НАВЧАЛЬНО-МЕТОДИЧНА ЛІТЕРАТУРА

Міністерство освіти та науки України
Тернопільський національний технічний університет
імені Івана Пулюя

Кафедра біотехнічних систем

МЕТОДИЧНІ ВКАЗІВКИ

для виконання лабораторних робіт
з дисципліни

ПЕРЕДАЧА БІОМЕДИЧНОЇ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

для студентів за напрямом підготовки
6.050902"Радіоелектронні апарати

Тернопіль, 2015

Хвостівський М.О. Методичні вказівки для виконання лабораторних робіт з дисципліни “Передача біомедичної інформації в комп’ютерних мережах” для студентів за напрямом підготовки 6.050902 “Радіоелектронні апарати” // Хвостівський М.О. – Тернопіль: ТНТУ імені Івана Пулюя, 2015. – 157 с.

Укладач: к.т.н., доц. Хвостівський М.О.

Відповідальний за випуск: в.о. зав. кафедрою Хвостівський М.О.

ЗМІСТ

Лабораторна робота №1
Мережеві пристрої і засоби комунікацій

Мета роботи: вивчення мережевих пристроїв та засобів комунікацій

ТЕОРЕТИЧНІ ВІДОМОСТІ

У якості засобів комунікації найбільше часто використовуються вита пара, коаксіальний кабель і оптоволоконні лінії. При виборі типу кабелю враховують наступні показники:

- **Вартість монтажу та обслуговування;**
- **Швидкість передачі інформації;**
- **Обмеження на величину відстані передачі інформації (без додаткових підсилювачів-повторювачів (репітерів));**
- **Безпека передачі даних.**

Головна проблема полягає в одночасному забезпеченні цих показників, наприклад, найвища швидкість передачі даних обмежена максимально можливим відстанню передачі даних, при якому ще забезпечується необхідний рівень захисту даних. Легка нарощуваність, простота розширення кабельної системи впливають на її вартість і безпеку передачі даних.

1.1 Мережні пристрої

Мережеві карти відповідають за передачу інформації між одиницями мережі. Будь-яка мережева карта складається з роз'єму для мережевого провідника і мікропроцесора, що кодує/декодує мережні пакети, а також допоміжних програмно-апаратних комплексів і служб. Кожна карта має свій MAC-адрес - унікальний ідентифікатор пристрою.

Рисунок 1.1 – Мережева карта

1.1.1 Коаксіальний кабель

Коаксіальний кабель має середню ціну, добре завадозахищений і застосовується для зв'язку на великі відстані (декілька кілометрів).

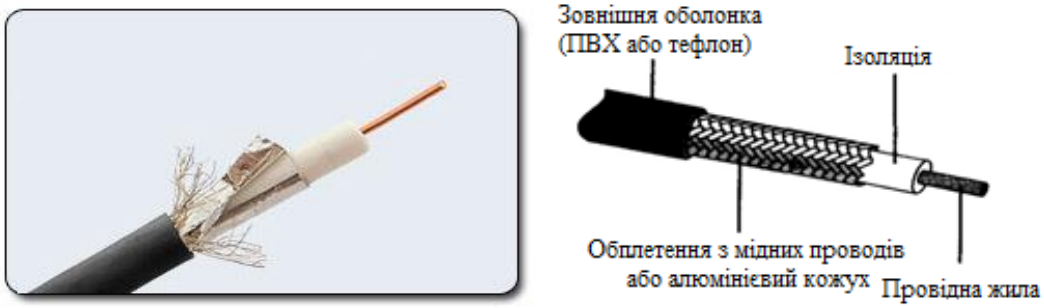


Рисунок 1.2 – Коаксіальний кабель

Швидкість передачі інформації від 1 до 10 Мбіт/с, а в деяких випадках може досягати 50 Мбіт/с. Коаксіальний кабель використовується для основної і широкосмугової передачі інформації.

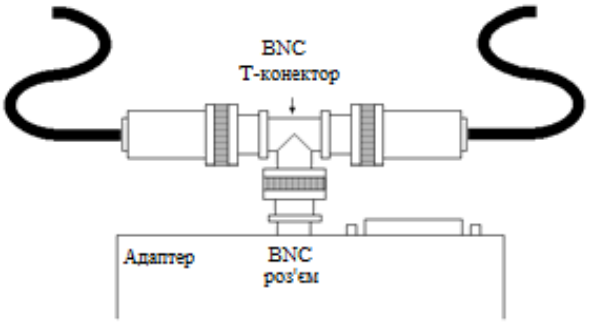


Рисунок 1.3 –Приєднання адаптера до тонкого коаксіальному кабелю

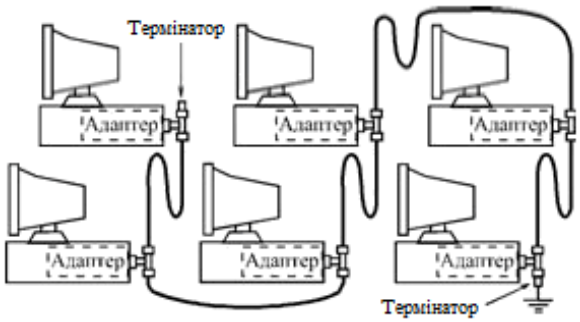


Рисунок 1.4 – З'єднання комп'ютерів мережі тонким кабелем

Мінімальний набір обладнання для односегментної мережі на тонкому кабелі повинен включати в себе наступні елементи:

- мережеві адаптери (за кількістю поєднуваних у мережу комп'ютерів) - (англ. *network interface card*) - периферійний пристрій, що дозволяє комп'ютеру взаємодіяти з іншими пристроями мережі;
- відрізки кабелю з *BNC-роз'ємами* на обох кінцях, загальна довжина яких достатня для об'єднання всіх комп'ютерів;
- *BNC Т-коннектори* (по числу мережевих адаптерів) (рис.1.5,а) (призначений для з'єднання трьох кабелів);
- один *BNC* термінатор без заземлення (термінатор - поглинач енергії на кінці довгої лінії, опір якої дорівнює хвильовому опору даної лінії) (рис.1.5,б);
- один *BNC* термінатор із заземленням (рис.1.5,в).

(а) (б) (в)

Рисунок 1.5 – Загальний вигляд BNC: (а) - BNC Т-коннектори, BNC термінатор без заземлення (б) і із заземленням (в)

Якщо мережа створюється з декількох сегментів з використанням репітерів і концентраторів, то треба враховувати, що деякі концентратори мають вбудовані 50-омні термінатори (іноді - відключаються), що спрощує проблеми узгодження.

Концентратор – це з'єднувальний компонент, до якого підключають усі комп'ютери в мережі за топологією «зірка» (рис.1,5,б).

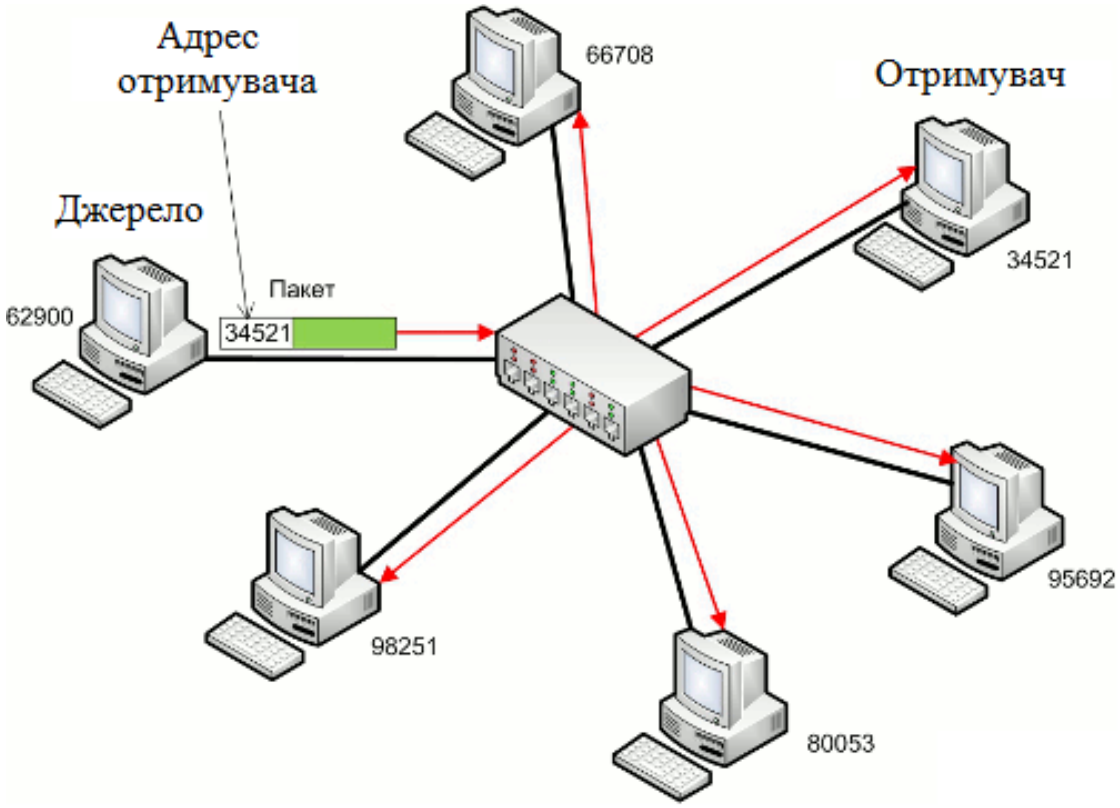


Рисунок 1.5,б – Приклад роботи з концентратором

1.1.2 Ethernet-кабель (RG-8, 10Base5)

Ethernet- кабель також є коаксіальним кабелем з хвильовим опором 50 Ом (рис.1.6).

Рисунок 1.6 – Загальний вигляд Ethernet-кабелів (RG-8, 10Base5)

Його називають ще товстий Ethernet (англ. thick) або жовтий кабель (англ. yellow cable). Він використовує 15 -контактне стандартне включення. Внаслідок завадозахищеності є дорогою альтернативою звичайним коаксіальним кабелям. Середня швидкість передачі даних 10 Мбіт/с. Максимально доступна відстань без повторювача не перевищує 500 м, а загальна відстань мережі Ethernet - близько 3000 м. Ethernet - кабель, завдяки своїй магістральної топології, використовує в кінці лише один навантажувальний резистор.

1.1.3 Cheapernet–кабель (RG-58, 10Base2)

Більш дешевим, ніж Ethernet-кабель є з'єднання Cheapernet-кабель (RG-58) (рисунок 1.7) або, як його часто називають, тонкий (англ. thin) Ethernet. Це також 50-омний коаксіальний кабель зі швидкістю передачі інформації в 10 Мбіт/с. При з'єднанні сегментів Cheapernet-кабелю також потрібні повторювачі. Обчислювальні мережі з Cheapernet-кабелем мають невелику вартість і мінімальні витрати при нарощуванні. З'єднання мережевих плат проводиться за допомогою широко використовуваних малогабаритних байонетних роз'ємів (СР-50) (рисунок 1.8) (байонет – тип з’єднання).

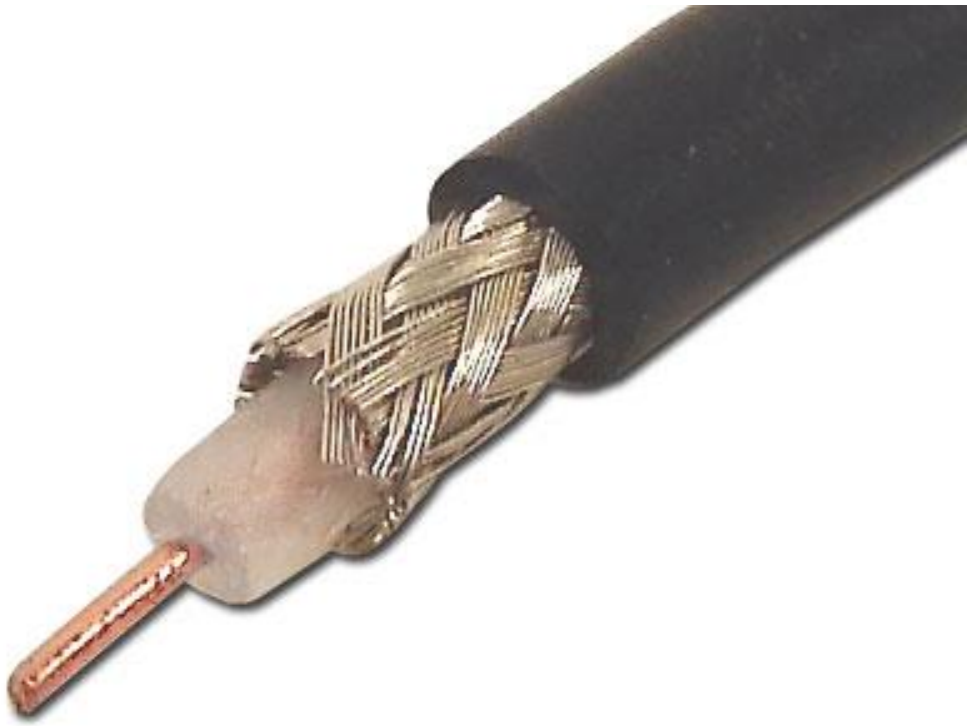


Рисунок 1.7 – Загальний вигляд Cheapernet–кабелю (RG-58, 10Base2)

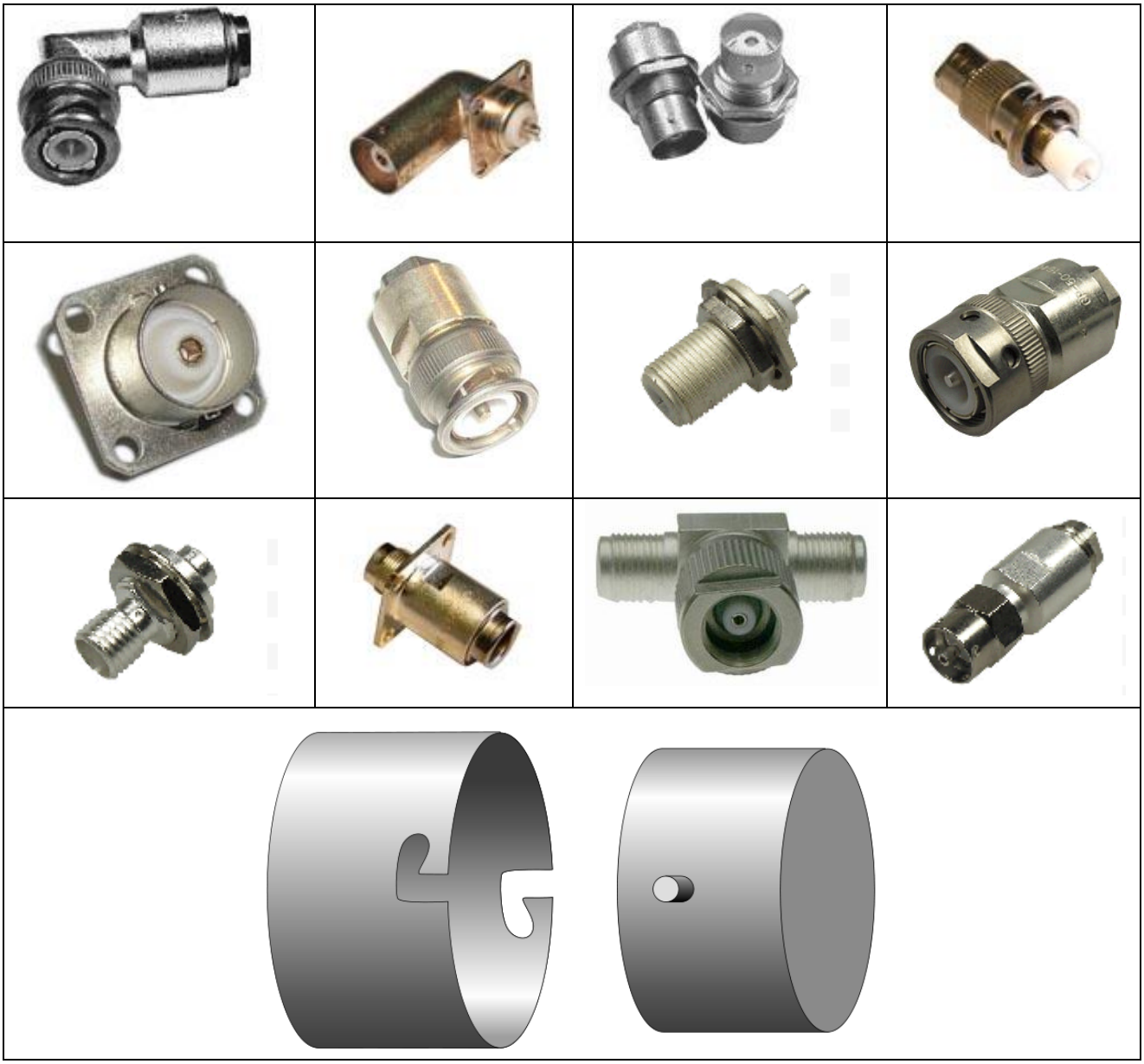


Рисунок 1.8 – Загальний вигляд роз’ємів типу СР-50

Додаткове екранування не потрібно. Кабель приєднується до ПК за допомогою трійникових з'єднувачів (T-connectors). Відстань між двома робочими станціями без повторювачів може становити максимум 300 м, а мінімум - 0,5 м, загальна відстань для мережі на Cheapernet-кабелю - близько 1000 м. Приймач Cheapernet розташований на мережевий платі як для гальванічної розв'язки між адаптерами, так і для підсилення зовнішнього сигналу

1.1.4 Широкосмуговий коаксіальний кабель

Широкосмуговий коаксіальний кабель (рисунок 1.9) несприйнятливий до завад, легко нарощується, але ціна його висока

Рисунок 1.9 – Загальний вигляд широкосмугового коаксіального кабелю RG-59 (75 Ом): жила - 24 AWG(0.6 мм, мідь, багатожильний), зовн. діам. - 6.1 мм, екран (сітка 95%), легкий, гнучкий

Швидкість передачі інформації дорівнює 500 Мбіт/с. При передачі інформації в базисної смузі частот на відстань більше 1,5 км потрібно підсилювач, або так званий репітер (англ. repeater - повторювач). Тому сумарну відстань при передачі інформації збільшується до 10 км. Для обчислювальних мереж з топологією типу «шина» або «дерево» коаксіальний кабель повинен мати на кінці узгоджувальний резистор (термінатор).

1.1.5 Вита пара (10BaseT)

Найбільш дешевим кабельним з'єднанням є вите двожильнопровідне з'єднання часто зване «витою парою» (англ. twisted pair) (рис. 1.10). Вона дозволяє передавати інформацію зі швидкістю до 10 Мбіт/с, легко нарощується, проте є завадонезахищеною. Довжина кабелю не може перевищувати 1000 м при швидкості передачі 1 Мбіт/с. Перевагами є низька ціна і безпроблемна установка.

Неекранована кручена пара складається з восьми проводів. Кожен провід ізольований окремо; всі вісім проводів зібрані в чотири звиті пари. Завивка проводів запобігає перехресним перешкодам, що наводяться сусідніми парами і зовнішніми джерелами. Всі чотири пари поміщені в загальну оболонку.

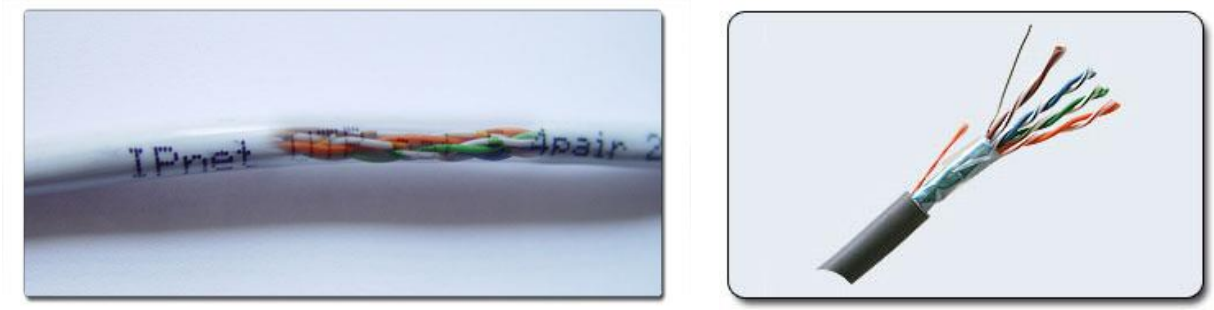


Рисунок 1.10 – Вита пара

З кабелями типу «вита пара» використовуються роз'єми RJ45 (рис.1.11), ті ж, що і у стандартних телефонних кабелів, тільки з вісьмома контактами замість чотирьох або шести.

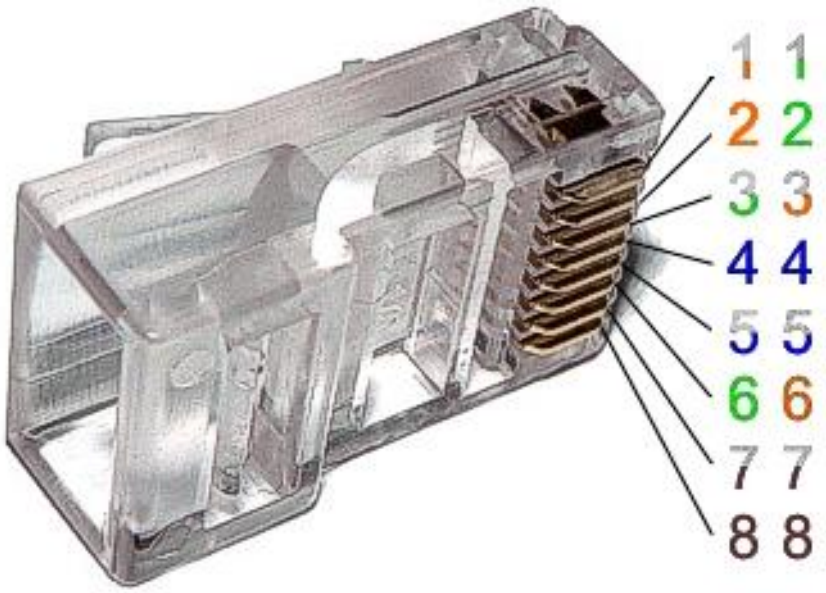


Рисунок 1.11 – Загальний вигляд роз'єму RJ45

Для підвищення завадозахищеності інформації часто використовують екрановану виту пару, тобто виту пару, вміщену в екрану оболонку, подібно екрану коаксіального кабелю. Це збільшує вартість витої пари і наближає її ціну до ціни коаксіального кабелю.

У телефонних мережах вита пара використовується вже не одне десяти - річчя, а ось до комп'ютерних мереж її пристосували відносно недавно. Вита пара витіснила коаксіальний кабель зі світу ЛОМ завдяки кільком явним перевагам. По-перше, кабель «вита пара »складається з восьми окремих проводів, що робить його гнучкіше коаксіального і, відповідно, полегшує його укладання. По-друге, до прокладання кабелів для ЛОМ можна сміливо залучати тисячі готових кваліфікованих монтажників телефонних кабелів. У нових будівлях часто телефонний і мережевий кабелі одночасно укладає один і той же підрядник.

Мінімальний набір обладнання для мережі на витій парі включає в себе наступні елементи:

- мережеві адаптери (за кількістю поєднуваних у мережу комп'ютерів), що мають UTP-роз'єми *RJ-45;*
- відрізки кабелю з роз'ємами *RJ-45* на обох кінцях (по числу об'єднуються комп'ютерів);
- один концентратор, що має стільки UTP-портів з роз'ємами *RJ-45,* скільки необхідно об'єднати комп'ютерів.

1.1.6 Оптоволоконні лінії (10 BaseFL)

Найбільш дорогими є оптопровідники (рис.1.12), звані також кабелем.

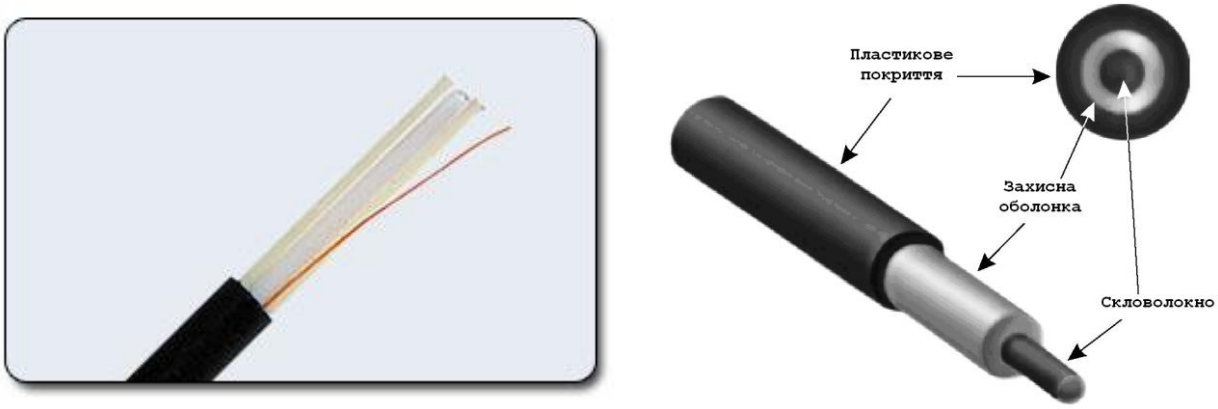


Рисунок 1.12 – Оптоволокно

Швидкість поширення інформації з них досягає 100 Мбіт/с, а на експериментальних зразках обладнання - 200 Мбіт/с. Допустиме видалення більш 50 км. Зовнішній вплив завад практично відсутній. На даний момент це найбільш дороге з'єднання для ЛОМ. Застосовуються там, де виникають електромагнітні поля завад або потрібна передача інформації на дуже великі відстані без використання повторювачів. Вони володіють властивостями, тому що техніка відгалужень в оптоволоконних кабелях дуже складна. Оптопровідники об'єднуються в ЛВМ за допомогою зіркоподібного з'єднання.

Передача інформації в цьому випадку йде по двох оптоволоконним кабелях, що передають сигнали в різні сторони (як і в *10BASE-T).* Іноді використовуються двопровідні оптоволоконні кабелі, що містять два кабелі в загальній зовнішній оболонці, але частіше - два одиночних кабелі. Всупереч поширеній думці, вартість оптоволоконного кабелю не занадто висока (вона близька до вартості тонкого коаксіального кабелю). Правда, в цілому апаратура в даному випадку виявляється помітно дорожче, тому що вимагає використання дорогих оптоволоконних трансиверів (англ. *Transceiver* — приймодавач).

1.1.7 Специфікація IEEE 802.3d FOIRL

Специфікація IEEE 802.3d Fiber Optic Inter Repeater Link (FOIRL) була запропонована в 1987 році. Вона була призначена для забезпечення інформаційної взаємодії репітерів (*мережеве обладнання для підсилювання сигналу*), які знаходяться на значній (до 1000 м) відстані один від одного. Для підключення до волоконно-оптичної лінії (ВОЛ) використовувалися з'єднувачі типу SMA і ST.

Надалі, проте дана технологія не отримала розвитку, оскільки з'явилися нові мережеві технології сімейства 10 Base-F, які також використовували волоконно-оптичний кабель для передачі даних і забезпечували найкращі інформаційні та експлуатаційні характеристики.

Використання волоконно-оптичного кабелю для передачі даних

Основними перевагами передачі даних по волоконно-оптичних лініях зв'язку (ВОЛЗ) є:

- Висока швидкість передачі даних - межа для промислових ВОЛЗ 3ГГц, в той час, як для мідного кабелю це значення становить не більше 500 МГц.
- Нечутливість до електромагнітних завад

- Відсутність електромагнітного випромінювання при передачі даних
- Забезпечення гальванічної розв'язки між передавачем і приймачем даних

Волоконно-оптичний кабель складається з таких компонентів: оптичне волокно, оптичний екран, захисний екран.

Власне середовище передачі - оптичне волокно являє собою скляну або пластмасову жилу, товщина якої залежно від призначення кабелю може змінюватися в межах від одиниць до сотень мікрон. Діаметр центрального волокна однозначно визначає експлуатаційні характеристики використовуваного волоконно-оптичного кабелю. Кабелі з діаметром волокна 10 мікрон називаються одномодовими за назвою режиму випромінювання передавального елемента - лазера. Кабелі з діаметром волокна 60 і більше мікрон називаються багатомодовими. Одномодові волоконно-оптичні кабелі (Single Mode Fiber - SMF) більш складні у виготовленні та експлуатації, однак, вони здатні забезпечувати більшу дальність поширення інформаційного сигналу. Дешевші у виготовленні і зручні в експлуатації багатомодові (Multi Mode Fiber - MMF) кабелі забезпечують меншу дальність розповсюдження інформаційного сигналу.

Для позначення типу волоконно-оптичного кабелю використовують вислів види:

<Діаметр волокна> / <Діаметр екрана>, в мікро метрах наприклад: 62.5/125

Найбільше поширення для передачі даних в локальних мережах в даний час отримав багатомодовий волоконно-оптичний кабель, однак, для забезпечення передачі даних зі швидкістю понад 1 ГГц на великі відстані може бути використаний тільки одномодовий волоконно-оптичний кабель.

1.1.8 Специфікації 10 Base F

Сукупність стандартів 10 Base F (IEEE 802.3j) визначає протоколи фізичного рівня для передачі даних по волоконно-оптичному кабелю в мережах IEEE 802.3.

1.1.9 Специфікація 10 Base FB

Специфікація 10 Base FB (Fiber Back Bone) визначає спеціальний протокол фізичного рівня, який призначений для забезпечення підвищення ефективності інформаційної взаємодії репітерів в мережах IEEE 802.3.

Для забезпечення синхронізації тактових генераторів в відсутність надісланих та кадрів передавач і приймач обмінюються синхронізуючими послідовностями 2.5 МГц.

Протокол 10 Base FB не є універсальним і не забезпечує, зокрема, інформаційну взаємодію між репітером і робочою станцією.

1.1.10 Специфікація 10 Base FP

Специфікація 10 Base FP (Fiber Passive) визначає інтерфейс фізичного рівня для забезпечення взаємодії компонентів локальної мережі з використанням принципу пасивного оптичного розгалужувача. При використанні технології 10 Base FP можлива побудова пасивної об'єднуючої структури, яка може забезпечити взаємодію 33 робочих станцій знаходяться на віддаленні до 500 м.

1.1.11 Специфікація 10 Base FL

Специфікація 10 Base FL (Fiber Link) визначає протокол передачі даних по двох волоконно-оптичним кабелям зі швидкістю 10 Мбіт/сек на відстань до 2000м. Протокол фізичного рівня 10 Base FL забезпечує інформаційну взаємодію в різних варіантах:

- Робоча станція - робоча станція
- Робоча станція - репітер
- Репітер - репітер

Таблиця 1.1 – Параметри протоколу фізичного рівня 10 Base FL

№	Параметр	Значення параметру
1	Швидкість передачі даних	10 Мбіт
2	Тип кабелю	62,5/125
3	Макс. довжина сегмента	2000 м
4	Тип з'єднувачів	ST

У *10BASE-FL* застосовується мультимодовий кабель і світло з довжиною хвилі 850 нанометрів, однак є апаратура і для використання одномодового кабелю (з граничною довжиною до 5 км). Оптоволоконний трансивер називається *FOMAU* (Fiber Optic MAU). Він виконує всі функції звичайного трансивера *(MAU),* але, крім того, перетворює електричний сигнал в оптичний при передачі і назад при прийомі. *FOMAU* також формує і контролює сигнал цілісності лінії зв'язку, що передається в паузах між пакетами. Цілісність лінії зв'язку, як і у випадку *10BASE-T* , відображається світлодіодами "Link" і визначається за наявністю між переданими пакетами сигналу "Idle" частотою 1 МГц. Для приєднання трансивера до адаптера застосовується стандартний *AUI* –кабель (рис.1.13), такий же, як і у випадку*10BASE5* , але довжина його не повинна перевищувати 25 метрів. Є також мережеві адаптери з вбудованими трансиверами *FOMAU* , які мають тільки зовнішні оптоволоконні роз'єми і не потребують трансиверного кабелях.

Рисунок 1.13 – Загальний вигляд *AUI*-кабелю

Довжина оптоволоконних кабелів, що з'єднують трансивер і концентратор, може досягати 2 кілометрів без застосування яких би то не було ретрансляторів. Таким чином, можливе об'єднання в локальну мережу комп'ютерів, що знаходяться в різних будівлях, рознесених територіально.

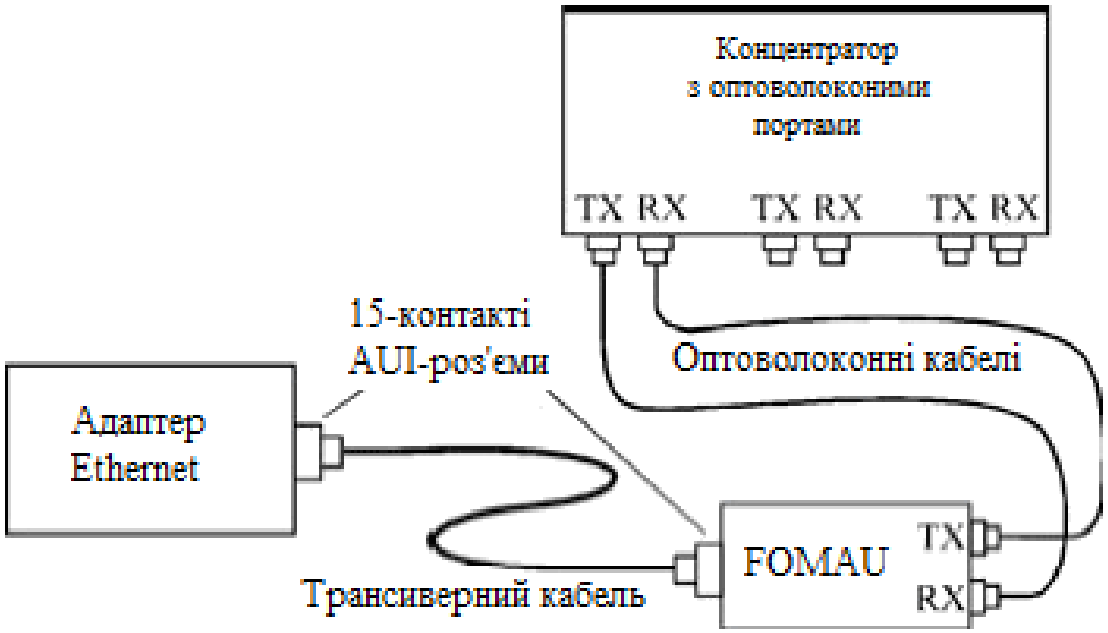


Рисунок 1.14 – З'єднання адаптера і концентратора в 10BASE-FL

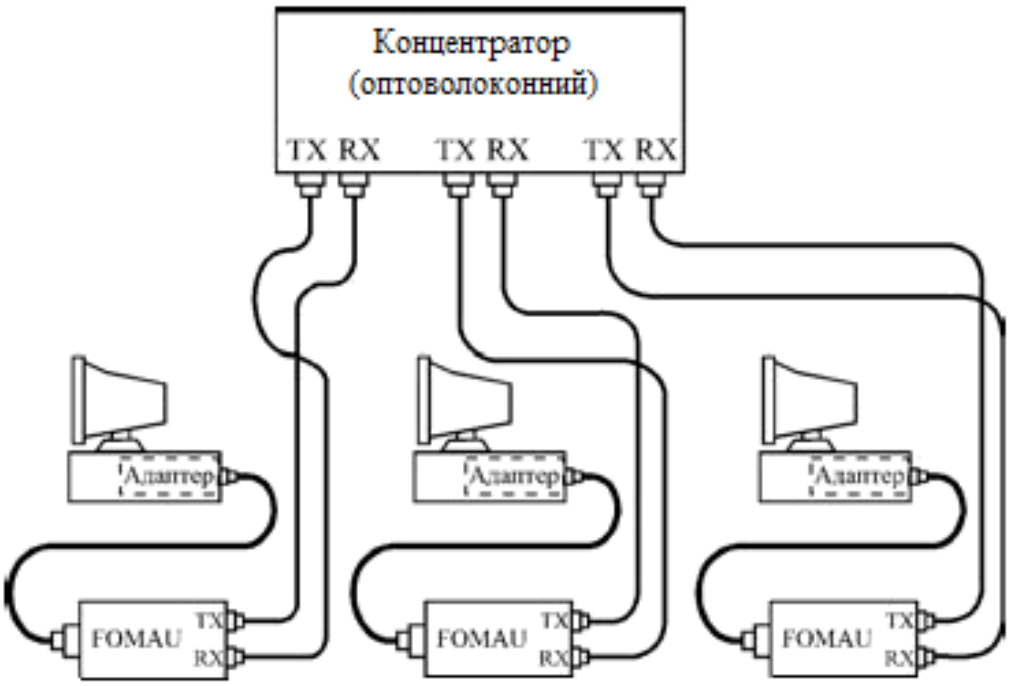


Рисунок 1.15 – Об'єднання комп'ютерів у мережу за стандартом 10BASE-FL

Як і у випадку 10BASE-T, кілька концентраторів можуть об'єднуватися між собою для отримання деревовидної топології. Взагалі, найбільш часто сегмент 10BASE-FL якраз і використовується для з'єднання двох концентраторів. А до концентраторів підключаються комп'ютери за стандартом

10BASE-T. Таким чином, вдається поєднати переваги обох сегментів - низьку вартість 10BASE-T і великі відстані 10BASE-FL.

Мінімальний набір обладнання для з'єднання оптоволоконним кабелем двох комп'ютерів включає в себе наступні елементи:

- два мережевих адаптера з трансиверними роз'ємами;
- два оптоволоконних трансиверів (FOMAU);
- два трансиверних кабелів;
- два оптоволоконних кабелів з ST-роз'ємами (або з SC або з MIC роз'ємами) на кінцях.

Існує безліч оптичних коннекторів. Основні їх типи представлені в таб.1.1.

Таблиця 1.2 – Типи оптичних коннекторів

Позначення	**Зовнішній вигляд**	**Опис**	**Втрати (Дб) при 1300 нм для багатомода / одномод**
1	2	3	4
ST - **S**traight **T**ip connector		Початковий тип, на даний момент застарілий. Фіксація за допомогою повороту навколо осі на 1/4 обороту. Обертання основи виключається за рахунок поздовжнього паза в роз'ємі розетки. Вимагає багато вільного місця при монтажі / демонтажі. Оптичний наконечник - кераміка, діаметром 2.5 мм з округленим торцем.	0.25/0.3
FC - **F**iber-Optic **C**onnector		Розвиток ST-типу. Різьбова фіксація оправи забезпечує чудові характеристики.	0.2/0.6
SC - **S**quare/**S**ubscriber **C**onnector		Установка / демонтаж здійснюється тільки зворотно-поступальним рухом, ніяких обертових частин (переважно). Оптичний наконечник - 2.5 мм в діаметрі, майже повністю прихований корпусом. Корпус має засувки для фіксації в гнізді. Можуть мати пристосування для кріплення парного наконечника або випускатися в дуплексному варіанті. Колір корпусу для одномод - блакитний, для многомода - сірий.	0.2/0.25

Продовження таблиці 1.1

1	2	3	4
LC -Little *or* Local Connector		Малогабаритний варіант SC-конектора. Корпус оснащений засувкою, подібної клямці на RJ-45 роз'ємі. Наконечник керамічний, діаметр 1.25 мм.	0.1/0.1

Варіант виконання коннектора SC у форматі Double (двійної) для багатомодового волокна (рис.1.16).

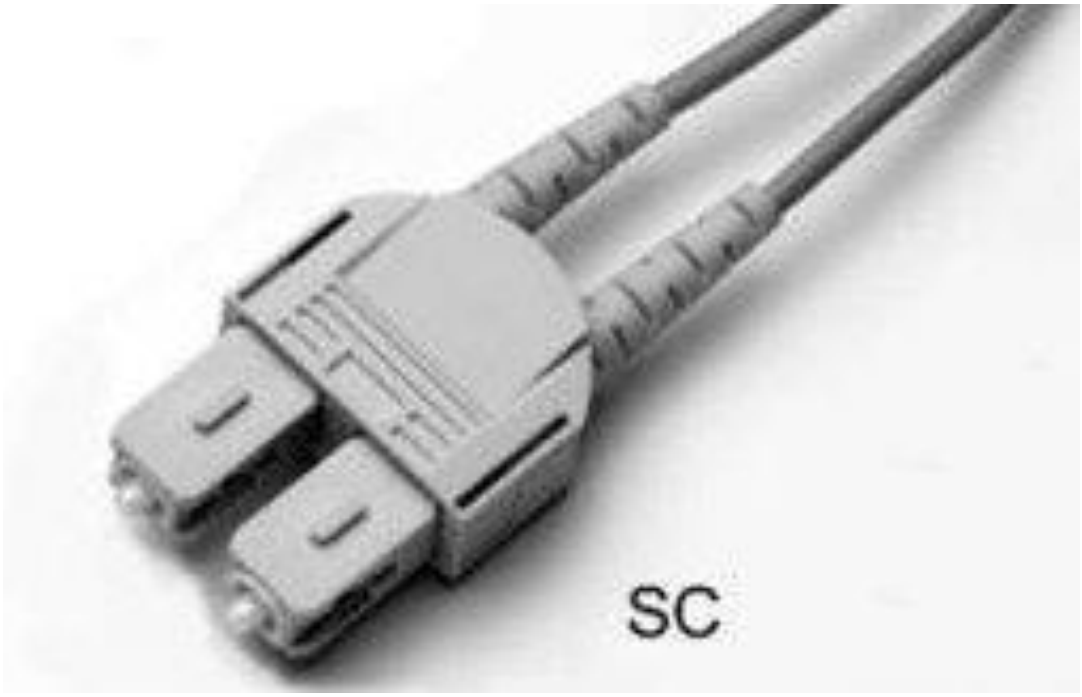


Рисунок 1.16 – Коннектор SC у форматі Double

Показники трьох найбільш типових засобів комунікацій для передачі даних наведено в таблицях 1.3-1.4.

Таблиця 1.3 – Основні показники засобів комунікації

Показники	**Засоби комунікацій для передачі даних**		
	Двожильна вита пара	*Коаксіальний кабель*	*Оптоволоконний кабель*
Ціна	Невисока	Відносно висока	Висока
Нарощування	Дуже просте	Проблематично	Просте
Захист від прослуховування	Незначна	Хороша	Висока
Проблеми з заземленням	Ні	Можливі	Ні
Сприйнятливість до перешкод	Існує	Існує	Відсутня

Таблиця 1.4 – Порівняльні характеристики мережевих провідників

Тип кабелю (10 Мбіт / с = близько 1 Мб в сек)	Швидкість передачі даних (мегабіт в секунду)	Макс офіційна довжина сегмента, м	Макс неофіційна довжина сегмента, м	Можливість відновлення при пошкодженні / Нарощування довжини	Схильність до завад	Вартість
Вита пара						
Неекранована Вита пара	100/10/1000 Мбіт / с	100/100/100 м	150/300/100 м	Хороша	Середня	Низька
Екранована кручена пара	100/10/1000 Мбіт / с	100/100/100 м	150/300/100 м	Хороша	Низька	Середня
Кабель польовий П-296	100/10 Мбіт / с	------	300 (500) / 800 м	Хороша	Низька	Висока
Чотирижильний телефонний кабель	30/10 Мбіт / с	------	Не більше 30 м	Хороша	Висока	Дуже низька
Коаксіальний кабель						
Тонкий коаксіальний кабель	10 Мбіт / с	185 м	250 (300) м	Погана Необхідна пайка	Висока	Низька
Товстий Коаксіальний кабель	10 Мбіт / с	500 м	600 (700)	Погана Необхідна пайка	Висока	Середня
Оптоволокно						
Одномодове оптоволокно	100-1000 Мбіт	До 100 км	----	Потрібно спец обладнання	Відсутня	1-3 $ за метр
Багатомодове оптоволокно	1-2 Гбіт	До 550 м	----	Потрібно спец обладнання	Відсутня	1-3 $ за метр

Існує ряд принципів побудови ЛОМ на основі вище розглянутих компонентів. Такі принципи ще називають топологіями.

1.2 Топології обчислювальних мереж

1.2.1 Топологія «зірка»

Концепція топології мережі у вигляді зірки прийшла з області великих ЕОМ, у якій головна машина одержує й обробляє всі дані з периферійних пристроїв як активний вузол обробки даних. Цей принцип застосовується в системах передачі даних, наприклад, в електронній пошті мережі RelCom. Вся

інформація між двома периферійними робочими місцями проходить через центральний вузол обчислювальної мережі.

Пропускна здатність мережі визначається обчислювальною потужністю вузла і гарантується для кожної робочої станції. Колізій (зіткнень) даних не виникає.

Кабельне з'єднання досить просте, тому що кожна робоча станція пов'язана з вузлом. Витрати на прокладку кабелів високі, особливо коли центральний вузол географічно розташований не в центрі топології.

При розширенні обчислювальних мереж не можуть бути використані раніше виконані кабельні зв'язки: до нового робочого місця необхідно прокладати окремий кабель з центра мережі.

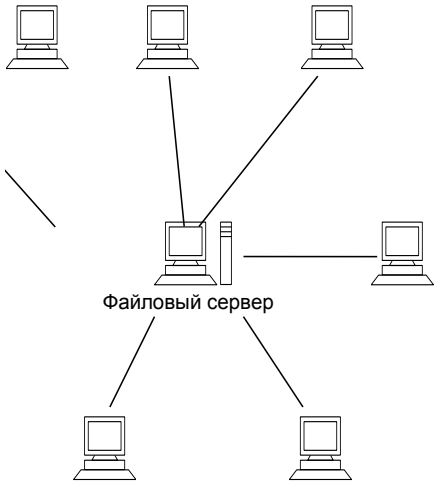


Рисунок 1.17 – Структура топології ЛОМ в вигляді «зірки»

Топологія у виді зірки є найбільш швидкодіючої з усіх топологій обчислювальних мереж, оскільки передача даних між робочими станціями проходить через центральний вузол (при його гарній продуктивності) по окремих лініях, використовуваним тільки цими робочими станціями. Частота запитів передачі інформації від однієї станції до іншої невисока в порівнянні з досягається в інших топологіях.

Продуктивність обчислювальної мережі в першу чергу залежить від потужності центрального файлового сервера. Він може бути вузьким місцем обчислювальної мережі. У разі виходу з ладу центрального вузла порушується робота всієї мережі.

Центральний вузол керування - файловий сервер реалізує оптимальний механізм захисту проти несанкціонованого доступу до інформації. Вся обчислювальна мережа може управлятися з її центру.

1.2.2 Кільцева топологія

При кільцевій топології мережі робочі станції пов'язані одна з іншою по колу, тобто робоча станція 1 з робочою станцією 2, робоча станція 3 з робочою станцією 4 і т.д. Остання робоча станція пов'язана з першою. Комунікаційна зв'язок замикається в кільце (рисунок 1.18).

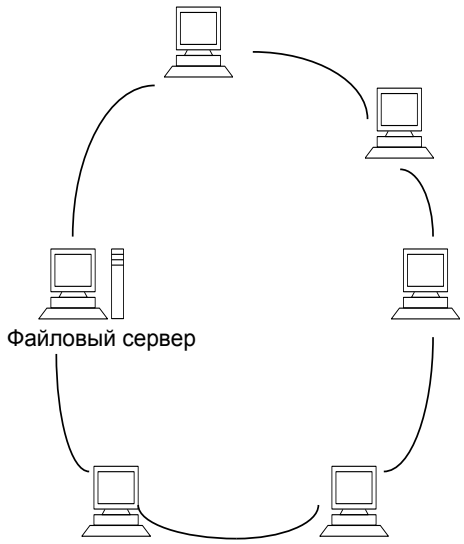


Рисунок 1.18 – Структура кільцевої топології ЛОМ

Прокладка кабелів від однієї робочої станції до іншої може бути досить складною і дорогою, особливо якщо географічне розташування робочих станцій далеко від форми кільця (наприклад, у лінію).

Повідомлення циркулюють регулярно по колу. Робоча станція посилає по визначеній кінцевій адресі інформацію, попередньо отримавши з кільця запит. Пересилання повідомлень є дуже ефективною, тому що більшість повідомлень можна відправляти «у дорогу» по кабельній системі одне за іншим. Дуже просто можна зробити кільцевий запит на всі станції. Тривалість передачі інформації збільшується пропорційно кількості робочих станцій, що входять в обчислювальну мережу.

Основна проблема при кільцевій топології полягає в тому, що кожна робоча станція повинна активно брати участь у пересиланні інформації, і у разі виходу з ладу хоча б однієї з них вся мережа паралізується. Несправності в кабельних з'єднаннях локалізуються легко.

Підключення нової робочої станції вимагає коротко термінового вимикання мережі, тому що під час установки кільце повинне бути розімкнутими. Обмеження на довжину обчислювальної мережі не існує, так як воно, в кінцевому рахунку, визначається винятково відстанню між двома робочими станціями.

Спеціальною формою кільцевої топології є логічна кільцева мережа. Фізично вона монтується як з'єднання зоряних топологій. Окремі зірки включаються за допомогою спеціальних комутаторів (англ. Hub - концентратор), які іноді називають «хаб». Залежно від числа робочих станцій і довжини кабелю між робочими станціями застосовують активні або пасивні концентратори. Активні концентратори додатково містять підсилювач для підключення від 4 до 16 робочих станцій. Пасивний концентратор є винятково розгалужувальний пристроєм (максимум на три робочі станції). Управління окремою робочою станцією в логічній кільцевій мережі відбувається так само, як і в звичайній кільцевій мережі. Кожній робочій станції присвоюється відповідний їй адрес, за яким передається керування (від старшого до

молодшого і від самого молодшого до самого старшого). Розрив з'єднання відбувається тільки для нижче розташованого (найближчого) вузла обчислювальної мережі, так що лише в рідких випадках може порушуватися робота всієї мережі.

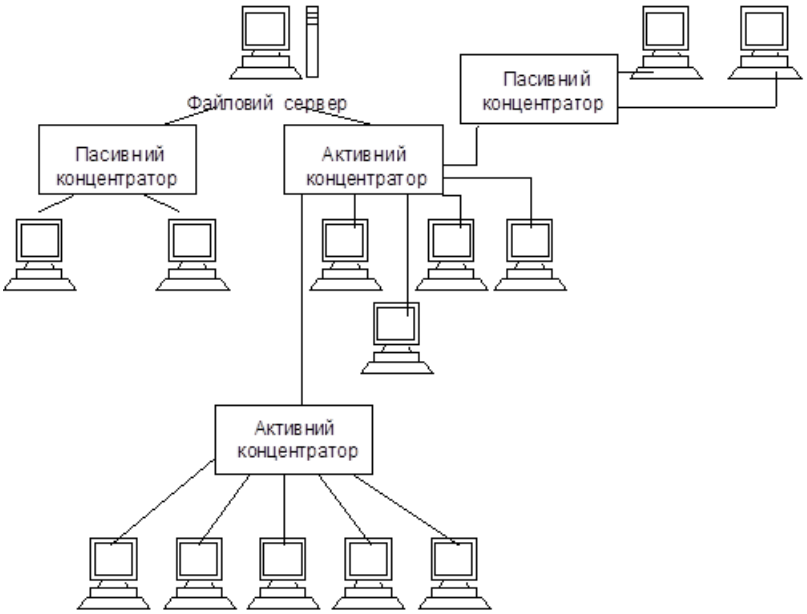


Рисунок 1.19 – Структура логічного кільцевого вузла ЛОМ

1.2.3 Шинна топологія

При шинній топології середовище передачі інформації представляється у формі комунікаційного шляху, доступного для всіх робочих станцій, до якого вони всі повинні бути підключені. Всі робочі станції можуть безпосередньо вступати в контакт з будь-якою робочою станцією, наявною в мережі.

Рисунок 1.20 – Структура шинної топології ЛОМ

Робочі станції в будь-який час, без переривання роботи всієї обчислювальної мережі, можуть бути підключені до неї або відключені. Функціонування обчислювальної мережі не залежить від стану окремої робочої станції.

У стандартній ситуації для шинної мережі Ethernet часто використовують тонкий кабель або Cheapernet-кабель з трійниковим з'єднувачем. Відключення і особливо підключення до такої мережі вимагають розриву шини, що викликає порушення циркулюючого потоку інформації і зависання системи.

Нові технології пропонують пасивні штепсельні коробки, через які можна відключати і/або підключати робочі станції під час роботи обчислювальної мережі.

Завдяки тому, що робочі станції можна підключати без переривання мережних процесів і комунікаційного середовища, дуже легко прослухувати інформацію, тобто відгалужувати інформацію з комунікаційного середовища.

У ЛОМ з прямою (не модулюючою) передачею інформації завжди може існувати тільки одна станція, що передає інформацію. Для запобігання колізій у більшості випадків застосовується часовий метод поділу, згідно з яким для кожної підключеної робочої станції у визначені моменти часу надається виключне право на використання каналу передачі даних. Тому вимоги до пропускної здатності обчислювальної мережі при підвищеному навантаженні підвищуються, наприклад, при введенні нових робочих станцій. Робочі станції приєднуються до шини за допомогою пристроїв ТАР (англ. Terminal Access Point - точка підключення термінала). ТАР являє собою спеціальний тип приєднання до коаксіального кабелю. Зонд голчастої форми впроваджується через зовнішню оболонку зовнішнього провідника і шар діелектрика до внутрішнього провідника і приєднується до нього.

У ЛОМ з модульованою широкосмуговою передачею інформації різні робочі станції отримують, у міру потреби, частоту, на якій ці робочі станції можуть відправляти і отримувати інформацію. Надсилаються дані модулюють на відповідних несучих частотах, тобто між середовищем передачі інформації і робочими станціями знаходяться відповідно модеми для модуляції і демодуляції. Техніка широкосмугових повідомлень дозволяє одночасно транспортувати в комунікаційному середовищі досить великий обсяг інформації. Для подальшого розвитку дискретного транспортування даних не грає ролі, яка первісна інформація подана в модем (аналогова чи цифрова), так як вона все одно надалі буде перетворена.

Основні характеристики трьох найбільш типових топологій обчислювальних мереж приведені в таблиці 1.5.

Таблиця 1.5 – Основні характеристики топологій обчислювальних мереж

Характеристики	**Топології обчислювальних мереж**		
	Зірка	*Кільце*	*Шина*
Вартість розширення	Незначна	Середня	Середня
Приєднання абонентів	Пасивне	Активне	Пасивне
Захист від відмов	Незначна	Незначна	Висока
Розміри системи	Будь-які	Будь-які	Обмежений
Захищеність від прослуховування	Хороша	Хороша	Незначна
Вартість підключення	Незначна	Незначна	Висока
Поведінка системи при високих навантаженнях	Хороше	Задовільний	Погане

Продовження таблиці 1.5

Можливість роботи в реальному режимі часу	Дуже хороша	Хороша	Погана
Розведення кабелю	Хороша	Задовільна	Хороша
Обслуговування	Дуже гарне	Середнє	Середнє

1.2.4 Деревоподібна структура ЛОМ

Поряд з відомими топологіями обчислювальних мереж «кільце», «зірка» і «шина», на практиці застосовується і комбінована, на приклад деревовидна структура. Вона утворюється в основному у вигляді комбінацій вищезгаданих топологій обчислювальних мереж. Підстава дерева обчислювальної мережі (корінь) розташовується в точці, в якій збираються комунікаційні лінії інформації (гілки дерева).

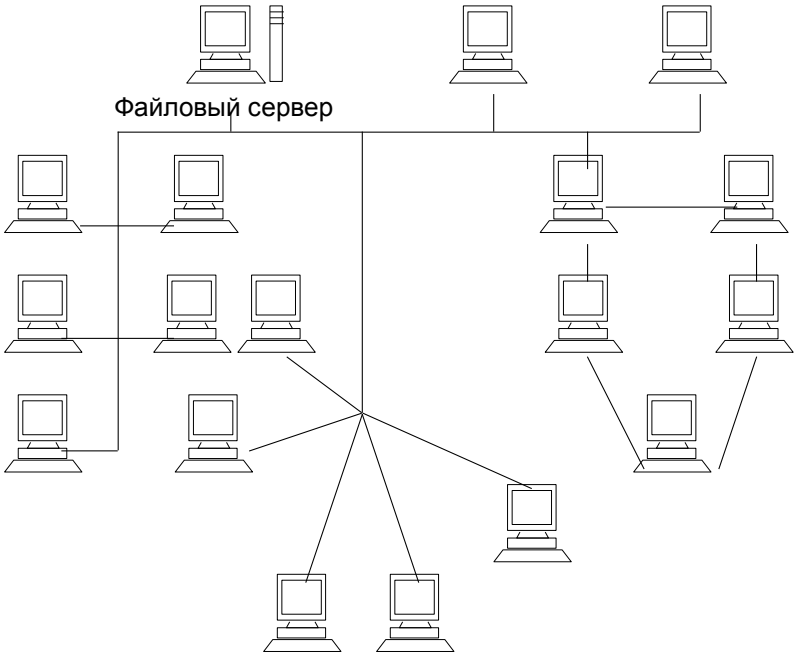


Рисунок 1.21 – Деревовидна структура ЛОМ

Обчислювальні мережі з деревоподібною структурою застосовуються там, де неможливо безпосереднє застосування базових мережних структур в чистому вигляді. Для підключення великої кількості робочих станцій відповідно адаптерним платам застосовують мережні підсилювачі і/або комутатори. Комутатор, що володіє одночасно і функціями підсилювача, називають активним концентратором.

На практиці застосовують дві їх різновиди, що забезпечують підключення відповідно восьми або шістнадцяти ліній.

Пристрій, до якого можна приєднати максимум три станції, називають пасивним концентратором. Пасивний концентратор звичайно використовують як розгалужувач. Він не потребує підсилювачі. Передумовою для підключення пасивного концентратора є те, що можливе максимальна відстань до робочої станції не повинно перевищувати декількох десятків метрів.

1.3. Оброблення мережевих кабелів

1.3.1 Обжимання витої пари

Багато хто вважає, що це найскладніший етап прокладання мережі, оскільки провідників так багато, в них так легко заплутатися, потрібно купувати спеціальний обтискаючий інструмент і т.д. Насправді все досить просто. Для обтискання витої пари вам будуть потрібні спеціальні кліщі та пара коннекторів RJ-45.

Рисунок 1.22 – Коннектори RJ-45

Послідовність дій при обтисканні:

1. Акуратно обріжте кінець кабелю, при цьому найкраще користуватися різаком, який вбудованим в обтискаючий інструмент.

Обтискаючий інструмент RJ-45	Ніж для зачистки ізоляції витої пари

Рисунок 1.23 – Обтискаючий інструмент RJ-45

2. Зніміть з кабелю ізоляцію. Можна використовувати спеціальний ніж для зачистки ізоляції витої пари, його лезо виступає рівно на товщину ізоляції, так ви не пошкодити провідники.

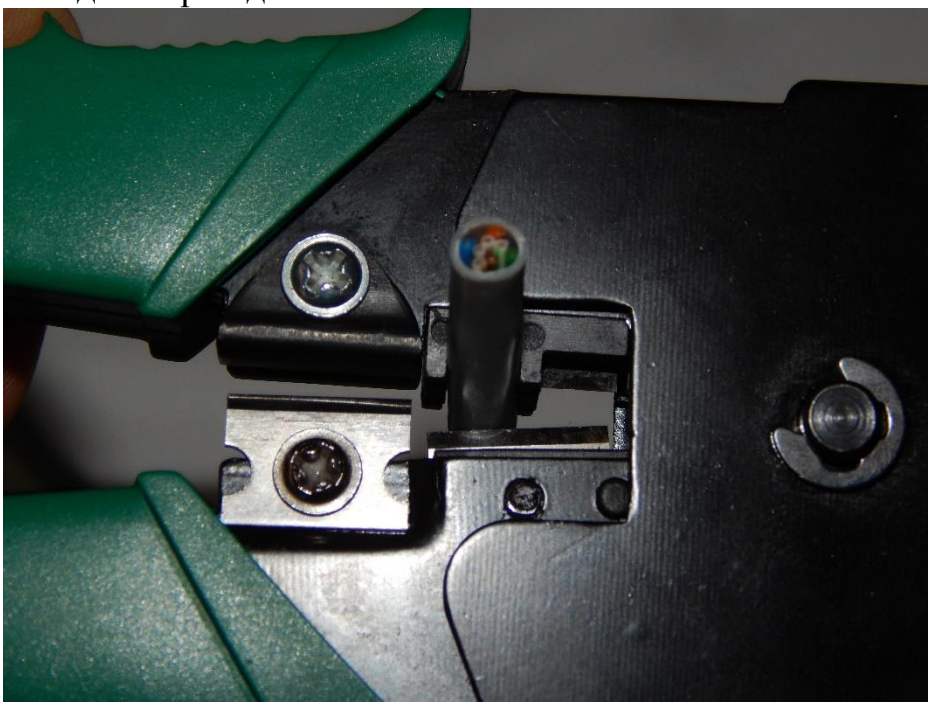


Рисунок 1.24 – Зачистки ізоляції витої пари

Втім, якщо немає спеціального ножа, можна скористатися звичайним або взяти ножиці, або використовувати ножі обтискного інструменту.

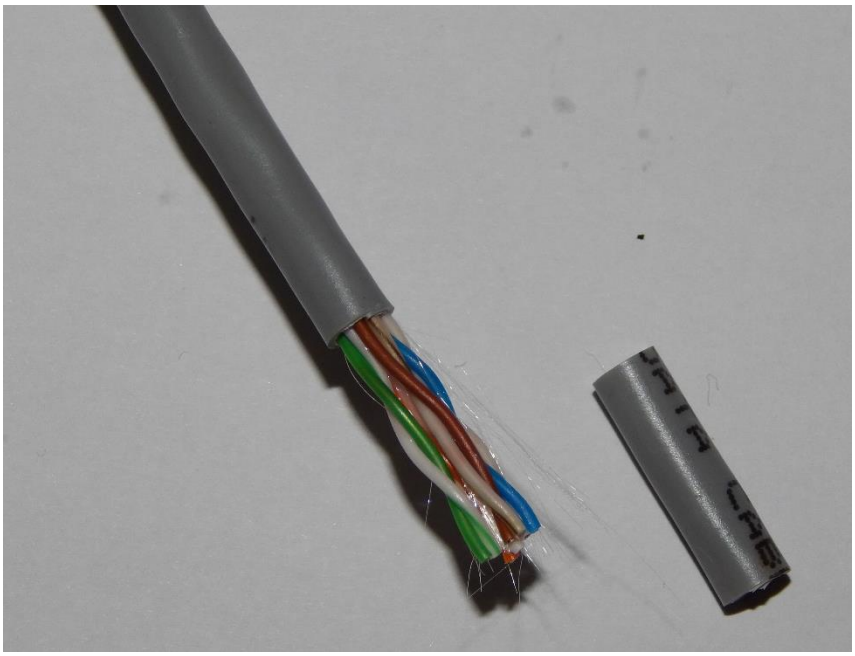


Рисунок 1.25 –Вита пара без ізоляції

3. Розведіть і розплетіть проводки, вирівняйте їх в один ряд, при цьому дотримуючись колірну послідовність

Рисунок 1.26 –Розкладка колірної послідовності

4. Відкусивши проводки так, щоб їх залишилося трохи більше сантиметра

Рисунок 1.27 –Довжина обрізання проводів витої пари

5. Вставляйте провідники в роз'єм RJ-45

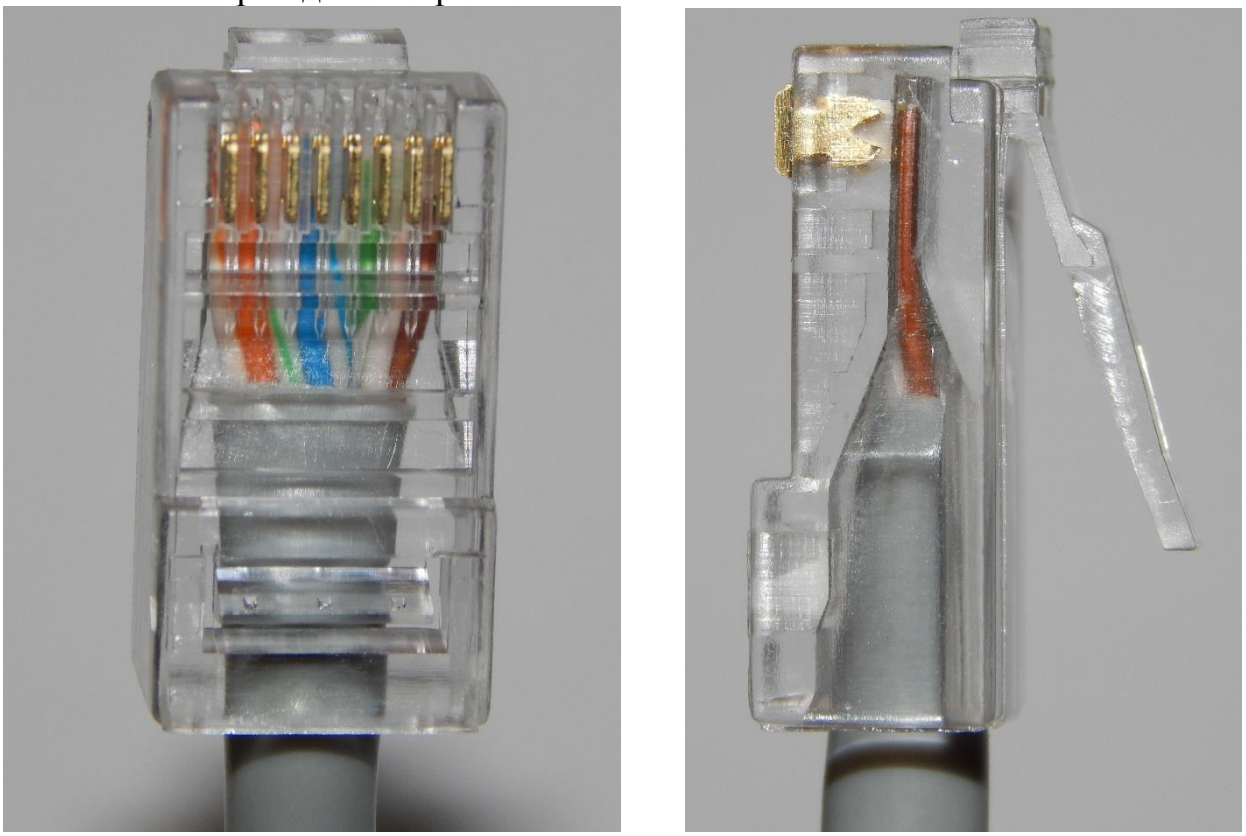


Рисунок 1.28 – Вставлені провідники в роз'єм RJ-45

6. Перевірте, чи правильно ви розташували проводки
7. Переконайтеся чи всі дроти повністю увійшли в роз'єм і вперлися в його передню стінку
8. Помістіть коннектор з встановленою парою в кліщі, потім плавно, але сильно зробіть обтиск

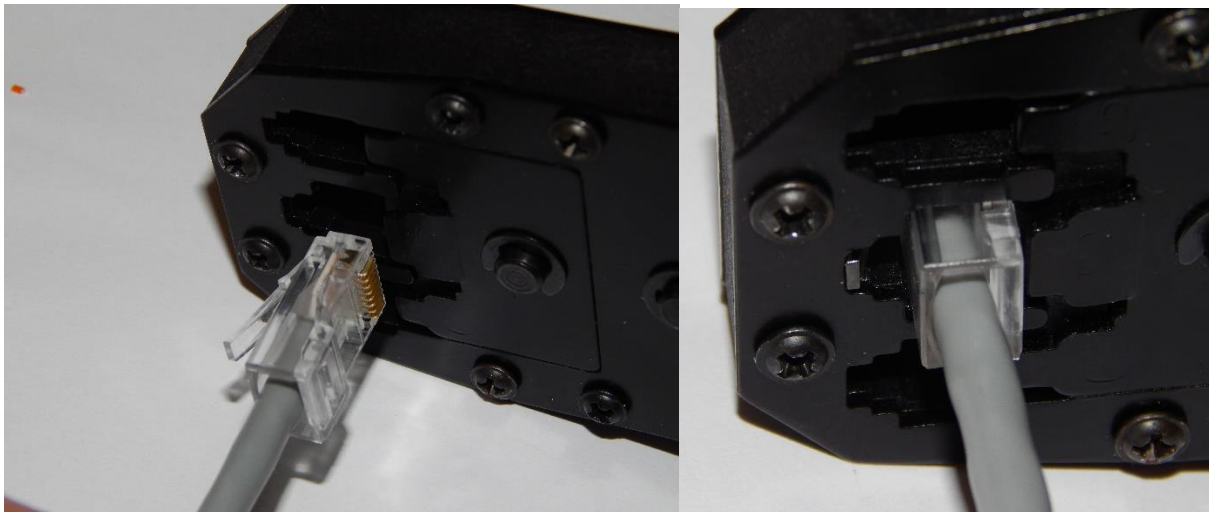


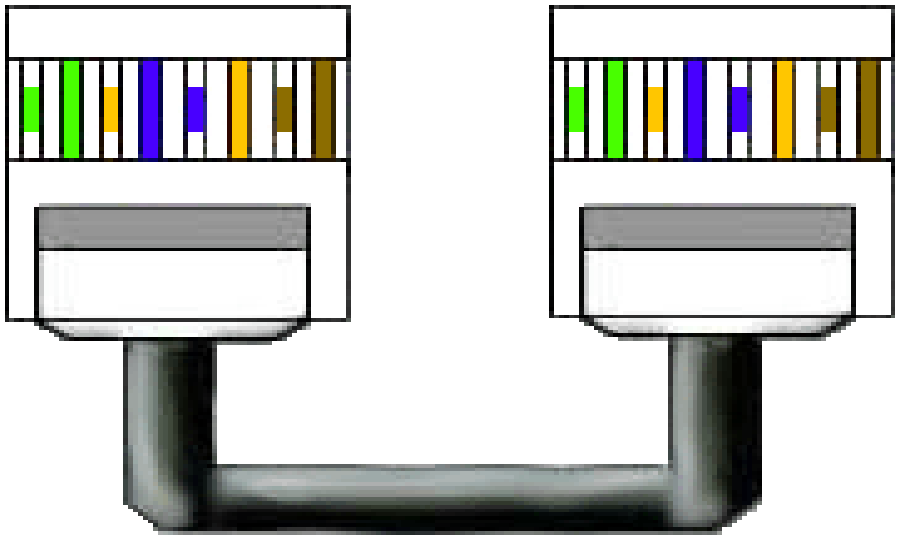
Рисунок 1.29 – Обтискання коннектора з встановленою парою

1.3.2 Колірна послідовність провідників

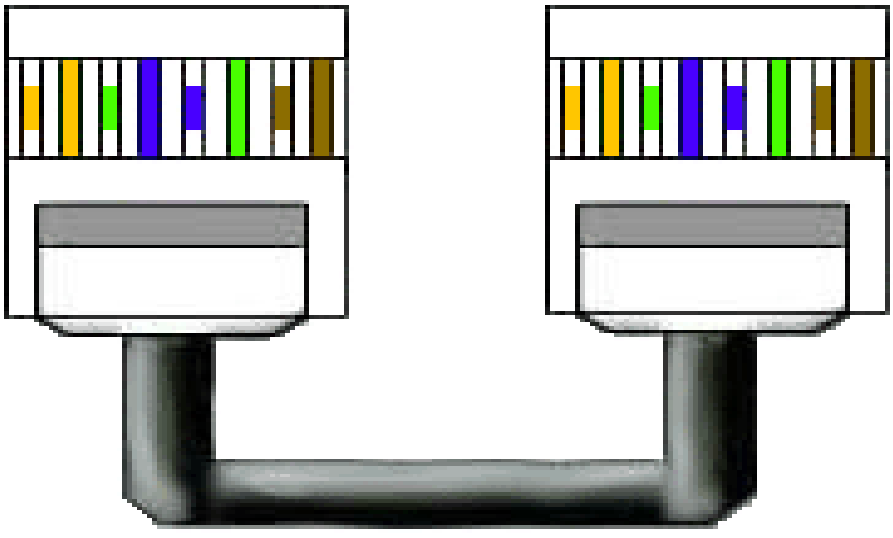
Існує два поширених стандарти з розведення кольорів по парам: T568A компанії Siemon і T568B компанії AT & T. Обидва цих стандарти абсолютно рівнозначні.

Мережева карта <-> Комутатор за стандартом: T568A

При такій розкладці інформацію несуть провідники: Біло-зелений, Зелений, Біло-помаранчевий, Оранжевий.

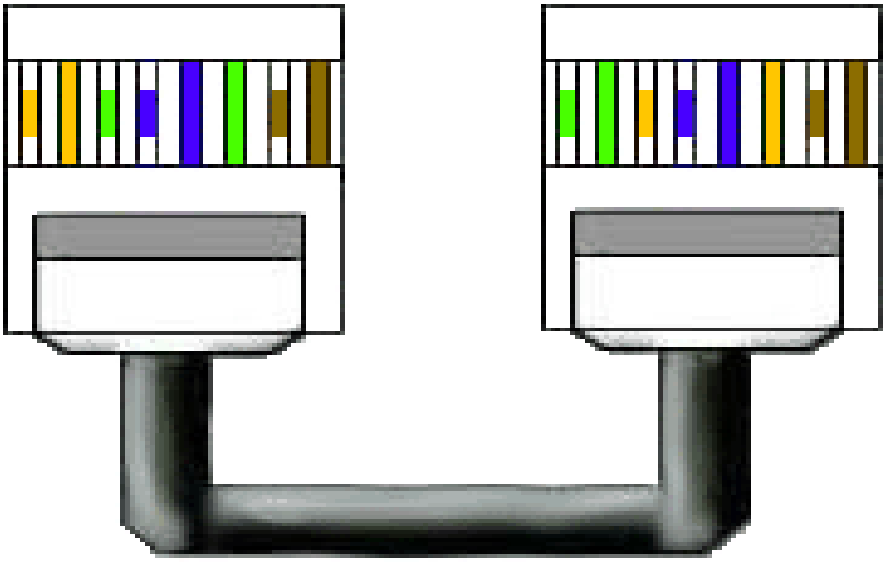


Мережева карта <-> Комутатор за стандартом: T568B



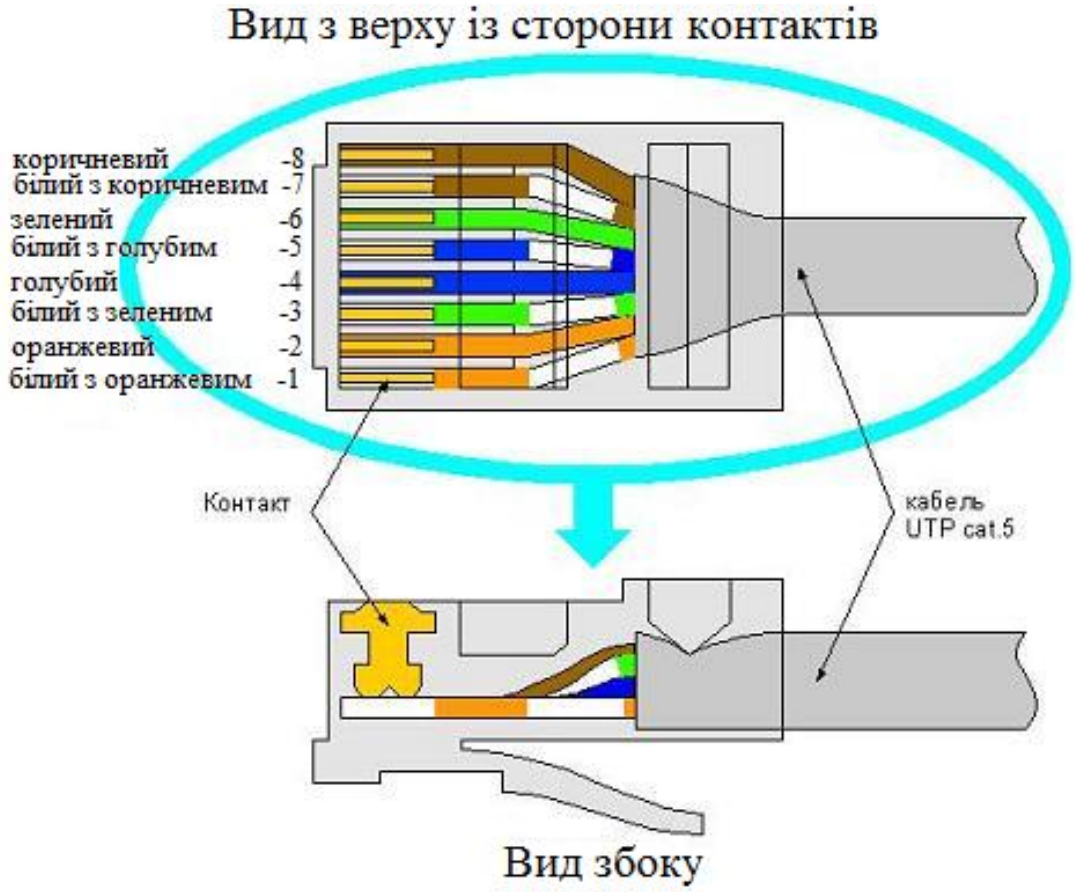
При такій розкладці інформацію несуть провідники: Біло-помаранчевий, Помаранчевий, Біло-зелений, Зелений.

Мережева карта <-> Мережева карта (Кросовер кабель)



Обтиснення таким чином, вита пара може вам знадобитися в 2 випадках:

1. Для з'єднання 2 комп'ютерів без комутатора.
2. Для з'єднання 2 або більше Hub / Switch



Завдання

1. Вивчити за літературними джерелами обладнання ЛОМ.
2. Провести оброблення кабелю RG -58.

3. Провести оброблення кабелю «вита пара».
4. Перевірити працездатність кабелю RG -58 тестером.
5. Перевірити працездатність кабелю вита пара підключенням ПЕОМ до мережі.
6. Описати словесно процес та особливості оброблення кабелів.

Лабораторна робота №2
Діагностичні мережеві утиліти і їх використання

Мета роботи: вивчення методів контролю і моніторингу мереж, які побудовані на базі стеку протоколів TCP/IP за допомогою діагностичних утиліт операційної системи Windows.

ТЕОРЕТИЧНІ ВІДОМОСТІ

2.1 Адресація в IP-мережах

Мережева операційна система WINDOWS містить набір утиліт, корисних при діагностиці мережі, що використовує протоколи TCP / IP.

Основними завданнями цих утиліт є:

- Визначення параметрів і характеристик мережі;
- Визначення працездатності мережі;
- У разі неправильного функціонування мережі - локалізація сегмента або сервісу, що викликають несправність.

Головними параметрами мережевих підключень є їх канальні і мережеві адреси та інші параметри, що впливають на роботу мережевого рівня.

Кожен комп'ютер в мережі Internet (їх прийнято називати **хостами**) має адреси двох рівнів: канального і мережевого.

Канальний адрес хоста визначається технологією, за допомогою якої здійснюється його підключення до Internet. Для машин, що входять в локальні мережі Ethernet, це так званий MAC-адрес (Media Access Control - управління доступом до середовища) мережного адаптера, який призначається виробником обладнання і є унікальним. Для існуючих технологій локальних мереж MAC-адреса має 48-розрядний формат (6 байтів):

- Перший біт вказує: для одиночного (0) або групового (1) адресата призначений кадр;
- Наступний біт вказує, чи є MAC-адрес глобально (0) або локально (1) адмініструючим;
- Наступні 22 біта є ідентифікатором фірми виробника;
- Молодші 3 байти призначаються унікальним чином самим виробником.

MAC-адреси звичайно представляються в 16-розрядної системі, наприклад, 00-E0-4C-78-23-FD. Адреса FF-FF-FF-FF-FF-FF є широкомовною.

В якості мережевого адресу хоста Internet використовується IP-адрес (Internet Protocol Address), який характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання. При зв'язку через мережу Internet потрібно глобальна унікальність адреси, що забезпечується рекомендаціями спеціального підрозділу Internet InterNIC (Network Information Center). Провайдери послуг Internet одержують діапазони адрес у підрозділів InterNIC, а потім розподіляють їх між своїми абонентами. У разі ізольованої від Internet локальної мережі унікальність мережевого адресу необхідна лише в її межах,

при цьому IP-адреси повинні вибиратися адміністратором із спеціально зарезервованих для таких мереж блоків «закритих» адрес.

У найбільш поширеній четвертій версії протоколів Internet (IP.v4) IP-адреса являє собою 32-бітове двійкове число, що записується у вигляді чотирьох десяткових чисел (значення від 0 до 255), розділених крапками (наприклад, 192.168.0.1). Адреса складається з двох логічних частин - номера мережі і номера хоста в мережі.

При класової моделі форматування адрес значення перших бітів адреси визначають, яка його частина відноситься до номера мережі, а яка - до номера хоста, як показано в табл. 2.1.

Таблиця 2.1 – Класова модель форматування адрес

Класс	IP адрес																Діапазон адресів
	31	30	29	28	27	25	24	23	16	15	8	7	0				
A	0	№мережі						№мережі									0.1.0.0–126.0.0.0
B	1	0	№ сети							№ хоста							128.0.0.0–191.255.0.0
C	1	1	0	№мережі								№ хоста					192.0.1.0–223.255.255.0
D	1	1	1	0	адрес групи multicast												224.0.0.0–239.255.255.255
E	1	1	1	1	0	зарезервовано											240.0.0.0–247.255.255.255

Ряд адрес мереж і підмереж є особливими:

- Якщо весь IP-адрес складається тільки з двійкових нулів, то він позначає адресу того хоста, який згенерував цей пакет;
- Якщо всі двійкові розряди IP-адреси хоста рівні 1, то пакет з таким адресом призначення є широкомовним, тобто повинен розсилатися всім хостам, що знаходяться в тій же мережі, що й джерело цього пакета;
- Якщо всі двійкові розряди IP-адреси хоста рівні 0, то ця адреса позначає не окремий адресу, а всю мережу;
- Адреса 127.0.0.1 означає пересилання в межах одного і того ж хоста (використовується для автономної налагодження мережевого ПЗ);
- Адреси закритих мереж (приватна мережа, мережа інтернет) лежать в діапазонах 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255.

З метою більш економного розподілу IP-адрес між користувачами класова модель витісняється безкласовою, при якій виділення розрядів в адресі, що відводяться для нумерації мережі, задається спеціальним чотирьохбайтовим кодом - маскою підмережі. Розряди маски, використовувані для нумерації мереж, мають поодинокі значення. Наприклад, маска 255.255.255.240 (код 11111111.11111111.11111111.11110000 у двійковій системі) вказує, що для нумерації мережі використовується 28 старших розрядів, а для нумерації хоста - тільки 4 молодших розряду відповідного IP-адреси. Часто застосовується запис IP-адрес виду 192.96.10.0/28. Число після косої риски означає кількість одиничних розрядів в масці підмережі.

IP-адреси для конкретних комп'ютерів можуть встановлюватися адміністратором мережі вручну, що дуже важко. Для автоматизації процесу призначення IP-адрес хостам мережі локальної мережі застосовується спеціальний протокол DHCP (Dynamic Host Configuration Protocol), який забезпечує статичне або динамічне призначення IP-адрес. Призначенні адреси формує DHCP-сервер за запитами DHCP-клієнтських програм, що встановлюються на окремих хостах.

При автоматичному статичному способі DHCP-сервер без втручання оператора присвоює IP-адресу та інші параметри конфігурації клієнта з пулу (набору) наявних IP-адрес. Межі пулу призначених адрес задає адміністратор при конфігуруванні DHCP-сервера. Між ідентифікатором клієнта і його IP-адресою і раніше, як і при ручному призначенні, існує постійну відповідність. Воно встановлюється в момент первинного призначення сервером DHCP IP-адреси клієнта. При всіх наступних запитах сервер повертає той же самий IP-адресу.

При динамічному розподілі адрес DHCP-сервер призначає адресу клієнту на обмежений час, що дає можливість згодом повторно використовувати IP-адреси іншими комп'ютерами.

2.2 Відображення символьних адрес на IP-адреси: служба DNS

Комп'ютери використовують для взаємодії числові IP-адреси, тоді як людям зручніше працювати зі словесними іменами. Щоб в мережевих додатках можна було застосовувати словесні імена, необхідний механізм перетворення імен в IP-адреса, який реалізовується службою доменних імен DNS (Domain Name System) розподіленою базою даних, яка підтримує ієрархічну систему імен для ідентифікації хостів в мережі Internet.

Служба DNS призначена для автоматичного пошуку IP-адреси за відомим символьним іменем хоста. DNS-сервери зберігають частину бази даних про відповідність символьних імен і IP-адрес. Ця база даних розподілена по адміністративним доменам мережі Internet. Клієнти сервера DNS знають IP-адресу сервера DNS свого адміністративного домену і за протоколом IP передають запит, в якому повідомляють відоме символьне ім'я і просять повернути відповідний йому IP-адрес.

Якщо дані про запрошену відповідність зберігаються в базі даного DNS-сервера, то він відразу посилає відповідь клієнту, якщо ж ні, то він надсилає запит DNS-серверу іншого домену, який або сам обробляє запит, або передає його іншому DNS-серверу. Усі DNS-сервери з'єднані ієрархічно, відповідно до ієрархії доменів мережі Internet.

База даних DNS має структуру дерева, який називається **доменним простором імен**, в якому кожний домен (вузол дерева) має ім'я і може містити піддомени. Ім'я домену ідентифікує його положення в цій базі даних стосовно батьківського домену, причому крапки в імені відокремлюють частини, які відповідають хостам домену.

Домени верхнього рівня призначаються для кожної країни, а також на організаційній основі. Доменне ім'я будується з слів, розділених крапками і містять латинські букви, цифри та знак «мінус» (-). Доменні імена можуть містити до 63 символів і нечутливі до регістру букв, тобто великі і малі літери вважаються однаковими.

Організація InterNIC, керуюча всім адресним простором Internet, а також усім простором імен, делегує деяким організаціям право ведення доменів першого рівня, до яких відносяться наступні «організаційні» зони (**com** - комерційні, **edu** - освітні, **gov** - урядові, **int** - міжнародні, **mil** - військові, **net** - організації, що забезпечують роботу мережі, **org** - некомерційні організації, **biz** - те ж саме, що і **com**, **info** - інформаційні ресурси), а також більше двохсот «географічних» доменів (**ru** і **su** - Росія, **uk** - Великобританія , **de** - Німеччина, **fr** - Франція, **ua** - Україна і т.д.).

Власник доменної зони може організовувати в ній будь-які піддомени і делегувати функції адміністрування цих піддоменів іншим організаціям. Піддомен створюється шляхом дописування до імені домену ще одного відокремленого точкою слова зліва. Кожен домен має унікальне ім'я, а кожен з піддоменів має унікальне ім'я усередині свого домену. Кожен хост в мережі Internet однозначно визначається своїм повним доменним ім'ям, яке включає імена всіх доменів по напрямку від хоста до кореня. Приклад повного DNS-імені: alice.pnzgu.ru.

2.3 Системні утиліти мережевої діагностики

2.3.1 Утиліта i*pconfig*

Утиліта ***ipconfig*** призначена для перевірки правильності конфігурації TCP/IP для операційної системи Windows. Виводить значення для поточної конфігурації стека TCP/IP: MAC- і IP-адрес, маску підмережі, адрес шлюзу за замовчуванням, адреси серверів WINS (Windows Internet Naming Service) і DNS, використання DHCP.

При усуненні несправностей в мережі TCP/IP слід спочатку перевірити правильність конфігурації за допомогою утиліти ***ipconfig*.**

Синтаксис утиліти: ***ipconfig [/ all] [/ renew [adapter]] [/ release [adapter]]*.** Параметри (тут і далі в квадратних дужках вказані необов'язкові параметри):

- ***all*** видає весь список параметрів, без цього ключа відображається тільки IP-адреса, маска і шлюз за умовчанням;
- ***renew [adapter]*** оновлює параметри конфігурації DHCP для зазначеного мережного адаптера ім'ям ***adapter*;**
- ***release [adapter]*** звільняє виділений DHCP IP-адрес.

Таким чином, утиліта ipconfig (рис. 2.1) дозволяє з'ясувати, чи ініціалізована конфігурація і чи не дублюються IP-адреси:

- якщо конфігурація ініціалізована, то з'являються IP-адреса, маска, шлюз;
- якщо IP-адреси дублюються, то маска мережі буде 0.0.0.0;
- якщо при використанні DHCP комп’ютер не зміг отримати IP-адресу, то він буде дорівнює 0.0.0.0.

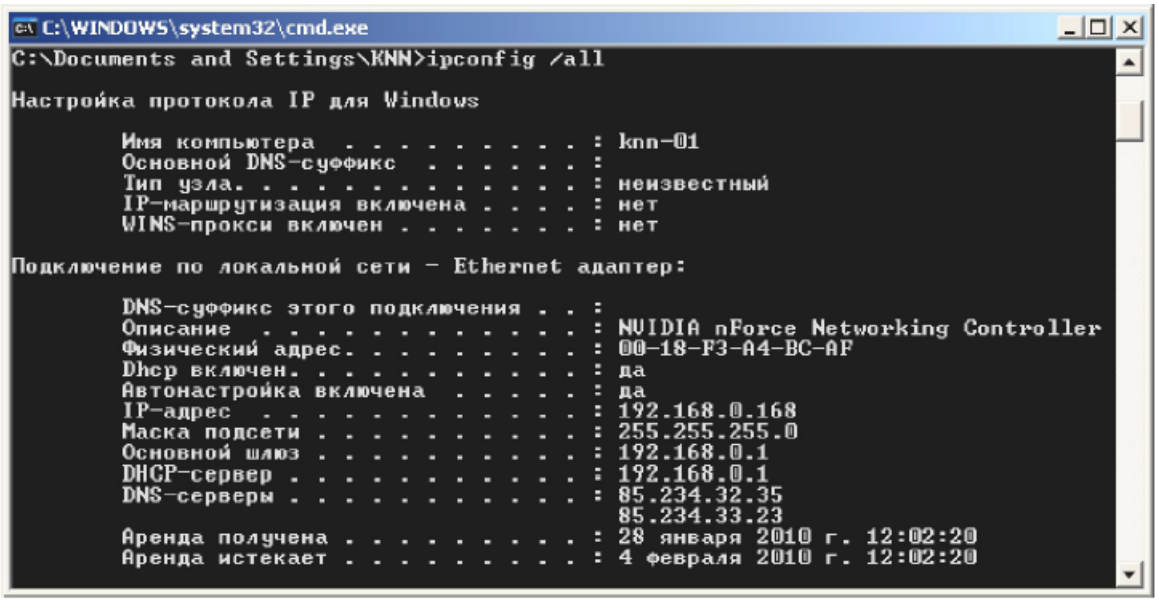


Рисунок 1.1 – Відображення встановлених на комп’ютері мережевих конфігурацій утилітою ***ipconfig***

2.3.2 Утиліта *ping*

Утиліта ***ping*** (*Packet Internet Grouper*) використовується для перевірки конфігурації TCP/IP і діагностики помилок з'єднання. Вона визначає доступність і функціонування конкретного хоста - будь-якого мережевого пристрою, що обмінюється інформацією з іншими мережевими пристроями по TCP/IP. Використання ***ping*** є кращий спосіб перевірки існування маршруту між локальним комп'ютером і мережним хостом.

Команда **ping** перевіряє з'єднання з віддаленим хостом шляхом посилки до нього ехо-пакетів протоколу ICMP (*Internet Control Message Protocol*) і прослуховування ехо-відповідей. ***Ping*** виводить кількість переданих та прийнятих пакетів. Кожен прийнятий пакет перевіряється відповідно з переданим повідомленням. Якщо зв'язок між хостами поганий, з повідомлень ***ping*** стане ясно, скільки пакетів втрачено.

По замовчуванню передаються чотири ехо-пакета довжиною 32 байта, що представляють собою послідовність символів алфавіту в верхньому регістрі. ***Ping*** дозволяє змінити розмір і кількість пакетів, вказати, чи слід записувати маршрут, який вона використовує, яку величину часу життя встановлювати, чи можна фрагментувати пакет і т.д. При отриманні відповіді в полі визначається, за який час (у мілісекундах) посланий пакет доходить до віддаленого хоста і повертається назад. Так як значення за замовчуванням для очікування відгуку дорівнює 1 с, то всі значення даного поля будуть менше 1000 мс. Якщо виходить повідомлення «Перевищено інтервал очікування», то, можливо, збільшення часу очікування відгуку дозволить пакету дійди до віддаленого хоста.

При користуванні утиліти ***ping*** слід пам'ятати:

- затримка, яка визначена утилітою, викликана не тільки пропускною здатністю каналу передачі даних до перевіряючої машини, але і завантаженістю цієї машини;

- деякі сервери в цілях безпеки можуть не посилати ехо-відповіді, оскільки з утиліти ***ping*** може починатися хакерська атака.

Ping можна використовувати для тестування як з доменним ім'ям хоста, так і з його IP-адресом. Якщо ***ping*** з IP-адресом виконалася успішно, а з ім'ям - невдало, це означає, що проблема полягає в розпізнаванні відповідності адреси та імені, а не в мережевому з'єднанні.

Синтаксис: ***ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host -list | [-k host-list]] [-w timeout] destinationlist***. Параметри:

- ***-t*** виконує команду ***ping*** до переривання (**Ctrl-Break** - подивитися статистику і продовжити, **Ctrl-C** - перервати виконання команди);
- ***-a*** дозволяє визначити доменне ім'я віддаленого комп'ютера за його IP-адресом;
- ***-n count*** посилає кількість пакетів *Echo*, вказане параметром ***count*** (за замовчуванням передається чотири запиту);
- ***-l length*** посилає пакети довжиною ***length*** байт (максимальна довжина 8192 байти);
- ***-f*** посилає пакет з встановленим прапором «Не фрагментувати», заборонним фрагментованість пакету на транзитних маршрутизаторах;
- ***-i ttl*** встановлює час життя пакету в величину ***ttl*** (кожен маршрутизатор зменшує ***ttl*** на одиницю, тобто час життя є лічильником пройдених маршрутизаторів (хопів));
- ***-v tos*** встановлює значення поля «сервіс», що задає пріоритет обробки пакета;
- ***-r count*** записує шлях вихідного пакету та повертаючого пакета в полі запису шляху, ***count*** - від 1 до 9 хостів;
- ***-s count*** задає максимально можливу кількість переходів з однієї підмережі в іншу (хопів);
- ***-j host-list*** направляє пакети за допомогою списку хостів, визначеного параметром ***host-list***.), максимальна кількість хостів дорівнює 9;
- ***-k host-list*** направляє пакети через список хостів, визначений у ***host-list,*** причому зазначені хости не можуть бути розділені проміжними маршрутизаторами (жорстка статична маршрутизація);
- ***-w timeout*** вказує час очікування ***timeout*** відповіді від віддаленого хоста в мілісекундах (за замовчуванням - 1с);
- ***-destination-list*** вказує віддалений вузол, до якого необхідно направити пакети ***ping***, може бути ім'ям хоста або IP-адресою машини.

На практиці у форматі команди найчастіше використовуються опції ***-t*** і ***-n***.

Приклад роботи утиліти ***ping*** зображено на рисунку 2.2.

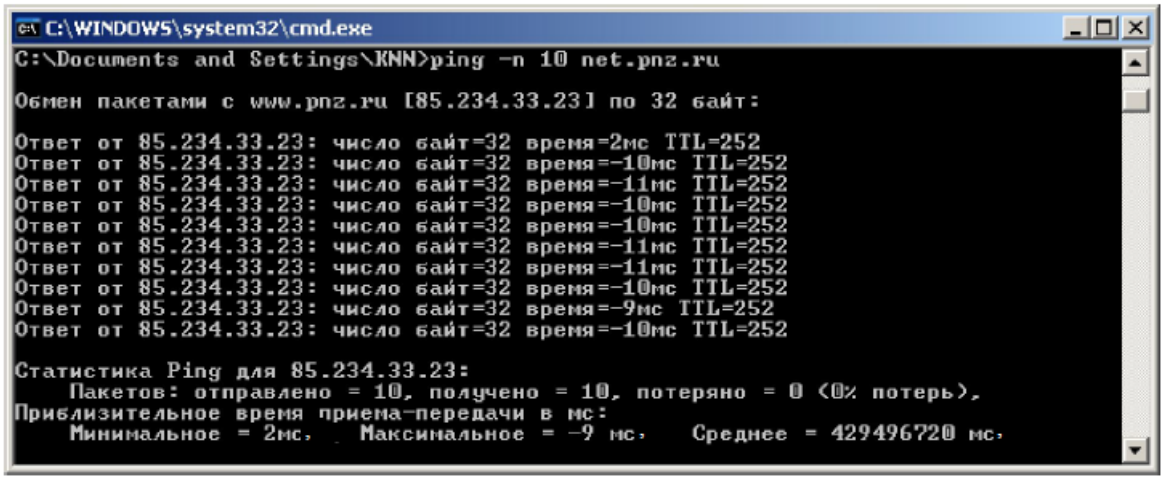


Рисунок 2.2 – приклад використання утиліти ***ping***

Утиліта ***ping*** може використовуватися такими способами:

1. Для перевірки того, що TCP/IP встановлений і правильно налаштований на локальному комп'ютері, в команді ***ping*** задається адрес петлі зворотного зв'язку: ***ping 127.0.0.1***.

Якщо тест успішно пройдено, то ви отримаєте таку відповідь:

Відповідь від 127.0.0.1: число байт = 32 час <1мс TTL = 128
Відповідь від 127.0.0.1: число байт = 32 час <1мс TTL = 128
Відповідь від 127.0.0.1: число байт = 32 час <1мс TTL = 128
Відповідь від 127.0.0.1: число байт = 32 час <1мс TTL = 128

2. Щоб переконатися в тому, що комп'ютер правильно доданий в мережу і IP-адреса не дублюється, використовується IP-адреса локального комп'ютера: ***ping IP-адрес_локального_хоста***.

3. Щоб перевірити, що шлюз за замовчуванням функціонує і можна встановити з'єднання з будь-яким хостом в локальній мережі, задається IP-адреса шлюзу за замовчуванням: ***ping IP-адрес_шлюза***.

4. Для перевірки можливості встановлення з'єднання через маршрутизатор в команді ***ping*** задається IP-адреса віддаленого хоста: ***ping IP-адрес_віддаленного хоста***.

2.3.3 Утиліта *tracert*

Утиліта ***tracert*** (*trace route*) дозволяє виявляти послідовність маршрутизаторів, через які проходить IP-пакет на шляху до пункту свого призначення шляхом вивчення повідомлень ICMP, які надсилаються назад проміжними маршрутизаторами.

Утиліта ***tracert*** працює таким чином: відсилаю по три пробних ехо-пакети протоколу ICMP з TTL = 1 на вузол призначення, перший маршрутизатор пошле в комп'ютер-джерело повідомлення ICMP «Час вийшов». Потім TTL збільшується на 1 у кожній наступній посилці доти, поки пакет не досягне хоста призначення або не буде досягнута максимально можлива величина TTL (за замовчуванням 30).

Ім'я машини може бути ім'ям хоста або IP-адресом машини. Вихідна інформація являє собою список хостів, починаючи з першого шлюзу і закінчуючи пунктом призначення. На екран при цьому виводиться час очікування відповіді на кожен пакет.

У тих випадках, коли видалений вузол не можна досягти, застосування утиліти **tracert** більш зручно, ніж ***ping***, оскільки з її допомогою можна локалізувати район мережі, в якій є проблеми зі зв'язком.

Якщо виникли проблеми, то утиліта виводить на екран зірочки (*) або повідомлення типу «Задана мережа недоступна», «Час вийшов».

Слід пам'ятати, що деякі маршрутизатори просто знищують пакети з вичерпаним TTL і не будуть видні утиліті ***tracert.***

Синтаксис утиліти: ***tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] destination-list***. Параметри:

- ***-d*** вказує, що не потрібно розпізнавати адреси для імен хостів;
- ***-h maximum_*hops** вказує на максимальну кількість хопів (за замовчуванням - 30);
- ***-j host-list*** вказує нежорстку статичну маршрутизацію відповідно до ***host-list***;
- ***-w timeout*** вказує, що потрібно очікувати відповідь на кожен ехо-пакет задане число мс;
- ***-destination-list*** вказує віддалений вузол, до якого треба направити пакети ***ping***.

Приклад роботи утиліти ***tracert*** наведено на рис. 2.3.

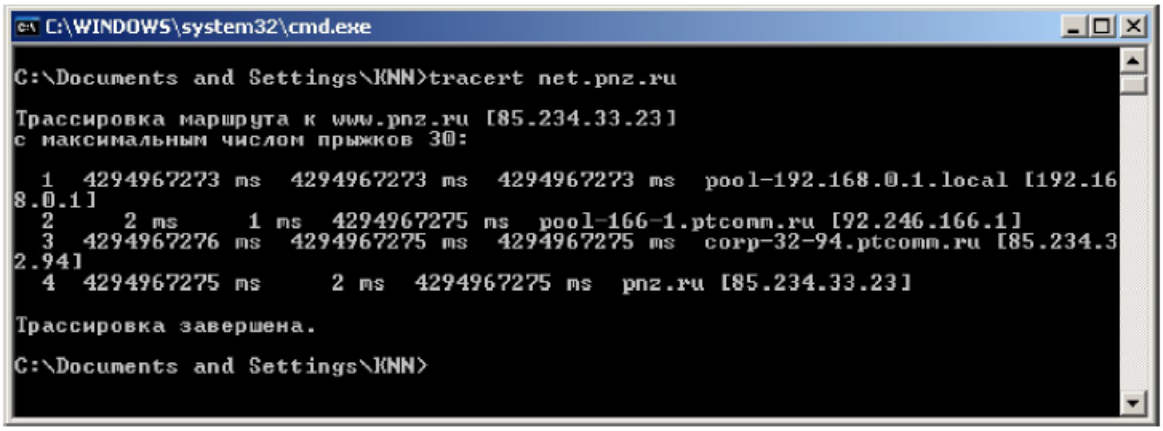


Рисунок 2.3 – Приклад використання утиліти **tracert**

2.3.4 Утиліта *arp*

Утиліта a***rp*** (*Address Resolution Protocol* - протокол дозволу адрес) дозволяє керувати так званим ARP-кешем - таблицею, яка використовується для трансляції IP-адрес у відповідні локальні адреси. Записи в ARP-кеші формує протокол ARP. Якщо необхідний запис в таблиці не знайдено, то протокол ARP відправляє широкомовний запит до всіх комп'ютерів локальної підмережі, намагаючись знайти власника даного IP-адреси.

У кеші можуть міститися два типи записів: статичні і динамічні. Статичні записи вводяться вручну і зберігаються в кеші постійно. Динамічні записи поміщаються в кеш в результаті виконання широкомовних запитів. Для них існує поняття часу життя. Якщо протягом певного часу (за замовчуванням 2 хв) запис не був потрібен, то він видаляється з ARP-кешу.

Синтаксис утиліти: ***arp [-s inet_addr eth_addr] [-d inet_addr] [-a]***. Параметри:

- ***-s inet_addr eth_addr*** заносить в кеш статичний запис із зазначеними IP-адресом і MAC-адресою;
- ***-d inet_addr*** видаляє з кешу запис для певного IP-адреси;
- ***-a*** переглядає вміст кеша для всіх мережевих адаптерів локального комп'ютера, як зображено на рис. 2.4.
-

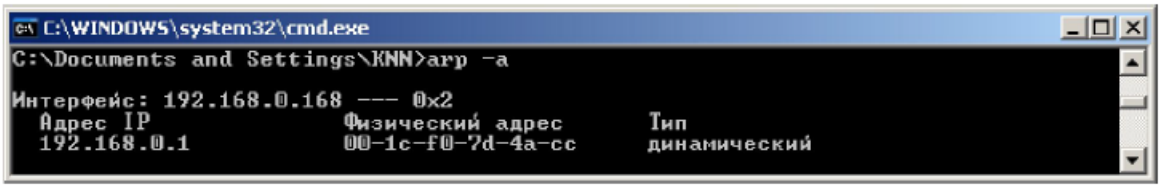


Рисунок 2.4 – Приклад використання утиліти *arp*

2.3.5 Утиліта *netstat*

Утиліта ***netstat*** виводить статистику протоколів і поточних TCP / IP з'єднань і має наступний синтаксис: ***netstat [-a] [-e] [-n] [-S] [-p name] [-r] [interval]***. Параметри:

- ***-a*** відображає повну інформацію по всіх з'єднаннях і портам, на яких комп'ютер чекає з'єднання;
- ***-e*** відображає статистику Ethernet (цей ключ може застосовуватися разом з ключем ***- s***);
- ***-n*** відображає адреси і номери портів в числовому форматі, без їх перетворення в символьні імена DNS і в назву мережевих служб, що робиться за замовчуванням ***t***;
- ***-p name*** задає відображення інформації для протоколу ***name*** (допустимі значення ***name***: ***tcp***, ***udp*** або ***ip***) і використовується разом з ключем ***s***;
- ***-r*** відображає вміст таблиці маршрутів (таблиця маршрутизації);
- ***-s*** відображає докладну статистику по протоколах. По замовченню виводяться дані для TCP, UDP і IP. Ключ ***p*** дозволяє задати вивід даних по певному протоколу, ключ ***interval*** ініціює повторний висновок статистичних даних через вказаний в секундах інтервал (у цьому випадку для припинення виведення даних треба натиснути клавіші ***Ctrl + C***).

Результатом виконання команди є список активних підключень, в який входять встановлені з'єднання і відкриті порти (рис. 2.5).

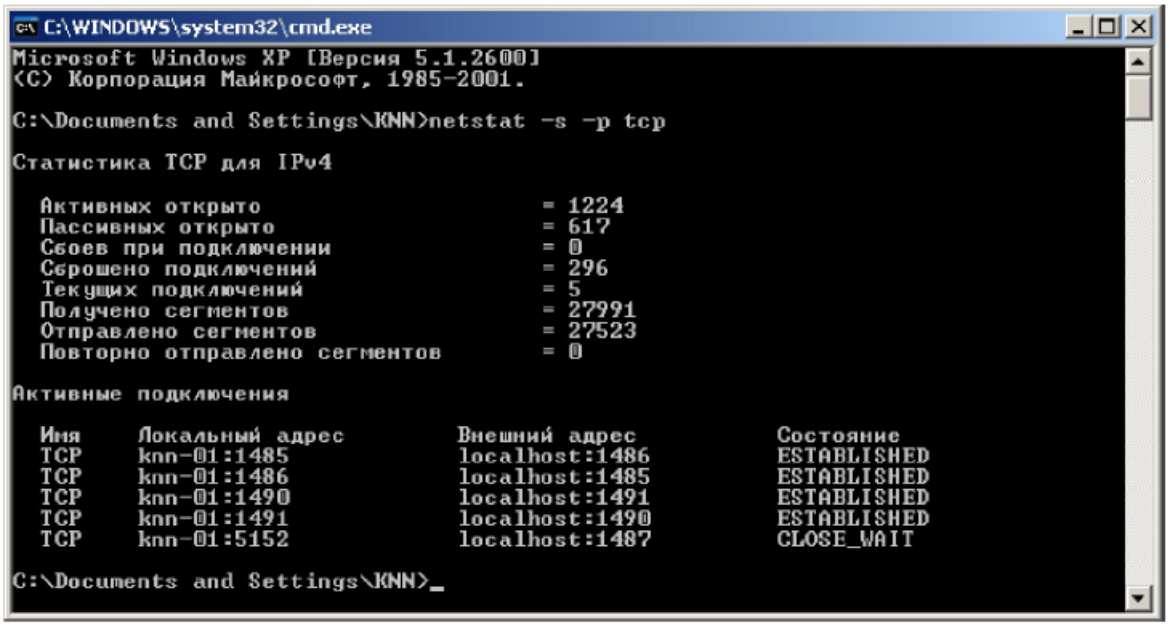


Рисунок 2.5 – Приклад відображення утилітою ***netstat*** встановлених на комп'ютері TCP-з'єднань

Відкриті TCP-порти позначаються у колонці «Стан» рядком **LISTENING** - пасивно відкриті з'єднання («слухові» сокети) або **ESTABLISHED** - встановлені з'єднання, тобто вже використовувані мережевими сервісами.

Частина портів пов'язана з системними службами Windows і відображається не за номером, а за назвою - ***epmap***, ***microsoft-ds***, ***netbios-ss*** та ін Порти, що не відносяться до стандартних службам, відображаються за номерами. UDP-порти не можуть перебувати в різних станах, тому спеціальна позначка **LISTENING** в їх відношенні не використовується. Як і TCP-порти, вони можуть відображатися за іменами чи за номерами.

2.3.6 Утиліта *nslookup*

Утиліта ***nslookup*** призначена для виконання запитів до DNS-серверів на дозвіл імен в IP-адреси та в простому випадку має наступний синтаксис: ***nslookup [host [server]]***. параметри:

- ***host*** - доменне ім'я хоста, яке має бути перетворено в IP-адресу;
- ***server*** - адреса DNS-сервера, який буде використовуватися для дозволу імені. Якщо цей параметр опущений, то будуть використані адреси DNS-серверів з параметрів настройки протоколу TCP/IP (відображаються утилітою ***ipconfig***).

Результати виконання команди ***nslookup*** зображено на рис. 2.6.

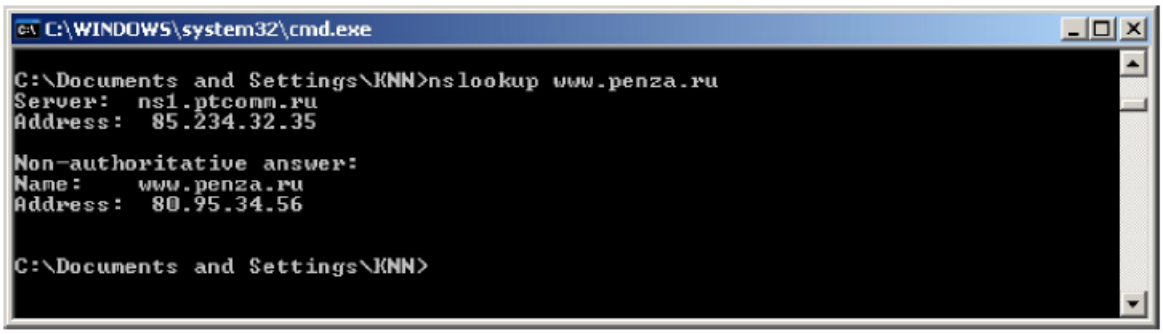


Рисунок 2.6 – Приклад відображення утилітою ***nslookup***

Перші два рядки відповіді містять ім'я і IP-адрес DNS-сервера, який був використаний для дозволу імені. Наступні рядки містять реальне доменне ім'я хоста і його IP-адресу та вказівку ***Nonauthoritative answer***, що означає, що відповідь отримана не з DNS-сервера, відповідального за зону ***penza.ru***. Також може бути присутнім рядок ***Aliase***, який містить альтернативні імена шуканого сервера.

2.3.7 Сервіс *Whois*

При трасуванні маршрутів або перевірці доступності хоста в Internet часто виникає необхідність визначити за IP-адресом хоста його юридичного власника і контактні дані його адміністратора.

У відношенні доменів другого рівня ця інформація стає вільно доступною для будь-якого користувача мережі Internet через сервіс ***Whois***. On-line сервісу ***Whois*** можна отримати через форму на сторінці сайту http://www.nic.ru/whois.

2.4 Завдання на лабораторну роботу

2.4.1. За допомогою утиліти ***ipconfig***, запущеної з командного рядка, визначити ім'я, IP-адресу та фізичну адресу основного мережевого інтерфейсу комп'ютера, IP-адреса шлюзу, IP-адреси DNS-серверів і використання DHCP. Результати представити у вигляді таблиці.

2.3.2. За допомогою утиліти ***nslookup*** визначити IP-адресу одного з віддалених серверів, доменні імена яких вказані в табл. 2.2.

Таблиця 2.2 – Домени імен віддалених серверів

№ варіанту	Адрес	№ варіанту	Адрес
1	tntu.edu.ua	11	ternopol.ter.slando.ua
2	net.pnz.ru	12	mypenza.ru
3	mon.gov.ua	13	www.kyivstar.ua
4	penza.vt.ru	14	google.com.ua
5	fcnyva.te.ua	15	www.penza-gsm.ru
6	www.penza.ru	16	www.rozum.org.ua
7	www.facebook.com	17	svidok.com
8	www.ukr.net	18	forum.te.ua/

9	penza.citydom.ru	19	20minut.ua
10	www.gismeteo.ua	20	ex.ua

2.3.3. За допомогою утиліти ***ping*** перевірити стан зв'язку с будь-якими комп'ютером і шлюзом локальної мережі, а також з одним з віддалених серверів, доменні імена яких вказані в табл. 2.2.

Число відправляючих запитів має становити не менше 10. Для кожного з досліджуваних хостів відобразити у вигляді таблиці IP-адреса хоста призначення, середній час прийому-передачі, відсоток втрачених пакетів.

2.3.4. За допомогою утиліти ***arp*** перевірити стан ARP-кешу. Провести пінгування якого-небудь хоста локальної мережі, адресу якого не було відображено в кеші. Повторно відкрити ARP-кеш і проконтролювати модифікацію його вмісту. Уявити отримані значення ARP-кешу у звіті.

2.3.5. Провести трасування одного з віддалених хостів у відповідності з варіантом, обраним у п. 2.3.2. Якщо є втрати пакетів, то для відповідних хостів середній час проходження необхідно визначати за допомогою утиліти ***ping*** по 10 пакетам. У звіті привести копію вікна з результатами роботи утиліти ***tracert***.

Визначити ділянку мережі між двома сусідніми маршрутизаторами, який характеризується найбільшою затримкою при пересиланні пакетів. Для знайдених маршрутизаторів за допомогою сервісу ***Whois*** визначити назву організацій та контактні дані адміністратора (тел., e-mail). Отриману інформацію привести в звіті.

2.3.6. За допомогою утиліти ***netstat*** подивитися активні поточні мережеві з'єднання та їх стан на вашому комп'ютері, для чого:

- запустити кілька екземплярів веб-браузера, завантаживши в них різні сторінки з різних веб-сайтів (за вказівкою викладача);
- закрити браузери і за допомогою ***netstat*** перевірити зміне списку мережевих підключень.

Проконтролювати мережеві з'єднання в реальному масштабі часу, для чого:

- закрити раніше відкриті мережеві додатки;
- запустити з командного рядка утиліту ***netstat***, задавши числовий формат відображення адрес і номерів портів і повторний вивід з періодом 20-30 с;
- в окремому вікні командного рядка запустити утиліту ***ping*** в режимі «до переривання»;
- спостерігати відображення ***netstat***, поточної статистики мережевих додатків;
- за допомогою клавіш ***Ctrl + C*** послідовно закрити утиліти ***ping*** і ***netstat***.

У звіті привести копії вікон з результатами роботи утиліти ***netstat*** з поясненням що відображається.

Зміст звіту

Звіт повинен містити наступні розділи:

1. Назва, мету роботи

2. Опис виконаних лабораторних завдань, з висновками до кожного завдання

Лабораторна робота №3
Вивчення конфігурації мереж ETHERNET

Мета роботи: вивчення конфігурації мереж ETHERNET

ТЕОРЕТИЧНІ ВІДОМОСТІ

Найбільшого поширення серед локальних обчислювальних мереж отримала мережа Ethernet (стандарт IEEE 802.3). Стандарт визначає множинний доступ до моноканалу типу "шина" з виявленням конфліктів і контролем передачі (по-англійськи CSMA / CD - Carrier - Sense Multiple Access / CollisionDetection - метод доступу з контролем несучої і виявленням колізій (зіткнень)). Основні характеристики стандарту IEEE 802.3 наступні: топологія - "шина", швидкість передачі - 10 Мбіт/с, метод доступу - CSMA / CD, передача вузькосмугова (моноканал). Передача йде пакетами змінної довжини. Передбачена індивідуальна, групова і широкомовна адресація.

Крім стандартної топології типу "шина" застосовуються також топології типу "пасивна зірка" і "дерево". При цьому передбачається використання репітерів (повторювачів) і пасивних (репітерних) концентраторів, що з'єднують між собою різні частини (сегменти) мережі (рис. 3.1).

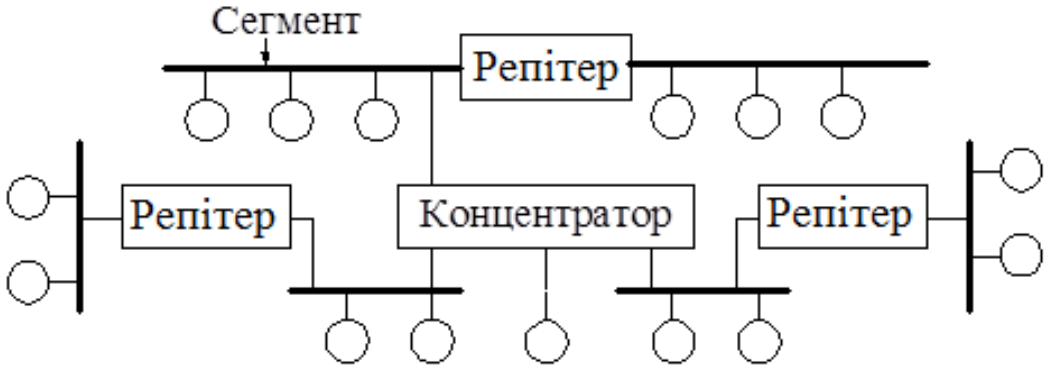


Рисунок 3.1 –Приклад використання репітерів і концентраторів

В якості сегмента може виступати одиничний абонент. Головне - щоб у отриманої в результаті топології не було замкнутих шляхів (петель). Фактично виходить, що абоненти з'єднані все в ту ж "шину", так як сигнал від кожного з них поширюється відразу в усі сторони і не повертається назад.

Для мережі Ethernet стандарт визначає чотири основних типи середовища передачі:

- 10 BASE 5 ("товстий" коаксіальний кабель);
- 10 BASE 2 ("тонкий" коаксіальний кабель);
- 10 BASE - T (вита пара);
- 10 BASE - F (оптоволоконний кабель).

Позначення середовища передачі включає в себе три елементи: цифра "10" означає швидкість передачі 10 Мбіт/с, слово BASE означає передачу в основній смузі частот (тобто без модуляції високочастотного сигналу), а

останній елемент означає допустиму довжину сегмента: "5 "- 500 метрів," 2 "- 200 метрів (точніше, 185 метрів) або тип лінії зв'язку:" T "- вита пара (від англійського" twisted - pair "," F "- оптоволокно (від англійського" Fiber Optic").

2.2. Апаратура 10 BASE 5 ("товстий" кабель)

Апаратні засоби 10 BASE 5 зображено на рис. 3.2, а схема під'єднання адаптера до "товстого" кабелю - на рис. 3.3.

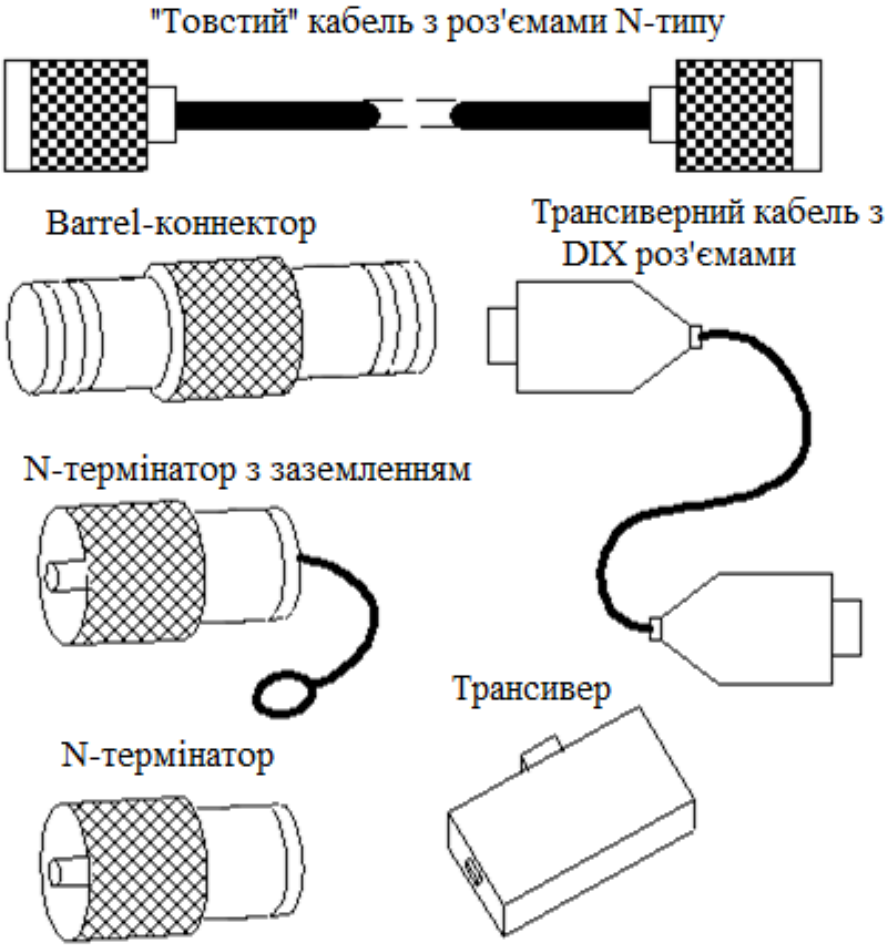


Рисунок 3.2 – Апаратні засоби 10 BASE 5

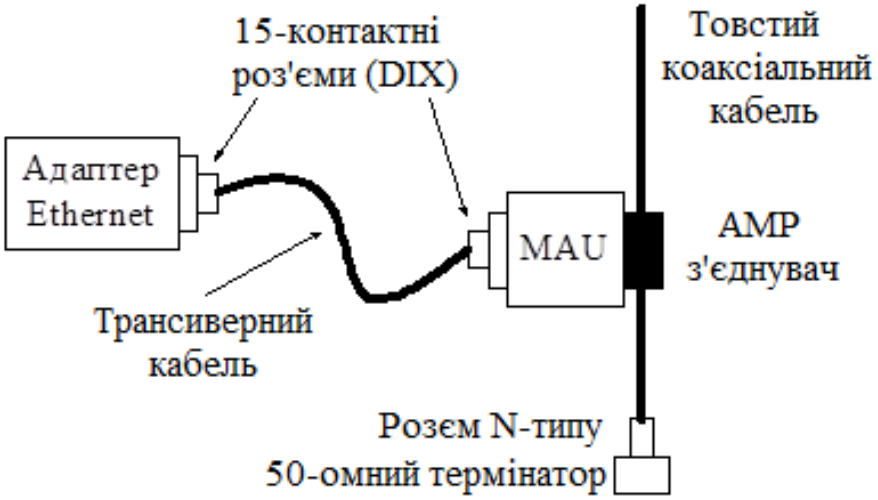


Рисунок 3.3 – Схема під'єднання адаптера до "товстого" кабелю

"Товстий" коаксіальний кабель має діаметр 0,5 дюйма (близько 1 см) і відрізняється високою жорсткістю, що призводить до великих труднощів монтажу апаратури. Хвильовий опір "товстого" коаксіального кабелю – 50 Ом. Максимальна довжина сегмента - 500 метрів (без репітерів). Широко поширені "товсті" кабелі типу RG -8 і RG -11.

Для з'єднання кусків "товстого" коаксіального кабелю і приєднання до нього термінаторів використовуються роз'єми N-типу. Два роз'єми N-типу з'єднуються за допомогою Barrel-коннекторів.

На кінцях кабелю сегмента повинні бути встановлені 50-омні термінатори N-типу, один з яких треба заземлити.

Для приєднання трансиверів до "товстого" кабелю найчастіше використовують AMP з'єднувач.

Безпосередньо на кабелі розміщується спеціальний трансивер (або MAU - Medium AttachmentUnit), що приєднується до мережного адаптера за допомогою гнучкого багатопровідного трансиверного кабелю AUI (діаметром близько 1 см), що складається з 4 витих пар, що має на кінцях 15-контактні роз'єми (DIX-роз'єми типу "вилка"). Довжина звичайного трансиверного кабелю може досягати 50 м, а більш тонкого і гнучкого офісного варіанту трансиверного кабелю - до 12,5 м. Трансивер живиться від джерела живлення комп'ютера.

Трансивер (tr ansmitter + receiver = transceiver - приймач) - це частина мережного адаптера, що виконує наступні функції:

- прийом і передачу даних з кабелю на кабель;
- визначення колізій на кабелі;
- електрична розв'язка між кабелем і іншою частиною адаптера;
- захист кабелю від некоректної роботи адаптера.

Допускається підключення до одного сегмента не більше 100 трансиверів, причому відстань між підключеннями трансиверів не повинна бути менше 2,5 м.

Схему з'єднання комп'ютерів сегмента мережі на "товстому" кабелі зображено на рис. 3.3.

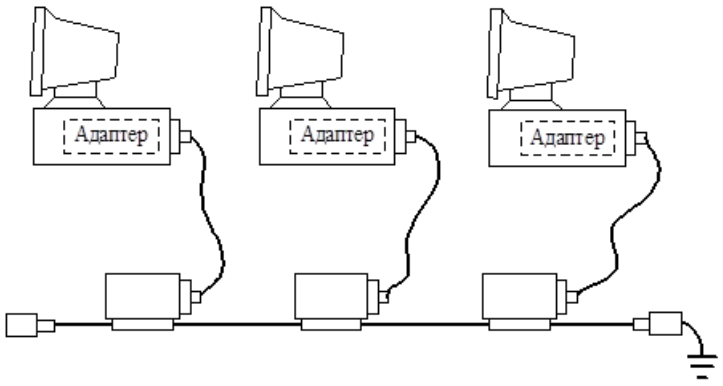


Рисунок 3.3 – Схема з'єднання комп'ютерів сегмента мережі на "товстому" кабелі

Мережевий адаптер, що працює з "товстим" кабелем, повинен мати зовнішній 15-контактний AUI-роз'єм (роз'єм DIX типу "розетка").

Стандарт дозволяє використання в мережі не більше 4 репітерів (репітерних концентраторів) і, відповідно, не більше 5 сегментів кабелю. Це дає максимальну довжину мережі 10 BASE 5 рівну 2500 метрів. Тільки 3 сегменти з 5 можуть бути навантаженими, тобто такими, до яких підключаються комп'ютери. Між навантаженими сегментами повинні бути ненавантажені сегменти, так що максимальна конфігурація мережі являє собою два навантажених крайніх сегмента, які з'єднуються ненавантаженими сегментами ще з одним центральним навантаженим сегментом.

Правило застосування репітерів (репітерних концентраторів) у мережі Ethernet 10 BASE 5 носить назву "правило 5-4-3": 5 сегментів, 4 репітера (репітерних концентратора), 3 навантажених сегмента.

Кожен репітер (репітерний концентратор) підключається до сегмента одним своїм трансивером, тому до навантажених сегментів можна підключити не більше 99 комп'ютерів. Максимальна кількість комп'ютерів в мережі 10 BASE 5 становить 99.3 = 297 комп'ютерів.

Мінімальний набір обладнання для односегментної мережі на "товстому" кабелі включає в себе наступні елементи:

- мережеві адаптери (за кількістю поєднуваних комп'ютерів);
- "Товстий" кабель з роз'ємами N-типу на кінцях, загальна довжина якого достатня для об'єднання всіх комп'ютерів мережі;
- трансиверні кабелі з 15-контактними роз'ємами на кінцях довжиною від комп'ютера до "товстого" кабелю (за кількістю мережевих адаптерів);
- трансивери (за кількістю мережевих адаптерів);
- два Barrel-коннектора N-типу для приєднання термінаторів на кінцях кабелю;
- один N-термінатор без заземлення;
- один N-термінатор із заземленням.

3.3. Апаратура 10BASE2 (“тонкий” кабель)

"Тонкий" коаксіальний кабель відрізняється від "товстого" меншою товщиною - діаметр близько 0,5 дюйма (5 мм), більшою гнучкістю, великою зручністю монтажу, меншою вартістю. "Тонкий" кабель має хвильовий опір 50 Ом і вимагає 50-омного кінцевого узгодження. Максимальна довжина сегмента - 185 метрів (без репітерів).

Найбільшим недоліком "тонкого" кабелю є менша допустима довжина сегмента (до 185 м). Найбільш поширені типи "тонкого" коаксіального кабелю - це RG -58 / U, RG -58 A / U, RG -58 C / U.

Апаратні засоби 10 BASE 2 зображено на рис. 3.4, а схема під'єднання адаптера по "тонкому" кабелю - на рис. 3.5.

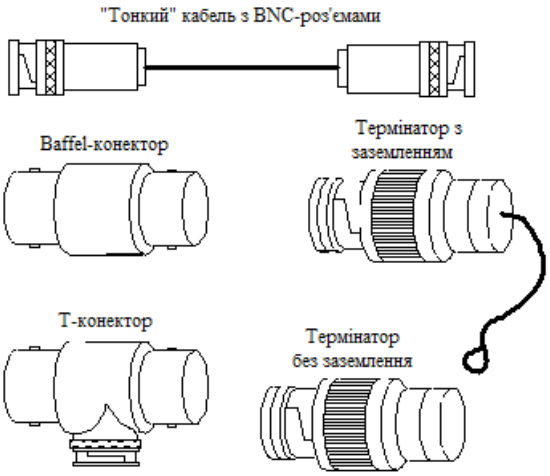


Рисунок 3.4 – Апаратні засоби 10 BASE 2

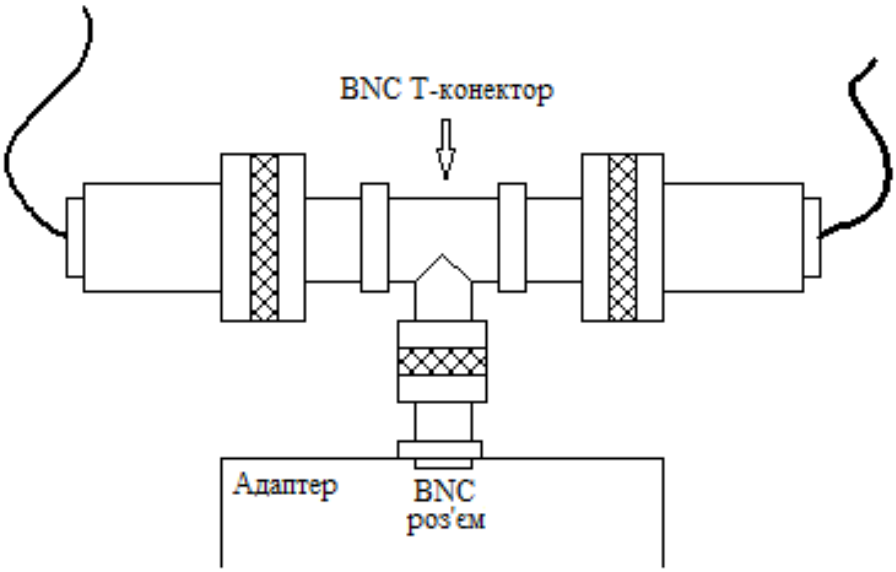


Рисунок 3.5 – Схема під'єднання адаптера по "тонкому" кабелю

Якщо вся мережа виконується на "тонкому" кабелі, то, згідно зі стандартом, кількість сегментів не повинна перевищувати п'яти (загальна довжина мережі складе 925 м, буде потрібно чотири репітера). При цьому на одному сегменті не повинно бути більше 30 абонентів, включаючи репітери, тобто загальне число комп'ютерів в мережі на базі "тонкого" кабелю не може бути більше (30-1)*3 = 87. Мінімальна відстань між комп'ютерами - 1 м.

Стандарт 10 BASE 2 передбачає використання репітерів (репітерних концентраторів), застосування яких також повинно відповідати "правилу 5-4 - 3".

Мінімальний набір обладнання для односегментної мережі на "тонкому" кабелі повинен включати в себе наступні елементи:

- Мережеві адаптери (за кількістю поєднуваних у мережу комп'ютерів);
- відрізки кабелю з BNC-роз'ємами на двох кінцях, загальна довжина яких достатня для об'єднання всіх комп'ютерів;
- BNC Т-коннектори (по числу мережевих адаптерів);
- один BNC термінатор без заземлення;
- один BNC термінатор із заземленням.

3.4. Апаратура 10BASE-T (вита пара)

У мережі Ethernet на базі витої пари (UTP-кабелі, Unshielded Twisted - Pair Cable) передача сигналів здійснюється по двох витих парах проводів, кожна з яких передається тільки в одну сторону (одна пара - передавальна, інша - приймаюча). Кожен з абонентів мережі приєднується кабелем до концентратора, використання якого обов'язкове.

Довжина з'єднувального кабелю між адаптером і концентратором не повинна перевищувати 100 м. Кабель використовується гнучкий, діаметром близько 6 мм. Найбільш поширений тип кабелю - телефонний кабель EIA / TIA категорії 3.

Кабелі приєднуються 8-контактними роз'ємами типу RJ -45, в яких використовуються тільки чотири контакти. У концентраторах іноді застосовуються також 50-контактні роз'єми типу Telco.

У стандарті визначено максимальне число концентраторів між двома станціями мережі, а саме 4. Це правило зветься "правило 4-х хабів". При створенні мережі 10 BASE - T з великим числом станцій концентратори можна з'єднувати один з одним ієрархічним способом, утворюючи деревоподібну структуру.

Петлевидні з'єднання концентраторів у стандарті 10 BASE-T заборонено. Резервування зв'язків (створення паралельних каналів зв'язку між важливими концентраторами для резервування зв'язків на випадок відмови порту, концентратора або кабелю) можливо тільки за рахунок переведення однієї з паралельних зв'язків у неактивний (заблокований) стан.

Загальна кількість комп'ютерів в мережі 10 BASE-T-1024, максимальна довжина мережі (максимальна відстань між двома комп'ютерами мережі) – 500 м.

Мінімальний набір обладнання для мережі на витій парі включає в себе наступні елементи:

- Мережеві адаптери (за кількістю поєднуваних у мережу комп'ютерів), що мають роз'єми RJ -45;
- відрізки кабелю з роз'ємами RJ -45 на кінцях (по числу об'єднуються комп'ютерів);
- Один концентратор, що має стільки UTP-портів, скільки необхідно об'єднати комп'ютерів.

3.5. Апаратура 10BASE-FL (оптоволоконний кабель)

Застосування оптоволоконного кабелю в Ethernet крім забезпечення повної гальванічної розв'язки комп'ютерів мережі, дозволило збільшити довжину сегмента й істотно підвищити стійкість передачі.

Передача інформації йде по двох оптоволоконним кабелях, що передають сигнали в різні боки.

Стандарт 10 BASE FL забезпечує зв'язок між двома комп'ютерами, між двома репітерами або між комп'ютером і репітером. Стандарт гарантує довжину оптоволоконного зв'язку між репітерами (репітерні повторювачами) до 1 км при загальній довжині мережі не більше 2500 м. Максимальна відстань між комп'ютером і концентратором - 2000 м. Максимальне число репітерів (репітерних концентраторів) між будь-якими комп'ютерами мережі - 4. Максимальна довжина оптоволоконного кабелю 10 BASE - FL, що з'єднує репітерні концентратори (репітери) з комп'ютерами, не повинно перевищувати 400 метрів. До всіх сегментах можуть підключатися комп'ютери.

Апаратура 10 BASE - FL має схожість як з апаратурою 10 BASE 5 (застосовуються зовнішні трансивери з'єднані з адаптером трансиверного кабелем), так і з апаратурою 10 BASE - T (застосовуються топології типу "пасивна зірка" і два різноспрямовані кабелі). Схема з'єднання мережного адаптера і концентратора показана на рис. 3.6.

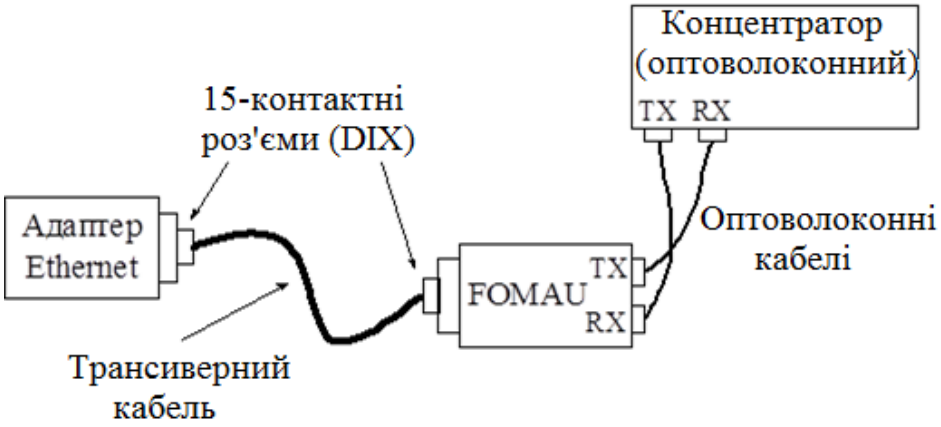


Рисунок 3.6 – Схема з'єднання мережного адаптера і концентратора

Мінімальний набір обладнання для з'єднання оптоволоконним кабелем двох комп'ютерів включає в себе наступні елементи:

- два мережевих адаптера з трансиверними роз'ємами;
- два оптоволоконних трансивера (FOMAU);
- два трансиверних кабелі;
- два оптоволоконних кабелі з ST-роз'ємами на кінцях.

3.6. Вибір конфігурації Ethernet

Дотримання численних обмежень, встановлених для різних стандартів фізичного рівня мереж Ethernet, гарантує коректну роботу мережі.

Правила "5-4-3" для коаксіальних мереж і "4-х хабів" для мереж на основі витої пари і оптоволокна не тільки дають гарантії працездатності мережі, але і залишають великий "запас міцності" мережі.

Для мереж, що складаються із змішаних кабельних систем, на які правила про кількість повторювачів не розраховані, необхідно проводити додаткові розрахунки.

Щоб мережа Ethernet, що складається із сегментів різної фізичної природи, працювала коректно, необхідне виконання чотирьох основних умов:

- кількість комп'ютерів в мережі не більше 1024;
- максимальна довжина кожного фізичного сегмента не більше величини, визначеної у відповідному стандарті фізичного рівня;
- час подвійного обороту сигналу між двома найбільш віддаленими один від одного комп'ютерами мережі не більше 575 бітового інтервалу;
- скорочення міжкадрового інтервалу при проходженні послідовності кадрів через всі повторювачі повинно бути не більше, ніж 49 бітового інтервалу.

Дотримання цих вимог забезпечує коректність роботи мережі навіть у випадках, коли порушуються прості правила конфігурування, що визначають максимальну кількість повторювачів і загальну довжину мережі в 2500 м.

3.6.1. Розрахунок часу подвійного обороту сигналу (PDV-Path Delay Value or RDT - Round Trip Delay)

Модель, що застосовується для оцінки зміни Ethernet, заснована на підрахунку часових характеристик даної конфігурації. У ній застосовується дві системи розрахунків: одна передбачає обчислення подвійного (кругового) часу проходження сигналу по мережі, а інша - перевірку допустимості одержуваного (міжкадрового) часового інтервалу. При цьому розрахунки в обох системах розрахунків ведуться для найгіршого випадку.

При першій системі розрахунків використовуються такі поняття, як "початковий сегмент", "проміжний сегмент" і "кінцевий сегмент". Відзначимо, що проміжних сегментів може бути кілька, а початковий і кінцевий сегменти при різних розрахунках можуть мінятися місцями. Для розрахунків використовуються величини затримок, які представлені в таблиці 3.1.

Таблиця 3.1 – Величини затримок

Тип сегмента Ethernet	Макс. довжин, м	Початковий сегмент		Початковий сегмент		Початковий сегмент		Початко-вий сегмент
		t0	tm	t0	tm	t0	tm	t1
10BASE5	500	11,8	55,0	46,5	89,8	169,5	212,8	0,0866
10BASE2	185	11,8	30,8	46,5	65,5	169,5	188,5	0,1026
10BASE-T	100	15,3	26,6	42,0	53,3	165,0	176,3	0,1130
10BASE-FL	2000	12,3	212,3	33,5	233,5	156,5	356,5	0,1000
FOIRL	1000	7,8	107,8	29,0	129,0	152,0	252,0	0,1000
AUI (> 2 м)	2+48=50	0	5,1	0	5,1	0	5,1	0,1026

Примітка. Затримки дано в бітових інтервалах.

Розрахунок зводиться до наступного:

1. У мережі виділяється шлях найбільшої довжини;

2. Якщо довжина сегмента не максимальна, то розраховується подвійний (круговий) час проходження в кожному сегменті виділеного шляху за формулою: ts= L*t1+t0, де L - довжина сегмента в метрах (при цьому треба враховувати тип сегмента: початковий, проміжний або кінцевий);

3. Якщо довжина сегмента максимальна, то з таблиці для нього береться величина затримки tm;

4. Сумарна величина затримок всіх сегментів виділеного шляху не повинна перевищувати 575 бітових інтервалів;

5. Потім необхідно виконати ті ж дії для зворотного напрямку обраного шляху (тобто, вважаючи кінцевий сегмент початковим, і навпаки);

6. Якщо затримки в обох випадках не перевищують 575 бітових інтервалів, то мережа працездатна.

Якщо у вибраній вами конфігурації мережі шлях найбільшої довжини не настільки очевидний, то подібні розрахунки необхідно провести для всіх шляхів, що претендують на найбільшу затримку сигналу. У будь-якому випадку подвійний час проходження відповідно до стандарту недостатній, щоб зробити остаточний висновок про працездатність мережі.

3.6.2. Розрахунок скорочення міжкадрового інтервалу (PVV - Path variability Value)

Щоб визнати конфігурацію мережі коректною, потрібно розрахувати також зменшення міжкадрового інтервалу репітерами (репітерні концентраторами).

Ця величина не повинна бути менше, ніж 49 бітових інтервалів. Для обчислень тут також використовуються поняття початкового сегмента і проміжного сегмента (кінцевий сегмент не вносить вкладу в скорочення міжкадрового інтервалу, оскільки пакет доходить по ньому до приймаючого комп'ютера без проходження репітерів і репітерних концентраторів).

Для розрахунку скорочення міжкадрового інтервалу можна скористатися значеннями максимальних величин зменшення міжкадрового інтервалу при проходженні репітеров (репітерних концентраторів) різних фізичних середовищ наведеними в таблиці 3.2.

Таблиця 3.2 – Фізичні середовища

Тип сегмента	Початковий сегмент	Проміжний сегмента
10BASE5	16	11
10BASE2	16	11
10BASE-T	10,5	8
10BASE-FL	10,5	8

Підсумовуючи величини скорочень міжкадрового інтервалу для найбільшого шляху в обраній конфігурації і порівнюючи суму з граничною величиною в 49 бітових інтервалів, ми можемо зробити висновок про працездатність мережі.

Такі ж обчислення проводяться і для зворотного напрямку по цьому ж шляху.

3.3 Порядок виконання роботи

1. Ознайомитися з теоретичною частиною до лабораторної роботи.
2. Відповідно до заданого варіантом спроектуйте локальну обчислювальну мережу організації (ДОДАТОК 3.1).
3. Підготуйте специфікацію на обладнання та матеріали спроектованої локальної обчислювальної мережі організації (ДОДАТОК 3.2).

Приклад виконання роботи наведений у ДОДАТКУ 3.3.

3.4 Вимоги до звіту

Звіт з лабораторної роботи повинен містити:

а) титульний лист;
б) завдання;
в) конфігурацію спроектованої мережі;
г) розрахунки, що підтверджують працездатність мережі;
д) специфікацію на обладнання та матеріали.

3.5 Контрольні питання

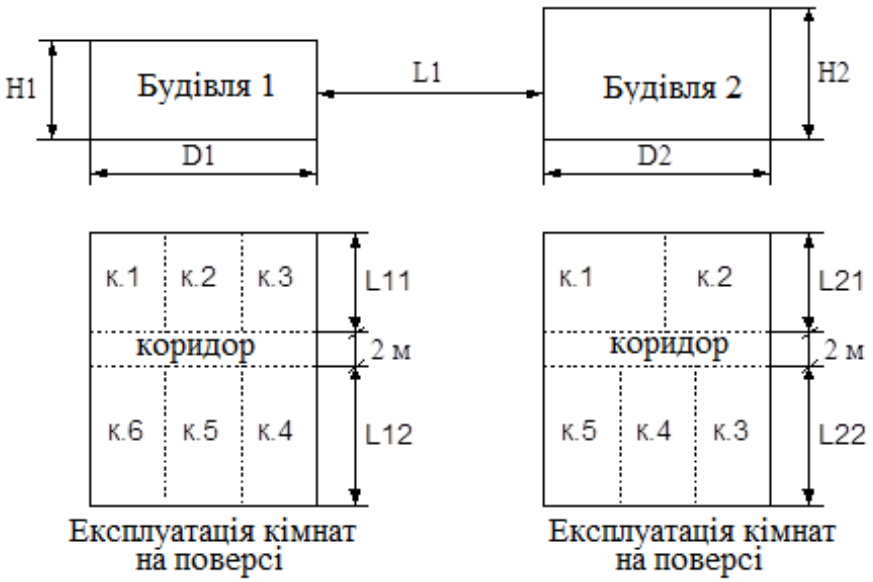
1. Середовища передачі для мережі Ethernet.
2. Апаратура 10BASE5.
3. Апаратура 10BASE2.
4. Апаратура 10BASE-T.
5. Апаратура 10BASE-FL.
6. Порядок вибору конфігурації Ethernet?
7. Що означає число 575, як воно формується?

Список використаних джерел

1. Новиков Ю.В., Карпенко Д.Г. Апаратура локальних мереж: функції, вибір, розробка / Під загальною редакцією Ю.В. Новикова. - М., Видавництво ЕКОМ, 1998. - 288с.: Ил.

2. Комп'ютерні мережі. Принципи, технології, протоколи / В.Г. Оліфер, Н.А. Оліфер. - СПб: Видавництво "Пітер", 2000. - 672 с.: Ил.

ДОДАТОК 3.1



Варіант	**L1,** м	**H1,** м	**D1,** м	**L11,** м	**L12,** м	**H2,** м	**D2,** м	**L21,** м	**L22,** м	Кількість поверхів будівлі1	Кількість поверхів будівлі 2
1.	max	**9**	**60**	**15**	**30**	**8**	**150**	**30**	**15**	**3**	**2**
2.	max	**6**	**75**	**20**	**25**	**12**	**120**	**25**	**20**	**2**	**3**
3.	max	***9***	***90***	***25***	***20***	***8***	***90***	***20***	***25***	***3***	***2***
4.	max	**6**	**120**	**30**	**15**	**12**	**60**	**15**	**30**	**2**	**3**

Варіант	**Приміщення**	**Поверх**	**Кількість комп'ютерів**					
			к.1	**к.2**	**к.3**	**к.4**	**к.5**	**к.6**
1.	**1**	**1**	**1**	**2**	**1**	**2**	**1**	**3**
		2	**3**	**1**	**2**	**1**	**2**	**1**
		3	**1**	**3**	**1**	**2**	**1**	**2**
	2	**1**	**2**	**1**	**3**	**1**	**2**	**1**
		2	**2**	**3**	**1**	**2**	**2**	**-**
2.	**1**	**1**	**3**	**1**	**2**	**1**	**2**	**1**
		2	**1**	**3**	**1**	**2**	**1**	**2**
	2	**1**	**2**	**1**	**3**	**1**	**3**	**-**
		2	**2**	**3**	**1**	**2**	**2**	**-**
		3	**4**	**2**	**1**	**2**	**1**	**-**
3.	**1**	**1**	**3**	**1**	**2**	**1**	**2**	**1**
		2	**1**	**2**	**1**	**2**	**1**	**3**
		3	**2**	**1**	**2**	**1**	**3**	**1**
	2	**1**	**3**	**1**	**3**	**1**	**2**	**-**
		2	**1**	**2**	**1**	**2**	**4**	
4.	**1**	**1**	**1**	**3**	**1**	**2**	**1**	**2**
		2	**3**	**1**	**2**	**1**	**2**	**1**
	2	**1**	**3**	**1**	**2**	**3**	**1**	**-**
		2	**4**	**1**	**2**	**1**	**2**	**-**
		3	**3**	**3**	**1**	**2**	**1**	**-**

Варіант	Приміщення	Поверх	Тип середовища передачі	Тип середовищ передачі між приміщеннями
1.	1	1	10BASE5	10BASE5
		2	10BASE2	
		3	10BASE-T	
	2	1	10BASE-FL	
		2	10BASE5	
2.	1	1	10BASE2	10BASE2
		2	10BASE-T	
	2	1	10BASE-FL	
		2	10BASE5	
		3	10BASE2	
3.	1	1	10BASE-T	10BASE-T
		2	10BASE-FL	
		3	10BASE5	
	2	1	10BASE2	
		2	10BASE-T	
4.	1	1	10BASE-FL	10BASE-FL
		2	10BASE5	
	2	1	10BASE2	
		2	10BASE-T	
		3	10BASE-FL	

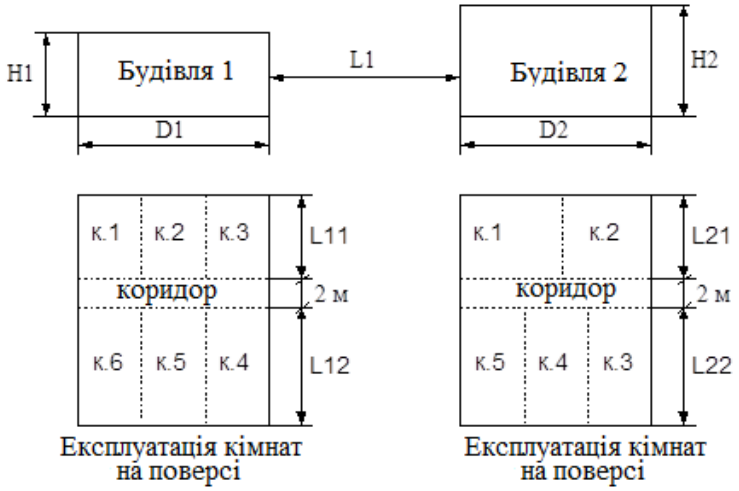
Примітка. Можна застосовувати репітери і репітерні концентратори на 4, 8, 12 портів.

ДОДАТОК 3.2

№	Назва	Одиниця вимірювання	Кількість
Обладнання			
1.	Репітер	шт.	
2.	Репітерний концентратор на 4 порта	шт.	
3.	Репітерний концентратор на 8 портів	шт.	
4.	Репітерний концентратор на 12 портів		
5.			
6.			
7.			
Матеріали			
1.	“Товстий” коаксіальний кабель	м	
2.	“Тонкий” коаксіальний кабель	м	
3.	UTP-кабель категорії 3	м	
4.	Оптичний кабель	м	
5.			

ДОДАТОК 3.3

Приклад виконання варіанту № 3



1) Розрахунок часу подвійного обороту сигналу

Таблиця 3.3.1

Тип сегменту Ethernet	Макс. довжина, м	Початковий сегмент		Проміжний сегмент		Кінцевий сегмент		Затримка метр довжини
		t0	tm	t0	tm	t0	tm	t1
10BASE5	500	11,8	55,0	46,5	89,8	169,5	212,8	0,0866
10BASE2	185	11,8	30,8	46,5	65,5	169,5	188,5	0,1026
10BASE-T	100	15,3	26,6	42,0	53,3	165,0	176,3	0,1130
10BASE-FL	2000	12,3	212,3	33,5	233,5	156,5	356,5	0,1000
FOIRL	1000	7,8	107,8	29,0	129,0	152,0	252,0	0,1000
AUI (> 2 м)	2+48=50	0	5,1	0	5,1	0	5,1	0,1026

Формула для розрахунку: $t_s = L \cdot t_1 + t_0$

У вибраній конфігурації мережі найбільший шлях складає 1214 м.

10BASE5 →10BASE2	10BASE5 ← 10BASE2
$t_1 = 99 \cdot 0{,}0866 + 11{,}8 = 20{,}3734$	$t_4 + t_5 = 311 \cdot 0{,}1026 + 15{,}3 = 47{,}2086$
$t_2 = 400 \cdot 0{,}1130 + 42{,}0 = 87{,}2$	$t_3 = 400 \cdot 0{,}1130 + 42{,}0 = 87{,}2$
$t_3 = 400 \cdot 0{,}1130 + 42{,}0 = 87{,}2$	$t_2 = 400 \cdot 0{,}1130 + 42{,}0 = 87{,}2$
$t_4 + t_5 = 311 \cdot 0{,}1026 + 169{,}5 = 201{,}4086$	$t_1 = 99 \cdot 0{,}0866 + 169{,}5 = 20{,}3734$
$t_1 + t_2 + t_3 + t_4 + t_5 = 396{,}182 < 575$	$t_1 + t_2 + t_3 + t_4 + t_5 = 399{,}682 < 575$

Затримки в обох випадках не перевищують 575 бітових інтервалів, отже мережа працездатна.

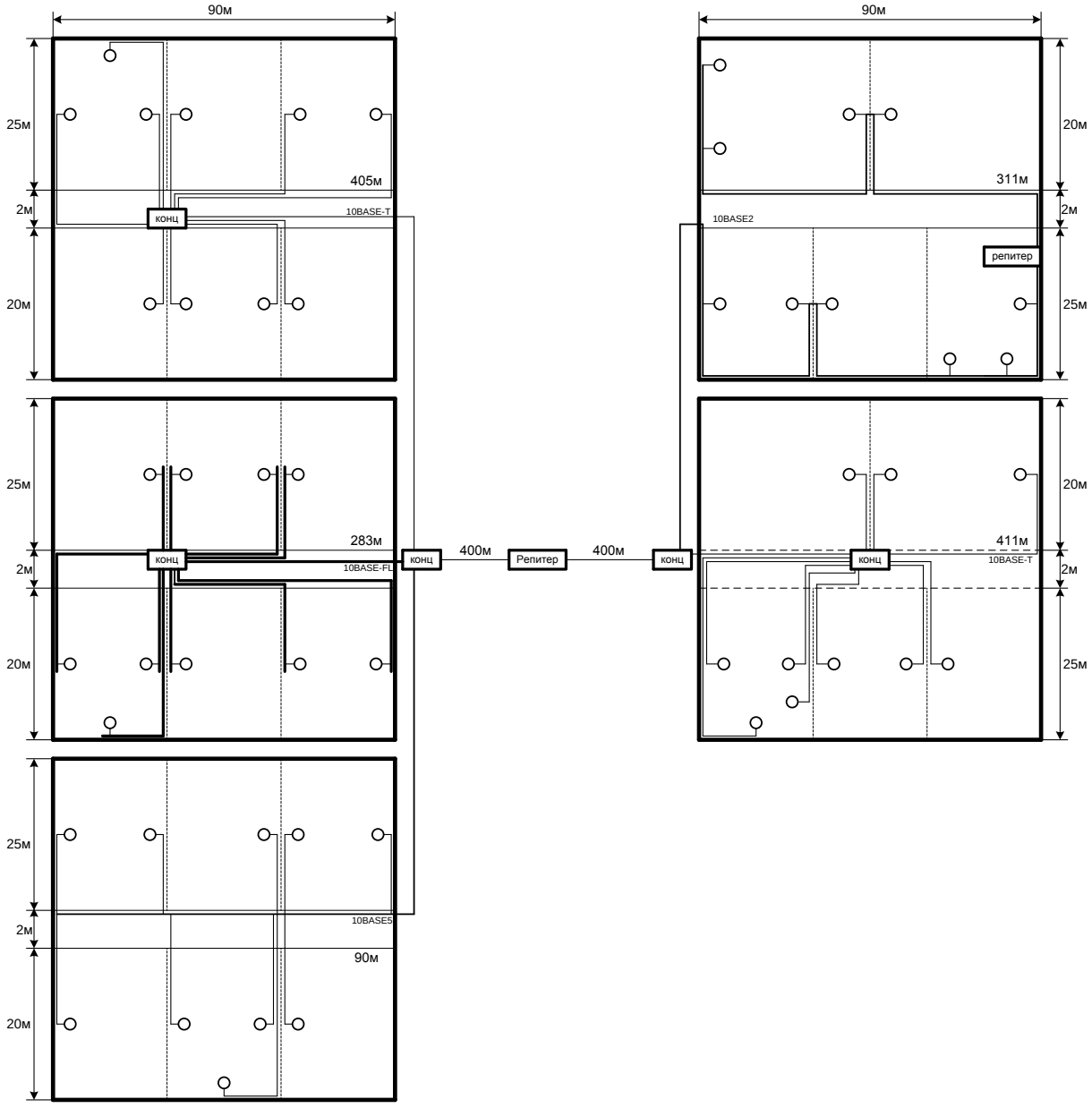
2) Розрахунок скорочення міжкадрового інтервалу

Таблиця 3.3.2

Тип сегмента	Початковий сегмент	Проміжний сегмент
10BASE5	16	11
10BASE2	16	11
10BASE-T	10,5	8
10BASE-FL	10,5	8

Суми величин скорочень міжкадрового інтервалу для усіх шляхів у обраної конфігурації менше граничної величини в 49 бітових інтервалах, отже мережа працездатна.

3) Схема спроектованої мережі



4) Специфікація:

№	Назва	Одиниця вимірювання	Кількість
Обладнання			
1.	Репітер	шт.	
2.	Репітерний концентратор на 4 порту	шт.	
3.			
4.	Репітерний концентратор на 12 портів		
5.	Мережевий адаптер	шт.	
Матеріали			
6.	“Товстий” кабель з роз’ємами N-типу на кінцях	м	
7.	Трансиверні кабелі з 15-контактними роз’ємами на кінцях	шт.	
8.	Трансивери	шт.	
9.	Оптоволоконні трансивери (FOMAU)	шт.	
10.	Barrel-коннектор N-типу для під’єднання термінаторів на кінцях кабелю	шт.	
11.	N-термінатор	шт.	
12.	N-термінатор з заземленням	шт.	
13.	Відрізки «тонкого» кабелю с BNC-роз’ємами на двох кінцях	шт.	
14.	BNC Т-коннектори	шт.	
15.	BNC термінатор без заземлення	шт.	
16.	BNC термінатор с заземленням	шт.	
17.	Відрізки кабелю с роз’ємами RJ-45 на кінцях	шт.	
18.	Оптичний кабель	м	

Лабораторна робота №4
Механізм адресації в IP-мережах

Мета роботи: вивчити адресацію, загальну класифікацію адресів в стеці TCP/IP, принцип призначення IP-адрес вузлам окремих підмереж.

ТЕОРЕТИЧНІ ВІДОМОСТІ

4.1 Типи адрес стека TCP/IP

У стеці TCP/IP використовуються три типи адрес:

- локальні (звані також апаратними)
- IP-адреси
- символьні доменні імена

4.1.1. Локальні адреси

Локальний адрес в термінології TCP/IP - це такий тип адреси, який використовується засобами базової технології для доставки даних в межах підмережі, яка сама є елементом складеної інтермережі.

У різних підмережах допустимі різні мережеві технології, різні стеки протоколів, тому при створенні стека TCP/IP вже заздалегідь передбачалося наявність різних типів локальних адрес.

Якщо підмережею інтермережі є локальна мережа, то локальна адреса - це **MAC-адреса**, яка призначається мережевим адаптерам і мережевим інтерфейсам маршрутизаторів.

MAC-адреси призначаються виробниками обладнання і є унікальними, тому що управляються централізовано.

Для всіх існуючих технологій локальних мереж **MAC**-адреса має формат 6 байт, наприклад 11-AO-17-3D-BC-01.

Треба відзначити, що оскільки протокол IP може працювати і над протоколами більш високого рівня. У цьому випадку локальними адресами для протоколу IP відповідно будуть адреси відповідних протоколів більш високого рівня.

Слід врахувати, що комп'ютер в локальній мережі може мати декілька локальних адрес навіть при одному мережевому адаптері. І навпаки, деякі мережеві пристрої взагалі не мають локальних адрес. Наприклад, до таких пристроїв відносяться глобальні порти маршрутизаторів, призначені для з'єднань типу "точка-точка".

4.1.2 IP-адреси - основний тип адрес мережевого рівня

На підставі IP-адрес мережевий рівень передає пакети між мережами:

- IP-адреси складаються з 4 байт (32 біт).
- IP-адрес призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів.
- IP-адреса складається з двох частин: номера мережі і номери вузла.

Номер мережі	Номер вузла (хоста)

Номер мережі може бути обраний адміністратором довільно, або призначений за рекомендацією спеціального підрозділу Internet (Internet Network Information Center, InterNIC), якщо мережа повинна працювати як складова частина Internet. Зазвичай постачальники послуг Internet одержують діапазони адрес у підрозділів InterNIC, а потім розподіляють їх між своїми абонентами.

Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла.

Маршрутизатор з визначення входить відразу в кілька мереж. Тому кожен порт маршрутизатора має власний IP-адрес (рис.4.1).

Рисунок 4.1 – Приклад нераціонального використання простору IP-адрес

Перед тим як відправити пакет у наступну мережу, маршрутизатор повинен визначити на підставі знайденої IP-адреси наступного маршрутизатора його локальну адресу. Для цього протокол IP, як показано на рис.4.2, звертається до протоколу дозволу адрес (ARP).

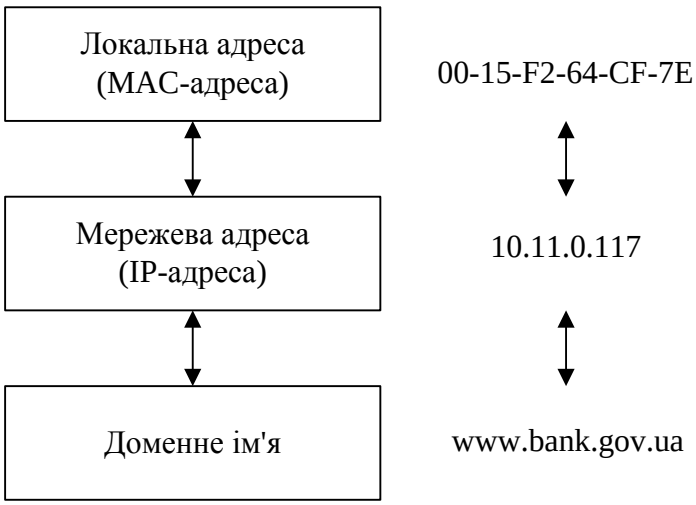


Рисунок 4.2 – Перетворення адрес

Кінцевий вузол також може входити в кілька IP-мереж. У цьому випадку комп'ютер повинен мати кілька IP-адрес, по числу мережевих зв'язків.

Таким чином, IP-адрес характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання.

4.1.3 Символьні імена

Символьні імена мають символьний вигляд і в IP-мережах називаються **доменними.**

Доменні імена будуються за ієрархічною ознакою. Повне символьне ім'я в IP-мережах складається з декількох складових, які розділяються крапкою. Вони перераховуються в наступному порядку (зліва-направо):

ім'я кінцевого вузла	.	ім'я групи вузлів (наприклад, ім'я організації)	.	ім'я більш великої групи (піддомену)

Рисунок 4.3 – Символьна структура доменного імені

Домен позначається за географічним принципом: UA - Україна, RU - Росія, UK - Великобританія, SU - США)

Прикладом доменного імені може служити ім'я base2.sales.zil.ru. Між доменним ім'ям та IP-адресою вузла немає ніякої відповідності, тому необхідно використовувати якісь додаткові таблиці або служби, щоб вузол інтермережі однозначно міг визначатися в мережі, як по доменному імені, так і за IP-адресою.

4.2 IP адреси. Класи IP адрес

4.2.1 Структура IP-адреси

IP-адреси призначаються не вузлам складової мережі, а мережним інтерфейсам вузлів складової мережі.

Більшість комп'ютерів в IP мережі мають єдиний мережевий інтерфейс (і як наслідок одна IP адреса). Але комп'ютери та інші пристрої можуть мати кілька (якщо не більше) мережевих інтерфейсів - і кожен інтерфейс буде мати свою власну IP адресу.

Так пристрій з 6 активними інтерфейсами (наприклад, маршрутизатор) матиме + 6 IP адрес - по одній на кожен інтерфейс в кожній мережі, до якої він підключений.

Отже, IP адрес визначає однозначно мережу і вузол, який підключений до цієї мережі. IP адрес має довжину 4 байти (4 по 8 біт), це дає в сукупності 32 біта доступної інформації.

Для покращення читабельності, IP адрес записується у вигляді чотирьох чисел, розділених крапками:

Двійкова форма: **XXXXXXXX . XXXXXXXX . XXXXXXXX . XXXXXXXX** X= стан біту, 0 або 1 XXXXXXXX - байт
Дестякова форма: **YYY . YYY . YYY . YYY** YYY= число в межах від 0 до 255

Наприклад, **128.10.2.30** - десяткова форма представлення адреси - 4 (десяткових) числа, розділених (.) крапками, а **10000000 00001010 00000010 00011110** - двійкова форма представлення цього ж адреси.

Двійкова система	7-біт	6-біт	5-біт	4-біт	3-біт	2-біт	1-біт	0-біт
Десяткова система	2^7=128	2^6=64	2^5=32	2^4=16	2^3=8	2^2=4	2^1=2	2^0=1
Сума всіх чисел в десятковій системі числення в межах одного байту $2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0=255$								

Оскільки кожна з чотирьох чисел - це десяткове подання 8-бітного байта, то кожне число може приймати значення від 0 до 255 (дає 256 унікальних значень - пам'ятайте, нуль - це теж величина).

Десяткова форма запису IP-адреси використовується в основному в операційних системах, як найбільш зручна при налаштуванні.

Крім двійкової форми, зустрічається шістнадцяткова форма запису IP-адреси: **C0.94.1.3**

Використання 32-розрядних двійкових чисел дозволяє створювати **4294967296** унікальних IP-адрес - більш ніж достатньо для будь-якої приватної інтрамережі.

IP адрес складається з двох логічних частин - **номера мережі і номера вузла в мережі** (рис.4.3) (загалом 32 біти виділено для IP адреси, і з них, N-біт для ідентифікації вузла, і 32-N – для ідентифікаї номера мережі).

32 - N біт	**N - біт**
Номер мережі	Номер вузла

Рисунок 4.3 – Структура IP-адреси

4.2.2 Класи IP-адрес

Звичайно ж, відразу виникає питання: а як визначити в одній адресі, де номер мережі, а де номер вузла? Можна домовиться використовувати, наприклад, перші 8 біт адреси для номера мережі, а решта для номерів вузлів в тій мережі, або перші 16 біт, або перші 24 біта. Але в такому випадку адресація виходить абсолютно гнучкою, ми будемо мати або багато маленьких мереж і мало великих, або навпаки.

Для того щоб більш раціонально визначитися з величиною мережі і при тому розмежувати яка частина IP-адреси відноситься до номера мережі, а яка – до номера вузла домовилися використовувати систему класів. Система класів використовує значення першого біту адреси.

Але, таким чином, що значення цих перших біт адреси є ознаками того, до якого класу належить той чи інший IP-адрес.

На рисунку 4.4 зображено класи адрес.

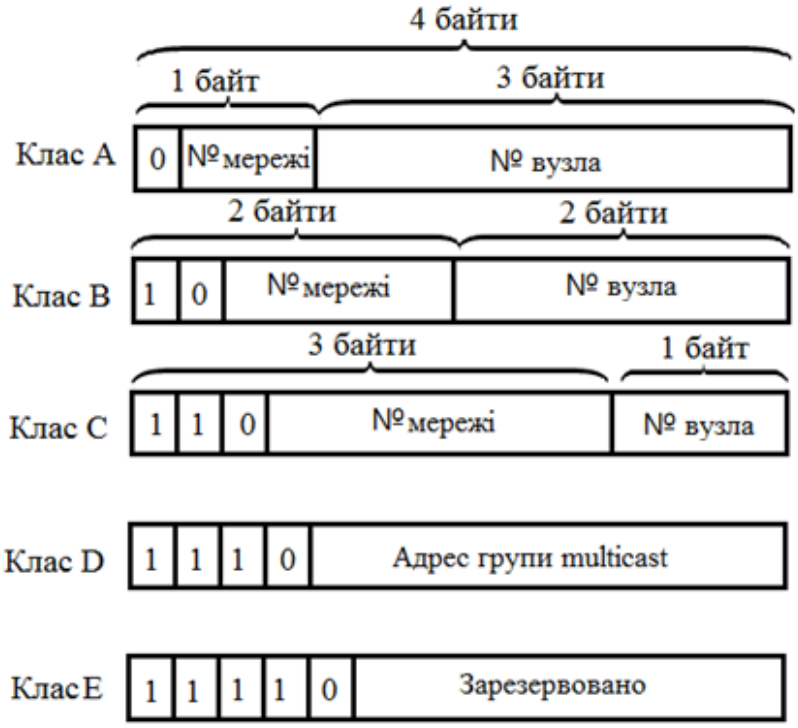


Рисунок 4.4 – Класи адресів

В окремій таблиці наведено діапазони номерів мереж і максимальне число вузлів, що відповідають кожному класу мереж:

Таблиця 4.1 – Діапазони номерів мереж і максимальне число вузлів

Клас	**Перші біти**	**Найменший адрес мережі**	**Найбільший адрес мережі**	**Максимальна кількість вузлів**
A	**0**	1.0.0.0	126.0.0.0	2^{24} (16 777 216-2)
B	**10**	128.0.0.0	191.255.0.0	2^{16} (65536-2)
C	**110**	192.0.1.0	223.255.255.0	2^{8} (256-2)
D	**1110**	224.0.0.0	239.255.255.255	Multicast
E	**11110**	240.0.0.0	247.255.255.255	зарезервовано

Якщо адреса починається з послідовності 1110, то вона є адресою класу D і позначає особливий, груповий адрес – **multicast** (від. анг. групова передача).

Якщо в пакеті як адрес призначення вказано адрес класу D, то такий пакет повинен отримати всі вузли, яким визначено цю адресу.

Якщо адреса починається з послідовності 11110, то це означає, що дана адреса відноситься до класу E. Адреси цього класу зарезервовані для майбутніх застосувань.

Таким чином, можна однозначно визначити, що: великі мережі отримують адреси класу A, середні -класу B, а маленькі - класу C (рис.4.5).

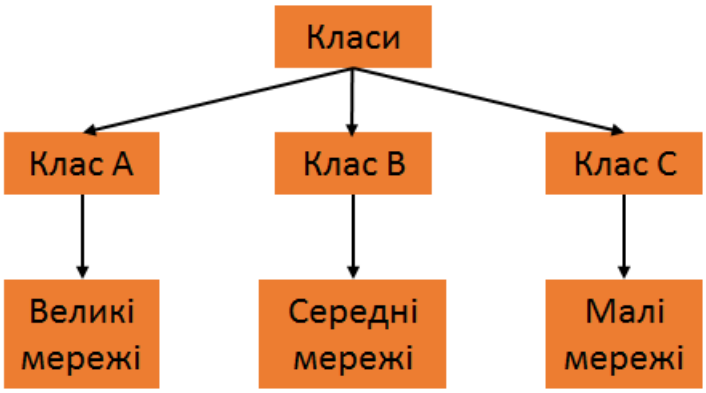


Рисунок 4.5 – Призначення класів IP-адрес

Залежно від того до якого класу (A B C) належить адрес, номер мережі може бути представлений першими 8, 16 або 24 розрядами, а номер хоста (вузла) - останніми 24, 16 або 8 розрядами.

Існують деякі значення IP-адрес, які зарезервовані заздалегідь, тобто існують IP-адреси, які призначені для особливих цілей:

1) Якщо всі IP-адреси складається тільки з двійкових нулів, то він позначає адресу того вузла, який згенерував цей пакет

0	0	0	0	…….		0	0	0	0

цей режим використовується тільки в деяких повідомленнях протоколу міжмережевих керуючих повідомлень ICMP.

2) Якщо в полі номера мережі містяться нулі, то за замовчуванням вважається, що вузол призначення належить тій же самій мережі, що і вузол, який відправив пакет.

0	0	0	0	…….	0	Номер вузла

IP-адрес з нульовим номером хоста використовується для адресації всієї мережі. Наприклад, в мережі класу C з номером 199.60.32 IP-адрес 199.60.32.0 позначає мережу в цілому.

3) Якщо всі двійкові розряди IP-адреси рівні 1, то пакет з такою адресою призначення повинен розсилатися всім вузлам, що знаходяться в тій же мережі, що й джерело цього пакета.

1	1	1	1	…….	1	1	1	0

Така розсилка називається обмеженим широкомовним повідомленням (limited broadcast).

4) Якщо в полі номера вузла призначення стоять тільки одиниці, то пакет, що має такий адреса, розсилається всім вузлам мережі із заданим номером мережі. Наприклад, пакет з адресою 192.190.21.255 доставляється всім вузлам мережі 192.190.21.0.

Номер мережі	1	1	1	……	1	1	1	1

Така розсилка називається широкомовним повідомленням (**broadcast**), тобто поток даних призначений для прийому всіма ділянками мережі (в межах одного сегменту мережі (рис.4.6).

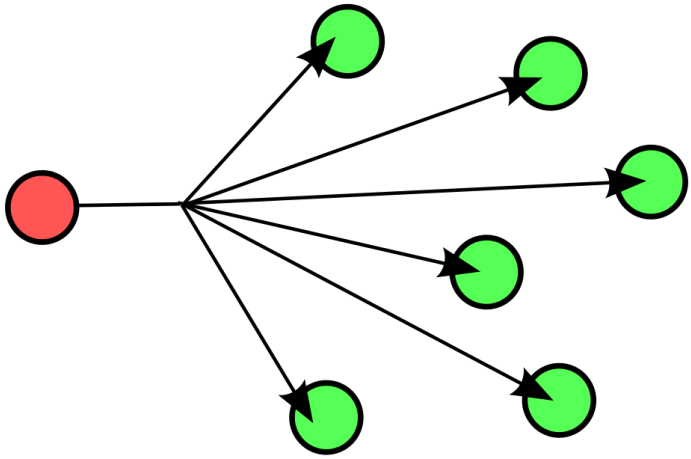


Рисунок 4.6 – Схема широмовної передачі

Припустимо, наприклад, що один з хостів в мережі класу С з мережевою адресою **199.60.32.0** збирається направити повідомлення всім іншим хостам, що знаходяться в тій же мережі. У цьому випадку повідомлення повинно бути передано на адресу **199.60.32.255** (останій байт 255 є broadcast).

Таким чином ні номер мережі, ні номер вузла не може складатися тільки з одних двійкових одиниць або тільки з одних двійкових нулів. Звідси випливає, що максимальна кількість вузлів, яка наведене в таблиці 4.1 для мереж кожного класу, на практиці повинна бути зменшена на 2 (broadcast + номера вузла).

Особливий сенс має IP-адрес, перший октет (байт) якого дорівнює 127 і є зарезервованим для тестування програм і взаємодії процесів в межах однієї машини.

Коли програма посилає дані по IP-адресу **127.0.0.1**, то утворюється як би "петля", тобто дані не передаються по мережі, а повертаються модулям верхнього рівня, як тільки що прийняті.

Тому в IP-мережі забороняється присвоювати машинам IP-адреси, що починаються із 127. Ця адреса має назву **loopback**.

Можна віднести адресу 127.0.0.0 до внутрішньої мережі модуля маршрутизації вузла, а адресу 127.0.0.1 - до адреси цього модуля на зовнішній мережі.

Насправді будь-яка адреса мережі 127.0.0.0 служить для позначення свого модуля маршрутизації, а не тільки 127.0.0.1, наприклад 127.0.0.3.

У протоколі IP немає поняття широкомовного в тому сенсі, в якому воно використовується в протоколах канального рівня локальних мереж, коли дані повинні бути доставлені абсолютно усіх вузлів.

Як обмежена широкомовна IP-адреса, так і широкомовна IP-адреса мають свої межі поширення в інтермережі - вони обмежені або мережею, до якої належить вузол-джерело пакету, або мережею, номер якої зазначений в адресі призначення. Тому поділ мережі за допомогою маршрутизаторів на частини локалізує широкомовний шторм межами однієї зі складових загальної мережі частин просто тому, що немає способу адресувати пакет одночасно всім вузлам всіх мереж складовою мережі.

IP адрес **multicast** означає, що даний пакет повинен бути доставлений відразу декільком вузлам, які утворюють групу з номером, зазначеним у полі адреси.

Вузли самі ідентифікують себе, тобто визначають, до якої з груп вони відносяться. Один і той же вузол може входити в кілька груп. Члени якої-небудь групи **multicast** не обов'язково повинні належати одній мережі. У загальному випадку вони можуть розподілятися по зовсім різним мережам, що знаходяться одна від одної на довільній кількості хопів (транзитна ділянка компютерної мережі).

Груповий адрес не ділиться на поля номера мережі й вузла й обробляється маршрутизатором особливим чином.

Основне призначення **multicast-адреси** - розповсюдження інформації по схемі "один-до-багатьох".

Рисунок 4.4 – Технологія **multicast**

Вона працює таким чином: хост, який хоче передавати одну і ту ж інформацію багатьом абонентам, за допомогою спеціального протоколу IGMP (Internet Group Management Protocol) повідомляє про створення в мережі нової мультітранслювальної групи з певною адресою.

Машрутизатори, що підтримують мультитранслювання, поширюють інформацію про створення нової групи в мережах, підключених до портів цього маршрутизатора.

Хости, які хочуть приєднатися до новостворюваної мультитранслювальної групи, повідомляють про це своїм локальним маршрутизаторам і ті передають цю інформацію хосту, ініціаторові створення нової групи.

Щоб маршрутизатори могли автоматично поширювати пакети з адресою multicast по складеній мережі, необхідно використовувати в кінцевих маршрутизаторах спеціальні модифіковані протоколи обміну маршрутною інформацією.

Загалом, групова адресація була призначена для економічного поширення в Internet або великої корпоративної мережі аудіо-або відеопрограм, призначених відразу великій аудиторії слухачів або глядачів.

Треба сказати, що якщо такі засоби знайдуть широке застосування (зараз вони представляють в основному невеликі експериментальні ділянки в загальній Internet), то Internet зможе створити серйозну конкуренцію радіо і телебаченню.

Отже, IP адрес може означати одне з трьох:

1. Адрес IP мережі (група IP пристроїв, що мають доступ до загального середовища передачі - наприклад, всі пристрої в сегменті Ethernet). Мережева адреса завжди має біти інтерфейсу (хоста) адресного простору встановленими в 0 (якщо мережа НЕ розбита на підмережі);
2. Широкомовна адреса IP мережі (адреса для «розмови» із усіма пристроями в IP мережі). Широкомовні адреси для мережі завжди мають хостової біти адресного простору встановленими в 1 (якщо мережа нерозбита на підмережі).
3. Адреса інтерфейсу (наприклад Ethernet – адаптер або PPP інтерфейс хоста, маршрутизатора, сервера друк і т.д.). Ці адреси можуть мати будь-які значення хостових бітів, виключаючи всі нулі або всі одиниці – щоб не плутати з адресами мереж і широкомовними адресами.

Для мережі класу А ...
(Один байт підадреси мережі, три байта під номер хоста)
10.0.0.0 мережа **класу А,** тому що всі хостові біти рівні 0.
10.0.1.0 адреса хоста в цій мережі
10.255.255.255 широкомовна адреса цієї мережі, оскільки всі мережеві біти встановлені в **1**
Для мережі класу В...
(Два байти під адреса мережі, два байти під номер хоста)
172.17.0.0 мережа класу В
172.17.0.1 адреса хоста в цій мережі
172.17.255.255 мережева широкомовна адреса
Для мережі класу С. ..
(Три байти під адреса мережі, один байт під номер хоста)
192.168.3.0 адреса мережі класу С

192.168.3.42 хостової адреси в цій мережі
192.168.3.255 мережевий **широкомовний адрес**
Чи не всі доступні мережеві IP адреси належать класу С.

4.2 Маски в IP адресації

Отже, розглянута традиційна схема розподілу IP-адреси на номер мережі, і номер вузла, яка базується на понятті класу. Клас визначається значеннями декількох перших біт адреси. Тепер, наприклад, можна визначити, що оскільки перший байт адреси 185.23.44.206 потрапляє в діапазон 128-191, то ця адреса відноситься до класу В, а значить, номером мережі є перші два байти, доповнені двома нульовими байтами 185.23.0.0, а номером вузла - 0.0.44.206.

Очевидно, що визначення номерів мережі по перших байтам адреси також не цілком гнучкий механізм для адресації. А що якщо використовувати який-небудь іншу ознаку, за допомогою якої можна було б більш гнучко встановлювати межу між номером мережі і номером вузла?

В якості такої ознаки зараз одержали широке поширення маски.

Маска - це 32-розрядне число, яке має такий же вигляд, як і IP-адрес. Маска використовується в парі з IP-адресою, але не збігається з нею.

Принцип відділення номера мережі і номера вузла мережі з використанням маски полягає в наступному: двійковий запис маски містить *одиниці* в тих розрядах, які в IP-адресі повинні представлятися як номер мережі і *нулі* в тих розрядах, які представляються як номер хоста.

Маска (накладається на IP-адрес)	
111…..1111	000…..000
Визначає мережу	Визначає хост (вузол)

Кожен клас IP-адрес (А, В і С) має свою маску, яка використовується за замовчуванням.

Оскільки номер мережі є цілою частиною адреси, одиниці в масці також повинні представляти неперервну послідовність.

Таким чином, для стандартних класів мереж маски мають такі значення:

Клас А	**11111111. 00000000. 00000000. 00000000**	**255.0.0.0**
Клас В	**11111111. 11111111. 00000000. 00000000**	**255.255.0.0**
Клас С	**11111111. 11111111. 11111111. 00000000**	**255.255.255.0**

Наприклад:

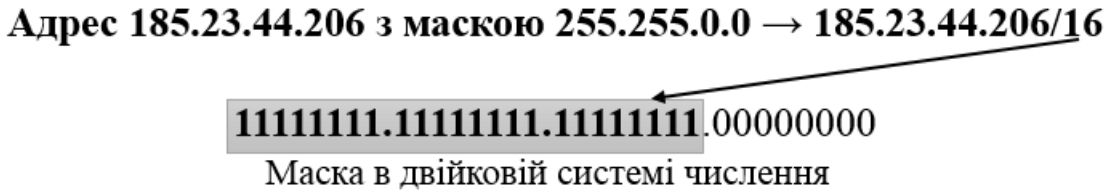
Якщо адресі **185.23.44.206** призначити маску **255.255.255.0** (**11111111.111111.1111111.0000000**), то номером мережі буде **185.23.44.0**, а не **185.23.0.0**, як це визначено правилами системи класів:

AND	10111001.00010111.00101100.11001110	**185.23.44.206**	IP-адрес
	11111111.11111111.11111111.00000000	**255.255.255.0**	Маска
	10111001.00010111.00101100.00000000	**185.23.44.0**	Мережа

Для запису **масок** використовуються й інші формати, наприклад, зручно інтерпретувати значення маски,записаної в шістнадцятковому коді:

FF.FF.00.00 - маска для адрес класу B.

Часто зустрічається і таке позначення: IP-адреса/префікс мережі. Наприклад, **185.23.44.206/16** - цей запис говорить про те, що маска для цієї адреси містить 16 одиниць (префікс мережі), або що у вказаній IP-адресі під номер мережі відведено **16** двійкових розрядів:



Нотація з префіксом мережі також відома як безкласова міждоменна маршрутизація (Classless Interdomain Routing - CIDR).

Таким чином, дуже легко, постачаючи кожен IP-адрес довільної (не обов'язково кратної 8), відмовитися від понять класів адрес тим самим зробити більш гнучкою систему IP адресації.

Розглянемо приклад: для IP-адреси **129.64.134.5** призначимо маску **255.255.128.0**, що в двійковому вигляді буде виглядати так:

IP адрес - 129.64. 134.5	**10000001.01000000.1 0000110.00000101**
Маска - 255.255.128.0	**11111111.11111111.1 0000000.00000000**

Тут перших 17 послідовних одиниць у масці, "накладаються" на IP-адрес за принципом «AND» (тобто, при двох одиницях буде одиниця, а при нулі і одиниці буде нуль), і визначають номер мережі:

IP адрес вузла 129.64.128.0	**10000001. 01000000. 10000000. 00000000**

а 15 нулів визначають номер вузла:

0000110.00000101 або **0.0.6.5.**

Механізм масок дуже широко поширений в IP-маршрутизації , причому маски можуть використовуватися для самих різних цілей. З їх допомогою адміністратор може структурувати свою мережу, не вимагаючи від постачальника послуг додаткових номерів мереж.

На основі цього ж механізму постачальники послуг можуть об'єднувати адресні простори декількох мереж шляхом введення так званих "префіксів" з метою зменшення обсягу таблиць маршрутизації , і підвищення за рахунок цього продуктивності маршрутизаторів.

Маски при записі завжди "нерозлучні" з відповідними адресами, IP-адрес маски підмережі - саме так тепер і ми будемо описувати адресу будь-якого хоста мережі.

4.5 Порядок призначення IP адрес. Автономні IP адреси. Автоматизація призначення IP адрес

У ситуації, яка наведена в прикладі (рисунок 4.5), для виродженої мережі, утвореної каналом, що зв'язує порти двох суміжних маршрутизаторів, доводиться виділяти окремий номер мережі, хоча в цій мережі є всього 2 вузла.

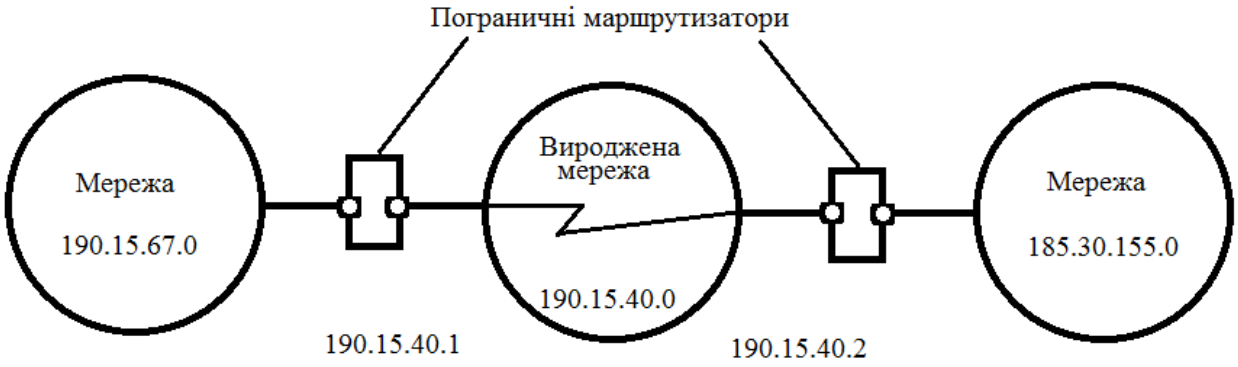


Рисунок 4.5 – Приклад виродженої мережі

Давайте розглянемо іншу ситуацію: які IP-адреси може використовувати адміністратор, якщо провайдер послуг Internet не призначив йому ніякого адресу? Якщо, наприклад, ми точно знаємо, що мережа, яку ми адмініструємо ніколи в майбутньому не буде підключатися до Internet (працює в "автономному режимі"), тоді ми можемо використовувати будь-які IP-адреси, дотримуючись правил їх призначення, про які йшла мова вище.Для простоти можна використовувати адреси класу C: у цьому випадку не доведеться обчислювати значення маски підмережі і обчислювати адресу для кожного хоста.

У цьому випадку ми повинні будемо просто призначити кожному сегменту нашої локальної мережі його власний мережевий номер класу C.

Якщо всі сегменти нашої локальної мережі мають власні мережеві номера класу C , то в кожному сегменті можна створити по 254 номери хостів.

Проте якщо у нас є хоча б невелика ймовірність того, що коли-небудь в майбутньому наша мережа може бути підключена до Internet, не слід використовувати такі IP-адреси. Вони можуть призвести до конфлікту з іншими адресами в Internet. Щоб уникнути таких конфліктів, потрібно використовувати IP-адреси, зарезервовані для приватних мереж.

Для цієї мети зарезервовано спеціально кілька блоків IP-адрес, які називаються автономними.

Автономні адреси зарезервовані для використання приватними мережами. Вони зазвичай використовуються організаціями, які мають свою приватну

велику мережу – intranet (локальні мережі з архітектурою і логікою Internet), але й маленькі мережі часто знаходять їх корисними.

Ці адреси не обробляються маршрутизаторами Internet, ні за яких умов. Ці адреси обрані з різних класів:

Клас	**Від IP-адреси**	**До IP-адреси**	**Всього вузлів адрес в діапазоні**
A	10.0.0.0	10.255.255.255	16 777 216-2
B	172.16.0.0	172.31.255.255	65 536-2
C	192.168.0.0	192.168.255.255	256-2

Ці адреси є зарезервованими для приватних мереж. Таким чином, якщо в майбутньому ми вирішимо таки підключити свою мережу до Internet, то навіть якщо трафік з однієї з хостів в нашій мережі і потрапить будь-яким чином в Internet, конфлікту між адресами статися не повинно. Маршрутизатор в Internet запрограмований так, щоб не транслювати повідомлення, що направляються з зарезервованих адрес або на них.

Треба сказати, що використання автономних IP-адрес має і недоліки, які полягають у тому, що якщо ми будемо підключати свою мережу до Internet, то нам доведеться заново налаштувати конфігурацію хостів, що з'єднуються з Internet.

Можна сказати, що підмережа - це метод, який полягає в тому, щоб взяти мережевий IP адресі локально розбити його так, щоб цей один мережевий IP адрес міг насправді використовуватися в декількох взаємопов'язаних локальних мережах.

Один мережевий IP адрес може використовуватися тільки для однієї мережі. Найважливіше: розбиття на підмережі – цел локальна настройка, вона не видна "зовні". Розбиття однієї великої мережі на підмережі, значно розвантажує загальний трафік і дозволяє підвищити безпеку всієї мережі в цілому.

Алгоритм розбиття мережі на підмережі:

1) Встановлюємо фізичні з'єднання (мережеві кабелі і мережеві з'єднувачі - такі як маршрутизатори);

2) Приймаємо рішення наскільки великі/маленькі підмережі вам потрібні, виходячи з кількості пристроїв, яке буде підключено до них, тобто, скільки IP адрес потрібно використовувати в кожному сегменті мережі.

3) Обчислюємо відповідні мережеві маски і мережеві адреси;

4) Роздаємо кожному інтерфейсу в кожній мережі свій IP адрес і відповідну мережеву маску;

5) Налаштовуємо кожен маршрутизатор і всі мережеві пристрої;

6) Перевіряємо систему, виправляємо помилки.

Зараз наше завдання розібратися з тим, як виконати 2-й і 3-й кроки.

Приклад 1

Припустимо, що ми хочемо розбити нашу мережу на підмережі, але маємо тільки один IP-адрес мережі:

IP адрес мережі	**210.16.15.0**

Рішення:

Клас	**C** (визначено за діапазоном адрес)
Маска по замовчуванню	**255.255.255.0** (в залежності від класу)
Максимальна кількість хостів	**254** - адрес мережі - широкомовна адреса = **252**
Адреса мережі	**210.16.15.0** (накладена маска на адресу)
Широкосовна адреса	**210.16.15.255** (останій адрес хосту)

1) ***Перший крок: визначити "розмір" підмережі.***

Існує залежність між кількістю створюваних підмереж і "витраченими" IP адресами.

Кожна окрема IP мережа має дві адреси, які невикористовуються для інтерфейсів (хостів):

- IP адреса власне мережі
- Широкомовна адреса.

При розбивці на підмережі кожна підмережа вимагає свій власний унікальний IP адрес мережі і широкомовну адресу - і вони повинні бути коректно обрані з діапазону адрес IP мережі, яку ми ділимо напідмережі.

Отже, якщо при розбивці IP мережі на підмережі, в кожній з яких є два мережевих адреси і два широкомовних адреси - треба пам'ятати, що кожна з них зменшить кількість використовуваних інтерфейсних (хостових) адрес на два.

Це ми повинні завжди враховувати при обчисленні мережевих номерів.

2) ***Наступний крок - обчислення маски підмережі і мережевих номерів.***

Мережева маска - це те, що виконує всі логічні маніпуляції з розділення IP мережі на підмережі .

Для всіх трьох класів IP мереж існують стандартні мережеві маски :

- **Клас A** (8 мережевих бітів): **255.0.0.0**
- **Клас B** (16 мережевих бітів): **255.255.0.0**
- **Клас C** (24 мережевих біта): **255.255.255.0**

Щоб створити **підмережу**, потрібно змінити маску підмережі для даного класу адрес.

Номер підмережі можна задати, запозичивши потрібне для нумерації підмереж кількість розрядів в номері хоста:

<table>
<tr><th>XXXXXXXX.XXXXXXXX.XXXXXXXX</th><th>XXX</th><th>XXXX</th></tr>
<tr><td>Наприклад: область мережі
X – стан біта, 0 або 1</td><td colspan="2">Область хостів до розбивання на підмережі</td></tr>
<tr><td>У даному прикладі: 24 біта для мережі, 3 біта для підмережі і 4 біта для хостів
Область підмережі, хостів і мережі в IP-адресі може бути різною для різних мереж</td><td>Запозичення області хостів для ідентифікації підмережі</td><td>Область хостів, які залишаються при розбиванні на підмережі</td></tr>
<tr><td colspan="3">Вхідна маска у наведеному прикладі:
1111111.1111111.1111111.00000000
Новоутворена маска для ідентифікації підмережі у наведеному прикладі:
1111111.1111111.1111111.11100000
В останоьому байті, добавлено 3 старших біти для ідентифікації підмереж</td></tr>
</table>

Для цього беруться ліві (старші) розряди з номера хоста, в масці самовзяті розряди заповнюються одиницями, щоб показати, що ці розряди тепер нумерують НЕ вузол, а підмережу. Значення в розрядах маски підмережі залишаються рівними нулю; це означає, що залишилися розряди в номері хоста в IP-адресі повинні використовуватися як новий (менший) номер хоста.

Наприклад, щоб розбити мережеву адресу на дві підмережі, ми повинні запозичити один хостовий біт, встановивши відповідний біт в мережевій масці першого хостового біта в 1.

Якщо нам потрібно чотири підмережі – використовуємо два хостових біта, якщо вісім підмереж - три біта і т.д. Однозначно, що якщо нам потрібно п'ять підмереж, то ми будемо використовувати три хостових біта. Відповідним чином змінюється і маска підмережі :

Процедура визначення кількості бітів, які виділяються ідентифікації N-підмереж зображено на рис.4.6.

Рисунок 4.6 – Алгоритм визначення кількості бітів для ідентифікації N підмереж

Для адрес **класу С**, при розбитті на 2 підмережі це дає маску -

11111111.11111111.11111111.10000000 або **255.255.255.128**

при розбитті на **4 підмережі** маска в двійковому вигляді -

11111111.11111111.11111111.11000000
або в десятковому **255.255.255.192**

і т.д.

Для нашої адреси мережі класу С **210.16.15.0**, можна визначити наступних кілька способів розбивки на підмережі.

Таблиця 4.2 – Способи розбивки на підмережі

Чимсло підмереж	Число хостів	Мережева маска
2	126	255.255.255.128 (11111111.11111111.11111111.10000000)
4	62	255.255.255.192 (11111111.11111111.11111111.11000000)
8	30	255.255.255.224 (11111111.11111111.11111111.11100000)
16	14	255.255.255.240 (11111111.11111111.11111111.11110000)
32	6	255.255.255.248 (11111111.11111111.11111111.11111000)
64	2	255.255.255.252 (11111111.11111111.11111111.11111100)

Тепере потрібно розв’язати питання про адреси мереж і широмовні адреси, і про діапазон IP адрес.

Знову, приймаючи до уваги тільки мережеві адреси класу С, і вказавши тільки послідовно (хостову), отримано таблицю 4.3.

Таблиця 4.3 – Структура адреси

Мережева маска	Підмережа	Мережа	Broadcast	minIP	maxIP	Хости	Всього хостів
128	2	0	127	1	126	126	252
		128	255	129	254	126	
192	4	0	63	1	62	62	248
		64	127	65	126	62	
		128	191	129	190	62	
		192	255	193	254	62	
224	8	0	31	1	30	30	240
		32	63	33	62	30	
		64	65	65	94	30	
		96	97	97	126	30	
		128	129	129	158	30	
		160	161	161	190	30	
		192	193	193	222	30	
		224	225	225	254	30	

З таблиці 4.3 відразу видно, що збільшення кількості підмереж скорочує загальну кількість доступних хостових адрес. На підставі цієї іноформації можна призначати хостові і мережеві IP адреси і мережеві маски.

Приклад 2.

Визначимо, скільки потрібно підмереж для нашої мережі класу С, щоб розбити її на підмережі по 10 хостів у кожній.

Рішення:

Мережа класу С може обслуговувати всього 254 хоста плюс адреса мережі і широкомовна адреса.

Для адресації 10-ти хостів 3-х розрядів недостатньо, тому необхідно 4-ий розряд. Отже, з восьми можливих для класу С, нам потрібно тільки 4 розряди для адресації 10 хостів, інші можна використовувати як мережеві для адресації підмереж. Кожна підмережа зменшує кількість можливих хостових адрес в два рази.

Для адресації 16 підмереж необхідно використовувати 4 розряди. Отже, порахуємо тепер кількість вузлів в кожній з 16 підмереж:2^4 -2 =14 хостів. Ця кількість із запасом задовольняє умову задачі.

Обчислимо маску підмережі, в цьому випадку вона має вигляд:

11111111.11111111.11111111.11110000 або 255.255.255.240

Ми повинні будемо вказати цю маску при налаштуванні конфігурації кожного хоста в нашій мережі (незалежно від того, в якій підмережі знаходиться хост).

Тепер, наприклад, ми можемо сказати, адреса **192.168.200.246** з маскою **255.255.255.240** - означає номер мережі **192.168.200.240** і номер вузла **0.0.0.6**.

Приклад 3.

Тепер, для всіх трьох класів визначимо відповідно маски підмережі, і максимальну кількість можливих вузлів в кожній з цих підмереж, якщо необхідно розбити відповідно мережу класу А, мережу класу В, мережу класу С на окремі 4 підмережі.

Рішення:

Для мережі класу А.

Максимальна кількість вузлів 16 777 216. Для адресації 4-х підмереж необхідно 2 розряди (00000010), значить залишається 22 розряди для адресації хостів. Таким чином, кожна з чотирьох підмереж здатна обслуговувати 2^{22}-2=4194302 хоста в кожній з підмереж.

Число підмереж	Число хостів	Мережева маска
4	4 194 302	255.192.0.0 (11111111. 11000000.00000000.00000000)

Для мережі класу В.

Максимальна кількість вузлів - **65536**. Для адресації **4-х** підмереж в мережевому адресу **класу В** також потрібно використовувати **2 розряди**, але

тепер вільними залишається **14 розрядів**. Таким чином, кожна з підмереж може обслуговувати **2^{14}-2 =16 382** хостів.

Число підмереж	Число хостів	Мережева маска
4	16 382	255.255.192.0 (11111111.11111111.1000000.00000000)

Приклад 4.

Розділити IP-мережу 192.168.0.0 з маскою 255.255.255.0 на 4 підмережі. Для підмережі вказати широкомовний адрес.

Рішення:

Мережа класу С. Загальна кількість хостів **2^8-2 =254**.

Маска 255.255.255.0 виділяє 24 старших бітів для ідентифікаї мережі і 8 бітів для ідентифікації хостів:

192.168.0.0	**11000000.10101000.00000000.**	**0000000**	адрес мережі
255.255.255.0	**11111111.11111111.11111111.**	**0000000**	маска
	Мережа (24 біти)	Хости (8 біт)	

Число 4 підмереж, має відповідати 2 станам бітів в порядку їх збільшення від 0 до четвертого стану. Тобто 4 стани 00000000, 00000001, 00000010, 00000011 відповідають кількості бітам, які будуть виділенні для ідентифікації підмереж.

Два старших біти з осласті хостів виділяємо для ідентифікації підмережі, шляхом утворенн нової маски підмережі:

192.168.0.0	**11000000.10101000.00000000.**	**00**	**000000**	адрес мережі
255.255.255.192	**11111111.11111111.11111111.**	**11**	**000000**	Маска підмережі
	Мережа (24 біти)	Підмережі (2 біт)	Хости (6 біт)	

Крок зміни адреси рівний значенню молодшого розряду підмережі, тобто 64, тобто: 0 - початок першої підмережі, 0+64=64 - початок другої підмережі, 64+64=128 - початок третьої підмережі, 128+64=192 - початок четвертої підмережі

Відповідно адреси розбито на підмережи:

192.168.0.0-192.168.63.255 - 1-ша підмережа

192.168.64.0-192.168.127.255 - 2-га підмережа
192.168.128.0-192.168.191.255 - 3-тя підмережа
192.168.192.0-192.168.255.255 - 4-та підмережа

В кожній підмережі є 256 адрес від 0 до 255, з них є доступними 254 для хостів, оскільки 0 ідентифікує підмережу:

192.168.0.0
192.168.64.0
192.168.128.0
192.168.192.0,

а 255 – широкомовну адресу:

192.168.63.255
192.168.127.255
192.168.127.255
192.168.127.255

Оскільки призначення **IP-адрес** вузлам мережі навіть при не дуже великому розмірі мережі становить для адміністратора дуже тяжку процедуру, тому відразу другим кроком в **IP адресації** розробники вирішили автоматизувати цей процес.

З цією метою був розроблений протокол **Dynamic Host Configuration Protocol (DHCP)**, який звільняє адміністратора від цих проблем, **автоматизуючи процес призначення IP-адрес** .

DHCP може підтримувати спосіб автоматичного динамічного розподілу адрес, а також більш прості способи ручного та автоматичного статичного призначення адрес. Протокол DHCP працює відповідно з моделлю клієнт-сервер .

Під час старту системи комп'ютер, що є DHCP-клієнтом, посилає в мережу широкомовний запит на отримання IP-адреси. DHCP – сервер відгукується і посилає повідомлення-відповідь, що містить IP-адресу. Передбачається, що DHCP-клієнт і DHCP-сервер знаходяться в одній IP-мережі.

При динамічному розподілі адрес DHCP-сервер видає адрес клієнту на обмежений час, воно називається часом оренди (lease duration). Це дає можливість згодом повторно використовувати цей IP-адрес для призначення іншому комп'ютеру.

Основна перевага DHCP - автоматизація рутинної роботи адміністратора по конфігурації стека TCP/IP на кожному комп'ютері . Іноді динамічне поділ адрес дозволяє будувати IP-мережу , кількість вузлів якої перевищує кількість наявних у розпорядженні адміністратора IP-адрес .

У ручній процедурі призначення статичних адрес активну участь приймає адміністратор, який надає DHCP – серверу інформацію про відповідність IP-адрес фізичним адресами або іншим ідентифікаторів клієнтів. DHCP-сервер, користуючись цією інформацією, завжди видає певному клієнту призначений адміністратором адресу.

При автоматичному статичному способі DHCP-сервер присвоює IP-адреса з пулу наявних IP-адрес без втручання оператора. А межі пулу призначаючих адрес задає адміністратор при конфігуруванні DHCP-сервера.

Адреса дається клієнту з пулу в постійне користування, тобто з необмеженим терміном оренди. Між ідентифікатором клієнта і його IP-адресою і раніше, як і при ручному, існує постійна відповідність. Вона встановлюється в момент першого призначення DHCP-сервером IP-адреси клієнта. При всіх наступних запитах сервер повертає той же самий IP-адресу.

DHCP забезпечує надійний і простий спосіб конфігурації мережі TCP/IP, гарантуючи відсутність дублювання адрес за рахунок централізованого управління їх розподілом.

Адміністратору в цьому випадку залишається тільки управляти процесом призначення адрес за допомогою параметра "тривалість оренди", яка визначає, як довго комп'ютер може використовувати призначений IP-адрес, перед тим як знову запросити його від DHCP-сервера в оренду.

4.6 Завдання на лабораторну роботу

1) IP-адреса 190.235.130.N, мережева маска 255.255.192.0. Визначте, адресу мережі і адресу вузла.

2) Визначте маски підмережі для випадку розбиття мережі з номером N.0.0.0 на 32 підмережі .

3) Існує єдина корпоративна мережа, кількість вузлів мережі - 50450. Цією мережею виділений адрес для виходу в Internet N.124.0.0 . Ви вирішили не вимагати від провайдера додаткових адрес і організувати 8 філій у цій мережі. Питання:

- Яка максимальна кількість вузлів може бути в кожному з філій? Обчисліть мережеві маски і можливий діапазон адрес хостів для кожного з філій.

4) Ви є адміністратором корпоративної мережі з 6 підмереж, в кожній підмережі по 25 комп'ютерів. Необхідно використовуючи один номер мережі класу C 192.168.10.0, визначити чи правильно обраний розмір підмережі, і призначити маски і можливі IP-адреси хостам мережі.

5) Розділити IP-мережу на підмережі відповідно до варіанта з таблиці 4.4. Для кожної підмережі вказати широкомовний адрес.

Таблиця 4.4 – Завдання для лабораторної 4

Варіант	Мережа	Підмережі
1.	192.168.16.0/24	5 підмереж з 100, 20, 10, 6 і 40 вузлами
2.	194.45.27.0/24	5 підмереж з 34, 20, 62,10 і 40 вузлами
3.	56.1.1.0/16	4 підмережі з 65, 22, 10 і 30 вузлами
4.	147.168.0.0/16	5 підмереж з 56, 16, 10 і 70 вузлами
5.	193.68.61.0/24	5 підмереж з 100, 20, 10 і 40 вузлами
6.	192.100.0.0/24	4 підмережі з 80, 20, 12 і 20 вузлами

7.	195.18.11.0/24	4 підмережі з 110, 11, 10 і 40 вузлами
8.	207.15.0.0/24	4 підмережі з 28, 80, 10 і 40 вузлами
9.	222.11.0.0/24	4 підмережі з 110, 20, 10 і 50 вузлами
10.	200.2.2.0/24	4 підмережі з 100, 20, 10 і 40 вузлами
11.	201.111.32.0/16	5 підмереж з 170, 590, 1500, 800 і 254 вузлами
12.	128.200.1.0/16	5 підмереж з 115, 300, 200, 128 і 420 вузлами
13.	53.11.0.0/16	5 підмереж з 165, 222, 128, 110 і 430 вузлами
14.	146.77.0.0/16	5 підмереж з 550, 116, 200, 256 і 170 вузлами
15.	194.54.45.0/24	4 підмережі з 103, 39, 10 і 16 вузлами
16.	142.51.0.0/16	4 підмережі з 180, 120, 12 і 30 вузлами
17.	43.0.0.0/16	4 підмережі з 151, 211, 16 і 70 вузлами

Контрольні запитання

1. Які бувають класи IP - адрес.
2. Як по першому байту адреси визначити його клас?
3. Що таке маска, на що вона вказує?
4. Для чого потрібні маски змінної довжини?
5. Викладіть алгоритм розподілу мереж на підмережі за допомогою VLM (variable length mask).

Лабораторна робота №5
Симуляція роботи комп’ютерної мережі в Cisco Packet Tracer

Мета роботи: вивчення програми для симуляції комп’ютерних мереж із застосуванням додатку Cisco Packet Tracer

ТЕОРЕТИЧНІ ВІДОМОСТІ

Cisco Packet Tracer - це емулятор мережі, створений компанією Cisco .

Цей додаток дозволяє будувати мережі на різноманітному обладнанні в довільних топологіях з підтримкою різних протоколів.

Програмне рішення Cisco Packet Tracer дозволяє імітувати роботу різних мережевих пристроїв: маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп'ютерів, мережевих принтерів, IP-телефонів і т.д. Робота з інтерактивним симулятором дає відчуття налаштування реальної мережі, що складається з десятків або навіть сотень пристроїв.

Устаткування, у свою чергу, залежать від характеру пристроїв: одні можна налаштувати за допомогою команд операційної системи Cisco IOS, інші - за рахунок графічного веб-інтерфейсу, треті - через командний рядок операційної системи або графічні меню.

Завдяки такій властивості Cisco Packet Tracer, як режим візуалізації, користувач може відстежити переміщення даних по мережі, появу і зміну параметрів IP-пакетів при проходженні даних через мережеві пристрої, швидкість і шляхи переміщення IP-пакетів. Аналіз подій, що відбуваються в мережі, дозволяє зрозуміти механізм її роботи і виявити несправності.

Cisco Packet Tracer може бути використаний не тільки як симулятор, але і як мережевий додаток для симулювання віртуальної мережі через реальну мережу, в тому числі Інтернет. Користувачі різних комп'ютерів, незалежно від їх місця розташування, можуть працювати над однією мережевий топологією, виробляючи її настройку або усуваючи проблеми. Ця функція багато режиму Cisco Packet Tracer може застосовується для організації командної роботи.

В Cisco Packet Tracer користувач може симулювати побудова не тільки логічною, але й фізичної моделі мережі і, отже, отримувати навички проектування. Схему мережі можна накласти на креслення реально існуючої будівлі або навіть міста і спроектувати всю його кабельну проводку, розмістити пристрої в тих чи інших будівлях і приміщеннях з урахуванням фізичних обмежень, таких як довжина і тип прокладається кабелю або радіус зони покриття бездротової мережі.

Симуляція, візуалізація, багатокористувацький режим і можливість проектування роблять Cisco Packet Tracer унікальним інструментом для навчання мережевим технологіям.

5.1 Головне вікно Cisco Packet Tracer

На рис.5.1 зображено інтерфейс програми, який розділено на області.

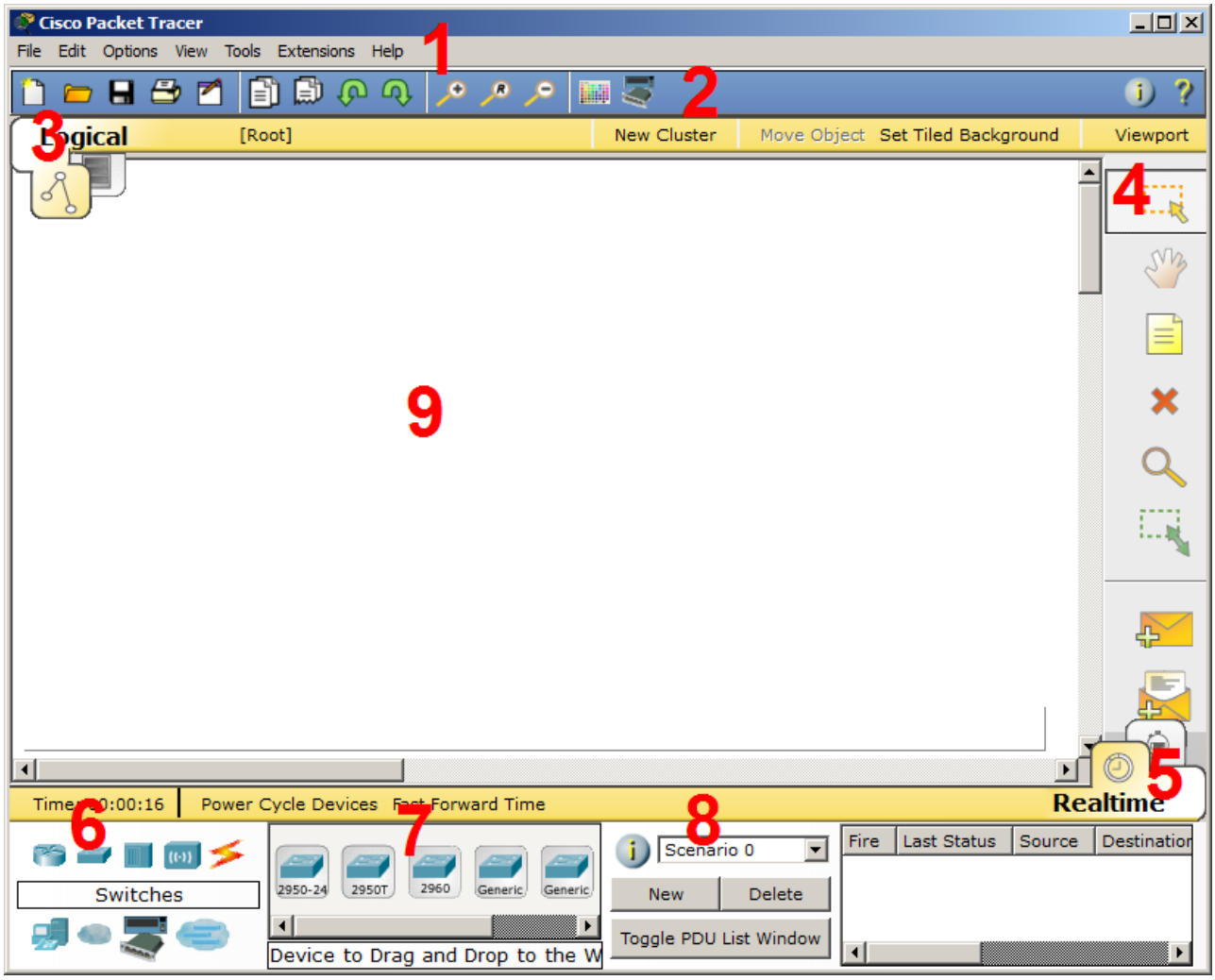


Рисунок 5.1 – Інтерфейс програми Cisco Packet Tracer

1. Головне меню програми зі наступним вмістом:
   - 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 - кольорова палітра і кастомізація кінцевих пристроїв;
   - Розширення - майстер проектів, багатокористувацький режим і кілька функцій, які з CPT (так я іноді буду ласкаво називати Cisco Packet Tracer) можуть зробити цілу лабораторію;
   - Допомога – в допомогу користувачу
2. Панель інструментів, частина яких просто дублює пункти меню;
3. Перемикач між логічної і фізичної організацією;
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 (Simulation);

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 користувальницьких сценаріїв;

9. Робочий простір.

Приклад розміщення колірних областей (рис.5.2), що дозволяє наприклад відокремлювати візуально одну підмережу від іншої.

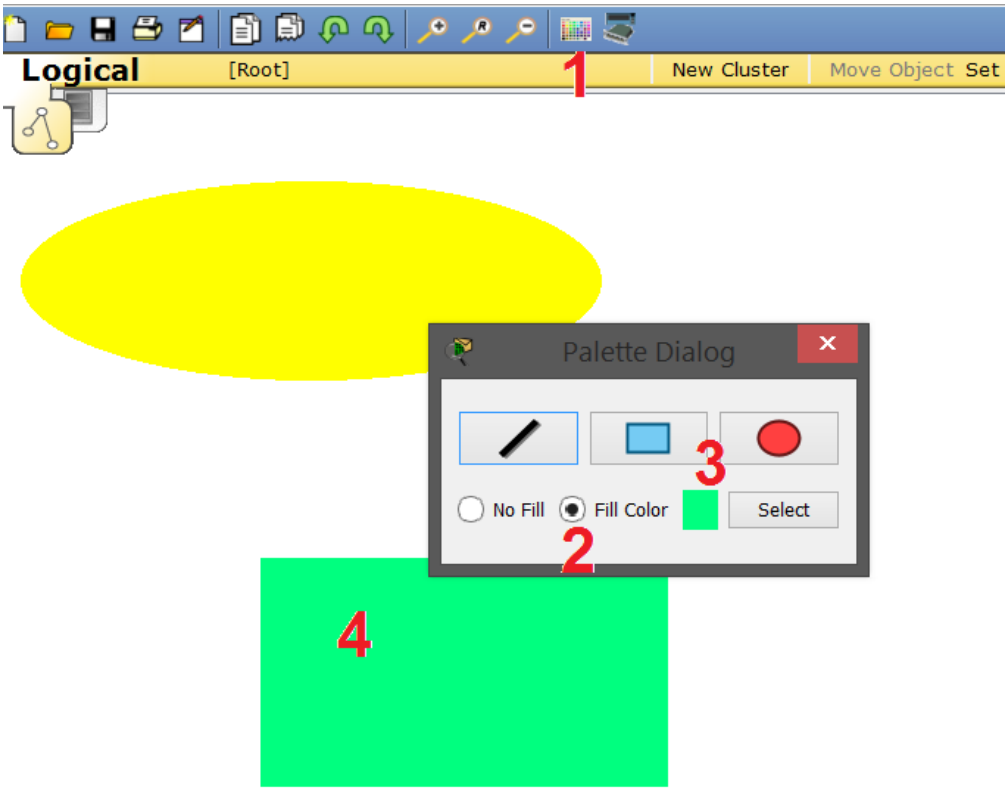


Рисунок 5.2 – Приклад розміщення колірних областей

Для установки кольорових областей виконаєте 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.

5.2 Обладнання і лінії зв’язку в Cisco Packet Tracer

5.2.1 Маршрутизатори

Маршрутизатори використовується для пошуку оптимального маршруту передачі даних на підставі спеціальних алгоритмів маршрутизації, наприклад вибір маршруту (шляху) з найменшим числом транзитних вузлів (табл.5.1).

Таблиця 5.1 – Умовні та реальні позначення маршрутизаторів

Умовне позначення	Реальне зображення обладнання
	
	
	
	

Працюють на мережному рівні моделі OSI (Лекція №4).

5.2.2 Комутатори

Комутатори - це пристрої, що працюють на канальному рівні моделі OSI і призначені для об'єднання декількох вузлів в межах одного або декількох сегментах мережі (табл.5.2). Передає пакети комутатор на підставі внутрішньої таблиці - таблиці комутації, отже трафік йде тільки на той MAC-адрес, якій він призначається, а не повторюється на всіх портах (як на концентраторі)

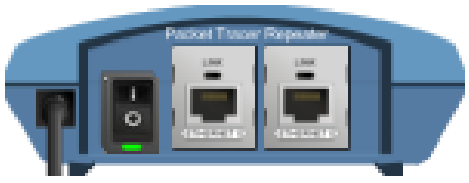
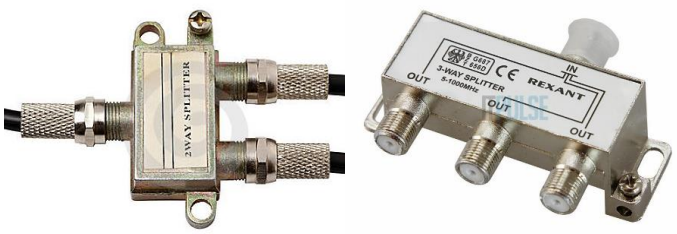
Таблиця 5.2 – Умовні та реальні позначення комутаторів

Умовне позначення	Реальне зображення обладнання
	
	
	
	

5.2.3 Концентратори

Концентратор (hub) повторює пакет, прийнятий на одному порту на всіх інших портах (табл.5.3).

Таблиця 5.3 – Умовні та реальні позначення концентраторів

Умовне позначення	Реальне зображення обладнання
 Загальний 1 (6 портів)	
 Загальний 2 (2 порти)	
	

5.2.4 Бездротові пристрої

Бездротові технології Wi-Fi і мережі на їх основі. Включає в себе точки доступу (табл.5.4).

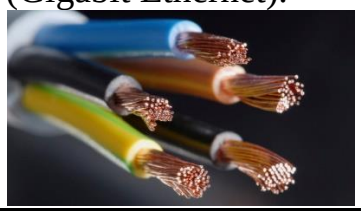
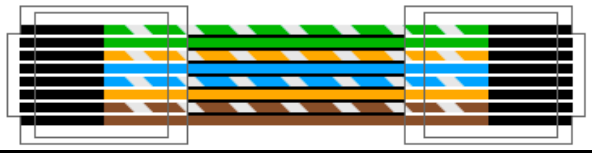
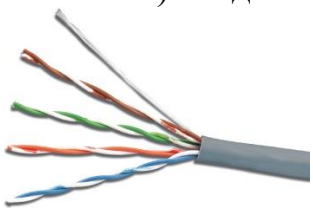
Таблиця 5.4 – Умовні та реальні позначення бездротових пристроїв

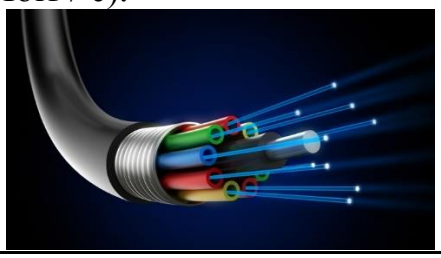
Умовне позначення	Реальне зображення обладнання
	
 Загальні	 Cisco Hardened 819  Cisco 1941W-E/K9

5.2.5 Лінії зв’язку

За допомогою цих компонентів створюються з'єднання вузлів в єдину схему. Packet Tracer підтримує широкий діапазон мережевих з'єднань (див. табл. 5.5). Кожен тип кабелю може бути з'єднаний лише з певними типами інтерфейсів.

Таблиця 5.5 – Типи кабелів

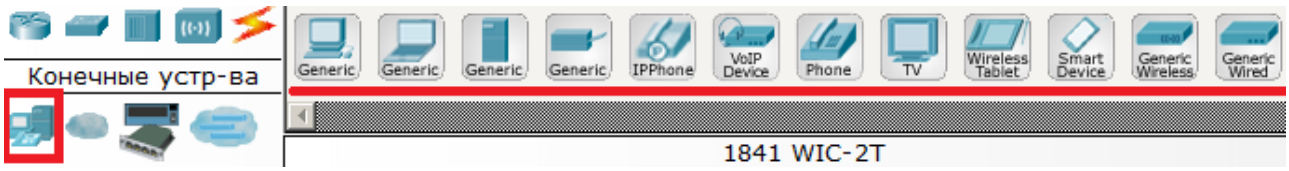
Тип кабелю	Опис
1	**2**
Консоль 	Консольне з'єднання може бути виконано між ПК і маршрутизаторами або комутаторами. Повинні бути виконані деякі вимоги для роботи консольного сеансу з ПК: швидкість з'єднання з обох сторін повинна бути однакова, має бути 7 біт даних (або 8 біт) для обох сторін, контроль парності має 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.  DB9-RJ45 (Com/Lpt порт-Ethernet)
Мідний прямий 	Цей тип кабелю є стандартною 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 кросовер 	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)  

1	2
Оптика 	Оптоволоконна середовище використовується для з'єднання між оптичними портами (100 Мбіт / с або 1000 Мбіт / с).  
Телефонний 	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), додзвонюєтеся в мережеву хмару. 
Коаксільний 	Коаксіальна середовище використовується для з'єднання між коаксіальними портами, такі як кабельний модем, з'єднаний з хмарою Packet Tracer. 

Продовження таблиці 5.5

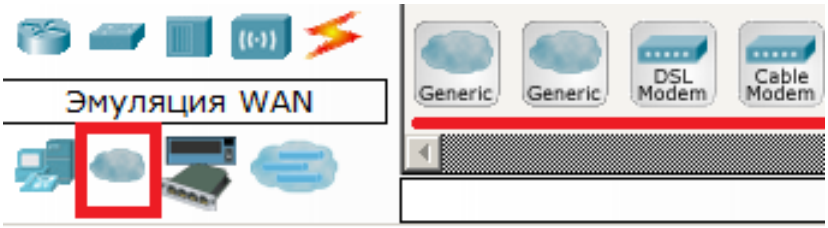
1	2
Серійний DCE  Серійний DTE 	З'єднання через послідовні порти, часто використовуються для зв'язків WAN. Для настройки таких з'єднань необхідно встановити синхронізацію на стороні DCE-пристрої. Синхронізація DTE виконується за вибором. Бік DCE можна визначити по маленькій іконі "годин" поруч з портом. 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. 

5.2.6 Кінцеві пристрої



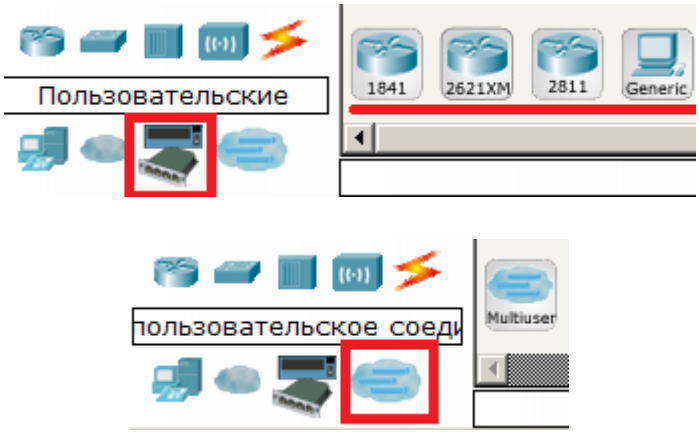
Тут представлені кінцеві вузли, хости, сервера, принтери, телефони і т.д.

5.2.7 Емуляції Інтернету



Приклад емуляція глобальної мережі. Модем DSL, "хмара" і т.д.

5.2.8 Пристрої користувача та хмара для багатокористувацької роботи



Пристрою можна комплектувати самостійно. Можна створювати довільні підключення.

5.3 Фізична комплектація обладнання

Встановіть в робочому полі роутер Cisco 1841  (рис.5.3), реальне зображення кого зображено на рис.5.4.

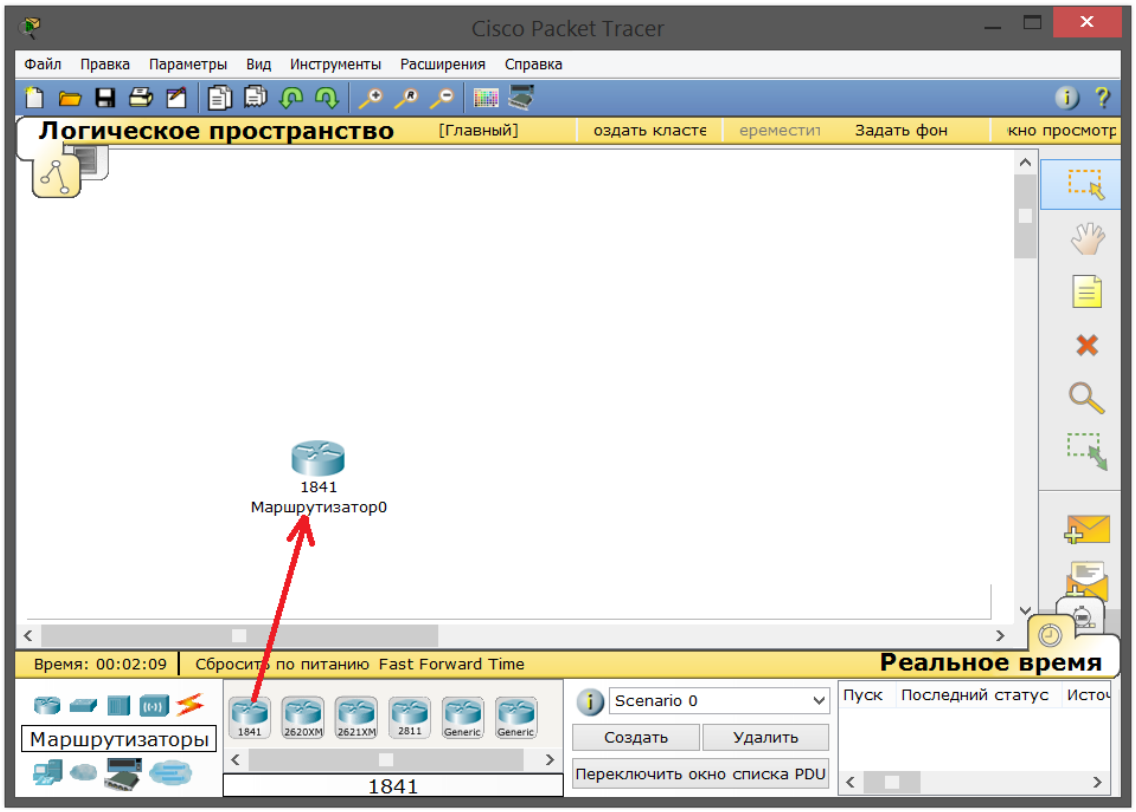


Рис.5.3. Встановлення роутера Cisco 1841 на робочий простір

Рис.5.4. Реальне зображення роутер Cisco 184

У налаштуваннях роутера відкриваємо його **фізичну конфігурацію** (рис.5.5).

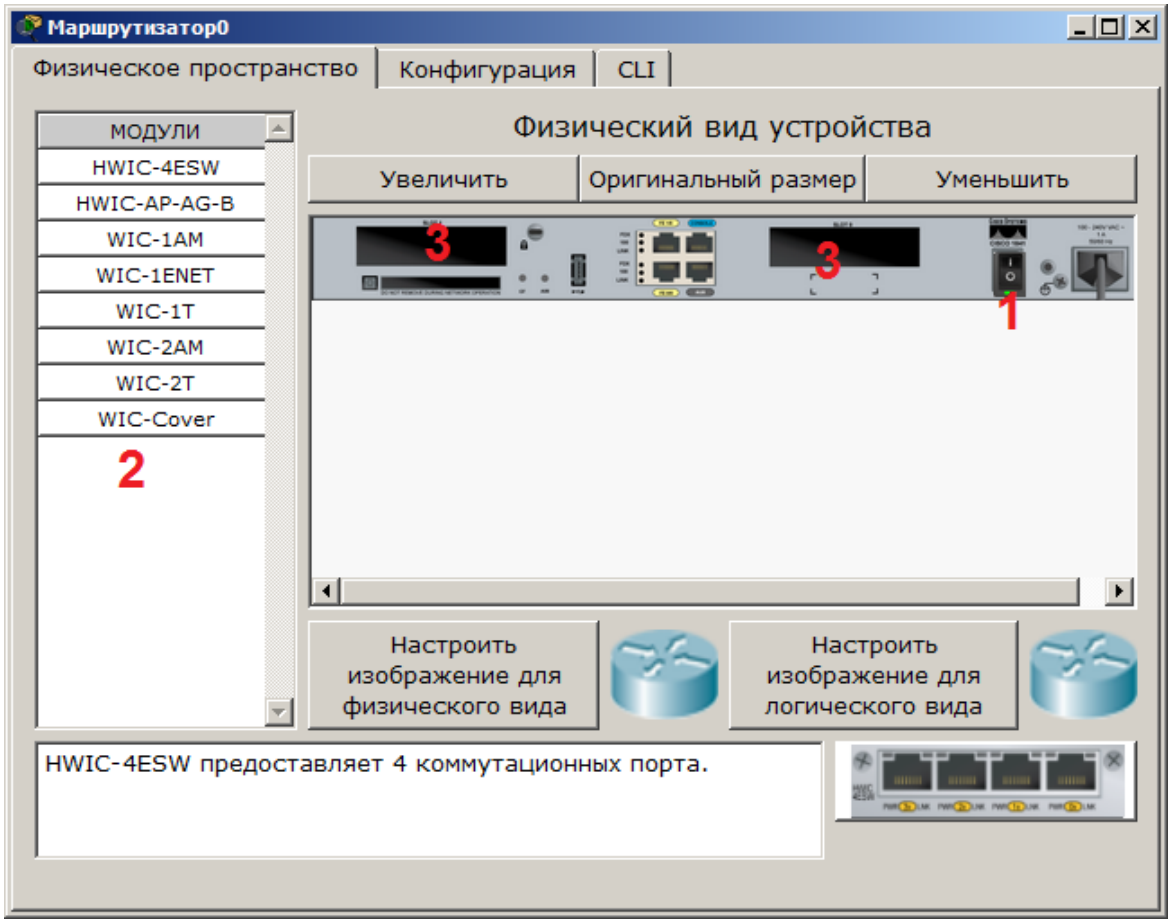


Рисунок 5.5 – Фізична конфігурація пристрою

Зліва розташований список модулів (цифра 2), якими можна укомплектувати роутер. Зараз у ньому 2 порожніх місця (цифра 3), в які можна встановити ці модулі при при вимкненому живленні (цифра 1).

Модулі WIC (HWIC, VWIC) - це плати розширення, що збільшують функціонал пристрою:

1. **WIC** - WAN interface card. The first original models (рис.5.6)

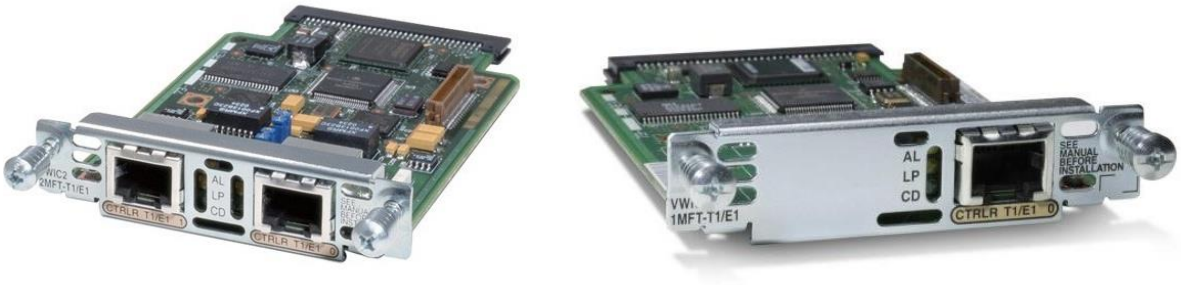


Рисунок 5.6 – Приклади WAN інтерфейсних карт (**WIC)**

2. **HWIC** - high-speed WAN interface card- the evolution of wic that is now in use on the ISR routers (рис.5.7)

Рисунок 5.7 – Приклади високо-швидкісних WAN інтерфейсних карт (**WHIC)**

3. **VIC** - voice interface card, support voice only (рис.5.8)

Рисунок 5.8 – Приклади високо-швидкісних WAN інтерфейсних карт (**WHIC)**

4. VIC2 - мережевий модуль з голосовим/факс інтерфейсом (рис.5.9)

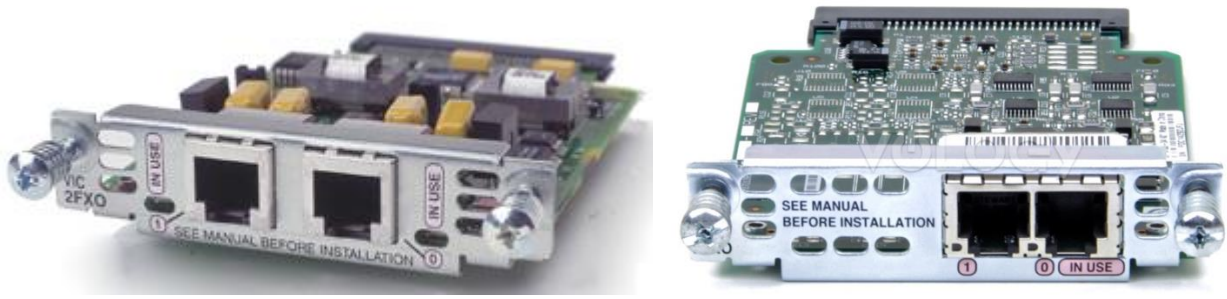


Рисунок 5.9 – Приклади мережевих модулів з голосовим/факс інтерфейсом (VIC2**)**

5. VWIC – мережевий модуль, який підтримує функцію голосового трафіку і передачу даних (рис.5.10)

Рисунок 5.10 – Приклади інтерфейсних карт, які підтримують функцію голосового трафіку і передачу даних,

6. VWIC2 – мережевий модуль 2-го покоління, який підтримує функцію голосового трафіку і передачу даних (рис.5.11)

Рисунок 5.11 – Приклади інтерфейсних карт 2-го покоління, які підтримують функцію голосового трафіку і передачу даних

Наприклад для комп'ютера є плати, що підключаються до PCI-шині (TV-тюнери, звукові карти, USB-розгалужувачі, мережеві карти), так і тут. Взагалі, пристрій Cisco - це той же системний блок зі своєю операційною системою і багатьма мережевими картами, який може працювати тільки з мережею.

Нижче представлена інформація про кожному модулі:

- **HWIC - 4ESW** - високопродуктивний модуль з 4-ма комутаційними портами Ethernet під роз'єм RJ-45. Дозволяє поєднувати в маршрутизаторе можливості комутатора.

- **HWIC-AP-AG-B** - це високошвидкісна WAN- карта, забезпечує функціонал вбудованої точки доступу для роутерів лінійки Cisco 1800 (модульних), Cisco 2800 і Cisco 3800. Даний модуль підтримує радіоканали Single Band 802.11b / g або Dual Band 802.11a / b / g.
- **WIC-1AM** включає в себе два роз'єму RJ-11 (телефонний апарат), використовуваних для підключення до базової телефонної службі. Карта використовує один порт для з'єднання з телефонної лінією, інший може бути підключений до аналоговому телефону для дзвінків під час простою модему.
- **WIC-1ENET** - це однопортова 10 Мб / с Ethernet карта для 10BASE-T Ethernet LAN.
- **WIC-1T** надає однопортове послідовне підключення до віддалених офісів або застарілих серійних мережевих пристроїв, наприклад SDLC концентраторам, системам сигналізації і пристроям packet over SONET (POS).
- **WIC-2AM** містить два роз'єму RJ-11, що використовуються для підключення до базової телефонної службі. В WIC-2AM два модемних порти, що дозволяють використовувати обидва канали для одночасного з'єднання.
- **WIC-2T** - 2-портовий синхронний/асинхронний серійний мережевий модуль, який надає гнучку підтримку багатьох протоколів з індивідуальними налаштуваннями кожного порту в синхронний або асинхронний режим. Застосування для синхронної/асинхронної підтримки представляють:
    - низькошвидкісну агрегацію (до 128 Кб / с);
    - підтримку dial-up модемів;
    - синхронні або асинхронні з'єднання з портами управління іншого обладнання та передачу застарілих протоколів типу Bi-sync і SDLC.
- **WIC-Cover** - стінка для WIC слота, необхідна для захисту електронних компонентів і для поліпшення циркуляції охолоджуючого повітряного потоку.

Для зміни комплектації устаткування необхідно:

– відключити живлення , натиснувши мишею на кнопку живлення  ,
– перетягнути мишею модуль HWIC-**4ESW** у вільний слот і включити живлення  .
– почекати закінчення завантаження роутера.

У конфігурації GUI можемо побачити 4 нових інтерфейси (рис.5.12).

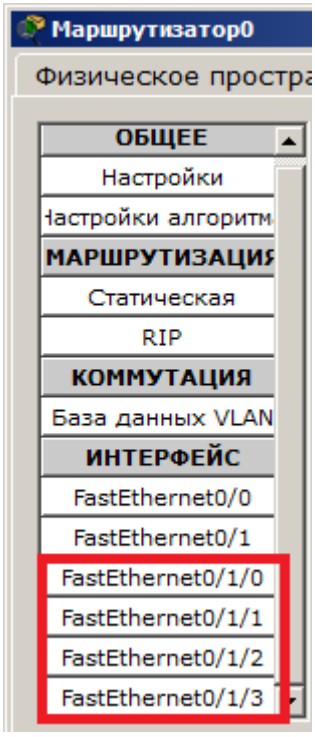


Рисунок 5.12 – Конфігурація інтерфейсів пристрою.

Решта пристроїв комплектуються аналогічно. Додаються нові модулі Ethernet (10/100/1000), оптоволоконні роз'єми декількох типів, адаптери бездротової мережі. На робочий комп'ютер є можливість додати наприклад мікрофон з навушниками, жорсткий диск для зберігання даних.

ЕКСПЕРИМЕНТАЛЬНА ЧАТИНА

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 буде реагувати мережу в разі збоїв або наприклад що станеться, якщо від'єднати який або кабель або відключити живлення одного з мережевих пристроїв.

Режим симуляції дозволяє простежити структуру пакету і переглянути, з якими параметрами пакет проходить по рівням моделі OSI.

Складіть комп’ютерну мережу: 4 вузли, сервер, принтер і два концентратора. Концентратори між собою з'єднуються кроссоверним кабелем (рис.5.13).

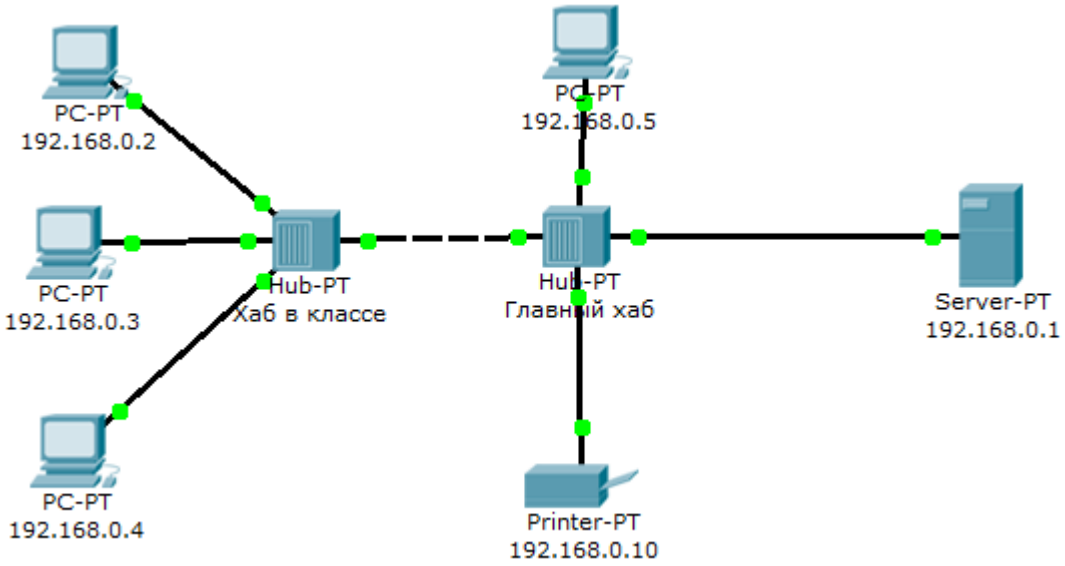


Рисунок 5.13 – Схема комп’ютерної мережі

Опишемо процедуру складання схеми комп’ютерної мережі (рис.5.13).

Етапи створення:

1. Встановлення на робочу просторі необхідного мережевого обладнання (рис.5.14-5.16) (зберігати порядок встановлення обладнання не є обов’язковим);

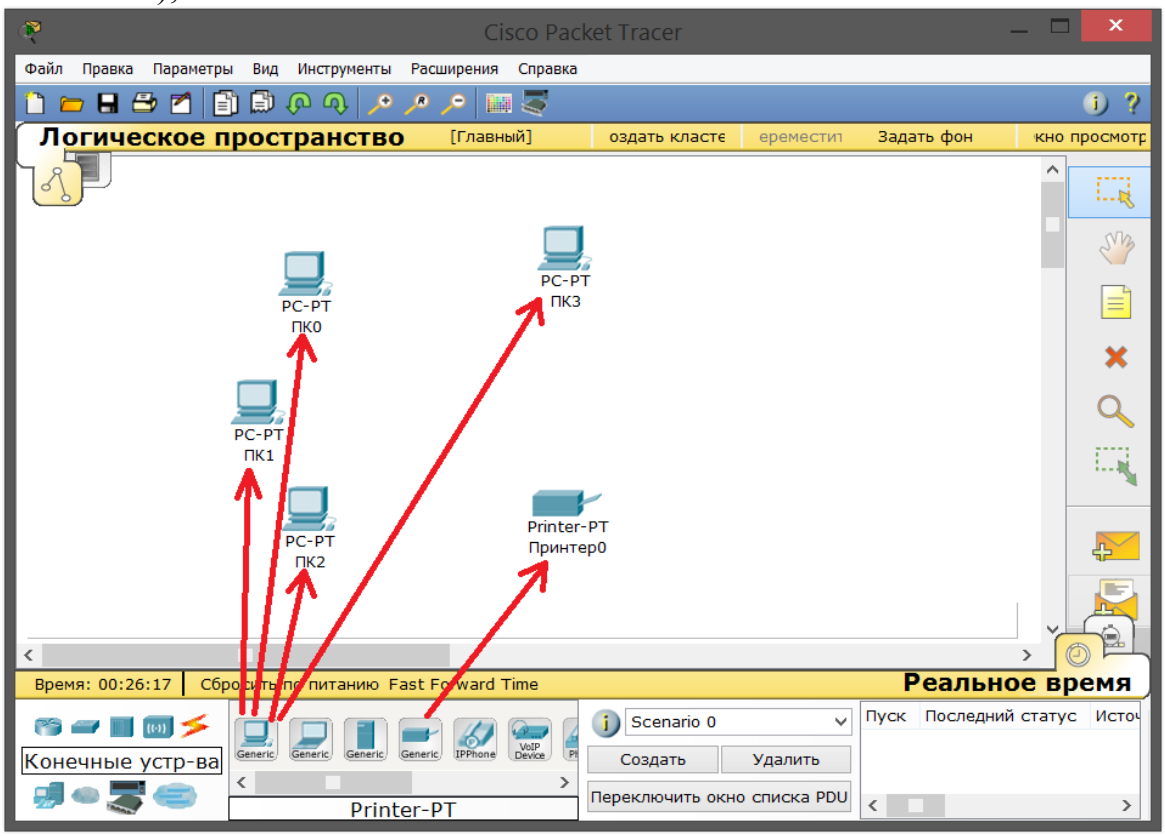


Рисунок 5.14 – Встановлення кінцевих пристроїв (персональних комп’ютерів та принтера) на робочий простір

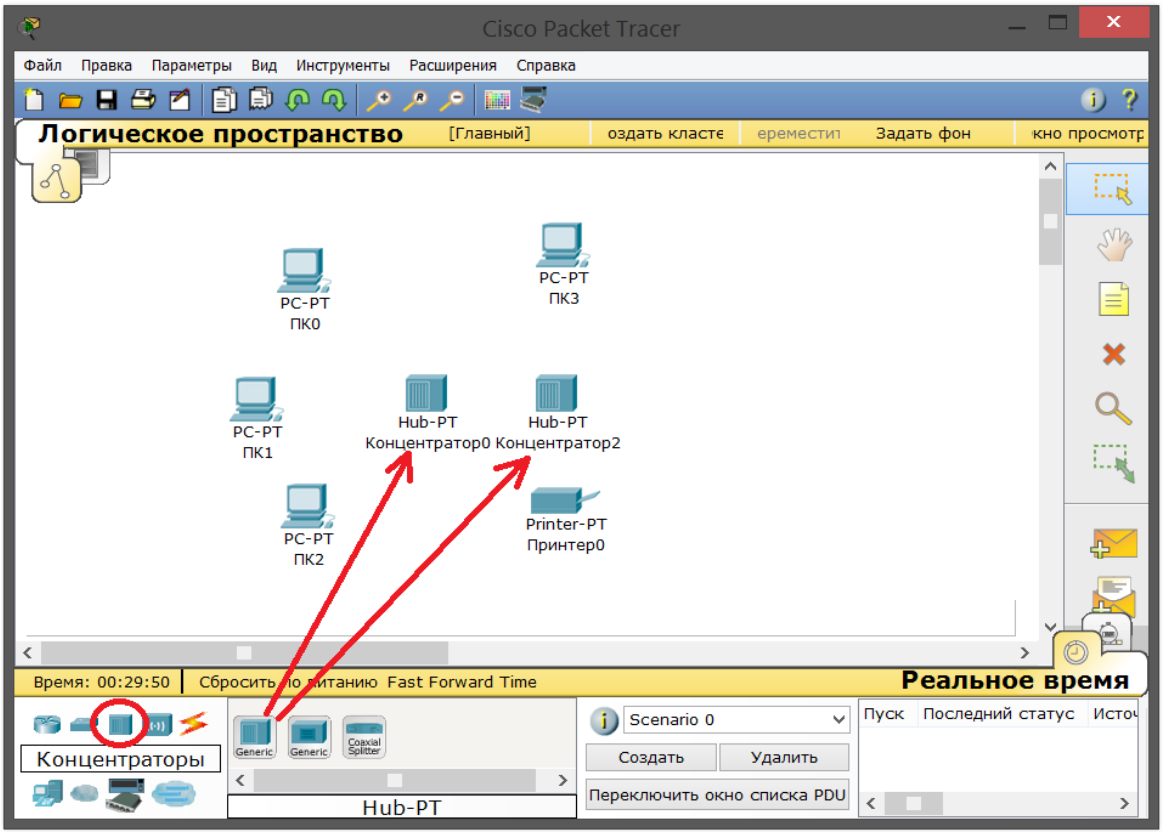


Рисунок 5.15 – Встановлення концентраторів (хабів) на робочий простір

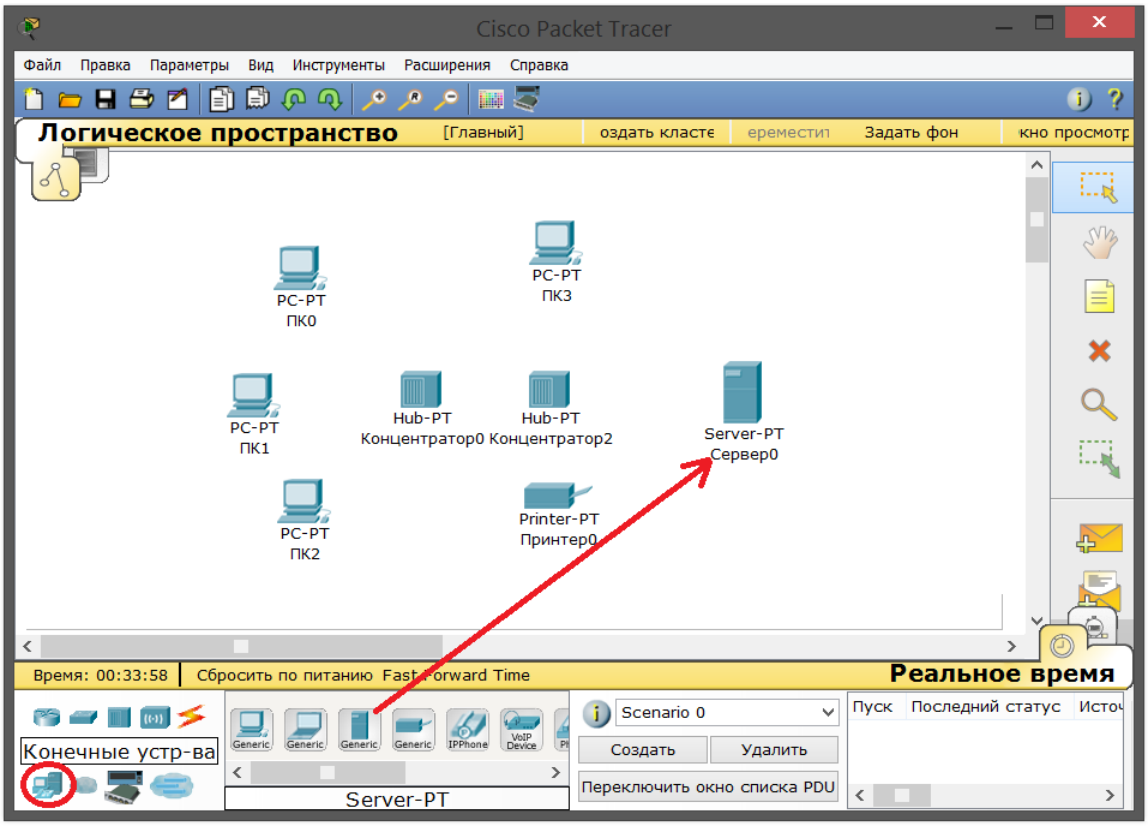


Рисунок 5.16 – Встановлення сервера на робочий простір

2. Встановлення ліній зв’язку (рис.5.17-5.19);

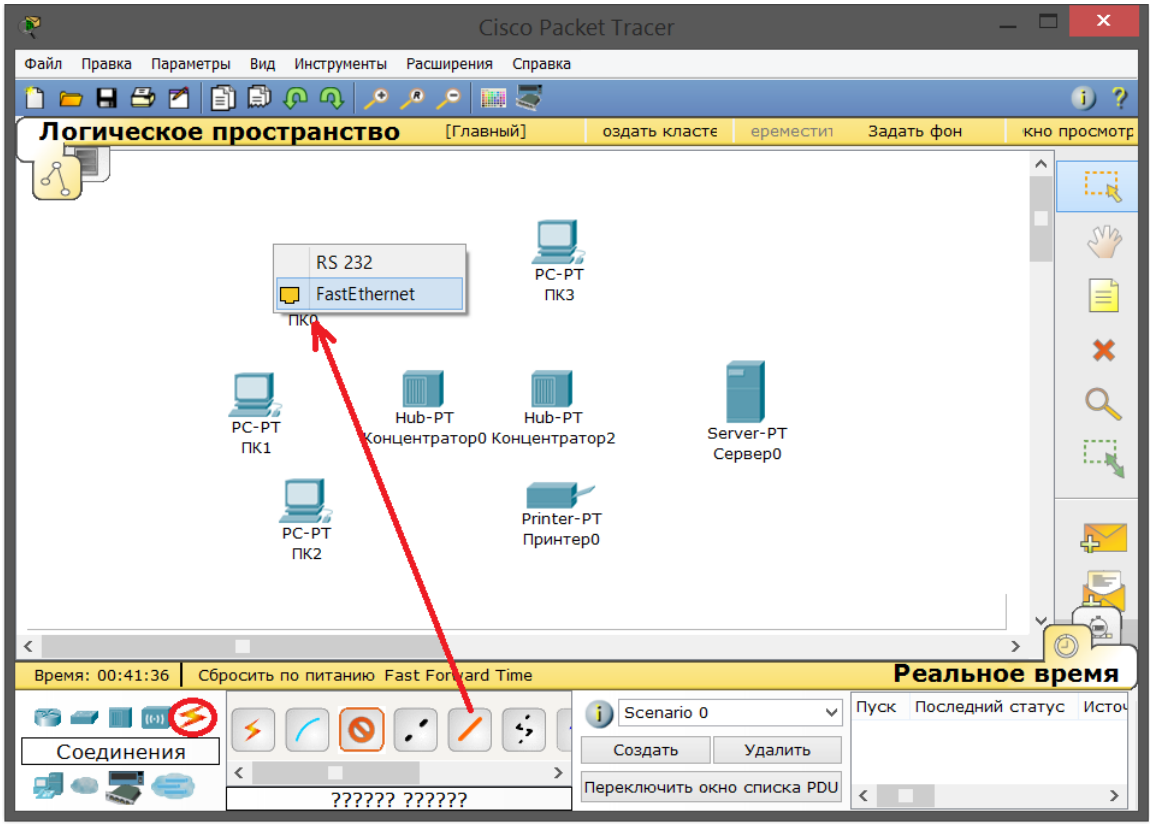


Рисунок 5.17 – Встановлення початку з’єднання виходу FastEthernet до концентратора

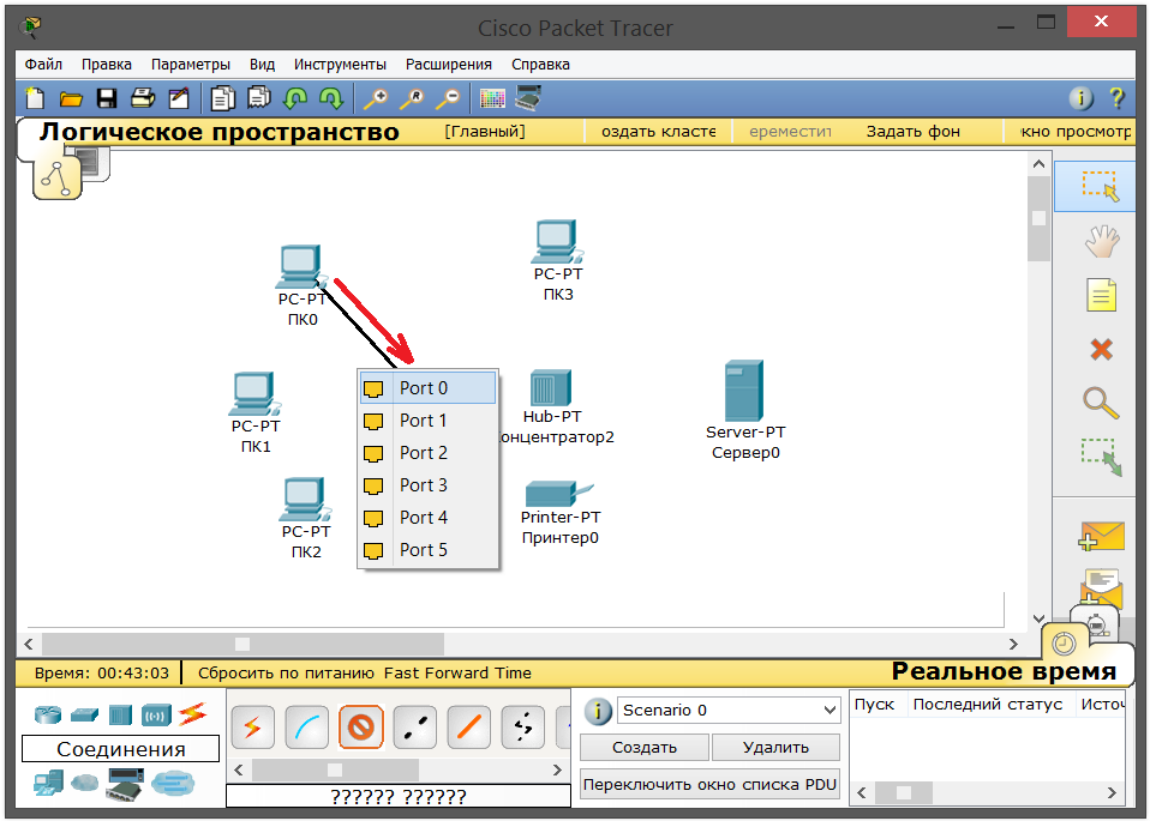


Рисунок 5.18 – З’єднання виходу FastEthernet ПК із одним із портів (Port0-Port5) концентратора

За аналогією з’єднаємо між собою ксі мережеві вузли (рис.5.19).

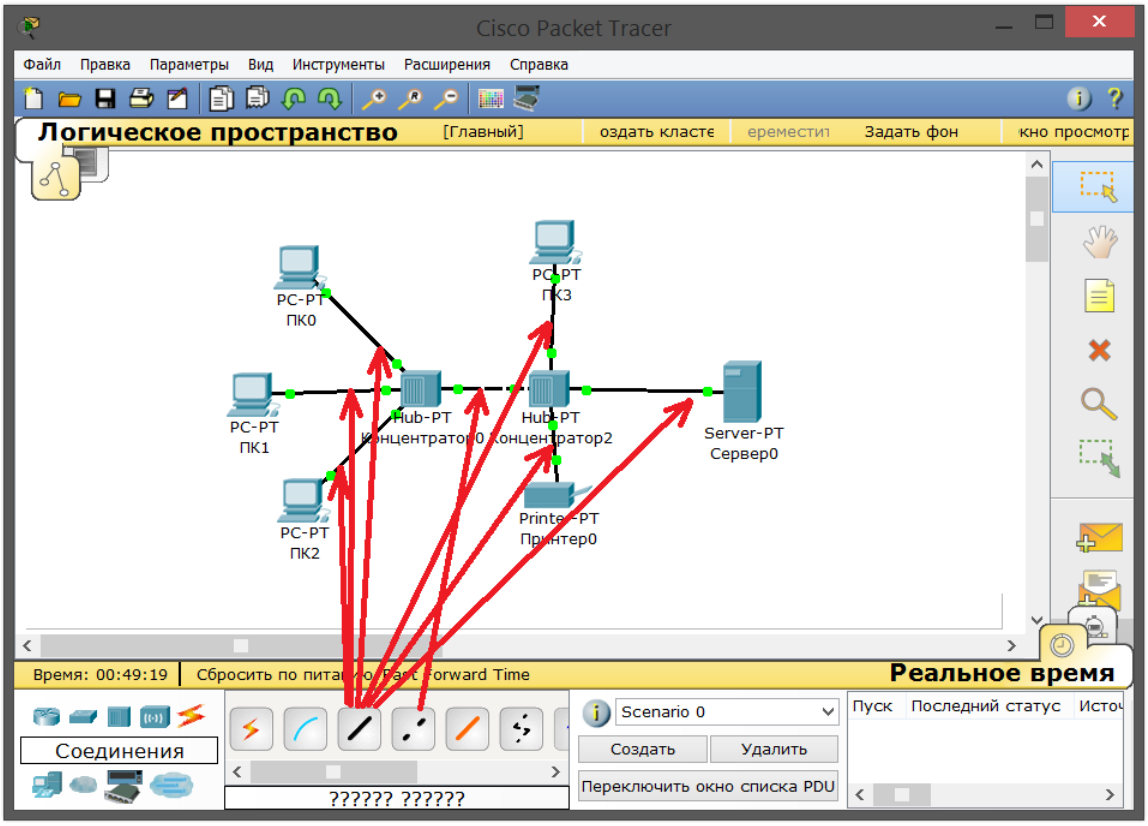
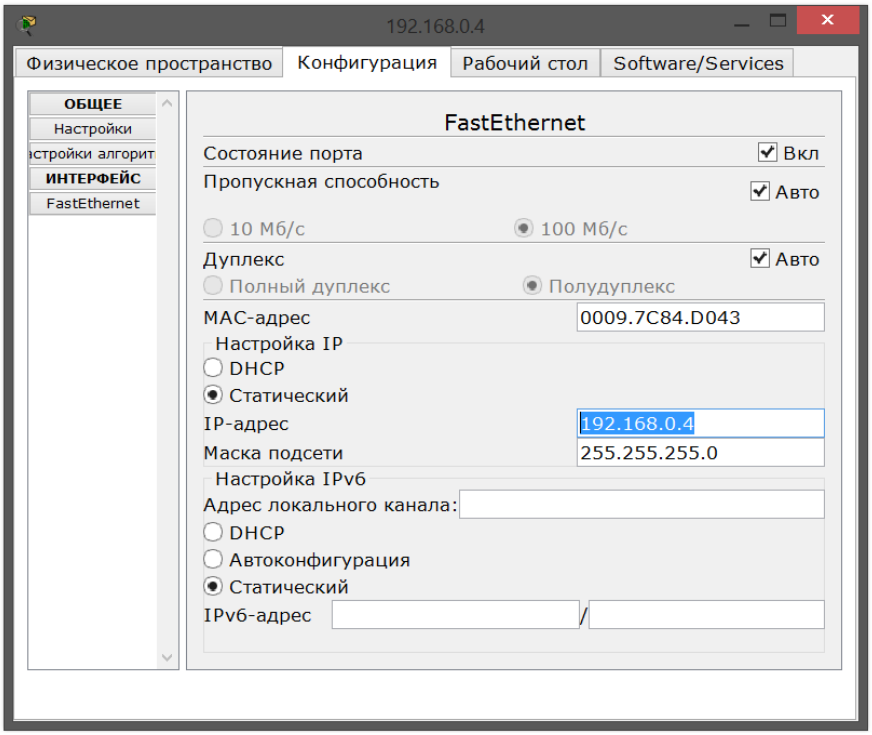


Рисунок 5.19 – Кінцева схема мережевого з’єднання

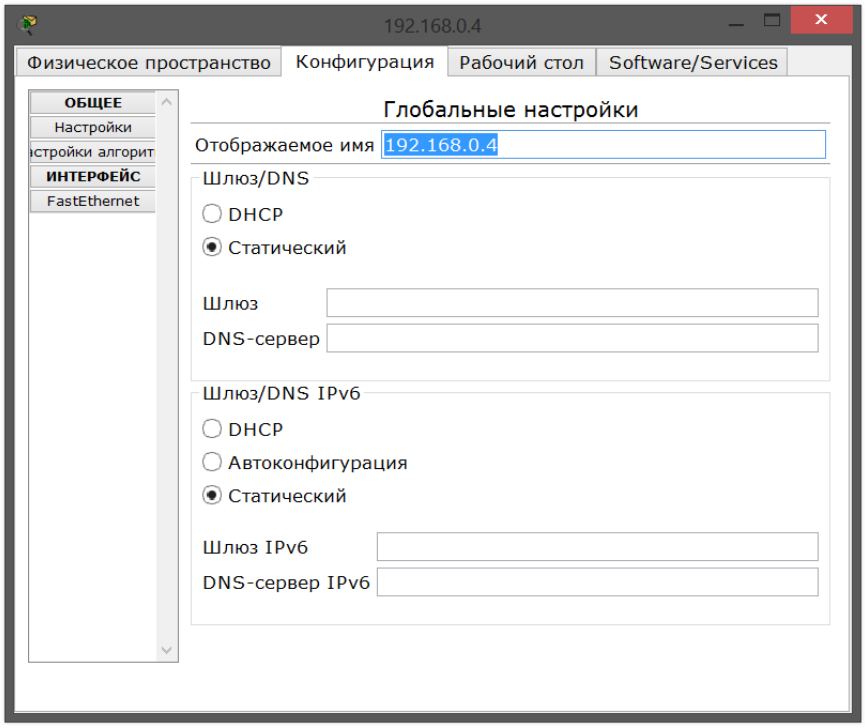
3. Налаштування обладнання (описано нижче по тексту).

Присвойте кожному із об’єктів мережі власні IP-адреси:

- зайдіть на конкретний об’єкт мережі лівою кнопкою миші;
- зайдіть в пункти Конфугурация/FasEthernet та присвойте значення статистичної IP-адреси, відповідно до рис.5.13.
-



- у пункті Конфугурация/Общие присвойте ім’я об’єкту, яке буде відображатися на робочому просторі (для зручності вказати IP-адрес).



Результат присвоєння імен та IP-адрес вузлам комп’ютерної мережі зображено на рис.5.20.

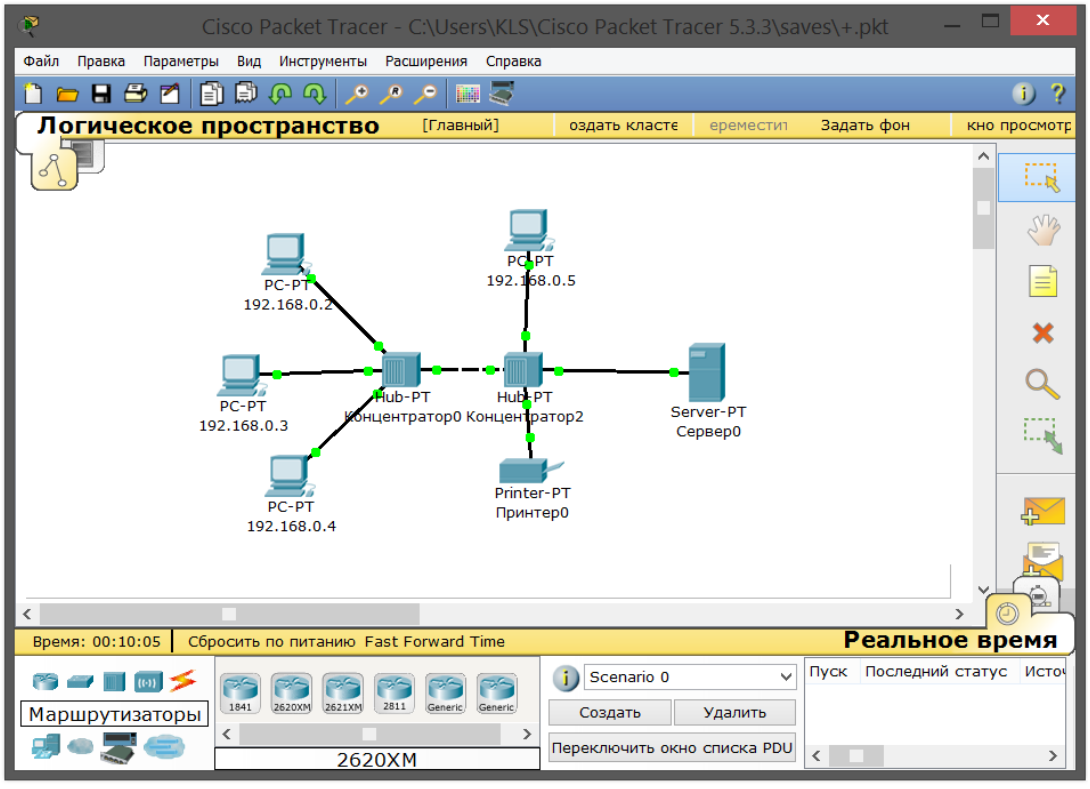
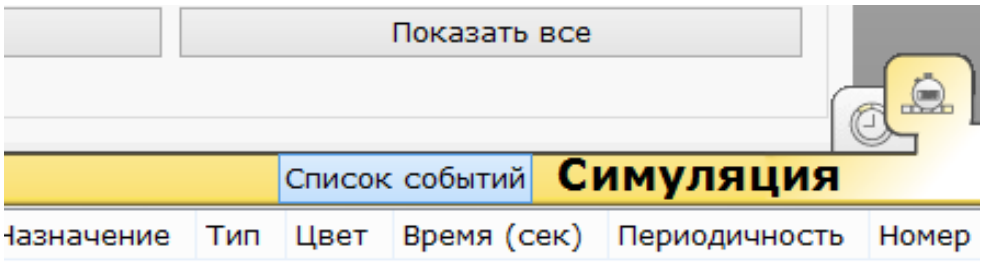


Рисунок 5.20 – Комп’ютерна мережа із присвоєними іменами та IP-адресами

Перейдіть в режим симуляції (Shift+S), або натиснувши на іконку симуляції в правому нижньому куті робочого простору.



В режимі симуляції будуть доступними вікно подій (рис.5.20), кнопка скидання (очищає список подій), управління відтворенням і фільтр протоколів та запропоновано багато протоколів, але відфільтруємо поки тільки ICMP (натиснувши на кнопку «Изменить фильтры»), це виключить випадковий трафік між вузлами.

Рисунок 5.20 – Фрейм із списком подій

Надішліть PING-запит за допомогою кнопки , яка організовує надсилання IP-пакетів від відправника до одержувача. З одного з вузлів пропінгуйте інший вузол. Виберіть далеко розташовані вузли, щоб наочніше побачити як проходитимуть пакети по мережі в режимі симуляції. Отже, увійшовши на вузол 4 і здійсніть процес пінг-запиту на вузол 5 (після натиснення кнопки виберіть спочатку відправника, а потім одержувача) (5.21).

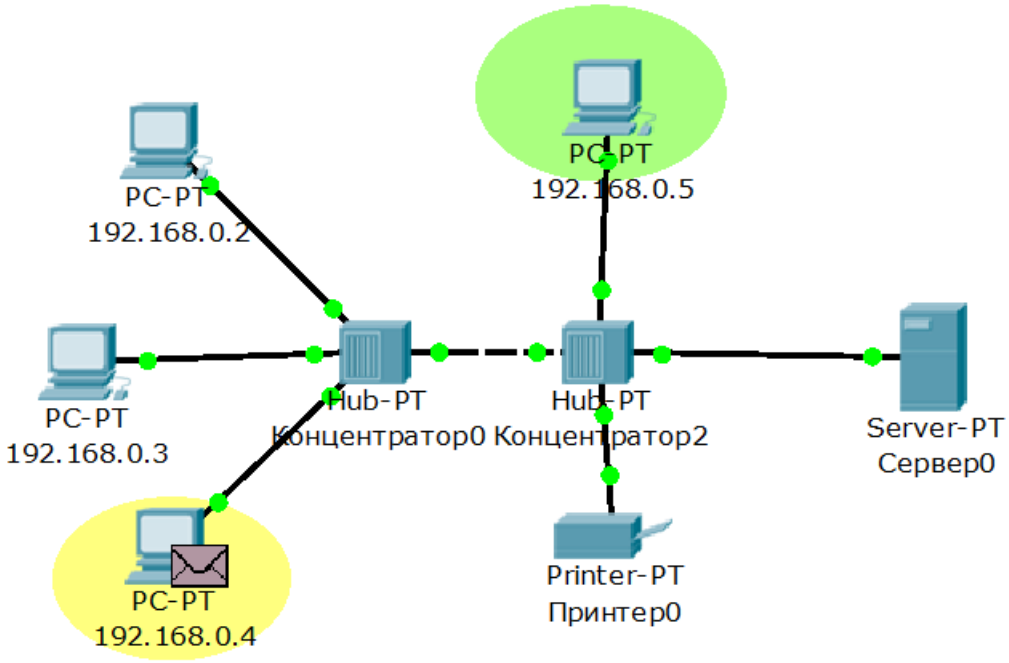


Рисунок 5.21 – Демонстрація роботи симулятора

З жовтого вузла пінгуйте зелений. В результаті пінгування на жовтому вузлі утвориться пакет очікування (конвертик). Процес запуску пакету в мережу відбувається шляхом натиснення кнопки "Захват/Вперед" у вікні симуляції (рис.5.22).

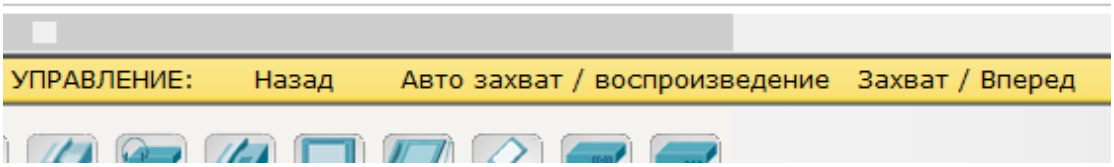


Рисунок 5.22 – Фрагмент вікна симуляції

У вікні симуляції буде відображено цей пакет, зокрема його тип (ICMP) і джерело (192.168.0.4) - рис.5.23.

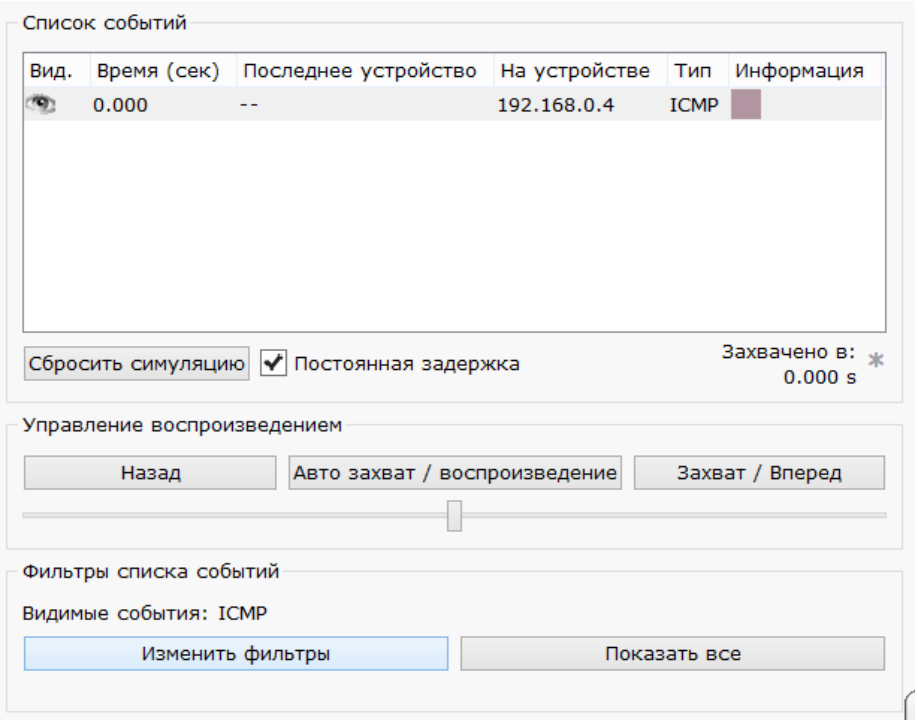


Рисунок 5.23 – Моніторинг роботи протоколів

Натиснувши кнопкою миші на пакет можна отримати докладнішу інформацію про нього. При цьому буде відображено модель OSI. Відразу видно, що на 3-му рівні (мережевий) виник пакет у вихідному напрямку, який піде до другого рівня, потім до першого, на фізичне середовище і передасться на наступний вузол (рис.5.24).

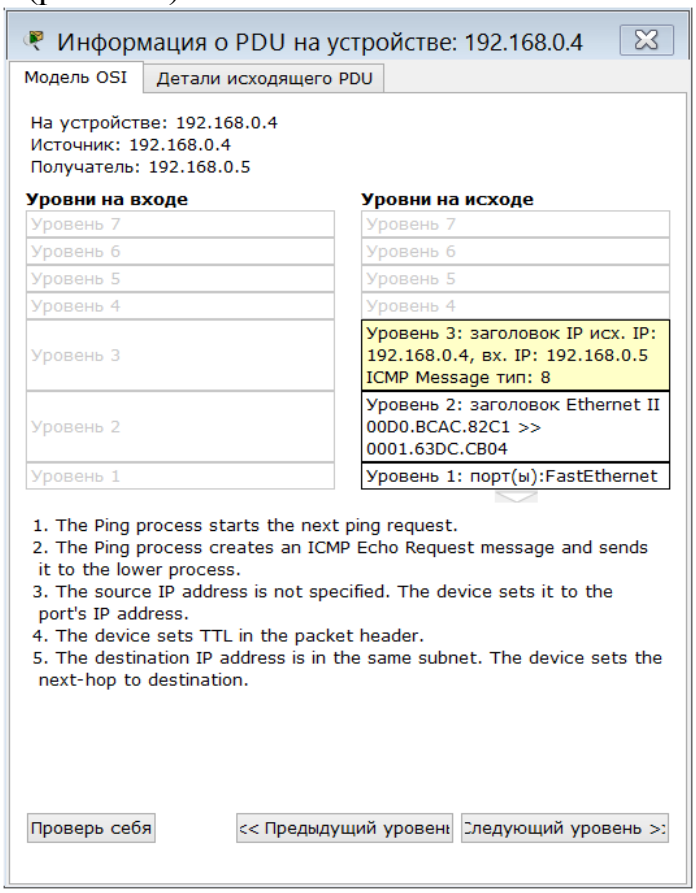


Рис.5.24 – Моніторинг роботи на моделі OSI

На вкладці «Детали исходящего PDU» можна проаналізувати структуру пакету (рис.5.25)

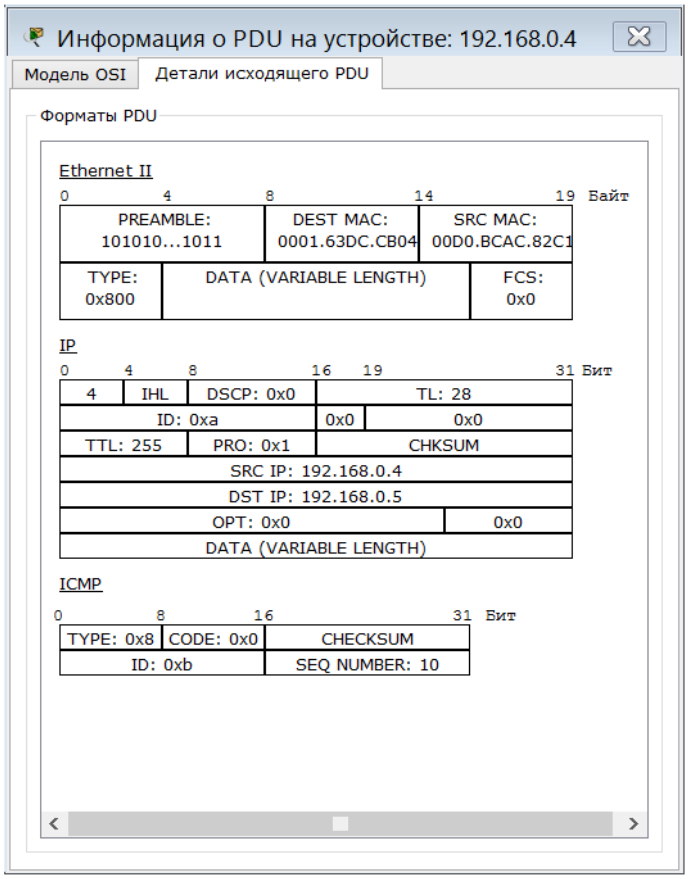


Рисунок 5.25 – Структура пакету

Після натиснення кнопку "Вперед" пакет почне рухатися до концентратора. Це єдине мережеве підключення з цього боку (5.26).

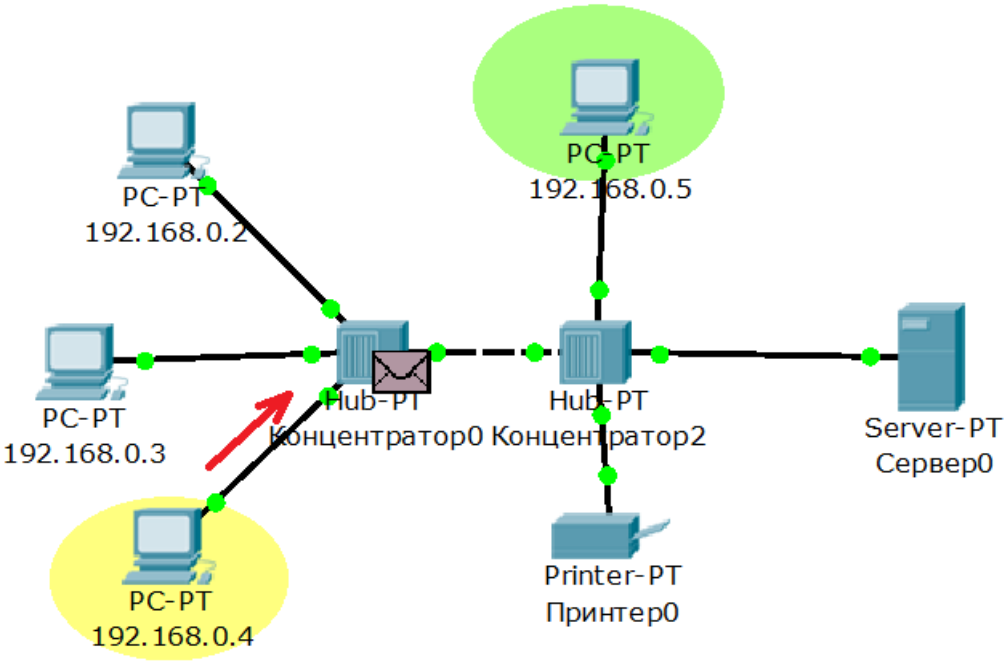


Рисунок 5.26 – Проходження пакету. Перший етап

Концентратор повторює пакет на всіх інших портах в надії, що на одному з них є адресат (отримувач пакету) (рис.5.27)

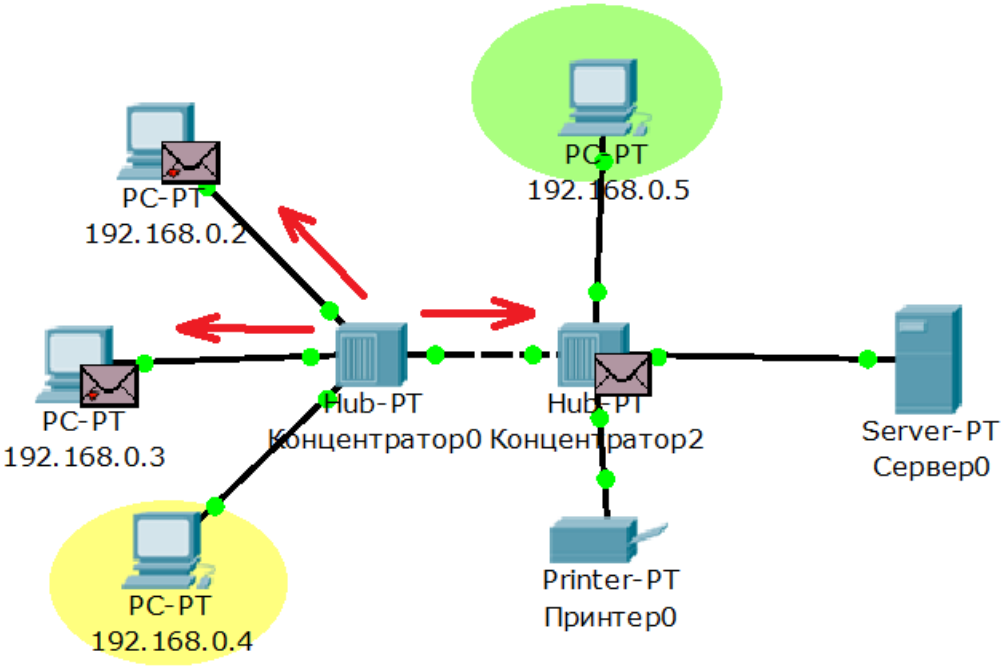


Рисунок 5.27 – Проходження пакету. Другий етап

Якщо пакети якимось вузлам не призначені, вони просто ігнорують їх (рис.5.28).

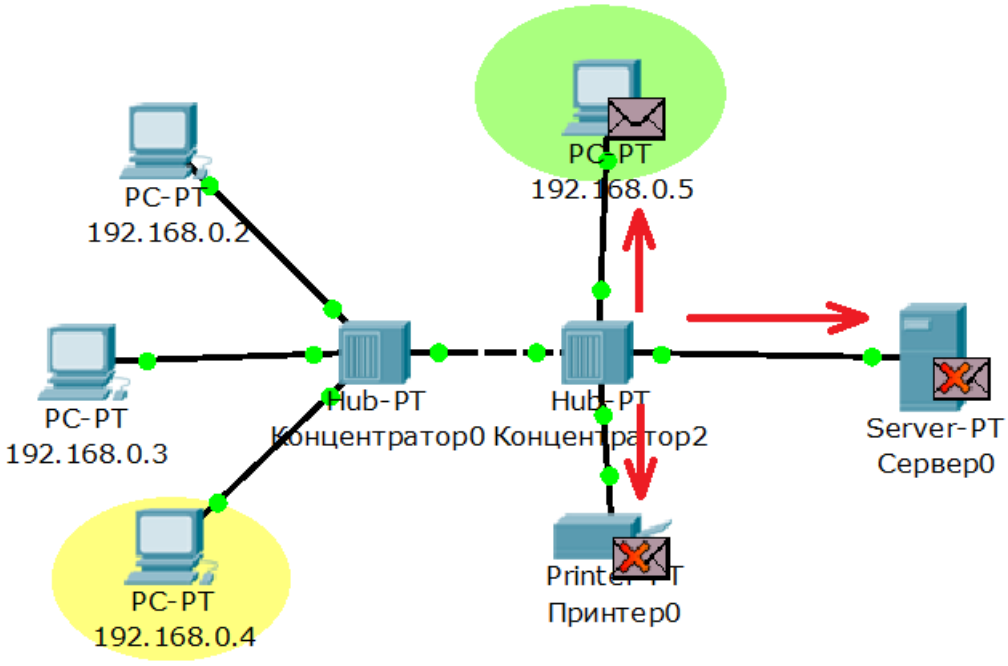


Рисунок 5.28 – Проходження пакету. Третій етап

Після знаходження адресату IP-пакету, пакет від адресата повертається по мережі назад до відправника (рис.5.29).

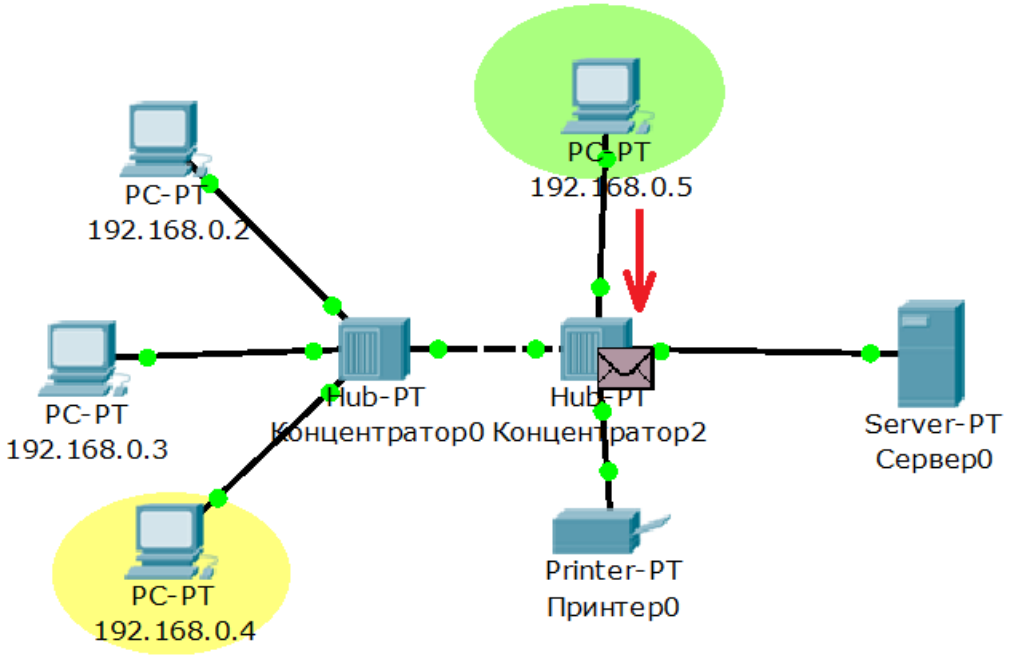


Рисунок 5.29 – Проходження пакету. Четвертий етап

Концентратор повторює пакет на всіх інших портах в надії, що на одному з них є відправник (підтвердження відповіді від отримувача) (рис.5.30)

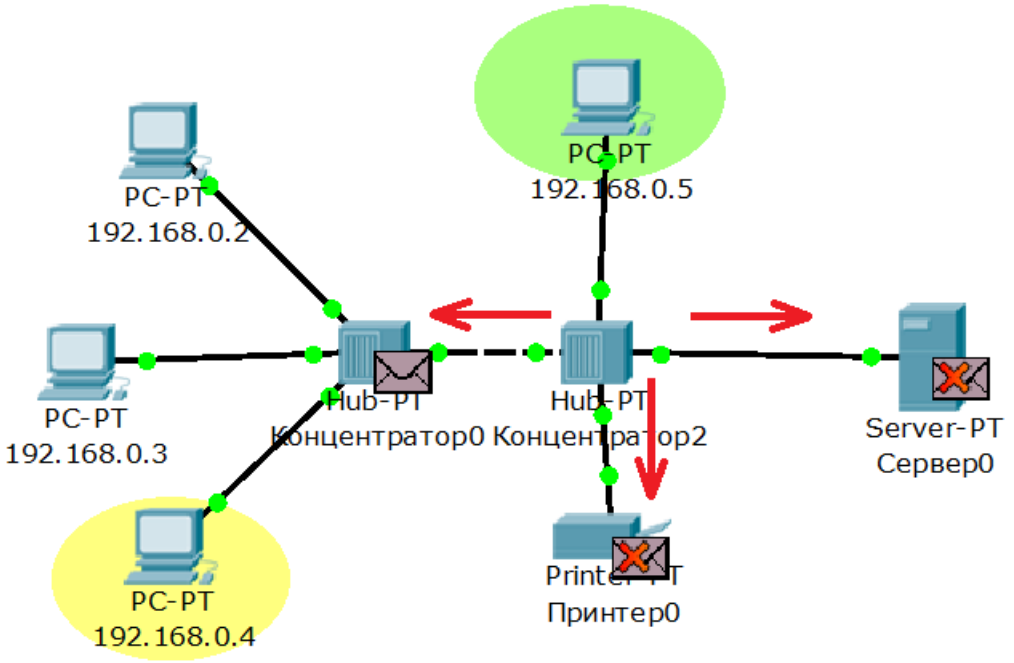


Рисунок 5.30 – Проходження пакету. П’ятий етап

Коли пакет повернеться до відправника IP-пакету назад через останній концентратор мережі, то побачимо підтвердження з'єднання (рис.5.31) у вигляді листа з галочкою .

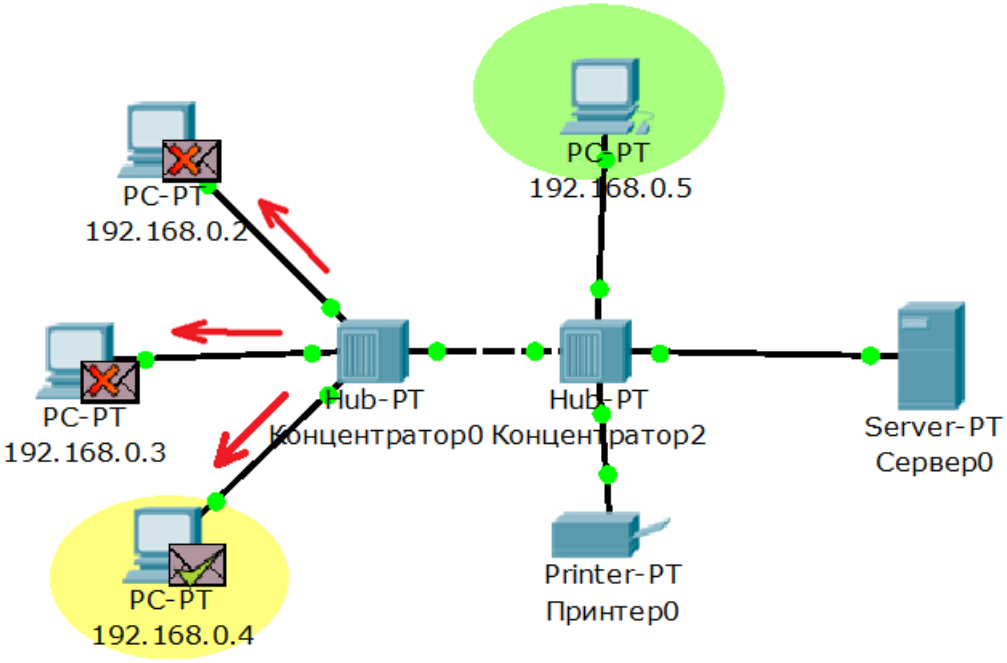


Рисунок 5.31 – Проходження пакету. Кінцевий етап

Зміст звіту

1. Титульний аркуш
2. Мета роботи
3. Відобразити результати поетапного симулювання роботи комп'ютерної мережі **Cicso Packet Tracer**.
4. Дайте відповіді на контрольні питання
5. Висновки

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 мережевим пристроям?
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 мережам?
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, використовуваних в Cisco Paket Tracer і вкажіть їх призначення.
14. Для чого використовується режим симуляції?
15. Як переглянути проходження пакету по рівням моделі OSI?
16. Можно чи визначити причину того, що посланий в режимі симуляції пакет не дійшов до адресата і на якому етапі стався збій роботи мережі?
17. Вкажіть у 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

Лабораторна робота №6
Налаштування мережевих сервісів

Мета роботи: вивчення принципу налаштування мережевих сервісів із застосуванням додатку Cisco Packet Tracer

ТЕОРЕТИЧНІ ВІДОМОСТІ

6.1 Мережеві сервіси

6.1.1 DHCP

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамічної конфігурації вузла) — це протокол прикладного рівня, що дозволяє комп'ютерам автоматично одержувати IP-адресу й інші параметри, необхідні для роботи в мережі. Для цього комп'ютер звертається до спеціального серверу, під назвою сервер DHCP. Мережевий адміністратор може задати діапазон адрес, що розподіляють серед комп'ютерів. Це дозволяє уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок. Протокол DHCP використовується в більшості великих мереж TCP/IP.

Протокол DHCP працює за схемою клієнт-сервер. Під час запуску системи комп'ютер, який є DHCP-клієнтом, відправляє в мережу запит на отримання IP-адреси. DHCP-сервер відповідає і відправляє повідомлення-відповідь, яке містить IP-адресу і деякі інші конфігураційні параметри. При цьому сервер DHCP може працювати в різних режимах, включаючи:

1. Динамічний розподіл - адміністратор присвоює IP-діапазон адрес на сервері DHCP. Кожен клієнтський комп'ютер в мережі повинен запросити IP-адресу від DHCP-сервера, коли мережа ініціалізується за концепцією "оренди". Коли закінчується термін оренди, якщо вона не буде продовжена, DHCP-сервер має право повернути адресу і призначити її на інші комп'ютери.
2. Автоматичне виділення - сервер DHCP буде постійно призначати вільний IP-адрес з діапазону, встановленого адміністратором, запитуючому комп'ютеру. Основна відмінність з динамічним розподілом в тому, що сервер зберігає записи минулих завдань IP і намагається привласнити ту ж адресу тому ж комп'ютеру для майбутніх мережних підключень.
3. Статичний розподіл - сервер DHCP робить призначення IP-адрес виключно на основі таблиці MAC-адрес, які зазвичай заповнені вручну адміністратором мережі. Якщо MAC-адреса комп'ютера не зазначена в таблиці, йому не буде призначений мережевий адрес.

6.1.2 DNS

DNS **(Доменна система імен)** (англ. *Domain Name System,* DNS) – ієрархічна розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в IP-адресу (і, при необхідності, навпаки).

Кожен комп'ютер в Інтернеті має свою власну унікальну адресу – число, яке складається з чотирьох байтів. Оскільки запам'ятовування десятків чи навіть сотень — не досить приємна процедура, то всі (чи майже всі) машини

мають імена, запам'ятати які (особливо якщо знати правила утворення імен) значно легше.

DNS-сервер - програма, призначена для відповідей на DNS-запити за відповідним протоколом. Також DNS-сервером можуть називати хост, на якому запущено відповідну програму.

6.1.3 HTML

HTML (англ. *HyperText Markup Language* — **Мова розмітки гіпертекстових документів**) — стандартна мова розмітки веб-сторінок в Інтернеті. Більшість веб-сторінок створюються за допомогою мови HTML (або XHTML). Документ HTML оброблюється браузером та відтворюється на екрані у звичному для людини вигляді.

Веб-се́рвер (англ. *Web Server*) — це сервер, що приймає HTTP-запити від клієнтів, зазвичай веб-браузерів, видає їм HTTP-відповіді, зазвичай разом з HTML-сторінкою, зображенням, файлом, медіа-потоком або іншими даними. Веб-сервер — основа Всесвітньої павутини.

Додатковими функціями багатьох веб-серверів є:

- Ведення журналу серверу про звернення користувачів до ресурсів
- Автентифікація користувачів
- Підтримка сторінок, що динамічно генеруються
- Підтримка HTTPS для захищених з'єднань з клієнтами

6.2 Налаштування мережевих сервісів із застосуванням додатку Cisco Packet Tracer

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

Створіть наступну схему мережі, яка зображена на рис. 6.1

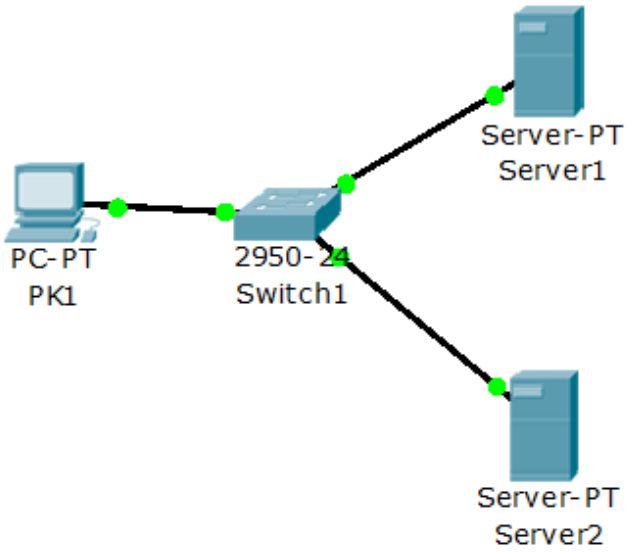


Рисунок 6.1 – Схема мережі

У даній схемі встановимо, що:

– Server1 – DNS (відповідає на DNS-запити) і Web сервер (приймає HTTP-запити від клієнтів);
– Server2 - DHCP сервер (призначає значення вільних IP-адрес клієнтам);
– Комп'ютер PK1 – клієнт, який автоматично отримує параметри протоколу TCP/IP з DHCP-сервера і користується WEB-сервером Server1 для перегляду WEB-сторінок (рис.6.2).

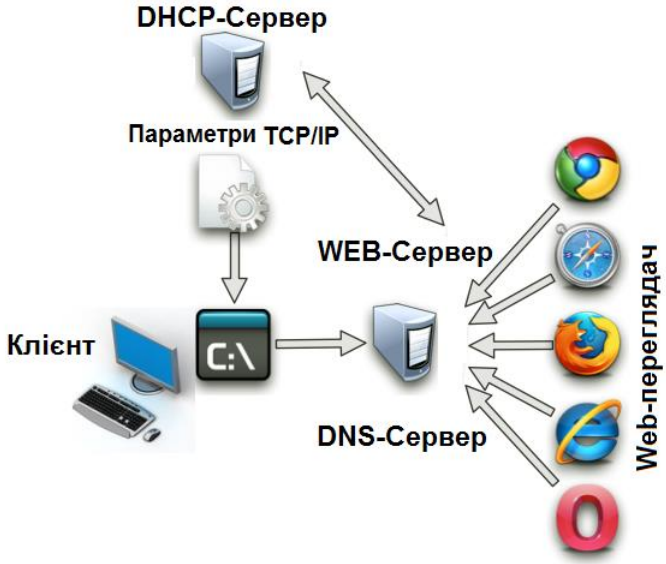


Рисунок 6.2 – Зв’язки між клієнтом та DNS-,WEB-серверами

Наведено етапи налаштування мережевих сервісів із застосуванням додатку Cisco Packet Tracer

6.2.1 Етап 1. Налаштування IP-адрес

Задайте параметри протоколу TCP/IP на ПК1 і серверах.

Увійдіть в конфігурацію ПК1 і встановіть налаштування IP-адреси через DHCP-сервер рис.6.3.

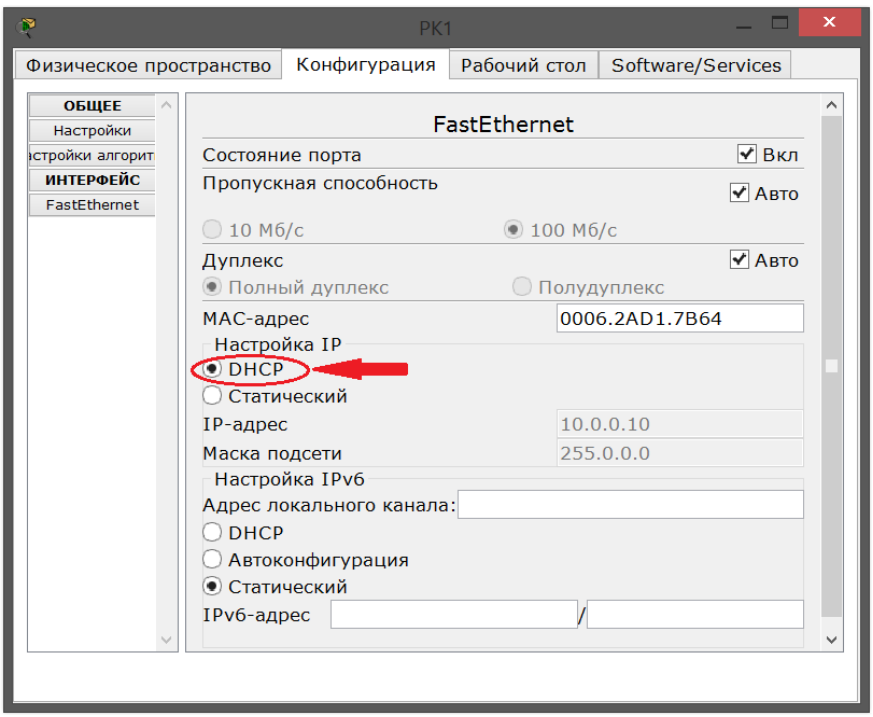


Рисунок 6.3 – Налаштування IP-адеси на PK1

Задайте в конфігурації серверів значення IP адрес (приклад):

- 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

6.2.2 Етап 2. Налаштування служби DNS на Server1

В конфігурації Server1 увійдіть на вкладку DNS і задайте два ресурсних записи в прямій зоні DNS:

1. у ресурсному записі типу A (1) зв'яжіть доменне ім'я комп'ютера (2) з його IP-адресом (3) рис.6.4 і натисніть кнопку ДОДАТИ (4):

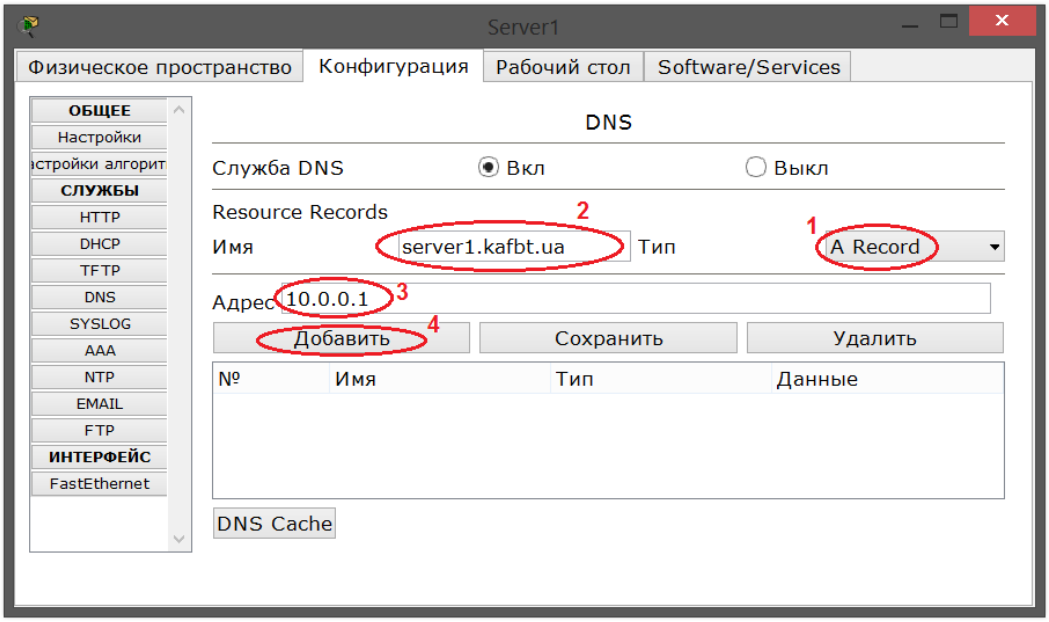


Рисунок 6.4 – Введення ресурсної записи типу A

2. у ресурсному записі типу CNAME (1) зв'яжіть псевдонім сайту (2) з комп'ютером (3) і натисніть кнопку ДОБАВИТИ (4) (рис.6.5).

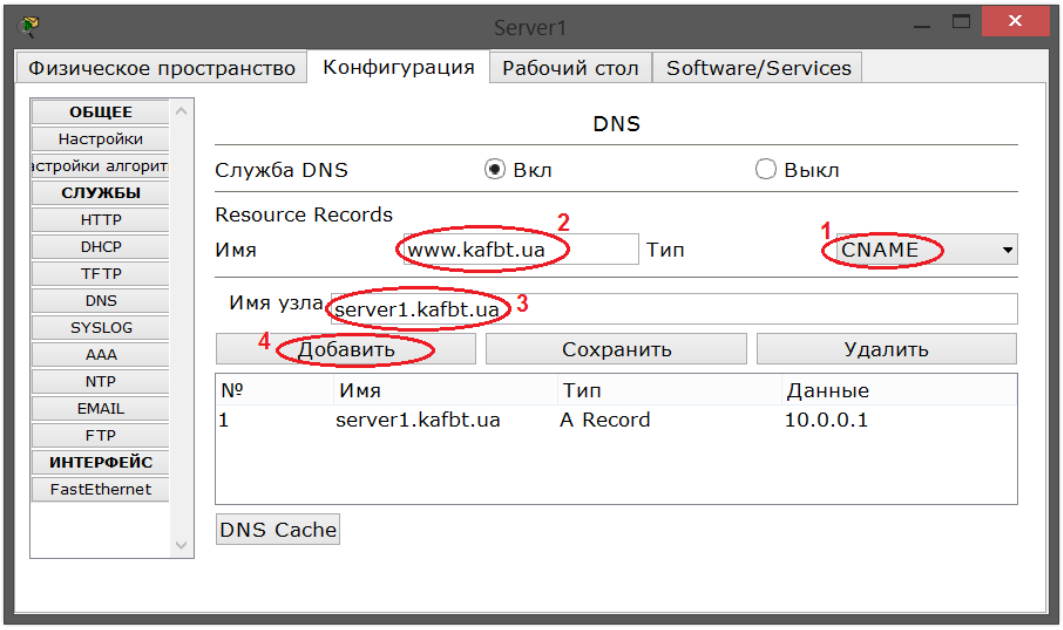


Рисунок 6.5 - Введення ресурсного запису типу CNAME

У конфігурації Server1 на вкладці HTTP і задайте стартову сторінку сайту www.kafbt.ua (рис.6.6):

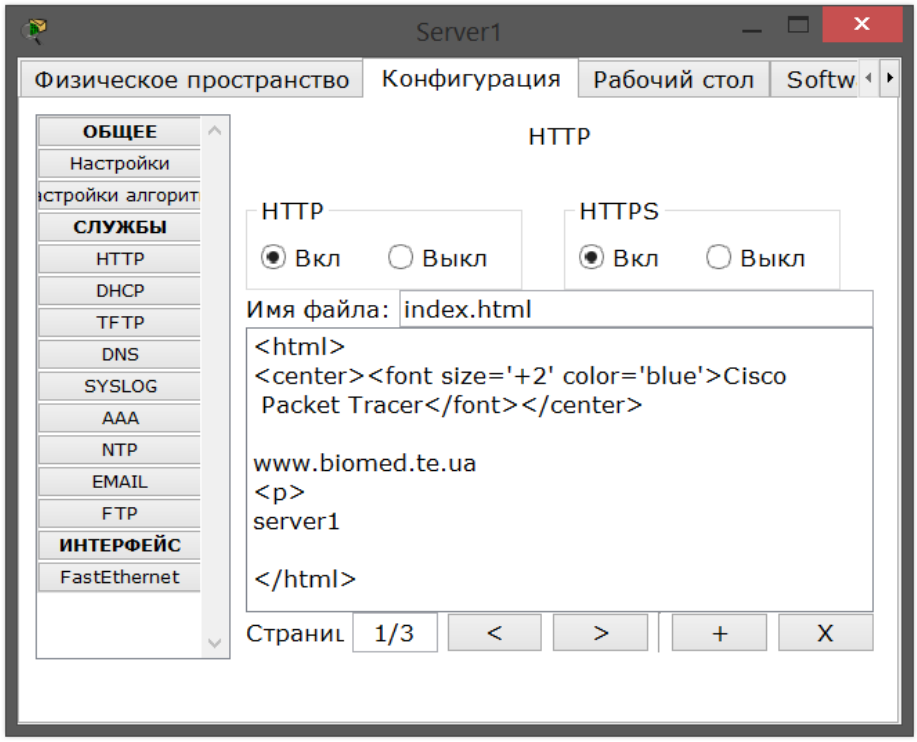


Рисунок 6.6 – Стартова сторінка сайту

Увімкніть командний рядок на Server2 і перевірте роботу служби DNS Server 1. Для перевірки прямої зони DNS сервера введіть команду:

SERVER> nslookup www.kafbt.ua

Якщо все правильно, то буде отримано відгук, який зображено на рис.6.7, із зазначенням повного доменного імені DNS сервера в мережі і його IP адресу.

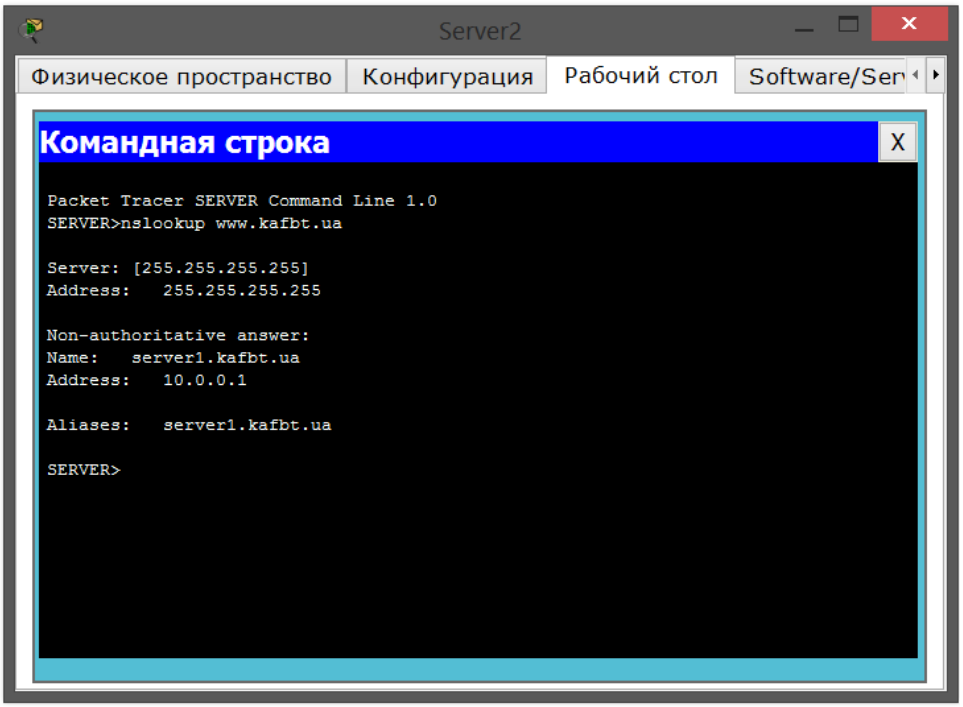


Рисунок 6.7 – Перевірка прямий зони DNS

6.2.3 Етап 3. Налаштування DHCP служби на Server2

Увійдіть в конфігурацію Server2 і на вкладці DHCP налаштуйте службу (рис.6.8): адресу DNS-сервера (1); початкове значення IP-адреси (2) з якої буде присвоюватися адреса клієнтам з активованим DHCP IP-адресом; максимальну кількість користувачів (клієнтів) (3).

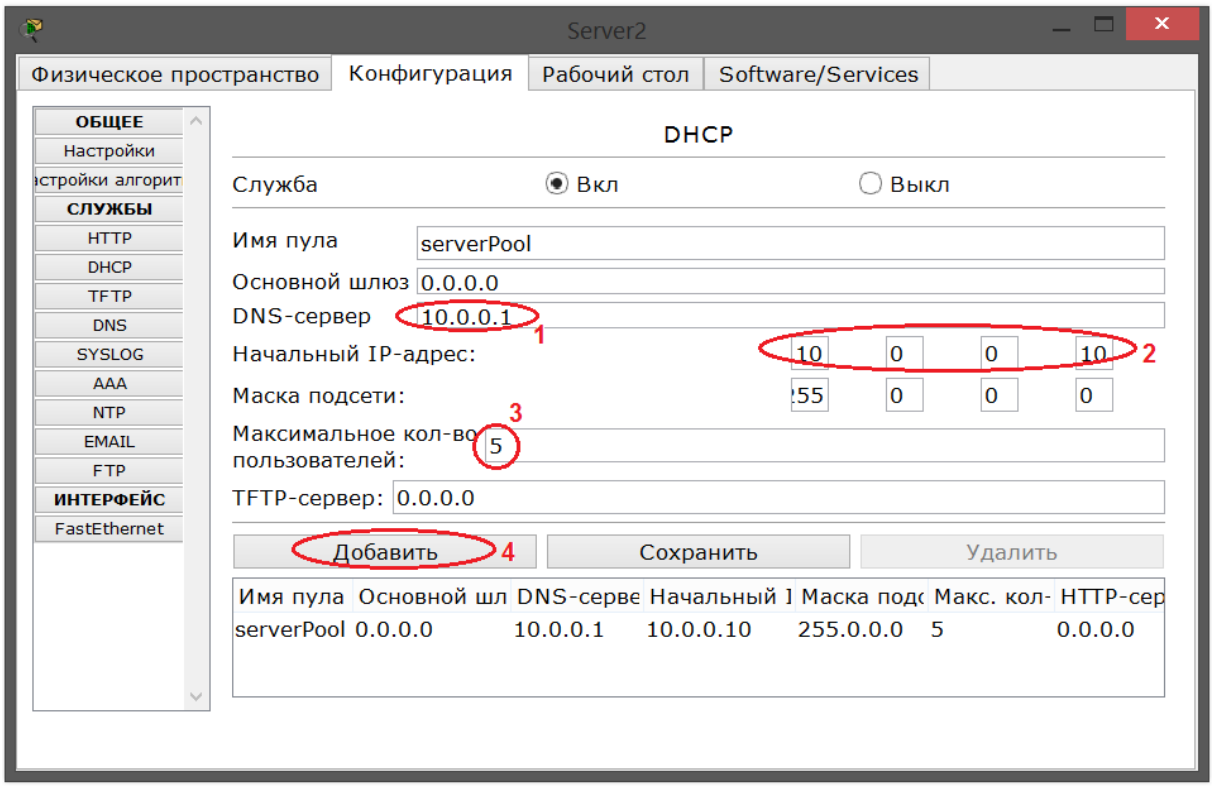


Рисунок 6.8 – Налаштування DHCP сервера

6.2.4 Етап 4. Перевірка роботи клієнта

Увійдіть в конфігурацію хоста PK1 на робочий стіл і в командному рядку налаштуйте протокол TCP/IP (рис.6.9)

Рисунок 6.9 – Робочий стіл ПК1

Командою **ipconfig / release** в командній стрічці робочого стола (рис.6.9) звільніть виділений DHCP IP-адрес за допомогою команди (рис.6.10):

PC> ipconfig / release

```
Packet Tracer PC Command Line 1.0
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>
```

Рисунок 6.10 – Результат звільнення виділеної DHCP IP-адреси клієнта PK1 команди **ipconfig / release**

а командою **ipconfig/renew** оновіть параметри конфігурації DHCP для зазначеного мережного адаптера:

PC> ipconfig / renew

Отримані нові параметри з DHCP сервера зображено на рис.6.11:

```
PC>ipconfig /renew

IP Address......................: 10.0.0.11
Subnet Mask.....................: 255.0.0.0
Default Gateway.................: 0.0.0.0
DNS Server......................: 10.0.0.1
```

Рисунок 6.11 – Конфігурація протокол TCP/IP клієнта

Відкрийте сайт www.kafbt.ua в браузері на клієнті PK1 (рис.6.12).

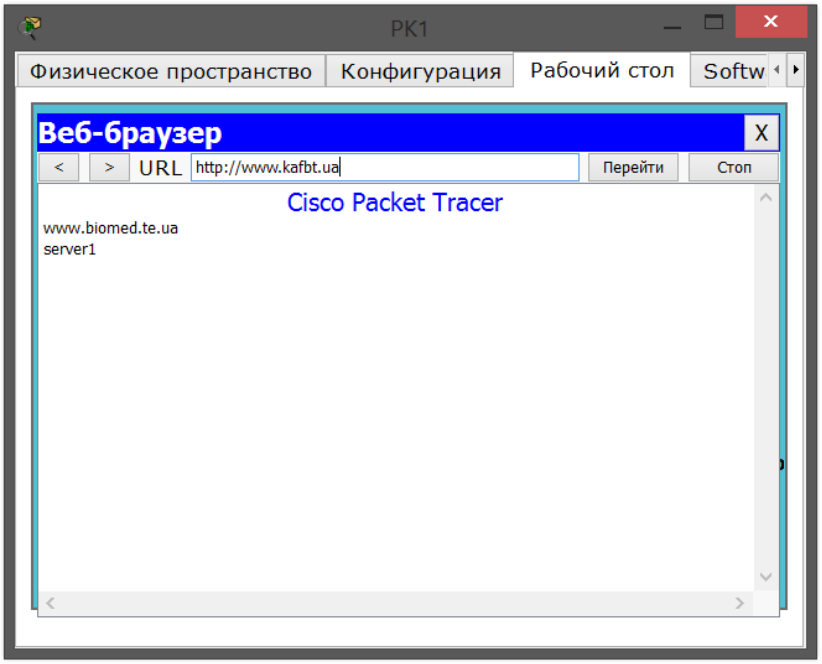


Рисунок 6.12 – Перевірка роботи клієнта

Завдання

Налаштуйте комп'ютерну мережу:
1 - Server1 - DNS і Web сервер (таблиця 6.1);
2 - Server2 - DHCP сервер (таблиця 6.2);
3 - Комп'ютер ПК1 отримує параметри протоколу TCP/IP з DHCP сервера і відкриває сайт www.kafbt.ua на Server1.

Таблиця 6.1 – завдання для виконання лабораторної роботи №6

№ варіанту	Server1: IP адреса	Server2: IP адреса	Маски підмереж	Web-сайт
1	20.0.0.1	20.0.0.2	255.0.0.0	www.server11.ua
2	192.168.0.1	192.168.0.2	255.255.255.0	www.kafedra.com
3	192.168.2.1	192.168.2.2	255.255.255.0	www.student.ua
4	10.1.0.1	10.1.0.2	255.255.255.0	www.odbject.com
5	192.168.11.1	192.168.11.2	255.255.255.0	www.ukraine.com
6	192.169.5.1	192.169.5.2	255.255.255.0	www.ternopil.ua
7	192.0.0.1	192.0.0.2	255.255.255.0	www.univer.te.ua
8	192.0.1.1	192.0.1.2	255.255.255.0	www.biomed.te.ua
9	192.1.1.2	192.1.1.1	255.255.255.0	www.RM2015.com
10	192.0.10.1	192.2.10.5	255.255.255.0	www.server22.com

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 пересилка 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 корпоративної мережі.
8. Продемонструйте настройку служби 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 WEB сервера в Cisco Paket Tracer?

Лабораторна робота №7
Статична маршрутизація

Мета роботи: вивчення налаштування статистичної маршрутизації комп'ютерної мережі застосуванням додатку Cisco Packet Tracer

ТЕОРЕТИЧНІ ВІДОМОСТІ

7.1 Протоколи маршрутизації

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

Одне з головних завдань маршрутизатора полягає у визначенні найкращого шляху до заданого адресату. Маршрутизатор визначає шляхи (маршрути) до адресатів або з статичної конфігурації, введеної адміністратором, або динамічно на підставі маршрутної інформації, отриманої від інших маршрутизаторів. Маршрутизатори обмінюються маршрутною 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 слідують правилам, визначеним 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 декількох шляхів до адресата призначення. Якщо від маршрутизатора до маршрутизатора є тільки один шлях, то часто використовують статичну маршрутизацію.

ЕКСПЕРИМЕНТАЛЬНА ЧАСТИНА

7.2 Налаштування статистичної маршрутизації із застосуванням додатку Cisco Packet Tracer

7.2.1 Створення схеми комп'ютерної мережі. Задачі налаштування маршрутизації

Наведено основні етапи налаштування статичної маршрутизації за допомогою графічних майстрів інтерфейсу Cisco Packet Tracer.

Для прикладу створимо схему мережі, яка зображена на рис.7.1.

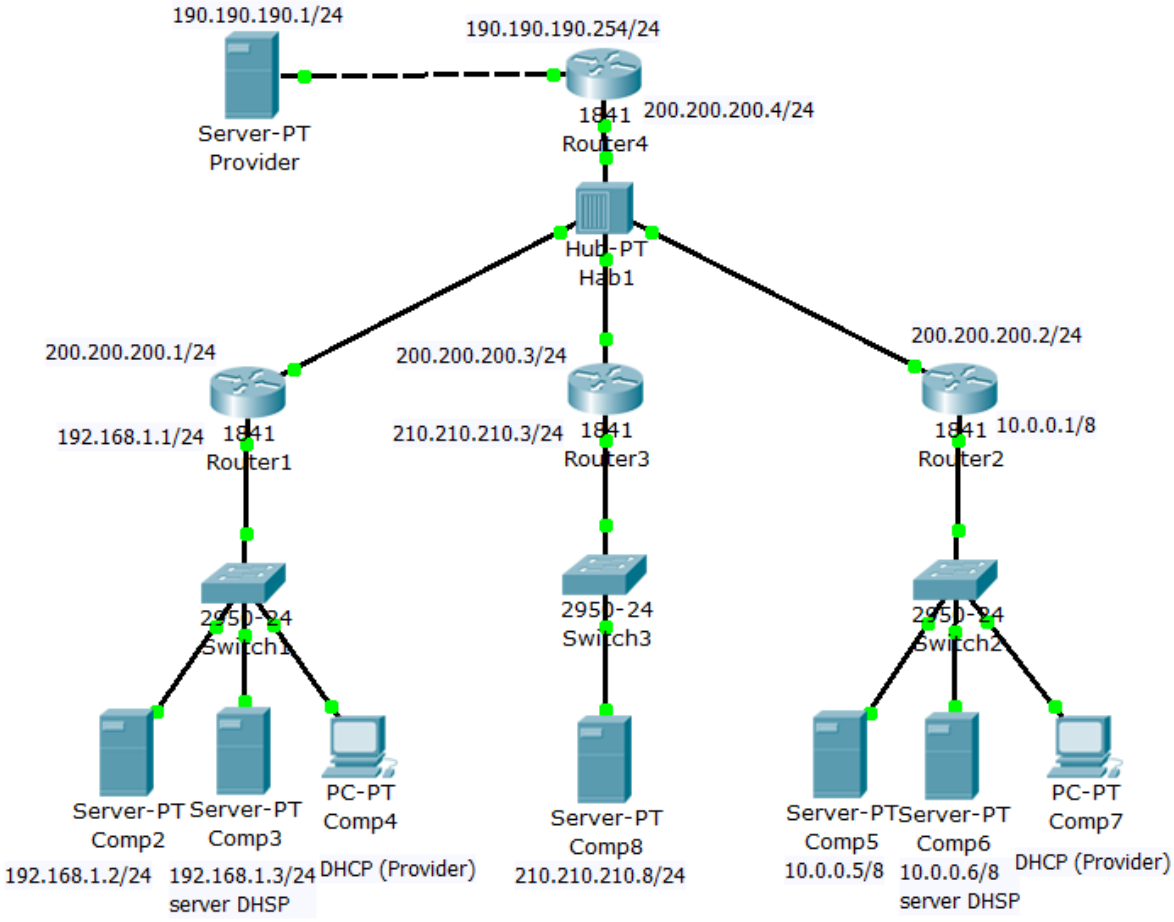


Рисунок 7.1 – Схема мережі

На схемі, яка зображена на рис. 7.1, зображено корпоративну мережа, що складається з таких компонентів:

- **Мережа 1** - на Switch1 замикається мережа першої організації (таблиця 7.1):

Таблиця 7.1 – 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 мережі 1 на Comp2 встановлений DNS і Web-сервер з сайтом організації.

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

- **Мережа 2** - на Switch2 замикається мережа другої організації (таблиця 7.2):

Таблиця 7.2. 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 мережі 2 на Comp5 встановлений DNS і Web сервер з сайтом організації.

На Comp6 встановлений DHCP сервер. Комп'ютер Comp7 отримує з DHCP сервера IP адрес, адрес DNS сервера провайдера (сервер Provider) і шлюз. Шлюз в мережі - 10.0.0.1/8.

- **Мережа 3** - на Hub1 замикається мережа 190.190.190.1/24. У мережі встановлений DNS сервер провайдера (комп'ютер Provaider з IP адресою - 190.190.190.1/24), що містить дані по всіх сайтах 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.

Маршрутизатори мають по два інтерфейси:

– **Router1** - 192.168.1.1/24 і 200.200.200.1/24 (рис.7.2-7.3 (після внесення IP-адреса та маски підмережі (1) необхідно включити порт (2))).

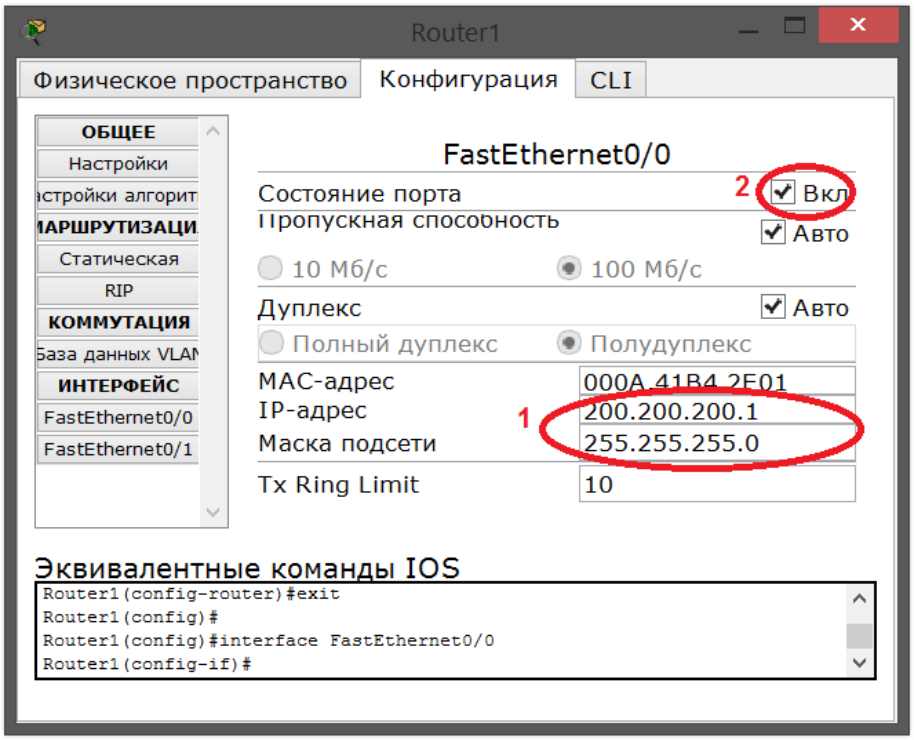


Рисунок 7.2 – Налаштування інтерфейсу FastEthernet 0/0 роутера Router1

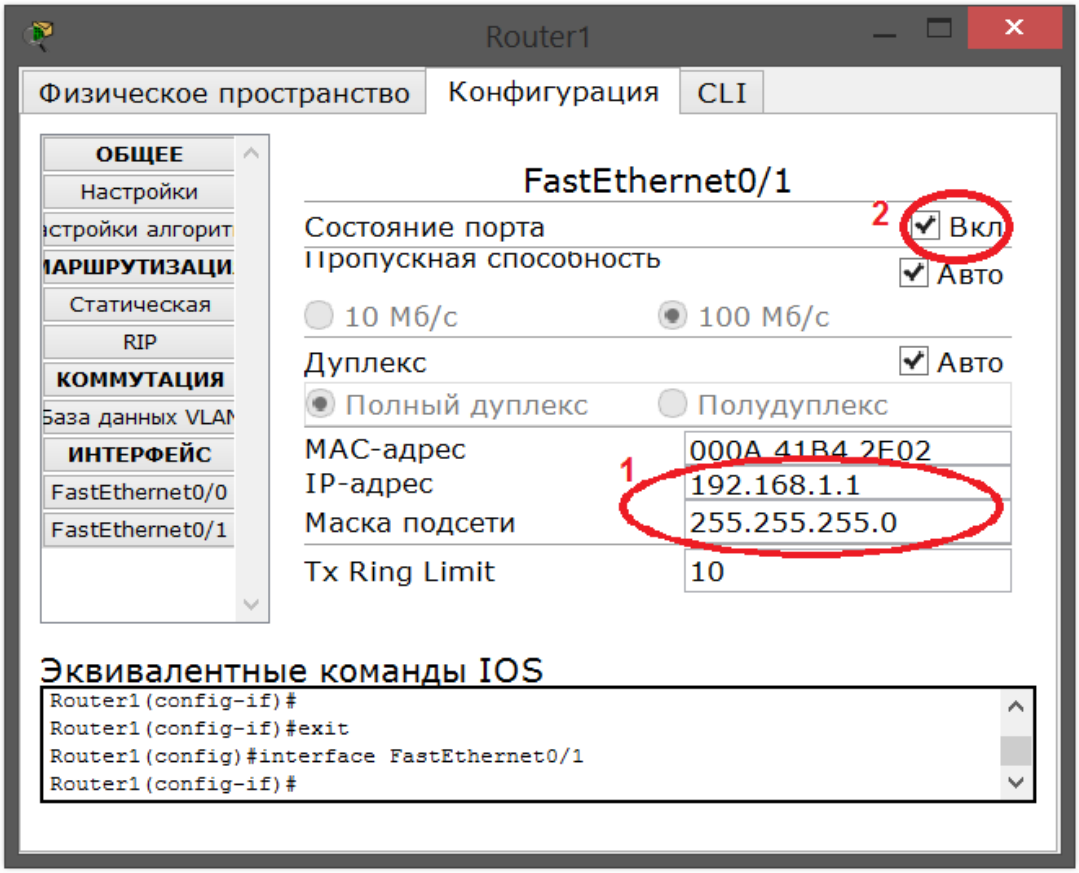


Рисунок 7.3 – Налаштування інтерфейсу FastEthernet 0/1 роутера Router1

Таким чином налаштовуються інтерфейси FastEthernet 0/0 та 0/1 для роутерів Router2, Router3 Router4:

- **Router2** - 10.0.0.1/8 і 200.200.200.2/24.
- **Router3** - 210.210.210.3/24 і 200.200.200.3/24.
- **Router4** - 190.190.190.254/24 і 200.200.200.4/24.

Задачі, які необхідно розв’язати при налаштування статистичної маршрутизації:

1. налаштувати мережі організацій;
2. налаштувати DNS сервер провайдера;
3. налаштувати статичні таблиці маршрутизації на роутерах;
4. перевірити роботу мережі - на кожному з комп'ютерів - Comp4, Comp7 і Comp8.

З кожного з них повинні відкриватися всі три сайти корпоративної мережі.

У попередніх лабораторних роботах розглядалося налаштування мережевих служб і DNS сервера. Приступимо до налаштування статичної маршрутизації на роутерах. Оскільки на представленій схемі чотири мережі, то в таблиці маршрутизації як мінімум повинні містити записи до кожної з цих мереж – тобто шість записів. На роутерах Cisco в таблицях маршрутизації як правило,

не прописуються шляхи до мереж, до яких приєднані інтерфейси роутера. Тому на кожному роутері необхідно внести по три записи.

7.2.2 Налаштування роутерів мережі.

Увійдіть в конфігурацію маршрутизатора і в інтерфейсах встановіть IP-адрес і маску підмережі. Потім у розділі маршрутизації відкрийте вкладку СТАТИЧНА, внесіть дані (рис.7.4) і натисніть кнопку ДОДАТИ.

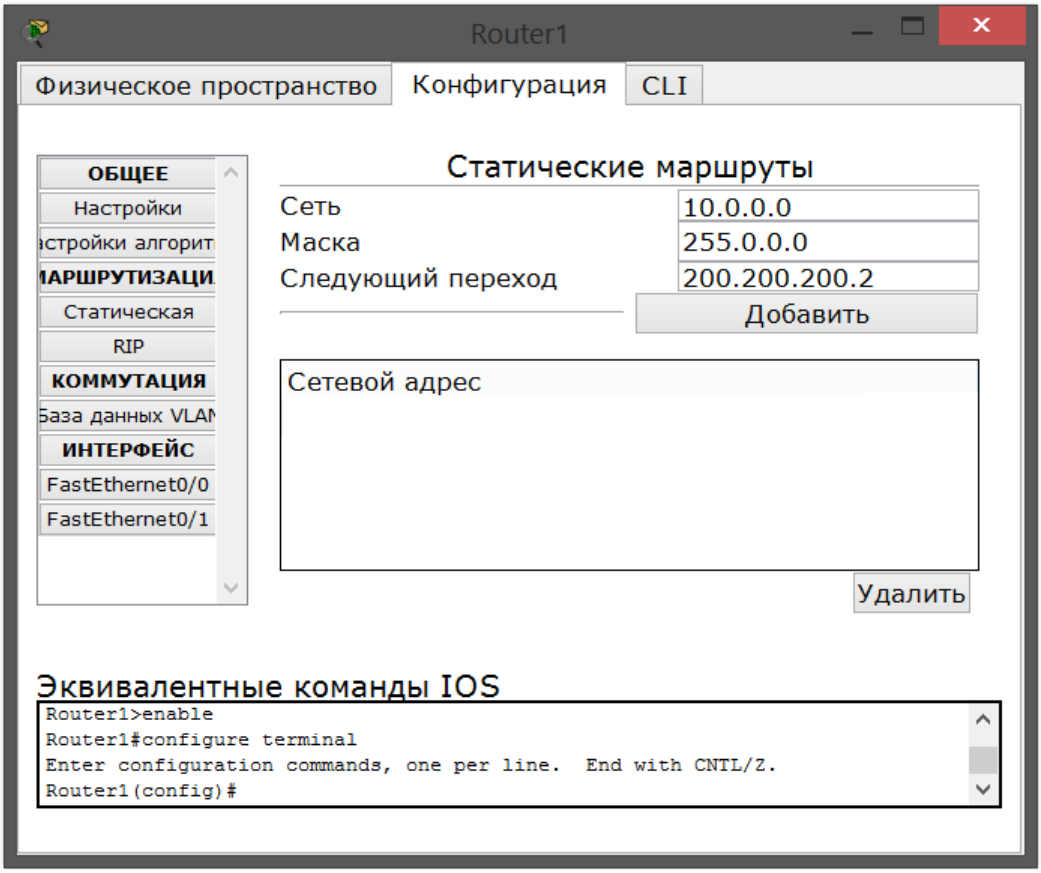


Рисунок 7.4 – Дані для мережі 10.0.0.0/8

Такий запис у таблиці вказує на маршрут з'єднання внутрішньої мережі 10.0.0.0 (маска 255.0.0.0) (інший вид запису - 10.0.0.0/8, де 10.0.0.0 – адрес мережі; 8 – кількість бітів маски, яка визначає адрес мережі) з зовнішньою мережею через порт 200.200.200.2.

В результаті внесення даних про всі мережі отримано три записи в таблиці маршрутизації (рис.7.5).

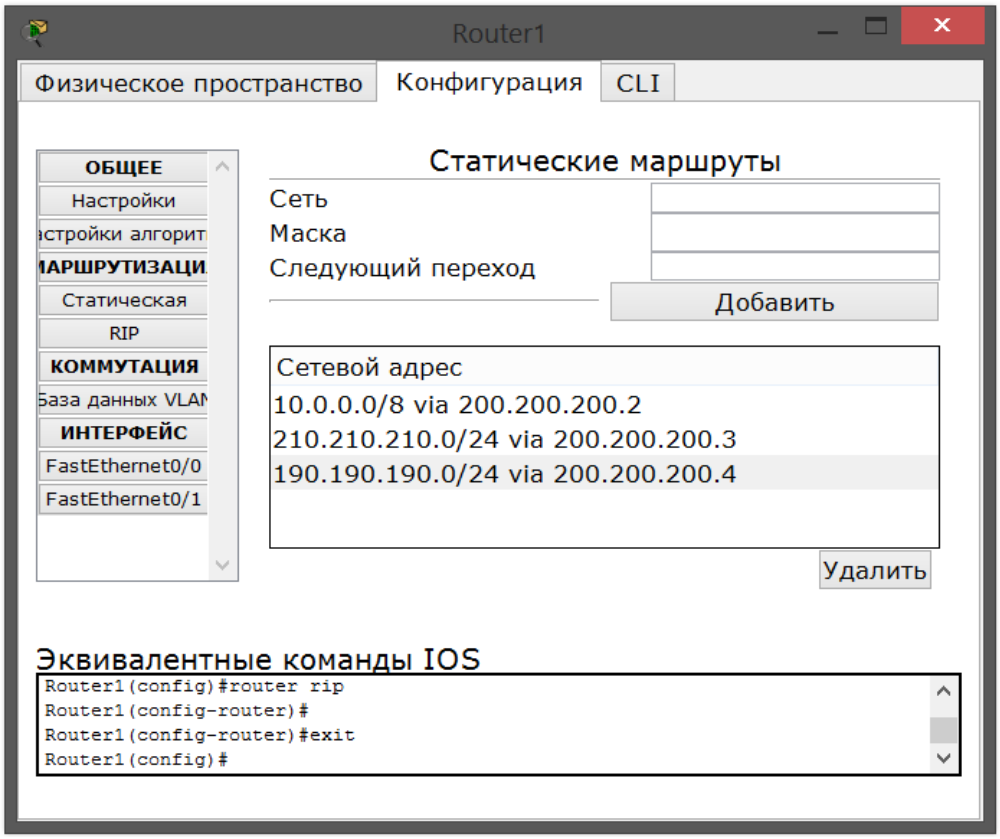


Рисунок 7.5 – Формування статичної таблиці маршрутизації

Для перегляду повного налаштування таблиці маршрутизації, виберіть у бічному графічному меню інструмент ПЕРЕВІРКА (піктограма лупи), клацніть в схемі на роутері і виберіть у спадному меню пункт таблиці маршрутизації (рис.7.6).

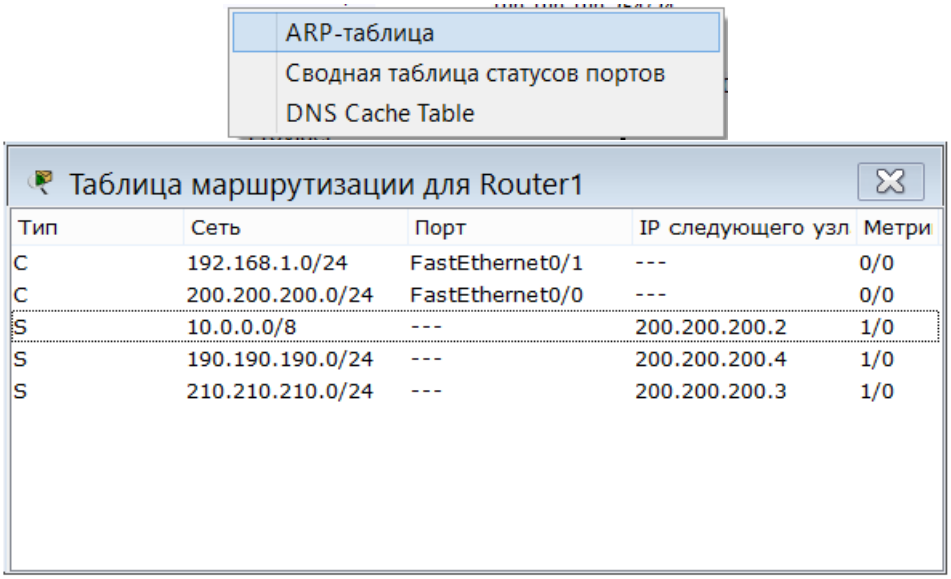


Рисунок 7.6 – Таблиця маршрутизації для роутера Router1

Таким чином налаштовано усі роутери комп’ютерної мережі.

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

Створіть схему комп’ютерної мережі, яка зображена на рис.7.7.

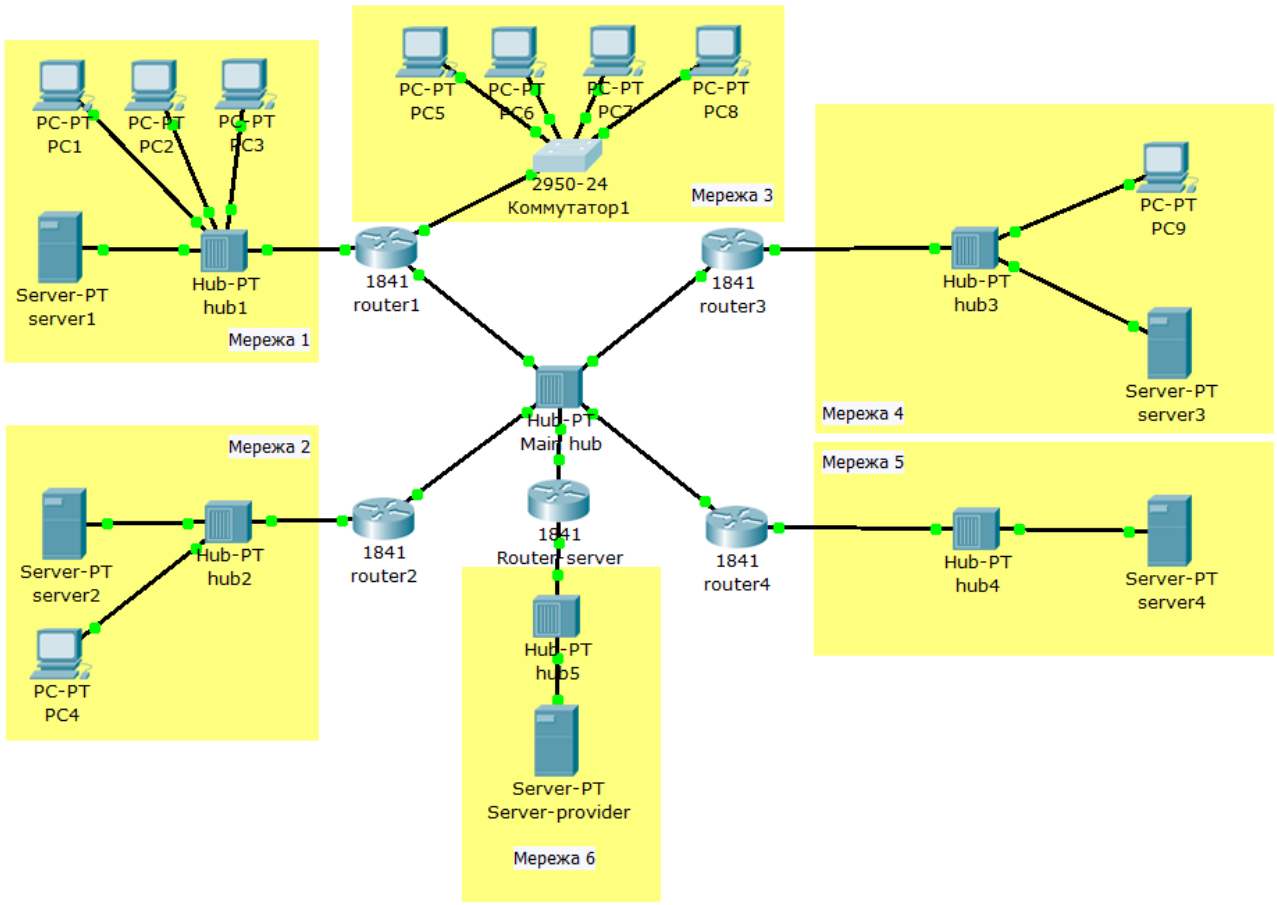


Рисунок 7.7 – Схема мережі

IP-адреси мереж подано у таблиці 7.3.

Таблиця 7.3 – Варіанти завдань

Варіант	Мережа 1	Мережа 2	Мережа 3	Мережа 4	Мережа 5	Мережа 6
1	111.0.0.0	112.0.0.0	113.0.0.0	114.0.0.0	1115.0.0.0	116.0.0.0
2	117.0.0.0	18.0.0.0	119.0.0.0	120.0.0.0	121.0.0.0	122.0.0.0
3	123.0.0.0	124.0.0.0	125.0.0.0	126.0.0.0	127.0.0.0	128.0.0.0
4	129.0.0.0	130.0.0.0	131.0.0.0	132.0.0.0	133.0.0.0	134.0.0.0
5	135.0.0.0	136.0.0.0	137.0.0.0	138.0.0.0	139.0.0.0	140.0.0.0
6	141.0.0.0	142.0.0.0	143.0.0.0	144.0.0.0	145.0.0.0	146.0.0.0
7	147.0.0.0	148.0.0.0	149.0.0.0	150.0.0.0	151.0.0.0	152.0.0.0
8	153.0.0.0	154.0.0.0	155.0.0.0	156.0.0.0	157.0.0.0	158.0.0.0
9	159.0.0.0	160.0.0.0	161.0.0.0	162.0.0.0	163.0.0.0	164.0.0.0
10	165.0.0.0	166.0.0.0	167.0.0.0	168.0.0.0	169.0.0.0	170.0.0.0
11	11.0.0.0	12.0.0.0	13.0.0.0	14.0.0.0	15.0.0.0	16.0.0.0
12	11.0.0.0	12.0.0.0	13.0.0.0	14.0.0.0	15.0.0.0	16.0.0.0
13	11.0.0.0	12.0.0.0	13.0.0.0	14.0.0.0	15.0.0.0	16.0.0.0

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

У мережі чотири веб-вузли на Server1, Server2, Server3 і Server4.

Сервера і комп'ютери **PC1-9** мають довільні IP адреси зі шлюзами своїх роутерів в межах мережі згідно варіанту завдання (табл.7.3).

Комп’ютери PC1-3 отримують адреси автоматично за допомогою сервера Server1 в межах мережі згідно варіанту завдання (табл.7.3).

Необхідно, щоб комп'ютери PC1-9 відкривали всі чотири сайти на серверах Server1-4 корпоративної мережі. У налаштуваннях комп'ютерів PC1-9 в якості DNS сервера вказано DNS сервер провайдера на Server-provider.

Контрольні питання

1. Що таке протоколи маршрутизації?
2. Що таке статистична маршрутизація?
3. Яка процедура налаштування портів FastEthernet роутера?
4. Як процедура налаштування статичної таблиці маршрутизації?
5. Як перевірити працездатність комп’ютерної мережі?

Лабораторна робота №8
Динамічна маршрутизація

Мета роботи: вивчення налаштування динамічної маршрутизації комп'ютерної мережі із застосуванням додатку Cisco Packet Tracer

ТЕОРЕТИЧНІ ВІДОМОСТІ

8.1 Динамічна маршрутизація

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

Маршрутизатори 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 згідно 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 та протоколи стану зв'язку.

8.2 Дистанційно-векторна маршрутизація

Маршрутизатори 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 як метрика кількість переходів (хопів).

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 всі інтерфейси маршрутизатора в широкомовному режимі без уточнення точної адреси конкретного сусіднього маршрутизатора.

Сусідній маршрутизатор, отримуючи широкомовлення, порівнює інформацію зі своєї поточної таблицею маршрутів. В 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

ЕКСПЕРИМЕНТАЛЬНА ЧАСТИНА

8.3 Налаштування протоколу RIP в додатку Cisco Packet Tracer

Розглянемо створену схему, яка зображена на рис.8.1.

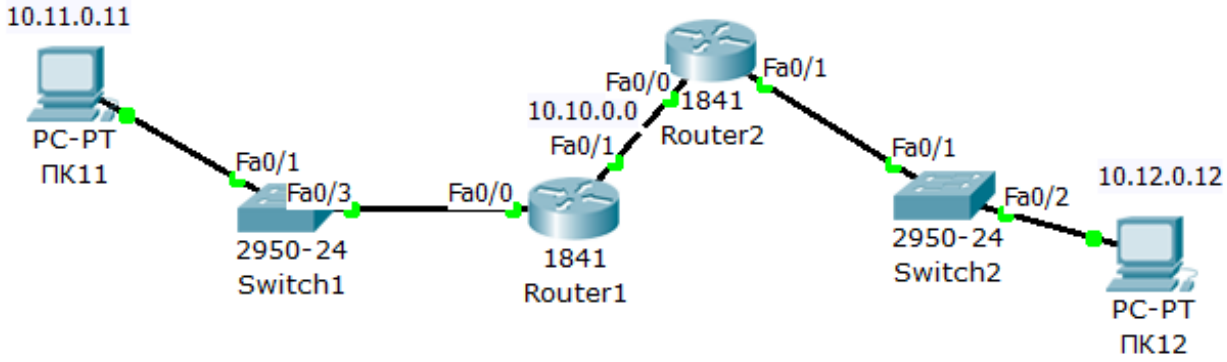


Рисунок 8.1 – Схема мережі

На схемі представлено 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:

Маршрутизатори 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. (шлюз - 10.11.0.1)
- ПК12 - 10.12.0.12/16 (шлюз - 10.12.0.1).

Наведемо процедуру налаштування 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):

Вхід в привілейований режим:

Router1> **enable**

Вхід в режим конфігурації:

Router1> # **conf term**

Вхід в режим конфігурування протоколу RIP:

Router1 (config) # **router rip**

Підключення клієнтської мережі до роутера:

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

Підключення другої мережу до роутера:

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

Задання використання другої версії протоколу RIP:

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

Вихід з режиму конфігурації протоколу RIP:

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

Вихід з консоллю налаштувань:

Router1 (config) # **exit**

Збережіть налаштування в пам'ять маршрутизатора:

Router1> # **write memory**

В закладці «Конфигурация» налаштування Router 1 маршрутизація/RIP має вигляд після програмного налаштування, який зображено на рис.8.2.

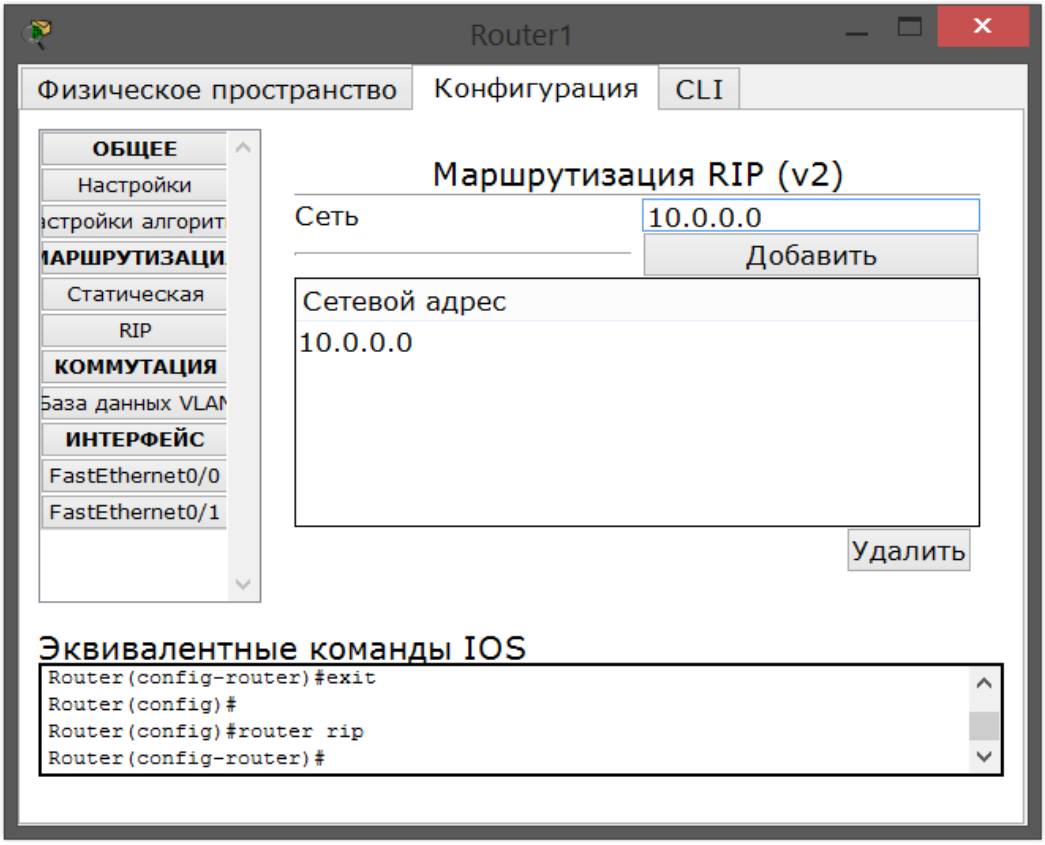


Рисунок 8.2 – Вигляд закладки «Конфигурация» Router1 налаштування маршрутизації/RIP

Аналогічно проводиться налаштування протоколу RIP на маршрутизаторі Router2.

Перевірку зв'язу між комп'ютерами ПК11 і ПК12 здійснюється командою **ping** (рис.8.3).

```
PC>ping 10.12.0.12

Pinging 10.12.0.12 with 32 bytes of data:

Reply from 10.12.0.12: bytes=32 time=156ms TTL=126
Reply from 10.12.0.12: bytes=32 time=141ms TTL=126
Reply from 10.12.0.12: bytes=32 time=154ms TTL=126
Reply from 10.12.0.12: bytes=32 time=141ms TTL=126

Ping statistics for 10.12.0.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% l
Approximate round trip times in milli-seconds:
    Minimum = 141ms, Maximum = 156ms, Average = 14
```

Результати пінгування ПК12 з ПК11

```
PC>ping 10.11.0.11

Pinging 10.11.0.11 with 32 bytes of data:

Reply from 10.11.0.11: bytes=32 time=125ms TTL=126
Reply from 10.11.0.11: bytes=32 time=152ms TTL=126
Reply from 10.11.0.11: bytes=32 time=156ms TTL=126
Reply from 10.11.0.11: bytes=32 time=156ms TTL=126

Ping statistics for 10.11.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 125ms, Maximum = 156ms, Average = 147ms
```

Результати пінгування ПК11 з ПК12

Рисунок 8.3 – Результати перевірки зв’язку між комп'ютерами ПК11 і ПК12

Якщо зв'язок є - всі налаштування зроблені вірно.

8.4 Завдання

Створіть схему, яка зображена на рис.8.4.

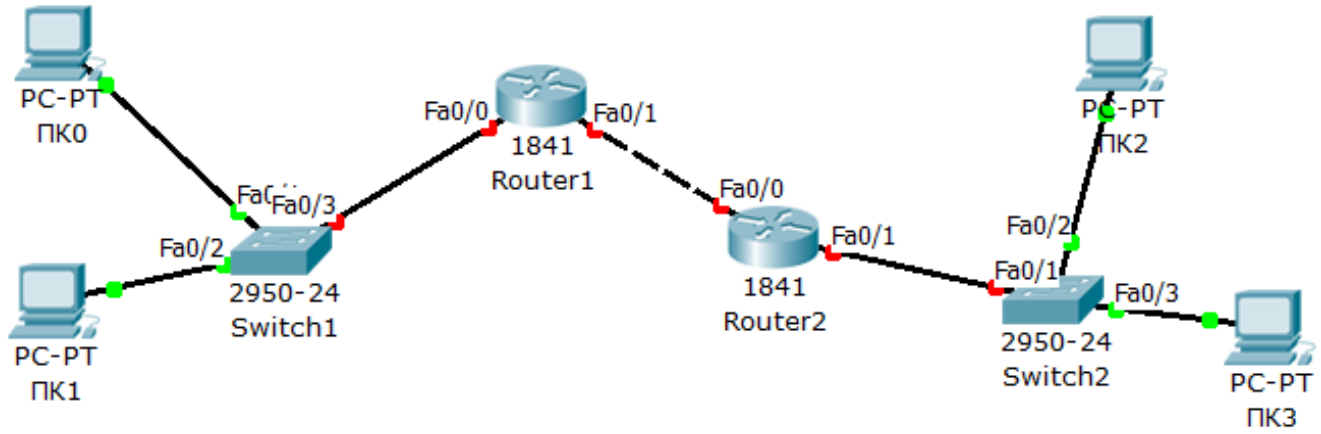


Рисунок 8.4 – Схема експериментальної мережі

Два концентратори представляють наступні мережі:

- Hub11 – мережа 192.168.1.0
- Hub12 – мережа 12.168.2.0

Для мережі (рис.8.2) налаштуйте динамічну маршрутизації шляхом налаштування протоколу RIP.

Необхідно, щоб між комп'ютерами ПК0-ПК3 були двосторонні зв'язки (наведені результати пінгування).

Контрольні питання

1. Чому статистична маршрутизація не підходить для великих комп’ютерних мереж?
2. Що таке автономна система?

3. Що таке динамічна маршрутизація?
4. Яке призначення протоколів IGP і EGP?
5. З якою метою маршрутизатори використовують метрики?
6. На якому алгоритмі базується дистанційно-векторна маршрутизація базується?
7. Як підключити клієнтську мережі до роутера у середовищі Cisco Packet Tracer
8. Як встановити номер протоколу RIP роутера у середовищі Cisco Packet?

Лабораторна робота №9
Протокол RIP в корпоративній мережі

Мета роботи: вивчення налаштування протоколу RIP в корпоративній мережі із застосуванням додатку Cisco Packet Tracer

ТЕОРЕТИЧНІ ВІДОМОСТІ

9.1 Корпоративна мережа

9.1.1 Визначення

Корпоративна мережа – це мережа, головним призначенням якої є підтримка роботи конкретного підприємства, що володіє даною мережею. Користувачами корпоративної мережі є тільки співробітники даного підприємства (рис.9.1).

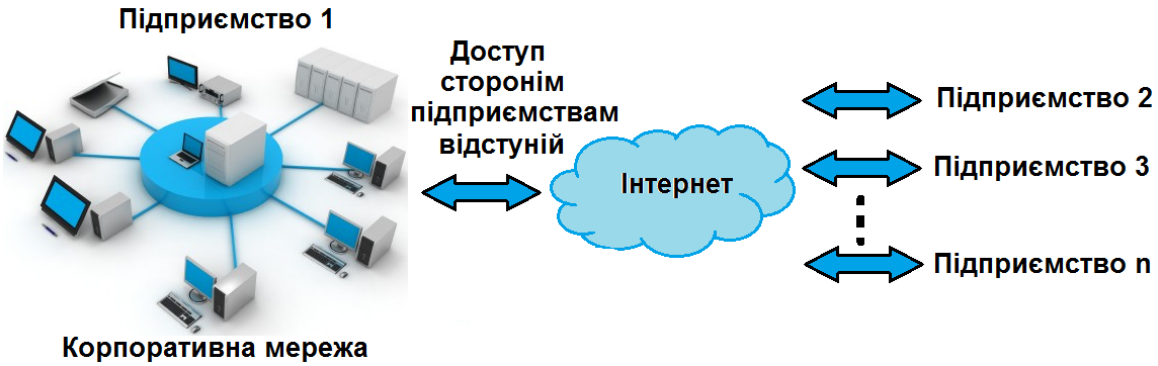


Рисунок 9.1 – Загальний вигляд корпоративної мережі

На відміну від мереж операторів зв'язку, корпоративні мережі, в загальному випадку, не надають послуг стороннім організаціям або користувачам. Залежно від масштабу підприємства, а також від складності і різноманіття вирішуваних завдань розрізняють мережі відділу, мережі кампусу і корпоративні мережі (термін «корпоративні» в даній класифікації набуває вузького значення – мережу великого підприємства).

9.1.2 Концепція корпоративної мережі

Будь-яка організація - це сукупність взаємодіючих елементів (підрозділів), кожен з яких може мати свою структуру. Елементи зв'язані між собою функціонально, тобто вони виконують окремі види робіт в рамках єдиного бізнес процесу, а також інформаційно, обмінюючись документами, факсами, письмовими і усними розпорядженнями і так далі крім того, ці елементи взаємодіють із зовнішніми системами, причому їх взаємодія також може бути як інформаційною, так і функціональною. І ця ситуація справедлива практично для всіх організацій, яким би видом діяльності вони не займалися - для урядової установи, банку, промислового підприємства, комерційної фірми і так далі.

Такий загальний погляд на організацію дозволяє сформулювати деякі загальні принципи побудови корпоративних інформаційних систем, тобто інформаційних систем в масштабі всієї організації.

9.1.3 Призначення корпоративної мережі

Корпоративною мережею вважається будь-яка мережа, що працює по протоколу TCP/IP і використовує комунікаційні стандарти Інтернету, а також сервісні застосування, що забезпечують доставку даних користувачам мережі. Наприклад, підприємство може створити сервер Web для публікації оголошень, виробничих графіків і інших службових документів. Службовці здійснюють доступ до необхідних документів за допомогою засобів (коштів) перегляду Web.

Сервери Web корпоративної мережі можуть забезпечити користувачам послуги, аналогічні послугам Інтернету, наприклад роботу з гіпертекстовими сторінками (що містять текст, гіперпосилання, графічні зображення і звукозаписи), надання необхідних ресурсів по запитах клієнтів Web, а також здійснення доступу до баз даних. У цьому керівництві всі служби публікації називаються “Службами Інтернету” незалежно від того, де вони використовуються (у Інтернеті або корпоративній мережі).

Корпоративна мережа, як правило, є територіально розподіленою, тобто об'єднуючою офіси, підрозділи і інші структури, що знаходяться на значному віддаленні один від одного. Принципи, по яких будується корпоративна мережа, досить сильно відрізняються від тих, що використовуються при створенні локальної мережі. Це обмеження є принциповим, і при проектуванні.

9.1.4 Структура корпоративної мережі

Для підключення віддалених користувачів до корпоративної мережі найпростішим і доступнішим варіантом є використання телефонного зв'язку. Там, де це можливо, можуть використовуватися мережі ISDN. Для об'єднання вузлів мережі в більшості випадків використовуються глобальні мережі передачі даних. Навіть там, де можлива прокладка виділених ліній (наприклад, в межах одного міста) використання технологій пакетної комутації дозволяє зменшити кількість необхідних каналів зв'язку і - що важливо - забезпечити сумісність системи з існуючими глобальними мережами.

Підключення корпоративної мережі до Internet виправдане, якщо вам потрібний доступ до відповідних послуг. Використовувати Internet як середовище передачі даних вартує тільки тоді, коли інші способи недоступні і фінансові міркування переважують вимоги надійності і безпеки. Якщо ви використовуватимете Internet тільки як джерело інформації, краще користуватися технологією "з'єднання за запитом" (dial-on-demand), тобто у такий спосіб підключення, коли з'єднання з вузлом Internet встановлюється тільки за вашою ініціативою і на потрібний вам час. Це різко знижує ризик несанкціонованого проникнення у вашу мережу ззовні.

9.2 Протокол RIP

Протокол RIP (**Routing Information Protocol, RIP)** – один із найрозповсюдженіших протоколів маршрутизації в невеликих комп'ютерних мережах, який дозволяє маршрутизаторам динамічно оновлювати маршрутну

інформацію (напрямок і дальність в хопах), отримуючи її від сусідніх маршрутизаторів.

Маршрут характеризується вектором відстані до місця призначення. Передбачається, що кожен маршрутизатор є відправною точкою декількох маршрутів до мереж, з якими він пов'язаний. Опису цих маршрутів зберігається в спеціальній таблиці, яка називається званої маршрутною.

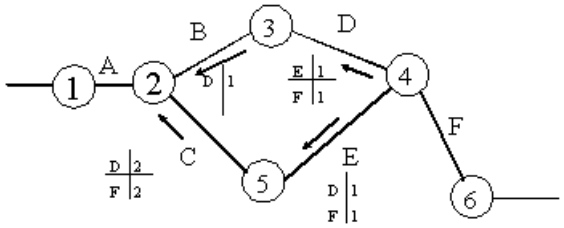
Таблиця маршрутизації RIP містить по запису на кожну обслуговуючу машину (на кожен маршрут). Запис повинен включати в себе:

- IP-адрес місця призначення.
- Метрика маршруту (від 1 до 15; число кроків до місця призначення).
- IP-адрес найближчого маршрутизатора (gateway) по дорозі до місця призначення.
- Таймери маршруту.

Першим двом полям запису ми зобов'язані появі терміну вектор відстані (місце призначення - напрям; метрика - модуль вектора). Періодично (раз в 30 сек) кожен маршрутизатор посилає широкомовно копію своєї маршрутної таблиці всім сусідам-маршрутизаторам, з якими він пов'язаний безпосередньо. Маршрутизатор-одержувач переглядає таблицю. Якщо в таблиці присутній новий шлях або повідомлення про більш короткий маршрут, або відбулися зміни довжин шляху, то ці зміни фіксуються одержувачем в своїй маршрутній таблиці. Протокол RIP повинен бути здатний обробляти три типи помилок:

- Циклічні маршрути. Так як в протоколі немає механізмів виявлення замкнутих маршрутів, необхідно або сліпо вірити партнерам, або вживати заходи для блокування такої можливості.
- Для подавлення нестабільностей RIP повинен використовувати мале значення максимально можливе числа кроків (<16).
- Повільне поширення маршрутної інформації з мережі створює проблеми при динамічній зміні маршрутної ситуації (система не встигає за змінами). Мале граничне значення метрики покращує збіжність, але не усуває проблему.

На рис. 9.2 наведено приклад роботи протоколу



Початкова інформація на вузлі 2			Поле після 2-ох кроків		
Мережа	Відстань	Сусід	Мережа	Відстань	Сусід
A	1	-	A	1	-
B	1	-	B	1	-
C	1	-	C	1	-
			D	2	3
			E	2	5
			D	3	5
			F	3	5

Рисунок 9.2 – Приклад роботи протоколу RIP

На рис 9.2: маршрутизатори 1-6, сегменти мереж A..F; наведена початкова інформація в маршрутизаторі 2 і інформація в ньому після двох ітерацій обміну маршрутними пакетами RIP; після певного числа ітерацій маршрутизатор буде знати про відстані до всіх сегментів, а також альтернативні маршрути)

Нехай мережею призначення є сегмент D. При необхідності відправити пакет у мережу D маршрутизатор переглядає свою базу даних маршрутів і вибирає порт, що має найменшу відстань до мережі призначення (у даному випадку порт, що зв'язує його з маршрутизатором 3).

Для адаптації до зміни стану зв'язків та обладнання з кожним записом таблиці маршрутизації пов'язаний таймер. Якщо за час тайм-ауту не прийде нове повідомлення, яке підтверджує цей маршрут, то він видаляється з маршрутної таблиці.

Отже, результатом роботи протоколу на конкретному маршрутизаторі є таблиця, де для кожної мережі даної RIP-системи вказано відстань до цієї мережі (в хопах) і адреса наступного маршрутизатора. Інформація про номер мережі та адресу наступного маршрутизатора з цієї таблиці вноситься в таблицю маршрутів, інформація про відстань до мережі використовується при обробці векторів відстаней.

9.3 Налаштування протоколу RIP в корпоративній мережі в додатку Cisco Packet Tracer

Розглянемо схему, яка зображена на рис. 9.3.

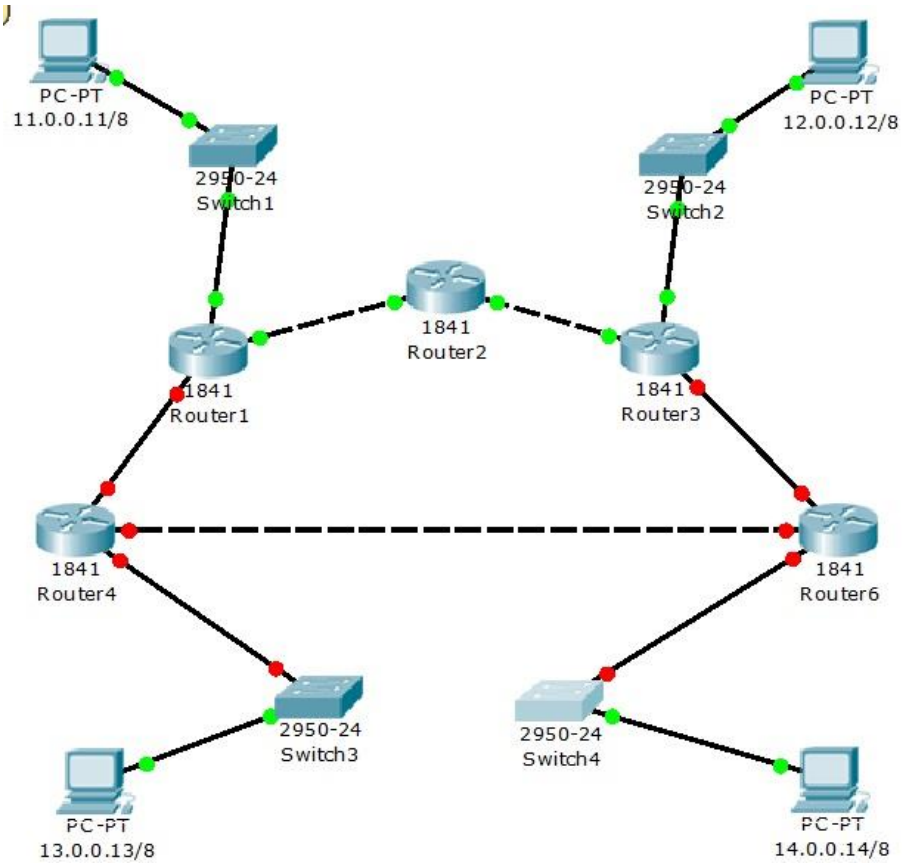


Рисунок 9.3 – Схема мережі

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, які подано у таблиці 9.1.

Таблиця 9.1 – Значення інтерфейсів

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

Для налаштування маршрутизації по протоколу RIP на кожному з роутерів необхідно:

1 - налаштування всіх маршрутизаторів, як це було показано в лабораторній роботі №8;

2 - перевірка налаштування маршрутизаторів по таблиці маршрутизації.

Для перевірко коректної конфігурації маршрутизації і працездатності необхідно переглянути таблицю RIP роутера, використовуючи команду show наступним чином:

Router # **show ip route rip**

Наприклад для шостого маршрутизатора Router6 таблиця буде має вигляд, який зображено на рис.9.4.

```
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
                [120/2] via 81.0.0.4, 00:00:08, FastEthernet0/1
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 9.4 – 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).

Після перевірки таблиці необхідно провести діагностику мережі, в наступному порядку:

– перевірка правильності налаштування за допомогою команд **ping** і **tracert** в консолі кожного комп'ютера;

– діагностування мережі при вимкненому маршрутизаторі Router9.

– перевірка зв'язку 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 роутері 6 має бути різною. При включеному роутері 6 повинно бути на одиницю менше, ніж при вимкненому.

9.4 Завдання

Створіть схему, яка представлена на рис.9.5.

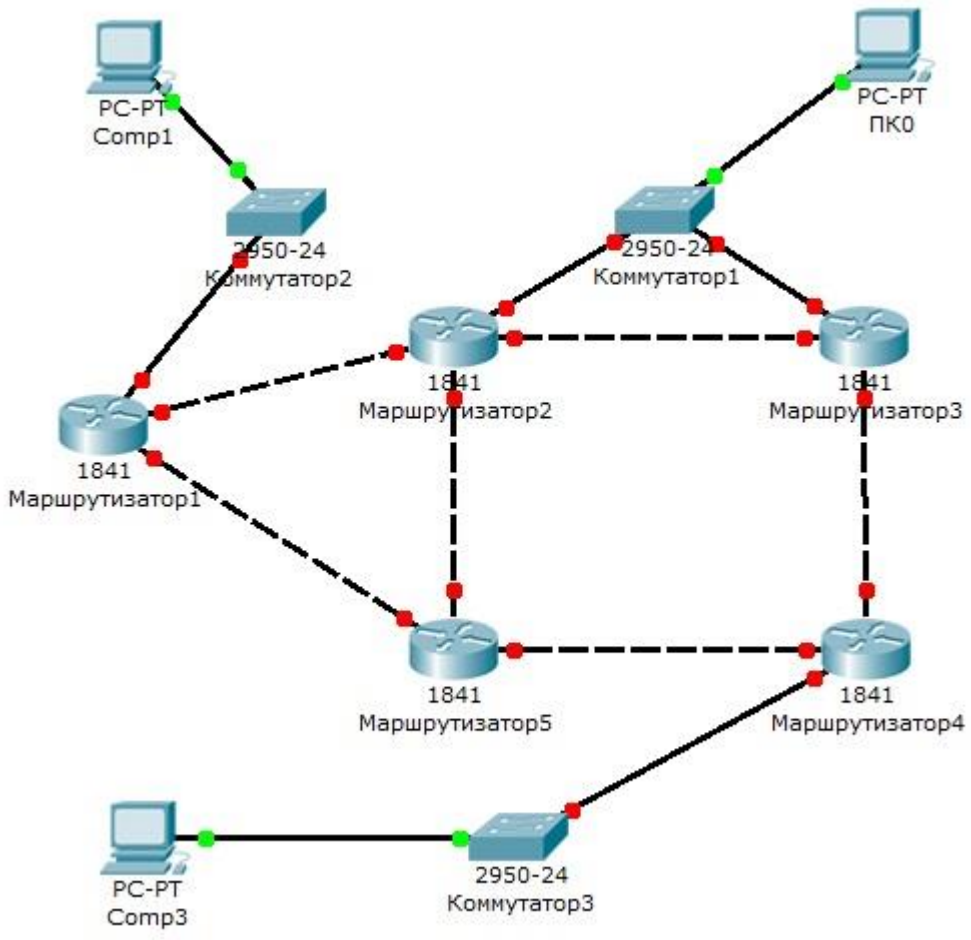


Рисунок 9.5 – Схема мережі

Послідовність виконання 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 з допомогою команд **ping** і **tracert** при включеному і вимкненому другому маршрутизаторі.

Контрольні запитання

1. Що таке корпоративна мережа?
2. Як функціонує протокол RIP?
3. Яке призначення таблиці маршрутизації?
4. Які записи повинна містити таблиця маршрутизації згідно протоколу RIP?
5. Яке призначення таймерів маршруту?
6. Які типи помилок повинен обробляти протокол RIP?
7. Як переглянути таблицю RIP роутерів у додатку Cisco Packet Tracer?

Лабораторна робота №10
Служба NAT

Мета роботи: вивчення налаштування служби NAT із застосуванням додатку Cisco Packet Tracer

ТЕОРЕТИЧНІ ВІДОМОСТІ

10.1 Служба NAT

NAT (Network Address Translation) - трансляція мережевих адрес, технологія, яка дозволяє перетворювати (змінювати) IP адреси і порти в мережевих пакетах.

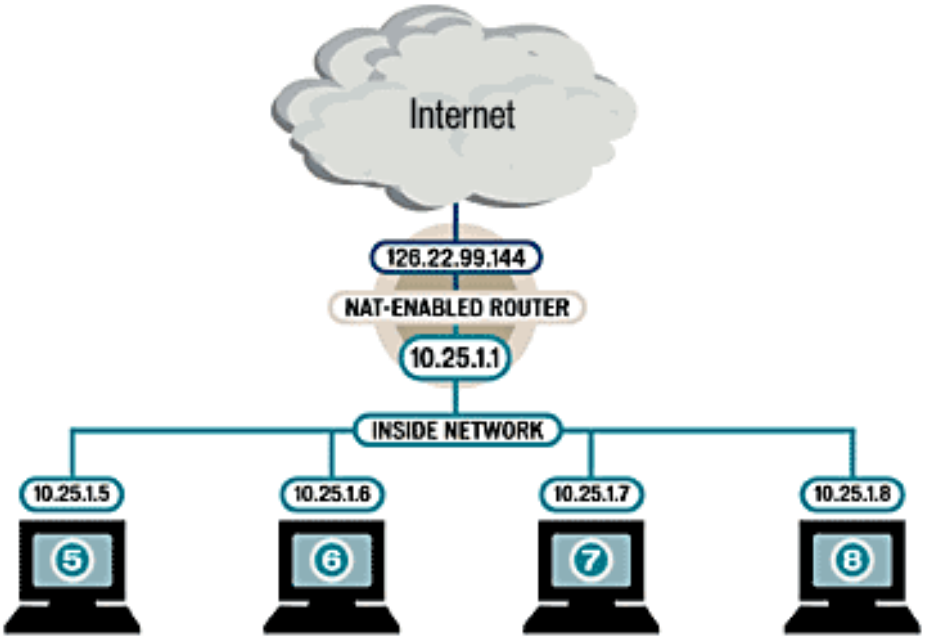


Рисунок 10.1 – Мережа з службою NAT

NAT використовується найчастіше для здійснення доступу пристроїв з мережі підприємства (будинку) в Інтернет, або навпаки для доступу з Інтернет на який-небудь ресурс всередині мережі.

Мережа підприємства зазвичай будується на приватних IP адресах. Згідно RFC 1918 під приватні адреси виділено три блоки:

- 10.0.0.0 - 10.255.255.255 (10.0.0.0/255.0.0.0 (/ 8))
- 172.16.0.0 - 172.31.255.255 (172.16.0.0/255.240.0.0 (/ 12))
- 192.168.0.0 - 192.168.255.255 (192.168.0.0/255.255.0.0 (/ 16))

Ці адреси не маршрутизируются в Інтернеті, і провайдери повинні відкидати пакети з такими IP адресами відправників або одержувачів.

Для перетворення приватних адрес в Глобальні (маршрутизовані в Інтернеті) застосовують NAT.

Крім можливості доступу в зовнішню мережу (Інтернет), NAT має ще кілька позитивних сторін. Так, наприклад, трансляція мережевих адрес дозволяє приховати внутрішню структуру мережі і обмежити до неї доступ, що підвищує безпеку. А ще ця технологія дозволяє економити Глобальні IP адреси, так як під одною Глобальною адресою в Інтернет може виходити безліч хостів.

Налаштування NAT на маршрутизаторах Cisco під управлінням IOS включає в себе наступні кроки

1. Призначити внутрішній (Inside) і зовнішній (Outside) інтерфейси.

Внутрішнім інтерфейсом зазвичай виступає той, до якого підключена локальна мережа. Зовнішнім - до якого підключена зовнішня мережа, наприклад мережу Інтернет провайдера.

2. Визначити для кого (яких ip-адрес) варто робити трансляцію.
3. Вибрати який вид трансляції використовувати.
4. Здійснити перевірку трансляцій.

Існує три види трансляції Static NAT, Dynamic NAT, Overloading.

Static NAT - статичний NAT, перетворення IP адреси один до одної, тобто зіставляється одна адреси з внутрішньої мережі з однією адресою з зовнішньої мережі.

Dynamic NAT - динамічний NAT, перетворення внутрішньої адрес(и) в один з групи зовнішніх адрес. Перед використанням динамічної трансляції, потрібно задати nat-пул зовнішніх адрес

Overloading - дозволяє перетворювати декілька внутрішніх адрес в один зовнішній. Для здійснення такої трансляції використовуються порти, тому іноді такий NAT називають PAT (Port Address Translation). За допомогою PAT можна перетворювати внутрішні адреси в зовнішній адресу, яка задана через пул або через адресу на зовнішньому інтерфейсі.

10.2 Налаштування служби NAT із застосуванням додатку Cisco Packet Tracer

Список команд для налаштування NAT:

позначення Інтернет інтерфейсу:
interface FastEthernet0 / 0
ip nat outside

позначення локального інтерфейсу:
interface Vlan1
ip nat inside

створення списку IP, що має доступ до NAT:
ip access-list extended NAT
permit ip host 192.168. ???. ??? any

включення NAT на зовнішньому інтерфейсі:

ip nat inside source list NAT interface FastEthernet0 / 0 overload

Подивитися існуючі трансляції можна командою "show ip nat translations".

Налагодження запускається командою "debug ip nat"

Налаштування Static NAT
router (config) #ip nat inside source static <local-ip> <global-ip>
router (config) #interface fa0 / 4
router (config-if) #ip nat inside
router (config) #interface fa0 / 4
router (config-if) #exit
router (config) #interface s0
router (config-if) #ip nat outside

Налаштування Dynamic NAT
router (config) #ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}
router (config) # access-list <acl-number> permit <source-IP> [source-wildcard]
router (config) #ip nat inside source list <acl-number> pool <name>
router (config) #interface fa0 / 4
router (config-if) #ip nat inside
router (config-if) #exit
router (config) #interface s0
router (config-if) #ip nat outside

Налаштування Overloading
router (config) # access-list acl-number permit source-IP source-wildcard
router (config) #ip nat inside source list acl-number interface interface overload
router (config) #interface fa0 / 4
router (config-if) #ip nat inside
router (config-if) #exit
router (config) #interface s0
router (config-if) #ip nat outside

ЕКСПЕРИМЕНТАЛЬНА ЧАСТИНА

10.3 Завдання

В роботі необхідно вирішити завдання виведення комп'ютерів локальної мережі організації в інтернет. Локальна мережа налаштована у приватній адресації - в мережі 10.0.0.0, адреси якої не мають виходу в інтернет. Для вирішення цього завдання необхідно налаштувати службу NAT. Схему мережі зображено на рис.10.2.

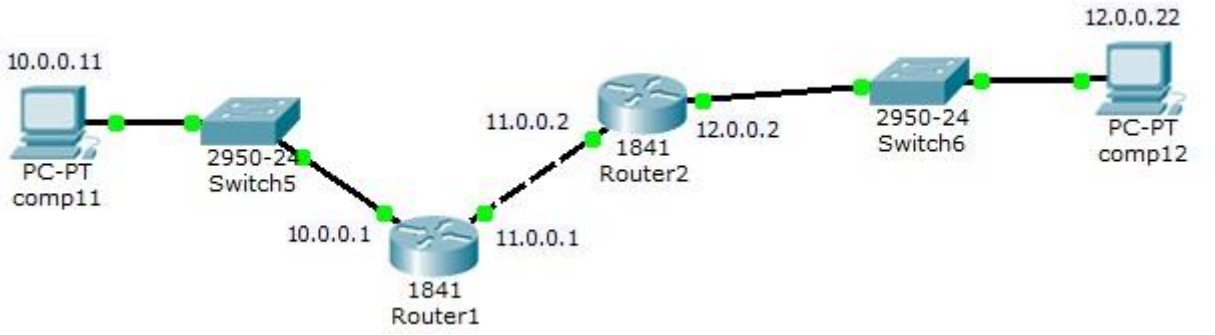


Рисунок 10.2 – Схема мережі

Створіть мережу, яка зображена на рис.10.2. Задайте імена пристроїв і адресацію, як зображено на рис.10.2.

В початковий момент NAT на роутері не налаштований, в цьому переконатися, використовуючи режим симуляції.

Перейдіть в режим симуляції і проаналізуйте склад пакету при проходженні через обидва роутери (рис. 10.3).

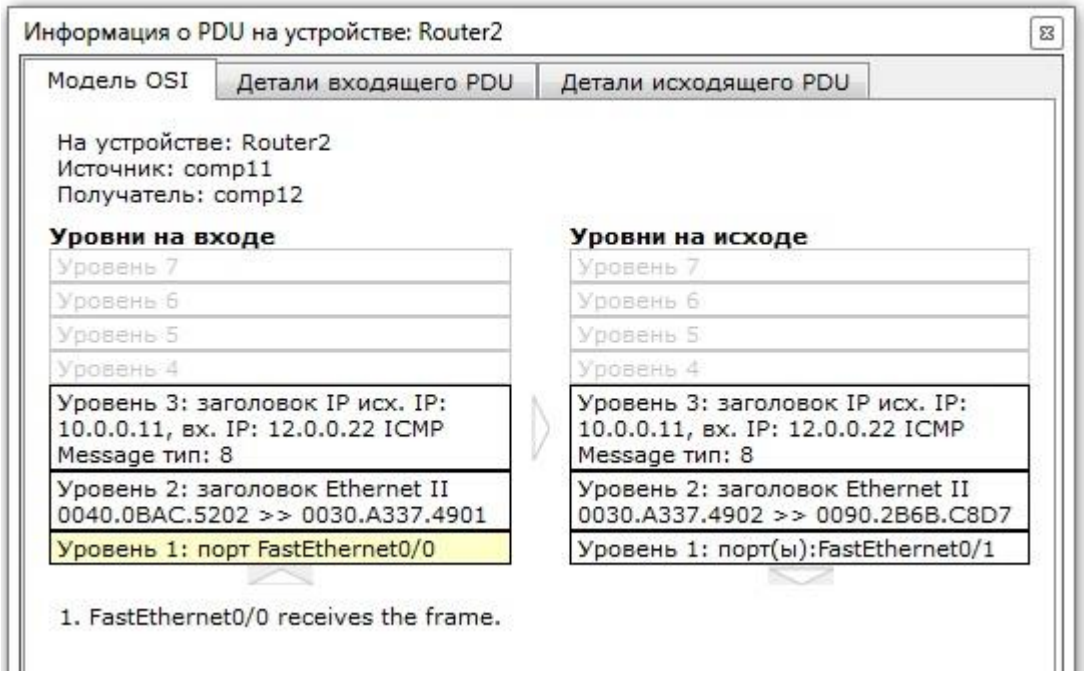


Рисунок 10.3 – Параметри пакета при проходженні Router2

При проходженні пакету через другий маршрутизатор IP-адрес відправника не змінився (10.0.0.11).

Сконфігуруйте NAT на маршрутизаторі Router1.

1. Для налаштування NAT на роутері необхідно виконати наступні кроки:

- знайдіть в налаштування Router1 підвкладку CLI
- для входу в режим адміністратора введіть команду enable (en)

Router> **en**

2. Для входу в режим налаштування введіть команду config t

Router # **config t**

3. Інтерфейс FastEthernet 0/0 є нашим внутрішнім інтерфейсом, до якого підключені робочі станції. Для налаштування NAT на роутері необхідно це позначити в налаштуваннях за допомогою наступних команд:

- увійдіть в налаштування інтерфейсу:

Router (config) # **int FastEthernet 0/0**

- оголосіть інтерфейс внутрішнім інтерфейсом:

Router (config-if) # **ip nat inside**

- вийдіть з налаштувань інтерфейсу

Router (config-if) # **exit**

4. Аналогічно налаштуйте інтерфейс FastEthernet 0/1, який підключений до мережі провайдера, лише з тією різницею, що він буде зовнішнім інтерфейсом NAT:

- увійдіть в налаштування інтерфейсу:

Router (config) # **int FastEthernet 0/1**

- оголосіть інтерфейс зовнішнім інтерфейсом NAT:

Router (config-if) # **ip nat outside**

- вицдіть з налаштувань інтерфейсу:

Router (config-if) # **exit**

5. Задайте пул зовнішніх адрес, в які транслюватимуться внутрішні адреси. Для задання пулу, який містить тільки один адреса - адреса зовнішнього інтерфейсу роутера - необхідно ввести команду:

Router (config) # **ip nat pool natpool 11.0.0.0 11.0.0.1 netmask 255.0.0.0**

При заданні пулу адрес необхідно вказати перший і останній адреси з вхідної в пул послідовності адрес. Якщо в пулі 1 адресу (як у нашому випадку) необхідно вказати його 2 рази.

6. Задайте список доступу:

Router (config) # **access-list 34 permit any**

Важливо: 34 - число від 1 до 99 позначає № списку доступу і задається адміністратором. Any - ключове слово, означає, що список доступу буде дозволяти пакети з будь-якою адресою відправника.

7. Введіть команду, яка, власне, і включає NAT на Router0. Команда є основною, але без задання всіх попередніх параметрів вона працювати не буде.

Router (config) # **ip nat inside source list 34 pool natpool overload**

Дана команда говорить роутеру, що у всіх пакетів, які отримані на внутрішній інтерфейс і дозволені списком доступу номер 34, адрес відправника буде трансльований на адресу з NAT пулу "natpool". Ключ overload вказує, що трансляції будуть перевантажені, дозволяючи кільком внутрішнім вузлам транслюватися на один IP адрес.

Тепер NAT налаштований, що підтверджується шляхом надсилання пакету з будь-якої робочої станції в підмережі на сервер google.com (пакет пройде). Якщо розглянути проходження пакету докладніше, перейшовши в режим симуляції, то побачимо, що при проходженні пакету через Router1 адрес відправника змінився (NAT налаштований).

Контрольні питання

1. Опишіть всі можливі схеми роботи служби NAT.
2. Які приватні IP адреси використовуються службою NAT в кожному класі адрес?
3. Перерахуйте переваги і недоліки служби NAT.
4. Перерахуйте етапи налаштування служби NAT.
5. Опишіть схему перевірки роботи служби NAT.
6. Опишіть основні проблеми в роботі сервера NAT.

Лабораторна робота №11
Віртуальні локальні мережі VLAN

Мета роботи: вивчення налаштування віртуальних локальних мереж VLAN із застосуванням додатку Cisco Packet Tracer

ТЕОРЕТИЧНІ ВІДОМОСТІ

11.1 Віртуальні локальні мережі VLAN

VLAN (аббр. від англ. Virtual Local Area Network) - логічна ("віртуальна") локальна комп'ютерна мережа, представляє собою групу хостів із загальним набором вимог, які взаємодіють так, як якщо б вони були підключені до широкомовному домену, незалежно від їх фізичного місцезнаходження. VLAN має ті ж властивості, що й фізична локальна мережа, але дозволяє кінцевим станціям групуватися разом, навіть якщо вони не знаходяться в одній фізичній мережі.

VLAN можуть бути налаштовані на комутаторах, маршрутизаторах, інших мережевих пристроях.

Переваги:

1 - Полегшує переміщення, додавання пристроїв і зміна їх з'єднань один з одним.

2 - Досягається велика ступінь адміністративного контролю внаслідок наявності пристрою, що здійснює між мережами VLAN маршрутизацію на 3-му рівні.

3 - Зменшується споживання смуги пропускання в порівнянні з ситуацією одного широкомовного домену.

4 - Скорочується невиробниче використання CPU за рахунок скорочення пересилання широкомовних повідомлень.

5 - Запобігання широкомовних штормів і запобігання петель.

11.2 Налаштування VLAN в одному комутаторі Cisco

У роботі розглянуто налаштування VLAN на комутаторі фірми Cisco на його портах доступу. Створіть мережу, логічна топологія якої представлена на рис.11.1. Комп'ютери з'єднані комутатором Cisco 2960-24TT. У таблиці 11.1 наведені адреси комп'ютерів.

Завдання роботи - зробити дві незалежні групи комп'ютерів: ПК0, ПК1 і ПК2 повинні бути доступні тільки один для одного, друга незалежна група - комп'ютери ПК3 і ПК4. Для цього створіть два окремих VLAN (рис.11.1)

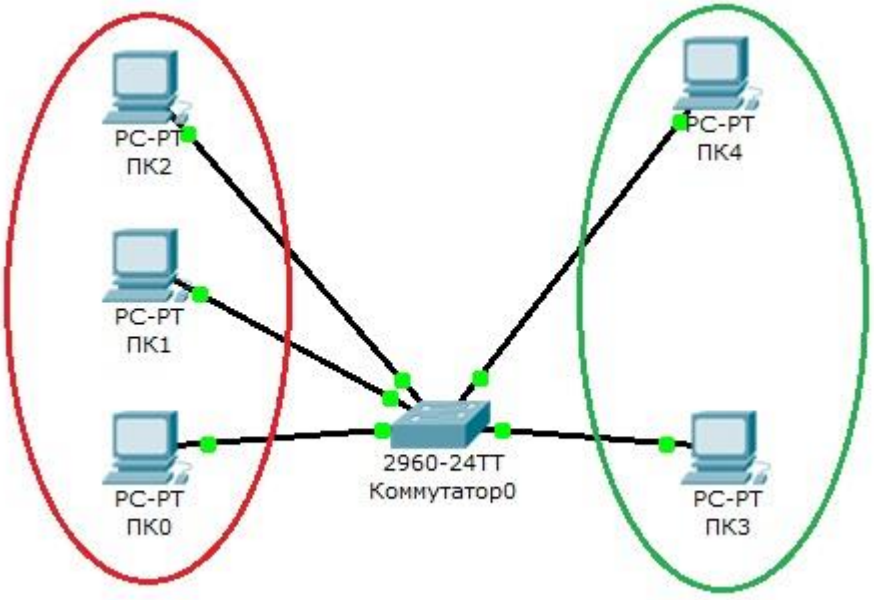


Рисунок 11.1 – Схема мережі з одним комутатором

Таблиця 11.1 – Адреси комп’ютерів

Комп'ютер	IP адреса	Порт комутатора
ПК0	10.0.0.1/8	1
ПК1	10.0.0.2/8	2
ПК2	10.0.0.3/8	3
ПК3	10.0.0.4/8	4
ПК4	10.0.0.5/8	5

Будемо вважати, що ПК0, ПК1 і ПК2 знаходяться в VLAN 2, а ПК3 і ПК4 знаходяться в VLAN 3.

Для перевірки конфігурації хоста ПК0 виконайте команду **ipconfig**. Результат виконання команди зображено на рис. 11.2. При бажанні можна виконати аналогічну перевірку на інших хостах.

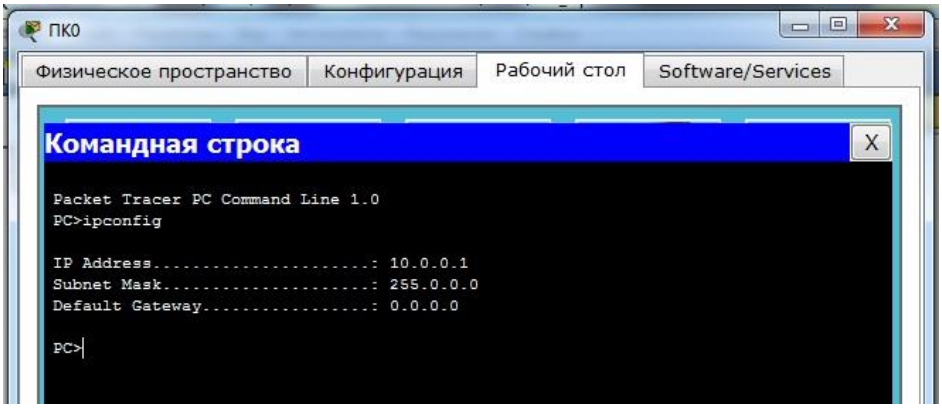


Рисунок 11.2 – Перевірка конфігурації хоста

Використовуючи команду **PING** перевірте зв'язок між всіма комп'ютерами. Зараз вони в одній мережі і всі доступні один для одного.

Тепер налаштуйте VLAN 2 і VLAN3, щоб структурувати мережі на комутаторі і навести в них лад.

Перейдіть до налаштування комутатора. Відкрийте його консоль. Для того щоб це виконати в Packet Tracer двічі клацніть лівою кнопкою миші по комутаторі на робочій області.

У вікні, перейдіть на вкладку CLI де розташоване вікно консолю. Натисніть Enter, щоб приступити до введення команд. Інформація, яка в даний момент відображена на консолі, свідчить про те що інтерфейси FasteEthernet 0/1 – FasteEthernet 0/5 знаходяться в робочому стані.

Перейдіть в привілейований режим виконавши команду **enable:**

Switch> **en**
Switch #

Перегляньте інформацію про існуючі на комутаторі VLAN-ах (рис.11.3). Для цього виконайтенаступну команду:

Switch # **sh vl br**

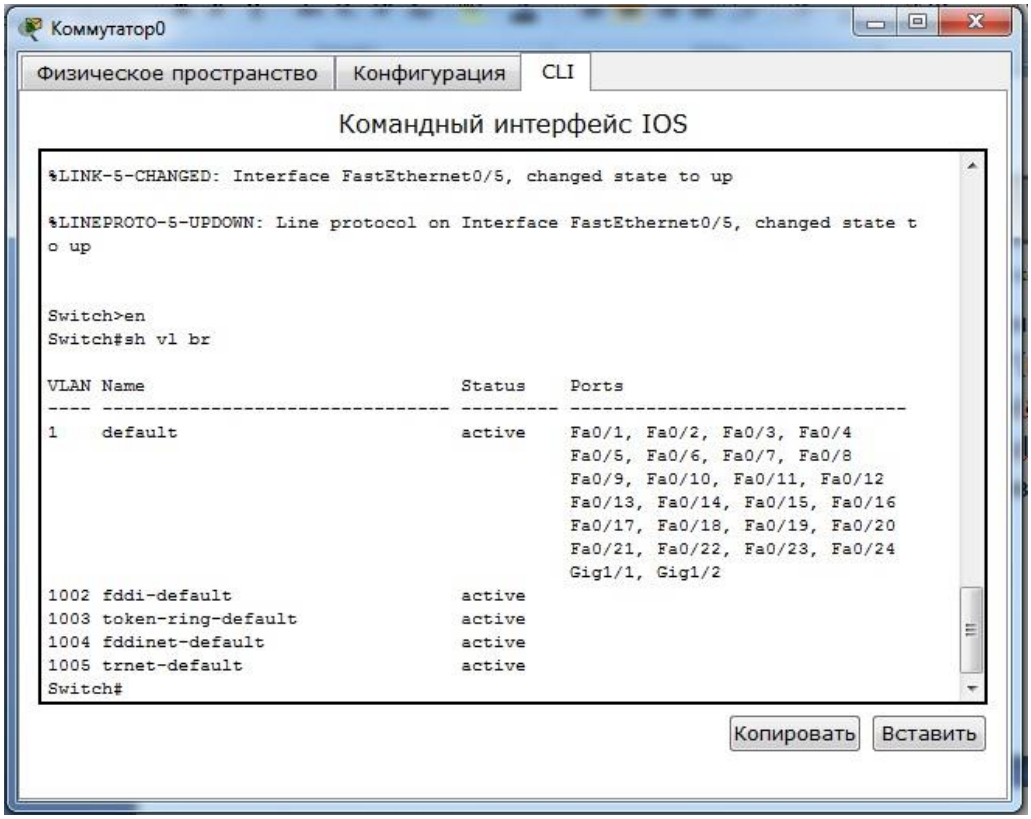


Рисунок 11.3 – Перегляд інформації про VLAN на комутаторі

В результаті виконання команди на екрані з'явиться:

- номера VLAN - перший стовпець,
- назва VLAN - другий стовпець,
- стан VLAN (працює він у даний момент чи ні) - третій стовпець,
- порти належать до даного VLAN - четвертий стовпець.

За замовчуванням на комутаторі існує п’ять VLAN-ів. Всі порти комутатора за замовчуванням належать VLAN1. Решта чотири VLAN є службовими і використовуються не дуже часто.

Для реалізації мережі, яку заплановано зробити, створіть на комутаторі ще два VLAN. Для цього в привілейованому режимі виконайте команду для переходу в режим конфігурації:

```
Switch # conf t
Enter configuration commands, one per line. End with CNTL / Z.
Switch (config) #
```

Введіть команду VLAN 2, яка створить на комутаторі VLAN з номером 2. Вказівник введення Switch (config) # зміниться на Switch (config-vlan) # це свідчитиме про те, що ви конфігуруєте вже не весь комутатор в цілому, а тільки окремий VLAN, в даному випадку VLAN номер 2. Якщо ви використовуєте команду «**vlan x**», де **x** номер VLAN, коли VLAN x ще не створений на комутаторі, то він буде автоматично створений і ви перейдете до його конфігурування. Перебуваючи в режимі конфігурування VLAN, можлива зміна параметрів обраної віртуальної мережі, наприклад можна змінити її ім'я за допомогою команди **name**.

Для досягнення поставленої в даному пості завдання, сконфігуруйте VLAN 2 наступним чином:

```
Switch (config) # vlan 2
Switch (config-vlan) # name subnet_10
Switch (config) # interface range fastEthernet 0 / 1-3
Switch (config-if-range) # switchport mode access
Switch (config-if-range) # switchport access vlan 2
```

Розберемо цю конфігурацію. Як уже говорилося раніше командою VLAN 2 створено на комутаторі новий VLAN з номером 2. Команда **name subnet_10** присвоює ім'я subnet_10 віртуальної мережі номер 2. Виконуючи команду **interface range fastEthernet 0/1-3** ми переходимо до конфігурації інтерфейсів fastEtherne t0/1, fastEthernet 0/2 і fastEthernet 0/3 комутатора. Ключове слово **range** в даній команді, вказує на те, що ми будемо конфігурувати не один єдиний порт, а цілий діапазон портів, в принципі її можна не використовувати, але тоді останні три рядки доведеться замінити на:

```
Switch (config) # interface fastEthernet 0/1
Switch (config-if) # switchport mode access
Switch (config-if) # switchport access vlan 2
Switch (config) # interface fastEthernet 0/2
Switch (config-if) # switchport mode access
Switch (config-if) # switchport access vlan 2
Switch (config) # interface fastEthernet 0/3
```

Switch (config-if) # **switchport mode access**
Switch (config-if) # **switchport access vlan 2**

Команда **switchport mode access** конфігурує обраний порт комутатора, як порт доступу (аксесуари порт).

Команда **switchport access vlan 2** вказує, що даний порт є портом доступу для VLAN номер 2.

Вийдіть з режиму конфігурації, двічі набравши команду **exit** і перегляньте результат конфігурування (рис.11.4), виконавши команду **sh vl br** ще раз.

```
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig1/1, Gig1/2
2    subnet_10                         active    Fa0/1, Fa0/2, Fa0/3
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Рисунок 11.4 – Розподіл портів на VLAN

На комутаторі з'явився ще один VLAN з номером 2 і ім'ям subnet_10, портами доступу якого є fastEthernet 0/1, fastEthernet 0/2 і fastEthernet 0/3.

Аналогічним чином створіть VLAN 3 з ім'ям subnet_192 і зробіть його портами доступу інтерфейсів fastEthernet 0/4 і fastEthernet 0/5. Результат повинен вийти наступним (рис.11.5).

```
Switch#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                 Gig1/2
2    subnet_10                         active    Fa0/1, Fa0/2, Fa0/3
3    subnet_192                        active    Fa0/4, Fa0/5
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Рисунок 11.5 – Розподіл портів на VLAN

Наступним етапом є тестування створених мереж. Перейдіть в консоль комп'ютера ПК0. Пропінгуйте з нього інші комп'ютери мережі. Комп'ютери ПК1 і ПК2 доступні, а комп'ютери ПК3 і ПК4 не доступні. Всі п'ять комп'ютерів теоретично повинні знаходиться в одній підмережі 10.0.0.0/8 і бачити один одного, на практиці вони знаходяться в різних віртуальних локальних мережах і тому не можуть взаємодіяти між собою.

11.3 Налаштування VLAN на двох комутаторах Cisco

Створіть мережу, логічна топологія якої представлена на рис.11.6. Комп'ютери з'єднані комутатором Cisco 2950-24. У таблиці 11.2 наведено адреси комп'ютерів.

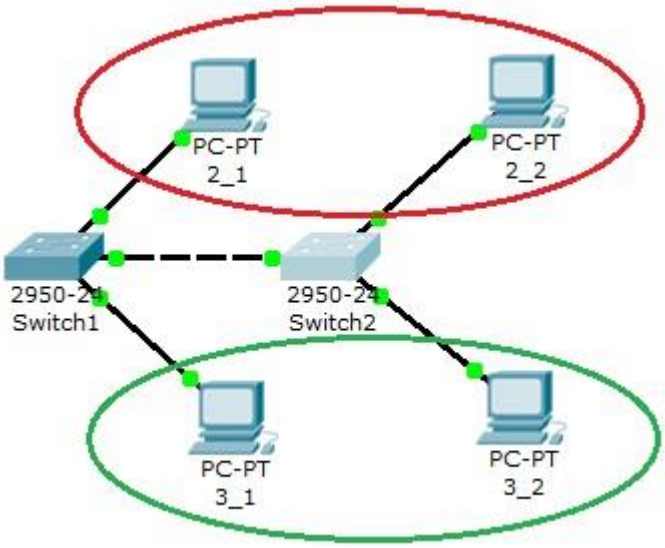


Рисунок 11.6 – Схема мережі

Таблиця 11.2 – Адреси комп’ютерів

Комп'ютер	IP адреса	Комутатор	Порт комутатора	VLAN
2_1	10.0.0.1/8	Switch1	1	VLAN 20
2_2	10.0.0.3/8	Switch2	1	VLAN 20
3_1	10.0.0.2/8	Switch1	2	VLAN 30
3_2	10.0.0.4/8	Switch2	2	VLAN 30

<удемо вважати, що 2_1 і 2_2 знаходяться в VLAN 20, а 3_1 і 3_2 знаходяться в VLAN 30.

Перевірпт зв'язність отриманої мережі шляхом пінгування з 2_1 всі інші комп'ютери. Оскільки поки в мережі немає поділу на VLAN, то всі комп'ютери повинні бути доступними.

Налаштуйте VLAN 20 і VLAN30, щоб структурувати мережі на комутаторах.

Перейдіть до налаштування комутатора Switch1. Відкрийте його консоль. У вікні, перейдіть на вкладку CLI, увійдіть в привілейований режим і налаштуйте VLAN 20 і VLAN30 згідно таблиці 11.2.

Створіть на комутаторі VLAN 20 шляхом виконання наступної команди . в привілейованому режимі:

Switch1 # **conf t**
Enter configuration commands, one per line. End with CNTL / Z.
Switch (config) #

для переходу в режим конфігурації і налаштуйте VLAN 20 і VLAN 30 наступним чином:

Switch1 (config) # **vlan 20**
Switch1 (config) # **interface fastEthernet 0/1**
Switch1 (config-if-range) # **switchport mode access**
Switch1 (config-if-range) # **switchport access vlan 20**
Switch1 (config-if-range) # **exit**
Switch1 (config) # **vlan 30**
Switch1 (config) # **interface fastEthernet 0/2**
Switch1 (config-if-range) # **switchport mode access**
Switch1 (config-if-range) # **switchport access vlan 30**

Перегляньте інформацію про існуючі на комутаторі VLAN-ах командою:

Switch1 # **sh vl br**

Повинен вийде результат, який зображено на рис.11.7.

```
Switch1#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
20   VLAN0020                          active    Fa0/1
30   VLAN0030                          active    Fa0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch1#
```

Рисунок 11.7 – Конфігурація Switch1

Аналогічним чином налаштуйте Switch2 (рис. 11.8).

```
Switch2#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
20   VLAN0020                          active    Fa0/1
30   VLAN0030                          active    Fa0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch2#
```

Рисунок 11.8 – Конфігурація Switch2

Оскільки в даний момент немає обміну інформації про VLAN, то комп'ютери будуть пінгувати тільки себе.

Тепер організуйте магістраль обміну між комутаторами. Для цього налаштуйте третій порт на кожному комутаторі як транковий.

Увійдіть в консоль комутатора Switch1 і задайте транковий порт:

Switch1> **en**
Switch1 # **conf t**
Switch1 (config) # **interface fastEthernet 0/3**
Switch1 (config) # **switchport mode trunk**
Switch1 (config) # **no shutdown**
Switch1 (config) # **exit**

Відкрийте конфігурацію комутатора на інтерфейсі FastEthernet 0/3 і переконайтеся, що порт транковий (рис.11.9).

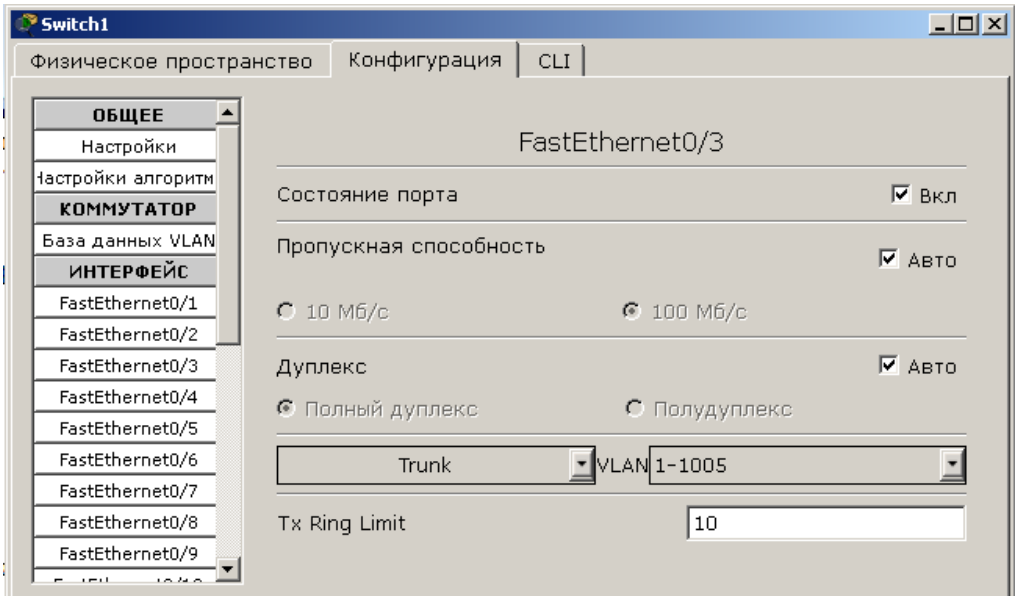


Рисунок11.9 – Конфігурація інтерфейсу FastEthernet 0/3

На комутаторі Switch2 інтерфейс FastEthernet 0/3 автоматично налаштується як транковий.

Тепер комп'ютери, що входять в один VLAN повинні пінгувати. У вас повинна з'явитися зв'язок між комп'ютерами 2_1 і 2_2, а так само між 3_1 і 3_2, комп'ютери в іншому VLAN будуть недоступними.

Збережіть схему мережі.

Об'єднайте дві віртуальні мережі за допомогою маршрутизатора.

Додайте в схему мережі маршрутизатор, як зображено на рис.11.10. Маршрутизатор з'єднаний з інтерфейсами **fastEthernet 0/4** комутаторів.

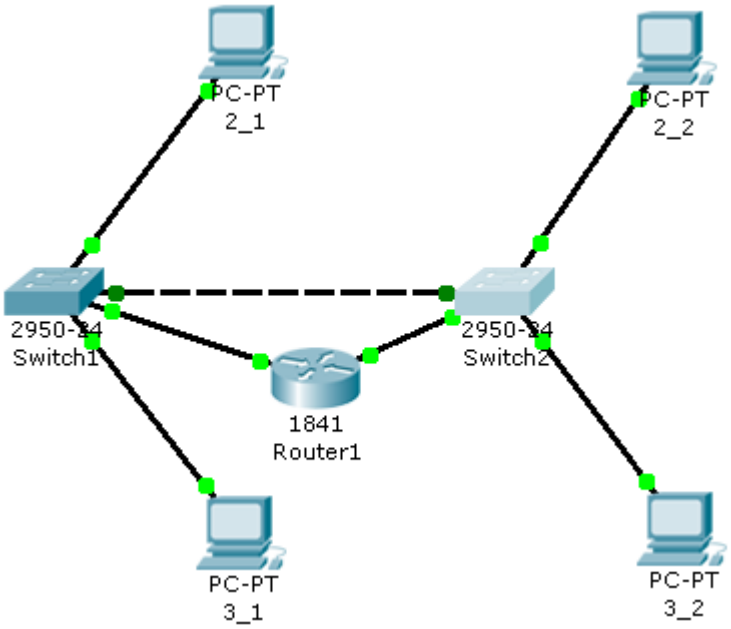


Рисунок 11.10 – Схема мережі

Розбийте нашу мережу 10.0.0.0 на дві підмережі: 10.2.0.0 та 10.3.0.0. Для цього поміняйте IP адреси і маску підмережі на 255.255.0.0, як зазначено в таблиці 11.3.

Таблиця 11.3 – Адреси комп'ютерів

Комп'ютер	IP адреса	Комутатор	Порт комутатора	VLAN
2_1	10.2.0.1/16	Switch1	1	VLAN 20
2_2	10.2.0.3/16	Switch2	1	VLAN 20
3_1	10.3.0.2/16	Switch1	2	VLAN 30
3_2	10.3.0.4/16	Switch2	2	VLAN 30

Комп'ютери повинні пінгуватися в межах одного VLAN і однієї підмережі.

Позначимо на комутаторах інтерфейси, приєднані до маршрутизатора у віртуальні мережі.

Увійдіть в конфігурацію першого комутатора Switch1 і задайте параметри четвертого порту:

Switch1 (config) # **interface fastEthernet 0/4**
Switch1 (config-if) # **switchport access vlan 20**

Перевірте налаштування першого комутатора Switch1 (рис.11.11).

```
Switch1#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
20   VLAN0020                          active    Fa0/1, Fa0/4
30   VLAN0030                          active    Fa0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch1#
```

Рисунок 11.11 – Налаштування комутатора Switch1

Увійдіть в конфігурацію другого комутатора Switch2 і задайте параметри четвертого порту:

Switch2 (config) # **interface fastEthernet 0/4**
Switch2 (config-if) # **switchport access vlan 30**

Перевірте налаштування другого комутатора Switch2 (рис.11.12).

```
Switch2#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
20   VLAN0020                          active    Fa0/1
30   VLAN0030                          active    Fa0/2, Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch2#
```

Рисунок 11.12 – Налаштування комутатора Switch2

Увійдіть в конфігурацію маршрутизатора і налаштуйте IP адреси на маршрутизаторі:

Router1 (config-if) # **interface fa0 / 0**
Router1 (config-if) # **ip address 10.2.0.254 255.255.0.0**
Router1 (config-if) # **no shutdown**
Router1 (config-if) # **interface fa0 / 1**
Router1 (config-if) # **ip address 10.3.0.254 255.255.0.0**
Router1 (config-if) # **no shutdown**

З цього моменту ми встановили маршрутизацію між двома підмережами. Залишилося встановити шлюзи на комп'ютерах (таблиця 11.4).

Таблиця 11.4 – Шлюзи

Комп'ютер	Gataway
2_1	10.2.0.254
2_2	10.2.0.254
3_1	10.3.0.254
3_2	10.3.0.254

Перевірте доступність комп'ютерів в мережі. Тепер всі комп'ютери повинні бути доступні і всі адреси повинні пінгувати.

11.4 Налаштування VLAN в корпоративній мережі.

Створіть схему мережі (рис.11.13):

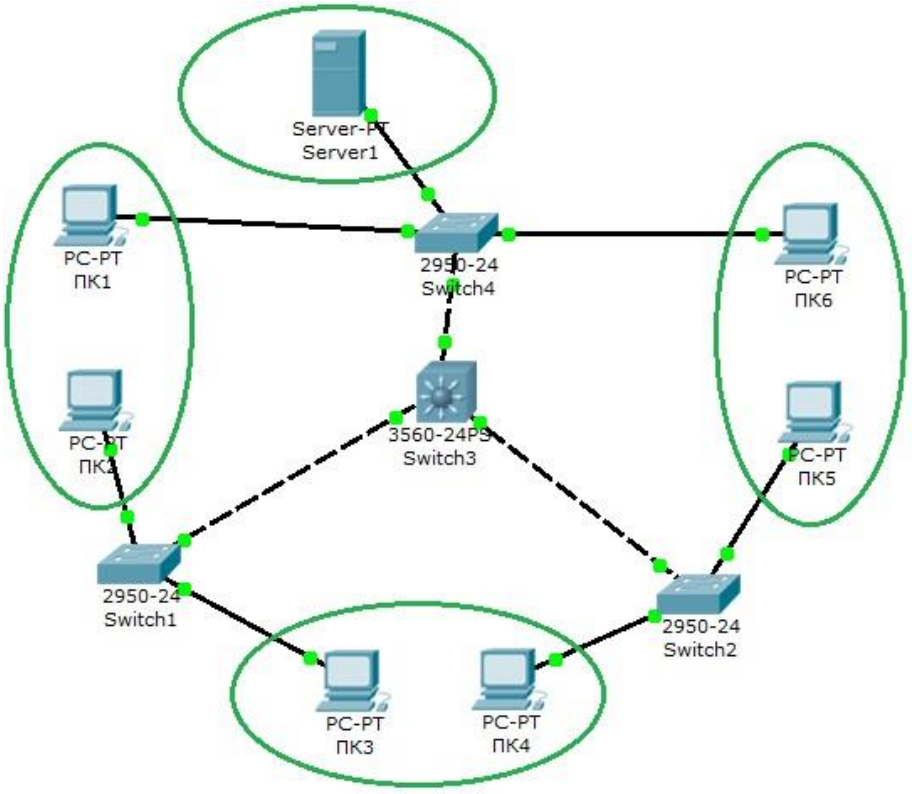


Рисунок 11.13 – Схема корпоративної мережі

Склад мережі:
- Три комутатора другого рівня розподілу 2950-24 (Switch1, Switch2, Switch4);
- Центральний комутатор третього рівня 3560-24PS (Switch3), що виконує роль роутера;
- Сервер (Server1);
- Три підмережі по два вузли в кожній

Задача:

Для будь-якого VLAN можуть бути доступні тільки вузли цього ж VLAN і сервер Server1.

У таблиці 11.5 та 11.6 наведено дані для установки параметрів комп'ютерів і комутаторів.

Таблиця 11.5 – Конфігурація комп'ютерів

Комп'ютер	IP адреса	Комутатор	Порт комутатора	VLAN
ПК1	10.11.0.11/16	Switch4	4	VLAN 11
ПК2	10.11.0.2/16	Switch1	1	VLAN 11
ПК3	10.13.0.3/16	Switch1	2	VLAN 13
ПК4	10.13.0.4/16	Switch2	1	VLAN 13
ПК5	10.12.0.5/16	Switch2	2	VLAN 12
ПК6	10.12.0.6/16	Switch4	2	VLAN 12
Server1	10.10.0.7/16	Switch4	1	VLAN 10

Таблиця 11.6 – Зв'язок комутаторів по портах

Порт центрального комутатора Switch3	Порт комутатора другого рівня розподілу
1	Switch1 - 3 порт
2	Switch4 - 3 порт
3	Switch2 - 3 порт

Після налаштування всіх комутаторів встановіть самостійно шлюзи на всіх комп'ютерах і сервері.

Конфігуруйте центральний комутатор:

Етап 1.

Перейдіть до конфігурації центрального комутатора Switch3 і створіть на ньому базу VLAN.

1. Створіть VLAN 10:

```
Switch3> en
Switch3 # conf t
Switch3 (config) # vlan 10
Switch3 (config-vlan) # exit
```

2. Створіть VLAN 11, VLAN 12 і VLAN 13.

3. Налаштуйте протокол VTP в режимі сервера:

Switch3 (config) # **vtp domain HOME**
Switch3 (config) # **vtp password HOME**
Switch3 (config) # **vtp mode server**

4. Перегляньте інформацію про конфігурацію VTP:

Switch # **sh vtp status**

5. Налаштуйте всі інтерфейси на транк:

Switch3 (config) # **int fa0 / 1**
Switch3 (config-if) # **switchport mode trunk**
Switch3 (config-if) # **exit**

і повторіть ці налаштування для другого і третього інтерфейсів.

Етап 2.

Перейдіть до конфігурації комутатора Switch4 і переведіть його в режим client:

1. Створіть на комутаторі VLAN 10 і задайте в ньому порт 1 як access порт:

Switch4> **en**
Switch4 # **conf t**
Switch4 (config) # **vlan 10**
Switch4 (config-vlan) # **exit**
Switch4 (config) # **int fa0 / 1**
Switch4 (config-if) # **switchport access vlan 10**
Switch4 (config-if) # **switchport mode access**
Switch4 (config-if) # **no shut**

2. Створіть на комутаторі VLAN 11 і задайте в ньому порт 4 як access порт.
3. Створіть на комутаторі VLAN 12 і задайте в ньому порт 2 як access порт.
4. Переведіть комутатор в режим clint:

Switch4 (config) # **vtp domain HOME**
Switch4 (config) # **vtp password HOME**
Switch4 (config) # **vtp mode client**

ВАЖЛИВО! При введенні імені домену та пароля дотримуйтеся потрібного регістра.

Етап 4.

Перейдіть до конфігурації комутатора Switch1 і виподніте наступні налаштування:

1. Створіть на комутаторі VLAN 11 і задайте в ньому порт 1 як access порт.

2. Створіть на комутаторі VLAN 13 і задайте в ньому порт 2 як access порт.
3. Переведіть комутатор в режим client.

Етап 5.

Перейдіть до конфігурації комутатора Switch2.

1. Створіть на комутаторі VLAN 12 і задайте в ньому порт 2 як access порт.
2. Створіть на комутаторі VLAN 13 і задайте в ньому порт 1 як access порт.
3. Переведіть комутатор в режим client.

Етап 6.

Перевірте працездатність мережі на канальному рівні моделі OSI.

Після встановлення всіх налаштувань таблиця VLAN розійдеться по коммутаторам за допомогою протоколу VTP.

В результаті комп'ютери, розташовані в одному Віллані, будуть доступні один для одного, а інші комп'ютери недоступні. Перевірте зв'язок командою PING між наступними парами комп'ютерів:

- ПК1 - ПК2;
- ПК3 - ПК4;
- ПК5 - ПК6.

Якщо Ви все зробили правильно, то ping між парами пройде, якщо ні - перевірте наступні установки:

- Транкового портами є: на Switch3 всі порти, на Switch1, Switch2 і Switch4 - третій порт;
- Сполуки інтерфейсів на комутаторах;
- Назви і паролі доменів на кожному комутаторі (команда sh vtp status);
- Прив'язку інтерфейсів до вілланам на комутаторах (команда sh vl br).

Етап 7.

Налаштування маршрутизації на центральному комутаторі.

Створимо інтерфейси для кожного VLAN.

Налаштування інтерфейсу для vlan 10 (шлюз за замовчуванням):

Switch3 (config) # **int vlan 10**
Switch3 (config-if) # **ip address 10.10.0.1 255.255.0.0**
Switch3 (config-if) # **no shut**
Switch3 (config-if) # **exit**

Повторіть ці настройки для кожного VLAN, задаючи адресу IP: 10. [VLAN] .0.1 і маску / 16.

Після цього зайдіть в налаштування кожного комп'ютера і встановіть потрібний шлюз за замовчуванням. Наприклад для ПК1 - 10.11.0.1.

Увімкніть маршрутизацію командою:

Switch3 (config) # **ip routing**

Етап 8.

Перевірте працездатність мережі на мережевому рівні моделі OSI.

Після включення маршрутизації всі комп'ютери будуть доступні з будь-якого хоста.

Етап 9.

Виконаємо основну задачу роботи: для будь-якого Віла можуть бути доступні тільки вузли цього ж Віла і сервер Server1.

Для цього введемо такі обмеження на трафік мережі:

1 - Дозволити пакети від будь-якого хоста до сервера.

2 - Дозволити пакети від сервера до будь-якого хоста.

3 - Трафік від однієї підмережі до цієї ж підмережі дозволити.

4 - Правило за замовчуванням: заборонити все інше.

Обмеження на трафік мережі задаються за допомогою команди фільтрації **access-list.** Дана команда задає критерії фільтрації в списку опцій дозволу і заборони, званому списком доступу. Списки доступу мають два правила: **permit** - дозволити і **deny** - заборонити. Дані правила або пропускають пакет далі по мережі, або блокують його доступ.

Більш докладно списки доступу будуть розглянуті в лабораторній роботі №14.

Відкриваємо центральний комутатор (Switch3) і міняємо його конфігурацію за допомогою команди фільтрації **access-list:**

Switch3 (config) # **ip access-list extended 100**

(Створюється розширений список доступу під номером 100)

Switch3 (config-ext-nacl) # **permit ip any 10.10.0.0 0.0.0.255**
Switch3 (config-ext-nacl) # **permit ip 10.10.0.0 0.0.0.255 any**

(Дозволяється доступ до мережі 10.10.0.0/24)

Switch3 (config-ext-nacl) # **permit ip 10.11.0.0 0.0.0.255 10.11.0.0 0.0.0.255**
Switch3 (config-ext-nacl) # **permit ip 10.12.0.0 0.0.0.255 10.12.0.0 0.0.0.255**
Switch3 (config-ext-nacl) # **permit ip 10.13.0.0 0.0.0.255 10.13.0.0 0.0.0.255**

(Дозволяється: доступ з мережі 10.11.0.0/24 в цю ж мережу;

доступ з мережі 10.12.0.0/24 в цю ж мережу;
доступ з мережі 10.13.0.0/24 в цю ж мережу).

Switch3 (config-ext-nacl) # **exit**

Тепер цей access-list накладемо на конкретний інтерфейс і застосуємо до всіх VLAN-ам на вхідний трафік (опція **in -** на вхідний трафік, **out -** на вихідний трафік):

Switch3 (config) # **int vlan 10**

Switch3 (config-if) # **ip access-group 100 in**

Цей крок повторюємо для кожного з VLAN-ів.

В результаті отримаємо: для будь-якого VLAN можуть бути доступні тільки вузли цього ж VLAN і сервер Server1.

Завдання

На підприємстві є два відділи, схема мереж яких представлена на рис.11.14.

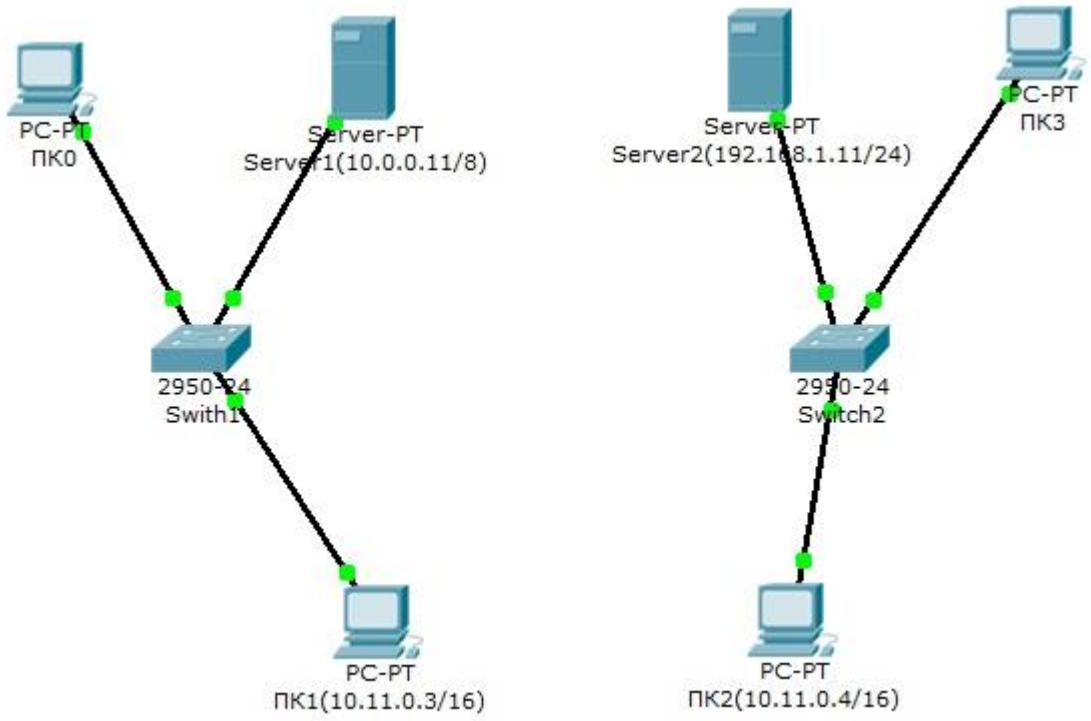


Рисунок 11.14 – Схема мереж відділів підприємства

Відділ 1 - Switch1, відділ 2 - Switch2.

У кожній мережі є сервер зі службами DHCP, DNS і HTTP (на серверах Server1 і Server2 розташовані інтернет-сайти відділів).

Комп'ютери ПК0 і ПК3 з DHCP серверів своїх мереж отримують параметри IP адреси і шлюз.

Комп'ютери ПК1 і ПК2 знаходяться в окремій мережі в одному VLAN.

Доповніть схему мережі маршрутизатором або комутатором третього рівня, щоб забезпечити роботу корпоративної мережі в наступних режимах:
1 - комп'ютери ПК0 і ПК3 повинні відкривати сайти кожного відділу;
2 - комп'ютери ПК1 і ПК2 повинні бути доступні тільки один для одного.

Контрольні питання

1. Для чого створюються віртуальні локальні мережі? Які їх переваги?
2. Як зв'язуються між собою VLAN і порти комутатора?

3. Як забезпечується спілкування між вузлами різних віртуальних мереж?

4. Як забезпечується управління віртуальними локальними мережами?

5. Чи можна побудувати VLAN на декількох комутаторах? Як це зробити?

6. Для чого служить ідентифікатор кадру (tag)? Де він розміщується?

7. Що таке транк? Як він створюється на комутаторі і маршрутизаторі?

8. Які команди використовуються для призначення VLAN на інтерфейси?

9. Які команди використовуються для створення транкових з'єднань?

10. Які команди використовуються для верифікації VLAN?