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

Секція інформаційно-комунікаційних технологій

КОМПЛЕКСНА КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему: «Графічний інтерфейс інтелектуальної системи керування трансляцією мережевих адрес на основі протоколу NAT»

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

Керівник роботи **Великодний Д. В.**

Студент гр. Ін.м-81н **Василенко М. Ю.**

СУМИ 2020

Сумський державний університет

Факультет *ЕлІТ* Кафедра *Комп'ютерних наук*

Спеціальність *122 – Комп'ютерні науки*

Затверджую:
зав. кафедрою комп'ютерних наук
_____ А.С. Довбиш
"_____"_____ 2020р.

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТОВІ

Василенку Максиму Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) *Графічний інтерфейс інтелектуальної системи керування трансляцією мережевих адрес на основі протоколу NAT*
затверджую наказом по університету від "____" _____2020 р. № _____
2. Термін здачі студентом закінченого проекту (роботи)_____
3.Вхідні данні до проекту (роботи)

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)
1) огляд існуючих рішень та постановка задачі;
2) моделювання протоколів NAT з використанням симулятора Packet Tracer;
3) графічний інтерфейс налаштування протоколу NAT.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання_____

Керівник _____

(підпис)

Завдання прийняв до виконання _____

(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проекту (роботи)	Термін виконання проекту (роботи)	Примітка
1	Огляд існуючих рішень та постановка задачі		
2	Моделювання протоколів NAT з використанням симулятора Packet Tracer		
3	Створення графічного інтерфейсу налаштування протоколу NAT		
4	Оформлення магістерської кваліфікаційної роботи		

Студент-дипломник _____

(підпис)

Керівник проекту _____

(підпис)

РЕФЕРАТ

Записка: 43 стор., 24 рис., 1 додаток, 11 джерел.

Мета роботи – дослідження протоколу NAT і засобів розробки систем управління комп’ютерними мережами та розробка автоматизованої інформаційної системи управління мережевими сервісами.

Об'єктом дослідження є комп’ютерні мережі на базі роутерів з налаштованим на них протоколом NAT.

Предметом дослідження є процес управління сервісами NAT е комп’ютерних мереж передачі даних на базі технології Ethernet.

Методи досліджень. Для вирішення поставлених задач використано методи системного аналізу та імітаційного моделювання.

Результати — спроектовано та розроблено систему управління мережевими сервісами в мережах Ethernet на базі протоколу NAT. Систему реалізовано у формі веб-додатку з використанням мов програмування Java та JavaScript.

СИСТЕМА УПРАВЛІННЯ МЕРЕЖВИМИ СЕРВІСАМИ,
ETHERNET, ВЕБ-ДОДАТОК, ГРАФІЧНИЙ ІНТЕРФЕС,
ІНТЕЛЕКТУАЛЬНА МЕРЕЖА, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

ЗМІСТ

ВСТУП

NAT − це механізм в мережах TCP/IP, що дозволяє перетворювати IP-адреси транзитних пакетів і використовується в основному для реалізації двох основних задач: розширення діапазону IP-адрес стандарту v4 та приховування структури внутрішньої мережі від зовнішнього світу шляхом перетворення запитів від внутрішніх ПК на запити від пограничного роутера компанії.

На сьогоднішній день користувачам локальної мережі недостатньо IP-адреси, тому нам на допомогу приходить технологія NAT, вона дозволяє з економити велику кількість IP-адрес, саме тому цю технологію використовують великі компанії, офіси , учбові заклади.

Але в даній технології є недоліки. Головним недоліком є однобічний зв’язок внутрішньої мережі з мережею Інтернет. Тобто комп’ютер може запросити контент з мережі Інтернету, але самі з зовнішнього світу будуть недоступні. Оскільки крім зовнішньої IP-адреси 50.0.0.1 зовнішнім вузлам потрібно знати ще й значення відповідного TCP/ UDP сесії, який постійно змінюється.

У роботі практично реалізовані чотири різних варіанта налаштування технології NAT: «Налаштування динамічного NAT», «Налаштування динамічного NAT на пул зовнішніх IP-адрес», «Налаштування динамічного і статичного NAT», «Налаштування технології NAT з використанням Port Forwarding». Приведено їх переваги та недоліки, а також рекомендації до їх використання при налаштуванні комп’ютерних мереж.

1 ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

1.1 Характеристики технології Network Address Translation (NAT)

NAT – це протокол, який перетворює внутрішню IP-адресу локальної мережі, у адресу зовнішньої мережі і навпаки. Механізм NAT описаний в RFC 1631, RFC 3022. Перетворення адрес даною технологією виконується майже будь-яким маршрутизатором, який підключає комп’ютер до мережі Інтернет. Коли інші комп’ютери в Інтернеті намагаються отримати доступ до комп’ютерів у локальній мережі, вони бачать лише IP-адресу маршрутизатора, що дозволяє забезпечити додатковий рівень безпеки, оскільки маршрутизатор може бути налаштований як брандмауер, дозволяючи лише авторизованим системам отримувати доступ до комп’ютерів у мережі. Після того, як системі із зовнішньої мережі було дозволено отримати доступ до комп’ютера всередині мережі, IP-адреса переводиться з адреси маршрутизатора на унікальну адресу комп’ютера. Адреса знаходиться у «таблиці NAT», яка визначає внутрішні IP-адреси комп’ютерів у мережі і визначає глобальну адресу, яку бачать комп’ютери інших мереж. Незважаючи на те, що кожен комп’ютер у локальній мережі має певну IP-адресу, зовнішні системи можуть бачити лише одну IP-адресу під час підключення до будь-якого з комп'ютерів у межах мережі [1].

1.1.1 Використання IPv4-адрес

Всі IPv4-адреси можна розділити на дві основні групи: глобальні (публічні), цю групу також можна назвати «WAN-адресами» – це адреси, які використовуються в Інтернеті; приватні або локальні – це адреси використовуються у локальній мережі (LAN). Існують також адреси спеціального використання, призначені для технічних цілей, таких як функції протоколу тощо. Як правило, вони взагалі не розподіляються для звичайних користувачів мережі [2].

Дослідження, у рамках проблеми вичерпання адресного простору протоколу IPv4 , показали, що багато організацій, які брали IP-адресацію, не підключені до Інтернету. Тому в 1994 році проблемна група проектування Інтернету (Internet Engineering Task Force, IETF) запропонувала виділити діапазон IP-адрес для приватних мереж. У результаті для внутрішнього застосування були зарезервовані три блоки IP-адрес:

- 10.0.0.0 – 10.255.255.255/8 (16777216 хостів);
- 172.16.0.0 – 172.31.255.255/12 (1048576 хостів);
- 192.168.0.0 – 192.168.255.255/16 (65536 хостів).

Приватні IP-адреси (сіра IP-адреса) є внутрішньо мережевими і будь-яка організація має право використовувати їх на свій розсуд без будь-якої реєстрації, тобто одна і та сама адреса, яка є унікальною у даній мережі, може бути призначена іншому пристрою в інший локальній мережі. Пакети, які використовують ці адреси у якості джерела або призначення, не повинні з’являтися в публічному Інтернеті. Маршрутизатор або пристрій мережевого доступу по периметру цих приватних мереж повинні блокувати або перетворювати ці адреси. Приватні адреси визначені в документі RFC 1918 «Присвоєння адрес для приватного Інтернету» [3-5].

Публічні (білі) IP-адреси маршрутизуються в Інтернеті, на відміну від приватних адрес. Наявність публічної IP-адреси на маршрутизаторі чи комп’ютері дозволяє організувати власний сервер (VPN, FTP, WEB тощо), віддалений доступ до комп’ютера, камери відеоспостереження та доступ до них з будь-якої точки глобальної мережі. Маючи загальнодоступну IP-адресу можна налаштувати будь-який домашній сервер для публікації в Інтернеті: Web (HTTP), VPN (PPTP / IPSec / OpenVPN), медіа (аудіо / відео), FTP, мережевий накопичувач NAS, ігровий сервер, тощо. Усі сервери та сайти в Інтернеті використовують загальнодоступні IP-адреси (наприклад, google.com – 172.217.22.14, DNS-сервер Google – 8.8.8.8). Усі загальнодоступні IP-адреси в Інтернеті унікальні для свого хоста або сервера і не можуть дублювати

призначення. Для домашніх користувачів провайдер може надати лише одну або декілька публічних IP-адрес (як правило, це платна послуга) .

Маршрутизатор, що підтримує NAT, підтримує IPv4, щоб пристрої домашньої мережі використовували одну і ту ж загальнодоступну IP-адресу, яку система отримала від постачальника в WAN-інтерфейсі пристрою для підключення до Інтернету. Саме ця зовнішня загальнодоступна IP-адреса може використовуватися і для доступу до домашнього комп'ютера з Інтернету, але для цього необхідно встановити переадресацію портів на маршрутизаторі [3-5].

На рисунку 1 представлено маршрутизацію з локальних мереж в Інтернет.

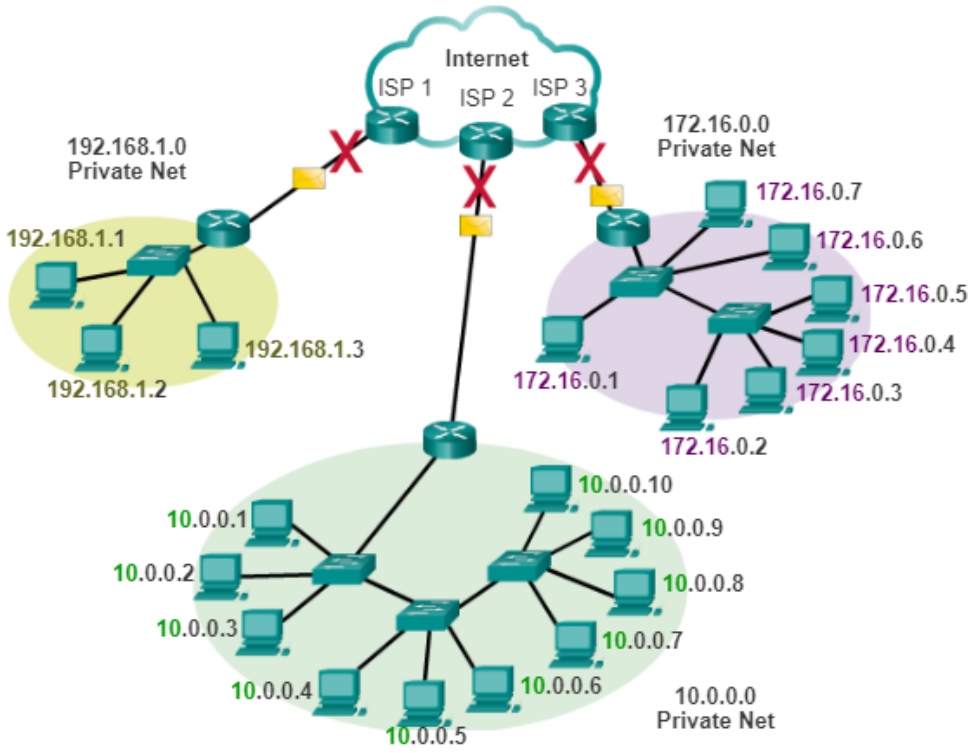


Рисунок 1 – Маршрутизація приватних адрес в Інтернет [6]

1.1.2 Термінологія NAT

У термінології NAT внутрішня мережа це набір мереж, що підлягають трансляції, а зовнішня мережа відноситься до всіх інших мереж. При використанні NAT, адреси IPv-4 мають різні позначення, залежно від того до якої

з мереж вони належать, до локальної або зовнішньої, і чи є трафік вхідним або вихідним. NAT включає в себе чотири типи адрес:

- внутрішня локальна адреса (Inside local address) – адреса джерела, видима з внутрішньої мережі;
- внутрішня глобальна адреса (Inside global address) – адреса джерела, видима із зовнішньої мережі;
- зовнішня локальна адреса (Outside local address) – адреса одержувача, видима з внутрішньої мережі;
- зовнішня глобальна адреса (Outside global address) – адреса адресата, видима із зовнішньої мережі.

При визначенні того, який тип адреси використовується, важливо пам'ятати, що термінологія NAT завжди застосовується з точки зору пристрою з трансльованою адресою:

- внутрішня адреса (Inside address) – адреса пристрою, яка транслюється NAT;
- зовнішня адреса (Outside address) – адреса пристрою призначення;
- локальна адреса (Local address) – це будь-яку адреса, яка відображається у внутрішній частині мережі;
- глобальна адреса (Global address) – це будь-яка адреса, яка відображається в зовнішній частині мережі [7].

Розглянемо це на прикладі схеми (рис.2):

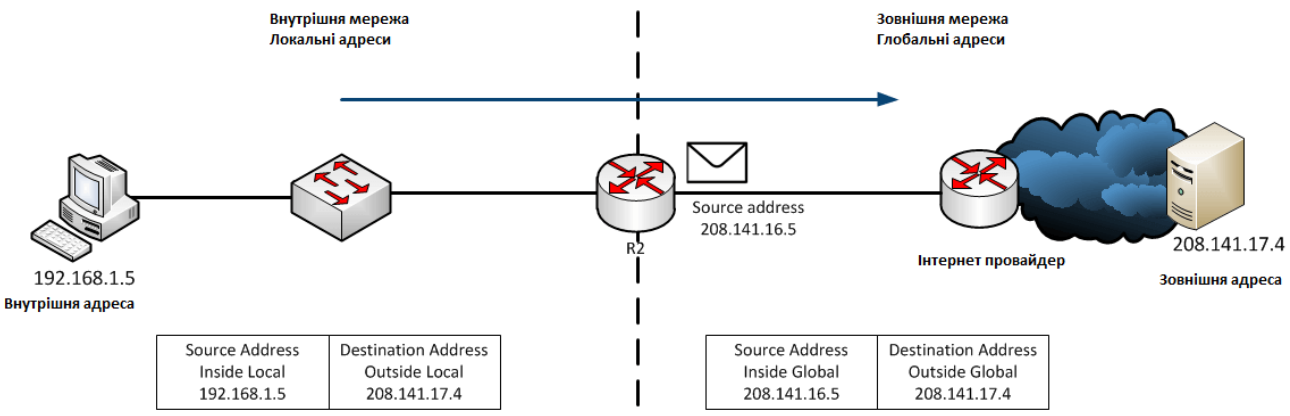


Рисунок 2 – Схематичне зображення перетворення

На рисунку ПК має внутрішню локальну адресу 192.168.1.5, а веб-сервер має зовнішню адресу 208.141.17.4. Коли з ПК відправляються пакети на глобальну адреса веб-сервера, внутрішня локальна адреса ПК транслюється в 208.141.16.5. Адреса зовнішнього серверу зазвичай не транслюється, оскільки він має загальнодоступну IPv-4 адресу. ПК має різну локальну і глобальну адреси, тоді як веб-сервер має однаковий публічну IP-адресу. З його точки зору трафіка, що виходить із ПК надходить з внутрішньої глобальної адреси 208.141.16.5. На рисунку показано як трафік відправляється з внутрішнього ПК на зовнішній веб-сервер, через маршрутизатор з підтримкою NAT.

1.1.3 Функції NAT

Технологія NAT виконує наступні функції:

- перетворення внутрішніх локальних адрес;
- поєднання внутрішніх глобальних адрес;
- застосування розподілу навантаження TCP;
- перекриття мереж.

Перетворення внутрішніх локальних адрес – це механізм об’єднання двох мереж на маршрутизаторі. Протокол NAT транслює локальні, неприпустимі для використання в Інтернеті, IP-адреси у зареєстровані IP-адреси перед переміщенням пакетів з локальної мережі в Інтернет або в іншу зовнішню мережу. Для цього NAT виконує наступний алгоритм перетворень:

1. Користувач (рис.2) з IP-адресою 192.168.1.5 надсилає пакет і намагається встановити з’єднання з мережею 208.141.17.4.

2. Коли на граничний маршрутизатор NAT приходить перший пакет, маршрутизатор перевіряє, чи є запис адреси джерела, який збігається з адресою в таблиці.

3. Якщо в таблиці NAT запис адреси джерела збігається з адресою в таблиці, починається етап 4. Якщо відповідність не знаходиться, маршрутизатор NAT використовує простий запис зі свого пулу зареєстрованих Інтернет адрес. Простий запис відбувається тоді, коли маршрутизатор NAT зіставляє внутрішню

IP-адресу з публічною, допустимою IP-адресою в мережі Інтернет. У даному прикладі маршрутизатор NAT співставляє адреси 192.168.1.5 з адресою 208.141.16.5.

4. Граничний маршрутизатор NAT змінює локальну адресу 192.168.1.5 (вихідна адреса пакета) на адресу 208.141.16.5.

5. Коли в Інтернеті використовується вузол з IP-адресою 208.141.17.4, він використовує у якості кінцевої адреси виділену маршрутизатор NAT IP-адресу 208.141.16.5.

6. Коли граничний маршрутизатор NAT отримує відповідь від 208.141.17.4 з пакетом, призначеним для 208.141.16.5, він знову перевіряє свою таблицю NAT. Таблиця показує, що внутрішня адреса 192.168.1.5 має отримати пакет, призначений для 208.141.16.5, і замінює адресу призначення на IP-адресу внутрішнього інтерфейсу. Дії 2-6 повторюються для кожного пакета.

Поєднання внутрішніх глобальних адрес дозволяє маршрутизаторам використовувати одну глобальну адресу для багатьох локальних адрес, і таким чином можна заощадити адреси пулу внутрішніх глобальних адрес. Коли увімкнено поєднання NAT, маршрутизатор підтримує в таблиці NAT відомості протоколу вищого рівня для номерів портів TCP і UDP, щоб перетворювати глобальну адресу в потрібну внутрішню локальну адресу. Коли кілька локальних адрес відповідають одній глобальній адресі, NAT використовує номер порту TCP або UDP кожного внутрішнього вузла. Таким чином, створюється унікальна адреса внутрішньої мережі. Схема адресації портів допускає одночасне використання однієї внутрішньої глобальної IP-адреси приблизно 4000 різними вузлами, завдяки численним наявним номерам портів TCP і UDP.

Розподіл навантаження TCP – це динамічний спосіб перетворення цільових IP-адрес. Його можна застосувати для зіставлення певного трафіку зовнішньої мережі з допустимим трафіком внутрішньої мережі, призначеним більш ніж для одного вузла. Після створення структури зіставлення цільові IP-адреси, які мають відповідності в списку доступу, змінюються на адресу з пулу адрес по циклічній схемі. Коли створюється нове з’єднання із зовнішньої мережі

з внутрішньою мережею, увесь трафік що не відноситься до TCP проходить без перетворення, якщо тільки до інтерфейсів не застосований інший вид трансляції.

Перекриття мереж

При перетворенні перекриваються адрес проводяться наступні дії.

1. Вузол внутрішньої мережі ініціює з’єднання з вузлом зовнішньої мережі за допомогою повного доменного імені, запитуючи перетворення ім'я-адреса на сервері доменних імен Інтернету DNS.

2. Граничний маршрутизатор NAT приймає відповідь сервера DNS і починає процес перетворення з виданими адресами, якщо є адреси які перекриваються.

3. Для трансляції повернутої адреси граничний маршрутизатор створює простий запис перетворення. Він зіставляє адресу яка перекривається у внутрішній мережі з адресою з пулу адрес, які можуть використовуватися у зовнішній мережі.

4. Граничний маршрутизатор NAT змінює адресу джерела на нову внутрішню глобальну адресу, а адресу призначення на зовнішню глобальну адресу і пересилає пакет. Вузол зовнішньої мережі отримує пакет і продовжує діалог. Для кожного пакету, отриманого між внутрішнім і зовнішнім вузлами, маршрутизатор виконує перегляд таблиці NAT, змінює адресу призначення на внутрішню локальну адресу і вихідну адреса на зовнішню локальну адресу.

1.2 Механізми перетворення IP-адрес

Існує 3 основних механізми перетворення мережевих адрес [8]:

− статичне перетворення (SAT, Static Network Address Translation) – взаємно-однозначна відповідність між локальними і глобальними адресами;

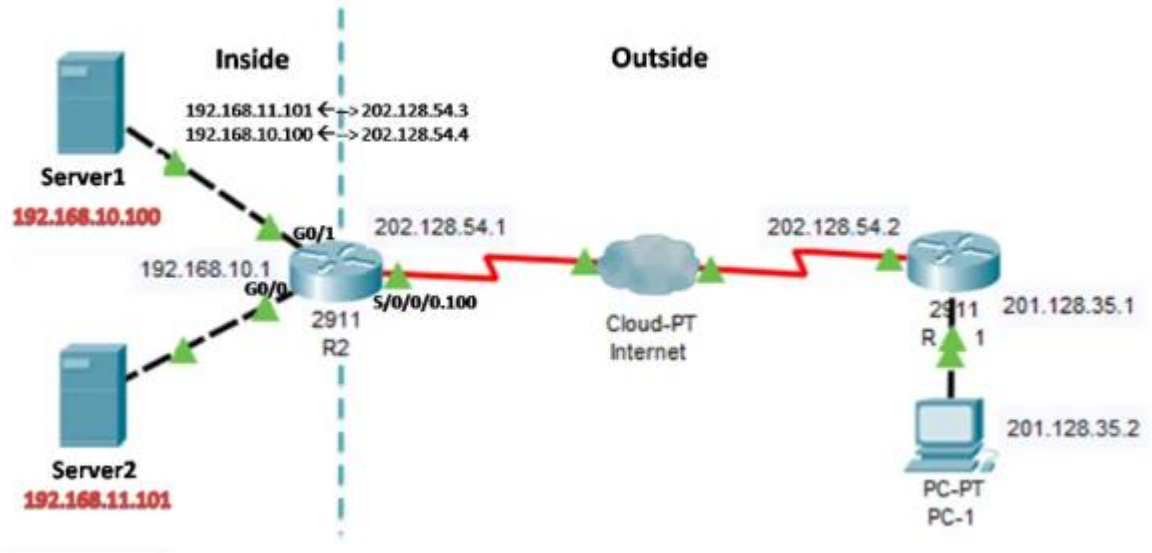
− динамічне перетворення (DAT, Dynamic Address Translation) – співставлення адрес за схемою «багато до багатьох» між локальними і глобальними адресами;

− перетворення адрес портів (NAPT, NAT Overload, PAT) – співставлення адрес за схемою «багато до одного» між локальними і глобальними адресами.

Розглянемо більш детально кожний із видів перетворення адрес.

1.2.1 Статичний NAT

Для статичного NAT схему співставлення локальних і глобальних адресе виконує адміністратор мережі. Даний метод доцільно використовувати для веб-серверів або приладів, які повинні мати постійну Інтернет-адресу. Іншим прикладом може бути робота приладів, які мають бути доступними постійно для авторизованих користувачів мереж поза межами локальної мережі, але при цьому має залишатись закритим для загального доступу через інтернет. Для даної технології необхідна достатня кількість публічних адрес, які доступні для загальної кількості користувачів при одночасних сеансах.

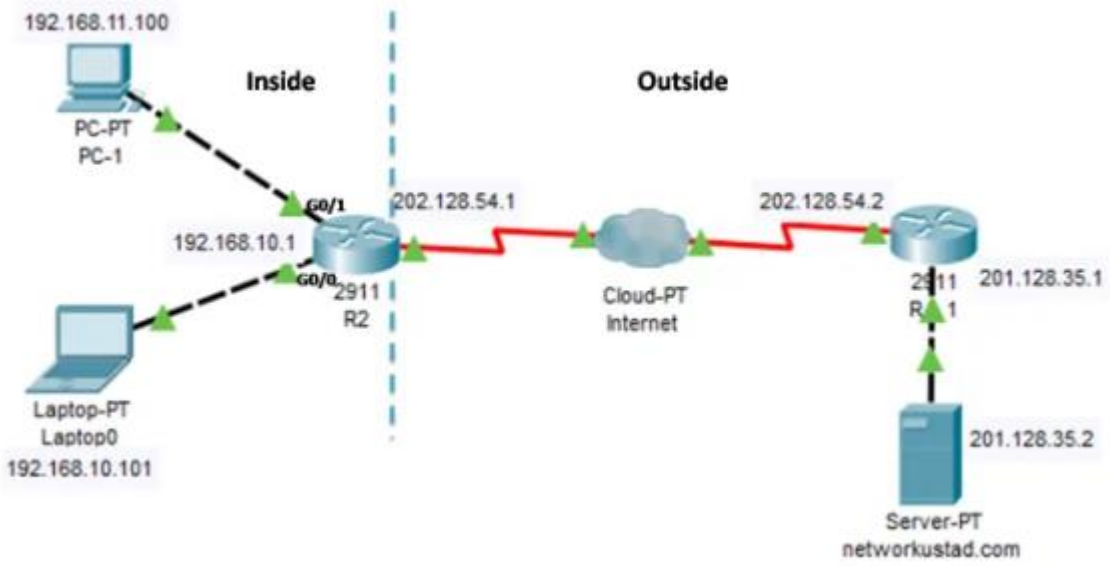



```
R2#
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  202.128.54.3      192.168.10.101     ---                ---
---  202.128.54.4      192.168.11.100     ---                ---
tcp 202.128.54.3:80    192.168.10.101:80  201.128.35.2:1025  201.128.35.2:1025
tcp 202.128.54.4:80    192.168.11.100:80  201.128.35.2:1026  201.128.35.2:1026
```

Рисунок 3 – Приклад мережі та результат пінгування мережі зі статичним NAT [9]

1.2.2 Динамічний NAT

Динамічне перетворення мережевих адрес означає використання пулу публічних адрес, які присвоюються почергово, у порядку нових запитів. Якщо для пристрою у внутрішній мережі необхідно вихід у зовнішню мережу, то для нього привласнюється доступна публічна адреса з пулу.




```
R2#
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 202.128.54.3:48   192.168.11.100:48  201.128.35.2:48    201.128.35.2:48
icmp 202.128.54.3:49   192.168.11.100:49  201.128.35.2:49    201.128.35.2:49
tcp 202.128.54.3:1029  192.168.11.100:1029201.128.35.2:80    201.128.35.2:80
```

Рисунок 4 – Приклад мережі та результат пінгування мережі з динамічним NAT [9]

1.2.3 Перетворення адрес портів (PAT)

Дана технологія широко застосовується домашніми маршрутизаторами і базується на співставленні кількох приватних IPv4-адрес у одну публічну. Інтернет-провайдер призначає маршрутизатору одну публічну адресу, проте до мережі мають доступ усі під’єднані до нього пристрої. Реалізація такого співставлення реалізується через відстежування приватних адрес за номерами портів. Коли пристрій починає сеанс TCP/IP створюється значення порту TCP або UDP для джерел, для того щоб унікально визначити сенс. Технологія PAT гарантує, що пристрої використовують різні номери портів TCP для кожного

виходу в Інтернет. Коли від серверу приходить відповідь номер порту джерела, визначається номер порту призначення і таким чином визначається пристрій, якому маршрутизатор має переслати пакети. Такий підхід підвищує безпеку сеансу обміну пакетами.

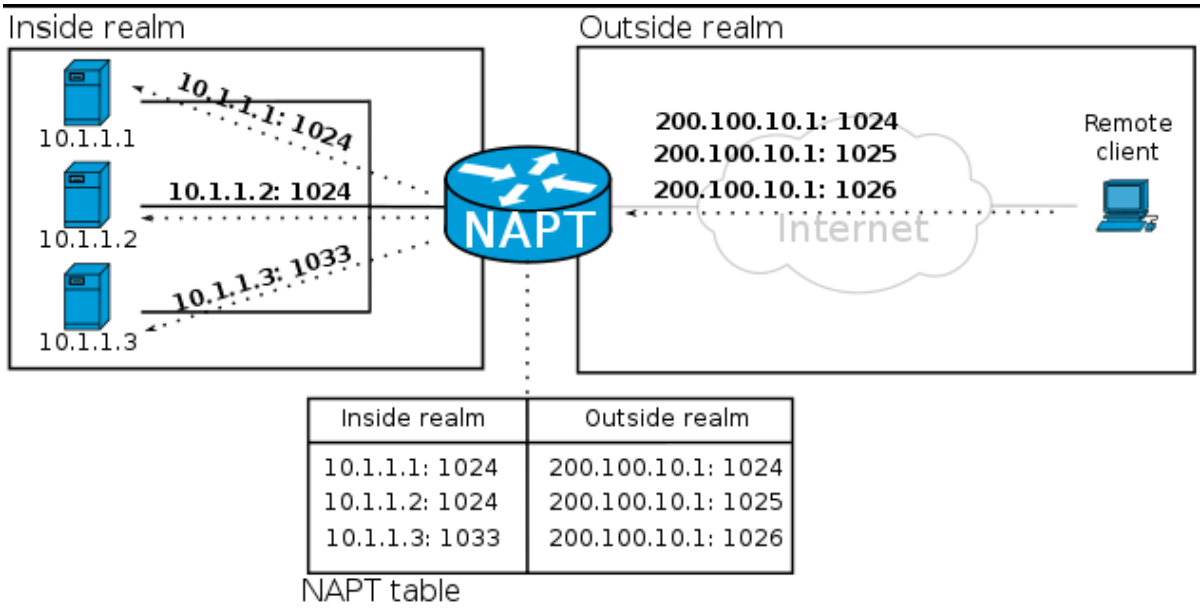


Рисунок 5 – Приклад мережі з використанням технології перетворення адрес портів [9]

1.2.4 Порівняння технологій перетворення NAT і PAT

Порівняння технологій NAT і PAT показує наступне:

1. як видно з таблиць, NAT переводить IPv4-адреси на основі 1:1 між приватними адресами IPv-4 і загальнодоступними IPv4-адресами. Однак PAT змінює адресу і номер порту.

Таблиця 1 – Порівняння перетворення адрес технологіями NAT і PAT

NAT		PAT	
Пул внутрішніх глобальних адрес	Внутрішня локальна адреса	Внутрішня глобальна адреса	Внутрішня локальна адреса
209.165.200.226	192.168.10.10	209.165.200.226:1444	192.168.10.10:1444
209.165.200.227	192.168.10.11	209.165.200.226:1445	192.168.10.11:1445
209.165.200.228	192.168.10.12	209.165.200.226:1555	192.168.10.12:1555
209.165.200.229	192.168.10.13	209.165.200.226:1556	192.168.10.13:1556

2. NAT перенаправляє вхідні пакети на їх внутрішню адресу, орієнтуючись на вхідну IP-адресу джерела, заданну хостом в загальнодоступній мережі. Для PAT зазвичай є тільки одна або дуже мало публічно відкритих IPv4-адрес, і вхідні пакети перенаправляються, орієнтуючись на NAT таблицю маршрутизатора.

3. PAT переводить найбільш поширені протоколи, що переносяться IPv-4, які не використовують TCP або UDP як протокол транспортного рівня. Найбільш поширеними з них є ICMPv-4. Кожен з цих типів протоколів по-різному обробляється PAT. Наприклад, повідомлення запиту ICMPv-4, exo-запити і відповіді включають ідентифікатор запиту Query ID. ICMPv-4 використовує Query ID для ідентифікації exo-запиту з відповідною відповіддю. Ідентифікатор запиту збільшується з кожним відправленим exo-запитом. PAT використовує ідентифікатор запиту замість номера порту рівня 4.

1.3 Переваги та недоліки використання технології NAT

Застосування NAT має багато позитивних моментів:

− якщо необхідно змінити внутрішні адреси через зміну провайдера або злиття з іншою компанією, технологія NAT дозволяє переводити адреси з однієї мережі в іншу;

− NAT дозволяє нарощувати або скорочувати зареєстрований адресний простір IP, не змінюючи вузли, комутатори або маршрутизатори мережі (виняток становлять граничні маршрутизатори NAT, що з'єднують внутрішні і зовнішні мережі);

− NAT може налаштовуватися статично або динамічно;

− NAT розподіляє обробку пакетів між маршрутизаторами за допомогою функції розподілу навантаження протоколу TCP. Розподіл навантаження NAT може здійснюватися за допомогою однієї зовнішньої адреси, співставленої з внутрішньою адресою маршрутизатора. Цей циклічний підхід використовується

з декількома маршрутизаторами. Кожне окреме з'єднання можна налаштувати так, щоб воно використовувало один окремий маршрутизатор.

Окрім переваг існує ряд недоліків NAT:

– NAT збільшує мережеву затримку. Затримки відбуваються на маршрутах комутації через велику кількості трансляцій кожної IP-адреси, що міститься в заголовках пакетів. CPU маршрутизатора використовується для обробки кожного пакету, щоб визначити, чи слід маршрутизатору переводити і змінювати заголовок IP;

– NAT приховує IP-адреси від вузла до вузла. У зв'язку з цим не можна використовувати деякі додатки. Дані додатків, які вимагають використання фізичних адрес, а не повного доменного ім'я, а тому не дійдуть до точки призначення, коли NAT транслює IP-адреси через граничний маршрутизатор NAT;

– так як NAT змінює IP-адреси, відбувається втрата трасування IP між вузлами. Зміни адрес численних пакетів викликають деякі перебої у роботі додатків які відстежують IP. У той же час це є перевагою з точки зору безпеки: зменшуються шанси хакерів визначити джерело пакету.

1.4 Постановка задачі

Виконавши ґрунтовний аналіз літературних джерел за темою роботи, мету наукової роботи можна сформулювати наступним чином: необхідно створити веб-орієнтований графічний інтерфейс, що дозволить початківцям у мережевих технологіях автоматично налаштувати мережеві інтерфейси та протокол NAT на роутерах Cisco (у тому числі і з використанням симулятору Cisco Packet Tracer). Графічний інтерфейс має забезпечувати зручне перенесення згенерованого коду налаштувань в симулятор та реальне обладнання Cisco.

Програмне забезпечення повинно дозволяти початківцям успішно налаштовувати мережі Ethernet, не вимагаючи на початковому етапі знання команд конфігурації роутерів Cisco. Інтерфейс має бути інтуїтивно зрозумілим

навіть користувачу, що не має спеціальних навичок та досвіду у роботі з подібними інтерфейсами.

Для створення графічного інтерфейсу необхідно створити веб-сторінку, на якій можна буде ввести вхідні дані та в результаті отримати налаштування, які можна скопіювати та ввести у симулятор.

Постановка задачі:

1. Налаштування різних варіантів технології NAT на базі роутерів Cisco у симуляторі Packet Tracer.
2. Розробка графічного інтерфейсу налаштування протоколу NAT.
3. Тестування розробленого веб-орієнтованого графічний інтерфейсу в симуляторі та на реальному обладнанні Cisco.

2 МОДЕЛЮВАННЯ ПРОТОКОЛІВ NAT З ВИКОРИСТАННЯМ СИМУЛЯТОРА PACKET TRACER

2.1 Налаштування динамічного NAT

На рисунку 6 зображено схему в середовищі Cisco Packet Tracer для моделювання динамічного NAT.

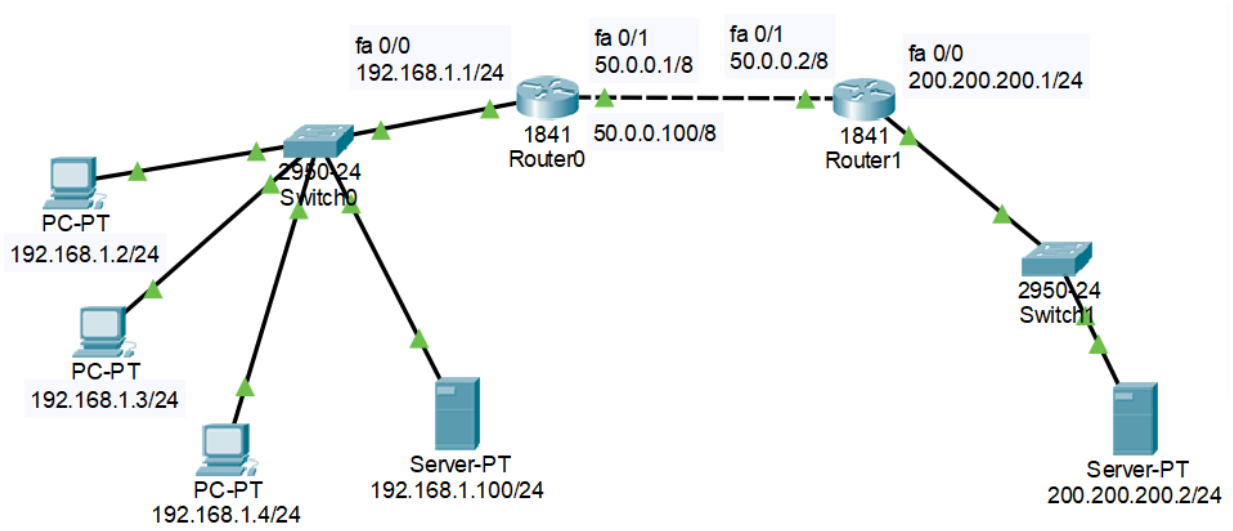


Рисунок 6 – Налаштування динамічного NAT у мережі Ethernet

Особливістю роботи динаміного протоколу NAT є те, що всі ПК та сервера внутрішньої мережі у зовнішню мережу виходять під загальною для всіх IP-адресою 50.0.0.1 але з унікальним номером вихідного порту TCP/UPD сесії (рисунок 7).

NAT Table for Router0

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	50.0.0.1:1026	192.168.1.100:3	200.200.200.2:3	200.200.200.2:1026
icmp	50.0.0.1:3	192.168.1.2:3	200.200.200.2:3	200.200.200.2:3
icmp	50.0.0.1:1024	192.168.1.3:3	200.200.200.2:3	200.200.200.2:1024
icmp	50.0.0.1:1025	192.168.1.4:3	200.200.200.2:3	200.200.200.2:1025

Рисунок 7 – Таблиця трансляції IP-адрес динамічного NAT

Такий підхід дозволяє значно розширити простір адресації, але недоліком такого підходу є той фактор, що почати сеанс зв’язку можуть лише внутрішні ПК, оскільки таблиця NAT динамічна і порти TCP/UPD сесії постійно оновлюються, зовнішній сервер знаючи IP-адресу 50.0.0.1 не може знати який підставити порт TCP/UPD сесії щоб направити дані для початку сеансу зв’язку на необхідний внутрішній ПК. Виконаємо налаштування для маршрутизатора Router 0:

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
interface FastEthernet0/1
ip address 50.0.0.1 255.0.0.0
ip nat outside
access-list 10 permit 192.168.1.0 0.0.0.255
ip nat inside source list 10 interface FastEthernet0/1 overload
ip route 200.200.200.0 255.255.255.0 50.0.0.2
```

Як можна бачити з рисунка 8 запити з зовнішнього серверу на внутрішні ПК видають помилку, що підтверджує коректність роботи схеми при відправці запитів із зовнішніх вузлів на внутрішні. При цьому запити з внутрішньої мережі в зовнішню будуть виконуватись коректно.

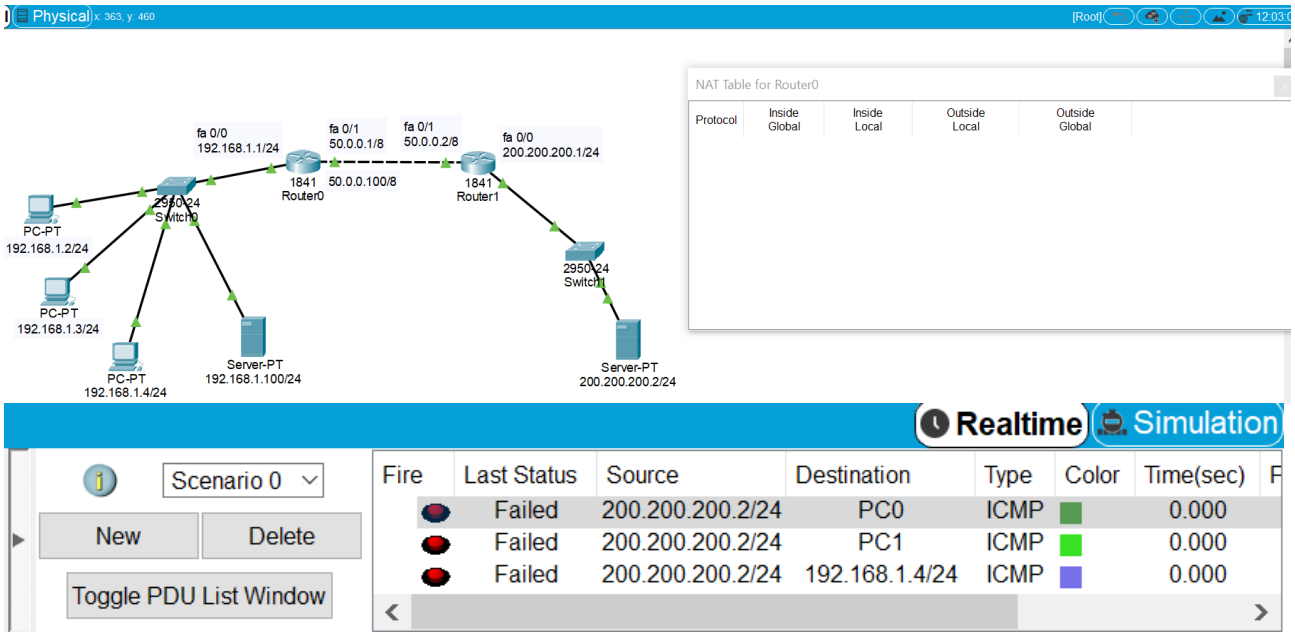


Рисунок 8 – Перевірка тестових запитів з зовнішніх вузлів на внутрішні.

2.2 Налаштування динамічного NAT на пул зовнішніх IP-адрес

Взявши в «оренду» пул зовнішніх IP-адрес у діапазоні від 50.0.0.10 до 50.0.0.12 з’являється можливість виводити ПК з внутрішньої мережі у зовнішню під пулом унікальних адрес. Таким чином реалізується умова, що не всі пристрої під одною зовнішньою адресою, але при цьому не кожен пристрій під своєю унікальною адресою, що зменшує ризик блокування запитів на серверах при значній активності з однієї ip-адреси.

Конфігурація роутера Router 0 для динамічного NAT на пул зовнішніх IP-адрес:

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
interface FastEthernet0/1
ip address 50.0.0.1 255.0.0.0
ip nat outside

access-list 10 permit 192.168.1.0 0.0.0.255
ip nat pool net-21 50.0.0.10 50.0.0.12 netmask 255.0.250.0
ip nat inside source list 10 pool net-21
```

Результат симуляції після конфігурації наведено на рисунках 9 та 10:

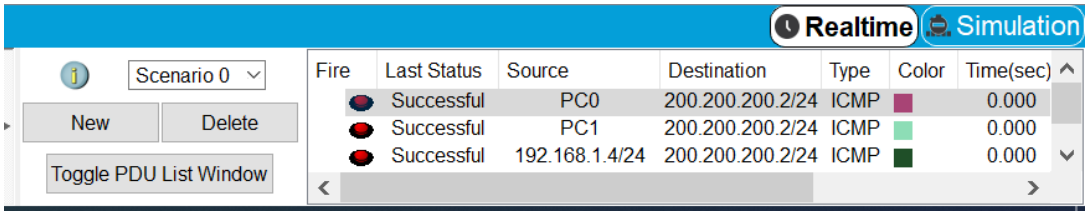


Рисунок 9 – Перевірка успішності налаштування динамічного NAT на пул зовнішніх IP-адрес

NAT Table for Router0

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	50.0.0.12:6	192.168.1.2:6	200.200.200.2:6	200.200.200.2:6
icmp	50.0.0.10:6	192.168.1.3:6	200.200.200.2:6	200.200.200.2:6
icmp	50.0.0.11:5	192.168.1.4:5	200.200.200.2:5	200.200.200.2:5

Рисунок 10 – Таблиця трансляції внутрішніх адрес на пул зовнішніх IP-адрес

2.3 Налаштування динамічного і статичного NAT

Для конфігурації було використано початкову схему, що зображена на рисунку 6. Комп'ютери з внутрішньої мережі виходять у зовнішній мережу із загальною для всіх IP-адресою 50.0.0.1, але з унікальним номером вихідного порту TCP/UPD сесії (рис.11).

NAT Table for Router0

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	50.0.0.100:2	192.168.1.100:2	200.200.200.2:2	200.200.200.2:2
icmp	50.0.0.1:2	192.168.1.2:2	200.200.200.2:2	200.200.200.2:2
icmp	50.0.0.1:1024	192.168.1.3:2	200.200.200.2:2	200.200.200.2:1024
icmp	50.0.0.1:1025	192.168.1.4:2	200.200.200.2:2	200.200.200.2:1025
---	50.0.0.100	192.168.1.100	---	---

Рисунок 11 – Таблиця трансляції внутрішніх адрес при налаштуванні динамічного і статичного NAT

Конфігурація роутера Router 0 для динамічного і статичного NAT:

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
interface FastEthernet0/1
```

```
ip address 50.0.0.1 255.0.0.0
ip nat outside

access-list 10 permit 192.168.1.0 0.0.0.255
ip nat inside source list 10 interface FastEthernet0/1 overload

ip nat inside source static 192.168.1.100 50.0.0.100

ip route 200.200.200.0 255.255.255.0 50.0.0.2
```

Для внутрішнього серверу 192.168.1.100 виділено статичну зовнішню IP-адресу 50.0.0.100 і саме під цією адресою зовнішній сервер може успішно звертатися до внутрішнього серверу, що підтверджується рисунком 12:

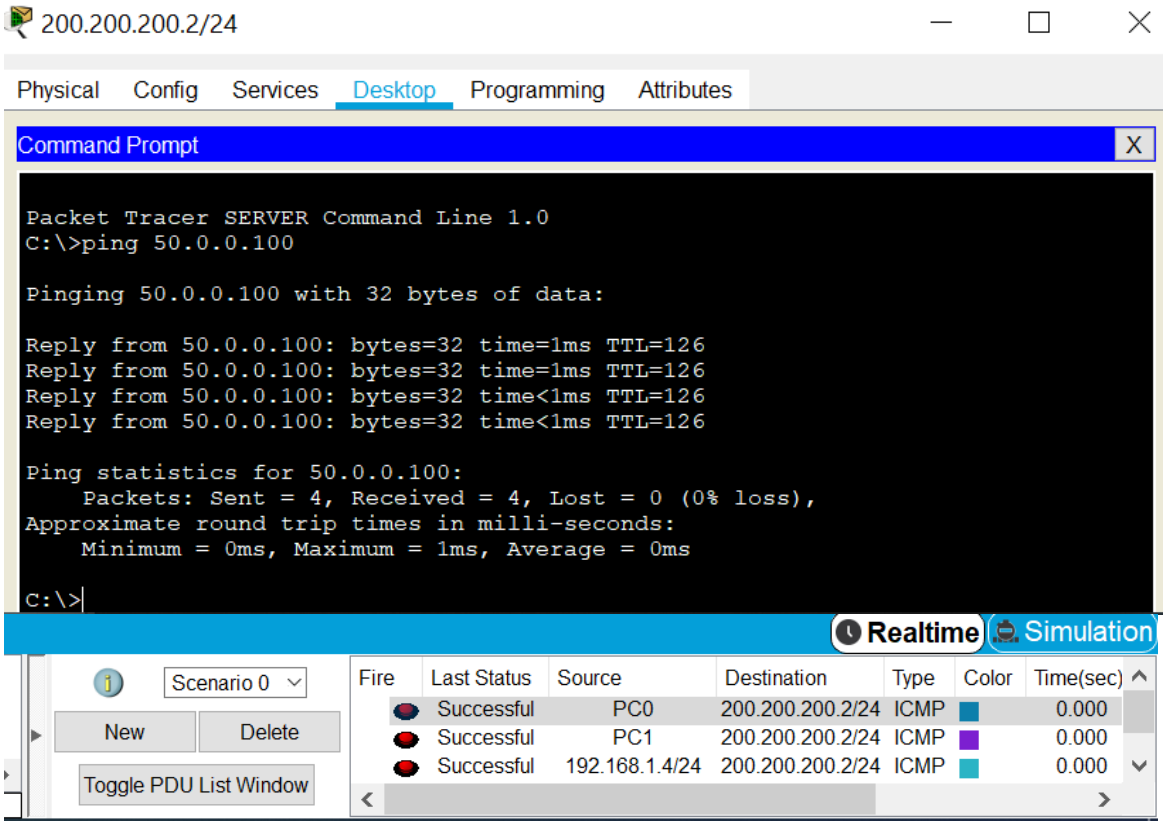


Рисунок 12 – Успішні запити з зовнішнього серверу до внутрішнього при налаштуванні статичного NAT

2.4 Налаштування технології NAT з використанням Port Forwarding

У даній схемі приведено варіант налаштування технології NAT коли всі комп’ютери та сервер внутрішньої мережі виходять у зовнішню під загальною

для всіх IP-адресою 50.0.0.1, але з унікальним номером вихідного порту TCP/UPD сесії. Розпочати сеанс зв’язку можуть лише внутрішні комп’ютери, оскільки таблиця NAT динамічна і порти TCP/UPD сесії постійно оновлюються, зовнішній сервер навіть знаючи IP-адресу 50.0.0.1 не може знати який підставити порт TCP/UPD сесії щоб направити дані для початку сеансу зв’язку на необхідний внутрішній ПК.

Але якщо зовнішній сервер звертаючись на адресу 50.0.0.1 «повідомить» порт призначення 8080, то варіант перенаправлення портів налаштоване на роутері Router 0 переадресує цей запит на відповідний внутрішній сервер 192.168.1.100 з портом призначення 80, що підтверджується таблицею NAT наведеною на рисунках 13-15:

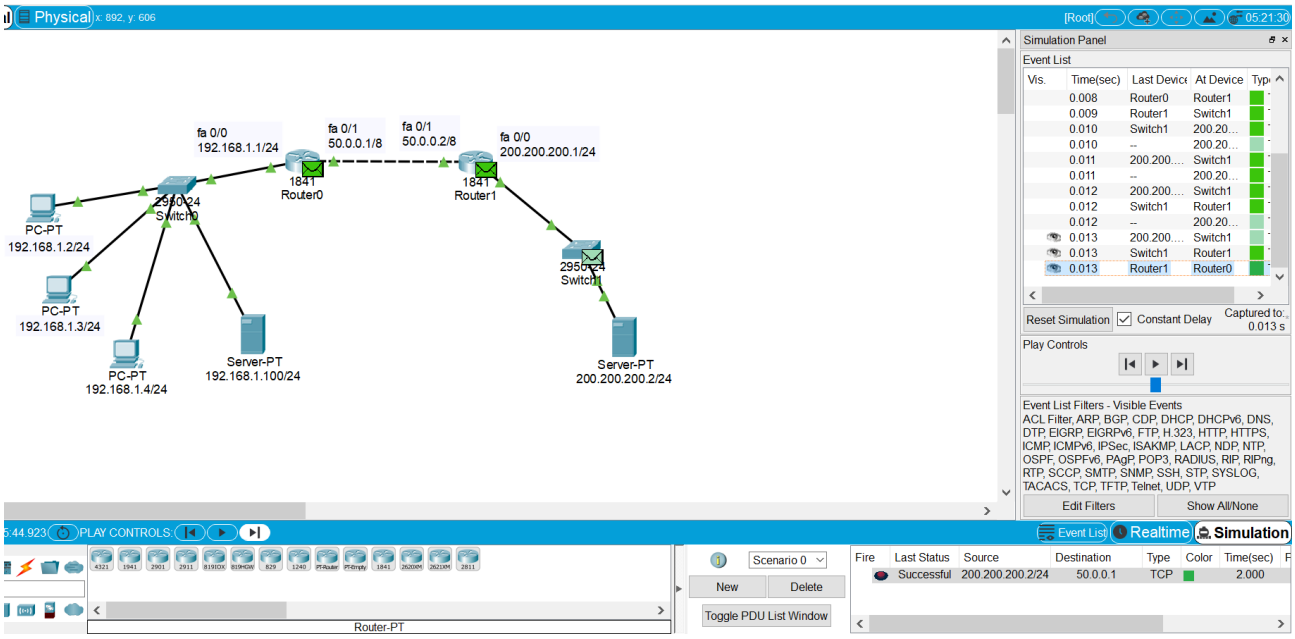


Рисунок 13 – Успішні запити із зовнішнього серверу до внутрішнього при налаштуванні NAT з перенаправленням портів

NAT Table for Router0

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	50.0.0.1:7	192.168.1.100:7	200.200.200.2:7	200.200.200.2:7
icmp	50.0.0.1:9	192.168.1.2:9	200.200.200.2:9	200.200.200.2:9
icmp	50.0.0.1:1024	192.168.1.3:9	200.200.200.2:9	200.200.200.2:...
icmp	50.0.0.1:8	192.168.1.4:8	200.200.200.2:8	200.200.200.2:8
tcp	50.0.0.1:8080	192.168.1.100:80	---	---
tcp	50.0.0.1:8080	192.168.1.100:80	200.200.200.2:81	200.200.200.2:81

Рисунок 14 – Таблиця трансляції адрес та портів при запитах із зовнішнього серверу до внутрішнього

Налаштування Router0 для технології NAT з використанням технології перенаправлення портів:

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
interface FastEthernet0/1
ip address 50.0.0.1 255.0.0.0
ip nat outside

access-list 10 permit 192.168.1.0 0.0.0.255

ip nat inside source list 10 interface FastEthernet0/1 overload

ip nat inside source static tcp 192.168.1.100 80 50.0.0.1 8080

ip route 200.200.200.0 255.255.255.0 50.0.0.2
```

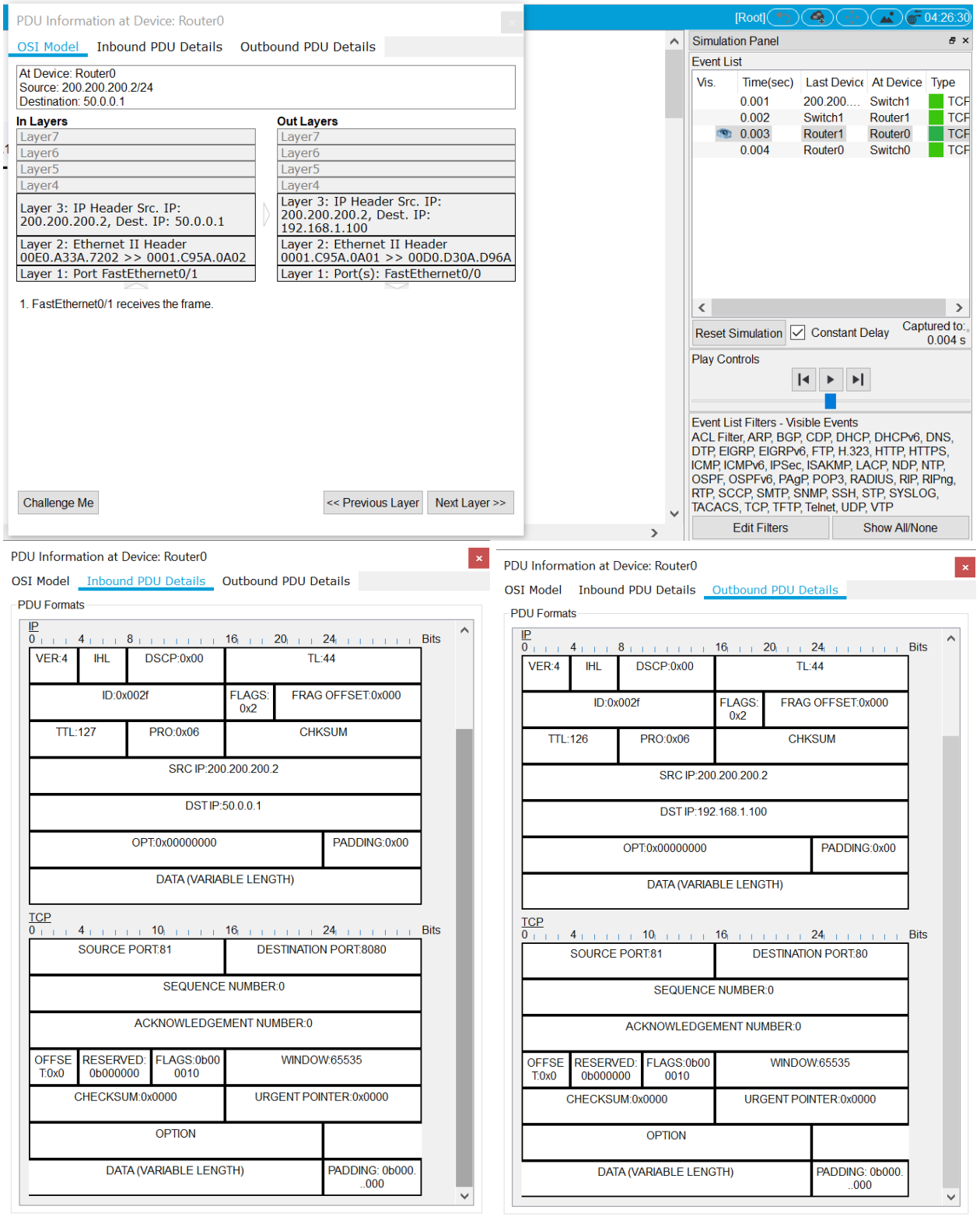


Рисунок 15 – Структура кадрів Ethernet з ілюстрацією заміни зовнішніх адрес та портів на внутрішні при налаштуванні NAT з перенаправленням портів

Такий підхід поєднує переваги схем динамічного NAT та статичного NAT, але дозволив обійтися лише однією зовнішньою IP-адресою.

3 ГРАФІЧНИЙ ІНТЕРФЕЙС НАЛАШТУВАННЯ ПРОТОКОЛУ NAT

3.1 Розробка графічного інтерфейсу

Мережу Ethernet для симуляції реального налаштування було сконфігуровано за допомогою емулятора Cisco Packet Tracer (рис.16):

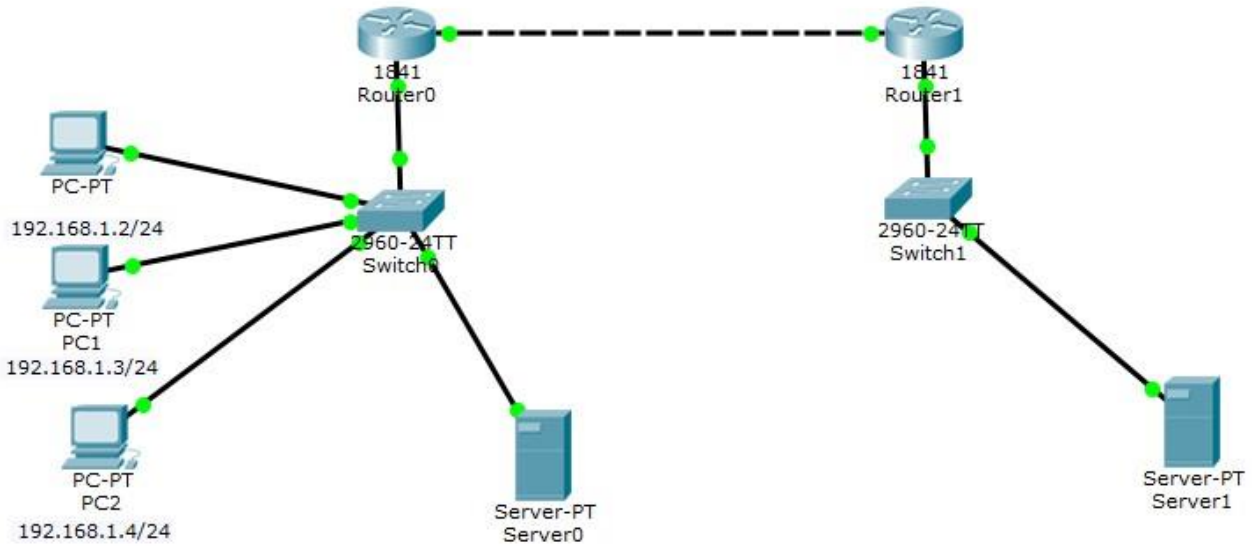


Рисунок 16 – Мережа Ethernet в емуляторі Cisco Packet Tracer

Недоліком роботи як з емулятором, так і реальним устаткуванням є відсутність графічного інтерфейсу налаштувань. Це значною мірою сповільнює час налаштування мережі. Таким чином розробка графічного інтерфейсу для автоматизації налаштувань є актуальним питанням. Основною вимогою для інтерфейсу є лаконічність і зрозумілість для будь-якого користувача.

Для розробки веб-інтерфейсу було використано мову розмітки HTML, для стилізації – CSS, та JavaScript для функціоналу. Лістинг програми приведено у Додатку А.

3.2 Моделювання мережі

Графічний веб-інтерфейс налаштувань мережі містить поля для введення IP-адреси та маски мережі на всіх інтерфейсах. Користувачу необхідно заповнити всі дані і натиснути на кнопку «Зберегти налаштування» для того щоб було згенеровано відповідний код. На рисунку 17 представлено відповідний інтерфейс:

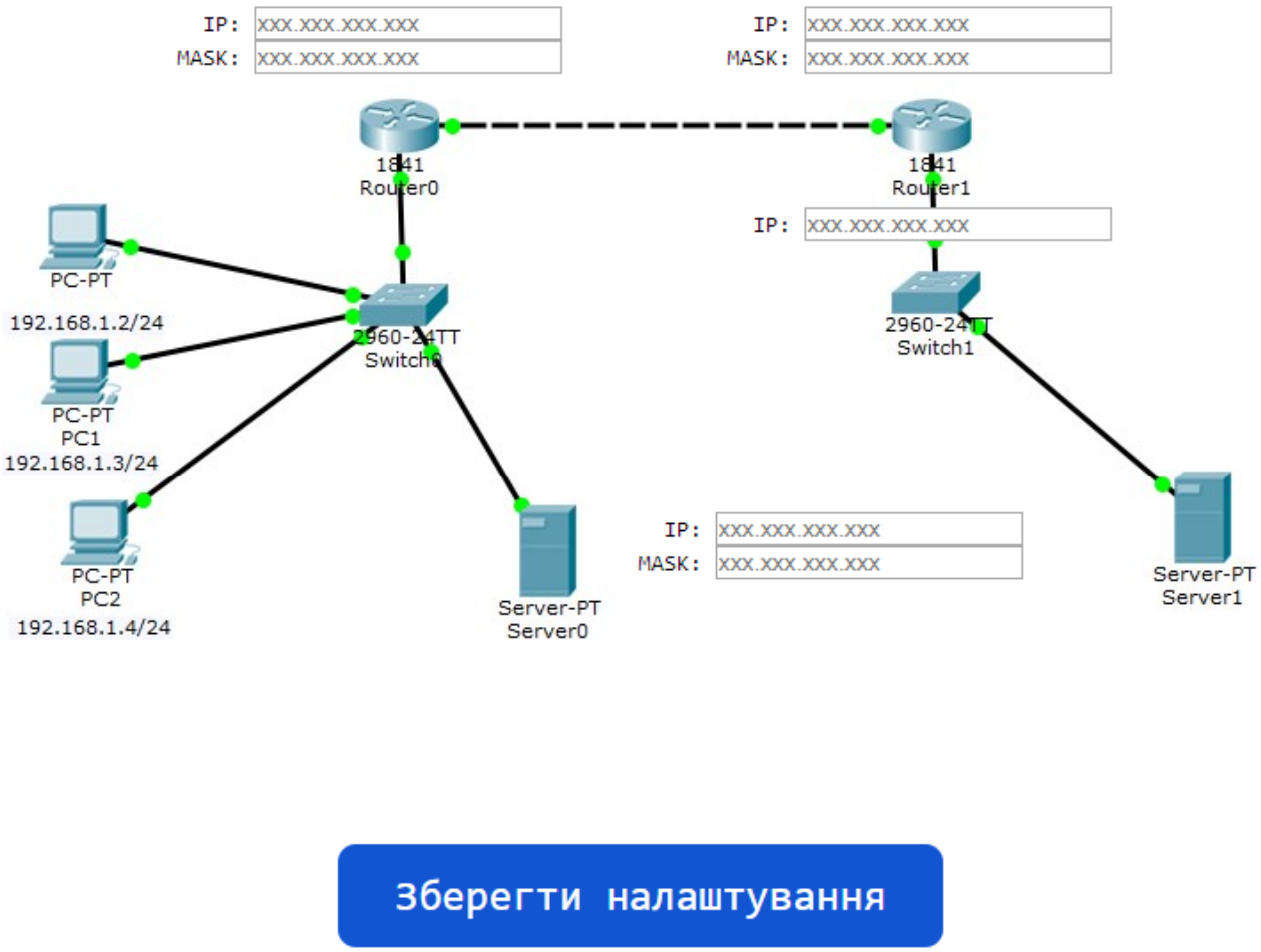


Рисунок 17 – Графічний інтерфейс налаштувань

Приклад згенерованих налаштувань (рис.18). Кнопка «Copy» дозволяє скопіювати повністю необхідний код.

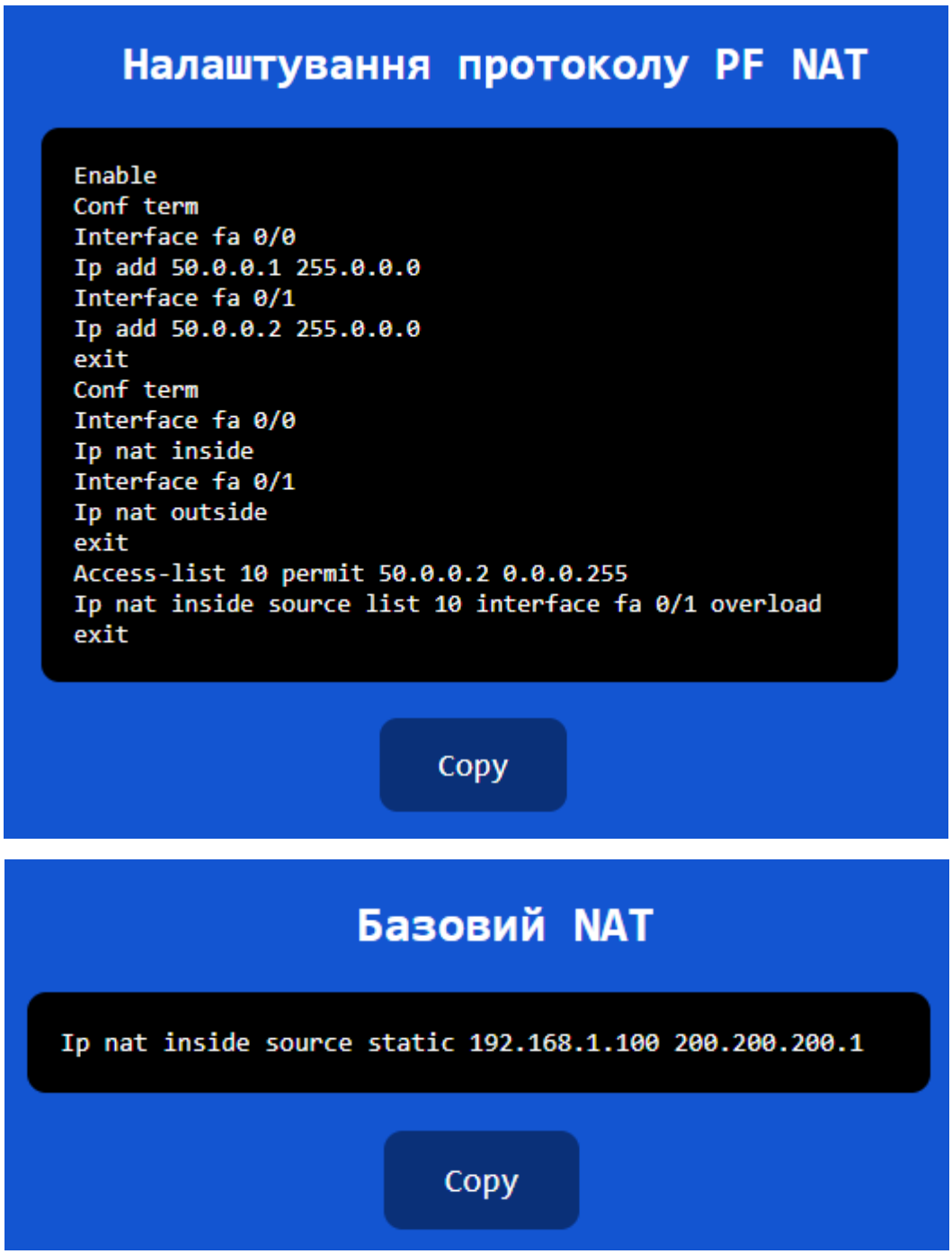


Рисунок 18 – Приклад згенерованого коду налаштувань

3.3 Тестування роботи графічного інтерфейсу

Перевіримо працездатність згенерованого коду в емуляторі для створеної мережі. По черзі генеруємо код для всіх необхідних роутерів і вставляємо скопійований згенерований код (рис.19). Аналогічним чином будуть виглядати налаштування на всіх пристроях.

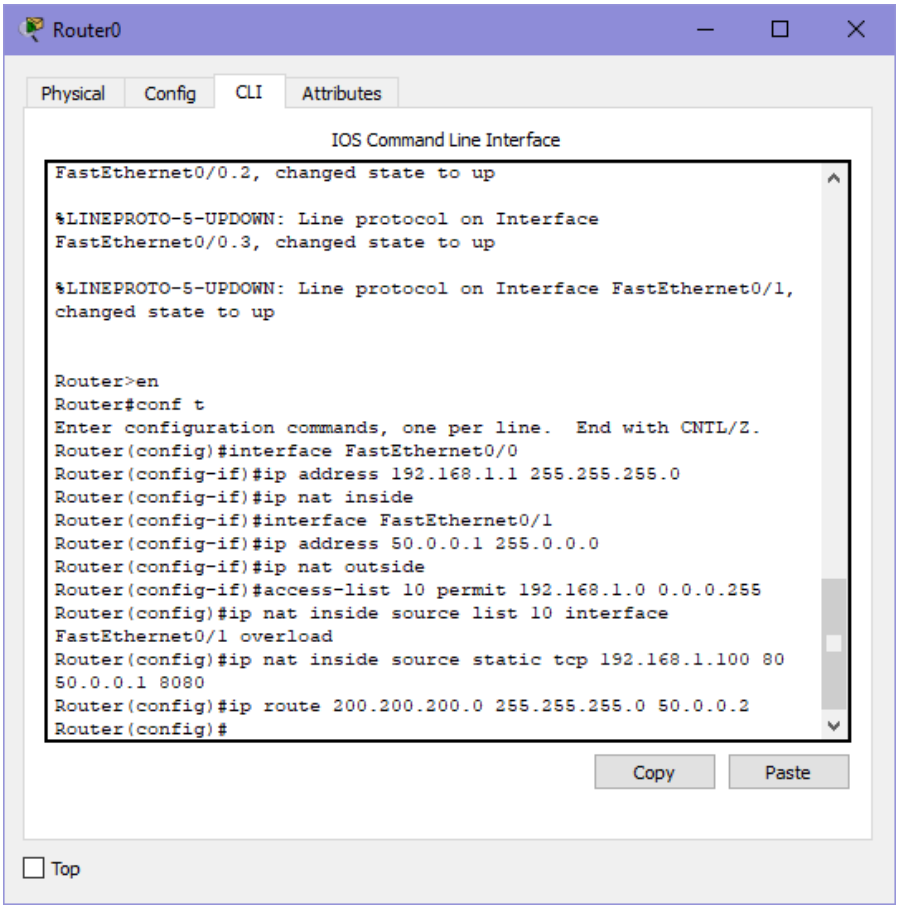


Рисунок 19 – Вікно налаштування Router0 за допомогою згенерованого кода

Зберігаємо налаштування на всіх пристроях і переходимо до тестування правильності налаштувань. Для того щоб перевірити чи всі налаштування було виконано і збережено використаємо команду «show run» (рис.20). З рисунку видно, що налаштування, які було зконфігуровано за допомогою розробленого веб-інтерфейсу є коректними.

За допомогою команди «show ip nat translations» перевіримо коректність перетворення внутрішніх адре у зовнішні і навпаки (рис.21). Як можна бачити з рисунку результат налаштувань є успішним.

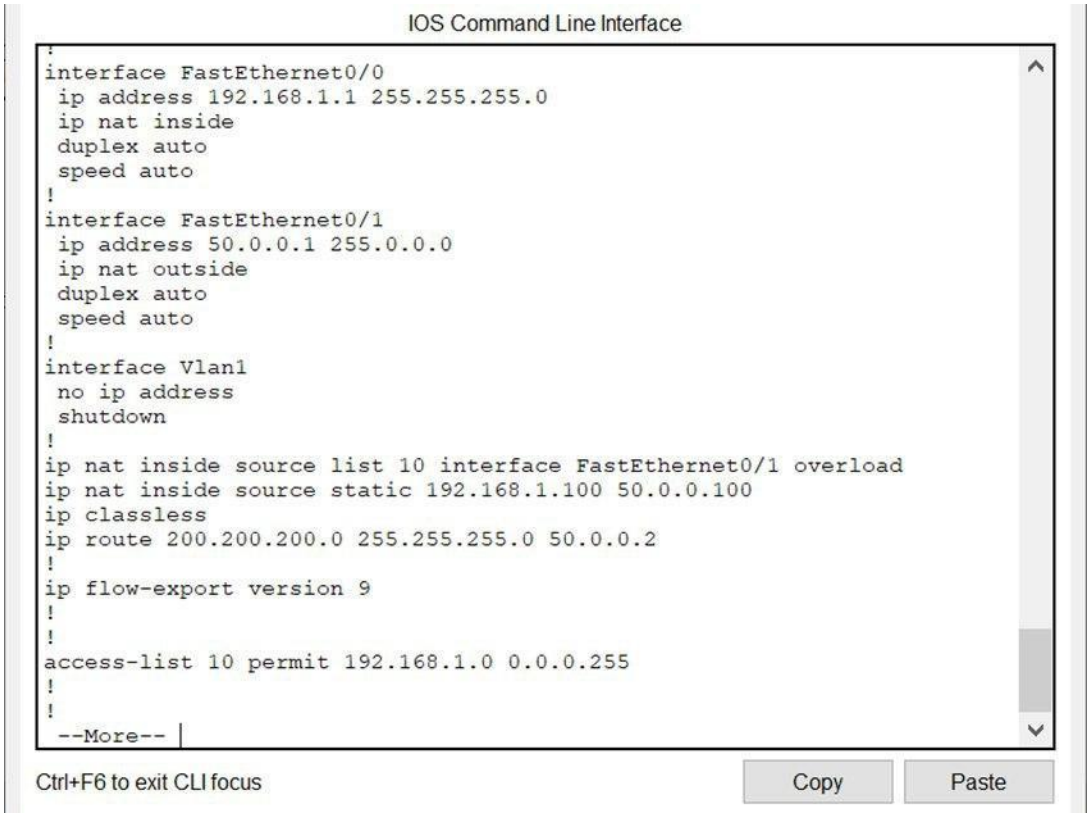


Рисунок 20 – Результат виконання команди «show run»

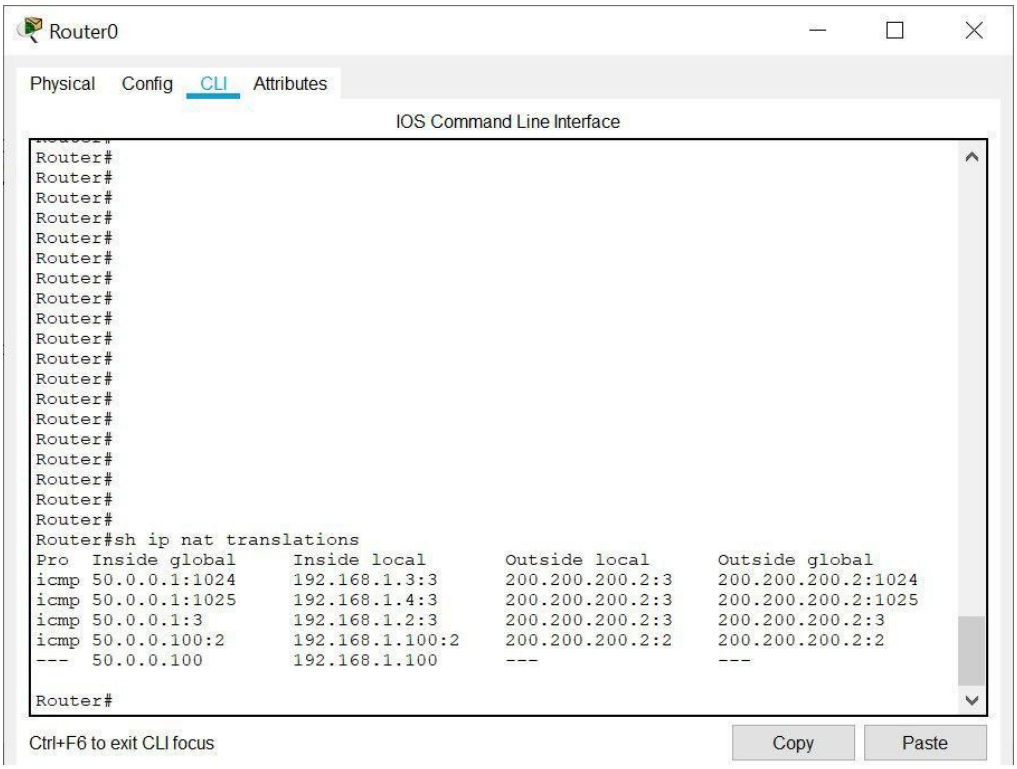


Рисунок 21 – Результат виконання команди «show ip nat translations»

3.3.1 Команда «debug ip nat»

Після того як виконано перевірку працездатності попередніми способами, необхідно додатково застосувати команду «debug ip nat», яка використовується для перевірки більш складних мереж, у яких декілька перетворень, а тому у разі виникнення помилок, проблему важко знайти. Результат виконання команди показано на рисунку 22:

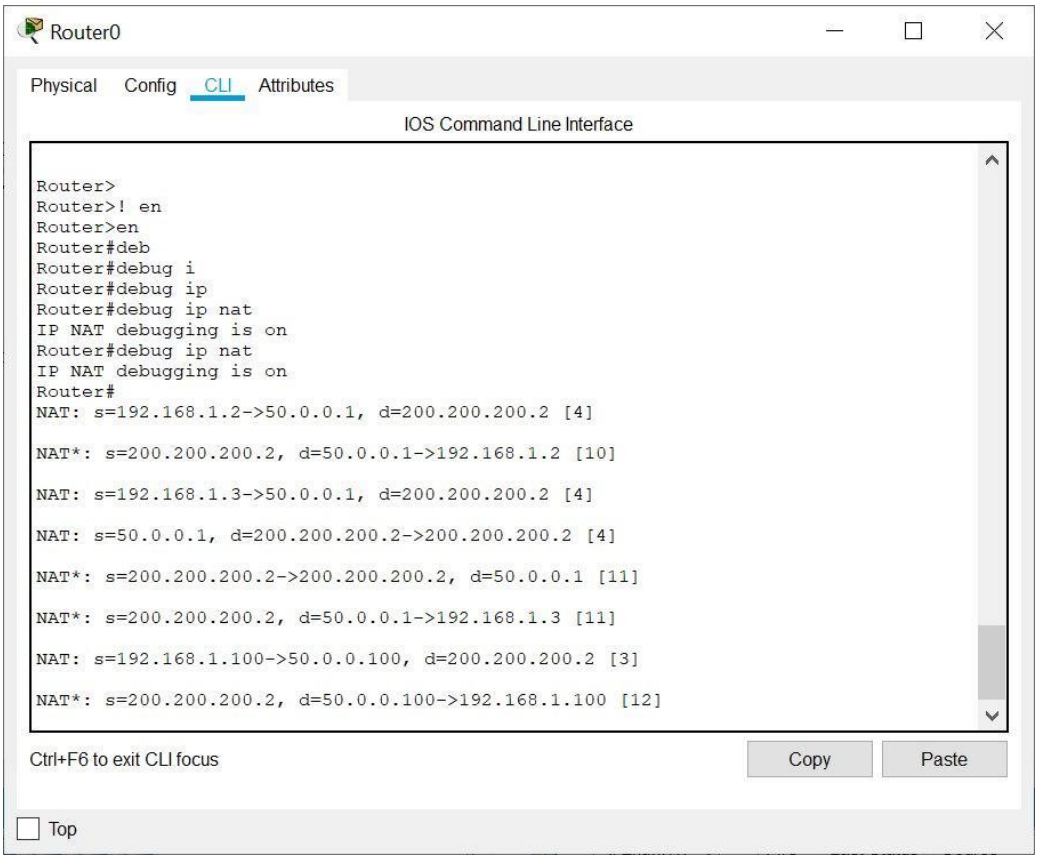


Рисунок 22 – Результат виконання команди «debug ip nat»

Результат показує, що, наприклад, внутрішній вузол (192.168.1.2) створив трафік до зовнішнього вузла (200.200.200.2), і адреса джерела була перетворена на адресу 50.0.0.1. Даний результат засвідчує коректну роботу.

Перевіримо працездатність схеми використовуючи команду «ping» та передачу пакетів за допомогою симуляційного пакету від роутера до сервера. Результат показано на рисунку 23.

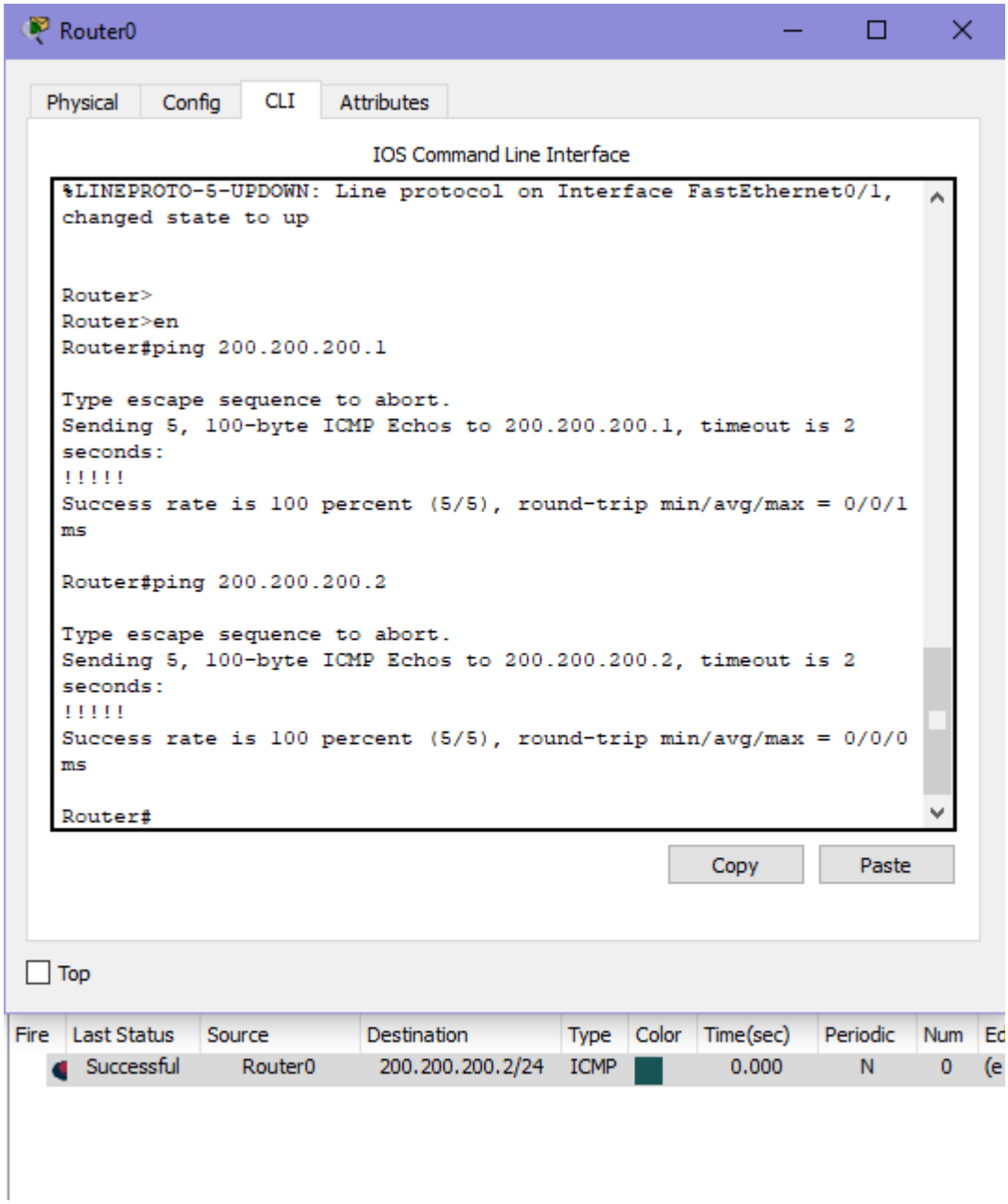


Рисунок 24 – Результат перевірки працездатності схеми

Отже, розроблений веб-інтерфейс налаштувань показав хороший результат роботи, який значною мірою може прискорити налаштування мережі будь-яким користувачем.

ВИСНОВОК

Дана робота присвячена вивченню принципів роботи технології NAT при налаштуванні локальних домашніх та корпоративних мереж. Використовуючи симулятор Pacet Tracer у роботі практично реалізовані чотири різних варіанта налаштування технології NAT: «Налаштування динамічного NAT», «Налаштування динамічного NAT на пул зовнішніх IP-адрес», «Налаштування динамічного і статичного NAT», «Налаштування технології NAT з використанням Port Forwarding». Зазначено переваги та недоліки кожного з варіантів, але нашу думку варіант «Налаштування технології NAT з використанням Port Forwarding» є найбільш економічно вигідним та функціональним оскільки дозволяє маючи лише одну зовнішню ip-адресу виходити у зовнішній світ внутрішнім ПК, а також дозволяє внутрішнім серверам бути доступними з зовнішнього світ при запиті відповідних сервісів (наприклад http за портом 8080).

У результаті виконання роботи було розроблено веб-інтерфейс для налаштування мережі. Результат перевірки роботи розробленого графічного інтерфейсу підтвердив коректність налаштувань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NAT Definition [Електронний ресурс] - https://techterms.com/definition/nat

2. Yassine, Khlifi & Boudriga, N. & Obaidat, Mohammad. (2007). The Handbook of Computer Networks.

3. Tamimi, Abdelfatah & Khalifa, Jamal. (2010). Computer networks and Communications.

4. IP Addressing Guide [Електронний ресурс] - https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-business-architecture/sba_ipAddr_dg.pdf

5. Understanding Public and Private IP Addresses [Електронний ресурс] - https://docs.netgate.com/pfsense/en/latest/book/network/understanding-public-and-private-ip-addresses.html

6. IPv4 Network Addresses [Електронний ресурс] - http://ccna.mpei.ac.ru/IntroductionToNetwork/course/module8/index.html#8.1.4.1

7. IPv4 – Quick Guide [Електронний ресурс] - https://www.tutorialspoint.com/ipv4/ipv4_quick_guide.htm

8. Л.М. Олещенко, Організація комп'ютерних мереж. Конспект лекцій. - КПІ ім.Ігоря Сікорського. -2018 р. – 225 С.

9. Networkustud [Електронний ресурс] - https://networkustad.com/2019/10/11/static-nat-configuration/

10. CCNA Semester 2 v6. 0 study Materials and Lab [Електронний ресурс] – https://itexamanswers.net/ccna–semester–2–v6–0–study–materials–labs–online–course. html

11. Грайвороновський М.В. Безпека інформаційно-комунікаційних систем: підручник для ВНЗ / М.В. Грайвороновський, О.М. Новіков; М-вопраці та соц. Політики України. Держнаглядохоронпраці України.- К. : ВНV, 2019. - 307с.

Додаток А

```
<!DOCTYPE html>
<html>
 <head>
  <title>Configuration NAT</title>
  <meta charset="utf-8">

   <style type="text/css">
      * {margin: 0; padding: 0;}
      body
        {
      text-align: center;
      background: #fff;
      }
      .center {
      width: 1110px;
      margin: 0 auto;
}
  p {
   white-space: nowrap;
   font-family:monospace
  }
     .btn-clipboard3 {
   background-color: #1355d1;
   border: none;
   border-radius: 10px;
   color: white;
   padding: 15px 32px;
   text-align: center;
   text-decoration: none;
   display: inline-block;
   font-size: 16px;
}

  .btn-clipboard, .btn-clipboard2 {
   background-color: #0a3078;
   border: none;
   color: white;
   border-radius: 10px;
   padding: 15px 32px;
   text-align: center;
   text-decoration: none;
   display: inline-block;
```

```
    font-size: 16px;
}
   .tabl {
    background: #000 none repeat scroll 0 0;
    border-radius: 10px;
    color: #fff;
    float: left;
    font-family: monospace;
    font-size: 14px;
    margin-bottom: 20px;
    margin-top: 20px;
    padding: 18px;
    text-align: left;
    width: 440px;
          }
    .stolbec {
          width: 480px;
          float: left;
     margin: 20px;
          padding: 18px;

                  }
.okno1 {
  font-family:monospace;
    margin-left: 290px;
    margin-top: -400px;
    position: absolute;
    text-align: right;
       width: 220px;
    height: 100px;
          }

.okno2 {
  font-family:monospace;
    margin-left: 600px;
    margin-top: -400px;
    position: absolute;
      text-align: right;
        width: 220px;
    height: 100px;
          }

.okno3 {
    font-family:monospace;
    margin-left: 550px;
```

```
        margin-top: -115px;
        position: absolute;
          text-align: right;
            width: 220px;
        height: 100px;

              }
    .bg {

        margin-top: 20px;
        background: #1355d1 none repeat scroll 0 0;
        border-radius: 20px;

        position: absolute;

        }

    .stolbec h1 {
        color: #fff;
        font-family: monospace;
        margin-left: 25px;
              }
      </style>


    <script type="text/javascript" src="http://ff.kis.v2.scr.kaspersky-labs.com/A9987657-C496-AF41-BCED-37D6D7D4B965/main.js" charset="UTF-8"></script><script src="http://code.jquery.com/jquery-1.11.0.min.js" type="text/javascript"></script>

    <script src="https://raw.githubusercontent.com/digitalBush/jquery.maskedinput/1.3.1/dist/jquery.maskedinput.js" type="text/javascript"></script>

    <script src="https://cdn.rawgit.com/zenorocha/clipboard.js/master/dist/clipboard.min.js"></script>

    <script type="text/javascript">

        function ValidateIPaddress(inputText)
                {
                    var ipformat = /^(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$/;
```

```
                    if(inputText.value.match(ipformat))
                {
                    document.form1.text1.focus();
                    return true;
                }
                    else
                {
                    alert("You have entered an invalid IP address!");
                    document.form1.text1.focus();<br>return false;
                    }
                }

    </script>

     </head>
    <body>
    <div class="center">

    <div style="margin-top: 50px">
    <img src="ip.jpg">
    </div>

    <div class="okno1">
    IP: <input type="text" id="myText" title="Адреса IP" placeholder='xxx.xxx.xxx.xxx' pattern="\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}"><br />
    MASK: <input type="text" id="myText2" title="Маска мережі" placeholder='xxx.xxx.xxx.xxx' pattern="\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}">
    </div>

    <div class="okno2">
    IP: <input type="text" id="myText3" title="Адреса IP" placeholder='xxx.xxx.xxx.xxx' pattern="\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}"><br />
    MASK: <input type="text" id="myText4" title="Маска мережі" placeholder='xxx.xxx.xxx.xxx' pattern="\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}"><br /><br /><br /><br /><br /><br />
    IP: <input type="text" id="myText5" title="Адреса IP" placeholder='xxx.xxx.xxx.xxx' pattern="\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}">
    </div>
    <div class="okno3">
    IP: <input type="text" id="myText6" title="Адреса IP" placeholder='xxx.xxx.xxx.xxx' pattern="\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}"><br />
    MASK: <input type="text" title="Маска мережі" placeholder='xxx.xxx.xxx.xxx' pattern="\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}">
    </div>
```

```
<br /><br /><br /><br />

<button onclick="myFunction()" class="btn-clipboard3" style="margin: 0 auto;font-size:24px;font-family:monospace">Зберегти налаштування</button>
<br />


<div class="bg">

<div class="stolbec">
<h1>Налаштування протоколу PF NAT</h1>

<div id="textarea-example" class="tabl">Enable<br />
Conf term<br />
Interface fa 0/0<br />
Ip add <w id="demo"></w> <w id="demo2"></w><br />
Interface fa 0/1<br />
Ip add <w id="demo3"></w> <w id="demo4"></w><br />
exit<br />
Conf term<br />
Interface fa 0/0<br />
Ip nat inside<br />
Interface  fa 0/1<br />
Ip nat outside<br />
exit<br />
Access-list 10 permit <w id="demo6"></w> 0.0.0.255<br />
Ip nat inside source list 10 interface fa 0/1 overload<br />
exit</div>



<button class="btn-clipboard" data-clipboard-target="#textarea-example" style="margin: 0 auto;font-size:18px;font-family:monospace">Copy</button>
<script type="text/javascript">
new Clipboard('.btn-clipboard');
</script>
</div>



<div class="stolbec">
<h1>Базовий NAT</h1>
<div id="textarea-example2"  class="tabl">Ip nat inside source static <w id="demo7"></w> <w id="demo5"></w></div>
```

```
<button class="btn-clipboard2" data-clipboard-target="#textarea-example2" style="margin: 0 auto;font-size:18px;font-family:monospace">Copy</button>
<script>
new Clipboard('.btn-clipboard2');
</script>
</div>
</div>
</div>
<script type="text/javascript">
function myFunction() {

   var a = document.getElementById("myText").value;

   var b = document.getElementById("myText2").value;

   var c = document.getElementById("myText3").value;

   var d = document.getElementById("myText4").value;

   var e = document.getElementById("myText5").value;

   var f = c;

   var g = document.getElementById("myText6").value;


   document.getElementById("demo").innerHTML = a;

   document.getElementById("demo2").innerHTML = b;

   document.getElementById("demo3").innerHTML = c;

   document.getElementById("demo4").innerHTML = d;

   document.getElementById("demo5").innerHTML = e;

   document.getElementById("demo6").innerHTML = f;

   document.getElementById("demo7").innerHTML = g;
}
</script>


<script type="text/javascript">
```

```
    jQuery(function($){

   $("input").mask("9?99.9?99.9?99.9?99", {placeholder:" "});

});

</script>
</body>
</html>
```