Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Навчально-науковий центр заочної форми навчання*
(повна назва)
Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Побудова корпоративної мережі за допомогою мережного протоколу IPv6
(тема)

Виконав:
студент 2 курсу, групи *ІМІзм-20-2*
Бараненко О.В.
(прізвище, ініціали)
Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми *освітньо-наукова програма*

Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)

Керівник *доц. Скорик Ю.В.*
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2022 р.

.

Не містить відомостей заборонених до відкритого публікування

Студент / *Бараненко О.В.*/

Керівник  /*Скорик Ю.В.*/

Харківський національний університет радіоелектроніки
(повна назва вищого навчального закладу)
Навчально-науковий центр заочної форми навчання
Кафедра *Інформаційно-мережної інженерії*
Освітній рівень *другий (магістерський)*
Спеціальність *172 Телекомунікації та радіотехніка*
(код і назва)
Тип програми *освітньо-наукова програма*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Бараненко Олегу Вікторовичу*
(прізвище, ім'я, по батькові)
1. Тема роботи *Побудова корпоративної мережі за допомогою протоколу IPv6*

затверджена наказом університету від « *25* » *березня 2022 року* № *34 Стз*

2. Термін подання студентом роботи до екзаменаційної комісії *17 травня 2022 р.*
3. Вихідні дані до роботи *Побудувати корпоративну мережу за допомогою протоколу IPv6. Характеристики протоколу IPv6. Вибір мережного обладнання. Застосувати для моделювання програмне забезпечення Packet Tracer.*

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Опис характеристик мережевого протоколу IPv6
2. Вибір структури та топології ЛМЗ організації
3. Вибір мережного обладнання
4. Логічна організація ЛМЗ
5. Логічна організація ЛМЗ
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____

Слайди у форматі Power Point (назва та мета кваліфікаційної роботи, актуальність роботи, вступ, узагальнена структура корпоративної мережі, структурна схема корпоративної мережі компанії, заголовки IPv4 та IPv6, адресний простір IPv6, підсистема СКС, вибір мережного обладнання, логічна структура мережі, організація мережі на основі адресів IPv6, команди, що прописані у глобальному режимі конфігурації маршрутизатора, розподіл, висновки)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням.*	*25.03.22*	*виконано*
2	*Підбір літератури за темою роботи*	*26.03 – 30.03.22*	*виконано*
3	*Виконання розділу 1*	*31.03 – 12.04.22*	*виконано*
4	*Виконання розділу 2*	*13.04 – 23.04.22*	*виконано*
5	*Виконання розділу 3*	*24.04 – 06.05.22*	*виконано*
6	*Виконання розділу 4*	*07.05 – 10.05.22*	*виконано*
7	*Виконання розділу 5*	*11.05 – 15.05.22*	*виконано*
8	*Оформлення пояснювальної записки*	*16.05 – 19.05.22*	*виконано*

Дата видачі завдання *25 березня 2022 р.*

Студент _____ *Бараненко О.В.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Скорик Ю.В.*
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 67 с., 14 рис., 7 табл., 19 джерел

Мета роботи – побудова корпоративної мережі за допомогою мережного протоколу IPv6.

Розглянути основні характеристики протоколу IPv6. Вибрати структуру та топологію ЛМЗ. Розробити корпоративну мережу за допомогою обладнання Cisco та D-Link. Описати маршрутизацію на основі мережного протоколу IPv6.

ПРОТОКОЛ, КОРПОРАТИВНА МЕРЕЖА, МАРШРУТИЗАЦІЯ, ТОПОЛОГІЯ, МЕРЕЖНЕ ОБЛАДНАННЯ, КОМУТАТОР, МАРШРУТИЗАТОР

THE ABSTRACT

Explanatory note: 67p., 14 fig., 7 tabl., 19 sources

The purpose of work – create a corporate network using the IPv6 network protocol.

A review of the main characteristics of an IPv6 network protocol. Select the struct and topology of the network. Develop corporate network with Cisco and D-Links equipment.

PROTOCOL, CORPORATE NETWORK, ROUTING, TOPOLOGY, NETWORK EQUIPMENT, SWITCH, ROUTER.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

IP – Internet Protocol

IPv6 – Internet protocol version 6

IPv4 – Internet protocol version 4

CIDR – Classless Inter-Domain Routing

NAT – Network Address Translation

RFC – Request for Comments

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

ICMP – Internet Control Message Protocol

ICMPv4 – Internet Control Message Protocol for IPv4

ICMPv6 – Internet Control Message Protocol for IPv6

ToS – Type of Service

ID – Identification

NSAP – Network Service Access Point

IPS – Image Packaging System

DHCP – Dynamic Host Configuration Protocol

IGMP – Internet Group Management Protocol

ARP – Address Resolution Protocol

NTP – Network Time Protocol

MTU – Maximum transmission unit

OSI – Open Systems Interconnection basic reference model

DNS – Domain Name System

ESP – Encapsulating Secyrity Payload

IPsec – IP Security

ROHC – Robust Header Compression

RIP – Routing Information Protocol

RIPng – Routing Information Protocol

OSPF – Open Shortest Path First

IS-IS – Intermediate System to Intermediate System

ISO – International Standarts Organization

IGP – lnterior Gateway Protocol

BGP – Border Gateway Protocol

AS – autonomous system

IDRP – Interdomain Routing Protocol

IETF – Internet Engineering Task Force

VPN – Virtual private network

AH – Application Header

QoS – Quality of Service

HTTP – HyperText Transfer Protocol

SMTP – Simple Mail Transfer Protocol

RSVP – Resourse Reservation Protocol

MPLS – Multiprotocol label switching

IEEE – Institute of Electrical and Electronics Engineers

MS – Microsoft

BASE-T – Baseband twister pair

SFP – Small Form-factor Pluggable

MAC – Media Access Control

DSR – Dynamic Sourse Routing

WAN – Wide Area Network

LAN – Local Area Network

USB – Universal Serial Bus

RJ – Registered Jack

VLAN – Virtual Local Area Network

КМПД – Корпоративна мережа передачі даних

ЛСС – локальна мережа зв'язку

СКС – структурована кабельна система

ВСТУП

IPv6 розвивається вже більше 12 років, і зроблений ним шлях далеко не легкий. Стимулом процесу був дефіцит адресного простору IPv4, а також прагнення запустити нові програми, що виходять за межі обмежень старого протоколу. Криза адресного простору була відкладена завдяки декільком новим підходам до IP-адресації, найбільш значущі з яких – це CIDR, NAT та приватний адресний простір, описаний у RFC 1918. У той же час було зрозуміло, що ці рішення тільки відкладуть неминуче, тому було розпочато реконструкцію протоколу IP. Все це призвело до створення IPv6.

І хоча CIDR, NAT та приватний адресний простір виявилися успішними проектами, вони не вирішили проблему, а лише відстрочили її. Сьогодні політики виділення адрес IPv4 регіональних регістрів Internet відлякують всіх бажаючих отримати відкритий адресний простір. Адресний простір IPv4 став дефіцитним ресурсом, отримання блоку відкритих адрес тягне за собою занадто багато паперів і бюрократичної тяганини.

Якщо збільшити довжину IP-адрес, їх можна буде вільно роздавати та використовувати; вони не будуть дефіцитним ресурсом, який слід заощаджувати. IPv6 також дає можливість розгорнути нові типи програм, які засновані на використанні відкритого адресного простору або шифрують інформацію в самій IP-адресі, наприклад, множинна адресація та організація мереж з контрольованою безпекою.

Специфікації IPv6 зараз досить стабільні. Багато реалізацій були розгорнуті і використовувалися протягом багатьох років; якщо ми хочемо почати працювати з IPv6, нам більше не потрібні латки та спеціальне програмне забезпечення. У більшості операційних мереж є підтримка IPv6, а деякі постачальники активують її за промовчанням. IPv6 досягнув того стану, коли його може використовувати кожен.

1 ПРИНЦИПИ ПОБУДОВИ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ ЗА ДОПОМОГОЮ ПРОТОКОЛУ IPv6

1.1 Корпоративна мережа

Корпоративна мережа, це звичайні комп'ютерні мережі, до яких входять локальні мережі філій і відділень однієї компанії чи організації.

У корпоративній мережі локальні мережі, що знаходяться віддалено розташовуються в одному місті, на території країни або різних країн. Великі мережі мають достатньо багато комп'ютерів користувачей, серверів чи інформаційних сервісів та інших ресурсів. Ціллю будь-яких корпоративних мереж це забезпечення прозорого використання ресурсов для її користувачів, такими як час доступу, надійність, забезпечення несанкціонованого доступу до інформаційних ресурсів та ін [1].

Організація каналів передачі даних між локальними мережами на віддалених територіях можуть здійснюватися на основі (рис. 1.1):

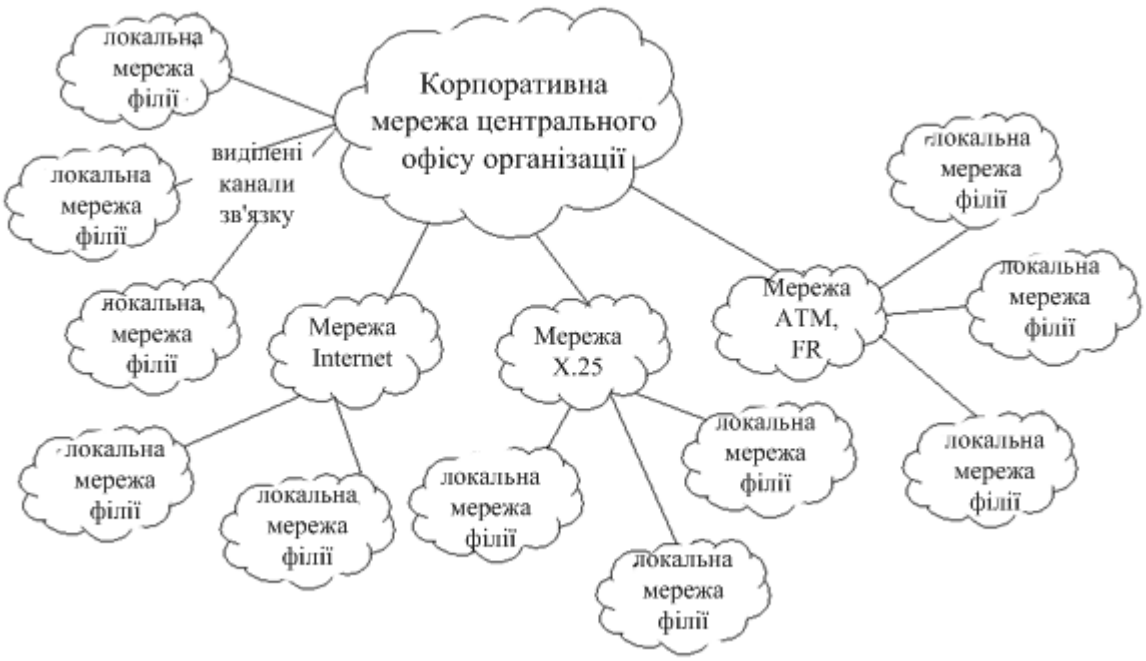

Рисунок 1.1 – Можливі варіанти організації каналів передачі даних між об'єктами корпоративної мережі

– виділених (орендованих) каналів зв'язку;

– використання ресурсів глобальних мереж.

Створення корпоративних мереж на виділених каналах є кращим варіантом. У даному випадку всі параметри мережі знаходяться у руках її власника (в т.ч. можливість використання). При цьому забезпечується необхідна пропускна здатність, використання протоколів засекречування, тобто повна незалежність від мережних операторів - постачальників послуг. Така мережа фізично відокремлена від інших мереж, що унеможливлює несанкціонований доступ до її ресурсів. Однак при великій кількості віддалених локальних мереж вартість створення і її експлуатація може виявитися досить високою [1-3].

1.2 Обладнання корпоративних мереж

Корпоративна мережа – це досить складна структура, яка використовує різні типи зв'язку, комунікаційні протоколи та засоби підключення ресурсів.

Усе обладнання мереж з передачі даних можна розділити на два великі класи – периферійне, яке використовується для підключення до мережі кінцевих вузлів, і магістральне або опорне, що реалізує основні функції мережі (комутацію каналів, маршрутизацію і т.д). Слід зазначити, що до магістрального обладнання зазвичай пред'являються підвищені вимоги в частині надійності, продуктивності, кількості портів і подальшої розширюваності. Периферійне обладнання є необхідним компонентом будь-якої корпоративної мережі. Функції ж магістральних вузлів може брати на себе глобальна мережа передачі даних, до якої підключаються ресурси. Як правило, магістральні вузли в складі корпоративної мережі з'являються тільки в тих випадках, коли використовуються орендовані канали зв'язку або створюються власні вузли доступу [2].

Периферійне обладнання корпоративних мереж це маршрутизатори (routers), які служать для об'єднання однорідних LAN (як правило, IP або IPX) через глобальні мережі передачі даних. Маршрутизатори можуть бути виконані

як у вигляді автономних пристроїв, так і програмними засобами на базі комп'ютерів і спеціальних комунікаційних адаптерів [1-3].

Серед маршрутизаторів найбільш відомі продукти компанії Cisco Systems, що реалізують широкий набір засобів і протоколів, використовуваних при взаємодії локальних мереж. Обладнання Cisco підтримує різноманітні засоби підключення, це й X.25, Frame Relay та ISDN, дозволяє створювати доволі складні системи.

Основною областю застосування маршрутизаторів Cisco – складні мережі, що використовують у якості основного протоколу IP або, рідше, IPX. Для корпоративної мережі призначеної для об'єднання віддалених LAN, передачі голосу і вимагає складної маршрутизації IP або IPX через різнорідні канали зв'язку і мережі передачі даних використання обладнання Cisco є оптимальним вибором [1].

1.3 Вимоги до корпоративних мереж

Корпоративна мережа передачі даних (КМПД) – це телекомунікаційна мережа, яка об'єднує в єдиний інформаційний простір всі структурні підрозділи компанії. Корпоративна мережа забезпечує одночасну передачу голосу, відео і даних, взаємодія системних додатків, розташованих в різних вузлах, і доступ до них користувачів.

КМПД це як єдина інформаційна система підприємства, що дозволяє спільно користуватися мережними ресурсами компанії – сервери, комп'ютери та багато інших пристроїв, що підключаються до мережі (принтери, модеми), і ще забезпечувати роботу необхідних для компанії бізнес-додатків, таких як мережні бази даних, файловий обмін, електронна пошта, IP-телефонія, системи взаємовідносин з клієнтами (CRM), системи управління (ERP-системи) і т.п. КМПД підприємства показана на рис. 1.3 [1-4].

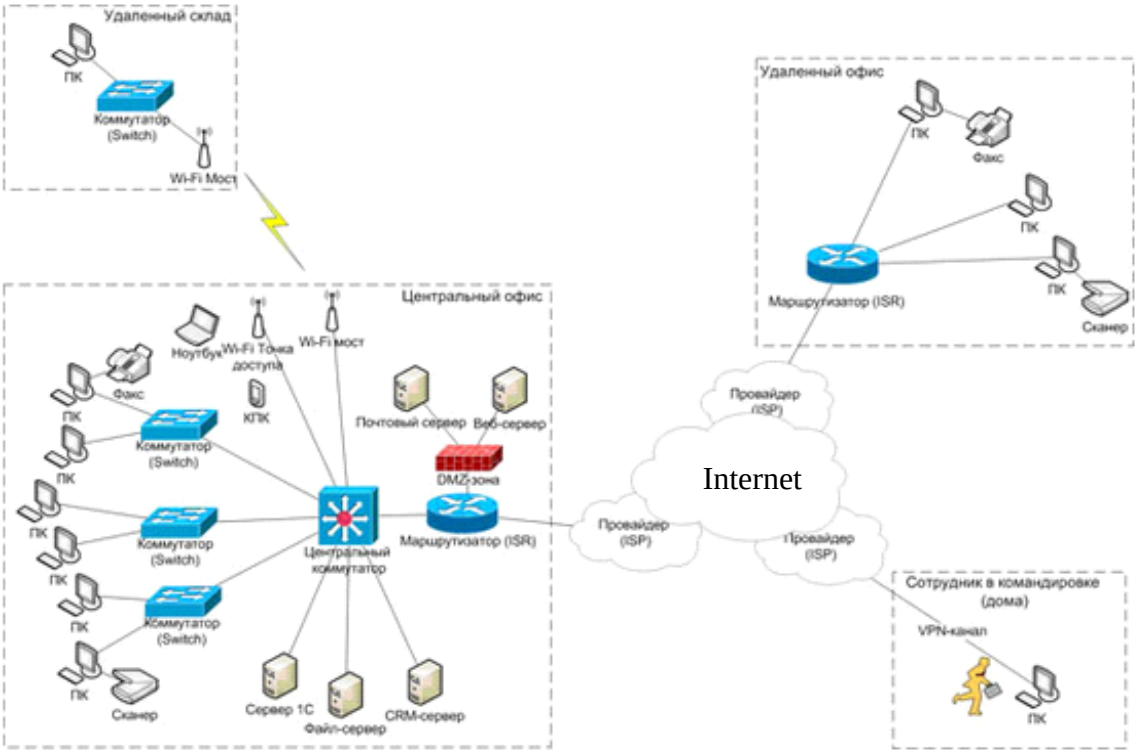

Рисунок 1.3 – КМПД підприємства

Корпоративна мережа є одним з ключових засобів розвитку бізнесу. Основні вимоги, що пред'являються до КМПД, полягають у наданні всіх необхідних телекомунікаційних та інформаційних сервісів підрозділам компанії при оптимізації капітальних витрат на створення мережі та мінімізації вартості обслуговування. Виходячи з цього, основні принципи побудови корпоративних мереж включають до себе наступне [5]:

- передача всіх типів трафіку повинна відбуватися за єдиними каналами зв'язку; іншими словами, корпоративна мережа повинна бути мультисервісною.

- корпоративна мережа повинна будуватися на базі відкритих стандартів і інтерфейсів з метою забезпечення можливості нарощування мережі і об'єднання її з іншими мережами.

- виходячи з принципу мінімізації витрат на створення і експлуатацію мережі, корпоративна мережа повинна бути мережею з комутацією пакетів. Обгрунтуванням цього принципу є висока ефективність використання каналів зв'язку в мережах з комутацією пакетів у порівнянні з мережами з комутацією

каналів. Це особливо важливо для мінімізації вартісних показників корпоративної мережі.

Найбільш ефективне рішення із побудування корпоративних мереж передачі даних запропоновано компанією Cisco Systems, воно представляє модульний підхід до побудови структури мережі і базується на композитній мережній моделі підприємства. Це рішення дозволяє будувати як невеликі мережі, які об'єднують кілька офісів, так і великі, що включають сотні вузлів. При цьому забезпечується передбачуваність якісних характеристик мережі при її розвитку шляхом додавання нових модулів або вузлів, і потрібний мінімальний час для пошуку та усунення несправностей [6].

На рис. 1.4 представлена композитна модель корпоративної мережі.

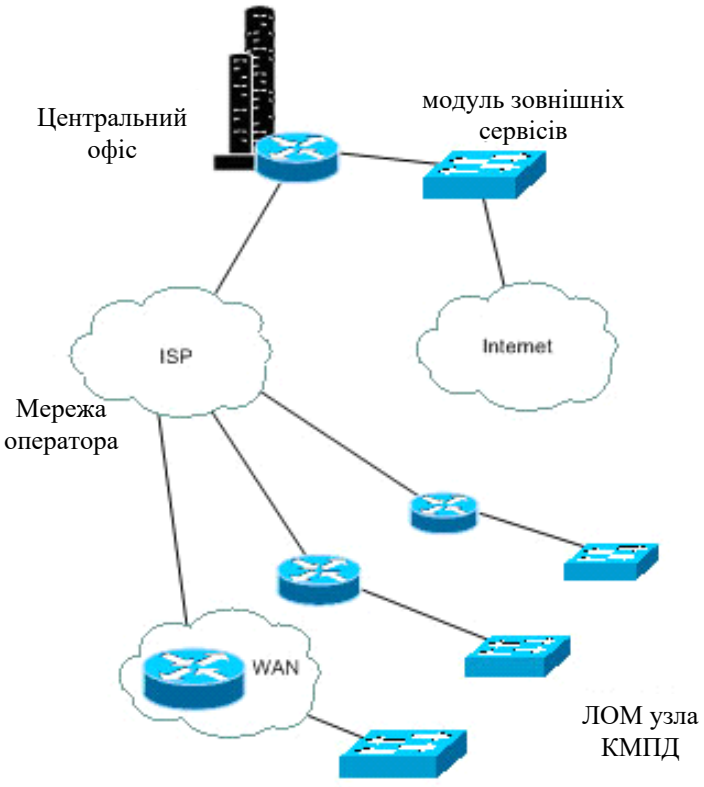

Рисунок 1.4 – Модель корпоративної мережі

Композитна модель базується на принципі розподілу мережі на окремі модулі, кожен з яких має особливі функції та свої особливості реалізації. Для кожного вузла системи передачі даних основними такими модулями є:

– модуль зовнішніх сервісів;

– модуль глобальної мережі (WAN, Wide Area Network);

– модуль локальної обчислювальної мережі (ЛОМ).

При проектуванні корпоративної мережі організації в залежності від функції, що пред'являється до мережі, можуть бути організовані наступні підсистеми КМПД: підсистема під’єднання до мережі загального користування Internet, підсистема доступа до корпоративної мережі, підсистема бездротового доступу до корпоративної мережі, підсистема безперебійного живлення, підсистема моніторингу параметрів навколишнього середовища, підсистема доступу віддалених співробітників до ресурсів підприємства [1-4].

На рис. 1.5 представлено побудову корпоративної мережі компанії.

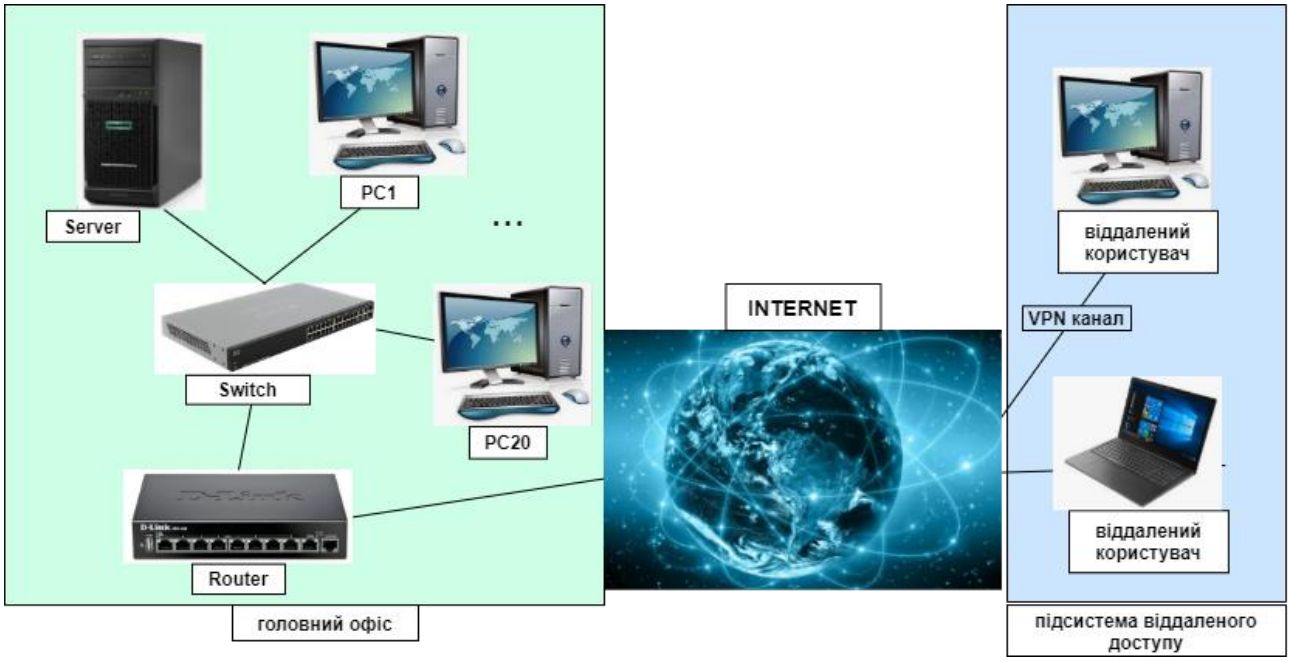

Рисунок 1.5 – Модель корпоративної мережі компанії

1.4 Організація корпоративних мереж на основі VPN: побудова, управління, безпека

VPN є технологією, яка забезпечує мережні з'єднання поверх інших мереж, наприклад, Інтернет. Комунікація усередині віртуальної мережі відбувається за базовими каналами з низьким рівнем довіри, а з використанням засобів шифрування дозволяє забезпечити максимальну безпеку передачі даних. Ця відносно недорога і проста в реалізації технологія останнім часом набуває все більш широкої популярності [2].

Існує кілька способів побудови корпоративних мереж. До недавнього часу найбільшою популярністю користувалися системи Local Area Network (LAN), які об'єднують обмежену кількість ПК. Вони забезпечують максимальну швидкість обміну файлами і абсолютну безпеку інформації, так як її потоки не потрапляють в загальний доступ. Використання структур цього типу є безкоштовним. До мінусів LAN можна віднести високу вартість і неможливість підключення віддалених користувачів.

Гідною альтернативою стали віртуальні мережі - Virtual Private Network (VPN), які будуються поверх глобальних мереж WAN, що охоплюють велику кількість ПК і комп'ютерних систем по всій планеті. До їх безперечних достоїнств відносяться простота (а відповідно, і невисока вартість) побудови, можливість підключення безлічі абонентів, що знаходяться в різних кінцях світу, і безпеку передачі даних [1-3].

Саме завдяки гнучкості та економічності, VPN активно витісняють LAN з ринку. Так, за результатами досліджень, проведених Forrester Research Inc. і Infonetics Research, витрати на використання та обслуговування VPN майже в три рази нижчі, ніж логістичних структур, побудованих за технологією LAN.

1.4.1 Переваги та недоліки VPN

Virtual Private Network легко масштабується і є оптимальним варіантом для підприємств, що володіють безліччю філій, а також для фірм, чиї

співробітники часто бувають у відрядженнях або працюють з дому. Підключення нового офісу або нового віддаленого співробітника здійснюється без додаткових витрат на комунікації. Крім того, первісна організація віртуальної системи вимагає мінімум грошових витрат. Надалі фінансові вкладення будуть зводитися до оплати послуг провайдера Інтернету.

Є у Virtual Private Network і певні недоліки. Так, фірмам, що використовують їх, слід подбати про безпеку переданих даних, тому що документи в процесі передачі проходять через Всесвітню мережу, Інтернет. Для вирішення цього завдання використовуються спеціальні алгоритми шифрування даних, що дозволяють захистити файли під час передачі [4-6].

Крім того, у віртуальній структурі швидкість обміну файлами помітно нижче, ніж в її приватних аналогах. Але для передачі невеликих обсягів інформації цього може бути цілком достатньо.

Згідно з відомостями, наданими дослідницькою організацією Forrester Research Inc., 41% підприємств віддають перевагу офісним мережам тому, що вони дозволяють вирішити проблеми з віддаленим доступом, 30% компаній цінують їх за економію коштів, а 20% - за суттєве спрощення роботи.

1.4.2 Безпека в корпоративних мережах

Захист даних передбачає їх шифрування, підтвердження автентичності та контроль доступу. Найбільш популярними алгоритмами кодування вважаються DES, Triple DES і AES.

Безпрецедентна безпека забезпечується спеціальними протоколами, які упаковують дані в єдиний компонент і формують з'єднання (тунель), а також шифрують інформацію всередині утвореного тунелю. В даний час найбільш широко використовуються наступні набори протоколів:

1. PPTP (Point-to-Point Tunneling Protocol) – тунельний протокол, що забезпечує збереження автентичності, стиснення і шифрування даних. Корпорація Microsoft пропонує для протоколу PPTP використовувати

метод шифрування MPPE. Крім того, інформацію можна передавати у відкритому, незашифрованому вигляді. Інкапсуляція даних здійснюється шляхом додавання заголовків GRE і IP.

2. L2TP (Layer Two Tunneling Protocol) – протокол, розроблений шляхом об'єднання протоколів PPTP і L2F. Він забезпечує більш надійний захист файлів, ніж PPTP. Шифрування здійснюється за допомогою протоколу IPSec (IP-security) або 3DES. Максимальну безпеку передачі даних забезпечує другий варіант, але його використання призводить до зниження швидкості з'єднання і підвищення навантаження на центральний процесор [4].

Підтвердження достовірності необхідно для того, щоб інформація дійшла до адресата в незміненому вигляді. Операція виконується за допомогою алгоритмів MD5 і SHA1 і включає перевірку цілісності документів, а також ідентифікацію об'єктів. Ідентифікація здійснюється як за допомогою традиційних операцій введення логіна і пароля, так і за допомогою більш надійних засобів - сертифікатів і серверів для перевірки їх достовірності [1-4].

1.4.3 Використання і управління корпоративною мережею на базі VPN

Мережа в офісі – це просте і зручне рішення як для фірм з великою кількістю філій і віддалених користувачів, так і для компаній, що бажають мати недорогу, легку в управлінні і гнучку систему. Ця технологія дозволяє додавати нові структурні елементи, а також істотно збільшувати розміри мереж без серйозного розширення інфраструктури. Робити це може сам замовник без залучення провайдера до вирішення цих завдань. Додавання нового абонента займе всього кілька хвилин [4].

Керування такими системами не становить труднощів для користувача, так як більша частина функцій адміністратора в Virtual Private Network автоматизована. Фахівці провайдера інсталюють на сервері клієнтської фірми необхідне програмне забезпечення, а також створюють базу суб'єктів і об'єктів

VPN (для кожного суб'єкта генерується ключ шифрування). Потім ця база зберігається на знімному носії та передається замовнику.

Користувачеві необхідно буде тільки підключати ключ-карту до комп'ютера для ідентифікації та отримання доступу. Якщо в процесі роботи захищеної корпоративної мережі виникають будь-які неполадки, то замовнику слід звернутися до провайдера, і він вирішить ці проблеми в термін, обумовлений умовами контракту [1-3].

VPN – це рішення, що актуальне для середніх та великих компаній, що мають у своєму штаті фахівців, що працюють віддалено, а також відділення в інших містах і країнах. Крім того, подібні системи просто незамінні для організацій, у яких:

- часто змінюється коло осіб і структурних підрозділів, які потребують у доступі до конфіденційних даних (відповідно, необхідно, щоб структура була досить гнучкою і легко конфігурується);

- є абоненти, яким потрібно надати доступ до даних різного рівня (співробітники, клієнти, постачальники);

- є необхідність у створенні декількох логічних мереж в рамках однієї фізичної структури (наприклад, якщо потрібно створити власну систему для кожного підрозділу підприємства) [4].

2 ХАРАКТЕРИСТИКА IPV6

2.1 Виснаження адресного простору

Адресний простір – ресурс, обмежений як IPv4, так IPv6. Існує лише стільки адрес, скільки можна виділити з будь-якого фіксованого діапазону. У цьому контексті оптимізація означає дві речі. По-перше, модель IPv6 враховує проблеми IPv4, концентруючись на тому, що отримає кінцевий користувач. Іншими словами, адресується нестача певних корисних функцій. Особливу увагу ми хотіли б звернути на такий елемент конструкції IPv6, як функції управління. В даний час управління IPv4 на підприємствах викликає серйозні проблеми та IPv6 має достатній потенціал, щоб ці проблеми вирішити, ніхто не обіцяє негайної вигоди при реалізації організацією IPv6 [7].

Другий аспект оптимізації конструкції IPv6 полягає в спрощенні механізмів побудови IP, наприклад, основні заголовки IP були урізані до необхідного мінімуму. Теоретично це має призвести до збільшення продуктивності і зниження вартості маршрутизаторів, так як пакет IPv6 вимагає меншої обробки, ніж пакет IPv4. Це також має призвести до покращень у таких областях, як стиснення заголовків [7].

2.2 Пакети та структури

Структура пакетів IPv6 багато схожа на структуру пакетів IPv4. Деякі поля були видалені, деякі – додані, але найпомітніші зміни стосуються розмірів адрес. У той час як адреси відправника та одержувача IPv4 мають довжину 32 біти, адреси IPv6 займають 128 біт.

На рис. 2.1 та 2.2 проілюстровані відмінності між заголовками IPv4 та IPv6 [7].

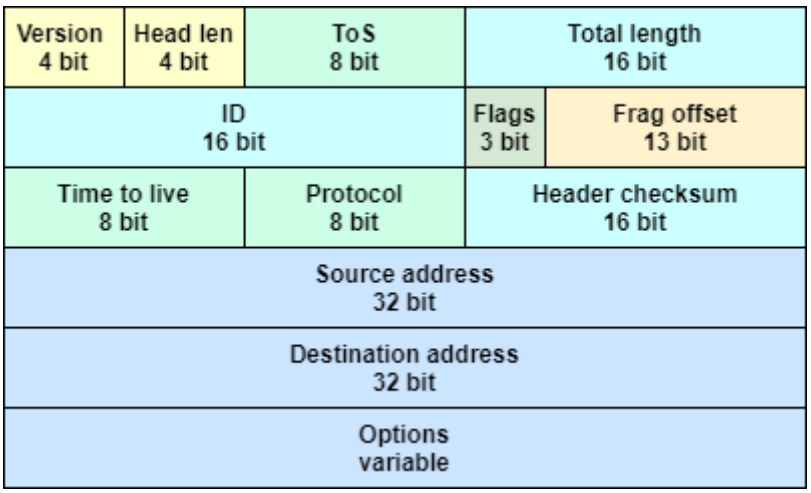

Рисунок 2.1 – Заголовок IPv4

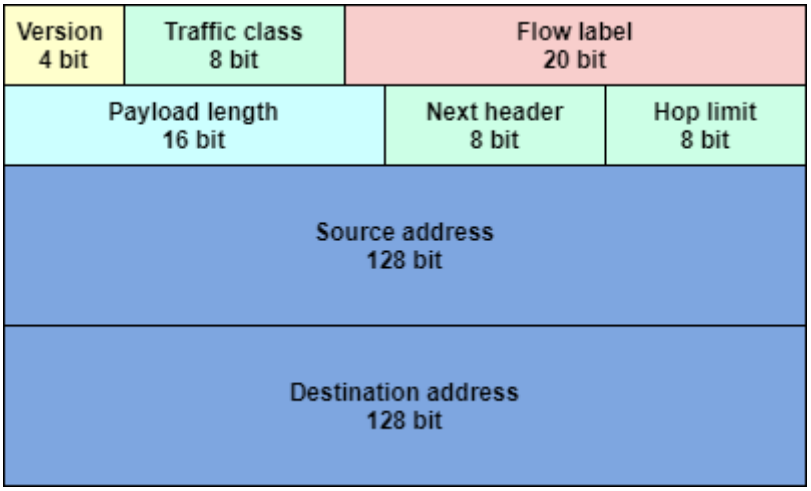

Рисунок 2.2 – Заголовок IPv6

У цілому IPv6 спрощує структуру основного заголовку, включаючи лише інформацію, яка необхідна передачі пакета. Це виливається в те, що, на відміну від IPv4, заголовок має фіксовану довжину. Заголовки фіксованої довжини сильно полегшують життя розробникам маршрутизаторів та програмістам, тому що вони дозволяють розподіляти пам'ять та реалізовувати алгоритми більш ефективно. Інша інформація, яка традиційно зберігалася в заголовку IPv4, тепер зберігається в ланцюзі за наступними заголовками, що визначаються полем next

header [8]. Кінцевими заголовками зазвичай є заголовки TCP, UDP або ICMPv6. Таким чином, завдання просування даних можна вирішити, працюючи лише з першими бітами отриманого пакета.

Багато знайомих полів мають еквіваленти в IPv6: Version (версія), ToS/Traffic Class (тип обслуговування/клас трафіку), Total Lengt/Payload Length (повна довжина/ефективна довжина), Time to Live/Hop Limit (час життя/граничний та кількість стрибків), Protocol/Next Header (протокол/наступний заголовок), адресу відправника та адресу одержувача. Проте відсутні поля фрагментації (ID, Flags, Offset) та контрольної суми заголовка, Поле Traffic Class замінено досконалішим полем Flow Label (мітка потоку), обидва використовуються для контролю за якістю обслуговування. Протоколи TCP і UDP не змінилися, проте окремо взяті протоколи рівня додатків, у яких жорстко визначено розмір адреси, під час переходу до нового світу можуть піднести неприємні сюрпризи [7,8].

2.3 Принципи адресації

Насамперед потрібно знати, що IPv6 бувають різних типів (індивідуальні, групові, альтернативні) і мають різну область дії (канальні, глобальні тощо). Тип адреси визначає, якій кількості машин призначаються пакети – однією чи багатьом. Область дії адреси визначає контекст, де використання цієї адреси має сенс. IPv6 надаються інтерфейсам вузлів, а не самим вузлам. Це велика відмінність від Pv4, в якому адреса, пов'язана з інтерфейсом машини, часто є самою машиною. Натомість в інтерфейсів IPv6 зазвичай буває більше однієї адреси IPv6, що, звичайно, корисніше. Фактично IPv6 допускає адреси з обмеженою областю Дії, які в певному контексті можуть трактуватися єдиним чином, наприклад, більшість інтерфейсів мають локальну канальну адресу, яка є унікальною тільки на цьому каналі. Це означає, що два інтерфейси вузла можуть мати однакові локальні канальні адреси за умови, що вони прикріплені до різних каналів [7-9].

Іншим важливим поняттям IPv6 є ідентифікатор інтерфейсу. У світі IPv4 адреса ділиться на мережну та хостову частини, прикладом у термінах CIDR є 137.43.0.0/16. У світі IPv6 хостова частина називається ID інтерфейсу. Він використовується для вибору певного інтерфейсу в межах зазначеної мережі так само, як хостова частина IPv4 адреси вибирає хост в певній підмережі.

Такий поділ має ряд корисних властивостей. Можливо, найцікавішим із них у перспективі є автоматичне призначення ідентифікаторів інтерфейсів.

Звичайно, ще залишається налаштування адрес та інтерфейсних ідентифікаторів вручну або за допомогою DHCPv6, і в деяких випадках цей варіант є більш привабливим [7-9].

2.4 Представлення IPv6

Подання адрес IPv6 сильно відрізняється від IPv4. Маючи значно збільшений адресний простір, ефективне використання та опис адрес lPv6 стає більш важливим, ніж у IPv4, де ніколи не потрібно більше 16 натискань клавіш, щоб дістатися до кінця адреси. Основні відмінності виділено нижче.

- Шістнадцяткове уявлення:

Замість звичної десяткової системи адреси IPv6 представлені у шістнадцятковій системі числення, звичайної у світі комп'ютерних та мережевих технологій. На даний момент досить помітити, що окремі «цифри» адрес IPv6 можуть змінюватися не тільки в діапазоні від 0 до 9, але і від A до E Таким чином, адреса може починатися, наприклад, з 2002, або з 20FE, або навіть з BD59 . І хоча в прикладах RFC 3513 використовуються великі літери, адреси IPv6 не є чутливими до регістру [9].

- Групування та поділ:

У поданні IPv4 адреси "групуються" друкарським способом - точками (.) на межі октетів. IPv6 адреси групуються за допомогою двокрапок (:) через кожні 16 біт. Якщо адреси мають довжину 128 біт, отримуємо 8 груп, у кожній з яких присутні 4 шістнадцяткові цифри.

Наприклад, 2001:0DB8:5002:2019:1111:76ff:FEAC:E8A6.

- Елізія:

Більшість адрес IPv6 містить повторювані елементи, особливо часто - нулі. Існують способи уникнути написання або приховати їх, щоб прискорити опис цих адрес. Можна уникнути написання всіх елементів адреси під час таких умов [9]:

- Елемент адресної групи починається одним чи більше нулями.

- За наявності однієї або більше груп нулів.

У першому випадку передні нулі можна опустити за умови, що у групі залишиться хоча б одна шістнадцяткова цифра. У другому випадку послідовність груп нулів може бути замінена знаком «::». Другу елізію можна зробити лише один раз, тому що в іншому випадку адресу не можна буде розшифрувати однозначно.

Існують певні класи адресного простору, для яких має сенс повернутися до старого запису IPv4. Досить сказати, що адреса ::137.43.4.16 також є дійсною адресою IPv6 і може бути записаний як 0000:0000:0000:0000:0000:0000:892b:0410 [7-9]

2.5 Робота з підмережами

В IPv4 робота з підмережами дозволяє обрати фрагменти адресного простору та розділяти їх, створюючи або більше мереж, або звільняти для деяких людей більше адрес. Звичайним прикладом поділу на підмережі для створення більшої кількості підмереж є надання провайдером послуг Internet частини свого адресного простору клієнту. Прикладом створення додаткових адрес може стати ситуація, коли відділ продажів компанії вичерпав надані йому адреси, а у відділу дослідження та розробки ще є невикористані. Якщо відділ розробки та дослідження використовує менше половини з 256 адрес у своїй

підмережі /24, то можна забрати у них підсіти /25 і віддати її відділу продажів [9].

IPv6 передбачається, що підмережі повинні мати розмір щонайменше 64 біти, навіть у з'єднаннях типу точка-точка. Так як одна мережа /64 дає простір для більш ніж мільярда хостів, є підстави вважати, що зміна структури підмереж для надання додаткових адрес в межах однієї мережі більше не знадобиться. Межа в 256 адрес (з яких, зрозуміло, використовується лише 254) у своїй /24. IPv4 не матиме іншого вибору, крім організації підмереж – створення іншого фрагмента мережі, суміжного або несумісного з вихідними адресами – і додавання туди серверів з подальшою зміною маршрутизації в межах підприємства. А в IPv6, оскільки сервери можуть мати різні ідентифікатори інтерфейсів, всі вони можуть існувати в одній підмережі. Це дозволяє великим групам машин мирно уживатися у будь-якій підмережі [8,9].

Отже, основною причиною використання підмереж стає призначення мереж для різних адміністративних і технічних цілей, таких, як безпека або маршрутизація. Щоб спростити цей процес, передбачається, що організаціям, які потребують внутрішнього розбиття на підмережі, завжди буде призначатися мережа /48 . Це означає, що кожен зможе працювати з 16 «мережевими» бітами, або з 65536 різними підмережами. Цього вистачить будь-кому [8].

2.6 Архітектура адреси

У мережах IPv4 було ознайомлено з поняттями приватного та відкритого адресних просторів. Приватним адресним простіром називається адресний простір, що використовується у межах мережі організації; теоретично до нього не можна звернутися ззовні (часто люди тішать себе думкою, що це дає їм додаткову безпеку). Ці адреси є представниками адресних просторів зі спеціальними властивостями – і часто адресні простори такого типу можна визначити, глянувши на адресу.

Також і в IPv6 є деяка кількість адресних просторів (табл. 2.1), які зазвичай виділяються за допомогою префікса з довжиною мережі CIDR [7-10].

Таблиця 2.1 – Поділ адресного простору IPv6

Префікс	Передбачуване використання
::0/96	Невстановлені/закільцьовані/IPv4-сумісні адреси
::ffff:0.0.0.0/96	Відображені адреси IPv4
200::/7	Зарезервовані для розміщення NSAP (RFC 1888)
400::/7	Зарезервовані для розміщення IPS
2000::/3	Глобальна одноправна передача
fe80::/10	Локальна канальна односпрямована передача
fec0::/10	Вузлова локальна однонаправлена передача
fc00::/7	Локальні адреси для однонаправленої передачі
ff00::/8	Багатоадресне розсилання

2.7 Локальна канальна адресація

Локальний канальний префікс містить адреси, що мають сенс тільки на одному каналі. Фактично цей префікс використовується практично на всіх каналах, на яких налаштований IPv6. Це означає, що локальна канальна адреса fe80::feed може відноситися до різних комп'ютерів залежно від того, яку мережу ви використовуєте, практично так само, як і адреса 127.0.0.1 відноситься до різних машин залежно від того, якою машиною користуватися.

У цьому контексті канал є групою машин, які можуть безпосередньо спілкуватися без залучення маршрутизатора IPv6. Це може бути канал типу точка-точка, широкомовний канал або щось складніше, але пакети, що використовують локальну канальну адресацію, ніколи не проходять через маршрутизатор. Адреси, що мають силу тільки на локальному каналі, можуть здатися не дуже корисними, однак вони є частиною автоматичного конфігурування IPv6 [9].

Важливо відзначити, що хости генерують локальну канальну адресу завдяки тому, що вони приєднані до каналу; для генерування цих адрес не потрібно ні маршрутизатора, ні втручання будь-яких інших зовнішніх факторів. Тому невеликий офіс з декількома з'єднаними комп'ютерами та одним комутатором може скористатися локальною канальною адресацією для забезпечення роботи нескладної мережі. Це один із найзначніших вкладів IPv6 у полегшення завдання управління, особливо для невеликих організацій [8,9].

Локальні канальні адреси можна використовувати, коли немає крайньої необхідності в «реальних» адресах. Наприклад, канали типу точка-точка між двома маршрутизаторами можуть працювати тільки з локальними каналами, не вимагаючи виділення глобальних однонаправлених адрес. Однак IPv6 був побудований так, щоб виключити брак адрес, і такий спосіб збереження адрес не повинен бути необхідним. До того ж, маршрутизаторам можуть знадобитися реальні адреси для надсилання повідомлень про помилки ICMP або для віддаленого керування [8].

Автоматично настроювані локальні канали в певному сенсі схожі на адреси 169.254.0.0/16 IPv4, які іноді використовуються у разі відсутності сервера DHCP або у разі передачі інформації тільки локальним каналом. Адреси IPv6 відрізняються тим, що передбачається їхня унікальність і незмінність, у той час як адреси IPv4 можуть накладатися один на одного і змінюватися внаслідок дозволу таких накладень [9].

2.8 Локальна об'єктна адресація

Локальна об'єктна адресація – дуже цікава ідея, яка чимось нагадує приватний адресний простір IPv4. Ці адреси призначені для використання в межах об'єкта, проте зовсім не обов'язково, що вони будуть досягатися із зовнішнього світу. Існує багато думок щодо визначення об'єкта, на яку можна виділити якийсь адресний простір. Підставою для такої адресації є те, що її

використання відбивається на застосуванні глобальної адресації, і тому вона має спростити управління адресами та спонукати до розумного використання обох адресацій [9].

На відміну від локальних канальних адрес, унікальність яких потрібно лише на каналі, для локальних об'єктних адрес потрібно так налаштувати маршрутизатор, щоб уникнути повторення в межах одного об'єкта.

На даний момент практичні подробиці того, навіщо і як розгортати локальну об'єктну адресацію все ще перебувають у стадії обговорення. Є спільне бажання уникнути низки проблем, що виникають при злитті приватних мереж. Можливо, це означає, що з'являться локальні об'єктні адреси, які будуть унікальними глобально. Однак здається, що від локальних об'єктних адрес, як це спочатку замислювалося в IPv6, відмовилися і подробиці нової «унікальної локальної індивідуальної адресації» скоро мають бути визначені. Враховуючи необхідність стабільної внутрішньооб'єктної адресації, незважаючи на виділені провайдером глобальні адреси, значні зусилля докладаються у напрямку пошуку відповідної заміни локальної об'єктної адресації [9].

Для того, щоб надати практично всім організаціям у світі унікальні адреси, було виділено досить великі локальні об'єктні та унікальні локальні адресні простори. Таким чином, з'являється ризик того, що ці адреси перестануть бути глобальними та маршрутизованими. Основна проблема полягає в тому, що поки що незрозуміло, як вирішувати технічні проблеми, пов'язані з маршрутизацією такого великого неструктурованого адресного простору.

На даний момент найкраще, що можна зробити з локальною адресацією, – це забути про її існування. Як тільки її майбутнє проясниться, деяким людям вона може бути корисною, але зараз абсолютна більшість людей може обійтися без об'єднання локальної канальної та глобальної адресацій [10].

2.9 Групова адресація IPv6

Груповий адресний простір, розбитий на частини, що відбивають різні типи індивідуальних адрес. Групові адреси мають форму ffXY:, де X відповідає 4 бітам прапорів, а Y - області дії групової розсилки [8-10].

Старший біт прапорів зарезервований і має бути нульовим. Молодший біт дорівнює одиниці, якщо групова адреса є тимчасовою, а не відомою. Для відомих адрес всі інші прапори повинні мати значення 0, інші значення зарезервовані для майбутнього використання.

Ситуація з тимчасовими адресами трохи заплутаніша, потрібен лише короткий її розгляд. Тут значення двох середніх прапорів є суттєвим. Значення середніх прапорів 00 означає довільне призначення адрес, при якому адреси призначаються тими, хто керує роботою каналу/вузла/мережі, які відповідають області дії адреси [11].

Значення середніх прапорів 01 вказує на призначення адрес, засноване на індивідуальному префіксі, в якому завдяки використанню блоків (префіксів) IPv6 адрес автоматично стає доступним блок групових адрес IPv6. І нарешті, значення середніх прапорів 11 відповідає ще одному призначенню розміщених індивідуальних адрес, але в цьому випадку груповий адрес включається також точка зустрічі. Точкою зустрічі називається місце у груповій мережі, яке працює як точка розподілу конкретного групового потоку. Локалізація точки зустрічі для деяких типів групової маршрутизації є нетривіальним завданням, тому її включення на адресу значно полегшує життя [10-13].

Значення області дії наведено у табл. 2.2 разом з відповідними ним префіксами для відомих та простих тимчасових адрес. Там же наведено схожі блоки адрес для інших значень прапорів.

В межах кожного відомого діапазону деякі адреси відведені для спеціального використання. Деякі призначення мають змінну область дії, тобто вони можуть призначатися для будь-якого дійсного значення області дії. Наприклад, ff0X::101 призначається NTP серверам з ділянкою X [12].

Таблиця 2.2 – Значення областей дії для групового розсилання

Область дії	Значення	Відомі	Тимчасові
Зарезервована	0	ff00::/16	ff10::/16
Локальна вузлова	1	ff01::/16	ff11::/16
Локальна канальна	2	ff02::/16	ff12::/16
Локальна об'єктна	5	ff05::/16	ff15::/16
Локальна, організації	8	ff08::/16	ff18::/16
Глобальна	E	ff0e::/16	ff1e::/16
Зарезервована	F	ff0f::/16	ff1f::/16

Інші призначення дійсні лише в межах певних областей, наприклад серверам DHCPv6 призначаються локальні об'єктні адреси ff05::1:3.

У деяких випадках можуть бути визначені діапазони адрес. Наприклад, ff02::1:ff00:0/104 – діапазон для групового розсилання на активних вузлах. Якщо у вузла є адреса, що закінчується, скажімо, a5: cdef, то він повинен бути частиною групи ff02:: 1: ffab: cdef. Якщо в інтерфейсу можливо кілька індивідуальних адрес, на цьому інтерфейсі можуть жити і кілька групових адрес активних вузлів. Однак, якщо ідентифікатор інтерфейсу для всіх індивідуальних адрес однаковий, то інтерфейсу потрібно буде об'єднати лише одну групу активних вузлів [13].

Однак є дві групові адреси, про які повинен знати кожен: ff02::1 та ff02::2. Перший є локальним канальним адрес всіх вузлів, приблизний еквівалент немаршрутизованого широкомовного адреси в 255.255.255.255 IPv4. Друга адреса – локальна канальна адреса всіх маршрутизаторів, що має велике значення для автоматичного конфігурування IPv6. Також існує термін "Альтернативна адресація" (англ. "Anycast"). Альтернативні адреси – щось середнє між: індивідуальними та груповими адресами. Індивідуальна адреса

призначається одній машині і всі пакети доставляються їй. Групова адреса призначається багатьом машинам і пакети доставляються всім таким машинам. Альтернативні адреси призначаються багатьом машинам, але кожен пакет доставляється лише з цих машин [13].

2.10 ICMPv6

TCP та UDP при переході з IPv4 на IPv6 не зазнали жодних змін. З ICMP зовсім інша історія, оскільки ICMPv6 виконує самі функції, що й ICMP, IGMP і ARP у світі IPV4. У RFC 2463 йдеться про ту частину ICMPv6, яка має найбільшу схожість із ICMPv4 [3]. У ній описані відповіді та запити ICMP, що використовуються при реалізації відомої програми ping. У ній також описані помилки, які повертаються у разі виникнення неполадок з пакетом: Destination Unreachable (мета недосяжна, через маршрутизацію, фільтрацію пакетів або відсутність чого-небудь ще), Packet Too Big (занадто великий розмір пакета), Time Exceeded (перевищено час очікування, пакет зробив занадто багато стрибків) та Parameter Problem (помилка параметра, невідомий чи неправильний заголовок). Повідомлення ICMP в IPv4 часто ігнорувалися, що, як правило, призводило до неспрацьовування таких інструментів, як ping і traceroute, або затримки при очікуванні повідомлень «мета не знайдена». IPv6 у цьому плані буде менш великодушним, оскільки коректна робота ICMP дуже істотна для протоколу. Для правильного функціонування TCP та UDP особливо актуальними стали повідомлення Packet Too Big, оскільки маршрутизаторам IPv6 заборонено фрагментувати пакети. Взлам потрібно повідомити про те, що розмір пакета потрібно зменшити у випадку, якщо він не міститься в каналі MTU. Процес обчислення максимального розміру пакета, який можна відправити даному одержувачу, називається визначенням шляху MTU (path MTU discovery). Визначення MTU шляху IPv6 описано в RFC 1981. Взлам IPv6 необов'язково використовувати визначення MTU шляху, однак у такому разі вони не зможуть відправляти пакети розміром більше 1280 байт - мінімальний MTU, що допускається в IPv6 [14].

Повідомлення про помилки ICMP також явно обмежені у швидкості стеком. Зазвичай це накладає жорсткі рамки на кількість повідомлень, що відправляються в одиницю часу, або призводить до зменшення смуги пропускання каналу. Це допоможе уникнути помилок, що здійснюються IPv4 щодо надмірно старанної або надто пасивної генерації повідомлень ICMP. Для дозволу адрес IPv4 використовується ARP; IPv6 застосовується механізм, відомий як виявлення сусідів. Виявлення сусідів дає нам додаткові можливості, яких не було у IPv4. Механізм виявлення сусідів описаний RFC 2461.

На відміну від ARP, виявлення сусідів ICMP є протоколом IP, що означає, що його безпеку можна забезпечити за допомогою IPsec (набір протоколів, що використовуються для забезпечення сервісів приватності та аутентифікації на мережевому рівні моделі OSI). Як обережність, більшість пакетів для виявлення сусідів спрацьовує тільки в тому випадку, якщо вони не були перенаправлені маршрутизатором. Це досягається шляхом встановлення максимально допустимої кількості стрибків, що ускладнює поширення пакетів у віддалені мережі [12-14].

Як і ARP, при виявленні сусідів адреси канального рівня явно включаються в тіло повідомлення, а не ховаються в заголовку канального рівня. Це полегшує процес реалізації та залишає відкритим питання про виявлення сусідів через проксі у таких випадках, як Mobile IP [14].

Є два типи пакетів для виявлення сусідів ICMPv6: для пошуку сусідів (Neighbor Solicitation) та для оголошення про сусідів (Neighbor Advertisement). Вони мають кілька застосувань; те, про який тут згадується, є еквівалентом ARP IPv4 [13].

Пакети для пошуку сусідів дуже нагадує пакети ARP-запитів. Вони відправляються, коли вузол хоче транслювати індивідуальну кінцеву адресу IPv6 на адресу канального рівня. Загалом він каже: «Чи може господар цієї адреси IPv6 вийти на зв'язок?» Якщо ми не знаємо, яка адреса канального рівня у кінцевого хоста, на групову адресу активного вузла, що відповідає кінцевій адресі, відправляється пакет для пошуку сусідів, причому кінцева адреса

включається до повідомлення ICMP. Вузол, що відправляє пакет, для полегшення відповіді зазвичай включає свою адресу канального рівня. Пакет для оголошення про сусідів є логічною відповіддю на такий пошук. Він відправляється запитуючій системі, несучи з собою вихідну адресу пошуку, адресу канального рівня кінцевої системи та деякі прапори [9].

На відміну від ARP, ICMPv6 уникає використання широкомовлення. Використання всього діапазону групових адрес активних вузлів означає, що вузлам зазвичай доведеться обробляти тільки пакети для пошуку сусідів, які представляють для них інтерес. Це означає, що завантаження перериваннями на хостах IPv6 має бути значно менше, ніж в еквівалентній мережі IPv4.

2.11 Вибір адреси

На даному етапі у типового вузла IPv6 може бути і швидше за все буде багато адрес. Деякі можуть бути налаштовані вручну, інші – автоматично налаштовані через оголошення маршрутизаторів; одні може бути локальними канальними, інші – глобальними; одні можуть бути постійними, інші – тимчасовими. Серед усього цього достатку вузол повинен вибрати, яку саме адресу використати. Залежно від критеріїв, що висуваються, вибір може постійно варіюватися з часом роботи хоста. У деяких випадках адреси можуть бути явно обрані програмою або користувачем, наприклад, коли користувач набирає telnet::1 або коли сервер прив'язаний до однієї IP-адреси. В інших ситуаціях потрібен передбачуваний механізм, який керуватиме вибором адрес хоста, тобто правила вибору адреси за замовчуванням, про які йдеться в RFC 3484 [15].

У будь-якому даному двоточковому з'єднанні, очевидно, потрібно визначити дві адреси - відправника та одержувача. Вибір адреси відправника визначає, яка адреса вузла буде використовуватися для ініціювання з'єднання з даною адресою одержувача. [9].

Процес вибору дається у термінах послідовності правил, які порівнюють дві адреси. Спочатку беремо правило номер 1, і, якщо воно не говорить нам, яку адресу слід вибрати, ми переходимо до правила номер 2 і т.д. 1.3, а адреси одержувача – в табл. 2.4. Правила вибору адреси одержувача залежать від правил вибору адреси відправника, оскільки у них входить розрахунок адреси відправника за умови, що обрано конкретну адресу одержувача. Після визначення адреси одержувача можна вибрати відповідну адресу відправника.

Таблиця 2.3 – Правила вибору адреси відправника

Пріоритет	Опис
1	Вибираємо, якщо відправник збігається із джерелом
2	Вибираємо адресу з відповідною областю дії
3	Намагаємося уникати застарілих адрес
4a	Вибираємо адреси, якщо вони одночасно є домашніми та гостьовими
4b	Вважаємо за краще домашні адреси гостьовим (або навпаки – гостьові домашнім, відповідно до конфігурованої настройки)
5	Вибір інтерфейсної адреси, найближчої до одержувача
6	Вибираємо, якщо позначка політики відправника відповідає одержувачу
7	Віддаємо перевагу відкритим адресам (або навпаки, залежно від конфігурованого налаштування)
8	Використання найдовшого збігається префікса

Таблиця 2.4 – Правила вибору адреси одержувача (залежно від відповідної адреси відправника)

Пріоритет	Опис
1	Уникаємо адрес одержувача, які є недоступними
2	Вибираємо адресу за узгодженістю області дії одержувача та відповідного відправника
3	Уникаємо, якщо відповідний відправник застарів
4a	Вибираємо, якщо відповідний відправник одночасно є домашнім та гостьовим
4b	Віддаємо перевагу домашнім відправникам гостьовим
5	Обираємо за узгодженістю міток політики одержувача та відповідного відправника
6	Обираємо вищий пріоритет політики адреси отримувача
7	Вибираємо місцеве транспортування
8	Обираємо адресу одержувача з меншою областю дії
9	Використання найдовшого збігається префікса
10	Вибираємо найвищий пріоритет, вказаний DNS

Область дії визначає, що адреса належить до локальних канальних /.../ глобальних адрес. Домашня та гостьова адреси відносяться до мобільних функцій IPv6.

З погляду провайдерів послуг Internet найбільш цікавим є правило «найдовшого префіксу, що збігається». Все дуже просто: найдовший збігається префікс пари відправник-одержувач - це число бітів, що збігаються в адрес, якщо рахувати з лівого кінця. Підставою цього є ієрархічна модель маршрутизації, якої дотримується IPv6 [16].

При виборі адреси можна опціонально застосовувати деякі політики, визначені користувачем або адміністратором. Сюди входять адресні «мітки» (пара відправник-одержувач буде кращою при збігу цих міток) та пріоритет (переважним є одержувач з вищим пріоритетом).

На даний момент ще не накопичено достатнього практичного досвіду щодо вибору адрес та використання пов'язаних з ним політик. Закінчена реалізація вибору адрес, що не просто відповідає специфікації, але і має зручну для використання форму, може виявитися досить хитрою, тому тільки час зможе сказати нам, які аспекти вибору адрес будуть мати практичний вплив на конфігурування IPv6 [17].

Наприклад, на рис. 2.4 показаний пакет IPv6 із заголовком IPv6, за яким слідує за головок маршрутизації, після якого йде заголовок та дані TCP.

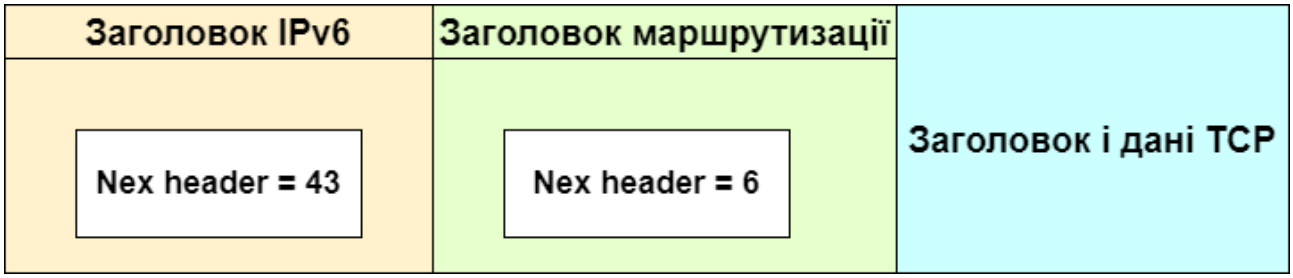

Рисунок 2.4 – Використання поля Next Header

За винятком заголовка пересування жоден із цих заголовків не обробляється вузлами, що просто пересилають пакет. Якщо в пакеті є заголовок пересування, він повинен слідувати відразу за заголовком Pv6. Це означає, що у

звичайній ситуації маршрутизатору не доведеться заглядати за заголовок IPv6 і йому не доведеться залазити в нетрі для аналізу заголовка Hop-by-Hop [15].

Ще однією корисною властивістю заголовків розширення є те, що, незважаючи на змінний розмір, їхня довжина повинна бути кратна восьми і поля в них повинні бути вирівняні відповідним чином для ефективного доступу.

Всі вузли IPv6 повинні розуміти заголовки розширення, що обговорюються RFC 2460, а також заголовки автентифікації і ESP, що мають відношення до IPsec. Якщо вузол зустрічає незрозумілий заголовок, пакет буде скинутий і буде згенеровано повідомлення про помилку параметра ICMPv6. Потрібно помітити, що проміжні маршрутизатори не заглядають за заголовок Hop-by-Hop, тому їм не потрібно розуміти всі заголовки, що пересилаються ними [18].

А що робити в ситуації, коли потрібно надіслати деяку опцію, розуміти яку вузлу, що обробляє її, зовсім не обов'язково. Для таких випадків є заголовки пересування та опцій одержувача, Опції, що включаються в ці заголовки, діляться на 4 класи згідно з тим, що відбувається, коли їх не вдається зрозуміти. Події, що відповідають цим класам, – це «ігнорувати та продовжувати обробку», «скинути пакет», «скинути пакет та надіслати повідомлення про помилку параметра ICMPv6» та «скинути пакет та відправити повідомлення про помилку параметра ICMPv6, за умови, що пакет не є груповим пакетом». Цим досягається достатня еластичність, що дозволяє опціям бути як підказками, які можуть бути проігноровані, так і необхідними критеріями коректної передачі пакета. В останньому випадку, щоб дізнатися, чи підтримується ця опція, можна надіслати її та чекати на відповідь ICMP [18].

Отже, що ж ми можемо робити з цими заголовками розширення та опціями, які можуть бути в них. У табл. 2.5 наведено зведення заголовків розширень.

Таблиця 2.5 – Зведення заголовків розширень IPv6

Тип заголовка	Подтип	RFC
Опції пересування	Заповнення Попередження маршрутизатора Корисне навантаження (Jumbo payload)	 2460 2711 2675
Опції одержувача	Заповнення Оновлення зв'язування Підтвердження зв'язування Запит зв'язування Домашня адреса	 2460 3775 3775 3775 3775
Заголовок маршрутизації	Тип 0	2460
Заголовок фрагмента		2460
Заголовок аутентифікації		2402
Заголовок ESP		2460

Можливо, найбільш привабливою опцією Hop-by-Hop є опція Jumbo Payload, визначена RFC 2675 [18]. Вона реалізує одне з найбільш часто використовуваних покращень IPv6 щодо IPv4, а саме ефективнішу обробку високошвидкісних даних. Зазвичай пакети IP мають обмеження за розміром 64 КВ, а ця опція дозволить у перспективі відсилати пакети розміром до 4 GB. Відправляючи пакети більшого розміру, зменшується частка часу, що йде на відправлення інформації у заголовках. Звичайно, ця опція буде найбільш корисною в тих мережах, де максимальний фізичний розмір пакета перевищує стару межу в 64 КВ [18].

Ще однією важливою опцією Hop-by-Hop є опція попередження маршрутизатора, яка може знайти застосування в групових пакетах і означає, що маршрутизатор повинен обробити пакет, крім його пересилання. Найменш цікавими опціями Hop-by-Hop та одержувача є опції заповнення, які дозволяють заповнити за головок опцій до правильного розміру, щоб опції у ньому були вирівняні коректно. Інші опції одержувача відносяться до мобільності IPv6 [18].

У заголовку маршрутизації IPv6 можуть бути вказані варіанти стандартної процедури маршрутизації. Варіант type 0 реалізує маршрутизацію джерела (source routing), що означає, що пакети повинні пройти через кілька заданих проміжних маршрутизаторів. У світі IPv4 це називалося маршрутизацією через задані вузли (loose source routing).

Заголовок фрагментації, що містить багато полів заголовка IPv4 і багато в чому виконує його функції, дозволяє відправнику розбивати пакети на фрагменти. Таким чином, ми отримуємо можливість відправляти пакети розміром більше MTU, проте пов'язана з цим нелегка праця буде покладена на кінцеві вузли, а не на маршрутизатори [19].

2.13 Маршрутизація

Протоколи маршрутизації, очевидно, мають велике значення у роботі Internet, проте у певному сенсі вони стоять окремо серед проблем функціонування низькорівневого IP. Отже, як IPv6 змінив протоколи маршрутизації? Найбільш явна зміна, яку слід зробити порівняно з адресами IPv4 – дозволити увімкнення префіксів. Фактично це єдино значуще різницю між IPv4- і IPv6-версіями відомих протоколів маршрутизації. Можливо, найцікавіші зміни у маршрутизації, викликані IPv6, відносяться до політики маршрутизації, тобто, вони відносяться не до обробки префіксу, а впливають на адміністративне привласнення та управління префіксами. Маршрути, які можуть бути оголошені в глобальній таблиці маршрутизації Internet в IPv6,

піддаються набагато жорсткому контролю, ніж IPv4. Наприклад, передбачається, що люди не стануть оголошувати індивідуальні префікси /48, тому що вони повинні бути об'єднані в блок більшого розміру, який буде оголошуватися Internet-провайдером. Спочатку розглянемо протоколи внутрішніх шлюзів (Interior Gateway Protocol, IGP). Такі протоколи застосовуються для маршрутизації в межах однієї організації. Протоколами IGP є такі протоколи, як RIP, OSPF та IS-IS [15-18].

2.14 Безпека IPv6

IPv6 вніс значні поліпшення мережної безпеки. Найважливіші його нововведення є скоріше не технічними нововведеннями, а питаннями політики – за стандартом стек IPv6 не можна реалізовувати без певної криптографічної підтримки. Важливо відзначити, що ця криптографічна підтримка знаходиться не на рівні додатків і не є окремим спеціальним механізмом, який по-різному конфігурується для поштових програм, web-браузерів та додатків потокового відео – воно знаходиться на нижньому рівні і також може убезпечити такі речі, як виявлення сусідів. Це досить серйозне досягнення IETF. У світі є багато судових органів, що використовують комп'ютери; у багатьох є жорсткі закони проти шифрування, деякі з них повністю забороняють його використання [18].

Форма, в якій забезпечується безпека, IPsec, вже знайома багатьом, оскільки вона є основою багатьох вже розгорнутих VPN-систем (VPN – virtual private network, віртуальна приватна мережа). IPsec є досить складною архітектурою. В IPv6 це реалізовано за допомогою заголовків розширення, які повідомляють, що частина пакету, що залишилася, зашифрована (заголовок ESP з RFC 2406) або має криптографічний підпис (заголовок AH з RFC 2402). В основному це ті ж технології, що використовуються і в IPv4.

IPsec, однак, має деякі недоліки. Наприклад, якщо трафік в мережі регулярно зашифровується, налагодження та пов'язане з безпекою

прослуховування вмісту пакетів стають неможливими, якщо немає ключа до шифру. Тільки з цієї причини для полегшення налагодження деякі мережні адміністратори наполягають на налаштуванні статичного ключа передачі інформації між комп'ютерами всередині об'єкта. Однак було вжито заходів для того, щоб шифрування заголовків (на відміну від шифрування вмісту) було необов'язковим за будь-яких обставин [19].

2.15 Якість обслуговування

Якість обслуговування, далі зване QoS – складна область. Основний принцип досить простий: ми, як адміністратори, так і користувачі, хочемо мати гарантію того, що заданий додаток матиме певну продуктивність у заданій мережі.

У загальному випадку гарантії продуктивності потрібні для мультимедійних програм, а не для стандартних транзакцій HTTP або SMTP, що проводяться мільйони разів на день (хоча іноді потрібні гарантії того, що певна частина мережі буде виділена для критичних служб). Це викликано тим, що при необхідності доставки даних для повторного складання та виведення на екран у певний час мультимедійні програми найбільш чутливі до втрати та спотворення пакетів. Є кілька теорій щодо того, як це можна зробити [15-17]:

1) Розумна мережа, дурні кінцеві хости;

2) Дурна мережа, розумні кінцеві хости;

3) Використання підвищених розмірів.

Перші дві теорії відрізняються тим, де міститься інтелект, який приймає рішення про QoS, тоді як остання намагається вирішити проблему повністю. Неочевидно, що певна схема дасть краще QoS за будь-яких обставин. Для різних схем потрібні різні засоби. IPv6 не робить пропозицій про те, як функціонувати QoS, а просто надає деякі загальні технічні засоби, які повинні допомогти розробникам QoS. Вони входять поля в заголовку IPv6 і, звичайно ж, заголовки розширення [16-19].

IPv6 надає два способи маніпулювання якістю обслуговування, Перший через поле класу трафіку (traffic class), другий -20-бітова потокова мітка в заголовку IPv6. Потрібно звернути увагу, що ці поля доступні в основному заголовку IPv6, отже вони доступні маршрутизатором безпосередньо, незалежно від наявності або відсутності наступних заголовків розширення.

Поле класу трафіку обговорюється RFC 2460, проте визначення класів відкладено до майбутніх досліджень. Диференційовані служби (Differentiated Services) – один з існуючих механізмів надання QoS – представляють свою інтерпретацію поля класу трафіку в RFC 2474. У мережах, що забезпечують QoS через маршрутизатори DiffServ, перевага деяким пакетам надається на основі інтерпретації поля класу трафіку [16].

Щоб пояснити, що таке потокове позначення, потрібно спочатку визначити, що таке потік. Потік – це деяке виділене підмножина трафіку, що переміщається з кінця мережі в інший. Зазвичай потік визначається термінах повного трафіку від конкретного виконується додатка, хоста чи мережі до інший.

В IPv6 потік розглядається як спосіб взаємодії між додатком на одному хості та іншим додатком, що знаходиться, як правило, в іншій точці мережі. Приналежність пакета певному потоку визначається його відправником, одержувачем та потоковою міткою. Єдине спеціальне значення потокової мітки – нуль – означає, що пакет належить ніякому певному потоку [18].

Механізм потокових міток робить потоки, що легко ідентифікуються, тому програма або операційна система може запросити певну обробку пакетів в межах потоку проміжними маршрутизаторами і кінцевими хостами. Запит про особливу обробку можна зробити за допомогою такого протоколу, як RSVP. Основна ідея RSVP полягає у надсиланні маршрутизаторам, через які проходить потік, повідомлення з описом спеціальної обробки для цього потоку.

Поточні мітки зазвичай вибираються випадково з метою ефективнішого використання хеш-таблиць, хоча передбачається, що маршрутизатори нічого не

винні залежати від цього. Було висунуто кілька пропозицій дозволити маршрутизаторам перезаписувати потокові мітки, щоб дати їм можливість використовувати MPLS-подібну маршрутизацію. Опис використання потокових міток наведено RFC 3697 [16].

Завдяки загальній гнучкості IPv6 є й інші способи забезпечення якості обслуговування, наприклад, за допомогою заголовка маршрутизації або заголовка опцій Hop-by-Hop. Однак всі ці техніки все ще знаходяться на стадії активного дослідження і їх застосування обмежено досить специфічними ситуаціями, Яке QoS не було у мережі, IPv6 повинен мати можливості його підтримувати [18].

На сьогоднішній день у реальному світі найпростіший і найпоширеніший підхід відноситься до використання завищених габаритів. Іншими словами, зробивши пропускну здатність каналу суттєво більше передбачуваного повного обсягу трафіку, так що ніколи не буде випробувано на собі перевантажень та погіршення продуктивності мережі, отриманим QoS має вирішити усі свої проблеми. Можливо це недешево, але, як правило, це працює. На жаль, якщо в організації є хоча б один канал з низькою пропускною здатністю, найімовірніше, рано чи пізно комусь захочеться зробити з ним щось незвичайне [17-19].

3 ВИБІР СТРУКТУРИ І ТОПОЛОГІЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

3.1 План будівлі поверху офісу

На поверсі використовується горизонтальна підсистема, яка проектується на крученій парі 5-ї категорії [17].

Приклад плану поверху, отриманий з допомогою MS Visio, представлений на рис. 3.1. та у Додатку А.

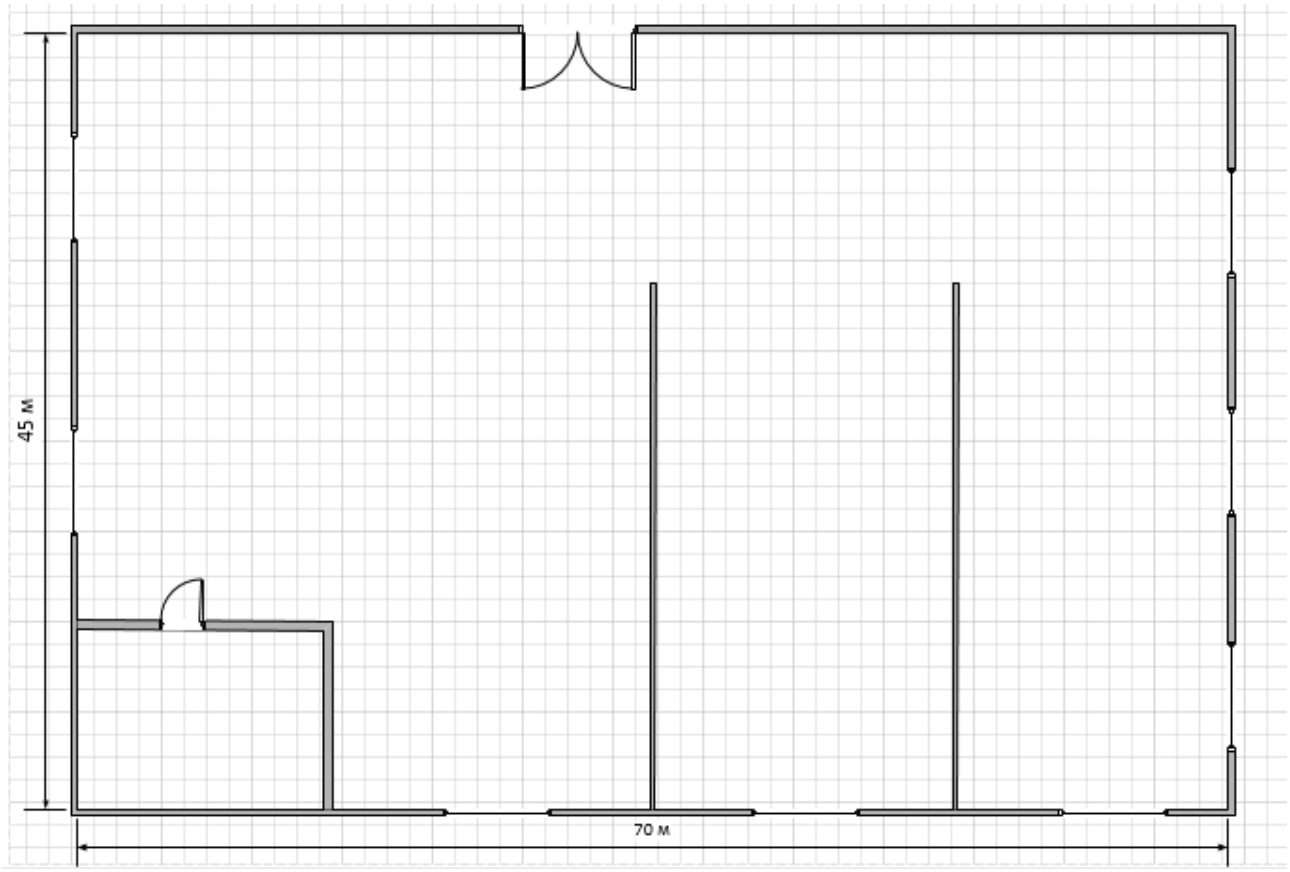

Рисунок 3.1 – План поверху офісу

3.2 Вибір канальної технології

За завданням один офіс в одній із будівель комплексів офісів. У цьому офісі розміщується одна робоча група, тому є не всі підсистеми СКС, а лише горизонтальна.

Незважаючи на це, а також, що для мережі може бути необхідна велика пропускна здатність, для її побудови використовуватимемо технологію Fast Ethernet (IEEE 802.3u) зі швидкістю 100 Мбіт/с, з використанням витої пари категорії 5 [18].

3.3 План розведення кабелю

Основні рекомендації при побудові ЛСС робочої групи та горизонтальних підсистем організації:

- для робочої групи характерне використання топології «зірка» з комутатором у центрі;

- для підключення робочих станцій доцільно використовувати кручені пари категорії 5 та технологію Fast Ethernet (з урахуванням перспективи розвитку);

- найчастіше для побудови СКС однієї робочої групи використовується комутатор («один в один»), але можливе використання одного комутатора на кілька робочих груп і навіть для горизонтальної підсистеми (за наявною відповідною кількістю портів);

- наявність маршрутизатора в горизонтальній системі допускається при логічній організації та фільтруванні трафіку між робочими групами на основі IPv6-адрес підмереж.

План розведення поверху повністю відображає горизонтальну підсистему СКС, що є об'єднанням робочої групи поверху. Для горизонтальної підсистеми було вибрано технологію Fast Ethernet (IEEE 802.3u) на основі крученої пари.

Машини розташовані у місцях для забезпечення зручності користувачів. Робоча група поєднується за допомогою комутатора. Комутатор офісу поєднується з маршрутизатором – одним на СКС. Маршрутизатор буде розташовано в серверному офісі [18].

Приклад розведення кабелю та розташування комутатора та маршрутизатора для горизонтальної підсистеми офісу, виконаний у MS Visio, представлений на рис. 3.2 та у Додатку А.

Кабель слід прокласти малодоступними місцями, щоб зменшити ризик його випадкового пошкодження. Також необхідно мінімізувати кількість кріплень через стіну, у цьому випадку лише чотири, при цьому не зловживаючи кабелем [19].

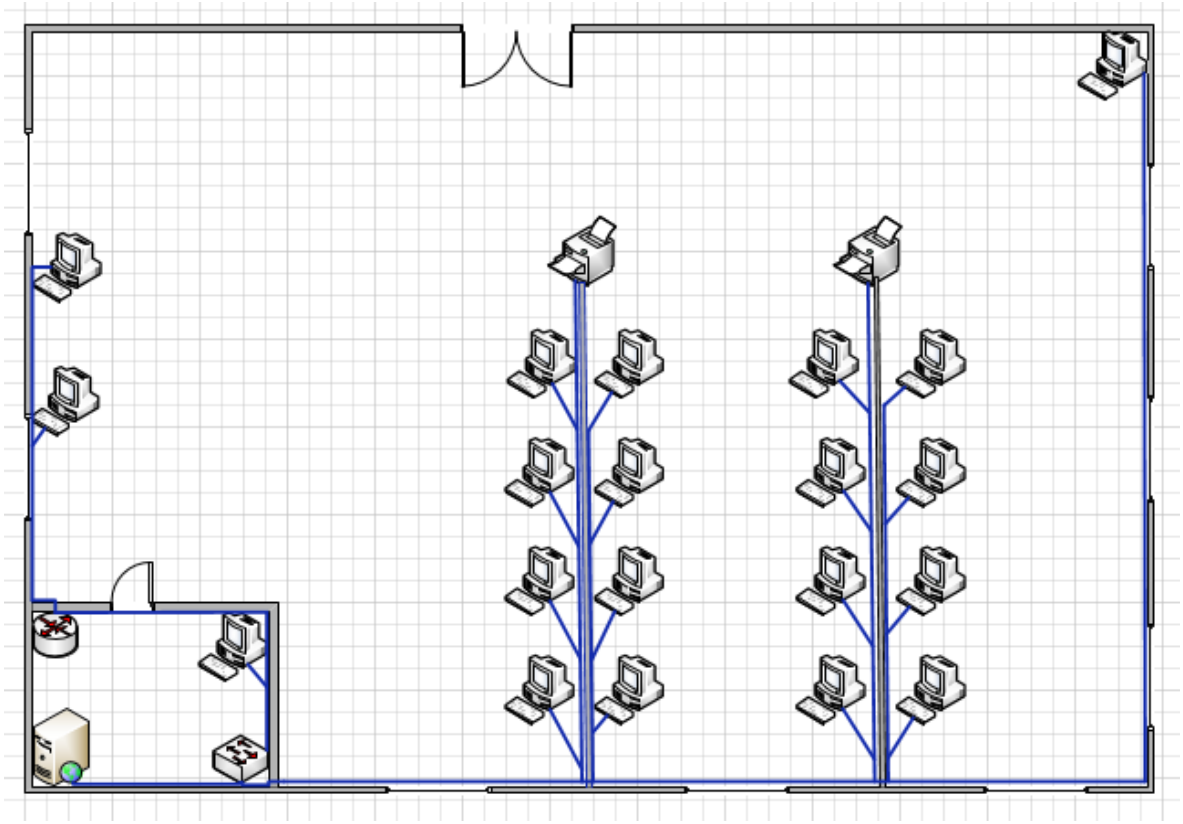

Рисунок 3.2 – Схема розведення крученої пари (синій колір) та розташування мережного обладнання та ПК

3.4 Розрахунок довжини кабелю

За умовами завдання параметри офісу 70м на 45м.

Для цієї СКС використовується один вид кабелю – кручена пара 5 категорії. У середньому довжина кабелю, необхідного групу становить g=1975 м.

Тому довжина кабелю, необхідна для прокладання в підсистемі робочої групи, дорівнює:

$$L_{кп} = g \times 1 \times 1 \times 1 = 1975 \times 1 \times 1 \times 1 = 1975 \text{ м.} \quad (2.1)$$

Але візьмемо 2000 м із урахуванням запасу [16-19].

4 ВИБІР МЕРЕЖНОГО ОБЛАДНАННЯ

4.1 Вибір комутатора та маршрутизатора

Вибір активного мережного обладнання, такого як комутатори та маршрутизатори здійснюється за такими параметрами:

1) Необхідна швидкість передачі;

2) Канальна технологія, яка використовується в робочих, горизонтальних, вертикальних та базових підсистемах;

3) Простота та зручність налаштування;

4) Відношення «ціна/якість».

Для реалізованої СКС необхідно визначитися з моделлю комутатора, який має 24 порти Fast Ethernet (802.3u) зі швидкістю 100 Мбіт/с на основі крученої пари, 2 порти Gigabit Ethernet (802.3u) зі швидкістю 1000 Мбіт/с на основі крученої пари [16].

Виберемо один комутатор Cisco SB SF300-24PP-K9-EU, який представлений на рис. 4.1.

Рисунок 4.1 – Комутатор Cisco SB SF300-24PP-K9-EU

Характеристики комутатора Cisco SB SF300-24PP-K9-EU на табл. 3.1

Таблиця 4.1 – Характеристики комутатора Cisco SB SF300-24PP-K9-EU

Інтерфейс	24 порта Fast Ethernet (10/100 Мбіт/с) 3 порта Gigabit Ethernet (10/100/1000 Мбіт/с 1 порт 100BASE T/SFP
Продуктивність	Комутаційна матриця 12,8 Гбіт/с Скорость передачі 64-байтних пакетів 9,52 Мбіт/с Розмір таблиці MAC-адресов 16К записів Буфер пакетів 8 МБ
Розміри	440 (Д) х 257 (Ш) х 44,45 (В) мм,
Рабочая температура	От 0 до +45 С

Також необхідно вибрати маршрутизатор, оскільки налаштування маршрутизації IPv6 організується саме в ньому. Уніфікований маршрутизатор D-Link DSR-250 (рис. 4.2) є високопродуктивним рішенням, яке забезпечує захист мережі та призначений для задоволення наростаючих проблем малого та середнього бізнесу. Характеристики роутера додані у табл. 4.2 [18].

Рисунок 4.2 – Маршрутизатор D-Link DSR-250

Таблиця 4.2 – Характеристики маршрутизатора D-Link DSR-250

Інтерфейс Ethernet	1 WAN-порт 10/100/10000 Мбіт/с 8 LAN-портов 10/100/1000 Мбіт/с
Порт USB	1 порт USB 2.0
Консольний порт	RJ-45
Продуктивність	Пропускна здатність фаервола: 45 Мбіт/с Пропускна здатність VPN: 35 Мбіт/с
Firewall	Статичний маршрут Динамічний DNS Маршрутизація між VLAN NAT, PAT Фільтрация web-содержания: URL, ключові слова
Сеть	Сервер/Кліент DHCP DHCP Relay IEEE802. 1q VLAN VLAN (на основі порту) Ipv6
Розміри (ДхШхВ)	140x203x35 мм
Рабоча температура	От 0 до +40 С

4.2 Логічна структура сформованої схеми мережі офісу

Схема виконана за допомогою програмного пакета Packet Tracer для моделювання мереж, побудованих на основі обладнання Cisco Sys, показана на рис 4.3 і в Додатку А.

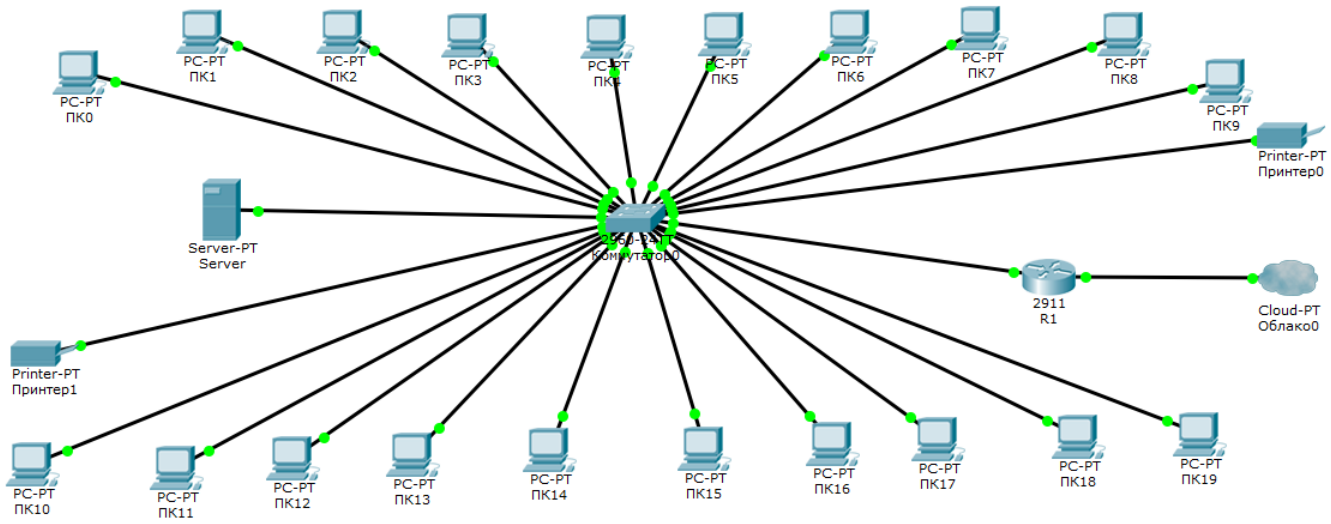

Рисунок 4.3 – Логічна структура мережі головного офісу

5 ЛОГІЧНА ОРГАНІЗАЦІЯ МЕРЕЖІ КОМПАНІЇ

5.1 Організація мережі на основі адрес IPv6

Для того, щоб маршрутизатор міг визначати, куди направляти кожен конкретний пакет інформації, що передається по мережі, в заголовку кожного пакета обов'язково вказується адреса відправника та адреса одержувача пакета. Тому, до кожної точки підключення будь-якого пристрою до мережі надається унікальний номер, який і називається IP-адресою. Комп'ютери та маршрутизатор «знають» свої IP-адреси та адреси своїх «сусідів» у мережі, а роутер ще й може визначити з допомогою таблиць маршрутизації, куди направляти пакети з усіма іншими IP-адресами. Діапазон адрес вибраний таким чином [16-19]:

2015::1/64
2015::2/64
2015::3/64
2015::4/64
2015::5/64
2015::6/64
2015::7/64
2015::8/64
2015::9/64
2015::A/64
2015::B/64
2015::C/64
2015::D/64
2015::E/64
2015::F/64
2015::10/64
2015::11/64
2015::12/64
2015::13/64
2015::14/64
2015::15/64
2015::16/64
2015::17/64
2015::FFFE

5.2 Маршрутизація IPv6

Гнучкий механізм маршрутизації – перевага IP версії 6. Через спосіб, в якому ідентифікатори мережі IPv4 виділені, знаходилися великим таблицям маршрутизації, що повинен бути підтримуваним маршрутизаторами, в базових мережах. Ці маршрутизатори повинні знати всі маршрути для переадресації пакетів, які, ймовірно, прямують до будь-якого вузла. Зі своєю можливістю виконати статистичне обчислення адрес IPv6 надає гнучку адресацію і значно зменшує розмір таблиць маршрутизації.

Команди, які були прописані у глобальному режимі конфігурації маршрутизатора [16-18]:

```
Router>
Router>en
Router#conf
Router(config)#
Router(config)#int Gig 0/0
Router(config-if)#ipv6 unicast-routing
Router(config-if)#ipv6 address 2015::FFFE/64
Router(config-if)#exit
Router(config)#int Gig 0/1
Router(config-if)#ipv6 unicast-routing
Router(config-if)#ipv6 address 2017::FFFE/64
Router(config)#exit
```

ВИСНОВКИ

У процесі пубоди корпоративної мережі було досліджено версію протоколу IP – IPv6, досліджено основні характеристики протоколу, такі як структура пакету IPv6, принципи адресації, архітектура адреси, робота з підмережами, групове розсилання, контрольна сума та стиснення заголовків, маршрутизація тощо. Також були розглянуті протоколи, які працюють безпосередньо під час маршрутизації з IPv6: ICMPv6, RIPng, OSPF, IS-IS, BGP-4. У другій частині кваліфікаційної роботи було розроблено структурну схему офісу. Незважаючи на задану предметну область, було вирішено використовувати таку технологію як Fast Ethernet зі швидкістю 100Мбіт/с. На основі типового плану структури офісу була розроблена горизонтальна підсистема СКС, ймовірне розташування обладнання користувача та розрахована середня кількість необхідного фізичного середовища. Проведено вибір мережного обладнання. Виходячи з необхідних характеристик, були обрані модель одного маршрутизатора – D-Link DSR 250, модель одного комутатора – Cisco SB SF300-24PP-K9-EU.

Розроблено логічну структуру сформованої схеми СКС мережі офісу за допомогою програмного пакету Packet Tracer. Перед цим було проведено структуризацію, розбиття простору IPv6: 2015::1 – 2015::17. При моделюванні мережі кожної робочої станції було призначено задану IP-адресу шостої версії з вибраного діапазону. Як шлюз була обрана адреса 2015::FFFE. Також велике значення має створене настроювання конфігурації маршрутизатора.

У результаті ми отримали повністю функціонувану мережу. Яка побудована на основі теоретичних рекомендацій та рішень, прийнятих виключно виконавцем роботи. Модель мережі є повністю актуальною і готовою до реалізації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Deering S., Hinden R. Internet Protocol. Version 6 (IPv6), 1998 – 438 p.

2. Hinden R., Deering S. IP Version 6 Addressing Architecture, 1998 – 361 p.

3. Hinden R., O'Dell M., Deering S. An IPv6 Aggregatable Global Unicast Address Format, 1998 – 393 p.

4. Narten T., Nordmark E., Simpson W. Neighbor Discovery for IP Version 6, 1998 – 140 p.

5. Джон Мой (John Moy) «OSPF: Anatomy of an Internet Routing Protocol» and «OSPF: Complete Implementation» - Издательство «Addison-Wesley» , 2002 – 284 p.

6. Ричард Н., Мэлоун Д. IPv6 Администрирование сетей. – 2006 – 321с.

7. Олифер В. Г. Олифер Н. А. Компьютерные сети: Принципы, технологии, протоколы. – СПб.: Питер, 2005. – 864 с .

8. Смирнов И. Г. Структурированные кабельные системы / проектирование, монтаж и сертификация – М: Экон-Информ, 2005 – 178 с.

9. Степанов А.Н. Архитектура вычислительных систем и компьютерных сетей – СПб: Питер, 2007. – 512 с.

10. Структура СКС. Топологія СКС [Електронний ресурс] – Режим доступу:http://life-prog.ru/1_27482_struktura-sks-topologiya-sks.html/

11. Оптоволокно [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Оптическое_волокно.

12. Новиков Ю.В. Локальные сети. Архитектура, алгоритмы, проектирование – М.: ЭКОМ, 2000 – 308.

13. Комутатор T2600G-18TS [Електронний ресурс] – Режим доступу: https://www.tp-link.com/ru-ua/products/details/cat-39_T2600G-18TS.html#overview

14. Маршрутизатор Archer-C7 [Електронний ресурс] – Режим доступу: https://www.tp-link.com/ru-ua/products/details/cat-9_Archer-C7.html

15. Маркування кабелю [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Маркировка_кабеля

16. Таненбаум Э. Компьютерные сети./Э. Таненбаум– СПб.: Питер, 2002. – 848 с.

17. Хелеби С. Принципы маршрутизации в Internet. – М: «Вильямс», 2001. – 448 с.

18. Леинванд А. Конфигурирование маршрутизаторов Cisco – Cisco Router Configuration. – 2-е изд. – М.: «Вильямс», 2001. – 368 с.

19. Спортак М. Компьютерные сети и сетевые технологии. – М.: ДиаСофт, 2005. – 711с.