**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)»**

на тему:  **Розробка комп’ютерної мережі та конфігурування мережевого обладнання**

Студента 3 курсу \_\_\_\_\_ групи спеціальності «Кібербезпека»

(прізвище та ініціали)

Керівник:

(посада, вчене звання, науковий ступінь,

прізвище та ініціали)

Національна шкала \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Кількість балів: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

Члени комісії

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

(підпис) (прізвище та ініціали)

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

(підпис) (прізвище та ініціали)

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

(підпис) (прізвище та ініціали)

м. Київ – 2020 рік

ЗМІСТ

[ЗМІСТ 1](#_Toc58321320)

[АНОТАЦІЯ 3](#_Toc58321321)

[АННОТАЦИЯ 3](#_Toc58321322)

[ANNOTATION 4](#_Toc58321323)

[ВСТУП 6](#_Toc58321324)

[ТЕХНІЧНЕ ЗАВДАННЯ 8](#_Toc58321325)

[РОЗДІЛ 1 ОСНОВНА ТЕОРЕТИЧНА ЧАСТИНА СТВОРЕННЯ КОМП’ЮТЕРНОЇ МЕРЕЖІ 13](#_Toc58321326)

[1.2 Розрахунок адресного простору 14](#_Toc58321327)

[1.3 Вибір та налаштування способу маршрутизації 15](#_Toc58321328)

[1.4 Конфігурування базових функцій маршрутизаторів 16](#_Toc58321329)

[1.5 Проектування віртуальних мереж 18](#_Toc58321330)

[1.6 Конфігурування базових функцій комутаторів LAN 20](#_Toc58321331)

[1.7 Конфігурування додаткових функцій маршрутизаторів (DHCP, NAT тощо) 21](#_Toc58321332)

[1.8 Налаштування захисту та конфігурування функцій безпеки (налаштування паролів, Port Security, ACL тощо) 23](#_Toc58321333)

[1.9 Налаштування віддаленого доступу до активного обладнання 26](#_Toc58321334)

[РОЗДІЛ 2 ПРАКТИЧНА ЧАСТИНА СТВОРЕННЯ КОМП’ЮТЕРНОЇ МЕРЕЖІ 28](#_Toc58321335)

[2.1 Проектування мережі центрального офісу (LAN1) 28](#_Toc58321336)

[2.2 Проектування мережі віддаленого офісу (LAN2) 34](#_Toc58321337)

[2.3 Проектування мережі датацентру (LAN3) 40](#_Toc58321338)

[2.4 Об’єднання LAN1-LAN3 та тестування роботи розробленої мережі 43](#_Toc58321339)

[ВИСНОВКИ 46](#_Toc58321340)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 48](#_Toc58321341)

АНОТАЦІЯ

Курсова робота складається з пояснювальної записки обсягом 49 сторінок, 1 таблиці, 21 рисунок.

Також курсова робота містить вступ, два розділи, висновки та список використаних джерел.

У вступі обґрунтована актуальність та практична цінність обраної теми роботи, поставлена мета і завдання розробки мережі.

У першому розділі висвітлена основна теоретична частина створення мережі. Зазначені команди, методи та інструментарій, який буде застосовано у другому розділі при проектуванні мереж.

У другому розділі роботи описана основна практична частина створення кожної з трьох LAN-мереж та об’єднання їх в одну WAN-мережу. Завершується другий розділ тестуванням створеної мережі та наведенням результатів перевірки її працездатності.

У висновках підводиться підсумок проведеної роботи.

У списку використаних джерел подаються джерела, на основі яких проведена робота.

АННОТАЦИЯ

Курсовая работа состоит из пояснительной записки объемом 49 страниц, 1 таблицы, 21 рисунок.

Также курсовая работа содержит введение, две главы, выводы и список использованных источников.

Во введении обоснована актуальность и практическая ценность темы работы, поставлена цель и задачи разработки сети.

В первой главе освещена основная теоретическая часть создания сети. Указаны команды, методы и инструментарий, который будет применен во второй главе при проектировании сетей.

Во втором разделе работы описана основная практическая часть создания каждой из трех LAN-сетей и объединение их в одну WAN-сеть. Завершается второй раздел тестированием созданной сети и указанием результатов проверки ее работоспособности.

В выводах подводится итог проведенной работы.

В списке использованных источников подаются источники, но основе которых проведена работа.

ANNOTATION

Course work consist of an explanatory note of 49 pages, 1 table, 21 figures.

Also, the course work contains an introduction, two chapters, conclusions and a list of sources used.

The introduction substantiates the relevance and practical value of the topic of work, sets the goal and objectives of the network development.

The first chapter covers the main theoretical part of networking. The commands, methods and tools that will be applied in the second chapter when designing networks are indicated.

The second section of the work describes the main practical part of creating each of the three LAN-networks and combining them into one WAN-network. The second section ends with testing the created network and indicating the results of testing its performance.

The conclusions summarize the work done.

In the list of sources used, sources are given, but on the basis of which the work was carried out.

ВСТУП

**Актуальність.** Комп’ютерні мережі необхідні сьогодні в кожній сфері діяльності людини. Виробничі, торговельні, фінансові, адміністративні установи та інші підприємства для своєї діяльності використовують надійну та ефективну комп’ютерну систему.

Кожен, хто хоча б трохи має уявлення про те, як влаштована мережа, розуміє, на скільки це складна багаторівнева система. Системні адміністратори налаштовують мережу, забезпечують її працездатність, поточний контроль, виправлення помилок, удосконалення, розширення і багато іншого.

**Значення роботи.** Розглянувши за допомогою спеціального інструментарію роботу мережі зсередини, можна пересвідчитись у багатогранності процесів, що забезпечують її коректну роботу.

Відповідно, проектування, впровадження та підтримка комп’ютерних мереж потребує спеціальних знань та практичної підготовки. Часто під час роботи виникають питання, відповіді на які можна знайти лише проконсультувавшись з іншими спеціалістами або на підставі власного досвіду.

**Сучасний рівень.** Постійно випускаються нові мережеві пристрої, ускладнюється існуюче обладнання, розширюються можливості протоколів, характеристики мережі зростають. Адміністратори повинні бути в курсі останніх подій та слідкувати за оновленнями.

**Мета курсової роботи** – отримання практичних навичок проектування та конфігурування комп’ютерних мереж.

Для досягнення мети ставимо наступні **задачі**:

- розробити комп’ютерну систему;

- розрахувати адресний простір для мереж LAN1-LAN3;

- створити конфігураційні фали для всіх мережевих пристроїв;

- виконати моделювання мережі засобами Cisco Packet Tracer.

У курсовій роботі використовується створення трьох різних LAN, які передбачають спільне користування ресурсами.

Під час проектування мережі ми навчимося розділяти адресний простір, налаштовувати DHCP-сервер для видачі IP-адрес хостам, проектувати Vlan. Маршрутизація буде використовуватися як статична, так і динамічна, за допомогою протоколу OSPF.

Розглянемо трансляцію NAT, віддалений доступ до обладнання та, загалом, конфігурування комутаторів і маршрутизаторів.

**Призначення курсової роботи.** Практичне створення мережі за допомогою програми Cisco Packet Tracer дає можливість розглянути внутрішню складову мереж, спробувати набори різних команд і побачити, як вони впроваджуються, як діють протоколи.

ТЕХНІЧНЕ ЗАВДАННЯ

На розробку і конфігурування комп’ютерної мережі

1. Область застосування — комп’ютерні мережі.
2. Основа розробки — робочий навчальний план дисципліни.
3. Мета та експлуатаційне призначення:
   1. мета - отримання практичних навичок проектування та конфігурування комп’ютерних мереж;
   2. призначення розробки — навчальна курсова робота із дисципліни «Комп’ютерні системи та мережі (Рівень D - Безпека комп’ютерних систем)»;
4. Джерела розробки — індивідуальне завдання на курсовий проект із дисципліни, технічні рекомендації щодо проектування локальних та розподілених мереж та інші технічні матеріали для налаштування окремих компонентів мережі.
5. Технічні вимоги
   1. Мережа складається з трьох окремих LAN, що об’єднуються WAN мережею, побудованою на основі технології віртуальних каналів.
   2. Вимоги для проектування LAN1
      1. Адреса мережі 172.16.2.0
      2. Складається з п’яти сегментів, кількість робочих станцій в кожному з яких становить: 120, 25, 4, 10, 12.
      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 NET3, NET5 та NET4 відповідно до мереж NET6 NET3 та NET2. Розширені ACL мають заборонити проходження трафіку протоколів IMAP, NETBIOS та TFTP з NET1 до NET4 та POP3, SFTP та SNMP з NET3 до NET5. ACL необхідно розмістити в найбільш вдалому місці.
      7. У середині мережі використовується статична маршрутизація.
      8. На маршрутизаторах Rt2-Rt4 налаштувати DHCP-сервіс і забезпечити динамічне призначення адрес хостам в мережах Net1-Net5.
      9. На маршрутизаторі Rt1 налаштовано сервіс трансляції адрес NAT.
   3. Вимоги для проектування LAN2
      1. Адреса мережі 192.168.2.0/24
      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-Rt2 та Rt1-Rt3 здійснюється за допомогою послідовних інтерфейсів. Інші з’єднання виконуються за допомогою скрученої пари.
      5. Під’єднання мережі LAN2 до мережі WAN виконується через маршрутизатор Rt2.
      6. В середині мережі використовується динамічна маршрутизація на основі протоколу OSPF.
      7. На маршрутизаторі Rt2 налаштовано сервіс трансляції адрес NAT.
   4. Вимоги для проектування LAN3
      1. Реалізована на основі комутаторів Catalyst 2960 з підтримкою технології віртуальних мереж.
      2. Поділена на три віртуальні сегменти, кожний з яких містить по два сервери.
      3. На комутаторах Sw1 Sw2 до Vlan 1 належать порти FastEthernet2-FastEthernet7 та FastEthernet12-FastEthernet14 відповідно, до Vlan 2 належать порти FastEthernet9-FastEthernet13 та FastEthernet3-FastEthernet6 відповідно, до Vlan 3 FastEthernet14-FastEthernet18 та FastEthernet16-FastEthernet20 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 200.15.5.0, 203.111.18.0 та 193.20.0.0 відповідно.
   5. Вимоги для проектування WAN
      1. Об’єднання локальних мереж здійснюється за допомогою Frame Relay комутатора з використанням топології Full Mesh.
      2. Адреси інтерфейсів маршрутизаторів, що під’єднані до Frame Relay мережі, належать до мережі з адресою 11.1.0.0/16
      3. З’єднання між локальними мережами здійснюється за допомогою послідовних інтерфейсів.
   6. Загальні вимоги до налаштувань маршрутизаторів
      1. Встановити на всіх маршрутизаторах паролі на консольне з’єднання та на привілейований режим.
      2. Налаштувати доступ через протокол SSH до шлюзових маршрутизаторів.
6. Апаратні вимоги - використання обладнання фірми Cisco
7. Текстова документація розробленої мережі повинна відповідати діючим стандартам України.
8. Стадії та етапи розробки мережі включать розробку та відлагодження окремих LAN та об’єднання LAN1-3 за допомогою WAN мережі.

Розробив студент групи \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ДВНЗ «УНІВЕРСИТЕТ БАНКІВСЬКОЇ СПРАВИ»**

**ІНСТИТУТ БАНКІВСЬКИХ ТЕХНОЛОГІЙ ТА БІЗНЕСУ**

**КАФЕДРА КІБЕРБЕЗПЕКИ ТА СОЦІАЛЬНИХ НАУК**

Спеціальність: Кібербезпека

Курс 3 Група 303 - КБ Семестр 1

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

**ЗАВДАННЯ**

**на курсову роботу студента**

(прiзвище, iм`я, по батьковi)

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

### 2. Термiн здачi студентом закiнченої роботи

**3. Постановка задачі.**

1. Розробити комп’ютерну мережу
2. Розрахувати адресний простір для мереж LAN1-LAN3
3. Створити конфігураційні файли для всіх мережевих пристроїв.
4. Виконати моделювання мережі засобами Cisco Packet Tracer.

Вихідні дані:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| LAN  №1 | підмережі | IP-адреса | | Кількість хостів | | | | | | | | | | |
| Net1 | Net2 | | | Net3 | | | Net4 | | Net5 | |
| 172.16.2.0 | | 120 | 25 | | | 4 | | | 10 | | 12 | |
| ст. ACL | відпр. | | отр. | відпр. | | | отр. | | | відпр. | | отр. | |
| Net 3 | | Net 6 | Net 5 | | | Net 3 | | | Net 4 | | Net 2 | |
| розш. ACL | відпр. | | отр. | № прот. | | | відпр. | | | отр. | | № прот. | |
| Net 1 | | Net 4 | 6, 7, 15 | | | Net 3 | | | Net 5 | | 9,10,12 | |
| LAN  №2 | № сх. |  | IP-адреса | | Serial | | Serial | | | Шлюз | | Тип маршрутизації | | |
| 2 |  | 192.168.2.0/24 | | Rt1-Rt2 | | Rt1-Rt3 | | | Rt2 | | OSPF | | |
| LAN  №3 | Net1 | Net2 | | Net3 | Switch1 | | | | | | Switch3 | | | |
| Vlan 1 | Vlan 2 | | | Vlan 3 | | Vlan 1 | Vlan 2 | | Vlan 3 |
| 200.15.5.0 | 203.111.18.0 | | 193.20.0.0 | 2-7 | 9-13 | | | 14-18 | | 12-14 | 3-6 | | 16-20 |

6. Дата видачі завдання “ ” 20\_\_\_\_ р

КАЛЕНДАРНИЙ ПЛАН

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Назва етапiв курсової роботи | Термiн виконання етапiв курсової роботи | Примiтки |
| 1 | Отримання завдання | 19 вересня |  |
| 2 | Аналіз технічної задачі | 26 вересня |  |
| 3 | Розробка структурної схеми | 03 жовтня |  |
| 4 | Встановлення Ip-аgрес мережевих інтерфейсів | 10 жовтня |  |
| 5 | Налагодження серверів | 17 жовтня |  |
| 6 | Планування дозволу імен | 31 жовтня |  |
| 7 | З’єднання частин мережі за допомогою маршрутизаторів | 14 листопад |  |
| 8 | Моделювання потоків трафіку в мережі | 21 листопад |  |
| 9 | Розрахунок PDV | 28 листопад |  |
| 10 | Оформлення пояснювальної записки | 12 грудень |  |
| 11 | Захист курсової роботи | 19 грудень |  |

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (пiдпис)

Керiвник \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (пiдпис)

РОЗДІЛ 1 ОСНОВНА ТЕОРЕТИЧНА ЧАСТИНА СТВОРЕННЯ КОМП’ЮТЕРНОЇ МЕРЕЖІ

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

Кожна сучасна мережа, як локальна, так і глобальна, має ряд складових: хости, периферійні пристрої, мережеві пристрої, мережеве середовище передачі даних.

Хости безпосередньо відправляють і приймають повідомлення в мережі, мають IP-адресу і забезпечують загальний доступ до периферійних пристроїв з мережі.

Мережеві пристрої, як і мережеве середовище передачі даних, з’єднують хости між собою. Іноді такі пристрої називають проміжними, оскільки вони розташовані на шляху повідомлень між вихідним і кінцевим хостами.

В даній роботі у якості проміжних пристроїв представлені комутатори і маршрутизатори.

Мережеве середовище передачі даних – кабелі та проводи, які використовуються в провідних мережах, а також радіохвилі, які використовуються в бездротових мережах. Вони забезпечують шляхи, по яких повідомлення передаються між різними мережевими компонентами.

Для проектування комп’ютерної мережі у курсовій роботі використані послідовні з’єднання між пристроями за допомогою кабелю Serial та скрученої пари Fast Ethernet і Gigabit Ethernet.

Управління IP-трафіком засноване на характеристиках і пристроях, пов’язаних з кожним з трьох рівнів ієрархічної моделі проектування мереж: доступу, розподілу і ядра.

Рівень доступу сполучає облаштування кінцевих користувачів з мережею і дозволяє декільком хостам підключатися до інших хостів через мережевий пристрій, комутатор. Так і в нашій спроектованій мережі, комутатори забезпечуватимуть зв’язок з облаштуваннями рівня розподілу - маршрутизаторами.

Рівень розподілу сполучає різні мережі і контролює потоки інформації між ними. Пристрої рівня розподілу контролюють тип і об’єм трафіку, що передається з рівня доступу на рівень ядра. В нашій мережі використовуються маршрутизатори.

Рівень ядра – високошвидкісний магістральний рівень, основне завдання якого – швидка передача даних. В нашій мережі рівень ядра відображений WAN мережею, яка об’єднує три мережі LAN: центральний офіс, віддалений офіс, а також датацентр.

1.2 Розрахунок адресного простору

Для розрахунку адресного простору необхідні три елементи конфігурації IP:

- IP-адреса ідентифікує хост в мережі;

- маска підмережі ідентифікує мережу, до якої підключений хост;

- основний шлюз ідентифікує мережевий пристрій, через який хост підключається до Інтернету або іншої віддаленої мережі [1].

У курсовій роботі для проектування мережі використовується VLSM – мережі з плаваючою маскою.

Коли нам необхідно розрахувати адресний простір в нашій мережі, ми орієнтуємось на кількість пристроїв (хостів), які необхідно або планується підключити в дану мережу.

Знаходимо маски підмережі для кожної мережі, вираховуємо межі кожної мережі.

Розраховуємо діапазон адрес мережі (її межі).

Спочатку розраховуємо або визначаємо адресу мережі. Після цього за допомогою формули визначаємо кількість адрес:

, (1.1)

де – кількість нулів у масці підмережі у мережі (в двійковому вигляді).

Після цього, до IP-адреси додаємо число, яке вийшло у попередьому розрахунку.

Остання адреса мережі буде широкомовною адресою.

Діапазон адрес мережі вираховуємо від першої адреси мережі до широкомовної адреси.

Формула кількості пристроїв в мережі:

– 2, (1.2)

де - кількість нулів у масці підмережі у мережі (в двійковому вигляді).

1.3 Вибір та налаштування способу маршрутизації

Маршрутизація – процес знаходження шляху для повідомлення.

Маршрутизатори працюють на підставі IP-адрес і створюють таблицю маршрутизації, яка заповнюється за допомогою протоколу ARP (Adress Resolution Protokol) – протоколу зіставлення адрес.

Маршрутизація необхідна для визначення найкращого шляху до вузла призначення. Маршрутизатор – мережевий пристрій, що зв’язує декілька IP-мереж рівня 3 (мережевого рівня).

У кожного маршрутизатора є таблиця локально підключених мереж і їх інтерфейсів, кожен порт (інтерфейс) маршрутизатора пов’язаний зі своєю локальною мережею. Процес переправлення пакетів в середу призначення і є маршрутизацією. Маршрутизатори переміщають дані між локальною і віддаленою мережею. Інформація зберігається в таблицях маршрутизації. Записи або динамічно оновлюються на підставі інформації, отриманої від інших маршрутизаторів в мережі, або вручну вводяться мережевим адміністратором.

Якщо маршрутизатор не може визначити адресата повідомлення, воно скидається. Щоб запобігти скидання, мережеві адміністратори вводять в таблицю маршрут по замовчуванню, який є інтерфейсом, через який маршрутизатор передає пакет з невідомою IP-адресою мережі призначення.

Про віддалені мережі маршрутизатор повідомляється одним з двох способів:

- вручну – віддалені мережі вносяться в таблицю маршрутизації за допомогою статичних маршрутів;

- динамічно – віддалені маршрути долаються за допомогою протокола динамічної маршрутизації.

Статичні маршрути не оновлюються автоматично та при змінах у топології їх необхідно повторно налаштовувати вручну.

У більшості мереж використовується комбінація протоколів динамічної маршрутизації та статичних маршрутів. Це призводить до того, що для маршрутизатора задається декілька шляхів до мережі призначення, отриманих за допомогою статичних і динамічно отриманих маршрутів.

Для створення таблиці маршрутизації вибираємо і вказуємо мережу, з якою хочемо з’єднатися і до якої необхідно прокласти маршрут, основний шлюз (порт), через який ми будемо зв’язуватися з даною мережею.

Метрика кожного протоколу динамічної маршрутизації відіграє важливу роль. Метрика протоколу динамічної маршрутизації RIP заснована на кількості переходів (де менше протоколів, той шлях і обирає маршрутизатор).

Протоколи динамічної маршрутизації IGRP і EIGRP використовують складову метрику залежно від пропускної здатності, затримки, надійності, завантаження і максимального розміру переданого блоку даних (MTU), де пропускна здатність і затримка є єдиними параметрами, використовуваними за замовчуванням. І у процесі перерозподілу маршрутів необхідно визначити метрику, зрозумілу приймаючому протоколу.

За нашим завданням, для створення таблиці маршрутизації в мережі віддаленого офісу LAN2, що проектується, буде використано протокол динамічної маршрутизації OSPF, що буде детально розглянуто у пункті 2.2 Розділу 2 курсової роботи.

1.4 Конфігурування базових функцій маршрутизаторів

У даній курсовій роботі налаштування пристроїв будемо проводити через консольне підключення, під’єднуючи консольний кабель в роз’єм RS232 на комп’ютері, з якого проводитимуться налаштування, до роз’єму Console на пристрої, який буде налаштовуватися.

На рисунку 1.4 зображено консольне з’єднання комп’ютера РС1 та маршрутизатора Rt2 в мережі центрального офісу LAN1.

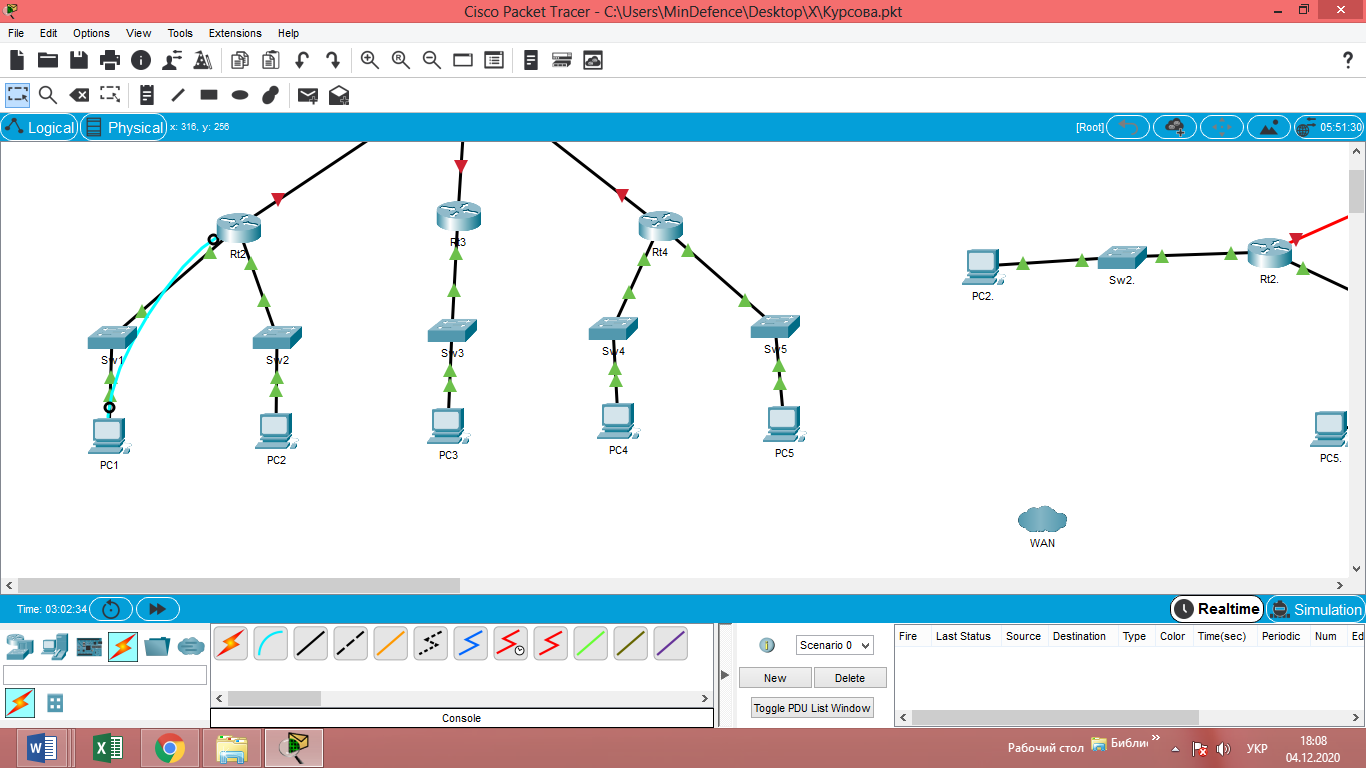


Рис. 1.1 Консольне з’єднання пристроїв для первинного налаштування

Усі базові налаштування маршрутизатора проводяться з режиму глобальної конфігурації у терміналі.

Для потрапляння в режим налаштувань вводимо:

enable – потрапляємо в привілейований режим, потім – configure terminal і потрапляємо в режим глобальної конфігурації.

Одне з перших базових налаштувань, яке необхідно провести і без якого не можливо буде зберегти ряд інших налаштувань - встановлення імені пристрою командою hostname «ім’я». Після цього ім’я пристрою перед ідентифікатором режиму зміниться на нове.

Також у базових конфігураціях маршрутизатора налаштовуємо інтерфейси командою interface «назва інтерфейсу».

Команда description використовується для визначення призначення інтерфейсу.

Далі присвоюємо IP-адресу кожному інтерфейсу командою ip address адреса маска підмережі.

Командою no shutdown вмикаємо інтерфейс, щоб він став активним.

Прописуємо маршрути для маршрутизаторів командою ip route адреса мережі призначення, маска підмережі мережі призначення, основний шлюз, через який здійснюватиметься зв’язок з віддаленою мережею.

Всі введені налаштування зберігаються командою copy running-config startup-config або write memory.

Ці та інші команди буде детально розглянуто та показано на прикладах при проектуванні окремих мереж у Розділі 2 курсової роботи.

1.5 Проектування віртуальних мереж

VLAN – Virtual Local Area Network – віртуальна локальна комп’ютерна мережа.

Мережі Vlan дозволяють згрупувати пристрої всередині локальної мережі так, ніби вони підключені за допомогою одного кабеля.

Мережі Vlan дозволяють адміністратору виробляти сегментацію за функціями, проектними групами або областями застосування. Кожна Vlan вважається окремою логічною мережею.

Vlan створює логічний широкомовний домен, який може охоплювати кілька фізичних сегментів LAN. Таким чином підвищується продуктивність мережі.

Переваги віртуальних локальних мереж:

- безпека – групи, що володіють уразливими даними, відокремлені від решти мережі, завдяки чому знижується ймовірність витоку конфіденційної інформації;

- зниження витрат – більш ефективне використання наявної смуги пропускання, без дорогих оновлень інфраструктури;

- підвищення продуктивності – поділ зменшує кількість зайвого мережевого трафіку і підвищує продуктивність;

- зменшення розміру доменів широкомовної розсилки – поділ мережі на мережі Vlan зменшує кількість пристроїв в домені широкомовної розсилки;

- підвищення продуктивності ІТ-відділу – мережі Vlan спрощують управління мережею, оскільки користувачі з аналогічними вимогами до мережі використовують одну і ту ж мережу Vlan;

- спрощене управління проектами та програмами – об’єднання пристроїв за вимогами.

Керуюча Vlan – будь-яка мережа Vlan, налаштована для доступу до функцій управління комутатора. Мережа Vlan 1 за замовчуванням є керуючою Vlan. Для створення керуючої Vlan віртуальному інтерфейсу комутатора (SVI) даної Vlan призначається IP-адреса і маска підмережі, завдяки чому комутатором можна управляти за протоколами HTTP, Telnet, SSH або SNMP.

Транк – канал типу «точка-точка» між двома мережевими пристроями, який підтримує більше однієї мережі Vlan. Транк віртуальної мережі є «кабельним каналом» передачі багатьох Vlan між комутаторами і маршрутизаторами, між мережевим пристроєм і сервером або іншим пристроєм, оснащеним відповідним мережевим адаптером з підтримкою стандарту 802.1Q.

Порядок налаштування Vlan на комутаторі, який ми будемо використовувати та показувати на прикладах при проектуванні мережі датацентру LAN3 -

з режиму глобальної конфігурації вводимо команду vlan «цифра мережі Vlan».

Присвоюємо назву мережі Vlan name «ім’я».

Призначаємо режим роботи порту комутатора access: interface порт > switchport mode access > switchport access vlan «номер» - призначаємо порт до Vlan.

Призначаємо режим роботи порту комутатора trunk: interface порт > switch port mode trunk > switch port trunk allowed vlan «номер».

Щоб налаштувати одразу діапазон портів, використовуємо команду interface range.

Міжвланова маршрутизація – створення підінтерфейсу (віртуального порта), сабінтерфейсу на маршрутизаторі interface число – число Vlan, для якої створюємо порт.

Далі вказуємо інкапсуляцію, або призначаємо сабінтерфейс до Vlan encapsulation dot1q …. (цифра Vlan).

Створюємо IP-адресу на сабінтерфейсі ip address адреса маска підмережі.

Повертаємось в режим налаштування фізичного порту маршрутизатора: interface «назва» і вмикаємо його командою no shutdown.

Такий комплекс команд вводимо для кожного Vlan, підключеного до порта маршрутизатора.

1.6 Конфігурування базових функцій комутаторів LAN

Комутатори Ethernet використовуються на рівні доступу. Хост відправляє повідомлення, а комутатор приймає і декодує кадри за MAC-адресою повідомлення.

Комутатори локальної мережі забезпечують зв’язок всередині локальної мережі.

Комутатори Ethernet Cisco Catalyst серії 2960 підходять для мереж малого і середнього розміру. Підтримують підключення 10/100 Fast Ethernet і 10/100/1000 Gigabit Ethernet. Тому саме цей комутатор використаємо при проектуванні нашої мережі LAN.

Необхідно налаштувати базові параметри безпеки перед підключенням комутатора до мережі.

Всі налаштування проходять в режимі глобальної конфігурації, з якого можна перейти в різні режими підконфігурації:

- режим лінійної конфігурації;

- режим інтерфейсного налаштування.

За умовчанням, кожен діалог починається з імені пристрою і знаку, який показує, в якому режимі знаходимося в даний час.

Для потрапляння в режим налаштувань вводимо:

enable – потрапляємо в привілейований режим, потім – configure terminal і потрапляємо в режим глобальної конфігурації.

Всі введені налаштування зберігаються командою copy running-config startup-config або write memory.

Більше налаштувань буде показано у Розділі 2 курсової роботи.

1.7 Конфігурування додаткових функцій маршрутизаторів (DHCP, NAT тощо)

При налаштуванні отримання хостом динамічної IP-адреси, пристрій запитує адресу з діапазону адрес, який призначається DHCP-сервером, розташованим в мережі. У нашій мережі DHCP-сервером будуть виступати маршрутизатори, які роздаватимуть IP-адреси хостам.

Для автоматичного призначення адрес IPv4 використовується протокол Dynamic Host Configuration Protocol – DHCP. DHCP передбачає механізм автоматичного призначення адреси IPv4, маски підмережі, основного шлюзу і інших параметрів конфігурації. Команда ipconfig / all дозволяє переглянути інформацію, яку клієнт отримав від DHCP-сервера.

DHCP – найбільш прийнятний спосіб призначення IPv4-адрес хостам у великій мережі, оскільки він полегшує роботу служби підтримки і практично усуває можливість помилки. На DHCP-сервері налаштовується діапазон (пул) адрес IPv4, які можна призначити DHCP-клієнтам.

Задати DHCP-сервер на маршрутизаторі можна командою ip dhcp excluded-address адреса, де зазначаємо, що ми хочемо видавати адреси після такої адреси або в діапазоні.

Командою ip dhcp pool «назва» називаємо наш DHCP-сервер.

Network адреса маска підмережі - означає, що сервер повинен видавати адреси з такої мережі і з такою маскою.

Командою default-router адреса вказуємо нашу адресу, яка буде видаватися пристроям мережі як основний шлюз.

Перетворення мережевих адрес – NAT (Network Address Translation), використовується для перетворення приватної IPv4-адреси в публічну IP-адресу. Виконується на маршрутизаторі, який забезпечує з’єднання між внутрішньою мережею і мережею Інтернет. Пакети, що входять, проходять зворотний процес. В такому разі багато приватних IPv4-адрес перетворюються в одну публічну адресу [2].

Статичний NAT – ручне відображення локальних та глобальна адреса, визначена адміністратором.

При налаштуванні статичного NAT необхідно вказати маршрутизатору, який із його портів буде транслювати NAT всередину, а який – назовні.

Для цього використовується команда ip nat inside / outside в режимі інтерфейсу, який налаштовується.

При налаштуванні статичного NAT можливо буде як вийти у зовнішню мережу, так і увійти із зовнішньої мережі у внутрішню через налаштований порт.

Якщо ж ми використовуємо у налаштуванні трансляцію з перекриттям (PAT), то з внутрішньої мережі у зовнішню вихід буде, а з глобальної мережі у локальну потрапити буде не можливо. Для цього використовується у поєднанні з налаштуванням NAT access-list, на якому детальніше зупинимося в пункті 1.8.

Динамічний же NAT використовує пул адрес ip nat pool починаючи з глобальної стартової адреси до глобальної кінцевої адреси.

Якщо порівняти статичний і динамічний NAT, виходить, що статичний NAT є зіставленням IP-адрес внутрішньої і зовнішньої одна до одної. Дозволяє використовувати зовнішнім джерелам підключення до внутрішніх з використанням статично призначеної загальної адреси. Для цього використовуємо команду ip nat inside source static локальна адреса глобальна адреса [3].

Динамічний NAT автоматично зіставляє внутрішні локальні і глобальні адреси. Використовує пул публічних адрес IPv4 для переводу ip nat pool ім’я адреса початкова адреса кінцева.

Налаштування DHCP-серверу і NAT на практиці буде розглянуто при проектуванні мережі у Розділі 2.

1.8 Налаштування захисту та конфігурування функцій безпеки (налаштування паролів, Port Security, ACL тощо)

Обмеження доступу до пристроїв для їх захисту можливе 4 способами:

- встановлення безпечного привілейованого режиму;

- встановлення безпечного користувацького режиму;

- встановлення безпечного доступу за протоколом Telnet / SSH;

- зашифрувати всі паролі.

У даній роботі встановлюємо паролі на користувацький режим як на комутаторах так і на маршрутизаторах. Робимо це командою – line console 0 і входимо в режим налаштування доступу до консолі. Вводимо password пароль і login для включення перевірки пароля.

Встановлюємо паролі на привілейований режим enable secret пароль.

Зашифруємо всі паролі, які вже введені і будуть введені командою service password-encryption. Тоді, при перегляді налаштувань за допомогою команд show, введення значення паролів виводитися не будуть так, як задавалися, а висвітлюватимуться шифром.

Port Security — це функція канального рівня, яка створена для попередження несанкціонованої зміни MAC-адреси мережевого підключення. Також, дана функція захищає комутатор від атак, які можуть бути направлені на переповнення таблиці MAC-адрес [4].

За допомогою Port Security можливо обмежити (на канальному рівні) кількість підключень (MAC-адрес) на інтерфейсі, а також, за необхідності, ввести безпечні MAC-адреси вручну (статичні MAC-адреси).

Для настройки Port Security будемо користуватися наступним чином: входимо в інтерфейс порта, вказуємо йому режим роботи access, далі призначаємо його до певної vlan і прописуємо команду switchport port-security > switchport port-security maximum 1/2/3 > switchport port-security violation restrict. Таким чином, ми вказали комутатору, що ми увімкнули Port Security на даному інтерфейсі;  
- «switchport port-security maximum 2» означає, що лише 1/2/3 MAC-адреси, можуть знаходитися на інтерфейсі одночасно; - «switchport port-security violation restrict» вказує режим реагування на порушення. Таким чином, якщо на даному інтерфейсі одночасно висвітиться зайва MAC-адреса, то всі пакети з цієї адреси будуть скидатися.

Дані налаштування будуть проводитись при конфігурації локальних мереж у Розділі 2.

ACL (Access Control List) – список прав доступу до об’єкта, який визначає, хто або що може отримувати доступ до нього і які саме операції дозволено або заборонено цьому суб’єкту проводити над об’єктом.

В системі з моделлю безпеки, заснованої на ACL, коли суб’єкт запитує виконання операції над об’єктом, система спочатку перевіряє список дозволених для цього суб’єкта операцій, і тільки після цього дає (або не дає) доступ до запитуваної дії.

У мережах ACL представляють список правил, що визначають порти служб або імена доменів, доступних на вузлі або іншому пристрої третього рівня OSI, кожен зі списком вузлів та/або мереж, яким дозволений доступ до сервісу. Мережеві ACL можуть бути налаштовані як на звичайному сервісі, так і на маршрутизаторі і можуть керувати як вхідним, так і вихідним трафіком, як брандмауер [5].

ACL-и бувають двох видів: стандартні і розширені. Стандартні дозволяють фільтрувати трафік тільки за одним критерієм – IP-адресою відправника.

Access-list 1 permit host ….IP – дозволяє вихід в Інтернет тільки з цієї IP-адреси.

Розширений ACL дозволяє фільтрувати трафік за великою кількістю параметрів:

- адреса відправника;

- адреса отримувача;

- TCP/UDP порт відправника;

- TCP/UDP порт отримувача;

- протоколу, завернутому в ip (відфільтрувати лише tcp, лише udp, лише icmp, лише gre);

- типу трафіка для даного протоколу (для icmp відфільтрувати лише icmp-reply);

- відділити TCP трафік, який встановлює з’єднання.

ACL необхідний для фільтрації трафіка на інтерфейсі. Стандартний ACL необхідно розміщувати максимально близько до отримувача трафіка.

Якщо розширений ACL – то на порт маршрутизатора, який підключаємо до порту відправника на вхід, тобто максимально близько до джерела трафіку.

ACL можна використовувати не лише для фільтрації трафіка, але і для обмеження адрес, з яких можна підключатися до маршрутизатора по telnet або ssh.

Детальне встановлення ACL та команди, які для цього використовуються буде висвітлено при проектуванні мережі у Розділі 2.

1.9 Налаштування віддаленого доступу до активного обладнання

Віддалений доступ до активного обладнання здійснюються за допомогою протоколів Telnet або SSH, які використовують порти 23 та 22, відповідно.

Протокол Telnet – один із найстаріших протоколів і сервісів рівня додатків в наборі TCP/IP. Telnet надає стандартний спосіб емуляції текстових термінальних пристроїв в мережі даних. Підключення по протоколу Telnet називається сеансом або підключенням віртуального терміналу (VTY). Віртуальний пристрій створюється за допомогою програмного забезпечення. Протокол Telnet є незахищеним, тому замість нього у нашій мережі використаємо протокол SSH, який забезпечує захищений віддалений вхід в систему і інші захищені мережеві сервіси, підтримує шифрування потоку даних.

Налаштувати адміністративний SVI (віртуальний інтерфейс комутатора) можна командою interface vlan1 (або іншої vlan, через мережу якої буде здійснюватися доступ до комутатора).

Комутатори – пристрої рівня 2, які не пересилають трафік по IP-адресі. IP-адреси призначаються для того, щоб пристрій міг бути доступний через мережу для управління і налаштування.

Далі присвоюємо комутатору IP-адресу командою ip address адреса маска підмережі.

Командою no shutdown вмикаємо інтерфейс, щоб він став активним.

Задаємо комутатору основний шлюз командою ip default-gateway адреса - IP-адреса маршрутизатора, до якого підключений даний комутатор.

Далі налаштовується відділений доступ для SSH.

Спочатку задаємо пристрою доменне ім’я командою ip domain-name і створюємо користувача – username користувач password пароль.

Генеруємо ключі шифрування командою crypto key generate rsa, задаємо значення 1024.

Комутатори Cisco підтримують до 16 каналів VTY, від 0 до 15, а маршрутизатори – 5 каналів, від 0 до 4.

Після цього переходимо в режим віддаленого доступу налаштування для комутатора - line vty 0 15, для маршрутизатора – line vty 0 4, і визначаємо використання протоколу SSH – transport input ssh.

Далі вказуємо, що для авторизації необхідно використовувати локальну базу користувачів і, що для підключення по SSH використовувати облікові дані створеного користувача: login local.

В кінці зазначаємо про використання протоколу SSH версії 2 – ip ssh version 2.

Встановлення віддаленого доступу до активного обладнання буде показано на рисунку в Розділі 2.

РОЗДІЛ 2 ПРАКТИЧНА ЧАСТИНА СТВОРЕННЯ КОМП’ЮТЕРНОЇ МЕРЕЖІ

2.1 Проектування мережі центрального офісу (LAN1)

Моделюємо мережу центрального офісу LAN1, відповідно до схеми завдання до курсової роботи.

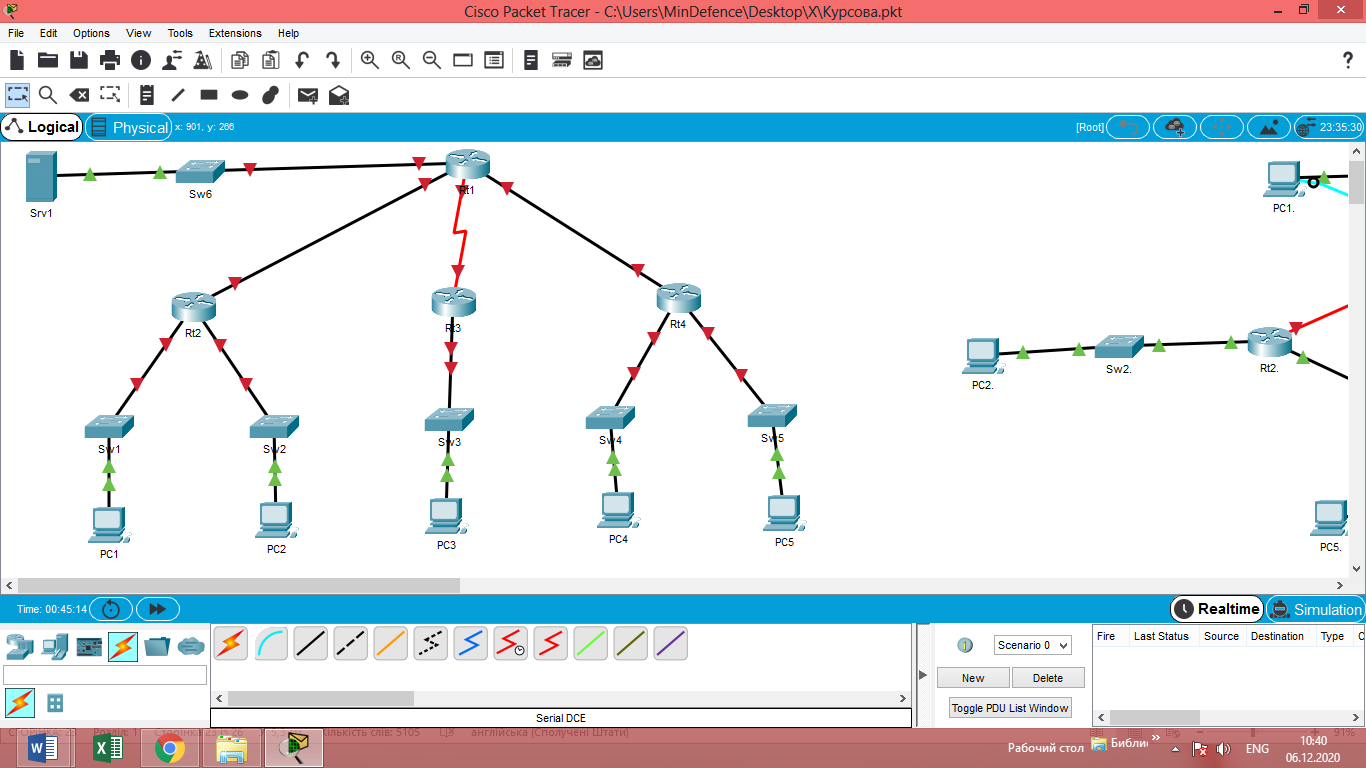


Рисунок 2.1 Мережа центрального офісу LAN1

При конфігурації даної мережі, відповідно до поставленого завдання, нам необхідно:

- вибрати маски підмереж, зробити оптимальний розрахунок адрес підмереж та хостів. Визначити, скільки адрес в кожній підмережі залишились вільними –

Переводимо за допомогою двійкової системи цифри, шукаємо найбільше значення, починаючи з найбільшої кількості пристроїв, використовуємо для розрахунку формули, вказані у пункті 1.2.

Наприклад, Net1 повинна бути розрахована на 120 пристроїв. Найближче значення – цифра 128, тобто 27. Це маска /25, тобто 255.255.255.128. Отже, за адресами підмережа Net1 матиме адресу 172.16.2.0/25, а адреса 172.16.2.127 буде широкомовною адресою даної підмережі. Хостам можуть бути призначені адреси з проміжку 172.16.2.1 – 172.16.2.126. Дана підмережа розрахована на 128 адрес і 126 пристроїв, а значить 6 вільних адрес.

Аналогічно вираховуємо адрес для інших підмереж і отримуємо:

- Net2 – адреса підмережі 172.16.2.128/27 і 5 вільних адрес;

- Net3 – адреса підмережі 172.16.2.160/29 і 2 вільні адреси;

- Net4 – адреса підмережі 172.16.2.176/28 і 4 вільні адреси;

- Net5 – адреса підмережі 172.16.2.192/28 і 2 вільні адреси.

- зробити кругову діаграму, показавши на ній всі сегменти адрес, які було виділено; визначити, скільки ще підмереж і якого обсягу залишились незадіяними –

діаграму виділених адрес зобразимо на рисунку 2.2

Рисунок 2.2 Діаграма виділених адрес

Для Net6 в завданні не вказана кількість пристроїв, проте за схемою видно, що нам знадобиться лише адреса для сервера Srv1 та порту маршрутизатора Rt1, до якого даний сервер підключено. Отже, адреса підмережі буде 172.16.2.208/30.

Резерв адрес із яких ще можна утворити підмережі, у такому випадку, буде у проміжку 172.16.2.212 – 172.16.2.254 і становитиме 43 адреси.

Із такого резерву можна утворити підмережі з маскою /26 і менше.

Підмережі між маршрутизаторами Rt1-Rt2, Rt1-Rt3, Rt1-Rt4 будуть 172.16.2.212/30, 172.16.2.216/30 та 172.16.2.220/30 відповідно.

- дати імена всім комутаторам і маршрутизаторам, поставити паролі на користувацький і привілейований режим маршрутизаторів –

даємо імена пристроям відповідно до завдання та встановлюємо паролі способами і за допомогою команд, вказаних у пунктах 1.4, 1.5 та 1.8.

Паролі скрізь поставимо на користувацький режим «lan1» і на режим привілейований «ofis».

На рисунку 2.3 зображений термінал з введеними командами для вищезазначених налаштувань для одного з маршрутизаторів.

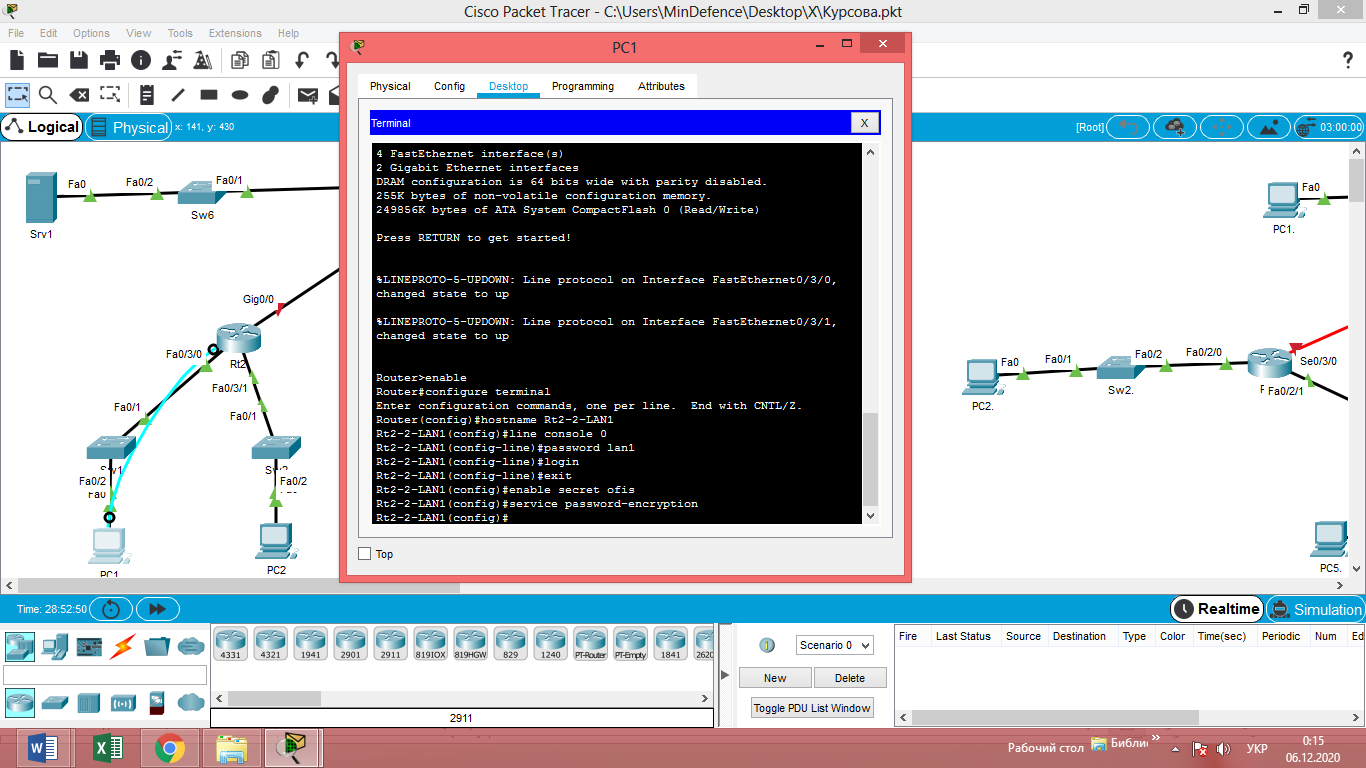


Рисунок 2.3 Базові налаштування маршрутизатора

Також, задаємо серверу IP-адресу з його підмережі;

- налаштувати віддалений доступ SSH та NAT на маршрутизаторі Rt1 –

доступ по SSH налаштовуємо за пунктом 1.9 та NAT за командами пункту 1.7.

Налаштування відділеного доступу зображено на рисунку 2.4.

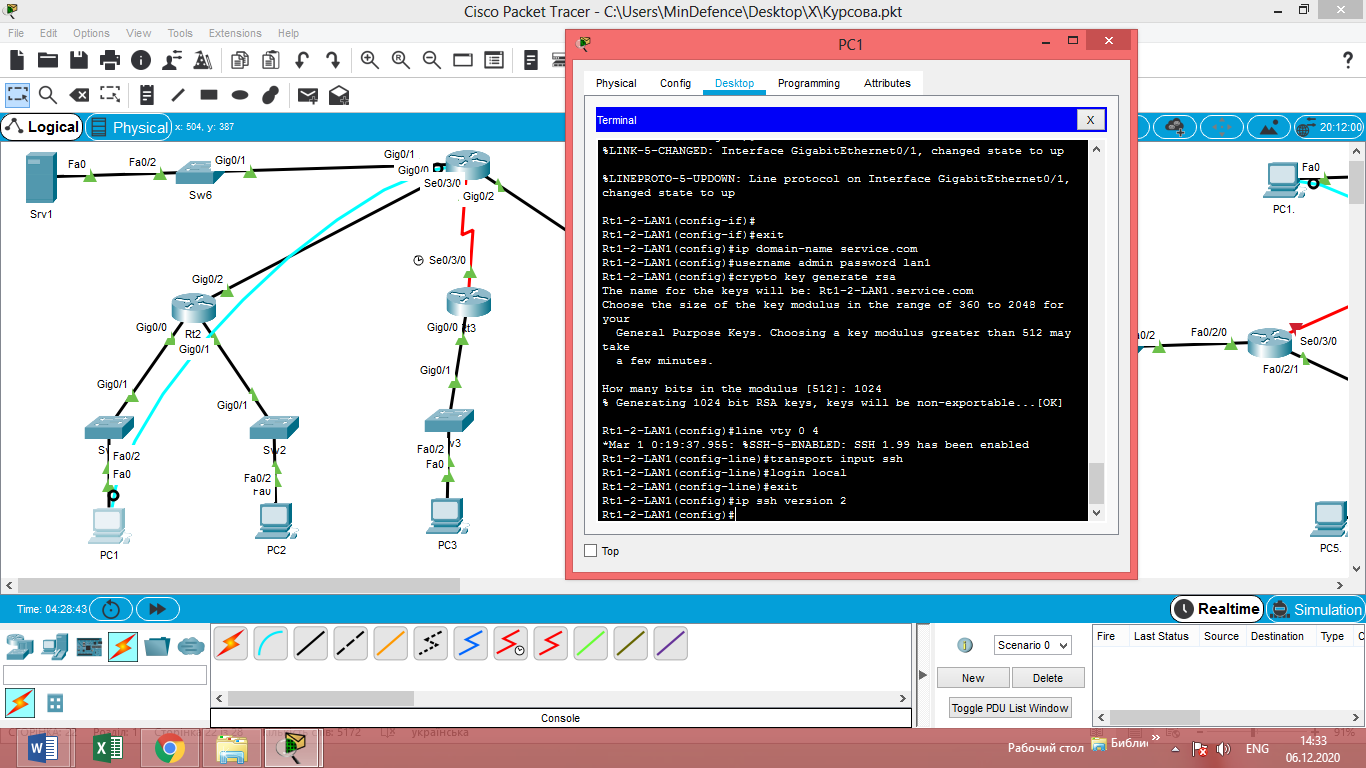


Рисунок 2.4 Налаштування віддаленого доступу

до маршрутизатора по SSH

Тобто віддалений доступ буде проходити за іменем користувача admin і паролем користувача lan1.

Налаштування NAT для сервера і комп’ютерів виглядають наступним чином.

Встановлюємо для сервера статичний NAT, а для всіх комп’ютерів трансляцію з перекриттям.

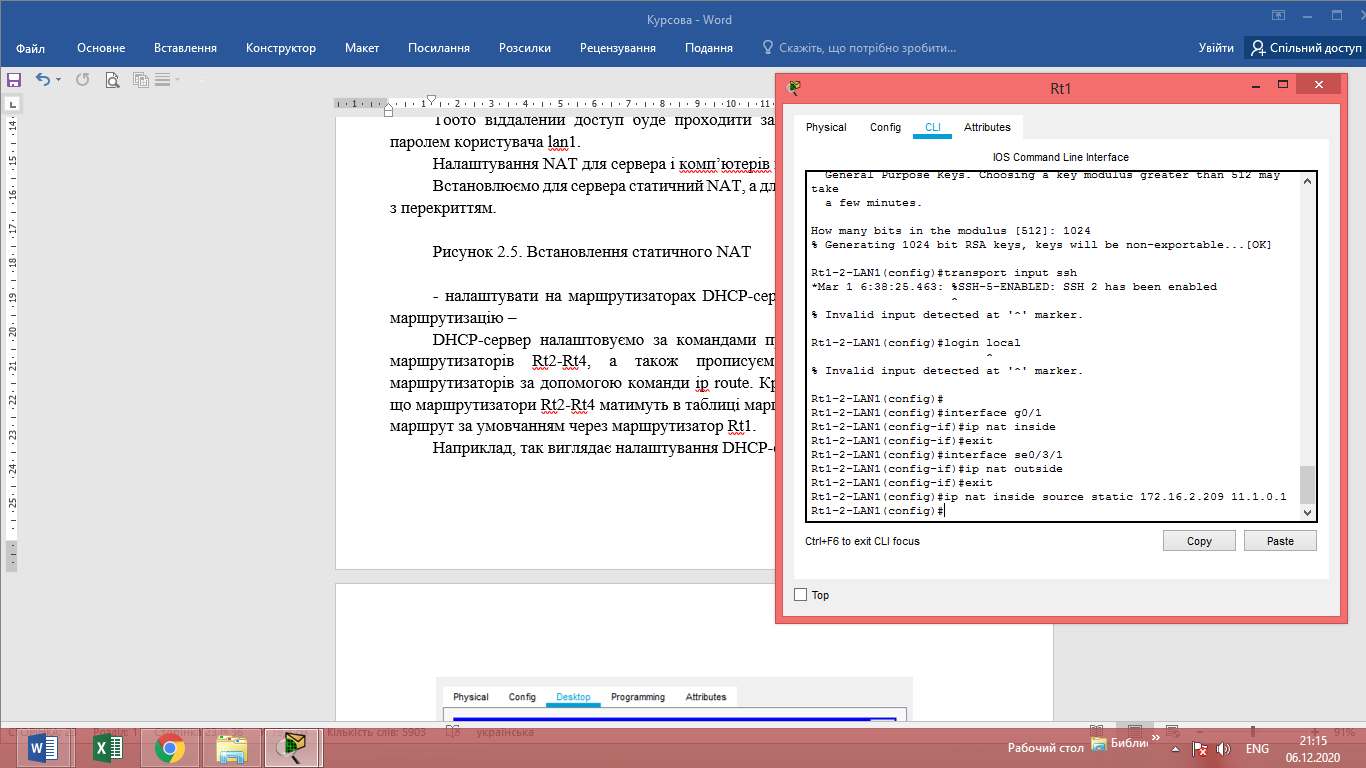


Рисунок 2.5 Встановлення статичного NAT

- налаштувати на маршрутизаторах DHCP-сервер, сконфігурувати статичну маршрутизацію –

DHCP-сервер налаштовуємо за командами пункту 1.7 на кожному порту маршрутизаторів Rt2-Rt4, а також прописуємо статичні маршрути для маршрутизаторів за допомогою команди ip route. Крім того, необхідно зазначити, що маршрутизатори Rt2-Rt4 матимуть в таблиці маршрутизації лише один запис як маршрут за умовчанням через маршрутизатор Rt1.

Наприклад, так виглядає налаштування DHCP-сервера на Rt1.

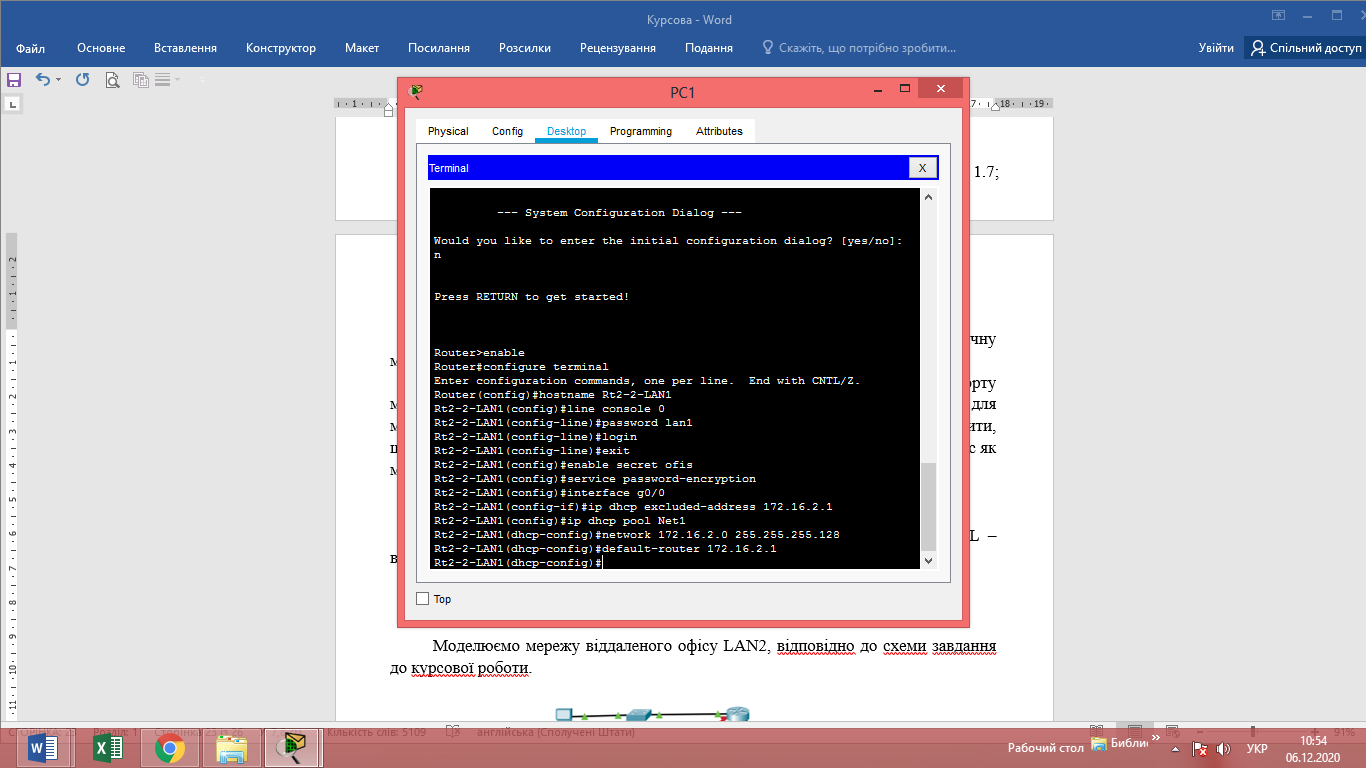


Рисунок 2.6 Конфігурування DHCP-сервера на маршрутизаторі

Таким чином, ми вказали маршрутизатору, що на інтерфейсі G0/0 повинен працювати DHCP-сервер з назвою Net1, який видаватиме адреси з мережі 172.16.2.0 з маскою підмережі 255.255.255.128 та у якості основного шлюза видаватиме IP-адресу маршрутизатора.

Тепер, перевіривши IP-адресу нашого комп’ютера з підмережі Net1, видно, що всі дані він отримав по DHCP, який ми налаштували.

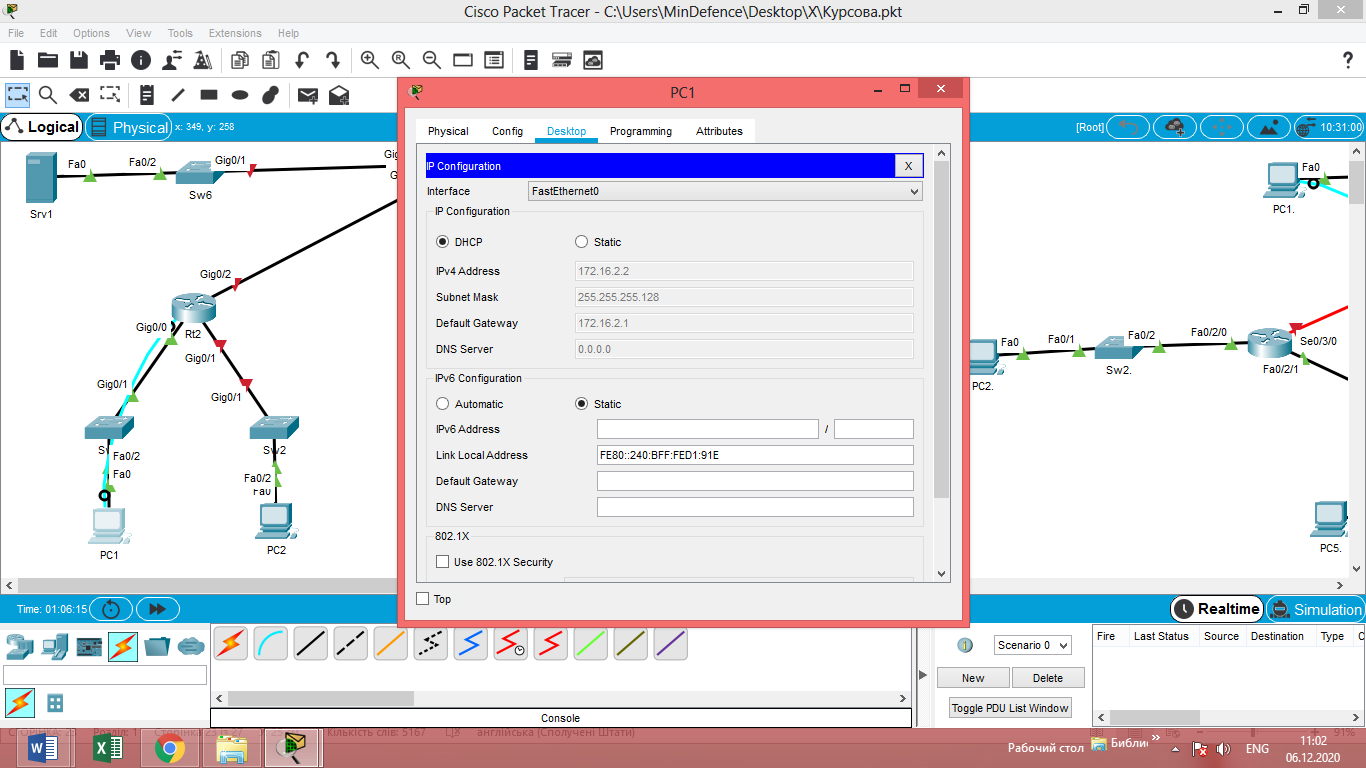


Рисунок 2.7 Динамічна IP-конфігурація комп’ютера

- налаштувати механізм пакетної фільтрації за допомогою списків ACL – відповідно до пункту 1.8,

Для встановлення стандартного ACL, тобто заборони відправлення трафіку з Net3 в Net6, ставимо ACL на порту маршрутизатора Rt1, який підключений до Net6 на вихід.

Для встановлення стандартного ACL, тобто заборони відправлення трафіку з Net5 в Net3, ставимо ACL на порту маршрутизатора Rt3, який підключений до Net3 на вихід.

Для встановлення стандартного ACL, тобто заборони відправлення трафіку з Net4 в Net2, ставимо ACL на порту маршрутизатора Rt2, який підключений до Net2 на вихід.

А розширений ACL ставитимемо на маршрутизатори Rt2, Rt3 на вхід з підмереж Net1 та Net3 відповідно.

На цьому налаштування мережі центрального офісу LAN1 завершено.

2.2 Проектування мережі віддаленого офісу (LAN2)

Моделюємо мережу віддаленого офісу LAN2, відповідно до схеми завдання до курсової роботи.

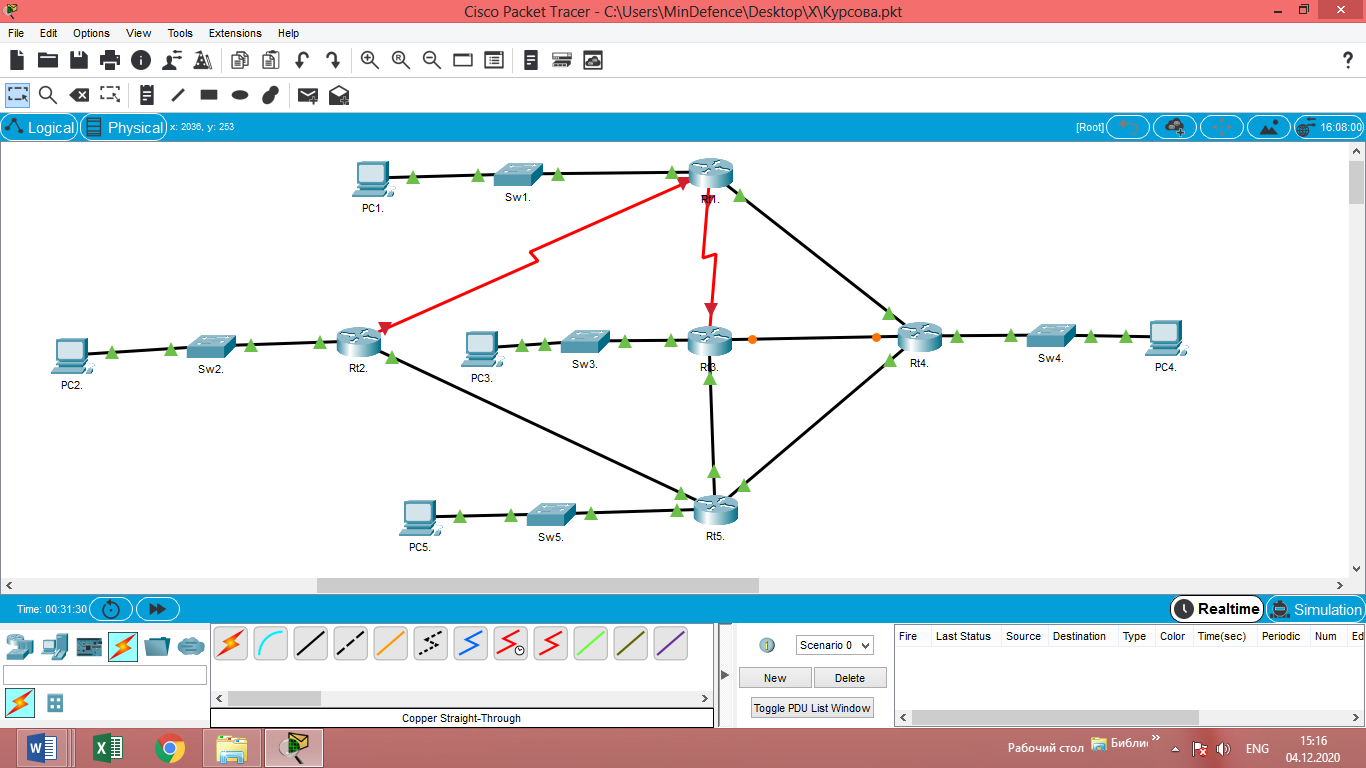


Рисунок 2.8 Мережа віддаленого офісу LAN2

При конфігурації даної мережі, відповідно до поставленого завдання, нам необхідно:

- поділити рівномірно простір мережі. Відповідно до схеми, у нас повинно вийти 12 підмереж. Між маршрутизаторами підмережі будуть мати /30 маску підмережі, в інших сегментах мережі – /27 маску підмережі. В такому разі простір буде розподілено рівномірно і залишиться резерв адрес.

Ділимо доступний простір аналогічно поділу в пункті 2.1.

Виходить 5 підмереж з адресами: 192.168.2.0/27, 192.168.2.32/27, 192.168.2.64/27, 192.168.2.96/27, 192.168.2.128/27 і 7 підмереж з адресами: 192.168.2.160/30, 192.168.2.164/30, 192.168.2.168/30, 192.168.2.172/30, 192.168.2.176/30, 192.168.2.180/30, 192.168.2.184/30.

Далі даємо імена пристроям відповідно до завдання та встановлюємо паролі способами і за допомогою команд, вказаних у пунктах 1.4, 1.5 та 1.8.

Паролі скрізь поставимо на користувацький режим «lan2» і на режим привілейований «ofis».

Прописуємо IP-адреси комп’ютерам, відповідно до утворених підмереж.

- проаналізувати переваги та недоліки різних протоколів маршрутизації, детально зупинившись на протоколі OSPF та налаштувати маршрутизацію за цим протоколом –

Протоколи LSA працюють найкраще в ситуаціях, коли: комп’ютерна мережа велика та ієрархічна; адміністратор має достатньо знань; швидка конвергенція у мережі дуже актуальна.

Порівняння деяких протоколів динамічної маршрутизації висвітлено у таблиці 2.1.

Таблиця 2.1

Порівняння деяких протоколів динамічної маршрутизації

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Критерій | DVA | | | | LSA | |
| RIPv1 | RIPv2 | IGRP | EIGRP | OSPF | IS-IS |
| Швидкість конвергенції | - | - | - | + | + | + |
| Масштаб мережі | - | - | - | + | + | + |
| VLSM | - | + | - | + | + | + |
| Використання ресурсів | - | - | - | +/- | + | + |
| Підтримка | + | + | + | - | - | - |

За завданням до курсової роботи, налаштування динамічної маршрутизації в мережі відділеного офісу LAN2 проектується за допомогою протоколу динамічної маршрутизації OSPF.

Протокол OSPF належить до алгоритмів стану зв’язків (LSA). Маршрутизатори знають про всю комп’ютерну мережу шляхом збирання інформації від усіх маршрутизаторів, кожен з них має повну топологічну карту мережі. LSA не здійснюють періодичних оновлень. Оновлення надсилаються лише у випадку зміни топології мережі.

OSPF (Open Shortest Part First) – протокол динамічної маршрутизації, заснований на технології відслідковування стану каналу (link-state technology) і такий, що використовує для знаходження найкоротшого шляху алгоритм Дейкстри [6].

Протокол OSPF призначений для використання у великих, складних мережах, спроектованих на основі продуманого підходу. Проте, протокол OSPF не допускає використання ієрархічних проектів у поєднанні з погано спроектованими структурами IP; є набагато більш складним порівняно з RIP; потребує більших ресурсів процесора і оперативної пам’яті; потребує більших витрат часу на проектування і реалізацію.

Переваги OSPF у порівнянні з EIGRP: сприяє створенню ієрархічних проектів мереж; має менш складну метрику порівняно із складеною метрикою EIGRP; не схильний до проблем, пов’язаних з постійним перебуванням маршруту в активному стані; не залежить від виробника конкретного продукту.

Недоліки OSPF у порівнянні з EIGRP: метрика не така гнучка; не забезпечує розподіл навантаження по маршрутах з нерівною вартістю; потребує більших ресурсів процесора і оперативної пам’яті; потребує більших витрат часу на проектування і реалізацію.

Властивості OSPF:

- висока швидкість збіжності;

- підтримка мережних масок змінної довжини VLSM;

- відсутність обмежень досяжності;

- оптимальне використання пропускної здатності мережі;

- оптимальний вибір шляху маршрутизації.

Маршрутизатори обмінюються hello-пакетами через всі інтерфейси, на яких активований OSPF. Маршрутизатори стають сусідами, розділяючи загальний канал передачі даних.

Для налаштування протоколу динамічної маршрутизації OSPF, заходимо в режим глобальної конфігурації маршрутизатора: enable > configure terminal.

Включаємо OSPF протокол командою router ospf 1.

Задаємо ID адресу маршрутизатору router-id ….

Далі вводимо команду network адреса мережі 0.0.0.255 area 1. За цією командою, маршрутизатор повідомляє іншим маршрутизаторам про мережі, які відомі йому за таблицею маршрутизації. Маска підмережі означає кількість пристроїв-адрес в цій мережі, а area1 – зона, про адреси якої повідомляє маршрутизатор.

При налаштуванні маршрутів за допомогою OSPF, літерою «о» в таблиці маршрутизації позначаються маршрути, отримані за протоколом OSPF, як видно на рисунку 2.9. Тоді вказується IP-адреса мережі призначення (віддаленої), адміністративна дистанція протоколу OSPF і метрика маршруту; IP-адреса порту наступного транзитного вузла на шляху до мережі призначення; час існування даного маршруту; локальний інтерфейс, через який слід надсилати пакети до мережі призначення.

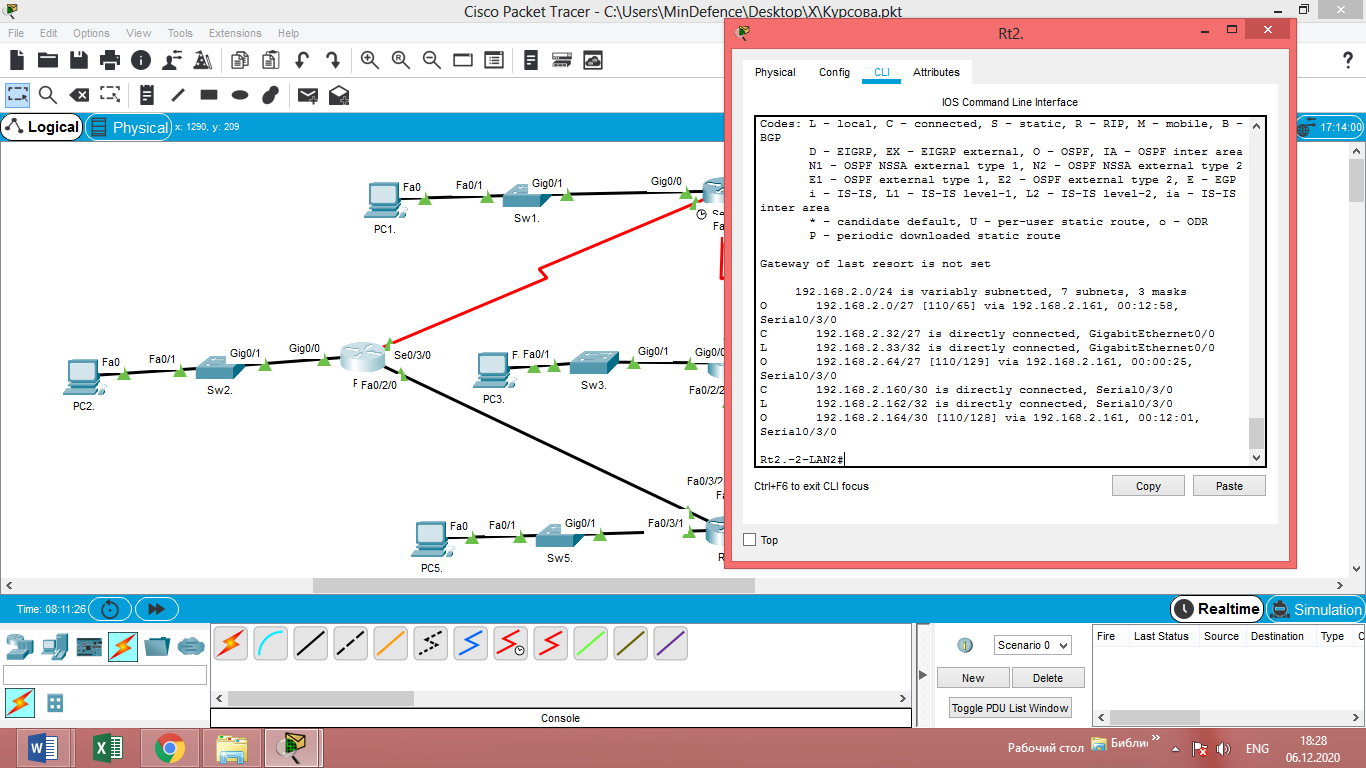


Рисунок 2.9 Таблиця маршрутизації

Для перевірки пропускної спроможності каналу вводимо команду show interfaces порт, на якому працює OSPF. Команда show ip ospf покаже нам роботу протоколу, а команда show ip ospf neighbor – сусідні OSPF-маршрутизатори, які знаходяться у сусідських відношеннях з даним маршрутизатором.

На рисунку 2.10 видно, що поки ми вводимо маршрути по черзі кожному маршрутизатору, вони вже обмінюються пакетами і повідомляють одне одному про відомі мережі.

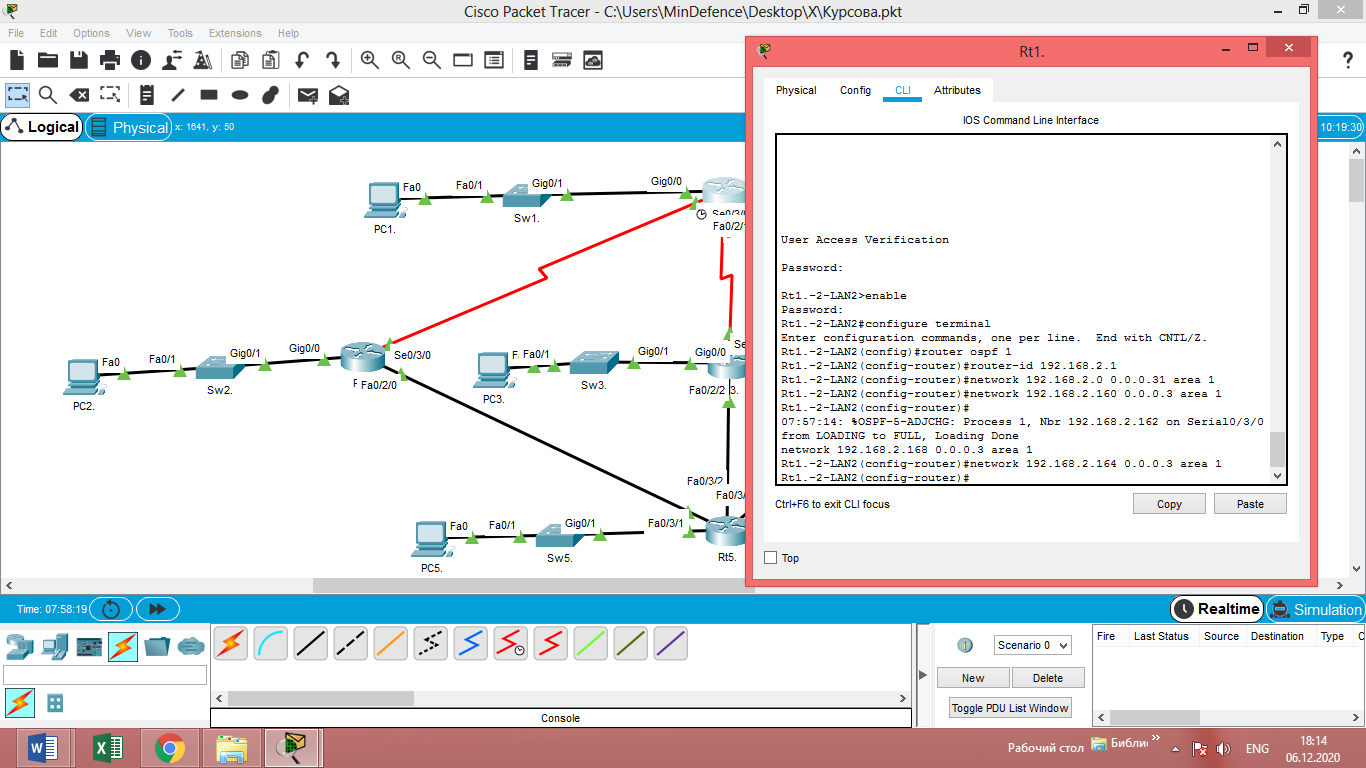


Рисунок 2.10 Налаштування маршрутизації за допомогою протоколу динамічної маршрутизації OSPF

- налаштувати динамічний NAT. Динамічний NAT використовує пул адрес ip nat pool. Він автоматично зіставляє внутрішні локальні і глобальні адреси. Використовує пул публічних адрес IPv4 для переводу. Тепер усі наші адреси з мережі 192.168.2.0/24 переводитимуться в пул глобальних адрес з проміжку 11.1.0.50-11.1.0.100 з маскою підмережі /16.

- налаштувати доступ по SSH до маршрутизатора Rt2. Налаштовуємо аналогічно, як в пункті 2.1 за іменем користувача admin і паролем користувача lan2.

Заходимо в термінал на РС2. і вводимо необхідні дані, як на рисунку 2.10.

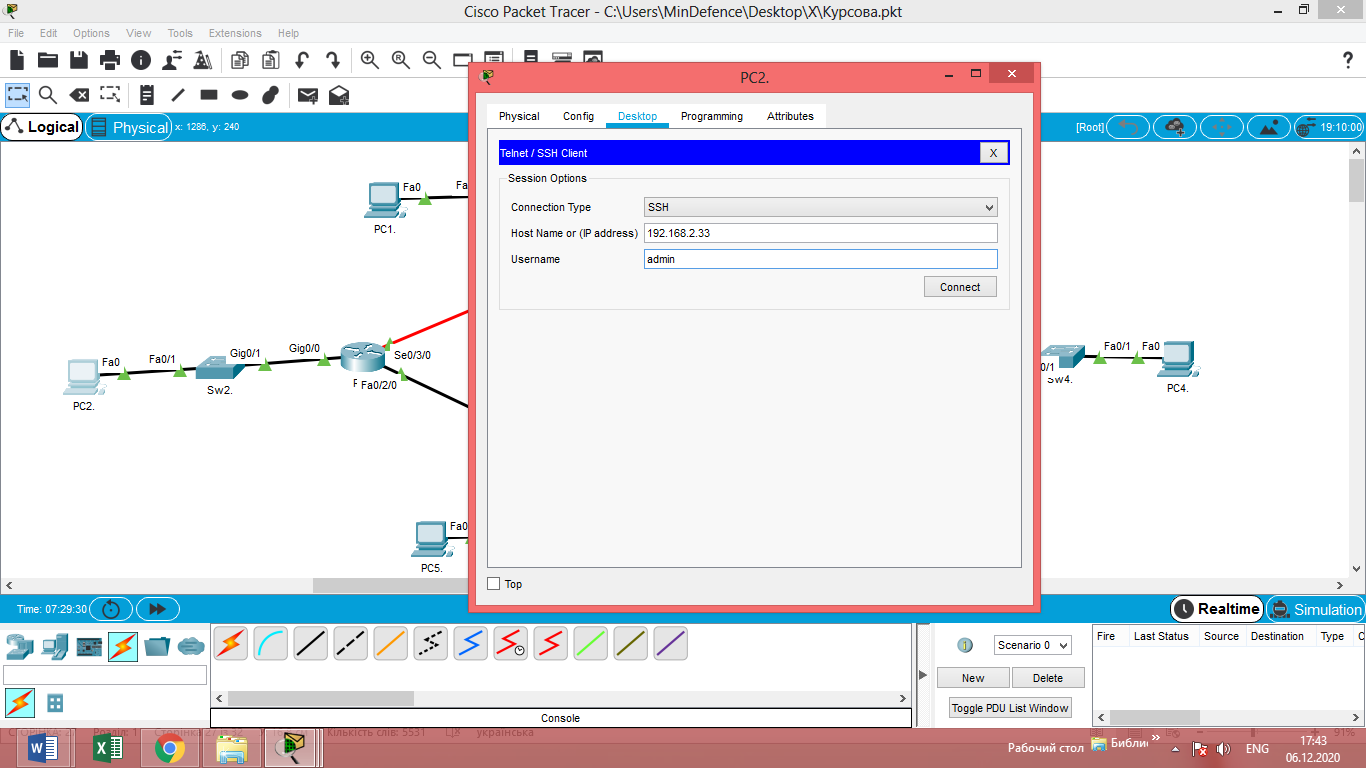


Рисунок 2.11 Встановлення віддаленого доступу по SSH

У новому вікні, яке відкриється, вводимо пароль і переходимо до маршрутизатора.

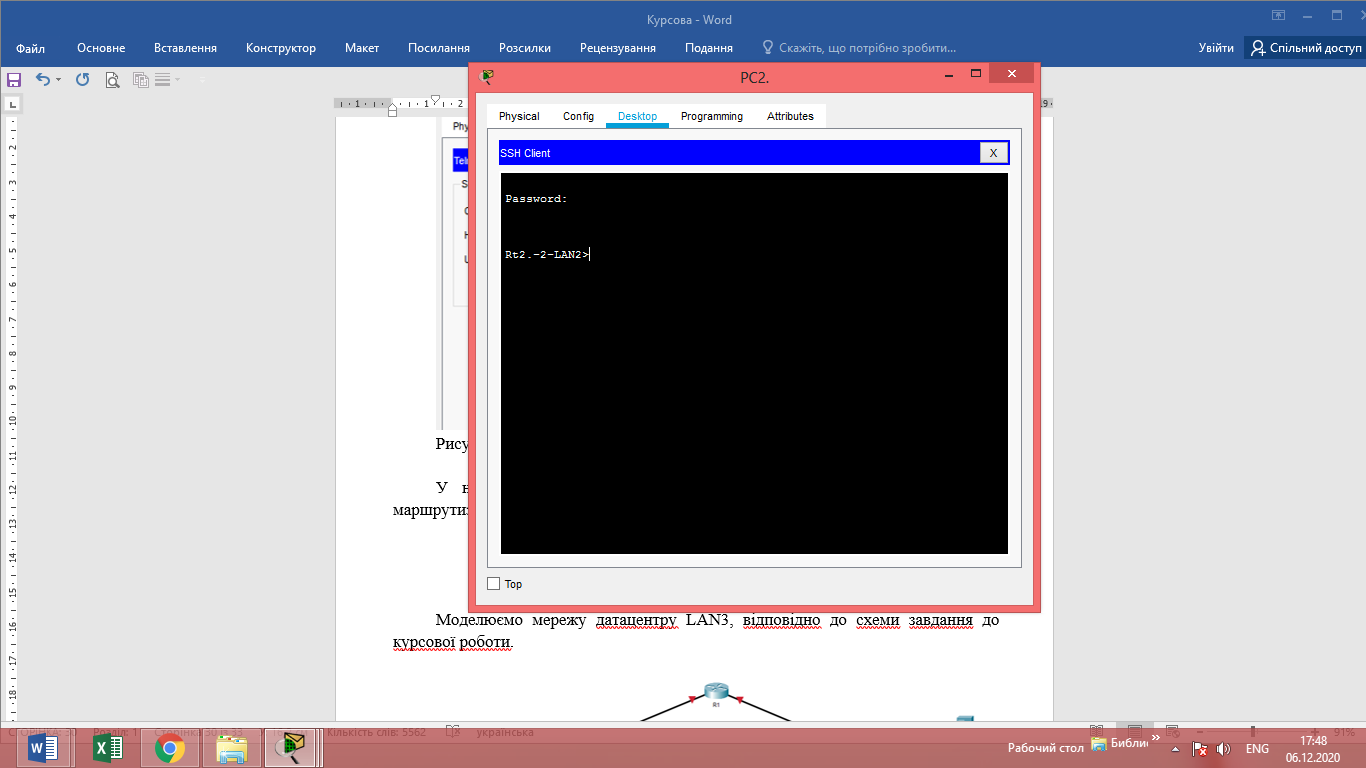


Рисунок 2.12 Віддалений доступ до маршрутизатора по SSH

На цьому налаштування мережі віддаленого офісу LAN2 завершено.

2.3 Проектування мережі датацентру (LAN3)

Моделюємо мережу датацентру LAN3, відповідно до схеми завдання до курсової роботи.

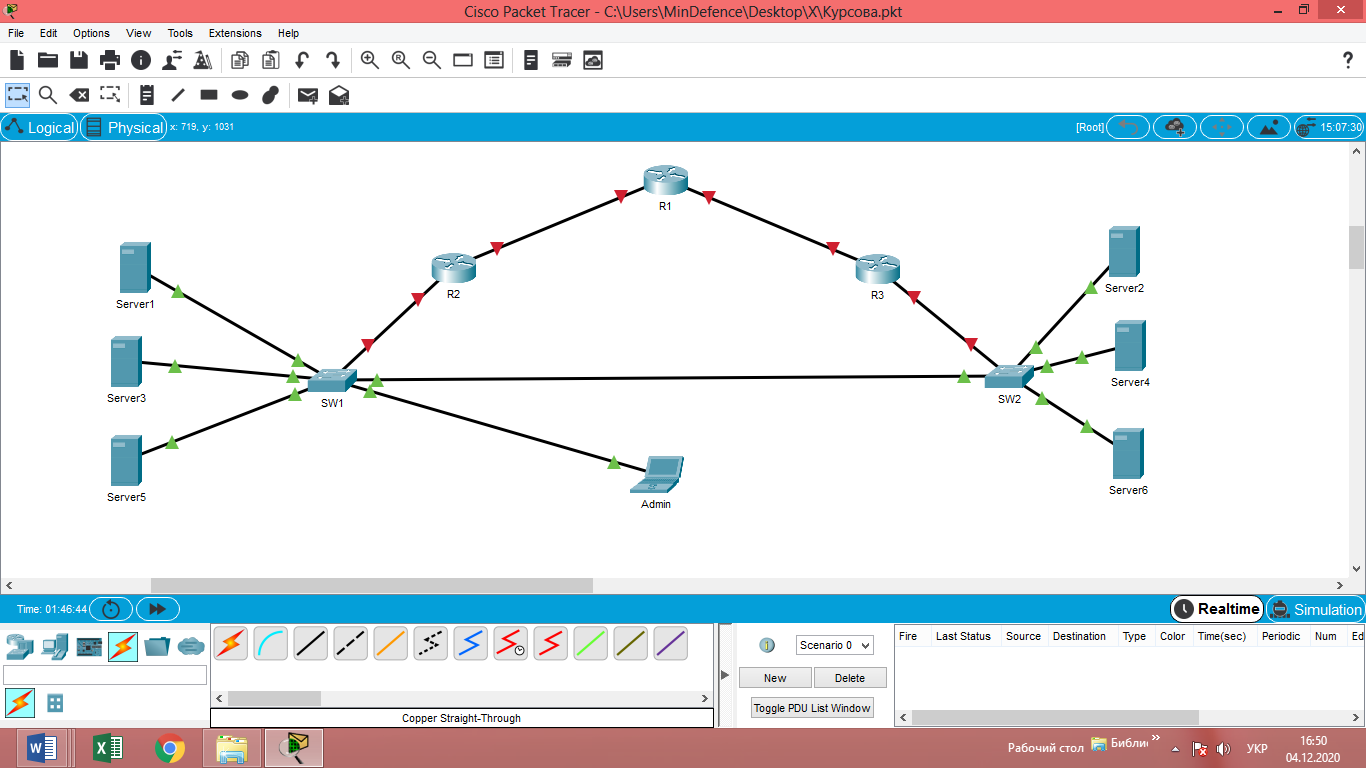


Рисунок 2.13 Мережа датацентру LAN3

При конфігурації даної мережі, відповідно до поставленого завдання, нам необхідно:

- на комутаторах створити Vlan1, Vlan2, Vlan3. Віднести сервери до кожного Vlan.

Даємо імена пристроям відповідно до завдання та встановлюємо паролі способами і за допомогою команд, вказаних у пунктах 1.4, 1.5 та 1.8.

Паролі скрізь поставимо на користувацький режим «lan3» і на режим привілейований «ofis».

Створюємо на комутаторах Vlan, визначаємо режими роботи портів access або trank, на маршрутизаторах R2 та R3 створюємо сабінтерфеси командами, відповідно до пункту 1.9.

Налаштування на комутаторах Vlan показано на рисунку 2.14.

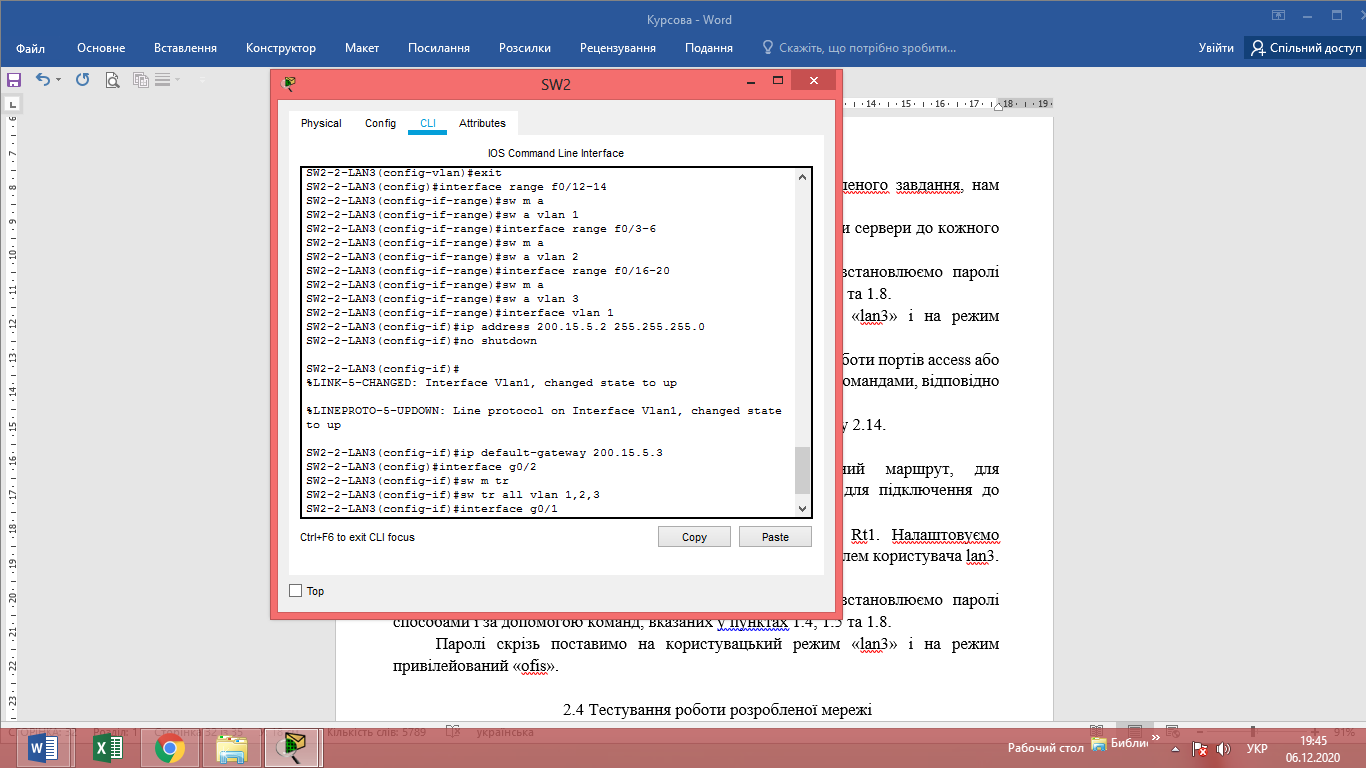


Рисунок 2.14 Створення Vlan на комутаторі

Створення сабінтерфейсів на порту маршрутизатора зображено на рисунку 2.15.

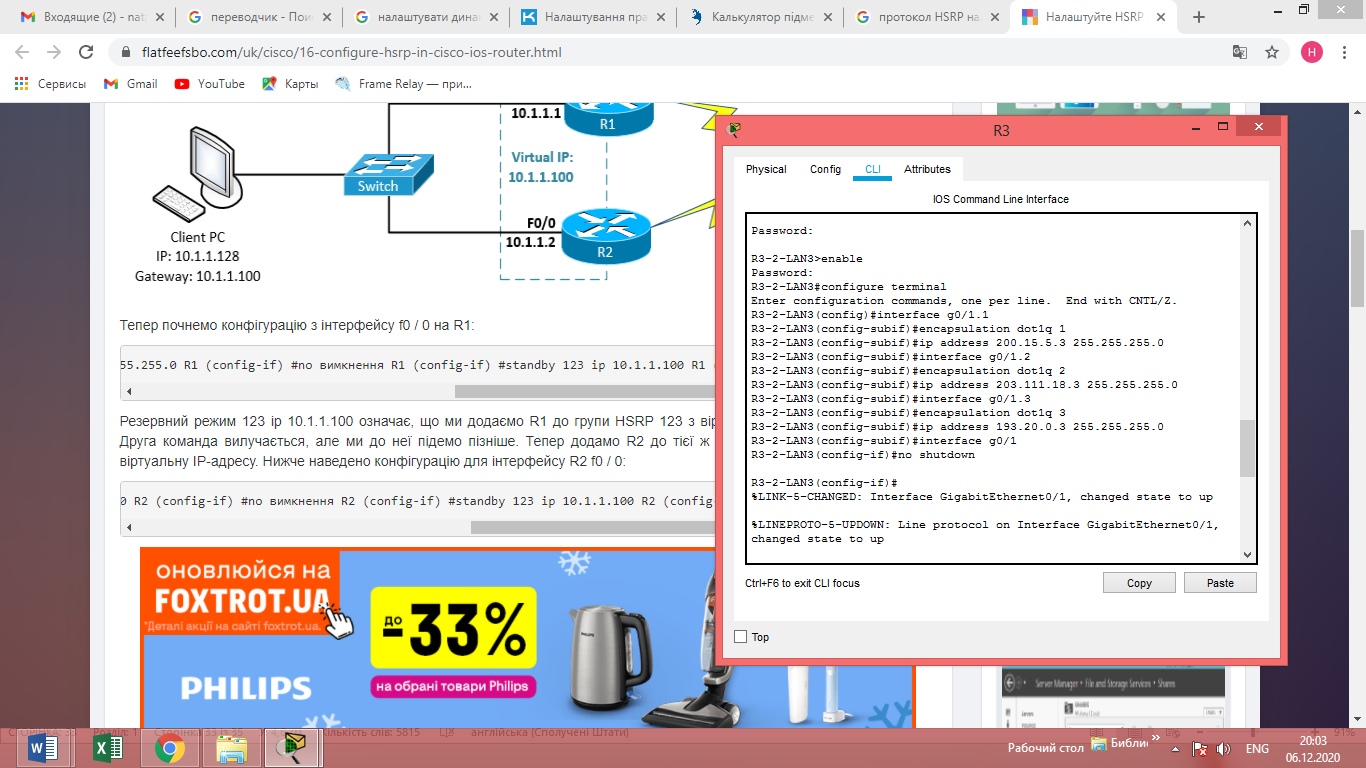


Рисунок 2.15 Створення сабінтерфейсів на маршрутизаторі

Також, налаштовуємо на маршрутизаторах R2 і R3 протокол HSRP для обслуговування Vlan, який передбачає резервний маршрут на випадок відмови основного. Одразу після увімкнення він починає працювати, що видно на рисунку 2.16.

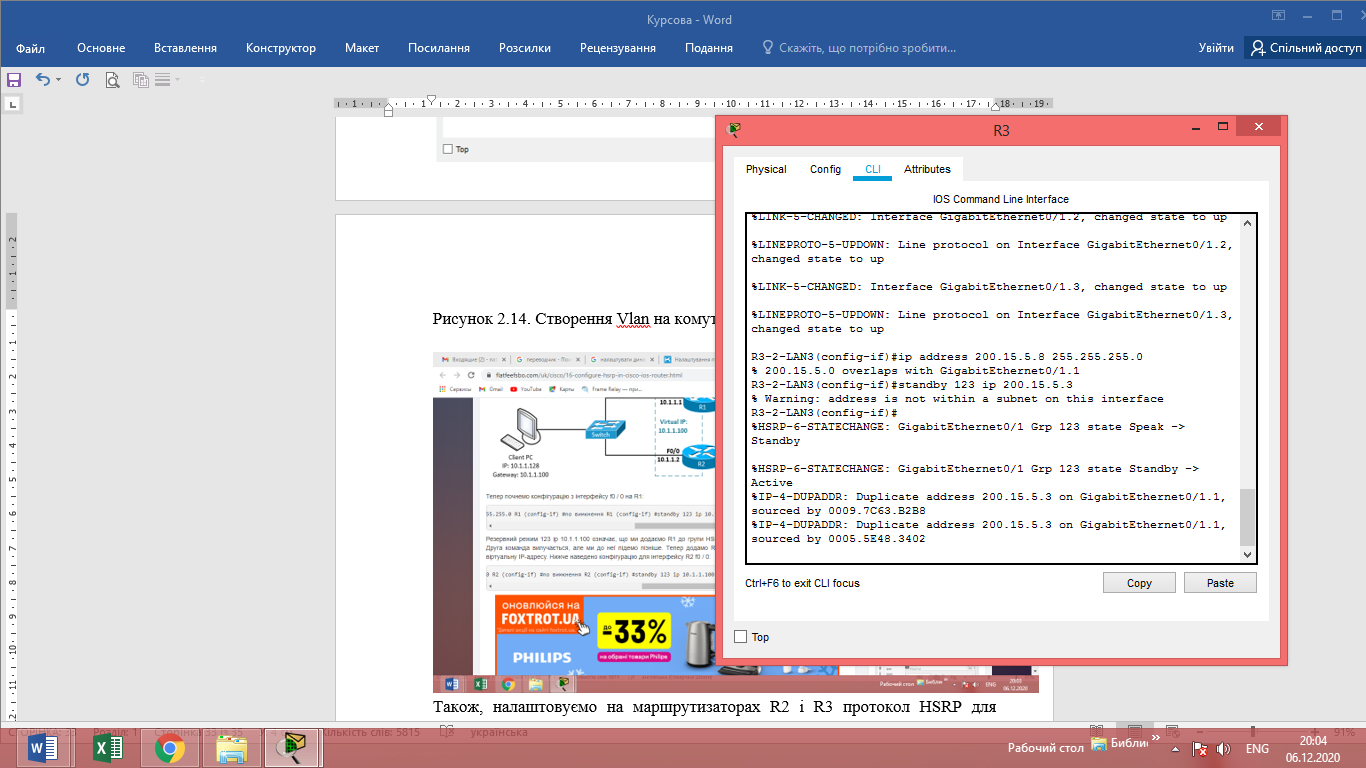


Рисунок 2.16 Включення протоколу HSRP на маршрутизаторі

- між маршрутизаторами конфігуруємо статичний маршрут, для маршрутизатора R1 створити маршрут за замовчуванням для підключення до глобальної мережі, аналогічно як при проектуванні мереж центрального та віддаленого офісу.

Для об’єднання маршрутизаторів R2 та R3 з маршрутизатором R1 створюємо мережі 172.16.2.0/30 та 172.16.3.0/30 відповідно.

- налаштувати доступ по SSH до маршрутизатора R1. Налаштовуємо аналогічно, як в пункті 2.1 за іменем користувача admin і паролем користувача lan3.

На цьому проектування мережі датацентру завершено і можна поєднувати всі три LAN між собою.

2.4 Об’єднання LAN1-LAN3 та тестування роботи розробленої мережі

Об’єднання LAN1-LAN3 проводимо за допомогою комутатора Frame Relay, відповідно до умов завдання. Повністю зконфігурована та об’єднана мережа представлена на рисунку 2.17.

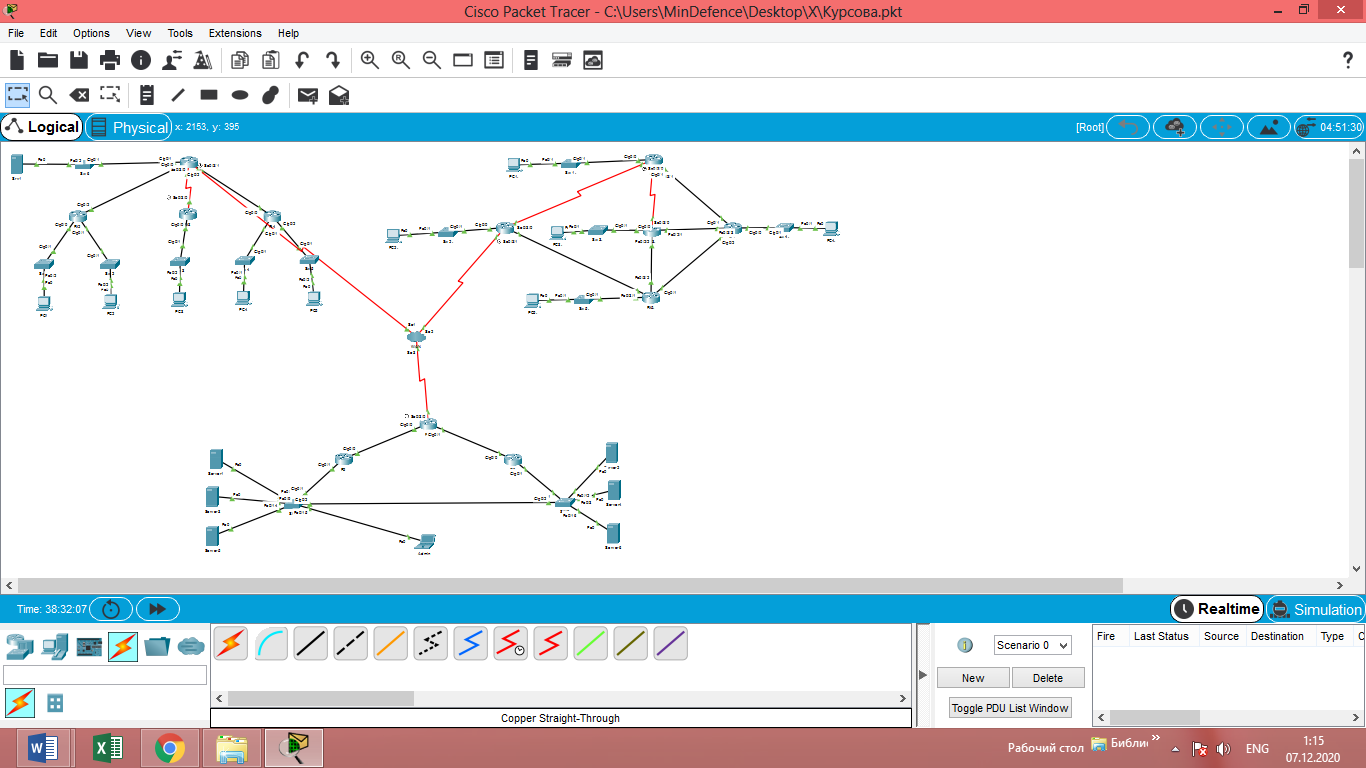


Рисунок 2.17 Мережа, розроблена за завданням курсової роботи

При тестуванні роботи розробленої мережі одразу видно, що мережі LAN та їх підмережі налаштовані вірно, ACL-списки та маршрутизація в мережі спрано працюють, адже при спробі зв’язатися одного комп’ютера з іншим, ping-запит проходить в тих підмережах, де не заборонені ACL-списки і не проходить там, де встановлена заборона. Результат ехо-запитів видно на рисунках 2.18 і 2.19.

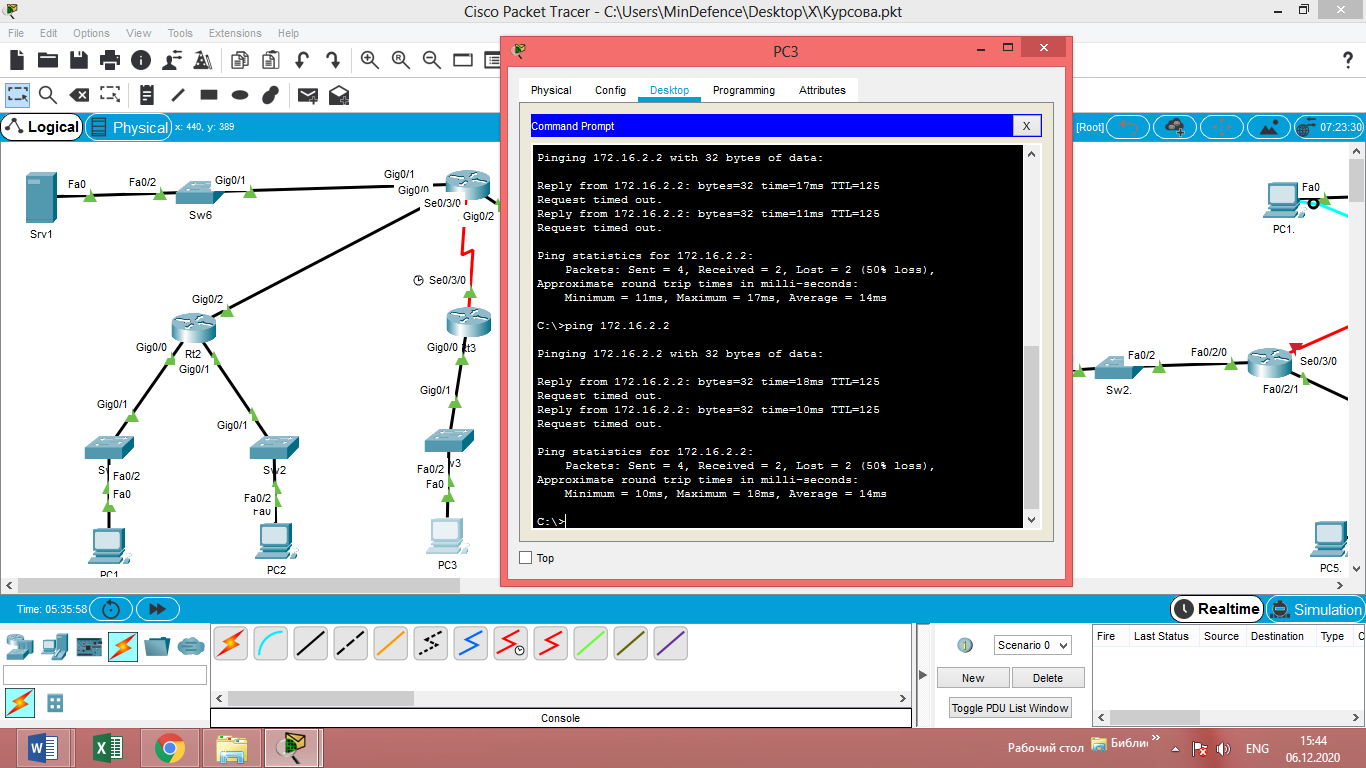


Рисунок 2.18 Проходження ехо-запиту з Net3 LAN1 до Net1 LAN1

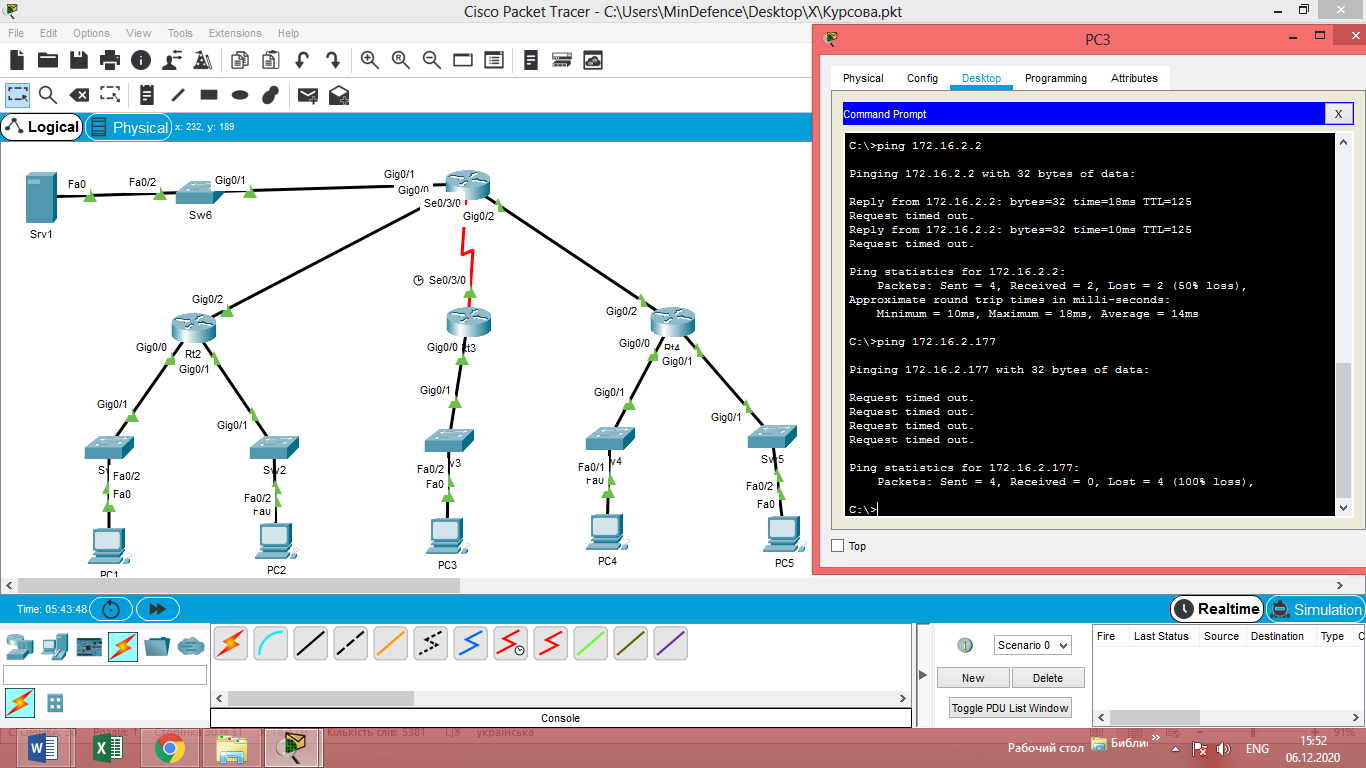


Рисунок 2.19 Не проходження ехо-запиту з Net3 LAN1 до Net5 LAN1

Коректну роботу мережі датацентру LAN3 проводимо, підключаючись до веб-серверу з мережі Vlan1 за допомогою ноутбука адміністратора, який належить до Vlan3. Результати підключення зображено на рисунку 2.20.

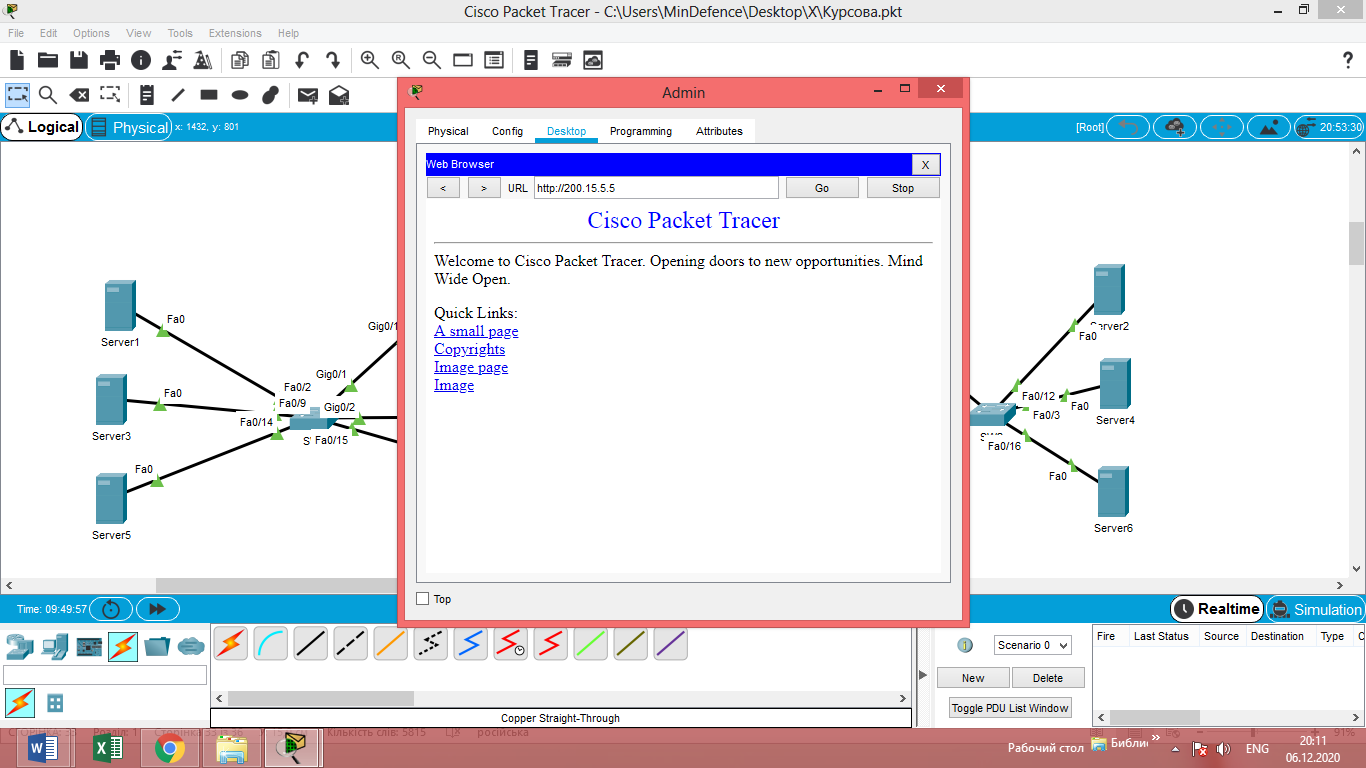


Рисунок 2.20 Заходження на веб-сторінку серверу з мережі Vlan1

ВИСНОВКИ

При написанні курсової роботи була розроблена корпоративна мережа, зконфігуроване активне обладнання та проведено комп’ютерне моделювання з використанням сучасного симулятора комп’ютерних мереж - Cisco Packet Tracer.

Зпроектована мережа складається з трьох LAN-мереж: центрального офісу, віддаленого офісу та дата центру, де знаходиться робоче місце адміністратора.

З’єднання між LAN-мережами проходить через комутатор Frame relay та послідовні інтерфейси.

Кожна мережа спроектована відповідно різних умов завдання, зокрема, стосовно розподілу адресного простору, способу маршрутизації, механізмів захисту та віддаленого доступу.

Проектуючи першу LAN, адресний простір був поділений з резервом адрес, налаштована статична маршрутизація, налаштовані механізми пакетної фільтрації.

Друга LAN розроблена також з поділом мережі на під мережі, налаштована всередині локальної мережі динамічна маршрутизація за допомогою протоколу OSPF.

Третя LAN складається з шести серверів, з’єднаних комутаторами, на яких налаштовані віртуальні локальні мережі VLAN, налаштований статичний маршрут всередині мережі.

В роботі показано у всіх трьох мережах зміна імені пристрою, встановлення паролів на користувацький і привілейований режим на маршрутизаторах, встановлення віддаленого доступу до шлюзових маршрутизаторів за допомогою SSH, трансляція NAT.

Крім того, по ходу написання роботи і проектування мережі, а також по закінченню створення мережі, проводилися перевірка коректності її роботи за допомогою перевірки налаштувань, утиліт ping, traceroute, вбудованим інструментарієм симулятора комп’ютерних мереж.

Дана мережа є надійною, захищеною мережею. Спроектована дуже вдало, в кожній LAN є запас резервних адрес, що, при необхідності, дасть змогу розширити межі мережі.

Крім того, динамічна маршрутизація в LAN2 спрощує роботу адміністратора.

Для вдосконалення роботи мережі можна провести динамічні маршрути і в інших LAN.

Під час виконання курсової роботи здобуті навички у налаштуванні безпеки обладнання, вибору маршрутизації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Олещенко Л. М. Організація комп’ютерних мереж. Конспект лекцій. – КПІ ім. Ігоря Сікорського. – 2018 р. – 225 с.

2. NAT Definition [Електронний ресурс] - Режим доступу: https://techterms.com/definition/nat

3. Налаштування статичного NAT в маршрутизаторі Cisco IOS [Електронний ресурс] - Режим доступу: https://flatfeefsbo.com/uk/cisco/20-configure-static-nat-in-cisco-ios-router.html.

4. Настройка Port Securiti на комутаторах Cisco [Електронний ресурс] - Режим доступу: http://ciscomaster.ru/content/nastroyka-port-security-na-kommutatorah-cisco.

5. Что такое ACL и как его настраивать [Електронний ресурс] - Режим доступу: http://ciscotips.ru/acl.

6. Порівняння деяких протоколів динамічної маршрутизації. Комп’ютерні мережі [Електронний ресурс] / Вінницький національний технічний університет - Режим доступу: https://web.posibnyky.vntu.edu.ua/fitki/3yarovijk\_komp\_merezhi/4.5.html.