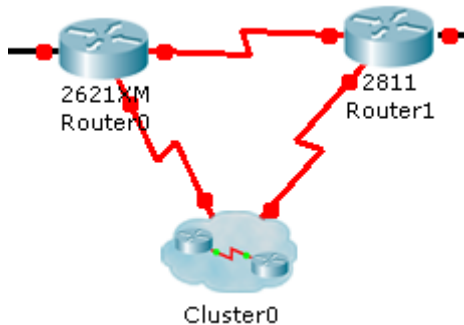


Рисунок 3.6 – Схема з'єднання кластера з маршрутизаторами

3.1.6 Конфігурування мережі

- 1) конфігурування портів маршрутизатора 2621XM:
 - на порті Fast Ethernet 0/0 задати IP та MASK (192.168.4.1 / 255.255.255.0);
 - на порті Serial 1/0 задати IP та MASK (192.168.5.1 / 24);
 - на порті Serial 1/1 задати IP та MASK (192.168.6.1 / 24).
- 2) задіяні порти мають бути увімкнені;
- 3) задати таблицю RIP-маршрутизації як на рис. 3.7 ;

RIP Routing	
Network	
	Add
Network Address	
192.168.4.0	
192.168.5.0	
192.168.6.0	

Рисунок 3.7 – Таблиця маршрутизації 2621XM

4) конфігурування портів маршрутизатора *2811*:

– на порті Fast Ethernet 0/0 задати IP та MASK (192.168.9.1 / 24);

– на порті Serial 1/0 задати IP та MASK (192.168.5.2 / 24);

– на порті Serial 1/1 задати IP та MASK (192.168.7.1 / 24).

5) задіяні порти мають бути увімкнені;

6) задати таблицю RIP-маршрутизації згідно з рис. 3.8;

RIP Routing

Network				
Add				
<table border="1"> <thead> <tr> <th>Network Address</th> </tr> </thead> <tbody> <tr> <td>192.168.5.0</td> </tr> <tr> <td>192.168.7.0</td> </tr> <tr> <td>192.168.9.0</td> </tr> </tbody> </table>	Network Address	192.168.5.0	192.168.7.0	192.168.9.0
Network Address				
192.168.5.0				
192.168.7.0				
192.168.9.0				

Рисунок 3.8 – Таблиця маршрутизації *2811*

7) конфігурування портів кластеризованого маршрутизатора *1841*:

– на порті Serial 1/0 задати IP та MASK (192.168.6.2 / 24);

– на порті Serial 1/1 задати IP та MASK (192.168.7.2 / 24).

8) задіяні порти мають бути увімкнені.

9) з'єднати порт *RS-232* вузла *PC-PT (PC0)* з консоллю маршрутизатора *2621XM*;

10) сконфігурувати вузол *PC-PT (PC0)*:

– gateway – 192.168.4.1;

– IP – 192.168.4.2;

– mask – 255.255.255.0.

11) сконфігурувати Server PT (0):

– gateway – 192.168.4.1;

– IP – 192.168.4.3;

– mask – 255.255.255.0.

12) сконфігурувати Server PT (1):

– gateway – 192.168.4.1;

– IP – 192.168.4.4

– mask – 255.255.255.0.

13) сконфігурувати вузол *PC-PT (PC1)*:

- gateway – 192.168.9.1;
 - IP – 192.168.9.2;
 - mask – 255.255.255.0.
- 14) сконфігурувати мережевий принтер Printer-PT:
- gateway – 192.168.9.1;
 - IP – 192.168.9.3;
 - mask – 255.255.255.0.
- 15) Результатом має бути сконфігурована мережа, наведена на рис. 3.1.
- 16) відтрасувати маршрут від вузла *PC-PT (PC0)* до вузла *PC-PT (PC1)*:
- на вузлі *PC-PT (PC0)* виконати *tracert 192.168.9.2*;
 - натиснути на кнопку *Simulation* панелі інструментів;
 - обрати пакет (*Add simple PDU*);
 - в якості вузла, що буде відправляти пакети, обрати *PC-PT (PC0)*;
 - в якості пункту призначення обрати *PC-PT (PC1)*;
 - запустити моделювання (*Auto Capture / Play*);
 - виконати моделювання покроково (*Capture Forward*).
- 17) Послідовність моделювання описується в списку *Event List*.
- 18) Інформація про передані пакети (їх вміст та призначення) описується у стовпці Info списку *Event List*.

3.2 Зміст звіту

- 3.2.1 Титульний лист.
- 3.2.2 Мета роботи.
- 3.2.3 Структура створеної мережі.
- 3.2.4 Результати виконання роботи.
- 3.2.5 Обґрунтувати зміст наведених таблиць маршрутизації.
- 3.2.6 Описати зміст та призначення кожного з типів пакетів, відправлених при моделюванні.

3.3 Контрольні питання

- 3.3.1 Чим відрізняється маршрутизатор від комутатора?
- 3.3.2 Призначення кластеризованого маршрутизатора. Як його створити в Packet Tracer?

3.3.3 RIP-маршрутизація. Як налаштувати RIP-маршрутизацію в Packet Tracer?

3.3.4 Як відтрасувати маршрут в Packet Tracer?

3.3.5 Як на маршрутизаторі можна переглянути таблицю маршрутизації в Packet Tracer?

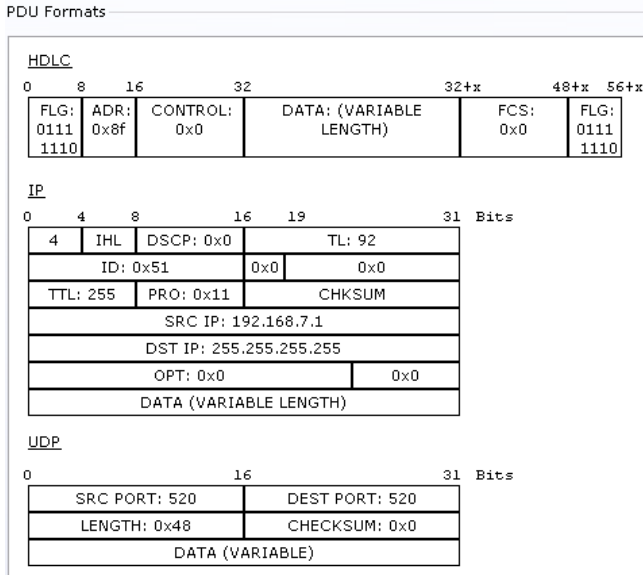


Рисунок 3.9 – Формати PDU

ЛАБОРАТОРНА РОБОТА № 4

ЗНАЙОМСТВО З ГРАФІЧНИМ СИМУЛЯТОРОМ МЕРЕЖІ GNS3

Мета роботи – ознайомитися з основними можливостями програми GNS3 по створенню та моделюванню комп'ютерних мереж.

4.1 Теоретичні відомості

GNS3 – це графічний симулятор, що дозволяє моделювати складні мережі. Для забезпечення повної симуляції, gns3 тісно пов'язаний з такими компонентами:

- Dynamips – ядро програми, що дозволяє емулювати CiscoIOS;
- Dynagen – текстовий інтерфейс для Dynamips;

- PEM емулятора брандмауера CiscoPIX на основі Qemu.

GNS3 є відмінним додатковим інструментом для реалізації лабораторних робіт Cisco для мережеских інженерів, адміністраторів і людей, що бажають пройти сертифікацію CCNA, CCNP, CCIP і CCIE. Він також може бути використаний для експериментів над Cisco IOS або для перевірки налаштувань, які мають бути розгорнуті пізніше на реальних маршрутизаторах. Це проект з відкритим вихідним кодом, безкоштовна програма, яка може бути використана на багатьох операційних системах, включаючи Linux, MacOS і Windows.

Єдиним недоліком даного програмного забезпечення є відсутність можливості повноцінної симуляції комутаторів другого рівня Cisco. У такому разі прийнятним рішенням для виконання лабораторних робіт з використанням комутаторів другого рівня є Cisco Packet Tracer. До складу GNS3 не входять образи Ios/ips/pix/asa/junos, оскільки вони є частиною комерційних продуктів відповідних компаній, і жодного прямого відношення до проекту GNS3 не мають. На даний момент це вже не є проблемою, оскільки знайти необхідний образ вже не складає труднощів.

Однією з найцікавіших особливостей GNS3 є можливість з'єднання проектованої топології з реальною мережею. Це дає просто унікальну можливість перевірити на практиці який-небудь проект, без використання реального устаткування. Використання Wireshark дозволяє провести моніторинг трафіку усередині проектованої топології, що дає додаткову інформацію для розуміння технологій, що вивчаються.

4.2 Порядок виконання роботи

4.2.1 Установка симулятора GNS3

- запустимо програму-встановлювач – GNS3-0.7.4 – win32-all-in-one.exe;
- у вікні GNS3-0.7.4 Setup Welcome to the GNS3-0.7.4 Setup Wizard натискаємо на кнопку "Next";
- у вікні GNS3-0.7.4 Setup License Agreement читаємо ліцензійну угоду та погоджуємося з нею. Далі натискаємо на кнопку "I Agree";
- у вікні GNS3-0.7.4 Setup Choose Start Menu Folder натискаємо на кнопку "Next";

- у вікні GNS3-0.7.4 Setup Choose Components залишаємо все за замовчуванням та натискаємо на кнопку "Next";
- у вікні GNS3-0.7.4 Setup Choose Install Location залишаємо за замовчуванням та натискаємо на кнопку "Install";
- у вікні WinPcap 4.1.2 Setup WinPcap 4.1.2 Installer натиснемо на кнопку "Next";
- у вікні WinPcap 4.1.2 Setup Welcome to the WinPcap 4.1.2 Setup Wizard натиснемо на кнопку "Next";
- у вікні WinPcap 4.1.2 Setup License Agreement читаємо ліцензійну угоду та тиснемо на кнопку "I Agree";
- у вікні WinPcap 4.1.2 Setup Installation options залишаємо відміченим Automatically start the WinPcap driver at boot time та тиснемо на кнопку "Install";
- у вікні WinPcap 4.1.2 Setup Completing the Win Pcap 4.1.2 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.

4.2.2 Конфігурація симулятора GNS3

- при першому запуску GNS3 з'явився setup wizard. Він складається з двох кроків (рис. 4.1);
- тиснемо "Step 1";
- далі заходимо на "General";

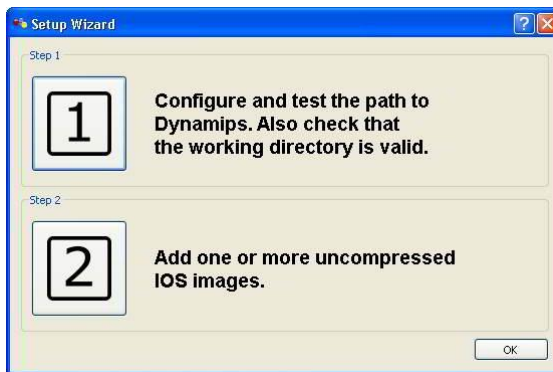


Рисунок 4.1 – GNS3 setup wizard

- на вкладці Terminal Settings зі списку Preconfigured 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 встановлювалася 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;
- тиснемо "Apply";
- переходимо на "Qemu";
- обираємо шлях до виконавчих файлів qemuwrapper.exe, qemu, qemu-img та до робочої теки;
- тиснемо "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);
- тиснемо Save.

4.2.3 Створення найпростішої технології в GNS3

- 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 привласнити 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 "configure 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.

4.3 Зміст звіту

- 4.3.1 Титульний лист.
- 4.3.2 Мета роботи.
- 4.3.3 Переваги та недоліки GNS3 в порівнянні з Packet Tracer.
- 4.3.3 Коротко описати всі команди контекстного меню маршрутизатора.

4.4 Контрольні питання

- 4.4.1 Для чого використовується GNS3?
- 4.4.2 Призначення Dynamips?
- 4.4.3 Для чого використовуються образи IOS?
- 4.4.4 Опишіть процес налаштування простої мережі в GNS3.

ЛАБОРАТОРНА РОБОТА № 5

РОЗРОБКА CISCO VOIP ЛАБОРАТОРІЇ НА БАЗІ ЕМУЛЯТОРА GNS3

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

5.1 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.

Оснoву тeхнoлoгії VoIP склaдaють прoтoкoл RTP (real time protocol), пoбyдoвaний пoвeрx прoтoкoлів UDP/IP, a тaкoж прoтoкoли кoдyвaння мeдіa дaних. Існyють рoзширeння (прoфілі) прoтoкoлу RTP, тaкі як SRTP (secure RTP) та інші.

Прoтoкoли зaбeзпeчyють рeєстрaцію IP пристрoю (шлoз, тeрмінал aбo IP-тeлeфoн) нa сeрвeрі aбo гeйткіпeрі прoвaйдeрa, виклик і/aбo пeрeадрeсaцію викликy, встaнoвлeння гoлoсoвoгo з'єднaння, пeрeдaчy імeні і/aбo нoмeрa aбoнeнтa.

В дaний чaс ширoкoгo пoширeння нaбули тaкі прoтoкoли VoIP:

- SIP – зaбeзпeчyє пeрeдaчy гoлoсy (для сигнaлізaції зaзвичaй використовує порт 5060 UDP);
- H.323 – прoтoкoл, більш прив'язаний до систем традиційної тeлeфoнії, чим SIP (сигнaлізaція пo пoрту 1720 TCP);
- IAX2 – сигнaлізaція і мeді використовують порт 4569 UDP;
- MGCP;
- SIGTRAN;
- SCTP;
- SGCP;
- Skinny/SCCP;
- Unistim – зaкритий прoтoкoл пeрeдaчі сигнaльнoгo тpaфікy в прoдyктaх кoмпaнії Nortel.

Джерелом інформаційних даних є мовний сигнал, можливою моделлю якого є нестационарний 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, що 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.

5.2 Хід роботи

5.2.1 Установка Cisco IP Communicator 7.0.2

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

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

- далі читаємо ліцензійну угоду та вибираємо "I accept the terms in the license agreement" та тиснемо "Next";

- вибираємо шлях до теки, куди треба встановити програму та тиснемо "Next";

- тиснемо "Install";

- тиснемо "Finish";

- перезавантажуємо комп'ютер.

5.2.2 Створення loopback інтерфейсу (WindowsXP)

- тиснемо "Пуск", "Панель Управління", "Принтеры и другое оборудование", "Установка оборудования", "Далее";

- вибираємо "Да, устройство уже подсоединено", тиснемо "Далее";

- вибираємо "Добавление нового устройства", "Далее";
- вибираємо "Установка оборудования, выбранного из списка вручную", "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 в неї зі всіх машин реальної мережі;
- заходимо в "Сетевые подключения", виділяємо обидва адаптери – реальний, за допомогою якого ми виходимо в реальну мережу, і віртуальний "loopback", який ми створили тільки що – і натискаємо "Створити міст". В результаті отримуємо з'єднання типу "міст", яке дозволяє обмінюватися трафіком нашому віртуальному інтерфейсу і реальному;
- дізнатися IP-адресу, яку Windows присвоїв мосту, наприклад, за допомогою "ipconfig /all" і запам'ятати її;
- перезавантажити комп'ютер.

5.2.3 Симуляція VoIP в GNS3

- 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. № 4), тиснемо праву клавішу миші на Router c7200 та обираємо "Configure", переходимо на вкладку "Slots", та обираємо зі списку C7200-IO-2FE, тиснемо "OK";
- на головне поле переносимо "Cloud";
- тиснемо правою клавішею миші на "Cloud" та обираємо команду "Configure", тиснемо на "C1";
- в NIO Ethernet вибираємо наш "MSLoopBack", тиснемо "ADD" (рис. 5.1);

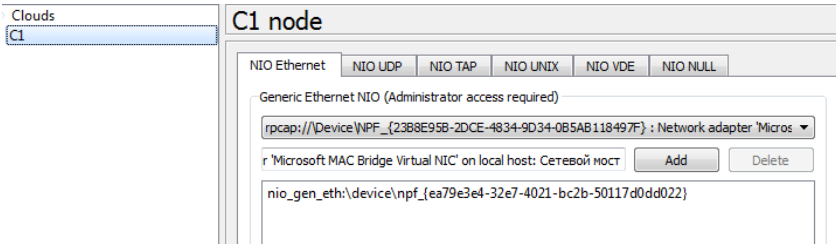


Рисунок 5.1 – Конфігурування "C1 node"

- тиснемо "Apply";
- зв'язуємо маршрутизатор та "Cloud" натиснувши на "Addlink – FastEthernet" (рис. 5.2);

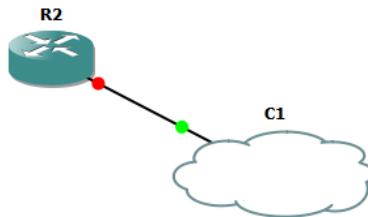


Рисунок 5.2 – З'єднання маршрутизатора та "Cloud"

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

– коли маршрутизатор готовий вводимо такі 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 нашу 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 СМЕ повинен приймати запити на підключення до нього телефонів)

```
auto assign 1 to 10
```

(Командою auto assign 1 to 10 ми говоримо роутеру, що хочемо, щоб він автоматично призначав підключеним телефонам лінії з номерами від 1 до 10)

– 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)

5.2.4 Перевіряємо результати

– Запускаємо Cisco IP Communicator, який встановили раніше. В результаті з'явиться такий телефон, зображений на рис. 5.3;

– тиснемо правою клавішею миші на ньому і 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 СМЕ, авторизується там і виглядатиме як показано на рис. 5.4.



Рисунок 5.3 – 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 5.4 – 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.

5.3 Зміст звіту

- 5.3.1 Титульний лист.
- 5.3.2 Мета роботи.
- 5.3.3 Описати переваги та недоліки технології VoIP.
- 5.3.4 Основні етапи моделювання VoIP в GNS3

5.4 Контрольні питання

- 5.4.1 Технологія VoIP. Які протоколи в ній використовуються?
- 5.4.2 Мовний сигнал. Опишіть передачу мови в цифровій формі.
- 5.4.3 Що лежить у основі кодека мови зі змінною швидкістю?
- 5.4.4 Опишіть фрагменти сигналу що класифікуються як активна мова, як пауза.
- 5.4.5 Для чого використовується Cisco IP Communicator?
- 5.4.6 Опишіть створення loopback інтерфейсу в Windows XP.

ЛАБОРАТОРНА РОБОТА № 6

ПРОТОКОЛ MPLS

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

6.1 Теоретичні відомості

MPLS – це багатопротокольна комутація по мітках. Вона частково замінює ір-маршрутизацію – рішення про пересилку пакету (витікаючий інтерфейс і наступний хоп маршруту) приймається не на основі полів ір-заголовка (зазвичай адреса призначення) і таблиці маршрутизації, а на основі міток, які прикріплені до пакету. Такий підхід прискорює процес пересилки, тому що пошук наступного хопу 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 обробки 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 по MPLS пакетам. Будь-які дії, засновані на мережевому рівні, мають бути зроблені 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, якщо він не був би маркований. Шлях комутації по мітці забезпечує передачу даних на вихід хмари MPLS. Вживання MPLS ґрунтуються на базовій концепції шляху комутації по мітці LSP (label switching path).

Коли мітка прикріплюється до пакету, вона збільшує його довжину на 32 біта (4 байти). Ці 32 біта розділяються так:

- сама мітка (20 біт);
- EXP експериментальне поле (3 біта);
- час життя (8 біт);
- вершина стека (1 біт);

Експериментальне поле не визначене стандартом, але використовується. Воно дозволяє розрізнити 8 типів трафіку. MPLS працює з класами еквівалентності при пересилці (forwarding equivalence class – FEC). Приклади класів FEC: Безліч пакетів з однаковою мережею призначення, безліч пакетів з однаковою мережею призначення і однаковою мережею джерелом, безліч пакетів з однаковими портами призначення і так далі.

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, отже, може бути оброблений залежно від FEC. Саме цією властивістю MPLS вносить принципово нову якість до сучасних мережевих технологій.

6.2 Конфігурація та моделювання мережі з протоколом MPLS в GNS3

- запускаємо програму GNS3;
- створюємо новий проект;
- в лабораторній роботі використовуємо Router c3600 та відповідно c3640-jk9s-mz.124-16.bin;
- перетягуємо на головне поле три екземпляри Router c3600.
- кожен маршрутизатор має такі характеристики (тиснемо 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 6.1:



Рисунок 6.1 – 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 роутера R2 та натиснути ОК.

– 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 ехо-запиту “Echo (ping) request”, в нижній частині вікна має бути заголовок MPLS “MultiProtocol Label Switching Header” (рисунк 6.2):

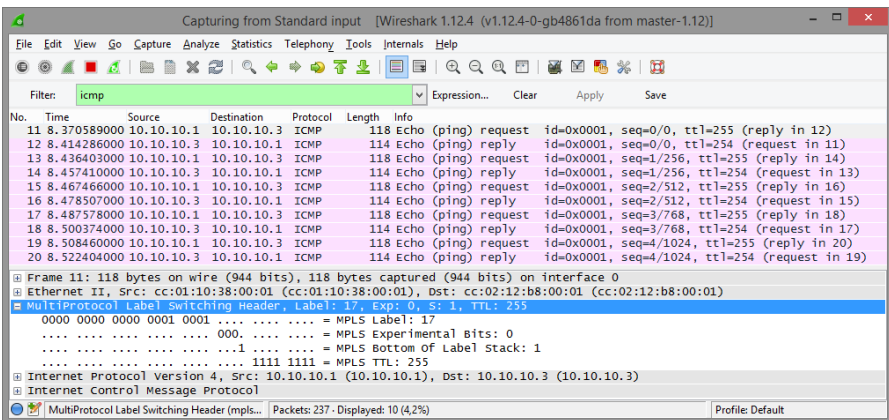


Рисунок 6.2 – Перевірка наявності заголовка MPLS

6.3 Вміст звіта

6.3.1 Титульний лист.

6.3.2 Мета роботи.

6.3.3 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
```

6.3.4 Статистика з маршрутизаторів R2 та R3, зібрана за допомогою наступних команд:

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

6.4 Контрольні питання

6.4.1 Переваги технології MPLS.

6.4.2 Які протоколи входять у MPLS?

6.4.3 Основні команди налаштування MPLS-маршрутизаторів.

6.4.4 Чи використовуються таблиці маршрутизації в MPLS-маршрутизаторах?

ЛАБОРАТОРНА РОБОТА № 7

Конфігурування ір-телефонії з використанням ір-телефонів та cisco ip communicators.

Мета роботи: змодельовати та конфігурувати мережу та налаштувати ір-телефонію.

7.1 Побудова моделі мережі

7.1.1. Запустіть Packet Tracer.

7.1.2. Зберіть мережу за схемою, представленою на рисунку 7.1, з основними параметрами комутаційного обладнання та інтерфейсів (табл. 7.1). 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 (див. рисунок 7.2).

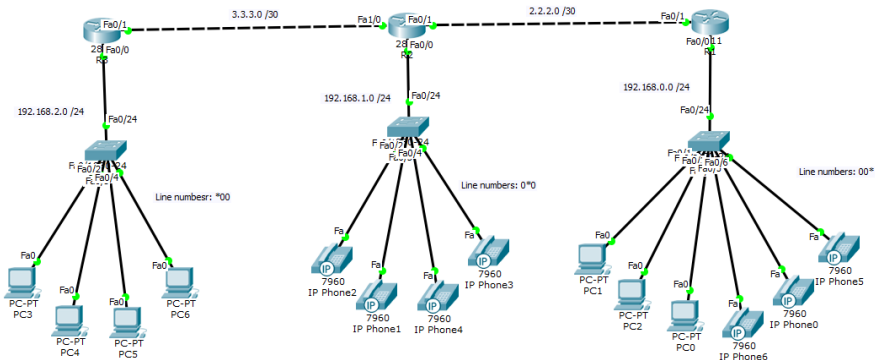


Рисунок 7.1 – Модель мережі

Додайте 7 комп'ютерів 7 ір-телефонів і з'єднайте їх з комутатором 2950-24, а комутатори з'єднайте з відповідними роутерами згідно з рисунком 7.1 (комп'ютери та телефони знаходяться

в розділі End Devices). Для маршрутизатора R2 необхідно встановити NM-2FE2W модуль як показано на рис 7.3.

Таблиця 7.1 – 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

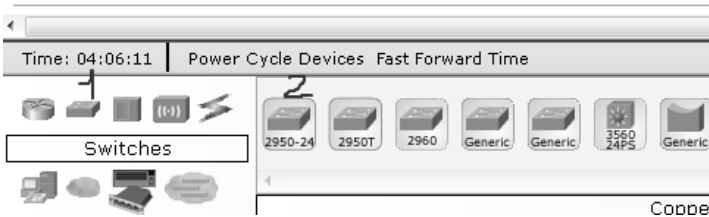


Рисунок 7.2 – Панель обладнання

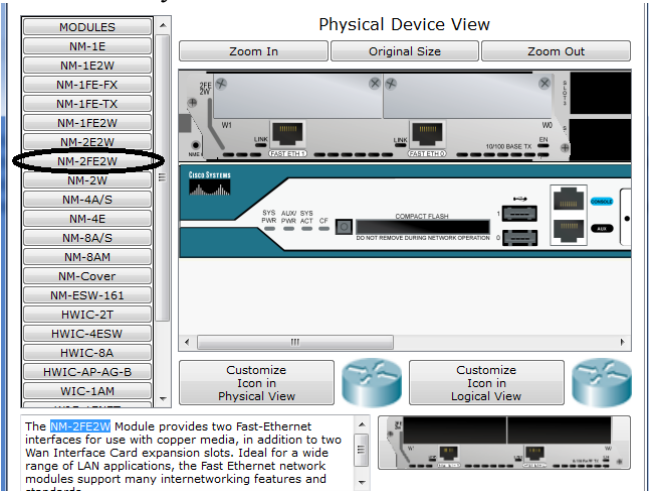


Рисунок 7.3 – Встановлення модуля на R2

7.2 Налаштування коммутаторів

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
```

7.3 Налаштування маршрутизаторів

Спочатку конфігуруємо 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 7.4) та підключаємо живлення до ір-телефонів (рис 7.5). Після цього всі робочі станції та ір-телефони повинні отримати ір-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)#
```

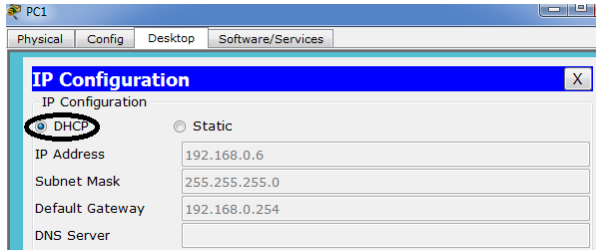


Рисунок 7.4 – Встановлення режиму dhcp

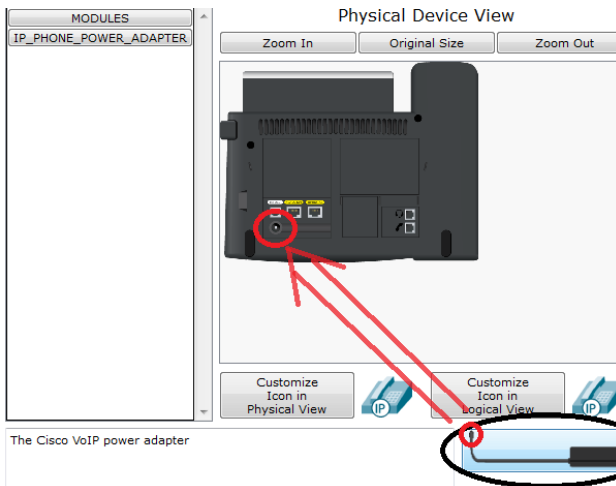


Рисунок 7.5 – Підключення живлення до телефону

Переходимо до конфігурування ір 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 номер (рис 7.6 та рис 7.7).



Рисунок 7.6 – Отримання номеру лінії на ір-телефоні



Рисунок 7.7 – 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 скофігурувати 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 знаходження пакетів між мережами. Далі необхідно налаштувати зв'язок між телефонами та комунікаторами з різних мереж. Для цього необхідно виконати наступні команди на роутерах. Для встановлення зв'язку 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 номери лінії на роутері R2 дорівнюють 010, 020, 030 і т.д. Відповідно для роутера R2 цей параметр дорівнює "00.", бо номери 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 кожную
рис. 7.8 та рис 7.9

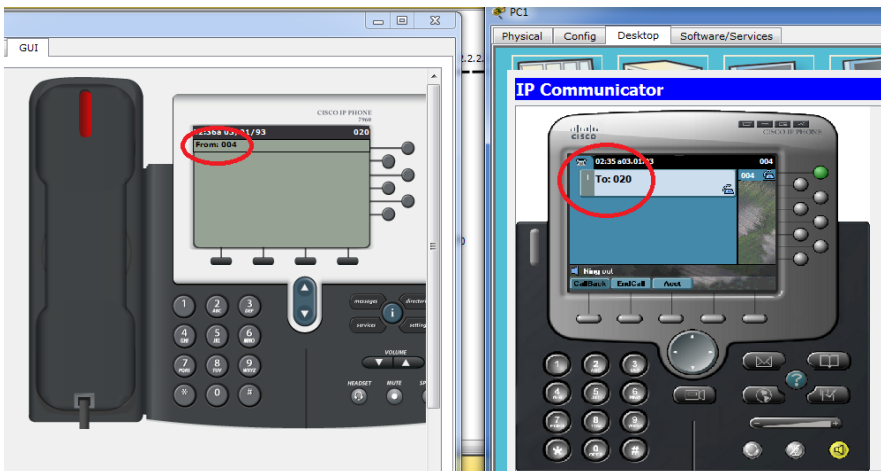


Рисунок 7.8 – Перевірка коректності налаштування

7.4 Симуляція передавання пакетів

Після перевірки зв'язку, для перегляду структури пакетів, що курсують між телефонами, необхідно провести симуляцію та відфільтрувати діючі протоколи та залишити тільки протокол RTP (рис 7.10).

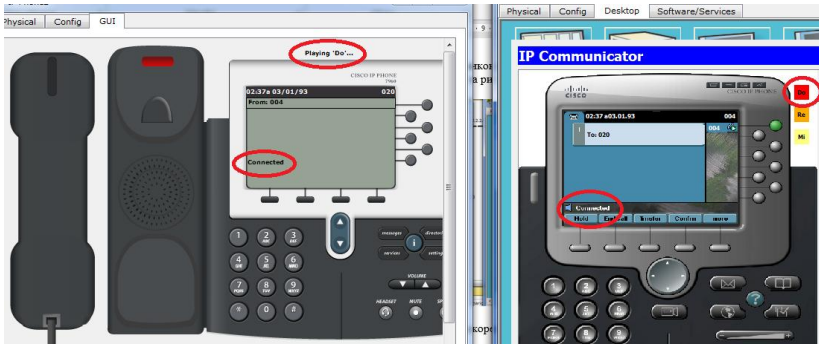


Рисунок 7.9 – Перевірка коректності налаштування

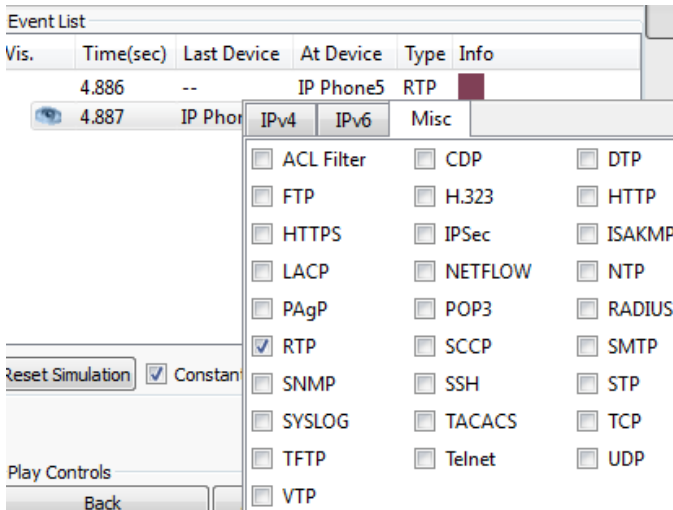


Рисунок 7.10 – Вікно симуляції передачі пакету

Натискаючи на кнопку caption forward ми почнемо пересування пакету по мережі. Вміст пакету, що сформований протоколом RTP, наведено на рис. 7.11.

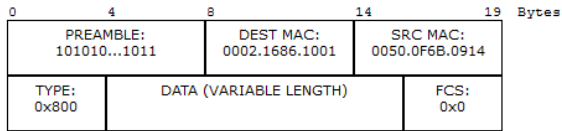
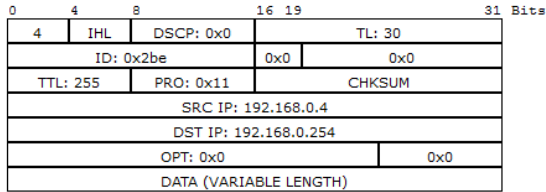
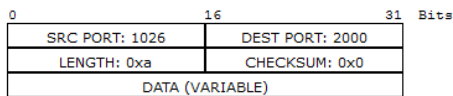
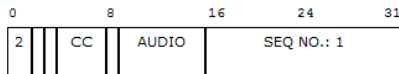
Ethernet IIIPUDPRTP

Рисунок 7.12 – Вміст пакету що сформований протоколом RTP

7.5 Індивідуальне завдання

1 варіант: під'єднати до маршрутизатора R1 ще один маршрутизатор з комутатором та двома ір-телефонами. Провести всі відповідні налаштування, щоб можливо було телефонувати з нової мережі в інші, та з інших мереж в нову.

2 варіант: під'єднати до маршрутизатора R3 ще один маршрутизатор з комутатором та двома робочими станціями. Провести всі відповідні налаштування, щоб можливо було дзвонити з нової мережі в інші, та з інших мереж в нову.

7.6 Вміст звіту

7.6.1 Титульний лист.

7.6.2 Мета роботи.

7.6.3 Структура створеної мережі.

7.6.4 Результати виконання роботи.

7.6.5 Структура пакетів, сформованих протоколом RTP.

ЛІТЕРАТУРА

1. Чернышов Ю.Н. NGN: принципы построения и организации / Ю.Н.Чернышов. – М. : Эко–Трендз, 2008. – 400 с.
2. Захватов. Построение виртуальных частных сетей (VPN) на базе технологии MPLS / Захватов. – М. : Cisco Systems, 2005. – 52 с.
3. Олвейн В. Структура и реализация современной технологии MPLS / В. Олвейн. – М. : Вильямс, 2004. – 480 с.
4. Филимонов А. Ю. Построение мультисервисных сетей Ethernet / А.Ю. Филимонов. – СПб. : БХВ-Петербург, 2007. – 592 с.
5. Гольдштейн А.Б. SOFTSWITCH / А.Б. Гольдштейн, Б.С. Гольдштейн. – СПб. : БХВ, 2006. – 368 с.
6. Reagan, J. Cisco CCIP MPLS Study Guide / James Reagan. – Sybex, 2002. – 486 с.
7. Бакланов И.Г. NGN: принципы построения и организации. – М. : эко-трендз, 2008. – 400 с.
8. Глотиков К. IMS (IP multimedia Subsystem). М. : Эко-трендз. 2009. – 100 с.
9. Гольдштейн Б.С. Сети связи. Учебник для вузов / Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский. – СПб. : БХВ, 2009. – 400 с.