**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 СИСТЕИ ТА МЕРЕЖІ**

**(РІВЕНЬ D БЕЗПЕКА КОМП’ЮТЕРНИХ СИСТЕМ)»**

(назва дисципліни)

на тему:  **.**

Студента(ки) 3 курсу 303 групи

спеціальності «Кібербезпека»

Тарасенко Ярослав Юрійович

(прізвище та ініціали)

Керівник

К.т.н. доцент

(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 – 2019 рік

**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 5

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

Завдання

На курсову роботу студента

Тарасенка Ярослава Юрійовича

1. Тема курсової роботи: проектування кооперативної мережі
2. Термін здачі студентом закінченої роботи 18.12.2019
3. Вхідні дані до (роботи) інформаційно-аналітичні інтернет джерела, зразки рішень практичних завдань та задач, нормативно-правова база, щодо оформлення технічної документації програмних продуктів, початкові значення для обробки.
4. Зміст пояснювальної записки (перелік питань, які належить розробити). Вступ. Формулювання вимог до програми. Проектування та практична реалізація розв’язку поставленої задачі. Тестування і результати виконання. Висновки.
5. Перелік графічного матеріалу (з точним зазначенням обов`язкових креслень) Таблиці та схеми представлено в роботі. Презентація додається.
6. Дата видачі завдання « 10 » жовтня 2019

**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**

[АНОТАЦІЯ 3](#_Toc60049933)

[ВСТУП 5](#_Toc60049934)

[РОЗДІЛ 1. Аналіз технічної складової 6](#_Toc60049935)

[6.1. Аналіз сучасних технологій локальних та глобальних мереж 6](#_Toc60049936)

[3.3 Кабельні системи 9](#_Toc60049937)

[3.3 Основні компоненти локальної мережі 14](#_Toc60049938)

[1.4 Розрахунок адресного простору 15](#_Toc60049939)

[1.5 Розподіл адрес для мережі центрального офісу (LAN1) 18](#_Toc60049940)

[1.6 Розподіл адрес для мережі офісу з віддаленим доступом (LAN2) 19](#_Toc60049941)

[РОЗДІЛ 2 Конфігурування мережевого обладнання 27](#_Toc60049942)

[2.1 Конфігурування базових функцій мережевого обладнання 27](#_Toc60049943)

[2.2 Проєктуввання віртуальних мереж (VLAN) 30](#_Toc60049944)

[РОЗДІЛ 3 Налаштування безпеки та віддаленого доступу на активне обладнання 32](#_Toc60049945)

[3.1 Налаштування захисту та додаткових функцій маршрутизаторів 32](#_Toc60049946)

[3.2 Налаштування віддаленого доступу до активного обладнання 34](#_Toc60049947)

[3.3 Тестування роботи розробленої межі 35](#_Toc60049948)

[Висновки 38](#_Toc60049949)

[Список використаних джерел 39](#_Toc60049950)

[ДОДАТОК А 41](#_Toc60049951)

[ДОДАТОК Б 45](#_Toc60049952)

**ВСТУП**

На сьогоднішній день цифрові технології присутні у кожному будинку, офісі та інших інфраструктурах. Актуальність використання технологій цифрової передачі інформації беззаперечно є важливою складовою безпечного та комфортного життя, що потребує захисту. Адже для кожного конфіденційність та цілісність інформації може стояти на пріоритетному рівні.

Кожен вид обладнання володіє свої рівнем безпеки, який встановлюється вповноваженим членом організації. В його обов’язки входить забезпечення максимально оптимізованого під потреби організації захисту цього обладнання та інформації відповідно. А також забезпечення безперебійного функціонування системи.

Захист обладнання та інформації забезпечує мінімізацію можливості втрати цілісності даних від втручання посторонніх втручань в системи захисту та баз даних.

Для організації як збій в роботі обладнання так і постороннє втручання може привести до великих фінансових збитків через втрату роботоспроможності, навіть на короткий період часу.

**РОЗДІЛ 1. Аналіз технічної складової**

* 1. **Аналіз сучасних технологій локальних та глобальних мереж**

Маршрутизація (routіng) є однією з ключових функцій мережного рівня. При цьому під маршрутизацією розуміється, перш за все, процес визначення в телекомунікаційній мережі одного або множини шляхів (маршрутів), оптимальних у рамках обраних критеріїв, між заданою парою або множиною мережних вузлів. Таким чином, шлях — це послідовність мережних вузлів і трактів передачі, які з’єднують задану пару вузлів мережі[1].

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

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

На сьогодні на практиці паралельно функціонує у різних мережних технологіях ціла низка різноманітних за своїми функціональними можливостями протоколів маршрутизації. У мережах ІP успішно застосовуються протоколи RIP (Routing Information Protocol), IGRP (Internet Gateway Routing Protocol), Enhanced IGRP, OSPF (Open Shortest Path First), IS-IS (Intermediate System-to-Intermediate System), BGP (Border Gateway Protocol) та EGP (Exterior Gateway Protocol). У технології ATM підтримуються протоколи IISP (Interim Inter-Switch Protocol) і PNNI (Private Network — Network Interface).

Локальна комп’ютерна мережа – це спосіб комунікації між двома і більше комп’ютерами, серверами, маршрутизаторми та іншим мережевим обладнанням в межах локальної мережі.

Локальні мережі можуть бути побудовані за типами топологій. Поняття топології відноситься, перш за все до локальних мереж, в яких структуру зв’язків можна прослідковувати. У глобальних мережах структура зв’язків прихована від користувачів і може змінюватись з часом.

Існують три базові топології локальних мереж:

Шина (Bus) – всі комп’ютери підключаються до однієї спільної лінії зв’язку;

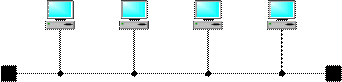


Рисунок 1 Топологія «шина»

Зірка (Star) – до одного центрального комп’ютера приєднуються інші комп’ютери, які використовують свою лінію зв’язку;

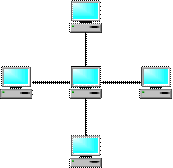


Рисунок 2 Топологія «зірка»

Кільце (Ring) – комп’ютери послідовно об’єднуються в «кільце»: кожен з них отримує дані після того як їх отримає попередній сегмент мережі.

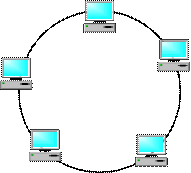


Рисунок 3 Топологія «кільце»

Усі топології можуть комбінуватись та розширюватись у різних варіантах, утворюючи більш складні топології.

Базові топології є основою для створення інших більш складних топологій.

В результаті комбінації декількох «зіркових» мереж утворюється топологія «дерево» (tree), як у даному випадку:

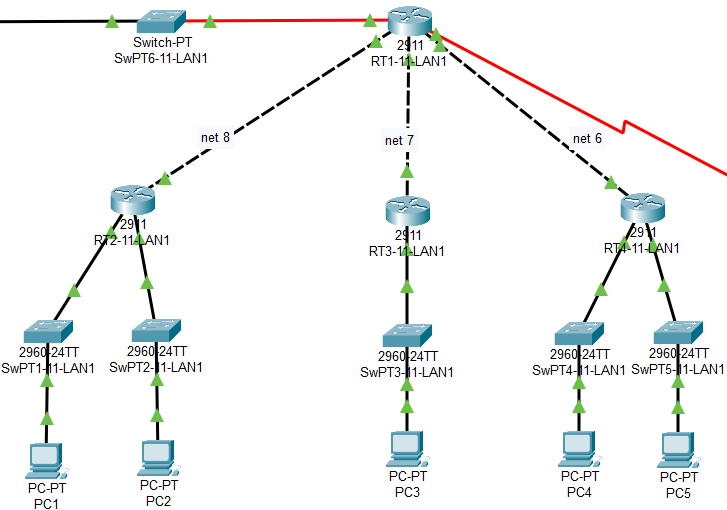


Рисунок 4 Топологія «дерево»

Ця топологія є досить поширеною, в якій підмережі з топологією «шина» підключаються до спільного центрального вузла.

У випадку об’єднання центральних вузлів у кільце утворюється зірково-кілцева (Star-Ring) топологія, що використовується як показано на даному рисунку

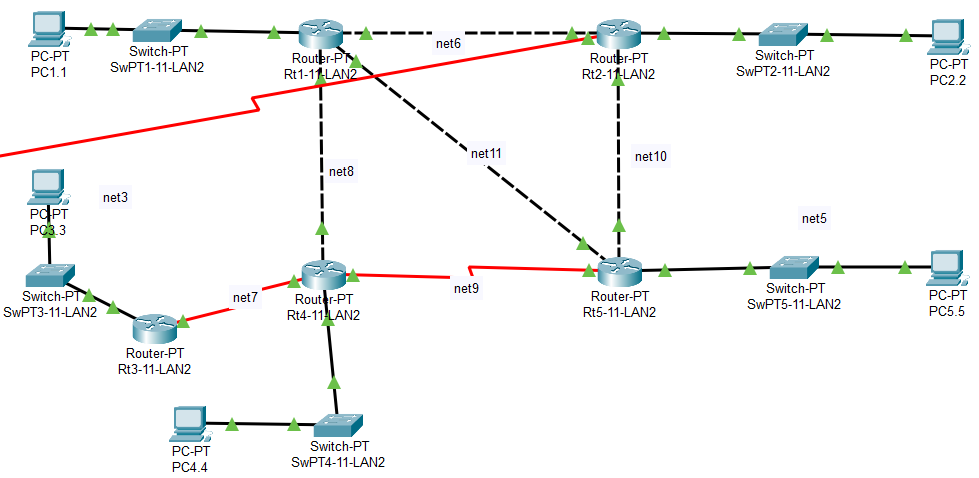


Рисунок 5 Топологія «зірка-кільце»

Розгорнуту топологію, відповідно до наданих рисунків можна побачити та ознайомитися з нею в додатку Б

* 1. **Кабельні системи**

Кабельна система – фізичний інструмент передачі даних, побудований на базі кабельних ліній зв’язку.

Основнимі типи кабелів:

Вита пара;

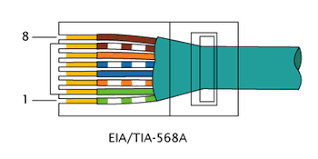


Рисунок 6 «Вита пара»

Існує два стандарти обжиму восьмижильної витої пари:

- Г568А;

- Г568В;

Вита пара з восьми жил використовується для глобальних мереж. Якщо планується передача на 100мбіт/с, достатньо буде і чотирьох жил. Перехресний обжим кабеля використовується для підключення типу «роутер-роутер», «свіч-свіч», та «комп’ютер-комп’ютер». Для підключення типу «роутер-роутер» прийнято використовувати «рос-оверний» обжим витої пари, але при використанні інтелектуальних вузлів, дане обмеження може бути необов’язкове, оскільки роутери здатні визначити тип підключення.

Підключення типу «ПК-ПК» не може бути з’єднане витою парою з прямим обжимом. В такому випадку допускається підключення тільки «крос-овером». Аналогічно і з підключенням типу «свіч-свіч».

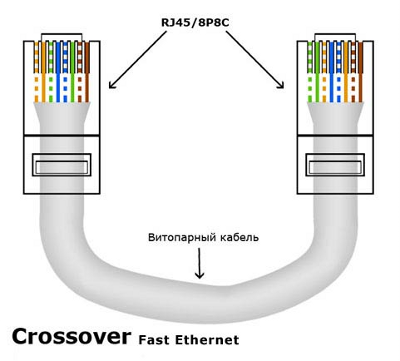


Рисунок 7 «Перехресний обжим витої пари для швидкості 100мбіт/с»

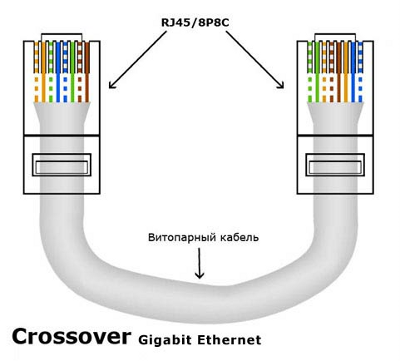


Рисунок 8 «Перехресний обжим витої пари для шидкості 1000мбіт/с»

Відповідно для підключення типу «ПК-роутер», можна використовувати прямий обжим витої пари, як показано на рисунку нижче.

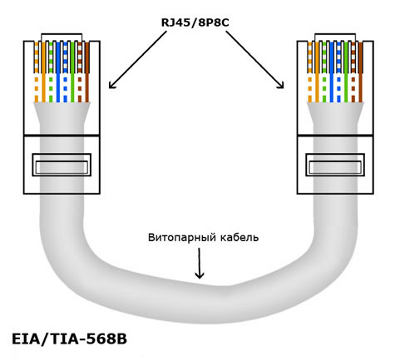


Рисунок 9 «Прямий обжим витої пари»

Волоконно-оптичні кабелі;

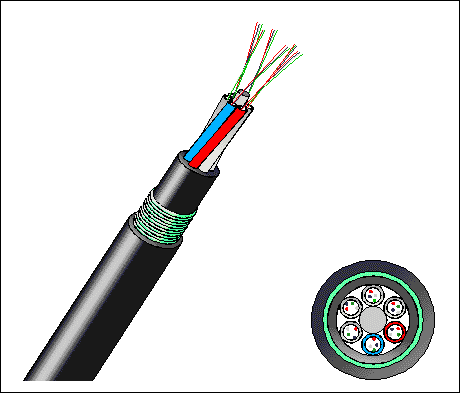


Рисунок 10 «Волоконно-оптичний кабель»

Оптоволоконний кабель складається з одного, або кількох, світловодів (оптичних волокон), що розміщуються у спільній захисній оболонці. Кожний світловод складається з центрального провідника (серцевини), який має високий показник переломлення світла, і скляної оболонки, яка має низький показник переломлення світла.

Перевагами оптоволоконного кабеля є:

- Висока перешкодозахищеність;

- Невисоке затухання кабелів;

- Висока швидкість розповюдження сигналів;

- Недоліки даного кабелю:

- Складність монтажу

Чутливість до температурних перепадів, що призводять до утворення тріщин.

Коаксіальні кабелі;



Рисунок 11 «Коаксіальний кабель»

Коаксіальний кабель представляє собою електричний кабель, що складається з центрального мідного провідника і металевої оплітки (екрану), розділених шаром діелектрика і поміщених у зовнішню ізолюючу оболонку. Металева оплітка відіграє подвійну роль – служить для передачі даних та захищає центральний провід від зовнішніх пошкоджень.

Для побудови ком’ютерних мереж використовують:

Товстий коаксіальний кабель з діаметром центрального провідника 2,17 мм і зовнішнім лдіаметром близько 1 см.

Тонкий коаксіальний кабель з діаметром центрального провідника 0,89 мм і зовнішнім діаметром близько 0,5 см.

* 1. **Основні компоненти локальної мережі**

Маршрутизатор або роутер – мережевий пристрій, що пересилає пакети даних між комп'ютерними мережами. Маршрутизатори виконують функції керування трафіком в Інтернеті. Пакет даних, як правило, пересилається з одного пристрою на інший як в одній локальній мережі, так і з одної мережі в іншу, які складають мережу Інтернет, доки він не досягне свого кінцевого вузла. Маршрутизатор підключається до двох, або більше, ліній зв’язку з різних мереж. Коли пакет даних надходить на маршрутизатор, він зчитує інформацію про ІР-адресу в пакеті, щоб визначити кінцевий пункт призначення. Потім, використовуючи інформацію у таблиці маршрутизації, або політику маршрутизації, направляє пакет до наступної мережі[2].

Такі маршрутизатори як показано на рисунку 2.1 здебільшого використовуюсться для корпоративних мереж. Для звичайних користувачів найбільш знайомими роутерами є невеликі, які виконують маршрутизацію між домашніми комп’ютерами та інтернетом.

Прикладом може виступати звичайний роутер компанії «TP-link».



Рисунок 12 «Маршрутизатори»

Комутатор або свіч – багатопортовий комунікаційний пристрій, який дозволяє об’єднувати кілька сегментів в одну мережу, забезпечуючи її високу продуктивність і пропускну здатність. Дозволяє підвищити швидкодію та продуктивність передачі даних в мережі. Комутатор дозволяє розділити мережу на кілька підмереж для збільшення радіусу мережі та зниження навантаження.



Рисунок 13 «Комутатор»

**1.4 Розрахунок адресного простору**

При об’єднанні в мережу трьох або більше вузлів виникає необхідність в ідентифікації кожного вузла, точніше – їх мережевих інтерфейсів, на основі певної схеми адресації. Адреси можуть використовуватись для ідентифікації не тільки окремих інтерфейсів, але й їх груп. За допомогою таких групових адрес дані можуть адресуватись відразу кільком вузлам. Окремим випадком групових адрес є широкомовні адреси – направлені за ними дані доставляються всім вузлам мережі.

Локальна, або апаратна адреса – це адреса канального рівня, яка використовується засобами базової мережевої технології для доставки даних в межах підмережі складеної мережі (інтермережі). Якщо підмережею інтермережі є локальна мережа, то локальна адреса – це МАС-адреса. Проте до складу інтермережі можуть входити також підмережі, що використовують технології глобальних мереж (Х.25, АТМ та інші). В цьому випадку локальними адресами будуть відповідні адреси цих технологій. МАС-адреса – унікальний ідентифікатор мережевого інтерфейсу в локальній мережі, що зафіксований в його апаратурі.

Мережева адреса, або ІР-адреса – це логічна адреса мережевого рівня, яка використовується в якості ідентифікатора вузла складеної мережі 100 (інтермережі). Протокол Ірv4 виділяє на ІР-адресу двійкове число довжиною 8 байтів (32 біти). Відповідно, протокол Ірv6 виділяє 16 байтів (128 бітів) і це найсуттєвіша різниця між Ipv4 та Ipv6. Двійкова нотація Ір-адреси не зручна для використання. Тому ІР-адреса записується в десятковій, або шістнадцятковій, системі числення. Наприклад, 32-біти для протоколу ІРv4 розбиваються на чотири октети (по 8 бітів), кожен з яких перетворюється в десяткове число (в діапазоні 0-255) і відділяється від інших крапкою, як показано на рисунку 2.3.

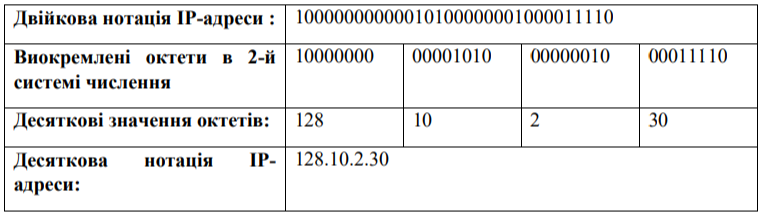


Рисунок 1.2.1 «Переведення двыйкової нотації IP-адреси в десяткову»

На даний час широко використовується гнучкий, спосіб визначення границі між номерами мережі і вузла – на основі маски підмережі. Згідно з визначенням, даним в RFC 950: Маска адреси, або маска підмережі – це 32-бітне число, що використовується для розрізнення номера мережі і номера вузла в IP-адресі, біти якої задаються так: − всі біти, що відповідають номеру мережі, встановлюються в 1. − всі біти, що відповідають номеру хосту, встановлюються в 0. Іншими словами, маска адреси – це двійкове число, яке використовується в парі з IP-адресою і має таку ж довжину. Маска адреси містить неперервну послідовність одиниць в тих розрядах, які позначають номер мережі, і неперервну послідовність нулів в тих розрядах, які позначають номер вузла. Маска «маскує» частину IP-адреси, яка використовується для отримання номера мережі[3].

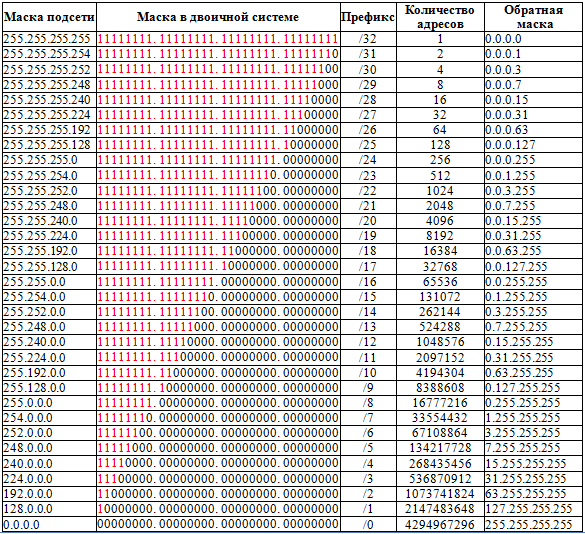


Рисунок 1.2.2 «Таблиця масок адрес для класів»

Крім двійкової нотації для представлення масок також використовуються:

− точково-десяткова нотація – використовує перетворення 32-бітного значення маски в точково-десяткову форму,

− шістнадцятирічна нотація – значення кожного октету 32-бітного значення маски записується у вигляді 16-кового числа,

− у вигляді префіксу адреси – вказується число бітів номера мережі в 32- бітному значенні маски; це число записується у вигляді / і називається префіксом адреси (мережі).

**1.5 Розподіл адрес для мережі центрального офісу (LAN1)**

Згідно із вихідними даними для проєктування мережі центрального офісу було надано таку IP-адресу: «172.19.11.0». Для офісу було встановлено п’ять підмереж: «Net1, Net2 Net3, Net4 Net5, » у яких виділено 28, 25, 70, 5, та 9 хостів відповідно. Для прикладу наведу першу підмережу

Отже, для першої мережі було взято маску «255.255.255.224», оскільки вона може включати в собі простір для тридцятидвох хостів. З них задіяно підмережею 28, адреса із номером «172.19.11.31» є широкомовною. Дві адреси з цієї підмережі залишаються незадіяними, для того щоб можна було розширити підмережу у випадку потреби.

Розподіл IP-адрес інших підмереж наведений у таблиці:

Таблиця 1

Розподіл IP-адрес та масок ПК-роутер в мережі LAN1

|  |  |  |  |
| --- | --- | --- | --- |
| Мережа | IP-мереж | IP-хостів | Широкомовна адреса |
| NET1 | 172.19.11.0/27 | 172.19.11.1-172.19.11.30 | 172.19.11.31 |
| NET2 | 172.19.11.32/27 | 172.19.11.33-172.19.11.62 | 172.19.11.63 |
| NET3 | 172.19.11.64/25 | 172.19.11.65-172.19.11.126 | 172.19.11.127 |
| NET4 | 172.19.11.128/28 | 172.19.11.129-172.19.11.142 | 172.19.11.143 |
| NET5 | 172.19.11.144/28 | 172.19.11.145-172.19.11.158 | 172.19.11.159 |

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 192.19.11.1 згідно таблиці 1.1), а крайня найбільша – порту маршрутизатора, що з’єднує його з комп’ютером (Rt2 має адресу 192.19.11.30). Алгоритм застосовується до всіх п’яти підмереж.

Для того, щоб налаштувати роботу маршрутизації потрібно розширити адресний простір і надати адреси для кожного звичайного маршрутизатора та шлюзового маршрутизатора (Rt1) . Шлюзовий маршрутизатор – апаратний маршрутизатор або програмне забезпечення для сполучення комп'ютерних мереж, що використовують різні протоколи.

На кожний логічний інтерфейс між маршрутизаторами була встановлена маска (255.255.255.252) та 2 хости для оптимальної роботи. Також була розроблена додаткова таблиця «Таблиця 1.2» розподілу адрес.

Таблиця 2

Розподіл IP-адрес та масок роутер-роутер в мережі LAN1

|  |  |  |  |
| --- | --- | --- | --- |
| Мережа | IP-мереж | IP-хостів | Широкомовна адреса |
| NET6 | 172.19.11.160/30 | 172.19.11.161-172.19.11.162 | 172.19.11.163 |
| NET7 | 172.19.11.164/30 | 172.19.11.165-172.19.11.166 | 172.19.11.167 |
| NET8 | 172.19.11.168/30 | 172.19.11.169-172.19.11.170 | 172.19.11.171 |
| NET9 | 172.19.11.172/30 | 172.19.11.173-172.19.11.174 | 172.19.11.175 |

Розподіл адрес для інтерфейсів між маршрутизаторами проходив аналогічно до розподілу адрес для підмереж

**1.6 Розподіл адрес для мережі офісу з віддаленим доступом (LAN2)**

Організація мережі LAN2 відбувався за схемою на рисунку 14, мережу в налаштованому вигляді подано в додатку Б.

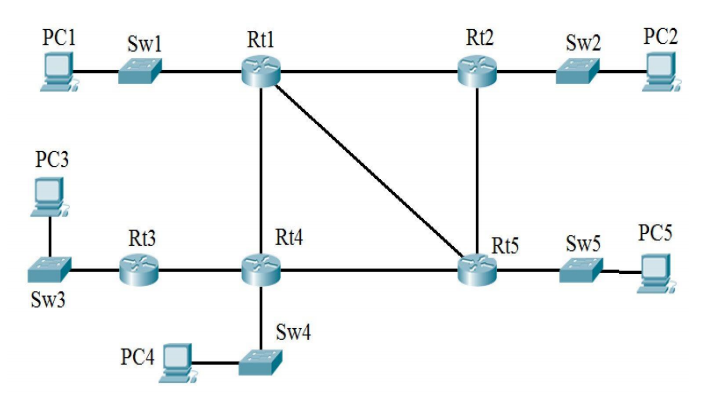


Рисунок 14 «Структурна схема LAN2»

Усі маршрутизатори підключені послідовно 100мбітним та гігабітним кабелем «RJ-45», окрім Rt3, Rt4 та Rt5, вони підключені «Serial» кабелем. Для цієї мережі розподіл IP-адрес полягав в оптимальному виділенні хостів на кожен інтерфейс між роутерами а також розподілу їх між кінцевими пристроями. З’єднання ПК-роутер мають адреси та маски відповідно до наведеної таблиці:

Таблиця 3

Розподіл IP-адрес ПК-роутер в мережі LAN2

|  |  |  |  |
| --- | --- | --- | --- |
| Мережа | IP-адреса | IP-хостів | Широкомовна адреса |
| NET1 | 192.168.11.0/26 | 192.168.11.1-192.168.11.62 | 192.168.11.63 |
| NET2 | 192.168.11.64/29 | 192.168.11.65-192.168.11.70 | 192.168.11.71 |
| NET3 | 192.168.11.72/28 | 192.168.11.73-192.168.11.85 | 192.168.11.87 |
| NET4 | 192.168.11.88/28 | 192.168.11.89-192.168.11.102 | 192.168.11.103 |
| NET5 | 192.168.11.104/29 | 192.168.11.105-192.168.11.110 | 192.168.11.111 |

Кожне з’єднання роутер-роутер має по 2 хости та адреси відповідно таблиці 1.2.2.2:

Таблиця 4

Розподіл IP-адрес роутер-роутер в мережі LAN2

|  |  |  |  |
| --- | --- | --- | --- |
| Мережа | IP-адреси | IP-хостів | Широкомовна адреса |
| NET6 | 192.168.11.112/30 | 192.168.11.113-192.168.11.114 | 192.168.11.115 |
| NET7 | 192.168.11.116/30 | 192.168.11.117-192.168.11.118 | 192.168.11.119 |
| NET8 | 192.168.11.120/30 | 192.168.11.121-192.168.11.122 | 192.168.11.123 |
| NET9 | 192.168.11.124/30 | 192.168.11.125-192.168.11.126 | 192.168.11.127 |
| NET10 | 192.168.11.128/30 | 192.168.11.129-192.168.11.130 | 192.168.11.131 |
| NET11 | 192.168.11.132/30 | 192.168.11.133-192.168.11.134 | 192.168.11.135 |

Розподіл адрес для мережі дата-центру (LAN3)

Мережа віддаленого дата-центру була розроблена з 3 підмереж згідно з технічним завданням (одна підмережа – з’єднання двох серверів з маршрутизатором). Для трьох основних підмереж в технічному завданні були прописані адреси (214.2387.0, 181.218.0.0, 223.10.78.0 відповідно).

Для підмереж, які складаються із двох серверів кожна, було виділено по два хости для кожної підмережі.

Таблиця 5

Розподіл адрес мережі дата-центру

|  |  |  |  |
| --- | --- | --- | --- |
| Мережа | IP-мереж | IP-хостів | Широкомовниа адреса |
| NET1 | 214.23.87.0/28 | 214.23.87.1-214.23.87.14 | 214.23.87.15 |
| NET2 | 181.218.0.0/28 | 181.218.0.1-181.218.0.14 | 181.218.0.15 |
| NET3 | 223.10.78.0/28 | 223.10.78.1-223.10.78.14 | 223.10.78.15 |

Вибір та налаштування способу маршрутизації

Як відомо маршрутизація – це процес визначення шляху проходження пакетів даних з однієї точки в іншу. Мається на увазі, що пакет із данимивідправляється із початкового пристрою і передається наступному в мережі. Наступний пристрій приймає ці дані, зчитує адресу отримувача і проводитьь сканування на наявність цієї адреси в найближчому доступі.

Якщо такий пристрій із заданою адресою знаходиться йому надходить запит на відправку даних. Кінцевий пристрій приймає дані. Після цього процедура повторюється заново, але у зворотньому порядку для коректної роботи комунікацій[4].

У тому випадку, якщо після відправки даних наступний пристрій не знаходить адресата, він передає ці дані наступному пристрою, але попутно модифікує адресу відправника для того щоб наступний сегмент зміг пропустити ці дані далі у мережу. Далі процес проходить ідентично.

Зауважу, що що основні принципи маршрутизації є спільними для всіх видів комутації.

Розрізняють централізовані та децентралізовані (розподілені) способи маршрутизації. У випадку централізованого способу маршрутизація здійснюється одним центром керування (менеджером мережі), який визначає напрямок руху пакетів через мережу передачі даних. Вузли комутації даної мережі беруть мінімальну участь у маршрутизації і прості за струк­турою. При збільшенні числа вузлів зростає складність організації централізованого керу­вання мережі передачі даних. Суттєвим недоліком централізованого керування є пряма залежність якості маршрутизації від надійності її менеджера, яка із збільшенням складності останнього має тенденцію до зниження. Крім того, менеджер мережі повинен мати опера­тивну інформацію про стан мережі, тому що вихід з ладу вузла або його перевантаження може спричинити втрату працездатності всієї мережі.

Розрізняють просту і табличну маршрутизацію. Проста маршрутизація реалізується без урахування топології і завантаження мережі передачі даних і, як правило, відрізняється низькою ефективністю. При табличній маршрутизації в кожному вузлі комутації формується спеціальна таблиця маршрутів, яка вказує, яким шляхом повинен передаватися пакет із заданою адресою, щоб у найкоротший термін досягти одержувача.

Табличні методи маршрутизації залежно;від моменту формування таблиць маршрутів, поділяють на статичні і динамічні. За статичної маршрутизації таблиці маршрутів формуються під час генерації мережі і після цього, як правило, не змінюються. І тільки при зміні конфігурації мережі, наприклад, у разі виходу якогось вузла з ладу, здійснюється коригування маршрутів.

До статичних способів відносяться маршрутизація фіксована і маршрутизація способом найкоротшої черги. При фіксованій маршрутизації для будь-якої пари абонентських систем установлюються одиничний або груповий канали передачі даних. У першому випадку йдеться про одношляхову маршрутизацію, тому що існує тільки один маршрут проходження пакетів від відправника до одержувача. Це найпростіший спосіб маршрутизації, проте він не враховує можливі аварійні ситуації і реальне завантаження окремих каналів, що може призвести до перевантаження окремих ділянок мережі при недовантаженні її в цілому. З метою вирівнювання навантаження на основних (магістральних) каналах передачі даних використовують багатошляхову маршрутизацію, коли між суміжними вузлами комутації утворюється група віртуальних каналів, кожний з яких може призначатися тому або іншому шляху проходження пакетів. Маршрутизація способом найкоротшої черги передбачає наявність для кожного вузла комутації таблиці маршрутів з зазначенням декількох варіантів напрямку прямування пакетів, при цьому вибір конкретного шляху здійснюється випадковим чином. Оскільки такий спосіб характеризується відносно низькою ефективністю, то в такому варіанті він використовується доволі рідко. Для підвищення ефективності такого способу маршрутизації встановлюють пріоритети напрямків передачі даних. Потім, у виборі каналу передачі, вузол ко­мутації переглядає в порядку зменшення пріоритету перелік допустимих шляхів передачі і вибирає перший вільний канал, який забезпечує найбільш оптимальний шлях прямування пакета з мінімальною затримкою його в проміжних вузлах. Завдяки відносній простоті і до­статній ефективності спосіб часто використовується в мережах комутації пакетів, зокрема у мережах з низькою надійністю комутаційних систем.

Найбільш ефективними, але і, мабуть, найскладнішими є способи динамічної маршрутизації. При динамічній маршрутизації вміст таблиць маршрутів змінюється залежно від стану і завантаження каналів передачі даних і вузлів комутації. Для адаптації до зміни навантаження кожний вузол комутації повинен мати певну інформацію про стан мережі передачі даних і в першу чергу про її топологію, інтенсивність потоків даних і затримки (черги) у вузлах комутації. Ця інформація відстежується (збирається) спеціальними керуючими пакетами, що ними обмінюються вузли комутації. Якість маршрутизації значною мірою залежить від оперативності відновлення керуючої інформації. Загалом, найбільш оптимальна маршрутизація досягається наявністю інформації про миттєвий стан мережі та її завантаження. Проте це, зазвичай, призводить до значного збільшення потоку керуючих пакетів у мережі передачі даних і до зниження її ефективності.

Для коректної передачі даних в мережах було використано статичну маршрутизацію. Прикладом може виступати інтерфейс настроювання статичної маршрутизації

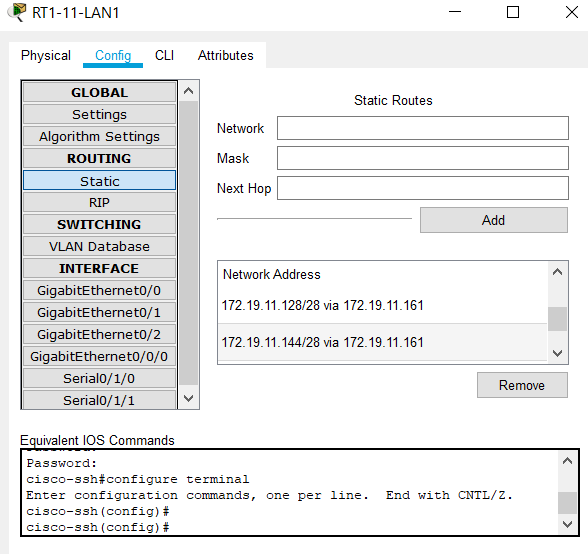


Рисунок 15 «Інтерфейс налаштування статичної маршрутизації»

Більш детально із налаштуваннями можна ознайомитись у додатку Б.

Для того щоб налаштувати статичну маршрутизацію у вікні графічного інтерфейсу маршрутизатора потрібно вказати три параметри:

Мережа (мережа в яку Ви хочете маршрутизувати дані)

Маска (маска цієї мережі)

Наступний стрибок (IP-адреса логічного інтерфейсу пристрою, який іде наступним в передачі даних у мережі до пункту призначення)

На поданому вище рисунку зазначений шлюзовий маршрутизатор. Саме цей роутер приймає усі дані про передачу інформації в межах мережі та поза нею. Відповідно на цьому маршрутизаторі потрібно вказати усі можливі напрямки передачі пакетів даних.

На усіх інших маршрутизаторах необхідно вказати цей маршрутизатор як пункт призначення, для того щоб усі дані надходили спочатку до нього, а після до мереж та підмереж призначення.

Тому в кожній мережі усієї топології налаштування шлюзових маршрутизаторів аналогічне.

**РОЗДІЛ 2 Конфігурування мережевого обладнання**

**2.1 Конфігурування базових функцій мережевого обладнання**

В мережі LAN1 використовувались маршрутизатори «Cisco 2960» . Ці маршрутизатори, як і маршрутизатори «Cisco switchPT», які використовувались у мережі LAN2, мають непогані характеристики пропускної здатності та достатню кількість портів і слотів, у які можна додатково вставити порти в умовах емулятора Cisco Packet Tracer.

Але оскільки комутатор «Cisco switchPT» можна використовувати лише в умовах емуляції, рекомендувати його для повсякденного використання в робочих умах не рекомендується.

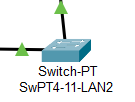


Рисунок 16 «Комутатор Csico SwitchPT»



Рисунок 17 «Комутатор Cisco 2960»

Зазвичай комутатори не потребують конкретних налаштувань, але у деяких випадках потребується розділяти порти на групи для більшу зручної комутації.

Аналогічно до комутаторів були підібрані маршрутизатори. Для маршрутизації в мережі LAN2 або віддаленого офісу був використаний протокол EIGRP[5].

EIGRP – покращений протокол маршрутизації внутрішніх шлюзів – вдосконалений протокол динамічної маршрутизації, який використовується для рішень маршрутизації та конфігурації на маршрутизаторах. EIGRP був розроблений Cisco Systems як фірмовий протокол, який можна використовувати лише на маршрутизаторах Cisco, але в 2013 році часткова функціональність EIGRP була перетворена на відкритий стандарт. EIGRP надсилає лише поступові оновлення, зменшуючи навантаження на маршрутизаторі та кількість даних, які потрібно передати. Розуміння основ протоколу маршрутизації EIGRP дуже важливо перед налаштуванням протоколу у виробничому середовищі. Програмний код налаштування протоколу EIGRP виглядає так:

R3(config)#ip route 0.0.0.0 0.0.0.0 192.168.34.4

Перевірити цей протокол на маршрутизаторі можна за допомогою комнди «show ip route», або поивитись перелік налаштованих протоколів у ддодатку Б на кожному шлюзовому маршрутизаторі.

R3#show ip route

Codes: L – local, C – connected, S – static, R – RIP, M – mobile, B – BGP

D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area

N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2

E1 – OSPF external type 1, E2 – OSPF external type 2

I – IS-IS, su – IS-IS summary, L1 – IS-IS level-1, L2 – IS-IS level-2

ia – IS-IS inter area, \* - candidate default, U – per-user static route

o – ODR, P – periodic downloaded static route, H – NHRP, l – LISP

a – application route

+ - replicated route, % - next hop override

Gateway of last resort is 192.168.34.4 to network 0.0.0.0

S\* 0.0.0.0/0 [1/0] via 192.168.34.4

D 192.168.12.0/24

[90/28416] via 192.168.23.2, 00:59:18, GigabitEthernet0/0/1

192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.23.0/24 is directly connected, GigabitEthernet0/0/1

L 192.168.23.3/32 is directly connected, GigabitEthernet0/0/1

192.168.34.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.34.0/24 is directly connected, Serial0/2/0

L 192.168.34.3/32 is directly connected, Serial0/2/0



Рисунок 18 «Маршрутизатор Cisco 2911»

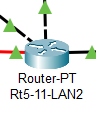


Рисунок 19 «Маршрутизатор Cisco RouterPT»

**2.2 Проєктуввання віртуальних мереж (VLAN)**

При правильному налаштуванні віртуальні локальні мережі можуть покращити загальну продуктивність зайнятих мереж. VLAN призначені для групування клієнтських пристроїв, які спілкуються один з одним найчастіше. Трафік між пристроями, розділеними на дві або більше фізичних мереж, як правило, повинен оброблятися основними маршрутизаторами мережі, але за допомогою VLAN, щоб трафік мав ефективніше обробляти мережеві комутатори.

VLAN також приносять додаткові переваги безпеці у великих мережах, дозволяючи краще контролювати, які пристрої мають локальний доступ один до одного. Гостьові мережі Wi-Fi часто реалізуються за допомогою бездротових точок доступу, що підтримують VLAN.

Для автоматичного обміну інформацією про VLAN через транкові порти потрібно налаштувати Cisco VLAN Trunk Protocol (VTP), який дозволяє комутаторам посилати інформацію про VLAN у формі «реклами» сусіднім пристроям. Транковий порт – це порт або група портів, що використовуються для передачі інформації про VLAN в інші мережеві пристрої, що приєднані до цього порту і використовують транковий протокол. Транковий протокол це «мова», яку комутатори використовують для обміну інформацією про VLAN. Приклади транкових протоколів – ISL і IEEE 802.1q. Звичайні порти не рекламують інформацію про VLAN, але будь-який порт може бути настроєний для прийому/передачі інформації про VLAN. Тому необхідно активізувати транковий протокол на потрібних портах, оскільки він вимкнений за замовчуванням. Транковий порт – це порт, призначений виключно для пересилки VLAN інформації використовуючи транковий протокол. Cisco комутатори, в основному, використовують протокол Inter-switch Link (ISL) для забезпечення сумісності інформації

Налаштування такого типу були використанні в мережі LAN3 або датацентру. Використовувалися конкретні порти на серверах та комутаторах [6].

**РОЗДІЛ 3 Налаштування безпеки та віддаленого доступу на активне обладнання**

**3.1 Налаштування захисту та додаткових функцій маршрутизаторів**

На маршрутизаторах в мережі центрального офісу був налаштований протокол статичного налаштування розподілу адрес. Такий розподіл дозволяє адміністраторам власноруч встановлювати адреси на кожному пристрої. Це надає зручності при розширенні підмереж, коли, наприклад в офісі для підключення нового співробітника потрібно створити його робоче місце та підключити його до локальної мережі. Мінусом даного споссобу може стати незручність налаштування самого протоколу, адже адміністратору доводится підключати кожного співробітника вручну. Також мінусом може бути збільшення кількості помилок в системі розподілу адрес зі збільшенням кількості кінцевих пристроїв та навантаження їх на мережу.

Як уже було описано в емуляторі Cisco Packet Tracer налаштувати статичну адресацію можна через графічну консоль у кожному пристрої програми. На практиці ж усі команди щодо налаштування потрібно вводити вручну в командній стрічці маршрутизатора або комп’ютера.

Також можна налаштувати протокол динамічної конфігурації вузла – DHCP.

Протокол динамічної конфігурації використовується на другому (канальному) рівні мережевої моделі OSI. Для цього мережевий адміністратор може задати діапазон адрес, які будуть розподілені між комп’ютерами. Це може облегшити роботу адміністраторам та прискорити їх роботу, проте робить неможливим розширенння мережі в тому ж діапазоні, оскільки цей діапазон встановлений із самого початку. Це робить розширення значно складнішим, тому, що для цього потрібно заново налаштовувати протокол DHCP[7].

Налаштування динамічної конфігурації для всіх маршрутизаторів виглядає так:

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

Дані налаштування також можна побачити та ознайомитись у додатку Б.

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.

Для того щоб різні мережі могли між собою комунікувати потрібно налаштувати протокол NAT.

NAT – Трансляція мережевих адрес – це процес, в якому один або кілька приватних IP-адресів перетворюються в один або кілька публічних IP-адрес і навпаки, щоб забезпечити доступ в Інтернет для локальних вузлів.

Крім того, NAT виконує перетворення номерів портів, тобто маскує номер порту хоста іншим номером порту в пакеті, який буде направлений до пункту призначення. При цьому NAT не тільки зберігає пул загальнодоступних IP-адресів, а й приховує схему адресації вашої мережі. Потім він вносить відповідні записи IP-адреси і номера порту в таблицю NAT.

Алгоритм роботи технології полягає в тому, що коли клієнт в мережі відправляє якийсь запит в Інтернет, маршрутизатор пересилає запит спеціального пристрою NAT. Далі він перетворює адресу відправника в загальнодоступну IP-адресу пристрою перед пересиланням запиту в Інтернет і для подальшого отримання інформації з сервера. Коли відповідь отримана від зовнішнього джерела, NAT перетворює загальнодоступну IP-адресу в приватну IP-адресу перед самим пересиланням пакету клієнту. Для цього NAT створює зіставлення між парою PrivateSrcIP, PrivateSrcPort і парою PublicSrcIP, PublicSrcPort, щоб знати напевно, як перетворити IP-адресу  і номер порту призначення. NAT зазвичай працює на маршрутизаторі або міжмережевому екрані.

Кожен маршрутизатор володіє зашифрованим паролем (secret) для уникнення постороннього втручання в роботу систем маршрутизаторів а також для уникнення несанкціонованого доступу до привілейованого режиму на тих самих маршрутизаторах.

**3.2 Налаштування віддаленого доступу до активного обладнання**

SSH («Secure Shell» — безпечна оболонка) – мережевий протокол призначений для управління даними і операційною системою на віддаленому комп'ютері, виконання на ньому команд, також може використовуватися для тунелювання TCP-з'єднань. SSH за допомогою різних алгоритмів шифрування шифрує весь переданий трафік включаючи передані паролі[8]

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.

**3.3 Тестування роботи розробленої межі**

Перевірка роботи мережі може відбуватися шляхом відправки пакетів даних з одного пристрою на інший.

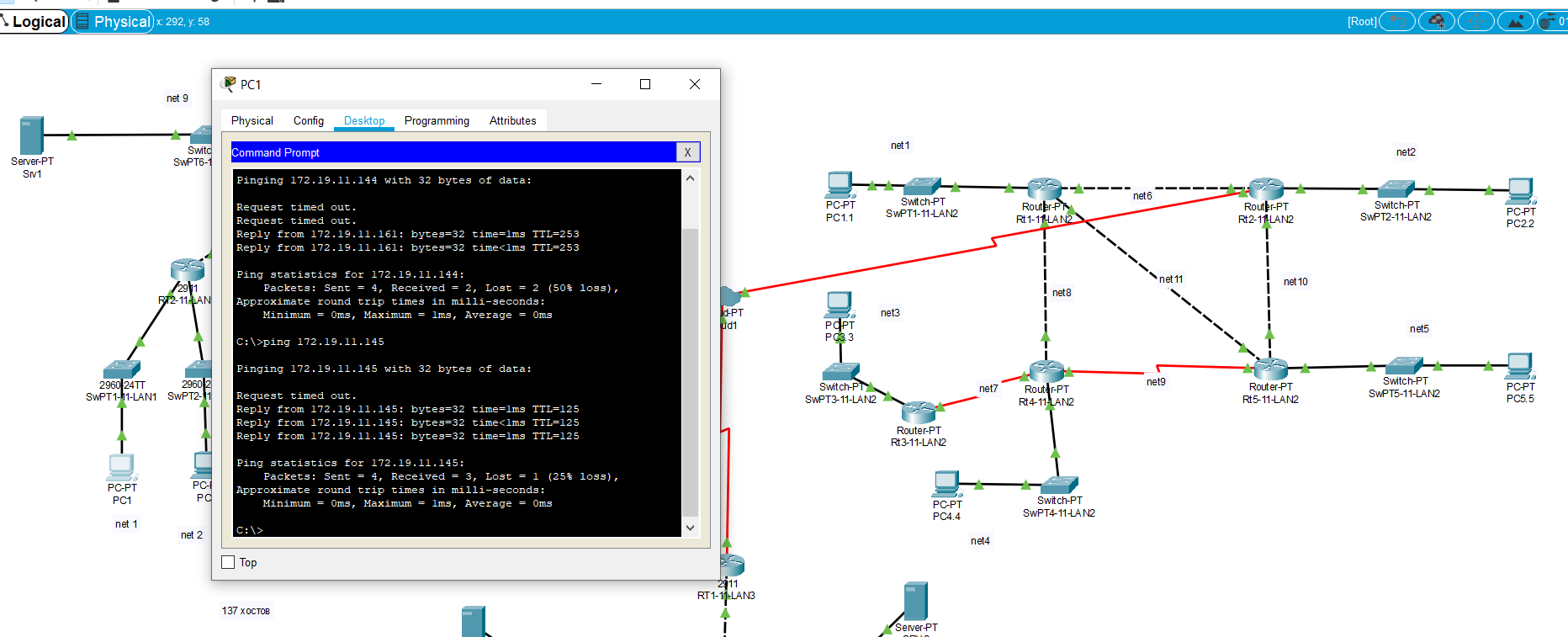


Рисунок 20 «Тестова передача пакетних даних»

Як бачимо передача пройшла успішно. Не дивлячись на те, що не всі пакети дійшли до свого адресата. Така похибкаозначає що навіть якщо не всі пакети дійши до кінця, вони все одно можуть прийти у наступній передачі даних. Тому це не є суттєвою проблемою.

В мережі LAN2 передача даних з одного комп’ютера на інший також проходить успішно, як і в першій мережі.

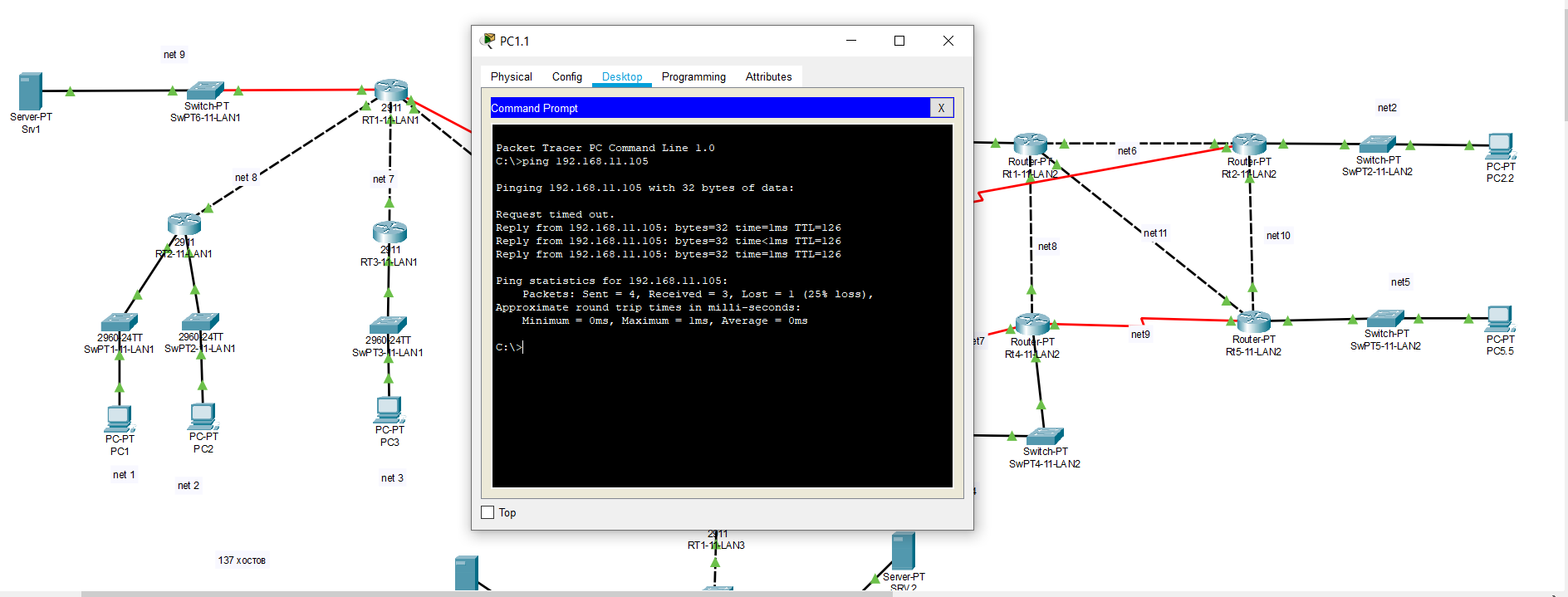


Рисунок 21 «Передача даних в мережі LAN2»

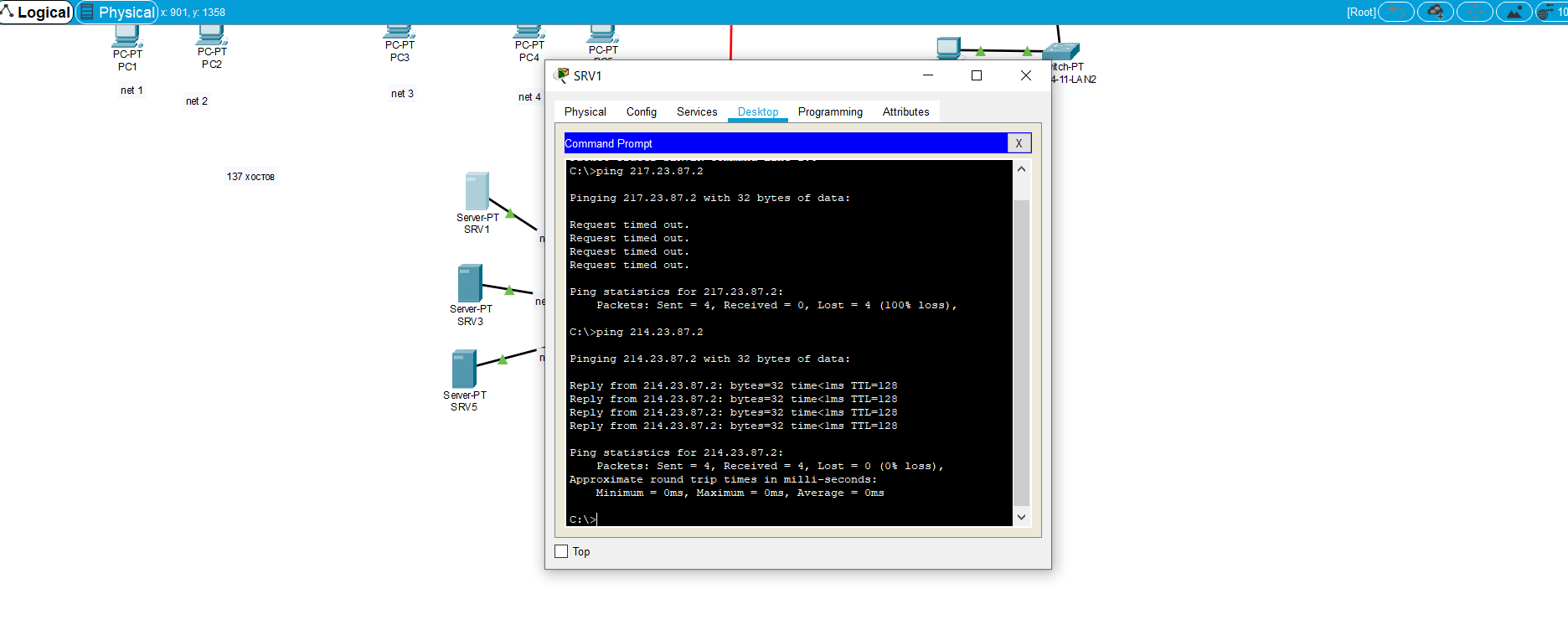


Рисунок 22 «Передача даних з сервера»

Виконання таких маніпуляцій потребує зв’язок між кінцевими пристроями. А отже потребує маршрутизації, яка була налаштована для передачі даних та підключення інших важливих для мережі та безпеки протоколів.

Для передачі даних між мережами був налаштований протокол NAT і PAT у першій мережі та статичний NAT у другій мережі. Нажаль в даному випадку ці протоколи хоч і були налаштовані, але не працюють з невідомих причин, тому вважати цю вимогу виконаною не можна[9]

**Висновки**

У результаті проведеної роботи були змодельовані схеми комп'ютерних мереж, в яких налаштована сумісна робота різних протоколів маршрутизації. Були відмічені особливості налаштувань маршрутизаторів та особливості функціонування таких систем.

Продумування системи маршрутизації даної моделі потребує знань маршрутизації та комутації, які можна отримати у вільному доступі в мережі інтернет або в курсі «Cisco Routing&Switching»[10]

Конкретно в даній роботі використовувалися різні види протоколів, комутації та маршрутизації таких як:

Розподіл IP-адрес;

Налаштування протоколів маршрутизації;

Проєктування мережі;

Налаштування основних протоколів безпечного доступу;

Конфігурування систем комутації;

На даному етапі виконання курсової роботи виконана була більшість вимог, які становлять основну частину завдань для повноцінного функціонування мареж. Завдання яке полягало у маршрутизації між основними мережами було виконано неповністю хоч усі необхідні команди для цього були приведені у виконання.

**Список використаних джерел**

1. Основи ком’ютерних мереж [Електронний ресурс] / 2019. – Режим доступу до ресурсу: https://habr.com/ru/post/335090/.
2. Юров М. Компоненти локальної мережі [Електронний ресурс] / М. Юров // Санкт-Петербурзький національний лісотехнічний університет ім. С.М. Кирова. – 2018. – Режим доступу до ресурсу: https://studfile.net/preview/6826315/page:10/.
3. Лінков В. Все про IP та як із ними працювати [Електронний ресурс] / Валерій Лінков. – 2018. – Режим доступу до ресурсу: https://habr.com/ru/post/350878/.
4. Компанія Cisco. IP-адресація [Електронний ресурс] / Компанія Cisco // Cisco. – 2019. – Режим доступу до ресурсу: https://static-course-assets.s3.amazonaws.com/ITN6/ru/index.html#5.
5. Мамадов Р. Принципи роботи протоколу EIGRP [Електронний ресурс] / Руслан Мамадов. – 2018. – Режим доступу до ресурсу: https://habr.com/ru/post/420667.
6. Компанія Cisco. Віртуальні мережі VLAN [Електронний ресурс] / Компанія Cisco // Cisco. – 2019. – Режим доступу до ресурсу: https://static-course-assets.s3.amazonaws.com/ITN6/ru/index.html#5.2.2.
7. Компанія LanMarket. Що таке DHCP [Електронний ресурс] / Компанія LanMarket // LanMarket. – 2018. – Режим доступу до ресурсу: https://lanmarket.ua/entsiklopediya/telekommunikatsionnye-tekhnologii/dhcp.html.
8. Що таке SSH [Електронний ресурс] // Компанія GoodHoster. – 2020. – Режим доступу до ресурсу: https://goodhoster.net/uk/tips/chto-takoe-ssh/.
9. Лінков В. Що таке PAT [Електронний ресурс] / Валерій Лінков. – 2018. – Режим доступу до ресурсу: https://habr.com/ru/post/351332/.
10. Компанія Cisco. Маршрутизація та комутація [Електронний ресурс] / Компанія Cisco // Cisco. – 2019. – Режим доступу до ресурсу: https://static-course-assets.s3.amazonaws.com/ITN6/ru/index.html#6.2.1.1.

**ДОДАТОК А**

**ТЕХНІЧНЕ ЗАВДАННЯ**

*Номер варіанту роботи 11*

На розробку і конфігурування комп’ютерної мережі

1. Область застосування – комп’ютерні мережі.
2. Основна розробка – робочий навчальний план
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. Виконати моделювання мережі засобами GNS3 на Packet Tracer.
   2. Мережа складається з трьох окремих LAN, що об’єднуються WAN мережею, побудованою на основі технології̈ віртуальних каналів.
   3. Вимоги для проектування LAN1
      1. Адреса мережі 10.0.3.0
      2. Складається з п’яти сегментів, кількість робочих станцій в кожному з яких становить: 60, 5, 13, 27, 25.
      3. Розподіл адресного простору має бути оптимальним;
      4. Для об’єднання окремих сегментів використовуються 4 маршрутизатори;
      5. З’єднання між маршрутизаторами здійснюються за допомогою скрученої пари;
      6. Для обмеження проходження трафіку з одного сегменту в інший мають бути застосовані стандартні і розширені ACL. Стандартні списки мають заборонити проходження трафіку з мереж NET1 NET3 та NET5 відповідно до мереж NET2 NET4 та NET6. Розширені ACL мають заборонити проходження трафіку протоколів DNS, FINGER та FTP з NET1 до NET4 та HTTP HTTPS та ICMP 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 Rt2 налаштовано сервіс трансляції адрес NAT.
   4. Вимоги для проектування LAN2
      1. Адреса мережі 172.17.3.0/24
      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 з використанням протоколів канального рівня HDLC та РРР відповідно. Інші з’єднання виконуються за допомогою скрученої пари.
      5. Під’єднання мережі LAN2 до мережі WAN виконується через маршрутизатор Rt2.
      6. В середині мережі використовується динамічна маршрутизація на основі протоколу OSPF.
      7. На маршрутизаторі Rt2 налаштовано сервіс трансляції адрес NAT.
   5. Вимоги для проектування LAN3
      1. Реалізована на основі комутаторів Catalyst 2960 з підтримкою технології віртуальних мереж.
      2. Поділена на три віртуальні сегменти, кожний з яких містить по два сервери.
      3. На комутаторах Sw1 Sw3 до Vlan 2 належать порти FastEthernet3- FastEthernet7 та FastEthernet6-FastEthernet9 відповідно, до Vlan 3 FastEthernet9-FastEthernet15 та FastEthernet15-FastEthernet18 відповідно.
      4. З’єднання між комутаторами здійснюються за допомогою скрученої пари і технології Gigabit Ethernet.
      5. В віртуальних мережах VLAN1, VLAN2 та VLAN3 використовуються адреси 141.134.0.0 7.0.0.0 та 92.0.0.0 відповідно.
   6. 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 11.0.0.0/8
      3. З’єднання між локальними мережами здійснюється за допомогою послідовних інтерфейсів.
   7. Загальні вимоги до налаштувань маршрутизаторів
      1. Встановити на всіх маршрутизаторах паролі на консольне з’єднання та на привілейований режим.
      2. Налаштувати доступ через протокол SSH до шлюзових маршрутизаторів.
6. Апаратні вимоги - використання обладнання фірми Cisco
7. Текстова документація розробленої мережі повинна відповідати діючим стандартам України.
8. Стадії та етапи розробки мережі включать розробку та відлагодження окремих LAN та об’єднання LAN1-4 за допомогою WAN мережі.

Розробив студент групи: 303-Кб Тарасенко Ярослав Юрійович.

**ДОДАТОК Б**

**ТОПОЛОГІЯ ТА НАЛАШТУВАННЯ МАРШРУТИЗАТОРІВ**

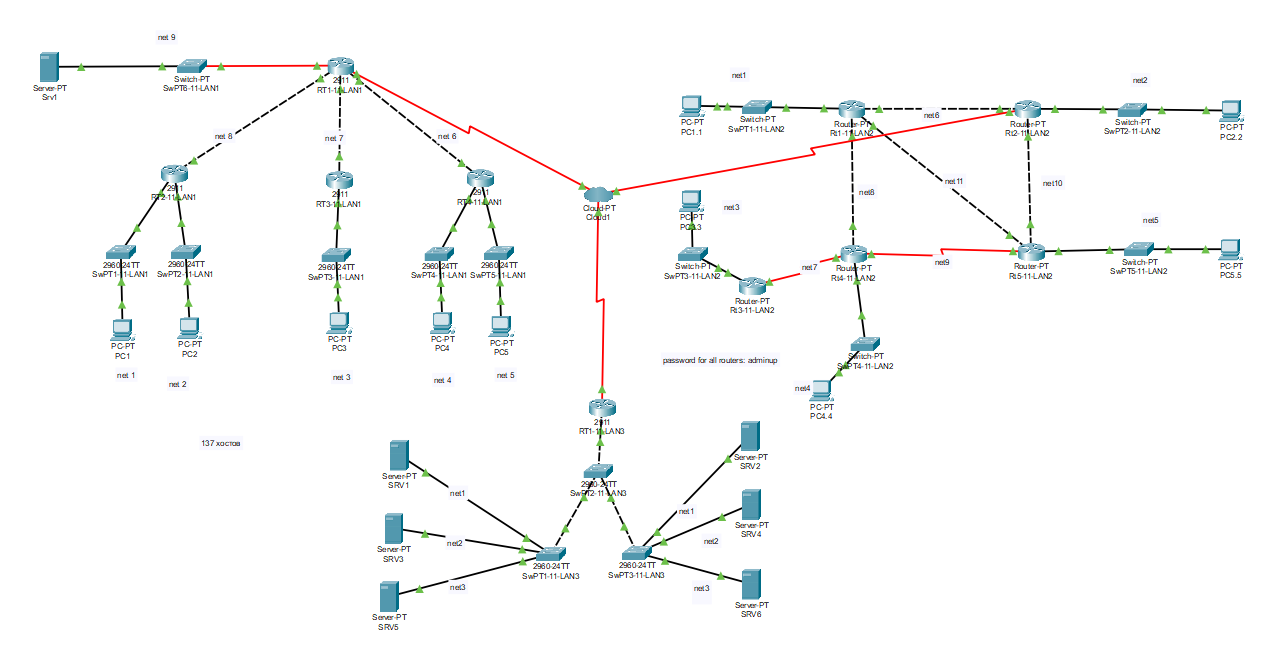
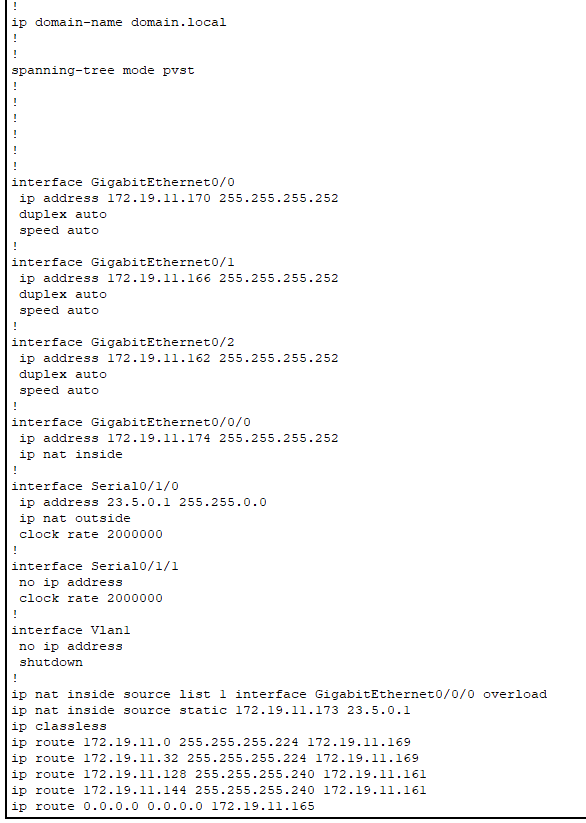


Рисунок 23 «топологія»



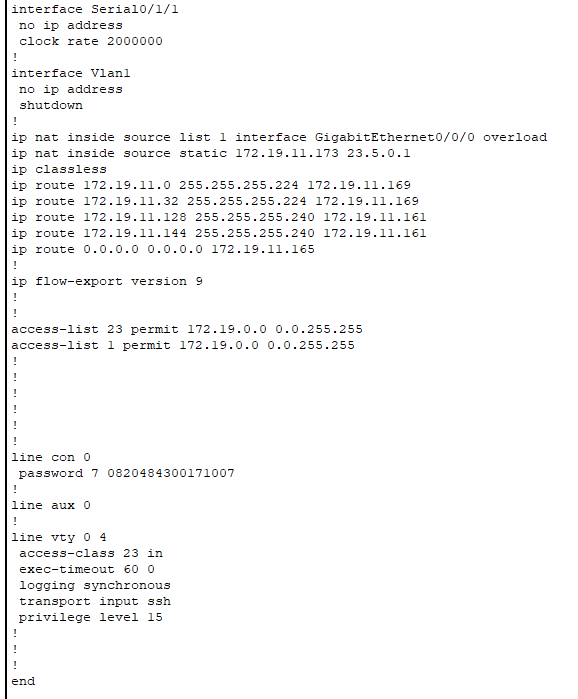


Рисунок 24, 25 «налаштування маршрутизатора 1 в мережі LAN1»

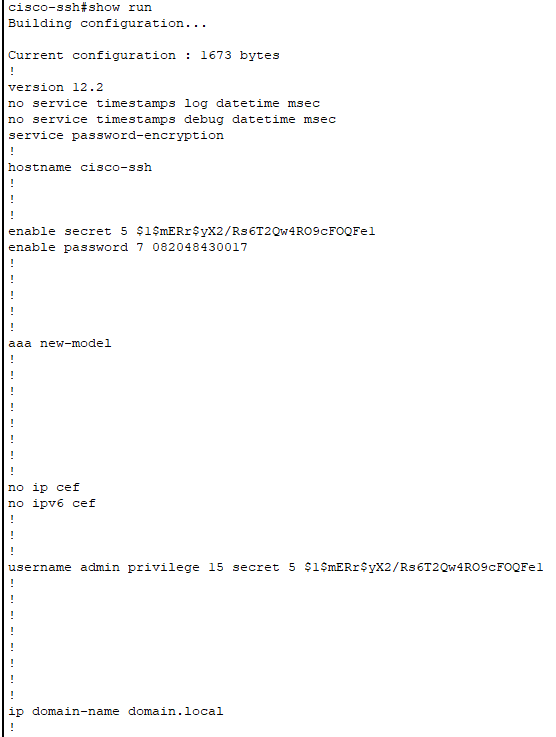


Рисунок 26 «налаштування маршрутизатора 2 в мережі LAN2»



Рисунок 27 «налаштування маршрутизатора 2 в мережі LAN2»

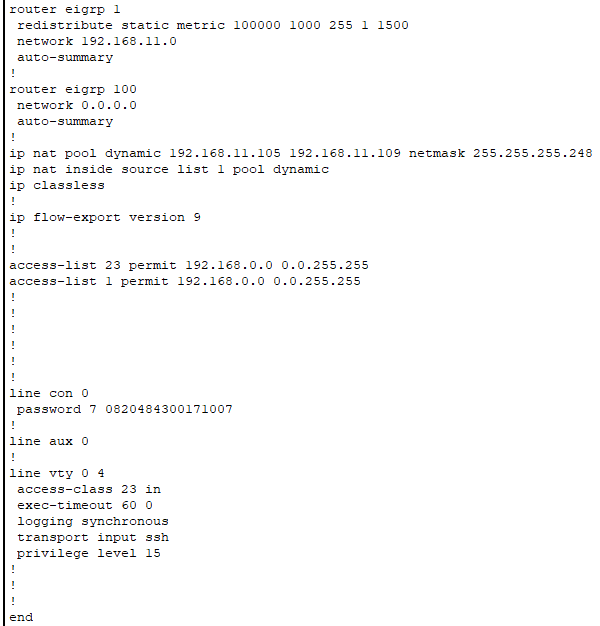


Рисунок 28 «налаштування маршрутизатора 2 в мережі LAN2»

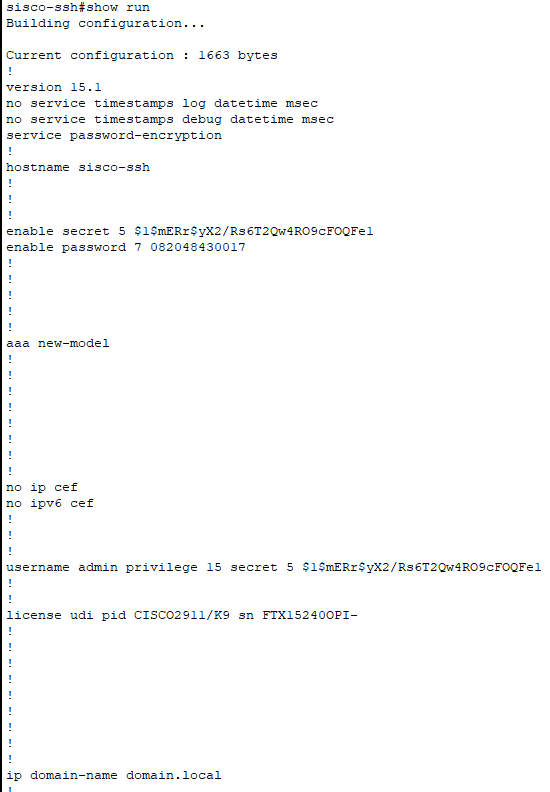


Рисунок 29 «налаштування маршрутизатора 1 в мережі LAN3»

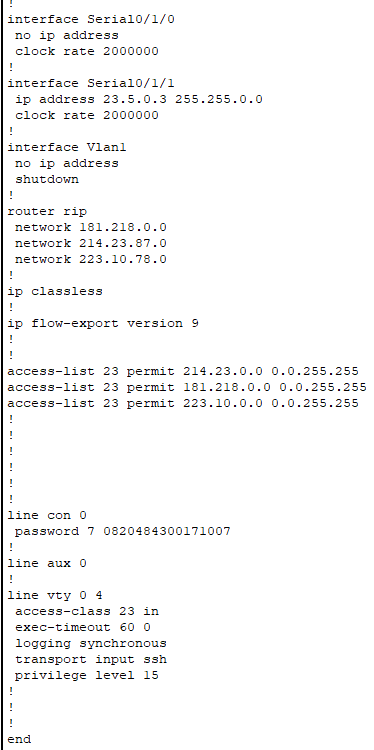
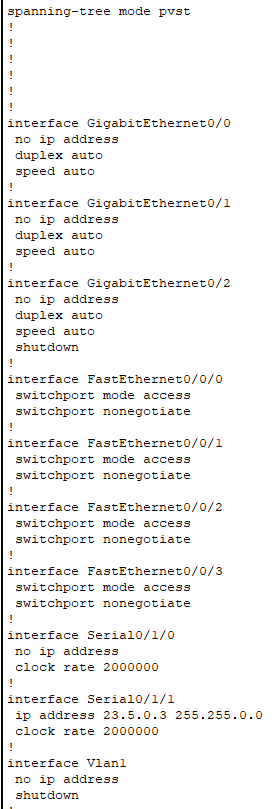


Рисунок 30, 31 «налаштування маршрутизатора 1 в мережі LAN3»