Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

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

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Розробка заходів безпеки мережі FTTB в житловому районі міста
(тема)

Виконав:
здобувач *4* року навчання,
групи *ТРІМІиз-21-1*
Тахмазлі Турал Рафік огли
(власне ім'я, прізвище)

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. Наталія Харченко*
(посада, власне ім'я, прізвище)

Допускається до захисту
Завідувач кафедри _____ *Валерій БЕЗРУК*
(підпис) (власне ім'я, прізвище)

2025 р.

Не містить відомостей заборонених до відкритого публікування.

Студент / Тахмазлі Турал Рафік огли /

Керівник / Наталія Харченко /

Харківський національний університет радіоелектроніки

Навчально-науковий центр заочної форми навчання
Кафедра *Інформаційно-мережної інженерії*
Рівень вищої освіти *перший (бакалаврський)*
Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)
Тип програми *освітньо-професійна*
Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«____»_____ 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Тахмазлі Туралу Рафіку огли*
(прізвище, ім'я, по батькові)

1. Тема роботи *Розробка заходів безпеки мережі FTTB в житловому районі міста*

затверджена наказом університету від 02 травня 2025 р. № 63 Стз

2. Термін подання здобувачем роботи до екзаменаційної комісії 24 червня 2025 р.

3. Вихідні дані до роботи *Провести планування мультисервісної мережі м. Чернівці. За основу взяти проєкт реального розташування оптичних кілець міста, зокрема ділянки ОК-6 та будинків, що розташовані на вул. Центральній. Дослідити принципи побудови та архітектуру мультисервісної мережі побудованої на базі FTTB. Розробити комплексну схему захисту для мережі на рівні доступу та рівні агрегації. Для розробки проєкту та дослідження принципів налаштувань системи захисту скористатися програмним пакетом Cisco Packet Tracer. Обрати необхідне обладнання для побудови мережі.*

.

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Огляд принципів побудови та технологій мультисервісних мереж
2. Розробка структурної схеми широкосмугового доступу
3. Вибір обладнання для проектованої мережі
4. Моделювання мережі у програмному пакеті Cisco Packet Tracer
5. Ідентифікація користувача за MAC-адресою на рівні доступу
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; архітектура мультисервісної мережі; структурна схема мультисервісної мережі м. Чернівці; схема мережі на базі FTTB; схема фізичного розміщення оптичного кільця ОК-6; вибір обладнання для мережі; розподіл адресного простору і VLAN у мережі; логічна схема мережі; розробка VLAN; конфігурування та маршрутизація комутатора рівня агрегації; забезпечення безпеки мережі; висновки*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*02.05.25*	*виконано*
2	*Підбір літератури за темою роботи.*	*03.05-03.06.25*	*виконано*
3	*Огляд принципів побудови та технологій мультисервісних мереж*	*04.06-06.06.25*	*виконано*
4	*Розробка структурної схеми широкосмугового доступу*	*07.06-09.06.25*	*виконано*
5	*Вибір обладнання для проектованої мережі*	*10.06-12.06.25*	*виконано*
6	*Моделювання мережі у програмному пакеті Cisco Packet Tracer*	*13.06-15.06.25*	*виконано*
7	*Ідентифікація користувача за MAC-адресою на рівні доступу*	*16.06-20.06.25*	*виконано*
8	*Оформлення презентаційного матеріалу, підготовка до захисту в ЕК*	*21.06-26.06.25*	*виконано*

Дата видачі завдання _02_ ___травня__ 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ доц. Наталія Харченко
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка 77 с., 10 рис., 1 табл., 11 джерел, 3 додатки.

Об'єкт дослідження – мультисервісна мережа району міста.

Мета роботи – розробка заходів безпеки мережі FTTB в житловому районі міста.

Мультисервісні мережі набувають все більшої популярності, критично важливим стає їх професійна розробка та надійний захист. Ефективність функціонування такої мережі безпосередньо залежить від якості її проєктування та дієвості системи безпеки. Тому в роботі було розроблено проєкт мультисервісної мережі та запропоновано комплексну схему захисту для оптичного кільця в житловому районі ОК-6 міста Чернівці.

Для перевірки працездатності мережі було створено її модель у програмі Packet Tracer. Крім того, розроблено дворівневу систему безпеки, що включає:

- ідентифікацію користувачів за MAC-адресою на рівні доступу;
- ідентифікацію користувачів за IP-адресою на рівні агрегації.

ЛОКАЛЬНА МЕРЕЖА, METRO ETHERNET, VLAN, ОПТИЧНЕ КІЛЬЦЕ, MAC-АДРЕСА, ACL.

THE ABSTRACT

Explanatory slip 77 p., 10 fig., 1 tab., 11 sources, 3 attach.

Object of research - multi-service network of the city district.

The purpose of the work - development of security measures for the FTTB network in a residential area of the city.

Multiservice networks are becoming increasingly popular, and their professional design and reliable protection are becoming critical. The efficiency of such a network directly depends on the quality of its design and the effectiveness of the security system. Therefore, in this paper, we developed a multiservice network design and proposed a comprehensive protection scheme for an optical ring in the residential area OK-6 of Chernivtsi.

To test the network's performance, we created its model in Packet Tracer. In addition, a two-level security system was developed, including:

- user identification by MAC address at the access level;
- user identification by IP address at the aggregation level.

LOCAL AREA NETWORK, METRO ETHERNET, VLAN, OPTICAL RING, MAC ADDRESS, ACL.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ACL – Access Control List – список контролю доступу;

BRAS – Broadband Remote Access Server – сервер широкосмугового віддаленого доступу;

IP – Internet Protocol – набір правил і стандартів, які керують маршрутизацією даних в мережі;

IPTV – Internet Protocol Television – Інтернет-протокольне телебачення;

FTTB – Fiber to the Building – волокно до будівлі;

QoS – Quality of Service – якість надання послуг;

SLA – Service Level Agreement – договір про рівень (якість) наданих послуг мережею;

VLAN – Virtual Local Area Network – віртуальна локальна мережа;

WRR – Weighted Round Robin – зважений циклічний перегляд - це алгоритм планування в мережах, який розподіляє ресурси між різними потоками даних;

ВД – вузол доступу;

ВОЛЗ – волоконно-оптична лінія зв’язку;

ОК – оптичне кільце.

ВСТУП

У світі, де телекомунікації розвиваються стрімко, суспільство постійно рухається до збільшення складності відносин між різними секторами виробництва та зростання обсягів інформаційних потоків у різноманітних сферах, включаючи технічну, наукову, політичну, культурну та побутову. Станом на сьогодні очевидно, що жодна діяльність у сучасному суспільстві не може обійтися без обміну інформацією, для передачі якої застосовуються різноманітні засоби та системи зв'язку.

Сьогоднішній розвиток телекомунікаційних мереж спрямований на розширення ринку мультисервісних послуг, введення в експлуатацію новітніх телекомунікаційних та інформаційних технологій та їх конвергенцію.

Послуга широкосмугового доступу до Інтернету стала однією з найбільш успішних у сфері телекомунікацій недавно, і за кілька років кількість її користувачів зросла до 200 млн., причому більшість з них наразі користуються Інтернетом через комп'ютер або ноутбук.

Широкосмуговий доступ до Інтернету з'явився в Європі менше ніж десять років тому. Тоді швидкість у 256 кбіт/с вважалася високою. Нині ж швидкість у 100 Мбіт/с є фактичним стандартом для широкосмугового доступу.

З іншого боку, на початкових етапах розвитку Інтернету не було великої потреби у високій пропускній спроможності, оскільки існуючі програми не вимагали великої швидкості передачі даних. Важливим фактором у розвитку технологій широкосмугового доступу є потреба ринку в економічно вигідному забезпеченні користувачів більшою пропускною спроможністю та швидкістю реакції. Зараз, коли середній обсяг даних на користувача в місяць оцінюється від 2 до 7 Гбайт і продовжує зростати завдяки популярності файлообмінних сервісів, онлайн-ігор та відео, ця потреба є дуже актуальною.

Основною причиною для подальшого удосконалення широкосмугових мереж є послуги IPTV, які вимагають значного збільшення пропускної спроможності для передачі HD-відео.

У контексті масової інформатизації сучасного суспільства знання морально-етичних норм та правових основ використання новітніх інформаційних технологій у повсякденному житті набуває все більшої

важливості. Яскравими прикладами, що демонструють необхідність захисту інформації та забезпечення інформаційної безпеки, є випадки комп'ютерних атак на банки, зростання комп'ютерного піратства та поширення вірусів.

Кількість комп'ютерних злочинів збільшується, а також зростають обсяги комп'ютерних зловживань.

Основною причиною втрат, пов'язаних з комп'ютерами, є низький рівень обізнаності в області безпеки.

Під інформаційною безпекою розуміється захист інформації від випадкових або умисних впливів, які можуть завдати шкоди власникам або користувачам цієї інформації.

Метою інформаційної безпеки є захист цінностей системи, забезпечення точності та цілісності інформації та мінімізація ризиків її пошкодження або втрати.

У практичному аспекті найважливішими є три складові інформаційної безпеки:

- доступність (здатність отримати необхідну інформацію в короткі терміни);

- цілісність (захист від пошкодження та несанкціонованих змін);

- конфіденційність (захист від неавторизованого доступу).

Крім того, важливо, щоб використання інформаційних систем відбувалося відповідно до діючого законодавства. Це правило є загальним для будь-якої діяльності, але для інформаційних технологій воно особливо важливе через їх швидкий розвиток. Законодавство часто не встигає за потребами практики, що створює напруженість у суспільстві. Для інформаційних технологій таке відставання нормативної бази є особливо проблематичним.

Створення ефективного режиму інформаційної безпеки є складним завданням. Заходи щодо її вирішення можна поділити на чотири основні категорії:

- законодавча (закони, регулятивні документи, стандарти та інше);

- адміністративна (загальні дії, які проводяться керівництвом компанії);

- процедурна (специфічні заходи безпеки, пов'язані з персоналом);

- програмно-апаратна (спеціалізовані технічні рішення).

У даній кваліфікаційній роботі основна увага приділяється саме програмно-апаратним методам захисту.

Основною метою кваліфікаційної роботи є створення та забезпечення безпеки мережі широкосмугового доступу з використанням технології FTTB у житловому секторі міста. Робота включає створення моделі в емуляторі мережі передачі даних Cisco Packet Tracer, налаштування її роботи, захист комутаційних портів. Також передбачено розробку мережевих фільтрів, налаштування паролів, планування заходів фізичного захисту та визначення критеріїв для вибору обладнання.

1 ОГЛЯД ПРИНЦИПІВ ПОБУДОВИ ТА ТЕХНОЛОГІЙ МУЛЬТИСЕРВІСНИХ МЕРЕЖ

Об'єктом вивчення вибрана мультисервісна мережа широкосмугового доступу, і для основи проектованої мережі було обрано реальний робочий проект «Мультисервісна мережа широкосмугового доступу у м. Чернівці (Модернізація основної мережі доступу та ОК-5, ОК-6, ОК-8). Друга черга введення в експлуатацію об'єктів зв'язку - «Основне кільце», зона ОК-6» представляє собою універсальне багатофункціональне середовище, призначене для трансляції звуку, відео та даних за допомогою технології комутації пакетів (IP). Мультисервісна мережа характеризується високим рівнем надійності, типовим для телефонних мереж (на відміну від негарантованої якості зв'язку через Інтернет) та забезпечує низьку ціну передачі за одиницю обсягу інформації (порівнянну з вартістю передачі даних через Інтернет). Варто відзначити, що мультисервісні мережі – це не просто технологія або технічна концепція, а скоріше технологічна доктрина або новий погляд на сучасну роль телекомунікацій, заснований на переконанні в тому, що комп'ютери та дані сьогодні займають перше місце порівняно з голосовим зв'язком. Основними концептами мультисервісних мереж є QoS (Quality Of Service) та SLA (Service Level Agreement), а саме якість обслуговування та договір про рівень (якість) наданих послуг мережею. Перехід до нових мультисервісних технологій змінює саму концепцію надання послуг, коли якість забезпечується не тільки на рівні договірних зобов'язань з провайдером послуг та вимог дотримання стандартів, а й на рівні технологій та операторських мереж (рис. 1.1). Архітектуру мультисервісної мережі можна уявити як кілька ключових рівнів: ядро (основний рівень), рівень розподілу та агрегації та рівень доступу. Структура мультисервісної мережі м. Чернівці представлена на рис. 1.2.

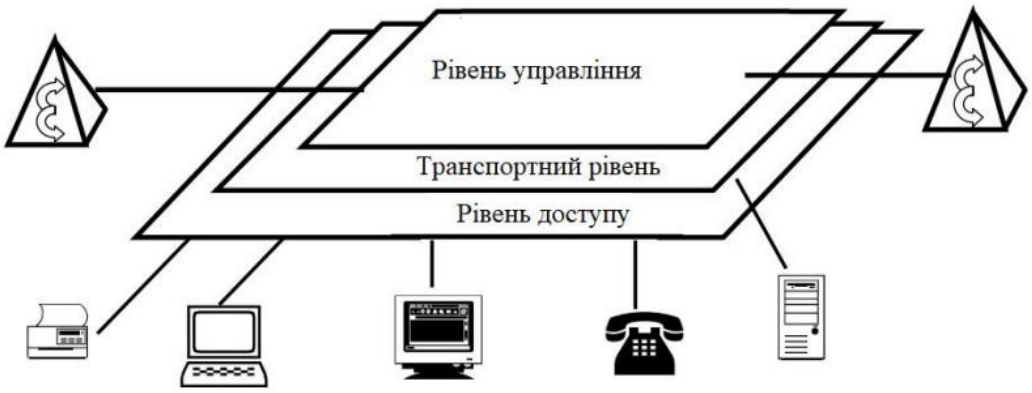


Рисунок 1.1 - Архітектура мультисервісної мережі

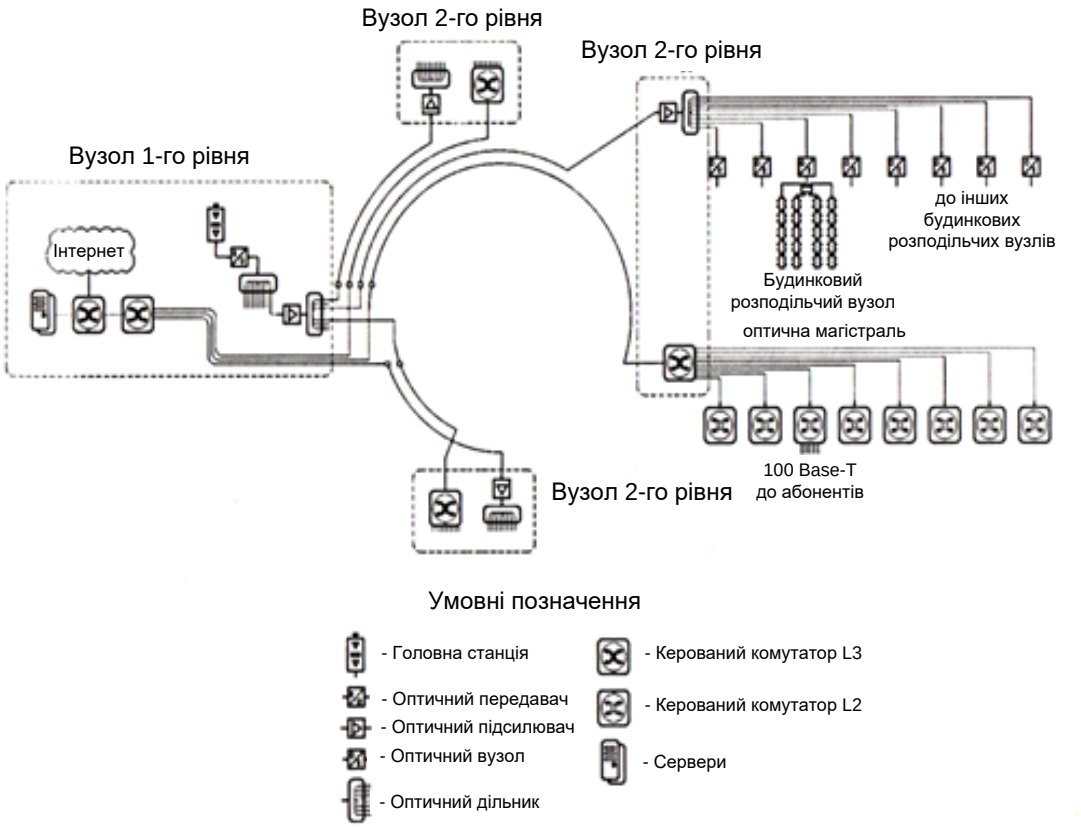


Рисунок 1.2 – Структурна схема мультисервісної мережі м. Чернівці

На рівні ядра розміщені високоефективні платформи для швидкого перемикання трафіку, що підтримують протоколи динамічної маршрутизації. Тут відбувається підключення до провайдерів і розміщення сервісних центрів. Магістральний рівень представляє собою універсальну високошвидкісну та, за можливості, однорідну платформу для передачі даних, створену на основі цифрових телекомунікаційних ліній [1].

Рівень розподілу охоплює вузлове обладнання мережі оператора, тоді як рівень агрегації займається агрегуванням трафіку з рівня доступу та його підключенням до магістральної (транспортної) мережі [1].

На рівні доступу здійснюється керування користувачами та робочими групами при доступі до ресурсів інтегрованої мережі. Рівень доступу включає корпоративні або внутрішньобудинкові мережі, а також комунікаційні канали, які забезпечують їх з'єднання з вузлами розподілу мережі [1].

1.1 Широкосмуговий доступ до Інтернет

Враховуючи вимоги замовника та особливості робочого проекту, які включають не тільки надання доступу до інтернету, але й ряд інших послуг, потрібно включити декілька обов'язкових вимог до проектованої мережі.

Основною вимогою до мереж є забезпечення можливості доступу до ресурсів усіх комп'ютерів, що входять до складу мережі.

Мультисервісна мережа, що розробляється, має надавати наступні зв'язкові послуги [1]:

- широкосмуговий доступ до мережі Інтернет дозволяє користувачам доступатися до інформаційних ресурсів глобальної мережі, використовувати віддалені файлові ресурси, обмінюватися великими обсягами даних, користуватися електронною поштою, месенджерами (Skype, Google Meet) та іншими онлайн-сервісами;

- IP телефонія – це метод надання телефонних послуг через мережі з пакетною комутацією, включаючи IP мережі передачі даних та Інтернет;

- IPTV – це сучасне цифрове інтерактивне телебачення. Завдяки IPTV плеєру можна дивитися понад 100 телеканалів без потреби в додатковому обладнанні.

Технічні вимоги до характеристик основних з'єднань мережі включають [1]:

- швидкість обміну інформацією – 10 Гбіт/с;

- автоматичне виявлення та діагностика виникаючих несправностей;

- підтримка QoS;

- мінімальна ймовірність втрати даних;

- коефіцієнт екранування використовуваних кабелів має бути не менше 80 дБ у діапазоні 30 - 1000 МГц.

Технічні вимоги до системи передачі даних:

- мережа передачі даних має бути розроблена з урахуванням технології Ethernet та протоколу IP;

- швидкість підключення будівлі до мережі передачі даних має становити не менше 100 Мбіт/с;

- пропускна здатність основної мережі передачі даних має бути не менше 1000 Мбіт/с;

- інтерфейс підключення абонента через UTP - Ethernet 10/100Base-T.

Для досягнення визначених цілей найкраще використовувати технологію широкосмугового доступу.

Широкосмуговий або високошвидкісний доступ до Інтернету надається за допомогою технологій, що дозволяють користувачам обмінюватися даними у значно більших обсягах і з вищою швидкістю, порівняно зі звичайним доступом через телефонні лінії. Це забезпечує не тільки високу швидкість передачі даних, але й постійне з'єднання з Інтернетом без необхідності комутованого з'єднання, а також «двосторонній» зв'язок, тобто можливість як завантажувати, так і відправляти інформацію з високою швидкістю [2].

Широкосмуговий доступ не лише забезпечує різноманіття інформаційного контенту та послуг, але й має потенціал радикально змінити весь Інтернет, як у плані сервісів, що пропонуються мережею, так і у способі їх використання. Безсумнівно, ми ще маємо відкрити багато майбутніх застосувань широкосмугового доступу, які дозволять використати його технологічний потенціал на повну [2].

Для забезпечення широкосмугового доступу до Інтернету існує багато різноманітних носіїв і технологій передачі даних. Серед них - кабельний зв'язок, цифрова абонентська лінія (DSL), супутниковий зв'язок, фіксований бездротовий доступ та інші. Попри те, що багато установ і комерційних організацій уже мають доступ до широкосмугового Інтернету, проблема "останньої милі" - забезпечення доступу до домівок користувачів - залишається невирішеною. В даний час конкуруючі телекомунікаційні компанії розробляють, впроваджують і просувають специфічні технології та послуги для надання широкосмугового доступу широким верствам населення.

Термін "широкосмуговий доступ" вживається для позначення постійного та швидкісного з'єднання з Інтернетом. Але широкосмуговий доступ означає не лише високу швидкість передачі даних, але й унікальний спосіб використання глобальної мережі. Користувачі широкосмугового доступу можуть в будь-який момент отримувати або відправляти великі обсяги інформації, включаючи кольорові зображення, аудіо- та відеокліпи, анімацію, телевізійний контент і багато іншого. Широкосмуговий доступ надає користувачам доступ до найновіших послуг, незалежно від місця підключення. Власники широкосмугового доступу отримують більше можливостей для використання мультимедійних послуг та інформаційного забезпечення свого бізнесу, включаючи файлообмін, відеоконференції, ігри, системи безпеки, телефонні та банківські послуги та інше. Все це стало можливим завдяки сучасним мережам широкосмугового доступу [2].

Широкосмуговий доступ також сприяє появі нових сфер діяльності та збагаченню існуючих. Він стимулює економічне зростання, відкриває нові можливості для інвестицій та працевлаштування.

Широкосмуговий доступ відіграє ключову роль у забезпеченні сталого розвитку віддалених та сільських районів, стаючи важливим елементом підтримки місцевої влади у створенні привабливих умов для бізнесу, наданні населенню віддалених районів можливості для дистанційної роботи, доступу до висококваліфікованих медичних послуг, підвищення освітнього рівня та участі у суспільному житті [2].

1.2 Технології мультисервісних мереж

У розробку мережі доступу інвестуються значні кошти - від 50% до 80% загального бюджету, тому вибір відповідних технологій та методів організації мережі є критично важливим. Ось деякі критерії, які впливають на вибір технології доступу для користувачів:

- ціна підключення на одного користувача;

- легкість підключення - аспект, що впливає на можливість швидкого залучення користувачів до мережі;

- достатній рівень пропускної спроможності або швидкості передачі даних для задоволення потреб користувача;

- забезпечення високої якості обслуговування для клієнтів;

- наявна кабельна інфраструктура - це може бути коаксіальний кабель, вита пара, телефонні лінії, оптичні волокна тощо.

На етапі проектування було обрано технологію абонентського доступу FTTB, оскільки вона задовольняє всі вищезазначені критерії і є найбільш придатною для досягнення поставлених цілей.

Технологія Fiber To The X (Оптичне волокно до…) представляє собою загальний метод організації кабельної інфраструктури мережі доступу, де оптоволокно прокладено від вузла зв'язку до певної точки (точка «х»), а звідти до користувача може йти мідний кабель (або ж оптика може бути прокладена прямо до кінцевого обладнання користувача) [3].

Отже, FTTx стосується лише фізичного рівня мережі. Проте, цей термін також охоплює широкий спектр технологій канального та мережевого рівнів. Завдяки великій пропускній спроможності систем FTTx, з'являється можливість надання широкого спектру нових послуг.

До родини FTTx відносяться різноманітні архітектурні рішення [3]:

FTTN (Fiber to the Node) – волокно до мережного вузла;

FTTC (Fiber to the Curb) – волокно до мікрорайону, кварталу або групи будинків;

FTTB (Fiber to the Building) – волокно до будівлі;

FTTH (Fiber to the Home) – волокно до житла (квартири або окремого котеджу).

Експерти одностайно підтримують рішення на користь FTTH, аналізуючи тривалість інвестиційного циклу та збільшення потреб у пропускній спроможності доступових каналів. Вони вказують, що якщо сьогоднішні технічні рішення для сегменту доступу не зможуть забезпечити швидкість у 100 Мбіт/с обладнання морально застаріє до завершення циклу інвестицій. Перевагами FTTB є [3]:

- серед усіх опцій FTTx вона пропонує найширшу пропускну здатність;

- цей варіант є повністю стандартизованим і має найбільший потенціал;

- FTTB дозволяє обслуговувати велику кількість абонентів на відстані до 20 км від комунікаційного вузла;

- ці рішення дозволяють значно знизити експлуатаційні витрати завдяки зменшенню площі технічних приміщень, потреби в енергії та витратах на технічне обслуговування.

Існують два основних підходи до організації мереж FTTB: з використанням технології Ethernet та на основі технології PON.

Технологія Gigabit Ethernet, яка є розвитком IEEE 802.3 Ethernet, використовує ту саму структуру пакетів, формат, підтримку протоколу CSMA/CD, повний дуплекс, контроль потоку тощо, але забезпечує теоретично в десять разів вищу продуктивність. Завдяки сумісності з Ethernet 10 Mbps та 100 Mbps, перехід на Gigabit Ethernet можливий без значних інвестицій у програмне забезпечення, кабельну інфраструктуру та навчання персоналу [3].

Як і у випадку з Fast Ethernet, Gigabit Ethernet не має єдиної схеми кодування сигналів. Для стандартів 1000Base-LX/SX/CX використовується кодування 8B/10B, а для стандарту 1000Base-T - спеціальний розширений лінійний код TX/T2. Кодування здійснюється на рівні PCS, який розташований нижче інтерфейсу GMII, незалежного від середовища. 1000Base-T є стандартним інтерфейсом Gigabit Ethernet для передачі через неекрановану кручену пару категорії 5 і вище на відстань до 100 метрів. Використовуються всі чотири пари мідного кабелю, зі швидкістю передачі 250 Мбіт/с по кожній парі. Стандарт передбачає дуплексну передачу даних, з одночасною передачею в обох напрямках по кожній парі - подвійний дуплекс (dual duplex) [3].

1.3 Технологія абонентського доступу FTTB

На даний момент, однією з найпопулярніших технологій для створення широкосмугових мереж в Україні є FTTB (Fiber to the Building - оптичне волокно до будівлі). Її широке розповсюдження обумовлене падінням вартості оптичного кабелю (ОК), появою недорогих оптичних приймачів, передавачів та оптичних підсилювачів (ОП). Застосування оптичних технологій у FTTB дозволяє використовувати швидкісну технологію Metro Ethernet для передачі даних, уникає необхідності заземлення несучого троса, знижує ризик поломки обладнання через статичну електрику та спрощує процес узгодження мережі з контролюючими органами [3].

Мережа FTTB, створена з використанням цієї технології, складається з двох окремих мереж: одна для надання послуг аналогового кабельного телебачення, інша - для передачі даних. Їх об'єднує використання різних оптичних волокон у тих же ОК на ділянках магістралі та в розподільчих мережах вузлів другого рівня. На відміну від DOCSIS, у FTTB вся апаратура строго спеціалізована: або для передачі ТБ, або для передачі даних, тому поломка одного типу обладнання не впливає на роботу іншого [3].

Сучасні оптоволоконні мережі доступу розробляються на основі різноманітних архітектур і технологій. Добре продумані стандарти цих технологій та доступність необхідного обладнання забезпечують розгортання мереж сервіс-провайдерами без значних ризиків. Їх успішна діяльність слугує стимулом для активного розвитку цього сектора. Можна з впевненістю стверджувати, що конкуренція з боку таких мереж спонукатиме великих телекомунікаційних операторів інвестувати в оптоволоконні мережі доступу [3].

Топологія мережі, створеної за технологією FTTB, представлена у додатку А.

Ця топологія значною мірою відтворює гібридну волоконно-коаксіальну мережу і включає вузол передачі даних, магістральну волоконно-оптичну лінію зв'язку (ВОЛЗ) та розподільчу мережу.

Особливість FTTB полягає в заміні оптичних вузлів на «вузли другого рівня» (підсилювальні пункти) та заміні кабелю розподільчих мереж з коаксіального на оптичний. Головна станція та будинкова розподільна мережа залишаються без змін під час модернізації, а для магістралі може знадобитися лише додавання оптичних волокон. Таким чином, у мережах FTTB збільшується кількість прокладених оптоволокон та встановлених оптичних приймачів.

2 РОЗРОБКА СТРУКТУРНОЇ СХЕМИ ШИРОКОСМУГОВОГО ДОСТУПУ

2.1 Загальні принципи побудови будинкової мережі Ethernet

Основа стратегії розгортання мережі полягає у широкому застосуванні оптичного зв'язку, окрім ділянки мережі, що розташована безпосередньо в приміщенні абонента. Доступність оптичних кабелів, різноманітні методи їх укладання, здатність забезпечити стабільну та імунну до перешкод передачу даних, широкий спектр підтримуваних швидкостей, що забезпечує довготривале використання, роблять інвестиції в оптичні лінії зв'язку привабливими та дозволяють створювати на їх основі мережі операторського рівня [1].

Для забезпечення стабільності, можливості розширення та управління мережею, з перспективою надання широкого асортименту послуг із забезпеченням потрібної якості обслуговування, Виконавець рекомендує стратегію, за якою домашня мережа організована за ієрархічним принципом.

Перерахуємо ці рівні:

- рівень доступу;
- рівень агрегації;
- рівень надання послуг (сервісний рівень);
- рівень магістралі.

Розглянемо їхнє призначення.

Рівень доступу.

Як можна зрозуміти з назви, це забезпечення фізичного з'єднання абонента з мережею. Загалом, технології доступу поділяють на три основні категорії: дротові, кабельні та бездротові. Дротові технології включають мережі xDSL, PON та Ethernet. У цій кваліфікаційній роботі ми зосереджуємось на Ethernet-доступі, але з точки зору мережевої архітектури, тобто впорядкування VLAN, логічного підключення абонентів, забезпечення резервування та інше, всі види дротових (і навіть бездротових) мереж доступу мають багато спільного. Таким чином, багато принципів можна застосувати і до інших технологій доступу [1].

На цьому етапі розміщені комутатори, до яких абоненти підключаються безпосередньо (або через абонентське обладнання) за допомогою внутрішньобудинкового мідного кабелю категорії 5. Для забезпечення більшості послуг на цьому рівні достатньо використовувати керовані комутатори 2 рівня. Підключення до квартальних комутаторів відбувається через оптичне волокно зі швидкістю 1 Гбіт/с або 100 Мбіт/с, залежно від потреб послуг.

Топологія підключення має форму «кільця». Комутатори на рівні під'їзду/будинку (так само як і квартальні комутатори) зазвичай встановлюються у закриваючихся приміщеннях, підвалах чи на горищах будівель. Варто зазначити, що квартальний комутатор і комутатори на рівні під'їзду/будинку, розташовані в одній будівлі, можуть підключатися за допомогою мідного кабелю.

Рівень агрегації.

Його місія – забезпечення з'єднання між рівнем доступу та ядром мережі через рівень надання послуг.

Розміри мережі агрегації можуть варіюватися в залежності від кількості користувачів та наявності оптичної інфраструктури, зазвичай охоплюючи велике місто або регіон. Ця мережа може бути реалізована повністю на другому рівні моделі OSI (рис. 2.1).

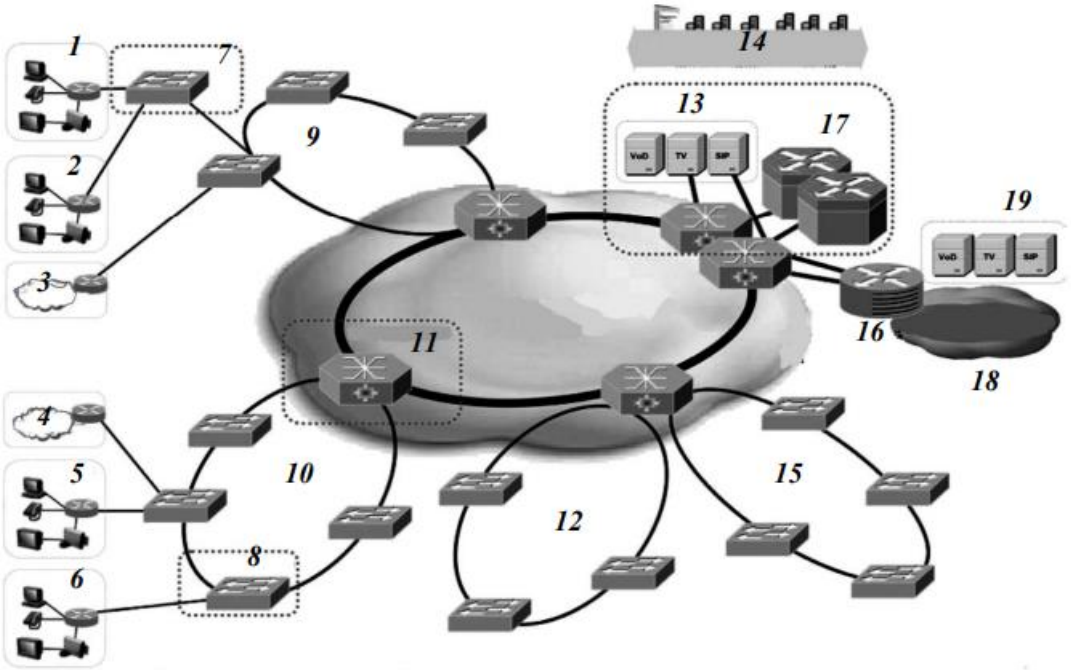
Агрегаційний рівень включає в себе районні комутатори 3-го рівня маршрутизації, які під'єднуються до найближчого вузла магістральної мережі. Підключення відбувається зі швидкістю 1 Гбіт/с за допомогою Ethernet. Районні комутатори можуть з'єднуватися з комутатором магістральної мережі (у цьому випадку з Центральним) за допомогою топологій «зірка» або «кільце» [1].

Сервісний рівень.

Функція сервісного рівня полягає у передачі трафіку та наданні сервісів, за які сплачує абонент. На цьому рівні відбувається аутентифікація та авторизація користувача, визначення доступних йому сервісів. Потім обладнання сервісного рівня забезпечує дотримання умов договору з абонентом, наприклад, обмеження швидкості доступу до Інтернету до договірних параметрів; тут же формується статистика для розрахунків з абонентом або контроль за використанням послуг абонентами з передоплатою.

На сервісному рівні створюється концепція абонентської сесії, яка є свого роду «віртуальним мережним інтерфейсом» для зв'язку з абонентом, та відбувається видача IP-адрес.

Власне, на рівні IP-протоколу користувач взаємодіє безпосередньо з сервісним рівнем.



1, 2, 5, 6 – квартира; 3, 4 – бізнес-корпорація; 7, 8 – вузол доступу; 9, 10, 12, 15 – рівень доступу Ethernet; 11 – вузол агрегації; 13 – місцевий контент; 14 – управління послугами/політиками; 16 – граничний маршрутизатор; 17 – сервісний рівень; 18 – рівень магістралі; 19 – глобальний контент

Рисунок 2.1 – Загальна архітектура мережі широкосмугового доступу рівня агрегації

Рівень магістралі.

Рівень магістралі створено для ефективної та безпечної передачі даних на великі відстані. В основному, магістраль з'єднує міські мережі агрегації, розташовані у різних населених пунктах. У випадку, коли оператор обслуговує мережу лише в одному місті чи регіоні, магістральний рівень може бути неявним, фактично представляючи собою з'єднання з більш великим магістральним провайдером [1].

Магістральний рівень (або основна мережа) включає Головний вузол та, за потреби, додаткові вузли, що з'єднані між собою за допомогою надійного високошвидкісного Ethernet зв'язку (1 Гбіт/с, N x 1 Гбіт/с або 10 Гбіт/с). В

основі вузлів основної мережі лежать гігабітні Ethernet комутатори з маршрутизацією на 3 рівні [1].

Оглянути детальну схему архітектури для широкосмугового доступу можна в додатку Б.

За даними схеми (рис. 2.1), мережева топологія організована у формі "кільця"

В цій роботі будуть детально розглянуті два основні рівні широкосмугових мереж доступу: рівень доступу та агрегаційний рівень, що об'єднані в єдине оптичне кільце.

2.2 Основні напрямки проектування мережі FTTx

Загальний обсяг мережних портів FTTx згідно з технічними вимогами проекту на ОК-6 складає 6216 портів.

Рівень доступу формують комутатори доступу (комутатори в будинках), які є керованими пристроями без можливості маршрутизації (L2). Ці комутатори підключені за допомогою кільцевої схеми розподілу. Функціонал комутаторів дозволяє забезпечити з'єднання зі швидкістю 1000 Мбіт/с. Порти для каскадування гігабітного Ethernet забезпечують з'єднання між комутаторами доступу та крайні комутатори підключаються до комутаторів агрегації через оптичні гігабітні інтерфейси у формі кільця.

Інтерфейси користувачів налаштовуються в режимі «access» у окремому VLAN для забезпечення ізоляції користувачів, підключених до різних комутаторів доступу в межах одного кільця.

Для обчислення встановленої потужності вузла доступу (ВД) в робочому проекті застосовується принцип 40% проникнення, а саме з 24 портів Fast Ethernet на кожні 108 квартир. У під'їздах, де кількість квартир перевищує 108, монтується комутатор на 48 портів. Кількість комутаторів у кільці доступу трохи перевищує 10 одиниць.

В будинках до 5 поверхів включно вузли доступу розміщуються з розрахунку один ВД на 4 під'їзди.

В будинках від 6 до 11 поверхів включно вузли доступу розміщуються з розрахунку один ВД на 2-3 під'їзди.

В будинках з кількістю поверхів понад 11 вузли доступу розміщуються з розрахунку один ВД на кожен під'їзд.

В роботі будемо розглядати одне оптичне кільце представлене на рис. 2.2.

А саме кільце, в яке входять будинки за адресами:

- вул. Центральна 45;
- вул. Центральна 47;
- вул. Центральна 51;
- вул. Центральна 53;
- вул. Центральна 55;
- вул. Центральна 57.

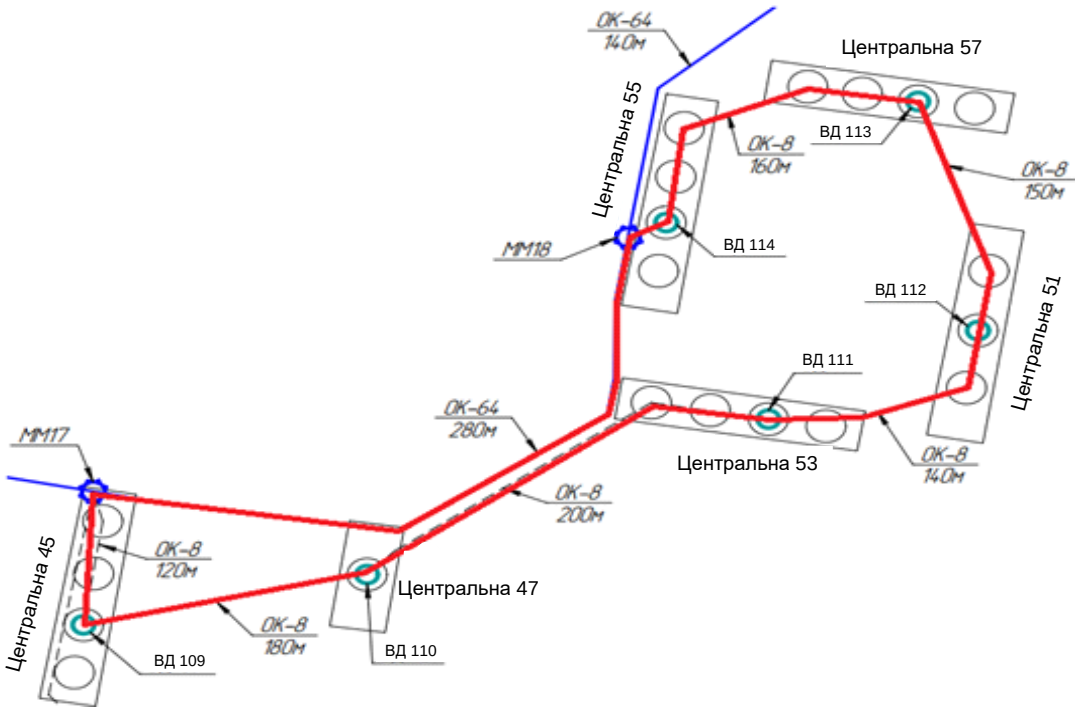


Рисунок 2.2 - Схема фізичного розміщення оптичного кільця ОК-6

3 ВИБІР ОБЛАДНАННЯ ДЛЯ ПРОЕКТОВАНОЇ МЕРЕЖІ

Мережеві пристрої класифікуються на пристрої основної мережі та пристрої рівня доступу.

До пристроїв основної мережі відносяться агрегатні комутатори.

До пристроїв мережі доступу входять: комутатори доступу.

Виходячи з вимог до проектування мережі, підберемо необхідний набір елементів обладнання.

3.1 Вибір обладнання рівня доступу

Основними аспектами вибору техніки в цьому випадку слугують:

- можливість підключення комутаторів доступу через оптоволоконні кабелі та присутність FSP модулів;
- комутатор L2;
- підтримка функцій VLAN 1:1;
- покращені функції безпеки.

Враховуючи баланс ціни та якості, було вирішено застосовувати комутатори доступу:

- LS-S2326TP-E1 виробництва фірми "HUAWEI" Technologies Co, Ltd;
- LS-S2352TP-E1 виробництва фірми «HUAWEI» Technologies Co, Ltd.

Комутатори LS-S2326TP-E1/LS-S2352TP-E1 - керований комутатор 2/4 рівня представлений на рис. 3.1.

Рисунок 3.1 - Зовнішній вигляд комутатора S2326 TP-PWR-E1

Опис: комутатор LS-S2326TP-E1/LS S2352TP-E1 - L2/L4 рівня має 24/48 портів них 24/48 портів 10/100BASE-TX і 2/4 комбінованих порту - 1000Base-T/SFP slot, що дозволяють використовувати гіга канал із застосуванням додатково SFP модуля [4].

Конфігурація портів комутаторів [4]:

- 24/48 порту 10/100Base-TX;

- 2/4 комбінованих порту – 1000Base-T/SFP slot;
- 1 порт RS232.

Характеристики серії S2300: управління послугами на базі VLAN.

Серія комутаторів S2300 підтримує широкий спектр стратегій ACL, дозволяючи застосовувати правила ACL через різні інтерфейси VLAN. Це дозволяє ефективно управляти інтерфейсами VLAN та оптимізувати ресурси. Модель S2300-EI забезпечує функціонал VLAN 1:1, що дозволяє надавати послуги IPTV без необхідності налаштування домашнього шлюзу. Також, S2300-EI підтримує VLAN переключення N:1, що є вкрай потрібним у цій сфері. Це дозволяє агрегувати VLAN на боці користувача, зменшуючи загальну кількість використовуваних VLAN. S2300-EI також підтримує технологію QinQ, при якій тег VLAN загальнодоступної мережі інкапсульований у пакет зовнішнього тега VLAN абонентської мережі, дозволяючи пакетам переносити 2 теги VLAN через операторську магістральну мережу [4].

Розширені можливості для багатоадресної розсилки

Комутатори з серії S2300 підтримують групи багатоадресної передачі та низку функцій для розповсюдження багатоадресної передачі на 2-му рівні, включно з IGMP snooping, фільтрацією IGMP, багатоадресною передачею VLAN та балансуванням навантаження через агрегацію портів. S2300 також забезпечує можливість обмеження швидкості та збору статистики багатоадресного трафіку на портах для задоволення потреб IPTV [4].

Характеристики QoS

Кожен інтерфейс у моделі S2300 обслуговує 4 черги з можливістю управління через WRR, SP та комбінований режим WRR+SP. Лінійка S2300 забезпечує детальну класифікацію трафіку, використовуючи VLAN, MAC-адресу, IP-адресу відправника/одержувача, пріоритет або порт, де запущено додатки. Ця серія також підтримує лімітування швидкості потоків та передачу даних з максимальною швидкістю для кожного порту. Це гарантує високу якість обслуговування для голосових та даних передач [4].

Переваги у сфері безпеки

S2300 пропонує широкий спектр захисних функцій для користувачів мережі: обширний набір правил ACL, прив'язку IP-адрес, MAC-адрес або портів, блокування MAC-адрес, ізоляцію портів, фільтрацію пакетів, обмеження кількості MAC-адрес, які може розпізнати порт, динамічне виявлення ARP, захист за допомогою HWTACACS, IEEE 802.1x та SSH [4].

Захист від блискавки

Серія S2300 використовує унікальний механізм захисту від перепадів напруги, розроблений Huawei. Комутатори цієї серії забезпечують захист від блискавки на рівні 6КВ без потреби у встановленні зовнішніх розрядників. Це дозволяє мінімізувати пошкодження від ударів блискавки навіть у складних умовах експлуатації [4].

Зручність у обслуговуванні та управлінні

Комутатори лінійки S2300 вирізняються легкістю в обслуговуванні та налаштуванні. Підтримується моніторинг стану обладнання в різних режимах. Крім того, S2300 підтримує HGMPv2, SNMP, NTP, SSHv2, HWTACACS+, RMON та збір статистики трафіку на VLAN портах. Серія S2300 пропонує зручні інструменти для обслуговування та управління, що спрощують адміністрування мережі. Це допомагає знизити OPEX та підвищити рентабельність S2300 [4].

3.2 Вибір комутатора рівня агрегації

Основним фактором для вибору техніки агрегаційного рівня є:

- комутатор L3 з можливістю маршрутизації;
- велика ефективність;
- здатність підключення доступних комутаторів через оптоволоконні кабелі та наявність FSP модулів.

Враховуючи баланс ціни та якості, було вирішено застосувати комутатор агрегації Cisco ME-4924 (рис. 3.2).

Рисунок 3.2 - Зовнішній вигляд комутатора Cisco ME-4924

Агрегаційний комутатор від провідного у світі виробника, що має 24 порти SFP 1000Base-X та 4 додаткові порти SFP 1000Base-X або 2 порти XFP з пропускною здатністю 10 Гбіт/с. Комутатори Cisco ME 4900 створені для постачальників послуг, які мають намір надавати послуги нового покоління, такі як відео та голос. Завдяки компактному розміру (висота - 1RU), його можна встановлювати в офісах з обмеженим простором для стійок. Комутатор Cisco ME 4924-10GE, призначений для агрегації, є комутатором Layer 2-4 U-PE для мереж з високою продуктивністю. Серія ME 4900 побудована на основі технологій серії 4900 і забезпечує продуктивність, яка потрібна телекомунікаційним операторам для надання послуг triple play своїм клієнтам. Комутатори Cisco ME 4900 створені для постачальників послуг, які мають намір надавати послуги нового покоління, такі як відео та голос [5].

Характеристики:

- висока продуктивність - 48 Гбіт/с та 71 мільйон пакетів за секунду;
- мінімальна затримка при комутації Layer 2-4;
- передові функції безпеки та QoS;
- роз’єми Gigabit Ethernet або 10 Gigabit Ethernet;
- за бажанням - вбудовані блоки живлення AC або DC з можливістю гарячого замінювання;
- система охолодження з можливістю гарячого замінювання та запасними вентиляторами.

4 МОДЕЛЮВАННЯ МЕРЕЖІ У ПРОГРАМНОМУ ПАКЕТІ CISCO PACKET TRACER

Packet Tracer – це інструмент для емуляції мереж, розроблений компанією Cisco Systems. Він дозволяє створювати робочі моделі мереж, конфігурувати маршрутизатори та комутатори за допомогою команд Cisco IOS, а також забезпечує можливість взаємодії між користувачами через хмарні сервіси. Підтримується робота з маршрутизаторами Cisco серій 1800, 2600, 2800 та комутаторами 2950, 2960, 3650. Також доступні сервери DHCP, HTTP, TFTP, FTP, робочі станції, різноманітні модулі для комп'ютерів і маршрутизаторів, пристрої WiFi та різні типи кабелів [6].

4.1 Розподіл адресного простору

Максимальна кількість абонентів становить 144. (Одне оптичне кільце).

На цій частині мережі для забезпечення оптимальної безпеки буде застосовано технологію VLAN 1:1 " VLAN для кожного абонента".

Серед її ключових переваг варто відзначити високий рівень ізоляції абонентів між собою по усій мережі доступу та агрегації. В цій схемі кожен абонент отримує власний присвоєний VLAN типу «точка-точка», нижче представлена таблиця розподілу адресного простору і VLAN (табл. 4.1).

Таблиця 4.1 - Розподіл адресного простору і VLAN у мережі

Комутатор	VLAN	IP-address	Mask
1	10	192.168.10.1	255.255.255.248
2	20	192.168.10.9	255.255.255.248
3	30	192.168.10.17	255.255.255.248
4	40	192.168.10.25	255.255.255.248
5	50	192.168.10.33	255.255.255.248
6	60	192.168.10.41	255.255.255.248

Максимальна кількість VLAN, яку можна налаштувати на кожному комутаторі, зазвичай залежить від кількості портів, доступних на цьому комутаторі. Враховуючи, що мережа є широкосмуговою, крім інтернет-послуг, можливе надання таких сервісів, як IP-телефонія та кабельне телебачення. Це

означає, що для обслуговування одного абонента може знадобитися більше ніж один порт на комутаторі [6].

4.2 Розробка мережі

Симульована мережа володіє низкою унікальних характеристик, а спосіб з'єднання в рамках одного оптичного кільця реалізовано через використання технології VLAN 1:1, що дозволяє впровадити досить ефективну і водночас просту схему захисту.

Варто підкреслити, що схема, представлена нижче, створена у спрощеній формі. Для кожного комутатора показано з’єднання лише одного користувача і налаштовано інтерфейси VLAN спеціально для одного абонента. Такий підхід до підключення абонентів ідеально демонструє ефективність роботи мережі в цілому.

Як відомо, структура мережі одного оптичного кільця включає в себе 6 комутаторів рівня доступу та один комутатор рівня агрегації.

У програмі Packet Tracer присутні аналогічні комутатори рівня доступу та агрегації.

Будемо використовувати 2960-24TT як комутатор рівня доступу та 3560-24PS як комутатор рівня агрегації.

На рис. 4.1 представлена схема, створена за допомогою Packet Tracer.

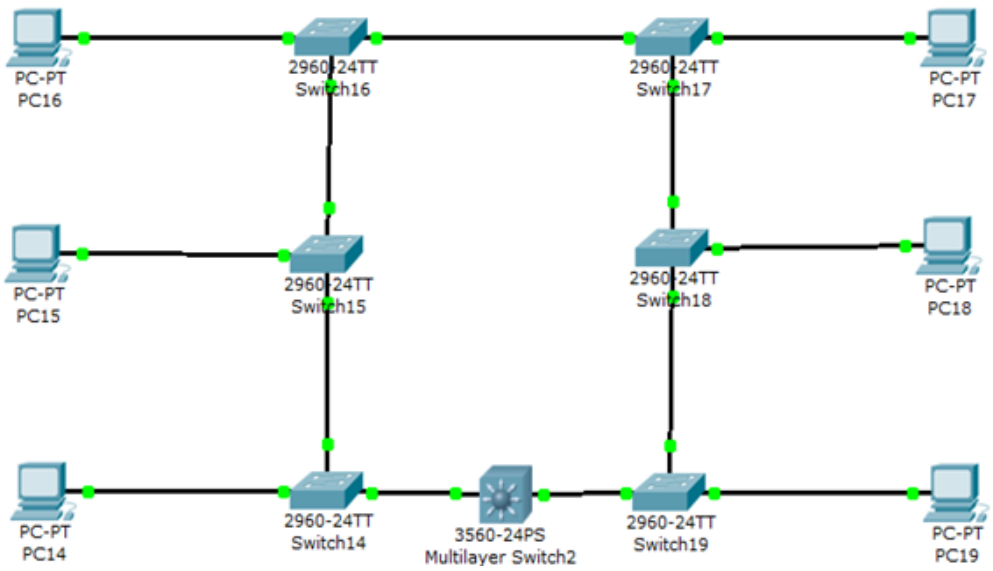


Рисунок 4.1 – Логічна схема мережі представлена засобами Packet Tracer

4.3 Розробка VLAN

Система доступу та агрегування забезпечує з'єднання абонентів з рівнем надання послуг. Послуги, що надаються через окремий сервісний інтерфейс, зазвичай потребують з'єднання абонента з апаратурою на сервісному рівні в межах другого шару моделі OSI. У системі доступу та агрегування таке з'єднання реалізується через використання набору VLAN. Послуги застосунків можуть використовувати апаратуру агрегування як спрощений сервісний інтерфейс, а відповідний VLAN служить засобом для підключення кінцевого пристрою користувача до точки агрегування лише на рівні доступу. Існує дві основні схеми використання VLAN у системах доступу та агрегування: «один VLAN на користувача» та «один VLAN на послугу/групу користувачів» [6].

Схема 1:1 заснована на принципі, де кожен користувач має власний унікальний VLAN по всій мережі до межі надання послуг (рис. 4.2). В той час як схема N:1 передбачає використання одного спільного VLAN для групи користувачів (рис. 4.3). Обидві стратегії мають свої плюси та мінуси, які ми розглянемо детальніше [6].

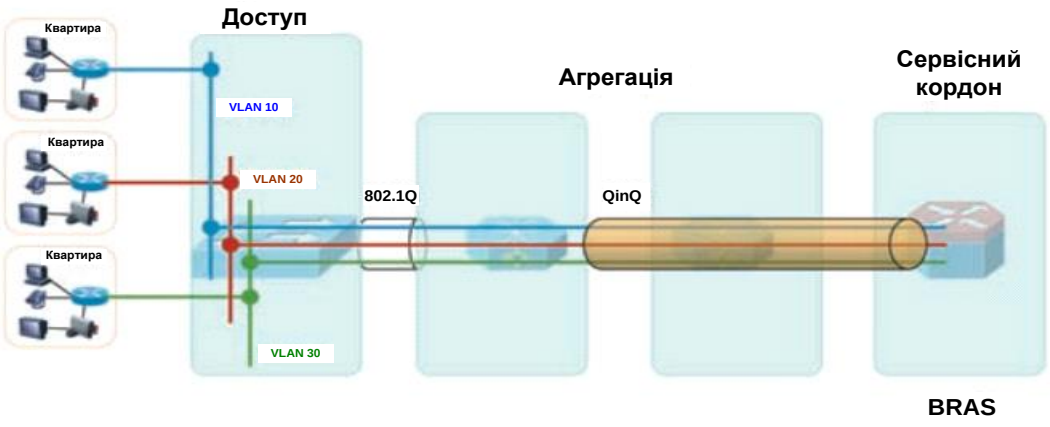


Рисунок 4.2 – Модель VLAN 1:1

Спочатку зупинимося на схемі 1:1, або VLAN на користувача. Основною перевагою є високий рівень ізоляції користувачів між собою у мережі доступу та агрегації. В цій моделі кожен користувач має свій власний VLAN типу «точка-точка», що містить лише два хости - самого користувача (його CPE) та відповідний інтерфейс на BRAS, що автоматично забезпечує ізоляцію та контроль трафіку між користувачами. Користувач може надсилати трафік лише

на свій відведений логічний інтерфейс BRAS, а перевірка правильності використання IP/MAC адреси користувача відбувається на BRAS. Схема 1:1 забезпечує точну ідентифікацію порту підключення користувача на пристрої BRAS за номером VLAN-користувача [6].

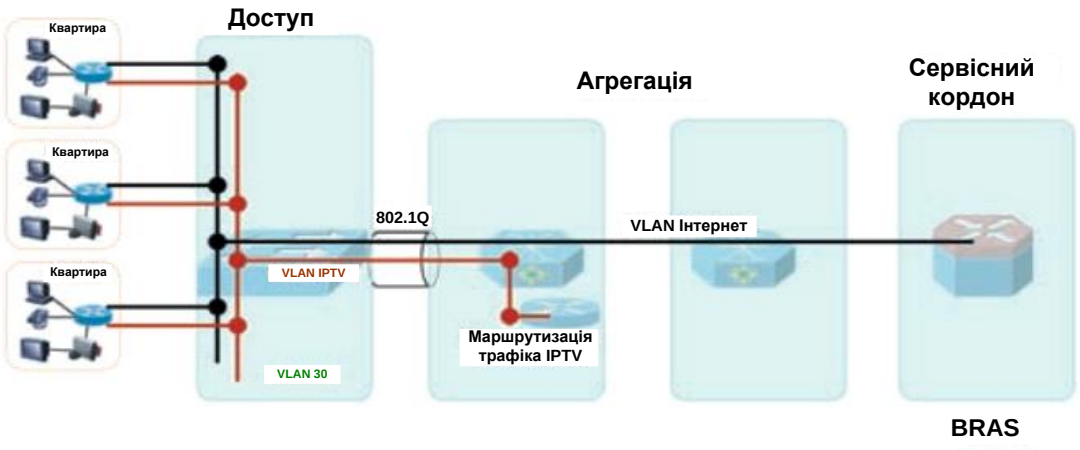


Рисунок 4.3 – Модель VLAN 1: N

Проте, ця модель вимагає наявності значної кількості VLAN у мережі доступу та агрегації, що стає проблемою через обмежену кількість доступних номерів VLAN (в стандарті 802.1q на номер VLAN виділено 12 біт) [6].

Отже, ми маємо 4095 унікальних номерів VLAN, що змушує застосовувати техніку подвійної 802.1q інкапсуляції, або QinQ-інкапсуляцію (ієрархічну нумерацію VLAN). Зазвичай, другий, верхній VLAN тег у цій схемі вказує на комутатор доступу або кільце комутаторів доступу. Також, ця модель потребує присвоєння унікального номера VLAN кожному користувачу, що вимагає від провайдера, по-перше, попереднього планування великої кількості номерів VLAN у мережі і, по-друге, присвоєння та призначення унікального номера при підключенні користувача, збільшуючи трудовитрати на таке підключення.

Альтернативою може стати розробка схеми нумерації VLAN, яка дозволить спочатку надати унікальні номери VLAN всім портам комутаторів доступу. Такі схеми часто застосовуються у DSL-мережах доступу. Однак, на практиці, створити відповідну схему для Ethernet-доступу часто виявляється складно або навіть неможливо. Це пов'язано з тим, що Ethernet-доступ має більш розподілений характер, різниця у використанні портів комутаторів

доступу від будинку до будинку, а також потреба періодично додавати новий комутатор до кільця, що може порушити прийняту схему [7].

Друга модель, N:1 або «VLAN на сервіс», передбачає виділення одного спільного VLAN для групи користувачів, які підключені до одного сервісу, з'єднуючи їх з віртуальним інтерфейсом на обладнанні, що забезпечує сервісний кордон для цього сервісу. Це може бути інтерфейс BRAS для доступу до Інтернету або інтерфейс на обладнанні агрегації для IPTV-сервісу. Для надання іншого сервісу цій групі користувачів може використовуватися інший, окремий загальний VLAN. Модель «VLAN на сервіс», на відміну від моделі ізольованих VLAN, значно спрощує управління простором номерів VLAN. Кількість VLAN у мережі значно зменшується, що в багатьох випадках дозволяє уникнути необхідності використання технології QinQ. Спрощується процес підключення користувача – всі порти комутаторів доступу налаштовуються однаково, не потрібно індивідуальних налаштувань номерів VLAN. Відмова від технології QinQ дозволяє спростити технологію трансляції мультикасту [6].

Однією з переваг архітектури N:1 є здатність створювати розгалужену мережу з численними сервісними межами, тобто VLAN, що використовується для доступу до Інтернету, може розміщуватися на BRAS, в той час як VLAN для сервісів IPTV – буде безпосередньо на агрегаційному обладнанні, тим самим знижуючи навантаження на BRAS і зменшуючи загальні витрати на мережу для провайдера [6].

4.4 Налаштування комутатора рівня доступу

Першими налаштовуємо імена та паролі:

```
Switch >enable
Switch #conf terminal
Switch (config) # hostname switch_UD109
```

Імена комутаторів задаються відповідно до паспортних даних розташування обладнання. Цей комутатор розташовуватиметься у вузлі доступу №109.

Другим етапом налаштуємо консоль і захищаємо паролем:

```
switch_UD109(config)#line console 0
switch_UD109(config-line)#password cisco
switch_UD109(config-line)#login
```

Конфігуруємо віртуальні лінії:

```
switch_UD109(config)#line vty 0 15
switch_UD109(config-line)#password cisco
switch_UD109(config-line)#login
```

Встановлюємо пароль:

```
switch_UD109(config)#enable password cisco
switch_UD109(config)#enable secret 7xcv79bc
```

Початкове конфігурування завершено. Переходимо до детального конфігурування. Як ми вже зазначали раніше у роботі, застосуємо технологію VLAN 1:1. Для кращого розуміння, у цьому прикладі показано підключення одного абонента. Налаштуємо VLAN згідно з табл. 4/1.

```
switch_UD109#enable
switch_UD109#conf terminal
switch_UD109(config)#vlan 10
```

Призначаємо створений VLAN порту комутатора fastEthernet 0/1 і задаємо параметри інтерфейсу:

```
switch_UD109(config)#interface fastEthernet 0/1
switch_UD109(config-if)#switchport mode access
switch_UD109(config-if)#switchport access vlan 10
```

Для забезпечення з'єднання між комутаторами задаємо параметри інтерфейсів. Тобто необхідно, щоб порти комутатора були в режимі Trunk.

```
switch_UD109(config)#interface gigabitEthernet 1/1
switch_UD109(config-if)#switchport mode trunk
switch_UD109(config)#interface gigabitEthernet 1/2
switch_UD109(config-if)#switchport mode trunk
```

Повне конфігурування комутатора завершено. Аналогічно конфігуруються і інші комутатори.

4.5 Конфігурування та маршрутизація комутатора рівня агрегації

По-перше задаються імена та паролі:

```
Switch>enable
Switch#conf terminal
Switch(config)#hostname switch_routing
switch_routing(config)#enable password cisco
switch_routing(config)#enable secret 7xcv79bc
switch_routing(config)#line console 0
switch_routing(config-line)#password cisco
switch_routing(config-line)#login
switch_routing(config)#line vty 0 4
switch_routing(config-line)#password cisco
switch_routing(config-line)#login
```

Далі створюється VLAN. IP-адреси VLAN задаємо відповідно до табл. 4.1:

```
switch_routing(config)#interface vlan 10
switch_routing(config-if)#ip address 192.168.10.1 255.255.255.248
switch_routing(config)#interface vlan 20
switch_routing(config-if)#ip address 192.168.10.9 255.255.255.248
```

switch_routing(config)#interface vlan 30
switch_routing(config-if)#ip address 192.168.10.17 255.255.255.248
switch_routing(config)#interface vlan 40
switch_routing(config-if)#ip address 192.168.10.25 255.255.255.248
switch_routing(config)#interface vlan 50
switch_routing(config-if)#ip address 192.168.10.33 255.255.255.248
switch_routing(config)#interface vlan 60
switch_routing(config-if)#ip address 192.168.10.41 255.255.255.248
далі налаштуємо інтерфейси GigabitEthernet 0/1 та 0/2
switch_routing(config)#interface gigabitEthernet 0/1
switch_routing(config-if)#switchport mode trunk
switch_routing(config-if)#switch trunk encapsulation dot1q
switch_routing(config)#interface gigabitEthernet 0/2
switch_routing(config-if)#switchport mode trunk
switch_routing(config-if)#switch trunk encapsulation dot1q

Вмикаємо функцію маршрутизації:

switch_routing(config)#ip routing

Настроювання завершено, мережа повністю працездатна.

5 ІДЕНТИФІКАЦІЯ КОРИСТУВАЧА ЗА MAC-АДРЕСОЮ НА РІВНІ ДОСТУПУ

5.1 Забезпечення безпеки мережі

У даній мережі було розроблено схему забезпечення безпеки, яка відповідає ключовим вимогам і принципам безпеки. Під час створення цієї схеми було враховано певні особливості, такі як:

- на рівні доступу застосовано стандартний механізм захисту портів на комутаторах, а саме введення списків дозволених MAC-адрес для кожного порту комутатора та призначення інтерфейсів VLAN до портів комутатора. Це означає, що лише певний кінцевий пристрій, який належить до певного VLAN, може отримувати трафік з конкретного порту на комутаторі;

- на рівні агрегації застосовується фільтрація кінцевих пристроїв за IP-адресами через створення списків доступу.

Варто підкреслити, що всі інтерфейси та налаштування VLAN були налаштовані на комутаторі рівня агрегації, що ускладнює для зловмисників можливість перехоплення трафіку та доступу до конфігурації агрегуючого обладнання.

Крім того, було обмежено доступ до віддаленого керування агрегуючим обладнанням для всіх кінцевих пристроїв, за винятком деяких. Це було здійснено за допомогою створення списків доступу для віддаленого доступу.

Отже, схема забезпечення безпеки базується на двох рівнях ідентифікації.

5.2 Безпека комутаторів. Загальні відомості

У багатьох організаціях маршрутизатори та комутатори налаштовані з базовими налаштуваннями безпеки, що робить їх вразливими до атак зловмисників. Атаки, запущені з внутрішніх пристроїв на другому рівні мережі будівлі, можуть швидко компрометувати решту мережі, при цьому атакуючий часто залишається непоміченим [8].

Значна увага приділяється захисту від зовнішніх атак та захисту протоколів верхніх рівнів моделі OSI. Безпека мережі зазвичай зосереджена на

крайових маршрутизаторах та фільтрації пакетів за допомогою заголовків, портів, аналізу стану пакетів та інших механізмів третього та четвертого рівнів. Цей підхід охоплює рівні, починаючи з третього, оскільки трафік входить до мережі будівлі з Інтернету, але часто ігнорується захист пристроїв доступу та комунікаційних каналів другого рівня [8].

Внутрішні маршрутизатори та комутатори Cisco в організаціях призначені для передачі трафіку всередині будівлі. За замовчуванням вони пропускають увесь трафік, якщо не вказано інше в налаштуваннях. Їх основна мета - забезпечення зв'язку, тому налаштування безпеки часто є мінімальними, що робить ці пристрої потенційною ціллю для атак. Атаки, запущені з внутрішніх пристроїв на другому рівні, можуть швидко компрометувати решту мережі, при цьому атакуючий часто залишається непоміченим [8].

Як і на третьому рівні, де заходи безпеки традиційно впроваджувались для захисту пристроїв всередині будівлі, другий рівень також потребує заходів безпеки для захисту від атак, що використовують стандартні операції комутації другого рівня. Існує багато функцій безпеки для маршрутизаторів та комутаторів, але для їх ефективної роботи їх потрібно активувати. Адміністратор має розробити політики та налаштувати ці функції для захисту від зловмисних дій (процес схожий на впровадження списків контролю доступу (ACL) для захисту верхніх рівнів), забезпечуючи при цьому нормальне функціонування мережі [8].

Рекомендовані методи: аналіз або створення корпоративних політик безпеки.

Захист комутаторів: забезпечення доступу до комутаторів.

Ризики для мережної безпеки включають порушення конфіденційності, викрадення даних, підробку особи та втрату цілісності даних. Для мінімізації наслідків недбалості користувачів та зловмисних дій необхідно вжити основних заходів безпеки для всіх мереж [8].

Рекомендовані методи включають два основні кроки, які потрібно виконати при введенні в експлуатацію нового обладнання:

Крок 1 - аналіз або створення корпоративних політик безпеки.

Крок 2 - забезпечення безпеки комутаторів шляхом захисту доступу до комутатора та протоколів комутації, зниження ризиків, пов'язаних з загрозами, ініційованими з комутатора.

5.3 Організаційні безпекові політики

При розробці політик мережевої безпеки важливо враховувати внутрішні політики організації. Необхідно знайти баланс між ефективним рівнем захисту мережі та адміністративними витратами, які можуть виникнути через надмірно строгі заходи безпеки. Тобто необхідно [8]:

- забезпечити процес для перегляду наявної системи мережевої безпеки;
- підтримувати основну структуру безпеки, на якій буде базуватися мережева безпека;
- визначити заборонені способи обробки даних в електронному вигляді;
- визначити необхідні інструменти та процедури для організації політики, що повинна бути побудована на угоді між керівництвом та встановлювати відповідальності користувачів та адміністраторів;
- встановити процедури реагування на інциденти мережевої безпеки;
- розробити план реалізації заходів безпеки, який включає всі локації підприємства, та його втілення в життя.

5.4 Забезпечення безпеки комутаторів рівня доступу

Розглянемо дії, що необхідно вжити, для забезпечення безпеки комутаторів:

- захист фізичного доступу до консолі;
- завдання системних паролів;
- захист доступу до Telnet;
- захист портів комутатора.

5.4.1 Захист фізичного доступу до консолі

Захист від несанкціонованого входу в мережеві системи передбачає, в першу чергу, відсутність можливості фізичного звернення до елементів мережі - комп'ютерів, серверів, мережевих проводів та пристроїв і так далі. Коли мережеве з'єднання перетинає межі вашого контролю, як-от у місці під'єднання до зовнішнього інтернет-провайдера, контроль за фізичними параметрами

мережі, звісно, зникає - і ви мусите спиратися на альтернативні методи. Проте обладнання всередині приміщень має перебувати під строгим контролем [8].

Незважаючи на здавалося б, абсурдність, простий замок на дверях часто врятує від неавторизованого доступу. Сервери, де зберігається критична або чутлива інформація, не мають бути вільно доступні на столі чи в незамкненому приміщенні, куди може увійти будь-хто. Так само мають бути захищені маршрутизатори, хаби, комутатори та інше обладнання. Приміщення з технікою мають бути замкнені або знаходитися під постійним спостереженням.

Фізичний захист обладнання рівня доступу забезпечать антивандальні шафи 10U, в які буде вмонтовано наступне обладнання:

- оптичний крос - ВРХ-16 або ВРХ-24;
- комутатори LS-S2326TP-E1 або LS S2352TP-E1;
- ДБЖ APC Back-UPC 750VA;
- автоматичний вимикач на Автомат ВА 47-29 1Р, Іном = 16А;
- блок розеток на 3 шт.;
- патч-панелі 19" на 24 порти.

Встановлення обладнання та монтаж телекомунікаційних шаф проводиться з урахуванням погоджених переліків та планів розміщення від Замовника.

Антивандальні шафи (рис. 5.1) розміщуються на верхніх поверхах будівель або в спеціально призначених для цього приміщеннях. Це може бути технічний поверх або горище.

Рисунок 5.1 - Антивандальна шафа, яка забезпечує фізичний захист обладнання рівня доступу

Доступ до цих приміщень додатково контролюється управляючою компанією житлово-комунального сектору. Для отримання доступу до цих місць проводяться погодження на етапі планування будівництва.

5.4.2 Захист доступу до Telnet

Основною здатністю захисту маршрутизаторів Cisco є керування доступом Telnet до маршрутизатора. Цей тип захисту важливий, оскільки за допомогою Telnet до маршрутизатора можливо отримати привілейований доступ. При спробі доступу до маршрутизатора за допомогою Telnet користувач одержує запрошення маршрутизатора в режимі користувача. Потім користувач може увійти в привілейований режим [9].

Розглянемо деякі зауваження, які слід враховувати під час керування доступом Telnet:

- порти Telnet у маршрутизаторі називаються портами віртуальних терміналів (портами vty);

- потрібно встановити пароль привілейованого режиму (пароль enable), який обмежує доступ до привілейованого режиму через Telnet. Стандартний пароль режиму enable для маршрутизатора не встановлено. Якщо ви намагаєтеся підключитися за допомогою Telnet до інтерфейсу, пароль для якого не встановлено, ви побачите повідомлення, яке інформує про те, що необхідний пароль, але його не було встановлено. Консольний порт є єдиним портом, що дозволяє доступ у привілейованому режимі, коли пароль vty не встановлено;

- програмне забезпечення Cisco IOS використовує той же пароль для портів vty та консолі;

- необхідно обмежити доступ Telnet за допомогою команд access-class та access-list, зокрема необхідно зробити таке:

- обмежити доступ Telnet джерел з конкретними IP-адресами;

- визначити стандартний список доступу з дозволеними адресами IP;

- використовувати список доступу ліній vty за допомогою команди access-class;

- необхідно налаштувати всі порти vty задані конфігурацією. Порти з номерами 0-4 є за замовчуванням, але можна призначити і більшу кількість портів;

- варто обмежити доступ до порту aux, заблокувати його або взагалі вимкнути за допомогою команди no exec у режимі конфігурації лінії;

- потрібно вимкнути команди, подібні ip alias, no cdp running і no cdp enable, щоб запобігти можливості доступу порушників до маршрутизатора через порти vty;

- потрібно заблокувати запити відгуку за допомогою команд no service tcp-small-serversino service udp-small-servers;

- слід встановити обмеження на типи з'єднань (secure shell, LAT, RCP), які можуть бути відкриті до маршрутизатора за допомогою команди transport input [9].

В нашому випадку забезпечити захист до віддаленого доступу досить просто при конфігуруванні, тому що у подібних мережах віддалений доступ з комп'ютерів не те щоб потрібен, а навпаки підвищує ризик злому віддаленого доступу з будь-якого кінцевого пристрою що в свою чергу може призвести до виведення з ладу мережі.

Тому нам потрібно тільки налаштувати пароль на віддалений доступ та створити список доступу до віддаленого доступу із певної IP адреси (в нашому випадку це буде адреса комп'ютера адміністратора).

```
Switch#ena
Switch#conf terminal
Switch(config)#line vty 0 15
```

Задаємо паролі на вхід у привілейований режим

```
Switch(config-line)#password cisco
Switch(config-line)#login
Switch (config-line) # exit
Switch(config)#enable secret ciscosecre
```

Створюємо список доступу та розріджуємо доступ з цієї IP-адреси

```
Switch(config)#ip access-list standard 99
Switch(config-std-nacl)#permit 192.168.10.2
```

```
Switch (config-std-nacl) # exit
Switch(config)#line vty 0 15

Застосовуємо список доступу на віртуальні лінії
Switch(config-line)#access-class 99 in
```

Виконані дії забезпечать нам віддалений доступ лише з 192.168.10.2
Для всіх інших хостів віддалений доступ буде закрито.

5.4.3 Захист портів комутатора

Функція Port Security на комутаторах Cisco Catalyst забезпечує контроль доступу на рівні порту, обмежуючи кількість та ідентичність пристроїв, які можуть використовувати цей порт. Вона дозволяє визначити список дозволених MAC-адрес, з яких порт прийматиме трафік. Ці MAC-адреси можуть бути додані до списку як статично, шляхом ручного налаштування, так і динамічно, шляхом автоматичного вивчення комутатором. Після активації Port Security, порт буде пересилати лише кадри, що надходять з дозволених MAC-адрес [9].

Функція Port Security дозволяє контролювати, які пристрої можуть використовувати порт комутатора, ідентифікуючи їх за MAC-адресами. Існує кілька способів налаштування цього контролю [9]:

- *динамічний режим:* у цьому режимі важлива лише *кількість* дозволених MAC-адрес, а не їх конкретні значення. Комутатор автоматично запам'ятовує MAC-адреси пристроїв, які першими почали використовувати порт, доки не буде досягнуто заданого ліміту. Ці динамічно вивчені адреси можуть з часом "забуватися" (старіти), якщо пристрій перестане надсилати трафік. Коли це відбувається, порт може запам'ятати нову MAC-адресу, якщо загальна кількість дозволених адрес ще не досягнута;
- *статичний режим:* тут адміністратор вручну вказує конкретні MAC-адреси, яким дозволено використовувати порт. Будь-який пристрій з MAC-адресою, не внесеною до цього списку, не зможе передавати дані через цей порт;
- *комбінований режим (статичний + динамічний):* цей режим поєднує обидва підходи. Адміністратор визначає кілька "статичних" MAC-адрес, яким завжди дозволено доступ, а комутатор автоматично вивчає

додаткові MAC-адреси до досягнення заданого максимального ліміту. Статичні адреси ніколи не старіють, а динамічно вивчені адреси можуть старіти, як і в динамічному режимі;

- *динамічний з закріпленням (Sticky Learning):* цей режим працює як динамічний, але з додатковою функцією. Коли комутатор динамічно вивчає MAC-адресу, він автоматично зберігає її в конфігурації, як якщо б її було налаштовано статично. Це означає, що ці адреси не старіють і залишаються дозволеними навіть після перезавантаження комутатора [9].

Port security - це потужний інструмент для підвищення безпеки мережі, який дозволяє обмежити доступ до портів комутатора лише авторизованим пристроям. Вибір режиму залежить від конкретних потреб і вимог безпеки мережі.

5.4.4 Безпечні MAC-адреси

Комутатор підтримує наступні види безпечних MAC-адрес [8]:

- статичні MAC-адреси: ці адреси вручну налаштовуються на конкретному порту комутатора за допомогою команди switchport port-security mac-address mac-address в режимі налаштування інтерфейсу. Вони постійно зберігаються в таблиці MAC-адрес і в конфігураційному файлі комутатора, тому залишаються активними навіть після перезавантаження;

- динамічні MAC-адреси: Комутатор автоматично вивчає ці адреси, спостерігаючи за трафіком на портах. Вони зберігаються лише в таблиці MAC-адрес і зникають після перезавантаження комутатора;

- Sticky MAC-адреси: Ці адреси можуть бути або налаштовані вручну, як статичні, або вивчені автоматично, як динамічні. Важливо, що вони зберігаються як в таблиці MAC-адрес, так і в конфігураційному файлі. Це означає, що після перезавантаження комутатора, "липкі" MAC-адреси відновлюються автоматично, без необхідності повторного налаштування.

Режими реагування на порушення безпеки

Port security вважає порушенням безпеки такі випадки: коли порт вже "запам'ятав" максимально дозволену кількість MAC-адрес, і пристрій з новою, незнайомою MAC-адресою намагається підключитися; або коли пристрій, чия MAC-адреса вже була "закріплена" за одним портом, з'являється на іншому порту в тій же VLAN [8].

При перевищенні ліміту дозволених MAC-адрес інтерфейс пропонує декілька варіантів реагування:

- Protect (Захист): Якщо кількість дозволених MAC-адрес досягає максимуму, інтерфейс просто ігнорує пакети з невідомими MAC-адресами, поки не буде видалено достатньо існуючих дозволених адрес або збільшено ліміт. При цьому жодні сповіщення про порушення не генеруються;

- Restrict (Обмеження): Подібно до режиму "Protect", інтерфейс відкидає пакети з невідомими MAC-адресами при перевищенні ліміту. Однак, на відміну від "Protect", в цьому режимі генеруються сповіщення про порушення безпеки: відправляються SNMP trap та syslog повідомлення, а також збільшується лічильник порушень;

- Shutdown (Вимкнення): Це найбільш агресивний режим. При виявленні порушення безпеки інтерфейс негайно вимикається та переходить у стан "error-disabled". Також вимикається індикатор порту (LED). Одночасно надсилаються SNMP trap та syslog повідомлення, а також збільшується лічильник порушень. Для відновлення роботи інтерфейсу необхідно або скористатися командою errdisable recovery cause psecure-violation, або вручну вимкнути та знову ввімкнути інтерфейс за допомогою команд shutdown та no shutdown в режимі конфігурації інтерфейсу. Цей режим є стандартним налаштуванням.

5.4.5 Налаштування port security

Функція port security застосовується до окремих інтерфейсів комутатора. Зазвичай, порти комутаторів Cisco за замовчуванням працюють в режимі dynamic auto, який не підтримує port security. Щоб використовувати port security, необхідно перевести інтерфейс в режим trunk або access. В мережах, де використовуються комутатори Cisco, на комутаторах рівня доступу, що підключені до кінцевих пристроїв через порти FastEthernet, слід налаштувати режим access. Натомість, на комутаторах рівня агрегації, які з'єднують між собою інші комутатори, потрібно використовувати режим trunk. Опишемо, як саме конфігурувати ці інтерфейси [8]:

```
Switch#conf terminal
switch_UD109(config)#interface fastEthernet 0/1
switch_UD109(config-if)#switchport mode access
```

Конфігурування для комутаторів рівня доступу проводимо аналогічно.

Конфігурування комутатора рівня агрегації:

```
Switch>enable
Switch#conf terminal
switch_routing(config)#interface fastEthernet 0/1
switch_routing(config-if)#switchport mode trunk
```

Далі необхідно налаштувати список дозволених MAC-адрес і приписати їх з портів комутатора.

MAC-адреса - це унікальний номер, що ідентифікує кожен мережевий пристрій, наприклад, комп'ютер або мережеву карту. У мережах, де дані передаються всім учасникам (наприклад, Ethernet), MAC-адреса дозволяє точно визначити, якому саме пристрою потрібно доставити інформацію. Фактично, MAC-адреси є фундаментом для роботи мережі на канальному рівні, на якому базуються протоколи більш високого рівня (наприклад, IP) [4].

Важливо, що обмеження на використання певних MAC-адрес можна налаштувати як для окремих портів комутатора, так і для віртуальних мереж (VLAN). У нашому випадку, оскільки VLAN вже прив'язані до конкретних портів комутатора, доцільніше налаштовувати обмеження MAC-адрес саме на рівні портів [4].

Перш ніж почати налаштування списку дозволених MAC-адрес, необхідно виконати наступні дії:

```
Switch>enable
Switch#conf terminal
switch_UD109(config)#interface fastEthernet 0/1
```

Далі необхідно увімкнути функцію port security:

```
switch_UD109(config)# port-security
```

Задається кількість безпечних адрес у кількості 1:

Switch_UD109(config-if)#switchport port-security maximum 1

Встановлюємо режим безпечних адрес sticky та вказуємо дозволену адресу:

Switch_UD109(config-if)#switchport port-security mac-address sticky 0001.6450.62DC

Встановлюємо режим реагування на порушення безпеки:

Switch_UD109(config-if)#switchport port-security violation protect

Після виконаних дій комп'ютер з MAC-адресою 0001.6450.62DC зможе отримати доступ до мережі тільки з конкретного комутатора і з конкретного порту, а саме з UD109 і з порту fastEthernet 0/1.

Така схема забезпечення безпеки максимально проста і в той же час достатньо забезпечена всіма необхідними засобами технічної безпеки.

Аналогічно проводиться конфігурування всіх інших комутаторів у оптичному кільці.

Тож маємо наступні списки конфігурацій комутаторів доступу:

Комутатор за адресою вул. Центральна 45 UD109

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname switch_UD109
enable secret 5 $1$mERr$oXudM0pt1ousyj22XJqei/
spanning-tree mode pvst
interface FastEthernet0/1
switchport access vlan 10
switchport mode access
switchport port-security
```

```
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0001.6450.62DC
interface FastEthernet0/2
switchport access vlan 11
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0010.6450.62DC
interface FastEthernet0/3
switchport access vlan 12
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0011.6450.62DC
interface FastEthernet0/9
switchport access vlan 18
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 1100.6450.62DC
interface GigabitEthernet1/1
switchport mode trunk
interface GigabitEthernet1/2
switchport mode trunk
interface Vlan1
no ip address
shutdown
line con 0
line vty 0 4
password cisco
```

```
login
line vty 5 15
password cisco
login
end
```

Комутатор за адресою вул. Центральна 47 UD110

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname switch_UD110
enable secret 5 $1$mERr$oXudM0pt1ousyj22XJqei/
spanning-tree mode pvst
interface FastEthernet0/1
switchport access vlan 20
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0001.6450.62DH
interface FastEthernet0/2
switchport access vlan 21
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0010.6450.62EC
interface FastEthernet0/3
switchport access vlan 22
switchport mode access
switchport port-security
switchport port-security mac-address sticky
```

```
switchport port-security violation protect
switchport port-security mac-address sticky 0011.6450.62KC
interface FastEthernet0/9
switchport access vlan 28
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 1100.6450.62DL
interface GigabitEthernet1/1
switchport mode trunk
interface GigabitEthernet1/2
switchport mode trunk
interface Vlan1
no ip address
shutdown
line con 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
end
```

Комутатор за адресою вул. Центральна 51 UD112

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname switch_UD112
enable secret 5 $1$mERr$oXudM0pt1ousyj22XJqei/
spanning-tree mode pvst
```

interface FastEthernet0/1
switchport access vlan 30
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0001.6650.62DC
interface FastEthernet0/2
switchport access vlan 31
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0010.6459.62DC
interface FastEthernet0/3
switchport access vlan 32
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0011.6430.62DC
interface FastEthernet0/9
switchport access vlan 38
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 1100.6650.62DH
nterface GigabitEthernet1/1
switchport mode trunk
nterface GigabitEthernet1/2
switchport mode trunk
interface Vlan1
no ip address

```
shutdown
line con 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
end
```

Комутатор за адресою вул. Центральна 53 UD111

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname switch_UD111
enable secret 5 $1$mERr$oXudM0pt1ousyj22XJqei/
spanning-tree mode pvst
interface FastEthernet0/1
switchport access vlan 40
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0001.6450.62EC
interface FastEthernet0/2
switchport access vlan 41
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0010.6450.627C
interface FastEthernet0/3
```

```
switchport access vlan 42
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0011.6450.6FDC
interface FastEthernet0/9
switchport access vlan 48
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 1100.6450.62YC
interface GigabitEthernet1/1
switchport mode trunk
interface GigabitEthernet1/2
switchport mode trunk
interface Vlan1
no ip address
shutdown
line con 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
```

Комутатор за адресою вул. Центральна 55 UD114

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

```
hostname switch_UD114
enable secret 5 $1$mERr$oXudM0pt1ousyj22XJqei/
spanning-tree mode pvst
interface FastEthernet0/1
switchport access vlan 50
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0001.6450.62DC
interface FastEthernet0/2
switchport access vlan 51
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0010.6450.62DC
interface FastEthernet0/3
switchport access vlan 52
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0011.6450.62DC
interface FastEthernet0/9
switchport access vlan 58
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 1100.6450.62DC
interface GigabitEthernet1/1
switchport mode trunk
interface GigabitEthernet1/2
```

```
switchport mode trunk
interface Vlan1
no ip address
shutdown
line con 0
line vty 0 4
password cisco
login
line vty 5 15
 password cisco
login
end
```

Комутатор за адресою вул. Центральна 57 UD113

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname switch_UD113
enable secret 5 $1$mERr$oXudM0pt1ousyj22XJqei/
spanning-tree mode pvst
interface FastEthernet0/1
switchport access vlan 60
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0001.6450.62DC
interface FastEthernet0/2
switchport access vlan 61
switchport mode access
switchport port-security
switchport port-security mac-address sticky
```

```
switchport port-security violation protect
switchport port-security mac-address sticky 0010.6450.62DC
interface FastEthernet0/3
switchport access vlan 62
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 0011.6450.62DC
interface FastEthernet0/9
switchport access vlan 68
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security violation protect
switchport port-security mac-address sticky 1100.6450.62DC
interface GigabitEthernet1/1
switchport mode trunk
interface GigabitEthernet1/2
switchport mode trunk
interface Vlan1
no ip address
shutdown
line con 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
end
```

5.5 Забезпечення безпеки комутатора рівня агрегації

Основний тягар забезпечення безпеки мережі в кваліфікаційній роботі покладається на обладнання агрегації. Саме на цьому рівні реалізуються ключові заходи захисту, такі як:

- контроль доступу: використання списків контролю доступу (ACL), статичне призначення IP-адрес VLAN, блокування небажаних IP-адрес;

- аутентифікація: застосування протоколу 802.1X або прив'язка IP-адрес до MAC-адрес;

- якість обслуговування (QoS): сегментація трафіку за пріоритетами для забезпечення належної продуктивності [9].

Розроблена схема безпеки відповідає основним вимогам і принципам захисту обладнання рівня агрегації.

Оскільки комутатори рівня агрегації відповідають за комутацію та розподіл трафіку, доступ до їх конфігурації є ключем до контролю над усією мережею. Тому, важливо зосередити основні зусилля з налаштування ACL та VLAN саме на обладнанні агрегації. Натомість, конфігурація обладнання рівня доступу має бути мінімальною, оскільки воно більш вразливе до несанкціонованого доступу. Відповідно, було прийнято рішення максимально посилити контроль за трафіком і доступом до конфігурації обладнання на рівні агрегації [9].

Для досягнення цих цілей необхідно зробити наступні дії.

На початку конфігурування треба задати імена та паролі.

```
Switch>enable
Switch#conf terminal
Switch(config)#hostname switch_routing
switch_routing(config)#enable password cisco
switch_routing(config)#enable secret 7xcv79bc
switch_routing(config)#line console 0
switch_routing(config-line)#password cisco
switch_routing(config-line)#login
switch_routing(config)#line vty 0 4
switch_routing(config-line)#password cisco
```

```
switch_routing(config-line)#login
```

Далі необхідно створити та конфігурувати VLAN:

```
switch_routing(config)#interface vlan 10
switch_routing(config-if)#ip address 192.168.10.1 255.255.255.248
switch_routing(config)#interface vlan 20
switch_routing(config-if)#ip address 192.168.10.9 255.255.255.248
switch_routing(config)#interface vlan 30
switch_routing(config-if)#ip address 192.168.10.17 255.255.255.248
switch_routing(config)#interface vlan 40
switch_routing(config-if)#ip address 192.168.10.25 255.255.255.248
switch_routing(config)#interface vlan 50
switch_routing(config-if)#ip address 192.168.10.33 255.255.255.248
switch_routing(config)#interface vlan 60
switch_routing(config-if)#ip address 192.168.10.41 255.255.255.248
```

Далі налаштуємо інтерфейси GigabitEthernet 0/1 та 0/2. А саме встановити з'єднання trunk оскільки за цими інтерфейсами проходитиме трафік у різні vlan.

```
switch_routing(config)#interface gigabitEthernet 0/1
switch_routing(config-if)#switchport mode trunk
switch_routing(config-if)#switch trunk encapsulation dot1q
switch_routing(config)#interface gigabitEthernet 0/2
switch_routing(config-if)#switchport mode trunk
switch_routing(config-if)#switch trunk encapsulation dot1q
```

Вмикаємо функцію маршрутизації:

```
switch_routing(config)#ip routing
```

Далі необхідно забезпечити контроль доступу на віддалений доступ.

В першу чергу така конфігурація настроюється на комутаторі рівня агрегації. В нашому випадку будемо її виконувати також на комутаторах рівня доступу.

Задаємо паролі на вхід у привілейований режим:

```
Switch_routing (config-line)#password cisco
Switch_routing (config-line) # login
Switch_routing (config-line) # exit
Switch_routing (config)#enable secret ciscosecret
```

Створюємо список доступу та дозволяємо доступ з цієї IP-адреси

```
Switch_routing(config)#ip access-list standard 98
Switch_routing (config-std-nacl)#permit 192.168.10.2
Switch_routing (config-std-nacl)#exit
Switch_routing (config)#line vty 0 15
```

Застосовуємо список доступу на віртуальні лінії:

```
Switch(config-line)#access-class 99 in
```

Тобто віддалений доступ буде доступний лише з IP-адреси 192.168.10.2.

5.5.1 Налаштування списків доступу

Списки доступу (ACL) – це важливий інструмент мережевої безпеки, який дозволяє контролювати потік даних через інтерфейси комутатора або маршрутизатора. Вони працюють, фільтруючи мережевий трафік на основі заданих правил, дозволяючи або блокуючи пакети, які відповідають певним критеріям [8].

ACL використовуються для різних цілей, включаючи:

- керування трафіком: фільтрація пакетів, що проходять через інтерфейси;
- контроль доступу: обмеження доступу до віртуальних мереж (VLAN);
- управління маршрутизацією: фільтрація інформації, що обмінюється протоколами динамічної маршрутизації [8].

Процес налаштування ACL складається з двох основних етапів:

- створення списку доступу: визначення набору правил (критеріїв), за якими буде фільтруватися трафік;

- застосування списку доступу: призначення створеного списку до конкретного інтерфейсу [8].

Кожен пакет, що проходить через інтерфейс, до якого застосовано ACL, перевіряється на відповідність критеріям, визначеним у списку. Типові критерії включають IP-адреси відправника та отримувача, а також тип протоколу. Набір доступних критеріїв залежить від конкретного протоколу [8].

Правила в ACL обробляються послідовно, одне за одним. Якщо пакет відповідає одному з правил, подальша перевірка припиняється. Важливо пам'ятати, що порядок правил в ACL має значення [8].

Кожен ACL має неявне правило "deny all" в кінці. Це означає, що якщо пакет не відповідає жодному з визначених правил, він буде автоматично відхилений [8].

На кожному інтерфейсі може бути застосовано лише один ACL для кожного протоколу та напрямку трафіку (вхідний або вихідний).

Вхідний трафік: ACL застосовується до пакетів, що надходять на інтерфейс. Якщо пакет дозволено ACL, він передається для подальшої обробки. Якщо заборонено – відкидається.

Вихідний трафік: ACL застосовується до пакетів, що покидають інтерфейс. Після того, як маршрутизатор вирішив відправити пакет через певний інтерфейс, він перевіряє ACL. Якщо пакет дозволено, він передається. Якщо заборонено – відкидається.

5.5.2 Стандартні та розширені списки доступу

Для IP-адрес доступні різні типи списків контролю доступу (ACL):

- стандартні ACL: фільтрують трафік на основі IP-адреси відправника;

- розширені ACL: забезпечують більш детальну фільтрацію, враховуючи IP-адреси відправника та отримувача, а також інші параметри пакетів;

- динамічні розширені ACL: це розширені ACL з обмеженим часом дії та додатковими умовами активації [8].

У нашій конфігурації ми будемо використовувати стандартні іменовані ACL. Процес створення та застосування ACL включає наступні кроки.

Спочатку створюються самі списки доступу. Враховуючи спрощену топологію мережі, де кожен з шести користувачів підключений до окремого комутатора через свою VLAN, було створено шість VLAN. (Така спрощена схема дозволяє продемонструвати функціональність мережі в цілому).

Для зручності адміністрування, нумерація ACL відповідає нумерації відповідних VLAN.

```
switch_routing#enable
switch_routing#configure terminal
switch_routing(config)#ip access-list standard 10
```

Вписуємо критерії у стандартні іменні списки. Приведемо список можливих:

- permit: дозволити;
- deny: заборонити;
- remark: коментар про список доступу;
- address: забороняємо або дозволяємо мережу;
- any: дозволяємо або забороняємо все;
- host: дозволяємо або забороняємо хосту;
- source-wildcard: WildCard маска мережі;
- log: включаємо логування пакети, що проходять через цей запис ACL.

Дозволяємо доступ лише хосту 192.168.10.2:

```
switch_routing(config-std-nacl)#permit host 192.168.10.2
switch_routing(config-std-nacl)#deny any
```

Далі присвоїмо ці умови до певного інтерфейсу. Для нас цей інтерфейс - Vlan 10. Входимо в інтерфейс і забороняємо вхідний та вихідний трафік за порушення умов даного списку.

```
switch_routing(config)#int vlan 10
switch_routing(config-if)#ip access-group 10 in
switch_routing(config-if)#ip access-group 10 out
```

Отже, лише вказана IP-адреса, що належить до конкретного VLAN, має право на отримання трафіку. Аналогічну конфігурацію слід застосувати до кожного створеного VLAN.

```
switch_routing(config)#ip access-list standard 20
switch_routing(config-std-nacl)#permit host 192.168.10.10
switch_routing(config-std-nacl)#deny any
switch_routing(config)#int vlan 20
switch_routing(config-if)#ip access-group 10 in
switch_routing(config-if)#ip access-group 10 out
switch_routing(config)#ip access-list standard 30
switch_routing(config-std-nacl)#permit host 192.168.10.18
switch_routing(config-std-nacl)#deny any
switch_routing(config)#int vlan 30
switch_routing(config-if)#ip access-group 10 in
switch_routing(config-if)#ip access-group 10 out
switch_routing(config)#ip access-list standard 40
switch_routing(config-std-nacl)#permit host 192.168.10.26
switch_routing(config-std-nacl)#deny any
switch_routing(config)#int vlan 40
switch_routing(config-if)#ip access-group 10 in
switch_routing(config-if)#ip access-group 10 out
switch_routing(config)#ip access-list standard 50
switch_routing(config-std-nacl)#permit host 192.168.10.34
switch_routing(config-std-nacl)#deny any
switch_routing(config)#int vlan 50
switch_routing(config-if)#ip access-group 10 in
switch_routing(config-if)#ip access-group 10 out
switch_routing(config)#ip access-list standard 60
switch_routing(config-std-nacl)#permit host 192.168.10.42
switch_routing(config-std-nacl)#deny any
switch_routing(config)#int vlan 60
switch_routing(config-if)#ip access-group 10 in
switch_routing(config-if)#ip access-group 10 out
```

Приведемо кінцеву конфігурацію обладнання рівня агрегації:

```
Building configuration...
Current configuration: 2064 bytes
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname switch_routing
enable secret 5 $1$mERr$wZMkJsj2RVk4hay2C4T32.
ip routing
spanning-tree mode pvst
interface FastEthernet0/1
interface FastEthernet0/2
interface FastEthernet0/24
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
interface GigabitEthernet0/2
switchport trunk encapsulation dot1q
interface Vlan1
no ip address
shutdown
interface Vlan10
ip address 192.168.10.1 255.255.255.248
ip access-group 10 in
ip access-group 10 out
interface Vlan20
ip address 192.168.10.9 255.255.255.248
ip access-group 20 in
ip access-group 20 out
interface Vlan30
ip address 192.168.10.17 255.255.255.248
ip access-group 30 in
```

```
ip access-group 30 out
interface Vlan40
ip address 192.168.10.25 255.255.255.248
ip access-group 40 in
ip access-group 40 out
interface Vlan50
ip address 192.168.10.33 255.255.255.248
ip access-group 50 in
ip access-group 50 out
interface Vlan60
ip address 192.168.10.41 255.255.255.248
ip access-group 60 in
ip access-group 10 out
ip classless
access-list 10 permit host 192.168.10.2
access-list 10 deny any
access-list 20 permit host 192.168.19.10
access-list 20 deny any
access-list 30 permit host 192.168.10.18
access-list 30 deny any
access-list 40 permit host 192.168.10.26
access-list 40 deny any
access-list 50 permit host 192.168.10.34
access-list 50 deny any
access-list 60 permit host 192.168.10.42
access-list 60 deny any
line con 0
password cisco
login
line vty 0 4
password cisco
login
end
```

ВИСНОВКИ

Оскільки мультисервісні мережі набувають все більшої популярності, критично важливим стає їх професійна розробка та надійний захист. Ефективність функціонування такої мережі безпосередньо залежить від якості її проєктування та дієвості системи безпеки.

В рамках даної роботи було розроблено проєкт мультисервісної мережі та запропоновано комплексну схему захисту для оптичного кільця ОК-6 в житловому районі міста Чернівці. Це оптичне кільце об'єднує будинки, розташовані на вулиці Центральній, і обслуговує 144 абоненти. Мережа надає доступ до Інтернету, IP-телефонії та цифрового інтерактивного телебачення, використовуючи послуги оператора "Укртелеком".

Мережа ОК-6 має дворівневу структуру: рівень агрегації та рівень доступу. На рівні агрегації використовується високопродуктивний комутатор 3-го рівня, що характеризується високою надійністю. Рівень доступу побудований за кільцевою топологією, що з'єднує всі вузли в кільце та забезпечує з'єднання з мережею "Укртелеком", що мінімізує ризик відмови. Район ОК-6 поділений на 15 секторів (оптичних кілець), кожен з яких має вузол агрегації. Розглянуто оптичне кільце включає мережу доступу, що складається з 6 комутаторів рівня доступу, підключених до вузла агрегації.

Для перевірки працездатності мережі було створено її модель у програмі Packet Tracer. Крім того, розроблено дворівневу систему безпеки, що включає:

- ідентифікацію користувачів за MAC-адресою на рівні доступу;
- ідентифікацію користувачів за IP-адресою на рівні агрегації.

Для реалізації цих заходів було зроблено наступне:

- встановлено паролі для доступу до конфігурації обладнання;
- забезпечено безпеку портів комутаторів рівня доступу шляхом створення таблиць дозволених MAC-адрес, прив'язаних до конкретних портів;
- налаштовано віртуальні інтерфейси VLAN за технологією VLAN 1:1, також прив'язані до певних портів комутатора;
- налаштовано фільтрацію трафіку за IP-адресами користувачів за допомогою списків доступу на комутаторі рівня агрегації;
- створено списки доступу для віддаленого підключення до конфігурації обладнання, захищені паролем.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Тарнавський Ю.А., Кузьменко І. М. Організація комп'ютерних мереж: підручник: для студ. спеціальності 121 "Інженерія програмного забезпечення" та 122 "Комп'ютерні науки" / КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 259 с.

2. Олещенко Л.М. Організація комп'ютерних мереж: конспект лекцій: навч. посіб. для студ. спеціальності 121 "Інженерія програмного забезпечення", спеціалізації "Програмне забезпечення комп'ютерних та інформаційно-пошукових систем" / КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 225 с.

3. Бахтеяров П. Основы построения Metro Ethernet сетей [Текст] /П. Бахтеяров // Вестник связи – 2004 – Вып. №10. – С. 45-51.

4. Попов І.І., Максимов Н.В. Комп'ютерні мережі: навчальний посібник. - М.: ФОРУМ: ІНФРА - М, 2015. – 365 с.

5. Офіційний сайт виробника Cisco Systems [Електронний ресурс] / Режим доступу – http://www.cisco.com .

6. Х'юкабі, Д., Мак-Квері, С. Посібник із конфігурування комутаторів Catalyst.: Пер. з англ. [Текст] - К.: Видавничий дім "Вільямс" - 2004. - 560 с.

7. Optix OSN 3500 Інтелектуальна система оптичної передачі Технічний посібник - Опис системи.

8. Технічний опис синхронного мультиплексора SMA4. Фірма «СІМЕНС». Варіант виконання S42022-D3502-H2-2-18.

9. https://www.dlink.com/ua/uk

10. Основи організації мереж Cisco, том 1 [Текст]: Пер. з англ. – К.: Видавничий дім «Вільямс», 2002. – 512 с.

11. https://prelogin-authoring.netacad.com/ru/courses/packet-tracer