

Міністерство освіти і науки України  
Львівський національний університет природокористування  
Факультет механіки, енергетики та інформаційних технологій

Методичні рекомендації  
до виконання лабораторних робіт з  
дисципліни  
"Мережеві технології"  
для студентів  
освітнього ступеня бакалавр  
спеціальності 126 «Інформаційні системи та технології».



## ЗМІСТ

Вступ .....	5
Лабораторна робота 1. Логічна організація локальних комп'ютерних мереж .....	6
Теоретичні відомості .....	6
Хід роботи.....	9
Зміст звіту .....	9
Контрольні питання .....	9
Лабораторна робота 2. Вивчення устаткування локальних мереж .....	10
Теоретичні відомості .....	10
Хід роботи.....	16
Зміст звіту .....	17
Контрольні питання .....	17
Варіанти завдань .....	17
Лабораторна робота 3 Створення мережі між двома комп'ютерами засобами ОС Linux.....	19
Теоретичні відомості .....	19
Хід роботи.....	21
Зміст звіту .....	22
Контрольні питання .....	22
Лабораторна робота 4 Дослідження мережевих властивостей операційної системи Windows.	23
Теоретичні відомості .....	23
Хід роботи.....	25
Зміст звіту .....	25
Контрольні запитання.....	26
Лабораторна робота 5 Побудова віртуальних локальних мереж .....	27
Теоретичні відомості .....	27
Хід роботи.....	28
Зміст звіту .....	32
Контрольні запитання.....	32
Лабораторна робота 6. Імітаційне Моделювання мережі в Cisco Packet Tracer .....	33
Теоретичні відомості .....	33
Хід роботи.....	38
Завдання для виконання: .....	43
Зміст звіту .....	43
Контрольні питання .....	43
Лабораторна робота 7. Налаштування мережевих сервісів.....	45
Теоретичні відомості .....	45
Хід роботи.....	45
Зміст звіту .....	48
Контрольні питання .....	48
Лабораторна робота 8. Основні команди операційної системи Cisco IOS .....	49
Теоретичні відомості .....	49
Хід роботи.....	50
Зміст звіту .....	54
Контрольні питання .....	54
Лабораторна робота 9. Налаштування статичної маршрутизації.....	55
Теоретичні відомості .....	55
Хід роботи.....	56
Зміст звіту .....	59
Контрольні питання .....	59
Лабораторна робота 10 Налаштування протоколу RIP .....	60

Теоретичні відомості .....	60
Хід роботи.....	60
Зміст звіту .....	61
Лабораторна робота №11. Налаштування протоколу RIP в корпоративній мережі. ....	62
Теоретичні відомості .....	62
Хід роботи.....	62
Зміст звіту .....	65
Контрольні питання .....	65
Лабораторна робота №12. Налаштування протоколу OSPF.....	66
Теоретичні відомості .....	66
Хід роботи.....	66
Зміст звіту .....	67
Контрольні питання .....	68
Список використаних джерел .....	69

## ВСТУП

**Мета викладання дисципліни** – дати студентам систематизовані відомості про основні принципи побудови, апаратне і програмне забезпечення комп'ютерних мереж.

В результаті вивчення дисципліни студент повинен:

- знати основні функції, архітектуру та основи функціонування комп'ютерних мереж;
- навчитись по технічних вимогах вибрати структуру і протоколи мережі, а також вміти працювати з комп'ютерною мережею.

**Найменування та опис компетентностей**, формування котрих забезпечує вивчення дисципліни “комп'ютерні мережі”

- Засвоєння основних нормативно-правових актів та довідкових матеріалів, чинних стандартів і технічних умов, інструкцій та інших нормативно-розпорядчих документів галузі інформаційних технологій.

- Здатність до застосування обчислювальної техніки та програмування, володіння навичками роботи з комп'ютером і сучасними САПР для вирішення задач спеціальності.

- Здатність до застосування сучасних технологій та САПР проектування і моделювання комп'ютерних систем та мереж.

- Здатність застосовувати професійно-профільовані знання й практичні навички для розв'язування типових задач спеціальності, а також експлуатації комп'ютерних систем, мереж та їх устаткування.

- Володіти методами логічної організації локальних комп'ютерних мереж.
- Знання специфіки ієрархічної організації локальних мереж.
- Аналіз структурної організації і протоколів канального рівня мережі Ethernet.
- Навички вибору устаткування локальних мереж.
- Аналіз властивостей операційної системи Windows.
- Розуміння Інтерфейсу командного рядка (CLI).
- Здатність застосовувати утиліти ping, tracert, ipconfig, netstat.
- Здатність будувати таблиці статичної маршрутизації для вузла мережі та для маршрутизатора.

- Знання принципів розподілу адресного простору IP засобами маскування.
- Використання програмного забезпечення для віддаленого управління робочою станцією у середовищі ОС Windows та Linux

Мета проведення лабораторних занять полягає у тому, щоб виробити у студентів практичні навички проектування, моделювання та експлуатації комп'ютерних мереж із застосуванням сучасних мережевих технологій.

**Завдання проведення лабораторних занять:**

- вивчити основні типові проекти комп'ютерних мереж різних класів;
- навчитись складати технічне завдання для проектування комп'ютерної мережі;
- навчитись проводити розрахунок основних параметрів комп'ютерної мережі, активного і пасивного мережевого обладнання;
- вивчити поширені засоби імітаційного моделювання та проектування комп'ютерних мереж.

## ЛАБОРАТОРНА РОБОТА 1. ЛОГІЧНА ОРГАНІЗАЦІЯ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Мета: Вивчення специфіки ієрархічної організації локальних мереж, дослідження структурної організації і протоколів канального рівня мережі Ethernet

### ТЕОРЕТИЧНІ ВІДОМОСТІ

#### **1. Ієрархічна організація локальних обчислювальних мереж**

##### **1.1. Семирівнева модель.**

У кожній системі можна виділити сім рівнів обробки інформації: прикладний, представницький, сеансовий, транспортний, мережний, канальний (інформаційний), фізичний. Обмін інформацією між системами здійснюється з ініціативи прикладного рівня. При цьому в межах системи послідовно, починаючи з прикладного рівня, працюють усі сім рівнів, а зв'язок між системами здійснюється через фізичний канал – сполучні лінії, прийомопередавачі, що поєднують перші, фізичні рівні. Таким чином, уся мережа виявляється розділеною на 7 рівнів. На кожному рівні знаходяться об'єкти цього рівня: на прикладному рівні – це прикладні програми, на представницькому рівні – програми перетворення форматів і т.д. Об'єкт прикладного рівня може взаємодіяти з іншими об'єктами цього рівня – це основне призначення мережі.

Для того щоб взаємодія була можливою, треба змусити об'єкти прикладного рівня обмінюватися інформацією, керуючись уніфікованими наборами правил. Ці набори правил називаються протоколами прикладного рівня.

Безпосередньо об'єкти прикладного рівня не взаємодіють, для цього вони повинні звернутися до представницького рівня. Він також складається з об'єктів, що взаємодіють, користуючись протоколами цього рівня і звертаючи для реалізації цієї взаємодії до лежачого нижче шару мережі. Об'єкт прикладного рівня, звертаючи до розташованого в тій же системі об'єкту представницького рівня, звертається як би до всього представницького рівня мережі, і при здійсненні взаємодії працюють принаймні два об'єкти представницького рівня: один у системі-джерелі, іншої – у системі-приймачі. Зв'язок між прикладним і представницьким рівнями описується міжрівневим стандартом, який називається міжрівневим інтерфейсом. Через інтерфейс прикладний рівень одержує обслуговування (сервіс) представницького рівня. За описаною схемою взаємодіють інші рівні мережі.

Сукупність рівнів 1–4 створює транспортну мережу, призначення якої полягає в організації обміну інформацією, що надходить з верхніх трьох рівнів. Трійки об'єктів рівнів 5–7, розташовані в одній зосередженій системі, між якими встановлена взаємодія, називаються процесами. Процеси з'єднуються з транспортною системою через точки входу, які називають портами. В багатьох випадках усі рівні, крім фізичного, реалізуються у виді програм і тільки фізичний рівень використовує спеціальне зв'язне устаткування. Однак це не обов'язково.

В транспортній мережі зв'язок між джерелом і приймачем інформації може здійснюватися як безпосередньо, так і через системи-посередники, що приймають інформацію і ретранслюють її далі але мережі до приймача, можливо з проміжним збереженням. Розглянемо функції кожного рівня моделі.

Рівень 7– прикладний рівень. Виконує задану ззовні обробку інформації, тобто основну задачу системи. На цьому рівні виконуються наступні види обслуговування: ініціація, виконання і завершення процесів: ініціація, використання і завершення міжпроцесорних з'єднань (сеансів); присвоєння, вибірка і звільнення системних ресурсів; присвоєння, вибірка і звільнення об'єктів даних.

Рівень 6– представницький рівень. Виконує необхідні перетворення переносимої інформації для усунення синтаксичних розбіжностей. Рівень посилає запити в рівень 5 на встановлення і завершення сеансів.

Рівень 5– сеансовий рівень. Підтримує діалог, тобто структурований обмін даними між процесами. Рівень 5 надає наступні види сервісу: адресацію через поштові скриньки; передачу даних і їхнє розмежування; повідомлення процесів про надходження даних; групування даних у блоки, поділ їх на сегменти; буферизацію даних і керування потоком даних; контроль і відновлення після помилок.

Рівень 4– транспортний рівень. Забезпечує двохточкове з'єднання користувачів транспортного рівня, що не залежить від реалізації цього з'єднання на мережному рівні. Користувачі транспортного рівня розрізняються на цьому рівні тільки по їхніх транспортних адресах, що не мають відношення до фізичного розміщення користувачів. Транспортний рівень потрібний для того, щоб оптимізувати використання зв'язних ресурсів і забезпечити необхідну для обміну інформацією поведінку системи за мінімальну вартість. Мінімізація досягається за рахунок обліку всіх заявок у системі і наявних ресурсах. Між парою транспортних адрес може бути встановлене одночасно кілька з'єднань. Транспортний рівень дозволяє розрізнити їх, постачати відповідними ідентифікаторами.

Транспортний рівень надає сеансовому рівню наступні види сервісу.

1. Обслуговування встановлення з'єднання об'єктів сеансового рівня. При встановленні з'єднання транспортне обслуговування вибирає одне з заданої безлічі видів обслуговування: пакетний режим, обслуговування в реальному часі і т.д. Ці види обслуговування визначають значення таких параметрів, як пропускна здатність, затримка в доставці повідомлення, час установлення з'єднання, характер і рівень помилок при передачі. Транспортний рівень установлює з'єднання, тільки якщо обоє партнери згодні на встановлення даного виду з'єднання. Транспортний рівень вибирає найбільш придатне мережне обслуговування з врахуванням інших заявок, встановлює необхідність мультиплексування декількох транспортних з'єднань в одне мережне, а також оптимальний розмір переданої одиниці даних, вибирає функції, що повинні виконуватися в процесі обміну, відображає транспортні адреси в мережні, організує розрізнення декількох з'єднань, виконуваних через пару транспортних засобів.

2. Обслуговування передачі даних. Воно складається в проведенні обміну з заданим значенням якості. Якщо такий обмін стає неможливим, то транспортне з'єднання знищується і про це інформуються користувачі транспортного рівня. Транспортний рівень розділяє довільні вхідні одиниці даних із сеансового рівня на стандартні транспортні одиниці, що передаються в заданій послідовності до приймача. Навпаки, при необхідності виробляється збірка декількох вхідних одиниць даних у стандартні транспортні. При звертанні до мережного рівня може бути виконане зчеплення декількох транспортних одиниць даних в одну мережну одиницю. Транспортний рівень у випадку роботи з мультиплексуванням організує спільне використання одного мережного з'єднання декількома транспортними з'єднаннями. При передачі транспортний рівень керує потоком даних, виявляє втрату повідомлень, перекручування, дублювання, неправильну адресацію, зміну в порядку доставки, коректує виявлені помилки. В задачу транспортного рівня входить робота з границями – початком і кінцем повідомлень.

3. Обслуговування завершення передачі. Транспортний рівень дає можливість об'єкту сеансового рівня завершити обмін і інформувати про це партнера по обміні з вказівкою причин завершення.

Фізичний рівень надає засоби для створення, підтримки і знищення фізичних з'єднань, по яких здійснюється передача двійкових одиниць інформації між об'єктами рівня 2. При цьому, крім безпосереднього зв'язку, між джерелом і приймачем інформації допускається зв'язок через проміжні системи – ретранслятори. Одиницею даних на фізичному рівні є біт при послідовній передачі і група бітів при паралельній передачі. Фізичне з'єднання може бути дуплексним і напівдуплексним. Воно може бути також двохточковим чи багатоточковим. Фізичний рівень постачає кожен кінець з'єднання ідентифікатором, що використовується об'єктами рівня 2, а також однозначно ідентифікує лінії зв'язку між сусідніми системами. Ці ідентифікатори використовуються на мережному рівні при

встановленні маршруту з'єднання. Рівень 1 передає біти інформації без зміни їхнього порядку в синхронному чи асинхронному режимі. При виявленні помилки на фізичному рівні посиляється повідомлення в рівень 2.

При переміщенні даних між рівнями системи вони повинні забезпечуватися керуючою інформацією, що дозволяє рівню-приймачу настроїтися на відповідну роботу. Прийнято наступні структуру і найменування керуючої інформації.

Сформоване прикладною програмою повідомлення перед передачею в транспортну мережу насамперед нормалізується по довжині: розбивається на чи блоки кілька коротких повідомлень збирається в сегмент. Отримана в такий спосіб одиниця даних (звичайно блок) забезпечується керуючою інформацією – заголовком процесу. Транспортний рівень формує фрагмент, додаючи до блоку заголовок передачі. Мережний рівень формує з фрагмента пакет, додаючи заголовок пакета. Канальний рівень формує з пакета кадр, додаючи до пакета заголовок каналу і кінцевик каналу. Кінцевик забезпечує перевірку пакета після передачі по мережі. Помітимо, що часто при описі конкретних мереж поняття «пакет» використовується замість поняття «кадр».

### **1.2. Відхід від семирівневої моделі, проект стандарту 802 IEEE.**

Семирівнева модель ISO в області локальних мереж вимагає подальшого уточнення, оскільки спосіб організації і функціонування останніх істотно відрізняються від прийнятих для великих мереж. Це, як відзначалося, різні швидкості роботи, різні затримки, різна довжина повідомлень і т.д. Важлива відмінність – перевага в ЛМ багатоточкових з'єднань без проміжної буферизації. Усе це спонукає внести зміни в ієрархічну мережну модель ISO і розробити нові стандарти протоколів, більш пристосовані для ЛМ. Одна з таких робіт – створення стандарту 802 для локальних мереж, що у даний час підготовлений до твердження в IEEE Computer Society (США). Цей стандарт орієнтований на локальні мережі, призначені для використання в легкій промисловості і торгівлі. Локальні мережі для важкої промисловості, для задач керування й інших задач реального часу, для високонадійних додатків залишилися поза розроблювальним стандартом. Передбачається, що стандарт охопить ЛМ, що працюють із середніми і високими швидкостями – від 1 до 20 Мбіт/с. Це істотно більш високі швидкості, чим застосовувані в глобальних мережах.

В даний час стандарт розглядає питання, що відносяться тільки до рівнів 1 і 2 моделі ISO. Однак уже тут довелося внести значні зміни в модель. На рисунку 1.1 показана відповідність між рівнями 1 і 2 моделі ISO і трьома рівнями моделі IEEE: керуванням логічним зв'язком (КЛЗ) (Logical Link Control), керуванням доступом (КД) (Media Access Control) і фізичним рівнем. При цьому передбачається, що джерело і приймач інформації зв'язуються безпосередньо без проміжного збереження інформації в системах-посередниках. Стандарт допускає як комутацію пакетів, так і комутацію каналів.

Рівень керування логічним зв'язком виконує функції, близькі до функцій інформаційного рівня в 7-рівневій моделі. Однак, як уже відзначалося, нижче цього рівня повинне бути розташоване керування доступом, що здійснює комутацію абонентів через багатоточкове з'єднання. Це керування здійснюється на рівні керування доступом. Нижче цього рівня повинний, як і раніш, знаходитися фізичний рівень, що виконує тієї ж функції.

На закінчення ще раз підкреслимо ряд особливостей ЛМ.

1. ЛМ мають особливості, що істотно відрізняють їх від глобальних мереж, що не дозволяє просто перенести отримані в одній області результати на іншу.

2. ЛМ відрізняють більш високі швидкості обміну, більш швидка комутація, малий час поширення сигналу, менші обсяги одиниць переданої інформації. ЛМ мають більш просту структуру зв'язків, широко використовують на фізичному рівні багатоточкове з'єднання і не застосовують буферизацію даних у ретрансляторах.

3. ЛМ не є однорідним поняттям, її організація залежить від розв'язуваної задачі. Незважаючи на велику поширеність ЛМ, роботи над ними знаходяться тільки в початковій стадії. Особливо це відноситься до мереж, орієнтованих на рішення задач у реальному



масштабі часу. Розроблювальні для ЛМ стандарти поки обмежені областями додатків, що не висувають високі вимоги до характеристик мережі.

4. Для досягнення високих характеристик ЛМ засобу обробки інформації в них повинні бути орієнтовані на роботу в мережі.

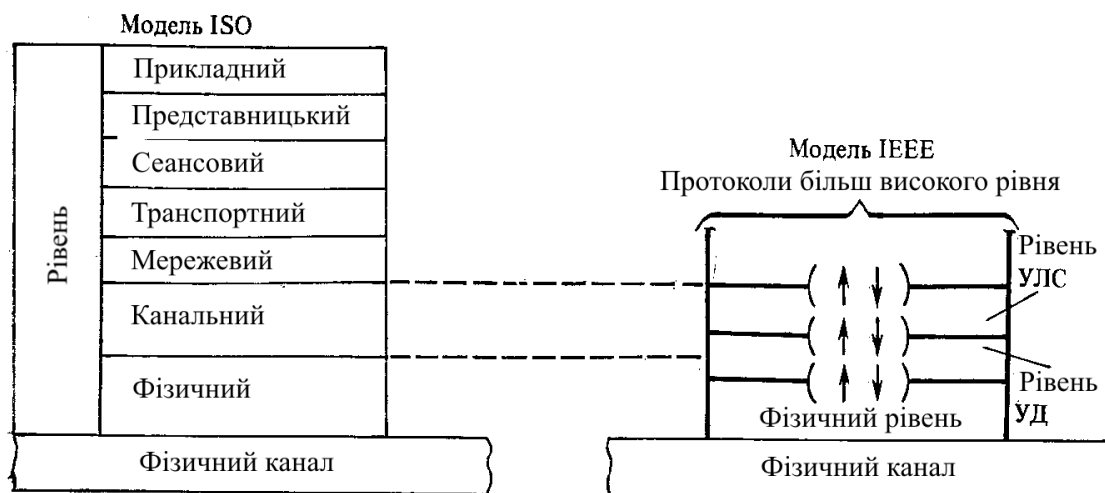


Рисунок 1.1 – Поділ на рівні в стандарті 802 IEEE

### ХІД РОБОТИ

1) Вивчити основні теоретичні відомості по логічній організації ЛМ, особливостям архітектури локальної мережі Ethernet.

2) Завантажити пакет SiSoft Sandra (Everest тощо), вибрати іконку “Інформація про мережу” (Network Information), проаналізувати подану інформацію, занотувати у звіт ресурси, подані для багатокористувацького використання.

### ЗМІСТ ЗВІТУ

1. Титульний лист
2. Короткий опис ієрархічної моделі ЛМ.
3. Функціональну схему архітектури і реалізації мережі Ethernet.
4. Опис функціонування устаткування мережі Ethernet.
5. Звіт по опису мережевих ресурсів “Інформація про мережу”

### КОНТРОЛЬНІ ПИТАННЯ

1. Семирівнева модель.
2. Види сервісу транспортного рівня.
3. Функції мережного, канального та фізичного рівня.
4. Проект стандарту 802 IEEE.
5. Протокол HDLC (High-Level Data Link Control)
6. Протокол КЛЗ.
7. Особливості ЛМ.
8. Логічна організація локальної мережі Ethernet
9. Архітектура і реалізація мережі Ethernet
10. Структура кадру Ethernet

## ЛАБОРАТОРНА РОБОТА 2. ВИВЧЕННЯ УСТАТКУВАННЯ ЛОКАЛЬНИХ МЕРЕЖ

Мета: вивчення специфіки ієрархічної організації локальних мереж, дослідження структурної організації з використанням пакету NetCracker

### ТЕОРЕТИЧНІ ВІДОМОСТІ

Для побудови локальних зв'язків в обчислювальних мережах у даний час використовуються різні види кабелів - коаксіальний кабель, кабель на основі екранованої (STP – Shielded twisted pair) і неекранованої витої пари (UTP - Unshielded twisted pair) і оптоволоконний кабель. Найбільш популярним видом середовища передачі даних на невеликі відстані (до 100 м) стає неекранована вита пара, що включена практично в усі сучасні стандарти і технології локальних мереж і забезпечує пропускну здатність до 100 Мб/с (на кабелях категорії 5). Оптоволоконний кабель широко застосовується як для побудови локальних зв'язків, так і для утворення магістралей глобальних мереж. Оптоволоконний кабель може забезпечити дуже високу пропускну здатність каналу (до декількох Гб/с) і передачу на значні відстані (до декількох десятків кілометрів без проміжного посилення сигналу).

Як середовище передачі даних в обчислювальних мережах використовуються також електромагнітні хвилі різних частот - КВ, УКВ, СВЧ. Однак, поки в локальних мережах радіозв'язок використовується тільки в тих випадках, коли виявляється неможливою прокладка кабелю, наприклад, у будинках, що є пам'ятниками архітектури. Це обумовлюється насамперед недостатньою надійністю мережних технологій, побудованих на використанні електромагнітного випромінювання. Для побудови глобальних каналів цей вид середовища передачі даних використовується ширше - на ньому побудовані супутникові канали зв'язку і наземні радіорелейні канали, що працюють у зонах прямої видимості у Свч-діапазонах.

Відповідно до закордонних досліджень, 70% часу простоїв обумовлено проблемами, що виникли внаслідок низької якості застосовуваних кабельних систем. Тому так важливо правильно побудувати фундамент мережі - кабельну систему. Останнім часом як таку надійну основу всі частіше використовується структурована кабельна система.

Структурована кабельна система (Structured Cabling System, SCS) - це набір комутаційних елементів (кабелів, рознімів, конекторів, кросових панелей і шаф), а також методика їхнього спільного використання, що дозволяє створювати регулярні, легко розширювані структури зв'язків в обчислювальних мережах.

Переваги структурованої кабельної системи:

- Універсальність. Структурована кабельна система при продуманій організації може стати єдиним середовищем для передачі комп'ютерних даних у локальній обчислювальній мережі, організації локальної телефонної мережі, передачі відеоінформації і навіть передачі сигналів від датчиків пожежної чи безпеки охоронних систем. Це дозволяє автоматизувати багато процесів по контролі, моніторингу і керуванню господарськими службами і системами життєзабезпечення.

- Збільшення терміну служби. Термін старіння добре структурованої кабельної системи може складати 8-10 років.

- Зменшення вартості додавання нових користувачів і зміни їхніх місць розміщення. Вартість кабельної системи в основному визначається не вартістю кабелю, а вартістю робіт з його прокладки. Тому більш вигідно провести однократну роботу по прокладці кабелю, можливо з великим запасом по довжині, чим кілька разів виконувати прокладку, нарощуючи довжину кабелю. Це допомагає швидко і дешево змінювати структуру кабельної системи при переміщеннях персоналу чи зміні додатків.

– Можливість легкого розширення мережі. Структурована кабельна система є модульною, тому її легко нарощувати, дозволяючи легко та ціною малих витрат переходити на більш сучасне устаткування, що задовольняє зростаючі вимоги до систем комунікацій.

– Забезпечення більш ефективного обслуговування. Структурована кабельна система полегшує обслуговування і пошук несправностей у порівнянні із шинною кабельною системою.

– Надійність. Структурована кабельна система має підвищену надійність, оскільки звичайне виробництво всіх її компонентів і технічний супровід здійснюється одною фірмою-виробником.

### **Мережні адаптери.**

Мережний адаптер (Network Interface Card, NIC) - це периферійний пристрій комп'ютера, безпосередньо взаємодіючий із середовищем передачі даних, що прямо через інше комунікаційне устаткування зв'язує його з іншими комп'ютерами. Цей пристрій вирішує задачі надійного обміну двійковими даними, представленими відповідними електромагнітними сигналами по зовнішніх лініях зв'язку. Як і будь-який контролер комп'ютера, мережний адаптер працює під керуванням драйвера операційної системи і розподіл функцій між мережним адаптером і драйвером може змінюватися від реалізації до реалізації.

У перших локальних мережах мережний адаптер із сегментом коаксіального кабелю являв собою весь спектр комунікаційного устаткування, за допомогою якого організовувалася взаємодія комп'ютерів. Мережний адаптер комп'ютера-відправника безпосередньо по кабелі взаємодівав з мережним адаптером комп'ютера-одержувача. У більшості сучасних стандартів для локальних мереж передбачається, що між мережними адаптерами взаємодіючих комп'ютерів встановлюється спеціальний комунікаційний пристрій (концентратор, міст, чи комутатор-маршрутизатор), що бере на себе деякі функції по керуванню потоком даних.

Мережний адаптер звичайно виконує наступні функції:

– Оформлення переданої інформації у виді кадру визначеного формату. Кадр включає кілька службових полів, серед яких мається адреса комп'ютера призначення і контрольна сума кадру, по якій мережний адаптер станції призначення робить висновок про коректність доставленої по мережі інформації.

– Одержання доступу до середовища передачі даних. У локальних мережах в основному застосовуються поділювані між групою комп'ютерів канали зв'язку (загальна шина, кільце), доступ до яких надається по спеціальному алгоритму (найбільше часто застосовуються метод випадкового чи доступу метод з передачею маркера доступу по кільцю). В останніх стандартах і технологіях локальних мереж намітився перехід від використання поділюваного середовища передачі даних до використання індивідуальних каналів зв'язків комп'ютера з комунікаційними пристроями мережі, як це завжди робилося в телефонних мережах, де телефонний апарат зв'язаний з комутатором АТС індивідуальною лінією зв'язку. Технологіями, що використовують індивідуальні лінії зв'язку, є 100VG-AnyLAN, ATM і комутуючі модифікації традиційних технологій - switching Ethernet, switching Token Ring і switching FDDI. При використанні індивідуальних ліній зв'язку у функції мережного адаптера часто входить встановлення з'єднання з комутатором мережі.

– Кодування послідовності біт кадру послідовністю електричних сигналів при передачі даних і декодування при їхньому прийомі. Кодування повинне забезпечити передачу вихідної інформації з ліній зв'язку з визначеною смугою пропускання і визначеним рівнем перешкод таким чином, щоб приймаюча сторона змогла розпізнати з високим ступенем імовірності послану інформацію. Тому що в локальних мережах використовуються широкосмугові кабелі, то мережні адаптери не використовують модуляцію сигналу, необхідну для передачі дискретної інформації з вузькосмугових ліній зв'язку (наприклад,

телефонним каналам тональної частоти), а передають дані за допомогою імпульсних сигналів. Представлення двійкових 1 і 0 може бути різним.

- Перетворення інформації з паралельної форми в послідовну і назад. Ця операція зв'язана з тим, що для спрощення проблеми синхронізації сигналів і здешевлення ліній зв'язку в обчислювальних мережах інформація передається в послідовній формі, біт за бітом, а не побайтно, як усередині комп'ютера.

- Синхронізація бітів, байтів і кадрів. Для стійкого прийому переданої інформації необхідна підтримка постійного синхронізму приймача і передавача інформації. Мережний адаптер використовує для рішення цієї задачі спеціальні методи кодування, що не використовують додаткової шини з тактовими синхросигналами. Ці методи забезпечують періодичну зміну стану переданого сигналу, що використовується тактовим генератором приймача для підстроювання синхронізму. Крім синхронізації на рівні бітів, мережний адаптер вирішує задачу синхронізації і на рівні байтів, і на рівні кадрів.

Мережні адаптери розрізняються по типу і розрядності використовуваної в комп'ютері внутрішньої шини даних - ISA, EISA, PCI, MCA. Мережні адаптери розрізняються також по типу використовуваної мережної технології - Ethernet, Token Ring, FDDI і т.п. Як правило, конкретна модель мережного адаптера працює по визначеній мережній технології (наприклад, Ethernet). У зв'язку з тим, що для кожної технології зараз мається можливість використання різних середовищ передачі даних (той же Ethernet підтримує коаксіальний кабель, неекрановану виту пару та оптоволоконний кабель), мережний адаптер може підтримувати як одну, так і одночасно кілька середовищ. У випадку, коли мережний адаптер підтримує тільки одне середовище передачі даних, а необхідно використовувати іншу, застосовуються трансівери і конвертори.

Трансівер (прийомопередавач, TRANSMitter+recEIVER) - це частина мережного адаптера, його кінцевий пристрій, що виходить на кабель. У першому стандарті Ethernet, що працює на товстому коаксіалі, трансівер розташовувався безпосередньо на кабелі і зв'язувався з іншою частиною адаптера, що розташовувалася усередині комп'ютера, за допомогою інтерфейсу AUI (attachment unit interface). В інших варіантах Ethernet виявилось зручним випускати мережні адаптери (та й інші комунікаційні пристрої) з портом AUI, до якого можна приєднати трансівер для необхідного середовища.

Замість підбору придатного трансівера можна використовувати конвертор, що може погодити вихід прийомопередавача, призначеного для одного середовища, з іншим середовищем передачі даних (наприклад, вихід на виту пару перетвориться у вихід на коаксіальний кабель).

### **Фізична структуризація локальної мережі.**

Концентратори утворюють з окремих фізичних відрізків кабелю загальне середовище передачі даних - логічний сегмент. Логічний сегмент також називають доменом колізій, оскільки при спробі одночасної передачі даних будь-яких двох комп'ютерів цього сегмента, хоча б і приналежних різним фізичним сегментам, виникає блокування передавального середовища. Варто особливо підкреслити, що яку би складну структуру не утворювали концентратори, наприклад, шляхом ієрархічного з'єднання (Рисунок 2.3), усі комп'ютери, підключені до них, утворюють єдиний логічний сегмент, у якому будь-яка пара взаємодіючих комп'ютерів цілком блокує можливість обміну даними для інших комп'ютерів.

Поява пристроїв, що централізують з'єднання між окремими мережними пристроями, потенційно дозволяє поліпшити керованість мережі і її експлуатаційні характеристики (модифікованість, ремонтпридатність і т.п.). З цією метою розроблювачі концентраторів часто вбудовують у свої пристрої, крім основної функції повторювача, ряд допоміжних функцій, дуже корисних для поліпшення якості мережі.

Різні виробники концентраторів реалізують у своїх пристроях різні набори допоміжних функцій, але найбільше часто зустрічаються наступні:

- Об'єднання сегментів з різними фізичними середовищами (наприклад, коаксіал, вита пара та оптоволокно) у єдиний логічний сегмент.
- Автосегментація портів - автоматичне відключення порту при його некоректному поводженні (ушкодження кабелю, інтенсивна генерація пакетів помилкової довжини і т.п.).
- Підтримка між концентраторами резервних зв'язків, що використовуються при відмовленні основних.
- Захист переданих по мережі даних від несанкціонованого доступу (наприклад, шляхом перекручування поля чи даних у кадрах, повторюваних на портах, що не містять комп'ютера з адресою призначення).
- Підтримка засобів керування мережами - протоколу SNMP, баз керуючої інформації MIB.

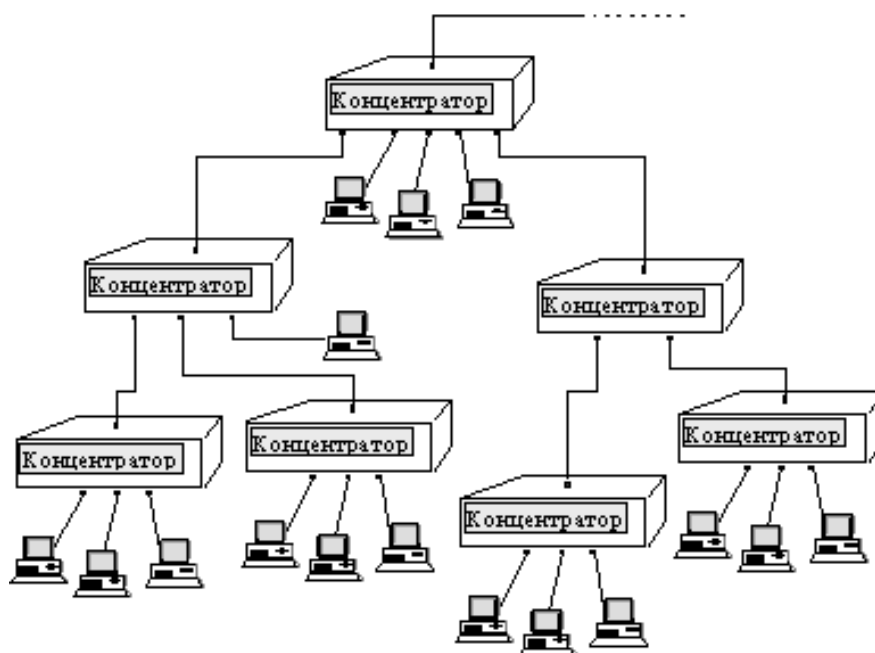


Рисунок 2.1 – Логічний сегмент, побудований з використанням концентраторів

### Логічна структуризація мережі.

При роботі комутатора середовище передачі даних кожного логічного сегмента залишається загальною тільки для тих комп'ютерів, що підключені до цього сегмента безпосередньо. Комутатор здійснює зв'язок середовищ передачі даних різних логічних сегментів. Він передає кадри між логічними сегментами тільки при необхідності, тобто тільки тоді, коли взаємодіючі комп'ютери знаходяться в різних сегментах.

Розподіл мережі на логічні сегменти поліпшує продуктивність мережі, якщо в мережі мають групи комп'ютерів, що переважно обмінюються інформацією між собою. Якщо ж таких груп ні, то введення в мережу комутаторів може тільки погіршити загальну продуктивність мережі, тому що ухвалення рішення про тім, потрібно чи передавати пакет з одного сегмента в іншій, вимагає додаткового часу. Однак такі групи, як правило, є навіть у мережі середніх розмірів. Тому поділ її на логічні сегменти дає вигоду у продуктивності - трафік локалізується в межах груп, і навантаження на їхні розділені кабельні системи істотно зменшуються.

Комутатори приймають рішення про те, на який порт потрібно передати кадр, аналізуючи адресу призначення, поміщена в кадрі, а також на підставі інформації про приналежність того чи іншого комп'ютера визначеному сегменту, підключеному до одному з портів комутатора, тобто на підставі інформації про конфігурацію мережі. Для того щоб зібрати й обробити інформацію про конфігурацію підключених до нього сегментів, комутатор повинний пройти стадію "навчання", тобто самостійно проробити деяку

попередню роботу з вивчення пройшовшого через нього трафіку. Визначення приналежності комп'ютерів сегментам можливо за рахунок наявності в кадрі не тільки адреси призначення, але й адреси джерела, яке згенерувало пакет. Використовуючи інформацію про адресу джерела, комутатор установлює відповідність між номерами портів і адресами комп'ютерів. У процесі вивчення мережі міст/комутатор просто передає отримані на входах його портів кадри на всі інші порти, працюючи якийсь час повторювачем. Після того, як міст/комутатор довідається про приналежність адрес сегментам, він починає передавати кадри між портами тільки у випадку міжсегментної передачі. Якщо, уже після завершення навчання, на вході комутатора раптом з'явиться кадр із невідомою адресою призначення, то цей кадр буде повторений на всіх портах.

Мости/комутатори, що працюють описаним способом, звичайно називаються прозорими (transparent), оскільки поява таких мостів/комутаторів у мережі зовсім не помітно для її кінцевих вузлів. Це дозволяє не змінювати їхнє програмне забезпечення при переході від простих конфігурацій, що використовують тільки концентратори, до більш складних, сегментованих.

Існує й інший клас мостів/комутаторів, що передають кадри між сегментами на основі повної інформації про міжсегментний маршрут. Цю інформацію записує в кадр станція-джерело кадру, тому говорять, що такі пристрої реалізують алгоритм маршрутизації від джерела (source routing). При використанні мостів/комутаторів з маршрутизацією від джерела кінцеві вузли повинні бути в курсі розподілу мережі на сегменти і мережні адаптери, у цьому випадку повинні у своєму програмному забезпеченні мати компонент, що займається вибором маршруту кадрів.

За простоту принципу роботи прозорого моста/комутатора приходить розплачуватися обмеженнями на топологію мережі, побудованої з використанням пристроїв даного типу - такі мережі не можуть мати замкнутих маршрутів - петель. Міст/комутатор не може правильно працювати в мережі з петлями, при цьому мережа засмічується пакетами, які зациклюються, і тому її продуктивність знижується.

Для автоматичного розпізнавання петель у конфігурації мережі розроблений алгоритм покриваючого дерева (Spanning Tree Algorithm, STA). Цей алгоритм дозволяє мостам/комутаторам адаптивно будувати дерево зв'язків, коли вони вивчають топологію зв'язків сегментів за допомогою спеціальних тестових кадрів. При виявленні замкнутих контурів деякі зв'язки будуть резервними. Міст/комутатор може використовувати резервний зв'язок тільки при відмовленні якої-небудь основного зв'язку. У результаті мережі, побудовані на основі мостів/комутаторів, що підтримують алгоритм покриваючого дерева, мають деякий запас надійності, але підвищити продуктивність за рахунок використання декількох рівнобіжних зв'язків у таких мережах не можна.

### **Маршрутизатори**

Маршрутизатор (router) дозволяє організовувати в мережі надлишкові зв'язки, що утворюють петлі. Він справляється з цією задачею за рахунок того, що приймає рішення про передачу пакетів на підставі більш повної інформації про графа зв'язків у мережі, чим чи міст комутатор. Маршрутизатор має у своєму розпорядженні базу топологічної інформації, що говорить йому, наприклад, про те, між якими підмережами загальної мережі є зв'язки і у якому стані (працездатному чи ні) вони знаходяться. Маючи таку карту мережі, маршрутизатор може вибрати один з декількох можливих маршрутів доставки пакета адресату. У даному випадку під маршрутом розуміють послідовність проходження пакетом маршрутизаторів. На рисунку 2.2 для зв'язку станцій L2 мережі LAN1 і L1 мережі LAN6 мається два маршрути: M1-M5-M7 і M1-M6-M7.

У відмінності від моста/комутатора, який не знає, як зв'язані сегменти один з одним за межами його портів, маршрутизатор бачить усю картину зв'язків під мереж один з одним, тому він може вибрати правильний маршрут і при наявності декількох альтернативних

маршрутів. Рішення про вибір того чи іншого маршруту приймається кожним маршрутизатором, через який проходить повідомлення.

Для того, щоб скласти карту зв'язків у мережі, маршрутизатори обмінюються спеціальними службовими повідомленнями, у яких міститься інформація про ті зв'язки між підмережами, про які вони знають (ці підмережі підключені до них чи безпосередньо ж вони знають цю інформацію від інших маршрутизаторів).

Побудова графа зв'язків між підмережами і вибір оптимального за яким-небудь критерієм маршруту на цьому графі являють собою складну задачу. При цьому можуть використовуватися різні критерії вибору маршруту - найменша кількість проміжних вузлів, час, вартість чи надійність передачі даних.

Маршрутизатори дозволяють поєднувати мережі з різними принципами організації в єдину мережу, що у цьому випадку часто називається інтермережа (internet). Назва інтермережа підкреслює ту особливість, що утворене за допомогою маршрутизаторів об'єднання комп'ютерів являє собою сукупність декількох мереж, що зберігають великий ступінь автономності, чим кілька логічних сегментів однієї мережі. У кожній з мереж, що утворюють інтермережу, зберігаються властиві їм принципи адресації вузлів і протоколи обміну інформацією. Тому маршрутизатори можуть поєднувати не тільки локальні мережі з різною технологією, але і локальні мережі з глобальними.

Маршрутизатори не тільки поєднують мережі, але і надійно захищають їхній одну від іншої. Причому ця ізоляція здійснюється набагато простіше і надійніше, ніж за допомогою мостів/комутаторів. Наприклад, при надходженні кадру з неправильною адресою міст/комутатор зобов'язаний повторити його на усіх своїх портах, що робить мережу незахищеною від некоректно працюючого вузла. Маршрутизатор же в такому випадку просто відмовляється передавати "неправильний" пакет далі, ізолюючи дефектний вузол від іншої мережі.

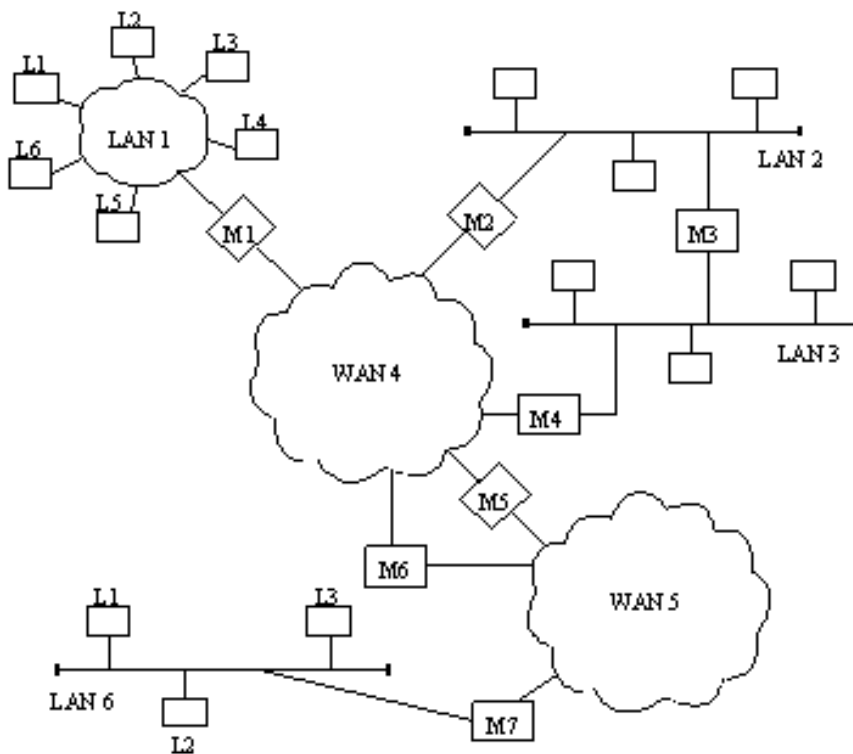


Рисунок 2.2 – Структура інтермережі, побудованої на основі маршрутизаторів

На рисунку зображено:

M1, M2, ... , M7 – маршрутизатори

LAN1, LAN2, LAN3, WAN4, WAN5, LAN6 - унікальні номери мереж у єдиному форматі

L1, L2, ... - локальні номери вузлів (дублюються, різний формат)

Крім того, маршрутизатор надає адміністратору зручні засоби фільтрації потоку повідомлень за рахунок того, що сам розпізнає службову інформацію в пакеті і дозволяє їх іменувати зрозумілим адміністратору образом. Потрібно відмітити, що деякі мости/комутатори також здатні виконувати функції гнучкої фільтрації, але задавати умови фільтрації адміністратор мережі повинний сам у двійковому форматі, що досить складно.

Крім фільтрації, маршрутизатор може забезпечувати пріоритетний порядок обслуговування буферизованих пакетів, коли на підставі деяких ознак пакетам надаються переваги при виборі з черги. В результаті, маршрутизатор виявляється складним інтелектуальним пристроєм, побудованим на базі одного, а іноді і декількох могутніх процесорів. Такий спеціалізований мультипроцесор працює, як правило, під керуванням спеціалізованої операційної системи.

## **Функціональна відповідність видів комунікаційного устаткування рівням моделі OSI**

Кращим способом для розуміння відмінностей між мережними адаптерами, повторювачами, мостами/комутаторами і маршрутизаторами є розгляд їхньої роботи в термінах моделі OSI. Співвідношення між функціями цих пристроїв і рівнями моделі OSI показано на малюнку 6.

Повторювач, що регенерує сигнали, за рахунок чого дозволяє збільшувати довжину мережі, працює на фізичному рівні. Мережний адаптер працює на фізичному і каналному рівнях. До фізичного рівня відноситься та частина функцій мережного адаптера, що зв'язана з прийомом і передачею сигналів по лінії зв'язку, а одержання доступу до розділеного середовища передачі, розпізнавання MAC-адреса комп'ютера - це уже функція каналного рівня. Мости виконують велику частину своєї роботи на каналному рівні. Для них мережа представляється набором MAC-адрес пристроїв. Вони витягають ці адреси з заголовків, доданих до пакетів на каналному рівні, і використовують їх під час обробки пакетів для ухвалення рішення про те, на який порт відправити той чи інший пакет. Мости не мають доступу до інформації про адреси мереж, що відноситься до більш високого рівня. Тому вони обмежені в прийнятті рішень про можливі шляхи чи маршрути переміщення пакетів по мережі.

Маршрутизатори працюють на мережному рівні моделі OSI. Для маршрутизаторів мережа - це набір мережних адрес пристроїв і безліч мережних шляхів. Маршрутизатори аналізують усі можливі шляхи між будь-якими двома вузлами мережі і вибирають самий короткий з них. При виборі можуть прийматися в увагу й інші фактори, наприклад, стан проміжних вузлів і ліній зв'язку, пропускна здатність чи ліній вартість передачі даних.

Для того, щоб маршрутизатор міг виконувати покладені на нього функції йому повинна бути доступна більш розгорнута інформація про мережу, ніж та, котра доступна мосту. У заголовку пакета мережного рівня крім мережної адреси маються дані, наприклад, про критерій, що повинний бути використаний при виборі маршруту, про час життя пакета в мережі, про те, якому протоколу верхнього рівня належить пакет. Завдяки використанню додаткової інформації, маршрутизатор може здійснювати більше операцій з пакетами, чим міст/комутатор. Тому програмне забезпечення, необхідне для роботи маршрутизатора, є більш складним.

## **ХІД РОБОТИ**

1. Використовуючи пакет NetCracker, вивчити склад і функціональні характеристики стандартного набору типового устаткування локальних мереж.



2. У відповідний розділ бази даних компонентів додати опис нового елемента з зазначеними характеристиками (табл. 1-4).

3. Вибрати в базі даних типи робочих станцій (PC), які будуть сумісні із заданим мережевим адаптером (МА), і тип сервера, який буде сумісний із комутатором без додавання додаткового МА.

4. Створити локальну комп'ютерну мережу по фізичній топології зірка на основі витої пари із 1-им комутатором у центрі, концентратори і сервери під'єднуються до комутатора, а робочі станції із зазначеними в таблиці мережевими адаптерами (МА) під'єднуються до концентраторів.

5. Встановити трафік пакетів між серверами і робочими станціями і запустити модель на виконання емуляції мережі.

### ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Короткі теоретичні відомості.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

### КОНТРОЛЬНІ ПИТАННЯ

1. Семирівнева модель OSI
2. Види сервісу транспортного рівня.
3. Функції мережного, канального та фізичного рівня.
4. Проект стандарту 802 IEEE.

### ВАРІАНТИ ЗАВДАНЬ

Таблиця 2.1 – Варіанти завдань.

№ варіанта	Тип МА (к-сть PC + к-сть серверів)	Тип концентратора	Тип комутатора
1	1 (32+3)	1	1
2	2 (16+4)	2	2
3	3 (48+2)	3	1
4	4 (33+3)	1	2
5	5 (17+4)	2	1
6	1 (49+2)	3	2
7	2 (31+3)	1	1
8	3 (15+4)	2	2
9	4 (47+2)	3	1
10	5 (34+3)	1	2
11	1 (18+4)	2	1
12	2 (50+2)	3	2
13	3 (35+3)	1	1
14	4 (19+4)	2	2
15	5 (51+2)	3	1

Таблиця 2.2 – Типи мережних адаптерів.

№	Виробник	Модель	Швидкість передачі, Мб/з	Тип слота розширення	Тип середовища передачі	Макс. відстань до концентратора, м
1	DLink	DFE538TX	10/100	PCI	Ethernet, UTP, TX	100
2	Intel	EtherExpress 100+ TX	10/100	PCI	Ethernet, UTP, TX	100
3	IBM	EtherJet 100+ TX	10/100	PCI	Ethernet, UTP, TX	100
4	3Com	3C905B-TX	10/100	PCI	Ethernet, UTP, TX	100
5	3Com	FastEtherlink 3C980C	10/100	PCI	Ethernet, UTP, TX	100

Таблиця 3. Типи концентраторів.

№	Виробник	Модель	Тип портів	Кількість портів	Швидкість передачі, Мб/з
1	DLink	DFE 916Dx	Ethernet, TX	16	10/100
2	3COM	3C16750A	Ethernet, TX	8	10/100
3	Allied Telesyn	AT-FH7024E	Ethernet, TX	24	10/100

Таблиця 4. Типи комутаторів.

№	Виробник	Модель	Тип портів	Кількість портів	Швидкість передачі, Мб/з
1	Allied Telesyn	AT-8316SX	Ethernet, TX	16	10/100
2	Cisco	Catalist 3512-XL	Ethernet, TX	12	10/100

## ЛАБОРАТОРНА РОБОТА 3 СТВОРЕННЯ МЕРЕЖІ МІЖ ДВОМА КОМП'ЮТЕРАМИ ЗАСОБАМИ ОС LINUX.

Мета роботи: використовуючи знання з апаратного та програмного забезпечення ЛМ створити, налаштувати та перевірити мережу між двома комп'ютерами, використовуючи нуль-хабне з'єднання.

### ТЕОРЕТИЧНІ ВІДОМОСТІ

#### 1.1 Прямий (Straight-through) порядок обтиску кручений пари

1. Прямий (Straight-through) порядок обтиску кручений пари, яка веде від робочої станції до концентратора. Нижче представлений варіант прямого кабелю 568В-568В. Зараз в основному тільки ці кабелі використовуються в якості всіляких пасивне. Є ще варіант 568А-568А. Обидва варіанти описані в таблиці.

Для стандарту Ethernet 100Base-T використовуються чотири жили (помаранчева і зелена пара), а решту чотири зарезервовані для стандарту Gigabit Ethernet (1000Base-T). Є два варіанти розведення 568А або 568В. Найчастіше використовується варіант 568В, як було зазначено раніше.

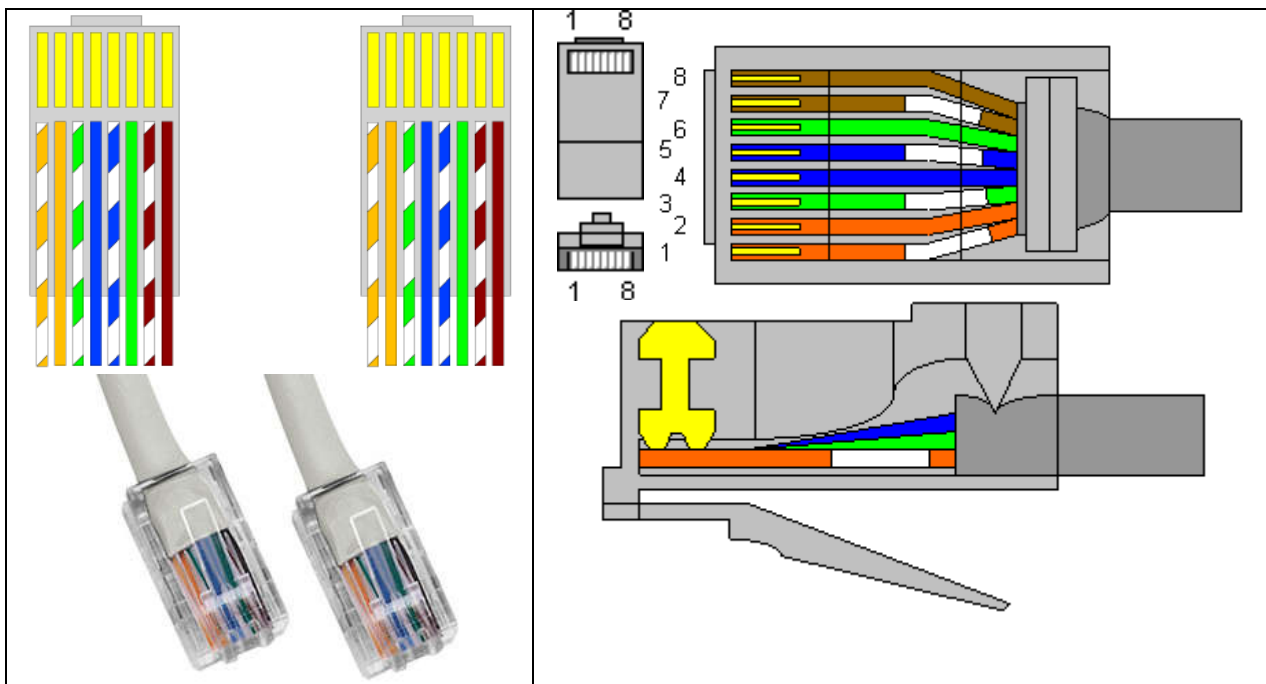


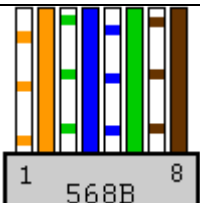
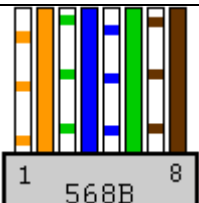
Рисунок 3.1 – Зовнішній вигляд конектора RJ-45 з нумерацією роз'ємів

Розведення кабелю для з'єднання комп'ютера з мережевим обладнанням (патч-корду) представлена в таблиці 3.1, на малюнках зображений зовнішній вигляд кабелю, підготовленого до вставки в конектор (обидва конектора обжимаються однаково).

#### Crossover cable

2. Крос-лінковий (перехресний, кросоверним, crossover) порядок обтиску кручений пари. Застосовується в разі, коли потрібно з'єднати між собою 2 концентратора, що не мають перемикання uplink / normal, а також для прямого з'єднання 2-х комп'ютерів. Часто кросоверним кабель не потрібен, тому що сучасні пристрої автоматично визначають, чи потрібно зробити кросовер. Нижче представлена картинка одного з варіантів обтискача кросовера: перший конектор обжати як 568В, другий як 568А.

Таблиця 3.1 – Розведення кабелю для з'єднання комп'ютера з мережевим обладнанням

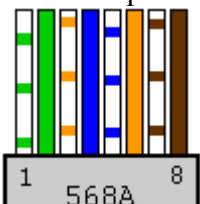
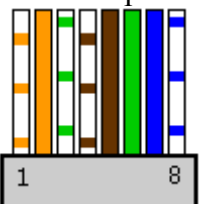
EIA/TIA-568B	перший	колір провода	другий	EIA/TIA-568B	перший	колір провода	другий
	1	біло-оранжевий (TX+)	1		1	біло-оранжевий (TX+)	1
	2	оранжевий (TX-)	2		2	оранжевий (TX-)	2
	3	біло-зелений (RX+)	3		3	біло-зелений (RX+)	3
	4	синій	4		4	синій	4
	5	біло-синій	5		5	біло-синій	5
	6	зелений (RX-)	6		6	зелений (RX-)	6
	7	біло-коричневий	7		7	біло-коричневий	7
	8	коричневий	8		8	коричневий	8

Таблиця 3.2. – Крос-лінковий

EIA/TIA-568B	перший	колір провода	другий	колір провода	EIA/TIA-568A
перший коннектор 	1	біло-оранжевий (TX+)	3	біло-зелений (RX+)	другий коннектор 
	2	оранжевий (TX-)	6	зелений (RX-)	
	3	біло-зелений (RX+)	1	біло-оранжевий (TX+)	
	4	синій	4	синій	
	5	біло-синій	5	біло-синій	
	6	зелений (RX-)	2	оранжевий (TX-)	
	7	біло-коричневий	7	біло-коричневий	
	8	коричневий	8	коричневий	

Рідше використовуються більш важкі для запам'ятовування варіанти розведення 568a-568ах.

Таблиця 3.4 – 568a-568ах

EIA/TIA-568A	перший	колір провода	другий	колір провода	EIA/TIA-568A
перший коннектор 	1	біло-зелений (TX+)	3	біло-оранжевий (RX+)	другий коннектор 
	2	зелений (TX-)	6	оранжевий (RX-)	
	3	біло-оранжевий (RX+)	1	біло-зелений (TX+)	
	4	синій	7	біло-коричневий	
	5	біло-синій	8	коричневий	
	6	оранжевий (RX-)	2	зелений (RX-)	
	7	біло-коричневий	4	синій	
	8	коричневий	5	біло-синій	

## Налаштування IP-адрес в ОС Linux

Отримавши права користувача `root`, створіть і налаштуйте на двох комп'ютерах мережеві інтерфейси, присвоївши їм відповідні IP-адреси. Налаштування полягає в присвоєнні відповідних адрес мережевому пристрою і установці потрібних значень для інших параметрів мережевого пристрою. Найбільш часто для цього використовується програма *ifconfig*.

```
root# ifconfig eth0 192.168.0.1 netmask 255.255.255.0 up
```

В цьому випадку мережевому пристрою *eth0* буде присвоєна IP-адреса 192.168.0.1 і маска 255.255.255.0. Ключ *up* в кінці команди робить інтерфейс активним. Ця дія за замовчуванням, тому Ви можете пропустити цей ключ. Для деактивації інтерфейсу використовуйте команду `ifconfig eth0 down`.

Для перевірки з'єднання можна використати команду `ping`.

Синтаксис команди

```
/usr/sbin/ping хост [таймаут]  
/usr/sbin/ping -s [-drvRlfnq] [-i час очікування] [-p шаблон]  
хост [розмір_даних [кількість_пакетів]]
```

Команда **ping** використовує датаграму ECHO\_REQUEST протоколу ICMP, щоб викликати відповідь ICMP ECHO\_RESPONSE вказаного хоста або мережевого шлюзу. Якщо хост відповідає, **ping** видає повідомлення, що хост живий (**хост is alive**), в стандартний вихідний потік і завершує роботу. В іншому випадку, після **таймаут** секунд вона видає повідомлення, що від хоста відповіді немає (**no answer from хост**). Стандартне значення тайм-ауту - 20 секунд.

## ХІД РОБОТИ

### Завдання 1. Апаратний рівень

Cross-over ("нуль хабний") - використовується для з'єднання двох комп'ютерів через мережні карти, прямо, тобто не використовується ні хаб, ні комутатор. У такий спосіб ви можете підключити тільки два комп'ютери одночасно, для підключення трьох і більш буде потрібно хаб чи деякий тип комутатора.

Послідовність дій для приєднання конектора до кабелю витой пари:

1. Відріжте необхідний по довжині шматок кабелю.
2. Зніміть ізоляцію приблизно на один дюйм.
3. Розплетіть жили кабелю, відсортуйте їх по кольорах згідно стандарту і

переконаєтесь, щоб вони були прямими і рівними

4. Вставте кабель в конектор і обіжміть кабель.

### Завдання 2. Програмний рівень

1. Підготувати обернений кабель, занотувати у звіті черговість (номери) під'єднання і кольори мідних з'єднань.

2. Об'єднайте 2 комп'ютери і налаштуйте на двох комп'ютерах мережеві інтерфейси, присвоївши їм відповідні IP-адреси, згідно номеру варіанту (НВ) по шаблону для 1-го ПК - 192.168.НВ.НВ, для 2-го ПК - 192.168.НВ.НВ+1 із маскою 255.255.255.0

3. Запустіть команду `ping` між комп'ютерами.

4. Ознайомитись із властивостями ярлика „Мій комп'ютер”, уважно дослідити закладки „Віддалені сеанси”, та ім'я комп'ютера.

5. Дослідити властивості “Мережевого оточення”, визначивши клієнтів служби та протоколи, які використовуються, а також назву мережевої карти, яка присутня в комп'ютері.

6. Створити на диску C в папці Share\_doc власну папку.

7. Через „Мережеве оточення” → „Вся мережа” → “Microsoft Windows Network” → подивитись, які робочі групи в мережі і спробувати під'єднати папку Share\_doc сусіднього

комп'ютера як мережевий диск M. Перевірити чи цей диск з'явився в папці „Мій комп'ютер”.

8. Використовуючи будь-який файл-менеджер (Far, Windows Commander, Midnight Commander etc.) переписати по мережі файл або папку (розміром не менше 4 Гб), занотувати швидкість запису.

9. Паралельно в диспетчері задач додати всі колонки, які стосуються мережі і також відслідкувати швидкість передачі файлу.

### ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Хід виконання лабораторної роботи та копії екранів
3. Висновки по виконаній роботі.

### КОНТРОЛЬНІ ПИТАННЯ

1. Опишіть характеристики фізичного середовища передачі сигналу ?
2. Назвіть стандарти обжимання роз'ємів витой пари?
3. Опишіть синтаксис і призначення команди ping.
4. Опишіть налаштування мережевого середовища в ОС Windiws.

## ЛАБОРАТОРНА РОБОТА 4

### ДОСЛІДЖЕННЯ МЕРЕЖЕВИХ ВЛАСТИВОСТЕЙ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS.

Мета роботи: Ознайомитись з мережевими налаштуваннями операційної системи Windows.

#### ТЕОРЕТИЧНІ ВІДОМОСТІ.

##### 1.1 Інтерфейс командного рядка CLI

Windows також має інтерфейс командного рядка (CLI, «консоль»), cmd.exe, для управління системою командами з консолі або запуску сценаріїв, званих «командними файлами» (з розширеннями cmd), заснованими на «пакетних» (batch) файлах MS-DOS. Синтаксис Windows CLI не дуже добре задокументований у вбудованій системі допомоги. Докладнішу загальну інформацію можна отримати, набравши в командному рядку «help» для отримання загальних відомостей про доступні команди і «ім'я команди /?».

Інтерфейс командного рядка доступний як у вигляді вікна, так і в повноекранному вигляді (перемикання між ними здійснюється натисненням Alt+Enter), вигляд, що віддається перевага, можна вказати у відповідному діалозі настройки, разом з такими параметрами, як розмір і тип шрифтів і т. д. При роботі в даному режимі користувач може викликати попередні команди (так, клавіша «вгору» повертає попередню команду), використовувати автодоповнення імен файлів і каталогів, а також команд. Багато дій з управління операційною системою можна виконати, використовуючи інтерфейс CLI. Найважливішими з них є команди:

- «**net**» з підкомандами, що дозволяє управляти локальними користувачами і групами («net user /?» і inet localgroup /?»), аккаунтами, загальним доступом до ресурсів на ПК («net share /?») і в мережі («net view /?») і т. д.
- Команди перегляду і управління процесами «**tasklist** /?» і «**taskkill** /?»
- Команда управління дозволами файлів " **cacls** /? ", що дозволяє переглядати і змінювати права доступу до файлів і тек (у Home Edition – це єдина можливість гнучко змінювати має рацію, оскільки відповідний графічний інструмент доступний тільки в безпечному режимі)
- а також команди, аналогічні командам «Командної мови» DOS, дозволяють копіювати, переміщати і видаляти файли і каталоги і т. д.
- **ping** – це службова комп'ютерна програма, призначена для перевірки з'єднань в мережах на основі TCP/IP.

##### Утиліта Ping.

Утиліта Ping відправляє запити Echo-Request протоколу ICMP зазначеному вузлу мережі й фіксує відповіді (ICMP Echo-Reply). Час між відправленням запиту й одержанням відповіді (RTT, від англ. Round Trip Time) дозволяє визначати *двосторонні затримки* (RTT) у маршруті й частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв.

Повна відсутність ICMP-відповідей може також означати, що віддалений вузол (або якийсь із проміжних маршрутизаторів) блокує ICMP Echo-Reply або ігнорує ICMP Echo-Request.

Програма ping є одним з основних діагностичних засобів у мережах TCP/IP і входить у поставку всіх сучасних мережесистем. Функціональність ping також реалізована в деяких вбудованих ОС маршрутизаторів, доступ до результатів виконання ping для таких пристроїв за протоколом SNMP визначається RFC 2925 (Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations).

Практичне застосування:

- можна взяти IP-адресу по доменному імені;
  - можна перевірити, чи є зв'язок з сервером;
  - перевірити якість каналу, подивившись, скільки пакетів не дійшло або час відклику.
- Термін пінг зазвичай використовується для опису передачі будь-якого повідомлення або

сигналу з метою виявлення і тестування мережевих послуг або функцій. Наприклад, пінг може бути надіслано за допомогою User Datagram Protocol (UDP) до пристрою, розташованого за транслятор мережевих адрес (NAT), щоб порт обов'язковими для NAT по тайм-ауту та видалення відображення. Інші приклади короткі або порожні миттєві повідомлення, електронну пошту, голосову пошту, або пропущених викликів, повідомлення, щоб вказати, доступність. У різних мережевих багатокористувацьких ігор, ping відеоігри виконує аналогічні функції, як ping програми для Інтернет-трафіку. Ігровий сервер вимірює час, необхідний для гри пакет для досягнення клієнта і відповідь буде отримана. Цей час прийому-передачі, як правило, називають, як ping гравця.

#### **Утиліта tracert**

Tracert - це службова комп'ютерна програма, призначена для визначення маршрутів прямування даних в мережах TCP / IP. Traceroute може використовувати різні протоколи передачі даних в залежності від операційної системи пристрою. Такими протоколами можуть бути UDP, TCP, ICMP або GRE. Комп'ютери, зі встановленою операційною системою Windows використовують ICMP протокол, при цьому маршрутизатори Cisco - протокол UDP.

#### **1.4 Утиліта ipconfig**

Ipconfig - утиліта командного рядка для управління мережевими інтерфейсами (налаштування, перевірка).

В операційних системах Microsoft Windows ipconfig - це утиліта командного рядка для виводу деталей поточного з'єднання і управління клієнтськими сервісами DHCP і DNS. Також є подібні графічні утиліти з назвами winipcfg і wntipcfg (остання передувала ipconfig). Утиліта ipconfig дозволяє визначати, які значення конфігурації були отримані за допомогою DHCP, APIPA або іншої служби IP-конфігурування або задані адміністратором вручну.

Часто в операційних системах Linux і UNIX деталі з'єднання відслідковуються декількома утилітами, головною серед них є ifconfig. Тим не менш, ipconfig поряд з ifconfig присутній в Mac OS X, там ipconfig команда сервісу як оболонка до агента IPConfiguration і може використовуватися для контролю BootP і DHCP клієнта з CLI.

#### **Утиліта netstat**

**Утиліта netstat** визначення кількості *відкритих сесій*. Також показує вміст різних структур даних, пов'язаних з мережею, в різних форматах в залежності від зазначених опцій. Використання

Перша форма команди показує список *активних сокетів* (sockets) для кожного протоколу. Друга форма вибирає одну з декількох інших мережевих структур даних. Третя форма показує динамічну статистику пересилання пакетів по сконфігурованим мережевим інтерфейсами; аргумент інтервал задає, скільки секунд збирається інформація між послідовними показами. Значення за замовчуванням для аргументу система - / unix; для аргументу core як значення за замовчуванням використовується / dev / kmem.

#### **Функція ARP**

Функція ARP. Визначення параметрів канального рівня.

Опис протоколу було опубліковано в листопаді 1982 року в RFC 826. ARP був спроектований для випадку передачі IP-пакетів через сегмент Ethernet. При цьому загальний принцип, запропонований для ARP, може, і був використаний і для мереж інших типів.

Існують такі типи повідомлень ARP: запит ARP (ARP request) і відповідь ARP (ARP reply). Система-відправник за допомогою запиту ARP запитує фізичну адресу системи-одержувача. Відповідь (фізичну адресу вузла-одержувача) приходить у вигляді відповіді ARP.

Перед тим як передати пакет мережевого рівня через сегмент Ethernet, мережевий стек перевіряє кеш ARP, щоб з'ясувати, не зареєстрована в ньому вже потрібна інформація про вузол-одержувачі. Якщо такого запису в кеші ARP ні, то виконується широкомовна запит ARP. Цей запит для пристроїв в мережі має наступний зміст: «Хто-небудь знає фізичну адресу пристрою, який володіє таким IP-адресою?» Коли одержувач з цим IP-адресою прийме цей пакет, то повинен буде відповісти: «Так, це мій IP-адресу . Мій фізичний адресу



наступний: ... »Після цього відправник оновить свій кеш ARP і буде здатний передати інформацію одержувачу. Нижче наведено приклад запиту і відповіді ARP. <См. внизу сторінки>

Записи в кеші ARP можуть бути статичними і динамічними. Приклад, даний вище, описує динамічну запис кеша. Можна також створювати статичні записи в таблиці ARP. Це можна зробити за допомогою команди:

arp-s <IP-адрес> <MAC-адрес>

Записи в таблиці ARP, створені динамічно, залишаються в кеші протягом 2-х хвилин. Якщо протягом цих двох хвилин сталася повторна передача даних за цією адресою, то час зберігання запису в кеші продовжується ще на 2 хвилини. Ця процедура може повторюватися до тих пір, поки запис в кеші проіснує до 10 хвилин. Після цього запис буде видалена з кеша, і буде відправлений повторний запит ARP.

## ХІД РОБОТИ

1. Виконати команду “Пуск” → “Виконати” → “**cmd**” і натиснути ОК. (Командний режим: будь-яка команда виконана із ключем „/?” – надає всі ключі із їх описами). Виконати в ньому команду “**ipconfig**” з ключем /all. Визначити ім’я комп’ютера, опис мережевої карти, фізичний адрес комп’ютера (MAC-адрес), IP адрес комп’ютера, маску підмережі, основний шлюз та сервер DNS.

2. Запустити в командному вікні команду „**ping**” з IP адресом сусіднього комп’ютера лабораторії, і визначити затримку між комп’ютерами. Змінити розмір пакета та час затримки і повторити команду. Виконати команду трасування шляху до серверів університету (проксі, поштовий, веб, ftp) при допомозі команди “**tracert**”.

3. Запустити в командному рядку команду “**netstat**” із ключами „-aon”, переглянути всі номери tcp/udp портів на яких працюють служби ОС, визначити номери портів, які використовують програми для під’єднання до зовнішніх серверів (веб,ftp,пошта тощо). Виконати команду “**tasklist**”, яка виводить всі запущені процеси і по параметру PID визначити процеси, які слухають на портах.

4. Виконати команду “**route print**” і переглянути таблицю маршрутизації ОС, додати запис в таблицю маршрутизації при допомозі команди “**route add**”, а потім видалити цей запис командою “**route del**”.

5. Виконати команду “**arp**” із різними ключами і переглянути таблиці відповідності MAC та IP адрес.

6. При допомозі командного режиму відіслати повідомлення на сусідній комп’ютер, за допомогою команди net send 10.xx.xx.xx.

7. Створити у редакторі (наприклад блокнот) файл із розширенням **.cmd** і помістити у нього всі команди (ping, tracert, ipconfig, route, netstat, tasklist). Цей командний файл має питати IP-адресу, яка буде пінгуватись і проходити трасування, а також автоматично вибирати і виводити імена служб які слухають на портах tcp/udp. Також командний файл має виводити результат виконання в файл звіту.

8. Результати оформити в звіт і роздрукувати.

## ЗМІСТ ЗВІТУ.

- 3.1. Тема та мета лабораторної роботи;
- 3.2. Хід роботи із копіями екрану;
- 3.3. Висновки по виконаній роботі.

#### КОНТРОЛЬНІ ЗАПИТАННЯ.

- 4.1. Призначення команди ping;
- 4.2. Призначення команди tracert;
- 4.3. Призначення команди ipconfig;
- 4.4. Призначення команди route;
- 4.5. Призначення команди netstat;
- 4.6. Призначення команди tasklist;
- 4.7 Адресація вузлів мережі для стеку протоколів TCP/IP

## ЛАБОРАТОРНА РОБОТА 5

### ПОБУДОВА ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ

Мета роботи: налаштувати віртуальні локальні мережі на комутаторах D-Link

### ТЕОРЕТИНІ ВІДОМОСТІ

Віртуальна локальна мережа (Virtual Local Area Network, VLAN) являє собою комутований сегмент мережі, який логічно виділений по виконуваних функціях, робочих групах або застосуваннях, незалежно від фізичного розташування користувачів. Віртуальні локальні мережі мають усі властивості фізичних локальних мереж, але робочі станції можна групувати, навіть якщо вони фізично розташовані не в одному сегменті, тому що будь-який порт комутатора можна настроїти на приналежність певної VLAN. При цьому одноадресний, багатоадресний і ширококомовний трафік буде передаватися тільки між робочими станціями, що належать одній VLAN. Кожна VLAN розглядається як логічна мережа, тобто пакети, призначені станціям, які не належать даній VLAN, повинні передаватися через маршрутизуючий пристрій (маршрутизатор або комутатор 3-го рівня). Таким чином, за допомогою віртуальних локальних мереж вирішується проблема обмеження області передачі ширококомовних пакетів і викликаних ними наслідків, які суттєво знижують продуктивність мережі, викликають ширококомовні шторми.

Типи VLAN:

- *VLAN на основі портів (Port-based VLAN)* - кожен порт комутатора призначається в певну VLAN і будь-який мережний пристрій, підключений в даний порт, буде знаходитись в призначеній віртуальній мережі;

- *VLAN на основі Mac-Адрес (Mac-based VLAN)* - членство в VLAN ґрунтується на MAC-Адресі робочої станції. У цьому випадку на комутаторі необхідно створити прив'язку MAC-Адрес усіх пристроїв до VLAN;

- *VLAN на основі портів і протоколів IEEE 802.1v* - тип протоколу й порт використовуються для визначення членства в VLAN;

- *VLAN на основі стандарту IEEE 802.1Q* - поле приналежності VLAN, інтегрується в структуру кадра Ethernet, що дозволяє передавати дану інформацію по мережі. Перевагою є гнучкість налаштування, використання не тільки на одному комутаторі, але й у межах усієї мережі, що комутується; можливість використання встаткування різних виробників при організації мережі. Даний тип VLAN використовується частіше інших.

Існують два методи призначення порту в певну VLAN:

- статичне призначення - коли приналежність порту VLAN задається адміністратором у процесі налаштування;

- динамічне призначення - коли приналежність порту VLAN визначається в ході роботи комутатора за допомогою процедур, описаних у спеціальних стандартах, таких, наприклад, як IEEE 802.1X. При використанні IEEE 802.1X для одержання доступу до порту комутатора, користувач проходить аутентифікацію на сервері RADIUS. За результатами аутентифікації порт комутатора міститься в ту або іншу VLAN.

Основні визначення IEEE 802.1Q:

- Tag («Тег») - додаткове поле даних довжиною 4 байта, що містить інформацію про VLAN, що й додається в кадр Ethernet. Перші 2 байта містять фіксоване значення 0x8100, інші 2 байта містять ідентифікатор VLAN (12 біт), поле пріоритету (3 біта), поле індикатору канонічного формату (1 біт);

- Tagging («Маркування кадра») - процес додавання інформації (тегу) про приналежність до 802.1Q VLAN у заголовок кадра;

- Untagging («Видалення тегу з кадра») - процес добування інформації 802.1Q VLAN із заголовка кадра;

- Ingress port («Вхідний порт») - порт комутатора, на який надходять кадри, і приймається рішення про приналежність VLAN;

– *Egress port* («Вихідний порт») - порт комутатора, з якого кадри передаються на інші мережні пристрої (комутатори, робочі станції) і на ньому, відповідно, приймається рішення про маркування кадра.

Будь-який порт комутатора може бути настроєний як *tagged* (маркований) або як *untagged* (немаркований). Функція *untagging* дозволяє працювати з тими мережними пристроями віртуальної мережі, які не розуміють тегів у заголовку кадра Ethernet. Функція *tagging* дозволяє налаштувати VLAN між декількома комутаторами, що підтримують стандарт IEEE 802.1Q, підключати мережні пристрої, що розуміють IEEE 802.1Q (наприклад, сервери з мережними інтерфейсами з підтримкою 802.1Q), забезпечувати можливість створення складних мережних інфраструктур.

## ХІД РОБОТИ

Устаткування: комутатори D-Link 2 шт., робоча станція 8 шт., кабель Ethernet 12 шт.

Перед виконанням завдання необхідно скинути налаштування комутаторів до заводських налаштувань за замовчуванням командою `reset config`

Завдання 1.

Побудувати схему уф hсbeure 5.1

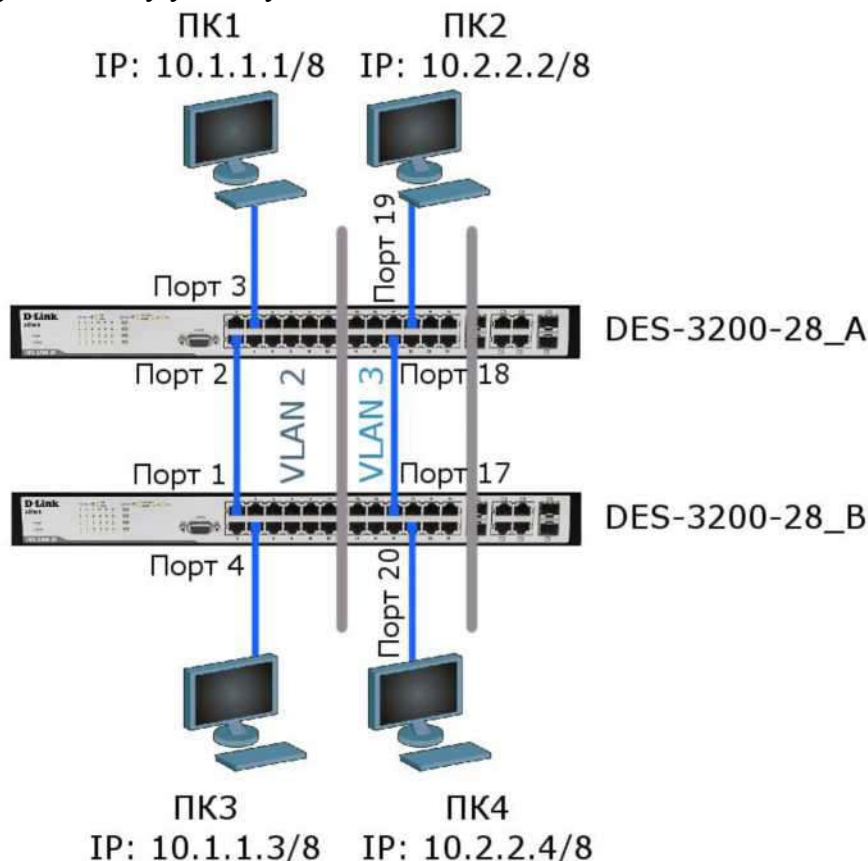


Рисунок 5.1 – Схема з'єднання обладнання №1

### 1.1. Налаштування DES-3200-28\_A

Видаліть порти з VLAN за замовчуванням для використання в інших VLAN  
`config vlan default delete 1-24`

Створіть VLAN v2 і v3, додайте у відповідні VLAN порти, які необхідно настроїти немаркованими

```
create vlan v2 tag 2  
config vlan v2 add untagged 1-12
```

```
create vlan v3 tag 3
config vlan v3 add untagged 13-24
```

### 1.2. Налаштування DES-3200-28\_B

Видаліть порти з VLAN за замовчуванням для використання в інших VLAN

```
config vlan default delete 1-24
```

Створіть VLAN v2 і v3, додайте у відповідні VLAN порти, які необхідно налаштувати немаркованими

```
create vlan v2 tag 2
config vlan v2 add untagged 1-12
create vlan v3 tag 3
config vlan v3 add untagged 13-24
```

Перевірте налаштування VLAN на обох комутаторах

```
show vlan
```

Перевірте доступність з'єднання командою ping:

- від ПК1 до ПК3
- від ПК2 до ПК4
- від ПК1 до ПК2 і ПК4
- від ПК2 до ПК1 і ПК3

```
ping <IP-address>
```

## Завдання 2. Налаштування VLAN на основі стандарту IEEE 802.1Q

Побудуйте схему 2 на рисунку 5.2.

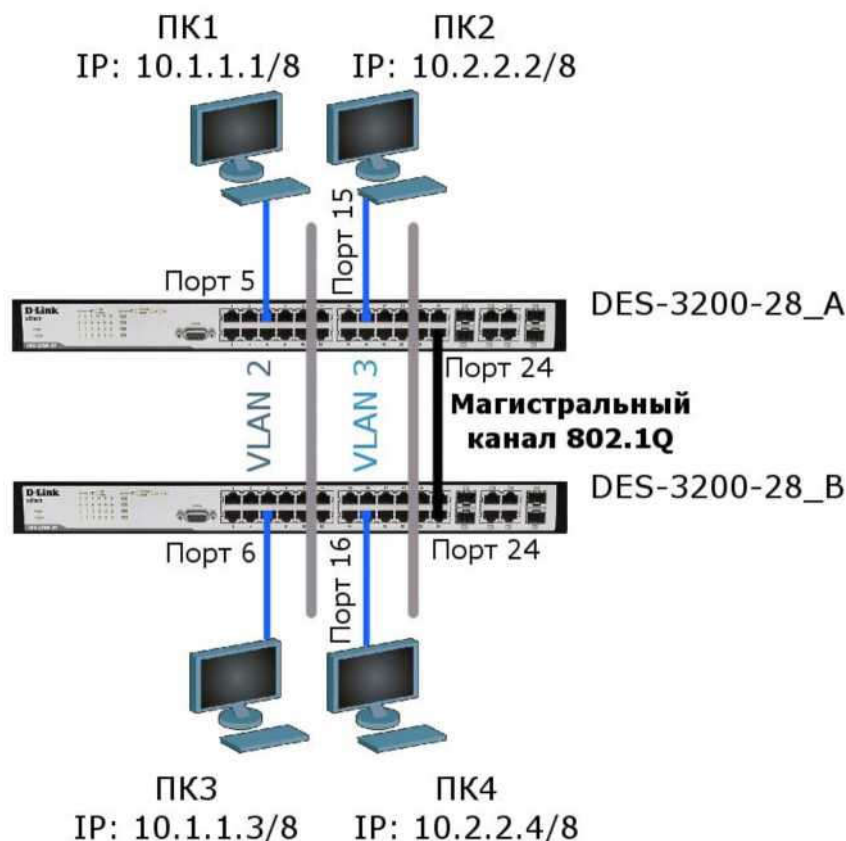


Рисунок 5.2 – Схема з'єднання обладнання №2

### 2.1. Налаштування DES-3200-28\_A

Скиньте налаштування комутатора до заводських налаштувань за замовчуванням

```
reset config
```

Видаліть порти з VLAN за замовчуванням для використання в інших VLAN

```
config vlan default delete 1-24
```

Створіть VLAN v2 і v3, додайте у відповідні VLAN порти, які необхідно настроїти немаркованими. Налаштуйте порт 24 маркованим

```
create vlan v2 tag 2
config vlan v2 add untagged 1-10
config vlan v2 add tagged 24
create vlan v3 tag 3
config vlan v3 add untagged 11-20
config vlan v3 add tagged 24
```

## 2.2. Налаштування DES-3200-28 В

Скиньте налаштування комутатора до заводських налаштувань за замовчуванням

```
reset config
```

Видаліть порти з VLAN за замовчуванням для використання в інших VLAN

```
config vlan default delete 1-24
```

Створіть VLAN v2 і v3, додайте у відповідні VLAN порти, які необхідно настроїти немаркованими. Налаштуйте порт 24 маркованим

```
create vlan v2 tag 2
config vlan v2 add untagged 1-10
config vlan v2 add tagged 24
create vlan v3 tag 3
config vlan v3 add untagged 11-20
config vlan v3 add tagged 24
```

Перевірте налаштування VLAN на обох комутаторах

```
show vlan
```

Перевірте доступність з'єднання командою ping:

- від ПК1 до ПК3
- від ПК2 до ПК4
- від ПК1 до ПК2 і ПК4
- від ПК2 до ПК1 і ПК3

```
ping <IP-address>
```

## Завдання 3. Оптимізація налаштування комутаторів з більшою кількістю VLAN

Метою даного завдання є вивчення команд оптимізації роботи при створенні, видаленні, конфігуруванні множини VLAN. На рисунку 5.3 наведено схему 3.

### 3.1. Налаштування DES-3200-28\_A

Скиньте налаштування комутатора до заводських налаштувань за замовчуванням

```
reset config
```

Видаліть порти з VLAN за замовчуванням для використання в інших VLAN

```
config vlan vlanid 1 delete 1-24
```

Створіть двадцять VLAN с тегами з 2 по 21

```
create vlan vlanid 2-21
```

Примітка. При створенні VLAN імена надаються по шаблону: VLAN x (де x - тег створеної VLAN).

Додайте марковані порти в декілька VLAN, включіть функцію оповіщення (advertisement) про створені VLAN

```
config vlan vlanid 2-21 add tagged 1-24 advertisement enable
```

Перевірте виконані дії

```
show vlan
```

Що ви спостерігаєте? Запишіть:

Видаліть порти з декількох VLAN

```
config vlan vlanid 2-21 delete 1-24
```

Змініть ім'я VLAN і додайте немарковані порти

```
config vlan vlanid 11 name SALE add untagged 1-4
config vlan vlanid 15 name SECURITY add untagged 5-8
config vlan vlanid 18 name MANAGER add untagged 9-11
config vlan vlanid 19 name LOGIST add untagged 12-16
```

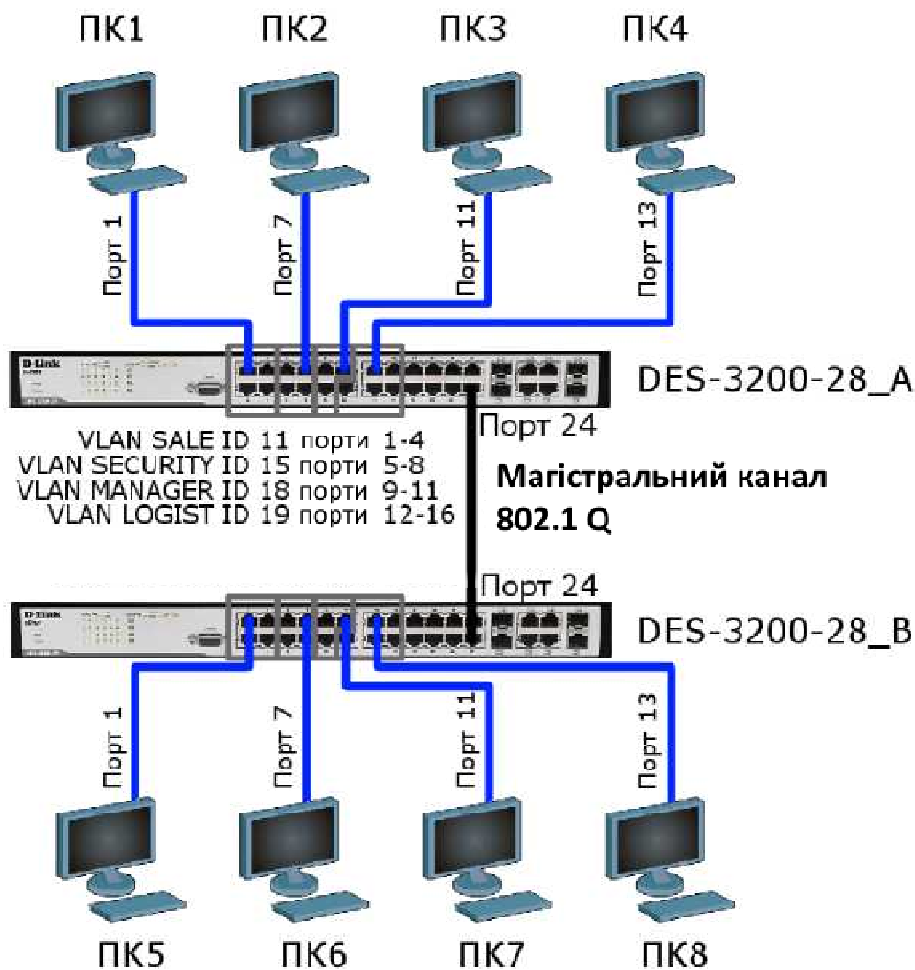


Рисунок 5.3 – Схема мережі №3

Перевірте виконані дії

```
show vlan
```

Призначте магістральний порт передачі VLAN

```
config vlan trunk ports 24 state enable
```

Перевірте виконані дії

```
show vlan trunk
```

Включіть можливість роботи магістрального порту

```
enable vlan trunk
```

Прмітка При налаштуванні порту в якості магістрального (vlan\_trunk) через нього можна передавати кадри з VID с 1-4094; порт динамічно додається в усі доступні VLAN як маркований

### 3.1. Налаштування DES-3200-28\_B

Скиньте налаштування комутатора до заводських налаштувань за замовчуванням

```
reset config
```

Видаліть порти з VLAN за замовчуванням для використання в інших VLAN

```
config vlan vlanid 1 delete 1-24
```

Створіть десять VLAN с тегами з 10 по 19

```
create vlan vlanid 10-19
```

Змініть ім'я VLAN і додайте немарковані порти

```
config vlan vlanid 11 name SALE add untagged 1-4 config vlan
```

```
vlanid 15 name SECURITY add untagged 5-8
```

```
config vlan vlanid 18 name MANAGER add untagged 9-11
```

```
config vlan vlanid 19 name LOGIST add untagged 12-16
```

Перевірте виконані дії

```
show vlan
```

Призначте магістральний порт передачі VLAN

```
config vlan trunk ports 24 state enable
```

Включіть можливість роботи магістрального порту

```
enable vlan trunk
```

Перевірте виконані дії

```
show vlan trunk
```

Перевірте доступність з'єднання командою ping:

- від ПК1 до ПК2 (Vlan SALE)

- від ПК3 до ПК4 (Vlan SECURITY)

- від ПК5 до ПК6 (Vlan MANAGER)

- від ПК7 до ПК8 (Vlan LOGIST)

- між станціями сусідніх VLAN

```
ping <Ip-address>
```

Що ви спостерігаєте? Запишіть

Відключіть магістральні порти на комутаторах А і В

```
disable vlan_trunk
```

### ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Короткі теоретичні відомості.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

### КОНТРОЛЬНІ ЗАПИТАННЯ

1. Призначення віртуальних локальних мереж (Virtual Local Area Network, VLAN)?
2. Які існують типи VLAN?
3. Що визначає стандарт IEEE 802.1Q?
4. Що таке транк?



## ЛАБОРАТОРНА РОБОТА 6.

### ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ МЕРЕЖІ В CISCO PACKET TRACER

Мета роботи: ознайомлення із пакетом Cisco Packet Tracer

### ТЕОРЕТИЧНІ ВІДОМОСТІ

Інтерфейс Cisco Packet Tracer. Головне вікно Cisco Packet Tracer, зображено на рисунку 6.1. Інтерфейс програми, розділений на області.

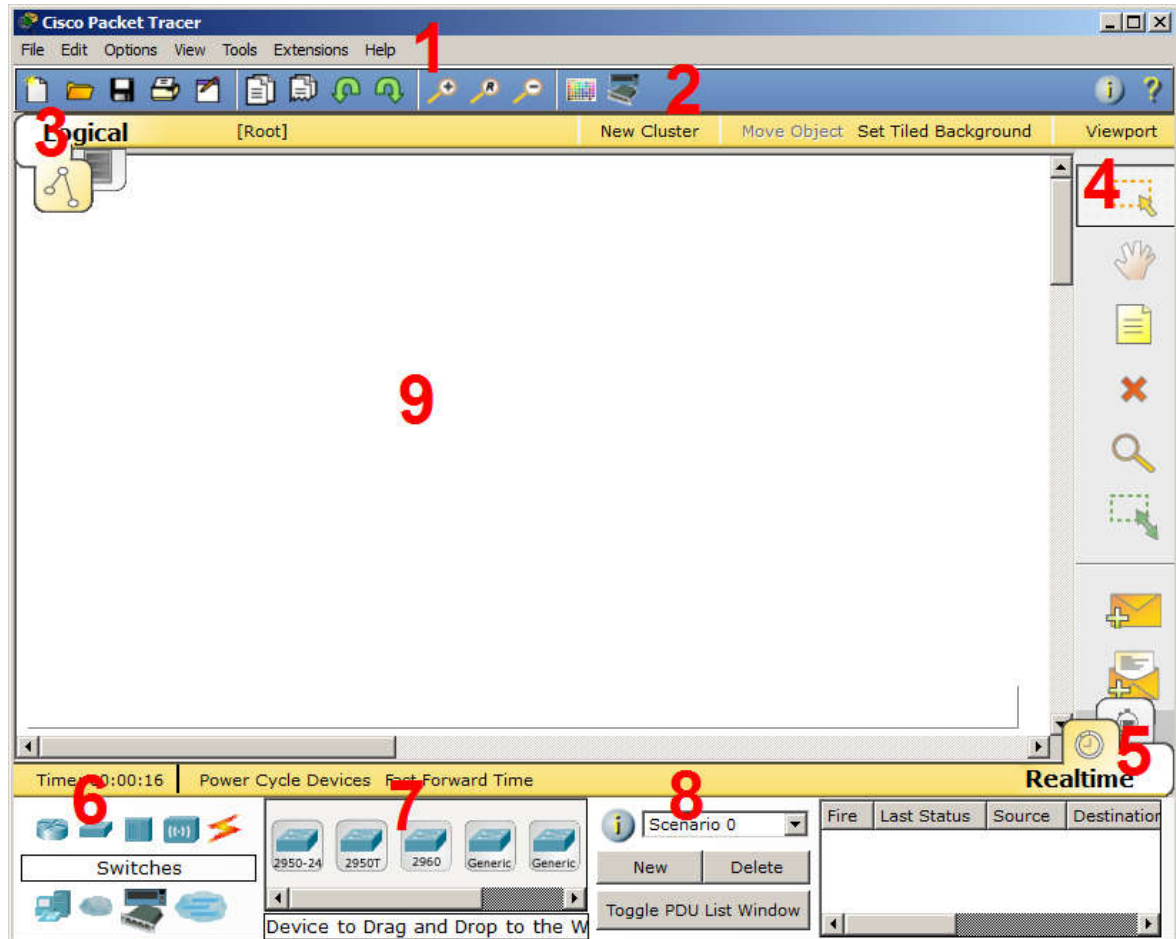


Рисунок 6.1 - Інтерфейс програми Cisco Packet Tracer.

1. Головне меню програми з наступним змістом:

- Файл - містить операції відкриття / збереження документів;
- Виправлення - стандартні операції "копіювати / вирізати, скасувати / повторити";
- Налаштування - говорить сама за себе;
- Вид - масштаб робочої області і панелі інструментів;
- Інструменти - колірна палітра і кастомізація кінцевих пристроїв;
- Розширення - майстер проектів, розрахований на багато користувачів режим і кілька

прибуд, які з СРТ (так я іноді буду ласкаво називати Cisco Packet Tracer) можуть зробити цілу лабораторію;

- Допомога - ні за що не вгадаєте, що там міститься;

2. Панель інструментів, частина яких просто дублює пункти меню;

3. Переключає між логічного і зниження фізичної організації;

4. Ще одна панель інструментів, містить інструменти виділення, видалення, переміщення, масштабування об'єктів, а так само формування довільних пакетів;

5. Перемикач між реальним режимом (Real-Time) і режимом симуляції;

6. Панель з групами кінцевих пристроїв і ліній зв'язку;

7. Самі кінцеві пристрої, тут містяться всілякі комутатори, вузли, точки доступу, провідники.
8. Панель створення призначених для користувача сценаріїв;
9. Робочий простір.

Приклад розміщення колірних областей (рисунок 6.2), що дозволяє наприклад відокремлювати візуально одну підмережу від іншої.

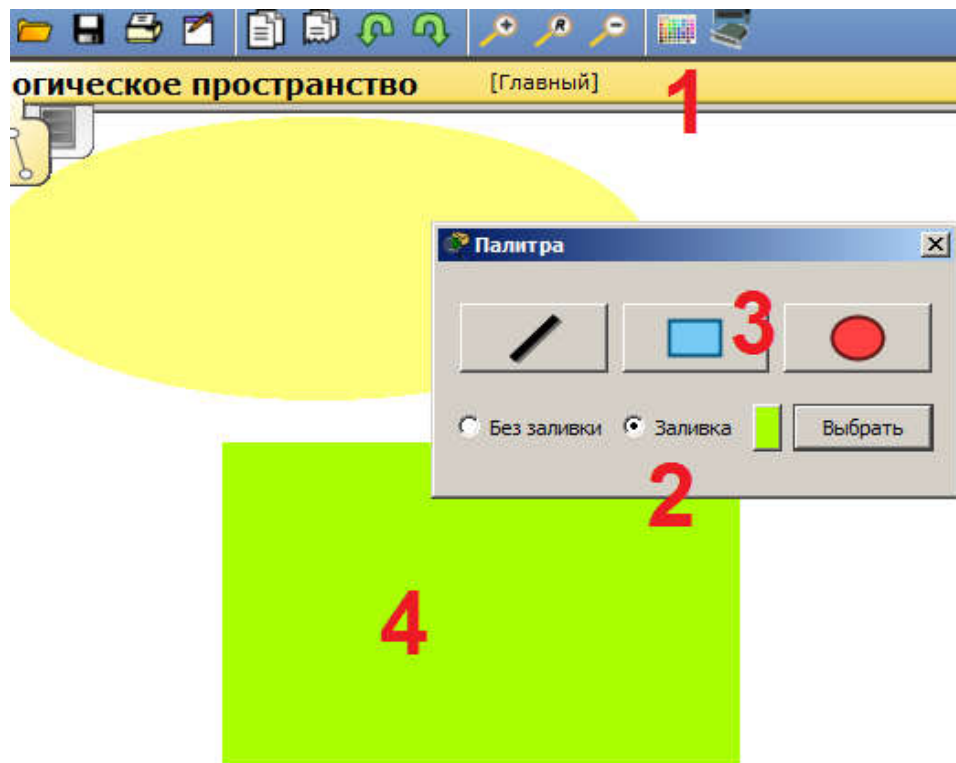


Рисунок 6.2 – Приклад розміщення колірних областей.

Для установки кольорових областей виконайте наступні дії:

- 1 - На панелі інструментів вибираємо відповідний значок;
- 2 - Вибираємо режим області "Заливка", наприклад;
- 3 - Вибираємо колір і форму;
- 4 - Малюємо область на робочому просторі.

Можна також додати підпис і переміщати / масштабувати цю область.

### Устаткування і лінії зв'язку в Cisco Packet Tracer

**Маршрутизатор** використовується для пошуку оптимального маршруту передачі даних на підставі спеціальних алгоритмів маршрутизації, наприклад вибір маршруту (шляху) з найменшим числом транзитних вузлів. Працюють на мережевому рівні моделі OSI.



Рисунок 6.3 – Маршрутизатор

**Комутатори** - це пристрої, що працюють на каналному рівні моделі OSI і призначені для об'єднання декількох вузлів в межах одного або декількох сегментах мережі. Передає пакети комутатор на підставі внутрішньої таблиці - таблиці комутації, отже трафік йде тільки на той MAC-адресу, якій він призначається, а не повторюється на всіх портах (як на концентраторі).



Рисунок 6.4 – Комутатор

Концентратор повторює пакет, прийнятий на одному порту на всіх інших портах.



Рисунок 6.5 – Концентратор

Безпроводні технології Wi-Fi і мережі на їх основі. Включає в себе точки доступу.



Рисунок 6.6 – Точки доступу



Рисунок 6.7 – Лінії зв'язку









За допомогою цих компонентів створюються з'єднання вузлів в єдину схему. Packet Tracer підтримує широкий діапазон мережевих з'єднань (див. таблицю 5.1). Кожен тип кабелю може бути з'єднаний лише з певними типами інтерфейсів.

На рисунку 6.8 представлені кінцеві вузли, хости, сервера, принтери, телефони і т.д.



Рисунок 6.8 – Лінії зв'язку

Таблиця 6.1 – Типи кабелів.

Тип кабеля	Опис
Консоль 	Консольне з'єднання може бути виконано між ПК і маршрутизаторами або комутаторами. Повинні бути виконані деякі вимоги для роботи консольного сеансу з ПК: швидкість з'єднання з обох сторін повинна бути однаковою, має бути 7 біт даних (або 8 біт) для обох сторін, контроль парності повинен бути однаковий, має бути 1 або 2 степових біта (але вони не обов'язково повинні бути однаковими), а потік даних може бути чим завгодно для обох сторін.
Мідний прямий 	Цей тип кабелю є стандартним середовищем передачі Ethernet для з'єднання пристроїв, який функціонує на різних рівнях OSI. Він повинен бути з'єднаний з наступними типами портів: мідний 10 Мбіт / с (Ethernet), мідний 100 Мбіт / с (Fast Ethernet) і мідний 1000 Мбіт / с (Gigabit Ethernet).
Мідний кросове 	Цей тип кабелю є середовищем передачі Ethernet для з'єднання пристроїв, які функціонують на однакових рівнях OSI. Він може бути з'єднаний з наступними типами портів: мідний 10 Мбіт / с (Ethernet), мідний 100 Мбіт / с (Fast Ethernet) і мідний 1000 Мбіт / с (Gigabit Ethernet).
Оптика 	Оптичне середовище використовується для з'єднання між оптичними портами (100 Мбіт / с або 1000 Мбіт / с).
Телефоний 	З'єднання через телефонну лінію може бути здійснено тільки між пристроями, що мають модемні порти. Стандартне подання модемного з'єднання - це кінцевий пристрій (наприклад, ПК), додзвонюється в мережеву хмара.
Коаксіальний 	Коаксіальне середовище використовується для з'єднання між коаксіальними портами, такі як кабельний модем, з'єднаний з хмарою Packet Tracer
Серійний DCE  Серійний DTE 	З'єднання через послідовні порти, часто використовуються для зв'язків WAN. Для настройки таких з'єднань необхідно встановити синхронізацію на стороні DCE-пристрої. Синхронізація DTE виконується за вибором. Сторону DCE можна визначити по маленькій іконці "годин" поруч з портом. При виборі типу з'єднання Serial DCE, перший пристрій, до якого застосовується з'єднання, ставати DCE-пристроєм, а друге - автоматично стане стороною DTE. Можливо і зворотне розташування сторін, якщо обраний тип з'єднання Serial DTE.

Емуляція Інтернету



Рисунок 6.9 – Хмари

Приклад емуляція глобальної мережі. Модем DSL, "хмара" і т.д.  
Користувачські пристрої та хмара призначені для багатокористувацької роботи.



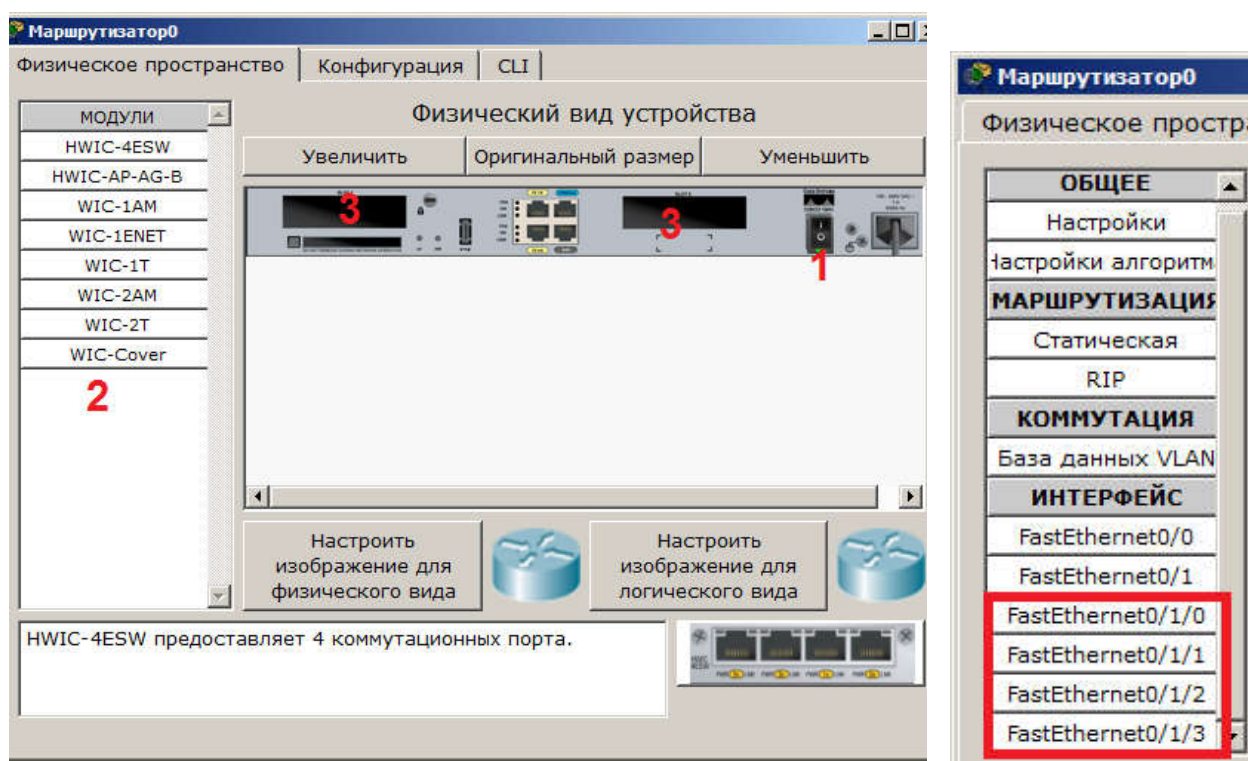


Рисунок 6.10 – Користувачькі пристрої та хмари

Пристрої можна комплектувати самостійно. Можна створювати довільні підключення.

#### Фізична комплектація обладнання.

Встановить в робочому полі маршрутизатор Cisco 1841 В налаштуваннях на роутері відкриваємо його фізичну конфігурацію (рисунок 6.11).



а) конфігурація пристрою

б) додавання інтерфейсів

Рисунок 6.11 – Конфігурація пристрою

Зліва, як ми бачимо, список модулів (цифра 2), якими можна укомплектувати даний маршрутизатор. Зараз в ньому 2 порожнечі (цифра 3). У них можна вкласти ці модулі. Зрозуміло, цю операцію потрібно робити при вимкненому живленні (цифра 1).

Для зміни комплектації устаткування необхідно вимкнути живлення, клікнувши мишкою на кнопці живлення, перетягнути мишею модуль у вільний слот і включити живлення. Почекаати закінчення завантаження роутера. У конфігурації GUI можемо побачити з'явилися 4 нових інтерфейси (рисунок 6.12).

Решта пристроїв комплектуються аналогічно. Додаються нові модулі Ethernet (100/1000), оптоволоконні роз'єми декількох типів, адаптери бездротового мережі. На робочий комп'ютер є можливість додати наприклад мікрофон з навушниками, жорсткий диск для зберігання даних.

## ХІД РОБОТИ

### Режим симуляції.

Cisco Packet Tracer містить інструмент для симуляції роботи мережі, в якому можна імітувати і симулювати стан роботи мережі і практично будь-які мережеві події. Наприклад можна простежити, як реагуватиме мережа в разі збоїв або наприклад що станеться, якщо від'єднати будь-якої кабель або вимкнути живлення одного з мережевих пристроїв.

Режим симуляції дозволяє простежити структуру пакета і переглянути, з якими параметрами пакет проходить за рівнями моделі OSI.

Склад мережі: 4 вузли, сервер, принтер і два концентратора. Концентратори між собою з'єднуються кроссоверним кабелем (рисунок 6.13).

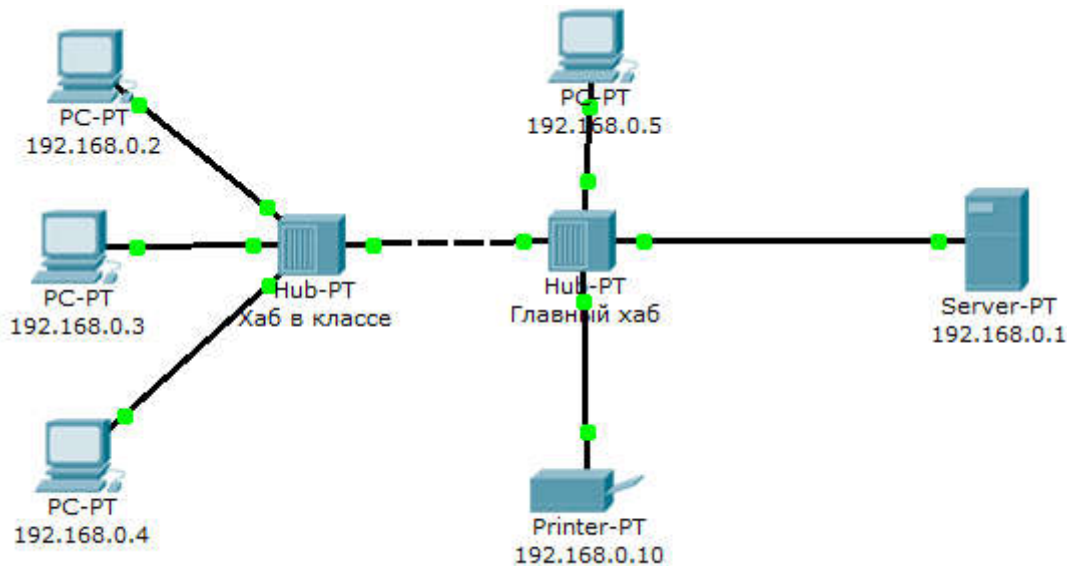


Рисунок 6.13 – Схема мережі.

Потрібно перейти в режим симуляції (Shift + S), або клікнувши на іконку симуляції в правому нижньому кутку робочого простору. Тут ми бачимо вікно подій, кнопка скидання (очищає список подій), управління відтворенням і фільтр протоколів. Запропоновано багато протоколів, але відфільтруємо поки тільки ICMP, це виключить випадковий трафік між вузлами.

Для переходу до наступної події використовуємо кнопку "Вперед", або автоматика (Рисунок 6.14).

Надсилаємо PING-запит. З одного з вузлів спробуємо пропінгувати інший вузол. Вибираємо далеко розташовані вузли, щоб наочніше побачити як будуть проходити пакети по мережі в режимі симуляції. Отже, входимо на вузол .4 і пошлемо пінг-запит на вузол .5.

З рожевого вузла пінгуємо зелений. На рожевому вузлі утворився пакет (конвертик), який чекає (іконка паузи на ньому). Запустити пакет в мережу можна натиснувши кнопку "Вперед" у вікні симуляції (Рисунок 6.15).

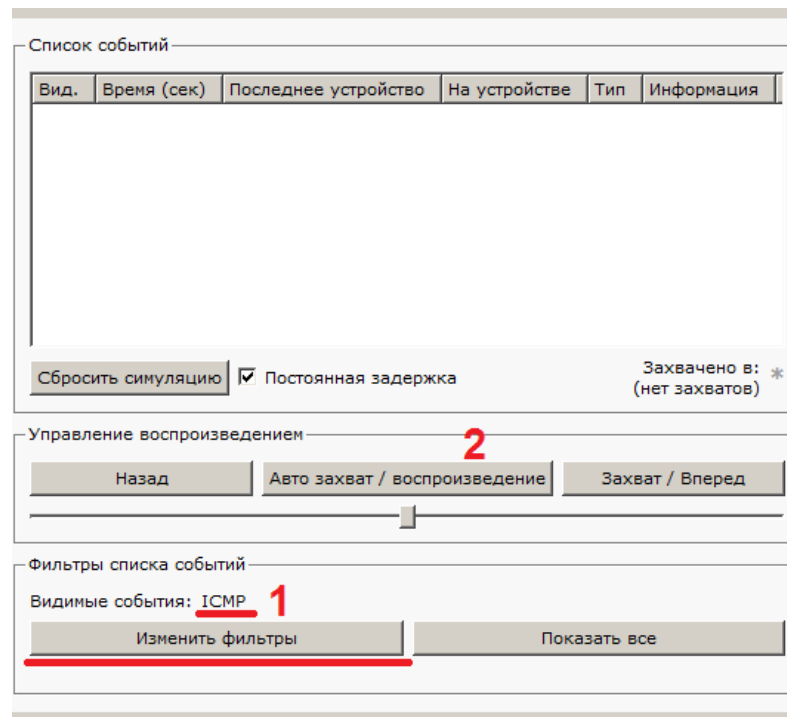


Рисунок 6.14 – Интерфейс симулятора.

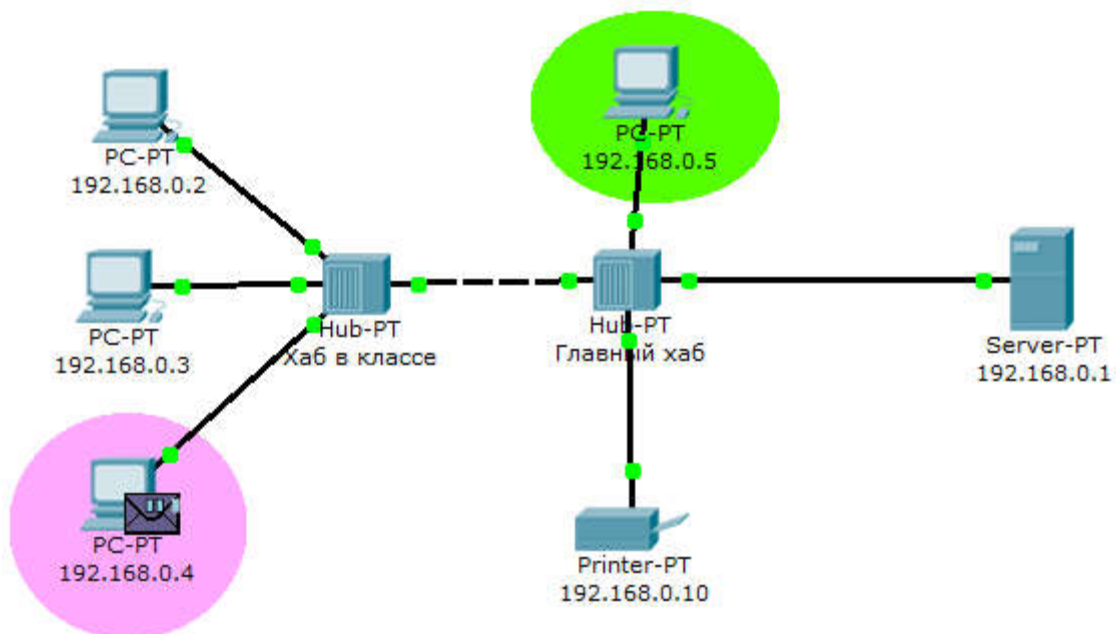


Рисунок 6.15 – Демонстрація роботи симулятора.

Так само у вікні симуляції ми побачимо цей пакет, зазначивши його тип (ICMP) і джерело (192.168.0.4) - рисунок 6.16.

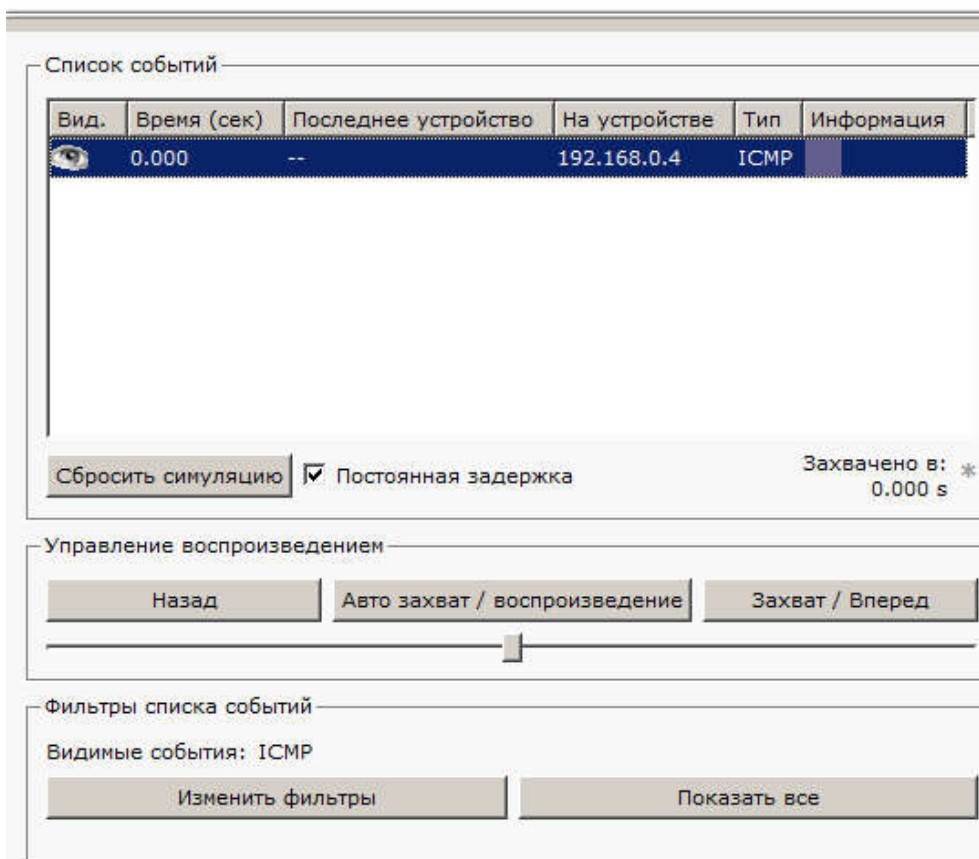


Рисунок 6.16 – Мониторинг работы протоколов

Клік на пакеті покаже нам докладну інформацію. При цьому ми побачимо модель OSI. Відразу видно, що на 3-му рівні (мережевий) виник пакет на вихідному напрямі, який піде до другого рівня, потім до першого, на фізичну середу і передасться на наступний вузол (рисунок 6.17).

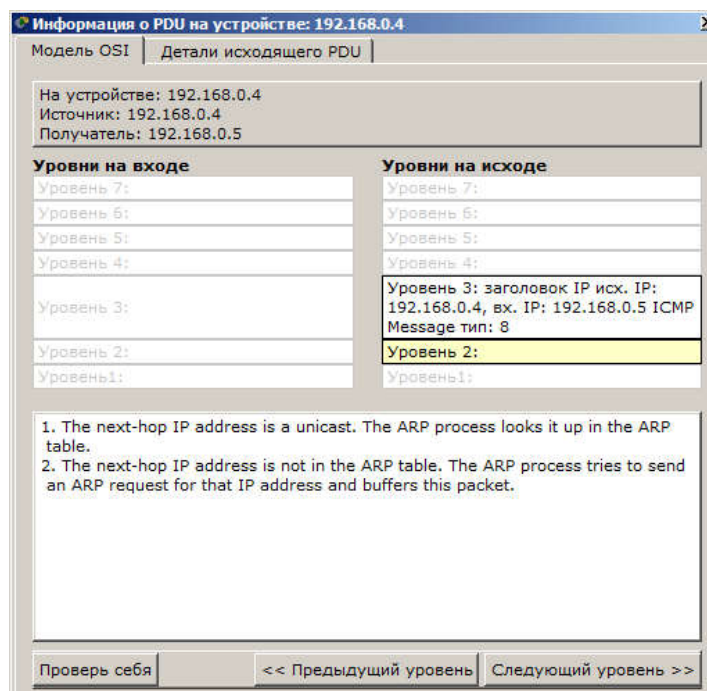


Рисунок 6.17 – Мониторинг работы на модели OSI

А на іншій вкладці можна подивитися структуру пакета (Рисунок 6.18).



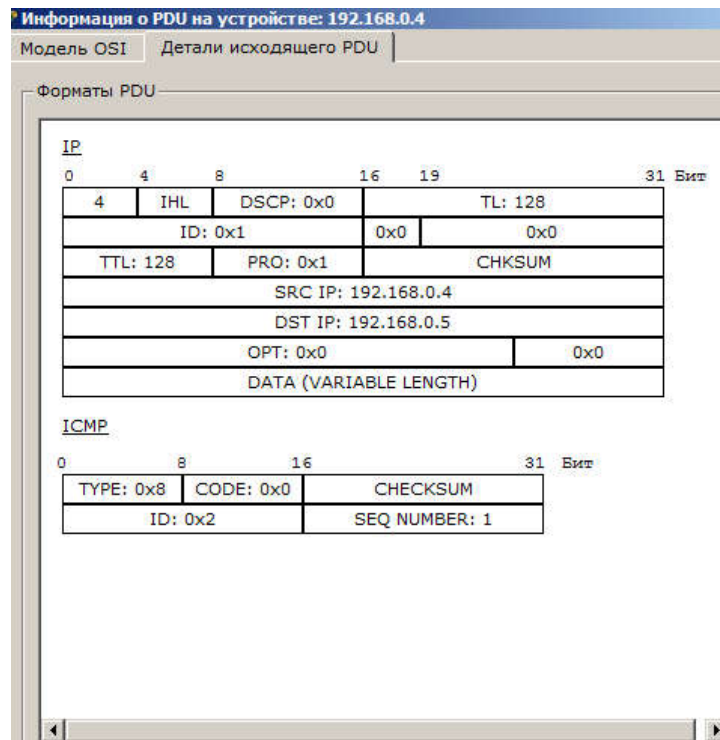


Рисунок 6.18 – Структура пакета

Натиснемо кнопку "Вперед". І пакет тут же рушить до концентратора. Це єдине мережеве підключення з цього боку (рисунок 6.19).

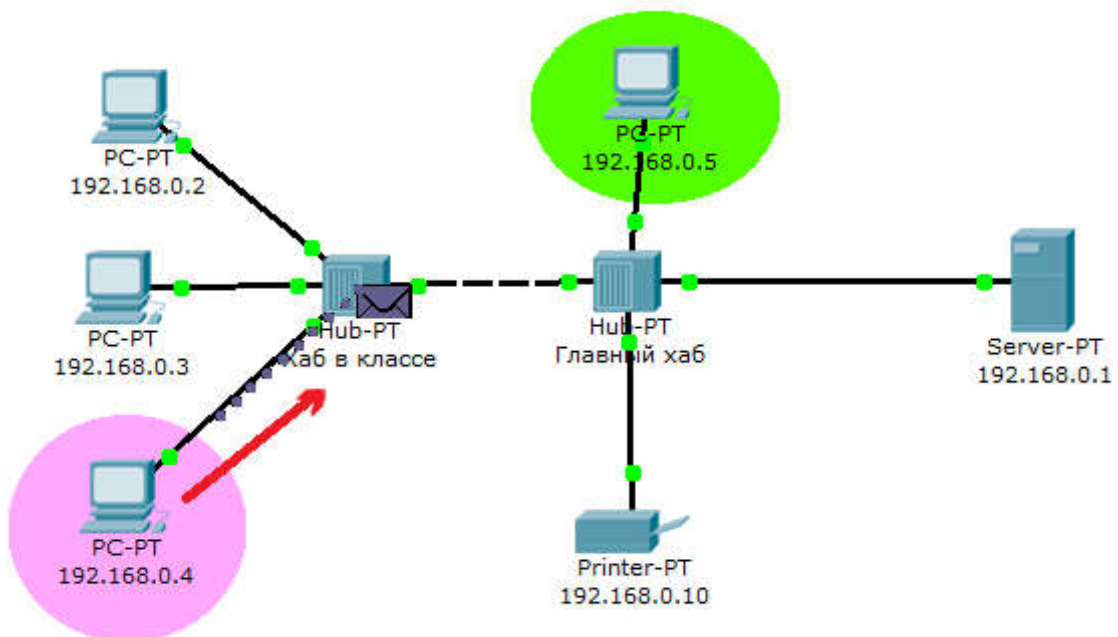


Рисунок 6.19 – Проходження пакета. Перший етап.

Концентратор повторює пакет на всіх інших портах в надії, що на одному з них є адресат (Рисунок 6.20)

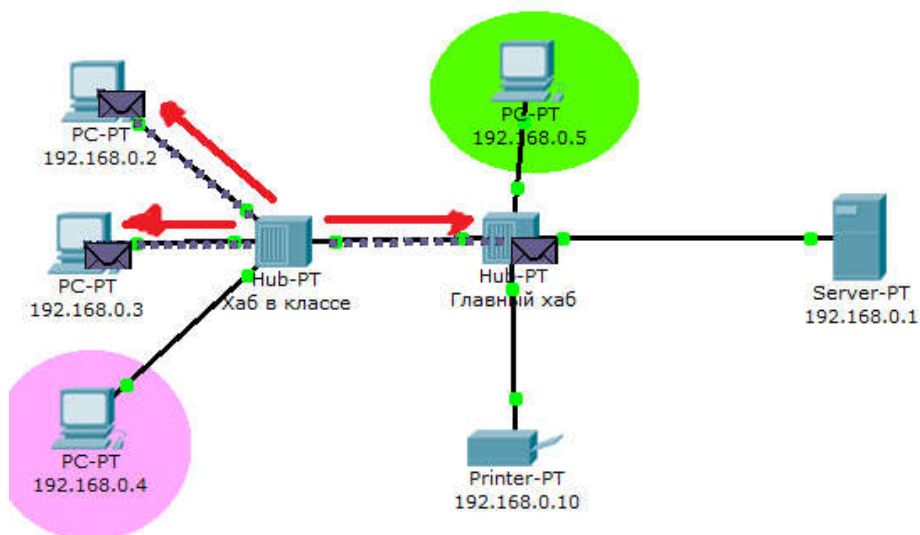


Рисунок 6.20 – Проходження пакета. Другий етап

Якщо пакети якимось вузлів які не призначені, вони просто ігнорують їх (рисунок 6.21).

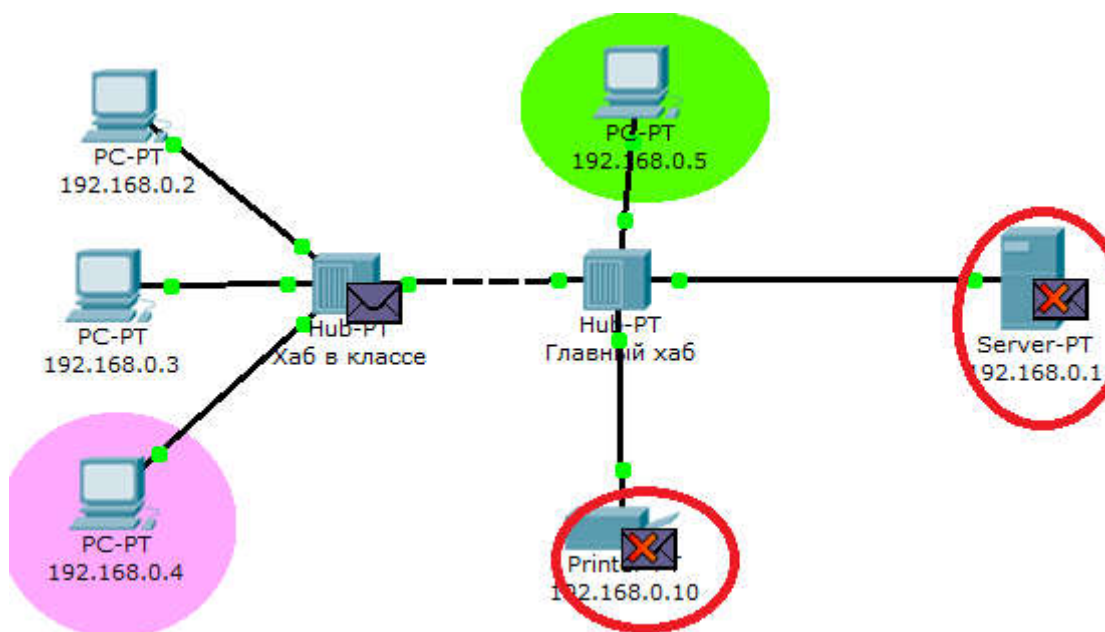


Рисунок 6.21 – Проходження пакета. Третій етап.

### ЗАВДАННЯ ДЛЯ ВИКОНАННЯ:

Варіант	К-сть підмереж	К-сть ПК в підмережі	К-сть принтерів
1	2	6	1
2	3	5	2
3	4	5	1
4	2	8	2
5	3	5	1
6	4	4	2
7	2	5	1
8	3	6	2
9	4	5	1
10	2	9	2
11	3	7	1
12	4	3	2
13	2	7	1
14	3	6	2
15	4	5	1
16	2	5	2
17	3	6	1
18	4	5	2
19	2	9	1
20	3	7	2
21	4	3	1
22	2	5	2
23	3	6	1
24	4	5	2
25	2	9	1
26	3	7	2
27	4	3	1
28	2	7	2
29	3	6	1
30	4	5	2

### ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Короткі теоретичні відомості.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

### КОНТРОЛЬНІ ПИТАННЯ.

1. Яка плата розширення забезпечує функціонал вбудованої точки доступу?
2. Яка плата розширення надає однопортове послідовне підключення до віддаленим офісам або застарілим серійним мережевих пристроїв?
3. Як називається високопродуктивний модуль з 4-ма комутаційними портами Ethernet під роз'єм RJ-45?
4. Перерахуйте мережеві карти, що дозволяють підключатися до WAN мереж?
5. Який тип інтерфейсу слід вибрати при створенні кластера?

6. Назвіть моделі комутаторів третього рівня?
7. Який тип кабелю слід використовувати при з'єднанні роутерів між собою?
8. Вкажіть серії магістральних маршрутизаторів.
9. У яких випадках використовується інтерфейс SERIAL?
10. Як організувати зв'язок двох магістральних маршрутизаторів?
11. Перерахуйте всі можливі режими роботи програми Cisco Paket Tracer?
12. Назвіть моделі комутаторів другого рівня?
13. Перерахуйте всі типи зв'язків, які використовуються в Cisco Paket Tracer і вкажіть їх призначення.
14. Для чого використовується режим симуляції?
15. Як переглянути проходження пакета по рівням моделі OSI?
16. Чи можна визначити причину того, що посланий в режимі симуляції пакет не дійшов до адресата і на якому етапі стався збій роботи мережі?
17. Вкажіть в складі пакету IP адреси відправника і одержувача.
18. Як змінити фільтри списку подій?
19. Як в режимі симуляції визначити, які протоколи були задіяні в роботі мережі?
20. Як в режимі симуляції простежити зміну вмісту пакета при проходженні його по мережі?
21. Перерахуйте основні можливості режиму симуляції.

## ЛАБОРАТОРНА РОБОТА 7. НАЛАШТУВАННЯ МЕРЕЖЕВИХ СЕРВІСІВ.

### ТЕОРЕТИЧНІ ВІДОМОСТІ

Емулятор Cisco Packet Tracer дозволяє проводити настройку таких мережесервісів, як: HTTP, DHCP, TFTP, DNS, NTP, EMAIL, FTP в складі сервера мережі. Розглянемо настройку деяких з них.

Створіть наступну схему мережі, представлену на рисунку 7.1:

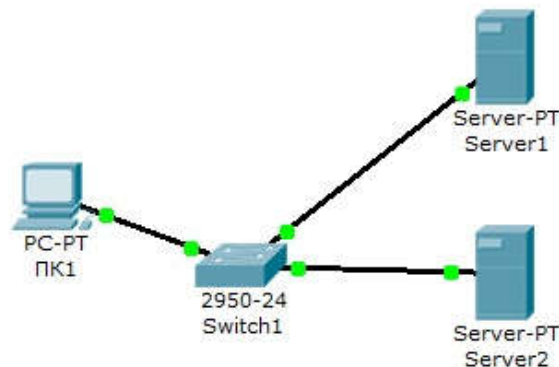


Рисунок 7.1 – Схема мережі

### ХІД РОБОТИ

Налаштувати мережу таким чином:

- 1 - Server1 - DNS і Web сервер;
- 2 - Server2 - DHCP сервер;
- 3 - Комп'ютер ПК1 отримує параметри протоколу TCP / IP в DHCP сервера і відкриває сайт [www.ukr.net](http://www.ukr.net) на Server1.

Етап 1.

Задайте параметри протоколу TCP / IP на ПК1 і серверах.

Увійдіть в конфігурацію ПК1 і встановіть налаштування IP через DHCP сервер

Рисунок 3.2.

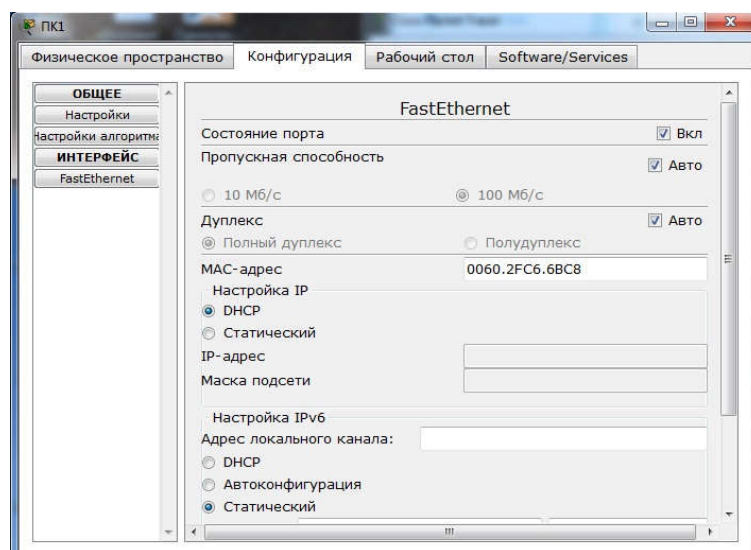


Рисунок 7.2 – Налаштування IP на ПК1.

Задайте в конфігурації серверів наступні настройки IP:  
Server1: IP адреса - 10.0.0.1, маска підмережі - 255.0.0.0  
Server2: IP адреса - 10.0.0.2, маска підмережі - 255.0.0.0

Етап 2. Налаштуйте службу DNS на Server1.

Для цього в конфігурації Server1 увійдіть вкладку DNS і задайте дві ресурсні записи в прямій зоні DNS:

1 - в ресурсному записі типу A зв'яжіть доменне ім'я комп'ютера з його IP адресою  
Рисунок 7.3 і натисніть кнопку ДОДАТИ:

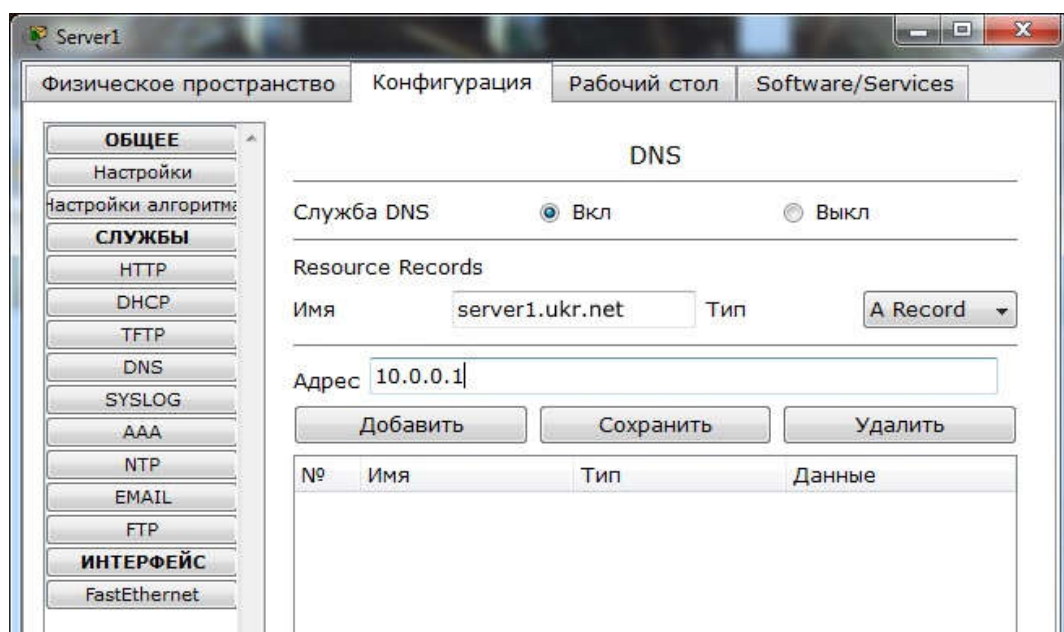


Рисунок 7.3 – Введення ресурсної записи типу A

2 - в ресурсній записі типу CNAME зв'яжіть псевдонім сайту з комп'ютером (рисунок 6.4):

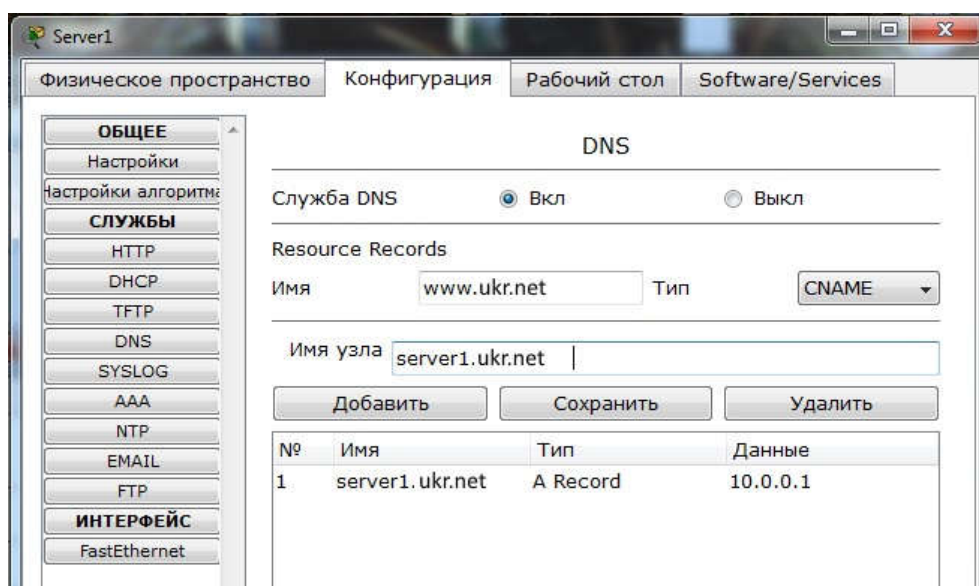


Рисунок 7.4 – Введення ресурсної записи типу CNAME

У конфігурації Server1 водите на вкладку HTTP і задайте стартову сторінку сайту www.ukr.net (Рисунок 7.5):

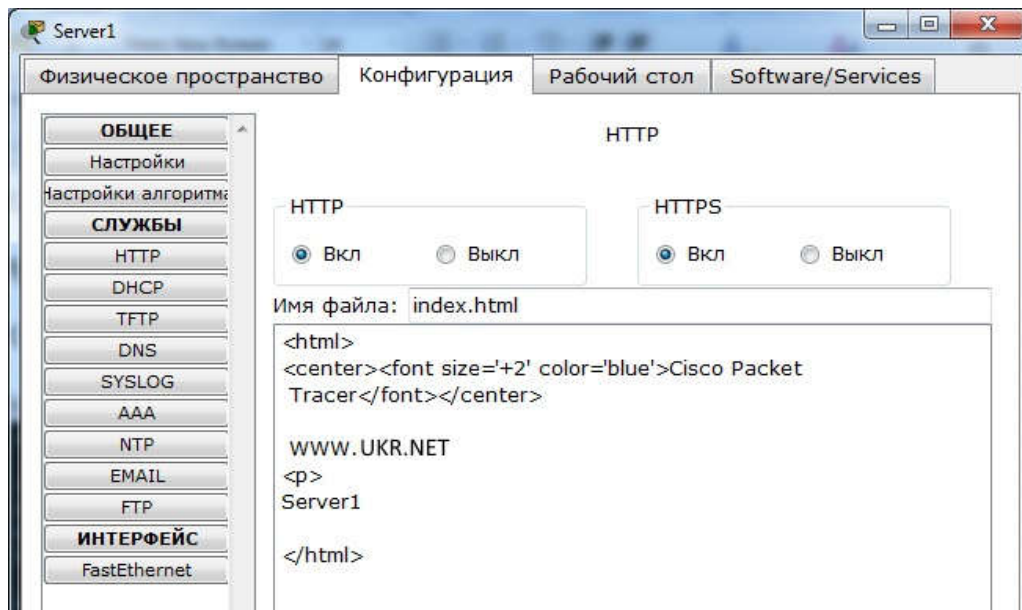


Рисунок 7.5 – Стартова сторінка сайту.

Увімкніть командний рядок на Server1 і перевірте роботу служби DNS. Для перевірки прямий зони DNS сервера введіть команду  
 SERVER> nslookup www.ukr.net

Якщо все правильно, то ви отримаєте відгук із зазначенням повного доменного імені DNS сервера в мережі і його IP адреса.

Етап 3. Налаштуйте DHCP службу на Server2.

Для цього увійдіть в конфігурацію Server2 і на вкладці DHCP налаштуйте службу (Рисунок 7.7):

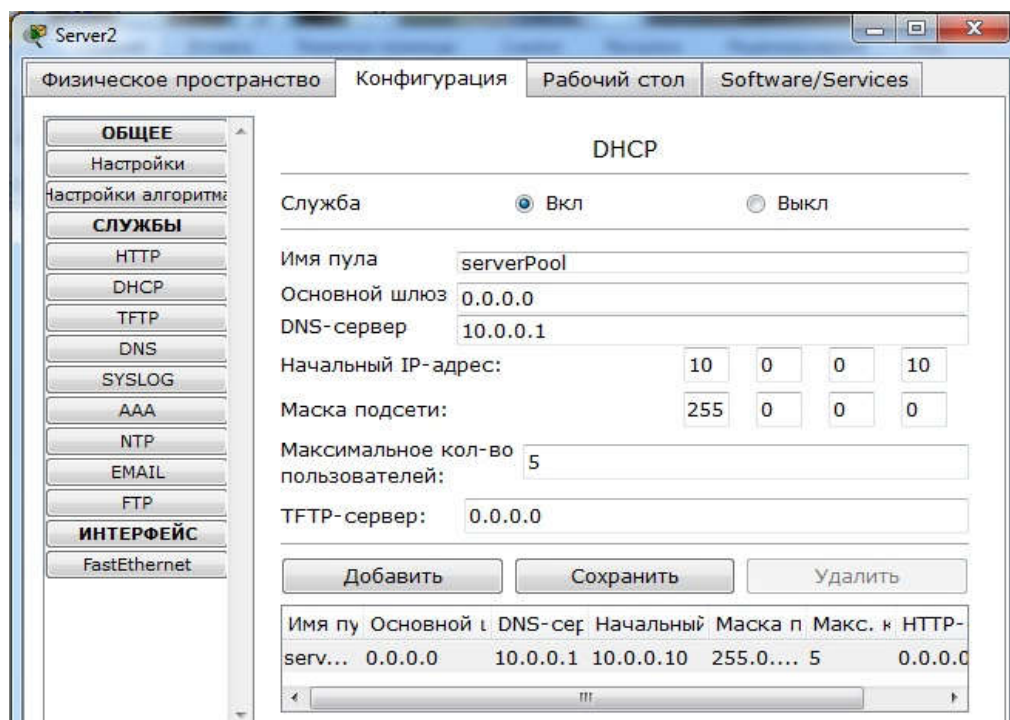


Рисунок 7.7 – Налаштування DHCP сервера.



### Етап 3. Перевірка роботи клієнта.

Увійдіть в конфігурації хоста ПК1 на робочий стіл і в командному рядку налаштуйте протокол TCP / IP.

командою

```
PC> ipconfig / release
```

скиньте старі параметри IP адреси, а командою:

```
PC> ipconfig / renew
```

Отримаєте нові параметри з DHCP сервера (Рисунок 7.8):



```
PC>ipconfig /release

IP Address. . . . . : 0.0.0.0
Subnet Mask. . . . . : 0.0.0.0
Default Gateway. . . . . : 0.0.0.0
DNS Server. . . . . : 0.0.0.0

PC>ipconfig /renew

IP Address. . . . . : 10.0.0.10
Subnet Mask. . . . . : 255.0.0.0
Default Gateway. . . . . : 0.0.0.0
DNS Server. . . . . : 10.0.0.1

PC>
```

Рисунок 7.8 – Конфігурація протокол TCP / IP клієнта.

Перевірка роботи клієнта. Відкрийте сайт [www.ukr.net](http://www.ukr.net) в браузері на клієнті

### ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Короткі теоретичні відомості.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

### КОНТРОЛЬНІ ПИТАННЯ.

1. Що таке рекурсивний запит DNS і яка схема його роботи?
2. Вкажіть призначення типів ресурсних записів в прямій і зворотній зонах DNS.
3. Як на DNS сервері налаштовується пересилання пакетів на інші DNS сервера?
4. Опишіть роботу служби DHCP.
5. Як налаштовується клієнт DHCP?
6. Вкажіть розташування папки з контентом Web вузла і FTP сервера.
7. Як визначається склад зворотних зон DNS сервера в корпоративній мережі.
8. Продемонструйте настройку служба DNS в Cisco Paket Tracer?
9. Продемонструйте настройку служба DHCP в Cisco Paket Tracer?
10. Продемонструйте настройку служба FTP в Cisco Paket Tracer?
11. Продемонструйте настройку Aіva WEB сервер в Cisco Paket Tracer?



## ЛАБОРАТОРНА РОБОТА 8.

### ОСНОВНІ КОМАНДИ ОПЕРАЦІЙНОЇ СИСТЕМИ CISCO IOS.

Мета: вивчити основні команди операційної системи Cisco IOS

### ТЕОРЕТИЧНІ ВІДОМОСТІ

Для настройки мережевого обладнання в вашому розпорядженні є різноманітні команди операційної системи Cisco IOS.

При вході в мережеве пристрій командний рядок має вигляд:

```
Switch>
```

Команди, доступні на призначеному для користувача рівні є підмножиною команд, доступних в привілейованому режимі. Ці команди дозволяють виводити на екран інформацію без зміни установок мережевого пристрою.

Щоб отримати доступ до повного набору команд, необхідно спочатку активізувати привілейований режим.

```
Press ENTER to start.
```

```
Switch>
```

```
Switch> enable
```

```
Switch #
```

Вихід з привілейованого режиму:

```
Switch # disable
```

```
Switch>
```

Про перехід в привілейований режим буде свідчити поява в командному рядку запрошення у вигляді знака #.

З привілейованого рівня можна отримувати інформацію про налаштування системи і отримати доступ до режиму глобального конфігурування та інших спеціальних режимів конфігурації, включаючи режими конфігурації інтерфейсу, під'інтерфейса, лінії, мережевого пристрою, карти маршрутів і т.п.

Для виходу з системи IOS необхідно набрати на клавіатурі команду exit (вихід):

```
Switch> exit
```

Можлива робота в наступних режимах:

- Призначений для користувача режим - це режим перегляду, у якому користувач може тільки переглядати певну інформацію про мережевому пристрої, але не може нічого міняти. В цьому режимі запрошення має вигляд:

```
Switch>
```

- Привілейований режим-підтримує команди настройки і тестування, детальну перевірку мережевого пристрою, маніпуляцію з файлами і доступ в режим конфігурації. В цьому режимі запрошення має вигляд:

```
Switch #
```

- Режим глобального конфігурування - реалізує потужні однорядкові команди, які вирішують завдання конфігурації. В тому режимі запрошення має вигляд:

```
Switch (config) #
```

Команди в будь-якому режимі IOS розпізнає по першим унікальним символам. При натисканні табуляції IOS сам доповнить команду до повного імені.

При введенні в командному рядку будь-якого режиму імені команди і знака питання (?) На екран виводяться коментарі до команди. При введенні одного знака результатом буде список всіх команд режиму. На екран може виводитися багато екранів рядків, тому іноді в

нижній частині екрана буде з'являтися підказка - More -. Для продовження слід натиснути enter або пробіл.

Команди режиму глобального конфігурування визначають поведінку системи в цілому. Крім цього, команди режиму глобального конфігурування включають команди переходу в інші режими конфігурації, які використовуються для створення конфігурацій, які потребують багаторядкових команд. Для входу в режим глобального конфігурування використовується команда привілейованого режиму configure. При введенні цієї команди слід вказати джерело команд конфігурації:

- terminal (термінал),
- memory (незалежна пам'ять або файл),
- network (сервер tftp (Trivial ftp -упрощений ftp) в мережі).

За замовчуванням команди вводяться з терміналу консолі, наприклад:

```
Switch (config) # (commands)
Switch (config) #exit
Switch #
```

Команди для активізації приватного виду конфігурації повинні передувати командами глобального конфігурування. Так для конфігурації інтерфейсу, на можливість якої вказує запрошення

```
Switch (config-if) #
```

спочатку вводиться глобальна команда для визначення типу інтерфейсу і номера його порту:

```
Switch # conf t
Switch (config) #interface type port
Switch (config-if) # (commands)
Switch (config-if) #exit
Switch (config) #exit
```

## ХІД РОБОТИ

### Основні команди мережевого пристрою

1. Увійдіть мережеве пристрій Router1

```
Router>
```

2. Ми хочемо побачити список всіх доступних команд в цьому режимі. Введіть команду, яка використовується для перегляду всіх доступних команд:

```
Router>?
```

Клавішу Enter натискати не треба.

3. Тепер увійдіть в привілейований режим

```
Router> enable
```

```
Router #
```

4. Перегляньте список доступних команд в привілейованому режимі

```
Router #?
```

5. Перейдемо в режим конфігурації

```
Router # config terminal
```

```
Router (config) #
```

6. Ім'я хоста мережевого пристрою використовується для локальної ідентифікації.

Коли ви входите в мережеве пристрій, ви бачите Ім'я хоста перед символом режиму (">" або "#"). Це ім'я може бути використано для визначення місця знаходження.

Встановіть "Router1" як ім'я вашого, мережевого пристрою.

```
Router (config) #hostname Router1
Router1 (config) #
```

7. Пароль доступу дозволяє вам контролювати доступ в привілейований режим. Це дуже важливий пароль, тому що в привілейованому режимі можна вносити конфігураційні зміни. Встановіть пароль доступу "parol".

```
Router1 (config) #enable password parol
```

1. Давайте спробуємо цей пароль. Вийдіть з мережевого пристрою і спробуйте зайти в привілейований режим.

2.

```
Router1> en
Password: *****
Router1 #
```

Тут знаки: \*\*\*\*\* - це ваш введення пароля. Ці знаки на екрані не помітні.

### **Основні Show команди.**

Перейдіть в призначений для користувача режим командою disable. Введіть команду для перегляду всіх доступних show команд.

```
Router1> show?
```

1. Команда show version використовується для отримання типу платформи мережевого пристрою, версії операційної системи, імені файлу образу операційної системи, час роботи системи, обсяг пам'яті, кількість інтерфейсів і конфігураційний регістр.

2. Перегляд часу:

```
Router1> show clock
```

3. У флеш-пам'яті мережного пристрою зберігається файл-образ операційної системи Cisco IOS. На відміну від оперативної пам'яті, в реальних пристроях флеш пам'ять зберігає файл-образ навіть при збої живлення.

```
Router1> show flash
```

4. ІКС мережевого пристрою за умовчанням сохранияет10 останніх введених команд

```
Router1> show history
```

5. Дві команди дозволяють вам повернутися до командам, введеним раніше. Натисніть на стрілку вгору або <ctrl> P.

6. Дві команди дозволяють вам перейти до наступної команді, збереженої в буфері.

Натисніть на стрілку вниз або <ctrl> N

7. Можна побачити список хостів і IP-Адреси всіх їх інтерфейсів

```
Router1> show hosts
```

8. Наступна команда виведе детальну інформацію про кожного інтерфейсі

```
Router1> show interfaces
```

9. Наступна команда виведе інформацію про кожну telnet сесії:

```
Router1> show sessions
```

10. Наступна команда показує конфігураційні параметри терміналу:

```
Router1> show terminal
```

11. Можна побачити список всіх користувачів, приєднаних до пристрою по термінальним лініях:

```
Router1> show users
```

12. Команда

```
Router1> show controllers
```

показує стан контролерів інтерфейсів.

13. Перейдемо в привілейований режим.

```
Router1> en
```

14. Введіть команду для перегляду всіх доступних show команд.

```
Router1 # show?
```

Привілейований режим включає в себе всі show команди призначеного для користувача режиму і ряд нових.

15. Подивимося активну конфігурацію в пам'яті мережного пристрою. Необхідний привілейований режим. Активна конфігурація автоматично не зберігається і буде втрачена в разі збою електроживлення. Щоб зберегти настройки роутера використовуйте наступні команди:

збереження поточної конфігурації:

```
Router # write memory
```

або

```
Router # copy run start
```

Перегляд збереженої конфігурації:

```
Router # Show configuration
```

або

```
Router1 # show running-config
```

У рядку more, натисніть на клавішу пробіл для перегляду наступної сторінки інформації.

16. Наступна команда дозволить вам побачити поточний стан протоколів третього рівня:

```
Router # show protocols
```

**Введення в конфігурацію інтерфейсів.**

Розглянемо команди настройки інтерфейсів мережевого пристрою.

На мережевому пристрої Router1 увійдемо в режим конфігурації:

```
Router1 # conf t
```

```
Router1 (config) #
```

2. Тепер ми хочемо налаштувати Ethernet інтерфейс. Для цього ми повинні зайти в режим конфігурації інтерфейсу:

```
Router1 (config) #interface FastEthernet0 / 0
```

```
Router1 (config-if) #
```

3. Подивимося всі доступні в цьому режимі команди:

```
Router1 (config-if) #?
```

Для виходу в режим глобальної конфігурації наберіть exit. Знову увійдіть в режим конфігурації інтерфейсу:

```
Router1 (config) #int fa0 / 0
```

Ми використовували скорочене ім'я інтерфейсу.

4. Для кожної команди ми можемо виконати протилежну команду, поставивши перед нею слово `no`. Наступна команда включає цей інтерфейс:

```
Router1 (config-if) #no shutdown
```

5. Додамо до інтерфейсу опис:

```
Router1 (config-if) #description Ethernet interface on Router 1
```

Щоб побачити опис цього інтерфейсу, перейдіть в привілейований режим і виконайте команду `show interface`:

```
Router1 (config-if) #end  
Router1 # show interface
```

6. Тепер приєднаєтеся до інших мережних пристроїв Router 2 і поміняйте ім'я його хоста на Router2:

```
Router # conf t  
Router (config) #hostname Router2
```

Увійдемо на інтерфейс FastEthernet 0/0:

```
Router2 (config) #interface fa0 / 0
```

Увімкніть інтерфейс:

```
Router2 (config-if) #no shutdown
```

Тепер, коли інтерфейси на двох кінцях нашого Ethernet з'єднання включені на екрані з'явиться повідомлення про зміну стану інтерфейсу на активну.

7. Перейдемо до конфігурації послідовних інтерфейсів. Зайдемо на Router1.

Перевіримо, яким пристроєм виступає наш маршрутизатор для послідовної лінії зв'язку: кінцевим пристроєм DTE (data terminal equipment), яким пристроєм зв'язку DCE (data circuit):

```
Router1 # show controllers fa0 / 1
```

Якщо бачимо повідомлення:

```
DCE cable
```

то наш маршрутизатор є пристроєм зв'язку та він повинен задавати частоту синхронізації тактових імпульсів, використовуваних при передачі даних. Частота береться з певного ряду частот.

```
Router1 # conf t  
Router1 (config) #int fa0 / 1  
Router1 (config-if) #clock rate?
```

Виберемо частоту 64000

```
Router1 (config-if) #clock rate 64000
```

і включаємо інтерфейс

```
Router1 (config-if) #no shut
```

## ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Короткі теоретичні відомості.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

## КОНТРОЛЬНІ ПИТАННЯ.

1. Якою командою можна подивитися поточні настройки маршрутизатора?
2. Якими командами налаштовується мережевий інтерфейс маршрутизатора.
3. Як переглянути конфігураційні налаштування комутатора?
4. Як визначити розподіл VLAN по портах комутатора?
5. Перерахуйте основні режими конфігурації при налаштуванні комутатора.
6. Перерахуйте основні режими конфігурації при налаштуванні роутера.
7. Як подивитися таблицю маршрутизації на роутері?
8. Які команди формують таблицю маршрутизації роутера?
9. Якими командами налаштовуються VLAN на комутаторі?
10. Якими командами налаштовується взаємодія між VLAN?

## ЛАБОРАТОРНА РОБОТА 9. НАЛАШТУВАННЯ СТАТИЧНОЇ МАРШРУТИЗАЦІЇ

Мета: налаштування статичної маршрутизації в Cisco Packet Tracer

### ТЕОРЕТИЧНІ ВІДОМОСТІ

Протоколи маршрутизації - це правила, за якими здійснюється обмін інформацією про шляхи передачі пакетів між маршрутизаторами. Протоколи характеризуються часом збіжності, втратами і масштабованістю. В даний час використовується кілька протоколів маршрутизації.

Одна з головних завдань маршрутизатора полягає у визначенні найкращого шляху до заданого адресату. Маршрутизатор визначає шляхи (маршрути) до адресатів або зі статичної конфігурації, введеної адміністратором, або динамічно на підставі маршрутної інформації, отриманої від інших маршрутизаторів. Маршрутизатори обмінюються маршрутної інформацією за допомогою протоколів маршрутизації.

Маршрутизатор зберігає таблиці маршрутів в оперативній пам'яті. Таблиця маршрутів це список найкращих відомих доступних маршрутів. Маршрутизатор використовує цю таблицю для прийняття рішення куди направляти пакет.

У разі статичної маршрутизації адміністратор вручну визначає маршрути до мереж призначення.

У разі динамічної маршрутизації - маршрутизатори дотримуються правил, що визначаються протоколами маршрутизації для обміну інформацією про маршрути і вибору кращого шляху.

Статичні маршрути не змінюються самим маршрутизатором. Динамічні маршрути змінюються самим маршрутизатором автоматично при отриманні інформації про зміну маршрутів від сусідніх маршрутизаторів. Статична маршрутизація споживає мало обчислювальних ресурсів і корисна в мережах, які не мають кількох шляхів до адресата призначення. Якщо від маршрутизатора до маршрутизатора є тільки один шлях, то часто використовують статичну маршрутизацію.

Проведемо налаштування статичної маршрутизації за допомогою графічних майстрів інтерфейсу Cisco Packet Tracer.

Створіть схему мережі, представлену На рисунку 9.1.

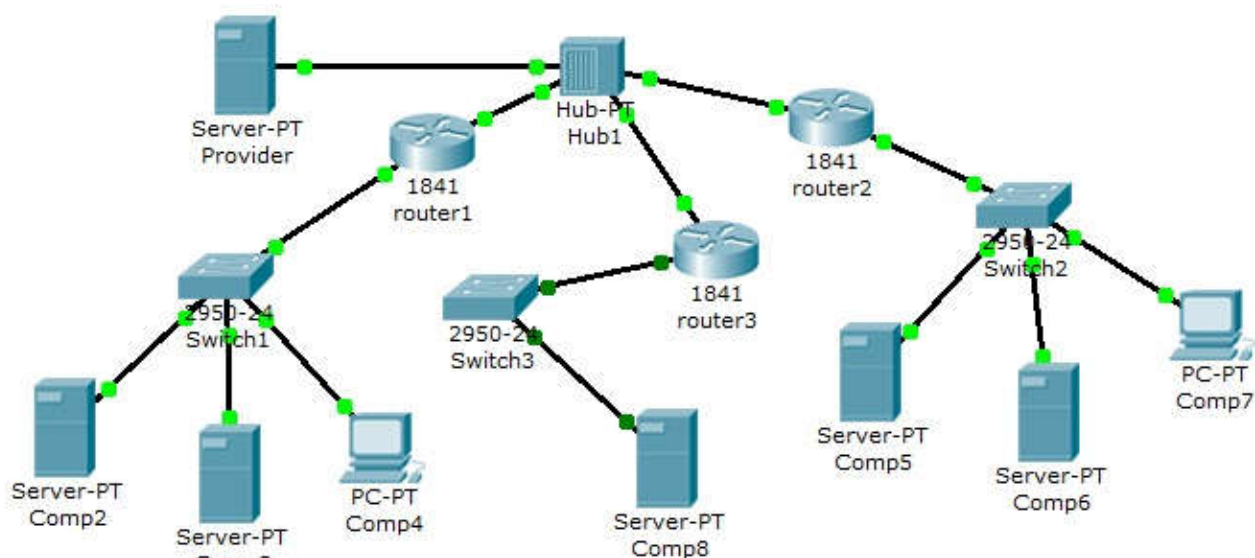


Рисунок 9.1 – Схема мережі.

На даній схемі представлена корпоративна мережа, що складається з наступних компонентів:

Мережа 1 - на Switch1 замикається мережу першої організації (таблиця 9.1):

Таблиця 9.1 – Мережа першої організації.

Комп'ютер	IP адреса	функції
Comp2	192.168.1.2/24	DNS і HTTP сервер
Comp3	192.168.1.3/24	DHCP сервер
Comp4	Отримано з DHCP сервера	клієнт мережі

В даній мережі на Comp2 встановлений DNS і Web сервер з сайтом організації.

На Comp3 встановлений DHCP сервер. Комп'ютер Comp4 отримує з DHCP сервера IP адреса, адреса DNS сервера провайдера (сервер Provider) і шлюз. Шлюз в мережі - 192.168.1.1/24.

Мережа 2 - на Switch2 замикається мережу іншої організації (таблиця 9.2):

Таблиця 9.2 – Мережа другий організації.

комп'ютер	IP адреса	функції
Comp5	10.0.0.5/8	DNS і HTTP сервер
Comp6	10.0.0.6/8	DHCP сервер
Comp7	Отримано з DHCP сервера	клієнт мережі

В даній мережі на Comp5 встановлений DNS і Web сервер з сайтом організації.

На Comp4 встановлений DHCP сервер. Комп'ютер Comp7 отримує з DHCP сервера IP адреса, адреса DNS сервера провайдера (сервер Provider) і шлюз. Шлюз в мережі - 10.0.0.1/8.

**Мережа 3** - на Hub1 замикається міська мережа 200.200.200.0/24. У мережі встановлено DNS сервер провайдера (комп'ютер Provider з IP адресою -200.200.200.10 / 24), що містить дані по всім сайтам мережі (Comp2, Comp5, Comp8).

**Мережа 4** - маршрутизатор Router3 виводить міську мережу в інтернет через комутатор Switch3 (мережа 210.210.210.0/24). На Comp8 (IP адреса 210.210.210.8/24, шлюз 210.210.210.3/24.) Встановлено DNS і Web сервер з сайтом.

Маршрутизатор мають по два інтерфейси:

Router1 - 192.168.1.1/24 і 200.200.200.1/24.

Router2 - 10.0.0.1/8 і 200.200.200.2/24.

Router3 - 210.210.210.3/24 і 200.200.200.3/24.

## ХІД РОБОТИ

### Завдання 1.

Налаштувати

1 - мережі організації;

2 - DNS сервер провайдера;

3 - статичні таблиці маршрутизації на роутерах;

4 - перевірити роботу мережі - на кожному з комп'ютерів - Comp4, Comp7 і Comp8. З кожного з них повинні відкриватися все три сайти корпоративної мережі.

У попередніх лабораторних роботах розглядалася настройка мережевих служб і DNS сервера. Приступимо до налаштування статичної маршрутизації на роутерах. Оскільки на представленій схемі чотири мережі, то таблиці маршрутизації як мінімум повинні містити записи до кожної з цих мереж - тобто чотири записи. На роутерах Cisco в таблицях маршрутизації як правило, не прописуються шляхи до мереж, до яких під'єднані інтерфейси роутера. Тому на кожному маршрутизаторі необхідно внести по два записи.



Налаштуйте перший маршрутизатор.

Для цього увійдіть в конфігурацію маршрутизатора і в інтерфейсах встановіть IP адресу і маску підмережі. Потім в розділі маршрутизації відкрийте вкладку СТАТИЧНА, внесіть дані (Рисунок 9.2) і натисніть кнопку ДОДАТИ:

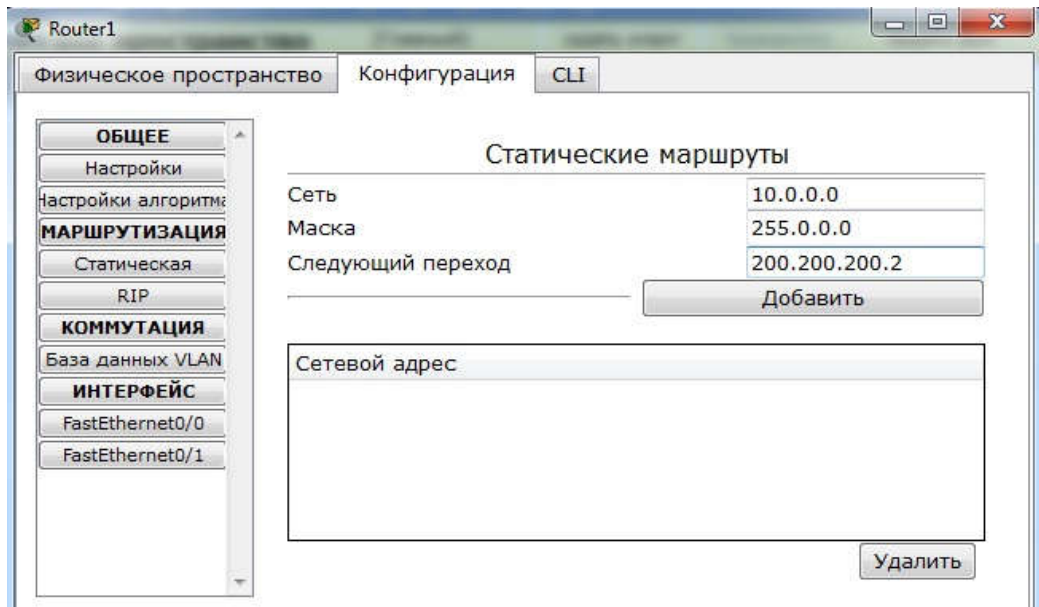


Рисунок 9.2 – Дані для мережі 10.0.0.0/8.

В результаті у вас повинні з'явитися два записи в таблиці маршрутизації (Рисунок 9.3):

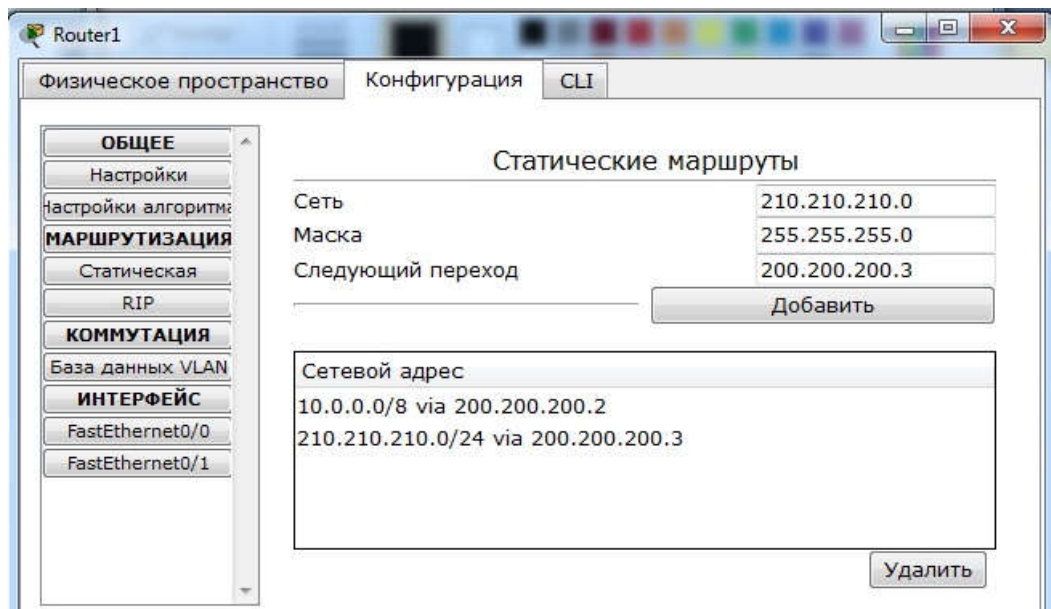


Рисунок 9.3 – Формування статичної таблиці маршрутизації.

Щоб подивитися повну настройку таблиці маршрутизації, виберіть в бічному графічному меню інструмент ПЕРЕВІРКА (піктограма лупи), клацніть у схемі на роутері і виберіть у спадному меню пункт ТАБЛИЦЯ МАРШРУТИЗАЦІЇ.

Після налаштування всіх роутерів у вашій мережі стануть доступні IP адреси будь-якого комп'ютера і ви зможете відкрити будь-який сайт з комп'ютерів Comp4, Comp7 і Comp8.

## Завдання 2

Виконайте самостійно наступну роботу, схема мережі для якої представлена на рисунку 9.4.

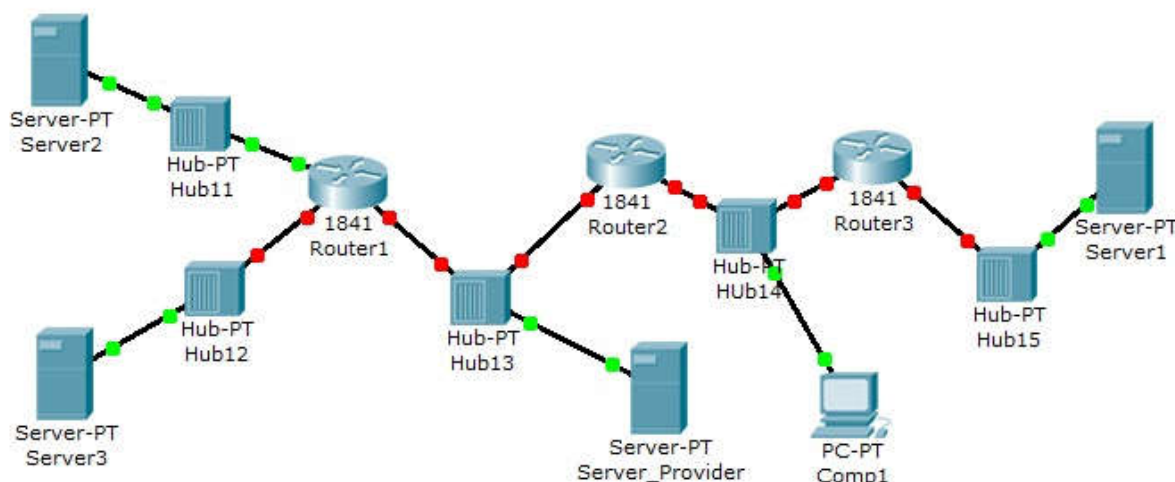


Рисунок 9.4 – Схема мережі.

П'ять концентраторів представляють наступні п'ять мереж:

Hub11 - мережа 11.0.0.0

Hub12 - мережа 12.0.0.0

Hub13 - мережа 13.0.0.0

Hub14 - мережа 14.0.0.0

Hub15 - мережа 15.0.0.0

Router 1 має додатковий мережевий інтерфейс, який додається з модуля WIC-1ENET при вимкненому маршрутизаторі.

У мережі три Web вузла на Server1, Server2 і Server3.

Сервера і комп'ютер мають довільні IP адреси зі шлюзами своїх роутерів.

Інтерфейси роутерів визначаються мережею на концентраторі і номером роутера.

Наприклад для Router3: 15.0.0.3 і 14.0.0.3

Задача:

комп'ютер Comp1 повинен відкрити всі три сайти на серверах корпоративної мережі.

В налаштуваннях Comp1 як DNS сервера вказано DNS сервер провайдера на Server\_Provider.

### Послідовність виконання.

Корпоративна мережа 15.0.0.0/8 розбита на десять підмереж, з них в даний момент задіяно шість підмереж в шести різних підрозділах організації. Пристрої мережі:

- три маршрутизатора;
- шість комутаторів (по одному в кожному відділі на підмережа);
- один комп'ютер в кожній мережі.

### Розрахунки.

1 - розрахуйте параметри підмереж і задайте на комп'ютерах IP адресу, маску і шлюз в кожній окремій підмережі;

2 - створіть довільну топологію мережі, з'єднавши маршрутизатори з підмережами в будь-якому порядку. При цьому з'єднайте маршрутизатори між собою довільно - безпосередньо, через штатні комутатори підрозділу або додаткові комутатори;

3 - перевірте працездатність корпоративної мережі командою PING - всі комп'ютери повинні бути доступні.

### ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Короткі теоретичні відомості.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

### КОНТРОЛЬНІ ПИТАННЯ.

1. Якою командою можна подивитися поточні настройки маршрутизатора?
2. Якими командами налаштовується мережевий інтерфейс маршрутизатора.
3. Як переглянути конфігураційні налаштування комутатора?
4. Як визначити розподіл VLAN по портах комутатора?
5. Перерахуйте основні режими конфігурації при налаштуванні комутатора.
6. Перерахуйте основні режими конфігурації при налаштуванні роутера.
7. Як подивитися таблицю маршрутизації на роутері?
8. Які команди формують таблицю маршрутизації роутера?
9. Якими командами налаштовуються VLAN на комутаторі?
10. Якими командами налаштовується взаємодія між VLAN?

## ЛАБОРАТОРНА РОБОТА 10 НАЛАШТУВАННЯ ПРОТОКОЛУ RIP

Мета: навчитись налаштовувати протокол RIP

### ТЕОРЕТИЧНІ ВІДОМОСТІ

Статична маршрутизація не підходить для великих, складних мереж тому, що зазвичай мережі включають надлишкові зв'язку, багато протоколів і змішані топології.

Маршрутизатор в складних мережах повинні швидко адаптуватися до змін топології і вибирати кращий маршрут з багатьох кандидатів.

IP мережі мають ієрархічну структуру. З точки зору маршрутизації мережу розглядається як сукупність автономних систем. В автономних підсистемах великих мереж для маршрутизації на інші автономні системи широко використовуються маршрути за замовчуванням.

Динамічна маршрутизація може бути здійснена з використанням одного і більше протоколів. Ці протоколи часто групуються відповідно до того, де вони використовуються. Протоколи для роботи всередині автономних систем називають внутрішніми протоколами шлюзів (interior gateway protocols (IGP)), а протоколи для роботи між автономними системами називають зовнішніми протоколами шлюзів (exterior gateway protocols (EGP)). До протоколів IGP відносяться RIP, RIP v2, IGRP, EIGRP, OSPF і IS-IS. Протоколи EGP3 і BGP4 відносяться до EGP. Всі ці протоколи можуть бути розділені на два класи: дистанційно-векторні протоколи і протоколи стану зв'язку.

Дистанційно-векторна маршрутизація.

Маршрутизатор використовують метрики для оцінки або вимірювання маршрутів. Коли від маршрутизатора до мережі призначення існує багато маршрутів, і всі вони використовують один протокол маршрутизації, то маршрут з найменшою метрикою розглядається як кращий. Якщо використовуються різні протоколи маршрутизації, то для вибору маршруту використовується адміністративні відстані, які призначаються маршрутам операційною системою маршрутизатора. RIP використовує в якості метрики кількість переходів (хопов).

Дистанційно-векторна маршрутизація базується на алгоритмі Белмана-Форда. Через певні моменти часу маршрутизатор передає сусіднім маршрутизаторам всю свою таблицю маршрутизації. Такі прості протоколи як RIP і IGRP просто поширюють інформацію про таблиці маршрутів через все інтерфейси маршрутизатора в ширококомовному режимі без уточнення точної адреси конкретного сусіднього маршрутизатора.

Сусідній маршрутизатор, отримуючи ширококомовлення, порівнює інформацію зі своєю поточною таблицею маршрутів. У неї додаються маршрути до нових мереж або маршрути до відомих мереж з кращого метрикою. Відбувається видалення неіснуючих маршрутів. Маршрутизатор додає свої власні значення до метрик отриманих маршрутів. Нова таблиця маршрутизації знову поширюється по сусідніх маршрутизаторів

### ХІД РОБОТИ

Створіть схему, представлену на рисунку 10.1.

На схемі представлені наступні три мережі:

Switch1 - мережа 10.11.0.0/16.

Switch2 - мережа 10.12.0.0/16.

Мережа для роутерів - 10.10.0.0/16.

Введіть на пристроях наступну адресацію:

Маршрутизатор мають по два інтерфейси:

Router1 - 10.11.0.1/16 і 10.10.0.1/16.

Router2 - 10.10.0.2/16 і 10.12.0.1/16.

ПК11 - 10.11.0.11/16.

ПК12 - 10.12.0.12/16.

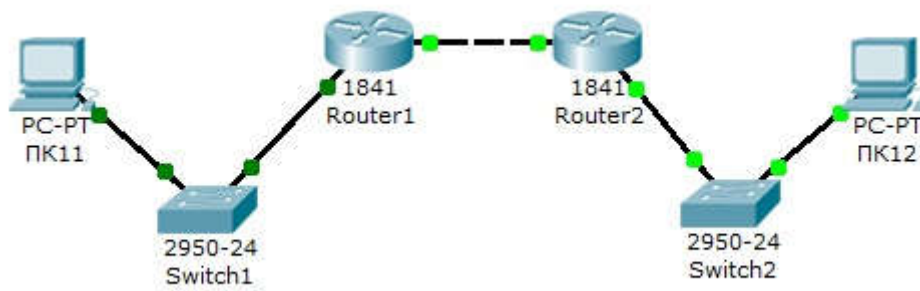


Рисунок 10.1 – Схема мережі.

Проведемо настройку протоколу RIP на маршрутизаторі Router1.

Увійдіть в конфігурації в консоль роутера і виконайте наступні настройки (при введенні команд маску підмережі можна не вказувати, тому що вона буде братися автоматично з налаштувань інтерфейсу роутера):

Увійдіть в привілейований режим:

```
Router1>en
```

Увійдіть в режим конфігурації:

```
Router1> #conf t
```

Увійдіть в режим конфігурації протоколу RIP:

```
Router1 (config) #router rip
```

Підключіть клієнтську мережу до роутера:

```
Router1 (config-router) #network 10.11.0.0
```

Підключіть другу мережу до роутера:

```
Router1 (config-router) #network 10.10.0.0
```

Задайте використання другої версії протокол RIP:

```
Router1 (config-router) #version 2
```

Вийдіть з режиму конфігурації протоколу RIP:

```
Router1 (config-router) #exit
```

Вийдіть з консолі налаштувань:

```
Router1 (config) #exit
```

Збережіть налаштування в пам'ять маршрутизатора:

```
Router1> #write memory
```

Аналогічно проведіть настройку протоколу RIP на маршрутизаторі Router2.

Перевірте зв'язок між комп'ютерами ПК11 і ПК12 командою ping.

Якщо зв'язок є - все налаштування зроблені вірно.

## ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Короткі теоретичні відомості.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

## ЛАБОРАТОРНА РОБОТА №11. НАЛАШТУВАННЯ ПРОТОКОЛУ RIP В КОРПОРАТИВНІЙ МЕРЕЖІ.

### ТЕОРЕТИЧНІ ВІДОМОСТІ

Протоколи маршрутизації пропонують кращу масштабованість і збіжність у порівнянні з дистанційно-векторними протоколами. Робота протоколів базується на алгоритмі Дейкстри, який часто називають алгоритмом «найкоротший шлях - першим» (shortest path first SPF). Найбільш типовим представником є протокол OSPF (Open Shortest Path First).

Маршрутизатор бере до розгляду стан зв'язку інтерфейсів інших маршрутизаторів в мережі. Маршрутизатор будує повну базу даних всіх станів зв'язку в своїй області, тобто має достатньо інформації для створення свого відображення мережі. Кожен маршрутизатор потім самостійно виконує SPF-алгоритм на своєму власному відображенні мережі або базі даних станів зв'язку для визначення кращого шляху, який заноситься в таблицю маршрутів. Ці шляхи до інших мереж формують дерево з вершиною в вигляді локального маршрутизатора.

Маршрутизатор сповіщають про стан своїх зв'язків всім маршрутизаторів в області. Таке повідомлення називають LSA (link-state advertisements).

На відміну від дистанційно-векторних маршрутизаторів, маршрутизатори стану зв'язку можуть формувати спеціальні відносини зі своїми сусідами.

Має місце початковий вплив LSA пакетів для побудови бази даних станів зв'язку. Далі оновлення маршрутів проводиться тільки при зміні станів зв'язку або, якщо стан не змінився протягом певного інтервалу часу. Якщо стан зв'язку змінилося, то часткове оновлення пересилається негайно. Воно містить тільки стану зв'язків, які змінилися, а не всю таблицю маршрутів.

Адміністратор, який дбає про використання ліній зв'язку, знаходить ці часткові і рідкісні поновлення ефективною альтернативою дистанційно-векторної маршрутизації, яка передає всю таблицю маршрутів через регулярні проміжки часу. Протоколи стану зв'язку мають більш швидку збіжність і краще використання смуги пропускання в порівнянні з дистанційно-векторними протоколами. Вони перевершують дистанційно-векторні протоколи для мереж будь-яких розмірів, проте мають два головні недоліки: підвищені вимоги до обчислювальної потужності маршрутизаторів і складне адміністрування.

### ХІД РОБОТИ

**Завдання №1.** Створіть схему, представлену на рисунку 11.1.

У чотирьох мережах: 11.0.0.0/8, 12.0.0.0/8, 13.0.0.0/8 і 14.0.0.0/8 встановлені комп'ютери з адресами:

Comp1 - 11.0.0.11, маска 255.0.0.0

Comp2 - 12.0.0.12, маска 255.0.0.0

Comp3 - 13.0.0.13, маска 255.0.0.0

Comp4 - 14.0.0.14, маска 255.0.0.0

Між ними знаходиться корпоративна мережа з шістьма маршрутизаторами. На маршрутизаторах задані наступні інтерфейси.

Таблиця 11.1 – Інтерфейси маршрутизаторів

маршрутизатор	інтерфейс 1	інтерфейс 2	інтерфейс 3
Router1	11.0.0.1/8	21.0.0.1/8	31.0.0.1/8
Router2	21.0.0.2/8	51.0.0.2/8	
Router3	12.0.0.3/8	61.0.0.3/8	51.0.0.3/8
Router4	31.0.0.4/8	81.0.0.4/8	13.0.0.4/8
Router6	61.0.0.6/8	81.0.0.6/8	14.0.0.6/8

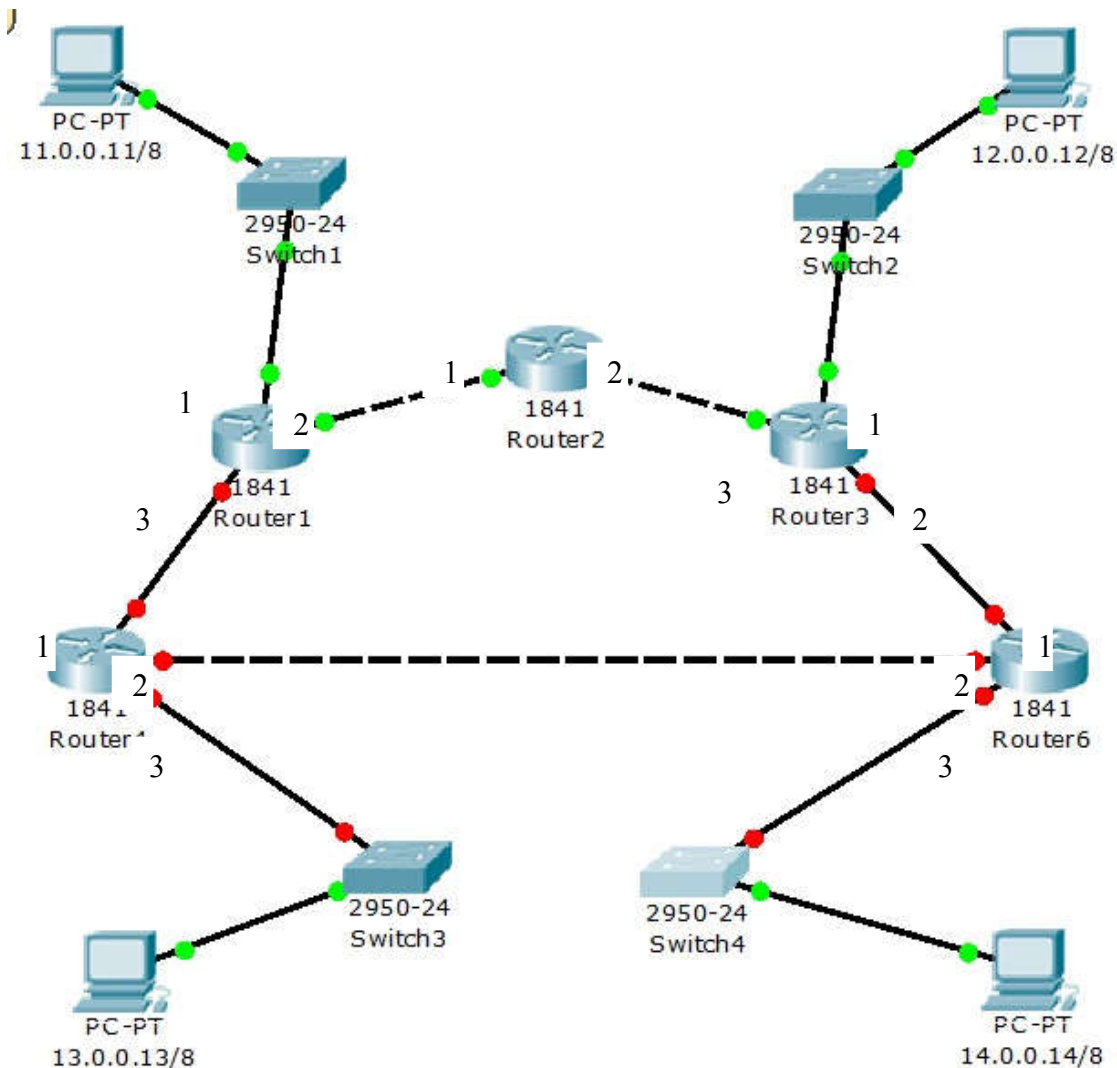


Рисунок 11.1 – Схема мережі.

Налаштуйте маршрутизацію по протоколу RIP на кожному з роутерів. Для цього:  
 1 - налаштуйте все маршрутизатори, як це було показано в лабораторній роботі №6;  
 2 - перевірте налаштування маршрутизаторів по таблиці маршрутизації.

Щоб переконатися в тому, що маршрутизатор дійсно правильно сконфігурували і працює коректно, перегляньте таблицю RIP роутера, використовуючи команду show наступним чином:

Router #**show ip route rip**

Наприклад для шостого маршрутизатора Router6 таблиця буде мати такий вигляд (рис.11.3):

```
Router6>en
Router6#show ip route rip
R    11.0.0.0/8 [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    12.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
R    13.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    21.0.0.0/8 [120/2] via 61.0.0.3, 00:00:08, Ethernet0/0/0
R    31.0.0.0/8 [120/1] via 81.0.0.4, 00:00:08, FastEthernet0/1
R    51.0.0.0/8 [120/1] via 61.0.0.3, 00:00:08, Ethernet0/0/0
Router6#
```

Рисунок 11.3 – Таблиця маршрутизації RIP



Дана таблиця показує, що до мережі 21.0.0.0 є два шляхи: через Router4 (мережа 81.0.0.0) і через Router3 (мережа 61.0.0.0).

Проведіть діагностику мережі:

1 - перевірте, чи правильно встановлена за допомогою команд ping і tracert в консолі кожного комп'ютера;

2 - проведіть ту ж діагностику мережі при вимкненому маршрутизаторе Router6.

3 - перевірте зв'язок між комп'ютерами з адресами 12.0.0.12 і 13.0.0.13.

Кількість проміжних роутерів при проходженні пакета по мережі при включеному і вимкненому маршрутизаторі 6 повинно бути різним. При включеному Router6 має бути на одиницю менше, ніж при вимкненому.

#### Завдання №2.

Створіть схему, представлену на рисунку 11.4.

Завдання.

1. Налаштуйте корпоративну мережу з використанням протоколу RIP.
2. Перевірте зв'язок між комп'ютерами Comp1 і Comp3 за допомогою команд ping і tracert при включеному і вимкненому п'ятому маршрутизаторі.
3. Перевірте зв'язок між комп'ютерами ПК0 і Comp1 за допомогою команд ping і tracert при включеному і вимкненому другому маршрутизаторі.

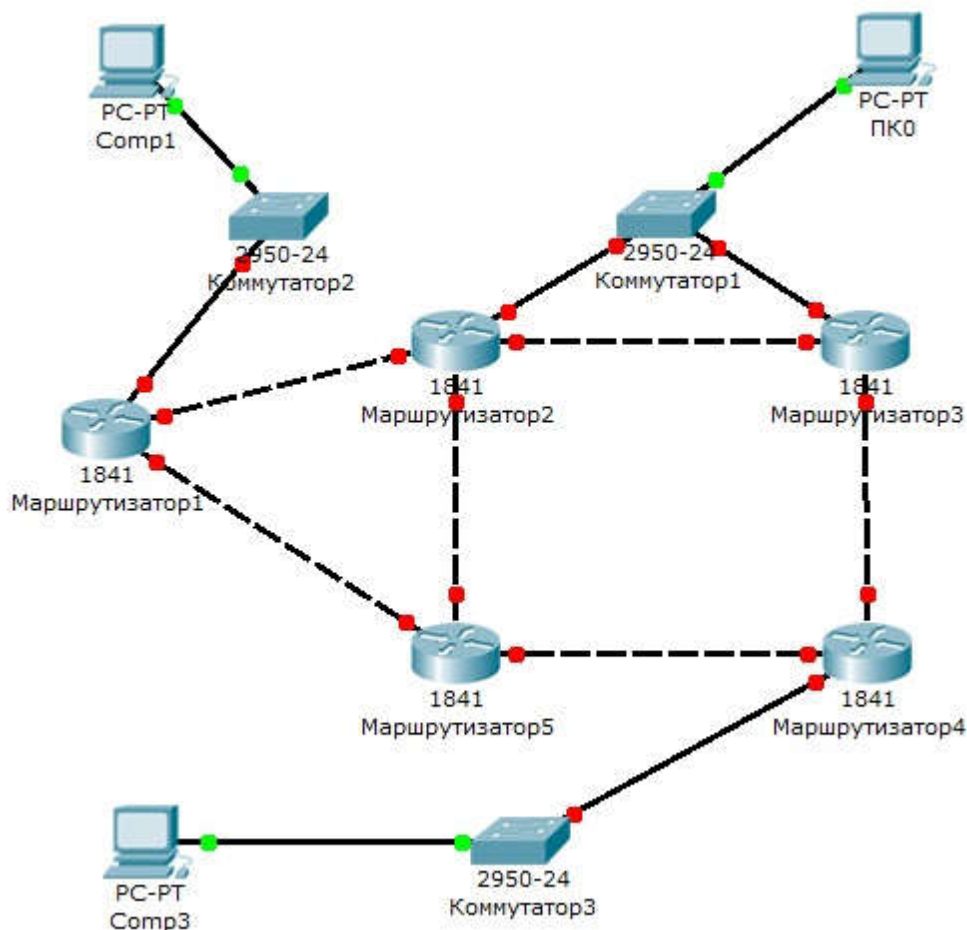


Рисунок 11.4 – Схема мережі.



## ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Короткі теоретичні відомості.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

## КОНТРОЛЬНІ ПИТАННЯ

1. У чому переваги статичної маршрутизації?
2. Дайте характеристику параметрам статичної таблиці маршрутизації?
3. Які етапи при установці пристрою притаманні маршрутизаторів компанії Cisco, але відсутні у комутаторів?
4. Яку із зазначених нижче команд можна зустріти в інтерфейсі командного рядка маршрутизатора, але не комутатора?
  - команда `clock rate`;
  - команда `ip address` маска адреса;
  - команда `ip address dhcp`;
  - команда `interface vlan 1`
5. Чим відрізняються інтерфейси командного рядка маршрутизатора і комутатора компанії Cisco?
6. Яка із зазначених нижче команд не покаже настройки IP-адрес і масок в своєму пристрої?
  - `show running-config`;
  - `show protocol` тип номер;
  - `show ip interface brief`;
  - `show version`
7. Перерахуйте основні функції маршрутизатора відповідно до рівнів моделі OSI.

## ЛАБОРАТОРНА РОБОТА №12. НАЛАШТУВАННЯ ПРОТОКОЛУ OSPF.

### ТЕОРЕТИЧНІ ВІДОМОСТІ

OSPF(англ. Open Shortest Path First) – протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology), що використовує для знаходження найкоротшого шляху Алгоритм Дейкстри (Dijkstra's algorithm).

Протокол OSPF був розроблений IETF в 1988 році. Остання версія протоколу представлена в RFC 2328. Протокол OSPF являє собою протокол внутрішнього шлюзу (Interior Gateway Protocol – IGP). Протокол OSPF поширює інформацію про доступні маршрути між маршрутизаторами однієї автономної системи.

Протоколи маршрутизації пропонують кращу масштабованість і збіжність у порівнянні з дистанційно-векторними протоколами. Робота протоколів базується на алгоритмі Дейкстри, який часто називають алгоритмом «найкоротший шлях - першим» (shortest path first SPF)). Найбільш типовим представником є протокол OSPF (Open Shortest Path First).

Властивості OSPF:

- висока швидкість збіжності;
- підтримка мережних масок змінної довжини VLSM;
- відсутність обмежень досяжності;
- оптимальне використання пропускної здатності мережі;
- оптимальний вибір шляху маршрутизації.

Згідно з RFC 2328 є незапатентований тобто відкритий для громадськості протокол, таким же, як є протокол RIP. Але OSPF на відміну від RIP, має значно більшу швидкість збіжності (рекалькуляції таблиці маршрутизації), немає обмеження на довжину шляху 15-ма хопами (англ. hop, укр. стрибок), враховує пропускну здатність мережі при виборі маршруту. Все це робить OSPF потужним, масштабованим протоколом маршрутизації.

### ХІД РОБОТИ

Створіть схему, представлену на рисунку 12.1.

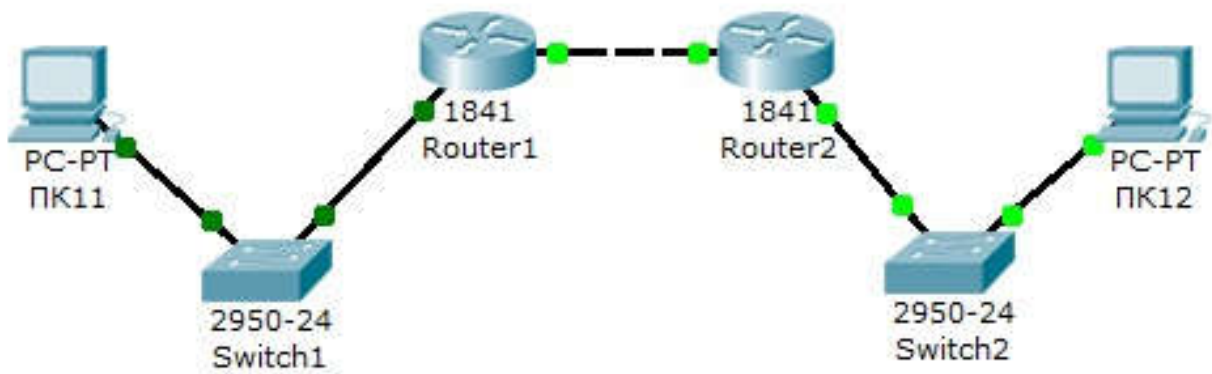


Рисунок 12.1 – Схема мережі.

На схемі представлені наступні три мережі:

Switch1 - мережа 10.11.0.0/16.

Switch2 - мережа 10.12.0.0/16.

Мережа для роутерів - 10.10.0.0/16.

Введіть на пристроях наступну адресацію. Маршрутизатор мають по два інтерфейси:  
Router1 - 10.11.0.1/16 і 10.10.0.1/16.  
Router2 - 10.10.0.2/16 і 10.12.0.1/16.  
ПК11 - 10.11.0.11/16.  
ПК12 - 10.12.0.12/16.

Візьміть схему мережі, представлену на рис 6.1.

Проведемо настройку протоколу OSPF на маршрутизаторі Router1.

Увійдіть в конфігурації в консоль роутера і виконайте наступні настройки (при введенні команд маску підмережі можна не вказувати, тому що вона буде братися автоматично з налаштувань інтерфейсу роутера):

Увійдіть в привілейований режим:

```
Switch>en
```

Увійдіть в режим конфігурації:

```
Switch1 #conf t
```

Увійдіть в режим конфігурації протоколу OSPF:

```
Router1 (config) #router ospf 1
```

У команді `router ospf <ідентифікатор_процеса>` під ідентифікатором процесу розуміється унікальне числове значення для кожного процесу роутінга на маршрутизаторі. Дане значення повинно бути більше в інтервалі від 1 до 65535. У OSPF процесам на роутерах однієї зони прийнято присвоювати один і той же ідентифікатор.

Підключіть клієнтську мережу до роутера:

```
Router1 (config-router) #network 10.11.0.0
```

Підключіть другу мережу до роутера:

```
Router1 (config-router) #network 10.10.0.0
```

Задайте використання другої версії протокол OSPF:

```
Router1 (config-router) #version 2
```

Вийдіть з режиму конфігурації протоколу OSPF:

```
Router1 (config-router) #exit
```

Вийдіть з консолі налаштувань:

```
Router1 (config) #exit
```

Збережіть налаштування в пам'ять маршрутизатора:

```
Switch1 #write memory
```

Аналогічно проведіть настройку протоколу OSPF на маршрутизаторі Router2.

### ЗМІСТ ЗВІТУ

1. Тема та мета лабораторної роботи.
2. Короткі теоретичні відомості.
3. Хід виконання роботи згідно з варіантом.
4. Висновки по виконаній роботі.

## КОНТРОЛЬНІ ПИТАННЯ

1. У чому відмінність між топологічною і дистанційно-векторною маршрутизацією?
2. Опишіть схему роботи протоколу RIP.
3. Опишіть схему роботи протоколу OSPF.
4. Перерахуйте основні етапи установки маршрутизатора.
5. Опишіть чотири етапи завантаження маршрутизатора.
6. Які із зазначених нижче протоколів працюють по дистанційно-векторному алгоритмі і які їхні основні відмінності?
  - RIP;
  - IGRP;
  - EIGRP;
  - OSPF
7. Дайте характеристику класів протоколів маршрутизації.
8. Наведіть класифікацію протоколів маршрутизації на основі алгоритмів їх роботи.
9. Зробіть порівняння класових і безкласових протоколів маршрутизації.
10. Зробіть порівняння протоколів маршрутизації внутрішнього шлюзу.
11. Опишіть етапи настройки протоколу маршрутизації RIP-2.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Радченко, Г.И. Распределенные вычислительные системы/ Г.И. Радченко. – Челябинск.: Фотохудожник, 2012. – 184 с.
2. Таненбаум Э. Распределенные системы. Принципы и парадигмы. / Э. Таненбаум, М. Ван-Стеен – Спб.: Питер, 2003. – 877 с.
3. Федоров А. Windows Azure. Облачная платформа Microsoft. / Федоров А., Д. Мартынов – Microsoft, 2010. – 96 с.
4. Соломон Д. Внутреннее устройство Microsoft Windows 2000. Мастер-класс./Пер. с англ. / Соломон Д., Русинович М. – Спб.: Питер, 2001. – 752с., илл.
5. Максвелл С. Ядро Linux в комментариях./Пер.с англ. – К.: Диасофт, 2000.
6. Костер Х. Основы Windows NT и NTFS. – М.: Издательский отдел "Русская редакция" ТОО "Channel Trading Ltd", 1996. - 440с., илл.
7. Таненбаум Э. Современные операционные системы. 2-ое изд. – Спб.:Питер, 2002, – 1040с.. илл.
8. Костер Х. Основы Windows NT и NTFS. – М.: Издательский отдел "Русская редакция" ТОО "Channel Trading Ltd", 1996. - 440с., илл.
9. Крюков А. А. Расширенное администрирование ОС Unix (Linux) – М.: Центр компьютерного обучения "Специалист" при МГТУ им. Н. Э. Баумана, 2006 – 446 с.
10. Таненбаум Э. Современные операционные системы. 2-ое изд. – Спб.:Питер, 2002, – 1040с.. илл.
11. Habrahabr [Электронный ресурс] Режим доступа: habrahabr.ru
12. Поляк-Брагинский А. Администрирование сети на примерах - Спб.: БХВ-Петербург, 2005 – 321 с.
13. Чекмарев А. Windows 7. Руководство администратора. - Спб.: БХВ-Петербург, 2010 – 896 с.
14. Русинович М. Утилиты Sysinternals. Справочник администратора. / Марк Русинович, Аарон Маргозис - Спб.: БХВ-Петербург, 2012 – 478 с.
15. Скембрей Дж. Секреты хакеров. Безопасность Windows Server 2003 - готовые решения. / Джоел Скембрей, Стюарт Мак-Клар – М.: Вильямс, 2004 – 512 с.

