**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 2 курсу 207-Кбс групи

спеціальності «Кібербезпека»

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

Гордєєв О. О.

(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)»;

1. 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.
2. Технічні вимоги
   1. Мережа складається з трьох окремих LAN, що об’єднуються WAN мережею, побудованою на основі технології віртуальних каналів.
   2. Вимоги для проектування LAN1
      1. Адреса мережі 192.168.19.0
      2. Складається з п’яти сегментів, кількість робочих станцій в кожному з яких становить: 28, 10, 12, 50, 61.
      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 NET1 NET3 та NET3 відповідно до

мереж NET2 NET4 та NET6. Розширені ACL мають заборонити проходження трафіку протоколів DNS, FINGER та FTP з NET4 до NET1 та HTTP HTTPS та ICMP з NET5 до NET4. ACL необхідно розмістити в найбільш вдалому місці.

* + 1. У середині мережі використовується статична маршрутизація.
    2. На маршрутизаторах Rt2-Rt4 налаштувати DHCP-сервіс і забезпечити динамічне призначення адрес хостам в мережах Net1- Net5.
    3. На маршрутизаторі Rt1 налаштовано сервіс трансляції адрес NAT.
  1. Вимоги для проектування LAN2
     1. Адреса мережі 10.6.19.0/24
     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 Rt2-Rt3 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 Rt1.
     6. В середині мережі використовується динамічна маршрутизація на основі протоколу EIGRP.
     7. На маршрутизаторі Rt1 налаштовано сервіс трансляції адрес NAT.
  2. Вимоги для проектування LAN3
     1. Реалізована на основі комутаторів Catalyst 2960 з підтримкою технології віртуальних мереж.
     2. Поділена на три віртуальні сегменти, кожний з яких містить по два сервери.
     3. На комутаторах Sw1 Sw3 до Vlan 2 належать порти FastEthernet3- FastEthernet7 та FastEthernet6-FastEthernet9 відповідно, до Vlan 3 FastEthernet9-FastEthernet15 та FastEthernet15-FastEthernet18 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 181.218.0.0 205.186.160.0 та 186.165.0.0 відповідно.
  3. 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 32.2.0.0/16
     3. З’єднання між локальними мережами здійснюється за допомогою послідовних інтерфейсів.
  4. 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.

1. Апаратні вимоги - використання обладнання фірми Cisco
2. Текстова документація розробленої мережі повинна відповідати діючим стандартам України.
3. Стадії та етапи розробки мережі включать розробку та від лагодження окремих LAN та об’єднання LAN1-4 за допомогою WAN мережі.

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ**

**Варіант 19**

Спеціальність: «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**

Хоружий Андрій Олегович \_

(прізвище, ім’я, по батькові)

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

**2.** **Термін здачі 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.

5. Вихідні дані:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| LAN №1 | | | підмережі | ІР-адреса | | | | Кількість хостів | | | | | | | | | |
| Net1 | Net2 | | Net3 | | | Net4 | | Net5 | |
| 192.168.19.0 | | | | 28 | 10 | | 12 | | | 50 | | 61 | |
| ст. ACL | відпр. | | | | отр. | відпр. | | отр. | | | відпр. | | отр. | |
| Net5 | | | | Net2 | Net3 | | Net4 | | | Net1 | | Net6 | |
| розш. ACL | відпр. | | | | отр. | № прот | | отр. | | | відпр. | | № прот | |
| Net2 | | | | Net3 | 6,9,12 | | Net3 | | | Net1 | | 2,7,11 | |
| LAN №2 | | | № сх. | ІР-адреса | | Serial HDLC | | | Serial PPP | | Шлюз | | Тип маршрутизації | | | | |
| 9 | 10 .6.19.0/24 | | | | Rt4-Rt5 | Rt2-Rt5 | | Rt1 | | EIGRP | | | | |
| LAN №3 | Net1 | | | Net2 | | Net3 | | | Switch1 | | | | | Switch3 | | | |
| Vlan 2 | | Vlan 3 | | | Vlan 2 | | Vlan 3 | |
| 181.218.0.0 | | | 205.186.160.0 | | 186.165.0.0 | | | 7-10 | | 12-14 | | | 20-22 | | 2-7 | |

6. Дата видачі завдання “ 16 вересня ” 2020 р.

ЗМІСТ

[**АНОТАЦІЯ** 3](#_Toc58983566)

[**ВСТУП** 4](#_Toc58983567)

[**РОЗДІЛ І. Аналіз технічної складової** 6](#_Toc58983568)

[1.1 Аналіз сучасних технологій локальних та глобальних мереж 6](#_Toc58983569)

[1.1.1 Фізичні топології локальних мереж 13](#_Toc58983570)

[1.1.2 Топології глобальних мереж 17](#_Toc58983571)

[1.2 Розрахунок адресного простору 21](#_Toc58983572)

[1.2.1 Розподіл адрес для мережі центрального офісу (Lan1) 21](#_Toc58983573)

[1.2.2 Розподіл адрес для мережі офісу з віддаленим доступом (Lan2) 26](#_Toc58983574)

[1.2.3 Розподіл адрес для мережі дата-центру (Lan3) 27](#_Toc58983575)

[1.3 Налаштування маршрутизації (Lan1) 28](#_Toc58983576)

[**РОЗДІЛ ІІ. Конфігурування мережевого обладнання** 31](#_Toc58983577)

[2.1 Конфігурування базових функцій маршрутизаторів 31](#_Toc58983578)

[2.1.1 Контекст глобального конфігурування. 33](#_Toc58983579)

[2.2 Проектування віртуальних мереж VLAN 36](#_Toc58983580)

[2.2.1 Проектування віртуальної мережі VLAN для мережі дата-центру (Lan3) 39](#_Toc58983581)

[2.3 Конфігурування базових функцій комутаторів LAN3 40](#_Toc58983582)

[**РОЗДІЛ ІІІ. Налаштування віддаленого доступу та захисту на активне обладнання** 43](#_Toc58983583)

[3.1 Налаштування захисту та конфігурування функцій безпеки 43](#_Toc58983584)

[3.2 Налаштування віддаленого доступу до активного обладнання 45](#_Toc58983585)

[3.3 Моделювання та тестування роботи розробленої мережі 47](#_Toc58983586)

[**ВИСНОВКИ** 50](#_Toc58983587)

[**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ** 51](#_Toc58983588)

[**ДОДАТОК А** 53](#_Toc58983589)

[**ДОДАТОК Б** 54](#_Toc58983590)

[**ДОДАТОК В** 55](#_Toc58983591)

# АНОТАЦІЯ

Курсова робота з дисципліни «Комп’ютерні системи та мережі (Рівень D - Безпека комп`ютерних систем)» передбачає розробку корпоративної мережі, конфігурування активного обладнання та комп’ютерне моделювання з використанням сучасних симуляторів комп’ютерних мереж. У даній курсовій роботі наведено огляд підходів до побудови корпоративної мережі. Проведено аналіз обладнання CISCO ( Cisco Packet Tracer). У якості демонстраційної частини розроблено модель корпоративної мережі на базі статичної маршрутизації в LAN1, EIRP маршрутизації в LAN2 та проектування VLAN в мережі :LAN3. Виконані потрібні налаштування та перевірена її працездатність.

Проект містить 54 сторінок тексту, 17 рисунків, 13 таблиць, 1 формула, 15 літературних джерел. Ключові слова: корпоративна мережа, CISCO, Cisco Packet Tracer, EGIRP, віртуальна мережа VLAN, мережа LAN1, мережа LAN2, мережа LAN3, статична маршрутизація, протокол TFTP, протокол NETBIOS, розрахунок Net.

# ВСТУП

Сучасні технології передачі даних надають своїм користувачам широкі можливості по організації різних видів послуг і сервісів:

* організація електронного документообігу й ведення загальних архівів документів;
* організація корпоративної телефонної мережі з єдиним планом нумерації; організація систем конференц-зв’язку, у тому числі відеоконференція.
* зв’язку; побудова розподілених систем відеоспостереження з єдиним центром
* зберігання даних; організація дистанційного доступу до файлів і серверів з базами даних;
* підключення до мережі Інтернет з можливістю організації єдиної корпоративної політики інформаційної безпеки і т. ін.

Перераховані можливості дозволяють спростити процедури по керуванню внутрішніми бізнес-процесами й надають компанії ряд конкурентних переваг, а саме забезпечуються: простота керування компанією, прозорість роботи компанії, оперативний контроль діяльності всіх служб і структурних підрозділів, доступ до всіх інформаційних ресурсів підприємства в реальному часі, оперативний зв’язок; економія засобів на міжнародних й міжміських дзвінках.

Більшість інформаційних рішень, що застосовуються сьогодні, носить розподілений характер і вимагає наявності на підприємстві або в організації високопродуктивної корпоративної мережі передачі даних.

Основним завданням корпоративної мережі є забезпечення взаємодії системних додатків та організація доступу до них віддалених користувачів.

Тому корпоративна мережа, як правило, є територіально розподіленою, тобто такою, що об’єднує офіси, підрозділи й інші структури, що перебувають на значному віддаленні одні від одних. Часто вузли корпоративної мережі виявляються розташованими в різних містах, а іноді й країнах.

Таким чином, корпоративна мережа – це складна система, що включає тисячі найрізноманітніших компонентів: комп’ютери різних типів, системне й прикладне програмне забезпечення, мережеві адаптери, концентратори, комутатори й маршрутизатори, кабельна система. Основне завдання полягає в тому, щоб ця громіздка й досить дорога система якнайкраще справлялася з обробкою потоків інформації, що циркулюють між співробітниками підприємства й дозволяла приймати їм своєчасні й раціональні рішення, що забезпечують виживання підприємства у жорсткій конкурентній боротьбі.

Оскільки широке застосування комп’ютерних мереж у наш час є незаперечним фактом, тому тема даної роботи є актуальною.

Метою роботи є проектування мереж центрального та віддаленого офісів підприємства з використанням списків контролю доступу та налаштуванням динамічної маршрутизації.

В процесі виконання роботи потрібно вирішити наступні завдання:

1. Розрахувати адресний простір мережі центрального офісу.
2. Розподілити адресний простір мережі віддаленого офісу.
3. Налаштували VLAN мережі дата-центру
4. Налаштувати динамічне присвоєння адрес на маршрутизаторах
5. Налаштувати маршрутизацію в мережах.
6. Реалізувати заходи безпеки шляхом застосування списків контролю доступу в мережі центрального офісу.

# РОЗДІЛ І. Аналіз технічної складової

## 1.1 Аналіз сучасних технологій локальних та глобальних мереж

Для класифікації комп’ютерних мереж використовуються різноманітні ознаки, але найчастіше мережі класифікують за територіальною ознакою – за величиною території, яку покриває мережа. І для цього є вагомі причини, оскільки відмінності локальних і глобальних мереж є дуже значними, незважаючи на їх постійне зближення.

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.

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. Для стійкої передачі дискретних даних по неякісних лініях зв’язку застосовуються методи та обладнання, що суттєво відрізняються від методів та обладнання, характерних для локальних мереж. Як правило, тут застосовуються складні процедури контролю та відновлення даних.

Міські мережі (**Metropolitan Area Networks** (**MAN**)) – з’явилися відносно недавно. Вони призначені для обслуговування великого міста і займають деяке проміжне місце між локальними та глобальними мережами. Вони використовують цифрові магістральні лінії зв’язку зі швидкостями від 45 Мбіт/с, і призначені для зв’язування локальних мереж в межах населеного пункту і з’єднання локальних мереж із глобальними.

**Відмінності між локальними та глобальними мережами та шляхи їх зближення**. Оскільки з часом відмінності між різними класами мереж стають все менш помітними, розглянемо тільки ті з них, які проявляються найбільш суттєво.

**Довжина, якість та спосіб прокладання ліній зв’язку**. Клас локальних мереж за означенням відрізняється від класу глобальних мереж невеликою відстанню між вузлами мережі. Це дає можливість використовувати в локальних мережах якісні лінії зв’язку: коаксіальний кабель, виту пару, оптоволокно, які не завжди доступні (із-за великої вартості) на великих відстанях, характерних для глобальних мереж. В глобальних мережах часто застосовують уже існуючі лінії зв’язку, а в локальних мережах вони прокладаються заново.

**Складність методів передачі та обладнання**. В умовах низької надійності фізичних каналів в глобальних мережах потрібні складніші, ніж у локальних мережах, методи передачі даних та відповідне обладнання. Так, в глобальних мережах широко застосовується модуляція, асинхронні методи, складні методи контрольного сумування та повторні передачі пошкоджених кадрів. З іншого боку, якісні лінії зв’язку в локальних мережах дозволили спростити процедури передачі даних за рахунок застосування не модульованих сигналів та відмови від обов’язкового підтвердження отримання пакету.

**Швидкість обміну даними**. Однією з головних відмінностей локальних мереж від глобальних є наявність високошвидкісних каналів обміну даними між комп’ютерами (порядку 100 Мбіт/с), яка порівняна зі швидкостями пристроїв та вузлів комп’ютерів. У зв’язку з цим у користувача локальної мережі, підключеного до віддаленого спільного ресурсу, складається враження, що він користується ресурсом свого комп’ютера. Для глобальних мереж типовими є значно менші швидкості передачі даних.

**Різноманітність послуг**. Локальні мережі надають, як правило, широкий набір послуг – різні види послуг файлової служби, послуги друку, послуги передачі факсимільних повідомлень, послуги баз даних, електронна пошта тощо, тоді як глобальні мережі в основному надають поштові та файлові послуги з обмеженими можливостями.

**Оперативність виконання запитів**. Час проходження пакету через локальну мережу зазвичай складає кілька мілісекунд, тоді як час його передачі через глобальну мережу може досягати кількох секунд. Низька швидкість передачі даних у глобальних мережах ускладнює реалізацію служб для режиму online, який є звичайним для локальних мереж.

**Розділення каналів**. В локальних мережах канали зв’язку використовуються, як правило, спільно одразу ж кількома вузлами мережі, а в глобальних – індивідуально.

**Використання методу комутації пакетів**. Важливою особливістю локальних мереж є нерівномірний розподіл навантаження. Відношення пікового навантаження до середнього може складати 100:1 і навіть більше. Такий трафік зазвичай називають пульсуючим. Внаслідок такої особливості трафіку в локальних мережах для зв’язку вузлів застосовується метод комутації пакетів, який для пульсуючого трафіку є значно ефективнішим, ніж традиційний для глобальних мереж метод комутації каналів.

**Масштабованість**. Класичні локальні мережі погано масштабуються із-за жорсткості базових топологій, які визначають спосіб підключення станцій та довжину лінії. При використанні багатьох базових топологій характеристики мережі значно погіршуються при досягненні певної кількості вузлів чи протяжності лінії зв’язку. Глобальним же мережам притаманна добра масштабованість, оскільки вони з самого початку розроблялися з розрахунку на роботу із різними топологіями.

Останнім часом в світі локальних та глобальних мереж намітилися тенденції до зближення. Одним із проявів такого зближення є поява міських мереж, які займають проміжне місце між локальними та глобальними мережами. При досить великих відстанях між вузлами вони володіють якісними лініями зв’язку та високими швидкостями обміну, навіть більшими, ніж у класичних локальних мережах. Як і у випадку локальних мереж, при побудові MAN не використовують існуючі лінії, а прокладають нові. Із-за різкого покращення якості каналів зв’язку в глобальних мережах почали відмовлятися від надлишкових процедур забезпечення коректності передачі даних. За рахунок нових мережних технологій та, відповідно, нового обладнання, швидкості в існуючих комерційних глобальних мережах потрохи наближаються до швидкостей локальних мереж.

В результаті цього служби, які працюють в режимі online, стають звичайними і в глобальних мережах. Найяскравішим прикладом цього є гіпертекстова інформаційна служба World Wide Web, яка стала основним постачальником інформації в мережі Інтернет. Її інтерактивні можливості перевершили можливості багатьох аналогічних служб локальних мереж, у зв’язку з чим багато служб глобальних мереж зараз мігрують і в локальні мережі. Процес перенесення служб та технологій з глобальних мереж в локальні набув такого масового характеру, що з’явився навіть спеціальний термін – intranet-технології, який позначає використання служб глобальних мереж в локальних.

Локальні мережі запозичують у глобальних мереж і транспортні технології. Усі нові швидкісні технології (FastEthernet, GigabitEthernet, 100VG-AnyLan) підтримують роботу з індивідуальними лініями зв’язку поряд з традиційними для локальних мереж спільно використовуваними лініями. В локальних мережах останнім часом приділяється також велика увага методам забезпечення захисту інформації від несанкціонованого доступу, як і в глобальних мережах. Така увага обумовлена тим, що локальні мережі перестали бути ізольованими, частіше за все вони мають вихід у «великий світ» через глобальні мережі. При цьому часто застосовуються ті ж методи – шифрування даних, автентифікація користувачів, створення захисних бар’єрів тощо.

І, нарешті, з’являються нові технології, призначені для двох видів мереж. Найяскравішим прикладом є технологія ATM, яка може служити основою не тільки локальних і глобальних мереж, а й телефонних чи відео мереж, об’єднуючи усі види трафіку в одній транспортній мережі.

**Мережі відділів, кампусів та корпорацій**. Іще одним популярним способом класифікації мереж є їх класифікація за масштабами організації, в межах якої функціонує мережа. Розрізняють мережі відділів, кампусів та корпоративні мережі [Error: Reference source not found].

Мережі відділів – це мережі, що використовуються порівняно невеликою групою співробітників, які працюють в одному відділі підприємства. Ці співробітники працюють над деякими спільними задачами, наприклад, ведуть бухгалтерський облік чи займаються маркетингом. Вважається, що відділ може налічувати до 100-150 співробітників. Головною метою мережі відділів є спільне використання локальних ресурсів, таких як програми, дані, принтери, модеми тощо. Мережі відділів зазвичай не розділяють на підмережі. В цих мережах локалізується більша частина трафіку підприємства. Мережі відділів зазвичай створюються на основі якоїсь одної мережної технології – Ethernet, Token Ring. Для таких мереж характерним є один чи, у рідких випадках, два типи операційних систем.

Задачі управління мережею на рівні відділу відносно прості: додавання нових користувачів, усунення простих відмов, інсталяція нових вузлів та встановлення нових версій програмного забезпечення. Такою мережею може управляти співробітник, який присвячує обов’язкам адміністратора тільки частину свого часу. Існує й другий тип мереж, близький до мереж відділів – мережі робочих груп. До таких мереж відносяться невеликі мережі, що містять до 10-20 комп’ютерів. Характеристики мереж робочих груп практично не відрізняються від описаних характеристик мереж відділів. Такі властивості, як простота мережі та однорідність тут проявляються в найбільшій мірі, тоді як мережі відділів можуть наближатися до наступного за масштабом типу мереж – мереж кампусів.

**Мережі кампусів** отримали свою назву від англійського слова campus – студентське містечко. Саме на території студмістечок часто виникала необхідність об’єднання кількох невеликих мереж в одну велику мережу. Зараз цю назву не зв’язують із студмістечками, а використовують для позначення мереж будь-яких підприємств та організацій. Мережі цього типу об’єднують множину мереж різних відділів одного підприємства в межах окремого приміщення чи в межах однієї території, що покриває площу в кілька квадратних кілометрів. При цьому глобальні з’єднання в мережах кампусів не використовуються.

Служби такої мережі включають взаємодію між мережами відділів, доступ до спільних баз даних підприємства, модемів, принтерів тощо. Важливою службою, що надається мережами кампусів, є доступ до корпоративних баз даних незалежно від того, на яких типах комп’ютерів вони розміщуються. Саме на рівні мережі кампусу виникають проблеми інтеграції неоднорідного апаратного та програмного забезпечення. Типи комп’ютерів, мережних операційних систем, мережного апаратного обладнання можуть розрізнятися в кожному відділі. Звідси витікають складності управління мережами кампусів. Адміністратори повинні бути в цьому випадку більш кваліфікованими, а засоби оперативного управління мережею – більш досконалими.

**Корпоративні мережі**, які також називають мережами масштабу підприємства, що відповідає дослівному перекладу терміну «enterprise-wide networks», який використовується в англомовній літературі для позначення цього типу мереж. Корпоративні мережі об’єднують велику кількість комп’ютерів на усіх територіях окремого підприємства. Вони можуть містити складні зв’язки і покривати місто, регіон чи навіть континент. Число користувачів та комп’ютерів може вимірюватися тисячами, а кількість серверів – сотнями, відстані між мережами окремих територій можуть виявитися такими, що стає необхідним використання глобальних зв’язків. Неодмінним атрибутом такої складної і багато-масштабної мережі є висока ступінь гетерогенності – неможливо задовольнити потреби тисяч користувачів за допомогою однотипних програмних і апаратних засобів. Неоднорідні частини корпоративної мережі повинні працювати як єдине ціле, надаючи користувачам по можливості прозорий доступ до всіх необхідних ресурсів.

Поява корпоративних мереж – це добра ілюстрація відомого філософського постулату про перехід кількості в якість. При об’єднанні окремих мереж великого підприємства, що має філії в різних містах і навіть країнах, в єдину мережу багато кількісних характеристик об’єднаної мережі переходять деяку критичну мережу, за якою починається нова якість. В цих умовах існуючі методи та підходи до розв’язання традиційних задач мереж менших масштабів для корпоративних мереж виявилися непридатними. На перший план вийшли такі задачі і проблеми, які в мережах робочих груп, відділів і навіть кампусів мали або другорядне значення, або зовсім не проявлялися.

Прикладом може служити проста (для невеликих мереж) задача – ведення ідентифікаційних даних про користувачів мережі. Найпростіший спосіб її вирішення – вміщення ідентифікаційних даних кожного користувача в локальну базу ідентифікаційних даних кожного комп’ютера, до ресурсів якого користувач повинен мати доступ. Для невеликої мережі, яка складається з 5-10 комп’ютерів та приблизно такої ж кількості користувачів, такий метод працює дуже добре. Однак зі зростанням кількості користувачів до сотень і навіть тисяч, кожному з яких потрібен доступ до певних мережних засобів, такий спосіб стає неефективним. Ефективним вирішенням такої проблеми для великої мережі є використання централізованої довідкової служби, в базі даних якої зберігаються ідентифікаційні записи усіх користувачів мережі.

При переході до корпоративних мереж висувається іще ряд важливих вимог – надійність, відмово-стійкість та продуктивність мережі. По мірі збільшення масштабів мережі, збільшуються і її функціональні можливості. По мережі циркулюють все більші об’єми даних, і мережа повинна забезпечувати їх безпеку і захищеність, залишаючи їх доступними. При кожному переході на наступний рівень складності комп’ютерне обладнання мережі стає все більш різноманітним, а географічні відстані збільшуються, роблячи досягнення мети складнішим, складнішим і дорожчим також стає управління такими з’єднаннями.

### 1.1.1 Фізичні топології локальних мереж

**Фізична топологія** – це граф, вершинами якого є вузли мережі, а ребрами – фізичні зв’язки між ними. **Логічна топологія** описує, як циркулюють потоки інформації між вузлами. Фізична і логічна топологія мережі можуть не співпадати між собою. Фактично логічна топологія визначає алгоритм, згідно із яким мережеві вузли будуть отримувати доступ до середовище передачі даних (буде описано далі).

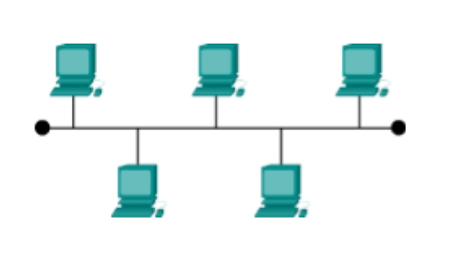
У шинної топології кожен комп'ютер підключений до загального кабелю. Кабель з'єднує один комп'ютер з наступним, як автобусна лінія, що проходить через місто. На кінці кабелю встановлений невеликий ковпачок, який називається заглушкою. Заглушка перешкоджає переміщенню сигналів вперед - назад і виникненню пов'язаних з цим мережних помилок (Рисунок 1.1.1.1). 

Рисунок 1.1.1.1 Шина топологія

У кільцевій топології вузли з'єднані у фізичне кільце або коло. Оскільки у кільцевої топології відсутні початок і кінець, на кабель не встановлюється заглушка. Маркер передається по кільцю, зупиняючись на кожному вузлі. Якщо вузлу необхідно передати дані, він додає до маркера дані та адресу призначення. Маркер продовжує переміщення по кільцю, поки не зупиниться на вузлі з адресою призначення. Вузол призначення приймає дані (Рисунок 1.1.1.2).

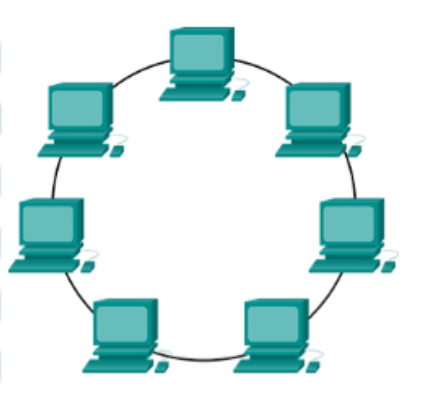


Рисунок 1.1.1.2 Кільце топологія

Зіркоподібна топологія має центральну точку підключення, якою зазвичай є такий пристрій, як концентратор, комутатор або маршрутизатор. Кожен вузол у мережі має сегмент кабелю, який під’єднає вузол безпосередньо до центральної точки підключення. Перевага зіркоподібній топології − простота усунення несправності. Кожен вузол підключений до центрального пристрою окремим проводом. При виникненні несправності з цим кабелем зачіпається тільки один вузол. Решта мережі продовжує працювати (Рисунок 1.1.1.3).



Рисунок 1.1.1.3 Зіркоподібна топологія

Ієрархічна або «розширена зірка» − це зіркоподібна топологія з додатковим мережним пристроєм, підключеним до основного мережного пристрою. Зазвичай мережний кабель підключений до комутатора, до якого підключені кілька інших комутаторів. У мережах більшого розміру, наприклад, мережах корпорацій чи університетів, використовується ієрархічна топологія типу «зірка» ( Рисунок 1.1.1.4).



Рисунок 1.1.1.4 Ієрархічна топологія

У повнозв'язній топології всі пристрої підключені один до одного. Коли кожен пристрій підключено до всіх інших, збій у роботі якого-небудь кабелю або пристрою не впливає на роботу всієї мережі. Повнозв'язна топологія використовується в глобальних мережах, що з'єднують локальні (Рисунок 1.1.1.5).

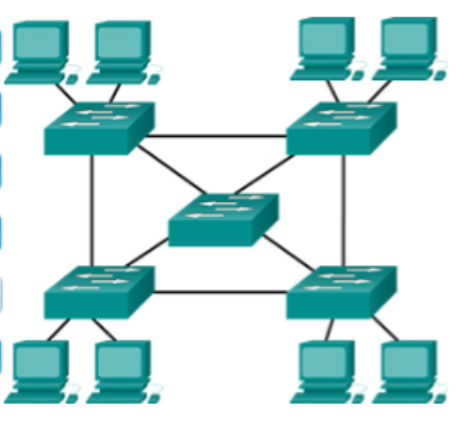


Рисунок 1.1.1.6 Повнозв'язна топології

Гібридна топологія − поєднання двох або більше основних топологій мережі, наприклад, «зірка-шина» або «зірка-кільце». Перевага гібридної топології у тому, що вона може бути реалізована для різних мережних середовищ.

Тип топології визначає можливості мережі, такі як простота налаштування, швидкість і довжина кабелю. Архітектура локальної мережі описує логічні та фізичні топології, що використовуються в мережі (Рисунок 1.1.1.7).

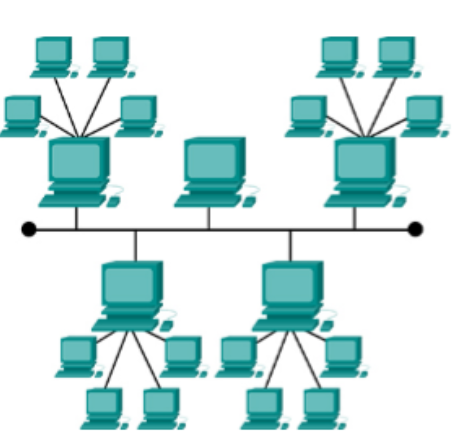


Рисунок 1.1.1.7 Гібридна топологія

### 1.1.2 Топології глобальних мереж

На відміну від локальних, глобальні мережі характеризуються досить складною нерегулярною топологією.

Основу передавального середовища глобальних мереж становлять вузли комутації, пов’язані між собою каналами передачі даних.

**Канали передачі даних** − це канали зв’язку, пристосовані для передачі дискретної інформації у вигляді масивів даних. При цьому висуваються достатньо високі вимоги до безпомилкової передачі інформації. Як правило, роботою мережі управляє спеціальний комп’ютер − **сервер мережі**.

**Файл - сервери** служать для збереження значних обсягів інформації й організації ефективного доступу до неї з боку робочих станцій.

**Сервери доступу** (проксі-сервери)- спеціальні комп’ютери, за допомогою яких забезпечується ефективний доступ певної кількості робочих станцій до комп’ютерної мережі. Кількість і місце розташування вузлів комутації вибирається таким чином, щоб при мінімальних витратах забезпечити необхідну пропускну спроможність мережі передачі даних( Рисунок 1.1.2.1).

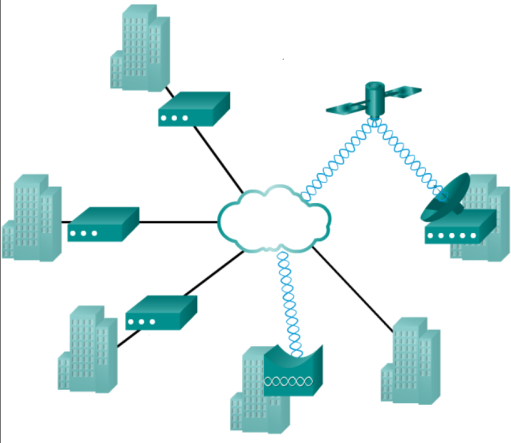


Рисунок 1.1.2.1 Структура глобальної комп’ютерної мережі

**Віртуальні мережі (VLAN).** Комутатор Ethernet фізично сегментує LAN на окремі колізійні домени. Однак кожен сегмент є частиною одного широкомовного домену. Всі сегменти комутатора складають один широкомовний домен. Це означає, що вузол одного сегмента здатний встановити широкомовний режим на всіх вузлах всіх сегментів.

**Віртуальна мережа** (virtual LAN, VLAN) являє собою логічне об'єднання мережевих пристроїв або користувачів, не обмежене одним фізичним сегментом. **Віртуальна локальна мережа** (virtual LAN, VLAN) - група пристроїв у локальній мережі, які сконфігуровані (з використанням керуючого програмного забезпечення) таким чином, що вони можуть обмінюватися інформацією так, ніби вони були з'єднані одним кабелем. У дійсності вони розташовуються в різних сегментах локальної мережі. Оскільки віртуальні мережі ґрунтуються на логічному, а не фізичному з'єднанні, вони є надзвичайно гнучкими.

Пристрої або користувачі VLAN можуть бути згруповані по виконуваних функціях, по приналежності до однієї організації, за характером використовуваних додатків тощо, незалежно від їх фізичного розташування в сегментах. VLAN створює єдиний широкомовний простір, не обмежений фізичним сегментом, і його можна розглядати як підмережу.

Створення мережі VLAN проводиться в комутаторі за допомогою відповідного програмного забезпечення. Мережі VLAN не стандартизовані і вимагають використання ліцензійного програмного забезпечення від виробника комутатора.

Конфігурація типової локальної мережі визначається фізичною інфраструктурою з'єднання пристроїв, які утворюють мережу. Угрупування користувачів здійснюється виходячи з розташування їхніх комп'ютерів по відношенню до концентратора (hub), і ґрунтується на структурі кабелів, прокладених до монтажної шафи. Маршрутизатор, який з'єднує між собою всі концентратори, зазвичай здійснює сегментацію мережі і діє як широкомовний брандмауер (broadcast firewall), в той час як сегменти, створені комутаторами, таку властивість не мають. Такий тип сегментації при угрупованні не враховує взаємозв'язку робочих груп та вимоги до ширини смуги пропускання. Внаслідок цього вони використовують один і той же сегмент і в рівній мірі претендують на одну і ту ж смугу пропускання, хоча вимоги до неї для різних груп і підрозділів можуть значно відрізнятися (Рисунок 1.1.2.2).

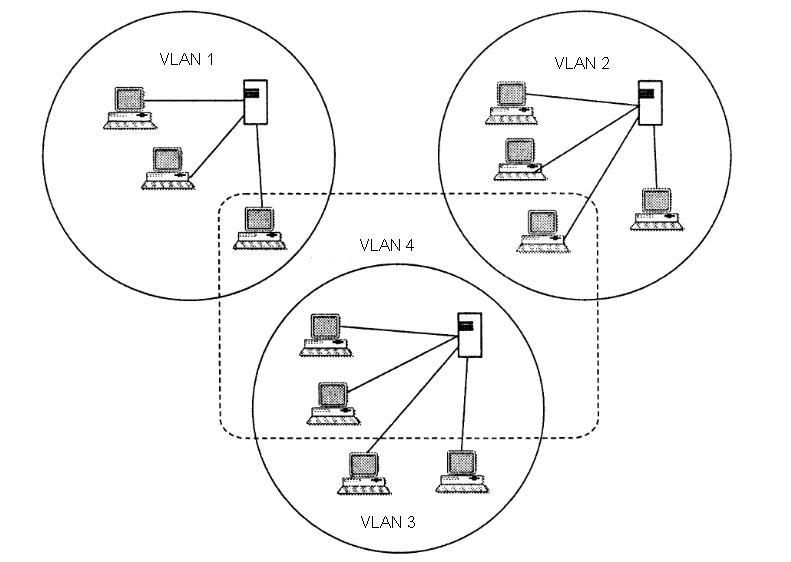


Рисунок 1.1.2.1 Приклад будови віртуальної мережі

**Необхідність в стандартах**

До недавнього часу існувала в деякій мірі плутана суміш стандартів, які управляють різними аспектами мережевих середовищ передачі даних. Ці стандарти охоплювали діапазон від правил протипожежної безпеки та будівельних норм до докладних специфікацій електричних характеристик.

Інші стандарти описували методи тестування, які б забезпечували безпечну експлуатацію і працездатність мережі. Перші стандарти, розроблені для мережевих середовищ передачі даних, являли собою в основному корпоративні стандарти, створені різними компаніями. Пізніше відбулося об'єднання численних організацій і урядових установ в рух за регламентацію та введення специфікацій типу кабелю, який можна використовувати в мережах.

Протягом двох останніх десятиліть спостерігалося значне зростання глобальних мереж. Переконавшись, що використання мережевих технологій обіцяє суттєву економію грошових коштів і підвищення продуктивності праці, великі організації стали приділяти особливу увагу цьому напрямку. Нові технології та продукти впроваджувалися відразу після їх появи, і тому багато мереж були сформовані з використанням різних апаратних і програмних засобів. Внаслідок цього багато мереж виявилися несумісними і стало складним організовувати обмін інформацією між комп'ютерами, використовуючи різні мережеві специфікації.

Найбільший інтерес представляють стандарти мережевих середовищ передачі даних, що розробляються і випускаються Інститутом інженерів з електротехніки та електроніки (Institute of Electrical and Electronic Engineers, IEEE), лабораторією з техніки безпеки (Underwriters Laboratories, UL), Асоціацією електронної промисловості (Electrical Industries Association, EIA) та Асоціацією телекомунікаційної індустрії (Telecommunications Industry Association, TIA). Крім цих груп і організацій випуском специфікацій і технічних вимог, які можуть вплинути на тип кабелю, що використовується в локальній мережі, займаються місцеві, окружні та національні урядові органи та установи.

Для вирішення проблеми сумісності Міжнародна організація по стандартизації (International Organization for Standardization, ISO) досліджувала існуючі схеми мереж. В результаті дослідження була визнана необхідність у створенні еталонної моделі мережі, яка змогла б допомогти постачальникам створювати сумісні мережі. І в 1984 році ISO випустила в світ еталонну модель взаємодії відкритих систем (OSI).

Еталонна модель OS1 швидко стала основною архітектурної моделлю взаємодії між комп'ютерами. Незважаючи на те, що були розроблені і інші архітектурні моделі, більшість постачальників мереж, бажаючи сказати користувачам, що їхні продукти сумісні і здатні працювати з різними виробленими в світі мережевими технологіями, посилаються на їх відповідність еталонної моделі OSI.

**Вимоги до сучасних обчислювальних мереж**. Головна функція мережі - це забезпечення користувачів потенційною можливістю доступу до розподілених ресурсів всіх комп’ютерів, об’єднаних у мережу. Всі вимоги пов’язані з виконанням цієї основної задачі.

## 1.2 Розрахунок адресного простору

### 1.2.1 Розподіл адрес для мережі центрального офісу (Lan1)

Вихідні дані до завдання наведені в таблиці. 1.2.1.1 та рисунку 1.2.1.1.

Таблиця 1.2.1.1

Вихідні дані для адресації хостів мережі центрального офісу

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № вар. | IP-адреса | Кількість хостів | | | | |
| Net1 | Net2 | Net3 | Net4 | Net5 |
| 14 | 172.20.14.0 | 15 | 7 | 11 | 48 | 50 |
| 15 | 10.4.15.0 | 13 | 10 | 2 | 46 | 110 |
| 16 | 192.168.16.0 | 10 | 110 | 5 | 12 | 10 |
| 17 | 172.21.17.0 | 58 | 55 | 7 | 15 | 5 |
| 18 | 10.5.18.0 | 100 | 28 | 13 | 4 | 5 |
| 19 | 192.168.19.0 | 28 | 10 | 12 | 50 | 61 |

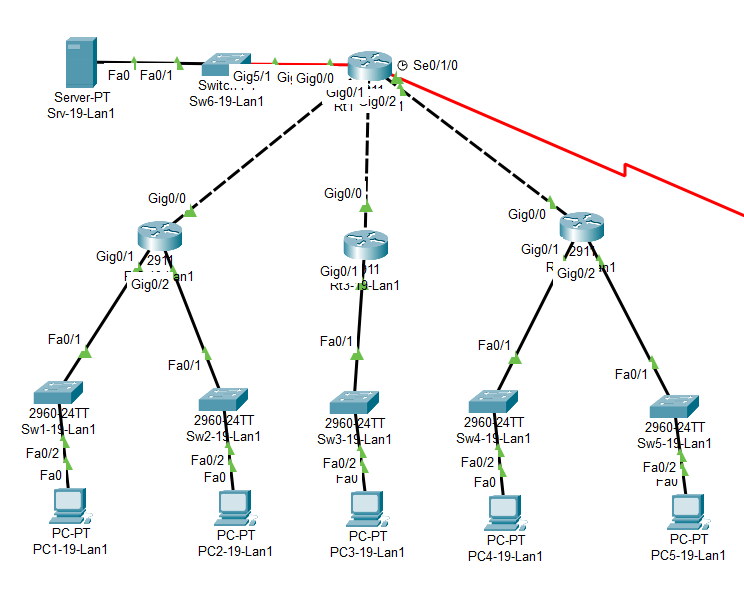


Рисунок 1.2.1.1 Структурна схема 1 мережі

Як видно з рисунку, мережа центрального офісу складається з шести підмереж та чотирьох маршрутизаторів. Спочатку присвоїмо адреси маршрутизаторам.

Відповідно до схеми, між маршрутизаторами є три мережі. Присвоїмо адреси портам маршрутизаторів, обравши префікс /30. Це дозволить утворити мережі тільки з двома адресами вузлів. Параметри мереж між маршрутизаторами показані в таблиці 1.2.1.2.

Таблиця 1.2.1.2

Параметри мереж між маршрутизаторами

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Мережа | Маршрутизатор | Номер порту | Адреса | Маска |
| Rt1-19-Lan1 – Rt2-19-Lan1 | Rt1-19-Lan1 | 0/1 | 192.168.19.202 | /30 |
| Rt1-19-Lan1 – Rt2-19-Lan1 | Rt2-19-Lan1 | 0/0 | 192.168.19.197 | /30 |
| Rt1-19-Lan1 – Rt3-19-Lan1 | Rt1-19-Lan1 | 0/2 | 192.168.19.206 | /30 |
| Rt1-19-Lan1 – Rt3-19-Lan1 | Rt3-19-Lan1 | 0/0 | 192.168.19.201 | /30 |
| Rt1-19-Lan1 – Rt4-19-Lan1 | Rt1-19-Lan1 | 0/2/0 | 192.168.19.194 | /30 |
| Rt1-19-Lan1 – Rt4-19-Lan1 | Rt4-19-Lan1 | 0/0 | 192.168.19.205 | /30 |

Підмережа сервера Net6 складається з одного вузла. Разом із тим потрібно врахувати те, що два значення адрес повинно відводитись на адресу підмережі та широкомовну адресу. Також потрібно врахувати, що одну із адрес повинен зайняти порт маршрутизатора, який направлений в дану мережу. Тому для адресації вузлів потрібно відвести як мінімум (заокругливши до більшого цілого(1.2.1.1))

(1.2.1.1)

Це означає, що префікс під мережі має бути 32-2=30. Зважаючи на це, одержимо наступні параметри мережі Net6 таблиця 12.1.3.

Таблиця 1.2.1.3

Параметри мережі Net6

|  |  |
| --- | --- |
| Назва мережі | Net 6 |
| Адреса мережі | 192.168.19.196 |
| Маска мережі | 255.255.255.252 |
| Префікс мережі | /30 |
| Адреса першого вузла | 192.168.19.197 |
| Адреса останнього вузла | 192.168.19.198 |
| Широкомовна адреса | 192.168.19.199 |
| Кількість вузлів мережі | 2 |
| Кількість зайнятих адрес | 2 |
| Кількість вільних адрес | 0 |

Мережа Net1 складається з 28 вузлів. Враховуючи адресу мережі та широкомовну адресу, отримуємо, що для адресації потрібно (заокругливши до більшого цілого(1.2.1.2))

(1.2.1.2)

Таке значення відповідає префіксу мережі /27, маска 255.255.255.224. Параметри мережі наведено в таблиці 1.2.1.4.

Таблиця 1.2.1.4

Параметри мережі Net1

|  |  |
| --- | --- |
| Назва мережі | Net 1 |
| Адреса мережі | 192.168.19.0 |
| Маска мережі | 255.255.255.224 |
| Префікс мережі | /27 |
| Адреса першого вузла | 192.168.19.1 |
| Адреса останнього вузла | 192.168.19.30 |
| Широкомовна адреса | 192.168.19.31 |
| Кількість вузлів мережі | 30 |
| Кількість зайнятих адрес | 29 |
| Кількість вільних адрес | 1 |

Мережа Net2 складається з 10 вузлів. Враховуючи адресу мережі та широкомовну адресу, отримуємо, що для адресації потрібно (заокругливши до більшого цілого(1.2.1.3))

(1.2.1.3)

Таке значення відповідає префіксу мережі /28, маска 255.255.255.240. Параметри мережі наведено в таблиці 1.2.1.5.

Таблиця 1.2.1.5

Параметри мережі Net2

|  |  |
| --- | --- |
| Назва мережі | Net 2 |
| Адреса мережі | 192.168.19.32 |
| Маска мережі | 255.255.255.240 |
| Префікс мережі | /28 |
| Адреса першого вузла | 192.168.19.33 |
| Адреса останнього вузла | 192.168.19.46 |
| Широкомовна адреса | 192.168.19.47 |
| Кількість вузлів мережі | 14 |
| Кількість зайнятих адрес | 11 |
| Кількість вільних адрес | 3 |

Мережа Net3 складається з 12 вузлів. Враховуючи адресу мережі та широкомовну адресу, отримуємо, що для адресації потрібно (заокругливши до більшого цілого(1.2.14))

(1.2.1.4)

Таке значення відповідає префіксу мережі /28, маска 255.255.255.240. Параметри мережі наведено в таблиці 1.2.1.6.

Таблиця 1.2.1.6

Параметри мережі Net3

|  |  |
| --- | --- |
| Назва мережі | Net 3 |
| Адреса мережі | 192.168.19.48 |
| Маска мережі | 255.255.255.240 |
| Префікс мережі | /28 |
| Адреса першого вузла | 192.168.19.49 |
| Адреса останнього вузла | 192.168.19.62 |
| Широкомовна адреса | 192.168.19.63 |
| Кількість вузлів мережі | 14 |
| Кількість зайнятих адрес | 13 |
| Кількість вільних адрес | 1 |

Мережа Net4 складається з 51 вузлів. Враховуючи адресу мережі та широкомовну адресу, отримуємо, що для адресації потрібно (заокругливши до більшого цілого(1.2.1.5)

(1.2.1.5)

Таке значення відповідає префіксу мережі /26, маска 255.255.255.192. Параметри мережі наведено в таблиці 1.2.1.7.

Таблиця 1.2.1.7

Параметри мережі Net4

|  |  |
| --- | --- |
| Назва мережі | Net 4 |
| Адреса мережі | 192.168.19.64 |
| Маска мережі | 255.255.255.192 |
| Префікс мережі | /26 |
| Адреса першого вузла | 192.168.19.49 |
| Адреса останнього вузла | 192.168.19.62 |
| Широкомовна адреса | 192.168.19.63 |
| Кількість вузлів мережі | 62 |
| Кількість зайнятих адрес | 51 |
| Кількість вільних адрес | 11 |

Мережа Net5 складається з 61 вузлів. Враховуючи адресу мережі та широкомовну адресу, отримуємо, що для адресації потрібно (заокругливши до більшого цілого(1.2.1.6))

(1.2.1.6)

Таке значення відповідає префіксу мережі /26, маска 255.255.255.192. Параметри мережі наведено в таблиці 1.2.1.8.

Таблиця 1.2.1.8

Параметри мережі Net5

|  |  |
| --- | --- |
| Назва мережі | Net 4 |
| Адреса мережі | 192.168.19.128 |
| Маска мережі | 255.255.255.192 |
| Префікс мережі | /26 |
| Адреса першого вузла | 192.168.19.49 |
| Адреса останнього вузла | 192.168.19.62 |
| Широкомовна адреса | 192.168.19.63 |
| Кількість вузлів мережі | 62 |
| Кількість зайнятих адрес | 51 |
| Кількість вільних адрес | 11 |

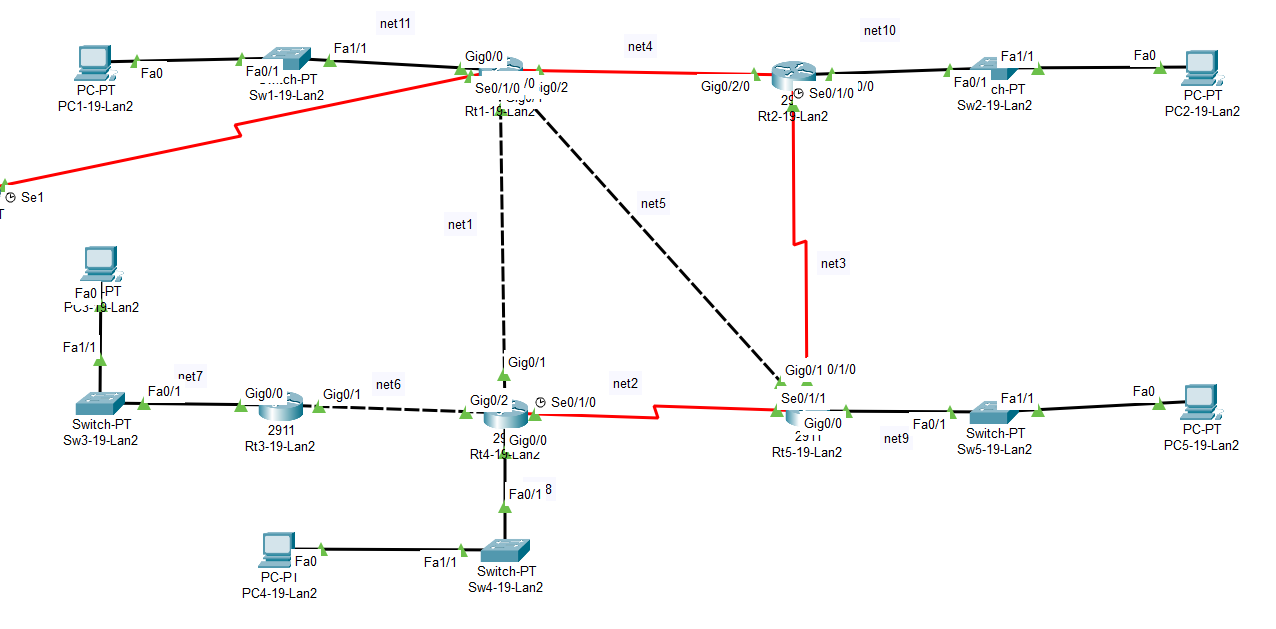
### 1.2.2 Розподіл адрес для мережі офісу з віддаленим доступом (Lan2)

Вихідні дані до завдання наведені в таблиці. 1.2.2.1 та рисунку 1.2.2.1.

Таблиця 1.2.2.1

Вихідні дані до розрахунку адресного простору мережі віддаленого офісу

|  |  |  |
| --- | --- | --- |
| № Вар. | IP-адрес | Шлюз |
| 19 | 10 .6.19.0/24 | Rt1 |

Рисунок 1.2.2.1 Структурна схема мережі

Відповідно до завдання потрібно розподілити адресний простір між маршрутизаторами так, щоб відповідні підмережі мали префікс /30. Такий префікс обмежує кількість вузлів значенням 2. Параметри мереж між маршрутизаторами показані в таблиці 1.2.2.2 (Додаток А).

Порти маршрутизаторів направлені у внутрішні мережі. Мережа маршрутизаторів займає адресний пул 10.6.19.0-10.6.19.30.

Розподілимо адреси, що залишилися між п’ятьма мережами. Для заданої кількості мереж на їх адресацію потрібно відвести (заокругливши до більшого цілого(1.2.1.6)).

(1.2.1.6)

Таким чином префікс мереж становитиме 24+3=27 біт. Параметри мереж наведено в таблиці 1.2.2.3 (Додаток Б).

### 1.2.3 Розподіл адрес для мережі дата-центру (Lan3)

Вихідні дані до завдання наведені в таблиці. 1.2.3.1 та рисунку 1.2.3.1.

Таблиця 1.2.3.1

Вихідні дані до розрахунку дата центру

|  |  |  |  |
| --- | --- | --- | --- |
| № Вар. | Net1 | Net2 | Net3 |
| 19 | 181.218.0.0 | 205.186.160.0 | 186.165.0.0 |

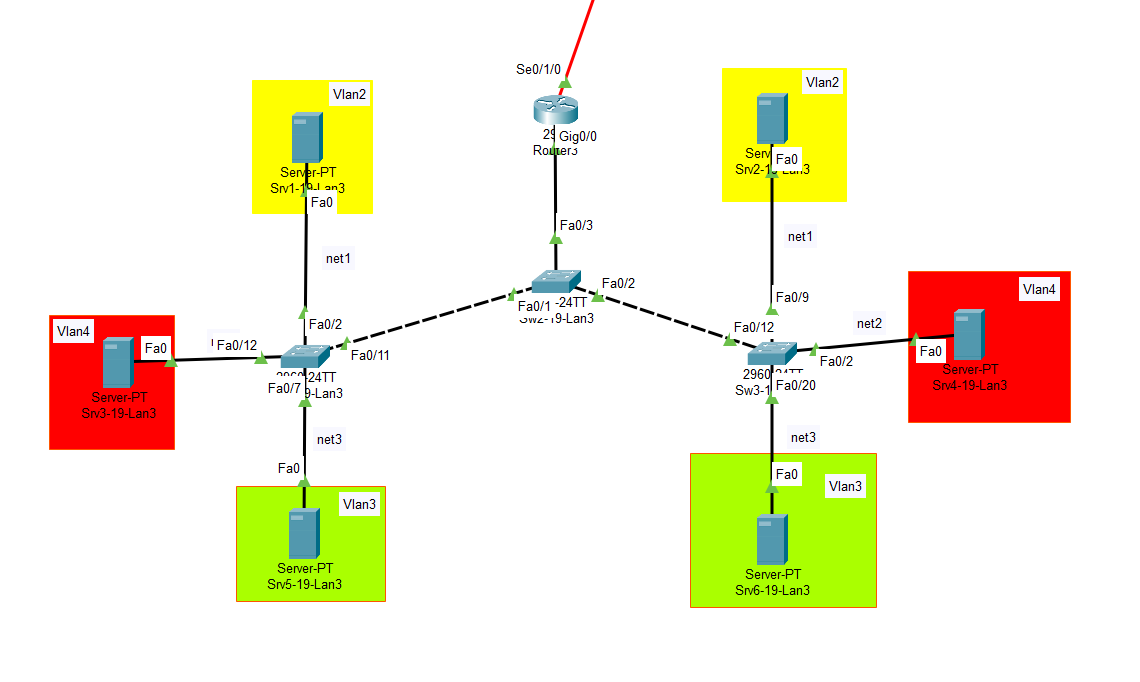


Рисунок 1.2.3.1 Структурна схема мережі

Розподілимо адреси, що залишилися між 3 мережами. Для заданої кількості мереж на їх адресацію потрібно відвести (заокругливши до більшого цілого(1.2.3.1)).

(1.2.3.1)

Таким чином префікс мереж становитиме 26+3=29 біт. Параметри мереж наведено в таблиці 1.2.3.2 (Додаток В).

## 1.3 Налаштування маршрутизації (Lan1)

Відповідно до завдання у мережі центрального офісу потрібно налаштувати статичну маршрутизацію.

**Додаємо статичні маршрути в маршрутизатор Rt1.**

Router(config)#ip route 192.168.19.0 255.255.255.224 192.168.19.197

Router(config)#ip route 192.168.19.192 255.255.255.252 192.168.19.193

Router(config)#ip route 192.168.19.32 255.255.255.240 192.168.19.197

Router(config)#ip route 192.168.19.48 255.255.255.240 192.168.19.201

Router(config)#ip route 192.168.19.64 255.255.255.192 192.168.19.205

Router(config)#ip route 192.168.19.128 255.255.255.192 192.168.19.205

На Rt2, Rt3, Rt4 налаштуємо маршрутизацію таким чином, щоб весь трафік маршрутизувався через Rt1.

**Додаємо статичний маршрут в Rt2.**

Router(config)#ip route 192.168.19.48 255.255.255.240 192.168.19.198

Router(config)#ip route 192.168.19.64 255.255.255.192 192.168.19.198

Router(config)#ip route 192.168.19.128 255.255.255.192 192.168.19.198

Router(config)#ip route 192.168.19.192 255.255.255.252 192.168.19.198

**Додаємо статичний маршрут в Rt3.**

Router(config)#ip route 192.168.19.192 255.255.255.252 192.168.19.202

Router(config)#ip route 192.168.19.0 255.255.255.224 192.168.19.202

Router(config)#ip route 192.168.19.32 255.255.255.240 192.168.19.202

Router(config)#ip route 192.168.19.128 255.255.255.192 192.168.19.202

Router(config)#ip route 192.168.19.64 255.255.255.192 192.168.19.202

**Додаємо статичний маршрут в Rt4.**

Router(config)#ip route 192.168.19.192 255.255.255.252 192.168.19.206

Router(config)#ip route 192.168.19.0 255.255.255.224 192.168.19.206

Router(config)#ip route 192.168.19.32 255.255.255.240 192.168.19.206

Router(config)#ip route 192.168.19.48 255.255.255.240 192.168.19.206

Таким чином таблиці маршрутизації Rt2, Rt3, Rt4 будуть мати мінімальний обсяг.

Для мережі віддаленого офісу згідно завдання налаштовуємо тип маршрутизації EIGRP.

**Налаштування EIGRP маршрутизації на маршрутизаторі Rt1.**

Router(config)#router eigrp 1

Router(config-router)#network 10.6.19.16 0.0.03

Router(config-router)#network 10.6.19.0 0.0.0.3

Router(config-router)#network 10.6.19.0 0.0.03

Router(config-router)#no auto-summary

**Налаштування статичної маршрутизації на маршрутизаторі Rt2.**

Router(config)#router eigrp 1

Router(config-router)#network 10.6.19.28 0.0.031

Router(config-router)#network 10.6.19.8 0.0.0.3

Router(config-router)#network 10.6.19.12 0.0.03

Router(config-router)#no auto-summary

**Налаштування статичної маршрутизації на маршрутизаторі Rt3**

Router(config)#router eigrp 1

Router(config-router)#network 10.6.19.32 0.0.031

Router(config-router)#network 10.6.19.20 0.0.0.3

Router(config-router)#no auto-summary

**Налаштування статичної маршрутизації на маршрутизаторі Rt4.**

Router(config)#router eigrp 1

Router(config-router)#network 10.6.19.64 0.0.031

Router(config-router)#network 10.6.19.0 0.0.0.3

Router(config-router)#network 10.6.19.20 0.0.03

Router(config-router)#network 10.6.19.4 0.0.03

Router(config-router)#no auto-summary

**Налаштування статичної маршрутизації на маршрутизаторі Rt5.**

Router(config)#router eigrp 1

Router(config-router)#network 10.6.19.96 0.0.031

Router(config-router)#network 10.6.19.16 0.0.0.3

Router(config-router)#network 10.6.19.8 0.0.03

Router(config-router)#network 10.6.19.4 0.0.03

Router(config-router)#no auto-summary

# РОЗДІЛ ІІ. Конфігурування мережевого обладнання

## 2.1 Конфігурування базових функцій маршрутизаторів

Конфігурування інтерфейсів здійснюється окремо для кожного інтерфейсу в контексті обраного інтерфейсу, перехід до якого здійснюється командою контексту глобального конфігурування:

***interface <тип><номер>***

В якості параметру <тип> допускаються наступні слова: Ethernet, Fast Ethernet, Serial, Loopback, Null.

Вказана команда приводить до зміни поточного контексту на контекст конфігурування обраного інтерфейсу (config-if#).

На інтерфейсах Ethernet, окрім встановлення ІР-адреси, як правило більше нічого робите не потрібно, однак Fast Ethernet може потребувати деяких примусових настройок дуплексного режиму або встановлення фіксованої швидкості (по умовчанню ці параметри встановлюються шляхом переговорів, однак в окремих випадках переговори можуть не дати необхідних результатів).

Послідовні інтерфейси по умовчанню на фізичному рівні є інтерфейсами DTE, а на канальному рівні –інтерфейсами HDLC (фірмову модифікацію Cisco HDLC). Якщо інтерфейс переведено в режим DCE, -для нього слід задавати тактову частоту синхронізації передачі даних.

Для надання фізичному інтерфейсу ІР адреси слід використовувати команду:

***ip address <IP-address><address-mask>*** де ***<IP-address>*** – ІР-адреса інтерфейсу; ***<address-mask>*** – маска під мережі.

В деяких випадках може бути необхідність встановлення ширини смуги пропускання командою:

***bandwith <ширина-смуги-пропускання, кБіт/с>***

По умовчанню значення bandwith мають наступні значення:

* для Ethernet 10000
* для Fast Ethernet 100000
* для Serial 1544

Слід зауважити, що значення параметра bandwith не впливає на фізичну швидкість передачі, а використовується деякими протоколами маршрутизації для оцінки маршруту.

Тип середовища передачі вказується командою:

***media-type <тип-середовища-передачі>***

Параметр ***<тип-середовища-передачі>*** може приймати значення:

* для Ethernet "10BASE-T"
* для Fast Ethernet "100BASE-T", "100BASE-TX"

Для послідовних інтерфейсів, які використовують функції DCE, необхідно вказати фізичну швидкість передачі даних. Це можна зробити командою:

clock rate ***<фізична-швидкість-передачі, кБіт/с>***

Параметр ***<фізична-швидкість-передачі, кБіт/с>*** може приймати фіксовані значення, перелік яких можна попередньо проглянути, ввівши clock rate ?.

Для послідовного інтерфейсу, що виконує функцію DTE також може бути вказаний цей параметр, однак він буде проігнорований Cisco IOS і жодного впливу на роботу інтерфейсу не матиме, оскільки обладнання DTE запозичує цей параметр від DCE.

По умовчанню фізичні інтерфейси виключені (неактивні – administratively down). Для їх активації використовується команда:

[no] shutdown

Ця команда переводить інтерфейс до стану manual up. Якщо зовнішнє обладнання вимкнено, то Cisco IOS автоматично переведе фізичний інтерфейс до стану manual down, а при активізації зовнішнього обладнання фізичний інтерфейс підніметься до стану manual up автоматично.

Для послідовних інтерфейсів іноді виникає необхідність використовувати протокол канального рівня, відмінний від протоколу по умовчанню (HDLC). Cisco IOS надає можливість вказати тип використовуваного протоколу командою:

***encapsulation <протокол>***

Параметр ***<протокол>*** може приймати фіксовані значення, для яких Cisco IOS передбачені зарезервовані ключові слова, наприклад PPP, Frame-Relay і т.п. Повний перелік значень параметра <протокол> доступний для перегляду командою encapsulation ?

Логічні інтерфейси конфігуруються тими ж командами, які наведені вище, за винятком того, що параметри media-type, clock rate та операція [no] shutdown для них не має сенсу.

### 2.1.1 Контекст глобального конфігурування.

Перехід до контексту глобального конфігурування здійснюється з контексту адміністратора командою configure

* з терміналу: configure terminal
* з NVRAM: configure memory
* з мережі: configure network

В контексті глобального конфігурування виконуються команди, які впливають на функціонування системи в цілому, а також команди переходу до контекстів конфігурування конкретних підсистем маршрутизатора. Контекст глобального конфігурування ідентифікується рядком запиту (config)# і допускає виконання наступних команд:

***hostname <назва маршрутизатора>***

Встановлює назву маршрутизатора замість назви по умовчанню "Router"

***[no] enable password <пароль>***

Команда парольного доступу до контексту адміністратора, який буде запитуватися під час виконання команди enable. Пароль прописується до файлу поточної конфігурації і зберігається там у відкритому (нешифрованому) вигляді. При відсутності цього пароля переключення до привілейованого режиму можна здійснити лише при використанні консолі, а з віртуального терміналу буде доступний лише контекст користувача.

***[no] enable secret <пароль>***

Команда, за своєю дією аналогічна попередньо описаній, однак пароль зберігається в зашифрованому MD5 –алгоритмом вигляді і має вищий пріоритет виконання.

***[no] ip domain-lookup***

Дозволити/заборонити звернення до DNS (Domain Name Service)

***[no] cdp run***

Дозволяє/забороняє використання протоколу CDP (Cisco Discovery Protocol) виявлення безпосередньо підключеної апаратури Cisco, тобто доступної на канальному рівні. Протокол з періодичністю 60 с. опитує порти маршрутизатора на предмет наявності апаратури Cisco і заносить інформацію про виявлені пристрої до бази даних.

Маршрути до безпосередньо приєднаних мереж заносяться до таблиці маршрутизації автоматично одразу ж після конфігурування інтерфейсу, при умові, що цей інтерфейс працездатній (line protocol up). Для формування додаткових статичних маршрутів призначена команда:

***[no] ip route <dest.address><dest.mask><next-hop>[options]***

* ***<destination address>*** адреса цільової мережі
* ***<destination mask>*** маска цільової мережі
* ***<next-hop>*** адреса сусіднього маршрутизатора
* ***<options>*** додаткові параметри, наприклад –параметри метрики

В якості параметра ***<next-hop>*** можна вказувати:

* безпосередню адресу сусіднього (доступного на канальному рівні) маршрутизатора.
* адресу віддаленої мережі або віддаленого хоста (опосередкована маршрутизація).
* локальний інтерфейс.

Опосередкований маршрут вказує на запис в таблиці маршрутизації, в якому знаходиться прямий маршрут. Дозволяється формувати таким чином послідовності маршрутів будь-якої довжини. Локальний інтерфейс рекомендується вказувати лише для двоточкових інтерфейсів.

Статичні маршрути фіксуються в файлі стартової конфігурації, а до таблиці маршрутизації піднімаються тільки при умові досяжності вказаного в них маршруту.

Для регулювання пріоритетами маршрутів слід користуватися параметром ***<адміндистанція>***, який може приймати значення від 0 до 255. Рівень пріоритету зворотно пропорційний значенню адміністративної дистанції і в таблицю маршрутизації з усіх активних маршрутів, що ведуть до даного префікса піднімається лише маршрут з найменшим значенням адміндистанції. По умовчанню адміндистанція статичних маршрутів рівна 1.

Нульове значення зарезервоване системою Cisco IOS і не може бути використане в явному вигляді, однак неявно нульову адміндистанцію можна задати, вказавши в якості параметра ***<next-hop>*** локальний інтерфейс. Нульове значення адміндистанції мають також маршрути до безпосередньо приєднаних мереж. Маршрути, які в якості адміндистанції містять значення 255, до таблиці маршрутів не піднімаються.

Команда: ***[no] ip default network <адреса віддаленої мережі>***

Дозволяє вказати маршрут по умовчанню, відмінний від стандартного. Параметр ***<адреса віддаленої мережі>*** повинен бути статично описаний в таблиці маршрутизації. Можливим є визначення декількох маршрутів по умовчанню – в цьому випадку при обранні маршруту Cisco IOS користується значеннями адміністративної дистанції та метричною інформацією. Маршрути по умовчанню в таблиці маршрутизації позначаються символом «\*».

Наведений нижче приклад демонструє використання маршруту в мережу 10.0.0.0 в якості маршруту по умовчанню.

ip route 10.0.0.0 255.0.0.0 10.108.3.4ip default-network 10.0.0.0

Cisco IOS має по умовчанню зарезервований маршрут для використання його в якості маршруту по умовчанню – 0.0.0.0/0. Cisco IOS надає можливість активації (деактивації) цього маршруту командою:

***[no] ip classless***

Команда ip classless активує зарезервований Cisco IOS маршрут по умовчанню (0.0.0.0/0), а команда no ip classless деактивує цей маршрут. По умовчанню цей маршрут активований, але не описаний.

## 2.2 Проектування віртуальних мереж VLAN

VLAN (англ. Virtual Local Area Network — віртуальна локальна комп'ютерна мережа) — є групою хостів з загальним набором вимог, що взаємодіють так, ніби вони прикріплені до одного домену, незалежно від їх фізичного розташування. VLAN має ті самі атрибути, як і фізична локальна мережа, але дозволяє кінцевим станціям бути згрупованими разом, навіть якщо вони не перебувають на одному мережевому комутаторі. Реконфігурація мережі може бути зроблена за допомогою програмного забезпечення замість фізичного переміщення пристроїв.

Щоб фізично копіювати функції VLAN, необхідно встановити окремий, паралельний збір мережевих кабелів і перемикачів, які зберігаються окремо від первинної мережі. Однак на відміну від фізичної відділеної мережі, VLAN ділить пропускну здатність; дві окремих одно-гігабітних віртуальних мережі які використовують одно-гігабітний зв'язок мають знижену пропускну здатність. Це віртуалізує поведінку VLAN (настроювання портів комутатора, позначки кадрів при вході в мережу VLAN, пошук MAC таблиці, щоб перейти до магістральних зв'язків і видалення тегів при виході з VLAN).

За традиційною технологією Ethernet робочі станції об’єднуються в локальну мережу за допомогою багатопортових комутаторів 2-го рівня.

Комутатор (switch) – пристрій канального рівня, який об’єднує кінцеві пристрої в єдину локальну мережу та здійснює одночасний прийом і передачу даних на кожному із своїх портів. Комутатор знижує перевантаженість мережі, зменшує мережний трафік та підвищує ефективну пропускну здатність мережі.

Використання різноманітних фільтрів, що враховують інформацію третього і четвертого рівнів (IP-адреси, тип протоколу, зазначений у заголовку IP-пакета, номера портів TCP/UDP) перетворюють маршрутизатори в найпростіші брандмауери, що складають основу системи захисту багатьох мереж.

Проте комутатори внесли в рішення проблеми "об'єднання-роз'єднання" новий механізм - технологію віртуальних мереж (Virtual LAN, VLAN). З появою цієї технології відпала необхідність утворювати ізольовані сегменти фізичним шляхом — його замінив програмний спосіб, більш гнучкий і зручний.

Віртуальною мережею (VLAN) називається група вузлів мережі, трафік якої в тому числі і широкомовний, на канальному рівні цілком ізольований від інших вузлів мережі.

Розрізняють статичні і динамічна VLAN. До статичної VLAN долучають порти комутатора, незалежно від того, що до них під’єднано. Членство у динамічній VLAN досягається через МАС-адресу під’єднаного пристрою, незалежно від порта підключення

Для налаштування IP-адреси та мережної маски на управлінській VLAN комутатор, необхідно перейти в режим налаштування інтерфейсу. Це єдина віртуальна локальна мережа, до якої звертаються як до інтерфейсу мережного рівня.

**Команди налаштування VLAN 1:**

Switch(config)#interface vlan 1

Switch(config-if)#ip address <ІР-адреса> <маска>

Switch(config-if)#no shutdown

Switch(config-if)#exit

**Приклад налаштування:**

Switch(config)#interface vlan 1

Switch(config-if)#ip address 172.17.99.110 255.255.255.0

**Магістральний протокол VTP** (англ. VLAN Trunking Protocol) –протокол ЛВС, службовець для обміну інформацією про VLAN (віртуальних мережах), наявних на обраному танковому порту. Розроблено і використовується компанією Cisco

Протокол VTP був створений для вирішення можливих проблем у середовищі комутації віртуальних локальних мереж VLAN. Наприклад, розглянемо домен, в якому є кілька пов'язаних один з одним комутаторів, що підтримують кілька VLAN-мереж. Для створення і підтримки з'єднань усередині VLAN-мереж кожна з них повинна бути налаштована вручну на кожному комутаторі. По мірі зростання організації збільшення кількості комутаторів в мережі, кожен новий комутатор повинен бути налаштований вручну з введенням інформації про VLAN-мережах. Всього лише одне неправильне призначення в мережі VLAN може викликати дві потенційні проблеми:

Перехресне з'єднання VLAN-мереж внаслідок неузгодженості конфігурації VLAN-мереж.

Суперечливість конфігурації в змішаному середовищі передачі, наприклад, в середовищі, що включає в себе сегменти Ethernet, Fiber Distributed Data Interface (FDDI).

У протоколі VTP узгодженість конфігурацій VLAN-мереж підтримується в загальному адміністративному домені. Крім того, протокол VTP зменшує складність управління і моніторингу VLAN-мереж.

Призначення протоколу VTP полягає у підтримці узгодженості конфігурацій в загальному адміністративному домені. Протокол VTP є протоколом обміну повідомленнями, які використовують магістральні фрейми 2-го рівня для управління додаванням, видаленням та перейменуванням VLAN-мереж в одному домені.

Крім того, протокол VTP дозволяє здійснювати централізовані зміни в мережі, про які повідомляється всім іншим комутаторів в мережі. Повідомлення протоколу VTP інкапсулюються в фірмові фрейми протоколів ISL або IEEE 802.1 Q і передаються далі по магістральних каналах іншим пристроям. До фреймах IEEE 802.1 Q в якості тега додається 4-х байтове поле. В обох форматах передаються ідентифікатор ID VLAN-мережі

### 2.2.1 Проектування віртуальної мережі VLAN для мережі дата-центру (Lan3)

Вихідні дані до завдання наведені в таблиці. 2.2.1 та рисунку 1.2.3.1.

Таблиця 2.2.1

Вихідні дані до завдання

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Switch1 | | | Switch2 | | |
| Vlan1 | Vlan2 | Vlan3 | Vlan1 | Vlan2 | Vlan3 |

Відповідно до завдання потрібно налаштувати 3 стандартні VLAN.

Заходимо в налаштування Switch далі переходимо в вкладку config бачимо VLAN Database . Заповнюємо VLAN Number вказуємо номер VLAN який нам потрібен це – VLAN 1 VLAN 2 VLAN 3 та VLAN Name вказуємо йому ім’я щоб потім можна було звернутись до нього. Після вказування даних натискаємо кнопку Add(Рисунок 2.2.1).

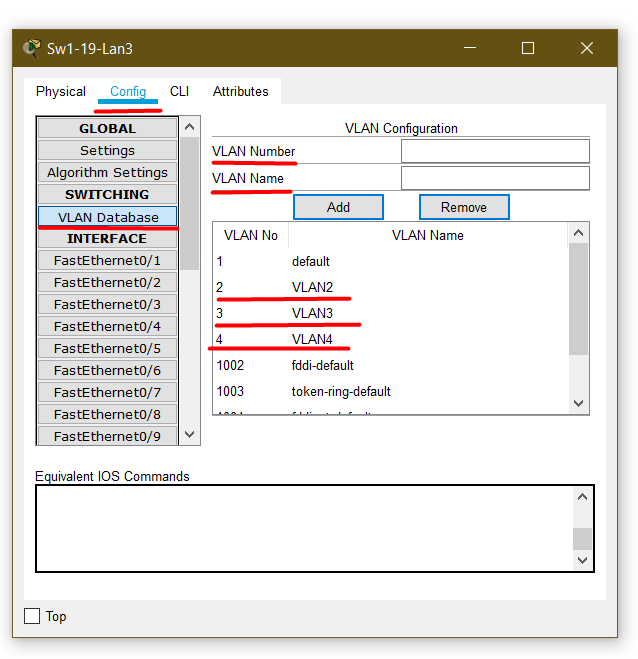


Рисунок 2.2.1 Налаштування VLAN

## 2.3 Конфігурування базових функцій комутаторів LAN3

Вихідні дані до завдання наведені в таблиці. 2.3.1 та рисунку 1.2.3.1.

Таблиця 2.3.1

Вихідні дані до завдання

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Switch1 | | | | Switch3 | | |
| № вар. | Vlan1 | Vlan2 | Vlan3 | Vlan1 | Vlan2 | Vlan3 |
| 19 | 2-6 | 7-10 | 12-14 | 9-11 | 20-22 | 2-7 |

Відповідно до завдання потрібно налаштувати Switch1, Switch2, Switch3 порти на VLAN1, VLAN2, VLAN3.

Переходимо в налаштування Switch1 вибираємо вкладку Config далі Interface. Потрібно порти налаштувати на VLANи.

Порт 2-го по 6-ий задаємо VLAN 1. Для цього потрібно вибрати FastEthernet 0/2-0/6 вказати стан підключення Access та вибрати потрібний лан, а це VLAN1.

Порт 7-го по 10-ий задаємо VLAN2. Для цього потрібно вибрати FastEthernet 0/7-0/10 вказати стан підключення Access та вибрати потрібний лан, а це VLAN2.

Порт 12-го по 14-ий задаємо VLAN3. Для цього потрібно вибрати FastEthernet 0/12-0/14 вказати стан підключення Access та вибрати потрібний лан, а це VLAN3.

Переходимо в налаштування Switch2 вибираємо вкладку Config далі Interface. Потрібно порти налаштувати на VLANи.

Порт 9-го по 11-ий задаємо VLAN1. Для цього потрібно вибрати FastEthernet 0/9-0/11 вказати стан підключення Access та вибрати потрібний лан, а це VLAN1.

Порт 20-го по 22-ий задаємо VLAN2. Для цього потрібно вибрати FastEthernet 0/20-0/22 вказати стан підключення Access та вибрати потрібний лан, а це VLAN2.

Порт 2-го по 7-ий задаємо VLAN3. Для цього потрібно вибрати FastEthernet 0/2-0/7 вказати стан підключення Access та вибрати потрібний лан, а це VLAN3.

Порт FastEthernet 0/11 на Switch1 вказуємо тип підключення Trunk та вибираємо всі VLAN1-3.

Порт FastEthernet 0/2 на Switch2 вказуємо тип підключення Trunk та вибираємо всі VLAN1-3.

Порт FastEthernet 0/1 на Switch2 вказуємо тип підключення Trunk та вибираємо всі VLAN1-3.

Порт FastEthernet 0/3 на Switch2 вказуємо тип підключення Trunk та вибираємо всі VLAN1-3.

Порт FastEthernet 0/12 на Switch3 вказуємо тип підключення Trunk та вибираємо всі VLAN1-3.

# РОЗДІЛ ІІІ. Налаштування віддаленого доступу та захисту на активне обладнання

## 3.1 Налаштування захисту та конфігурування функцій безпеки

Відповідно до завдання потрібно налаштувати стандартні списки контролю доступу на заборону проходження трафіку в наступних напрямках:

* відправник NET4, одержувач NET2;
* відправник NET2, одержувач NET1;
* відправник NET4, одержувач NET6.

Розширені списки налаштовуються на заборону проходження трафіку в наступних напрямках:

* відправник NET2, одержувач NET5, протокол TFTP;
* відправник NET1, одержувач NET3, протокол NETBIOS.

Налаштуємо стандартний список контролю доступу на маршрутизаторі Rt4.

Router(config)#access-list 1 deny 192.168.19.202 0.0.0. 255

Router(config)#access-list 1 permit 192.168.19.205 0.0.0.255

Застосуємо цей список до відповідного порту маршрутизатора у вихідному напрямку.

Router(config)#int g0/0

Router(config-if)#ip access-group 1 out

Налаштуємо стандартний список контролю доступу на маршрутизаторі Rt2.

Router(config)#access-list 1 deny 192.168.19.46 0.0.0.15

Router(config)#access-list 1 permit 192.168.19.197 0.0.0.255

Застосуємо цей список до відповідного порту маршрутизатора у вихідному напрямку.

Router(config)#int g0/2

Router(config-if)#ip access-group 1 out

Налаштуємо стандартний список контролю доступу на маршрутизаторі Rt1.

Router(config)#access-list 1 deny 192.168.19.128 0.0.0.63

Router(config)#access-list 1 permit 192.168.19.198 0.0.0.255

Застосуємо цей список до відповідного порту маршрутизатора у вихідному напрямку.

Router(config)#int g0/0

Router(config-if)#ip access-group 1 out

Налаштуємо розширений список контролю доступу на маршрутизаторі Rt2.(TFTP)

Router(config)# access-list 101 deny udp 192.168.19.46 0.0.0.15 192.168.19.30 0.0.0.31 eq 69

Router(config)#access-list 101 permit ip any any

Застосуємо цей список до відповідного порту маршрутизатора у вхідному напрямку.

Router(config)#int g2/0

Router(config-if)#ip access-group 1 in

Налаштуємо розширений список контролю доступу на маршрутизаторі Rt2.(NETBIOS)

Router(config)#access-list 101 deny tcp 192.168.19.30 0.0.0.31 192.168.19.197 0.0.0.255 eq 139

Router(config)#access-list 101 permit ip any any

Застосуємо цей список до відповідного порту маршрутизатора у вхідному напрямку.

Router(config)#int g0/0

Router(config-if)#ip access-group 1 in

Переглянемо списки контролю доступу на маршрутизаторах.

Списки контролю доступу маршрутизатора Rt2.

Router#show access-lists

Standard IP access list 1

10 deny 192.168.19.202 0.0.0. 255 (21 match(es))

20 permit 192.168.19.205 0.0.0.255 (16 match(es))

Extended IP access list 101

10 deny udp 192.168.19.46 0.0.0.15 192.168.19.30 0.0.0.31 eq snmp (1 match(es))

20 permit ip any any (6 match(es))

Списки контролю доступу маршрутизатора Rt3.

Router#show access-lists

Standard IP access list 1

10 deny 192.168.19.46 0.0.0.15 (22 match(es))

20 permit 192.168.19.197 0.0.0.255 (4 match(es))

Extended IP access list 101

10 deny tcp 192.168.19.30 0.0.0.31 192.168.19.197 0.0.0.255 eq www (12 match(es))

20 permit ip any any (6 match(es))

Списки контролю доступу маршрутизатора Rt4.

Router#show access-lists

Standard IP access list 1

10 deny 192.168.19.128 0.0.0.63 (5 match(es))

20 permit 192.168.19.198 0.0.0.255 (23 match(es))

## 3.2 Налаштування віддаленого доступу до активного обладнання

Вихідні дані до завдання наведені в таблиці. 3.2.1 та рисунку 3.2.1.

Таблиця 3.2.1

Вихідні дані до завдання

|  |  |
| --- | --- |
| № Вар. | IP-Адреса |
| 19 | 32.2.0.0/16 |

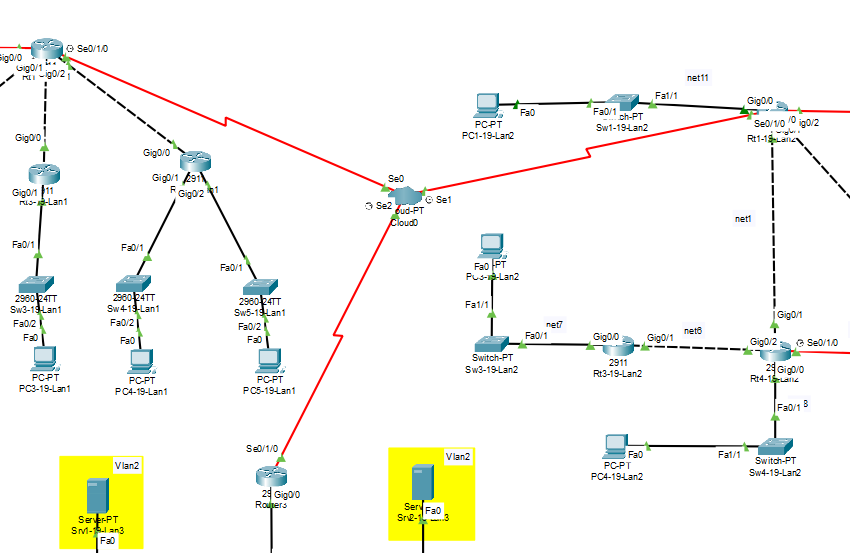


Рисунок 3.2.1 Структурна схема мережі

Вказуємо DLCI:

* R1-19-Lan1 – R1-19-Lan2 – 102
* R1-19-Lan2 – R1-19-Lan1 – 201
* R1-19-Lan1 – R1-19-Lan3 – 103
* R1-19-Lan3 – R1-19-Lan1 – 301
* R1-19-Lan2 – R1-19-Lan3 – 203
* R1-19-Lan3 – R1-19-Lan2 – 302

IP-адреси маршрутизаторів:

* R1-19-Lan1 – 32.2.0.1/16
* R1-19-Lan2 – 32.2.0.2/16
* R1-19-Lan3 – 32.2.0.3/16

Налаштування – все DLCI-і виходять назовні з нашого маршрутизатора через один загальний serial інтерфейс.

Router #

Router #configure terminal

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

Router (config)#interface serial0/0/0

Router (config-if)#no shutdown

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

Router (config-if)#encapsulation frame-relay

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

Router (config-if)#ip address 32.2.0.1 255.255.255.0

Router (config-if)#bandwidth 64

Router (config-if)#frame-relay map ip 32.2.0.2 102 broadcast

Router (config-if)#frame-relay map ip 32.2.0.3 103 broadcast

Налаштування досить проста: ми вказали включили інтерфейс, налаштували інкапсуляцію і ip адреса, за допомогою bandwith повідомили маршрутизатору реальну швидкість каналу (щоб потім, наприклад, метрика правильно вважалася) і додали два рядки в карту framerelay, повідомивши, що 32.2.0.2 знаходиться за DLCI-ем 102, а 32.32.0.3 – за 103. Слово broadcast означає В даному контексті ось що: Сам FR не підтримує широкомовний трафік, але якщо ми задаємо це слово, то при необхідності відправки брудкаста, він буде замінений на безліч юнікастових фреймів – для всіх одержувачів. Без цього слова не працюватимуть, наприклад, протоколи динамічної маршрутизації.

**Налаштування R2:**

Router #configure terminal

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

Router (config)#interface serial 0/0/0

Router (config-if)#no shutdown

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

Router (config-if)#encapsulation frame-relay

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

Router (config-if)#ip address 32.2.0.2 255.255.255.0

Router (config-if)#frame-relay map ip 32.2.0.1 201 broadcast

Router (config-if)#frame-relay map ip 32.2.0.3 203 broadcast

Router (config-if)#bandwidth 64

**Аналогічно налаштовуємо R3:**

Router #configure terminal

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

Router (config)#interface serial 0/0/0

Router (config-if)#no shutdown

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

Router (config-if)#encapsulation frame-relay

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

Router(config-if)#ip address 32.2.0.3 255.255.255.0

Router (config-if)#frame-relay map ip 32.2.0.1 301 broadcast

Router (config-if)#frame-relay map ip 32.2.0.2 302 broadcast

Router (config-if)#bandwidth 64

## 3.3 Моделювання та тестування роботи розробленої мережі

Нам було поставлене завдання створити 3 локальні мережі з трьома різними типами маршрутизації. Перша мережа – мережа центрального офісу її ми налаштовували за допомогою статичної маршрутизації та масок змінної довжини, результат тестування даної задачі можна подивитись на рисунку 3.3.1.

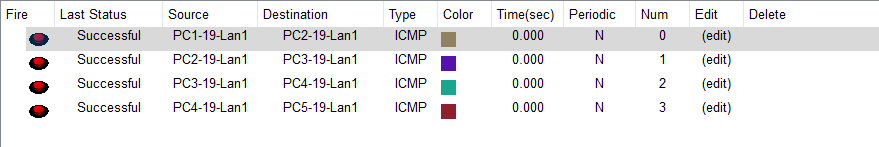


Рисунок 3.3.1 Результат ходження пакетів Lan1

Друга мережа – мережа віддаленого офісу була сконфігурована за допомогою масок фіксованої довжини та статичної маршрутизації, яку ми налаштували за допомогою протоколу Girp, результат тестування даної задачі можна подивитись на рисунку 3.3.2.

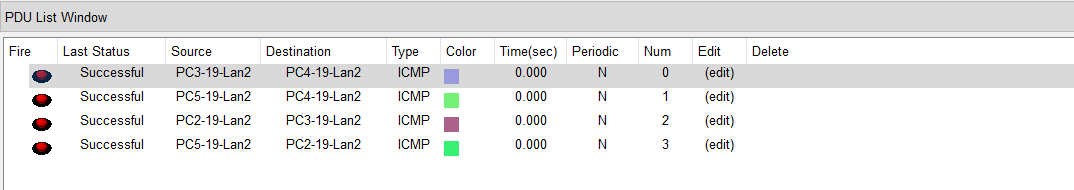


Рисунок 3.3.2 Результат ходження пакетів Lan2

І третя мережа – мережа дата-центру була спроектована за допомогою віртуальних локальних мереж VLAN, результат тестування даної задачі можна подивитись на рисунку 3.3.3.

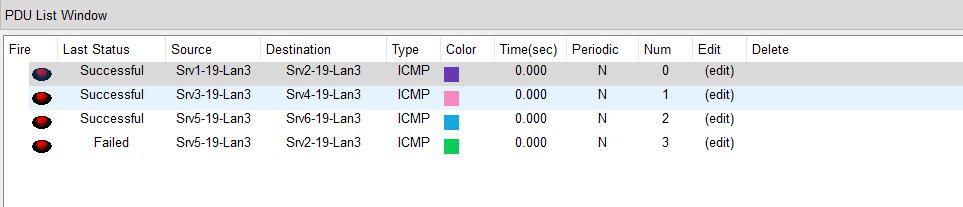


Рисунок 3.3.3 Результат ходження пакетів Lan3

Також для зв’язку між різними VLAN-ми був налаштований inter-VLAN routing. Всі маленькі підмережі були з’єднані в одну за допомогою serial-з’єднань і статичної маршрутизації, результат тестування даної задачі можна подивитись на рисунку 3.3.4.

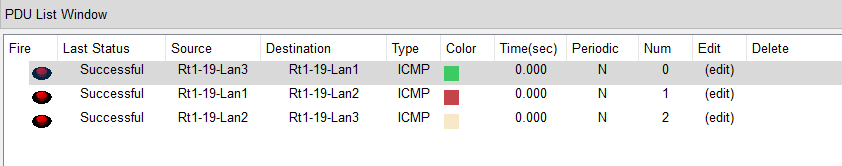
****

Рисунок 3.3.4 Результат ходження пакетів всієї мережі

# ВИСНОВКИ

В даній курсовій роботі було розв’язано наступні завдання:

* спроектовано локальну мережу центрального офісу;
* розраховано адресний простір мереж центрального та віддаленого офісів;
* налаштовано функції безпеки за допомогою списків контролю доступу за протоколами TFTP та NETBIOS;
* налаштовано VLANи дата центру
* здійснено конфігурацію маршрутизаторів мережі центрального офісу для статичної маршрутизації;
* на маршрутизаторах мережі віддаленого офісу налаштовано маршрутизацію EGIRP.

В результаті виконання даної курсової роботи були отримані навички проектування, розрахунку та налаштування корпоративної мережі. Дані комп’ютерні мережі стабільно функціонують, мають запас адресного простору для розширення та налаштовані для безпечного використання в корпоративному середовищі.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Виснадул Б.Д. Основы компьютерных сетей: учебное пособие / Виснадул Б.Д., Лупин С.А., Сидоров С.В., Чумаченко П.Ю.; под ред. Гагариной Л.Г. - М.: ИД «Форум» : ИНФРА-М, 2007. - 272 с.
2. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов / Олифер В.Г., Олифер Н.А. - СПб.: Питер, 2010. - 944 с.
3. Олифер В.Г. Сетевые операционные системы : Учебник для вузов / Олифер В.Г., Олифер Н.А. - СПб. : Питер, 2009. - 672 с.
4. Сергеев А. Офисные локальные сети / Сергеев А. - М.: Диалектика, 2009.- 320 с.
5. Столингс В. Современные компьютерные сети / Столингс В. - СПб.: Питер, 208. - 784 с.
6. Таненбаум Э.С. Компьютерные сети / Таненбаум Э.С. - М.: Питер, 2003. - 992 с.
7. Stevens W. R. TCP/IP Illustrated, Volume 1: The Protocols [Текст] / W. Richard Stevens - Addison Wesley Professional, 1994. - 1021 с.
8. Stevens W. R. Unix Network Programming, Volume 1: The Sockets Networking API [Текст] / W. Richard Stevens, Bill Fenner, Andrew M. Rudoff. - Addison Wesley Professional, 2004. - 1004 c.
9. Инфопедия [Електронний ресурс]. –

Режим доступу: <https://infopedia.su/7xd4cc.html>

1. Банк рефератов[Електронний ресурс]. –

Режим доступу: <https://www.bestreferat.ru/referat-53782.html>

1. Калькулятор[Електронний ресурс]. –

Режим доступу: [https://ip-calculator.ru/#!ip=192.168.19.64/27](https://ip-calculator.ru/%23!ip=192.168.19.64/27)

1. Студфайл [Електронний ресурс]. –

Режим доступу: <https://studfile.net/preview/5118185/page:37/>

1. Студопедия [Електронний ресурс]. –

Режим доступу: <https://studopedia.su/15_159458_topologiya-globalnih-merezh.html>

1. Топология [Електронний ресурс]. –

Режим доступу: <https://static-course-assets.s3.amazonaws.com/ITE50UK/course/module6/6.5.1.1/6.5.1.1.html>

1. Топология [Електронний ресурс]. –

Режим доступу: <http://ciscotips.ru/framerelay>

# ДОДАТОК А

Параметри мережі між маршрутизаторами

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Мережа | Маршрутизатор | Номер порту | Адреса | Маска |
| Rt1-19-Lan2 – Rt2-19-Lan2 | Rt1-19-Lan2 | g0/2/0 | 10.6.19.13 | /30 |
| Rt1-19-Lan2 – Rt2-19-Lan2 | Rt2-19-Lan2 | g0/2/0 | 10.6.19.14 | /30 |
| Rt1-19-Lan2 – Rt5-19-Lan2 | Rt1-19-Lan2 | g0/2 | 10.6.19.17 | /30 |
| Rt1-19-Lan2 – Rt5-19-Lan2 | Rt5-19-Lan2 | g0/1 | 10.6.19.18 | /30 |
| Rt1-19-Lan2 – Rt4-19-Lan2 | Rt1-19-Lan2 | g0/1 | 10.6.19.1 | /30 |
| Rt1-19-Lan2 – Rt4-19-Lan2 | Rt4-19-Lan2 | g0/1 | 10.6.19.2 | /30 |
| Rt2-19-Lan2 – Rt5-19-Lan2 | Rt2-19-Lan2 | Se0/1/0 | 10.6.19.9 | /30 |
| Rt2-19-Lan2 – Rt5-19-Lan2 | Rt5-19-Lan2 | Se0/1/0 | 10.6.19.10 | /30 |
| Rt3-19-Lan2 – Rt4-19-Lan2 | Rt3-19-Lan2 | g0/1 | 10.6.19.22 | /30 |
| Rt3-19-Lan2 – Rt4-19-Lan2 | Rt4-19-Lan2 | g0/2 | 10.6.19.21 | /30 |
| Rt4-19-Lan2 – Rt5-19-Lan2 | Rt4-19-Lan2 | Se0/1/0 | 10.6.19.5 | /30 |
| Rt4-19-Lan2 – Rt5-19-Lan2 | Rt5-19-Lan2 | Se0/1/1 | 10.6.19.6 | /30 |

# ДОДАТОК Б

Параметри під мережевого офісу

|  |  |  |
| --- | --- | --- |
| PC1-19-Lan2 | Адрес мережі: | 10.6.19.62 |
| Маска мережі: | 255.255.255.252 |
| Адрес першого вузла: | 10.6.19.63 |
| Широкомовна адреса: | 10.6.19.93 |
| Адреса останнього вузла: | 10.6.19.92 |
| PC2-19-Lan2 | Адрес мережі: | 10.6.19.94 |
| Маска мережі: | 255.255.255.252 |
| Адрес першого вузла: | 10.6.19.95 |
| Широкомовна адреса: | 10.6.19.125 |
| Адреса останнього вузла: | 10.6.19.124 |
| PC3-19-Lan2 | Адрес мережі: | 10.6.19.126 |
| Маска мережі: | 255.255.255.252 |
| Адрес першого вузла: | 10.6.19.127 |
| Широкомовна адреса: | 10.6.19.157 |
| Адреса останнього вузла: | 10.6.19.156 |
| PC4-19-Lan2 | Адрес мережі: | 10.6.19.158 |
| Маска мережі: | 255.255.255.252 |
| Адрес першого вузла: | 10.6.19.159 |
| Широкомовна адреса: | 10.6.19.189 |
| Адреса останнього вузла: | 10.6.19.188 |
| PC5-19-Lan2 | Адрес мережі: | 10.6.19.190 |
| Маска мережі: | 255.255.255.252 |
| Адрес першого вузла: | 10.6.19.191 |
| Широкомовна адреса: | 10.6.19.223 |
| Адреса останнього вузла: | 10.6.19.224 |

# ДОДАТОК В

Параметри дата центру

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| VLAN1 | | | VLAN2 | | VLAN3 | |
|  | Srv1-19-Lan3 | Srv2-19-Lan3 | Srv5-19-Lan3 | Srv6-19-Lan3 | Srv3-19-Lan3 | Srv4-19-Lan3 |
| Адреса мережі | 181.218.0.3 | 181.218.0.2 | 186.165.0.3 | 186.165.0.2 | 205.186.160.3 | 205.186.160.2 |
| Маска мережі | /29 | /29 | /29 | /29 | /29 | /29 |
| Адреса першого вузла | 181.218.0.1 | 181.218.0.1 | 186.165.0.1 | 186.165.0.1 | 205.186.160.1 | 205.186.160.1 |
| Адреса останнього вузла | 181.218.0.6 | 181.218.0.6 | 186.165.0.6 | 186.165.0.6 | 205.186.160.6 | 205.186.160.6 |
| Широкомовна | 181.218.0.7 | 181.218.0.7 | 186.165.0.7 | 186.165.0.7 | 205.186.160.7 | 205.186.160.7 |