МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

НКЦ заочної освіти

Кафедра інформаційних технологій

Бакалаврська кваліфікаційна робота

на тему: Проектування та конфігурування комп'ютерної мережі підприємства на базі обладнання Cisco

Виконав студент 5 курсу групи КН-5
Напрям 6.050101 комп'ютерні науки
Магерко Іван Володимирович

Керівник д.т.н., професор
Андрощук Олександр Степанович

Консультант

Рецензент д.т.н., професор
Мещеряков Володимир Іванович

Одеса 2020

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ЄМПД – єдина мережа передачі даних

ЛОМ – локальна обчислювальна мережа

ARP – Address Resolution Protocol (Протокол визначення адреси)

CDP – Cisco Discovery Protocol (Пропріетарний протокол Cisco)

CIDR – Classless Inter-Domain Routing (Безкласова адресація)

CLI – Command Line Interface (Інтерфейс командного рядка)

DHCP –Dynamic Host Configuration Protocol (Протокол динамічної настройки вузла)

EIGRP –Enhanced Interior Gateway Routing Protocol (Вдосконалений дистанційно-векторний протокол динамічної маршрутизації)

HTTP –HyperText Transfer Protocol (Протокол передачі гіпертексту)

ICMP –Internet Control Message Protocol (Протокол міжмережевих керуючих повідомлень)

IEEE – Institute of Electrical and Electronic Engineers (Інститут інженерів з електротехніки та електроніки)

IP – Internet Protocol (Інтернет-протокол міжмережевого обміну даних)

ISO –International Organization for Standardization(Міжнародна організація по стандартизації)

LAN – Local Area Network (Локальна обчислювальна мережа)

MAC – Media Access Control (Управління доступом до середовища)

MIMO –Multiple Input, Multiple Output (Багато входів, багато виходів)

OSI – Open System Interconnection (Взаємодія відкритих

систем)

QoS – Quality of Service (Якість надання послуг)

RIP – Routing Information Protocol (Протокол маршрутної інформації)

TCP – Transmission Control Protocol (Протокол управління передачею)

UDP – User Datagram Protocol (Протокол передачі даних користувача)

VLAN –Virtual Local Area Network (Віртуальна локальна мережа)

WFQ –Weighted Fair Queueing (Зважена справедлива черга)

WLAN –Wireless Local Network (Бездротова локальна мережа)

WRED –Weighted Random Early Detection (Виважене довільне раннє виявлення)

ВСТУП

Корпоративна мережа – комунікаційна система, що належить і/або керована єдиною організацією відповідно до правил цієї організації. Інтранет (intranet) – це приватна мережа всередині підприємства, захищена від несанкціонованого доступу, що володіє розширеними можливостями завдяки використанню протоколу IP і маршрутизації пакетів даних. У інтранет можуть застосовуватися технології Інтернет, інтранет можна визначити і як систему зберігання, передачі, обробки та доступу до інформації підприємства з використанням засобів локальних мереж і мережі Інтернет.

Створення комп'ютерної мережі підприємства дає наступні переваги:

– більш зручний і спрощений документообіг всередині організації;

– організація електронної бази даних, що спрощує роботу з нею і полегшує додавання нової інформації;

– спільний доступ декількох осіб до одного документу;

– спільна обробка інформації;

– зручність створення виходу в мережу Internet.

Всі достоїнства комп’ютерної мережі можна реалізувати тільки при грамотному виборі моделі, топології, апаратних і програмних засобів.

Метою бакалаврської роботи є проектування та конфігурування єдиної мережі передачі даних з використанням бездротового сегменту, побудованого за технологією Wi-Fi, на базі мережевого обладнання Cisco відповідно до технічного завдання замовника.

На підставі вихідної топології ядра мережі, в роботі необхідно виконати проектування єдиної мережі передачі даних, шляхом формування окремих підмереж із заданою кількістю робочих станцій в кожній.

Для досягнення поставленої мети в роботі необхідно вирішити наступні завдання:

– побудувати граф єдиної мережі передачі даних;

− обґрунтувати перелік технічних засобів (кількість необхідного телекомунікаційного обладнання, конфігурацію кожного елемента мережі, тип ліній зв'язку, технологію опорної мережі і пропускну здатність);

− підготувати IP-план адресації підмереж робочих станцій і підмереж маршрутизаторів відповідно до принципів безкласової адресації (CIDR);

− сформувати таблиці маршрутизації для статичної маршрутизації транспортного ядра єдиної мережі передачі даних;

− доповнити структуровану кабельну систему мережі обладнанням бездротового доступу, що підтримує стандарт IEEE 802.11;

− для перевірки працездатності проектованої мережі виконати її моделювання в мережевому емуляторі Cisco Packet Tracer.

Структура кваліфікаційної роботи складається з вступу, п’яти розділів, висновків, переліку посилань на 16 найменувань, додатків. Повний обсяг проекту становить 68 сторінок, містить 21 рисунок і 3 таблиці.

1 СТАНДАРТИЗАЦІЯ ТА КЛАСИФІКАЦІЯ МЕРЕЖ

1.1 Еталонна модель OSI

Важливим елементом стандартизації мереж є еталонна модель OSI (рис. 1.1), що була розроблена Міжнародною організацією по стандартизації ISO. Модель OSI визначає, по-перше, рівні взаємодії систем в мережах з комутацією пакетів, по-друге, стандартні назви рівнів, по-третє, функції, які повинен виконувати кожен рівень. Модель OSI не містить описів реалізацій конкретного набору протоколів.

У моделі OSI засоби взаємодії діляться на сім рівнів: прикладний, рівень представлень, сеансовий, транспортний, мережевий, канальний і фізичний. Кожний рівень пов'язаний з абсолютно певним аспектом взаємодії мережевих пристроїв.

Модель OSI описує тільки системні засоби взаємодії, що реалізовуються операційною системою, системними утилітами, системними апаратними засобами. Модель не включає засоби взаємодії застосунків кінцевих користувачів.

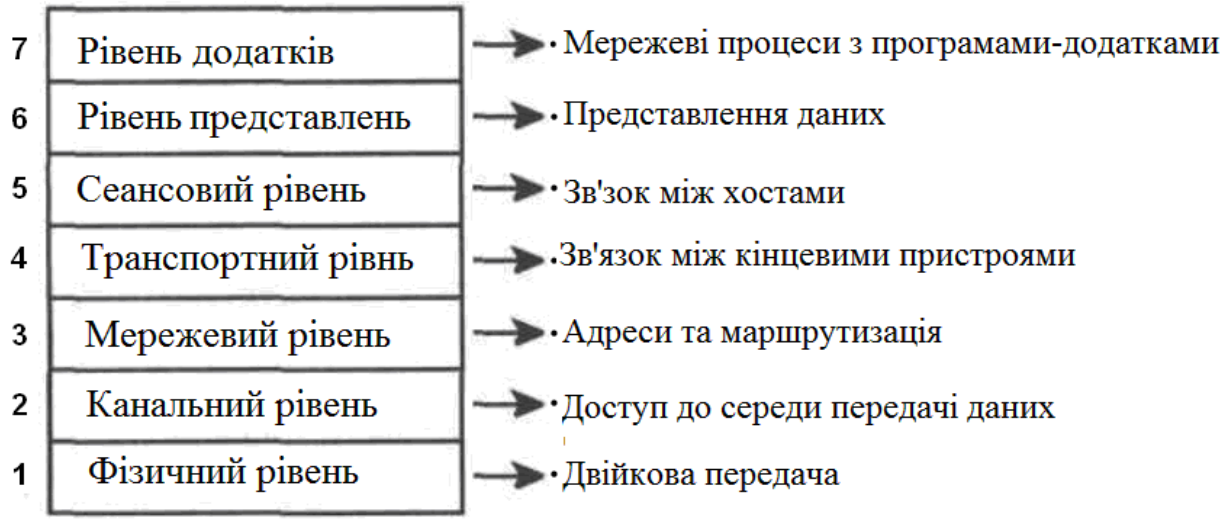

Рисунок 1.1 – Еталонна модель OSI

Модель OSI має сім рівнів. Поява саме такої структури було обумовлено наступними міркуваннями [1][1)]:

1) Рівень повинен створюватися в міру необхідності окремого рівня абстракції.

2) Кожен рівень повинен виконувати строго певну функцію.

3) Вибір функцій для кожного рівня повинен здійснюватися з урахуванням створення стандартизованих міжнародних протоколів.

4) Межі між рівнями повинні вибиратися так, щоб потік даних між інтерфейсами був мінімальним.

5) Кількість рівнів має бути достатньо великим, щоб різні функції не об'єднувалися в одному рівні без необхідності, але не надто високим, щоб архітектура не ставала громіздкою.

Модель OSI не є мережевою архітектурою, оскільки вона не описує служби та протоколи, що використовуються на кожному рівні. Вона просто визначає, що повинен робити кожен рівень. Нижче розглянемо кожен рівень моделі, починаючи з самого нижнього.

Фізичний рівень займається реальною передачею необроблених бітів по каналу зв'язку. При розробці мережі необхідно переконатися, що коли одна сторона передає одиницю, то приймаюча сторона отримує також одиницю, а не нуль. Принциповими питаннями тут є наступні: яка напруга має використовуватися для відображення одиниці, а яка для нуля; скільки мікросекунд триває біт; чи може передача проводитися одночасно в двох напрямках; як встановлюється початковий зв'язок і як він припиняється, коли обидві сторони закінчили свої завдання; з якої кількості проводів повинен складатися кабель і яка функція кожного проводу. Питання розробки в основному пов'язані з механічними, електричними і процедурними інтерфейсами, а також з фізичним носієм, що лежить нижче фізичного рівня.

[1)] [1] Олифер В.Г., Н.А. Олифер Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов, 4–е изд. СПб.: Питер, 2010. 944 с.

Основне завдання канального рівня – бути здатним передавати «сирі» дані фізичного рівня по надійної лінії зв'язку, вільної від невиявлених помилок, і маскувати реальні помилки, так щоб мережевий рівень їх не бачив. Це завдання виконується за допомогою розбиття вхідних даних на кадри, звичайний розмір яких коливається від кількох сотень до кількох тисяч байт. Кадри даних передаються послідовно з обробкою кадрів підтвердження, які відсилаються назад одержувачем.

Ще одна проблема, що виникає на канальному рівні (а також і на більшій частині більш високих рівнів), – як не допустити ситуації, коли швидкий передавач завалює приймач даними. Може бути передбачений якийсь механізм регуляції, який інформував би передавач про наявність вільного місця в буфері приймача на поточний момент.

У широкомовних мережах існує ще одна проблема канального рівня: як керувати доступом до каналу, що спільно використовується. Ця проблема вирішується введенням спеціального додаткового підрівня канального рівня – підрівня доступу до носія.

Мережевий рівень займається керуванням операціями підмережі. Найважливішим моментом тут є визначення маршрутів пересилки пакетів від джерела до пункту призначення. Маршрути можуть бути жорстко задані у вигляді таблиць і рідко змінюватися або, що буває частіше, автоматично змінюватися, щоб уникати компонентів, які відмовили. Крім того, вони можуть задаватися на початку кожного з'єднання, наприклад, термінальної сесії, такого як підключення до віддаленої машині. Нарешті, вони можуть бути у високому ступені динамічними, тобто обчислюваними заново для кожного пакета з урахуванням поточної завантаженості мережі.

Якщо в підмережі одночасно присутня дуже велика кількість пакетів, то вони можуть закрити дорогу один одному, утворюючи затори у вузьких місцях. Недопущення подібної закупорки також є завданням мережевого рівня в з'єднанні з більш високими рівнями, які адаптують завантаження. У

більш загальному сенсі, мережевий рівень займається наданням певного рівня сервісу (це стосується затримок, часу передачі, питань синхронізації).

При подорожі пакета з однієї мережі в іншу також може виникнути ряд проблем. Так, спосіб адресації, що застосовується в одній мережі, може відрізнятися від прийнятого в іншій. Мережа може взагалі відмовитися приймати пакети через те, що вони занадто великого розміру. Також можуть відрізнятися протоколи та інш. Саме мережевий рівень повинен вирішувати всі ці проблеми, дозволяючи об'єднувати різнорідні мережі.

Основна функція транспортного рівня – прийняти дані від сеансового рівня, розбити їх при необхідності на невеликі частини, передати їх мережному рівню і гарантувати, що ці частини в правильному вигляді прибудуть за призначенням. Крім того, все це повинно бути зроблено ефективно і таким чином, щоб ізолювати більш високі рівні від будь-яких змін в апаратній технології з плином часу.

Транспортний рівень також визначає тип сервісу, що надається сеансовому рівню і безпосередньо користувачам мережі. Найбільш популярним різновидом транспортного з'єднання є захищений від помилок канал між двома вузлами, що поставляє повідомлення або байти в тому порядку, в якому вони були відправлені. Однак транспортний рівень може надавати й інші типи сервісів, наприклад пересилання окремих повідомлень без гарантії дотримання порядку їх доставки або одночасну відправку повідомлення різним адресатам за принципом широкомовлення. Тип сервісу визначається при установці з'єднання. Строго кажучи, повністю захищений від помилок канал створити абсолютно неможливо. Кажуть лише про такому каналі, рівень помилок в якому досить малий, щоб їм можна було знехтувати на практиці.

Транспортний рівень є справжнім наскрізним рівнем, тобто доставляє повідомлення від джерела адресату. Іншими словами, програма на машині-джерелі підтримує зв'язок з подібною програмою на іншій машині за допомогою заголовків повідомлень і керуючих повідомлень. На більш низьких рів-

нях для підтримки цього з'єднання встановлюються з'єднання між усіма сусідніми машинами, через які проходить маршрут повідомлень.

Сеансовий рівень дозволяє користувачам різних комп'ютерів встановлювати сеанси зв'язку один з одним. При цьому надаються різні типи сервісів, серед яких управління діалогом (відстеження черговості передачі даних), управління маркерами (запобігання одночасного виконання критичною операції декількома системами) і синхронізація (установка службових міток всередині довгих повідомлень, що дозволяють продовжити передачу з того місця, на якому вона обірвалася, навіть після збою і відновлення).

На відміну від більш низьких рівнів, завдання яких – достовірна передача бітів і байтів, рівень представлення займається здебільшого синтаксисом і семантикою переданої інформації. Щоб було можливе спілкування комп'ютерів з різними внутрішніми поданням даних, необхідно перетворювати формати даних один до одного, передаючи їх по мережі в деякому стандартизованому вигляді. Рівень представлення займається цими перетвореннями, надаючи можливість визначення та зміни структур даних більш високого рівня (наприклад, записів баз даних).

Прикладний рівень містить набір популярних протоколів, необхідних користувачам. Одним з найбільш поширених є протокол передачі гіпертексту HTTP, який складає основу технології Всесвітньої павутини. Коли браузер запитує веб-сторінку, він передає її ім'я (адресу) і розраховує на те, що сервер, на якому розташована сторінка, буде використовувати HTTP. Сервер у відповідь відсилає сторінку . Інші прикладні протоколи використовуються для передачі файлів, електронної пошти, мережевих розсилок.

1.2 Стандартизація мереж

Розрізняють наступні види стандартів:

– стандарти окремих фірм, наприклад стек протоколів SNA компанії IBM або графічний інтерфейс OPEN LOOK для Unix-систем компанії Sun;

– стандарти спеціальних комітетів і об'єднань створюються декількома компаніями, наприклад стандарти технології ATM, що розробляються спеціально створеним об'єднанням ATM Forum, яка налічує близько 100 колективних учасників, або стандарти союзу Fast Ethernet Alliance, що стосуються технології 100 Мбіт Ethernet;

– національні стандарти, наприклад стандарт FDDI, що представляє один з численних стандартів інституту ANSI, або стандарти безпеки для операційних систем, розроблені центром NCSC міністерства оборони США;

– міжнародні стандарти, наприклад модель і стек комунікаційних протоколів Міжнародної організації зі стандартизації (ISO), численні стандарти Міжнародного союзу електрозв'язку (ITU), в тому числі стандарти на мережі з комутацією пакетів X.25, мережі Frame Relay, ISDN, модеми та багато інших.

Найважливішим напрямком стандартизації в області обчислювальних мереж є стандартизація комунікаційних протоколів. Найбільш відомими стеками протоколів є: OSI, TCP / IP, IPX / SPX, NetBIOS / SMB, DECnet, SNA (не всі з них застосовуються сьогодні на практиці).

Стек TCP/IP був розроблений з ініціативи Міністерства оборони США для зв'язку експериментальної мережі ARPAnet з іншими мережами як набір загальних протоколів для різнорідного обчислювального середовища. Великий внесок у розвиток стека TCP/IP, який отримав свою назву по назві популярних протоколах IP і TCP, вніс університет Берклі, який реалізував протоколи стека у своїй версії ОС UNIX. Популярність цієї операційної системи привела до широкого поширення протоколів TCP, IP і інших протоколів стека. Сьогодні цей стек використовується для зв'язку комп'ютерів в Інтернеті, а також у величезному числі корпоративних мереж.

Співвідношення рівнів стеків OSI і TCP/IP показано на рис. 1.2.

Прикладний рівень (application layer) поєднує всі служби, що надаються системою користувальницьким додаткам: традиційні мережеві служби типу telnet (протокол емуляції терміналу), FTP (протокол передачі файлів), DNS

(система доменних імен), SNMP (протокол пересилання поштових повідомлень), HTTP (протокол передачі гіпертексту), гіпертекстові сервіси служби WWW.

Розглянемо більш докладно функції кожного рівня і приклади протоколів.

Рисунок 1.2 – Співвідношення рівнів стеків OSI і TCP/IP

Транспортний рівень (transport layer) вирішує завдання забезпечення надійного інформаційного зв'язку між двома кінцевими вузлами. Він контролює, щоб всі пакети були доставлені в місце призначення цілими та непошкодженими і у тому же порядку, у якому вони були відправлені. На транспортному рівні працюють два основних протоколи: UDP і TCP. TCP (Transmission Control Protocol – протокол контролю передачі) – надійний протокол із встановленням з'єднання: він управляє логічним сеансом зв'язку (встановлює, підтримує і закриває з'єднання) між процесами та забезпечує надійну (безпомилкову і гарантовану) доставку прикладних даних від процесу до процесу. TCP ділить потік байтів на частини – сегменти, і передає їх нижньому мережевому рівню. Після того як ці сегменти будуть доставлені засобами мережевого рівня в пункт призначення, протокол TCP знову збирає їх у безперервний потік байтів. Протокол UDP (User Datagram Protocol – протокол користувальницьких дейтаграм) забезпечує передачу прикладних паке-

тів дейтаграмним способом, як і головний протокол мережевого рівня IP, і виконує тільки функції сполучної ланки (мультиплексора) між мережевим протоколом і службами прикладного рівня або користувальницькими процесами.

На мережевому рівні (network layer) основним протоколом є протокол IP (Internet Protocol), який доставляє блоки даних, що називаються дейтаграмами, від одного IP-адреса до іншого. Дані передаються протоколу IP транспортним рівнем. Протокол IP додає до цих даних заголовок, що містить IP-адреси відправника і одержувача та іншу службову інформацію, і сформована в такий спосіб дейтаграмма передається на рівень мережевого доступу (наприклад, одному з фізичних інтерфейсів) для відправлення каналом передачі даних. До рівня мережевого доступу відносяться і всі протоколи маршрутизації, такі як: протоколи збору маршрутної інформації RIP (Routing Internet Protocol) і OSPF (Open Shortest Path First), а також протокол мережевих керуючих повідомлень ICMP (Internet Control Message Protocol). Останній протокол призначений для обміну інформацією про помилки між маршрутизаторами мережі та вузлом-джерелом пакета. За допомогою спеціальних пакетів ICMP повідомляє про неможливість доставки пакета, про перевищення часу життя або тривалості зборки пакета із фрагментів, про аномальні величини параметрів, про зміну маршруту пересилання і типу обслуговування, про стан системи й т.п.

Рівень мережевого доступу (link layer) забезпечує інтеграцію в складену мережу інших підмереж, тому мережа TCP/IP повинна мати засоби включення в себе будь-якої іншої підмережі, яку б внутрішню технологію передачі даних ця підмережа не використовувала. Звідси зрозуміло, що цей рівень не можна визначити раз і назавжди. Рівень мережевого доступу у протоколах TCP/IP не регламентується, але він підтримує всі популярні стандарти фізичного і канального рівнів: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet.

Функції цього рівня:

- відображення IP-адрес у фізичні адреси мережі (MAC-адреси, наприклад, Ethernet-адреса у випадку мережі Ethernet);
- інкапсуляція IP-дейтаграм у кадри та вилучення дейтаграм із кадрів;
- визначення методу доступу до середовища передачі – тобто способу, за допомогою якого комп'ютер встановлює своє право на передачу даних;
- пересилання та прийом кадрів.

1.3 Класифікація мереж

Залежно від території покриття комп'ютерні мережі можна розділити на три групи:

- локальні мережі (Local Area Network, LAN);
- глобальні мережі (Wide Area Network, WAN);
- міські мережі, або мережі мегаполісу (Metropolitan Area Network, MAN).

Локальні і глобальні мережімають різний територіальний масштаб. Зокрема, в локальних мережах якість ліній зв'язку між вузлами зазвичай вище, ніж в глобальних мережах. Це обумовлено різними причинами:

- істотно меншою довжиною ліній зв'язку (метри замість сотень кілометрів), а значить, і меншими викривленнями сигналів, внесених неідеальним передавальним середовищем;
- меншим рівнем зовнішніх перешкод, тому що в локальній мережі обладнання та кабелі зазвичай розміщуються в спеціальних захищених екранованих приміщеннях, а лінії зв'язку глобальної мережі можуть проходити в сильно електромагнітно «зашумленному» середовищі, наприклад в тунелях підземних комунікацій, поруч з силовими кабелями, уздовж ліній електропередач тощо;
- економічними міркуваннями.

Висока якість ліній зв'язку і низький рівень перешкод дозволили спростити процедури передачі даних в технологіях локальних мереж, наприклад застосовувати прості методи кодування і модулювання сигналів, відмовитися від складних алгоритмів відновлення перекручених даних.

Мережі MAN призначені для обслуговування території великого міста - мегаполісу, і поєднують в собі ознаки як локальних, так і глобальних мереж. Від перших вони успадкували велику щільність підключення кінцевих абонентів і високошвидкісні лінії зв'язку, а від останніх - велику протяжність ліній зв'язку.

Відповідно до технологічних ознак, зумовлених середовищем передачі, комп'ютерні мережі поділяють на два класи:

- провідні мережі – мережі, канали зв'язку яких побудовані з використанням мідних або оптичних кабелів;
- бездротові мережі – мережі, в яких для зв'язку використовуються бездротові канали зв'язку, наприклад радіо, СВЧ, інфрачервоні або лазерні канали.

Залежно від способу комутації мережі поділяються на два фундаментально різні класи:

- мережі з комутацією пакетів;
- мережі з комутацією каналів.

Зараз в комп'ютерних мережах переважно використовується техніка комутації пакетів, хоча принципово допустимо і застосування в них техніки комутації каналів.

Техніка комутації пакетів, в свою чергу, допускає кілька варіацій, що відрізняються способом просування пакетів, відповідно до чого мережі діляться на:

- дейтаграммний мережі, наприклад Ethernet;
- мережі, засновані на логічних з'єднаннях, наприклад IP-мережі, що використовують на транспортному рівні протокол TCP;
- мережі, засновані на віртуальних каналах, наприклад MPLS-мережі.

Мережі можуть бути класифіковані на основі топології: повнозв’язна топологія, дерево, зірка, кільце, змішана топологія.

Залежно від того, якого типу користувачів призначаються послуги мережі, вони поділяються на мережі:

- мережі операторів зв'язку надають публічні послуги, тобто клієнтом мережі може стати будь-який індивідуальний користувач або будь-яка організація, яка уклала відповідний комерційний договір на надання тієї чи іншої телекомунікаційної послуги;
- корпоративні мережі надають послуги тільки співробітникам підприємства, яке володіє цією мережею;
- персональні мережі знаходяться в особистому користуванні.

Залежно від функціональної ролі, яку відіграють деякі частини мережі, її відносять до:

- мережі доступу – це мережі, що надають доступ індивідуальним і корпоративним абонентам від їх приміщень (квартир, офісів) до першого приміщення (пункту присутності) оператора мережі зв'язку або оператора корпоративної мережі;
- магістральні мережі – це мережі, що представляють собою найбільш швидкісну частину (ядро) глобальної мережі, яка об'єднує численні мережі доступу в єдину мережу.
- мережі агрегування трафіку – це мережі, що агрегують дані від численних мереж доступу для компактної передачі їх по невеликій кількості каналів зв'язку в магістраль.

2 МЕРЕЖЕВІ АРХІТЕКТУРНІ РІШЕННЯ

Для структуризації мережі використовують спеціальне комунікаційне устаткування – повторювачі, концентратори, комутатори, маршрутизатори.

Повторювач (repeater) – використовується для фізичного з'єднання різних сегментів кабелю локальної мережі з метою збільшення загальної довжини мережі і дозволяє перебороти обмеження на довжину ліній зв'язку за рахунок поліпшення якості переданого сигналу.

Повторювач, що має кілька портів і з'єднує кілька фізичних сегментів, часто називають концентратором (concentrator), або хабом (hub) – він повторює сигнали, що прийшли з одного порту, на інших своїх портах. Так, концентратор Ethernet повторює вхідні сигнали на всіх своїх портах, крім того, з якого сигнали поступають.

Відрізки кабелю, що з'єднують два комп'ютери або два інших мережевих пристрою називаються фізичними сегментам. Таким чином, концентратори і повторювачі, які використаються для додавання нових фізичних сегментів, є засобом фізичної структуризації мережі. Концентратори утворюють із окремих фізичних відрізків кабелю загальне середовище передачі даних – логічний сегмент.

Колективне використання багатьма комп'ютерами загальної кабельної системи в режимі поділу часу приводить до істотного зниження продуктивності мережі при інтенсивному трафіку. Тому мережі, побудовані на основі концентраторів, не можуть розширюватися в необхідних межах – при певній кількості комп'ютерів у мережі завжди відбувається насичення передавального середовища, і затримки в її роботі стають неприпустимими.

Ця проблема може бути вирішена шляхом логічної структуризації мережі, тобто завдяки локалізації трафіку, коли трафік призначений для комп'ютерів деякого сегмента мережі, поширюються тільки в межах цього сегмента. Таким чином, логічна структуризація мережі – це процес розбиття мережі на сегменти з локалізованим трафіком. Для логічної структуризації мережі ви-

користаються такі комунікаційні пристрої, як мости, комутатори, маршрутизатори і шлюзи.

Комутатор (switch) ділить поділюване середовище передачі мережі на логічні сегменти (рис.2.1). Логічний сегмент може утворюватися шляхом об'єднання декількох фізичних сегментів (відрізків кабелю) за допомогою одного або декількох концентраторів. Кожний логічний сегмент підключається до окремого порту комутатора. При надходженні кадру на який-небудь із портів комутатор повторює цей кадр, але не на всіх портах, а тільки на тому порту, до якого підключений сегмент, де знаходиться вузол-адресат. Тим самим комутатор ізолює трафік однієї підмережі від трафіка іншої. Локалізація трафіка не тільки економить пропускну здатність, але і зменшує можливість несанкціонованого доступу до даних [2][1)].

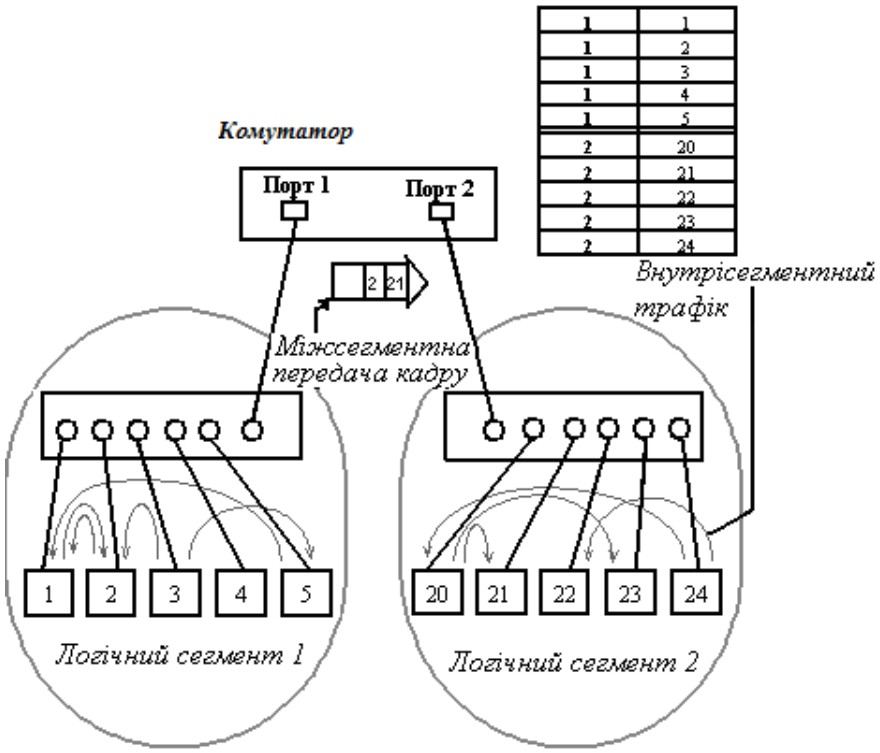

Рисунок 2.1 – Поділ мережі на логічні сегменти

[1)] [2] Кеннеди Кларк, Кевин Гамильтон. Принципы коммутации в локальных сетях Cisco. М.: Издательский дом «Вильямс», 2003. 971 с.

Для локалізації трафіка комутатор використовують апаратні адреси комп'ютерів. Це утрудняє розпізнавання приналежності того або іншого комп'ютера до певного логічного сегмента – сама адреса не містить ніякої інформації із цього приводу. Тому комутатор досить спрощено представляє розподіл мережі на сегменти – він запам'ятовує, через який порт на нього надійшов кадр даних від кожного комп'ютера мережі, і надалі передає кадри, призначені для цього комп'ютера, на цей порт.

Маршрутизатор (router) – ізолює трафік окремих частин мережі один від одного, утворюючи логічні сегменти за допомогою явної адресації, оскільки використовує не плоскі апаратні, а складові числові адреси. Всі комп'ютери, у яких значення поля адреси мережі однакові, належать до одного сегмента, який називається в цьому випадку підмережою (subnet). Сукупність декількох підмереж, з'єднаних між собою маршрутизаторами, утворює складену мережу або інтермережу (internetwork, або internet). Приклад інтермережі наведений на рис. 2.2. Компонентами інтермережі можуть бути як локальні, так і глобальні мережі. Всі вузли в межах однієї інтермережі взаємодіють, використовуючи єдину для них технологію.

Маршрутизатори здійснюють вибір найбільш раціонального маршруту з декількох можливих. В даному випадку під маршрутом розуміють послідовність проходження пакетом маршрутизаторів. Наприклад, на рис. 1.22 для зв'язку станцій L2 мережі LAN1 і L1 мережі LAN6 є два маршрути: M1-M5-M7 і M1-M6-M7.

Маршрутизатор може вибрати оптимальний маршрут при наявності декількох альтернативних маршрутів. Рішення про вибір того або іншого маршруту приймається кожним маршрутизатором, через який проходить повідомлення. Для того, щоб скласти топологію зв'язків у мережі, маршрутизатори обмінюються спеціальними службовими повідомленнями, у яких знаходиться інформація про ті зв'язки між підмережами, про які вони знають (ці підмережі підключені до них безпосередньо або ж вони дізналися про цю інформацію від інших маршрутизаторів).

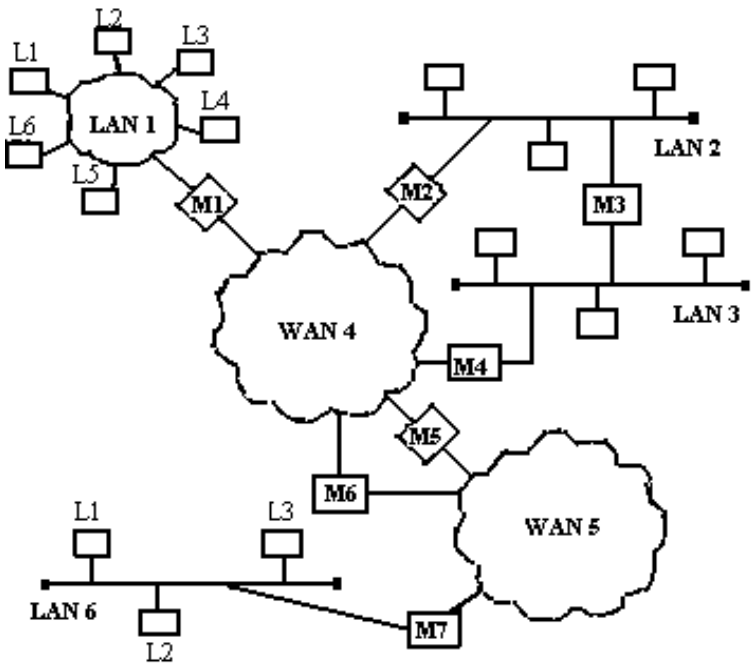

Рисунок 2.2 – Структура інтермережі, побудованої на основі маршрутизаторів

Побудова графа зв'язків між підмережами та вибір оптимального за яким-небудь критерієм маршруту на цьому графі являють собою складне завдання. При цьому можуть використовуватися різні критерії вибору маршруту – найменша кількість проміжних вузлів, час, вартість або надійність передачі даних. Важлива функція маршрутизаторів – здатність зв'язувати в єдину мережу (інтермережу) підмережі, що побудовані з використанням різних мережевих технологій. Тому маршрутизатори можуть поєднувати не тільки локальні мережі з різною технологією, але й локальні мережі із глобальними. Маршрутизатори не тільки поєднують мережі, але й надійно захищають їх, краще ніж комутатори. Наприклад, при надходженні кадру з неправильною адресою комутатор зобов'язаний повторити його на всіх своїх портах, що робить мережу незахищеною від некоректно працюючого вузла. Маршрутизатор же в такому випадку просто відмовляється передавати "неправильний" пакет далі, ізолюючи дефектний вузол від іншої мережі. Тому маршрутизатор – це складний інтелектуальний пристрій, побудований на базі одного, а

іноді і декількох потужних процесорів. Такий спеціалізований мультипроцесор працює, як правило, під керуванням спеціалізованої операційної системи.

Крім перерахованих пристроїв окремі частини мережі може з'єднувати шлюз (gateway). Звичайно основною причиною, за якою у мережі використають шлюз, є необхідність об'єднати мережі з різними типами системного та прикладного програмного забезпечення, а не бажання локалізувати трафік. Проте шлюз забезпечує і локалізацію трафіка як деякий побічний ефект.

Найбільш ефективне рішення з побудови єдиних мереж передачі даних запропоновано компанією Cisco Systems, воно являє собою модульний підхід до побудови структури мережі і базується на композитної мережевій моделі підприємства. Це рішення дозволяє будувати як невеликі мережі, що об'єднують кілька офісів, так і великі, що включають сотні вузлів. При цьому забезпечується передбачуваність якісних характеристик мережі при її розвитку шляхом додавання нових модулів або вузлів, і потрібний мінімальний час для пошуку і усунення несправностей.

Cisco – світовий лідер у галузі мережевих технологій, заснованих на інтернет- протоколі (IP), таких як маршрутизація, комутація, уніфіковані комунікації, бездротовий зв'язок і безпека. Компанія стала каталізатором переходу всієї галузі на IP-технології, послуги та рішення Cisco використовуються для створення комп'ютерних мереж, що дозволяють підвищити продуктивність праці, поліпшити якість послуг, що надаються, зміцнити конкурентоспроможність.

Для досягнення найкращих результатів по продуктивності, надійності, керованості і масштабованості необхідний багаторівневий підхід до дизайну мережі. Такий підхід дозволяє нарощувати мережу шляхом додавання нових блоків, забезпечує високий детермінізм поведінки мережі, вимагає мінімальних зусиль і коштів для пошуку та усунення несправностей. Інтелектуальні L3 сервіси забезпечують скорочення області, зачепленої при виникненні різноманітних проблем з несправним або невірно налаштованим обладнанням, а

також балансування навантаження між/всередині рівнів ієрархії і швидку збіжність (convergence).

Відповідно до цієї моделі, мережа розбивається на три логічних рівня, які зображені на рис.2.3 [3][1)]:

1) ядро мережі (Core layer) – високопродуктивні пристрої, головне призначення – швидкий транспорт;

2) рівень поширення (Distribution layer) – забезпечує застосування політик безпеки, QoS, агрегацію і маршрутизацію в VLAN, визначає широкомовні домени;

3) рівень доступу (Access–layer), як правило, L2 свічі, призначення – підключення кінцевих пристроїв, маркування трафіку для QoS, захист від кілець в мережі (STP) і широкомовних штормів, забезпечення живлення для PoE пристроїв.

Комутатори рівня Access надають користувачам порти 10/100 Ethernet, утворюють віртуальні мережі, замкнуті в межах цих комутаторів, і можуть бути виконані у вигляді модульних (переважно) або stackable пристроїв. Рівнем Distribution можуть бути виконані двома каналами Gigabit Ethernet (переважно) або Fast Ethernet з підтримкою EtherChannel. Комутатори рівня Distribution пов'язують блок будівлі по каналах Gigabit Ethernet з рівнем Core, що охоплює весь кампус L3/L4 комутацією, при цьому кожен з комутаторів блоку будівлі має по два L3 шляху в будь-яку точку мережі, чим досягається майже миттєва перемаршрутізація трафіку.

Теоретично можливе суміщення декількох логічних рівнів, наприклад Access/Distribution або Distribution/Core в одному фізичному пристрої. Такий підхід може бути економічно вигідний для невеликої мережі. Однак в процесі розвитку мережі перехід до класичного багаторівневому дизайну неминучий, оскільки лише при такому підході можливо раціональне використання функ-

[1)] [3] Вито Амато. Основы организации сетей Cisco. Том2. М.: Издательский дом «Вильямс», 2004. 464 с.

ціональних можливостей обладнання у відповідних точках мережі, а відповідно і мінімізація вартості.

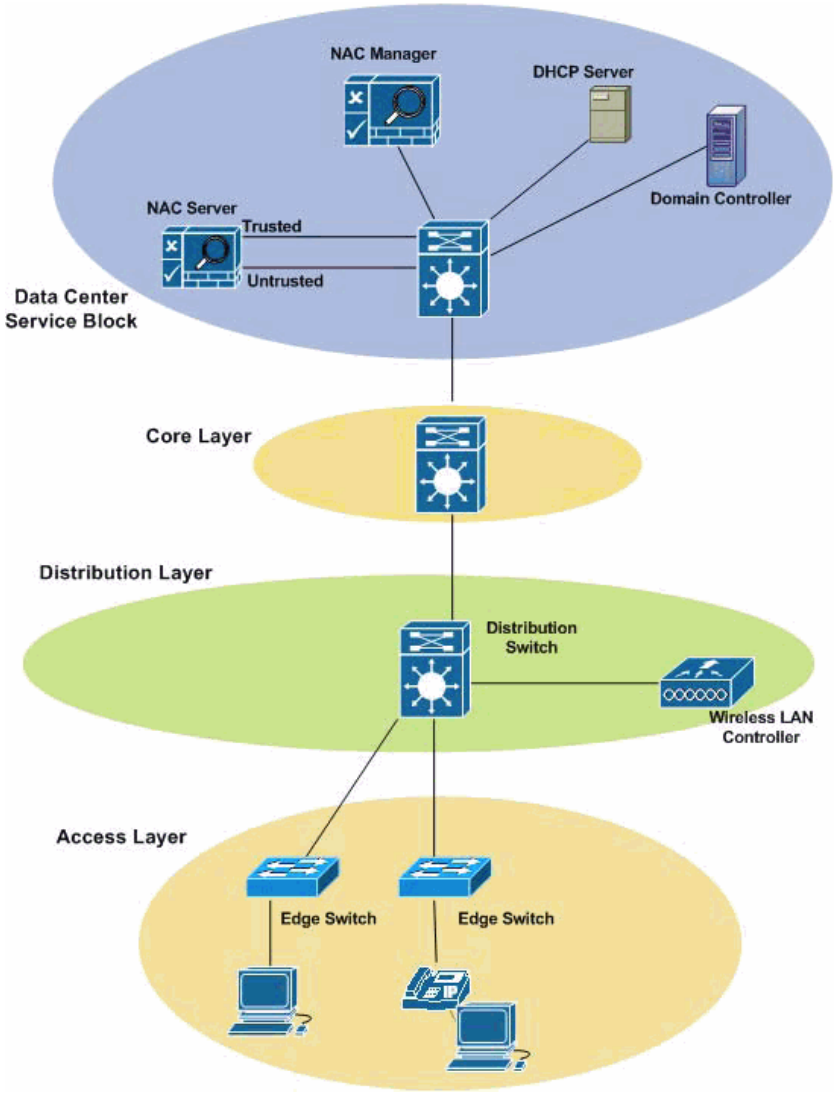

Рисунок 2.3 – Багаторівнева модель ЛОМ

3 ОГЛЯД БЕЗДРОТОВОЇ ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ WI-FI ТА СТАНДАРТУ 802.11

Стандарт IEEE 802.11 є базовим для всіх наступних специфікацій (802.11a, 802.11b, 802.11g, 802.11n). Комерційна назва цих мереж – Wi-Fi (Wireless Fidelity). Ця технологія використовується в таких областях, як бездротовий доступ в Інтернет, бездротове телебачення. Різні стандарти сімейства Wi-Fi визначають фізичний рівень (PHY) і підрівень управління доступом до середовища (каналу) MAC (Medium Access Control). Верхні рівні співпадають з своєю структурою як для бездротових, так і для провідних локальних мереж. Фізичний рівень визначає спосіб роботи з середовищем передачі, швидкість і методи модуляції. Підрівень MAC відповідає за розподіл каналу, тобто за те, яка станція буде передавати наступної. На MAC-рівні визначено принцип, за яким пристрої використовують (ділять) загальний канал, механізм аутентифікації користувача, механізм шифрування даних. Оскільки стандарт 802.11 розроблявся як «бездротовий Ethernet», він передбачає пакетну передачу з 48-бітовими адресами пакетів, як і будь-яка мережа Ethernet. Комітет IEEE 802 забезпечив сумісність усіх своїх стандартів. Бездротові мережі 802.11 легко сполучаються з провідними мережами Ethernet.

Стандарт 802.11 передбачає два основні способи (режиму) організації мережі, які розглядаються нижче [4,5][1)].

З базовою станцією або точкою доступу AP (Access Point). Зв'язок між пристроями відбувається тільки через AP. Через AP може бути вихід у зовнішні провідні мережі. Такі мережі називають також структурованими або працюють в режимі інфраструктури. Такий режим дозволяє транслювати мультимедійну інформацію для роботи в Інтернеті. У мережі 802.11 може бути

[1)] [4] Вишневский В.М., Портной С.Л., Шахнович И.В. Энциклопедия WiMAX. Путь к 4G. М.: Техносфера. 2009. 472с.

[5] Дэвис Д. Создание защищенных беспроводных сетей 802.11 в Microsoft Windows. Справочник профессионала. М.: ЭКОМ. 2006. 400с.

кілька точок доступу, об'єднаних провідною мережею Ethernet (рис. 3.1). Фактично така мережа являє набір базових станцій з перекриваються зонами охоплення. Точки доступу AP можуть бути доступні до Інтернету також через бездротову мережу WiMAX.

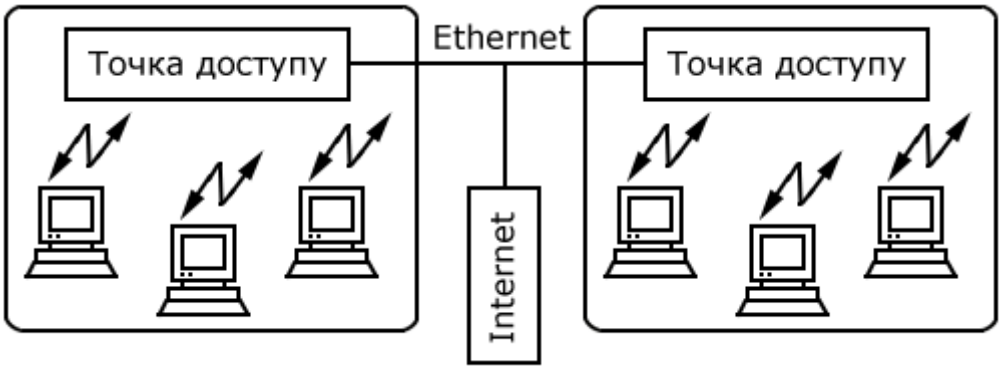

Рисунок 3.1 – Бездротова мережа з базовими станціями

Без базової станції (тобто без точки доступу), за принципом «рівний з рівним». Такі мережі називають бездротовими самоорганізації мережами Ad Hoc (рис. 3.2). WMN стандарт 802.11s називають також IBSS (Independent Basis Service Set). Мобільна Ad Hoc мережа (MANET, Mobile Ad Hoc Network) є розподіленою системою з мобільних терміналів, оснащених приймально-передавачем [6][1)]. Вони можуть динамічно організовувати тимчасові мережі. У мережах MANET мобільні пристрої виконують функції не тільки кінцевих станцій, але і мережевих вузлів, що виконують функції маршрутизаторів. Як правило, такі мережі не вимагають адміністрування. Термінали, які не перебувають в радіусі дії приймально-передавачів, здійснюють передачу через послідовність проміжних маршрутизаторів. Мережа MANET є багатокрокової (multihop) на відміну від мережею через цю точку доступу і може бути підключена за допомогою шлюзів до фіксованої мережі.

[1)] [6] Молчанов Д.А. Самоорганизующиеся сети и проблемы их построения. Электросвязь, №6. 2006. С.20-22.

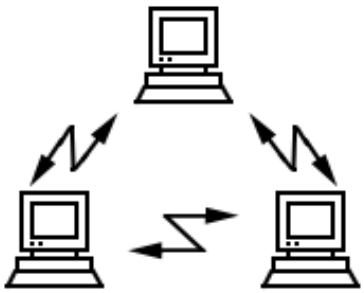

Рисунок 3.2 – Режим без точки доступу (мережа Ad Hoc)

Розглянемо фізичні рівні стандартів групи 802.11, які розрізняються технологіями і досяжними швидкостями:

– базовий 802.11;
– 802.11b;
– 802.11a;
– 802.11g;
– 802.11n.

Важливою проблемою у розвитку мереж Wi-Fi є виділення відповідної смуги робочих частот. Швидкий розвиток мереж забезпечується при виділенні діапазону частот, що не потребує ліцензування. В Україні дозволено неліцензійне використання діапазону частот 2,4 ГГц і 5,5 Ггц. Смуга пропускання 2,4 ГГц передбачений всіма стандартами даної групи, крім 802.11a, який допускає роботу тільки в неліцензійному діапазоні 5 ГГц. Неліцензійний діапазон частот використовується для промислових, медичних і наукових потреб ISM (Industrial, Scientific, Medical), включаючи домашні радіотелефони, СВЧ-печі та ін.).

Базовий стандарт 802.11. У базовому (первинному) стандарті 802.11 регламентується робота обладнання на центральній частоті 2,4 ГГц з максимальною швидкістю до 2 Мбіт/с. На фізичному рівні базового протоколу 802.11 реалізовано 2 методу передачі даних, що дозволяють передати кадр підрівня MAC з однієї станції на іншу:

- метод перескоку частоти FHSS (Frequency Hopping Spread Spectrum);
- опционно метод розширення спектра методом прямої послідовності DSSS (Direct Sequence Spread Spectrum).

Технологія FHSS і DSSS забезпечує максимальну швидкість передачі даних лише 2Мбіт / с, в той час як зараз є більш швидкодіючі мережі на основі стандартів 802.11b, 802.11a, 802.11g, 802.11n.

Стандарт 802.11b. На фізичному рівні 802.11b реалізований метод високошвидкісної передачі широкосмугового каналу за методом прямої послідовності HR-DSSS (High Rate Direct Sequence Spread Spectrum). При частоті модуляції несучої 11МГц загальна швидкість складає в залежності від типу модуляції 1 або 2 Мбіт/с. Стандарт 802.11b передбачає швидкості передачі 11 і 5,5 Мбіт/с. Для цього використовується кодування комплементарним кодом (ССК-модуляція, Complementary Code Keying), яке дозволяє кодувати 8 біт на один символ, що відповідає швидкості передачі 11 Мбіт/с. Щоб розвантажити діапазон 2,4 ГГц був розроблений стандарт 802.11a для частот 5 ГГц. У цьому діапазоні рівень сукупності шумів менше. У стандарті 802.11b прийнятий в якості додаткового ще один спосіб модуляції – пакетне бінарне сверточное кодування PBCCC. Цей механізм дозволяє домагатися в мережах пропускну здатність 5,5; 11 і 22 Мбіт/с.

У стандарті 802.11a використовуються дві центральні частоти в районі 5 ГГц і максимальна швидкість передачі складає до 54 Мбіт/с. Ця специфікація заснована на принципово іншому механізмі множинного доступу, ніж в розглянутих раніше в справжніх матеріалах стандартів бездротових систем стільникового зв'язку та Wi-Fi. У 802.11a в якості основного методу розширення спектра прийнято мультиплексування з ортогональним частотним поділом сигналів OFDM (Orthogonal Frequency Division Multiplexing). У стандарті 802.11a кожен діапазон розбивається на п'ять робочих піддіапазонів (далі будемо називати діапазоном) в залежності від накладається обмеження на потужність передавача. До недоліків технології 802.11a відносяться більш висока споживана потужність для частот 5 ГГц, а також менший радіус дії

(обладнання для 2,4 ГГц може працювати на відстані до 300 метрів, а для 5 ГГц близько 100 м).

Стандарт 802.11g є покращеною версією 802.11b. Він призначений для роботи на частотах 2,4 ГГц з максимальною швидкістю 54 Мбіт/с. Він аналогічний стандарту 802.11a по частоті і стандарту 802.11a по максимальній швидкості. У ньому допускається розширення спектра DSSS і OFDM. Виділена для 802.11g смуга частот в РФ становить 2400-2483,5 МГц.

Стандарт 802.11n призначений для підвищення швидкості передачі даних і збільшення дальності передачі інформації. Він грунтується, як і стандарт 802.11a на технології OFDM і передбачає використання обох центральних частот (2,4 і 5 ГГц). Підвищення швидкості передачі інформації в цьому стандарті досягається за рахунок наступних заходів. Подвоєння смуги пропускання каналу з 20 до 40 МГц, при цьому режим 20 МГц – обов'язковий і для нього встановлений базовий режим швидкостей передачі.

Застосування технології багатоканальних антенних систем MIMO (Multiple Input Multiple Output), тобто множинні входи і множинні виходи. В основу покладено застосування декількох передавальних і приймальних антен. Переданий потік даних розбивається на незалежні послідовності бітів, які пересилаються одночасно з використанням різних антен. За допомогою декількох антен система MIMO дозволяє здійснювати просторове мультиплексування потоків, що забезпечує підвищення швидкості передачі даних. Система MIMO дозволяє також за кількома антен передавати одночасно один і той же потік даних. Унаслідок багаторівневого поширення приймач отримує кілька сигналів. За допомогою технології MIMO ці сигнали обробляються і з них відновлюється вихідний сигнал, що сприяє поліпшенню співвідношення сигнал / перешкода. Так обладнання стандарту 802.11n з декількома передавальними і приймають антенами дозволяє підвищити швидкість передачі даних, покращуючи при цьому співвідношення сигнал / перешкода.

Стандарт 802.11s призначений для бездротових mesh-мереж WMN (Wireless mesh network). Їх називають комірчаним мережами. Бездротові

mesh-мережі називають також MBSS (Mesh BSS, Mesh Basis Service Set). Mesh-мережі – новий перспективний клас широкосмугових бездротових мереж передачі мультимедійної інформації, який знаходить широке застосування при побудові локальних і розподілених міських бездротових мереж. Для WMN характерний принцип самоорганізації побудови архітектури, самоконфігурації, самовідновлення, високою масштабованості і надійності [7][1)].

WMN відрізняє від MANET в тому, що включає додатково окрему опорну мережу (backbone) з маршрутизаторів, яка і надає їй переваги перед MANET. На рис. 3.3 наведена архітектура mesh-мережі стандарту 802.11s, що включає такі маршрутизатори (mesh-routers). Переваги mesh-мережі: мінімальний час і простота розгортання завдяки самоорганізації, самоадаптації і самовідновлення в обхід пошкодженої ділянки, здатність забезпечити зв'язок на території, де традиційні системи не можуть це виконати.

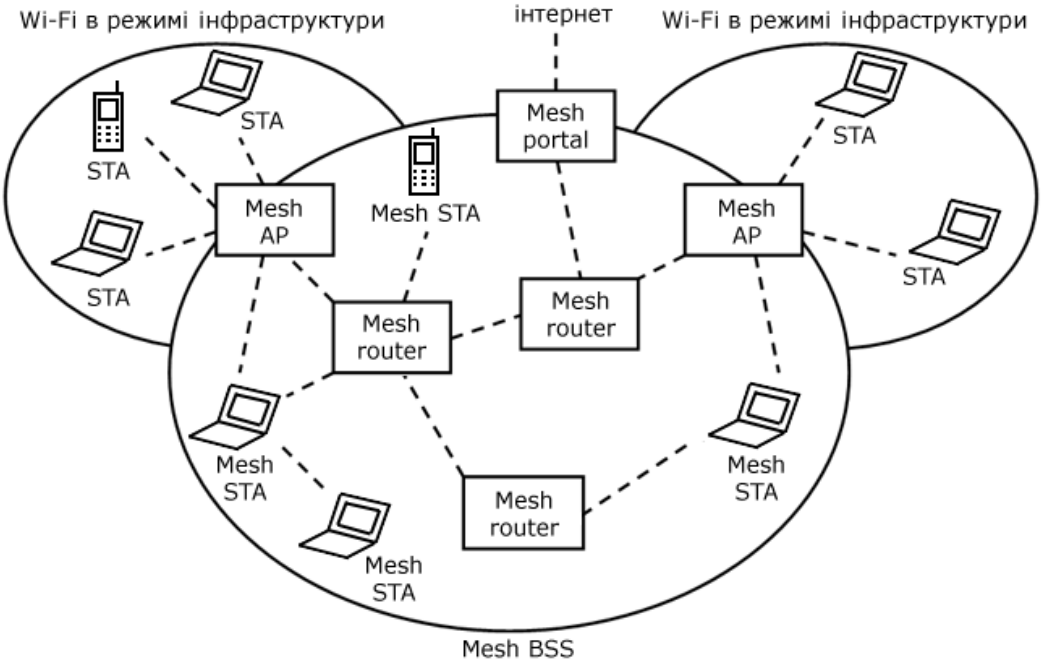

Рисунок 3.3 – Архітектура mesh-мережі 802.11s

[1)] [7] Ping Yi. A Survey on Security in Wireless Mesh Networks, IETE Technical Review, v.27, №1. 2010. P.6-14

У табл. 3.1 наведені основні технічні характеристики стандартів IEEE 802.11a, b, g і n [8]–[12][1)].

Таблиця 3.1 – Основні характеристики стандартів IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n

Стандарт	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Частотний діапазон, ГГц	5.15–5.25 5.67–5.85	2.4–2.483	2.4–2.483	2.4–2.483 5.15–5.25 5.67–5.85
Доступ до радіоканалу	CSMA-CA	CSMA-CA	CSMA-CA	CSMA-CA
Кількість абонентів на один канал	64	64	64	64
Максимальна швидкість обміну даними	54Мбіт/с	11 Мбіт/с	54 Мбіт/с	480 Мбіт/с
Метод модуляції	OFDM	BPSK,CCK	OFDM	BPSK, QPSK, 16-QAM, 64-QAM
Дальність дії в приміщенні, м	10–20	20–100	20–50	10–20

[1)] [8] Стандарт IEEE Std 802.11a-1999 (Reaff 2003). URL https://standards.ieee.org/standard/802_11a-1999.html (дата звернення 25.03.2020)

[9] Стандарт IEEE Std 802.11b-1999. URL. https://standards.ieee.org/standard/802_11b-1999.html (дата звернення 25.03.2020)

[10] Стандарт IEEE Std 802.11g-2003. URL. https://standards.ieee.org/standard/802_11g-2003.html (дата звернення 25.03.2020)

[11] Стандарт IEEE Std 802.11i-2004. URL. https://standards.ieee.org/standard/802_11i-2004.html (дата звернення 25.03.2020)

[12] Стандарт IEEE Std 802.11n-2009. URL. https://standards.ieee.org/standard/802_11n-2009.html (дата звернення 25.03.2020)

4 ЕТАПИ ПРОЕКТУВАННЯ ЄДИНОЇ МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ

4.1 Вихідні дані

Вихідні дані до проектування єдиної мережі передачі даних:

1) Кількість робочих станцій мережі – $N = 25$;

2) Кількість підмереж робочих станцій – $H = 5$;

3) Кількість бездротових клієнтів – 4;

4) Доступний адресний простір для підмереж маршрутизаторів S_R – 10.6.0.0/24;

5) Доступний адресний простір для підмереж робочих станцій S_H – 192.168.0.0/16;

Топологія ядра мережі представлена на рис. 4.1. Маючи достатню кількість вихідних даних можна приступити до послідовного виконання етапів проектування.

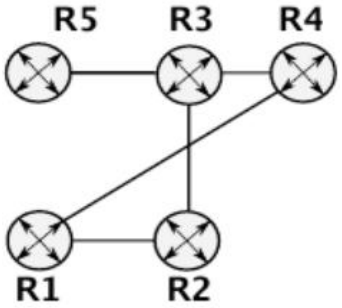

Рисунок 4.1 – Топологія ядра єдиної мережі передачі даних

4.2 Розподіл підмереж робочих станцій ЄМПД

Згідно з вихідними умовами завдання, єдина мережа передачі даних повинна забезпечувати роботу мінімум 25 робочих станцій ($N = 25$), які необхідно розділити рівномірно на 5 підмереж. Тобто в кожній підмережі може

перебувати 5 робочих станцій (*N/H* = 25/5 = 6), що в повній мірі задовольняє умові рівномірного розподілу.

Розподіливши робочі станції по підмережам, можна приступити до доповнення графа єдиної мережі передачі даних.

Об'єднання робочих станцій в кожній підмережі буде здійснюватись за допомогою некерованого *L2*-комутатора, з 8 фізичними портами FastEthernet. Тобто кожна робоча станція підключається до комутатора за допомогою кабелю UTP (неекранована кручена пара) категорії 5, утворюючи сегментоване повнодуплексне підключення.

З 8 фізичних портів комутатора, 6 портів використовуються для об'єднання робочих станцій і один порт для підключення до маршрутизатора R ядра єдиної мережі передачі даних.

Порт комутатора, який залишився, можна використовувати для каскадного підключення іншого комутатора при можливому розширенні підмережі або в якості технічного резерву.

Згідно вихідного графу єдиної мережі передачі даних, експлуатаційне навантаження мережі повинні забезпечувати 5 маршрутизаторів *R*. Залежно від розташування, маршрутизатори мають 3 або 4 інтерфейсу FastEthernet. Коректна маршрутизації пакетів між будь-якими підмережами забезпечиться при наявності 5 підмереж.

Розширений граф єдиної мережі передачі даних представлений на рис.4.2. На графі єдиної мережі передачі даних нанесені наступні буквено-цифрові найменування:

- *H1-H6* – робочі станції єдиної мережі передачі даних;
- *R1-R5* – маршрутизатори єдиної мережі передачі даних.
- *SW1-SW5* – комутатори підмережі робочих станцій
- *BRD1-BRD5* □ межі широкомовних доменів підмереж робочих станцій;
- S_H1-S_H6 – підмережі робочих станцій;
- S_R1-S_R8 – підмережі маршрутизаторів.

На графі також позначені відповідні номери інтерфейсів маршрутизаторів *R* і порти комутаторів *SW*.

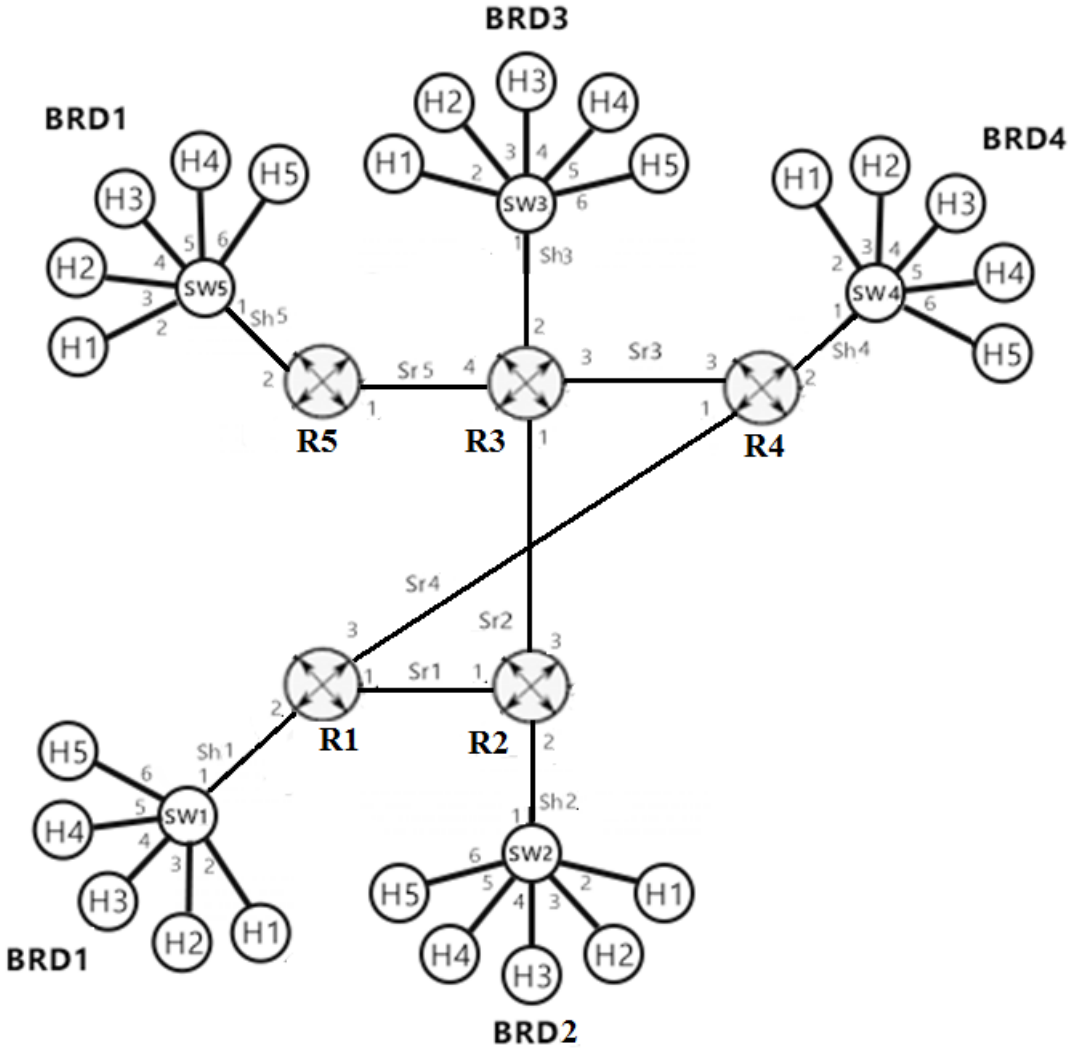

Рисунок 4.2 – Розширений граф єдиної мережі передачі даних

4.3 Перелік технічних засобів

За отриманим графом єдиної мережі передачі даних можна підрахувати загальну кількість технічних засобів, що витрачаються. Для коректного функціонування проектованої мережі необхідний наступний набір обладнання:

1) 5 маршрутизаторів (4 маршрутизатора з 3 інтерфейсами FastEthernet, 1 маршрутизатор з 4 інтерфейсами FastEthernet);

2) 5 некерованих комутаторів (8 фізичних портів на кожному пристрої, повнодуплекс, автоузгодження), що підтримують мережу FastEthernet на кабелі UTP5e;

3) по 1 мережевій карті на кожну робочу станцію (25 мережевих карт стандарту FastEthernet, повнодуплекс, автоузгодження);

4) Бездротова точка доступу (WiFi AP), яка підтримує стандарти 802.11b/g/n;

5) Опорна технологія мережі FastEthernet 100Мбіт/с, тип ліній зв'язку між усіма пристроями – неекранована кручена пара.

4.4 Плану IP-адресації підмереж робочих станцій

Відповідно до завдання, для адресації підмереж робочих станцій S_H виділено адресний простір мережі 192.168.0.0/16. Даний простір дозволяє виділити близько 65536 IP-адрес (32-16 = 16 біт, 216 = 65536). Виділена мережа 192.168.0.0/16 використовує 2 байта для адресації мережі, 2 байта, що залишилися вільні. Запис мережі в двійковій нотації матиме вигляд:

192.168.0.0– 1100 0000.1010 1000.0000 0000.0000 0000

255.255.0.0 – 1111 1111.1111 1111.0000 0000.0000 0000

За результатами виконання попередніх завдань відомо, що в кожній підмережі робочих станцій S_H розташовується 5 вузлів. Додатково до цього, слід врахувати, що кожна підмережа підключається до відповідного маршрутизатора єдиної мережі передачі даних. Тобто для коректної маршрутизації і обміну інформацією між вузлами підмережі потрібно 6 IP-адрес на кожну підмережу робочих станцій S_H, з яких 5 IP-адрес призначаються відповідним робочим станціям, а одна IP-адреса призначається маршрутизатору R, підключеному через вказаний інтерфейс до даної підмережі. Однак, також не слід забувати про необхідність наявності адреси самої підмережі і широкомовної адреси.

Для адресації 6 вузлів досить 3 біт ($2^3 = 8$). Однак, з огляду на наявність адреси мережі і широкомовної адреси, доступними з даного адресного простору залишаться 6 IP-адрес.

Використовуючи нотацію CIDR і безперервне виділення блоків IP-підмереж, виділимо 5 IP-підмереж з 8 доступними IP-адресами в кожній підмережі. Слід пам'ятати, що перші 2 байта мережі 192.168.0.0 не зміняться, а для виділення підмереж можна використовувати тільки останні 2 байта. Застосуємо маску підмережі довжиною 29 біт (32-3 = 29 біт для адресації мережі, 3 біта для адресації вузлів). Запис першої IP-підмережі в двійковій нотації буде мати вигляд:

192.168.0.0 – 1100 0000.1010 1000.0000 0000.0000 0000

255.255.255.248 – 1111 1111.1111 1111.1111 1111.1111 1000

Перша IP-адреса мережі буде відрізняться тільки одним молодшим бітом:

192.168.0.1 – 1100 0000.1010 1000.0000 0000.0000 0001

Далі послідовно другий, третій і наступні адреси формуються з 3 молодших біт:

192.168.0.2 – 1100 0000.1010 1000.0000 0000.0000 0010

192.168.0.3 – 1100 0000.1010 1000.0000 0000.0000 0011

192.168.0.4 – 1100 0000.1010 1000.0000 0000.0000 0100

192.168.0.5 – 1100 0000.1010 1000.0000 0000.0000 0101

192.168.0.6 – 1100 0000.1010 1000.0000 0000.0000 0110

Аж до широкомовної адреси мережі, в якої всі молодші біти дорівнюють одиниці:

192.168.0.7 – 1100 0000.1010 1000.0000 0000.0000 0111

Відповідно, наступна IP-підмережа буде мати адресу 192.168.0.7/29, або у двійковій нотації:

192.168.0.8 – 1100 0000.1010 1000.0000 0000.000 1000

255.255.255.248 – 1111 1111.1111 1111.1111 1111.1111 1000

З пулом IP-адрес, що відповідають масці підмережі:

192.168.0.9 – 1100 0000.1010 1000.0000 0000.0000 1001

192.168.0.10 – 1100 0000.1010 1000.0000 0000.0000 1010

192.168.0.11 – 1100 0000.1010 1000.0000 0000.0000 1011

192.168.0.12 – 1100 0000.1010 1000.0000 0000.0000 1100

192.168.0.13 – 1100 0000.1010 1000.0000 0000.0000 1101

192.168.0.14 – 1100 0000.1010 1000.0000 0000.0000 1110

Широкомовна адреса мережі 192.168.0.8/29:

192.168.0.15 – 1100 0000.1010 1000.0000 0000.0000 1111

Наступні мережі знаходяться аналогічним чином. Нарешті, п’ята IP-підмережа буде мати адресу 192.168.0.32/29, або в двійковій нотації:

192.168.0.32 – 1100 0000.1010 1000.0000 0000.0010 0000

255.255.255.248 – 1111 1111.1111 1111.1111 1111.1111 1000

Пул IP-адрес:

192.168.0.33 – 1100 0000.1010 1000.0000 0000.0010 0001

192.168.0.34 – 1100 0000.1010 1000.0000 0000.0010 0010

192.168.0.35 – 1100 0000.1010 1000.0000 0000.0010 0011

192.168.0.36 – 1100 0000.1010 1000.0000 0000.0010 0100

192.168.0.37 – 1100 0000.1010 1000.0000 0000.0010 0101

192.168.0.38 – 1100 0000.1010 1000.0000 0000.0010 0110

Широкомовна адреса мережі 192.168.0.32/29:

192.168.0.39 – 1100 0000.1010 1000.0000 0000.0010 0111

Адресний простір, що залишився дозволяє організувати додатковий резерв при розширенні мережі. Наприклад для підключення підмережі Wi-Fi.

Доступний пул IP-адрес в двійковій і десятковій нотації для кожної з 5 підмереж S_H наведено у додатку А.

4.5 План IP-адресації підмереж маршрутизаторів

Складемо план адресації для підмереж маршрутизаторів S_R. Відповідно до завдання, для адресації підмереж S_R виділено адресний простір мережі

10.6.0.0/16. Даний простір дозволяє виділити близько 65536 IP-адрес (32-16 = 16 біт, 2^{16} = 65536). Мережа 10.6.0.0/16 використовує 2 байти для адресації мережі, останні два байти вільні. Запис мережі в двійковій нотації матиме вигляд:

10.6.0.0/16 – 0000 1010.0000 0110.0000 0000.0000 0000

255.255.0.0 – 1111 1111.1111 1111. 0000 0000. 0000 0000

З розширеного графу мережі відомо, що маршрутизація пакетів між будь-якими підмережами забезпечується при наявності 5 IP-підмереж.

Кожна підмережа маршрутизаторів S_R об'єднує 2 маршрутизатора. Для адресації 2 маршрутизаторів в кожній підмережі S_R досить 1 біта (2^1 = 2). Однак, враховуючи наявність адреси мережі і широкомовної адреси, вузли залишаться неадресованими.

Отже, необхідно використовувати 2 біта, які дозволять адресувати 4 адреси (2^2 = 4 IP-адрес).

Використовуючи нотацію CIDR і безперервне виділення блоків IP-підмереж, виділимо 5 IP-підмереж з 4 доступними IP-адресами в кожній підмережі. Нагадаємо, що перші 2 байти мережі 10.6.0.0/16 не змінюються, а для виділення підмереж можна використовувати два останні байти. Застосуємо маску підмережі довжиною 30 біт (32 - 2 = 30 біт для адресації мережі, 2 біти для адресації маршрутизаторів). Запис першої IP-підмережі в двійковій нотації матиме вигляд:

10.6.0.0 – 0000 1010.0000 0110.0000 0000.0000 0000

255.255.255.252 – 1111 1111.1111 1111.1111 1111.1111 1100

Відповідно до маски, мережа має наступні IP-адреси (змінюються два молодших біта):

10.6.0.1 – 0000 1010.0000 0110.0000 0000.0000 0001

10.6.0.2 – 0000 1010.0000 0110.0000 0000.0000 0010

Широкомовна адреса мережі 10.6.0.0/30

10.6.0.3 – 0000 1010.0000 0110.0000 0000.0000 0011

Наступна IP-підмережа матиме адресу 10.6.0.4/30, або в двійковій нотації:

10.6.0.4 – 0000 1010.0000 0110.0000 0000.0000 0100

255.255.255.252 – 1111 1111.1111 1111.1111 1111.1111 1100

10.6.0.5 – 0000 1010.0000 0110.0000 0000.0000 0101

10.6.0.6 – 0000 1010.0000 0110.0000 0000.0000 0110

Широкомовна адреса мережі 10.6.0.4/30

10.6.0.7 – 0000 1010.0000 0110.0000 0000.0000 0111

Наступні мережі знаходяться аналогічним чином. Нарешті, п’ята IP-підмережа буде мати адресу 10.6.0.16/30, або в двійковій нотації:

10.6.0.16 – 0000 1010.0000 0110.0000 0000.0001 0000

255.255.255.252 – 1111 1111.1111 1111.1111 1111.1111 1100

Пул IP-адрес:

10.6.0.17 – 0000 1010.0000 0110.0000 0000.0001 0001

10.6.0.18 – 0000 1010.0000 0110.0000 0000.0001 0010

Широкомовна адреса мережі 10.6.0.28/30

10.6.0.19 – 0000 1010.0000 0110.0000 0000.0001 0011

Доступний пул IP-адрес в двійковій і десятковій нотації для кожної з 5 підмереж S_R наведено у додатку Б.

4.6 Формування таблиці маршрутизації ЄМПД

Виконавши завдання адресації підмереж і маючи схему графа мережі, можна приступити до наповнення таблиць маршрутизації маршрутизаторів *R*. Таблиці маршрутизаторів наповнюються статичними записами. Записи таблиці маршрутизації повинні задовольняти умові можливості зв'язку будь-якого вузла будь-якої підмережі з будь-яким вузлом будь-якої іншої підмережі.

В якості метрики відстані використовується число проміжних вузлів від вузла відправника єдиної до вузла призначення. Таблиці маршрутизації мережі передачі даних наведені у додатку В.

Виконаємо моделювання ситуації прийняття рішення про маршрутизацію пакета. В якості вихідних даних необхідно вибрати вузол відправника (IP-адреса вузла), маску підмережі відправника і вузол одержувача (IP-адреса). Основним критерієм вибору є використання довільних вузлів, що знаходяться на відстані мінімум двох підмереж.

Відповідно до принципів прийняття рішення про необхідність маршрутизації пакета в зовнішню підмережу, слід знайти адресу підмережі відправника (спочатку в двійковому вигляді, а потім в десятковому), застосувавши операцію логічного І (AND) для IP-адреси вузла відправника і маски підмережі відправника. Потім виконати операцію І (AND) для IP-адреси вузла одержувача і маски підмережі відправника. Порівнявши обидва результати, необхідно прийняти рішення про маршрутизації даного пакета в суміжну підмережу (якщо результат не збігається) або передачі його в межах власної підмережі (якщо результат збігається).

В якості вихідних даних для вирішення даного завдання оберемо вузол відправника *H2* з IP-адресою 192.168.0.11, з підмережі S_H2 – 192.168.0.8/29. Вузлом призначення довільно призначимо робочу станцію *H1* з IP-адресою 192.168.0.26 з підмережі S_H4 – 192.168.0.24/29.

Відповідно до завдання покажемо, що мережею відправника дійсно є зазначена мережа S_H2, зробивши множення IP-адреси відправника і маски підмережі відправника:

192.168.0.11–1100 0000.1010 1000.0000 0000.0000 1011

255.255.255.248 – 1111 1111.1111 1111.1111 1111.1111 1000

192.168.0.8 – 1100 0000.1010 1000.0000 0000.0000 1000

Дійсно IP-адреса належить вказаній мережі.

Накладемо маску підмережі на IP-адреса відправника і перевіримо чи належить цей IP-адреса тієї ж мережі:

192.168.0.26 – 1100 0000.1010 1000.0000 0000.0001 1010

255.255.255.248 – 1111 1111.1111 1111.1111 1111.1111 1000

192.168.0.24 – 1100 0000.1010 1000.0000 0000.0001 1000

IP-адреса одержувача належить іншій мережі. Тобто підмережа відправника і підмережа одержувачі не збігаються, отже необхідно маршрутизировати пакет.

4.7 Відображення адрес на мережевому і канальному рівнях

Виконаємо моделювання механізму відображення адрес на мережевому і канальному рівнях. Виконання моделювання слід починати з вибору двох довільних підмереж робочих станцій S_H, за умовою того, що дані підмережі будуть знаходитися на відстані, що розділена мінімум двома маршрутизаторами *R*. Далі, для обраних підмереж необхідно сформувати таблицю такого змісту:

1) Найменування підмережі;

2) Найменування комутатора *SW* даної підмережі;

3) Порт комутатора;

4) Адреса канального рівня вузла підключеного до даного порту;

5) Найменування вузла (робочої станції).

Залежно від вибраної кількості портів комутатора *SW* підмереж робочих станцій S_H не зайняті порти слід позначити резервними. Адреси канального рівня (Ethernet MAC) вузлів підключених до комутатора вибираються довільно. Закінчив підготовку вихідних даних, необхідних для вирішення даного завдання, можна приступити до його безпосереднього виконання.

Відповідно до умов моделювання, виберемо дві довільні підмережі робочих станций, вузли яких беруть участь в обміні інформацією. В якості вихідних підмереж використуємо підмережі S_H1 і S_H2. Вони повною мірою відповідають умові, згідно якої підмережі повинні бути розташовані на відстані, розділеному двома маршрутізаторамі *R*.

Для обраних підмереж створимо таблицю, що містить відомості про порти коммутатора SW і фізичних (канальних) адрес вузлів кожної окремої підмережі. Канальні адреси мають довільні значення. Однак необхідно враховувати розмір MAC-адреси мережі Ethernet (6 байт). Перелік вузлів обраних підмереж наведено в таб.4.1.

Таблиця 4.1 – MAC-адреси вузлів підмереж робочих станцій S_H1 і S_H2

Підмережа S_H	Комутатор SW	Порт	Адреса канального рівня	Вузол
S_H1	SW1	1	01:24:23:A3:5B:41	R1
		2	01:A2:B2:56:C1:42	H1
		3	01:AC:23:97:AA:43	H2
		4	01:EF:02:2E:00:44	H3
		5	01:D2:45:12:01:45	H4
		6	01:C1:11:09:D6:46	H5
		7	00:00:00:00:00:00	Резерв
S_H2	SW2	1	06:12:32:3A: B5:81	R3
		2	06:AC:2B:65:1C:82	H1
		3	06:CA:4C:78:AA:83	H2
		4	06:FE:A0:42:00:84	H3
		5	06:2D:A4:22:10:85	H4
		6	06:1C:A1:90:6D:86	H5
		7	00:00:00:00:00:00	Резерв

4.7.1 Локальний сегмент

Перша частина завдання полягає у визначенні послідовності виконання процедур протоколу ARP при перетворенні IP-адреси вузла підмережі на відповідну MAC-адресу, за умовою, що обидва вузла знаходяться в межах однієї підмережі. Два вузла, які беруть участь в обміні інформацією вибираються

довільно зі списку робочих станцій підмережі. Для вирішення завдання необхідно заповнити два псевдозаголовка фрейма канального рівня (псевдозаголовок містить заголовок фрейму Ethernet формату DIX і заголовок ARP), наведеного на рис.4.3.

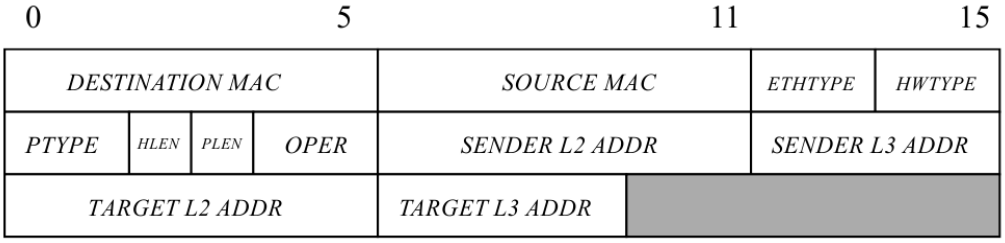

Рисунок 4.3 – Псевдозаголовок Ethernet DIX і ARP

Розшифровка полів, необхідних для заповнення [13, 14][1)]:

− DESTINATION MAC – Фізична (локальна) адреса одержувача в заголовку фрейма Ethernet. При широкомовній розсилки дорівнює FF: FF: FF: FF: FF: FF;

− SOURCE MAC – Фізична адреса відправника в заголовку фрейма Ethernet;

− OPER – Код операції протоколу відправника, запит (1) або відповідь (2);

− SENDER L2 ADDRESS – Фізична адреса відправника в заголовку протоколу ARP;

− SENDER L3 ADDRESS – Адреса протоколу мережевого рівня (логічний адресу) відправника в заголовку протоколу ARP;

− TARGET L2 ADDRESS – Фізична адреса одержувача в заголовку протоколу ARP. При ARP-запиті (1) невідомий (00: 00: 00: 00: 00: 00);

[1)] [13] An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses. URL http://tools.ietf.org/html/rfc826 (дата звернення 25.03.2020)

[14] Wikipedia. Address Resolution Protocol. URL http://en.wikipedia.org/wiki/ Address_Resolution_Protocol (дата звернення 25.03.2020)

− TARGET L3 ADDRESS – Логічна адреса одержувача в заголовку протоколу ARP.

Як було зазначено вище, необхідно заповнити два псевдозаголовка, один для фрейма запиту ARP-протоколу, другий для фрейма відповіді.

Заповнимо поля двох псевдозаголовків фрейма канального рівня при перетворенні IP-адреси на відповідну MAC-адресу робочої станції *H6* (вузол призначення) в підмережі S_H1. Запит на дозвіл виконує робоча станція *H3* (вузол відправлення).

Виходячи з раніше виконаних завдань відомо, що IP-адреса вузла *H5* в підмережі S_H1 дорівнює 192.168.0.6, MAC-адреса робочої станції, яку шукаємо, дорівнює 01:C1:11:09:D6:46. IP-адреса вузла *H3* в підмережі S_H1 дорівнює 192.168.0.4, MAC-адреса робочої станції дорівнює 01:EF:02:2E:00:44. Запит протоколу ARP в межах підмережі виконується широкомовною розсилкою фреймів Ethernet. Заповнений фрейм запиту представлений на рис.4.4.

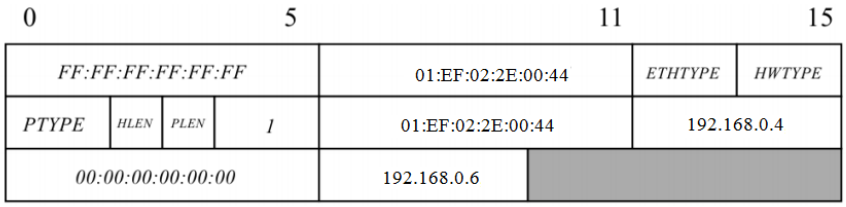

Рисунок 4.4 – Псевдозаголовок Ethernet і ARP при виконанні запиту MAC-адреси робочої станції H5

Відповідь робочої станції H5 буде містити кадр Ethernet з даними протоколу ARP, що відправляється безпосередньо вузлу H3. Заповнений фрейм відповіді вузла H5 разом з псевдозаголовка Ethernet представлений на рис.4.5.

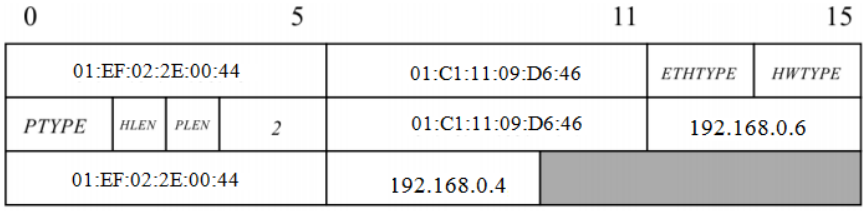

Рисунок 4.5 – Псевдозаголовок Ethernet і ARP при виконанні відповіді робочої станції H5 вузлу H3

Нанесемо графічні елементи, що зображують передачу фреймів між вузлами H3 (відправник) і H6 (одержувач) в підмережі S_H1 на граф сегмента єдиної мережі передачі даних. Отримані зображення наведені на рис.4.6.

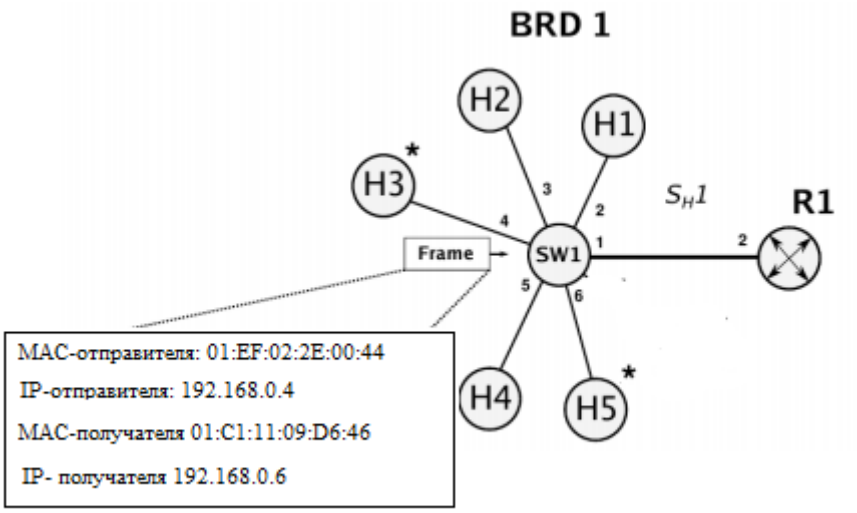

Рисунок 4.6 – Передача фреймів від вузла *H3* вузлу *H5* в межах підмережі S_H1

4.7.2 Дистанційні сегменти

Друга частина моделювання полягає в розгляді сценарію, згідно з яким виконується передача фреймів Ethernet між вузлами, розташованими у віддалених підмережах.

Умова полягає в тому, що вузли повинні розташовуватися в двох різних підмережах робочих станцій S_H, обраних в першій частині даного завдання. Вузли, які беруть участь в обміні, так само як і в попередньому пункті вибираються довільно зі списку робочих станцій підмереж.

Для виконання даного завдання не потрібно заповнювати псевдозаголовки фреймів, а лише нанести графічні елементи на граф єдиної мережі передачі даних, що зображують передачу фреймів Ethernet в віддалену підмережа вузлу призначення, із зазначенням коректних адрес відправника (поля *L2, L3*) і одержувача на даному сегменті мережі.

Вузлом-відправником призначена робоча станція *H2* з підмережі S_H1 (IP-адреса 192.168.0.3, MAC-адреса 01:A2:B2:56:C1:42), вузлом-одержувачем призначена робоча станція *H5* з підмережі S_H2 (IP-адреса 192.168.0.14, MAC-адреса 06:1C:A1:90:6D:86). Маршрутизатор *R1* має фізичну адресу 01:24:23:A3:5B:41, маршрутизатор *R2* має канальну адресу 06:12:32:3A:B5:81.

За вихідними умовами завдання, необхідності в заповненні полів фреймів Ethernet і псевдозаголовка протоколу ARP немає, тому що виконувані процедури дозволу адреси мережевого рівня на адресу канального рівня будуть аналогічні процедурам, що виконувалися при відображенні адрес вузлів, розміщених в одній підмережі, з різницею в тому, що замість MAC-адреси вузла одержувача у відповідному сегменті мережі буде використовуватися MAC-адреса маршрутизатора *R1* (в разі передачі пакетів від вузла *H2* з підмережі S_H1 вузлу *H5* з підмережі S_H2) або MAC-адреса маршрутизатора *R3* (в разі передачі пакетів від вузла *H5* з підмережі S_H2 вузлу *H2* з підмережі S_H1). Таким чином на кожному сегменті мережі в заголовках фреймів Ethernet будуть змінюватися адреси канального рівня (MAC-адреси) відправника і одержувача.

Адреси мережевого рівня вузлів відправника та одержувача змінюватися не будуть. На рис.4.7 наведено сегмент єдиної мережі передачі даних і зображена передача фреймів канального рівня з відповідним змістом заголовків

(MAC, IP-адреса відправника і MAC, IP-адреса одержувача) від вузла *H2* з підмережі S_H1 вузлу *H5* з підмережі S_H2.

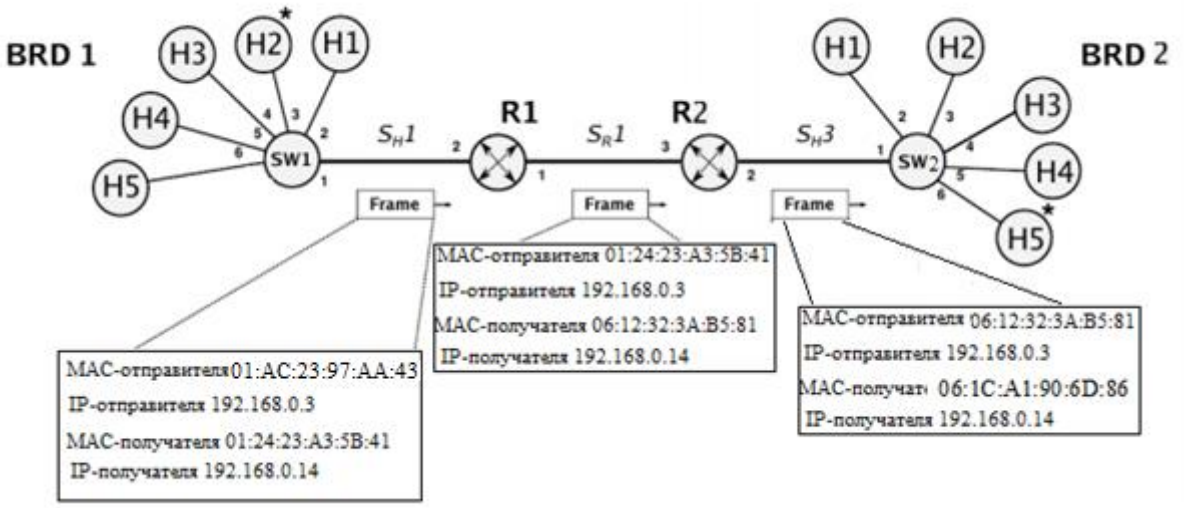

Рисунок 4.7– Передача фреймів канального рівня від вузла *H2* з підмережі S_H1 вузлу *H5* з підмережі S_H2

4.8 Організація бездротового доступу до ЄМПД

Для забезпечення бездротового доступу до інформаційно-обчислювальних ресурсів проектованої мережі, необхідно підключити бездротову точку доступу, що організує міст між дротовою мережею Ethernet і бездротовою зоною WiFi. При проектуванні мережі, зображеної на рис.3, були використані 8-портові комутатори FastEthernet, на кожному з яких один фізичний порт зарезервований для розширення. Таким чином підключення точки доступу можливо зробити до будь-якого комутатора *SWi* мережі. В такому випадку, бездротові станції можуть використовувати резервні IP-адреси з кожного діапазону. Запропоноване рішення досить просто при реалізації, проте має ряд істотних недоліків: обмежений адресний простір, складність контролю доступу бездротових клієнтів, змішання мережевого трафіку від

довірених станцій і тимчасових клієнтів. З наведених причин, розглянемо інший варіант структуризації мережі бездротового доступу.

З огляду на територіальне розташування об'єктів мережі і ступінь концентрації бездротових станцій в центральній області, найбільш доцільним видається підключення точки доступу до окремого інтерфейсу (3) маршрутизатора *R3*.

Виходячи з розрахунків проведених в розділах 4.4 і 4.5, адресний простір проектованої мережі має достатню глибину, для виділення окремої IP-підмережі, призначеної для організації доступу бездротових клієнтів. Припускаючи наявність одночасно не більше 20 бездротових клієнтів в зоні доступу можливо розрахувати діапазон адресного простору, що виділяється.

Відповідно до розрахункових даних з розділу 4.4, для створення неперекриваємого адресного простору можна використовувати діапазон адрес починаючи з 192.168.0.40.

Для адресації 4 клієнтів необхідно використовувати 5 біт ($2^3 = 8$). Отриманий простір забезпечить можливість адресувати 6 бездротових станцій, враховуючи витрати на службові адреси: IP-адреса інтерфейсу маршрутизатора, точки доступу, адреса мережі і широкомовна адреса. Додаток Г містить план адресації для бездротового сегмента.

Для коректної маршрутизації пакетів між дротовими і бездротовим сегментами мережі необхідно внести ряд змін. У таблицю маршрутизації кожного маршрутизатора мережі необхідно додати маршрут до мережі 192.168.0.40/29 через шлюз R5 (10.6.0.21/30). На бездротових станціях необхідно вказати шлюз по-замовчуванню R5 – 192.168.0.41.

В табл.4.2 зведені основні дані конфігурації бездротової точки доступу: ідентифікатор бездротової мережі, частотний діапазон, що використовується, спосіб шифрування, секретна фраза і ін.

Таблиця 4.2– Конфігурація бездротової точки доступу

Параметр	Значення
Місце включення	R5,інтерфейс 3
IP-адрес	192.168.0.42
Адресний простір	192.168.0.40/29
MAC-адреса точки доступу	BF:CC:1A:1E:AA:09
Стандарти, що підтримуються	802.11b/g/n, 2.4, 2.5, 5 GHz
Аутентифікація	WPA-PSK
SSID	EKSPD

5 МОДЕЛЮВАННЯ МЕРЕЖІ В ЕМУЛЯТОРІ CISCO PACKET TRACER

5.1 Опис емулятора Cisco Packet Tracer

Cisco Packet Tracer – емулятор мережі передачі даних, який випускається компанією Cisco System (рис.5.1). Програмні продукти Packet Tracer надають можливість створювати мережеві топології із широкого спектру маршрутизаторів і комутаторів Cisco, робочих станцій та мережевих з'єднань типу Ethernet, Serial, ISDN, Frame Relay. Ця функція може бути виконана як для навчання, так і для роботи. Наприклад, щоб провести настройку мережі ще на етапі планування або щоб створити копію робочій мережі з метою усування недоліків [15][1)].

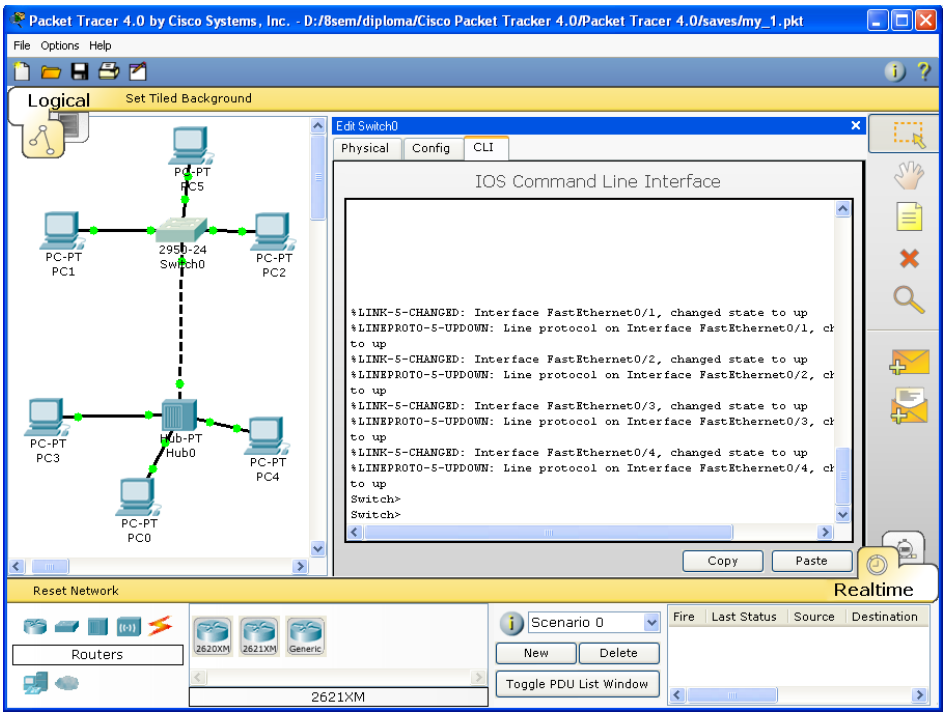

Рисунок 5.1 – Приклад використання командного рядку емулятору Cisco Packet Tracer

---

[1)] [15] Программа Cisco Packet Tracer. URL http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html (дата звернення 25.03.2020)

Користувачі мають можливість проектувати свої власні мережі, створюючи і відправляючи різноманітні пакети даних, зберігати і коментувати свою роботу. Вони можуть вивчати і використовувати різні мережеві пристрої: комутатори другого і третього рівнів, робочі станції, бездротові пристрої, глобальні мережі WAN, визначати типи зв'язків між ними і з'єднувати їх. Після того, як мережа спроектована, можна приступати до конфігурування обраного устаткування за допомогою термінального доступу або командного рядку (рис. 5.1).

Відмінною особливістю даного емулятору є наявність у нього «Режиму емуляції» (рис.5.2). У даному режимі всі пакети, що пересилаються всередині мережі, відображаються графічно. Ця можливість дозволяє наочно продемонструвати з якого інтерфейсу в даний момент переміщається пакет, який протокол використовується та ін.

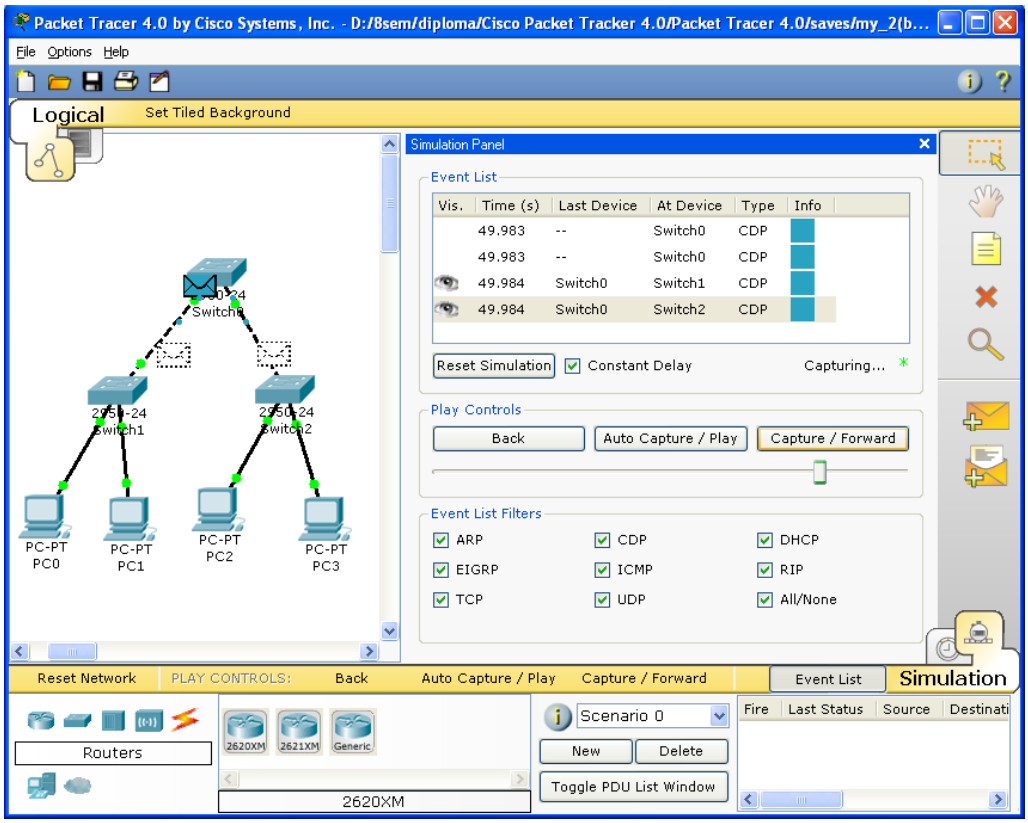

Рисунок 5.2 – Режим «Емуляції» в Cisco Packet Tracer

Однак, це не всі переваги Packet Tracer: в «Режимі емуляції» користувач може не тільки відслідковувати протоколи, що використовуються, але і бачити, на якому з семи рівнів моделі OSI даний протокол задіяний (рис.5.3).

Packet Tracer здатний моделювати велику кількість пристроїв різного призначення, а так само чимало різних типів зв'язків, що дозволяє проектувати мережі будь-якого розміру на високому рівні складності.

Можуть бути відслідковані наступні протоколи: ARP, CDP, DHCP, EIGRP, ICMP, RIP, TCP, UDP [16][1)].

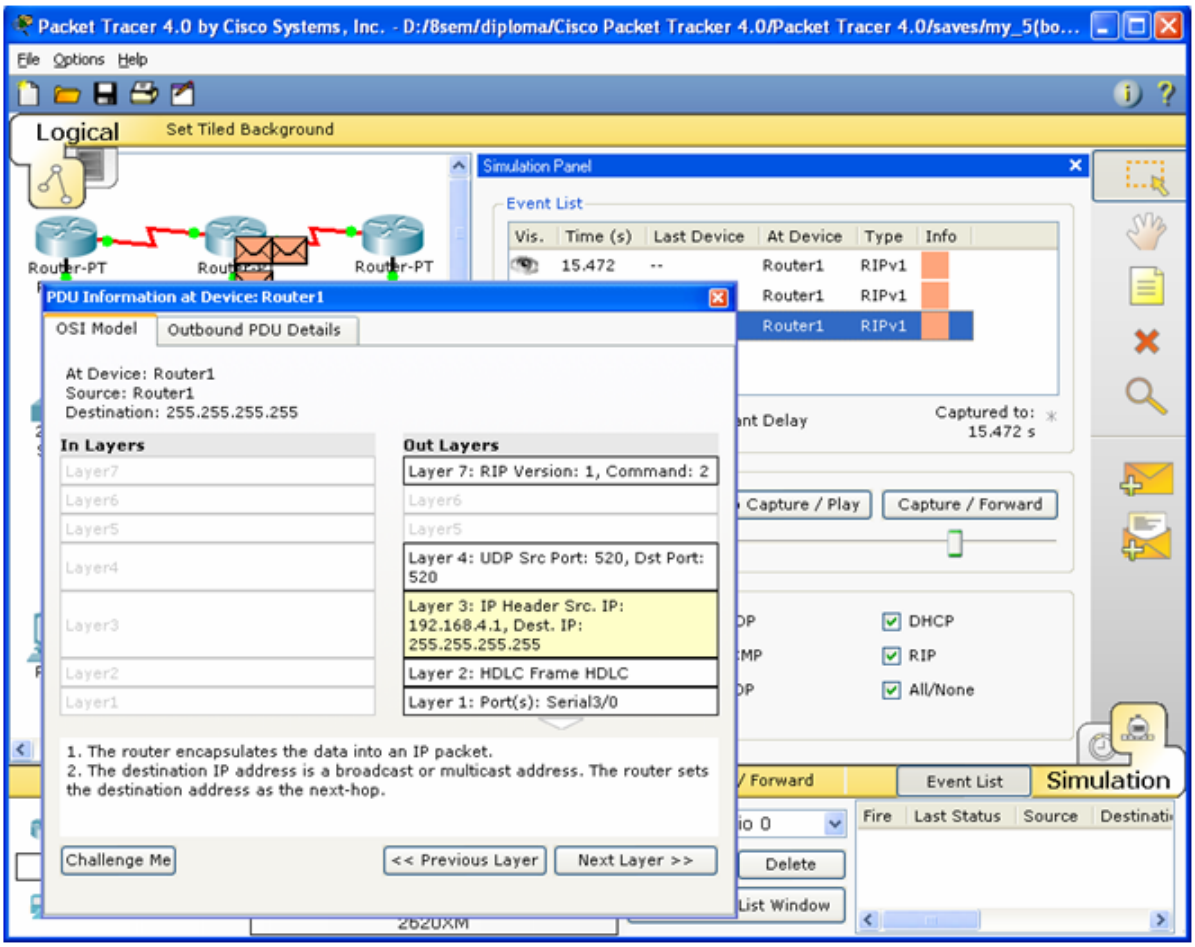

Рисунок 5.3 – Аналіз семі рівневої моделі OSI в Cisco Packet Tracer

[1)] [16] Джеймс Бони. Руководство по Cisco IOS. СПб.: Питер, М: Издательство «Русская редакция», 2008. 784 с.

5.2 Моделювання ЄМПД

Реалізуємо розподіл мережі на підмережі і представимо їх логічну структуру використовуючи програму Cisco Packet Tracer. Адреси підмереж наведені у додатку А.

Побудуємо мережу з 6-ма підмережами (рис. 5.1). Будемо використовувати модель маршрутизатора за замовчуванням – Generic. Сконфігуруємо стек протоколів кожного вузла мережі відповідно до даних вихідних даних.

Нижче приведений порядок конфігурування маршрутизатора за допомогою CLI Cisco IOS.

1) Для вибору мережевого пристрою Router0 треба натиснути в робочій області програми на його зображення. Відкриється вікно настройок мережевого пристрою. Вибираємо вкладку CLI для керування маршрутизатором.
2) В середині екрану можна побачити запрошення виду:

   Router>

   Це означає, що користувач підключений до мережевого пристрою і знаходиться в командному рядку режиму користувача. Тут “Router” – це і’мя мережевого пристрою, а “>” позначає режим користувача.
3) Далі вводимо команду enable, щоб потрапити в привілейований режим.

   Router> enable

   Router#
4) Перейдемо в режим конфігурації:

   Router# config terminal

   Router(config)#

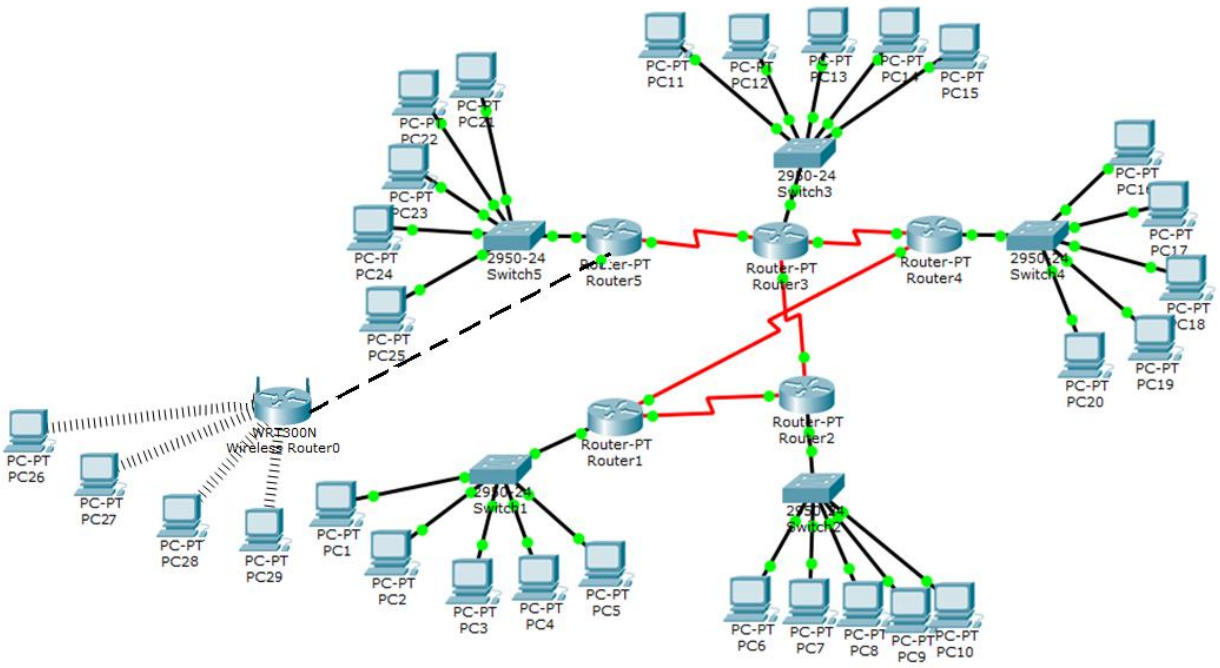

Рисунок 5.1 – Модель єдиної мережі передачі даних

Розглянемо команди, які дозволяють вмикати (піднімати) інтерфейси мережевого пристрою та переводити їх в стан UP.

1) На мережевому пристрої Router0 увійдемо в контекст конфігурації

   Router0#conf t

   Router0(config)#

2) Щоб настроїти Ethernet інтерфейс, треба зайти в контекст конфігурації інтерфейсу:

   Router0(config)#interface FastEthernet 0/0

   Router0(config-if)#

3) Переглянемо усі доступні в цьому контексті команди

   Router0(config-if)#?

4) Для виходу в контекст глобальної конфігурації треба набрати exit. Знову увійти в контекст конфігурації інтерфейсу:

   Router0(config)#int fa0/0

5) Встановимо IP адресу Ethernet інтерфейсу

   Router0(config-if)#ip address 192.168.0.1 255.255.255.248

6) Увімкнемо цей інтерфейс

   Router0(config-if)#no shutdown

7) Додамо до інтерфейсу опис:

   Router0(config-if)#description Ethernet interface on Router 0

8) Щоб побачити опис цього інтерфейсу, перейдіть в привілейований режим і виконайте команду show interface.

   Router0(config-if)#end

   Router0# show interface

9) Після того, як виконано конфігурування усіх інтерфейсів можна переглянути активну конфігурацію пристрою і переконатися, що з'явилися призначені IP - адреси

   Router0# show running-config

Здійснімо тестування мережі, використовуючи команду ping (рис.5.2 і 5.3).

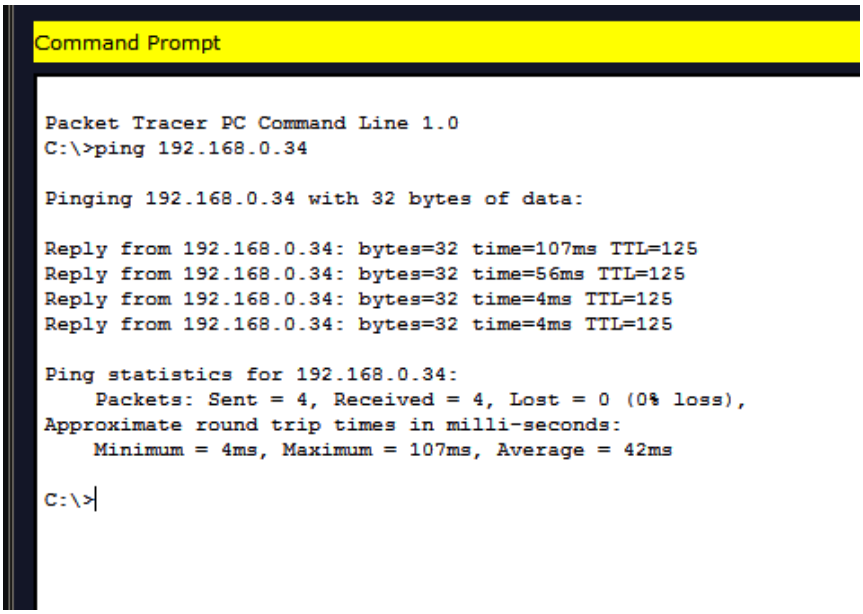

Рисунок 5.2 – Результат виконання команди ping між вузлами 192.168.0.25 і 192.168.0.34

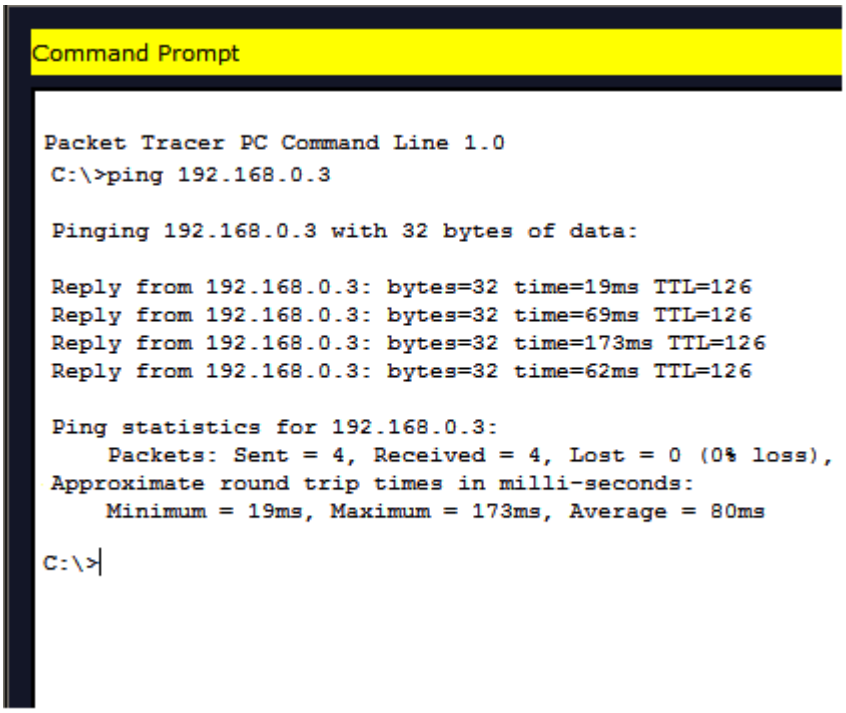

Рисунок 5.3 – Результат виконання команди ping між вузлами 192.168.0.13 і 192.168.0.3

ВИСНОВКИ

В результаті виконання бакалаврської роботи з проектування єдиної комп'ютерної мережі передачі даних були вирішені наступні завдання.

Виконано планування і розподіл виділених підмереж робочих станці, побудовано граф розширеної мережі, створений план IP-адресації підмереж робочих станцій і план IP-адресації підмереж маршрутизаторів. Виділено і обґрунтовано перелік потрібних технічних засобів для реалізації коректної роботи єдиної комп’ютерної мережі. Вирішена задача відображення адрес мережевого рівня на адресу канального рівня для різних сценаріїв місцезнаходження телекомунікаційних вузлів.

У роботі виконано моделювання проектованої мережі. У мережевому емуляторі Cisco Packet Tracer 5.3.2 налаштовані робочі станції статична маршрутизація і бездротовий сегмент Wi-Fi. Тестування мережі показало вірність виконаних налаштувань мережі.

Таким чином комп'ютерна мережа передачі даних, яка розроблена в рамках бакалаврської роботи, може використовуватися в якості попереднього плану при побудові аналогічних мереж передачі даних на практиці, із застосуванням сучасного обладнання. Досвід і знання, отримані в результаті проектування комп'ютерної мережі дозволять уникнути можливих помилок і провести оптимізацію характеристик реального проекту на попередньому етапі проектування.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Олифер В.Г., Н.А. Олифер Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов, 4–е изд. СПб.: Питер, 2010. 944 с.
2. Кеннеди Кларк, Кевин Гамильтон. Принципы коммутации в локальных сетях Cisco. М.: Издательский дом «Вильямс», 2003. 971 с.
3. Вито Амато. Основы организации сетей Cisco. Том2. М.: Издательский дом «Вильямс», 2004. 464 с.
4. Вишневский В.М., Портной С.Л., Шахнович И.В. Энциклопедия WiMAX. Путь к 4G. М.: Техносфера. 2009. 472с.
5. Дэвис Д. Создание защищенных беспроводных сетей 802.11 в Microsoft Windows. Справочник профессионала. М.: ЭКОМ, 2006, 400с.
6. Молчанов Д.А. Самоорганизующиеся сети и проблемы их построения. Электросвязь, №6. 2006. С.20-22.
7. Ping Yi. A Survey on Security in Wireless Mesh Networks, IETE Technical Review, v.27, №1. 2010. P.6-14
8. Стандарт IEEE Std 802.11a-1999 (Reaff 2003). URL https://standards.ieee.org/standard/802_11a-1999.html (дата звернення 25.03.2020)
9. Стандарт IEEE Std 802.11b-1999. URL https://standards.ieee.org/standard/802_11b-1999.html (дата звернення 25.03.2020)
10. Стандарт IEEE Std 802.11g-2003. URL https://standards.ieee.org/standard/802_11g-2003.html (дата звернення 25.03.2020)
11. Стандарт IEEE Std 802.11i-2004. URL https://standards.ieee.org/standard/802_11i-2004.html (дата звернення 25.03.2020)
12. Стандарт IEEE Std 802.11n-2009. URL https://standards.ieee.org/standard/802_11n-2009.html (дата звернення 25.03.2020)

13. An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses. URL_http://tools.ietf.org/html/rfc826_(дата звернення 25.03.2020)
14. Wikipedia. Address Resolution Protocol. URL http://en.wikipedia.org/wiki/Address_Resolution_Protocol (дата звернення 25.03.2020)
15. Программа Cisco Packet Tracer. URL http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html (дата звернення 25.03.2020)
16. Джеймс Бони. Руководство по Cisco IOS. СПб.: Питер, М: Издательство «Русская редакция», 2008. 784 с.

Д О Д А Т К И

ДОДАТОК А

Адресація підмереж робочих станцій

Таблиця А.1 – Адресація під мереж робочих станцій SH

Пі-дме ре-жа	Пул IP-адрес	Двійкова нотація	Призначення
S_h1	192.168.0.0/29	1100 0000.1010 1000.0000 0000.0000 0000	Адреса підмережі
	255.255.255.248	1111 1111.1111 1111.1111 1111.1111 1000	Маска підмережі
	192.168.0.1	1100 0000.1010 1000.0000 0000.0000 0001	R1, інтерфейс 2
	192.168.0.2	1100 0000.1010 1000.0000 0000.0000 0010	H1
	192.168.0.3	1100 0000.1010 1000.0000 0000.0000 0011	H2
	192.168.0.4	1100 0000.1010 1000.0000 0000.0000 0100	H3
	192.168.0.5	1100 0000.1010 1000.0000 0000.0000 0101	H4
	192.168.0.6	1100 0000.1010 1000.0000 0000.0000 0110	H5
	192.168.0.7	1100 0000.1010 1000.0000 0000.0000 0111	Широкомов. адр.
S_h2	192.168.0.8/29	1100 0000.1010 1000.0000 0000.0000 1000	Адреса підмережі
	255.255.255.248	1111 1111.1111 1111.1111 1111.1111 1000	Маска підмережі
	192.168.0.9	1100 0000.1010 1000.0000 0000.0000 1001	R2, інтерфейс 2
	192.168.0.10	1100 0000.1010 1000.0000 0000.0000 1010	H1
	192.168.0.11	1100 0000.1010 1000.0000 0000.0000 1011	H2
	192.168.0.12	1100 0000.1010 1000.0000 0000.0000 1100	H3
	192.168.0.13	1100 0000.1010 1000.0000 0000.0000 1101	H4
	192.168.0.14	1100 0000.1010 1000.0000 0000.0000 1110	H5
	192.168.0.15	1100 0000.1010 1000.0000 0000.0000 1111	Широкомов. адр.
S_h3	192.168.0.16/29	1100 0000.1010 1000.0000 0000.0001 0000	Адреса підмережі
	255.255.255.248	1111 1111.1111 1111.1111 1111.1111 1000	Маска підмережі
	192.168.0.17	1100 0000.1010 1000.0000 0000.0001 0001	R3, інтерфейс 2
	192.168.0.18	1100 0000.1010 1000.0000 0000.0001 0010	H1
	192.168.0.19	1100 0000.1010 1000.0000 0000.0001 0011	H2
	192.168.0.20	1100 0000.1010 1000.0000 0000.0001 0100	H3
	192.168.0.21	1100 0000.1010 1000.0000 0000.0001 0101	H4
	192.168.0.22	1100 0000.1010 1000.0000 0000.0001 0110	H5
	192.168.0.23	1100 0000.1010 1000.0000 0000.0001 0111	Широкомов. адр.
S_h4	192.168.0.24/29	1100 0000.1010 1000.0000 0000.0001 1000	Адреса підмережі
	255.255.255.248	1111 1111.1111 1111.1111 1111.1111 1000	Маска підмережі
	192.168.0.25	1100 0000.1010 1000.0000 0000.0001 1001	R4, інтерфейс 2
	192.168.0.26	1100 0000.1010 1000.0000 0000.0001 1010	H1
	192.168.0.27	1100 0000.1010 1000.0000 0000.0001 1011	H2

Продовження таблиці А.1

Пі-дме ре-жа	Пул IP-адрес	Двійкова нотація	Призначення
	192.168.0.28	1100 0000.1010 1000.0000 0000.0001 1100	H3
	192.168.0.29	1100 0000.1010 1000.0000 0000.0001 1101	H4
	192.168.0.30	1100 0000.1010 1000.0000 0000.0001 1110	H5
	192.168.0.31	1100 0000.1010 1000.0000 0000.0001 1111	Широкомов. адр.
S_h5	192.168.0.32/29	1100 0000.1010 1000.0000 0000.0010 0000	Адреса підмережі
	255.255.255.248	1111 1111.1111 1111.1111 1111.1111 1000	Маска підмережі
	192.168.0.33	1100 0000.1010 1000.0000 0000.0010 0001	R5, інтерфейс 2
	192.168.0.34	1100 0000.1010 1000.0000 0000.0010 0010	H1
	192.168.0.35	1100 0000.1010 1000.0000 0000.0010 0011	H2
	192.168.0.36	1100 0000.1010 1000.0000 0000.0010 0100	H3
	192.168.0.37	1100 0000.1010 1000.0000 0000.0010 0101	H4
	192.168.0.38	1100 0000.1010 1000.0000 0000.0010 0110	H5
	192.168.0.39	1100 0000.1010 1000.0000 0000.0010 0111	Широкомов. адр.

ДОДАТОК Б

Адресація підмереж маршрутизаторів

Таблиця Б.1 – Адресація підмереж маршрутизаторів S_R

Підмережа S_R	Пул IP-адрес	Двійкова нотація	Призначення
S_R1	10.6.0.0	0000 1010.0000 0110.0000 0000.0000 0000	Адреса підмережі
	255.255.255.252	1111 1111.1111 1111.1111 1111.1111 1100	Маска підмережі
	10.6.0.1	0000 1010.0000 0110.0000 0000.0000 0001	R1, інтерфейс 1
	10.6.0.2	0000 1010.0000 0110.0000 0000.0000 0010	R2, інтерфейс 1
	10.6.0.3	0000 1010.0000 0110.0000 0000.0000 0011	Широкомов. адр.
S_R2	10.6.0.4	0000 1010.0000 0110.0000 0000.0000 0100	Адреса підмережі
	255.255.255.252	1111 1111.1111 1111.1111 1111.1111 1100	Маска підмережі
	10.6.0.5	0000 1010.0000 0110.0000 0000.0000 0101	R2, інтерфейс 3
	10.6.0.6	0000 1010.0000 0110.0000 0000.0000 0110	R3, інтерфейс 1
	10.6.0.7	0000 1010.0000 0110.0000 0000.0000 0111	Широкомов. адр.
S_R3	10.6.0.8	0000 1010.0000 0110.0000 0000.0000 1000	Адреса підмережі
	255.255.255.252	1111 1111.1111 1111.1111 1111.1111 1100	Маска підмережі
	10.6.0.9	0000 1010.0000 0110.0000 0000.0000 1001	R3, інтерфейс 3
	10.6.0.10	0000 1010.0000 0110.0000 0000.0000 1010	R4, інтерфейс 3
	10.6.0.11	0000 1010.0000 0110.0000 0000.0000 1011	Широкомов. адр.
S_R4	10.6.0.12	0000 1010.0000 0110.0000 0000.0000 1100	Адреса підмережі
	255.255.255.252	1111 1111.1111 1111.1111 1111.1111 1100	Маска підмережі
	10.6.0.13	0000 1010.0000 0110.0000 0000.0000 1101	R1, інтерфейс 3
	10.6.0.14	0000 1010.0000 0110.0000 0000.0000 1110	R4, інтерфейс 1
	10.6.0.15	0000 1010.0000 0110.0000 0000.0000 1111	Широкомов. адр.
S_R5	10.6.0.16	0000 1010.0000 0110.0000 0000.0001 0000	Адреса підмережі
	255.255.255.252	1111 1111.1111 1111.1111 1111.1111 1100	Маска підмережі
	10.6.0.17	0000 1010.0000 0110.0000 0000.0001 0001	R5, інтерфейс 1
	10.6.0.18	0000 1010.0000 0110.0000 0000.0001 0010	R3, інтерфейс 4
	10.6.0.19	0000 1010.0000 0110.0000 0000.0001 0011	Широкомов. адр.

ДОДАТОК В

Інформація про маршрути вузлів в підмережах

Таблиця В.1 – Інформація про маршрути вузлів в підмережах

Маршрутизатор	Мереже призначення/ маска	Шлюз	Метрика
R1	10.6.0.0/255.255.255.252	Пряме підключення	-
	10.6.0.12/255.255.255.252	Пряме підключення	-
	10.6.0.8/255.255.255.252	10.6.0.12	1
	10.6.0.4/255.255.255.252	10.6.0.0	1
	10.6.0.16/255.255.255.252	10.6.0.12	2
	10.6.0.16/255.255.255.252	10.6.0.0	2
	192.168.0.0/29/255.255.255.248	Пряме підключення	-
	192.168.0.8/29/255.255.255.248	10.6.0.0	1
	192.168.0.16/29/255.255.255.248	10.6.0.12	2
	192.168.0.16/29/255.255.255.248	10.6.0.0	2
	192.168.0.24/29/255.255.255.248	10.6.0.12	1
	192.168.0.32/29/255.255.255.248	10.6.0.0	3
	192.168.0.32/29/255.255.255.248	10.6.0.12	3
R2	10.6.0.0/255.255.255.252	Пряме підключення	-
	10.6.0.4/255.255.255.252	Пряме підключення	-
	10.6.0.8/255.255.255.252	10.6.0.4	1
	10.6.0.12/255.255.255.252	10.6.0.0	1
	10.6.0.16/255.255.255.252	10.6.0.4	1
	192.168.0.8/29/255.255.255.248	Пряме підключення	-
	192.168.0.0/29/255.255.255.248	10.6.0.0	1
	192.168.0.16/29/255.255.255.248	10.6.0.4	1
	192.168.0.24/29/255.255.255.248	10.6.0.0	2
	192.168.0.24/29/255.255.255.248	10.6.0.4	2
	192.168.0.32/29/255.255.255.248	10.6.0.4	2
R3	10.6.0.4/255.255.255.252	Пряме підключення	-
	10.6.0.8/255.255.255.252	Пряме підключення	-
	10.6.0.16/255.255.255.252	Пряме підключення	-

Продовження таблиці В.1

Маршрутизатор	Мереже призначення/ маска	Шлюз	Метрика
	10.6.0.0/255.255.255.252	10.6.0.4	1
	10.6.0.12/255.255.255.252	10.6.0.8	1
	192.168.0.16/29/255.255.255.248	Пряме підключення	
	192.168.0.0/29/255.255.255.248	10.6.0.4	2
	192.168.0.0/29/255.255.255.248	10.6.0.8	2
	192.168.0.8/29/255.255.255.248	10.6.0.4	1
	192.168.0.24/29/255.255.255.248	10.6.0.8	1
	192.168.0.32/29/255.255.255.248	10.6.0.16	1
R4	10.6.0.8/255.255.255.252	Пряме підключення	-
	10.6.0.12/255.255.255.252	Пряме підключення	-
	10.6.0.0/255.255.255.252	10.6.0.12	1
	10.6.0.4/255.255.255.252	10.6.0.8	1
	10.6.0.16/255.255.255.252	10.6.0.8	1
	192.168.0.24/29/255.255.255.248	Пряме підключення	-
	192.168.0.0/29/255.255.255.248	10.6.0.12	1
	192.168.0.8/29/255.255.255.248	10.6.0.8	2
	192.168.0.8/29/255.255.255.248	10.6.0.12	2
	192.168.0.16/29/255.255.255.248	10.6.0.8	1
	192.168.0.32/29/255.255.255.248	10.6.0.8	2
R5	10.6.0.16/255.255.255.252	Пряме підключення	-
	10.6.0.0/255.255.255.252	10.6.0.16	2
	10.6.0.4/255.255.255.252	10.6.0.16	1
	10.6.0.8/255.255.255.252	10.6.0.16	1
	10.6.0.12/255.255.255.252	10.6.0.16	2
	192.168.0.32/29/255.255.255.248	Пряме підключення	-
	192.168.0.0/29/255.255.255.248	10.6.0.16	3
	192.168.0.8/29/255.255.255.248	10.6.0.16	2
	192.168.0.16/29/255.255.255.248	10.6.0.16	1
	192.168.0.24/29/255.255.255.248	10.6.0.16	2

ДОДАТОК Г

Адресація бездротового сегмента мережі

Таблиця Г.1 – Адреси бездротового сегменту мережі

Пул IP-адрес	Двійкова нотація	Призначення
192.168.0.40/29	1100 0000.1010 1000.0000 0000.0010 1000	Адреса підмережі
255.255.255.248	1111 1111.1111 1111.1111 1111.1111 1000	Маска підмережі
192.168.0.41	1100 0000.1010 1000.0000 0000.0010 1001	R5, інтерфейс 3
192.168.0.42	1100 0000.1010 1000.0000 0000.0010 1010	Точка доступу
192.168.0.43	1100 0000.1010 1000.0000 0000.0010 0011	Бездротовий клієнт 1
192.168.0.44	1100 0000.1010 1000.0000 0000.0010 0100	Бездротовий клієнт 2
192.168.0.45	1100 0000.1010 1000.0000 0000.0010 0101	Бездротовий клієнт 3
192.168.0.46	1100 0000.1010 1000.0000 0000.0010 0110	Бездротовий клієнт 4
192.168.0.47	1100 0000.1010 1000.0000 0000.0010 1111	Широкомовна адреса