Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)
Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Реорганізація схеми керування та оптимізація локальної мережі передачі даних
(тема)

Виконав:

студент *2* курсу, групи *ІМІм-21-1*

Ільченко Я.Е.
(прізвище, ініціали)

Спеціальність *172 «Телекомунікації та радіотехніка»*
(код і повна назва спеціальності)

Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)

Освітня програма

«Інформаційно-мережна інженерія»
(повна назва освітньої програми)

Керівник *доц. Харченко Н.А.*
(посада, прізвище, ініціали)

Допускається до захисту

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

2022 р.

Не містить відомостей заборонених до відкритого публікування.

Студент / Ільченко Я.Е /

Керівник / Харченко Н.А. /

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 «Телекомунікації та радіотехніка»*
(код і повна назва)

Тип програми *освітньо-професійна*

Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«____»_____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Ільченко Яніні Едуардівні*
(прізвище, ім'я, по батькові)

1. Тема роботи *Реорганізація схеми керування та оптимізація локальної мережі передачі даних*
затверджена наказом університету від 21 жовтня 2022 р. № 1376 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 14 грудня 2022 р.

3. Вихідні дані до роботи *Провести модернізацію будинкової локальної на основі наявного устаткування з мінімізацією матеріальних витрат. Локальна мережа є мережею другого рівня, побудована за технологією Gigabit Ethernet з використанням топології зірка. На магістральних оптичних лініях використовуються керовані комутатори другого рівня та програмований комутатор третього рівня у центрі топології. Мережа не поділена на логічні сегменти, тобто маршрутизація трафіку у мережі не здійснюється. Провести аналіз необхідних етапів реорганізації для підвищення контролю трафіку, збільшення пропускної здатності для впровадження послуги IP-телефонії та IPTV, а також створити запас продуктивності для підключення нових користувачів*

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Огляд та аналіз сучаснихіснуючих технологій локальних обчислювальних мереж
2. Особливості керування трафіком у локальних комп'ютерних мережах
3. Аналіз етапів реорганізації будинкової локальної мережі
4. Програмне забезпечення та налаштування комутаційного обладнання
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *назва, мета і актуальність кваліфікаційної роботи; базові технології локальних мереж; Ethernet, Fast Ethernet, Gigabit Ethernet, Wi-Fi, WiMAX; технологія віртуальних мереж VLAN; агент ретрансляції DHCP; управління багатоадресною розсилкою на 2 рівні; етапи реорганізації існуючої локальної мережі; схема модернізованої будинкової локальної мережі; результати реорганізації, висновки*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*21.10.22*	*виконано*
2	*Підбір літератури за темою роботи.*	*22.10-01.11.22*	*виконано*
3	*Огляд та аналіз сучаснихіснуючих технологій локальних обчислювальних мереж*	*02.11-20.11.22*	*виконано*
4	*Особливості керування трафіком у локальних комп'ютерних мережах*	*21.11-30.11.22*	*виконано*
5	*Аналіз етапів реорганізації будинкової локальної мережі*	*01.12-05.12.22*	*виконано*
6	*Програмне забезпечення та налаштування комутаційного обладнання*	*06.12-10.12.22*	*виконано*
7	*Оформлення презентаційного матеріалу, підготовка до захисту в ЕК*	*11.12-14.12.22*	*виконано*

Дата видачі завдання _21_ ___жовтня__ 2022 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Харченко Н.А.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка 77с., 26 рис., 2 табл., 12 джерел, 1 додаток.

Об'єкт дослідження – локальна обчислювальна мережа.

Мета роботи - реорганізація локальної мережі.

Головною вимогою до будинкових локальних мереж є виконання мережею її основної функції - забезпечення користувачам можливості доступу в Інтернет і внутрішнім ресурсам всіх комп'ютерів, що знаходяться в даній мережі. Інші вимоги, такі як продуктивність, надійність, сумісність, керованість та масштабованість, пов'язані з якістю виконання цього основного завдання надання послуг користувачу.

У роботі розглянуті базові технології побудови локальних комп’ютерних мереж. Проаналізовано існуючу мережу, визначено її основні недоліки та запропоновано шляхи їх вирішення. Для покращення показників адміністрування мережі запропоновано керування трафіком здійснювати за допомогою створення VLAN та DHCP-серверу.

ЛОКАЛЬНА КОМП'ЮТЕРНА МЕРЕЖА, VLAN, TRIPLE-PLAY, ETHERNET, DHCP.

THE ABSTRACT

Explanatory slip 77 p., 26 fig., 2 tab., 12 sources, 1 attach.

Object of research - local computer network.

The purpose of the work - reorganization of the local network.

The main requirement for home local networks is that the network fulfills its main function - providing users with access to the Internet and internal resources of all computers located in this network. Other requirements, such as performance, reliability, compatibility, manageability, and scalability, are related to the quality of performance of this primary task of providing services to the user.

Basic technologies for building local computer networks are considered in the work. The existing network was analyzed, its main shortcomings were identified, and ways to solve them were proposed. To improve the performance of network administration, it is proposed to manage traffic by creating a VLAN and a DHCP server.

LOCAL COMPUTER NETWORK, VLAN, TRIPLE-PLAY, ETHERNET, DHCP.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ 9
ВСТУП 11
1. ОГЛЯД ТА АНАЛІЗ СУЧАСНИХ ІСНУЮЧИХ ТЕХНОЛОГІЙ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ 12
1.1 Ethernet 12
1.2 Fast Ethernet 100 Мбіт/с 13
1.3 Gigabit Ethernet 1000 Мбіт/с 16
1.4 Wi-Fi (стандарт IEEE 802.11) 18
1.5 WiMAX 25
2 ОСОБЛИВОСТІ КЕРУВАННЯ ТРАФІКОМ У ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ 28
2.1 Концепція віртуальних локальних мереж 28
2.2 Огляд технології віртуальних локальних мереж 33
2.2.1 VLAN на основі угруповання портів 34
2.2.2 Віртуальні локальні мережі на основі угруповання MAC-адрес 35
2.2.3 Використання міток у додатковому полі кадру – стандарти 802.1Q/p та фірмові рішення 36
2.2.4 Використання специфікації LANE 39
2.2.5 Використання мережного протоколу 40
2.3 Агент ретрансляції DHCP 41
2.4 Протоколи маршрутизації 44
2.5 Багатоадресне розсилання 45
3 АНАЛІЗ ЕТАПІВ РЕОРГАНІЗАЦІЇ БУДИНКОВОЇ ЛОКАЛЬНОЇ МЕРЕЖІ 49
3.1 Вимоги до будинкових локальних мереж при їх модернізації 49
3.2 Аналіз будинкової локальної обчислювальної мережі 50
3.3 Концепція розвитку будинкової локальної обчислювальної мережі 52
3.4 Апаратне забезпечення модернізованої будинкової локальної обчислювальної мережі 53

4 ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА НАЛАШТУВАННЯ КОМУТАЦІЙНОГО ОБЛАДНАННЯ 61
ВИСНОВКИ 67
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 68
ДОДАТОК А СЛАЙДИ ПРЕЗЕНТАЦІЇ 69

ПЕРЕЛІК СКОРОЧЕНЬ

ACL – перелік прав доступу;

AUI – інтерфейс пристрою доступу до середовища передачі;

BRAS (broadband remote access server) – маршрутизатор широкосмугового віддаленого доступу, служить маршрутизації трафіку до/від користувачів. BRAS знаходиться в ядрі мережі провайдера і агрегує підключення користувача з мережі рівня доступу;

CoS – загальна підтримка необхідної якості передачі;

CPU – центральний процесор;

CSMA/CD – метод множинного доступу з виявленням несучої та виявленням колізій;

DHCP – протокол динамічного конфігурування хостів;

DHCP (Dynamic Host Configuration Protocol) – протокол динамічної конфігурації вузла;

DHCP-discover – запит до DHCP-сервера від кінцевого мережного обладнання з метою виявити себе в мережі та отримати необхідні параметри мережі для роботи;

DHCP-offer – відповідь від DHCP-сервера;

DHCP-snooping – функція комутатора, призначена захисту від атак з допомогою протоколу DHCP;

DHCP-ретранслятор – вузол у мережі, який перенаправляє DHCP -запит на вказаний у його налаштуваннях централізований DHCP-сервер;

DoS/DDos - розподілена відмова в обслуговуванні;

GVRP – протокол забезпечує сервіс реєстрації VLAN;

ICMP – протокол керуючих повідомлень Інтернет;

IGMP – протокол управління групами Інтернет;

IP – Інтернет протокол;

iSCSI – протокол здійснює контроль передачі блоків даних;

LAN – локальна мережа доступу;

LLC – управління логічним зв'язком;

MAC – канальний рівень;

MAU – багатостанційний пристрій доступу;

MII – інтерфейс незалежний від середовища (Fast Ethernet);

MSAU – багатостанційний пристрій доступу;

NIC – інтерфейсна картка;

NLP – імпульсні посилки контролю лінії;

PHY – пристрій фізичного рівня (Fast Ethernet);

PPP – протокол точка-крапка;

QoS – рівень підтримки необхідної якості передачі;

RAM – оперативна пам'ять;

SATA – послідовний інтерфейс жорсткого диска;

SCSI – високошвидкісний інтерфейс жорсткого диска;

SM – одномодове волокно;

SNMP – протокол управління мережевими ресурсами;

SSL – протокол конфіденційної передачі в протоколі TCP/IP;

STP – екранована кручена пара;

TCP – протокол контролю передачі;

TTL – час життя пакета;

UDP – протокол передачі дейтаграм;

UPS – джерело безперебійного живлення;

USB – універсальний послідовний інтерфейс;

UTP – неекранована кручена пара;

VLAN – віртуальна LAN. Домен широкомовний.

VoIP – IP телефонія;

VPN – приватна віртуальна мережа;

WAN – глобальна мережа;

WI-Fi – специфікація обладнання для бездротового доступу до локальних мереж загального користування;

xDSL – цифрова абонентська лінія;

КПК – кишеньковий персональний комп'ютер;

ЛОМ – локальна обчислювальна мережа;

ТКД – комутатор DES-3526 рівня доступу мережі (Точка комунікативного доступу).

У-1 – комутатор DXS-3326 GSR рівня розподілу деревоподібної топології мережі, що знаходяться на першому рівні (Вузол першого рівня);

У-2 - комутатор DXS-3326 GSR рівня розподілу деревоподібної топології мережі, що знаходяться на другому рівні (Вузол другого рівня);

ВСТУП

Світова спільнота все більш схильна до використання комп'ютерних мереж у різних сферах життєдіяльності. Це зумовлено такими причинами, як зниження часу на передачу інформації від одного абонента до іншого, можливість спілкування та роботи з людьми, віддаленими на значні відстані, і все це не виходячи з дому чи офісу. Наразі комп'ютерні мережі є невід'ємною частиною офісної інфраструктури будь-якої фірми чи організації. Вони дозволяють не лише прискорити процеси обміну інформацією, а й відкрити можливість спільного використання різних ресурсів, а також організувати спільні обчислення, підвищивши сумарну обчислювальну потужність за рахунок об'єднання кількох комп'ютерів.

Сучасне суспільство є інформаційним, а можливість об'єднання комп'ютерів у мережі дозволила збільшити швидкість передачі повідомлень та отримати безліч різних сервісів, використовуючи єдиний ПК. Ці можливості стали доступні не тільки вдома, а й на робочі місця, тому в будь-якій організації зараз існує власна обчислювальна мережа, яка є не даниною моді, а важливим елементом в інфраструктурі підприємства.

А технології не стоять на місці. Ще якихось п'ять років тому при згадці про комп'ютерну мережу відразу ж представлялися бухти проводів, що йдуть від шафи до офісних комп'ютерів. Зараз все більшу популярність набувають бездротові мережі, що надають користувачеві мобільність, а, відповідно, більший комфорт, багато в чому за рахунок «позбавлення» від проводів.

Таким чином, можна говорити про актуальність теми даної кваліфікаційної роботи, так як в ній розглядаються питання реорганізації локальної мережі з метою покращення параметрів передачі та керування трафіком, а також надання нових послуг triple play.

1 ОГЛЯД ТА АНАЛІЗ СУЧАСНИХ ІСНУЮЧИХ ТЕХНОЛОГІЙ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

На сьогоднішній день існує безліч мережних технологій передачі даних. Сфери застосування цих технологій дуже різні. Починаючи з малих локальних обчислювальних мереж і закінчуючи загальноміськими та світовими глобальними мережами.

Існують такі основні сучасні технології локальних мереж:

1. Ethernet; Fast Ethernet, Gigabit Ethernet;
2. Wi-Fi (Wireless Fidetly);
3. WiMAX (Worldwide Interoperability for Microwave Access).

1.1 Ethernet

Ветераном мережних технологій (архітектур) є Ethernet - ця специфікація була запропонована фірмами DEC, Intel і Xerox в 1980 році і трохи пізніше на її основі з'явився стандарт IEEE 802.3. За першими буквами назв них фірм утворено скорочення DIX, що фігурує в описах цієї технології. Слово Ether (ефір) у назві технології означає різноманіття можливих середовищ передачі. Перші версії - Ethernet v 1.0 та Ethernet v 2.0 призначалися тільки для коаксіального кабелю, стандарт IEEE 802.3 розглядає й інші варіанти середовища передачі - кручена пара і оптоволокно. Зараз під назвою Ethernet мають на увазі стандарт IEEE 802.3 (швидкість 10 Мбіт/с). У 1995 році був прийнятий стандарт IEEE 802.3u - Fast Ethernet зі швидкістю 100 Мбіт/с, а 1997 року IEEE 802.3z - Gigabit Ethernet (1000 Мбіт/с). Восени 1999 року прийнято стандарт IEEE 802.3a/b - Gigabit Ethernet на кручений парі категорії 5, пізніше була анонсована 10 GBit Ethernet (10000 Мбіт/с). Популярні різновиди Ethernet позначаються як 100BaseTX та ін. Тут перший елемент позначає швидкість передачі, Мбіт/с. Другий елемент: Base - пряма (немодульована) передача, Broad - використання широкосмугового кабелю з частотним ущільненням каналів. Третій елемент: середовище передачі (T, TX, T2, T4 - кручені пари, FX, FL, FB, SX і IX - оптоволокно, CX - твінаксіальний кабель для Gigabit Ethernet) [1].

Технологія Ethernet заснована на методі множинного доступу до середовища передачі з прослуховуванням несучої та виявленням колізій - CSMA/CD. Можлива схема локальної мережі показана на рис. 1.1.

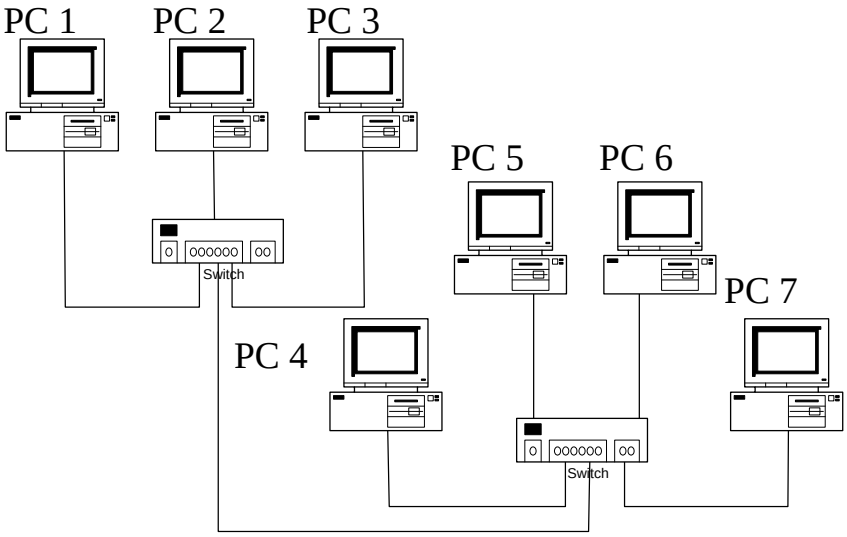

Рисунок 1.1 – Приклад побудови мережі Ethernet

1.2 Fast Ethernet 100 Мбіт/с

Варіанти Fast Ethernet зі швидкістю передачі 100 Мбіт/с описуються стандартом IEEE 802.3u – додатковими розділами 802.3, прийнятими 1995 року. Вони ґрунтуються на тому ж методі доступу CSMA/CD зі збереженням форматів кадрів. При цьому всі співвідношення, виміряні в бітових інтервалах, зберігаються. Оскільки тривалість бітового інтервалу скоротилася в 10 разів, максимально допустимий час проходження між двома вузлами скоротився до 2,6 мкс, що призвело до посилення топологічних обмежень. Всі різновиди використовують зіркоподібну топологію з активним пристроєм у центрі, можливе і безпосереднє з'єднання пари станцій [2].

Стандарт 802.3u спирається на ті ж рівні MAC та LLC, які були визначені у вихідному 802.3; зміни стосуються тільки фізичного рівня. Фізичний рівень Fast Ethernet є тришаровим:

- Reconciliation sublayer - рівень узгодження з MAC-рівнем 802.3, орієнтованим на UI-інтерфейс;

- MII (Media Independent Interface) - електричний інтерфейс, незалежний від середовища передачі. Є специфікацією сигналів TTL-рівня, використовує 40-контактний штирковий роз'єм. За ідеєю він нагадує інтерфейс AUI, але розташовується на іншому рівні. Довжина кабелю MII має перевищувати 0,5 м. Наявність доступного інтерфейсу MII перестав бути обов'язковим;

- PHY (Physical layer device) - пристрій фізичного рівня, прив'язаний до конкретного середовища передачі (100BaseTX, 100BaseFX або 100 BaseT4). Пристрій фізичного рівня виконує логічне кодування – перетворення 4B/5B або 6B/8T, фізичне кодування та приєднання до середовища передачі, та необов'язково – автоматичне узгодження режимів передачі. Фізичний рівень у 100BaseTX і 100BaseFX запозичений з технології FDDI, у 100 BaseT 4 застосована оригінальна розробка [2].

100BaseTX - найбільш популярна версія Fast Ethernet, що використовує дві кручені пари категорії 5. По використанню роз'ємів повністю відповідає 10 Base-T. Можлива робота у напівдуплексному та повнодуплексному режимах. Логічне кодування проводиться за схемою 4B/5B - 4 біти вихідної інформації перетворюються на 5-бітний символ. Надмірність використовується для підвищення достовірності та службових цілей. Метод фізичного кодування MLT-3 запозичений з TP-PMD - "мідної" реалізації FDDI. У паузі між кадрами в лінію надсилається послідовність символів Idle [2].

100 Base-T4 - версія, що використовує 4 кручені пари категорії не нижче 3. Крім однонаправлених пар, що використовуються в 100Base-TX, тут дві додаткові пари є двонаправленими і служать для розпаралелювання передачі даних. Кадр передається за трьома лініями паралельно, що дозволяє знизити пропускну здатність кожної пари до 33,3 Мбіт/с. Кожні 8 біт (двійкових розрядів - Binary), що передаються по конкретній парі, кодуються шістьма трійковими (Ternary) цифрами (кодування 8B/6T). В результаті при бітовій швидкості 33,3 Мбіт/с швидкість зміни сигналів лінії становить 25 Мбод (33,3x6/8=25). Ці заходи дозволяють звузити необхідну смугу пропускання кабелю вимог категорії 3 (16 МГц). Четверта пара при передачі використовується для прослуховування сигналу від протилежного передавача – за його появою визначається факт колізії. Для підключення кінцевих вузлів до портів активного обладнання використовується "прямий" кабель, для безпосереднього з'єднання кінцевих вузлів або з'єднання двох комунікаційних пристроїв "перехресний" кабель [2].

Для наведених вище реалізацій передбачено протокол узгодження режимів (autonegotiation), за допомогою якого порт може вибрати найефективніший з режимів, доступних обом учасникам обміну. Узгодження здійснюється шляхом обміну посилками FLP (Fast Link Pulse), які є ознакою справної активної лінії (аналогічно NLP 10 Base-T). На відміну від одиночних імпульсів NLP імпульси FLP йдуть групою. Розрізняють синхронізуючі та сигнальні імпульси FLP. Сигнальні імпульси можуть вставлятися між синхронізуючими, що йдуть групою по 17 штук. Місця між цими імпульсами відводяться під кодування 16-бітного слова: наявність сигнального відповідає одиничному біту, відсутність - нульовому. Слово містить інформацію про доступні режими. Перший вузол пропонує найефективніший режим, кодуючи його у посилці FLP. Приймач на цю посилку відповідає аналогічною, в якій кодує свої можливості. Як робітник вибирається найпріоритетніший з доступних обох вузлів. Пріоритети режимів у порядку зменшення: 100Base-TX повнодуплексний, 100 Base-T4, 100Base-TX напівдуплексний, 10 Base-T повнодуплексний, 10 Base-T напівдуплексний. Якщо другий вузол має порт 10 Base-T, що «не розуміє» FLP і посилає NLP, буде прийнятий протокол 10 Base-T. Протокол автоматичного узгодження може бути вимкнений (або не реалізований), у цьому випадку режим роботи визначається примусово при конфігуруванні порту. Можливість перемикання режимів відображається в назвах портів (Fast Ethernet 10/100) [1].

100Base-FX - версія для оптоволокна із довжиною хвилі 1300 нм. Логічно близька до 100Base-TX - те ж логічне кодування 4B/5B, але фізичне - NRZI (як у FDDI). У напівдуплексі дальність 412 м – через обмеження за часом подвійного обороту. У дуплексі дальність визначається властивістю волокна: по MM-волокну може досягати 2 км, по SM - 32 км.

100 Base-SX - стандарт на дешевих короткохвильових (830 нм) світлодіодних передавачах та багатомодовому волокні. Дальність зв'язку обмежена волокном і менше, ніж у FX - всього 300 м, зате підтримується сумісність з 10 Base-FL і автоматичне узгодження швидкості передачі 10/100 Мбіт/с (802.3u). Версія розроблена як дешева альтернатива дорогою 100 Base FX у випадках, коли не потрібно подолання великих відстаней [2].

Центральним мережним пристроєм у Fast Ethernet може бути повторювач або комутатор. Повторювачі за своїми можливостями поділяються на два класи:

- повторювач класу I є транслюючим, він підтримує різні схеми кодування, прийняті в технологіях 100 BaseTX / FX та 100 BaseT-4;

- повторювач класу II є прозорим (transparent repeater), він підтримує тільки одну зі схем кодування - технологію 100 Base-TX/FX або 100 Base-T4.

Завдяки надмірності кодування в порівнянні з Ethernet повторювачі Fast Ethernet працюють дещо складніше. У разі виявлення помилкового сигналу замість його прозорої трансляції до інших портів повторювач може посилати ознаку пошкодження кадру. Якщо повторювач підтримує дві схеми кодування, йому доводиться робити декодування за схемою 4B/5B і наступне кодування 6B/8T (або навпаки), що вносить додаткову затримку.

Топологічні обмеження Fast Ethernet жорсткіший — діаметр домену колізій для крученої пари не повинен перевищувати 205 м, в одному домені колізій може бути не більше двох повторювачів класу II, повторювач класу I може бути лише один. Якщо прийняти допустиму відстань від повторювача до станції рівним 100 м, то повторювачі можна з'єднувати між собою кабелем завдовжки трохи більше 5 м [3].

Можлива схема локальної мережі з оптичною лінією показана на рис. 1.2.

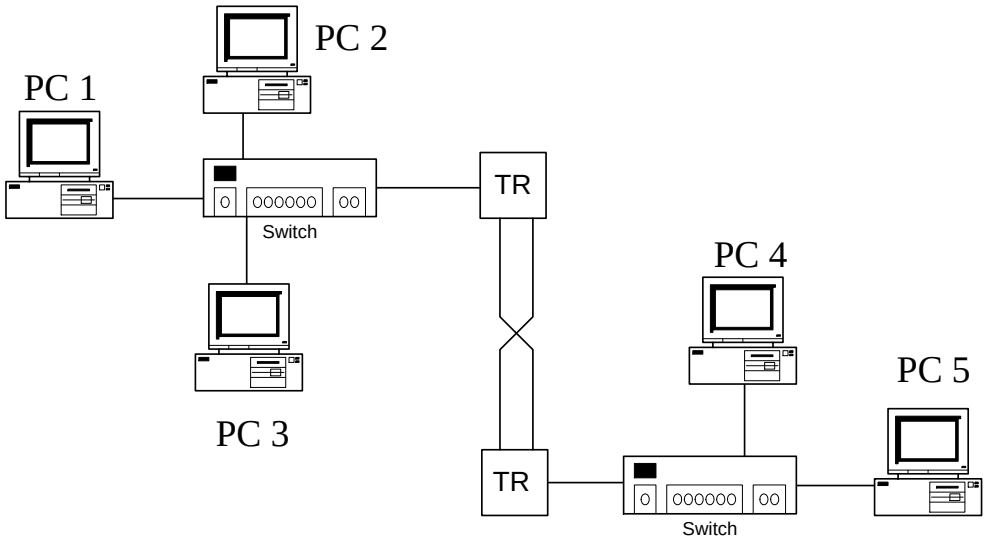

Рисунок 1.2 – Приклад мережі Ethernet з оптичною лінією

1.3 Gigabit Ethernet 1000 Мбіт/с

Технологія Gigabit Ethernet зі швидкістю передачі 1000 Мбіт/с розроблена для прискорення передачі при використанні найпопулярнішої технології

(Ethernet). Однак підвищення швидкості на порядок при збереженні всіх пропорцій попередніх технологій призвело до звуження діаметра домену колізій до неприйнятного розміру — 0,26 мкс затримки відповідає приблизно 50 м кабелю, а ще затримку вносить і повторювач. Тому мінімально допустимий розмір кадру, що визначає максимально допустиму затримку передачі, був збільшений до 512 байт (4096 bit). З урахуванням затримок у повторювачах та адаптерах діаметр домену колізій може досягати 200 м, тобто вписуватися в стандартну концепцію побудови СКС. Обмеження, породжені методом CSMA/CD, є актуальними лише для напівдуплексного режиму роботи портів. Для Gigabit Ethernet більш характерний повнодуплексний режим, при якому допустима довжина лінії зв'язку обмежується загасанням сигналу та частотними властивостями лінії [3].

Додатково передбачається можливість групової пакетної передачі кадрів (frame bursting). Вузол, що одержав доступ до середовища, після передачі одного кадру замість паузи посилає спеціальну послідовність, після якої передає наступний кадр. Кадри з такої групи можуть бути адресовані різним одержувачам. Сенс пакетної передачі полягає у скороченні накладних витрат на отримання доступу до середовища - між кадрами пакета середовище для інших вузлів виглядає зайнятим.

Gigabit Ethernet описується двома стандартами - IEEE 802.3z (1000 Base-SX, 1000 Base-LX і 1000 Base-CX), прийнятим у 1998 році, та IEEE 802.3ab (1000 Base-T), прийнятим восени 1999 року [1].

Стандарт 802.3z ґрунтується на напрацюваннях технології Fiber Channel. Тут використовується надмірне кодування 8B/10B, а схеми фізичного рівня "розігнані" зі швидкості 800 Мбіт/с до 1 Гбіт/с (тактова частота - 1,25 ГГц). Стандарт пропонує наступні версії:

- 1000 Base-SX (Short wavelength) - оптичний інтерфейс з короткохвильовими (850 нм) лазерними передавачами для зв'язку по MM-волокну на невеликі відстані. Для кабелю з невисокою смугою пропускання допустима довжина з'єднання виявляється меншою, ніж обмеження на довжину магістрального кабелю 500 м, встановлене стандартами СКС;

- 1000 Base-LX (Long wavelength) - інтерфейс з довгохвильовими (1310 м) лазерними передавачами для зв'язку по SM та MM-волокну на великі відстані;

- 1000 Base-LH - інтерфейс з лазерними передавачами 1310 нм для зв'язку по SM і MM-волокну на надвеликі відстані, поки стандарт IEEE не входить;

- 1000 Base-CX - електричний інтерфейс для зв'язку на короткі дистанції (25 м), призначений для зв'язку обладнання в межах апаратної кімнати або телекомунікаційного приміщення. Використовує двоосьовий (twinaxial) кабель або скручені четвірки проводів (quad cable) з частотними характеристиками, що перевищують STP типів 1 і 2. Як конектори поки що пропонується DB-9 (використовується для STP в Token Ring), розробляється новий тип конектора HSSDC (High - Speed Serial Data Connector);

- 1000 Base-T - електричний інтерфейс на крученій парі (4 пари проводів) категорії 5e (і навіть 5) при обмеженні на довжину лінії в 100 м. Фізичне кодування - 5-рівневе. Сигнал передається одночасно з чотирьох пар проводів, причому для повного дуплексу передача ведеться по кожній парі відразу в обох напрямках. Кінцеві ланцюги виділяють із суміші сигнал протилежного передавача. Вирішення цієї задачі на надвисоких частотах стало можливим завдяки застосуванню сучасних сигнальних процесорів. Для задоволення вимог до середовища передачі рекомендується застосування в кабельній системі компонентів категорії 5e (розетки, шнури, 4-парні кабелі стаціонарної проводки). Кількість з'єднань у каналі має бути мінімальною. У телекомунікаційних приміщеннях рекомендується схема безпосереднього підключення (interconnection), без крос-панелі. У горизонтальній кабельній системі виключається з'єднання двох шматків кабелів однієї лінії в точці переходу або консолідації [2].

1.4 Wi-Fi (стандарт IEEE 802.11)

На сьогоднішній день існують наступні різновиди даного стандарту побудови бездротових локальних мереж IEEE 802.11 a/b/g/n.

Стандарт IEEE 802.11, був прийнятий у 1997 р., став першим стандартом цього сімейства. Він передбачає використання діапазону частот 2,4 ГГц - 5 ГГц, а також технології розширення спектру стрибкоподібною зміною частоти (Frequency Hopping Spread Spectrum або технології розширення спектру за методом прямої послідовності - Direct Sequence Spread Spectrum DSSS). Стандарт IEEE 802.11 забезпечує пропускну здатність до 2 Мбіт/с. Можлива схема локальної мережі показана на рис. 1.6. Розглянемо детальніше різновиди сімейства 802.11.

Стандарт IEEE 802.11a

Стандарт IEEE 802.11a передбачає використання частотного діапазону 5 ГГц, що не вимагає ліцензування, і модуляції за методом ортогонального мультиплексування з розділенням частот (Orthogonal Frequency Domain Multiplexing, OFDM). Застосування цього стандарту дозволяє збільшити швидкість передачі у кожному каналі з 11 Мбіт/с до 54 Мбіт/с. При цьому одночасно може бути організовано до восьми каналів, що не перетинаються (або точок присутності), а не три, як у діапазоні 2,4 ГГц. Продукти стандарту IEEE 802.11a (мережні адаптери NIC та точки доступу) не мають зворотної сумісності з продуктами стандартів 802.11 та 802.11b, оскільки вони працюють на різних частотах [4].

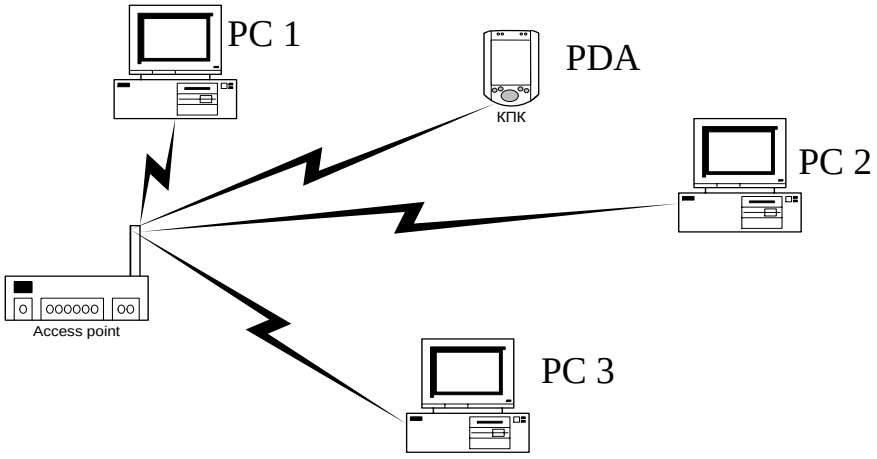

Рисунок 1.6 – Приклад мережі Wi-Fi

Стандарт IEEE 802.11b

Стандарт IEEE 802.11b було прийнято 1999 р. у розвиток прийнятого раніше стандарту IEEE 802.11. Він також передбачає використання діапазону частот 2,4 ГГц, але з модуляцією DSSS. Цей стандарт забезпечує пропускну здатність до 11 Мбіт/с для однієї точки доступу. Продукти стандарту IEEE 802.11b, що постачаються різними виробниками, тестуються на сумісність та сертифікуються організацією Wireless Ethernet Compatibility Alliance (WECA), яка нині більше відома під назвою Wi-Fi Alliance. Сумісні бездротові продукти, що пройшли випробування за програмою Альянсу WH, можуть бути марковані знаком Wi-Fi [4].

Стандарт IEEE 802.11g

Проект стандарту IEEE 802.11g був затверджений у жовтні 2002 р. Цей стандарт передбачає використання діапазону частот 2,4 ГГц, забезпечуючи швидкість передачі 54 Мбіт/с і перевищуючи, таким чином, чинний стандарт 802.11b. Крім того, він гарантує зворотну сумісність зі стандартом 802.11b. Зворотна сумісність стандарту IEEE 802.11g може бути реалізована в режимі модуляції DSSS, тоді швидкість передачі буде обмежена одинадцятьма мегабітами в секунду або в режимі модуляції OFDM, при якому швидкість становить 54 Мбіт/с. Таким чином, цей стандарт є найбільш прийнятним при побудові бездротових мереж [5].

Стандарт IEEE 802.11n

Стандарт Wi-Fi 4 (802.11n) для мереж Wi-Fi було затверджено організацією IEEE (Інститут інженерів з електротехніки та радіоелектроніки) 11 вересня 2009 року.

В основі стандарту 802.11n покладено наступні покращення:

- збільшення швидкості передачі;
- збільшення зони покриття;
- збільшення надійності передачі сигналу;
- збільшення пропускної спроможності.

Концепція 802.11n

Пристрої 802.11n можуть працювати в одному з двох діапазонів 2,4 ГГц або 5,0 ГГц.

На фізичному рівні (PHY) реалізовано вдосконалену обробку сигналу та модуляції, додано можливість одночасної передачі сигналу через чотири антени.

На канальному рівні управління доступом до середовища (MAC) реалізовано більш ефективне використання доступної пропускної здатності. Водночас ці вдосконалення дозволяють збільшити максимальну теоретичну швидкість передачі даних до 600 Мбіт/с – збільшення більш ніж у десять разів порівняно з 54 Мбіт/с стандарту 802.11a/g (нині ці пристрої вже вважаються застарілими) [6].

Насправді, продуктивність бездротової локальної мережі залежить від багатьох факторів, таких як середовище передачі даних, частота радіохвиль, розміщення пристроїв та їх конфігурація. При використанні пристроїв

стандарту 802.11n дуже важливо зрозуміти, які саме вдосконалення були реалізовані в цьому стандарті, на що вони впливають, а також як вони поєднуються і співіснують з мережами застарілих стандартів 802.11a/b/g бездротових мереж.

Багатоканальний вхід/вихід (MIMO)

Одним із основних моментів стандарту 802.11n є підтримка технології MIMO (Multiple-Input Multiple-Output, багатоканальний вхід/вихід).

За допомогою технології MIMO реалізована здатність одночасного прийому/передачі кількох потоків даних через кілька антен замість однієї (рис. 1.7).

Стандарт 802.11n визначає різні антенні конфігурації "MxN", починаючи з "1x1" до "4x4" (найпоширеніші на сьогоднішній день це конфігурації "3x3" або "2x3"). Перше число (M) визначає кількість передаючих антен (T), а друге число (N) визначає кількість приймальних антен (R). Наприклад, точка доступу з двома передаючими та трьома приймальними антенами є "2x3" (або 2T3R) MIMO-пристроєм.

Рисунок 1.7 – Приклад реалізації технології MIMO 2x2

Чим більше пристрій 802.11n використовує антен для одночасної роботи передачі/прийому, тим вище максимальна швидкість передачі даних. Однак, саме по собі використання кількох антен не збільшує швидкість передачі даних або розширення діапазону. Основним у пристроях стандарту 802.11n є те, що в них реалізовано вдосконалений метод обробки сигналу, який визначає алгоритм роботи MIMO-пристрою при використанні декількох антен.

Конфігурація "4x4" при використанні модуляції 64-QAM забезпечує швидкість до 600 Мбіт/с, конфігурація "3x3" при використанні модуляції 64-QAM забезпечує швидкість до 450 Мбіт/с, тоді як конфігурації "2x3" та "1x2" забезпечать швидкість до 300 Мбіт/с [6].

При використанні MIMO "2x2" та підтримці модуляції 256-QAM (TurboQAM) у діапазоні 2,4 ГГц максимальна швидкість підключення на стандарті 802.11n може становити 400 Мбіт/с.

При використанні MIMO "4x4" та підтримці модуляції 256-QAM (TurboQAM) у діапазоні 2,4 ГГц максимальна швидкість підключення на стандарті 802.11n вже становитиме 800 Мбіт/с (підтримується в Keenetic Ultra).

Ширина смуги пропускання каналу 40 МГц

Іншою додатковою особливістю стандарту 802.11n є збільшення ширини каналу з 20 МГц до 40 МГц.

У бездротових мережах використовуються два частотні діапазони 2,4 ГГц і 5 ГГц. Бездротові мережі стандарту 802.11b/g працюють на частоті 2,4 ГГц, мережі стандарту 802.11a працюють на частоті 5 ГГц, а мережі стандарту 802.11n можуть працювати як на частоті 2,4 ГГц, і на частоті 5 ГГц.

У смузі частот 2,4 ГГц для бездротових мереж доступно 13 каналів (у деяких країнах 11) з інтервалами 5 МГц між ними. Для передачі сигналу бездротові пристрої стандарту 802.11b/g використовують канали завширшки 20 МГц (рис. 1.8).

Бездротовий пристрій стандарту 802.11b/g використовує один із 13 каналів зі смуги 20 МГц в межах частоти 2,4 ГГц, але фактично задіює 5 каналів, що перетинаються. Наприклад, якщо точка доступу використовує канал 6, вона надає значні перешкоди на канали 5 і 7, і навіть перешкоди канали 4 і 8. Коли відбувається передача даних пристроєм, бездротовий сигнал відхиляється від центральної частоти каналу +/- 11 МГц. У деяких випадках відбувається відхилення енергії радіочастоти до 30 МГц центрального каналу. Для виключення взаємних перешкод між каналами необхідно, щоб їх смуги відстояли один від одного на 25 МГц. Таким чином, залишається всього 3 канали, що не перетинаються, на смузі 20 МГц: 1, 6 і 11. З шириною каналу 40 МГц непересічними є канали 3 і 11.

Бездротові точки доступу, що працюють у смузі ч астот 2,4 ГГц, в межах однієї зони обслуговування, що покривається, повинні уникати перекриття каналів для забезпечення якості бездротової мережі.

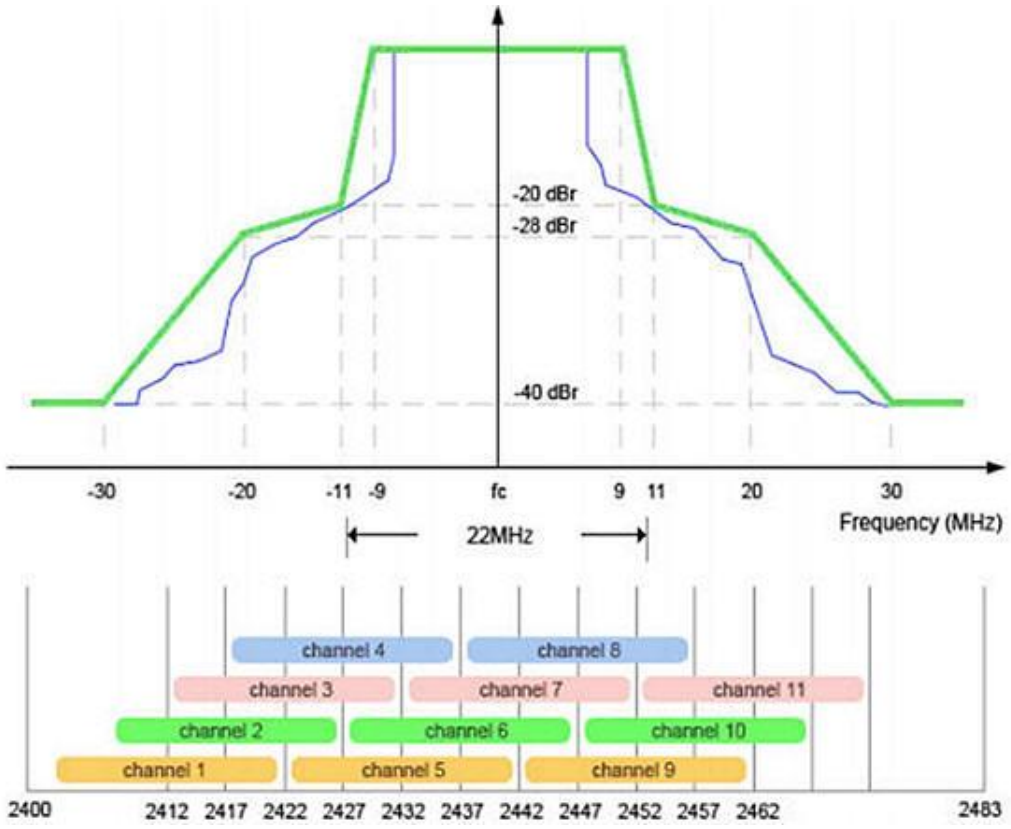

Рисунок 1.8 – Розподіл каналів у смузі частот 2,4 ГГц

Одним із основних моментів є питання сумісності бездротових пристроїв стандарту 802.11n з пристроями 802.11a/b/g.

Більшість бездротових локальних мереж 802.11n використовують канали 40 МГц лише у діапазоні частот 5 ГГц. У мережах, що використовують смугу частот 5 ГГц (802.11n), проблеми каналів, що перетинаються, не існує.

Пристрої стандарту 802.11n можуть використовувати ширину каналу 20 чи 40 МГц у будь-якому частотному діапазоні (2,4 чи 5 ГГц). При використанні ширини каналу 40 МГц (пристрою 802.11n) відбувається подвійне збільшення пропускної спроможності порівняно з шириною каналу 20 МГц (пристрої 802.11b/g).

У смузі частот 5 ГГц доступно 19 каналів, що не перетинаються, які більш придатні для застосування в пристроях стандарту 802.11n, що забезпечують максимально можливу швидкість передачі даних. Сигнали розподіляються без взаємного перекриття каналів із шириною смуги 40 МГц.

Однак, при використанні смуги 40 МГц пристроями 802.11n їх роботі можуть заважати існуючі 802.11b/g точки доступу, що призведе до зниження продуктивності всього сегмента мережі.

Режими роботи 802.11n

Існують три режими роботи 802.11n: HT, Non-HT та HT Mixed. Розглянемо докладніше кожен із режимів.

Режим з високою пропускною здатністю HT (High Throughput)

Точки доступу 802.11n використовують режим High Throughput (HT), відомий також як "чистий" режим (Greenfield-режим), який передбачає відсутність поблизу (у зоні покриття) працюючих пристроїв 802.11b/g, що використовують ту саму смугу частот. Якщо ж такі пристрої існують у зоні покриття, вони не зможуть спілкуватися з точкою доступу 802.11n. Таким чином, у цьому режимі дозволені до використання лише клієнти 802.11n, що дозволить скористатися перевагами підвищеної швидкості та збільшеною дальністю передачі даних, які забезпечують стандарт 802.11n [6].

Режим з невисокою пропускною здатністю Non-HT

Точка доступу 802.11n з використанням режиму Non-HT (відомий також як успадкований режим), відправляє всі кадри у форматі 802.11b/g, щоб застарілі станції змогли їх зрозуміти. У цьому режимі точка доступу повинна використовувати ширину каналів 20 МГц і не використовуватиме переваги стандарту 802.11n. Для забезпечення зворотної сумісності всі пристрої повинні підтримувати цей режим. Потрібно враховувати, що точка доступу 802.11n з використанням режиму Non-HT не забезпечуватиме високу продуктивність. При використанні цього режиму передача даних здійснюється зі швидкістю, що підтримується найповільнішим пристроєм.

Змішаний режим з високою пропускною здатністю HT Mixed

Змішаний режим HT Mixed буде найпоширенішим режимом для точок доступу 802.11n у найближчі кілька років. У цьому режимі удосконалення стандарту 802.11n можуть бути використані одночасно з існуючими станціями 802.11b/g. Режим HT Mixed забезпечить зворотну сумісність пристроїв, але пристрої 802.11n отримають зменшення пропускної здатності. У цьому режимі точка доступу 802.11n розпізнає наявність старих клієнтів і використовуватиме нижчу швидкість передачі даних, поки старий пристрій здійснює прийом-передачу даних.

Таким чином, при практичному застосуванні покращень стандарту 802.11n, переваги можуть бути досягнуті повною мірою лише за умови, що клієнти 802.11b/g відсутні і бездротова мережа працює в чистому режимі HT.

1.5 WiMAX

WiMAX - Worldwide Interoperability for Microwave Access, стандартизована інститутом IEEE технологія широкосмугового бездротового зв'язку, що доповнює лінії DSL і кабельні технології як альтернативне вирішення проблеми "останньої милі" на великих відстанях. Технологію WiMAX можна використовувати для реалізації широкосмугових з'єднань "останньої милі", розгортання точок бездротового доступу, організації високошвидкісного зв'язку між філіями компаній та вирішення інших подібних завдань [7].

Попередня версія технології WiMAX забезпечувала функціональність за допомогою обладнання, яке не піддане стандартизованому тестуванню на предмет сумісності з технологією WiMAX . Ціла низка провайдерів послуг досі використовують такі попередні апаратні рішення для реалізації пілотних проектів WiMAX у багатьох куточках світу. Як тільки тестування сумісності цих систем з технологією WiMAX буде виконано, їх швидше за все можна буде модернізувати програмним чином відповідно до вимог остаточного стандарту WiMAX.

В ідеалі бездротова технологія WiMAX, що заснована на галузевих стандартах, розроблена для організації недорогого швидкісного зв'язку для житла, підприємств та мобільних бездротових мереж у містах та сільській місцевості. Зверніть увагу на визначення, що в ньому заздалегідь "передбачено місце" для взаємодії магістрального WiMAX з "локальним" Wi-Fi.

Устаткування мереж WiMAX функціонує у кількох частотних каналах шириною 10 МГц не більше діапазону 2 ГГц - 11 ГГц. Зрозуміло, специфічне розподілення частотних діапазонів різних країн диктує необхідність можливості роботи WiMAX в різних ділянках. Такий широкий діапазон діапазонів обраний для обліку специфіки більшості країн світу. Так, у Північній Америці для WiMAX використовуються ділянки в діапазонах 2,5 та 5 ГГц, у Центральній та Південній Америці – 2,5, 3,5 та 5 ГГц, на Близькому Сході, в Африці, Західній та Східній Європі – 3,5 та 5 ГГц, в Азіатсько-

Тихоокеанському регіоні – 2,3, 3,5 та 5 ГГц. За своєю суттю WiMAX представляє технологію, що дозволяє забезпечити доступ в інтернет зі швидкістю мереж класу T1, з продуктивністю та покриттям, набагато більшим, ніж у сучасних мереж Wi-Fi. У свою чергу, продовженням "магістральних гілок" WiMAX якраз і стають локальні мережі Wi-Fi, різні типи бізнес та побутових кабельних DSL мереж кінцевих користувачів.

Забезпечуючи комунікації в радіусі 10 кілометрів і більше, точки WiMAX створюють покриття на значних площах, надаючи провайдерам послуг досить гнучкі умови для забезпечення "зв'язку останньої милі". Можлива схема локальної мережі показано на рис. 1.9.

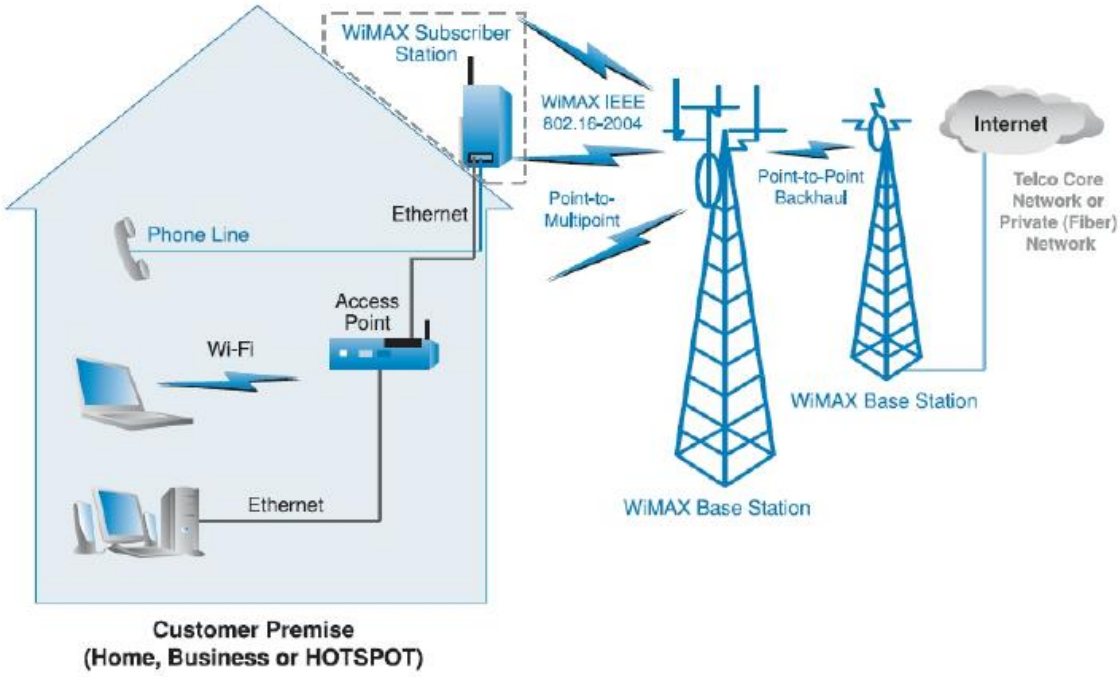

Рисунок 1.9 - Приклад мережі WiMAX

Загалом базові характеристики стандарту 802.16 передбачають дальність дії до 50 кілометрів, покриття з можливістю роботи поза прямою зоною видимості, у перспективі – пікову швидкість обміну даними до 70 Мбіт/с на сектор однієї базової станції при тому, що типова базова станція матиме до 6 секторів покриття [7].

Впровадження WiMAX нині поділено на три основні фази. Нинішня перша фаза впровадження передбачає впровадження і широке поширення технології WiMAX стандарту IEEE 802.16-2004, що замінив собою ранні версії

IEEE 802.16 a і 802.16d, при якому використовуються зовнішні антени за типом "стільникової тарілочки", фактично на цілі тарілочки.

Переваги та недоліки кабельної СКС та Wi-Fi наведені у таблиці 1.1.

Таблиця 1.1 - Переваги та недоліки СКС та Wi-Fi

	Переваги	**Недоліки**
СКС	Висока надійність та швидкість передачі даних.	Тривалі терміни проектування та монтажу. Відсутність мобільності як користувачів, так і самої мережі. Складність розширення нові території.
Wi-Fi	Швидкість розгортання. Бездротова мережа може бути запущена в роботу лише за кілька годин. Мобільність. Користувачі бездротової мережі можуть вільно переміщатися. Також мобільна та сама мережа, її легко перенести в інше місце.	Швидкість передачі даних нижча, ніж у дротовій мережі. Необхідність отримання дозволу використання смуги частот.

2 ОСОБЛИВОСТІ КЕРУВАННЯ ТРАФІКОМ У ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

2.1 Концепція віртуальних локальних мереж

Передумови впровадження технології віртуальної локальної мережі у локальних мережах

Спочатку комутатори не забезпечували можливості створення віртуальних локальних мереж, оскільки вони використовувалися для простого пересилання кадрів між пристроями. Ринок комутаторів почав швидко зростати, коли концентратори колективного доступу до середовища передачі даних (hubs) почали не справлятися зі зростаючими запитами на розширення смуги пропускання мережі у зв'язку з використанням програм клієнт-сервер, що забезпечують графічний інтерфейс користувача (GUI).

Ключова різниця між комутатором та концентратором полягає в тому, як вони працюють з кадрами. Концентратор отримує кадр, потім копіює та передає (повторює) кадр у всі інші порти. У цьому випадку сигнал повторюється, переважно продовжуючи довжину мережного сегмента до всіх підключених станцій. Комутатор повторює кадр у всі порти, крім того, з якого цей кадр був отриманий: *unicast* кадри (адресовані на конкретну MAC адресу), *broadcast* кадри, (адресовані для всіх MAC адрес у локальному сегменті), і *multicast* кадри (адресовані для набору пристроїв сегменті). Це робить їх неприйнятними для великої кількості користувачів, тому що кожна робоча станція і сервер, підключений до комутатора, повинен перевіряти кожен кадр для того, щоб визначити, чи цей кадр адресований йому чи ні. У великих мережах, з великою кількістю кадрів, що обробляються мережевою картою, втрачається цінний процесорний час. Це прийнятно для невеликих робочих груп, де передача даних має короткочасну "вибухову" природу.

Комутатор працює з кадрами "інтелектуально" - він зчитує MAC адресу вхідного кадру та зберігає цю інформацію у таблиці комутації. Ця таблиця містить адреси MAC і номери портів, пов'язаних з ними. Комутатор будує таблицю в розділеній пам'яті і тому він знає, яка адреса пов'язана з яким портом. Комутатори Cisco Catalyst створюють цю таблицю, перевіряючи кожен кадр, що потрапив у пам'ять, і додають нові адреси, які не були занесені раніше.

Маршрутизатори Cisco створили цю таблицю, адресуючи її за вмістом (content-addressable memory). Ця таблиця оновлюється та будується щоразу при включенні комутатора, але ми можемо налаштовувати таймер оновлення таблиці залежно від наших потреб [8]. На рис. 2.1 показано таблицю CAM комутатора Catalyst 5000.

У цьому прикладі стовпець VLAN посилається на номер VLAN, якому належить порт призначення. Стовпець Destination MAC посилається на MAC адресу, виявлену в порту. Слід зазначити, що один порт може бути пов'язаний з кількома MAC адресами, тому необхідно перевіряти кількість MAC адрес, які можуть підтримувати наш комутатор. Destination Ports описує порт, з якого комутатор дізнався MAC адресу.

Cat5500> show cam dynamic

VLAN	Destination MAC	Destination Ports or VCs
1	00-60-2f-9d-a9-00	3/1
1	00-b0-2f-9d-b1-00	3/5
1	00-60-2f-86-ad-00	5/12
1	00-c0-0c-0a-bd-4b	4/10

Cat5500>

Рисунок 2.1 - Таблиця комутації

Далі комутатор перевіряє MAC адресу призначення кадру і негайно дивиться в таблицю комутації. Якщо комутатор знайшов відповідну адресу, він копіює кадр у цей порт. Якщо він не може знайти адресу, він копіює кадр у всі порти. Unicast кадри надсилаються необхідні порти, тоді як multicast і broadcast кадри передаються у всі порти.

Комутація була оголошена як "нова" технологія, яка збільшує пропускну здатність та збільшує продуктивність, але насправді комутатори це високопродуктивні мости (bridges) з додатковими функціями. Комутація це термін, який використовується в основному для опису мережевих пристроїв 2 рівня, які переправляють кадри, ґрунтуючись на MAC адресі одержувача.

Два основних методи, що найчастіше використовуються виробниками для передачі трафіку це *cut-through* і *store and forward.*

Комутація cut-through зазвичай забезпечує менший час затримки, ніж store-and-forward тому, що в цьому режимі комутатор починає передачу кадру в порт призначення ще до того, як повністю отриманий весь кадр. Комутатору достатньо того, що він вважав MAC адреси відправника та одержувача, які спочатку Token Ring і Ethernet кадрів. Більшість cut-through комутаторів починає пересилання кадру, отримавши лише перші 30 - 40 байт заголовка кадру [8].

Store and forward копіює весь кадр перед тим, як надсилати кадр. Цей метод дає більшу затримку, але має більше переваг. Можливості фільтрації, управління та контроль над потоком інформації є головними перевагами цього методу. На додаток, неповні та пошкоджені кадри не надсилаються, оскільки вони не є правильними кадрами. Комутатори повинні мати буферну пам'ять для читання та збереження кадрів під час ухвалення рішення, що збільшує вартість комутатора [8].

У міру поліпшення технологій та захоплення ринку новою технологією почали виникати VLAN. Найпростіший шлях зрозуміти Віртуальні мережі – порівняти їх із фізичною мережею. Фізична мережа може складатися з кінцевих станцій, пов'язаних маршрутизатором (або маршрутизаторами), які використовують одне фізичне з'єднання. VLAN це логічне комбінування кінцевих станцій в одному сегменті на рівні 2 і рівні 3, які пов'язані безпосередньо без маршрутизатора. Зазвичай користувачам, фізично розділеним, потрібен маршрутизатор для зв'язку з іншим сегментом. Комутатори з можливістю побудови VLAN спочатку були запроваджені в основних навчальних містечках та невеликих робочих групах. Спочатку комутація розроблялася в міру потреби, але зараз це є звичайною практикою впроваджувати комутатори та VLAN у мережах

Функції технології віртуальної локальної мережі

Крім свого основного призначення - підвищення пропускної спроможності зв'язків у мережі - комутатор дозволяє локалізувати потоки інформації в мережі, а також контролювати ці потоки і керувати ними, використовуючи фільтри користувача. Однак фільтр користувача може заборонити передачі кадрів тільки за конкретними адресами, а широкомовний трафік він передає всім сегментам мережі. Так вимагає алгоритм роботи моста, який реалізований у комутаторі, тому мережі, створені на основі мостів та

комутаторів, іноді називають плоскими - через відсутність бар'єрів на шляху широкомовного трафіку [4].

Технологія віртуальних мереж *(Virtual LAN, VLAN)* дозволяє подолати зазначене обмеження. Віртуальною мережею називається група вузлів мережі, трафік якої, зокрема і широкомовний, на канальному рівні повністю ізольований з інших вузлів мережі. Це означає, що передача кадрів між різними віртуальними сегментами на підставі адреси канального рівня неможлива, незалежно від типу адреси - унікальної, групової або широкомовної. У той самий час усередині віртуальної мережі кадри передаються за технологією комутації, тобто тільки той порт, який пов'язані з адресою призначення кадру [5].

При використанні технології віртуальних мереж у комутаторах одночасно вирішуються два завдання:

- підвищення продуктивності кожної з віртуальних мереж, оскільки комутатор передає кадри у мережі лише вузлу призначення;

- ізоляція мереж один від одного для управління правами доступу користувачів та створення захисних бар'єрів на шляху широкомовних штормів.

Віртуальні мережі (VLAN) пропонують такі переваги:

- контроль за широкомовним трафіком;

- функціональні робочі групи;

- підвищена безпека.

Контроль над широкомовним трафіком: на відміну від традиційних LAN, побудованих за допомогою маршрутизаторів/мостів, VLAN може бути розглянутий як широкомовний домен із логічно налаштованими кордонами. VLAN пропонує більше свободи, ніж традиційні мережі. Раніше використовувані розробки грунтувалися на фізичному обмеження мереж, побудованих з урахуванням концентраторів; в основному фізичні межі LAN сегмента обмежувалися ефективною дальністю, яку електричний сигнал міг пройти від порту концентратора. Розширення LAN сегментів за ці межі вимагало використання повторювачів (repeaters), пристроїв, які посилювали та пересилали сигнал. VLAN дозволяє мати широкомовний домен незалежно від фізичного розміщення, середовища мережного доступу, типу носія та швидкості передачі. Члени можуть розташовуватись там, де необхідно, а не там, де є спеціальне з'єднання з конкретним сегментом. VLAN збільшують продуктивність мережі, поміщаючи широкомовний трафік усередині маленьких

та легко керованих логічних доменів. У традиційних мережах із комутаторами, які не підтримують VLAN, весь широкомовний трафік потрапляє у всі порти. Якщо використовується VLAN, весь широкомовний трафік обмежується окремим широкомовним доменом [6].

Функціональні робочі групи: Найбільш істотною перевагою технології VLAN є можливість створення робочих груп, ґрунтуючись на функціональності, а не на фізичному розташуванні чи типі носія. Традиційно адміністратори групували користувачів функціонального підрозділу фізичним переміщенням користувачів, їхніх робочих місць та серверів у загальний робочий простір, наприклад, в один сегмент. Всі користувачі робочої групи мали однакове фізичне з'єднання для того, щоб мати перевагу високошвидкісного з'єднання з сервером. VLAN дозволяє адміністратору створювати, групувати та перегруповувати мережеві сегменти логічно та негайно, без зміни фізичної інфраструктури та від'єднання користувачів та серверів. Можливість легкого додавання, переміщення та зміни користувачів мережі – ключова перевага VLAN [6].

Підвищена безпека: VLAN також пропонує додаткові переваги безпеки. Користувачі однієї робочої групи не можуть отримати доступ до даних іншої групи, тому що кожна VLAN є закритою, логічно оголошеною групою. Представимо компанію, де Фінансовий департамент, який працює з конфіденційною інформацією, розташований на трьох поверхах будівлі. Інженерний департамент та відділ Маркетингу також розташовані на трьох поверхах. Використовуючи VLAN, члени Інженерного відділу та відділу маркетингу можуть бути розташовані на всіх трьох поверхах як члени двох інших VLAN, а Фінансовий департамент може бути членом третьої VLAN, яка розташована на всіх трьох поверхах. Зараз мережевий трафік, який створюється Фінансовим департаментом, буде доступний лише співробітникам цього департаменту, а групи Інженерного та відділу Маркетингу не зможуть отримати доступ до конфіденційних даних Фінансового департаменту. Очевидно, є інші вимоги для забезпечення повної безпеки, але VLAN може бути частиною загальної стратегії безпеки мережі. Нижче показаний рис. 2.2, який говорить про те, як функціонування VLAN може розширити традиційні межі.

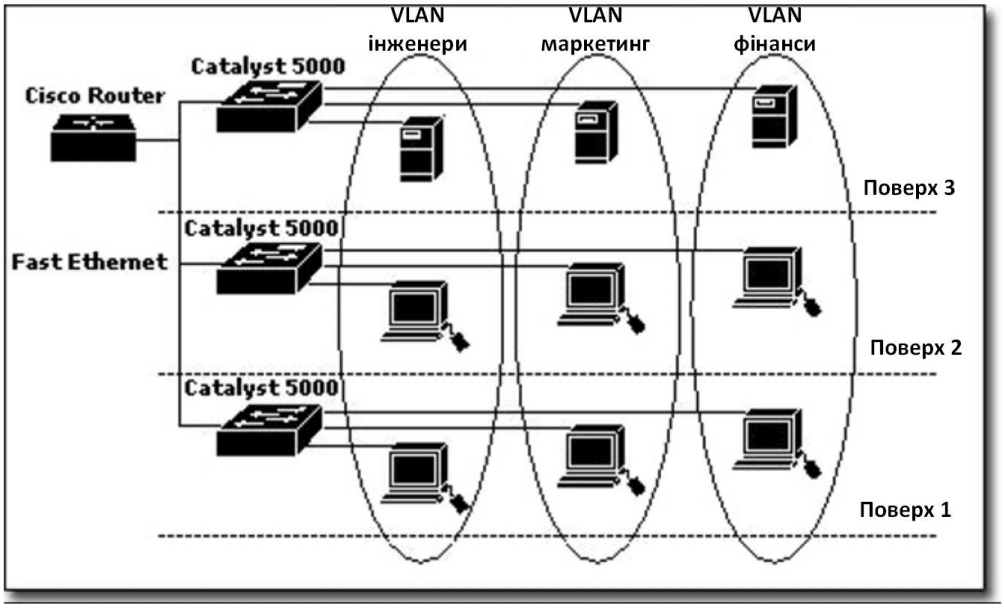

Рисунок 2.2 – Приклад функціонування VLAN

2.2 Огляд технології віртуальних локальних мереж

Типи віртуальних мереж

Технологія та робота віртуальних мереж за допомогою комутаторів довгий час була не стандартизована, хоч і була реалізована у дуже широкому спектрі моделей комутаторів різних виробників. Таке становище змінилося тільки тоді коли інститут IEEE остаточно прийняв специфікації 802.1q/p, які описують стандартний спосіб побудови віртуальних мереж [7].

Через довгу відсутність стандартів кожен виробник розробив свою технологію побудови віртуальних мереж, яка, як правило, була несумісна з технологією інших виробників. Тому віртуальні мережі простіше створювати поки що на обладнанні одного виробника. Винятком є лише віртуальні мережі, побудовані на основі специфікації LANE (LAN Emulation), призначеної для забезпечення взаємодії ATM-комутаторів з традиційним обладнанням локальних мереж. Існує кілька способів побудови віртуальних мереж:

- групування портів;
- групування MAC-адрес;
- використання міток у додатковому полі кадру – приватні протоколи та специфікації IEEE 802.1Q/p;
- специфікація LANE для комутаторів ATM;
- використання мережного рівня.

2.2.1 VLAN на основі угруповання портів

При створенні віртуальних мереж на основі одного комутатора зазвичай використовується механізм групування у віртуальні мережі портів комутатора (рис. 2.3). Це логічно, оскільки віртуальні мережі, побудовані на основі одного комутатора, не можуть бути більшими, ніж порти. Якщо до одного порту підключений сегмент, побудований на основі повторювача, то вузли такого сегмента не має сенсу включати до різних віртуальних мереж - все одно трафік цих вузлів буде загальним.

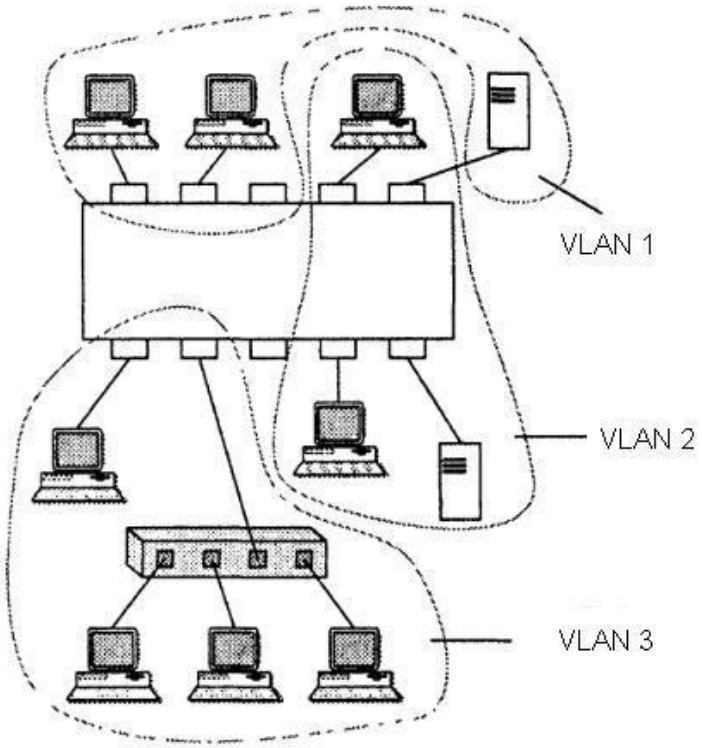

Рисунок 2.3 - Віртуальні мережі, побудовані на одному комутаторі за допомогою групування портів

Створення віртуальних мереж на основі групування портів не вимагає від адміністратора великого об'єму ручної роботи – достатньо кожен порт приписати до кількох заздалегідь названих віртуальних мереж. Зазвичай така операція виконується шляхом перетягування мишею графічних символів портів на графічні символи мереж.

2.2.2 Віртуальні локальні мережі на основі угруповання MAC-адрес

Другий спосіб, який використовується для утворення віртуальних мереж, базується на групуванні MAC-адрес. При наявності в мережі великої кількості вузлів, цей спосіб вимагає виконання великої кількості ручних операцій від адміністратора. Однак він виявляється гнучкішим при побудові віртуальних мереж на основі декількох комутаторів, ніж спосіб групування портів.

Рисунок 2.4 ілюструє проблему, що виникає під час створення віртуальних мереж з урахуванням кількох комутаторів, підтримують техніку групування портів. Якщо вузли будь-якої віртуальної мережі підключені до різних комутаторів, то для з'єднання комутаторів кожної такої мережі має бути виділено свою пару портів. В іншому випадку, якщо комутатори будуть пов'язані лише однією парою портів, інформація про належність кадру тієї чи іншої віртуальної мережі під час передачі з комутатора до комутатора буде втрачена. Таким чином, комутатори з угрупуванням портів вимагають для свого з'єднання стільки портів, скільки віртуальних мереж вони підтримують.

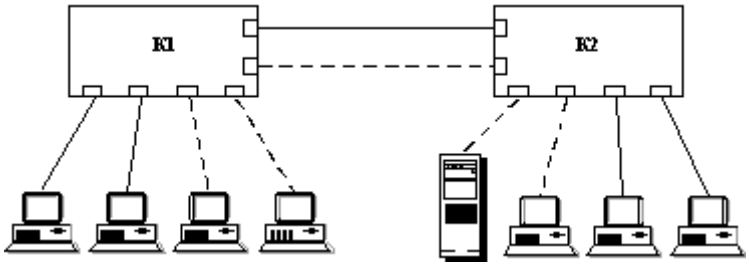

Рисунок. 2.4 - Побудова віртуальних мереж на кількох комутаторах із групуванням портів

Порти та кабелі використовуються при такому способі дуже марнотратно. Крім того, при з'єднанні віртуальних мереж через маршрутизатор для кожної віртуальної мережі виділяється в цьому випадку окремий кабель, що ускладнює вертикальне розведення, особливо якщо вузли віртуальної мережі присутні на декількох поверхах (рис. 2.5).

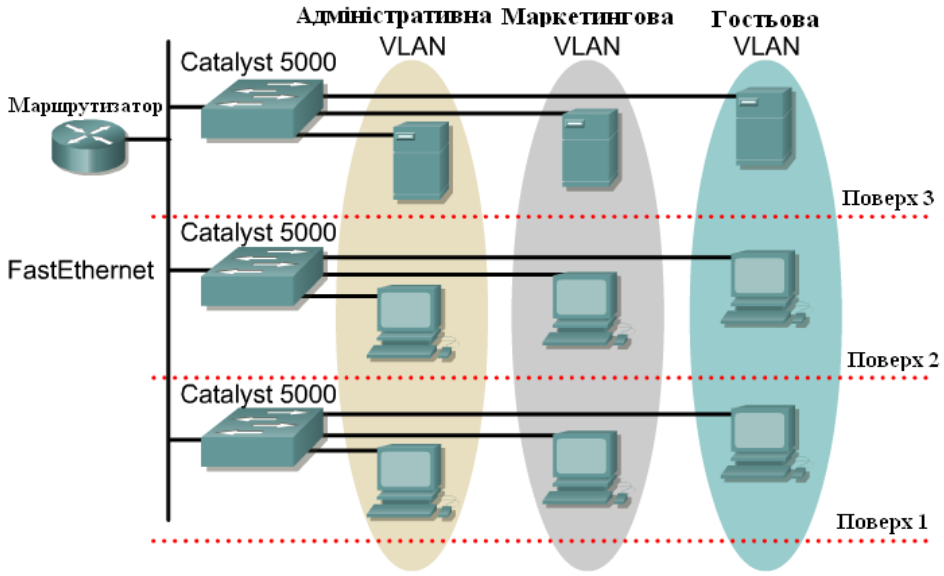

Рисунок 2.5 - З'єднання віртуальних мереж, побудованих на групуванні портів через маршрутизатор

Групування MAC-адрес у мережу на кожному комутаторі позбавляє необхідності їх зв'язку кількома портами, проте вимагає виконання великої кількості ручних операцій з маркування MAC-адрес на кожному комутаторі мережі.

2.2.3 Використання міток у додатковому полі кадру - стандарти 802.1Q/p та фірмові рішення

Описані два підходи засновані тільки на додаванні додаткової інформації до адресних таблиць мосту і не використовують можливості вбудовування інформації про належність кадру до віртуальної мережі в кадр, що передається. Інші підходи використовують наявні або додаткові поля кадру для збереження інформації та приналежності кадру під час його переміщення між комутаторами мережі. При цьому немає потреби запам'ятовувати в кожному комутаторі належність усіх MAC-адрес інтермережі віртуальним мережам.

Якщо використовується додаткове поле з позначкою про номер віртуальної мережі, воно використовується тільки тоді, коли кадр передається від комутатора до комутатора, а при передачі кадру кінцевому вузлу воно видаляється. У цьому модифікується протокол взаємодії "комутатор-комутатор", а програмне та апаратне забезпечення кінцевих вузлів залишається незмінним. Прикладів таких фірмових протоколів багато, але загальна вада у

них одна - вони не підтримуються іншими виробниками. Компанія Cisco запропонувала використовувати як стандартну добавку до кадрів будь-яких протоколів локальних мереж заголовок протоколу 802.10, призначеного для підтримки функцій безпеки обчислювальних мереж. Сама компанія використовує цей метод у тих випадках, коли комутатори поєднуються між собою за протоколом FDDI. Однак ця ініціатива не була підтримана іншими провідними виробниками комутаторів [5].

Новий стандарт IEEE 802.1Q визначає зміни у структурі кадру Ethernet, що дозволяють передавати інформацію про VLAN через мережу. Стандарт IEEE 802.1p специфікує метод вказівки на пріоритет кадру, заснований на використанні нових полів, визначених у стандарті IEEE 802.1Q. До кадру Ethernet додано два байти. Ці 16 біт містять інформацію про належність кадру Ethernet до VLAN і його пріоритет. Говорячи точніше, трьома бітами кодується до восьми рівнів пріоритету, 12 біт дозволяють розрізняти трафік до 4096 VLAN, а один біт зарезервований для позначення кадрів інших типів мереж (Token Ring, FDDI), що передаються по магістралі Ethernet. Треба сказати, що додавання двох байтів до максимального розміру кадру Ethernet веде до проблем в роботі багатьох комутаторів, що обробляють кадри Ethernet апаратно. Щоб уникнути їх, групи зі стандартизації запропонували скоротити на два байти максимальний розмір корисного навантаження у кадрі. Специфікація IEEE 802.1p, що створюється в рамках процесу стандартизації 802.1Q, визначає метод передачі інформації про пріоритет мережного трафіку. Стандарт 802.1p специфікує алгоритм зміни порядку розташування пакетів у чергах, за допомогою якого забезпечується своєчасна доставка чутливого до тимчасових затримок трафіку. На додаток до визначення пріоритетів стандарт 802.1p вводить важливий протокол GARP (Generic Attributes Registration Protocol) із двома спеціальними його реалізаціями. Перша з них – протокол GMRP (GARP Multicast Registration Protocol), що дозволяє робочим станціям робити запит на підключення до домену групового розсилання повідомлень. Концепцію, що підтримується цим протоколом, назвали приєднанням, ініційованим "листами". Протокол GMRP забезпечує передачу трафіку тільки в ті порти, з яких надійшов запит на груповий трафік, і добре узгоджується зі стандартом 802.1Q. Другою реалізацією GARP є протокол GVRP (GARP VLAN Registration Protocol), схожий на GMRP. Однак, працюючи по ньому, робоча станція замість запиту на підключення до домену групової розсилки

повідомлень надсилає запит на доступ до певної VLAN. Для узгодження роботи пристроїв, що підтримують формат кадру 802.1 Q з тими пристроями, які не розуміють цей формат, розробники стандарту запропонували ділити весь трафік у мережі на кілька типів [6]:

- трафік вхідного порту;
- внутрішній трафік;
- трафік вихідного порту.

Трафік вхідного порту (Ingress Port). Кожен кадр, що досягає комутованої мережі і йде від маршрутизатора, або від робочої станції, має певний порт-джерело. На підставі його номера комутатор повинен "ухвалити рішення" про прийом (або відкидання) кадру та передачу його в ту чи іншу VLAN. Рішення "долі" кадру, що здійснюється в єдиній логічній точці мережі, уможливлює співіснування різних видів VLAN. Прийнявши кадр, комутатор "прикріплює" щодо нього "ярлик" (tag) VLAN. Як тільки кадр з "ярликом" VLAN опиняється в мережі, він стає частиною проходить (Progress) або внутрішнього трафіку [7].

Внутрішній трафік (Progress Traffic). Кадр з "ярликом" комутується так само, як і без "ярлика". Рішення про його належність до тієї чи іншої VLAN приймаються в прикордонних елементах мережі та інші мережеві пристрої індиферентно "ставляться" до того, як саме кадр потрапив до мережі. Так як максимальний розмір кадру Ethernet залишився незмінним, пакети всіх VLAN зможуть оброблятися традиційними комутаторами і маршрутизаторами внутрішньої частини мережі [7].

Трафік вихідного порту (Egress Port). Щоб потрапити в міжмережевий маршрутизатор або кінцеву робочу станцію, кадр повинен вийти за межі комутованої мережі. Її вихідний пристрій "вирішує", якому порту (або портам) потрібно передати пакет і чи потрібно видаляти з нього службову інформацію, передбачену стандартом 802.1Q. Справа в тому, що традиційні робочі станції не завжди сприймають інформацію про VLAN за стандартом 802.1Q, але сервер, який обслуговує кілька підмереж за допомогою єдиного інтерфейсу, повинен її активно використовувати [7].

Умовний поділ трафіку на внутрішній, а також вхідний і вихідний порти дозволяє постачальникам нестандартних реалізацій VLAN створювати шлюзи для їх стикування з VLAN, що відповідають стандарту 802.1Q.

Налаштування VLAN транків

Транки використовуються обмінюватись інформацією про VLAN між комутаторами, забезпечуючи цим можливість побудови мереж VLAN, що перекривають фізичні межі комутатора. Концепція транкінгу подібна до протоколів маршрутизації, що використовуються для побудови мережевої топології. Комутатори використовують транкові протоколи для того, щоб визначити, на який порт надсилати кадри, якщо VLAN перекриває фізичні кордони. Використовуючи транковий протокол, одна й та сама VLAN може бути оголошена на кожному поверсі 12-поверхового будинку. Комутатори Catalyst підтримують різні транкові методи:

- Inter-Switch Link (ISL) Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps);
- IEEE 802.1Q Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps);
- IEEE 802.10 Fiber/Copper Distributed Data Interface (FDDI)/(CDDI) (100 Mbps);
- LAN Emulation ATM (155 Mbps OC-3 та 622 Mbps OC-12).

Це завжди гарна ідея подивитися "Release Notes" нових версій операційної системи комутатора, так як вони включають нові функції та можливості комутаторів. Це допоможе переконатися в тому, що комутатор підтримуватиме функції, необхідні для побудови мережі

2.2.4 Використання специфікації LANE

Існує два способи побудови віртуальних мереж, які використовують вже наявні поля для маркування належності кадру віртуальної мережі, проте ці поля належать не кадрам канальних протоколів, а осередкам технології ATM або пакетам мережного рівня.

Специфікація LANE вводить таке поняття як локальна мережа, що емулює - ELAN. Це поняття має багато спільного з поняттям віртуальної мережі:

- ELAN будується в мережі, що складається з комутаторів (ATM);
- зв'язок між вузлами однієї і тієї ж ELAN здійснюється на основі MAC-адрес без залучення мережного протоколу;
- трафік, що генерується будь-яким вузлом певної ELAN, навіть широкомовний, не виходить за межі цієї ELAN.

Кадри різних ELAN не зустрічаються один з одним всередині мережі комутаторів ATM, оскільки вони передаються за різними віртуальними

з'єднаннями і номер віртуального з'єднання VPI/VCI є тим самим ярликом, який позначає кадр певної VLAN у стандарті 802.1Q та аналогічних фірмових рішеннях.

Якщо VLAN будуються в змішаній мережі, де є не тільки комутатори ATM, то "чисті" комутатори локальних мереж, що не мають ATM-інтерфейсів, повинні використовувати для створення віртуальної мережі один з перерахованих вище методів, а прикордонні комутатори, що мають поряд з традиційними ще й ATM-інтерфейси повинні відображати номери VLAN на номери ELAN при передачі кадрів через мережу ATM.

2.2.5 Використання мережного протоколу

При використанні цього підходу комутатори повинні для утворення віртуальної мережі розуміти будь-який мережевий протокол. Такі комутатори називають комутаторами 3-го рівня, оскільки вони поєднують функції комутації та маршрутизації. Кожна віртуальна мережа отримує певну мережеву адресу - як правило, IP або IPX.

Тісна інтеграція комутації та маршрутизації дуже зручна для побудови віртуальних мереж, тому що в цьому випадку не потрібно введення додаткових полів у кадри, до того ж адміністратор лише одноразово визначає мережі, а не повторює цю роботу на канальному та мережному рівнях. Приналежність кінцевого вузла до тієї чи іншої віртуальної мережі у разі визначається традиційним способом - з допомогою завдання мережного адреси. Порти комутатора також отримують мережеві адреси, причому можуть підтримуватися нестандартні, для класичних маршрутизаторів ситуації, коли один порт може мати кілька мережевих адрес, якщо через нього проходить трафік кількох віртуальних мереж, або кілька портів мають ту саму адресу мережі, якщо вони обслуговують одну і ту саму віртуальну мережу [7].

При передачі кадрів у межах однієї і тієї ж віртуальної мережі комутатори 3-го рівня працюють як класичні комутатори 2-го рівня, а за необхідності передачі кадру з однієї віртуальної мережі до іншої - як маршрутизатори. Рішення про маршрутизації зазвичай приймається традиційним способом - його робить кінцевий вузол, коли бачить на підставі мережевих адрес джерела та призначення, що кадр потрібно надіслати в іншу мережу.

Однак використання мережного протоколу для побудови віртуальних мереж обмежує область їх застосування лише комутаторами 3-го рівня та

вузлами, що підтримують мережевий протокол. Звичайні комутатори не зможуть підтримувати такі віртуальні мережі і це є великим недоліком. За бортом також залишаються мережі на основі протоколів, що не маршрутизуються, насамперед мережі NetBIOS.

З цих причин найбільш гнучким підходом є комбінування віртуальних мереж на основі стандартів 802.1Q/p з подальшим відображенням їх на "традиційні мережі" в комутаторах 3-го рівня або маршрутизаторах. Для цього комутатори третього рівня та маршрутизатори повинні розуміти мітки стандарту 802.1Q.

2.3 Агент ретрансляції DHCP

Агент ретрансляції DHCP (dhcp-relay) дозволяє ретранслювати DHCP і BOOTP запити з підмережі, в якій немає DHCP сервера в іншу, або кілька інших підмереж, що мають DHCP сервери.

Комутатор може бути налаштований як агент DHCP Relay. У цьому випадку розширюються можливості застосування DHCP-серверів у мережі, оскільки вже не потрібно використовувати кілька DHCP-серверів по одному в кожній підмережі. Комутатор просто перенаправляє DHCP-запит від клієнта у локальній підмережі на віддалений DHCP-сервер.

Option 82 використовується передачі додаткової інформації в DHCP-запиті. До того ж цю інформацію додає сам комутатор. Ця інформація може бути використана при застосуванні політик для підвищення рівня безпеки та ефективності. Для простоти ці пакети містять BOOTP, тобто DHCP-запити обробляються комутатором як BOOTP-запити.

Коли DHCP клієнт запитує інформацію, агент ретрансляції DHCP пересилає запит списку DHCP серверів, вказаних під час запуску агента. Коли DHCP сервер повертає відповідь, він відправляється або широкомовно або направлено в мережу, з якої отримано початковий запит.

Формат поля DHCP option 82 для DES-35XX:

Формат поля опції з Circuit ID - в ній вказується порт комутатора, за яким знаходиться клієнт та VID відповідного VLAN:

1.	2.	3.	4.	5.	6.	7.
1	6	0	4	VLAN	Module	Port
1 байт	1 байт	1 байт	1 байт	2 байти	1 байт	1 байт

1. Тип опції.

2. Довжина.

3. Тип Circuit ID.

4. Довжина.

5. VLAN: VLAN ID DHCP-запиту клієнта.

6. Module: для автономного комутатора поле Module завжди 0; для стекування комутатора, Module = Unit ID.

7. Port: порт комутатора, з якого отримано DHCP-запит (починається з 1) port.

Формат поля опції з Remote ID - в ній вказується MAC-адреса комутатора, що є агентом DHCP Relay:

1.	2.	3.	4.	5.
2	8	0	6	MAC address
1 байт	1 байт	1 байт	1 байт	6 байтів

1. Тип опції.

2. Довжина.

3. Тип Remote ID type.

4. Довжина.

5. MAC address: MAC-адреса комутатора.

Приклад налаштування обладнання:

1. DHCP-сервер 10.51.8.1 у підмережі 10.0.0.0/8
2. Маршрутизатор або комутатор L3, що виступає в ролі шлюзу для двох підмереж
3. 10.51.8.11 для підмережі 10.0.0.0/8
4. 30.51.8.11 для підмережі 30.0.0.0/8
5. Комутатор L2 (DES-3526/DES-3550) у ролі агента DHCP Relay
6. 30.51.8.12 у підмережі 30.0.0.0/8

7. MAC-адреса: 00-80-C8-35-26-0A

8. 2 ноутбуки як DHCP - клієнтів, приєднані до портів 9 і 10 комутатора L2 відповідно

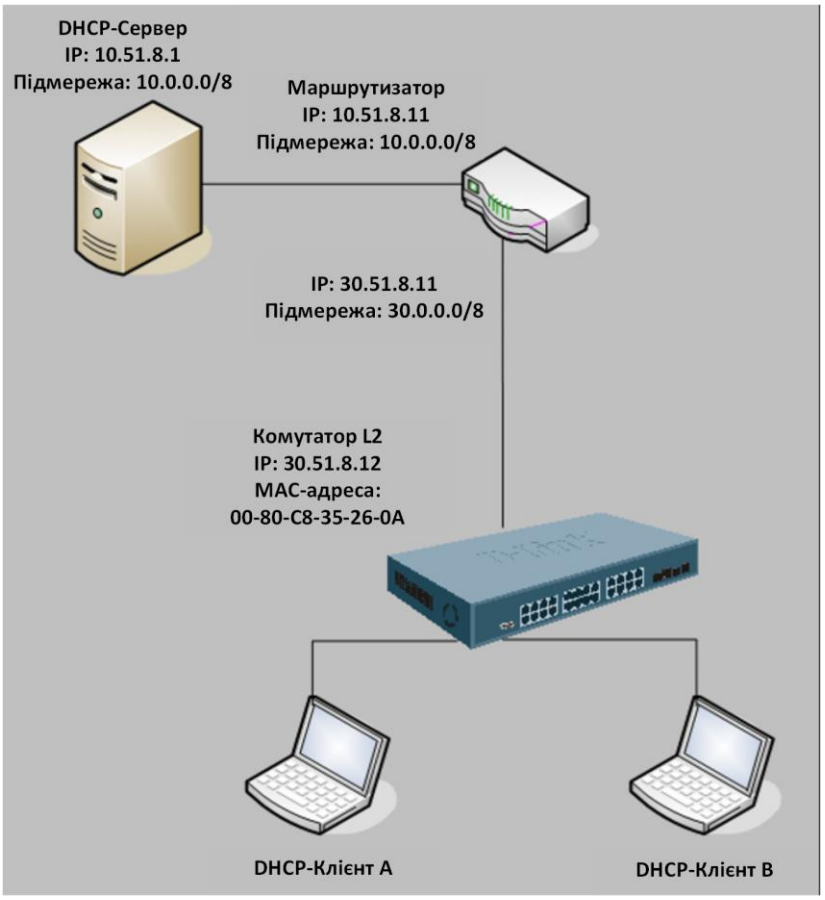

Рисунок 2.6 – Настроювання DHCP

Завдання:

1. DHCP-сервер використовує діапазон адрес 30.51.8.100 - 30.51.8.200 для видачі DHCP-клієнту, запити якого перенаправляються агентом DHCP Relay 30.51.8.12 (комутатор L2) - звичайний режим DHCP.

2. Як тільки клієнт DHCP підключається до порту 9 комутатора L2, DHCP-сервер видасть йому IP-адресу 30.51.8.161; якщо до порту 10 – то 30.51.8.162 - функція DHCP option 82.

Команди для налаштування комутатора L2 (DES-3526/DES-3550) наступні:

create iproute default 30.51.8.11

config dhcp_relay add ipif System 10.51.8.1

config dhcp_relay option_82 state enable

enable dhcp_relay

Налаштування DHCP-сервера:

У цьому прикладі використовується 30-денна версія haneWIN DHCP server 2.1.

1. У пункті Option -> Preferences -> DHCP зведіть галочку Accept Relay Agent Information (Option 82).

2. Конфігуруйте Option -> Default Client Profile -> Basic Profile Relay IP: 30.51.8.12 Dynamic IP Addresses: Від 30.51.8.100 до 30.51.8.200 Subnet mask: 255.0.0.0 Gateway Address: 30.51.8.11.

3. Налаштуйте DHCP option 82.

4. Задайте IP -адресу 30.51.8.161 для DHCP-клієнта A, підключеного до порту 9 комутатора L2.

5. "Add static entries".

6. Зведіть галочки "Circuit Identifier" та "Remote Identifier".

7. Hardware Address : 000400010009000600 80c835260a.

8. IP Address : 30.51.8.161.

9. Задайте IP- адресу 30.51.8.162 для DHCP- клієнта B, підключеного до порту 10 комутатора L2

10. "Add static entries"

11. Зведіть галочки "Circuit Identifier" та "Remote Identifier"

12. Hardware Address: 00040001000a00060080c835260a

13. IP Address: 30.51.8.162

2.4 Протоколи маршрутизації

RIP — так званий дистанційно-векторний протокол, який оперує хопами як метрику маршрутизації. Максимальна кількість хопів, дозволена в RIP - 15 (метрика 16 означає "нескінченно більшу метрику"). Кожен RIP-маршрутизатор за умовчанням веде мовлення в мережу свою повну таблицю маршрутизації раз на 30 секунд, генеруючи досить багато трафіку на низькошвидкісних лініях зв'язку. RIP працює на прикладному рівні стека TCP/IP, використовуючи порт UDP 520 [2].

У сучасних мережевих середовищах RIP — не найкраще рішення для вибору як протокол маршрутизації, оскільки його можливості поступаються більш сучасним протоколам, таким як EIGRP, OSPF. Обмеження на 15 хопів не дає застосовувати його у великих мережах. Перевага цього протоколу – простота конфігурування.

OSPF (англ. *Open Shortest Path First*) - протокол динамічної маршрутизації в мережах IPv4 і IPv6.

OSPF був розроблений для великих мереж, що розвиваються. Заснований на технології відстеження стану каналу (link-state technology), протокол виконує дві основні функції, притаманні будь-якому алгоритму маршрутизації:

- вибір шляху;
- комутація обраним шляхом.

Протокол OSPF був розроблений IETF у 1988 році. Остання версія протоколу представлена RFC 2328. Протокол OSPF є протоколом внутрішнього шлюзу (Interior Gateway Protocol — IGP) [9].

Протокол OSPF поширює інформацію про доступні маршрути між маршрутизаторами однієї автономної системи.

OSPF пропонує вирішення наступних завдань:

- збільшення швидкості збіжності;
- підтримка мережевих масок змінної довжини (VLSM);
- досяжність мережі;
- використання пропускної спроможності;
- метод вибору шляху.

2.5 Багатоадресне розсилання

Багатоадресне розсилання (Multicast) – це технологія економії смуги пропускання, яка скорочує трафік за рахунок доставки одного потоку інформації одразу тисячам корпоративних або приватних абонентів. Переваги багатоадресної розсилки використовують такі програми як відеоконференції, корпоративний зв'язок, дистанційне навчання. Суть багатоадресної розсилки полягає в тому, що вона дозволяє кільком одержувачам приймати повідомлення без передачі повідомлень кожному вузлу домену.

Багатоадресне розсилання передбачає надсилання повідомлень або даних на IP-адресу групи багатоадресної розсилки. Ця група не має фізичних чи

географічних обмежень: вузли можуть бути у будь-якій точці світу. Вузли, які зацікавлені в отриманні даних для певної групи, повинні приєднатися до цієї групи (підписатися на розсилку) за допомогою протоколу IGMP. Після цього пакети багатоадресної розсилки IP, що містять групову адресу в полі призначення заголовка, надходитимуть на цей вузол і оброблятимуться [10].

Групові адреси визначають довільну групу IP-вузлів, які приєдналися до цієї групи і бажають отримувати трафік, що адресований їй. Призначенням групових адрес управляє IANA (Internet Assigned Numbers Authority, Агентство з виділення імен та унікальних параметрів протоколів Інтернет). Воно виділило для групової IP-адресації старі адреси класу D. Це означає, що область багатоадресної розсилки охоплює адреси з 224.0.0.0 до 239.255.255.255 [10].

IANA зарезервувало область багатоадресної розсилки IP 224.0.0.0-224.0.0.255 для протоколів мережевих сегментів локальних мереж. Пакети з такими адресами ніколи не виходять за межі локальної мережі. Друга група адрес в діапазоні 224.0.1.0-224.0.1.255 – це глобальні адреси, які можуть використовуватися для багатоадресної передачі даних в Інтернет [10].

Сам собою багатоадресний трафік не знає нічого про те, де знаходяться його адресати. Як і для будь-якої програми, для цього потрібні протоколи.

Протокол IGMP (Internet Group Management Protocol, міжмережний протокол управління групами) використовується динамічної реєстрації окремих вузлів у багатоадресної групі локальної мережі. Вузли мережі визначають приналежність до групи, посилаючи повідомлення IGMP на свій локальний багатоадресний маршрутизатор. За протоколом IGMP маршрутизатори отримують IGMP-повідомлення та періодично надсилають запити, щоб визначити, які групи активні або неактивні в цій мережі [11].

Протокол IGMP v1

У версії 1 протоколу IGMP існують два типи IGMP-повідомлень:

- запит про приналежність до групи;
- відповідь про приналежність до групи.

Вузли надсилають IGMP-відповіді, які відповідають певній багатоадресній групі, щоб підтвердити своє бажання приєднатися до цієї групи. Маршрутизатор періодично надсилає IGMP-запит, щоб переконатися, що хоча б один вузол у підмережі ще має намір отримувати трафік, призначений для цієї групи. За відсутності відповіді на три послідовні IGMP-запити, маршрутизатор відключає групу і припиняє передавати адресований їй трафік.

Протокол IGMP v2

У версії 2 протоколу IGMP існують чотири типи IGMP-повідомлень:

- запит про приналежність до групи;
- відповідь про приналежність до групи за версією 1;
- відповідь про приналежність до групи за версією 2;
- залишити групу.

В основному робота IGMP 2 не відрізняється від IGMP 1. Різниця полягає в наявності повідомлень про вихід із групи. Тепер вузли самі можуть повідомити локальний багатоадресний маршрутизатор про намір покинути групу. У відповідь маршрутизатор надсилає групі спеціальний запит, щоб визначити, чи залишилися в ній ще вузли, які бажають отримувати цей трафік. Якщо відповіді не надійде, маршрутизатор відключає групу та припиняє передачу трафіку. Це може значно скоротити затримки, пов'язані з припиненням членства у групі, порівняно з IGMP 1. Небажаний та непотрібний трафік може бути припинений набагато швидше.

Управління багатоадресною розсилкою на 2 рівні

Стандартна поведінка комутатора 2-го рівня полягає у передачі всього багатоадресного трафіку на кожен порт, що належить локальній мережі-приймачу на даному комутаторі. Це пов'язано з тим, що комутатор не знаходить запису про MAC-адресу групової розсилки в таблиці комутації, і тому розсилає пакети через всі порти.

Це суперечить основному призначенню комутатора, яке полягає в обмеженні трафіку та доставці його тільки тим портам, для яких такі дані дійсно призначені.

Управління багатоадресною розсилкою на комутаторі може бути виконане декількома способами:

- віртуальні локальні мережі VLAN можуть визначати відповідні межі багатоадресної групи. Цей підхід простий, однак він не підтримує динамічне додавання або виключення членів групи;

- другий метод, що підтримується комутаторами D-Link – IGMP-прослуховування (IGMP-snooping). IGMP-прослуховування – це перевірки чи прослуховування локальної мережі на наявність у IGMP-пакетах, що передаються між вузлом та маршрутизатором, деякої інформації 3-го рівня (рис. 2.7). Коли комутатор отримує IGMP-звіт вузла для багатоадресної групи,

він заносить номер порту вузла запис своєї асоційованої багатоадресної таблиці. Коли комутатор отримує IGMP-повідомлення про вихід вузла із групи, він видаляє номер порту цього вузла із запису таблиці [10].

Оскільки управляючі IGMP-повідомлення передаються у вигляді багатоадресних пакетів, вони не відрізняються від багатоадресних даних 2-го рівня. Комутатор, на якому здійснюється IGMP-прослуховування, перевіряє всі багатоадресні пакети та шукає серед них ті, що містять інформацію, що управляє. IGMP-прослуховування сильно завантажує центральний процесор і може зменшити продуктивність комутатора. Тому в комутаторах зазвичай використовують спеціалізовані мікросхеми, які перевіряють IGMP-повідомлення на апаратному рівні.

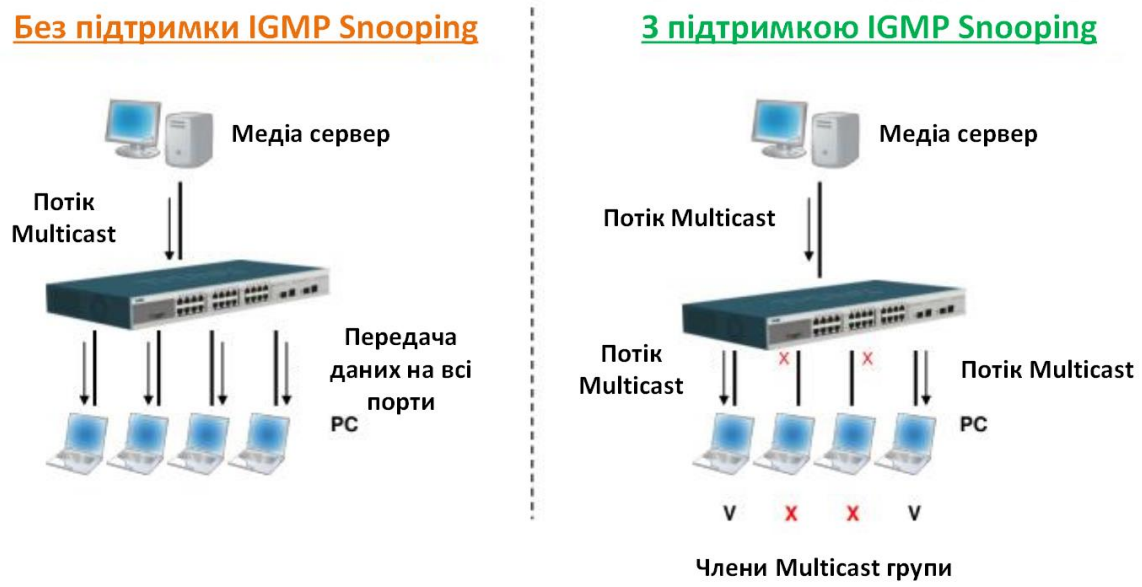

Рисунок 2.7 - IGMP-прослуховування у комутаторі 2-го рівня

3 АНАЛІЗ ЕТАПІВ РЕОРГАНІЗАЦІЇ БУДИНКОВОЇ ЛОКАЛЬНОЇ МЕРЕЖІ

3.1 Вимоги до будинкових локальних мереж при їх модернізації

Головною вимогою до будинкових локальних мереж є виконання мережею її основної функції - забезпечення користувачам можливості доступу в Інтернет і внутрішнім ресурсам всіх комп'ютерів, що знаходяться в даній мережі. Інші вимоги, такі як продуктивність, надійність, сумісність, керованість та масштабованість, пов'язані з якістю виконання цього основного завдання надання послуг користувачу.

Продуктивність - це властивість забезпечується можливістю розпаралелювання робіт між кількома комп'ютерами мережі. Існують такі основні характеристики продуктивності мережі - час реакції, пропускна здатність та затримка передачі, та варіація затримки передачі [1].

Час реакції мережі є інтегральною характеристикою продуктивності з погляду користувача. Загалом час реакції визначається як інтервал часу між виникненням запиту користувача до будь-якої мережної служби та отриманням відповіді на цей запит.

Пропускна здатність відображає обсяг даних, переданих мережею або її частиною за одиницю часу.

Затримка передачі визначається як затримка між моментом надходження пакета на вхід будь-якого мережного пристрою або частини мережі та моментом його появи на виході цього пристрою.

Надійність ЛОМ визначається такими показниками:

- готовністю чи коефіцієнтом готовності, що означає частку часу, протягом якого може бути використана система;

- ймовірністю доставки пакета вузлу призначення без спотворень (ймовірність втрати пакета);

- ймовірність спотворення окремого біта даних, що передаються (відношення втрачених пакетів до доставлених);

- здатність системи захистити дані від несанкціонованого доступу;

- стійкість до відмов - здатністю приховати від користувача відмову окремих елементів мережі;

- розширюваність означає можливість порівняно легкого додавання окремих елементів мережі (користувачів, комп'ютерів, додатків та служб), нарощуючи довжини сегментів мережі та заміни існуючої апаратури на більш потужну;

- масштабованість означає, що мережа дозволяє нарощувати кількість вузлів та протяжність зв'язків у дуже широких межах, при цьому продуктивність мережі не погіршується;

- підтримка різних видів трафіку. Мережа має забезпечити спільну передачу традиційного комп'ютерного та мультимедійного трафіку. Якщо мережа має підтримку різних видів трафіку цю мережу можна називати мультисервісною мережею;

- керованість має на увазі можливість централізовано контролювати стан магістральних та окремих елементів мережі, виявляти та вирішувати проблеми, що виникають при роботі мережі, виконувати аналіз продуктивності мережі та планувати подальший її розвиток;

- сумісність або інтегрованість означає, що мережа здатна включати найрізноманітніше програмне та апаратне забезпечення, тобто в ній можуть співіснувати різні операційні системи, що підтримують різні стеки комунікаційних протоколів, і працювати апаратні засоби і додатки від різних виробників.

3.2 Аналіз будинкової локальної обчислювальної мережі

Необхідність модернізації будинкової локальної мережі обумовлена такими основними причинами:

1. На даний момент будинкова мережа є мережею другого рівня, побудована за технологією Gigabit Ethernet з використанням топології зірка. На магістральних оптичних лініях використовуються керовані комутатори другого рівня та програмований комутатор третього рівня у центрі топології.

2. Мережа не поділена на логічні сегменти, тобто маршрутизація трафіку у мережі не здійснюється. Тому з мережі в одному broadcast домені виявляються близько 6500 комп'ютерів. Цей фактор позначається на якості послуг доступу в Інтернет, особливо вечорами, коли активність широкомовного трафіку в мережі зростає.

3. Вхідний гігабітний Інтернет канал у локальну мережу не може забезпечити належну швидкість і вимагає його розширення.

4. Впровадження IP-телебачення вносить низку проблем, пов'язаних із передачею даних у реальному режимі часу. Для цього розроблено методики пріоритезації трафіку у мережах передачі даних. Поточне мережеве обладнання, встановлене в локальній мережі, може забезпечити передачі даних у реальному режимі часу, але не за нинішньої логічної структури та налаштування, при наявній структурі можливі збої в роботі сервісу телебачення та сервісу IP-телефонії також критичне по часу.

5. Потрібно врахувати, що постійно надходять дзвінки від потенційних користувачів на підключення до мережі та потрібно забезпечити запас продуктивності мережі для нових користувачів.

6. Також на ринку послуг зв'язку існує конкуренція і для того, щоб не розгубити клієнтську базу, потрібно йти в ногу із сучасними технологіями та сервісами локальних мереж.

Таким чином, справжня архітектура мережі вже не може забезпечувати належну пропускну спроможність каналів зв'язку для впровадження нових послуг та підвищення якості обслуговування клієнтів.

Зростання клієнтської бази, впровадження L2 послуг на побудованій мережі, спричиняє постійне підвищення навантаження на комутатори всіх рівнів мережі та border'ів, з метою недопущення навантаження комутаторів, зняття існуючого граничного завантаження та для підвищення якості надання послуг triple-play (дані, голос та відео), пропонується провести реорганізацію мережі з мінімальними фінансовими вкладеннями.

Виходячи з аналізу будинкової локальної мережі, однозначно можна сказати, що технологія, що застосовується, при модернізації мережі залишиться Gigabit Ethernet, так як використання іншої технології економічно не вигідно та недоцільно. Також ця технологія економічно вигідна за ціною за порт. Топологію змінювати немає сенсу, так як це спричинить будівництво нових оптичних трас і вимагатиме великих фінансових вкладень, не кажучи про всілякі проблеми, що супроводжують будівництво нових каналів зв'язку. Необхідно використовувати якнайбільше функцій реалізованих у наявному обладнання (DES-3526, DXS-3326 GSR). Захист та керування на основі аналізу пакетів та відстеження стану з'єднань, блокування DoS-атак, списки контролю

доступу (ACL). Таким чином можна зробити висновок, що для оптимізації роботи мережі необхідно виконати наступні етапи:

1. Реорганізація інфраструктури опорної мережі для передачі голосу та відео, що забезпечують покращену якість обслуговування, включаючи підтримку технології управління трафіком. Використовуючи диференційовані IP-послуги для програм.

2. Винести інтерфейси управління комутаторів в окремий VLAN, це дозволить здійснювати віддалене управління та конфігурування, через графічний інтерфейс користувача за допомогою спеціального програмного забезпечення або за протоколами Telnet, Secure Shell або Rlogin.

3. Централізоване сповіщення про стан активного обладнання через протокол SNMP, що підвищить можливість запобігання та пошуку несправностей у мережі, спостереження за завантаженістю каналів зв'язку.

4. Централізувати динамічну видачу налаштувань мережі користувачам, шляхом перенесення dhcp-сервера з border'a на сервер, що знаходиться в датацентрі компанії.

3.3 Концепція розвитку будинкової локальної обчислювальної мережі

З розвитком інформаційних технологій люди передають мережами передачі не лише дані, а й голос, і зображення. Сукупність надання таких послуг, носить маркетинговий термін Triple-play, що передбачає наявність широкосмугового доступу до мережі Інтернет. Вимоги до такої послуги висуваються високі. Дані необхідно одержувати повністю. Голос необхідно чути чітко, не повинно бути проблем із встановленням зв'язку, чутністю. Відео має бути якісним, не повинно бути розсипання картинки, зависань зображень, звук та відео мають бути синхронізовані. Для того, щоб описані критерії дотримувалися, необхідно мати надійну і якісну опорну мережу, де буде оптимально збалансовано завантаження процесорної потужності комутаційного обладнання, пропускна здатність каналів зв'язку, паразитний трафік і шуми повинні бути мінімізовані, щоб не викликати тимчасових затримок.

Для реорганізації мережі пропонуються такі основні дії:

1. Винести інтерфейси керування комутаторів (management-інтерфейсів) в окремий VLAN з виділенням мережі /21 для комутаторів. Management-VLAN пропонується затермінувати на border. Виконання цього пункту дозволить

виключити негативний вплив клієнтського трафіку на комутатори та дозволить скоротити розмір ACL на ТКД за рахунок винесення з нього правил, що забороняють користувачам підставляти IP-адреси з підмережі management-інтерфейсів комутаторів. Винесення management'у буде здійснено, не торкаючись надання сервісів клієнтам.

2. Перенести термінацію підмережі користувача с Border на У-2. На кожен У-2 виділити мережу /21, тобто 2045 адрес для клієнтів. Виконання цього пункту дозволить скоротити існуючий величезний броадкаст домен у десятки разів, що в стільки ж разів знизить навантаження на комутатори.

3. Підняти OSPF-маршрутизацію між У-2 та border'ом, для направлення трафіку всередині району безпосередньо з У-2 на У-2 в обхід border'a.

4. Вивести багатоадресний трафік в окремий VLAN з підмережі користувача, це забезпечить безперешкодний транспорт для введення нового бізнес процесу IP телебачення.

5. Централізувати динамічну видачу налаштувань мережі користувачам, шляхом перенесення DHCP-сервера з граничного маршрутизатора на сервер, що знаходиться в датацентрі компанії. Перенесення буде здійснено шляхом увімкнення функції DHCP-relay на ТКД без переривання сервісу клієнтів. Виконання цього пункту дозволить нам виконати наступні пункти даного проекту та отримувати додаткову інформацію про клієнта в полях DHCP option 82, яка може стати в нагоді для подальших розробок.

6. Підняти дистрибуцію статичних маршрутів для мереж локальних ресурсів з У-2 у бік клієнтів, за допомогою протоколу динамічної маршрутизації OSPF. Цей протокол вибраний через підтримку операційними системами сімейства Microsoft Windows. Даний пункт зробить більш простим та зручним налаштування клієнтам. А головне додасть динамічність маршрутам статики, що прописуються зараз клієнтами.

7. Перевести лінки між ТКД та У-2 у повноцінні транки. Даний пункт при необхідності дозволить легко впроваджувати QoS на будинковій мережі.

3.4 Апаратне забезпечення модернізованої будинкової локальної обчислювальної мережі

Модернізована будинкова мережа, побудована за логічною схемою, представлена на рис. 3.1.

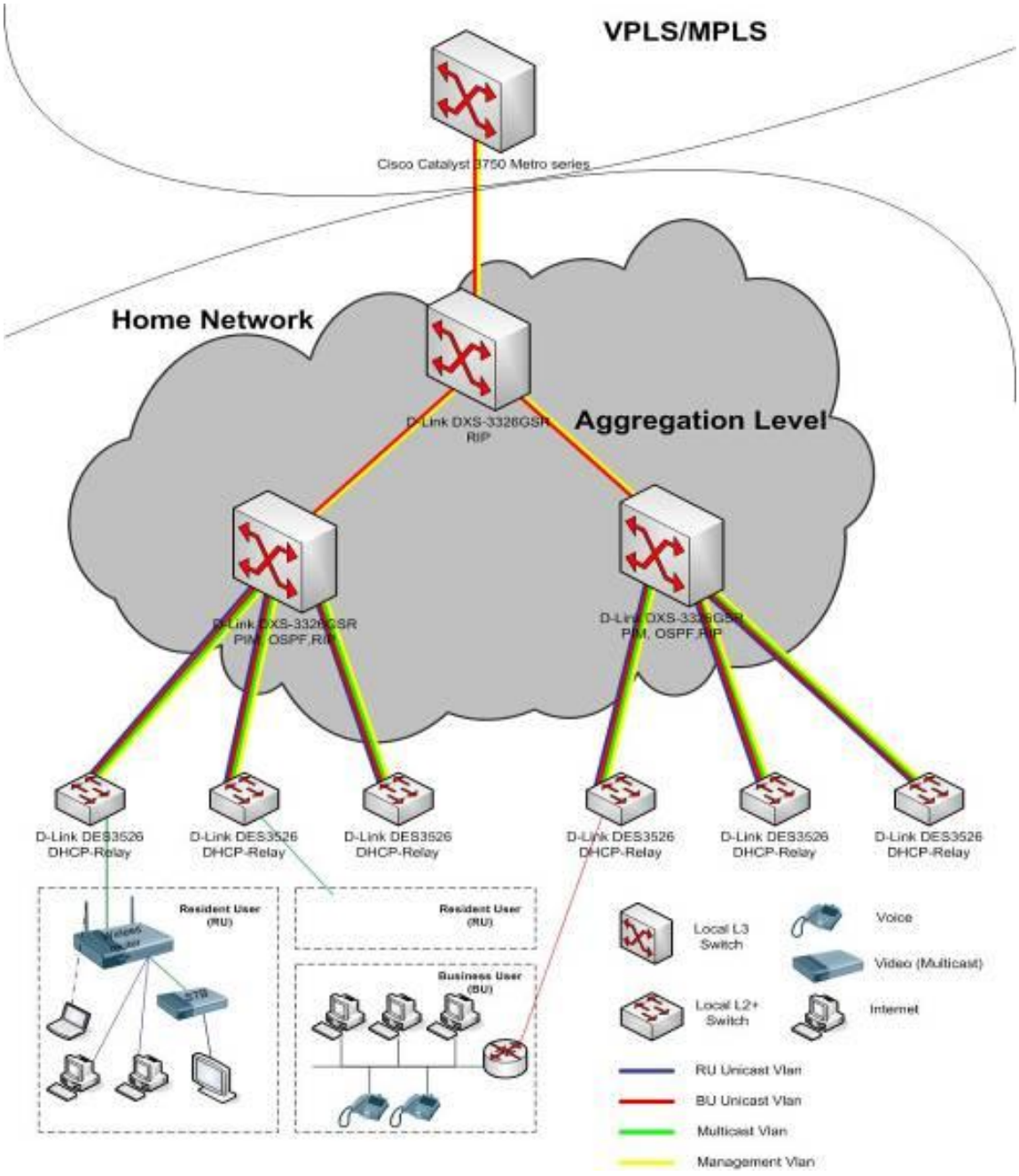

Рисунок 3.1 - Модернізована будинкова мережа

Розглянемо архітектуру широкосмугової мережі доступу. Ключовим моментом дизайну мережі є трирівнева модель побудови мережі. У мережі можна виділити обладнання рівня доступу (Access Layer) - це світчі, до яких підключені клієнти, рівня розподілу (Aggregation Layer) - вузлові комутатори (1-ий, 2-й рівні та агрегатори), рівня Ядра мережі (Backbone Layer).

Таким чином, загальна схема мережі поділяється на три рівні:

1. Рівень доступу – здійснює фізичну концентрацію абонентських ліній. Одиницю обладнання даного рівня називатимемо ТКД (точка колективного

доступу). ТКД організує поділ абонентів лише на рівні Ethernet з допомогою віртуальних мереж, забезпечує обмеження швидкості передачі на вході у мережу і здійснює базові функції безпеки.

2. Рівень розподілу - термінує віртуальні мережі доступу рівня з використанням протоколу IP.

3. Рівень ядра - служить високошвидкісною і надійною магістраллю, що об'єднує все в єдине ціле.

Сервери широкосмугового доступу (BRAS) – як сервери широкосмугового доступу встановлюються маршрутизатори Cisco 7301, на яких термінуються тунельні PPTP/L2TP сесії клієнтів, які звертаються до Інтернету. Трафік від клієнтів до Інтернету проходить крізь сервери широкосмугового доступу.

Для реорганізації мережі буде потрібно 1 сервер для перенесення dhcp-сервера з граничного маршрутизатора, комутаційне обладнання змінювати немає необхідності, оскільки комутаційної потужності та набору функцій комутаторів DES-3526, DXS-3326 GSR вистачить для основних пунктів модернізації.

Сервер HP ProLiant DL320 (G3)

Третє покоління серверів ProLiant DL320 (рис. 3.2) розроблено для роботи зі спеціалізованими пропозиціями, які використовуються на малих та середніх підприємствах. Крім того, завдяки новітнім мікросхем Intel з'явилося безліч нових технічних можливостей.

- оптимізовані для щільного розміщення, максимальної гнучкості та керованості;
- ідеальне рішення для розгортання багато серверної конфігурації;
- стійкові та кластерні моделі.

Рисунок 3.2 – Зовнішній вигляд сервера HP ProLiant DL320 (G3)

Таблиця 3.1 - Технічні характеристики HP ProLiant DL320 (G3)

Пристрій	Характеристика
1	2
Процесор	Intel Pentium 4 3,2 ГГц з підтримкою Hyper-Threading та EM64T
Кеш-пам'ять	2 МВ кеш-пам'яті другого рівня
Кількість процесорів	1
Набір мікросхем	Intel E7221 з шиною FSB 800 МГц
Пам'ять	2 ГБ PC3200 DDR SDRAM
Мережевий контролер	двопортовий інтегрований NC7782 10/100/1000
Слоти розширення	64-біт/133 МГц PCI-X - 1 (повнорозмірний), 64-біт/100 МГц PCI-X - 1 (у половину довжини)
Контролер/RAID-контролер	інтегрований двопортовий SATA контролер із підтримкою RAID 0/1.
Флоппі-дисковод	опціонально
оптичний привід	опціонально
Максимальна кількість стандартних внутрішніх дискових відсіків	2x1" (SATA або SCSI без гарячої заміни)
Дискові масиви	500 ГБ (SATA с/без гарячої заміни)
Інтерфейси	USB 4 послідовний 1 вказівний пристрій (миша) 1графічний 1клавіатура 1роз'єм RJ -45 2 iLO remote management
Графічний адаптер	інтегрований відеоконтролер ATI RAGE XL з 8 МБ відеопам'яті SDRAM
Форм-фактор	для монтажу у стійку 1U
Відповідність галузевим стандартам	ACPI 2.0, PCI 2.2 Compliant, PXE Support WOL Support, Microsoft® Logo certifications USB 2.0
Функції керування	ASR (Automatic Server Recovery); iLO Advanced Pack (додатково); HP Systems Insight Manager; вбудований журнал керування; монітор контролю параметрів накопичувача (з контролерами Smart Array); функція динамічного відновлення секторів (з контролерами Smart Array); профілактична гарантія на жорсткі диски SAS та SCSI, пам'ять та процесори
Управління безпекою	Пароль на включення живлення; пароль клавіатури; контроль дисководу гнучких дисків; контроль завантаження з дискети; контроль порту USB; знімні приводи для компакт-дисків та флоппі дисків; пароль адміністратора
Блок живлення	Блок живлення з автоматичним визначенням, 350 Вт, PFC, відповідність CE Mark

Стекований комутатор Gigabit Ethernet 2-го рівня D - Link DES -3526

Рисунок 3.3 - Стекований комутатор рівня доступу D-Link DES-3526

Комутатори серії 10/100 Мбіт/с D-Link DES-3500 є взаємно стековані комутаторами рівня доступу, що підтримують технологію Single IP Management (SIM, управління через єдину IP-адресу). Ці комутатори, що мають 24 або 48 10/100BASE-TX портів і 2 комбо-порти 1000BASE-T/SFP Gigabit Ethernet у стандартному корпусі для встановлення у стійку, розроблені для гнучкого та безпечного мережного підключення (рис. 3.3). Комутатори серії DES-3500 можуть легко об'єднуватися в стек і налаштовуватися разом з будь-якими іншими комутаторами з підтримкою D-Link Single IP Management, включаючи комутатори 3-го рівня ядра мережі, для побудови багаторівневої мережі, структурованої з магістраллю і централізованими швидкодіючими серверами [9].

В основному комутатори серії DES-3500 формують стек мережі рівня підрозділу, надаючи порти 10/100 Мбіт/с та можливість організації гігабітного підключення до магістралі. Трафік, що передається між пристроями стека, проходить через інтерфейси Gigabit Ethernet з підтримкою повного дуплексу та звичайні дроти мережі, дозволяючи уникнути використання дорогих та громіздких кабелів для стекування. Відмова від використання цих кабелів дозволяє усунути бар'єри, пов'язані з їх довжиною та обмеженнями методів стекування. У стек можуть бути об'єднані пристрої, розташовані в будь-якому місці мережі, за винятком можливості появи будь-якої точки єдиної відмови (single point of failure) [9].

Управління через єдину IP-адресу (Single IP Management)

Комутатори серії DES-3500 полегшують і прискорюють завдання управління, т.к. безліч комутаторів можуть налаштовуватися, контролюватись і обслуговуватися через унікальну IP-адресу з будь-якої робочої станції, що має Web-браузер.

Стек управляється як єдиний об'єкт, і всі пристрої стека визначаються за єдиною IP-адресою. За допомогою вбудованого Web-менеджера, можна отримати інформацію, представлену у вигляді дерева (Tree View) про членів стека та топології мережі із зазначенням розташування пристроїв стека та зв'язків між ними. Це просте і досить ефективне Web-управління унеможливлює встановлення дорогого ПЗ для SNMP-управління [9].

У стек можна легко об'єднати до 32 комутаторів, незалежно від моделі. Віртуальний стек підтримує будь-які моделі комутаторів із вбудованим Single IP Management. Це означає, що стек може бути розширений комутаторами, включаючи комутатори 3-го рівня для мережі ядра, комутатори на основі шасі або будь-які інші комутатори.

Серія DES-3500 забезпечує розширений набір функцій безпеки для керування підключенням та доступом користувачів. Цей набір включає Access Control Lists (ACL) на основі MAC-адрес, портів комутатора, IP адрес та/або номерів портів TCP/UDP, автентифікацію користувачів 802.1x і контроль MAC-адрес. Крім цього, DES-3500 забезпечує централізоване управління адміністративним доступом через TACACS+ та RADIUS. Разом з контролем над мережними додатками, ці функції безпеки забезпечують не лише авторизований доступ користувачів, але й запобігають розповсюдженню шкідливого трафіку по мережі [9].

Для підвищення продуктивності та безпеки мережі комутатори серії DES-3500 забезпечує розширену підтримку VLAN, включаючи GARP/GVRP, 802.1Q та асиметричні VLAN. Управління смугою пропускання дозволяє встановити ліміт трафіку для кожного порту, що дає змогу керувати обсягом трафіку на межі мережі. Комутатор підтримує встановлення резервного джерела живлення. Інші характеристики включають підтримку 802.3ad Link Aggregation, 802.1d Spanning Tree, 802.1w Rapid Spanning Tree та 802.1s Multiple Spanning Tree для підвищення надійності та доступності віртуального стека [9].

Серія DES-3500 має широкий набір багаторівневих (L2, L3, L4) QoS/CoS функцій для гарантії того, що критично важливі мережеві сервіси, подібні до VoIP, ERP, Intranet або відеоконференції будуть обслуговуватися з належним пріоритетом. Підтримуються 4 черги пріоритетів для 802.1p/TOS/DiffServ з класифікацією на основі MAC-адрес джерела та приймач, IP-адрес джерела або приймача та/або номерів портів TCP/UDP [9].

Стекований комутатор Gigabit Ethernet 3-го рівня D - Link DES-3326SR

Рисунок 3.4 - Стекований комутатор D - Link DES - 3326SR

Комутатори нового покоління серії xStack DGS-3300 надають мережам великих підприємств та підприємств малого та середнього бізнесу (SMB) високу продуктивність, гнучкість, безпеку, багаторівневу якість обслуговування (QoS) та можливість підключення резервного джерела живлення (рис. 3.4). Комутатори забезпечують високу щільність гігабітних портів для підключення робочих місць, оснащені слотами SPF для гнучкого підключення оптики, слотами для встановлення модулів розширення з портами 10 Gigabit Ethernet і підтримують розширені функції програмного забезпечення. Комутатори можна використовувати як пристрої рівня доступу підрозділів або в ядрі мережі для створення багаторівневої мережної структури з високошвидкісними магістралями та централізованим підключенням серверів. Провайдери послуг можуть використовувати переваги комутаторів з високою щільністю портів SFP для формування ядра оптичної мережі (FTTB) [9].

Віртуальний стек.

Будь-який з комутаторів серії DGS-3300 може функціонувати в якості автономного пристрою або частини стека, що масштабується. Вбудована підтримка технології Single IP Management дозволяє автономному комутатору стати частиною віртуального стека, в якому внутрішньостіковий трафік передається по звичайних мережних кабелях, за винятком необхідності використання дорогих спеціалізованих кабелів для стекування. Це дозволяє уникнути проблем, пов'язаних з довжиною кабелів та методом фізичного стекування та об'єднати у віртуальний стік пристрої, розташовані в будь-якому місці мережі, мінімізуючи вплив єдиної точки можливої відмови [9].

Безпека, продуктивність і доступність

Комутатори серії DGS-3300 пропонують широкий набір функцій безпеки, включаючи багаторівневі L2/L3/L4 списки контролю доступу та автентифікацію користувачів 802.1x через сервери TACACS+ та RADIUS. Крім того, вони підтримують статичну IP v.4/v.6 маршрутизацію на 3 рівні для підвищення продуктивності та безпеки мережі. Вбудована технологія ZoneDefense є механізмом, що дозволяє спільно працювати комутаторам D-Link серії xStack і міжмережевим екранам і забезпечує активну мережну безпеку. Функція Zone-Defense автоматично ізолює інфіковані комп'ютери мережі та запобігає поширенню ними шкідливого трафіку [9].

Для підвищення продуктивності та безпеки комутатори серії DGS-3300 забезпечують розширену підтримку VLAN, включаючи GARP/GVRP та 802.1Q. Для підтримки об'єднаних програм, включаючи VoIP, ERP та відеоконференцій, широкий набір функцій QoS/CoS 2/3/4 рівнів гарантує, що критичні до затримок мережеві сервіси будуть обслуговуватись у пріоритетному режимі. Для запобігання завантаженню центрального процесора обробкою шкідливого широкомовного трафіку, генерованого зловмисниками або обумовленого вірусною активністю, комутатори серії DGS-3300 надають функцію D-Link Safeguard Engine, що дозволяє підвищити надійність та доступність мережі. За допомогою функції контролю смуги пропускання для кожного порту можна встановлювати ліміти, гарантуючи певний рівень обслуговування кінцевих користувачів. Функція керування смугою пропускання для кожного потоку дозволяє настроювати типи обслуговування на основі певних IP-адрес або протоколів [9].

4 ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА НАЛАШТУВАННЯ КОМУТАЦІЙНОГО ОБЛАДНАННЯ

Структура вихідної мережі представлена на рис. 4.1 є працюючої системою приносить дохід, отже, надання сервісу кінцевим абонентам є пріоритетним завданням. Під час проведення всіх робіт з реорганізації схеми управління та оптимізації структури необхідно забезпечити мінімальне переривання сервісу та можливість відкату на стару працюючу схему.

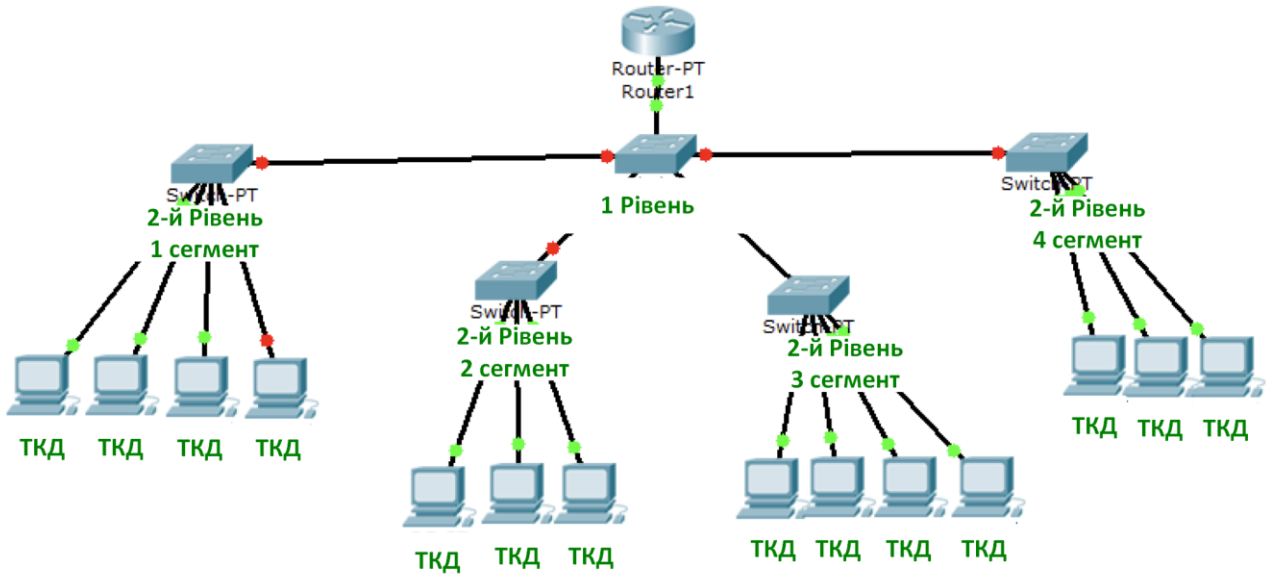

Рисунок 4.1 – Логічна побудова локальної мережі

1. Етап підготовки мережі.

Визначення точної топології домашньої мережі, якщо потрібно збір заявок на виправлення (за наявності будь-яких тимчасових каналів зв'язку, каскадних підключень). Перевірка комутаторів, визначення портів сегмента.

2. Виділення необхідної кількості мереж для реалізації проекту:

- мережі для роботи OSPF/30;
- мережі для users/21;
- мережі для management/22;
- формування конфігу DHCP сервера.

3. Підготовка конфігів:

- комутаторів ДС для динамічного формування неблокованого сервера DHCP;

- магістрального обладнання для організації належного пірингу.

4. Запуск маршрутизації:

- термінуємо інтерфейси на граничному маршрутизаторі;

- термінуємо інтерфейси на вузлах сегментів;

- переконуємося, що маршрутизація працює правильно та мережі анонсуються;

- видаляємо default route на вузлах, переконуємося, що маршрут прийшов по OSPF.

5.Запуск користувачів:

- видаляємо аплінк з VLAN-а користувачів;

- термінуємо користувачів на У2;

- запускаємо DHCP.

6. Переконуємося, що користувачі почали отримувати IP та підключатися до VPN серверу.

Всі пункти будуть виконуватися послідовно, з оповіщенням клієнтів та необхідними проміжками для переходу клієнтів на нову адресацію. Запланована перерва сервісу не більше хвилини на кожного клієнта. Проект впроваджується на існуючому обладнанні без істотних матеріальних витрат. L3 трафік проходить через У-2 досить малий і ресурсів DXS-3326GSR цілком вистачить для такої схеми організації, єдине обмеження, що нас зачіпає, в ньому це розмір таблиці ipfdb в 3000 записів, але при підключенні більше 2500 клієнтів в сегменті - його легко замінити на більш потужний наприклад, DGS-3627G з таблицею ipfdb в 8000 записів. L3 функції на У-1 не будуть задіяні, і значить підвищених вимог до нього не пред'являється.

Розширення вхідного каналу. Під час будівництва оптичних ліній зв'язку використовується багатожильний оптичний кабель. За наявності вільних волокон можна розширити вхідний канал, використовуючи технологію агрегування каналів - технологія, яка дозволяє об'єднати кілька фізичних каналів в один логічний. Таке об'єднання дозволяє збільшувати пропускну здатність каналу та збільшити надійність каналу. Агрегування каналів може бути налаштовано як між двома комутаторами, і між комутатором і сервером.

В якості платформи для сервера DHCP пропонується використовувати Unix-подібну операційну систему для ПК, засновану на різних, сучасних

архітектурах. Ця операційна система обрана в першу чергу через свою дуже високу надійність, стабільність, захищеність і високу продуктивність. Також важливу роль у виборі цієї операційної системи відіграли фактори, що вона є операційною системою з відкритим кодом і для неї доступні тисячі безкоштовних пакетів та прикладних програм. Можна налаштувати сервер DHCP, використовуючи файл конфігурації /etc/dhcpd.conf.

Інформаційна безпека модернізованої будинкової локальної обчислювальної мережі

Безпеку в локальній мережі повинна забезпечувати адміністрація мережі, але користувачі теж не повинні забувати про безпеку в мережі, оскільки більшість шкідливих програм розповсюджуються через комп'ютери користувачів. Таким чином, потрібен комплекс заходів для забезпечення інформаційної безпеки в мережі, як з боку адміністрації, так і з боку рядових користувачів.

Користувачам мережі потрібно захищати лише свій комп'ютер, щоб зберегти цілісність конфіденційної інформації, приховати її від інших користувачів мережі, так само комп'ютер може стати розсадником вірусів і всіляких мережевих черв'яків, які заважатимуть працювати всім користувачам мережі, створюючи великий локальний трафік. Щоб користувачеві захистити свій комп'ютер, йому необхідний комплекс програмного забезпечення для забезпечення безпеки.

Існує багато програмних комплексів захисту комп'ютера. Наприклад: Norton Internet Security, Panda Internet Security, F - Secure Internet Security і т.д.

Склад цих програмних комплексів майже однаковий і до них входять такі компоненти:

1. Антивірус:

- програма здійснює антивірусну перевірку поштового трафіку на рівні протоколу передачі даних (POP3, IMAP та NNTP для вхідних повідомлень та SMTP для вихідних повідомлень) незалежно від поштової програми;

- перевірка інтернет-трафіку. Забезпечує антивірусну перевірку інтернет-трафіку, що надходить за мережевими протоколами, також здійснюється окрема перевірка HTTP трафіку на предмет spyware. У режимі реального часу, дозволяючи таким чином запобігти зараженню ще до збереження файлів на жорсткому диску комп'ютера;

- захист файлової системи. Антивірусної перевірки піддаються будь-які окремі файли, каталоги та диски, так само можлива перевірка лише критичних областей операційної системи та об'єктів, що завантажуються при старті ОС;

- проактивний захист. Здійснюється постійне спостереження за активністю програм та процесів, запущених в оперативній пам'яті комп'ютера, та своєчасно попереджає користувача у разі появи небезпечних, підозрілих чи прихованих процесів; запобігає небезпечним змінам файлової системи та реєстру, а також відновлює систему після шкідливого впливу.

2. Брандмауер:

- блокує атаки мережі. Фіксує спроби сканування портів комп'ютера, що часто передують мережевим атакам, і успішно відображає найпоширеніші типи атак хакерів, забороняючи взаємодію з атакуючим комп'ютером. Моніторинг мережної активності дозволяє статистику всіх з'єднань;

- контролює всі мережеві взаємодії. На основі заданих правил програма контролює звернення додатків до джерел у мережі Інтернет та відстежує вхідні та вихідні пакети даних;

- робить безпечну роботу в будь-яких мережах;

- має режим невидимості під час роботи в інтернеті. Режим невидимості запобігає виявленню комп'ютера ззовні. При переключенні в цей режим забороняється вся мережева діяльність, крім передбачених правилами винятків, які визначаються користувачем.

За підсумками проведених етапів з реорганізації схеми управління та оптимізації мережі було досягнуто наступних результатів:

- знижено завантаження процесорної потужності обладнання рис. 4.2, 4.3;

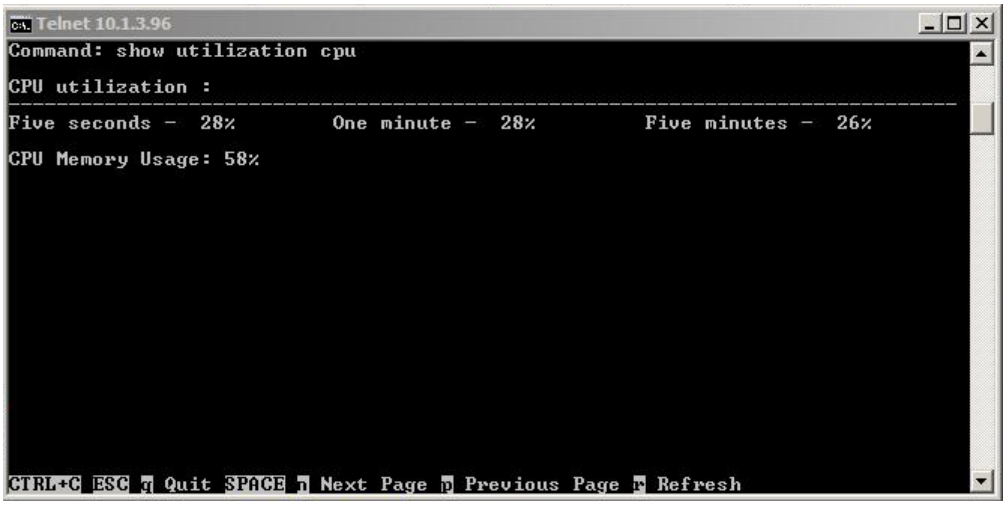

Рисунок 4.2 – Завантаження процесора до сегментації

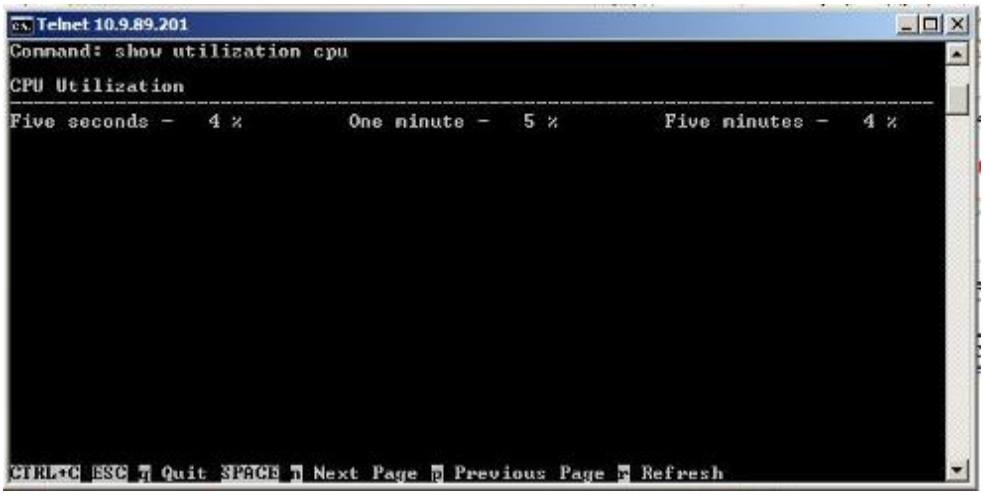

Рисунок 4.3 – Завантаження процесора після сегментації

- скорочено броадкаст домен у десятки разів. Виключено вплив користувачів на обладнання за рахунок рознесення термінації інтерфейсу користувача та інтерфейсу менеджменту на різному устаткуванні;

- у вузлових комутаторах створено 3 інтерфейси (рис. 4.4), на які можна віддалено потрапити, і у разі ненормальної активності в сегменті можна буде швидко локалізувати проблему, сегмент в середньому складається з 15-20 будинків;

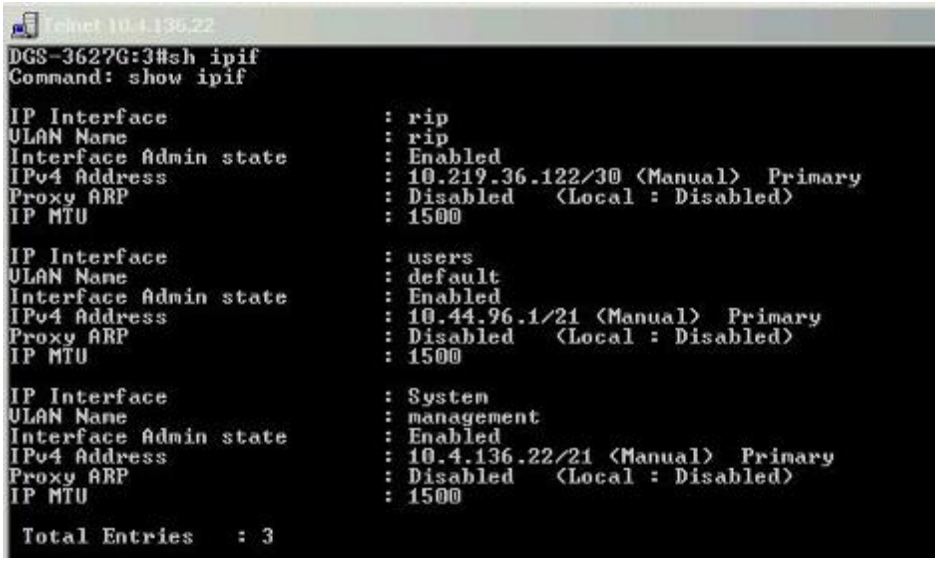

Рисунок 4.4 - Інтерфейси обладнання

- трафік між користувачами маршрутизується безпосередньо на вузлових комутаторах та не завантажує граничний маршрутизатор. Також для рівномірності завантаження з граничного маршрутизатора перенесено DHCP сервер у дата-центр компанії;

- мережа підготовлена до зростання клієнтської бази, введення в експлуатацію нового сервісу IPTV, розширено канал до 2 Гбіт/с, що дозволить збільшити швидкість на клієнтських тарифах.

ВИСНОВКИ

У даній кваліфікаційній роботі проведено огляд сучасних технологій побудови локальних обчислювальних мереж, розглянуті основні методи адміністрування та роботи з трафіком у мережі. Проаналізовано основні етапи, що необхідно реалізувати для оптимізації мережі при введенні нових сервісів.

В результаті проектування було здійснено успішне впровадження технології VLAN.

Завдяки даній технології завантаженість поточного обладнання значно знизилася, з'явилися перспективи масштабування користувацьких сервісів. Так із використанням технології VLAN став можливий запуск таких сервісів як IPTV (цифрове телебачення), VoIP (телефонія), з'явилася можливість збільшення швидкості на клієнтських тарифах, за рахунок збільшення пропускної спроможності зовнішнього каналу зв'язку.

Підбиваючи підсумки всього вищесказаного, слід зазначити, що всі завдання, поставлені в технічному завданні, виконані. Оптимізація роботи мережі проведена успішно і ми отримали помітний потенціал для впровадження та розвитку сучасних сервісів на мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. М. Гук «Аппаратные средства локальных сетей.» Энциклопедия - СПб.: Питер, 2004 г. – 573 с.

2. Дж. Скотт Хокдал «Анализ и диагностика компьютерных сетей.» - М.: Лори, 2001 г. – 353 с.

3. М. Величко Технологии строительства сетей доступа // LightWave Russian Edition, №3, 2005. – С. 31-33.

4. Олифер В. Г., Олифер Н. А. Компьютерные сети: принципы, технологии, протоколы. – Учебник для ВУЗов, СПб.: 2004. – 864 с.

5. СКС [Электронный ресурс] Режим доступа: www/ URL: http:// www.myshared.ru/ - 01.11.2022 г. - Загл. с экрана.

6. Поляк-Брагинский «Обслуживание и модернизация локальных сетей.» - Питер, 2005 г. – 546 с.

7. Терри Джонсон. Модернизация и ремонт сетей. – М.: Диалектика-Вильямс, 2000. – 944 с.

8. Сергеев А.П. Офисные локальные сети. Самоучитель [Текст] / А.П. Сергеев. - М.: Вильямс, 2003. – 323 с.

9. http://www.dlink.ru/products/index.php Технические характеристики оборудования фирмы dlink.

10. Дансмор Брэдли, Скандьер. Справочник по телекоммуникационным технологиям. – М.: Диалектика-Вильямс, 2003. – 640 с.

11. Амато, Вито. Основы организации сетей Cisco, том 1, Пер. с англ. – М.: Издательский дом “Вильямс”, 2004. – 512 с.

12. Шиндер Дебра. Основы компьютерных сетей. – М.: Диалектика-Вильямс, 2002. – 656 с.