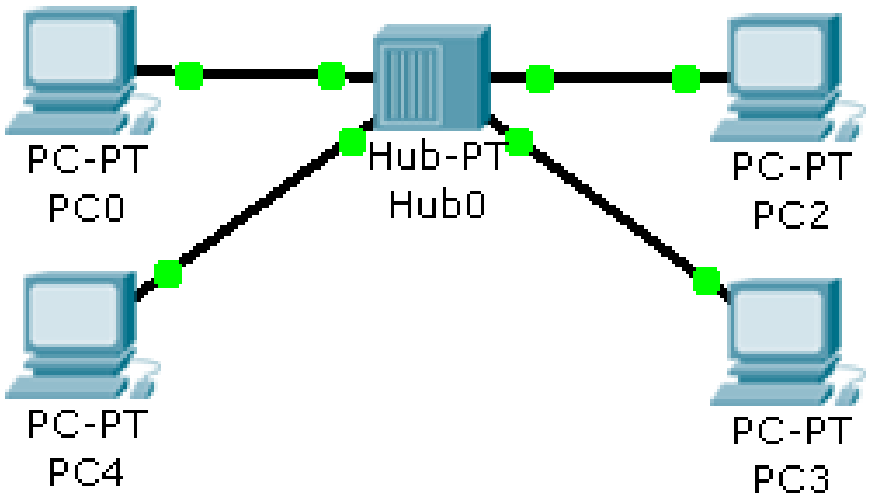
В. А. Гикавий, О. С. Городецька

Телекомунікаційні та інформаційні мережі



Міністерство освіти і науки України
Вінницький національний технічний університет

В. А. Гикавий, О. С. Городецька

Телекомунікаційні та інформаційні мережі

Лабораторний практикум

Вінниця
ВНТУ
2017

УДК [621.39+004.7](075)
ББК [32.88+32.973.202]я73
Г46

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки, молоді та спорту України (протокол № 10 від 30.05.2012 р.)

Рецензенти:
М. М. Климаш, доктор технічних наук, професор
О. М. Шинкарук, доктор технічних наук, професор
А. М. Пєтух, доктор технічних наук, професор

Гикавий, В. А.

Г46 Телекомунікаційні та інформаційні мережі : лабораторний практикум / В. А. Гикавий, О. С. Городецька. − Вінниця : ВНТУ, 2017. − 103 с.

У посібнику розкриваються основи побудови і функціонування телекомунікаційних мереж. Практичні завдання охоплюють проектування різних мереж з можливістю моделювання великої кількості пристроїв різного призначення та різних типів зв'язків, конфігурування вибраних пристроїв за допомогою термінального доступу чи командної стрічки, налаштування концентраторів та маршрутизаторів в мережах Ethernet, ознайомлення з принципом роботи різних протоколів стеку TCP/IP. Посібник розроблений відповідно до плану кафедри і відповідає програмам дисципліни «Телекомунікаційні та інформаційні мережі».

УДК [621.39+004.7](075)
ББК [32.88+32.973.202]я73

ЗМІСТ

ВСТУП

Початок XXI століття став часом стрімких технологічних змін в телекомунікаційній галузі. Виробники та оператори запропонували споживачам безліч нових послуг та пристроїв. Більшість технологічних інновацій виявилися затребуваними населенням, корпораціями і державами. Що стосується України, то протягом кількох років в країні реалізовується програма перебудови інфраструктури електрозв'язку і телекомунікаційних послуг за участю українських та іноземних компаній. Це потребує залучення фахівців телекомунікаційного напрямку, які б володіли достатнім багажем знань для впровадження та вдосконалення новітніх технологій.

В процесі підготовки фахівців у вищому навчальному закладі під час викладення дисциплін характерне становлення (як доповнення до теоретичної частини) ще однієї частини – обчислювальної, в основі якої лежить комп'ютерне моделювання. Безумовно, ця тенденція повинна знайти застосування у процесі викладання дисциплін. Комп'ютерний експеримент, який виконується не з реальною системою, а з її математичною моделлю, не лише багато в чому збагачує і полегшує вивчення традиційних аспектів дисципліни, а й дає ключ до вивчення багатьох важких для засвоєння питань, недоступних традиційним методам вивчення.

Включення в навчальний процес моделюючих комп'ютерних програм в галузі мережевих та комунікаційних технологій є своєчасним та абсолютно необхідним для майбутніх спеціалістів, що будуть займатися розробкою сучасних інформаційних систем і комплексів. У подальшому практичний досвід дозволить молодому спеціалісту набагато швидше та легше освоїтись на своєму першому робочому місці, оскільки практичні вміння, закладені ще у вищому навчальному закладі, гартують студента до реальної роботи.

Запропонований лабораторний практикум спрямований на освоєння принципів побудови та роботи мереж за допомогою безкоштовного емулятора Packet Tracer, що випускається фірмою Cisco.

Лабораторний практикум містить аналіз існуючих пакетів моделювання, опис середовища моделювання Packet Tracer, теоретичні відомості структурної та функціональної організації мереж. Практичні завдання спрямовані на побудову різних моделей мережі, налаштування маршрутизаторів та концентраторів, ознайомлення з принципом роботи різних протоколів, організацію взаємодії між декількома користувачами. Отримані знання дозволять створювати та моделювати мережі будь-якої складності, перевіряти на роботоздатність різні топології.

1 СПОСОБИ МОДЕЛЮВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Прогрес сучасної обчислювальної техніки уже зараз дає нам змогу набагато спростити процес практичного освоєння матеріалу. Це є дуже важливим моментом у технічних вузах, оскільки більшість із них не мають матеріальних ресурсів для закупівлі реального вузькопрофільного обладнання, для того, щоб навчати за допомогою нього студентів. Спрощення цієї задачі полягає у тому, що за допомогою сучасної обчислювальної техніки та відповідного програмного забезпечення можна замінити громіздке та неекономічне навчальне обладнання (стенди, макети, за допомогою яких досліджують роботу певних реальних моделей, систем чи пристроїв).

Що стосується процесу практичного освоєння дисциплін, які охоплюють сферу телекомунікацій, то це питання двояке. З однієї сторони є інформація, теоретичний матеріал. З іншої сторони – майже немає устаткування, яке б дало змогу практично освоїти отримані знання. Саме друга сторона цього аспекту буде вирішуватись.

Сфера телекомунікації достатньо стрімко розвивається і ледь не щороку відбувається прийняття все нових та нових стандартів роботи мереж та їх модифікацій. Із розрахунку на те, що кожен новий стандарт у подальшому буде широко використовуватись, програма моделювання, по-перше, повинна передбачати появу нового стандарту чи технології, по-друге, враховувати усі сучасні аспекти роботи обчислювальних мереж [1].

Якщо дивитись уже на комерційну діяльність з побудови мереж, то жоден проект великої мережі зі складною топологією в наш час не обходиться без вичерпного моделювання майбутньої мережі (принаймні таке правило прийнято у розвинутих країнах). Програми, що виконують це завдання, досить складні та дорогі. Метою моделювання є визначення оптимальної топології, адекватний вибір мережевого устаткування, визначення робочих характеристик мережі і можливих етапів майбутнього розвитку. Адже мережа, яка дуже точно оптимізована для рішень завдань поточного моменту, може потребувати серйозних переробок в майбутньому. На моделі можна випробувати вплив сплесків широкомовних запитів або реалізувати режим колізії (для Ethernet), що навряд чи хтось може собі дозволити в працюючій мережі.

У процесі моделювання з’ясовуються такі параметри.

1. Граничні пропускні спроможності різних фрагментів мережі і залежності втрат пакетів від завантаження окремих станцій і зовнішніх каналів.

2. Час відгуку основних серверів в різних режимах, у тому числі таких, які в реальній мережі украй небажані.

3. Вплив установлення нових серверів на перерозподіл інформаційних потоків (Proxy, Firewall тощо).

4. Рішення оптимізації топології при виникненні вузьких місць в мережі (розміщення серверів, DNS, зовнішніх шлюзів, організація опорних каналів та ін.).

5. Вибір того чи іншого типу мережевого обладнання або режиму його роботи (наприклад, cut-through, store-and-forward для мостів і перемикачів тощо).

6. Вибір внутрішнього протоколу маршрутизації і його параметрів (наприклад, метрики).

7. Визначення гранично допустимого числа користувачів того або іншого сервера.

8. Оцінювання необхідної смуги пропускання зовнішнього каналу для забезпечення необхідного рівня якості сервісу.

9. Оцінювання впливу мультимедійного трафіка на роботу локальної мережі, наприклад, при підготовці відеоконференцій.

Перераховані завдання висувають різні вимоги до програм. В одних випадках достатньо провести моделювання на фізичному (MAC) рівні, в інших потрібний вже рівень транспортних протоколів (наприклад, UDP і TCP), а для найбільш складних завдань потрібно відтворити поведінку прикладних програм. Все це повинно враховуватися при виборі або розробці моделюючої програми. Адже потрібно врахувати, що машина повинна тією чи іншою мірою відтворити дії всіх машин в модельованій мережі. Таким чином, машина ця повинна бути досить швидкодіючою та, незважаючи на це, моделювання однієї секунди роботи мережі може зайняти при певних умовах не одну годину.

Результати моделювання повинні мати точність 10-20%, тому що цього достатньо для більшості цілей і вона не потребує занадто багато машинного часу. Слід мати на увазі, що для моделювання поведінки реальної мережі треба знати всі її робочі параметри: довжину кабелю від концентратора до конкретної ЕОМ, затримку використовуваних кабелів, затримку концентраторів (цей параметр часто відсутній у документації і його доведеться брати з документації на мережевий протокол, наприклад з IEEE 802.3). Параметри можуть бути визначені і прямим вимірюванням. Чим точніше відтворюється поведінка мережі, тим більше машинного часу це потребуватиме. Крім того, необхідно зробити деякі припущення щодо розподілу завантаження для конкретних ЕОМ і інших мережевих елементів, затримок в перемикачах, мостах, часу обробки запитів в серверах. Тут потрібно враховувати і характер розв’язуваних на ЕОМ задач. http та ftp-сервер або звичайна персональна робоча станція створюють різні мережеві трафіки. Певний вплив на результат можуть надавати і використовувані ОС. У разі моделювання мережі можна здійснити відповідні вимірювання, що складно реалізувати в реальних умовах.

2 АНАЛІЗ ІСНУЮЧИХ ПАКЕТІВ МОДЕЛЮВАННЯ

Вирішення проблеми практичного навчання має два шляхи. З однієї сторони можна мати реальне обладнання та за допомогою нього виконувати процес навчання. Але при цьому треба враховувати, що таке обладнання не є розповсюдженим і є, відповідно, дорогим, а також воно достатньо громіздке та потребує належного обслуговування.

З іншої сторони, процес можна у багатьох моментах автоматизувати, спростити та здешевити шляхом віртуалізації вищезгаданого обладнання – звичайна програмна симуляція роботи пристроїв на персональних комп'ютерах.

Специфіка проектування лабораторного практикуму з дисципліни «Телекомунікаційні та інформаційні мережі» полягає у тому, що нам потрібно найоптимальніше визначити, яким чином має здійснюватись процес симуляції і віртуалізації навчального процесу. І лише після того, як ми визначимось із цими моментами, ми поставимо перед собою задачу розробки методики реалізації цього процесу.

Виходячи із специфіки нашої дисципліни, яка полягає у вивченні роботи різного типу локальних та глобальних мереж (далі ТКІМ), варто відзначити, що симулювати ми будемо саме роботу інформаційних мереж.

Виходячи із цих міркувань, ми повинні дослідити усі можливі варіанти програмної симуляції роботи ТКІМ, що полягає у вибранні програмного забезпечення, яке б могло задовольнити такі наші вимоги:

– програма симуляції роботи ТКІМ повинна відповідати технічним обчислювальним можливостям сучасної наявної обчислювальної техніки;

– програма симуляції роботи ТКІМ повинна бути зрозумілою для користувача і забезпечувати максимум комфорту у роботі з нею;

– програма симуляції роботи ТКІМ повинна дати змогу досліджувати максимально реальні процеси, які проходять у процесі роботи певного обладнання мереж;

– програма симуляції роботи ТКІМ повинна мати можливість моделювати роботу максимальної кількості сучасних пристроїв разом із усіма сучасними технологіями.

Враховуючи усі вищеперераховані вимоги до даного програмного забезпечення, приступимо до дослідження усіх широкорозповсюджених наявних програм симуляції роботи ТКІМ [4]. Продукти для моделювання роботи мережі значно відрізняються один від одного за ціною, складністю і функціональними можливостями.

CNET – симулятор комп'ютерних мереж, який не зосереджений на промисловому моделювання, а лише для ознайомчих чи навчальних цілей. Дає змогу експериментувати із різними даними канального, мережевого та транспортного рівнів мереж. Вона була спеціально розроблена для відвідувачів підготовчих комп'ютерних курсів.

NetMaker XA від Make Systems отримав нагороду World Class ("Продукт світового класу"). Обчислювальне ядро моделювання, що використовується в NetMaker XA - одне з найбільш потужних на ринку. До переваг програми відноситься висока продуктивність, величезна кількість додаткових модулів, у тому числі бібліотек пристроїв від різних виробників, додатковий модуль для аналізу витрат, функція розробки планів відновлення після відмови. Головні недоліки NetMaker XA – необхідність серйозного навчання користувача та висока вартість. Якщо до ціни базової конфігурації додати вартість додаткових модулів, вийде досить значна сума. Основу продукту складають модулі Visualizer, Planner і Designer. Кожен з них виконує якусь одну функцію; щоб змоделювати роботу мережі, необхідні всі три. Вартість базового комплекту – від 37 тисяч доларів. Якщо є необхідність придбати модулі Accountant, Interpreter і Analyzer, доведеться заплатити ще 30 тисяч доларів. Встановити NetMaker XA можна тільки на SPARCstation від Sun Microsystems.

COMNET Predictor від CACI Products – пакет для моделювання роботи мережі, до переваг якого відносяться можливість введення даних про трафік в режимі реального часу, простота введення гіпотез про зростання трафіка з плином часу. Вартість продукту 29 тисяч доларів.

GloMoSim – масштабоване середовище для моделювання проводових та безпроводових мережевих систем (стільникових). Програма є комерційною і обмежує багато можливостей при використанні безкоштовної версії.

GTNetS – повнофункціональне мережеве середовище моделювання, яке дозволяє досліджувати дію невеликих за розміром мереж у різних умовах.

NCTUns – високоякісна і розширювана система моделювання мереж і емулятора, здатна імітувати різні протоколи, що використовуються як в проводових, так і безпроводових мережах IP. NCTUns може бути використана як емулятор, який безпосередньо використовує Linux TCP/IP стек протоколів і дає високу достовірність результатів моделювання, і має багато інших цікавих властивостей.

NetSim – освітнє програмне забезпечення для моделювання мереж, яке містить модулі для програмування мереж. Протоколи, які охоплюються в моделюванні: Aloha, slotted Aloha, Ethernet, Token Ring, Token Bus, W-Lan, X.25 Frame Relay, ATM, TCP; також пристрої, такі як комутатори, маршрутизатори, точки доступу тощо. Програмний продукт є комерційним.

Ns2 – дискретний симулятор, направлений на створення дослідницьких мереж. Ns2 надає істотну підтримку для моделювання TCP, маршрутизації і багатоадресових протоколів по проводових і безпроводових (місцевих і супутникових) мережах. Ns2 – це програмний продукт з відкритим вихідним кодом.

OMNeT++ – тренажер, який використовується для моделювання: комунікаційних протоколів, комп’ютерних мереж і моделювання руху, багатопроцесорних і розподілених систем тощо. OMNeT++ також підтримує

анімацію та інтерактивні дії. Програмний продукт розповсюджується на вільній основі.

Suite OPNET's – середовище прогнозованого моделювання і вивчення мережевих технологій, яке дозволяє проектувати, розгортати і керувати мережевими інфраструктурами, мережевим обладнанням та мережевими додатками. Зокрема OPNET Modeler це середовище розробки, що дозволяє розробляти і досліджувати комунікаційні мережі, пристрої, протоколи та програми.

ARSEC – мова моделювання, яка ґрунтується на основі мови програмування C, розроблена в Каліфорнійському університеті для послідовного і паралельного виконання дискретного моделювання. Вона також може бути використана паралельно з мовою програмування. Вона доступна у вигляді бінарних файлів тільки для академічних інститутів.

Packet Tracer – потужний симулятор мереж, розроблений з метою надання студентам і викладачам інструментів, які дадуть змогу освоїти принципи побудови та роботи мереж. Дає змогу симулювати мережі практично будь-якої складності. Також дає можливість:

– симулювати локальну мережу з використанням маршрутизаторів, комутаторів, точок доступу тощо;

– робити великий вибір різних конфігурацій мережевого обладнання;

– симулювати командний рядок і багато іншого.

Середовище дає змогу працювати у двох режимах. Перший – простий, який дозволить початківцям ознайомитись із основами роботи з середовищем та мережами в цілому. Звичайний режим дає багато можливостей щодо налаштування мереж і є більш інформативним та деталізованим.

Програма є кросплатформовою, тобто, може працювати під управлінням різних операційних систем.

Порівнюючи усі вищеперераховані програмні додатки, можемо зробити висновок що для нас найбільше підходить програмний пакет Packet Tracer, оскільки він має найширші можливості для вивчення мереж [5]. У ньому є адаптовані режими як для початківців, так і для більш досвідчених користувачів. Програмний пакет не обмежується вузьким переліком технологій та пристроїв і дає можливість розробляти, реалізувати, випробовувати нові технології. Важливим є той факт, що програмний продукт розповсюджується вільно.

3 СЕРЕДОВИЩЕ МОДЕЛЮВАННЯ PACKET TRACER 5.2

Середовище моделювання локальних обчислювальних мереж має віконну структуру та може запускатись під операційними системами Microsoft Windows та Linux.

Мінімальні системні вимоги пакета:

– центральний процесора: x86-сувмісний, 300 МГц;

– операційна система: Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Vista, Fedora 7 (або вище), Ubuntu 7.10 (або вище);

– оперативна пам’ять: 96 MB;

– жорсткий накопичувач: 250 MB вільного місця;

– роздільна здатність екрана: 800 на 600 пікселів;

– наявність встановленого програвача Adobe Flash Player.

Умовно головне вікно програми розділено на функціональні поля (рисунок 3.1).

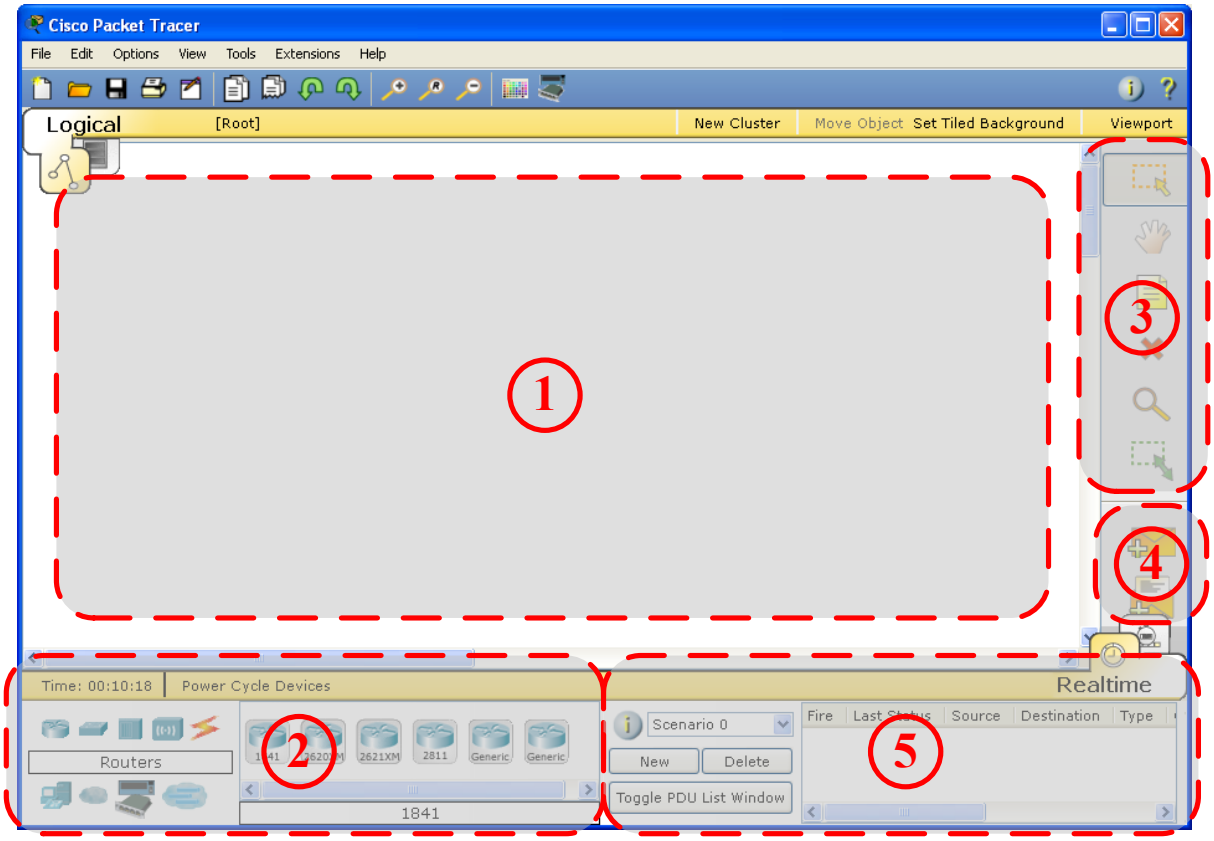


Рисунок 3.1 – Головне вікно пакета Packet Tracer 5.2

1. Поле логічної структури мережі. На дане поле перетягується обладнання, з якого формується майбутня мережа.

2. Бібліотека обладнання. У ній міститься усе обладнання, яке класифіковано за класами (ліворуч) та за типами чи моделями (праворуч):

– – маршрутизатори (роутери);

– – комутатори (свіч);
– – концентратори (хаб);
– – безпроводове обладнання
– – фізичні з’єднання, серед яких можна вибрати:
– – автоматичний вибір типу з’єднання;
– – консольний кабель;
– – прямий тип з’єднувального кабелю (патч-корд) ;
– – тип з’єднувального кабелю «крос-овер» (перехресний);
– – волоконно-оптичний кабель;
– – телефонний кабель;
– – коаксіальний кабель;
– – дата-кабель стандарту RS-232 DCE;
– – дата-кабель стандарту RS-232 DTE;
– – кінцеві пристрої:
– – ПК/ноутбук;
– – сервер;
– – принтер;
– – телефон;
– – емулятор глобальних мереж;
– – обладнання зі встановленим набором кількох плат розширення;
– – багатокористувацький інтерфейс.

3. Кнопки керування об’єктами логічної структури мережі:
– – кнопка вибору обладнання;
– – кнопка переміщення поля логічної структури мережі;
– – кнопка підписування обладнання;
– – кнопка видалення обладнання з поля логічної структури;
– – кнопка виклику меню перевірки окремих властивостей обладнання;
– – кнопка зміни розміру.

4. Кнопки, які відповідають за візуальне моделювання потоків даних.
– – кнопка виконання ping-запиту між двома вузлами (пінгування);
– – кнопка формування складного пакета даних.

5. Вікно спостереження за пакетами візуального моделювання потоків даних. Дане вікно використовується для прослідковування передачі ping-запитів чи складних пакетів. Поле Source вказує на ім’я вузла, від якого надходить пакет, поле Destination вказує на ім’я вузла-приймача пакета. У полі Last Status показується чи вдало відправлено чи прийнято пакет.

3.1 Робота з логічним полем

Розглянемо основні операції при роботі з логічним полем [2]. Винесемо потрібне нам обладнання на логічне поле. Для початку має бути активна

кнопка вибору обладнання. Далі серед бібліотеки обладнання вибираємо категорію «маршрутизатори», праворуч – маніпулятором клацаємо на модель «1841», після цього повторно маніпулятором клацаємо на логічне поле. Після цих операцій на логічному полі має з'явитись зображення маршрутизатора.

Аналогічними діями винесемо на логічне поле маршрутизатор моделі «2620XM».

Для зручної роботи з логічним полем пакет Packet Tracer передбачає переміщення одного або кількох об'єктів всередині логічно поля. Щоб перемістити об'єкт або групу об'єктів, їх необхідно виділити мишею. Для цього потрібно поза об'єктом натиснути лівою кнопкою миші та провести мишею таким чином, щоб усі необхідні елементи помістились у створений прямокутник із пунктирної лінії. Виділений об'єкт чи групу об'єктів можна переміщувати по логічному полі затиснувши їх лівою кнопкою миші.

Розглянемо, яким чином здійснюється фізичне з'єднання двох маршрутизаторів між собою. Для цього у бібліотеці активного обладнання зробимо активною категорію «Фізичні з'єднання». У полі типу фізичного з'єднання одинарним клацанням маніпулятора виберемо тип з'єднання «крос-овер» (кросовий). Далі клацаємо на один із пристроїв, які ми раніше винесли на логічне поле. Після цього з'явиться меню, у якому будуть відображатись можливі для підключення порти. Вибираємо порт «FastEthernet0/0». Далі, клацаємо маніпулятором на другий маршрутизатор і аналогічним чином вибираємо однойменний порт «FastEthernet0/0» для другого маршрутизатора. Таким чином на логічному полі має знаходитись два маршрутизатори, між якими виконано фізичне кросове з'єднання (рисунок 3.2). Аналогічним шляхом виконується з'єднання між іншими типами пристроїв та фізичними з'єднаннями інших типів.

Рисунок 3.2 – Виконання фізичного з'єднання між обладнанням

Червона, оранжева або зелена індикація на фізичному з'єднані біля кожного пристрою показує, чи увімкнений порт пристрою і чи виконано з'єднання. Червона чи оранжева індикація показує, що зв'язку немає, зелена індикація показує, що зв'язок виконано.

Для зручності у роботі з численним обладнанням варто його підписувати, для чого існує кнопка підписування. Для цього робимо її активною і клацаємо маніпулятором на відповідний маршрутизатор і підписуємо його зручним для нас чином.

Для видалення обладнання чи частини фізичних з'єднань з логічного поля робимо активною кнопку видання обладнання і клацаємо маніпулятором на непотрібне нам обладнання.

Перейдемо до перегляду властивостей обладнання. Для цього подвійним клацанням миші на перший маршрутизатор викликаємо вікно властивостей (рисунок 3.3). Активною є вкладка Physical.

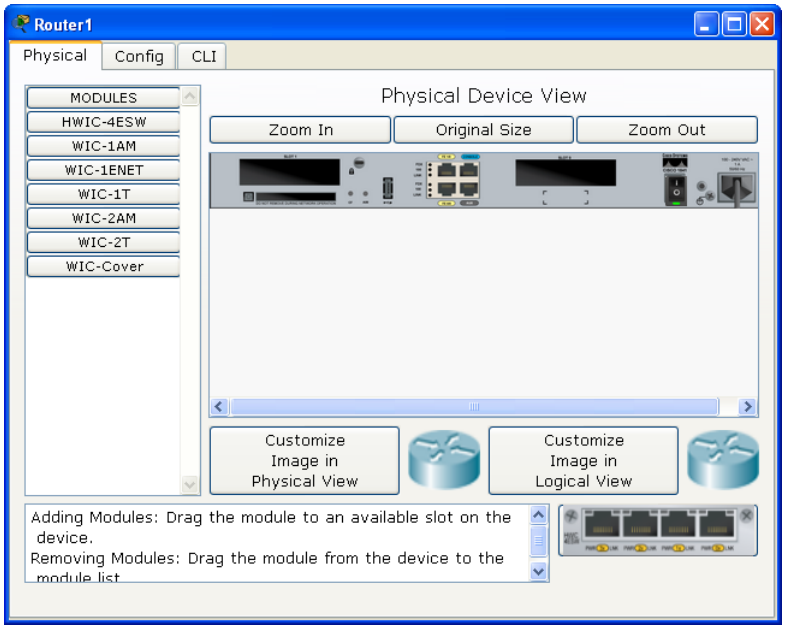


Рисунок 3.3 – Вікно властивостей обладнання

У вікні наочно відображено, які інтерфейси має маршрутизатор, а також вільні місця, куди можна вмонтувати додаткове обладнання (платами розширення). Безпосередньо самі плати розширення знаходяться під кнопкою «Modules» у лівій частині вікна властивостей маршрутизатора.

Перед тим, як розпочати монтувати додаткові плати розширення, обов'язково потрібно вимкнути живлення маршрутизатора. Для цього потрібно маніпулятором клацнути на зображення кнопки живлення у вікні властивостей маршрутизатора. Після цього має згаснути індикація живлення.

Далі ліворуч вибираємо необхідну нам плату розширення, скажімо, WIC-2T. У низу вікна з'явиться її наочне зображення, яке ми повинні перетягнути маніпулятором у вільний слот (роз'єм) на зображенні маршрутизатора (рисунок 3.4). Якщо живлення не було вимкнуто, то про це нагадає повідомлення, і плату розширення неможливо буде встановити.

Вкладка Config дає можливість ручного настроювання маршрутизатора, яке полягає у звичайному введені параметрів у заздалегідь визначені поля.

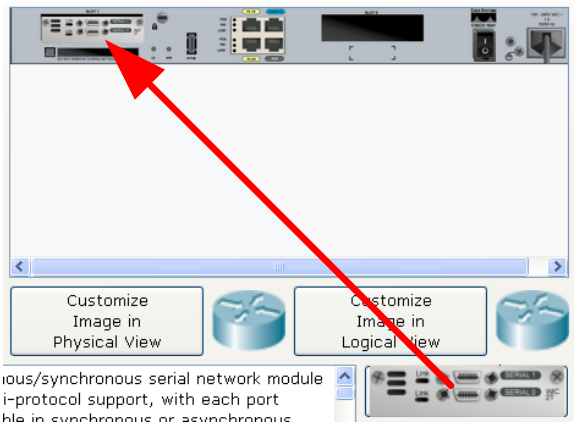


Рисунок 3.4 – Наочне зображення апаратури у вікні властивостей

Вкладка CLI дає змогу задавати параметри роботи маршрутизатора з консолі (командного рядка Cisco OIS) і спостерігати за їх виконанням. Даний режим дає більше можливостей для налаштування апаратури. Перехід на вкладку CLI автоматично запускає командний термінал, з якого виконується введення необхідних команд.

3.2 Опис режиму термінала

Маршрутизатор чи комутатор конфігурується у командному рядку операційної системи Cisco IOS. При роботі в командному рядку Cisco IOS існує кілька контекстів (режимів введення команд).

Контекст користувача відкривається при підключенні до маршрутизатора; зазвичай при підключенні через мережу потрібно пароль, а при підключенні через консольний порт пароль не потрібен. У контексті користувача доступні тільки прості команди (деякі базові операції для моніторингу), які не впливають на конфігурацію маршрутизатора. Вигляд запрошення командного рядка – «router>». Замість слова маршрутизатор виводиться ім’я маршрутизатора, якщо воно встановлено.

Контекст адміністратора (контекст «axes») відкривається командою «enable», поданою в контексті користувача. У контексті адміністратора доступні команди, що дозволяють отримати повну інформацію про конфігурацію маршрутизатора та його стан, команди переходу в режим конфігурування, команди збереження та завантаження конфігурації. Вигляд запрошення командного рядка – «router #».

Зворотний перехід до контексту користувача відбувається за командою «disable» або після закінчення встановленого часу неактивності. Завершення сеансу роботи – команда «exit».

Глобальний контекст конфігурування відкривається командою конфігурації термінала ("конфігурувати через термінал"), поданою в контексті адміністратора. Глобальний контекст конфігурування містить як безпосе-

редньо команди конфігурування маршрутизатора, так і команди переходу в контексти конфігурування підсистем маршрутизатора, наприклад:

- контекст конфігурування інтерфейсу відкривається командою interface імя_інтерфейсу (наприклад interface serial0), поданою у глобальному контексті конфігурування;
- контекст конфігурування процесу динамічної маршрутизації відкривається командою router протокол номер_процесу (наприклад, router ospf 1, поданою в глобальному контексті конфігурування.

Існує безліч інших контекстів конфігурування. Деякі контексти конфігурування знаходяться всередині інших контекстів конфігурування.

Вигляд запрошення командного рядка в контекстах конфігурування, які будуть зустрічатись найчастіше:

- router (config) # /глобальний/;
- router (config-if) # /інтерфейсу/;
- router (config-router) # /динамічної маршрутизації/;
- router (config-line) # /термінальної лінії/.

Вихід з глобального контексту конфігурації в контекст адміністратора, а також вихід з будь-якого підконтексту конфігурації в контекст верхнього рівня здійснюється командою «exit» або Ctrl-Z. Крім того, команда «end», подана в будь-якому з контекстів конфігурування негайно завершує процес конфігурування і повертає оператора в контекст адміністратора.

Будь-яка команда конфігурації вступає в дію негайно після введення, а не після повернення в контекст адміністратора.

Всі команди і параметри можуть бути скорочені (наприклад, «enable» – «en», «configure terminal» – «conf t»); якщо скорочення виявиться неоднозначним, маршрутизатор повідомить про це, а після натискання табуляції видасть варіанти, відповідні введеному фрагменту].

У будь-якому місці командного рядка для отримання допомоги може бути використаний знак питання:

- router #? /Список всіх команд даного контексту з коментарями/;
- router # co? /Список всіх слів у такому контексті введення, що починаються на «co», пробілу перед знаком питання немає/;
- router # conf ? /Список всіх параметрів, які можуть слідувати за командою «config» перед знаком запитання є пробіл/.

3.3 Список команд

Список команд згрупований відповідно до контекстів, відповідно до яких вони застосовуються [3]. У списку виділено основні команди.

1. Глобальний контекст конфігурування.

1.1. Команда «Access-list».

Критерії фільтрації задаються в списку операторів дозволу та заборони, який називається списком доступу. Рядки списку доступу порівнюють-

ся з IP-адресами та іншою інформацією пакета даних послідовно в тому порядку, в якому були задані, поки не буде знайдено збігу. При збігу здійснюється вихід зі списку. При цьому робота списку доступу безпосередньо залежить від порядку проходження рядків.

Списки доступу мають 2 правила: «permit» – дозволити, і «deny» – заборонити. Саме вони визначають, пропустити пакет далі чи заборонити йому доступ.

Списки доступу бувають двох типів: standard – стандартні (номери від 1 до 99) і extended – розширені (номери від 100 до 199). Відмінності полягають у можливості фільтрувати пакети не тільки за IP-адресою, але і за іншими параметрами.

Формат команди (стандартні списки доступу):

access-list номер_списку/ім'я правило ABCD abcd, де ABCD abcd – IP-адреса та маска, відповідно.

1.2. Команда «Enable secret».

Зазвичай при вході в привілейований режим потрібно ввести пароль. Ця функція дозволяє запобігти несанкціонованому доступу в даний режим, адже саме з нього можна змінювати конфігурацію пристрою. Ця команда дозволяє встановити такий пароль.

Формат команди:

enable secret пароль.

Після того, як було встановлено пароль, при спробі входу в привілейований режим, комутатор видає запит на введення пароля – в іншому випадку вхід буде неможливий.

1.3. Команда «Interface».

Команда для входу в режим конфігурування інтерфейсів пристрою. Даний режим є одним з підмножин режиму глобального конфігурування і дозволяє настроювати один з наявних мережевих інтерфейсів (fa 0/0, s 2/0 тощо). Всі зміни, що вносяться в конфігурацію комутатора в даному режимі, відносяться тільки до вибраного інтерфейсу.

Можливі варіанти формату команд:

interface тип порт;

interface тип слот/порт;

interface тип слот/підслот/порт.

Після введення команди із зазначеним інтерфейсом користувач має можливість приступити до його конфігурації. Необхідно зауважити, що, перебуваючи в режимі конфігурування інтерфейсу, вид запрошення командного рядка не відображає ім'я даного інтерфейсу.

1.4. Команда «Ip route».

Статична маршрутизація передбачає фіксовану структуру мережі: кожен маршрутизатор в мережі точно знає, куди потрібно відправляти пакет, щоб він був доставлений за призначенням. Для цього можна прописати статичні маршрути, використовуючи дану команду. Команда може бути записана у двох форматах:

ip route A.B.C.D a.b.c.d A1.B1.C1.D1,

де ABCD і abcd – мережева адреса і маска підмережі, куди необхідно доставити пакети, A1.B1.C1.D1 – IP-адреса наступного маршрутизатора або адреса мережі іншого маршрутизатора з таблиці маршрутизації, куди повинні переадресовуватися пакети;

ip route ABCD abcd вихідний_інтерфейс_поточного_ маршрутизатора.

1.5. Команда «Hostname».

Ця команда використовується для зміни імені пристрою.

Формат команди:

hostname нове_ім'я.

1.6. Команда «Router rip».

Ця команда дозволяє включити RIP-протокол. При його використанні відпадає необхідність вручну прописувати всі маршрути – необхідно лише вказати адреси мереж, з якими потрібно обмінюватися даними.

Приклад виконання команди:

Router (config) # router rip

Router (config-router) #

Ця команда включає RIP-протокол у конкретному маршрутизаторі. Подальше налаштування проводиться з відповідного контексту маршрутизації.

2. Контекст конфігурування інтерфейсу.

2.1. Команда «Ip access-group».

Ця команда використовується для накладання списків доступу. Список накладається на конкретний інтерфейс, і вказується один з двох параметрів: «in» (на вхідні пакети) або «out» (на вихідні). Необхідно знати, що на кожному інтерфейсі може бути включений тільки один список доступу.

Формат команди:

ip access-group номер_списку/імя_параметр

2.2. Команда «Bandwidth».

Ця команда використовується тільки в послідовних інтерфейсах і служить для встановлення ширини смуги пропускання. Значення встановлюється в кілобітах.

Формат команди:

bandwidth ширина_смуги_пропускання.

2.3. Команда «Clock rate».

Для коректної роботи ділянки мережі, де використовується послідовний мережевий інтерфейс, один з комутаторів третього рівня повинен задавати тактову частоту. Це може бути кінцевий кабельний пристрій DCE. Оскільки маршрутизатори CISCO є за замовчуванням пристроями DTE, то необхідно явно вказати інтерфейсу на надання тактової частоти, якщо цей інтерфейс працює в режимі DCE. Для цього використовують дану команду (значення встановлюється в бітах за секунду).

Формат команди:

clock rate тактова_частота.

2.4. Команда «Ip address».

Кожен інтерфейс повинен мати свою унікальну IP-адресу – інакше взаємодія пристроїв з даного інтерфейсу не зможе бути здійснена. Ця команда використовується для задання IP-адреси вибраному інтерфейсу.

Формат команди:

ip address A.B.C.D a.b.c.d,

де A.B.C.D a.b.c.d – IP-адреса і маска підмережі, відповідно.

2.5. Команда «No».

Ця команда застосовується у разі необхідності скасувати дію якої-небудь команди конфігурування.

Формат команди:

no команда_яку_необхідно_сксувати.

3. Контекст адміністратора.

3.1. Команда «Configure terminal».

Для конфігурації пристрою, що працює під управлінням IOS, слід використовувати привілейовану команду configure. Ця команда переводить контекст користувача в так званий «режим глобальної конфігурації» і має три варіанти:

- конфігурування з термінала;
- конфігурування з пам’яті;
- конфігурування через мережу.

У рамках даного лабораторного практикуму конфігурування буде проводитися тільки за допомогою термінала.

З режиму глобальної конфігурації можна робити зміни, які стосуються пристрою в цілому. Також даний режим дозволяє входити в режим конфігурування певного інтерфейсу.

Приклад виконання команди:

Router # configure terminal

Enter configuration commands, one per line. End with CNTL / Z.

Router (config) #

Перехід в режим глобальної конфігурації, про що свідчить змінений вигляд запрошення командного рядка.

3.2. Команда «Copy».

Після налаштування комутатора рекомендується зберігати його поточну конфігурацію. Інформація міститься в енергонезалежну пам’ять і зберігається там стільки, скільки потрібно. При необхідності всі налаштування можуть бути відновлені або скинуті.

Формат команди:

copy running-config startup-config - команда для збереження конфігурації;

copy startup-config running-config - команда для завантаження конфігурації.

3.3. Команда «Show».

Show (англ. – показувати) – одна з найголовніших команд, які використовуються під час налаштування комутаторів. Вона застосовується для перегляду інформації будь-якого роду і застосовується практично у всіх контекстах. Ця команда має більше всіх параметрів.

Розглянемо основні параметри.

3.3.1. Параметр «running-config» команди «Show».

Дана команда використовується для перегляду поточного роботоздатного стану комутатора.

Приклад виконання команди:

Switch # show running-config

!

version 12.1

!

hostname Switch

...

На екран виводяться поточні налаштування комутатора.

3.3.2. Параметр «startup-config» команди «Show».

Дана команда використовується для перегляду збереженої конфігурації.

Приклад виконання команди:

Switch # show startup-config

Using 1540 bytes

!

version 12.1

!

...

Якщо енергонезалежна пам’ять не містить інформації, тоді комутатор видасть повідомлення про те, що конфігурація не була збережена. (startup-config is not present).

3.3.3. Параметр «ip route» команди «Show».

Ця команда застосовується для перегляду таблиці маршрутів.

3.3.4. Параметр «ip protocols» команди «Show».

Ця команда використовується для перегляду протоколів маршрутизації, включених на конкретному пристрої.

3.4. Команда «Ping».

Для перевірки зв’язку між пристроями мережі можна використовувати дану команду. Вона відправляє луна-запити зазначеному вузлу мережі й фіксує відповіді.

Формат команди:

ping A.B.C.D.

4. Контекст користувача.

4.1. Команда «Enable».

Виконання конфігураційних або керуючих команд потребує входження в привілейований режим, використовуючи дану команду.

Приклад виконання команди:

Router> enable

Router #

При введенні команди маршрутизатор перейшов у привілейований режим. Для виходу з цього режиму використовується команда «disable» або «exit».

Також слід зазначити, що в даному контексті можна користуватися командою show для перегляду деякої службової інформації.

5. Контекст конфігурування маршрутизації.

5.1. Команда «Network».

Даною командою вказують адреси мереж, які будуть доступні даному маршрутизатору.

Формат команди:

network ABCD,

де ABCD – адреса мережі.

4 ВИМОГИ ДО ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ

Лабораторна робота є видом навчального заняття, на якому студенти під керівництвом викладача проводять натурні або імітаційні експерименти чи досліди в спеціально обладнаних навчальних лабораторіях з використанням устаткування, пристосованого до умов навчального процесу. Метою лабораторного заняття є практичне підтвердження окремих теоретичних положень даної навчальної дисципліни, набуття практичних умінь та навичок роботи з лабораторним обладнанням, обчислювальною технікою та вимірювальною апаратурою.

Виконання лабораторних робіт у обсязі, передбаченому навчальним планом, є обов'язковим. Студенти, які не виконали лабораторні роботи, відповідно до програми і робочого плану дисципліни до іспиту не допускаються.

Лабораторні роботи виконуються за фронтальним принципом – усі студенти виконують одну і ту ж лабораторну роботу в комп'ютерному класі за розкладом і під керівництвом викладача. При цьому для лабораторних робіт, які передбачають варіативність початкових даних, кожна бригада виконує індивідуальне завдання.

У випадку пропуску лабораторних занять студент зобов'язаний відпрацювати пропущене заняття за кафедральним графіком відпрацювання пропущених занять.

При підготовці до лабораторних занять студент повинен засвоїти лекційний матеріал та проглянути літературу з відповідних питань, уважно прочитати методичні вказівки до конкретної лабораторної роботи, уяснити послідовність її виконання і вимоги до оформлення кінцевих результатів, підготувати відповіді на контрольні запитання.

Під час виконання роботи студент зобов'язаний неухильно дотримуватись правил техніки безпеки. До самостійної роботи на комп'ютерах допускаються студенти після проходження інструктажу з охорони праці. При цьому дисплеї комп'ютерів повинні розташовуватись при однорядному їх розміщенні на відстані не менше 1,5 м. Забороняється встановлювати дисплеї екранами один проти одного. Кут нахилу екрана відносно вертикалі повинен складати 10 − 15 градусів, а відстань до екрана – 400 − 500 мм. Вмикати і вимикати комп'ютер студент повинен тільки вимикачами, забороняється проводити вимкнення вийманням вилки із розетки. При виявленні будь-яких несправностей комп'ютера під час роботи студенту необхідно доповісти викладачу. Забороняється переміщати і переносити блоки, обладнання, яке знаходиться під напругою, самостійно розбирати чи проводити ремонт комп'ютера. Під час роботи студент повинен бути уважним, не займатися сторонніми справами, не заважати іншим працюючим, сконцентрувати увагу на виконанні плану роботи та отриманих результатах.

Документування результатів роботи здійснюється у формі звіту, де вказується мета та порядок виконання роботи, наводяться схеми досліджу-

ваних мереж чи комунікаційного обладнання, аналізуються одержані результати, формулюються аргументовані висновки.

Виконана і належним чином оформлена лабораторна робота захищається шляхом співбесіди з викладачем. На захист студент має продемонструвати ґрунтовні знання з теорії, уміння застосовувати теорію на практиці. Захист виконаної лабораторної роботи здійснюється, як правило, під час виконання наступної роботи або за графіком консультацій. Результати захисту відображаються в журналі викладача. Звіти про виконання лабораторних робіт зберігаються і всі повинні бути наявними до початку іспиту.

5 ЛАБОРАТОРНІ РОБОТИ З ДОСЛІДЖЕННЯ РІЗНИХ МЕРЕЖ

Лабораторні роботи направлені на закріплення і розширення положень і навичок, набутих при вивченні теоретичного матеріалу та проведенні практичних занять.

Лабораторна робота № 1
IP-адресація

Мета: розглянути правила адресації мереж різних класів, провести моделювання IP-адресації в середовищі моделювання Packet Tracer 5.2, дослідити пряме та перехресне з'єднання комп'ютерів .

Теоретичні відомості

IP-адреса – унікальна мережева адреса вузла в комп'ютерній мережі, побудованій за протоколом IP. IP-адреса складається з двох частин: номера мережі і номера хоста. IP-адреса має довжину 4 байта і звичайно записується у вигляді чотирьох чисел, що являють значення кожного байта в десятковій формі, розділені крапками.

Існує 5 класів IP-адрес. Ці класи відрізняються один від одного кількістю бітів, що відведені на адресу мережі і адреси хостів в мережі [3]. У таблиці 4.1 наведені п'ять класів IP-адрес.

Особливі IP-адреси:

- якщо всі двійкові розряди IP-адреси рівні 1, то пакет з такою адресою призначення повинен розсилатися всім вузлам, що перебувають у тій же мережі, що й джерело цього пакета. Таке розсилання називається обмеженим широкомовним повідомленням (limited broadcast);
- якщо в полі номера вузла призначення стоять тільки одиниці, то пакет, що має таку адресу, розсилається всім вузлам мережі із заданим номером мережі. Таке розсилання називається широкомовним повідомленням (broadcast). Наприклад, в мережі 192.190.21.0 з маскою 255.255.255.0 пакет з адресою 192.190.21.255 доставляється всім вузлам цієї мережі.

Таблиця 5.1 - П'ять класів IP-адрес

Клас мережі	Розряди 0 - 7								Розряди 8 - 15	Розряди 16 - 23	Розряди 24 - 31
Клас A	0	Номер мережі							Номер хоста		
Клас B	1	0	Номер мережі							Номер хоста	
Клас C	1	1	0	Номер мережі							Номер хоста
Клас D	1	1	1	0	Групова адреса						
Клас E	1	1	1	1	0	Зарезервоване					

IP протокол (англ. IP − Internet protocol) − найбільш широко розповсюджена реалізація ієрархічної схеми мережевої адресації. Протокол відповідає за адресацію пакетів, але не відповідає за встановлення з'єднань, не є

надійним і дозволяє реалізувати тільки негарантовану доставку даних. Термін «протокол без встановлення з'єднань» (англ. connectionless) означає, що протокол для взаємодії не потребує виділеного каналу, як це відбувається під час телефонної розмови і не існує процедури виклику перед початком передачі даних між мережевими вузлами. Протокол IP вибирає найбільш ефективний шлях з числа доступних на основі рішень прийнятих протоколом маршрутизації [4].

У кожній наступній мережі, що лежить на шляху переміщення пакета, протокол IP звертається до засобів транспортування цієї мережі, щоб з їх допомогою передати пакет на маршрутизатор, що веде до наступної мережі, або безпосередньо на вузол-одержувач. Таким чином, однією з найважливіших функцій IP є підтримка інтерфейсу із нижчими рівнями мереж, що утворюють складову мережу. Крім того, у функції протоколу IP входить підтримка інтерфейсу з протоколами вищого транспортного рівня, зокрема з протоколом TCP, який вирішує всі питання забезпечення надійної доставки даних по складовій мережі в стеку TCP/IP. Протокол IP відноситься до протоколів без встановлення з'єднань, він підтримує обробку кожного IP-пакета як незалежної одиниці обміну, не пов'язаної з іншими IP-пакетами. У протоколі IP немає механізмів, які звичайно застосовуються для забезпечення достовірності скінченних даних. Якщо під час просування пакета відбувається будь-яка помилка, то протокол IP за своєю ініціативою нічого не робить для виправлення цієї помилки. Наприклад, якщо на проміжному маршрутизаторі пакет був відкинутий через помилку контрольної суми, то модуль IP не намагається наново послати втрачений пакет.

Відсутність надійності і негарантована доставка не означає, що система працює погано або ненадійно, а вказує лиш на те, що протокол IP не докладає ніяких зусиль, щоб перевірити чи був пакет доставлений за призначенням. Ці функції делеговані протоколам транспортного та вищих рівнів.

Формат IP-пакета. Є прямий зв'язок між кількістю полів заголовка пакета і функціональною складністю протоколу, який працює з цим заголовком. Чим простіший заголовок - тим простіший відповідний протокол. Більша частина дій протоколу пов'язана з обробкою тієї службової інформації, яка переноситься в полях заголовка пакета. Вивчаючи призначення кожного поля заголовка IP-пакета, ми отримуємо не тільки формальні знання про структуру пакета, але і ознайомлюємось із основними функціями протоколу IP. IP-пакет складається із заголовка і поля даних. Нижче перераховані поля заголовка (рисунок 5.1) [5].

Поле номера версії займає 4 біти і ідентифікує версію протоколу IP. Зараз повсюдно використовується версія 4 (IPv4), хоча все частіше зустрічається і нова версія (IPv6).

Значення довжини заголовка IP-пакета також посідає 4 біти і вимірюється у 32-бітових словах. Зазвичай заголовок має довжину в 20 байт (п'ять 32-бітових слів), але при додаванні деякої службової інформації це значен-

ня може бути збільшено за рахунок додаткових байтів в полі параметрів. Найбільш тривалий заголовок складає 60 байт.

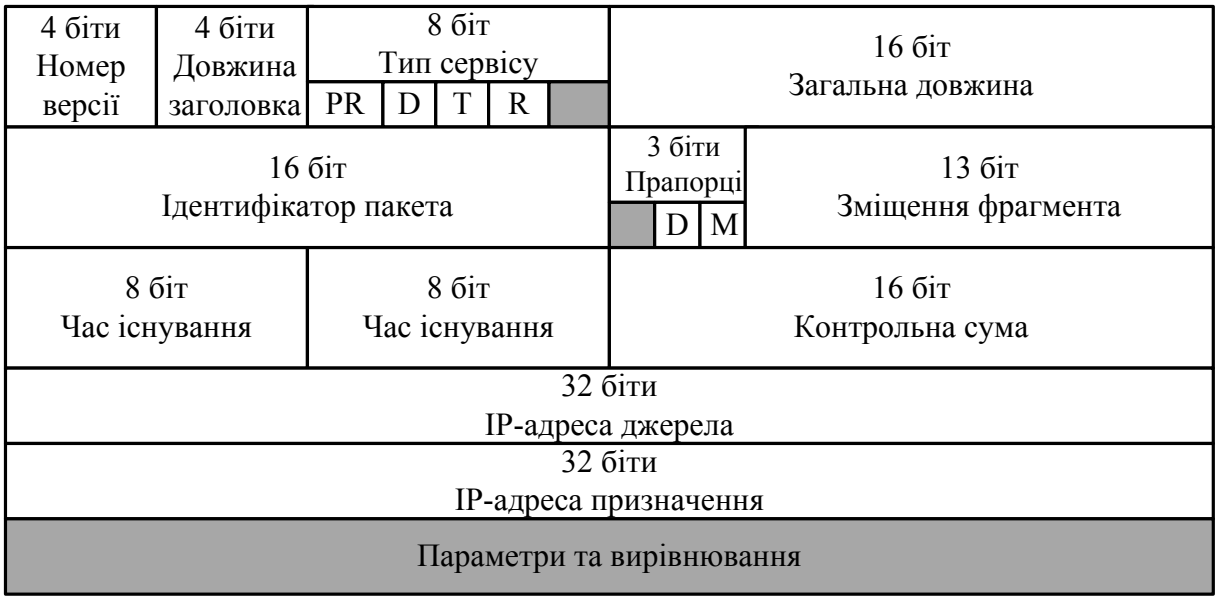


Рисунок 5.1 – Структура заголовка IP-пакета

Поле типу сервісу (Type of Service, ToS) має і іншу, більш сучасну назву – байт диференційованого обслуговування або DS-байт. Цим двом назвами відповідають два варіанти інтерпретації цього поля. В обох випадках поле використовується з однією метою – зберігання ознак, які відображають вимоги до якості обслуговування пакета. У попередньому варіанті перші три біти містять значення пріоритету пакета: від найнижчого – 0 до найвищого – 7. Маршрутизатори та комп'ютери можуть брати до уваги пріоритет пакета і обробляти більш важливі пакети в першу чергу. Наступні три біти поля ToS визначають критерій вибору маршруту. Якщо біт D (Delay – затримка) встановлений в 1, то маршрут повинен вибиратися для мінімізації затримки доставки даного пакета, встановлений біт T (Throughput – пропускна здатність) – для максимізації пропускної здатності, а біт R (Reliability – надійність) – для максимізації надійності доставки. Останніх два біти мають нульове значення.

Стандарти диференційованого обслуговування, прийняті наприкінці 90-х років, дали нове ім'я цьому полю і перевизначають призначення його бітів. У DS-байті також використовуються тільки старші 6 біт, а два молодших біти залишаються як резерв. Поле загальної довжини займає 2 байти і характеризує загальну довжину пакета з урахуванням заголовка і поля даних. Максимальна довжина пакета обмежена розрядністю поля, що визначає цю величину, і становить 65 535 байт, проте у більшості комп'ютерів та мереж настільки великі пакети не використовуються. При передачі мережами різного типу довжина пакета вибирається з урахуванням максимальної довжини пакета протоколу нижнього рівня, що несе IP-

пакети. Якщо це кадри Ethernet, то вибираються пакунки з максимальною довжиною 1500 байт, які розміщуються у полі даних кадру Ethernet. У стандартах TCP/IP передбачається, що всі хости повинні бути готові приймати пакети довжиною аж до 576 байт (незалежно від того, чи приходять вони цілком або фрагментами).

Ідентифікатор пакета займає 2 байти і використовується для розпізнавання пакетів, що утворилися шляхом поділу на частини (фрагментації) вихідного пакета. Всі частини (фрагменти) одного пакета повинні мати однакове значення цього поля.

Прапори займають 3 біти і містять ознаки, пов'язані з фрагментацією. Установлені в 1 біт DF (Do not Fragment – не фрагментувати) забороняє маршрутизатору фрагментувати даний пакет, а встановлений в 1 біт MF (More Fragments – більше фрагментів) вказує на те, що даний пакет є проміжним (не останнім) фрагментом. Залишковий біт зарезервований.

Поле зміщення фрагмента займає 13 біт і задає зсув у байтах поля даних цього фрагмента щодо початку поля даних вихідного нефрагментованого пакета. Використовується при складанні чи розбиранні фрагментів пакетів. Зсув повинен бути кратний 8 байтам.

Поле часу життя (Time Te Live, TTL) займає один байт і використовується для встановлення граничного терміну, протягом якого пакет може переміщатися мережею. Час життя пакета вимірюється в секундах і задається джерелом. Після закінчення кожної секунди перебування на кожному з маршрутизаторів, через які проходить пакет під час проходження по мережі, із його поточного часу життя віднімається одиниця; одиниця віднімається і в тому випадку, якщо час перебування був менший секунди. Оскільки сучасні маршрутизатори рідко обробляють пакет довше, ніж за одну секунду, то час життя можна інтерпретувати як максимальне число транзитних вузлів, які дозволено пройти пакету. Якщо значення поля часу життя стає нульовим до того часу, коли пакет досягає одержувача, пакет знищується. Таким чином, час життя є свого роду годинниковим механізмом самознищення пакета.

Поле протоколу верхнього рівня займає один байт і містить ідентифікатор, який вказує, до якого протоколу верхнього рівня належить інформація, яка розміщена у поле даних пакета. Наприклад, 6 означає, що в пакеті знаходиться повідомлення TCP, 17 – повідомлення UDP, 1 – повідомлення ICMP.

Контрольна сума заголовка займає 2 байти (16 біт) і розраховується тільки по заголовку. Оскільки деякі поля заголовка змінюють своє значення у процесі передачі пакета мережею (наприклад, поле часу життя), контрольна сума перевіряється і повторно розраховується на кожному маршрутизаторі і кінцевому вузлі як доповнення до суми всіх 16-бітових слів заголовка. При обчисленій контрольній сумі значення самого поля контрольної суми установлюється в нуль. Якщо контрольна сума неправильна, то пакет відкидається (виявлена помилка).

Поля IP-адрес джерела і приймача мають однакову довжину – 32 біти. Поле параметрів є необов'язковим і використовується зазвичай лише при налагодженні мережі. Це поле складається з декількох підполів. У цих підполях можна вказувати точний маршрут, реєструвати маршрутизатори, які проходить пакет, поміщати дані системи безпеки або тимчасові позначки.

Оскільки число підполів у полі параметрів може бути довільним, то у кінці заголовка повинно бути додано кілька нульових байтів для вирівнювання заголовка пакета по 32-бітовій границі.

Нижче наведено приклад значень полів заголовка одного з реальних IP-пакетів, отриманих у мережі Ethernet засобами аналізатора протоколів мережевого монітора. Тут в дужках подано шістнадцяткові значення полів.

IP: Version = 4 (0x4)
IP: Header Length = 20 (0x14)
IP: Service Type - 0 (0x0)
IP: Precedence = Routing
IP:.0 .... - Normal Delay
IP:.0 ... = Normal Throughput
IP: 0. = Normal Reliability
IP: Total Length = 54 (0x36)
IP: Identification = 31746 (0x7C02)
IP: Flags Summary = 2 (0x2)
IP: 0 - Last fragment in datagram
IP: 1. = Cannot fragment datagram
IP: Fragment Offset = 0 (0x0) bytes
IP-Time to Live - 128 (0x80)
IP: Protocol = TCP - Transmission Control
IP: Checksum = 0xEB86
IP: Source Address = 194.85 135.75
IP: Destination Address = 194.85.135.66
IP: Data: Number of data bytes remaining = 34 (0x0022)

Підмережа − це фізичний сегменг TCP/IP-мережі (наприклад, сегмент Ethernet), в якому використовується IP-адреса із загальним ідентифікатором мережі.

Використання підмереж надає такі основні переваги, як можливість використання в різних сегментах різних мережевих технологій (наприклад, Ethernet і Token Ring) та подолання обмежень на максимальну кількість хостів в одному сегменті.

Механізм розподілу на підмережі (subnetting, subnetworking) полягає у розбитті ідентифікатора вузла на дві групи бітів, перша з яких служить для ідентифікації сегмента об'єднаної мережі, а друга - для ідентифікації окремого вузла.

Адміністратор мережі маскує частину IP-адреси з метою використання її для призначення номерів підмережам. ***Маска підмережі*** − це 32-бітове значення, яке використовується для виділення (маскування) з IP-адреси її

частин: ідентифікаторів мережі і вузла. У масці підмережі всі біти, що відповідають ідентифікатору мережі встановлюються в 1, а всі біти, що відповідають ідентифікатору вузла, скидаються в 0.

Хід роботи

Дослідження перехресного з'єднання комп'ютер-комп'ютер.

1. Винести на логічне поле із бібліотеки обладнання комп'ютер та лептоп (ноутбук).

2. З'єднати комп'ютер та лептоп між собою перехресним кабелем, використовуючи у обох вузлах порти Fast Ethernet (рисунок 5.2).

3. Для того, щоб підняти зв'язок між двома вузлами, необхідно виконати конфігурацію їхніх мережевих адаптерів. Конфігурація полягає у присвоєнні адаптерам IP-адрес, причому діапазони нумерації IP-адрес мають знаходитись у межах нумерації мережі одного класу.

4. У логічному полі, клацнувши мишею на комп'ютер, викликати вікно його властивостей.

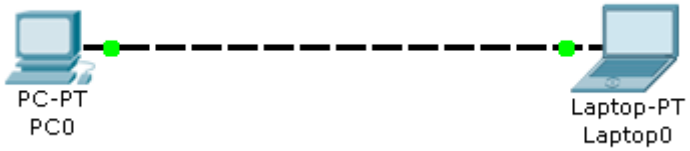


Рисунок 5.2 – Перехресне з'єднання двох вузлів

5. Потім потрібно перейти на вкладку Config та вибрати тип інтерфейсу Fast Ethernet.

6. У правій частині віна знайти поле IP Configuration і прослідкувати, чи радіокнопка увімкнена навпроти Static.

7. У полі для введення навпроти IP Address ввести наступну IP-адресу порту Fast Ethernet: 192.168.1.1. Крапка після останньої цифри не ставиться. Одразу після цього клацнути у поле для введення навпроти Subnet Mask. Поле автоматично має заповнити маску підмережі у вигляді: 255.255.255.0. Закрити вікно.

8. Аналогічним чином надати портові Fast Ethernet лептопу свою IP-адресу, причому її значення повинне відрізнятись від значення IP-адреси комп'ютера, а номер класу мережі у межах IP-адреси (у нашому випадку перших 3 байти) повинен бути таким самим, як і у комп'ютера.

9. Виконати перевірку правильності настроювання портів. Для цього серед кнопок, які відповідають за візуальне моделювання потоків даних, натиснути на кнопку ping-запитую. Вона має стати активною. Після цього натиснути на зображення комп'ютера на логічному полі, після цього на ньому має зафіксуватись зображення конверта. Не виконуючи жодних інших дій, натиснути на зображення лептопу.

10. Після виконання вищевказаних операцій необхідно проконтролювати, чи пакет дійшов від комп'ютера до лептопу. З цією метою у вікні

спостереження за пакетами ведеться облік передачі пакетів. Якщо після виконаної операції пінгування у полі Last Status помічено як Successful, то пінгування виконано вдало, якщо – Failed, то щось виконано неправильно і потрібно виконати налаштування портів спочатку.

11. Виконати пінгування у зворотному напрямку – від лептопу до комп'ютера.

Дослідження прямого з'єднання

1. Винести на логічне поле із бібліотеки обладнання: комп'ютер, лептоп та комутатор 2950-24.

2. З'єднати комп'ютер та лептоп із комутатором прямим мідним кабелем, використовуючи порти Fast Ethernet (рисунок 5.3). При цьому варто дочекатись, поки внутрішнє програмне забезпечення комутатора завантажиться, слідкуючи за тим, щоб індикація біля під'єднаних до комутатора ліній стала зеленою. Власне це і є ознакою того, що автоматична конфігурація портів комутатора виконана.

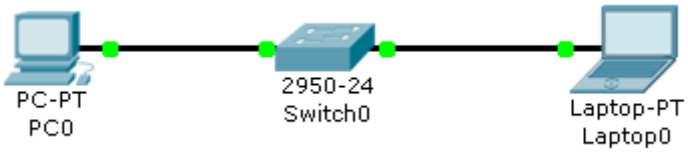


Рисунок 5.3 – Пряме з'єднання двох вузлів

3. Виконати пп. 4 – 11 з попереднього досліду.

4. Зробити загальні висновки по роботі.

Зміст звіту

1. Тема і мета роботи.
2. Короткі теоретичні відомості.
3. Завдання до лабораторної роботи.
4. Знімки екрана зі складеними схемами мереж при прямому і перехресному з'єднанні.
5. Результати проведеного пінгування.

Контрольні запитання

1. Що являє собою IP-адреса? Який розмір IP-адреси?
2. Скільки є класів адрес? Поясніть різницю між ними?
3. Поясніть, як клас IP-адреси визначає тип мережі і можливу кількість вузлів в ній.
4. Які спеціальні IP-адреси вам відомі?
5. До якого класу мереж відносяться адреси:

а) 10.45.195.174; б) 119.74.92.165; в) 127.0.0.1; г) 185.29.52.235;
д) 30.20.10.0; е) 191.255.67.244.

6. Для чого робиться розбиття на підмережі? Поясніть поняття маски підмережі? Для чого вони призначені?

7. Що таке широкомовна адреса?

8. Чому стандарти 100Base-T і 100Base-F витиснули стандарти Ethernet на коаксіальному кабелі?

9. Поясніть зміст кожного поля IP-кадра.

10. В чому полягає механізм розподілу на підмережі.

11. Поясніть принципи прямого і перехрестного з'єднання.

12. Що таке пінгування?

13. Які з наведених адрес не можуть бути використані як IP-адреса мережевого інтерфейсу для вузлів Інтернету? Для синтаксично правильних адрес визначте їхній клас: A, B, C, D або E. Варіанти адрес:

а) 223.13.123.245; б) 225.0.0.105; в) 194.87.45.0; г) 10.24.255.252;

д) 125.24.255.255; е) 157.213.255.305; ж) 129.12.255.255;

з) 127.0.23.255; і) 1.0.0.13; к) 221.1.1.1; л) 192.134.216.255;

м) 193.256.254.11.

14. Нехай IP-адреса деякого вузла підмережі рівна 108.5.18.167, а значення маски для цієї підмережі − 255.255.240.0. Визначіть номер підмережі. Яке максимальне число мережевих інтерфейсів може бути в цій підмережі?

Лабораторна робота № 2
Протокол ARP

Мета: ознайомитися з принципом роботи протоколу ARP, промоделювати роботу протоколу ARP в середовищі Packet Tracer 5.2.

Теоретичні відомості

ARP *(Address Resolution Protocol)* – протокол визначення адрес, який використовується для визначення локальної адреси за IP-адресою. Протокол реалізовується різними шляхами залежно від того, чи працює в даній мережі протокол локальної мережі (Ethernet, Token Ring, FDDI) з можливістю широкомовлення або ж який-небудь з протоколів глобальної мережі (X.25, Frame Relay), які, як правило, не підтримують широкомовний доступ [6].

Робота ARP в локальних мережах з широкомовленням. На рисунку 5.4 зображено фрагмент IP-мережі, яка включає дві мережі – Ethernet l (з трьох кінцевих вузлів A, B і C) і Ethernet 2 (з двох кінцевих вузлів D і E). Мережі підключені відповідно до інтерфейсів 1 і 2 маршрутизатора. Кожен мережевий інтерфейс має IP-адресу та MAC-адресу. Нехай у якийсь момент IP-модуль вузла C направляє пакет вузлу D. Протокол IP вузла C визначив IP-адресу інтерфейсу наступного маршрутизатора – це IP1. Тепер, перш ніж упакувати пакет в кадр Ethernet і направити його до маршрутизатора, необхідно визначити відповідну MAC-адресу. Для вирішення цього завдання протокол IP звертається до протоколу ARP. Протокол ARP містить на кожному інтерфейсі мережевого адаптера або маршрутизатора окрему ARP-таблицю, в якій у ході функціонування мережі накопичується інформація про відповідність між IP-адресами й MAC-адресами інших інтерфейсів даної мережі. Спочатку при увімкненні комп'ютера або маршрутизатора в мережу всі його ARP-таблиці порожні.

На першому кроці відбувається передача від протоколу IP протоколу ARP запиту MAC-адреси інтерфейсу за адресою IP_1.

Робота протоколу ARP починається з перегляду ARP-таблиці відповідного інтерфейсу. Нехай серед наявних у ній записів відсутня IP-адреса, яка запитується.

У цьому випадку вихідний IP-пакет, для якого виявилося неможливим визначити локальну адресу з ARP-таблиці, запам'ятовується в буфері, а протокол ARP формує ARP-запит, вкладає його в кадр протоколу Ethernet і широкомовно розсилає.

Всі інтерфейси мережі Ethernetl отримують ARP-запит і спрямовують його до свого протоколу ARP. ARP порівнює зазначену у запиті адресу IP_1 з IP-адресою інтерфейсу, на який надійшов запит. Протокол ARP, який констатував збіг (в даному випадку це ARP-маршрутизатор 1), формує ARP-відповідь.

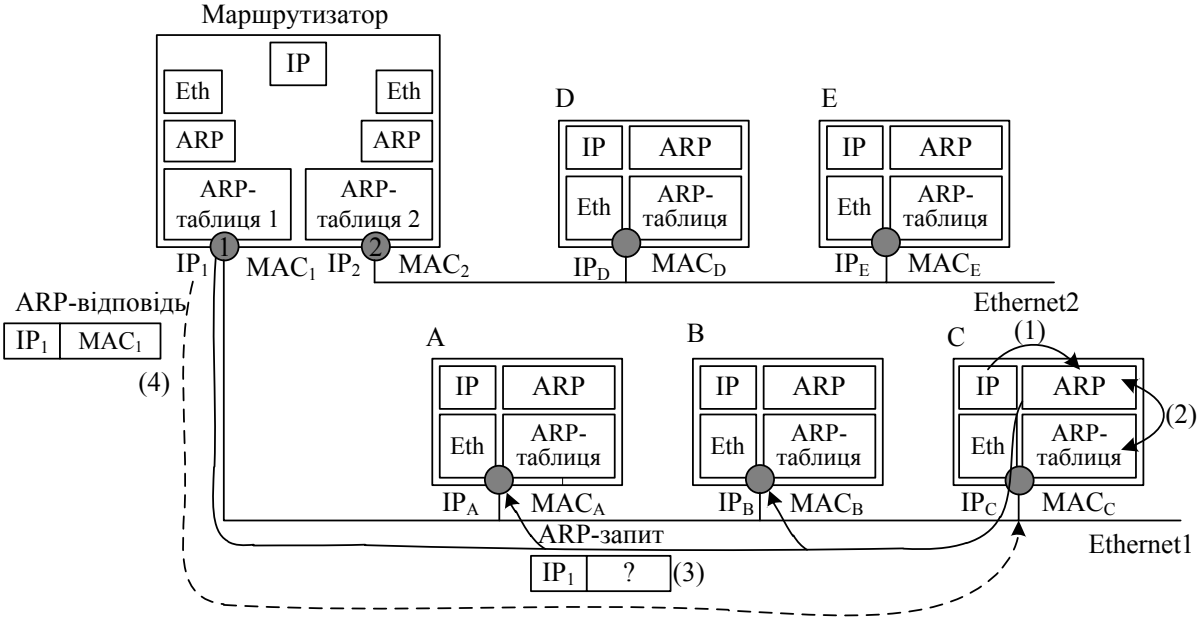


Рисунок 5.4 – Схема роботи протоколу ARP

У ARP-відповіді маршрутизатор вказує локальну адресу MAC_1 свого інтерфейсу і відправляє його до вузла, який сформував запит (в прикладі на рис. 5.4 до вузла С), використовуючи його локальну адресу. Широкомовна відповідь у цьому випадку не потрібна, оскільки формат ARP-запиту передбачає поля локальної адреси і мережевої адреси відправника. Варто відзначити, що зона поширення ARP-запитів обмежується мережею Ethernetl, оскільки на шляху широкомовних кадрів бар'єром стоїть маршрутизатор.

ARP-запити і ARP-відповіді мають один і той же формат. У таблиці 5.2 як приклад наведені значення полів реального ARP-запиту, переданого по мережі Ethernet1.

У полі типу мережі для мереж Ethernet вказується значення 1. Поле типу протоколу дозволяє використовувати протокол ARP не тільки з протоколом IP, але і з іншими мережевими протоколами. Для IP значення цього поля одне 0×0800. Довжина локальної адреси для протоколу Ethernet рівна 6 байт, а довжина IP-адреси – 4 байти. У полі операції для ARP-запитів вказується значення 1, для ARP-відповідей – значення 2.

З цього запиту видно, що в мережі Ethernet вузол з IP-адресою 194.85.135.75 намагається визначити, яку MAC-адресу має інший вузол тієї ж мережі, мережева адреса якого 194.85.135.65. Поле шуканої локальної адреси заповнено нулями. Відповідь надсилає вузол, який упізнав свою IP-адресу. Якщо в мережі немає машини, яка використовує шукану IP-адресу, то ARP-відповіді не буде. Протокол IP знищує IP-пакети, які надійшли за цією адресою.

Таблиця 5.2 – Приклад ARP-запиту

Поле	Значення
Тип мережі	1 (0×1)
Тип протоколу	2048 (0×800)
Довжина локальної адреси	6(0×6)
Довжина мережевої адреси	4 (0×4)
Операція	1 (0×1)
Локальна адреса відправника	008048EB7E60
Мережева адреса відправника	194.85.135.75
Локальна (шукана) адреса одержувача	000000000000
Мережева адреса одержувача	194.85.135.65

У таблиці 5.3 показані значення полів ARP-відповіді, яка могла б надійти на наведений в таблиці 5.2 ARP-запит.

Таблиця 5.3 – Приклад ARP-відповіді

Поле	Значення
Тип мережі	1 (0×1)
Тип протоколу	2048 (0×800)
Довжина локальної адреси	6(0×6)
Довжина мережевої адреси	4 (0×4)
Операція	1 (0×1)
Локальна адреса відправника	00E0F77F1920
Мережева адреса відправника	194.85.135.65
Локальна (шукана) адреса одержувача	008048EB7E60
Мережева адреса одержувача	194.85.135.75

В результаті обміну ARP-повідомленнями модуль IP, який послав запит з інтерфейсу, що має адресу 194.85.135.75, визначив, що IP-адресі 194.85.135.65 відповідає MAC-адреса 00E0F77F1920. Ця адреса буде потім поміщена у заголовок кадру Ethernet, який очікує відправлення IP-пакета.

Щоб зменшити кількість ARP-звернень до мережі, раніше знайдена відповідність між IP-адресою та MAC-адресою зберігається в ARP-таблиці відповідного інтерфейсу, в даному випадку – це запис: 194.85.135.65 – 00E0F77F1920.

Даний запис в ARP-таблиці з’явиться автоматично, через кілька мілісекунд після того, як модуль ARP проаналізував ARP-відповідь. І якщо раптом знову виникне необхідність послати пакет за адресою 194.85.135.65, то протокол IP, перш ніж посилати широкомовний запит, перевірить, чи немає вже такої адреси в ARP-таблиці.

ARP-таблиця поповнюється не тільки за рахунок надходжень на даний інтерфейс ARP-відповідей, але і в результаті вилучення корисної інформації з широкомовних ARP-запитів. Дійсно, в кожному запиті, як це видно з таблиць 5.2 і 5.3, містяться IP-адреса та MAC-адреса відправника. Всі інтерфейси, що одержали цей запит, можуть помістити інформацію про відповідність локальної та мережевої адрес відправника у власну ARP-таблицю. Зокрема, всі вузли, які отримали ARP-запит (таблиця 5.2), можуть поповнити свою ARP-таблицю записом: 194.85.135.75 - 008048EB7E60.

Таким чином, вигляд ARP-таблиці, у яку в процесі роботи мережі були додані два вищезгадані записи, демонструє таблиця 5.4.

Таблиця 5.4 – Приклад ARP-таблиці

IP-адреса	MAC-адреса	Тип запису
194.85.135.65	00E0F77F1920	Динамічний
194.85.135.75	008048EB7E60	Динамічний
194.85.60.21	008048EB7567	Статичний

У ARP-таблицях існує два типи записів: динамічні та статичні. Статичні записи створюються вручну за допомогою утиліти «arp» і не мають терміну старіння, точніше вони існують до тих пір, поки комп'ютер або маршрутизатор залишається увімкненим. Динамічні записи повинні періодично оновлюватись. Якщо запис не оновлювався протягом певного часу (протягом декількох хвилин), то він виключається з таблиці. Таким чином, в ARP-таблиці містяться записи не про всі вузли мережі, а тільки про ті, які активно беруть участь в мережевих операціях. Оскільки такий спосіб зберігання інформації називають кешуванням, то ARP-таблиці іноді називають ARP-кешом.

Деякі реалізації протоколів IP та ARP не ставлять IP-пакети в чергу на час очікування ARP-відповідей. Замість цього IP-пакет просто знищується, а його відновлення покладається на модуль TCP або прикладний процес, який працює через протокол UDP. Таке відновлення виконується за рахунок тайм-аутів і повторних передач. Повторна передача повідомлення проходить успішно, оскільки перша спроба вже викликала заповнення ARP-таблиці.

Зовсім інший спосіб визначення адрес використовується в глобальних мережах, у яких не підтримується широкомовне розсилання. Тут записи найчастіше доводиться вручну формувати і розміщувати на який-небудь сервер ARP-таблиці, в яких він задає, наприклад, відповідність IP-адрес адресам X.25, які мають для протоколу IP значення локальних адрес. У той же час на сьогодні з'явилась тенденція автоматизації роботи протоколу ARP і в глобальних мережах. З цією метою серед всіх маршрутизаторів, підключених до певної глобальної мережі, виділяється спеціальний маршрутизатор, який веде ARP-таблицю для всіх інших вузлів і маршрутизаторів цієї мережі.

При такому централізованому підході для всіх вузлів і маршрутизаторів вручну потрібно задати лише IP-адресу та локальну адресу виділеного для цих цілей маршрутизатора. При увімкненні кожен вузол і маршрутизатор реєструє свої адреси у виділеному маршрутизаторі. Кожного разу, коли виникає необхідність визначення за IP-адресою локальної адреси, модуль ARP звертається до виділеного маршрутизатора із запитом і автоматично отримує відповідь без участі адміністратора. Маршрутизатор, який працює таким чином, називають ARP-сервером.

У деяких випадках виникає обернена задача – знаходження IP-адреси за відомою локальною адресою. Тоді в дію вступає реверсивний протокол ARP (Reverse Address Resolution Protocol, RARP). Цей протокол використовується, наприклад, при старті станцій без накопичувачів, які не знають у початковий момент часу своєї IP-адреси, але знають MAC-адресу свого мережевого адаптера.

Хід роботи

1. Винести на логічне поле два комп'ютери, два комутатори та маршрутизатор.

2. Використовуючи порти Fast Ethernet, під'єднати перший комп'ютер до першого комутатора, а комутатор до одного з портів маршрутизатора. Аналогічним чином під'єднати другий комп'ютер до другого комутатора, а комутатор до вільного порту маршрутизатора (рисунок 5.5).

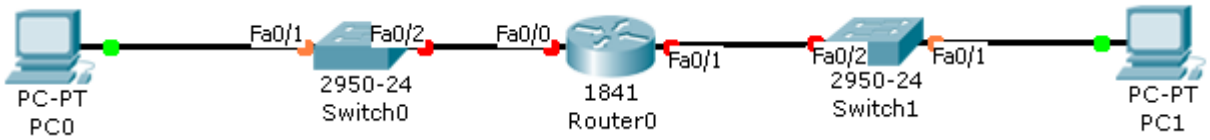


Рисунок 5.5 – Структура мережі для дослідження роботи протоколу ARP

3. Настроювання комп'ютерів. Портові першого комп'ютера присвоїти IP-адресу 192.168.1.11. IP-адреса шлюзу – 192.168.1.1. Маска підмережі – 255.255.255.0. Іншому комп'ютеру присвоїти IP-адресу 192.168.2.11, IP-адреса шлюзу – 192.168.2.1, маска підмережі – 255.255.255.0.

4. Настроювання маршрутизатора. Порту, до якого підключено перший комутатор, присвоїти IP-адресу 192.168.1.1, а порту, до якого підключено другий комутатор, присвоїти IP-адерсу 192.168.2.1.

5. Перейти у режим моделювання (Shift+S). Відправити простий ping-запит від одного комп'ютера до другого. При кожному кроці відкривати вікно інформації про пакет та дослідити вміст кадру (MAC-адреси) другого рівня (Layer 2) багаторівневої моделі OSI. Вікно інформації про пакет відривається клацанням на зображення повідомлення на топології мережі. Звести у таблицю MAC-адресу при передачі пакета на кожному вузлі мережі, порівнюючи при цьому із MAC-адресами портів Fast Ethernet (Рис. 5.6).

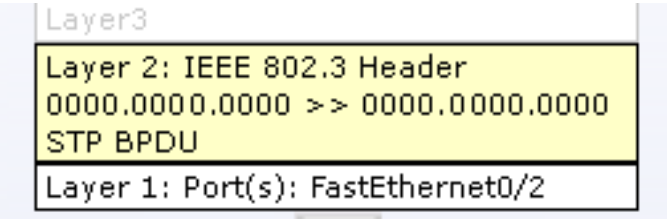


Рисунок 5.6 – Інформація другого рівня моделі OSI

Зміст звіту

1. Тема і мета роботи.
2. Короткий опис роботи протоколу ARP.
3. Таблиці ARP-запиту та ARP-відповіді.
4. Завдання до лабораторної роботи.
5. Знімки екрана зі структурою мережі для дослідження роботи протоколу ARP.
6. Результати проведеного пінгування.

Контрольні запитання

1. Поясніть принцип роботи ARP в локальних мережах з широкомовленням .
2. Поясніть структуру MAC-адреси.
3. Поясніть структуру ARP-запиту.
4. Поясніть структуру ARP-відповіді.
5. Як складається ARP- таблиця?
6. Скільки ARP-таблиць має комп’ютер?
7. Скільки ARP-таблиць має маршрутизатор?
8. Чим відрізняється робота ARP в локальних та глобальних мережах?
9. Як можна визначити IP-адресу за MAC-адресою?
10. Поясніть, як працює Proxy- ARP.

Лабораторна робота № 3
Використання концентраторів у мережах Ethernet

Мета: визначити призначення концентраторів, їх переваги та недоліки, навчитися моделювати роботу концентраторів в середовищі моделювання Packet Tracer 5.2.

Теоретичні відомості

Концентратор *(Hub)* – багатопортовий повторювач мережі із автоматичною сегментацією [7]. Всі порти концентратора рівноправні. Отримавши сигнал від однієї з підключених до нього станцій, концентратор транслює його на всі свої активні порти. При цьому, якщо на якому-небудь з портів виявлена несправність, цей порт автоматично відключається, а після її усунення знову робиться активним. Обробка колізій і поточний контроль за станом каналів зв'язку звичайно здійснюється самим концентратором. Концентратори можна використовувати як автономні пристрої або з'єднувати один з одним, збільшуючи тим самим розмір мережі і створюючи більш складні топології. Крім того, можливе їхнє з'єднання магістральним кабелем у шинну топологію. Автосегментація необхідна для підвищення надійності мережі.

Призначення концентраторів – об'єднання окремих робочих місць в робочу групу в складі локальної мережі. Для робочої групи характерні такі ознаки: певна територіальна зосередженість; колектив користувачів робочої групи вирішує подібні задачі, використовує однотипне програмне забезпечення і загальні інформаційні бази; в межах робочої групи існують загальні вимоги щодо забезпечення безпеки і надійності, відбувається однаковий вплив зовнішніх джерел перешкод (кліматичних, електромагнітних тощо); спільно використовуються високопродуктивні периферійні пристрої, які зазвичай містять свої локальні сервери, нерідко територіально розташовані на території робочої групи.

Концентратори працюють на фізичному рівні (рівень 1 багаторівневої моделі OSI). Тому вони не чутливі до протоколів верхніх рівнів. Результатом цього є можливість спільного використання різних операційних систем (Novell NetWare, SCO UNIX, EtherTalk, LAN Manager тощо, сумісних з мережами Ethernet або IEEE 802.3).

Всі концентратори мають такі характерні експлуатаційні ознаки:

- оснащені світлодіодними індикаторами, що вказують стан портів (Port Status), наявність колізій (Collisions), активність каналу передачі (Activity), наявність несправності (Fault) і наявність живлення (Power), що забезпечує швидкий контроль стану всього концентратора і діагностику несправностей;
- при включенні електроживлення виконують процедуру самотестування, а в процесі роботи – функцію самодіагностики;
- мають стандартний розмір по ширині – 19 дюймів;

- забезпечують автосегментацію портів для ізоляції несправних портів і поліпшення життя мережі (network integrity);
- виявляють помилку полярності при використанні кабелю на крученій парі й автоматично переключають полярність для усунення помилки монтажу;
- підтримують конфігурації із застосуванням декількох концентраторів, з'єднаних один з одним або за допомогою спеціальних кабелів і stack-портів, або тонкої коаксіальної магістралі, включеної між портами BNC, або за допомогою оптоволоконного чи товстого коаксіального кабелю підключеного через відповідні трансивери до порту AUI, або за допомогою UTP кабелів, підключених між портами концентраторів;
- підтримують мовний зв'язок і передачу даних через один і той кабельний джгут;
- прозорі для програмних засобів мережевої операційної системи;
- можуть бути змонтовані і введені в дію у продовж декількох хвилин.

Концентратори початкового рівня – 8-ми, 5-ти, рідше 12-ти та 16-ти портові концентратори. Не забезпечені можливістю керування ні через консольний порт, ні через мережу. Є простим і дешевим рішенням для організації робочої групи невеликого розміру.

Концентратори середнього класу – 12-ти, 16-ти, 24-х портові концентратори, мають консольний порт, часто додаткові порти даних. Цей тип концентраторів надає можливості для позасмугового керування мережею (out-of-band management) через консольний порт RS232 під керуванням будь-якої стандартної термінальної програми, що дає можливість конфігурувати інші порти і зчитувати статистичні дані концентратора. Ці типи концентраторів позиціонують для побудови від малих до середніх мереж, які в подальшому будуть розвиватися і потребуватимуть введення програмного керування.

SNMP-керовані концентратори – 12-ти, 16-ти, 24-х і 48-ми портові концентратори. Їх відрізняє не тільки наявність консольного порту RS-232 для керування, але і можливість здійснення керування і збір статистики по мережі, використовуючи протоколи SNMP/IP або IPX. Стає можливий збір статистики на вузлах мережі (концентратор), її первинна обробка й аналіз: ідентифікуються головні джерела повідомлень – top talkers – найбільш активні користувачі, heavy users – джерела помилок і комунікаційні пари – communications pairs. Ці типи концентраторів доцільно застосовувати для побудови середніх і більше LAN-мереж, що безумовно будуть розвиватися. Ці мережі завжди потребують програмного керування мережею, у тому числі віддаленого.

BNC-концентратори або концентратори ThinLAN – багатопортові повторювачі для тонких коаксіальних кабелів, які використовуються у мережах стандартів 10Base2. Вони мають у своєму складі порти BNC і, як правило, один порт AUI, часто підтримують SNMP-протоколи. Вони, як і кон-

центратори 10Base-T, сегментують порти (відключаючи при цьому не одну станцію, а абонентів усієї гілки) і транслюють вхідні пакети в усі порти. На кожен BNC-порт поширюються всі ті ж обмеження, що і на фрагмент мережі стандарту 10Base-2: підтримується робота сегментів тонкого коаксіального кабелю довжиною до 185 метрів на кожен порт, забезпечується до 30 мережевих з'єднань на сегмент, якщо відбудеться порушення цілісності кабельного сегмента, цей сегмент виключається з роботи, але інша частина концентратора буде продовжувати функціонувати. Сфера застосування концентраторів даного типу – модернізація старих мереж стандарту 10Base2 з метою підвищення їх надійності, модернізація мереж, що досягли обмежень на застосування повторювачів і не потребують частих змін.

Концентратори 10/100. Особливість їх полягає у тому, що якщо до концентратора такого типу підключена хоча б одна станція стандарту 10Base-T, то всі порти будуть працювати на швидкості 10 Мбіт/с. Тому умовою роботи концентратора на повній швидкості 100 Мбіт/с є обов'язкове підключення усіх станцій, які працюють на такій самій швидкості.

Концентратори Redundant link – середнього класу і SNMP-керовані концентратори, які підтримують один надлишковий зв'язок (redundant link) на кожен концентратор для створення резервного зв'язку (back up link) між будь-якими двома концентраторами. Це забезпечує відмовостійкість мережі на апаратному рівні. Резервний зв'язок являє собою окремий кабель, змонтований між двома концентраторами. Використовуючи консольний порт концентратора, необхідно задати конфігурацію основного каналу зв'язку і резервного каналу зв'язку одного з концентраторів. Резервний канал зв'язку автоматично вмикається при відмові основного каналу зв'язку двох концентраторів. Не дивлячись на те, що концентратор може контролювати тільки один резервний зв'язок, він може перебувати на віддаленому кінці одного резервного зв'язку та на контролюючому кінці резервного зв'язку з іншим концентратором. Після усунення несправності на основному кабельному сегменті, основний зв'язок автоматично не відновить роботу. Для відновлення роботи головного зв'язку доведеться використовувати консоль концентратора чи перезавантажити концентратор.

Зв'язковий біт у концентраторів являє собою періодичний імпульс тривалістю 100 нс, що посилається через кожні 16 мс. Він не впливає на трафік мережі. Зв'язковий біт посилається в той період, коли мережа не передає дані. Ця функція здійснює поточний контроль збереження UTP каналу. Цю функцію слід використовувати у всіх можливих випадках і блокувати її тільки тоді, коли до порту концентратора приєднується пристрій, який не підтримує її.

Хід роботи

1. Винести на логічне поле чотири комп'ютери та концентратор.

2. Під’єднати усі комп’ютери до концентратора, використовуючи порти Fast Ethernet (рисунок 5.7).

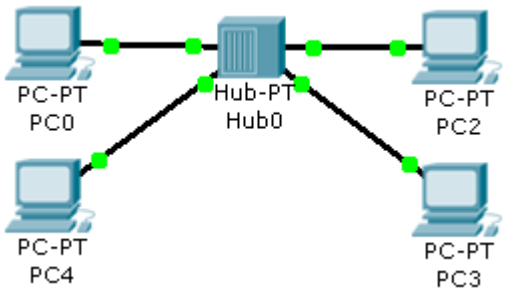


Рисунок 5.7 – Структура локальної мережі на базі концентраторів

3. Налаштувати порти Fast Ethernet комп’ютерів, присвоївши їм IP-адреси у діапазоні 192.168.1.10 – 192.168.1.13.

4. Виконати просте пінгування усіх комп’ютерів, використовуючи командний рядок у вікні властивостей комп’ютера.

5. Перейти у режим моделювання (Shift+S). Виконати покрокове дослідження передачі пакета від комп’ютера до комп’ютера. Для цього необхідно у режимі моделювання поставити на передачу простого ping-запиту між двома клієнтами мережі. Покрокове відслідковування відбувається натисканням кнопки Capture/Forward. Під час кожного натискання кнопки демонструється передача пакета від одного вузла мережі до іншого. Зробити знімки екрана при кожному кроці передачі пакета.

6. Виконати у режимі моделювання покрокове дослідження передачі одночасно двох пакетів. Зробити знімки екрана покрокової передачі пакетів.

7. Винести на логічне поле ще один концентратор та комп’ютер.

8. З’єднати між собою концентратори, використовуючи перехресне з’єднання. Від’єднати один із комп’ютерів та підключити його до другого концентратора.

9. Підключити п’ятий комп’ютер до другого концентратора та присвоїти йому IP-адресу у межах нумерації даної локальної мережі.

10. Виконати пп. 5, 6.

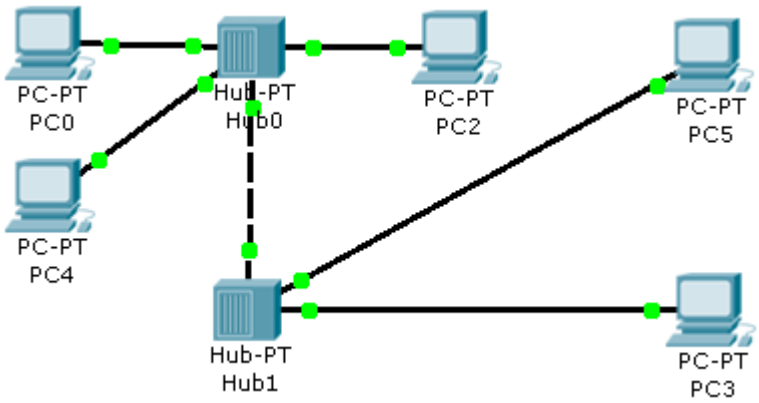


Рисунок 5.8 – Розширення ємності мережі додатковим концентратором

Зміст звіту

1. Тема і мета роботи.
2. Короткий опис побудови та роботи концентраторів.
3. Завдання до лабораторної роботи.
4. Знімки екрана із мережею на базі концентраторів та налаштуванням портів.
5. Результати проведеного пінгування.

Контрольні запитання

1. Поясніть принцип дії та побудову концентраторів для різних специфікацій стандарту 802.x.
2. Назвіть причини виникнення правила «чотирьох хабів».
3. Призначення концентраторів.
4. На якому рівні моделі OSI працюють концентратори.
5. Що впливає на максимальну довжину сегмента локальної мережі?
6. Що таке пряме і перехресне з'єднання між вузлами мережі?
7. Як впливає на продуктивність мережі пропускна здатність мережевого адаптера й пропускна здатність порту концентратора?
8. Як концентратор підтримує резервні зв'язки?
9. Відповідно до основної функції концентратора — повторення сигналу — його відносять до пристроїв, що працюють на фізичному рівні моделі OSI. Наведіть приклади додаткових функцій концентратора, для виконання яких концентратору потрібна інформація протоколів більш високих рівнів.

Лабораторна робота № 4
Використання маршрутизаторів у мережах Ethernet

Мета: визначити призначення маршрутизаторів, їх переваги та недоліки, провести моделювання роботи мережі, побудованої на маршрутизаторах.

Теоретичні відомості

Маршрутизатор (від англ. Router) – мережевий пристрій, який на підставі інформації про топологію мережі і певних правил приймає рішення про пересилання пакетів мережевого рівня (рівень 3 моделі OSI) між різними сегментами мережі [8].

Маршрутизатор, перш за все, необхідний для визначення подальшого шляху даних, посланих у велику і складну мережу. Користувач такої мережі відправляє свої дані в мережу і вказує адресу свого абонента. Дані проходять по мережі і в точках з розгалуженням маршрутів поступають на маршрутизатори, які і встановлюються в таких точках. Маршрутизатор вибирає подальший найкращий шлях. Те, який шлях краще, визначається кількісними показниками, які називаються метриками. Кращий шлях – це шлях з найменшою метрикою. У метриці може враховуватися декілька показників, наприклад, довжина шляху, час проходження тощо.

Маршрутизатори реалізуються різним чином. Їх поділяють на пристрої верхнього, середнього і нижнього класів.

Високопродуктивні маршрутизатори верхнього класу служать для об'єднання мереж підприємства. Вони підтримують безліч протоколів і інтерфейсів. Пристрої даного типу можуть мати до 50 портів локальних або глобальних мереж.

За допомогою маршрутизаторів середнього класу формуються менші мережеві об'єднання масштабу підприємства. Стандартна конфігурація включає два-три порти локальних мереж і від чотирьох до восьми портів глобальних мережі. Такі маршрутизатори підтримують найбільш поширені протоколи маршрутизації і транспортні протоколи.

Маршрутизатори нижнього класу призначаються для локальних мереж підрозділів; вони пов'язують невеликі офіси з мережею підприємства. Типова конфігурація: один порт локальної мережі (Ethernet або Token Ring) і два порти глобальної мережі, розраховані на низькошвидкісні виділені лінії або комутовані з'єднання.

Маршрутизатори базових мереж і віддалених офісів мають різну архітектуру, оскільки до них висуваються різні функціональні та операційні вимоги. Маршрутизатори базових мереж обов'язково повинні бути розширюваними. Маршрутизатори локальних мереж підрозділи, для яких, як правило, заздалегідь встановлюється фіксована конфігурація портів, містять тільки один процесор, керуючий роботою трьох або чотирьох інтерфейсів. У них використовуються приблизно ті ж протоколи, що і в марш-

рутизаторах базових мереж, однак програмне забезпечення більше направлено на полегшення інсталяції та експлуатації, оскільки в більшості віддалених офісів відсутні достатньо кваліфіковані фахівці з мережевого обслуговування.

У ролі маршрутизатора може виступати робоча станція або сервер, що мають кілька мережевих інтерфейсів та обладнаний спеціальним програмним забезпеченням. Маршрутизатори верхнього класу – це, як правило, спеціалізовані пристрої, що поєднують в окремому корпусі безліч маршрутизуючих модулів.

За визначенням, основне призначення маршрутизаторів - це маршрутизація трафіку мережі. Процес маршрутизації можна розділити на два ієрархічно пов’язаних рівня [9].

Перший рівень – рівень маршрутизації. На цьому рівні відбувається робота з таблицею маршрутизації. Таблиця маршрутизації служить для визначення адреси (мережевого рівня) наступного маршрутизатора або безпосередньо одержувача за наявним адресою (мережевого рівня) і одержувача після визначення адреси передачі вибирається певний вихідний фізичний порт маршрутизатора. Цей процес називається визначенням маршруту переміщення пакета. Налаштування таблиці маршрутизації ведеться протоколами маршрутизації. На цьому ж рівні визначається перелік необхідних сервісів, що надаються.

Другий рівень – рівень передачі пакетів. Перед тим як передати пакет, необхідно: перевірити контрольну суму заголовка пакету, визначити адресу (канального рівня) одержувача пакету і провести безпосередньо відправку пакету з урахуванням черговості, фрагментації, фільтрації тощо. Ці дії виконуються на підставі команд, що надходять з рівня маршрутизації.

Для визначення напрямку (маршруту) передачі дейтаграми маршрутизатор використовує таблиці, які можуть бути сформовані адміністратором мережі або автоматично, за допомогою спеціальних алгоритмів.

Процес визначення маршруту в мережах TCP/IP називається ***IP-маршрутизація***. Станції користувача, які формують і приймають IP дейтаграми, зазвичай використовують лише для однієї мережі.

Станція користувача, яка для підключення до мережі використовує не більше одного інтерфейсу, називається IP хостом.

Хост також може брати участь у виконанні процесу маршрутизації.

На рисунку 5.9 поданий варіант мережі, в якій знаходяться два маршрутизатора, кожен з яких може забезпечити доставку дейтаграми від хоста A до хоста B. У цьому випадку, незважаючи на те, що хост A має тільки одне мережеве підключення, він повинен самостійно виконати вибір між двома можливими маршрутами, які проходять через R1 і R2. Залежно від того, чи належить джерело дейтаграми і станція її кінцевого призначення до однієї і тієї ж мережі чи ні, можуть бути використані два види маршрутизації: безпосередня (direct) і опосередкована (indirect).

У тому випадку, якщо джерело і станція призначення дейтаграми знаходяться на одній мережі, доставка може бути виконана безпосередньо, без участі маршрутизатора. Виконуючи безпосередню доставку дейтаграми, джерело використовує процедуру ARP і визначає фізичну адресу станції призначення. Після цього ним можуть бути сформовані кадр чи група кадрів, у полі корисного навантаження яких повинна бути розміщена дейтаграма.

Однак у мережі Internet значно частіше використовується інший варіант доставки дейтаграм – опосередкована доставка. При використанні даного режиму дейтаграма повинна бути передана по мережі в напрямку посередника, яким у цьому випадку є маршрутизатор. Цей маршрутизатор, у свою чергу, передає дейтаграму по одній зі своїх мереж у напрямку того маршрутизатора, який, на його думку, знаходиться ближче до станції призначення. Таким чином, ланцюжок маршрутизаторів, які беруть участь у процедурі опосередкованої доставки, являє собою віртуальний канал, по якому передається дейтаграма у напрямку станції її призначення. Останній маршрутизатор з даного ланцюжка передає цю дейтаграму станції призначення, використовуючи при цьому режим безпосередньої доставки.

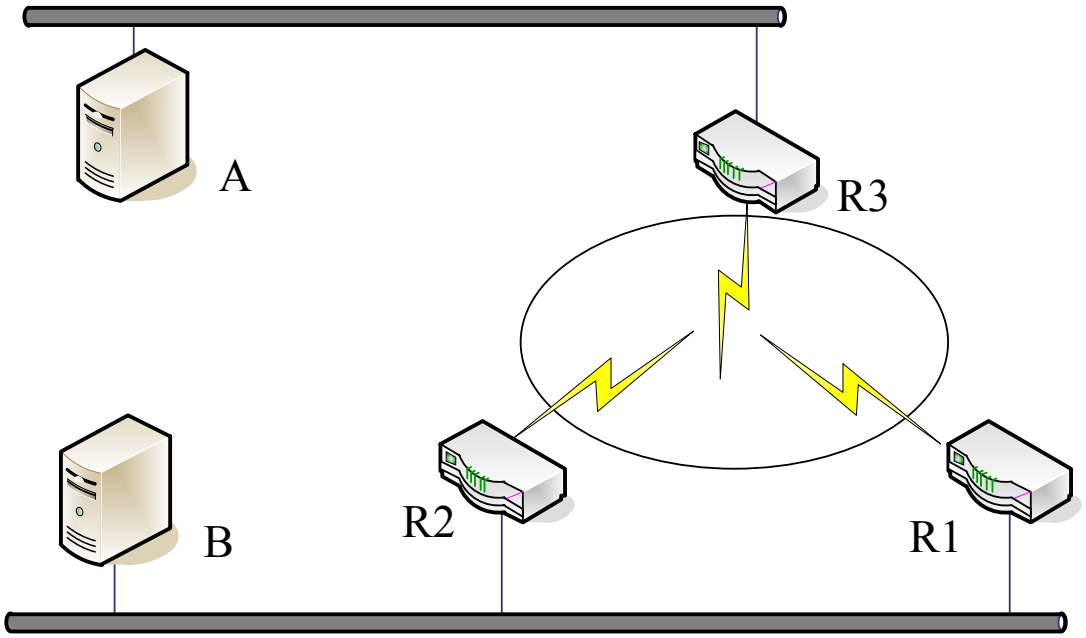


Рисунок 5.9 – Топологія мережі ARP-маршрутизації

Принципи побудови таблиць маршрутизації. Для визначення напрямку, в якому повинна бути передана дейтаграма, маршрутизатор і хост використовують спеціальні таблиці – таблиці маршрутизації (IP routing table).

Суттєвим є те, що в цих таблицях маршрутизації розташовується інформація не про хости призначення, а про мережі, до яких ці хости належать.

Для визначення напрямку в таблицях маршрутизації IP використовується принцип, який називається next hop routing. Цей принцип полягає в

тому, що кожній мережі або групі мереж ставиться у відповідність мережева адреса маршрутизатора (IP-шлюзу), у напрямок якого повинна бути передана дейтаграма для того, щоб досягти станції призначення, підключеної до цієї мережі. Важливо відзначити, що як «хопи» в таблиці маршрутизації можуть бути вказані тільки маршрутизатори, відносно яких може бути виконана процедура безпосередньої доставки.

На рисунку 5.10 наведена сукупність мереж для забезпечення інформаційної взаємодії, між компонентами яких використовуються три маршрутизатори (R1, R2, R3). Нижче, у таблиці 5.5, наведена таблиця маршрутизації для R1.

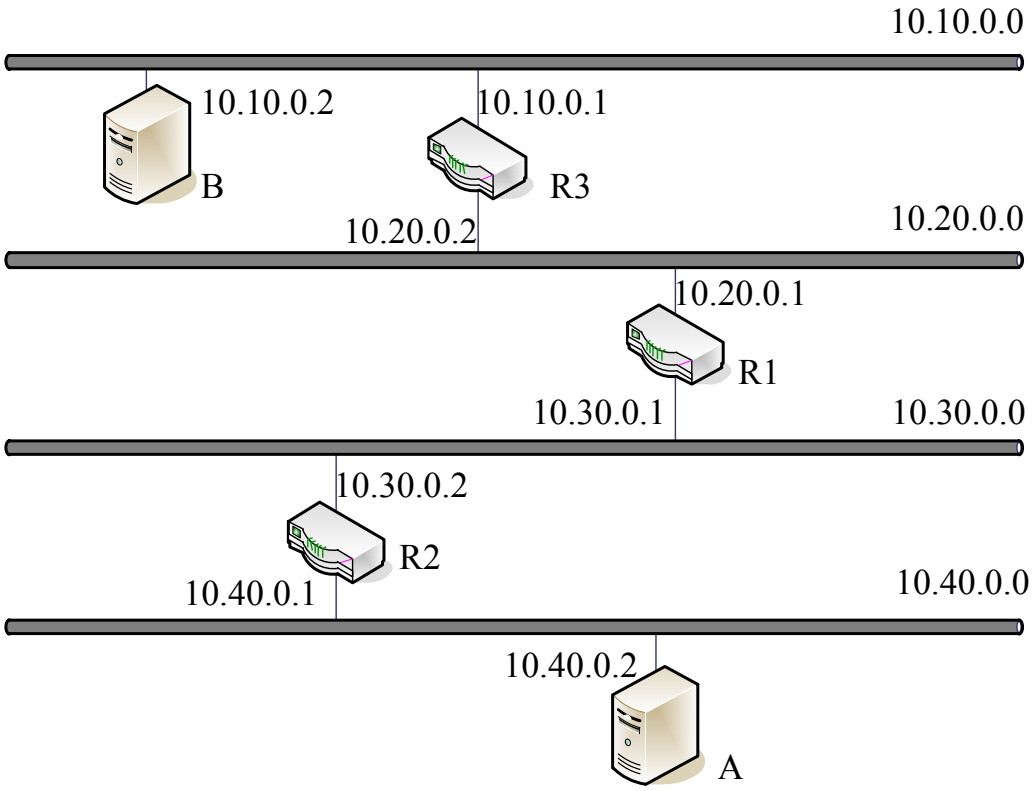


Рисунок 5.10 – Взаємодія IP-адрес між компонентами мереж

Мережі 10.20.0.0 і 10.30.0.0 є безпосередньо підключеними для даного маршрутизатора. Для направлення дейтаграм в мережу 10.40.0.0 маршрутизатор повинен використовувати R3, який поданий в таблиці маршрутизації інтерфейсом 10.30.0.2. Для направлення дейтаграм в мережу 10.10.0.0 маршрутизатор повинен використовувати R3, який наведений в таблиці маршрутизації інтерфейсом 10.20.0.2.

Маршрутизація «за замовчуванням». Зовсім необов’язково перераховувати в таблиці маршрутизації всі номери мережі, які існують в Internet, замість цього можна просто вказати там адресу хопу, куди повинні передаватися дейтаграми, адреси мережі призначення яких не вказано в таблиці маршрутизації.

Таблиця 5.5 – Таблиця маршрутизації маршрутизатора R1

Network	Next Hop
10.10.0.0	10.20.0.2
10.20.0.0	Connected
10.30.0.0	Connected
10.40.0.0	10.30.0.2

Маршрутизатор, який використовується як next hop для дейтаграм, адреса мережі призначення яких не вказана в таблиці маршрутизації, називається default gateway.

Маршрутизація по хосту. Можливе виникнення ситуації, коли правила визначення маршруту, які вказані в таблиці маршрутизації, з якихось причин не повинні поширюватися на один з хостів. У цьому випадку можливе зазначення в таблиці маршрутизації не адреси мережі, а безпосередньої адреси хоста. Для того, щоб механізм маршрутизації за адресою хоста міг працювати, необхідно, щоб рядки таблиці маршрутизації, в яких вказані маршрути на хост, повинні бути розглянуті в першу чергу.

Належність мережі до певного класу однозначно визначає структуру мережевої адреси – розміри полів Net ID і Host ID. Для того, щоб забезпечити можливість більш ефективного використання адресного простору в мережах TCP/IP, широко використовуються позакласові мережі.

Позакласовими називаються мережі, IP структура мережевої адреси яких визначається шляхом явного вказання і не відповідає класу даної мережі.

Структура адреси позакласових мереж (довжина полів Net ID і Host ID) визначається значенням маски даної мережі. Маска мережі має такий самий формат і спосіб подання (dotted decimal), як і мережева адреса IP.

Біти маски, які відповідають полю Net ID, встановлюються значенням «1», біти маски, які відповідають полю Host ID, встановлюються значенням «0». Таким чином маска мережі класу B може бути подана у вигляді: 255.255.0.0.

Для визначення позакласових мереж використовуються подовжені або скорочені маски. Як загальне найменування для масок подібного типу іноді використовується термін Variable Length Subnet Mask (VLSM) - мережеві маски змінної довжини. Існують два типи позакласових мереж, які мають назви підмережі (subnets) і супермережі (supernets).

Найширше поширення на практиці отримали позакласові мережі типу subnets. Для забезпечення зручності адміністрування на мережевому рівні часто буває дуже зручно і доцільно асоціювати деяку групу користувачів з певною адресою мережі. Обмеженість адресного простору (особливо це стосується відкритого простору) найчастіше не дозволяє забезпечити таку можливість.

Кожна із щойно організованих мереж буде мати подовжену відносно вихідної мережі маску. Наприклад, мережа класу А 10.0.0.0 може бути розбита на 255 мереж класу В (таблиця 5.6).

Таблиця 5.6 – Надання масок мережам

Мережа	Маска
10.1.0.0	255.255.0.0
10.2.0.0	255.255.0.0
10.255.0.0	255.255.0.0

Документами, які регламентують застосування позакласових мереж, не встановлено однозначно, що маска мережі повинна являти собою безперервну послідовність одиниць. Отже, принаймні теоретично можливе використання підмереж, які мають маски такого вигляду: 255.255.255.160.

Розглянемо приклад розбиття з використанням даної маски мережі 192.168.68.0:

– 192.168.66.0: 192.168.66.1 – 192.168.66.31, 192.168.66.64 – 192.168.66.95;
– 192.168.66.32: 192.168.66.33 – 192.168.66.63, 192.168.66.96 – 192.168.66.127;
– 192.168.66.128: 192.168.66.129 – 192.168.66.159, 192.168.66.192 – 192.168.66.233;
– 192.168.66.160: 192.168.66.161 – 192.168.66.191, 192.168.66.224 – 192.168.66.255.

У даному випадку вихідна мережа була розділена на 4 мережі, кожна з яких мала в цілому по 64 хости. Однак слід відзначити, що використання масок подібного типу не передбачено в апаратурі провідних виробників телекомунікаційного обладнання.

У деяких випадках може виявитися корисним об’єднати групу мереж низького класу в мережу, що має більш коротку маску. Основною перевагою в даному випадку буде різке скорочення обсягу інформації, який повинен бути використаний для виконання процесу маршрутизації.

Застосування обох типів позакласових мереж може бути комбінованим – наприклад, кілька підмереж можуть бути об’єднані в одну супермережу.

У загальному вигляді алгоритм маршрутизації в мережах IP може бути сформульовано таким чином:

а) маршрутизатор визначає IP-адресу станції призначення AD у прийнятій дейтаграми і аналізує належність цієї адреси до однієї з безпосередньо підключених до нього мереж;

1. Якщо можлива безпосередня доставка дейтаграми, вона не потребує маршрутизації і знищується.

2. Якщо адреса AD належить до однієї з безпосередньо підключених мереж, дейтаграма направляється в цю мережу через відповідний інтерфейс маршрутизатора.

б) маршрутизатор перевіряє наявність або відсутність в таблиці маршрутизації вказання маршруту для хоста AD. Якщо такий маршрут є, дейтаграма передається на адресу next hop для даного маршруту;

в) маршрутизатор аналізує відповідність Net ID шуканої адреси записам, які розташовані в таблиці маршрутизації.

1. Якщо кілька записів відповідає шуканій адресі, маршрутизатор передає дейтаграму на адресу next hop тієї мережі, якій відповідає найдовша маска.

2. Якщо таких записів не виявлено, дейтаграма передається в напрямку default gateway.

3. Якщо default gateway не визначений для даного маршрутизатора, формується повідомлення про помилку маршрутизації.

Хід роботи

1. Винести на логічне поле комп'ютер, лептоп, сервер, комутатор 2950-24 та маршрутизатор 1841 (рисунок 5.11).

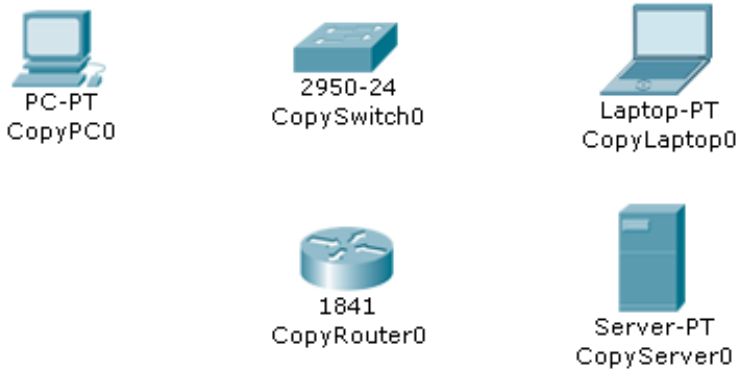


Рисунок 5.11 – Винесене на логічне поле обладнання

2. З'єднати, використовуючи порти Fast Ethernet, маршрутизатор, лептоп та комп'ютер з комутатором прямим кабелем. Сервер і маршрутизатор з'єднати між собою перехресним кабелем.

3. Портові Ethernet комп'ютера надати IP-адресу 192.168.1.1, портові Ethernet лептопу надати IP-адресу 192.168.1.2, присвоїти маску підмережі.

4. Не закриваючи вікна властивостей комп'ютера та лептопу, надати IP-адресу шлюзу. Для цього на вкладці Config у лівій частині вікна необхідно розгорнути список GLOBAL та натиснути кнопку Settings. У правій частині вікна з'являться поля для настроювання портів шлюзу та DNS. У полі Gateway/DNS переконатись, що радіокнопка увімкнена навпроти Static. У полі для введення навпроти Gateway (шлюз) ввести IP-адресу 192.168.1.3. Закрити вікно.

5. Налаштувати аналогічним чином сервер. Портові сервера Ethernet присвоїти IP-адресу 198.168.1.1. IP-адресі шлюзу присвоїти значення 198.168.1.2.

6. Викликати вікно властивостей маршрутизатора. Маршрутизатор можна налаштувати двома шляхами: через діалогове вікно та через командний рядок. Варто відзначити, що у реальних умовах налаштування апаратури здійснюється через термінал введенням спеціальних команд.

Розглянемо налаштування через діалогове вікно властивостей. Для цього у вікні властивостей маршрутизатора потрібно перейти на вкладку Config. У полі вибору настроювань натиснути на кнопку, що позначає порт FastEthernet 0/0. Після цього у правій частині вікна необхідно заповнити два поля для введення: IP-адреси порту, яка налаштовується, – 192.168.1.2 та маску підмережі – 255.255.255.0. Згори навпроти поля Port Status поставити прапорець, що означає увімкнення даного порту.

Аналогічним чином виконати настроювання для порту FastEthernet 0/1. При цьому IP-адреса його має бути 198.168.1.2, а маска підмережі – 255.255.255.0. Не забути увімкнути його.

7. Після настроювання портів маршрутизатора потрібно зачекати приблизно хвилину, щоб установився зв’язок маршрутизатора із комутатором, ознакою чого стане зелена індикація біля кожного порту. Якщо ж індикація оранжева або червона, то необхідно повторно пройти етапи настроювань і прослідити, чи все виконано правильно.

8. Виконати пінгування кожного вузла побудованої мережі і переконатись, що кожен вузол передає та приймає пінг.

Налаштування маршрутизатора через командний рядок.

9. Побудувати аналогічну мережу, виконавши пп. 1 – 5.

10. Викликати вікно властивостей маршрутизатора та перейти на вкладку CLI. Маршрутизатор стане доступним для налаштування у режимі командного рядка (термінала).

11. Натиснути клавішу введення, після чого відобразиться запрошення до настроювання маршрутизатора у вигляді «Router>».

12. Виконати введення таких команд, після кожної натискати клавішу введення:

```
Router>enable
Router #config
Router(config)#iterface fastEthernet 0/0
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if) #no shutdown
Router(config-if) #description Interface_To_Local_Metwork
Router(config-if)#exit
Router(config)#interface FastEthernet 0/1
Router(config-if)#ip address 198.168.1.2 255.255.255.0
Router(config-if) #no shutdown
Router(config-if) #description Interface_To_Local_Metwork
Router(config-if)#exit
Router(config)#exit
Router#copy running-config startup-config
```

Destination filename [startup-config]?

[OK]

Таким чином виконано налаштування портів маршрутизатора аналогічно п. 6.

13. Виконати п. 8.

Зміст звіту

1. Тема і мета роботи.
2. Короткий опис побудови та роботи маршрутизаторів.
3. Завдання до лабораторної роботи.
4. Знімки екрана із мережею, побудованою на маршрутизаторах.
5. Знімки екрана налаштування властивостей маршрутизатора через діалогове вікно та через командний рядок.
6. Результати проведеного пінгування.

Контрольні запитання

1. Які елементи мереж можуть виконувати фрагментацію пакетів при маршрутизації? Коли застосовується ця процедура?
2. Дайте класифікацію маршрутизаторів, наведіть структурну схему маршрутизатора.
3. Поясніть порядок програмування портів маршрутизатора.
4. Що є метрикою протоколу RIP? Чому максимальне її значення складає 16.
5. Чи передається в IP-пакеті маска, коли маршрутизація відбувається з використанням масок?
6. Які існують засоби прискорення роботи протоколу RIP?
7. Скільки записів про маршрути за замовчуванням може містити таблиця маршрутизації?
8. Чи можна пересилати IP-пакети, якщо в маршрутизаторі немає таблиці маршрутизації?

Лабораторна робота № 5
Протокол OSPF

Мета: ознайомитися з принципом роботи протоколу OSPF, промоделювати роботу протоколу OSPF в середовищі Packet Tracer 5.2.

Теоретичні відомості

Відкритий протокол, що базується на алгоритмі пошуку найліпшого шляху (Open Shortest Path Fisrt – OSPF) є протоколом маршрутизації, розробленим для мереж IP [1, 10].

Як і всі протоколи маршрутизації, побудовані на алгоритмі стану зв'язків, OSPF розбиває процес побудови таблиці маршрутизації на два етапи.

На першому етапі кожен маршрутизатор будує граф зв'язків мережі, у якому вершинами графа є маршрутизатори і IP-мережі, а ребрами – інтерфейси маршрутизаторів. Всі маршрутизатори для цього обмінюються зі своїми сусідами тією інформацією про граф мережі, до якої вони відносяться в даний момент. Цей процес схожий на процес розповсюдження векторів відстаней до мереж в протоколі RIP, проте сама інформація якісно інша – це інформація про топологію мережі. Повідомлення, за допомогою яких поширюється топологічна інформація, називаються оголошеннями про стан зв'язків мережі (Link State Advertisements, LSA). Крім того, при передачі топологічної інформації OSPF маршрутизатори її не модифікують, як це роблять RIP-маршрутизатори, а передають у незмінному вигляді. У результаті всі маршрутизатори мережі мають у своєму розпорядженні ідентичні відомості про граф мережі, які зберігаються в базі даних про топологію мережі.

Другий етап полягає у знаходженні оптимальних маршрутів за допомогою отриманого графа. Завдання знаходження оптимального шляху за графом є достатньо складним і трудомістким. У протоколі OSPF для його вирішення використовується ітеративний алгоритм Дійкстри. Кожен маршрутизатор умовно вважає себе центром мережі і шукає оптимальний маршрут до кожної відомої йому мережі. У кожному знайденому таким чином маршруті запам'ятовується тільки один крок – до наступного маршрутизатора, відповідно до принципу однокрокової маршрутизації. Дані про цей крок і потрапляють в таблицю маршрутизації. Якщо кілька маршрутів мають однакову метрику до мережі призначення, то в таблиці маршрутизації запам'ятовуються перші кроки всіх цих маршрутів.

Для того, щоб база даних про топологію мережі відповідала поточному стану мережі, OSPF-маршрутизаторам необхідно постійно відслідковувати зміни стану мережі та вносити необхідні корективи в таблицю маршрутизації. Для контролю за станом зв'язків та сусідніх маршрутизаторів OSPF-маршрутизатори регулярно передають один одному повідомлення HELLO. Повідомлення HELLO відправляються через кожні 10 секунд, щоб підви-

щити швидкість адаптації маршрутизаторів до змін, що відбуваються в мережі. Невеликий обсяг цих повідомлень робить можливим таке часте тестування стану сусідів та зв'язків з ними. На підставі прийнятих від безпосередніх сусідів повідомлень HELLO маршрутизатор формує записи про стан зв'язків зі своїми безпосередніми сусідами в базі даних про топологію мережі.

У тому випадку, коли повідомлення HELLO перестають надходити від будь-якого безпосереднього сусіда, маршрутизатор робить висновок про те, що стан зв'язку змінився з роботоздатного на нероботоздатний і робить відповідну позначку у своїй базі даних. Одночасно він надсилає всім безпосереднім сусідам оголошення LSA про ці зміни, і ті також коректують свої бази даних і, в свою чергу, розсилають дане оголошення LSA своїм безпосереднім сусідам (зрозуміло, крім того сусіда, від якого воно було отримано). Після коректування графа мережі кожен маршрутизатор знову шукає оптимальні маршрути і коригує свою таблицю маршрутизації. Конвергенція таблиць маршрутизації до нового стабільного стану здійснюється дуже швидко. Цей час складається з часу передачі оголошення LSA і часу роботи алгоритму Дійкстри для знаходження нових маршрутів. Аналогічний процес відбувається і в тому випадку, коли в мережі з'являється новий сусід, який оголошує про себе за допомогою своїх повідомлень HELLO, або новий зв'язок.

Якщо ж стан мережі не змінюється, то оголошення про зв'язки не генеруються і таблиці маршрутизації не коригуються, що заощаджує пропускну здатність мережі та обчислювальні ресурси маршрутизаторів. Однак у цього правила є виняток: кожні 30 хвилин OSPF-маршрутизатори обмінюються всіма записами бази даних топологічної інформації, тобто взаємно синхронізують їх для більш надійної роботи мережі. Оскільки цей період досить тривалий, то цей виняток незначно позначається на роботі мережі.

Маршрутизатори з'єднані як з локальними мережами, так і безпосередньо між собою глобальними двоточковими лініями зв'язку, наприклад каналами T1. Протокол OSPF в своїх оголошеннях поширює інформацію про зв'язки двох типів: маршрутизатор-маршрутизатор і маршрутизатор-мережа.

Розглянемо ці типи зв'язку на прикладі мережі, поданої на рисунку 5.12. Даній мережі відповідає граф, наведений на рисунку 5.13.

Прикладом зв'язку першого типу служить зв'язок R3-R4, другого – зв'язок R4-195.46.17.0/24 (тут R3 і R4 також є IP-адресами, але використовуються символьні ідентифікатори, щоб відрізняти ці вершини графа від мереж, для яких було збережено звичайну нотацію IP-адрес).

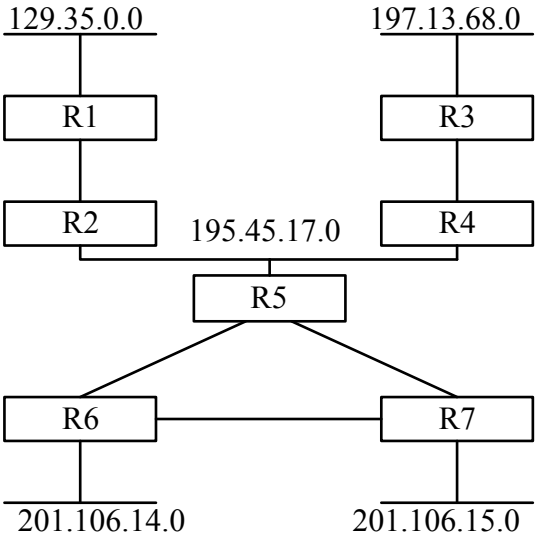


Рисунок 5.12 – Фрагмент мережі OSPF

Якщо двоточковими лініями зв’язати IP-адреси, то вони стануть додатковими вершинами графа, як і локальні мережі. Разом з IP-адресою мережі передається також інформація про маску мережі.

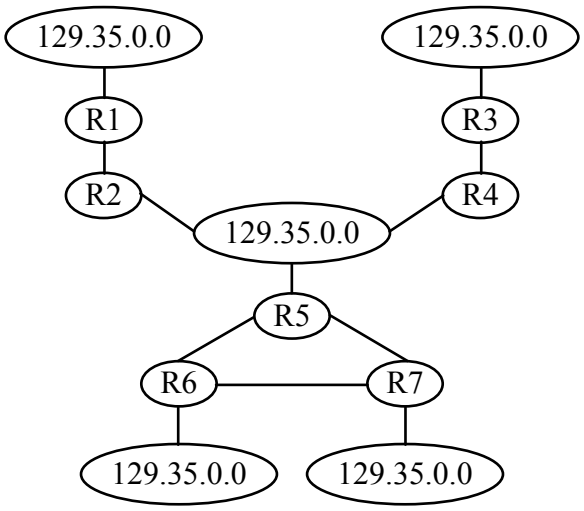


Рисунок 5.13 – Граф мережі, побудований протоколом OSPF

Кожен зв’язок характеризується атрибутами. Протокол OSPF за замовчуванням використовує метрику, що враховує пропускну спроможність каналів зв’язку. Крім того, допускається використання двох інших метрик, що враховують затримки і надійність передачі пакетів каналами зв’язку. Для кожної з метрик протокол OSPF будує окрему таблицю маршрутизації. Вибір потрібної таблиці відбувається залежно від значень бітів TOS в заголовку отриманого IP- пакета.

Протокол OSPF підтримує стандартні для багатьох протоколів (наприклад, для протоколу, що охоплює дерева мереж) значення відстаней для метрики, яка відображає пропускну здатність: так, для мережі Ethernet вона дорівнює 10, для Fast Ethernet - 1, для каналу T1 - 65, для каналу

56 Кбіт/с – 1785 [11]. При використанні високошвидкісних каналів, таких як Gigabit Ethernet або STM-16/64, адміністраторові потрібно задати іншу шкалу швидкостей, призначивши одиничну відстань найбільш швидкісному каналу. При виборі оптимального шляху на графі з кожним ребром графа пов'язана метрика, яка додається до шляху, якщо дане ребро до нього входить. Нехай на наведеному прикладі маршрутизатор R5 пов'язаний з маршрутизаторами R6 і R7 каналами T1, а маршрутизатори R6 і R7 пов'язані між собою каналом 56 Кбіт/с. Тоді R7 визначить оптимальний маршрут до мережі 201.106.14.0 як складової, яка проходить спочатку через R5, а потім через R6, оскільки у цього маршруту метрика буде дорівнює 65 + 65 = 130 одиниць. Безпосередній маршрут через R6 не буде оптимальним, оскільки метрика дорівнює 1785. При використанні хопів був би вибраний маршрут через R6, що було б неоптимально.

Протокол OSPF дозволяє зберігати в таблиці маршрутизації кілька маршрутів до однієї мережі, якщо вони мають рівні метрики. Якщо такі записи утворюються в таблиці маршрутизації, то маршрутизатор реалізує режим балансу завантаження маршрутів, відправляючи пакети по черзі по кожному з маршрутів.

На жаль обчислювальна складність протоколу OSPF швидко зростає зі збільшенням розмірності мережі. Для подолання цього недоліку в протоколі OSPF вводиться поняття області мережі. Маршрутизатори, які належать деякій території, будують граф зв'язків тільки для цієї області, що скорочує розмірність мережі. Між областями інформація про зв'язки не передається, а прикордонні для областей маршрутизатори обмінюються тільки інформацією про адреси мереж, які є в кожній з областей, і відстанню від прикордонного маршрутизатора до кожної мережі. При передачі пакетів між областями вибирається один з прикордонних маршрутизаторів області, а саме той, у якого відстань до потрібної мережі менша.

Порівняння протоколів RIP і OSPF за витратами на широкомовний трафік

У мережах, де використовується протокол RIP, накладні витрати на обмін маршрутною інформацією строго фіксовані. Якщо в мережі є певне число маршрутизаторів, то трафік, створюваний переданою маршрутною інформацією, описуються формулою:

$$F_{RIP} = \frac{n_м}{25} \cdot 528 \cdot n_к \cdot 8, \qquad (5.1)$$

де $n_м$ – кількість оголошених маршрутів;
528 – байтів у повідомленні; 8 – бітів у байті;
$n_к$ – кількість копій в одиницю часу.

У мережі із протоколом OSPF завантаження при незмінному стані ліній зв'язку створюється повідомленнями HELLO і оновленими оголошеннями про стан зв'язків, що описується формулою:

$$F_{OSPF} = (20 + 24 + 20 + 4 \cdot n_c) \cdot n_h \cdot 8 + n_м \cdot V_c \cdot n_к \cdot 8, \quad (5.2)$$

де 20 – розмір заголовка IP-пакета;
24 – заголовок пакета OSPF;
20 – розмір заголовка повідомлення HELLO;
4 – дані на кожного сусіда;
n_c – кількість сусідів;
n_h – кількість копій HELLO в одиницю часу;
V_c – середній розмір оголошення.

Інтенсивність розсилання повідомлень HELLO – кожні 10 секунд, оголошень про стан зв'язків – щопівгодини. По зв'язках «точка-точка» або по широкомовних локальних мережах в одиницю часу посилається тільки одна копія повідомлення, по глобальних мережах типу FRAME RELAY кожному сусідові посилається своя копія повідомлення. У мережі FRAME RELAY з 10 сусідніми маршрутизаторами й 100 маршрутами в мережі (нехай кожний маршрут являє собою окреме OSPF-узагальнення про мережеві зв'язки й RIP поширює інформацію про всі ці маршрути) трафік маршрутної інформації визначається співвідношеннями (5.1) і (5.2):

$$F_{RIP} = \frac{100 \text{ маршрутів}}{25 \text{ маршрутів в оголошенні}} \cdot 528 \cdot \frac{10 \text{ копій}}{30c} \cdot 8 = 5632 \text{ біт/с};$$

$$F_{OSPF} = (20 + 24 + 20 + 4 \cdot 10) \cdot \frac{10 \text{ копій}}{10c} \cdot 8 +$$
$$+ 100 \text{ маршрутів} \cdot (32 + 24 + 20) \cdot \frac{10 \text{ копій}}{30 \cdot 60c} \cdot 8 = 1170 \text{ біт/с}.$$

Як видно з отриманих результатів, для досліджуваного прикладу трафік, що створюється протоколом RIP, майже в 5 разів інтенсивніший за трафік, що створюється протоколом OSPF.

Хід роботи

1. Винести на логічне поле шість маршрутизаторів 1841 та два комп'ютери.

2. Відкрити вікно властивостей одного із маршрутизаторів та додати у вільні слоти порти даних типу WIC-2T. Перед початком монтажу плат не забувати вимкнути живлення маршрутизатора та потім увімкнути його.

3. Виконати з'єднання між вузлами мережі, як зображено на рисунку. При цьому з'єднання маршрутизатора і комп'ютера здійснювати перехресним кабелем, використовуючи інтерфейс Fast Ethernet. З'єднувати маршрутизатори між собою кабелем RS-232 DCE, використовуючи інтерфейс Serial. Робоча структура мережі зображена на рисунку 5.14.

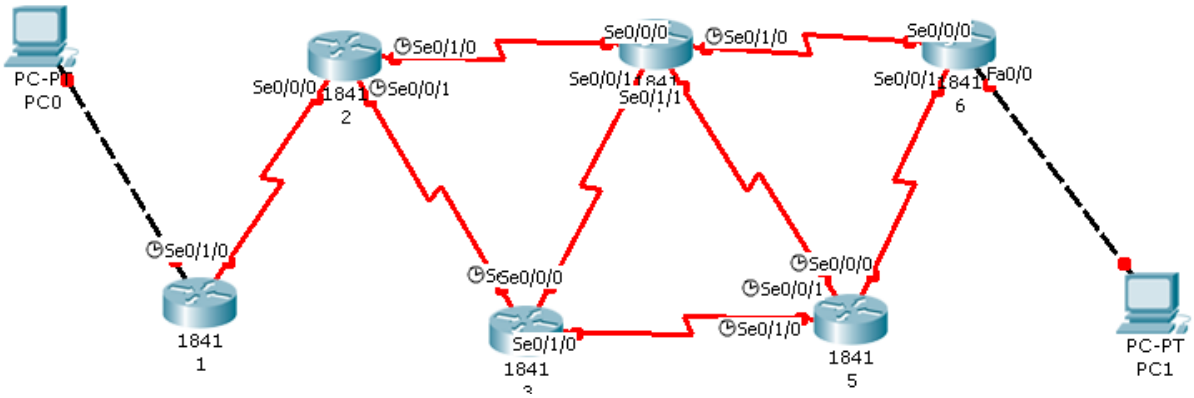


Рисунок 5.14 – Структура мережі для дослідження протоколу OSPF

4. Інтерфейсу Fast Ethernet першого комп'ютера присвоїти IP-адресу 200.1.1.10, IP-адреса шлюзу – 200.1.1.1, маска підмережі – 255.255.255.0. Інтерфейсу Fast Ethernet другого комп'ютера присвоїти IP-адресу 200.2.2.10, IP-адреса шлюзу – 200.2.2.1, маска підмережі – 255.255.255.0.

5. Карта IP-адресації між маршрутизаторами:

– комп'ютер 1 – маршрутизатор 1: 200.1.1.0;
– маршрутизатори 1 – 2: 192.1.1.0;
– маршрутизатори 2 – 3 192.2.2.0;
– маршрутизатори 2 – 4 192. 3.3.0;
– маршрутизатори 3 – 4 192.4.4.0;
– маршрутизатори 3 – 5 192.5.5.0;
– маршрутизатори 4 – 5 192.6.6.0;
– маршрутизатори 4 – 6 192.7.7.0;
– маршрутизатори 5 – 6 192.8.8.0;
– комп'ютер 2 – маршрутизатор 5: 200.2.2.0.

Детальна карта маршрутизації наведена у додатку Б графічної частини.

6. Налаштування маршрутизатора 1. Відкрити вікно властивостей маршрутизатора та перейти у термінал. Виконати введення таких команд:

Router>enable
Router#conf ter
Router(config)#iterface fastEthernet 0/0
Router(config-if)#ip address 200.1.1.1 255.255.255.0
Router(config-if) #no shutdown
Router(config-if)#exit
Router(config)#interface serial x/x/x // x/x/x номер порту Serial, до //якого підключено сусідній маршрутизатор

Виходячи із вищевказаної межі адресації, порту Serial x/x/x присвоюється IP-адреса 192.1.1.1:

Router(config-if)#ip address 198.1.1.1 255.255.255.0
Router(config-if) #no shutdown
Router(config-if)#clock rate 64000 // частота синхронізації

Router(config-if)#exit
Router(config)#exit
Router#wr mem

7. Аналогічним чином присвоїти адресу усім задіяним портам усіх маршрутизаторів, керуючись картою IP-адресації, вказаної у п. 5.

8. Налаштування протоколу OSPF. Після налаштувань усіх портів усіх маршрутизаторів перейти у термінал першого маршрутизатора та виконати введення таких команд:

Router>enable
Router#conf ter
Router(config)# router ospf 10 // вказання налаштування таблиці OSPF під //обліковим записом 10

Вказання сусідніх напрямів (нумерації сусідніх локальних мереж):

Router(config-router)#net 200.1.1.0 0.0.0.255 area 0
Router(config-router)#net 192.1.1.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#exit
Router#wr mem

Після налаштування виконати ping-запит між першим комп'ютером та маршрутизатором 1.

9. Аналогічно п. 8 виконати налаштування таблиці OSPF для кожного маршрутизатора, виходячи із сусідніх для нього вихідних напрямів і карти IP-адресації. Після налаштування кожного маршрутизатора виконувати ping-запити між уже налаштованими вузлами (включно із комп'ютером).

10. Після налаштування усіх маршрутизаторів перейти у режим моделювання (Shift+S). Покроково дослідити передачу OSPF-пакетів між маршрутизаторами, здійснити ping-запит між комп'ютерами, відслідковуючи його переміщення та аналізуючи інформацію про пакет згідно із багаторівневою моделлю OSI.

11. Виконати дослідження роботи протоколу OSPF, промоделювавши його роботу у пакеті моделювання Packet Tracer 5.2. На логічне поле винести 6 маршрутизаторів 1841 та два комп'ютери. Кожен маршрутизатор пронумерувати у діапазоні від 0 до 6.

Перед початком виконання фізичних з'єднань між вузлами мережі у кожному вузлі маршрутизації у вільні місця необхідно додати кінцеве обладнання (інтерфейси) лінії зв'язку, яка умовно прокладається між маршрутизаторами. Кількість портів, яких необхідно додати – 4. На рис. 5.15 зображено знімок вікна властивостей маршрутизатора. Перед початком монтажу портів вимкнути обладнання, а потім із бібліотеки доступних модулів додати обладнання WIC-2T. Після цього ввімкнути живлення маршрутизатора.

Аналогічним чином виконати додавання обладнання у інших п'яти маршрутизаторах.

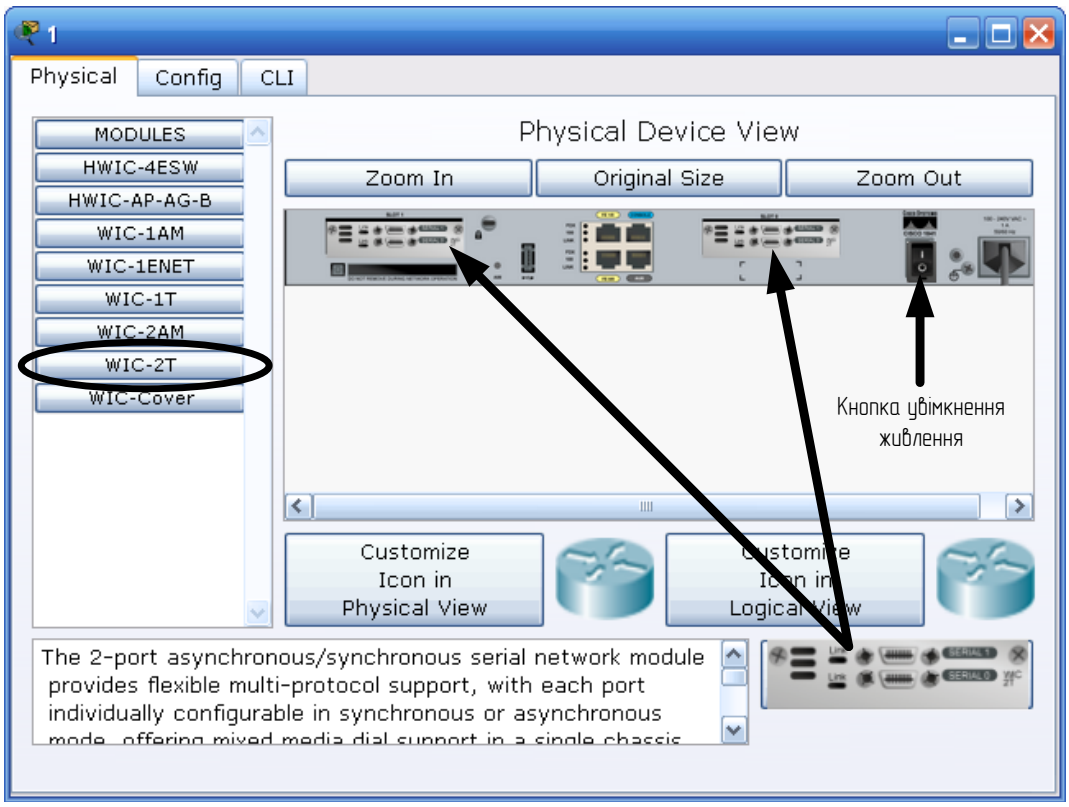


Рисунок 5.15 – Знімок вікна налаштувань маршрутизатора

Фізичні з'єднання між маршрутизаторами та комп'ютерами зображено на рисунку 5.16. Обидва комп'ютери з маршрутизаторами з'єднуються перехресним кабелем UTP, використовуючи інтерфейс Fast Ethernet , з'єднання між маршрутизаторами виконується кабелем кінцевого обладнання Serial DCE, використовуючи інтерфейс Serial. Загальна структура побудованої мережі зображена на рисунку 5.16.

У таблиці 5.7 наведено номери портів відповідних задіяних інтерфейсів, відповідно напрямків (сусідніх маршрутизаторів), до яких вони підключені.

Перед початком налаштування маршрутизаторів у таблицю 5.8 звести мапу IP-адрес між вузлами мережі.

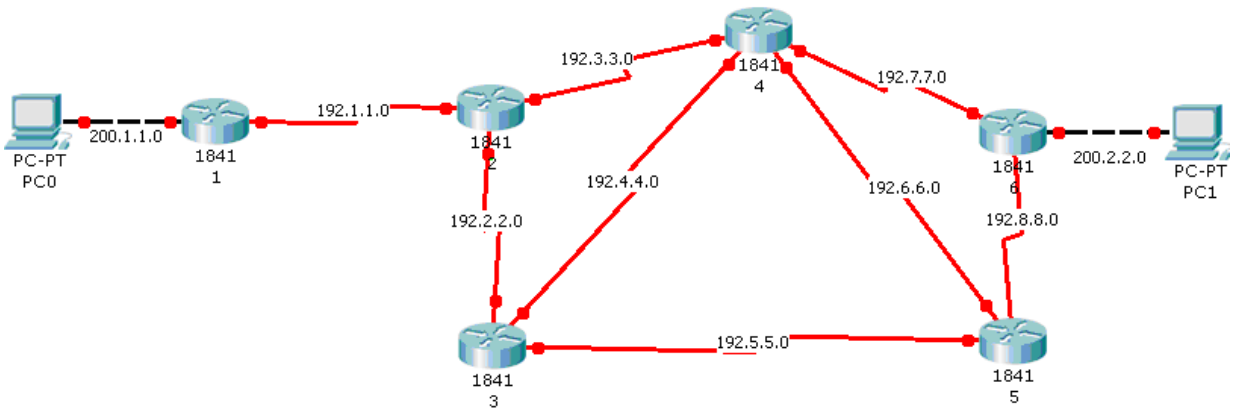


Рисунок 5.16 – Структура досліджуваної мережі

Таблиця 5.7 – Номери портів у відповідних напрямках

Маршрути-затор	1	2	3	4	5	6
Напрямок	Номер порту інтерфейсу					
1		Se 0/0/0				
2	Se 0/1/0		Se 0/0/0	Se 0/1/1		
3		Se 0/0/1		Se 0/0/0	Se 0/1/0	
4		Se 0/1/0	Se 0/0/1		Se 0/0/0	Se 0/0/1
5			Se 0/1/0	Se 0/0/1		Se 0/0/0
6				Se 0/1/0	Se 0/0/1	
PC0	Fa 0/0					
PC1						Fa0/0

Таблиця 5.8 – Діапазони IP-нумерації у відповідних напрямках

Маршрути-затор	1	2	3	4	5	6
Напрямок	IP-нумерація					
1	192.1.1.0	192.1.1.0				
2			192.2.2.0	192.3.3.0		
3		192.2.2.0		192.4.4.0	192.5.5.0	
4		192.3.3.0	192.4.4.0		192.6.6.0	192.7.7.0
5			192.5.5.0	192.6.6.0		192.8.8.0
6				192.7.7.0	192.8.8.0	
PC0	200.1.1.0					
PC1						200.2.2.0

Таким чином, молодший розряд IP-нумерації кожного маршрутизатора буде відповідати порядковому номеру відповідного маршрутизатора. При цьому порти Fa 0/0 першого та шостого маршрутизаторів, які мають пряме підключення до комп'ютерів, матимуть IP-адреси 200.1.1.1 та 200.2.2.1, відповідно. Комп'ютери PC0 та PC1 матимуть IP-адреси 200.1.1.2 та 200.2.2.2, відповідно.

12. Виконати налаштування обладнання. На рисунку 5.17 зображено знімок вікна властивостей комп'ютера, у якому виконано налаштування комп'ютера PC0. Аналогічно налаштувати комп'ютер PC1 відповідно до своєї IP-нумерації.

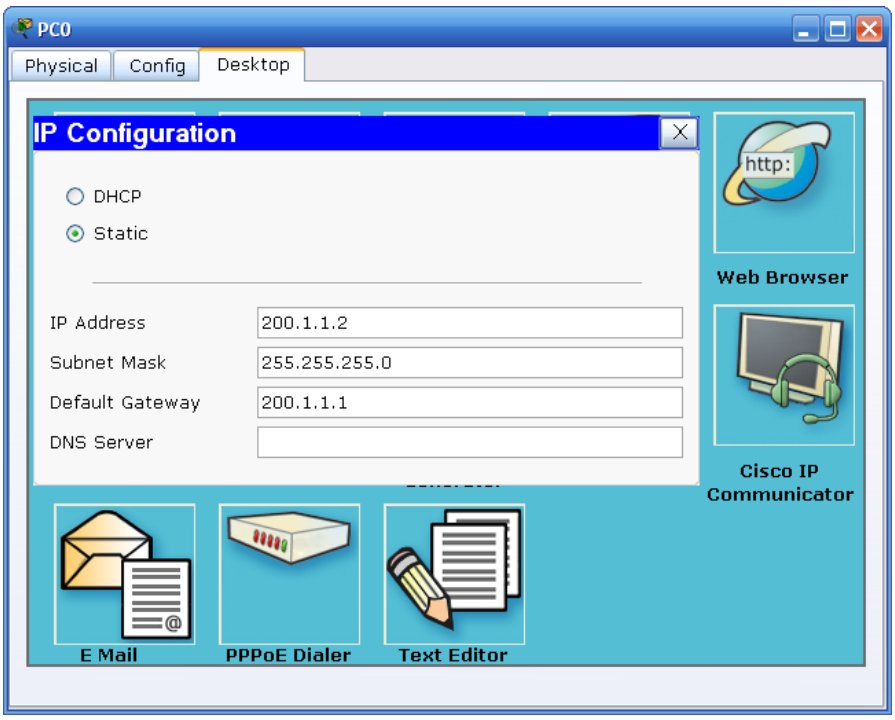


Рисунок 5.17 – Налаштування комп'ютера PC0

13. Виконати налаштування першого маршрутизатора. Для цього відкрити вікно його властивостей та перейти у режим термінала. Виконати введення таких команд

```
Router>enable
Router#conf ter
Router(config)#iterface fastEthernet 0/0
Router(config-if)#ip address 200.1.1.1 255.255.255.0
Router(config-if) #no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/1/0
Router(config-if)#ip address 198.1.1.1 255.255.255.0
Router(config-if) #no shut
Router(config-if)#clock rate 64000
Router(config-if)#exit
Router(config)# router ospf 10
Router(config-router)#net 200.1.1.0 0.0.0.255 area 0
Router(config-router)#net 192.1.1.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#exit
Router#wr mem
```

Таким чином, по-перше, було виконано налаштування підключених інтерфейсів маршрутизатора, по-друге, було виконано налаштування роботи протоколу OSPF шляхом вказання двох вихідних для даного маршрутизатора напрямків – комп'ютера PC0 та маршрутизатора 2.

14. Виконати випробовування роботоздатності налаштованого маршрутизатора шляхом посилання луна-запиту від комп'ютера до маршрутизатора. Для цього переключитися у режим покрокового моделювання та поставити на відправлення луна-запит. Результат моделювання зображено на рисунку 5.18.

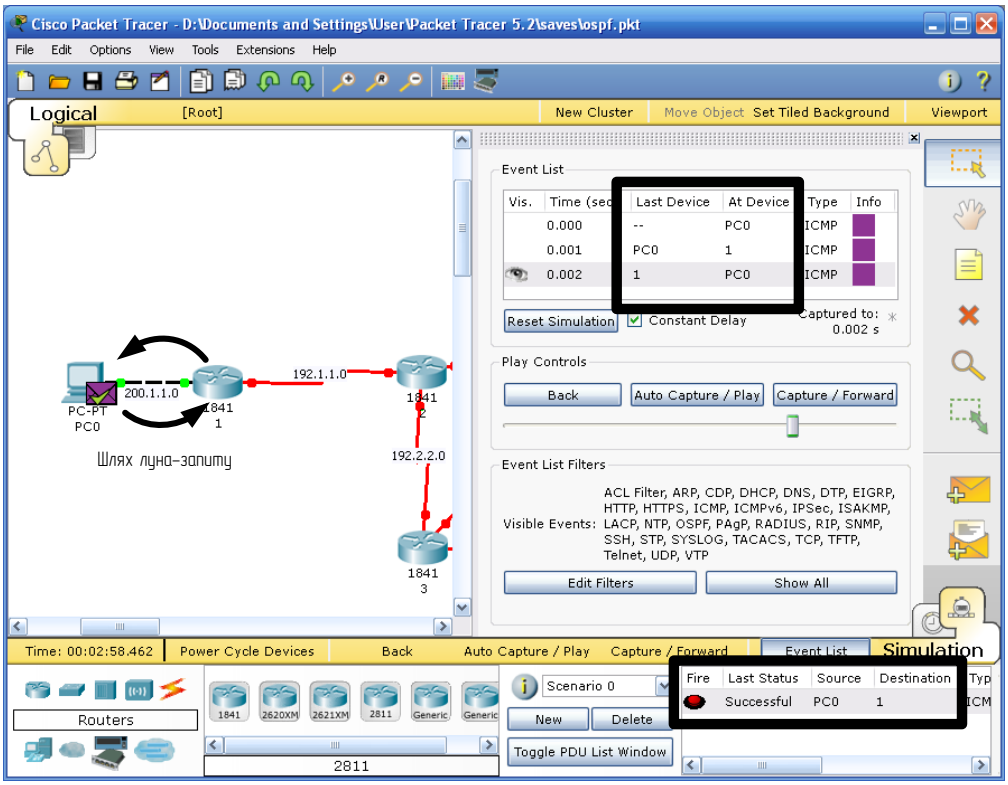


Рисунок 5.18 – Відправлення луна-запиту від комп'ютера PC0 до маршрутизатора 1

Із поля статусу видно, що пакет доставлено успішно. Таким чином, маршрутизатор 1 налаштовано правильно.

Аналогічним чином виконати налаштування маршрутизатора 2:

```
Router>enable
Router#conf ter
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 198.1.1.2 255.255.255.0
Router(config-if) #no shut
Router(config-if)#clock rate 64000
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 198.2.2.2 255.255.255.0
Router(config-if) #no shut
Router(config-if)#clock rate 64000
Router(config-if)#exit
Router(config)#interface serial 0/1/0
Router(config-if)#ip address 198.3.3.2 255.255.255.0
```

Router(config-if) #no shut
Router(config-if)#clock rate 64000
Router(config-if)#exit

Router(config)# router ospf 10
Router(config-router)#net 192.1.1.0 0.0.0.255 area 0
Router(config-router)#net 192.2.2.0 0.0.0.255 area 0
Router(config-router)#net 192.3.3.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#exit
Router#wr mem

Після цього виконати моделювання шляхом передачі луна-запиту від комп'ютера PC0 до маршрутизатора 2. Результат моделювання подано на рисунку 5.19.

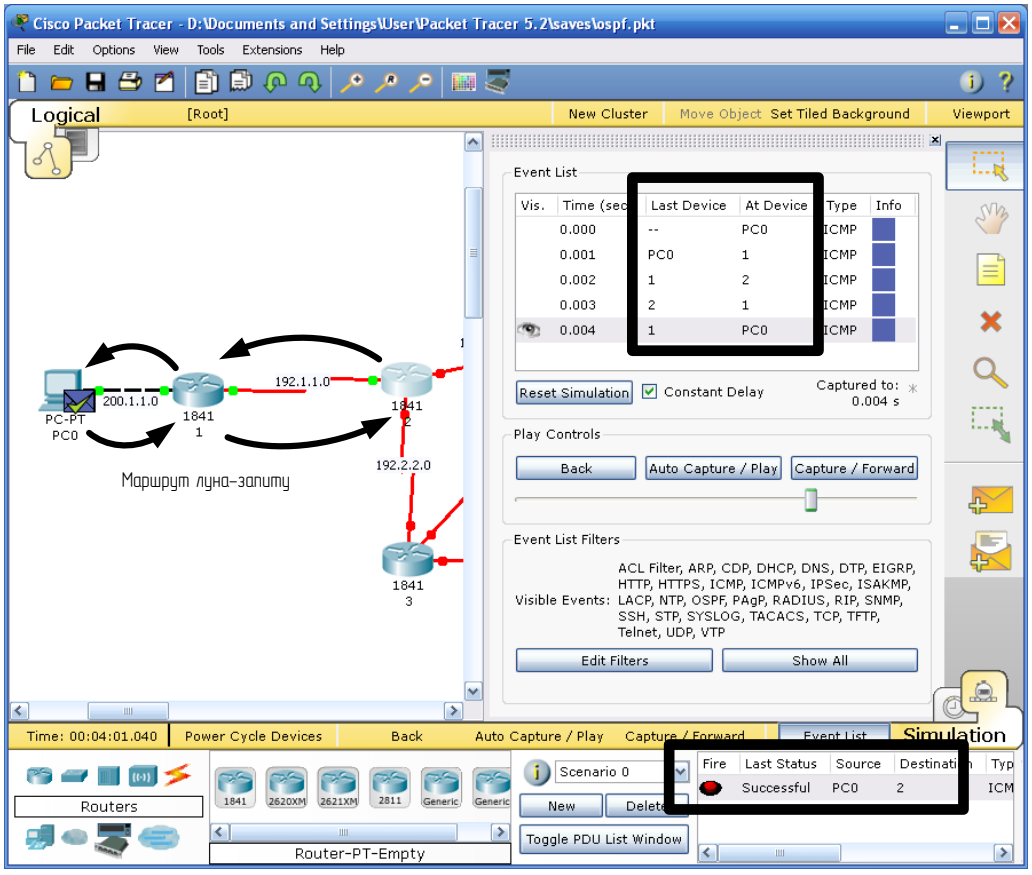


Рисунок 5.19 – Відправлення луна-запиту від комп'ютера PC0 до маршрутизатора 2

Із поля статусу відправлення пакетів видно, що він дійшов успішно. У таблиці подій видно, у якій послідовності виконувалась передача пакета.

Виконати налаштування усіх маршрутизаторів згідно з таблицями 5.9 та 5.10.

15. Після виконання налаштування усього обладнання виконати моделювання луна-запиту між комп'ютерами PC0 та PC1. Знімок екрана вико-

наного моделювання зображено на рисунку 5.20. Тут ми бачимо послідовність передачі пакета, що підтверджується таблицею подій. Ознакою того, що пакет відправився вдало, є напис Successful у полі статусу.

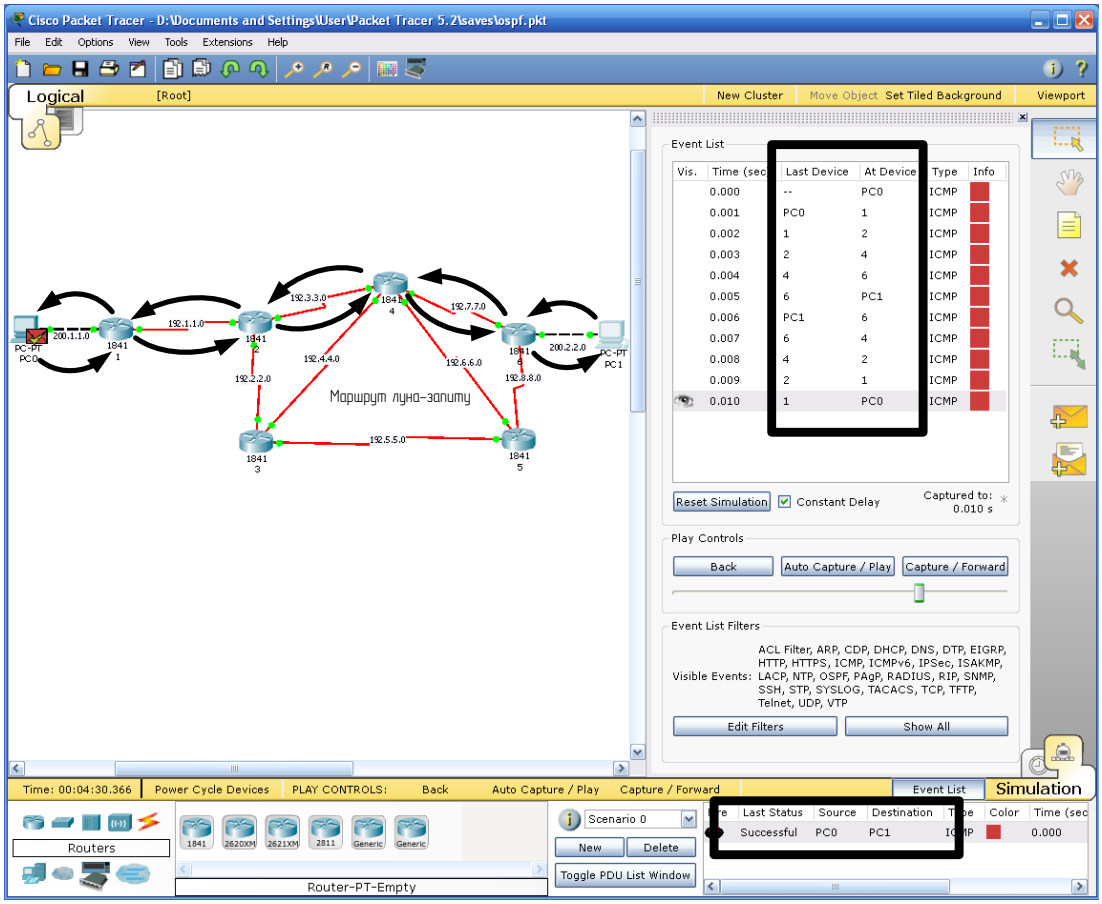


Рисунок 5.20 – Відправлення луна-запиту від комп’ютера PC0 до комп’ютера PC1

16. Дослідити передачу пакетів протоколу OSPF. Для цього видалити усі сценарії та перейти до режиму покрокового моделювання. Щоб прослідкувати автоматичну передачу пакетів між маршрутизаторами, кілька разів натиснемо на панелі покрокового моделювання кнопку Capture/Forward. Періодично із кожного маршрутизатора відправляються пакети OSPF. Кожна передача пакета фіксується у таблиці подій (рис. 5.21), де можна побачити, що таке пересилання відбувається періодично від кожного маршрутизатора до кожного сусіднього маршрутизатора.

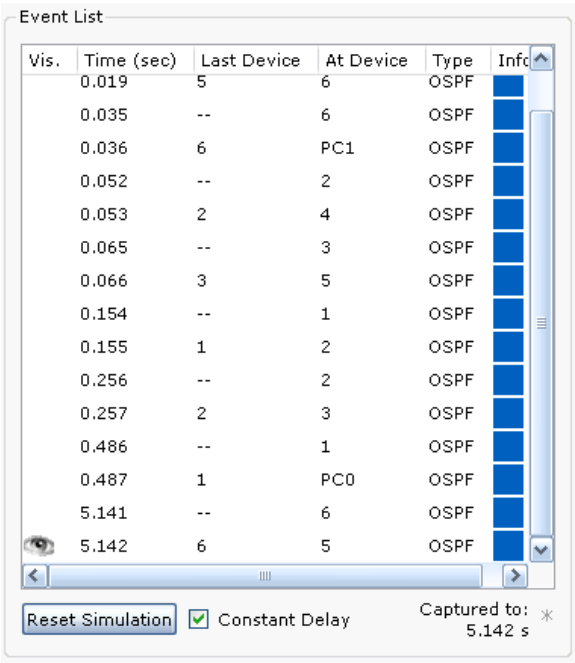


Рисунок 5.21 – Таблиця подій передачі пакетів OSPF

Клацнувши на будь-який пакет, можна побачити його структуру у вікні інформації про пакет (рис. 5.22)

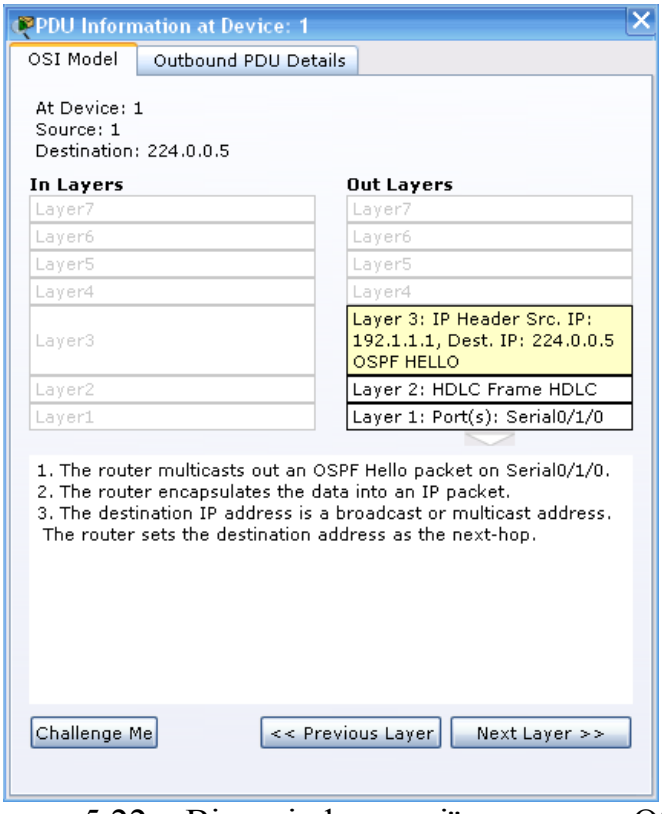


Рисунок 5.22 – Вікно інформації про пакет OSPF

На першій вкладці наочно зображено, що протокол OSPF займає верхній рівень над транспортним та фізичним протоколами.

На другій вкладі зображено структури кадрів усіх задіяних рівнів багаторівневої моделі OSI. Основна інформація, яка нас цікавить – це структура OSPF-кадру типу «HELLO», у якому міститься інформація про адресу сусіднього маршрутизатора на іншому інтерфейсі.

Структура такого кадру зображена на рисунку 5.23.

Видалити усі колишні сценарії. Не виходячи із режиму покрокового моделювання, вимкнути маршрутизатор 4. Вимкнення даного маршрутизатора перекриє найкоротший шлях передачі пакетів від комп'ютера PC0 до комп'ютера PC1 і навпаки. Реакцією на вимкнення даного маршрутизатора стане поява на усіх портах усіх маршрутизаторів OSPF-пакетів, задача яких – оновити таблиці маршрутизації кожного з маршрутизаторів і проінформувати про відсутність з'єднання із маршрутизатором 4 (рис. 5.24). Передача пакетів OSPF лиш не буде проводитись у напрямку відключеного маршрутизатора 4, оскільки саме відсутність з'єднання з цим маршрутизатором стала причиною оперативного оновлення таблиці маршрутизації.

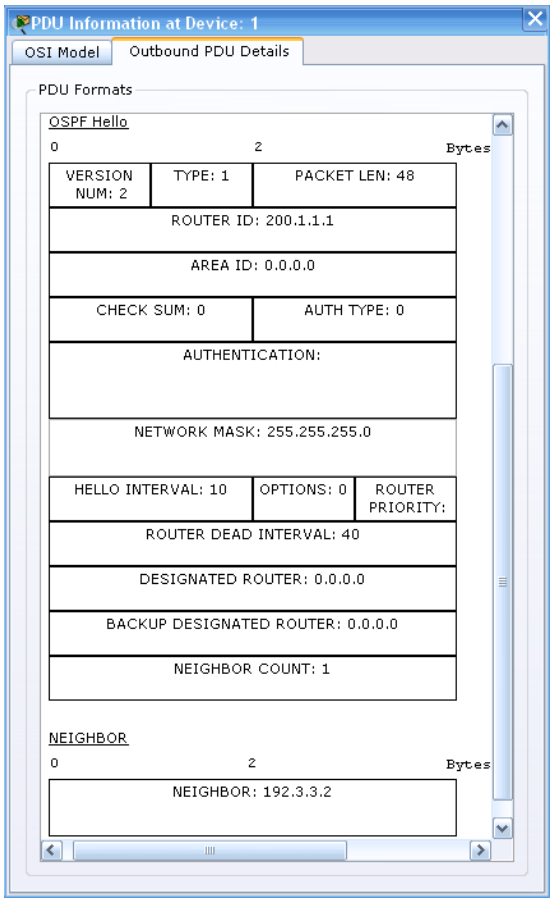


Рисунок 5.23 – Структура кадру OSPF типу «HELLO»

Очистити сценарії та провести передачу луна-запиту між комп'ютерами PC0 та PC1. На рисунку 5.25 зображено знімок екрана проведення даного моделювання. Тут передача пакета змінила свій маршрут із попереднього коротшого на більш довгий, але робочий. Пакет передається успішно.

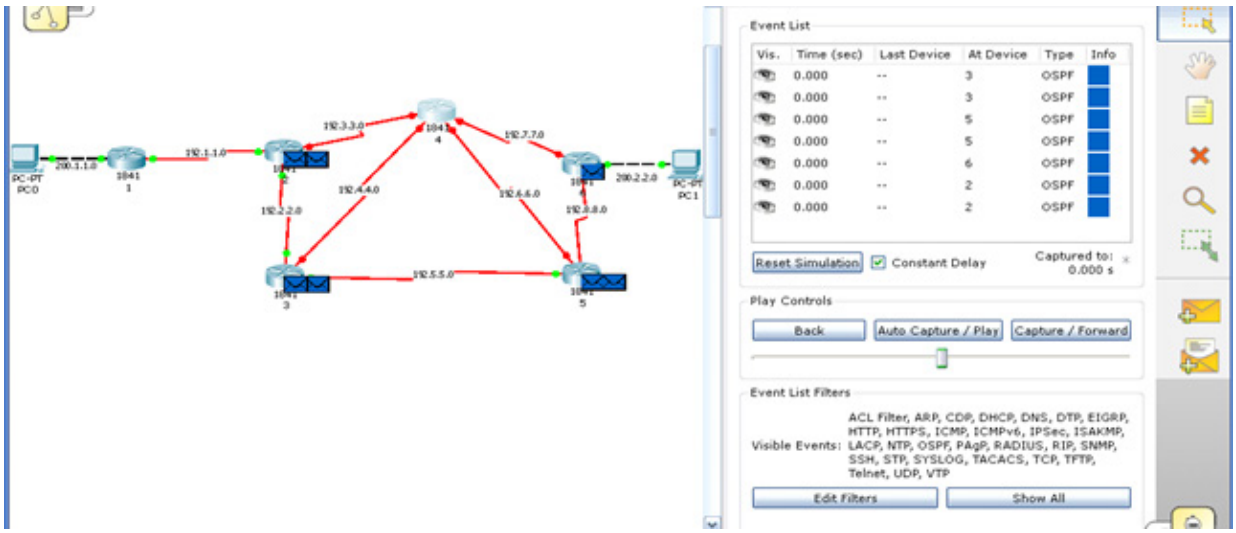


Рисунок 5.24 – Оновлення таблиць маршрутизації

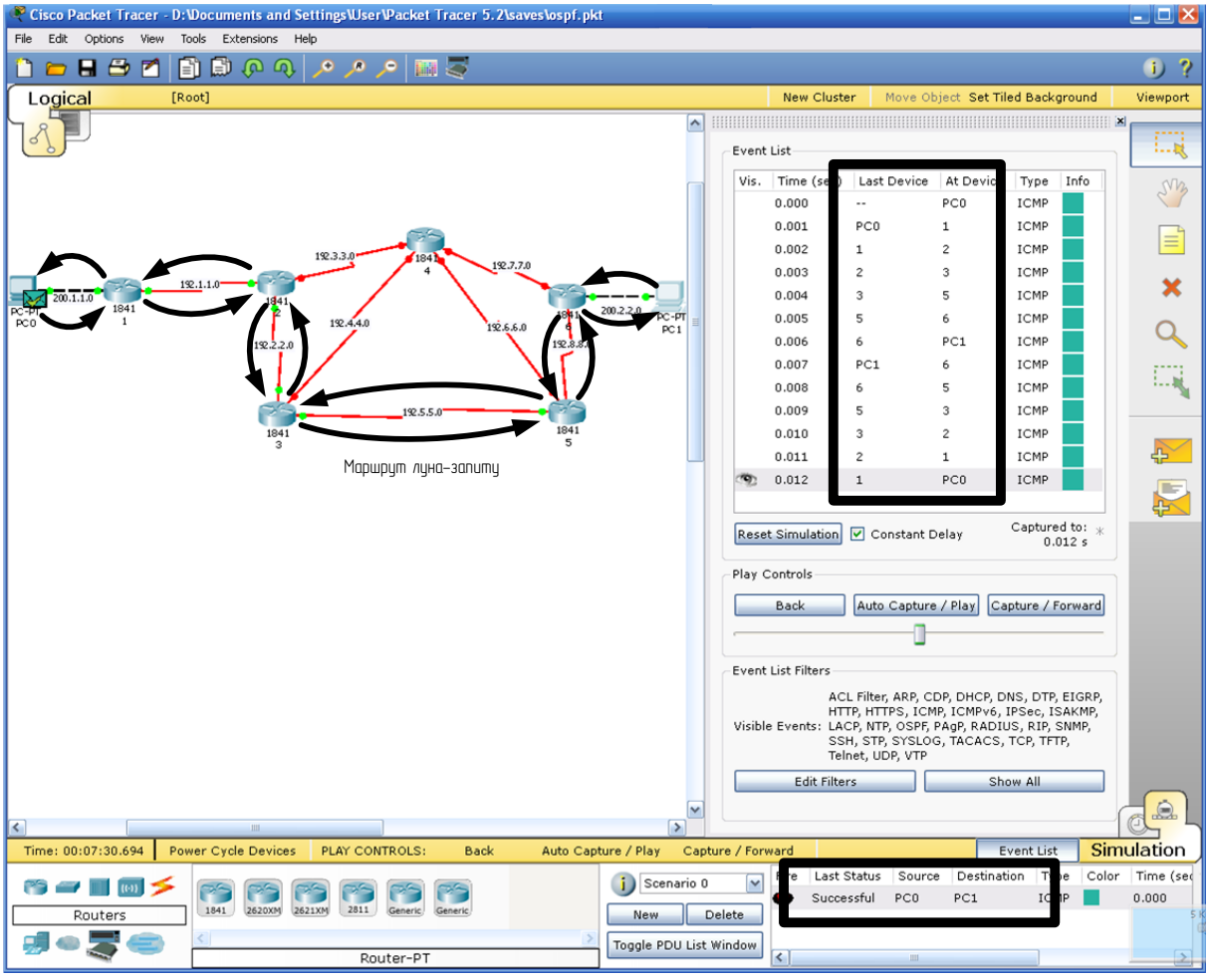


Рисунок 5.25 – Передача луна-запиту альтернативним шляхом

Якщо назад увімкнути маршрутизатор 4, то для того, щоб новий найкоротший шлях був задіяний, необхідно буде почекати певний час (приблизно десять секунд), поки таблиці маршрутизації знову не оновляться.

Зміст звіту

1. Тема і мета роботи.
2. Короткий опис принципу роботи протоколу OSPF.
3. Завдання до лабораторної роботи.
4. Знімки екрана із мережею, побудованою на маршрутизаторах, для дослідження роботи протоколу OSPF.
5. Знімки екрана налаштування властивостей маршрутизатора через діалогове вікно та через командний рядок.
6. Знімки екрана налаштування таблиці OSPF для маршрутизаторів.
7. Результати проведеного пінгування.

Контрольні запитання

1. В чому полягає основний принцип роботи протоколів маршрутизації, які будуються на алгоритмах стану зв'язків?
2. Які параметри мережі враховують метрики, підтримувані протоколом OSPF?
3. Які параметри мережі враховуються при машрутизації на основі протоколу OSPF?
4. Як змінити еталонну пропускну здатність в OSPF?
5. Як OSPF розраховує метрику або вартість?
6. Чи виконується аутентифікація для обміну даними в протоколі OSPF?
7. Що таке інтервал повторної передачі стану каналу і якою командою він задається?
8. Чи можна створити маршрут OSPF за замовчуванням в системі, яка основана на зовнішніх даних маршрутизатора і не має маршруту за замовчуванням?
9. Яку роль відіграють повідомлення HELLO в протоколі OSPF ?
10. Для чого мережу маршрутизаторів, що працюють за протоколом OSPF, розбивають на області?
11. Запропонуйте варіанти метрики, яка одночасно враховує пропускну здатність, надійність і затримку ліній зв'язку.
12. Чому об'єм службової інформації OSPF значно менший, ніж у RIP?

Лабораторна робота № 6
Система DNS

Мета: навчитися налаштовувати DNS-сервер.

Теоретичні відомості

Система імен доменів (DNS – Domain Name System) – це розподілена база даних, яка використовується стеком протоколів TCP/IP, для встановлення відповідності між іменами хостів та IP адресами [4]. DNS також використовується для маршрутизації електронної пошти. Використано термін «розподілена», тому що на одному вузлі Internet не зберігається вся необхідна інформація. Кожен вузол (університет, університетське містечко, компанія або відділ всередині компанії) підтримує власну інформаційну базу даних і запускає програму сервер, яка може відправити запит по Internet до інших систем. DNS надає протокол, який дозволяє клієнтам і серверам спілкуватися один з одним.

Ієрархія доменних імен аналогічна ієрархії імен файлів, прийнятій у багатьох поширених файлових системах (рисунок 5.26) [6]. Дерево імен починається з кореня, який позначається точкою (.). Потім слідує старша символьна частина імені, друга за старшинством символьна частина імені тощо. Молодша частина імені відповідає кінцевому вузлу мережі. На відміну від імен файлів, під час запису яких спочатку вказується сама старша складова, потім складова більш низького рівня тощо, запис доменного імені починається з наймолодшої складової, а закінчується найстаршою. Складові частини доменного імені відділяються одна від одної точкою. Наприклад, в імені mail.google.com складова mail є ім’ям одного з комп’ютерів в домені google.com.

Поділ імені на частини дозволяє розділити адміністративну відповідальність за призначення унікальних імен між різними людьми або організаціями в межах свого рівня ієрархії. Так, для прикладу, наведеного на рисунку, одна людина може нести відповідальність за те, щоб всі імена, які мають закінчення «ua», мали унікальну прямуючу униз по ієрархії частину. Якщо ця людина справляється зі своїми обов’язками, то всі імена типу www.ua, mail.meta.ua або m2.shop.meta.ua будуть відрізнятися другою за старшинством частиною.

Поділ адміністративних обов’язків дозволяє вирішити проблему створення унікальних імен без взаємних консультацій між організаціями, які відповідають за імена одного рівня ієрархії. Очевидно, що повинна існувати одна організація, що відповідає за призначення імен верхнього рівня ієрархії.

Сукупність імен, у яких кілька старших складових частин збігаються, утворюють домен імен (domain). Наприклад, імена www1.shop.meta.ua, ftp.dlink.com.ua, i.ua та mail.meta.ua входять у домен ua, тому що всі вони мають одну загальну старшу частину – ім’я ua. Іншим прикладом є домен

vn.ua. З наведених на рисунку імен в нього входять імена s1.vn.ua, s2. vn.ua і ss.vn.ua. Цей домен утворюють імена, у яких дві старші частини завжди дорівнюють vn.ua. Адміністратор домену vn.ua несе відповідальність за унікальність імен наступного рівня, що входять в домен, тобто імен s1, s2 і ss. Створені домени s1.vn.ua, s2.vn.ua і ss.vn.ua є піддоменами домену vn.ua, оскільки мають загальну старшу частину імені. Часто піддомени для стислості називають тільки молодшою частиною імені, тобто піддомени s1, s2 і ss.

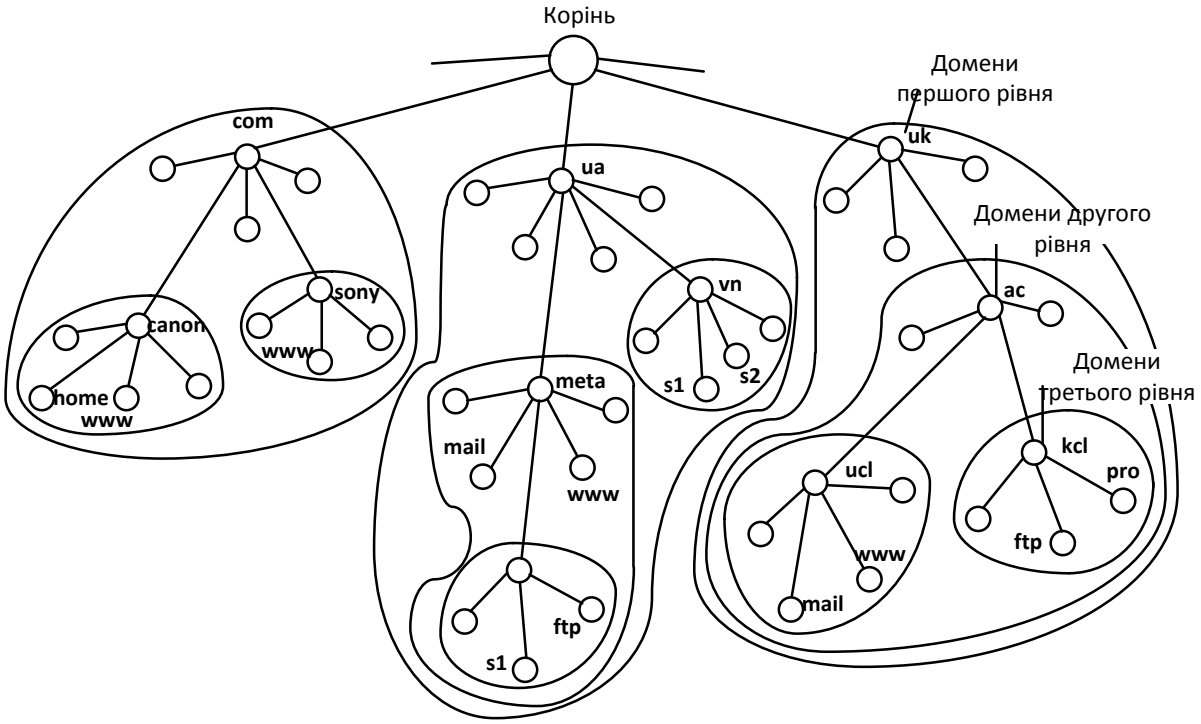


Рисунок 5.26 – Простір доменних імен

Якщо в кожному домені і піддомені забезпечується унікальність імен наступного рівня ієрархії, то й вся система імен буде складатися з унікальних імен. За аналогією з файловою системою в доменній системі імен розрізняють короткі імена, відносні імена й повні доменні імена. Коротке ім’я – це ім’я кінцевого вузла мережі: хоста або порту маршрутизатора. Коротке ім’я – це лист дерева імен. Відносне ім’я – це складене ім’я, що починається із деякого рівня ієрархії, але не найвищого. Наприклад, wwwl.shop – це відносне ім’я. Повне доменне ім’я (Fully Qualified Domain Name, FQDN) включає складові всіх рівнів ієрархії, починаючи від короткого імені і закінчуючи кореневою точкою: www1.shop.meta.ua.

Кореневий домен управляється центральними органами Інтернету IANA і InterNIC. Домени верхнього рівня призначаються для кожної країни, а також для типів організацій. Імена цих доменів повинні відповідати міжнародному стандарту ISO 3166. Для позначення країн використовуються трибуквені і двобуквені абревіатури, наприклад ua (Україна), uk (Велика Британія), pl (Польща), us (Сполучені Штати Америки), а для різних типів організацій – наприклад, такі позначення:

– com – комерційні організації (наприклад, microsoft.com);
– edu – освітні організації (наприклад, nic.edu);
– gov – урядові організації (наприклад, rada.gov);
– org – некомерційні організації (наприклад, wikipedia.org);
– net – мережеві організації (наприклад, speedtest.net).

Кожен домен адмініструє окрема організація, яка зазвичай розбиває свій домен на піддомени і передає функції адміністрування цих піддоменів іншим організаціям. Щоб отримати доменне ім'я, необхідно зареєструватися у будь-якій організації, якій орган InterNIC делегував свої повноваження з розподілу імен доменів.

Доменна система імен реалізована в Інтернеті, але вона може працювати і як автономна система імен у будь-якій великій корпоративній мережі, яка хоч і використовує стек TCP/IP, але ніяк не пов'язана з Інтернетом.

Схема роботи DNS

Широкомовний спосіб встановлення відповідності між символьними іменами і локальними адресами, подібно протоколу ARP, добре працює тільки в невеликій локальній мережі, не розділеній на підмережі. У великих мережах, де можливість загального широкомовного розсилання не підтримується, потрібен інший спосіб дозволу символьних імен. Вдалою альтернативою широкомовного розсилання є застосування централізованої служби, яка підтримує відповідність між різними типами адрес всіх комп'ютерів мережі. Наприклад, компанія Microsoft для своєї корпоративної операційної системи Windows NT розробила централізовану службу WINS, яка підтримувала базу даних NetBIOS-імен і відповідних їм IP-адрес.

У мережах TCP/IP відповідність між доменними іменами та IP-адресами може встановлюватись засобами як локального хоста, так і централізованої служби [12].

На ранньому етапі розвитку Інтернету на кожному хості вручну створювався текстовий файл з відомим ім'ям hosts.txt. Цей файл складався з деякої кількості рядків, кожен з яких містить одну пару «доменне ім'я - IP-адреса », наприклад: rhino.acme.com – 102.54.94.97.

Із зростанням Інтернету файли hosts.txt також збільшувалися в обсязі, та створення масштабованого рішення для розв'язання імен стало необхідністю. Таким рішенням стала централізована служба DNS (Domain Name System − система доменних імен), основана на розподіленій базі відображень «доменне ім'я – IP-адреса ». Служба DNS використовує у своїй роботі DNS-сервери і DNS-клієнти. DNS-сервери підтримують розподілену базу відображень, а DNS-клієнти звертаються до серверів із запитами про дозвіл доменного імені в IP-адресу.

Служба DNS використовує текстові файли майже такого формату, як і файл hosts, і ці файли адміністратор також готує вручну. Однак служба DNS опирається на ієрархію доменів, і кожен сервер служби DNS зберігає тільки частину імен мережі, а не всі імена, як це відбувається при викорис-

танні файлів hosts. При зростанні кількості вузлів у мережі проблема масштабування вирішується створенням нових доменів і піддоменів імен і додаванням до служби DNS нових серверів.

Для кожного домену імен створюється свій DNS-сервер. Є два розподіли імен на серверах. У першому випадку сервер може зберігати відображення «доменне ім'я – IP-адреса» для всього домену, включаючи всі його піддомени. Однак таке рішення виявляється погано масштабованим, тому що при додаванні нових піддоменів навантаження на цей сервер може перевищити його можливості. Частіше використовується інший підхід, коли сервер домену зберігає тільки імена, які закінчуються на наступному нижче рівні ієрархії в порівнянні з ім'ям домену. (Аналогічно каталогу файлової системи, що містить записи про файли і підкаталоги, які безпосередньо входять у нього). Саме при такій організації служби DNS навантаження з вирішення імен розподіляється більш рівномірно між усіма DNS-серверами мережі. Наприклад, у першому випадку DNS-сервер домена meta.ua буде зберігати відображення для всіх імен, які закінчуються на meta.ua (www1.shop.meta.ua, , mail.meta.ua тощо). У другому випадку цей сервер зберігає відображення тільки імен типу mail.meta.ua, www.meta.ua, а всі інші відображення повинні зберігатися на DNS-сервер піддомену meta. Кожен DNS-сервер крім таблиці відображень імен містить посилання на DNS-сервери своїх піддоменів. Ці посилання зв'язують окремі DNS-сервери в єдину службу DNS. Посилання являють собою IP-адреси відповідних серверів. Для обслуговування кореневого домена виділено декілька дублюючих один одного DNS-серверів, IP-адреси яких є широко відомими (Їх можна дізнатися, наприклад, в InterNIC).

Процедура дозволу DNS-імені багато в чому аналогічна процедурі пошуку файловою системою адреси файлу за його символьним іменем. В обох випадках складене ім'я відображає ієрархічну структуру організації відповідних довідників – каталогів файлів або DNS-таблиць. Тут домен і доменний DNS-сервер є аналогом каталога файлової системи. Для доменних імен, так само як і для символьних імен файлів, характерна незалежність іменування від фізичного місця розташування.

Процедура пошуку адреси файлу за символьним іменем полягає в послідовному перегляді каталогів, починаючи з кореневого. При цьому попередньо перевіряються кеш і поточний каталог. Для визначення IP-адреси за доменним іменем також необхідно переглянути всі DNS-сервери, що обслуговують ланцюжок піддоменів, які входять в ім'я хоста, починаючи з кореневого домену.

Істотною відмінністю файлової системи від служби DNS є те, що перша розташована на одному комп'ютері, а друга за своєю природою є розподіленою. Існує дві основні схеми дозволу DNS-імен. У першому варіанті роботу з пошуку IP-адреси координує DNS-клієнт.

1. DNS-клієнт звертається до кореневого DNS-сервера із зазначенням повного доменного імені.

2. DNS-сервер відповідає клієнту, вказуючи адресу наступного DNS-сервера, який обслуговує домен верхнього рівня, заданий в наступній старшій частині запитаного імені.

3. DNS-клієнт робить запит наступного DNS-сервера, який відсилає його до DNS-сервера потрібного піддомену тощо, поки не буде знайдений DNS-сервер, в якому зберігається відповідність до запитаного імені IP-адреси. Цей сервер дає остаточну відповідь клієнту.

Така процедура дозволу імені називається нерекурсивною, коли клієнт сам ітераційно виконує послідовність запитів до різних серверів імен. Ця схема завантажує клієнта досить складною роботою, і вона застосовується рідко.

У другому варіанті реалізується рекурсивна процедура.

1. DNS-клієнт запитує локальний DNS-сервер, тобто той сервер, який обслуговує піддомен, якому належить ім’я клієнта.

2. Далі можливі два варіанти дій.

Якщо локальний DNS-сервер знає відповідь, то він відразу ж повертає його клієнту (це може статися, коли запитуване ім’я входить у той же піддомен, що й ім’я клієнта, або коли сервер вже дізнавався дану відповідність для іншого клієнта і зберіг його у своєму кеші).

Якщо локальний сервер не знає відповідь, то він виконує ітеративні запити до кореневого сервера тощо, точно так само, як це робив клієнт у попередньому варіанті, а отримавши відповідь, передає його клієнту, який весь цей час просто чекає її від свого локального DNS-сервера.

У цій схемі клієнт передоручає роботу своєму серверу, тому схема називається непрямою, або рекурсивною. Практично всі DNS-клієнти використовують рекурсивну процедуру.

Для прискорення пошуку IP-адрес DNS-сервери широко застосовують кешування (буферизацію) відповідей, що проходять через них. Щоб служба DNS могла оперативно опрацьовувати зміни, що відбуваються в мережі, відповіді кешуються на відносно короткий час – зазвичай від кількох годин до декількох днів.

Хід роботи

1. Винести на логічне поле комп’ютер, два сервери, комутатор 2950-24 та маршрутизатор 1841 (рисунок 5.27).

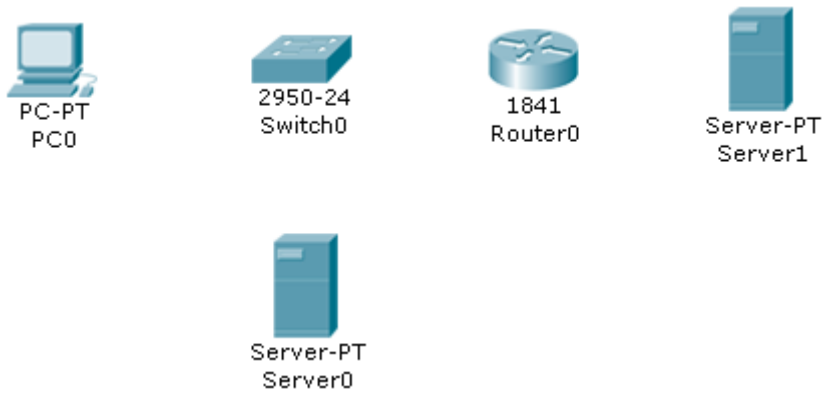


Рисунок 5.27 – Винесене на логічне поле обладнання

2. Виконати фізичне з'єднання, використовуючи інтерфейс Fast Ethernet: комп'ютер, перший сервер і маршрутизатор підключити до портів комутатора (у нашому випадку ці вузли будуть належати до локальної мережі), а другий сервер підключити до вільного порту маршрутизатора (другий сервер буде виконувати роль віддаленого Internet-сервера) (рисунок 5.28). Не варто забувати, що комутація сервера з маршрутизатором виконується перехресним кабелем.

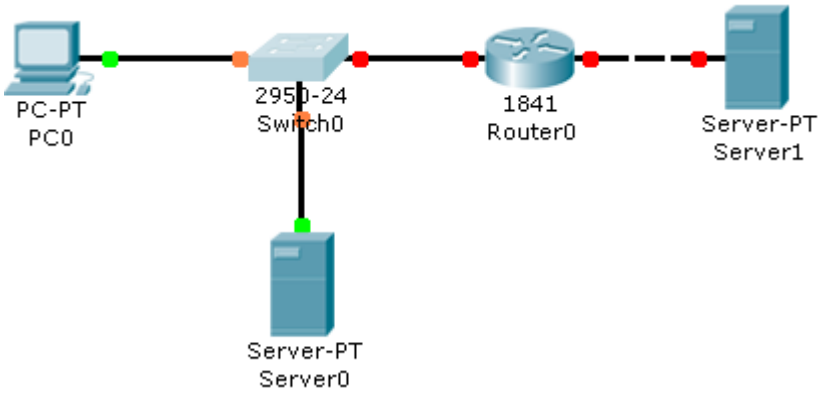


Рисунок 5.28 – Топологія мережі

3. Настроювання комп'ютера. Портові комп'ютера присвоїти IP-адресу 192.168.1.2. IP-адреса шлюзу – 192.168.1.1. У полі для введення IP-адреси DNS-сервера ввести адресу 192.168.1.3.

4. Настроювання локального сервера. IP-адреса порту – 192.168.1.3, IP-адреса шлюзу – 192.168.1.1.

5. Настроювання віддаленого сервера. IP-адреса порту – 198.168.1.2, IP-адреса шлюзу – 198.168.1.1.

6. Настроювання маршрутизатора. Порту, який має вихід у локальну мережу, присвоїти IP-адресу 192.168.1.1, а порту, який має вихід до віддаленого сервера, присвоїти IP-адресу 198.168.1.1. Не варто забувати, що порти Fast Ethernet після настроювання треба увімкнути.

7. Виконати пінгування усіх вузлів мережі.

8. Побудова DNS-сервера на основі локального сервера. Викликати вікно властивостей сервера. Перейти на вкладку Config. У групі SERVICES натиснути кнопку DNS. У правій частині вікна у полі для введення Name

ввести наступну HTTP-адресу: vstu.vinnica.ua (крапку у кінці не ставити). У полі для введення Address ввести IP-адресу сервера, який має прив'язку до вищевказаної HTTP-адреси. У нашому випадку це другий віддалений сервер. Відповідно IP-адреса, яку необхідно ввести, буде 198.168.1.2. Суть таких операцій полягає у тому, щоб сервер знав, яка пряма IP-адреса віддаленого сервера, на який подають запит через протокол HTTP.

9. Для перевірки роботи DNS-сервера необхідно відкрити вікно властивостей комп'ютера, перейти на вкладку Desktop та запустити термінал командного рядка Command Prompt. Там прописати таке:

ping vstu.vinnica.ua,

після чого відбувається пінгування:

Pinging 198.168.1.2 with 32 bytes of data:
Reply from 198.168.1.2: bytes=32 time=10ms TTL=127
Reply from 198.168.1.2: bytes=32 time=6ms TTL=127
Reply from 198.168.1.2: bytes=32 time=6ms TTL=127
Reply from 198.168.1.2: bytes=32 time=6ms TTL=127
Ping statistics for 198.168.1.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 10ms, Average = 7ms

Кількість отриманих (Recieved) пакетів має дорівнювати кількості відісланих (Sent). У такому випаду пінгування виконано успішно, і DNS-сервер, який перенаправляє запити на віддалений сервер, працює нормально.

10. Виконати таку перевірку для різної кількості пакетів.

Зміст звіту

1. Тема і мета роботи.
2. Короткий опис принципу роботи системи DNS.
3. Завдання до лабораторної роботи.
4. Знімки екрана із мережею, що містить DNS-сервер, та налаштуванням портів серверів та маршрутизатора.
5. Результати проведеного пінгування.

Контрольні запитання

1. Наведіть основні функції DNS.
2. Поясніть ієрархічну структуру DNS і структуру доменного імені.
3. Структура DNS запиту і відповіді.
4. Що таке рекурсивний запит?
5. Що таке віртуальний хостинг і балансування навантаження?
6. Що таке DNS- клієнт, DNS-сервер?
7. Типи серверів, назвіть число кореневих серверів.

Лабораторна робота № 7
Реалізація DHCP-сервера

Мета: навчитися налаштовувати DHCP-сервер в середовищі моделювання Packet Tracer 5.2.

Теоретичні відомості

Для нормальної роботи мережі кожному мережевому інтерфейсу комп'ютера і маршрутизатора повинна бути призначена IP-адреса. Процедура присвоєння адрес відбувається в ході конфігурування комп'ютерів і маршрутизаторів. Призначення IP-адрес може відбуватися вручну в результаті виконання процедури конфігурування інтерфейсу, наприклад, для комп'ютера − це заповнення системи екранних форм. При цьому адміністратор повинен пам'ятати, які адреси з наявної безлічі він вже використовував для інших інтерфейсів, а які ще вільні. При конфігуруванні окрім IP-адрес мережевих інтерфейсів (і відповідних масок) пристрою повідомляється ряд інших конфігурацій. При конфігуруванні адміністратор повинен призначити клієнту не тільки IP-адресу, але і інші параметри стека TCP/IP, необхідні для його ефективної роботи, наприклад маску та IP-адресу маршрутизатора за замовчуванням, IP-адресу сервера DNS, доменне ім'я комп'ютера тощо. Навіть при не дуже великому розмірі мережі ця робота являє для адміністратора складну процедуру.

Протокол динамічного конфігурування хостів (Dynamic Host Configuration Protocol, DHCP) автоматизує процес конфігурування мережевих інтерфейсів, гарантуючи від дублювання адрес за рахунок централізованого управління їх розподілом. Робота DHCP описана у документації RFC 2131 і 2132.

Режими DHCP. Протокол DHCP працює згідно 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 та деякі інші конфігураційні параметри. При цьому сервер DHCP може працювати в різних режимах: ручне призначення статичних адрес; автоматичне призначення статичних адрес; автоматичний розподіл динамічних адрес.

У всіх режимах роботи адміністратор при конфігуруванні DHCP-сервера повідомляє йому один або кілька діапазонів IP-адрес, причому всі ці адреси відносяться до однієї мережі, тобто мають одне і те ж значення в полі номера мережі.

У ручному режимі адміністратор, крім пулу доступних адрес, надає DHCP-серверу інформацію про чітку відповідність IP-адрес фізичним адресам або іншим ідентифікаторам клієнтських вузлів. DHCP-сервер, користуючись цією інформацією, завжди видає певному DHCP-клієнту одну і

ту саму призначену йому адміністратором IP-адресу (а також набір інших конфігураційних параметрів).

В режимі автоматичного призначення статичних адрес DHCP-сервер самостійно без втручання адміністратора довільним чином вибирає клієнту IP-адресу з пулу наявних IP-адрес. Адреса дається клієнту з пулу в постійне користування, тобто між ідентифікуючою інформацією клієнта та його IP-адресою, як і раніше, як і при ручному призначенні, існує постійна відповідність. Вона встановлюється в момент першого призначення DHCP-сервером IP-адреси клієнта. При всіх наступних запитах сервер повертає клієнтові ту ж саму IP-адресу.

При динамічному розподілі адрес DHCP-сервер видає адресу клієнту на обмежений час, званий строком оренди. Коли комп'ютер, який є DHCP-клієнтом, видаляється з підмережі, призначена йому IP-адреса автоматично звільняється. Коли комп'ютер підключається до іншої підмережі, то йому автоматично призначається нова адреса. Ні користувач, ні мережевий адміністратор не втручаються в цей процес.

Це дає можливість згодом повторно використовувати цю IP-адресу для призначення іншому комп'ютеру. Таким чином, крім основної переваги DHCP – автоматизації роботи адміністратора із конфігурацій стека TCP/IP на кожному комп'ютері, динамічне розділення адрес в принципі дозволяє будувати IP-мережу, кількість вузлів у якої перевищує кількість наявних у розпорядженні адміністратора IP-адрес.

Алгоритм динамічного призначення адрес

Адміністратор управляє процесом конфігурування мережі, визначаючи два основних параметри конфігурації DHCP-сервера: пул адрес, доступних для розподілення, і термін оренди. Термін оренди визначає, як довго комп'ютер може використовувати призначену IP-адресу, перед тим як знову запросити її від DHCP-сервера. Термін оренди залежить від режиму роботи користувачів мережі. Якщо це невелика мережа навчального закладу, куди зі своїми комп'ютерами приходять багаточисленні студенти для виконання лабораторних робіт, то термін оренди може бути рівний тривалості лабораторної роботи. Якщо ж це корпоративна мережа, в якій співробітники підприємства працюють на регулярній основі, то термін оренди може бути досить тривалим – кілька днів або навіть тижнів. DHCP-сервер повинен знаходитися в одній підмережі з клієнтами, враховуючи, що клієнти посилають йому широкомовні запити. Для зниження ризику виходу мережі з ладу через відмову DHCP-сервера у мережі іноді ставлять резервний DHCP-сервер (такий варіант відповідає мережі 1 на рисунку 5.29).

Іноді спостерігається і протилежна картина: в мережі немає ні одного DHCP-сервера, його підмінює зв'язковий DHCP-агент – програмне забезпечення, яке відіграє роль посередника між DHCP-клієнтами та DHCP-серверами (приклад такого варіанта – мережа 2 на рисунку). Зв'язковий агент переправляє запити клієнтів з мережі 2 DHCP-сервера мережі 3. Та-

ким чином, один DHCP-сервер може обслуговувати DHCP-клієнтів декількох різних мереж.

Нижче дана спрощена схема обміну повідомленнями між клієнтськими і серверними частинами DHCP (рисунок 5.29).

1. Коли комп'ютер вмикають, встановлений на ньому DHCP-клієнт посилає обмежене широкомовне повідомлення DHCP-пошуку (IP-пакет з адресою призначення, що складається з одних одиниць, який повинен бути доставлений до усіх вузлів даної IP-мережі).

2. DHCP-сервери, що знаходяться у мережі. отримують це повідомлення. Якщо в мережі DHCP-сервери відсутні, то повідомлення DHCP-пошуку отримує зв'язковий DHCP-агент. Він пересилає це повідомлення в іншу, можливо, значно віддалену від нього мережу DHCP-сервера, IP-адреса якого йому заздалегідь відома.

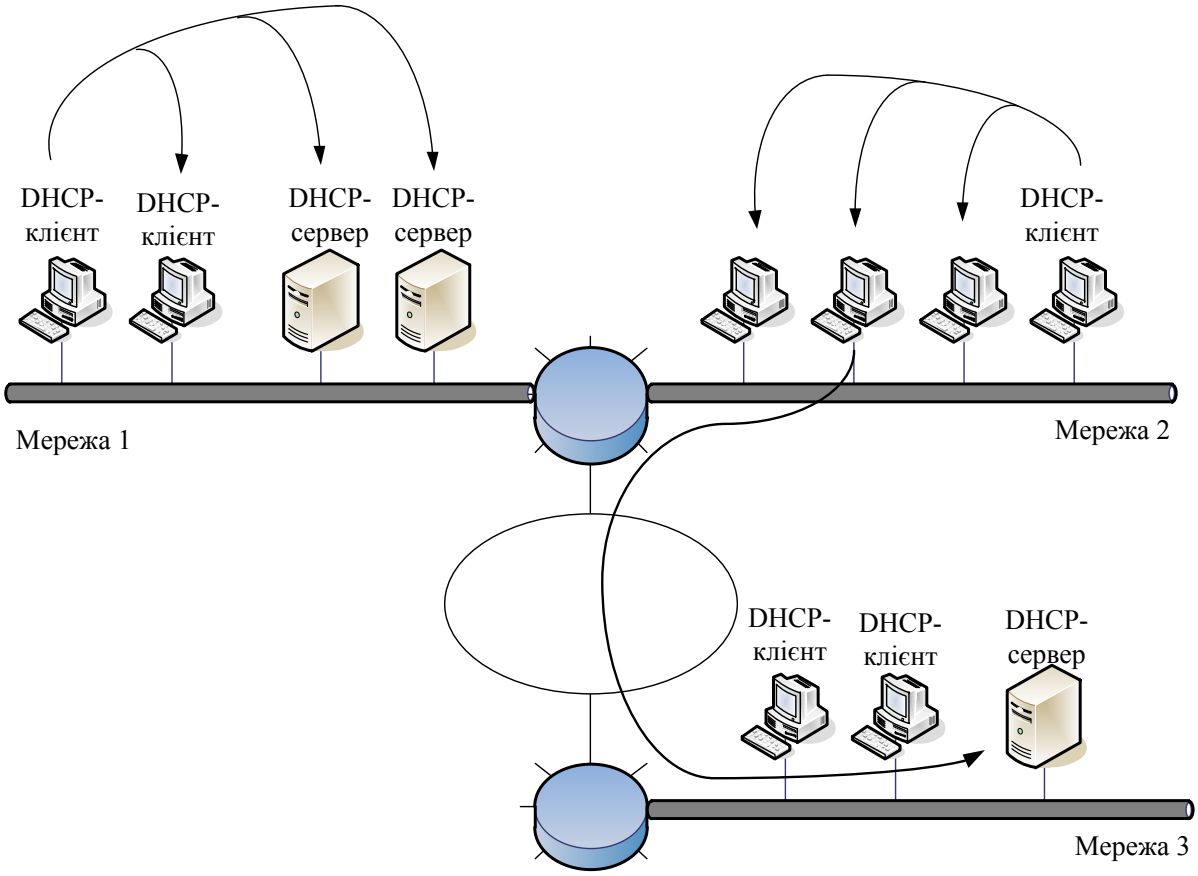


Рисунок 5.29 – Схема взаємного розташування DHCP-серверів та DHCP-клієнтів

3. Всі DHCP-сервери, що одержали повідомлення DHCP-пошуку, посилають DHCP-клієнтові, який звернувся із запитом, свої DHCP-пропозиції. Кожна пропозиція містить IP-адресу та іншу конфігураційну інформацію. (DHCP-сервер, що знаходиться в іншій мережі, посилає відповідь через агента.)

4. DHCP-клієнт збирає конфігураційні DHCP-пропозиції від усіх DHCP-серверів. Як правило, він вибирає першу із надійшовших пропозицій і відправляє в мережу широкомовний DHCP-запит. У цьому запиті містяться ідентифікаційна інформація про DHCP-сервер, пропозиція якого прийнята, а також значення прийнятих конфігураційних параметрів.

5. Всі DHCP-сервери отримують DHCP-запит, і тільки один вибраний DHCP-сервер посилає позитивну DHCP-квитанцію (підтвердження IP-запиту і параметрів оренди), а інші сервери анулюють свої запити, зокрема повертають у свої пули запропоновані адреси.

6. DHCP-клієнт отримує позитивну DHCP-квитанцію і переходить у робочий стан.

Час від часу комп'ютер намагається оновити параметри оренди у DHCP-сервера. Першу спробу він робить задовго до закінчення терміну оренди, звертаючись до того сервера, від якого він отримав поточні параметри. Якщо відповіді немає або відповідь негативна, він через деякий час знову надсилає запит. Так повторюється кілька разів, і, якщо всі спроби отримати параметри у того ж сервера виявляються безуспішними, клієнт звертається до іншого сервера. Якщо і другий сервер відповідає відмовою, то клієнт втрачає свої конфігураційні параметри і переходить в режим автономної роботи.

DHCP-клієнт може за своєю ініціативою достроково відмовитися від виділених йому параметрів.

У мережі, де адреси призначаються динамічно, не можна бути впевненим в адресі, яка на даний момент має той чи інший вузол. І така мінливість IP-адрес тягне за собою деякі проблеми.

По-перше, виникають складності при перетворенні символьного доменного імені в IP-адресу. З огляду на цю обставину, для серверів, до яких користувачі часто звертаються за символьними іменами, призначають статичні IP-адреси, залишаючи динамічні тільки для клієнтських комп'ютерів. Проте в деяких мережах кількість серверів настільки велика, що їх ручне конфігурування стає занадто обтяжливим. Це призвело до розробки вдосконаленої версії DNS (так званої динамічної системи DNS), в основі якої лежить узгодження інформаційної адресної бази в службах DHCP і DNS.

По-друге, важко здійснювати віддалене управління і автоматичний моніторинг інтерфейсу (наприклад, збір статистики), якщо як його ідентифікатор виступає динамічно мінлива IP-адреса.

Нарешті, для забезпечення безпеки мережі багато мережевих пристроїв можуть блокувати (фільтрувати) пакети, певні поля яких мають деякі заздалегідь задані значення. Іншими словами, при динамічному призначенні адрес ускладнюється фільтрація пакетів за IP-адресами.

Останні дві проблеми найпростіше вирішуються відмовою від динамічного призначення адрес для інтерфейсів, які використовуються в системах моніторингу та безпеки.

Хід роботи

1. Винести на логічне поле маршрутизатор 1841, комутатор 2950-24 та три комп'ютери.

2. Використовуючи порти Fast Ethernet, підключити маршрутизатор до комутатора, а комутатор до комп'ютерів (рисунок 5.30).

3. Настроювання маршрутизатора. Запустити вікно властивостей маршрутизатора, перейти у термінал.

Входження у режим налаштувань маршрутизатора:

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host r1
```

Присвоєння IP-адреси портові Fast Ethernet 0/0:

```
r1(config)#int fa 0/0
r1(config-if)#ip add 192.168.1.1 255.255.255.0
```

Увімкнення порту Fast Ethernet 0/0:

```
r1(config-if)#no shut
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
r1(config-if)#exit
```

Налаштування внутрішнього DHCP-сервера:

```
r1(config)#ip dhcp pool ip1
r1(dhcp-config)#net 192.168.1.0 255.255.255.0
```

Вказання, яка початкова адреса порту, з якого присвоюються IP-адреси клієнтам:

```
r1(dhcp-config)#default 192.168.1.1
r1(dhcp-config)#exit
```

Вказання виконувати роздачу IP-адрес, починаючи із 192.168.1.10 (виключно):

```
r1(config)#ip dhcp exc 192.168.1.1 192.168.1.10
r1(config)#exit
r1#
%SYS-5-CONFIG_I: Configured from console by console
```

Запис усіх змін із ОП маршрутизатора у його ПЗП:

```
r1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```

Вихід із налаштувань:

```
r1#exit
```

Закрити вікно властивостей маршрутизатора.

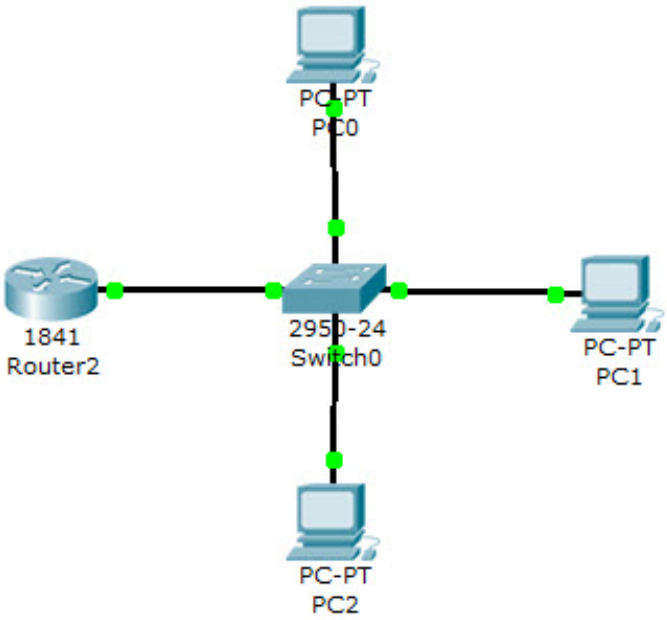


Рисунок 5.30 – DHCP-сервер на базі комутатора

4. Відкрити вікно властивостей одного із трьох комп'ютерів. Перейти на вкладку Desktop та запустити IP Configuration. У вікні IP Configuration перемкнути радіокнопку на DHCP та почекати кілька секунд, слідкуючи за появою у неактивних полях IP-адрес даного комп'ютера, вихідного шлюзу (адреси порту Fast Ethernet 0/0 маршрутизатора) та маски підмережі. Якщо IP-адреси не було присвоєно, прослідкувати, чи усі порти було ввімкнено і прослідкувати, чи правильно виконано налаштування маршрутизатора. Аналогічним чином прослідкувати роботу DHCP для інших двох комп'ютерів.

5. Винести на логічне поле два комп'ютери, два комутатори 2950-24, сервер та маршрутизатор 1841.

6. З'єднання між об'єктами виконувати, використовуючи порти Fast Ethernet. Один комп'ютер підключити до комутатора, комутатор до порту Fast Ethernet 0/1. Другий комп'ютер та сервер підключити до другого комутатора, а останній – до порту Fast Ethernet 0/0 маршрутизатора (рисунок 5.31).

7. Присвоїти серверу IP-адресу 192.168.1.10, маску – 255.255.255.0.

8. Налаштування DHCP-сервера для локальної мережі. Відкрити вікно властивостей сервера, перейти на вкладку Config. Серед списку служб SERVICES клацнути на службу DHCP. У правій частині вікна у текстовому полі Name надати запису назву Pool1, у полі Gateway прописати IP-адерсу шлюзу 192.168.1.1. У полі Start IP Address вказати 192.168.1.11, у Subnet Mask – 255.255.255.0. Maximum number of Users: 50. Після введення всіх даних натиснути кнопку Add, після чого запис збережеться на сервері.

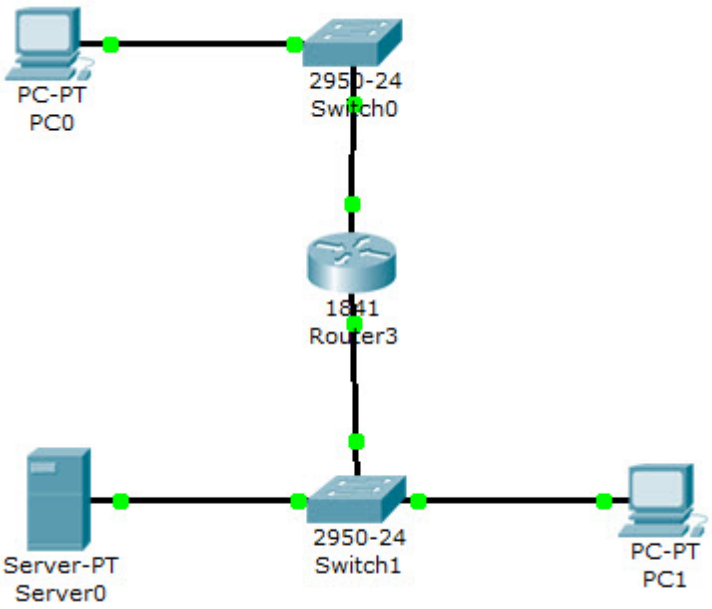


Рисунок 5.31 – Віддалений DHCP-сервер

9. Налаштування DHCP-сервера для віддаленої мережі. Не закриваючи вікна властивостей сервера, ввести параметри для такого запису: назва Pool198, IP-адреса шлюзу 192.168.2.1, Start IP Address – 198.168.1.11, Subnet Mask – 255.255.255.0, Maximum number of Users: 50. Після введення всіх даних натиснути кнопку Add.

У деяких модифікаціях пакета Packet Tracer у налаштуваннях DHCP-сервера є обліковий запис ServerPool, у ньому усі IP-адреси мають бути 0.0.0.0.

10. Налаштування маршрутизатора. Запустити вікно властивостей маршрутизатора, перейти у термінал.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#in fa 0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#ip helper-address 192.168.1.10
Router(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#int fa 0/1
Router(config-if)#ip add 192.168.2.1
% Incomplete command.
Router(config-if)#ip add 192.168.2.1 255.255.255.0
Router(config-if)#ip helper 192.168.1.10
```

Router(config-if)#no shut

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#net 192.168.1.0
Router(config-router)#net 192.168.2.0
Router(config-router)#exit
Router(config)#ip route 192.168.1.1 255.255.255.0 fa 0/0 1
Router(config)#ip route 192.168.2.1 255.255.255.0 fa 0/1 1
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#wr mem
Building configuration...
[OK]

11. Відкрити вікно властивостей комп'ютера віддаленої мережі. Перейти на вкладку Desktop та запустити IP Configuration. У вікні IP Configuration перемкнути радіокнопку на DHCP та почекати кілька секунд, слідкуючи за появою у неактивних полях IP-адрес даного комп'ютера, вихідного шлюзу (адреси порту Fast Ethernet 0/0 маршрутизатора) та маски підмережі. Якщо IP-адреси не було присвоєно, прослідкувати, чи усі порти було ввімкнено і прослідкувати, чи правильно виконано налаштування маршрутизатора. Аналогічним чином прослідкувати роботу DHCP для інших двох комп'ютерів.

Зміст звіту

1. Тема і мета роботи.
2. Короткий опис принципу роботи DHCP-сервера.
3. Завдання до лабораторної роботи.
4. Знімки екрана із мережею, що містить DHCP-сервер.
5. Знімки екрана із налаштуванням портів маршрутизатора, комутаторів та DHCP-сервера для локальної та віддаленої мережі.
6. Результати проведеного пінгування.

Контрольні запитання

1. Що таке пул-адреса? Нехай префіксна частина пулу складає 15 двійкових розрядів. Скільки адрес входить до пулу?
2. Назвіть три можливих способи розподілу IP-адрес.
3. Які відомі опції має протокол DHCP ?
4. Наведіть структуру повідомлень DHCP .
5. Поясніть 4 етапи роботи протоколу.

Лабораторна робота № 8
Технологія VLAN

Мета: навчитися будувати локальну мережу за технологією VLAN.

Теоретичні відомості:

VLAN *(Virtual Local Area Network – віртуальна локальна мережа)* – група пристроїв, що мають можливість взаємодіяти між собою безпосередньо на канальному рівні, хоча фізично при цьому вони можуть бути підключені до різних мережевих комутаторів. І навпаки, пристрої, що знаходяться в різних віртуальних мережах, невидимі один для одного на канальному рівні, навіть якщо вони підключені до одного комутатора, і зв'язок між цими пристроями можливий тільки на мережевому і більш високих рівнях [1].

У сучасних мережах VLAN – головний механізм для створення логічної топології мережі, що не залежить від її фізичної топології. Технологія VLAN використовується для скорочення широкомовного трафіка в мережі та має велике значення з точки зору безпеки, зокрема як засіб боротьби з мережевими атаками.

Спочатку комутатори не забезпечували можливість створення віртуальних локальних мереж, оскільки вони використовувалися для простого пересилання фреймів між пристроями. Ринок комутаторів почав швидко зростати, коли концентратори колективного доступу до середовища передачі даних (hubs) почали не справлятися зі зростаючими запитами на розширення смуги пропускання мережі у зв'язку з використанням додатків клієнт-сервер, що забезпечують графічний інтерфейс користувача (GUI).

Ключова різниця між комутатором і концентратором полягає в тому, як вони працюють з фреймами. Концентратор отримує фрейм, потім копіює і передає (повторює) фрейм у всі інші порти. У цьому випадку сигнал повторюється, в основному збільшуючи довжину мережевого сегмента до всіх підключених станцій. Комутатор повторює фрейм в усі порти крім того, з якого цей фрейм був отриманий: unicast фрейми (адресовані на конкретну MAC-адресу), broadcast фрейми, (адресовані для всіх MAC-адрес в локальному сегменті), і multicast фрейми (адресовані для набору пристроїв у сегменті). Це робить їх неприйнятними для великої кількості користувачів, оскільки кожна робоча станція і сервер, підключені до комутатора, повинні перевіряти кожен фрейм для того, щоб визначити, адресований цей фрейм їм чи ні. У великих мережах, з великою кількістю фреймів, які обробляються мережевим інтерфейсом, втрачається час роботи процесора. Це прийнятно для невеликих робочих груп, де передача даних має короткочасну природу.

Комутатор працює з фреймами таким чином, що він зчитує MAC-адресу вхідного фрейму і зберігає цю інформацію в таблиці комутації. Ця таблиця містить MAC-адреси і номери портів, пов'язаних з ними. Комута-

тор будує таблицю в розділеній пам'яті і тому він знає, яка адреса пов'язана з яким портом. Для прикладу, комутатори Cisco Catalyst створюють цю таблицю, перевіряючи кожен фрейм, що потрапив в пам'ять, і додають нові адреси, які не були занесені туди раніше. Маршрутизатори Cisco створюють цю таблицю, адресуючи її за вмістом (content-addressable memory). Ця таблиця оновлюється і будується кожного разу при включенні комутатора, але можливе настроювання таймера оновлення таблиці залежно від потреб користувача. На рисунку 5.32 зображено CAM таблицю комутатора [13].

У цьому прикладі стовпець VLAN посилається на номер VLAN, якому належить порт призначення. Стовпець Destination MAC посилається на MAC-адресу, виявлену в порту. Один порт може бути пов'язаний з декількома адресами MAC, тому варто перевіряти кількість MAC-адрес, яку може підтримувати комутатор. Destination Ports описує порт, з якого комутатор дізнався MAC-адресу.

VLAN	Destination MAC	Destination Ports or VCs
1	00-60-2f-9d-a9-00	3/1
1	00-b0-2f-9d-b1-00	3/5
1	00-60-2f-86-ad-00	5/12
1	00-c0-0c-0a-bd-4b	4/10

Рисунок 5.32 – Приклад таблиці комутації комутатора

Далі, комутатор перевіряє MAC-адресу призначення фрейму і одразу аналізує таблицю комутації. Якщо комутатор знайшов відповідну адресу, він копіює фрейм тільки в цей порт. Якщо він не може знайти адресу, він копіює фрейм в усі порти. Unicast фрейми посилаються на необхідні порти, тоді як multicast і broadcast фрейми передаються в усі порти.

Така комутація стала новою технологією, яка збільшує пропускну здатність і збільшує продуктивність, але насправді комутатори це високопродуктивні мости (bridges) з додатковими функціями. Комутація − це термін, що використовується в основному для опису мережевих пристроїв рівня 2 багаторівневої системи OSI, які переправляють фрейми, ґрунтуючись на MAC-адресі одержувача.

Два основні методи, які найчастіше використовуються виробниками для передачі трафіка, − це cut-through і store and forward.

Комутація cut-through зазвичай забезпечує менший час затримки, ніж store-and-forward тому, що в цьому режимі комутатор починає передачу фрейму в порт призначення ще до того, як було повністю отримано весь фрейм. Комутатору досить того, що він прочитав MAC-адреси відправника та одержувача, що знаходяться на початку Token Ring і Ethernet фреймів. Більшість cut-through комутаторів починає пересилання кадру, отримавши тільки перші 30 - 40 байт заголовка фрейму.

Store and forward копіює весь фрейм перед тим, як пересилати фрейм. Цей метод дає велику затримку, але має більше переваг. Можливості фільтрації, управління та контролю за потоком інформації є головними перевагами цього методу. Також неповні та пошкоджені фрейми не пересилаються, оскільки вони не є правильними фреймами. Комутатори повинні мати буферну пам'ять для читання і збереження фреймів під час прийняття рішення, що збільшує вартість комутатора.

Із поліпшенням технологій і поширення на даній технології, почали виникати VLAN. Фізична мережа може складатися з кінцевих станцій, пов'язаних маршрутизатором (або маршрутизаторами), які використовують одне фізичне з'єднання. VLAN – це логічне комбінування кінцевих станцій в одному сегменті на рівні 2 і рівні 3, які пов'язані безпосередньо, без маршрутизатора. Зазвичай користувачам, розділеним фізично, потрібен маршрутизатор для зв'язку з іншим сегментом. Комутатори з можливістю побудови VLAN спочатку були впроваджені в основних навчальних містечках і невеликих робочих групах. Спочатку комутація розроблялася із потребою, але зараз це є звичайною практикою впроваджувати комутатори та VLAN в стаціонарних системах.

Кожна робоча станція в VLAN (і тільки ці кінцеві станції) обробляють широкомовний трафік, що посилається іншим членам VLAN. Наприклад, робочі станції A, B, C і приєднані до VLAN 1. VLAN 1 складається з трьох комутаторів. Всі комутатори розташовані на різних поверхах і з'єднані між собою оптоволокном і пов'язані транковим протоколом. Робоча станція A приєднана з комутатором A, робоча станція B приєднана у комутатор B і робоча станція C приєднана у комутатор C. Якщо станція A посилає широкомовний пакет, станції B і C отримають цей фрейм, навіть якщо вони фізично приєднані до інших комутаторів. Робоча станція D приєднана у комутатор A, але оголошена в VLAN 2. Коли D посилає широкомовний пакет, станція A не побачить цей трафік, хоча вона знаходиться в тому ж фізичному комутаторі, але оскільки вона знаходиться не в тій же віртуальній мережі, комутатор не буде пересилати цей трафік на A. VLAN працюють на рівні 2, тому зв'язок між VLAN потребує прийняття рішень маршрутизації на рівні 3. Так само станції B і C не побачать трафік від станції D.

Віртуальні мережі (VLAN) надають такі переваги:

- контроль за широкомовним трафіком;
- функціональні робочі групи;
- підвищена безпека.

Контроль за широкомовним трафіком. На відміну від традиційних LAN, побудованих за допомогою маршрутизаторів чи мостів, VLAN може бути розглянуто як широкомовний домен з логічно налаштованими кордонами. VLAN пропонує більше свободи, ніж традиційні мережі. Ранні розробки були основані на фізичному обмеженні мереж, побудованих на основі концентраторів; в основному фізичні кордони сегмента мережі обмежувалися ефективною дальністю, на яку електричний сигнал міг пройти

від порту концентратора. Розширення сегментів мереж за ці межі потребувало використання повторювачів (repeaters), пристроїв, які посилювали і пересилали сигнал. VLAN дозволяє мати широкомовний домен незалежно від фізичного розміщення, середовища мережевого доступу, типу носія і швидкості передачі. Члени можуть розташовуватися там, де необхідно, а не там, де є спеціальне з'єднання з конкретним сегментом. VLAN збільшують продуктивність мережі, розміщуючи широкомовний трафік усередині маленьких і легко керованих логічних доменів. У традиційних мережах з комутаторами, які не підтримують VLAN, весь широкомовний трафік потрапляє в усі порти. Якщо використовується VLAN, весь широкомовний трафік обмежується окремим широкомовним доменом.

Функціональні робочі групи. Найфундаментальнішою перевагою технології VLAN є можливість створення робочих груп, ґрунтуючись на функціональності, а не на фізичному розташуванні або типі носія. Традиційно адміністратори групували користувачів функціонального підрозділу фізичним переміщенням користувачів, їх столів і серверів в загальний робочий простір, наприклад в один сегмент. Всі користувачі робочої групи мали однакове фізичне з'єднання для того, щоб мати перевагу високошвидкісного з'єднання з сервером. VLAN дозволяє адміністратору створювати, групувати і перегруповувати мережеві сегменти логічно, без зміни фізичної інфраструктури і від'єднання користувачів і серверів. Можливість легкого додавання, переміщення та зміни користувачів мережі – ключова перевага VLAN.

Підвищена безпека. VLAN також пропонує додаткові переваги для безпеки. Користувачі однієї робочої групи не можуть отримати доступ до даних іншої групи, тому що кожна VLAN це закрита, логічна група. Очевидно є інші вимоги для забезпечення повної безпеки, але VLAN може бути частиною загальної стратегії мережевої безпеки.

Коли VLAN оголошені для пристроїв, вони можуть бути легко і швидко змінені для додавання, переміщення або зміни користувача у міру потреби.

Мережі VLAN можуть бути визначені за:

- портом (найчастіше використовується);
- MAC-адресою (дуже рідко);
- ідентифікатором користувача User ID (дуже рідко);
- фіксованою адресою (рідко у зв'язку із зростанням використання DHCP).

VLAN, що базуються на номері порту, дозволяють визначити конкретний порт в VLAN. Порти можуть бути визначені індивідуально, за групами, рядами і навіть у різних комутаторах через транковий протокол. Це найбільш простий і часто використовуваний метод визначення VLAN. Таке найпоширеніше використання впровадження VLAN, побудоване на портах, коли робочі станції використовують протокол DHCP.

VLAN, що базуються на MAC-адресах, дозволяють користувачам знаходитися в тій же VLAN, навіть якщо користувач переміщується з одного місця на інше. Цей метод потребує, щоб адміністратор визначив MAC-адресу кожної робочої станції і потім вніс цю інформацію в комутатор. Цей метод може викликати великі труднощі при пошуку несправностей, якщо користувач змінив MAC-адресу. Будь-які зміни у конфігурації повинні бути узгоджені з мережевим адміністратором, що може викликати адміністративні затримки.

Віртуальні мережі, що базуються на мережевих адресах, дозволяють користувачам знаходитися в тій же VLAN, навіть коли користувач переміщається з одного місця на інше. Цей метод переміщує VLAN, пов'язуючи її з мережевою адресою рівня 3 робочої станції для кожного комутатора, до якого користувач підключений. Цей метод може бути дуже корисним в ситуації, коли важливою є безпека і коли доступ контролюється списками доступу в маршрутизаторах. Тому користувач VLAN може переїхати в іншу будівлю, але залишитися підключеним до тих же пристроїв тому, що у нього залишилася та сама мережева адреса. Мережа, побудована на мережевих адресах, може потребувати комплексного підходу при пошуку несправностей.

Хід роботи

1. Винести на логічне поле маршрутизатор 1841, комутатор 2950-24 та чотири комп'ютери.

2. Використовуючи порти комутатор Fast Ethernet 0/2 – 0/5, підключити комп'ютери до комутатора, а порт Fast Ethernet 0/1 комутатора – до порту Fast Ethernet 0/0 маршрутизатора (рисунок 5.33).

3. Двом комп'ютерам, підключеним до портів маршрутизатора Fast Ethernet 0/2 та0/3, присвоїти IP-адреси 192.168.2.10 та 192.168.2.11, відповідно. Маска підмережі 255.255.255.0, зовнішній шлюз – 192.168.2.1.

4. Іншим двом комп'ютерам, підключеним до портів маршрутизатора Fast Ethernet 0/4 та0/5, присвоїти IP-адреси 192.168.3.10 та 192.168.3.11, відповідно. Маска підмережі 255.255.255.0, зовнішній шлюз – 192.168.3.1.

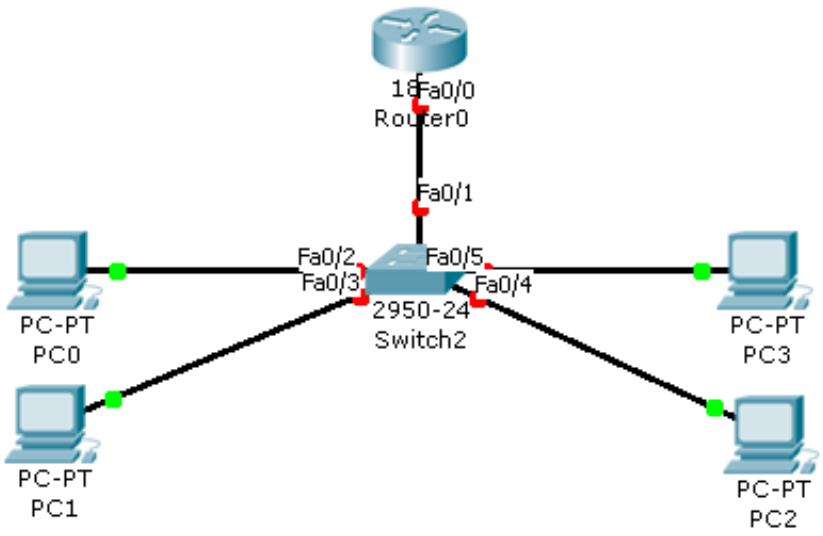


Рисунок 5.33 – Топологія віртуальної локальної мережі

5. Налаштування комутатора. Відкрити вікно властивостей комутатора та відкрити його термінал. Налаштувати комутатор, вводячи такі команди:

Switch>enable
Switch#vlan database
Switch(vlan)#vlan 10 name a
Switch(vlan)#vlan 20 name b
Switch(vlan)#exit
Switch#conf t
Switch(config)#int fa 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa 0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int fa 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#end
Switch(config)#int fa 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#end

6. Налаштування маршрутизатора. Відкрити вікно властивостей маршрутизатора та відкрити його термінал. Налаштувати комутатор, вводячи такі команди:

Router>enable
Router #config

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa 0/0
Router(config-if)#no shut
Router(config-if)#int fa 0/0.1
Router(config-subif)#encapsulation dot1q 1
Router(config-subif)#ip add 192.168.1.1 255.255.255.0
Router(config-subif)#int fa 0/0.2
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip add 192.168.2.1 255.255.255.0
Router(config-subif)#int fa 0/0.3
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip add 192.168.3.1 255.255.255.0
Router(config-subif)#end
```

7. Виконати пінгування між усіма комп'ютерами.

Зміст звіту

1. Тема і мета роботи.
2. Короткий опис технології VLAN.
3. Завдання до лабораторної роботи.
4. Знімки екрана із віртуальною локальною мережею та налаштуванням портів маршрутизатора та комутатора через командний рядок.
5. Результати проведеного пінгування.

Контрольні запитання

1. Назвіть причини і методи побудови VLAN .
2. Як будується VLAN на одному комутаторі?
3. Поясніть принцип дії і побудову комутатора, назвіть його відмінності від маршрутизатора.
4. Яким чином можна побудувати VLAN на декількох комутаторах? Назвіть недоліки цього методу.
5. Яким чином мережа розбивається на декілька VLAN?
6. Як при необхідності можна об'єднати між собою окремі VLAN?
7. Як різні специфікації стандарту 802.x впливають на якість обслуговування VLAN?

Лабораторна робота № 9
Система радіодоступу

Мета: промоделювати систему радіодоступу в середовищі моделювання Packet Tracer 5.2.

Теоретичні відомості

У комп'ютерних системах взагалі під системами радіодоступу розуміють мережеві системи типу Wireless LAN (англ. Wireless Local Area Network; WLAN) - безпроводова локальна обчислювальна мережа [14].

Для розробки стандартів безпроводових локальних комп'ютерних мереж (WLAN) в 1989 р. створена робоча група (комітет) Інституту інженерів електротехніки та радіоелектроніки США IEEE 802.11. Метою групи була розробка архітектури безпроводових мереж WLAN і специфікацій канального та фізичного рівнів, що забезпечують швидкості передачі даних в каналі 1 Мбіт/с і вище [7].

Структура системи передбачає наявність у своєму складі точок доступу (ТД) до проводової мережі загального користування та великої кількості абонентських станцій, між якими забезпечується безпроводовий зв'язок, і які можуть зв'язуватися з абонентами провідної мережі через точки доступу.

Стандарт визначає специфікації двох рівнів моделі OSI: фізичний рівень і канальний рівень в частині управління середовищем доступу (MAC). Точки доступу забезпечують взаємодію по радіоканалу з абонентськими станціями через радіоінтерфейс стандарту 802.11 і взаємодію з мережею передачі даних загального користування по одному з протоколів. Точка доступу в загальному випадку може бути подана як безпроводовий міст, який підключається через комутатор до загальної мережі.

Кожна точка доступу забезпечує покриття деякого простору, званого зоною обслуговування. Радіус зони обслуговування залежить від параметрів фізичного рівня. Точка доступу в стандарті 802.11 формується на базі абонентської станції за рахунок спеціального програмного забезпечення, що реалізує взаємодію з логікою комутатора або моста локальної мережі, яка організовує розподільну мережу, яка підключається до проводової локальної мережі через маршрутизатор або міст.

Мережа стандарту 802.11 підтримує базові служби для можливості сумісності з проводовою локальною мережею. Перш за все, це служби, що забезпечують взаємодію комп'ютерів, підключених до безпроводової мережі на MAC-рівні з локальною мережею, і служби, які вирішують задачі аутентифікації, безпеки та конфіденційності.

Рівень MAC-стандарту 802.11 реалізує доставку даних, управління доступом за фізичним рівнем і безпеку передачі даних.

Стандарти WLAN. Визначаючи різні аспекти взаємодії безпроводових продуктів, стандарти містять детальні вимоги до фізичного і MAC-

рівня безпроводових локальних мереж у діапазоні 2,4 ГГц і вище для промислових, наукових і медичних цілей. На фізичному рівні стандарти передбачають два радіочастотних методи передачі: метод прямої послідовності розмитого спектра (Direct Sequence Spread Spectrum, DSSS) і метод змінної частоти розмитого спектра (Frequency Hopping Spread Spectrum, FHSS), а також інфрачервоний зв'язок. На MAC-рівні стандарт використовує різновид методу доступу CSMA/CD із запобіганням колізій під назвою CSMA/CA.

Слід відзначити особливості існуючих промислових стандартів.

IEEE 802.11 був прийнятий у 1997. Він визначає протокол роботи мережі в двох режимах: радіоканалу (режим adhoc – прямий доступ кожного абонента один до одного) і роботу мережі клієнта-сервера 802.11 (через точку доступу)

У режимі мережі adhoc всі абоненти мають рівноправний доступ до загального каналу передач. Робота забезпечується без головної станції-сервера, тобто всі абоненти мають прямий доступ один до одного.

У режимі мережі клієнт - сервер (прийнято називати "режим інфраструктури" – infrastructure mode) трафік віддалених станцій проходить через точку доступу. Це блок, що складається з приймача і передавача та інтерфейсу з проводовою LAN. Виконує роль моста між безпроводовою та проводовою мережами. IEEE 802.11 допускає максимальну швидкість 2 Мбіт/с.

IEEE 802.11b – 11 Мбіт/с. Цей стандарт з'явився в 1999 році. В основному використовується діапазон 2.4 GHz (ISM band) на якому можлива передача даних зі швидкістю до 11 Мбіт/с. Також така швидкість передачі можлива у діапазонах 1, 2, 5,5 та 11 Мбіт/с.

Для збільшення швидкості передачі використовується більш досконала техніка модуляції Complementary Code Keying (CCK) – модуляція за допомогою додаткового коду. Тут замість стандартного коду, що визначає формат поля даних, застосовується послідовність кодів, так званих додаткових (Complementary Sequences). Це додає до символу ще два біти. Символи посилаються зі швидкістю 1,375 Мбіт/с, що і дає в результаті пропускну здатність 11 Мбіт/с.

IEEE 802.11a – 54 Мбіт/с прийнятий і ратифікований IEEE комітетом у вересні 2001 року. Використовується діапазон 5 ГГц на неліцензованій ділянці (ISM band). Використовується ортогональне мультиплексування поділу частоти (OFDM). Можлива передача даних на швидкості 6, 9, 12, 18, 24, 36, 48 та 54 Мбіт/с. Регламентовано обов'язкові, стандартні ряди швидкостей 6, 12 і 24 Мбіт/с. Системи використовують 52 підносійні, які модулюються за допомогою двійково-квадратурної фазової модуляції, 16-квадратурної амплітудної або 64-квадратурної амплітудної модуляції (QAM).

Стандарт 802.11g є розвитком 802.11b і передбачає передачу даних в тому ж частотному діапазоні. Крім того, стандарт 802.11g повністю суміс-

ний з 802.11b, тобто будь-який пристрій 802.11g повинен підтримувати роботу з пристроями 802.11b. У той же час, за способом кодування 802.11g є гібридом стандартів 802.11b і 802.11a. Максимальна швидкість передачі в стандарті 802.11g становить 54 Мбіт/с (як і в стандарті 802.11a), тому на сьогоднішній день це найбільш перспективний стандарт безпроводового зв'язку. Проте максимальні його значення досягаються лише при дуже невеликій відстані: якщо при використанні 802.11b на відкритій місцевості можна отримати 11 Мбіт/с на відстані до 300 м, то у випадку 802.11g передача зі швидкістю 54 Мбіт / с можлива, тільки коли пристрої віддалені один від одного не більше ніж на кілька метрів.

При розробці стандарту 802.11g розглядалися дві конкуруючі технології: метод ортогонального частотного поділу OFDM, запозичений зі стандарту 802.11a і запропонований до розгляду компанією Intersil, та метод двійкового пакетного згорткового кодування PBCC, реалізований у стандарті 802.11b і запропонований компанією Texas Instruments. У результаті стандарт 802.11g містить компромісне рішення: як базові застосовуються технології OFDM і CCK, а за вимогою передбачено використання технології PBCC.

На MAC-рівні визначаються два основних типи архітектури мереж Ad Hoc та Infrastructure Mode.

У режимі Ad Hoc, який називають Independent Basic Service Set (IBSS) або режимом Peer to Peer (точка-точка), станції безпосередньо взаємодіють одна з одною. Для цього режиму потрібно мінімум обладнання: кожна станція повинна бути оснащена безпроводовим адаптером. При такій конфігурації немає потреби створення мережевої інфраструктури. Основним недоліком Ad Hoc є обмежений діапазон дії можливої мережі і неможливість підключення до зовнішньої мережі (наприклад, до Інтернет).

Для повнішого розуміння роботи безпроводових пристроїв розглянемо технології розширеного спектра.

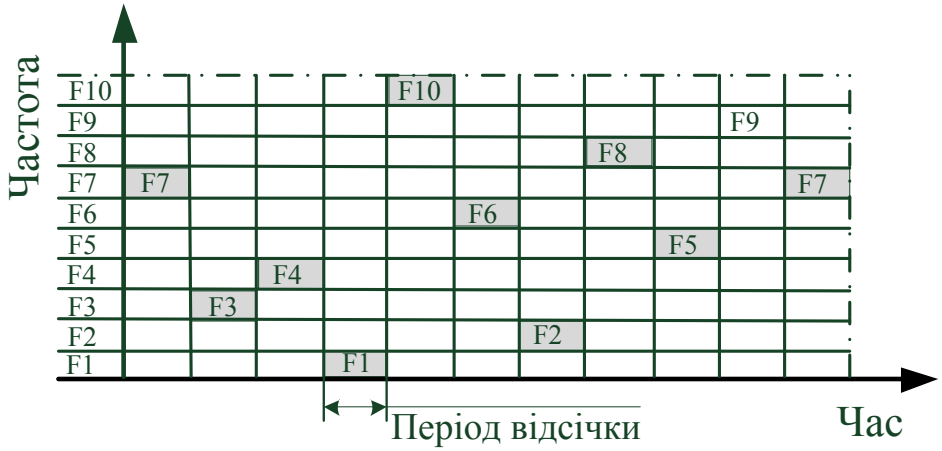
Технологія розширеного спектра

Спочатку метод розширеного спектра створювався для розвідувальних і військових цілей. Основна ідея методу полягає в тому, щоб розподілити інформаційний сигнал по широкій смузі радіодіапазону, що у результаті дозволить значно ускладнити приглушення або перехоплення сигналу. Перша розроблена схема розширеного спектра відома як метод перебудови частоти. Сучаснішою схемою розширеного спектра є метод прямого послідовного розширення. Обидва методи використовуються в різних стандартах і продуктах безпроводового зв'язку.

Розширення спектра стрибкоподібною перебудовою частоти *(Frequency Hopping Spread Spectrum - FHSS).*

Для того, щоб радіообмін не можна було перехопити або приглушити вузькосмуговим шумом, було запропоновано вести передачу з постійною зміною, що несе в межах широкого діапазону частот. В результаті потужність сигналу розподілялася по всьому діапазону, і прослуховування якоїсь

певної частоти давало тільки невеликий шум. Послідовність несучих частот була псевдовипадковою, відомою тільки передавачу і приймачу. Спроба приглушення сигналу в якомусь вузькому діапазоні також не дуже погіршувала сигнал, оскільки приглушувалась тільки невелика частина інформації. Ідею цього методу ілюструє рисунок 5.34. Протягом фіксованого інтервалу часу передача ведеться на незмінній несучій частоті. На кожній несучій частоті для передачі дискретної інформації застосовуються стандартні методи модуляції, такі як FSK або PSK. Для того, щоб приймач синхронізувався з передавачем, для позначення початку кожного періоду передачі протягом деякого часу передаються синхробіти. Отже, корисна швидкість цього методу кодування виявляється менша через постійні накладні витрати на синхронізацію.



Послідовність перестроювання частот F7-F3-F4-F1-F10-F6-F2-F8-F5-F9-F7

Рисунок 5.34 − Розширення спектра стрибкоподібною перебудовою частоти

Несуча частота змінюється відповідно до номерів частотних підканалів, псевдовипадкових чисел, що виробляються алгоритмом. Псевдовипадкова послідовність залежить від деякого параметра, який називають ***початковим*** числом. Якщо приймачу і передавачу відомі алгоритм і значення початкового числа, то вони змінюють частоти в однаковій послідовності, званою послідовністю псевдовипадкової перебудови частоти.

Пряме послідовне розширення спектра *(Direct Sequence Spread Spectrum - DSSS).*

У методі прямого послідовного розширення спектра також використовується частотний діапазон, виділений для однієї безпроводової лінії зв'язку. На відміну від методу FHSS, частотний діапазон займається не за рахунок постійних перемикань з частоти на частоту, а за рахунок того, що кожен біт інформації замінюється N-бітами так, що тактова швидкість передачі сигналів збільшується в N разів. А це, у свою чергу, означає, що спектр сигналу також розширюється в N разів. Достатньо відповідним чином вибрати швидкість передачі даних і значення N, щоб спектр сигналу

заповнив весь діапазон. Мета кодування методом DSSS та ж, що і методом FHSS, - підвищення стійкості до перешкод. Вузькосмугова перешкода спотворюватиме тільки певні частоти спектра сигналу, так що приймач з великим ступенем вірогідності зможе правильно розпізнати передавану інформацію.

Код, яким замінюється двійкова одиниця початкової інформації, називається ***розширювальною послідовністю***, а кожен біт такої послідовності - чіпом. Відповідно швидкість передачі результуючого коду називають чіповою швидкістю. Двійковий нуль кодується інверсним значенням розширювальної послідовності. Приймачі повинні знати розширювальну послідовність, яку використовує передавач, щоб зрозуміти передавану інформацію. Кількість бітів в розширювальній послідовності визначає коефіцієнт розширення початкового коду. Як і у разі FHSS, для кодування бітів результуючого коду може використовуватися будь-який вид модуляції, наприклад BFSK. Чим більший коефіцієнт розширення, тим ширший спектр результуючого сигналу і вищий ступінь приглушення перешкод. Але при цьому росте займаний каналом діапазон спектра. Зазвичай коефіцієнт розширення має значення від 10 до 100.

Дуже часто як значення розширювальної послідовності беруть послідовність Баркера (Barker), яка складається з 11 бітів: `10110111000`. Якщо передавач використовує цю послідовність, то передача трьох бітів `110` веде до передачі таких бітів: `10110111000 10110111000 01001000111`. Послідовність Баркера дозволяє приймачу швидко синхронізуватися з передавачем, тобто надійно виявляти початок послідовності. Приймач визначає таку подію, по черзі порівнюючи отримувані біти із зразком послідовності.

Безпроводові локальні мережі DSSS використовують канали шириною 22 Мгц, завдяки чому багато WLAN можуть працювати в одній і тій же зоні покриття. У Північній Америці і більшій частині Європи, у тому числі і в Росії, канали шириною 22 МГц дозволяють створити в діапазоні 2,4-2,473 ГГц три канали передачі, що не перекриваються. Ці канали показані на рисунку 5.35.

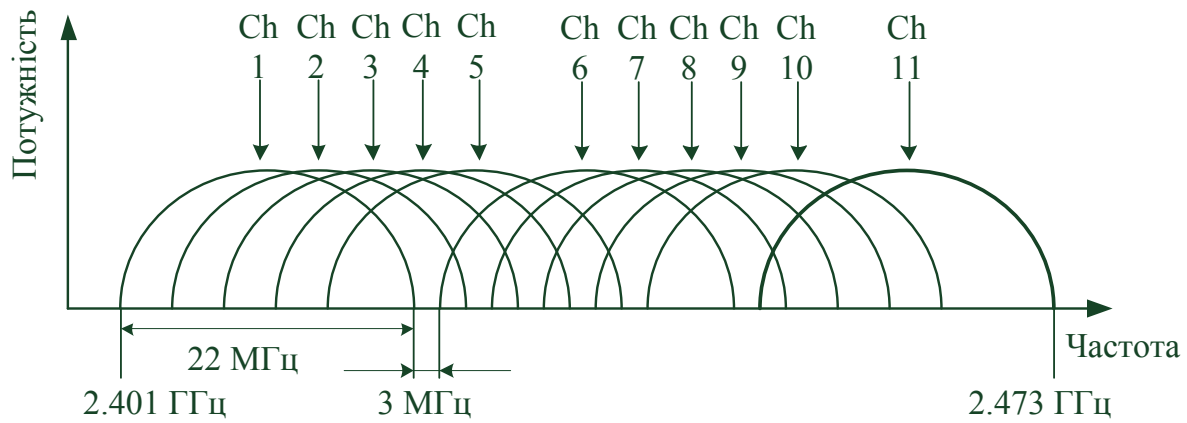


Рисунок 5.35 − Канали, що використовуються в технології DSSS

Рівень доступу до середовища стандарту 802.11

У мережах 802.11 рівень MAC забезпечує два режими доступу до середовища, що розділяється :

- розподілений режим DCF (Distributed Coordination Function);
- централізований режим PCF (Point Coordination Function).

1. Розподілений режим доступу DCF

Розглянемо спочатку як забезпечується доступ в розподіленому режимі DCF. У цьому режимі реалізується метод *множинного доступу з контролем несучої частоти і запобіганням колізіям* (Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA). Замість неефективного в безпроводових мережах прямого розпізнавання колізій за методом CSMA/CD тут використовується їх непряме виявлення. Для цього кожен переданий кадр повинен підтверджуватися кадром позитивної квитанції, що посилається станцією призначення. Якщо ж після закінчення обумовленого тайм-ауту квитанція не поступає, станція-відправник вважає, що відбулася колізія. Режим доступу DCF потребує синхронізації станцій. У специфікації 802.11 ця проблема вирішується достатньо елегантно − тимчасові інтервали починають відлічуватися від моменту закінчення передачі чергового кадру (рисунок 5.36). Це не потребує передачі будь-яких спеціальних синхронізуючих сигналів і не обмежує розмір пакета розміром слота передати кадр, зобов’язана заздалегідь прослуховувати середовище. Стандарт IEEE 802.11 передбачає два механізми контролю активності в каналі (виявлення несучої частоти): фізичний і віртуальний. Перший механізм реалізований на фізичному рівні і зводиться до визначення рівня сигналу в антені і порівняння його з пороговою величиною. Віртуальний механізм виявлення оснований на тому, що в передаваних кадрах даних, а також в кадрах, що управляють, міститься інформація про час, необхідний для передачі пакета (або групи пакетів) і отримання підтвердження. Всі пристрої мережі отримують інформацію про поточну передачу і можуть визначити, скільки часу канал буде зайнятий, тобто пристрій при встановленні зв’язку повідомляє всіх, на який час він резервує канал. Як тільки станція фіксує закінчення передачі кадру, вона зобов’язана відлічити інтервал часу, рівний міжкадровому інтервалу (IFS). Якщо після закінчення IFS середовище все ще вільне, починається відлік слотів фіксованої тривалості. Кадр можна передавати тільки на початку будь-якого зі слотів за умови, що середовище вільне. Станція вибирає для передачі слот на підставі зрізаного експоненціального двійкового алгоритму відстрочення, аналогічного використовуваному в методі CSMA/CD. Номер слота вибирається як випадкове ціле число, рівномірно розподілене в інтервалі `[0, CW]`, де "CW" означає "Contention Window" (конкурентне вікно).

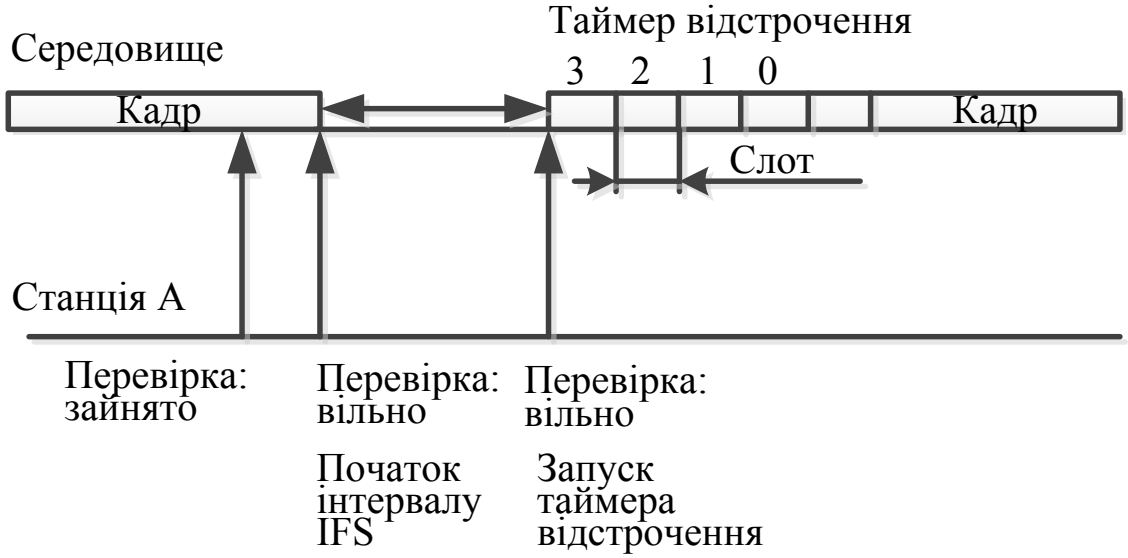


Рисунок 5.36 − Режим доступу DCF

Розглянемо цей метод доступу на прикладі рис. 5.36. Нехай станція А вибрала для передачі на підставі зрізаного експоненціального двійкового алгоритму відстрочки слот 3. При цьому вона присвоює таймеру відстрочення (призначення якого буде ясне з подальшого опису) значення 3 і починає перевіряти стан середовища на початку кожного слота. Якщо середовище вільне, то із значення таймера відстрочення віднімається 1, і якщо результат рівний нулю, починається передача кадру. Таким чином, забезпечується умова незайнятості всіх слотів, включаючи вибраний. Ця умова є необхідною для початку передачі. Якщо ж на початку будь-якого слота середовище виявляється зайнятим, то віднімання одиниці не відбувається, і таймер "заморожується". В цьому випадку станція починає новий цикл доступу до середовища, змінюючи тільки алгоритм вибору слота для передачі. Як і в попередньому циклі, станція стежить за середовищем і при її звільненні робить паузу протягом міжкадрового інтервалу. Якщо середовище залишилося вільним, то станція використовує значення "замороженого" таймера як номер слота і виконує описану вище процедуру перевірки вільних слотів з відніманням одиниць, починаючи із замороженого значення таймера відстрочення. Розмір слота залежить від способу кодування сигналу; так, для методу FHSS розмір слота рівний 28 мкс, а для методу DSSS - 1 мкс. Розмір слота вибирається так, щоб він перевершував час розповсюдження сигналу між будь-якими двома станціями мережі плюс час, що витрачається станцією на розпізнавання зайнятості середовища. Якщо така умова дотримується, то кожна станція мережі зуміє правильно розпізнати початок передачі кадру при прослуховуванні слотів, передуючих вибраному нею для передачі слоту. Це, у свою чергу, означає, що колізія може мати місце тільки у тому випадку, коли декілька станцій вибирають один і той же слот для передачі. В цьому випадку кадри спотворюються, і квитанції від станцій призначення не приходять. Не отримавши протягом певного часу квитанцію, відправники фіксують факт колізії і намагаються пере-

дати свої кадри знову. При кожній повторній невдалій спробі передачі кадру інтервал [0, CW], з якого вибирається номер слота, подвоюється. Якщо, наприклад, початковий розмір вікна вибраний рівним 8 (тобто CW = 7), то після першої колізії розмір вікна повинен бути рівний 16 (CW = 15), після другої послідовної колізії - 32 і т. д. Початкове значення CW, відповідно до стандарту 802.11, повинне вибиратися залежно від типу фізичного рівня, використовуваного в безпроводовій локальній мережі. Як і в методі CSMA/CD, в даному методі кількість невдалих спроб передачі одного кадру обмежена, але стандарт 802.11 не дає точного значення цієї верхньої межі. Коли верхня межа в N спроб досягнута, кадр відкидається, а лічильник послідовних колізій встановлюється в нуль. Цей лічильник також встановлюється в нуль, якщо кадр після деякої кількості невдалих спроб все ж таки передається успішно. У безпроводових мережах можлива ситуація, коли два пристрої (A і B) видалені і не чують один одного, проте обидва потрапляють в зону охоплення третього пристрою C (рисунок 5.37) - так звана проблема прихованого термінала. Якщо обидва пристрої A і B почнуть передачу, то вони принципово не зможуть виявити конфліктну ситуацію і визначити, чому пакети не проходять.

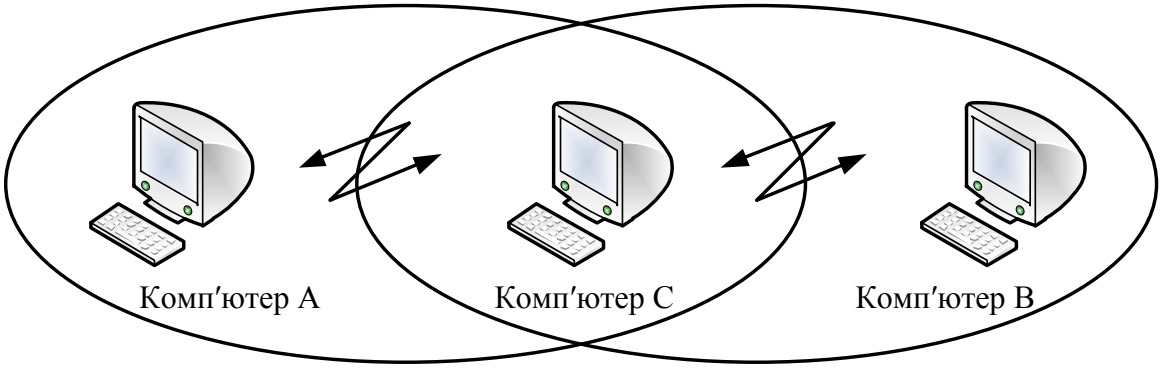


Рисунок 5.37 − Проблема прихованого термінала

У режимі доступу DCF застосовуються заходи для усунення ефекту прихованого терміналу. Для цього станція, яка хоче захопити середовище і відповідно до описаного алгоритму починає передачу кадру в певному слоті, замість кадру даних спочатку посилає станції призначення короткий службовий кадр RTS (Request To Send - запит на передачу). На цей запит станція призначення повинна відповісти службовим кадром CTS (Clear To Send - вільна для передачі), після чого станція-відправник посилає кадр даних. Кадр CTS повинен оповістити про захоплення середовища ті станції, які знаходяться поза зоною сигналу станції-відправника, але в зоні досяжності станції-одержувача, тобто є прихованими терміналами для станції-відправника. Максимальна довжина кадру даних 802.11 рівна 2346 байт, довжина RTS-кадру − 20 байт, CTS-кадру − 14 байт. Оскільки RTS- і CTS-кадри набагато коротші, ніж кадр даних, втрати даних в результаті колізії RTS- або CTS-кадрів значно менші, чим при колізії кадрів даних.

При перешкодах іноді трапляється, що втрачаються великі фрейми даних, тому можна зменшити довжину цих фреймів шляхом *фрагментації*. Фрагментація фрейма − це виконувана на рівні MAC функція, призначення якої − підвищити надійність передачі фреймів через безпроводове середовище. Під фрагментацією розуміється дроблення фрейма на менші фрагменти і передача кожного з них окремо (рис. 5.38). Передбачається, що вірогідність успішної передачі меншого фрагмента через зашумлене безпроводове середовище вища. Отримання кожного фрагмента фрейма підтверджується окремо; отже, якщо будь-який фрагмент фрейма буде переданий з помилкою або вступить в колізію, передавати повторно доведеться тільки його, а не весь фрейм. Це збільшує пропускну спроможність середовища. Розмір фрагмента може задавати адміністратор мережі. Фрагментації піддаються тільки одноадресні фрейми. Широкомовні або багатоадресні фрейми передаються цілком. Крім того, фрагменти фрейма передаються пакетом, з використанням тільки однієї ітерації механізму доступу до середовища DCF.

Хоча за рахунок фрагментації можна підвищити надійність передачі фреймів в безпроводових локальних мережах, вона приводить до збільшення "накладних витрат" MAC-протоколу стандарту 802.11. Кожен фрагмент фрейма включає інформацію, що міститься в заголовку 802.11 MAC, а також потребує передачі відповідного фрейма підтвердження. Це збільшує число службових сигналів MAC-протоколу і знижує реальну продуктивність безпроводової станції. Фрагментація − це баланс між надійністю і непродуктивним завантаженням середовища.

2. Централізований режим доступу PCF

У тому випадку, коли в мережі є станція, яка виконує функції точки доступу, може також застосовуватися централізований режим доступу PCF, що забезпечує пріоритетне обслуговування трафіка. В цьому випадку говорять, що точка доступу відіграє роль арбітра середовища. Режим доступу PCF в мережах 802.11 співіснує з режимом DCF. Обидва режими координуються за допомогою трьох типів міжкадрових інтервалів (рисунок 5.38).

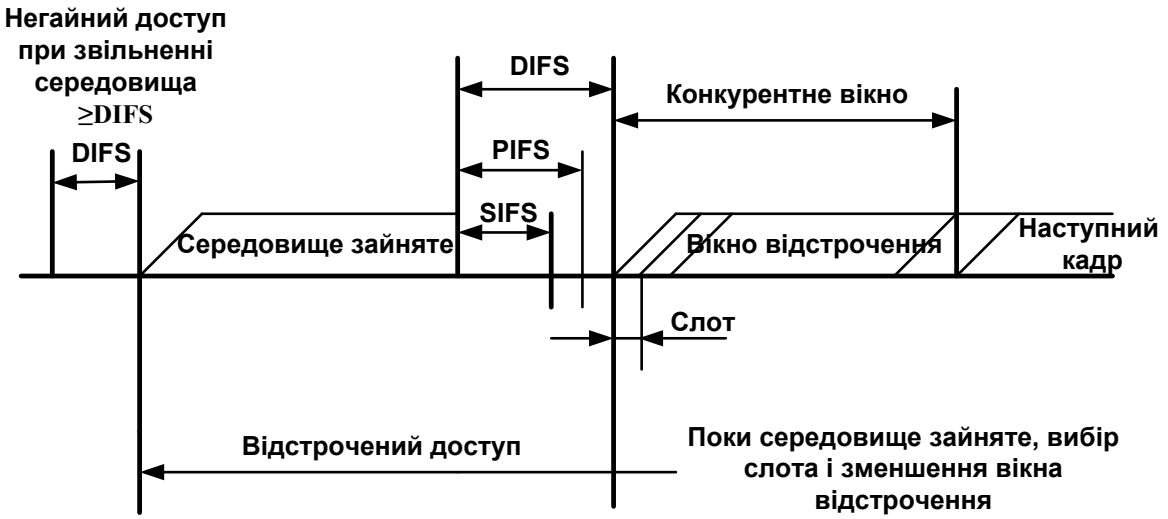


Рисунок 5.38 − Співіснування режимів PCF і DCF

Після звільнення середовища кожна станція відлічує час простою середовища, порівнюючи його з трьома значеннями:

– короткий міжкадровий інтервал (Short IFS - SIFS);

– міжкадровий інтервал режиму PCF (PIFS);

– міжкадровий інтервал режиму DCF (DIFS).

Захоплення середовища за допомогою розподіленої процедури DCF можливе тільки у тому випадку, коли середовище вільне протягом часу, рівного або більшого, ніж DIFS. Тобто як IFS в режимі DCF потрібно використовувати інтервал DIFS - найтриваліший період з трьох можливих, що дає цьому режиму найнижчий пріоритет. Міжкадровий інтервал SIFS має найменше значення, він служить для першочергового захоплення середовища у відповідь CTS-кадрами або квитанціями, які продовжують або завершують передачу кадру, що вже почалася. Значення міжкадрового інтервалу PIFS більше, ніж SIFS, але менше, ніж DIFS. Проміжком часу між завершенням PIFS і DIFS користується арбітр середовища. У цьому проміжку він може передати спеціальний кадр, який говорить всім станціям, що починається контрольований період. Отримавши цей кадр, станції, які хотіли б скористатися алгоритмом DCF для захоплення середовища, вже не можуть цього зробити, вони повинні чекати закінчення контрольованого періоду. Його тривалість оголошується в спеціальному кадрі, але цей період може закінчитися і раніше, якщо у станцій немає чутливого до затримок трафіка. В цьому випадку арбітр передає службовий кадр, після якого після закінчення інтервалу DIFS починає працювати режим DCF. На керованому інтервалі реалізується централізований метод доступу PCF. Арбітр виконує процедуру опиту, щоб по черзі надати кожній такій станції право на використання середовища, направляючи їй спеціальний кадр. Станція, отримавши такий кадр, може відповісти іншим кадром, який підтверджує прийом спеціального кадру і одночасно передає дані (або за адресою арбітра для транзитної передачі, або безпосередньо для станції). Для

того, щоб якась частка середовища завжди діставалася асинхронному трафіку, тривалість контрольованого періоду обмежена. Після його закінчення арбітр передає відповідний кадр і починається неконтрольований період. Кожна станція може працювати в режимі PCF, для цього вона повинна підписатися на дану послугу при приєднанні до мережі.

Хід роботи

1. Винести на логічне поле із бібліотеки безпроводових пристроїв точку доступу AccessPoint-PT та п'ять комп'ютерів.

2. Відкрити вікно властивостей одного із комп'ютерів. Вимкнути його та перетягнути присутній в комп'ютері модуль розширення із портом Fast Ethernet у список обладнання. Таким чином було видалено плату. На її місце зі списку обладнання перетягнути модуль PT-HOST-NM-1W, який є безпроводовим мережевим адаптером, який використовує аналогічно протокол Fast Ethernet, але передача здійснюється через радіохвилі. Після цього увімкнути живлення комп'ютера.

3. Аналогічно п. 2 замінити наявні Fast Ethernet адаптери на безпроводові. Після увімкнення усіх комп'ютерів адаптери кожного із них виконають встановлення з'єднання із точкою доступу, що стане зрозуміло при появі між ними умовного зображення радіохвиль (рисунок 5.39).

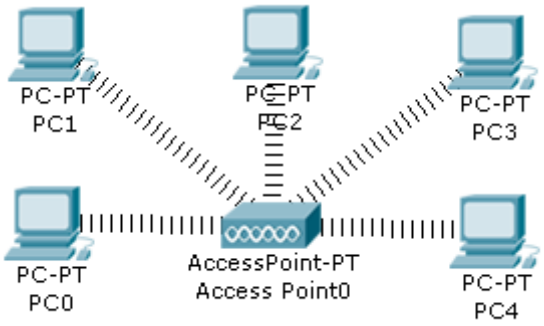


Рисунок 5.39 – Структура безпроводової локальної мережі

4. Присвоїти усім безпроводовим адаптерам комп'ютерів IP-адреси у межах 192.168.1.11 – 192.168.1.15. Маска підмережі – 255.255.255.0.

5. Виконати пінгування між комп'ютерами безпроводової мережі.

6. Перейти у режим моделювання (Shift+S). Виконати покрокове дослідження передачі ICMP-пакета від комп'ютера до комп'ютера. Зробити знімки екрана при кожному кроці передачі пакета.

7. Зробити покрокове моделювання одночасної передачі двох ICMP-пакетів від різних комп'ютерів.

Зміст звіту

1. Тема і мета роботи.

2. Короткий опис системи радіодоступу.

3. Завдання до лабораторної роботи.

4. Знімки екрана із безпроводовою мережею та заміною наявних мережевих адаптерів на безпроводові.

5. Знімки екрана при кожному кроці передачі пакета.

6. Результати проведеного пінгування між комп'ютерами безпровідної мережі.

Контрольні запитання

1. Які методи кодування сигналів використовуються в стандарті 802.11?

2. Яким чином визначає колізії MAC-рівень в мережі 802.11?

3. Чи може станція мережі 802.11 передати кадр інший станції цієї ж мережі не безпосередньо, а через точку доступу?

4. З якою метою в режимі DCF дозволений для передачі кадрів період часу ділиться на слоти? З яких міркувань вибирається тривалість слота?

5. За рахунок чого режим PCF завжди має пріоритет перед режимом DCF?

6. Як здійснюється розширення спектра стрибкоподібною перебудовою частоти?

7. Як здійснюється пряме послідовне розширення спектра?

8. На що впливає і як розв'язується ефект прихованого термінала?

ПЕРЕЛІК ПОСИЛАНЬ

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : [учебник для вузов. 4-е изд.] / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2010. – 958 с.
2. Таненбаум Э. Компьютерные сети. [4-е изд.] / Таненбаум Э. – СПб. : Питер, 2003. – 992 с.
3. Бонн Дж. Руководство по Cisco IOS / Дж. Бонн. − СПб. : Питер «Русская Редакция», 2008. – 784 с.
4. Пакет К. Создание масштабируемых сетей CISCO : [перев. с англ.] / К. Пакет, Д. Тир. – М. : Изд. дом «Вильямс», 2002. – 976 с.
5. Крейг Хаит. Персональные компьютеры в сетях TCP/IP : [перев. с англ.] / Хаит Крейг. – К. : BHV-Киев, 1997. – 415 с.
6. Крук Б. И. Телекоммуникационные системы и сети: в 2 т. Том 1. Современные технологи / Крук Б. И., Попантонопуло В. Н., Шувалов В. П. – М. : Горячая линия – Телеком, 2003. – 647 с.
7. Ткаченко В. А. Комп’ютерні мережі та телекомунікації : [навч. посібник] / Ткаченко В. А., Касілов О. В., Рябик В. А. – Харків : НТУ «ХПІ», 2011. – 224 с.
8. Бройдо В. Л. Вычислительные системы, сети и телекоммуникации : [учебник для вузов. 2-е изд.]. / Бройдо В. Л. – СПб. : Питер, 2006. – 703 с.
9. Кравчук С. О. Основи комп’ютерної техніки: компоненти, системи, мережі : [навч. посібник для студ. ВНЗ] / С. О. Кравчук, В. О. Шанін. – К. : „Політехніка”, 2005. – 344 с.
10. Стеклов В. К. Телекомунікаційні мережі [підруч. для студ. вищ. навч. закл. за напрямком «Телекомунікації»] / В. К. Стеклов, Л. Н. Беркман. – К. : Техніка, 2001. – 392 с.
11. Стеклов В. К. Проектування телекомунікаційних мереж [підруч. для студ. вищ. навч. закл. за напрямком «Телекомунікації»] / В. К. Стеклов, Л. Н. Беркман. – К. : Техніка, 2002. – 792 с.
12. Фриман Р. Волоконно-оптические системы связи / Фриман Р. – М. : Техносфера, 2007. – 512 с.
13. Ватаманюк А. И. Создание, обслуживание и администрирование сетей на 100% / Ватаманюк А. И. – СПб. : Питер, 2010 – 232 с.
14. Григорьев В. А. Сети и системы радиодоступа / Григорьев В. А., Лагутенко О. И., Распаев Ю. А. – М. : Эко-Трендз, 2005. – 384 с.

Навчальне видання

Віктор Арсентійович Гикавий
Оксана Степанівна Городецька

Телекомунікаційні та інформаційні мережі
Лабораторний практикум

Редактор В. Дружиніна
Коректор З. Поліщук

Оригінал-макет підготовлено О. Городецькою

Підписано до друку 19.06.2017 р.
Формат 29,7 × 42¼. Папір офсетний.
Гарнітура Times New Roman.
Ум. друк. арк. 6,14
Наклад 50 (1-й запуск 1-20) пр. Зам. 2017-198

Видавець та виготовлювач
Вінницький національний технічний університет,
інформаційний редакційно-видавничий центр.
ВНТУ, ГНК, к. 114.
Хмельницьке шосе, 95,
м. Вінниця, 21021.
Тел. (0432) 59-85-32, 59-87-38.
press.vntu.edu.ua;
E-mail: kivc.vntu@gmail.com.

Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.