МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Сімончук Владислав Олегович

Засоби автоматизації переходу з протоколу IPv4 на протокол IPv6 / Automating tools for the transition from IPv4 to IPv6

напрям підготовки: 6.050102 - Комп'ютерна інженерія
фахове спрямування - Комп'ютерні системи та мережі
Бакалаврська робота

Виконав студент групи КСМ-42/1
Сімончук Владислав Олегович

Науковий керівник:
Вербовий С.О.

Тернопіль - 2018

РЕЗЮМЕ

Дипломний проект містить 68 сторінок пояснюючої записки, 14 рисунків, 12 таблиць та 2 додатки. Обсяг графічного матеріалу 2 аркуші формату А3.

Метою проекту є здійснення ефективного переходу на протокол Ipv6 у змодельованій мережі з ефективними основними показниками послуг передачі даних.

До недавнього часу в мережі Інтернет застосовувався тільки протокол IPv4. Якщо подивитися на різницю між четвертою та шостою версією, абсолютно очевидно, що у разі використання IPv4, повна довжина адреси становить 32 біта, IPv6-адреса має розмірність 128 біт, що дозволяє генерувати кількість ймовірних ідентифікаторів, в мільйони разів перевищує можливості четвертої версії. В сенсі перспектив розвитку цієї технології можна сказати, що вона має всі шанси стати найбільш бажаною в усьому світі, оскільки кількість генеруючих 128-бітових адрес настільки велике, що вичерпати їх, навіть у найближчі років п'ятдесят буде просто неможливо.

В даному проекті здійснено моделювання мережі на основі технології IP з версіями 4 і 6 в програмі Packet Tracer. Був виконаний аналіз технологій, що дозволяє мережам IPv4 і IPv6 взаємодіяти між собою та здійснено перехід за методом 6to4. А також здійснено аналіз, який показав, що протокол версії IPv6 швидше і надійніше попередньої версії, незважаючи на більш широке використання IPv4.

У дипломному проекті представлений план і здійснення автоматизації переходу з протоколу IPv4 на протокол IPv6.

В роботі розглянуті аналіз версій протоколу IP та технології взаємодії мереж IPv4 та IPv6, вибір обладнання, метод переходу на IPv6, розрахунок основних параметрів до і після впровадження IPv6.

Ключові слова: МЕРЕЖА, IPv4, IPv6, IP, ПРОТОКОЛ, ІНТЕРНЕТ.

RESUME

The degree project comprises 68 pages explanatory note 14 figures, 12 tables and 2 appendices. The volume of graphic material 2 sheets of A3.

The purpose of the project is to implement an effective transition to the IPv6 protocol in a simulated network with effective core indicators of data services.

Until recently, only the IPv4 protocol was used on the Internet. If you look at the difference between the fourth and sixth versions, it is clear that if using IPv4, the full length of the address is 32 bits, the IPv6 address has a dimension of 128 bits, which allows you to generate the number of probable identifiers, which is millions of times greater than the fourth version. In terms of the prospects for developing this technology, we can say that it has all the chances to become the most desirable in the world, since the number of generating 128-bit addresses is so large that it will be impossible to exhaust them even in the coming years.

In this project, the network modeling based on IP technology with versions 4 and 6 in the Packet Tracer program was implemented. An analysis of technologies was made that allows IPv4 and IPv6 networks to interact with each other and to implement the 6to4 method. An analysis was also conducted that showed that the IPv6 version of the protocol was faster and more reliable than the previous version, despite wider use of IPv4.

The diploma project presents a plan and implementation of automation of the transition from the IPv4 protocol to the IPv6 protocol.

The paper considers the analysis of versions of the IP protocol and the technology of interaction of networks IPv4 and IPv6, the choice of equipment, the method of transition to IPv6, the calculation of the basic parameters before and after the introduction of IPv6.

Keywords: NETWORK, IPv4, IPv6, IP, PROTOCOL, INTERNET.

ЗМІСТ

Вступ 9
1 Основні поняття протоколів IP 11
1.1 Визначення та структура протоколу IP 12
1.2 Аналіз версій протоколу IP 14
1.3 Аналіз технологій взаємодії мереж IPv4 та IPv6 21
1.4 Постановка задач дипломного проекту 24
2 Проектування корпоративної мережі з адресацією IPv4 26
2.1 Розробка логічної структури мережі 27
2.2 Вибір технології локальної та глобальної мережі 29
2.3 Вибір мережевого обладнання 31
2.4 Налаштування локальної мережі в PacketTracer 37
3 Автоматизація переходу з IPv4 на IPv6 40
3.1 Технологія переходу 6to4 41
3.2 Аналіз мережі на основі IPv4 та IPv6 43
3.3 Розрахунок пропускної смуги 46
4 Техніко-економічний розділ 51
4.1 Визначення витрат на оплату праці та відрахувань на соціальні заходи 51
4.2 Розрахунок ціни проекту 57
4.3 Визначення економічної ефективності і терміну окупності капітальних вкладень 58
Висновки 60
Список використаних джерел 61
Додаток А Команди налаштування мережевого обладнання **Ошибка! Закладка не опре**
Додаток Б Довідка про використання ..... **Ошибка! Закладка не определена.**

ВСТУП

В сучасному світі число користувачів глобальної мережі Інтернет зростає з величезною швидкістю. Потреба в інтернеті викликана безліччю наданих їм повноважень і послуг. При здійсненні підключення до глобальної, комп'ютерної мережі Інтернет, використовуються спеціальні протоколи доступу. Одним з нових є протокол IPv6.

Незважаючи на те, що сьогодні існує досить багато протоколів для підключення до інтернету у вигляді найбільш часто використовуваного IPv4 або доступу до поштових серверів, типу POP3 і SMTP. Сама процедура доступу до Всесвітньої павутини полягає в тому, щоб ідентифікувати кожний підключений комп'ютер. При цьому будь-який комп'ютерний або мобільний пристрій повинен мати свій абсолютно унікальний ідентифікатор, що називається адресою. Іншими словами, суть використання будь-якого протоколу полягає в тому, щоб у світі не траплялося жодного повторюваного значення. Це потрібно, щоб відповідь запитуваного сервера або завантаження даних проводилася саме на вказаний пристрій, а не в іншу систему. Сам же протокол відповідає за генерування і присвоєння таких ідентифікаторів. При його залученні створюється унікальна комбінація, яка відповідає кожному пристрою. При цьому саме він генерує практично необмежену кількість таких ідентифікаторів, що за умови розвитку комп’ютерної техніки в наші дні стає особливо актуальним.

До недавнього часу в мережі Інтернет застосовувався тільки протокол IPv4. За версією цього протоколу на IP-адресу виділяється 32 біта. Але так як число користувачів мережі Інтернет невблаганно зростає, то постає питання про загрозу нестачі мережевих адрес. У зв'язку з цим був розроблений прокол IPv6. За версією цього протоколу на IP-адресу користувача виділяється замість 32 біт - 128 біт, що дозволяє значно розширити розмір адресного простору. Також у цього протоколу є ще ряд позитивних сторін у порівнянні з протоколом IPv4: більш ефективна маршрутизація, підтримка якості обслуговування (Qos),

полегшення заголовка, автоматична конфігурація адрес і інші.

Найбільш використовуваним протоколом мережевого рівня в стеці протоколів TCP / IP є протокол IP, головне завдання якого - забезпечення передачі пакетів даних в мережах, які складаються з певної кількості дрібніших мереж. Саме це пояснює те, що протокол IP прекрасно проявляє себе в мережах подібних топологій і раціонально користуючись наявністю підсистем і дбайливо витрачає задану пропускну спроможність ліній зв'язку з низькими швидкостями передачі даних. IP об'єднує передачу пакетної інформації від одного вузла до іншого вузла IP-мережі, не налаштовуючи при цьому з'єднання між відправником і отримувачем інформації.

Дана тема актуальна тим, що IPv6 поки ще не так поширений в світі, як IPv4, але настане день, коли IPv4 вичерпає свій адресний простір, і тоді всім доведеться вирішувати одну з найгостріших проблем - як найбільш ефективно здійснити перехід на нову версію протоколу, одним з плюсів якого є величезний адресний простір.

Метою дипломної роботи є здійснення ефективного переходу на протокол Ipv6 у змодельованій мережі з ефективними основними показниками.

Необхідно вирішити такі завдання:

- проаналізувати існуючі версії протоколу IP;
- створити логічну структуру мережі;
- здійснити моделювання мережі на основі технології IP з версіями 4 і 6;
- вибрати найбільш оптимальний метод переходу на IPv6;
- провести розрахунок основних параметрів до і після впровадження IPv6;
- розрахувати економічну ефективність проекту.

1 ОСНОВНІ ПОНЯТТЯ ПРОТОКОЛІВ IP

Інтернет складається з багатьох тисяч корпоративних, наукових, урядових та домашніх мереж. Об'єднання різнорідних по архітектурі мереж стало можливо завдяки протоколу IP (англ. Internet Protocol) і принципу маршрутизації пакетів даних. Протокол IP був спеціально створений агностичним по відношенню до фізичних каналів зв'язку. Тобто будь-яка мережа передачі цифрових даних може передавати інтернет-трафік. На стиках мереж спеціальні маршрутизатори займаються сортуванням та перенаправленням пакетів даних, базуючись на IP-адресах одержувачів цих пакетів. Протокол IP утворює єдиний адресний простір у масштабах всього світу, але в кожній окремо взятій мережі може існувати свій власний адресний підпростір. Така організація IP-адрес дозволяє маршрутизаторам однозначно визначати подальший напрямок для кожного, навіть найменшого, пакету даних. В результаті між різними мережами Інтернету не виникає конфліктів і дані точно і без перешкод передаються від мережі до мережі по всій планеті.

Сам протокол IP був народжений в дискусіях всередині організації IETF (англ. Internet Engineering Task Force, Task force − група спеціалістів, покликана вирішити певну задачу), назву котрої можна перекласти як «Група для вирішення задач проектування Інтернету». IETF і її робочі групи досі займаються розвитком протоколів Всесвітньої мережі. Вона відкрита для публічної участі та обговорень. Комітети цієї організації публікують т.зв. документи RFC (англ. Request for Comments − запит коментарів). В цих документах даються технічні специфікації і точні пояснення багатьох питань. Деякі документи RFC організація IAB (англ. Internet Architecture Board − Рада по архітектурі Інтернету) оголошує Стандартами Інтернету. З 1992 року IETF, IAB та ряд інших організацій утворюють Товариство Інтернету (англ. Internet Society, ISOC) − організаційну основу для різноманітних дослідницьких та консультативних груп, що займаються розвитком Інтернету.

В даному випадку протокол − це спосіб взаємодії, обміну даними між комп’ютерами при роботі у мережі. Щоб різні комп’ютери могли разом працювати, вони повинні «розмовляти однією мовою», тобто використовувати однакові протоколи. Сукупність цих протоколів називають стеком протоколів TCP/IP (TCP/IP − це абревіатура терміну Transmission Control Protocol / Internet Protocol (Протокол керування передачею / Протокол Internet). Фактично TCP/IP не один протокол, а декілька.

Фактично TCP/IP представляє цей базовий набір протоколів Інтернету, відповідальний за розбивку вихідного повідомлення на пакети (TCP), доставку пакетів на вузол адресата(IP) і збирання (відновлення) вихідного повідомлення з пакетів (TCP)).

1.1 Визначення та структура протоколу IP

IP-протокол — найпоширеніша реалізація ієрархічної схеми мережевої адресації. Використовуваний в мережі Інтернет, протокол відповідає за адресацію пакетів, але не відповідає за встановлення з'єднань, не є надійним і дозволяє реалізувати тільки негарантовану доставку даних. Термін «протокол без встановлення з'єднань» (англ. connectionless) означає, що протокол для взаємодії не потребує виділеного каналу, як це відбувається під час телефонної розмови і не існує процедури виклику перед початком передачі даних між мережевими вузлами. Протокол IP вибирає найефективніший шлях з числа доступних на основі рішень прийнятих протоколом маршрутизації. Відсутність надійності і негарантована доставка не означає, що система працює погано або ненадійно, а вказує лиш на те, що протокол IP не докладає ніяких зусиль, щоб перевірити чи був пакет доставлений за призначенням. Ці функції делеговані протоколам транспортного та вищих рівнів. Транспортний рівень також

відповідає за збірку пакетів у повідомлення в потрібній послідовності. Інкапсуляція

Інформація, проходячи вниз по рівням моделі OSI, на кожному рівні певним чином обробляється протоколами цього рівня.

Протокол IP розпізнає формат заголовка пакета (адресну частину та іншу службову інформацію включно), але ніяким чином не аналізує і не піклується про фактичні дані. Він приймає і передає будь-які дані, передані протоколами верхніх рівнів.

IP-пакети складаються з даних верхнього рівня та IP-заголовку. За специфікацією протоколу, пакет має бути не більший за 65535 бітів (з заголовком та даними включно).

Версія (Version) — 4-бітове поле, що описує використовувану версію протоколу IP. Всі пристрої зобов'язані використовувати протокол IP однієї версії, пристрій що використовує іншу версію буде відкидати пакети.

Довжина IP-заголовку (IP header Length — HLEN) — 4-бітове поле, що описує довжину заголовку пакету в 32-бітових блоках. Це значення — це повна довжина заголовку з врахуванням двох полів змінної довжини.

Тип обслуговування (Type of Service — TOS) — 8-бітове поле, що вказує на ступінь важливості інформації, що привласнена протоколом верхнього рівня.

Загальна довжина (Total Length) — 16-бітове поле, що описує довжину пакету в байтах, із заголовком та даними включно. Для того щоб вирахувати довжину блока даних, потрібно від повної довжини відняти значення поля HLEN.

Ідентифікація (Identification) — шістнадцятибітове поле, що зберігає ціле число, яке описує даний пакет. Це число являє собою послідовний номер.

Прапорці (Flags) — 3-бітове поле, в якому два молодших біта контролюють фрагментацію пакетів. Перший біт визначає чи було пакет фрагментовано, а другий чи є цей пакет останнім фрагментом в серії фрагментів.

Зміщення фрагментації (Fragment Offset) — 13-бітове поле, що допомагає зібрати разом фрагменти пакетів. Це поле дозволяє використовувати 16 бітів в сумі для прапорів фрагментації.

Час життя (Time-to-Live — TTL) — 8-бітове поле — лічильник, в якому зберігаються послідовно зменшуване значення кількості пройдених вузлів (роутерів, що їх ще іноді в цьому випадку називають хопами (hops)) на шляху до місця призначення. У випадку коли лічильник пройдених хопів дорівнюватиме нулю — пакет буде відкинуто, таким чином попереджується нескінченна циклічна пересилка пакетів.

Протокол (Protocol) — 8-бітове поле, що вказує на те, який протокол верхнього рівня отримає пакет, після завершення обробки IP-протоколом. Наприклад TCP або UDP.

Контрольна сума заголовку (Header Checksum) — 16-бітове поле, що допомагає перевірити цілісність заголовку пакету.

1.2 Аналіз версій протоколу IP

IPv4 — четверта версія мережевого протоколу IP. Перша версія протоколу, яка набула широко розповсюдження. Протокол IPv4, описаний у RFC 791 (вересень 1981 року), прийшов на заміну описаному у RFC 760 (січень 1980 року). Використовує 4 байтну форму запису адрес пристроїв в комп’ютерній мережі.

IPv4 використовує 32-бітні (4 байтні) адреси, які обмежують адресний простір 4 294 967 296 (себто 28×4) можливими унікальними адресами.

Формою запису IP-адреси (IPv4) зазвичай є запис у вигляді 4 десяткових чисел від 0 до 255 (28), розділених крапками, наприклад: 127.0.0.1 (посилання пристрою на самого себе), або 91.198.174.225.

Деякі адреси IPv4 зарезервовані для спеціальних цілей та не можуть бути глобально маршрутизованими (доступними з будь-якого пристрою, що підключений до мережі інтернет). Так для приватних IP-адрес в локальних мережах зарезервовано близько 18 млн адрес. Ще близько 270 млн адрес зарезервовано для групових передач (англ. multicast).

Обмежене число унікальних адрес у ~4.3 млрд у зв'язку з бурхливим розвитком Інтернету та резервуванням діапазону ~290 млн було вичерпане. 3 лютого 2011 року організація IANA видала останні 5 блоків IP-адрес організації Регіональних Інтернет Регістрів (RIR). Задля вирішення цієї проблеми ще з 1990-их розвивався протокол IPv6, запущений з 2006 року.

Оцінки повного вичерпання IPv4 адрес різнились у 2000-их, були різні прогнози. Так у 2003 році директор APNIC Пол Уілсон (англ. Paul Wilson) заявляв, що виходячи з темпів розростання мережі Інтернет, вільного адресного простору вистачить на одне—два десятиліття. У вересні 2005 року компанія Cisco Systems зазначила, що кількість доступних адрес вистачить на 4—5 років. У вересні 2010, виходячи з даних IANA, вся кількість адрес IPv4 буде виділена реєстратурам (RIR) до середини 2011 року, в листопаді ця дата була перенесена на березень 2011. 3 лютого 2011 року IANA виділила останні п'ять блоків IP-адрес /8 (IPv4).

IPv4 Header Format

Відступ	Октет	0								1								2								3							
Октет	Біт	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8	23	22	21	20	19	18	17	16	31	30	29	28	27	26	25	24
0	0	Версія				Розмір заголовку				Differentiated Services Code Point						Explicit Congestion Notification		Розмір пакету (повний)															
4	32	Ідентифікатор																Прапори			Зміщення фрагменту											
8	64	Час життя								Протокол								Контрольна сума заголовку															
12	96	IP-адреса джерела																															
16	128	IP-адреса призначення																															
20	160	Опції (якщо розмір заголовку > 5)																															
20 або 24+	160 або 192+	Дані																															

Рисунок 1.1 – Структура пакету IPv4

Як видно з рисунку 1.1 пакет IP містить 14 полей, з яких 13 є обов'язковими. Чотирнадцяте поле призначене для необов'язкових опцій. Поля використовують порядок байтів від старшого до молодшого, старші біти йдуть

першими. Перший біт має номер 0. Таким чином, наприклад, поле знаходиться в чотирьох старших бітах першого байту. При передачі багатооктатних значень старший октет передається першим.

Першим полем пакета є версія протоколу розміром в чотири біта. Для IPv4 це 4.

Наступні чотири біти містять заголовок пакета в 32-бітних словах. Оскільки число опцій не постійне, вказання розміру важливо для відділення заголовку від даних. Мінімальне значення дорівнює 5 (5 × 32 = 160 біт, 20 байт), максимальне - 15 (60 байт).

Спочатку називалося «тип обслуговування» (Type of Service, ToS), в даний час визначається RFC 2474, як «Differentiated Services». Використовується для поділу трафіку на класи обслуговування, наприклад, для установки чутливого до затримок трафіку, такого як VoIP, більшого пріоритету.

Покажчик перевантаження (Explicit Congestion Notification, ECN). Попередження про перевантаження мережі без втрати пакетів є необов'язковою функцією і використовується тільки якщо обидва хоста її підтримують.

16-бітний повний розмір пакета в байтах, включаючи заголовок і дані. Мінімальний розмір дорівнює 20 байт (заголовок без даних), максимальний - 65535 байт. Хости повинні підтримувати передачу пакетів розміром до 576 байт, але сучасні реалізації зазвичай підтримують набагато більший розмір. Пакети більшого розміру, ніж підтримує канал зв'язку - фрагментуються.

Переважно використовується для ідентифікації фрагментів пакета, якщо він був фрагментований. Існують експерименти щодо його використання для інших цілей, таких як додавання інформації про трасування пакета для спрощення відстеження шляху пакета з підробленою адресою джерела.

Поле розміром три біта містить прапори контролю над фрагментацією. Біти, від старшого до молодшого, означають:

0: зарезервовано, має дорівнювати 0;

1: не фрагментувати;

2: У пакета ще є фрагменти.

Якщо встановлений прапор «Не фрагментувати», то в разі необхідності фрагментації такий пакет буде знищений. Може використовуватися для передачі даних хостам, які не мають достатніх ресурсів для обробки фрагментованих пакетів.

Прапор «є фрагменти» повинен бути встановлений в 1 у всіх фрагментів пакета, крім останнього. У нефрагментованих встановлюється в 0 - такий пакет вважається власним останнім фрагментом.

Поле розміром в 13 біт вказує зсув поля даних поточного фрагмента щодо початку поля даних першого фрагментованного пакета в блоках по 8 байт. Дозволяє (213-1) × 8 = 65528 байт зміщення. При обліку розміру заголовка підсумкове зміщення може перевищити максимальний розмір пакета (65528 + 20 = 65548 байт). Перший фрагмент в послідовності має нульовий зсув.

Визначає максимальну кількість маршрутизаторів на шляху проходження пакету. Наявність цього параметра не дозволяє пакету нескінченно ходити по мережі. Кожен маршрутизатор при обробці пакету повинен зменшити значення TTL на одиницю. Пакети, час життя яких стало дорівнювати нулю, знищуються, а відправнику надсилається повідомлення ICMP Time Exceeded. На відправку пакетів з різним часом життя засноване трасування їх шляху проходження (traceroute). Максимальне значення TTL = 255. Звичайне початкове значення TTL = 64 (залежить від ОС). Вказує дані якого протоколу IP містить пакет (наприклад, TCP або ICMP).

16-бітна контрольна сума, яка використовується для перевірки цілісності заголовка. Кожен хост або маршрутизатор порівнює контрольну суму заголовка зі значенням цього поля і відкидає пакет, якщо вони не збігаються. Цілісність даних IP не перевіряє - вона перевіряється протоколами більш високих рівнів (такими, як TCP або UDP), які теж використовують контрольні суми.

Оскільки TTL зменшується на кожному кроці проходження пакета, сума теж повинна обчислюватися на кожному кроці. Метод перерахунку контрольної суми визначений в RFC 1071.

32-бітова адреса відправника пакета. Може не збігатися з реальною адресою відправника через трансляцію адрес.

За адресою призначення може слідувати поле додаткових опцій, але воно використовується рідко. Розмір заголовка в цьому випадку повинен бути достатнім, щоб вмістити всі опції (з урахуванням доповнення до цілого числа 32-бітових слів).

Уже в 1980-і роки стало очевидно, що розподіл адресного простору відбувається значно швидшими темпами, ніж було закладено в архітектуру IPv4. Це призвело спочатку до появи класової адресації, пізніше безкласової адресації, і в кінцевому підсумку до розробки нового протоколу IPv6.

У лютому 2011 року IANA виділила 5 останніх блоків адрес RIRам. Блоки вільних IP-адрес почали закінчуватися у регіональних реєстраторів з 2011 року.

IPv5 (англ. Internet Protocol version 5) — це експериментальний протокол для UNIX-систем. Згідно зі стандартною UNIX (операційної системи комп'ютера) випуск конвенцій, всі непарні версії вважаються експериментальними. Він ніколи не був призначений для використання широкою публікою.

Інтернет співтовариство зробило спробу створити протокол, зручний для мовлення голосових і відео даних. Було це в кінці 70-х років. Так був створений в експериментальних цілях протокол ST - Internet Stream Protocol (RFC-1819). Трохи пізніше цей протокол був модернізований в ST2 і почав використовуватися в комерційних проектах таких брендів, як IBM, Sun, NeXT, Apple. Цей протокол відрізнявся від IPv4 тим, що вмів встановлювати з'єднання і підтримував стандарти QoS, але він планувався лише як доповнення до IPv4 для вузького кола користувачів і не увійшов в TCP / IP. Саме ST і ST2 було присвоєно номер версії 5, хоча його так і не назвали IPv5, хіба що неформально. Але цього вистачило для того, щоб перескочити в офіційній нумерації через цифру 5. Більш того, спочатку протоколу IPng хотіли привласнити цифру 7 по безглуздій помилці творців. Але перечитавши RFC помилка була виправлена до виходу протоколу в світ. Вперше принцип маршрутизації по «мітках» для

протоколу ST був викладений в IEN-119 (в 1979 році). IEN публікував замітки однієї з спільнот всередині DARPA в 80-их роках. Після 1982 року було прийнято рішення масового переходу на протокол TCP / IP, в результаті чого ST так і залишився заміткою з журналу експериментальних пропозицій.

IPv6 — нова версія IP-протоколу — IP версії 6. Розробка протоколу IPv6 почалася 1992 року, а з 2003 р. його підтримку забезпечують виробники більшості телекомунікаційного устаткування (корпоративного рівня). IPv6 — новий крок у розвитку Інтернету. Цей протокол розроблено з урахуванням вимог до Глобальної мережі, що постійно зростають. 3 лютого 2011 року IANA виділила останні п'ять блоків IP-адрес /8 (IPv4). Найбільш суттєва різниця між IPv4 та IPv6 полягає в тому, що раніше на інтернет-адресу виділяли 4 байти (32 біта), що відповідає стандартній на сьогодні чотирьохблоковій адресі IP, а протокол IPv6 виділяє на адресу 16 байтів (128 біт). Це відповідає 340 трильйонам адрес (3,4x1038) або по 5x1028 адрес на кожну людину. Вночі 5 лютого 2008 року організація ICANN, яка наглядає за використанням інтернет-протоколів, почала додавати в DNS-сервери записи, що містять адреси у форматі протоколу IPv6. Це поклало початок переходу з нинішнього протоколу IPv4 на сучасніший IPv6. У квітні 2009 у мережі UA-IX запущено процес перевірки протоколу IPv6. У числі перших компаній, що ухвалили рішення про участь в тестуванні — «ТопНЕТ» і «Датагруп». Вони встановили IPv6 BGP-з'єднання з маршрутизатором UA-IX, і здійснили обмін маршрутною інформацією між ними. У квітні 2011 розпочалось масове впровадження IPv6 серед домашніх користувачів інтернет.

Основна причина появи IPv6 (за винятком менш істотних змін) - це рішення проблеми вичерпання адресного простору, тобто зміна структури пакетів транспорту і довжини адрес.

Наприкінці 1980-х стала очевидною нестача адресного простору Інтернет. На початку 1990-х, навіть після введення безкласової адресації, виявилось, що однієї економії та використання NAT'у буде замало для попередження вичерпання адресного простору, і необхідна зміна адресації. Крім того,

накопичилась певна кількість пропозицій щодо усунення недоліків наявної моделі Інтернет. Наприкінці 1992 року IETF оголосила конкурс на створення протоколу Інтернет наступного покоління (англ. IP Next Generation — IPng). 25 липня 1994 року IETF ствердила модель IPng з утворенням кількох робочих груп IPng. У 1996 було створено серію RFC, що визначали новий протокол Інтернету. Оскільки версія 5 вже була раніше призначена експериментальному протоколу передачі мультимедійних потоків, новий протокол отримав версію 6.

Зміщення в байтах		0								1								2								3							
	Відступ в бітах	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Traffic Class								Flow Label																			
4	32	Payload Length																Next Header								Hop Limit							
8	64	Source Address																															
C	96																																
10	128																																
14	160																																
18	192	Destination Address																															
1C	224																																
20	256																																
24	288																																

Рисунок 1.2 – Структура пакету IPv6

Як видно з рисунка 1.2 опис полів: Version - версія протоколу. Для IPv6 це значення дорівнює 6 (значення в бітах — 0110). Traffic class - пріоритет пакету (8 біт). Це поле містить два параметри. Старші 6 біт використовуються DSCP для класифікації пакетів. Решта два біта використовуються ECN для контролю перевантаження. Flow label - відмітка потоку. Payload length на відміну від поля Total length протоколу IPv4 дане поле не включає заголовок пакету (16 біт). Максимальний розмір, що визначається розміром поля — 64 Кбайти. Для пакетів більшого розміру використовується Jumbo payload. Next header - вказує тип розширеного заголовку, що розміщений одразу за основним. В останньому розширеному заголовку поле Next header вказує тип транспортного протоколу (TCP, UDP і т. д.) Hop limit – аналог поля time to live в IPv4 (8біт).

Таблиця 1.1 – Зарезервовані адреи IPv6

IPv6 адреса	Довжина префікса (біти)	Опис	Примітки
::	128	-	0.0.0.0 в IPv4
::1	128	Loopback адреса	127.0.0.1 в IPv4
::xx.xx.xx.xx	96	Вбудований IPv4	Нижні 32 біти – це IPv4 адреса. Також називається IPv4-сумісною IPv6 адресою. Застарілий, більше не використовується.
::ffff:xx.xx.xx.xx	96	Адреса IPv6, що відображена на IPv4	Нижні 32 біти – це IPv4 адреса. Для хостів, що не підтримують IPv6.
2001:db8::	32	Документування	Зарезервовано для прикладів в документації в rfc3849
fe80:: — febf::	10	Link-local	Аналог 169.254.0.0/16 в IPv4
fec0:: — feff::	10	Site-local	Відмічений як застарілий в rfc3879
fc00::	7	Unique Local Unicast	Прийшов на заміну Site-Local rfc4193
ffxx::	8	Multicast	

Таблиця 1.1 містить інформацію про зарезервовані адреси в IPv6 та їх опис.

1.3 Аналіз технологій взаємодії мереж IPv4 та IPv6

Спочатку вузли, що підтримують протокол IPv6 не пропонують необхідних сервісів. Тому є необхідні вимоги для вузлів IPv6: можливість взаємодії з вузлами IPv4; можливість передачі пакетів IPv6 через існуючу інфраструктуру IPv4.

З вище сказаного випливає, що необхідні механізми, які забезпечуватимуть співіснування мереж IPv4 і IPv6. Цей симбіоз систем, що використовують різні

стеки протоколів в більшості випадках здійснюється за допомогою застосування наступних методів.

- Трансляція. Трансляція відповідає за узгодження стеків протоколів шляхом конвертації форматів повідомлень. Крім цього даний процес включає в себе: надання адрес вузлів і мереж, які різним чином задаються цими протоколами. Даний сервіс можуть здійснювати: програмний або апаратний шлюз, міст, комутатор, маршрутизатор та інше мережеве обладнання. Розташування транслюючого елемента знаходиться між взаємодіючими мережами. Дана дислокація наділяє цей пристрій правами посередника при передачі повідомлень з мережі, що використовує один протокол в мережу, яка використовує інший протокол.

- Мультиплексування. В процесі мультиплексування в мережеве обладнання або в серверні ОС поміщаються кілька стеків протоколів. На вузлах мережі поміщається певна кількість стеків комунікаційних протоколів, в залежності від числа мереж, що використовують різні мережеві протоколи. Необхідно налаштувати безперебійну обробку запитів певних протоколів. Для цього використовується спеціальний програмний елемент - мультиплексор протоколів або протокольний менеджер, в завдання якого входить визначення шляху призначення запиту, відправленим клієнтом.

- Інкапсуляція. Даний процес є одним з методів, який надає допомогу при взаємодії мереж, що використовують різні мережеві протоколи. Інкапсуляція застосовна, в необхідності здійснення взаємодії двох мереж з однією технологією за допомогою транзитної мережі, в якій використовується інша технологія.

Протоколи які беруть участь в тунелюванні:

- протокол інкапсуляції;

- транспортуємий протокол;

- несучий протокол.

Протокол який транспортується - це протокол на чию частку припадає синдикат мереж, протокол транзитної мережі за визначенням буде несучим.

Протокол інкапсуляції допомагає пакетам транспортуємого протоколу поміщатися в поле даних несучого протоколу. У змішаних мережах IPv4-IPv6 найбільш використовуваними методами є: мультиплексування і тунелювання. Дані методи дозволяють вузлам мережі, що використовує протокол IPv6, проводити обмін з вузлами іншої IPv6 мережі за допомогою мережі, в якій застосовується протокол IPv4. Для того, щоб вузли, які підтримують протокол IPv6, мали можливість звертатися до ресурсів мережі IPv4, необхідні спеціальні сервіси: шлюзи транспортного і прикладного рівня, транслятори протоколів тощо. Зараз розробляються механізми, які надавали б можливість протоколу IPv6 без перешкод діяти поверх мереж, які підтримують тільки протокол IPv4.

Механізм мультиплексування надає одночасну підтримку вузлам двох стеків протоколів. Здійснюється це, щоб кожен вузол мав 2 адреси: IPv4 і IPv6. Дані адреси не мають зв'язків один до одного. Унікальність адрес IPv4 повинна зберігатись. До того моменту, як адресний простір IPv4 вичерпає себе повністю, процес переходу на IPv6 повинен зайти досить далеко, щоб недавно підключені вузли мали можливість отримання всіх необхідних послуг, використовуючи виключно засоби протоколу IPv6.

Інкапсуляція довгий час застосовується в IPv4 для передачі не IP- пакетів. У випадку з IPv6 застосовується механізм інкапсуляції. Пакет IPv6 поміщається в поле даних пакета IPv4, потім транспортується по мережі IPv4. На момент прибуття в пункт призначення пакет IPv6 виходить з поля даних пакета IPv4 і йде на обробку звичайним чином. У нього є два шляхи: 1 або він транспортується далі (це відбувається вже по IPv6-мережі), і 2 - або він використовується одержувачем. Несучим протоколом є IPv4, а який транспортується IPv6. Протокол IPv4 грає роль протоколу канального рівня з точки зору IPv6, тому поле HopLimit в пакеті IPv6 буде зменшено тільки на одиницю (якщо буде потрібно подальше перенаправлення пакета). Зазвичай цілий маршрут пакета даних IPv6 підключає безліч тунелів по транзитних мережах IPv4. Наявність механізму інкапсуляції збільшує функціональні можливості вузлів, які є кінцевими точками тунелю. Велика сила накладає

велику відповідальність. Вузол який приймає дані має впізнати пакет IPv6 в поле даних пакета IPv4. Перевірка в заголовку пакета IPv4 поля «Протокол» провидится саме з цією метою. Значення цього поля в даному випадку має дорівнювати десятковому числу 41.

Максимально можливий розмір пакета - MTU, який повинен відправитися через інтерфейс IPv6 - 12240 біт. З метою, щоб запобігти фрагментацію, система використовує значення MTU пакета IPv6, які разом з заголовком помістилися в дозволеному значенні MTU пакета IPv4.

Під час прийому пакета IPv4, який несе в середині поля даних пакет IPv6, система повинна звичайним чином відфільтрувати трафік по вихідній адресі, пакет ігнорується, якщо це спец-адреса для широкомовної або багатоадресної розсилки і якщо цей вихідний адрес дорівнює 0.0.0.0 або 127. x.x.x. Потім ігнорується тунелюючий заголовок пакета IPv4, і методи фільтрації застосовні вже до пакету IPv6. Протокол IPv6 так само має особливі адреси. Це адреси багатоадресної розсилки, невизначені адреси, особливі адреси, отримані відображенням IPv4 на IPv6, а також адреси зворотної петлі. Потім віддається IPv6 стеку і піддається обробці, як нормальний пакет даних IPv6.

Обробка інших повідомлень IPv4 залежить від того, що будь-яка частина повідомлення, яка викликала помилку міститься в ICMP-пакеті. Залежно від передачі ICMP, повідомлення цього протоколу крім зовнішнього заголовка IPv4 може містити 8 і більше байт поля пакета IPv4, якому належить це керуюче повідомлення. Якщо цих даних достатньо для реконструкції заголовка IPv6, то генерується повідомлення ICMPv6 і відправляється вузлу-джерелу IPv6.

1.4 Постановка задач дипломного проекту

Якщо подивитися на різницю між четвертою та шостою версією, абсолютно очевидно, що у разі використання IPv4, повна довжина адреси

становить 32 біта, IPv6-адреса має розмірність 128 біт, що дозволяє генерувати кількість ймовірних ідентифікаторів, в мільйони разів перевищує можливості четвертої версії. В сенсі перспектив розвитку цієї технології можна сказати, що вона має всі шанси стати найбільш бажаною в усьому світі, оскільки кількість генеруючих 128-бітових адрес настільки велике, що вичерпати їх, навіть у найближчі років п'ятдесят буде просто неможливо. І, судячи з усього, незабаром можна буде прогнозувати відмову від підтримки четвертої версії, а на перше місце все-таки вийде шоста, незважаючи навіть на гучні заяви конкурентів про те, що вони можуть уявити щось абсолютно нове.

У даній дипломній роботі необхідно проаналізувати існуючі версії протоколу IP. Створити логічну структуру підприємства, після чого змоделювати її та здійснити вибір мережевого обладнання. Виконати перехід з протоколу Ipv4 на IPv6. Ефективність після переходу на IPv6 має бути доведена за допомогою замірів і розрахунків основних показників комп'ютерних мереж. В економічній частині обгрунтовати економічний ефект впровадження даного проекту на підприємстві.

2 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ З АДРЕСАЦІЄЮ IPV4

Мережі − це системи, що формуються каналами. Мережі використовують у таких формах: система доставки пошти; телефонна система; система громадського транспорту; корпоративна комп'ютерна мережа; Інтернет. Мережі дозволяють обмінюватися інформацією і використовувати різні методи контролю над способом її передачі. Дані по мережі передаються з одного пункту до іншого, іноді різними шляхами, і зрештою доставляються в необхідний пункт призначення.

У комп'ютерній мережі також діють правила для керування потоком даних між вузлами мережі. Вузол − це будь-який пристрій, що відправляє та отримує інформацію з мережі. Окремі пристрої можуть служити або як вузли, або як периферійні пристрої. Наприклад, принтер, підключений до ноутбука, який у свою чергу підключений до мережі, виступає як периферійний пристрій. Якщо ж принтер підключений до мережі безпосередньо, він функціонує як вузол.

До мережі можна підключити різні типи пристроїв: настільні комп'ютери; ноутбуки; планшетні комп'ютери; смартфони; принтери; файлові сервери і сервери друку; ігрові консолі; домашні пристрої. Комп'ютерні мережі використовуються по всьому світу в організаціях, школах, державних установах і вдома. Багато мереж підключені один до одного через Інтернет, що дозволяє обмінюватися різними типами ресурсів і даних: послугами (наприклад, друк або сканування); ємністю системи зберігання на знімних пристроях (таких як жорсткі диски або оптичні); застосуванням (наприклад базами даних); інформацією, що зберігається на інших комп'ютерах; документами; календарем (наприклад, синхронізуючи його між комп'ютером і смартфоном). Мережні пристрої для підключень і передачі інформації можуть використовувати різні типи середовища передачі даних: мідні кабелі - застосовуються електричні сигнали; волоконно-оптичні кабелі - застосовуються світлові імпульси;

бездротові підключення - застосовуються радіосигнали, інфрачервона технологія та супутниковий зв'язок.

Адреса IPv4 являє собою серію з 32 біт (одиниць і нулів). Людині важко прочитати двійкову адресу IPv4. Тому 32 біти групуються по чотири восьмибітних сегменти − в так звані октети. Навіть у такому форматі людині складно читати, записувати і запам'ятовувати адреси IPv4. Тому кожен октет поданий у вигляді десяткового значення, відокремленого крапкою. Цей формат називається точково-десятковою нотацією.

Логічна 32-бітна адреса IPv4 являє собою ієрархічну систему і складається з двох частин. Перша ідентифікує мережу, друга − вузол у цій мережі. Обидві частини є обов'язковими.

Працювати зі 128-бітними числами важко, тому 128 бітів в адресах IPv6 подають у вигляді 32 шістнадцяткових чисел, які у свою чергу поділяються на вісім груп з чотирьох шістнадцяткових чисел. Як роздільник використовується двокрапка. Кожна група з чотирьох шістнадцяткових значень називається блоком.

2.1 Розробка логічної структури мережі

У мережах з невеликим числом комп'ютерів (10-30) найчастіше використовується одна з типових топологій – загальна шина, кільце, зірка або повнозв’язна мережа. Усі перераховані топології мають властивість однорідності, тобто всі комп'ютери в такій мережі мають однакові права у відношенні доступу до інших комп'ютерів (за винятком центрального комп'ютера при з'єднанні зірка). Така однорідність структури робить простою процедуру нарощування числа комп'ютерів, полегшує обслуговування й експлуатацію мережі.

Схема логічної структури мережі підприємства, яке має 4 відділи: директор, бухгалтерія, технічний відділ та загальний відділ представлена на ДП.КСМ.07256/16.00.00.000 С1.

На підприємстві знаходиться 7 комп’ютерів, 1 ноутбук, 2 принтери, 2 свіча та 3 роутери.

Фізична структуризація мережі корисна в багатьох випадках, однак іноді, в мережах великого і середнього розміру, неможливо обійтися без логічної структуризації мережі. Найбільш важливою проблемою, яка не розв'язується шляхом фізичної структуризації, залишається проблема перерозподілу переданого трафіка між різними фізичними сегментами мережі

У великій мережі виникає неоднорідність інформаційних потоків: мережа складається з безлічі підмереж робочих груп, відділів, філій підприємства й інших адміністративних утворень. Дуже часто найбільш інтенсивний обмін даними спостерігається між комп'ютерами, що належать до однієї підмережі, і тільки невелика частина звертань відбувається до ресурсів комп'ютерів, що знаходяться поза локальними робочими групами.

План приміщення підприємства зі всіма відділами представлено на ДП.КСМ.07256/16.00.00.001 С1.

Мережа з типовою топологією (шина, кільце, зірка), у якій усі фізичні сегменти розглядаються в якості одного поділюваного середовища, виявляється неадекватній структурі інформаційних потоків у великій мережі. Наприклад, у мережі з загальною шиною взаємодія будь-якої пари комп’ютерів займає її на увесь час обміну, тому при збільшенні числа комп’ютерів у мережі шина стає вузьким місцем. Комп’ютери одного відділу змушені чекати, коли закінчить обмін пари комп’ютерів іншого відділу, і це при тім, що необхідність у зв’язку між комп’ютерами двох різних відділів виникає набагато рідше і вимагає зовсім невеликої пропускної здатності.

Якщо логічна структура мережі залишається однорідною – вона ніяк не враховує збільшення інтенсивності трафіка всередині відділу і надає всім парам комп’ютерів рівні можливості по обміну інформацією.

2.2 Вибір технології локальної та глобальної мережі

Локальні мережі. Комп’ютерна мережа – це комп’ютери, що зв’язані між собою системою пересилання інформації. Таку систему утворюють програмне забезпечення і технічні пристрої відповідного призначення. Мережі поділяють за зонами обслуговування на локальні та глобальні. За допомогою локальної мережі один комп'ютер отримує доступ до ресурсів іншого, таких, як дані та периферійні пристрої (принтери, модеми, факси тощо).

У локальні мережі об’єднуються комп’ютери, розташовані в одному будинку чи одній організації. Короткі лінії зв’язку дали змогу використати для пересилання інформації дорогі коаксіальні (подібні до телевізійних) кабелі чи оптичні світловоди з великою швидкістю – 20 Мбіт/с і більше. Сьогодні для об’єднання комп’ютерів у локальні мережі застосовують економну технологію, що називається «вита пара».

Найпростіший приклад локальної мережі – два з’єднані спеціальним кабелем через послідовні чи паралельні порти комп’ютери. Такий спосіб з’єднання називають прямим.

Якщо в мережі є комп’ютер, з якого черпають інформацію робочі станції, то такий комп’ютер називають сервером, робочі станції – клієнтами, а з’єднання – мережею типу клієнт-сервер. На таких комп’ютерах встановлюють спеціальне програмне забезпечення: програму-сервер для серверу і програму-клієнт для кожної робочої станції.

Локальні мережі можуть взаємодіяти між собою, якщо вони під’єднані до деякої глобальної мережі.

Однією з найбільш важливих вимог, що представляються до проектованої мережі є продуктивність. Для забезпечення достатньої швидкості з’єднання і прийнятного рівня затримок всі хости підключаються по FastEthernet (100BASE-T) до мережевих пристроїв рівня доступу UTP-кабелями, всі магістральні

з’єднання між пристроями розподілу реалізуються за допомогою Gigabit Ethernet (1000BASE-T) з використанням екранованої витої пари (STP).

Глобальні мережі (WAN – Wide Area Network) не обмежені територіально і можуть забезпечувати швидкості передавання, які сягають кількох терабіт за секунду. Крім цих мереж розрізняють регіональні та корпоративні мережі, які можуть поєднувати у собі технології локальних і глобальних комп’ютерних мереж. Регіональні мережі утворюються у масштабах міста, району, області.

Корпоративні мережі об’єднують локальні мережі і комп’ютери однієї організації. Потреба в обміні даними і сучасні технічні досягнення зробили глобальні комп’ютерні мережі невід’ємною частиною здійснення програм співпраці між людьми усього світу. Мережею, що здатна об’єднати безліч мереж і дозволяє увійти у світове співтовариство є Інтернет (Internet), який надає користувачу практично необмежені інформаційні ресурси. Порівняння глобальних технологій WAN наведено в таблиці 2.1.

Таблиця 2.1 – Порівняння глобальних технологій

Технології				
X.25	Frame Relay	ISDN	ATM	TCP/IP
1	2	3	4	5
Швидкість використовуваних каналів				
12-64 кб/с до 2мб/с	64 кб/с – 2 Мб/с до 44,736мб/с	128кб/с 1.544 (2,048) Мб/с	25Мб/с –622,08 Мб/с	1.2 Мб/с – 2.048 Мб/с
Надійність доставки і організація повторної передачі даних				
Гарантує	Доставку не гарантує	Не гарантує	З протоколом SSCOP	Доставку не гарантує
Наявність механізмів в технології контролю перевантажень комутуючих пристроїв				
Є	Є	Немає	Є	Немає
Можливість групової доставки (доставки до групи адрес)				
Не забезпечує	Забезпечує	Забезпечує	Забезпечує	Забезпечує

Продовження таблиці 2.1

1	2	3	4	5
Ефективність передачі корисних даних				
	Близько 100%	Меньше 80%	Залежить від типу послуг 77-90 %	
Забезпечення якості обслуговування				
Не забезпечує	Не гарантує затримку передачі даних	Класи доступу	Забезпечує повністю	Не забезпечує

Основними вимогами, що постають до мережі є: безпека, відмовостійкість і продуктивність. З огляду на специфіку організації, можна висунути такі критерії вибору технології WAN:

- надійність і гарантія доставки даних;
- трафік транзакцій;
- трафік реального часу;
- забезпечення якості обслуговування (QoS) для пріоритезації трафіку.

2.3 Вибір мережевого обладнання

При виборі мережевого обладнання треба враховувати безліч чинників, зокрема:

- рівень стандартизації обладнання та його сумісність з найбільш поширеними програмними засобами;
- швидкість передачі інформації і можливість її подальшого збільшення;
- можливі топології мережі та їх комбінації (шина, кільце, пасивна зірка, пасивне дерево);
- метод управління обміном у мережі (CSMA/CD, повнодуплексний або маркерний метод);

- дозволені типи кабелю мережі, максимальну його довжину, захищеність від перешкод;

- вартість і технічні характеристики конкретних апаратних засобів (мережевих адаптерів, повторювачів, концентраторів, комутаторів тощо).

На сьогодні для організації локальних мереж у переважній більшості випадків використовується неекранована вита пара UTP. Більш дорогі варіанти на основі екранованої витої пари, оптоволоконного кабелю або бездротових з'єднань застосовуються на підприємствах, де в цьому дійсно існує гостра необхідність. Наприклад, оптоволокно може використовуватися для зв'язку між віддаленими сегментами мережі без втрати швидкості.

Дивлячись, що на підприємстві знаходиться понад десяток комп'ютерної техніки, необхідно брати обладнання з запасом на майбутнє, так як є можливість збільшення мережі. Підприємство має 11 вузлів підключених через FastEthernet до комутаторів рівня доступу, що в середньому, з огляду на специфіку інформації та обмеження, передбачає потік трафіку у великому розмірі. З ростом мережі ця цифра пропорційно збільшиться, отже необхідно підбирати обладнання, як мінімум в 2 рази більшою пропускною спроможністю.

На підставі даних вимог було вибрано наступне обладнання.

Комутатор – це мережевий пристрій, за участю якого підключені користувачі проводять обмін інформацією усередині мережі. Вони використовуються при з'єднанні доменів колізій локальної мережі між собою, для запобігання втрат переданих даних. Ці пристрої бувають керовані та некеровані. Комутатор Cisco 24950-24 зображений на рисунку 2.1, а технічні характеристики наведені в таблиці 2.2.

Рисунок 2.1 – Комутатор Cisco 2950-24

Таблиця 2.2 – Технічні характеристики Cisco 2950-24

Загальні характеристики	
Тип пристрою	Комутатор (switch)
Можливість установки в стійку	є
Об'єм оперативної пам'яті	64 Мб
Об’єм флеш-пам'яті	32 Мб
LAN	
Кількість портів комутатора	24 x Ethernet 10/100 Мбіт/сек
Максимальна швидкість uplink / SFP-портів	10/100/1000 Мбіт/сек
Внутрішня пропускна здатність	16 Гбіт/сек
Розмір таблиці MAC адреси	8192
Управління	
Web-інтерфейс	є
Підтримка Telnet	є
Підтримка SNMP	є
Маршрутизатор	
Протоколи управління групами інтернету	IGMP v1, IGMP v2, IGMP v3
Додатково	
Підтримка стандартів	Auto MDI/MDIX, IEEE 802.1p (Priority tags), IEEE 802.1q (VLAN), IEEE 802.1d (Spanning Tree), IEEE 802.1s (Multiple Spanning Tree)
Розміри	445 x 44 x 236 мм
Вага	1.6 кг

Маршрутизатор – активний мережевий пристрій, що функціонує на третьому мережевому рівні моделі OSI. Він призначений, як правило, для здійснення виходу користувачів з локальної мережі в глобальну. Також використовуються для організації розподіленої мережі підприємства, що забезпечує доступ всіх співробітників компанії до інформації. Маршрутизатор ASUS BRT-AC828 зображений на рисунку 2.2, технічні характеристики маршрутизатора ASUS BRT-AC828 вміщує таблиця 2.3.

Рисунок 2.2 – Маршрутизатор ASUS BRT-AC828

Таблиця 2.3 – Технічні характеристики ASUS BRT-AC828

Загальні характеристики	
Тип пристрою	Маршрутизатор (роутер)
Вхід (WAN порт)	3x10/100/1000BASE-T Ethernet
Інтерфейс підключення (LAN-порт)	3x10/100/1000BASE-T Ethernet
Маршрутизатор	
Межмережевий екран(Firewall)	+
NAT	+
Підтримка VPN (віртуальних мереж)	+
DHCP-сервер	Немає даних
Моніторинг та конфігурація	
Веб-інтерфейс	Немає даних
Підтримка SNMP	+
Додатково	
Живлення (PoE/адаптер)	+/+
Можливість установки поза приміщення	-
Інше	2 порти USB 2.0; форм-фактор 2U; підтримка SSL; містить два слота під модулі GBIC;
Розміри (мм)	438,2x304,8x88,9
Вага (г)	3600

Вита пара (рисунок 2.3) - найпоширеніший на сьогоднішній день вид кабелю, який використовується для побудови локальних мереж. Кабель складається з попарно перевитих мідних ізольованих провідників. Типовий кабель несе в собі 8 провідників (4 пари), хоча випускається і кабель з 4 провідниками (2 пари). Кольори внутрішньої ізоляції провідників суворо стандартні. Відстань між пристроями, з'єднаними кручений парою, не повинна перевищувати 100 метрів.

Рисунок 2.3 – Вита пара

Мережеві карти відповідають за передачу інформації між комп'ютерами мережі. Мережевий адаптер (рисунок 2.4) складається з роз'єму для мережевого провідника (зазвичай, витої пари) і мікропроцесора, який кодує/декодує мережеві пакети. Типова мережева карта являє собою плату, що вставляють у гніздо шини PCI. Практично у всіх сучасних комп'ютерах електроніка мережевого адаптера розпаяна безпосередньо на материнській платі.

Рисунок 2.4 – Мережевий адаптер

Сервер — це комп'ютер у локальній чи глобальній мережі, що забезпечує функціонування мережі, а також всі, або частину її функцій. Він надає користувачам свої обчислювальні і дискові ресурси, а також доступ до встановлених сервісів. Технічні характеристики сервера Barebone server Asus подані в таблиці 2.4.

Таблиця 2.4 – Технічні характеристики сервера

Назва	Barebone server Asus RS720-X7-RS8, Dual S2011 Xeon, iC602-A,12 DDR3 ECC, 5xLAN, VGA, 4SATA, 2U
Опис	Потужна серверна система на базі процесорної платформиIntel Xeon
Виробник	ASUS
Модель	RS720-X7-RS8
Чіпсет мат. плати	Intel C602-A PCH
Гніздо процесора	2x Socket LGA2011
Підтримка типів процесорів	Intel Xeon processor E5-2600
QPI(QuickPath Interconnect)	6.4 / 7.2 / 8.0 GT/s
Пам’ять	12x DDR3 (4-channel per CPU, 8 DIMM for CPU1,4 DIMM for CPU2) – 128GB RAM
Максимальний об’єм пам'яті	Maximum 384GB RDIMM Maximum 384GB LRDIMM/Maximum
Кількість роз'ємів PCI Express	PCI-E x16 (Gen3 x16 Link) + 5 PCI-E x8 (Gen3 x8 Link) PCI-E x16 (Gen3 x8 Link) + 6 PCI-E x8 (Gen3 x8 Link) (PIKE Slot for Stroage Enhancement)
SATA	Intel C602-A 2x SATA3 6Gb/s 4x SATA2 3Gb/s
RAID-контролер	Опціонально можлива установка ASUS PIKE RAID card
Відсіки для накопичувачів	8 кошиків для SAS / SATA HDD з можливістю гарячої заміни (панель в комплекті)
Відео	Aspeed AST2300 відеопам’ять 16MB
Оптичний привід	DVD-RW
Мережа	4x Intel 82574L + 1x Mgmt LAN
Набір портів взаді	2x Serial Port Header 5x RJ-45 (One for ASMB6-iKVM) 4x USB 2.0 Front x 2, Rear x 2) 1x PS/2 mouse 1x Internal A Type USB 1x VGA 1x PS/2 keyboard
Управління	KVM-over-Internet (ASMB6-iKVM for KVM-over-IP)

Продовження таблиці 2.4.

Живлення	1+1 Redundant 770W
Підтримувані ОС	CentOS 5.6 32/64-bit Windows Server 2008 R2 Windows Server 2008 R2 Enterprise Windows Server 2008 Enterprise 32/64-bit RedHat Enterprise Linux AS5.6/6.0 32/64-bit SuSE Linux Enterprise Server 11.2 32/64-bit VMWare ESX4.1/ESXi4.1
Розміри	61.5 x 44.4 x 8.7 см
Вага	10 кг

2.4 Налаштування локальної мережі в PacketTracer

Для того щоб розробити модель мережі я використовував програмне забезпечення фірми Cisco Packet Tracer.

Програмне рішення Cisco Packet Tracer дозволяє імітувати роботу різних мережних пристроїв: маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп'ютерів, мережевих принтерів, IP-телефонів і т.д. Робота з інтерактивним симулятором дає дуже правдоподібне відчуття налаштування реальної мережі, що складається з десятків пристроїв. Установки, у свою чергу, залежать від характеру пристроїв: одні можна налаштувати за допомогою команд операційної системи Cisco IOS, інші - за рахунок графічного веб-інтерфейсу, треті - через командний рядок операційної системи або графічні меню.

Завдяки такій властивості Cisco Packet Tracer, як режим візуалізації, користувач може відстежити переміщення даних по мережі, поява і зміна параметрів IP-пакетів при проходженні даних через мережеві пристрої, швидкість і шляхи переміщення IP-пакетів. Аналіз подій, що відбуваються в мережі, дозволяє зрозуміти механізм її роботи і виявити несправності.

Для побудови мережі потрібно витягнути мишкою потрібні пристрої на робоче поле, після чого встановити потрібні зв’язки між ними використовуючи піктограму.

Єдиним суттєвим недоліком системи можна вважати неможливість проектування в мережі використання відмінного від обладнання фірми Cisco обладнання.

Успішно дозволяє створювати навіть складні макети мереж, перевіряти на працездатність топології.

Згідно логічної структури мережі (рисунок 2.5), відділи поміщені в VLAN і в підмережу. Дана локальна структура відповідає логічній структурі, існує чотири відділень, які з’єднанні через два комутатора і за допомогою трьох роутерів.

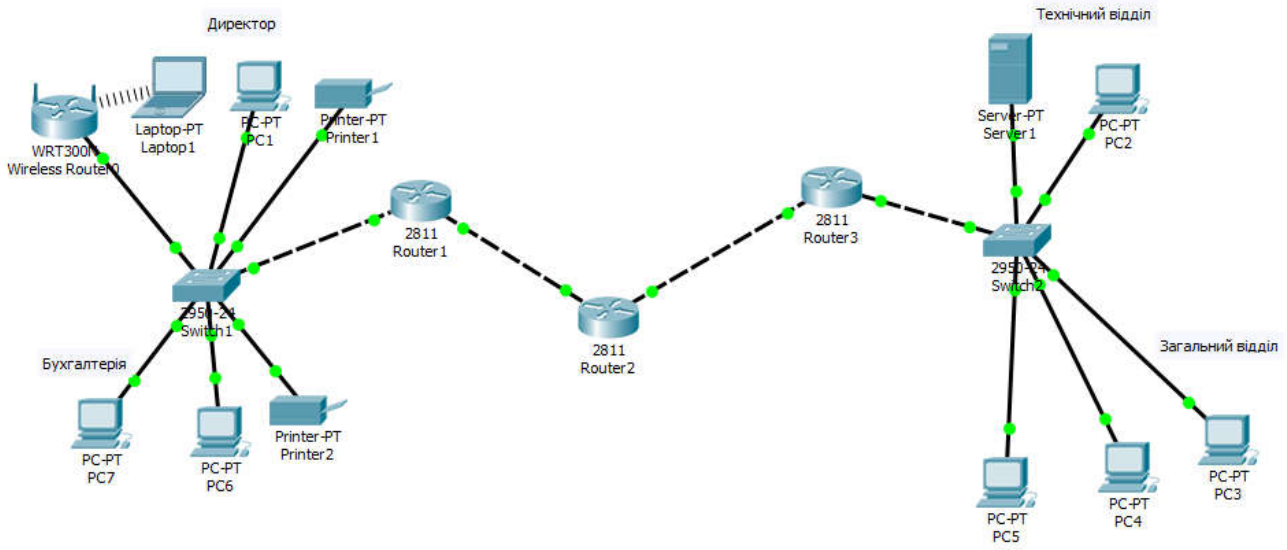

Рисунок 2.5 – Локальна мережа в Cisco Packet Tracer

У відділі директора є ноутбук, який підключений до точки доступу Wi-Fi і має вихід до інтернету (рисунок 2.6).

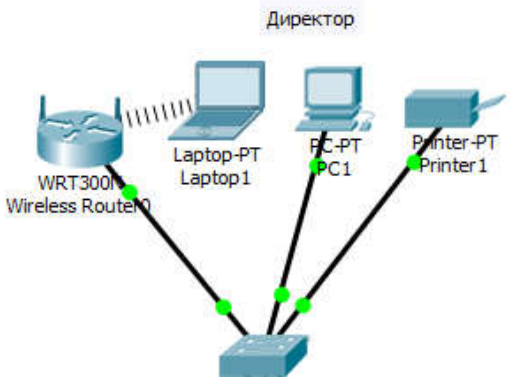

Рисунок 2.6 – Відділ директора з точкою доступа WI-FI

Налаштування безпровідного маршрутизатора Wi-Fi зображено на рисунку 2.7.

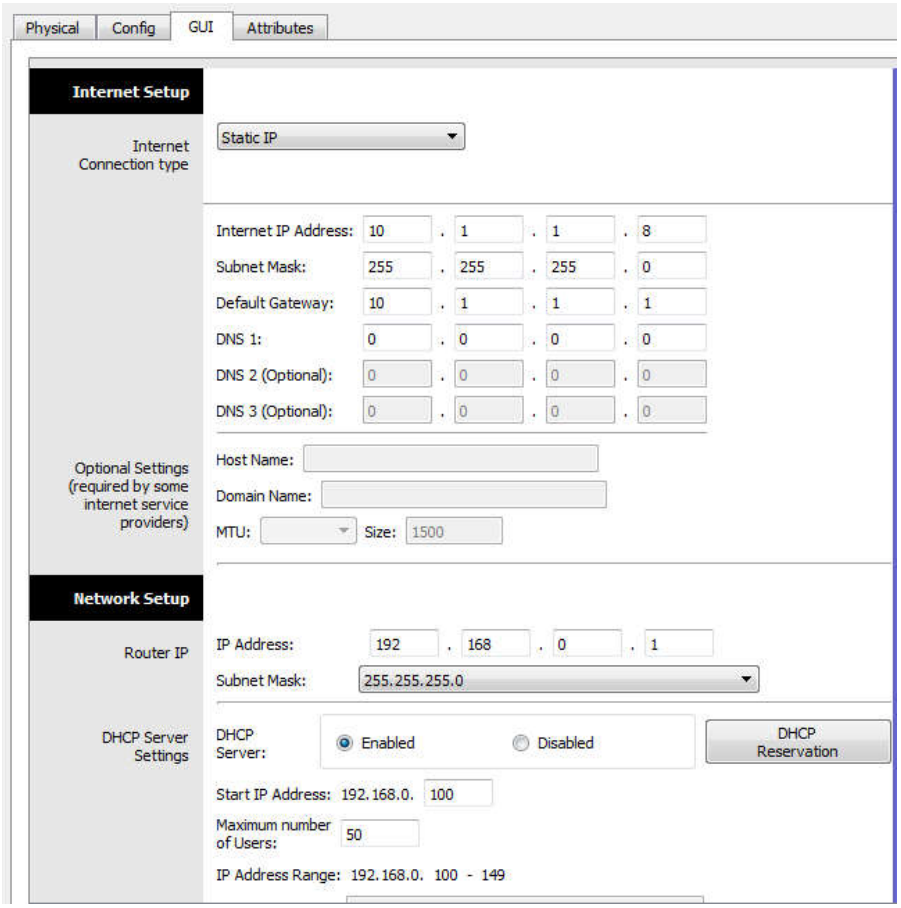

Рисунок 2.7 – Налаштування на точці доступу Wi-Fi

Всі пристрої, які призначені для користувачів в корпоративній мережі повинні мати обліковий запис з обмеженим функціоналом.

3 АВТОМАТИЗАЦІЯ ПЕРЕХОДУ З IPV4 НА IPV6

Протокол IP настільки поширений, що планомірна заміна його четвертої версії на шосту представляється вельми непростою справою. Саме тому і розробляються технології, які не будучи частиною специфікації IPv6, здатні забезпечити одночасне використання обох версій протоколу IP в глобальних мережах.

Хоча IPv4 вирішує безліч проблем, проте миттєвий перехід з IPv4 на IPv6, на жаль, неможливий. Кількість пристроїв на Землі, що використовують IPv4, обчислюється мільйонами, а в окремих випадках, навіть якщо захочеться перейти на IPv6, пристрої або програмне забезпечення можуть ще не підтримувати IPv6 або, щонайменше, немають проведеного повного тестування такої підтримки. Перехід з IPv4 на IPv6 може зайняти роки або навіть десятиліття.

Таблиця 3.1 містить інформацію про технології для здійснення переходу з протоколу IPv4 на протокол IPv6 та їх види і взаємодію.

Таблиця 3.1 – Взаємодія технологій

Технологія	Вид технології	Опис
1	2	3
Подвійний стек	-	Підтримка обох протоколів одночасно
Тунелювання	MCT	Тунель налаштовується вручну; відсилання IPv6 пакетів через IPv4 мережу, зазвичай між роутерами
Тунелювання	6to4	Динамічне виявлення кінцевих точок тунелю; відсилання IPv6 пакетів через IPv4 мережу, зазвичай між роутерами
Тунелювання	ISATAP	Динамічне виявлення кінцевих точок тунелю; відсилання IPv6 пакетів через IPv4 мережу, зазвичай між роутерами; не працює при налаштованому IPv4 NAT

Продовження таблиці 3.1.

1	2	3
Тунелювання	Teredo	Тунель зазвичай налаштовується між хостами; хост створює IPv6 пакет і інкапсулює його в IPv4 заголовок; працює при налаштованому IPv4 NAT
Трансляція	-	Роутер перетворює заголовки IPv6 пакетів в заголовки IPv4 і назад; дозволяє IPv6 пристроїв взаємодіяти з IPv4 пристроями

Отже, перехід з протоколу IPv4 на протокол IPv6 буде здійснено технологією 6to4.

3.1 Технологія переходу 6to4

На сьогодні існує досить розгалужена інфраструктура мереж IPv4, які використовуються і будуть використовуватись. Навіть якщо підприємство почне будувати свою власну мережу тільки з використанням IPv6, як протокол мережного рівня, може виявитись що всі ISP в регіоні використовують лише IPv4. Отож, для підключення до глобальної мережі IPv6 все-одно потрібно використовувати наявні мережі IPv4. Для вирішення проблеми взаємодії мереж IPv6 через мережі IPv4 були розроблені так звані механізми переходу.

6to4 - це технологія переходу, яка дозволяє відправляти IPv6 - пакети через IPv4-канали і не вимагає створення обопільних тунелів. Дана технологія використовується, коли користувач кінцевого пристрою або сайт бажають отримувати з'єднання з IPv6-Інтернетом, але не мають можливості отримати його від провайдера.

6to4 виконує три функції:

- виділяє блок / 48 адресного простору IPv6 кожному хосту, у якого є глобальний IPv4-адрес;

- інкапсулює пакети IPv6 в пакети IPv4 для передачі по мережі IPv4;

- дозволяє передавати пакети між 6to4-хостами і хостами з «рідною» IPv6-мережею.

У найпростішому випадку кілька мереж починають використовувати IPv6 паралельно з IPv4 і застосовують механізм 6-to-4 для забезпечення зв'язку між собою по IPv6. На один з маршрутизаторів такої мережі одночасно встановлюються протоколи IPv4 і IPv6 і активізується механізм 6-to-4. Кожен з таких маршрутизаторів повинен бути доступний вузлам IPv6 зі своєї мережі і мати, як мінімум, одну глобальну адресу IPv4. Зв'язок вузлів мережі з виділеним маршрутизатором може бути реалізований за допомогою внутрішньої інфраструктури маршрутизаторів IPv6, або через маршрутизатори IPv4 / IPv6, або з використанням інших методів тунелювання.

На рисунку 3.1 можна побачити типовий приклад IPv6-to-IPv4 тунелю, де хости в одних підмережах вже мігрували на IPv6, а транзитна між ними мережа все ще використовує протокол IPv4. Це може бути випадок початкового етапу тестування IPv6 всередині підприємства або це може бути клієнт, який бажає перейти на IPv6, у провайдера, який працює з IPv4. IPv6 хост посилає IPv6 пакет, після чого роутер R1 інкапсулює пакет в IPv4 заголовок, в якому адреса призначення - це IPv4 адреса роутера R4. Роутери R2 і R3 перенаправляють пакет в пункт призначення R4, так як пакет має заголовок IPv4. R4 декапсулює отриманий пакет і перенаправляє оригінальний IPv6 пакет хосту PC2.

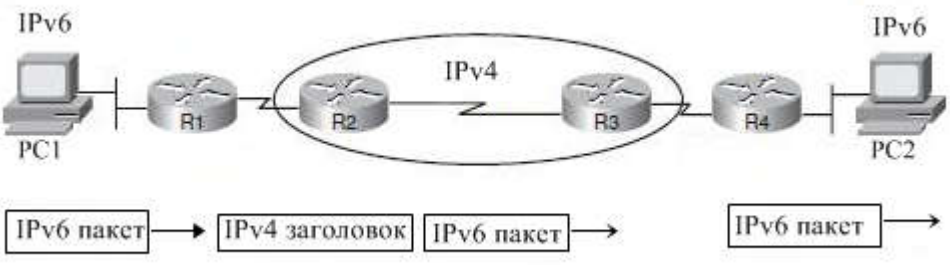

Рисунок 3.1 – Приклад IPv6 to IPv4 тунеля

6to4 має наступні переваги перед іншими способами тунелювання IPv6:

- відсутність реєстрації перед його налаштуванням, а так само швидкість і простота конфігурування;

- прямий зв'язок по IPv6 між будь-якими двома машинами - без посередників у вигляді будь-яких шлюзів або тунельних серверів;

- найближчий шлюз, через який пакети будуть надсилатися іншим користувачам IPv6, вибирається повністю автоматично.

Недоліком є те, що найближчий шлюз, через який пакети будуть надсилатися іншим користувачам IPv6, вибирається повністю автоматично.

Одна з переваг одночасно є і недоліком. Іноді може статися, що автоматично обраний шлюз погано функціонує, перевантажений або просто не працює. При чому не завжди очевидно, від кого і на якій підставі можна вимагати виправлення цих проблем. Хоча подібні випадки дуже рідкісні, але цей момент змушує багатьох віддавати перевагу тунелям, які конфігуруються вручну від тунельного брокера, де завжди чітко відомі контакти технічної підтримки, яку можна потурбувати в разі проблеми з використовуваним тунельним сервером.

3.2 Аналіз мережі на основі IPv4 та IPv6

Швидкість передачі пакетів – один із найважливіших параметрів в будь-якій мережі. Спосіб сполучення комп'ютерів каналами зв'язку для передавання даних між ними називають методом комутації. При комутації пакетів всі повідомлення передані користувачем мережі розбиваються у вихідному вузлі на порівняно невеликі частини, які називаються пакетами. Повідомлення можуть мати довільну довжину, від декількох байт до багатьох мегабайт. Навпроти, пакети звичайно теж можуть мати перемінну довжину, але у вузьких межах, наприклад від 46 до 1500 байт. Кожен пакет забезпечується заголовком, у якому вказується адресна інформація, необхідна для доставки пакета вузлу

призначення, а також номер пакета, що буде використовуватися вузлом призначення для зборки повідомлення.

Пакети транспортуються в мережі як незалежні інформаційні блоки. Комутатори мережі приймають пакети від кінцевих вузлів і на підставі адресної інформації передають їх один одному, а на при кінці — вузлу призначення.

Ком'пютер повинен мати IP адресу версії IPv4 та IPv6, як показано на рисунку 3.2. Наприклад, PC1 має IPv4 – 10.1.1.2 з маскою 255.255.255.0 та шлюзом – 10.1.1.1, а також IPv6 – 2001:1:1:1::2 з маскою 64 та шлюзом 2001:1:1:1::1.

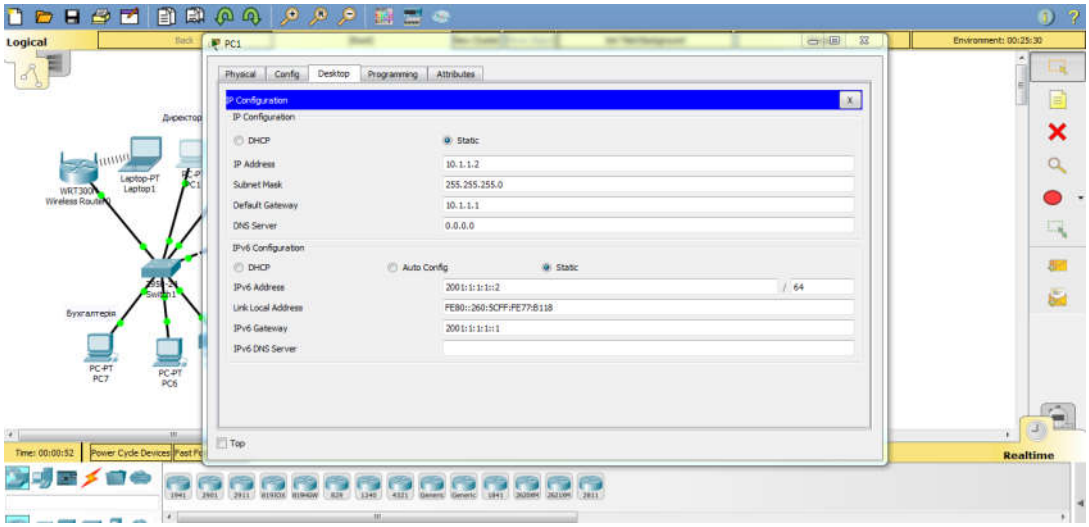

Рисунок 3.2 – Налаштування IP

Програма Packet Tracer надає можливість вимірювати швидкість передачі пакетів за допомогою панелі симуляції (рисунок 3.3). За допомогою даної можливості були проведені заміри в мережі на IPv4 і на IPv6.

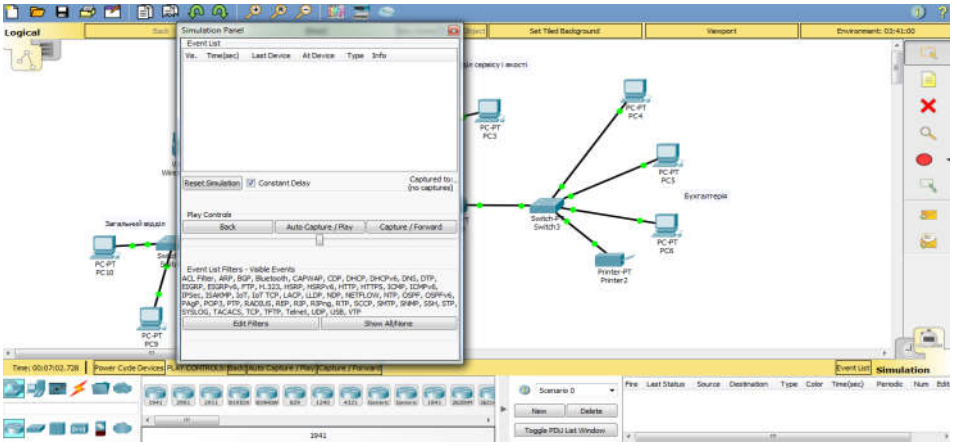

Рисунок 3.3 –Панель симуляції

На рисунку 3.4 представлені дані про швидкість передачі пакетів для версії IPv4.

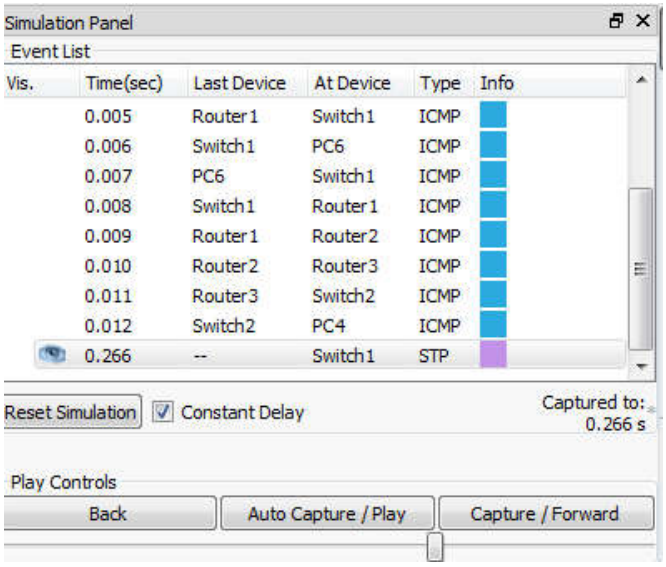

Рисунок 3.4 –Передача пакетів для IPv4

Даний сервіс надає можливість вимірювання часу передачі пакету на кожному пристрої, через яке пройшов пакет, а також тип пакета. Було передано пакети з PC4 до PC6, які проходили через Switch2, Router3, Router2, Router1 та Switch1. Час передачі – 0,145 с. На рисунку 3.5 представлена швидкість передачі пакета для IPv6.

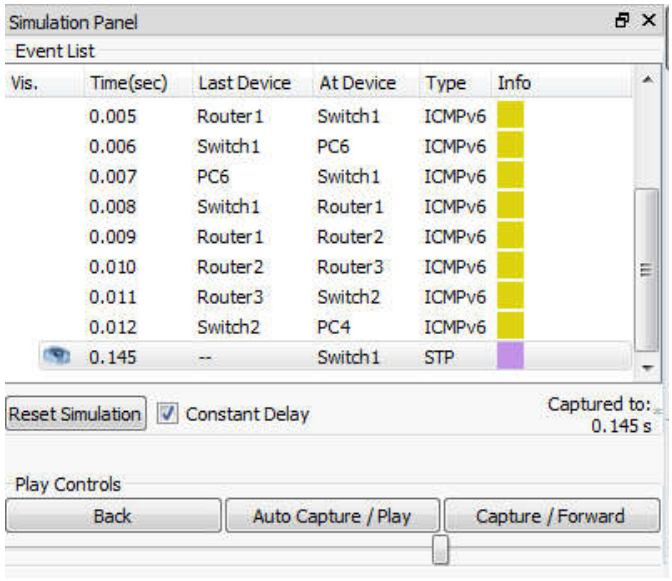

Рисунок 3.5 –Передача пакетів для IPv6

Дивлячись на результати передачі пакетів по версії IPv4 та IPv6, можна зробити висновок, що за допомогою версії IPv6 передача пакетів здійснюється швидше, тому краще використовувати саме цю версію.

3.3 Розрахунок пропускної смуги

Гарантія якості обслуговування, яка надається оператором для користувачів, безпосередньо залежить від смуги пропускання. У загальному випадку, затримка поширення від пункту відправки до пункту призначення передачі не перевищує 0,1 с, а ймовірність перевищення затримки порога в 0,05 не повинна перевищувати 0,1, тобто: $t_p \le 0{,}1\,\text{с}$,

$$P[t_p > 50] \le 0{,}001 \qquad (3.1)$$

Затримка від початку до кінця складається з наступних складових:

$$t_p = t_{pack} + t_{ад} + t_{core} + t_{буф} \ , \qquad (3.2)$$

де t_p - час передачі пакета від краю до краю;

t_{pack} - час перетворення пакетів (тип кодека і трафік впливає на її значення);

$t_{ад}$ - час затримки транспортування в мережі;

t_{core} - час затримки при поширенні в транзитній мережі;

$t_{буф}$ - час затримки в приймальному буфері.

Використання низькошвидкісних кодеків знижує затримку в цілому. У буфері прийому затримка буде також велика, тому на рівень доступу і на транспортний рівень повинна надаватися мінімальна затримка.

Допускається, що затримка на рівні доступу не перевищує 0,005 секунд. Час обробки заголовка IP-пакета приймається константою, так як воно практично незмінне і на його значення не впливають інші чинники. Інтервали перерозподілені між надходженнями пакетів, що підпорядковується експоненціальним законом. Для даного випадку може бути застосована формула, яка знаходить середній час виклику в системі (формула Полячека- Хінчина):

$$\tau_{adj} = \frac{\tau_j (1 + c\frac{2}{b})}{2(1 - \lambda_j \cdot \tau_j)} \ , \qquad (3.3)$$

де τ_j - середній час обслуговування одного пакета;

$c\frac{2}{b}$ - квадрат коефіцієнта варіації, $c\frac{2}{b} \approx 0{,}2$;

λ_j - параметр потоку;

τ_{adj} - середній час затримки пакета в мережі доступу, $\tau_{adj} \approx 0{,}005$ коефіцієнт варіації, який відмінний від нуля, піддається впливу можливим відхиленням для застосування їх в заголовках IP полів ToS. Час обробки IP-пакета так само піддається впливу правилами обробки на маршрутизаторі.

На підставі формули (3.2) є залежність середньої тривалості обслуговування одного пакета (максимальне значення) від середнього часу затримки в мережі на рівні доступу.

$$\tau_j = \frac{1}{\lambda_j + \frac{1 + c\frac{2}{b}}{2 \cdot \tau_{adj}}}, \tag{3.4}$$

$$\tau_{j1} = \frac{1}{\lambda_{j1} + \frac{1 + c\frac{2}{b}}{2 \cdot \tau_{adj}}} = \frac{1}{(89480 + \frac{1 + 0{,}2}{2 \cdot 0{,}005})} = 13{,}10 \cdot 10^{-6} \text{ с.}$$

$$\tau_{j2} = \frac{1}{\lambda_{j2} + \frac{1 + c\frac{2}{b}}{2 \cdot \tau_{adj}}} = \frac{1}{(131450 + \frac{1 + 0{,}2}{2 \cdot 0{,}005})} = 8{,}46 \cdot 10^{-6} \text{ с.}$$

Розрахунок за формулами 3.1 і 3.2 показує середній час затримки в мережі на рівні доступу, а також інтенсивність обслуговування при $\tau_{ad} = 0{,}005$с для декількох типів кодеків.

При середньому значенні затримки в мережі на рівні доступу 0,005 коефіцієнт використання дорівнює:

$$p_j = \lambda_j \cdot \tau_j, \tag{3.5}$$

$$p_{j1} = \lambda_{j1} \cdot \tau_{j1} = 89480 \cdot 13{,}10 \cdot 10^{-6} = 1{,}17$$

$$p_{j2} = \lambda_{j2} \cdot \tau_{j2} = 131450 \cdot 8{,}46 \cdot 10^{-6} = 1{,}12$$

При такому високому ступені використання найменші флуктуації параметрів призводять збій в роботі системи. Визначені показники мережі при зниженні її використання на 50%. Середня тривалість обслуговування знаходиться за наступною формулою:

$$\tau_j = \frac{\rho_j}{\lambda_j}\ , \tag{3.6}$$

$$\tau_{j1} = \frac{\rho_{j1}}{\lambda_{j1}} = \frac{0{,}5}{89480} = 5{,}6 \cdot 10^{-6}\ \text{с.}$$

$$\tau_{j2} = \frac{\rho_{j2}}{\lambda_{j2}} = \frac{0{,}5}{131450} = 3{,}8 \cdot 10^{-6}\ \text{с.}$$

Інтенсивність обслуговування визначається за формулою:

$$\beta_j = \frac{1}{\tau_j}\ , \tag{3.7}$$

$$\beta_{j1} = \frac{1}{\tau_{j1}} = \frac{1}{5{,}6 \cdot 10^{-6}} = 178571\ \text{с.}$$

$$\beta_{j2} = \frac{1}{\tau_{j2}} = \frac{1}{3{,}8 \cdot 10^{-6}} = 263157\ \text{с.}$$

Затримка в мережі доступу розраховується за формулою 3.3:

$$\tau_{adj1} = \frac{\tau_{j1}(1 + c\frac{2}{b})}{2(1 - \lambda_{j1} \cdot \tau_{j1})} = \frac{5{,}6 \cdot 10^{-6}(1 + 0{,}2)}{2(1 - 89480 \cdot 5{,}6 \cdot 10^{-6})} = 6{,}73 \cdot 10^{-6}\ \text{с.}$$

$$\tau_{adj2} = \frac{\tau_{j2}(1 + c\frac{2}{b})}{2(1 - \lambda_{j2} \cdot \tau_{j2})} = \frac{3{,}8 \cdot 10^{-6}(1 + 0{,}2)}{2(1 - 131450 \cdot 3{,}8 \cdot 10^{-6})} = 4{,}56 \cdot 10^{-6}\ \text{с.}$$

Розрахунок ймовірності $s(t) = 1 - e^{-(\frac{1}{t} - \lambda)t}$ при відомих λ і τ проводити недоцільно, так як в Y.1541 ймовірність P [t>0,005]<0,001 визначена для передачі від краю до краю.

На підставі відомого середнього виміру пакета h_j визначена смуга пропускання за такою формулою:

$$\varphi_j = \beta_j \cdot h_j, \text{ біт/сек.} \quad (3.8)$$

$$\varphi_{j1} = \beta_{j1} \cdot h_{j1} = 178571 \cdot 220 \cdot 8 = 314 \cdot 10^6 \text{ біт/сек.}$$

$$\varphi_{j2} = \beta_{j2} \cdot h_{j2} = 263157 \cdot 140 \cdot 8 = 294 \cdot 10^6 \text{ біт/сек.}$$

За даними, визначеними вище, показано, що протокол IPv6 має більшу пропускну здатність, ніж IPv4, що демонструє таблиця 3.2.

Таблиця 3.2 – Пропускна здатність

Параметри	IPv4	IPv6
Середня тривалість обслуговування	$3{,}8 \cdot 10^{-6} c$	$5{,}6 \cdot 10^{-6} c$
Інтенсивність обслуговування	263157 с	178571 с
Затримка в мережі доступу	$4{,}56 \cdot 10^{-6} c$	$6{,}73 \cdot 10^{-6} c$
Пропускна смуга	$294 \cdot 10^6$	$314 \cdot 10^6$

Розрахунок параметрів мережі, таких як: час і інтенсивність обслуговування одного IP пакета певної довжини залежить від часу затримки в мережі доступу. Для відправки даних одного розміру, необхідна різна смуга пропускання, під час відправки кодека G.521 (100 байт) необхідна менша смуга пропускання, ніж при використанні кодека G.930 (250 байт).

4 ТЕХНІКО-ЕКОНОМІЧНИЙ РОЗДІЛ

Метою техніко-економічного розділу є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проекту мережі для підприємства і прийняття рішення про його подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

Для визначення загальної тривалості проведення НДР дані витрат часу з окремих операцій доцільно звести у таблицю 4.1.

4.1 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Витрати на оплату праці включають заробітну плату (ЗП) всіх категорій працівників, безпосередньо зайнятих на всіх етапах проектування. Розмір ЗП обчислюється на основі трудоємності відповідних робіт та середньої ЗП відповідних категорій працівників.

У розробці проектного рішення задіяні наступні спеціалісти - розробники, а саме: керівник проекту; студент-дипломник; консультант техніко-економічного розділу (таблиця 4.1).

Таблиця 4.1 - Вихідні дані для розрахунку витрат на оплату праці

Посада виконавців	Місячний оклад (стипендія), грн.
Керівник ДП, викладач	4916,00
Консультант техніко-економічного розділу, доцент	6026,00
Студент	1300,00

Витрати на оплату праці розробників проекту визначаються за формулою:

$$B_{ОП} = \sum_{i=1}^{N} \sum_{j=1}^{M} n_{ij} \cdot t_{ij} \cdot C_{ij} , \qquad (4.1)$$

де n_{ij} – чисельність розробників *i*-ої спеціальності *j*-го тарифного розряду, осіб;

t_{ij} – затрачений час на розробку проекту співробітником *i*-ої спеціальності *j*-го тарифного розряду, год;

C_{ij} – годинна ставка працівника *i*-ої спеціальності *j*-го тарифного розряду, грн.

Середньогодинна ставка працівника може бути розрахована за формулою:

$$C_{ij} = \frac{C_{ij}^{0}(1+h)}{РЧ_i}, \qquad (4.2)$$

де C_{ij} – основна місячна заробітна плата розробника *i*-ої спеціальності *j*-го тарифного розряду, грн;

h – коефіцієнт, що визначає розмір додаткової заробітної плати (при умові наявності доплат);

$РЧ_i$ - місячний фонд робочого часу працівника *i*-ої спеціальності *j*-го тарифного розряду, год. (приймаємо 168 год).

Коефіцієнт *h*, який визначає розмір додаткової заробітної плати, для керівника та консультанта техніко-економічного розділу дорівнює 1,47.

Середньогодинна ставка керівника ДП дорівнює:

$$C_{ij} = \frac{4916 \cdot (1+1{,}47)}{168} = 72{,}28 \text{ грн/год.}$$

Середньогодинна ставка консультанта техніко-економічного розділу ДП дорівнює:

$$C_{ij} = \frac{6026 \cdot (1 + 1{,}47)}{168} = 88{,}60 \text{ грн/год.}$$

Середньогодинна оплата студента дорівнює:

$$C_{ij} = \frac{1300}{168} = 7{,}73 \text{ грн/год.}$$

Звідси, загальні витрати на оплату праці ($B_{ОП}$) дорівнюють:

$$B_{ОП} = 16 \cdot 72{,}28 + 144 \cdot 7{,}73 + 2 \cdot 88{,}60 = 2446{,}80 \text{ грн.}$$

Дані для розрахунку витрат на оплату праці наведено в таблиці 4.2

Таблиця 4.2 - Середній час виконання НДР та стадії (операції) технологічного процесу

Назва операції (стадії)	Середній час виконання операції, год.	Погодинна заробітна плата, грн/год.	Витрати на розробку, грн.
Керівник ДП, викладач	16	72,28	1156,48
Консультант ТЕР, доцент	2	88,60	177,20
Розробка проекту мережі, студент	144	7,73	1113,12
Разом			2446,80

Крім того, слід визначити відрахування на соціальні заходи. Величну відрахувань у спеціальні державні фонди визначають у відсотковому співвідношенні від суми основної та додаткової заробітних плат. Згідно діючого нормативного законодавства сума відрахувань у спеціальні державні фонди складає 20,5% від суми заробітної плати:

$$B_Ф = 0{,}205 \cdot B_{\text{ОП}},$$

$$B_Ф = \frac{20{,}5}{100} \cdot 2446{,}80 = 501{,}59 \text{ грн.}$$

Загальна сума витрат на матеріальні ресурси (B_M) визначається за формулою:

$$B_M = \sum_{i=1}^{n} K_i \cdot Ц_i, \quad (4.3)$$

де K_i - витрата і-го типу матеріалу, натуральні одиниці вимірювання;

$Ц_i$ - ціна за одиницю *i*-го типу матеріалу, грн;

i - тип матеріального ресурсу;

n - кількість типів матеріальних ресурсів.

Звідси, витрати на матеріальні ресурси дорівнюватимуть:

B_M =48000,00+24000,00+2530,00+20890,00+450,00+1100,00=96970,00 грн.

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна за одиницю, грн.	Загальна сума, грн.
Маршрутизатор Cisco 2811	шт.	3	16000,00	48000,00
Комутатор 2950-24	шт.	2	12000,00	24000,00
Безпровідний маршрутизатор 300N	шт.	1	2530,00	2530,00
Server PT	шт.	1	20890,00	20890,00
Перехресний кабель	м.	25	18,00	450,00
Прямий кабель	м.	100	11,00	1100,00
Разом		9		96970,00

Загальна сума витрат на електроенергію розраховується за формулою:

$$B_E = \sum_{i=1}^{n} P_i \cdot k_i \cdot T_i \cdot Ц \,, \qquad (4.4)$$

де P_i - паспортна потужність *i*-го електрообладнання, кВт;

k_i - коефіцієнт використання потужності *i*-го електрообладнання (приймається 0,7¸ 0,9);

T_i - час роботи і-го обладнання за весь період розробки, год;

Ц - ціна електроенергії, грн / кВт·год;

i - тип електрообладнання;

n - кількість електрообладнання.

Для розробки проекту даної комп'ютерної мережі використовується один ПК потужністю P = 0,22 кВт з монітором потужністю P = 0,013 кВт, який за весь період розробки працює 25 годин, та друкуючий пристрій потужністю P = 0,37 кВт, який працює 3 години.

$$B_E = 0{,}9 \cdot (0{,}22 + 0{,}013) \cdot 25 \cdot 0{,}9 + 0{,}9 \cdot 0{,}37 \cdot 3 \cdot 0{,}9 = 5{,}61 \text{ грн.}$$

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Для визначення амортизаційних відрахувань застосуємо метод прямолінійного списання. Загальна сума амортизаційних відрахувань (B_{AM}) визначається за формулою:

$$B_{AM} = \sum_{i=1}^{n} \frac{B_i \cdot H_i}{100}, \qquad (4.5)$$

де B_i - вартість *i*-го обладнання на початок звітного періоду, грн;

H_i - річна норма амортизації *i*-го обладнання, %;

i - тип обладнання;

n - кількість обладнання.

Для проектування даної комп'ютерної мережі використовуються один ноутбук вартістю 7300 грн., та принтер вартістю 4150 грн.

Тоді:

$$B_{AM} = \frac{7300 \cdot 10}{100} + \frac{4150 \cdot 20}{100} = 1560{,}00 \text{грн.}$$

Транспортні витрати слід прогнозувати у розмірі 8–12 % від загальної суми матеріальних витрат.

$$B_T = 0.08 \cdot B_M \,, \qquad (4.6)$$

де B_T – транспортні витрати.

$$B_T = 0{,}08 \cdot 96970\,{,}00 = 7757\,{,}60 \text{ грн.}$$

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створенням необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати становлять 150 % від суми основної та додаткової заробітної плати працівників.

$$H_B = 1{,}5 \cdot B_{ОП} \,, \qquad (4.7)$$

де H_B – накладні витрати.

$$H_B = 1{,}5 \cdot 2446{,}80 = 3670{,}20 \text{ грн.}$$

Загальні витрати $(B_{КС})$ розрахуємо за формулою:

$$B_{КС} = B_{ОП} + B_{Ф} + B_M + B_E + B_{АМ} + B_T + H_B \quad (4.8)$$

Результати проведених розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 - Кошторис витрат

Зміст витрат	Сума, грн.
Витрати на оплату праці (осн. і дод. ЗП)	2446,80
Відрахування на соціальні заходи	501,59
Матеріальні витрати	96970,00
Витрати на електроенергію	5,61
Амортизаційні відрахування	1560,00
Транспортні витрати	7757,60
Накладні витрати	3670,20
РАЗОМ по кошторису	112911,80

4.2 Розрахунок ціни проекту

Договірна ціна $(Ц_Д)$ для проектних рішень розраховується за формулою:

$$Ц_Д = B_{КС} \cdot \left(1 + \frac{p}{100}\right), \quad (4.9)$$

де $B_{КС}$ – кошторисна вартість, грн;

p - середній рівень рентабельності, % (приймаємо 26% за погодженням з керівником).

$$Ц_Д = 112911,80 \cdot (1+0,26) = 142268,86 \text{ грн.}$$

4.3 Визначення економічної ефективності і терміну окупності капітальних вкладень

Економічна ефективність (E_P) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_P = \frac{П}{B_{КС}}, \quad (4.10)$$

де $П$ – прибуток, грн;

$B_{КС}$ – кошторисна вартість, грн.

$$E_P = 30016,81 / 112911,80 = 0,26$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_P):

$$T_P = \frac{1}{E_P} \quad (4.11)$$

Тобто:

$$T_P = 1/0,26 = 3,8 \text{ р.}$$

Прийнятним вважається термін окупності близький до 7 років.

Розраховані економічні показники проекту занесемо до таблиці 4.5.

Таблиця 4.5 - Економічні показники розробки

Показник	Значення
Собівартість, грн.	112911,80
Плановий прибуток, грн.	30016,81
Ціна, грн.	142268,86
Економічна ефективність	0,26
Термін окупності, рік	3,8

Враховуючи основі економічні показники з таблиці 4.5, можна зробити висновок, що при економічній ефективності 0,26 та терміні окупності – 3,8 роки проводити роботи по впровадженню даної мережі є доцільним та економічно вигідним. Як можна побачити із розрахунків, основними є матеріальні витрати. Тому, з метою зниження вартості мережі, варто було б здійснювати закупівлю обладнання у офіційних дилерів вказаних марок обладнання.

ВИСНОВКИ

У даній дипломній роботі були вирішені поставлені завдання, такі як:

1. Проведено аналіз версій протоколу IP, тобто було розглянуто переваги і недоліки версій протоколу IP.

2. Здійснено розробку структури мережі. В результаті було створено логічну структуру мережі підприємства, а також змодельовано мережу на основі технології IP з версіями 4 і 6.

3. Розглянуто основні технології переходу на IPv6. Так як не можливо відразу повністю перейти на мережі, що використовують тільки протокол IPv6, був виконаний аналіз технологій, що дозволяє мережам IPv4 і IPv6 взаємодіяти між собою.

4. Обрано метод переходу і здійснено на програмному продукті - PacketTracer. Після чого було проведено зміни в мережі та здійснено аналіз, який показав, що протокол версії IPv6 швидше і надійніше попередньої версії, незважаючи на більш широке використання IPv4.

5. Зроблено розрахунок економічної ефективності проекту.

Важливість переходу на технологію IPv6 полягає в тому, що глобальна павутина «Інтернет» буде вдосконалюватися і розвиватись тривалий час. Завдяки концепції IPv6 в наступні пару століть, немає необхідності пошуку альтернативних рішень проблем розширення мереж які не в змозі вирішити нинішній IPv4.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Смирнов И.Г. Структурированные кабельные системы - проектирование, монтаж и сертификация./ И.Г. Смирнов – СПб.: Экон-Информ, 2005.- 131 с.

2. Новиков Ю.В., Карпенко Д.Г. Аппаратура локальных сетей. функции, выбор, разработка./ Ю.В. Новиков., Д.Г. Карпенко – Москва: ЭКОМ, 1998.- 110 с.

3. Платонов В.В. Программно-аппаратные средства защиты информации./ В.В. Платонов – Москва: Информационная безопасность, 2013 . – 69 с.

4. Одом У. Компьютерные сети. Первый шаг./ У. Одом – СПб.: «Вильямс», 2006 . – 240 с.

5. Сайт: методичні рекомендації до виконання дипломного проекту з освітньо-кваліфікаційного рівня “Бакалавр” 2011р [Електронний ресурс] – Режим доступу: http://buklib.net/books/23878/

6. Купер Д. Архитектура корпоративных сетей/ Д. Купер – Москва: МПРЕСС, 2014 – 94 с.

7. Методичні рекомендації до виконання дипломного проекту з освітньо-кваліфікаційного рівня “Бакалавр” напряму підготовки 6.050102 «Комп’ютерна інженерія» фахового спрямування «Комп’ютерні системи та мережі» / О.М. Березький, Л.О. Дубчак, Р.Б Трембач, Г.М. Мельник, Ю.М. Батько, С.В. Івасьєв / Під ред. О.М. Березького. - Тернопіль: ТНЕУ, 2016.– 65 с.

8. Методичні вказівки до написання техніко-економічного розділу дипломних проектів освітньо-кваліфікаційного рівня «бакалавр» напряму підготовки 6.050102 комп’ютерна інженерія/ І.Р. Паздрій – Тернопіль: ТНЕУ, 2014. – 37 с.

9. Гамаюн І. П. Оцінювання міри схожості між об’єктам, що характеризуються кількісними і номінальними ознаками / І.П. Гамаюн, О.П. Безменова – Харків : НТУ «ХПІ», 2013. – 9 с.

10. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. / Б. Скляр - Москва: Информатика. Компьютеры, 2003. – 1106 с.

11. Сапаров В.Е. Руководящий документ. Выпускные квалификационные работы. Общие требования по оформлению пояснительной записки / В.Е. Сапаров - Самара: ПГУТИ, 2009. - 28 с.

12. Кулаков Ю.А. Локальні мережі. Навчальний посібник. / Ю.А. Кулаков, Г.М. Луцький - Київ: Юніор, 1998. – 45 с.

13. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире./ Б.Шнайер – СПб.: «Питер», 2003. – 368 с.

14. Портнов, Э.Л. Оптические кабели связи [Текст] / Э.Л. Портнов– М. «Информсвязь», 2000 – 112 с.

15. Руководство по Cisco IOS [Текст]. - СПб.: Питер, М.: Издательство «Русская Редакция», 2008. -784 с

16. Официальный сайт произвоизводителя оборудования Cisco Systems [Электронный ресурс] / Режим доступа – http://www.cisco.com.

17. Транспортные сети и системы электросвязи. Системы мультиплексирования: Учебник для студентов ВУЗов по специальности «Телекоммуникации» [Текст] / Под ред. В.К. Стеклова. – К.; 2003 – 352 с.

18. Дональд, Дж. Стерлинг. Техническое руководство по волоконной оптике [Текст] / Дональд Дж. Стерлинг., пер. Московченко А. – Издательство «ЛОРИ» – 1998.

19. Официальный сайт компании D-Link. Техническое описание медиаконвертора DMC-920 [Электронный ресурс] / Режим доступа – http://ftp.dlink.ru/pub/transciever_mediaconverter/DMC-920/Data_sh.

20. Основы организации сетей Cisco, том 2 [Текст].: Пер. с англ. - М.: Издательский дом «Вильямс», 2005. - 215 с.

21. Слепов Н.Н. Оптоволоконные системы дальней связи. Перспективы развития [Текст] // Н.Н. Слепов. - Электроника: НТБ – 2004. – 109 с.

22. Кульгин М. Технологии корпоративных сетей. / М. Кульгин. - Изд. «Питер», 1999. – 154 с.

23. Виткев О. Основы сетей Cisco, том 1. / Виткев О. М.: Издательский дом "Вильяме", 2005. – 231 с.

24. Перминов С. Построение розничных и дистрибьюторских сетей. / С. Перминов. - СПБ.: Информатика. Компьютеры, 2014. - 55с.

25. Олексюк В., Балик Н., Балик А. Організація комп’ютерної локальної мережі. / В. Олексюк, Н. Балик, А. Балик. – Тернопіль: Підручники та посібники, 2006. – 41 с.