МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Інститут інженерії та інформаційних технологій

Кафедра комп'ютерної інженерії та електромеханіки

ДИПЛОМНА БАКАЛАВРСЬКА РОБОТА

на тему

АРХІТЕКТУРА РОЗПОДІЛЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОФІСУ КОМПАНІЇ

Виконав: студент групи БКІ-19

спеціальності 123 «Комп'ютерна інженерія»

Бутенко А.О.
(прізвище та ініціали)

Керівник проф. Злотенко Б.М.
(прізвище та ініціали)

Рецензент_____
(прізвище та ініціали)

Київ 2023

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
Інститут інженерії та інформаційних технологій
Кафедра комп'ютерної інженерії та електромеханіки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри КІЕМ
_____проф. Злотенко Б.М.
"_____" _____2023 року

З А В Д А Н Н Я
НА ДИПЛОМНУ БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ
Бутенку Артему Олександровичу .
(прізвище, ім'я, по батькові)

1. Тема дипломної бакалаврської роботи Архітектура розподіленої комп'ютерної мережі офісу компанії
Науковий керівник роботи д.т.н., проф. Злотенко Б.М
затверджені наказом вищого навчального закладу від _____ № _____
2. Строк подання студентом роботи 1 червня 2023 року
3. Вихідні дані до дипломної бакалаврської роботи: Провести аналіз та дослідження існуючих рішень по реалізації комп'ютерної мережі офісу. Описати етапи дослідження. Виконати обґрунтування та побудову комп'ютерної мережі розподіленого офісу на базі відомих моделей створення систем віддаленого офісу, яка забезпечить стабільну роботу та взаємодію будь-яких сервісів.
4. Зміст дипломної бакалаврської роботи (перелік питань, які потрібно розробити):
1. Особливості проектування локально-обчислювальних мереж. 2. Структурна організація підприємства. Висновки.
5. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної бакалаврської роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	01.02.2023	
2	Розділ 1. Особливості проектування локально-обчислювальних мереж	15.02.2023	
3	Розділ 2. Структурна організація підприємства	15.03.2023	
4	Висновки	10.05.2023	
5	Оформлення дипломної бакалаврської роботи (чистовий варіант)	20.05.2023	
6	Здача дипломної бакалаврської роботи на кафедру для рецензування (за 14 днів до захисту)	25.05.2023	
7	Перевірка дипломної бакалаврської роботи на наявність ознак плагіату (за 10 днів до захисту)	28.05.2023	
8	Подання дипломної бакалаврської роботи на затвердження завідувачу кафедри (за 7 днів до захисту)	05.06.2023	

Студент _____ Бутенко А.О. .
(підпис) (прізвище та ініціали)

Науковий керівник роботи _____ д.т.н., проф. Злотенко Б.М.
(підпис) (прізвище та ініціали)

Рецензент _____ _____.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Бутенко А. О. Архітектура розподіленої комп'ютерної мережі офісу компанії : дипломна бакалаврська робота за спеціальністю 123 Комп'ютерна інженерія / А. О. Бутенко; наук. кер. Б. М. Злотенко. – Київ : КНУТД, 2023. – 61 с.

Дипломна бакалаврська робота за спеціальністю 123 «Комп'ютерна інженерія», освітньою програмою «Комп'ютерна інженерія». – Київський національний університет технологій та дизайну, Київ, 2023 рік.

Дипломну бакалаврську роботу присвячено вдосконаленню вже існуючої локальної обчислювальної мережі малого підприємства "Форміка", що має відповідати сучасним науково-технічним вимогам. Поставлена у дипломній бакалаврській роботі мета досягається розв'язанням наступних задач:

1) виконати дослідження та аналіз особливостей проектування локально-обчислювальних мереж;

2) розробити структури ЛОМ і визначити склад використовуваних програмно-апаратних засобів.

Отримані результати і їх новизна – комп'ютерна мережа розподіленого офісу повинна забезпечити параметри якісної роботи для співробітників розподіленої віддаленої комп'ютерної мережі, що дозволить задавати необхідні параметри для якісної їх роботи.

Ключові слова: комп'ютерна мережа, передача інформаційних потоків, ефективність роботи, віддалений офіс.

ABSTRACT

Butenko A.O. Architecture of a distributed computer network of the company's office. – Manuscript.

Bachelor's thesis in specialty 123 "Computer Engineering", educational program "Computer Engineering". – Kyiv National University of Technologies and Design, Kyiv, 2023.

The bachelor thesis is devoted to the improvement of the already existing local computer network of the small enterprise "Formika", which should meet modern scientific and technical requirements. The goal set in the bachelor thesis is achieved by solving the following problems:

1) perform research and analysis of design features of local computing networks;

2) develop LOM structures and determine the composition of the software and hardware used.

The obtained results and their novelty - the computer network of a distributed office should provide quality work parameters for employees of a distributed remote computer network, which will allow setting the necessary parameters for their quality work.

Keywords: computer network, transfer of information flows, work efficiency, remote office.

ЗМІСТ

ВСТУП

У сучасному складному і багатоликому світі ні одну велику технологічну проблему не можна вирішити без переробки значних обсягів інформації і комунікаційних процесів. Поряд з енерго і фондо озброєністю сучасному виробництву необхідна й інформаційна озброєність, що визначає ступінь застосування прогресивних технологій. Особливе місце в організації нових інформаційних технологій займає комп'ютер. Телефонна мережа, а потім спеціалізовані мережі передачі даних послужили гарною основою для об'єднання комп'ютерів в інформаційно-обчислювальні мережі. Комп'ютерні мережі передачі даних є результатом інформаційної революції й у майбутньому зможуть утворити основний засіб комунікації.

Мережі з'явилися в результаті творчого співробітництва фахівців з обчислювальної техніки, техніки в'язку і є сполучною ланкою між базами даних, терміналами користувачів, комп'ютерами.

На сьогоднішній день у світі існує більш 130 мільйонів комп'ютерів і більш 80 % з них об'єднані в різні інформаційно-обчислювальні мережі від малих локальних мереж в офісах до глобальних мереж типу Internet, FidoNet, FREEnet і т.і. Всесвітня тенденція до об'єднання комп'ютерів у мережі обумовлена поруч важливих причин, таких як прискорення передачі інформаційних повідомлень, можливість швидкого обміну інформацією між користувачами, одержання і передача повідомлень (факсів, E-Mail листів, електронних конференцій і т.д.) не відходячи від робочого місця. Можливість миттєвого одержання будь-якої інформації з будь-якої точки земної кулі, а так само обмін інформацією між комп'ютерами різних фірм виробників працюючих під різним програмним забезпеченням.

Такі величезні потенційні можливості, що несе в собі обчислювальна мережа і той новий потенційний підйом, що при цьому випробує інформаційний комплекс, а так само значне прискорення виробничого процесу не дають нам право ігнорувати і не застосовувати їх на практиці.

Найчастіше виникає необхідність у розробці принципового рішення питання

по організації ІОМ (інформаційно-обчислювальної мережі) на базі вже існуючого комп'ютерного парку і програмного комплексу, що відповідає сучасним науково-технічним вимогам з урахуванням зростаючих потреб і можливістю подальшого поступового розвитку мережі в зв'язку з появою нових технічних і програмних рішень.

Магістральна мережа зв'язку України на сучасному етапі розвитку базується на використанні кабельних, радіорелейних і супутникових ліній зв'язку. Ці лінії доповнюють одна одну, забезпечуючи передачу великих потоків інформації будь-якого призначення на базі використання цифрових і аналогових систем передачі. Кабельні лінії зв'язку, що володіють високою захищеністю каналів зв'язку від атмосферних впливів і різних перешкод, експлуатаційним надійністю і довговічністю, є основною мережею зв'язку країни. По кабельних мережах передається до 75% всієї інформації.

В даний час найбільш ефективними є коаксіальні кабелі, що дозволяють передавати великі пучки зв'язку різного призначення. Швидкими темпами впроваджуються на мережах оптичні кабелі.

Вирішальними факторами при впровадженні нових систем зв'язки сьогодні є швидкість передачі інформації і забезпечення високої якості передачі.

Впровадження інтелектуальних мереж, ISDN, мереж рухливого зв'язку вимагає створення систем передачі інформації, що задовольняють найсучаснішим вимогам.

Нові вимоги до продуктивності мереж, пропоновані сучасними додатками, такими як мультимедіа, розподілені обчислення, системи оперативної обробки транзакцій, викликають нагальну потребу розширення відповідних стандартів. Звичний десятимегабітний Ethernet, довгий час займає чільні позиції, у всякому разі, дивлячись з України, активно витісняється більш сучасними й істотно більш швидкими технологіями передачі даних.

На ринку високошвидкісних (більш 100 Мбіт/с) мереж, пари років тому представлених лише мережами FDDI, сьогодні пропонується біля десятка різних технологій, що як розвивають вже існуючі стандарти, так і заснованих на

концептуально нових рішеннях. Серед них варто особливо виділити: старий добрий оптоволоконний інтерфейс FDDI, а також його розширений варіант, FDDI II, спеціально адаптований для роботи з інформацією мультимедіа, і CDDI, що реалізує FDDI на мідних кабелях. Усі версії FDDI підтримують швидкість обміну 100 Мбіт/с.

100Base X Ethernet, що представляє собою високошвидкісний Ethernet із множинним доступом до серед і виявленням колізій. Дана технологія - екстенсивний розвиток стандарту IEEE802.3.

100Base VG AnyLAN, нову технологію побудови локальних мереж, що підтримує формати даних Ethernet і Token Ring зі швидкістю передачі 100 Мбіт/сек по стандартних кручених парах і оптоволокну.

Gigabit Ethernet. Продовження розвитку мереж Ethernet і Fast Ethernet.

ATM, технологію передачі даних, працюючу як на існуючому кабельному устаткуванні, так і на спеціальних оптичних лініях зв'язку. Підтримує швидкості обміну від 25 до 622 Мбіт/сек з перспективою збільшення до 2,488 Гбіт/сек.

Fibre Channel, оптоволоконну технологію з комутацією фізичних з'єднань, призначену для додатків, що вимагають надвисоких швидкостей. Орієнтири - кластерні обчислення, організація взаємодії між суперкомп'ютерами і високошвидкісними масивами нагромаджувачів, підтримка з'єднань типу робоча станція - суперкомп'ютер. Декларовано швидкості обміну від 133 Мбіт до гігабіта в секунду (і навіть більш).

Привабливі, але далеко не ясні обриси технології FFOL (FDDI Follow on LAN), ініціативи ANSI, покликаної в майбутньому замінити FDDI з новим рівнем продуктивності 2,4 Гбайт/сек.

Отже, метою даного дипломного проекту є вдосконалення вже існуючої локальної обчислювальної мережі малого підприємства "Форміка", що має відповідати сучасним науково-технічним вимогам.

Дипломна бакалаврська робота складається зі вступу, 3 розділів, висновків, списку використаних джерел та додатків. Основний текст роботи викладений на 61 сторінках, містить 7 рисунків, 3 таблиць, список джерел з 17 найменувань.

РОЗДІЛ 1
ОСОБЛИВОСТІ ПРОЕКТУВАННЯ ЛОКАЛЬНО-ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

1.1. ЛОМ – розвиток, мета і задачі

Під ЛОМ розуміють спільне підключення декількох окремих комп'ютерних робочих місць (робітників станцій) до єдиного каналу передачі даних. Найпростіша мережа (англ. network) складається як мінімум із двох комп'ютерів, з'єднаних один з одним кабелем. Це дозволяє їм використовувати дані спільно. Усі мережі (незалежно від складності) ґрунтуються саме на цьому простому принципі. Народження комп'ютерних мереж було викликано практичними потребою – мати можливість для спільного використання даних.

Поняття локальна обчислювальна мережа – ЛОМ (англ. LAN – Local Area Network) відноситься до географічно обмеженого (територіально чи виробниче) апаратно-програмним реалізаціям, у яких кілька комп'ютерних систем зв'язані одна з одною за допомогою відповідних засобів комунікацій. Завдяки такому з'єднанню користувач може взаємодіяти з іншими робочими станціями, підключеними до цієї ЛОМ.

Існує два основних типи мереж: однорангові і мережі на основі сервера. В одноранговій мережі всі комп'ютери рівноправні: немає ієрархії серед комп'ютерів і немає виділеного (англ. dedicated) сервера. Як правило, кожен комп'ютер функціонує і як клієнт, і як сервер; інакше кажучи, немає окремого комп'ютера, відповідального за адміністрування всієї мережі. Усі користувачі самостійно вирішують, які дані на своєму комп'ютері зробити загальнодоступним по мережі. На сьогоднішній день однорангові мережі безперспективні. Якщо до мережі підключено більш 10 користувачів, то однорангова мережа, де комп'ютери виступають у ролі і клієнтів, і серверів, може виявитися недостатньо продуктивною. Тому більшість мереж використовує виділені сервери. Виділеним називається такий сервер, що функціонує тільки як сервер (крім функції чи клієнта робочої станції). Вони спеціально оптимізовані для швидкої обробки запитів від

мережних клієнтів і для керування захистом файлів і каталогів. Мережі на основі сервера стали промисловим стандартом, і саме вони будуть розглянуті в цій роботі. Існують і комбіновані типи мереж, що сполучають кращі якості одноранговых мереж і мереж на основі сервера.

У виробничій практиці ЛОМ грають дуже велику роль. За допомогою ЛОМ у систему поєднуються персональні комп'ютери, розташовані на багатьох вилучених робочих місцях, що використовують спільне устаткування, програмні засоби й інформацію. Робочі місця співробітників перестають бути ізольованими і поєднуються в єдину систему. Розглянемо переваги, одержувані при мережному об'єднанні персональних комп'ютерів у виді внутрівиробничої обчислювальної мережі.

– Поділ ресурсів.

Поділ ресурсів дозволяє ощадливо використовувати ресурси, наприклад, керувати периферійними пристроями, такими як друкувальні пристрої, зовнішні пристрої збереження інформації, модеми і т.д. із усіх підключених робочих станцій.

– Поділ даних.

Поділ даних надає можливість доступу і керування базами даних з периферійних робочих місць, що бідують в інформації.

– Поділ програмних засобів.

Поділ програмних засобів надає можливість одночасного використання централізованих, раніше встановлених програмних засобів.

– Поділ ресурсів процесора.

При поділі ресурсів процесора можливе використання обчислювальних потужностей для обробки даних іншими системами, що входять у мережу. Надана можливість полягає в тім, що на наявні ресурси не «накидаються» моментально, а тільки лише через спеціальний процесор, доступний кожної робочої станції.

– Багатокористувальницький режим.

Багатокористувальницькі вла*стивості системи* сприяють одночасному використанню централізованих прикладних програмних засобів, звичайно заздалегідь установлених на сервері додатка (англ. Application Server).

Усі ЛОМ працюють в одному стандарті прийнятому для комп'ютерних мереж – у стандарті Open Systems Interconnection (OSI).

1.2. Мережні топології

Топологія типу «зірка»

Концепція топології мережі у виді зірки прийшла з області великих ЕОМ, у якій головна машина одержує й обробляє всі дані з периферійних пристроїв як активний вузол обробки даних. Цей принцип застосовується в системах передачі даних, наприклад, в електронній пошті мережі RelCom. Вся інформація між двома периферійними робітничими місцями проходить через центральний вузол обчислювальної мережі.

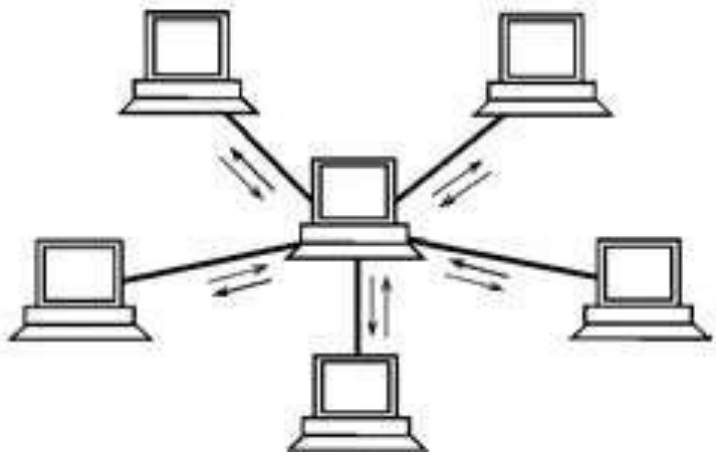

Рис. 1.1. Структура топології ЛОМ у виді «зірки»

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

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

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

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

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

Центральний вузол керування – файловий сервер реалізує оптимальний механізм захисту проти несанкціонованого доступу до інформації. Вся обчислювальна мережа може керуватися з її центра.

Кільцева топологія

При кільцевій топології мережі робочі станції зв’язані одна з іншої по колу, тобто робоча станція 1 з робочою станцією 2, робоча станція 3 з робочою станцією 4 і т.д. Остання робоча станція зв’язана з першою. Комунікаційний зв’язок замикається в кільце.

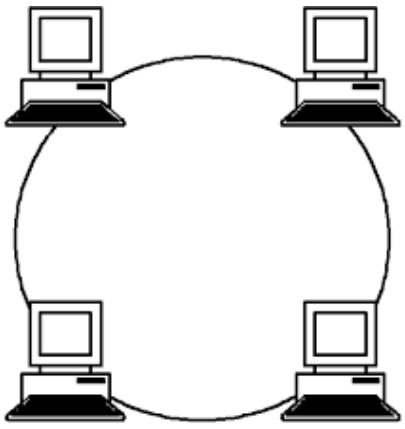

Рис. 1.2. Структура кільцевої топології ЛОМ

Прокладка кабелів від однієї робочої станції до іншої може бути досить складної і дорогою, особливо якщо географічне розташування робочих станцій

далеко від форми кільця (наприклад, у лінію).

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

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

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

Спеціальною формою кільцевої топології є логічна кільцева мережа. Фізично вона монтується як з'єднання зоряних топологій. Окремі зірки включаються за допомогою спеціальних комутаторів (англ. Hub – концентратор), що по-російському також іноді називають «хаб». У залежності від числа робочих станцій і довжини кабелю між робочими станціями застосовують активні чи пасивні концентратори. Активні концентратори додатково містять підсилювач для підключення від 4 до 16 робочих станцій. Пасивний концентратор є винятково розгалужувальним пристроєм (максимум на три робітничі станції). Керування окремою робочою станцією в логічній кільцевій мережі відбувається так само, як і в звичайній кільцевій мережі. Кожної робочої станції привласнюється відповідна їй адреса, по який передається керування (від старшого до молодшого і від самого молодшого до самого старшого). Розрив з'єднання відбувається тільки для нижчерозташованного вузла обчислювальної мережі, так що лише в рідких випадках може порушуватися робота всієї мережі.

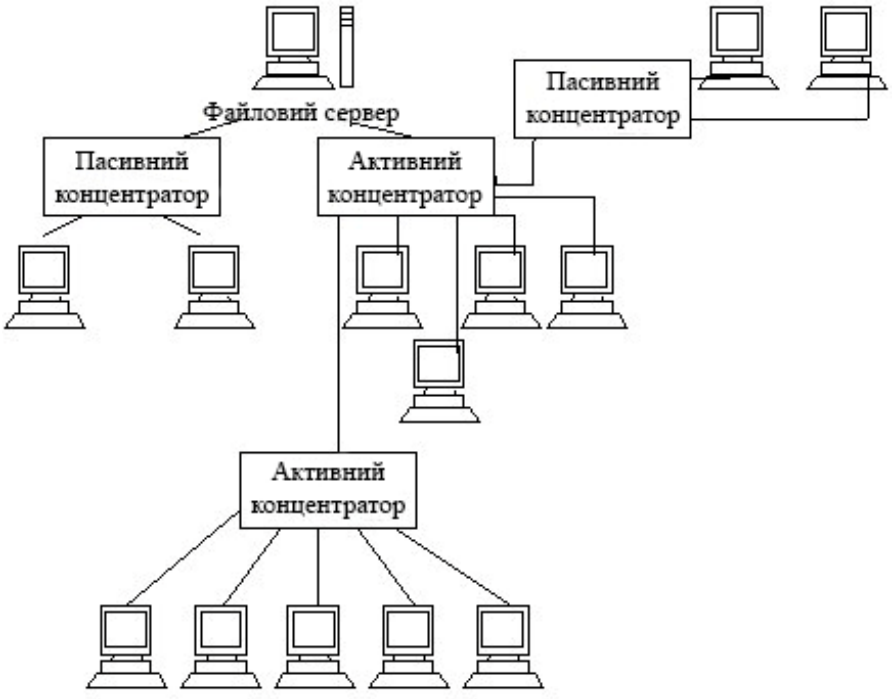

Рис. 1.3. Структура логічного кільцевого ланцюга ЛОМ

Шинна топологія

При шинній топології середовище передачі інформації представляється у формі комунікаційного шляху, доступного дня всіх робочих станцій, до якого вони усі повинні бути підключені. Усі робочі станції можуть безпосередньо вступати в контакт із будь-якою робочою станцією, що мається в мережі.

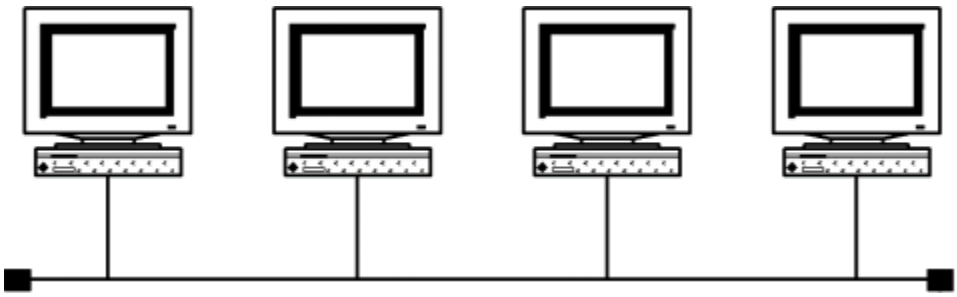

Рис. 1.4. Структура шинної топології ЛОМ

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

У стандартній ситуації для шинної мережі Ethernet часто використовують

тонкий чи кабель Cheapernet-кабель із трійниковим з’єднувачем. Відключення й особливе підключення до такої мережі вимагають розриву шини, що викликає порушення циркулюючого потоку інформації і зависання системи.

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

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

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

У ЛОМ із модульованої широко смужною передачею інформації різні робочі станції одержують, у міру потреби, частоту, на якій ці робочі станції можуть відправляти й одержувати інформацію. Дані, що пересилаються, модулюються на відповідних несучих частотах, тобто між середовищем передачі інформації і робітничими станціями знаходяться відповідно модеми для модуляції і демодуляції. Техніка широко смужних повідомлень дозволяє одночасно транспортувати в комунікаційному середовищі досить великий обсяг інформації. Для подальшого розвитку дискретного транспортування даних не грає ролі, яка первісна інформація подана в модем (аналогова чи цифрова), тому що вона все рівно надалі буде перетворена.

Основні характеристики трьох найбільш типових топологій обчислювальних мереж приведені в таблиці 1.1.

Таблиця 1.1

Основні характеристики топології обчислювальних мереж

Характеристики	Топології обчислювальних мереж		
	Зірка	Кільце	Шина
Вартість поширення	Незначна	Середня	Середня
Приєднання абонентів	Пасивне	Активне	Пасивне
Захист від відмовлень	Незначний	Незначний	Високий
Розміри системи	Будь-які	Будь-які	Обмежені
Захищеність від прослуховування	Гарна	Гарна	Незначна
Вартість підключення	Незначна	Незначна	Висока
Поведінка системи при високих навантаженнях	Гарна	Задовільна	Погана
Можливість роботи у реальному режимі часу	Дуже гарна	Гарна	Погана
Розведення кабелю	Гарне	Задовільне	Гарне
Обслуговування	Дуже гарне	Середнє	Середнє

Деревоподібна структура ЛОМ

Поряд з відомими топологіями обчислювальних мереж «кільце», «зірка» і «шина», на практиці застосовується і комбінована, на приклад деревовидна структура. Вона утвориться в основному у виді комбінацій вищезгаданих топологій обчислювальних мереж. Підстава дерева обчислювальної мережі розташовується в крапці, у якій збираються комунікаційні лінії інформації.

Обчислювальні мережі з деревоподібною структурою застосовуються там, де неможливо безпосереднє застосування базових мережних структур у чистому виді. Для підключення великого числа робочих станцій відповідно адаптерним платам застосовують мережні підсилювачі і/чи комутатори. Комутатор, що володіє

одночасно і функціями підсилювача, називають активним концентратором.

На практиці застосовують два їхні різновиди, що забезпечують підключення відповідно вісьмом чи шістнадцятьом ліній.

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

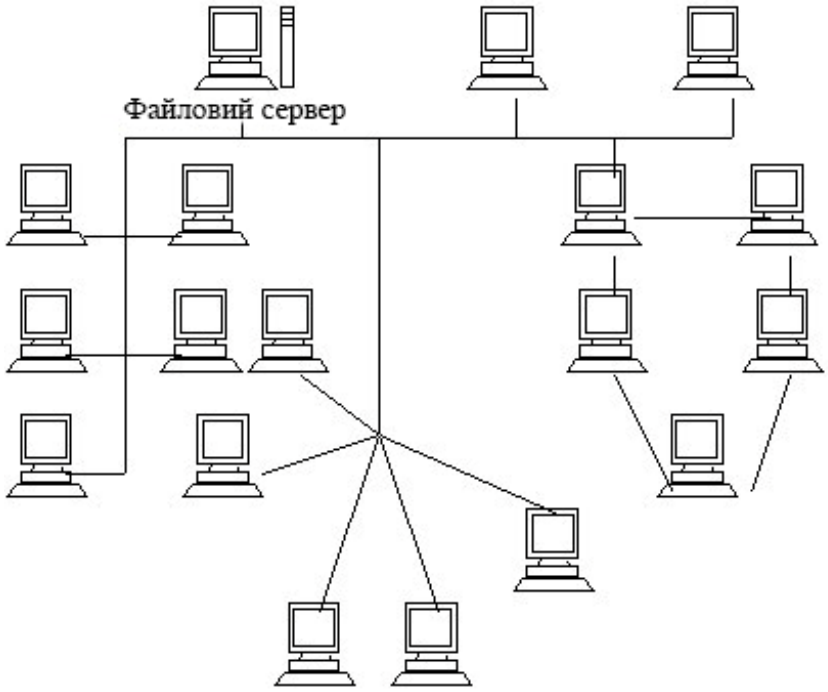

Рис. 1.5. Деревоподібна структура ЛОМ

1.3. Мережні пристрої, засоби комунікацій та сервіси

Міст (від англ. bridge – міст). Пристрій, що з’єднує дві чи кілька фізичних мереж і передає пакети з однієї мережі в іншу. Мости можуть фільтрувати пакети, тобто передавати в інші сегменти мережі чи тільки частину трафіка, на основі інформації канального рівня (MAC-адреса). Якщо адреса одержувача присутня у таблиці адрес моста, кадр передається тільки в той сегмент чи мережу, де знаходиться одержувач. Схожими пристроями є повторювачі (repeater),які просто передають електричні сигнали з одного кабелю в іншій і маршрутизатори (router),

які приймають рішення про передачу пакетів на основі різних критеріїв, заснованих на інформації мережного рівня. У термінології OSI міст є проміжною системою на рівні каналу передачі даних (Data Link Layer).

Шлюз (від англ. gateway - шлюз). Оригінальний термін Internet. Зараз для позначення таких пристроїв використовується термін маршрутизатор (router) чи більш точно маршрутизатор IP. У сучасному варіанті терміни "gateway" і "application gateway" використовуються для позначення систем, що виконують перетворення з одного природного формату в іншій. Прикладом шлюзу може служити перетворювач X.400 - RFC 822 electronic mail.

Вузол (від англ. node – вузол). Точка приєднання до мережі, пристрій, підключений до мережі.

Проксі (від англ. proxy – проксі). Механізм, за допомогою якого одна система представляє іншу у відповідь на запити протоколу. Proxy-системи використовуються в мережному керуванні, щоб позбутися від необхідності реалізації повного стека протоколів для таких простих пристроїв, як модеми.

Повторювач (від англ. repeater - повторювач). Пристрій, що передає електричні сигнали з одного кабелю в інший без маршрутизації чи фільтрації пакетів. У термінах OSI репітер являє собою проміжний пристрій фізичного рівня.

Хаб (від англ. Hub – хаб). Є обов’язковим (крім двукрапкової мережі) сполучним елементом мережі на крученій парі і засобом розширення топологічних, функціональних і швидкісних можливостей для будь-яких середовищ передачі. Найпростіші хаби є багато портовими повторювачами. Хаби можуть мати набір рознімань BNC, RJ-45, AUI, забезпечуючи вибір кабелю для передачі від джерела до приймача. До порту хаба можна підключити як окремий вузол, так і інший хаб. Хаби з набором різнотипних портів дозволяють поєднувати сегменти мереж з різними кабельними системами.

Stackable Hub - нарощуваний хаб - має спеціальні засоби з’єднання декількох хабів у стек, що виступає в ролі єдиного цілого. При цьому звичайно інтелектуальність одного хаба робить інтелектуальним весь стек. Відстань між хабами в стеці може бути коротким (локальний стік) і довгим, до сотень метрів

(розподілений стік, більш гнучкий елемент для оптимізації кабельної системи).

Switched Hub – комутуючий хаб - подальший розвиток технології Ethernet, підвищувальне продуктивність роботи мережі. У цьому випадку керування доступом до середовища практично переноситься з вузлів у центральний комутуючий пристрій, що забезпечує установлення віртуальних виділених каналів між парами портів - джерелами й одержувачами пакетів. Від вузлів-передавачів комутуючий хаб майже завжди готовий прийняти пакет або у свій буфер, або практично без затримки передати його в порт призначення (комутація з таким хабом двох комп'ютерів, що обмінюються "на лету" - On-the-fly Switching). Використовуючи обмін даними між собою через комутуючий хаб, комп'ютери не будуть завантажувати загальний трафік. Такі хаби також застосовуються для з'єднання між собою мереж Ethernet і Fast Ethernet.

Маршрутизатор (від англ. router - маршрутизатор). Система, що відповідає за прийняття рішень про вибір одного з декількох шляхів передачі мережного трафіку. Для виконання цієї задачі використовуються маршрутизуємі протоколи, що містять інформацію про мережі й алгоритми вибору найкращого шляху на основі декількох критеріїв, називаних метрикою маршрутизації ("routing metrics"). У термінах OSI маршрутизатор є проміжною системою Мережного рівня.

Designated Router (відзначений маршрутизатор). У кожній мережі, що має принаймні 2 маршрутизатори, мається відзначений маршрутизатор. Доповнений протоколом вітання (Hello Protocol),цей маршрутизатор генерує інформацію про стан каналу (link state advertisement) для мережі з множинним доступом і виконує ряд інших дій.

Neighboring Routers (сусідні маршрутизатори). Два маршрутизатори, підключені до однієї мережі. У мережах із множинним доступом, сусіди визначаються динамічно за допомогою протоколу OSPF Hello.

Трансівер (від англ. transceiver - трансівер). Приймач-передавач. Фізичний пристрій, що з'єднує інтерфейс хоста з локальною мережею, такий як Ethernet. Трансівери Ethernet містять електронні пристрої, що передають сигнал у кабель і знаходять колізії.

FTP: File Transfer Protocol. Використовуваний у Internet протокол (і програма) передачі файлів між хост - комп’ютерами. FTAM: File Transfer, Access, and Management. Вилучений сервіс і протокол OSI для файлів.

SMTP: Simple Mail Transfer Protocol. Протокол електронної пошти Internet.

Telnet. Протокол віртуального термінала в наборі протоколів Internet. Дозволяє користувачам одного хосту підключатися до іншого вилученому хосту і працювати з ним як через звичайний термінал.

Routing – маршрутизація. Процес вибору оптимального шляху для передачі повідомлення.

Ping: Packet internet groper. Програма, використовувана для перевірки приступності адресата шляхом передачі йому спеціального сигналу (ICMP echo request - запит відгуку ICMP) і чекання відповіді. Термін використовується як дієслово: "Ping host X to see if it is up!".

1.4. Протоколи, адресація й імена в Internet

Протоколами називають розподілені алгоритми, що визначають, яким образом здійснюється обмін даними між фізичними пристроями чи логічними об’єктами. Під сімейством протоколів TCP/IP у широкому змісті звичайно розуміють весь набір реалізацій стандартів RFC (Requests For Comments), а саме:

- Internet Protocol (IP);
- Address Resolution Protocol (ARP);
- Internet Control Message Protocol (ICMP);
- User Datagram Protocol (UDP);
- Transport Control Protocol (TCP);
- Routing Information Protocol (RIP);
- Telnet;
- Simple Mail Transfer Protocol (SMTP);
- Domain Name System (DNS) і інші.

Загальним і основним елементом цього сімейства є IP протокол. Усі

протоколи Internet є відкритими і доступними. Більшість специфікацій протоколів доступно з RFC. Необхідно відзначити, що наприкінці 80-х років спостерігався справжній бум, викликаний розробкою Міжнародної організації по стандартизації комунікаційних протоколів - ISO (International Standard Organization). Розроблена ISO специфікація, названа моделлю взаємодії відкритих систем (OSI - Open Systems Interconnection), заполонила наукові публікації. Здавалося, що ця модель займе перше місце і відтіснить широко поширився TCP/IP. Але цього не відбулося. Однією з причин цього з'явилося ретельне пророблення протоколів TCP/IP, їхня функціональність і відкритість до нарощування функціональних можливостей, хоча до дійсного часу досить очевидно, що вони мають і безліч недоліків.

Кожен рівень моделей використовує визначений формат повідомлень. При переході повідомлення з вищого рівня на нижчий воно формується за правилами нижчого рівня і забезпечується заголовком, тобто повідомлення закладається в конверт. Фізичний і канальний рівень моделі TCP/IP аналогічні відповідним рівням OSI:

– на фізичному рівні здійснюється фізичне з'єднання між комп'ютерною системою і фізичним середовищем передачі. Він визначає розташування кабельних контактів, напруги і т.п. Одиницею даних на цьому рівні є біт;

– на канальному рівні здійснюється пакування даних для передачі і розпакування для прийому. Одиниця даних на цьому рівні називається фреймом;

– на мережному рівні здійснюється маршрутизація даних у мережі. Одиницею даних цього рівня є датаграмма.

Адресація в Internet

Концепція протоколу IP представляє мережу як безліч комп'ютерів (хостів - hosts), підключених до деякої інтермережі. Інтермережа, у свою чергу, розглядається як сукупність фізичних мереж, зв'язаних маршрутизаторами. Фізичні мережі представляють із себе комунікаційні системи довільної фізичної природи. Фізичні об'єкти (хости, маршрутизатори, підмережі) ідентифікуються за допомогою спеціальних так званих IP-адрес. Кожна IP-адреса являє собою 32-бітовий ідентифікатор. Прийнято записувати IP-адреси у виді 4-х десяткових чисел,

розділених точками. Кожна адреса є сукупністю двох ідентифікаторів: мережі - NetID, і хосту - HostID. Усі можливі адреси розділені на 5 класів. Класи мереж визначають як можливу кількість цих мереж, так і число хостів у них. Практично використовуються тільки перші три класи:

Клас А визначений для мереж з числом хостів до 16777216. Під поле NetID відведено 7 біт, під поле HostID - 24 біта.

Клас В використовується для середньомасштабових мереж (NetID - 14 біт, HostID - 16 біт). У кожній такій мережі може бути до 65 536 хостів.

Клас С застосовується для невеликих мереж (NetId - 21 біт, HostID - 8 біт) з числом хостів до 255.

Служба імен доменів Internet

В часи, коли ARPANET складалася з досить невеликого числа хостів, усі вони були перераховані в одному файлі (***HOSTS.TXT***). Цей файл зберігався в мережному інформаційному центрі Стенфордського дослідницького інституту (SRI-NIC - Stanford Research Institute Network Information Center). Кожен адміністратор сайта посилав у SRI-NIC доповнення і зміни, що здійснилися в конфігурації його системи. Періодично адміністратори переписували цей файл із SRI-NIC у свої системи, де з нього генерували файл /etc/hosts. З ростом ARPANET це стало надзвичайно скрутним. З переходом на TCP/IP удосконалювання цього механізму стало необхідністю, оскільки, наприклад, якийсь адміністратор міг привласнити новій машині ім’я вже існуючої. Рішенням цієї проблеми з’явилося створення доменів, чи локальних повноважень, у яких адміністратор міг привласнювати імена своїм машинам і керувати даними адресації у своєму домені.

Служба імен доменів - DNS (Domain Name Service) одержує і надає інформацію про хости мережі. Під доменом розуміється безліч машин, що адмініструються і підтримуються як одне ціле. Можна сказати, що всі машини локальної мережі складають домен у більшій мережі, хоча можна і розділити машини локальної мережі на трохи доменів. При підключенні до Internet домен повинний бути пойменований відповідно до угоди про імена Internet. Internet організований як ієрархія доменів. Кожен рівень ієрархії є галуззю рівня ***root***. На

кожнім рівні Internet знаходиться сервер імен - машина, що містить інформацію про машини нижчого рівня і відповідність їхніх імен IP-адресам.

Домен кореневого рівня формується NIC. Домени верхнього рівня мають наступні галузі: ***gov*** (будь-які урядові заклади), ***edu*** (освітні установи), ***arpa*** (ARPANET), ***com*** (комерційні підприємства), ***mil*** (військові організації), ***org*** (інші організації, що не попадають у попередні). Починаючи з весни 1997 IAHC додав ще 7 доменів: ***firm*** (фірми і напрямки їх діяльності), ***store*** (торгові фірми), ***web*** (об'єкти, зв'язані з WWW), ***arts*** (об'єкти, зв'язані з культурою і мистецтвом), ***rec*** (розваги і відпочинок), ***info*** (інформаційні послуги) і ***nom*** (інші). Ці імена відповідають типам мереж, що складають дані домени.

Члени організацій на другому рівні керують своїми серверами імен.

Домени локального рівня адмініструються організаціями. Локальні домени можуть складатися з одного хосту чи включати не тільки безліч хостів, але і свої піддомени. Кожен вузол дерева є домен, що обран як мітка. Ім'я домену утвориться конкатенацією ("склеюванням") усіх міток доменів від кореневого до поточного, перерахованих праворуч ліворуч і розділених точками. Наприклад, в імені ***kernel.generic.edu*** : ***edu*** - відповідає верхньому рівню, ***generic*** - показує поддомен edu, ***kernel*** - є ім'ям хоста.

Число рівнів доменів не обмежено. Імена доменів є іншим засобом досягнення цільового хосту. У Internet можна зустріти імена типу ***netcom.com*** чи ***spry.com***. Ці імена є іменами доменів, і вони зареєстровані подібним же чином.

1.5. Мережа FDDI

1.5.1. Принцип дії мережі FDDI

Мережа FDDI являє собою волоконно - оптичне маркерне кільце зі швидкістю передачі даних 100 Мбіт/сек. Стандарт FDDI був розроблений комітетом X3T9.5 Американського національного інституту стандартизації (ANSI). Мережі FDDI підтримуються усіма ведучими виробниками мережного устаткування. В даний час комітет ANSI X3T9.5 перейменований у X3T12.

Використання як середовища поширення волоконної оптики дозволяє

істотно розширити смугу пропущення кабелю і збільшити відстані між мережними пристроями.

Порівняємо пропускну здатність мереж FDDI і Ethernet при багато користувальницькому доступі. Припустимий рівень утилізації мережі Ethernet лежить у межах 35% (3.5 Мбіт/сек) від максимальної пропускної здатності (10 Мбіт/сек), у противному випадку імовірність виникнення колізій стає не занадто високою і пропускна здатність кабелю різко знизиться. Для мереж FDDI припустима утилізація може досягати 90-95% (90-95 Мбіт/сек). Таким чином, пропускна здатність FDDI приблизно в 25 разів вище.

Детермінірована природа протоколу FDDI (можливість прогнозування максимальної затримки при передачі пакета по мережі і можливість забезпечити гарантовану смугу пропущення для кожної зі станцій) робить його ідеальним для використання в мережних АСУ в реальному часі й у додатках, критичних вчасно передачі інформації (наприклад, для передачі відео і звукової інформації).

Багато що зі своїх ключових властивостей FDDI успадкувала від мережі Token Ring (стандарт IEEE 802.5). Насамперед - це кільцева топологія і маркерний метод доступу до середовища. Маркер - спеціальний сигнал, що обертається по кільцю. Станція, що одержала маркер, може передавати свої дані. Однак FDDI має і ряд принципових відмінностей від Token Ring, що робить її більш швидкісним протоколом. Наприклад, змінений алгоритм модуляції даних на фізичному рівні. Token Ring використовує схему манчестерського кодування, що вимагає подвоєння смуги переданого сигналу щодо переданих даних. У FDDI реалізований алгоритм кодування "п’ять з чотирьох" - 4B/5B, що забезпечує передачу чотирьох інформаційних біт п’ятьма переданими бітами. При передачі 100 Мбіт інформації в секунду фізично в мережу транслюється 125 Мбіт/сек, замість 200 Мбіт/сек, що треба було б при використанні манчестерського кодування.

Оптимізовано і керування доступу до середовища (Medium Access Control - VAC). У Token Ring воно засновано на побітовій основі, а в FDDI на рівнобіжній обробці групи з чотирьох чи восьми переданих бітів. Це знижує вимоги до швидкодії устаткування.

Фізично кільце FDDI утворене волоконно - оптичним кабелем із двома світлопроводящими волокнами. Одне з них утворить первинне кільце (primary ring), є основним і використовується для циркуляції маркерів даних. Друге волокно утворить вторинне кільце (secondary ring), є резервним і в нормальному режимі не використовується.

Станції, підключені до мережі FDDI, підрозділяються до двох категорій.

Станції класу А мають фізичні підключення до первинного і вторинного кілець (Dual Attached Station - дворазово підключена станція);

Станції класу В мають підключення тільки до первинного кільця (Single Attached Station - однократно підключена станція) і підключається тільки через спеціальні пристрої, називані концентраторами.

Порти мережних пристроїв, що підключаються до мережі FDDI, класифікуються на 4 категорії: А порти, S порти, М порти і S порти. Портом А називається порт, що приймає дані з первинного кільця і передавальний їх у вторинне кільце. Порт S - це порт, що приймає дані з вторинного кільця і передавальний їх у первинне кільце. М (Master) і S (Slave) порт передають і приймають дані з того самого кільця. М порт використовується на концентраторі для підключення Single Attached Station через S порт.

Стандарт X3T9.5 має ряд обмежень. Загальна довжина подвійного волоконно - оптичного кільця - до 100 км. До кільця можна підключити до 500 станцій класу А. Відстань між вузлами при використанні багатомодового волоконно - оптичного кабелю - до 2 км, а при використанні одномодового кабелю визначається в основному параметрами волокна і приймально-передавальним устаткуванням (може досягати 60 і більш км).

1.5.2. Топологія

Застосовувані при побудові ЛОМ механізмів контролю потоків є топологіческі залежним, що унеможливлює одночасне використання Ethernet IEEE 802.x, FDDI ANSI, Token Ring IEEE 802.6 і інших у межах єдиного середовища поширення. Незважаючи на той факт, що Fibre Channel якоюсь мірою може

нагадувати настільки звичні нам ЛОМ, його механізм контролю потоків ніяк не зв’язаний з топологією середовища поширення і базується на зовсім інших принципах.

Кожен N_порт при підключенні до ґрат Fibre Channel проходить через процедуру реєстрації (log-in) і одержує інформацію про адресний простір і можливості всіх інших вузлів, на підставі чого стає ясно, з ким з них він зможе працювати і на яких умовах. А тому що механізм контролю потоків у Fibre Channel є прерогативою самих ґрат, то для вузла зовсім неважливо, яка топологія лежить у її основі.

Найпростіша схема, заснована на послідовному дуплексному з’єднанні двох N_портів із взаємоприйнятими параметрами фізичного з’єднання й однакових класів сервісу. Один з вузлів одержує адреса 0, а іншої – 1.

По суті, така схема може розглядатися як окремий випадок кільцевої топології, де немає необхідності в розмежуванні доступу шляхом арбітражу. Як типовий приклад такого підключення можемо привести найбільше що часто зустрічається з’єднання сервера з зовнішнім RAID масивом.

Петля з арбітражним доступом

Класична схема підключення до 126 портів, з якою все й починалося, якщо судити по абревіатурі FC-AL. Будь-які два порти в кільці можуть обмінюватися даними за допомогою дуплексного з’єднання точно так само, як і у випадку "точка-точка". При цьому всі інші виконують роль пасивних повторювачів сигналів рівня FC-1 з мінімальними затримками, у чому, мабуть, полягає одне з основних переваг технології FC-AL перед SSA. Справа в тім, що адресація в SSA побудована на знанні кількості проміжних портів між відправником і одержувачем, тому адресний заголовок кадру SSA містить лічильник переходів (hop count). Кожен порт, що зустрічається на шляху кадру, зменшує вміст цього лічильника на одиницю і після цього заново генерує CRC, тим самим істотно збільшуючи затримку передачі між портами. Для запобігання цього небажаного ефекту розроблювачі FC-AL зволіли використовувати абсолютну адресацію, що в підсумку дозволило ретранслювати кадр у незмінному виді і з мінімальної латентністю.

Передане з метою арбітражу слово ARB не розуміється і не використовується звичайними N_портами, тому при такій топології додаткові властивості вузлів позначаються, як NL_порт.

Основною перевагою петлі з арбітражним доступом є низька собівартість у перерахуванні на кількість підключених пристроїв, тому найбільше часто вона використовується для об'єднання великої кількості твердих дисків з дисковим контролером. На жаль, вихід їх будуючи будь-якого NL_ чи порту сполучного кабелю розмикає петлю і робить її непрацездатної, через що в чистому виді така схема зараз уже не вважається перспективною. Крім того, додавання чи видалення NL_порту викликає досить тривалий процес ініціалізації LIP (Loop Initialization Process), що може вимірятися десятками секунд при великій кількості підключених вузлів.

В даний час найбільше поширення одержала схема організації петлі за допомогою активних концентраторів, що вміють ізолювати ушкоджений NL_порт шляхом автоматичного підключення внутрішнього резервного шляху.

Ще одним вагомим доводом на користь використання концентратора є розширені можливості керування і більш зручна схема міжпортових з'єднань.

Комутуємі грати

Найбільш перспективна топологія, що дозволяє перебороти всі обмеження петлі з арбітражним доступом і представити кожному N_порту виділений канал FC-AL. Як уже зрозуміло з назви, в основу ґрат покладений Fibre Channel комутатор з F_портами (Fabric ports).

Приблизно так само, як і в ЛОМ, до портів комутатора можуть підключатися інші комутатори чи концентратори, у такому випадку це буде називатися з'єднанням через E_ порт чи FL_порт відповідно.

1.5.3. Синхронна й асинхронна передача

Підключені до мережі FDDI станції можуть передавати свої дані в кільце в двох режимах - у синхронному й в асинхронному.

Синхронний режим улаштований у такий спосіб. У процесі ініціалізації

мережі визначається очікуваний час обходу кільця маркером - TTRT (Target Token Rotation Time). Кожній станції, що захопила маркер, приділяється гарантований час для передачі її даних у кільце. Після закінчення цього часу станція повинна закінчити передачу і послати маркер у кільце.

Кожна станція в момент посилки нового маркера включає таймер, що вимірює часовий інтервал до моменту повернення до неї маркера - TRT (Token Rotation Timer). Якщо маркер повернеться до станції раніш очікуваного часу обходу TTRT, то станція може продовжити час передачі своїх даних у кільце і після закінчення синхронної передачі. На цьому заснована асинхронна передача. Додатковий часовий інтервал для передачі станцією буде дорівнює різниці між очікуваним і реальним часом обходу кільця маркером.

З описаного вище алгоритму видно, що якщо одна чи кілька станцій не мають достатнього обсягу даних, щоб цілком використовувати часовий інтервал для синхронної передачі, те невикористана ними смуга пропущення відразу стає доступної для асинхронної передачі іншими станціями.

1.5.4. Кабельна система

Підстандарт FDDI PMD (Physical medium-dependent layer) у якості базової кабельної системи визначає багатомодовий волоконно - оптичний кабель з діаметром світловодів 62.5/125 мкм. Допускається застосування кабелів з іншим діаметром волокон, наприклад: 50/125 мкм. Довжина хвилі - 1300 нм.

Середня потужність оптичного сигналу на вході станції повинна бути не менш -31 dBm. При такій вхідній потужності імовірність помилки на біт при ретрансляції даних станцією не повинна перевищувати $2.5*10^{-10}$. При збільшенні потужності вхідного сигналу на 2 dBm, ця імовірність повинна знизитися до 10^{-12} .

Максимально припустимий рівень утрат сигналу в кабелі стандарт визначає рівним 11 dBm. Підстандарт FDDI SMF-PMD (Single-mode fiber Physical medium-dependent layer) визначає вимоги до фізичного рівня при використанні одномодового волоконно - оптичного кабелю. У цьому випадку як передавальний елемент звичайно використовується лазерний світлодіод, а дистанція між

станціями може досягати 60 і навіть 100 км.

FDDI модулі для одномодового кабелю випускає, наприклад, фірма Cisco Systems для своїх маршрутизаторів Cisco 7000 і AGS+. Сегменти одномодового і багатомодового кабелю в кільці FDDI можуть чергуватися. Для названих маршрутизаторів фірми Cisco мається можливість вибору модулів із усіма чотирма комбінаціями портів: багатомодовий - багатомодовий, багатомодовий - одномодовий, одномодовий - багатомодовий, одномодовий - одномодовий.

Фірма Cabletron Systems Inc. випускає повторювачі Dual Attached - FDR-4000, що дозволяють підключити одномодовий кабель до станції класу А с портами, призначеними для роботи на багатомодовому кабелі. Ці повторювачі дають можливість збільшити відстань між вузлами FDDI кільця до 40 км.

Підстандарт фізичного рівня CDDI (Copper Distributed Data Interface - розподілений інтерфейс даних по мідних кабелях) визначає вимоги до фізичного рівня при використанні екранованої (IBM Type 1) і не екранованої (Category 5) кручених пар. Це значно спрощує процес інсталяції кабельної системи й знижує вартість, мережні адаптери й устаткування концентраторів. Відстані між станціями при використанні кручених пар не повинні перевищувати 100 км.

Фірма Lannet Data Communications Inc. випускає FDDI модулі для своїх концентраторів, що дозволяють працювати в стандартному режимі, чи коли вторинне кільце використовується тільки з метою відказостійкості при обриві кабелю, чи в розширеному режимі, коли вторинне кільце теж використовується для передачі даних. В другому випадку смуга пропущення кабельної системи розширюється до 200 Мбіт/сек.

1.5.5. Підключення устаткування до мережі FDDI

Є два основних способи підключення комп’ютерів до мережі FDDI: безпосередньо, а також і через чи мости маршрутизатори до мереж інших протоколів.

Безпосереднє підключення

Цей спосіб підключення використовується, як правило, для підключення до

мережі FDDI файлових, архіваційних і інших серверів, середніх і великих ЕОМ, тобто ключових мережних компонентів, що є головними обчислювальними центрами, що надають сервіс для багатьох користувачів і потребуючих високих швидкостей вводу - виводу по мережі.

Аналогічно можна підключити і робочі станції. Однак, оскільки мережні адаптери для FDDI дуже дороги, цей спосіб застосовується тільки в тих випадках, коли висока швидкість обміну по мережі є обов'язковою умовою для нормальної роботи додатка. Приклади таких додатків: системи мультимедіа, передача відео і звукової інформації.

Для підключення до мережі FDDI персональних комп'ютерів застосовуються спеціалізовані мережні адаптери, що звичайним образом вставляються в один з вільних слотів комп'ютера. Такі адаптери виробляються фірмами: 3Com, IBM, Microdyne, Network Peripherials, SysKonnect і ін. На ринку маються карти під усі розповсюджені шини - ISA, EISA і Micro Channel; є адаптери для підключення станцій класів А чи В для усіх видів кабельної системи – волоконно - оптичної, екранованої і неекранованої кручених пар.

Усі ведучі виробники UNIX машин (DEC, Hewlett-Packard, IBM, Sun Microsystems і інші) передбачають інтерфейси для безпосереднього підключення до мереж FDDI.

Підключення через мости і маршрутизатори

Мости (bridges) і маршрутизатори (routers) дозволяють підключити до FDDI мережі інших протоколів, наприклад, Token Ring і Ethernet. Це уможливлює економічне підключення до FDDI великого числа робочих станцій і іншого мережного устаткування як у нових, так і у вже існуючих ЛОМ.

Конструктивно мости і маршрутизатори виготовляються в двох варіантах - у закінченому виді, що не допускає подальшого апаратного нарощування чи реконфігурації (так називані standalone-пристрої), і у виді модульних концентраторів.

Прикладом standalone-пристроїв є: Router BR фірми Hewlett-Packard і EIFO Client/Server Switching Hub фірми Network Peripherals.

Модульні концентратори застосовуються в складних великих мережах у якості центральних мережних пристроїв. Концентратор являє собою корпус із джерелом живлення і з комунікаційною платою. У слоти концентратора вставляються мережні комунікаційні модулі. Модульна конструкція концентраторів дозволяє легко зібрати будь-яку конфігурацію ЛОМ, об'єднати кабельні системи різних типів і протоколів. Вільні слоти можна використовувати для подальшого нарощування ЛОМ.

Концентратори виробляються багатьма фірмами: 3Com, Cabletron, Chipcom, Cisco, Gandalf, Lannet, Proteon, SMC, SynOptics, Wellfleet і іншими.

Концентратор - це центральний вузол ЛОМ. Його відмовлення може привести до зупинки всієї мережі, чи принаймні, значної її частини. Тому більшість фірм, що роблять концентратори, уживають спеціальних заходів для підвищення їх відказостійкості. Такими мірами є резервування джерел живлення в режимі поділу чи навантаження гарячого резервування, а також можливість зміни чи доповнення модулів без відключення живлення (hot swap). Для того щоб знизити вартість концентратора, усі його модулі мають живлення від загального джерела. Силові елементи джерела живлення є найбільш ймовірною причиною його відмовлення. Тому резервування джерела живлення істотно продовжує термін безвідмовної роботи. При інсталяції кожне із джерел живлення концентратора може бути підключено до окремого джерела безперебійного живлення (UPS) на випадок несправностей у системі електропостачання. Кожний з UPS бажано підключити до готельних силових електричних мереж від різних підстанцій.

Можливість зміни чи доповнення модулів без відключення концентратора дозволяє провести ремонт чи розширення мережі без припинення сервісу для тих користувачів, мережні сегменти яких підключені до інших модулів концентратора.

1.5.6. Приклади використання FDDI

Приведемо два найбільш типові приклади можливого використання мереж FDDI.

Додаток клієнт-сервер. FDDI застосовується для підключення

устаткування, що вимагає широкої смуги пропущення від ЛОМ. Звичайно це файлові сервери NetWare UNIX машини і великі універсальні ЕОМ (mainframes). Крім того, як було відзначено вище, безпосередньо до мережі FDDI можуть бути підключені і деякі робітники станції, що вимагають високих швидкостей обміну даними.

Робочі станції користувачів підключаються через багатопортові мости FDDI-Ethernet. Міст здійснює фільтрацію і передачу пакетів не тільки між FDDI і Ethernet, але і між різними Ethernet-мережами. Пакет даних буде переданий тільки в той порт, де знаходиться вузол призначення, зберігаючи смугу пропущення інших ЛОМ. З боку мереж Ethernet їхня взаємодія еквівалентна зв'язку через магістраль (backbone), тільки в цьому випадку вона фізично існує не у виді розподіленої кабельної системи, а цілком зосереджена в багатопортовому мосту (Collapsed Backbone чи Backbone-in-a-box).

У залежності від кожного конкретного випадку (відстані між серверами, умови експлуатації, вимог до надійності, вартість і т.д.) сервери можуть підключатися до FDDI або як станції класу А, або як станції класу В.

FDDI у якості backbone магістралі. FDDI застосовується для зв'язку ЛОМ протоколу Ethernet, розташованих у декількох будинках. Як правило, у кожнім з будинків досить розмістити по одному багатопортовому мосту. У залежності від концентрації робочих станцій, кожний з Ethernet портів може обслуговувати один чи кілька поверхів будинку.

1.6. Мости FDDI-Ethernet

Мости працюють на перших двох рівнях моделі взаємодії відкритих систем - на фізичному і канальному - і призначені для зв'язку декількох ЛВС однотипних чи різних протоколів фізичного рівня, наприклад, Ethernet, Token Ring і FDDI. По своєму принципі дії мости підрозділяються на два типи (Sourece Routing - маршрутизація джерела) вимагають, щоб вузол-відправник пакета розміщав у ньому інформацію про шлях його маршрутизації. Іншими словами, кожна станція повинна мати убудовані функції по маршрутизації пакетів. Другий тип мостів

(Transparent Bridges - прозорі мости) забезпечують прозорий зв’язок станцій, розташованих у різних ЛВС, і усі функції по маршрутизації виконують тільки самі мости. Нижче ми будемо вести мову тільки про такі мости. Усі мости можуть поповнювати таблицю адрес (Learn addresses), маршрутизувати і фільтрувати пакети. Інтелектуальні мости, крім того, з метою підвищення чи безпеки продуктивності можуть фільтрувати пакети за критеріями, що задається через систему керування мережею.

Коли на один з портів моста приходить пакет даних, міст чи повинний переправити його на той порт, до якого підключений вузол призначення пакета, чи просто відфільтрувати його, якщо вузол призначення знаходиться на тім же самому порту, з якого прийшов пакет. Фільтрація дозволяє уникнути зайвого трафіка в інших сегментах ЛВС.

Кожен міст будує внутрішню таблицю фізичних адрес підключених до мережі вузлів. Процес її заповнення полягає в наступному. Кожен пакет має у своєму заголовку фізичні адреси вузлів відправлення і призначення. Одержавши на один зі своїх портів пакет даних, міст працює по наступному алгоритму. На першому кроці міст перевіряє, чи занесений у його внутрішню таблицю адреса вузла відправника пакета. Якщо ні, то міст заносить його в таблицю і зв’язує з ним номер порту, на який надійшов пакет. На другому кроці перевіряється, чи занесений у внутрішню таблицю адреса вузла призначення. Якщо ні, то міст передає прийнятий пакет в усі мережі, підключені до всіх інших його портів. Якщо адреса вузла призначення знайдений у внутрішній таблиці, міст перевіряє, чи підключена ЛВС вузла призначення до того ж самому порту, з якого прийшов пакет, чи ні. Якщо ні, то міст відфільтровує пакет, а якщо так, те передає його тільки на той порт, до якого підключений сегмент мережі з вузлом призначення.

Три головних параметри моста:

- розмір внутрішньої адресної таблиці;
- швидкість фільтрації;
- швидкість маршрутизації пакетів.

Розмір адресної таблиці характеризує максимальне число мережних

пристроїв, трафік яких може маршрутизувати міст. Типові значення розмірів адресної таблиці лежать у межах від 500 до 8000. Що ж відбудеться у випадку, якщо кількість підключених вузлів перевищить розміри адресної таблиці?

Оскільки більшість мостів зберігають у ній мережні адреси вузлів, останніми передававшими свої пакети, міст поступово буде "забувати" адреси вузлів, резе інших передавальних пакети. Це може привести до зниження ефективності процесу фільтрації, але не викликає принципових проблем у роботі мережі.

Швидкості фільтрації і маршрутизації пакетів характеризують продуктивність моста. Якщо вони нижче максимально можливої інтенсивності передачі пакетів по ЛВС, то міст може бути причиною затримок і зниження продуктивності. Якщо вище - значить вартість моста вище мінімально необхідної. Розрахуємо, який повинна бути продуктивність моста для підключення до FDDI декількох ЛВС протоколу Ethernet.

Обчислимо максимально можливу інтенсивність пакетів мережі Ethernet. Структура пакетів Ethernet показана в таблиці 1. Мінімальна довжина пакета дорівнює 72 чи байт 576 біт. Час, необхідне для передачі одного біта по ЛВС протоколу Ethernet зі швидкістю 10 Мбіт/сек дорівнює 0.1 мксек. Тоді час передачі мінімального по довжині пакета складе $57.6*10^{-6}$ сек. Стандарт Ethernet вимагає паузи між пакетами в 9.6 мксек. Тоді кількість пакетів, переданих за 1 сек, буде дорівнює $1/((57.6+9.6)*10^{-6})=14880$ пакетів у секунду.

Якщо міст приєднує до мережі FDDI N мереж протоколу Ethernet, то, відповідно, його швидкості фільтрації і маршрутизації повинні бути рівні N*14880 пакетів у секунду.

Таблиця 2.1.

Структура пакета в мережах Ethernet

Довжина в байтах	8	6	6	2	від 46 до 1500	4
Поле	Преамбула	Адреса одержувача	Адреса відправника	Тип/Довжина	Дані	Контрольна сума

Структура пакета в мережах Ethernet

З боку порту FDDI швидкість фільтрації пакетів повинна бути значно вище. Для того, щоб міст не знижував продуктивність мережі, вона повинні складати близько 500000 пакетів у секунду.

За принципом передачі пакетів мости підрозділяються на Encapsulating Bridges і Translational Bridges пакети фізичного рівня однієї ЛВС цілком переносять у пакети фізичного рівня інший ЛВС. Після проходження по другий ЛВС інший аналогічний міст видаляє оболонку з проміжного протоколу, і пакет продовжує своє руху у вихідному виді.

Такі мости дозволяють зв’язати FDDI-магістраллю два ЛВС протоколи Ethernet. Однак у цьому випадку FDDI буде використовуватися тільки як середовище передачі, і станції, підключені до мереж Ethernet, не будуть "бачити" станцій, безпосередньо підключених до мережі FDDI.

Мости другого типу виконують перетворення з одного протоколу фізичного рівня в іншій. Вони видаляють заголовок і замикаючу службову інформацію одного протоколу і переносять дані до іншого протоколу. Таке перетворення має істотна перевага: FDDI можна використовувати не тільки як середовище передачі, але і для безпосереднього підключення мережного устаткування, прозоро видимого станціями, підключеними до мереж Ethernet.

Таким чином, подібні мости забезпечують прозорість усіх мереж по протоколах мережного і більш верхніх рівнів (TCP/IP, Novell IPX, ISO CLNS, DECnet Phase IV і Phase V, AppleTalk Phase 1 і Phase 2, Banyan VINES, XNS і ін.).

Ще одна важлива характеристика моста - чи наявність відсутність підтримки алгоритму резервних шляхів (Spannig Tree Algorithm - STA) IEEE 802.1D. Іноді його називають також стандартом прозорих мостів (Transparent Bridging Standard - TBS).

Ситуація, коли між ЛВС1 і ЛВС2 існують два можливих шляхи - через міст 1 чи через міст 2 і аналогічні цим, називаються активними петлями. Активні петлі можуть викликати серйозні мережні проблеми: дублюючі пакети порушують логіку роботи мережних протоколів і приводять до зниження пропускної здатності

кабельної системи. STA забезпечує блокування всіх можливих шляхів, крім одного. Утім, у випадку проблем з основною лінією зв'язку, одні з резервних шляхів відразу буде призначений активним.

Інтелектуальні мости

Дотепер ми обговорювали властивості довільних мостів. Інтелектуальні мости мають ряд додаткових функцій. Для великих комп'ютерних мереж однієї з ключових проблем, що визначають їхня ефективність, є зниження вартості експлуатації, рання діагностика можливих проблем, скорочення часу пошуку й усунення несправностей.

Для цього застосовуються системи централізованого керування мережею. Як правило вони працюють по SNMP протоколі (Simple Network Management Protocol) і дозволяють адміністратору мережі з його робочого місця:

- конфігорувати порти концентраторів;
- робити набір статистики й аналіз трафік.

Наприклад, для кожної підключеної до мережі станції можна одержати інформацію про тім, коли вона останній раз посилала пакети в мережу, про число пакетів і байт, прийнятих кожною станцією з ЛВС, відмінних від тієї, до якої вона підключена, число переданих широкомовних (broadcast) пакетів і т.д.;

- установлювати додаткові фільтри на порти концентратора по номерах ЛВС чи по фізично адресах мережних пристроїв з метою посилення захисту від несанкціонованого доступу до ресурсів чи мережі для підвищення ефективності функціонування окремих сегментів ЛВС;
- оперативно одержувати повідомлення про усіх виникаючих проблемах у мережі і легко їхній локалізувати;
- проводити діагностику модулів концентраторів;
- переглядати в графічному виді зображення передніх панелей модулів, встановлених у вилучені концентратори, включаючи і поточне стан індикаторів (це можливо завдяки тому, що програмне забезпечення автоматично розпізнає, який саме з модулів встановлений у кожен конкретний слот концентратора, і одержує інформацію і поточному статусі всіх портів модулів);

- переглядати системних журнал, у який автоматично записується інформація про всі проблеми з мережею, про час включення і вимикання робочих станцій і серверів і про всіх інших важливим для адміністратора подіях.

Перераховані функції властиві всі інтелектуальним мостам і маршрутизаторам. частина з них (наприклад, Prism System фірми Gandalf), крім того, мають наступними важливі розширені можливості:

1. Пріоритети протоколів. По окремих протоколах мережного рівня деякі концентратори працюють як маршрутизатори. У цьому випадку може підтримуватися установка пріоритетів одних протоколів над іншими. Наприклад, можна установити пріоритет TCP/IP над всіма іншими протоколами. Це означає, що пакети TCP/IP будуть передаватися в першу чергу (це буває корисно у випадку недостатньої смуги пропущення кабельної системи).

2. Захист від "штормів широкомовних пакетів" (broadcast storm). Одна з характерних несправностей мережного устаткування і помилок у програмному забезпеченні - мимовільна генерація з високою інтенсивністю broadcast-пакетів, тобто пакетів, адресованих всім іншим підключеним до мережі пристроям. Мережна адреса вузла призначення такого пакета складається з одних одиниць. Одержавши такий пакет на один зі своїх портів, міст повинний адресувати його на всі інші порти, включаючи і FDDI порт. У нормальному режимі такі пакети використовуються операційними системами для службових цілей, наприклад, для розсилання повідомлень про появу в мережі нового сервера. Однак при високій інтенсивності їхньої генерації, вони відразу займуть усю смугу пропущення. Міст забезпечує захист мережі від перевантаження, включаючи фільтр на тім порту, з якого надходять такі пакети. Фільтр не пропускає broadcast-пакети й інші ЛВС, охороняючи тим самим іншу мережу від перевантаження і зберігаючи її працездатність.

3. Збір статистики в режимі "Що, якщо?" Ця опція дозволяє віртуально установлювати фільтри на порти моста. У цьому режимі фізично фільтрація не проводиться, але ведеться збір статистики про пакети, що були б відфільтровані при реальному включенні фільтрів. Це дозволяє адміністратору попередньо

оцінити наслідку включення фільтра, знижуючи тим самим імовірність помилок при неправильно встановлених умовах фільтрації і не приводячи до збоїв у роботі підключеного устаткування.

1.7. Коди, що самосинхронізуються

При передачі цифрових сигналів по аналогових лініях зв'язку передавальна і приймаюча станції повинні бути синхронізовані між собою по частоті передачі біт у каналі. У противному випадку неминучі помилки при прийомі.

У випадку, якщо приймач і передавач розташовані близько друг від друга, то для синхронізації можна використовувати окремий чи канал лінію. Якщо ж станції рознесені на великі відстані, то стає вигідніше вмонтувати можливість частотного настроювання в сам сигнал. Для цього застосовуються коди, що сам-синхронізуються. Ідея полягає в тому, щоб переданий сигнал часто змінював свій стан (з 0 на 1 і навпаки) навіть у випадку, якщо передаються довгі послідовності даних, що складаються тільки з одних 0 чи тільки з одних 1.

Манчестерське кодування - один зі способів побудови коду, що сам-синхронізується. Цей код забезпечує зміна стану сигналу при представленні кожного біта. Манчестерське кодування вимагає подвоєної швидкості передачі сигналу в бодах щодо переданих даних.

Застосований у FDDI код, що сам-синхронізується, 5B/4B є однієї з можливих альтернатив для манчестерського кодування. У таблиці представлений спосіб кодування чотирьох інформаційних біт п'ятьма сигнальними бітами коду 5B/4B. Коди перетворення підібрані таким чином, щоб забезпечити можливо більш часта зміна сигналу, незалежно від виду переданих даних.

Таблиця 2.2.

Таблиця кодів

4 біти даних	5 біт даних
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

1.8. Відказостійкість мереж FDDI

Стандарт ANSI X3T9.5 регламентує 4 основних відказостійкі властивості мереж FDDI:

1. Кільцева кабельна система зі станціями класу А відказостійка до однократного обриву кабелю в будь-якім місці кільця. Станції, що знаходяться по обох сторони обриву, реконфігурують шлях циркуляції маркера і даних, підключаючи для цього вторинне волоконно-оптичне кільце.

2. Вимикання харчування, відмовлення однієї зі станцій класу В чи обривши кабелю від концентратора до цієї станції буде виявлений концентратором, і відбудеться відключення станції від кільця.

3. Дві станції класу В підключені відразу до двох концентраторів. Цей

спеціальний вид підключення називається Dual Homing і може бути використаний для відказостійкого (до несправностей у чи концентраторі в кабельній системі) підключення станцій класу В за рахунок дублювання підключення до основного кільця. У нормальному режимі обмін даними відбувається тільки через один концентратор. Якщо з якої-небудь причини зв’язок губиться, то обмін буде здійснюватися через другий концентратор.

4. Вимикання чи харчування відмовлення однієї зі станцій класу А не приведе до відмовлення інших станцій, підключених до кільця, тому що світловий сигнал буде просто пасивно передаватися до наступного станції через оптичний перемикач (Optical Bypass Switch). Стандарт допускає мати до трьох послідовно розташованих виключених станцій. Оптичні перемикачі роблять фірми Molex і А.

РОЗДІЛ 2
СТРУКТУРНА ОРГАНІЗАЦІЯ ПІДПРИЄМСТВА

2.1. Розробка структури ЛОМ і визначення складу використовуваних програмно-апаратних засобів

Мале підприємство „Форміка” знаходиться в комп’ютерному бізнесі на протязі восьми років. До не давнього часу основною формою діяльності підприємства була продаж комп’ютерної техніки, аксесуарів, засобів мобільного зв’язку, ремонт комп’ютерної техніки, заправка принтерів, картриджів. На сьогоднішній день на підприємстві працює 12 осіб. З ростом конкуренції і здешевленням техніки з’явилася необхідність пошуку нових сфер діяльності так як підприємство є платоспроможним, було прийнято рішення відкрити комп’ютерний клуб як дочірнє підприємство.

Досить довгий час потреби підприємства задовольняли 4 комп’ютери: сервер і 3 робочі станції. Комп’ютерна мережа була побудована на базі 8 портового SVICH із швидкістю передачі даних 100 Мб/с. З переходом на бухгалтерську програму „X-DOOR – Торгівля і Складський облік” дана мережа перестала забезпечувати нормальну швидкість передачі даних.

Тому при побудові нової комп’ютерної мережі було прийняте рішення створити ЛОМ с топологією „Зірка” з використанням 32-портового свіча із швидкістю передачі даних 100 Мб/с. Мережа повинна включати в себе:

– 1 сервер, на який підключений Інтернет через точку доступу Zyxel Mini omni, яка забезпечує швидкість передачі даних на вході 512 МБ/с.

– На сервері повинна бути розміщена спільна база даних за допомогою якої з 3 робочих машин менеджери по продажу повинні надавати консультації і виконувати операції оприбутковування-продажу товарів.

– До сервера повинен бути підключений лазерний принтер Samsung ML-1210, до якого повинні мати доступ 3 робочі машини менеджерів.

– До сервера повинен бути підключений цифровий ксерокс Canon з можливістю друку листів формату А3 з комп’ютера.

– На сервері повинна зберігатися база даних програмного забезпечення та драйверів засобів мобільного зв’язку.

– Робочі станції комп’ютерного клубу також повинні залежити від центрального сервера.

– Сервер повинен бути захищений від несанкціонованого доступу зі сторони Інтернету, а також зі сторони робочих станцій комп’ютерного клубу.

Виходячи з цих вимог, була побудована ЛОМ. Найбільшою проблемою при побудові стало питання захисту інформації, маршрутизації доступу.

Схема мережі знаходиться в додатках.

Локально-обчислювальна мережа у новому варіанті побудови має ряд особливостей. Необхідність побудови нового варіанта локально-обчислювальної мережі виникла через проблеми старої мережної архітектури:

– користувачам не вистачає пропускної здатності мережі;

– мала швидкість відповіді серверів на запити;

– необхідність переходу на більш швидкісне чому 10 Мбіт/с виділене з’єднання, без заміни всього устаткування;

– забезпечення високої надійності мережі;

– зручне керування мережею

Для усунення цих проблем новий варіант побудови локально-обчислювальної мережі повинен бути модернізований в такому напрямі:

– Перехід на більш швидкісну, чим Ethernet, технологію Fast Ethernet 100 Мбіт/с;

– Організацію Віртуальних мереж (VLAN), трафік яким на канальному рівні цілком ізольований від інших вузлів мережі;

– Здійснення Агрегування каналів (Транкинга) використовуючи кілька активних рівнобіжних каналів одночасно для підвищення пропускної здатності і надійності мережі.

2.2. Програмно-апаратні методи захисту від вилучених атак у IP мережі

До програмно-апаратних засобів забезпечення інформаційної безпеки

засобів зв’язку в обчислювальних мережах відносяться:

- апаратні шифратори мережного трафіка;
- методика Firewall, реалізована на базі програмно-апаратних засобів;
- захищені мережні криптопротоколи;
- програмно-апаратні аналізатори мережного трафіка;
- захищені мережні ОС.

Опишемо дані засоби захисту, застосовувані в Internet. При цьому ми переслідуємо наступні цілі: по-перше, ще раз повернемося до міфу про "абсолютний захист" , що нібито забезпечують системи Firewall, мабуть, завдяки старанням їхніх продавців; по-друге, порівняємо існуючі версії криптопротоколів, застосовуваних у Internet, і дамо оцінку, по суті, критичному положенню в цій області; і, по-третє, ознайомимося з можливістю захисту за допомогою мережного монітора безпеки, призначеного для здійснення динамічного контролю за виникаючими ситуаціями в сегменті IP-мережі, який захищається, що свідчать про здійснення на даний сегмент однієї з вилучених атак.

2.3. Методика Firewall, як основний програмно-апаратний засіб здійснення мережної політики безпеки у виділеному сегменті IP-мережі

У загальному випадку методика Firewall реалізує наступні основні три функції:

1. Багаторівнева фільтрація мережного трафіка.

Фільтрація звичайно здійснюється на трьох рівнях OSI:

- мережному (IP);
- транспортному (TCP, UDP);
- прикладному (FTP, TELNET, HTTP, SMTP і т.д.).

Фільтрація мережного трафіка є основною функцією систем Firewall і дозволяє адміністратору безпеки мережі централізовано здійснювати необхідну мережну політику безпеки у виділеному сегменті IP-мережі, тобто, настроївши відповідним чином Firewall, можна дозволити чи заборонити користувачам як

доступ із зовнішньої мережі до відповідного службам хостів чи до хостів, що знаходяться в сегменті, що захищається, так і доступ користувачів із внутрішньої мережі до відповідного ресурсам зовнішньої мережі. Можна провести аналогію з адміністратором локальної ОС, що для здійснення політики безпеки в системі призначає необхідним образом відповідні відносини між суб'єктами (користувачами) і об'єктами системи (файлами, наприклад), що дозволяє розмежувати доступ суб'єктів системи до її об'єктів відповідно до заданого адміністратором правами доступу. Ті ж міркування застосовні до Firewall-фільтрації: як суб'єктів взаємодії будуть виступати IP-адреси хостів користувачів, а як об'єкти, доступ до яких необхідно розмежувати, - IP-адреси хостів, використовувані транспортні протоколи і служби надання вилученого доступу.

2. Proxy-схема з додатковою ідентифікацією й аутентифікацією користувачів на Firewall - хості.

Proxy-схема дозволяє, по-перше, при доступі до захищеного Firewall сегменту мережі здійснити на ньому додаткову ідентифікацію й аутентифікацію вилученого користувача і, по-друге, є основою для створення приватних мереж з віртуальними IP-адресами. Зміст proxy-схеми складається в створенні з'єднання з кінцевим адресатом через проміжний proxy-сервер (proxy від англ. повноважний) на хості Firewall. На цьому proxy-сервері і може здійснюватися додаткова ідентифікація абонента.

3. Створення приватних мереж (Private Virtual Network - PVN) з "віртуальними" IP-адресами (NAT - Network Address Translation).

У тому випадку, якщо адміністратор безпеки мережі вважає за доцільне сховати щиру топологію своєї внутрішньої IP-мережі, то йому можна порекомендувати використовувати системи Firewall для створення приватної мережі (PVN-мережа). Хостам у PVN-мережі призначаються будь-які "віртуальні" IP-адреси. Для адресації в зовнішню мережу (через Firewall) необхідно або використання на хості Firewall описаних вище proxy-серверів, або застосування спеціальних систем роутінгу (маршрутизації), тільки через який і можлива зовнішня адресація. Це відбувається через те, що використовувана у внутрішній

PVN-мережі віртуальна IP-адреса, мабуть, не придатна для зовнішньої адресації (зовнішня адресація - це адресація до абонентів, що знаходиться за межами PVN-мережі). Тому чи proxy-сервер засіб роутінгу повинний здійснювати зв'язок з абонентами з зовнішньої мережі зі своєї дійсної IP-адреси. До речі, ця схема зручна в тому випадку, якщо вам для створення IP-мережі виділили недостатню кількість IP-адрес (у стандарті IPv4 це случається суцільно і поруч, тому для створення повноцінної IP-мережі з використанням proxy-схеми досить тільки однієї виділеної IP-адреси для proxy-сервера).

Будь-який пристрій, що реалізує хоча б одну з цих функцій Firewall-методики, і є Firewall-пристроєм. Наприклад, ніщо не заважає використовувати в якості Firewall - хосту комп'ютер зі звичайної ОС FreeBSD чи Linux, у якої відповідним чином необхідно скомпілювати ядро ОС. Firewall такого типу буде забезпечувати тільки багаторівневу фільтрацію IP-трафіка. Інша справа, пропоновані на ринку могутні Firewall-комплекси, зроблені на базі ЕОМ чи міні - ЕОМ, звичайно реалізують усі функції Firewall-методики і є повно функціональними системами Firewall. На наступному малюнку зображений сегмент мережі, відділений від зовнішньої мережі повно функціональним Firewall - хостом.

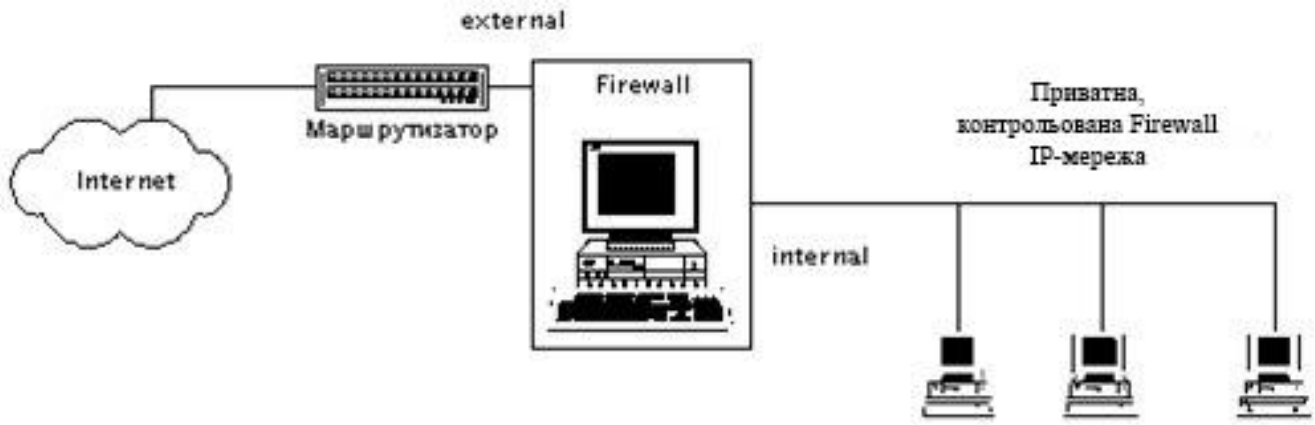

Рис. 2.1. Узагальнена схема повно функціонального хосту Firewall

Однак адміністраторам IP-мереж, піддавшись на рекламу систем Firewall, не варто помилятися на той рахунок, що Firewall це гарантія абсолютного захисту від вилучених атак у мережі Internet. Firewall - не стільки засіб забезпечення безпеки,

скільки можливість централізовано здійснювати мережну політику розмежування вилученого доступу до доступних ресурсів вашої мережі. Так, у тому випадку, якщо, наприклад, до даного хосту заборонений вилучений TELNET-доступ, то Firewall однозначно запобіжить можливість даного доступу. Але справа в тім, що більшість вилучених атак мають зовсім інші мети (безглуздо намагатися одержати визначений вид доступу, якщо він заборонений системою Firewall). Дійсно, задамо собі питання, а які з вилучених атак може запобігти Firewall? Аналіз мережного трафіка ? Помилковий ARP-сервер? Помилковий DNS-сервер? Ні, на жаль, Firewall вам отут не помічник. Нав'язування помилкового маршруту за допомогою протоколу ICMP? Так, цю атаку шляхом фільтрації ICMP-повідомлень Firewall легко відіб'є (хоча досить буде фільтруючого маршрутизатора, наприклад Cisco). Підміна одного із суб'єктів TCP-з'єднання? Відповідь негативна; Firewall отут абсолютно не при чому. Порушення працездатності хосту шляхом створення спрямованого шторму помилкових запитів чи переповнення черги запитів? У цьому випадку застосування Firewall тільки погіршить усю справу. Атакуючому для того, щоб вивести з ладу (відрізати від зовнішнього світу) усі хости усередині захищеного Firewall-системою сегмента, досить атакувати тільки один Firewall, а не трохи хостів (це легко порозуміється тим, що зв'язок внутрішніх хостів із зовнішнім світом можливий тільки через Firewall).

З усього вищесказаного аж ніяк не випливає, що використання систем Firewall абсолютно безглуздо. Ні, на даний момент цій методиці немає альтернативи. Однак треба чітко розуміти і пам'ятати її основне призначення. Нам представляється, що застосування методики Firewall для забезпечення мережної безпеки є необхідною, але аж ніяк не достатньою умовою, і не потрібно вважати, що, поставивши Firewall, ви разом вирішите всі проблеми з мережною безпекою і позбудетеся від усіх можливих вилучених атак з мережі Internet. Прогнила з погляду безпеки мережа Internet ніяким окремо узятим Firewall'ом не захистиш!

2.4. Програмні методи захисту, застосовані в мережі Internet

До програмних методів захисту в мережі Internet можна віднести насамперед

захищені криптопротоколи, з використанням яких з’являється можливість надійного захисту з’єднання. Далі піде мова про існуючі на сьогоднішній день у Internet підходах і основних, уже розроблених, криптопротоколах.

До іншого класу програмних методів захисту від вилучених атак відносяться існуючі на сьогоднішній день програми, основна мета яких - аналіз мережного трафіка на предмет наявності одного з відомих активних вилучених впливів.

2.5. SKIP-технологія і криптопротоколи SSL, S-HTTP, як основний засіб захисту з’єднання і переданих даних у мережі

Одна з основних причин успіху вилучених атак на розподілені ВР криється у використанні мережних протоколів обміну, що не можуть надійно ідентифікувати вилучені об’єкти, захистити з’єднання і передані по ньому дані. Тому зовсім природно, що в процесі функціонування Internet були створені різні захищені мережні протоколи, що використовують криптографію як із закритим, так і з відкритим ключем. Класична криптографія із симетричними криптоалгоритмами припускає наявність у передавальної і приймаючої сторони симетричних (однакових) ключів для шифрування і дешифрування повідомлень. Ці ключі передбачається розподілити заздалегідь між кінцевим числом абонентів, що в криптографії називається стандартною проблемою статичного розподілу ключів. Очевидно, що застосування класичної криптографії із симетричними ключами можливо лише на обмеженій безлічі об’єктів. У мережі Internet для всіх її користувачів вирішити проблему статичного розподілу ключів, мабуть, не представляється можливим. Однак одним з перших захищених протоколів обміну в Internet був протокол Kerberos, заснований саме на статичному розподілі ключів для кінцевого числа абонентів. Таким же шляхом, використовуючи класичну симетричну криптографію, наші спецслужби змушені йти на те, що розробляють свої захищені криптопротоколи для мережі Internet. Це порозуміється тим, що чомусь дотепер немає стандартного криптоалгоритму з відкритим ключем. Скрізь у світі подібні стандарти шифрування давно прийняті і сертифіковані, а ми, видимо, знову йдемо другим шляхом.

Отже, зрозуміло, що для того, щоб дати можливість захиститися всій безлічі користувачів мережі Internet, а не обмеженій його підмножині, необхідно використовувати динамічно вироблювані в процесі створення віртуального з'єднання ключі при використанні криптографії з відкритим ключем. Далі ми розглянемо основні на сьогоднішній день підходи і протоколи, що забезпечують захист з'єднання.

SKIP (Secure Key Internet Protocol)- технологією називається стандарт інкапсуляції IP-пакетів, що дозволяє в існуючому стандарті IPv4 на мережному рівні забезпечити захист з'єднання і переданих по ньому даних. Це досягається в такий спосіб: SKIP-пакет являє собою звичайний IP-пакет, поле даних якого представляє із себе SKIP-заголовок визначеного специфікацією формату і криптограму (зашифровані дані). Така структура SKIP-пакета дозволяє безперешкодно направляти його будь-якому хосту в мережі Internet (міжмережна адресація відбувається по звичайному IP-заголовку в SKIP-пакеті). Кінцевий одержувач SKIP-пакета по заздалегідь визначеному розроблювачами алгоритму розшифровує криптограму і формує звичайний TCP- чи UDP-пакет, що і передає відповідному звичайному модулю (TCP чи UDP) ядра операційної системи. У принципі, ніщо не заважає розроблювачу формувати за даною схемою свій оригінальний заголовок, відмінний від SKIP-заголовка.

S-HTTP (Secure HTTP) - це розроблений компанією Enterprise Integration Technologies (EIT) спеціально для Web захищений HTTP-протокол. Протокол S-HTTP дозволяє забезпечити надійний криптозахист тільки HTTP-документів Web-півночі і функціонує на прикладному рівні моделі OSI. Ця особливість протоколу S-HTTP робить його абсолютно спеціалізованим засобом захисту з'єднання, і, як наслідок, неможливе його застосування для захисту всіх інших прикладних протоколів (FTP, TELNET, SMTP і ін.). Крім того, жоден з існуючих на сьогоднішній день основних Web-браузерів (ні Netscape Navigator , ні Microsoft Explorer) не підтримують даний протокол.

SSL (Secure Socket Layer) - розробка компанії Netscape - універсальний протокол захисту з'єднання, що функціонує на сеансовому рівні OSI. Цей

протокол, що використовує криптографію з відкритим ключем, на сьогоднішній день, на нашу думку, є єдиним універсальним засобом, що дозволяє динамічно захистити будь-яке з'єднання з використанням будь-якого прикладного протоколу (DNS, FTP, TELNET, SMTP і т.д.). Це зв'язано з тим, що SSL, на відміну від S-HTTP, функціонує на проміжному сеансовому рівні OSI (між транспортним - TCP, UDP, - і прикладним - FTP, TELNET і т.д.). При цьому процес створення віртуального SSL-з'єднання відбувається за схемою Діффі і Хеллмана, що дозволяє виробити криптостійкий сеансовий ключ, використовуваний надалі абонентами SSL-з'єднання для шифрування переданих повідомлень. Протокол SSL сьогодні вже практично оформився як офіційний стандарт захисту для HTTP-з'єднань, тобто для захисту Web-серверів. Його підтримують, природно, Netscape Navigator і, як не дивно, Microsoft Explorer. Звичайно, для встановлення SSL-з'єднання з Web-сервером ще необхідно і наявність Web-сервера, що підтримує SSL. Такі версії Web-серверів вже існують (SSL - Apache, наприклад). У висновку розмови про протокол SSL не можна не відзначити наступний факт: законами США донедавна був заборонений експорт криптосистем з довжиною ключа більш 40 біт (недавно він був збільшений до 56 біт). Тому в існуючих версіях браузерів використовуються саме 40-бітні ключі. Криптоаналітиками шляхом експериментів було з'ясовано, що в наявній версії протоколу SSL шифрування з використанням 40-бітного ключа не є надійним захистом для переданих по мережі повідомлень, тому що шляхом простого перебору (2^{40} комбінацій) цей ключ підбирається за час від 1,5 (на супер ЕОМ Silicon Graphics) до 7 доби (у процесі обчислень використовувалося 120 робочих станцій і трохи міні ЕОМ).

Отже, мабуть, що повсюдне застосування цих захищених протоколів обміну, особливо SSL (звичайно, з довжиною ключа більш 40 біт), поставить надійний бар'єр на шляху усіляких вилучених атак і серйозно ускладнить життя зловмисників усього світу. Однак весь трагізм сьогоднішньої ситуації з забезпеченням безпеки в Internet полягає в тому, що поки жоден з існуючих криптопротоколів (а їх уже чимало) не оформився як єдиний стандарт захисту з'єднання, що підтримувався б усіма виробниками мережних ОС. Протокол SSL, з

наявних на сьогодні, підходить на цю роль щонайкраще. Якби його підтримували всі мережні ОС, то не треба було б створення спеціальних прикладних SSL-сумісних серверів (DNS, FTP, TELNET, WWW і ін.). Якщо не домовитися про прийняття єдиного стандарту на захищений протокол сеансового рівня, то тоді буде потрібно прийняття багатьох стандартів на захист кожної окремої прикладної служби. Наприклад, уже розроблений експериментальний, ніким не підтримуваний протокол Secure DNS.

Також існують експериментальні SSL-сумісні Secure FTP- і TELNET-сервери. Але все це без прийняття єдиного підтримуваного усіма виробниками стандарту на захищений протокол не має абсолютно ніякого змісту. А на сьогоднішній день виробники мережних ОС не можуть домовитися про єдину позицію на цю тему і, тим самим, перекладають рішення цих проблем безпосередньо на користувачів Internet і пропонують їм вирішувати свої проблеми з інформаційною безпекою самим.

2.6. Мережний монітор безпеки IP Alert-1

У мережі Internet, як і в інших мережах (наприклад, Novell NetWare, Windows NT), відчувається серйозна недостача програмного засобу захисту, що здійснює комплексний контроль (моніторинг) на канальному рівні за всім потоком переданої по мережі інформації з метою виявлення всіх типів вилучених впливів. Дослідження ринку програмного забезпечення мережних засобів захисту для Internet виявило той факт, що подібних комплексних засобів виявлення вилучених впливів не існує, а ті, що маються, призначені для виявлення впливів одного конкретного типу (наприклад, ICMP Redirect). Тому і була почата розробка засобу контролю сегмента IP-мережі, призначеного для використання в мережі Internet і наступна назва, що одержала: мережний монітор безпеки IP Alert-1. Основна задача цього засобу, що програмно аналізує мережний трафік у каналі передачі, складається не у відображенні здійснюваних по каналі зв’язку вилучених атак, а в їхньому виявленні, протоколюванні (веденні файлу аудита з протоколюванням у зручній для наступного візуального аналізу формі всіх подій, зв’язаних з

вилученими атаками на даний сегмент мережі) і негайним сигналізовуванні адміністратору безпеки у випадку виявлення вилученої атаки. Основною задачею мережного монітора безпеки IP Alert-1 є здійснення контролю за безпекою відповідного сегмента мережі Internet. Мережний монітор безпеки IP Alert-1 володіє наступними функціональними можливостями і дозволяє, шляхом мережного аналізу, знайти наступні вилучені атаки на контрольований їм сегмент мережі Internet.

Функціональні можливості мережного монітора безпеки IP Alert-1:

1. Контроль за відповідністю IP- і Ethernet-адрес у пакетах, переданих хостами, що знаходяться усередині контрольованого сегмента мережі.

На хості IP Alert-1 адміністратор безпеки створює статичну ARP-таблицю, куди заносить зведення про відповідний IP- і Ethernet-адресах хостів, що знаходяться усередині контрольованого сегмента мережі. Дана функція дозволяє знайти несанкціоновану зміну IP-адреси чи її підміну (IP Spoofing).

2. Контроль за коректним використанням механізму вилученого ARP-пошуку.

Ця функція дозволяє, використовуючи статичну ARP-таблицю, визначити вилучену атаку "Помилковий ARP-сервер".

3. Контроль за коректним використанням механізму вилученого DNS-пошуку. Ця функція дозволяє визначити всі можливі види вилучених атак на службу DNS.

4. Контроль на наявність ICMP Redirect повідомлення.

Дана функція оповіщає про виявлення ICMP Redirect повідомлення і відповідної вилученої атаки.

5. Контроль за коректністю спроб вилученого підключення шляхом аналізу переданих запитів.

Ця функція дозволяє знайти, по-перше, спробу дослідження закону зміни початкового значення ідентифікатора TCP-з’єднання - ISN, по-друге, вилучену атаку "відмовлення в обслуговуванні", здійснювану шляхом переповнення черги запитів на підключення, і, по-третє, спрямований "шторм" помилкових запитів на

підключення (як TCP, так і UDP), що приводить також до відмовлення в обслуговуванні.

Таким чином, мережний монітор безпеки IP Alert-1 дозволяє знайти, сповістити і запротоколювати усі види вилучених атак. При цьому дана програма ніяким образом не є конкурентом системам Firewall. IP Alert-1, використовуючи систематизовані особливості вилучених атак на мережу Internet, служить необхідним доповненням - до речі, незрівнянно більш дешевим, - до систем Firewall. Без монітора безпеки більшість спроб здійснення вилучених атак на ваш сегмент мережі залишиться приховано від ваших очей. Жоден з відомих FireWall не займається подібним інтелектуальним аналізом минаючих по мережі повідомлень на предмет виявлення різного роду вилучених атак, обмежуючи, у кращому випадку, веденням журналу, у який заносяться зведення про спроби підбора паролів для TELNET і FTP, про сканування портів і про сканування мережі з використанням знаменитої програми вилученого пошуку відомих уразливостей мережних ОС - SATAN. Тому, якщо адміністратор IP-мережі не бажає залишатися байдужим і задовольнятися роллю простого статиста при вилучених атаках на його мережу, то йому бажано використовувати мережний монітор безпеки IP Alert-1. До речі, Цутому Шимомура зміг запротоколювати атаку Кевіна Митника, багато в чому, видимо, завдяки програмі tcpdump - найпростішому аналізатору IP-трафіка.

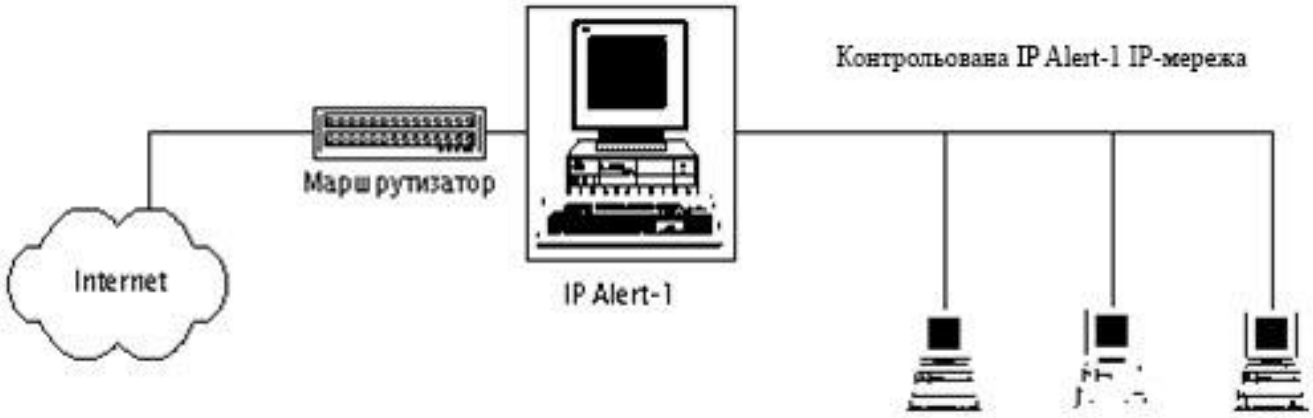

Рис. 2.2. Мережний монітор безпеки IP Alert-1

2.7. Засоби автоматизованого контролю безпеки

Ми вже говорили про корисність засобу автоматизованого контролю безпеки окремого комп'ютера, а також усієї подмережі, за якої він відповідає, для системного адміністратора. Природно, що такі засоби вже з'являлися, і частіше інших зустрічаються назви ISS (Internet Security Scaner), COPS (Computer Oracle and Password System) і, звичайно, SATAN (Security Administrator Tool for Analizyng Networks). На жаль, їм звичайно властиві наступні недоліки:

- системозалежність - звичайно вони розраховані на цілком конкретну ОС чи навіть її версію;
- ненадійність і неадекватність - якщо ці програми повідомляють, що всі "О'кеу", це зовсім не виходить, що так насправді і є; і навпаки - деяка "уразливість", з їхнього погляду, може виявитися спеціальним варіантом конфігурації системи;
- малий час життя - тому що з моменту виявлення уразливості до її використання проходить не дуже великий час (порядку року), програма швидко застаріває;
- не актуальність - більш того, з моменту виходу програми у світ всі нові (тому самі небезпечні) уразливості виявляються невідомими для неї, і її цінність швидко зводиться до нуля. Цей недолік є самим серйозним;
- нарешті, це можливість їхнього використання з прямо протилежними цілями - для пошуку вад у вашій системі.

Можна помітити явну аналогію цих програм з антивірусними сканерами першого покоління - ті знали лише строго визначений набір вірусів, нові віруси додавалися тільки в наступному випуску програми. Якщо подивитися на можливості сучасних антивірусних програм - це й оперативне лікування вірусів, і автоматизоване поповнення бази вірусів самим користувачем, і пошук невідомих вірусів, - то можна побажати, щоб гарний сканер Інтернету зміг запозичити деякі з них. У першу чергу - це можливість поповнення бази новими уразливостями. Причому в наші дні це нескладно зробити - коштує лише переписувати інформацію з джерел, що займаються саме збором таких зведень, типу CERT чи CIAC.

2.8. Програма SATAN

SATAN, іноді вважається чи ледве ні самою небезпечною програмою з абиколи написаних, починаючи від своєї лиховісної назви до можливості влізти чи ледве не в самий захищений комп'ютер. А що стосується влізання в комп'ютер - якщо подібна програма і мається в зломщиків чи спецслужб, то вона ніколи не стала б вільно поширюватися по Інтернету, як це відбувається з SATAN.

Насправді SATAN - це добротно зроблена, із сучасним інтерфейсом, програма для пошуку проломів у вашої підмережі (Intranet, як модно говорити останнім часом), написана на машинно-незалежних мовах Perl і З, тому вона в деякій мері переборює перший з вищеописаних недоліків. Вона навіть допускає можливість для розширення і вставки нових модулів. На жаль, у всім іншому їй властиві зазначені недоліки, у т.ч. і самий головний - вона вже застаріла, і не може зараз серйозно використовуватися ні адміністраторами, ні зломщиками. Однак на момент виходу це була досить актуальна програма. Вона містила в собі пошук більшості уразливостей. Зокрема, програма шукає уразливості в:

- FTP і TFTP;
- NFS і NIS;
- rexd;
- sendmail;
- r-службах;
- X-Windows.

Існують також більш пізні версії SaTaN'а, у які включений пошук і інших уразливостей. Для цього вона спочатку всіляким образом збирає інформацію про вашу систему, причому рівень цього конфігурується користувачем і може бути: легкий, нормальний і твердий. Легкий рівень, за твердженням авторів програми, не може бути ніяк виявлений стороною, що атакується, (принаймні, така активність програми ніяк не може бути прийнята за ворожу) і містить у собі DNS-запити для з'ясування версії операційної системи й іншої подібної інформації, що може бути легально отримана з використанням DNS. Далі вона надсилає запит на службу RPC (remote procedure call) для з'ясування, які rpc- сервіси працюють. Нормальний

рівень розвідки містить у собі всі ці запити, а також доповнює їхньою посилкою запитів (скануванням) деяких строго визначених портів, таких як FTP, telnet, SMTP, NNTP, UUCP і ін. для визначення встановлених служб. Нарешті, твердий рівень містить у собі всі попередні рівні, а також доповнюється повним скануванням усіх (можливих) UDP- і TCP-портів для виявлення нестандартних служб чи служб на нестандартних портах. Автори застерігають, що таке сканування може бути легко зафіксовано навіть без спеціальних програм - наприклад, на консолі можуть з'являтися повідомлення від вашого FireWall.

Іншою важливою опцією, що задається при настроюванні SaTaN'а, є глибина перегляду підмереж (proximity). Значення 0 означає тільки один хост, 1 - підмережу, у яку він входить, 2 - усі підмережі, у які входить підмережа даного хосту, і т.д. Автори підкреслюють, що ні при яких обставинах це число не повинне бути більш 2, інакше SATAN вийде з-під контролю і просканує занадто багато зовнішніх підмереж.

Власне, нічим більш страшним, крім як скануванням портів і виявленням працюючих служб і їхньої конфігурації, SATAN не займається. При цьому, якщо знаходяться потенційні уразливості, він сповіщає про це. Як пишуть самі автори, фаза проникнення у вилучену систему не була реалізована.

Користувач може відсортувати знайдені уразливості (по типі, серйозності і т.п.) і відразу одержати розгорнуту інформацію з кожній з них. Цікаво, що у версіях до 1.1.1 у цій схемі аутентифікації теж була помилка, що навіть потрапила в один з бюлетенів CERT.

Отже, типовий сценарій роботи з SATAN полягає в наступному:

- настроїти бажані параметри, у тому числі глибину сканування;
- задати адреси, мети і рівень сканування;
- переглянути отримані результати й одержати по них більш докладну інформацію;
- усунути знайдені уразливості.

Адміністратору безпеки рекомендується просканувати на твердому рівні усі свої хости, а також усі довірені хости, обов'язково запитавши на це дозвіл у їхніх

адміністраторів. Це рекомендується зробити навіть сьогодні, незважаючи на те, що SATAN застарів - ви зможете швидко одержати список використовуваних мережних служб і їхніх версій і перевірити, немає чи серед них уразливих, скориставшись матеріалами CERT чи CIAC.

2.9. Internet Scaner (ISS)

Програма, що більш-менш задовольняє перерахованим вимогам до сучасного засобу автоматизованої перевірки безпеки хосту. Принаймні, вона регулярно обновляється. Вона оригінально називається Internet Scaner SAFESuite і поширюється компанією Internet Security Systems (ISS - не плутати з Internet Security Scaner) за адресою http://www.iss.net. Для запуску вона вимагає ключ, що пересилається вам при покупці пакета, а в оцінну (evaluation) версію включений ключ, що дозволить вам сканування тільки свого власного хосту.

Ця програма реалізована під 6 платформ:

- сімейство Windows NT,
- HP/UX 9.x і 10.x,,
- AIX 3.2.5 і 4.1,
- Linux (ELF),
- SunOS 4.1.3,
- Solaris (SPARC) 2.x, при цьому кожна з реалізацій знає уразливості й інших платформ.

Функціонально вона складається з трьох частин: сканер FireWall, Web-сканер і сканер Intranet. При цьому, як і в SATAN, користувач набудовує рівень сканування. При цьому він має можливість редагувати наступні зацікавлені класи уразливостей:

- у NFS,
- у RPC,
- у Sendmail/FTP,
- у X Windows,

– IP Spoofing (включаючи можливість пророкування TCP-послідовності й атаки на r-служби),

– відмовлення в обслуговуванні (різні способи),

– наявність користувачів за замовчуванням,

– тестування стандартних демонів і правильності їхніх настроювань,

– правильність настроювань FireWall,

– наявність помилок і правильність адміністрування Web-сервера.

На сьогоднішній день вона є однією з кращих.

ВИСНОВКИ

У дипломній бакалаврській роботі були розглянуті основні складові частини ЛОМ та принципи її побудови. На сьогоднішній день розробка і впровадження ЛОМ є однієї із самих цікавих і важливих задач в області інформаційних технологій. Усе більше зростає необхідність в оперативній інформації, постійно росте трафік мереж усіх рівнів. У зв'язку з цим з'являються нові технології передачі інформації в ЛОМ.

Серед останніх відкриттів слід зазначити можливість передачі даних за допомогою звичайних ліній електропередач, при чому даний метод дозволяє збільшити не тільки швидкість, але і надійність передачі. Мережні технології дуже швидко розвиваються, у зв'язку з чим вони починають виділятися в окрему інформаційну галузь. Учені прогнозують, що найближчим досягненням цієї галузі буде повне витиснення інших засобів передачі інформації (телебачення, радіо, печатка, телефон і т.д.).

На зміну цим «застарілим» технологіям прийде комп'ютер, він буде підключений до деякого глобального потоку інформації, можливо навіть це буде Internet, і з цього потоку можна буде одержати будь-як інформацію в будь-якім представленні. Хоча не можна затверджувати, що усе буде саме так, оскільки мережні технології, як і сама інформатика – наймолодші науки, а все молоде – дуже непередбачено.

У дипломній роботі так само була розглянута проблема забезпечення безпеки інформації в локальній обчислювальній мережі на базі TCP/IP протоколу. Основною вимогою, пропонованим до проектованої ЛОМ, є безпека даних.

Рекомендується застосовувати разом із програмно-апаратними й організаційні міри попередження витоку закритої інформації. Це повинно дати максимальний ефект.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арсенюк І.Р. Комп’ютерні мережі: навчальний посібник / І.Р. Арсенюк, А.А. Яровий Вінниця: ВНТУ, 2020. 145 с.

2. Бабич В.Д. Завадостійкість для каналів зв’язку : навч. посіб. / В.Д. Бабич, О.Д. Кувшинов, О.П. Лежнюк, С. Лівенцев // К.: КВІУЗ, 2021. 150 с.

3. Безрук В. М. Інформаційні мережі зв’язку. Ч. 2. Телекомунікаційні технології стаціонарних мереж зв’язку : навч. посібник / Безрук В. М., Бідний Ю. М., Колтун Ю. М., Астраханцев А. А., Свид І. В., Ширяєв А. В., Харченко Н.А // Харків: ХНУРЕ, 2011. 492 с.

4. Воргуль О.В. Проблеми безпеки при використанні віртуальних приватних мереж / О.В. Воргуль, О.Г. Білоцерківець, А.О. Серіков // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. ЛДУ БЖ, 2020. С. 29-30.

5. Горбатий, І.В. Телекомунікаційні системи і мережі. Принципи функціонування, технології і протоколи : навч. посібник / І.В. Горбатий, А.В. Бондарєв Львів : Видав. Львівської політехніки, 2016. 336 с.

6. Горбатий, І.В. Телекомунікаційні системи і мережі. Принципи функціонування, технології і протоколи : навч. посібник / І.В. Горбатий, А.В. Бондарєв // Львів : Видав. Львівської політехніки, 2016. 336 с.

7. Жидецький В.Ц. Основи охорони праці / В.Ц. Жидецький, В.С. Джигирей, О.В. Мельников // видання 2-е, стереотипне. Львів: Афіша, 2010. 371с.

8. Казимир В.В. Інформаційні основи побудови їх телекомунікаційних мереж / В. В. Казимир, В.А. Литвинов, С.М. Шкарлет, С.В. Зайцев // Вісник Чернігівського держав. техн. універ. Чернігів : ЧДТУ, 2013. 340 с.

9. Кирик М.І. Багаторівнева модель для буферу даних в вузлах обслуговування мультисервісного потоку навантаження / М.І. Кирик, Н.К. Плесканка, Ю.В. Климаш *// Фізико – технолог. проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано - та мікроелектроніки*: матеріал. IV Міжнародн. науково-практичних конференцій (23-25 жовтня 2014 р. м. Чернівці),

2014. С. 110-111.

10. Климаш М.М. Сучасні перетворення в архітектурах розподілених їх систем: монографія / М.М. Климаш, А. Лунтовський, В. Романчук // – Львів-Дрогобич: Коло, 2015. 328 с.

11. Кривуца В.Г. Управління телекомунікаціями з застосуванням новітніх технологій / В.Г. Кривуца, В.К. Стеклов, Л.Н. Беркман, Б. Костік, В. Олійник, С. Скляренко // Підручник для ВНЗ. К.: Техніка, 2007. 384 с.

12. Лунтовський А.О. Етапи розвитку сучасних інфо-телекомунікаційних сервісів та енергетична ефективність мережевих технологій / А.О. Лунтовський, П. Гуськов, А. Масюк // *Вісник Націон. Універ. «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації*. Львів: Вид. Львів. політ., 20 14. № 796. С. 131-139.

13. Лунтовський А. О. Етапи розвитку сучасних інфо-телекомунікаційних сервісів та енергетична ефективність мережевих технологій / А.О. Лунтовський, П. Гуськов, А. Масюк // *Вісник Націон. Універ. «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації*. Львів: Вид. Львів. політ., 20 14. № 796. С. 131-139.

14. Романец, Ю.В. Защита информации в компьютерных системах и сетях / Ю.В .Романец, П.А. Тимофеев, В.Ф. Шаньгин // К. : Зв’язок, 2019. 328 с.

15. Романчук В.І. Дослідження методів для оцінювання якості сприйняття їх послуг для різних типів телекомунікаційних мереж / В.І. Романчук, М. Климаш, Б. Янишин *// Радіоелектроніка і телекомунікації [зб. пр.] / ред. Б.А. Мандзій*. Л. : Вид-тво Нац. ун-т "Львів. Політех.", 2012. № 73. С. 165-172.

16. Стасєв Ю.Б. Комп’ютерні мережі. Технології та протоколи для моделювання: навчал. посіб. / І.В. Рубан, С.В. Дуденко, О.І. Тимочко // – Х.: ХУПС, 2014. 359 с.

17. Стеклов В. К. Інформаційна система: підручник студентам вищих навчальних закладів по напрямку «Телекомунікації» / В.К. Стєклов, Л.Б. Беркман К.: Техніка, 2014. 792 с.