МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА КОМП’ЮТЕРНИХ НАУК

МИХАЛЬСЬКИЙ НАЗАР ВАСИЛЬОВИЧ

УДК 004.73; 004.77

ДОСЛІДЖЕННЯ СИСТЕМ ПІДВИЩЕННЯ ВІДМОВОСТІЙКОСТІ КОРПОРАТИВНИХ МЕРЕЖ

8.05010101 «Інформаційні управляючі системи та технології»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2017

Роботу виконано на кафедрі комп'ютерних наук Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат технічних наук, доцент кафедри комп'ютерних наук
Мацюк Олександр Васильович,
Тернопільський національний технічний університет імені Івана Пулюя

Рецензент: кандидат технічних наук, доцент кафедри інформатики та математичного моделювання
Гащин Надія Богданівна,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 23 лютого 2017 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії №31 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 46, навчальний корпус №1, ауд.701.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Моніторинг мережі може бути дуже корисний для боротьби з хакерами. Хоча вони і зможуть проникнути в мережу непоміченими — або вкравши паролі, або обходячи систему безпеки — вони не зможуть приховати свою діяльність, вже знаходячись усередині. Низькорівневий мережевий монітор може бачити все. Як же виявити хакерів в мережевому оточенні?

Незаконний сервер DHCP є особливо неприємним. Сервер DHCP розташовується в мережі, отримує клієнтський запит IP-адреса, а потім видає свої власні адреси. Вони можуть бути законними або незаконними для мережі або дублювати незаконні адреси, створюючи в мережі великі проблеми. У реальності моніторинг мережі є кращим способом знайти незаконний сервер DHCP. Мережевий монітор Microsoft версії 2 спрощує виконання цього завдання.

Імітація IP-адреса є улюбленим прийомом хакерів, коли один комп'ютер маскує інший, використовуючи IP-адресу іншої машини і потім відповідаючи на запити, адресовані комусь іншому. Можна виявити імітацію адреси, запускаючи утиліту мережевого моніторингу. Імітація IP-адреси може відбуватися також при неправильній конфігурації маршрутизаторів. В цьому випадку машина відповідає на запити, направлені іншій машині з тією ж IP-адресом. Це може викликати великі проблеми, перш ніж помилка буде виявлена.

Очевидно, що непрацюючу плату Ethernet виявити легко. Проте карту, яка вважає себе хорошою і реально передає і отримує час від часу інформацію, знайти значно важче. Це називається нестабільною роботою. Карта Ethernet заповнює мережу фіктивною інформацією, приводячи до уповільнення всієї комунікації в мережі. Це можна виявити за допомогою інструментів моніторингу мережі.

Одне погане застосування може вплинути на будь-яку іншу програму, що працює в мережі. Погані застосування можуть проявити себе безліччю різних способів. Вони можуть шукати файли, які знаходяться не тут, викликаючи зайве навантаження пошуку на сервері, або навіть створювати непотрібний трафік.

Моніторинг мережі чудово допомагає вирішити важкі проблеми з'єднання. Очевидно, що якщо використовується TCP/IP, то для тестування основної комунікації між машинами можна зробити луну-запит (ping). Але це тільки перший крок.

Актуальністю роботи є запровадження технологій проектування відмовостійких корпоративних мереж способом використання відповідних протоколів.

Мета роботи: створення методики проектування відмовостійкої корпоративної мережі.

Об’єкт, методи та джерела дослідження. Діюча корпоративна комп’ютерна мережа.

Практичне значення отриманих результатів.

Розглянуто математичну будову мережі, наведено основні аспекти забезпечення відмостійкості мережі, описано методику створення відмовостійкості корпоративних мереж

Апробація. Окремі результати роботи доповідались на IX Всеукраїнській студентській науково-технічній конференції «Природничі та гуманітарні науки. Актуальні питання» (20-21 квітня 2016 р., м. Тернопіль).

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 8 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 173 арк. формату А4, графічна частина – 9 аркушів формату А1

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі розглянуто актуальність відмовостійкості корпоративних мереж.

В першому розділі розглянуто основи передачі інформації.

В другому розділі розглянуто основи відмовостійкості корпоративних мереж.

В третьому розділі розглянуто питання відмостійких рішень в комутаторах.

В четвертому розділі описано процес проектування відмостійких корпоративних мереж.

В частині "Спеціальна частина" описано виявлення мережевих атак шляхом аналізу трафіка.

В частині "Обґрунтування економічної ефективності" проведено економічні розрахунки, спрямовані на визначення економічної ефективності від дослідження систем підвищення відмовостійкості корпоративних мереж, а також прийнято рішення щодо подальшого розвитку. Розраховано значення економічної ефективності становить 0,559, що є високим значенням. Так само нормальним є термін окупності. Для даного дослідження він становить 1.78 року.

В частині "Охорона праці та безпека в надзвичайних ситуаціях" розглянуто вплив світла на організм людини та оцінку стійкості роботи об'єкта економіки до впливу вражаючої ядерної зброї.

В частині "Екологія" розглянуто роботу з банками екологічної інформації та статистичний аналіз тенденцій і закономірностей динаміки в екології.

У загальних висновках щодо дипломної роботи описано прийняті в роботі технічні рішення.

ВИСНОВКИ

Фундаментальні математичні основи передачі інформації інтенсивно розвивалися протягом останніх 50 років минулого сторіччя, починаючи з робіт Шенона і Котельникова. Із затримкою в декілька десятків років результати цих досліджень почали реалізовуватися на практиці, і сьогодні – тимчасовий етап, коли будь-які елементи теорії передачі інформації реалізуються в реальних системах. Як правило, реалізація цих ідей відбувається на фізичному рівні (PHY) моделі взаємодії відкритих систем (OSI) і іноді на підрівні керування доступом до каналу (MAC) канального рівня.

Всі системи передачі даних об'єднує декілька загальних властивостей.

– Всі системи передачі даних прагнуть використовувати середовище передачі (канал зв'язку) на межі фізичних можливостей, тобто пропускній спроможності, що спричиняє за собою застосування новітніх методів синтезу і прийому сигналів, код і сигнально-кодових конструкцій.

– Всі системи широкосмугового доступу використовують ефективні методи доступу до середовища передачі і мультиплексування повідомлень в цьому середовищі, що спричиняє за собою застосування новітніх методів множинного доступу.

– Всі системи передачі даних для максимізації своєї ефективності використовують стислу інформацію, що спричиняє за собою використання новітніх методів кодування джерела.

– При передачі безперервних повідомлень використовується їх оцифрування і дискретна передача. Якщо на початковому етапі розвитку таких методів оцифрування повідомлення приводило до істотного збільшення смуги сигналу, то тепер оцифроване повідомлення часто займає смугу в три-чотири рази менше початкового аналогового.

– І нарешті, всі системи передачі даних, замінюючи собою вузькополосні і средньополосні системи, істотно розширюють призначені для користувача властивості і приводять до мультисервісності послуг для абонентів.

Інформація — кількісна міра ступеня впорядкованості досліджуваної системи. Інформацією володіють джерело сигналів, приймач сигналів, канал передачі.

Сигнал — функція $s = S\left(t;\overline{p}\right)$, що характеризує процес передачі енергії від джерела (передавача) до приймача через спеціально організоване середовище — канал. У виразі $S\left(t;\overline{p}\right)$ змінна S - енергетична характеристика сигналу (амплітуда, фаза, частота), $\overline{p}$ набір параметрів, t — час. Очевидно, характеристика буде енергетичною, якщо вона виражає безпосередньо енергію сигналу (амплітуда, квадрат амплітуди, потужність) або функціонально пов'язана з енергією (спектральна щільність і ін.). Сигнал аналоговий, якщо його характеристика континуальная (безперервна) величина, і дискретний, якщо S приймає значення з кінцевого або нескінченного дискретного ряду.

Відмовостійкість означає, що проблеми, викликані програмним або апаратним забезпеченням, не приводять до завершення роботи системи, що дозволяє мінімізувати ризик втрати даних. Для забезпечення відмовостійкості застосовуються наступні технології:

– корекція помилок пам'яті;

– самоконтроль критичних компонентів, таких як пам'ять, дискове сховище і мережеі підключення;

– надлишкові пам'ять, дискові масиви, блоки живлення, а також мережеві підключення;

– керування мережевим підключенням.

Щоб створити дійсно відмовостійку мережу, слід розглянути декілька з приведених нижче методів забезпечення надлишкових зв'язків між пристроями в мережі.

– Підтримка командних (teaming) і відмовостійких (failover) з'єднань між серверами і магістральними комутаторами. Подібні мережі забезпечують швидкісні і надлишкові з'єднання між серверами і іншими мережевими пристроями.

– Протокол Hot Standby Router Protocol (HSRP, RFC 2281) і новіший протокол Virtual Router Redundancy Protocol (VRRP, RFC 2338). Ці протоколи дозволяють декільком маршрутизаторам використовувати одну віртуальну IP - адресу і MAC-адресу для швидкого відновлення після збою в роботі маршрутизатора; ці протоколи також забезпечують вирівнювання навантаження.

Відмовостійкість комутаторів – це здатність комутатора або стеку комутаторів обробляти різні аварії, такі як відмови блоків живлення, центральних процесорів, модулів вентиляторів, комутаційної матриці і так далі.

Відмовостійкість комутаторів дуже важлива для будь-якого місця мережі, але вона стає особливо критичною на магістралі через велику кількість сеансів зв'язку, що проходять через центральні комутатори. Оскільки комутатор Passport 8600 позиціонується як магістральний комутатор, в основному будемо розглядати саме його.

Відмовостійкість – це один з основних чинників, який потрібно враховувати при побудові сучасних мереж IP. Більшість корпоративних користувачів переносять у свої мережі IP критичні до якості і надійності застосування, такі як телефонія, відеоконференції, фінанси, електронну комерцію і так далі. І для забезпечення надійної роботи цих застосувань надійність мережі має бути не менше, ніж "п'ять дев'яток" (99.999%).

Рівень надійності мережі залежить від рівня і типу відмовостійких рішень, застосованих в мережі. Відмовостійкість мережі визначається двома чинниками: 1) Рівень надмірності мережевої інфраструктури; 2) Час відновлення мережі, тобто час, необхідний для перемикання потоків даних на працездатні частини мережі у разі відмови її частини.

MLT з'єднання, описані в стандарті IEEE 802.3ad, надають дуже ефективний і зручний метод розподілу навантаження між декількома фізичними з'єднаннями.

Зазвичай при роботі з MLT використовується наступне:

– MLT – Multi-Link Trunk, багатоканальне з'єднання. Це група каналів, об'єднаних в одне логічне з'єднання. Нині MLT найчастіше використовується для з'єднань між комутаторами, проте, є зростаючий попит на використання цієї технології для підключення серверів і робочих станцій, завдяки можливостям по відмовостійкості і розподілу навантаження MLT;

– 802.3ad – стандарт IEEE, що визначає функціональність і реалізацію MLT. Дуже важливо відмітити, що багато виробників мережевого устаткування використовують свої версії MLT, сумісні з IEEE 802.3ad. Проте, на комутаторах Nortel Networks для правильної роботи IEEE 802.3ad необхідно відключити функцію MLT Link Aggregation Control Protocol (LACP);

– Distributed MLT (DMLT) з'єднання відрізняються від стандартних тим, що фізичні канали, що входять в з'єднання, можуть закінчуватися на різних модулях вводу/виводу на шасі або на різних комутаторах в стеку. Ця функція забезпечують кращу відмовостійкість;

– Split MLT (SMLT) з'єднання дозволяють різним фізичним каналам закінчуватися на різних магістральних комутаторах, таким чином, з точки зору пристроїв, підключених до них через стандартний MLT, ці комутатори працюють як один логічний пристрій. SMLT має дуже важливе значення при побудові мереж з надійністю в 99,999%. SMLT ще не є стандартом, ця функція була придумана Nortel Networks кілька років тому, активно використовується в багатьох великих мережах, і нині ведуться роботи по стандартизації SMLT.

ECMP може працювати спільно з такими протоколами маршрутизації як RIP, OSPF і BGP для визначення вартостей маршрутів і пошуку маршрутів з однаковою вартістю, які можуть бути використані для розподілу навантаження і оптимізації пропускної спроможності мережі. Використання протоколів маршрутизації без ECMP і використання їх же спільно з ECMP можна приблизно порівняти з використанням Spanning Tree проти використання MLT, якщо розглядати пропускну спроможність мережі. З точки зору відмовостійкості, ECMP також як і MLT, забезпечує відновлення за долі секунди.

Протокол HSRP дозволяє об'єднати групу маршрутизаторів в один віртуальний маршрутизатор, який і забезпечує маршрут по замовчуванню для кінцевих станцій. Один з маршрутизаторів групи стає активним (active), ще один резервним (standby).

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Н. Михальський. Соціальні медіа / Михальський Н. – Тези доповіді на IX Всеукраїнській студентській науково-технічній конференції «Природничі та гуманітарні науки. Актуальні питання». Том І, Тернопіль, 20-21 квітня 2016 року. – Тернопіль, ТНТУ, 2016. – с. 89-90.

АНОТАЦІЯ

В роботі висвітлено питання побудови відмовостійких мереж.

Одне погане застосування може вплинути на будь-яку іншу програму, що працює в мережі. Погані застосування можуть проявити себе безліччю різних способів. Вони можуть шукати файли, які знаходяться не тут, викликаючи зайве навантаження пошуку на сервері, або навіть створювати непотрібний трафік.

Моніторинг мережі чудово допомагає вирішити важкі проблеми з'єднання. Очевидно, що якщо використовується TCP/IP, то для тестування основної комунікації між машинами можна зробити луну-запит (ping). Але це тільки перший крок.

Актуальністю роботи є запровадження технологій проектування відмовостійких корпоративних мереж способом використання відповідних протоколів.

Об’єктом аналізу є корпоративна мережа.

Метою роботи є створення методики проектування відмовостійкої корпоративної мережі.

Основні результати – розглянуто математичну будову мережі, наведено основні аспекти забезпечення відмостійкості мережі, описано методику створення відмовостійкості корпоративних мереж.

Ключові слова: АНАЛОГОВИЙ, ЦИФРОВИЙ, ПЕРЕДАЧА, ІНФОРМАЦІЯ, ЕНТРОПІЯ ДИСКРЕТНИЙ, КАНАЛ, МОДЕЛЬ, ВІДМОВОСТІЙКІСТЬ, ТОПОЛОГІЯ, ПІДВИЩЕННЯ, ШВИДКІСТЬ, ТРАФІК, МЕРЕЖА, РІШЕННЯ, КЕРУВАННЯ, ПРОТОКОЛ.

ANNOTATION

A network is a noisy enough place. At consideration of network records foremost the enormous volume of data, which is carried on wires every second, strikes the eyes. Strange, that such plenty of data is not lost. We will consider a few methods of diminishing of this "noise". However during optimization of network traffic governed: "Nothing is free of charge" it remains as never just. It is necessary to check at tuning of the operating system, what we renounce, to shorten part of traffic. In many situations it is possible to do changes, casting aside nothing substantial. In any case it must be the carefully self-weighted decision, which leans against the complete understanding of concrete network configuration and functionality, given by the special service or tuning. This analysis and is one of tasks during optimization of network.

One bad application can influence on any other program which works in a network. Bad applications can prove безліччю different methods. They can search files which are not here, causing the superfluous loading of search on a server, or even to create an unnecessary traffic.

Monitoring of network remarkably helps to work out the heavy problems of connection. Obviously, that if TCP/IP is used, then for testing of basic communication between machines it is possible to do an echo-query (ping). But it only the first step.

Actuality of work is an input of technologies of planning of fault-tolerant corporate networks by the method of the use of corresponding protocols.

The object of analysis are corporate networks.

The purpose of work are сторення design techniques of fault-tolerant corporate network.

The basic tasks of work are: the analysis of the state of operating structure of informative space of enterprise, analysis of basic elements which provide fault-tolerant of corporate networks, analysis of decisions of fault-tolerant in switchboards, creation of design technique of fault-tolerant of networks.

Basic results - the mathematical structure of network is considered, basic aspects over of providing of fault-tolerant network are brought, the methods of creation of fault-tolerant of corporate networks are described.

The novelty of the use of such decisions is: providing stable work of corporate network regardless of the state of environment, for this purpose there can be protocols used of Spanning Tree, MLT, ECMP.

Keywords: ANALOG, DIGITAL, TRANSMISSION, INFORMATION, ENTROPY DISCRETE, CHANNEL, MODEL, TOPOLOGY, INCREASE, SPEED, TRAFFIC, NETWORK, DECISION, MANAGEMENT, PROTOCOL.