**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)»**

(назва дисципліни)

на тему: **Розробка комп’ютерної мережі та конфігурування**

**мережевого обладнання**

Студента(ки) 3 курсу 303 групи

спеціальності Кібербезпека»

Шевченко В.С

(прізвище та ініціали)

Керівник

к.т.н, доцент

(посада, вчене звання, науковий ступінь,

Гордєєва Д.В.

прізвище та ініціали)

Національна шкала

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кількість балів: \_\_\_\_

Оцінка: ECTS \_\_\_\_

Члени комісії

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (прізвище та ініціали)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (прізвище та ініціали)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (прізвище та ініціали)

Київ - 2020 рік

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**

**ІНСТИТУТ БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ ТА СОЦІАЛЬНИХ НАУК**

Спецiальність: «Кібербезпека»

Курс 3 Група 303 - Кб Семестр 5

**ЗАВДАННЯ**

**на курсову роботу студента/студентки**

Шевченко Вероніки Сергіївни

(прiзвище, iм`я, по батьковi)

**1. Тема курсової роботи**: Розробка комп’ютерної мережі та конфігурування мережевого обладнання

**2. Термiн здачi студентом закiнченої роботи \_\_\_\_\_\_**

**3. Постановка задачі:**

1. Розробити комп’ютерну мережу

2. Розрахувати адресний простір для мереж LAN1-LAN3

3. Створити конфігураційні файли для всіх мережевих пристроїв.

4. Виконати моделювання мережі засобами GNS3.

Вихідні дані:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| LAN №1 | підмережі | | | ІР-адреса | | Кількість хостів | | | | | | | | | |
| Net1 | | | Net2 | | Net3 | | Net4 | | Net5 |
| 192.168.13.0 | | 12 | | | 10 | | 58 | | 25 | | 5 |
| ст. ACL | | | відпр. | | отр. | | | відпр. | | отр. | | відпр. | | отр. |
| Net1 | | Net6 | | | Net5 | | Net2 | | Net3 | | Net1 |
| розш. ACL | | | відпр. | | отр. | | | № прот. | | отр. | | відпр. | | отр. |
| Net4 | | Net1 | | | 3,12,14 | | Net2 | | Net3 | | 5,9,12 |
| LAN №2 | № сх. | | ІР-адреса | | | | Serial HDLC | | | Serial PPP | | Шлюз | | Тип маршрутизації | |
| 10 | | 10 .3.10.0/24 | | | | Rt4-Rt5 | | | Rt4-Rt2 | | Rt1 | | OSPF | |
| LAN №3 | Net1 | Net2 | | | Net3 | | | Switch1 | | | | Switch3 | | | |
| Vlan 2 | | Vlan 3 | | Vlan 2 | | | Vlan 3 |
| 7.0.0.0 | 4.0.0.0 | | | 134.79.0.0 | | | 17-20 | | 21-23 | | 12-16 | | | 3-7 |

6. Дата видачі завдання “ 16 вересня ” 2020 р

**ТЕХНІЧНЕ ЗАВДАННЯ**

На розробку і 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 із дисципліни «Комп’ютерні системи та мережі (Рівень D - Безпека комп`ютерних систем)»;
4. Джерела розробки — індивідуальне завдання на курсовий проект із дисципліни, технічні рекомендації щодо проектування локальних та розподілених мереж та 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 192.168.13.0
      2. Складається з п’яти сегментів, кількість робочих станцій в кожному з яких становить: 15,7,11,48,50.
      3. Розподіл адресного простору має бути оптимальним;
      4. Для об’єднання окремих сегментів використовуються 4 маршрутизатори;
      5. З’єднання між маршрутизаторами здійснюються за допомогою скрученої пари;
      6. Для обмеження проходження трафіку з одного сегменту в інший мають бути застосовані стандартні і розширені ACL. Стандартні списки мають заборонити проходження трафіку з мереж NET2 NET1 та NET5 відповідно до мереж NET3 NET5 та NET3. Розширені ACL мають заборонити проходження трафіку протоколів NETBIOS, PING та POP3 з NET5 до NET4 та HTTPS, POP3 та ICMP з NET3 до NET6. ACL необхідно розмістити в найбільш вдалому місці.
      7. У середині 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 налаштовано сервіс трансляції адрес NAT.
   3. Вимоги для проектування LAN2
      1. Адреса мережі 10.4.13.0/24
      2. Складається з 5 сегментів, в яких розташовані ПК користувачів.
      3. Розподілити адресний простір таким чином: в мережах, що з’єднують маршрутизатори, використовувати префікс 30 (маска 255.255.255.252), весь вільний простір, що залишається, рівномірно поділити між мережами, в яких розташовані Switch1- Switch5.
      4. Під’єднання мережі LAN2 до мережі WAN виконується через маршрутизатор Rt1.
      5. В середині мережі використовується динамічна маршрутизація на основі протоколу RIP.
      6. На маршрутизаторі Rt1 налаштовано 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, кожний з яких містить по два сервери.
      3. На комутаторах Sw1 Sw3 до Vlan 2 належать порти FastEtherne17-FastEthernet20 та FastEthernet12-FastEthernet16 відповідно, до Vlan 3 FastEthernet21-FastEthernet123 та FastEthernet3-FastEthernet7 відповідно.
      4. . З’єднання між комутаторами здійснюються за допомогою скрученої пари і технології Gigabit Ethernet.
      5. В віртуальних мережах VLAN1, VLAN2 та VLAN3 використовуються адреси 7.0.0.0 4.0.0.0 та 134.79.0.0 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, що під’єднані до Frame Relay мережі, належать до мережі з адресою 18.0.0.0/8
      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.
      3. Апаратні вимоги - використання обладнання фірми Cisco
      4. Текстова документація розробленої мережі повинна відповідати діючим стандартам України.
      5. Стадії та етапи розробки мережі включать розробку та відлагодження окремих LAN та об’єднання LAN1-4 за допомогою WAN мережі.

Розробила студентка групи 303-Кб Шевченко Вероніка Сергіївна

**Зміст**

[АНОТАЦІЯ 8](#_Toc59000053)

[ВСТУП 9](#_Toc59000054)

[РОЗДІЛ 1 Теоретичні аспекти видів та методів сегментації компьютерної мережі 11](#_Toc59000055)

[1.1. Локальні мережі (LAN - Local Area Network) 11](#_Toc59000056)

[1.2. Глобальні мережі (WAN - Wide Area Network) 12](#_Toc59000057)

[1.3. Розрахунок адресного простору 13](#_Toc59000058)

[РОЗДІЛ 2 Налаштування компьютерної мережі 17](#_Toc59000059)

[2.1. Вибір та налаштування способу маршрутизації 17](#_Toc59000061)

[2.2. Конфігурування базових функцій маршрутизаторів 18](#_Toc59000062)

[2.3. Проектування віртуальних мереж 21](#_Toc59000063)

[2.3.1. Створення VLAN 21](#_Toc59000064)

[2.3.2. Призначення портів мережі VLAN 23](#_Toc59000065)

[2.3.3. Перевірка інформації стосовно налаштування 25](#_Toc59000066)

[2.4. Конфігурування базових функцій комутаторів LAN 27](#_Toc59000067)

[2.5. Конфігурування додаткових функцій маршрутизаторів 30](#_Toc59000068)

[2.5.1. Конфігурування протоколу DHCP 30](#_Toc59000069)

[2.5.2. Налаштування NAT 33](#_Toc59000070)

[2.6. Налаштування захисту та конфігурування функцій безпеки 36](#_Toc59000071)

[2.6.1. Створення списків ACL 36](#_Toc59000072)

[2.6.2. Налаштування паролів 40](#_Toc59000073)

[2.7. Налаштування віддаленого доступу до активного обладнання 41](#_Toc59000074)

[РОЗДІЛ 3 Моделювання та тестування роботи розробленої мережі 44](#_Toc59000075)

[3.1. Моделювання мережі LAN 1 44](#_Toc59000077)

[3.2. Моделювання мережі LAN 2 49](#_Toc59000078)

[3.3. Проектування мережі датацентру LAN3 51](#_Toc59000079)

[3.4. Загальні налаштування активного обладнання та об’єднання локальних мереж 53](#_Toc59000080)

[3.5. Тестування 55](#_Toc59000081)

[3.5.1. Відправка пакетів у LAN1 55](#_Toc59000082)

[3.5.2. Відправка пакетів у LAN2 55](#_Toc59000083)

[3.5.3. Відправка пакетів у LAN3 56](#_Toc59000084)

[3.5.4. Відправка пакетів між мережами 56](#_Toc59000085)

[ВИСНОВКИ 57](#_Toc59000086)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 58](#_Toc59000087)

[ДОДАТОК А конфігураця шлюзового маршрутизатора мережі LAN1 60](#_Toc59000088)

[ДОДАТОК Б Конфігурація шлюзового маршрутищатора мережі LAN2 64](#_Toc59000089)

[ДОДАТОК В Конфігурація шлюзового маршрутизатора мережі LAN3 67](#_Toc59000090)

[ДОДАТОК Г Повна топологія побудованої мережі 70](#_Toc59000091)

# АНОТАЦІЯ

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

Основна частина курсової роботи складається з трьох частин: Теоретичні аспекти мереж, моделювання і розробка мереж, тестування

Для досягнення поставленої задачі була розроблена модель мережі у програмі Cisco Packet Tracer, усі елементи мережі були налаштовані за вимогами, вказаними у технічному завданні, а модель протестована.

Курсовий проект містить:

* Сторінок - 71;
* Таблиць - 2;
* Рисунків - 49;
* Джерел використаної літератури - 13.

# ВСТУП

З появою персональних комп'ютерів питання обміну даними взяли глобальний характер. Завдяки спеціальним програмних і апаратних засобів стало можливим організувати взаємодію між людьми, відокремленими один від одного на відстань у десятки тисяч кілометрів.

Створення комп'ютерних мереж викликане потребою спільного використання інформації на віддалених один від одного комп'ютерах. Мережі надають ПК можливість не тільки обміну інформацією, але також спільного використання обладнання одночасної роботи з документами.

Комп'ютери вже не так давно увійшли в сучасний світ, в усі сфери людської діяльності, тим самим, створюючи необхідність у забезпеченні різним програмним забезпеченням. Об'єднання комп'ютерів у мережі дозволило значно підвищити продуктивність праці. Комп'ютери використовуються як для виробничих (чи офісних) потреби, так і для навчання в навчальних закладах.

В даний час комп'ютерні мережі отримали дуже широке поширення.

Якщо в одній будівлі або комплексі будівель є кілька комп'ютерів, користувачі яких повинні спільно вирішувати якісь завдання, обмінюватися даними чи можуть використовувати загальні дані, то ці комп'ютери доцільно об'єднати в комп'ютерну мережу.

Комп'ютерна мережа - це група з декількох комп'ютерів, з'єднаних між собою за допомогою кабелів (іноді також телефонних ліній або радіоканалів), через які комп'ютери можуть обмінюватися інформацією. Використання комп'ютерних мереж дозволяє забезпечити:

* Колективну обробку даних користувачами підключених до мережі комп'ютерів і обмін даними між ними;
* Спільне використання програм, а також принтерів, модемів та інших пристроїв.
* Тому практично всі фірми, що мають більше одного комп'ютера, об'єднують свої комп'ютери в комп'ютерні мережі.
* Навичками організації ефективної комунікативної діяльності в локальних і глобальних комп'ютерних мережах.
* Методами і засобами пошуку та отримання інформації з використанням сучасних технологій в локальних і глобальних комп'ютерних мережах.
* Навичками роботи з інформацією в глобальних комп'ютерних мережах і корпоративних інформаційних системах.

# РОЗДІЛ 1 Теоретичні аспекти видів та методів сегментації компьютерної мережі

## Локальні мережі (LAN - Local Area Network)

До локальних мереж зазвичай відносять мережі, комп'ютери яких зосереджені на відносно невеликих територіях (менше 2000 м). Прикладом локальної мережі є мережа малого підприємства, розташованого в одному або декількох будівлях. Невеликий розмір локальних мереж дозволяє використовувати для їх побудови досить дорогі і високоякісні технології, що забезпечує високу швидкість обміну інформацією між комп'ютерами[1].

Крім того, в локальних мережах, як правило, використовуються прості способи взаємодії окремих комп'ютерів мережі. Локальна обчислювальна мережа будується на базі середовища передачі даних, що надається структурованої кабельної системою (СКС) будівлі. Для надання користувачу мережевих сервісів до кабельної системи підключається активне мережеве обладнання (комутатори, маршрутизатори і т.д.).

Залежно від технології передачі даних розрізняють:

* локальні мережі з маршрутизацією даних;
* локальні мережі з селекцією даних.

Залежно від використовуваних фізичних засобів з'єднання локальні мережі підрозділяються на *кабельні* та *бездротові*.

У невеликих локальних мережах кожен комп'ютер має певним ступенем самостійності, тобто працює на ньому користувач має право вирішувати, які інформаційні ресурси, розташовані на цьому комп'ютері, він хоче зробити загальнодоступними.

Класифікація комп'ютерних мереж однорангових мережами. Якщо локальна мережа містить більше 10 комп'ютерів, то для збільшення її пропускної спроможності і надійності, тобто для більшої ефективності роботи в цій мережі, а також для забезпечення безпеки, в мережі виділяють спеціальні комп'ютери, на яких зберігаються найбільш затребувані користувачами програмні додатки і файли. Такі комп'ютери називаються серверами. У локальній мережі для зв'язку комп'ютерів зазвичай використовують спеціальні кабелі або спеціальні засоби бездротового зв'язку (останнім часом для цієї мети найчастіше використовується технологія Wi-Fi).

## Глобальні мережі (WAN - Wide Area Network)

До глобальних відносять мережі, призначені для об'єднання окремих комп'ютерів і локальних мереж, розташованих на значній відстані (сотні і тисячі кілометрів) один від одного. Оскільки організація спеціалізованих високоякісних каналів зв'язку великої протяжності є досить дорогою, то в глобальних мережах нерідко використовуються вже існуючі і спочатку не призначені для побудови комп'ютерних мереж лінії (наприклад, телефонні або телеграфні). У зв'язку з цим швидкість передачі даних в таких мережах істотно нижче, ніж в локальних[1].

Це телекомунікаційні структури, що об'єднують локальні комп'ютерні мережі, які мають загальний протокол зв'язку, методи підключення і протоколи обміну даними. Кожна з глобальних мереж (INTERNET, BITNET, DECNET і ін.) організовувалася для певних цілей, а надалі розширювалася завдяки підключенню локальних мереж, що використовують її послуги і ресурси.

Найбільшою глобальною інформаційною мережею є Internet. Internet- глобальна всесвітня мережа інформаційного обміну, яка об'єднує кілька мільйонів людей із більш ніж 100 країн світу за допомогою сучасних і зручних засобів зв'язку. Своє існування Internet розпочала з 1969 року.

Архітектура мережі Internet розроблена на основі концепції взаємо поєднуваного або між мережевого поєднання різнорідних мереж, побудованих на базі різних фізичних систем зв'язку і комунікаційних технологій.

Таким чином, Internet- це сукупність технічних засобів, стандартів і домовленостей, яка дає змогу підтримувати зв'язок між різними комп'ютерними мережами у світі.

Основою функціонування Internet є базовий протокол TCP/IP (TransmissionControlProtocol/InternetProtocol). Він становить сукупність протоколів – систем стандартів і правил зв'язку та передавання інформації у глобальній мережі.

*Протокол*- це домовленості про сигнали, якими обмінюються комп'ютери під час встановлення зв'язку між собою і приймання чи передавання інформації.

*Сервіс-провайдери* – це установи, які надають комерційні послуги з підключення до Internet (Internet service provider, ISP) індивідуальним та колективним користувачам. В організаціях сервіс-провайдерах встановлені сервери Internet – це комп'ютер або програма, що надає послуги іншим комп'ютерам чи програмам.

*Клієнт* – це комп'ютер чи програма, що використовує ресурси серверу Internet. Як правило, на комп'ютері користувача Internet одночасно працюють кілька програм-клієнтів (наприклад, це програми для роботи з електронною поштою, програма-браузер для перегляду гіпертекстових Web-документів тощо). Більшість користувачів Internet працюють на звичайних персональних комп'ютерах.

Кількість доступних їм послуг Internet залежить від типу сполучення з мережею[2].

## Розрахунок адресного простору

Розподіл АП - це процес закріплення конкретних фізичних адрес за окремими функціональними областями пам'яті (сегментами) - програм, констант, даних, стека, вводу-виводу.

IP-мережа може бути розбита на дрібніші фрагменти, звані підмережами. Для цього необхідно перейти від використання дворівневої ієрархії IP адрес (номер мережі і номер вузла) до трирівневої (номер мережі, номер підмережі і номер вузла).

Для завдання номера підмережі виділяється деяка частина розрядів з поля номера вузла. Розмірність поля номера підмережі змінюється залежно від необхідної кількості підмереж і кількості вузлів в кожній з них.

Кожна підмережа представляється як звична IP-мережа, що додає велику гнучкість схемі розподілу адрес, дозволяє ефективніше витратити адреси і уникнути їх марної трати.

Сукупність номера мережі і номера підмережі називають розширеним мережевим префіксом. Для виділення номера підмережі використовується маска підмережі (Subnet Mask). Формат маски підмережі аналогічний формату IP-адреси. Проте маска підмережі в двійковому представленні завжди містить послідовність одиниць в тій частині, яка відповідає номеру мережі і підмережі, і послідовність нулів в тій частині, яка відповідає номеру вузла «рис.1.1»[3].

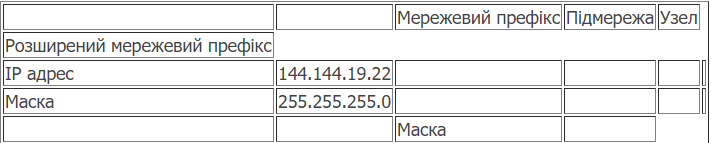


Рисунок 1.2 Елементи IP адреси і маска

Маску в десятковому представленні зручно використовувати лише тоді, коли розширений мережевий префікс закінчується на межах байтів, в інших випадках її розшифрувати складніше. Допустимо, що в прикладі на рисунку 1.3 ми хотіли б для підмережі використовувати не 8 біт, а десять. Тоді в останньому (4-му) байті маски ми мали б не нулі, а число 11000000 (11111111.11111111.11111111.11000000 – елементи маски, що ідентифікують підмережу виділені жирним шрифтом).

У десятковому представленні одержуємо 255.255.255.192. Очевидно, що таке представлення не дуже зручне. Зручнішим є позначення виду «/xx», де хх - кількість бітів в розширеному мережевому префіксі. Таким чином, замість вказівки: «144.144.19.22 з маскою 255.255.255.192», можна записати: 144.144.19.22/26.

Для розрахування адресного простору для підмережі потрібно у першу чергу знати яка кількість хостів буде у ній міститися.

Розглянемо таблицю, варіант 13 «рис. 1.2».

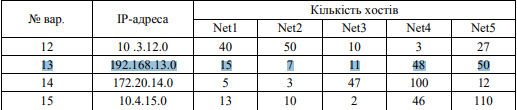


Рисунок 1.3 Вихідні дані для адресації хостів мережі центрального офісу

Мережа центрального офісу складається з п’яти підрозділів (Net1- Net5), кількість комп’ютерів в кожному з яких визначається у таблиці.

Для кожної підмережі потрібно виділити кількість хостів, яка буде оптимальною. Для цього необхідно виділити 2n хостів, які будуть перевищувати задану нам кількість у таблиці, проте число буде найближчим більшим числом. Також, потрібно мати на увазі те, що 2 адреси будуть виділені на адрес самої мережі та broadcast адресу.

Наприклад, у Net2 ми маємо 7 хостів, найближчім блищим числом 2n є 8, проте, так як нам виділити ще 2 адреси на мережу та broadcast адресу – ми виділяємо 16 хостів з маскою підмережі /28.

Відобразимо розподілені підмережі у круговій діаграмі «рис. 1.3»

Рисунок 1.3 Виділена кількість хостів у мережі LAN1

Виходячи з кругової діаграми, можна побачити, що з 256 можливих адресів у нас залишилось незадіяними 64 хости, які можна було б виділити мінімально ще для однієї підмережі.

# РОЗДІЛ 2 Налаштування компьютерної мережі



## Вибір та налаштування способу маршрутизації

*Маршрут* – це послідовність портів маршрутизаторів, які повинен пройти пакет від джерела до адресата. Сам маршрутизатор адреси не має, а кожний порт маршрутизатора має числову адресу і локальну адресу тієї мережі, до складу якої він входить. Тип і формат числових адрес залежить від стека комунікаційних протоколів, який використовується в об'єднаній мережі. Здебільшого числові адреси складаються з номера мережі, в якій знаходиться адресат, та номера кінцевого вузла в цій мережі.

*Маршрутиза́ція* (англ. Routing) — процес визначення маршруту прямування інформації між мережами. Маршрутизатор (або роутер від англ. router) приймає рішення, що базується на IP-адресі отримувача пакету. Для того, щоб переслати пакет далі, всі пристрої на шляху слідування використовують IP-адресу отримувача. Для прийняття правильного рішення маршрутизатор має знати напрямки і маршрути до віддалених мереж. Є два типи маршрутизації:

*Статична маршрутизація* — маршрути задаються вручну адміністратором.

*Динамічна маршрутизація* — маршрути обчислюються автоматично за допомогою протоколів динамічної маршрутизації — RIP, OSPF, EIGRP, IS-IS, BGP, HSRP та ін, які отримують інформацію про топологію і стан каналів зв'язку від інших маршрутизаторів у мережі[4].

Оскільки статичні маршрути конфігуруються вручну, будь-які зміни мережної топології вимагають участі адміністратора для додавання і видалення статичних маршрутів відповідно до змін. У великих мережах підтримка таблиць маршрутизації вручну може вимагати величезних витрат часу адміністратора. У невеликих мережах це робити легше. Статична маршрутизація не має можливості масштабування, яку має динамічна маршрутизація через додаткові вимоги до налаштування і втручання адміністратора. Але і у великих мережах часто конфігуруються статичні маршрути для спеціальних цілей у комбінації з протоколами динамічної маршрутизації, оскільки статична маршрутизація є стабільнішою і вимагає мінімум апаратних ресурсів маршрутизатора для обслуговування таблиці.

Динамічні маршрути виставляються іншим чином. Після того, як адміністратор активізував і налаштував динамічну маршрутизацію за одним з протоколів, інформація про маршрути оновлюється автоматично в процесі маршрутизації після кожного отримання з мережі нової інформації про маршрути. Маршрутизатори обмінюються повідомленнями про зміни у топології мережі в процесі динамічної маршрутизації.

Маршрутизація є однією з основних функцій мережевого рівня і загалом зводиться до вибору вузлом комутації шляху подальшої передачі інформації, яка надійшла на його вхід.

Просте, на перший погляд, завдання — вибір оптимального маршруту — досить складна проблема, що не має однозначного вирішення для мереж з різною топологією, обсягом і характером потоку даних. Складність вирішення цього завдання зумовлена низкою причин.

По-перше, маршрутизація, звичайно, потребує координації роботи всіх вузлів мережі передачі даних. По-друге, система маршрутизації має нормально функціонувати у разі виходу з ладу окремих вузлів і ліній зв’язку. По-третє, система повинна враховувати перевантаження окремих ділянок мережі передачі даних і змінювати маршрути проходження повідомлень

## Конфігурування базових функцій маршрутизаторів

Логічні функції маршрутизатора так само важливі, як і забезпечення фізичного взаємозв'язку множини мереж. Наприклад, для об'єднаної мережі потрібний, аби між відправником і одержувачем був хоча б один фізичний канал передачі даних. Проте існування і використання фізичного каналу – це дві різні речі. Природно, що для нормальної роботи відправник і одержувач повинні "розмовляти" однією мовою (використовувати єдиний протокол маршрутизації). Крім того, така мова (протокол маршрутизації) дає можливість шляхом спілкування з проміжними маршрутизаторами знаходити найкоротший маршрут для передачі даних[5].

Маршрутизатор Cisco 2911 «рис.2.1» розроблено для малих і середніх підприємств, яким потрібні сучасні технологічні рішення, що забезпечують надійне високопродуктивне підключення до мережі Інтернет. Серія маршрутизаторів Cisco ISR G2 2900 представлена 4 фіксованими і декількома розширеними моделями, у даній серії маршрутизаторів є велика кількість різних інтерфейсів і модулів.

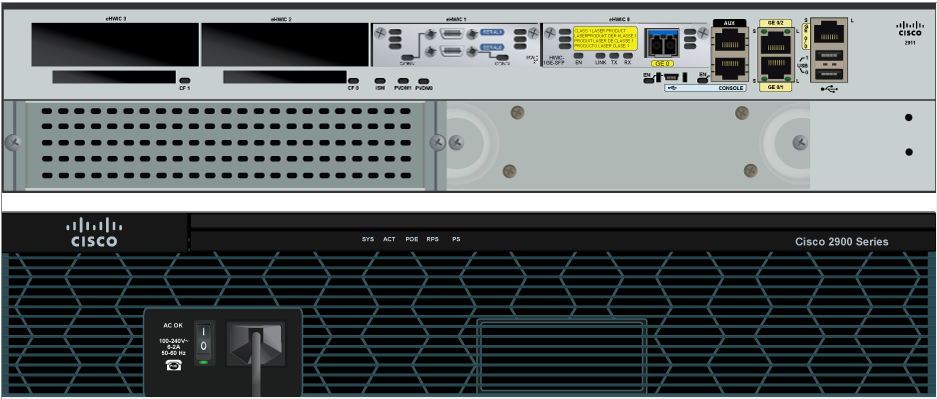


Рисунок 2.1 Маршрутизатор Cisco 2911

Першочергово, потрібно підключити до інтерфейсів маршрутизатора з’єднання, та у вкладці config підняти інтерфейси( переключити port status на on) та надати їм айпі-адреси та маски підмережі. Для прикладу візьмем конфігурацію маршрутизатора Cisco 2911 з LAN1 та розглянемо її «рис. 2.2».

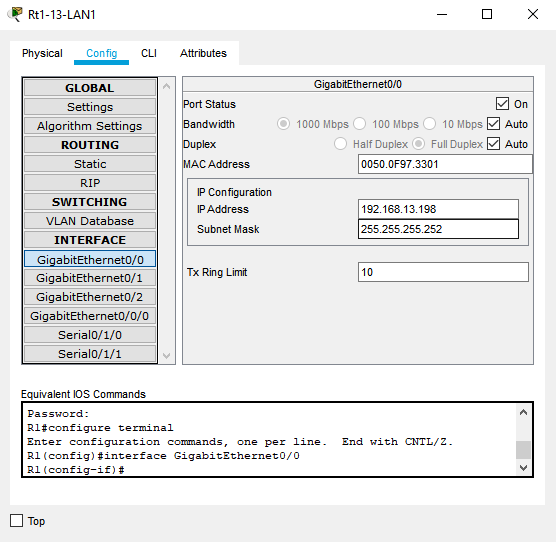


Рисунок 2.2 Першочергове налаштування маршрутизатора

Другим кроком буде налаштування маршрутизації, яка буває як статична, так і динамічна. Статичну маршрутизацію можна настроїти у вкладці config, розділ routing static «рис2.3».

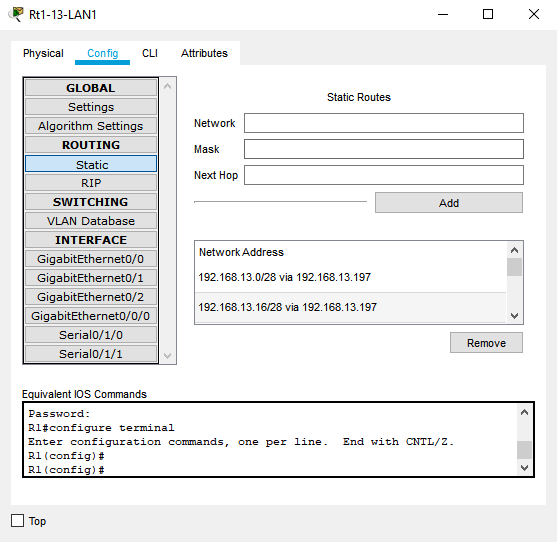


Рисунок 2.3 Налаштування статичної маршрутизації

Де прописуємо адресу мережі, її маску та адрес найближчого інтерфейсу наступного пристрою.

Динамічну маршрутизацію потрібно налаштовувати у вкладці CLI у привілейованому глобальному режимі, прописавши команди в залежності від протоколів, які потрібно налаштувати.

Наступним кроком для безпеки доступу потрібно встановити пароль на режим привілейованого доступу, консольного доступу, та ССШ.

Для цього потрібно перейти у вкладку CLI та прописати наступні команди у привілейованому глобальному режимі:

* Enable secret Shevchenko // *встановити пароль на привілейований режим «Shevchenko».*
* Console line 0

Enable secret Shevchenko // *встановлення паролю на консольне з’єднання «Shevchenko».*

* Line vty 0 15
  + - Enable secret Shevchenko

Transport input ssh // *Встановлення доступу на видалене керування з інших пристроїв маршрутизатором, а також пароль на під’єднання «Shevchenko».*

## Проектування віртуальних мереж

### Створення VLAN

Під час настроювання мереж VLAN стандартного діапазону інформація про конфігурацію зберігається у флеш-пам'яті перемикача, у файлі vlan.dat файлу. Флеш-пам'ять є постійною, тому не вимагає виконання copy running-config startup-config. Однак, оскільки інші параметри часто потрібно налаштувати під час створення мереж VLAN на перемикачі Cisco, варто зберегти поточні зміни конфігурації початкової конфігурації завантаження.

На «рис2.4» показує синтаксис команди Cisco iOS, який використовується для додавання мережі VLAN до комутатора та дати йому назву. Під час настроювання перемикача варто назвати кожну мережу VLAN.

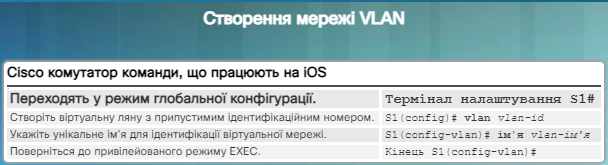


Рисунок 2.4 Команди комутатора

На «рис.2.5» показує, як перемикач S1 налаштовує мережу VLAN для студентів (VLAN 20). У прикладі топології комп'ютер учня (PC2) не був прив'язаний до мережі VLAN, але має IP-адресу 172.17.20.22.

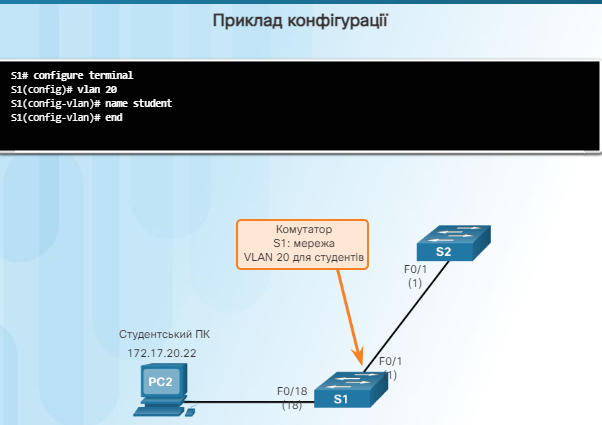


Рисунок 2.5 Приклад конфігурації

Скористайтеся командою vlan, щоб створити мережу VLAN.

S1# configure terminal

Введите построчно команды настройки. В конце нажмите CNTL/Z.

S1(config)# vlan 20

S1(config-vlan)# name Student

S1(config-vlan)# end

S1#

\*Mar 31, 08:55:14.5555: %SYS-5-CONFIG\_I: Configured from console by console

S1#

Введіть команду show vlan brief для відображення вмісту файлу vlan.dat.

S1# show vlan brief

VLAN Name Status Ports

---- ------------------ --------- -----------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/18, Fa0/19, Fa0/20

Fa0/21, Fa0/22, Fa0/23, Fa0/24

1 Gig0/1, Gig0/2

20 Student active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

S1#

Окрім одного ідентифікатора VLAN, можна ввести групу ідентифікаторів VLAN, розділених комами, або діапазон ідентифікаторів VLAN, розділених дефісами, за допомогою мереж vlan *vlan\_id* [7]. Наприклад, для створення мереж VLAN 100, 102, 105, 106 та 107 скористайтеся такою командою:

S1(config)# vlan 100,102,105-107

### Призначення портів мережі VLAN

Наступним кроком після створення мережі VLAN є призначення портів для мереж VLAN.

На «рис. 2.6» показує синтаксис для визначення порту як порту доступу та призначення його мережі VLAN. Команда switchport mode access не є обов'язковою, але настійно рекомендується з міркувань безпеки. За допомогою цієї команди інтерфейс переходить у режим постійного доступу.

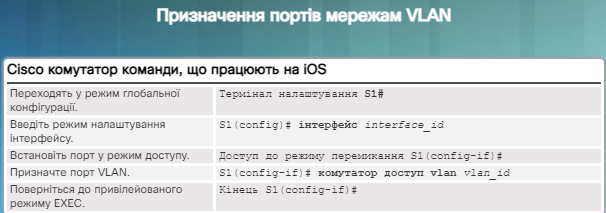


Рисунок 2.6 Призначення портів мережі VLAN

Використовуйте команду interface range, щоб настроїти кілька інтерфейсів одночасно.На прикладі «рис. 2.7» Мережа VLAN 20 призначається порту F0/18 на комутаторі S1. Будь-який пристрій, підключений до цього порту, підключено до VLAN 20. Таким чином, у нашому прикладі комп'ютер PC2 знаходиться в мережі VLAN 20.

S3(config)# interface F0/18

S3(config-if)# switchport mode access

S3(config-if)# switchport access vlan 20

S3(config-if)#



Рисунок 2.7 Приклад топології

Важливо відзначити, що мережі VLAN налаштовані на порту перемикача, а не на кінцевому пристрої. Для pc2 IPv4-адреса та маска підмережі пов'язані з мережею VLAN, налаштованою на порту комутатора.[8] У цьому прикладі це мережа VLAN 20. Під час настроювання VLAN 20 на інших перемикачах адміністратор мережі повинен настроїти комп'ютери інших студентів у тій самій підмережі, що й PC2 (172.17.20.0/24).

Порт доступу може належати лише до однієї віртуальної мережі.

Скористайтеся командою show vlan brief для відображення вмісту файлу vlan.dat.

S3# show vlan brief

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/7, Fa0/8

Fa0/9, Fa0/10, Fa0/11, Fa0/12

Fa0/13, Fa0/14, Fa0/15, Fa0/16

Fa0/17, Fa0/19, Fa0/20, Fa0/21

Fa0/22, Fa0/23, Fa0/24, Gi0/1

Gi0/2

20 student active Fa0/18

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

S3#

Команда switchport access vlan примусово створює VLAN, якщо її ще немає на комутаторі. Наприклад, мережа VLAN 30 не присутня у виводі даних короткою командою show vlan brief на перемикачі. Якщо ви вводите команду switchport access vlan 30 на будь-якому інтерфейсі без попередньої конфігурації, перемикач відобразить наступне:

% доступу до VLAN не існує. Створення vlan 30

### Перевірка інформації стосовно налаштування

Налаштувавши мережу VLAN, ви можете перевірити за допомогою команд Cisco iOS "show". На «рис. 2.8» показано show vlan і show interfaces.



Рисунок 2.8 Параметри команд show vlan і show interfaces.

На прикладі «рис. 2.9» show vlan name student команда генерує вихід, який нелегко інтерпретувати. У зведеній команді show vlan summary відображається список усіх налаштованих мереж VLAN.

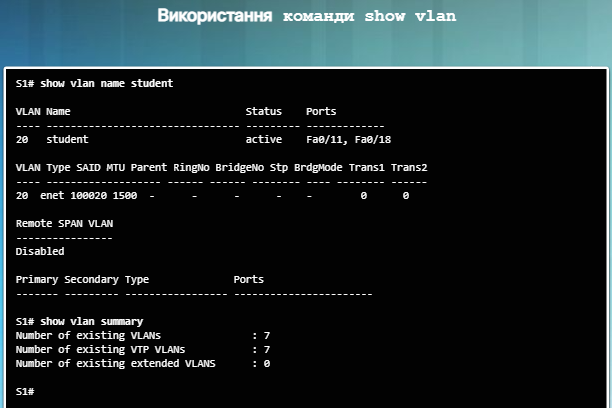


Рисунок 2.9 Використання команди show vlan

Командаshow interfaces vlan vlan\_id відображає у другій лінії на «рис. 2.10» важливу інформацію, яка вказує на те, що мережа VLAN 20 знаходиться в робочому порядку.

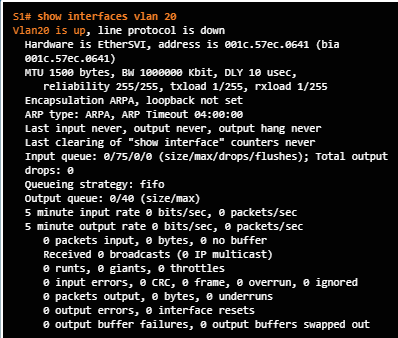


Рисунок 2.10 Використання команди show interfaces vlan

Скористайтеся зазначеними командами для перевірки налаштування vlan.

S1# show vlan name student

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

20 student active Fa0/11, Fa0/18

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2

---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

20 enet 100020 1500 - - - - - 0 0

Remote SPAN VLAN

----------------

Disabled

Primary Secondary Type Ports

------- --------- ----------------- ------------------------------------------

S1#

S1# show vlan summary

Number of existing VLANs : 7

Number of existing VTP VLANs : 7

Number of existing extended VLANS : 0

S1#

S1# show interfaces vlan 20

Vlan20 is up, line protocol is up

Hardware is CPU Interface, address is 0007.ec74.61d3 (bia 0007.ec74.61d3)

MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 21:40:21, output never, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

1682 packets input, 530955 bytes, 0 no buffer

Received 0 broadcasts (0 IP multicast)

0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

563859 packets output, 0 bytes, 0 underruns

0 output errors, 23 interface resets

0 output buffer failures, 0 output buffers swapped out

S1#

S1# show interfaces F0/18 switchport

Name: Fa0/18

Switchport: Enabled

Administrative Mode: static access

Operational Mode: down

Administrative Trunking Encapsulation: dot1q

Operational Trunking Encapsulation: native

Negotiation of Trunking: Off

Access Mode VLAN: 20 (Students)

Trunking Native Mode VLAN: 1 (default)

Voice VLAN: none

## Конфігурування базових функцій комутаторів LAN

Основними параметрами налаштування комутатора є:

* Ім'я вузла;
* Пароль консолі;
* Пароль VTY;
* Пароль привілейованого режиму EXEC;
* Таємний пароль привілейованого режиму EXEC;
* Шлюз по замовчуванню.

Так як, у даній курсовій роботі використовувався комутатор Cisco Catalyst 2960 – ми його будемо розглядати на прикладі «рис. 2.11».

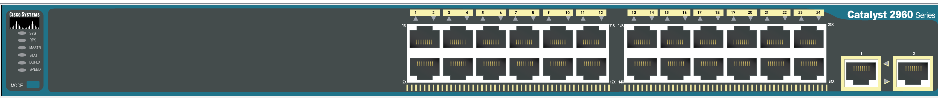


Рисунок 2.11 Комутатор Cisco Catalyst 2960

Першочергово потрібно підключити до комутатора з’єднання у вільні порти. Наступним кроком буде підняття інтерфейсів у владці config interface переключивши port status на ON «рис. 2.12»[10].

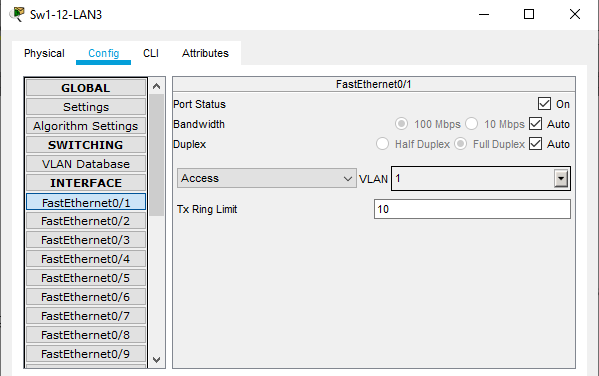


Рисунок 2.12 Підняття портів комутатора

Далі, потрібно надати комутатору дісплейне ім’я та ім’я хоста також у вкладці config settings «рис. 2.13».

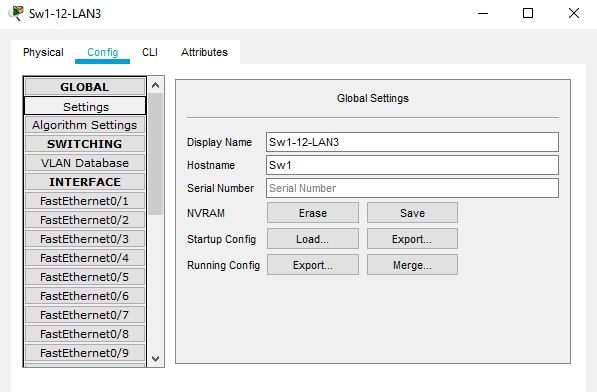


Рисунок 2.13 Надання імен комутатору

Наступним кроком для безпеки доступу потрібно встановити пароль на режим привілейованого доступу, консольного доступу, та ССШ.

Для цього потрібно перейти у вкладку CLI та прописати наступні команди у привілейованому глобальному режимі:

* Enable secret Shevchenko // *встановити пароль на привілегійований режим «Shevchenko».*
* Console line 0

Enable secret Shevchenko // *встановлення паролю на консольне з’єднання «Shevchenko».*

* Line vty 0 15

Enable secret Shevchenko

Transport input ssh // *Встановлення доступу на видалене керування з інших пристроїв маршрутизатором, а також пароль на під’єднання «Shevchenko».*

## Конфігурування додаткових функцій маршрутизаторів

### Конфігурування протоколу DHCP

Для кожного пристрою, підключеного до мережі, потрібна унікальна IP-адреса. Адміністратори мережі призначають статичні IP-адреси маршрутизаторам, серверам, принтерам та іншим мережевим пристроям, фізичне та логічне розташування яких навряд чи зміниться. У більшості випадків це пристрої, які надають послуги користувачам і пристроям в мережі; таким чином, призначені їм адреси повинні бути постійними. Крім того, статичні адреси дозволяють адміністраторам керувати цими пристроями віддалено. Адміністраторам мережі легше отримати доступ до пристрою, якщо його IP-адресу легко ідентифікувати.

Однак фізичне та логічне розташування користувачів і комп'ютерів часто змінюється всередині організації. Призначення нових IP-адрес щоразу, коли працівник переміщується, може бути складним і трудомістким процесом. Під час настроювання настройок мережі вручну для співробітників, які працюють із віддалених розташувань, адміністратор також може зіткнутися з низкою проблем. Крім того, вручну призначення IP-адрес і налаштування інших відомостей про адресу робочого стола також вимагає зусиль і час витрат системного адміністратора, особливо коли мережа розширюється.

Введення сервера з протоколом динамічного налаштування вузла (DHCP) в локальну мережу спрощує призначення IP-адрес як стаціонарним, так і мобільним пристроям. Використання централізованого DHCP-сервера дозволяє організації керувати привласненням всіх динамічних IP-адрес з одного сервера. Ця практика робить управління IP-адресами більш ефективним і забезпечує узгодженість процесів і узгодженість даних по всій організації, включаючи філії.

Протокол DHCP доступний як для IPv4 (DHCPv4), так і для IPv6 (DHCPv6). У цьому розділі описано функції, настройки та пошук і виправлення неполадок протоколів dhCPv4 та DHCPv6.

Крок 1. Виключення адрес IPv4

Маршрутизатор, який діє як сервер DHCPv4, призначає всі адреси IPv4 з пулу DHCPv4, якщо конфігурація не передбачає виключення окремих адрес. Як правило, деякі IPv4-адреси з пула призначаються мережних пристроїв для постійного використання. Таким чином, ці адреси IPv4 не слід призначати іншим пристроям. Щоб виключити певні адреси, скористайтеся командою ip dhcp-address, як показано на «рис. 2.14» [6].

R1(config)# ip dhcp excluded address 192.168.13.14



Рисунок 2.14 виключення адресів

Можна виключити одну адресу або діапазон адрес, установлюючи адреси нижньої та верхньої меж діапазону. Виключені адреси мають містити адреси, призначені маршрутизаторам, серверам, принтерам та іншим пристроям, які були або будуть налаштовані вручну.

Крок 2. Настроювання пулу адрес DHCPv4

Під вільний час настроювання сервера DHCPv4, встановити пул адрес для розповсюдження. Як показано на «рис. 2.15», IP DHCP POOL пул ім'я команди створює пул з заданим ім'ям і ставить маршрутизатор в режимі конфігурації DHCPv4, який визначається запит на змінення рядок: маршрутизатор (dhcp-конфігурації).

R1(config)# ip dhcp pool DHCPnet1

R1(dhcp-config)# network 192.168.13.0 255.255.255.240

R1(dhcp-config)# default-router 192.168.13.14

R1(dhcp-config)# dns-server 8.8.8.8

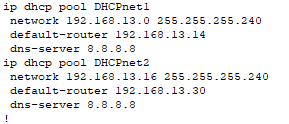


Рисунок 2.15 Конфігурація DHCP-пула

Адресний пул і головний шлюз маршрутизатора повинні бути налаштовані. Команда "Network" використовується для визначення діапазону доступних адрес.

За допомогою команди default-router установлюється головний шлюз маршрутизатора. Шлюз, як правило, інтерфейс маршрутизатора локальної мережі найближче до клієнтських пристроїв. Потрібен лише один шлюз, але якщо у вас кілька шлюзів, можна перерахувати до восьми адрес.

Решта пулу DHCPv4 є додатковими. Наприклад, IPv4 DNS-сервер адресу, доступну для DHCPv4 для клієнта настроєно за допомогою команди dns-server. Команда domain-name домену використовується для встановлення імені домену. Довжина оренди DHCPv4 змінюється командою lease. За замовчуванням тривалість оренди становить один день. Команда netbios-name-serverвикористовується для настроювання NetBIOS WINS.

DHCPv4 увімкнуто за промовчанням. Щоб вимкнути службу, введіть команду в глобальному режимі no service dhcp. Щоб перезапустити DHCPv4, використовуйте команду в глобальному режимі service dhcp. Якщо настройки не налаштовано, активація служби не діє.

### Налаштування NAT

Перетворення NAT використовується для різних цілей, але основною метою цього механізму є збереження загальнодоступних адрес IPv4. Це досягається за допомогою приватних адрес IPv4 для внутрішньої взаємодії та перетворення на загальнодоступні адреси лише за потреби. Додатковою перевагою NAT є підвищена конфіденційність і безпека мережі, оскільки цей механізм приховує внутрішні адреси IPv4 із зовнішніх мереж[7].

Для маршрутизатора з підтримкою NAT можна настроїти одну або кілька наявних загальнодоступних адрес IPv4. Ці загальнодоступні адреси відомі як пул адрес NAT. Якщо внутрішній пристрій надсилає трафік за межами мережі, маршрутизатор з підтримкою NAT перетворює внутрішній IPv4-адресу пристрою на загальнодоступну адресу з nat пула. Зовнішні пристрої вважають, що весь трафік, що надходить і виходить з мережі, використовує загальнодоступні адреси IPv4 з наданого пулу адрес.

Маршрутизатор NAT зазвичай працює на краю тупик мережі. Мертва мережа - це мережа, яка має лише одне підключення до сусідньої мережі, і, як наслідок, єдиний вихід і єдиний шлях до цієї мережі. У прикладі, показаному на зображенні, R2 є прикордонним маршрутизатором. З точки зору інтернет-провайдера, маршрутизатор R2 створює глухий кут мережі.

Коли пристрій у мертвій мережі вимагає підключення пристрою від мережі, пакет надсилається до прикордонного маршрутизатора. Прикордонний маршрутизатор виконує процес NAT, перетворюючи внутрішню приватну адресу пристрою на загальнодоступну, зовнішню, маршрутизуючу адресу.

*Статична трансформація NAT* – це взаємно однозначна позиція внутрішньої та зовнішньої адрес. Статичний NAT дозволяє зовнішнім пристроям ініціювати підключення до внутрішніх пристроїв за допомогою статичної публічної адреси. Наприклад, внутрішній веб-сервер можна порівняти з внутрішньою глобальною адресою, визначеною таким чином, щоб вона була доступна із зовнішніх мереж.

На «рис. 2.16» показує внутрішню мережу з веб-сервером з приватною адресою IPv4. Маршрутизатор R2 має статичний NAT, налаштований для забезпечення доступу до Інтернету для пристроїв із зовнішньої мережі (Інтернет). Зовнішній клієнт отримує доступ до веб-сервера за допомогою загальнодоступної адреси IPv4. Статичний NAT перетворює загальнодоступну адресу IPv4 на приватну IPv4-адресу.

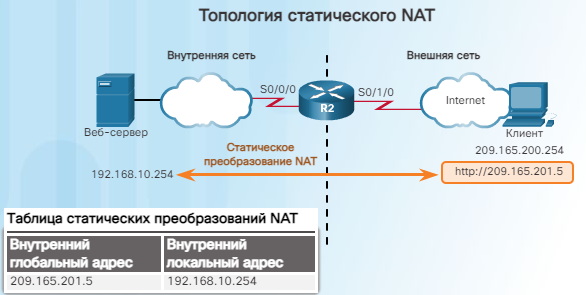


Рисунок 2.16 Топологія статичного NAT

Налаштування статичного NAT має два основних завдання:

1. Перше завдання – створити відповідність між внутрішньою локальною та внутрішньою глобальною адресами. Наприклад, на «рис. 2.22» як статичні перетворення NAT створити внутрішню локальну адресу 192.168.10.254 і внутрішній глобальної адреси 209.165.201.5.
2. Після того, як відповідні інтерфейси, що беруть участь у перетворенні, регулюються як внутрішні або зовнішні на NAT. У цьому прикладі послідовний інтерфейс 0/0/0 маршрутизатора R2 є внутрішнім, а послідовний 0/1/0 – зовнішнім інтерфейсом.

Пакети, які потрапляють у внутрішній інтерфейс маршрутизатора R2 (послідовний 0/0/0) з налаштованої внутрішньої локальної адреси IPv4 (192.168.10.254) перетворюються а потім передаються до зовнішньої мережі. Пакети на зовнішній інтерфейс маршрутизатора R2 (послідовний 0/1/0), адресовані налаштованої внутрішньої глобальної адреси IPv4 (209.165.201.5), перетворюються на внутрішню локальну адресу (192.168.10.254) і потім передаються до внутрішньої мережі.

На «рис. 2.17» - це команди, потрібні для налаштування статичного NAT.

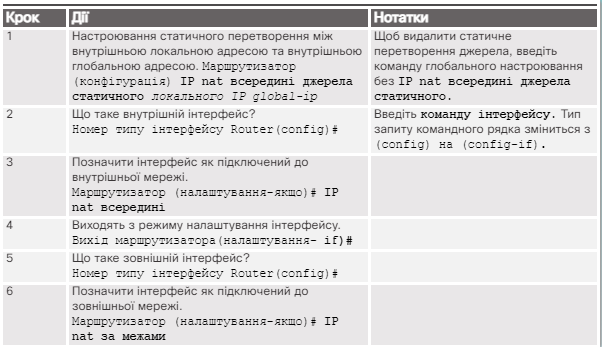


Рисунок 2.17 Команди для налаштування статичного NAT

На «рис. 2.18» показує команди, необхідні для створення статичного NAT зіставлення для веб-сервера на маршрутизаторі R2 у прикладі топології. У рамках показаних налаштувань R2 перетворює адресу 192.168.168.10.254 на загальнодоступну адресу IPv4 в пакетах 209.165.201.5. Інтернет-клієнт надсилає веб-запити на загальнодоступну адресу IPv4 209.165.201.5. Маршрутизатор R2 надсилає цей трафік на веб-сервер за номером 192.168.10.254.

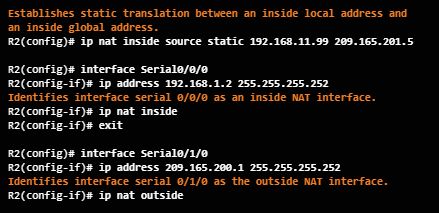


Рисунок 2.18 Приклад налаштування статичного NAT

## Налаштування захисту та конфігурування функцій безпеки

### Створення списків ACL

Створення списків ACL може бути складним завданням. Для кожного інтерфейсу може бути кілька правил для керування типами трафіку, які дозволено вводити або виходити через цей інтерфейс. Маршрутизатор на зображенні має два інтерфейси, налаштовані для IPv4 та IPv6. Якщо обидва протоколи вимагають списки ACL на обох інтерфейсах і в обох напрямках, вам потрібно буде створити 8 окремих списків ACL. Кожен інтерфейс матиме чотири списки керування Доступом: два списки для протоколу IPv4 та два для IPv6. Кожен протокол вимагає один ACL для вхідного трафіку і один для вихідного трафіку.

Списки керування доступом не потрібно налаштовувати в обох напрямках. Номери ACL та їх напрямки, застосовані до інтерфейсу, залежать від заявлених вимог.

Нижче наведено кілька рекомендацій щодо використання списків ACL:

1. Використовуйте списки керування доступом у маршрутизаторах брандмауера, розташованих між внутрішніми та зовнішніми мережами, наприклад Інтернетом.
2. Щоб керувати вхідним або вихідним трафіком у певній частині внутрішньої мережі, використовуйте списки ACL на маршрутизаторі, розташованому між двома сегментами мережі.
3. Налаштуйте списки ACL на прикордонних маршрутизаторах, тобто маршрутизаторах, розташованих на межі мережі. Це забезпечить базовий буфер із зовнішньої мережі або між менш контрольованими та більш чутливими областями мережі.
4. Настроювання списків керування Доступом для кожного мережного протоколу, створеного в інтерфейсі прикордонного маршрутизатора.

Правила для списків керування доступом (ACL):

Ви можете налаштувати один список керування доступом для протоколу, напрямку, інтерфейсу.

1. Один список списку керування доступом для одного протоколу полягає в тому, що для керування потоком трафіку в інтерфейсі ACL список має бути визначено для кожного протоколу, що працює на інтерфейсі.
2. Один список списку ACL для одного напрямку список керування доступом одночасно контролює трафік в одному напрямку одного інтерфейсу. Для керування вихідним і вхідним трафіком необхідно створити два окремі списки керування доступом.
3. Один список ACL для одного інтерфейсу полягає в тому, що список керування доступом на одному інтерфейсі, наприклад GigabitEthernet 0/0.

Щоб використовувати стандартні нумеровані списки списку керування Доступом на маршрутизаторі Cisco, спочатку потрібно створити стандартний список керування доступом, а потім активувати його в інтерфейсі.

Глобальна команда конфігурації access-list визначає стандартний список керування доступом з числом від 1 до 99. Cisco IOS версії 12.0.1, цей діапазон був розширений; стандартні списки ACL можуть бути використані для чисел з 1300 по 1999 рік. Це дозволяє створювати до 798 можливих стандартних списків ACL. Списки з цими додатковими номерами називаються додатковими списками керування доступом (ACL) IPv4.

Повний синтаксис стандартної команди ACL-list:

Router(config)# access-list номер списка доступа { deny | permit | remark } source [ source-wildcard ][ log ]

«Рис. 2.19» містить докладний опис синтаксису для стандартного списку списку ACL.

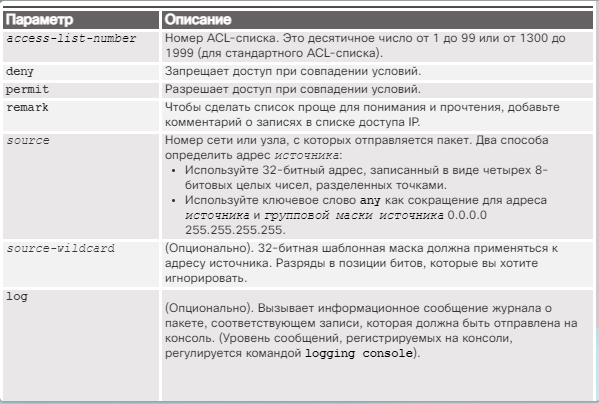


Рисунок 2.19 Команди для конфігурації списку доступу

Записи зі списку керування доступом дозволяють або забороняють трафік на певну адресу хоста або діапазон таких адрес. Щоб створити запис 10 пунктів у нумерований список керування доступом (ACL) на основі ключового слова хоста, що дозволяє трафік для хоста з IP-адресою 192.168.10.10, потрібно ввести таку команду:

R1(config)# access-list 10 permit host 192.168.10.10

Як показано на «рис. 2.20», щоб створити запис А, який дозволяє IPv4 діапазон адрес у списку нумеровані список ACL 10, що дозволяє всі IPv4-адреси в мережі 192.168.10.0/24, потрібно ввести таку команду:

R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255.



Рисунок 2.20 Видалення списку доступу

No access-list команда використовується для видалення списку списку ACL. Введення команди show access-list підтверджує видалення списку ACL з 10.

Як правило, коли адміністратор створив список керування доступом, застосунок кожного запису відомий і очевидний. Однак для того, щоб адміністратор та інші користувачі пам'ятали мету запису, потрібно додати відповідні коментарі. Ключове слово remark використовується для документування та спрощення читання списків ACL. Довжина коментаря обмежена 100 символами. Досить простий список ACL на «рис. 2.21» наводиться як приклад. Під вільний час перегляду конфігурації списку керування доступом show running-config команди, ви також бачите коментар.



Рисунок 2.21 Огляд списку контроля доступу

### Налаштування паролів

За промовчанням мінімальна довжина пароля становить 6 символів. Щоб збільшити мінімальну довжину пароля, використовуйте security passwords min-length.

За замовчуванням, за винятком пароля, створеного командою enable secret, всі паролі маршрутизатора Cisco зберігаються як простий текст у файлах конфігурації завантаження та маршрутизатора. Щоб зашифрувати всі паролі, передані звичайним текстом, скористайтеся командою service password-encryption в режимі глобальної конфігурації. Шифрування дуже легко зламати, якщо ви використовуєте правильний інструмент. Таким чином, цю команда не слід використовувати для зшивання конфігураційних файлів з серйозних атак.

За замовчуванням інтерфейс адміністратора залишається активним, з введенням, протягом 10 хвилин після справи останнього сеансу. Щоб вимкнути без нагляду підключення, використовуйте exec-timeout (хвилин) команди в режимі конфігурації рядка для кожного з рядків, які настроєно для доступу.

Також можна вимкнути execпроцес для певного рядка, наприклад, aux-порт, використовуючи команду no exec у режимі конфігурації рядка. Ця команда дозволяє лише вихідні рядки підключення, вимкнувши exec процес для підключень, які можуть спробувати надіслати небажані дані маршрутизатора.

Для безпеки доступу потрібно встановити пароль на режим привілегійованного доступу, консольного доступу, та ССШ.

Для цього потрібно перейти у вкладку CLI та прописати наступні команди у привілейованому глобальному режимі:

* Enable secret Shevchenko // *встановити пароль на привілейований режим «Shevchenko».*
* Console line 0

Enable secret Shevchenko // *встановлення паролю на консольне з’єднання «Shevchenko».*

* Line vty 0 15

Enable secret Shevchenko

Transport input ssh // *Встановлення доступу на видалене керування з інших пристроїв маршрутизатором, а також пароль на під’єднання «Shevchenko».*

## Налаштування віддаленого доступу до активного обладнання

Доступ до маршрутизатора в адміністративних цілях може здійснюватися локально або віддалено.

*Локальний доступ*. Усі пристрої мережевої інфраструктури можна отримати локально. Локальний доступ до маршрутизатора зазвичай вимагає прямого підключення до порту консолі на маршрутизаторі Cisco, а також використання комп'ютера, на який працює програмне забезпечення емуляції терміналів, як показано на «рис. 2.22». Адміністратор повинен мати фізичний доступ до маршрутизатора та використовувати консольний кабель для підключення до порту консолі. Локальний доступ зазвичай використовується для вихідної конфігурації пристрою.



Рисунок 2.22 Топологія локального доступу

*Віддалений доступ*. Адміністратори також можуть входити на інфраструктурні пристрої віддалено, як показано на «рис. 2.23». Хоча параметр порту з допоміжною допомогою доступний, найбільш поширеним доступом є telnet, SSH, HTTP, HTTPS або SNMP з вашого комп'ютера. Комп'ютер може бути як локально, так і віддалено.



Рисунок 2.23 Віддалений доступ за протоколом SSH

Деякі протоколи віддаленого доступу відправляють дані на маршрутизатор, включаючи імена користувачів і паролі, у вигляді простого тексту. Якщо зловмисник може збирати мережний трафік, коли адміністратор віддалено входить до маршрутизатора, зловмисник може отримати паролі або дані конфігурації маршрутизатора. Таким чином, краще дозволити лише локальний доступ до маршрутизатора. Однак у деяких випадках віддалений доступ також може знадобитися. Нижче наведено такі запобіжні заходи, коли ви можете отримати віддалений доступ до маршрутизатора.

1. Шифрувати весь трафік між комп'ютером адміністратора та маршрутизатором. Наприклад, замість Telnet використовуйте SSH версії 2 або використовуйте HTTPS замість HTTP.
2. Створіть спеціальну мережу керування. Мережа керування має містити лише визначені адміністративні хости та підключення до виділеного інтерфейсу маршрутизатора.
3. Налаштуйте фільтр пакета, щоб доступ до маршрутизатора могли отримати лише визначені адміністративні хости та привілейовані протоколи. Наприклад, щоб ініціювати підключення до мережі до маршрутизаторів, дозволяйте лише запити SSH з IP-адреси адміністрації хоста.
4. Налаштуйте та інсталюйте підключення VPN до локальної мережі, перш ніж підключатися до інтерфейсу керування маршрутизатором.

Ці запобіжні заходи важливо вжити, але вони не зможуть повністю захистити мережу. Також потрібно використовувати інші засоби захисту. Одним з основних і важливих способів є використання надійних паролів.

# РОЗДІЛ 3 Моделювання та тестування роботи розробленої мережі



## Моделювання мережі LAN 1

Мережа центрального офісу складається з п’яти підрозділів (Net1- Net5),

кількість комп’ютерів в кожному з яких визначається «рис. 3.1», та мережі Net6, де розташований локальний сервер ого офісу «рис. 3.2».

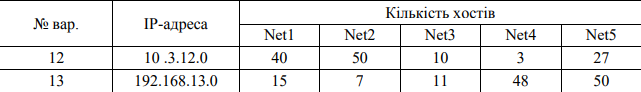


Рисунок 3.1 Вихідні дані для адресації хостів мережі центрального офісу

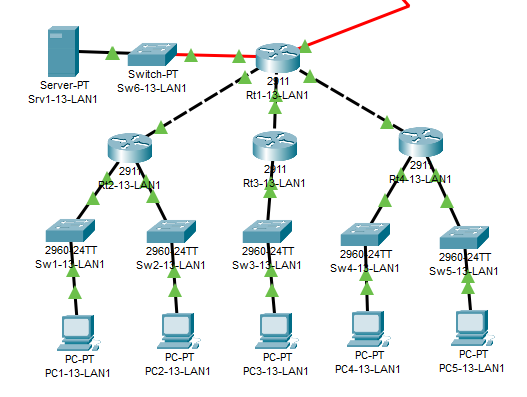


Рисунок 3.2 Топологія LAN1

Відповідно до кількості комп’ютерів в кожному підрозділі потрібно було вибрати маски підмереж, зробити розрахунок адрес підмереж та адрес хостів. Маски мали бути вибрані оптимальними. Також, визначити, скільки адрес в кожній підмережі залишились вільними. Нарисувати кругову діаграму «рис. 3.3», позначивши на ній всі сегменти адрес, які було виділено. Визначити, скільки ще підмереж і якого обсягу залишились незадіяними «табл. 3.1».

Таблиця 3.1

Таблиця адрес першої мережі

|  |  |  |  |
| --- | --- | --- | --- |
| № Net | Адреса мережі | Адреси хостів | Широкомовна адреса |
| 1 | 192.198.13.0/28 | 192.168.13.1-14 | 192.168.13.15 |
| 2 | 192.168.13.16/28 | 192.168.13.17-30 | 192.168.13.31 |
| 3 | 192.168.13.32/28 | 192.168.13.33-44 | 192.168.13.45 |
| 4 | 192.168.13.64/26 | 192.168.13.65-126 | 192.168.13.127 |
| 5 | 192.168.13.128/26 | 192.168.13.129-190 | 192.168.13.191 |
| 6 | 192.168.13.192/30 | 192.168.13.193-194 | 192.168.13.195 |
| 7 | 192.168.13.196/30 | 192.168.13.197-198 | 192.168.13.199 |
| 8 | 192.168.13.200/30 | 192.168.13.201-202 | 192.168.13.203 |
| 9 | 192.168.13.204/30 | 192.168.13.205-206 | 192.168.13.207 |

На маршрутизаторах Rt2-Rt4 налаштувати DHCP-сервіс і забезпечити динамічне призначення адрес хостам в мережах Net1-Net5 «рис. 3.4», «рис. 3.5», «рис. 3.6». Налаштувати статичну маршрутизацію таким чином, щоб кількість записів в таблиці маршрутизації кожного маршрутизатора була мінімальною «рис. 3.7». Налаштувати 3 стандартні та 2 розширені списки керування доступом (ACL), які будуть забороняти проходження трафіку відповідно до «рис. 3.8». ACL мають бути розташовані в найоптимальнішому місці. Типи протоколів для розширених ACL наведено в «рис. 3.9».

Рисунок 3.3 Виділена кількість хостів у LAN1

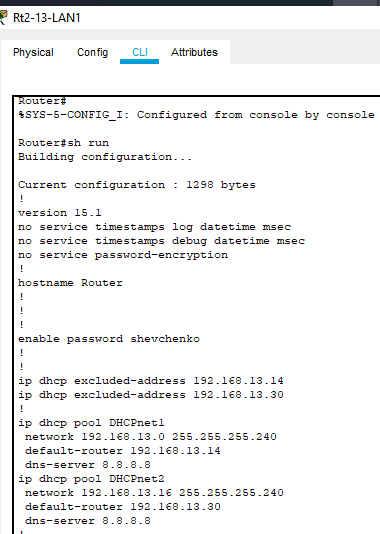


Рисунок 3.4 Налаштований DHCP-сервіс на другому роутері

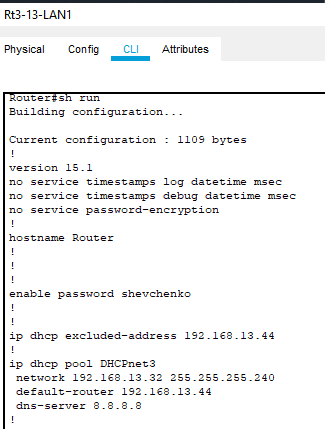


Рисунок 3.5 Налаштований DHCP-сервіс на третьому роутері

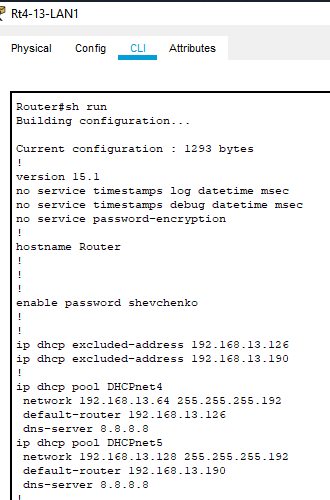


Рисунок 3.6 Налаштований DHCP-сервіс на четвертому роутері

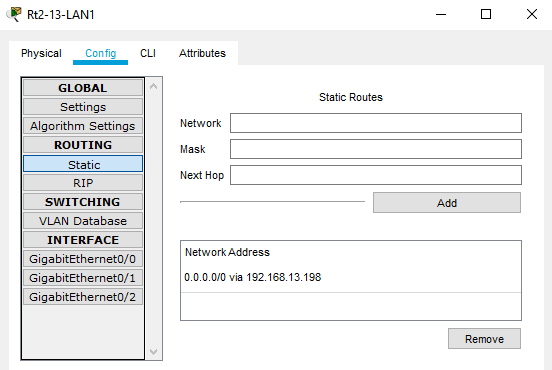


Рисунок 3.7 Налаштована статична маршрутизація на другому роутері

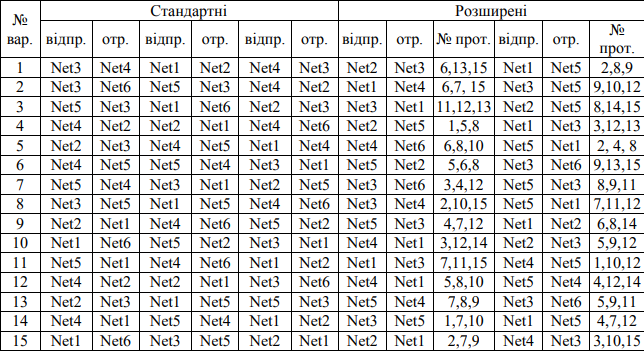


Рисунок 3.8 Вихідні дані для налаштування списків доступу (варіант 13)

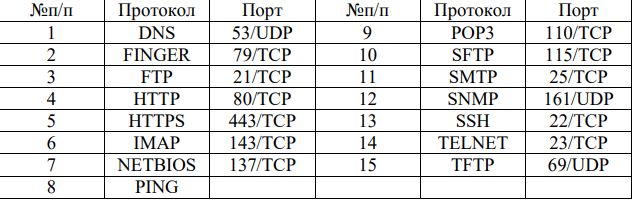


Рисунок 3.9 Перелік протоколів для налаштування ACL (варіант 13)

## Моделювання мережі LAN 2

Необхідно було створити мережу відповідно номеру варіанту «рис. 3.10», враховуючи тип з’єднання між маршрутизаторами. На «рис. 3.11» вказано тільки послідовні (Serial) з’єднання та відповідні протоколи, всі інші — FastEthernet. Потрібно було розподілити адресний простір таким чином: в мережах, що з’єднують маршрутизатори, використовувався префікс 30 (маска 255.255.255.252), весь вільний простір, що залишався, рівномірно поділений між мережами, в яких розташовані Switch1-Switch5 «табл. 3.2».

Табл. 3.2

Таблиця адрес другої мережі

|  |  |  |  |
| --- | --- | --- | --- |
| № Net | Адреса мережі | Адреси хостів | Широкомовна адреса |
| 1 | 10.4.13.0/30 | 10.4.13.1-2 | 10.4.13.3 |
| 2 | 10.4.13.4/30 | 10.4.13.5-6 | 10.4.13.7 |
| 3 | 10.4.13.8/30 | 10.4.13.9-10 | 10.4.13.11 |
|  | 10.4.13.12/30 | 10.4.13.13-14 | 10.4.13.15 |
|  | 10.4.13.16/30 | 10.4.13.17-18 | 10.4.13.19 |
|  | 10.4.13.32/27 | 10.4.13.33-62 | 10.4.13.63 |
|  | 10.4.13.64/27 | 10.4.13.65-94 | 10.4.13.95 |
|  | 10.4.13.96/27 | 10.4.13.97-126 | 10.4.13.127 |
|  | 10.4.13.128/27 | 10.4.13.129-158 | 10.4.13.159 |
|  | 10.4.13.160/27 | 10.4.13.161-190 | 10.4.13.191 |

Також налаштувати маршрутизацію відповідно до номера варіанту «рис. 3.12».

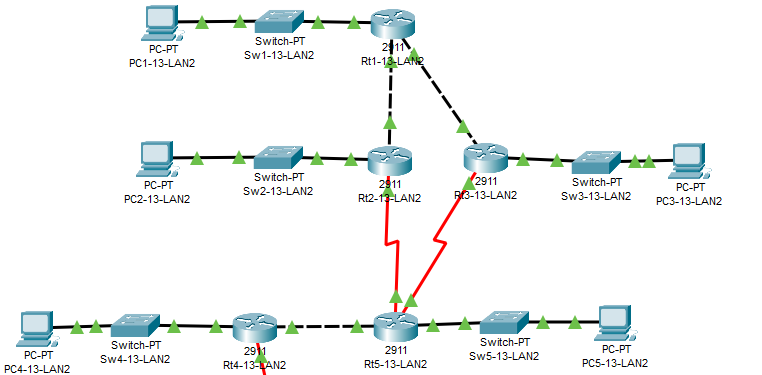


Рисунок 3.10 Топологія LAN2

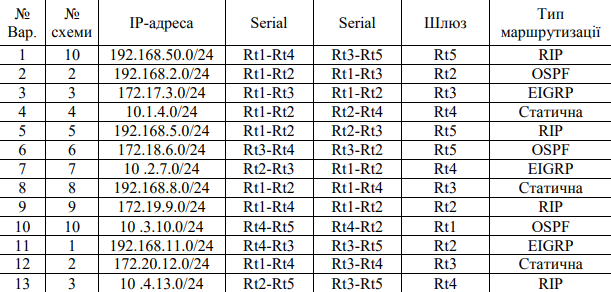


Рисунок 3.11 Вихідні дані для налаштування мережі віддаленого офісу (варіант 13)

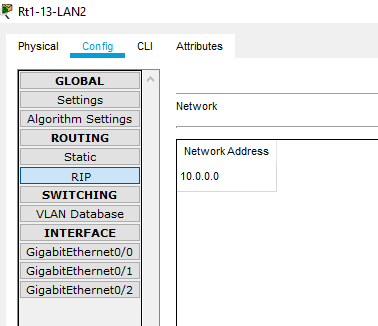


Рисунок 3.12 Налаштована маршрутизація RIP на одному з роутерів

## Проектування мережі датацентру LAN3

Необхідно було побудувати мережу датацентру «рис. 3.13». Створити на кожному комутаторі VLAN1, VLAN2 та VLAN3. Увести до VLAN1, VLAN2 та VLAN3 порти відповідно номеру варіанту «рис. 3.14». Srv1 і Srv2 під’єднати до портів, що входять до VLAN1, Srv3 і Srv4 під’єднати до портів, що входять до VLAN2, Srv5 і Srv6 під’єднати до портів, що входять до VLAN3. Призначити IP-адреси VLAN1 кожного комутатора, вибравши для цього перші доступні адреси мережі Net1 «рис. 3.15». Призначити ІР адреси серверам таким чином, щоб всі хости, що підключені до портів VLAN1, VLAN2 та VLAN3 знаходились, відповідно, в мережах Net1, Net2 та Net3.

Створити три під інтерфейси на фізичному інтерфейсі маршрутизатора R1 який підключений до комутатора SW1 «рис. 3.16». Налаштувати статичну маршрутизацію з урахування, що R1 буде мати запис про маршрут за замовченням та підключений до глобальної мережі.

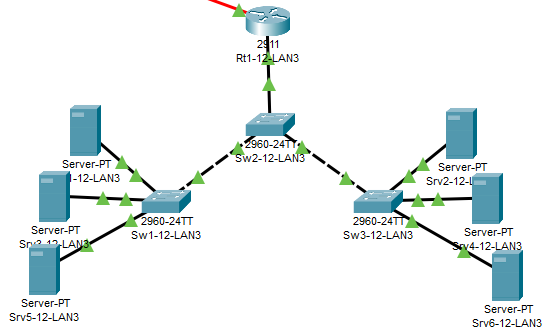


Рисунок 3.13 Топологія дата центру

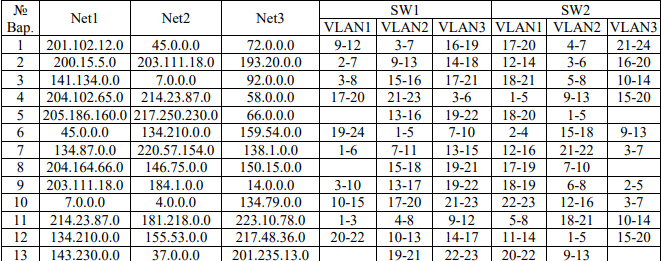


Рисунок 3.14 Вихідні дані для проектування мережі дата центру (використовувався варіант №12)

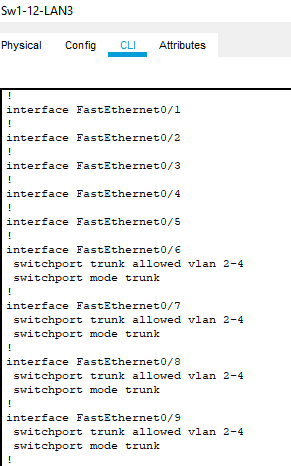


Рисунок 3.15 Налаштовані порти комутатора відповідно до віртуальних мереж

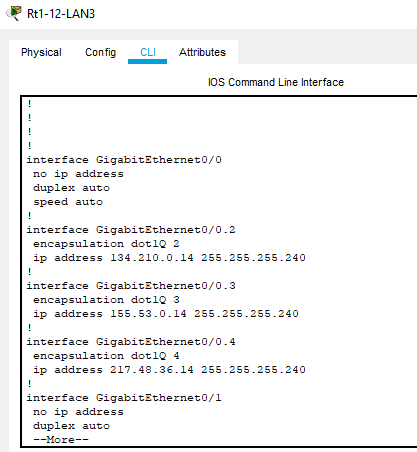


Рисунок 3.16 Налаштовані під інтерфейси на першому роутері

## Загальні налаштування активного обладнання та об’єднання локальних мереж

Згідно настанов, усі елементи були проіменовані за таким принципом: X-Y-Z, де Х - назва пристрою на рисунку, Y - № варіанту, Z - назва мережі (LAN1, LAN2 або LAN 3). Були встановлені на всіх маршрутизаторах паролі на консольне з’єднання та на привілейований режим. Налаштовано доступ через протокол SSH до шлюзових маршрутизаторів.

Об’єднання локальних мереж LAN1-LAN3 здійснювалося через шлюзові маршрутизатори, відповідні послідовні інтерфейси яких підключалися до комутатора Frame Relay «рис. 3.17». Функцію шлюзового маршрутизатора в мережах LAN1 та LAN3 виконує Rt1, а в мережі LAN2 визначається номером варіанту «рис. 3.18». Адреса та топологія мережі Frame Relay наведена «рис. 3.19». На шлюзових маршрутизаторах мереж LAN1 і LAN2 налаштувати трансляцію адрес NAT, причому для сервера Srv1 в мережі LAN1 має бути налаштований статичний NAT, а для решти комп’ютерів - трансляція з перекриттям (РАТ). Для комп’ютерів РС1-РС5 мережі LAN2 налаштувати динамічний NAT.

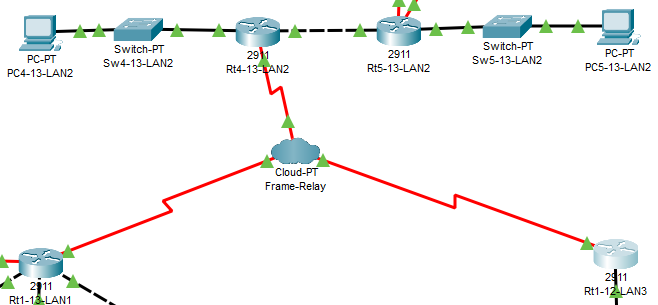


Рисунок 3.17 Топологія глобальної мережі

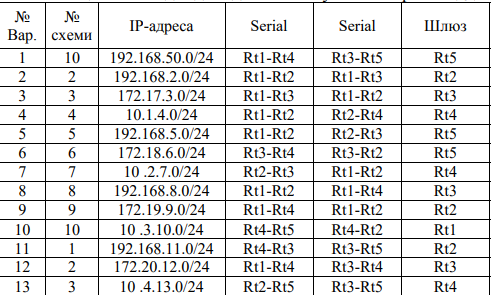


Рисунок 3.18 Таблиця вихідних даних зі вказанням шлюзового маршрутизатора (варіант 13)

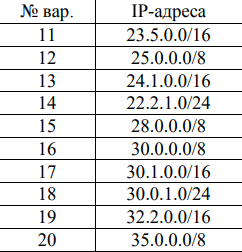


Рис. 3.19 Вихідні для об’єднання локальних мереж (варіант 13)

## Тестування

У цьому розділі буде наведена відправка пакетів у мережах, та між ними. Результати продемонстровані у вигляді фото екрану з програми Cisco Packet Tracer.

### Відправка пакетів у LAN1

Зроблена відправка пакетів у першій локальній мережі у реальному часі. Результати продемонстровані на «рис. 3.20», «рис. 3.21».

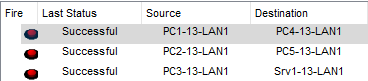


Рисунок 3.20 Відправка пакетів у LAN1

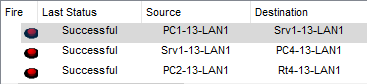


Рисунок 3.21 Відправка пакетів у LAN1

### Відправка пакетів у LAN2

Зроблена відправка пакетів у другій локальній мережі у реальному часі. Результати продемонстровані на «рис. 3.22», «рис. 3.23».

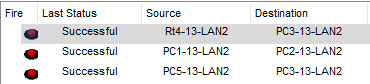


Рисунок 3.22 Відправка пакетів у LAN2

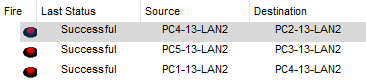


Рисунок 3.23 Відправка пакетів у LAN2

### Відправка пакетів у LAN3

Зроблена відправка пакетів у третій локальній мережі у реальному часі. Результати продемонстровані на «рис.3.24».

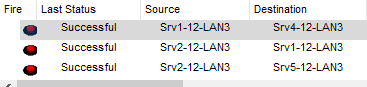


Рисунок 3.24 Відправка пакетів у LAN3

### Відправка пакетів між мережами

Зроблена відправка пакетів між трьома мережами у реальному часі. Результати продемонстровані на «рис.3.25», «рис.3.26».

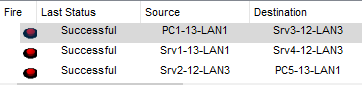


Рисунок 3.25 Відправка пакетів між LAN

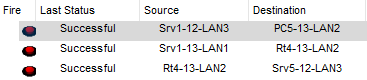


Рисунок 3.26 Відправка пакетів між LAN

# ВИСНОВКИ

Метою курсової роботи було отримання практичних навичок моделювання та розрахунку параметрів комп’ютерних мереж (КМ) та аналіз їх функціонування у сучасному середовищі; навичок адміністрування та конфігурування КМ, організації доступу до мережі Internet та заходів захисту інформації. У процессі виконання проекту були удосконалені навички налаштування, як:

* + 1. Налаштування маршрутизаторів
    2. Налаштування комутаторів
    3. Проектування локальної та глобальної мережі
    4. Налаштування протоколів динамічної маршрутизації
    5. Створення під інтерфейсів

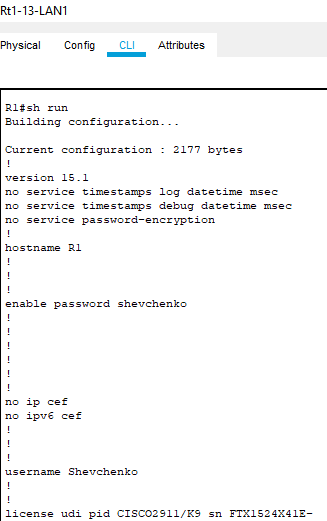
Завдяки багатоетапній авторизації, безпека доступу до маршрутизаторів є досить високою. На роутерах було налаштовано 3 етапи авторизації: консольний доступ, доступ до привілейованого режиму, доступ до маршрутизатора через віддалений доступ.

Усі вимоги були виконані послідовно за допомогою методичних вказівок, наданих науковим керівником, завдяки чому, мета курсового проекту була досягнена і завдання було виконано.

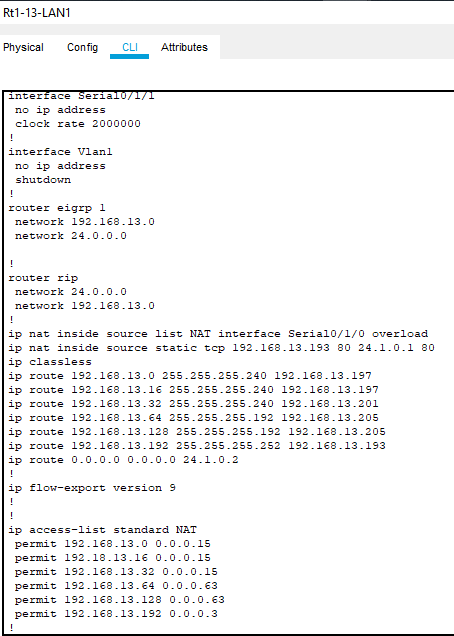
# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

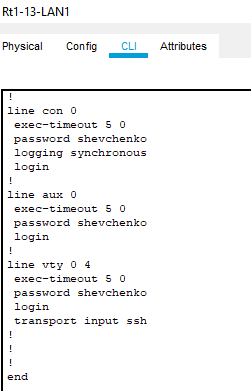
* + 1. Локальні і глобальні комп'ютерні мережі, мережеві технології обробки інформації [Електронний ресурс] – Режим доступу до ресурсу: <https://stud.com.ua/43313/informatika/lokalni_globalni_kompyuterni_merezhi_merezhevi_tehnologiyi_obrobki_informatsiyi>.
    2. Класифікація комп’ютерних мереж [Електронний ресурс] – Режим доступу до ресурсу: <https://comp-net.at.ua/index/klasifikacija_komp_juternikh_merezh/0-4>.
    3. Компьютерные сети [Електронний ресурс] – Режим доступу до ресурсу: <https://www.polnaja-jenciklopedija.ru/nauka-i-tehnika/kompyuternye-seti.html>.
    4. Распределение адресного пространства [Електронний ресурс] – Режим доступу до ресурсу: <https://studbooks.net/2277981/informatika/raspredelenie_adresnogo_prostranstva>.
    5. Динамічна маршрутизація [Електронний ресурс] – Режим доступу до ресурсу: <https://helpiks.org/4-70742.html>.
    6. Проектування комп’ютерної мережі [Електронний ресурс] – Режим доступу до ресурсу: <https://revolution.allbest.ru/programming/00246961_0.html>.
    7. UBS\_CyberNetSecurity\_2020 [Електронний ресурс] – Режим доступу до ресурсу: <https://1391723.netacad.com/courses/1078565>.
    8. Networks\_R&S\_2020 [Електронний ресурс] – Режим доступу до ресурсу: https://539765719.netacad.com/courses/973734.
    9. Основні функції та класифікація маршрутизаторів [Електронний ресурс] – Режим доступу до ресурсу: <https://lektsii.com/1-35899.html>.
    10. Шаблон базовой настройки маршрутизатора Cisco [Електронний ресурс] – Режим доступу до ресурсу: <https://habr.com/ru/post/87680/>.
    11. Налаштування Cisco 2960 [Електронний ресурс] / web-city – Режим доступу до ресурсу: <http://web-city.org.ua/nalashtuvannya-cisco-2960-vstanovlyuyemo-komutator/>.
    12. Налаштування початкової конфігурації комутатора [Електронний ресурс] – Режим доступу до ресурсу: <https://works.doklad.ru/view/_mtcwI-K2Xo.html>.
    13. Комутатор Cisco 2960: налаштування підключення, конфігурації, установка [Електронний ресурс] – Режим доступу до ресурсу: <https://hi-news.pp.ua/kompyuteri/16660-komutator-cisco-2960-nalashtuvannya-pdklyuchennya-konfguracyi-ustanovka.html>.

# ДОДАТОК А конфігураця шлюзового маршрутизатора мережі LAN1

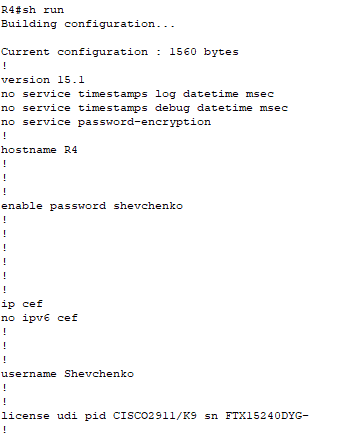


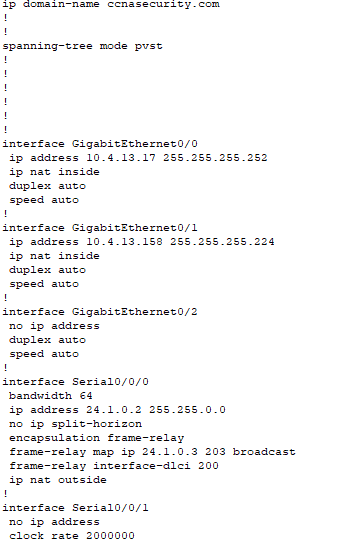


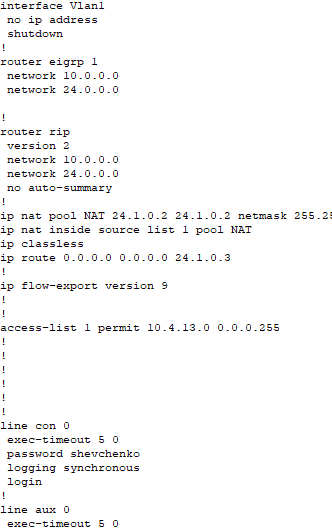


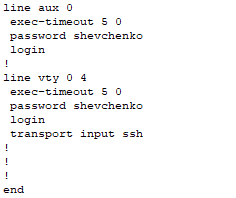


# ДОДАТОК Б Конфігурація шлюзового маршрутищатора мережі LAN2

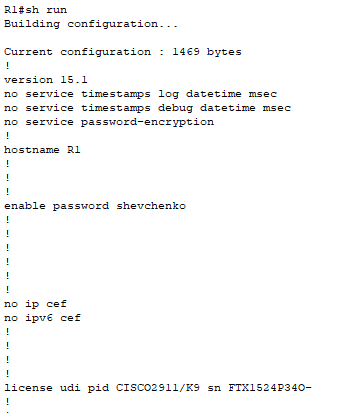


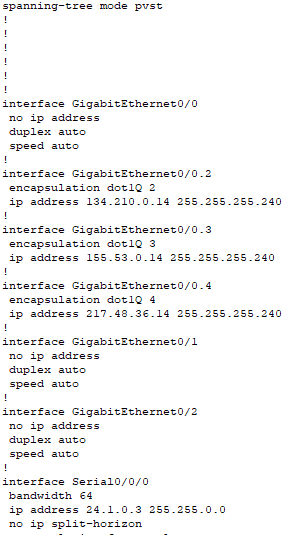


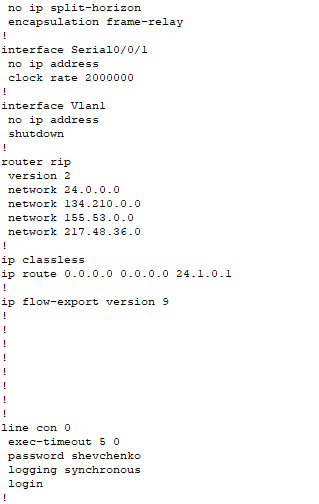


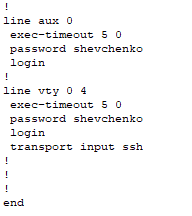


# ДОДАТОК В Конфігурація шлюзового маршрутизатора мережі LAN3









# ДОДАТОК Г Повна топологія побудованої мережі

