МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний технічний університет

«Харківський політехнічний інститут»

Навчально-науковий інститут комп’ютерного моделювання, прикладної фізики та математики

Кафедра динаміки та міцності машин

Звіт

про виконання

Комп’ютерного практикуму №8

по курсу «Комп’ютерної мережі"

з теми "Налаштування статичних та динамічних трансляцій мережних адрес (NAT). Налаштування статичного NAT "

Виконав:

студент групи ІКМ-220б

Пономаренко О. В.

Викладач:

доцент кафедри ДММ

Трубаєв О.І.

Харків 2022

**Завдання лабораторної роботи**

**Завдання №1.** Статична трансляція адрес NAT

**Завдання №2.** Налаштування статичного NAT

**Завдання №3.** Налаштування динамічного NAT

**Завдання №4.** Динамічний NAT Overload: налаштування PAT (маскарадинг)

**Теоретичні відомості**

Нехватка IP адресів. Технологія NAT

У 80-х роках ХХ століття було закладено основу IPv4, що дозволило створити ~4,3 млрд. адреси, але ніхто не очікував, що цей запас так швидко закінчиться. З кожним роком користувачів з’являлося все більше і з 25 листопада 2019р. Термін дії IP-адрес офіційно закінчився в Росії та Європі. Ліміт вичерпано.

Було розроблено кілька методів вирішення цієї проблеми:

**Перший спосіб** - посилення контролю над IP-адресами.

Нехай існує якийсь сайт N з IPv4 xxx.xxx.xxx.xxx, і його хост вирішив припинити підтримку цього сайту. Сайт заброшен, а IP продовжує значитися як зайнятий і таких випадків може бути дуже багато. Щоб продати нерухомість "інвентаризувати" IP-адреси та вилучити некористувані/заброшені.

**Другий спосіб** - у масовому використанні системи IPv6.

Протокол IPv6 розроблений як наступник протоколу IPv4. Основні переваги IPv6 перед IPv4 полягають у збільшеному адресному просторі (IPv4 мав 32 біти, що дорівнювало 232 адресам, а IPv6 мав 128 бітів, що дорівнювало 2128 адресам), шоста версія протоколу стала безпечнішою (оскільки v4 не забезпечувала багато аспектів безпеки, тому що розрахунок проводився на сторонньому ПЗ, а контрольні суми і шифрування пакетів з'явилися в v6), однак це далеко не всі переваги IPv6 перед IPv4.

Здається, проблема вирішена, але перехід з IPv4 на IPv6 викликає труднощі, оскільки ці протоколи несумісні. І основна причина складного переходу на 6-ту версію протоколу – це грошова вартість. Багато кампаній не готові інвестувати достатньо коштів для переходу, хоча варто зазначити, що процес переходу від версії 4 до версії 6 відбувається поступово.

І **третій спосіб** - використання технології трансляції мережевих адрес - NAT.

Згідно з RFC 1918, IANA зарезервувала 3 блоки адрес для приватних IP (сірий), решта IP-адреси називаються публічними адресами (білими).

10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))

172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))

192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Трансляція мережевих адрес — це механізм у мережах TCP/IP, який дозволяє змінювати IP-адресу в заголовку пакета, що проходить через пристрій маршрутизації трафіку.

Отримавши пакет від локального комп'ютера, маршрутизатор переглядає IP-адресу призначення. Якщо це локальна адреса, пакет пересилається на інший локальний комп’ютер. Якщо ні, тоді пакет потрібно надіслати в Інтернет.

Маршрутизатор замінює зворотну IP-адресу пакета своєю зовнішньою (видимою в Інтернеті) IP-адресою та змінює номер порту (щоб розрізняти пакети відповідей, адресовані різним локальним комп’ютерам). Маршрутизатор зберігає комбінацію, необхідну для зворотної заміни, у своїй тимчасовій таблиці. Через деякий час, після завершення обміну пакетами між клієнтом і сервером, роутер побачить у себе в таблиці запис про n-му порту протягом деякого часу.

Основною функцією NAT є збереження публічних адрес, але додатковою функцією є конфіденційність мережі шляхом приховування внутрішніх IPv4-адрес від зовнішніх.

Існує кілька типів технології NAT, але основними з них є: статичний NAT (трансляція статичної мережевої адреси), динамічний NAT (динамічна трансляція мережевої адреси) і перевантажений NAT (перевантаження трансляції мережевої адреси). [1]

**NAT (Network Address Translation)** — трансляція мережевих адрес, технологія, що дозволяє перетворювати (змінювати) IP-адреси і порти у мережевих пакетах. NAT використовується найчастіше для здійснення доступу пристроїв з локальної мережі підприємства в Інтернет, або навпаки для доступу з Інтернет на який-небудь ресурс усередині мережі. Локальна мережа підприємства будується на приватних IP-адресах:

10.0.0.0 — 10.255.255.255 (10.0.0.0/255.0.0.0 (/8))

172.16.0.0 — 172.31.255.255 (172.16.0.0/255.240.0.0 (/12))

192.168.0.0 — 192.168.255.255 (192.168.0.0/255.255.0.0 (/16))

Ці адреси не маршрутизуються в Інтернеті, і провайдери повинні відкидати пакети з такими IP-адресами відправників або одержувачів. Для перетворення приватних адрес у глобальні (маршрутизовані в Інтернеті) застосовують NAT.

NAT — технологія трансляції мережевих адрес, тобто підміни адрес (чи портів) у заголовку IP-пакету. Іншими словами, пакет, проходячи через маршрутизатор, може змінити свою адресу джерела та/чи призначення. Подібний механізм служить для забезпечення доступу з LAN, де використовуються приватні IP-адреси, у Internet, де використовуються глобальні IP-адреси.

Існує три види трансляції:

1. Static NAT (статичний NAT) здійснює перетворення IР-адреси один до одного, тобто зіставляється одна адреса з внутрішньої мережі з однією адресою з зовнішньої мережі. Іншими словами, при проходженні через маршрутизатор, адреса змінюються на строго задану адресу, один-до-одного (Наприклад, 10.1.1.5 завжди замінюється на 11.1.1.5 і назад). Запис про таку трансляцію зберігається необмежено довго, поки є відповідний рядок в конфігурації роутера.
2. Dynamic NAT (динамічний NAT) виконує перетворення внутрішньої адреси в одну з групи зовнішніх адрес. Тобто, перед використанням динамічної трансляції, потрібно задати nat-пул зовнішніх адрес. У цьому випадку при проходженні через маршрутизатор, нова адреса вибирається динамічно з деякого діапазону адрес, званого пулом (pool). Запис про трансляцію зберігається деякий час, щоб відповідні пакети могли бути доставлені адресату. Якщо протягом деякого часу трафік по цій трансляції відсутній, трансляція видаляється і адреса повертається в пул. Якщо потрібно створити трансляцію, а вільних адрес в пулі немає, то пакет відкидається. Іншими словами, добре б, щоб число внутрішніх адрес було ненабагато більше числа адрес в пулі, інакше висока ймовірність проблем з виходом в WAN.
3. Overloading(чи PAT) дозволяє перетворювати кілька внутрішніх адрес в одну зовнішню. Для здійснення такої трансляції використовуються порти, тому такий NAT називають PAT (Port Address Translation). За допомогою PAT можна перетворювати внутрішню адресу в зовнішню адресу, задану через пул або через адресу на зовнішньому інтерфейсі. [2]

**Хід роботи**

**Завдання №1.**

Створюємо та налаштовуємо мережу з лабораторної роботи(рис. 1). Є зовнішня адреса 20.20.20.20 (зовнішній інтерфейс fa0/1) і внутрішня мережа 10.10.10.0 (внутрішній інтерфейс fa0/0). Потрібно налаштувати NAT.

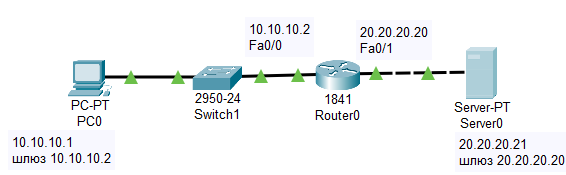


Рисунок 1. Схема мережні завдання 1.

На R0 додаємо access-list, дозволяємо всі (any). Дозволяємо весь трафік, тобто, будь-яку IP-адресу (рис. 2).

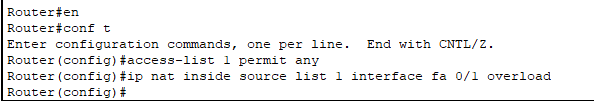
****

Рисунок 2, Складаємо лист допуску

**Створюємо правило трансляції**

Налаштуємо трансляцію на інтерфейсах (на внутрішньому inside, на зовнішньому – outside), тобто, для R0 вказуємо внутрішній і зовнішній порти (рис. 3)

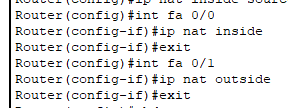
****

Рисунок 3. . Для R0 призначаємо внутрішній і зовнішній порти

Виходимо з режиму глобального конфігурування і записуємо налаштування роутера у мікросхему пам’яті (рис. 4)

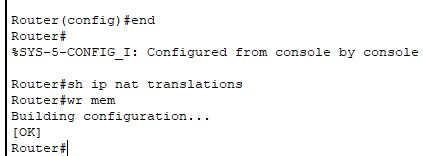


Рисунок 4. . Зберігаємо налаштування

**Перевіряємо роботу мережі (перегляд стану таблиці NAT)**

З PC0 пінгуємо провайдера і переконаємося, що PC1 і сервер можуть спілкуватися (рис. 5).

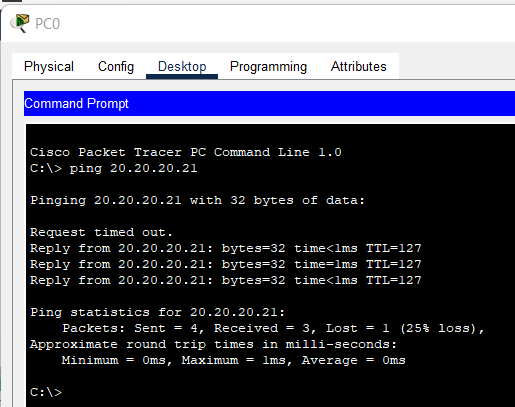
****

Рисунок 5. З внутрішньої мережі пінгуємо зовнішню мережу

Для перегляду стану таблиці NAT, одночасно з пінгом використовуйте команду Router # sh ip nat translations (запущено пінг з машини 10.10.10.1, тобто, з PC1 на адресу 20.20.20.21, тобто, на S0) – рис. 6.

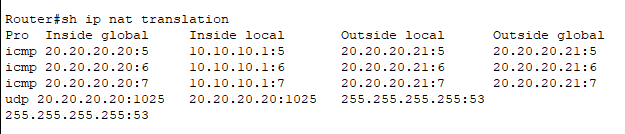
****

Рисунок 6. Під час пінгу переглядаємо стан таблиці NAT

Переконаємося в успішній маршрутизації в режимі симуляції.

**Завдання №2.**

Створюємо та налаштовуємо мережу з лабораторної роботи(рис. 7).

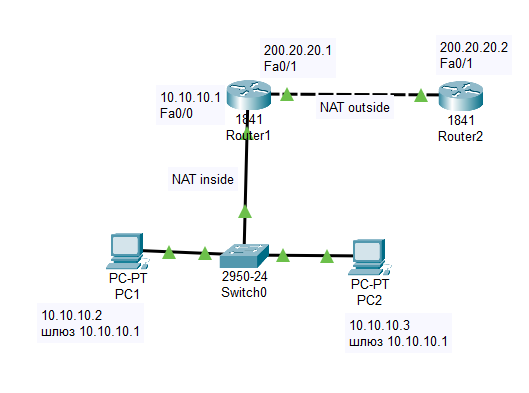


Рисунок 7. Схема мережні завдання 2

**Налаштування R1**

Крок 1. Налаштування дефолту на R1

**R1(config)# ip route 0.0.0.0 0.0.0.0 200.20.20.2 102**

Крок 2. Налаштування внутрішнього інтерфейсу у відношення NAT

***R1(config)# interface fastethernet 0/0***

***R1(config-if)# ip nat inside***

Крок 3. Налаштування зовнішнього інтерфейсу у відношення NAT

***R1(config)# interface fastethernet 0/1***

***R1(config-if)# ip nat outside***

Крок 4. Налаштування зіставлення ІР-адрес.

***R1(config)# ip nat inside source static 10.10.10.2 200.10.21.5***(рис. 8)

У результаті цієї команди ІР-адресі 200.10.21.5 завжди буде відповідати внутрішня ІР-адреса 10.10.10.2, тобто якщо звертатимемося за адресою 200.10.21.5 то відповідати буде PC1.

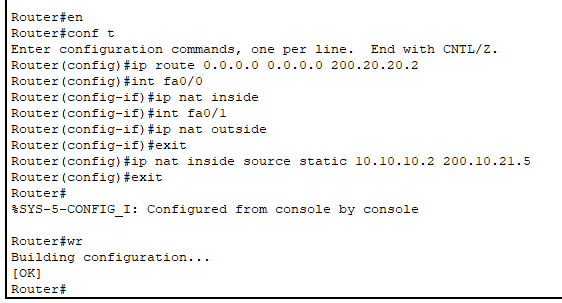
**

Рисунок 8. Налаштування R1

Перевіримо, що R1 бачить сусідні мережі (рис. 9).

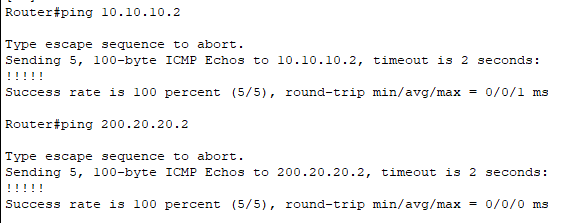


Рисунок 9. R1 бачить PC1 і R2

Перевіримо механізм роботи статичного NAT: команда ***show ip nat* *translations*** виводить активні перетворення, а команда ***show ip nat statistics***виводить статистику по NAT перетворенням (рис. 10).

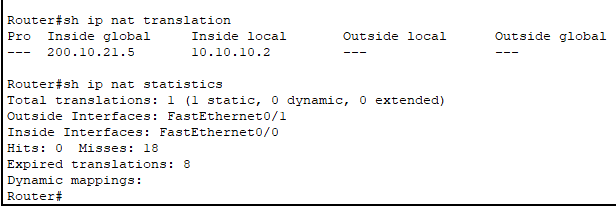
****

Рисунок 10. Перевірка механізму роботи NAT

З рисунку бачимо, що глобальній ІР-адресі 200.10.21.5 відповідає локальна ІР-адреса 10.10.10.2, а також, який інтерфейс є зовнішнім, а який - внутрішній.

**Завдання №3.**

Використовуємо мережу аналогічну як в завданні 2.

**Налаштування R1**

Крок 1. Налаштування на R1 списку доступу, що відповідає адресам LAN

***R1 (config) # access-list 1 permit 10.10.10.0 0.0.0.255***

Тут 0.0.0.225 - зворотна (інверсна) маска для адреси 10.10.10.0.

Крок 2. Налаштування пулу адрес

***R1 (config) # ip nat pool white-address 200.20.20.1 200.20.20.30 netmask 255.255.255.0***

Крок 3. Налаштування трансляції

***R1 (config) # ip nat inside source list 1 pool white-address***

Крок 4. Налаштування внутрішнього інтерфейсу у відношення NAT

***R1 (config) # interface fastethernet 0/0***

***R1 (config-if) # ip nat inside***

Крок 5. Налаштування зовнішнього інтерфейсу в відношення NAT

***R1 (config)# interface fastethernet 0/1***

***R1 (config-if)# ip nat outside*** (рис. 11).

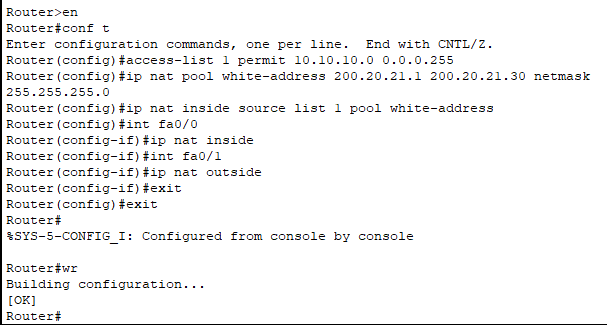


Рисунок 11. Налаштування Router 1

Перевіримо, що R1 бачить сусідні мережі (рис. 12)

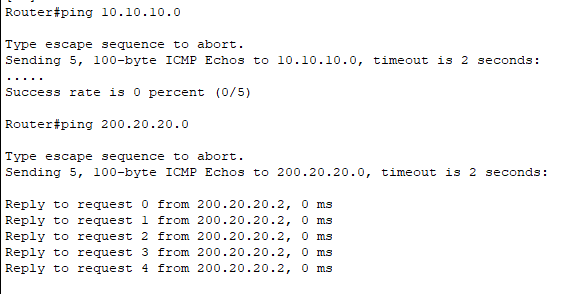


Рисунок 12. R1 бачить підмережі 10.10.10.0 і 200.20.20.0

Перевіримо механізм роботи динамічного NAT: для цього виконаємо одночасно(паралельно) команди ***ping*** і ***show ip nat translations***. *Командою* ***show ip nat statistics*** виведемо статистику по NAT перетворенням(рис. 13).

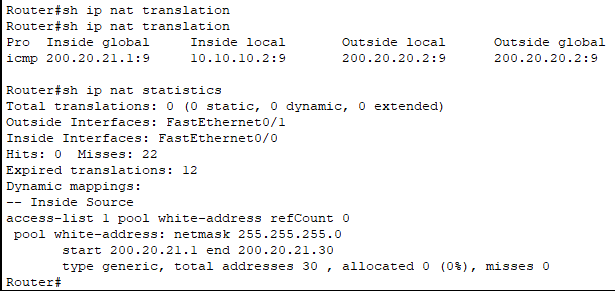


Рисунок 13. Адреси: глобальна, внутрішня, зовнішня та статистика роботи динамічного NAT

Бачимо, що локальним адресам відповідає пул зовнішніх адрес від 200.20.20.1 до 20.20.20.30.

**Завдання №4.**

Використовуємо мережу аналогічну як в завданні 2.

**Налаштування R1**

Крок 1. Налаштування списку доступу, що відповідає внутрішнім приватним адресам.

***R1(config)# access-list 1 permit 10.10.10.0 0.0.0.255***

Крок 2. Налаштування трансляції

***R1(config)# ip nat inside source list 1 interface fastethernet 0/1 overload***

Крок 3. Налаштування внутрішнього інтерфейсу у відношенні NAT

***R1(config)# interface fastethernet 0/0***

***R1(config-if)# ip nat inside***

Крок 4. Налаштування NAT на інтерфейсі

***R1(config)# interface fastethernet 0/1***

***R1(config-if)# ip nat outside***

Нижче дано повний лістинг команд по конфігуруванню R1 (рис. 14)

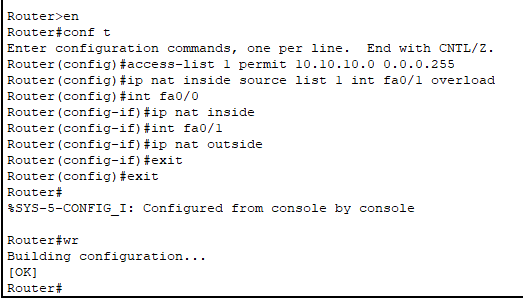


Рисунок 14. Налаштування Router 1

Перевіримо, що R1 бачить сусідні мережі. Перевіримо механізм роботи динамічного NAT: для цього виконаємо одночасно(паралельно) команди ***ping*** і ***show ip nat translations***. (рис. 15)

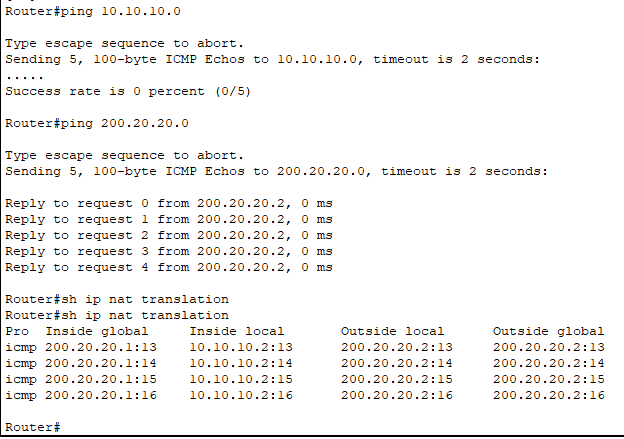


Рисунок 15. Перевірка роботи маскардингу

Перевіряємо роботу в режимі симуляції.

**Висновки**

Виконуючи дану лабораторну роботу я дізнався про те, що таке NAT, та навчився налаштовувати статичний та динамічний NAT, а також динамічний NAT Overload(PAT).

**Список джерел**

1. https://habr.com/ru/post/583172/
2. Комп’ютерний практикум № 8.