**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-Кб групи

спеціальності «Кібербезпека»

Собчук Анни Вікторівни

(прізвище та ініціали)

Керівник:

к.е.н., доц,

Гордєєва Дар’я Валеріївна.

(посада, вчене звання, науковий ступінь,

прізвище та ініціали)

Національна шкала \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кількість балів: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Оцінка: ECTS \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члени комісії

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

(підпис) (прізвище та ініціали)

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

(підпис) (прізвище та ініціали)

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

(підпис) (прізвище та ініціали)

м. Київ – 2020 рік

**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:

3.1. мета - отримання практичних навичок проектування та конфігурування комп’ютерних мереж;

3.2. 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

5.1. Мережа складається з трьох окремих LAN, що об’єднуються WAN мережею, побудованою на основі технології віртуальних каналів.

5.2. Вимоги для проектування LAN1

5.2.1. Адреса мережі 192.168.10.0

5.2.2. Складається з п’яти сегментів, кількість робочих станцій в кожному з яких становить: 12, 10, 58, 25, 5.

5.2.3. Розподіл адресного простору має бути оптимальним;

5.2.4. Для об’єднання окремих сегментів використовуються 4 маршрутизатори;

5.2.5. З’єднання між маршрутизаторами здійснюються за допомогою скрученої пари;

5.2.6. Для обмеження проходження трафіку з одного сегменту в інший мають бути застосовані стандартні і розширені ACL. Стандартні списки мають заборонити проходження трафіку з мереж NET1 NET6 та NET5 відповідно до мереж NET2 NET3 та NET1. Розширені ACL мають заборонити проходження трафіку протоколів DNS, FINGER та FTP з NET4 до NET1 та HTTP HTTPS та ICMP з NET2 до NET3. ACL необхідно розмістити в найбільш вдалому місці.

5.2.7. У середині мережі використовується статична маршрутизація.

5.2.8. На маршрутизаторах Rt4-Rt5 налаштувати DHCP-сервіс і забезпечити динамічне призначення адрес хостам в мережах Net1-Net5.

5.2.9. На маршрутизаторі Rt1 налаштовано сервіс трансляції адрес NAT.

5.3. Вимоги для проектування LAN2

5.3.1. Адреса мережі 10.3.10.0/24

5.3.2. Складається з 5 сегментів, в яких розташовані ПК користувачів.

5.3.3. 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.

5.3.4. З’єднання між маршрутизаторами Rt4-Rt5 та Rt4-Rt2 здійснюється за допомогою послідовних інтерфейсів з використанням протоколів канального рівня HDLC та РРР відповідно. Інші з’єднання виконуються за допомогою скрученої пари.

5.3.5. Під’єднання мережі LAN2 до мережі WAN виконується через маршрутизатор Rt1.

5.3.6. В середині мережі використовується динамічна маршрутизація на основі протоколу OSPF.

5.3.7. На маршрутизаторі Rt1 налаштовано сервіс трансляції адрес NAT.

5.4. Вимоги для проектування LAN3

5.4.1. Реалізована на основі комутаторів Catalyst 2960 з підтримкою технології віртуальних мереж.

5.4.2. Поділена на три віртуальні сегменти, кожний з яких містить по два сервери.

5.4.3. На комутаторах Sw1 Sw3 до Vlan 2 належать порти FastEtherne17-FastEthernet20 та FastEthernet12-FastEthernet16 відповідно, до Vlan 3 FastEthernet21-FastEthernet23 та FastEthernet3-FastEthernet7 відповідно.

5.4.4. З’єднання між комутаторами здійснюються за допомогою скрученої пари і технології Gigabit Ethernet.

5.4.5. В віртуальних мережах VLAN1, VLAN2 та VLAN3 використовуються адреси 7.0.0.0 4.0.0.0 та 134.79.0.0 відповідно.

5.5. Вимоги для проектування WAN

5.5.1. Об’єднання локальних мереж здійснюється за допомогою Frame Relay комутатора з використанням топології Full Mesh.

5.5.2. Адреси інтерфейсів маршрутизаторів, що під’єднані до Frame Relay мережі, належать до мережі з адресою 18.0.0.0/8

5.5.3. З’єднання між локальними мережами здійснюється за допомогою послідовних інтерфейсів.

5.6. Загальні вимоги до налаштувань маршрутизаторів

5.6.1. Встановити на всіх маршрутизаторах паролі на консольне з’єднання та на привілейований режим.

5.6.2. Налаштувати доступ через протокол SSH до шлюзових маршрутизаторів.

6. Апаратні вимоги - використання обладнання фірми Cisco

7. Текстова документація розробленої мережі повинна відповідати діючим стандартам України.

8. 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 Собчук Анна Вікторівна

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**

**БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ ТА СОЦІАЛЬНИХ НАУК**

Спецiальність: «Кібербезпека»

Курс 3 Група 303-Кб Семестр 5

Дисципліна Комп’ютерні системи та мережі (Рівень D - Безпека комп`ютерних систем)

**ЗАВДАННЯ**

**на курсову роботу студента/студентки**

Собчук Анни Вікторівни

(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 |
| 192.168.10.0 | | | 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

**ЗМІСТ**

[АНОТАЦІЯ 7](#_Toc58968649)

[ВСТУП 8](#_Toc58968650)

[РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОЇ ЧАСТИНИ 10](#_Toc58968651)

[1.1 Аналіз сучасних технологій локальних та глобальних мереж 10](#_Toc58968652)

[1.1.1 Види топологій 13](#_Toc58968653)

[1.1.2 Мережеві кабелі 14](#_Toc58968654)

[1.2 Розрахунок адресного простору 16](#_Toc58968655)

[1.3 Вибір та налаштування способу маршрутизації 20](#_Toc58968656)

[РОЗДІЛ 2. Конфігурування мережевого обладнання 22](#_Toc58968657)

[2.1 Конфігурування базових функцій маршрутизаторів 22](#_Toc58968658)

[2.2 Проектування віртуальних мереж 25](#_Toc58968659)

[2.3 Конфігурування базових функцій комутаторів LAN 28](#_Toc58968660)

[2.4 Конфігурування додаткових функцій маршрутизаторів 30](#_Toc58968661)

[РОЗДІЛ 3. Налаштування віддаленого доступу та безпеки на активному обладнанні 36](#_Toc58968662)

[3.1 Налаштування захисту та конфігурування функцій безпеки 36](#_Toc58968663)

[3.2 Налаштування віддаленого доступу до активного обладнання 38](#_Toc58968664)

[3.3 Моделювання та тестування роботи розробленої мережі 41](#_Toc58968665)

[ВИСНОВКИ 46](#_Toc58968666)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 47](#_Toc58968667)

[ДОДАТОК А 48](#_Toc58968668)

[ДОДАТОК Б 50](#_Toc58968669)

# АНОТАЦІЯ

Курсова робота призначена для закріплення, розширення, узагальнення і практичного використання знань, умінь і навичок, одержаних під час навчання. Метою є 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.

Завдання до курсової роботи передбачає розробку структурної схеми комп’ютерної мережі, згідно варіанту, встановлення Ір-адрес мережевих інтерфейсів, налагодження серверів; планування дозволу імен, з’єднання окремих частин мережі за допомогою маршрутизаторів, моделювання потоків трафіку в мережі, розрахунок подвоєної затримки розповсюдження сигналу (PDV), формулювання висновків відносно працездатності та захисту комп’ютерної мережі.

Також описано повний процес налаштування, а саме:

* аналіз сучасних технологій локальних та глобальних мереж;
* розрахунок адресного простору;
* вибір та налаштування способу маршрутизації;
* конфігурування базових функцій маршрутизаторів;
* проектування віртуальних мереж;
* конфігурування базових функцій комутаторів LAN;
* конфігурування додаткових функцій маршрутизаторів (DHCP, NAT тощо);
* налаштування захисту та конфігурування функцій безпеки (налаштування паролів, Port security, ACL тощо);
* налаштування віддаленого доступу до активного обладнання;
* моделювання та тестування роботи розробленої мережі;

# ВСТУП

Сучасні умови розвитку інформаційних технологій диктують необхідність їх прискореного застосування, як найбільш оперативного засобу контролю, управління та обміну даними, як всередині окремого підрозділу, так і в масштабах великого підприємства.

Завдяки виникненню та розвитку мереж передачі даних з'явився новий, високоефективний спосіб взаємодії між людьми. Спочатку мережі використовувались для наукових дослідів, але згодом вони почали проникати у всі області людської діяльності.

Основним призначенням комп'ютерних мереж є спільне використання ресурсів і встановлення зв'язку як всередині одного підрозділу чи організації, так і за її межами. Під ресурсами слід розуміти програми, дані, додатки, периферійні пристрої. [1]

**Створенню локальних мереж і глобальної єдиної мережі комп'ютерів надають таке ж значення, що й будівництву швидкісних автомагістралей у шістдесяті роки XX ст. Тому комп'ютерну мережу називають «інформаційною супермагістраллю». Підкреслюючи вигоду, що принесе застосування мереж усім користувачам, фахівці говорять про інформацію «на кінчиках пальців».**

**Комп'ютерна мережа -- це сукупність комп'ютерів і різних пристроїв, що забезпечують інформаційний обмін між комп'ютерами в мережі без використання яких-небудь проміжних носіїв інформації.**

Актуальність курсового проекту полягає у тому, що комп'ютерні мережі і мережеві технології обробки інформації стали основою для побудови сучасних інформаційних систем. Корпоративні мережі передавання даних охоплюють, як правило, всі підрозділи окремої організації, які можуть бути розташованими на великій території. До їх складу можуть входити декілька як локальних (LAN), так і глобальних (WAN) мереж. Вони можуть використовувати складне комунікаційне обладнання і багатофункціональну апаратуру передавання даних, різноманітні лінії зв'язку - телефонні канали, радіо і супутниковий зв'язок.

**Все різноманіття комп'ютерних мереж можна класифікувати по групі ознак:**

* **Територіальна поширеність;**
* **Відомча приналежність;**
* **Швидкість передачі інформації;**
* **Тип середовища передачі;**

**По територіальній поширеності мережі можуть бути локальними, глобальними, і регіональними. Локальні - це мережі, що перекривають територію не більше 10 м2, регіональні - розташовані на території міста чи області, глобальні на території держави або групи держав, наприклад, всесвітня мережа Internet.**

# ****РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОЇ ЧАСТИНИ****

## Аналіз сучасних технологій локальних та глобальних мереж

**Комп’ютерна мережа — це сукупність комп’ютерів та інших пристроїв, сполучених каналами передавання даних.**

**Комп’ютерні мережі забезпечують спільний доступ до даних. У мережі виділяють комп’ютери, на яких розміщують великі масиви даних, а користувачі інших комп’ютерів мережі одержують доступ до них. Це дає можливість людям, котрі працюють над одним проектом, використовувати дані, створені іншими, тобто працювати над проектом одночасно.**

**За допомогою комп’ютерної мережі стає можливим також спільне користування периферійними пристроями: принтерами, сканерами, модемами тощо. Невигідно мати їх біля кожного персонального комп’ютера, наприклад, у комп’ютерному класі або у банку.**

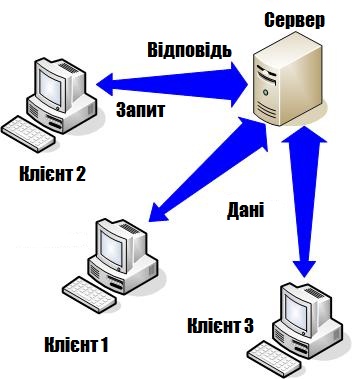
**Основне призначення всіх комп’ютерних мереж — це спільний доступ до мережних ресурсів (апаратного забезпечення комп’ютерів, периферійних пристроїв), спільне використання даних і швидкий обмін ними, спільне використання програмного забезпечення.**

**Мережна взаємодія передбачає віддалений доступ до мережних ресурсів за певною технологією.**

**Залежно від повноважень комп’ютери мережі розподіляють на сервери й клієнтів. (рис. 1.1)**

**Клієнт — це комп’ютер користувача, який здійснює запит.**

**Сервер — комп’ютер, що обробляє цей запит і відповідає на нього.**



**Рисунок 1.1 – схема призначення ролей у мережі.**

**Локальна комп'ютерна мережа – це система, що дозволяє проводити обмін інформацією між пристроями, підключеними до системи. Локальна комп'ютерна мережа включає до себе спеціалізоване програмне забезпечення та апаратну частину, необхідну для підключення пристроїв до комп'ютерних каналам, які взаємодіють між собою, та знаходяться на відстані один від одного, в одному приміщенні, будівлі, в різних місцях однієї організації або в регіоні. Можливості мережі дозволяють обмінюватися даними та забезпечувати широкий доступ до можливостей центрального комп'ютеру. Функції комп'ютерної мережі Базова комунікативна модель складається з: джерела (персональний комп'ютер); приймача (сервер); сполучення між ними (кабель або телефонна лінія). Основні функції локальної мережі: надання користувачам загального доступу до папок, файлів та інших ресурсів; спільне використання файлів; обмеження, при бажанні доступу до спільних папок та каталогів; настройка прав доступу; архівація потрібної інформації та зберігання даних на файловому сервері; можливість надійно зашифровувати свої дані на файловому сервері, що дає високий рівень захисту від зовнішніх атак [4]**

**Протягом останнього десятиліття дедалі ширший розвиток отримують глобальні обчислювальні й інформаційні мережі – унікальний симбіоз комп'ютерів і комунікацій. Відбувається активне приєднання всіх країн до всесвітніх мережних структур. Світовою системою комп'ютерних комунікацій щодня користуються більш як 30 млн. людей. Зростає потреба в засобах структурування, накопичення, збереження, пошуку і передачі інформації. Задоволенню цих потреб служать інформаційні мережі та їхні ресурси. Спільне використання ресурсів мереж (бібліотек програм, баз даних, обчислювальних потужностей) забезпечується технологічним комплексом і засобами доступу.**

**Глобальні мережі (Wide Area Network, WAN) – 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.**

**Основою функціонування Internet є базовий протокол TCP/IP (Transmission Control Protocol/Internet Protocol). 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. .[3]**

## 1.1.1 Види топологій

Існує безліч способів з'єднання мережевих пристроїв. Виділяють 3 базових топології:

* шина (bus)
* зірка (star)
* кільце (ring)

І додаткові (похідні):

* подвійне кільце
* сотова топологія
* решітка
* дерево
* Fat Tree
* сніжинка
* повнозв'язна

Додаткові способи є комбінаціями базових. У загальному випадку такі топології називаються змішаними або гібридними, але деякі з них мають власні назви, наприклад «Дерево». (рис.1.2)

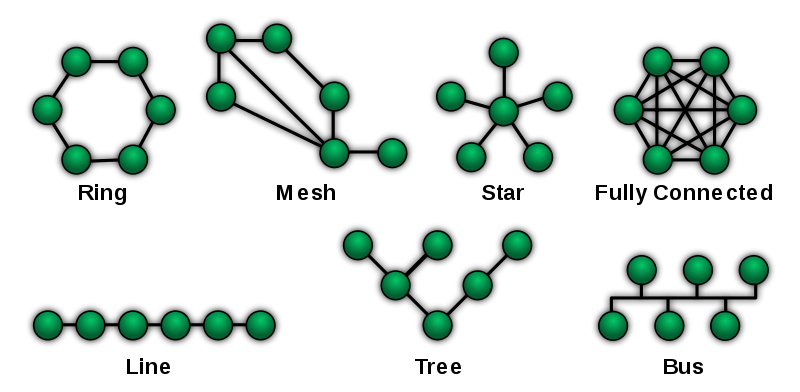


Рисунок1.2 – види топологій

## 1.1.2 Мережеві кабелі

Мережеві кабелі використовуються для підключення одного мережного пристрою до інших пристроїв мережі або для з'єднання двох або більше комп'ютерів, для мережевого користування принтером, сканером і т. д. Різні типи мережевих кабелів, як звита пара, оптоволоконний кабель, коаксіальний кабель, використовуються в залежності від топології, протоколів і розміру мережі. Пристрої можуть бути розділені відстанню від кількох метрів (наприклад, через Ethernet) або майже необмеженою відстанню (наприклад, через Інтернет).

На практиці в більшості мереж застосовуються тільки три основні групи кабелів:

* вита пара (twisted pair):
* неекранована (unshielded);
* екранована (shielded);
* оптоволоконний кабель(fiber optic)
* коаксіальний кабель (coaxial cable)

Вита пара

Це два перевитих навколо один одного ізольовані мідні дроти. Існує два типи витої пари:

* неекранована (unshielded) вита пара (UTP)
* екранована (shielded) вита пара (STP).

Декілька витих пар проводів часто поміщають в одну захисну оболонку. Їх кількість в такому кабелі може бути різною. Завивка проводів дозволяє позбавитися електричних перешкод, що наводяться сусідньою парою і іншими зовнішніми джерелами, наприклад двигунами, реле і трансформаторами.

Оптоволоконний кабель

У оптоволоконному кабелі цифрові дані розповсюджуються оптичними волокнами у вигляді модульованих світлових імпульсів. Це відносно захищений спосіб передачі, оскільки при ньому не використовуються електричні сигнали. Отже, до оптоволоконного кабелю неможливо підключитися, не руйнуючи його, і перехоплювати дані, від чого не застрахований будь-який кабель, що проводить електричні сигнали. Оптоволоконні лінії призначені для передачі великих обсягів даних на дуже високих швидкостях, оскільки сигнал в них практично не затухає і не спотворюється.

Коаксіальний кабель

Не так давно найпоширенішим типом вважався коаксіальний кабель. Це пояснювалося двома причинами. По-перше, він був відносно недорогим, гнучким і зручним в застосуванні, а по-друге, надійним і простим в установці. Найпростіший коаксіальний кабель складається з мідної жили (core), ізоляції що її оточує, екрану у вигляді металевого обплетення і зовнішньої оболонки. Якщо кабель, окрім металевого обплетення, має і шар фольги, він називається кабелем з подвійною екранізацією. За наявності сильних перешкод можна скористатися кабелем з чотирьохразовою екранізацією. Він складається з подвійного шару фольги і подвійного шару металевого обплетення.

Існує два типи коаксіальних кабелів: тонкий (thinnet) коаксіальний кабель та товстий (thicknet) коаксіальний кабель. Вибір того або іншого типу кабелю залежить від потреб конкретної мережі.

## Розрахунок адресного простору

IP-адреса (Internet Protocol Address) - це унікальний мережевий ідентифікатор, який присвоюється кожному учаснику локальної або глобальної комп'ютерної мережі. Це може бути як Всесвітня павутина, так і приватна мережа підприємства. Головне - вона повинна бути заснована на протоколі TCP / IP.

Незалежно від типу мережі, айпі-адреси в її межах не повинні повторюватися. Завдяки можливості привласнення унікального ідентифікатора кожному користувачеві з'являється можливість розмежування дій. Система вміє розпізнавати користувачів, отже, кожному з них можна давати той чи інший рівень доступу, відстежити дії або зовсім заблокувати.

32-бітний IP-адреса має такий вигляд: 192.180.0.255

Він складається з чотирьох числових значень від 0 до 255, між якими ставлять крапку.

Мінус даного формату - малий охоплення. З ростом популярності інтернету зросла і кількість унікальних вузлів (користувачів). Унікальні IP-адреси просто закінчувалися. Тому в 1996 році був створений IPv6.

Всі IP-адреси класифікуються за кількома критеріями.

За способом використання:

* зовнішні - використовуються в глобальних мережах. Саме цей тип айпі-адрес дозволяє власникам сайтів відстежувати статистику відвідувань, визначати характеристики відвідувачів, виконувати аналітику;
* внутрішні - використовуються всередині локальної (приватної)

мережі. Така адреса не можна застосовувати в глобальних системах. Відстежити його можуть тільки учасники цієї ж мережі.

Через обмеженість кількості зовнішніх IP-адрес часто застосовують технологію NAT (Network Address Translation), яка перетворює внутрішні ідентифікатори в зовнішні.

За способом визначення:

* статичні (постійні). Кожному вузлу привласнюється свій ідентифікатор на необмежений час. Один адреса використовується тільки на одному пристрої. Відстежити такого користувача легко;
* динамічні (непостійні). Ідентифікатори присвоюються на обмежений час - від початку до кінця сесії. Один адреса може використовуватися необмежену кількість разів різними пристроями. При завершенні сесії айпі стає вільним і може бути присвоєний іншому вузлу. Відстеження користувачів з динамічними IP-адресами важко. Для цього необхідний спеціальний інструмент.[2]

**Адресний простір** — це просто набір адрес, які уміє формувати процесор; зовсім не обов'язково всі ці адреси відповідають реально існуючим елементам пам'яті. Залежно від модифікації персонального комп'ютера і складу його периферійного устаткування, розподіл адресного простору може декілька розрізнятися [28]

**У варіанті було надано таку IP-адресу 192.168.10.0 та кількість хостів. для Net1 – Net5 відповідно 12, 10, 58, 25, 5.**

**Розрахунок відбувався так:**

**для початку визначила яка маска буде оптимальною для кожного Net. Для цього потрібно було знайти до кожної кількості хостів найближче значення, яке може бути окремою підмережою (табл. 1.1)**

**Таблиця 1.1**

**Підбір значень**

|  |  |  |
| --- | --- | --- |
| **№ Net** | **Кількість хостів** | **Найближче число** |
| **1** | **12** | **16** |
| **2** | **10** | **16** |
| **3** | **58** | **64** |
| **4** | **25** | **32** |
| **5** | **5** | **8** |

**Наступним кроком було переведення підібраних чисел у двійкову систему, але не обійшлось без нюансів. А саме, в результаті переведення мало вийти 8-значне число з 0 та 1. Якщо ж цифр не вистачало – попереду усього двійкового значення додавалось стільки одиниць, скільки не вистачало (табл 1.2)**

**Таблиця 1.2**

**Переведення у двійкову систему**

|  |  |  |
| --- | --- | --- |
| **№ Net** | **Значення** | **У двійковій системі** |
| **1** | **16** | **11110000** |
| **2** | **16** | **11110000** |
| **3** | **64** | **11000000** |
| **4** | **32** | **11100000** |
| **5** | **8** | **11111000** |

**Наступним кроком було переведення отриманих чисел у десяткову систему. Результат наведено у таблиці 1.3**

**Таблиця 1.3**

**Переведення у десяткову систему**

|  |  |  |
| --- | --- | --- |
| **№ Net** | **Значення** | **У двійковій системі** |
| **1** | **11110000** | **240** |
| **2** | **11110000** | **240** |
| **3** | **11000000** | **192** |
| **4** | **11100000** | **224** |
| **5** | **11111000** | **248** |

**Але для коректної роботи підмережі було недостатньо 5 Net тому розрахунки були ще для Net6-Net9.**

**Далі у відповідності до маски підмережі було розраховано самі адреси для кожного Net. Для цього починали з 0 і додавали числа-1, які було знайдені до відповідних кількостей хостів, та перевірені за допомогою споміжних засобів. (Додаток А, табл.1.4)**

**За таким самим принципом відбувався в подальшому розрахунок адресного простору для Lan2(Додаток А, табл.1.5) та Lan3 (табл. 1.6.).**

**Таблиця 1.6**

**Розрахунок адресного простору для Lan3**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **Net** | **Адреса мережі** | **Адреса хостів мережі** | Broadcast **адреса** |
| **1** | **7.0.0.0/28** | **7.0.0.1 - 7.0.0.14** | **7.0.0.15** |
| **2** | **4.0.0.0/28** | **4.0.0.1 - 4.0.0.14** | **4.0.0.15** |
| **3** | **134.79.0.0/28** | **134.79.0.1 - 134.79.0.14** | **134.79.0.15** |

## **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.**

**Маршрутизація (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.**

**Основні вимоги до сучасних протоколів маршрутизації. Під час розробки протоколів маршрутизації необхідно задовольнити ряду важливих, але іноді суперечливих вимог:**

* **Оптимальність, яка характеризує здатність протоколу забезпечувати вибір найкращого в рамках певних критеріїв шляху (множини шляхів), наприклад, шлях з мінімальною кількістю переприйомів або шлях, який має максимальну пропускну здатність.**
* **Простота апаратно-програмної реалізації та мінімальні обсяги створюваного службового трафіка при зборі даних про стан ТКС або розсиланні інформації управління.**
* **Стійкість, яка характеризує здатність протоколу забезпечувати ефективне розв’язання маршрутних задач в умовах непередбаченої зміни умов функціонування мережі, наприклад, при відмові мережного обладнання, сплеску абонентського навантаження та ін..**
* **Висока оперативність одержання остаточних маршрутних рішень, особливо в умовах реалізації розподіленої маршрутизації, пов’язаної із забезпеченням збіжності відповідних обчислювальних алгоритмів з розрахунку шуканих шляхів.**
* **Адаптивність, пов’язана зі здатністю протоколу постійно (періодично) відстежувати та своєчасно реагувати на поточні зміни топології мережі, параметрів мережних вузлів (розміри черг) і трактів передачі (пропускна здатність, затримки, втрати пакетів), а також характеристик абонентського навантаження.**
* **Масштабованість, яка характеризує здатність протоколу виконувати визначені функції із заданою якістю при збільшенні розмірності мережі (числа мережних вузлів, трактів передачі та ін.).**

# ****РОЗДІЛ 2. Конфігурування мережевого обладнання****

## 2.1 Конфігурування базових функцій маршрутизаторів

Підключення до маршрутизатора здійснюється через Telnet на IP-адресу будь-якого з його інтерфейсів або за допомогою будь термінальної програми через послідовний порт комп'ютера, пов'язаний з консольним портом маршрутизатора. Останній спосіб краще, тому що процес конфігурування маршрутизатора може змінювати параметри IP-інтерфейсів, що призведе до втрати з'єднання, встановленого через Telnet. Крім того, з міркувань безпеки доступ до маршрутизатора через Telnet слід заборонити.

При роботі в командному рядку Cisco IOS існує кілька контекстів (режимів введення команд). Контекст користувача відкривається при приєднанні до маршрутизатора; зазвичай при підключенні через мережу потрібно пароль, а при підключенні через консольний порт пароль не потрібен. У цей же контекст командний рядок автоматично переходить при тривалій відсутності введення в контексті адміністратора. У контексті користувача доступні тільки прості команди (деякі базові операції для моніторингу), що не що впливають на конфігурацію маршрутизатора. Вид запрошення командного рядка:

маршрутизатор>

Замість слова маршрутизатора виводиться ім'я маршрутизатора, якщо воно встановлено.

Контекст адміністратора (контекст "Exec") відкривається командою дозволу, поданої в контексті користувача, при цьому зазвичай потрібно пароль адміністратора. У контексті адміністратора доступні команди, що дозволяють отримати повну інформацію про конфігурації маршрутизатора і його стані, команди переходу в режим конфігурування, команди збереження та завантаження конфігурації. вид запрошення командного рядка:

Router #

Зворотний перехід в контекст користувача проводиться за командою відключення або по закінчення встановленого часу не активності. Завершення сеансу роботи – команда виходу.

Глобальний контекст конфігурування відкривається командою конфігурації терміналу ("Конфігурувати через термінал»), поданої в контексті адміністратора. Глобальний контекст конфігурування містить як безпосередньо команди конфігурування маршрутизатора, так і команди переходу в контексти конфігурування підсистем маршрутизатора.

Контекст конфігурування інтерфейсу відкривається командою інтерфейсу ім’я інтерфейсу (наприклад, інтерфейс serial0), поданої в глобальному контексті конфігурування;

Контекст конфігурування процесу динамічної маршрутизації відкривається командою маршрутизатора протокол номер процесу (наприклад, маршрутизатора OSPF 1, поданої в глобальному контексті конфігурації). Існує безліч інших контекстів конфігурування. деякі контексти конфігурування знаходяться всередині інших контекстів конфігурування.

Вид запрошення командного рядка в контекстах конфігурування, які будуть зустрічатися найчастіше:

router(config)# / глобальний /

outer(config-if)# / інтерфейсу /

rounter(config-router)# / динамічної маршрутизації /

rounter(config-line)# / термінальної лінії /

Користувачі повинні запам'ятати вид запрошень командою рядка у всіх вищевказаних контекстах і правила переходу з контексту в контекст. Надалі приклади команд завжди будуть даватися разом із запрошеннями, з яких студенти повинні визначати контекст, в якому подається команда. Приклади не міститимуть вказівок, як потрапити в необхідний контекст.

Вихід з глобального контексту конфігурування в контекст адміністратора, а також вихід з будь-якого під контексту конфігурування в контекст верхнього рівня виробляється командою виходу або Ctrl-Z. Крім того, команда кінця, подана в будь-якому з контекстів конфігурування негайно завершує процес конфігурування і повертає оператора в контекст адміністратора.

Всі команди і параметри можуть бути скорочені (наприклад "enable" - "en", "configure terminal" - "conf t"); якщо скорочення виявиться неоднозначним, маршрутизатор повідомить про це, а після натискання табуляції видасть варіанти, відповідні введеному фрагменту.

У будь-якому місці командного рядка для отримання допомоги може бути використаний знак питання:

Router #? / Список всіх команд даного контексту з коментарями /

Router # Co? / Список всіх слів у цьому контексті введення, що починаються на "Со" /

Router # Conf? / Список всіх параметрів, які можуть слідувати за командою Config /

## 2.2 Проектування віртуальних мереж

Віртуальною локальною мережею VLAN (Virtual Local Area Network) будемо називати логічну групу вузлів мережі, кадри яких, у тому числі й широкомовні, на канальному рівні повністю ізольовані від інших вузлів мережі, що не входять до даної групи. Із цього випливає, що передача кадрів між різними VLAN на підставі MАС-адреси неможлива незалежно від типу адреси (одиночної, групової або широкомовної). У той же час усередині VLAN кадри передаються відповідно до технології канального рівня. Тому така логічна сегментація дозволяє логічну структуру мережі Ethernet зробити незалежною від її фізичної структури. Треба також відмітити, що вузли, які належать до однієї логічної групи можуть бути фізично приєднані до різних комутаторів. Таким чином, застосування VLAN призводить до обмеження розповсюдження широкомовних кадрів, а також кадрів, які розсилає комутатор по всіх своїх портах у випадку відсутності МАС-адреси отримувача кадру в його МАС-таблиці, тільки в межах однієї VLAN. Це в свою чергу дає можливість зменшити частку широкомовних кадрів у мережі й імовірність виникнення широкомовних штормів, що можуть суттєво погіршити характеристики продуктивності мережі. Застосування VLAN забезпечує можливість гнучкого розділення користувачів на ізольовані групи, тобто кінцеві вузли користувачів (наприклад, персональні комп’ютери) будуть ізольовані один від одного на канальному рівні. Також VLAN дозволяє покращити характеристики безпеки мережі за рахунок обмеження області розповсюдження кадрів другого рівня і реалізації необхідної політики взаємодії користувачів з різних VLAN за допомогою обладнання комутації третього рівня. Крім того, VLAN надає можливість спрямування за необхідними трактами передачі у випадку, якщо їх декілька, кадрів другого рівня, що дозволяє встановити необхідний розподіл потоків кадрів у певному сегменті мережі.

Передача інформації між користувачами з різних віртуальних мереж можлива тільки через мережевий рівень (на канальному рівні віртуальні мережі повністю незалежні). Для цього один з портів, що належить кожній VLAN, приєднується до окремого порту маршрутизатора, який забезпечує пересилання IP-пакетів між користувачами, що перебувають у різних віртуальних мережах. При цьому слід зазначити, що IP-адреси користувачів з різних віртуальних мереж повинні знаходиться у різних IP-мережах (підмережах), тобто префікси IP-мереж мають відрізнятися (це необхідно для того, щоб порти маршрутизатора перебували в різних IP-мережах).

При проектуванні мережі будемо дотримуватися ієрархічної моделі мережі, яка має багато переваг в порівнянні з «плоскою мережею»: − спрощується розуміння організації мережі; − модель має на увазі модульність, що означає простоту нарощування потужностей саме там, де необхідно; − легше знайти і ізолювати проблему; − підвищена відмовостійкість за рахунок дублювання пристроїв і / або сполук; − розподіл функцій щодо забезпечення працездатності мережі по різним пристроях.

Модульний маршрутизатор Cisco 2811 призначений для невеликих офісів, що підтримує до 36 мережних закінчень. Відрізняється гнучкою модульною конструкцією. Пристрої оснащені слотами для установки мережевих модулів (NME), для встановлення інтерфейсних модулів (HWIC), для підтримки додаткових голосових інтерфейсів (EVM), а також Спеціальний слотами на системній платі маршрутизатора для установки модулів обробки голосу і сервісних модулів (PVDM і AIM). Інтерфейси NME і HWIC мають зворотну сумісність з модулями NM і WIC відповідно.

Комутатори Cisco Catalyst 2960 Series пропонують комплекс функцій, в число яких входять: − підтримка передачі даних, голосу і бездротового зв'язку, завдяки чому можна встановити єдину мережу, яка обслуговує всі потреби в зв'язку; − можливість харчування комутатора через Ethernet дозволяє легко розгортати нові функції, наприклад голосовий і бездротовий зв'язок, без необхідності повторної прокладки кабелів; − вибір між Fast Ethernet (швидкість передачі даних 100 мегабіт в секунду) і Gigabit Ethernet (швидкість передачі даних тисяча мегабіт в секунду) залежить від фінансових можливостей і потреби в продуктивності; − безліч конфігурацій моделі з можливістю підключення настільних комп'ютерів, серверів, IP-телефонів, точок бездротового доступу, камер для замкнутої телевізійної системи та інших мережевих пристроїв; − можливість налаштовувати віртуальні локальні мережі, завдяки чому співробітники об'єднуються з організаційних функцій, проектним групам або додатків, а не на фізичній або географічної основі; − інтегрований захист і можливості контролю мережі і розширеної діагностики проблем підключень; − безкоштовні оновлення програмного забезпечення комутатора і обмежена довічна гарантія на обладнання.

## 2.3 Конфігурування базових функцій комутаторів LAN

Залежно від площі охоплюваної території загалом розрізняють два типи мереж — локальні та глобальні. Локальні мережі (LAN) забезпечують обмін даними в межах однієї будівлі або невеликої території. Глобальні мережі (WAN) використовують для з’єднання локальних мереж та передавання даних на значні відстані — у межах регіону, країни чи навіть світу. Локальна мережа — це група комп’ютерів та інших допоміжних пристроїв, які спільно використовують проводові або безпровідні канали зв’язку в межах невеликої території (наприклад, у межах будівлі). Локальна мережа дає змогу персональним комп’ютерам обмінюватися даними і здійснювати доступ до спільно використовуваних серверів і принтерів. Таке спільне використання даних та апаратних і програмних ресурсів сприяє скороченню витрат і збільшенню продуктивності праці.

Щоб налаштувати IP-адресу для інтерфейсу VLAN комутатора необхідно виконати наступні команди interface vlan 1 і ip address в CLI.

S1 # conf t // переходимо в режим глобальної конфігурації

S1 (config) # interface vlan 1 // переходимо в режим конфігурації інтерфейсу

S1 (config-if) # ip address 192.168.1.253 255.255.255.0 // присвоюємо інтерфейсу ip-адреса і маску мережі

S1 (config-if) # no shutdown // включаємо інтерфейс

S1 (config-if) # ex // виходимо з режиму глобальної конфігурації

S1 #[6]

Налаштування SSH і Telnet для локального входу і рівня привілеїв 15.

Router(config)# line vty 0 4

Router(config-line)# privilege level 15

Router(config-line)# login local

Router(config-line)# transport input telnet

Router(config-line)# transport input telnet ssh

Router(config-line)# exit

Налаштування ACL

ACL (Access Control List) - це набір текстових виразів, які щось дозволяють, або щось забороняють. Зазвичай ACL дозволяє або забороняє IP-пакети, але крім усього іншого він може заглядати всередину IP-пакета, переглядати тип пакету, TCP і UDP порти

Функціонал ACL складається в класифікації трафіку, потрібно його перевірити спочатку, а потім щось з ним зробити в залежності від того, куди ACL застосовується. ACL застосовується скрізь, наприклад:

* На інтерфейсі: пакетна фільтрація
* На лінії Telnet: обмеження доступу до маршрутизатора
* VPN: який трафік потрібно шифрувати
* QoS: який трафік обробляти у пріоритеті
* NAT: які адреси транслювати

ACL поділяються на два типи:

* Стандартні (Standard): можуть перевіряти тільки адреси джерел
* Розширені (Extended): можуть перевіряти адреси джерел, а також адреси отримувачів, в разі IP ще тип протоколу і TCP / UDP порти

Стандартний список доступу

Router (config) # access-list <номер списку від 1 до 99> {permit | deny | remark} {address | any | host} [source-wildcard] [log]

* permit: дозволити
* deny: заборонити
* remark: коментар про список доступу
* address: забороняємо або дозволяємо мережу
* any: дозволяємо або забороняємо все
* host: дозволяємо або забороняємо хосту
* source-wildcard: WildCard маска мережі
* log: включаємо логування пакети проходять через даний запис ACL[7]

## 2.4 Конфігурування додаткових функцій маршрутизаторів

Загалом, СЕРВЕР – це комплексне рішення, яке поглинає основні функції:

HTTP - дозволяє створювати примітивні веб-сторінки і перевіряти проходження пакетів до 80-го порту сервера.

DHCP - дозволяє організувати пули параметрів мережі для автоматичного налаштування мережевих інтерфейсів.

TFTP - це простий протокол передачі файлів, який підходить для обладнання CISCO та прошивки.

DNS - дозволяє організувати примітивну службу роздільної здатності доменних імен.

SYSLOG - дозволяє організувати збір повідомлень, відправлених різними пристроями на сервер журналу подій, будь то відключення електроенергії, збій безпеки і т.д.

AAA - це сервер авторизації;

NTP - це сервер синхронізації часу;

EMAIL - це поштовий сервер для перевірки основних правил електронної пошти;

FTP - це файловий сервер, корисна річ для налагодження різних ALS і завантаження прошивки;

OSPF([англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *Open Shortest Path First*) — протокол динамічної [маршрутизації](https://uk.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%8F), заснований на технології відстеження стану каналу (link-state technology), що використовує для знаходження найкоротшого шляху [Алгоритм Дейкстри](https://uk.wikipedia.org/wiki/%D0%90%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC_%D0%94%D0%B5%D0%B9%D0%BA%D1%81%D1%82%D1%80%D0%B8) (Dijkstra's algorithm).

Налаштування OSPF

Запустимо процес ospf:

R1(config)# router ospf 1

Останнє число - це PID процесу, може відрізнятися на різних маршрутизаторах, але виключно для зручності краще ставити одне і теж число. Тепер відключимо відправку hello пакетів на всіх інтерфейсах. З міркувань безпеки ми будемо явно задавати інтерфейси, на яких будуть встановлюватися neighbour відносини.

R1(config-router)#passive-interface default

Тепер зазначимо інтерфейси, на яких ми будемо відправляти hello пакети. Для R1 це fa0 / 0:

R1(config-router)#no passive-interface fa0/0

За допомогою команди network ми можемо зробити 2 речі - повідомити, які мережі ми хочемо анонсувати по OSPF іншим маршрутизаторам і на яких інтерфейсах ми будемо відправляти hello пакети. Саме тому раніше ми вказали конкретні інтерфейси для hello пакетів. Наприклад, на маршрутизаторі R1 нам потрібні 3 мережі: 10.5.0.0/30, 10.5.0.4/30 і 172.16.0.0/26. Але в останній мережі будуть виключно призначені для користувача пристрої і нам би зовсім не хотілося, щоб хтось мав можливість з неї впливати на таблиці маршрутизації роутерів. Формат команди network:

network 0.0.0.0 255.255.255.255 area 0

Першим параметром йде номер мережі, другим - wildcart маска і останнім номер зони.[5]

Розширений список доступу

Router (config) # access-list <номер списку від 100 до 199> {permit | deny | remark}

protocol source [source-wildcard] [operator operand] [port <порт або назва протоколу> [established]

* protocol source: який протокол будемо дозволяти або закривати (ICMP, TCP, UDP, IP, OSPF і т.д)
* deny: заборонити
* operator:

A.B.C.D - адреса одержувача

any - будь-який кінцевий хост

eq - тільки пакети на цьому порте

gt - тільки пакети з великим номером порту

host - єдиний кінцевий хост

lt - тільки пакети з нижчим номером порту

neq - тільки пакети не на даному номері порту

range - діапазон портів

* port: номер порту (TCP або UDP), можна вказати ім'я
* established: дозволяємо проходження TCP-сегментів, які є частиною вже створеної TCP-сесії

Прикріплюємо до інтерфейсу

Router (config-if) #ip access-group <номер списку або ім'я ACL> {in | out}

* in: вхідний напрямок
* out вихідний напрямок[20]

Налаштування статичного NAT (Static Network Address Translation)

Статичний NAT - зіставляє єдиний внутрішній локальний (приватний) ip-адреса з єдиним глобальним (публічним) ip-адресою.

1. Створення статичного маршруту на стороні ISP.

R2 (config) # ip route 200.20.21.1 255.255.255.224 200.20.20.1

1. . Налаштування дефолту на R1.

R1 (config) # ip route 0.0.0.0 0.0.0.0 200.20.20.2

1. Налаштування внутрішнього інтерфейсу в відношення NAT.

R1 (config) # interface fastethernet 0/0

R1 (config-if) # ip nat inside

1. Налаштування зовнішнього інтерфейсу в відношення NAT.

R1 (config) # interface fastethernet 0/1

R1 (config-if) # ip nat outside

1. Налаштування зіставлення ip-адрес.

R1 (config) # ip nat inside source static 10.10.10.2 200.10.21.5

В результаті ip-адресою 200.10.21.5 завжди буде відповідати внутрішній ip-адреса 10.10.10.2, тобто якщо ми будемо звертатися до адресою 200.10.21.5 то відповідати буде computer 1

Налаштування PAT (NAPT, NAT Overload)

PAT (Port Address Translation) - відображає кілька локальних (приватних) ip-адрес в глобальний ip-адреса, скориставшись різними портами.

1. Налаштування списку доступу відповідного внутрішнім приватним адресами, зверніть увагу що використовується зворотна маска.

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

1. Налаштування трансляції.

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

1. Налаштування внутрішнього інтерфейсу в відношення NAT.

R1 (config) # interface fastethernet 0/0

R1 (config-if) # ip nat inside

1. Настройка зовнішнього інтерфейсу в відношення NAT.

R1 (config) # interface fastethernet 0/1

R1 (config-if) # ip nat outside

Команди для перевірки роботи NAT

show ip nat translations - Виводить активні перетворення.

show ip nat statistics - виводить статистику по NAT перетворенням.

Налаштування Frame Relay

Frame Relay - WAN-протокол, що працює на другому рівні моделі OSI, тобто, там же, де працюють Ethernet, PPP, HDLC і ін.

DLCI - це «Data Link Connection Identifier», ідентифікатор з'єднання.

Налаштування без сабінтерфейсів

Нехай провайдер нам повідомив номера DLCI:

R1 - R2 - 102

R2 - R1 - 201

R1 - R3 - 103

R3 - R1 – 301

R2 - R3 - 203

R3 - R2 - 302

IP адреси маршрутизаторів:

R1 – 18.0.0.1

R2 - 18.0.0.2

R3 - 18.0.0.3

Налаштування Frame Relay

R1#

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#interface serial0/0/0

R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R1(config-if)#encapsulation frame-relay

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

R1(config-if)#ip address 18.0.0.1 255.255.255.0

R1(config-if)#bandwidth 64

R1(config-if)#frame-relay map ip 18.0.0.2 102 broadcast

R1(config-if)#frame-relay map ip 18.0.0.3 103 broadcast

Налаштування DHCP.

Протокол DHCP дозволяє автоматично налаштувати мережу на комп'ютерах та інших пристроях. DHCP може бути налаштований на маршрутизатори Cisco або на основі будь-якого сервера. У цій статті описано, настроювання DHCP-сервера на маршрутизаторі Cisco.

Настроювання маршрутизатора, який буде видавати мережу 192.168.1.0/24 в мережі DHCP, починаючи з 192.168.1.11.

R1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#ip dhcp excluded-address 192.168.1.1 192.168

Ми просимо маршрутизатор не видавати адреси з 192.168.1.1 до 192.168.1.10. Оскільки перша адреса буде використовуватися сам маршрутизатор (шлюз), а інші дев'ять має сенс зарезервувати для різних серверів в цій мережі. Сервери не повинні видавати адреси на DHCP - з ними часто зв'язаються, тому адресу слід вводити статично і ніколи не змінювати. У нашому прикладі, наприклад, є DNS-сервер з адресою 192.168.1.5, який забитий статичним. Тепер створюємо пул:

R1(config)#ip dhcp pool MY-POOL

R1(dhcp-config)#network 192.168.1.0 255.255.255.0

R1(dhcp-config)#default-router 192.168.1.1

R1(dhcp-config)#domain-name my-domain.com

R1(dhcp-config)#dns-server 192.168.1.5

R1(dhcp-config)#exit

Адреси будуть видаватися з мережі 192.168.1.0/24 (за винятком тих, які ми виключили раніше), як шлюз ми видамо 192.168.1.1 - наш маршрутизатор. Дану адресу потрібно налаштувати:

R1(config)#interface fa0/0

R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

R1(config-if)#exit

R1(config)#exit

R1#

%SYS-5-CONFIG\_I: Configured from console by console

Отримавши адресу комп'ютера, можна перевірити список виданих адрес:

R1#show ip dhcp binding [9]

# РОЗДІЛ 3. Налаштування віддаленого доступу та безпеки на активному обладнанні

## 3.1 Налаштування захисту та конфігурування функцій безпеки

Встановлення паролю на маршрутизатор

R1(config)#line console 0//Входимо в режим налаштування консолі.

R1(config-line)#password cisco//Назначаємо пароль на вхід.

R1(config-line)#login//Включаем запит паролю перед входом в консоль.

R1(config-line)#exit

R1(config)#line vty 0 4//Входимо в режим налаштування телнета.

R1(config-line)#password cisco//Назначаємо пароль на вхід.

R1(config-line)#login//Включаємо запит паролю перед входом за допомогою телнета.

R1(config-line)#end

R1#show running-config//Перевіряємо введенні дані.[8]

Шифрування паролю

Вводимо sh run і бачимо, що пароль зашифрований, тепер він був оброблений спеціальною функцією і вийшов у вигляді коду літерного типу.

R2(config)#service password-encryption

Налаштування рівня привілеїв

Cisco має лише 16 рівнів привілеїв - нумерації від 0 до 15. Рівень 1 є користувачем за замовчуванням, рівень "15" є найвищим привілейованим (права на повний доступ).

Privileged EXEC — є привілейованим режимом; Ми переміщуємося в нього з режиму User EXEC за допомогою команди enable; має найвищий рівень привілеїв , відповідно, і повний контроль над пристроєм.

Global configuration — є глобальним режимом конфігурації; ми переміщуємося в нього з привілейованого режиму EXEC за допомогою команди налаштувати термінал.

Далі від режиму глобальної конфігурації ми можемо перейти в режим налаштування інтерфейсу, лінії, vlan і т.д.

Режими CISCO CLI є, як бачимо, ієрархічними: для того, щоб підняти 100-мегабітний порт #17, потрібно пройти через ланцюжок Login -> (User EXEC) -> enable -> (Privileged Exec) -> configure terminal -> (Global configuration) -> interface Fa0/17 -> (Interface configuration) -> no shutdown

R2 (config)#username admin secret 0 strongpass

R2 (config)#username admin privilege 3

## 3.2 Налаштування віддаленого доступу до активного обладнання

Налаштування SSH

1. cisco> enable
2. cisco# clock set 17:10:00 28 Aug 2009
3. cisco# configure terminal
4. cisco(config)# ip domain name test.dom
5. cisco(config)# crypto key generate rs
6. cisco(config)# service password-encryption
7. cisco(config)# username user privilege 15 password 7 Pa$$w0rd
8. cisco(config)# aaa new-model
9. cisco(config)# line vty 0 4
10. cisco(config-line)# transport input ssh
11. cisco(config-line)# logging synchronous
12. cisco(config-line)# exec-timeout 60 0
13. cisco(config-line)# exit
14. cisco(config)# exit
15. cisco# copy running-config startup-config

Пояснення:

1. Ми вступаємо в привілейований режим
2. Встановіть точний час для створення ключа
3. Введіть режим конфігурації
4. Дайте доменне ім'я (необхідно для створення ключа)
5. Створити ключ RSA (вам потрібно буде вибрати розмір ключа)
6. Активуйте шифрування пароля у файлі конфігурації
7. Ми отримуємо користувача з ім'ям користувача, Pa $ $w-й пароль і 15-річний рівень привілеїв
8. Активуйте протокол AAA. (Перед активацією AAA має бути активовано принаймні одного користувача)
9. Введіть режим конфігурації термінальної лінії від 0 до 4
10. Наведення середовища доступу через мережу за замовчуванням SSH
11. Активуйте автоматичну лінію після того, як система реагує на зміни, внесені
12. Вкажіть час очікування перед автоматичним закриттям сеансу SSH за 60 хвилин
13. Вийшов з режиму конфігурації термінала
14. Вийти з режиму конфігурації
15. Збереження файлу конфігурації в енергонезалежній пам'яті

Перегляд активних сеансів SSH

Виконуємо таку команду, щоб перевірити кількість сеансів SSH, підключених до PIX і стан підключень:

pix#show ssh session

Налаштування Telnet

Щоб додати telnet доступ до консолі та встановити час очікування, виконайте команду telnet у режимі глобальної конфігурації. За промовчанням Telnet сеансів, які останні п'ять хвилин закриті пристроєм безпеки. Використовуйте жодну форму наступної команди, щоб заборонити Telnet отримати доступ до раніше вказаних IP-адрес.

telnet {{hostname | IP\_address mask interface\_name} | {IPv6\_address interface\_name} | {timeout number}}

no telnet {{hostname | IP\_address mask interface\_name} | {IPv6\_address interface\_name} | {timeout number}}

Команда telnet дає змогу вказати, які вузли мають доступ до консолі безпеки Telnet. Ви можете дозволити використовувати Telnet для підключення до пристрою безпеки на всіх інтерфейсах. Однак, цей пристрій захисту вимагає, щоб весь трафік Telnet до зовнішнього інтерфейсу був захищений IPsec. Щоб дозволити сеансу Telnet підключатися до зовнішнього інтерфейсу, налаштуйте протокол IPsec на зовнішньому інтерфейсі, щоб увімкнути IP-трафік, створений цим пристроєм безпеки, і дозволити Telnet на цьому зовнішньому інтерфейсі.

Якщо ви використовуєте IPsec, ви можете вказати назву небезпечного інтерфейсу, як правило, зовнішнього інтерфейсу. Як мінімум, ви можете використовувати команду crypto map для позначення назви інтерфейсу за допомогою команди telnet.

Виконайте команду пароля, щоб установити пароль для доступу Telnet до консолі. Типовим паролем є cisco. Виконайте команду ВООЗ, щоб дізнатися IP-адреси вузлів, які наразі мають доступ до консолі пристрою безпеки. Виконайте команду вбити , щоб зупинити сеанс консолі Active Telnet.

Ми працюємо telnet тайм-аут, щоб встановити максимальний час для сеансу консолі Telnet, щоб бути пролиті, після чого ви вийдіть із пристрою безпеки. Не можна використовувати команду telnet з командою часу очікування telnet.

У цьому прикладі показано зміну максимального періоду бездіяльності сеансу: IPsec може бути надана назва небезпечного інтерфейсу, як правило, зовнішнього інтерфейсу. Як мінімум, ви можете використовувати команду crypto map для позначення назви інтерфейсу за допомогою команди telnet.

Виконаємо команду telnet тайм-аут встановити максимальний час сеансу консолі Telnet не закінчується. Не можна використовувати команду telnet з командою часу очікування telnet.

У цьому прикладі показано зміну максимального періоду бездіяльності сеансу:

hostname(config)#telnet timeout 10

hostname(config)#show running-config telnet timeout

telnet timeout 10 minutes[27]

## 3.3 Моделювання та тестування роботи розробленої мережі

Моделювання мережі розпочиналось з розрахунку адресного простору, який описано у Розділі 1. Побудова розпочиналась з LAN1(рис.3.1).



Рисунок 3.1 – Структурна схема LAN1

Тестування проводилось двома способами. Перший – запуском пакетів за допомогою команди ping (рис.3.2). Другий – запуск пакетів у режимі симуляції (рис.3.3)

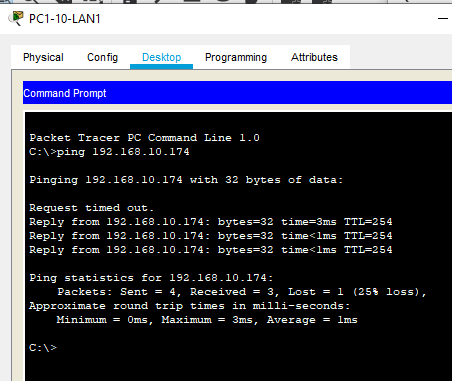


Рисунок 3.2 – Тестування командою ping

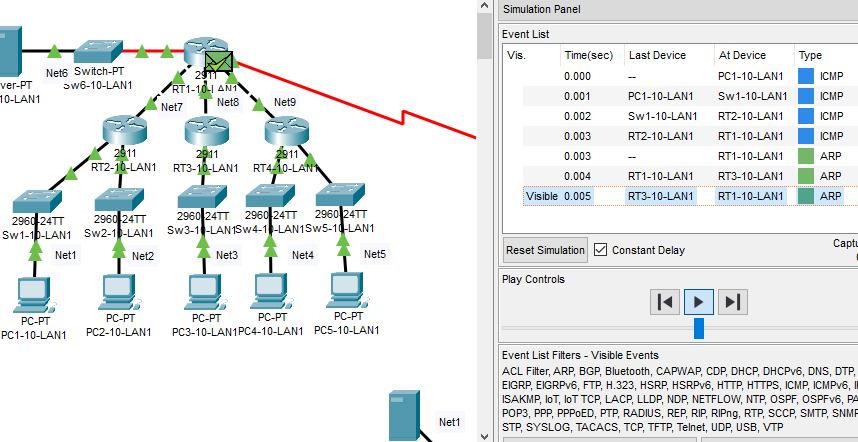


Рисунок 3.3 – Тестування у режимі симуляції

**Далі було налаштовано** DHCP-сервіс на маршрутизаторах Rt2-Rt4, а також статичну маршрутизацію таким чином, щоб кількість записів в таблиці маршрутизації кожного маршрутизатора була мінімальною (рис 3.4-3.7).

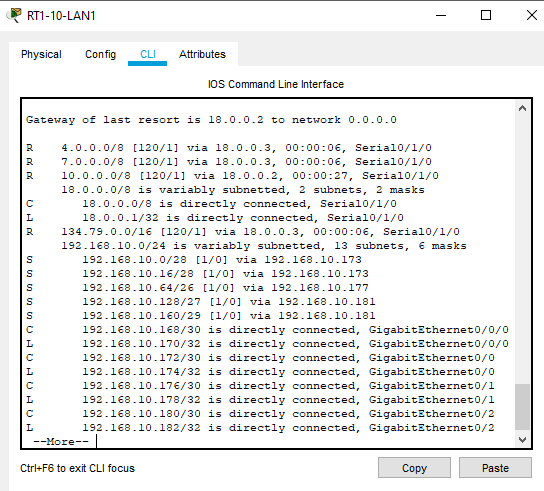


Рисунок 3.4 – таблиця маршрутизації Rt1

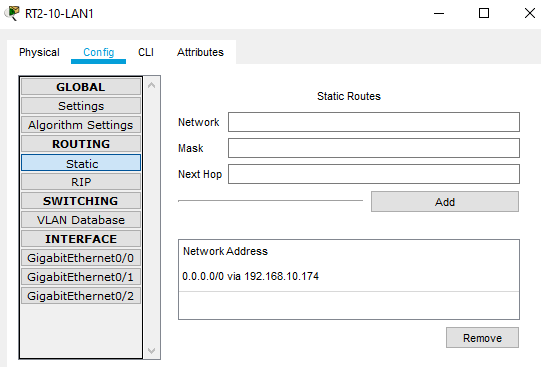


Рисунок 3.5 – таблиця маршрутизації Rt2

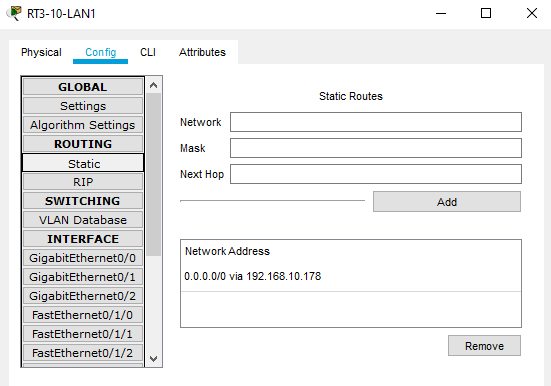


Рисунок 3.6 – таблиця маршрутизації Rt3

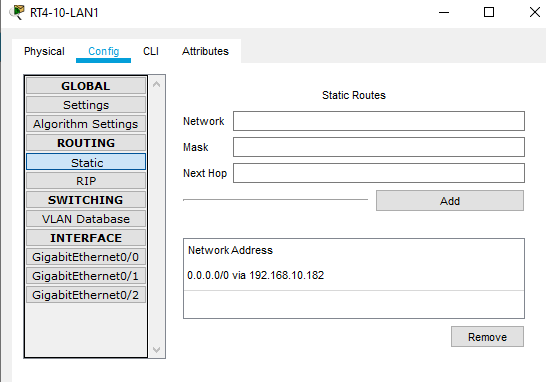


Рисунок 3.7 – таблиця маршрутизації Rt4

**Далі було налаштовано** 3 стандартні та 2 розширені списки керування доступом (ACL), згідно з завданням

Результат налаштування маршрутизаторів можна перевірити за допомогою команди sh run (Додаток Б)

Наступним завданням було проектування та налаштування LAN2(рис 3.12).

****

**Рисунок 3.12 – Структурна схема LAN2.**

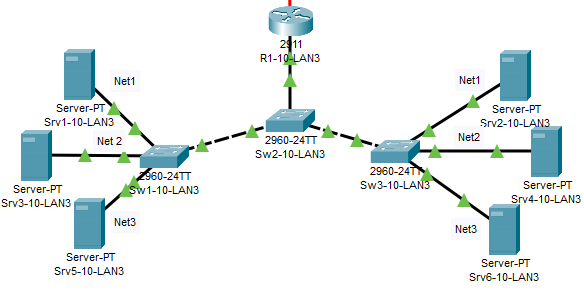
**Було надано наступні дані:**

* **ір-адресу мережі 10.3.10.0/24**
* **тип маршрутизації OSPF**
* **шлюзовий маршрутизатор Rt1**
* **маршрутизатори, що мають бути з’єднані Serial**

**За принципом розрахунку адресного простору для LAN1 розраховуємо для LAN2.**

**В останню чергу відбувалося проектування LAN3.**

**Згідно до опису та схеми (рис.3.13) було спроектовано мережу датацентру.**



**Рисунок 3.13 – Структурна схема LAN3**

**На даній мережі було налаштовано VLAN1-VLAN3 згідно з умовою завдання. ІР адреси призначались відповідно таблиці.**

**Наступними етапами було налаштування протоколу** HSRP та статичної маршрутизації.

Призначення імен всім пристроям за вимогами. Встановити на всіх маршрутизаторах паролі на консольне з’єднання та на привілейований режим.

Також налаштовано доступ через протокол SSH до шлюзових маршрутизаторів.

Заключним кроком є під’єднання та налаштування Frame Relay.

На шлюзових маршрутизаторах мереж LAN1 і LAN2 було налаштовано трансляцію адрес NAT. Для сервера Srv1 в мережі LAN1 - статичний NAT, а для решти комп’ютерів - трансляція з перекриттям (РАТ). Для комп’ютерів РС1-РС5 мережі LAN2 налаштувано динамічний NAT.

# ****ВИСНОВКИ****

За допомогою виконання даної роботи було отримано практичні навички моделювання та розрахунку параметрів комп’ютерних мереж та аналіз їх функціонування у сучасному середовищі; навички адміністрування та конфігурування комп’ютерної мережі, організації доступу до мережі Internet та заходів захисту інформації, навички проектування комп’ютерних мереж, налаштування мережного обладнання, розробка відмово стійких конфігурацій, моделювання роботи мережі в цілому та її окремих вузлів за допомогою сучасних симуляторів.

Було розроблено структурну схему комп’ютерної мережі(рис1), згідно варіанту, встановлено ІР-адреси мережевих інтерфейсів, налагоджено сервери.

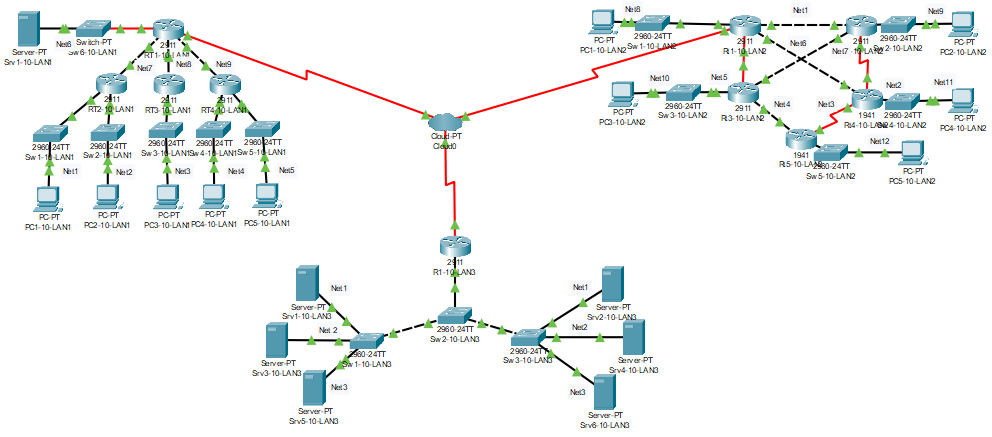


Рисунок 1 – Налаштована мережа

За результатами тестування можна зробити висновки, що мережа працює коректно

# ****СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ****

1. Проектування комп’ютерної мережі [Електронний ресурс] // Режим доступу до ресурсу: [Проектування комп’ютерної мережі (allbest.ru)](https://knowledge.allbest.ru/programming/2c0b65625b3bc69a5d53a89521216d26_0.html).
2. IP-АДРЕС [Електронний ресурс] // Режим доступу до ресурсу: <https://www.activetraffic.ru/wiki/ip-adres/>
3. Інформаційні системи і технології в управлінні організацією [Електронний ресурс] // Режим доступу до ресурсу: [Глобальні комп'ютерні мережі - Інформаційні системи і технології в управлінні організацією - Навчальні матеріали онлайн (pidru4niki.com)](https://pidru4niki.com/74236/informatika/globalni_kompyuterni_merezhi)
4. Що таке локальна мережа? Функції комп'ютерної мережі [Електронний ресурс] // Режим доступу до ресурсу: <https://www.klaster-plus.ua/ua/stati-i-obzory/chto-takoe-lokalnaja-set-funkcii-kompjuternoi-seti/>
5. ACL: списки контроля доступа [Електронний ресурс] // Режим доступу до ресурсу: <https://habr.com/ru/post/121806/>
6. Frame relay [Електронний ресурс] // Режим доступу до ресурсу: <http://ciscotips.ru/framerelay>
7. Конфігурація NAT [Електронний ресурс] // Режим доступу до ресурсу: <https://admin-gu.ru/device/cisco/cisco-nat-configure>
8. DHCP сервер на маршрутизаторе [Електронний ресурс] // Режим доступу до ресурсу: [DHCP сервер на маршрутизаторе cisco | CiscoTips](http://ciscotips.ru/dhcp-server)
9. SSH [Електронний ресурс] // Режим доступу до ресурсу: <https://www.cisco.com/cisco/web/support/RU/10/105/105417_ssh-inside-out-pix7x.html#telnet>

# ДОДАТОК А

**РОЗРАХУНОК АДРЕСНОГО ПРОСТОРУ**

Рис. 1.2 – розподіл хостів Lan1

**Таблиця 1.4**

**Розрахунок адресного простору для Lan1**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **Net** | **Адреса мережі** | **Адреса хостів мережі** | Broadcast **адреса** |
| **1** | **192.168.10.0/28** | **192.168.10.1 - 192.168.10.14** | **192.168.10.15** |
| **2** | **192.168.10.16/28** | **192.168.10.17 - 192.168.10.30** | **192.168.10.31** |
| **3** | **192.168.10.64/26** | **192.168.10.65 - 192.168.10.126** | **192.168.10.127** |
| **4** | **192.168.10.128/27** | **192.168.10.129 - 192.168.10.158** | **192.168.10.159** |
| **5** | **192.168.10.160/29** | **192.168.10.161 - 192.168.10.166** | **192.168.10.167** |
| **6** | **192.168.10.168/30** | **192.168.10.169 - 192.168.10.170** | **192.168.10.171** |
| **7** | **192.168.10.172/30** | **192.168.10.173 - 192.168.10.174** | **192.168.10.175** |
| **8** | **192.168.10.176/30** | **192.168.10.177 - 192.168.10.178** | **192.168.10.179** |
| **9** | **192.168.10.180/30** | **192.168.10.181 - 192.168.10.182** | **192.168.10.183** |

**Таблиця 1.5**

**Розрахунок адресного простору для Lan2**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **Net** | **Адреса мережі** | **Адреса хостів мережі** | Broadcast **адреса** |
| **1** | **10.3.10.0/30** | **10.3.10.0 - 10.3.10.2** | **10.3.10.3** |
| **2** | **10.3.10.4/30** | **10.3.10.5 - 10.3.10.6** | **10.3.10.7** |
| **3** | **10.3.10.8/30** | **10.3.10.9 - 10.3.10.10** | **10.3.10.11** |
| **4** | **10.3.10.12/30** | **10.3.10.13 - 10.3.10.14** | **10.3.10.15** |
| **5** | **10.3.10.16/30** | **10.3.10.17 - 10.3.10.18** | **10.3.10.19** |
| **6** | **10.3.10.20/30** | **10.3.10.21 - 10.3.10.22** | **10.3.10.23** |
| **7** | **10.3.10.24/30** | **10.3.10.25 - 10.3.10.26** | **10.3.10.27** |
| **8** | **10.3.10.32/27** | **10.3.10.33 - 10.3.10.62** | **10.3.10.63** |
| **9** | **10.3.10.64/27** | **10.3.10.65 - 10.3.10.94** | **10.3.10.95** |
| **10** | **10.3.10.96/27** | **10.3.10.97 - 10.3.10.126** | **10.3.10.127** |
| **11** | **10.3.10.128/27** | **10.3.10.129 - 10.3.10.158** | **10.3.10.159** |
| **12** | **10.3.10.160/27** | **10.3.10.161 - 10.3.10.190** | **10.3.10.191** |

# ДОДАТОК Б

КОНФІГУРАЦІЯ МАРШРУТИЗАТОРА RT1

RT1-10-LAN1#sh run

Building configuration...

Current configuration : 2694 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname RT1-10-LAN1

!

enable password MyEnablePassword

!

interface GigabitEthernet0/0

ip address 192.168.10.174 255.255.255.252

ip nat inside

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 192.168.10.178 255.255.255.252

ip nat inside

duplex auto

speed auto

!

interface GigabitEthernet0/2

ip address 192.168.10.182 255.255.255.252

ip nat inside

duplex auto

speed auto

!

interface GigabitEthernet0/0/0

ip address 192.168.10.170 255.255.255.252

ip access-group 1 in

ip nat inside

!

interface Serial0/1/0

bandwidth 64

ip address 18.0.0.1 255.0.0.0

no ip split-horizon

encapsulation frame-relay

frame-relay map ip 18.0.0.2 102 broadcast

ip nat outside

clock rate 2000000

!

interface Serial0/1/1

no ip address

clock rate 2000000

!

interface FastEthernet0/2/0

switchport mode access

switchport nonegotiate

!

interface FastEthernet0/2/1

switchport mode access

switchport nonegotiate

!

interface FastEthernet0/2/2

switchport mode access

switchport nonegotiate

!

interface FastEthernet0/2/3

switchport mode access

switchport nonegotiate

!

interface FastEthernet0/3/0

switchport mode access

switchport nonegotiate

!

interface FastEthernet0/3/1

switchport mode access

switchport nonegotiate

!

interface FastEthernet0/3/2

switchport mode access

switchport nonegotiate

!

interface FastEthernet0/3/3

switchport mode access

switchport nonegotiate

!

router rip

network 18.0.0.0

network 192.168.10.0

!

ip nat inside source list FOR-NAT interface Serial0/1/0 overload

ip nat inside source static tcp 192.168.10.169 80 18.0.0.1 80

ip classless

ip route 192.168.10.0 255.255.255.240 192.168.10.173

ip route 192.168.10.16 255.255.255.240 192.168.10.173

ip route 192.168.10.64 255.255.255.192 192.168.10.177

ip route 192.168.10.128 255.255.255.224 192.168.10.181

ip route 192.168.10.160 255.255.255.248 192.168.10.181

ip route 192.168.10.168 255.255.255.252 192.168.10.169

ip route 0.0.0.0 0.0.0.0 18.0.0.2

!

ip flow-export version 9

!

ip access-list standard FOR-NAT

permit 192.168.10.0 0.0.0.15

permit 192.168.10.16 0.0.0.15

permit 192.168.10.64 0.0.0.63

permit 192.168.10.128 0.0.0.31

permit 192.168.10.160 0.0.0.7

permit 192.168.10.168 0.0.0.3

!

line con 0

password sobchuk

logging synchronous

login

!

line aux 0

!

line vty 0 4

exec-timeout 5 0

password sobchuk

login

transport input ssh