**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) 2 курсу 207-Кбс групи

спеціальності «Кібербезпека»

(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 172.21.17.0

5.2.2. Складається з п’яти сегментів, кількість робочих станцій в кожному з яких становить: 58, 55, 7, 15, 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 192.168.17.0/24

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 Rt3-Rt5 та Rt5-Rt4 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 Rt3.

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

5.3.7. На маршрутизаторі Rt3 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 FastEtherne1-FastEthernet4 та FastEthernet16-FastEthernet19 відповідно, до Vlan 3 FastEthernet6-FastEthernet9 та FastEthernet7-FastEthernet12 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 4.0.0.0 94.0.0.0 та 12.0.0.0 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 30.1.0.0/16

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.

Розробив студент групи 207-Кбc Москалик Артем Вадимович

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**

**БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ ТА СОЦІАЛЬНИХ НАУК**

Спецiальність: «Кібербезпека»

Курс 2 Група 207-Кбс Семестр 3

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

**ЗАВДАННЯ**

**на курсову роботу студента/студентки**

\_\_\_\_\_\_\_\_\_\_\_\_\_Москалика Артема Вадимовича\_\_\_\_\_\_\_\_\_\_\_\_\_

(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 | | |
| 172.21.17.0 | | | 58 | | | 55 | | | | 7 | | | 15 | | | 5 | | |
| ст. ACL | | відпр. | | | отр. | | | відпр. | | | | отр. | | | відпр. | | | отр. | | |
| Net2 | | | Net5 | | | Net1 | | | | Net3 | | | Net5 | | | Net4 | | |
| розш. ACL | | відпр. | | | отр. | | | відпр. | | | | отр. | | | відпр. | | | отр. | | |
| Net5 | | | Net1 | | | 6,9,12 | | | | Net3 | | | Net4 | | | 1,8,11 | | |
| LAN №2 | № сх. | | | ІР-адреса | | | | Serial HDLC | | | Serial PPP | | | Шлюз | | | | Тип маршрутизації | | | |
| 7 | | | 192.168.17.0/24 | | | | Rt3-Rt5 | | | Rt5-Rt4 | | | Rt3 | | | | Static | | | |
| LAN №3 | | Net1 | Net2 | | | Net3 | | Switch1 | | | | | | | | Switch3 | | | | | |
| Vlan1 | | | Vlan 2 | | Vlan 3 | | | Vlan1 | | Vlan 2 | | | Vlan 3 |
| 4.0.0.0 | 94.0.0.0 | | | 12.0.0.0 | | 11-13 | | | 1-4 | | 6-9 | | | 3-5 | | 16-19 | | | 7-12 |

6. Дата видачі завдання “\_\_\_16 вересня\_\_\_” 20\_20\_ р.

**ЗМІСТ**

[АНОТАЦІЯ 7](#_Toc58967855)

[ВСТУП 8](#_Toc58967856)

[РОЗДІЛ 1. Аналіз технічної частини 10](#_Toc58967857)

[1.1 Аналіз сучасних технологій локальних та глобальних мереж 10](#_Toc58967858)

[1.2 Розрахунок адресного простору 12](#_Toc58967859)

[1.3 Вибір та налаштування способу маршрутизаторів 16](#_Toc58967860)

[РОЗДІЛ 2. Конфігурування мережевого обладнання 18](#_Toc58967861)

[2.1 Конфігурування базових функцій маршрутизаторів 18](#_Toc58967862)

[2.2 Проектування віртуальних мереж 22](#_Toc58967863)

[2.3 Конфігурування базових функцій комутаторів LAN 24](#_Toc58967864)

[2.4 Конфігурування додаткових функцій маршрутизаторів 27](#_Toc58967865)

[РОЗДІЛ 3. Налаштування безпеки та віддаленого доступу на активному обладнанні 30](#_Toc58967866)

[3.1 Налаштування захисту та конфігурування функцій безпеки 30](#_Toc58967867)

[3.2 Налаштування віддаленого доступу до активного обладнання 32](#_Toc58967868)

[3.3 Моделювання та тестування роботи розробленої мережі 35](#_Toc58967869)

[ВИСНОВКИ 39](#_Toc58967870)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 40](#_Toc58967871)

[ДОДАТОК А 42](#_Toc58967872)

[ДОДАТОК Б 44](#_Toc58967873)

АНОТАЦІЯ

Курсова робота призначена для закріплення теоретичних знань і практичних навичок, отриманих при вивченні лекційної та практичної частин навчання. Основною метою є формування системи знань про основні підходи до розробки системи інформаційної безпеки комп'ютерних систем, сучасні апаратні і програмні засоби, призначені для захисту інформації, основні принципи функціонування систем захисту, що розроблені з використанням сучасних методів, технологій та засобів в середовищі електронно-обчислювальних систем і мереж.

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 мета курсової роботи:

* 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

В наш час життя без комп’ютерів майже неможливо. Компьютери необхідні вдома, на виробництві, в банковській справі, в кіно-індустрії і ще багато-багато де. Зараз не можна навіть уявити життя без комп’ютерів. Вони відкрили якісно новий етап в житті і розвитку людської цивілізації. Проте інформацію, яка міститься на одному комп’ютері, досить важко, особливо при великих об’ємах інформації, перенести на інших інший комп’ютер для подальшої роботи. Ці труднощі значно знижували продуктивність праці на комп’ютері, але вони майже повністю відпали з появою комп’ютерних мереж. Комп’ютерні мережі відкрили зовсім нові і значно ширші можливості використання комп’ютерів. Тепер комп’ютери – це не тільки засоби для обробки інформації, це – також засоби для отримання та обміну інформацією.

Комп’ютери підключаються до мережі через вузли комутації. Вузли комутації з'єднуються між собою канали зв'язку. Вузли комутації разом з каналами зв'язку утворюють середовище передачі даних. Комп'ютери, підключені до мережі, у літературі називають вузлами, абонентськими пунктами чи робочими станціями. Комп'ютери, що виконують функції керування мережею чи надають які-небудь мережеві послуги, називаються серверами. Комп'ютери, що користуються послугами серверів, називаються клієнтами.

Кожен комп’ютер, підключений до мережі, має ім'я (адресу). Комп'ютерні мережі можуть обмінюватися між собою інформацією у вигляді повідомлень. Природа цих повідомлень може бути різна (лист, програма, книга і т.д.). У загальному випадку повідомлення по шляху до абонента-одержувача проходить декілька вузлів комутації. Кожний з них, аналізуючи адресу одержувача в повідомленні і володіючи інформацією про конфігурацією мережі, вибирає канал зв'язку для наступного пересилання повідомлення. Таким чином, повідомлення "подорожує" по мережі, поки не досягає абонента-одержувача.

Для підключення до мережі комп'ютери повинні мати:

* апаратні засоби, що з'єднують комп'ютери із середовищем передачі даних;
* мережеве програмне забезпечення, за допомогою якого здіснюється доступ до послуг мережі.

У світі існують тисячі різноманітних комп'ютерних мереж. Найбільш істотними ознаками, що визначають тип мережі, є ступінь територіального розсередження, топологія і застосовані методи комутації.

**РОЗДІЛ 1. Аналіз технічної частини**

**1.1 Аналіз сучасних технологій локальних та глобальних мереж**

Комп'ю́терна мере́жа **–** [система](https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) зв'язку між двома чи більше [комп'ютерами](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80). У ширшому розумінні комп'ютерна мережа **–** це система зв'язку через кабельне чи бездротове середовище, самі [комп'ютери](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%B8) різного функціонального призначення і [мережеве обладнання](https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B5_%D0%BE%D0%B1%D0%BB%D0%B0%D0%B4%D0%BD%D0%B0%D0%BD%D0%BD%D1%8F).

Основні можливості комп’ютерних мереж

* Можливість швидкої передачі інформації на великі відстані;
* Оперативний пошук інформації;
* Обмін інформацією в режимі offline;
* Обмін текстовою, звуковою та відеоінформацією у реальному часі;
* Можливість збереження інформації, розміщеної на серверах Internet, на локальному комп'ютері для подальшої обробки;
* Можливість інтерактивності і оперативного зворотного зв'язку. [1]

До локальних мереж (Local Area Networks, LAN) – відносять мережі комп’ютерів, зосереджених на невеликій території (зазвичай в радіусі 1-2 км).

В загальному випадку локальна мережа представляє собою комунікаційну систему, що належить одній організації. Із-за невеликих відстаней в локальних мережах є можливість використання відносно дорогих високоякісних ліній зв’язку, які дозволяють, застосовуючи прості методи передачі даних досягати високих швидкостей обміну даними порядку 100 Мбіт/с.

Перевагами об'єднання комп'ютерів у локальну мережу є:

* Розподіл даних (Data Sharing). Дані в мережі зберігаються на центральному РС та можуть бути доступні для будь-якого РС, підключеного до мережі, тому не потрібно на кожному робочому місці мати накопичувач для зберігання однієї й тієї ж інформації.
* Розподіл ресурсів (Resource Sharing). Периферійні пристрої можуть бути доступні для всіх користувачів мережі (наприклад, факс або лазерний принтер).
* Розподіл програм (Software Sharing). Усі користувачі мережі можуть мати доступ до програм, які були один раз централізовано встановлені. При цьому повинна працювати мережна версія відповідних програм.
* Електронна пошта (Electronic Mail). Усі користувачі мережі можуть передавати або приймати повідомлення.

Глобальні мережі (Wide Area Networks, WAN) – об’єднують територіально віддалені комп’ютери, які можуть розміщуватися в різних містах чи навіть країнах і континентах.

Оскільки прокладання високоякісних ліній зв’язку на великі відстані коштує досить дорого, в глобальних мережах часто використовуються існуючі лінії зв’язку, які спочатку призначалися зовсім для інших цілей. Наприклад, багато глобальних мереж створюється на основі телефонних та телеграфних каналів загального призначення. Із-за низьких швидкостей таких ліній зв’язку в глобальних мережах набір послуг часто обмежується передачею файлів, переважно не в оперативному, а у фоновому режимі.

Найбільшою у світі глобальною мережею є мережа Internet,яка охоплює всі континенти Землі.

Інтернет **–** це глобальна міжнаціональна мережа, яка складається з набору зв'язаних мереж, що взаємодіють як одне ціле. Складовими Інтернету є мережі різного масштабу: великі національні магістральні мережі, багато регіональних і локальних мереж.

Інтернет **–** це з'єднання багатьох мереж, що забезпечує поширення інформаційних потоків по всій Земній кулі. [2]

**1.2 Розрахунок адресного простору**

IP-адреса, адреса Ай-Пі (від [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) Internet Protocol address) **–** це [ідентифікатор](https://uk.wikipedia.org/wiki/%D0%86%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%82%D0%BE%D1%80) (унікальний числовий номер) [мережевого рівня](https://uk.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_OSI), який використовується для [адресації](https://uk.wikipedia.org/wiki/%D0%90%D0%B4%D1%80%D0%B5%D1%81%D0%B0%D1%86%D1%96%D1%8F_%D0%B2_IP-%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0%D1%85) комп'ютерів чи пристроїв у [мережах](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0), які побудовані з використанням [протоколу](https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) [TCP/IP](https://uk.wikipedia.org/wiki/TCP/IP) (н-д [Інтернет](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)). У мережі Інтернет потрібна глобальна унікальність адрес, у разі роботи в [локальній мережі](https://uk.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0) **–** у межах мережі.

У версії протоколу [IPv4](https://uk.wikipedia.org/wiki/IPv4) IP-адреса має довжину 4 [байти](https://uk.wikipedia.org/wiki/%D0%91%D0%B0%D0%B9%D1%82), а у версії [IPv6](https://uk.wikipedia.org/wiki/IPv6) **–** 16 байтів.

Прикладом IP-адреси може бути адреса 127.0.0.1 (локальна IP-адреса, змінити її неможливо, і вона на кожній ОС лише одна **–** [localhost](https://uk.wikipedia.org/wiki/Localhost)).

Процес перетворення [доменного імені](https://uk.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%BD%D0%BD%D0%B5_%D1%96%D0%BC%27%D1%8F) на адресу IP виконується [DNS-сервером](https://uk.wikipedia.org/wiki/DNS-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80).

IP-адресу називають статичною (постійною, незмінною), якщо вона задається користувачем у налаштуваннях пристрою, або якщо надається автоматично при підключенні пристрою до мережі та не може бути присвоєна іншому пристрою.

IP-адресу називають динамічною (непостійною, змінною), якщо вона надається автоматично при підключенні пристрою до мережі і використовується протягом обмеженого проміжку часу, зазначеного в службі, яка надала IP-адресу ([DHCP](https://uk.wikipedia.org/wiki/DHCP)).

Динамічні адреси IP також бувають віртуальними. Обслуговування уявної адреси IP проводиться за технологією [NAT](https://uk.wikipedia.org/wiki/NAT): користувачам надається можливість безперешкодно отримувати інформацію з мережі Інтернет, при цьому втрачається усіляка можливість іншого доступу до комп'ютера з мережі, так наприклад, комп'ютер з такою адресою IP не може використовуватися як веб-сервер. Не уявні адреси ІР називають реальними, прямими, зовнішніми, громадськими або публічними, «білими», усі такі адреси IP є статичними.

Архітектура протоколів [TCP/IP](https://uk.wikipedia.org/wiki/TCP/IP) призначена для об'єднаної мережі, що складається зі з'єднаних між собою за допомогою шлюзів окремих різнорідних комп'ютерних підмереж.

Протоколи цієї сім'ї розроблялись для мережі [ARPANET](https://uk.wikipedia.org/wiki/ARPANET) Міністерства оборони США, а пізніше отримали широке використання у мережах UNIX-машин та всесвітній мережі [Internet](https://uk.wikipedia.org/wiki/Internet). Стек протоколів [TCP/IP](https://uk.wikipedia.org/wiki/TCP/IP) розроблено та протестовано ще до прийняття стандартів [ISO](https://uk.wikipedia.org/wiki/ISO), а тому ієрархію управління в IP-мережах визначають п'ятьма рівнями:

* Hardware level ;
* Network interface ;
* Internet level ;
* Transport level ;
* Application level .

1 **–** нижній рівень Hardware level описує середовище передавання.

2 **–** рівень Network interface (мережний інтерфейс) містить апаратнозалежне програмне забезпечення, яке забезпечує поширення інформації на певному відрізку середовища передавання.

3 **–** рівень Internet (міжмережний) level представлений протоколами IP, ARP, RARP та ICMP.

4 **–** протокол IP не забезпечує гарантовану доставку пакетів, збереження порядку та цілісності їх потоку. Ці завдання вирішують протоколи [TCP](https://uk.wikipedia.org/wiki/TCP) (Transmission Control Protocol) та [UDP](https://uk.wikipedia.org/wiki/UDP) (User Datagram Protocol), які відносяться до Transport (транспортного) level.

5 **–** рівню Application (прикладному) level відповідають прикладні задачі, серед яких найбільш відомими є гіпертекстові засоби віддаленого доступу [WWW](https://uk.wikipedia.org/wiki/WWW), обмін файлами [FTP](https://uk.wikipedia.org/wiki/FTP) (File Transfer Protocol), протокол служби логічних імен [DNS](https://uk.wikipedia.org/wiki/DNS) (Domain Name Service), електронна пошта [SMTP](https://uk.wikipedia.org/wiki/SMTP) (Simple Mail Transfer Protocol) та емуляція терміналу віддаленого UNIX-сервера TelNet. [3]

**У варіанті було надано таку IP-адресу 172.21.17.0 та кількість хостів. для Net1 – Net5 відповідно 58, 55, 7, 15, 5.**

**Розрахунок відбувався так:**

**По-перше, визначення маски для оптимального налаштування 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** | **58** | **64** |
| **2** | **55** | **64** |
| **3** | **7** | **8** |
| **4** | **15** | **16** |
| **5** | **5** | **8** |

По-друге, переведення отриманих чисел у двійкову систему **(табл. 1.2)**

**Таблиця 1.2**

**Переведення у двійкову систему**

|  |  |  |
| --- | --- | --- |
| **№ Net** | **Значення** | **Двійкова система** |
| **1** | **64** | **11000000** |
| **2** | **64** | **11000000** |
| **3** | **8** | **11111000** |
| **4** | **16** | **11110000** |
| **5** | **8** | **11111000** |

По-третє, переведення отриманих чисел у десяткову систему **(табл. 1.3)**

**Таблиця 1.3**

**Переведення у двійкову систему**

|  |  |  |
| --- | --- | --- |
| **№ Net** | **Значення** | **Двійкова система** |
| **1** | **11000000** | **192** |
| **2** | **11000000** | **192** |
| **3** | **11111000** | **248** |
| **4** | **11110000** | **240** |
| **5** | **11111000** | **248** |

Але нам ще знадобиться додаткові Net, для коректної роботи підмережі, в кількості 4 штуки (Net6 – Net9).

Надалі ми розраховуємо адреси у відповідності до їх маски, для Lan1 – Lan3. Для цього починаючи з 0-ї адреси та додаючи числа-1, знайдені до відповідних кількостей хостів(Додаток А, табл.1.4-табл.1.6).

**1.3 Вибір та налаштування способу маршрутизації**

Маршрутизація (routіng) є однією з ключових функцій мережного рівня ЕМВВС. При цьому під маршрутизацією розуміється, перш за все, процес визначення в телекомунікаційній мережі одного або множини шляхів (маршрутів), оптимальних у рамках обраних критеріїв, між заданою парою або множиною мережних вузлів. Таким чином, шлях (маршрут) — це послідовність мережних вузлів і трактів передачі, які з’єднують задану пару вузлів мережі (рис. 1.1).

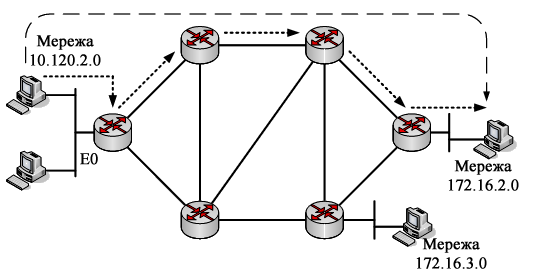


Рисунок 1.1 – Приклад шляху в мережі

Основні цілі маршрутизації полягають у мінімізації (максимізації) значень обраних показників якості обслуговування (швидкості передачі, середньої затримки, джитера, втрат пакетів й ін.), а також у забезпеченні збалансованого завантаження мережі, її канальних і буферних ресурсів. Тому основними завданнями, які належать до галузі маршрутизації, є: контроль і збір інформації про стан мережі (її топології, завантаження мережних ресурсів тощо), розрахунок шуканих шляхів (маршрутів) і реалізація маршрутних рішень.

Мережний рівень за допомогою маршрутизації також реалізує функції об’єднання мереж, побудованих з використанням різнотипних технологій, що використовують різні принципи адресації, пересилання даних, управління. Для об’єднання мереж на третьому рівні ЕМВВС, як правило, використовується спеціальний пристрій — маршрутизатор мережі, який підтримує різні технології канального рівня і обробляє блоки даних мережного рівня. При такому підключенні протокольні особливості локалізуються в межах однієї ділянки мережі, а пересилання пакетів здійснюється на базі єдиного протоколу мережного рівня, який має бути налаштований на кожному кінцевому пристрої.

Інформація про маршрути зберігається на маршрутизаторі у вигляді спеціальних інформаційних структур, які називаються маршрутними таблицями (МТ). Основна робота зі створення таблиць маршрутизації виконується автоматично, але передбачається й можливість корегування або доповнення їх вручну, тобто адміністративно. Для автоматичної побудови таблиць маршрутизатори обмінюються інформацією про топологію об’єднаної мережі у відповідності зі спеціальним службовим протоколом. Протоколи цього типу називаються протоколами маршрутизації або маршрутними протоколами.

Вибір протоколу маршрутизації (routіng protocols) — це досить складне та багатопланове завдання. Під час його розв’язання слід враховувати такі основні фактори:

* розмір і зв’язність топології мережі (кількість мережних вузлів і трактів передачі, порядок їхнього з’єднання), а також планове зростання або зміну її структури;
* характер і обсяг мережного трафіка;
* підтримуваний рівень безпеки та надійності;
* вимоги до якості обслуговування;
* необхідність підтримки масок змінної довжини (VLSM).[4]

**РОЗДІЛ 2. Конфігурування мережевого обладнання**

**2.1 Конфігурування базових функцій маршрутизаторів**

Маршрутизатори - найважливіша частина будь-якої досить великої мережі і всього Інтернету в цілому. У маршрутизаторів добре окреслене коло обов'язків - маршрутизація пакетів. Для успішного виконання цієї роботи маршрутизаторам звичайно потрібно набагато менше апаратури, ніж потрібно домашнього комп'ютера. Приміром, маршрутизаторам не потрібні графічні можливості. Апаратне і програмне забезпечення маршрутизатора вибираються таким чином, щоб маршрутизація здійснювалася ефективно, наскільки можливо, наявність операційної системи на зразок Windows 7 на маршрутизаторі (якби це було можливо) було б марним і, швидше за все, забирало б ресурси від основної функції - від маршрутизації пакетів .

Маршрутизатори CISCO випускаються з операційними системами CISCO IOS (Internetwork Operating System). У більшої частини версій цієї ОС використовується монолітне ядро. Тобто всі функції, які потрібно запускати ОС, працюють всередині простору ядра, що дозволяє робити системні виклики для управління процесами, забезпечення паралелізму і управління пам'яттю.

Сisco Systems має більш ніж широкий асортимент мережевих пристроїв, маршутізаторов, пристроїв доступу. Для успішної роботи з цими пристроями необхідні знання операційної системи Internetwork Operating System (IOS). Знання її допоможе Вам не розгубитися побачивши будь-який пристрій виробництва Cisco. Нехай різниця в реалізаціях операційної системи IOS для різних пристроїв не дасть можливості налаштовувати складні специфічні можливості, але все ж загальні розуміння і стандартні функції будуть цілком до снаги.

Отже IOS володіє двома режимами роботи (користувач) і (адміністратор - привілейований користувач)

Router>

Це вид консолі користувача.

Router>?

Знак питання видасть всі доступні кореневі команди. Знак питання взагалі вкрай корисний його можна ставити також після кореневої команди щоб подивитися варіанти можливих продовжень команд. Або навіть після кількох букв щоб побачити які команди можливі з урахуванням цих букв.

Також корисно знати що всі команди які ви вводите можливо скорочувати приміром переглянути всі доступні інтерфейси на пристрої cisco можна командою.

show interfaces

або скоротити цю команду для зручності

sh int

І так можна чинити з будь-якими командами cisco IOS які після скорочення залишають за собою однозначність у трактуванні. Щоб перейти в режим привілеїв адміністратора необхідно ввести команду enable.

Router> enable

Password:

Router #

Це вид консолі привілейованого користувача. Для початку конфігурування пристрою необхідно активувати команду configure terminal, це можливо тільки в режимі enable.

Router # configure terminal

Router (config) #

Так виглядає режим конфігурування. Вийти з режиму конфігурації можна двома командами exit і end. Вийти з привілейованого режиму - disable. enable увійти disable вийти. Розглянемо можливості режиму config (режим конфігурації). Для конфігурації інтерфейсу необхідно його вказати командою interface та ім'я інтерфейсу наприклад ethernet0, fastEthernet1, serial1.

Router (config-if) #

Це запрошення режиму конфігурації обраного Вами інтерфейсу. Для конфігурації лінії (line) потрібно в режимі конфігурації викликати команду line з ім'ям наприклад vty, console, tty.

Router (config-line) #

Запрошення режиму конфігурації лінії (line). Перехід в режим конфігурування маршрутизації відбувається з допомогою команди router із зазначенням протоколу маршрутизації, приклад - rip, igrp, bgp.

Router (config-router) #

Запрошення цього режиму. Найпопулярніша команда для Вас це швидше за все команда show.

Router> show?

Router # show?

В обох режимах роботи з пристроєм Cisco вона має безліч значень і підзначень, але звичайно в enable (режим привілеїв) їх значно більше. Розглянемо деякі з них.

Router # show version

Виводить величезну кількість інформації серед якої тип пристрою, версія IOS, тривалість роботи після останнього перезавантаження, всі доступні інтерфейси і об'єм пам'яті. Якщо необхідно виділити тільки певну інформацію для відображення, необхідно скористатися наступною конструкцією –

Router> show version | include uptime

Router uptime is 1 hour, 6 minutes

Або - sh ver | i uptime в скороченому варіанті.

Router # show history

Виводить на екран журнал введених команд за замовчуванням 10 останніх.

Router # show user

Повертає список всіх хто підключений до пристрою на поточний момент. Конфігурацій пристрою є два типу Перший running-config переглянути її можна тільки в режимі enable.

Router # show running-config

Ця конфігурація зберігає всі зміни які були внесені в налаштування Cisco IOS протягом роботи з ним, і вона буде стерта при перезавантаженні. другий startup-config.

Router # show startup-config

Це налаштування Cisco IOS з якими вона буде завантажена, воно зберігаються в пам'яті яка не залежить від електроживлення. Якщо в процесі конфігурування ви досягли тих налаштувань із якими Cisco має працювати постійно необхідно скопіювати running-config в пам'ять, яка не залежить від електроживлення.

Router # copy running-config startup-config

Якщо навпаки:

Router # copy startup-config running-config

Коротко базові команди:

IOS володіє двома режимами роботи користувач та адміністратор

show interfaces - говорить сам за себе

enable - перемкнутися в режим адміністратора

disable - вийти з режиму адміністратора

configure terminal - для початку конфігурування пристрою

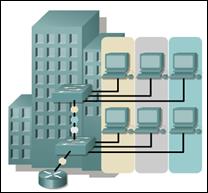
exit, end - вихід з режиму конфігурації

interface та ім'я інтерфейсу наприклад ethernet0, fastEthernet1, serial1 - для конфігурації інтерфейсу. [5]

**2.2 Проектування віртуальних мереж**

Одною з важливих функцій, що реалізовуються в технології Ethernet, є віртуальні локальні мережі VLAN, в яких для об'єднання робочих станцій і серверів в логічні групи, використовуються комутатори. Зв'язок пристроїв, що належать до однієї VLAN-мережі, можливий тільки з пристроями цієї ж мережі, тому в загальному мережа функціонує як декілька індивідуальних, не сполучених одна з одною локальних мереж LAN. Важко дати загальне строге визначення мережі VLAN, оскільки різні виробники використовують різні підходи до створення таких мереж.

Мережі VLAN вирішують завдання масштабування мережі, забезпечення безпеки і мережевого управління. В мережах з топологією VLAN маршрутизатори забезпечують фільтрацію широкомовних(broadcast) пакетів, вирішують завдання захисту мережі і управління потоками даних. Мережа VLAN є групою мережевих пристроїв і служб, не обмеженою фізичним сегментом або комутатором.



**Рисунок** 2.1.Проектування віртуальної локальної мережі

Компанії часто використовують мережі VLAN, як спосіб логічного групування комп'ютерів користувачів. Це можна порівняти з традиційною організацією робочих місць, в якій декілька відділів, зазвичай, групуються до локального департаменту. В даний час співробітники часто не пов'язані з конкретним фізичним робочим місцем, тому мережі VLAN створюють не фізичну, а логічну групу користувачів. Тобто, мережі VLAN логічно сегментують мережі, що використовують комутацію, на основі їх організаційних функцій, приналежності до різних робочих колективів (груп) або використовуваних додатків, а не на базі фізичного або географічного розташування. На рис. 2.1 приведений приклад проектування мережі VLAN у фізичній мережі. В даному випадку створюються три мережі VLAN, в яких робочі станції сполучені одна з одною через комутатори, а самі комутатори сполучені один з одним через маршрутизатор.

Мережу VLAN можна розглядати як широкомовний домен, який існує в певному наборі комутаторів. Мережі VLAN складаються з ряду кінцевих систем, таких як робочі станції або мережевих пристроїв (мостів і маршрутизаторів), сполучених один з одним через окремий мостовий домен.

Мережі VLAN можуть бути створені двома описаними нижче способами

Статичні мережі – цей спосіб також називається членством на базі порта. Призначення портів мережам VLAN створює статичний розподіл VLAN. Коли пристрій під'єднується до порта, він автоматично потрапляє у VLAN-мережу цього порта. Якщо пристрій змінює порт, який використовується для підключення, але йому потрібен доступ до тієї ж мережі VLAN, то мережевий адміністратор повинен включити відповідний порт у потрібну мережу VLAN для нового з’єднання.

Динамічні мережі VLAN – динамічні мережі VLAN створюються з використанням пакетного програмного забезпечення, такого як CiscoWorks 2000. За допомогою сервера політик управління мережами VLAN можна назначити приналежність портів до певної VLAN. [6]

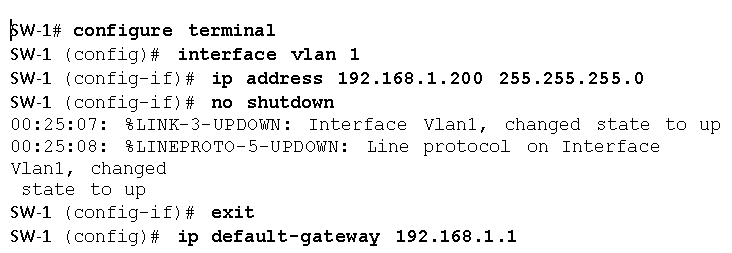
**2.3 Конфігурування базових функцій комутаторів LAN**

Існує кілька критеріїв класифікації комп'ютерних мереж .

В залежності від відносного розташування комп'ютерів розрізняють локальні і глобальні мережі.

Локальні мережі об'єднують комп'ютери, які знаходяться на обмеженій площі в одній будівлі. Зазвичай - це мережа невеликої організації, установи, або мережа структурного підрозділу. Для таких мереж характерне спільне використання програмних засобів і периферійних пристроїв. Локальні мережі можуть бути або одноранговими, або можуть мати виділений сервер.[7]

Приклад налаштування статичної IP-адресації (Рис. 2.2)



**Рисунок** 2.2. Налаштування статичної IP-адресації

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[8]

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. Також ACL існує для різних мережевих протоколів (IP, IPX, AppleTalk і так далі). В основному застосування списків доступу розглядають з точки зору пакетної фільтрації, тобто пакетна фільтрація необхідна в тих ситуаціях, коли у вас коштує обладнання на кордоні Інтернет і вашої приватної мережі і потрібно відфільтрувати непотрібний трафік.

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 приоритетнее

• NAT: які адреси транслювати

Налаштування

Самі ACL створюються окремо, тобто це просто якийсь список, який створюється в глобальному конфіги, потім він присвоюється до інтерфейсу і тільки тоді він і починає працювати. Необхідно пам'ятати деякі моменти, для того, щоб правильно налаштувати списки доступу:

• Обробка ведеться строго в тому порядку, в якому записані умови

• Якщо пакет збігся з умовою, далі він не обробляється

• В кінці кожного списку доступу варто неявний deny any (заборонити все)

• Розширені ACL потрібно розміщувати як можна ближче до джерела, стандартні ж якомога ближче до одержувача

• Не можна розмістити понад 1 списку доступу на інтерфейс, на протокол, на напрям

• ACL не діє на трафік, згенерований самим маршрутизатором

• Для фільтрації адрес використовується WildCard маска

Стандартний список доступу[9]

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 логгірованіе пакети проходять через даний запис ACL

Рефлексивні списки ACL дозволяють фільтрувати IP-пакети на основі інформації сеансу верхнього рівня. Як правило, вони використовуються для вирішення вихідного трафіку і для обмеження вхідного трафіку в якості реакції на сеанси, що виникають всередині маршрутизатора.

Рефлексивні списки ACL можна задати тільки за допомогою розширених іменованих списків ACL для протоколу IP. Їх не можна визначити за допомогою нумерованих або стандартних списків ACL для протоколу IP або за допомогою списків ACL для інших протоколів. Рефлексивні списки ACL можуть використовуватися спільно з іншими стандартними і статичними розширеними списками ACL.

**2.4 Конфігурування додаткових функцій маршрутизаторів**

Поряд з функцією маршрутизації багато маршрутизаторів мають наступні важливими додатковими функціональними можливостями, які значно розширюють сферу застосування цих пристроїв.

Підтримка одночасно декількох протоколів маршрутизації. У протоколах маршрутизації зазвичай передбачається, що маршрутизатор будує свою таблицю на основі роботи тільки цього одного протоколу. Розподіл Internet на автономні системи також спрямована на виключення використання в одній автономній системі декількох протоколів маршрутизації. Проте іноді у великій корпоративної мережі доводиться підтримувати одночасно кілька таких протоколів, найчастіше це складається історично. При цьому таблиця маршрутизації може виходити суперечливою - різні протоколи маршрутизації можуть вибрати різні наступні маршрутизатори для будь-якої мережі призначення. Більшість маршрутизаторів вирішує цю проблему за рахунок надання пріоритетів рішенням різних протоколів маршрутизації. Вищий пріоритет віддається статичним маршрутам (адміністратор завжди правий), наступний пріоритет мають маршрути, обрані протоколами стану зв'язків, такими як OSPF або NLSP, а нижчим пріоритетів мають маршрути дистанційно-векторних протоколів, як самих недосконалих.

Пріоритети мережевих протоколів. Можна встановити пріоритет одного протоколу мережевого рівня над іншими. На вибір маршрутів ці пріоритети не роблять ніякого впливу, вони впливають тільки на порядок, в якому мультипротокольний маршрутизатор обслуговує пакети різних мережевих протоколів. Це властивість буває корисно в разі недостатньої смуги пропускання кабельної системи і існування трафіку, чутливого до тимчасових затримок, напрімертрафіка SNA або голосового трафіку, що передається одним з мережевих протоколів.

Підтримка політики маршрутних оголошень. У більшості протоколів обміну маршрутної інформації (RIP, OSPF, NLSP) передбачається, що маршрутизатор оголошує в своїх повідомленнях про всі мережах, які йому відомі. Аналогічно передбачається, що маршрутизатор при побудові своєї таблиці враховує всі адреси мереж, які надходять йому від інших маршрутизаторів мережі. Однак існують ситуації, коли адміністратор хотів би приховати існування деяких мереж в певній частині своєї мережі від інших адміністраторів, наприклад, з міркувань безпеки. Або ж адміністратор хотів би заборонити деякі маршрути, які могли б існувати в мережі. При статичному побудові таблиць маршрутизації рішення таких проблем не складає труднощів. Динамічні ж протоколи маршрутизації не дозволяють стандартним способом реалізовувати подібні обмеження. Існує тільки один широко використовуваний протокол динамічної маршрутизації, в якому описана можливість існування правил (policy), що обмежують поширення деяких адрес в оголошеннях, - це протокол BGP. Необхідність підтримки таких правил в протоколі BGP зрозуміла, так як це протокол обміну маршрутною інформацією між автономними системами, де велика потреба в адміністративному регулюванні маршрутів (наприклад, деякий постачальник послуг Internet може не захотіти, щоб через нього транзитом проходив трафік іншого постачальника послуг). Розробники маршрутизаторів виправляють цей недолік стандартів протоколів, вводячи в маршрутизатори підтримку правил передачі і використання маршрутної інформації, подібних до тих, які рекомендує BGP.

**Проста настройка протоколу RIP. Увійдемо в конфігурацію маршрутизації протоколу RIP:**

**Router # router rip**

**Зазначимо мережі, яку маршрутизатор буде транслювати в інші мережі:**

**Router # network 192.168.0.0 255.255.255.0**

**Проста настройка протоколу OSPF. OSPF - протокол маршрутизації з урахуванням стану каналів. Увійдемо в конфігурацію маршрутизації протоколу OSPF:**

**200 - тут ідентифікатор процесу для маршрутизатора.**

**Router # router OSPF 200**

**Зазначимо мережі, яку маршрутизатор буде транслювати в інші мережі:**

**area в кінці - область, яка призначена мереж**

**Router # network 192.168.0.0 255.255.255.0 area 0**

**Router # network 172.16.0.0 255.255.255.0 area 1**

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

**3.1 Налаштування захисту та конфігурування функцій безпеки**

Для захисту пристроїв cisco від несанкціонованого доступу використовується декілька видів паролів.

Пароль на привілейований режим

Цей важливий пароль використовується для переходу з режиму користувача в привілейований. При вході на пристрій, незалежно від того, робимо ми це через VTY або через консоль, ми потрапляємо в призначений для користувача режим. Далі можна здійснити перехід в привілейований. Якщо встановлено пароль на привілейований режим, то його потрібно ввести, якщо не заданий - то все залежить від того способу, за яким ми підключилися до пристрою. При підключенні по консолі і відсутньому паролі на enable, перехід в привілейований режим відбудеться без введення пароля, якщо ж доступ здійснюється через Telnet або SSH, то без пароля на enable, нас в цей режим не пустять якщо пароль не заданий. З цієї причини початкова настройка маршрутизатора завжди проводиться через консоль і повинна включати в себе завдання всіх необхідних паролів.

Router # configure terminal

Router (config) #enable password MyEnablePassword

Router (config) #exit

Захист доступу до лінії

За замовчуванням консольний і aux-порти не вимагають пароля для адміністративного доступу. Крім того, команда password, сконфигурированная на консолі, vty і допоміжні (aux) лінії можуть використовувати тільки тип 7. Таким чином, для аутентифікації по імені користувача / пароля консольную і допоміжну лінії потрібно конфігурувати за допомогою команди login local. Крім того, vty-лінії повинні конфигурироваться тільки для SSH-доступу.

Скористайтеся програмою перевірки синтаксису, щоб захистити адміністративний доступ до маршрутизатора.

Примітка. Деякі пристрої Cisco мають більше п'яти vty-ліній. Перш ніж налаштувати пароль, перевірте кількість vty-ліній в активних конфігураційних установках. Наприклад, комутатори Cisco одночасно підтримують до 16 vty-ліній, пронумерованих від 0 до 15.

Можна також відключити процес EXEC для певної лінії, наприклад порту aux, використовуючи команду no exec в режимі конфігурації ліній. Ця команда дозволяє тільки виходить підключення по лінії, відключаючи процес EXEC для підключень, які можуть намагатися відправляти незатребуваної дані на маршрутизатор.[11]

**3.2 Налаштування віддаленого доступу до активного обладнання**

Telnet (TELetype NETwork)— [мережевий протокол](https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D1%96_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85) для реалізації [текстового інтерфейсу](https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BA%D1%81%D1%82%D0%BE%D0%B2%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81_%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87%D0%B0) по [мережі](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0).

Налаштування доступу telnet:

dyn1 (config) # line vty 0 15

dyn1 (config-line) # login

dyn1 (config-line) # password cisco

При підключенні відразу потрапити в привілейований режим:

dyn1 (config) # line vty 0 15

dyn1 (config-line) # privilege level 15

Для обмеження доступу до маршрутизатора за протоколом telnet можна використовувати ACL і застосувати їх до vty.

Наприклад, налаштований ACL, який дозволяє підключатися до маршрутизатора по telnet тільки з адреси 4.4.4.4:

dyn5 (config) # access-list 10 permit 4.4.4.4

dyn5 (config) # line vty 0 4

dyn5 (config-line) # access-class 10 in

Підключившись по telnet, наприклад, з адреси 4.4.4.4 до маршрутизатора dyn5, можна потім з цієї сесії ініціювати telnet сесію до іншого маршрутизатора. Для того щоб контролювати куди можна підключатися зсередини сесії telnet необхідно налаштувати ACL в вихідному напрямі. Наприклад, підключившись до маршрутизатора dyn5 по telnet, ініціювати вихідну сесію telnet можна буде тільки на адресу 1.1.1.1:

dyn5 (config) # access-list 11 permit 1.1.1.1

dyn5 (config) # line vty 0 4

dyn5 (config-line) # access-class 11 out [10]

Налаштування SSH

Заходимо в привілейований режим;

cisco> enable

Встановлюємо дату і час (потрібні для генерації ключа);

cisco # clock set 6:22:06 16 Dec 2020

Входимо в режим конфігурації;

cisco # conf t

Вказуємо домен та ім'я пристрою (для генерації ключа);

cisco (config) #ip domain name domain.local

cisco (config) #hostname cisco-ssh

Генеруємо ключ для SSH;

cisco-ssh (config) #crypto key generate rsa

Зберігаємо паролі в зашифрованому вигляді;

cisco-ssh (config) #service password-encryption

Створюємо користувача admin з паролем Pa $$ w0rd і максимальними привілеями;

cisco-ssh (config) #username admin privilege 15 secret Pa $$ w0rd

Задаємо пароль для привілейованого режиму;

cisco-ssh (config) #enable secret Pa $$ w0rd

Активуємо протокол ААА;

cisco-ssh (config) #aaa new-model

Дозволяємо комп'ютерів внутрішньої мережі заходити на Cisco по SSH;

cisco-ssh (config) # access-list 23 permit 192.168.0.0 0.0.0.255

Входимо в режим конфігурації термінальний ліній;

cisco-ssh (config) #line vty 0 4

Забороняємо все, крім SSH;

cisco-ssh (config-line) #transport input ssh

Активуємо автоматичне підняття рядки після відповіді системи на пророблені зміни;

cisco-ssh (config-line) #logging synchronous

Дозволяємо входити відразу в прівілігірованним режим;

cisco-ssh (config-line) #privilege level 15

Налаштовуємо автоматичне закриття SSH сесії через 60 хвилин;

cisco-ssh (config-line) # exec-timeout 60 0

Прив'язуємо групу доступу, створену на кроці 10, до термінальної лінії;

cisco-ssh (config-line) # access-class 23 in

Виходимо з налаштувань і зберігаємо конфігурацію.

cisco (config-line) exit

cisco (config) exit

cisco # copy run start[12]

**3.3 Моделювання та тестування роботи розробленої мережі**

Побудова розпочалась з LAN1(рис.3.1).

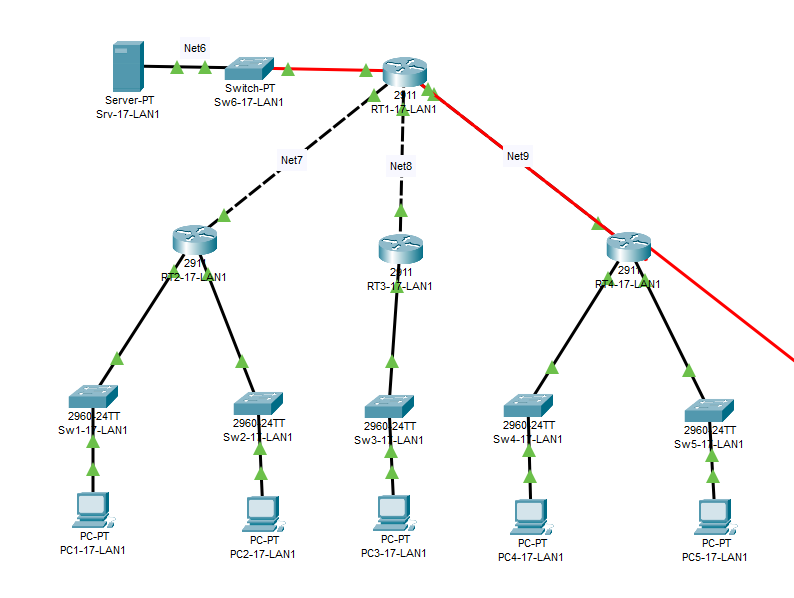


Рисунок 3.1 – Структурна схема LAN1

Надалі проводимо тестування налаштованого LAN1. Існує два методи тестування:

* запуск пакетів за допомогою команди ping в консолі(рис.3.2)
* запуск пакетів у режимі симуляції(рис.3.3)

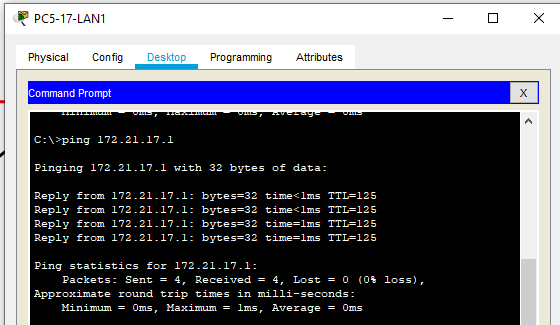


Рисунок 3.2 – Тестування командою ping

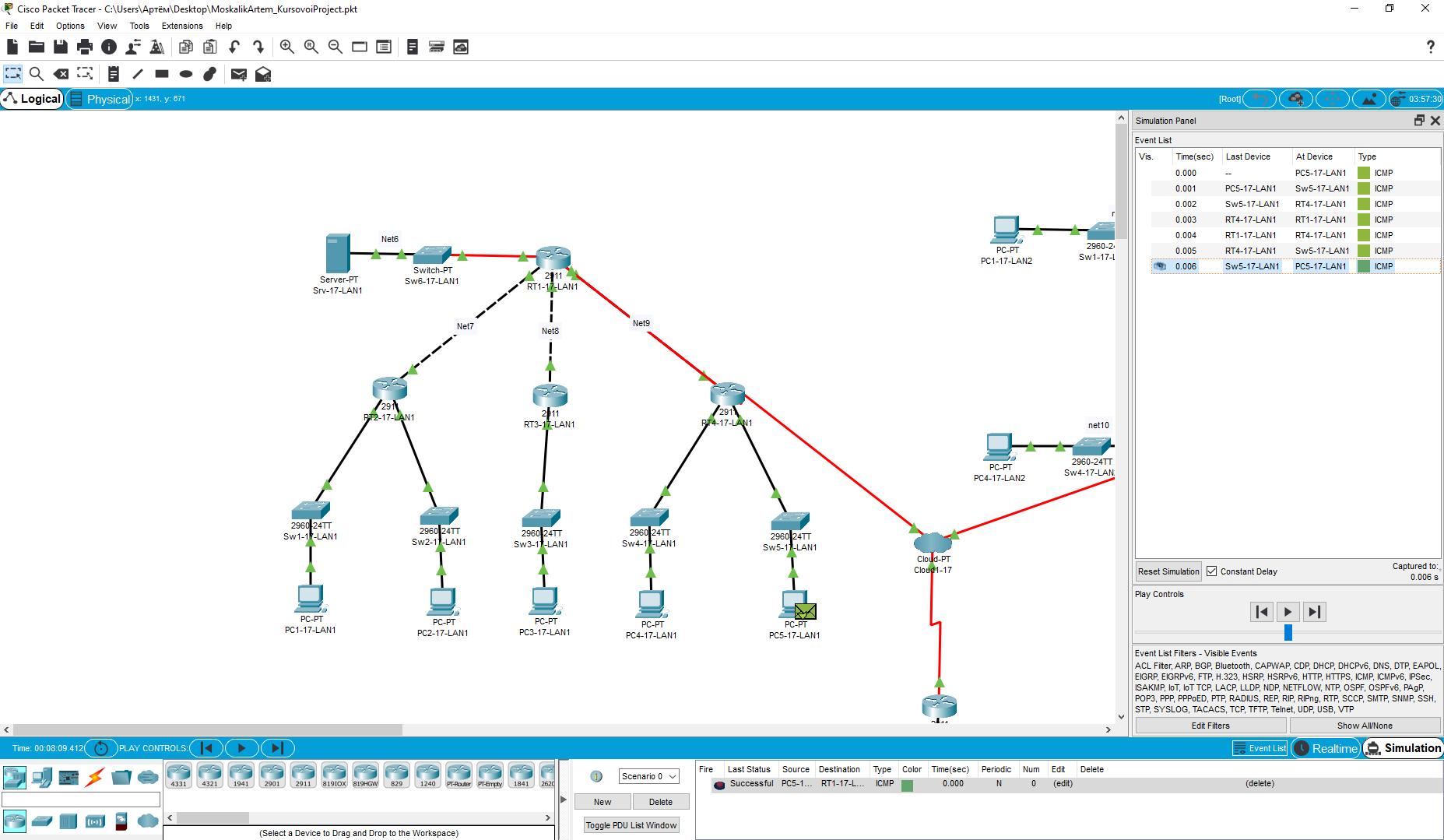


Рисунок 3.3 – Тестування у режимі симуляції

Статична маршрутизація була налаштована мінімальною кількістю записів (рис.3.4).

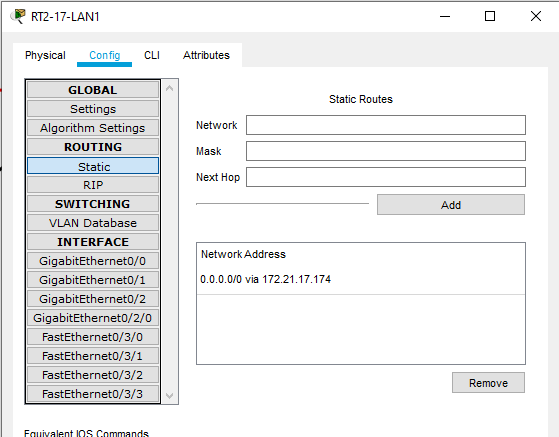


Рисунок 3.4 – таблиця маршрутизації RT2

Також було налаштовано списки керування доступом (ACL), результат налаштування можна перевірити за допомогою команди show run (Додаток Б).

Побудова LAN2 (рис3.5).

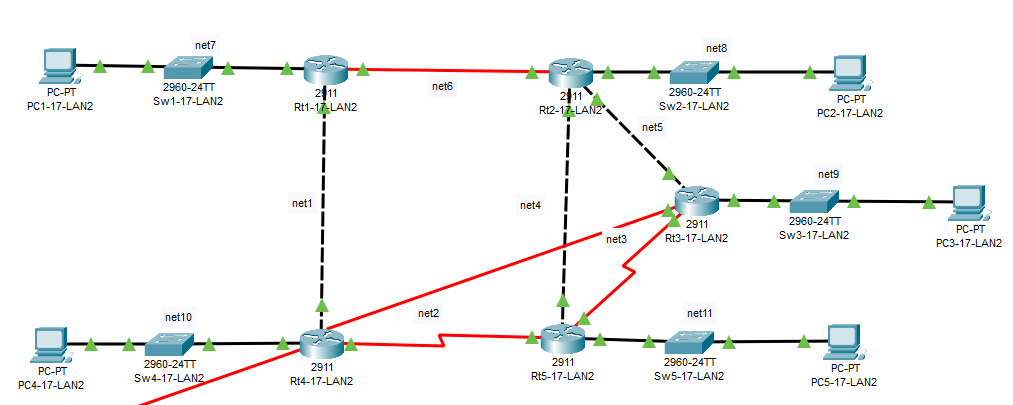


Рисунок 3.5 – Структурна схема LAN2

Надалі проводимо тестування налаштованого LAN2 (рис3.6).

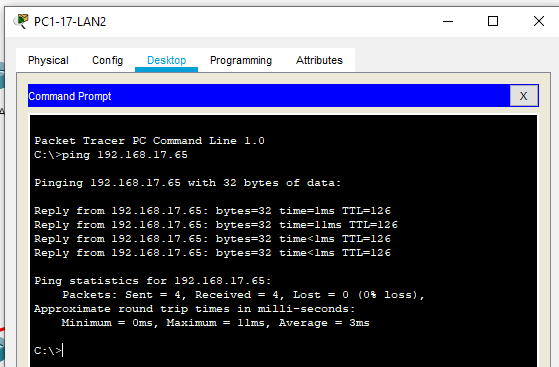


Рисунок 3.6 – Тестування командою ping

Побудова LAN3 (рис3.7).

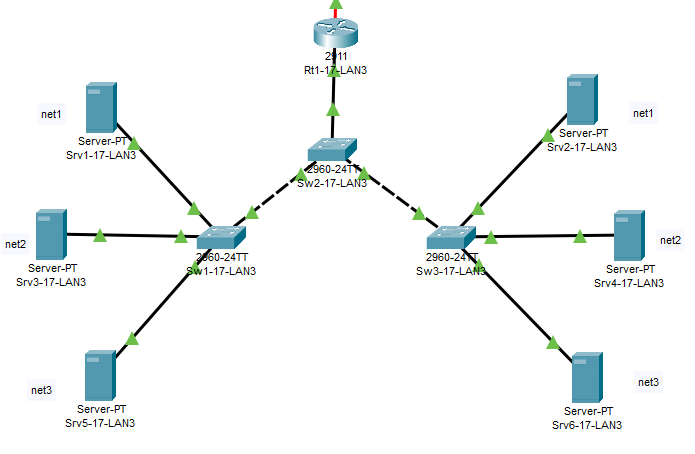


Рисунок 3.7 – Структурна схема LAN3

В даній мережі налаштовано VLAN1-VLAN3.

Останнім етапом є підключення та налаштування Frame Relay. Всі пакети проходять за двома тестами, по всім меражам.

**ВИСНОВКИ**

Під час виконання даної роботи було отримано навички розрахунку параметрів комп’ютерних мереж, внаслідок чого на практиці перевірено моделювання та аналіз функціонування. Також отримані навички адміністрування та налаштування комп’ютерної мережі та вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно міжнародним вимогам та стандартам.

Внаслідок отриманих навичок було розроблено схему комп’ютерної мережі(рис.1), згідно варіанту, налаштовані IP-адреси всіх мережевих інтерфейсів.

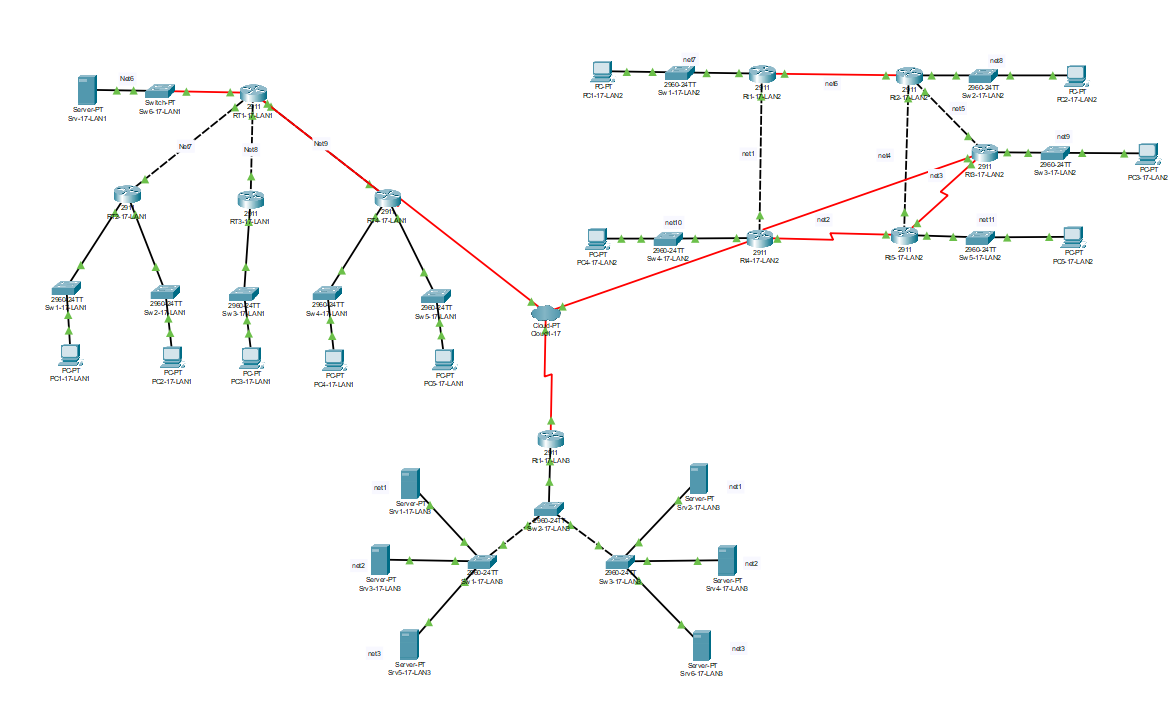


Рисунок 1 – Комп’ютерна мережа

За результатами тестування ця мережа працює коректно.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комп'ю́терна мере́жа [Електронний ресурс] // Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0>
2. Глобальні мережі [Електронний ресурс] // Режим доступу до ресурсу: <https://step.org.ua/konspekt/lanwan/tema3>
3. IP-АДРЕС [Електронний ресурс] // Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%B0>
4. Визначення маршрутизації [Електронний ресурс] // Режим доступу до ресурсу: <https://www.znanius.com/3820.html>
5. Конфігурування маршрутизаторів [Електронний ресурс] // Режим доступу до ресурсу: <https://studopedia.su/3_27878_tema--konfiguruvannya-marshrutizatoriv.html>
6. Призначення мереж VLAN [Електронний ресурс] // Режим доступу до ресурсу: <https://studopedia.org/12-86780.html>
7. Класифікації комп'ютерних мереж [Електронний ресурс] // Режим доступу до ресурсу: <http://www.cpk.org.ua/index.php?option=com_content&view=article&id=181>
8. Frame Relay [Електронний ресурс] // Режим доступу до ресурсу: <http://ciscotips.ru/framerelay>
9. ACL [Електронний ресурс] // Режим доступу до ресурсу: <https://habr.com/ru/post/121806/#:~:text=%D0%92%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5,%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D0%B0%2C%20TCP%20%D0%B8%20UDP%20%D0%BF%D0%BE%D1%80%D1%82%D1%8B>.
10. Telnet [Електронний ресурс] // Режим доступу до ресурсу: <http://xgu.ru/wiki/Cisco_Telnet>
11. Cisco password [Електронний ресурс] // Режим доступу до ресурсу: <http://pyatilistnik.org/kak-postavit-parol-na-privilegirovannyiy-rezhim-v-cisco-na-primere-cisco-2960-48tc-s/>
12. SSH[Електронний ресурс] // Режим доступу до ресурсу: <https://www.dmosk.ru/instruktions.php?object=cisco-ssh>

**ДОДАТОК А**

**РОЗРАХУНОК АДРЕСНОГО ПРОСТОРУ**

**Таблиця 1.4**

**Розрахунок адресного простору для Lan1**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **Net** | **Адреса мережі** | **Адреса хостів мережі** | Broadcast **адреса** |
| **1** | **172.21.17.0/26** | **172.21.17.1 - 172.21.17.62** | **172.21.17.63** |
| **2** | **172.21.17.64/26** | **172.21.17.65 - 172.21.17.126** | **172.21.17.127** |
| **3** | **172.21.17.128/29** | **172.21.17.129 - 172.21.17.134** | **172.21.17.135** |
| **4** | **172.21.17.144/28** | **172.21.17.145 - 172.21.17.158** | **172.21.17.159** |
| **5** | **172.21.17.160/29** | **172.21.17.161 - 172.21.17.166** | **172.21.17.167** |
| **6** | **172.21.17.168/30** | **172.21.17.169 - 172.21.17.170** | **172.21.17.171** |
| **7** | **172.21.17.172/30** | **172.21.17.173 - 172.21.17.174** | **172.21.17.175** |
| **8** | **172.21.17.176/30** | **172.21.17.177 - 172.21.17.178** | **172.21.17.179** |
| **9** | **172.21.17.180/30** | **172.21.17.181 - 172.21.17.182** | **172.21.17.183** |

**Таблиця 1.5**

**Розрахунок адресного простору для Lan2**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **Net** | **Адреса мережі** | **Адреса хостів мережі** | Broadcast **адреса** |
| **1** | **192.168.17.0/30** | **192.168.17.1 - 192.168.17.2** | **192.168.17.3** |
| **2** | **192.168.17.4/30** | **192.168.17.5 - 192.168.17.6** | **192.168.17.7** |
| **3** | **192.168.17.8/30** | **192.168.17.9 - 192.168.17.10** | **192.168.17.11** |
| **4** | **192.168.17.12/30** | **192.168.17.13 - 192.168.17.14** | **192.168.17.15** |
| **5** | **192.168.17.16/30** | **192.168.17.17 - 192.168.17.18** | **192.168.17.19** |
| **6** | **192.168.17.20/30** | **192.168.17.21 - 192.168.17.22** | **192.168.17.23** |
| **7** | **192.168.17.32/27** | **192.168.17.33 - 192.168.17.62** | **192.168.17.63** |
| **8** | **192.168.17.64/27** | **192.168.17.65 - 192.168.17.94** | **192.168.17.95** |
| **9** | **192.168.17.96/27** | **192.168.17.97 - 192.168.17.126** | **192.168.17.127** |
| **10** | **192.168.17.128/27** | **192.168.17.129 - 192.168.17.158** | **192.168.17.159** |
| **11** | **192.168.17.160/27** | **192.168.17.161 - 192.168.17.190** | **192.168.17.191** |

**Таблиця 1.6**

**Розрахунок адресного простору для Lan3**

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **Net** | **Адреса мережі** | **Адреса хостів мережі** | Broadcast **адреса** |
| **1** | **4.0.0.0/29** | **4.0.0.1 - 4.0.0.6** | **4.0.0.7** |
| **2** | **94.0.0.0/29** | **94.0.0.1 - 94.0.0.6** | **94.0.0.7** |
| **3** | **12.0.0.0/29** | **12.0.0.1 - 12.0.0.6** | **12.0.0.7** |

**ДОДАТОК Б**

КОНФІГУРАЦІЯ МАРШРУТИЗАТОРА RT1

Router#show run

Building configuration...

Current configuration : 1950 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

interface GigabitEthernet0/0

ip address 172.21.17.174 255.255.255.252

duplex auto

speed auto

!

interface GigabitEthernet0/1

ip address 172.21.17.178 255.255.255.252

duplex auto

speed auto

!

interface GigabitEthernet0/2

ip address 172.21.17.182 255.255.255.252

duplex auto

speed auto

!

interface Serial0/0/0

bandwidth 64

ip address 30.1.0.1 255.255.0.0

encapsulation frame-relay

frame-relay map ip 30.1.0.2 102 broadcast

frame-relay map ip 30.1.0.3 103 broadcast

clock rate 2000000

!

interface Serial0/0/1

no ip address

clock rate 2000000

shutdown

!

interface Serial0/1/0

no ip address

clock rate 2000000

shutdown

!

interface Serial0/1/1

no ip address

clock rate 2000000

shutdown

!

interface GigabitEthernet0/2/0

ip address 172.21.17.170 255.255.255.252

!

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

!

interface Vlan1

no ip address

shutdown

!

router rip

network 30.0.0.0

network 172.21.0.0

!

ip classless

ip route 172.21.17.0 255.255.255.192 172.21.17.173

ip route 172.21.17.64 255.255.255.192 172.21.17.173

ip route 172.21.17.144 255.255.255.240 172.21.17.181

ip route 172.21.17.160 255.255.255.248 172.21.17.181

ip route 172.21.17.168 255.255.255.252 172.21.17.169

ip route 172.21.17.128 255.255.255.248 172.21.17.177

ip route 0.0.0.0 0.0.0.0 30.1.0.2

!

ip flow-export version 9

!

ip access-list standard FOR-NAT

permit 172.21.17.0 0.0.0.15

permit 172.21.17.64 0.0.0.15

permit 172.21.17.144 0.0.0.63

permit 172.21.17.160 0.0.0.31

permit 172.21.17.168 0.0.0.7

permit 172.21.17.128 0.0.0.3

!

line con 0

!

line aux 0

!

line vty 0 4

login