ФАКУЛЬТЕТ АВТОМАТИКИ, ТЕЛЕМЕХАНІКИ ТА ЗВ'ЯЗКУ

Кафедра «Спеціалізовані комп'ютерні системи»

ТЕХНОЛОГІЇ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

МЕТОДИЧНІ ВКАЗІВКИ

до самостійної роботи з дисципліни

«*МЕРЕЖНІ ТЕХНОЛОГІЇ ТА ІНТЕРНЕТ*»

Харків 2013

Методичні вказівки розглянуто і рекомендовано до друку на засіданні кафедри «Спеціалізовані комп'ютерні системи» 19 травня 2011 р., протокол № 11/11.

Методичні вказівки розрблені з метою самостійного вивченя деяких тем з дисципліни «Мережні технології та Інтернет», які не увійшли в аудиторний курс лекцій, але є корисними для майбутніх мережних фахівців. Четвертий розділ містить методичні вказівки для позааудиторної підготовки до лабораторних робіт.

Методичні вказівки призначені для студентів факультету «Автоматика, телемеханіка та зв'язок», що вивчають дисципліну «Мережні технології та Інтернет», денної й заочної форм навчання.

Укладачі:

доц. В.М. Добрянський (розділи 1,2,3 і 4.2),
асист. А.О. Махота (розділ 4.1)

Рецензент

проф. С.В. Лістровий

ТЕХНОЛОГІЇ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

МЕТОДИЧНІ ВКАЗІВКИ

до самостійної роботи з дисципліни

«*МЕРЕЖНІ ТЕХНОЛОГІЇ ТА ІНТЕРНЕТ*»

Відповідальний за випуск Добрянський В.М.

Редактор Еткало О.О.

Підписано до друку 27. 05. 11 р.

Формат паперу 60x84 1/16. Папір писальний.

Умовн.-друк.арк. 2,0. Тираж 50. Замовлення №

Видавець та виготовлювач Українська державна академія залізничного транспорту,
61050, Харків-50, майдан Фейєрбаха, 7.
Свідоцтво суб'єкта видавничої справи ДК № 2874 від 12.06.2007 р.

ЗМІСТ

Вступ

Методичні вказівки розроблені з метою самостійного вивчення деяких тем з дисципліни «Мережні технології та Інтернет», які не увійшли в аудиторний курс лекцій, але є корисними для майбутніх мережних фахівців.

Вказівки являють собою доповнення до курсу лекцій «Технології локальних комп'ютерних мереж на розподіленому середовищі».

Методичні вказівки містять чотири розділи.

Перший розділ присвячений мережній технології 100VG-AnyLAN. Ця технологія була розроблена з ініціативи фірм HP і AT@T і увійшла у світову практику у вигляді стандарту IEEE 802.12. Незважаючи на те, що технологія, в порівнянні з близькою до неї за продуктивністю технологією Fast Ethernet, не набула значного поширення, інтерес до неї не знижується внаслідок використання оригінальних технічних рішень. Мережні фахівці з вищою освітою зобов'язані не просто знати про її існування, але мати уявлення про технічні рішення, які лежать в її основі.

У другому розділі більш детально розглядаються апаратні засоби, які використовуються при створенні мереж на розподіленому середовищі. Особливий інтерес має функціональна орієнтація мережних адаптерів для серверів і клієнтських комп'ютерів, а також додаткові функції концентраторів і їх конструктивні особливості.

Мережі на розподіленому середовищі, незважаючи на безперечні їх переваги (невисока вартість обладнання і простота розширення), мають і серйозні недоліки. Насамперед до таких недоліків потрібно віднести обмеження на кількість вузлів у мережі і максимальну відстань між вузлами. У третьому розділі і розглядаються алгоритм роботи і функціональні та конструктивні особливості мостів і комутаторів як пристроїв, що забезпечують побудову локальних мереж, позбавлених вказаних вище недоліків.

У робочій програмі дисципліни «Мережні технології та Інтернет» передбачені дві лабораторні роботи «Організація безпроводових мереж» і «Підключення до Інтернету і

настроювання електронної пошти». У четвертому розділі подані методичні вказівки з виконання цих робіт, що передбачають самостійну, позааудиторну попередню підготовку до їх виконання.

1 Мережна технологія 100VG-AnyLAN

1.1 Загальна характеристика технології 100VG-AnyLAN

Як альтернативу технології Fast Ethernet фірми AT&T і HP висунули проект нової технології із швидкістю передачі даних 100 Мб/с – 100Base-VG. У цьому проекті було запропоновано удосконалити метод доступу з урахуванням потреби мультимедійних пристроїв, при цьому зберегти сумісність формату пакета з форматом пакета мереж 802.3. У вересні 1993 року за ініціативою фірм IBM і HP був утворений комітет IEEE 802.12, який зайнявся стандартизацією нової технології. Проект був розширений за рахунок підтримки в одній мережі кадрів не тільки формату Ethernet, але і формату Token Ring. В результаті нова технологія отримала назву 100VG-AnyLAN, тобто технологія для будь-яких мереж (Any LAN – будь-які мережі), маючи на увазі, що в локальних мережах технології Ethernet і Token Ring використовуються в переважній кількості вузлів.

Влітку 1995 року технологія 100VG-AnyLAN отримала статус стандарту IEEE 802.12.

У технології 100VG-AnyLAN визначені новий метод доступу Demand Priority і нова схема квартетного кодування Quartet Coding, що використовує надмірний код 5B/6B.

Метод доступу Demand Priority заснований на передачі концентратору функцій арбітра вирішуєя проблему доступу до розподіленого середовища. Метод Demand Priority підвищує коефіцієнт використання пропускної спроможності мережі за рахунок введення простого, детермінованого методу розділення загального середовища, що використовує два рівні пріоритетів: низький – для звичайних пристроїв і високий – для мультимедійних.

Технологія 100VG-AnyLAN має меншу популярність серед виробників комунікаційного устаткування, ніж конкуруюча пропозиція – технологія Fast Ethernet. Компанії, які не підтримують технологію 100VG-AnyLAN, пояснюють це тим, що для більшості сьогоднішніх пристроїв і мереж достатньо можливостей технології Fast Ethernet, яка не так помітно відрізняється від звичної більшості користувачів технології Ethernet. У майбутньому ці виробники пропонують використовувати для мультимедійних пристроїв технологію ATM, а не 100VG-AnyLAN. Проте, кількість прихильників технології 100VG-AnyLAN збільшується і досягла близько 30 компаній. Серед них – не тільки компанії Hewlett-Packard і IBM, але і такі лідери, як Cisco Systems, Cabletron, D-Link та інші. Всі ці компанії підтримують обидві конкуруючі технології у своїх продуктах, випускаючи модулі з портами як Fast Ethernet, так і 100VG-AnyLAN.

1.2 Структура мережі 100VG-AnyLAN

Мережу 100VG-AnyLAN завжди включає центральний концентратор, що називається концентратором рівня 1 або кореневим концентратором (рисунок 1.1).

Кореневий концентратор має зв'язки з кожним вузлом мережі, утворюючи топологію типу каскадована зірка. Цим концентратором є інтелектуальний центральний контролер, який управляє доступом до мережі, постійно виконуючи цикл колового сканування своїх портів і перевіряючи наявність запитів на передачу кадрів від приєднаних до них вузлів. Концентратор приймає кадр від вузла, що видав запит, і передає його тільки через той порт, до якого приєднаний вузол з адресою, яка збігається з адресою призначення, вказаною в кадрі.

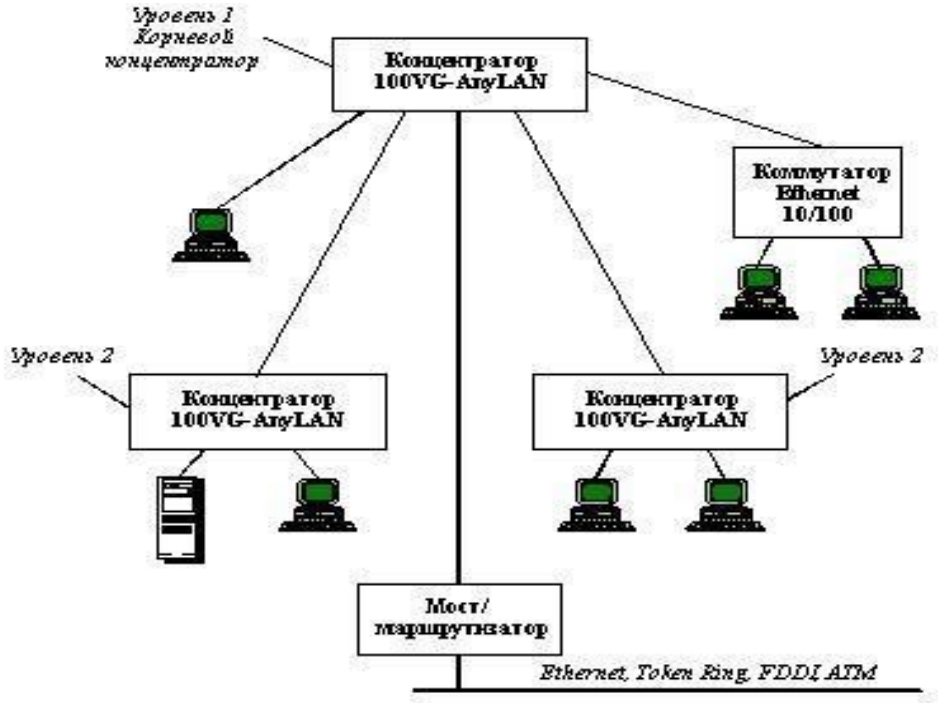

Рисунок 1.1 – Структура мережі 100VG-AnyLAN

Кожен концентратор може бути сконфігурований на підтримку або кадрів 802.3 (Ethernet), або кадрів 802.5 (Token Ring). Всі концентратори, розташовані в одному і тому ж логічному сегменті (не розділеному мостами, комутаторами або маршрутизаторами), мають бути конфігуровані на підтримку кадрів одного типу. Для з'єднання мереж 100VG-AnyLAN, що використовують різні формати кадрів 802.3, потрібний міст, комутатор або маршрутизатор. Аналогічний пристрій потрібний і у тому випадку, коли мережа 100VG-AnyLAN повинна бути сполучена з мережею FDDI або ATM. Кожен концентратор має один "висхідний" (up-link) порт і N "низхідних" портів (down-link), як це показано на рисунку 1.2.

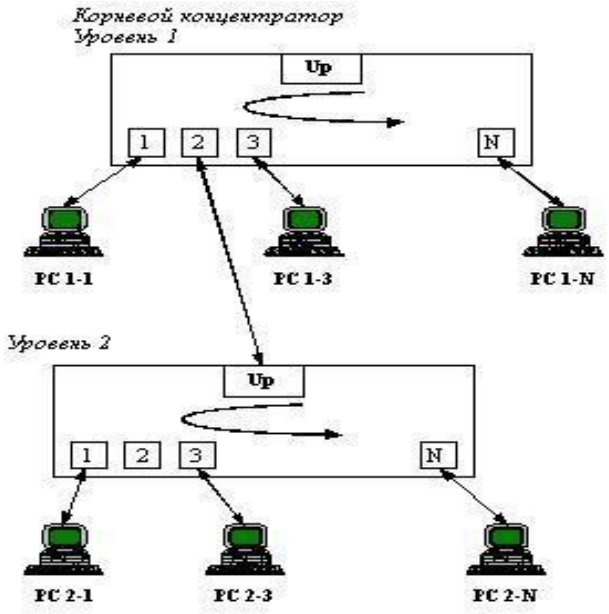

Рисунок 1.2 – Колове опитування портів концентраторами мережі 100VG-AnyLAN

Висхідний порт працює як порт вузла, але він зарезервований для приєднання як вузол до концентратора більш високого рівня. Низхідні порти служать для приєднання вузлів, у тому числі і концентраторів нижнього рівня. Кожен порт концентратора може бути конфігурований для роботи в нормальному режимі або в режимі монітора. Порт, конфігурований для роботи в нормальному режимі, передає тільки ті кадри, які призначені вузлу, під'єднаному до даного порту. Порт, конфігурований для роботи в режимі монітора, передає всі кадри, що обробляються концентратором. Такий порт може використовуватися для підключення аналізатора протоколів.

Вузлом є комп'ютер або комунікаційний пристрій технології 100VG-AnyLAN – міст, комутатор, маршрутизатор або концентратор. Концентратори, що приєднуються як вузли, називаються концентраторами 2-го і 3-го рівнів. Всього дозволяється утворювати до трьох рівнів ієрархії концентраторів. Зв'язок, що сполучає концентратор і вузол, може бути утворений або 4 парами неекранованої витої пари категорій 3, 4 або 5 (4-UTP Cat 3, 4, 5), або 2 парами неекранованої крученої пари категорії 5 (2-UTP Cat 5), або 2 парами екранованої крученої пари

типу 1 (2-STP Type 1), або 2 парами багатомодового оптоволоконного кабелю. Варіанти кабельної системи можуть використовуватися будь-які, але нижче буде розглянутий варіант 4-UTP, який був розроблений першим і набув найбільшого поширення.

На закінчення розділу наведемо таблицю 1.1, складену компанією Hewlett-Packard, в якій наводяться результати порівняння цієї технології з технологіями 10Base-T і 100Base-T.

Таблиця 1.1 – Порівняльна характеристика мереж 10Base-T і 100Base-T

Характеристика	**10Base-T**	**100VG-AnyLAN 100Base-T**
Топологія		
Максимальний діаметр мережі	2500 м	8000 м 412 м
Каскадує концентраторів	Так, 3 рівні	Так, 5 рівнів Два концентратори максимум
Кабельна система		
UTP Cat 3,4	100 м	100 м 100 м
UTP Cat 5	150 м	200 м 100 м
STP Type 1	100 м	100 м 100 м
Оптоволокно	2000 м	2000 м 412 м
Продуктивність		
При довжині мережі 100 м	80% (теоретична)	95% (продемонстрована) 80% (теоретична)
При довжині мережі 2500 м	80% (теоретична)	80% (продемонстрована) Не підтримується
Технологія		
Кадри IEEE 802.3	Так	Та Так
Кадри 802.5	Немає	Та ні
Метод доступу	CSMA/CD	Demand Priority CSMA/CD + підрівень узгодження (Reconciliation sublayer)

1.3 Кодування інформації в мережі 100VG-AnyLAN

Кожен концентратор містить у внутрішній пам'яті таблицю MAC-адрес усіх абонентів, під’єднаних до його портів нижнього рівня. Це дозволяє йому перенаправляти отримані пакети саме

тим абонентам, яким вони адресовані. Концентратори верхніх рівнів зберігають таблиці адрес і тих абонентів, які підключені до концентраторів нижчих рівнів. Таким чином, основний (кореневий) концентратор містить у собі інформацію про всіх абонентів мережі. Формується таблиця адрес на етапі ініціалізації мережі. Крім власне передачі пакетів і пересилання запитів на передачу, в мережі застосовується також спеціальна процедура підготовки до зв'язку (Link Training), під час якого концентратор і абоненти обмінюються між собою пакетами спеціального формату, що управляють. При цьому перевіряється правильність приєднання ліній зв'язку і їх справність, а також рівень помилок: якщо 24 пакети підряд не проходять без помилок, то абонент не включається в роботу. Одночасно концентратор отримує інформацію про особливості абонентів, під'єднаних до нього, їх призначення і мережні адреси, які він заносить в таблицю. Запускається дана процедура абонентом при включенні живлення або після під'єднання до концентратора, а також автоматично при великому рівні помилок.

Цікаво вирішена в мережі 100VG-AnyLAN проблема кодування передаваних даних. Вся передавана інформація проходить такі етапи обробки:

• Розділення на квінтети.

• Перемішування, скремблювання (scrambling) отриманих квінтетів.

• Кодування квінтетів спеціальним кодом 5B/6B (цей код забезпечує у вихідній послідовності не більше трьох одиниць або нулів підряд, що використовуються для детектування помилок).

• Додавання початкового і кінцевого роздільників кадру.

Сформовані таким чином кадри передаються в 4 лінії передачі (при використанні зчетвереної крученої пари). При здвоєній крученій парі і оптоволоконному кабелі застосовується часове мультиплексування інформації в каналах. В результаті всіх цих дій досягається рандомізація сигналів, тобто вирівнювання кількості передаваних одиниць і нулів, зниження взаємовпливу кабелів один на одного і самосинхронізація передаваних сигналів без подвоєння необхідної смуги пропускання, як у разі манчестерського коду. При використанні зчетвереної крученої пари передача по кожній з чотирьох витих

пар проводиться із швидкістю 30 Мбіт/с. Сумарна швидкість передачі складає 120 Мбіт/с. Проте корисна інформація унаслідок використання коду 5B/6B передається всього лише зі швидкістю 100 Мбіт/с. Таким чином, пропускна спроможність кабелю має бути не менше 15 МГц. Цю вимогу задовольняє кабель з витими парами категорії 3 (смуга пропускання – 16 МГц).

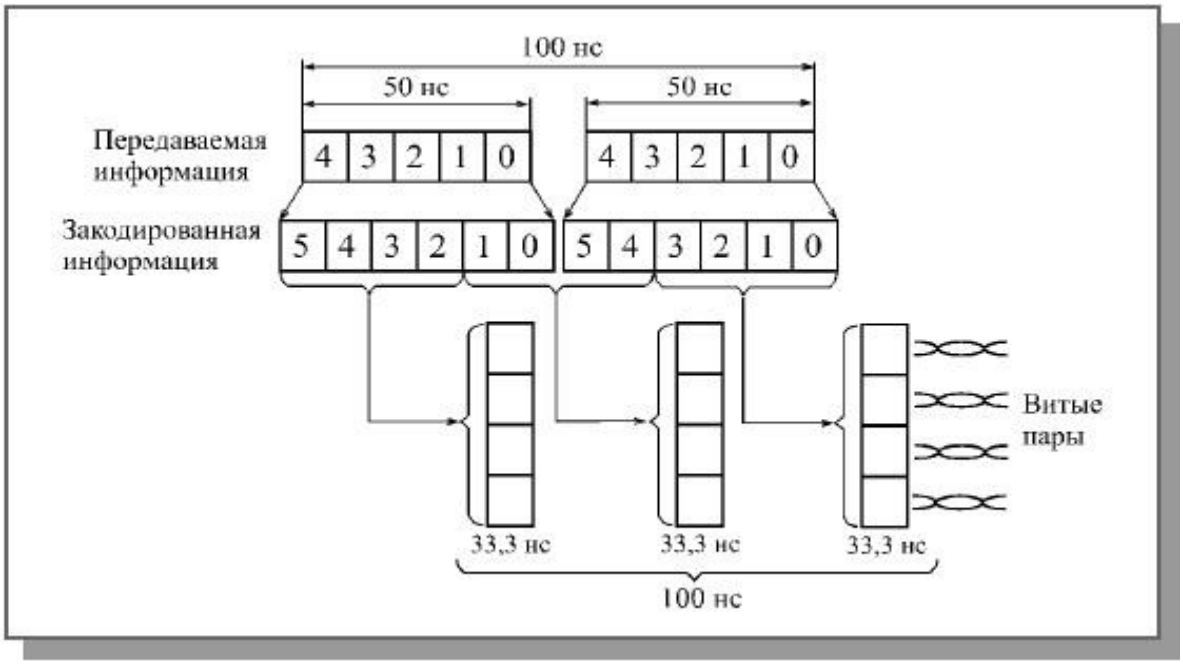

Рисунок 1.3 – Кодування інформації в мережі 100VG-AnyLAN

У мережі 100VG-AnyLAN передбачено два режими обміну: напівдуплексний і повнодуплексний.

При напівдуплексному обміні всі чотири кручені пари використовуються для передачі одночасно в одному напрямі (від абонента до концентратора або навпаки). Даний режим використовується для передачі пакетів.

При повнодуплексному обміні дві кручені пари (1 і 4) передають в одному напрямі, а дві інші (2 і 3) – в іншому напрямі. Цей режим використовується для передачі сигналів, що управляють.

Для управління використовуються два тональні сигнали. Перший з них є послідовністю з 16 логічних одиниць і 16 логічних нулів, які пересуваються із швидкістю 30 Мбіт/с (у результаті частота сигналу дорівнює 0,9375 Мгц). Другий тональний сигнал має удвічі більшу частоту (1,875 Мгц) і

утворюється чергуванням восьми логічних одиниць і восьми логічних нулів. Все управління мережею здійснюється комбінаціями цих двох тональних сигналів.

В таблиці 1.2 наведена розшифровка різних комбінацій цих сигналів, передаваних абонентові і концентратору. Коли ні в абонента, ні у концентратора немає інформації для передачі, обидва вони посилають по обох лініях перший тоновий сигнал (комбінація 1—1). Якщо пакет, що приймається концентратором, може бути адресований даному абонентові, йому посилається комбінація сигналів 1—2. При цьому абонент повинен припинити передачу концентратору сигналів, що управляють, і звільнити ці дві лінії зв'язку для пересилання інформаційних пакетів. Така ж комбінація (1—2), що отримується концентратором, означає запит на передачу пакета з нормальним пріоритетом. Запит на передачу пакета з високим пріоритетом передається комбінацією 2—1. Нарешті, комбінація 2—2 повідомляє як абонента, так і концентратор про необхідність перейти до процедури підготовки до зв'язку (Link Training).

Таблиця 1.2 – Розшифровка кодів в мережі 100VG-AnyLAN

Розшифровка комбінацій тональних сигналів		
Передавальні сигнали	Розшифровка абонентом	Розшифровка концентратором
1 –1	Немає інформації для передачі	Немає інформації для передачі
1 –2	Концентратор приймає пакет	Запит нормального пріоритету
2 –1	Зарезервовано	Високопріоритетний запит
2 –2	Запит процедури підготовки до зв’язку	Запит процедури підготовки до зв’язку

Таким чином, мережа 100VG-AnyLAN є доступне рішення для збільшення швидкості передачі до 100 Мбіт/с. Проте вона не має повної сумісності із жодною із стандартних мереж, тому її

подальша доля проблематична. До того ж, на відміну від мережі FDDI, вона не має ніяких рекордних параметрів. Швидше за все, 100VG-AnyLAN, незважаючи на підтримку солідних фірм і високий рівень стандартизації, залишиться всього лише прикладом цікавих технічних рішень. Якщо говорити про найбільш поширену 100-мегабитну мережу Fast Ethernet, то 100VG-AnyLAN забезпечує удвічі більшу довжину кабелю UTP категорії 5 (до 200 метрів), а також безконфліктний метод управління обміном.

1.4 Приклад мережі з технології 100VG-AnyLAN

Як приклад застосування технології 100VG-AnyLAN для великої корпоративної мережі розглянемо пропозицію компанії Hewlett-Packard щодо модернізації тієї ж мережі університетського кампуса. У плани організаторів заходу High-Speed LAN Shoot-Out III якраз і входило порівняння проектів, заснованих на конкуруючих високошвидкісних технологіях, для однієї і тієї ж реальної великої мережі.

Пропозицію компанії Hewlett-Packard ілюструє рисунок 1.4.

Цікаво, що компанія Hewlett-Packard, як і компанія 3Com, вирішила залишити як магістраль мережі, що охоплює всі «будови» кампуса, кільце FDDI .

Основна увага в проекті приділяється мережам «будови». Робочі групи утворюються на основі концентраторів 100VG Hub-15. На відміну від пропозиції 3Com, що вирішила централізувати основні сервери «будови» за рахунок їх безпосереднього підключення до комутатора «будови», у проекті Hewlett-Packard сервери залишені там, де вони і містилися – в робочих групах.

Кожна «будова» забезпечується одним центральним комутатором LAN Switch 16, здатним комутувати сегменти Ethernet, 10Base-T і сегменти 100VG. Пристрої LAN Switch 16 використовуються для комутації мереж поверхів, а також для комутації сегментів Ethernet, утворених 60 користувачами комп'ютерів Macintosh. Для підключення мережі «будови» до магістрального кільця FDDI використовується маршрутизатор

моделі 650 компаній Hewlett-Packard з інтерфейсом 100VG і FDDI.

Модернізацію мережі пропонується провести за п’ять етапів.

На першому етапі потрібно провести тестування всіх чотирьох пар кабельної системи на відповідність вимогам 100VG. Потім ця технологія упроваджується в деяких робочих групах, там, де підвищена продуктивність потрібна в першу чергу.

На другому етапі в «будови» встановлюється комутатор LAN Switch 16 і маршрутизатор 100VG/FDDI. Кількість робочих груп, що перейшли на 100VG, також істотно збільшується.

На третьому етапі всі робочі групи в усіх «будовах» переходять на технологію 100VG.

Четвертий етап полягає в моніторингу мережного трафіка з метою виявлення сегментів, які необхідно виділити для прямого під’єднання до комутаторів. Можливе збільшення числа комутаторів у деяких «будовах».

І, нарешті, п'ятий етап може полягати в переході від технології FDDI на магістралі мережі до гігабітних технологій, до яких збирається приєднатися і варіант 1000VG, що розробляється в даний час.

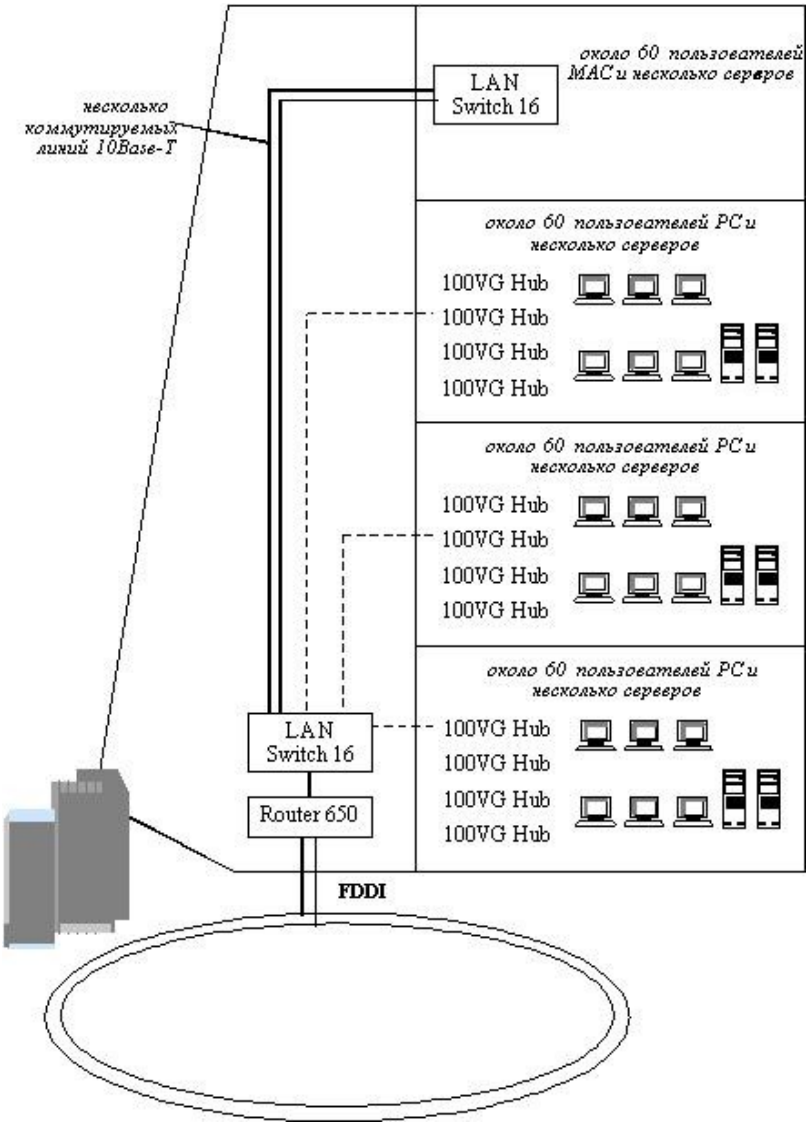

Рисунок 1.4 – Застосування технології 100VG-AnyLAN у мережі університетського кампуса

Висновки

Мережа 100VG-AnyLAN – це одна з останніх розробок високошвидкісних локальних мереж, що з'явилася на ринку. Вона розроблена компаніями Hewlett-Packard та IBM і відповідає міжнародному стандарту IEEE 802.12, тому рівень її стандартизації досить високий.

Головною її перевагою є велика швидкість обміну, порівняно невисока вартість апаратури (приблизно вдвічі дорожче устаткування найбільш популярної мережі Ethernet

10BASE-T), централізований метод керування обміном без конфліктів, а також сумісність на рівні форматів пакетів з мережами Ethernet й Token-Ring.

У назві мережі 100VG-AnyLAN цифра 100 відповідає швидкості 100 Мбіт/с, букви VG позначають дешеву неекрановану кручену пару категорії 3 (Voice Grade), а AnyLAN (будь-яка мережа) позначає те, що мережа сумісна із двома найпоширенішими мережами.

Контрольні питання:

1 Які типи карт мережного адаптера використовуються в технології 100VG-AnyLAN?
2 Назвіть метод доступу до середовища передачі даних, який використовується в технології 100VG-AnyLAN.
3 Які пристрої управляють доступом до середовища в технології 100VG-AnyLAN?
4 Опишіть алгоритм доступу до середовища передачі даних у технології 100VG-AnyLAN?
5 Яку топологію мають мережі 100VG-AnyLAN?
6 Назвіть типи кабелів, які можуть використовуватися в технології 100VG-AnyLAN?
7 Скільки рівнів в ієрархії концентраторів може бути в мережі 100VG-AnyLAN?
8 Яким може бути максимальний діаметр мережі 100VG-AnyLAN?
9 Опишіть процес кодування даних у технології 100VG-AnyLAN?
10. Яке логічне кодування даних використовується в технології 100VG-AnyLAN?

2 Обладнання для локальних мереж із розподіленим середовищем

Повторювачі з мережними адаптерами і кабельною системою являють собою той мінімум обладнання, за допомогою якого можна побудувати локальну мережу з розподіленим середовищем. Природно, що така мережа не може бути дуже великою, оскільки при великій кількості вузлів загальне середовище передачі швидко стає вузьким місцем, що знижує продуктивність мережі. Тому повторювачі і мережні адаптери дозволяють будувати невеликі базові фрагменти мереж, які потім можна об'єднувати за допомогою комутаторів, мостів і маршрутизаторів.

2.1 Основні функції мережних адаптерів

Мережний адаптер або **мережна інтерфейсна карта (**network interface Card, NIC). Мережний адаптер разом з своїм драйвером виконує функції фізичного рівня і MAC-підрівня Канального рівня. LLC-підрівень Канального рівня реалізовується програмним модулем операційної системи, єдиним для драйверів і мережних адаптерів різних технологій локальних мереж. Так, наприклад, в ОС Windows XP LLC-підрівень реалізовується в модулі NDIS (Network Drivers Interface Specification – специфікація стандартного інтерфейсу мережних адаптерів. Специфікація розроблена компанією Microsoft для того, щоб зробити комунікаційні протоколи незалежними від мережного обладнання).

Разом з драйвером мережний адаптер виконує дві операції: передачу і прийом кадру.

Передача кадру з комп'ютера в кабель вимагає виконання таких етапів:

- Прийом кадру даних LLC-підрівня через міжрівневий інтерфейс разом з адресною інформацією MAC-підрівня.
- Формування кадру даних MAC-підрівня, в який інкапсулюється кадр LLC-підрівня; заповнення адрес приймача і джерела;обчислення контрольної суми.

- Формування символів кодів при використанні надмірних кодів типу 4B/5B; скремблювання (шифрування) кодів для отримання більш рівномірного спектра сигналів (виконується не в усіх протоколах, наприклад, технологія Ethernet 10 Мбіт/с обходиться без нього).
- Видача сигналів у кабель відповідно до прийнятого лінійного коду – манчестерського, NRZI, MLT-3 тощо.

Прийом кадру з кабеля в комп'ютер вимагає виконання таких дій:

- Прийом з кабелю сигналів, що кодують бітовий потік.
- Виділення сигналу на фоні шуму. Цю операцію можуть виконувати різні спеціалізовані мікросхеми або процесори DSP(Digital Signal Processor – потужні процесори, які здатні виконувати складні алгоритми обробки сигналів у реальному часі).
- Якщо дані перед відправленням зазнавали скремблювання, то зазнають зворотного процесу – дескремблювання, після чого в мережному адаптері відновлюються символи коду, які були надіслані передавачем вузла-відправника.
- Перевірка контрольної суми кадру. Якщо контрольна сума неправильна, то кадр відкидається, а через міжрівневий інтерфейс LLC-підрівню передається код помилки. Якщо контрольна сума правильна, то з MAC-кадру витягується LLC-кадр і передається протоколу LLC.

Розподіл функцій між картою мережного адаптера і драйвером стандартом не регламентується. Кожний виробник програмно-апаратний функціональний інтерфейс між картою і драйвером визначає самостійно (відстежується тільки точне дотримання інтерфейсу між драйвером карти мережного адаптера і драйвером віртуального пристрою, наприклад, NDIS в ОС Windows XP). Звичайно мережні адаптери поділяються на адаптери для клієнтських комп'ютерів і для серверів.

В адаптерах, призначених для клієнтських комп'ютерів, значна частина роботи перекладається на драйвер, внаслідок чого сам адаптер стає простішим і, відповідно, дешевшим. Однак при

цьому збільшується міра завантаження центрального процесора рутинними операціями з передавання даних з оперативної пам'яті в мережу.

Адаптери, призначені для серверів, велику частину роботи з передавання даних з оперативної пам'яті в мережу і зворотно виконують самостійно.

Залежно від того, протокол якої локальної технології реалізовує адаптер, вони поділяються на адаптери Ethernet, Token Ring, FDDI і т.д. Оскільки протокол Fast Ethernet за рахунок процедури автопереговорів може автоматично вибирати швидкість роботи мережного адаптера, то багато які мережні адаптери Ethernet підтримують дві швидкості роботи і мають у своїй назві префікс 10/100.

Мережні адаптери базуються на спеціалізованих інтегральних схемах. Мережні адаптери, що випускаються в цей час, мають інтегральну схему ASIC (Application-Specific Integrated Circuit), що виконує функції MAC-підрівня і велику кількість високорівневих функцій, таких як підтримка агента віддаленого моніторингу, схема пріоритезації кадрів, функції дистанційного управління комп'ютером тощо. В серверних варіантах адаптерів обов'язкова наявність потужного **процесора**, що розвантажує центральний процесор.

2.2 Основні функції повторювачів

Практично в усіх сучасних технологіях локальних мереж є певний пристрій, який має декілька назв – повторювач, концентратор, хаб. Залежно від сфери використання значною мірою змінюється склад його функцій і конструктивне виконання. Незмінною залишається тільки основна функція – повторення кадру або на всіх портах (як, наприклад, у стандарті Ethernet), або тільки на деяких портах, відповідно до алгоритму, визначеного тим або іншим стандартом.

У технології Ethernet пристрої, що об'єднують декілька сегментів коаксіального кабелю в єдинє розподілене середовище, використовувалися спочатку і отримали назву "повторювач" за своєю основною функцією – повторенням на всіх своїх портах

сигналів, отриманих на вході одного з портів. У мережах на основі коаксіального кабелю звичайними є двопортові повторювачі, тому термін "концентратор" для них не застосовується.

З появою стандарту 10BASE-T повторювач став невід'ємною частиною мережі, оскільки без нього можна об'єднати в мережу тільки два комп'ютери. Багатопортові повторювачі Ethernet на крученій парі стали називати **концентраторами**, або **хабами** (в перекладі з англ. – ступиця), оскільки в одному пристрої зв'язувалися один з одним велика кількість вузлів. Основна частина портів концентратора Ethernet стандарту 10BASE-T має рознімач RJ-45. Але може мати і порт AUI для підключення до нього трансивера, сполученого з товстим коаксіальним кабелем або оптоволоконним кабелем.

Для з'єднання концентраторів в ієрархічну систему можна використати ті ж порти, що і для підключення станцій, але з урахуванням однієї специфічної обставини. Справа в тому, що звичайний порт RJ-45, призначений для підключення мережного адаптера і званого MDI-X (кросований інтерфейс MDI), має рознімач, що інвертує розводення контактів, щоб мережний адаптер можна було підключити до концентратора за допомогою стандартного з'єднувального кабелю, не кросуючого контакти. У разі з'єднання концентраторів через кросуючі порти (стандартний порт MDI-X) доводиться використовувати нестандартний кабель з перехресним з'єднанням пар. Деякі виробники забезпечують концентратор виділеним портом MDI, в якому немає кросованих пар, і тоді два концентратори можна з'єднати звичайним некросованим кабелем, якщо це робити через порт MDI одного концентратора і порт MDI-X іншого концентратора. Найчастіше один і той самий порт концентратора може працювати і як порт MDI-X, і як порт MDI залежно від кнопкового перемикача на корпусі концентратора.

Багатопортовий повторювач-концентратор може по-різному розглядатися при урахуванні правила **чотирьох хабів**. У більшості моделей всі порти пов'язані з єдиним блоком повторення, і при проходженні сигналу між портами блок повторення вносить затримку лише один раз. Тому такий концентратор потрібно вважати одним повторювачем при

урахуванні обмежень, що накладаються правилом чотирьох хабів. Разом з тим існують і концентратори і інших типів, коли на декілька портів є свій блок повторення. У такому випадку при обліку обмежень правила чотирьох хабів кожний блок повторення вважається окремим повторювачем.

2.3 Додаткові функції концентраторів

Крім основної функції – відновлення первинної форми сигналів, що кодують на фізичному рівні кадр, у концентраторів є порівняно численні додаткові функції, включаючи **автосегментацію** – здатність відключати некоректно працюючі порти, ізолюючи тим самим іншу частину мережі від проблем, що виникли у вузлі.

Автосегментація. Основною причиною відключення порту в технологіях Ethernet і Fast Ethernet є відсутність відповіді на послідовність імпульсів тесту зв'язності, що посилаються в усі порти кожні 16 мкс. У цьому випадку порт відключається, але імпульси тесту зв'язності продовжують на нього подаватися з тим, щоб після відновлення пристрою робота з ним була продовжена автоматично.

Концентратори Ethernet і Fast Ethernet виконують відключення портів також у таких випадках:

- **Помилка на рівні кадру.** Якщо інтенсивність проходження через порт кадрів, що містять помилки, перевищує деякий поріг, то порт відключається. Такими помилками можуть бути неправильна контрольна сума, неправильна довжина кадру (більше 1528 байтів або менше 64 байтів), неоформлений заголовок кадру.
- **Множинні колізії.** Якщо концентратор фіксує, що джерелом колізій був один і той самий порт 60 разів підряд, то порт відключається. Через деякий час порт буде знову включений.
- **Перевищення тривалості передачі кадру.** Як і мережний адаптер, концентратор контролює час проходження кадру через

порт: якщо він перевищує час проходження кадру максимальної довжини в три рази, то цей порт відключається.

Підтримка резервних зв'язків. Використання резервних зв'язків визначене тільки в технології FDDI. В інших технологіях розробники концентраторів підтримують резервні зв'язки за допомогою своїх приватних рішень.

Захист від несанкціонованого доступу. Розподілене середовище надає дуже широкі можливості для несанкціонованого доступу. Для цього досить підключити комп'ютер до вільного порту концентратора, записати всю інформацію, що проходить через порт, на диск, а потім виділити з неї потрібну.

Розробники концентраторів передбачають деякі засоби захисту даних від несанкціонованого доступу в розподілених середовищах. Найбільш просте рішення – призначення дозволених MAC-адрес портам концентратора. У стандартному концентраторі Ethernet порти MAC-адрес не мають. Захист полягає в тому, що адміністратор мережі вручну зв'язує з кожним портом концентратора деяку MAC-адресу.

Іншим засобом захисту даних від несанкціонованого доступу є шифрування.

Висновки

Концентратори (повторювачі) разом з мережними адаптерами, а також кабельною системою являють собою повний набір обладнання, за допомогою якого можна створити локальну мережу на розподіленому середовищі.

Карта мережного адаптера разом із своїм драйвером виконує функції фізичного рівня і MAC-підрівня канального рівня, а LLC-підрівень канального рівня звичайно реалізовується модулем операційної системи, єдиним для всіх драйверів і мережних адаптерів.

Мережний адаптер разом з своїм драйвером виконує дві операції: передачу і прийом кадру.

Функціональний інтерфейс між адаптером і драйвером стандартом не визначений. Звичайно їх поділяють на адаптери для клієнтських комп'ютерів і адаптери для серверів.

Основною функцією концентратора, що реалізовується в усіх його конструктивних варіантах, є повторення на фізичному рівні кадру або на всіх його портах (як у технології Ethernet), або на деяких портах відповідно до конкретного алгоритму, визначеного тим або іншим стандартом.

Крім основної функції, концентратори завжди виконують і ряд додаткових функцій: автосегментацію, підтримку резервних зв'язків, захист від несанкціонованого доступу.

Контрольні питання:

1 Назвіть етапи, що реалізовуються картою мережного адаптера при передачі і при прийомі кадру.

2 Назвіть основні відмінності між NIC робочої станції і NIC сервера.

3 Назвіть основні функції повторювачів.

4 Назвіть додаткові функції повторювачів.

5 Порти якого типу можуть використовуватися в повторювачі-концентраторі 10BASE-T?

3 Комутовані локальні мережі

Розподілене середовище застосовується в локальних мережах з моменту появи мереж цього типу. Такий підхід до використання комунікаційного каналу має декілька переваг, одною з яких є простота комунікаційного обладнання локальної мережі. Однак наявність розподіленого середовища пов'язана і з очевидним недоліком – поганою масштабованістю, оскільки продуктивність, що виділяється одному вузлу мережі, знижується по мірі збільшення кількості вузлів у мережі.

Природним вирішенням проблеми масштабованості є розподіл мережі на сегменти, кожний з яких являє собою окреме

розподілене середовище. Така логічна сегментація локальної мережі виконується за допомогою мостів або комутаторів.

Локальні мережі, що розділяються на окремі сегменти за допомогою мостів або комутаторів, в деяких джерелах називають **комутованими локальними мережами.**

3.1 Логічна структуризація мережі за допомогою мостів і комутаторів

3.1.1 Переваги і недоліки мережі на розподіленому середовищі

При побудові невеликих мереж, що складаються з 10 – 30 вузлів, використання стандартних технологій на розподіленому середовищі приводить до економічних і ефективних рішень, що виявляється насамперед у таких властивостях:

- Проста топологія мережі дозволяє легко нарощувати кількість вузлів (у невеликих межах).
- Відсутні втрати кадрів через переповнення буферів комунікаційних пристроїв, оскільки сам метод доступу регулює потік кадрів.
- Простота протоколів забезпечує низьку вартість мережних адаптерів, повторювачів і концентраторів.

Разом з тим, справедливе і інше твердження: велику мережу, що нараховує сотні і тисячі вузлів, на одному розподіленому середовищі побудувати не можна.

Головна проблема мереж із розподіленим середовищем – дефіцит пропускної спроможності.

Із зростанням коефіцієнта завантаженості середовища, починаючи з деяких значень, різко збільшується час очікування доступу до середовища (рисунок 3.1).

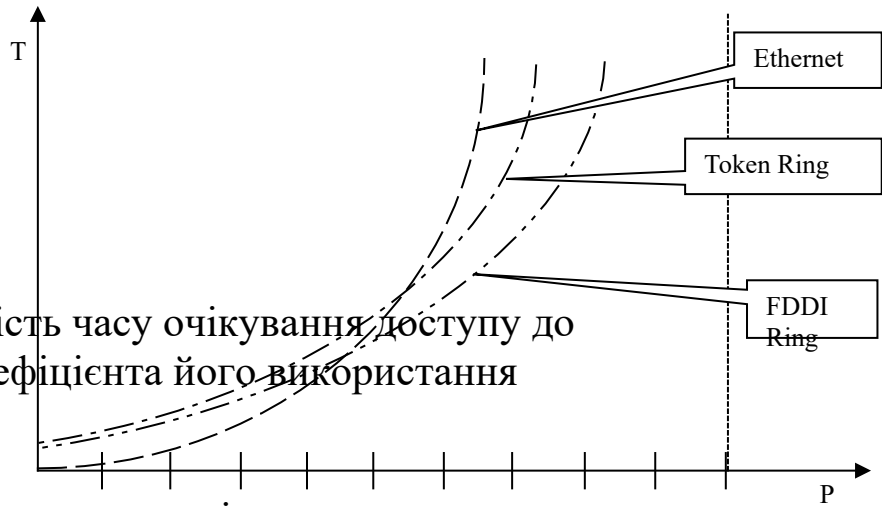

Рисунок 3.1 – Залежність часу очікування доступу до середовища від коефіцієнта його використання

Усім технологіям властива якісно однакова картина зростання величини затримок доступу при збільшенні коефіцієнта використання мережі, коли практично лінійна залежність переходить у круту експонентну. Для технології Ethernet прийнятним порогом коефіцієнта використання середовища можна вважати 30 – 50 %, для технології Token Ring – 60 % і для технології FDDI – порядку 70 – 80 %.

Кількість вузлів, при яких коефіцієнт використання мережі починає виходити за межі допустимого, залежить від типу мережних додатків, що використовуються. Ще і зараз в багатьох літературних джерелах як гранична кількість вузлів на тонкому коаксіальному сегменті, що розділяється, вважається рівною 30, в той час як при переважанні в мережі мультимедійних додатків (що в цей час не рідкість) виявляється, що гранична кількість вузлів на сегменті не перевищує 10.

3.1.2 Переваги логічної структуризації мережі

Обмеження, виникаючі через використання одного середовища, що розділяється, можна подолати, виконавши **логічну структуризацію мережі**, тобто сегментувати єдине розподілене середовище на декілька і з'єднати отримані сегменти мережі за допомогою мостів, комутаторів і маршрутизаторів.

Мости, комутатори і маршрутизатори передають кадри з одного свого порту на інший, аналізуючи адресу призначення, розміщену в кадрі. Мости і комутатори виконують операцію передачі кадрів на основі адрес канального рівня (MAC-адрес), а маршрутизатори використовують для цієї мети ієрархічні адреси мережного рівня (наприклад, IP-адреси).

Логічна структуризація дозволяє вирішити декілька задач, основні з яких: підвищення продуктивності, гнучкості, безпеки і керованості мережі.

Підвищення продуктивності. При сегментуванні мережі трафік в одному сегменті стає менше на величину внутрішнього трафіка другого сегмента. Але при цьому треба пам'ятати, що сегментування не завжди знижує навантаження в нових сегментах. Якщо уявити собі такий варіант сегментації, коли внутрішньосегментний трафік дорівнює нулю (наприклад, вузли сегмента S1 обмінюються тільки з вузлами сегмента S2 і навпаки), то в цьому випадку весь трафік буде повністю міжсегментним.

На практиці завжди можна виділити групу комп'ютерів, які належать співробітникам, що вирішують одну задачу, і в більшості випадків їм потрібен доступ до ресурсів власної групи і тільки зрідка – до ресурсів інших груп. У 80-ті роки існувало правило, що в нормально структурованій мережі 80 % трафіка має бути внутрішньосегментним і тільки 20 % міжсегментним. У цей час ця закономірність не завжди дотримується, і вже нікого не дивує розподіл внутрішньосегментного трафіка і міжсегментного 50 % на 50 % і навіть 20 % на 80 %.

Підвищення гнучкості мережі. При побудові мережі як сукупності сегментів кожний з них може бути адаптований до

специфічних потреб групи або відділу. Наприклад, в одному сегменті може використовуватися технологія Ethernet і ОС Windows 2003, а в іншому – Token Ring і OS-400. Разом з тим користувачі обох сегментів можуть обмінюватися даними через мости/комутатори. Процес розподілу на логічні сегменти можна розглядати і у зворотному напрямі як процес створення великої мережі з невеликих мереж, що вже існують.

Підвищення безпеки мережі. Встановлюючи різні логічні фільтри на мости/комутатори, можна контролювати доступ користувачів до ресурсів інших сегментів, чого не можна зробити за допомогою повторювачів.

Підвищення керованості мережі. Побічним ефектом зниження трафіка і підвищення безпеки даних є спрощення управління мережею. Проблеми дуже часто локалізуються всередині сегмента і, таким чином, сегменти утворюють логічні домени управління мережею.

Отже, мережу можна структурувати за допомогою двох пристроїв: мостів і комутаторів. Відразу ж після появи комутаторів на початку 90-х років деякі виробники комутаторів намагалися нав'язати думку, що мости і комутатори принципово різні пристрої. Насправді це далеко не так: **міст і комутатор – це функціональні близнюки, що працюють за одним і тим самим алгоритмом** (алгоритмом прозорого моста). **Основна відмінність комутатора від моста полягає в тому, що комутатор обробляє кадри паралельно, а міст – послідовно.**

3.1.3 Алгоритм прозорого моста

Мости і комутатори не враховують у своїй роботі існування в мережі мережних адаптерів кінцевих вузлів, повторювачів та концентраторів (цим і пояснюється поява в назві алгоритму слова "прозорий"). З іншого боку, мережні адаптери, повторювачі і концентратори працюють "не помічаючи" наявності в мережі мостів і комутаторів.

Алгоритм прозорого моста не залежить від технології локальної мережі, в якій встановлюється міст/комутатор, тому прозорі мости/комутатори Ethernet працюють точно так само, як прозорі мости/комутатори FDDI або Token Ring.

Мости/комутатори будують свою адресну таблицю на основі пасивного спостереження за трафіком, циркулюючим у сегментах, які під'єднуються до його портів. Кожний порт комутатора працює як самостійний вузол сегмента, за одним винятком – порт комутатора не має своєї MAC-адреси, оскільки комутатори працюють у режимі захоплення кадрів, коли всі поступаючі на порт кадри запам'ятовуються на час у буфері. Працюючи в нерозбірливому режимі, комутатор "слухає" весь трафік, що передається в приєднаних до нього сегментах, і використовує кадри, що проходять через нього, для вивчення структури мережі.

У початковому стані комутатор не знає того, які MAC-адреси мають комп'ютери, що підключені до кожного з його портів. У цій ситуації комутатор просто передає захоплений і буферизований кадр на всі свої порти, за винятком того порту, від якого цей кадр був отриманий. У моста тільки два порти, тому він передає кадри з порту 1 на порт 2 і навпаки. Відмінність роботи комутатора від повторювача полягає в тому, що він передає кадр заздалегідь буферизовуючи його, а не біт за бітом, як це робить повторювач. Буферизація розриває логіку роботи всіх сегментів як єдиного розподіленого середовища. Коли комутатор намагається передати кадр із сегмента на сегмент, він як звичайний кінцевий вузол намагається отримати доступ до середовища, що розділяється за правилами алгоритму доступу, наприклад, за правилами алгоритму CSMA/CD.

3.1.4 Топологічні обмеження комутаторів у локальних мережах

Серйозним обмеженням функціональних можливостей мостів і комутаторів є відсутність підтримки петльової конфігурації мережі.

Наявність петлі в мережі призводить до таких наслідків:

- Розмноження кадру, тобто поява декількох його копій.
- Нескінченна циркуляція всіх копій кадру в петлі, а це означає засмічення мережі непотрібним трафіком.
- Постійна перебудова комутаторами своїх адресних таблиць.

З метою уникнення всіх перелічених небажаних ефектів комутатори треба застосовувати так, щоб між логічними сегментами не було жодної петлі, тобто будувати за допомогою комутаторів тільки деревоподібні структури, гарантуючі наявність єдиного шляху між будь-якими двома сегментами. Тоді кадри від кожної станції будуть надходити в комутатор завжди з одного і того ж порту, і комутатор зможе правильно вирішувати задачу вибору раціонального маршруту в мережі.

У невеликих мережах порівняно легко гарантувати існування одного і тільки одного шляху між двома сегментами. Але коли кількість з'єднань зростає, то імовірність ненавмисного утворення петлі виявляється високою. У великих мережах зі складними зв'язками використовуються алгоритми, які дозволяють виявляти створення петель автоматично. Найбільш відомим з них є стандартний алгоритм покриваючого дерева (Spaning Tree Algorithm, STA).

3.2 Комутатори

3.2.1 Особливості комутаторів

Комутатор – це мультипроцесорний міст, здатний паралельно передавати кадри відразу між всіма парами портів. Згодом комутатори витіснили з локальних мереж класичні однопроцесорні мости. Основна причина цього – істотно більш висока продуктивність, з якою комутатори передають кадри між сегментами.

Технологія комутації сегментів Ethernet була запропонована в 1990 році компанією Kalpana. У комутатора компанії Kaplana при вільному в момент прийому кадру стані вихідного порту затримка між отриманням першого байта кадру і

появою цього ж кадру на виході порту адреси призначення становила всього 40 мкс, що було набагато менше затримки кадру при передачі його мостом. Структура комутатора EtherSwitch, запропонованого фірмою Kalpana, має вигляд, поданий на рисунку 3.2.

Кожний з 8 портів обслуговується одним **процесором пакетів Ethernet (**Ethernet Packet Processor, EPP). Крім того, комутатор має системний модуль, який координує роботу всіх процесорів EPP, зокрема веде загальну адресну таблицю комутатора. Для передачі кадрів між портами використовується комутаційна **матриця. Вона** працює за принципом комутації каналів, з'єднуючи порти комутатора.

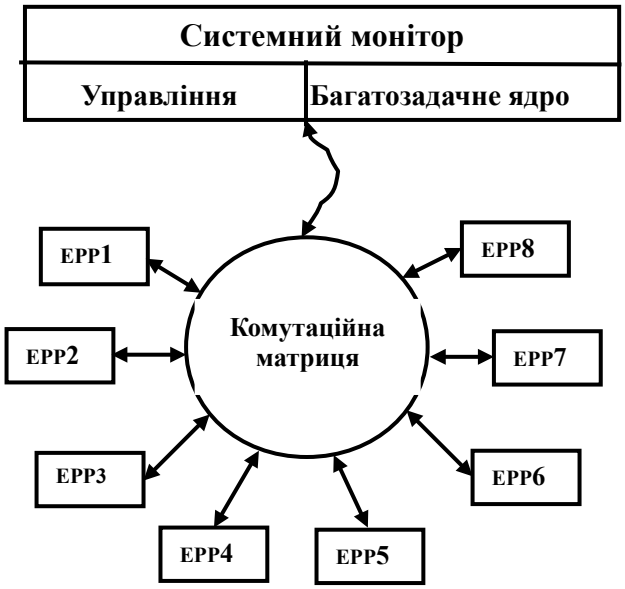

Рисунок 3.2 – Структура комутатора EtherSwitch компанії Kalpana

При надходженні кадру на який-небудь порт відповідний процесор EPP буферизує декілька перших байтів кадру, щоб прочитати адресу призначення. Після встановлення адреси призначення процесор відразу ж приступає до обробки кадру, не дожидаючись надходження інших байтів кадру, за такою схемою:

- Процесор EPP переглядає свій кеш адресної таблиці, і якщо не знаходить потрібної адреси, звертається до системного модуля, який працює в багатозадачному режимі, паралельно

обслуговуючи запити всіх процесорів EPP. Системний модуль знаходить потрібну адресу в своїй, загальній адресній таблиці і повертає процесору EPP знайдений рядок, який той вміщує у свій кеш для подальшого використання.

- Якщо адреса призначення знайдена в адресній таблиці і кадр треба відфільтровувати – процесор просто припиняє записувати його в буфер, очищає буфер і чекає надходження нового кадру.
- Якщо адреса призначення знайдена в адресній таблиці і кадр треба передати на інший порт, процесор, продовжуючи прийом кадру в буфер, звертається до комутаційної матриці, намагаючись встановити в ній шлях, зв'язуючий його порт з портом, через який йде маршрут до вузла з адресою призначення.
- Комутаційна матриця може організувати зв'язок між портами тільки в тому випадку, якщо порт призначення вільний – не сполучений ні з яким іншим портом даного комутатора.
- Якщо порт призначення зайнятий, то комутаційна матриця у зв'язку портів відмовляє. У цьому випадку кадр повністю буферизується процесором вхідного порту і процесор чекає звільнення вихідного порту і утворення комутаційною матрицею потрібного шляху.
- Після того як вхідний і вихідний порти сполучені (встановлений потрібний шлях через комутаційну матрицю), процесор вхідного порту починає передавати байти буферизованого кадру на вихідний порт, які і приймаються процесором вихідного порту. Вихідний порт починає конкурувати за алгоритмом CSMA/CD з вузлами підключеного до нього сегмента за середовище передачі даних. Як тільки середовище стає доступним вихідному порту, він починає передавати кадр у сегмент. Процесор вхідного порту постійно зберігає у своєму буфері декілька байтів кадру, що передається, що дозволяє йому одночасно і асинхронно вести прийом кадру і передавати його на вихідний порт (рисунок 3.3).

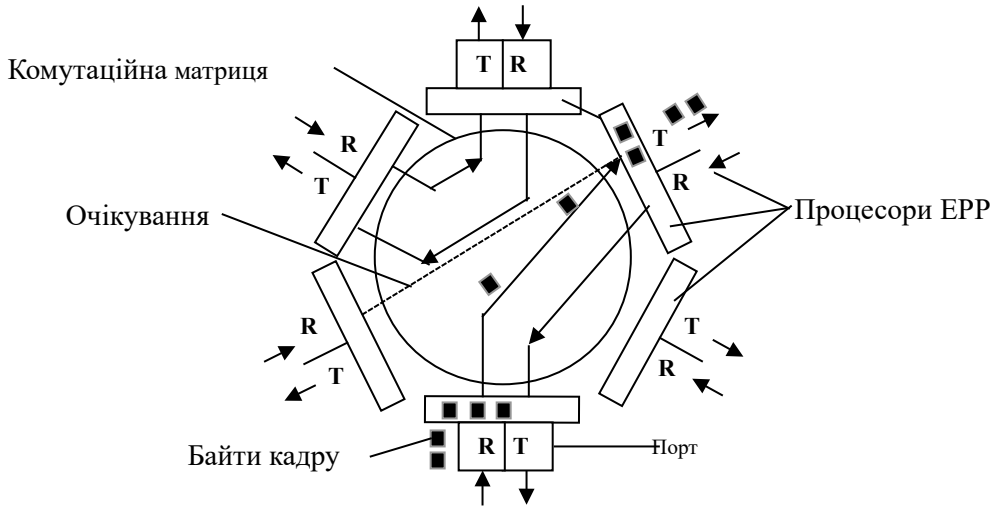

Рисунок 3.3 – Комутація портів та передача кадру через комутаційну матрицю

Описаний алгоритм передачі кадрів між портами комутатора являє собою **конвейєрну обробку**, коли у часі частково поєднуються декілька етапів передачі, і отримав назву **комутації "на льоту" (**on-the-fly), або **"безперервної"** комутації **(cut-through)**.

При комутації "на льоту" можливе поєднання таких етапів передачі:

1 Прийом і буферизація байтів кадру вхідним портом (після прийому перших байтів кадру аж до байтів адреси призначення).

2 Пошук адреси в адресній таблиці комутатора (в кеші порту або загальній адресній таблиці) і комутація портів через комутаційну матрицю.

3 Прийом інших байтів кадру процесором вхідного порту.

4 Прийом байтів кадру (включаючи і перші) процесором вихідного порту.

5 Отримання доступу до середовища передачі даних процесором вихідного порту.

6 Передача кадрів байта процесором вихідного порту в підключений до нього сегмент.

На діаграмі (рисунок 3.4) зображені циклограми для режиму комутації "на льоту" і для режиму з повною буферизацією кадру,

з яких видно, що режим комутації "на льоту" більш ефективний з точки зору часу передачі кадру через комутатор.

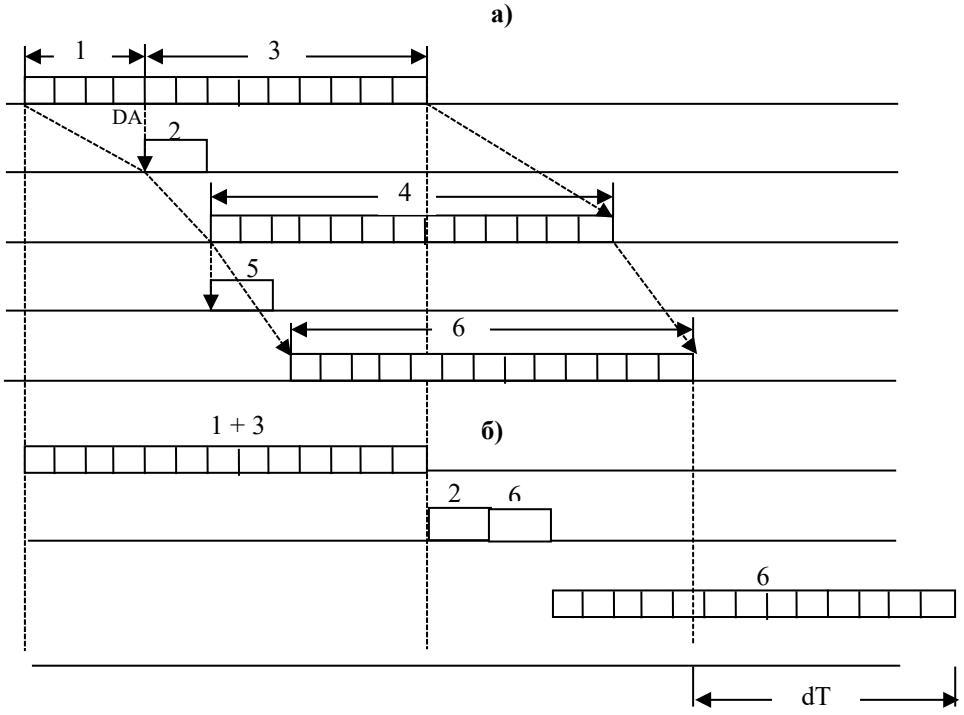

Рисунок 3.4 – Циклограма передачі кадрів комутатором:
а) конвейєрна обрабка;
б) обрабка з повною буферизацією

3.2.2. Неблокуючі комутатори

Комутатор називають **неблокуючим**, якщо він спроможний передавати кадри через свої порти з тією ж швидкістю, з якою вони на них надходять. Кажуть, що комутатор може підтримувати **стійкий неблокуючий режим** роботи, якщо він передає кадри з швидкістю їх надходження протягом довільного проміжку часу. Для забезпечення такого режиму треба так розподілити потоки кадрів по вихідних портах, щоб, по-перше, порти справлялися з навантаженням, а по-друге, комутатор міг завжди в середньому передати на вихід стільки кадрів, скільки їх надійшло на входи. Якщо кожний вхідний потік (просумований

по всіх портах) у середньому буде перевищувати вихідний потік кадрів (також просумуваний по всіх портах), то кадри будуть нагромаджуватися в буфері комутатора і при переповненні буфера – просто відкидатися.

Для підтримки стійкого неблокуючого режиму роботи комутатора необхідно, щоб його продуктивність задовольняла умову

$$\text{Ck} = (\sum_i Cpi) / 2,$$

де Ck – продуктивність комутатора,

Cpi – максимальна продуктивність протоколу, що підтримується і-м портом комутатора.

Сумарна продуктивність портів враховує кожний кадр, що проходить через комутатор двічі: той, що входить, та як й той, що виходить. У стійкому режимі вхідний трафік дорівнює вихідному, тому мінімально достатня продуктивність комутатора, яка необхідна для підтримки неблокуючого режиму, дорівнює половині сумарної продуктивності портів. Якщо порт, наприклад Ethernet 10 Мбіт/с, працює в напівдуплексному режимі, то продуктивність порту Cpi дорівнює 10 Мбіт/с, а якщо в дуплексному – 20 Мбіт/с.

Якщо комутатор спроможний приймати і обробляти кадри від усіх своїх портів на максимальній швидкості протоколу, незалежно від того, чи забезпечуються умови стійкої рівноваги між вхідним і вихідним трафіком, то такий режим називають **миттєвим неблокуючим режимом.** При цьому обробка кадрів може бути неповною – при зайнятості вихідного порту кадр вміщується в буфер комутатора.

Для підтримки миттєвого неблокуючого режиму комутатор повинен володіти більшою власною продуктивністю – вона має дорівнювати сумарній продуктивності портів: $\text{Ck} = \sum_i Cpi$.

3.2.3. Боротьба з перевантаженнями

Переповнення буфера комутатора здатне викликати не тільки зниження продуктивності, але і втрату кадрів. Тому фірми-виробники комутаторів вживають деякі заходи боротьби з перевантаженнями. Застосовуються два основних методи управління потоком кадрів: зворотний тиск на кінцевий вузол і агресивне захоплення середовища. Обидва методи підтримуються напівдуплексним режимом, при якому у комутатора є можливість впливати на кінцевий вузол за допомогою алгоритму доступу до середовища.

Метод зворотного тиску **(**backpressure) (рисунок 3.5, а) полягає у створенні штучних колізій у сегменті, який інтенсивно посилає кадри в комутатор. Для цього комутатор звичайно використовує jam-послідовність, що надсилається на вихід порту, до якого підключений сегмент (або вузол), щоб припинити його активність.

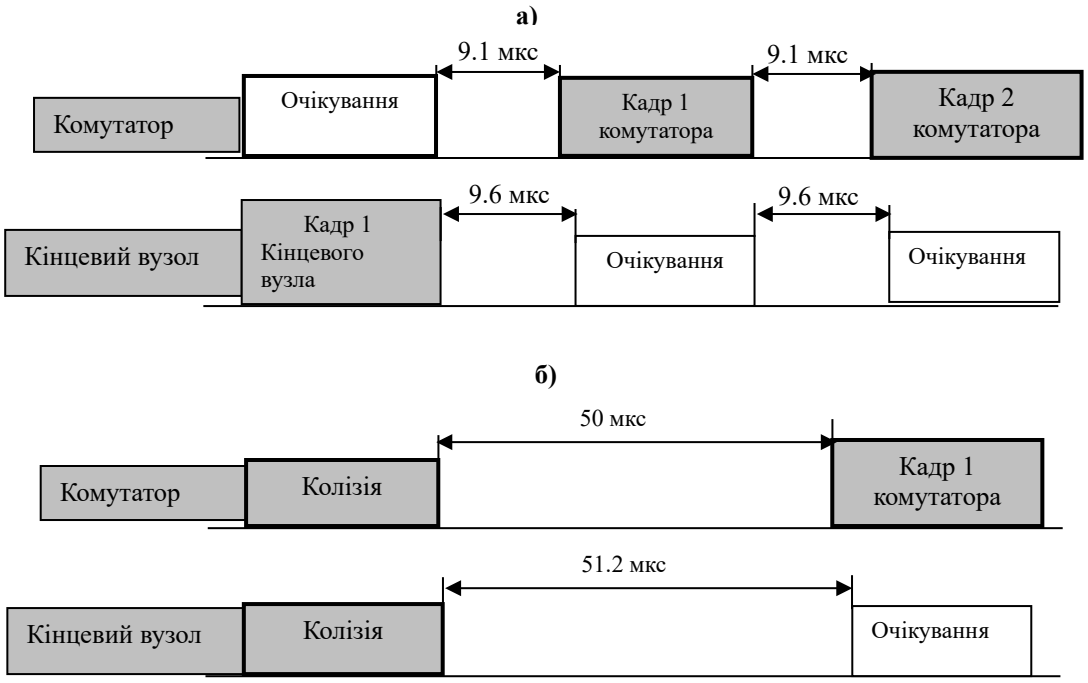

Рисунок 3.5 – Агресивне захоплення середовища комутатором

Метод агресивного захоплення середовища застосовується в тому випадку, коли сусідом є кінцевий вузол. Існують два

різновиди захоплення середовища: або після закінчення передачі чергового кадру, або після колізії (рисунок 3.5, б). У першому випадку комутатор після закінчення передачі чергового кадру замість технологічної паузи в 9.6 мкс робить паузу в 9.1 мкс, після чого починає передачу нового кадру. Комп'ютер не зміг захопити середовище, оскільки витримав паузу в 9.6 мкс і виявив після цього, що середовище вже зайняте. У другому випадку кадри комутатора і комп'ютера зіткнулися, тобто була зафіксована колізія. Оскільки мінімальна відмінна від нуля затримка у вузла між двома колізіями дорівнює 51.2 мкс (512 бітових інтервалів), то комутатор, роблячи затримку в 50 мкс, випереджає кінцевий вузол і йому не вдається передати свій кадр. Комутатор може користуватися цим методом адаптивно, збільшуючи міру власної агресивності по мірі необхідності.

Розглянуті механізми управління потоками кадрів дозволяють комутатору в критичних ситуаціях на кожний кадр, що приймається, відправляти декілька вже буферизованих кадрів, розвантажуючи тим самим буфер. При цьому інтенсивність прийому кадрів не знижується до нуля, а просто меншає до прийнятного рівня.

3.2.4 Трансляція протоколів канального рівня

Відповідно до специфікацій 802.1 H і RFC 1042 комутатори можуть виконувати трансляцію одного протоколу канального рівня в інший, наприклад, Ethernet у FDDI, Fast Ethernet у Token Ring тощо. Трансляцію протоколів локальних мереж полегшує той факт, що найбільш складні перетворення – трансляцію адрес, яку при об'єднанні гетерогенних мереж виконують маршрутизатори і шлюзи, в цьому випадку виконувати не треба – всі кінцеві вузли локальних мереж мають унікальні адреси одного і того ж формату (MAC-адреси) незалежно від протоколу, що використовується. З цієї причини адреса мережного адаптера Ethernet зрозуміла мережному адаптеру FDDI, і вони обидва можуть використати ці адреси в полях своїх кадрів, не беручи до уваги ту обставину, що вузол, з яким вони взаємодіють, працює за цілком іншою технології. При узгодженні протоколів

локальних мереж комутатори просто переносять адреси приймача і джерела з кадру одного протоколу в кадр іншого.

При трансляції протоколів Ethernet і Fast Ethernet у протоколи Token Ring і FDDI можуть виконуватися такі операції:

1 Обчислення довжини поля даних кадру і розміщення цього значення в полі довжини при передачі з мережі FDDI або Token Ring у мережу Ethernet 802/LLC.

2 Заповнення полів статусу кадру при передачі кадрів з мереж FDDI або Token Ring у мережу Ethernet. Кадри FDDI і Token Ring мають два біти, що встановлюються станцією, який був адресований кадр, – біт розпізнавання адреси і біт копіювання кадру в буфер. При передачі комутатором кадру в іншу мережу немає стандартних правил для установлення цих бітів у кадрі, який повертається по кільцю до станції-відправника. Тому виробники комутаторів вирішують цю проблему кожний на свій розсуд.

3 Відкидання кадрів, що передаються з мереж FDDI або Token Ring в мережу Ethernet з розміром поля даних більше, ніж 1500 байтів. Надалі, не дочекавшись відповіді від станції призначення з мережі Ethernet, протокол верхнього рівня з мережі FDDI/Token Ring, можливо, зменшить розмір даних, що передаються в одному кадрі, і тоді комутатор зможе передавати кадри між цими вузлами. Іншим варіантом вирішення цієї проблеми є підтримка комутатором IP- фрагментації, але це вимагає, по-перше, реалізації в комутаторі протоколу мережного рівня, а по-друге, підтримки протоколу IP взаємодіючими вузлами з гетерогенних мереж.

4 Заповнення поля типу протоколу Ethernet DIX при переході кадрів з мереж FDDI/Token Ring, в яких це поле відсутнє, але зате є поля LLC/SNAP, які мають те ж поле типу і з тими самими значеннями, що і в полі типу протоколу Ethernet DIX. Якщо в мережі Ethernet є формати кадрів, відмінні від Ethernet DIX, вони також повинні мати поля LLC/SNAP.

5 Перерахунок контрольної суми кадру відповідно до сформованих значень службових полів кадру.

Висновки

Логічна структуризація мережі необхідна при побудові мереж середніх і великих розмірів. Використання загального розподіленого середовища прийнятне тільки для мережі, що складається приблизно з 10 комп'ютерів.

Розподіл мережі на логічні сегменти підвищує продуктивність, надійність, гнучкість побудови і керованість мережі.

Для логічної структуризації мережі використовуються мости/комутатори.

Застосування комутаторів дозволяє мережним адаптерам використати дуплексний режим роботи протоколів локальних мереж.

У дуплексному режимі для боротьби з перевантаженнями комутаторів використовується метод зворотного зв'язку. Він дозволяє припинити на деякий час надходження кадрів від безпосередніх сусідів переобтяженого комутатора.

При напівдуплексному режимі для боротьби з перевантаженнями використовуються два методи: агресивне захоплення середовища і зворотний тиск на кінцевий вузол.

Основними характеристиками продуктивності комутатора є: швидкість фільтрації кадрів, швидкість просування кадрів, загальна пропускна спроможність по всіх портах у мегабітах у секунду, затримка передачі кадру.

На характеристики продуктивності комутатора впливає: тип комутації «на льоту» або з повною буферизацією, розмір адресної таблиці, розмір буферів кадрів.

Контрольні питання:

1 Дайте визначення поняття «комутована локальна мережа».
2 Назвіть переваги мережі на розподіленому середовищі.
3 Назвіть недоліки мережі на розподіленому середовищі.
4 Що означає поняття «масштабованість мережі»?
5 Опишіть алгоритм прозорого моста.
6 Назвіть наслідки, до яких призводить наявність петлі в мережі.
7 Що таке комутатор?

8 Опишіть структуру комутатора EtherSwitch компанії Kalpana.

9 Опишіть принцип комутації портів і передачі кадру через комутаційну матрицю «на льоту».

10 Опишіть принцип передачі кадрів через комутатор з повною буферизацією.

11 Дайте визначення поняття «неблокучий комутатор».

12 Назвіть методи боротьби з перевантаженнями комутатора.

13 Опишіть суть методу зворотного тиску.

14 Опишіть метод агресивного захоплення середовища.

15 Опишіть особливості трансляції протоколів канального рівня.

4. Лабораторний практикум

4.1 Організація безпроводової мережі

Мета роботи: ознайомитись зі структурою стандарту IEEE 802.11 (безпроводові мережі), принципами їх побудови та набути практичних навичок настроювання безпроводової карти мережного адаптера і точки доступу.

Вступ

Розвиток безпроводових локальних мереж (WLAN), Bluetooth (мережі середніх і коротких відстаней) досить перспективний. Безпроводові мережі розгортаються в аеропортах, університетах, готелях, ресторанах, на підприємствах. Точкою відліку у сфері розроблення стандартів безпроводових мереж є створення всесвітньою організацією IEEE комітету 802.11 в 1990 році. Значний імпульс розвитку безпроводових технологій дала Всесвітня павутина й ідея роботи в Мережі за допомогою безпроводових пристроїв. Наприкінці 90-х років користувачам була запропонована WAP-послуга, що спочатку не викликала великого інтересу. Це були основні

інформаційні послуги – новини, погода, усілякі розклади тощо. Також спочатку не мали попит і Bluetooth, і WLAN – в основному через високу вартість цих засобів зв'язку. Однак у міру зниження цін зростає й інтерес з боку рядових користувачів.

Лабораторна робота «Організація безпроводової мережі» ставить метою вивчення основ організації безпроводової мережі, набуття базових навичок з настроювання її компонентів.

4.1.1 Мережі RadioEthernet

Безпроводові мережі RadioEthernet одержали масове поширення завдяки прийняттю в 1997 р. Інститутом інженерів електротехніки й електроніки (IEEE) базового стандарту IEEE 802.11, що визначив протоколи, які стали основою для створення сучасних високошвидкісних і надійних стандартів.

Специфікації RadioEthernet

Основними протоколами стандарту IEEE 802.11 є MAC (Media Access Control) – протокол управління доступу до середовища й PHY (physical layer protocol – протокол фізичного рівня) – протокол передачі даних на фізичному рівні, що визначає середовище передачі даних.

Протокол доступу до середовища (MAC)

Стандартом 802.11 визначений єдиний підрівень MAC, взаємодіючий із трьома типами протоколів фізичного рівня, що відповідають різним технологіям передачі сигналів – по радіоканалах у діапазоні 2,4 ГГц із широкосмуговою модуляцією із прямим розширенням спектра (DSSS) і перескоком частоти (FHSS), а також за допомогою інфрачервоного випромінювання. Специфікаціями стандарту передбачені два значення швидкості передачі даних – 1Мбіт/с і 2 Мбіт/с.

У порівнянні із проводовими ЛКМ Ethernet можливості підрівня MAC розширені за рахунок включення в нього ряду функцій, що зазвичай виконуються протоколами більш високого рівня, зокрема процедур фрагментації й ретрансляції пакетів. Це викликано прагненням підвищити ефективну пропускну

спраможність системи завдяки зниженню накладних витрат на повторну передачу пакетів.

Як основний метод доступу до середовища стандартом 802.11 визначений механізм CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance – множинний доступ з виявленням несучої й запобіганням колізіям).

Керування живленням для економії енергоресурсів мобільних робочих станцій, використовуваних у безпроводових ЛКМ, стандартом 802.11 передбачений механізм перемикання станцій у так званий пасивний режим з мінімальним споживанням потужності.

Архітектура й компоненти мережі

В основу стандарту 802.11 покладена стільникова архітектура, причому мережа може складатися як з однієї, так і декількох чарунок, що управляється базовою станцією, називаною точкою доступу (Access Point, AP), що разом з робочими станціями, що перебувають у межах радіуса її дії, утворює базову зону обслуговування (Basic Service Set, BSS). Точки доступу багатостільникової мережі взаємодіють між собою через розподільну систему (Distribution System, DS), що являє собою еквівалент магістрального сегмента кабельних ЛКМ. Вся інфраструктура, що включає точки доступу й розподільну систему, утворює розширену зону обслуговування (Extended Service Set).

Стандартом передбачений також одностільниковий варіант безпроводової мережі, що може бути реалізований і без точки доступу, при цьому частина її функцій виконуються безпосередньо робочими станціями.

Роумінг

Для забезпечення переходу мобільних робочих станцій із зони дії однієї точки доступу до іншої в багатостільникових системах передбачені спеціальні процедури сканування (активного й пасивного прослуховування ефіру) і приєднання (Association), однак строгих специфікацій щодо реалізації роумінгу стандарт 802.11 не передбачає.

Забезпечення безпеки

Для захисту WLAN стандартом IEEE 802.11 передбачений цілий комплекс заходів безпеки передачі даних під загальною назвою Wired Equivalent Privacy (WEP). Він включає засоби протидії несанкціонованому доступу до мережі (механізми й процедури аутентифікації), а також запобігання перехопленню інформації (шифрування).

Перспективи розвитку

У стандарт 802.11 згодом можуть бути включені два інших частотних діапазони. FCC розпорядилося виділити смугу в 20 МГц для PCS у районі 1,9 ГГц для безліцензійних служб. Усередині цієї смуги 10 МГц будуть виділені для синхронного доступу й 10 МГц – для асинхронного.

Інша можлива смуга частот розташовується в діапазоні між 5,150 ГГц і 5,250 ГГц, зарезервованому в усьому світі для НВЧ-систем посадки літальних апаратів (MLS). Однак Глобальна система позиціонування (GPS) швидко витісняє MLS-технологію. Таким чином, частоти MLS, можливо, стануть доступними для безпроводових локальних мереж.

У Європі відповідні служби вже дозволили Європейському Інституту Стандартів Зв'язку використати зарезервовані частотні смуги MLS у проекті, названому "Локальна високопродуктивна радіомережа" (HIPERAN). У результаті фізична підгрупа 802.11 включила в розгляд діапазони 1,9 ГГЦ і 5,2 Ггц на додаток до ISM-діапазону 2,4 ГГц.

Комітет 802.11, однак, не одержав жодної пропозиції щодо розроблення фізичного стандарту в діапазонах 1,9 ГГц і 5,2 ГГц. Відсутність інтересу до діапазону 1,9 ГГц викликана, можливо, тим, що він буде доступний тільки у Сполучених Штатах, до того ж не так просто домогтися високої швидкості передачі даних у смузі шириною 10 Мгц. Крім того, знадобиться багато часу на розчищення смуги для використання компонентів 802.11.

Чорновий проект стандарту 802.11 включає також опис фізичного рівня в інфрачервоному діапазоні для малогабаритного устаткування й низькошвидкістних додатків. Базовий темп даних для цього методу 1 Мбіт/с при використанні 16 ppm (імпульсної

позиційної модуляції) і підвищена швидкість 2 Мбіт/с при використанні 4 ppm.

На рівні MAC стандарт дозволяє декільком станціям ділити між собою один фізичний діапазон частот. Підгрупа MAC робочої групи 802.11 зосередила зусилля на розробленні єдиного MAC-рівня для стандарту 802.11. Чернетка MAC-стандарту містить все необхідне для підтримки асинхронних систем і систем із прив'язкою за часом (TSB-систем), а також узгодження різних темпів для кожного фізичного рівня.

4.1.2 Методи передачі послідовностей у RadioEthernet

Метод прямої послідовності (DSSS)

У методі прямої послідовності сигнал, що несе дані користувача, комбінується з високошвидкісною послідовністю бітів або послідовністю чипа. У результаті послідовність сигналів значно швидше вихідної. Назва даного методу визначила ту обставину, що процес розподілу застосовується безпосередньо до кожного біта інформації.

Ефективність систем з безперервним розподілом визначається виграшем методу (processing gain) або коефіцієнтом розподілу (spreading ratio), рівним відношенню темпу передачі даних (data rate) сигналу з розподіленим спектром до темпу передачі вихідного сигналу. Мінімально припустимий коефіцієнт розподілу в США і Японії дорівнює 10. Щоб виключити, наскільки це можливо, перехресні перешкоди, робоча група 802.11 установила мінімальний коефіцієнт 11.

У порівнянні з методом частотних стрибків, метод прямої послідовності менш підданий перешкодам через багаторазові відбиття радіохвиль від навколишніх предметів. Системи із прямою послідовністю, у свою чергу, гірше протистоять потужним перешкодам, що виникають через близькість іншої безпроводової мережі.

Вплив перешкоди в малому інтервалі діапазону при прямій послідовності призводить до часткового перекручування переданих даних. За допомогою схеми демодуляції послідовних

сигналів дані легко відновити, чого не можна сказати про сигнал, що перекручений потужними перешкодами.

Головний недолік методу прямої послідовності полягає в тім, що заснована на ньому система споживає у два – три рази більше енергії, ніж аналогічна, що використовує метод частотних стрибків. Це може викликати серйозні проблеми при впровадженні безпроводових адаптерів для портативних комп'ютерів.

У березні 1993 року комітет 802.11 почав приймати пропозиції щодо фізичної частини стандарту, що стосується використання методу прямої послідовності. Після багатьох дебатів комітет погодився включити в стандарт главу про використання прямої послідовності з розподіленим спектром.

Фізична частина цього стандарту включає два темпи передачі даних: 2 Мбіт/с, що використовує модуляцію з диференціальним четвірковим перемиканням зі зрушенням фази (DQPSK), і 1 Мбіт/с із диференціальним двійковим перемиканням зі зрушенням фази (DBPSK). Стандарт визначає сім каналів прямої послідовності, один із яких виділений спеціально для Японії, а інші шість – для Сполучених Штатів і Європи. Пари каналів можуть працювати, не викликаючи взаємних перешкод, крім того, всі три пари можуть використовуватися одночасно при належному плануванні частот для запобігання конфліктів.

Метод частотних стрибків (FHSS)

На противагу методу прямої послідовності, передавачі за методом частотних стрибків посилають сигнали, перемикаючись із однієї частоти на іншу; вони відправляють по трохи біт на кожній частоті, перш ніж перемкнутися на наступну. Системи із стрибковою міняють частоти за схемою, що задається випадково. У дійсності ж використовується схема із заздалегідь певною послідовністю стрибків, іменована звичайно каналом розподіленого спектра стрибкових частот.

Системи розподіленого спектра частотних стрибків більше придатні для застосування в портативних пристроях: вони дешевші в реалізації й не споживають так багато енергії, як їхні аналоги з безперервною послідовністю. Однак ці системи

змушені передавати заново дані, перекручені при передачі на одній із частот у послідовності, оскільки метод частотних стрибків менш стійкий до перешкод, викликаних відбиттями сигналів і інших джерел.

Комітет 802.11 визначив на фізичному рівні для методу частотних стрибків темп даних 1 Мбіт/с із використанням дворівневого гаусового перемикання частот (GFSK). Ця специфікація описує 79 центральних частот для каналів, виділених для Сполучених Штатів, з яких визначаються три набори з 22 частот.

4.1.3 Структура комітету 802.11

Існують такі специфікації сімейства 802.11:

802.11a – розширення специфікації 802.11, застосовується для безпроводових локальних мереж і забезпечує до 54 Мбіт/с у смузі 5 ГГц. У специфікації 802.11a використовується ортогональний частотний поділ сигналів і мультиплексування замість FHSS або DSSS.

802.11b (відомий також як 802.11 High Rate або Wi-Fi розширення 802.11, забезпечує 11 Мбіт/с (а також 5.5, 2 і 1 Мбіт/с) у смузі 2.4 ГГц. 802.11b використовує тільки DSSS.

802.11d. Специфікація IEEE, що дозволяє вносити конфігураційні зміни на рівні контролю доступу до мережі (MAC – media access control) для забезпечення сумісності із правилами (законами) країни, у якій передбачається використання мережі.

802.11e. Стандарт IEEE, що додає сервіс QoS (якості сервісу) і підтримку мультимедіа до існуючих безпроводових мереж 802.11b, 802.11g, і 802.11a.

802.11g забезпечує 20 (і більше) Мбіт/с у смузі 2.4 ГГц.

802.11h підтримує вимоги динамічного вибору частоти (DFS – Dynamic Frequency Selection) і контролю потужності передачі (TPC – Transmit Power Control) для забезпечення співіснування Wi-Fi і з іншими радіопристроями, що працюють на частоті 5 ГГц.

802.11i. Стандарт IEEE, що визначає механізми безпеки для мереж 802.11. Описує застосування блокового шифрування AES (Advanced Encryption Standard). Також стандарт включає нововведення в управлінні ключами, аутентифікації

користувачів за допомогою 802.1x і у функціях контролю цілісності заголовків.

802.11j. Специфікація IEEE для безпроводових мереж, що забезпечує відповідність японським вимогам до безпроводових мереж в аспектах потужності передавача, режимів роботи, розподілу каналів тощо.

802.11n. Робоча група комітету 802.11n, метою якої є розроблення стандарту безпроводових мереж з високою швидкістю передачі (від 100 Мбіт/с).

4.1.4 Точка доступу

Точка доступу (AP – access point) призначена для формування середовища передачі безпроводової мережі (БЛОМ).

Режими роботи точки доступу

AP може працювати в трьох режимах: «точка доступу» (AP-mode), «система поширення безпроводового зв'язку» (WDS – Wireless Distribution System), комбінованому. Режим «точка доступу» – всі вузли, що мають безпроводові мережні адаптери, взаємодіють через точку доступу (рисунок 4.1), у цьому режимі AP аналогічний концентратору в провідних мережах.

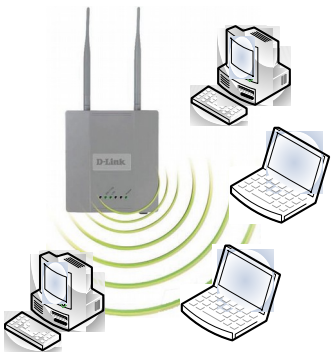

Рисунок 4.1 – Режим «точка доступу»

У режимі AP-mode всі безпроводові пристрої мають однаковий ідентифікатор безпроводової мережі (SSID - Service Set Identifier). SSID – унікальне найменування безпроводової мережі, що відрізняє одну БЛКМ від іншої. У настройках всіх пристроїв, які повинні працювати в одній безпроводовій мережі, має бути зазначений однаковий SSID. SSID вибирається адміністратором мережі самостійно й може містити до 32 символів. Значення SSID на клієнтському пристрої, рівне «ANY», означає можливість підключення до будь-якої доступної мережі.

Режим WDS служить для збільшення площі покриття безпроводової мережі, тобто аналогічна репитеру. У комбінованому режимі (WDS with AP) точка доступу поєднує обидва режими (рисунок 4.2).

В режимі WDS точка доступу підтримує декілька SSID, чим досягається об'єднання декількох БЛКМ.

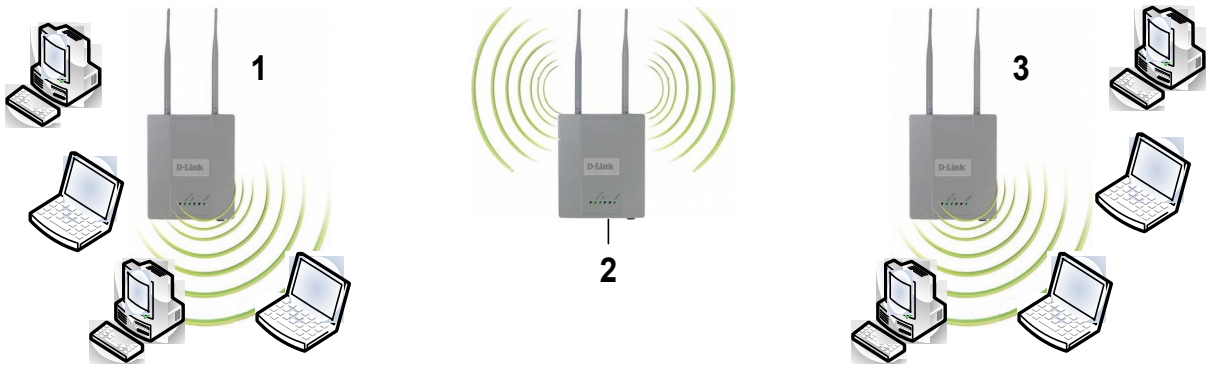

Рисунок 4.2 – Інфраструктура безпроводової мережі. AP 1 і 3 працюють у режимі «WDS with AP», AP 2 – у режимі «WDS»

Захист даних

Точки доступу підтримують декілька методів захисту даних.WEP (Wired Equivalent Privacy) – протокол безпеки для мереж Wi-Fi, визначений стандартом IEEE 802.11b. WEP був розроблений для забезпечення рівня безпеки, аналогічного тому, який існує в провідних локальних мережах. WEP забезпечує шифрування даних, переданих по радіоканалу. Основним його

недоліком є використання статичного ключа для шифрування даних. Зловмисник може тим або іншим способом довідатися про цей ключ і одержати доступ до безпроводової мережі. На зміну WEP приходять більш надійні протоколи WPA і 802.11i. Проте протокол WEP продовжує широко використовуватися, тому що не всі пристрої підтримують нові протоколи безпеки.

При використанні протоколу WEP можливі два типи взаємної аутентифікації безпроводових пристроїв (Authentication Type): Open System і Shared Key. При аутентифікації Open System до безпроводової мережі може підключитися будь-який пристрій з відповідним значенням (SSID). Ключі WEP у процесі аутентифікації не перевіряються. Аутентифікація типу Shared Key вимагає, щоб точка доступу й безпроводовий адаптер мали однаковий ключ WEP.

802.1x. Протокол, впроваджений стандартом IEEE 802.1x, використовується при аутентифікації й авторизації користувачів з наступним наданням доступу до середовища передачі даних. При цьому застосовуються динамічні ключі замість статичних, використовуваних у WEP. Протокол припускає спільну роботу трьох протоколів: EAP (Extensible Authentication Protocol) – розширюваний протокол аутентифікації; TLS (Transport Layer Security) – протокол безпеки транспортного рівня; RADIUS (Remote Authentication Dial-In User Server) – сервер аутентифікації вилучених користувачів. Запит користувача на доступ до мережі переадресовується на сервер RADIUS, що виконує аутентифікацію й дозволяє або забороняє доступ. Протокол 802.1x передбачає часту зміну ключів шифрування, що дуже ускладнює зламування мережі. Великим недоліком протоколу 802.1x для користувачів домашніх і малих офісів є вимога обов'язкової наявності сервера RADIUS.

WPA, 802.11i. У цей час існують два дуже схожих стандарти аутентифікації й шифрування в мережах Wi-Fi – WPA і 802.11i. WPA (Wi-Fi Protected Access) був розроблений у Wi-Fi Alliance як рішення, яке можна застосувати негайно, не чекаючи завершення тривалої процедури ратифікації 802.11i в IEEE. Обидва протоколи використовують механізм 802.1x для забезпечення надійної аутентифікації, обидва використовують сильні алгоритми шифрування, обидва призначені для заміни протоколу

WEP. Основна відмінність двох стандартів полягає у використанні різних механізмів шифрування. В WPA застосовується Temporal Key Integrity Protocol (TKIP), що так само, як і WEP, використовує шифр RC4, але значно більш безпечним способом. Стандарт 802.11i передбачає шифрування за допомогою алгоритмів, заснованих на технології Advanced Encryption Standard (AES), і забезпечує найбільш стійке шифрування з доступних у цей час. Стандартами WPA і 802.11i передбачений режим Pre-Shared Key (PSK), що дозволяє обійтися без сервера RADIUS.

4.1.5 Настроювання точки доступу D-Link DWL-3200AP

Точка доступу може конфігуруватися за допомогою утиліти, яка поставляється разом з нею або через WEB-інтерфейс у браузері. Обидва інтерфейси повністю охоплюють настроювання пристрою й відрізняються лише зовнішнім виглядом.

Виробники настійно рекомендують робити настроювання через вузол, що підключений до AP через проводовий інтерфейс.

Розглянемо настроювання через WEB-інтерфейс (рисунок 4.3). Для його виклику відкрийте браузер і в рядку адреси наберіть *http://<адреса_AP>*, де *адреса_AP* – IP-адреса точки доступу, за замовчуванням – 192.168.0.1. Буде запитане ім'я користувача й пароль, заводські настройки: користувач – admin, пароль – admin.

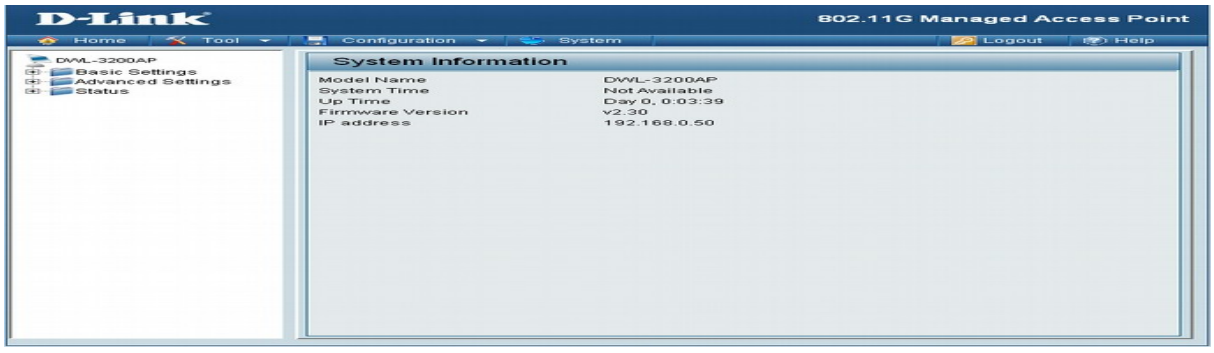

Рисунок 4.3 – WEB-інтерфейс настроювання точки доступу D-Link DWL-3200 AP

На першій сторінці зазначена марка (Model Name), системний час і час роботи з моменту включення (System, Up time), версія програмного забезпечення (Firmware version) і мережна адреса (IP address).

Загальні настройки системи D-Link для (Wireless Settings) проводних установок подано на рисунку 4.4. На сторінці вказується режим роботи AP (поточний – access point), SSID (D-Link), SSID broadcast - широкомовне розсилання SSID - AP періодично передає свій ідентифікатор, відключення цього режиму дозволяє сховати SSID і тим самим обмежити доступ до безпроводової мережі, однак може утруднити й санкціонованим користувачам відновлювати з'єднання при його розриві. Канал (Channel) дозволяє вибрати канал (див. розділ 4.1).

Рисунок 4.4 – Загальні настройки D-Link

Аутентифікация (Autentification) – вибирається за алгоритмом захисту каналу (обраний WPA-personal – захист по

алгоритму WPA). У цьому випадку RADIUS-сервер не потрібний, на відміну від алгоритму WPA-enterprise. Область вікна PassPhrase Settings відрізняється для різних алгоритмів захисту. Для алгоритму WPA-personal: cipher type – тип шифру (Auto, TKIP, AES); інтервал відновлення групи ключів (Group key update interval); Pass Phrase – фраза-пароль, від 8 до 64 символів. Чим менше інтервал відновлення групи ключів, тим менше часу в зломщиків на підбір ключа, але занадто часто знижується продуктивність мережі через накладні витрати на передачу ключів і перенастроювання процедур шифрування.

Якщо ви змінюєте настройки, то, щоб вони набули чинності, необхідно натиснути кнопку «Apply».

Сторінка Basic settings\LAN Settings – основні настройки\ настройки ЛКМ (рисунок 4.5).

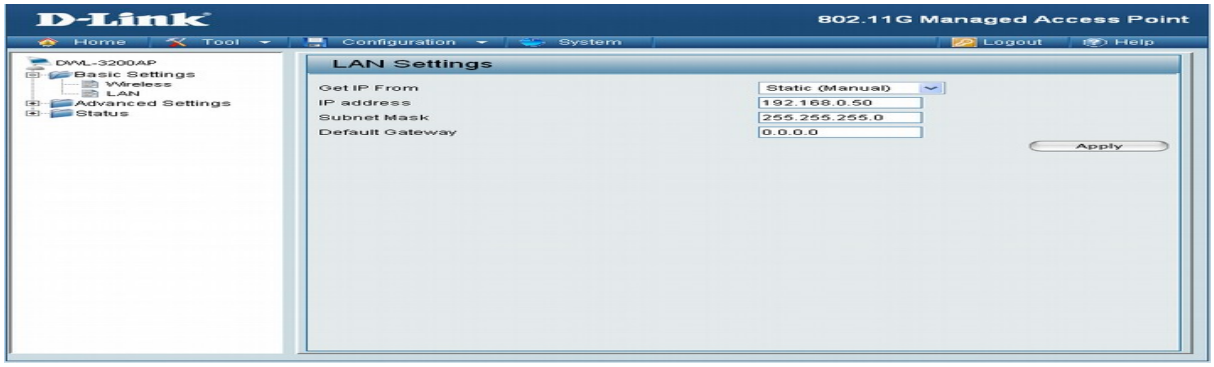

Рисунок 4.5 – Настроювання ЛКМ

Сторінка настройок ЛКМ містить настройки інтерфейсу із провідною мережею, Get IP From - «одержати адресу від...», дозволяє вибрати статичну (Static) адресу (поля IP address і Subnet mask) або вказати адресу DHCP-сервера. Крім того, AP сама може виступати в ролі DHCP-сервера (рисунок 4.6) який настроюється на сторінці Advanced settings\DHCP Dynamic pools (Розширені настроювання\Динамічний пул адрес DHCP).

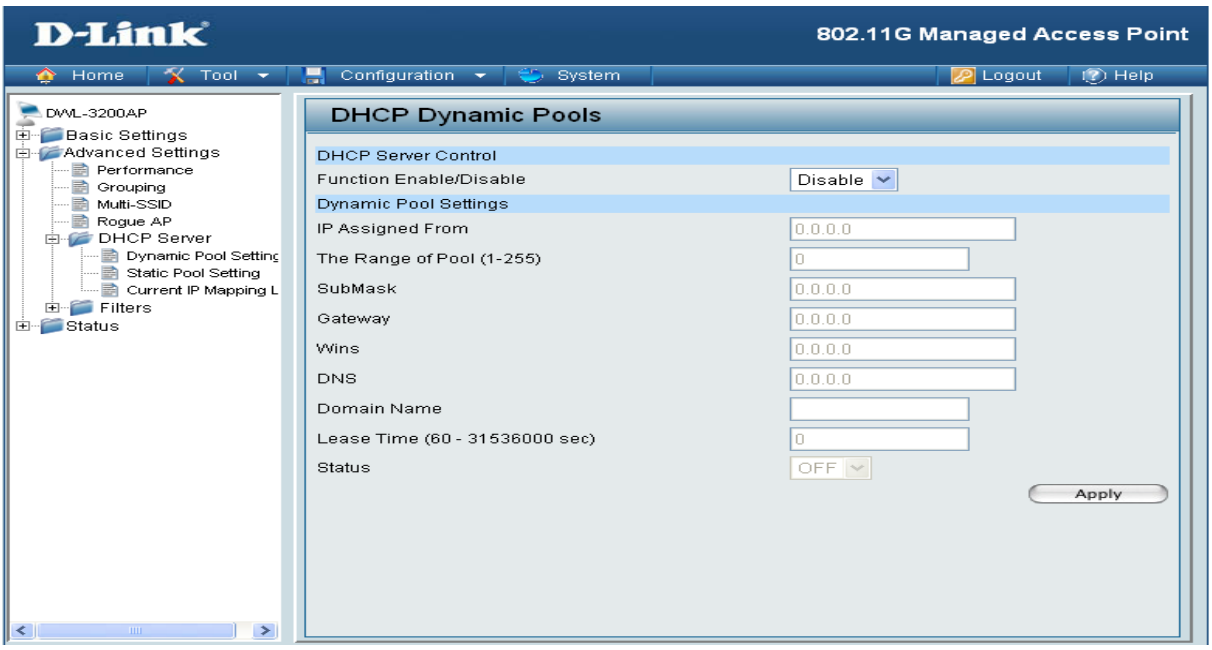

Рисунок 4.6 – Настроювання DHCP-сервера

Настройки включають такі параметри: IP assigned from, SubMask - параметри виділюваних адрес, базова адреса мережі й маска підмережі; The Range of Pool, обсяг пула – кількість вузлів підтримуваних DHCP-сервером; Geteway, WINS, DNS – адреси відповідних серверів мережі; Lease Time – час оренди адреси, після закінчення цього часу клієнт надсилає запит на нову IP-адресу.

Крім динамічного присвоювання IP-адрес, можна настроїти статичне зв'язування IP-адреса – MAC-адреса у вікні Advanced settings\Static Pool Settings (рисунок 4.7), це дозволяє підвищити надійність і захищеність БЛОМ.

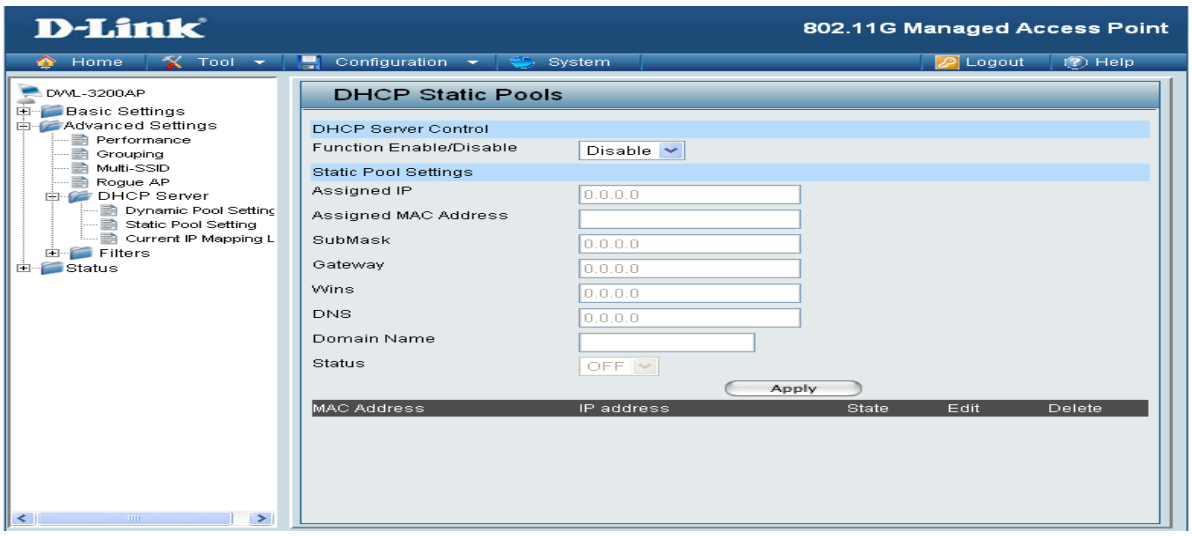

Рисунок 4.7 – Статичне зв'язування IP-адреса – MAC-адреса

Поля аналогічні попередній сторінці. Заповнивши поля й натиснувши кнопку Apply, ви побачите додатковий запис у таблиці, розташованій внизу вікна.

Довідатися MAC-адресу можна, наприклад, скориставшись командою ipconfig із ключем -all. Для цього необхідно викликати консоль (CMD) (у меню пуск вибрати пункт «Виконати...», у вікні, що з'явилося, увести cmd).

Якщо після експериментування з настройками точки доступу ви втратили з нею зв'язок або забули пароль, або відбувся збій у роботі AP, можна скористатися кнопкою апаратного скидання, що поверне стан AP до заводських параметрів. Розташування кнопки на D-Link DWL-3200 AP зображено на рисунку 4.8.

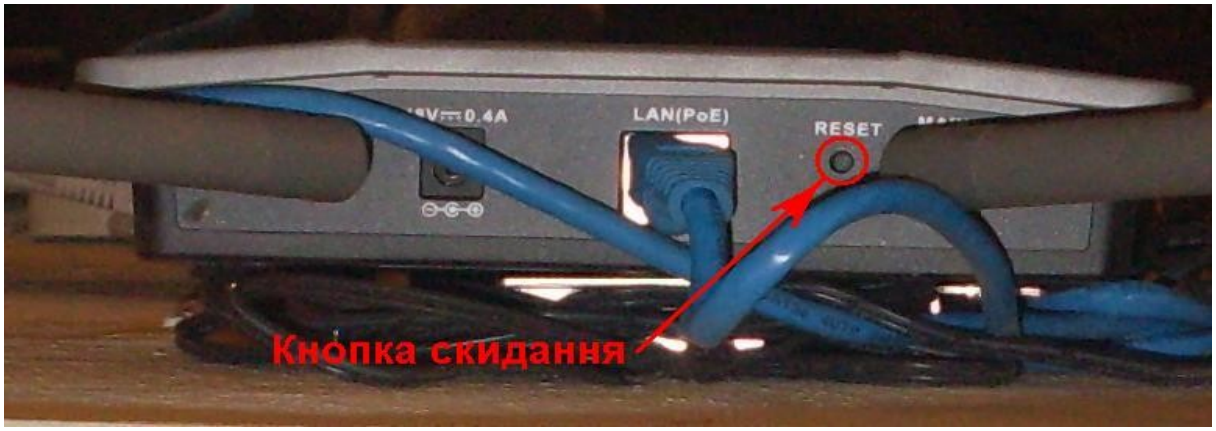

Рисунок 4.8 – Розташування кнопки скидання

4.1.6 Конфігурування плати безпроводового мережного адаптера

Установлення безпроводового мережного адаптера аналогічна установці проводового (див. лабораторну роботу «Конфігурація плати мережного адаптера»). Після установлення драйвера в системному треї з'являється піктограма, що свідчить про наявність безпроводового адаптера й відображує стан підключення. Натиснувши правою клавішею миші на піктограмі й вибравши пункт «View Available Wireless Networks» («Відобразити доступні безпроводові мережі») (рисунок 4.9), можна викликати вікно, що відображує безпроводові мережі, «видимі» адаптером (рисунок 4.10).

Натиснувши кнопку Connect (Підключити), ви можете спробувати підключитися до мережі.

Рисунок 4.9 – Виклик вікна властивостей безпроводового підключення

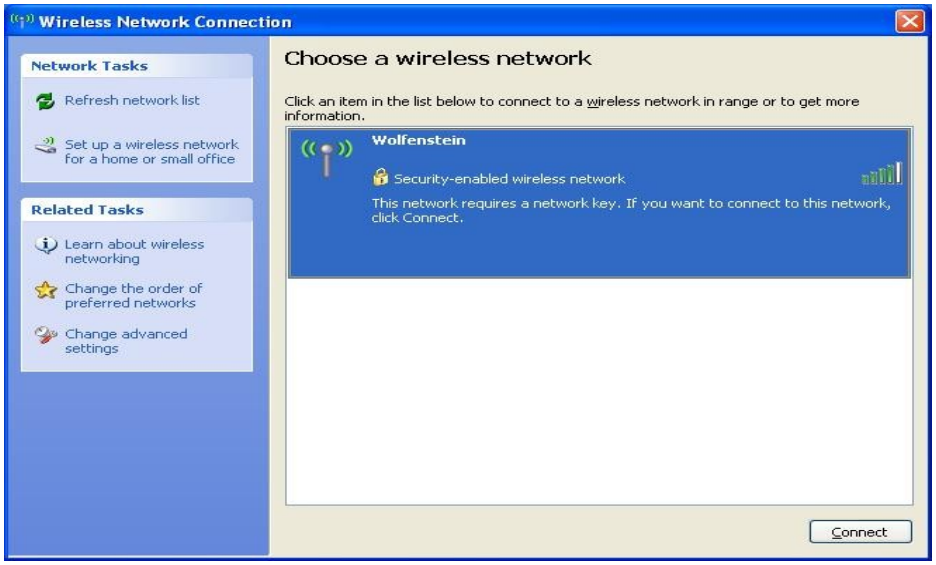

Рисунок 4.10 – Вікно, що відображує «видимі» мережі (видно мережу з SSID «Wolfenstein», що використовує захист (security-enabled))

Вікно настроювання безпроводового зв'язку (рисунок 4.11) викликається звичайним шляхом: «Панель керування»>«Мережні підключення» або ж з меню, що випадає, зображеного на рисунку 4.9, вибором пункту Open Network Connections (Відкриті мережні підключення).

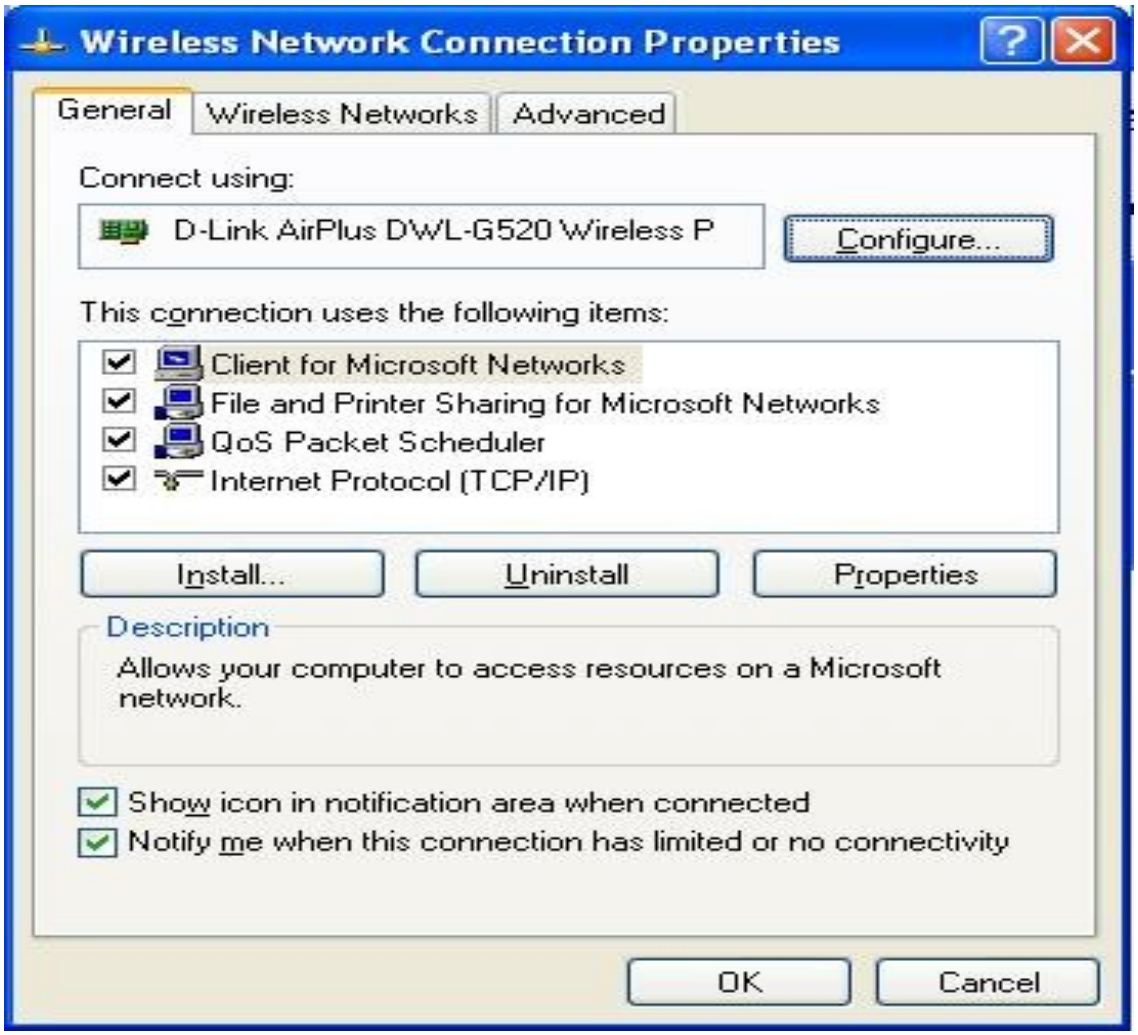

Рисунок 4.11 – Вікно властивостей безпроводового підключення

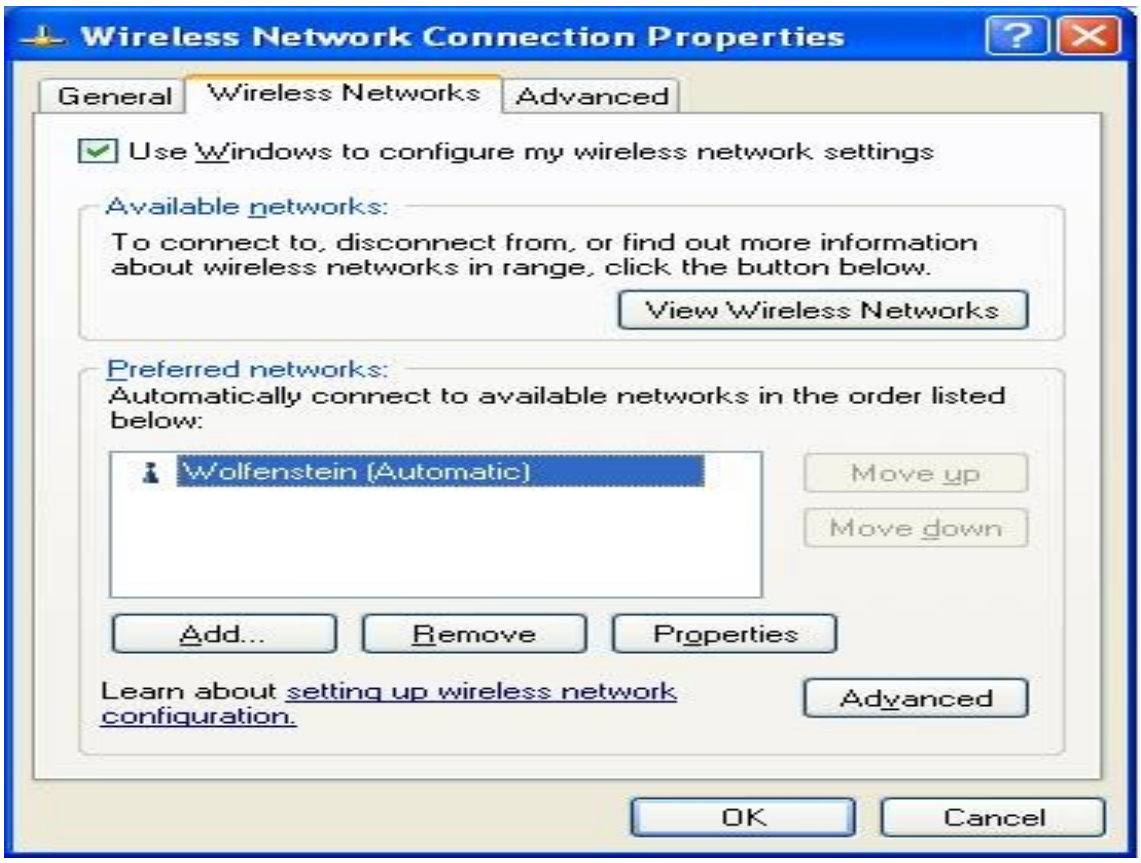

Рисунок 4.12 – Закладка «Безпроводові мережі (Wireless network)»

Натискання кнопки «Перегляд безпроводових мереж (View Wireless Networks)» у групі «Доступні мережі (Available networks)» викликає вікно, що відображає безпроводові мережі, «видимі»адаптером (рисунок 4.12).

Список у групі «Довірені мережі (Preferred networks)» відображає мережі, для яких збережені настройки підключення (при цьому вони не обов'язково перебувають у зоні видимості). Якщо в зоні видимості перебуває кілька мереж, для яких збережені настройки підключення, то підключення здійснюється до мережі, що перебуває в списку вище. При натисканні кнопки «Додати... (Add...)» або «Властивості (Properties)» виводиться вікно властивостей безпроводової мережі (рисунок 4.13).

Рисунок 4.13 – Вікно властивостей підключення до обраної безпроводової мережі

У вікні настроюються (відображаються) SSID мережі й параметри захисту. Залежно від обраного методу захисту додаткові параметри вводяться також у закладці «Безпека (Autentication)». У закладці «Підключення (Connection)» доступна опція автоматичного підключення, якщо мережа в зоні видимості (Connect if this network is in range).

4.1.7 Завдання та зміст звіту

1 Використовуючи робочу станцію, підключену до точки доступу через кабель, викликати в браузері інтерфейс конфігурації.

2 Установити IP-адресу точки доступу 210.210.210.1.

3 Настроїти точку доступу на використання методу шифрування WPA-PSK.

4 Включити DHCP-сервер, обмежити кількість вузлів десятьма.

5 Перемістится на робочу станцію із установленим безпроводовим мережним адаптером, сконфігурувати його.

6 Скориставшись командою ipconfig, з'ясувати MAC-адресу безпроводового мережного адаптера й IP-адреса привласнену безпроводовому підключенню DHCP-сервером.

7 Виключити DHCP-сервер на точці доступу й змінити конфігурацію безпроводового підключення на робочій станції з урахуванням цього.

8 Наприкінці заняття делегувати студента для скидання точки доступу до заводських настройок.

Звіт з лабораторної роботи має містити короткий опис дій, необхідних для виконання завдання. В частині звіту, що стосується пункту 6 завдання, навести знімок екрана (screenshot), отриманий у результаті виконання.

Контрольні питання

1 Який підкомітет проекту 802 створений для стандартизації безпроводових мереж?

2 Основний метод доступу до середовища передачі в безпроводових мережах.

3 Який частотний діапазон виділений для мереж RadioEthernet?

4 Що називають коефіцієнтом розподілу (spreading ratio)?

5 Що таке WEP?

6 Яка фізична швидкість передачі в мережах RadioEthernet?

7 Що таке точка доступу?

8 Перелічте режими роботи точки доступу.

9 Що таке SSID?

10 Перелічте основні параметри БЛОМ, які необхідно знати для підключення до неї.

11 У чому полягає відмінність аутентифікації Shared Key від Open System?

12 Які задачі виконує RADIUS-сервер?

13 У чому відмінність WPA-personal від WPA-enterprise?

14 Як переглянути список доступних безпроводових мереж?

15 Що таке «Довірені мережі (Preferred networks)»?

16 Що означають рядки, виведені на екран у пункті 6 завдання?

4.2 Настроювання Інтернету в операційній системі Windows XP

Мета роботи: Ознайомитися з основними інформаційними послугами, що надаються Інтернетом користувачам, а також набути практичних навичок з організації доступу до Інтернету і підключення електронної пошти.

4.2.1 Настроювання Інтернету

Інтернет – це глобальна комп'ютерна мережа, що містить безліч вузлів у різних країнах, що надають множину інформаційних послуг. У цей час в Інтернеті існує ряд сервісів, що забезпечують роботу з усім спектром інформаційних ресурсів. До найбільш відомих можна віднести такі:

- Word Wide Web (WWW Всесвітня павутина) гіпертекстова система, яка призначена для інтеграції різних мережних ресурсів в єдиний інформаційний простір;
- електронна пошта (E-mail), що забезпечує обмін повідомленнями однієї людини з одним або декількома абонентами;

- телеконференції або групи новин (Usenet), що забезпечують колективний обмін повідомленнями;
- сервіс FTP – система файлових архівів, що забезпечує зберігання і пересилку файлів різних типів;
- сервіс Telnet, призначений для управління віддаленими комп'ютерами в термінальному режимі;
- сервіс DNS, або система доменних імен, що забезпечує використання для адресації вузлів мережі символьних (мнемонічних) імен замість числових адрес;
- сервіс IRC, призначений для підтримки текстового спілкування в реальному часі (chat);
- потокове мультимедіа.

Перелічені вище сервіси належать до стандартних. Це означає, що принципи побудови клієнтського і серверного програмного забезпечення, а також протоколи взаємодії сформульовані у вигляді міжнародних стандартів. Отже, розробники програмного забезпечення при практичній реалізації зобов'язані витримувати загальні технічні вимоги.

Поряд із стандартними сервісами існують і нестандартні, що являють собою оригінальну розробку тієї або іншої компанії. Як приклад можна навести різні системи типу ICQ, системи Інтернет-телефонії, трансляції радіо і відео тощо. Принциповою особливістю таких систем є відсутність міжнародних стандартів, що може призвести до виникнення технічних конфліктів з іншими подібними сервісами.

Для стандартних сервісів також стандартизується і інтерфейс з протоколами транспортного рівня. Зокрема, за кожним програмним сервісом резервуються стандартні номери TCP- та UDP-портів, які залишаються незмінними незалежно від особливостей тієї або іншої фірмової реалізації як компонентів сервісу, так і транспортних протоколів. Це пояснюється тим, що, по-перше, на призначеному для користувача вузлі може функціонувати декілька копій клієнтської програми, і кожна з них має однозначно ідентифікуватися транспортним протоколом, тобто за кожною копією повинен бути однозначно закріплений свій унікальний номер порту; а по-друге, клієнту важлива регламентація портів сервера, щоб знати, куди направляти запит.

Тільки при таких умовах сервер зможе відповісти клієнту, дізнавшись адресу із запиту, що надійшов.

У цей час до найбільш популярних послуг Інтернету можна віднести такі:

- Всесвітня павутина (веб-форуми, блоги, WiKi-проекти, інтернет-магазини, інтернет-аукціони, соціальні мережі);
- електронна пошта і списки розсилки;
- групи новин (в основному Usenet);
- мережі для обміну файлами;
- електронні платіжні системи;
- інтернет-радіо;
- інтернет-телебачення;
- IP-телефонія;
- FTP-сервери;
- IRC (реалізовано також як веб-чати);
- пошукові системи;
- інтернет-реклама;
- віддалені термінали;
- багатовикористовувані ігри.

Раніше, ніж отримати можливість користуватися інформаційними послугами Інтернету, до нього необхідно підключитися. Підключення до Інтернету може здійснюватися декількома способами. Найбільш поширений: підключення комп'ютера безпосередньо до провайдера. Провайдер – це фірма, що надає доступ до Інтернету. Другий варіант підключення через локальну мережу.

4.2.2 Створення з'єднання з Інтернетом через провайдера

4.2.2.1 Настроювання модема і створення з'єднання

Для організації зв'язку комп'ютера, що підключається до Інтернету через провайдера, він (комп'ютер) має бути оснащений модемом. Модем – це пристрій, що дозволяє віддаленим один від

одного комп'ютерам обмінюватися інформацією по телефонних лініях. Швидкість передачі даних залежить від продуктивності модема, яка, у свою чергу, залежить від побудови модему і протоколів, що використовуються. Крім основних функцій, більшість сучасних модемів виконують і ряд додаткових: відправляти/приймати факси (факс-модеми), підтримувати голосовий зв'язок (голосові модеми).

Оскільки процедури настроювання модема не передбачаються даною лабораторною роботою (бажаючі їх освоїти можуть скористатися докладними інструкціями, поданими, наприклад, в [2]), то будемо вважати, що модем настроєний і розглянемо схему зв'язку комп'ютера з Інтернетом через провайдера (рисунок 4.14).

Перед підключенням до Інтернету заздалегідь необхідно купити або Інтернет-карту відповідного провайдера, або укласти з провайдером договір. В обох випадках (і в інтернет-карті, і в договорі) мають бути вказані такі параметри:

- номер телефону для виходу в Інтернет;
- ім'я користувача і пароль;
- можливі додаткові параметри.

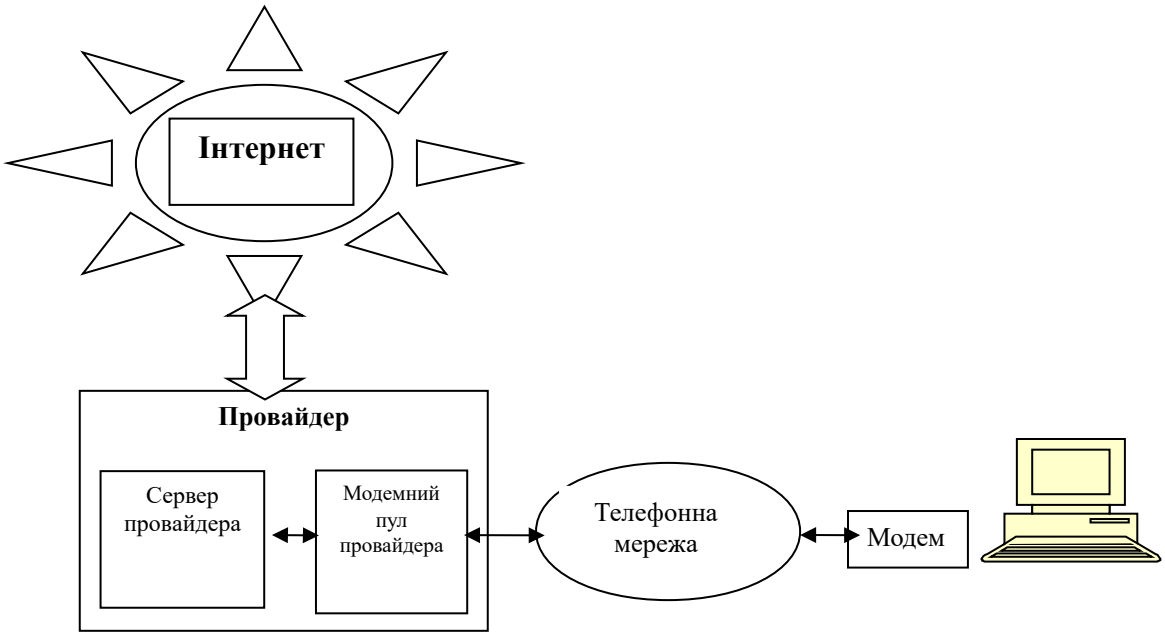

Рисунок 4.14 – З’єднання комп’ютера з Інтернетом за допомогою провайдера

Для створення підключення необхідно відкрити папку «Мережне підключення». У вікні, що відкрилося (рисунок 4.15), знайти посилання на програму «Мастер нового подключения», послідовно відповідаючи на питання якої і створюється з'єднання.

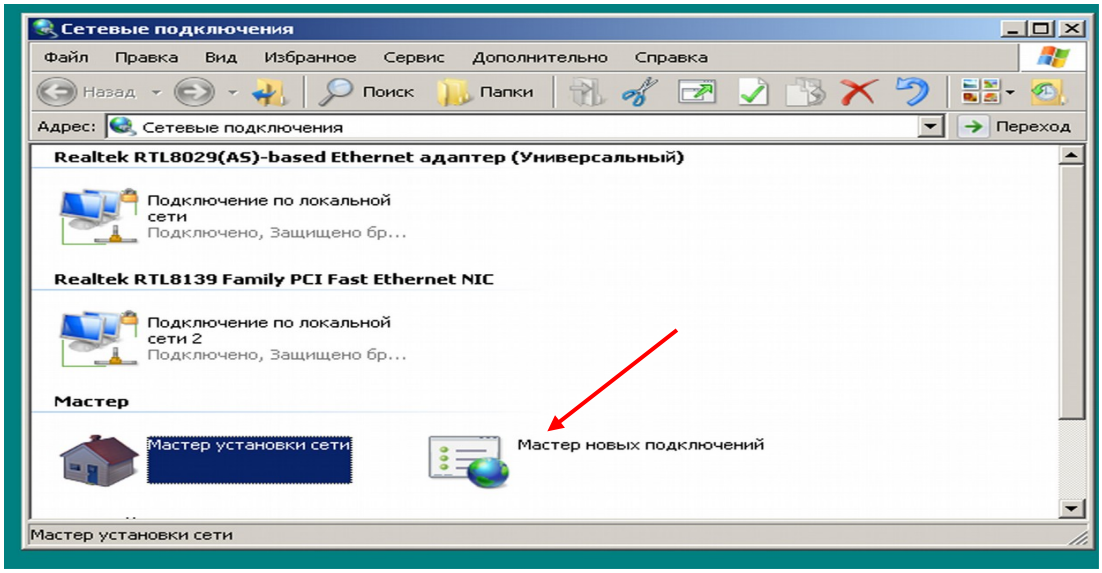

Рисунок 4.15 – Запуск майстра нових підключень

Вікно, що завершує процес встановлення з'єднання, зображено на рисунку 4.16.

.

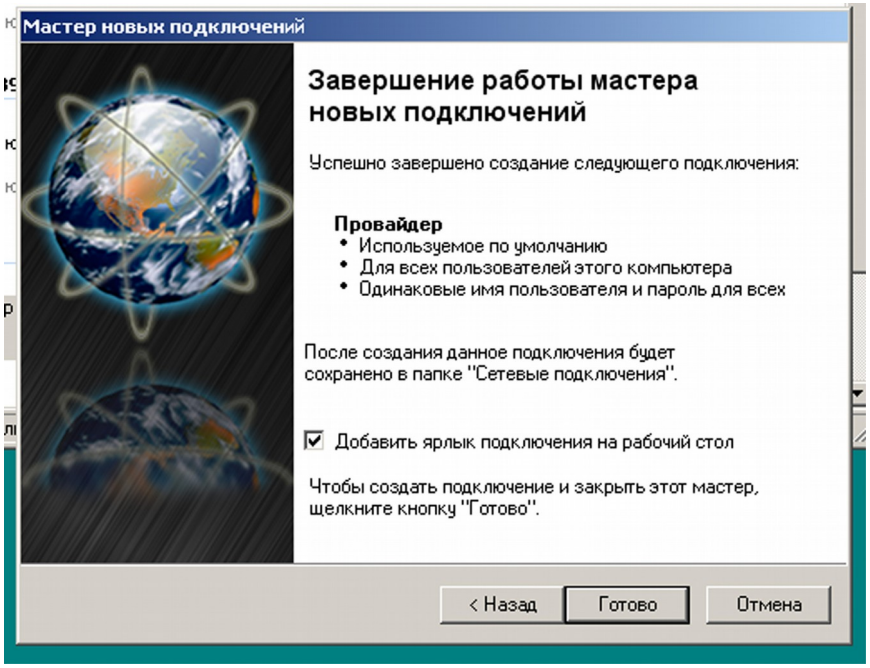

Рисунок 4.16 – Завершення процесу підключення до Інтернету

Внаслідок натиснення на кнопку «Готово» (рисунок 4.16) у папці «Сетевые подключения» з'являється піктограма нового підключення (рисунок 4.17).

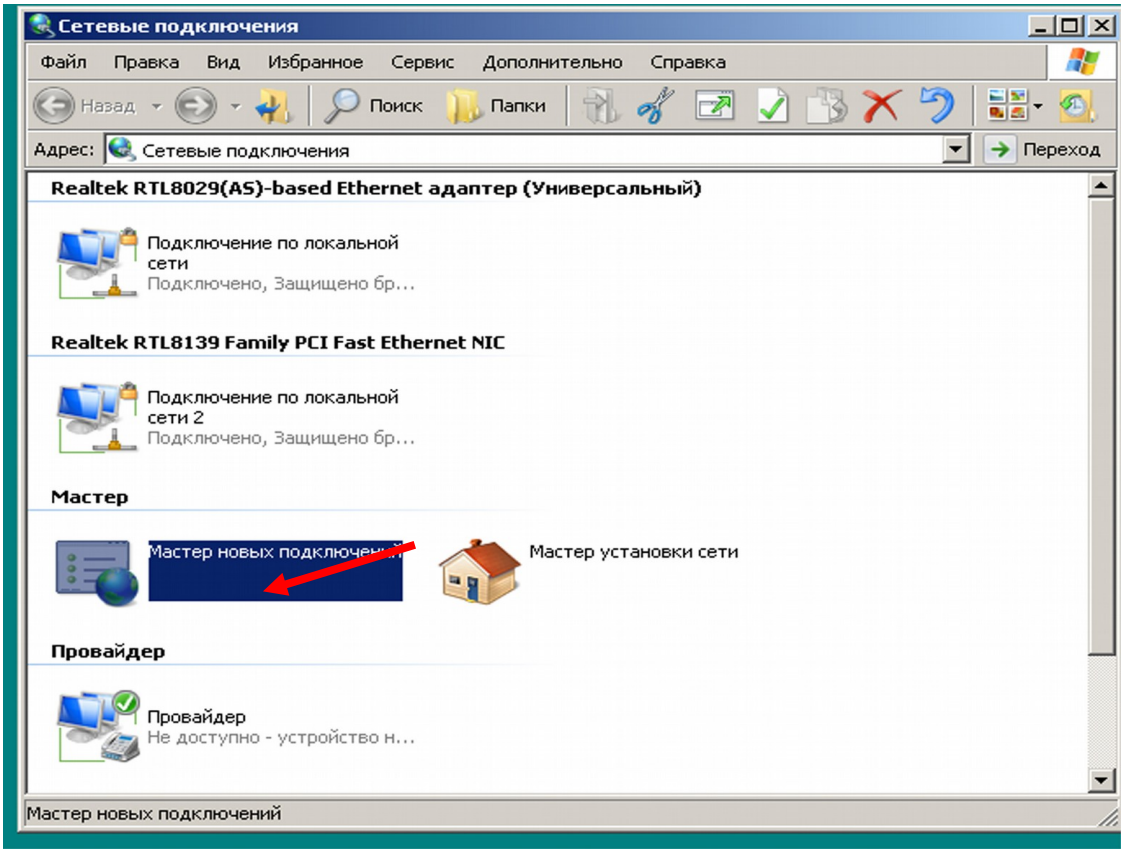

Рисунок 4.17 – З'явлення нового мережного підключення

Після встановлення з'єднання необхідно зробити його настроювання. Для цього в папці «Сетевые подключения» відкрити вікно властивостей нового підключення (в нашому прикладі «Провайдер») (рисунок 4.18), і послідовно переглядаючи закладки «Общие», «Параметры», «Безопасность», «Сеть» і «Дополнительные», відповісти на питання, що пропонуються.

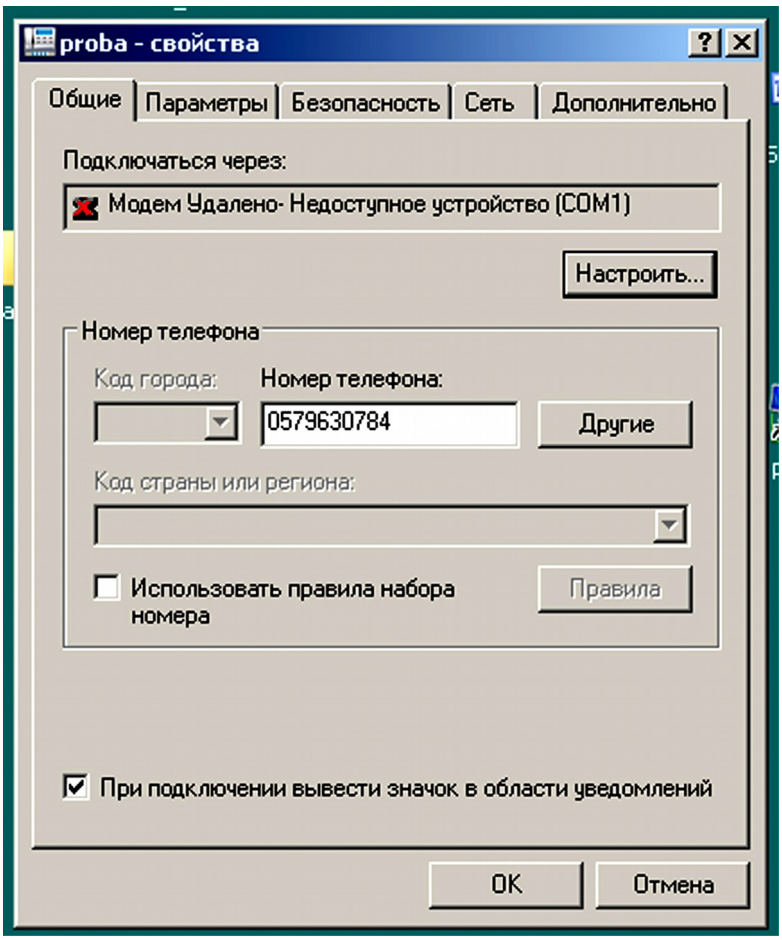

Рисунок 4.18 – Настроювання нового мережного підключення

4.2.2.2 Вихід в Інтернет

Створивши і настроївши з'єднання з провайдером, можна здійснити вихід в Інтернет. Подвійне натиснення по піктограмі нового з'єднання (або його ярлику) відкриє невелике діалогове вікно для установлення зв'язку.

Якщо в настройках з'єднання вказаний запит імені користувача і пароля, то будуть відображені відповідні поля, куди їх і потрібно ввести, а якщо вказаний і запит номера телефону, то у відповідне поле (поле введення «Набрать») потрібно ввести і номер телефону.

Додзвонившись, модем почне спілкуватися з модемом провайдера, і після встановлення правильності імені і пароля з'єднає комп'ютер з Інтернетом.

4.2.3 Створення і настроювання електронної пошти

Електронна пошта є другим основним ресурсом Інтернету (після перегляду Web-сайтів), що набув найбільшого поширення.

Для того щоб скористатися електронною поштою, спочатку треба створити поштовий ящик (зареєструвати користувача). Для реєстрації нового користувача спочатку необхідно вибрати сервер провайдера електронної пошти. Таких провайдерів дуже багато. Їх списки можна виявити в Інтернеті, користуючись будь-якою пошуковою програмою і вводячи, наприклад, запит «Бесплатные почтовые ящики».

4.2.3.1 Створення поштової скриньки

Допустимо, що вибраний сервер «ukr.net». Після звернення до сайту http://freemail.ukr.net/ на екрані з'явиться вікно, зображене на рисунку 4.19.

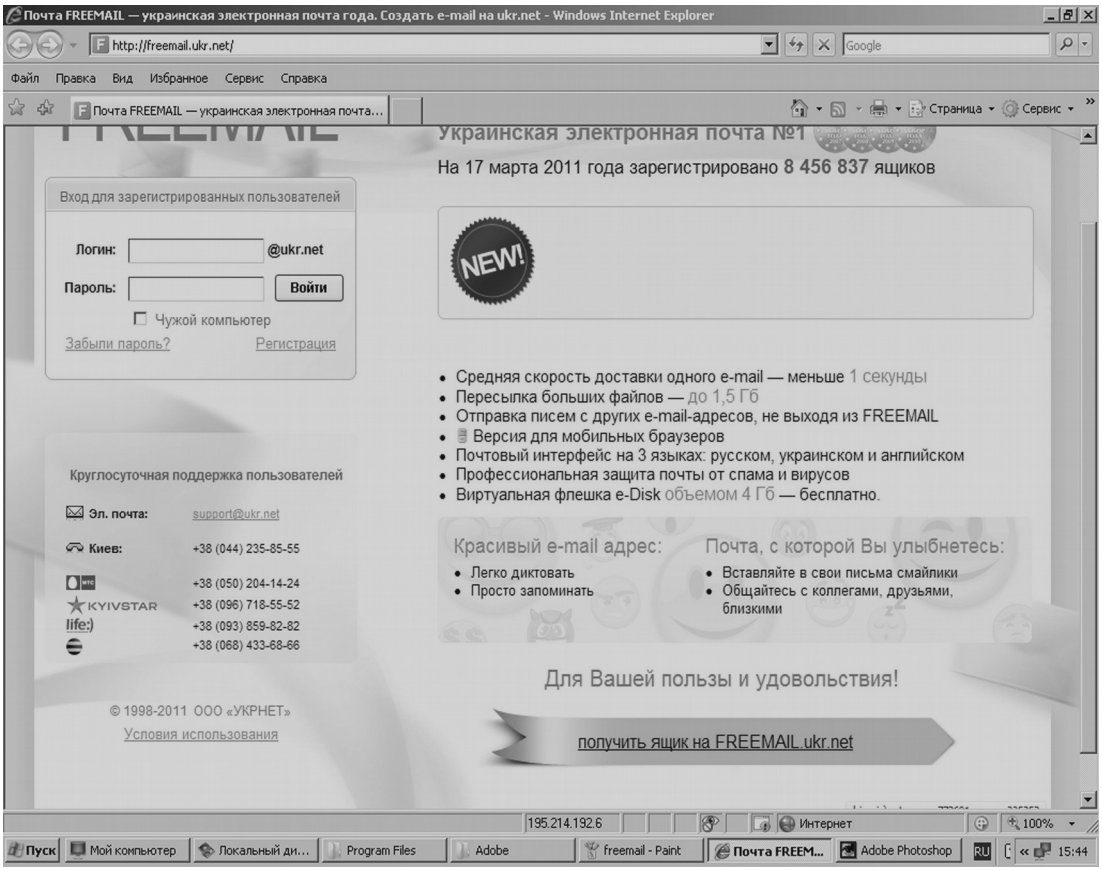

Рисунок 4.19 – Freemail – українська електронна пошта

Після прийняття рішення про створення поштової скриньки (натиснення на закладці «ящик на Freemail.ukr.net») на екрані з'являється вікно «Регистрация нового пользователя» (рисунок 4.20), всі поля якого потрібно заповнити. У першому полі вводиться логин, наприклад, «Proba», внаслідок чого адреса електронної пошти користувача, що реєструється, буде мати вигляд «Proba.@ukr.net». Потім вводиться пароль, який має містити не менше 6 символів (при цьому має вплив регістр, на якому набираються символи. Наприклад, VMDUSE і vmduse – цілком різні паролі).

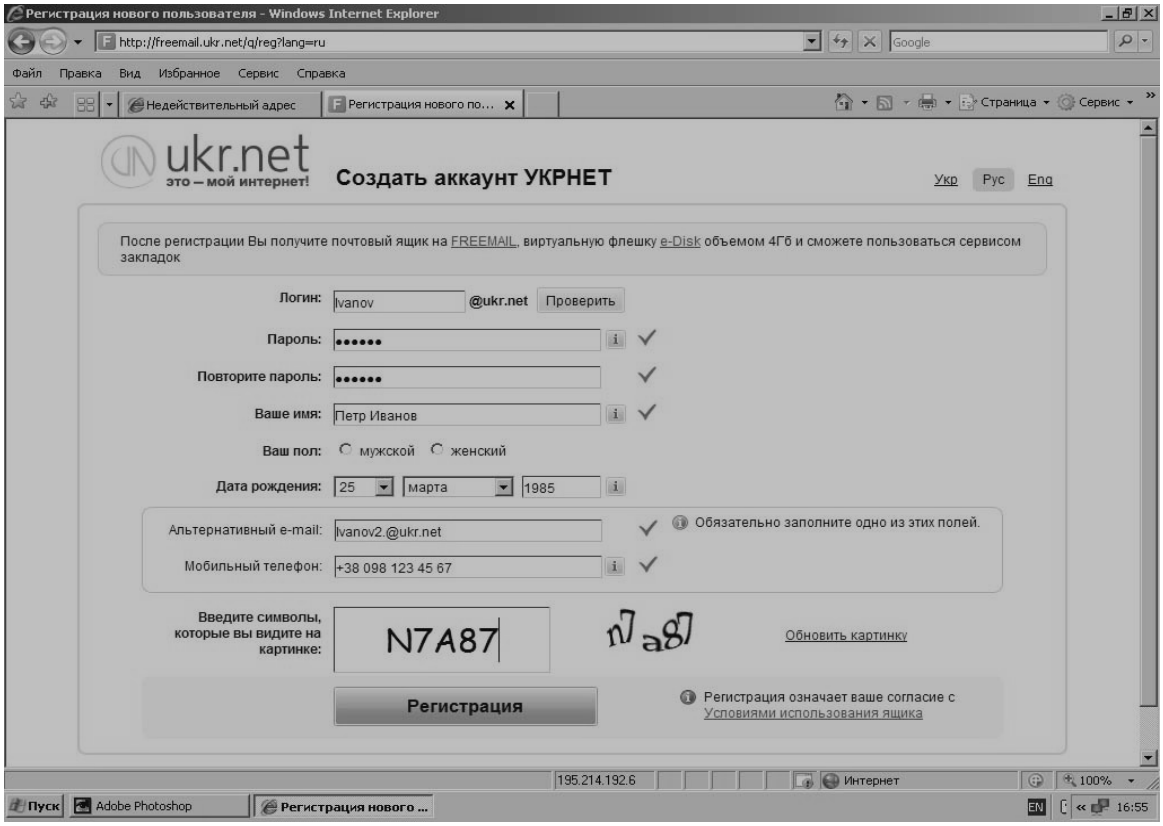

Рисунок 4.20 – Створення поштової скриньки

Отже, поштову скриньку створено. Розглянемо загальну схему передачі електронної пошти від одного абонента до іншого (рисунок 4.21).

Електронний лист, що підлягає передачі, від вузла **A** до вузла **B** ведеться в режимі з проміжним зберіганням на диску сервера. Режим цей називається «хранение-и-передача» (store-and-forward) і передбачає, що все повідомлення, хоч і розбивається на окремі пакети, що передаються автономно, але

передаються не одержувачу, а деякому транзитному вузлу (серверу вихідної пошти), на диску якого і зберігається деякий час. Час зберігання може бути досить великим і залежить від завантаженості вихідної пошти або тимчасового перевантаження мережі. Передача ведеться по протоколу вихідної пошти SMTP (Simple Mail Transfer Protocol).

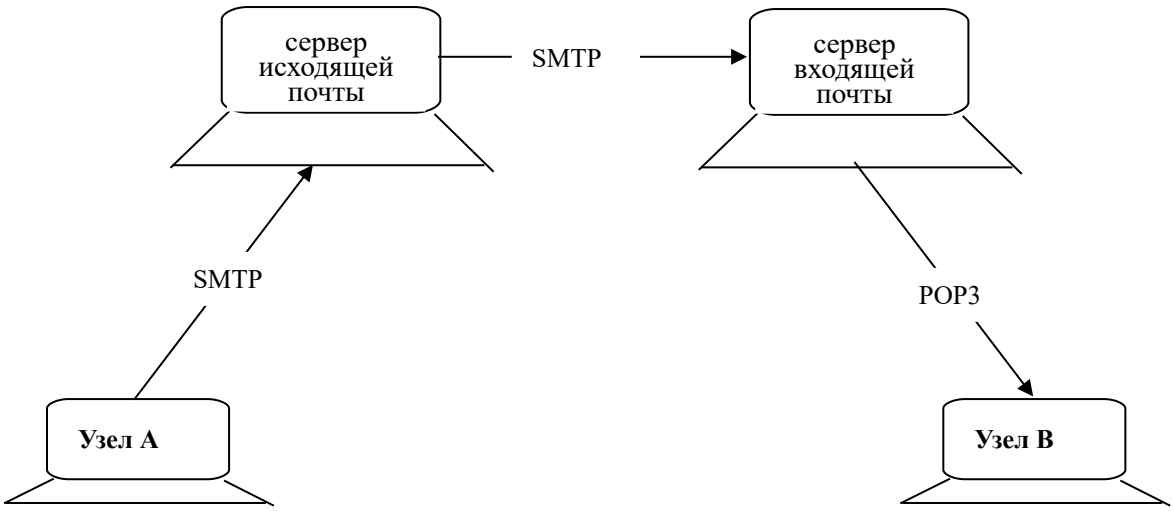

Рисунок 4.21 – Схема передачі електронної пошти

Коли мережа або сервер вихідної пошти розвантажуються, повідомлення повністю в тому ж режимі (і по тому ж протоколу SMTP) передається на сервер вхідної пошти, де і зберігається доти, поки користувач вузла В не виявить бажання перевірити свою поштову скриньку. Читання електронного листа (пересилка його з сервера вхідних повідомлень у комп'ютер адресата) проводиться по протоколу POP3 (Post Office Protocol версії 3). На цьому акт передачі електронного листа від вузла А до вузла В вважається завершеним.

Імена серверів вхідної пошти (POP-сервер) і вихідної пошти (SMTP-сервер) мають надаватися провайдером або поштовою службою, якщо використовується безкоштовна поштова скринька.

Для роботи з електронною поштою передбачаються спеціальні поштові програми. В операційній системі Windows

XP, так само, як для роботи в Інтернеті і перегляду WEB-сторінок, передбачена програма Internet Explorer. Так, для роботи з електронною поштою в ній є програма Outlook Express.

Outlook Express є поштовою програмою, призначеною для відправлення і отримання електронних листів, а також для отримання новин.

4.2.3.2 Настроювання поштової програми Outlook Express

Після створення поштової скриньки необхідно настроїти Outlook Express, щоб він міг працювати з поштовою скринькою. Для цього спочатку треба запустити Outlook Express. Якщо Outlook Express запускається вперше, то в ньому автоматично запуститься «Мастер подключения к Интернету», за допомогою якого і здійснюється підключення. Якщо майстер не запуститься, то його можна запустити вручну. Для цього в рядку меню треба вибрати «Сервис»-«Учетные записи» (рисунок 4.22), а потім у вікні, що з'явилося – «Облікові записи», натиснути кнопку «Добавить» і вибрати «Почта» (рисунок 4.23).

Після натиснення по закладці «Пошта» з'явиться вікно, в якому в спеціальне поле потрібно ввести ім'я користувача. Це ім'я буде відображатися в полі «От» у всіх повідомленнях, що відправляються по електронній пошті.

Після натиснення на кнопку «Далі» на екрані з'явиться вікно, в якому необхідно буде ввести адресу електронної пошти, яка була вказана при створенні поштової скриньки (наприклад, «Proba@ukr.net»).

У наступному вікні потрібно ввести імена серверів вхідних (у нашому прикладі «Freemail.mail.net») і вихідних (в нашому прикладі «Mail.main.kart») повідомлень (рисунок 4.24).

При переході до наступного вікна (натиснення на клавішу «Дальше») потрібно ввести ідентифікатор облікового запису (в нашому прикладі «Proba») і пароль, який був зареєстрований при створенні поштової скриньки (рисунок 4.25).

Наступне вікно завершує процес створення облікового запису (натиснення на клавішу «Готово»), а у вікні «Учетные записи в Інтернете» з'являється відповідний запис.

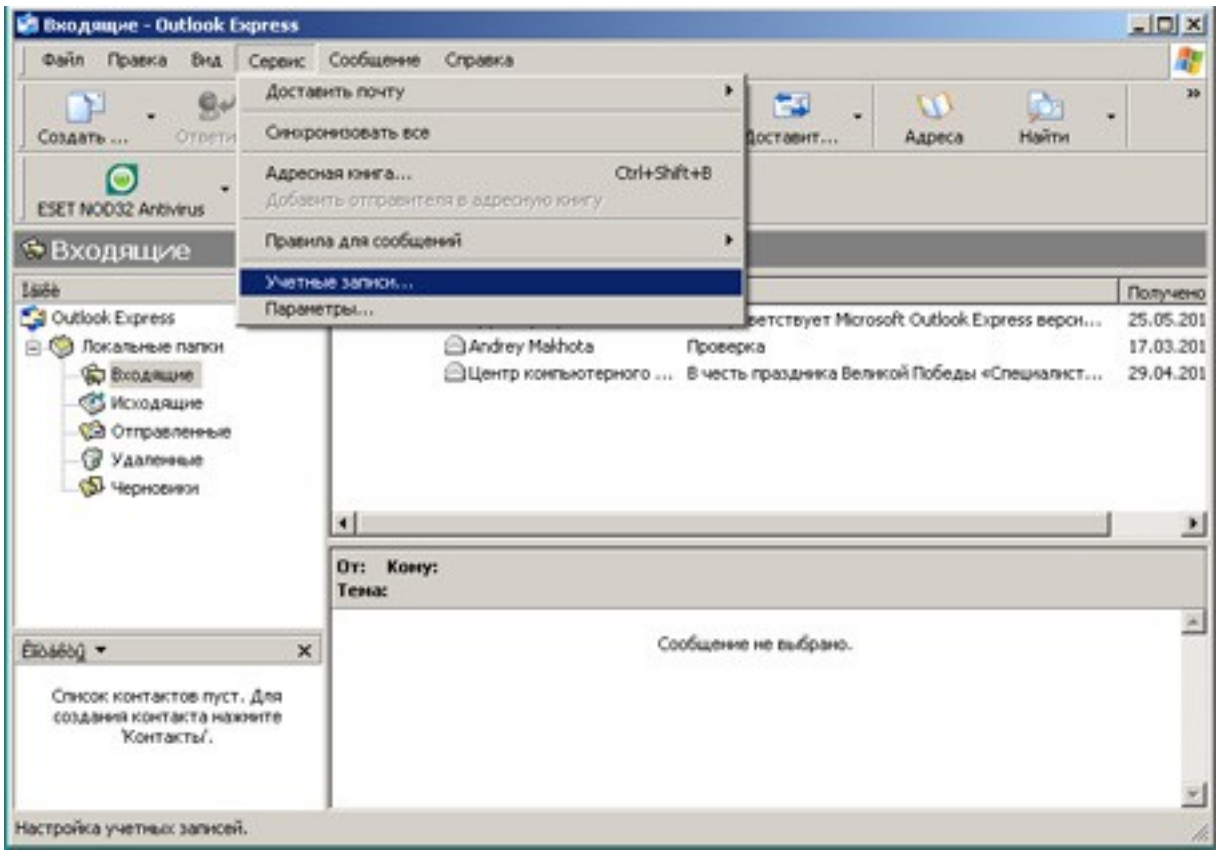

Рисунок 4.22 – Вибір сервісу «Учетные записи»

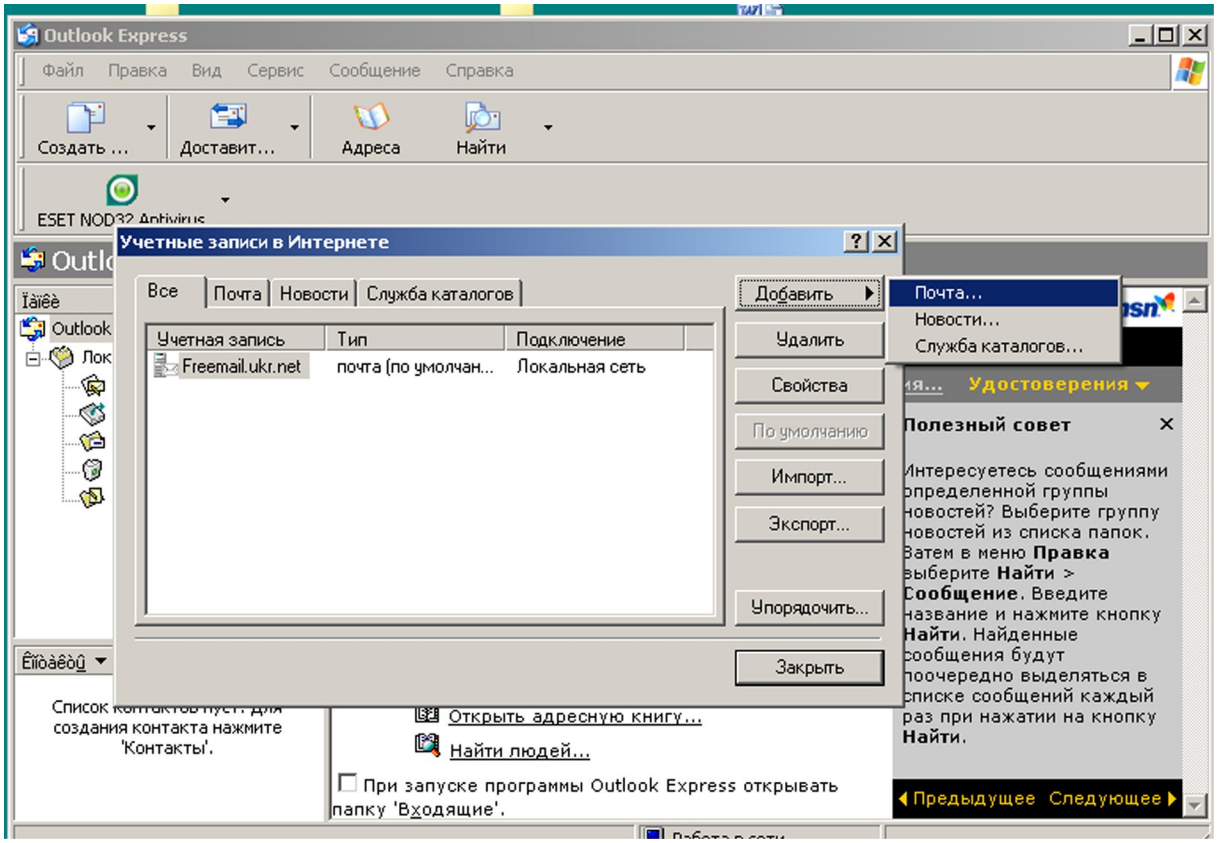

Рисунок 4.23 – Вибір режиму настроювання електронної пошти

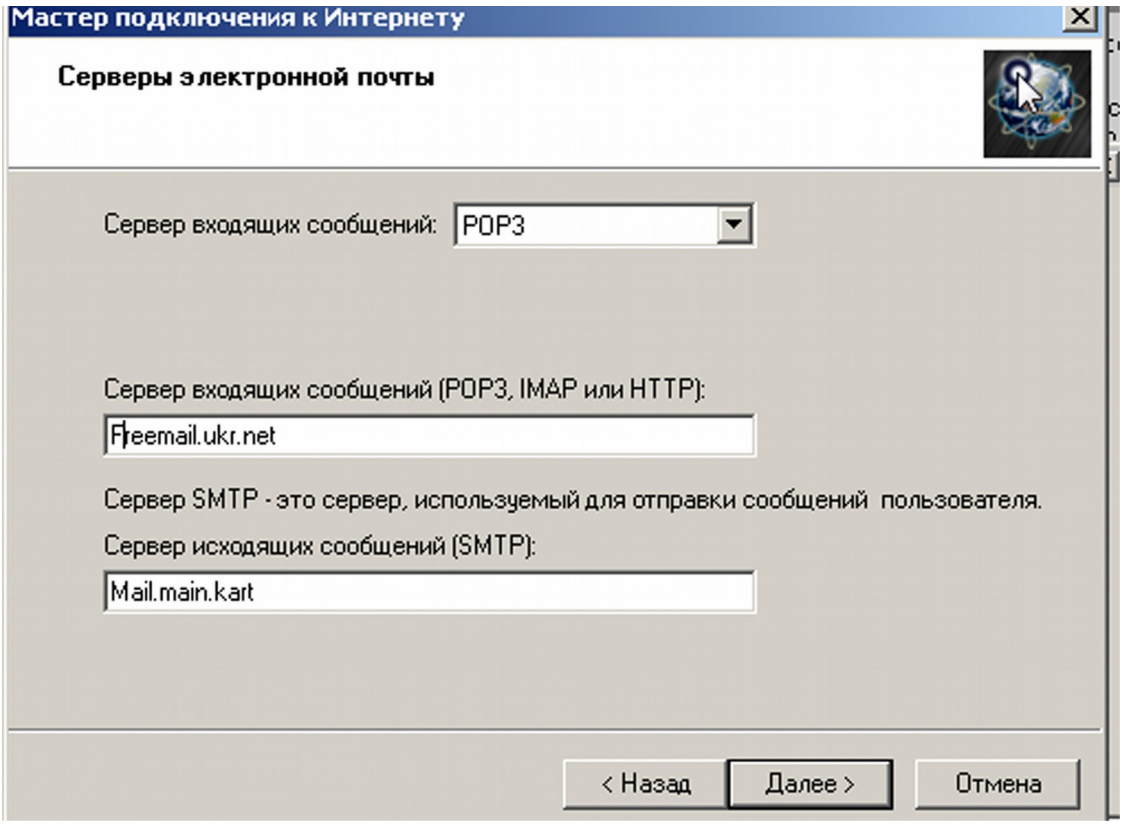

Рисунок 4.24 – Введення імен серверів вхідних та вихідних повідомлень

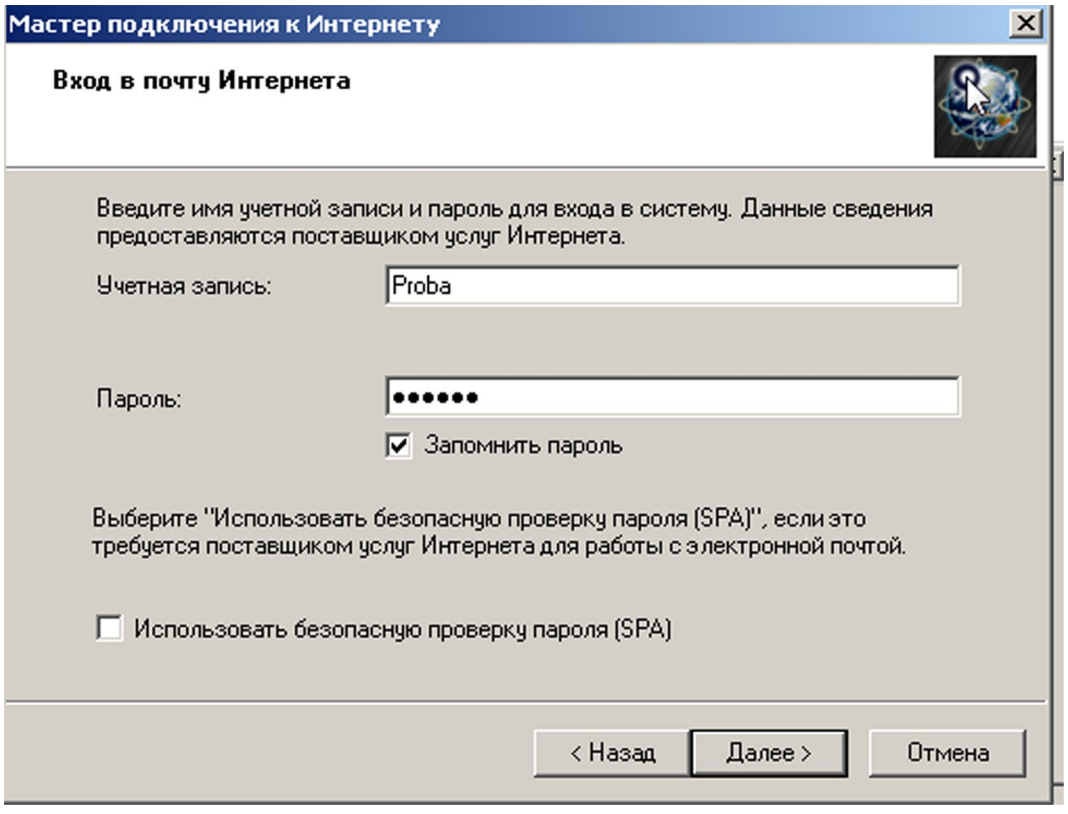

Рисунок 4.25 – Вхід у пошту Інтернету

4.2.4 Завдання та зміст звіту

1 Прочитати електронний підручник «Як працювати в Інтернеті?

2 Вивчити розділ 4.2 даних методичних вказівок.

3 Скориставшись «Мастером новых подключений», створити нове мережне підключення з ім'ям «Провайдер».

4 Переконатися, що у вікні «Сетевые подключения» з'явилася піктограма нового підключення.

5 Вивчити і відобразити у звіті всі процедури настроювання нового підключення.

6 Знищити створене мережне підключення.

7 Звернувшись до інтернет-сервіс провайдера ukr.net, виконати всі процедури з створення поштової скриньки з ім'ям Proba@ukr.net. Поштову скриньку не створювати.

8 Настроїти поштову програму Outlook Express, використовуючи дані про поштову скриньку (див. пункт 5 даного завдання), і ідентифікатори серверів вхідних і вихідних повідомлень, рекомендованих у методичних вказівках (див. рисунок 4.24).

9 Переконатися, що новий обліковий запис з'явився у вікні «Учетные записи в Интернете».

10 Вивчити і відобразити у звіті всі процедури настроювання створеного облікового запису.

11 Знищити створений обліковий запис.

Контрольні питання

1 Дайте визначення поняття «Інтернет».

2 Назвіть основні сервіси Інтернету.

3 Дайте визначення терміна «Провайдер».

4 Назвіть, яким чином надаються послуги Інтернету споживачеві.

5 Дайте визначення поняття «модемний пул».

6 Дайте визначення терміна «хостінг».

7 Опишіть технологію «клієнт-сервер». Назвіть хоч би по одній програма-сервер і програма-клієнт, що використовуються при роботі з Інтернетом.

8 Опишіть алгоритм настроювання модема.

9 Опишіть процес створення поштової скриньки.

10 Опишіть процес створення облікового запису користувача електронної пошти при використанні поштової програми Outlook Express.

11 Опишіть процес настроювання Windows XP при з'єднанні з провайдером.

Список літератури

1 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебн. для вузов. – С. Пб.: ИД «Питер», 2007 – 957 с.

2 Матвеев М.Д., Юдин М.В., Куприянова А.В. Самоучитель Microsoft Windows XP. Все об использовании и настройках – С. Пб.: Наука и техника, 2006 – 620 с.

3. Москвин Э.К. Локальная сеть без проводов – М.: НТ Пресс, 2006.

4 Рошан П., Лиэри Дж. Основы построения беспроводных локальных сетей стандарта 802.11 – М.: ИД "Вильямс", 2004 – 304 с.

5 Пролетарский А.В., Баскаков И.В. и др. Беспроводные сети Wi-Fi. – М.: БИНОМ, 2007.

6 М. Максим, Д. Полино. Безопасность беспроводных сетей – М.: Компания "АйТи"; ДМК Пресс, 2004 – 288 с.