**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**

**БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ**

**КУРСОВА РОБОТА**

з дисципліни

**КОМП’ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ (РІВЕНЬ D - БЕЗПЕКА КОМП`ЮТЕРНИХ СИСТЕМ).**

(назва дисципліни)

на тему: **ПРОЕКТУВАННЯ КООПЕРАТИВНОЇ МЕРЕЖІ.**

Студента(ки) 3 курсу 303 групи

спеціальності «Кібербезпека»

Дегтерьов О.О. (прізвище та ініціали)

Керівник

доцент кафедри

(посада, вчене звання, науковий ступінь,

Гордєєв О.О.

(прізвище та ініціали)

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

Кількість балів: \_\_\_\_

Оцінка: ECTS \_\_\_\_

Члени комісії

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

(підпис) (прізвище та ініціали)

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

(підпис) (прізвище та ініціали)

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

(підпис) (прізвище та ініціали)

Київ - 2020 рік

**ТЕХНІЧНЕ ЗАВДАННЯ**

Варіант 3

На розробку і конфігурування комп’ютерної мережі

1. Область застосування — комп’ютерні мережі.

2. Основа розробки — робочий навчальний план дисципліни.

3. Мета та експлуатаційне призначення:

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

3.2. призначення розробки — навчальна курсова робота із дисципліни «Комп’ютерні системи та мережі (Рівень D - Безпека комп`ютерних систем)»;

4. Джерела розробки — індивідуальне завдання на курсовий проект із дисципліни, технічні рекомендації щодо проектування локальних та розподілених мереж та інші технічні матеріали для налаштування окремих компонентів мережі.

5. Технічні вимоги

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

5.2. Вимоги для проектування LAN1

5.2.1. Адреса мережі 10.0.3.0

5.2.2. Складається з п’яти сегментів, кількість робочих станцій в кожному з яких становить: 60, 5, 13, 27, 25.

5.2.3. Розподіл адресного простору має бути оптимальним;

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

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

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

5.2.7. У середині мережі використовується статична маршрутизація.

5.2.8. На маршрутизаторах Rt2-Rt4 налаштувати DHCP-сервіс і забезпечити динамічне призначення адрес хостам в мережах Net1-Net5.

5.2.9. На маршрутизаторі Rt1 налаштовано сервіс трансляції адрес NAT.

5.3. Вимоги для проектування LAN2

5.3.1. Адреса мережі 172.13.0.0/24

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

5.3.3. Розподілити адресний простір таким чином: в мережах, що з’єднують маршрутизатори, використовувати префікс 30 (маска 255.255.255.252), весь вільний простір, що залишається, рівномірно поділити між мережами, в яких розташовані Switch1- Switch5.

5.3.4. З’єднання між маршрутизаторами Rt4-Rt5 та Rt5-Rt3 здійснюється за допомогою послідовних інтерфейсів з використанням протоколів канального рівня HDLC та РРР відповідно. Інші з’єднання виконуються за допомогою скрученої пари.

5.3.5. Під’єднання мережі LAN2 до мережі WAN виконується через маршрутизатор Rt5.

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

5.3.7. На маршрутизаторі Rt5 налаштовано сервіс трансляції адрес NAT.

5.4. Вимоги для проектування LAN3

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

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

5.4.3. На комутаторах Sw1 Sw2 до Vlan 2 належать порти FastEtherne16-FastEthernet19 та FastEthernet4-FastEthernet7 відповідно, до Vlan 3 FastEthernet20-FastEthernet123 та FastEthernet10-FastEthernet15 відповідно.

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

5.4.5. В віртуальних мережах VLAN1, VLAN2 та VLAN3 використовуються адреси 10.0.3.0, 172.13.0.0 та 7.0.0.0 відповідно.

5.5. Вимоги для проектування WAN

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

5.5.2. Адреси інтерфейсів маршрутизаторів, що під’єднані до Frame Relay мережі, належать до мережі з адресою 22.2.1.0/24

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

5.6. Загальні вимоги до налаштувань маршрутизаторів

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

5.6.2. Налаштувати доступ через протокол SSH до шлюзових маршрутизаторів.

6. Апаратні вимоги - використання обладнання фірми Cisco

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

8. Стадії та етапи розробки мережі включать розробку та відлагодження окремих LAN та об’єднання LAN1-4 за допомогою WAN мережі.

Розробив студент групи 303-Кб Дегтерьов Олександр Олександрович

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ**

**БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ**

Спецiальність: «Кібербезпека»

Курс 3 Група 303-Кб Семестр 5

Дисципліна Компютерні системи та мережі (Рівень D - Безпека комп`ютерних систем)

**ЗАВДАННЯ**

**на курсову роботу студента/студентки**

**Дегтерьова Олександра Олександровича**

(прiзвище, iм`я, по батьковi)

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

2. **Термiн здачi студентом закiнченої роботи**  18.12.2020

**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 |
| 10.0.3.0 | | 60 | | | 5 | | | 13 | | 27 | | | | 25 |
| ст. ACL | | відпр. | | отр. | | | відпр. | | | отр. | | відпр. | | | | отр. |
| Net5 | | Net3 | | | Net1 | | | Net6 | | Net2 | | | | Net3 |
| розш. ACL | | відпр. | | отр. | | | відпр. | | | отр. | | відпр. | | | | отр. |
| Net3 | | Net1 | | | 11,12,13 | | | Net2 | | Net5 | | | | 8,14,15 |
| LAN №2 | № сх. | | | ІР-адреса | | Serial HDLC | | | Serial PPP | | | Шлюз | | | Тип маршрутизації | | |
| 3 | | | 172.17.3.0/24 | | Rt1-Rt3 | | | Rt1-Rt2 | | | Rt3 | | | EIGRP | | |
| LAN №3 | Net1 | Net2 | | | Net3 | | Switch1 | | | | | | | Switch3 | | | |
| Vlan 2 | | | Vlan 3 | | | | Vlan 2 | | Vlan 3 | |
| 141.134.0.0 | 7.0.0.0 | | | 92.0.0.0 | | 3-8 | | | 15-16 | | | | 17-21 | | 18-21 | |

6. Дата видачі завдання “ 16.09 ” 20 20 р



**КАЛЕНДАРНИЙ ПЛАН**

|  |  |  |
| --- | --- | --- |
| № з/п | Назва етапу роботи | Термін виконання |
| 1 | Отримання завдання | 16.09 |
| 2 | Аналіз технічної задачі | 26.09 |
| 3 | Розробка структурної схеми | 03.10 |
| 4 | Встановлення IР-адрес мережевих інтерфейсів | 10.10 |
| 5 | Налагодження серверів | 17.10 |
| 6 | Планування дозволу імен | 31.10 |
| 7 | З’єднання частин мережі за допомогою маршрутизаторів | 14.11 |
| 8 | Моделювання потоків трафіку в мережі | 21.11 |
| 9 | Розрахунок PDV | 28.11 |
| 10 | Оформлення пояснювальної записки | 12.12 |
| 11 | Захист курсової роботи | 18.12 |

Студент Дегтерьов О.О. (підпис)

Керівник Гордєєв О.О. (підпис)

АНОТАЦІЯ

Даний курсовий проект присвячений побудові симуляції кооперативної мережі в середовищі Cisco Packet Tracer. Повинна бути побудована загальна мережа, що складається з трьох, поєднаних віддаленим доступом одна до одної. В мережах налаштовується кожен кінцевий пристрій на предмет безпеки функцій, до яких повинен мати доступ лише мережевий адміністратор.

Для виконання завдання будуть використовуватись навички отримані під час вивчення нинішнього курсу з безпеки кооперативних мереж та при вивченні попереднього курсу основ мережевого проектування та маршрутизації.

**ЗМІСТ**

[ВСТУП 6](#_Toc58703924)

[РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОЇ СКЛАДОВОЇ 7](#_Toc58703925)

[1.1 Аналіз сучасних технологій локальних та глобальних мереж 7](#_Toc58703926)

[1.1.1 Основні види фізичних топологій 8](#_Toc58703927)

[1.1.2 Кабелі та інтерфейси 10](#_Toc58703928)

[1.1.3 Комунікаційна апаратура 14](#_Toc58703929)

[1.2 Розрахунок адресного простору 15](#_Toc58703930)

[1.2.1 Розподіл адрес для мережі центрального офісу (LAN1) 18](#_Toc58703931)

[1.2.2 Розподіл адрес для мережі офісу з віддаленим доступом (LAN2) 20](#_Toc58703932)

[1.2.3 Розподіл адрес для мережі дата-центру (LAN3) 21](#_Toc58703933)

[1.3. Вибір та налаштування способу маршрутизації 22](#_Toc58703934)

[РОЗДІЛ 2 КОНФІГУРУВАННЯ МЕРЕЖЕВОГО ОБЛАДНАННЯ 26](#_Toc58703935)

[2.1 Конфігурування базових функцій маршрутизаторів 26](#_Toc58703936)

[2.2 Проектування віртуальних мереж (VLAN) 27](#_Toc58703937)

[2.3 Конфігурування базових функцій комутаторів LAN 28](#_Toc58703938)

[РОЗДІЛ 3 НАЛАШТУВАННЯ БЕЗПЕКИ ТА ВІДДАЛЕНОГО ДОСТУПУ НА АКТИВНЕ ОБЛАДНАННЯ 29](#_Toc58703939)

[3.1 Налаштування захисту та додаткових функцій маршрутизаторів 29](#_Toc58703940)

[3.2 Налаштування віддаленого доступу до активного обладнання 32](#_Toc58703941)

[3.3 Моделювання та тестування роботи розробленої межі 32](#_Toc58703942)

[ВИСНОВКИ 37](#_Toc58703943)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 38](#_Toc58703944)

[ДОДАТОК А 39](#_Toc58703945)

# ВСТУП

Широке використання інформаційних технологій у всіх сферах життя суспільства робить досить актуальною проблему захисту інформації, її користувачів, інформаційних ресурсів, каналів передачі даних від злочинних зазіхань зловмисників.

Складність створення системи захисту інформації визначається тим, що дані можуть бути викрадені з комп'ютера (скопійовані), одночасно залишаючись на місці. Цінність деяких даних полягає у володінні ними, а не в їх знищенні або зміні.

Забезпечення безпеки інформації – справа дорога, і не стільки через витрати на закупівлю або установку різних технічних або програмних засобів, скільки через те, що важко кваліфіковано визначити межі розумної безпеки і відповідної підтримки системи в працездатному стані.

Об'єктами зазіхань можуть бути як самі матеріальні технічні засоби (комп'ютери і периферія), так і програмне забезпечення і бази даних.

Кожен збій роботи комп'ютерної мережі - це не тільки моральний збиток для працівників підприємства і мережевих адміністраторів. В міру розвитку технологій електронних платежів, «безпаперового» документообігу серйозний збій локальних мереж може паралізувати роботу цілих підприємств, що приведе до відчутних збитків. Не випадково захист даних у комп'ютерних мережах стає однією із найгостріших проблем.

# РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОЇ СКЛАДОВОЇ

## 1.1 Аналіз сучасних технологій локальних та глобальних мереж

Локальна комп’ютерна мережа – це набір комп’ютерів, периферійних пристроїв ( принтерів, сканерів тощо ) і комутаційних пристроїв, які з’єднані кабелями. Досвід експлуатації мереж показує, що майже 80% всієї інформації, що пересилається по мережі, замикається в рамках одного офісу. За міжнародними стандартами мережа вважається локальною при відстанях до декількох кілометрів та при швидкостях передачі 1-20 Мбіт/сек.

Локальні мережі бувають двох типів: однорангові мережі та мережі з виділеним сервером. Однорангові мережі, прикладом яких є мережі на основі Windows, не передбачають виділення спеціальних комп’ютерів, які організовують роботу мережі. Кожен користувач виділяє для мережі певні ресурси (дисковий простір, принтер) і підключається до ресурсів, які надають інші користувачі. Мережі з виділеним сервером складніші та дорожчі, ніж однорангові мережі, але вони дозволяють здійснювати централізоване управління з використанням спеціальних комп’ютерів (серверів).

Глобальна комп’ютерна мережа – це єдина мережа із стійкою структурою, що обслуговується тільки однією групою спеціалістів, які відповідають за її функціонування. В Україні існує декілька глобальних комп’ютерних мереж (Relcom, Sprint, Glasnet, Roshet), які можуть спілкуватись між собою та зарубіжними комп’ютерними мережами. Коли комп’ютерна мережа надає послуги з міжнародного обміну, то вона стає частиною Internet. Internet була створена на основі американської мережі ARPAnet (Advanced Research Projects Agency net – мережа Управління перспективними дослідженнями), яку розробили наприкінці 60-х років на замовлення Міністерства оборони США. Основоположним принципом побудови цієї мережі було те, що кожний комп’ютер міг спілкуватись як вузол з будь-яким іншим комп’ютером. Принципи організації ARPAnet виявилися настільки вдалими, що багато інших організацій (особливо університети та урядові органи США) почали створювати за цими принципами власні мережі, які згодом почали з’єднувати між собою. Internet – це група комп’ютерних мереж, поєднаних між собою комп’ютерами-шлюзами, які відповідають за передачу та конвертацію повідомлень згідно з протоколами мереж учасників. Internet має багато спільних рис із звичайною глобальною мережею, але відрізняється своєю побудовою. Internet складається з великої кількості незалежних мереж, які спілкуються між собою єдиною мовою зв’язку, тобто з допомогою міжмережевого протоколу IP (Internet Protocol), і немає жодної окремої групи людей або організації, що відповідають за її роботу.

### 1.1.1 Основні види фізичних топологій

Існує чотири основних фізичних топології, що використовуються при побудові локальних обчислювальних мереж.

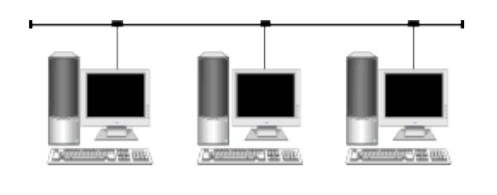


Рисунок 1.1 Топологія «Шина»

Топологія шини «рисунок1.1» передбачає підключення всіх комп'ютерів до одного спільного провідника. На обох кінцях такого провідника розміщуються спеціальні узгоджувальні пристрої, які називаються термінаторами. Основні переваги даної топології – дешевизна і простота монтажу. До недоліків відносяться проблематичність локалізації місця несправності і низька надійність: пошкодження кабелю в будь-якому місці призводить до припинення обміну інформацією між усіма комп'ютерами, що входять в мережу. Через особливості поширення електричного сигналу, навіть якщо два комп'ютери, які намагаються здійснити обмін інформацією, фізично з'єднані один з одним, при відсутності термінатора на одному кінці такого «обривка» шини зв'язок між ними буде неможливий.



Рисунок 1.2 Топологія «Кільце»

У топології «кільце» «рисунок 1.2» кожен абонент мережі пов'язаний з двома прилеглими абонентами. Переваги і недоліки аналогічні розглянутим для топології шини.

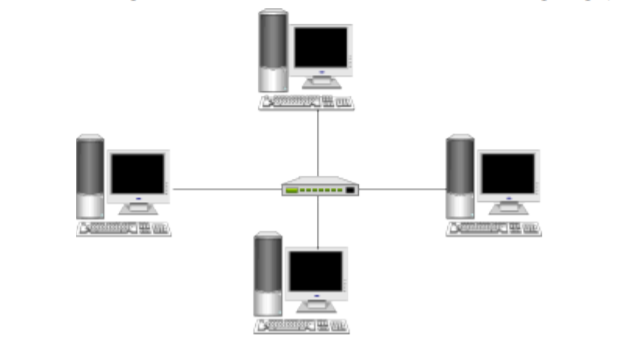


Рисунок 1.3 Топологія «Зірка»

З точки зору надійності і швидкості обміну інформацією найкращими характеристиками володіє повнозв’язана топологія «рисунок 1.3». В цьому випадку абонентам мережі надається окремий канал зв'язку з кожним з інших абонентів. Однак за вартістю дана топологія програє всім іншим варіантам. Перераховані топології є базовими. Більшість локальних обчислювальних мереж, що створюються в різних організаціях, мають більш складну структуру і є різними варіантами комбінування вищезазначених топологій.

### 1.1.2 Кабелі та інтерфейси

В даний час в локальних обчислювальних мережах використовується кілька типів провідників. За фізичну природу сигналу, що передається, розрізняють електричні провідники і оптичні провідники. Крім цього може використовуватися апаратура для організації локальних обчислювальних мереж засобами бездротових каналів.

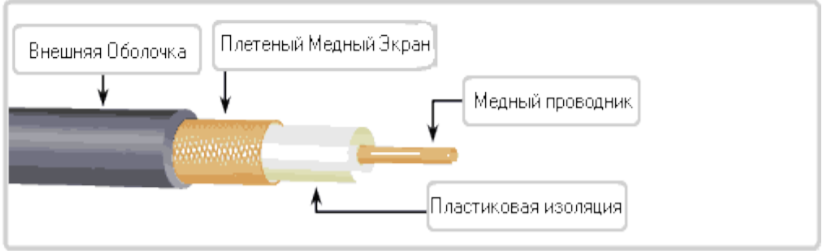


Рисунок 1.4 Коксіальний кабель

Коаксіальний кабель «рисунок 1.4» являє собою провідник, укладений в екрануюче обплетення. Від контакту з опліткою провідник захищений трубчастим ізолятором. Важливою характеристикою кабельних систем взагалі і коаксіального кабелю зокрема є хвильовий опір або імпеданс. У локальних обчислювальних мережах застосовується коаксіальний кабель з хвильовим опором 50 Ом і (набагато рідше) в мережах ARCnet кабель з хвильовим опором 93 Ом. Існує два різновиди коаксіального кабелю - товстий (зовнішній діаметр близько 10 мм) і тонкий (зовнішній діаметр близько 5 мм). При однаковому значенні хвильового опору у товстого і тонкого коаксіального кабелю різні характеристики по довжині кабельного сегмента і кількості підтримуваних абонентів мережі. У товстого коаксіального кабелю максимальна довжина сегмента 500 метрів, максимальна кількість точок підключення 100. У тонкого коаксіального кабеля максимальна довжина сегмента 185 метрів, максимальна кількість точок підключення 30.

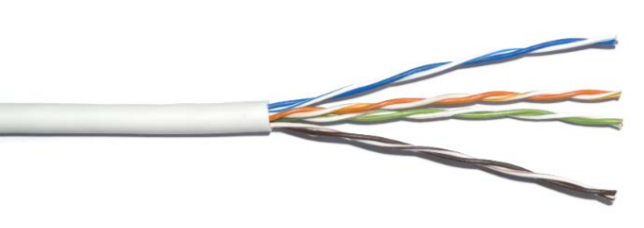


Рисунок 1.5 Кручена вита пара

Другий варіант електричного провідника, який використовується при монтажі локальних обчислювальних мереж, отримав назву кручена пара. Фактично кабель, який називається витою парою, являє собою вісім (рідше чотири) провідника звитих попарно з певним кроком (шість оборотів на дюйм) і укладених в загальну ізолюючу трубку «рисунок 1.5». Такий кабель називається неекранована кручена пара UTP (Unshielded Twisted Pair - неекрановані скорочені пари). Якщо кожна пара перевитих проводів укладена в металевий екран (фольга або обплетення), і потім вся сукупність таких екранованих пар закрита загальним екраном, такий кабель називають екранованою крученою парою STP (Shielded Twisted Pairs - екрановані 10 скручені пари). Застосування екранів дозволяє знизити рівень перешкод, створюваних таким кабелем, і збільшити перешкодозахищеність такого кабелю від зовнішніх перешкод. Швидкість передачі інформації по таким кабелям досягає, в даний час 1000 Мегабіт в секунду.



Рисунок 1.6 Розетка і роз'єм RJ-45

Для підключення мережевої апаратури за допомогою крученої пари найбільш часто використовуються роз'єми RJ-45 «рисунок 1.6», зовні схожі на телефонні, але з вісьмома контактами.

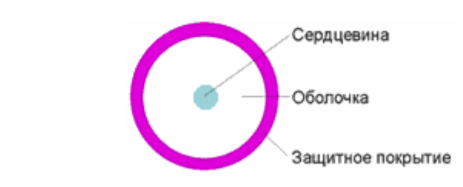


Рисунок 1.7 Оптоволокно

За своєю конструкцією «рисунок 1.7» волоконно-оптичний кабель схожий на коаксіальний, тільки замість центрального металевого провідника розташовується скляне або пластикове волокно через який поширюється пучок світла і замість електричної ізоляції таке волокно оточене оптичної оболонкою, основне завдання якої - не дати пучку світла покинути центральне волокно. Волоконно-оптичний кабель не потребує зовнішнього екрануючого обплетення, оскільки електромагнітні перешкоди не впливають на оптичні сигнали, проте в деяких конструкціях волоконно-оптичних кабелів металеве обплетення застосовується з метою підвищення механічної міцності кабеля і захисту оптичного волокна від механічних пошкоджень. Такий волоконно-оптичний кабель називається броньованим. Залежно від траєкторії поширення променя світла через оптичне волокно розрізняють одномодовий (фактично один промінь) і багатомодовий (сукупність променів з практично однаковими характеристиками, що рухаються по сусідніх траєкторіях) волоконно-оптичний кабель. У багатомодового волоконно-оптичного кабеля діаметр серцевини відносно великий (50, 62,5 або 100 мікрон). Світловий потік, що пропускається багатомодовим волоконно-оптичним кабелем, має довжину хвилі 850 або 1300 нм і, проходячи по такому волокну, відбиваючись від його стін, дробиться на окремі промені (моди) які, накладаючись один на одного, призводять до зниження якості сигналу. Такий кабель називають багатомодовим із ступінчастим профілем. Пізніша модифікація - багатомодовий волоконно-оптичний кабель з градієнтним профілем. За рахунок складної обробки (легування) оптоволокна можна домогтися плавного зменшення показника заломлення світла від центру серцевини до оболонки волокна. Тоді моди, хоча і будуть як і раніше проходити різні шляхи, але робити це за однаковий час. Такий кабель коштує дорожче, але більш якісно (з меншими спотвореннями) передає сигнал. Перевагою багатомодового волоконно-оптичного кабелю є можливість використання в якості джерела світла поряд з лазерами, відносно дешевих спеціальних світлодіодів. Однак навіть багатомодовий волоконно-оптичний кабель з градієнтним профілем за своїми характеристиками поступається одномодовому волоконно-оптичному кабелю.

### 1.1.3 Комунікаційна апаратура



Рисунок 1.8 Комутатор

Комутатор «рисунок 1.8» може розбивати порти на групи, організовуючи логічні сегменти мережі. Комп'ютери «спілкуються» один з одним в межах сегментів, тим 16 самим зменшується кількість колізій і підвищується загальна швидкодія мережі. Окремим випадком комутатора є міст (bridge).



Рисунок 1.9 Маршрутизатор

Маршрутизатор (router) – пристрій «рисунок 1.9» з декількома фізичними інтерфейсами, які можуть належати до однієї або різних мережевих технологій. Використовується для поділу або об'єднання декількох комп'ютерних мереж (наприклад, мережа 100VG-AnyLAN з мережею Ethernet). Завдання маршрутизатора фільтрувати пакети і пропускати з одного інтерфейсного входу на інший тільки ті пакети, які адресовані комп'ютером, що знаходяться в одній мережі комп'ютера, що знаходиться в іншій мережі.

## 1.2 Розрахунок адресного простору

IP-адреса складається з 4 номерів (кожний з них за своєю величиною не більше ніж 255 у десятковому записі). Вони відокремлюються один від одного крапками. Наприклад, 192.33.33.22, 155.66.77.1 – це IP-адреси. Крайнє ліве число означає номер великої мережі, числа, що знаходяться праворуч, – означають більш дрібні ділянки мереж і так далі, поки не дійдемо до конкретного комп'ютера.

IP-адреса складається з 4 номерів (кожний з них за своєю величиною не більше ніж 255 у десятковому записі). Вони відокремлюються один від одного крапками. Наприклад, 192.33.33.22, 155.66.77.1 – це IP-адреси. Крайнє ліве число означає номер великої мережі, числа, що знаходяться праворуч, – означають більш дрібні ділянки мереж і так далі, поки не дійдемо до конкретного комп'ютера. З таким представленням адреси існує багато проблем. Вони дуже важко запам'ятовуються і є довгими. Щоб полегшити розуміння адреси, почали використовувати спеціальні назви (наприклад, dlab.kiev.ua). Таке ім'я називається доменним. З такими адресами легше працювати, тому що доменні імена мають постійну структуру, дивлячись на яку можна легко зрозуміти, якій організації належить ім'я.

Розуміння двійкової системи числення необхідне для того, щоб встановити, чи знаходяться два вузли в одній і тій же мережі. IP -адреса є ієрархічною адресою, яка складається з двох частин: мережевої і вузлової. У 32-бітовому потоці одна частина бітів складає мережу, а інша – вузол. Біти в мережевій частині адреси мають бути однаковими для усіх пристроїв, які знаходяться в одній і тій же мережі. Біти у вузловій частині адреси мають бути унікальними, щоб можна було визначити конкретний вузол в мережі. Незалежно від того, чи співпадають десяткові числа в двох IPv4-адресах, якщо два вузли мають одну бітову комбінацію в певній мережевій частині 32-бітового потоку, то ці два вузли знаходяться в одній і тій же мережі.

При налаштуванні IP -вузла йому привласнюється не лише IP -адреса, але і маска підмережі. Як і IP -адреса, маска складається з 32 біт. Вона визначає, яка частина IP -адреси відноситься до мережі, а яка – до вузла. Маска порівнюється з IP-адресою побітно, зліва направо. У масці підмережі одиниці відповідають мережевій частині, а нулі – адресі вузла «рисунок 1.10».



Рисунок 1.10 Мережева і вузлова частини IP–адреси

Довжина префікса– це ще один спосіб представлення маски підмережі. Довжина префікса означає кількість біт, встановлених на одиницю (1) в масці підмережі. Вона позначається похилою риска вправо («/»), після якої йде набір одиниць. Наприклад, якщо маска підмережі 255.255.255.0, то в двійковій версії маски підмережі на одиницю налаштовані 24 біта, тому довжина префікса складає 24 біта або /24. Префікс і маска підмережі – це різні способи представлення одного і того ж – мережевої частини адреси.

Мережам не завжди призначається префікс /24. Залежно від кількості вузлів в мережі префікс може відрізнятися. Різний префікс призводить до зміни діапазону вузлів і широкомовної адреси для кожної мережі.

У діапазоні адрес кожної мережі IPv4 існують три типи адрес:

* мережева адреса;
* вузлові адреси;
* широкомовна адреса.

Мережева адреса– це стандартний спосіб позначення мережі. Маска підмережі або довжина префікса можуть використовуватися для позначення мережевої адреси. Для обміну даними по мережі кожному крайовому пристрою потрібна унікальна адреса. У IPv4-адресах значення між мережевим і широкомовним адресами можуть бути призначені крайовим пристроям в мережі.

Широкомовна IPv4-адреса– це особлива адреса для кожної мережі, яка здійснює зв’язок для усіх вузлів, розташованих в цій мережі. Для одноразової відправки даних на усі вузли в мережі вузол може відправити один пакет, призначений широкомовній адресі мережі, а кожен вузол в цій мережі, який отримає цей пакет, обробить його вміст.

Для широкомовної розсилки використовується найвища адреса діапазону мережі. У цій адресі усі частини вузла представлені одиницями. Сума одиниць октету в двійковій формі дорівнює значенню 255 в десятковому форматі. Вузлова частина не завжди представлена усім октетом цілком. Також цю адресу називають прямою широкомовною розсилкою.

Щоб упевнитися, що усім вузлам в мережі присвоєна унікальна IP-адреса усередині діапазону мережі, спочатку треба визначити адреси першого і останнього вузлів. У цьому діапазоні вузлам усередині мережі можуть бути присвоєні IP -адреси. Вузлова частина останньої адреси вузла міститиме усі одиниці з нулем в крайньому справа біті. Значення цієї адреси завжди на одиницю менше, ніж значення широкомовної адреси.

### 1.2.1 Розподіл адрес для мережі центрального офісу (LAN1)

Серед вхідних даних до мережі центрального офісу була надана IP-адреса мережі (10.0.3.0), кількість хостів на кожен з комп’ютерів (60, 5, 13, 27, 25). Були виділені хости на кожен з комп’ютерів серед чисел, які є степенем числа 2, які є найближчими, але не меншими за число хостів, що було надано у завданні (60 – 64, 5 – 8, 13 – 16, 27 – 32, 25 – 32). Кожне з чисел кількості виділених хостів було переведено у двійкову систему числення (8 – 1000, 16 – 10000, 32 – 100000, 64 – 1000000), потім перед ними було дописано потрібну кількість одиниць для того, щоб двійкове представлення мало 8 символів, після чого цей двійковий код був переведений у шістнадцяткову систему числення ( 8 – 11111000 – 248, 16 – 11110000 – 240, 32 – 11100000 – 224, 64 – 1100000 – 192). Ці числа будуть займати місце четвертого октету маски підмережі (NET 1 – 255.255.255.192 і т.д.). Далі була створена кругова діаграма розподілу хостів в мережі «рисунок 1.11».

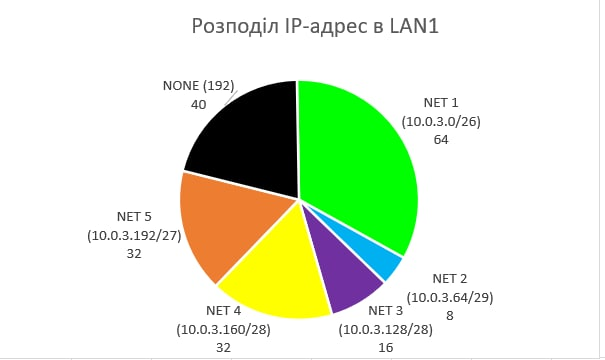


Рисунок 1.11 Розподіл адрес в мережі центрального офісу

На основі кругової діаграми була створена таблиця «таблиця 1.1» більш точного розподілу адрес з урахуванням IP-адреси мережі та широкомовної адреси.

Таблиця 1.1

Розподіл IP-адрес в мережі LAN1

|  |  |  |  |
| --- | --- | --- | --- |
| Мережа | Адреса мережі | Адреси хостів | Широкомовна адреса |
| NET 1 | 10.0.3.0/26 | 10.0.3.1 – 10.0.3.62 | 10.0.3.63 |
| NET 2 | 10.0.3.64/29 | 10.0.3.62 – 10.0.3.70 | 10.0.3.71 |
| NET 3 | 10.03.128/28 | 10.0.3.129 – 10.0.3.158 | 10.0.3.159 |
| NET 4 | 10.0.3.160/27 | 10.0.3.161 – 10.0.3.190 | 10.0.3.191 |
| NET 5 | 10.0.3.192/27 | 10.0.3.193 – 10.0.3.223 | 10.0.3.224 |

Адреси хостів використовуються для налаштування маршрутизації в межах топології центрального офісу. Алгоритм полягає в тому, що крайня найменша адреса надається комп’ютеру (PC-1 має адресу 10.0.3.1 згідно таблиці 1.1), а крайня найбільша – порту маршрутизатора, що з’єднує його з комп’ютером (Rt2 має адресу 10.0.3.62). Алгоритм застосовується до всіх п’яти зв’язків комп’ютер-маршрутизатор.

Для подальшого налаштування маршрутизації потрібно було розширити адресний простір і надати адреси зв’язків для кожного з маршрутизаторів та шлюзового маршрутизатора Rt1, який з’єднує між собою 3 маршрутизатори. На кожен зв’язок маршрутизатор-маршрутизатор було виділено по 2 хости (маска підмережі 255.255.255.252) для оптимальної роботи та була побудована додаткова таблиця «таблиця 1.2» розподілу адрес.

Таблиця 1.2

Розподіл адрес між маршрутизаторами в мережі центрального офісу

|  |  |  |  |
| --- | --- | --- | --- |
| Мережа | Адреса мережі | Адреси хостів | Широкомовна адреса |
| NET 1 | 10.0.3.224/30 | 10.0.3.225 – 10.0.3.226 | 10.0.3.227 |
| NET 2 | 10.0.3.228/30 | 10.0.3.229 – 10.0.3.230 | 10.0.3.231 |
| NET 3 | 10.03.232/30 | 10.0.3.233 – 10.0.3.234 | 10.0.3.235 |
| NET 4 | 10.0.3.236/30 | 10.0.3.237 – 10.0.3.238 | 10.0.3.239 |

Адреси розподілялись за таким самим алгоритмом, тільки крайня найбільша адреса призначалась центральному маршрутизатору Rt1, а крайня найменша – маршрутизаторам Rt2, Rt3 та Rt4.

### 1.2.2 Розподіл адрес для мережі офісу з віддаленим доступом (LAN2)

В мережі офісу з віддаленим доступом розподіл відбувався за допомогою виділення оптимальної кількості хостів на кожне з’єднання маршрутизатор-маршрутизатор (по 2 хости на кожне з’єднання) та розподілом його між кінцевими пристроями. Оскільки на кожну з підмереж було виділено по 2 хости, то адреса мережі матиме вигляд 172.17.3.0/30. З’єднання комп’ютер-маршрутизатор має по 32 хоста кожне, адресу 172.17.3.0/27 та маску 255.255.255.224. Розподіл описано в таблиці «таблиця 1.3».

Таблиця 1.3

Розподіл адрес в мережі LAN2

|  |  |  |  |
| --- | --- | --- | --- |
| Мережа | Адреса мережі | Адреси хостів | Широкомовна адреса |
| NET 1 | 172.17.3.0/30 | 172.17.3.1 – 172.17.3.2 | 172.17.3.2 |
| NET 2 | 172.17.3.4/30 | 172.17.3.5 – 172.17.3.6 | 172.17.3.7 |
| NET 3 | 172.17.3.8/30 | 172.17.3.9 – 172.17.3.10 | 172.17.3.11 |
| NET 4 | 172.17.3.12/30 | 172.17.3.13 – 172.17.3.14 | 172.17.3.15 |
| NET 5 | 172.17.3.16/30 | 172.17.3.17 – 172.17.3.18 | 172.17.3.19 |
| NET 6 | 172.17.3.32/27 | 172.17.3.33 – 172.17.3.62 | 172.17.3.63 |
| NET 7 | 172.17.3.64/27 | 172.17.3.65 – 172.17.3.94 | 172.17.3.95 |
| NET 8 | 172.17.3.96/27 | 172.17.3.97 – 172.17.3.126 | 172.17.3.127 |
| NET 9 | 172.17.3.128/27 | 172.17.3.129 – 172.17.3.158 | 172.17.3.159 |
| NET 10 | 172.17.3.0/27 | 172.17.3.161 – 172.17.3.190 | 172.17.3.191 |

Підмережі з ідентифікаторами 1-5 відповідають за з’єднання маршрутизатор-маршрутизатор, ті, що під номерами 6-10 – комп’ютер-комп’ютер.

### 1.2.3 Розподіл адрес для мережі дата-центру (LAN3)

Мережа віддаленого дата-центру була розбита на 3 підмережі згідно з технічним завданням (одна підмережа – з’єднання двох серверів з маршрутизатором). Для зручності було додано дві додаткових мережі, що відповідали за з’єднання маршрутизаторів між собою. Для трьох основних підмереж в технічному завданні були прописані адреси (141.134.0.0, 7.0.0.0, 92.0.0.0 відповідно). Адреси додаткових підмереж створені на основі уже існуючих адрес (за основу були взяті адреси першої підмережі). Оскільки підмережі 1-3 складаються більше, ніж з двох кінцевих пристроїв, на них було виділено 6 хостів замість двох. На прикладі першої підмережі адреса кожної основної підмережі матиме вигляд 141.134.0.0/29 з маскою 255.255.255.248, в свою чергу для додаткових підмереж було виділено по 2 хости. Так само, як і для перших двох топологій, була створена таблиця «таблиця 1.4» розподілу адрес.

Таблиця 1.4

Розподіл адрес мережі дата-центру

|  |  |  |  |
| --- | --- | --- | --- |
| Мережа | Адреса мережі | Адреси хостів | Широкомовна адреса |
| NET 1 | 141.134.0.0/29 | 172.17.3.1 – 172.17.3.2 | 172.17.3.2 |
| NET 2 | 7.0.0.0/29 | 7.0.0.1 – 7.0.0.6 | 7.0.0.7 |
| NET 3 | 92.0.0.0/29 | 92.0.0.1 – 92.0.0.6 | 92.0.0.7 |
| NET 4 | 141.134.0.8/30 | 141.134.0.9 – 141.134.0.10 | 141.134.0.11 |
| NET 5 | 141.134.0.12/30 | 141.134.0.13 – 141.134.0.14 | 141.134.0.15 |

Кожна адреса була перевірена на коректність сервісом для генерування IP-адрес мереж на основі адреси мережі та маски підмережі.

## 1.3. Вибір та налаштування способу маршрутизації

Комутатори Ethernet функціонують на канальному рівні, тобто 2-му рівні, і використовуються для пересилання кадрів Ethernet між пристроями в межах однієї мережі. Проте коли IP -адреса джерела і призначення знаходяться в різних мережах, кадр Ethernet необхідно відправити на маршрутизатор.

Маршрутизатор використовується для підключення однієї мережі до іншої. Маршрутизатор відповідає за доставку пакетів в різні мережі. Пунктом призначення для IP-пакета може бути веб-сервер, розташований в іншій країні, або сервер електронної пошти в локальній мережі.

Маршрутизатор використовує свою таблицю маршрутизації, щоб знайти оптимальний шлях для пересилки пакетів. Саме маршрутизатори забезпечують своєчасну доставку цих пакетів. Ефективність передачі даних між мережами залежить від можливості маршрутизаторів пересилати пакети по найбільш оптимальному шляху.

Коли вузол відправляє пакет пристрою в іншу IP-мережу, цей пакет пересилається на шлюз за замовчуванням, оскільки вузол не може безпосередньо взаємодіяти з пристроями, розташованими поза локальною мережею. Пунктом призначення в маршрутах трафіку з локальної мережі до пристроїв у віддалених мережах є шлюз за замовчуванням. Цей шлюз часто використовується для підключення локальної мережі до Інтернету.

Розглянемо ключові структури і властивості, пов’язані з продуктивністю мережі.

* + Топологія: існують фізичні і логічні топології. Фізична топологія – схема розташування кабелів, мережевих пристроїв і кінцевих систем. У ній описується, як мережеві пристрої сполучені між собою за допомогою дротів і кабелів. Логічна топологія – це шлях, по якому дані передаються по мережі. У ній описується, як користувачі бачать з’єднання мережевих пристроїв.
  + Швидкість - це кількість переданих даних по якому-небудь каналу мережі, вимірюється у бітах в секунду (біт/с).
  + Вартість вказує загальні витрати на придбання компонентів мережі, установку і обслуговування мережі.
  + Безпека вказує на міру захищеності мережі, у тому числі захищеності інформації, що передається по мережі. Чинник безпеки грає дуже важливу роль, тому технології і методи забезпечення безпеки постійно розвиваються. При будь-яких діях, які можуть вплинути на роботу мережі, необхідно звертати увагу на забезпечення безпеки.
  + Доступність вказує на можливість використання мережі у момент звернення користувача.
  + Масштабованість показує, наскільки легко мережа може вміщати більше число користувачів і відповідати вимогам передачі даних. Якщо проект мережі оптимізований тільки для виконання поточних завдань, то розширення мережі для відповідності зростаючим вимогам несе за собою великі труднощі і високі витрати.
  + Надійність вказує на міру безвідмовності компонентів, з яких складається мережа: маршрутизаторів, комутаторів, комп’ютерів і серверів. Надійність часто вимірюється як вірогідність збою або як середній час безвідмовної роботи (MTBF, Mean time between failures).

Для роботи всіх трьох мереж була обрана статична маршрутизація, оскільки весь трафік може рухатись між пристроями сталими маршрутами і це ніяк не порушить роботу всієї мережі.

Статична маршрутизація налаштовувалась на основі адресних таблиць та була налаштована на кожному маршрутизаторі в обидві сторони для з’єднання між собою комп’ютерів у всій мережі.

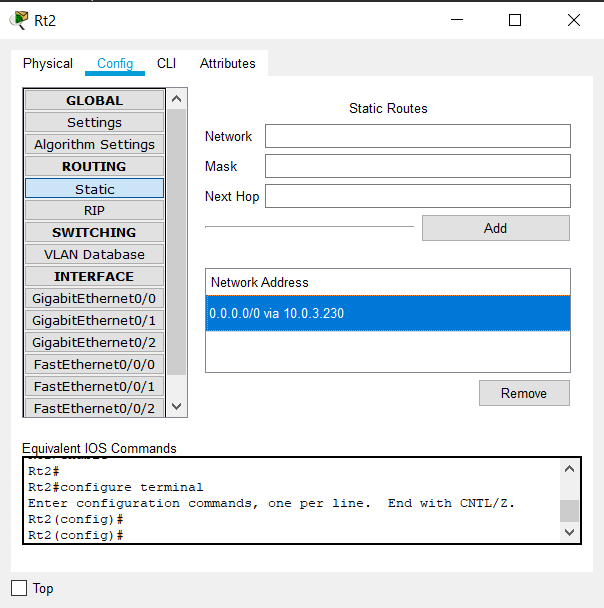


Рисунок 1.12 Інтерфейс налаштування статичної маршрутизації на прикладі маршрутизатора підмережі

Налаштування маршрутизації відбувалось у графічному інтерфейсі Cisco Packet Tracer «рисунок 1.12». Для всіх маршрутизаторів в мережі була прописана мережа 0.0.0.0 з такою ж маскою, а в поле наступного кроку була вписана адреса наступного маршрутизатора.

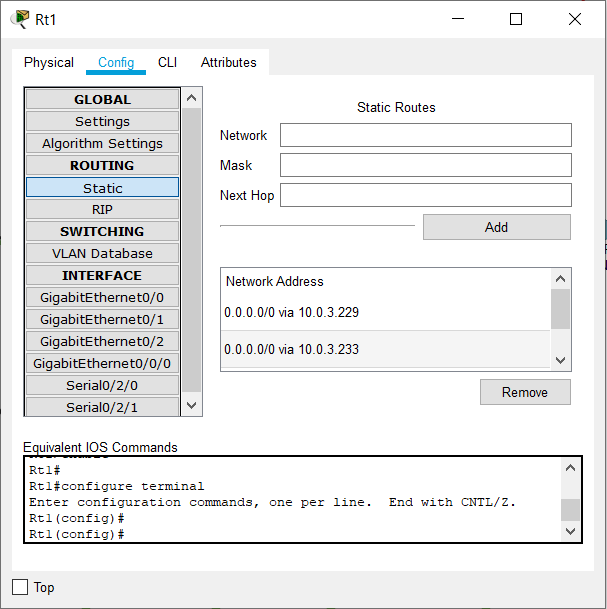


Рисунок 1.13 Налаштування статичної маршрутизації на прикладі шлюзового маршрутизатора

На відміну від маршрутизаторів підмереж, шлюзовий маршрутизатор «рисунок 1.13» має в таблиці адресації більше записів, оскільки кожен з маршрутизаторів підмереж відправляє пакети лише на шлюзовий маршрутизатор, а шлюзовий, в свою чергу, на кожен маршрутизатор підмереж.

Аналогічне налаштування було здійснене в кожній мережі загальної топології.

# РОЗДІЛ 2 КОНФІГУРУВАННЯ МЕРЕЖЕВОГО ОБЛАДНАННЯ

## 2.1 Конфігурування базових функцій маршрутизаторів

Для роботи кожної з мереж було обрано маршрутизатори Cisco 2911, оскільки вони в умовах роботи в середовищі Cisco Packet Tracer одразу мають порти Gigabit Ethernet, які мають найвищу пропускну здатність, що добре впливає на швидкість передачі пакетів даних та які мають зручний інтерфейс для налаштування IP-адрес для кожного такого порту.

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



Рисунок 2.1 Маршрутизатор Cisco 2911

Основними моментами налаштування маршрутизатора є призначення відповідних до описаних вище ІР-адрес, а також налаштування маршрутизації в межах кожної мережі.

## 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).

Віртуальні мережі були налаштовані в топології мережі дата-центру. Відповідно технічного завдання були використанні конкретні пори на серверах, які і були використані для налаштування VLAN на кожному з них.

## 2.3 Конфігурування базових функцій комутаторів LAN

Вибір комутаторів в Cisco Packet Tracer є досить обширним, але найзручнішим та з достатнім функціоналом для запропонованої мережі є Cisco 2960, що має 24 Fast Ethernet порти та можливість доставити велику кількість додаткових портів будь-якого типу. Для кожного з таких комутаторів були доставлені порти Gigabit Ethernet для зручного налаштування адрес та кращої пропускної здатності обладнання.

Інтелектуальні Ethernet-комутатори Cisco Catalyst серії 2960 (Cisco Catalyst 2960 Series Intelligent Ethernet Switch) дозволяють реалізувати розширені сервіси в локальних мережах великих і середніх підприємств, а також в мережах філій. Представники цього сімейства автономних комутаторів з фіксованою конфігурацією забезпечують підключення робочих місць на швидкостях 10/100 Fast Ethernet і 10/100/1000 Gigabit Ethernet.

Комутатори в кожній з мереж виконують функцію посередника між комп’ютером та маршрутизатором. Аналогічно кожному маршрутизатору, на комутаторах був встановлений пароль на привілейований режим, а також в мережі дата-центру кожне з’єднання між двома комутаторами були налаштоване для поділу серверів на підмережі та для можливості їх взаємної роботи у разі вимкнення одного з маршрутизаторів. Вони зможуть отримувати сигнал з іншого маршрутизатора та передавати його на з одного комутатора на інший.

Оскільки два сервери, котрі знаходять в одній підмережі, під’єднані до двох різних комутаторів, вони були об’єднані за допомогою налаштування trunk режиму на портах комутаторів, що з’єднують ці сервери.

# РОЗДІЛ 3 НАЛАШТУВАННЯ БЕЗПЕКИ ТА ВІДДАЛЕНОГО ДОСТУПУ НА АКТИВНЕ ОБЛАДНАННЯ

## 3.1 Налаштування захисту та додаткових функцій маршрутизаторів

На кожному з маршрутизаторів в мережі центрального офісу був налаштований протокол динамічного розподілу адрес (DHCP) для більш надійної роботи мереж у рази спонтанного вимкнення одного з маршрутизаторів, оскільки статична адреса при цьому скидається навіть при збереженій конфігурації.

DHCP (англ. Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла) – це стандартний протокол прикладного рівня, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі. Для цього комп'ютер звертається відповідно – до DHCP-сервера. Мережевий адміністратор може задати діапазон адрес, які будуть розподілені між комп'ютерами. Це дозволяє уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок. Протокол DHCP використовується в більшості великих мереж TCP/IP.

Протокол динамічної конфігурації ЕОМ DHCP служить надання конфігураційних параметрів ЕОМ, підключених до Інтернету. DHCP має дві компонента: протокол надання специфічних для ЕОМ конфігураційних параметрів із боку DHCP-сервера і надання ЕОМ мережевих адрес. Протокол DHCP використовується, крім завантаження бездискових станцій чи Х-терміналів, сервіс-провайдерами для пулів модемів, коли кількість одночасно зайнятих модемів значно коротші їх повного числа. Це дозволяє заощадити помітне число IP-адрес. DHCP побудований за схемою клієнт-сервер, де DHCP-сервер виділяє мережні адреси й доставляє конфігураційні параметри динамічно сконфігурованим ЕОМ. ЕОМ має діяти як DHCP-сервер, якщо вона спеціально несконфігурована системним адміністратором. IP-протокол вимагає встановлення багатьох параметрів. Оскільки IP-протокол можна використовувати найрізноманітнішим мережним устаткуванням, значення цих параметрів неможливо знайти вгадані заздалегідь. З іншого боку, схема розподіленого присвоєння адрес залежить від механізму виявлення вже використовуваних адрес. DHCP підтримує три механізму виділення IP-адрес. При "автоматичному виділенні", DHCP привласнює клієнту постійний IP-адрес. При "динамічному присвоєнні", DHCP привласнює клієнту IP-адрес на обмежений час. При "ручному виділенні", IP-адрес виділяється клієнту мережним адміністратором, а DHCP використовується просто передачі адреси клієнту.

Для кожного маршрутизатора код в CLI Cisco IOS мав наступний вигляд:

Router#conf t

Router(config)#ip dhcp excluded-address 10.3.0.1 10.3.0.10

Router(config)#ip dhcp pool DHCP

Router(dhcp-config)#network 10.3.0.0 255.255.255.224

Router(dhcp-config)#default-router 10.3.0.1

Router(dhcp-config)#ex

Router(config)#ip dhcp pool DHCP

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

Router(dhcp-config)#dns-server 10.3.0.5

Router(dhcp-config)#ex

Router(config)#interface fa0/1/0

Router(config-if)#ip address 10.3.0.1 255.255.255.224

Технологія трансляції мережевих адрес має кілька різновидів, найбільш популярна з яких традиційна технологія трансляції мережевих адрес - Дозволяє вузлам з приватної мережі прозорим для користувачів чином отримувати доступ до вузлів зовнішніх мереж. Підкреслимо, що в даному варіанті NAT вирішується проблема організації тільки тих сеансів зв'язку, які виходять з приватної мережі. Напрямок сеансу в даному випадку визначається положенням ініціатора: якщо обмін даними ініціюється додатком, що працює на вузлі внутрішньої мережі, то сеанс називається вихідним незважаючи на те, що в його рамках в мережу можуть надходити дані ззовні.

Ідея технології NAT полягає в наступному. Нехай мережу підприємства утворює тупиковий домен, вузлів якого присвоєні приватні адреси. На маршрутизаторі, що зв'язує мережу підприємства з зовнішньою мережею, встановлено програмне забезпечення NAT. Це NAT-пристрій динамічно відображає набір приватних адрес на набір глобальних адрес, отриманих підприємством від постачальника послуг і привласнених зовнішнього інтерфейсу маршрутизатора підприємства.

Важливим для роботи NAT-пристрої є правило поширення маршрутних оголошень через кордони приватних мереж. Оголошення протоколів маршрутизації про зовнішні мережах «пропускаються» прикордонними маршрутизаторами у внутрішні мережі і обробляються внутрішніми маршрутизаторами. Протилежне твердження невірно – маршрутизатори зовнішніх мереж не отримують оголошень про внутрішні мережах, оголошення про них фільтруються при передачі на зовнішні інтерфейси. Тому внутрішні маршрутизатори «знають» маршрути до всіх зовнішніх мереж, а зовнішнім маршрутизаторів нічого не відомо про існування приватних мереж.

Традиційна технологія NAT підрозділяється на технології базової трансляції мережевих адрес (Basic Network Address Translation, Basic NAT) і трансляції мережевих адрес і портів (Network Address Port Translation, NAPT). В технології Basic NAT для відображення використовуються тільки IP-адреси, а в технології NAPT - ще й так звані транспортні ідентифікатори, в якості яких найчастіше виступають TCP- і UDP-порти.

На всіх маршрутизаторах та комутаторах був встановлений зашифрований пароль (secret) для уникнення роботи з привілейованим режимом з боку інших працівників офісу окрім мережевого адміністратора.

## 3.2 Налаштування віддаленого доступу до активного обладнання

Secure Shell, SSH (англ. Secure Shell – «безпечна оболонка») – мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером або маршрутизатором і тунелювання TCP-з'єднань (наприклад, для передачі файлів). Схожий за функціональністю з протоколом Telnet і rlogin, проте шифрує весь трафік, в тому числі і паролі, що передаються.

Криптографічний захист протоколу SSH не фіксований, можливий вибір різних алгоритмів шифрування. Клієнти і сервери, що підтримують цей протокол, доступні для різних платформ. Крім того, протокол дозволяє не тільки використовувати безпечний віддалений shell на машині, але і туннелювати графічний інтерфейс – X Tunnelling (тільки для Unix-подібних ОС або застосунків, що використовують графічний інтерфейс X Window System). Так само SSH здатний передавати через безпечний канал (Port Forwarding) будь-який інший мережевий протокол, забезпечуючи (при належній конфігурації) можливість безпечної пересилки не тільки X-інтерфейсу, але і, наприклад, звуку.

На кожному з маршрутизаторів був налаштований описаний вище протокол віддаленого доступу SSH для можливості керування налаштуваннями маршрутизатора через комп’ютер.

## 3.3 Моделювання та тестування роботи розробленої межі

Перевірка роботоспроможності мережі здійснювалась за допомогою передачі пакетів даних з одного комп’ютера або сервера на інший командою ping, що прописувалась в командній консолі кінцевого пристрою «рисунок 3.1».

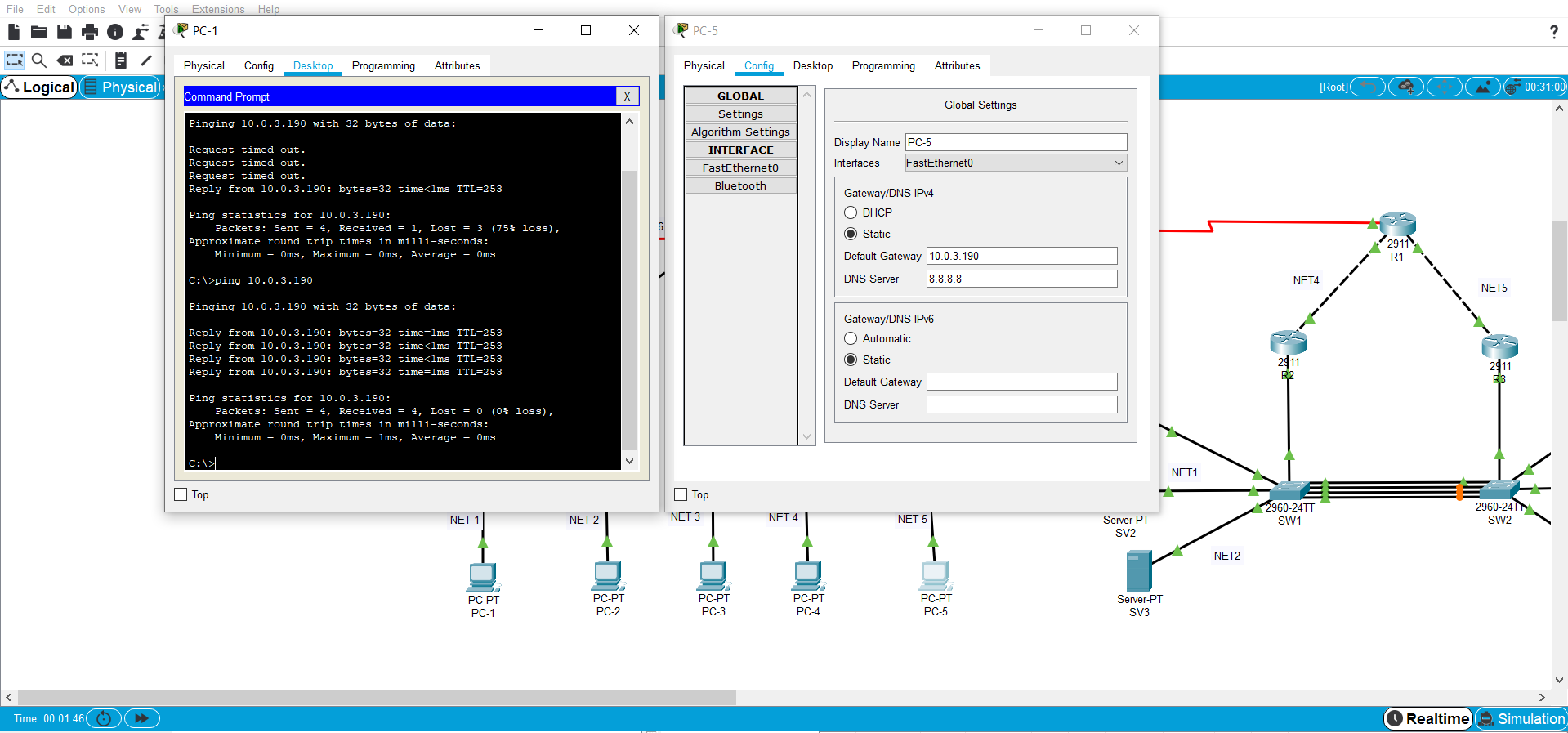


Рисунок 3.1 Тестова відправка пакетів з одного комп’ютера на інший

Мережа дата-центру, де з кінцевих пристроїв були в основному сервери, була поділена на три віртуальні мережі, в яких були використані відповідні то технічного завдання порти обох комутаторів. Основна задумка поділу мережі на віртуальні мережі полягає в тому, щоб пакети даних можна було відправити лише на пристрої в одній такій підмережі. Тобто, якщо сервери з ідентифікаторами 1 і 2 знаходять в одній підмережі, то вони повинні мати змогу відправляти успішний ping запит лише між собою, а на інші сервери – ні. Так як два сервери (3 і 4) знаходяться по різні боки мережі, тобто, з’єднані різними комутаторами, то на самих свічах на відповідних портах був налаштований trunk режим, що дозволяє передавати пакети даних по з’єднанню комутатор-комутатор. Тестові відправки пакетів між серверами «рисунок 3.2»:

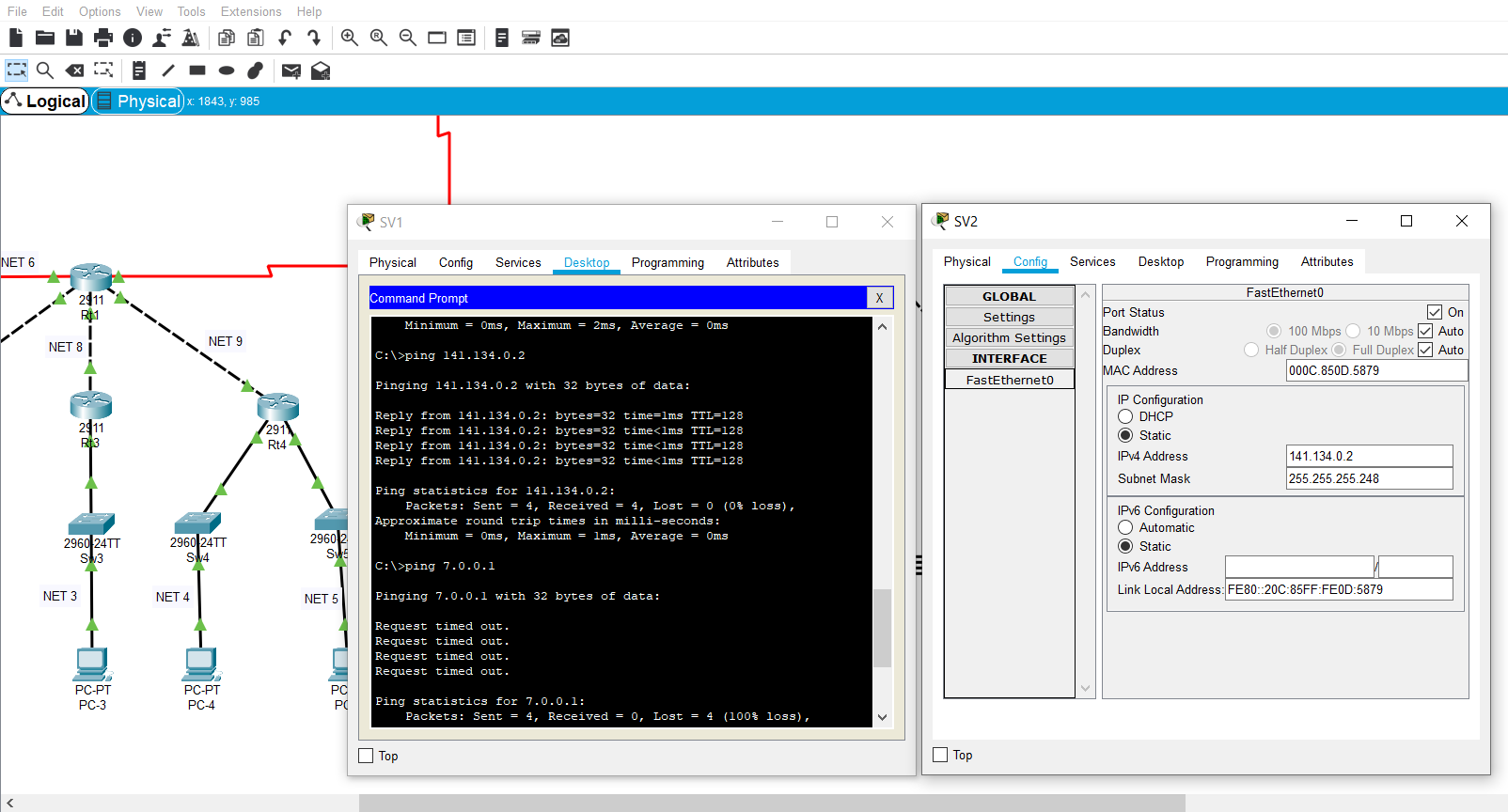


Рисунок 3.2 Відправка запиту ping між серверами однієї віртуальної мережі

На скріншоті видно, що пакет вдалось відправити тільки на сервер, що належить тій самій віртуальній підмережі, що і сервер-відправник, а на сервер з іншої підмережі запит відправити не вдалось.

Також були здійснені тестування віддаленого доступу до маршрутизаторів через комп’ютер за допомогою протоколу SSH «рисунок 3.3».

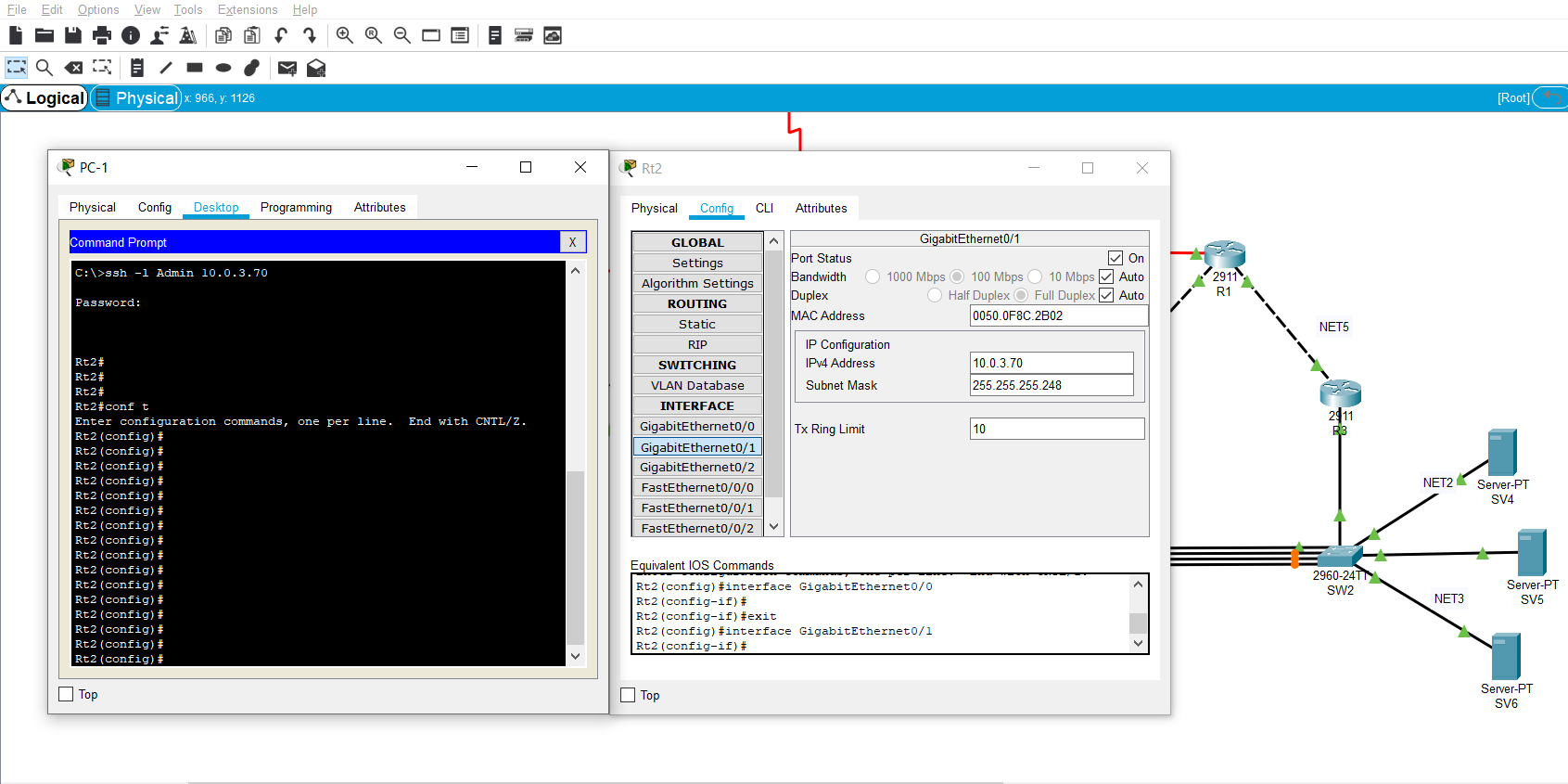


Рисунок 3.3 Тестове підключення до маршрутизатора з комп’ютера

Також тестові запити ping були здійснені в мережі віддаленого офісу «рисунок 3.4». Маршрутизація та призначення адрес було здійснено аналогічно іншим мережам.

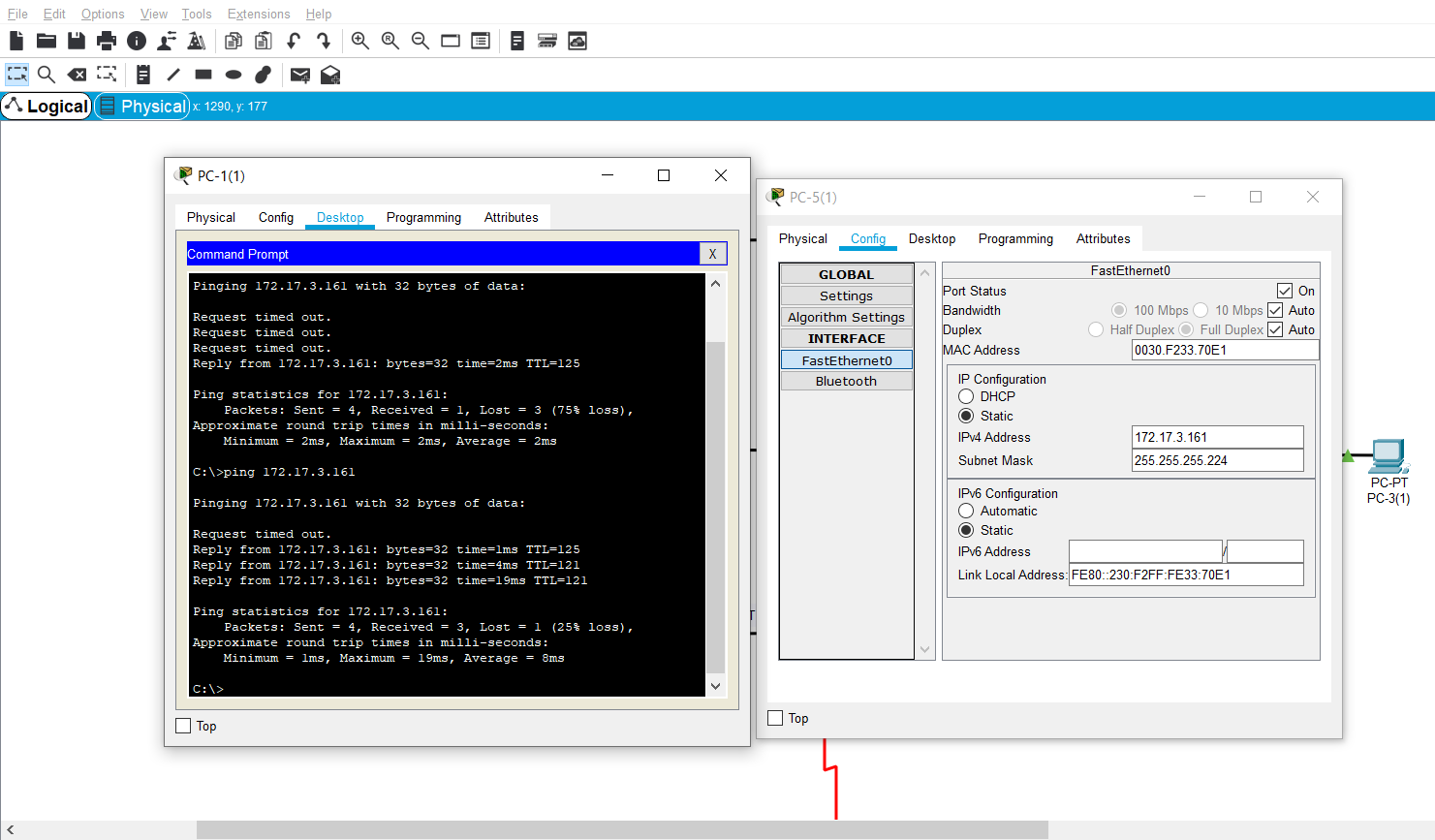


Рисунок 3.4 Тестовий запуск пакета даних в мережі віддаленого офісу

Також серед вимог до роботи була потреба реалізації можливості передачі пакетів даних між трьома мережами. Дана вимога до проектування мережі не була виконана.

# ВИСНОВКИ

В даному курсовому проекті була реалізована симуляція реальної кооперативної мережі в середовищі Cisco Packet Tracer. Були отримані нові навички такі як:

* Проектування мережі максимально наближеної до реальної
* Покращення навичок розподілу ІР-адресації в мережі
* Покращення навичок налаштування маршрутизації

Також були закріплені уже отримані в попередньому та нинішньому курсах навички:

* Конфігурація політики безпеки маршрутизаторів та комутаторів
* Налаштування віддаленого доступу до мережевих пристроїв
* Розрахунок адресного простору
* Проектування віртуальних мереж

В даному курсовому проекті були виконані майже всі вимоги визначені в технічному завданні. Не була виконана лише вимога з передачею пакетів даних між віддаленими мережами.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кульгін М. Комп'ютерні мережі, практика побудови / Максим Кульгін. Санкт-Петербург: СПб, 2003. – 464 с.
2. Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. Комп’ютерні мережі : навчальний посібник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.] Вінниця : ВНТУ, 2013. – 371 с.
3. Оліфер В. Г. Комп'ютерні мережі. Принципи, технологї, протоколи. Підручник для вузів / В. Г. Оліфер, Н. А. Оліфер. Санкт-Петербург: СПб, 2007. – 960 с
4. Біляєв А. В. Методи та засоби захисту інформації [Електронний ресурс] / А. В. Біляєв. 2000. – Режим доступу до ресурсу: http:// www.citforum.ru/internet/infsecure/its2000\_01.shtml.
5. Колбін Р. В. Глобальні та локальні мережі: створення, налаштування та використання / Р. В. Колбін. М.: Біном. Лабораторія знань, 2008. – 55 с.
6. Платонов В. В. Програмно-апаратні засоби забезпечення інформаційної безпеки обчислювальних мереж / В. В. Платонов. М.: Академія, 2006. – 240 с.
7. Алгоритми: побудова та створення / Т.Корман, Ч. Лейзерсон, Р. Рівест, К. Штайн. М.: Видавничий дім "Вільямс", 2007. – 1296 с. – (2).
8. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп’ютерні мережі [навчальний посібник] – Львів, «Магнолія 2006», 2013. – 256 с.

# ДОДАТОК А

**ІЛЮСТРАЦІЇ СКОНФІГУРОВАНОЇ МЕРЕЖІ**

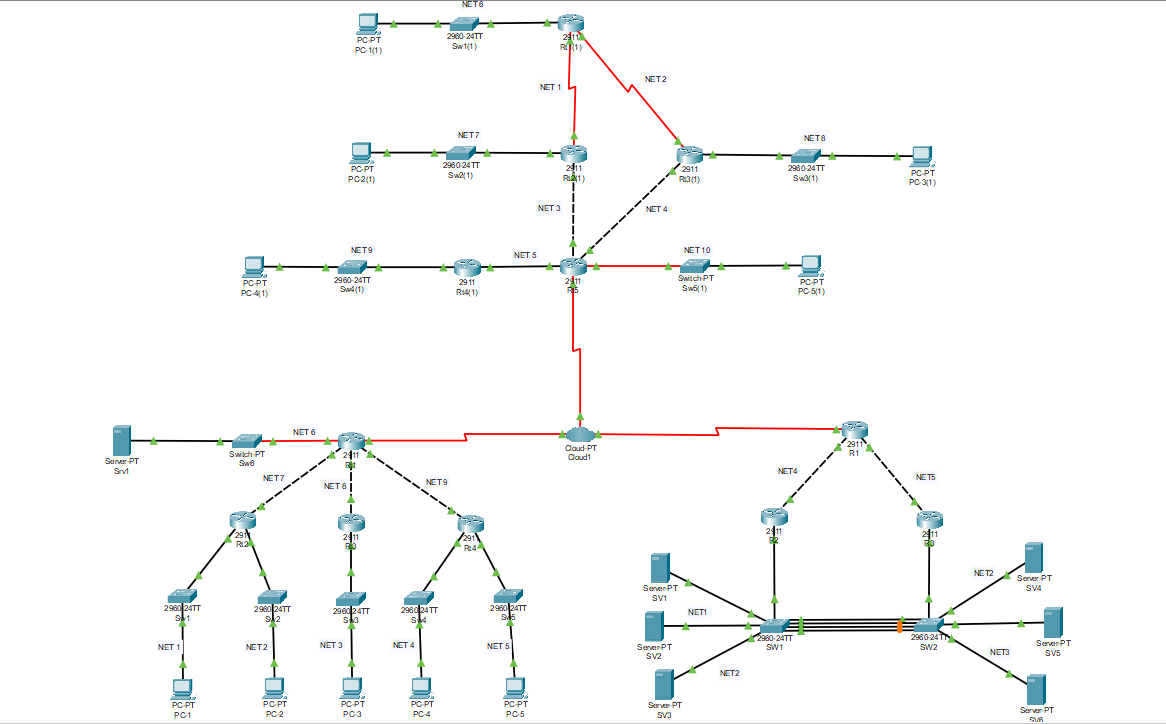


Рисунок А.1 Загальний вигляд розробленої топології мережі

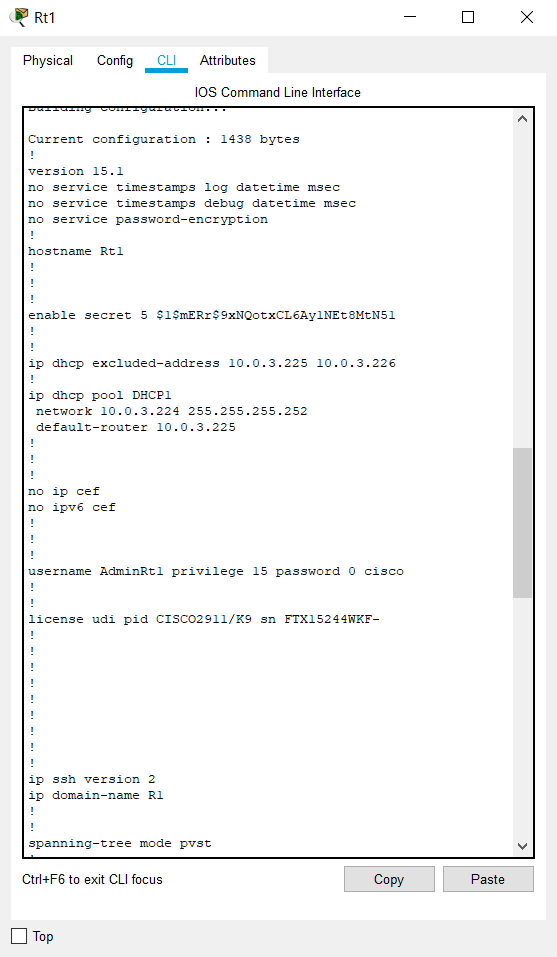


Рисунок А.2 Конфігурація шлюзового маршрутизатора на прикладі Rt1 у мережі центрального офісу

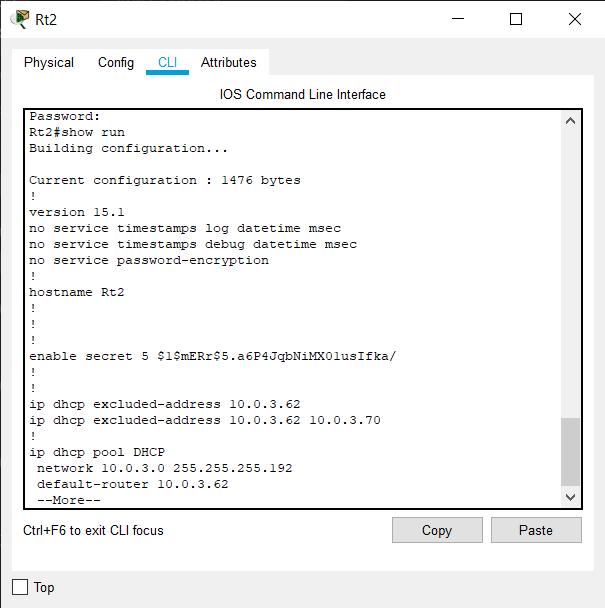


Рисунок А.3 Конфігурація базового маршрутизатора

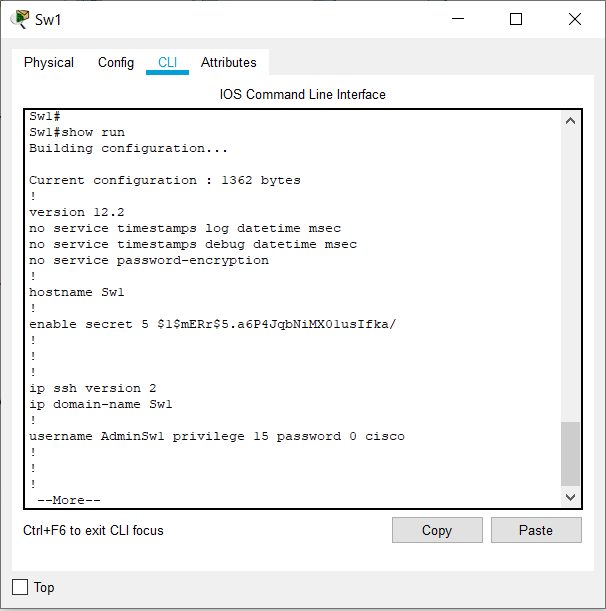


Рисунок А.4 Конфігурація комутатора на прикладі комутатора з мережі центрального офісу

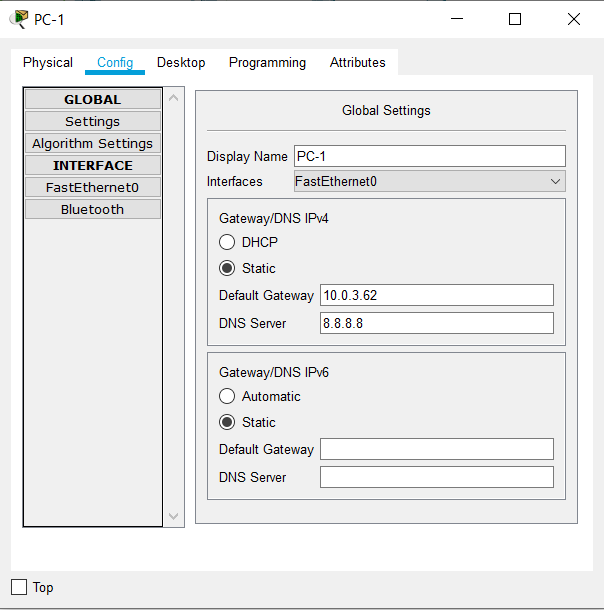


Рисунок А.5 Конфігурація робочого комп’ютера на прикладі комп’ютера в мережі центрального офісу

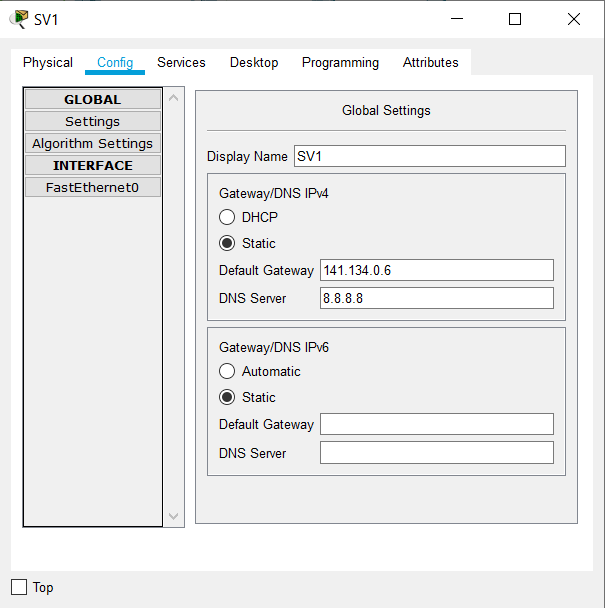


Рисунок А.6 Конфігурація сервера на прикладі сервера з мережі дата-центру

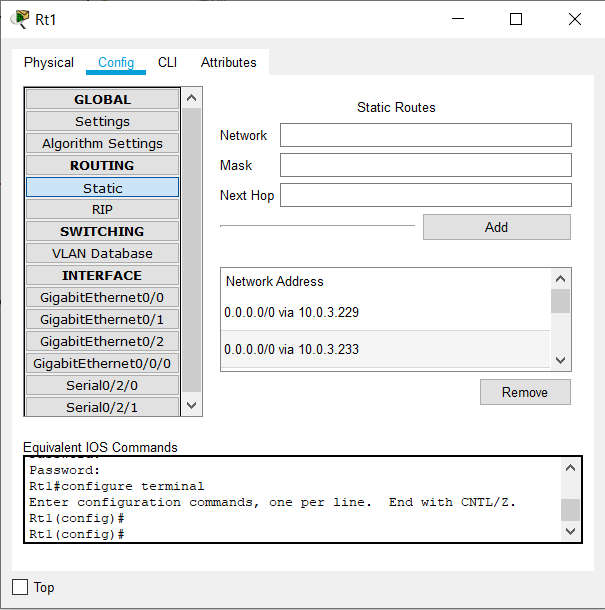


Рисунок А.7 Конфігурація маршрутизації на маршрутизаторі на прикладі маршрутизатора з мережі центрального офісу