ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ЛОМ – локальна обчислювальна мережа
ОС – операційна система
ПЗ – програмне забезпечення
ПК – персональний комп'ютер
РС – робоча станція
ACL – Access Control List
BDR – Backup Designated Router
BPDU – Bridge Protocol Data Unit
CPU – Central Processing Unit
DDOS – Distributed Denial of Service
DHCP – Dynamic Host Configuration Protocol
DOS – Denial of Service
DR – Designated Router
ECC – Error-Correcting Code
EIGRP – Enhanced Interior Gateway Routing Protocol
HDD – Hard Disk Drive
IDS – Intrusion Detection System
IP – Internet Protocol
IPS – Intrusion Prevention System
ISP – Internet Service Provider
LAN – Local Area Network
NAT – Network Address Translation
OSPF – Open Shortest Path First
PAT – Port Address Translation
RAID –Redundancy Array of Independent Disks
RAM – Random Access Memory
RIP – Routing Information Protocol
STP – Shielded Twisted Pair

STP – Spanning Tree Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

UTP – Unshielded Twisted Pair

VLAN – Virtual Local Area Network

Умовні познаки

Gb – гигабіт (10^9біт)

ВСТУП

Сьогодні все більше компаній різних розмірів і цілей зосереджуються на IT-інфраструктурі та ресурсах для підвищення якості обслуговування та розширення сфери своєї діяльності. Це стосується не лише тих, хто надає послуги в області управління, наприклад, центрів обробки даних або мереж – багато фірм піклуються про те, як вони керують внутрішнім потоком документів, безпекою даних та енергоефективністю.

Компанія ТОВ «АСТ-Світлотехніка», що займається продажем електрообладнання, після деяких серйозних проблем з безпекою і втрат документів вирішила вдосконалити власну IT-інфраструктуру. Компанія збирається покращити безпеку – як внутрішню, так і зовнішню – і впровадити сучасні технології для запобігання вищезазначених проблем у майбутньому.

Для вдосконалення існуючої корпоративній мережі підприємства необхідно переглянути апаратне і програмне забезпечення, яке компанія використовує, виправити помилки впровадження, якщо вони є, і розгорнути нове програмне і апаратне забезпечення для заміни застарілих і несправних. Для цього доцільно використати різні ресурси, такі як навчальні посібники, існуючі плани мережі та ISP-документи, симулятор Packet Tracer та інші конфігурації, включаючи конфігурації мереж, безпеки та кінцевих пристроїв.

Метою кваліфікаційної роботи є вдосконалення існуючої локально-обчислювальної мережі компанії ТОВ «АСТ-Світлотехніка», що займається продажем електрообладнання, за рахунок впровадження нового програмного та апаратного забезпечення, що базуються на сучасних телекомунікаційних технологій.

Додаткова мета роботи полягає в пошуку потенційних або наявних проблем з безпекою, зв’язністю або загальною зручністю використання поточної комп’ютерної мережі підприємства та пропозиції списку покра-

щень, змін і технологій, які зможуть допомогти вирішити проблеми, з якими зіткнулася компанія.

Для досягнення поставленої мети в роботі необхідно вирішити наступні завдання:

- здійснити дослідження існуючої мережі підприємства та виявити потенційні проблеми;
- здійснити планування заходів щодо покращення існуючої корпоративної мережі підприємства за рахунок використання нових мережевих технологій;
- обґрунтувати вибору проміжного мережевого обладнання мережі;
- обрати спосіб управління мережними ресурсами і користувачами мережі;
- забезпечити необхідний рівень захисту даних;
- виконати моделювання мережі у симуляторі Packet Tracer.

1 ІТ ІНФРАСТРУКТУРА МАЛОГО БІЗНЕСУ

В цьому розділі роботи наведемо основні технології та принципи, які зазвичай реалізуються та використовуються в ІТ-інфраструктурі малого бізнесу. Крім того, розглянемо відомості про конфігурації мережі, протоколювання маршрутизаторів, прокладку кабелів тощо, у другій частині – про конфігурації кінцевих пристроїв – як апаратної, так і програмної, у третій частині – про безпеку апаратного та програмного забезпечення мережі та кінцевих пристроїв, таких як ПК.

1.1 Конфігурації мережі

1.1.1 Типи кабелю

Існує декілька типів кабелю, які можуть бути використані для з’єднання вузлів в залежності від обраної мережевої технології. По-перше,

кабель з крученими парами, який зазвичай використовується в будівлях, офісах і будинках. Кручена пара (Twisted Pair Cable) має два варіанти маркування – STP і UTP. UTP кабель – неекранована кручена пара, є найпопулярнішим кабельним рішенням: він порівняно дешевий, його легко встановити і його легко ремонтувати. Зазвичай кабель UTP складається з декількох пар скручених дротів, які покриті непровідним матеріалом. Кабель, що найбільш часто використовується, має чотири кручені пари всередині. Кожен дріт у парі покритий ізоляційним матеріалом [1][1)]. В даний час існує сім категорій кабелю UTP, їх характеристики наведені в табл. 1.1.

Таблиця 1.1 – Категорії кабелів UTP

Категорія UTP	Швидкість передачі даних	Максимальна довжина	Типове застосування
CAT1	до 1 Мбіт/с	–	старий телефонний кабель
CAT2	до 4 Мбіт/с	–	мережі Token Ring
CAT3	до 10 Мбіт/с	100м	Token Ring і 10BASE-T Ethernet
CAT4	До 16 Мбіт / с	100м	Мережа Token Ring
CAT5	До 100 Мбіт / с	100м	Ethernet, FastEthernet,
CAT5e	До 1 Гбіт / с	100м	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	До 10 Гбіт / с	100м	Gigabit Ethernet, 10G Ethernet (55 м)
CAT6a	До 10 Гбіт / с	100м	Gigabit Ethernet, 10G Ethernet (55 м)
CAT7	До 10 Гбіт / с	100м	Gigabit Ethernet, 10G Ethernet (100 м)

[1)] [1] Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. Комп'ютерні мережі. Навчальний посібник Вінниця : ВНТУ, 2013. 371 с.

Вигляд кабелю кручена пара представлений на рис.1.1.

Рисунок 1.1 – Кручена пара категорії 5е

STP-кабель, як правило, дорожчий і більш складний у виробництві, хоча і має певні переваги. Основна його відмінність від неекранованого кабелю в тому, що в STP є тонкий шар провідного екрану, розміщений навколо скручених дротів, або кожна пара дротів захищена фольгою окремо. Цей щит зберігає дроти і дані, які проводить електропровід від електромагнітних перешкод [2][1)].

Волоконно-оптичний кабель використовує скло або пластик для передачі даних за допомогою світла, тому цей кабель не є електричним. Оптоволоконний кабель використовує в якості джерела сигналу для передачі світла світлодіоди. Як правило, пластиковий волоконно-оптичний кабель дешевше і простіше реалізувати, ніж скляний оптичний кабель, але максимальна відстань для цього кабелю менше, ніж при використанні скла.

Волоконно-оптичний кабель складається з зовнішньої оболонки, діелектричного матеріалу, захисного шару, малопотужної оболонки і самого волокна серцевини – скла або пластику [2][1)]. У сучасних мережах використо-

[1)] [2] Зайченко О. Ю., Зайченко Ю. П. Комп'ютерні мережі Підручник К. : Видавничий Дім «Слово», 2010. 520 с.

вуються два типи волоконно-оптичних кабелів – одномодовий і багатоходовий (рис.1.2).

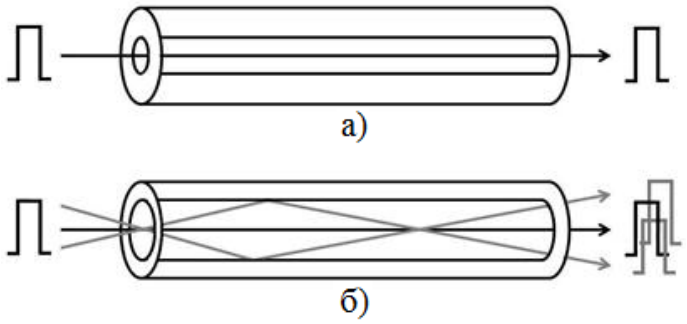

Рисунок 1.2 – Схема проходження світла: а) по одномодовому оптоволокну; б) по багатомодовому оптоволокну

Світло в одномодовому кабелі йде прямо через серцевину до місця призначення і не торкається оболонки. У багатомодовому волоконно-оптичному кабелі є кілька променів світла, що заломлюється від оболонки. Щоб не змішувати різні послідовності даних, ядро і оболонка мають відмінну різницю показників заломлення між ними.

Основні відмінності між оптичним кабелем і крученою парою: відстань передачі даних – кручена пара – не більше 100 метрів, оптоволоконний – декілька кілометрів; пропускна здатність оптичного кабелю перевищує пропускну здатність мідних кабелів; оптичний кабель не схильний до електромагнітних і перехресних перешкод. Недоліком волоконно-оптичного кабелю є його вартість і складність реалізації, а також те, що не все обладнання підтримує цей вид кабелів.

1.1.2 Топології мереж

Існує кілька типів мережевих топологій, які користуються популярністю в мережах малих компаній. Треба розрізняти фізичну і логічну

топології. Фізична топологія мереж показує, яким чином мережні пристрої підключаються до основної мережі. Тоді як, логічна топологія показує спосіб переміщення даних між пристроями в мережі – незалежно від фізичних з'єднань.

Перша базова топологія – шина, в якій пристрої з'єднаються одним мережним кабелем. Ця топологія вважається найпростішою і найдешевшою, оскільки вона проста в реалізації, і потребує найменшу кількість кабелю, але проблеми виникають, коли два або більше хостів надсилають пакети по одній шині майже одночасно.

Цю проблему можна уникнути в топології зірка, де кожен хост має свій власний спеціальний кабель, який підключається до концентратора або комутатора – таким чином, зв'язок між пристроями не переривається. На додаток до цього, мережа, яка використовує топологію зірка, легко масштабується. Однак ця топологія є дорогою для реалізації, оскільки кожен з хостів вимагає свого кабелю.

В топології кільце кожен хост з'єднується з двома іншими хостами, так що формується кільце. Цю топологію відносно легко розширити, але цей процес вимагає відключення хостів від мережі, що порушує роботу мережі.

Наступною топологією є сіткова (коміркова) топологія, де кожен пристрій має окреме приватне з'єднання зі всіма іншими пристроями в мережі. Такий підхід полегшує діагностику несправностей мережі, але, враховуючи загальну кількість зв'язків у мережі, це також одна з найдорожчих топологій відносно часу і грошей, витрачених на підключення всіх хостів.

Топологія дерево або ієрархічна топологія має тільки один хост між будь-якими двома в мережі. З цією топологією, легко розширити мережу і додати нові хости і з'єднання, але одним з головних недоліків є те, що якщо центральний вузол виходить з ладу, то мережа не працює. Топології, згадані вище, показані на рис.1.3.

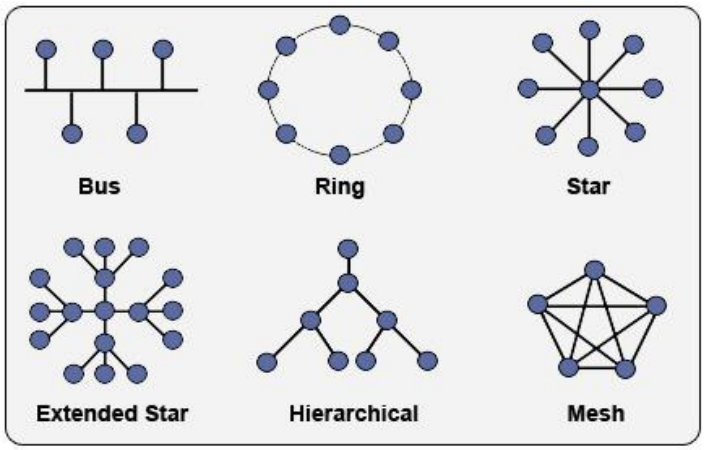

Рисунок 1.3 – Мережеві топології

В підсумку можна сказати, що дуже рідко, коли тільки один тип топології ідеально підходить для мережі – наприклад, сіткова топологія вимагає значних інвестицій і її важко реалізувати, а топології шина не вистачає надмірності. Рішення полягає в тому, щоб об'єднати і змішати різні типи топологій, щоб отримати мережеву схему, яка відповідає певному підприємству. Гібридною топологією називається поєднання двох або більше простих типів топологій, які зазвичай є дуже гнучкими, надзвичайно надійними і розроблені окремо для потреб компанії [3][1)].

1.1.3 Протоколи маршрутизації

Маршрутизація – це процес пошуку шляху в мережі від початкової точки до місця призначення. Маршрутизація складається з пошуку всіх можливих шляхів і вибору оптимального як правило, найкоротшого або найменш трудомісткого шляху. Протокол маршрутизації створює таблицю маршрутизації для хостів у мережі.

[1)] [3] Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп'ютерні мережі. Книга 2// Навчальний посібник. Львів: Магнолія 2006, 2014. 328 с.

Протокол BGP (Border Gateway Protocol) – передає дані між або в межах автономних систем. Система вважається автономною, якщо вона є мережею або низкою мереж, які слідують одному і тому ж набору правил і політикам маршрутизації. Зазвичай цей протокол використовується для обміну даними між провайдерами. Якщо два або більше провайдерів обмінюються даними за допомогою цього протоколу, це називається зовнішнім BGP. Аналогічно, якщо провайдер використовує цей протокол в автономній системі, він називається внутрішнім BGP. Коли дві сусідні мережі, що використовують BGP, встановлюють з'єднання, то вони обмінюються повною інформацією про маршрутизацію, зібрану BGP. Потім таблиця оновлюється тільки тоді, коли виявляються зміни таблиці маршрутизації. Тим не менш, BGP не надсилає періодичні оновлення таблиці маршрутизації. Протокол надзвичайно масштабований і стабільний – це досягається за допомогою багатьох атрибутів маршрутів, які визначають різні політики маршрутизації. В основному, це протокол, який використовує Інтернет. Зазвичай локальна мережа компанії будується з використанням IGP, а не протоколу BGP [4][1)].

Протокол RIP (Routing Information Protocol) – напевно, один з найдавніших протоколів і один з найпростіших для реалізації. При обміні інформацією про маршрутизацію він використовує пакетні протоколи користувача [5][2)]. На рис.1.4 наведено приклад простої мережі, в якій реалізований протокол RIP , так що кожні 30 секунд кожен маршрутизатор посилає оновлення до сусідніх маршрутизаторів, щоб тримати таблицю маршрутизації оновленою.

Якщо Router 3 повинен відправити пакет до Network A, то спочатку необхідно підрахувати кількість переходів до місця призначення. Справа від Router3 потрібно два переходи, щоб дістатися до Network A, зліва – три пере-

---

[1)] [4] Border Gateway Protocol – Вікіпедія. (загол. з екрану). URL: https:// uk.wikipedia.org /wiki/BGP (дата звернення 13.03.2019)

[2)] [5] Routing Information Protocol – Вікіпедія. (загол. з екрану). URL: https:// uk.wikipedia.org/wiki/Routing_Information_Protocol (дата звернення 13.03.2019)

ходи до пункту призначення. RIP вибирає правильний шлях, однак, якщо найкоротший шлях через Router 4 виходить з ладу, потрібно деякий час для відкидання неактивного маршруту і оновлення таблиці маршрутизації. Зазвичай це займає три періоди оновлення, кожні 30 секунд. Після цього Router 2 повертає маршрут до Network A, це також займає до 30 секунд. На закінчення, RIP займає приблизно дві хвилини для вирішення проблеми з мережею.

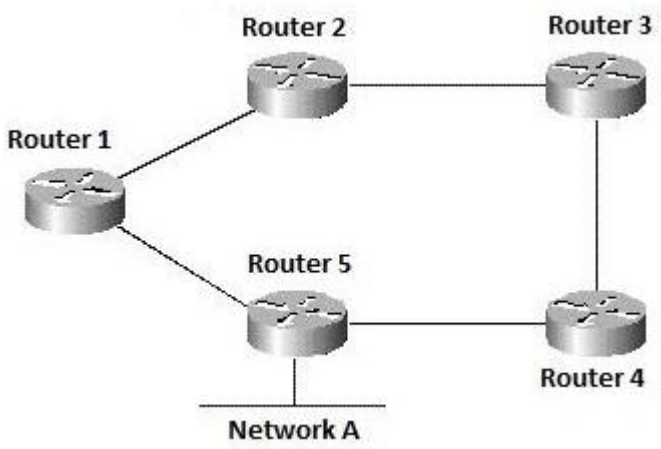

Рисунок 1.4 – Приклад простої мережі

Протокол OSPF (Open Shortest Path First) – протокол маршрутизації, який використовує стан зв'язків замість векторів відстані. Маршрутизатор генерує оголошення про стан каналу (link-state advertisement, LSA), яке є сукупністю всіх станів каналу на цьому маршрутизаторі. Після цього всі маршрутизатори обмінюються наборами станів каналу. Якщо колекція станів каналу, яка отримана маршрутизатором, відрізняється від тієї, яку він має, маршрутизатор зберігає її і посилає оновлену версію на інші маршрутизатори. Після того, як кожен має оновлену версію, база даних стану каналів буде

побудована, а дерево найкоротшого шляху розраховано з використанням алгоритму Дейкстри [6][1)].

Однією з основних концепцій OSPF є концепція зони. Зона (area) – сукупність мереж і маршрутизаторів, які мають один і той же ідентифікатор зони. Зони використовуються для прискорення процесу створення таблиці маршрутизації – маршрутизатор, який належить до зони, зберігає таблицю маршрутизації тільки в межах зазначеної зони. Для обміну даними про мережу необхідно, щоб маршрутизатори стали сусідами. Для цього вони відправляють один одному пакет hello, який складається з полів: ID маршрутизатора, інтервал hello/dead, сусідів (neighbors), ID зони, пріоритету маршрутизатора, IP-адреса виділеного маршрутизатор (DR) і запасного виділеного маршрутизатора (BDR), пароль аутентифікації і прапор тупикової зони.

ID маршрутизатора – це найбільша IP-адреса маршрутизатора на будь-якому з активних інтерфейсів. Hello/dead інтервал – це період часу, коли відношення сусідів є дійсним. Коли закінчується час, відправляється новий пакет hello і формується сусідство. ID зони – це номер області, де знаходяться маршрутизатори, вона повинна бути однаковою з обох сторін для формування сусідства. Пріоритет маршрутизатора – це номер, який визначає призначений і резервний маршрутизатор [7][2)].

Виділений маршрутизатор (DR) використовується для того, щоб запобігти переповненню смуги пропускання мережі пакетами hello та оновленнями таблиці маршрутизації. Щоб кожен маршрутизатор не відправлял пакет hello всім іншим, вибирається виділений маршрутизатор, який буде отримувати пакети hello від кожного маршрутизатора в цій зоні, а потім пере-

---

[1)] [6] Open Shortest Path First Protocol – Вікіпедія. (загол. з екрану).. URL: https://uk.wikipedia.org/wiki/OSPF (дата звернення 13.03.2019)

[2)] [7] В.Чернега, Б. Платтнер Компьютерные сети// Навчальний посібник Севастополь: Вид-во СевНТУ, 2006. 500 с.

силати ці пакети кожному члену зони. У цьому випадку сусідство формується тільки з DR і резервного DR.

Таким чином, мережа, яка налаштована за допомогою протоколу OSPF, сходиться швидше, ніж за протоколом RIP. Маршрутизатор, який налаштований за протоколом OSPF, має базу даних стану каналів, яка оновлюється рідше, ніж у випадку RIP. Крім того, рішення про те, який шлях вибрати, базується на вартості інтерфейсу, а не на кількості стрибків. Повертаючись до рис. 1.4, якщо протокол OSPF використовується в цій топології і найкоротший шлях стає недоступним, другий найкоротший шлях обчислюється і використовується замість невдалого.

Протокол EIGRP (Enhanced Interior Gateway Routing Protocol) – це поліпшений протокол маршрутизації внутрішніх шлюзів і це розширений векторний протокол. Вектори відстані використовуються тут для визначення найкоротшого шляху до місця призначення. Після увімкнення EIGRP пакети hello надсилаються іншим маршрутизаторам – подібно до OSPF: якщо отримано відповідь, формується сусідство. Однак процес вибору найкращого шляху відрізняється від OSPF. EIGRP використовує набір метрик для визначення найкращого шляху: пропускну здатності, навантаження, затримки і надійності. У EIGRP кожне посилання має значення, яке зберігається в таблицях топології маршрутизаторів. Виходячи з цих значень, обчислюється вартість від одного вузла до іншого. Найнижча вартість є найкращою, і шлях, який найменше коштує, стає наступником і записується в таблицю маршрутизації [8][1)].

EIGRP використовує кілька таблиць: таблиця сусідів, таблиця топології і таблиця маршрутизації. Перша таблиця містить усіх сусідів, які безпосередньо підключені до маршрутизатора. Таблиця топології містить призначення, метрику та список маршрутів, які були отримані від інших сусідів. Коли

[1)] [8] Enhanced Interior Gateway Routing Protocol – Вікіпедія. (загол. з екрану).URL: https://uk.wikipedia.org/wiki/EIGRP (дата звернення 13.03.2019)

маршрутизатори стають сусідами, вони обмінюються вмістом своїх таблиць топології. Потім наступники копіюються в таблицю маршрутизації [9][1)].

EIGRP не витрачає час на очікування періодичних оновлень таблиць маршрутизації. Він будує таблицю маршрутизації на кожному пристрої на основі відповідей від сусідніх маршрутизаторів. Після цього кожен маршрутизатор рис.1.4, Router 3 посилає пакет даних в Network A через Router 4, оскільки це найкоротший шлях. Якщо цей шлях стає недоступним, Router 3 знаходить другого наступника (Router 2 – Router 1 – Router 5 – Network A) і використовує його, поки найкоротший шлях знову не стане доступним. Таблиця порівняльних характеристик протоколів динамічної маршрутизації наведена у додатку А.

2.1.4 Налаштування VLAN

VLAN (англ. Virtual Local Area Network – віртуальна локальна комп'ютерна мережа) – є групою хостів з загальним набором вимог, що взаємодіють так, ніби вони прикріплені до одного домену, незалежно від їх фізичного розташування [10][2)]. І навпаки, пристрої, що знаходяться в різних VLAN, невидимі один для одного на канальному рівні, навіть якщо вони підключені до одного комутатора, і зв'язок між цими пристроями можливий тільки на мережевому і більш високих рівнях. VLAN використовуються для групування мережевих пристроїв та іншого обладнання відповідно до типу даних або правил безпеки, якими вони користуються.

У сучасних мережах VLAN – головний механізм для створення логічної топології мережі, що не залежить від її фізичної топології. VLAN використовуються для скорочення широкомовного трафіка в мережі. Мають

[1)] [9] Буров Є.В. Комп’ютерні мережі// Підручник Львів: Магнолія 2006, 2013. 262 с.

[2)] [10] Virtual Local Area Network – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/VLAN (дата звернення 13.03.2019)

велике значення з точки зору безпеки, зокрема як засіб боротьби з ARP-spoofing.

Віртуальні локальні мережі ефективно застосовуються при вирішення наступних проблем:гнучкого поділу пристроїв на групи; зменшення кількості широкомовного трафіка в мережі; збільшення безпеки і керованості мережі.

Найбільш поширеним способом реалізації є VLAN на основі портів. Коли пристрій підключено до порту, що належить до певної VLAN, цей пристрій автоматично стає членом цієї VLAN. Якщо необхідно однієї VLAN зв'язуватися з іншою VLAN, то для цього налаштовують транкові порти. Транковий порт – це порт на комутаторі, який зайнятий трафіком VLAN за допомогою транкових протоколів. Найбільш поширеним транковим протоколом є IEEE 802.1Q. Кадр 802.1Q містить ідентифікатор VLAN, який допомагає визначити, до якої віртуальної мережі належить трафік.

Транковий порт працює в транковому режимі (trunk mode) – один з декількох режимів комутації, доступних під час налаштування VLAN. Інші режими – режим доступу (access mode), динамічний автоматичний режим (dynamic auto mode) і динамічний бажаний режим (dynamic desirable mode). Порт, налаштований з режимом доступу, здійснює трафік, до якого належить тільки VLAN, до якого призначений порт. Транковий порт передає трафік для декількох VLAN. Порт, налаштований з динамічним автоматичним режимом, залишається в режимі доступу, якщо його не просять стати транком. Порт в динамічному бажаному режимі стає транком, якщо порт з іншого боку також погоджується бути транком. Зазвичай використовуються тільки режим trunk та режим access [11][1)].

Можна призначити різні порти на різних комутаторах до однієї VLAN. Це корисно, коли пристрої підключені до різних комутаторів, але вони все ще належать до однієї VLAN і дотримуються тих самих правил. Рішенням для цього є тегування кадрів (рис.1.5). Чотири байта вводяться в заголовок

[1)] [11] Абрамов В.О., Клименко С.Ю. Базові технології комп’ютерних мереж. Навчальний посібник. К: Київ. ун-т ім. Б.Грінченка, 2011. 291 с.

пакету Ethernet – два байта – це Tag Protocol Identifier, який використовується як сповіщення про те, що дані VLAN є наступними, а ще два байти – Tag Control Information (TCI). У TCI, три байти надаються User Priority levels – нуль є найнижчим рівнем пріоритету, а сім є найвищим рівнем пріоритету. Canonical Format Indicator або CFI задається одним бітом: цей індикатор використовується для забезпечення сумісності між мережею Ethernet і мережею Token Ring. Останні дванадцять бітів надані ідентифікатору VLAN. Отже, якщо тег реалізований, тегированний пакет з одного комутатора переходить на інший, а потім другий комутатор шукає той же ідентифікатор VLAN, що і в заголовку пакета [12][1)].

Рисунок 1.5 – Структура тега 802.1Q

Тим не менш, можливо, що пакет може прийти не тегований. Це означає, що порт, з якого він прийшов, теж не має тегів – він належить до native VLAN, яка в мережі може бути тільки одна, або комутатори не зможуть зрозуміти, до якої VLAN вони повинні пересилати нетеговані пакети.

1.1.5 Налаштування NAT / PAT

У випадку коли існує лише одна публічна IP-адреса, що надається компанії, необхідно реалізувати або трансляцію мережевих адрес (NAT, Network Address Translation), або трансляцію порт-адреса (PAT, Port Address Translation). Трансляція мережевих адрес – це технологія, яка дозволяє пев-

[1)] [12] Николайчук Я.М., Возна Н.Я., Пітух І.Р. Проектування спеціалізованих комп'ютерних систем. Навчальний посібник. Тернопіль.: ТзОВ «Терно-граф», 2010. 394 с.

ному мережевому пристрою, брандмауеру або маршрутизатору, представляти інший пристрій у приватній мережі, коли він працює в загальнодоступній мережі. З NAT можна використовувати одну публічну IP-адресу, навіть якщо в локальній мережі існує більше одного пристрою. Ця технологія відображає IP-адресу в одній мережі (в нашому випадку, LAN) на IP-адресу в іншій мережі (публічна IP-адреса в Інтернеті) [13][1)].

Існує два типи трансляції мережевих адрес. Перший тип – це статичний NAT, найпростіший з усіх типів. Статичний NAT використовує один-на-один трансляцію IP-адреси. Іншими словами, в локальній мережі існує одна конкретна IP-адреса, яка відображається в конкретній IP-адресі в Інтернеті. Другий, динамічний NAT дозволяє конфігурувати статичні записи NAT автоматично, на ходу, створюючи пул адрес на внутрішній локальній мережі та аналогічний пул на зовнішній локальній мережі. Таким чином, відображення один на один створюється автоматично і, отже, багато часу зберігається у випадку, якщо в пулах адрес існують численні записи.

Більш просунутим інструментом є перевантаження NAT або трансляція порт–адреса (PAT). Цей інструмент дозволяє декільком користувачам зсередини LAN використовувати одну IP-адресу на зовнішній мережі. Для цього перевантаження NAT використовує не тільки внутрішні IP-адреси, але й номери портів, щоб відрізнити одного користувача від іншого. Кожному хосту з внутрішньої локальної мережі присвоюється номер порту, який виступає як вихідний порт і порт призначення [14][2)].

1.1.6 Налаштування DHCP

DHCP (англ. Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла) – це методом, розробленим з Bootstrap прото-

---

[1)] [13] Network Address Translation – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/NAT (дата звернення 13.03.2019)

[2)] [14] Port Address Translation – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/PAT (дата звернення 13.03.2019)

колом і використовуваний для передачі необхідних конфігурацій через мережу TCP/IP. DHCP може автоматично призначати IP-адреси та інші конфігурації хостам мережі. DHCP працює на основі клієнт/сервер, де сервер надає клієнтам попередньо виділені мережеві адреси.

DHCP може працювати різними способами. По-перше, адміністратор мережі надає DHCP-сервер з відповідною IP-адресою вручну, а потім сервер пересилає адресу хосту. По-друге, DCHP-конфігурований сервер може призначити постійну мережеву адресу хосту в мережі. Останнім шляхом є динамічне виділення: сервер DHCP надає хосту IP-адресу протягом обмеженого часу, який називається орендою. Також можна створити пул відповідних IP-адрес і призначити хостам динамічні мережеві адреси [15][1)].

По-першу адміністратор повинен створити пул доступних IP-адрес, а потім IP-адреса призначається клієнту протягом певного часу. Після закінчення цього часу сервер знову призначає IP-адресу – не обов'язково ту саму, що була раніше. Час оренди може бути продовжений клієнтом, а також адміністратором динамічно. Перевага цього методу полягає в тому, що немає необхідності призначати IP-адресу вручну кожному хосту в мережі. З іншого боку, програмне забезпечення відстежує вільні IP-адреси та призначає одну з них хосту, який підключається до локальної мережі.

Процес призначення IP-адреси відносно простий. По-перше, клієнт надсилає в мережу широкомовний пакет DISCOVER, що дозволяє серверу DCHP узнати, що існує хост, який вимагає конфігурації мережі. Після цього сервер DCHP надсилає OFFER пакет з необхідною інформацією про оренду. Коли клієнт підтверджує пакет OFFER, він посилає пакет REQUEST на сервер, який відповідає пакетом ACK. Інформація про мережу отримується, і робоча станція клієнта тепер є членом мережі.

[1)] [15] Dynamic Host Configuration Protocol – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/PAT (дата звернення 13.03.2019)

1.2 Кінцеві пристрої

1.2.1 Конфігурації ПК

Хорошим рішенням є зменшення кількості різних версій ОС, встановлених на комп'ютерах, таким чином адміністратор мережі витрачає значно менше часу на налаштування ПК. Те ж саме стосується програмного забезпечення та драйверів – комп'ютери можуть не підтримувати останню версію або користувачі не потребують її для своєї роботи. Проте, коли більшість PC компанії (або, принаймні, певної групи) використовують одне і те ж програмне забезпечення, переміщення між ПК або усунення несправностей не є проблемою ні для користувачів, ні для адміністраторів.

Важливе значення мають апаратні конфігурації. Маленькі компанії часто не готові розлучатися з грошима і підвищувати продуктивність PC, які вони вже мають. Тим не менш, в певний момент ПЗ, яке використовує компанія, буде оновлено і потребує більше сучасного процесора або більше пам'яті на жорстких дисках. Крім того, один з компонентів PC може вийти з ладу і пошкодити важливі дані. Таким чином, оновлення апаратних засобів є неминучими, а іноді важливими для безпеки даних і темпів роботи компанії.

1.2.2 Конфігурації сервера

Існують певні відмінності між сервером і ПК як апаратні, так і програмні. Хоча загальні апаратні конфігурації майже однакові, деякі компоненти є більш потужними, ніж у ПК. CPU сервера зазвичай складається з декількох ядер і великого кешу. Метою кеш-процесора є зберігання даних, які використовуються частіше, ніж інша інформація. Теж стосується і дискової підсистеми. У сервера є кілька дисків. Більш того, вони зазвичай налаштовані як один логічний диск. Ця функція називається RAID. Її мета полягає в захисті даних, які зберігаються на сервері від збоїв диска. Якщо

один з дисків переходить в автономний режим, інший диск все ще має необхідні дані. У серверах зазвичай використовуються кілька рівнів RAID.

RAID 0 розбиває дані на смуги і записує їх на два або більше дисках без інформації про паритет або відмовостійкість. RAID 0 використовується, коли метою є продуктивність, а не безпека даних. У разі виходу з ладу одного диска, масив також виходить з ладу, і дані втрачаються, оскільки вони зберігаються на всіх дисках.

RAID 1 використовує дзеркальне копіювання для забезпечення відмовостійкості: дані записуються на два диски одночасно, а якщо один диск виходить з ладу, інший надає користувачам дані. Цей метод використовується, коли продуктивність читання є більш важливою, ніж оптимальне використання зберігання даних.

RAID 5 – один з найпоширеніших рівнів RAID – він передає дані та дані паритету на декілька дисків. У разі виходу з ладу одного диска дані можуть бути відновлені з інформації про парність, яка зберігається на іншому диску. Крім того, продуктивність читання краща, оскільки всі диски беруть участь у виконанні запитів на читання.

RAID 6 використовує той самий принцип, що і RAID 5, але, на відміну від RAID 5, інформація про парність подвоюється. Іншими словами, RAID 6 може пережити не один, а два збою. Продуктивність читання така ж хороша, як у RAID 5, але процес запису займає більше часу через розрахунки паритету [16][1)].

Інша відмінність серверів – це оперативна пам'ять – оскільки сервер виконує кілька операцій і програм одночасно, потрібно багато оперативної пам'яті для швидкого обслуговування користувачів. Основним принципом RAM є той самий, але в серверах ECC RAM використовується для забезпечення цілісності даних, коли дані обробляються в RAM.

[1)] [16] Горбатий І. В., Бондарєв А. П. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи. Навчальний посібник Львів.: Видавництво Львівської політехніки, 2016. 336 с.

Форм-фактор сервера може сильно відрізнятися від звичайних ПК. Коли в компанії є декілька серверів, зазвичай використовується спеціальна стійка. Однак, якщо компанія досить мала або потрібні лише один або два сервери, використовується форм-фактор башти. Як правило, сервери налаштовують через мережу і часто не мають вхідних і вихідних пристроїв, але у випадку, якщо компанія невелика, а серверів не так вже й багато, звичайно простіше налаштувати сервер за допомогою монітора і клавіатури, ніж мережевого інтерфейсу. Однак, в будь-якому випадку сервер має принаймні один гігабітний мережевий інтерфейс, як правило, два.

1.3 Конфігурації безпеки

Під «мережевою безпекою» мають на увазі не тільки безпеку кінцевих пристроїв, які обмінюються інформацією, але і мережу між ними, включаючи мережеве обладнання та його налаштування. Крім того, необхідно враховувати такі фактори: доступ – можливість уповноважених осіб користуватися мережею; конфіденційність – дані в мережі не доступні для тих, кому це не дозволено; аутентифікація – користувачі повинні довести, що вони є такими, якими вони є; цілісність – дані не були змінені під час передачі; невідмовлення – користувач не заперечує своїх дій в мережі.

Хоча мережеві загрози та атаки постійно розвиваються, можна виділити декілька їх типів.

Прослуховування – процес збору даних, коли вони передаються по дротах. Зазвичай прослуховування виконується за допомогою певного типу програмного забезпечення, що називається пакетним сніфером, програми, яка може слухати і записувати дані, що проходять через кабель LAN. Перехват також використовується з бездротовими передачами. Кабелі з оптичних волокон вважаються найбезпечнішими серед інших, оскільки вони не мають електричних сигналів у своїх передачах.

TCP session hijacking – суть цієї атаки полягає в тому, щоб спочатку взяти сесію TCP, яка вже створена, а потім заповнити її пакетами, які обробляються іншим хостом, так якщо б вони надходили від фактичного учасника сесії. Щоб взяти на себе сеанс TCP, зловмисник повинен спочатку вгадати послідовний номер пакета, який в даний час передається через мережу – використовуючи сніфери пакетів або пробуючи всі можливі варіанти. Коли зловмисник знаходиться в мережі і починає відправляти свої власні пакети, сервер підтверджує ці пакети і посилає пакет ACK новим порядковим номером, який, швидше за все, не очікується клієнтом. Клієнт повинен ресинхронізуватись з сервером і відправити пакет ACK з новим номером послідовності – цього разу він несподіваний для сервера. Процес надсилання та повторного надсилання пакетів ACK називається атакою шторму TCP ACK. Це може різко зменшити продуктивність мережі і знизити клієнтське з'єднання з сервером.

Атака «Людина посередині» або Man-In-The-Middle – зловмисник читає, модифікує і змінює дані між двома сторонами, не знаючи, що в мережі є хтось інший. Щоб досягти цього, зловмисник повинен отримати відкритий ключ однієї з сторін, надіслати іншій стороні повідомлення зі своїм відкритим ключем, отримати пакет від іншої сторони з зашифрованим повідомленням, розшифрувати його власним закритим ключем і надіслати його назад першій стороні з її розкриттям відкритого ключа. Суть цього нападу полягає в тому, що Людина посередині може змінити інформацію, отриману від другої сторони [17][1)].

Отруєння DNS – мета полягає в тому, щоб змінити таблицю DNS на сервері, щоб клієнт не знав, що дані надсилаються на ненадійний сервер, оскільки доменне ім'я є однаковим, але IP-адреса не є такою. Таким чином,

[1)] Б. А. Демида, К. М. Обельовська, В. С. Яковина Основи адміністрування LAN у середовищі MS Windows Навчальний посібник Львів.: Видавництво Львівської політехніки, 2013. 488 с.

робоча станція клієнта може отримувати підроблені пакети з неправильного сервера з шкідливим програмним забезпеченням всередині.

Distributed Denial of Service або DDoS атака – ця атака вимагає значної кількості робочих станцій по всьому Інтернету – іноді навіть тисяч – для встановлення програмного забезпечення, такого як Low Orbit Ion Cannon, а потім треба замовити ці машини для запуску програмного забезпечення та початку атаки. Цей тип атаки використовується для переповнення пропускної здатності мережі з подібними запитами, такими як ping-пакети, так що сервер остаточно перестає реагувати не тільки на зловмисників, але й на всіх інших [18][1)].

2 ПРОЕКТУВАННЯ ЛОКАЛЬНО-ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

У цьому розділі кваліфікаційної роботи перелічимо технології та принципи, які будуть реалізовані в мережі, щоб вирішити проблеми, які були описані раніше.

2.1 Ресурси компанії

2.1.1 Кінцеві пристрої

Компанія розташована на двох поверхах будівлі – першому і третьому. Другий поверх займає інша компанія, яка не має відношення до бізнесу «АСТ-Світлотехніка». На першому поверсі – чотири офісні приміщення та головний склад. Інші офіси знаходяться на третьому поверсі. План на рис. 2.1 показує, як кінцеві пристрої та мережні розетки розміщені в будівлі.

[1)] Мінухін С. В. Кавун С. В. Знахур С.В. Комп'ютерні мережі. Загальні принципи функціонування комп’ютерних мереж. Навчальний посібник Харків: Вид. ХНЕУ, 2008. 210 с.

Апаратні конфігурації ПК компанії дещо відрізняться, але загальна продуктивність і способи використання майже однакові. Є також два принтери: один з них включений в мережу і розміщений в кімнаті 304, інший знаходиться в кімнаті 302, але не використовується спільно з іншими ПК.

Відповідно до плану, в даний час існує двадцять два комп'ютери з наступними конфігураціями (приблизно):

– CPU: AMD Sempron 2650, AM1, 1.45GHz, Radeon HD 8240, 2-core;
– Motherboard: MSI AM1I, AM1, DDR3, mITX;
– RAM: 2x A-Tech 1GB DDR3 PC3-10600 Desktop Memory Module;
– HDD: 120 Gb Generic 2.5 SATA Internal Hard Drive;
– Power Supply: EVGA 400 N1, 400W Continuous Power;
– Case: HP XW4600 Tower Case.

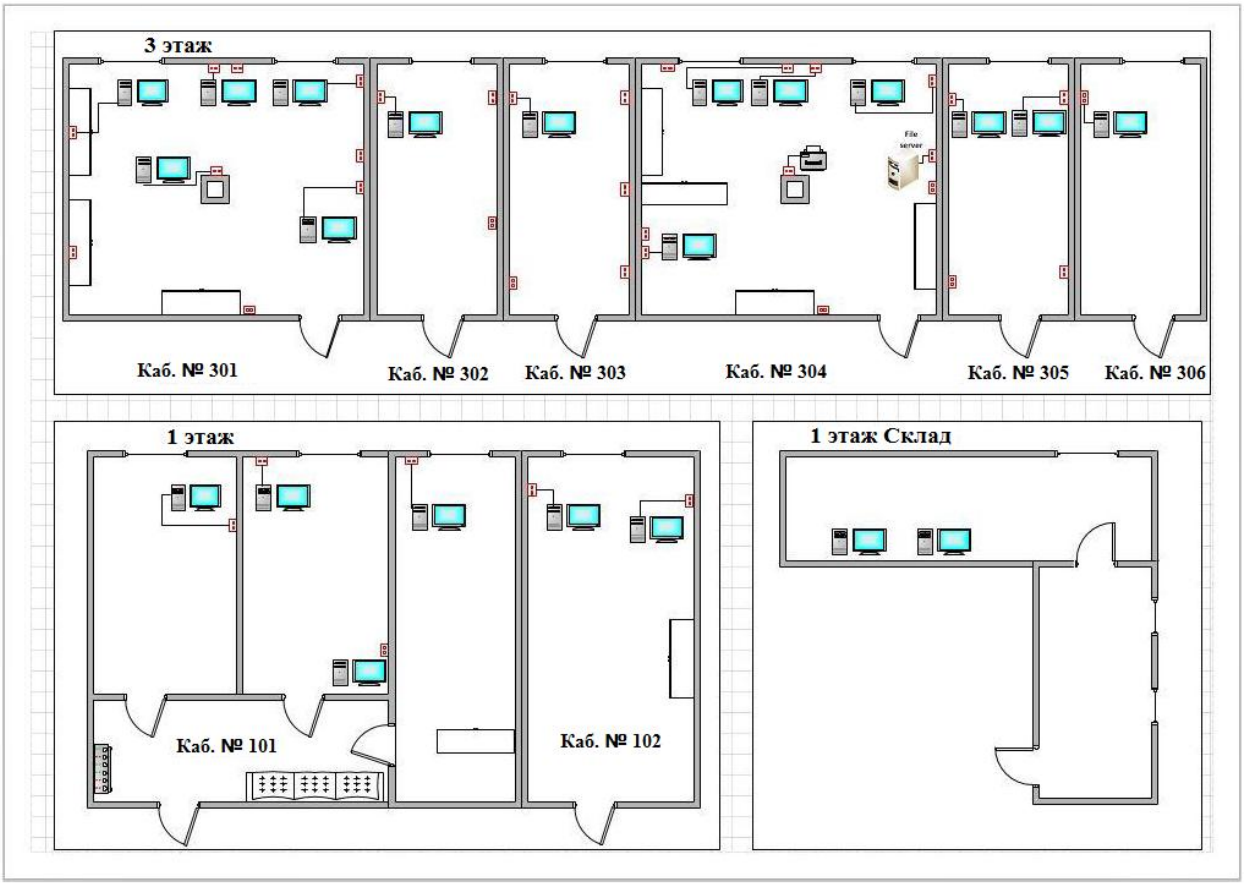

Рисунок 2.1 – Схема розташування кінцевих пристроїв мережі

Як видно на схемі мережі, є двадцять третій ПК. Однак він використовується як файловий сервер. Апаратні конфігурації приблизно такі ж, як і у двадцяти двох комп'ютерів. Не встановлено і налаштовано жодної серверної ОС, не реалізовані розширені правила або функції безпеки. Однак існує спільний доступ до файлів, які можна отримати, модифікувати та видалити з інших ПК.

2.1.2 Схема мережі

Компанія має одну загальнодоступну IP-адресу, яку вони орендують у Інтернет-провайдера. Їх локальна мережа складається з одного маршрутизатора і трьох комутаторів, які підключені відповідно до загальної топології мережі (рис. 2.2).

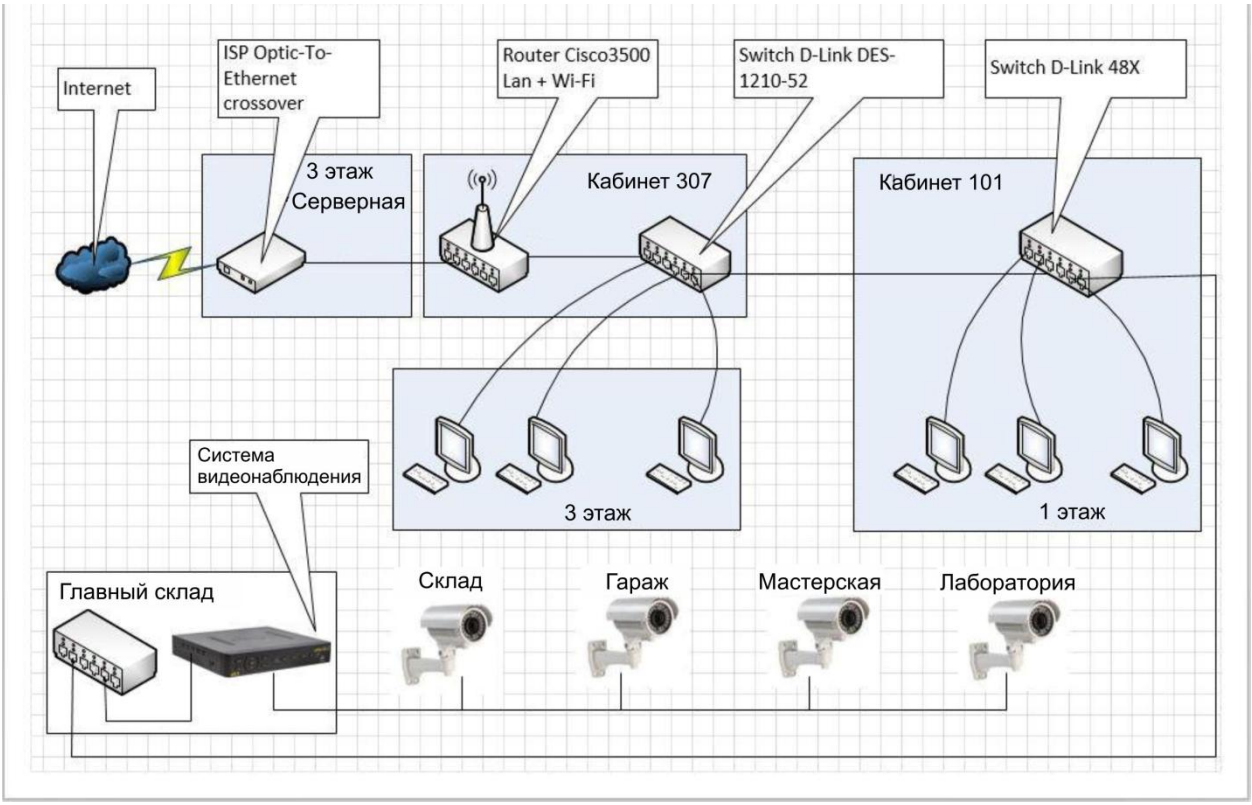

Рисунок 2.2 – Схема мережі

Маршрутизатор підключений до першого комутатора на третьому поверсі, цей комутатор підключений до першого комутатора на першому поверсі будівлі, і, нарешті, цей комутатор підключений до останнього комутатора, який розміщений в головному складі на першому поверсі. Вся інформація по мережевому обладнанню компанії наведена у таблиці 2.1.

Таблиця 2.1 – Інформація про поточне мережеве обладнання ЛОМ організації

Підключення обладнання	Протяжність кабелю, м	Обладнання	Номер порту	Розташування
Обладнання 1-го поверху				
Switch Asus (16 ports) – Switch D-link (48 ports)	21	Switch Asus (16 ports)	3	склад
Switch D-link (48 ports) – Switch D-link DES 1210-52 (48 ports)	35	Switch D-link (48 ports)	2	каб. 101
Обладнання 3-го поверху				
Switch D-link DES 1210-52 (48 ports) – Router Cisco 3500 LAN+Wi-Fi (4 ports)	7	Switch D-link DES 1210-52 (48 ports)	1	каб. 307
Router Cisco 3500 LAN+Wi-Fi – ISP Optic-To-Ethernet crossover	9	Router Cisco 3500 LAN+Wi-Fi (4 ports)	WAN	каб. 307

2.2 Конфігурації мережі

У цьому розділі будуть запропоновані деякі вдосконалення для сучасного дизайну мережі. Деякі методи не підтримуються поточним обладнан-

ням, яке вже налаштовано для цієї мережі, тому є необхідність у виборі нового мережевого обладнання.

Почнемо з топології мережі компанії. Відповідно до схеми мережі, яку було надано компанією, поточна топологія мережі є розширеною топологією зірка (рис. 2.3). Комутатор S1 являє собою комутатор третього поверху, комутатор S2 являє собою комутатор лабораторії на першому поверсі і комутатор S3 являє собою комутатор майстерні (робочого цеху) на першому поверсі.

Аналогічно, комп’ютери синьої зони, з'єднаної з S1, являють собою робочі станції на третьому поверсі, зеленої зони, з'єднаної з S2 – комп'ютери лабораторії, а помаранчевої зони, з'єднаної з S, – комп'ютери майстерні. Однак цій топології не вистачає надмірності, що дуже важливо для працівників компанії.

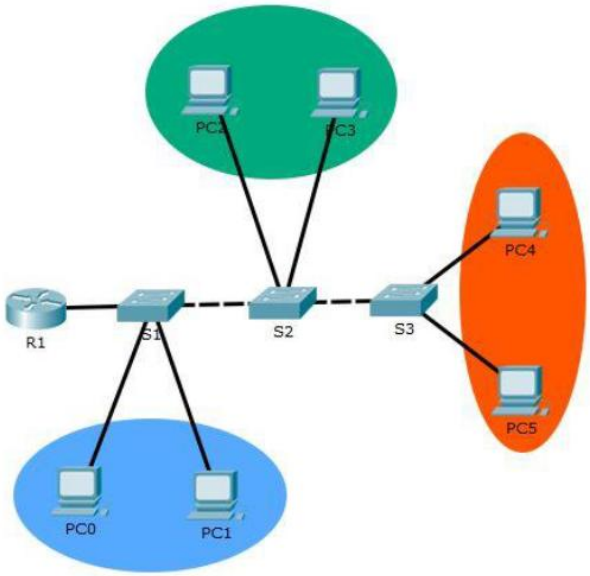

Рисунок 2.3 – Поточна топологія мережі

Наприклад, якщо другий комутатор S2 відключається, не тільки лабораторія втрачає зв'язок з локальною мережею та Інтернетом, а також майстерня та її комп'ютери. Враховуючі ці проблеми, найбільш ефективна топологія для мережі компанії наведена на рис.2.4.

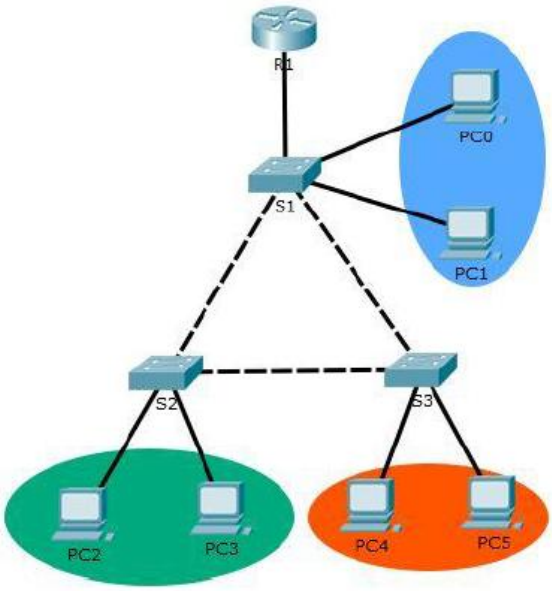

Рисунок 2.4 – Нова топологія мережі

Три комутатори з'єднані за допомогою топології сітки. Однак у цьому випадку, якщо зв'язок між двома комутаторами не працює, дані не втрачаються, а надсилаються по іншому.

Зміни в топології мережі потребують зміни кабельного зв'язку. Кабелі мережі компанії будуються відповідно до поточної топології мережі. Використовується кабель UTP CAT5 на третьому поверсі будівлі та в лабораторії на першому поверсі. Однак у зоні головного складу розведений кабель STP для запобігання електромагнітних і перехресних перешкод у кабелях. Оскільки топологія мережі змінена, для підключення комутаторів потрібно більше кабелів, тому компанії рекомендується придбати приблизно 60 метрів кабелю UTP CAT5e.

Після внесення необхідних змін у топологію мережі та підключення кабелів, схема мережі прийме вигляд такий, як це показано на рис.2.5, де третій комутатор поверху знаходиться у верхньому лівому кутку з назвою S1 і підключений до чотирнадцяти робочих станції, комутатор лабораторії S2 знаходиться в нижньому лівому куті і з'єднує разом шість лабораторних ро-

бочих місць, а комутатор майстерні S3 знаходиться в нижньому правому куті зображення, з'єднуючи два комп'ютери в мережу.

На рис.2.5 показаний тільки один маршрутизатор у всій мережі. Це означає, що в даний час немає необхідності в реалізації будь-яких протоколів маршрутизації. Однак у випадку розширення компанії доцільно попередньо вибрати маршрутизатор, який підтримує принаймні найпоширеніші протоколи маршрутизації, такі як OSPF і EIGRP, згадані раніше. Як відповідний приклад маршрутизатора був обраний відремонтований маршрутизатор Cisco 1841 з двома портами LAN і підтримкою протоколів маршрутизації BGP, OSPF, EIGRP і RIP. Придбати нове обладнання завжди надійніше. Проте, у випадку невеликої компанії типу «АСТ-Світлотехніка», нове обладнання Cisco є занадто дорогим для покупки. Замість цього було запропоновано компанії придбати відремонтований маршрутизатор, ціна якого значно нижча, але якість все ще висока.

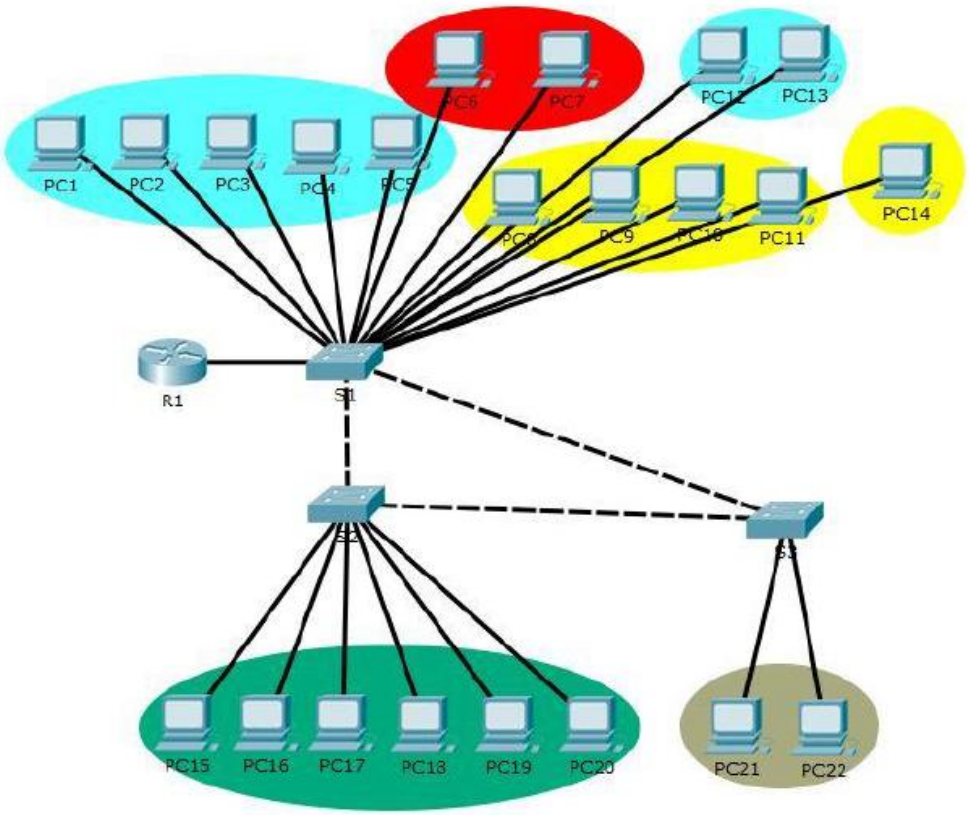

Рисунок 2.5 – Схема підключення робочих станцій в мережі

Аналогічно, з кількох причин було вирішено вибрати три Cisco 2950-24 відремонтованих комутаторів. По-перше, ця модель комутатора має 24 порту 10/100 Мбіт /с, що достатньо для поточного стану мережі компанії. Хоча існують більш просунуті комутатори практично за однакову ціну, але функції, які роблять їх більш досконалими (наприклад, підтримка оптичного кабелю), в даний час не потрібні для компанії.

Комутатори потребують конфігурацій VLAN. У мережі працює п'ять груп користувачів – головний відділ з двома користувачами (VLAN 10), відділ досліджень і розвитку із сімома користувачами (VLAN 20), відділ маркетингу та продажів з п'ятьма користувачами (VLAN 30), відділ лабораторії із семи користувачів (VLAN 40) і відділ головного складу і з двома користувачами (VLAN 50). Також native VLAN 1 і VLAN 99 для керування мережею. У табл. 2.2 наведений список VLAN.

Таблиця 2.2 – Список VLAN

№ VLAN	VLAN name	Примітка
1	default	Не використовується
10	Office	Для користувачів Головного офісу
20	RDD	Для користувачів Відділу досліджень і розвитку
30	MSD	Для користувачів Відділу маркетингу та продажів
40	Laboratory	Для користувачів лабораторії
50	Storehouse	Для користувачів складу
99	Management	Для керування мережею

Для цього проекту було вирішено налаштувати DHCP для декількох VLAN. Спочатку ідея полягала в тому, щоб налаштувати VLAN і призначити кожному користувачеві IP-адресу вручну. Проте, якщо в компанії буде більше робочих місць і більше користувачів, підхід до ручного керування бу-

де важким і трудомістким. Замість цього, було вирішено використовувати сабінтерфейси (subinterfaces) маршрутизатора і призначити IP-адреси автоматично, вибираючи їх з пулу доступних IP-адрес. Перелік сабінтерфейсів маршрутизатора наведений у табл.2.2.

Таблиця 2.2 – Перелік налаштованих сабінтерфейсів маршрутизатора

INTERFACE	IP ADDRESS	№ VLAN
FastEthernet0/0	10.10.1.1/24	1
	10.10.10.1/ 24	10
	10.10.20.1/24	20
	10.10.30.1/24	30
	10.10.40.1/24	40
	10.10.50.1/24	50
	10.10.99.1/24	99

Щоб зробити роботу DHCP, необхідно включити сабінтерфейс, потім включити інкапсуляцію, вказати конкретний номер VLAN, для якого встановлено DHCP, а потім вказати IP-адресу для сабінтерфейсу.

```
R1(config)# interface FastEthernet0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 10.10.10.1 255.255.255.0
```

Аналогічно, інші чотири сабінтерфейси:

```
R1(config)# interface FastEthernet0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 10.10.20.1 255.255.255.0
R1(config)# interface FastEthernet0/0.30
R1(config-subif)# encapsulation dot1Q 30
R1(config-subif)# ip address 10.10.30.1 255.255.255.0
R1(config)# interface FastEthernet0/0.40
R1(config-subif)# encapsulation dot1Q 40
R1(config-subif)# ip address 10.10.40.1 255.255.255.0
R1(config)# interface FastEthernet0/0.50
R1(config-subif)# encapsulation dot1Q 50
R1(config-subif)# ip address 10.10.50.1 255.255.255.0
```

Також була встановлена native VLAN 1 і VLAN 99 для керування мережею наступним чином:

```
R1(config)# interface FastEthernet0/0.1
R1(config-subif)# encapsulation dot1Q 1 native
```

```
R1(config-subif)# ip address 10.10.1.1 255.255.255.0
R1(config)# interface FastEthernet0/0.99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# ip address 10.10.99.1 255.255.255.0
```

Після цього необхідно налаштувати інтерфейси комутаторів як транкових портів – інтерфейсів, що несуть трафік з різних VLAN одночасно. У нашому випадку, транкові інтерфейси – це комутатор S1 порт Fa0/1, порт Fa0/2 і порт Fa0/4, комутатор S2 порт Fa0/2 і порт Fa0/3 і комутатор S3 порти Fa0/3 і порт Fa0/4.

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config)# interface FastEthernet0/2
S1(config-if)# switchport mode trunk
S1(config)# interface FastEthernet0/4
S1(config-if)# switchport mode trunk
S2(config)# interface FastEthernet0/2
S2(config-if)# switchport mode trunk
S2(config)# interface FastEthernet0/3
S2(config-if)# switchport mode trunk
S3(config)# interface FastEthernet0/3
S3(config-if)# switchport mode trunk
S3(config)# interface FastEthernet0/4
S3(config-if)# switchport mode trunk
```

Крім того, для кожного з комутаторів треба встановити інтерфейс керування VLAN. Керування VLAN, як правило, використовується для доступу до функцій комутаторів віддалено – через Telnet або SSH – і для зміни конфігурацій, якщо це необхідно.

```
S1(config)# interface vlan 99
S1(config-if)# ip address 10.10.99.10 255.255.255.0
S1(config)# ip default-gateway 10.10.99.1
S2(config)# interface vlan 99
S2(config-if)# ip address 10.10.99.20 255.255.255.0
S1(config)# ip default-gateway 10.10.99.1
S3(config)# interface vlan 99
S3(config-if)# ip address 10.10.99.30 255.255.255.0
S1(config)# ip default-gateway 10.10.99.1
```

Далі, потрібно призначити порти, які використовуються робочими станціями для відповідних VLAN. План підключення по портах проміжних мережевих пристроїв наведений в табл. 2.3.

Порти від 10 до 14 і порти 21 і 22 на комутаторі S1 належать VLAN 20, порти 15 і 16 – до VLAN 10, порти від 17 до 20 і порту 23 – до VLAN 30. Порти від 10 до 15 на S2 належить до VLAN 40. Нарешті, порти 10 і 11 на S3 належать до VLAN 50.

Таблиця 2.3 – План підключення по портах проміжних мережевих пристроїв

Ім’я пристрою	Порт	Назва	VLAN	
			Access	Trunk
gw1	FE0/0	UpLink		
	FE0/1	sw1		1,10,20,30,40,50,99
sw1	FE0/1	gw1		1,10,20,30,40,50,99
	FE0/2	sw2		1,10,20,30,40,50,99
	FE0/4	sw3		1,10,20,30,40,50,99
	FE0/5, FE0/7	LACP		1,10,20,30,40,50,99
	FE0/10-FE0/14, FE0/21,FE0/22	RDD	20	
	FE0/15,FE0/16	Office	10	
	FE0/23	MSD	30	
sw2	FE0/2	sw1		1,10,20,30,40,50,99
	FE0/3	sw3		1,10,20,30,40,50,99
	FE0/5, FE0/6	LACP		1,10,20,30,40,50,99
	FE0/10-FE0/15	Laboratory	40	
sw3	FE0/3	sw2		1,10,20,30,40,50,99
	FE0/4	sw1		1,10,20,30,40,50,99
	FE0/6, FE0/7	LACP		1,10,20,30,40,50,99
	FE0/10,FE0/11	Storehouse	50	

Наступні конфігурації показують призначення портів на S1:

```
interface FastEthernet0/10
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/11
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/12
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/13
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/14
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/15
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/16
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/17
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/18
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/19
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/20
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/21
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/22
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/23
switchport access vlan 30
switchport mode access
spanning-tree portfast
```

Аналогічні конфігурації застосовуються до комутатора S2 і комутатора S3. Тут використовується командний рядок spanning-tree portfast і збільшується швидкість присвоєння IP адрес за допомогою DHCP. Однак, щоб запобігти виникненню циклів у мережі, також був включений BPDU Guard.

Для цієї мережі необхідні п'ять різних пулів DHCP. Вирішено використовувати нову мережу для кожного з пулів – мережу 10.10.10.0/24 для VLAN 10, мережу 10.10.20.0/24 для VLAN 20, мережу 10.10.30.0/24 для VLAN 30, мережу 10.10.40.0/24 для VLAN 40 і мережу 10.10.50.0/24 для VLAN 50. План IP-адресації представлений в табл.2.4.

Наступні конфігурації описують кожен пул оголошень для кожної VLAN:

```
ip dhcp pool Head
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
ip dhcp pool R&D
network 10.10.20.0 255.255.255.0
default-router 10.10.20.1
ip dhcp pool M&S
network 10.10.30.0 255.255.255.0
default-router 10.10.30.1
ip dhcp pool Lab 31
network 10.10.40.0 255.255.255.0
default-router 10.10.40.1
ip dhcp pool WS
network 10.10.50.0 255.255.255.0
default-router 10.10.50.1
```

Таблиця 2.4 – План IP-адресації

Пул IP-адрес	Примітка	VLAN
10.10.10.0/24	Office	10
10.10.20.0/24	RDD	20
10.10.30.0/24	MSD	30
10.10.40.0/24	Laboratory	40
10.10.50.0/24	Storehouse	50

Одним з варіантів, які можуть бути корисними, є виключення перших десяти IP-адрес з кожного пулу. Причиною цього може бути новий пристрій, підключений до мережі, або просто необхідність запасної IP-адреси. Проте відповідальна особа компанії дала зрозуміти, що ці заходи не є необхідними, оскільки навряд чи в найближчому майбутньому будуть підключені нові пристрої. Після цього всі пристрої в мережі мають IP-адреси з пулів IP-адрес, де вони належать. Нижче наведена робоча станція з головного відділу з IP-адресою з пулу для VLAN 10 і робоча станція з відділу лабораторії з IP-адресою з пулу для VLAN 30. На рис.2.6 показано правильно призначені IP-адреси.

Наступне, що було вирішено здійснити, це трансляцію NAT. Для простоти проектування та впровадження мережі зручно використовувати динамічний NAT, оскільки інтернет-провайдер надає компанії тільки одну загальнодоступну IP-адресу, але в локальній мережі є багато приватних IP-адрес.

Щоб налаштувати трансляцію NAT або PAT, необхідно спочатку встановити внутрішній інтерфейс і зовнішній інтерфейс. Для внутрішнього інтерфейсу є порт Fa0/0 на R1. Аналогічно, для зовнішнього інтерфейсу є порт Fa0/1 на тому ж R1.

```
R1(config)# interface FastEthernet0/0
R1(config-if)# ip nat inside
R1(config)# interface FastEthernet0/1
R1(config-if)# ip nat outside
```

Після цього необхідно налаштувати ACL, що включає приватні IP-адреси з локальної мережі. ACL необхідний для переліку певного хоста в локальній мережі. Потім ACL застосовується до конфігурації трансляції NAT.

```
R1(config)# ip nat inside source list 1 interface
FastEthernet0/1 overload
```

У попередній команді зазначається, що джерело IP-адрес, які знаходяться на внутрішньому інтерфейсі, знаходяться в списку номер один, а зовнішній порт для цих конфігурацій – порт FastEthernet0/1.

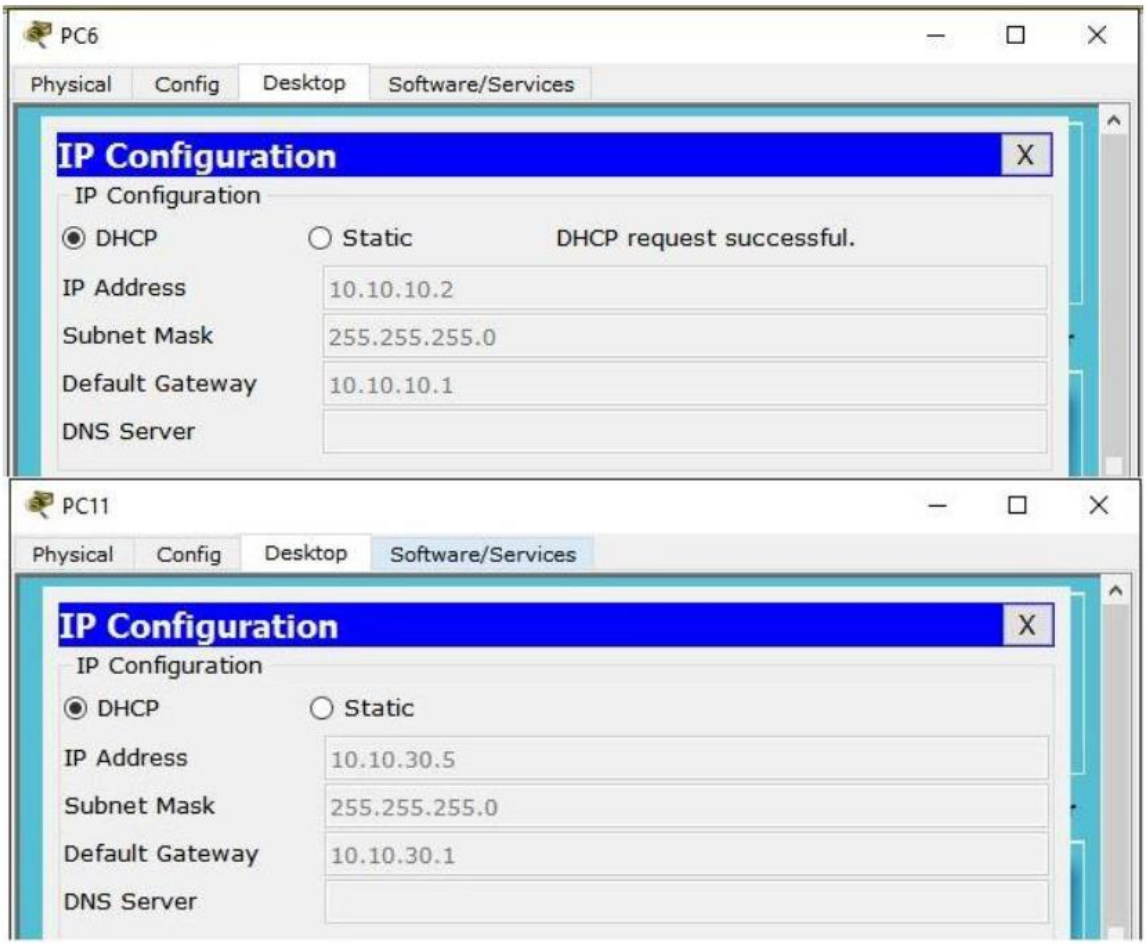

Рисунок 2.6 – Налаштування DHCP для різних VLAN

Також було вирішено налаштувати агрегацію каналів, тобто реалізувати протокол LACP (Link Aggregation Control Protocol) між комутаторами. Протокол LACP дозволяє об'єднати декілька зв'язків між двома пристроями в один логічний, щоб збільшити безпеку та пропускну здатність каналу зв'язку. Це означає, що у випадку, якщо одна ланка не працює, інша займає своє місце, не перериваючи з'єднання. Щоб реалізувати LACP, необхідно поставити порти майбутнього з’єднання в стан транка. Оскільки на кожному з комутаторів вже є два транкових порти, необхідно включити ще два порти на кожному з комутаторів і налаштувати режим транкінгового з'єднання. Для S1 обрані порти Fa0/2 і Fa0/5, щоб був зв'язок з S2 з портами Fa0/2 і Fa0/5 відповідно. Для зв'язку між S2 і S3 обрані порти Fa0/3 і Fa0/6 з обох сторін. Для зв'язку між S3 і S1 обрані порти Fa0/4 і Fa0/7 з обох сторін.

Після того, як необхідні порти були ввімкнені і переведені в режим транкових, були об’єднані порти кожного зв’язку в один канал з активним режимом.

```
S1(config)# interface Fa0/5
S1(config-if)# switchport mode trunk
S1(config)# channel-group 1 mode active
S1(config)# no shutdown
```

Такі ж конфігурації застосовуються до інших портів зв'язку між першим і другим комутаторами. Зв'язок між другим і третім комутаторами здійснюється груповим номером 2, в той час як зв'язок між першим і третім комутаторами здійснюється груповим номером 3. Після внесення цих змін в топологію мережна схема виглядає так, як показано на рис.2.7.

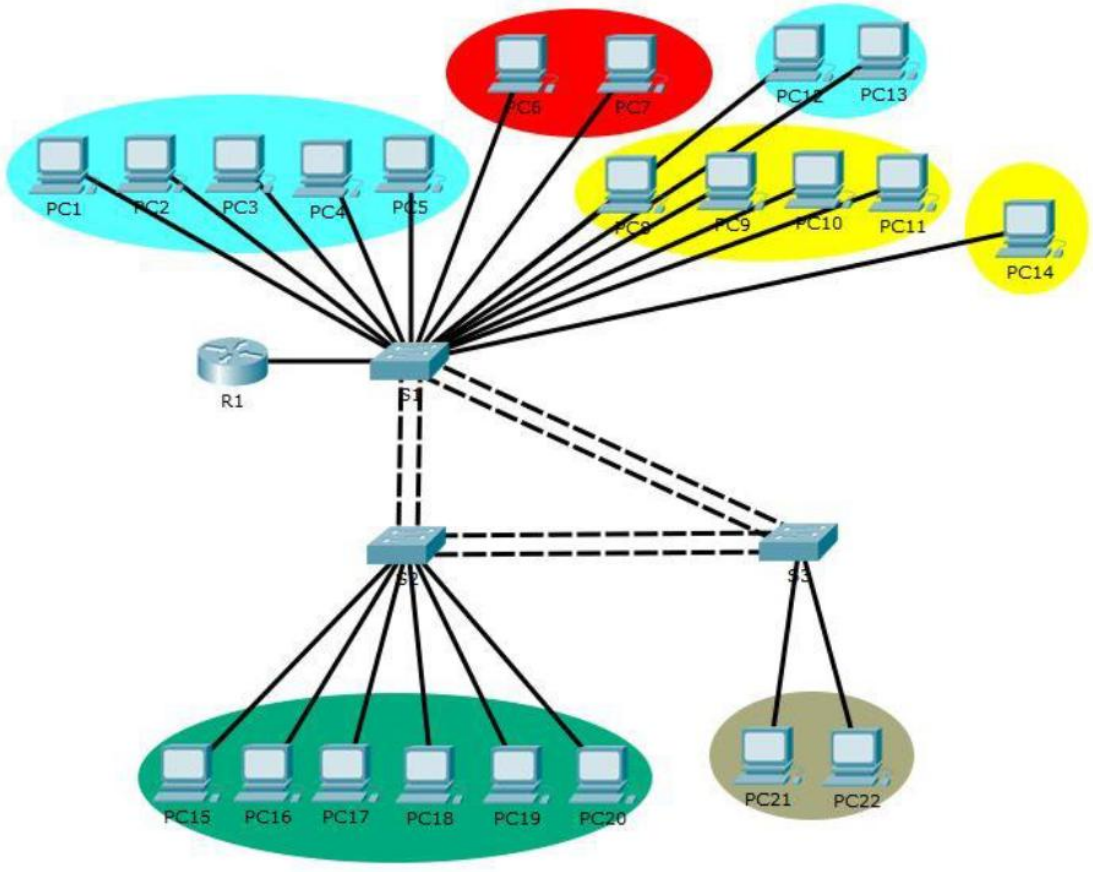

Рисунок 2.7 – Вдосконалена схема топології мережі

Групи каналів також видно через команду show etherchannel:

```
S1#show etherchannel
Channel-group listing:
----------------------
Group: 1
```

```
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP 34
Group: 3
----------
Group state = L2
Ports: 2 Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol: LACP
```

2.3 Кінцеві пристрої

2.3.1 Конфігурації ПК

Єдине, що було згадано про конфігурації ПК, це те, що в них встановлено кілька різних операційних систем. Наприклад, два ноутбуки, які належать до головного відділу, мають встановлені на них Windows XP, тоді як найпотужніший комп'ютер у відділі досліджень і розробок має Windows 7. В цілому, є шість ПК з Windows 7 і чотирнадцять ПК з Windows XP. «Файловий сервер» також має Windows XP.

Хоча різні операційні системи можуть значно збільшити час для зняття проблем, або пошуку необхідних драйверів та програм, у випадку цієї компанії вирішено залишити операційні системи таким, яким вони є зараз. Насправді, деякі комп'ютери навряд чи можуть керувати Windows 7. Існує ще один варіант – практично будь-який вільний дистрибутив Linux може бути встановлений на ці комп'ютери, так що вони можуть працювати навіть трохи швидше, ніж зараз, але це займе багато часу для користувачів, щоб пристосуватися до нової операційної системи і звикнути до нових команд і функцій.

Однак, було вирішено змінити чотири старі ноутбуки (два головного відділу і два відділу досліджень і розробок) на ПК, оскільки апаратна конфігурація цих ноутбуків не може вирішувати багато повсякденних завдань, таких як кілька вікон браузера. Апаратні конфігурації цих ПК наведені в табл. 2.5.

Таблиця 2.5 – Нові конфігурації комп’ютерів

Обладнання	Назва
CPU	Intel Celeron G4900 CoffeLake (BX80684G4900)
Motherboard	Asus H110M-CS/C/SI Bulk (H110M-CS/C/SI Bulk)
RAM	TEAM 4 GB DDR4 2400 MHz
SSD	Team L5 240Gb 3D Gold
Power supply	EVGA 400 N1, 400W Continuous Power
Case	P XW4600 Tower Case

Орієнтовна вартість одного ПК з апаратними конфігураціями, переліченими в таблиці 2.5, не перевищує 150 євро, припускаючи, що компанія має чотири запасні копії операційної системи Windows 7.

Проте нові комп'ютери потребують нового програмного забезпечення, такого як простий офісний пакет для роботи з таблицями, текстами та презентаціями, а також нові антивірусні програми. Інформація про антивірус, а також про інші заходи безпеки буде надана у наступній частині роботи. Для офісного пакету рекомендуємо використовувати LibreOffice 6.2.1. Ця версія є останньою стабільною на даний момент і вона безкоштовна для використання. LibreOffice візуально дуже схожий на програми Microsoft Office, тому користувачі не витрачають багато часу, щоб звикнути до нового програмного забезпечення.

Також було запропоновано деякі нові правила та зміни до звичайного способу ведення справ в компанії. Перш за все, рекомендуємо включити функцію, яка завантажує критичні оновлення для операційної системи, але вимкнути функцію, яка автоматично встановлює їх. Таким чином, комп'ютери користувачів будуть мати очікувані оновлення, але системний адміністратор закріпить їх замість користувачів. Це рішення допоможе запобігти практично всі проблеми людського фактора під час установки (наприклад, випадково вимкнення ПК під час оновлення). Є й інший спосіб:

системний адміністратор може віддалено оновлювати кожен ПК без переходу з одного офісу в інший. Проте цей параметр вимагає віддаленого підключення до ПК користувачів, таких як Windows Remote Desktop Connection, TeamViewer або подібне програмне забезпечення. Також рекомендуємо, щоб системний адміністратор встановлював не тільки оновлення, а й необхідне програмне забезпечення замість користувачів. Так можна відстежувати встановлені програми та запобігати виникненню проблем у процесі встановлення.

2.3.2 Конфігурації сервера

Як вже було згадано раніше, є ще один ПК. Його основною метою є надання іншим користувачам даних зі спільної папки. Наскільки відомо, користувачам дозволяється створювати, модифікувати та видаляти файли в цій папці. Немає інших дозволів для цих файлів і жодних інших цілей для цього ПК. Апаратні конфігурації цього ПК такі ж, як і інші комп'ютери, однак не встановлено жодної серверної ОС. Отже, технічно це не зовсім правильно називати цей комп'ютер сервером, хоча є кілька рішень цієї проблеми.

По-перше, можна встановити ОС сервера (можливо, Windows Server 2012) замість звичайної користувальницької ОС. Таким чином можна налаштувати функції безпеки, такі як дозволи, групи користувачів і обмеження, щоб доступ до документа контролювався. З одного боку, це рішення є більш безпечним, ніж те, що вже реалізовано, оскільки серверна ОС, як правило, краще підходить для роботи з багатьма користувачами, ніж ОС користувача. З іншого боку, це рішення може вимагати додаткових витрат на нове обладнання, оскільки сучасне обладнання не є найбільш надійним.

Існує кілька типів дозволів, які можна встановити на файли та/або папки на сервері. Ці дозволи існують для визначення рівня доступу до певного документа або папки і, якщо необхідно, для його обмеження. Типи дозволів і функції відхиляються також від типу папки, встановленої адміністратором

або іншою відповідальною особою. Найбільш поширеними є дозвіл загального доступу (share permissions) та дозвіл NTFS. Відмінність між ними видно, коли користувач звертається до потрібного файлу різними способами. Якщо користувач має дозвіл загального доступу, він може отримати доступ до файлу – від своєї робочої станції за допомогою певної папки. Якщо користувач має дозвіл NTFS, він може отримати доступ до файлу під час входу на сервер.

Налаштування дозволу Share можуть бути: «Read», «Change» або «Full Control». Зрозуміло, що дозвіл «Read» не допускає будь-яких змін у файлі, а дозвіл «Change» дозволяє переписувати, але не переміщати або видаляти файл. «Full Control» дає користувачеві можливість читати, писати, змінювати або видаляти файл. На рис.2.8 наведено приклад дозволів загального доступу до певної папки.

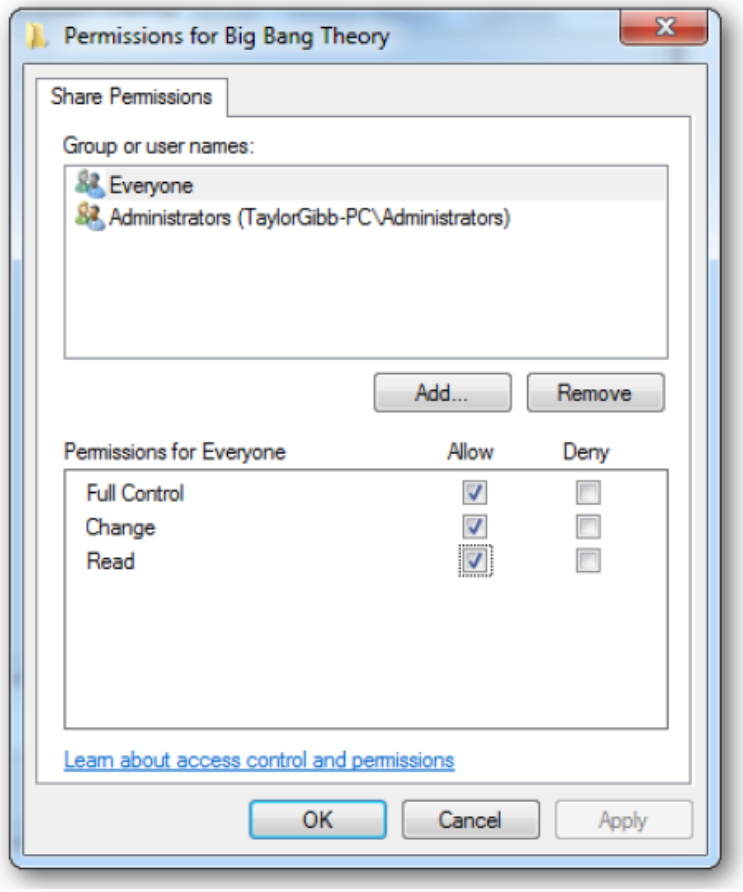

Рисунок 2.8 – Налаштування дозволу загального доступу

Дозволи NTFS більш різноманітні. Хоча дозволи Read та Full Control такі ж, як і для дозволів загального доступу, інші – різні. List Folder Contents дозволяє користувачам переглядати всередині папки, Write дозволяє їм додавати нові файли. Read та Execute дозволяє переглядати самі файли та запускати їх, а Modify дозволяє змінювати файли у вказаній папці. Різниця між дозволами Share і NTFS видно на рис.2.9.

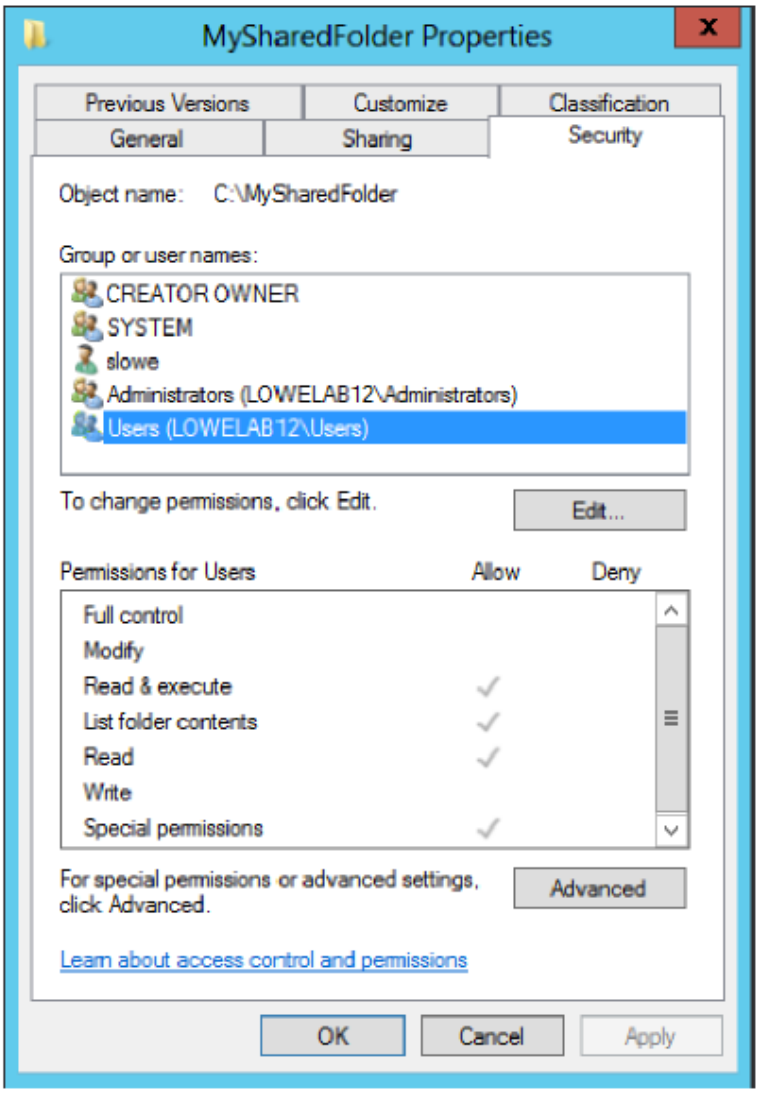

Рисунок 2.9 – Налаштування дозволу NTFS

Щоб визначитися з правом доступу до файлу, ОС Windows враховує обидва набори місій: Share і NTFS. Однак у випадку конфлікту дозволів пе-

реважають суворіші правила або набір правил. Наприклад, якщо дозвіл загального доступу дозволяє доступ до папки, але правила NTFS говорять про її відсутність, користувач не матиме доступу до цієї папки.

Інше рішення – розмістити потрібну папку з документами на найнадійнішому комп'ютері та налаштувати папку з папкою Share, яка використовується для обміну папками та дисками по мережі. Список дозволів, однак, значно коротший – читання або читання і запис. Це дає менше контролю над діями користувачів, але не вимагає великих зусиль для налаштування. Таким чином можна зафіксувати файли до певної міри, а також дозволити спільний доступ до не-Windows-ПК.

Третій і найменш надійний варіант – залишити конфігурацію ПК, як вони є, і налаштувати відповідні обмеження на спільну папку. Однак це не є прийнятним рішення, тому що, цей ПК має тенденцію перезавантажуватися сам і в цілому працює повільніше, ніж інші. Але це найдешевший варіант, тому що компанії не потрібно буде нічого витрачати. Однак попередній варіант здається більш надійним, він також є безкоштовним.

Гадаємо, що зручніше реалізовувати спільну папку на новому комп'ютері замість використання старого ПК або інсталяції серверної ОС. Причина полягає в тому, що для встановлення та налаштування серверної операційної системи потрібна достатня кількість часу, але для копіювання файлів на новий ПК і створення спільної папки потрібно набагато менше часу. Також нерозумно робити сервер зі старого ПК, тому що його апаратні конфігурації навряд чи підходять для цього. Тому для того, щоб зробити сервер необхідно побудувати новий набір апаратних конфігурацій і це коштує грошей. Проте їх можна зберегти, виконавши спільну папку на новому ПК.

Хоча місце, де зберігаються файли, є ПК, необхідно застосувати деякі додаткові правила для обмеження фізичного доступу до ПК та налаштування спільного доступу. Рекомендуємо надавати дозвіл «Full Control» обліковому запису адміністратору і дозволяти йому віддалений доступ до ПК, щоб заощадити час і налаштовувати все з його офісу.

2.4 Конфігурації безпеки

2.4.1 Фізична безпека мережі

Хоча безпеку мережі не слід сприймати легковажно, але мережеві пристрої компанії можуть бути забезпечені краще.

Зараз в мережі компанії, пристрої практично неможливо відрізнятися один від одного, і кабелі злегка переплутані. Також, можна відкрити замок кімнати будь-яким ключем з кімнат одного поверху. Це може бути зручно до певної міри в розумінні того, що весь час має доступ до пристроїв, але це також є великою загрозою безпеці для мережі. Пропонуємо, щоб замок для цієї двері був замінений на унікальний. Крім того, вважаємо більш доцільним, щоб тільки адміністратор мережі мав фізичний доступ до цієї кімнати і пристроїв, які знаходяться всередині.

Має місце занепокоєння не тільки станом безпеки самих пристроїв, а й дротів. Це неприємно, коли провід неможливо відрізнити один від одного. Однак, коли дроти та розетки знаходяться в розладі, це може призвести до серйозної небезпеки, наприклад, короткого замикання або навіть пожежі.

Крім того, вважаємо за необхідне запровадити систему маркування. У мережі не так вже й багато кінцевих пристроїв, а отже, не так багато дротів, але все ще можна змішувати дроти, якщо вони не в порядку.

Система маркування проста у використанні і допомагає відстежувати фізичні підключення на мережевому пристрої. Суть цієї системи полягає в тому, щоб назвати кожний провід, підключений до пристрою, і накласти на нього наклейку з її назвою.

Також добре покласти пристрої в закриту стійку з замком на ній. Тим не менш, все ще можна зберегти хороший рівень безпеки без блокування пристроїв.

2.4.2 Безпека мережі на основі програмного забезпечення

Існує декілька способів запобігання поширенню мережі від зловмисних програм і атак. Все більше і більше передових технологій постійно розвиваються. Але, у випадку цієї компанії важливо думати не тільки про функції безпеки, але й про ціну пристроїв, що їх підтримують.

Пропоную увімкнути функції безпеки, такі як BPDU Guard на комутаторах, щоб запобігти петлям і проблемам підключення в мережі. Модуль захисту даних протоколу Bridge запобігає отриманню порту (зазвичай порту зовнішньої лінії) від прийому одиниць даних протокольного протоколу протоколу Spanning-Tree. Однак порт здатний посилати STP BPDU. Коли порт отримує STP BPDU, він переходить у стан, відключений від помилок, і може бути знову ввімкнено вручну. Це означає, що, якщо до мережі підключено несанкціонований комутатор, порт зовнішньої лінії отримує повідомлення BPDU від цього комутатора і переходить у стан відключення, водночас запобігаючи переходу пакетів даних з нового комутатора в мережу. Це звичайний спосіб захисту мережі. Наполегливо рекомендую також використовувати паролі для запобігання несанкціонованому доступу до консолі. Паролі повинні відрізнятися один від одного (привілейовані та глобальні режими конфігурації), і вони повинні бути достатньо довгими, щоб не можна було підібрати. Для регулювання складності паролів для мережних і кінцевих пристроїв може бути створена політика паролів.

2.4.3 Фізична безпека кінцевих пристроїв

Як вже було згадано раніше, кімнати, де знаходяться комп'ютери, зазвичай блокуються, якщо в неї нікого немає. Вони також закриті протягом ночі. Крім того, будівля має політику обмеження доступу, так що кожен, хто входить у приміщення, використовує карту доступу на вхідних дверях

будівлі. Фізична безпека кінцевих пристроїв знаходиться на пристойному рівні, що підходить для компанії з певними розмірами та завданнями.

2.4.4 Безпека програмного забезпечення кінцевих пристроїв

Існує багато способів захистити інформацію, що зберігається на ПК користувачів. Пропоную встановити на кожному комп'ютері компанії антивірусну програму. Рекомендую використовувати або безкоштовне антивірусне програмне забезпечення, як Avira, або комерційні, такі як Avast або Syman-tec. Це антивірусне програмне забезпечення зазвичай надає кінцевому користувачеві набір правил, обмежень і перевірок, які допомагають користувачеві зберігати дані в безпеці. Як вже говорили раніше, установка повинна бути запущена адміністратором мережі, щоб запобігти можливим проблемам під час процесу.

Інша практика полягає у використанні пароля для входу, щоб запобігти доступу до будь-якого неавторизованого персоналу. Я вважаю, що пароль повинен містити принаймні вісім символів довжини та суміжні літери верхнього та нижнього регістрів, принаймні один номер і принаймні один символ. Крім того, паролі потрібно змінювати кожні два-два місяці. Цей період може бути дещо змінений у випадку будь-яких непередбачених ситуацій.

ВИСНОВКИ

Метою кваліфікаційної роботи було вдосконалення існуючої локальної мережі компанії ТОВ «АСТ-Світлотехніка» за рахунок впровадження нового програмного та апаратного забезпечення, що базуються на сучасних телекомунікаційних технологій.

В ході дослідження поточної топології мережі і характеристик існуючого обладнання, стало зрозуміло, що локальні та мережеві пристрої компанії можуть бути змінені та оновлені. Мережа побудована з використанням топології шини – досить популярна, але недостатньо захищена. Крім того, всі комп'ютери використовували кілька версій операційних систем, а також різне програмне забезпечення. В роботі була розроблена нова топологія мережі, включаючи нові налаштування мережі та запропоновані деякі покращення для кінцевих пристроїв.

Теоретична частина дослідження містить основні методи та принципи, які використовуються в сучасних ЛОМ малих і середніх компаній. Хоча були перераховані прості у впровадженні і досить просунуті методи, мета практичної частини полягала не тільки в покращенні існуючої мережі, а й у використанні простих і зрозумілих методів. Причина цього полягає в тому, що співробітники компанії зосереджені в основному на ринкових успіхах компанії а не в області IT освіти. Тому метою розробки було створити мережевий дизайн, який одночасно є корисним і простим в обслуговуванні. Це також причина, уникнення будь-яких технологій, які важко зрозуміти і налаштувати – наприклад, Linux або Active Directory.

У практичній частині роботи був створений мережевий прототип для компанії. Для цього було використане реальне обладнання, а також програмне забезпечення Packet Tracer 6.2. Остаточна версія мережі була виконана в Packet Tracer за допомогою технологій, які перераховані у теоретичній частині. В мережі виконано налаштування протоколу DHCP та VLAN. Наведені таблиці підключення по портах, перелік VLAN, та пулів IP-адрес.

Також були запропоновані деякі методи для поліпшення поточного стану ПК, наприклад, використання однакових версій програмного забезпечення, зміна чотирьох старих комп'ютерів і ноутбуків на нові і блокування мережевих пристроїв в офісі, в якості міри безпеки. У майбутньому треба спростити обслуговування мережі та зробити її більш безпечною. На ПК краще реалізувати ОС Linux, яка працює як файловий сервер.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. Комп’ютерні мережі. Навчальний посібник Вінниця: ВНТУ, 2013. 371 с.
2. О. Ю. Зайченко, Ю. П. Зайченко Комп'ютерні мережі Підручник К.: Видавничий Дім «Слово», 2010. 520 с.
3. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп’ютерні мережі. Книга 2. Навчальний посібник. Львів: Магнолія 2006, 2014. 328 с.
4. Border Gateway Protocol – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/BGP (дата звернення 13.03.2019)
5. Routing Information Protocol – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/Routing_Information_Protocol (дата звернення 13.03.2019)
6. Open Shortest Path First Protocol – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/OSPF (дата звернення 13.03.2019)
7. В.Чернега, Б. Платтнер Компьютерные сети. Навчальний посібник Севастополь: Вид-во СевНТУ, 2006. 500 с.
8. Enhanced Interior Gateway Routing Protocol – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/EIGRP (дата звернення 13.03.2019)
9. Буров Є.В. Комп’ютерні мережі. Підручник Львів: Магнолія 2006, 2013. 262 с.
10. Virtual Local Area Network – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/VLAN (дата звернення 13.03.2019)
11. Абрамов В.О., Клименко С.Ю. Базові технології комп’ютерних мереж. Навчальний посібник. К: Київ. ун-т ім. Б.Грінченка, 2011. 291 с.
12. Николайчук Я.М., Возна Н.Я., Пітух І.Р. Проектування спеціалізованих комп’ютерних систем. Навчальний посібник. Тернопіль.: ТзОВ «Терно-граф», 2010. 394 с.

13. Network Address Translation – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/NAT (дата звернення 13.03.2019)
14. Port Address Translation – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/PAT (дата звернення 13.03.2019)
15. Dynamic Host Configuration Protocol – Вікіпедія. (загол. з екрану). URL: https://uk.wikipedia.org/wiki/PAT (дата звернення 13.03.2019)
16. Горбатий І. В., Бондарєв А. П. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи. Навчальний посібник Львів.: Видавництво Львівської політехніки, 2016. 336 с.
17. Б. А. Демида, К. М. Обельовська, В. С. Яковина Основи адміністрування LAN у середовищі MS Windows Навчальний посібник Львів.: Видавництво Львівської політехніки, 2013. 488 с.
18. Мінухін С. В. Кавун С. В. Знахур С.В. Комп'ютерні мережі. Загальні принципи функціонування комп’ютерних мереж. Навчальний посібник Харків: Вид. ХНЕУ, 2008. 210 с.

ДОДАТОК А

Порівняльна характеристика протоколів маршрутизації

Таблиця А.1 – Порівняльна характеристика протоколів динамічної маршрутизації

Критерії	RIP	IGRP	OSPF	EIGRP
1	2	3	4	5
Безпека	Відкритий пароль чи аутентифікація по ключу MD5	–	Відкритий пароль чи аутентифікація по ключу MD5	Аутентифікаціяпо ключу MD5
Тип алгоритму	Вектор відстані	Вектор відстані	Стан каналов зв’язку	Комбінований
Балансування навантаження	–	Різні метрики	Однакові метрики	Різні метрики
Об’єднання маршрутів	–	–	+	+
Маска підмереж змінної довжини	+	–	+	+
Максимальна кількість маршрутизаторів в мережі	15	255	65534	255
Підтримка IPv6	–	–	+	+
Доступність реалізації	Відкритость	Тільки на обладнанні Cisco	Відкритий	Тільки на обладнанні Cisco
Врахування у метриці різних характеристик	Одна основна	Комбінована	Одна основна і три додаткові	Комбінована
Оновлення маршрутної інформації	Вся таблиця	Вся таблиця	Тільки зміни	Тільки зміни

Продовження таблиці А.1

1	2	3	4	5
Максимальна кількість маршрутизаторів в мережі	15	255	65534	255
Підтримка IPv6	–	–	+	+
Доступність реалізації	Відкритость	Тільки на обладнанні Cisco	Відкритий	Тільки на обладнанні Cisco
Врахування у метриці різних характеристик	Одна основ-на	Комбінована	Одна основ-на і три додаткові	Комбінована
Оновлення маршрутної інформації	Вся таблиця	Вся таблиця	Тільки зміни	Тільки зміни