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

Кафедра комп’ютерних систем та мереж

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт

з дисципліни

«ДОСЛІДЖЕННЯ І ПРОЄКТУВАННЯ КОМП’ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ»

для здобувачів другого (магістерського) рівня вищої освіти спеціальності 123 «Комп’ютерна інженерія» усіх форм навчання

Тернопіль, 2021

Методичні вказівки до виконання лабораторних робіт з дисципліни «Дослідження і проєктування комп’ютерних систем та мереж» для здобувачів другого (магістерського) рівня вищої освіти спеціальності 123 «Комп’ютерна інженерія» усіх форм навчання / Укладачі: А.В. Чайковський, Р.О. Жаровський, Ю.З. Лещишин,. Тернопіль: ТНТУ, 2021. 94 с.

Укладачі: доц., к.т.н. Чайковський А.В., ст.викл., к.т.н. Жаровський Р.О., доц., к.т.н. Лещишин Ю.З.

Рецензент: д.т.н., професор, завідувач кафедри Паламар М.І.

Затверджено на засіданні кафедри комп’ютерних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя.

Протокол № 1 від 30.08.2021 р.

Методичні вказівки складені з урахуванням методичних розробок інших закладів вищої освіти, а також матеріалів літературних джерел, наведених у переліку.

Зміст

Вступ

Методичні вказівки до лабораторних робіт з курсу “ Дослідження і проектування комп’ютерних систем та мереж” покликані допомогти студентам денної форми навчання засвоїти використання сучасних систем інформаційного обміну в комп’ютерних мережах.

Зміст та структура методичних вказівок відповідає програмі підготовки фахівців з напрямку 123 "Комп'ютерна інженерія". Лабораторний практикум охоплює основний зміст матеріалу дисципліни “Дослідження і проектування комп’ютерних систем та мереж”.

Мета курсу. «Дослідження і проєктування комп’ютерних систем та мереж» полягає у отриманні знань, вмінь та навичок, необхідних фахівцю, який спеціалізується в області проєктування та експлуатації комп’ютерних систем та мереж.

У ході виконання лабораторних робіт студенти повинні:

- ознайомитись з середовищами передачі даних в КМ їх характеристиками;
- вміти здійснювати розподіл адресного простору в КМ;
- здійнювати розрахунки для проектування надійної роботи КМ;
- вміти оцінювати швидкодію КМ; вміти використовувати програмні засоби для моніторингу роботи КМ.

Кожна лабораторна робота містить наступні розділи:

- тема,мета роботи;
- теоретичні відомості, необхідні для виконання роботи;
- порядок виконання роботи;

Лабораторна робота №1.

Тема: ” Дослідження роботи пошукових систем мережі Інтернет ”

Мета роботи: ознайомитись з основними методами пошуку інформації в мережі Інтернет.

Теоретичні відомості

Пошук інформації в Інтернет

Кількість пошукових інструментів, що існують нині в Інтернет, досить велика. І розібратися користувачу початківцю в механізмах їх роботи досить проблематично, оскільки доведеться витратити досить велику кількість часу. У даній роботі пропонується опис найбільш загальних рис пошукових інструментів, а потім детально розглядаються структури запитів для найбільш популярних українських, білоруських, російських і англомовних систем.

Технологія пошуку інформації в Інтернет

Сьогодні про World Wide Web (WWW) говорять як про інформаційний ресурс Інтернет або як про спеціальну технологію підготовки і розміщення документів в Інтернет, web-технології. Технологія WWW була розроблена в 1991 р. для обміну науковими документами (CERN, Швейцарія). Починаючи з 1993 року, інформаційна служба WWW стала особливо популярна, і з часом перетворилася на один з основних інформаційних ресурсів Інтернет. У складі World Wide Web існують самі різні "документи": особисті Web-сторінки, електронні бібліотеки онлайн, віртуальні музеї, каталоги по продуктах і послугах, науково-дослідні публікації і ін. При такій великій кількості інформації виникає питання: "Як знайти в цьому морі інформації те, що нам необхідно?".

При вирішенні даної проблеми на допомогу нам приходять пошукові інструменти.

Пошукові інструменти (ПІ) - це спеціальне програмне забезпечення, основне завдання якого - забезпечити найбільш оптимальний пошук інформації в Інтернет. Розміщуються ПІ на спеціальних серверах, і кожний з них виконує наступних чотири основні завдання:

1. аналіз web-сторінок;
1. занесення результатів аналізу Web-сторінок на той або інший рівень бази даних пошукового сервера залежно від методів автоматичного індексування, тобто методів аналізу вмісту сторінок;
1. пошук документів по запиту користувача;
1. забезпечення зручного інтерфейсу для пошуку інформації і проглядання результатів пошуку користувачем.

Прийоми роботи, використовувані при роботі з тими або іншими пошуковими інструментами, практично однакові. Перш ніж перейти до їх обговорення розглянемо наступні поняття:

Призначений для користувача інтерфейс пошукового інструменту представлений у вигляді HTML-сторінки з URL-посиланнями, що активізуються, рядком формування запиту (рядком пошуку) і інструментами активізації запиту.

Індекс пошукової системи - результат аналізу web-сторінок, розміщений в базі даних пошукового сервера за певними правилами.

Запит - фраза або ключові слова, записувані користувачем в рядку пошуку. Для формування запиту використовуються спеціальні символи ("" |, ~), математичні символи (*, +, ?), булеві оператори (AND, OR, NOT, NEAR).

Користувач, набравши ключові слова і активізувавши пошук, одержує список документів по сформульованому (заданому) запиту. Цей список ранжирується по певних критеріях так, щоб вверху списку опинилися ті документи, які найбільш відповідають запиту користувача. Кожний з пошукових інструментів використовує різні критерії ранжирування документів, як при аналізі результатів пошуку, так і при формуванні індексу (наповненні індексної бази даних web-сторінок). Внаслідок цього, якщо ви вкажете в рядку пошуку для кожного пошукового інструменту однакової конструкції запит, отримайте різні результати пошуку. Велике значення має для користувача, які документи опиняться в першій десятці документів за результатами пошуку і на скільки ці документи відповідають очікуванням користувача.

Кожний з пошукових інструментів пропонує два способи пошуку, простій (simple search) і розширений (advanced search) з використанням спеціальної форми запиту і без неї.

Yahoo зручно використовувати при отриманні поточних новин, наприклад, світових політичних, прогнозу погоди, біржових новин і т.д. На відміну від інших інструментів пошуку AltaVista надає користувачу можливість довільно формулювати запит при простому пошуку, наприклад, набрати фразу "Where can I find information about Computer Science" або запит типу "computer information technology in high school". Освоївши критерії уточнення запиту і прийоми розширеного пошуку, ви можете збільшити ефективність пошуку і достатньо швидко знайти потрібну інформацію. Перш за все, збільшити ефективність пошуку ви можете за рахунок використання в запитах логічних операторів (операцій) Or, And, Near, Not, математичних і спеціальних символів. За допомогою операторів і/або символів користувач зв'язує ключові слова в потрібній послідовності, щоб отримати найбільш адекватний запиту результат пошуку. Форми запитів приведені в таблиці 1.1.

Таблиця 1.1

Простий запит
computer technology
computer information technology
"computer technology"
"computer information technology"
Розширений запит з використанням булевих операторів
computer and information and technology
computer near technology near edu*
computer near technology near education
computer near technology near (education or commerce)
Розширений запит з використанням математичних символів
+computer +information +technology
computer ~technology ~edu*
computer ~technology ~education
computer ~technology ~(education | commerce)

Простий запит дає значну кількість посилань на документи, оскільки в список потрапляють документи що містять одне із слів, введених при запиті, або просте словосполучення (див. таблицю 1.1). Оператор **and** дозволяє вказати вам на те, що в змісті документа повинні бути включені всі ключові слова. Проте, кількість документів може бути все ще великою, і їх перегляд займе багато часу. Тому у ряді випадків набагато зручніше застосувати оператор **near**, показуючого, що слова повинні розташовуватися в документі в достатній близькості. Використання **near** значно зменшить кількість знайдених вами документів.

Наявність символу "*****" в рядку запиту означає, що здійснюватиметься пошук слова по його масці. Наприклад, одержимо список документів, що містять слова, що починаються на "edu", якщо в рядку запиту запишемо "edu*". Це можуть бути слова education, educator, educable і т.д.

Ще один спосіб звузити пошук - використовувати спеціальні ключові слова. Основні ключові слова представлені в таблиці 1.2. Використовувати їх потрібно уважно, оскільки не всі пошукові інструменти підтримують пошук за перерахованими ключовими словами. Щоб упевнитися, які ключові слова підтримуються даним пошуковим інструментом, не забувайте проглядати його довідкову інформацію або "Допомогу".

Таблиця 1.2

Термін	Значення
domain: ім’я_домена	Знаходить сторінки у вказаному адресному просторі. Наприклад: запит domain:edu - для пошуку сторінок тих, що містяться на вузлах в домені edu
host: адрес_вузла	Видає список документів з вузлів, в імені яких присутнє значення, введене в параметрі адрес_вузла. Наприклад, за запитом host:www.iatp.unibel.by буде одержаний список документів, розташованих на сервері, чия адреса www.iatp.unibel.by
url: текст	Знаходить сторінки, в адресу яких входить певне слово або фраза. Вказавши url:unibel, ви знайдете всі сторінки, адреси (URL) яких містять слово unibel
link: URLтекст	Знаходить документи, на яких є посилання на вказаний URL. Запит link:www.altavista.com допоможе знайти всі сторінки, які містять посилання на AltaVista
image: текст	Знаходить документи із зображеннями, в назву або опис яких входить слово, введене як параметр текст
title: текст	Знаходить документи, в заголовок яких входить вказана фраза (мається на увазі назву документа, яка відображається в рядку заголовка при відкритті документа в браузере|).

Пошукові інструменти

Англомовні пошукові інструменти

Тематичні каталоги:	Пошукові машини:	Пошукові служби:
www.yahoo.com www.northernlight.com www.google.com	www.altavista.com www.infoseek.com www.alltheweb.com	www.metacrawler.com www.mamma.com

Українські пошукові інструменти

Тематичні каталоги:	Пошукові машини:	Пошукові служби:
http://holms.ukrnet.net http://www.webber.net.ua http://www.brama.com/ukr.html	http://www.search.kiev.ua http://poshuk.dnepr.net http://holms.ukrnet.net	http://meta-ukraine.com

Приклади формування запитів з використанням спеціальних символів:

Символ	Операція	Приклад	Значення
+	Символ "+"	+вакансія +працевлаштування	Буде запропонований список документів, в яких міститиметься як слово "вакансія", так і слово "працевлаштування"
-	Символ "-"	+вакансія - працевлаштування	Буде запропонований список документів, в яких міститиметься слово "вакансія", а слово "працевлаштування" буде відсутнє
& або and	Логічна операція "І"	вакансія & працевлаштування вакансія AND працевлаштування	Буде запропонований список документів, в яких міститиметься як слово "вакансія", так і слово "працевлаштування"
| або or	Логічна операція "АБО"	вакансія | працевлаштування вакансія OR працевлаштування	Буде запропонований список документів, в яких міститиметься або слово "вакансія", або слово "працевлаштування"
! або not	Логічна операція "НЕМАЄ"	вакансія ! програміст вакансія NOT програміст	Буде запропонований список документів, в яких зустрічається слово "вакансія", але не зустрічається "програміст"
( )	Групування виразів	(вакансія ! програміст) | (бухгалтер & менеджер)	Буде запропонований список документів, в яких зустрічається слово "вакансія", але| не зустрічається слово "програміст", а також список документів, в яких зустрічається і слово "бухгалтер" і слово "менеджер"
*	Пошук за шаблоном	прогр*	Буде запропонований список документів, які містять слова, що починаються на прогр|

Порядок виконання роботи

1. Ознайомитись з роботою пошукових серверів.
2. Обрати тему по якій будете проводити пошук інформації.
3. Оформити звіт по роботі

Звіт повинен включати:

1. тему, мету роботи;
2. короткий огляд теоретичних відомостей;
3. методи якими проводився пошук інформації (чи використовувались пошукові сервери, сервери конференцій UseNet, спеціалізовані сайти по даній тематиці);
4. які використовувались ключові слова, символи при формуванні запиту;
5. навести приклади запитів по вашій темі;
6. які види запитів і на яких пошукових серверах були найбільш ефективними (запити які дозволили досягти кращого результату);
7. привести посилання на сайти з яких було взято інформацію (приклади)
8. висновки.

Контрольні запитання

1. Дайте визначення поняття пошукові інструменти.
2. Основні завдання які виконують пошукові сервери.
3. Які математичні символи використовуються для формування запитів?
4. Які булеві оператори використовуються для формування запитів?
5. Які ключові слова використовуються в запитах?
6. Назвіть які ви знаєте пошукові сервера?

Лабораторна робота №2.

Тема: ” Дослідження роботи системи передачі електронних повідомлень в мережі Інтернет **”**

Мета роботи: ознайомитись з роботою SMTP і POP3 протоколів. Ознайомитись з принципами роботи поштових серверів на прикладі Kerio Mail Server. Отримати практичні навички по налаштуванню поштового сервера Kerio Mail Server. Розглянути можливості по створенню доменів, користувачів.

Теоретичні відомості

Протокол SMTP.

Основна задача SMTP протоколу (Simple Mail Transfer Protocol) полягає в тому, щоб забезпечувати передачу електронних повідомлень (почту). Для роботи через протокол SMTP клієнт створює TCP з'єднання з сервером через порт 25. Потім клієнт і SMTP сервер обмінюються інформацією поки з'єднання не буде закрито або перервано. Основною процедурою в SMTP є передача пошти (Mail Procedure). Далі йдуть процедури форвардингу пошти (Mail Forwarding), перевірка імен поштового ящика і виведення списків поштових груп. Найпершою процедурою є відкриття каналу передачі, а останньої - його закриття.

Команди SMTP.

Команди SMTP вказують серверу, яку операцію хоче провести клієнт. Команди складаються з ключових слів, за якими слідує один або більш параметрів. Ключове слово складається з 4-х символів і розділено від аргументу одним або декількома пропусками. Кожний командний рядок закінчується символами CRLF.

SEND - використовується замість команди MAIL і вказує, що пошта повинна бути доставлена на термінал користувача.

SOML, SAML - комбінації команд SEND або MAIL, SEND і MAIL відповідно.

RSET - вказує серверу перервати виконання поточного процесу. Всі збережені дані (відправник, одержувач і ін.) стираються. Сервер повинен відправити позитивну відповідь.

VRFY - просить сервер перевірити, чи є переданий аргумент ім'ям користувача. У разі успіху сервер повертає повне ім'я користувача.

EXPN - просить сервер підтвердити, що переданий аргумент - це список поштової групи, і якщо так, то сервер виводить членів цієї групи.

HELP - запрошує у сервера корисну допомогу про передану як аргумент команду.

NOOP - на виклик цієї команди сервер повинен позитивно відповісти. NOOP нічого не робить і ніяк не впливає на вказані до цього дані.

Протокол POP3

Перед роботою через протокол POP3 сервер прослуховує порт 110. Коли клієнт хоче використовувати цей протокол, він повинен створити TCP з'єднання з сервером. Коли з'єднання встановлено, сервер відправляє запрошення. Потім клієнт і POP3 сервер обмінюються інформацією поки з'єднання не буде закрито або перервано.

Команди POP3 складаються з ключових слів, за деякими слідує один або більш аргументів. Всі команди закінчуються парою CRLF (в Visual Basic константа vbCrLf). Ключові слова і аргументи складаються з друкованих ASCII символів. Ключове слово і аргументи розділено одиночним пропуском. Ключове слово складається від 3-х до 4-х символів, а аргумент може бути завдовжки до 40-ка символів.

Відповіді в POP3 складаються з індикатора стану і ключового слова, за яким може слідувати додаткова інформація. Відповідь закінчується парою CRLF. Існує тільки два індикатори стану: "+OK" - позитивний і "-ERR" - негативний.

Відповіді на деякі команди можуть складатися з декількох рядків. В цих випадках кожний рядок розділений парою CRLF, а кінець відповіді закінчується ASCII символом 46 (".") і парою CRLF.

POP3 сесія складається з декількох режимів. Як тільки з'єднання з сервером було встановлено і сервер відправив запрошення, то сесія переходить в режим **AUTHORIZATION (Авторизація)**. В цьому режимі клієнт повинен ідентифікувати себе на сервері. Після успішної ідентифікації сесія переходить в режим **TRANSACTION (Передача)**. В цьому режимі клієнт просить сервер виконати певні команди. Коли клієнт відправляє команду QUIT, сесія переходить в режим **UPDATE**. В цьому режимі POP3 сервер звільняє всі зайняті ресурси і завершує роботу. Після цього TCP з'єднання закривається.

Протокол IMAP 4

IMAP 4 (Internet Message Access Protocol) - це Інтернет протокол, який надає можливість клієнту мати доступ до електронної пошти на сервері а не завантажувати її до комп'ютера користувача. IMAP4 розробляється для оточення, в якому користувач може реєструватися на сервері від різних робочих станцій (таким чином користувачі можуть мати доступ до всієї пошти яка їм потрібна в будь який час). В такому випадку, завантажувати пошту користувача до одного комп'ютера звичайно непрактично, тому що користувач не завжди використовує один і той же комп'ютер.

Протоколи поштового сервера Kerio Mail Server.

Цей поштовий сервер являє собою програму, яка підтримує протоколи POP (протокол вхідної пошти), SMTP (протокол вихідної пошти), IMAP (протокол вхідної пошти), LDAP(протокол для роботи зі спеціальними серверами), Sekure POP (протокол вхідної пошти з використанням протоколу шифрування SSL), Sekure SMTP (протокол вихідної пошти з використанням протоколу шифрування SSL), Sekure IMAP (протокол вхідної пошти з використанням протоколу шифрування SSL), Sekure LDAP (протокол для роботи зі спеціальними серверами з використанням протоколу шифрування SSL) і Web Mail.

Можливості і сервіси поштового сервера Kerio Mail Server

SMTP сервер.

Повнофункціональний SMTP сервер, який може обслуговувати декілька незалежних доменів, створювати віртуальні адреси (псевдоніми), одержувати пошту використовуючи ETRN і так далі. Вихідна пошта може бути послана як безпосередньо в домен одержувача (використовуючи записи DNS MX), так і ретрансльована, з

використнням SMTP сервера-ретранслятора (наприклад, SMTP сервера постачальника Інтернет послуг).

POP3 сервер

POP3 (Поштовий протокол версії 3) - це протокол Інтернету, який дозволяє POP3 клієнтам завантажувати пошту з сервера. Цей протокол добре працює для комп'ютерів, які не можуть забезпечити постійне з'єднання до сервера.

IMAP сервер

IMAP4 (Протокол доступу до Інтернет повідомленням версії 4) - це протокол повідомлень Інтернет, який дозволяє поштовому клієнту дістати доступ до пошти на сервері не завантажуючи її на призначений для користувача комп'ютер.

NNTP сервер

(Протокол передачі мережевих новин) - це протокол, який використовується для передачі новинних повідомлень і виведення загальних тек для користувача. NNTP сервер зберігає архіви повідомлень всіх новинних груп.

Веб інтерфейс (Kerio WebMail)

Вбудований HTTP сервер дозволяє здійснювати віддалений доступ до облікового запису користувача. Це дозволяє читати і писати поштові повідомлення, управляти теками і змінювати персональні установки. Для обробки пошти не потрібно встановлювати яке-небудь клієнтське програмне забезпечення і не потрібні ніякі персональні настройки.

WAPmail

Дозволяє дістати доступ до пошти через мобільний телефон.

Персональні і загальні списки контактів

У Kerio MailServer можна керувати персональними і Загальними списками контактів (призначені для користувача дані, наприклад, поштові адреси). Користувачі можуть дістати доступ до своєї пошти і списків контактів через будь-який поштовий клієнт або інтерфейс Kerio WebMail.

Особистий і загальний календарі, завдання

У Kerio MailServer 6.x, користувачі можуть зберігати особистий і загальний календарі і завдання на сервері. Ця інформація управляється за допомогою інтерфейсу Kerio WebMail і додатками MS Outlook з Kerio Outlook Connector.

Захищені канали зв'язку

Всі сервіси Kerio MailServer пропонують стандартні не секретні з'єднання і SSL-шифровані захищені з'єднання. Також можливо посилати повідомлення через безпечне з'єднання, за умови, що що приймає сервер теж підтримує цю можливість.

Антивірусний контроль

Вся вхідна і вихідна пошта може перевірятися на зміст вірусів. Антивірусний контроль здійснюється зовнішньою антивірусною програмою (такий як AVG NOD32, і так далі).

Захист від небажаної пошти (спама)

Поштовий сервер може бути захищений від небажаної пошти (спама). Є можливість блокувати вхідні повідомлення від серверів, що знаходяться в списку інтернетних баз даних по спамерам, або в призначеному для користувача списку.

Архівація пошти

Kerio MailServer може робити резервні копії всієї пошти (або тільки відправленої пошти) локально або на видалений сервер.

Резервне копіювання призначених для користувача тек

Є можливість робити декілька типів резервних копій призначених для користувача тек. Основний тип резервного копіювання - це повне копіювання, яке може бути зроблене тільки один раз.

Фільтрація і повідомлення

Кожен користувач може визначити набір дій, які будуть виконані після того, як повідомлення буде одержано (переміщення повідомлення в особливу теку, фільтрація, відправка повідомлення на мобільний телефон, автоматичну відповідь

Планувальник

Адміністратор сервера має абсолютний контроль над тим, чи відправляти повідомлення відразу, в певний час або через задані тимчасові інтервали . Завдяки цьому можна оптимізувати витрати на з'єднання (при з'єднанні по телефону).

Сервер розсилки пошти

Усередині локального домена може бути створено будь-яку кількість поштових розсилок. Учасники списку розсилок можуть бути визначені адміністратором сервера, схвалені модератором або учасник може бути доданий автоматично поштою.

Підтримка Active Directory

Kerio MailServer забезпечує повну підтримку для Microsoft Active Directory. Немає необхідності імпортувати призначені для користувача облікові записи у внутрішню базу даних. Для того, щоб додати або видалити призначений для користувача обліковий запис/групу використовуйте системну утиліту Active Directory.

Kerio Outlook Connector

Kerio Outlook Connector використовує MAPI для зв'язку між Kerio MailServer і MS Outlook. Це дозволяє зберігати різні типи тек (такі як поштові повідомлення, контакти, календарі і завдання) на сервері. Це також дозволяє розділяти і відображати теки, а також встановлювати правила сортування повідомлень.

Встановлення.

Перший крок під час установки - вибір мови.

Наступний крок - вибір типу установки. Доступні наступні типи установки:

- Typical - повна установка
- Minimal - мінімальна установка
- Custom - вибір компонентів Kerio MailServer, які повинні бути встановлені, а також вибір мови допомоги для Kerio MailServer.

Всі компоненти, які потрібно зберегти, повинні бути відмічені.

Після цього кроку, установка продовжується (тобто файли копіюються на жорсткий диск і проводяться всі необхідні системні установки). Потім запускається майстер установки базових параметрів сервера.

Після успішного завершення процесу установки, запуститься майстер настройки. Введіть ім'я первинного домена і пароль для адміністрування.

Kerio MailServer Engine є ядром поштового сервера, працює як сервіс, і буде запущений відразу після завершення установки. Це означає, що утиліта Kerio MailServer Monitor теж запуститься. За допомогою цієї утиліти зможна подивитися статус Engine, зупинити або запустити поштовий сервер і виконати інші завдання. Kerio MailServer Monitor відображається у вигляді ікони в системному треї.

Первинний домен

Щоб зареєструвати користувача (або групу) в Kerio MailServer, необхідно як мінімум створити один локальний домен. Перший створений локальний домен є первинним доменом. У відмінності від інших локальних доменів, користувачі можуть входити в первинний домен використовуючи тільки свій логін (інші домена вимагають адресу поштової скриньки користувача як ім'я для входу).

Рисунок 2.1 - Майстер установок - створення первинного домена

Установка пароля адміністратора

Дуже важливим аспектом безпеки Вашого сервера є пароль адміністратора. Порожній пароль не приймається. З причин безпеки пароль повинен складатися не менше ніж з шести символів.

Пароль і його підтвердження повинно бути введено в діалозі реєстрації. Ім'я 'адміністратор' може бути змінено в полі введення Username.

Вибір директорії для зберігання

Kerio MailServer зберігає відносно великий об'єм даних (поштові повідомлення, інформація про теки, записи користувача і інше). Адміністратор може зажадати зберігати дані на інший диск (на інший розділ, RAID і т.д.). Директорія для зберігання пізніше може бути змінена у будь-який час через Kerio Administration Console, після цього необхідно

перемістити файли в цю директорію. Оскільки виконання цієї операції вимагає дуже багато часу, то Kerio MailServer Engine повинен бути зупинений. Тому, рекомендується вибрати відповідну теку під час інсталяції, використовуючи майстер конфігурації (рис. 2.5).

Кнопка Change відкриє стандартний системний діалог для вибору теки.

Захист встановленого продукту

Для того, щоб гарантувати максимальний захист поштового сервера, необхідно заборонити неавторизований доступ до файлів програми (зокрема до конфігураційних файлів). Якщо використовується файлова система NTFS, то система встановлюватиме права доступу до директорії, де розташований Kerio MailServer (включаючи всі його піддиректорії - навіть якщо шлях був змінений) перед кожним стартом: право читання і запису буде дозволено тільки членам групи Administrators і локальному системному екаунту (SYSTEM); більше ніхто не зможе дістати доступу до системних файлів.

Компоненти поштового сервера Kerio

Kerio MailServer складається з наступних компонентів:

Kerio MailServer Engine - це основа програми, що забезпечує всі функції і служби. Вона запускається як фоновий додаток (як сервіс в Windows NT 4.0, 2000 або XP, або як демон в UNIX-подібних системах).

Kerio Administration Console - це універсальна програма, розроблена для локального і видаленого адміністрування продуктів Kerio. Для встановлення зв'язку з певним додатком необхідний модуль, що містить в собі інтерфейс даного додатку. В процесі установки Kerio MailServer Administration Console встановлюється разом з необхідним плагіном.

Performance Monitor. Цей компонент призначений для моніторингу компонентів KMS у реальному часі. Компонент доступний тільки для NT-систем і може бути задіяний через performance management console (perfmon.exe).

Kerio MailServer Monitor - дозволяє бачити і змінювати статус Kerio MailServer Engine (зупинено/запущено) і встановлювати властивості запуску (Engine і Monitor можуть автоматично запускатися). Крім того Monitor надає легший доступ до Administration Console. Використовується для контролю і управління станом MailServer Engine. Ця компонента працює тільки під управлінням Операційних систем Windows.

Показане зображення (ікона) - символ mailserver. Якщо mailserver зупинений, над символом з'являється червона смужка . Пуск і зупинка сервісу може зайняти декілька секунд. В цей час ікона сірого кольору і неактивна .

У Windows, подвійний клік лівою кнопкою миші по іконі запускає Kerio Administration Console (описану нижче). Клік правою кнопкою миші на іконі відкриває наступне меню.

Параметри запуску - опції для запуску Kerio MailServer і Kerio MailServer Monitor автоматично стартують при запуску системи. Обидві опції доступні за умовчанням.

Адміністрування Kerio MailServer - ця опція запускає програму Kerio Administration Console (те ж саме досягається подвійним кліком на іконі Kerio MailServer Monitor).

Запуск і зупинка Kerio MailServer - запуск або зупинка MailServer Engine (Запуск або зупинка, показані в поєднанні із статусом Engine).

Вихід - вихід з утиліти Kerio MailServer Monitor. Ця опція не зупиняє службу MailServer Engine. Користувач інформується про це вікном з попередженням.

Адміністрування Kerio Mail Server

Вікно адміністрування

Kerio Administration Console - це додаток загального призначення для адміністрування програмних продуктів Kerio Technologies. Консоль дозволяє адмініструвати продукти як локально (тобто з комп'ютера, де запущений Kerio MailServer Engine), так і видалено (з будь-якого іншого комп'ютера). Зв'язок між Kerio Administration Console і Kerio MailServer Engine шифрується, що захищає її від впроваджень і неправомірного використання.

Kerio Administration Console встановлюється разом з додатком Kerio MailServer.

Базові настройки

Служби

У меню Конфігурація > Служби користувач може встановити які служби Kerio MailServer запускатимуться і з якими параметрами. Кнопки Старт і Стоп, під таблицею використовуються, щоб запустити або зупинити відповідну службу. Доступні наступні служби:

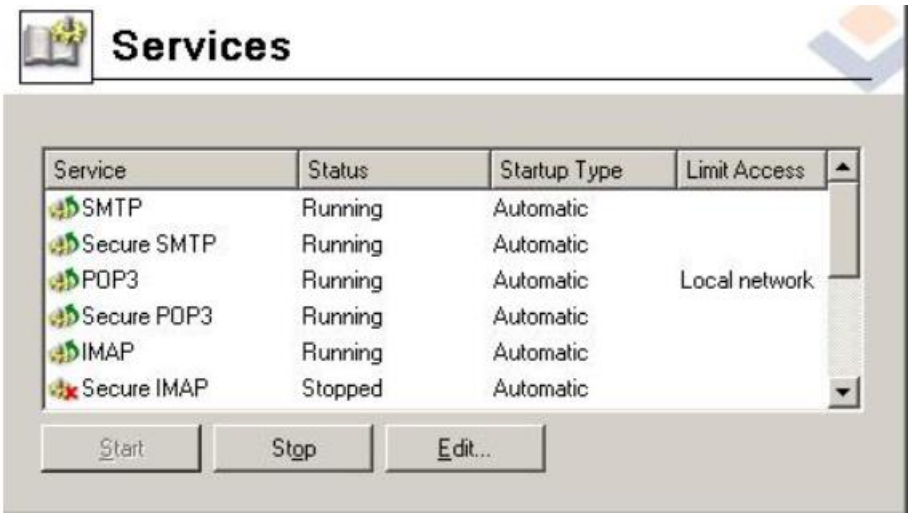


Рисунок 2.2 - Служби

SMTP

Сервер протоколу SMTP, підтримує відкриті (не зашифровані) або SSL захищені з'єднання. Сервер SMTP використовується для передачі витікаючих поштових повідомлень і для прийому вхідної пошти (якщо це первинний або резервний поштовий сервер домена).

Захищений SMTP — є сервером SMTP із захищеним доступом. Всі з'єднання зашифровані за допомогою SSL.

POP3

Сервер протоколу POP3. Цей сервер дозволяє користувачам-клієнтам відновлювати повідомлення з їх облікових записів. Часто згадується як сервер вхідних повідомлень.

Захищений POP3- є сервером POP3 із захищеним доступом. Всі з'єднання зашифровані за допомогою SSL, який запобігає несанкціонованому доступу до з'єднань.

IMAP

Сервер протоколу IMAP (протокол доступу до повідомлень в Інтернеті). Цей сервер також дозволяє користувачам діставати доступ до їх повідомлень . Проте в цьому випадку повідомлення залишаються в теках, доступ до яких може здійснюватися з будь-якого місця і в будь-який слушний для користувача час.

Захищений IMAP — є сервером IMAP із захищеним доступом.

NNTP

Протокол NNTP (Протокол передачі новин по мережі) — протокол передачі новинних конференцій через інтернет. Ця служба дозволяє користувачам бачити архів поштових відправлень до списку адресатів.

Захищений NNTP — є версією сервера NNTP, зашифрований за допомогою SSL.

LDAP

Простій LDAP сервер. Дозволяє користувачам отримувати доступ централізований керованим контактам.

Захищений LDAP — є сервером LDAP що використовує SSL шифрування.

HTTP

Протокол HTTP використовується для:

- доступу до поштових скриньок користувача через Kerio WebMail
- доступу до пошти, використовуючи мобільний телефон з WAP-поштою
- доступу до пошти, з використанням поштового клієнта — Microsoft Entourage,
- доступу до сервера — Free/Busy (для детальної інформації, дивіться розділи.
- автоматичного оновлення Kerio Outlook Connector (тільки незахищена версія).

Захищений HTTP — є захищеною версією протоколу (HTTPS — SSL або TLS шифрування).

Настройки параметрів служб

Список служб містить наступні пункти:

- Служби
- Статус (Зупинений /Запущений)
- Запуск (Вручну / Автоматично)
- Слухати IP-адреси і порти, яким дозволений доступ до служби

Параметри вибраних служб можуть бути змінені (використовується кнопка — Редагування). Ці функції так само можуть бути викликані з контекстного меню яке відкривається після кліка правою кнопкою миші по вибраній службі.

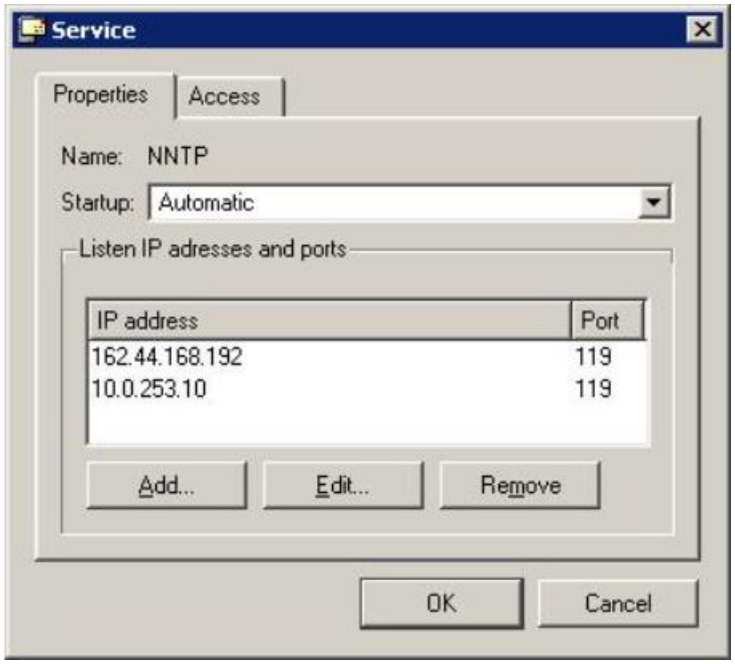


Рисунок 2.3 - Параметри служб

Настройки служби (Закладка - Свойства):

- Ім'я
- Тип служби.
- Запуск

Спосіб запуску служби (автоматично/вручну). Якщо вибраний автоматичний запуск, служба стартує негайно після завантаження Kerio MailServer. Якщо вибраний запуск уручну, служба зупинена і вона може бути знову запущена адміністратором.

Прослуховування IP-адрес і портів

Ця команда використовується для призначення портів і адрес сервера. Клацніть по кнопці Add для призначення відповідних адрес і портів. Використовуючи Kerio MailServer, служби можуть бути сполучені з різними IP-адресами. Служба на кожній IP-адресі може використовувати різні порти для зв'язку. Це означає те, що два різних веб-сервера на двох різних IP-адресах можуть бути сполучені через стандартний порт 80.

Більшість служб використовують стандартні порти і не рекомендується змінювати їх без необхідності (наприклад, у разі конфлікту з іншим додатком того ж типа). Кликніть Default для відновлення настройок за умовчанням.

Обмеження доступу до служби (Закладка — Доступ):

Дозволити доступ тільки від.

Дозволяє доступ до вибраної служби тільки обмеженим IP-адресам (визначений у вибраній групі). Група IP-адрес може бути визначена в секції — Конфигурация/Определения/Группы IP-адрес або безпосередньо в цьому діалоговому вікні, натиснувши на Кнопку-Редактировать.

Детальна політика доступу для служби SMTP може бути встановлена в секції — Конфигурацыя/АнтиСпам.

Дозволити доступ анонімам

Ця опція доступна тільки в службі NNTP (S), тому вона не міститься в діалогових вікнах інших служб. Ця опція дозволяє анонімний доступ до сервера NNTP. Це означає що будь-хто може реєструватися в списку розсилки анонімно.

Максимальна кількість паралельних з'єднань

Ця опція обмежує кількість паралельних з'єднань у вибраній службі. Дуже велика кількість паралельних з'єднань можуть стати причиною перевантаження сервера, яке згодом може привести до його відмови. Це також хороша ідея для запобігання так званих DoS — атак (Відмова в обслуговуванні).

Домени

Kerio MailServer може служити декільком незалежним поштовим доменам. Кожен домен може містити будь-яке число псевдонімів (тобто еквівалентних доменів). Еквівалентні домени — ті домени, де всі облікові записи користувачів рівнозначні і повідомлення, фізично, зберігаються в одній поштовій скриньці.

Цей принцип краще всього буде проілюстрований наступним прикладом:

Поштовий сервер обслуговує два домени, що належать двом різним компаніям. Перша компанія використовує доменні імена ourcompany.com і ourproduct.com, тоді як інша компанія використовує доменне ім'я anothercompany.com. Очевидно, що адреси info@ourcompany.com і info@ourproduct.com рівнозначні (доставляються одному адресату), тоді як пошта для info@anothercompany.com повинна бути доставлена в іншу поштову скриньку. Це має на увазі, що, тоді як домен ourproduct.com може бути визначений як псевдонім ourcompany.com, домен othercompany.com повинен бути незалежним від двох інших.

В цьому випадку облікові записи користувачів визначені в кожному домені окремо. Тому домени повинні бути визначені до створення облікових записів. У Kerio MailServer один з доменів завжди встановлюється як первинний. Первинний домен може бути замінений на будь-який інший домен створений в Kerio MailServer. Звичайно, первинним доменом є той який був створений першим. Як тільки домен встановлюється як первинний цього вже не можна змінити (якщо тільки ви не видаляєте всі домени). При реєстрації в первинному домені користувачі використовують тільки свої імена, тоді як для реєстрації у всіх інших доменах вони повинні реєструвати повну електронну адресу. Це знову краще всього показати на прикладі:

Домен ourcompany.com встановлений як первинний домен. Домен anothercompany.com також створений. Користувач визначений в обох доменах з одним ім'ям user. При реєстрації в домені ourcompany.com користувач використовує тільки ім'я user, тоді як при реєстрації в другому домені користувач повинен буде реєструватися з ім'ям user@anothercompany.com

Відзначте: Користувачі первинного домена також можуть авторизуватися свої повним ім'ям.

Визначення доменів

Домени визначаються в Конфігурація > Домени

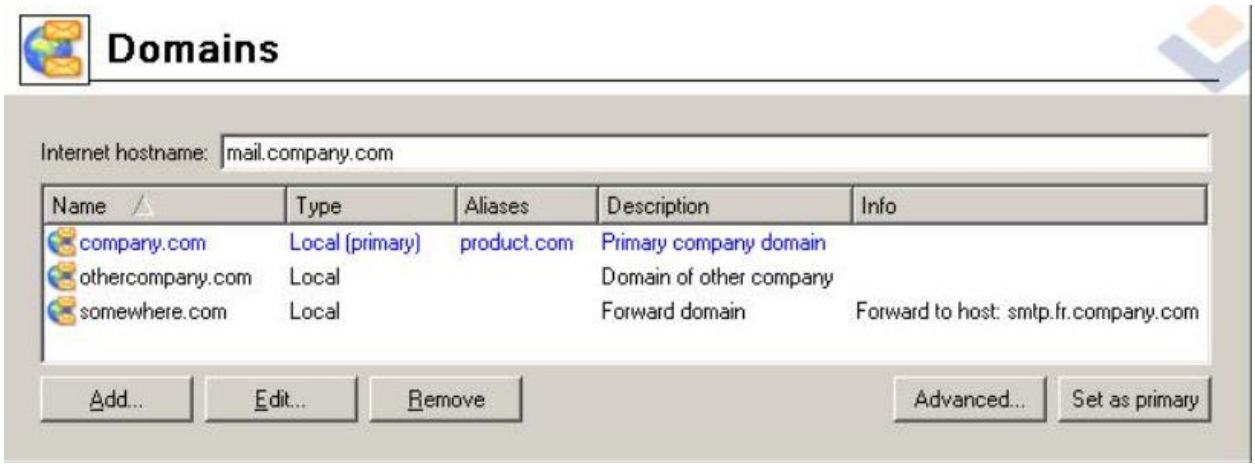


Рисунок 2.4 - Домени

У полі ім'я Інтернет хосту введіть Інтернет ім'я комп'ютера на який встановлений Kerio MailServer (звичайно це ім'я комп'ютера з приєднаним ім'ям первинного домена — в цьому випадку ім'я сервера автоматично генерується майстром настройок (configuration wizard)). Імена серверів використовуються для розпізнавання сервера під час обміну інформацією протоколом SMTP.

Натисніть (Advanced) Розширений вибір для установки місцеположення загальнодоступних тек:

- Unique for each domain (унікальні для кожного домена) — кожен домен містить власні загальнодоступні теки. Ця конфігурація не дозволяє користувачам одержувати доступу до тек іншого домена.
- Global for all domains (загальні для всіх доменів) — користувачі всіх доменів спільно використовують одні і ті ж загальнодоступні теки.

Використовуйте Set as primary (Встановити як первинний) для установки типу домена (те ж саме може бути виконано з використанням контекстного меню). Будь-який домен визначений першим завжди є первинним [Local (primary)]. Інші домени можуть бути встановлені як Local (primary) або просто як Local. Таким чином після даної операції новий домен стає первинним, а старий тільки локальним (Local)

Створіть новий домен натисненням клавіші «Додати».

Основні параметри домена

Закладка Загальна:

Домен - Ім'я нового домена

Опис - Запис про створення домена (тільки для адміністраторів).

Еквівалентні домени — закладка псевдонімів

У цьому діалоговому меню можуть бути визначені домени еквівалентні поточному. Адреси електронної пошти усередині цих доменів ідентичні (листи доставляються користувачам з однаковим ім'ям). Мета цієї опції — дозволити користувачу бути частиною безлічі доменів.

Попередження: повинні бути зроблені відповідні записи DNS для кожного окремого домена, якщо це не локальний псевдонім. Просте визначення домена як псевдонім іншого домена не створюватиме домена в Інтернеті.

Forwarding (Пересилка)

Використовуючи дане поле ви можете встановити автоматичну пересилку повідомлень до іншого SMTP сервера.

Якщо одержувач не був знайдений.

Повідомлення буде переслане іншому SMTP серверу, якщо одержувач не був знайдений в даному домені. Повідомлення пересилаються, якщо адреса одержувача не є адресою користувача, групи користувачів або псевдоніма даного домена. Якщо в даному домені користувачі, групи користувачів або псевдоніми не визначені, всі повідомлення також пересилаються.

Переслати серверу

- Ім'я DNS або IP адреса SMTP сервера, якому пересилаються всі листи для цього домена.
- Порт

У нормальних обставинах Kerio MailServer посилає пошту для Forward domain (домена пересилки) до вказаного SMTP сервера негайно. Якщо сервер використовує dial-up комутоване з'єднання з Internet — це може викликати дуже часте з'єднання і розрив зв'язку (і високу вартість з'єднання). Вибір цієї опції дозволяє ставити в чергу планувальника повідомлення, що пересилаються.

Черга буде до запуску ETRN

Kerio MailServer Kerio MailServer не відправляє листи цього домена до вказаного SMTP сервера, поки не одержить ETRN команду від сервера. Цим Способом Kerio MailServer може скористатися як вторинний сервер для домена, чий первинний SMTP сервер в даний момент не сполучений з Інтернетом.

Якщо домен…

Тут Ви можете визначити, чи будуть переслані повідомлення, які містять один з псевдонімів домена в адресі одержувача. Ця опція дозволяє уникнути зациклення, у випадку якщо потрібний одержувач не був знайдений ні на одному з серверів з якими працює даний домен.

Видалення доменів

Ви можете видалити домен використовуючи клавішу видалення. Домен не може бути видалений, якщо це первинний домен.

Проте, ви може зробити новий домен і визначити його як первинний, а потім видалити потрібний вам домен.

Облікові записи і групи користувачів.

Облікові записи користувачів

Облікові записи користувачів в Kerio MailServer є фізичними поштовими скриньками. Користувачі дістають доступ до поштових скриньок, ідентифікуючись ім'ям користувача і паролем. Оскільки Kerio MailServer може обслуговувати декілька

незалежних доменів, облікові записи користувачів дійсні не скрізь, а тільки для конкретного домена. Це припускає, що домен повинен бути визначений до того, як будуть створені облікові записи користувачів (детальніше про це можна прочитати у розділі Домени).

Обліковий запис адміністратора

Разом з доступом до поштової скриньки, обліковий запис користувача також використовується для доступу до адміністрування Kerio MailServer, за умови, що користувач має відповідні права. Основний обліковий запис адміністратора створюється під час установки. Вона має ті ж властивості, що і інші облікові записи користувачів, і може бути видалена будь-яким користувачем з правами доступу на читання/запис.

За умовчанням, обліковий запис адміністратора може створювати загальні теки і управляти ними. Загальні теки можуть бути створені за допомогою Kerio WebMail (за детальнішою інформацією звернетеся до керівництва по Kerio WebMail) або за допомогою MS Outlook, якщо він містить розширення Kerio Outlook Connector.

За умовчанням, обліковий запис адміністратора також управляє теками архівів. Будь-яке повідомлення, що пройшло через Kerio MailServer, може бути знайдено в архіві.

Адміністратор може дозволити іншим користувачам доступ до архівних тек. Проте, після того, як повідомлення всіх користувачів заархівували, доступ до цих тек повинен одержати тільки конфіденційний адміністратор (або вузька група конфіденційних персон).

Спеціальні облікові записи: Anyone і authuser

Anyone і authuser — це спеціальні призначені для користувача облікові записи, які допомагають управляти правами окремих користувачів. Ці облікові записи не присутні в таблиці користувачів Users.

Опція anyone вирішує доступ для всіх користувачів. Опція authuser може бути використана для дозволу доступу всім користувачам, авторизованим на Kerio MailServer.

Створення нового облікового запису

Новий обліковий запис для користувача може бути визначений в секції Domain Settings > Users.

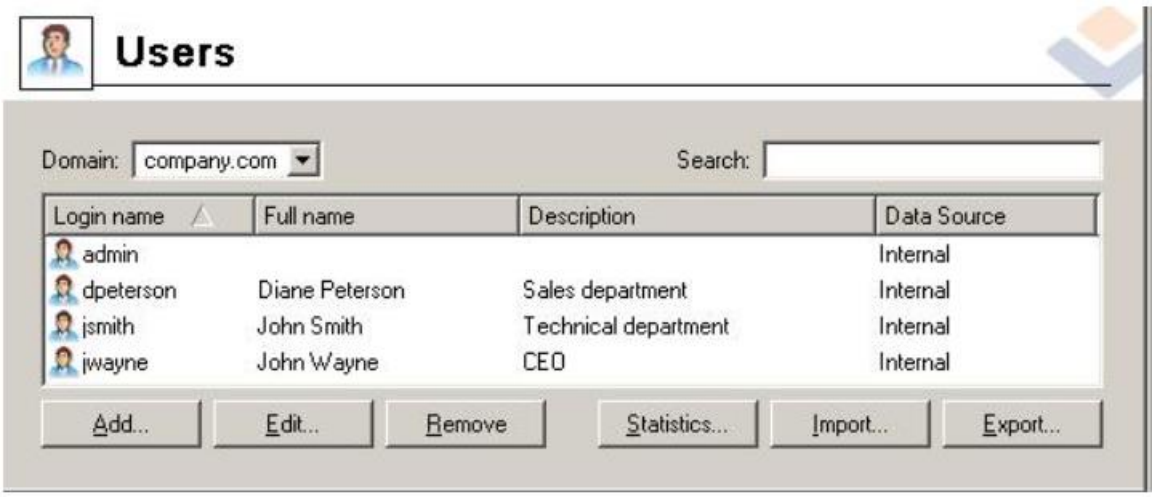


Рисунок 2.5 - Облікові записи користувачів

Спочатку, виберіть локальний домен в полі Domain, в якому цей обліковий запис буде визначений. Кожен домен може включати локальні облікові записи, а також облікові

записи, що зберігаються в службі каталогів (наприклад, Microsoft Active Directory). І ті, та інші можуть бути показані в розділі користувачів Users в Kerio Administration Console. Проте, додані можуть бути тільки локальні облікові записи (облікові записи для служби каталогів повинні бути створені відповідними адміністраторськими утилітами, наприклад Active Directory Users and Computers). Облікові записи, що входять в службу каталогів, не можуть бути видалені. Можна тільки відредагувати деякі їх характеристики.

Натисніть на кнопку Add, щоб відкрити керівництво по створенню нового призначеного для користувача облікового запису. Якщо домен налаштований на використання служби каталогів (дивися Домени), то висвітиться діалог, де ви зможете визначити, чи хочете ви активувати користувача із служби каталогів, або створити новий локальний обліковий запис.

Якщо користувач активований, то обліковий запис записується в службу каталогів. З моменту активації обліковий запис може бути використаний Kerio MailServer. Всі події і інформація будуть записані в службу каталогів.

Якщо вибрана опція активації користувача в службі каталогів Activate user in directory service, то відкриється діалог із списком користувачів бази даних LDAP, який використовує Kerio MailServer. Виберіть необхідних користувачів і підтвердіть вибір. Також, ви можете використовувати кнопку Select all щоб вибрати всіх користувачів, або кнопку Unselect all щоб відмінити виділення.

Далі в буде показано, як можуть бути визначені локальні облікові записи.

Крок 1 — основні дані:

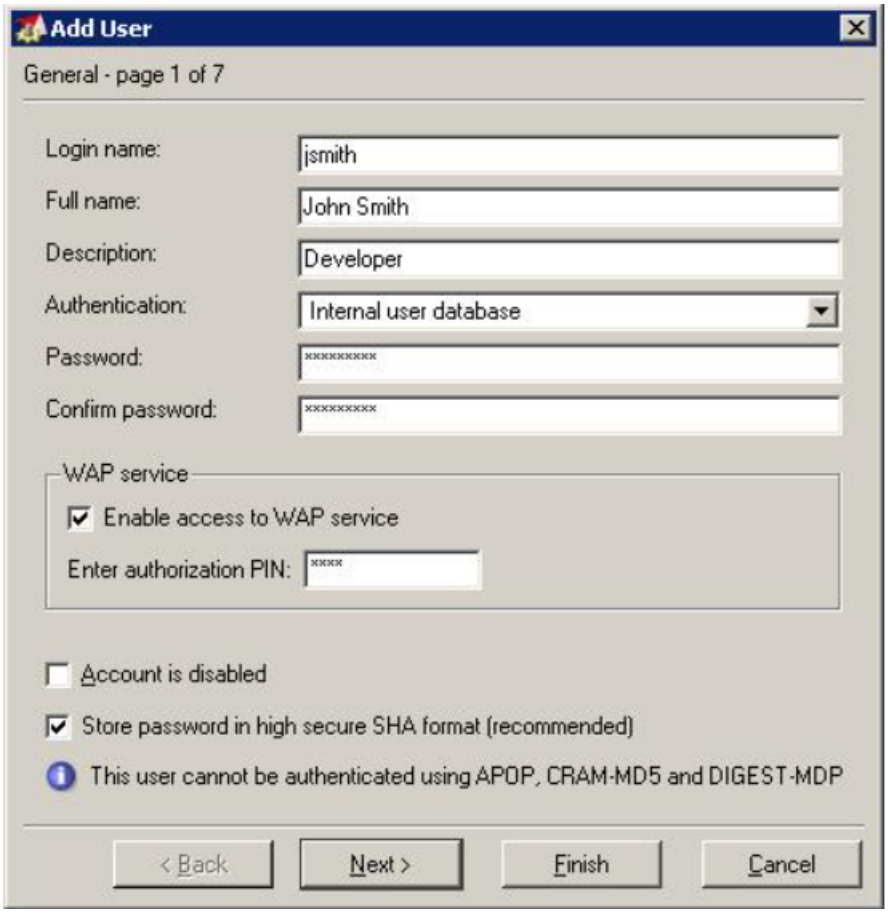


Рисунок 2.6 - Додавання нового користувача — основні дані

Login Name

Реєстраційне ім'я (Примітка: якщо домен не локальний і не первинний, то користувач повинен входити в систему, використовуючи свою поштову адресу, наприклад user@othercompany.com, а не просто user).

Ім'я користувача нечутливо до регістра.

Full Name

Звичайно ім'я і прізвище користувача.

Description

Опис користувача (наприклад, посада в компанії).

Поля Full Name і Description використовуються тільки в інформативних цілях. Вони можуть містити будь-яку інформацію або залишатися порожніми.

Authentication

Метод, по якому відбувається ідентифікація користувача (дивися нижче).

Password / Confirm Password

Пароль може бути введений або змінений тільки для локального користувача. Ми настійно рекомендуємо змінити пароль відразу після створення облікового запису.

WAP Service

Kerio MailServer дозволяє дістати доступ до пошти з мобільного телефону через протокол WAP. Цей інтерфейс називається WAPmail (він використовує ті ж порти, що і сервіси HTTP і Secure HTTP).

Для запуску цього сервісу, відзначте Enable access to WAP service і введіть як мінімум 4 цифри (максимально можна ввести 32 цифри) для визначення свого цифрового PIN коду. Цей код використовуватиметься для авторизації в сервісі.

Store password in high secure SHA Store password in high secure SHA format (recommended)

Паролі користувачів шифруються симетричним ключем (DES). Опція Store password in high secure SHA format дозволяє використовувати безпечніший, не симетричний метод шифрування (алгоритм SHA), так що немає ніякої можливості одержати пароль. Проте, коли використовується шифрування SHA, неможливо авторизувати користувачів для доступу до Kerio MailServer, користуючись методами APOP CRAM-MD5 і Digest-MDP. Авторизація вимагає перевірки NTLM, реєстраційного імені або незашифровану перевірку — у разі незашифрованої перевірки, настійно рекомендується використовувати для зв'язку тільки SSL протокол.

Після того, як опція буде відмічена, необхідно змінити пароль користувача. Це може зробити тільки адміністратор через консоль адміністратора (Administration Console).

Account is disabled

Тимчасове блокування облікового запису. Видаляти для тимчасового блокування запис не знадобиться.

Можливі способи авторизації:

Internal user database

Користувач авторизується тільки усередині Kerio MailServer. В цьому випадку необхідно ввести пароль в поля Password і Confirm Password (надалі, користувач зможе змінити свій пароль за допомогою інтерфейсу Kerio WebMail).

Увага: Пароль може містити друкарські символи (цифри, знаки пунктуації) і є регістро залежним.

Kerberos 5

Авторизація проводиться системою, авторизації Kerberos версії, 5. Цей метод авторизації використовує Active Directory.

PAM service

Авторизація з використанням сервісу PAM (Змінний модуль авторизації) доступна тільки в операційних системах Linux.

Apple Open Directory

Авторизація до бази даних Apple Open Directory (тільки для Apple Macintosh).

Крок 2 — поштові адреси

У цьому кроці будуть визначені всі необхідні користувачу поштові адреси. Первинна адреса користувача (він не може бути видалений) складається з імені користувача і домена, в який входить обліковий запис користувача. Інші адреси називаються aliases (псевдоніми). Вони можуть бути визначені як під час створення користувача, так і в Domain Settings/Aliases. Рекомендується використовувати перший варіант — він простіший і псевдоніми доступні через Active Directory.

Крок 3 — пересилка повідомлень на інші адреси

Якщо відмічено, то повідомлення для користувача можна пересилати на інші поштові облікові записи. Якщо активована кнопка Deliver messages to., то повідомлення будуть записані в локальному обліковому записі, а потім послані на адреси, визначені користувачем (інакше повідомлення будуть тільки послані і не записані).

Крок 4 — Групи

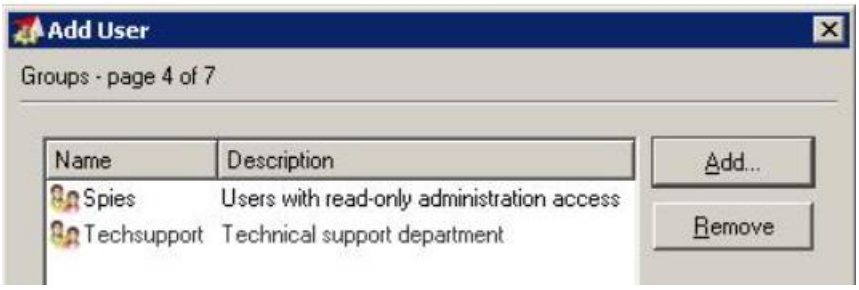


Рисунок 2.7 - Додавання нового користувача — групи

У цьому вікні діалогу ви можете додати або видалити групи, в яких полягає користувач. Спочатку групи повинні бути створені в секції Domain Settings > Groups. Ви можете додати користувачів до груп під час визначення груп. Проте, не важливо що створено першим — користувачі або групи.

Крок 5 — Права доступу:

Кожному користувачу повинен бути призначений один з трьох рівнів прав доступу, перерахованих нижче.

No access to administration

Ці користувачі не мають якого-небудь доступу до адміністрування Kerio MailServer. Більшість користувачів мають цей рівень доступу, так що вони мають доступ тільки до своїх поштових скриньок.

Read only access

Ці користувачі мають доступ до адміністрування Kerio MailServer, але можуть тільки дивитися журнали і установки; вони не можуть нічого міняти.

Read/Write access

Ці користувачі мають повні права доступу на адміністрування і прирівнюються до облікового запису Admin. Якщо в системі є хоч би один користувач з такими правами, то обліковий запис Admin може бути видалений.

Крок 6 — Квота:

Ви можете встановити обмеження для поштової скриньки кожного користувача.

Disk space

Максимальна кількість місця для поштової скриньки. Для більшої зручності, значення для введення ви можете вказати в кілобайтах (KB), мегабайтах (MB) або гігабайтах (GB).

Number of messages

Максимальна кількість повідомлень в поштовій скриньці. Повідомлення, що перевищують цю кількість, будуть знехтувані поштовим сервером.

Призначені для користувача квоти запобігають захаращенню диска сервера. Якщо яке-небудь з обмежень досягнуте, будь-які нові повідомлення будуть знехтувані сервером.

Якщо квота перевищена, то користувач буде проінформований про це поштою і йому буде дана рада видалити деяку кількість повідомлень в своїй поштовій скриньці.

Значення будь-якого з цих пунктів може бути встановлено в 0 (нуль), що означає відсутність обмеження для поштової скриньки по цьому пункту.

Крок 7 — розширені установки

Відзначте цю опцію, щоб додати користувача до теки загальних контактів.

Редагування облікових записів користувача

Кнопка Edit відкриває діалогове вікно, де ви можете редагувати параметри облікового запису користувача. Це діалогове вікно містить всі описані вище характеристики облікового запису, розділені в одному вікні на вкладки.

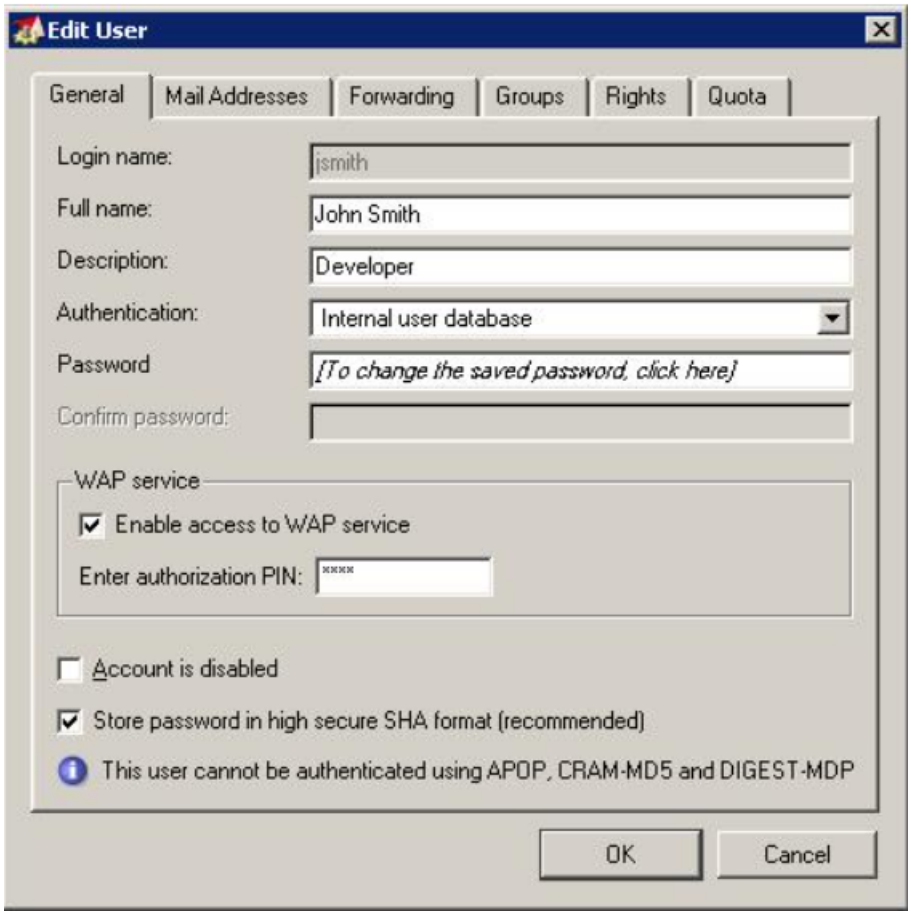


Рисунок 2.8 - Редагування облікового запису користувача

Поточні значення квот можуть бути знайдені у вкладці Quota. Відсоток використання не виводиться, поки квота не визначена (обмежена).

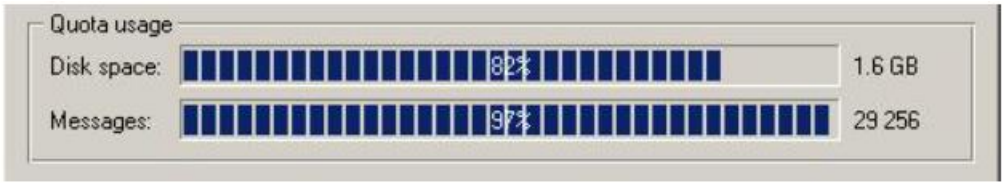


Рисунок 2.9 - Квота визначена

У вкладці Rights, для користувача може бути дозволено або заборонено адміністрування загальними теками.

Редагування декількох користувачів

Kerio MailServer дозволяє користувачам редагувати одночасно декілька облікових записів користувача. Просто натисніть клавішу Shift і відзначайте облікові записи мишкою, а потім натисніть кнопку Edit.

Діалогове вікно містить три вкладки. За допомогою цих вкладок можна змінювати установки квот, права користувача і інші основні настройки (опис облікового запису, тип авторизації, безпечніша форма пароля, тимчасове виключення облікового запису).

Це діалогове вікно дозволяє редагувати тільки ті елементи, які можуть бути змінені у всіх вибраних облікових записах. Те ж саме можна сказати про Store password in high secure SHA format і Account is disabled на вкладці General. Для опцій доступні наступні стани:

- Неактивно, сірого кольору — кожний з вибраних облікових записів зберігає своє значення за умовчанням.
- Відмічено — елемент буде відмічений у всіх облікових записах.
- Не відмічено — елемент не буде відмічений у всіх облікових записах.

Вкладки Rights і Quota звичайно використовуються для редагування облікових записів поодинці.

Пошук

Використовуйте поле Search для проглядання специфічних опцій в списку користувачів. Коли ви вводите текст в поле Search, таблиця виведе список опцій, що містять цей рядок.

Статистика

Статистика користувача починає записуватися відразу після того, як буде встановлений Kerio MailServer. Щоб зберегти статистику навіть у тому випадку, коли сервер вимкнений, дані по кожному користувачу записуються у файл stats.usr у кореневій директорії сервера.

Використовуйте кнопку Statistics в секції Domain Settings > User Accounts для того, щоб відкрити таблицю статистики, в яку входять вибрані облікові записи, сервіси, на які посилається статистика, останній вхід (день і час самої останньої авторизації в сервісі) і сума входів (загальна кількість авторизацій для кожного користувача).

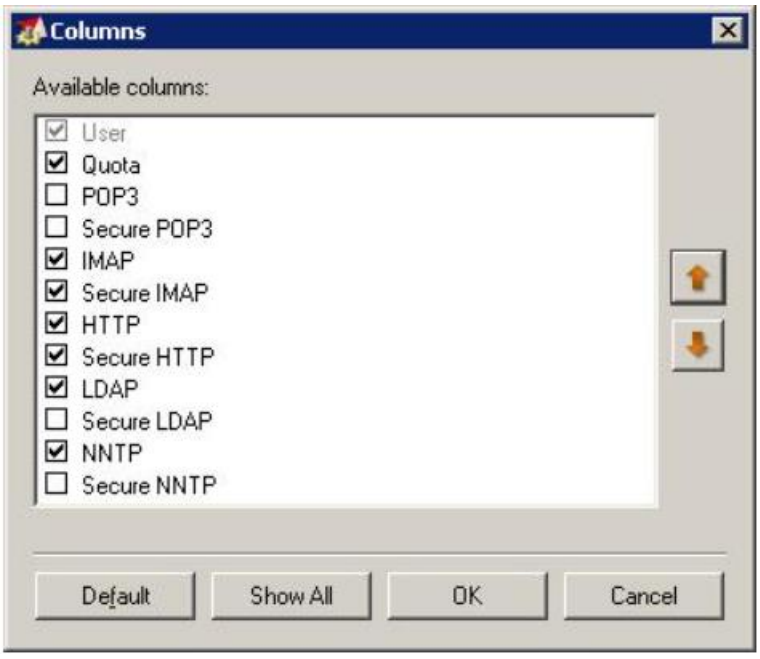


Рисунок 2.10 - Вибір колонок для статистики

Адміністратор Kerio MailServer може набудувати вид відображення інформації в індивідуальних секціях. Клацніть правою клавішею миші в діалозі Statistics щоб викликати контекстне меню з опцією Modify columns. Під час вибору цієї опції висвітиться діалогове вікно, де адміністратор може вибрати, які колонки показувати, а які приховати.

Натисніть на кнопку Default щоб відновити установки за умовчанням, а також порядок проходження елементів. Натисніть на кнопку Show All щоб відзначити всі колонки без змін у порядку їх проходження.

Кнопки Move up і Move down переміщають вибрану колонку вгору або вниз усередині групи. Це дозволяє користувачам визначати порядок, в якому висвічуватимуться колонки.

Імпорт Користувачів

Облікові записи користувачів можуть бути як заведені вручну, так і імпортовані з інших джерел .

Кнопка Import розташована під списком користувачів і відкриває діалогове вікно для імпорту користувачів. Використовуйте опцію Import users from щоб вибрати джерело, з якого імпортуватимуться користувачі.

NT Domain

В цьому випадку, необхідним параметром є NT domain name. Комп'ютер, на якому запущений Kerio MailServer, повинен входити в цей домен.

Не імпортуйте користувачів цим шляхом, якщо контроллер доменів працює під операційною системою Windows 2003 Server! У разі наявності доменів під контролем цих операційних систем, імпортуйте користувачів з Active Directory — дивитеся нижче.

Active Directory

Для того, щоб імпортувати користувачів з Microsoft Active Directory, вам потрібно надати наступну інформацію:

- Active Directory domain name — ім'я домена, звідки будуть імпортовані користувачі (у форматі доменів DNS — тобто domain.com)
- Import from server — ім'я сервера, на якому, під вищезгаданим доменом, працює Active Directory
- Login as user, Password — ім'я і пароль користувача, що має обліковий запис в домені. Для зміни і запису настройок не потрібні права на запис.
- LDAP filter — за допомогою цього елементу, можуть бути визначені запити до сервера LDAP для імпорту користувачів.

Рекомендується, щоб цю опцію використовували тільки досвідчені користувачі. За детальнішою інформацією про синтаксис цих запитів ви можете звернутися до технологічного керівництва до сервера LDAP.

Якщо вся необхідна інформація була введена правильно і відповідний сервер доступний, після натиснення на кнопку OK висвітиться список користувачів. З цього списку ви можете вибрати користувачів, які будуть імпортовані в Kerio MailServer. Ви можете також вибрати шаблон, який використовуватиметься для створення цих користувачів в Kerio MailServer. Якщо шаблон не буде вибраний, то використовуватиметься шаблон за умовчанням.

Якщо користувачі імпортуються з Active Directory, то не важливо на якій платформі працює Kerio MailServer.

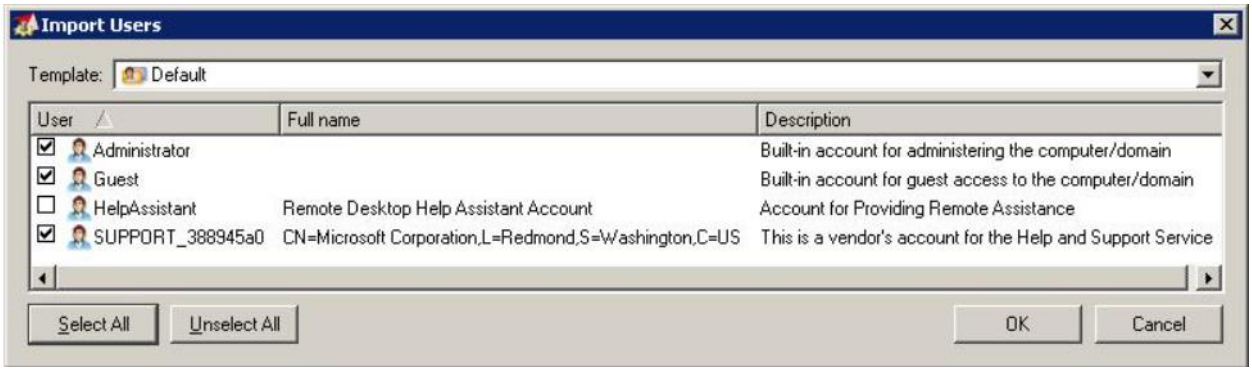


Рисунок 2.11 - Вибір користувачів для імпорту

Спосіб авторизації буде встановлений залежно від того, звідки були імпортовані користувачі: NT Domain для користувачів, імпортованих з домена NT і Kerberos 5 для користувачів, імпортованих з Active Directory (Active Directory використовує за умовчанням систему авторизації Kerberos 5).

Експорт в Адресну Книгу

Інформація про вибраних користувачів (локальних облікових записах або облікових записах в службі каталогів) може бути експортована в загальний файл (загальну адресну книгу) шляхом натиснення на кнопку Export to Address Book. Ця кнопка виводить діалог, де може бути вибрана тека для даних, що експортуються, і користувачів.

Якщо жодної загальнодоступної адресної книги не визначено, то в процесі першого експорту буде автоматично створена тека #public/Contacts

Експортуються тільки повні імена і поштові адреси. Інші параметри неістотні, проте вони можуть бути додані користувачами з відповідними правами, наприклад через інтерфейс Kerio WebMail.

Групи користувачів.

Облікові записи користувачів в межах кожного домена можуть бути відсортовані по групах.

Головні причини для створення груп користувачів — це:

- Для деяких груп користувачів з псевдонімами може бути створений групова адреса— пошта, послана на цю адресу, буде одержана всіма членами групи.
- Для групи користувачів можуть бути призначені певні права доступу. Ці права доступу доповнюють права доступу, визначені для кожного конкретного користувача.

Ви можете визначити групи користувачів в секції Domain Settings > Groups.

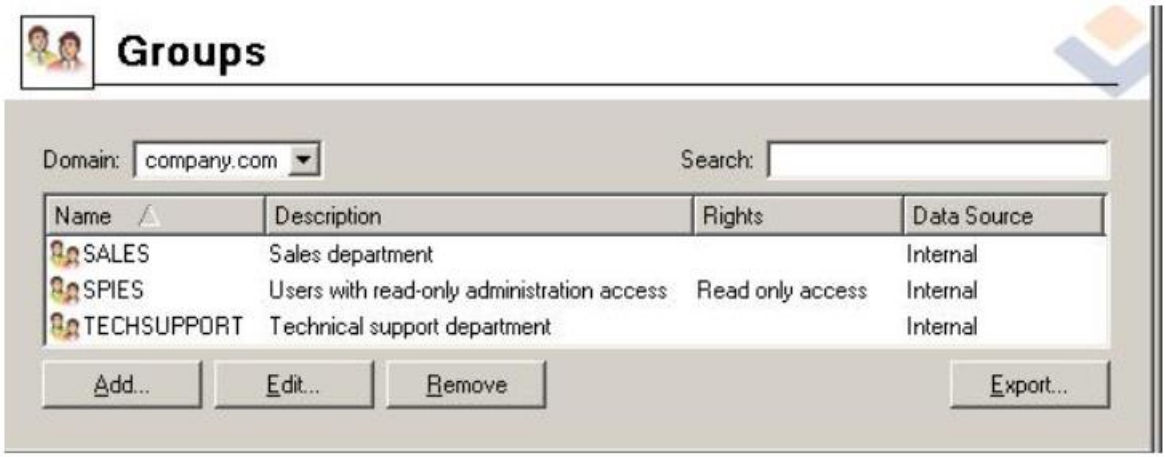


Рисунок 2.12 - Групи

Поле Search і кнопка Export мають те ж призначення, що і для секції Users.

Створення Груп Користувачів

Створіть нову групу, натиснувши на кнопку Add. Відкриється керівництво по створенню груп користувачів.

Крок 1 — Ім'я і опис групи:

Name Унікальне ім'я групи.

Description Опис групи. Може залишатися незаповненим.

Крок 2 — поштові облікові записи

Цей крок визначає всі необхідні поштові облікові записи (псевдоніми) для групи. На відміну від користувачів, групи не мають неявних псевдонімів. Інакше кажучи, якщо група створюється без псевдонімів, то KMS не зможе доставити жодного листа в цю групу до тих пір, поки їй не буде зіставлена поштова адреса.

Адреси груп можуть бути визначені як в описі групи, так і в секції Domain Settings > Aliases. Рекомендується визначати псевдоніми в описі груп, оскільки в цьому випадку їх краще і простіше адмініструвати.

Крок 3 — Члени групи

Використовуючи кнопки Add і Remove ви можете додавати або видаляти користувачів в групі. Якщо не створено жодного облікового запису користувача, то група може залишатися порожньою і користувачі можуть бути додані в ній у міру додавання в систему.

Крок 4 — Права доступу для групи

Групі може бути привласнений один з трьох рівнів прав доступу:

- No access to administration Користувачі в цій групі не мають доступу до адміністрування Kerio MailServer.
- Read only access Користувачі в цій групі можуть входити в адміністрування Kerio MailServerале можуть тільки проглядати журнали роботи і настройки. Користувачі з цієї групи не можуть змінювати настройки.
- Read/Write access Користувачі в цій групі мають повні права доступу.

Групові права доступу комбінуються з правами доступу користувача. Це має на увазі, що підсумкові права доступу для користувача відповідатимуть як його власним правам доступу, так і правам доступу для групи, залежно від того, чиї права мають вищий пріоритет.

Крок 5 — розширені настройки:

Відзначте цю опцію, щоб додати користувача в загальну теку контактів.

Шаблони користувацьких екаунтів

Шаблони спрощують створення велику кількість призначених для користувача екаунтів (наприклад, для користувачів одного домена). У шаблоні можна визначити всі параметри екаунта, окрім імені користувача і пароля (якщо використовується внутрішня аутентифікація). При використанні шаблонів призначений для користувача екаунт може бути визначений заповненням наступних полів: NameFull Name і Description (а також, можливо, полів Password і Confirm Password). Поля Full Name і Description не обов'язкові для заповнення. У простому випадку необхідно заповнити тільки одне поле — ім'я користувача.

Задання шаблону

Задати шаблон можна в розділі Configuration > Definitions > User Templates. Діалогове вікно створення або редагування шаблону практично ідентично вікну створення призначеного для користувача екаунта.

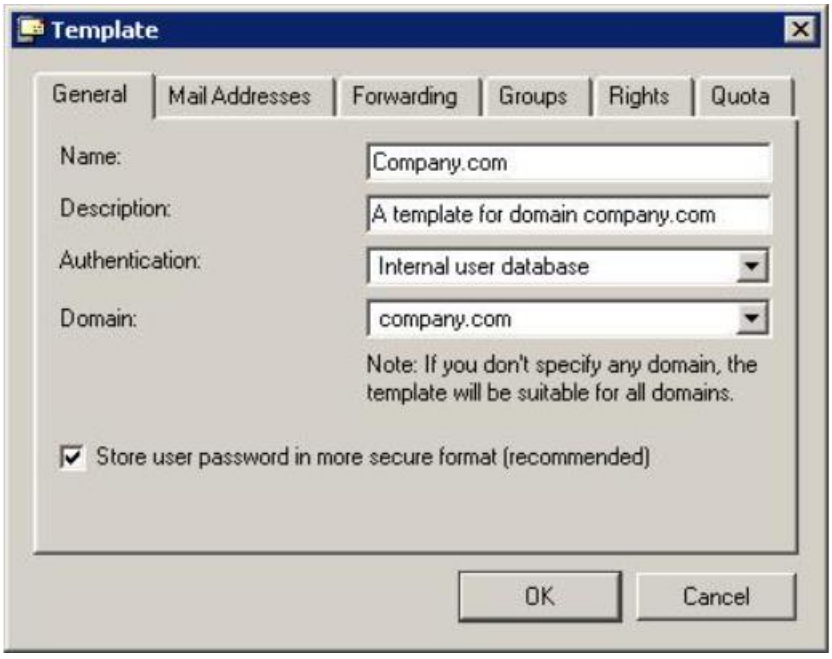


Рисунок 2.13 - Задання шаблону

Ім'я

Назва шаблону (унікальне ім'я, яке використовується для ідентифікації шаблону).

Опис Тут указується опис шаблону, воно відображається поряд з його назвою в списку шаблонів. Також воно копіюється в полі Description у призначеному для користувача екаунте, що використовує даний шаблон.

Аутентифікація

Використовуваний метод аутентифікації.

Домен

Домен, для якого використовуватиметься даний шаблон. Можна вибрати один з локальних доменів, визначених в Kerio MailServer. Якщо домен не вказаний, шаблон може бути використаний для створення і редагування призначених для користувача екаунтів в будь-якому домені (загальний шаблон).

Зберігати пароль в найбільш безпечному форматі

Паролі користувачів кодуються симетричними ключами (DES). Опція Store user password in more secure format дозволяє використовувати безпечніший, несиметричний метод кодування (алгоритм SHA), що робить відновлення пароля неможливим. При використанні SHA неможлива аутентифікація користувачів Kerio MailServer методами APOP CRAM-MD5 і Digest-MD5. Аутентефікация вимагає перевірки NTLM або незашифрованої текстової перевірки. У останньому випадку рекомендується використовувати тільки SSL з'єднання.

При включенні цієї опції необхідно змінити пароль користувача. Це може зробити тільки адміністратор або користувач (наприклад, за допомогою програми WebMail або іншого поштового клієнта).

Всі поля в діалоговому вікні ті ж, що і у вікні налаштувань екаунта користувача. Значення, введені тут, автоматично змінять відповідні поля в створюваному екаунті.

Використання шаблонів

Створений шаблон може бути відразу ж використаний для створення призначеного для користувача екаунта в розділі Domain Settings > Users. Якщо визначений хоч би один шаблон те при натисненні кнопки Add з'явиться вікно вибору шаблону.

У вікні відображатимуться тільки шаблони, визначені для вказаного домена або шаблони з не вказаним доменом (загальні шаблони). Опція Default дозволяє створювати екаунт без використання шаблонів (більшість полів будуть порожньою або міститиме значення за умовчанням).

При виборі шаблону вікно створення призначеного для користувача екаунта міститиме відповідні значення в тих або інших полях.

Тестування роботи протоколів з використанням Telnet

SMTP

Запускаємо cmd.exe і набираємо команду:

telnet your smtp server порт.

Порт smtp сервера за замовчуванням – 25 Після установки з'єднання з віддаленим сервером ми отримаємо вітання:

Сервер дав нам відповідь і нам необхідно відповісти. Для цього відправляємо команду HELO Ім’я свого домену:

HELO SPIDER

У разі успішного виконання команди сервер нам поверне код 250> можна продовжувати далі.

Повідомимо серверу відправника листа:

MAIL FROM:

У відповідь на цього отримаємо знову повідомлення з кодом 250, що свідчить про успішне виконання команди. Зверніть увагу, що в MAIL FROM потрібно указувати свій ящик на цьому сервері. Хоча ніщо не заважає вказати ящик іншого користувача на цьому ж сервері.

Нижче приведена решта частини «діалогу» з smtp сервером, з необхідними коментарями. Стрічки, що починаються з символу «>» означають, що цю команду посилає клієнт, а символом «<» символізуватимуться відповіді сервера.

> RCPT TO: //Отримувач (і) повідомлення

< 250 Accepted

> DATA //Після цієї команди відправляється заголовок і тіло листа

//Сервер дозволяє введення тексту повідомлення. По завершенню набору потрібно відправити символ крапки на новому рядку.

< 354 Enter message. Ending with “.” on a line by itself

> From: //Від кого

> To: //Кому

//Кодування листа

> Mime-Version: 1.0

> Content-Type: text/plain; charset=”windows-1251”

//Текст повідомлення

> Це текст повідомлення

//Даємо зрозуміти серверу, що наше повідомлення сформоване

>.

< 250 OK id = 1bKd33kk33

//Завершуємо з'єднання з сервером

> QUIT

< 221 smtp.inbox.ua closing connection

Завершення сеансу

POP3

Спілкування клієнта з POP3 сервером схоже з SMTP. У цьому протоколі також визначений набір команд, за допомогою якого і відбувається обмін інформацією. Для кращого розуміння, знову ж таки приведу приклад – типову сесію з'єднання через telnet з pop3 сервером провайдера.

//З'єднання з pop3 сервером встановлене
<+OK

//Відправляємо свій логін
> USER spider_net@inbox.ua

//Такий користувач існує
< +OK Password required for user spider_net@inbox.ua

//Надсилаємо свій пароль
> PASS 1234

//Вхід успшний, в ящику 7 листів
< +OK spider_net@inbox.ua maildrop has 7 messages (45056 octets)

//Запит списку листів
> LIST

//Всього сім листів, загальним розміром 45056
< +OK 7 messages (45056)
//далі йде список листів у форматі: «номер листа» «розмір»
< 1 2204
< 2 2304
..
.
//Запит листа з ідентифікатором 1
> RETR 1

//Текст листа
.

//Позначаємо на видалення лист з ідентифікатором 1
> DELE 1
< +OK message 1 deleted

//Повернемо його назад. Зняття позначки видалення
> RSET
< +OK maildrop has 7 messages

//Закриваємо з'єднання з pop3 сервером
< QUIT
> OK POP3 server at inbox.ua signing off

У відмінності від smtp, в протоколі pop3 не реалізовані коди помилок, замість них передбачені службові +OK (команда успішно виконалася) і – ERR (Опис помилки).

Порядок виконання роботи

1. Ознайомитись з роботою протоколів роботи з електроною поштою.
2. Розглянути команди які використовують протоколи SMTP і POP3.
3. Розглянути можливості поштового сервера Kerio MailServer.
4. Встановити поштовий сервер Kerio MailServer. Встановити первинний домен.
5. Встановити пароль адміністратора – ADMINISTRATOR.
6. Запустити браузер і перевірити роботу встановленого поштового сервера.
7. Провірити роботу команд протоколів електронної пошти.
8. Розглянути служби які використовує Kerio MailServer, параметри їх налаштування.
9. Розглянути можливості створення доменів. Створити власні домени згідно прикладу але використовуючи свої імена доменів.
10. В кожному домені створити не менше 5 користувачів.

11. Створити групи користувачів: Адміністратори, користувачі, студенти, викладачі.
12. Створити шаблони для цих груп.
13. Оформити звіт по роботі

Індивідуальні завдання

№ варіанту	Кількість додаткових доменів	Кількість користувачів в домені	Кількість груп	Квоти користувачів	Кількість шаблонів користувачів
1	2	8, 7	4	Кількість повідомлень 5	2
2	3	6, 8, 4	3	Дискового простору 1 Мб	2
3	2	8, 3	4	Кількість повідомлень 8	1
4	3	5, 6, 2	3	Дискового простору 2 Мб	1
5	2	5, 8	4	Кількість повідомлень 6	1
6	3	2, 4, 2	3	Дискового простору 1,5 Мб	2
7	2	5,9	4	Кількість повідомлень 10	2
8	3	4, 3, 5	3	Дискового простору 3 Мб	2
9	2	2,10	4	Кількість повідомлень 7	1
10	3	3, 8,2	3	Дискового простору 2 Мб	1

Звіт повинен включати:

- тему, мету роботи;
- короткий огляд теоретичних відомостей;
- хід встановлення сервера (приклади вікон);
- вікно браузера з відкритим поштовим сервером;
- вікна в яких використовувались команди роботи з поштовим сервером;
- процедуру створення доменів, встановлення первинних доменів;
- налаштування користувачів, груп, шаблонів;
- висновки.

Контрольні запитання

1. Що таке протокол SMTP?
2. Що таке протокол POP3?
3. Команди протоколу SMTP, приклади.
4. Команди протоколу POP3, приклади.
5. З яких режимів складається POP3 сесія?
6. Протокол IMAP4.
7. Основний (первинний) домен. Типи і методи доступу до доменів.
8. Можливості сучасних поштових серверів.
9. Для чого використовується вікно адміністрування?
10. Які служби використовуються в Kerio MailServer?
11. Що таке домен?
12. Як створюються домени?
13. Як видалити домен?
14. Порядок створення користувача.
15. Для чого використовується імпорт користувачів?
16. Що таке група користувачів?
17. Для чого використовують групи користувачів?
18. Як створити нову групу користувачів?
19. Для чого використовують шаблони користувацьких екаунтів?
20. Як використовуються шаблони?

Лабораторна робота №3.

Тема: ” Дослідження роботи FTP протоколу ”

Мета роботи: Ознайомитись з протоколами передачі файлів, отримати практичні навички по встановленню і налаштуванню FTP сервера.

Теоретичні відомості

Файлова служба мережі на основі протоколу FTP (File Transfer Protocol) являє собою одну з найбільш ранніх служб, яку використовували для доступу до файлів, які знаходяться на відстані. До появи служби WWW це була найпопулярніша служба доступу до даних в Інтернеті й корпоративних IP - мережах. Перші специфікації FTP відносяться до 1971 року (RFC114 (File Transfer Protocol A.K. Bhushan Apr-10-1971), RFC959 (File Transfer Protocol J. Postel, J.K. Reynolds Oct-01-1985)). Сервери й клієнти FTP є практично в кожній ОС сімейства UNIX, WINDOWS, а також у багатьох інших мережних ОС. Клієнти FTP вбудовані сьогодні в програми перегляду (браузери) Інтернету, тому що файлові архіви на основі протоколу FTP як і раніше популярні й для доступу до таких архівів браузером використовується протокол FTP

Головне призначення FTP - це пересилати (копіювати, передавати) файли. FTP можна використовувати самостійно, а також через інші системи. File Transfer Protocol протокол високого рівня а саме, рівня додатків.

FTP служба побудована по добре відомій схемі клієнт-сервер.

Клієнт (браузер,Windows Commander, NetVampir ...) посилає запити серверу і приймає файли. Сервер HTTP (Apeche, IIS ...) обробляє запити клієнта на отримання файлу.

FTP відрізняється від інших додатків тим, що він використовує два TCP з'єднання для передачі файлу. **Канал керування**- для надсилання команд серверу і отримання відповідей від нього. Для каналу керування використовується протокол Telnet. **Канал даних** - з'єднання для передачі файлів.

Рисунок 3.1 - Схема з'єднання по протоколу FTP

Режими роботи FTP

Протокол FTP підтримує два режими роботи: активний і пасивний.

В обох режимах FTP використовує контрольне з’єднання, яке встановлюється клієнтом по 21 порту (за замовчуванням). По контрольному з’єднанню ніякі данні, файли чи заголовки каталогів не передаються. Для передачі будь-якого файлу чи заголовку створюється окреме з’єднання.

Протокол FTP використовує при взаємодії клієнта із сервером кілька команд (не треба їх плутати з командами користувацького інтерфейсу клієнта, які використовує людина).

Ці команди діляться на три групи:

1. команди керування доступом до системи;
2. команди керування потоком даних;
3. команди служби FTP.

Встановлення FTP-сервер Gene6.

Запускаємо програму інсталяції, вибираємо мову натискаємо «ОК» після чого запуститься майстер встановлення програми.

Вибираємо шлях для встановлення (**шлях для встановлення потрібно уточнити у викладача**) і натискаємо «Next»

У вікні вибору компонентів відмічаємо всі позиції.

Натискаємо «Next»

Вибираємо порт для адміністрування (**не ставити порт 21**)

Вводимо пароль для управління сервером, і натискаємо натискаємо «Next» (даний Administrator немає жодного відношення до користувача Administrator у Windows, він використовується тільки для адміністрування FTP- сервера):

Галочку «Launch Tray monitor at windows startup» залишаємо увімкненою, інші по бажанню:

Натискаємо «Install» і чекаємо коли завершиться встановлення

Знімаємо галочку «Launch administration tool» і натискаємо «Finish»

Налаштування FTP-сервер Gene6

Два рази натискаємо лівою кнопкою мишки на значок Tray monitor:

Вводимо пароль, який був заданий при встановленні, встановлюємо галочку «Remember password» і натискаємо «ОК»

Створення домену

Зліва вибираємо «Domains» і два рази клікаємо лівою кнопкою мишки по надпису «Double click here to add a domain»:

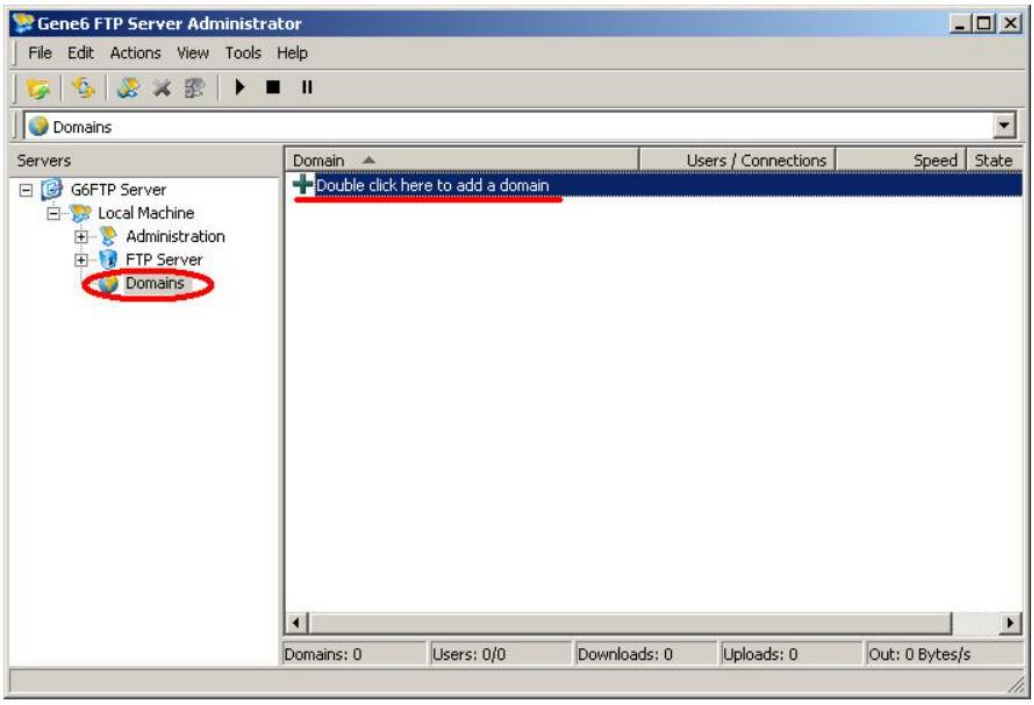


Рисунок 3.2 - Створення домену

Пишемо назву домену і вибираємо бажану кількість одночасно підключених клієнтів і кількість одночасно підключених до одного IP адреса (**дані налаштування видає викладач**), натискаємо «Next». Із списку вибираємо ваш IP адрес в мережі, інші налаштування не міняємо.

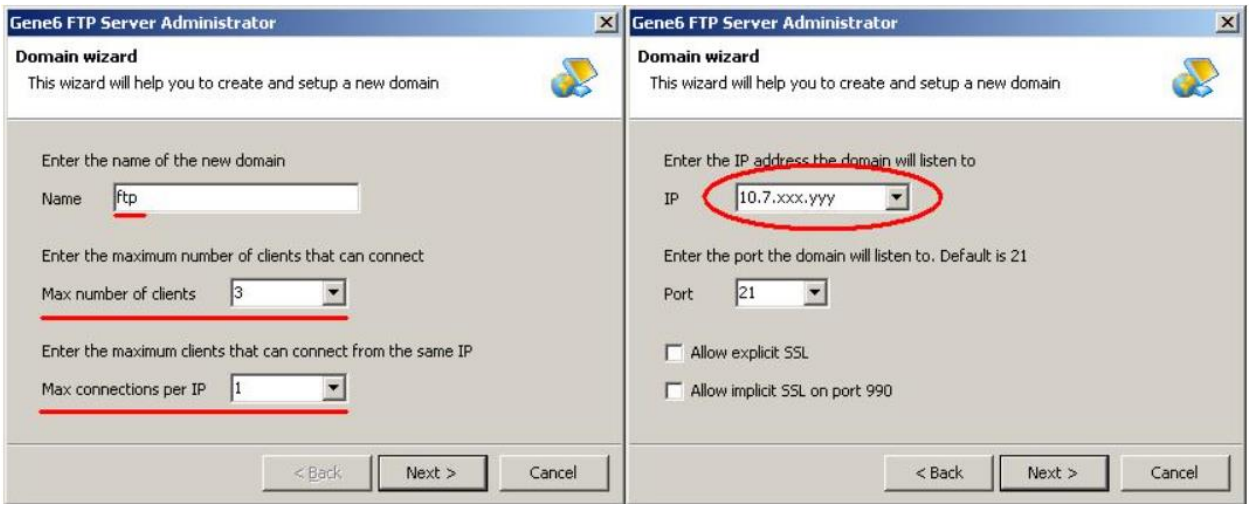


Рисунок 3.3 - Додаткові налаштування домену

Натискаємо «Next». Перевіряємо, щоб була встановлена галочка «Create anonymous FTP account» і в значенні Home пишемо «empty://» (без кавичок).

Після натискання «Finish» відкриється вікно налаштування:

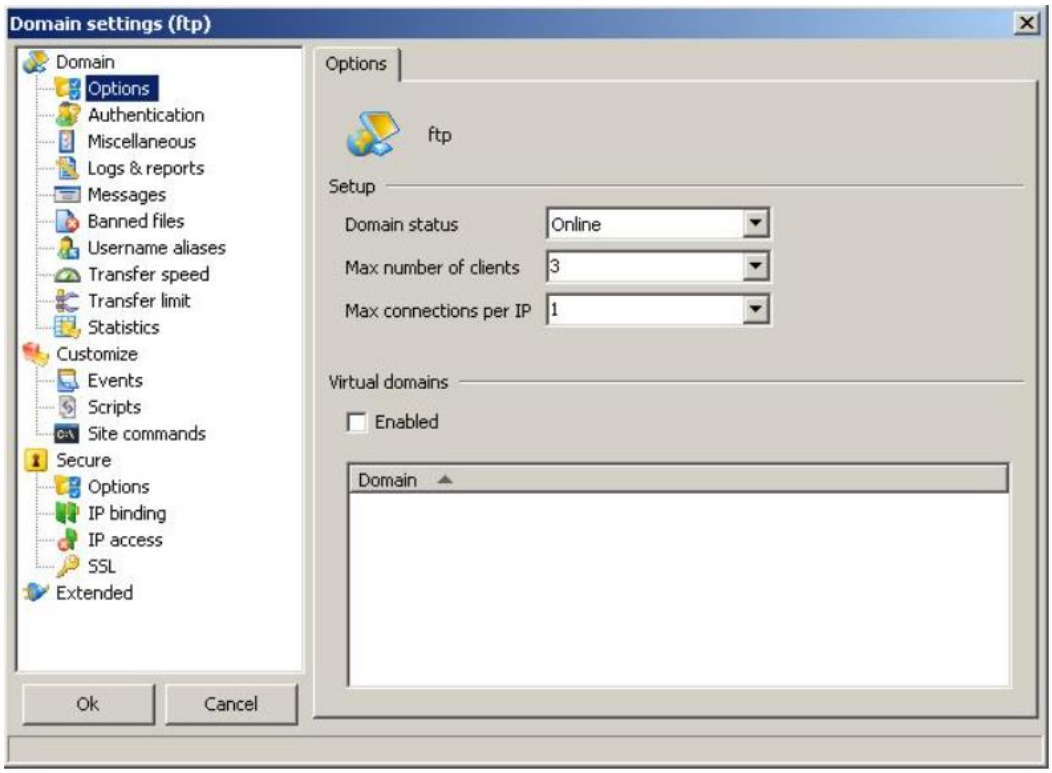


Рисунок 3.4 - Властивості створенного домену

В розділі «Logs & reports» обмежуємо розмір журналів:

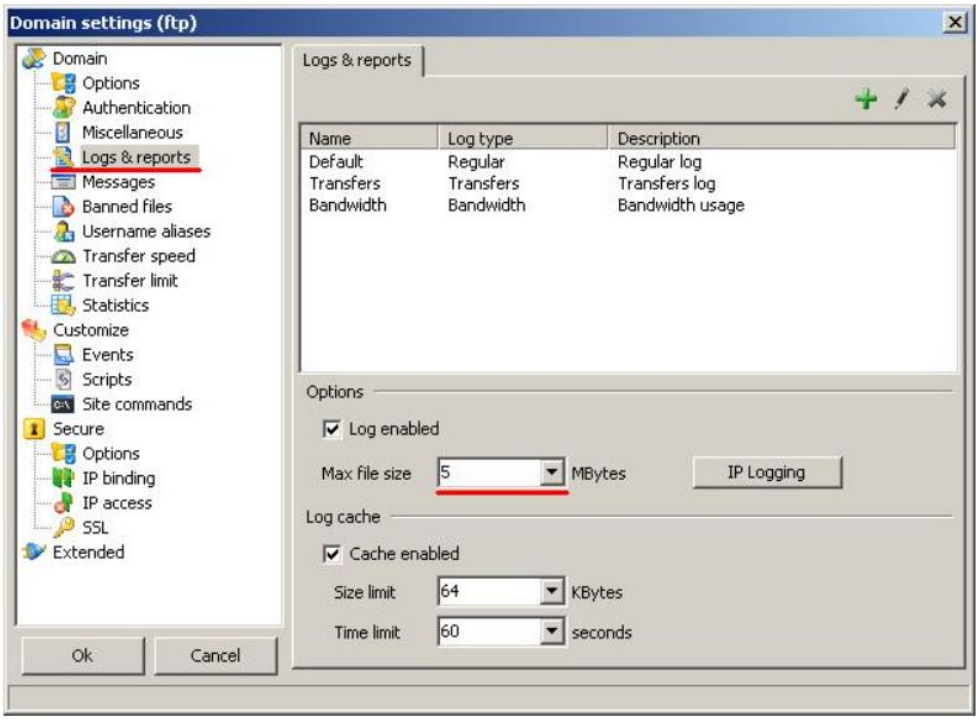


Рисунок 3.5 - Встановлення параметрів журналів

Дальше натискаємо «ОК», щоб вікно закрилось. Якщо його потрібно буде відкрити занову, то натискаємо правою кнопкою мишки на створеному домені і вибираємо «Properties».

Налаштування анонімного користувача.

Для цього переходимо в розділ «Users» і два рази клікаємо по імені Anonymous:

Переходимо в розділ «Access rights» з допомогою кнопки «+» добавляємо папки для загального доступу:

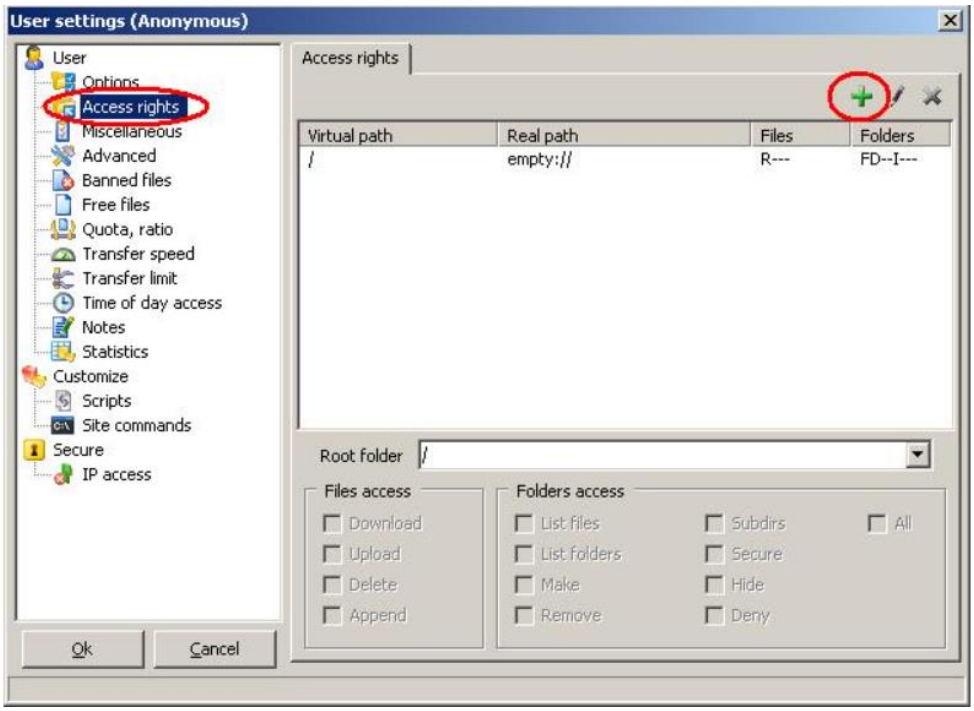


Рисунок 3.6 - Вибір папок загального доступу

Для додання папки пишемо віртуальний шлях (який буде видимий користувачам по FTP) і реальний шлях в себе на диску (зверніть увагу, що на початку віртуального шляху стоїть вліво нахилена коса риска):

Додавати, видаляти і редагувати папки для загального доступу по FTP можна за допомогою кнопок зверху.

Внизу для вибраної папки встановлюються права доступу. По замовчуванню вони встановлюються тільки в читанні для файлів і отримання списку файлів і підпапок для папок. Для користувача Anonymous тут нічого міняти не потрібно:

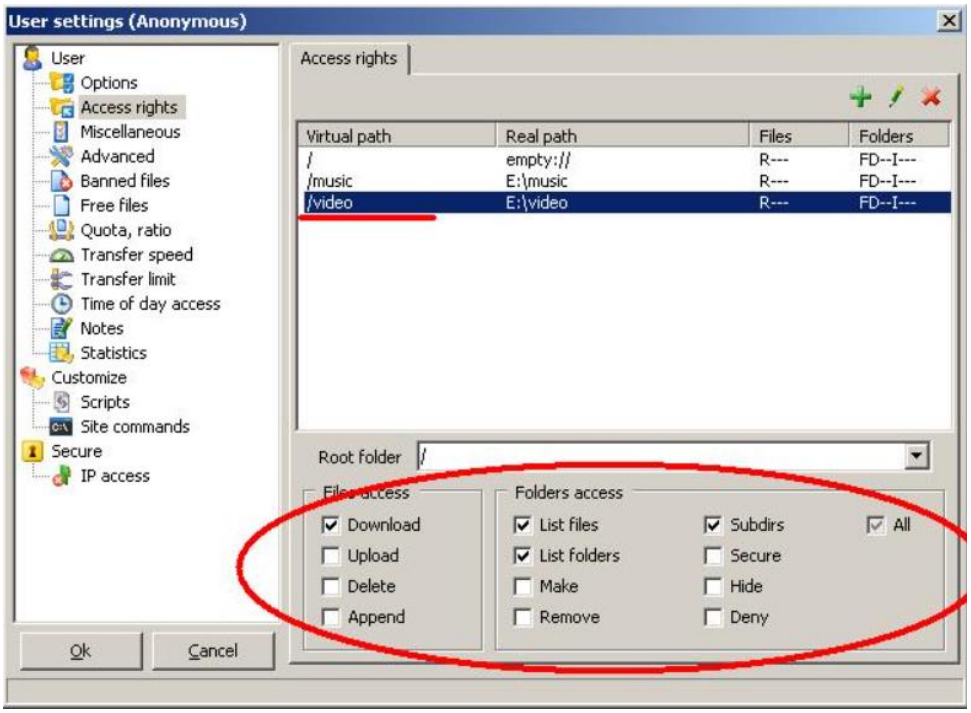


Рисунок 3.7 - Вибір прав доступу

В розділі «IP access» можна заборонити визначеним користувачам заходити на FTP-сервер.

З допомогою кнопки «+» додаємо небажаного користувача. Замість aaa.bbb.ccc.ddd пишемо небажаний IP-адрес, по бажанню можна написати причину, по якій ви не бажаєте, щоб даний користувач до вас заходив і переставляємо вибір на «Denied»:

Налаштування прав користувача

Якщо ви хочете дати будь-кому більше прав, ніж анонімному користувачеві (наприклад можливість записувати файли чи мати доступ до більшої кількості інформації), то вибираємо розділ «Users» і настикаємо конпку на панелі інтрументів (на рисунку вона обведена):

Дальше вказуємо імя користувача і пароль. І задаємо каталог, в який він буде попадати відразу після підключення (empty:// означає пустий каталог, тобто всі доступні цьому користувачу каталоги потрібно додавати в налаштуваннях):

Після натиснення «Finish» відкриється вікно з налаштування для цього користувача, в розділі «Miscellaneous» можна задати більшу кількість одночасних підключень, ніж анонімному користувачеві (галочка біля «By-pass...» означає, що для цього користувача загалі налаштування кількості підключень будуть ігноруватися):

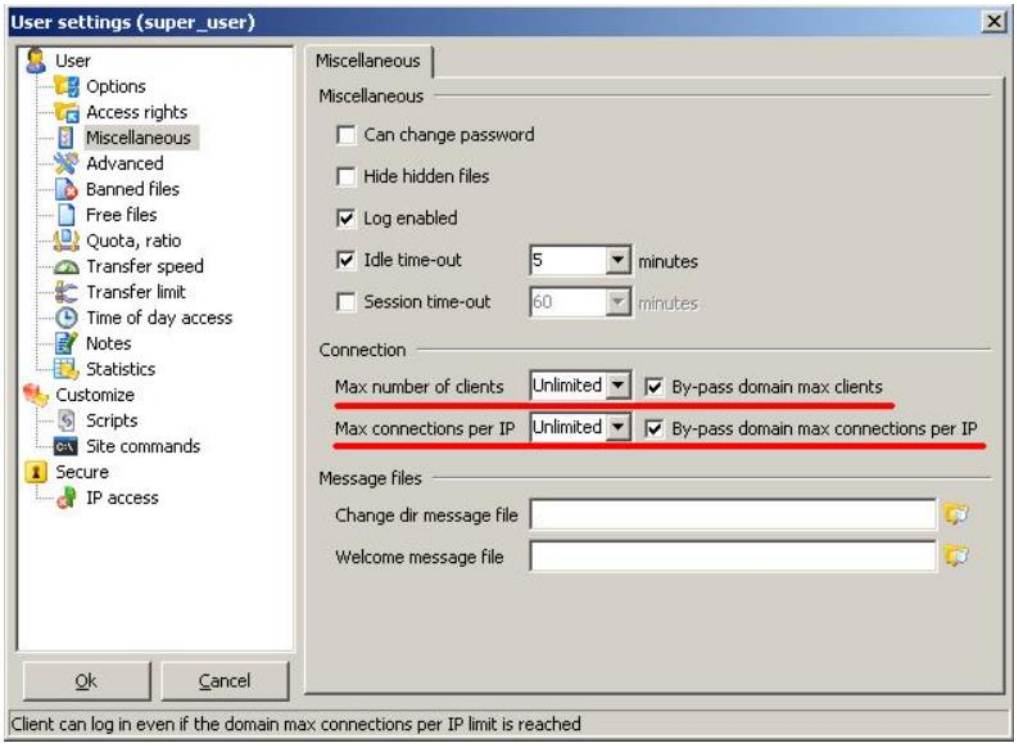


Рисунок 3.8 - Задання кількості одночасних підключень

В розділі «Access rights» можна поставити інший набір відкритих для доступу папок, а також встановити можливість запису в них:

Статистика роботи сервера

В розділі «Info» можна продивитись інформацію про сервер. В підрозділі «Activity» видимі поточні підключення користувачів. В підрозділі «History» відображаєть історія підключень.

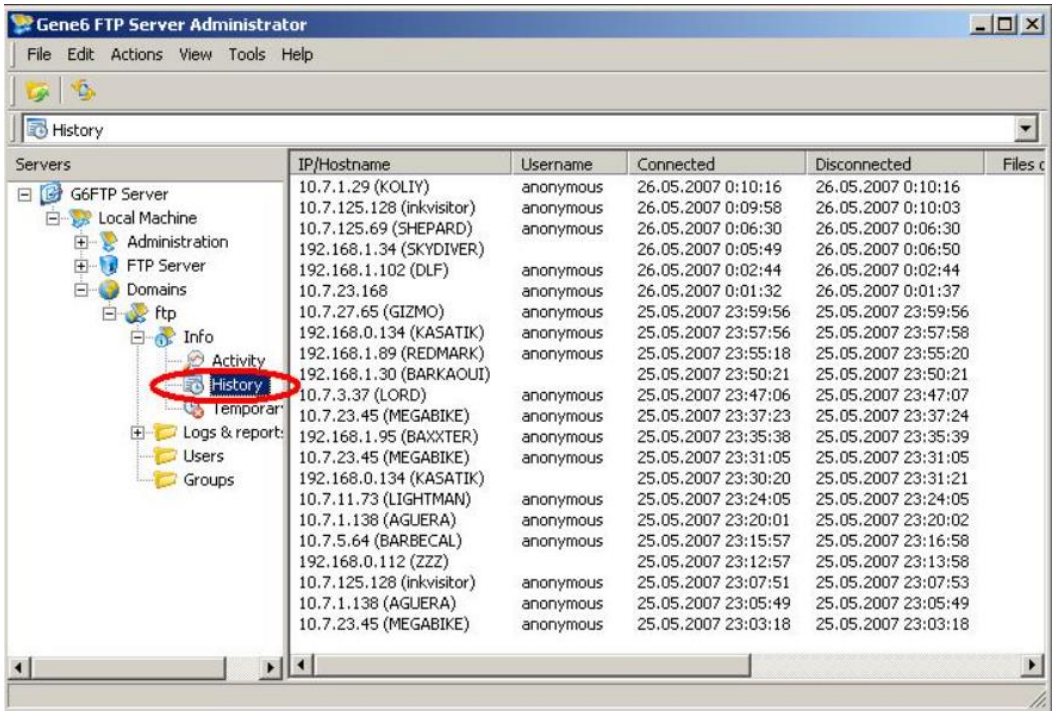


Рисунок 3.9 - Статистика роботи сервера

Тут описаний мінімальний набір налаштувань, який достатній для нормальної роботи FTP-сервера в локальні мережі. Якщо потрібна додаткова інформація то вибираємо «Gene6 FTP Server Administrator» пункт меню «Help -> Manual/Help», відкриється детальний і добре ілюстрований мануал по Gene6 (на англійській мові).

Порядок виконання роботи

1. Ознайомитись з протоколом передачі файлів FTP.
2. Розглянути команди які використовуються при роботі з FTP протоколом.
3. Встановити FTP сервер.
4. Провести налаштування користувачів.
5. Протестувати роботу FTP сервера.
6. Оформити звіт.

Індивідуальні завдання

№ варіанту		Кількість користувачів в групі	Кількість груп		
1		8, 7	4		
2		6, 8, 4	3		
3		8, 3	4		
4		5, 6, 2	3		
5		5, 8	4		
6		2, 4, 2	3		
7		5,9	4		
8		4, 3, 5	3		
9		2,10	4		
10		3, 8,2	3		

Звіт повинен включати:

1. тему, мету роботи;
2. короткий огляд теоретичних відомостей;
3. хід встановлення сервера (приклади вікон);
4. вікно клієнта з відкритим FTP сервером;
5. вікна в яких проводилось налаштування користувачів, прав і т.д.;
6. вікна з тестуванням роботи встановленого сервера;
7. висновки.

Контрольні запитання

1. Що таке FTP протокол?
2. Принцип роботи FTP протоклу.
3. Особливості роботи FTP протоколу.
4. Режими роботи FTP протоколу.
5. Які існують типи команд і для чого вони використовуються?
6. Що таке анонімний користувач?
7. Які інують протоколи передачі файлів крім FTP протоколу?
8. Чи можлива передача файлів з одного FTP сервера на інший?
9. Що таке коди обробки команд, для чого вони використовуються?

Лабораторна робота №4.

Тема: ” Технологія багатоточкової передачі інформації ”

Мета роботи: Ознайомитись з процедурою встановлення та функціями роботи BitTorrent-сервера на основі TBDev Yuna Scatari Edition.

Теоретичні відомості

Серед моделей світових трекерів можна виділити кілька самих популярних шаблонів.

PpkBB3cker

Додає функції торрент-трекера у форум phpBB3. Представлений у вигляді мода інтегрованого в інсталятор форуму phpBB3. Підтримує різні мови інтерфейсу.

PpkBB3cker входить в трійку самих популярних через свою паралельність з phpBB3 форумом, який є відкритим та безкоштовним. За рахунок чого в проекті бере участь значна кількість людей з різними інтересами.

TorrentPier

Остання версія модифікованого TorrentPier SVN 1.0.1.5

Варто відзначити що даний сервер комбінований з повноцінним форумом, що дозволяє розміщувати та обговорювати новини поза межами розділу релізів.

TBDev

Виконаний у вигляді системи управління вмістом. Повністю написаний на PHP, включаючи анонсер. У основі організації лежить принцип новина > торрент або новина > торрент > реліз, тобто торренту зіставлена певне місце на головній сторінці або окрема сторінка з повним описом і коротке повідомлення про реліз на головній сторінці сайту. Торрент-файл завантажується через спеціальну сторінку, де користувачеві надано ввести опис, після чого відбувається реєстрація цього торрента на трекері. Існує багато модифікацій TBDev, найпопулярніші Kinokpk.com releaser (русифікований), CyBERhype Tracker (русифікований), TBDev original (англ.), TBDev YSE (русифікований).

Був написаний для сайту TorrentBits.org, користувачем RedBeard. Надалі, після прилюдного релізу, він став дописуватися співтовариством. Поширюється за ліцензією GNU GPL.

В країнах Східної Європи використовуються різні його інтерпретації. Самою популярною з них на даний час є «TBDev v2.1.8 Yuna Scatari Edition Pre 6 RC». Цей скрипт використовується на таких популярних серверах як http://tracker.0day.kiev.ua/ , і на обох Тернопільських http://tracker.all-in.org.ua/ та http://torrent.te.ua/ .

Встановлення трекера

Установити зв’язку «Apache 2.x.x, PHP 5.x.x, MySQL 5.x.x, PhpMyAdmin» для роботи трекера. Самий легший спосіб – готова збірка Vertrigo (http://vertrigo.sourceforge.net/) або на файлообміннику (http://dl.tntu.edu.ua/mods/_standard/file_storage/index.php?ot=1&oid=589&folder=1080)

З підключенням БД трекера PhpMyAdmin не завжди коректно справляється. Тому ці налаштування легше проводити на EMS SQL Manager for MySQL (http://www.sqlmanager.net/en/products/mysql/manager)або на файлообміннику (http://dl.tntu.edu.ua/mods/_standard/file_storage/index.php?ot=1&oid=589&folder=1080)

Сам шаблон трекера «TBDev Yuna Scatari Edition» можна завантажити з офіційного сайту автора (http://bit-torrent.kiev.ua/downloads.php) або на файлообміннику (http://dl.tntu.edu.ua/mods/_standard/file_storage/index.php?ot=1&oid=589&folder=1080)

Створити в директорії веб-сервера (c:\Program Files\VertrigoServ\www\ ) папку з назвою трекера (для прикладу – tbdevlab) і розпакувати туди файли «TBDev Yuna Scatari Edition».

Запустити SQL Manager , підключити в ньому базу трекера. В меню програми: «База данных – создать базу данных»

В наступному кроці слід додати пароль до БД веб сервера – vertrigo (паролі вказано в файлі c:\Program Files\VertrigoServ\readme.txt), а також конкретизувати кодування

По завершенні бачимо інформаційне вікно характеристики БД, тиснемо кнопку готово. В вікні реєстрації інформацій БД знову міняємо налаштування кодування.

Після цього підключаємося до БД через меню програми: «База данных – подключится к базе данных» і виконуємо SQL скрипт

По завершені операції відключаємося від БД: Для того аби трекер повністю запрацював в браузері (http://127.0.0.1/TBDev/) слід відредагувати деякі файли в директорії веб сервера.

В файлі …\www\TBDev\include\secrets.php вписуємо пароль до БД і назву новоствореної:

$mysql_pass = "vertrigo";

$mysql_db = "tracker";

Для доступу до сторінки створюємо файл …\www\TBDev\.htaccess з коротким вмістом:

php_value register_globals 0

Примітка: якщо при першому запуску в браузері показує помилку пов’язану з «COOKIE_SALT», - виконайте вказані дії для файлу …www\TBDev\include\init.php.

Щоб змінити шапку трекера, варто підмінити файл …\www\TBDev\themes\TBDev\images\logo.gif, або ж вказати в коді на альтернативний.

Якщо трекер закритий чи внутрішньомережевий, то можна спростити форму реєстрації. А саме відключити перевірку логіки captcha …www\TBDev\include\config.php

$use_captcha = 0;

Та зупинити активацію по пошті, оскільки не всі користувачі можуть мати вихід в глобальний інтернет:

$use_email_act = 0;

Перший реєстрований користувач автоматично отримує самий вищий ранг в системі трекера – «Директор». Перевірити змогу керування трекером.

BitTorrent як протокол

«БітТóррент» (BitTorrent) — відкритий протокол обміну інформацією у мережах типу peer-to-peer. Автором проекту є Брам Коен (Bram Cohen), який створив першу версію у квітні 2001 разом із першим клієнтом з тією ж назвою.

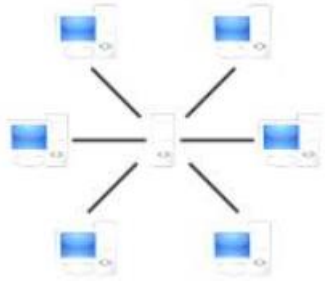


Рисунок 2.1 – Звичайна серверна мережа (не peer-to-peer)

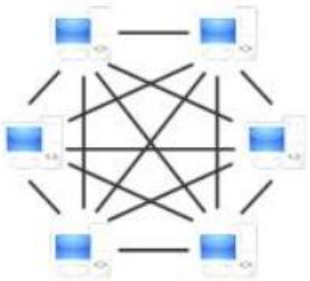


Рисунок 2.2 – BitTorrent мережа типу peer-to-peer

Протокол розроблявся таким чином, щоб обмін файлами великих розмірів у мережі був полегшений для її учасників. Один з принципів роботи протоколу BitTorrent наступний: навантаження на учасника що розповсюджує деякий файл зменшується, завдяки тому що клієнти, які його скачують починають обмінюватися даними між собою одразу, навіть поки файл повністю не скачано. Таким чином, клієнти які скачали певну частину великого файлу одразу можуть бути джерелами його розповсюдження.

Така ідея організації протоколу має переваги порівняно до протоколів peer-to-peer мереж першого покоління, де файл скачується з одного розповсюджувача чи з декількох розповсюджувачів по частинах.

Для отримання інформації про розповсюджувачів деякого файлу, клієнт може звернутися до так званих трекерів.

Трекер

Трекер (англ. tracker) — спеціалізований сервер, якій працює по HTTP протоколу. Трекер використовується для того, щоб клієнти могли знайти один одного. На трекері зберігаються IP-адреси клієнтів, вхідні порти клієнтів та хеш-суми, які унікальним чином ідентифікують об'єкти, що беруть участь у скачуваннях. За стандартом, імена файлів на трекері не зберігаються, та взнати їх по хеш-сумам не можна. Проте на практиці часто трекер окрім своєї основної функції виконує також функцію невеличкого веб-серверу. Такий сервер зберігає файли метаданих що містять значення хеш-функції, та разом з ними опис файлів що розповсюджується, кількість розповсюджувачів статистику завантажень та ін.

Перед початком завантаження файлу, клієнт з'єднується з трекером, повідомляє йому свою IP-адресу та хеш-суму файла що завантажується. У відповідь клієнт отримує адреси інших учасників мережі, які розповсюджують або скачують той самий файл. Далі клієнт періодично інформує трекер про хід процесу завантаження та отримує оновлений перелік адрес.

Клієнти з'єднуються один з одним, та обмін даними відбувається без безпосередньої участі трекера. Учасники завантаження обмінюються інформацією про наявність сегментів файлу. Клієнт, що бажає завантажити певний фрагмент, надсилає запит, і якщо інший клієнт готовий його надати відбувається процес завантаження. Після цього клієнт перевіряє контрольну суму сегменту та сповіщає всіх приєднаних учасників завантаження про його наявність.

Для ефективної роботи мережі BitTorrent необхідно, щоб якомога більше клієнтів були здатні приймати вхідні з'єднання. Неправильна настройка NAT чи файрволу можуть цьому заважати.

Для кожного файлу, що розповсюджується, створюється файл метаданих з розширенням .torrent, який містить наступну інформацію: URL трекеру, загальну інформацію про файл (ім'я, розмір та ін.), контрольні суми сегментів файлу.

Файли метаданих можуть розповсюджуватися через будь-які канали зв'язку: вони, чи посилання на них, можуть розміщатися на веб-серверах, пересилатися по електронній пошті, публікуватися у блогах та ін. Клієнт може розпочинати завантаження, отримавши будь-яким чином файл з метаданими, у якому є посилання на трекер.

У нових версіях протоколу розроблено безтрекерні (англ. trackerless) механізми обміну інформацією. Таким чином працездатність всієї мережі не залежатиме від роботи трекера.

DHT

Розподілена хеш-таблиця (англ. Distributed hash table, DHT) — протокол передачі даних та механізм збереження інформації про ресурси та учасників файлообмінної мережі типу peer-to-peer децентралізовано (без виділеного сервера), безпосередньо на клієнтах мережі.

Однією з реалізацій DHT є протокол Kademlia.

Опишемо типову організацію децентралізованої мережі, яка використовує розподілену хеш-таблицю. Кожен учасник мережі при першому підключенні до мережі отримує унікальний номер (ID), що вибирається із певної множини, в деяких реалізаціях це 160-бітове число, яке генерується випадковим чином. Для порівняння двох ID вводиться поняття метрики або відстані. У випадку Kademlia воно обчислюється як виключне "або" двох чисел (XOR). Чим менше значення такої відстані — тим два учасники мережі вважаються ближчими один до одного. Метрика введена таким чином не відображає географічної близькості учасників мережі.

Коли учасник хоче розмістити у мережі деякий ресурс (файл), він обробяє його зміст та обчислює значення хеш-функції яка буде, ідентифікувати ресурс у мережі. Хешувальна функція обирається таким чином, щоб унікальні номери учасників та хеш-функція набували значень з однієї множини. Обрахувавши значення хеш-функції, учасник намагається відшукати іншого учасника мережі, ID якого близький до знайденого хешу. Знайшовши, розміщувач ресурсу передає знайденому учаснику свою IP-адресу та хеш, які той зберігає у себе.

Таким чином, клієнт мережі, який потім хоче завантажити ресурс, знаючи з деяких джерел його хеш, намагається взнати відомості про знаходження ресурсу в тих учасників мережі, унікальний номер яких близький до хешу.

Пошук ресурсів за назвами файлів може бути організовано у такий спосіб. Ім'я файлу розбивається на ключові слова, які при розміщенні ресурсу хешуються та зберігаються у мережі разом із назвою файлу та його хешем. Номер учасника на якому ці відомості зберігаються знаходиться аналогічним чином — він має бути якомога ближче до значення хешу відповідного ключового слова. Пошук за іменем файлу відбувається наступним чином — за ключовими словами обчислюється їх хеш, та в учасників мережі, які мають ID близькі до цього хешу відшуковується повна назва файлу разом зі значенням хеш-функції.

На даний момент не всі BitTorrent-клієнти використовують сумісні протоколи. Між собою сумісні BitComet, µTorrent, KTorrent та офіційний клієнт BitTorrent. Azureus також має режим безтрекерної роботи, але його реалізація відрізняється від офіційної, через що він не може працювати через DHT з наведеними вище клієнтами.

µTorrent

µTorrent (також відомий як uTorrent або microTorrent) — безкоштовний BitTorrent-клієнт для Microsoft Windows, написаний на мові C++, що відрізняється невеликим розміром та достатньою функціональністю.

Виконавчий файл µTorrent займає на диску біля 0,3 МБ, програма використовує мінімум оперативної пам'яті і ресурсів процесора, і може працювати навіть на застарілих комп'ютерах з процесором рівня Intel486.

Деякі можливості програми:

-обмеження максимальних швидкостей завантаження і віддачі

-налаштування цих обмежень залежно від часу

-обмеження максимальних швидкостей кожного завдання

-налаштування кешування файлів на жорсткому диску

-підтримка DHT і Peer Exchange

-режим початкової роздачі (суперсид)

-автоматичне закачування торрентов із стрічки новин RSS

-підтримка проксі-серверів

-можливість підключення до трекера по HTTPS

-шифрування протоколу, сумісне з Azureus, BitTorrent і BitComet

-підтримка Юнікода у всіх версіях Windows

-підтримка UPnP в всіх версіях Windows

-повна підтримка операційної системи Windows Vista

-налаштування інтерфейсу програми

-локалізація на 38 мов, включаючи українську

-веб-інтерфейс (віддалене управління програмою з браузеру) — доступний в бета-версії

-можливість запуску на GNU/Linux і Macintosh з допомогою Wine

Порядок виконання роботи

1. Установити клієнт uTorrent (http://www.utorrent.com/downloads)
2. Змінити початкові налаштування клієнта (Опції – Налаштування); рекомендується змінити:

- Загальне: ввімкнути «.!ut» для незавершених файлів.
- Пропускна здатність: зменшити дані показники при помічені навантаження на лінію Інтернет каналу.
- Додатково – Дисковий кеш: вказати статичний розмір кешу (~64-512) та вимкнути методи кешування ОС Windows при відчутному навантаженні на ЖМД ПК.

1. Ввімкнути та перевірити роботу веб-інтерфейсу клієнта (Опції – Налаштування – Веб-Інтерфейс). Для прикладу, при вказаному альтернативному порті 8383 звернутись до інтерфейсу в браузері можна за адресою: http://127.0.0.1:8383/gui/
2. Додати в завантаження файли з будь-якого трекера.
3. Установити торрент сервер.
4. Здійснити підключення клієнта до сервера
5. Провести тестування роботи трекера
6. Оформити звіт.

Звіт повинен включати:

1. тему, мету роботи;

2. короткий огляд теоретичних відомостей;
3. хід встановлення;
4. приклад створення торенту;
5. приклад роботи (завантаження, відвантаження, статистика);
6. висновки.

Контрольні запитання

1. Перерахуйте основні види шаблонів трекер-сайтів ?
2. Які з популярних сайтів використовують дані шаблони?
3. Які програмні вимоги для встановлення веб-трекера?
4. Який файл в директорії веб-сервера відповідає за доступ до сторінки?.
5. Які основні переваги роботи протоколу BitTorrent?
6. Чи можливо бути одночасно учасником і завантаження і роздачі недокачаного файлу в мережі BitTorrent?
7. Наведіть основні функції роботи Трекер-сервера.
8. Чи іде через сервер весь трафік при завантаженні файлів клієнтом?
9. Чи можливий обмін інформацією без участі трекера?
10. Яке основне призначення протоколу DHT?
11. Наведіть приклади популярних BitTorrent-клієнтів.

Лабораторна робота №5.

Тема: ” Дослідження роботи систем передачі мультимедійної інформації в комп’ютерних мережах ”

Мета роботи: Отримати практичні навички по організації відеоконференцзв’язку.

Теоретичні відомості

1.1 Установка програмного забезпечення

Знаходимо і запускаємо файл інсталяції для встановлення програмного забезпечення.

На даному етапі пропонується вказати робочу директорію сервера (наприклад, C: \ Program Files \ VideoPort VCS \), і натиснути кнопку «Продовжити» («Next»).

Після завершення інсталяції запуститься програма конфігурації сервера «Налаштування VideoPort VCS».

Для успішної роботи сервера необхідно його зареєструвати (активувати) в єдиній реєстраційній системі VideoPort.

Для реєстрації сервера виконайте наступні дії:

1. Запустіть Настройку VideoPort VCS.

2. Для успішної реєстрації в цей момент повинен бути відкритий вихід в Інтернет по порту 4310.

3. Якщо реєстрація сервера виробляється вперше, то відкриється діалогове вікно реєстрації.

Введіть реєстраційний код і ім'я сервера. Ім'я сервера повинно бути унікальним.

4. За наявності підключення до інтернету та успішної реєстрації з'явиться вікно:

Після цього програма налаштування VideoPort VCS автоматично перезапуститься. Сервер зареєстрований і готовий до роботи.

Offline реєстрація

1. За відсутності підключення до інтернету з'явиться вікно:

2. Після натискання кнопки «ОК» буде запропоновано зробити реєстрацію без підключення до інтернету:

3. Клацніть по посиланню «off-line registration». Для створення і збереження файлу реєстрації натисніть кнопку «Створити файл»

4. Створений файл необхідно відправити за адресою: vp_sales@video-port.com, або будь-яким іншим зручним для Вас способом.

5. Після отримання файлу з ліцензією, повторно запустіть програму установки VideoPort VCS і натисніть посилання «натисніть тут і виберіть отриманий файл». У вікні, що з'явилося виберіть отриманий файл з ліцензією.

6. Якщо ліцензія не пошкоджена, програма налаштування VideoPort VCS автоматично перезапуститься. Сервер зареєстрований і готовий до роботи.

1.2 Конфігурування сервера

Закладка «Служби». Елементи цієї закладки дозволяють запускати і відключати сервер, переглядати статистику і службову інформацію від сервера.

Закладка «Мережа». Закладка налаштувань параметрів мережі.

Використовувані з'єднання відображаються в полі "Поточне підключення». Для зміни налаштувань мережі необхідно натиснути кнопку «Змінити».

Вікно Установка UDP мультикаст

Дозволяє задати multicast / broadcast IP-адреса, що використовується у конференціях типу UDP Multicast. Для цієї адреси можна вказати діапазон портів, у форматі <ip_address>: <first_port> - <last_port>. Наприклад: 224.0.1.224:4000-6000. Порти за замовчуванням: 4000-6000. Якщо необхідно, цей же IP-адресу слід прописати в IGMP параметрах комутаторів і маршрутизаторів вашої корпоративної мережі.

Закладка «SMTP Mailer». Поштовий сервер використовується для відправки користувачам листів про пропущені дзвінки й надсилання системного адміністратора службової інформації про роботу сервера.

Вікно Налаштування шаблонів. У разі пропуску дзвінка зареєстрованим або не зареєстрованим у системі абонентом дана подія фіксується на сервері і на e-mail відповідного абонента направляється спеціальне повідомлення.

Закладка «Облікові записи користувачів». Директорія користувачів, зареєстрованих на сервері відеоконференцій.

Форма для зміни (вводу) даних про користувача

Закладка «Групи». Закладка Групи дозволяє створювати групи користувачів і визначати їх права на сервері. У режимі Registry користувач може належати одній з створених груп; його приналежність можна змінювати в вікні редагування користувача. У режимі LDAP ця закладка надає можливість вказати права на сервері для кількох вибраних груп LDAP. Належність користувача до груп визначається в LDAP директорії.

Зміни в правах групи вступають у силу відразу після натискання кнопки «Apply».

Закладка «Application». Установки даної закладки передаються клієнтського додатку і дозволяють контролювати процес автоматичного оновлення клієнтів.

Закладка «Сховище користувачів». Переключення між режимами зберігання даних про користувачів

1.3 режими зберігання даних

VideoPort VCS підтримує два режими зберігання даних - Registry і LDAP. Переключення між ними можливо в будь-який момент шляхом натискання кнопки «Переключити» в закладці «Сховище користувачів».

Режим Registry

У цьому режимі зберігання даних сервер зберігає інформацію про користувачів на локальному комп'ютері. Додавання нових користувачів і видалення можливо з конфігуратора. Якщо сервер з режиму зберігання Registry Mode був переключений в LDAP режим зберігання даних, то існуючі записи про користувачів більше не будуть використовуватися.

Закладка «Сховище користувачів» в режимі Registry

Режим LDAP

У цьому режимі зберігання сервер використовує інформацію про користувачів з видаленою або локальної LDAP директорії. За замовчуванням конфігураційні установки для LDAP відповідають Microsoft Active Directory. Існуючою інформацією про користувачів можливо керувати за допомогою стандартного інструментарію управління LDAP Directory. Для Active Directory права користувачів можуть бути визначені приналежністю користувача до тієї або іншої групи Active Directory.

Закладка Сховище користувачів у режимі LDAP

Закладка «LDAP» Закладка доступна в програмі налаштування VideoPort VCS в режимі LDAP. Доступність режиму LDAP регулюється ліцензією.

При перемиканні з режиму LDAP Mode в режим Registry можливо імпортувати записи про користувачів. Для цього у вікні повідомлення, що з'явилося після натискання кнопки Switch, слід відзначити галочкою пункт Import User information.

Після успішного імпортування облікових записів користувачів з'явиться повідомлення:

Закладка «Групові конференції»

Дана закладка дозволяє адміністратору створювати і конфігурувати групові конференції різних типів.

VideoPort VCS підтримує групові конференції чотирьох типів:

UDP Multicast

UDP Multicast дозволяє використовувати мережеві ресурси більш ефективно. У цьому режимі відео і аудіо потоки передаються тільки всередині UDP Multicast домену. Ці домени можуть бути використані в локальній мережі або VPN. По-замовчуванню UDP Multicast відключений для мережі інтернет.

Наявність даного режиму регулюється ліцензією.

Симетрична групова конференція (Symmetric)

• може брати участь до 6 осіб

• всі учасники чують і бачать один одного

Асиметрична групова конференція (Asymmetric

• може брати участь до 12 осіб

• один користувач - Ведучий - чує і бачить всіх учасників

• інші учасники чують і бачать тільки Ведучого

Наявність даного типу конференцій регулюється ліцензією.

Конференція Role based (Селекторна нарада)

• До 90 учасників у нормальному режимі і до 250 в режимі UDP Multicast;

• віщати (передавати свою відео і аудіо інформацію) всім учасникам конференції можуть не більше 3 учасників, які називаються «віщають»;

• Решта учасників можуть чути і бачити ведуть мовлення. Вони можуть передавати аудіо повідомлення (репліки) всім учасникам конференції і можуть ставати віщали, якщо ведучий дозволить їм.

Наявність даного типу конференцій регулюється ліцензією.

Запрошення користувача в конференцію (Invite)

Відкривається вікно в лівому частині якого знаходиться список всіх користувачів, а в правому список користувачів яким буде вислане запрошення до конференції. Переміщення користувачів відбувається за допомогою кнопок «->» і «<-». Кнопка «Відправити» відправляє запрошення вибраним користувачам

Закладка «Підключення». На даній закладці можна подивитися інформацію про користувача робочих місцях.

2 Тестування

2.1 Передача текстових повідомлень

Текстовий чат являє собою послугу обміну текстовими повідомленнями, на зразок ICQ і MSN Messenger. Чат може стати в нагоді тим, кому потрібне спілкування з колегами та друзями, які перебувають як в сусідньому офісі, так і в інших країнах.

При проведенні відео-конференцій в групі одному з абонентів може знадобитися задати персональне питання іншому абоненту, без залучення уваги інших учасників конференції. Для цього можна скористатися відправкою персонального повідомлення за

допомогою чату. Також при проведенні нарад абонент, що бажає виступити на відео-трибуні, може відправити персональне повідомлення ведучому або модератору і обговорити тему виступу і черговість. Відповідно при виникненні необхідності припинити участь у відео-конференції абонент зможе попередити про це тільки ведучого і відключитися від відео-конференції, не перериваючи її.

Для чату необхідно клієнт VideoPort SBS, VideoPort SBS Plus, VideoPort Enterprise, або VideoPort Online, і підключення всіх учасників спілкування до мережі VideoPort. Ви можете відправляти текстові повідомлення відключеному в даний час користувачеві, і він отримає повідомлення, коли з'явиться в мережі. Для відправки текстового повідомлення поза відео-конференції адресат повинен бути записаний в адресній книзі.

Запуск чату проводиться двома способами: з адресної книги (за допомогою правої кнопки миші) або під час відео-конференції за допомогою іконки на загальному інтерфейсі:

Для початку розмови по чату досить запустити вікно чату з необхідним співрозмовником і написати йому текстове повідомлення.

Співрозмовник буде повідомлений про це повідомленням.

При бажанні може відкрити вікно чату для спілкування.

Власне вікно чату:

При відправленні текстових повідомлень у групових відео-конференціях є можливість відправляти єдине повідомлення всім учасникам або персональне повідомлення необхідному абоненту.

Для різних типів повідомлень відкриваються окремі вкладки у вікні чату. Кожен новий співрозмовник текстового чату з'являється в окремій вкладці. Групові повідомлення видно також в окремій вкладці.

2.2 Передача файлів

Передача файлів - це додаткова опція сервера відео-конференцій, що дозволяє передавати файли співрозмовнику прямо, без використання додаткових файлообмінних програм. Використання файлообмінних програм часто несе додаткові витрати за швидкість передачі інформації або мають обмеження у часі передачі файлу. А технічні засоби (зовнішні жорсткі диски, оптичні диски, flash-накопичувачі) вимагають фізичного переміщення користувача, що не завжди можливо і зручно, особливо на великих відстанях.

Передача файлів може знадобитися користувачам, що бажають передати файл іншим користувачам або отримати файл від іншого користувача. Це можуть бути фотографії, музичні та відео файли, креслення, презентації та електронні документи.

Для передачі файлів у програмі VideoPort необхідно відкрити головне вікно клієнта VideoPort і встановити з'єднання з приймаючою стороною.

Далі потрібно клацнути мишкою на піктограмі з папкою, після чого відкриється вікно для передачі файлів.

Для передачі файлу необхідно перетягнути потрібний файл з провідника у вікно програми, або натиснути кнопку "Додати файл" і вибрати потрібний файл. Після цього файл відобразиться у списку у вікні передачі файлів.

Для кожного файлу в списку відображається стан передачі: чи почав користувач приймати файл, чи закінчена відправка і т.д.

2.3 Слайдшоу

Слайдшоу - це функція системи відео-конференцій VideoPort, яка дозволяє демонструвати під час проведення відео-конференції слайди: малюнки, фотографії, діаграми тощо. Дана функція дозволяє не відволікатися на пересилання учасникам відео-конференції файлів з зображеннями, а також не витрачати час на вказівку і пошук потрібного зображення кожним учасником.

Режим слайдшоу стане в нагоді тим користувачам, яким необхідно показати графічну інформацію іншим користувачам під час проведення конференції.

Для проведення слайдшоу необхідно встановити клієнт VideoPort, а також графічні файли, які необхідно продемонструвати.

Під час проведення персональної відеоконференції один з учасників запускає функцію слайдшоу для показу графічних об'єктів зі свого комп'ютера і дає їм словесне пояснення.

2.4 Електронна дошка

Електронна дошка - це функція програми, що дозволяє учасникам відеоконференцій по мережі за допомогою різних графічних інструментів малювати, креслити, вводити і редагувати текстові або графічні дані в окремому вікні. Завдяки цій функції учасники конференції можуть керувати спільною розробкою схем, діаграм і т.д., так, ніби то учасники перебувають поруч.

Можливість обговорення різних видів документів, використовуючи візуальні позначки. Також при організації робочої групи важливо розуміти, що не кожна зустріч може бути проведена з особистою участю запрошених експертів. При проведенні зборів з наданням звітів кожен учасник конференції буде мати можливість представити результат своєї роботи у вигляді таблиць, графіків, презентацій. При цьому інший учасник може звернути увагу слухачів на певний показник, помітивши його маркером.

Також система дає можливість спільно розробляти схеми взаємодії структурних підрозділів та інші документи. Кожен учасник конференції може щось міняти, доповнювати, помічати в єдиному документі.

Складнощі, пов'язані з організацією зустрічей для обговорення дизайну, великих структурних схем та інших візуальних матеріалів, можуть бути подолані за допомогою модуля електронної дошки на сервері відеоконференцій відеопорт. Користувачі економлять час на організацію зустрічі та не обмежують себе в можливих способах обговорення, матеріалів будь-якого масштабу і складності.

Що необхідно для використання електронної дошки

Встановіть клієнт VideoPort SBS, VideoPort SBS Plus, VideoPort Enterprise, або VideoPort Online. Під час персональної відеоконференції відкрийте електронну дошку.

Іншому користувачеві буде висланий запит-підтвердження про початок спільного сеансу електронної дошки:

Після підтвердження іншим користувачем, почнеться сеанс електронної дошки. У ньому можна з допомогою тексту, числових даних і інших інструментів у реальному часі спільно виробляти рішення, креслити схеми, або просто пояснювати учасникам обговорення свої думки.

На додаток до фігур можуть знадобитися текстові пояснення, наприклад для того, щоб вказати назви об'єктів або зв'язку між ними. Для залучення уваги до тих чи інших елементів, ці елементи можна виділення кольором.

При запуску слайд-шоу потрібно вибрати файли, які будуть демонструватися, а також визначитися з їх порядком. Також у процесі показу можна змінювати порядок показу слайдів. Для того щоб інші користувачі програми відеоконференцій мали можливість бачити слайдшоу, вони повинні бути в одній відеоконференції з користувачем, керуючим слайдшоу.

2.5 Показ віддаленого робочого столу

Показ віддаленого робочого столу (Screen Sharing) - це опція сервера відеоконференцій, що дозволяє передавати зображення робочого столу співрозмовникам.

Використання інших програм вимагає організації серверів, або не володіє необхідним для проведення показу функціоналом і змушує вигадувати особливі способи трансляції. Такі способи часто не дають можливості досягти очікуваного результату, а також якості переданої інформації. Саме для таких ситуацій розроблено функціонал "Показу віддаленого робочого столу".

"Показ віддаленого робочого столу" може стати в нагоді будь-яким користувачам, охочим отримати наочну інформацію від інших користувачів. Дуже добре використовувати "Показ віддаленого робочого столу" як інструмент онлайн-співробітництва в режимі реального часу.

Наприклад, при проведенні відеоконференції між головним офісом компанії та її філіями, які знаходяться в інших містах, необхідно провести презентацію за результатами роботи за певний період. Припустимо, що презентація була підготовлена у вигляді стандартного документа Office Power Point. Зрозуміло, її можна було заздалегідь розіслати всім учасникам конференції, а можна легко запустити програму "Показ віддаленого робочого столу" і в режимі реального часу здійснити показ готового документа прямо зі свого робочого столу, супроводжуючи його необхідними коментарями.

Також можлива і більш складна ситуація, коли з'являється необхідність проведення тренінгу з використання нового програмного забезпечення. Дуже важливим є наочне уявлення процесу роботи в деталях, що вимагає організувати тренінг з відривом фахівців від робочих місць. На багато менше витрат буде при використанні віддаленого процесу навчання з безпосереднім показом робочого столу викладача. "Показ віддаленого робочого столу" в цій ситуації є ідеальним рішенням так як викладач має можливість показати весь процес роботи, не відходячи від свого робочого місця, а ті, яких навчають, так само можуть не залишати свої робочі місця, проходячи курс навчання і задаючи необхідні питання. Також викладач може проконтролювати процес засвоєння матеріалу учнями, не виїжджаючи до них.

Для показу віддаленого робочого столу необхідно встановлений клієнт VideoPort SBS Plus, VideoPort Enterprise, або VideoPort Online.

Під час проведення відеоконференції один з учасників повинен запустити функцію "Показ віддаленого робочого столу". Однак, отримуючи запрошення, учасник може відмовитися від участі в сеансі "Показу віддаленого робочого столу".

Учасник, котрий організовує від себе процес "Показ віддаленого робочого столу", повинен підтвердити готовність почати сеанс:

Після цього відео вікно згорнеться в трей, щоб не заважати під час процесу передачі робочого екрану, а в лівому нижньому кутку екрану з'явиться кнопка завершення

сеансу, натиснувши на яку можна припинити передавати зображення свого робочого столу.

Примітка: при наявності декількох робочих столів програма попросить вибрати те, зображення яке буде передаватися.

Учасник, який приймає у себе сеанс "Показ віддаленого робочого столу", повинен підтвердити своє бажання брати участь у сеансі:

Примітка: якщо новий учасник приєднується до групової конференції, в якій відбувається сеанс "Показ віддаленого робочого столу", то в момент встановлення з'єднання з конференцією він отримає запрошення до участі в сеансі "Показу віддаленого робочого столу".

Після цього у нього відкриється вікно, в якому він зможе побачити робочий стіл передавального учасника.

Якщо учасник бажає припинити перегляд, він може закрити вікно перегляду.

Примітка: якщо сеанс "Показ віддаленого робочого столу" здійснюється під час індивідуальної конференції, то в цьому випадку він так само буде припинений і на передавальній стороні. Якщо сеанс "Показ віддаленого робочого столу" здійснюється в груповий конференції, то він буде припинений тільки у того учасника, що припинив перегляд. Повернутися до перегляду в такому випадку можна, натиснувши на кнопку сеансу "Показ віддаленого робочого столу".

Порядок виконання роботи

1. Ознайомитись протоколами організацій відеоконференцій.
2. Розглянути архітектуру стандарту Н.323.
3. Провести налаштування програмного забезпечення для організації відеоконференцій.
4. Здійснити організацію відооконференцій різного типу.
5. Оформити звіт по роботі.

Контрольні запитання

1. Відеоконференції основні поняття.
2. Типи відекрнференцій
3. Протоколи для організації відеконференцій
4. Стек протоколів Н.323.
5. Архітектура стандарту Н.323.
6. Термінал відеоконференції
7. Мультимедіа шлюз відеоконференції
8. Контроллер зони відеоконференції
9. Пристрій для організації багатоточкового зв’язку.
10. Гібридна схема організації конференцзв'язку.
11. Децентралізована багатоточкова конференція.

Лабораторна робота №6.

Тема: ”Дослідження середовищ передачі даних в комп’ютерних мережах”

Мета роботи: Ознайомитись з характеристиками кабелів КМ; вивчити основні алгоритми кодування/декодування; розглянути будову, складові частини та параметри адаптера; навчитися користуватися довідковими джерелами Інтернет.

Теоретичні відомості

1.1. Середовища передавання

1.1.1. Параметри

Техніко-експлуатаційні характеристики:

- ✓ час і щвидкість розповсюдження сигналів
- ✓ вартість
- ✓ швидкість загасання сигналу певної частоти на одиницю довжини кабелю (визначає довжину кабелю у КМ)
- ✓ опір та маса одного метра
- ✓ завадостійкість у різних навколишніх середовищах
- ✓ випромінювання у довкілля

Перехідне загасання на ближньму кінці (*Near End Crosstalk - NEXT)*

Електричний струм створює електромагнітне поле, яке спричиняє завади в сусідніх дротах, причому чим більше частота - більше завади, а їх ступінь характеризує NEXT (якщо він високий, рівень корисного сигналу вищий, ніж рівень завад).

Випромінювання в довкілля (*Electromagnetic Interference - EMI)*

Ступінь та параметри паразитного випромінювання під час передавання сигналу.

1.1.2. Види середовищ передавання даних

а. Коаксиальний кабель (складається з центральної мідної жили, внутрішнього ізолюючого шару, екрану та зовнішньої оболонки). Його характеризує висока швидкість передавання, завадостійкість, довговічність, помірна вартість. Відрізняють:

- *Широкосмугові* – швидкість до 300-500 Мбіт/с, загасання сигналу на частоті 100 МГц – до 7 Дб на 100 м, термін придатності - до 12 років, погонна затримка сигналу – 2-5 нс/м;
- *Вузькосмугові* – швидкість до 50 Мбіт/с, загасання сигналу на частоті 10 МГц – 4Дб на 100 м.

б. Волоконно-оптичний кабель (складається з серцевини з прозорого скловолокна або пластика в оболонці з плівки з меншим коефіцієнтом відбиття). Забезпечує швидкість передавання 0.2-1.0 Гбіт/с, теоретично можливий максимум - 200 Гбіт/с, довжина сполучень 110 км. Відрізняють:

Одномодові – діаметр 10 мкм, загасання 0.7 Дб/км, довжина сполучень до 110 км.

Багатомодові – діаметр 50-140 мкм, загасання 0.5-7.0 Дб/км, довжина сполучень до декількох км, в кабелі передаються кілька променів під різними кутами. ***Мода* – кількість шляхів розповсюдження променів.**

Цей тип середовища характеризують менше загасання, вища швидкість, нечутливість до електромагнітних завад, але при цьому мала механічна стійкість. Потрібні також джерела світлових сигналів (світлодіоди, лазери) та приймачі (фотодіоди, фототранзистори).

в. Вита пара дротів (сама популярна і дешева, це два ізольованих мідних дроти, які скручені між собою, щоби компенсувати вплив електромагнітних полів та випромінювання). Забезпечує відстань передавання до 1.5-2.0 км, швидкість до 1.2 Гбіт/с, погонну затримку сигналу – 8-12 нс/м, загасання на частоті 10 МГЦ - 12-28 Дб на 100 м, термін експлуатації - 2-5 років, але має гірший захист від завад, ніж коаксіальний кабель. Відрізняють такі типи пар:

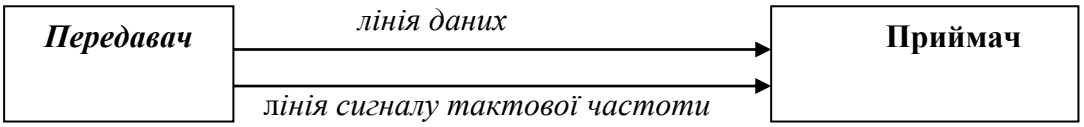
Неекранована (*Unshielded Twisted Pair* **UTP**) **Фольгована** *(Folged Twisted Pair* **FTP**)
Екранована *(Shielded Twisted Pair* **STP**)

За технічними параметрами **UTP** кабелі поділяються на категорії, всього їх 7. Найбільш широко в КМ застосовуються кабелі: 3 категорії – швидкість до 16 Мбіт/с та
5 категорії – швидкість до 100 Мбіт/с, постійна кількість скручень на метр довжини.

1.2. Форми передавання даних у каналах КМ

Цифрові дані в КМ передаються послідовно, бітами, що суттєво відрізняється від передавання між пристроями одного ПК, де воно відбувається паралельно. Фізично біти передаються сигналами. Цифрові дані звичайно передаються без модуляції у формі дворівневого сигналу без повернення до нуля (Non Return to Zero **NRZ**) Тут важко визначити, де починаються та закінчуються логічні 1 та 0. Для розпізнання моментів закінчення та початку логічних сигналів використовують **синхронізацію**. Існує декілька способів передавання синхросигналу.

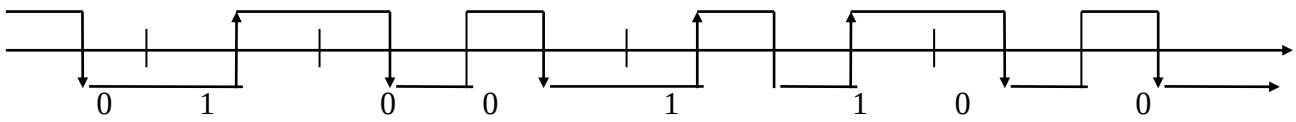
1. *Синхронне передавання*: сигнал тактової частоти-синхросигнал передається по окремій лінії (другій дріт в витій парі)



Синхросигнал можна передавати без окремої лінії: разом з даними або у проміжках між їх передаванням.

2. *Асинхронне передавання або з автоналагодженням*: синхросигнал у проміжках не передається. Потік бітів діліться на байти. Приймач та передавач мають вбудовані тактові генератори з однаковими частотами (стабільними). Перед кожним байтом передається стоп-біт. Він також передається, якщо канал вільний. Під час переходу з високого рівня на низький генератор налагоджується, пропускає один біт і приймає один байт.

Прикладом передавання з автоналагодженням є манчестерське кодування, яке використовується у ЛМ Ethernet. В середині кожного бітового інтервалу є перехід від одного рівня напруги до іншого. Тактовий генератор приймача синхронізується саме під час цього переходу. “1” представлена переходом від L до H, а “0” — переходом від H до L. На початку бітового інтервалу може бути додатковий перехід, якщо передаються послідовності 00 або 11.



Зміна рівня сигналу

Кодування	На середині бітового інтервалу	На границі бітового інтервалу
NRZ	немає	при зміні розряду

Манчестерське	0→ 1 при 1 1→ 0 при 0	0→ 1 при 00 1→ 0 при 11

1.2 Мережеві адаптери Мережевий адаптер — це пристрій (плата), яка забезпечує зв'язок ПК з середовищем передавання мережі. Адаптери станцій локальних мереж безпосередньо приєднуються до внутрішньої шини ПК, що забезпечує більшу швидкість передавання, ніж через послідовний або паралельний порт. В адаптері реалізовані протоколи фізичного та канального рівнів еталонної моделі взаємодії відкритих систем. ***Основні характеристики***:

- До якої мережі належить (Ethernet, Token Ring, FDDI, etc);
- Яку розрядність (8, 16, 32) має та до якої шини (ISA, EISA, PCI, MCA) приєднується;
- Яку має потужність та які алгоритми використовує (для робочих станцій або серверів);
- Які має роз'єднувачі та до якого кабельного середовища ЛМ приєднується.

Роз'єднувачі:

- **BNC** - Для приєднання тонкого коаксіального кабелю;
- **AUI** - Для приєднання товстого коаксіального кабелю;
- **RJ45** - Для приєднання витої пари;
- **MIC, ST, SC** - Для приєднання волоконно-оптичного кабелю

Складові частини адаптера

Співпроцесор — виконує обробку кадрів протоколу канального рівня. Він кодує інформацію перед передаванням у мережу, декодує після приймання, виправляє помилки, повідомляє ЦП про надходження інформації. Використання співпроцесора дозволяє розвантажити ЦП та підвищити загальну швидкодію системи. Оперативна пам'ять — 8 Кбайт. Для запису інформації перед передаванням та після приймання. Пам'ять відображається на адресний простір ПК (параметр Base Memory Address), її може одночасно читати і записувати як ЦП, так і мережний співпроцесор.

Роз'єднувач розширення — для приєднання додаткової мікросхеми пам'яті або мікросхеми постійної пам'яті для завантаження ПК через мережу.

8 регістрів стану та керування – для обміну командами між ЦП та співпроцесором. Вони пронумеровані від 00h до 77h за їхнім зміщення від базового значення (параметр I/O Base Address).

ПЗП адреси — містить унікальну мережеву адресу ПК, встановлену фірмою-виробником адаптера. Перемикач – дає змогу конфігурувати параметри адаптера.

Кабельні роз'єднувачі — для приєднання адаптера до мережі.

Трансівер – для роботи з тонким Ethernet, товстий Ethernet використовує зовнішній.

Роз'єднувач приєднання до системної шини ПК — визначає розрядність та тип шини.

Передавання даних

Комунікаційне ПЗ будує кадри Ethernet та записує їх у пам'ять адаптера. У регістрі керування та стану записується команда передати кадр, адреса та кількість інформації для передавання. Мережний співпроцесор аналізує значення регістрів, бере кожен кадр, обробляє його згідно протоколу і передає у мережу.

Приймання даних

Мережевий співпроцесор стежить через трансівер за кадрами в мережі та виділяє ті, які призначені для даного адаптера. Коли надходить такий кадр, співпроцесор перевіряє правильність даних, розміщує їх у пам'яті, записує у регістр керування та стану команду приймання даних, адресу розміщення у пам'яті і видає для ЦП переривання з визначеним номером. ЦП та комунікаційне ПЗ відкидає службові дані, аналізує прийняті дані та переміщує їх в головну пам'ять.

Конфігурування адаптера

Задають такі параметри:

- **I/O Base Address** – адреса пам'яті, куди відображаються регістри керування та стану;
- **Base Memory Address** — адреса пам'яті, куди відображається внутрішня пам'ять адаптера;
- **IRQ** — номер переривання, за яким ЦП повідомляють про прийняті дані.

Конфігурування може відбуватися з використанням перемикачів, спеціальних програм або автоматично, засобами операційної системи (якщо вони відповідають вимогам стандартів PnP).

Порядок виконання роботи

1. Вивчити типи кабелів КМ; визначити, який кабель використовується в лабораторній мережі.
2. Вивчити алгоритми кодування NRZ та манчестерського:
   a) Побудувати діаграму сигналу для байту даних (Додаток 1)
   - у коді без повернення до нуля NRZ
   - у манчестерському коді;

   b) Декодувати NRZ-сигнал та записати байт даних (Додаток 1);

   c) Декодувати сигнал манчестерського коду та записати байт даних (Додаток 1).
3. Ознайомитись зі структурою мережевого адаптера; визначити, які має роз'єднувачі та до якого кабельного середовища ЛМ приєднується, яку розрядність має та до якої шини (ISA, EISA, PCI, MCA) приєднується.
4. Визначити, який мережевий адаптер встановлений на вашому ПК та його основні параметри.
5. Оформити звіт по роботі

- Звіт повинен включати: тему, мету роботи; короткий огляд теоретичних відомостей;
- подати діаграми сигналів для NRZ- та манчестерського кодів;
- описати типи кабелю та мережних адаптерів, що використовуються в лабораторії;
- зробити висновки щодо отриманих результатів.

Контрольні запитання

1. Які параметри характеризують середовища передавання даних?
2. Які типи середовищ передавання даних ви знаєте?
3. В якій формі передається сигнал в мережі Ethernet?
4. Опишіть основні характеристики мережевого адаптеру.

5. Що входить до складу адаптера?
6. Назвіть основних виробників мережевих адаптерів.

Лабораторна робота №7.

Тема: ” Адресація в комп’ютерних мережах”

Мета роботи : Ознайомитись з типами адрес, які використовуються в комп’ютерних мережах; проаналізувати їх переваги та недоліки; вивчити їх призначення; навчитися визначати адреси ПК в мережі, аналізувати їх структуру та користуватися масками підмереж.

Теоретичні відомості

Вимоги до адреси ПК в комп’ютерній мережі:

- Адреса повинна унікально ідентифікувати ПК в мережі будь-якого масштабу
- Схема призначення адрес повинна бути зручною та зменшити імовірність дублювання адрес
- Адреса повинна бути ієрархічною, тому що це зручно при побудові великих мереж
- Адреса повинна бути зрозумілою для користувача, тобто символьною
- Адресу бажано мати компактною.

Очевидно, що це суперечливі вимоги: ієрархічна адреса менш компактна, ніж апаратна (або плоска), в той час як символьна адреса довше, ніж числова. Тому як правило поєднують декілька схем адресації – ПК має декілька адрес-імен, і вибирається та, що більш відповідає ситуації, а перетворення адрес здійснюється за допомогою спеціальних протоколів Найбільш поширені три схеми адресації.

Апаратні адреси

Призначені для мережі невеликого розміру, тому вони не є ієрархічними. Прикладом може бути адреса мережевого адаптеру ЛМ. Оскільки таку адресу використовує апаратура, її роблять компактною. Наприклад, апаратна адреса мережі Ethernet має довжину 6 байтів і таку структуру:

1 біт – ознака індивідуальної (0) або групової (1) адреси. *2 біт* – спосіб призначення адреси: централізований (0) або локальний (1). В стандартній апаратурі цей біт майже завжди 0, тобто адреса визначена централізовано в IEEE. Комітет IEEE розподіляє між виробниками обладнання так звані організаційно унікальні ідентифікатори. Цей ідентифікатор займає 3 старших байта (наприклад, 000081 означає, що мережевий адаптер вироблений компанією Bay Networks). За унікальність 3 молодших байтів відповідає сам виробник обладнання (зауважимо, що 24 біта дозволяють випустити 16 млн. пристроїв). Апаратна адреса вбудована в апаратуру або автоматично генерується при кожному включенні. НЕДОЛІКИ такої адреси – відсутність ієрархії, при заміні адаптера міняється адреса ПК. Символьні адреси

Такі адреси призначені для того, щоб їх сприймала людина, і тому вони мають смислове навантаження. Використовують як для невеликих, так і для крупних мереж. Приклад: tu.edu.te.ua. Для внутрішньої роботи це забагато – можна використовувати молодшу частину. НЕДОЛІКИ такої адреси – змінний формат і велика довжина. Тому є також числові складні адреси.

Числові складені адреси

Ці адреси мають фіксований і компактний формат. Наприклад, IP-адреси з 2-рівневою ієрархію включають адресу мережі і адресу ПК в мережі. При передачі даних

між мережами працює старша частина адреси, а її молодша частина використовується вже в межах потрібної мережі

IP-адреса (адреса протоколу мережевого рівня) вузла є унікальною логічною адресою і не залежить від апаратури та конфігурації мережі. Її довжина 4 байта, які розділяють крапками для наочності, наприклад 102.54.94.97. Адреса включає **дві частини:** *адресу локальної мережі* і *адресу хосту*. Де пролягає межа між цими частинами, визначають перші біти адреси, вони ж визначають и клас IP-адреси.

01234	8	16	24
0 № мережі	№ хосту		
10 № мережі		№ хосту	
110 № мережі			№ хосту
1110 групова адреса			
11110 зарезервовано			

Клас	Перші біти	Мін. № мережі	Макс. № мережі	Макс. кіль-кість мереж	Макс. кіль-кість хостів
A	0	1.0.0.0.	126.0.0.0	2^7-2 (126)	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{14}	2^{16}
C	110	192.0.0.0	223.255.255.0	2^{21}	2^8 - 2
D	1110	224.0.0.0.	239.255.255.255		
E	11110	240.0.0.0	247.255.255.255		

Клас А: адреса 0 не використовується, а адреса 127 зарезервована для тестування зв'язку ПК з собою (дані відразу вертаються на верхні рівні, ніби то щойно прийняті, при цьому утворюється петля). *Клас В*: призначений для мереж середніх розмірів.

Клас С: використовується в найбільш поширених мережах з невеликою кількістю вузлів. Причому, дві адреси виключаються: 0 – це номер самої мережі, а 255 – широковещательна адреса.

Адреси класу D називаються **груповими**. Повідомлення з такими адресами призначення передаються всім хостам певної групи за допомогою протоколу IGMP (Internet Group Management Protocol).

Маска

Крім поняття класу адреси, який визначається першими її бітами, використовується інший, більш гнучкий механізм встановлення границі між номерами мережі та вузлу. Це маска.

Маска – це число, яке використовується у парі з IP-адресою, воно містить "1" у тих бітах, які мають бути інтерпретовані як номер мережі, "0" – в бітах, що утворюють адресу хосту. Маски стандартних класів:

Клас А – 255.0.0.0

Клас В – 255.255.0.0

Клас С – 255.255.255.0

Кількість "1" в масці не обов'язково має бути кратною 8, тому маски використовуються для розподілу мереж на підмережі з метою ефективного використання адресного простору. Наприклад, 129.64.134.5 – це адреса класу В, тоді номер мережі 129.64.0.0, а номер вузлу 0.0.134.5. Якщо використовувати не стандартну маску, а задати

маску 255.255.128.0, то адреса мережі буде мати вже 17 бітів, тобто виглядати як 129.64.128.0, а номер вузлу займе 15 бітів, що містять значення 0.0.6.5.

Таким чином, для користувачів більш зручні символьні адреси, числові адреси необхідні для забезпечення доставки інформації в потрібну мережу, а апаратні використовують для передачі інформації на потрібний ПК. Так робиться навіть в невеликих мережах, щоб не треба було міняти адреси при включенні такої мережі до складу великої мережі.

- Відповідність адрес встановлює служба розділення (визначення, відображення) імен. Вона може бути двох типів: *централізована* – є сервер імен з таблицею відповідності імен різних типів, до якого звертаються інші ПК, якщо треба по символьній адресі, наприклад, найти числове ім'я. Прикладом є DNS - Domain Name System в Internet;
- *розподілена* – кожний ПК сам вирішує цю задачу. Для цього він розсилає запити з потрібним йому числовим ім'ям, усі ПК порівнюють це ім'я з власним, і потім один з них (той, що має це ім'я) посилає свою апаратну адресу, після чого вже можлива передача по мережі. Переваги – не треба окремого ПК, недолік – надмірне навантаження мережі. З цих причин цей підхід використовується в невеликих локальних мережах.

Порядок виконання роботи

1. Визначити апаратну, символьну та IP-адреси вашого ПК за допомогою команд Run – Cmd – ipconfig /all. Проаналізуйте IP-адресу і визначить, до якого класу відноситься мережа, в якій ви працюєте. Визначить, яка маска встановлена в мережі. Чи є розподіл мережі на окремі під мережі? По заданій IP-адресі вузла та масці підмережі визначити номер під мережі, номер вузлу та максимальну кількість вузлів в такій підмережі (Додаток 2).
2. Визначити вид маски, за допомогою якої можна розбити мережу вказаного класу на потрібну кількість підмереж (Додаток 2).
3. Визначити кількість вузлів в підмережах.
4. Оформити звіт по роботі.

- Звіт повинен включати: тему, мету роботи; короткий огляд теоретичних відомостей;
- отримані дані по результатах виконнання роботи;
- висновки.

Контрольні запитання

1. Яки типи адрес ви знаєте? Які їх недоліки та переваги?
2. Чому в комп'ютерних мережах використовують різні типи адрес?
3. Яким чином встановлюється взаємна відповідність різних адрес для одного ПК?
4. Для чого потрібна маска підмережі?
5. Яку частину всіх IP-адрес складають адреси класу А? Класу В ? Класу С?
6. Чи можна за апаратною адресою визначити виробника мережевого адаптеру? Що для цього потрібно?

Лабораторна робота №8.

Тема: ”Дослідження принципів побудови ЛКМ. Розрахунок конфігурації мережі Ethernet ”

Мета роботи : *Ознайомитись з структурою та призначенням структурних одиниць локальних комп’ютерних мереж. Розглянути специфікації фізичного середовища Ethernet, вивчити механізм виникнення колізій та алгоритм їх розпізнавання, навчитися оцінювати коректність конфігурації мережі та розраховувати необхідні параметри*

Теоретичні відомості

Основні поняття архітектури локальних мереж.

Топологія мережі (кільце, зірка, багаторівнева). Для підвищення ефективності використання комп'ютерної техніки в різних галузях людської діяльності комп'ютери об'єднують в мережі. Користувачі комп'ютерів, які об'єднанні в мережу, можуть передавати один одному повідомлення, спільно використовувати дані, програми, пристрої (наприклад принтери), що значно підвищує зручність і ефективність колективної праці.

Прикладом найпростішої мережі можуть служити два комп'ютери з'єднані між собою через паралельні або послідовні порти. Для створення повноцінної локальної мережі потрібно використовувати спеціальний додатковий пристрій – мережевий адаптер. Топологія мережі визначає фізичне розташування сітьових кабелів, а також фізичне підключення клієнтів до мережі. В даний час використовуються три схеми (топології) побудови мереж: шина, зірка і кільце. Кожній із цих схем властиві свої переваги і недоліки. ***Шина***

Найбільш дешевою схемою організації мережі є топологія шини, що припускає безпосереднє підключення всіх мережевих адаптерів до мережевого кабелю. Як Thin Ethernet, так і Thick Ethernet є варіантами шинної організації мережі. Структура такої мережі показана на мал. 1. Всі комп'ютери в мережі підключаються до одного кабелю. Перший і останній комп'ютери повинні бути *розв'язані.* У ролі розв'язки (термінатора) виступає простий резистор, що використовується для гасіння сигналу, що досягає кінця мережі, щоб запобігти виникненню перешкод. Крім того, один і тільки один із кінців мережевого кабелю повинний бути заземлений, що дозволить уникнути виникнення петлі заземлення. Основним недоліком топології шини є ймовірність виходу з ладу всієї мережі при виникненні несправності на будь-якій ділянці мережевого кабелю. Для виявлення місця несправності шину доведеться розбити на дві окремі частини, що дозволить з'ясувати, у який із них виник обрив. Потім сегмент кабелю, у якому був виявлений обрив, також розділяється на дві частини, і подібна процедура повторюється, доти, поки несправність не буде локалізована Цей процес забирає достатньо багато часу Проте це не виключає можливості використання топології шини. Вона щонайкраще підходить для об'єднання комп'ютерів у навчальних класах і створення невеликих мереж, де кабелі можна прокласти в легко доступних місцях.

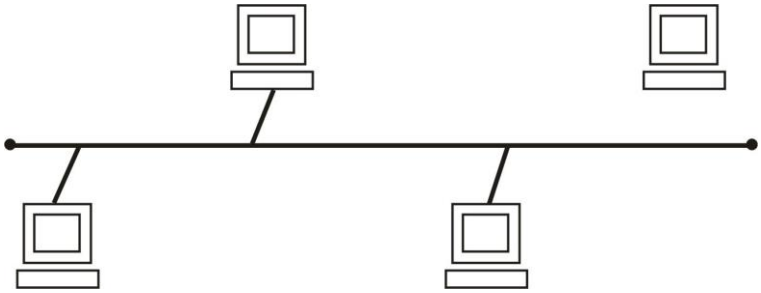


Рисунок 1 Організація мережі з використанням топології шини

Зірка

Для організації більшості мереж у даний час застосовується топологія зірки. У даному випадку недолік, пов'язаний із ймовірністю виникнення обриву в загальному кабелі, вирішується застосуванням окремих кабелів для підключення кожного з комп'ютерів до головного мережевого кабелю.

Кожна робоча станція підключається до повторювача, який має декілька портів, що називається *хабом,* або *концентратором*. Хаб, у свою чергу, підключається до головного мережевого кабелю. Основним призначенням хаба є передача сигналів від головного кабелю мережі до окремих робочих станцій, як показано на мал. 2. У випадку обриву кабелю, що з'єднує хаб із робочою станцією, зв'язок із мережею втратить тільки ця станція. Інші ж зможуть безперешкодно продовжувати роботу в мережі. Проте у випадку виходу з ладу хабу зв'язок із мережею втрачають всі залучені до нього користувачі станцій. Звичайно, такого роду несправність виявляється досить легко, оскільки всі користувачі, залучені до цьому хабу, негайно звернуть увагу адміністратора мережі на неполадку, що виникла. На відміну від топології шини, де на пошук неполадки йде велика кількість сил і часу, а хаб, що вийшов із ладу, буквально заявляє про себе сам. На випадок виникнення подібної аварії необхідно мати про запас резервний хаб, яким можна було б замінити хаб, що вийшов з ладу. Тому має сенс обладнувати всю мережу хабами одного типу. Крім того, гарні результати дає застосування інтелектуальних хабів. Подібні хаби підтримують протокол SNMP, що можна використовувати для віддаленого керування і тестування хаба, не покидаючи робочого місця.

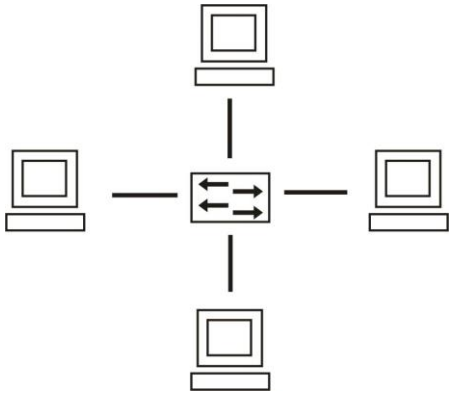


Рисунок 2 Організація мережі з використанням топології зірки

Кільце

Топологія кільця застосовується головним чином фірмою IBM для організації кільцевих мереж з естафетним доступом. Структура мережі, побудованої на основі даної топології, нагадує структуру у випадку топології зірки (Мал. 2). Замість хабу користувачі станції підключаються до пристрою множинного доступу (Multiple Access Unit, або

MAU), що робить логічне з'єднання комп'ютерів мережі в кільце, як показано на мал. 3. Топологія кільця має ті ж переваги, що і топологія зірки, оскільки фізична організація цих двох типів мереж ідентична. Звідси випливає, що топології кільця властиві і ті ж самі недоліки, оскільки частіше усього з ладу виходить пристрій множинного доступу.

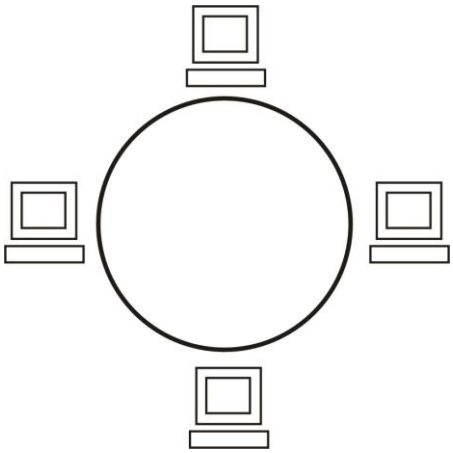
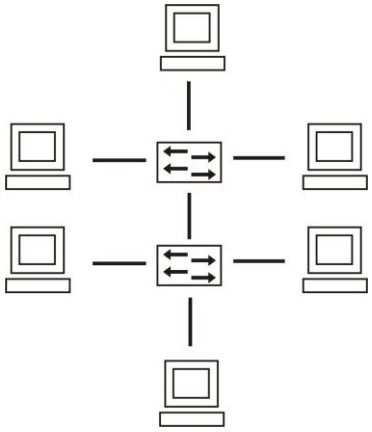


Рисунок 3. Організація мережі з використанням топології кільця.

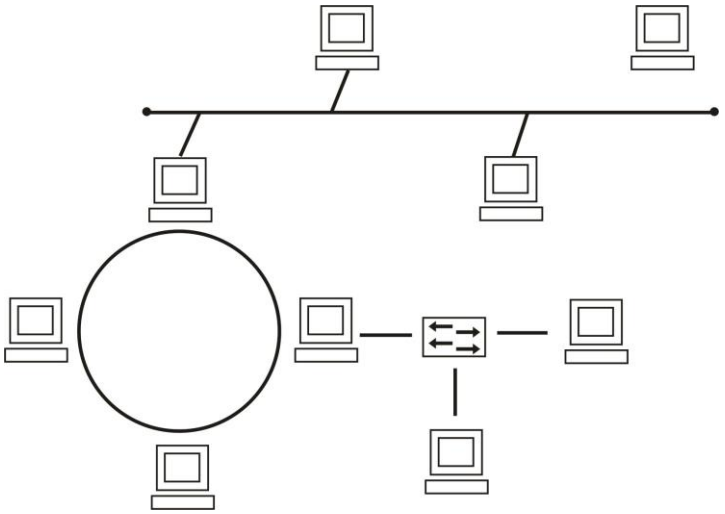
„Розширена зірка" топологія мережі. Являє собою об'єднання декількох топологій



"зірка".

Рисунок 4. Топологія "Розширена зірка"

„Гібридна" топологія мережі. Дана топологія є об'єднанням декількох різних за



структурою топологій.

Рисунок 5. Топологія "Гібридна"

Комунікаційні пристрої

Більшість комп'ютерних систем організацій розташовується або на платформі великих машин (Mainframes) і міні-комп'ютерів, або з використанням мереж UNIX-комп'ютерів, що працюють по принципу "клієнт-сервер", тобто в режимі зберігання і обробки основних даних на центральній ЕОМ (на так званому сервері) і формування запитів на робочому місці з пересиланням по мережі на центральну машину і отриманням з неї готових форм звітності. В економічній діяльності для створення локальних мереж найчастіше використовують кабельні (коаксіальні та на витій парі), а в останній час і оптичні канали; для створення розподілених мереж - провідні, радіорелейні, тропосферні та космічні канали. Для побудови мережі використовується топологія зірки. Структура типової мережі наведена на наступному малюнку:

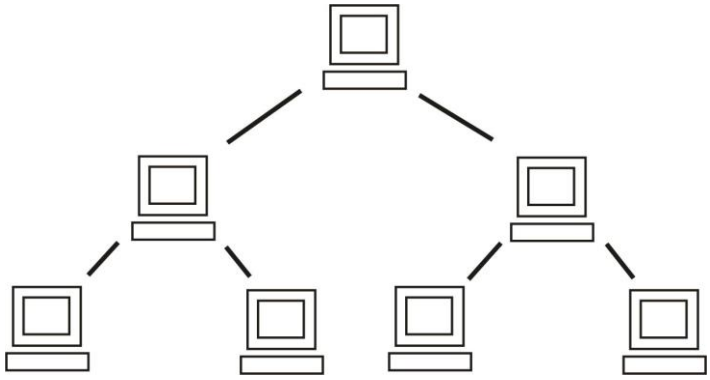


Рисунок 6. Топологія “Деревовидна”

Топологічно мережа представляє собою "дерево", де розвилками служать вузлові пристрої, "гілками" - кабелі, що закінчуються розетками, на яких знаходяться "листя" - кінцеві пристрої. Прокладка кабелю з розетками здійснюється по всьому приміщенню, а підключення кінцевих пристроїв по мірі необхідності. Ефективність мережі може бути значно підвищена за рахунок використання МОСТІВ (Local bridge), які пропускають пакет інформації з одного свого порту на інший тільки в тому випадку, коли його відправник і отримувач знаходяться по різні сторони; МАРШРУТИЗАТОРІВ (router), які керують маршрутом проходження пакету інформації; КОНЦЕНТРАТОРІВ (hub), багатопортових активних елементів, здатних здійснювати більш складні операції з потоками інформації, зокрема підсилення сигналу і фільтрацію шумів, а також контроль за станом пристроїв, що підключені до портів; КОММУТАТОРІВ (switch), що забезпечують передачу пакету інформації між будь-якими двома із своїх портів, що збільшує в відповідне число раз пікову пропускну спроможність мережі. ***Керування мережею***

- Поняття КЕРУВАННЯ МЕРЕЖЕЮ містить наступні дії: управління конфігурацією, тобто можливість контролю і управління всією мережею з будь-якого місця в ній;
- виявлення і ліквідацію несправностей, в тому числі і автоматизовані;
- контроль продуктивності, що дозволяє виявити джерела великих потоків інформації, вузькі місця і надання можливості моделювання поведінки в мережі в різних умовах;
- керування використанням мережі, що передбачає можливість керування використанням ресурсів мережі окремими користувачами та групами користувачів;
- керування доступом, що дозволяє адміністратору мережі регулювати використання ресурсів мережі користувачами.

Розпізнавання колізій

Чітке розпізнавання колізій всіма станціями – необхідна умова коректної роботи мережі Ethernet: якщо колізія не розпізнана, станція вирішить, що кадр передано правильно, він буде спотворений і втрачений, тому що приймач його не розпізнає, хоча спотворена інформація пізніше може бути передана протоколами верхнього рівня (транспортним), але це займе більше часу, ніж на рівні Ethernet – звідси зниження перепускної спроможності мережі. Для надійного виявлення колізій необхідно:

$$T_{min} \geq PDV$$

Tmin – час передавання кадру мінімальної довжини

PDV – час подвійного обертання (Path Delay Value). Це час, за який сигнал колізії встигає розповсюдитися до самого далекого вузла мережі. В найгіршому випадку сигнал повинен пройти двічі між найбільш віддаленими ПК (в одну сторону йде неспотворений сигнал, а назад – сигнал, спотворений колізією). Ця умова гарантує, що передавач встигне виявити колізію, яку спричинив його кадр, ще до того, як буде закінчене передавання цього кадру.

Виконання умови залежить від довжини мінімального кадру та перепускної здатності мережі, а також довжини кабельної системи та швидкості розповсюдження сигналу в кабелі, вона різна для різних середовищ передавання.

В стандарті Ethernet мінімальна довжина кадру разом з службовими полями та преамбулою становить 72 байта або 576 бітів.

Отже, при 10 Мбіт/с час передавання кадру мінімальної довжини становить 575 bt, де bt – це бітовий інтервал, тобто час між появою двох послідовних бітів в кабелі, тому PDV має бути менше 57,5 мкс. Відстань, яку може пройти сигнал за цей час, залежить від типу кабелю.

Основні параметри рівня MAC передавання кадру за стандартом IEEE 802.3

Бітова швидкість	10 Мбіт/с
Інтервал очикування	512 bt
Міжкадровий інтервал (IPG Inter Packet Gap) (після закінчення передавання всі ПК витримують цю технологічну паузу, щоби привести адаптери у початковий стан)	9.6 мкс
Максимальна кількість спроб передавання	16
Максимальне зростання діапазону паузи	10
Довжина jam-послідовності, яку передає станція, що виявила колізію	32 біт
Максимальна довжина кадру без преамбули	1518 байт
Мінімальна довжина кадру без преамбули	64 байт (512 біт)
Довжина преамбули	64 біт
Мінімальна довжина випадкової паузи після колізії	0 bt

Максимальна довжина випадкової паузи після колізії	524000 bt
Максимальна відстань між ПК	2500 м
Максимальна кількість станцій в мережі	1024

Специфікації фізичного середовища Ethernet

Метод доступу МДКН/ВК та часові параметри є загальними для всіх специфікацій. 10 – означає бітову швидкість передавання, Base – метод передавання на одній базовій частоті (на відміну від широкосмугових методів Broadband, які використовують декілька частот-носіїв), останній символ – тип кабелю.

	10Base-5	**10Base-2**	**10Base-T**	**10Base-F**
Кабель	товстий коаксіальний кабель діаметром 0.5" RG-8 і RG-11	тонкий коаксіальний кабель діаметром 0.25" RG-58	неекранована вита пара категорій 3, 4, 5	Багатомодовий волоконно-оптичний кабель
Максимальна довжина сегменту, м	500	185	100	2000
Максимальна відстань між вузлами мережі (при використанні повторювачів), м	2500	925	500	2500 (2740 для 10Base-FB)
Максимальна кількість станцій в сегменті	100	30	1024	1024
Максимальне число повторювачів між двома станціями в мережі	4	4	4	4 (5 для 10Base-FB)

Домен колізій Домен колізії ДК (collisiom domain) – частина мережі Ethernet, всі вузли якої розпізнають колізію, незалежно від того, в якій частині мережі ця колізія виникла. Мережа Ethernet, яку побудовано на повторювачах, завжди один ДК. Мости, комутатори та маршрутизатори – розділяють на декілька ДК.

Методика розрахунку конфігурації мережі Ethernet

Дотримання всіх обмежень, які встановлені для різних стандартів фізичного рівня мереж Ethernet, гарантує їх коректну роботу. Найчастіше доводиться перевіряти обмеження на довжину окремого сегменту кабелю, кількість повторювачів та загальну довжину мережі. Правило "4 хабів" і аналогічне правило "5-4-3" в коаксіальній мережі залишають великий запас (час передавання мінімального кадру – 575 bt, а час подвійного обертання в мережі 10Base-5 із 4 повторювачів - 5 сегментів максимальної довжини 500 м

буде 537, тобто 38 bt залишається для надійності, хоча комітет IEEE 802.3 каже, що і 4 bt теж надійно).

Комітет IEEE 802.3 розробив таблиці затримок, які вносять повторювачі та різні середовища передавання, щоби можна було самостійно розрахувати макс. кількість повторювачів та макс. загальну довжину мережі, не передбачені правилами “4 хабів” і “5-4-3”. Особливо це потрібно, якщо сегменти мережі побудовані на різних кабельних системах, але кожен сегмент повинен відповідати певному стандарту. Щоби така мережа працювала, необхідно виконання 4 умов:

Кількість станцій в мережі не більше 1024;

Максимальна довжина кожного фізичного сегменту неповинна перевищувати величину, вказану у відповідному стандарті;

Час подвійного обертання між самими віддаленими вузлами (Path Delay Value, PDV) не більше 575 bt;

Зменшення міжкадрового інтервалу IPG (Path Variability Value, PVV) після проходження через всі повторювачі не більше 49 bt (початкове значення 96 bt).

Дотримання цих правил забезпечує нормальну роботу мережі навіть, якщо її загальна довжина більше 2500 м або в ній є більше 4 хабів. Розрахунок PDV

Таблиці IEEE містять затримки в різних повторювачах і середовищах, причому, ці величини враховують всі етапи проходження сигналу в пристрої, причому вони наведені для подвійної довжини кабелю.

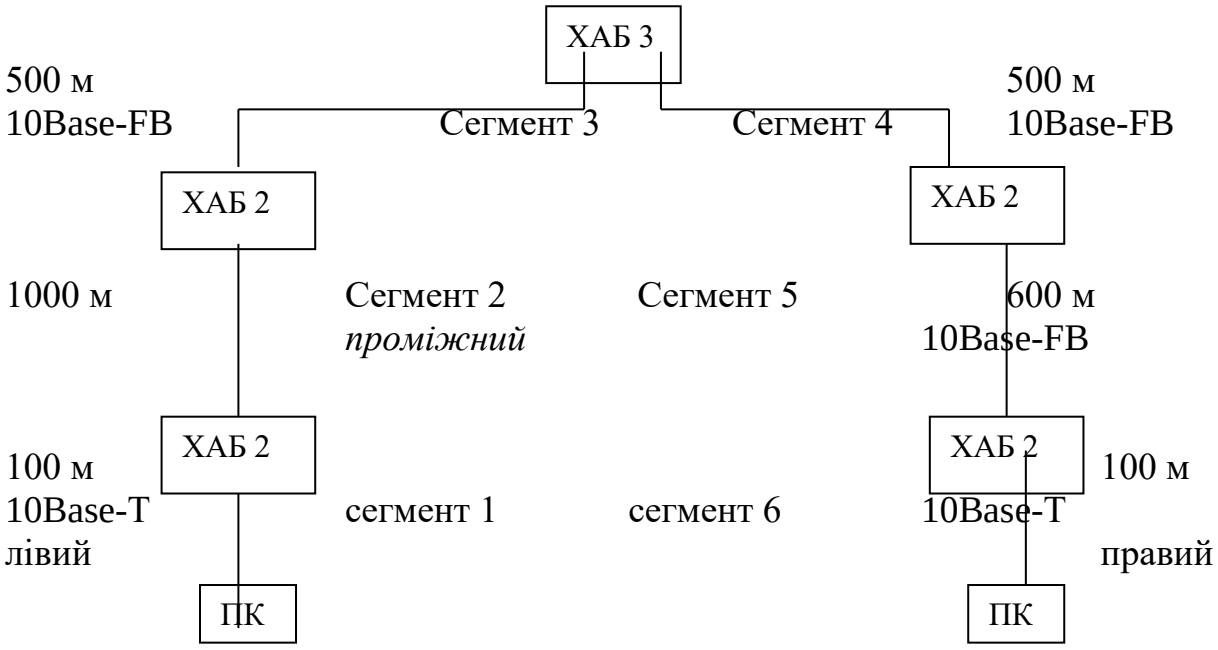
Тип сегменту	База лівого сегменту, bt	База проміжного сегменту, bt	База правого сегменту, bt	Затримка середовища на 1 м, bt	Максимальна довжина сегменту, м
10Base-T	15.3	42.0	165.0	0.113	100
10Base-FB	-	24.0	-	0.1	2000
10Base-FL	12.3	33.5	156.5	0.1	2000
10Base-5	11.8	46.5	169.5	0.0866	500
10Base-2	11.8	46.5	169.5	0.1026	185
FOIRL	7.8	29.0	152.0	0.1	1000
AUI	0	0	0	0.1026	50

Лівий сегмент – той, в якому починається шлях сигналу від виходу передавача Tx кінцевого вузла– це сегмент 1 га малюнку. Далі він йде через проміжні сегменти 2-5 і доходить до входу Rx найбільш віддаленого вузлу сегменту 6, який називається правим. Тут і відбувається колізія в найгіршому випадку.

З кожним сегментом пов’язана постійна затримка, яка називається базою і залежить від типу сегменту на його положення на шляху сигналу (лівий, проміжний, правий). База правого сегменту, де виникає колізія, більше. База сегменту враховує затримки вхідного трансіверу, блока повторювання та вихідного трансіверу.

Крім того, з кожним сегментом пов’язана затримка розповсюдження сигналу уздовж кабелю, яка залежить від його довжини і дорівнює: (час розповсюдження сигналу по 1 м) х (довжина кабелю, м).

Розрахунок складається з обчислювання затримок з боку кожного відрізку, а потім додавання їх до баз сегментів (лівий, проміжний, правий). Загальне PDV не повинно перевищувати 575. Оскільки лівий і правий сегменти мають різні бази, то якщо по краях мережі сегменти різних типів, треба провести розрахунок двічі і вибрати максимальне значення.



З точки зору правила 4 хабів мережа некоректна, загальна довжина 2800 м > 2500 м.

1: 15,3 + 100 x 0,113 = 26,6
2: 33,5 + 1000 x 0,1 = 133,5
3: 24 + 500 x 0,1 = 74
4: 24 + 500 x 0,1 = 74
5: 24 + 600 x 0,1 = 84
6: 165 + 100 x 0,113 = 176,3

PDV=568.4 < 575, тобто мережа задовольняє критерій PDV.

Розрахунок PVV

Треба також визначити зменшення міжкадрового інтервалу повторювачами, тобто PVV. Для розрахунку PVV є відповідні таблиці максимальних величин зменшення міжкадрового інтервалу при проходженні через повторювачі різних фізичних середовищ:

Тип сегменту	Передавальний сегмент, bt	Проміжний сегмент, bt
10Base-T	10,5	8
10Base-FB	-	2
10Base-FL	10,5	8
10Base-5	16	11
10Base-2	16	11

1: 10,5 4: 2
2: 8 5: 2
3: 2

Сума=24,5, що менше 49. Отже, мережа відповідає стандартам Е.

Порядок виконання роботи

1. За допомогою програми NetCracker Professional зобразити графічно структуру локальної мережі на основі коаксиального кабелю з топологією “загальна шина”. (перелік індивідуальних завдань наведено в додатку 4)
    a. На робочій панелі Top розмістити: сервер, 5 робочих станцій, мережевий принтер, сегмент товстого коаксиального кабелю; при цьому вибірати обладанання типу Ethernet;
    b. Дати назви всім вузлам та середовищу передавання;
    c. Встановити сполучення між всіма вузлами мережі та загальною шиною (Modes → Link Devices → Link Assistant → задати довжину), при цьому звернути увагу на зміст полів, де вказані протоколи, середовище, швідкість передавання;
    d. Встановити мережевий трафік типу InterLAN traffic (Modes → Set Traffic → Profiles → Assign). Враховуйте при цьому, які вузли взаємодіють між собою.
    e. Запустити моделювання мережі (F5) і спостерігати її роботу.
    f. Зупинити моделювання (Alt + F5). Зберегти проект.
2. За допомогою програми NetCracker Professional зобразити графічно структуру локальної мережі на основі витої пари з топологією “зірка”. (перелік індивідуальних завдань наведено в додатку 4)
    a. На робочій панелі Top розмістити: файловий та поштовий сервери, 5 робочих станцій, концентратор з достатньою кількістю портів; при цьому вибірати обладанання типу Ethernet;
    b. Дати назви всім вузлам;
    c. Встановити сполучення між всіма вузлами мережі та загальною шиною (Modes → Link Devices → Link Assistant → задати довжину), при цьому звернути увагу на зміст полів, де вказані протоколи, середовище, швідкість передавання;
    d. Встановити мережевий трафік типу InterLAN traffic (Modes → Set Traffic → Profiles → Assign). Враховуйте при цьому, які вузли взаємодіють між собою.
    e. Запустити моделювання мережі (F5) і спостерігати її роботу.
    f. Зупинити моделювання (Alt + F5). Зберегти проект.
3. За допомогою програми NetCracker Professional зобразити графічно структуру локальної мережі відповідно до завдання на курсовий проект і спостерігати її роботу за допомогою моделювання аналогічно до попереднього завдання. Зберегти проект..
4. Оформити звіт по роботі

- Звіт повинен включати: тему, мету роботи; короткий огляд теоретичних відомостей;
- описати створені проекти;

- зробити висновки щодо характеристик та результатів спостерігання за роботою змодельованих мереж.
- Побудувати схему конфігурації мережу (дані дає викладач).
- Підрахувати час подвіного обертання сигналу між самими віддаленими вузлами.
- Підрахувати зменшення міжкадрового інтервалу.
- Оцінити коректність мережі. Підрахувати аналогічні величини для мережі в аудиторії.

Контрольні запитання

1. Порівняйте переваги та недоліки топологій типу шина та зірка.
2. Які є основні комунікаційні пристрої? Їх функції?
3. За якими стандартами побудована мережа в аудиторії? Основні робочі характеристики?
4. До якого рівня моделі взаємодії відкритих систем відносяться протоколи, що використані при побудові проектів в межахі даної лабораторної роботи?
5. Що таке колізія:
6. ситуація, коли станція, яка хоче передати пакет, виявляє, що в цей момент інша станція вже зайняла середовище передавання даних;
7. ситуація, коли дві робочі станції одночасно передають дані в розподілене середовище передавання.
8. Що таке домен колізій?
9. З яких міркувань вибрано максимальну довжину фізичного сегменту в стандартах Ethernet?
10. Чому треба дотримуватися правила “4 хабів”?
11. Чому в стандарті 10Base-5 вибрали мінімальний розмір кадру 64 байта?

Лабораторна робота №9.

Тема: ”Оцінка роботи комп’ютерної мережі. Моніторинг стану мережі ”

Мета роботи : *Вивчити основні показники продуктивності комп’ютерної мережі; навчитися будувати проект багатосегментної мережі за допомогою засобів NetCracker; проаналізувати залежність перепускної здатності мережі від параметрів протокольних блоків даних. Вивчити основні показники продуктивності комп’ютерної мережі; навчитися будувати проект багатосегментної мережі за допомогою засобів NetCracker; проаналізувати залежність перепускної здатності мережі від параметрів протокольних блоків даних.*

Теоретичні відомості

Продуктивність комп’ютерної мережі

Характеристики продуктивності включають:

- *Час реакції* – інтервал часу між тим моментом, коли у користувача виник запит до мережевої служби, і тим моментом, коли він отримав відповідь. Це узагальнена характеристика, що складається з багатьох компонентів і залежить від поточного стану мережі (наприклад, деколи ми кажемо, що сьогодні мережа працює повільно).

Перепускна здатність – об’єм даних, що передається мережею за одиницю часу, біт/с або пакет/с. Це вже не оцінка користувача, а характеристика виконання основної функції мережі – транспортування повідомлень. Є різні перепускні здатності (середня, максимальна, миттєва). *Затримка передачі та варіація затримки* – затримка між поступленням пакету на вхід мережевого пристрою або частини мережі та моментом його появлення на виході цього пристрою. Відрізняється від часу реакції тим, що характеризує тільки мережеві етапи обробки даних , не враховує обробку на ПК. Не всі види трафіку чутливі до затримки (пошта, файли, друк – не чутливі; але звук та зображення – чутливі). Цей параметр і перепускна здатність – незалежні параметри, тобто може бути висока перепускна здатність, але вносяться великі затримки, як наприклад, у супутникових каналах (велика довжина та час розповсюдження сигналу).

Формат кадру 802.3/LLC Кадр складається з заголовку та поля даних Заголовок є результатот об’єднання полів заголовків кадрів, визначених в стандартах IEEE 802.3 і 802.2. Стандарт IEEE 802.3 визначає 8 полів заголовку (преамбула та початковий обмежувач не показані):

6	6	2	1	1	1(2)	46-1497(1496)	4
DA	SA	L	DSAP	SSAP	Control	Data	FCS
						Заголовок LLC ⟷	

- *Преамбула* (Preamble) – 7 байтів 10101010 для синхронізації
- *Початковий обмежувач кадру (Start-of-frame-delimiter, SFD)* – 10101011, вказує, що наступний байт – це перший байт заголовку.
- *Адреса призначення (Destination Address, DA)* – довжина 6 байтів. *Адреса відправлення* (Source Address, SA) –6 байтів адреси вузла-відправника, 1 біт завжди 0.
- *Довжина (Length, L)* – 2 байта довжини поля даних.

- *Поле даних (Data, D)* – від 0 до 1500 байтів; якщо менше 46 байтів, то кадр доповнюється до мінімальної довжини 46 байтів. Це забезпечує виявлення колізій.
- *Контрольна сума* (Frame Check Sequence, FCS) – 4 байта.
- *DSAP Destination Service Access Point* – адреса точки входу служби призначення.
- *SSAP Source Service Access Point* - адреса точки входу служби відправника.
- *Control* – поле керування (визначає режими взаємодії).

Кадр 802.3 – кадр MAC-підрівня, тому в його поле даних вкладається кадр LLC 802.2 з видаленими флагами початку та кінця. Його заголовок - 3 або 4 байта, залежно від режиму, тому поле даних зменшено до 1497 або 1496 байтів. DSAP і SSAP вказують, який протокол верхнього рівня вклав свій пакет до поля даних, щоби при отриманні йому ж його і передати (наприклад, якщо SAP=0x6, то це протокол IP).

Максимальна швидкодія мережі Ethernet

Кількість кадрів Ethernet, яка обробляються за секунду, часто вказується виробниками мостів, комутаторів та маршрутізаторів як основна характеристика швидкодії цих пристроїв. З іншого боку, бажано знати “чисту” перепускну здатність сегменту Ethernet (у відсутності колізій і затримок від мостів/комутаторів та маршрутізаторів), тому що це верхня межа вимог до комунікаційного обладнання з боку протоколу. Найбільше навантаження створюють кадри мінімальної довжини. При цьому час на обробку кадру приблизно однаковий, він пов’язаний з переглядом таблиць, формуванням нового пакету, ін., а кількість пакетів більше, ніж у випадку кадрів любої іншої довжини. **Кадр мінімальної довжини** з преамбулою - 576 біт, тому на його передавання витрачається 57,5 мкс. Додаємо міжкадровий інтервал 9,6 мкс, і отримаємо інтервал надходження кадрів мінімальної довжини - 67.1 мкс. Звідси максимальна перепускна здатність **14 880 кадр/с у випадку кадрів мінімальної довжини**. Для кадрів максимальної довжини 1526 байт (12 208 біт) отримаємо 813 кадр/с. Як можна бачити, при роботі з великими кадрами навантаження на комунікаційне обладнання суттєво знижується.

Корисна перепускна здатність протоколу

Корисна перепускна здатність $C_п$ – це швидкість передавання даних користувача, які переносяться полем даних кадру. Вона завжди менше номінальної бітової швидкості протоколу Ethernet за рахунок таких факторів:

- Службова інформація кадрів;
- Міжкадрові інтервали;
- Очікування доступу до середовища.

Для кадрів мінімальної довжини: $C_п$=14880 кадр/с *46 байт (дані) * 8=5.48 Мбіт/с

Це значно менше 10 Мбіт/с, але ці кадри – в основному квитанції, а не дані.

Для кадрів максимальної довжини: $C_п$=813 кадр/с *1500 байт (дані) * 8=9,76 Мбіт/с

Це значення дуже близько до номінальної швидкості протоколу, але це можливо тільки якщо двом вузлам не заважають інші, що буває дуже рідко. Відношення поточної перепускної здатності мережі до її максимальної перепускної здатності називається коефіцієнтом використання мережі (network utlizaton).

Моніторинг стану мережі

Структура протокольного стеку TCP/IP

Прикладн.	Telnet	FTP	SNMP	SMTP	DNS	інші	прикладн. відображ.
Основ. (трансп.)	TCP			UDP			сеансовий транспорт.
Рівень міжмереж. взаємодії	протоколи маршрутизації RIP	**ICMP IGMP OSPF IP** ARP RARP					мережевий.
Рівень мережев. інтерфейсів	Ethernet, Token Ring, FDDI, ATM, PPP, SLIP, інші						канальний фізичний

Рівень міжмережевої взаємодії.

Це основа стеку. Рівень реалізує передачу пакетів без встановлення з'єднань, тобто *даграмним* способом і просування пакетів по найбільш раціональному маршруту. **IP** Internet Protocol (протокол для складених мереж) –основний протокол мережевого рівня цього стеку, який забезпечує передавання пакетів по складеній мережі, але не підтримує послідовне передавання і не гарантує надійність передавання, хоча і намагається це зробити.

Декілька протоколів цього рівня виконують допоміжні функції, такі як створення та модифікація таблиць маршрутизації, збір маршрутної інформації. До них відносяться: **ICMP** Internet Control Message Protocol – діагностичний протокол для передавання інформацій між вузлами про помилки та збої, аномальні значення параметрів, неможливість доставки;

Повідомлення з адресами призначення класу D (**груповими)** передаються всім хостам певної групи за допомогою протоколу **IGMP** (Internet Group Management Protocol). Інформація про склад групи є в маршрутизаторі.

ARP Address Resolution Protocol - перетворює IP-адресу в канальну (локальну) адресу, що потрібно для спільної роботи мереж, побудованих на різних технологіях, а протокол **RARP** Reverse Address Resolution Protocol виконує зворотну функцію;

RIP Routing Internet Protocol – збір маршрутної інформації.

Основний рівень.

Оскільки на рівні міжмережевої взаємодії з'єднання не встановлюються, то немає гарантії, що пакети дійдуть непошкодженими і в тому порядку, в якому вони були відправлені. Цю задачу – забезпечення надійного інформаційного зв'язку між кінцевими вузлами вирішує основний або транспортний рівень. На цьому рівні працюють два протоколи:

TCP Transmission Control Protocol – протокол керування передачею транспортного рівня з попереднім налагодженням логічного сполучення. Протокол ділить потік байтів на сегменти, передає їх рівню міжмережевої взаємодії. Коли вони будуть доставлені до пункту призначення, TCP знову їх об'єднає в неперервний потік байтів. Він гарантує надійне передавання пакетів та забезпечує їхню правильну послідовність за рахунок нумерації сегментів в чергах, використання квитанцій при відповідному виборі розміру скользящего вікна та тайм-ауту.

UDP User Datagram Protocol - протокол даграм користувача, який використовується замість протоколу TCP, якщо немає потреби в додаткових заходах щодо забезпечення надійного передавання. Передає даграмним способом, як і протокол IP. Це

фактично зв'язка (мультиплексор) між мережевим протоколом та багатьма службами прикладного рівня. ***Прикладний рівень.***

- Цей рівень об'єдную усі служби, які система надає програмам користувача. Серед протоколів прикладного рівня вкажемо: telnet – емуляція терміналу, FTP File Transfer Protocol - протокол передавання файлів, SMTP Simple Mal Transfer Protocol – електронна пошта, SNMP Simple Network Management Protocol - керування мережею, DNS Domain Name Service –служба логічних імен,
- HTTP – протокол передачи гіпертекстової інформації.

Рівень мережевих інтерфейсів

Рівень мережених інтерфейсів – це те, що відрізняє TCP/IP від інших стеків. Для кожної технології розробляються власні інтерфейсні засоби – так звані протоколи інкапсуляції IP-пакетів в кадри локальних технологій. На цьому рівні використовують протоколи відомих мережевих архітектур (Ethernet, Token Ring, FDDI – для *локальних мереж*, для *глобальних мереж* – протоколи роботи через призначені або комутовані телефонні лінії **SLIP** Serial Line IP, **PPP** Point to Point Protocol, протоколи територіальних мереж, тощо).

В цілому структура протокольного стеку TCP/IP відповідає моделі OSI.

Структура IP- пакету

IP-пакет складається із заголовка та поля даних.

Заголовок 20 байт	блок даних

4 біта 8 16 24

версія протоколу	довжина заголовку	тип сервісу				загальна довжина, байт, 65535 макс. *З врахуванням заголовку та даних*
		PR	D	T	R	
ідентифікатор						Флаг 3 біта / зміщення від початку фрагментованого пакету 13 біт
час перебування пакету в мережі (час життя в секундах) 8 бітів		протокол трансп. рівня, якому спрямований пакет				КС заголовку
IP адреса джерела інформації						
IP адреса призначення						
необов'язкові параметри безпеки та маршрутизації *використовуються під час налагодження мережі*						наповнення пропусками до цілого числа 32 біт. слів

Довжина заголовку IHL – вимірюється в 32-бітових словах. Звичайно це 5 слів (20 байтів), але може стати більше за рахунок додаткових байтів в останньому полі.

Тип сервісу – задають пріоритет пакету PR(біти 0-2, від 0 для звичайного повідомлення до 7 для мережевого керування), бажаний тип якості транспортування (біти 3-6, вибір між швидкістю та надійністю): D delay – треба вибрати маршрут з мінімальною затримкою даного пакету; T – забезпечити максимальну перепускну здатність; R – забезпечити максимальну надійність доставки.

Загальна довжина – вибирається з врахуванням максимальної довжини кадру нижнього рівня, в який вкладається IP-пакет (для Ethernet це буде 1500 байтів, це як раз поле даних кадру Ethernet).

Ідентифікатор – для розпізнавання пакетів, що утворилися внаслідок фрагментації вихідного пакету, однаковий для всіх фрагментів. Всі системи мають обмеження на

максимальний розмір кадру, тому деколи потрібно розділяти пакети на менші, а потім знов їх об'єднувати. **Флаг** – ознака того, чи можна фрагментувати пакет, а також що пакет фрагментовано і це не останній фрагмент.

Час перебування пакету в мережі – щоби уникнути необмеженого в часі перебування пакету у мережі. При формуванні записують час, потім при кожному опрацюванні пакету в маршрутизаторі цей час зменшується, після досягнення 0 – пакет знищується. Оскільки час перебування в маршрутизаторі рідко перевищує 1 секунду, можна вважати, що це кількість вузлів до пункту призначення.

Протокол верхнього рівня – це може бути TCP, UDP, ICMP etc.

КС – розраховується тільки по заголовку, вона повторно підраховується під час кожної обробки IP- пакету, тому що деякі його поля змінюються (час життя, наприклад).

Формат повідомлень UDP

Якщо задачею мережевого рівня є передача даних між довільними вузлами мережі, то задача транспортного рівня полягає в передачі даних між будь-якими *прикладними процесами*, що виконуються на будь-яких вузлах мережі. Коли пакет засобами протоколу IP доставлено в комп'ютер - адресат, дані необхідно скерувати конкретному процесу - одержувачу. Кожний комп'ютер може виконуваним декілька процесів. Пакети, які поступають на транспортний рівень, впорядковуються в черги до точок входу різних прикладних процесів. В термінології TCP/IP такі системні черги називаються *портами*. Таким чином, адресою призначення, що використовується на транспортному рівні, є ідентифікатор (номер) порту прикладного сервісу. Номер порту разом з номером мережі і номером комп'ютера, однозначно визначають прикладний процес в мережі. UDP-пакет або данограма містить заголовок і полі даних, в якому розміщується пакет прикладного рівня. Заголовок складається з чотирьох 2-байтових полів: UDP source port - номер порту процесу -відправника, UDP destination port - номер порту процесу - отримувача, UDP message length - довжина UDP-пакета в байтах, UDP checksum - контрольна сума UDP-пакета ***Формат повідомлень TCP***

Протокольний блок даних TCP – це сегмент. Не всі сегменти, що посилаються через одне TCP- сполучення, мають однаковий розмір, але при цьому чітко визначається максимально припустимий розмір. Як і на мережевому рівні, де максимальний розмір IP-пакету повинен відповідати полю даних в кадрі канального рівня, так і сегмент має повністю входити до поля даних IP- пакету. В TCP- протоколі порти використовуються трохи інакшим способом, ніж в UDP. Для організації надійної передачі даних передбачено встановлення *логічного з'єднання* між двома прикладними процесами. В рамках *логічного з'єднання* здійснюється обов'язкове підтвердження правильності прийому для всіх переданих повідомлень, і при необхідності виконується повторна передача. Сегмент складається з заголовка і блока даних. Заголовок включає такі основні поля: Порт відправлення (SOURS PORT), 2 байта, ідентифікує процес-відправник; Порт призначення (DESTINATION PORT) 2 байта, ідентифікує процес - отримувач; Послідовний номер (SEQUENCE NUMBER) 4 байта, це номер байта, який визначає зсув сегмента відносно потоку даних; Номер, який підтверджено (ACKNOWLEDGEMENT NUMBER) 4 байта, це максимальний номер байта в отриманому сегменті, збільшений на 1, саме це значення використовується як квитанція; Довжина заголовка (HLEN) 4 біта, вказує довжину заголовка сегменту TCP в 32-бітовых словах; Резерв (RESERVED) 6 бітів, поле зарезервовано для подальшого використання; 6 службових (FLAG BITS) бітів, містять інформацію про тип сегмента: URG – термінове повідомлення; ACK - квитанція на

прийнятий сегмент; PSH - запит на відправку повідомлення без очікування заповнення буферу; RST - запит на відновлення сполучення; SYN – повідомлення для синхронізації лічильників переданих даних при встановленні сполучення; FIN – ознака останнього байту в потоці даних, що передаються. Вікно (WINDOW) 2 байта, розмір вікна в байтах (відповідає кількості кадрів, яку можна передати без отримання квитанцій); Контрольна сума (CHECKSUM) 2 байта, розраховується по сегменту; Ознака терміновості (URGENT POINTER) 2 байта, разом з URG вказує на кінець даних, які необхідно терміново прийняти, незважаючи на переповнення буферу. ***Стандартні команди аналізу трафіка в мережі.*** Ping – відповідь від вказаної машини:

ping [-t] [-a] [-n число] [-l розмір] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j список вузлів] | [-k список вузлів]] [-w інтервал] адрес машини -t - відправка пакетів на вказаний вузол до команди переривання;

-a - визначення адрес за іменами вузлів;

-n число - число запитів;

-l розмір - розмір буфера;

-f - заборона фрагментації пакета;

-i TTL - час життя пакета (поле "Time To Live");

-v TOS - тип служби (поле "Type Of Service");

-r число - запис маршруту для вказаного числа переходів;

-s число - штамп часу для указаного числа переходів;

-j список вузлів – вільний вибір маршруту по списку вузлів;

-k список вузлів - фіксований вибір маршруту по списку вузлів;

-w інтервал - інтервал очікування відповіді в мсек.

Tracert – виявлення послідовності вузлів, через які проходить IP-пакет на шляху до пункту свого призначення:

tracert [-d] [-h максЧисло] [-j список вузлів] [-w інтервал] ім´я_машини

-d - Без визначення адрес за іменами вузлів;

-h максЧисло - максимальне число переходів при пошуку вузла;

-j список вузлів - вільний вибір маршруту по списку вузлів;

-w інтервал - інтервал очікування відповіді в мсек.

Netstat - відображення статистики протоколу и поточних мережених сполучень TCP/IP:

netstat [-a] [-e] [-n] [-s] [-p им´я] [-r] [інтервал]

-a - відображення всіх підключень и портів;

-e - відображення статистики Ethernet;

-n - відображення адрес и номерів портів в числовому форматі;

-p им´я - відображення підключень для протоколу "им´я". Припустимі значення "им´я": tcp, udp або ip;

-r - відображення таблиці маршрутів;

-s - відображення статистики по протоколам.

інтервал - повторний вивід статистичних даних через указаний інтервал в секундах. Якщо параметр не задано, вивід здійснюється один раз.

Порядок виконання роботи

Контрольні запитання

Порядок виконання роботи

1. Відкрийте файл мережі, побудованої за топологією «зірка» під час виконання лабораторної роботи № 3.
2. Встановіть індикатор використання для 2 сполучень (вибір довільний), щоб виводити дані про коефіцієнт використання мережі в процентному вигляді і як прямокутну діаграму.
3. Запустить моделювання і спостерігайте, як змінюються показники індикатора. Виконайте 4-5 сеансів моделювання для різних значень розміру кадру та міжкадрового інтервалу (Global-Profiles-вибрати трафік-Edit, поля Transaction Size і Time between transactions).
4. Проаналізуйте залежність завантаженості мережі від розміру кадру та міжкадрового інтервалу:

Розмір кадру (байт)	Міжкадровий інтервал (сек)	Процент використання

5. Побудуйте мережу, яка складається з 2-х сегментів. Для цього використовуйте: (1) сегмент, побудований вами за топологією «зірка» під час виконання лабораторної роботи № 3; (2) сегмент, створений студентом вашої групи (виберіть ПІБ перед вами в списку групи), але поміняйте концентратори на комутатори. Розташуйте сегменти в окремих приміщеннях (вкладка Projects). З'єднайте комутатори маршрутизатором. Виберіть по 2 вузли в кожному сегменті і встановіть між ними міжсегментний трафік. Встановіть індикатори для моніторингу робочого навантаження для 4 сполучень:

№ сполучення	Перепускна здатність, байт/с

6. Оформити звіт по роботі.
7. Запустіть програму EtherDetect Packet Sniffer.
8. У вікні сполучень (ліве верхнє) виберіть TCP сполучення. Проаналізуйте, які вузли з'єднані через це сполучення, і яка кількість пакетів передана.
9. У вікні пакетів (праве верхнє) виберіть по черзі пакети двох типів (з даними і без них). Опишіть структуру обраних пакетів по дереву (нижнє ліве вікно), порівняйте з адресними даними в лаб. роботі № 2, проаналізуйте, які дані передаються.
10. Виконайте п. 2-4 для UDP сполучення.
11. Проаналізуйте, чим відрізняються UDP та TCP сполучення.
12. Виконайте команду tracert для двох вузлів, один з яких належить до мережі ТДТУ, другий – за її межами. Проаналізуйте маршрут (довжина і час проходження) і класи мереж, через які йдуть пакети.
13. Виконайте команду ping для цих вузлів з виводом маршруту. Порівняйте дані з п.7. Зверніть увагу на можливі зміни маршруту і поясніть їх.

14. За допомогою команди netstat виведіть таблицю маршрутизації та проаналізуйте її зміст.
15. Оформити звіт.
16. Звіт повинен включати: тему, мету роботи; короткий огляд теоретичних відомостей;
17. описати та проаналізувати структуру протокольних блоків даних, які спостерігалися;
18. зробити висновки щодо маршрутів передавання даних під час спостерігання за роботою мережі.
19.

Контрольні запитання

1. З якою метою канальний рівень розділено на два підрівня ?
2. Як аналізує місце призначення кадру міст/комутатор? Якого типу адреси при цьому використовуються?
3. Чим відрізняється робота концентратору від роботи моста/комутатору з точки зору доступу до середовища передавання?
4. Якого типу адреси використовує маршрутизатор?
5. Як реагує мережа на пошкодження сполучення до певного маршрутизатору?
6. Скільки рівнів має протокольний стек TCP/IP?
7. В чому ненадійність протоколу IP?
8. Яким чином міст/комутатор будує свою внутрішню таблицю?
9. Що відбувається, якщо під час роботи міста/комутатора зміниться конфігурація мережі, наприклад, будуть підключені нові ПК? Про що свідчить розмір адресної таблиці моста? Що буде, якщо вона переповниться?
10. Чи може бути в таблиці маршрутизації декілька записів про маршрутизатори default?
11. Чим відрізняється обробка поля MAC-адреси кадру в маршрутизаторі та комутаторі?

Вимоги до оформлення звітів по лабораторних роботах.

Звіт з лабораторної роботи оформлюється на аркушах формату А4, які заповнюються з однієї сторони. Текст повинен бути рукописним або друкованим на принтері. Використання кольорових чорнил дозволяється лише для ілюстративних матеріалів. Звіт до лабораторної роботи формується відповідно до змісту і повинен містити такі розділи:

- титульна сторінка;
- мета роботи;
- короткі теоретичні відомості;
- порядок виконання роботи;
- опис усіх етапів виконання роботи; опис отриманих результатів; висновки за результатами роботи.

Звіт зшивається з лівої сторони листів формату А4. Титульна сторінка звіту обов'язково друкується на принтері.

Організація, контроль виконання та захист лабораторних робіт. Лабораторні роботи виконуються кожним студентом згідно з графіком, який встановлений робочою програмою курсу. Графік виконання роботи студентом контролюється викладачем. Перед виконанням лабораторної роботи викладач опитує студентів, щоб визначити їх підготовленість до виконання роботи.

До виконання лабораторної роботи допускаються студенти, які мають теоретичні знання, що необхідні для виконання цієї роботи. Захист лабораторної роботи відбувається тільки за наявності належно оформленого звіту з цієї роботи. Лабораторна робота подається і захищається безпосередньо після її виконання згідно з графіком, який встановлений робочою програмою курсу. Роботи, які захищені із запізненням, зараховуються з мінімальною кількістю балів. При захисті роботи студент демонструє результати виконаної роботи та відповідає на контрольні запитання за темою лабораторної роботи.

Кожна лабораторна робота, що виконана і захищена за графіком, оцінюється за бальною системою, яка встановлена робочою програмою курсу.

Список використаної літератури

Базова

1. Steven Elliot. Modeling and Simulation of Computer Networks and Systems/ Steven Elliot, Benjamin Rearick, Punithavathy Govindaradjane. – Elsevier Inc, 2015. 924p

2. Коба О.В., Масловський Б.Г., Дрововозов В.І. Технології проєктування комп'ютерних систем: навч. посіб. – К.: Ін-т кібернетики ім. В.М. Глушкова НАН України, 2015. 500 с.

3. Шестопалов С.В. Дослідження та проектування комп'ютерних систем та мереж: конспект лекцій Одеська національна академія харчових технологій, 2017. 82с.

4. Рудницький В.М., Пантелєєва Н.М., Шувалова Л.А., Бабенко В.Г. Дослідження і проектування природно-надійних комп'ютерних систем: навч. посіб. – Черкаси: ЧДТУ, 2012. 187 с.

5. Савленко О. К., Якименко Н. М., Колодочкіна А. В., Сорокін В. В. Технології проектування комп'ютерних систем: навч. посіб - Кропивницький : Лисенко В.Ф., 2017. 308 с.

Допоміжна

1. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп'ютерні мережі [навчальний посібник] – Львів, «Магнолія 2006», 2013. 256 с.

2. Тарнавський Ю.А., Кузьменко І.М. Організація комп'ютерних мереж: підручник для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки». Київ: КПІ ім. Ігоря Сікорського, 2018. 259с.

3. Теслюк В.М. Моделі та інформаційні технології синтезу мікроелектромеханічних систем: Монографія. – Львів: Видавництво ПП "Вежа і Ко", 2018 – 192 с.

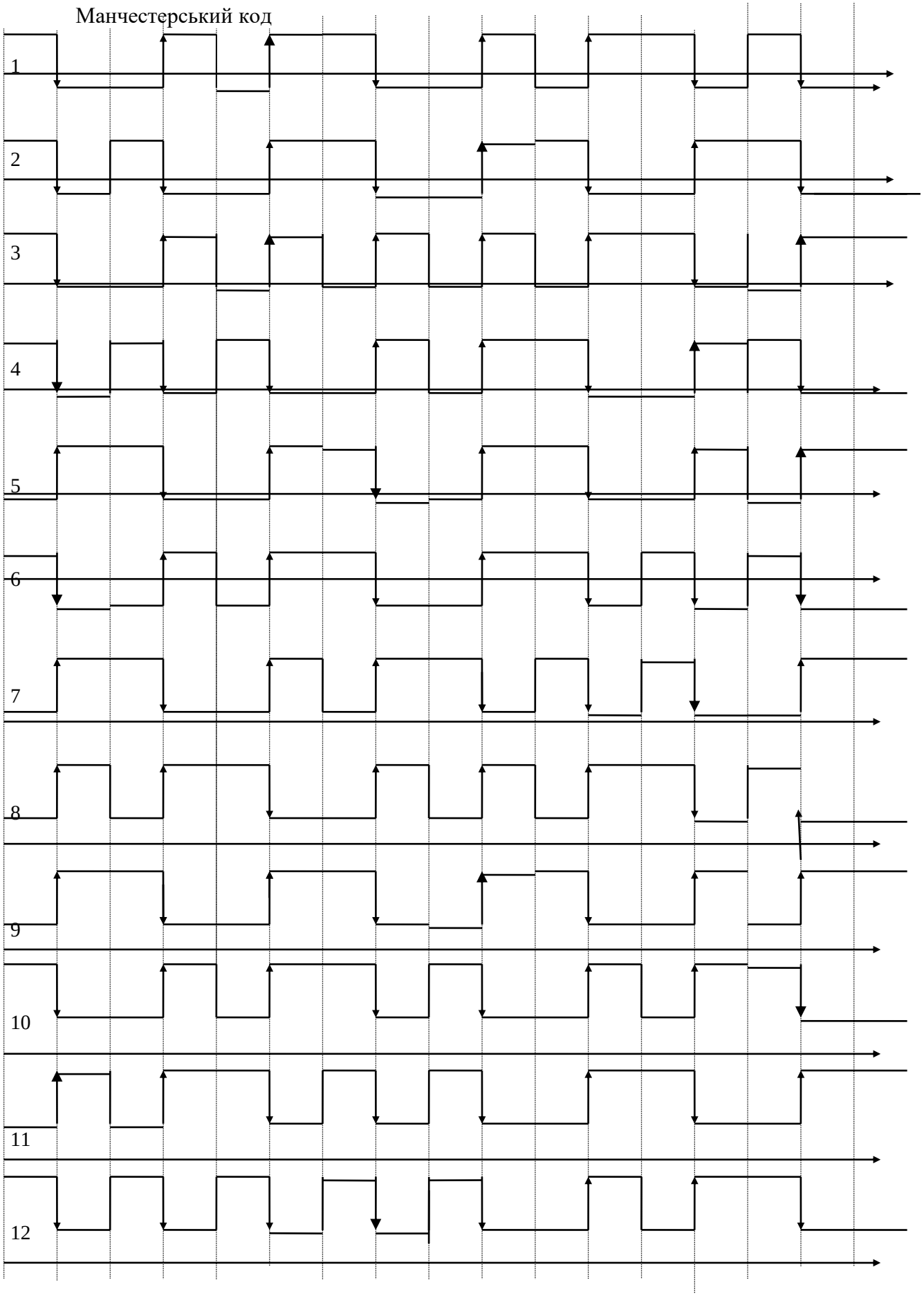
ДОДАТКИ

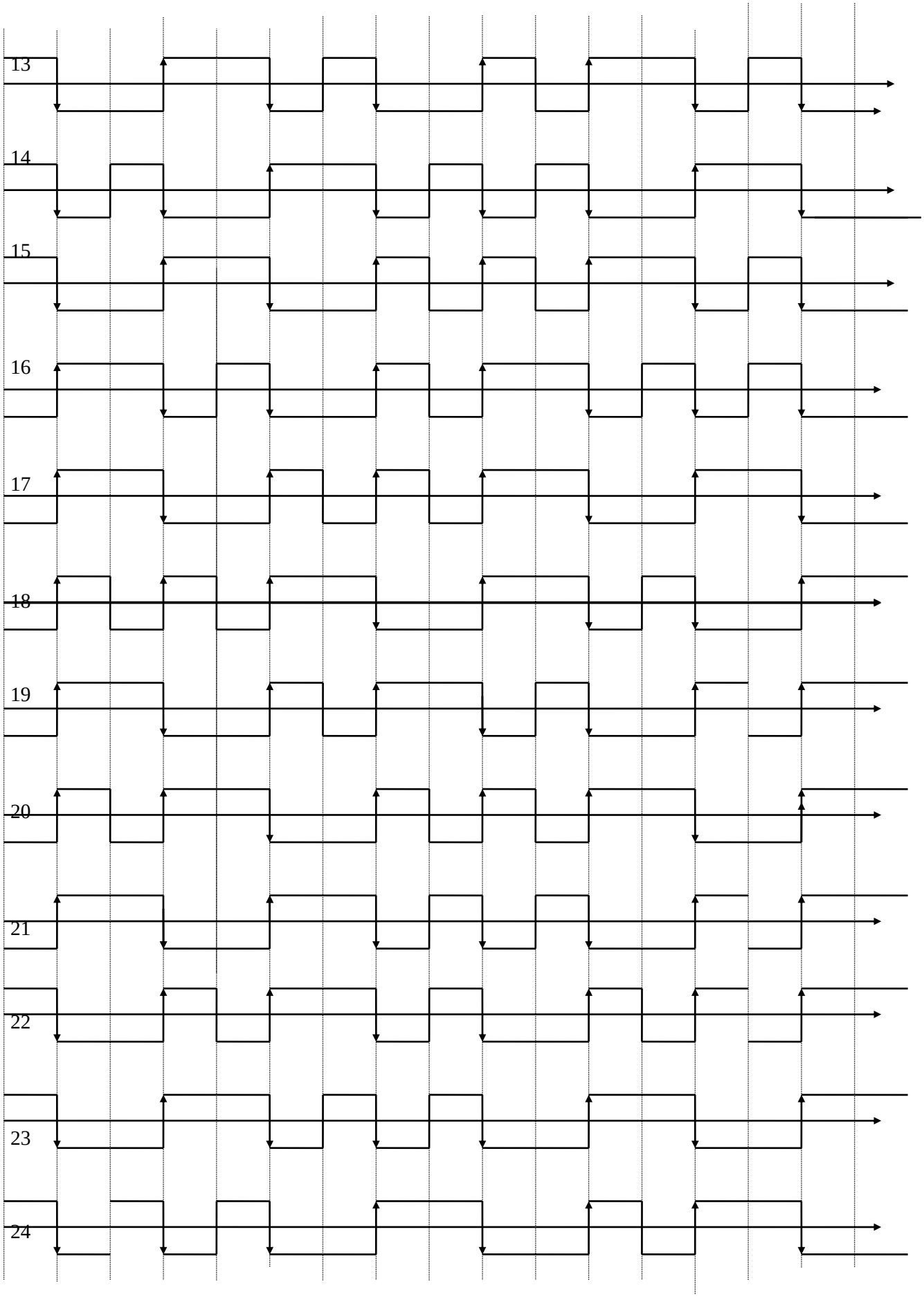
Додаток 1

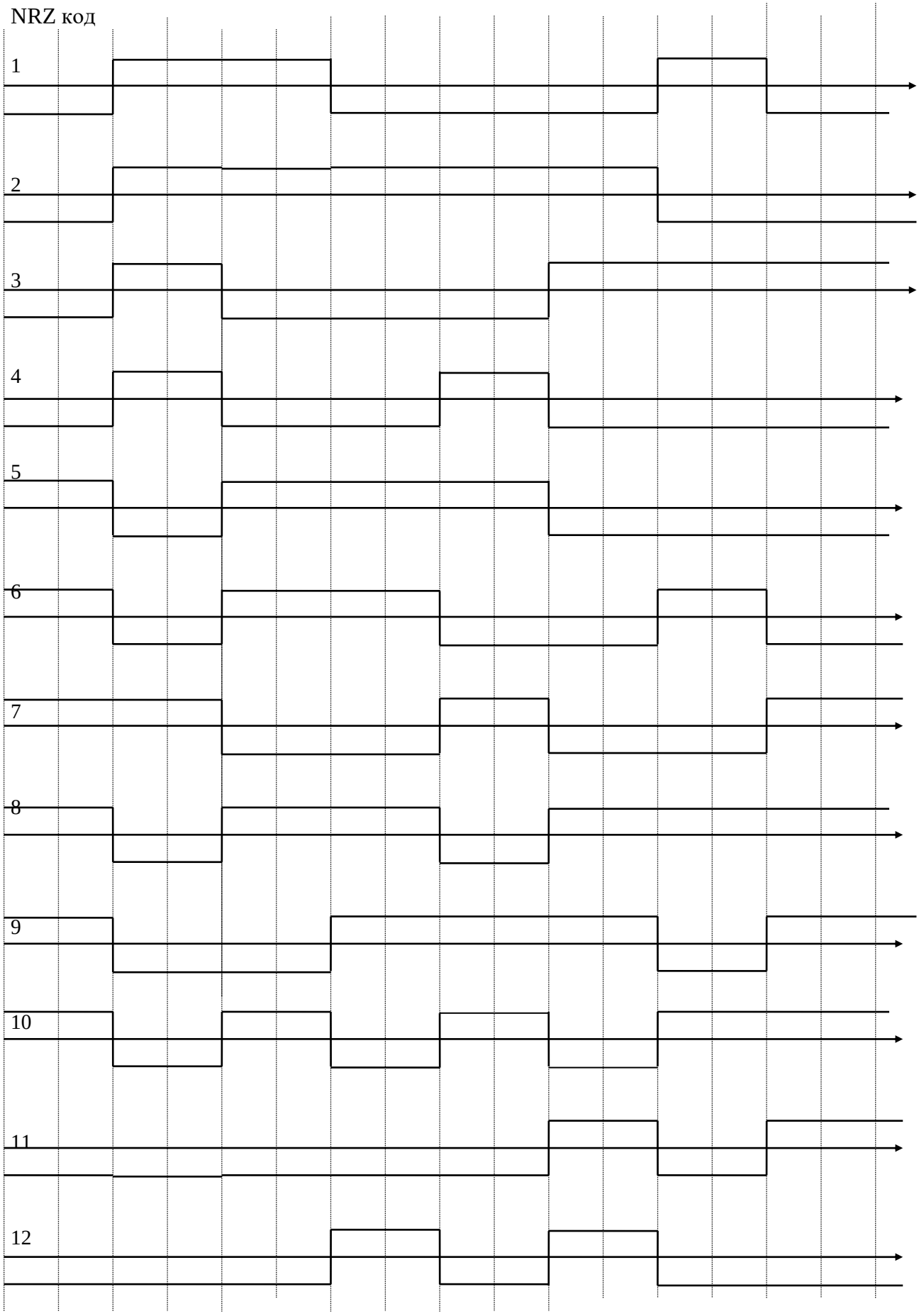
Індивідуальні завдання до лаболаторної роботи №6

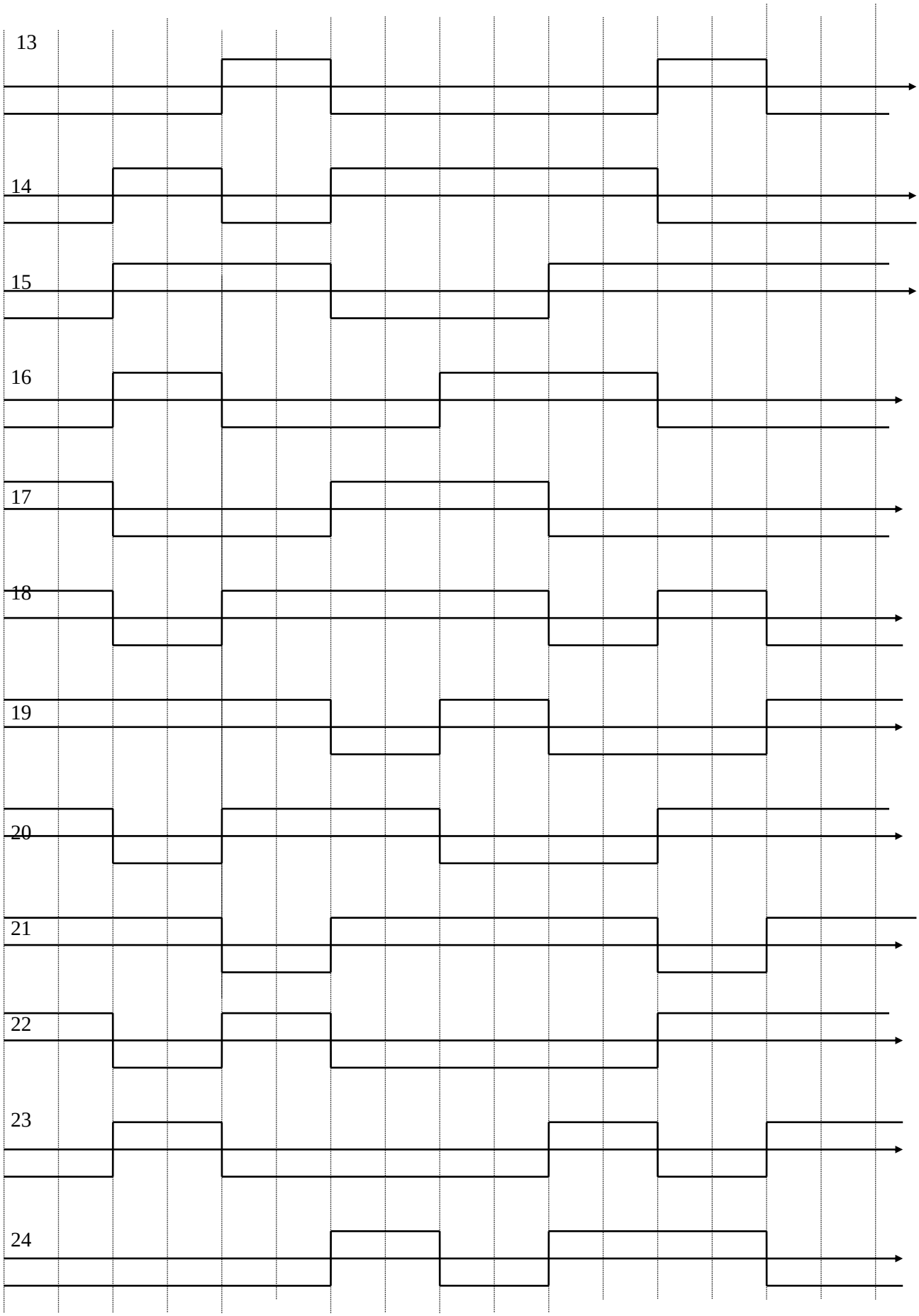
	Байт даних
1	1010 0110
2	0110 0010
3	1001 0001
4	1000 1001
5	0111 0110
6	0011 0011
7	1100 0011
8	1101 0111
9	0011 0111
10	1001 0110
11	1010 1011
12	0011 1101
13	1000 1000
14	1001 0111
15	0111 1000
16	1001 0101
17	0111 1110
18	1110 0001
19	1010 0101
20	1000 0000
21	1100 0011
22	0101 1100
23	0000 1000
24	1111 1010

Манчестерський код




13
14
15
16
17
18
19
20
21
22
23
24


NRZ код
1
2
3
4
5
6
7
8
9
10
11
12


13
14
15
16
17
18
19
20
21
22
23
24

Додаток 2

Індивідуальні завдання до лабораторної роботи №7

До завдання 4

	IP-адреса	Маска
1	198.65.12.67	255.255.255.240
2	201.28.244.19	255.255.255.224
3	194.44.250.63	255.255.255.192
4	201.28.244.19	255.255.255.240
5	194.44.250.63	255.255.255.224
6	198.65.12.67	255.255.255.192
7	194.44.250.63	255.255.255.240
8	198.65.12.67	255.255.255.224
9	201.28.244.19	255.255.255.192
10	129.54.94.97	255.255.128.0
11	143.126.44.53	255.255.192.0
12	133.19.224.240	255.255.224.0
13	143.126.44.53	255.255.128.0
14	133.19.224.240	255.255.192.0
15	129.54.94.97	255.255.224.0
16	133.19.224.240	255.255.128.0
17	129.54.94.97	255.255.192.0
18	143.126.44.53	255.255.224.0
19	129.54.94.97	255.255.240.0
20	143.126.44.53	255.255.240.0

До завдання 5

	Клас мережі	Кількість підмереж
1	C	2
2	C	4
3	C	8
4	C	30
5	C	20
6	B	100
7	B	50
8	B	200
9	B	850
10	B	30
11	B	150
12	B	500
13	B	1500
14	B	2000
15	B	300
16	B	400
17	B	700
18	B	10
19	C	12
20	C	10

Додаток 3

Індивідуальні завдання до лабораторної роботи №8

	Станції, що обмінюються даними із сервером	Станції, що посилають дані на сервер	Станції, що отримують дані від серверу	Станції, що обмінюються даними між собою	Станції, що друкують документи
1	2	-	3	2	2
2	3	1	1	2	1
3	3	-	2	3	1
4	4	-	1	3	1
5	1	1	3	3	2
6	1	2	2	3	2
7	1	3	1	4	3
8	1	4	-	4	1
9	2	1	2	2	2
10	2	2	1	2	1
11	2	3	-	2	2
12	3	1	1	2	1
13	3	2	-	2	1
14	4	1	-	2	-
15	1	3	1	3	3
16	1	2	2	2	3
17	1	1	3	2	3
18	1	-	4	3	2
19	2	2	1	2	1
20	2	1	2	2	1

	Станції, що обмінюються даними із сервером	Станції, що посилають дані на сервер	Станції, що отримують дані від серверу	Станції, що обмінюються даними між собою	Станції, що надсилають поштyt
1	2	-	3	2	2
2	3	1	1	2	1
3	3	-	2	3	1
4	4	-	1	3	1
5	1	1	3	3	2
6	1	2	2	3	2
7	1	3	1	4	3
8	1	4	-	4	1
9	2	1	2	2	2
10	2	2	1	2	1
11	2	3	-	2	2
12	3	1	1	2	1
13	3	2	-	2	1
14	4	1	-	2	-
15	1	3	1	3	3
16	1	2	2	2	3
17	1	1	3	2	3
18	1	-	4	3	2
19	2	2	1	2	1
20	2	1	2	2	1

Додаток 4

Індивідуальні завдання до лабораторної роботи №8

#	Кількість хабів	Сегмент1	Сегмент2	Сегмент3	Сегмент4	Сегмент5	Сегмент6
1	5	10Base-T 80 м	10Base-FL 1000 м	10Base-FB 700 м	10Base-FB 400 м	10Base-FL 200 м	10Base-2 150 м
2	5	10Base-T 50	10Base-FL 1200	10Base-FL 500	10Base-FB 400	10Base-FB 400	10Base-2 170
3	5	10Base-T 70	10Base-FB 800	10Base-FB 400	10Base-FL 350	10Base-FL 1000	10Base-2 160
4	5	10Base-T 60	10Base-FL 600	10Base-FB 700	10Base-FB 850	10Base-FL 550	10Base-2 110
5	5	10Base-T 90	10Base-FB 1100	10Base-FL 550	10Base-FB 400	10Base-FL 600	10Base-2 120
6	5	10Base-T 100	10Base-FB 750	10Base-FL 950	10Base-FB 350	10Base-FB 440	10Base-2 130
7	5	10Base-T 100	10Base-FL 900	10Base-FL 750	10Base-FB 350	10Base-FB 500	10Base-2 180
8	5	10Base-2 150	10Base-FB 700	10Base-FB 800	10Base-FL 400	10Base-FL 700	10Base-T 70
9	5	10Base-2 140	10Base-FB 500	10Base-FL 500	10Base-FB 650	10Base-FL 800	10Base-T 40
10	5	10Base-2 160	10Base-FL 800	10Base-FB 750	10Base-FL 500	10Base-FB 500	10Base-T 20
11	4	10Base-5 350	10Base-FL 600 м	10Base-FB 1000 м	10Base-FL 700 м	10Base-T 50 м	
12	4	10Base-5 200 м	10Base-FL 900 м	10Base-FB 800 м	10Base-FL 800 м	10Base-T 60 м	
13	4	10Base-5 300	10Base-FL 1000	10Base-FB 1000	10Base-FL 500	10Base-T 80	
14	4	10Base-5 400	10Base-FB 1000	10Base-FL 700	10Base-FL 600	10Base-T 60	
15	4	10Base-5 500	10Base-FB 1200	10Base-FL 400	10Base-FL 600	10Base-T 50	
16	4	10Base-5 350	10Base-FL 750	10Base-FL 600	10Base-FB 1100	10Base-T 90	
17	5	10Base-2 170	10Base-FB 600	10Base-FL 500	10Base-FB 500	10Base-FL 600	10Base-T 20
18	5	10Base-2 120	10Base-FB 700	10Base-FL 400	10Base-FB 600	10Base-FB 800	10Base-T 40
19	5	10Base-2 130	10Base-FL 600	10Base-FB 600	10Base-FL 500	10Base-FB 500	10Base-T 30
20	5	10Base-2 150	10Base-FL 700	10Base-FB 500	10Base-FB 800	10Base-FL 500	10Base-T 20