МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Корпоративні мережі з підтримкою протоколу IPv6»

Завідувач випускаючої кафедри **Довбиш А.С.**

Керівник роботи **Великодний Д.В.**

Студента групи ІНдн – 62с **Спічак О.В**

СУМИ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних наук

Затверджую_____

Зав. кафедрою Довбиш А.С.

"_____"_____2020 р.

ЗАВДАННЯ

до випускної роботи

Студента четвертого курсу, групи ІНдн-62с спеціальності "Інформатика" дистанційної форми навчання Спічака Олексія Васильовича

Тема: " Корпоративні мережі з підтримкою протоколу IPv6"

Затверджена наказом по СумДУ

№_____ від _____2020 р.

Зміст пояснювальної записки: 1) Аналітичний огляд технології IPv6; 2) Поставнока задачі; 3)Огляд симуляторів комп'ютерних мереж; 4) Моделювання у Cisco Packet Tracer 7 корпоративної мережі;

Дата видачі завдання "_____"_____2020 р.

Керівник випускної роботи _____Великодний Д.В.

Завдання прийняв до виконання _____Спічак О.В.

РЕФЕРАТ

Записка: 58 стор., 44 рис., 32 джерел.

Об’єкт дослідження – Internet protocol IPv6.

Предмет дослідження – особливості роботи та налаштування корпоративної мережі з підтримкою протоколу IPv6.

Мета роботи – створення та налаштування корпоративної мережі з підтримкою протоколу IPv6 у симуляторі Cisco Packet Tracer 7.

Методи дослідження – моделювання мережі на базі протоколу IPv6 у симуляторі Cisco Packet Tracer 7.

Результати – у результаті роботи, на базі протоколу IPv6, було створено корпоративну мережу, з’єднану між собою міднім дротом «вита пара». Мережа була поділена між трьома роутерами, за допомогою яких став можливий розділ мережі на три незалежних один від одного сегмента мережі. Завдяки налаштуванню роутерів, мережі між собою змогли обмінюватись інформацією. Другим етапом було використання «access-list» для обмеження доступу у окрему мережу, з пристроїв, котрі не мають права туди потрапляти. В результаті було отримано діючу корпоративну мережу з обмеженим доступом до окремих сегментів мережі. Виконавши процес створення мережі доведено, що такий вид мережі є зручним та простим у користуванні для побудови та використанні у різних корпоративних рішеннях.

ЗМІСТ

ВСТУП

Базовим завданнями протоколів 3-го рівня моделі OSI (протоколів L3) є адресація різноманітних пристроїв у мережах та визначення шляху пересування – маршрутизація – пакетів між ними. Адресація полягає в призначенні унікального ідентифікатора, – адреси – кожному з пристроїв мережі, кількість яких може сягати від десятків для малих офісів, сотень та тисяч для середніх підприємств до мільярдів, якщо мова йде про всесвітню мережу Інтернет.

Маршрутизація здійснюється шляхом покрокової передачі пакетів між проміжними пристроями – маршрутизаторами – для наближення до кінцевого пункту – пристрою призначення. Загальна кількість пристроїв, під'єднаних до мережі Інтернет, має чітку тенденцію до зростання, тому до протоколів L3 ставиться вимога забезпечення можливості адресації та маршрутизації в мережах підприємств дедалі більшого обсягу.

Обмежені можливості адресації протоколу IPv4 стали очевидними вже в 1994 році. Це призвело до початку розробки нового протоколу L3 – IPv6, характеристики якого вважаються цілком достатніми для забезпечення потреб адресації в глобальній мережі Інтернет та в локальних мережах великих підприємств сьогодні і в найближчому майбутньому. Тому перехід до нового протоколу без «обмежень», які є у четвертій версії, стає все актуальнішим в корпоративних мережах підприємств різних рівнів.

У роботі розглянута можливість роботи та виконане модулювання мережі у додатку Cisco Packet Tracer на базі протоколу L3 – IPv6 з можливістю використання цієї схеми у подальшій роботі локальної мережі підприємства.

1. ПРОБЛЕМА ОБМЕЖЕННЯ АДРЕСНОГО ПРОСТОРУ

1.1 Обмеження адресного простору

IPv6 протокол завдячує своєю появою істотним обмеженням, з якими зіткнувся його попередник IPv4. Найчастіше серед цих обмежень зазначають такі [1]:

1) нестача адрес для глобальної адресації;

2) складність заголовка пакетів, яка підвищує складність його аналізу в пристроях;

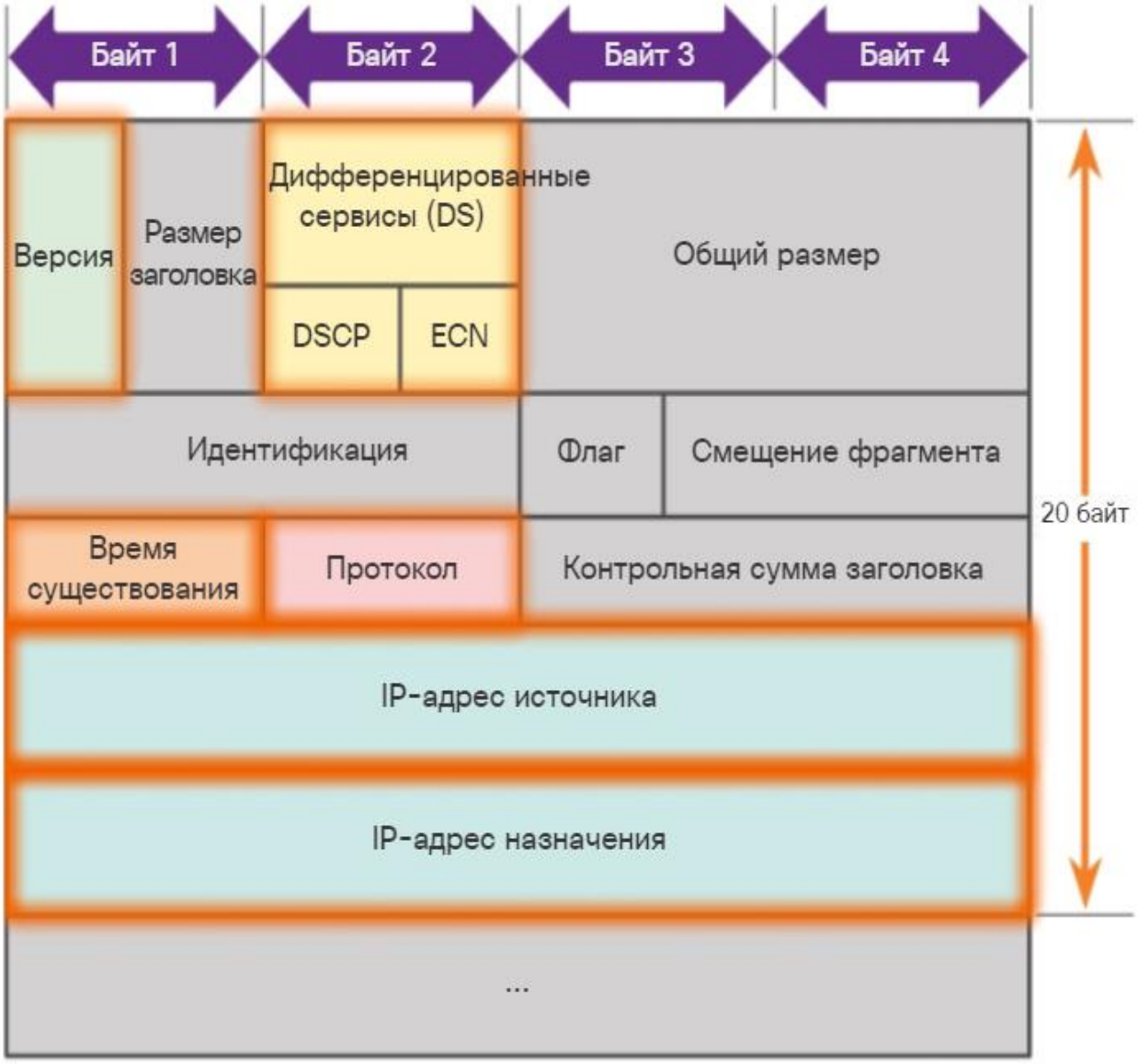

Рисунок 1.1 - Заголовок пакета IPv4 [2]

3) відсутність інтегрованих засобів для забезпечення якості обслуговування Quality-of-Service (QoS);

Рисунок 1.2 - Quality-of-Service [3]

4) відсутність інтегрованих засобів для захисту даних, які передаються, опціонально застосування технології IPSec [4];

5) використання фрагментації «на шляху» передачі пакетів у разі, коли їх розмір перевищує максимум, підтримуваний транзитним пристроєм.

Усунення зазначених вище обмежень вважають ключовими перевагами протоколу IPv6. Але не тільки нестача унікальних IP-адрес виявилась проблемою, яка мала непереборний характер.

Апаратна реалізація обробки пакетів та використання багатопротокольної комутації Multiprotocol Label Switching (MPLS) знизили вплив складності заголовків на навантаження центральних процесорів пристроїв. Сумісне використання з IPv4 додаткових технологій захисту даних, як IPSec, та забезпечення QoS, особливо з апаратною підтримкою, знизило критичність відсутності відповідних інтегрованих засобів в IPv4.

Технологія автоматичного визначення максимального розміру пакету на повному шляху передачі – Path MTU Discovery [5], дозволила позбуватися фрагментації пакетів.

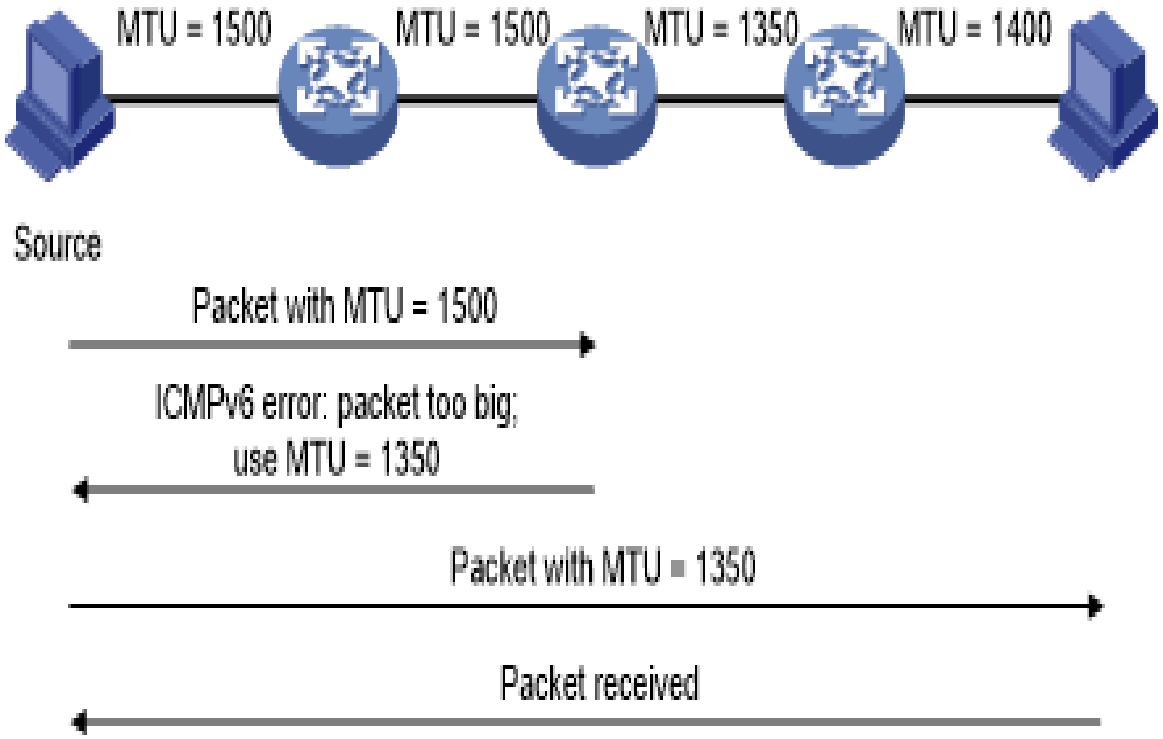

Рисунок 1.3 - MTU Discovery[6]

Як захід для уповільнення швидкості вичерпання адрес IPv4 значного поширення набула технологія підміни мережевих адрес – Network Address Translation (NAT).

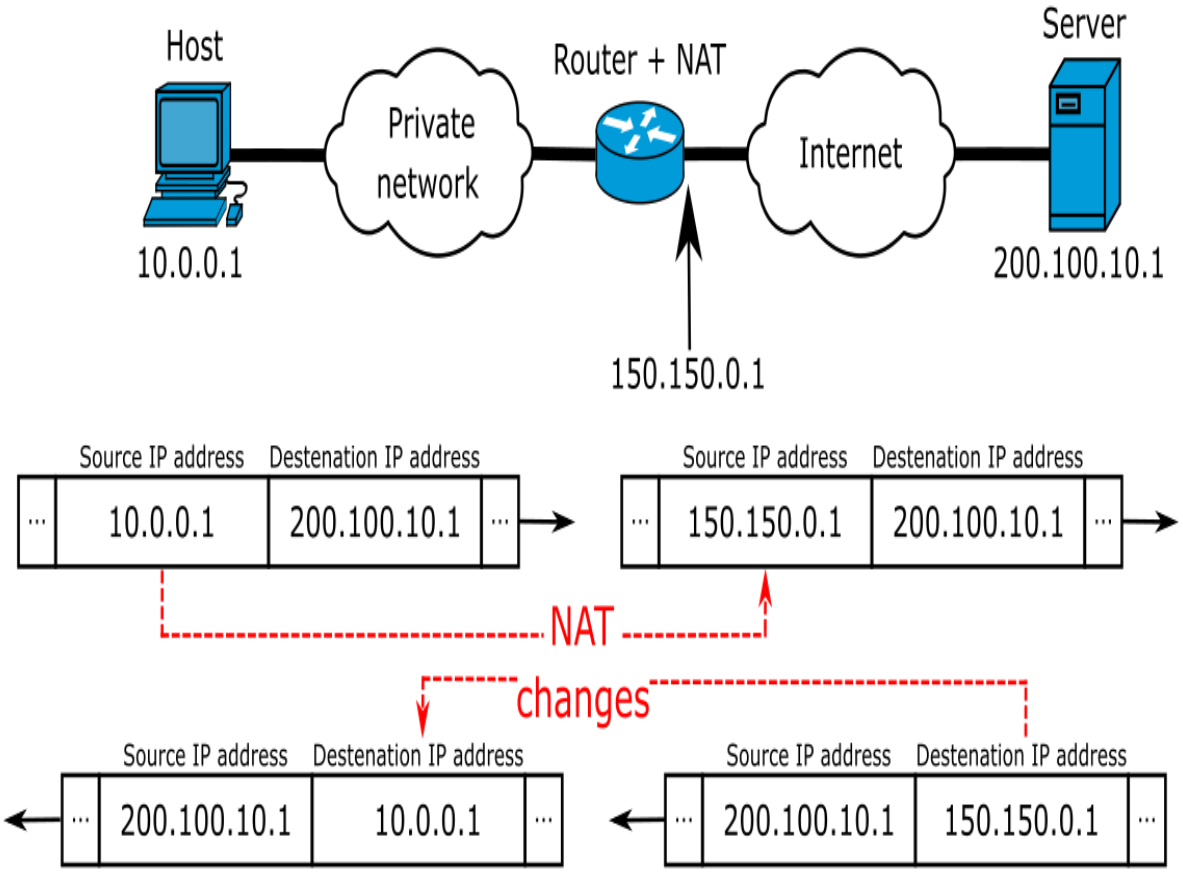

Рисунок 1.4 - Network Address Translation [7]

Утім, відсутність NAT в IPv6 і забезпечення прозорої двобічної передачі пакетів між пристроями, що взаємодіють, не варто вважати самостійною перевагою IPv6 перед IPv4, оскільки поява NAT була зумовлена обмеженими можливостями адресації в IPv4. Додатковими перевагами IPv6 також вважають зокрема:

6) автоматичне самоналаштування адрес пристроїв без використання додаткових процесів типу DHCP – Stateless Address Autoconfiguration (SLAAC);

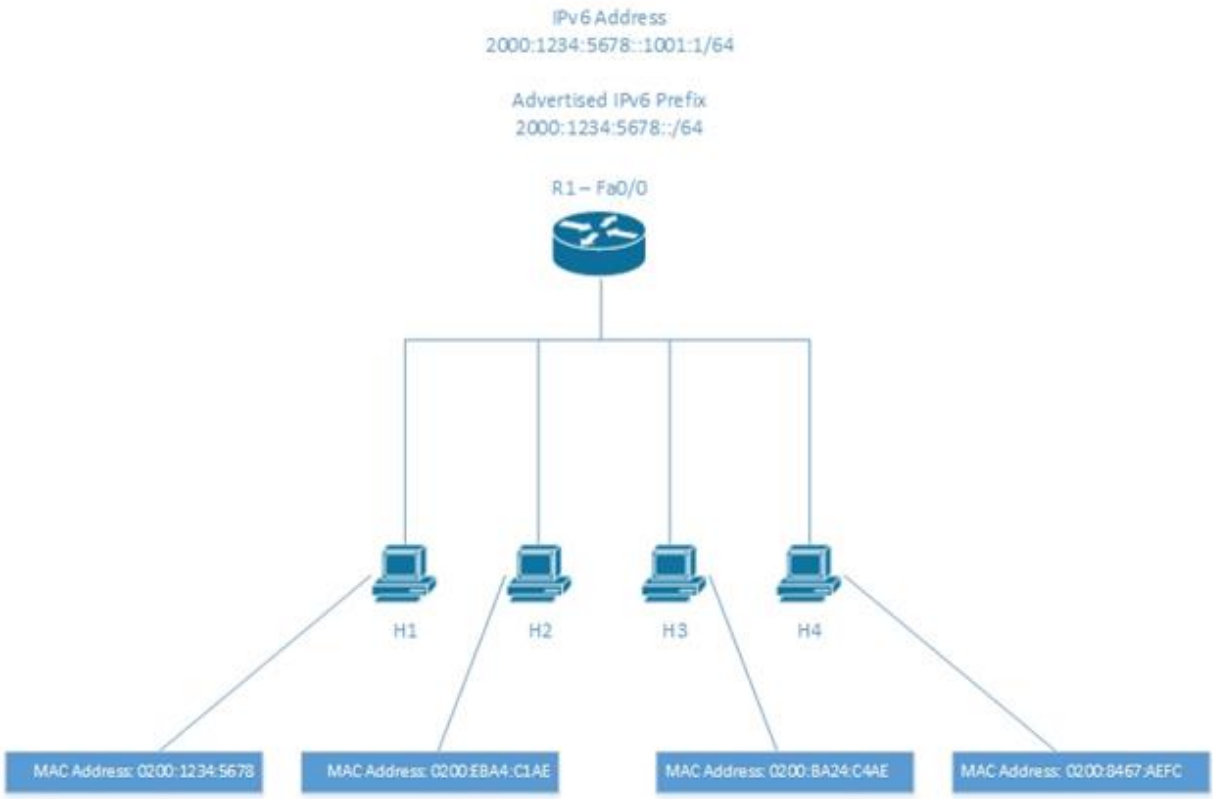

Рисунок 1.5 - Stateless Address Autoconfiguration [8]

7) спрощення глобального розподілу адресного простору IPv6 за рахунок використання фіксованої довжини мінімального префікса мережі 48 біт замість гнучкого вибору довжини префікса згідно з методом Classless Interdomain Routing (CIDR) в IPv4;

IPv4 CIDR IP/CIDR	Δ to last IP addr	Mask	Hosts (*)	Class
a.b.c.d/32	+0.0.0.0	255.255.255.255	1	1/256 C
a.b.c.d/31	+0.0.0.1	255.255.255.254	2	1/128 C
a.b.c.d/30	+0.0.0.3	255.255.255.252	4	1/64 C
a.b.c.d/29	+0.0.0.7	255.255.255.248	8	1/32 C
a.b.c.d/28	+0.0.0.15	255.255.255.240	16	1/16 C

Рисунок 1.6 - Classless Interdomain Routing [9]

8) спрощення планування внутрішнього розподілу адресного простору локальних мереж. Це зроблено за рахунок використання для всіх її сегментів єдиної довжини префікса 64 біта (/64) замість змінної довжини маски згідно з методом Variable Length Subnet Mask (VLSM), який використовується в IPv4;

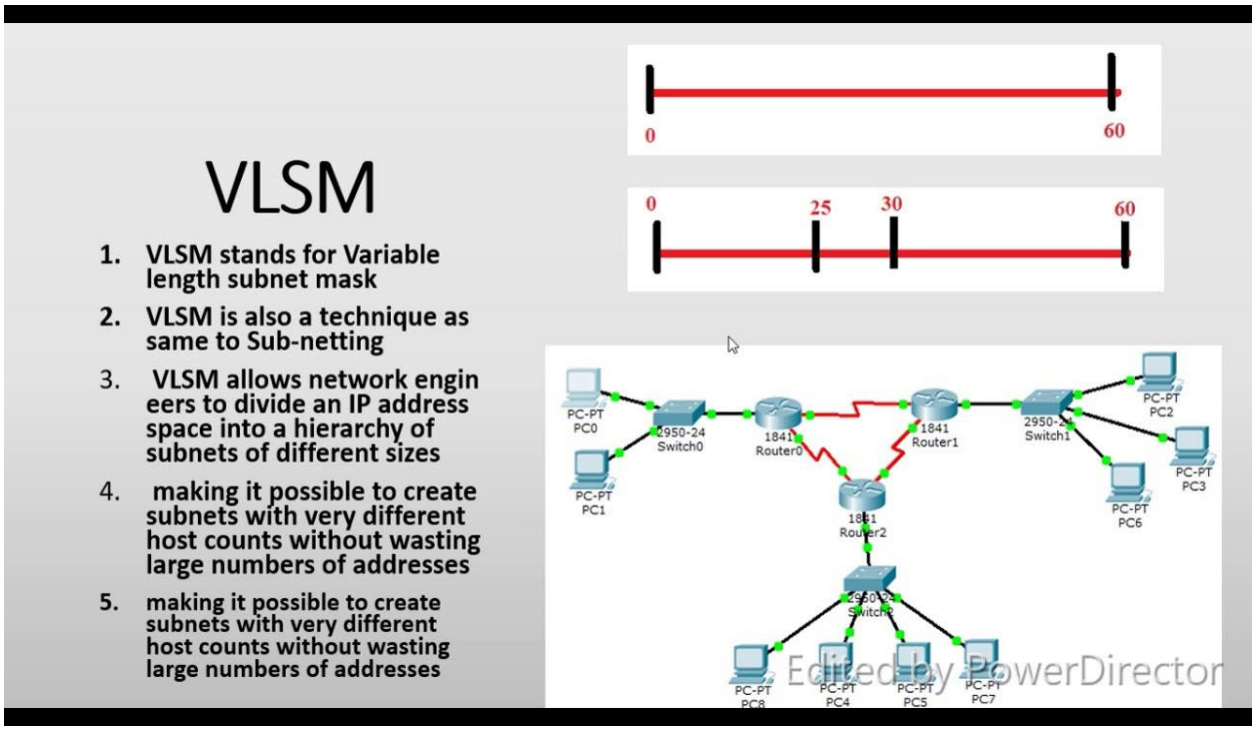

Рисунок 1.7 - Variable Length Subnet Mask [10]

9) активне використання локальних канальних (link local) адрес;

10) «anycast» адресація для взаємодії з будь-яким пристроєм групи (на відміну від адресації групової «multicast», яка передбачає взаємодію з усіма пристроями групи). Але зазначені переваги неможна визнати такими, що роблять впровадження IPv6 вкрай необхідним.

Зараз вже можна дійти висновку, що саме нестача адрес в IPv4 стала ключовим фактором, який прискорив початок реального використання IPv6 в мережі Інтернет. За рахунок використання 128-бітових адрес IPv6 забезпечує загальну кількість адрес на багато порядків більшу, ніж IPv4. Проте, можливості адресації в IPv6 не безкінечні, а особливості розподілу адрес IPv6 для глобальної адресації (global

unicast) ще більше обмежують загальну кількість пристроїв, яка може бути під’єднана до мережі [11]. До таких особливостей слід віднести такі:

11) стандартна довжина адресного префікса для кожного сегмента локальної мережі становить 64 біти (/64);

12) максимальна довжина адресного префікса для блоку адрес, який призначається локальній мережі, що має множину сегментів, становить 48 бітів (/48);

13) адреси для глобальної адресації виділяються з діапазону 2000::/3. Зважаючи на вказане, охарактеризувати наявний обсяг адрес глобальної маршрутизації можна як 245 локальних мереж (а не 2128 пристроїв, які можна під’єднати до мережі). Зростання обсягу використаних адрес IPv6 наразі має лінійний характер [12], при цьому здебільшого IPv6 впроваджується у вже існуючих мережах, які використовують IPv4. Створення мереж із виключним використанням IPv6 має дослідницький характер [13], але з початком їх масового використання (що є неминучим, оскільки адресний простір IPv4 уже вичерпано) темпи використання адрес IPv6 зростатимуть.

Зокрема, суттєве прискорення використання адрес IPv6 відбудеться з початком надання доступу до Інтернету по IPv6 для «retail» дрібних клієнтів – приватних помешкань та малих офісів. Окрім великої кількості користувачів зазначеної категорії, кожному з них окрім адреси для під’єднання до провайдера Інтернету – Internet Service Providers (ISP) – необхідно делегувати один чи декілька префіксів /64 для пристроїв локальної мережі цього користувача [14].

Значну додаткову кількість адрес потребуватиме впровадження архітектури мікросервісів, яка набуває дедалі більшої популярності [15]. Використання контейнерів для кожного з мікросервісів вимагатиме виділення одного чи декількох префіксів /64 для кожного кластеру. Певна втрата ефективності розподілу адрес IPv6 може статися внаслідок виділення великих адресних блоків континентальним (регіональним) інтернет-реєстрам – Regional Internet Registries (RIR).

Рисунок 1.8 - Regional Internet Registries [16]

Надлишкова витрата адрес IPv6 матиме місце внаслідок неоптимального їх використання підприємствами. Наприклад, у разі під'єднання локальної мережі підприємства до декількох ISP, оптимальним є використання власного мережевого префікса /48, який не залежить від конкретного ISP.

Однак, для спрощення конфігурації (усунення налаштування протоколу BGP з кожним ISP) підприємство може обрати сумісне використання префіксів /48 від кожного з провайдерів [4], що, вочевидь, є надлишковістю. Прискоренню зростання обсягу використаного адресного простору IPv6 сприятимуть новітні тренди, як-от Internet of Things (IoT) [17].

Рисунок 1.9 - Internet of Things (IoT) [18]

У майбутньому можлива поява нових технологій, які також потребуватимуть великих обсягів адрес.

Одночасно з наданням значного за обсягом адресного простору впровадження IPv6 призведе до збільшення обсягів оперативної пам'яті пристроїв, відведених для таблиць маршрутизації та інших, пов'язаних із ними структур даних, підвищення обчислювального навантаження для підтримки протоколів динамічної маршрутизації [BGP].

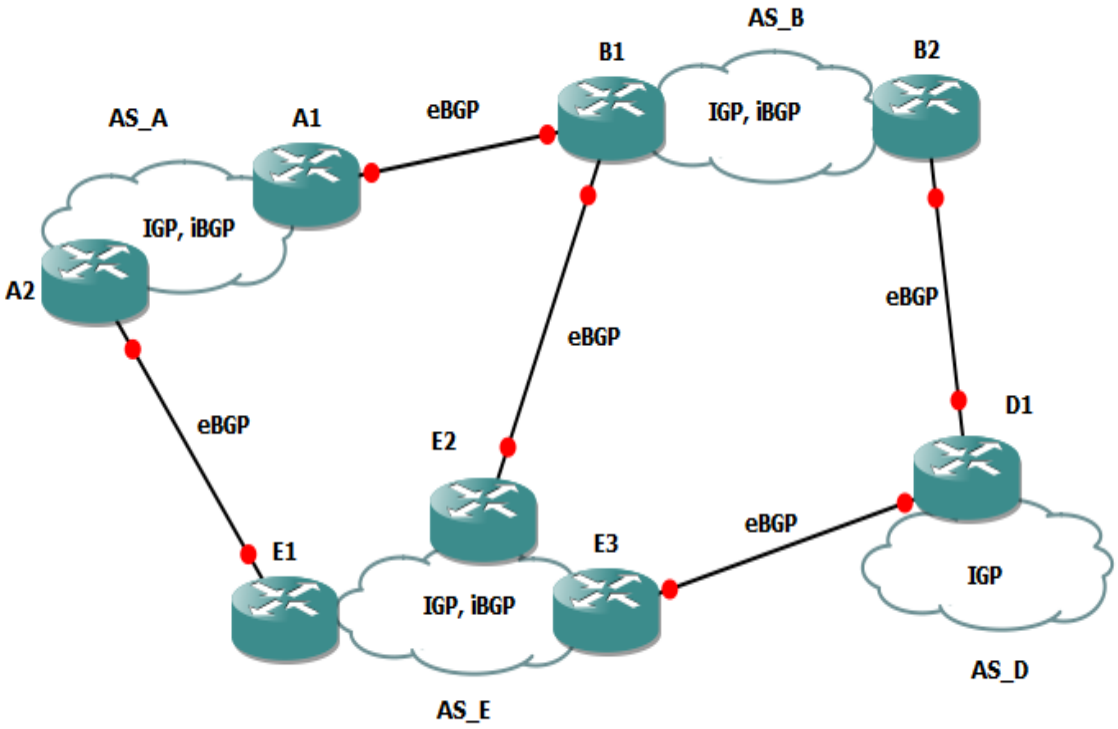

Рисунок 1.10 - Border Gateway Protocol [19]

Збільшення адресного простору призведе до розширення можливого фронту здійснення атак і ускладнення протидії їм. Оскільки протокол IPv6 справді суттєво розширює можливості адресації порівняно з IPv4, зазначені фактори дають підстави для дуже обережних оцінок щодо можливого терміну вичерпання адрес IPv6, а отже, обґрунтовують необхідність системного їх розподілу.

1.2 IPV6 стратегії впровадження протоколу

Несумісність IPv4 та IPv6 протоколів визначила неможливість поступового еволюційного переходу від одного до іншого. Оскільки революційний перехід шляхом одночасної заміни IPv4 на IPv6 також не є реальним, обидва протоколи будуть вимушені співіснувати принаймні протягом певного перехідного періоду. Упродовж зазначеного перехідного періоду IPv6, як вважається, має поступово замістити IPv4. Серед стратегій міграції від IPv4 до IPv6 протягом перехідного періоду найчастіше розглядають такі [20]:

1) тунелювання (інкапсуляція) – передача пакетів між мережами IPv6 через тунелі, які створюються в мережах IPv4;

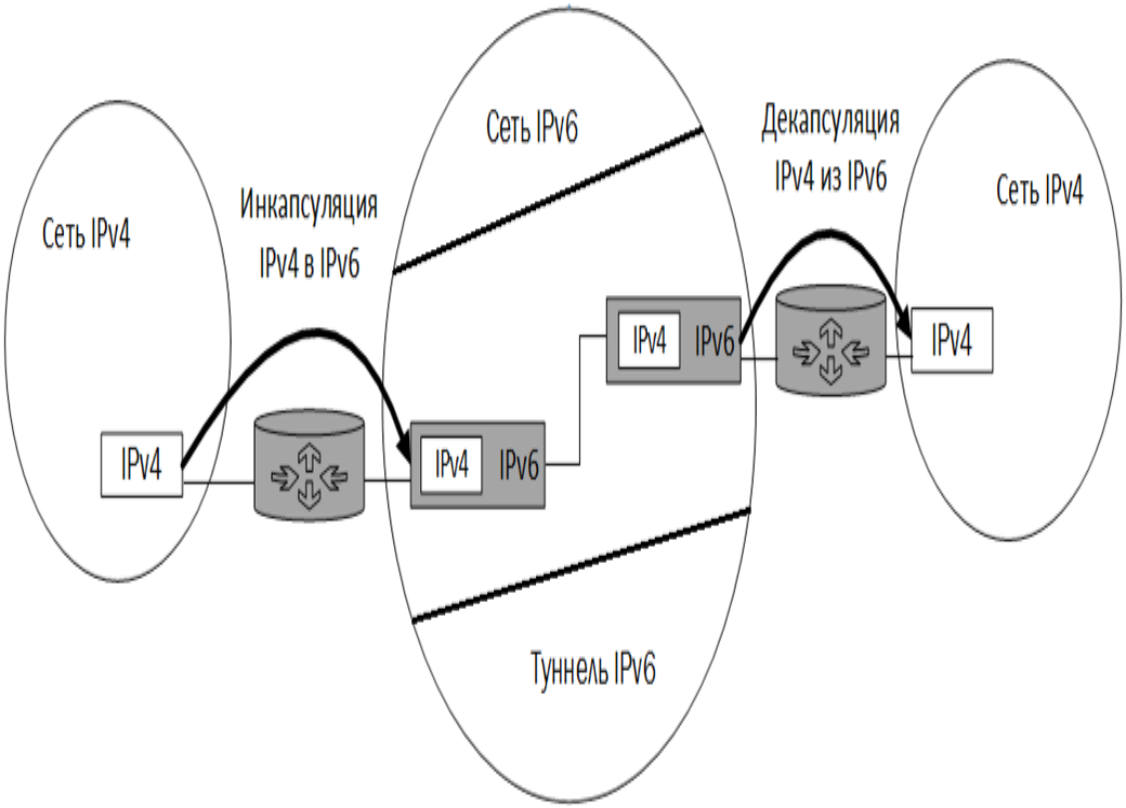

Рисунок 1.11 - Тунелювання пакетів [21]

2) перетворення (трансляція) пакетів між протоколами – Network Address Translation (NAT64);

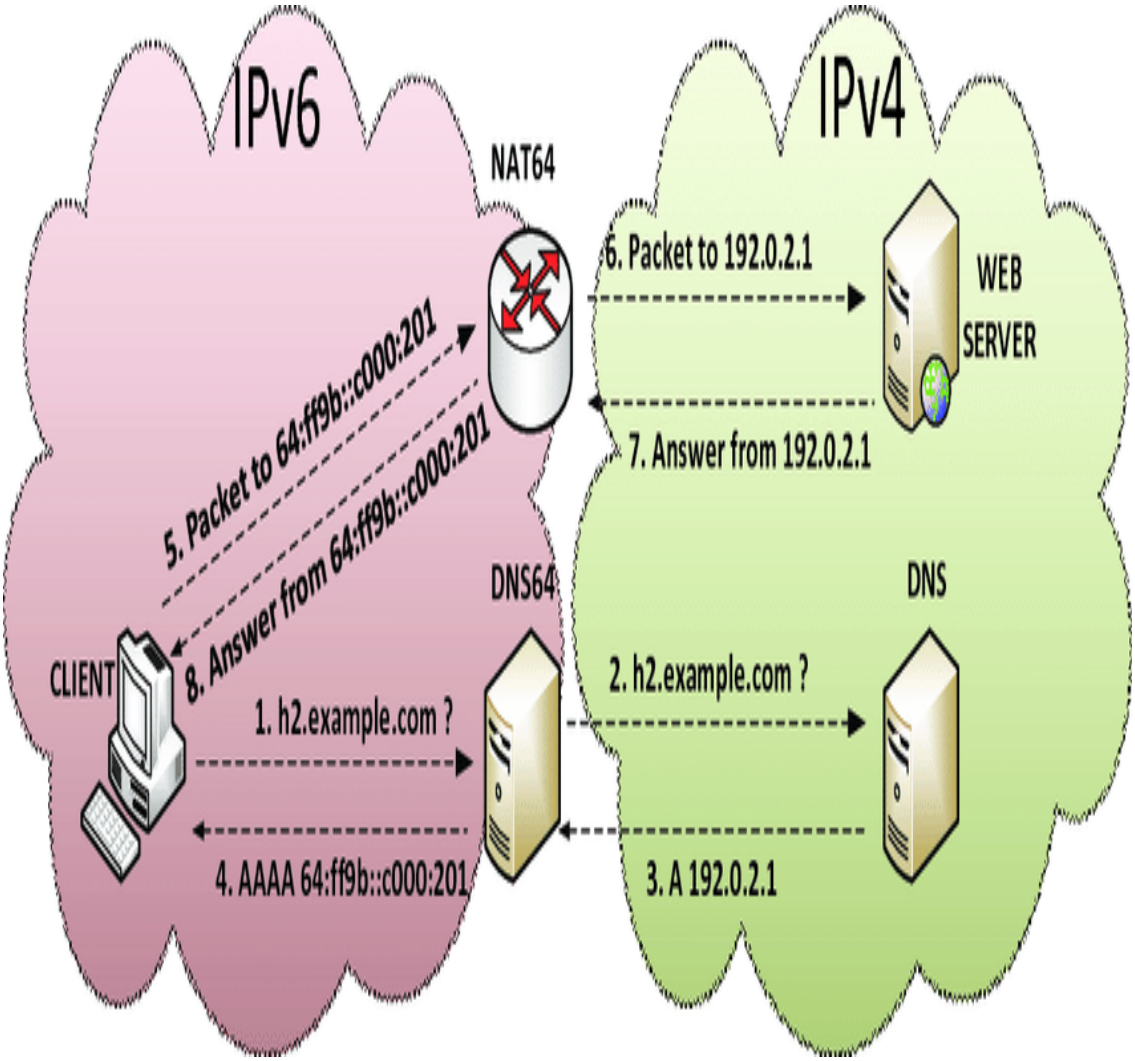

Рисунок 1.12 - Network Address Translation (NAT64) [22]

3) подвійний стек – одночасна підтримка пристроями обох протоколів із переважним використанням IPv6. Тунелювання забезпечує транспортування пакетів між мережами IPv6 у випадку, якщо між цими мережами не існує з'єднання з підтримкою IPv6. Цей захист не забезпечує можливості взаємодії між пристроями, що підтримують різні протоколи. Технологія NAT має декілька різновидів [23] і призначена для забезпечення взаємодії пристроїв з підтримкою різних протоколів, але така взаємодія має обмежену функціональність [24].

Повну функціональність забезпечує лише взаємодія в межах одного протоколу. Отже, лише підтримка пристроями подвійного стеку – IPv4 та IPv6, єдина забезпечує повноцінну взаємодію з будь-якими пристроями, які підтримують лише один із протоколів.

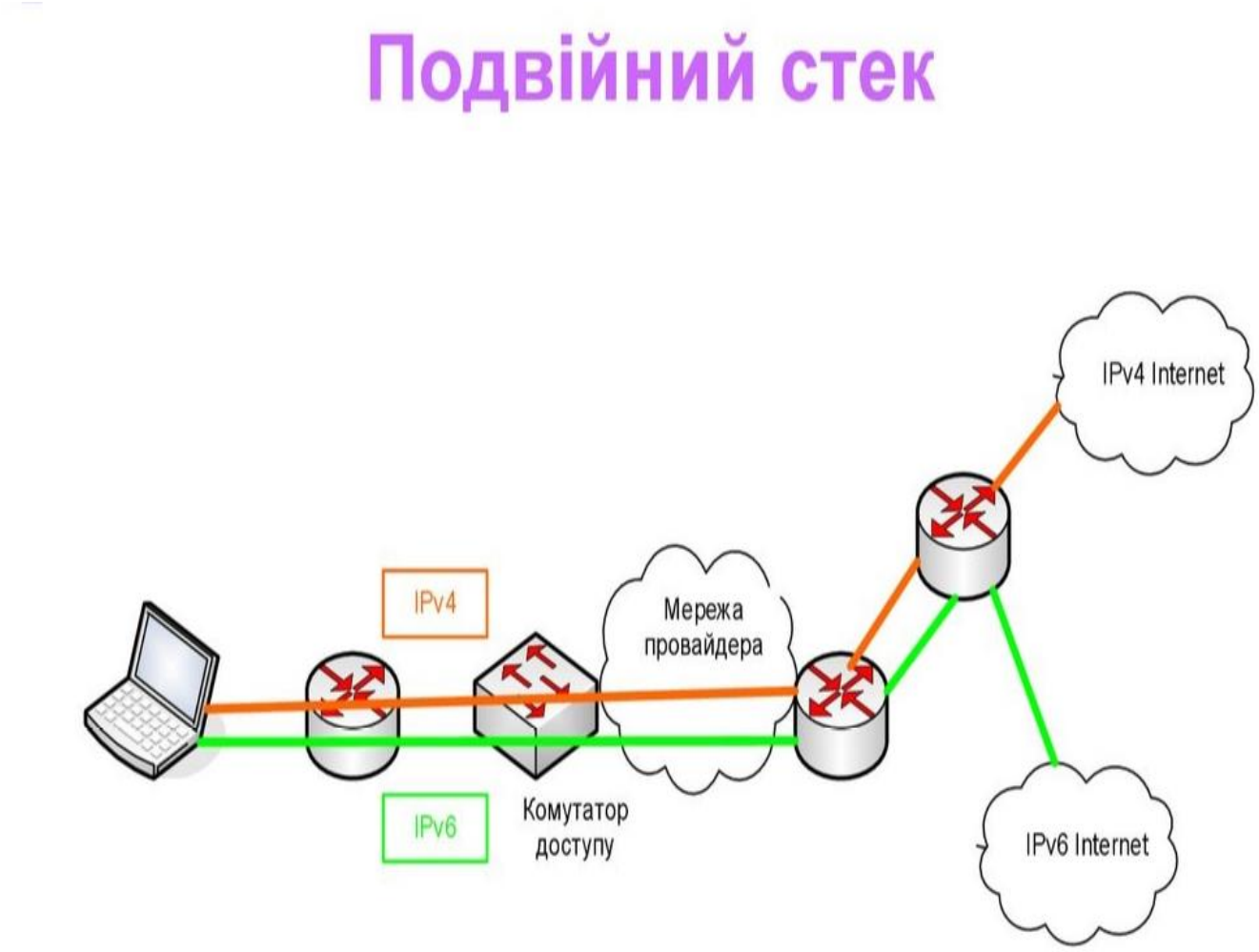

Рис 1.13 - Подвійний стек [25]

1.3 Потреби в підтримці протоколу IPV4 та IPV6

Інтернет – глобальна мережа обміну інформацією. Для аналізу особливостей використання в Інтернеті протоколів IPv4 та IPv6 (які за визначенням є базовими протоколами Інтернету) застосуємо поняття інтернет-об'єктів (далі – «об'єкти»), які беруть участь в інформаційному обміні. Серед об'єктів в мережі Інтернет можна виділити такі класи:

1. Інформаційні ресурси (далі – «ресурси»), які надають інформацію в різних форматах за запитом.

2. Запитувачі, які звертаються із запитами до ресурсів.

3. Партнери за симетричною (peer-to-peer) взаємодією (далі – «партнери»).

4. Компоненти транспортної інфраструктури, які здійснюють транзитну передачу інформації. Як будьяка мережа, Інтернет утворена пристроями і каналами зв'язку між ними. Пристрої можуть мати апаратну або програмну (зокрема віртуальну) реалізацію. Об'єкт є ширшим поняттям, ніж пристрій. Приклади об'єктів наведено нижче.

Ресурс:

1) сайт, який може мати у своєму складі низку серверів, організованих у вигляді кластеру, або територіально рознесених для балансування навантаження та забезпечення високої доступності, а також мережа доставки вмісту – Content Delivery Network (CDN);

2) група серверів доменної системи імен – Domain Name System (DNS), які здійснюють підтримку певних доменів або тимчасове проміжне збереження інформації DNS – кешування (caching).

Запитувач:

1) мережа офісу або житлового будинку, яка об'єднує в собі множину кінцевих користувачів, що здійснюють запити до ресурсів;

2) сервери-посередники (proxy), які здійснюють запити до ресурсів за дорученням користувачів.

Партнери:

1) сукупності прикордонних маршрутизаторів мереж підприємств, які обмінюються інформацією про маршрутизацію за протоколом Border Gateway Protocol (BGP);

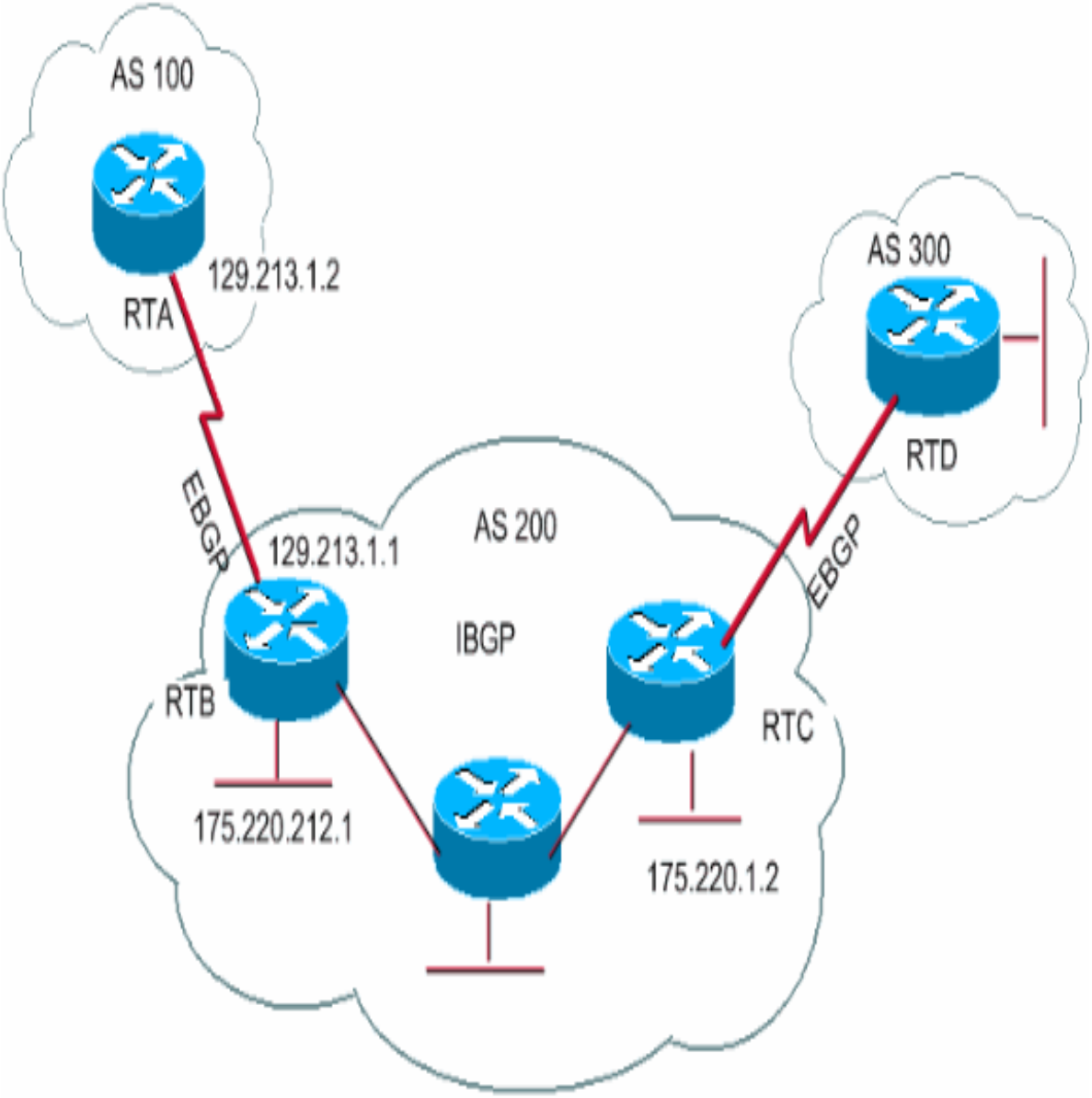

Рисунок 1.15 - Border Gateway Protocol [26]

2) сервери електронної пошти, які передають між собою електронні листи;

3) вузли керування телефонними викликами в IP-телефонії. Компоненти транспортної інфраструктури;

4) транспортні мережі провайдерів, створені за технологією MPLS;

5) магістральні транспортні мережі Інтернет, які утворюються сукупністю транспортних мереж низки провайдерів;

6) мережа глобального зв'язку – World Area Network (WAN), яка поєднує в корпоративну мережу територіально рознесені компоненти підприємства. Для створення об'єкта використовуються один чи декілька пристроїв. Кожен пристрій може входити до складу одного чи декількох об'єктів (наприклад, у разі створення декількох інформаційних ресурсів на одному сервері). Кожен обмін інформацією в Інтернеті передбачає участь об'єктів двох типів:

1) кінцеві об'єкти – ті, що, власне, обмінюються інформацією між собою;

2) проміжні об'єкти – ті, що здійснюють підтримку передачі інформації між кінцевими об'єктами. Як кінцеві об'єкти виступають ресурси, запитувачі, партнери.

Проміжні об'єкти є компонентами транспортної інфраструктури. Очевидно, що обов'язковою умовою для можливості взаємодії кінцевих пристроїв є підтримка єдиного спільного протоколу – IPv4 або IPv6. У разі, якщо підтримуються обидва протоколи, використовується один з них. Згідно з рекомендаціями Ради з архітектури Інтернету (Internet Architecture Board (IAB)), на сьогодні IPv6 є пріоритетним протоколом [27], отже, у разі підтримки обох протоколів, перевагу слід віддати IPv4. Так само очевидно, що протокол, обраний для взаємодії кінцевих об'єктів, має підтримуватися проміжними об'єктами, які безпосередньо контактують із зазначеними кінцевими об'єктами.

Для інших проміжних об'єктів підтримка протоколу взаємодії кінцевих об'єктів не є обов'язковою. У випадку, якщо такої підтримки немає, передача інформації

можлива, наприклад, через тунель, кінці якого розташовані на проміжних об’єктах, які контактують із кінцевими об’єктами.

Проміжні об’єкти, через які передається інформація між кінцевими об’єктами, мають задовольняти вимогу: проміжні об’єкти, які безпосередньо контактують між собою, повинні підтримувати єдиний спільний протокол. Відповідно, у випадку, якщо частина проміжних об’єктів, що здійснюють передачу інформації між кінцевими об’єктами, не підтримує протокол, що використовується кінцевими об’єктами, на шляху передачі інформації повинні бути об’єкти, які підтримують обидва протоколи.

Ці об’єкти мають здійснювати тунелювання протоколу, що використовується кінцевими об’єктами, використовуючи як зовнішній протокол, що підтримується проміжними об’єктами. Ці тези ілюструють застосування стратегії впровадження IPv6 на основі тунелювання. Складність її використання визначається додатковими вимогами до проміжних об’єктів: підтримка протоколів і створення тунелів. Оскільки проміжні об’єкти в загальному випадку не перебувають під технічним контролем власників кінцевих об’єктів, ця стратегія є ненадійною.

1.4 Оптимальне співіснування IPV4 та IPV6 у мережі підприємства

Згідно з поширеною моделлю архітектури підприємства воно містить у собі територіально рознесені регіональні відділення, обмін інформацією між якими здійснюється через WAN [28]. Окремі відділення виконують роль головного офісу та дата-центру (можуть бути поєднані). Реалізація WAN здійснюється у вигляді проміжного об’єкта рівня L2 або L3 у разі, якщо всі відділення під’єднані до єдиного провайдера передачі даних, або у вигляді захищених тунелів – Virtual Private Network (VPN) через Інтернет.

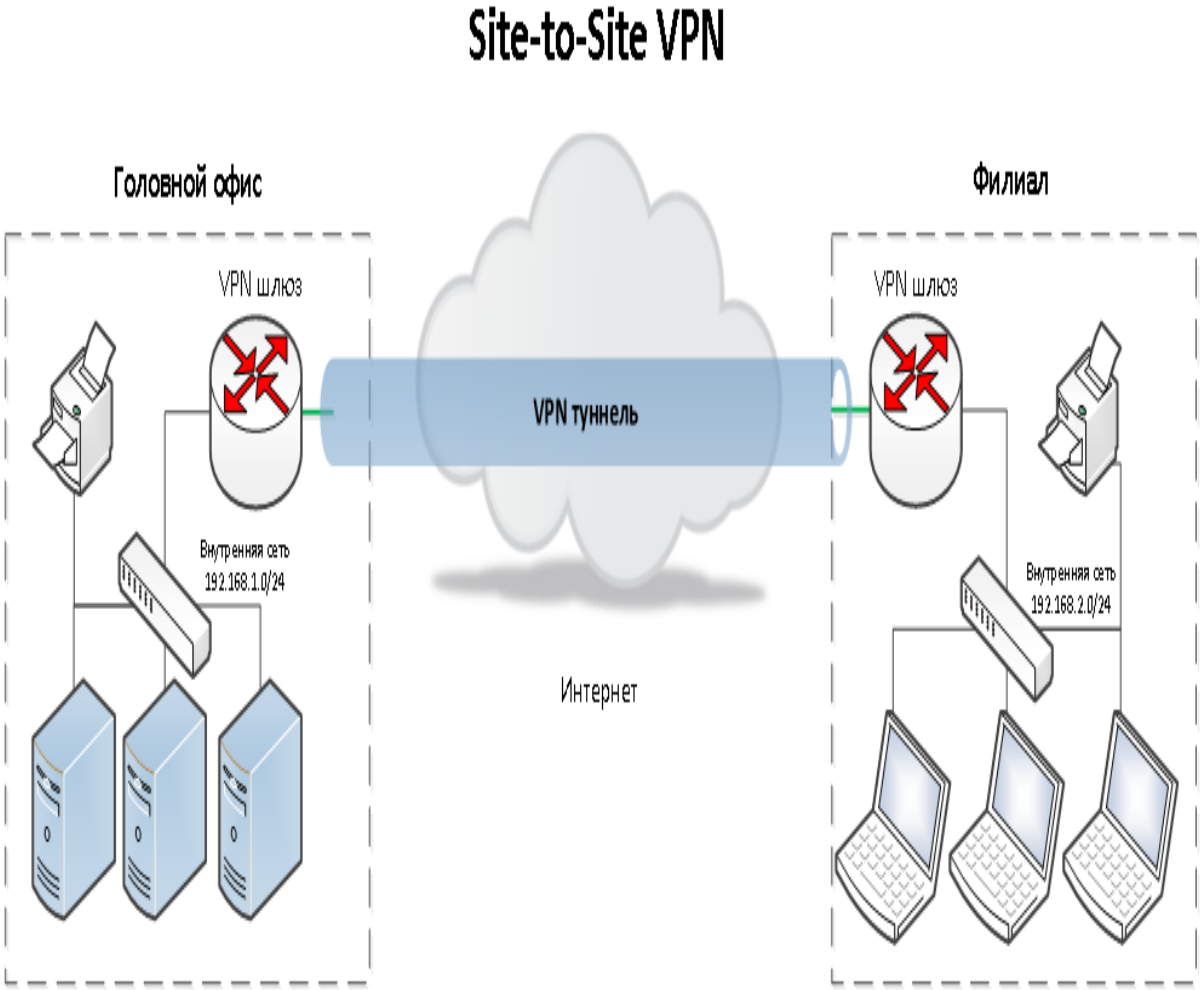

Рисунок 1.16 - Virtual Private Network [29]

Технологія VPN також використовується для доступу до ресурсів мережі підприємства працівників, що перебувають поза її межами (вдома, у відрядженні і т.п.). На відміну від Інтернету, корпоративні мережі підприємств, які не спеціалізуються на наданні послуг широкому загалу інтернет-користувачів, мають такі особливості:

1) єдине адміністративно-технічне керування;

2) однорідний і контрольований спектр обладнання, що використовується, та програмного забезпечення;

3) обмежений і контрольований перелік застосувань, що використовуються, всередині підприємства;

4) переважна частка передачі інформації між кінцевими об’єктами, які належать мережі підприємства;

5) обмежений і контрольований перелік зовнішніх ресурсів, з якими здійснюють обмін інформацією кінцеві об’єкти;

6) прихованість кінцевих об’єктів від доступу з боку мережі Інтернет (за винятком об’єктів, які призначені для використання як ресурси в Інтернеті);

7) обмежена загальна кількість кінцевих пристроїв.

У корпоративній мережі наявні можливості для забезпечення підтримки всіма кінцевими та проміжними об’єктами єдиного базового протоколу – IPv4 або IPv6. Відсутність тунелювань, перетворень пакетів між протоколами і надлишкової підтримки обох протоколів у межах кожного регіонального відділення сприятиме вищій надійності, функціональності та оптимальному використанню ресурсів.

Щодо зв’язку між відділеннями, у разі використання єдиного провайдера для WAN цей провайдер надає транспорт L2 або L3 з підтримкою потрібного протоколу (на сьогодні підтримка обох протоколів – IPv4 та IPv6 – є нормою для провайдерів [30]).

У разі зв’язку через Інтернет використання тунелів із кінцями на прикордонних маршрутизаторах відділень є неминучим. У цьому разі будь-яке співвідношення внутрішніх та зовнішніх протоколів для тунелів характеризується однаковим рівнем складності, функціональності та обсягом витрачених ресурсів. Для зв’язку із зовнішніми ресурсами в разі, якщо підтримуваний ресурсом протокол не збігається з базовим протоколом корпоративної мережі, можливе вжиття таких заходів:

1) для доступу до HTTP/HTTPS ресурсів із базовою функціональністю – використання серверів-посередників (proxy), які підтримують IPv4 та IPv6;

2) для зв’язку з ресурсами партнера – використання тунелю до мережі партнера;

3) для окремих випадків, які вимагають нетипової функціональності і для яких недостатньо зазначених вище методів – використання NAT із перетворенням протоколів або спеціалізованих рішень. Для адресації в корпоративних мережах, у випадку базового протоколу IPv4, стандартом є використання так званих «приватних» адрес [31]. Один з блоків приватних адрес – 10.0.0.0/8, забезпечує можливість надання унікальних адрес 16x106 пристроям, що на сьогодні є достатнім для переважної більшості підприємств. Оскільки найкритичніше обмеження IPv4, нестача адрес, в цьому випадку не актуальне, протокол IPv6 як базовий для корпоративної мережі не має суттєвих переваг. Стандартним технічним заходом у разі застосування приватних адрес для внутрішньої адресації в корпоративній мережі є використання NAT для зв’язку із зовнішніми ресурсами. Важливим побічним ефектом від використання NAT є захист об’єктів корпоративної мережі від контактів з боку Інтернету. Відсутність подібного захисту в IPv6 створює додаткові виклики щодо безпеки.

Цей фактор, а також використання застарілого апаратного та програмного забезпечення, що склалося історично, можуть стати аргументами на користь обрання IPv4 як базового протоколу в корпоративній мережі. Прооте, для щойно

створюваних нових мереж доцільно розглядати можливість їх базування на протоколі IPv6.

Розвиток мереж – як Інтернету, так і корпоративних мереж – невпинно здійснюється в бік збільшення кількості об’єктів у їхньому складі, а отже, використання більшої кількості адрес. Це призводитиме до переважного використання IPv6 у нових мережах і поступового зростання загальної частки мереж із цим протоколом як базовим. На певному етапі ключовим фактором на користь IPv6 стане вже не кількість доступних адрес, а потреба в сумісності з переважаючою кількістю існуючих об’єктів у мережах (на сьогодні цей фактор працює на користь IPv4). Після цього частка мереж IPv4 почне стрімко скорочуватися, зокрема за рахунок міграції старих мереж з IPv4 до IPv6.

Одним із підходів для міграції корпоративної мережі з базовим протоколом IPv4 до IPv6 є використання технології так званих «накладених» (overlay) мереж [32], яка дає змогу створити і розвивати мережеву інфраструктуру, базовану на IPv6, незалежно і не порушуючи існуючої інфраструктури на IPv4.

1.5 Постановка задачі по створенню корпоративної мережі.

Створити у мережевому симуляторі Cisco Packet Tracer 7, макет діючої мережі з трьох роутерів, на базі протоколу IPv6, які будуть шлюзами окремих сегментів мережі. Мережу розділити на сегменти та дати їм назву «офіс один, офіс два, бухгалтерія». У сегменти мережі під назвою «офіс один» та «офіс два» помісти по два персональних комп’ютера, та по одному ноутбуку. У сегмент мережі під назвою «бухгалтерія» помістити два персональних комп’ютери, та один сервер. Обмежити доступ до сегменту мережі «бухгалтерія» з сегменту мережі «офіс два» за допомоги функції «access list».

2. Сучасні симулятори комп'ютерних мереж

2.1 Cisco Packet Tracer 7

Cisco Packet Tracer – це симулятор мережі, створений компанією Cisco. Це програмне забезпечення дозволяє імітувати роботу різних мережевих пристроїв, проектувати свої власні мережі, створюючи і відправляючи різноманітні пакети даних, зберігати і коментувати свою роботу. Користувачі можуть вивчати і використовувати такі мережні пристрої, як комутатори другого і третього рівнів, робочі станції, визначати типи зв’язків між ними і з’єднувати їх.

Після того, як мережа спроектована, користувачі можуть приступати до конфігурації вибраних пристроїв за допомогою термінального доступу або командного рядка. Особливість даного симулятора є наявністю у ньому "Режиму симуляції". У даному режимі всі пакети, що пересилаються всередині мережі, відображаються графічно. Ця можливість дозволяє наочно продемонструвати, з якого інтерфейсу в даний момент часу переміщається пакет, який протокол використовується і т.д.

Однак, це не всі переваги Packet Tracer: у "Режимі симуляції" користувач може не тільки відслідковувати використовувані протоколи, а й бачити, на якому з семи рівнів моделі OSI даний протокол задіяний.

Cisco Packet Tracer може бути використано не тільки як симулятор, але й як мережеве програмне забезпечення для симулювання віртуальної мережі через реальну мережу, та мережу Інтернет. Користувачі різних комп’ютерів, незалежно від їх місцезнаходження, можуть працювати над однією мережевою топологією, роблячи її налаштування чи то усунення проблем. Ця функція багатокристувацького режиму Cisco Packet Tracer може бути задіяна для організації командної роботи.

У Cisco Packet Tracer користувач може симулювати будівництво не тільки логічної, а також фізичної моделі мережі, а тому отримувати навички проектування.

Схему мережі можна покласти на креслення на реальну, схему будівлі чи то навидь міста та спроектувати усю його кабельну мережу, розмістити пристрої у тих чи інших будівлях та приміщеннях с урахуванням фізичних обмежень, таких як довжина та тип кабелю що прокладається, чи то радіус зони покриття безпровідної мережі.

В основній панелі інструментів знаходяться ярлики команд, такі як New (створити), Open (відкрити), Save (зберегти), Cut (вирізати), Paste (вставити) та Zoom (масштабування). Тут також знаходяться ярлик Custom Device (користувацький пристрій), що дозволяє створювати користувальницькі конфігурації апаратного забезпечення.

Інформацію про топологію мережі можна ввести у вікні Network Information (данні про мережу).

Ярлик довідки знаходиться поряд з кнопкою Network Information.

З допомогою кнопки Set Tiled Background (фон) можливо змінювати фонове зображення робочої області.

Параметр New Cluster (створити кластер) дозволяє групувати пристрої та економити робочу область.

Параметр Viewport (точка огляду) дозволяє масштабувати представлені мережі.

Вкладка фізичного простору дозволяє перейти у вікно фізичної області, де вказано розміри логічної топології мережі. Воно створює відчуття простору та дозволяє відобразити знаходження пристроїв та мереж.

В загальній панелі інструментів знаходяться всі команди, що використовуються в робочому полі Packet Tracer (рис.1):

- Select (вибір) дозволяє перетягувати, виділяти і вибирати пристрої та бездротові канали;

- Move Layout (переміщення фону) дозволяє переміщувати робочу область;

- Place Note (замітки) дозволяє робити замітки в робочій області:

- Delete (видалення) дозволяє видаляти пристрої та бездротові канали;

- Inspect (відображення) дозволяє проглядати різні таблиці пристроїв;

- Add Simple PDU (добавити простий PDU) дозволяє формувати простий пакет ICMP даних між двома вузлами;

- Add Complex PDU (добавити складний PDU) дозволяє формувати складний пакет ICMP даних між пристроями.

- Power Cycle Devices кнопка вмикання та вимикання всіх пристроїв в робочій області.

Вкладка Simulation Mode дозволяє перейти в режим моделювання. Цей режим дозволяє відслідковувати мережний трафік в повільному, детальному режимі.

У вікні "Клас обладнання" відображається дев’ять класів. Головними класами є:

Роутер (маршрутизатор) – мережний пристрій, на підставі інформації про топологію мережі і певних правил приймає рішення про пересилання пакетів мережного рівня (рівень 3 моделі OSI) між різними сегментами мережі.

Світч (комутатор) – пристрій, призначений для з’єднання декількох вузлів комп’ютерної мережі в межах одного сегменту мережі (рівень 2 моделі OSI). Світч відрізняється від роутера тим, що не може поєднувати різні мережі (роз’єми всі однакові). Комутатор зберігає в пам’яті таблицю комутації (зберігається в асоціативній пам’яті), в якій вказується відповідність MAC-адреси вузла порту комутатора.

Хаб (концентратор) – мережний пристрій, призначений для об’єднання кількох пристроїв Ethernet в спільний сегмент мережі. Пристрої підключаються за допомогою витої пари, коаксіального кабелю чи оптоволоконна. Концентратор працює на фізичному рівні мережевої моделі OSI, повторює надісланий на один порт сигнал, на всі активні порти.

Кабелі (з’єднувачі) в Cisco Packet Tracer є декількох типів:

- автоматичний – програма автоматично підбирає потрібний тип кабелю (для новачків);

- консольний – з’єднує комп’ютер – роутер;

- прямий патч-корд – з’єднує: комп’ютер – світч та роутер – світч;

- кросовий патч-корд – з’єднує комп’ютер – комп’ютер, світч – світч, роутер–роутер та роутер – комп’ютер;

Кінцеві пристрої – в Cisco Packet Tracer це комп’ютер, сервер, принтер та телефон.

Рисунок 2.1 Cisco packet tracer 7

2.2 Графічний симулятор GNS (Graphical Network Simulator)

GNS3 – це безкоштовний графічний симулятор мережі, який дозволяє змоделювати віртуальну мережу з маршрутизаторів і віртуальних машин. Надійний інструмент для навчання та тестів. Працює практично на всіх платформах. Дуже добре підходить для створення стендів на десктоп машинах.

Залежно від апаратної платформи, на якій буде використовуватися GNS3, можлива побудова комплексних проектів, що складаються з маршрутизаторів Cisco, Cisco ASA, Juniper, а також серверів під управлінням мережевих операційних систем. При відсутності можливості отримати доступ до реального обладнання, GNS3 стане практично повноцінної лабораторією. Крім того, лабораторні роботи виконуються в GNS3, можуть стати доповненням до занять в реальній лабораторії студентам готуються до сертифікаційних іспитів CCNA / CCNP і CCIE

Єдиним недоліком даного програмного забезпечення є відсутність можливості повноцінної симуляції комутаторів другого рівня Cisco. Цей недолік не буде виправлений в нових версіях, так як його причиною є кардинальна відмінність в апаратній платформі маршрутизаторів і світчей Cisco. У деяких випадках цей недолік виходить обійти за допомогою мережевого модуля NM-16ESW. На жаль, лістинг команд трохи відрізняється в разі використання NM-16ESW і реальних світчей Cisco, але цілком підходить для навчання.

До складу GNS3 не належать образи IOS / IPS / PIX / ASA / JunOS, так як вони є частиною комерційних продуктів відповідних компаній, і ніякого прямого відношення до проекту GNS3 не мають. На даний момент це вже не є проблемою, так як 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 будь-якої проект, без використання реального обладнання.

Використання WireShark дозволяє провести моніторинг трафіку всередині проектованої топології, що дає додаткову інформацію для розуміння досліджуваних технологій. На даний момент є версії для Linux, MS Windows XP і Windows 7, а також для MacOS. Найважливішим чеснотою GNS3 є простота і зручність при створенні проектів для виконання лабораторних робіт. Встановлена програма вимагає мінімум початкових налаштувань які робляться за пару хвилин.

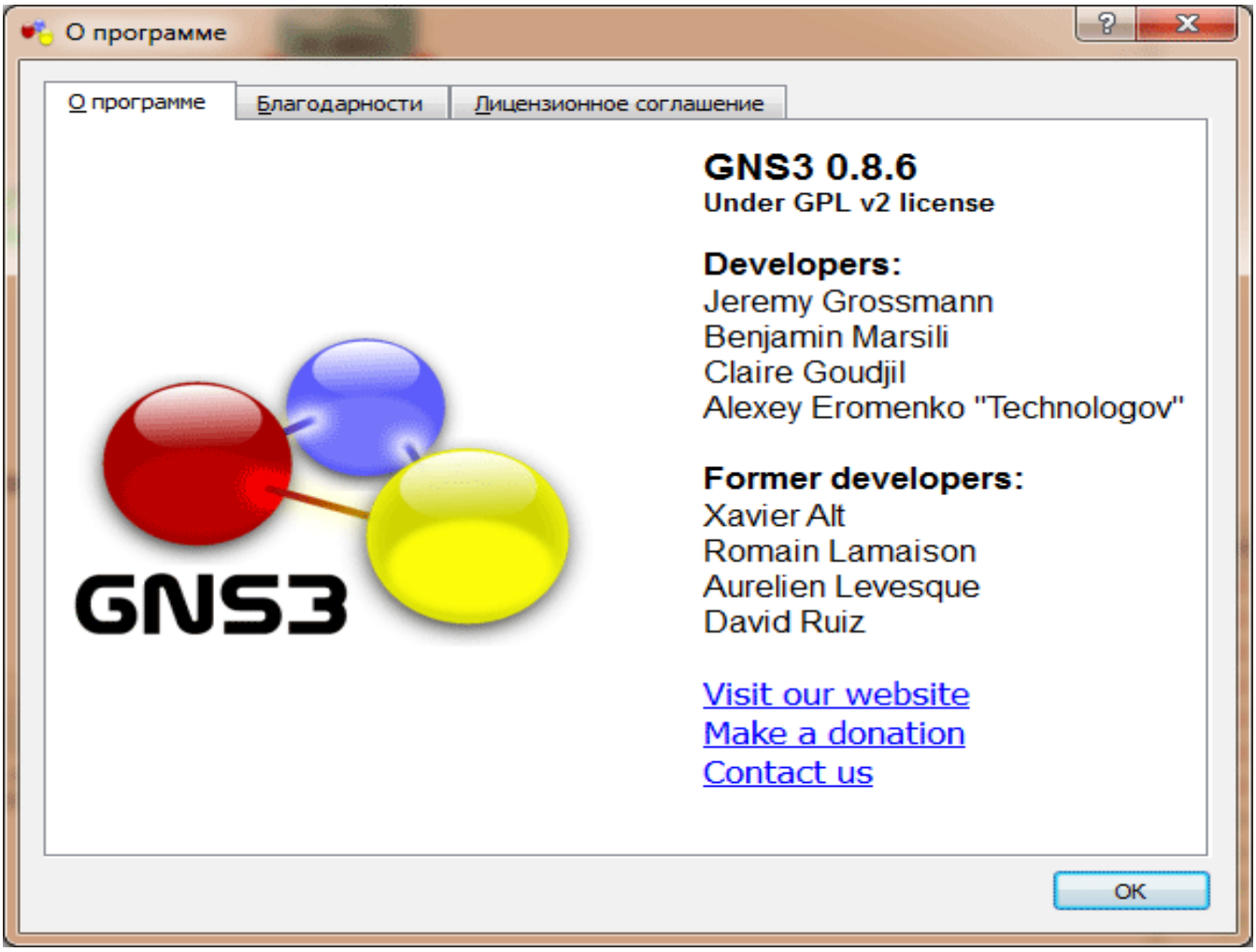

Рисунок 2.2 Graphical Network Simulator

2.3 Емулятор мережі UNenLab (Unified Networking Lab)

UNenLab (Unified Networking Lab, UNL) - це мульті-вендорна і багатокористувачська платформа для створення і моделювання найрізноманітніших лабораторій і дизайнів, яка дозволяє змоделювати віртуальну мережу з маршрутизаторів, комутаторів, пристроїв безпеки.

UnetLab - повністю безкоштовний. Ви можете запускати стільки екземплярів обладнання (роутерів, комутаторів, пристроїв безпеки тощо) скільки ви хочете і будь хочете. Наприклад, в тому ж Cisco VIRL Personal Edition ви обмежені 15-ю вузлами і набір пристроїв досить скромний. Наприклад повноцінну ASA отримати не представляється можливим, так само як і маршрутизатор з Serial-інтерфейсом.

На відміну від попереднього проекту IOU-WEB, в UNetLAB реалізований повністю графічний інтерфейс дизайну топології, приблизно так, як це робиться в GNS. Тепер немає необхідності писати netmap файли для кожної топології. Недоліком є повна відсутність сумісності з попереднім проектом. Файли топології зібрані в iou-web необхідно переписувати для UNL. Але в останній версії розробники надають скрипт який допоможе автоматизувати процес.

Також в UNL включена підтримка так званої Custom Topology, тобто «клікабельних» красивих картинок-діаграм, які ви можете намалювати в MS Visio і імпортувати в вашу лабораторну, так як це було в iou-web.

Починаючи з версії UNetLab 0.9.54 з'явився функціонал на багато користувачів. На одній і тій же VM, кожен авторизований користувач може створювати свої стенди незалежно один від одного, а також спільно працювати з загальним стендом, який поділяють кілька користувачів одночасно. При цьому користувачі запускають спільний стенд незалежно один від одного.

Підтримка обладнання в UNetLab дуже широка. Ви можете запускати Cisco IOL-образи, образи з VIRL (vIOS-L2 і vIOS-L3), образи ASA Firewall (як портируемі 8.4 (2), 9.1 (5), так і офіційні ASAv), образ Cisco IPS, образи XRv і CSR1000v, образи

dynamips з GNS, образи Cisco vWLC і vWSA, а також образи інших вендорів, таких як Juniper, HP, Checkpoint.

На поточний момент підтримуються наступний список обладнання:

- Aruba ClearPass
- Alcatel 7750 SR
- Arista vEOS
- Brocade Virtual ADX
- Citrix Netscaler VPX virtual
- Checkpoint Firewall
- Cisco ASA (porting)
- Cisco ASAv
- Cisco CSR 1000V
- Cisco IPS (porting)
- Cisco IOS 1710/3725/7206 (dynamips, ethernet only)
- Cisco IOL (for Cisco internal use only)
- Cisco NX-OSv – titanium (for VIRL customers only)
- Cisco vIOS (for VIRL customers only)
- Cisco vIOS L2 (for VIRL customers only)
- Cisco XRv
- Cisco WSA virtual appliance
- Cisco Wireless controller – vwlc
- Extreme Networks virtual
- F5 BIG-IP LTM VE
- Fortinet FortiGate (new)
- HP VSR1000
- Juniper Olive (porting)

- Juniper Networks vMX router
- Juniper vSRX
- Palo Alto VM-100 Firewall
- VyOS
- MS Windows hosts

Дана платформа підійде як новачкам для підготовки до CCNA / CCNP, так і для професіоналів для підготовки CCIE Routing and Switching, CCIE Security, CCIE Service Provides, CCIE Data Centers, а також для інших різноманітних інженерних задач.

Рисунок 2.3 UNenLab

3. МОДЕЛЮВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ IPV6 У СИМУЛЯТОРІ PACKET TRACER

3.1 Створення базової моделі мережі

У моделюванні мережі була використана схема, що складається з двох, незалежних одна від одної мереж, які після налаштування роутерів змогли обмінюватись пакетами між собою.

Перший етап моделювання, це створення мережі між двома роутерами (cisco 2911), які з'єднані між собою мідним дротом (вита пара).

Також було зроблено дві офісні мережі, до складу яких входять, комутатор «cisco 2960-24», два персональних комп'ютера, та по одному ноутбуку, у кожній. Всі вони на першому етапі об'єднані мідним дротом (вита пара). Мережа представлена на рисунку 3.1

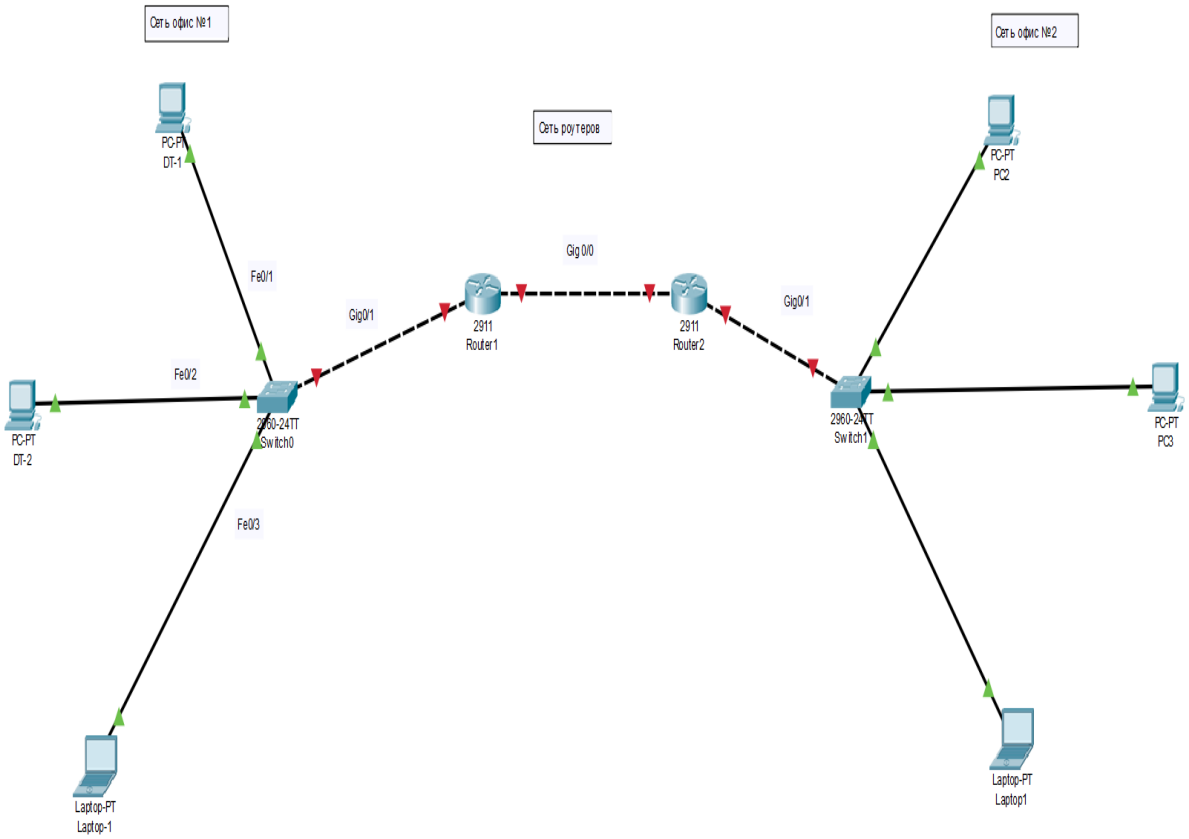

Рисунок 3.1 – Схема мережі двох офісів та роутерів.

Наступний етап у цьому моделюванні – призначення адреси в відокремлених мережах «офіс один» та «офіс два».

У мережі «офіс один» комп'ютер №1 отримає адресу 2001:abcd:adbc:1::1, комп'ютер №2 2001:abcd:adbc:1::2, ноутбук буде з адресою 2001:abcd:adbc:1::3. Шлюз мережі «офіс один» буде мати адресу 2001:abcd:adbc:1::4

У мержі «офіс два» комп'ютер №1 – 2001:abcd:adbc:2::1, комп'ютер №2 – 2001:abcd:adbc:1::2, ноутбук – 2001:abcd:adbc:2::3, шлюз мережі офіс два» – 2001:abcd:adbc:2::4.

Роутери між собою будуть мати мережу 2001:abcd:adbc:3::/64, відповідно роутер один матиме адресу 2001:abcd:adbc:3::1, а другий 2001:abcd:adbc:3::2

Конфігурування роутерів.

Включення порту «Router(config-if)#no shutdodnown»

Додавання ip-адреси «ipv6 address 2001:abcd:adbc:3::1/64»

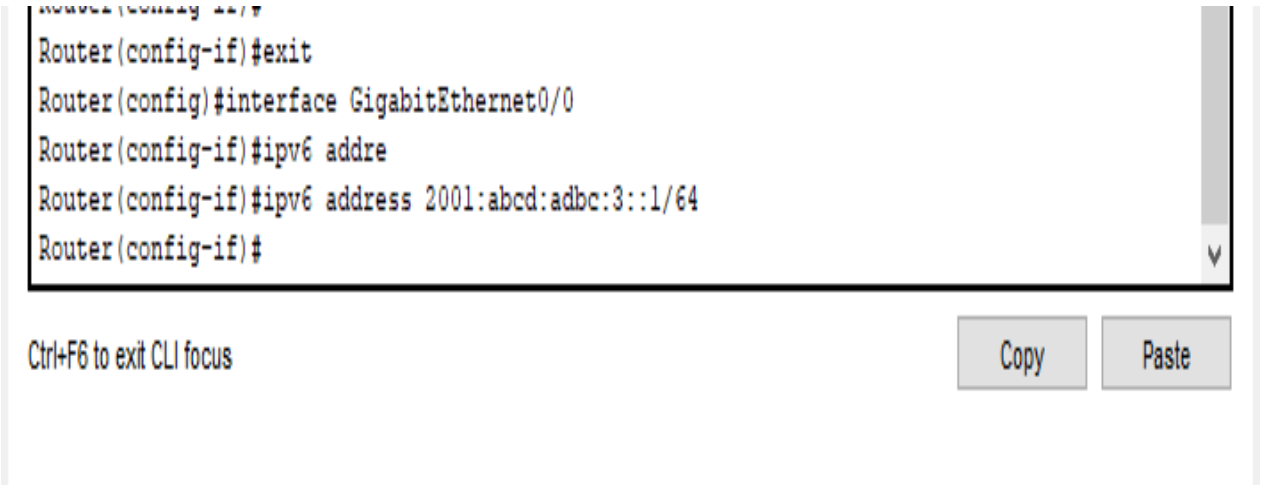

Рисунок 3.2 - Додавання ip-адреси на порт GigabitEthernet0/0 роутера один

За аналогією вмикається порт на роутері два, та прописується для порту GigabitEthernet0/0 наступна адреса «2001:abcd:adbc:3::2».

Проходимо перевірку мережі з двох роутерів за допомогою команди «ping».

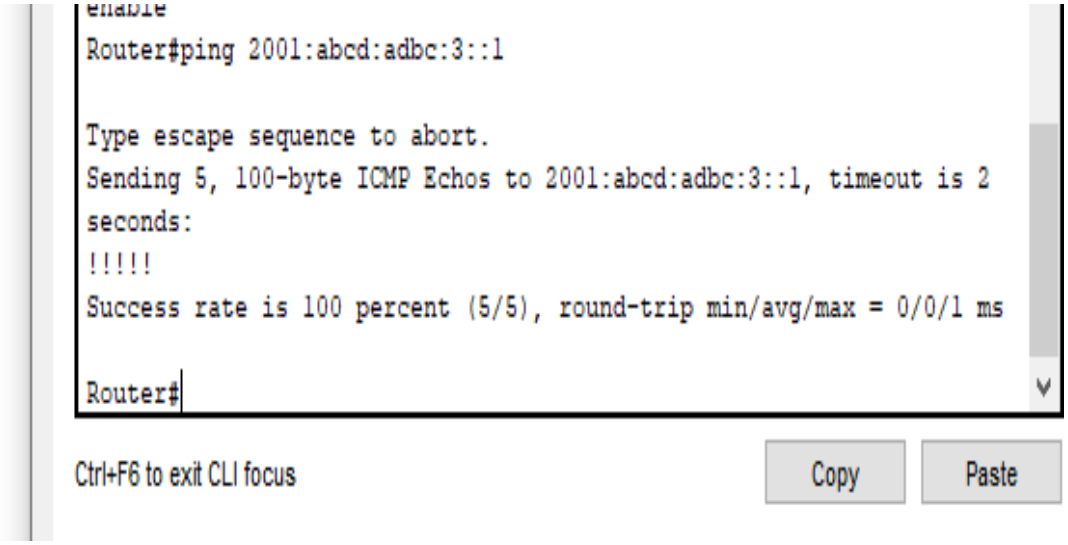

Рисунок 3.3 - Ping з роутера два на роутер один

На рисунку 3.3 пакети від роутера два без втрат добігають до роутера один. З чого робиться висновок, що мережа між роутерами працює.

Присвоюємо адреси, які були наведені раніше комп'ютерам, у мережах «офіс один» та «офіс два».

Мережі «офісу один» була задана адреса з номером один (2001:abcd:adbc:1::/64). Комп'ютерам були надані адресі 1 та 2, ноутбук отримав адресу під номером 3. Після надання адрес пристроям у мережі «офіс один», розпочато перевірку роботи мережі між ними за допомогою команди "ping". На рисунку 3.4 відображений результат перевірки.

Пакети добігають кінцевих точок без втрат, з чого робиться висновок, що мережа працює добре.

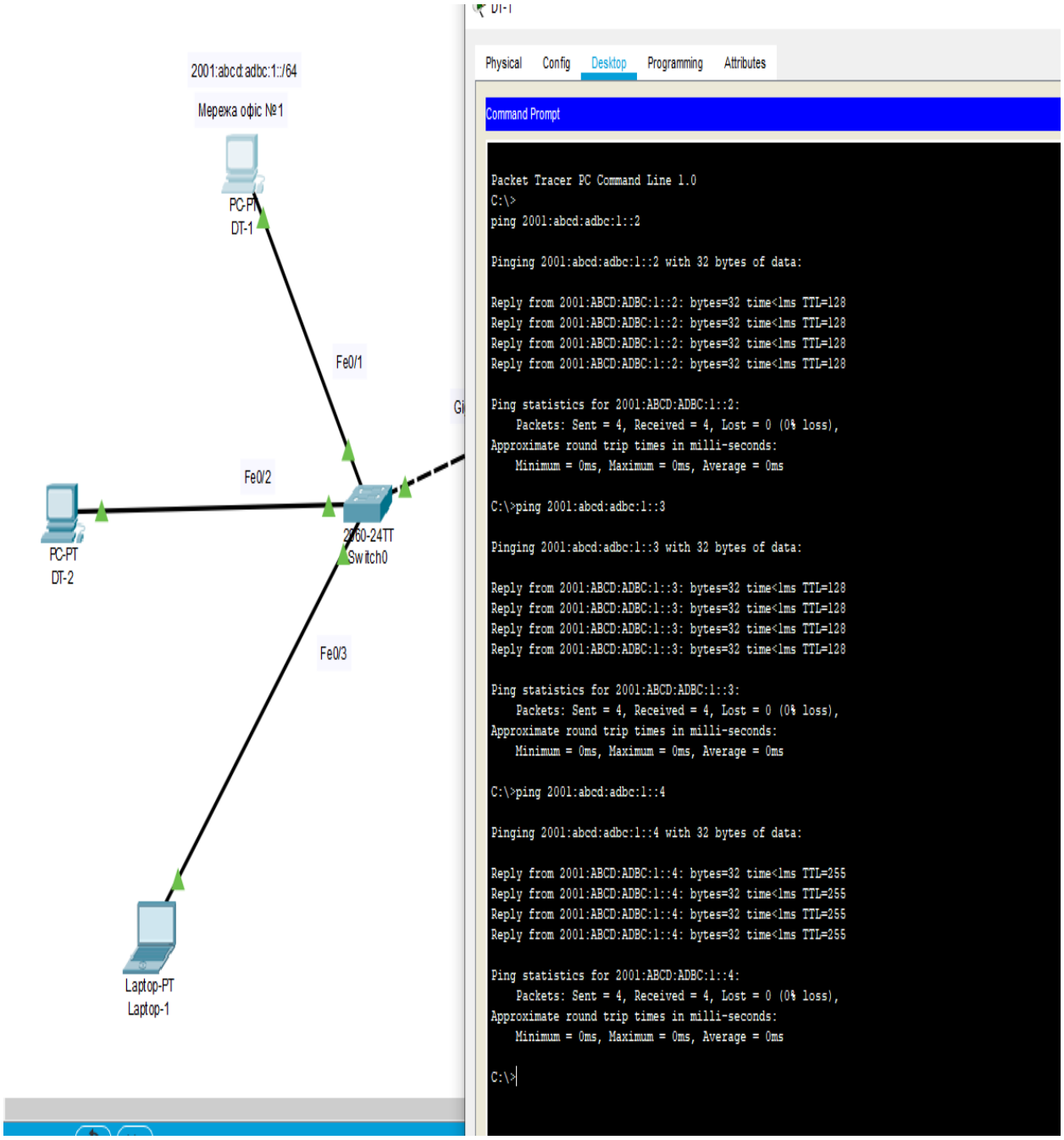

Рисунок 3.4 - Ping з PC2 на PC1 та PC2 на laptop1

Присвоюємо адресу для порту interface GigabitEthernet0/1 роутеру один, який буде вихідним шлюзом мережі «офіс один». Перевіряємо шлюз командою “ping”.

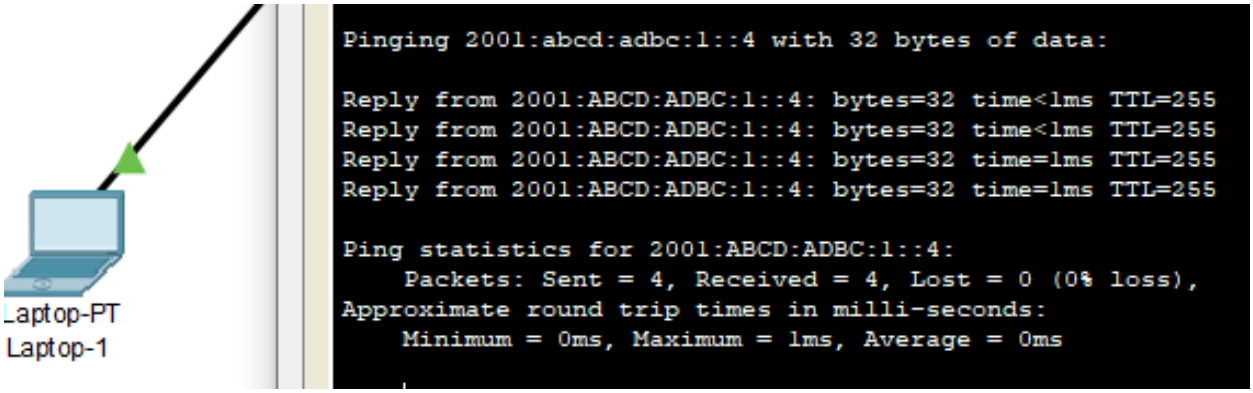

Рисунок 3.5 - Ping шлюза мережі «офіс один»

Всім пристроям мережі «офіс один» було встановлено, як основний шлюз мережі, адресу «2001:abcd:adbc:1::4».

Перевірка конфігурації роутера один командою «show running-config». На рисунку 3.6 відображена конфігурація маршрутів роутера на початковому етапі конфігурування.

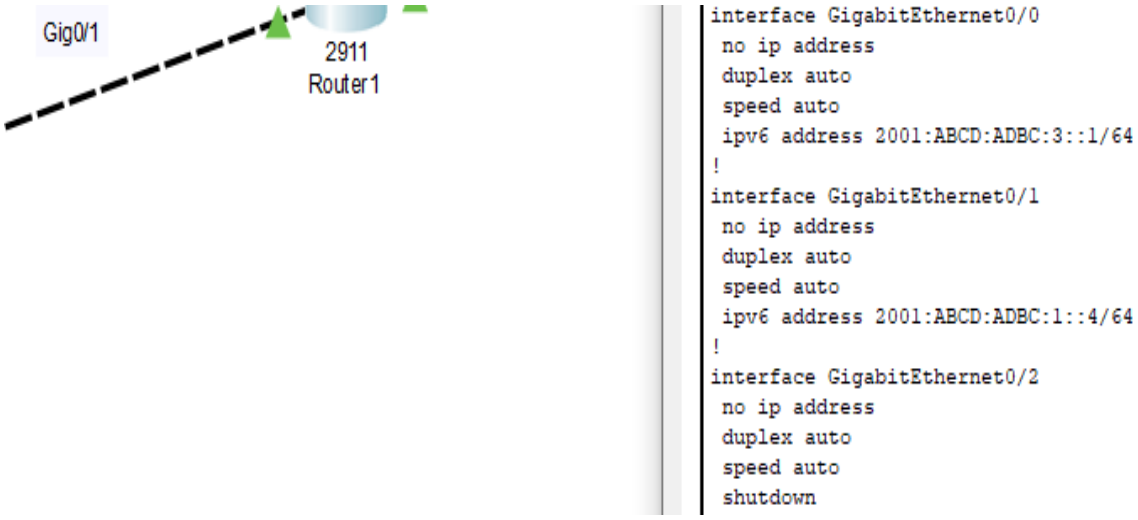

Рисунок 3.6 - Конфігурація роутера, початковий етап

Мережа «офіс один» налагоджена.

Налагодження мережі «офіс два» було виконане за аналогією з мережею «офіс один». Після призначення адрес пристроям мережі «офіс два» була проведена

перевірка роботи мережі за допомогою команди “ping” з PC1 на інші пристрої мережі.

Результат коректної роботи мережі відображений на рисунку 3.7, а саме це перевірка доступності комп’ютера «PC2» та ноутбука «laptop1» з комп’ютера «PC1» за допомогою команди «ping» та шлюза мережі.

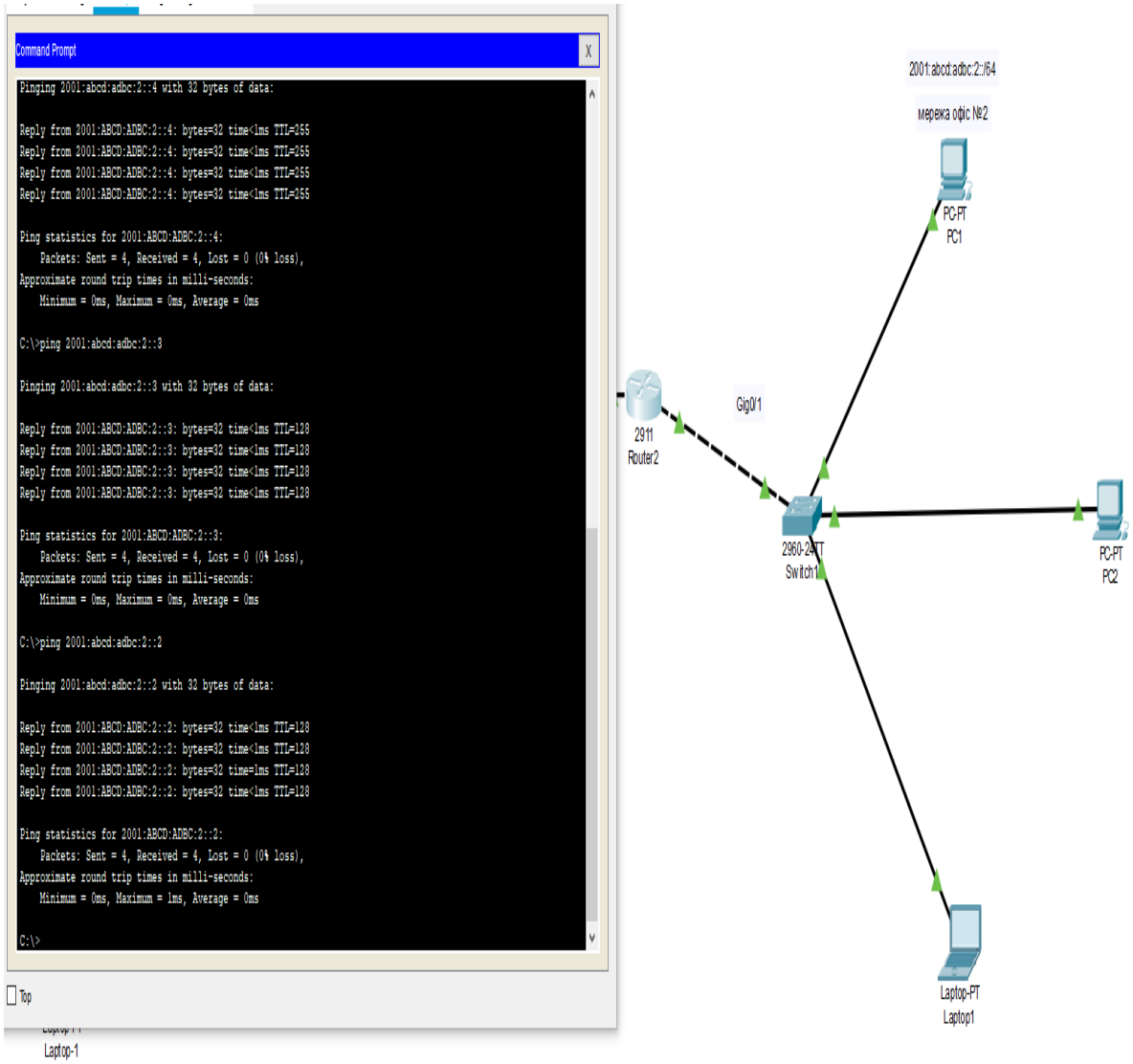

Рисунок 3.7 – Ping пристроїв мережі два

Командою «ipv6 unacast-routing» була увімкнена маршрутизація IPv6 на роутерах один та два. Прокладання маршрутів на роутерах для можливості обміну пакетами

між двома мережами у цій схемі має наступний вигляд: командою «ipv6 route» було вказано мережі і порти, з яких вони повинні передавати та приймати пакети. Маршрут для роутера один, відображений на рисунку 3.8, а маршрут для роутера два – на рисунку 3.9

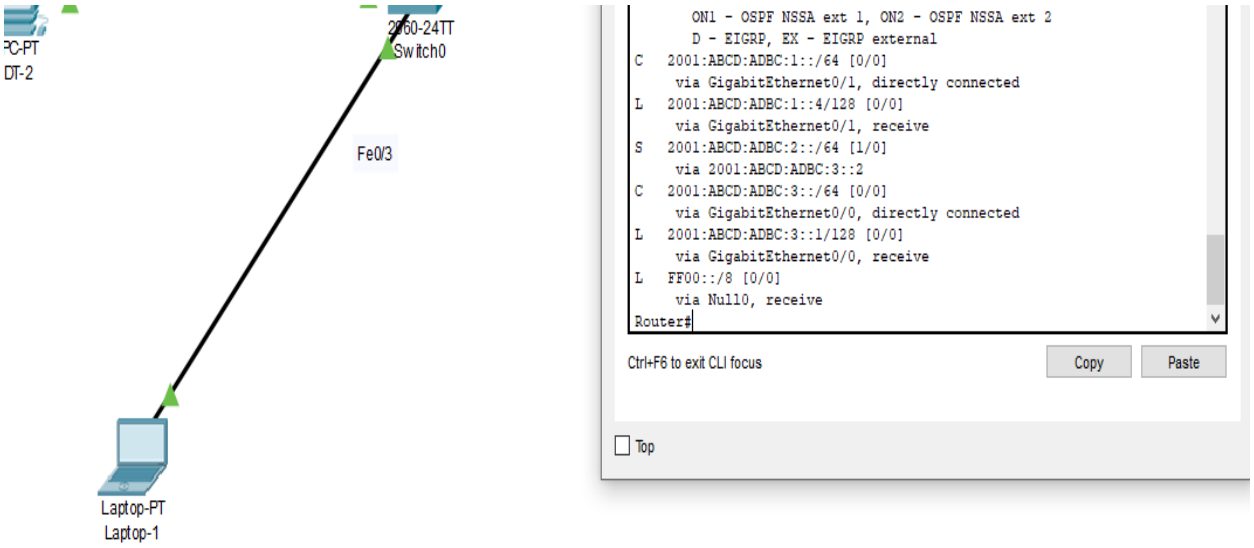

Рисунок 3.8 - Маршрут роутера один

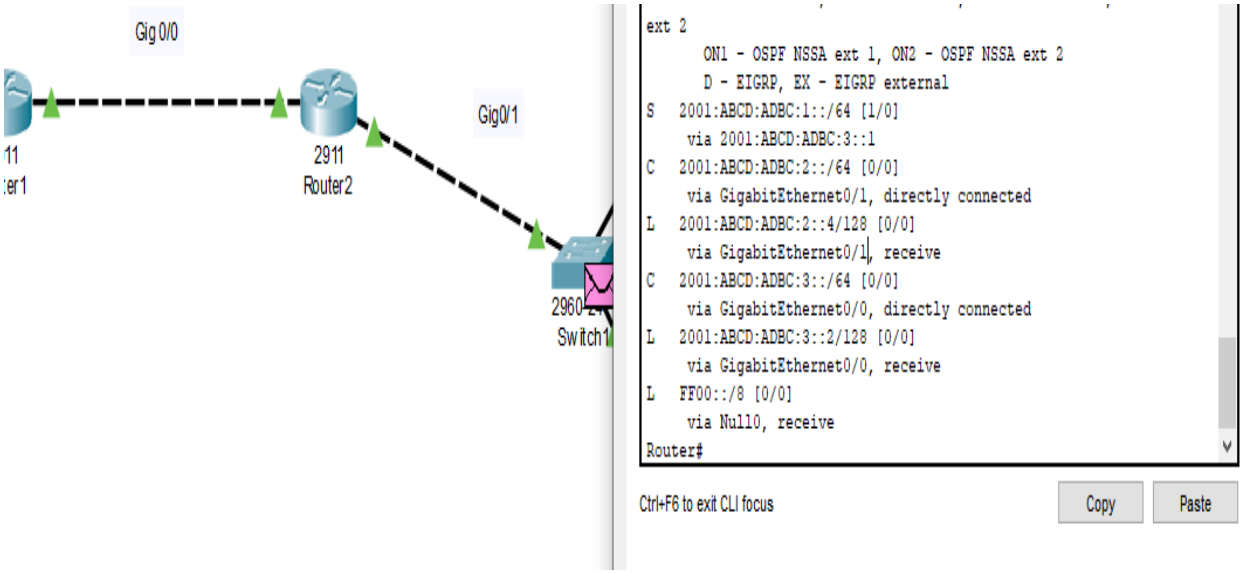

Рисунок 3.9 - Маршрут роутера два

Перевірка роботи маршрутизації двох незалежних мереж була здійснена за допомогою команді «ping». Результат перевірки відображений на рисунку 3.10,

пакети з комп’ютера мережі «офіс один», доходять до комп’ютера мережі «офіс два» без втрат та великої затримки.

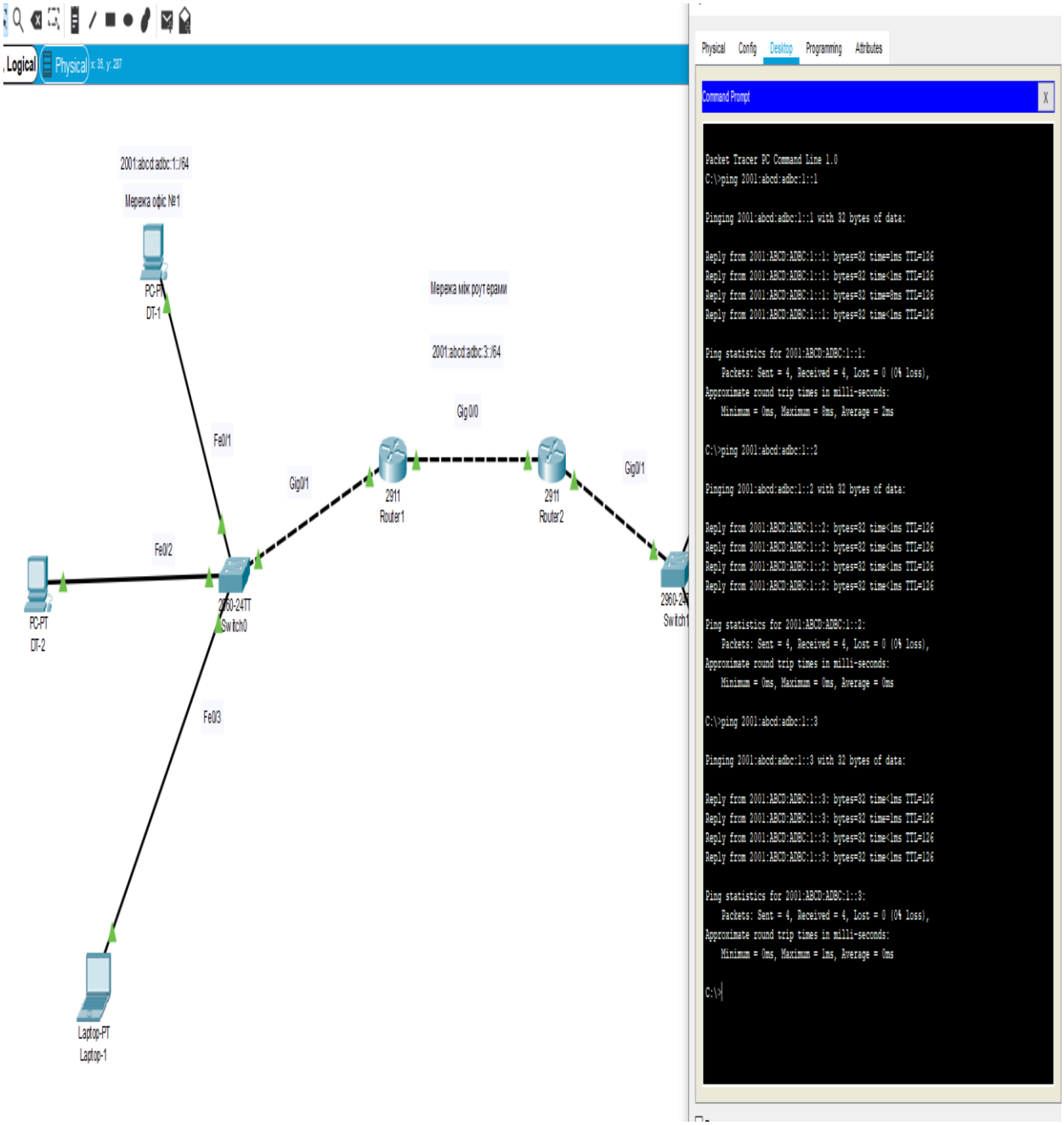

Рисунок 3.10 - Ping пристоїв мережі два з мережі один

На рисунку 3.11 відображена перевірка командою «ping» у зворотньому напрямку, з пристроїв мережі два до пристроїв мережі один. Як показано на

рисунку 3.11 пакети доходять до пристроїв мережі «офіс один» без втрат та великої затримки.

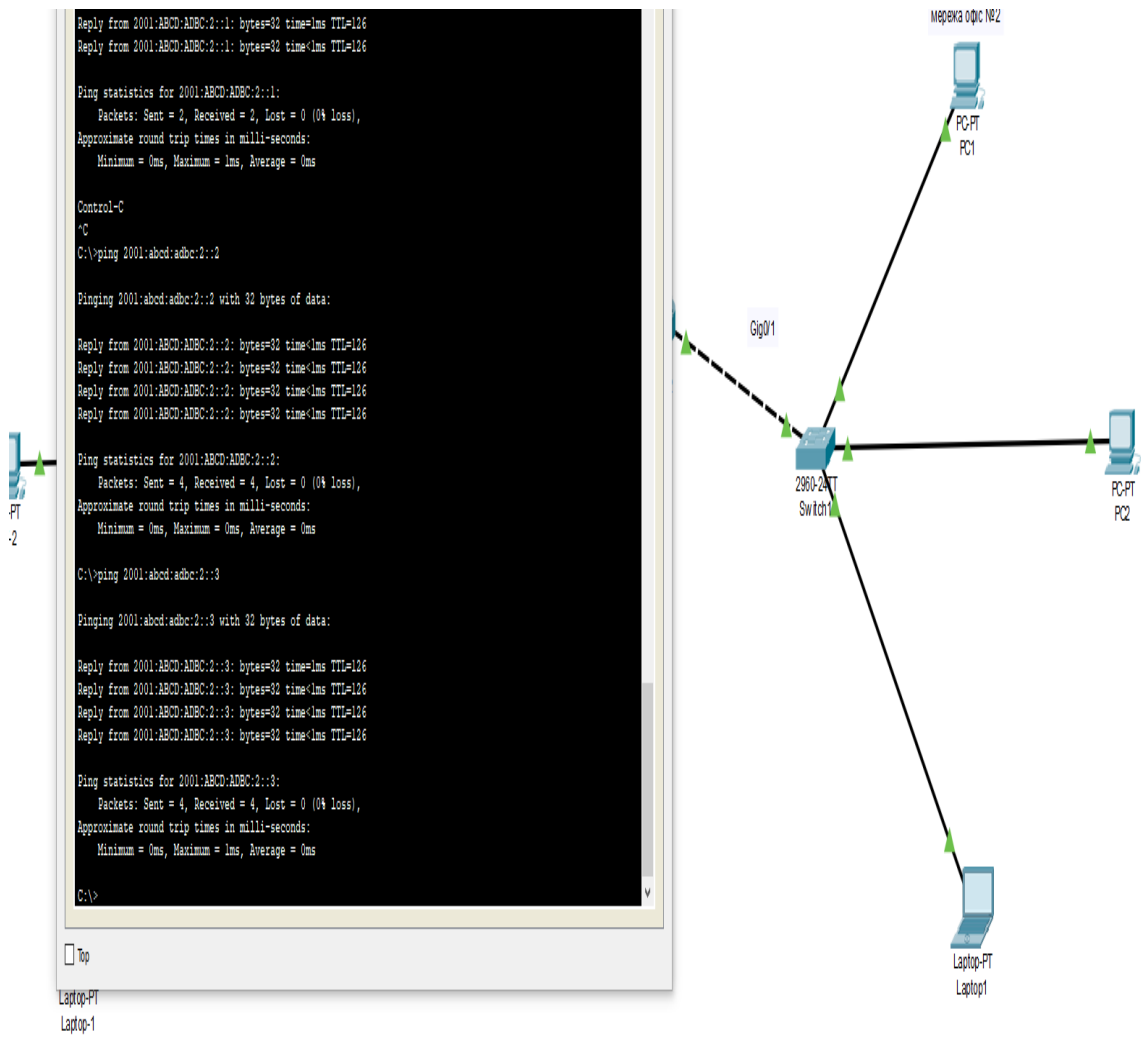

Рисунок 3.11 - Ping пристоїв мережі один з мережі два

3.1 Інтеграція мережі до існуючої схеми

Інтеграція чи то додавання до існуючої мережі іншої мережі завжди викликало багато перепон та ускладнень. Але з використанням протоколу IPv6 така інтеграція стала набагато легша. Нижче це буде доведено на практиці. Нова мережа буде складатись з двох комп'ютерів, роутера (cisco 2901), комутатора та сервера. Назвемо цю мережу «бухгалтерія».

Згідно з технічним завданням доступ до мережі «бухгалтерія» має бути лише у пристроїв які знаходяться в оточені мережі «бухгалтерія» та «офіс один». Але, роутер цієї мережі має бути під'єднаний до роутера, який є шлюзом мережі «офіс два». Першим етапом ми єднаємо комп'ютери та сервер крученим дротом з комутатором. Комутатор єднається з роутером мережі мідним дротом (вита пара). Між роутером три і роутером два, теж буде прокладено мідний дріт. На рисунку 3.12 відображена схема інтеграції мережі в існуючу схему з двох мереж та двох роутерів.

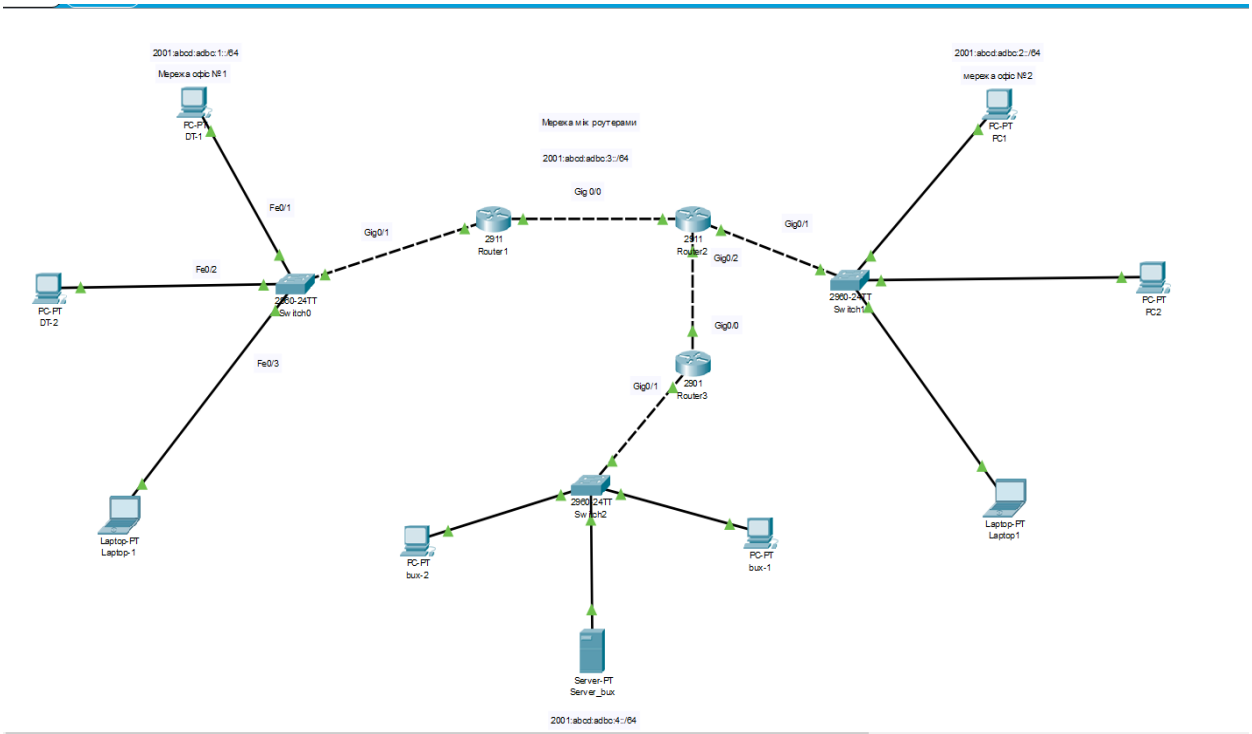

Рисунок 3.12 - Схема інтеграції мережі три

Адреса мережі буде мати наступний пул: «2001:abcd:adbc:4::/64».

Після привласнення адрес серверу та комп’ютерам, була проведене перевірка доступності пристроїв в мережі командою «ping». Результат відображений на рисунку 3.13: пакети проходять без втрат, з чого робиться висновок, що мережа працює добре.

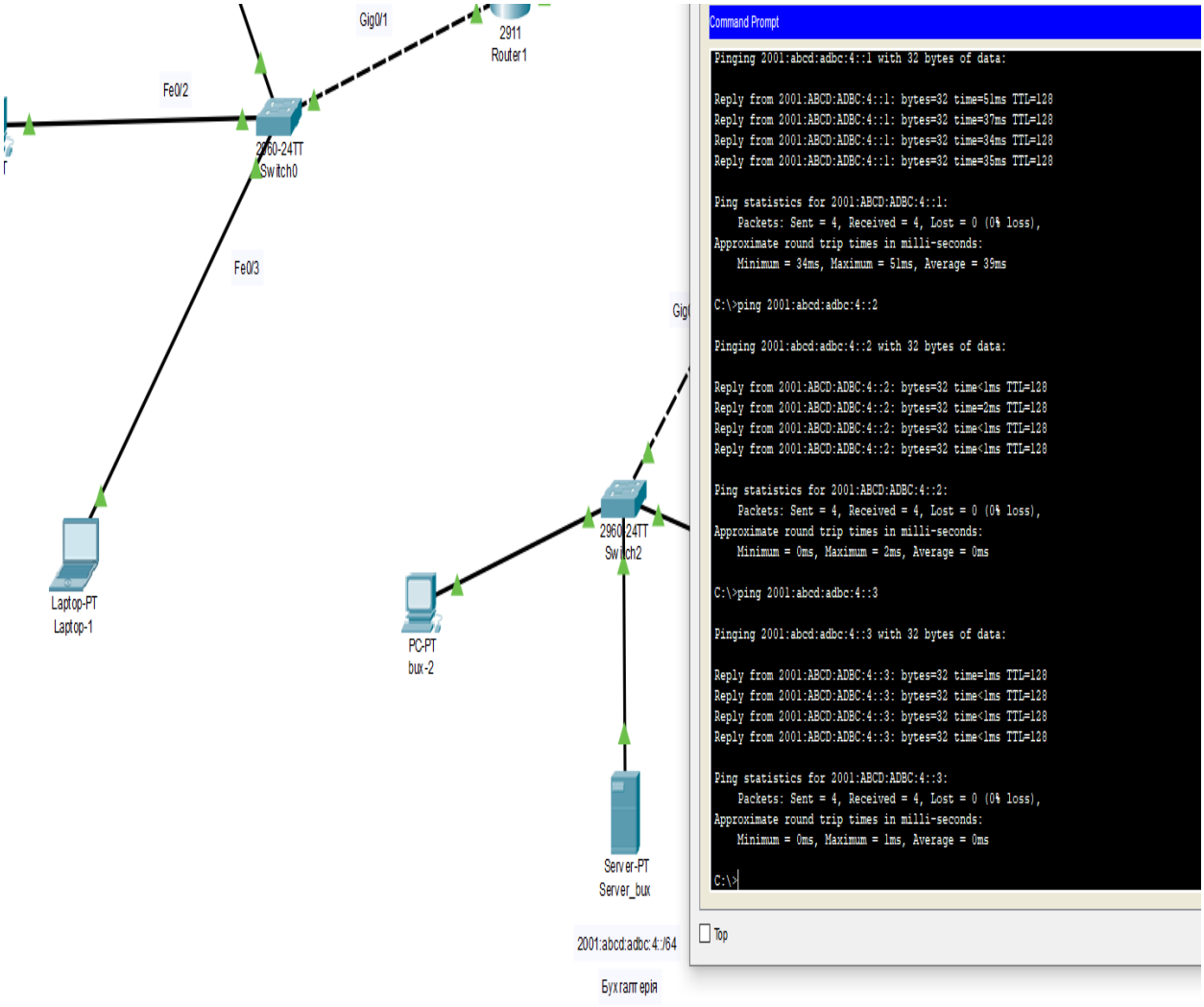

Рисунок 3.13 - Ping пристроїв мережі «бухгалтерія»

Наступний крок – привласнення адреси «шлюзу» мережі на роутері три. Це робиться з допомогою наступних команд:

1) включення порту «Router(config-if)#no shutdown»;
2) додаємо на порт ip адресу «ipv6 address 2001:abcd:adbc:4::4/64»;
3) перевіряємо доступність командою «ping».

Результат відображений на рисунку 3.14

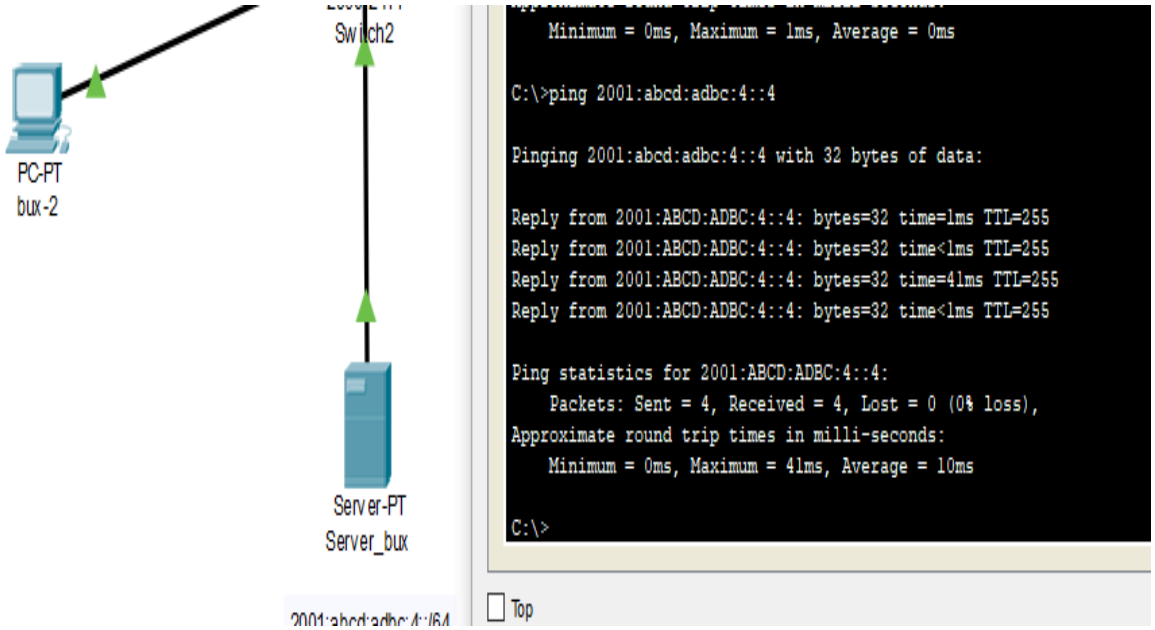

Рисунок 3.14 - Ping роутера три

Далі треба додати роутер три до мережі роутерів, щоб роутери мали можливість між собою вільно обмінюватись даними.

Під час налаштування роуетра під номером три, були увімкнені обидва гігабітних порти за допомогою команди «no shutdown». За аналогією з двома іншими роутерами була ввімкнена маршрутизація IPv6 командою «ipv6 unicast-routing». Це дає можливість здійснювати маршрутизацію у середині мережі між трьома роутерами. Наступним кроком було додавання адреси «2001:abcd:adbc:5::1/64» на порт «interface GigabitEthernet0/0» роутера три, та «2001:abcd:adbc:5::2/64» на порт

«interface GigabitEthernet0/2» роутера два. Після виконання цього кроку була проведена перевірка роботи мережі роутерів командою «ping».

На рисунку 3.15 відображено результат виконання команди «ping» з роутера номер два на роутер номер три.

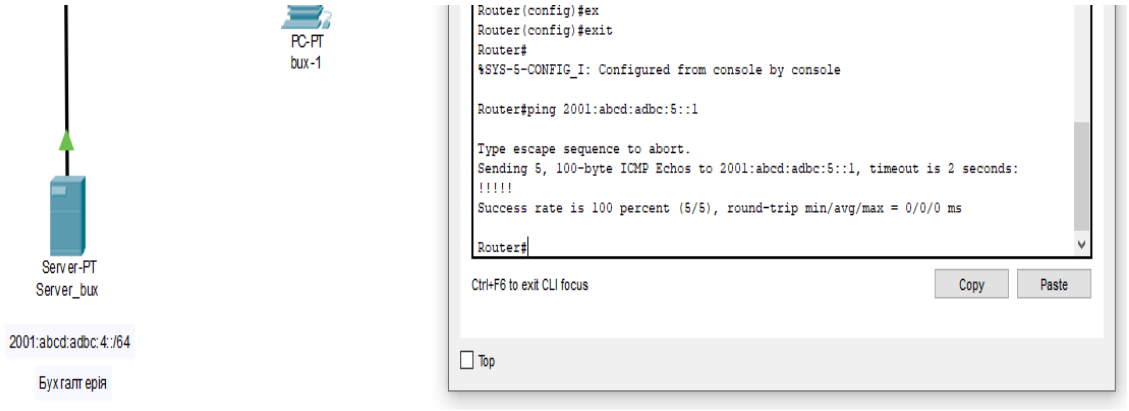

Рисунок 3.15 - Ping з роутера два на роутер три

Як видно з рисунку 3.15 мережа «2001:abcd:adbc:5::/64» працює.

Наступним етапом налагодження мережі є прокладання маршрутів нової мережі в тій, що вже існує. Прокладання робиться за допомогою команди «ipv6 route».

Після послідовного виконання команди «ipv6 route» на трьох роутерах, з вказанням мережі, маршрут був встановлений.

Маршрути на усіх роутерах відображені на рисунках: 3.16 – для роутера один, 3.17 – для роутера два, 3.18 – для роутера три.

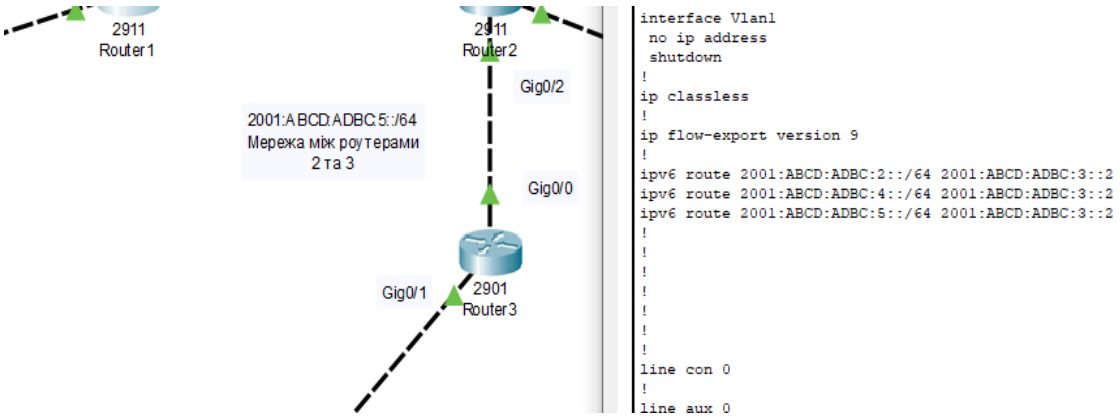

Рисунок 3.16 - Маршрут роутера один

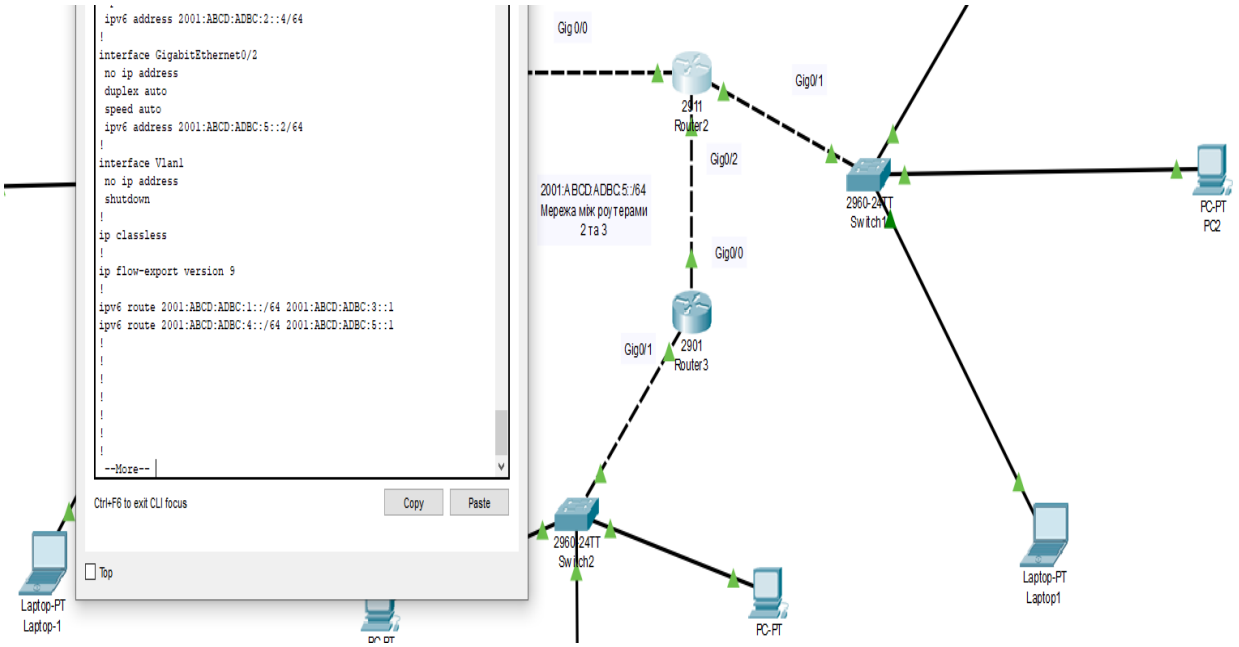

Рисунок 3.17 - Маршрут роутера два

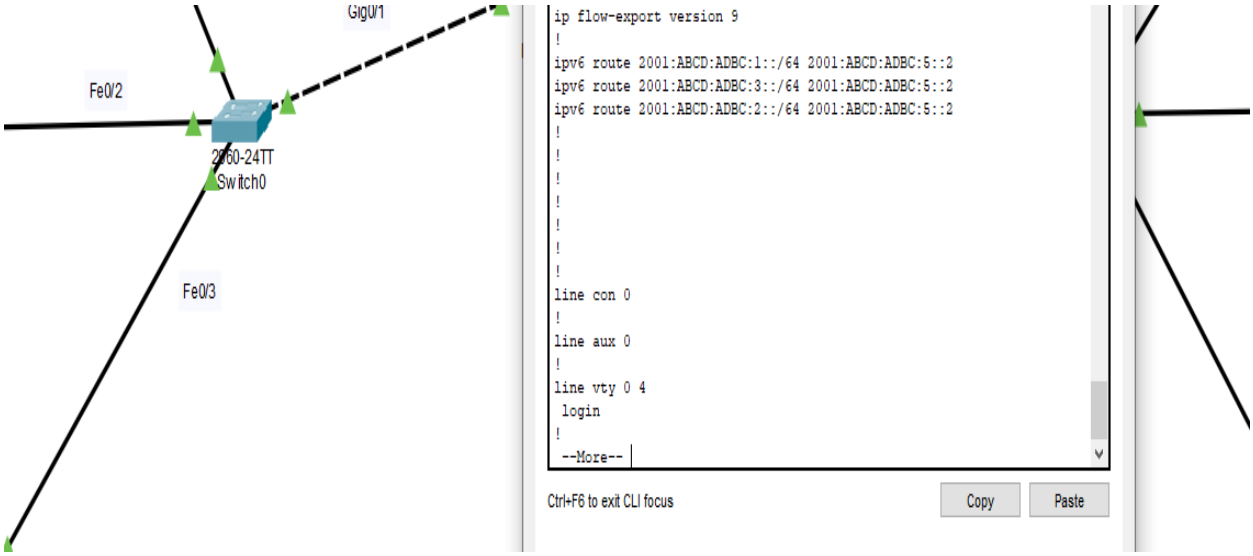

Рисунок 3.18 - Маршрут роутера три

Перегляд маршрутів здійснено за допомогою команди «show running-config».

Командою «ping» була здійснена перевірка роботи пристроїв різних мереж.

На рисунку 3.19 відображено виконання команди «ping» з комп’ютера «bux-2», що знаходиться у мережі чотири, на усі пристрої мережі один.

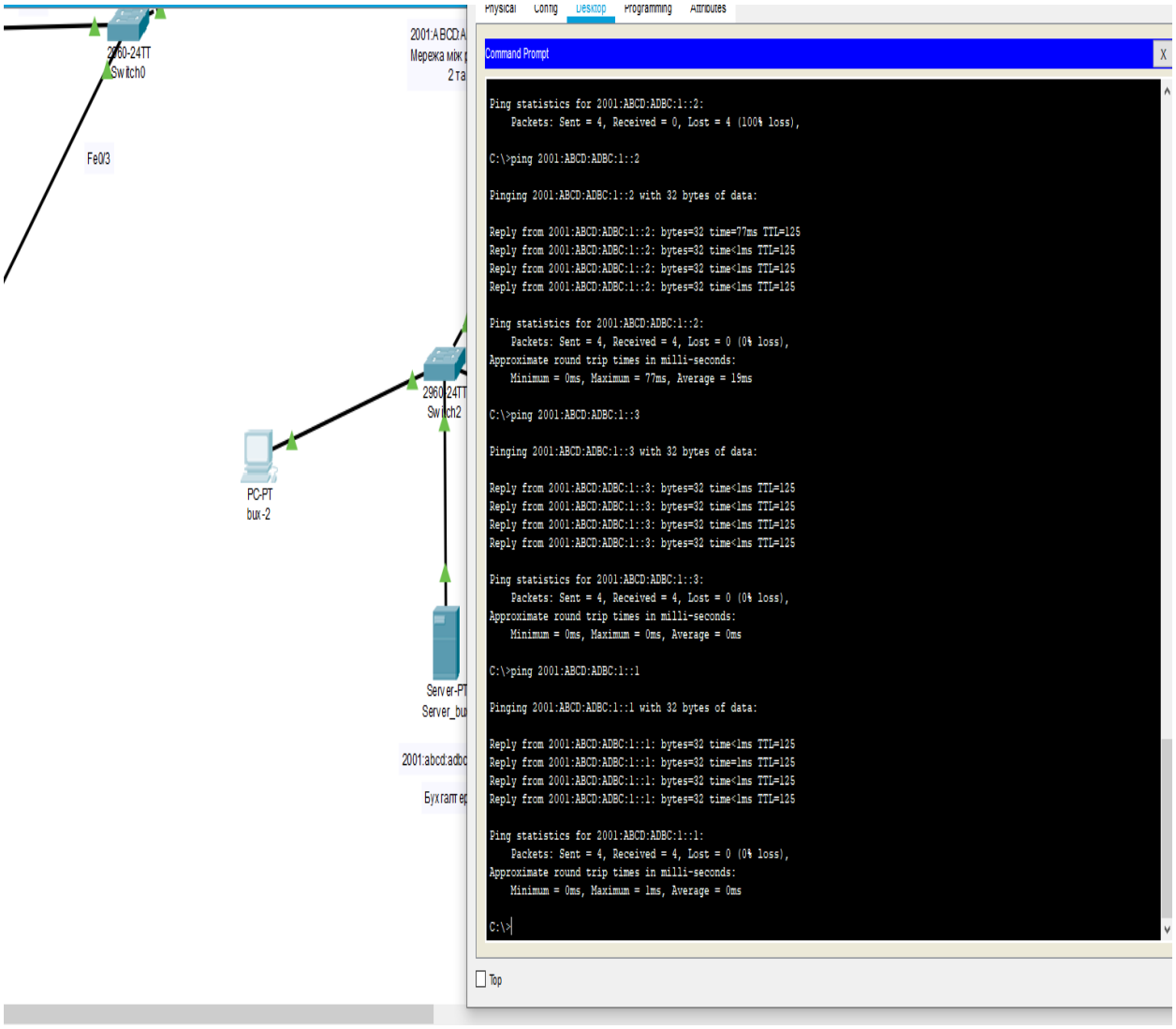

Рисунок 3.19 Ping з комп’ютера «bux-2» на пристрої мережі один

На рисунку 3.20 зображено виконання команди «ping» з комп’ютера «DT-1», що знаходиться у мережі один, на усі пристрої мережі чотири.

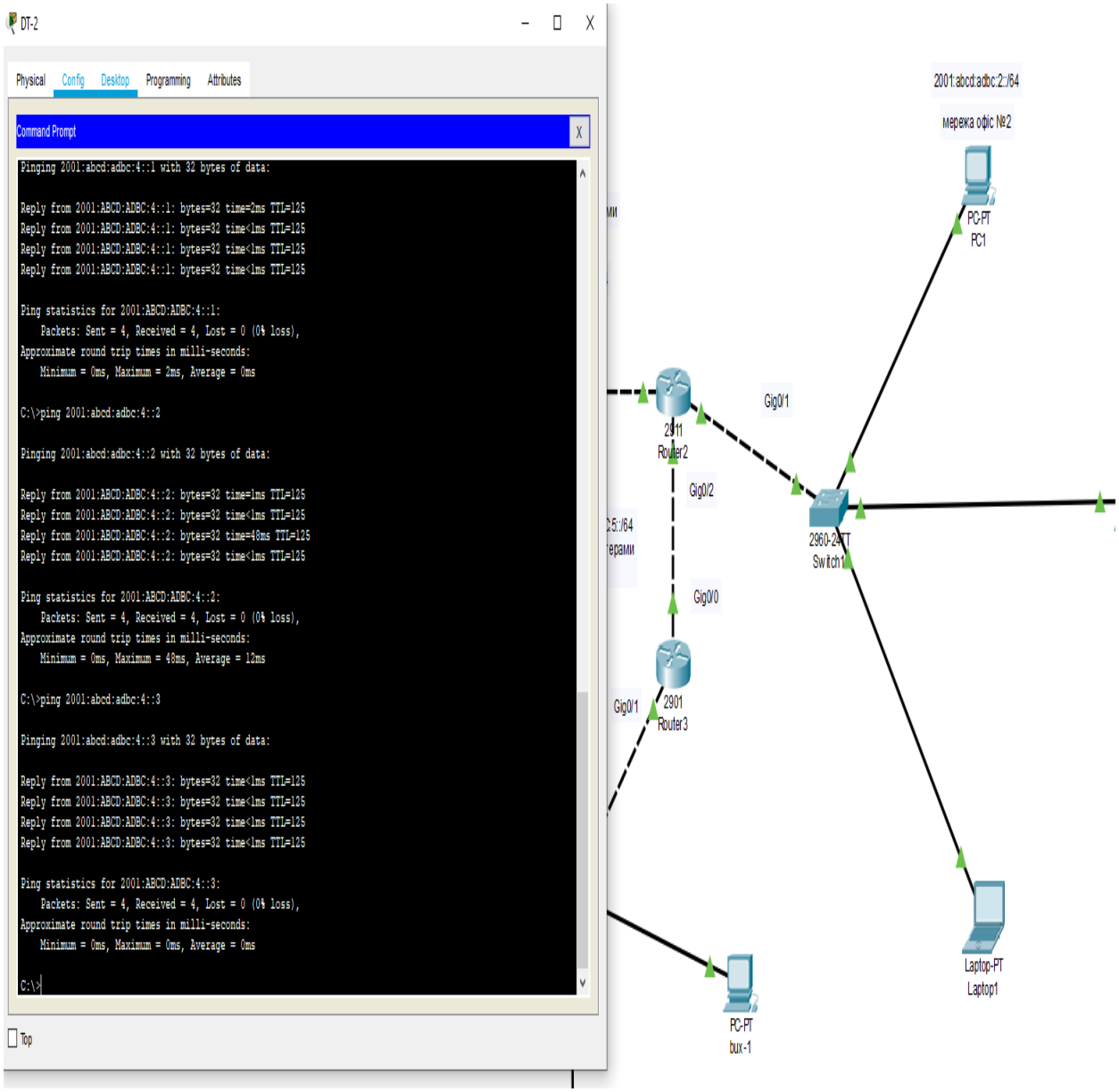

Рисунок 3.20 - Ping з мережі два пристроїв мережі «бухгалтерія»

Технічними умовами було вказано, що доступ до мережі «бухгалтерія» повинен бути лише з мережі один. Однак, після прокладання маршрутів, до мережі «бухгалтерія» мають доступ пристрої мережі два.

Перевірка командою «ping», яка спрямована на пристрої у мережі «бухгалтерія» з комп’ютера «PC1», який знаходиться у мережі два це підтверджує і відображене на рисунку 3.21.

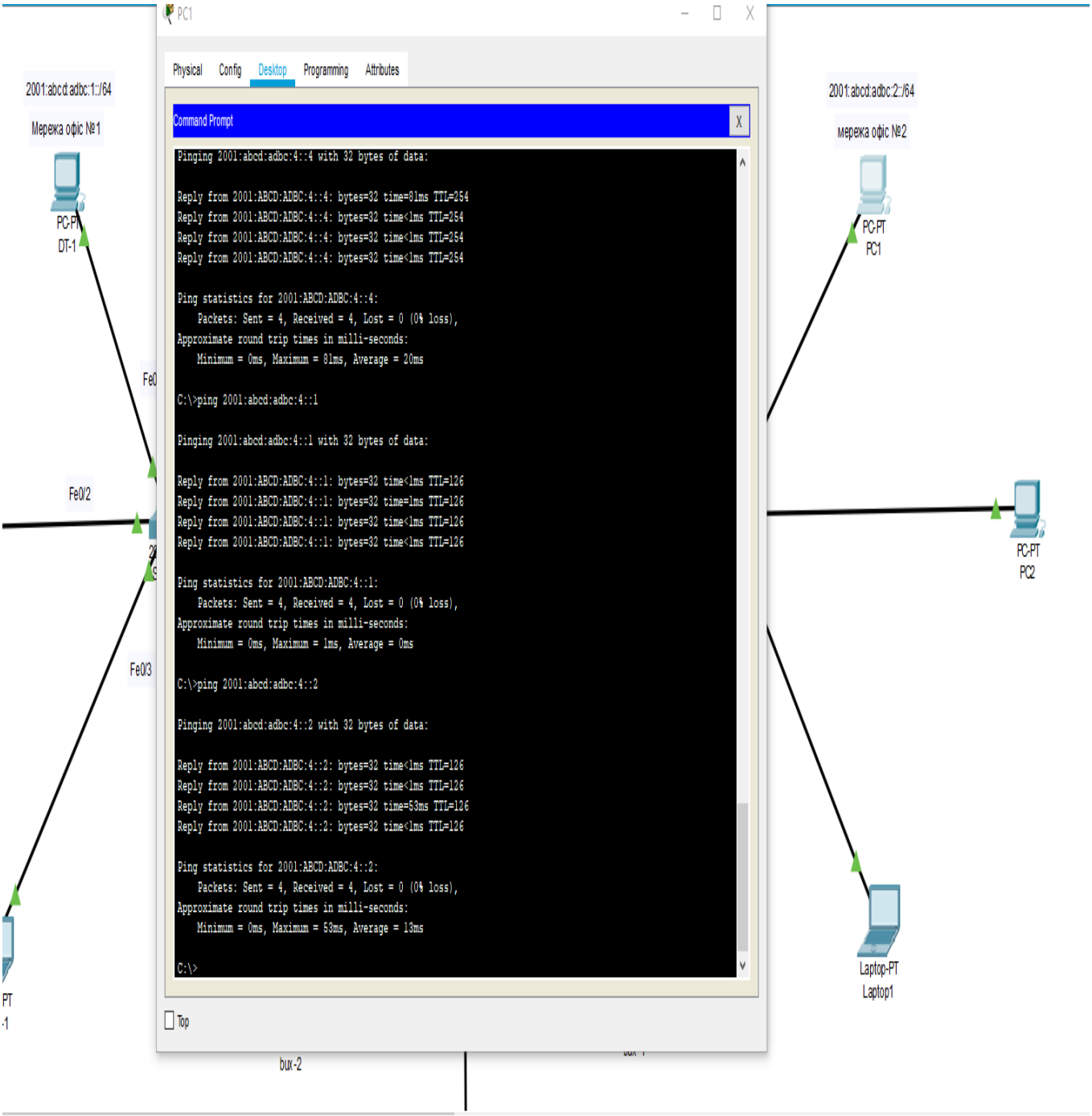

Рисунок 3.21 - Ping з мережі два пристроїв мережі «бухгалтерія»

3.2 Access lists для мережі з підтрикою IPV6

Для розмежування доступу до мережі були використані так звані «access lists».

Налаштування ACL для IPv4 відрізняється від IPv6. IPv6 не підтримує жодні списки окрім «іменних». Тому для початку роботи було створено список «net2». Зроблено це за допомогою команди «ipv6 access-list net2». До цього листа був внесений запис за допомогою команди «deny ipv6 2001:abcd:adbc:2::/64 any», який не дозволяє проходити трафіку з мережі «2001:abcd:adbc:2::/64» через порти роутера номер три.

Далі за допомогою команди «permit ipv6 any any» було дозволено проходити іншому трафіку, який не стосується мережі «2001:abcd:adbc:2::/64»

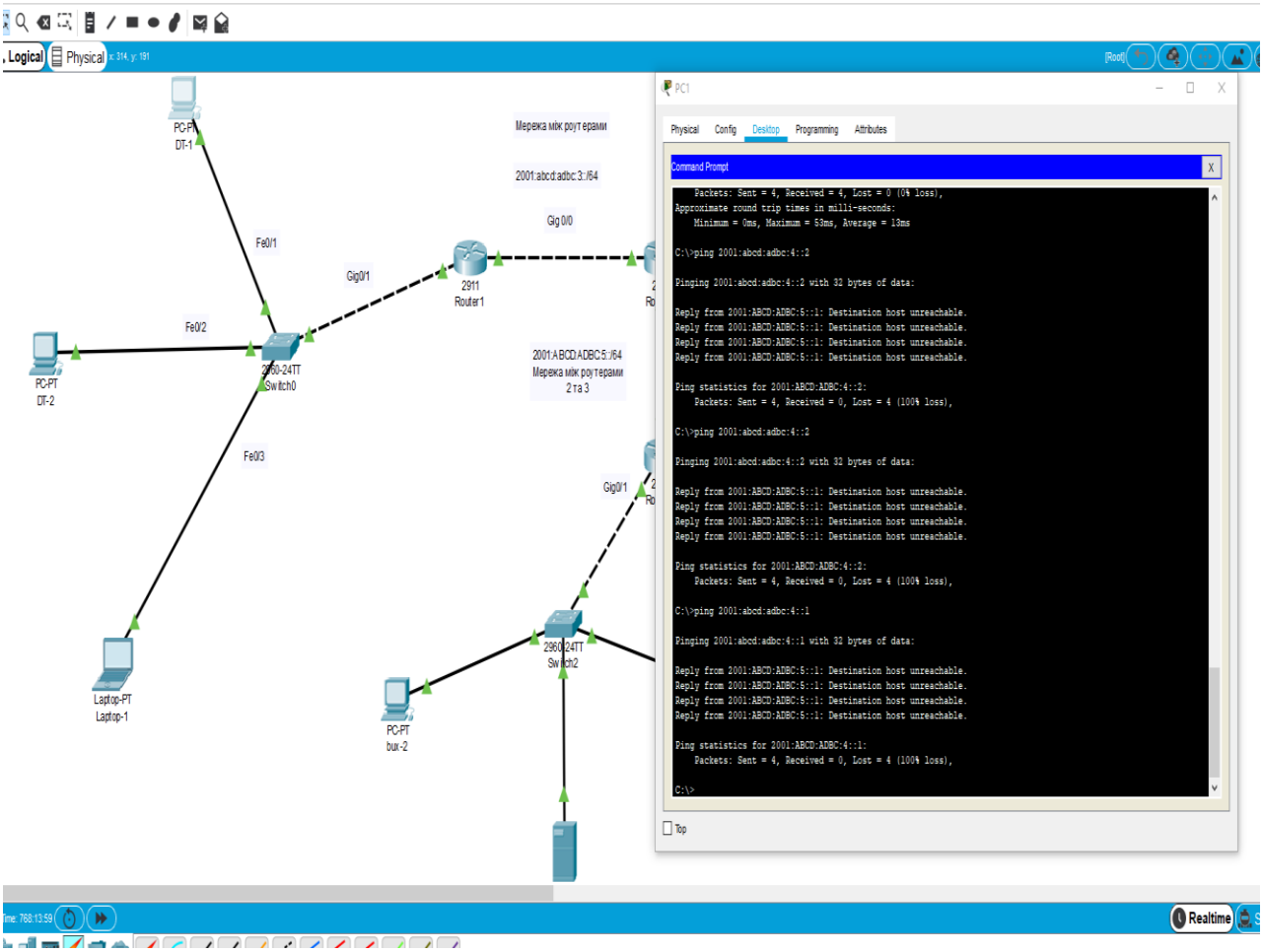

Рисунок 3.22 - Ping з мережі два пристроїв мережі «бухгалтерія»

На рисунку 3.22 була здійснена перевірка доступності пристроїв мережі «2001:abcd:adbc:4::/64» з комп’ютера «PC1» мережі «2001:abcd:adbc:2::/64» за допомогою команди «ping». На рисунку 3.22 чітко видно, що відповідь надходить від інтерфейсу роутера три про недоступність зазначеної адреси.

На рисунку 3.23 відображена перевірка доступності пристроїв мережі один, а на рисунку 3.24 – доступність пристроїв мережі два. Перевірка здійснювалась за допомогою команди «ping» з комп’ютера «PC1», який знаходиться у мережі два.

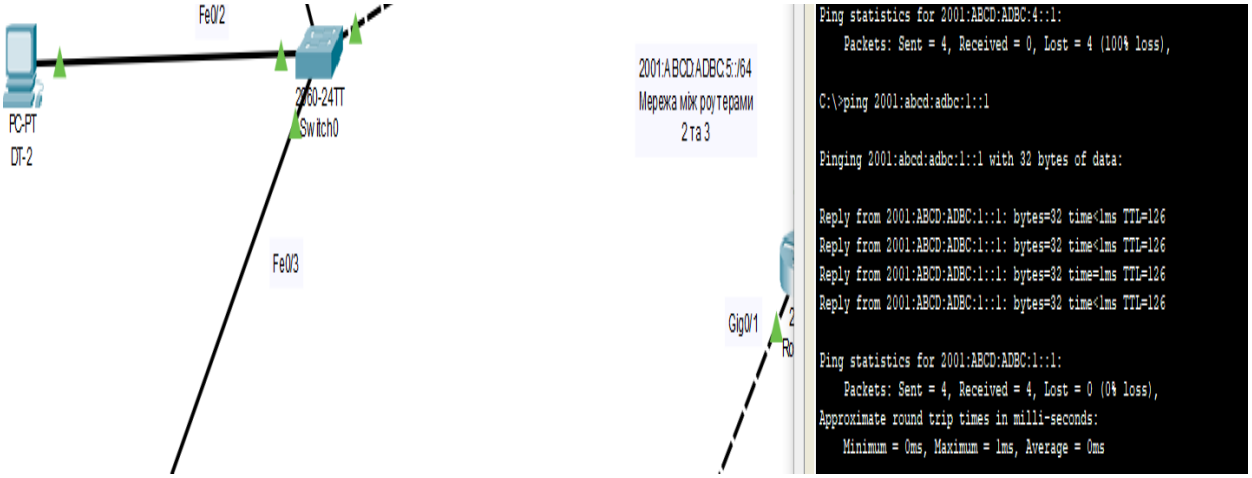

Рисунок 3.23 - Ping з мережі два пристроїв мережі один

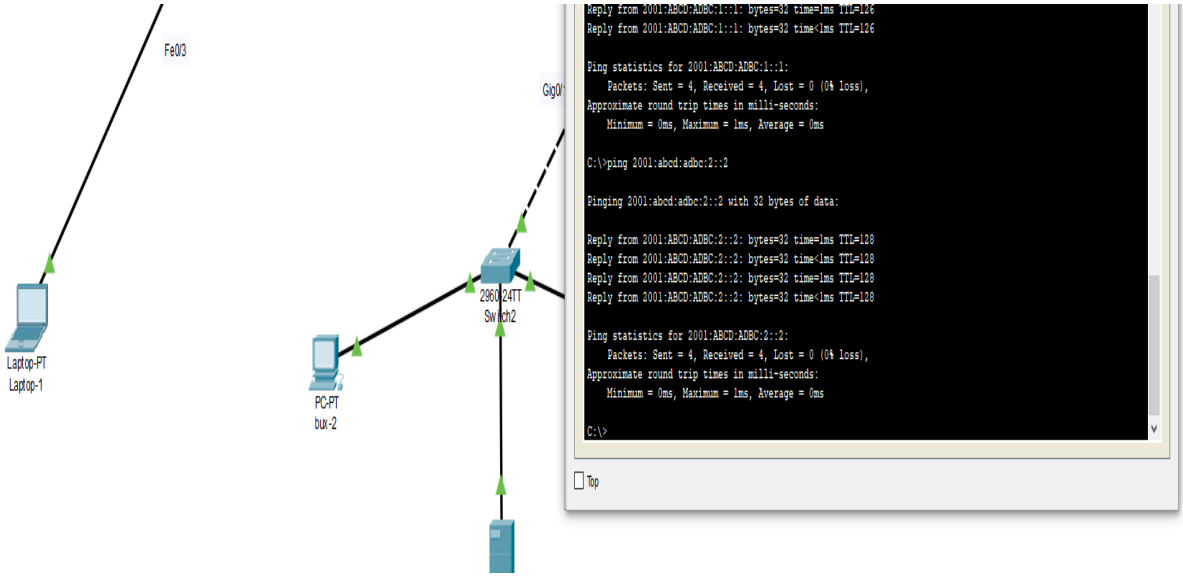

Рисунок 3.24 - Ping з мережі два пристроїв мережі два

Був отриманий наступний результат.

Мережа «бухгалтерія» закрита за допомогою налаштованого «access-list» від мережі два та усіх пристроїв що знаходяться у ній.

Наступним кроком була зроблена перевірка доступності мережі «бухгалтерія» з мережі один з комп'ютера «DT-1», якій знаходиться у мережі один.

На рисунку 3.25 відображена перевірка за допомогою команди «ping» на доступність усіх пристроїв мережі «бухгалтерія» з мережі один.

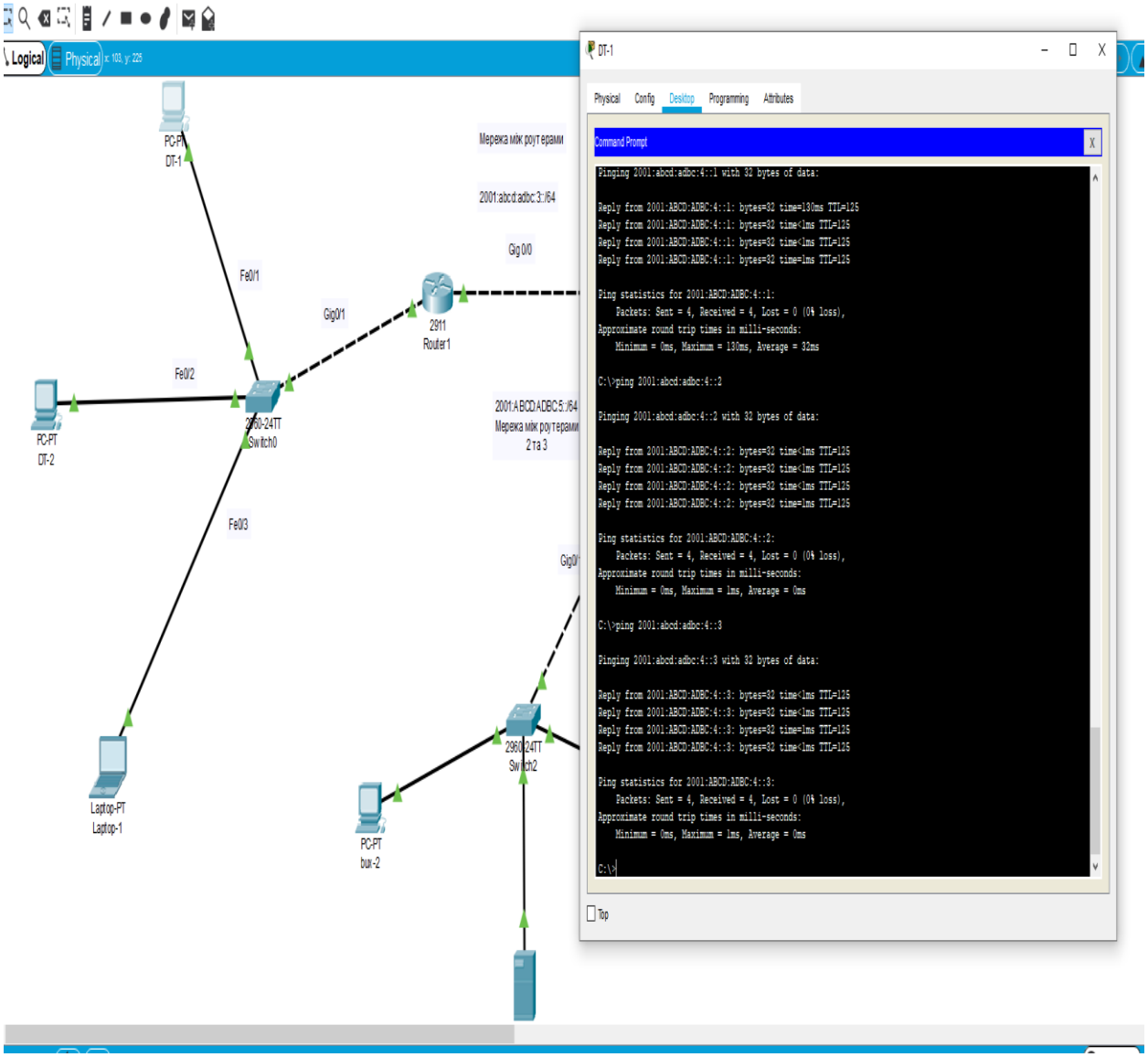

Рисунок 3.25 - Ping з мережі один пристроїв мережі «бухгалтерія»

На рисунку 3.26 відображена зворотна перевірка доступності пристроїв мережі один з мережі «бухгалтерія» за допомогою команди «ping» з пристрою «Server_bux».

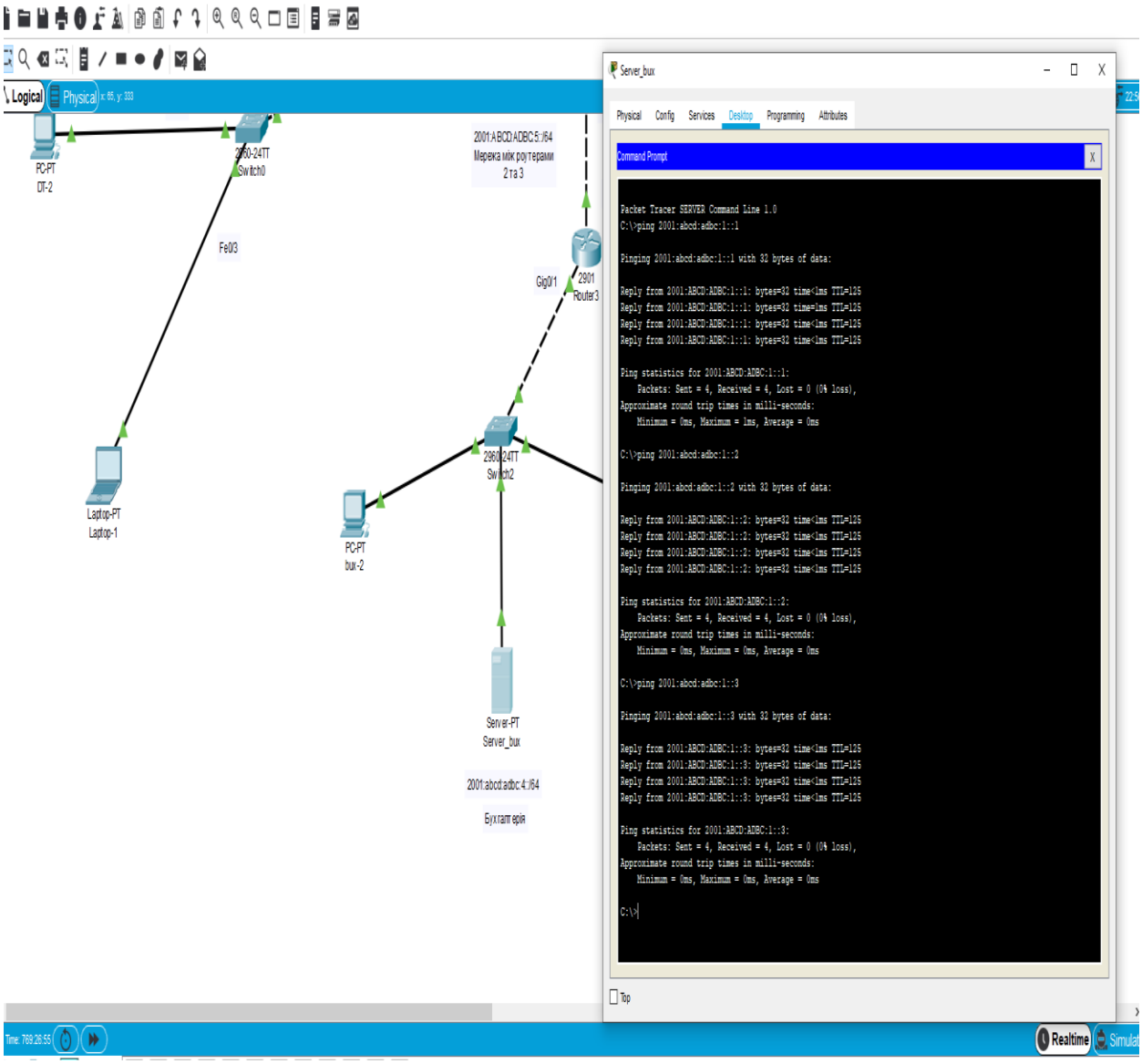

Рисунок 3.26 - Ping пристроїв мережі один

У результаті проведеної роботи з модулювання, створення та налагодження корпоративної мережі з трьох окремих, незалежних одна від іншої мереж, було створено діючу модель мережі на базі протоколу IPv6 з розділенням доступів на рівні маршрутизаторів.

ВИСНОВКИ

Провівши теоретичне дослідження за тематикою випускної роботи, можна зробити висновок, що розвиток мереж усіх різновидів здійснюється в бік зростання кількості об’єктів у них, а отже, важливість фактору більшої кількості адрес в IPv6 порівняно з IPv4 зростатиме. Швидке зростання кількості об’єктів в мережі Інтернет, зокрема під впливом новітніх трендів, як-от IoT, призводитиме до активного впровадження IPv6 у найближчі роки. Натомість у корпоративних мережах підприємств внаслідок їх більшої консервативності і контрольованості (що дає змогу зменшити вплив фактору нестачі адрес за рахунок ефективності централізованого адміністративного керування) використання IPv4 як базового протоколу збережеться протягом довшого часу. Передовсім це стосується вже існуючих мереж із розвинутою інфраструктурою на базі IPv4. Наявність технологій для взаємодії із зовнішніми ресурсами IPv6 також сприятиме тривалості використання підприємствами IPv4. Проте, оскільки зростання загальної частки IPv6 у мережах є невпинним, міграція мереж корпоративного сегмента з IPv4 до IPv6 є неминучою.

У ході роботи було отримано проект робочої схеми корпоративної мережі у симуляторі Cisco Packet Tracer 7 на базі протоколу IPv6. Перевірено, що усі компоненти мережі доступні і працюють за належною схемою. Розроблена модель показала високу продуктивність та легкість в налаштуванні у симуляторі Cisco Packet Tracer 7. Розроблена схема мережі є базовою, вона здатна приймати безліч трансформацій та модернізацій, щоб задовольняти сучасні потреби бізнесу.

СПИСОК ЛІТЕРАТУРИ

1. Крэйг Х. TCP/IP Network Administration 2016 - 816с
2. Академия Cisco [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://artemsannikov.ru/wp-content/uploads/2018/05/zagolovok-paketa-ipv4.jpg
3. Internet of Things Wiki [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://vignette.wikia.nocookie.net/iot-fpms/images/d/dd/Untitled3.png/
4. Таненбаум Э. С., Уэзеролл Д. Компьютерные сети. 5-е изд.2019 - 960с
5. Request for Comments: 1191. Path MTU Discovery [Електронний ресурс]. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc1191.
6. Hewlett Packard Enterprise Development LP [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3942_l3-ip-svcs_cg/content/images/image54.png
7. Wikimedia Commons [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://upload.wikimedia.org/wikipedia/commons/thumb/c/c7/NAT_Concept-en.svg/1200px-NAT_Concept-en.svg.png
8. Pearson [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://ptgmedia.pearsoncmg.com/images/art_wilkins_ipv6slaacconfig/elementLinks/thwilkins_fig01.jpg
9. Whatismyipaddress [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://cdn.whatismyipaddress.com/images-v4/cidr-notation.png
10. Nro [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.nro.net/wp-content/uploads/RIR-Map-Website-1024x576.jpg
11. Request for Comments: 4291. IP Version 6 Addressing Architecture [Електронний ресурс]. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc4291
12. State of IPv6 Deployment 2017 [Електронний ресурс]. – Internet Society, 25 May 2017. – Режим доступу до ресурсу: https://www.internetsociety.org/resources/doc/2017/state-of-ipv6-deployment-2017/
13. Request for Comments: 6586. Experiences from an IPv6-Only Network [Електронний ресурс]. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc6586.
14. Request for Comments: 3769. Requirements for IPv6 Prefix Delegation [Електронний ресурс]. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc3769.

15. Pattern: Microservice Architecture [Електронний ресурс]. – Режим доступу до ресурсу: http://microservices.io/patterns/microservices.html.
16. Nro [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.nro.net/wp-content/uploads/RIR-Map-Website-1024x576.jpg
17. Meola A. What is the Internet of Things (IoT)? [Електронний ресурс] / A. Meola. – Dec. 19, 2016. – Режим доступу до ресурсу: http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8.
18. CITIC Telecom CPC [Електронний ресурс]. – Режим доступу до ресурсу: https://www.citictel-cpc.com/editor/image/20190926/20190926092451_8418.png
19. Wikipedia [Електронний ресурс]. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/BGP
20. Wilkins S. IPv6 Translation and Tunneling Technologies [Електронний ресурс]. / S. Wilkins. – Cisco Press, Jun 26, 2013. – Режим доступу до ресурсу: http://www.ciscopress.com/articles/article.asp?p=2104947.
21. Лаборатория "Обработки и передачи данных" [Електронний ресурс]. – 2018 – Режим доступу до ресурсу: http://opds.spbsut.ru/ecourse/2016ipv6proto/data/_uploaded/image/%21%21.png
22. Researchgate [Електронний ресурс]. – Режим доступу до ресурсу: https://www.researchgate.net/profile/Gabor_Lencse/publication/273030287/figure/fig1/AS:670039900422153@1536761369366/Operation-of-DNS64-NAT64-Based-on-11-3-The-examined-NAT64-implementations-31.png
23. NAT64–Stateless versus Stateful [Електронний ресурс]. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676277.html.
24. Request for Comments: 4966. Reasons to Move the Network Address Translator – Protocol Translator (NAT-PT) to Historic [Електронний ресурс]. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc4966.
25. Ppt-online [Електронний ресурс]. – Режим доступу до ресурсу: https://cf.ppt-online.org/files/slide/0/0niRBuOVLeIzPo9YCN81dq3kvsQcZDSfEtxj4W/slide-44.jpg
26. Cisco [Електронний ресурс]. – Режим доступу до ресурсу: https://www.cisco.com/c/dam/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc2.gif
27. IAB Statement on IPv6 [Електронний ресурс]. – Режим доступу до ресурсу: https://www.iab.org/documents/correspondence-reports-documents/2016-2/iab-statement-on-ipv6/

28. Tiso J. Designing Cisco Network Service Architectures (ARCH). Foundation Learning Guide / John Tiso. – Third Edition. – Cisco Press, 2012. – 698 p.
29. Rtcloud [Електронний ресурс]. – Режим доступу до ресурсу: https://www.rtcloud.ru/wp-content/uploads/2016/11/Site-to-Site-VPN.png
30. Крэйг Х. TCP/IP Network Administration 2016 - 816с
31. Request for Comments: 1918. Address Allocation for Private [Електронний ресурс]. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc1918
32. Tarkoma S. Overlay Networks: Toward Information Networking / S. Tarkoma. – Auerbach Publications, 2010. – ISBN 9781439813713 – CAT# K10708.