**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**

**ІНСТИТУТ БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ ТА СОЦІАЛЬНИХ НАУК**

**КУРСОВА РОБОТА**

з дисципліни

**«КОМП’ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ**

**(РІВЕНЬ D - БЕЗПЕКА КОМП`ЮТЕРНИХ СИСТЕМ)»**

на тему: Розробка комп’ютерної мережі та конфігурування мережевого обладнання.

Студента 3 курсу \_\_\_\_\_ групи

спеціальності «Кібербезпека»

Керівник:

Гордєєва Д. В.

Національна шкала

Кількість балів:

Оцінка: ECTS

Члени комісії

м. Київ – 2020 рік

ТЕХНІЧНЕ ЗАВДАННЯ

На розробку та конфігурування комп'ютерної мережі

1. Область застосування — комп'ютерні мережі.
2. Основа розробки — робочий навчальний план дисципліни.
3. Мета та експлуатаційне призначення:
   1. Мета — отримання практичних навичок проектування та конфігурування комп'ютерних мереж;
   2. Призначення розробки — навчальна курсова робота з дисципліни  
      «Комп'ютерні системи та мережі (Рівень D — Безпека комп'ютерних систем)»;
4. Джерела розробки — індивідуальне завдання на курсовий проект з  
   дисципліни, технічні рекомендації з проектування локальних і  
   розподілених мереж і інші технічні матеріали для налаштування окремих компонентів мережі.
5. Технічні вимоги
   1. Мережа складається з трьох окремих LAN, що об'єднуються WAN  
      мережею, побудованою на основі технології віртуальних каналів.
   2. Вимоги для проектування LAN1
      1. Адреса мережі 192.168.4.0
      2. Складається з п'яти сегментів, кількість робочих станцій в кожному з яких становить: 5, 4, 11, 25, 120
      3. Розподіл адресного простору має бути оптимальним;
      4. Для об'єднання окремих сегментів використовуються маршрутизатори;
      5. З'єднання між маршрутизаторами здійснюються за допомогою скрученої пари;
      6. Для обмеження проходження трафіку з одного сегмента в інший повинні бути застосовані стандартні та розширені ACL. Стандартні списки повинні заборонити проходження трафіку з мережі Net4 в мережу Net2, з мережі Net2 в мережу Net1, і з мережі Net1 в мережу Net4. Розширені ACL повинні заборонити проходження трафіку протоколів DNS, HTTP і PING з Net2 до Net5 і FTP, SNMP і SSH з Net1 до Net3. ACL необхідно розмістити в найбільш вдалому місці.
      7. Усередині мережі використовується статична маршрутизація.
      8. На маршрутизаторах Rt2-Rt4 налаштувати DHCP-сервіс і забезпечити динамічне призначення адрес хостам в мережах Net1-Net5.
      9. На маршрутизаторі Rt1 налаштований сервіс трансляції адрес NAT.
   3. Вимоги для проектування LAN2
      1. Адреса мережі 10.0.4.0/24
      2. Складається з 5 сегментів, в яких розташовані ПК користувачів.
      3. Розподілити адресний простір в такий спосіб: в мережах, які з'єднують маршрутизатори, використовувати префікс 30 (маска 255.255.255.252), весь вільний простір, що залишається, рівномірно розділити між мережами, в яких розташовані Switch1 – Switch5.
      4. З'єднання між маршрутизаторами Rt1-Rt4 і Rt2-Rt3 здійснюється за допомогою послідовних інтерфейсів з використанням протоколів канального рівня HDLC і РРР відповідно. Інші з'єднання виконуються за допомогою скрученої пари.
      5. Підключення мережі LAN2 до мережі WAN виконується через маршрутизатор Rt1.
      6. Усередині мережі використовується статична маршрутизація.
      7. На маршрутизаторі Rt1 налаштований сервіс трансляції адрес NAT.
   4. Вимоги для проектування LAN3
      1. Реалізована на основі комутаторів Catalyst 2960 з підтримкою технології віртуальних мереж.
      2. Поділена на три віртуальні сегменти, кожен з яких містить по два сервери.
      3. На комутаторах Sw1 Sw3 до Vlan 2 належать порти FastEthernet3 FastEthernet7 і FastEthernet6-FastEthernet9 відповідно, до Vlan 3 FastEthernet9-FastEthernet15 і FastEthernet15-FastEthernet18 відповідно.
      4. З'єднання між комутаторами здійснюються за допомогою скрученої пари та технології Gigabit Ethernet.
      5. У віртуальних мережах VLAN1, VLAN2 і VLAN3 використовуються адреси 204.10265.0, 214.23.87.0 і 58.0.0.0 відповідно.
   5. Вимоги для проектування WAN
      1. Об'єднання локальних мереж здійснюється за допомогою Frame Relay комутатора з використанням топології Full Mesh.
      2. Адреси інтерфейсів маршрутизаторів, підключених до Frame Relay мережі, що відносяться до мережі з адресою 12.2.0.0/16
      3. З'єднання між локальними мережами здійснюється за допомогою послідовних інтерфейсів.
   6. Загальні вимоги до налаштувань маршрутизаторів
      1. Встановити на всіх маршрутизаторах паролі на консольне з'єднання та на привілейований режим.
      2. Налаштувати доступ через протокол SSH до шлюзових маршрутизаторів.
6. Апаратні вимоги – використання обладнання фірми Cisco
7. Текстова документація розробленої мережі повинна відповідати чинним стандартам України.
8. Стадії та етапи розробки мережі включать розробку та налагодження окремих LAN і об'єднання LAN1-4 за допомогою ГЛОБАЛЬНОЇ мережі.

Розробив студент групи \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ЗМІСТ

[АНОТАЦІЯ 7](#_Toc58419518)

[ВСТУП 8](#_Toc58419519)

[Проектування мережі LAN1 9](#_Toc58419520)

[Побудова мережі 9](#_Toc58419521)

[Розрахунок адресного простору для мереж користувачів 10](#_Toc58419522)

[Розрахунок адресного простору для маршрутизаторів і сервера 12](#_Toc58419523)

[Налаштування адресації DHCP 13](#_Toc58419524)

[Налаштування маршрутизації в мережі 14](#_Toc58419525)

[Налаштування захисту та конфігурація безпеки 16](#_Toc58419526)

[Налаштування правил ACL 16](#_Toc58419527)

[Перевірка роботи правил 18](#_Toc58419528)

[Проектування мережі LAN2 20](#_Toc58419529)

[Створення схеми мережі 20](#_Toc58419530)

[Розрахунок адресного простору 20](#_Toc58419531)

[Налаштування маршрутизації 23](#_Toc58419532)

[Проектування мережі LAN3 29](#_Toc58419533)

[Побудова мережі 29](#_Toc58419534)

[Агрегування каналів 29](#_Toc58419535)

[Налагодження та комутація VLAN 31](#_Toc58419536)

[Підключення серверів 34](#_Toc58419537)

[Налаштування адресації серверів 35](#_Toc58419538)

[Налаштування протоколу HSRP на маршрутизаторах 36](#_Toc58419539)

[Налаштування маршрутизації 38](#_Toc58419540)

[Загальні налаштування активного обладнання 40](#_Toc58419541)

[Налаштування обладнання 40](#_Toc58419542)

[Об'єднання локальних мереж 42](#_Toc58419543)

[Створення та налагодження FrameRelay 42](#_Toc58419544)

[Налаштування трансляції мережевих адрес NAT 46](#_Toc58419545)

[Маршрутизація WAN 47](#_Toc58419546)

[Перевірка зв'язності мережі, перевірка NAT 49](#_Toc58419547)

[ВИСНОВКИ 52](#_Toc58419548)

[ДЖЕРЕЛА 53](#_Toc58419549)

**АНОТАЦІЯ**

# ВСТУП

Сучасний світ нерозривно пов'язаний з інформатизацією. Комп'ютери грають величезну роль в житті нашого суспільства. Для більш ефективного використання їх об'єднують в комп'ютерні мережі, які дозволяють одним комп'ютерам мережі використовувати ресурси як інших комп'ютерів, так і спеціально виділених сервером і мережевого устаткування.

При проектуванні комп'ютерних мереж постає питання їх безпеки та надійності. В окремих випадках, таких як домашні мережі – цими питаннями можна знехтувати, однак комп'ютерна мережа організації, особливо фінансової – повинна відповідати всім вимогам по надійності та безпеки. Це означає, що вона повинна забезпечувати роботу мережевих пристроїв навіть в разі виходу з ладу обладнання, та регламентувати доступ до елементів комп'ютерної мережі, як ззовні її, так і всередині.

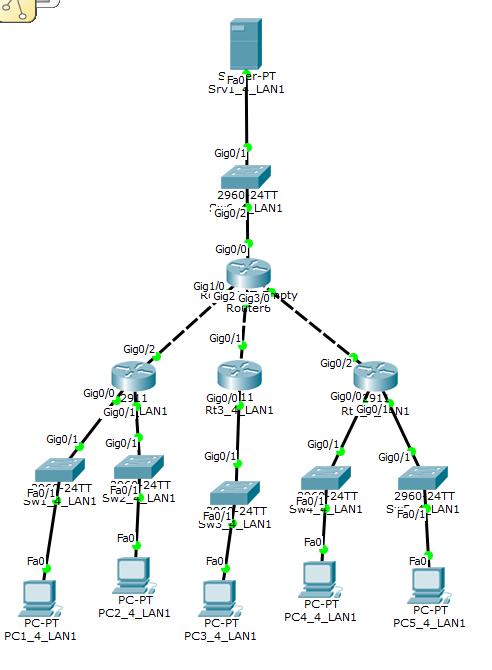
Створення ефективної та безпечної комп'ютерної мережі – складне завдання, яке не може бути вирішено без попереднього проектування та розробки. Для вирішення завдань безпеки та надійності існує багато рішень, як апаратних, так і програмних. Деякі такі рішення будуть розглянуті в даній роботі.

Актуальність даної роботи полягає в тому, що в ній буде спроектована спеціальна комп'ютерна мережа, що складається з трьох окремих локальних мереж, що взаємодіють один з одним. При проектуванні будуть враховані різні аспекти безпеки комп'ютерних мереж, проведено налаштування обладнання, що забезпечує захист від несанкціонованого доступу. Також будуть розглянуті аспекти відмовостійкості комп'ютерних мереж, на прикладі мережі ЦОД.

# Проектування мережі LAN1

## Побудова мережі

Створимо мережу в програмі Cisco Packet Tracer, розмістивши обладнання, підписавши його та з'єднавши. (Мал. 1)



Малюнок 1 створена мережа

## Розрахунок адресного простору для мереж користувачів

Вихідні дані – мережеву адресу 192.168.4.0, це підмережа класу D, що має маску 255.255.255.0. Вона може містити 254 хоста (адресовані можуть бути 256 пристроїв, при цьому 192.168.4.0 – адреса мережі, а 192.168.4.255 – адреса широкомовної розсилки). Потрібно розбити мережу на підмережі, що містять:

* Net1 – 5 вузлів
* Net2 – 4 вузла
* Net3 – 11 вузлів
* Net4 – 25 вузлів
* Net5 – 120 вузлів.

Для максимально ефективного використання адресного простору, необхідно розглядати ці підмережі в порядку зменшення хостів. Тобто, спочатку виділимо підмережу, яка буде мати 120 хостів. Для цього можна розділити вихідну мережу навпіл: вона буде записуватися як 192.168.4.0/25, мати маску 255.255.255.128, адреса широкомовної розсилки 192.168.4.127, і включати адреси з 192.168.4.1 до 192.168.4.126 – всього 126 штук. Потім виділимо підмережу, яка змогла б адресувати 25 вузлів – 192.168.4.128/27, її маска 255.255.255.224, адреса широкомовної розсилки 192.168.4.159, адреси 192.168.4.129-192.168.4.158, 30 хостів.

Потім – підмережа на 11 вузлів: 192.168.4.160/28, маска 255.255.255.240, адреса широкомовної розсилки 192.168.4.175, адреси 192.168.4.161-192.168.4.174,. І дві однакові підмережі, що вміщають максимум 6 вузлів: 192.168.4.176/29, маска 255.255.255.248, адреса широкомовної розсилки 192.168.4.183, адреси 192.168.4.177-192.168.4.182, і підмережа 192.168.4.184/29 з такою-ж маскою, адреса широкомовної розсилки 192.168.4.191, адреси 192.168.4.185-192.168.4.190. При цьому залишиться вільний пул адрес, з 192.168.4.192-192.168.4.255.

Отримані дані відобразимо в таблиці:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ме-режа | Адреса мережи | Маска підмережі | Діапазон | Шіроковещ.  адреса | Місткість мережі |
| Net5 | 192.168.4.0 | 255.255.255.128 | 192.168.4.1-192.168.4.126 | 192.168.4.127 | 126 |
| Net4 | 192.168.4.128 | 255.255.255.224 | 192.168.4.129-192.168.4.158 | 192.168.4.159 | 60 |
| Net3 | 192.168.4.160 | 255.255.255.240 | 192.168.4.161-192.168.4.174 | 192.168.4.175 | 14 |
| Net1 | 192.168.4.176 | 255.255.255.248 | 192.168.4.177-192.168.4.182 | 192.168.4.183 | 6 |
| Net2 | 192.168.4.184 | 255.255.255.248 | 192.168.4.185-192.168.4.190 | 192.168.4.191 | 6 |
| Ост. |  |  | 192.168.4.192-192.168.4.255 |  |  |

Таблиця 1. Розподіл адрес мережі Lan1

Розподіл адрес можна відобразити на діаграмі:

Діаграма 1. Розподіл адрес мережі Lan1

Отриманий залишок адрес дозволяє організувати ще одну підмережу на 62 хости – 192.168.1.192/26, з маскою 255.255.255.192, або розбити її на підмережі меншого розміру – по 30, 14, 6, або 2 хости відповідно. Таким чином, було досягнуто оптимальне використання адресного простору.

## Розрахунок адресного простору для маршрутизаторів і серверу

Оскільки в завданні до роботи не було визначено адресний простір для міжмережової маршрутизації, а також для серверу, я виберу його сам.

Для адресації між маршрутизаторами я використовую підмережі з приватного діапазону 10.0.0.0, причому в підсетях буде всього по два вузли – тобто це буде підмережі з маскою 30.

Зведемо їх в таблицю:

|  |  |  |  |
| --- | --- | --- | --- |
| Вузол | Порт | Адреса | З ким з'єднує |
| Rt1\_4\_LAN1 | Gig0/0 | 10.0.0.13/30 | Sw6\_4\_LAN1 |
| Gig1/0 | 10.0.0.2/30 | Rt2\_4\_LAN1 |
| Gig2/0 | 10.0.0.6/30 | Rt3\_4\_LAN1 |
| Gig3/0 | 10.0.0.10/30 | Rt4\_4\_LAN1 |
| Rt2\_4\_LAN1 | Gig0/2 | 10.0.0.1/30 | Rt1\_4\_LAN1 |
| Rt3\_4\_LAN1 | Gig0/1 | 10.0.0.5/30 |
| Rt4\_4\_LAN1 | Gig0/2 | 10.0.0.9/30 |

Таблиця 2. Адреси мереж для комутації маршрутизаторів

Налаштуємо ці адреси для інтерфейсів маршрутизаторів, наприклад, для маршрутизатору Rt1\_4\_LAN1:

Rt1\_4\_LAN1#conf t

Rt1\_4\_LAN1(config)#int gig1/0

Rt1\_4\_LAN1(config-if)#ip add 10.0.0.2 255.255.255.252

Rt1\_4\_LAN1(config)# int gig2/0

Rt1\_4\_LAN1(config-if)#ip add 10.0.0.6 255.255.255.252

Rt1\_4\_LAN1(config)#int gig3/0

Rt1\_4\_LAN1(config-if)#ip add 10.0.0.10 255.255.255.252

Rt1\_4\_LAN1(config)#int gig0/0

Rt1\_4\_LAN1(config-if)#ip add 10.0.0.13 255.255.255.252

Аналогічно налаштуємо на інших маршрутизаторах.

## Налаштування адресації DHCP

Для автоматичної видачі адрес вузлам підмереж налаштуємо DHCP-зони на маршрутизаторах. Наведемо як приклад послідовність команд для налаштування зони DHCP для мережі Net1:

Rt2\_4\_LAN1(config)#int gig 0/0

Rt2\_4\_LAN1(config-if)#ip add 192.168.4.177 255.255.255.248

Rt2\_4\_LAN1(config-if)#ex

Rt2\_4\_LAN1(config)#ip dhcp pool net1

Rt2\_4\_LAN1(dhcp-config)#net 192.168.4.176 255.255.255.248

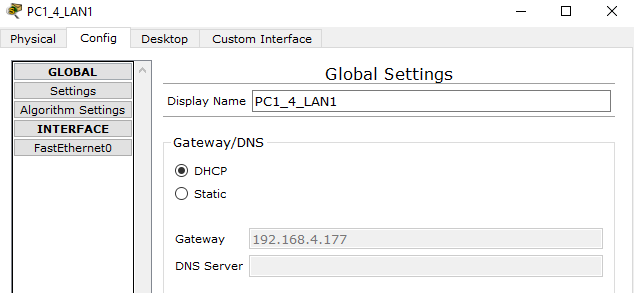
Rt2\_4\_LAN1(dhcp-config)#default-router 192.168.4.177

Rt2\_4\_LAN1(dhcp-config)#ex

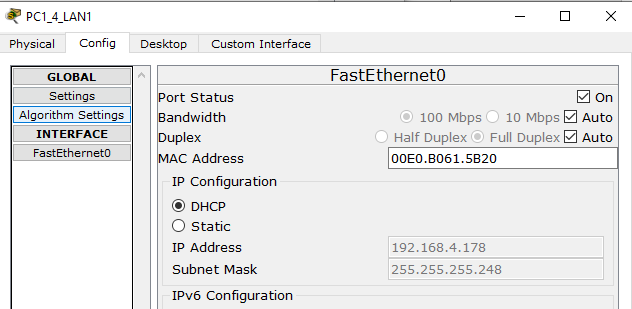
Rt2\_4\_LAN1(config)#ip dhcp excluded-address 192.168.4.177

За допомогою даних команд ми налаштували адресу для інтерфейсу gig0/0 маршрутизатору Rt2\_4\_LAN1, підключеного до мережі Net1 (була взята перша адреса діапазону), потім створили зону з ім'ям net1, вказали для неї адресу мережі та маршрут за замовчуванням. Також, після виходу з налаштування зони, ми додали адресу маршрутизатору в виключення – щоб він не був виданий клієнтам.

Щоб перевірити коректність налаштувань, досить активувати DHCP на клієнті (Мал. 2-3):



Малюнок 2 отримання налаштувань по DHCP



Малюнок 3 отримання налаштувань по DHCP

Аналогічно налаштовуємо зони для усіх цих служб в усіх інших маршрутизаторах.

## Налаштування маршрутизації в мережі

Згідно з завданням, необхідно налаштувати статичну маршрутизацію – тобто вказати маршрути в таблицях маршрутизації явно. Для маршрутизаторів Rt2\_4\_LAN1, Rt3\_4\_LAN1 і Rt4\_4\_LAN1 досить буде просто вказати маршрут за замовчуванням – в якості такого маршруту виступить відповідний інтерфейс маршрутизатору Rt1\_4\_LAN1. Наприклад, для Rt3\_4\_LAN1 команда буде виглядати так:

Rt3\_4\_LAN1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.6

На маршрутизаторі Rt1\_4\_LAN1 потрібно налаштувати таблицю маршрутизації, вказавши шляхи до мереж. При цьому, можна об'єднати дві мережі, Net1 і Net2, в одну – зменшивши таким чином розмір таблиці маршрутизації. Команди будуть такі:

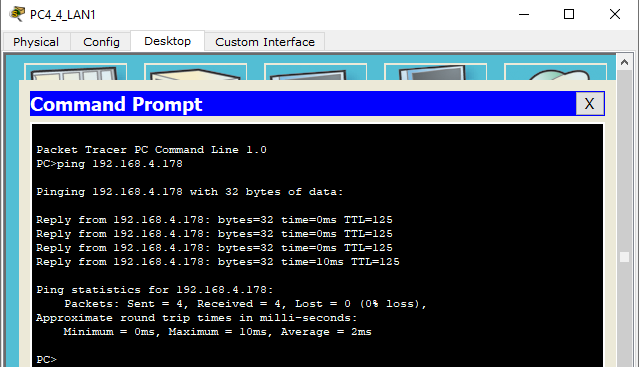
Rt1\_4\_LAN1(config)#ip route 192.168.4.0 255.255.255.128 10.0.0.9

Rt1\_4\_LAN1(config)#ip route 192.168.4.128 255.255.255.224 10.0.0.9

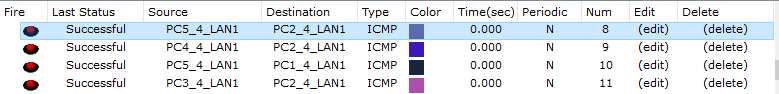
Rt1\_4\_LAN1(config)#ip route 192.168.4.160 255.255.255.240 10.0.0.5

Rt1\_4\_LAN1(config)#ip route 192.168.4.176 255.255.255.240 10.0.0.1

Щоб перевірити коректність налаштувань маршрутизації, можна пропінгувати вузли або використовувати інструмент Simple PDU (мал. 4-5):



Малюнок 4 перевірка командою ping



Малюнок 5 перевірка інструментом Simple PDU

## Налаштування захисту та конфігурація безпеки

### Налаштування правил ACL

Для налаштування захисту та безпеки в створюваної мережі, налаштуємо списки контролю доступу ACL, згідно із завданням. Необхідно заборонити проходження трафіку:

* З мережі Net4 в мережу Net2
* З мережі Net2 в мережу Net1
* З мережі Net1 в мережу Net4
* З мережі Net2 в мережу Net5 – для протоколів DNS, HTTP, PING
* З мережі Net1 в мережу Net3 – для протоколів FTP, SNMP, SSH

Налаштуємо ACL для заборони трафіку з мережі Net2 в мережу Net1:

Rt2\_4\_LAN1(config)#ip access-list standard Net2\_Net1

Rt2\_4\_LAN1(config-std-nacl)#deny 192.168.4.184 0.0.0.7

Rt2\_4\_LAN1(config-std-nacl)#permit any

Rt2\_4\_LAN1(config-std-nacl)#ex

Rt2\_4\_LAN1(config)#int gig 0/0

Rt2\_4\_LAN1(config-if)#ip access-group Net2\_Net1 out

Це правило працює для вихідного трафіку на інтерфейсі Gig0/0 маршрутизатору Rt2\_4\_LAN1.

Налаштуємо ACL для заборони трафіку з мережі Net4 в мережу Net2:

Rt2\_4\_LAN1(config)#ip access-list standard Net4\_Net2

Rt2\_4\_LAN1(config-std-nacl)#deny 192.168.4.128 0.0.0.127

Rt2\_4\_LAN1(config-std-nacl)#permit any

Rt2\_4\_LAN1(config-std-nacl)#ex

Rt2\_4\_LAN1(config)#int gig 0/1

Rt2\_4\_LAN1(config-if)#ip access-group Net4\_Net2 out

Це правило працює для вихідного трафіку на інтерфейсі Gig0/1 маршрутизатору Rt2\_4\_LAN1.

Налаштуємо ACL для заборони трафіку з мережі Net1 в мережу Net4:

Rt4\_4\_LAN1(config)#ip access-list standard Net1\_Net4

Rt4\_4\_LAN1(config-std-nacl)#deny 192.168.4.176 0.0.0.7

Rt4\_4\_LAN1(config-std-nacl)#permit any

Rt4\_4\_LAN1(config-std-nacl)#ex

Rt4\_4\_LAN1(config)#int gig 0/0

Rt4\_4\_LAN1(config-if)#ip access-group Net1\_Net4 out

Це правило працює для вихідного трафіку на інтерфейсі Gig0/0 маршрутизатору Rt4\_4\_LAN1.

Налаштуємо розширені правила на маршрутизаторі Rt1\_4\_LAN1:

Rt1\_4\_LAN1(config)#ip access-list extended Other

Rt1\_4\_LAN1(config-ext-nacl)#deny tcp 192.168.4.184 0.0.0.7 192.168.4.0 0.0.0.127 eq www

Rt1\_4\_LAN1(config-ext-nacl)#deny udp 192.168.4.184 0.0.0.7 192.168.4.0 0.0.0.127 eq 53

Rt1\_4\_LAN1(config-ext-nacl)#deny icmp 192.168.4.184 0.0.0.7 192.168.4.0 0.0.0.127 echo

Rt1\_4\_LAN1(config-ext-nacl)#deny tcp 192.168.4.176 0.0.0.7 192.168.4.160 0.0.0.15 eq ftp

Rt1\_4\_LAN1(config-ext-nacl)#deny udp 192.168.4.176 0.0.0.7 192.168.4.160 0.0.0.15 eq snmp

Rt1\_4\_LAN1(config-ext-nacl)#deny tcp 192.168.4.176 0.0.0.7 192.168.4.160 0.0.0.15 eq 22

Rt1\_4\_LAN1(config-ext-nacl)#permit ip any any

Rt1\_4\_LAN1(config-ext-nacl)#ex

Rt1\_4\_LAN1(config)#int gig 1/0

Rt1\_4\_LAN1(config-if)#ip acce

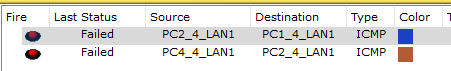
Rt1\_4\_LAN1(config-if)#ip access-group Other in

У цих правилах забороняються зазначені в завданні протоколи, при цьому вказується протокол 3 рівня, для якого працює правило, та який використовується порт або тип сервісу. Правило застосовується на інтерфейс Gig1/0, для вхідного трафіку.

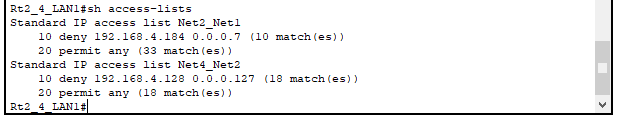
### Перевірка роботи правил

Для перевірки роботи правил ACL можна використовувати як інструмент Simple PDU, так і підключення на певні порти (для перевірки доступності по окремим протоколам). Спрацьовування правила на комутаторі відбивається в зміні значень лічильників.

Перевіримо правила, що працюють на маршрутизаторі 2 (мал. 6-7):

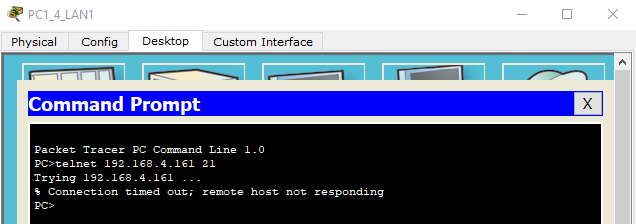


Малюнок 6 перевірка правил – блокування трафіку

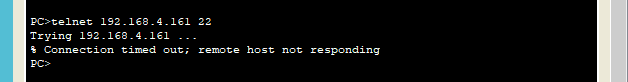


Малюнок 7 перевірка правил – значення лічильників

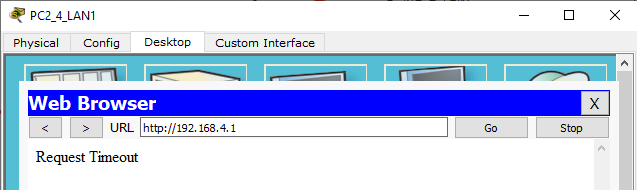
Також перевіримо роботу ACL, спрямованих на блокування певних протоколів (мал. 8-11):



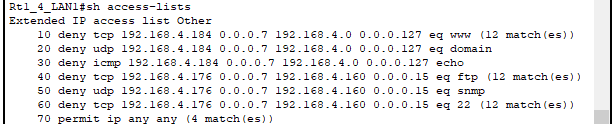
Малюнок 8 перевірка блокування протоколу FTP



Малюнок 9 перевірка блокування протоколу SSH



Малюнок 10 перевірка блокування протоколу HTTP

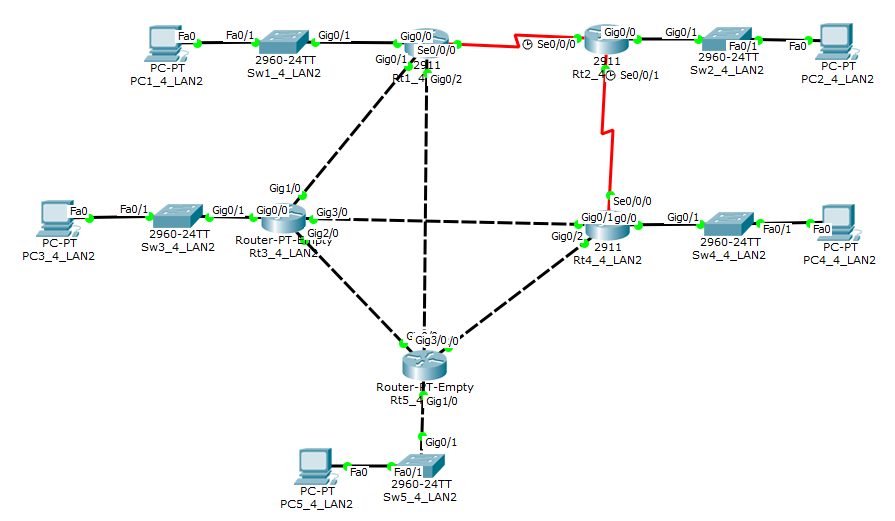


Малюнок 11 лічильники спрацьовування правил

# Проектування мережі LAN2

## Створення схеми мережі

Створимо схему мережі відповідно до варіанту, розташувавши обладнання, підписавши його та з'єднавши (мал. 12).



Малюнок 12 схема мережі LAN2

## Розрахунок адресного простору

Згідно з вимогами завдання, потрібно використовувати мережу 10.1.4.0/24, при цьому для зв'язку між маршрутизаторами використовувати підмережі з маскою 255.255.255.252, що складаються з 2 хостів.

Таких підмереж повинно вийти 7 штук. Також потрібно адресувати 5 підмереж з комутаторами, рівномірно розподіливши адресний простір. Абсолютно рівномірно розподілити адреси в такому випадку неможливо, але з урахуванням вимоги використовувати весь адресний простір, оптимальним мені здається наступний поділ:

* Виділити дві підмережі з маскою 255.255.255.192, що містять по 62 вузли – для двох мереж користувачів
* Виділити три підмережі з маскою 255.255.255.224, що містять по 30 вузлів – для трьох мереж користувачів
* Діапазон, який залишився розбити на підмережі з маскою 255.255.255.252, що містять по 2 вузли – для мереж комутаторів

Складемо таблицю розподілу адрес:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Мережа | Адреса | Маска | Діапазон  адрес | Шіроковещ.  адреса | Розмір мережі |
| Net1 | 10.1.4.0 | 255.255.255.192 | 10.1.4.1-10.1.4.62 | 10.1.4.63 | 62 |
| Net2 | 10.1.4.64 | 10.1.4.65-10.1.4.126 | 10.1.4.127 | 62 |
| Net3 | 10.1.4.128 | 255.255.255.224 | 10.1.4.129-10.1.4.158 | 10.1.4.159 | 30 |
| Net4 | 10.1.4.160 | 10.1.4.161-10.1.4.190 | 10.1.4.191 | 30 |
| Net5 | 10.1.4.192 | 10.1.4.193-10.1.4.221 | 10.1.4.223 | 30 |
| Rt1-Rt2 | 10.1.4.224 | 255.255.255.252 | 10.1.4.225-10.1.4.226 | 10.1.4.227 | 2 |
| Rt2-Rt4 | 10.1.4.228 | 10.1.4.229-10.1.4.230 | 10.1.4.231 | 2 |
| Rt3-Rt1 | 10.1.4.232 | 10.1.4.233-10.1.4.234 | 10.1.4.235 | 2 |
| Rt3-Rt5 | 10.1.4.236 | 10.1.4.237-10.1.4.238 | 10.1.4.239 | 2 |
| Rt5-Rt4 | 10.1.4.240 | 10.1.4.241-10.1.4.242 | 10.1.4.243 | 2 |
| Rt1-Rt5 | 10.1.4.244 | 10.1.4.245-10.1.4.246 | 10.1.4.247 | 2 |
| Rt3-Rt4 | 10.1.4.248 | 10.1.4.249-10.1.4.250 | 10.1.4.251 | 2 |

Таблиця 3. Розподіл адрес мережі LAN2

Як видно, при такому розподілі адресний простір використовується повністю.

Складемо таблицю мережевих адрес для маршрутизаторів:

|  |  |  |  |
| --- | --- | --- | --- |
| Маршрутизатор | Порт | Адреса | З ким з'єднує |
| Rt1\_4\_LAN2 | Gig0/0 | 10.1.4.1/26 | Sw1\_4\_LAN2 |
| Gig0/1 | 10.1.4.234/30 | Rt3\_4\_LAN2 |
| Gig0/2 | 10.1.4.245/30 | Rt5\_4\_LAN2 |
| Se0/0/0 | 10.1.4.225/30 | Rt2\_4\_LAN2 |
| Rt2\_4\_LAN2 | Gig0/0 | 10.1.4.65/26 | Sw2\_4\_LAN2 |
| Se0/0/0 | 10.1.4.226/30 | Rt1\_4\_LAN2 |
| Se0/0/1 | 10.1.4.229/30 | Rt4\_4\_LAN2 |
| Rt4\_4\_LAN2 | Gig0/0 | 10.1.4.161/27 | Sw4\_4\_LAN2 |
| Gig0/1 | 10.1.4.250/30 | Rt3\_4\_LAN2 |
| Gig0/2 | 10.1.4.242/30 | Rt5\_4\_LAN2 |
| Se0/0/0 | 10.1.4.230/30 | Rt2\_4\_LAN2 |
| Rt3\_4\_LAN2 | Gig0/0 | 10.1.4.129/27 | Sw3\_4\_LAN2 |
| Gig1/0 | 10.1.4.233/30 | Rt1\_4\_LAN2 |
| Gig2/0 | 10.1.4.237/30 | Rt5\_4\_LAN2 |
| Gig3/0 | 10.1.4.249/30 | Rt4\_4\_LAN2 |
| Rt5\_4\_LAN2 | Gig0/0 | 10.1.4.238/30 | Rt3\_4\_LAN2 |
| Gig1/0 | 10.1.4.193/27 | Sw5\_4\_LAN2 |
| Gig2/0 | 10.1.4.246/30 | Rt1\_4\_LAN2 |
| Gig3/0 | 10.1.4.241/30 | Rt4\_4\_LAN2 |

Таблиця 4. Мережеві адреси портів маршрутизаторів мережі LAN2

Налаштуємо мережеві адреси на пристроях, відповідно до складеного плану. Також налаштуємо на кожному маршрутизаторі пул DCHP для тих мереж, які вони обслуговують. Наприклад, для першого маршрутизатору:

Rt1\_4\_LAN2(config)#int gig 0/0

Rt1\_4\_LAN2(config-if)#ip add 10.1.4.1 255.255.255.192

Rt1\_4\_LAN2(config-if)#int gig 0/1

Rt1\_4\_LAN2(config-if)#ip add 10.1.4.234 255.255.255.252

Rt1\_4\_LAN2(config-if)#int gig 0/2

Rt1\_4\_LAN2(config-if)#ip add 10.1.4.245 255.255.255.252

Rt1\_4\_LAN2(config-if)#int se 0/0/0

Rt1\_4\_LAN2(config-if)#ip add 10.1.4.225 255.255.255.252

Rt1\_4\_LAN2(config-if)#ex

Rt1\_4\_LAN2(config)#ip dhcp pool Net1

Rt1\_4\_LAN2(dhcp-config)#net 10.1.4.0 255.255.255.192

Rt1\_4\_LAN2(dhcp-config)#default-router 10.1.4.1

Rt1\_4\_LAN2(dhcp-config)#ex

Rt1\_4\_LAN2(config)#ip dhcp excluded-address 10.1.4.1

Аналогічно налаштуємо інші маршрутизатори.

## Налаштування маршрутизації

Маршрутизація – це процес визначення маршруту в мережах мережі. Маршрутизація в локальних обчислювальних мережах необхідна, коли мережа розбита на підмережі, і одержувач мережевого пакету знаходиться в іншій мережі, ніж відправник (або ж пакет адресований в глобальну мережу). Розрізняють статичну та динамічну маршрутизацію. У разі статичної маршрутизації необхідно вказати мережу або вузол призначення, та відповідну адресу, куди буде передано пакет. Також може бути зазначена не адреса, а інтерфейс, на який буде переданий пакет. Можна також не вказувати окремі мережі та вузли, а використовувати так званий маршрут за замовчуванням – тобто передавати всі пакети, призначені для інших мереж, на який-небудь маршрутизатор. В такому випадку часто вказують маршрут як запис 0.0.0.0 з маскою 0.0.0.0 (для адресації IPv4).

Статична маршрутизація простіше в налаштуванні в невеликих мережах, однак при великій кількості вузлів вона стає скрутною. Крім того, в разі зміни конфігурації мережі статично сконфігурована маршрутизація може виявитися непрацездатною. Щоб вирішити ці проблеми, застосовується динамічна маршрутизація.

Протоколи динамічної маршрутизації створюють таблиці маршрутизації на мережевих пристроях, відштовхуючись від отриманої від сусідніх маршрутизаторів інформації. У загальному випадку, можна сказати, що кожен маршрутизатор сповіщає своїх сусідів про ті мережі, які йому доступні – і отримує аналогічну інформацію від них. Крім автоматичного заповнення таблиць маршрутизації, динамічно протоколи дозволяють гнучко реагувати на зміни топології мережі – міняти маршрут в разі виходу з ладу лінії зв'язку або пристрою.

Згідно з вимогами завдання, потрібно налаштувати статичну маршрутизацію.

Оскільки розглянута мережа має надмірність – тобто до хосту може вести кілька маршрутів – ми налаштуємо статичну маршрутизацію так, щоб існували додаткові маршрути. Для цього можна використовувати параметр ваги маршруту. У таблиці маршрутизації будуть вибиратися маршрути з меншою вагою. За замовчуванням статичний маршрут має вагу 1, тому маршрути з будь-якою вагою, більшим 1, з'являться в таблиці тільки в тому випадку, якщо маршрут з меншою вагою недосяжний.

Rt1\_4\_LAN2(config)#ip route 10.1.4.236 255.255.255.252 10.1.4.233

Rt1\_4\_LAN2(config)#ip route 10.1.4.236 255.255.255.252 10.1.4.244 10

Rt1\_4\_LAN2(config)#ip route 10.1.4.236 255.255.255.252 10.1.4.226 20

Rt1\_4\_LAN2(config)#ip route 10.1.4.240 255.255.255.252 10.1.4.246

Rt1\_4\_LAN2(config)#ip route 10.1.4.240 255.255.255.252 10.1.4.233 10

Rt1\_4\_LAN2(config)#ip route 10.1.4.240 255.255.255.252 10.1.4.226 20

Rt1\_4\_LAN2(config)#ip route 10.1.4.228 255.255.255.252 10.1.4.226

Rt1\_4\_LAN2(config)#ip route 10.1.4.228 255.255.255.252 10.1.4.246 10

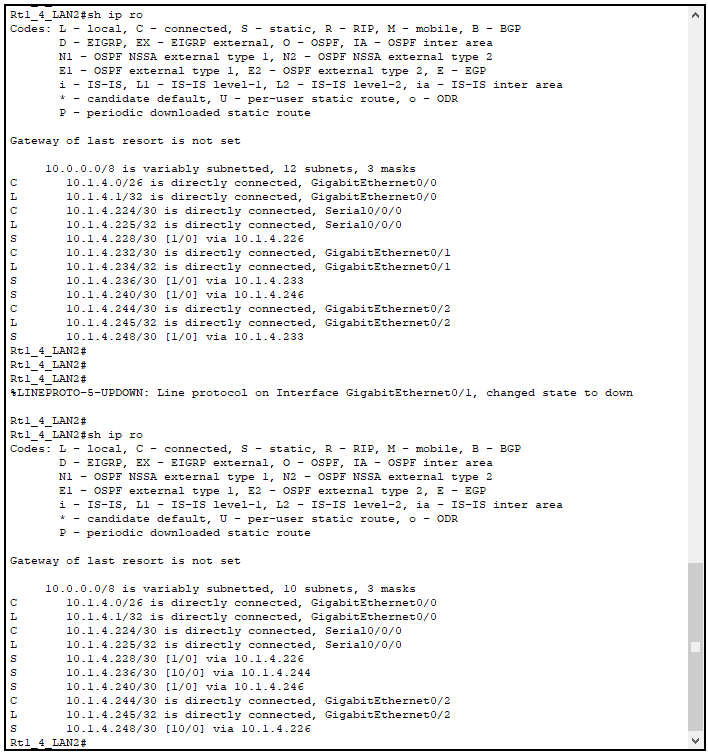
Rt1\_4\_LAN2(config)#ip route 10.1.4.228 255.255.255.252 10.1.4.233 20

Rt1\_4\_LAN2(config)#ip route 10.1.4.248 255.255.255.252 10.1.4.233

Rt1\_4\_LAN2(config)#ip route 10.1.4.248 255.255.255.252 10.1.4.226 10

Rt1\_4\_LAN2(config)#ip route 10.1.4.248 255.255.255.252 10.1.4.246 20

В такому випадку маршрутизатор відреагує на пропажу лінії зв'язку – прибравши з таблиці недосяжний маршрут, і застосувавши замість нього маршрут з великою вагою – але досяжний. Перевіримо це. Для цього спочатку переглянемо таблицю маршрутизації, потім відключимо інтерфейс на сусідньому маршрутизаторі, та перевіримо таблицю знову.



Малюнок 13 Перевірка роботи статичної маршрутизації

Як видно, спочатку маршрут до мережі 10.1.4.236/30 лежав через маршрутизатор 10.1.4.233, а коли він став недоступний – змінився на 10.1.4.244. Таким чином була реалізована відмовостійкість створеної мережі.

Аналогічно поступимо на всіх інших маршрутизаторах – вкажемо дублюючі маршрути з великими вагами.

Також на всіх маршрутизаторах, крім 4, вкажемо найближчий інтерфейс маршрутизатора №4 як маршрут за замовчуванням. Налаштування маршруту на маршрутизаторі 4 буде виконано пізніше, при об'єднанні мереж.

Результуючі таблиці маршрутизації такі:

Rt1\_4\_LAN2#sh ip ro static

10.0.0.0/8 is variably subnetted, 16 subnets, 4 masks

S 10.1.4.64/26 [1/0] via 10.1.4.226

S 10.1.4.128/27 [1/0] via 10.1.4.233

S 10.1.4.160/27 [1/0] via 10.1.4.226

S 10.1.4.192/27 [1/0] via 10.1.4.246

S 10.1.4.228/30 [1/0] via 10.1.4.226

S 10.1.4.236/30 [1/0] via 10.1.4.233

S 10.1.4.240/30 [1/0] via 10.1.4.246

S 10.1.4.248/30 [1/0] via 10.1.4.233

S\* 0.0.0.0/0 [1/0] via 10.1.4.230

Rt2\_4\_LAN2#sh ip ro stat

10.0.0.0/8 is variably subnetted, 15 subnets, 4 masks

S 10.1.4.0/26 [1/0] via 10.1.4.225

S 10.1.4.128/27 [1/0] via 10.1.4.225

S 10.1.4.160/27 [1/0] via 10.1.4.230

S 10.1.4.192/27 [1/0] via 10.1.4.225

S 10.1.4.232/30 [1/0] via 10.1.4.225

S 10.1.4.236/30 [1/0] via 10.1.4.230

S 10.1.4.240/30 [1/0] via 10.1.4.230

S 10.1.4.244/30 [1/0] via 10.1.4.225

S 10.1.4.248/30 [1/0] via 10.1.4.230

S\* 0.0.0.0/0 [1/0] via 10.1.4.230

Rt3\_4\_LAN2#sh ip ro stat

10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks

S 10.1.4.0/26 [1/0] via 10.1.4.234

S 10.1.4.64/26 [1/0] via 10.1.4.234

S 10.1.4.160/27 [1/0] via 10.1.4.250

S 10.1.4.192/27 [1/0] via 10.1.4.238

S 10.1.4.224/30 [1/0] via 10.1.4.234

S 10.1.4.228/30 [1/0] via 10.1.4.250

S 10.1.4.240/30 [1/0] via 10.1.4.238

S 10.1.4.244/30 [1/0] via 10.1.4.234

S\* 0.0.0.0/0 [1/0] via 10.1.4.250

Rt4\_4\_LAN2#sh ip ro stat

10.0.0.0/8 is variably subnetted, 16 subnets, 4 masks

S 10.1.4.0/26 [1/0] via 10.1.4.229

S 10.1.4.64/26 [1/0] via 10.1.4.229

S 10.1.4.128/27 [1/0] via 10.1.4.249

S 10.1.4.192/27 [1/0] via 10.1.4.241

S 10.1.4.224/30 [1/0] via 10.1.4.229

S 10.1.4.232/30 [1/0] via 10.1.4.249

S 10.1.4.236/30 [1/0] via 10.1.4.241

S 10.1.4.244/30 [1/0] via 10.1.4.241

Rt5\_4\_LAN2#sh ip ro stat

10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks

S 10.1.4.0/26 [1/0] via 10.1.4.245

S 10.1.4.64/26 [1/0] via 10.1.4.245

S 10.1.4.128/27 [1/0] via 10.1.4.237

S 10.1.4.160/27 [1/0] via 10.1.4.242

S 10.1.4.224/30 [1/0] via 10.1.4.245

S 10.1.4.228/30 [1/0] via 10.1.4.242

S 10.1.4.232/30 [1/0] via 10.1.4.237

S 10.1.4.248/30 [1/0] via 10.1.4.237

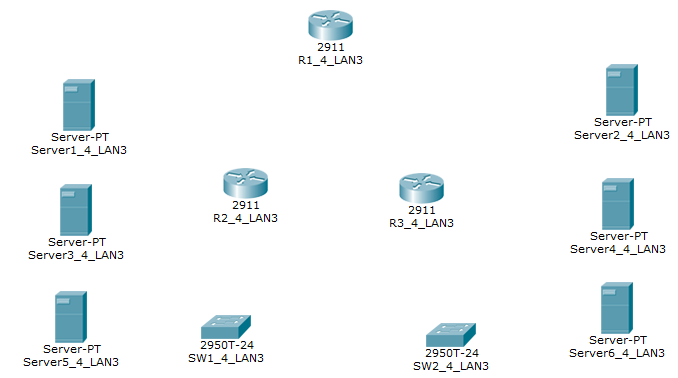
S\* 0.0.0.0/0 [1/0] via 10.1.4.242

Перевірка коректності налаштування мережі була проведена за допомогою інструменту Simple PDU. Всі вузли мережі Lan2 можуть взаємодіяти один з одним, що говорить про вірно налаштованій маршрутизації в цій локальній мережі.

# Проектування мережі LAN3

## Побудова мережі

Створимо схему мережі відповідно до варіанту, розташувавши обладнання та підписавши його (мал. 12).



Малюнок 14 Схема мережі Lan3

## Агрегування каналів

Комутатори SW1 і SW2 з'єднаємо 4 мережевими інтерфейсами, об'єднавши їх у віртуальний канал. Для цього використовуємо порти, які не будуть приймати участь в VLAN – відповідно до завдання. Нижче наведені команди, які потрібно ввести на комутаторах, щоб зібрати чотири фізичні інтерфейси на кожному з них в один логічний канал.

SW1\_4\_LAN3(config)#int range fa 0/7-10

SW1\_4\_LAN3(config-if-range)#sw mode tr

SW1\_4\_LAN3(config-if-range)#channel-group 1 mode active

SW1\_4\_LAN3(config-if-range)#

Creating a port-channel interface Port-channel 1

SW1\_4\_LAN3(config-if-range)#ex

SW1\_4\_LAN3(config)#int port-channel 1

SW1\_4\_LAN3(config-if)#switchport mode trunk

SW2\_4\_LAN3(config)#int range fa 0/21-24

SW2\_4\_LAN3(config-if-range)#sw mode tr

SW2\_4\_LAN3(config-if-range)#channel-group 1 mode active

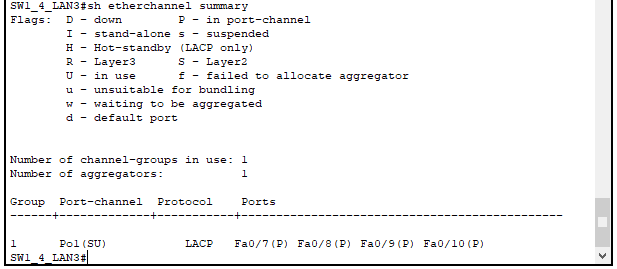
SW2\_4\_LAN3(config-if-range)#

Creating a port-channel interface Port-channel 1

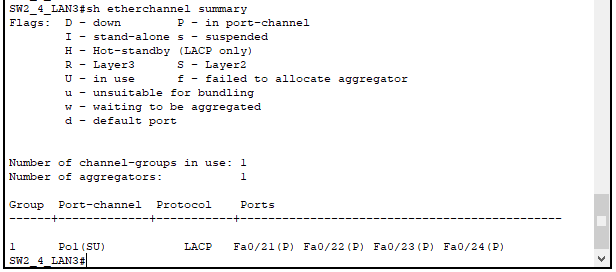
SW2\_4\_LAN3(config)#int port-channel 1

SW2\_4\_LAN3(config-if)#switchport mode trunk

Статус отриманого інтерфейсу можна переглянути простою командою (мал. 15-16):



Малюнок 15 статус інтерфейсу Port-Channel



Малюнок 16 статус інтерфейсу Port-Channel

## Налаштування та комутація VLAN

На кожному комутаторі створимо VLANи, згідно із завданням. У завданні сказано про те, що необхідно створити VLAN1-3, але vlan1 – це VLAN за замовчуванням на всіх мережевих пристроях, і використовувати його мені здається небезпечним, крім того – адміністративному VLAN не може бути призначено ім'я. Тому я створю VLAN з іншими позначеннями – 10, 20 і 30. Нижче наведені команди, які використовувалися для створення VLAN:

SW1\_4\_LAN3(config)#vlan 10

SW1\_4\_LAN3(config-vlan)#name VLAN1

SW1\_4\_LAN3(config-vlan)#vlan 20

SW1\_4\_LAN3(config-vlan)#name VLAN2

SW1\_4\_LAN3(config-vlan)#vlan 30

SW1\_4\_LAN3(config-vlan)#name VLAN3

SW1\_4\_LAN3(config-vlan)#ex

SW1\_4\_LAN3(config)#int range fa 0/17-20

SW1\_4\_LAN3(config-if-range)#sw acc vlan 10

SW1\_4\_LAN3(config-if-range)#int range fa 0/21-23

SW1\_4\_LAN3(config-if-range)#sw acc vlan 20

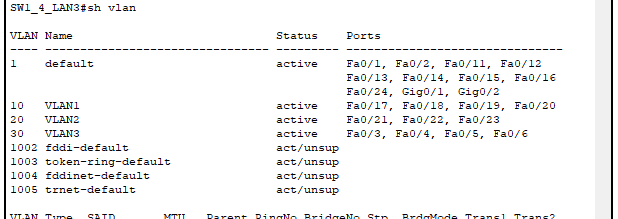
SW1\_4\_LAN3(config-if-range)#int range fa 0/3-6

SW1\_4\_LAN3(config-if-range)#sw acc vlan 30

SW1\_4\_LAN3(config-if-range)#ex

SW1\_4\_LAN3(config)#ex

Статус VLAN і портів в них можна переглянути простою командою (мал. 17-18)



Малюнок 17 статус VLAN

SW2\_4\_LAN3(config)#vlan 10

SW2\_4\_LAN3(config-vlan)#name VLAN1

SW2\_4\_LAN3(config-vlan)#vlan 20

SW2\_4\_LAN3(config-vlan)#name VLAN2

SW2\_4\_LAN3(config-vlan)#vlan 30

SW2\_4\_LAN3(config-vlan)#name VLAN3

SW2\_4\_LAN3(config-vlan)#ex

SW2\_4\_LAN3(config)#int range fa 0/1-5

SW2\_4\_LAN3(config-if-range)#sw acc vlan 10

SW2\_4\_LAN3(config-if-range)#int range fa 0/9-13

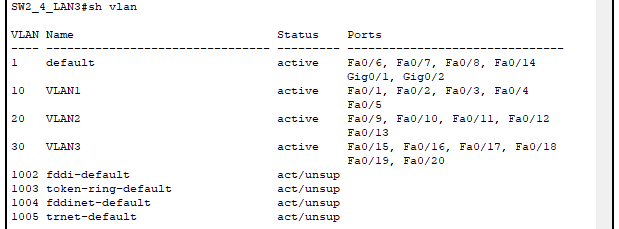
SW2\_4\_LAN3(config-if-range)#sw acc vlan 20

SW2\_4\_LAN3(config-if-range)#int range fa 0/15-20

SW2\_4\_LAN3(config-if-range)#sw acc vlan 30

SW2\_4\_LAN3(config-if-range)#ex

SW2\_4\_LAN3(config)#ex



Малюнок 18 статус VLAN

Також призначимо адреси VLAN1 комутаторів, для цього візьмемо перші дві адреси в діапазоні 204.102.65.0. Невідомо, яка саме маска у цій мережі, але припустимо, що це мережа класу D, з маскою 255.255.255.0. Перші дві адреси будуть 204.102.65.1 і 204.102.65.2.

SW1\_4\_LAN3(config)#int vlan 10

SW1\_4\_LAN3(config-if)#

%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

SW1\_4\_LAN3(config-if)#ip add 204.102.65.1 255.255.255.0

SW2\_4\_LAN3(config)#int vlan 10

SW2\_4\_LAN3(config-if)#

%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

SW2\_4\_LAN3(config-if)#ip add 204.102.65.2 255.255.255.0

Перевірити доступність комутаторів можна командою ping:

SW2\_4\_LAN3#ping 204.102.65.1

Type escape sequence to abort.

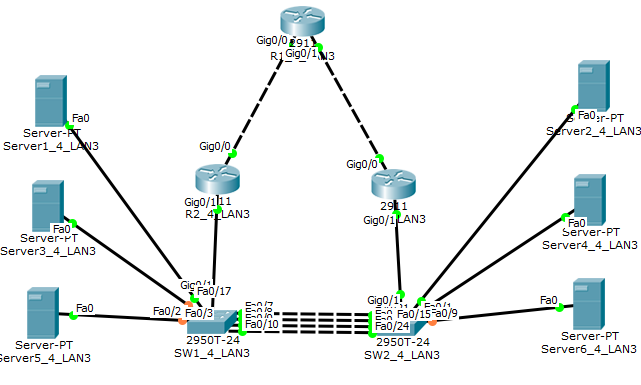
Sending 5, 100-byte ICMP Echos to 204.102.65.1, timeout is 2 seconds:

..!!!

Success rate is 60 percent (3/5), round-trip min/avg/max = 0/2/8 ms

## Підключення серверів

Сервера, як потрібно в завданні, підключимо до портів комутаторів, що знаходяться в відповідних VLAN-ах. Після цього схема мережі матиме такий вигляд (мал. 19):



Малюнок 19 схема мережі LAN3

Таблиця підключення комутаторів така:

|  |  |  |  |
| --- | --- | --- | --- |
| Сервер | VLAN | Комутатор | Порт |
| Server1\_4\_LAN3 | VLAN1 | SW1\_4\_LAN3 | Fa 0/17 |
| Server2\_4\_LAN3 | VLAN1 | SW2\_4\_LAN3 | Fa 0/1 |
| Server3\_4\_LAN3 | VLAN2 | SW1\_4\_LAN3 | Fa 0/21 |
| Server4\_4\_LAN3 | VLAN2 | SW2\_4\_LAN3 | Fa 0/9 |
| Server5\_4\_LAN3 | VLAN3 | SW1\_4\_LAN3 | Fa 0/3 |
| Server6\_4\_LAN3 | VLAN3 | SW2\_4\_LAN3 | Fa 0/15 |

Таблиця 6. Підключення серверів до комутаторів в мережі LAN3

## Налаштування адресації серверів

Серверам необхідно призначити адреси таким чином, щоб вони знаходилися в відповідних мережах, згідно із завданням.

Мережі, зазначені в завданні:

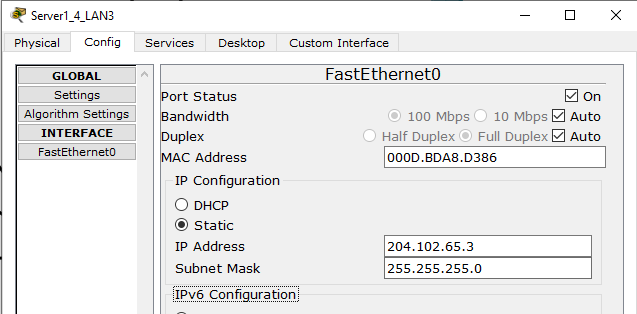
* Net1 – 204.102.65.0
* Net2 – 214.23.87.0
* Net3 – 58.0.0.0

Складемо для цього таблицю адрес:

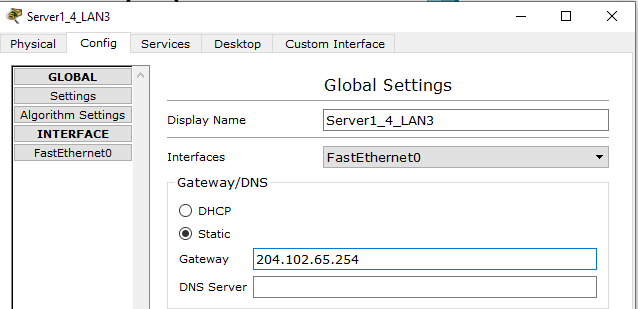
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Сервер | Мережа | Адреса | Маска підмережі | Шлюз |
| Server1\_4\_LAN3 | Net1 | 204.102.65.3 | 255.255.255.0 | 204.102.65.254 |
| Server2\_4\_LAN3 | Net1 | 204.102.65.4 | 255.255.255.0 | 204.102.65.254 |
| Server3\_4\_LAN3 | Net2 | 214.23.87.1 | 255.255.255.0 | 214.23.87.254 |
| Server4\_4\_LAN3 | Net2 | 214.23.87.2 | 255.255.255.0 | 214.23.87.254 |
| Server5\_4\_LAN3 | Net3 | 58.0.0.1 | 255.255.255.0 | 58.0.0.254 |
| Server6\_4\_LAN3 | Net3 | 58.0.0.2 | 255.255.255.0 | 58.0.0.254 |

Таблиця 7. Адреси серверів в мережі LAN3

Призначимо адреси серверів, використовуючи для цього графічний інтерфейс (мал. 20-21):

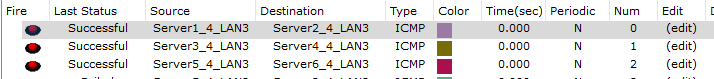


Малюнок 20 призначення адреси серверу



Малюнок 21 призначення шлюзу серверу

Успішність налаштувань адрес, а також роботу VLAN і транкових портів можна перевірити за допомогою інструменту Simple PDU (мал.22)



Малюнок 22 перевірка роботи мережі LAN3

## Налаштування протоколу HSRP на маршрутизаторах

Створимо на маршрутизаторах підінтерфейсів для відповідних мереж:

R2\_4\_LAN3 (config)#int gig0/1.10

R2\_4\_LAN3 (config-subif)#encapsulation dot1Q 10

R2\_4\_LAN3 (config-subif)#ip add 204.102.65.5 255.255.255.0

R2\_4\_LAN3 (config-subif)#int gig0/1.20

R2\_4\_LAN3 (config-subif)#encapsulation dot1Q 20

R2\_4\_LAN3 (config-subif)#ip add 214.23.87.3 255.255.255.0

R2\_4\_LAN3 (config-subif)#int gig0/1.30

R2\_4\_LAN3 (config-subif)#encapsulation dot1Q 30

R2\_4\_LAN3 (config-subif)#ip add 58.0.0.3 255.255.255.0

R3\_4\_LAN3 (config)#int gig 0/1.10

R3\_4\_LAN3 (config-subif)#encapsulation dot1Q 10

R3\_4\_LAN3 (config-subif)#ip add 204.102.65.6 255.255.255.0

R3\_4\_LAN3 (config-subif)#int gig 0/1.20

encapsulation dot1Q 20

R3\_4\_LAN3 (config-subif)#ip add 214.23.87.4 255.255.255.0

R3\_4\_LAN3 (config-subif)#int gig 0/1.30

encapsulation dot1Q 30

R3\_4\_LAN3 (config-subif)#ip add 58.0.0.4 255.255.255.0

Тепер налаштуємо протокол HSRP. Це протокол дозволяє створити віртуальну адресу маршрутизатору, який буде підтримуватися кількома реальними маршрутизаторами. У разі виходу з ладу основного маршрутизатору (він називається active), його роль перехопить вторинний, що знаходиться до того часу в стані passive.

R2\_4\_LAN3 (config)#int gig 0/1.10

R2\_4\_LAN3 (config-subif)#standby 1 ip 204.102.65.254

R2\_4\_LAN3 (config-subif)#standby 1 priority 120

R2\_4\_LAN3 (config-subif)#standby 1 preempt

R2\_4\_LAN3(config)#int gig 0/1.20

R2\_4\_LAN3(config-subif)#standby 2 ip 214.23.87.254

R2\_4\_LAN3(config-subif)#standby 2 priority 120

R2\_4\_LAN3(config-subif)#standby 2 preempt

R2\_4\_LAN3(config)#int gig 0/1.30

R2\_4\_LAN3(config-subif)#standby 3 ip 58.0.0.254

R2\_4\_LAN3(config-subif)#standby 3 priority 120

R2\_4\_LAN3(config-subif)#standby 3 preempt

R3\_4\_LAN3 (config)#int gig 0/1.10

R3\_4\_LAN3 (config-subif)#standby 1 ip 204.102.65.254

R3\_4\_LAN3(config)#int gig 0/1.20

R3\_4\_LAN3(config-subif)#sta

R3\_4\_LAN3(config-subif)#standby 2 ip 214.23.87.254

R3\_4\_LAN3(config-subif)#int gig 0/1.30

R3\_4\_LAN3(config-subif)#standby 3 ip 58.0.0.254

## Налаштування маршрутизації

Оскільки адреси для зв'язку маршрутизаторів 2 і 3 з маршрутизатором 1 в завданні не обумовлені, я призначу їх самостійно з приватного діапазону: нехай це будуть мережі 10.0.0.0/30 і 10.0.0.4/30.

Тоді таблиця адрес маршрутизаторів буде виглядати так:

|  |  |  |  |
| --- | --- | --- | --- |
| Маршрутизатор | Порт | Адреса | З ким з'єднує |
| R1\_4\_LAN3 | Gig0/0 | 10.0.0.2/30 | R2\_4\_LAN3 |
| Gig0/1 | 10.0.0.6/30 | Rt3\_4\_LAN3 |
| R2\_4\_LAN3 | Gig0/0 | 10.0.0.1/30 | R1\_4\_LAN3 |
| Gig0/1.10 | 204.102.65.5/24 | Net1 |
| Gig0/1.20 | 214.23.87.3/24 | Net2 |
| Gig0/1.30 | 58.0.0.3/24 | Net3 |
| Rt3\_4\_LAN3 | Gig0/0 | 10.0.0.5/30 | R1\_4\_LAN3 |
| Gig0/1.10 | 204.102.65.6/24 | Net1 |
| Gig0/1.20 | 214.23.87.4/24 | Net2 |
| Gig0/1.30 | 58.0.0.4/24 | Net3 |

Таблиця 8. Адреси інтерфейсів маршрутизаторів мережі LAN3

Призначимо адреси відповідним інтерфейсам маршрутизаторів. Також, вкажемо на маршрутизаторах 2 і 3 перший маршрутизатор в якості маршруту за замовчуванням.

R2\_4\_LAN3(config)#interface GigabitEthernet0/0

R2\_4\_LAN3(config-if)#ip address 10.0.0.1 255.255.255.252

R2\_4\_LAN3(config-if)#ex

R2\_4\_LAN3(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2

R3\_4\_LAN3(config)#interface GigabitEthernet0/0

R3\_4\_LAN3(config-if)#ip address 10.0.0.5 255.255.255.252

R3\_4\_LAN3(config-if)#exit

R3\_4\_LAN3(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.6

Необхідно анонсувати мережі серверів на маршрутизаторі R1. Щоб використовувати для цього обидва нижчих маршрутизатори, використовуємо статичні маршрути із зазначенням ваги. Основний маршрут буде вказувати на маршрутизатор 2, вторинний – на маршрутизатор 3. Команди для цього:

ip route 204.102.65.0 255.255.255.0 10.0.0.1

ip route 204.102.65.0 255.255.255.0 10.0.0.5 10

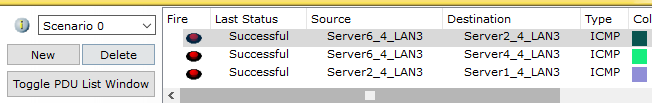
ip route 214.23.87.0 255.255.255.0 10.0.0.1

ip route 214.23.87.0 255.255.255.0 10.0.0.5 10

ip route 58.0.0.0 255.255.255.0 10.0.0.1

ip route 58.0.0.0 255.255.255.0 10.0.0.5 10

Мережа Lan3 налаштована, перевірити працездатність мережі можна за допомогою команди Ping або інструменту Simple PDU (Мал. 23).



Малюнок 23 перевірка працездатності мережі LAN3

# Загальні налаштування активного обладнання

## Налаштування обладнання

Для всіх маршрутизаторів потрібно налаштувати паролі на консольне з'єднання та на привілейований режим. Найпростіше це зробити, заздалегідь підготувавши необхідні команди у вигляді тексту, та вставляючи його в CLI-інтерфейс маршрутизатору:

en

conf t

line con 0

password cisco

login

exit

line vty 0 15

password cisco

login

exit

enable secret cisco

service password-encryption

no ip domain lookup

exit

copy run start

Цей набір команд активує паролі на доступ до пристрою, на привілейований режим, встановлює режим шифрування паролів (щоб вони не зберігалися у відкритому вигляді до конфігураційного файлу), а також забороняє звернення до серверу DNS – інакше невірно введена команда може бути розцінена як запит DNS, і пристрій буде досить довго намагатися його обробити, що викликає затримки в роботі.

Також, потрібно включити на шлюзових маршрутизаторах доступ по SSH. Для цього виконаємо такі команди:

R1\_4\_LAN3(config)#ip domain name MEGANET

R1\_4\_LAN3(config)#crypto key generate rsa

The name for the keys will be: R1\_4\_LAN3.MEGANET

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1\_4\_LAN3(config)#ip ssh version 2

R1\_4\_LAN3(config)#line vty 0 15

R1\_4\_LAN3(config-line)#transport input ssh

Цим ми встановлюємо ім'я домену, потім генеруємо ключ для шифрування довжиною 1024 біта, активуємо протокол SSH і встановлюємо для ліній віртуального терміналу доступ по протоколу SSH.

Аналогічно налаштуємо SSH на інших комутаторах

# Об'єднання локальних мереж

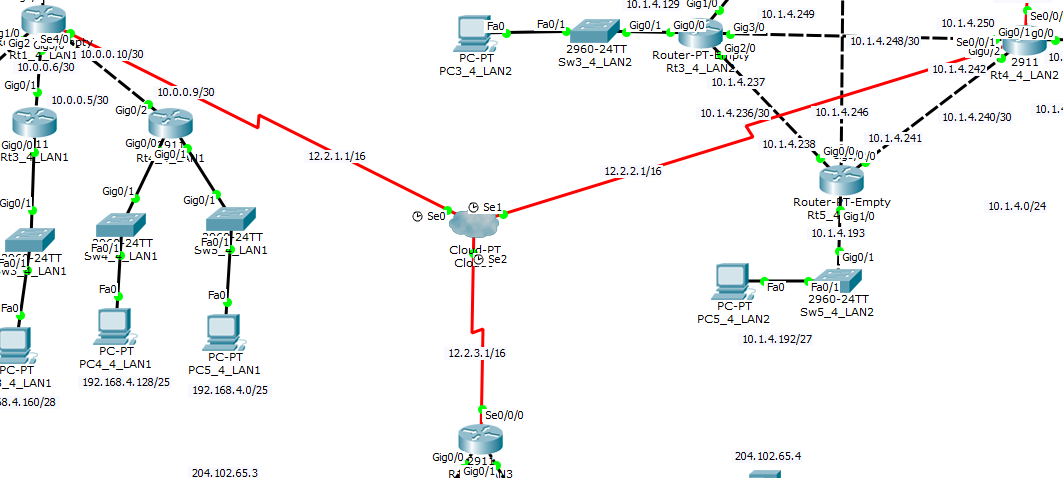
## Створення та налагодження FrameRelay

Згідно з завданням, створені локальні мережі необхідно об'єднати, використовуючи для цього технологію FrameRelay. Для мережі FR виділений діапазон адрес 12.2.0.0/16. Необхідно призначити адреси граничним маршрутизаторам. Додамо в граничні маршрутизатори адаптери для послідовного підключення, та призначимо їм адреси згідно з таблицею:

|  |  |  |  |
| --- | --- | --- | --- |
| Маршрутизатор | Порт | Адреса | З ким з'єднує |
| Rt1\_4\_LAN1 | Se4/0 | 12.2.1.1/16 | Cloud-PT |
| Rt4\_4\_LAN2 | Se0/0/1 | 12.2.2.1/16 |
| Rt1\_4\_LAN3 | Se0/0/0 | 12.2.3.1/16 |

Таблиця 11. Адреси маршрутизаторів в мережі FR

Розташуємо на робочому полі зону WAN, і підключимо до неї граничні маршрутизатори локальних мереж, використовуючи зазначені вище інтерфейси (мал. 24).



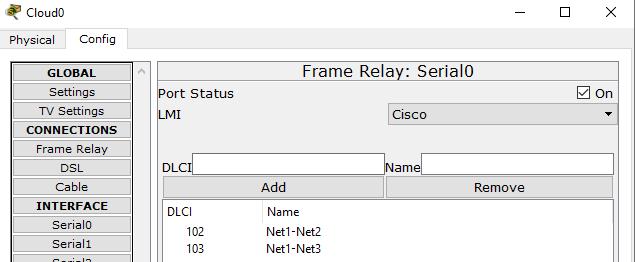
Малюнок 24 створення WAN

Для роботи FrameRelay необхідно створити записи DLCI в зоні WAN, які будуть визначати напрямки передачі даних. Запишемо їх у вигляді таблиці:

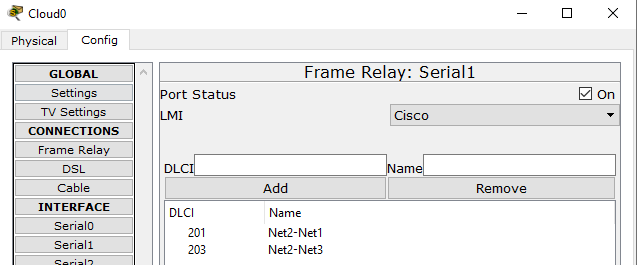
|  |  |
| --- | --- |
| Напрямок | DLCI |
| Net1-Net2 | 102 |
| Net2-Net1 | 201 |
| Net1-Net3 | 103 |
| Net3-Net1 | 301 |
| Net2-Net3 | 203 |
| Net3-Net2 | 302 |

Таблиця 12. DLCI в мережі FR

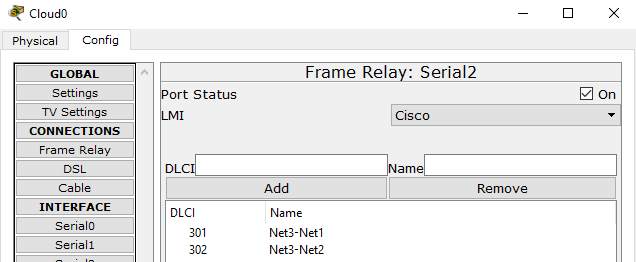
Зазначимо ці DLCI в самій зоні, використовуючи графічний інтерфейс (мал. 25-28):



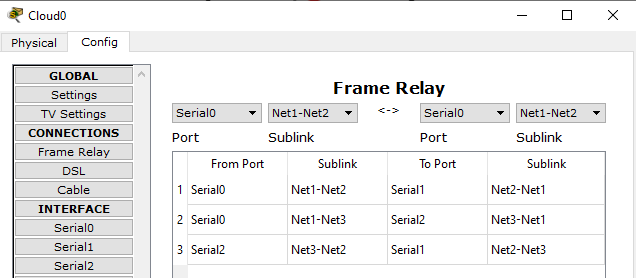
Малюнок 25 вказівка DLCI



Малюнок 26 вказівка DLCI



Малюнок 27 вказівка DLCI



Малюнок 28 налаштування Frame Relay

Також потрібно налаштувати інтерфейси на граничних маршрутизаторах. Для цього введемо такі команди:

Rt1\_4\_LAN1(config)#int se4/0

Rt1\_4\_LAN1(config-if)#encapsulation frame-relay

Rt1\_4\_LAN1(config-if)#ip add 12.2.1.1 255.255.0.0

Rt1\_4\_LAN1(config-if)#bandwidth 64

Rt1\_4\_LAN1(config-if)#frame-relay map ip 12.2.2.1 102 broadcast

Rt1\_4\_LAN1(config-if)#frame-relay map ip 12.2.3.1 103 broadcast

Rt4\_4\_LAN2(config)#int se 0/0/1

Rt4\_4\_LAN2(config-if)#enc frame-relay

Rt4\_4\_LAN2(config-if)#ip add 12.2.2.1 255.255.0.0

Rt4\_4\_LAN2(config-if)#band 64

Rt4\_4\_LAN2(config-if)#frame-relay map ip 12.2.1.1 201 broadcast

Rt4\_4\_LAN2(config-if)#frame-relay map ip 12.2.3.1 203 broadcast

R1\_4\_LAN3(config)#int se 0/0/0

R1\_4\_LAN3(config-if)#encapsulation frame-relay

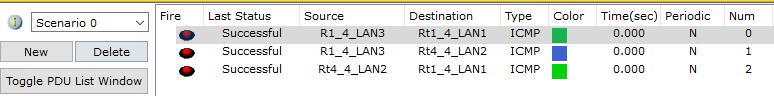
R1\_4\_LAN3(config-if)#ip add 12.2.3.1 255.255.0.0

R1\_4\_LAN3(config-if)#band 64

R1\_4\_LAN3(config-if)#frame-relay map ip 12.2.1.1 301 broadcast

R1\_4\_LAN3(config-if)#frame-relay map ip 12.2.2.1 302 broadcast

Перевірити доступність маршрутизаторів всередині мережі FR можна за допомогою інструменту SimplePDU (мал. 29):



Малюнок 29 перевірка доступності маршрутизаторів FR

## Налаштування трансляції мережевих адрес NAT

Технологія NAT дозволяє виробляти трансляцію мережевих адрес, замінюючи їх за певними правилами при проходженні пакету через маршрутизатор. Це переслідує кілька цілей: по-перше, дозволяє декільком вузлам підключатися до інших мереж, використовуючи для цього одну адресу, по-друге – підвищує безпеку, оскільки в зовнішніх мережах не буде відомо про стан мережі, що працює через NAT.

Налаштуємо NAT в мережі LAN1. Потрібно, щоб сервер використовував статичний NAT, тобто завжди «представлявся» однією і тою-самою зовнішньою адресою. Комп'ютери мережі повинні використовувати NAT з перекриттям – тобто використовувати одну адресу. Для налаштування введемо такі команди:

Rt1\_4\_LAN1(config)#int se 4/0

Rt1\_4\_LAN1(config-if)#ip nat outside

Rt1\_4\_LAN1(config-if)#ex

Rt1\_4\_LAN1(config)#int gig 0/0

Rt1\_4\_LAN1(config-if)#ip nat inside

Rt1\_4\_LAN1(config-if)#int gig 1/0

Rt1\_4\_LAN1(config-if)#ip nat inside

Rt1\_4\_LAN1(config-if)#int gig 2/0

Rt1\_4\_LAN1(config-if)#ip nat inside

Rt1\_4\_LAN1(config-if)#int gig 3/0

Rt1\_4\_LAN1(config-if)#ip nat inside

Rt1\_4\_LAN1(config)#ip nat inside source static 10.0.0.14 12.2.1.2

Rt1\_4\_LAN1(config)#access-list 1 permit 192.168.4.0 0.0.0.255

Rt1\_4\_LAN1(config)#access-list 1 deny any

Rt1\_4\_LAN1(config)#ip nat inside source list 1 int se4/0 overload

У мережі LAN2 повинен використовуватися динамічний NAT – тобто адреси для зіставлення будуть братися з певного пулу. Налаштуємо його такими командами:

Rt4\_4\_LAN2(config)#int se0/0/0

Rt4\_4\_LAN2(config-if)#ip nat inside

Rt4\_4\_LAN2(config-if)#int range gig 0/0-2

Rt4\_4\_LAN2(config-if-range)#ip nat inside

Rt4\_4\_LAN2(config-if-range)#int se 0/0/1

Rt4\_4\_LAN2(config-if)#ip nat outside

Rt4\_4\_LAN2(config-if)#ip nat pool lan2 12.2.2.2 12.2.2.6 netmask 255.255.255.0

Rt4\_4\_LAN2(config)#access-list 1 permit 10.1.4.0 0.0.0.255

Rt4\_4\_LAN2(config)#access-list 1 deny any

Rt4\_4\_LAN2(config)#ip nat inside source list 1 pool lan2

## Маршрутизація WAN

На граничних маршрутизаторах необхідно вказати маршрути до мереж, до яких потрібно забезпечити доступ. Потрібно розуміти, що через використання NAT комп'ютери мереж LAN1 і LAN2 не зможуть взаємодіяти один з одним. Тому необхідно провести налаштування для доступу до мереж LAN3, і для маршрутизатору мережі LAN3 – до мереж LAN1 і LAN2.

Налаштування граничного комутатору LAN1:

Rt1\_4\_LAN1#sh ip ro stat

10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks

S 10.1.4.0/24 [1/0] via 12.2.2.1

58.0.0.0/24 is subnetted, 1 subnets

S 58.0.0.0 [1/0] via 12.2.3.1

192.168.4.0/24 is variably subnetted, 4 subnets, 3 masks

S 192.168.4.0/25 [1/0] via 10.0.0.9

S 192.168.4.128/27 [1/0] via 10.0.0.9

S 192.168.4.160/28 [1/0] via 10.0.0.5

S 192.168.4.176/28 [1/0] via 10.0.0.1

S 204.102.65.0/24 [1/0] via 12.2.3.1

S 214.23.87.0/24 [1/0] via 12.2.3.1

Налаштування граничного комутатору LAN2:

Rt4\_4\_LAN2#sh ip ro stat

10.0.0.0/8 is variably subnetted, 16 subnets, 4 masks

S 10.1.4.0/26 [1/0] via 10.1.4.229

S 10.1.4.64/26 [1/0] via 10.1.4.229

S 10.1.4.128/27 [1/0] via 10.1.4.249

S 10.1.4.192/27 [1/0] via 10.1.4.241

S 10.1.4.224/30 [1/0] via 10.1.4.229

S 10.1.4.232/30 [1/0] via 10.1.4.249

S 10.1.4.236/30 [1/0] via 10.1.4.241

S 10.1.4.244/30 [1/0] via 10.1.4.241

12.0.0.0/8 is variably subnetted, 3 subnets, 2 masks

S 12.2.1.2/32 [1/0] via 12.2.1.1

58.0.0.0/24 is subnetted, 1 subnets

S 58.0.0.0 [1/0] via 12.2.3.1

S 192.168.4.0/24 [1/0] via 12.2.1.1

S 204.102.65.0/24 [1/0] via 12.2.3.1

S 214.23.87.0/24 [1/0] via 12.2.3.1

Налаштування граничного комутатору LAN3:

R1\_4\_LAN3#sh ip ro stat

10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks

S 10.1.4.0/24 [1/0] via 12.2.2.1

12.0.0.0/8 is variably subnetted, 8 subnets, 2 masks

S 12.2.1.2/32 [1/0] via 12.2.1.1

S 12.2.2.2/32 [1/0] via 12.2.2.1

S 12.2.2.3/32 [1/0] via 12.2.2.1

S 12.2.2.4/32 [1/0] via 12.2.2.1

S 12.2.2.5/32 [1/0] via 12.2.2.1

S 12.2.2.6/32 [1/0] via 12.2.2.1

58.0.0.0/24 is subnetted, 1 subnets

S 58.0.0.0 [1/0] via 10.0.0.1

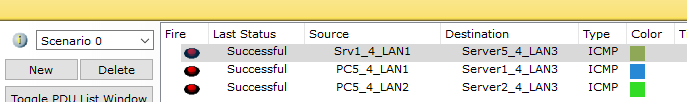
S 192.168.4.0/24 [1/0] via 12.2.1.1

S 204.102.65.0/24 [1/0] via 10.0.0.1

S 214.23.87.0/24 [1/0] via 10.0.0.1

# Перевірка зв'язності мережі, перевірка NAT

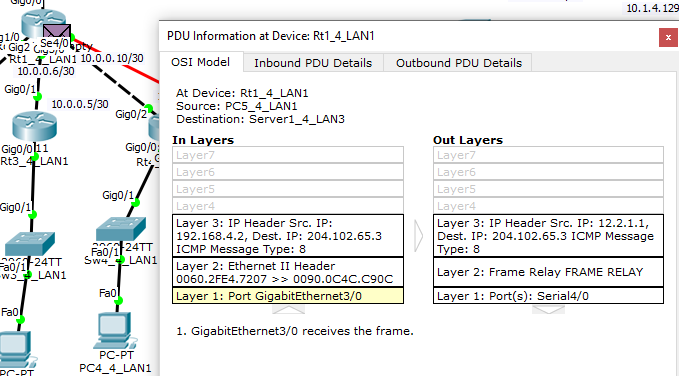
Щоб перевірити функціонування мережі, використовуємо інструмент SimplePDU. Перевіримо доступність сервером LAN3 з мережі LAN1 і мережі LAN2 (мал. 30):



Малюнок 30 перевірка міжмережової доступності

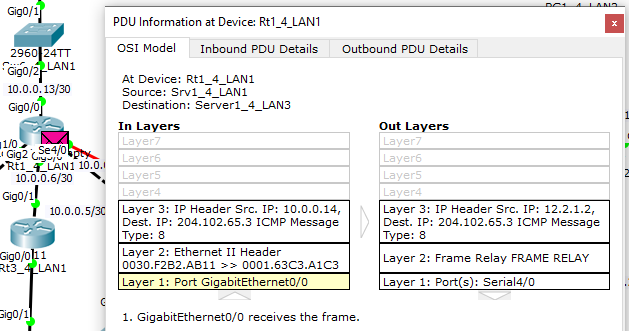
Як видно, різні сервера мережі LAN3 доступні як з сервера мережі LAN1, так і з комп'ютерів обох мереж.

Перевіримо перетворення адрес NAT. Для цього можна використовувати режим симуляції CiscoPacketTracer, що дозволяє розглянути зміни в пакеті на кожному вузлі.



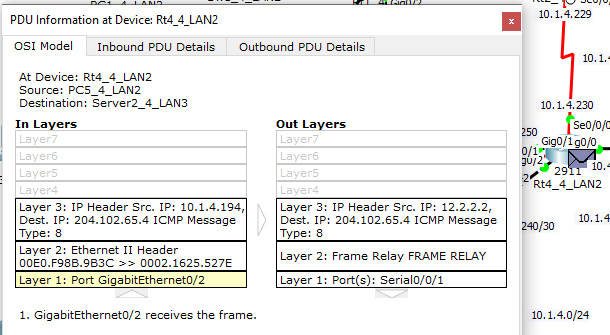
Малюнок 31 робота NAT з перекриттям

Видно, що пакет ICMP, відправлений з вузла PC5 мережі LAN1, з початковою адресою 192.168.4.2, при проходженні через маршрутизатор змінив адресу на 12.2.1.1. Це робота NAT, який перекриває.



Малюнок 32 Робота статичного NAT

Аналогічно, видно як пакет з сервера змінив адресу відправника з 10.0.0.14 на 12.2.1.2 – це дія статичної NAT.



Малюнок 33 робота динамічного NAT

У другій мережі також працює NAT – адреса відправника 10.1.4.194 була замінена на першу адресу з пулу, 12.2.2.2.

# ВИСНОВКИ

У даній роботі мною була розроблена, згідно сформованому технічному завданню, складна корпоративна мережа, що складається з трьох окремих локальних мереж, що взаємодіють через WAN на основі технології Frame Relay.

У ході роботи мною були проведені налаштування, спрямовані на підвищення надійності та безпеки проектованої мережі. Адресний простір, виділений для вирішення завдання, було використано оптимально. Всі проведені випробування показали працездатність мережі та коректність вироблених налаштувань.

# ДЖЕРЕЛА:

1. В.Г.Оліфер, Н.А.Оліфер Комп'ютерні мережі. Принципи, технології, протоколи. Підручник для вузів Серія: Підручник для вузів. Видавництво: Пітер, 2007 р. 960 стор.
2. Азаров О.Д., Захарченко С.М., Кадук А.В., Орлова М.М., Тарасенко В.П. Комп'ютерні мережі: навчальний посібник / [Азаров О.Д., Захарченко С.М., Кадук А.В. та ін.] – Вінниця: ВНТУ, 2013. — 371 с.
3. Бєляєв А.В. Методи та засоби захисту інформації [Електронний ресурс] / А.В.Беляев. – 2000. – Режим доступу до ресурсу: http://www.citforum.ru/internet/infsecure/its2000\_01.shtml.
4. Платонов, В.В. Програмно-апаратні засоби забезпечення інформаційної безпеки обчислювальних мереж [Текст] / В.В.Платонов. – Академія, 2006. – 240 с.
5. А.Г.Мікітішін, М.М.Таможеннік, П.Д.Стухляк, В.В.Пасечнік Комп'ютерні мережі [навчальний посібник] – Львів, «Магнолія 2006», 2013. – 256 с.