**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 корпоративної комп’ютерної мережі** .

Студента(ки) 3 курсу 303-Кб групи

спеціальності «Кібербезпека»

Молібог А. С.

(прізвище та ініціали)

Керівник:

(посада, вчене звання, науковий ступінь,

Гордєєва Д. В.

прізвище та ініціали)

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

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

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

Члени комісії

(підпис) (прізвище та ініціали)

(підпис) (прізвище та ініціали)

(підпис) (прізвище та ініціали)

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:
   1. мета - отримання практичних навичок проектування та конфігурування комп’ютерних мереж;
   2. призначення розробки — навчальна курсова робота із дисципліни «Комп’ютерні системи та мережі (Рівень D - Безпека комп`ютерних систем)»;
4. Джерела розробки — індивідуальне завдання на курсовий проект із дисципліни, технічні рекомендації щодо проектування локальних та розподілених мереж та інші технічні матеріали для налаштування окремих компонентів мережі.
5. Технічні вимоги:
   1. Мережа складається з трьох окремих LAN, що об’єднуються WAN мережею, побудованою на основі технології віртуальних каналів.
   2. Вимоги для проектування LAN1
      1. Адреса мережі 10.2.9.0
      2. Складається з п’яти сегментів, кількість робочих станцій в кожному з яких становить: 55, 24, 11, 20, 18.
      3. Розподіл адресного простору має бути оптимальним;
      4. Для об’єднання окремих сегментів використовуються 4 маршрутизатори;
      5. З’єднання між маршрутизаторами здійснюються за допомогою скрученої пари;
      6. Для обмеження проходження трафіку з одного сегменту в інший мають бути застосовані стандартні і розширені ACL. Стандартні списки мають заборонити проходження трафіку з мереж NET2 NET4 та NET5 відповідно до мереж NET1 NET6 та NET2. Розширені ACL мають заборонити проходження трафіку протоколів HTTP, NETBIOS та SNMP з NET5 до NET3 та IMAP PING та TELNET з NET1 до NET2. ACL необхідно розмістити в найбільш вдалому місці.
      7. У середині мережі використовується статична маршрутизація.
      8. На маршрутизаторах Rt2-Rt4 налаштувати DHCP-сервіс і забезпечити динамічне призначення адрес хостам в мережах Net1-Net5.
      9. На маршрутизаторі Rt1 налаштовано сервіс трансляції адрес NAT.
   3. Вимоги для проектування LAN2
      1. Адреса мережі 172.19.9.0/24
      2. Складається з 5 сегментів, в яких розташовані ПК користувачів.
      3. Розподілити адресний простір таким чином: в мережах, що з’єднують маршрутизатори, використовувати префікс 30 (маска 255.255.255.252), весь вільний простір, що залишається, рівномірно поділити між мережами, в яких розташовані Switch1- Switch5.
      4. З’єднання між маршрутизаторами Rt1-Rt4 та Rt1-Rt2 здійснюється за допомогою послідовних інтерфейсів з використанням протоколів канального рівня HDLC та РРР відповідно. Інші з’єднання виконуються за допомогою скрученої пари.
      5. Під’єднання мережі LAN2 до мережі WAN виконується через маршрутизатор Rt2.
      6. В середині мережі використовується динамічна маршрутизація на основі протоколу RIP.
      7. На маршрутизаторі Rt1 налаштовано сервіс трансляції адрес NAT.
   4. Вимоги для проектування LAN3
      1. Реалізована на основі комутаторів Catalyst 2960 з підтримкою технології віртуальних мереж.
      2. Поділена на три віртуальні сегменти, кожний з яких містить по два сервери.
      3. На комутаторах Sw1, Sw2 до Vlan 2 належать порти FastEthernet13-FastEthernet17 та FastEthernet6-FastEthernet8 відповідно, до Vlan 3 FastEthernet19-FastEthernet22 та FastEthernet2-FastEthernet5 відповідно.
      4. З’єднання між комутаторами здійснюються за допомогою скрученої пари і технології Gigabit Ethernet.
      5. В віртуальних мережах VLAN1, VLAN2 та VLAN3 використовуються адреси 203.111.18.0, 184.1.0.0 та 14.0.0.0 відповідно.
   5. Вимоги для проектування WAN
      1. Об’єднання локальних мереж здійснюється за допомогою Frame Relay комутатора з використанням топології Full Mesh.
      2. Адреси інтерфейсів маршрутизаторів, що під’єднані до Frame Relay мережі, належать до мережі з адресою 12.2.1.0/24
      3. З’єднання між локальними мережами здійснюється за допомогою послідовних інтерфейсів.
   6. Загальні вимоги до налаштувань маршрутизаторів
      1. Встановити на всіх маршрутизаторах паролі на консольне з’єднання та на привілейований режим.
      2. Налаштувати доступ через протокол SSH до шлюзових маршрутизаторів.
6. Апаратні вимоги - використання обладнання фірми Cisco
7. Текстова документація розробленої мережі повинна відповідати 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 Молібог А. С.

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**

**БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ ТА СОЦІАЛЬНИХ НАУК**

Спеціальність: «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**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_Молібог Анни Сергіївни \_\_\_\_\_\_\_\_\_\_\_**

(прізвище, ім’я, по-батькові)

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

2. **Термін здачi студентом закінченої 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 |
| 10.2.9.0 | | 55 | | | 24 | | | 11 | | 20 | | | | 18 |
| ст. ACL | | відпр. | | отр. | | | відпр. | | | отр. | | відпр. | | | | отр. |
| Net2 | | Net1 | | | Net4 | | | Net6 | | Net5 | | | | Net2 |
| розш. ACL | | відпр. | | отр. | | | № прот. | | | отр. | | відпр. | | | | № прот. |
| Net5 | | Net3 | | | 4, 7, 12 | | | Net1 | | Net2 | | | | 6, 8, 14 |
| LAN №2 | № сх. | | | ІР-адреса | | Serial HDLC | | | Serial PPP | | | Шлюз | | | Тип маршрутизації | | |
| 9 | | | 172.19.9.0/24 | | Rt1-Rt4 | | | Rt1-Rt2 | | | Rt2 | | | RIP | | |
| LAN №3 | Net1 | Net2 | | | Net3 | | Switch1 | | | | | | | Switch3 | | | |
| Vlan 2 | | | Vlan 3 | | | | Vlan 2 | | Vlan 3 | |
| 203.111.18.0 | 184.1.0.0 | | | 14.0.0.0 | | 13-17 | | | 19-22 | | | | 6-8 | | 2-5 | |

6. Дата видачі завдання “ 16 вересня ” 20 20 р

## **ЗМІСТ**

[ЗМІСТ 6](#_Toc58810655)

[АНОТАЦІЯ 8](#_Toc58810656)

[ВСТУП 9](#_Toc58810657)

[1. РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ ТА ПОПЕРЕДНІ РОЗРАХУНКИ 11](#_Toc58810658)

[1.1. Аналіз сучасних технологій локальних та глобальних мереж 11](#_Toc58810659)

[1.2. Скорочена постановка задачі 13](#_Toc58810660)

[1.3. Розрахунок адресного простору 17](#_Toc58810661)

[2. РОЗДІЛ 2 ПОБУДОВА МЕРЕЖІ ТА КОНФІГУРУВАННЯ БАЗОВИХ ФУНКЦІЙ 22](#_Toc58810662)

[2.1. Побудова мережі та базові налаштування 22](#_Toc58810663)

[2.2. Вибір та налаштування способу маршрутизації 26](#_Toc58810664)

[2.3. Проектування віртуальних мереж 27](#_Toc58810665)

[2.4. Конфігурування базових функцій маршрутизатора 27](#_Toc58810666)

[2.5. Підключення Frame Relay 28](#_Toc58810667)

[2.6. Конфігурування додаткових функцій маршрутизаторів (DHCP, NAT тощо) 31](#_Toc58810668)

[3. РОЗДІЛ 3 ЗАХИСТ ТА ТЕСТУВАННЯ МЕРЕЖІ 33](#_Toc58810669)

[3.1. Налаштування захисту та конфігурування функцій безпеки(налаштування паролів, ACL) 33](#_Toc58810670)

[3.2. Налаштування віддаленого доступу до активного обладнання 34](#_Toc58810671)

[3.3. Тестування роботи розробленої мережі 35](#_Toc58810672)

[ВИСНОВКИ 42](#_Toc58810673)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 43](#_Toc58810674)

[ДОДАТОК А ТЕХНІЧНЕ ЗАВДАННЯ 45](#_Toc58810675)

# **АНОТАЦІЯ**

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

Виконала – Молібог А. С.

Керівник – Гордєєва Д. В.

Курсова робота складається з 3 частин: пояснювальної записки, основної (технічної) частини та графічної частини. Основна частина складається з 3 розділів, а саме: .

Для розробки даної курсової роботи, був побудований прототип комп’ютерної мережі за допомогою програми “Packet Tracer”. Було розраховано адресний простір, налаштовано різні види маршрутизації, спроектовано віртуальні мережі, зконфігуровано базові та додаткові функції маршрутизаторів та комутаторів, а також було налаштовано віддалений доступ до активного обладнання і захист та конфігурування функцій безпеки. Розроблена комп’ютерна мережа була протестована.

Курсова робота містить:

* Сторінок - ;
* Таблиць - ;
* Рисунків - ;
* Джерел використаної літератури - .

# **ВСТУП**

Комп’ютерна мережа являє собою два або більше комп’ютерів з’єднаних між собою за допомогою мережевого обладнання. У мережах комп’ютери можуть бути з’єднані між собою як через кабельне, так і через бездротове середовище.

За допомогою комп’ютерних мереж, люди можуть обмінюватися інформацією через комп’ютери, знаходячись у різних кімнатах, будинках, містах та, навіть, на різних континентах. Розрізняють контролюючі (CAN), локальні (LAN), регіональні (MAN), та глобальні (WAN) комп’ютерні мережі.

Контролюючі комп’ютерні мережі (CAN) широко використовується в промисловій автоматизації, технологіях «розумного будинку» та автомобільній промисловості. Вони прості у реалізації та потребують мінімальні затрати на використання, а також такі мережі стійкі до перешкод і мають широкий діапазон швидкостей.

Локальні комп’ютерні мережі (LAN) об’єднують деяку кількість комп’ютерів на невеликій відстані один від одного. Доступ до таких мереж є обмеженим і дозволяється лише певній кількості користувачів. Усередині мережі користувачі можуть вільно обмінюватися даними за високої швидкості та низькому рівні помилок.

Регіональні комп’ютерні мережі (MAN) об’єднують багато локальних мереж одного або декількох міст.

Найяскравішим прикладом глобальних комп’ютерних мереж (WAN) є Internet. Глобальні мережі об’єднують віддалені одна від одної локальні мережі. На відміну від локальних, глобальні мережі можуть обслуговувати необмежену кількість користувачів, проте для цього не завжди використовується якісний зв’язок та висока швидкість передачі даних [1].

Незалежно від типу мережі, вона буде вразлива до зовнішніх та внутрішніх загроз. На сьогодні, існує велика кількість вірусів, видів атак та загроз для комп’ютерних мереж. Кожного дня кіберзлочинці здійснюють напади на мережі, бажаючи захопити або зіпсувати особисті дані користувачів і, навіть, конфіденціальні документи приватних та державних підприємств. Саме тому, необхідно шифрувати та захищати дані та обладнання у мережах.

Найпростішим способом захистити мережу – встановити паролі на обладнання у мережі. Слід встановлювати надійні паролі, аби їх було складно розгадати. Проте, наразі, існує велика кількість способів обходження паролів, тому одного паролю буде мало для захисту обладнання.

Для кращого захисту мережі встановлюють захисне обладнання, захищається віддалений доступ до пристроїв, створюються облікові записи і т. д. У даній курсовій роботі, розглядаються деякі з них.

# **РОЗДІЛ 1 ТЕОРЕТИЧНІ ВІДОМОСТІ ТА ПОПЕРЕДНІ РОЗРАХУНКИ**

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

Рішенням задачі по оперативному обміну інформацією між комп'ютерами, доступу до різних інформаційних ресурсів та мережі Інтернет є локальна мережа (LAN - Local Aria Network). Локальна мережа (LAN) може об'єднати в єдиний інформаційний простір комп'ютери, сервери, телефони, периферійні обладнання не тільки в межах одного офісу, але і територіально віддалених офісів (рис. 1.1).

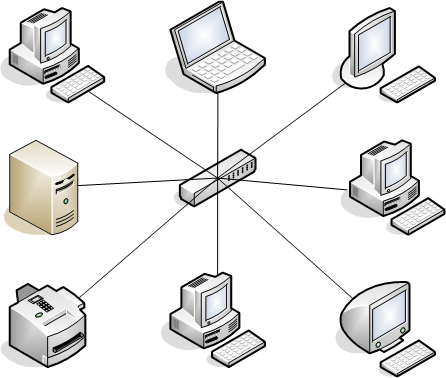


Рисунок 1.1 – Локальна мережа

Обмін даними між комп'ютерами на фізичному рівні може здійснюватися по спеціальному кабелю, телефонної лінії, волоконно-оптичному кабелю або по радіоканалу. Але так як всі комп'ютери обмінюються даними один з одним, то обов'язковими основними елементами локальної мережі є:

* активне мережеве обладнання (комутатори, маршрутизатори і т.д.);
* пасивне мережеве обладнання або СКС (кабелі, комутаційні панелі, шафи, стійки і т.д.);
* мережеві екрани для забезпечення безпеки і захисту інформації;
* серверне обладнання [2].

Глобальна мережа (WAN) — це з'єднання локальних мереж і окремих комп'ютерів, розташованих на далекій відстані один від одного (рис. 1.2).

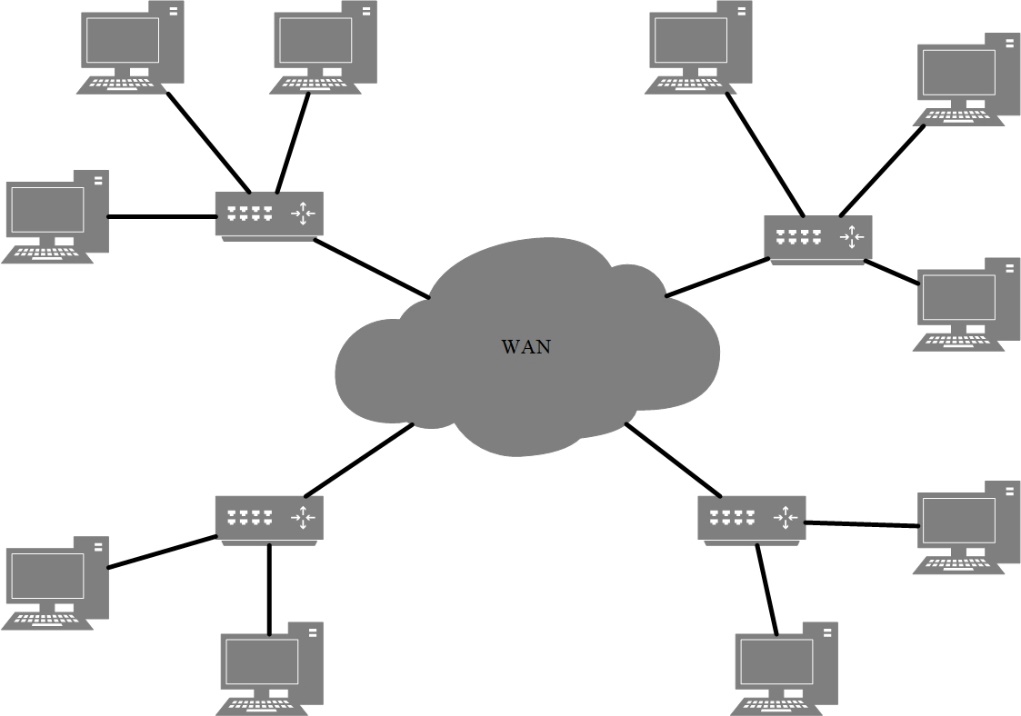


Рисунок 1.2 – глобальна мережа

У таких мережах є додаткові пристрої для обробки великих обсягів інформації та пересилання її на далеку відстань. Передусім, це сервери глобальних мереж, які є дуже потужними комп'ютерами.

Через великі відстані між комп'ютерами використання простих ліній зв'язку в глобальних мережах не можливе. Сучасні глобальні мережі використовують найрозвиненіший у світі зв'язок — телефонний. Проте зв'язок між серверами глобальної мережі здійснюється не по звичайних телефонних лініях, а по виділених лініях або по спеціальних каналах зв'язку. У глобальних мережах найчастіше використовуються системи супутникового зв'язку, що значно розширює масштаби та можливості таких мереж.

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

Internet — 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.

Мережі, які є складовими Інтернету, поширюються на великі відстані та можуть перекривати одна одну, тому будь-яка пара вузлів пов'язана між собою не одним, а багатьма каналами зв'язку, завдяки чому Інтернет забезпечує стійкий зв'язок навіть в умовах військових дій. При руйнуванні частини мережі пакети інформації можуть обходити ушкоджені ділянки [3].

## **Скорочена постановка задачі**

Метою курсової роботи є розробка корпоративної комп’ютерної мережі, що складається з трьох локальних мереж (центральний офіс, віддалений офіс та датацентр), з’єднаних через магістральну мережу з використанням багато зонової маршрутизації (рис. 1.3).

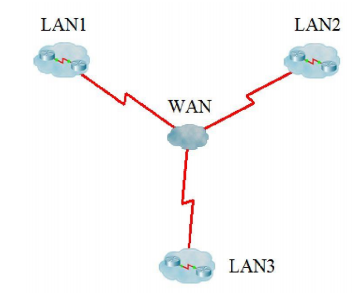


Рисунок 1.3 – Структурна схема корпоративної мережі

Мережа LAN1 (центральний офіс) складається з п’яти підрозділів (Net1- Net5) та мережі Net6, де розташований локальний сервер офісу (рис. 1.4). Кількість хостів у підрозділах Net1- Net5 – 55, 24, 11, 20 та 18 відповідно. ІР-адреса центрального офісу – 10.2.9.0.

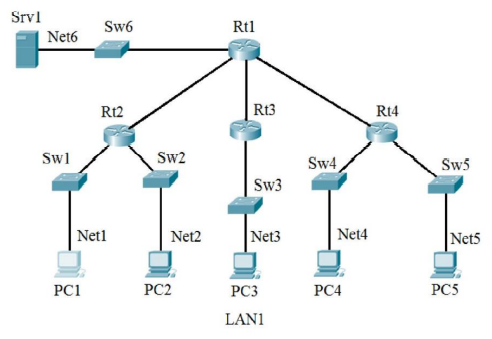


Рисунок 1.4 – Структурна схема мережі центрального офісу

Зробити розрахунок адрес підмереж та адрес хостів. Маски мають бути вибрані оптимальними. Визначити, скільки адрес в кожній підмережі залишились вільними. Нарисувати кругову діаграму, позначивши на ній всі сегменти адрес, які було виділено. Визначити, скільки ще підмереж і якого обсягу залишились незадіяними.

На маршрутизаторах Rt2-Rt4 налаштувати DHCP-сервіс і забезпечити динамічне призначення адрес хостам в мережах Net1-Net5. Налаштувати статичну маршрутизацію таким чином, щоб кількість записів в таблиці маршрутизації кожного маршрутизатора була мінімальною.

Налаштувати 3 стандартні та 2 розширені списки керування доступом (ACL), які будуть забороняти проходження трафіку відповідно до табл. 1.1.

Таблиця 1.1

Вихідні дані для налаштування списків керування доступом

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Стандартні | | | | | | | Розширені | | | | | |
| Відпр. | Отр. | Відпр. | Отр. | Відпр. | Отр. | Відпр. | | Отр. | Протоколи | Відпр. | Отр. | Протоколи |
| Net2 | Net1 | Net4 | Net6 | Net5 | Net2 | Net5 | | Net3 | HTTP, NETBIOS, SNMP | Net1 | Net2 | IMAP, PING, TELNET |

Для віддаленого офісу LAN2 (рис. 1.5), 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. Налаштувати маршрутизацію RIP. Усі інші налаштування вказані в табл. 1.2.

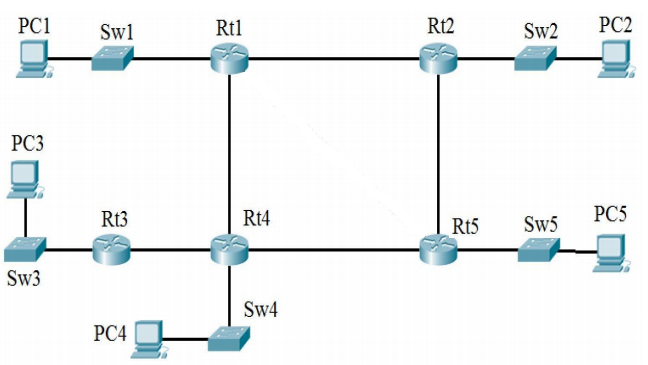


Рисунок 1.5 – Структурна схема віддаленого офісу

Таблиця 1.2

Вихідні дані для налаштування мережі віддаленого офісу

|  |  |  |  |
| --- | --- | --- | --- |
| ІР-адреса | Serial | Serial | Шлюзовий маршрутизатор |
| 172.19.9.0/24 | Rt1-Rt4 | Rt1-Rt2 | Rt2 |

Побудувати дата центр LAN3, яку показано на рис. 1.6.

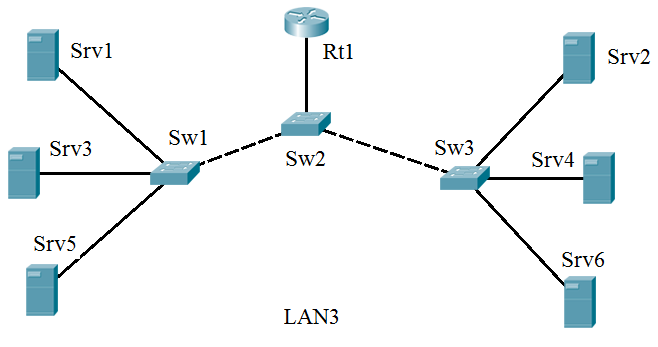


Рисунок 1.6 – Структурна схема дата центру

Створити на кожному комутаторі VLAN2 та VLAN3. Увести до VLAN2 та VLAN3 порти відповідно до табл. 1.3. Srv1 і Srv2 під’єднати до портів, що входять до VLAN1, Srv3 і Srv4 під’єднати до портів, що входять до VLAN2, Srv5 і Srv6 під’єднати до портів, що входять до VLAN3.

Призначити IP-адреси VLAN1 кожного комутатора, вибравши для цього перші доступні адреси мережі Net1 з табл. 1.3. Призначити ІР адреси серверам таким чином, щоб всі хости, що підключені до портів VLAN1, VLAN2 та VLAN3 знаходились, відповідно, в мережах Net1, Net2 та Net3.

Таблиця 1.3

Вихідні дані для проектування мережі дата центру

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Net1 | Net2 | Net3 | SW1 | | | SW3 | | |
| VLAN1 | VLAN2 | VLAN3 | VLAN1 | VLAN2 | VLAN3 |
| 203.111.18.0 | 184.1.0.0 | 14.0.0.0 | 3-10 | 13-17 | 19-22 | 18-19 | 6-8 | 2-5 |

Для всіх локальних мереж:

1. Призначити імена всім маршрутизаторам і комутаторам за таким принципом: X-Y-Z, де Х - назва пристрою на рисунку, Y - № варіанту, Z – назва мережі (LAN1, LAN2 або LAN 3).
2. Встановити на всіх маршрутизаторах паролі на консольне з’єднання та на привілейований режим.
3. Налаштувати доступ через протокол SSH до шлюзових маршрутизаторів.

Об’єднання локальних мереж LAN1-LAN3 здійснюється через шлюзові маршрутизатори, відповідні послідовні інтерфейси яких підключаються до комутатора Frame Relay. Функцію шлюзового маршрутизатора в мережах LAN1 та LAN3 виконує Rt1, а в мережі LAN2 визначається номером варіанту (див. табл. 1.2). Адреса мережі Frame Relay – 12.2.1.0/24.

На шлюзових маршрутизаторах мереж LAN1 і LAN2 налаштувати трансляцію адрес NAT, причому для сервера Srv1 в мережі LAN1 має бути налаштований статичний NAT, а для решти комп’ютерів - трансляція з перекриттям (РАТ). Для комп’ютерів РС1-РС5 мережі LAN2 налаштувати динамічний NAT [4].

## **Розрахунок адресного простору**

1. Розрахунок адресного простору для LAN1:

Необхідно створити 9 підмереж, серед яких:

* 5 підмереж з комп’ютерами;
* 1 підмережа з сервером;
* 3 підмережі, що з’єднують між собою маршрутизатори.

За умовою, у першій підмережі має бути виділено адреси для 55 хостів, значить необхідно взяти 64 (керуючись степенями двійки). Розраховуємо маску табл. 1.4. вписуємо одиниці до числа, що відповідає кількості виділених нами адрес включно. Далі записуються нулі:

Таблиця 1.4.

Розрахунок маски для першої підмережі у LAN1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

Необхідно перевести отримане число 11000000 з двоїчної системи числення (далі с. ч.) у десятичну с. ч. Необхідно скласти ті значення степенів двійки, яким відповідають одиниці (табл. 1.4):

(1.1)

де 128 - ;

64 - .

Отримали число 192, це означає, що перша підмережа буде мати маску 255.255.255.192 (префікс 26). Тому адресу Net1, можна записати наступним чином: 10.2.9.0/26. Остання адреса у підмережі (10.2.9.63) буде широкомовною, її не можна призначати хостам. Тобто, з 64 виділених адрес на підмережу, перша назначається адресою мережі, остання – широкомовною адресою і для хостів залишається 62 адреси, тому діапазон адрес хостів буде наступним: 10.2.9.1 - 10.2.9.62. Розрахуємо також шаблонну маску, для цього необхідно від маски мережі 255.255.255.255 відняти маску підмережі 255.255.255.192. Отримаємо 0.0.0.63

Проводимо аналогічні розрахунки, для інших підмереж LAN1.

У другій підмережі має бути 24 хости, виділяємо 32 адреси. Отримуємо підмережу 10.2.9.64/27. У третій підмережі має бути 11 хостів, виділяємо 16 адрес. Отримуємо підмережу 10.2.9.96/28. У четвертій підмережі має бути 20 хостів, виділяємо 32 адреси. Отримуємо підмережу 10.2.9.128/27. У другій підмережі має бути 18 хостів, виділяємо 32 адреси. Отримуємо підмережу 10.2.9.160/27.

У шостій підмережі знаходиться сервер. Виділяємо 8 адрес, щоб була можливість підключити інші пристрої. Отримуємо підмережу 10.2.9.192/290

У підмережах Net7 – Net9 будуть з’єднуватися маршрутизатори, тому достатньо по 2 адреси хостів на кожну підмережі. Виділяємо по 4 адреси. Отримуємо підмережі 10.2.9.200/30, 10.2.9.204/30 та 10.2.9.208/30 відповідно.

Усі розраховані адреси у табл. 1.5.

Таблиця 1.5

Адресний простір LAN1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № підмережі | Адреса підмережі | Маска підмережі | Адреси хостів у підмережі | Широкомовна адреса | Шаблонна маска |
| Net1 | 10.2.9.0/26 | 255.255.255.192 | 10.2.9.1 - 10.2.9.62 | 10.2.9.63 | 0.0.0.63 |
| Net2 | 10.2.9.64/27 | 255.255.255.224 | 10.2.9.65 - 10.2.9.94 | 10.2.9.95 | 0.0.0.31 |
| Net3 | 10.2.9.96/28 | 255.255.255.240 | 10.2.9.97 - 10.2.9.110 | 10.2.9.111 | 0.0.0.15 |
| Net4 | 10.2.9.128/27 | 255.255.255.224 | 10.2.9.129 - 10.2.9.158 | 10.2.9.159 | 0.0.0.31 |
| Net5 | 10.2.9.160/27 | 255.255.255.224 | 10.2.9.161 - 10.2.9.190 | 10.2.9.191 | 0.0.0.31 |
| Net6 | 10.2.9.192/29 | 255.255.255.248 | 10.2.9.193 - 10.2.9.198 | 10.2.9.199 | 0.0.0.7 |
| Net7 | 10.2.9.200/30 | 255.255.255.252 | 10.2.9.201 - 10.2.9.201 | 10.2.9.203 | 0.0.0.3 |
| Net8 | 10.2.9.204/30 | 255.255.255.252 | 10.2.9.205 - 10.2.9.206 | 10.2.9.207 | 0.0.0.3 |
| Net9 | 10.2.9.208/10 | 255.255.255.252 | 10.2.9.209 - 10.2.9.210 | 10.2.9.211 | 0.0.0.3 |

Розраховуємо вільні адреси у кожній підмережі:

(1.2)

де 62 – кількість адрес хостів у першій підмережі;

55 – задана умовою кількість хостів;

7 – кількість вільних адрес.

Аналогічно розраховуємо вільні адреси для інших підмереж. Результати у табл. 1.6.

Таблиця 1.6

Кількість вільних адрес у підмережах

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Net1 | Net2 | Net3 | Net4 | Net5 | Net6 | Net7 | Net8 | Net9 |
| 7 | 6 | 3 | 10 | 12 | 4 | 0 | 0 | 0 |

Необхідно визначити, скільки ще підмереж і якого обсягу залишились незадіяними. Для цього необхідно розрахувати скільки ще залишилось вільних адрес у мережі. Остання використовувана адреса у підмережах – 10.2.9.211. Отже, необхідно від 255 відняти 211, отримуємо 44 адреси. У результаті обчислень, визначаємо, що залишилось ще 3 незадіяні підмережі, а саме:

* 10.2.9.212/30;
* 10.2.9.216/29;
* 10.2.9.224/27.

На основі даних обчислень, складається кругова діаграма сегментів адрес (рис. 1.7). У діаграмі відображено кількість задіяних та незадіяних адрес по підмережам. Було визначено, що у мережі 10.2.9.0/24 є 3 повністю задіяні підмережі (Net7, Net8 та Net9) і 3 вільні підмережі Net10, Net11 та Net12 з 2, 6 та 30 вільними адресами відповідно.

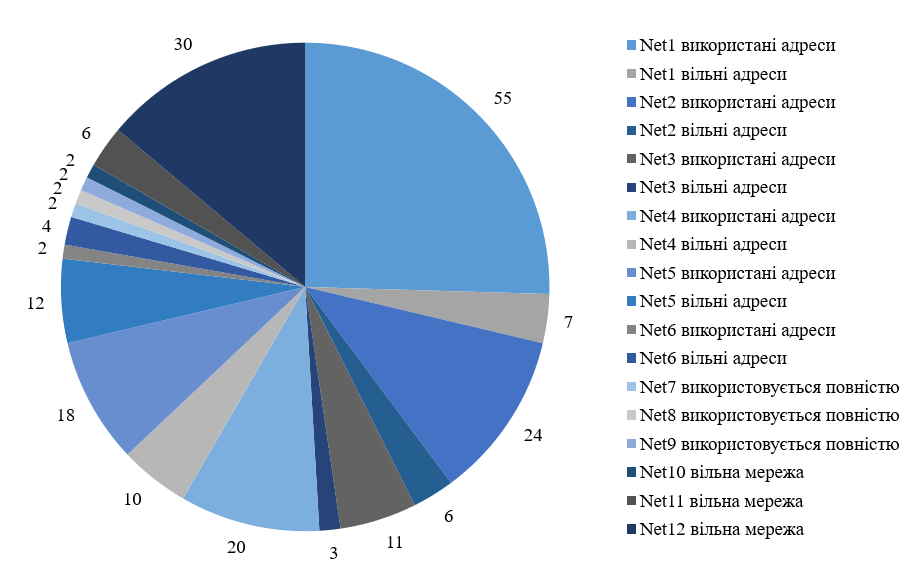


Рис. 1.7 – Діаграма сегментів адрес

1. Розрахунок адресного простору для LAN2:

Для мережі віддаленого офісу надана IP-адреса 172.19.9.0/24. За умовою, адресний простір необхідно розподілити 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. Щоб рівномірно розподілити адреси для мереж із комутаторами, найкраще підходить маска 255.255.255.224 (префікс 27). Усі розрахунки робляться аналогічно до розрахунків адрес LAN1. Отримані результати занесені до табл. 1.7:

Таблиця 1.7

Адресний простір LAN2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № підмережі | Адреса підмережі | Маска підмережі | Адреси хостів у підмережі | Широкомовна адреса | Шаблонна маска |
| Net1 | 172.19.9.0/27 | 255.255.255.224 | 172.19.9.1 – 172.19.9.30 | 172.19.9.31 | 0.0.0.31 |
| Net2 | 172.19.9.32/27 | 255.255.255.224 | 172.19.9.33 – 172.19.9.62 | 172.19.9.63 | 0.0.0.31 |
| Net3 | 172.19.9.64/27 | 255.255.255.224 | 172.19.9.65 – 172.19.9.94 | 172.19.9.95 | 0.0.0.31 |
| Net4 | 172.19.9.96/27 | 255.255.255.224 | 172.19.9.97 – 172.19.9.126 | 172.19.9.127 | 0.0.0.31 |
| Net5 | 172.19.9.128/27 | 255.255.255.224 | 172.19.9.129 – 172.19.9.158 | 172.19.9.159 | 0.0.0.31 |
| № підмережі | Адреса підмережі | Маска підмережі | Адреси хостів у підмережі | Широкомовна адреса | Шаблонна маска |
| Net6 | 172.19.9.160/30 | 255.255.255.252 | 172.19.9.161 – 172.19.9.162 | 172.19.9.163 | 0.0.0.3 |
| Net7 | 172.19.9.164/30 | 255.255.255.252 | 172.19.9.165 – 172.19.9.166 | 172.19.9.167 | 0.0.0.3 |
| Net8 | 172.19.9.168/30 | 255.255.255.252 | 172.19.9.169 – 172.19.9.170 | 172.19.9.171 | 0.0.0.3 |
| Net9 | 172.19.9.172/30 | 255.255.255.252 | 172.19.9.173 – 172.19.9.174 | 172.19.9.175 | 0.0.0.3 |
| Net10 | 172.19.9.176/30 | 255.255.255.252 | 172.19.9.177 – 172.19.9.178 | 172.19.9.179 | 0.0.0.3 |

1. Розрахунок адресного простору для LAN3:

На мережу LAN3 надано 3 IP-адреси: 203.111.18.0, 184.1.0.0 та 14.0.0.0. розподіляємо їх на три мережі Net1, Net2 та Net3 відповідно. Для кожної мережі підбираємо маску 255.255.255.240 (префікс 28), цього достатньо для визначеної умовою кількості хостів. Розрахунки робляться відповідно до розрахунків адрес у LAN1 та LAN2. Отримані результати занесені до табл. 1.8:

Таблиця 1.8

Адресний простір LAN3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № підмережі | Адреса підмережі | Маска підмережі | Адреси хостів у підмережі | Широкомовна адреса | Шаблонна маска |
| Net1 | 203.111.18.0/28 | 255.255.255.240 | 203.111.18.1 – 203.111.18.14 | 203.111.18.15 | 0.0.0.15 |
| Net2 | 184.1.0.0/28 | 255.255.255.240 | 184.1.0.1 – 184.1.0.14 | 184.1.0.15 | 0.0.0.15 |
| Net3 | 14.0.0.0/28 | 255.255.255.240 | 14.0.0.1 – 14.0.0.14 | 14.0.0.15 | 0.0.0.15 |

# **РОЗДІЛ 2 ПОБУДОВА МЕРЕЖІ ТА КОНФІГУРУВАННЯ БАЗОВИХ ФУНКЦІЙ**

## **Побудова мережі та базові налаштування**

Збираємо LAN1 (рис. 2.1). Для побудови, використовуються:

* 4 маршрутизатори Cisco 2911;
* 6 комутаторів Cisco 2960;
* 5 комп’ютерів;
* 1 сервер.

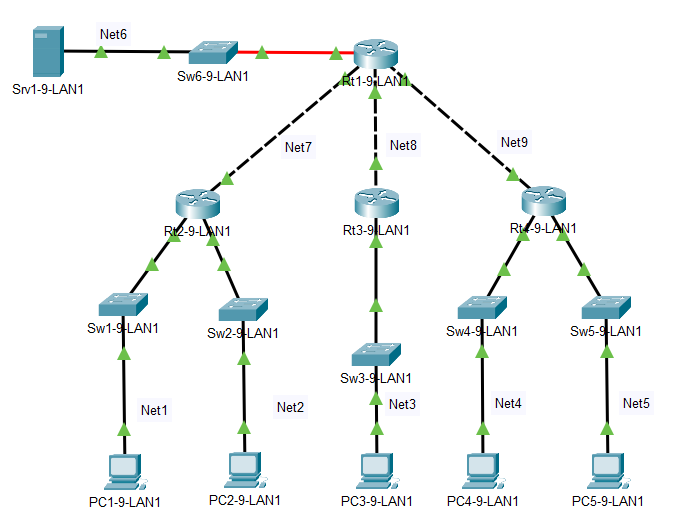


Рисунок 2.1 – Структурна схема зібраної мережі центрального офісу

На маршрутизатор Rt1-9-LAN1 встановлено 2 додаткові модулі, а саме HWIC-1GE-SFP та GLC-LH-SMD. Це необхідно для забезпечення маршрутизатора додатковими портами Gigabit Ethernet.

Між собою маршрутизатори з’єднуються перехресним кабелем. З’єднання між Rt1-9-LAN1 та Sw6-9-LAN1 здійснюється кабелем Fiber. Усі інші з’єднання здійснюються прямим кабелем. Далі надана таблиця адресації LAN1 (табл.2.1):

Таблиця 2.1

Таблиця адресації LAN1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Пристрій | Інтерфейс | ІР-адреса | Маска підмережі | Шлюз за замовчуванням |
| Rt1-9-LAN1 | Gig0/0 | 10.2.9.202 | 255.255.255.252 | Н/П |
| Gig0/1 | 10.2.9.206 | 255.255.255.252 | Н/П |
| Gig0/2 | 10.2.9.210 | 255.255.255.252 | Н/П |
| Gig0/2/0 | 10.2.9.198 | 255.255.255.248 | Н/П |
| Rt2-9-LAN1 | Gig0/0 | 10.2.9.62 | 255.255.255.192 | Н/П |
| Gig0/1 | 10.2.9.94 | 255.255.255.224 | Н/П |
| Gig0/2 | 10.2.9.201 | 255.255.255.252 | Н/П |
| Rt3-9-LAN1 | Gig0/0 | 10.2.9.110 | 255.255.255.240 | Н/П |
| Gig0/1 | 10.2.9.205 | 255.255.255.252 | Н/П |
| Пристрій | Інтерфейс | ІР-адреса | Маска підмережі | Шлюз за замовчуванням |
| Rt4-9-LAN1 | Gig0/0 | 10.2.9.158 | 255.255.255.224 | Н/П |
| Gig0/1 | 10.2.9.190 | 255.255.255.224 | Н/П |
| Gig0/2 | 10.2.9.209 | 255.255.255.252 | Н/П |
| PC1-9-LAN1 | Fa0 | 10.2.9.1 | 255.255.255.192 | 10.2.9.62 |
| PC2-9-LAN1 | Fa0 | 10.2.9.65 | 255.255.255.224 | 10.2.9.94 |
| PC3-9-LAN1 | Fa0 | 10.2.9.97 | 255.255.255.240 | 10.2.9.110 |
| PC4-9-LAN1 | Fa0 | 10.2.9.129 | 255.255.255.224 | 10.2.9.158 |
| PC5-9-LAN1 | Fa0 | 10.2.9.161 | 255.255.255.224 | 10.2.9.190 |
| Srv1-9-LAN1 | Fa0 | 10.2.9.193 | 255.255.255.248 | 10.2.9.198 |

Збираємо LAN2 (рис. 2.2). Для побудови, використовуються:

* 5 маршрутизатори Cisco 2911;
* 5 комутаторів Cisco 2960;
* 5 комп’ютерів.

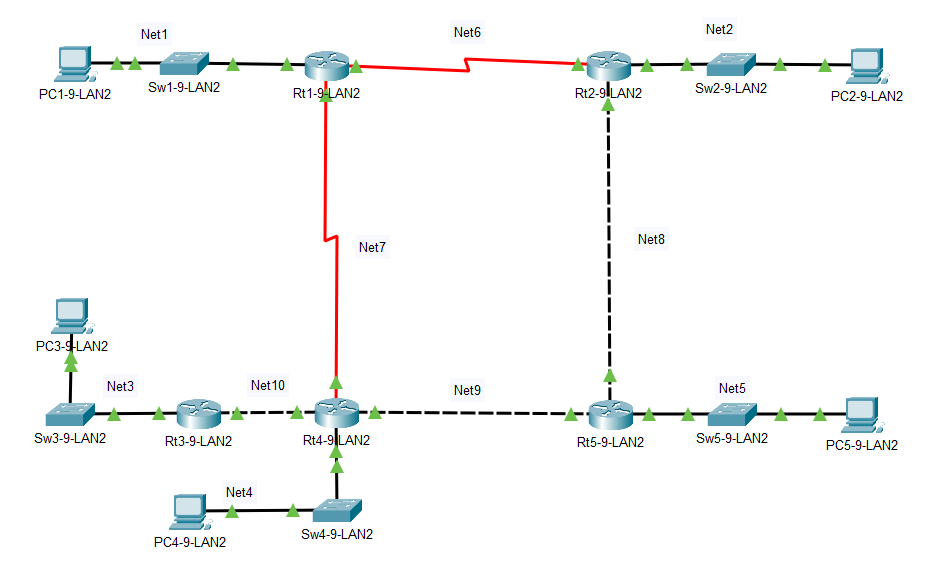


Рисунок 2.2 – Структурна схема зібраної мережі віддаленого офісу

На маршрутизаторах Rt1-9-LAN2, Rt2-9-LAN2 та Rt4-9-LAN2 встановлено по одному додатковому модулю, а саме HWIC-2Т. Це необхідно для забезпечення маршрутизаторів додатковими портами Serial.

Маршрутизатори Rt2-9-LAN2 та Rt4-9-LAN2 з’єднуються з маршрутизатором Rt1-9-LAN2 кабелями Serial DCE. Інші з’єднання між маршрутизаторами здійснене перехресним кабелем. Усі інші з’єднання здійснюються прямим кабелем. Далі надана таблиця адресації LAN2 (табл.2.2):

Таблиця 2.2

Таблиця адресації LAN2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Пристрій | Інтерфейс | ІР-адреса | Маска підмережі | Шлюз за замовчуванням |
| Rt1-9-LAN2 | Gig0/0 | 172.19.9.30 | 255.255.255.224 | Н/П |
| Se0/3/0 | 172.19.9.165 | 255.255.255.252 | Н/П |
| Se0/3/1 | 172.19.9.161 | 255.255.255.252 | Н/П |
| Rt2-9-LAN2 | Gig0/0 | 172.19.9.62 | 255.255.255.224 | Н/П |
| Gig0/2 | 172.19.9.169 | 255.255.255.252 | Н/П |
| Se0/3/0 | 172.19.9.162 | 255.255.255.252 | Н/П |
| Rt3-9-LAN2 | Gig0/0 | 172.19.9.94 | 255.255.255.224 | Н/П |
| Gig0/1 | 172.19.9.177 | 255.255.255.252 | Н/П |
| Rt4-9-LAN2 | Gig0/0 | 172.19.9.178 | 255.255.255.252 | Н/П |
| Gig0/1 | 172.19.9.173 | 255.255.255.252 | Н/П |
| Gig0/2 | 172.19.9.126 | 255.255.255.224 | Н/П |
| Se0/3/0 | 172.19.9.166 | 255.255.255.252 | Н/П |
| Rt5-9-LAN2 | Gig0/0 | 172.19.9.158 | 255.255.255.224 | Н/П |
| Gig0/1 | 172.19.9.174 | 255.255.255.252 | Н/П |
| Gig0/2 | 172.19.9.170 | 255.255.255.252 | Н/П |
| PC1-9-LAN2 | Fa0 | 172.19.9.1 | 255.255.255.224 | 172.19.9.30 |
| PC2-9-LAN2 | Fa0 | 172.19.9.33 | 255.255.255.224 | 172.19.9.62 |
| PC3-9-LAN2 | Fa0 | 172.19.9.65 | 255.255.255.224 | 172.19.9.94 |
| PC4-9-LAN2 | Fa0 | 172.19.9.97 | 255.255.255.224 | 172.19.9.126 |
| PC5-9-LAN2 | Fa0 | 172.19.9.129 | 255.255.255.224 | 172.19.9.158 |

Збираємо LAN3 (рис. 2.3). Для побудови, використовуються:

* 1 маршрутизатор Cisco 2911;
* 3 комутатори Cisco 2960;
* 6 сервери.

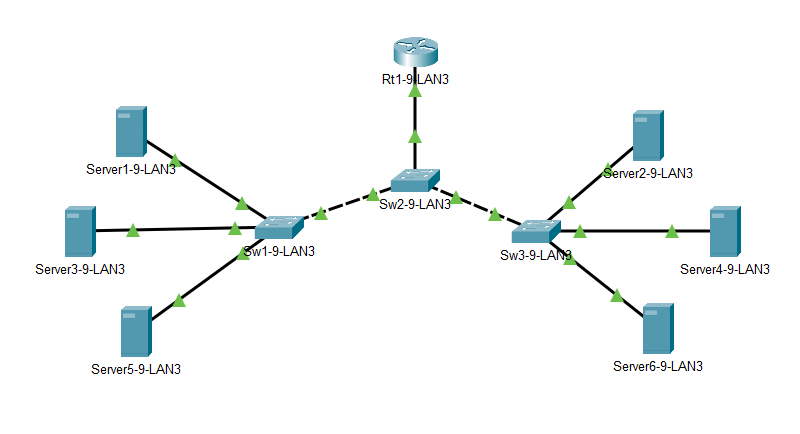


Рисунок 2.3 - Структурна схема зібраної мережі дата центру

Комутатори Sw1-9-LAN3 та Sw3-9-LAN3 з’єднуються з комутатором Sw2- 9-LAN3 перехресними кабелями. Усі інші з’єднання здійснюються прямим кабелем. Далі надана таблиця адресації LAN3 (табл.2.3):

Таблиця 2.3

Таблиця адресації LAN2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Пристрій | Інтерфейс | ІР-адреса | Маска підмережі | Шлюз за замовчуванням |
| Rt1-9-LAN3 | Gig0/0.2 | 184.1.0.14 | 255.255.255.240 | Н/П |
| Gig0/0.3 | 14.0.0.14 | 255.255.255.240 | Н/П |
| Gig0/0.4 | 203.111.18.14 | 255.255.255.240 | Н/П |
| Server1-9-LAN3 | Fa0 | 203.111.18.1 | 255.255.255.240 | 203.111.18.14 |
| Server2-9-LAN3 | Fa0 | 203.111.18.2 | 255.255.255.240 | 203.111.18.14 |
| Server3-9-LAN3 | Fa0 | 184.1.0.1 | 255.255.255.240 | 184.1.0.14 |
| Server4-9-LAN3 | Fa0 | 184.1.0.2 | 255.255.255.240 | 184.1.0.14 |
| Server5-9-LAN3 | Fa0 | 14.0.0.1 | 255.255.255.240 | 14.0.0.14 |
| Server6-9-LAN3 | Fa0 | 14.0.0.2 | 255.255.255.240 | 14.0.0.14 |

Сервера Server1-9-LAN3, Server3-9-LAN3 та Server5-9-LAN3 підключаються до портів Fa0/3, Fa0/13 та Fa0/19 комутатора Sw1-9-LAN3 відповідно. Сервера Server2-9-LAN3, Server4-9-LAN3 та Server6-9-LAN3 підключаються до портів Fa0/18, Fa0/6 та Fa0/2 комутатора Sw3-9-LAN3 відповідно. Комутатор Sw1-9-LAN3 підключається через порт Fa0/11 до порту Fa0/1 комутатора Sw2-9-LAN3. Комутатор Sw3-9-LAN3 підключається через порт Fa0/11 до порту Fa0/2 комутатора Sw2-9-LAN3. Комутатор Sw2-9-LAN3 підключається до маршрутизатора через порт Fa0/3.

## **Вибір та налаштування способу маршрутизації**

Для LAN1, необхідно налаштувати статичну маршрутизацію, так, щоб у таблиці маршрутизації була мінімальна кількість записів. Тому, для маршрутизаторів Rt2-9-LAN1 – Rt4-9-LAN1 буде найрозумнішим рішенням прописати наступні команди відповідно:

#ip route 0.0.0.0 0.0.0.0 10.2.9.202

#ip route 0.0.0.0 0.0.0.0 10.2.9.206

#ip route 0.0.0.0 0.0.0.0 10.2.9.210

На Rt1-9-LAN1 треба налаштувати наступні 6 маршрутів, враховуючи, що буде налаштовано ще один маршрут для виходу з мережі:

#ip route 10.2.9.192 255.255.255.248 10.2.9.193

#ip route 10.2.9.0 255.255.255.192 10.2.9.201

#ip route 10.2.9.64 255.255.255.224 10.2.9.201

#ip route 10.2.9.96 255.255.255.240 10.2.9.205

#ip route 10.2.9.128 255.255.255.224 10.2.9.209

#ip route 10.2.9.160 255.255.255.224 10.2.9.209

Для LAN2 необхідно налаштувати динамічну маршрутизацію RIP. Для цього, на всіх маршрутизаторах треба прописати наступні команди (приклад для маршрутизатора Rt1-9-LAN2):

#router rip

#verison 2

#network 172.19.9.30

#network 172.19.9.161

#network 172.19.9.165

Після команди «network» прописуються ІР-адреси сусідніх до маршрутизатора мереж.

Аналогічно налаштовується динамічна маршрутизація RIP на LAN3.

## **Проектування віртуальних мереж**

У мережі LAN3 необхідно створити 3 віртуальні мережі та включити до них дані за умовою інтерфейси. Спочатку, на комутаторах створюються 3 віртуальні мережі VLAN 2, VLAN 3 та VLAN 4 з іменами VLAN2, VLAN3 та VLAN1 відповідно:

Switch(config)#vlan vlan\_number

Switch(config-vlan)#name vlan\_name

Switch(config-vlan)#exit

Наступним кроком, до створених віртуальних мереж додаються інтерфейси (див. табл. 1.3):

Switch(config)#interface range fa#/start\_of\_range - end\_of\_range

Switch(config)#switchport mode access

Switch(config-if)#switchport access vlan vlan\_number

Switch(config-if)#exit[5]

На комутаторі Sw2-9-LAN3 порт, через який відбувається з’єднання з маршрутизатором налаштовується як транковий:

Switch(config)#interface fa0/3

Switch(config)#switchport mode trunk

Switch(config-if)#switchport trunk vlan 1

## **Конфігурування базових функцій маршрутизатора**

У мережі LAN3 на маршрутизаторі Rt1-9-LAN3 необхідно створити 3 підінтерфейси з ІР-адресами 203.111.18.14, 184.1.0.14 та 14.0.0.14, кожен з яких буде відповідати VLAN 2, VLAN 3 та VLAN 4 відповідно:

#int gi0/0.2

#encapsulation dot1Q 200

#ip address 184.1.0.14 255.255.255.240

#int gi0/0.2

#encapsulation dot1Q 300

#ip address 14.0.0.14 255.255.255.240

#int gi0/0.2

#encapsulation dot1Q 400

#ip address 203.111.18.14 255.255.255.240[6]

## **Підключення** **Frame Relay**

Для забезпечення обміну пакетами між мережами, створюється з’єднання Frame Relay. На шлюзові маршрутизатори, встановлюється по одному додатковому модулю, а саме HWIC-2Т. Це необхідно для забезпечення маршрутизаторів додатковими портами Serial. Маршрутизатори підключаються до комутатора Frame Relay кабелями Serial DCE (рис. 2.4).

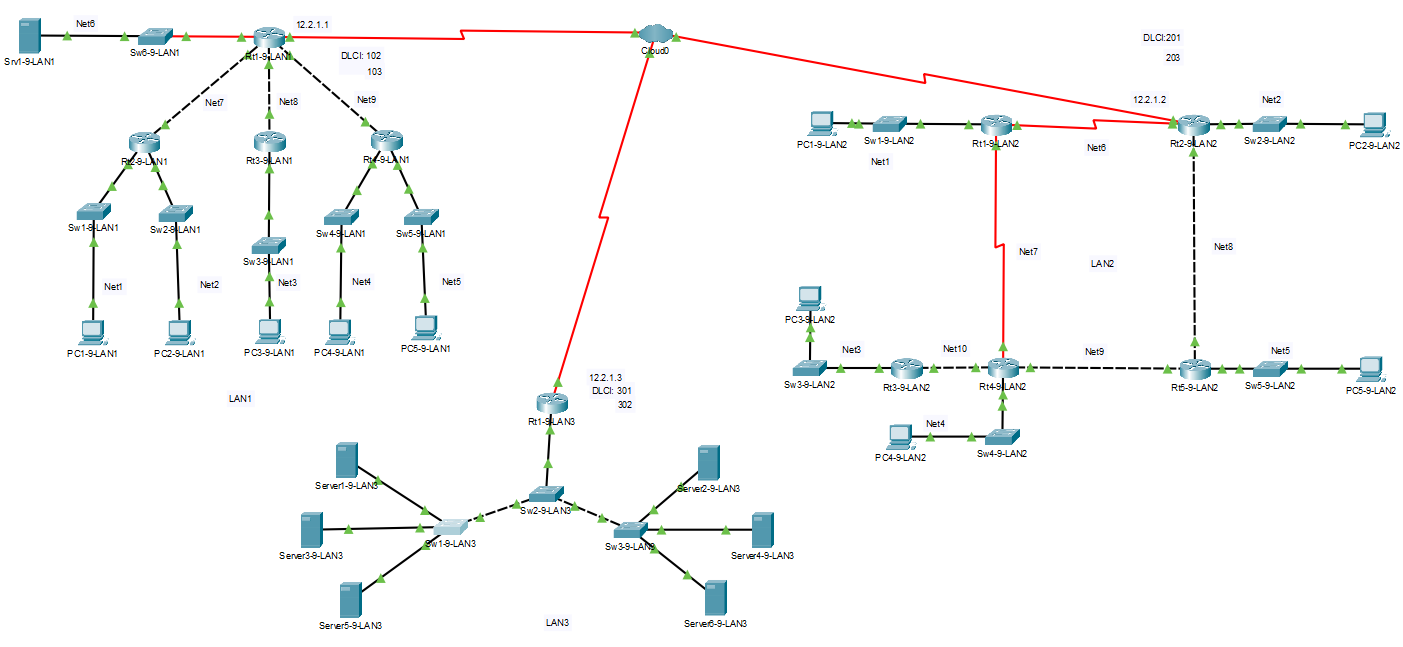


Рисунок 2.4 - З’єднання Frame Relay

Далі надана таблиця адресації Frame Relay (табл.2.4):

Таблиця 2.4

Таблиця адресації Frame Relay

|  |  |  |  |
| --- | --- | --- | --- |
| Пристрій | Інтерфейс | ІР-адреса | Маска підмережі |
| Rt1-9-LAN1 | Se0/1/0 | 12.2.1.1 | 255.255.255.255 |
| Rt2-9-LAN2 | Se0/3/1 | 12.2.1.2 | 255.255.255.255 |
| Rt1-9-LAN3 | Se0/3/0 | 12.2.1.3 | 255.255.255.255 |

Далі налаштовуються Frame Relay та його інтерфейси (рис. 2.5 - 2.8):

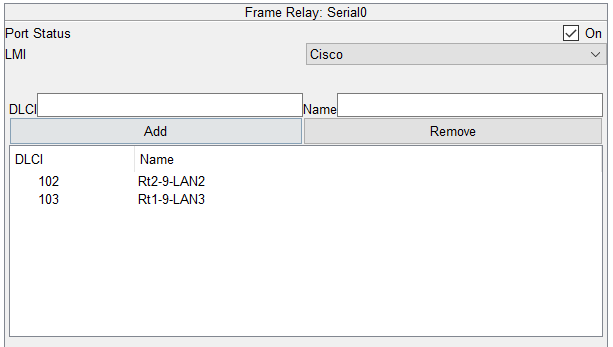


Рисунок 2.5 – Налаштування порту Frame Relay Serial0

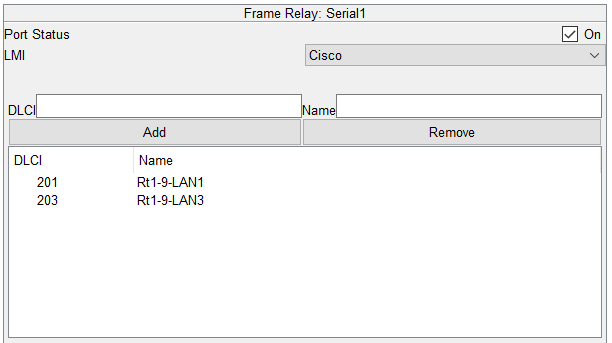


Рисунок 2.6 - Налаштування порту Frame Relay Serial1

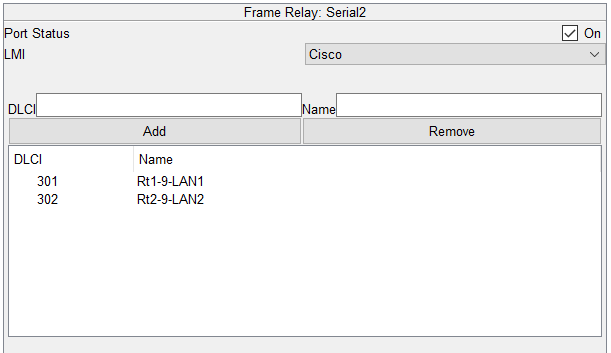


Рисунок 2.7 – Налаштування порту Frame Relay Serial2

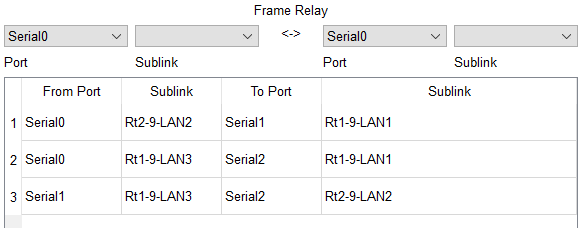


Рисунок 2.8 – Налаштування Frame Relay

Після налаштування базових функцій Frame Relay, необхідно забезпечити маршрутизацію. Налаштовуємо динамічну маршрутизацію RIP. На шлюзових маршрутизаторах прописуються наступні команди:

#router rip

#verison 2

#network 12.2.1.0

Це забезпечить передачу пакетів між локальними мережами.

## **Конфігурування додаткових функцій маршрутизаторів (****DHCP, NAT тощо)**

У мережі LAN1 необхідно налаштувати DHCP для підмереж Net1 – Net5. Для цього, на маршрутизаторах Rt2-9-LAN1 – Rt4-9-LAN1 необхідно прописати наступні команди (наведений приклад для Rt2-9-LAN1 gi0/0):

#int gi0/0

#ip address 10.2.9.62 255.255.255.192

#exit

#ip dhcp pool DHCP1

#network 10.2.9.0 255.255.255.192

#default-router 10.2.9.62

#dns-server 8.8.8.8

#exit

# ip dhcp excluded-address 10.2.9.62[7]

Після виповнення даних команд, на вкладці комп’ютера «Desktop» у додатку «IP Configuration» та його розділі «IP Configuration» необхідно переключити радіо-кнопку з «Static» на «DHCP».

Також, на шлюзових маршрутизаторах необхідно налаштувати NAT, причому для LAN1, налаштовується статичний NAT (для підмереж Net1 – Net5) і PAT для сервера, а в LAN2 налаштовується динамічний NAT. Усі команди прописуються на шлюзових маршрутизаторах.

Налаштування статичного NAT:

#ip route 0.0.0.0 0.0.0.0 12.2.1.2

#int se0/1/0

#ip nat outside

#exit

#int range gi0/0-2

#ip nat inside

#exit

#int gi0/2/0

# ip nat inside

#ip access-list standard FOR-NAT

#permit 10.2.9.0 0.0.0.63

#permit 10.2.9.64 0.0.0.31

#permit 10.2.9.96 0.0.0.15

#permit 10.2.9.128 0.0.0.31

#permit 10.2.9.160 0.0.0.31

#permit 10.2.9.192 0.0.0.7

#ip nat inside source list FOR-NAT int se0/1/0 overload

Налаштування PAT здійснюється після налаштування статичного NAT, тому більша частина команд вже прописана при налаштуванні статичного NAT. Залишається прописати наступну команду:

#ip nat inside source static tcp 10.2.9.193 80 12.2.1.1 80[8]

Налаштування динамічного NAT:

#access-list 1 permit 172.19.9.0 0.0.0.255

#int se0/3/1

#ip nat outside

#exit

#int se0/3/0

#ip nat inside

#int gi0/0

#ip nat inside

#exit

#int gi0/2

# ip nat inside

#exit

#ip route 0.0.0.0 0.0.0.0 12.2.1.3

#ip nat pool DNAT 12.2.1.2 12.2.1.2 netmask 255.255.255.252

#ip nat inside source list 1 pool DNAT

# **РОЗДІЛ 3 ЗАХИСТ ТА ТЕСТУВАННЯ МЕРЕЖІ**

## **Налаштування захисту та конфігурування функцій безпеки(налаштування паролів, ACL)**

На всіх маршрутизаторах необхідно встановити паролі на консольне з’єднання (cisco67890) та на привілейований режим (cisco12345). Для цього, на кожному маршрутизаторі прописуються наступні команди:

#line console 0

#password cisco67890

#login

#exit

#enable secret cisco12345

Для LAN1 необхідно налаштувати ACL згідно до табл. 1.1. Перший ACL налаштовуємо на Rt2-9-LAN1:

#access-list 1 deny 10.2.9.64 0.0.0.31

#access-list 1 permit any

Прив’язуємо ACL до інтерфейсу gi0/1:

#int gi0/1

#ip access-group 1 in

Другий ACL налаштовуємо на Rt1-9-LAN1:

#access-list 2 deny 10.2.9.128 0.0.0.31

#access-list 2 permit any

Прив’язуємо ACL до інтерфейсу gi0/2/0:

#int gi0/2/0

#ip access-group 2 in

Третій ACL налаштовуємо на Rt2-9-LAN1:

#access-list 3 deny 10.2.9.160 0.0.0.31

#access-list 3 permit any

Прив’язуємо ACL до інтерфейсу gi0/1:

#int gi0/1

#ip access-group 3 out

Далі налаштовуємо розширені ACL. Перший розширений список налаштовуємо на Rt5-9-LAN1:

#ip access-list extended HTTP\_ONLY

#deny tcp 10.2.9.160 0.0.0.31 10.2.9.96 0.0.0.15 eq www

#ip access-list extended NETBIOS

#deny tcp 10.2.9.160 0.0.0.31 10.2.9.96 0.0.0.15 eq 137

#ip access-list extended SNMP

#deny udp 10.2.9.160 0.0.0.31 10.2.9.96 0.0.0.15 eq snmp

Прив’язуємо ACL до інтерфейсу gi0/1:

#int gi0/1

#ip access-group HTTP\_ONLY in

# ip access-group NETBIOS in

# ip access-group SNMP in

Другий розширений список налаштовуємо на Rt2-9-LAN1:

#ip access-list extended IMAP

#deny tcp 10.2.9.0 0.0.0.63 10.2.9.64 0.0.0.31 eq 143

#ip access-list extended PING

#deny icmp 10.2.9.0 0.0.0.63 10.2.9.64 0.0.0.31 echo

#permit ip any any

#ip access-list extended TELNET

#deny tcp 10.2.9.0 0.0.0.63 10.2.9.64 0.0.0.31 eq telnet

Прив’язуємо ACL до інтерфейсу gi0/0:

#int gi0/0

#ip access-group IMAP in

# ip access-group PING in

# ip access-group TELNET in

## **Налаштування віддаленого доступу до активного обладнання**

Необхідно налаштувати доступ через протокол SSH до шлюзових маршрутизаторів. Для цього, на шлюзових маршрутизаторах треба встановити дату та час, вказати домен, згенерувати ключі, створити обліковий запис та пароль до нього, активувати протокол ААА. Після цього, налаштувати параметри сесії протоколу SSH. Зробити це можна за допомогою наступних команд:

#clock set hh:mm:ss day mon year

#ip domain name domain.local

#crypto key generate rsa

#service password-encryption

#username admin privilege 15 secret Admin1

#aaa new-model

#line vty 0 4

#transport input ssh

#logging synchronous

#exec-timeout 60 0

## **Тестування роботи розробленої мережі**

Для перевірки працездатності розробленої мережі необхідно запустити пакети всередині мереж та між мережами. При тестуванні першої локальної мережі, слід урахувати налаштовані списки доступу.

Тестування LAN1:

Відправка пакетів з PC1-9-LAN1 на PC2-9-LAN1 має завершитись невдачею, через налаштований ACL (рис.3.1):

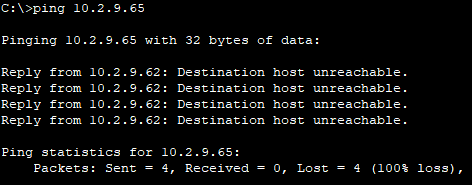


Рисунок 3.1 - Відправка пакетів з PC1-9-LAN1 на PC2-9-LAN1

Відправка пакетів з PC1-9-LAN1 на PC3-9-LAN1 має завершитись успішно (рис.3.2):

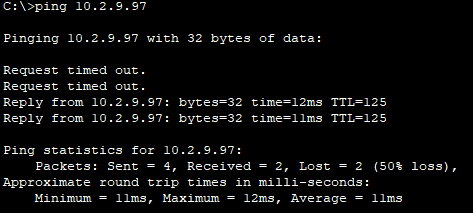


Рисунок 3.2 - Відправка пакетів з PC1-9-LAN1 на PC3-9-LAN1

Аналогічно перевіряємо інші з’єднання. Тестування завершились успішно. З’єднання, на які налаштовано списки доступу, завершились невдачею.

Тестування LAN2:

У другій локальній мережі усі відправлені пакети мають повернутися назад до відправника успішно.

Відправка пакетів з PC1-9-LAN2 на PC2-9-LAN2 має завершитись успішно (рис.3.3):

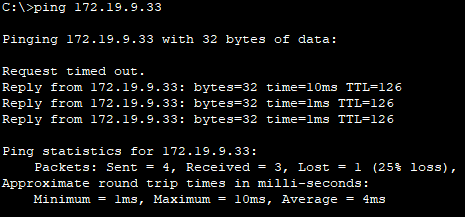


Рисунок 3.3 - Відправка пакетів з PC1-9-LAN2 на PC2-9-LAN2

Відправка пакетів з PC1-9-LAN2 на PC3-9-LAN2 має завершитись успішно (рис.3.4):

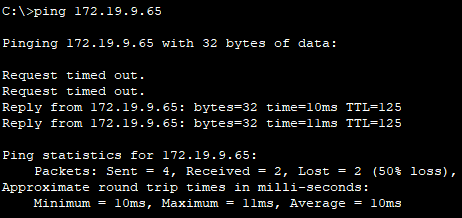


Рисунок 3.4 - Відправка пакетів з PC1-9-LAN2 на PC3-9-LAN2

Відправка пакетів з PC1-9-LAN2 на PC4-9-LAN2 має завершитись успішно (рис.3.5):

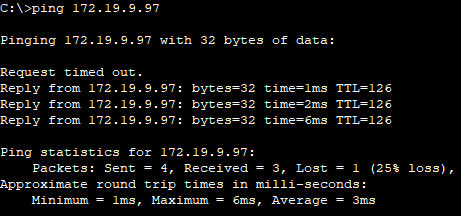


Рисунок 3.5 - Відправка пакетів з PC1-9-LAN2 на PC4-9-LAN2

Відправка пакетів з PC1-9-LAN2 на PC5-9-LAN2 має завершитись успішно (рис.3.6):

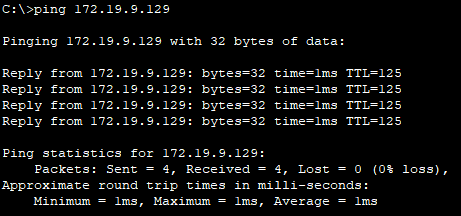


Рисунок 3.6 - Відправка пакетів з PC1-9-LAN2 на PC5-9-LAN2

Аналогічно перевіряємо інші з’єднання. Тестування завершились успішно.

Тестування LAN3:

У другій локальній мережі усі відправлені пакети мають повернутися назад до відправника успішно.

Відправка пакетів з Server1-9-LAN3 на Server2-9-LAN3 має завершитись успішно (рис.3.7):

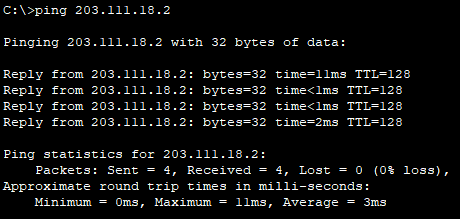


Рисунок 3.7 - Відправка пакетів з Server1-9-LAN3 на Server2-9-LAN3

Відправка пакетів з Server1-9-LAN3 на Server3-9-LAN3 має завершитись успішно (рис.3.8):

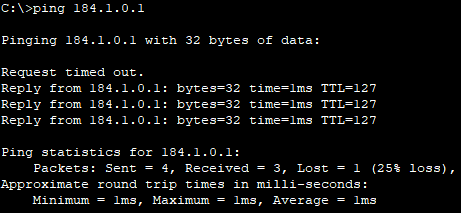


Рисунок 3.8 - Відправка пакетів з Server1-9-LAN3 на Server3-9-LAN3

Відправка пакетів з Server1-9-LAN3 на Server4-9-LAN3 має завершитись успішно (рис.3.9):

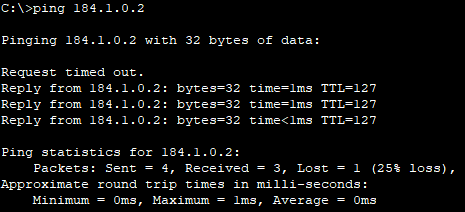


Рисунок 3.9 - Відправка пакетів з Server1-9-LAN3 на Server4-9-LAN3

Відправка пакетів з Server1-9-LAN3 на Server5-9-LAN3 має завершитись успішно (рис.3.10):

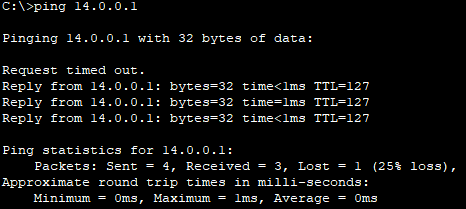


Рисунок 3.10 - Відправка пакетів з Server1-9-LAN3 на Server5-9-LAN3

Відправка пакетів з Server1-9-LAN3 на Server6-9-LAN3 має завершитись успішно (рис.3.11):

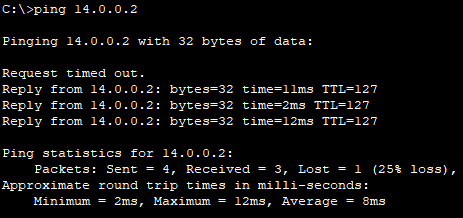


Рисунок 3.11 - Відправка пакетів з Server1-9-LAN3 на Server5-9-LAN3

Аналогічно перевіряємо інші з’єднання. Тестування завершились успішно.

Тестування Frame Relay:

Буде відправлено 6 тестових пакетів:

1. З LAN1 в LAN2;
2. З LAN1 в LAN3;
3. З LAN2 в LAN1;
4. З LAN2 в LAN3;
5. З LAN3 в LAN1;
6. З LAN3 в LAN2.

Відправка пакетів з LAN1 в LAN2 має завершитись успішно (рис.3.12):



Рисунок 3.12 - Відправка пакетів з LAN1 в LAN2

Відправка пакетів з LAN1 в LAN3 має завершитись успішно (рис.3.13):



Рисунок 3.13 - Відправка пакетів з LAN1 в LAN3

Відправка пакетів з LAN2 в LAN1 має завершитись успішно (рис.3.14):



Рисунок 3.14 - Відправка пакетів з LAN2 в LAN1

Відправка пакетів з LAN2 в LAN3 має завершитись успішно (рис.3.15):



Рисунок 3.15 - Відправка пакетів з LAN2 в LAN3

Відправка пакетів з LAN3 в LAN1 має завершитись успішно (рис.3.16):



Рисунок 3.16 - Відправка пакетів з LAN3 в LAN1

Відправка пакетів з LAN3 в LAN2 має завершитись успішно (рис.3.17):



Рисунок 3.17 - Відправка пакетів з LAN3 в LAN2

За результатами тестування робимо висновок, що пакети успішно відправляються з дата центру до мереж 1 та 2 і назад. Проте між мережами 1 та 2 відправлення пакетів завершається невдачею.

# **ВИСНОВКИ**

Сучасні локальні мережі забезпечують зв’язок між комп’ютерами на великих та малих відстанях. Сучасні технології дозволяють забезпечувати не тільки якісний зв’язок, вони також забезпечують безпеку такого з’єднання.

Налаштування паролів на обладнанні, забезпечить мінімальний захист мережі. Для більш якісного захисту можна використовувати ACL та забороняти проходження стороннього трафіку через мережі. Також гарним покращенням безпеки обладнання є захист віддаленого доступу до нього.

Щоб захистити пристрої від стороннього підключення, можна відключати незадіяні порти. Також можна ставити модулі-пластини на вільні роз’єми, що ускладнить стороннє підключення до портів.

Загалом, потрібно захищати мережу якнайкраще, аби забезпечити безпеку конфіденціальних даних користувачів мережі.

# **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Комп’ютерні мережі та їх класифікація [Електронний ресурс] // Електронний посібник "Комп'ютерні мережі". – 2011. – Режим доступу до ресурсу: http://km.ptngu.com/lections/2.html;
2. Локальні мережі та IT- інфраструктура [Електронний ресурс] // ІнфоТел-Дистрибуція. – 2011. – Режим доступу до ресурсу: https://infotel.ua/ua/local-aria-network-data-transfering;
3. Глобальні мережі [Електронний ресурс] // Піщанський НВК «ЗОШ І-ІІІ ступенів-гімназія». – 2020. – Режим доступу до ресурсу: https://step.org.ua/konspekt/lanwan/tema3;
4. Методичні вказівки до виконання курсової робіти з дисципліни «Комп’ютерні системи та мережі (Рівень D - Безпека комп`ютерних систем)» для здобувачів першого (бакалаврського) рівня освіти спеціальності 125 «Кібербезпека» за освітньою програмою «Кібербезпека у фінансових технологіях» / уклад. Вайганг Г.О., Комар К.В.; Київ: ДВНЗ «Університет банківської справи» - 2019.- 23 с;
5. Настройка vlan на cisco [Електронний ресурс] // Snakeproject.ru. – 2013. – Режим доступу до ресурсу: http://snakeproject.ru/rubric/article.php?art=cisco\_vlan;
6. Cisco VLAN — настройка vlan на маршрутизаторе Cisco [Електронний ресурс] // Админия. – 2013. – Режим доступу до ресурсу: http://www.adminia.ru/cisco-vlan-nastroyka-vlan-na-marshrutizatore-cisco/;
7. 11.Видео уроки Cisco Packet Tracer. Курс молодого бойца. DHCP [Електронний ресурс] // NetSkills. Видеоуроки. Cisco, zabbix, linux. – 2014. – Режим доступу до ресурсу: https://www.youtube.com/watch?v=MoElaNJn-9w&list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9&index=12;
8. 12.Видео уроки Cisco Packet Tracer. Курс молодого бойца. NAT [Електронний ресурс] // NetSkills. Видеоуроки. Cisco, zabbix, linux.. – 2014. – Режим доступу до ресурсу: https://www.youtube.com/watch?v=6d2kvuWuyI0&list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9&index=13;

# **ДОДАТОК А ТЕХНІЧНЕ ЗАВДАННЯ**

На розробку і конфігурування комп’ютерної мережі

1. Область застосування — комп’ютерні мережі.
2. Основа розробки — робочий навчальний план дисципліни.
3. Мета та експлуатаційне призначення:
   1. мета - отримання практичних навичок проектування та конфігурування комп’ютерних мереж;
   2. призначення розробки — навчальна курсова робота із дисципліни «Комп’ютерні системи та мережі (Рівень D - Безпека комп`ютерних систем)»;
4. Джерела розробки — індивідуальне завдання на курсовий проект із дисципліни, технічні рекомендації щодо проектування локальних та розподілених мереж та інші технічні матеріали для налаштування окремих компонентів мережі.
5. Технічні вимоги:
   1. Мережа складається з трьох окремих LAN, що об’єднуються WAN мережею, побудованою на основі технології віртуальних каналів.
   2. Вимоги для проектування LAN1
      1. Адреса мережі 10.2.9.0
      2. Складається з п’яти сегментів, кількість робочих станцій в кожному з яких становить: 55, 24, 11, 20, 18.
      3. Розподіл адресного простору має бути оптимальним;
      4. Для об’єднання окремих сегментів використовуються 4 маршрутизатори;
      5. З’єднання між маршрутизаторами здійснюються за допомогою скрученої пари;
      6. Для обмеження проходження трафіку з одного сегменту в інший мають бути застосовані стандартні і розширені ACL. Стандартні списки мають заборонити проходження трафіку з мереж NET2 NET4 та NET5 відповідно до мереж NET1 NET6 та NET2. Розширені ACL мають заборонити проходження трафіку протоколів HTTP, NETBIOS та SNMP з NET5 до NET3 та IMAP PING та TELNET з NET1 до NET2. ACL необхідно розмістити в найбільш вдалому місці.
      7. У середині мережі використовується статична маршрутизація.
      8. На маршрутизаторах Rt2-Rt4 налаштувати DHCP-сервіс і забезпечити динамічне призначення адрес хостам в мережах Net1-Net5.
      9. На маршрутизаторі Rt1 налаштовано сервіс трансляції адрес NAT.
   3. Вимоги для проектування LAN2
      1. Адреса мережі 172.19.9.0/24
      2. Складається з 5 сегментів, в яких розташовані ПК користувачів.
      3. Розподілити адресний простір таким чином: в мережах, що з’єднують маршрутизатори, використовувати префікс 30 (маска 255.255.255.252), весь вільний простір, що залишається, рівномірно поділити між мережами, в яких розташовані Switch1- Switch5.
      4. З’єднання між маршрутизаторами Rt1-Rt4 та Rt1-Rt2 здійснюється за допомогою послідовних інтерфейсів з використанням протоколів канального рівня HDLC та РРР відповідно. Інші з’єднання виконуються за допомогою скрученої пари.
      5. Під’єднання мережі LAN2 до мережі WAN виконується через маршрутизатор Rt2.
      6. В середині мережі використовується динамічна маршрутизація на основі протоколу RIP.
      7. На маршрутизаторі Rt1 налаштовано сервіс трансляції адрес NAT.
   4. Вимоги для проектування LAN3
      1. Реалізована на основі комутаторів Catalyst 2960 з підтримкою технології віртуальних мереж.
      2. Поділена на три віртуальні сегменти, кожний з яких містить по два сервери.
      3. На комутаторах Sw1, Sw2 до Vlan 2 належать порти FastEthernet13-FastEthernet17 та FastEthernet6-FastEthernet8 відповідно, до Vlan 3 FastEthernet19-FastEthernet22 та FastEthernet2-FastEthernet5 відповідно.
      4. З’єднання між комутаторами здійснюються за допомогою скрученої пари і технології Gigabit Ethernet.
      5. В віртуальних мережах VLAN1, VLAN2 та VLAN3 використовуються адреси 203.111.18.0, 184.1.0.0 та 14.0.0.0 відповідно.
   5. Вимоги для проектування WAN
      1. Об’єднання локальних мереж здійснюється за допомогою Frame Relay комутатора з використанням топології Full Mesh.
      2. Адреси інтерфейсів маршрутизаторів, що під’єднані до Frame Relay мережі, належать до мережі з адресою 12.2.1.0/24
      3. З’єднання між локальними мережами здійснюється за допомогою послідовних інтерфейсів.
   6. Загальні вимоги до налаштувань маршрутизаторів
      1. Встановити на всіх маршрутизаторах паролі на консольне з’єднання та на привілейований режим.
      2. Налаштувати доступ через протокол SSH до шлюзових маршрутизаторів.
6. Апаратні вимоги - використання обладнання фірми Cisco
7. Текстова документація розробленої мережі повинна відповідати 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 Молібог А. С.