МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
комп'ютерних систем та мереж

_____ Ігор ЖУКОВ
"_____"_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Локальна комп'ютерна мережа навчального закладу»

Виконавець: _____ Дмитрій НЕДІЛЬКО
(підпис)

Керівник: _____ Юрій ПУШКІН
(підпис)

Нормоконтролер: _____ Сергій ЖУРАВЕЛЬ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет комп’ютерних інформаційних технологій
Кафедра комп’ютерних систем та мереж
Спеціальність 123 «Комп’ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп’ютерних систем та мереж

Ігор ЖУКОВ
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Неділька Дмитрія Романовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Локальна комп'ютерна мережа навчального закладу»
затверджена наказом ректора від «26» квітня 2023 р. № 591/ст
2. Термін виконання роботи: з 22.05.2023 р. по 25.06.2023 р.
3. Вихідні дані до роботи: аналіз конфігурації мережевого обладнання; вибір топології локальної мережі; вибір способу управління мережею; вибір технологій з’єднань; проектування комп’ютерної мережі в кабінетах
4. Зміст пояснювальної записки: основні поняття комп’ютерних мереж та їх технологій; безпека комп’ютерних мереж; моделювання мережі навчального закладу в програмному пакеті Huawei eNSP
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: слайди презентації в програмному пакеті Microsoft PowerPoint

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	22.05.2023-24.05.2023	Виконано
2	Вступ	25.05.2023	Виконано
3	ОСНОВНІ ПОНЯТТЯ КОМП’ЮТЕРНИХ МЕРЕЖ ТА ЇХ ТЕХНОЛОГІЙ	26.05.2023-29.05.2023	Виконано
4	БЕЗПЕКА КОМП’ЮТЕРНИХ МЕРЕЖ	30.05.2023-07.06.2023	Виконано
5	МОДЕЛЮВАННЯ МЕРЕЖІ НАВЧАЛЬНОГО ЗАКЛАДУ В ПРОГРАМНОМУ ПАКЕТІ HUAWEI ENSP	08.06.2023-14.06.2023	Виконано
6	Усунення недоліків та захист кваліфікаційної роботи	15.06.2023-16.06.2023	Виконано

7. Дата видачі завдання: “22" травня 2023 р.

Керівник кваліфікаційної роботи _____ Юрій ПУШКІН
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Дмитрій НЕДІЛЬКО
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Локальна комп'ютерна мережа навчального закладу» містить 64 сторінки, 25 рисунків, 7 таблиць, 17 використаних джерел.

МЕРЕЖА, БЕЗПЕКА, ЗАХИСТ, ПРОЕКТУВАННЯ, ТОПОЛОГІЇ, АТАКА, DDoS, eNSP, VLAN, З'ЄДНАННЯ, КАМПУС, МОНІТОРИНГ, МАРШРУТИЗАТОР.

Об'єкт дослідження –. комп'ютерна мережа навчального закладу.

Предмет дослідження –. локальна комп'ютерна мережа.

Мета кваліфікаційної роботи –. створення комп'ютерної мережі для начального закладу.

Метод дослідження –. проєктування мереж, методи обчислення, методи аналізу комп'ютерних мереж.

Технічні та програмні засоби – середовище проєктування мереж draw.io. Huawei eNSP (Enterprise Network Simulation Platform) - це програмне забезпечення, розроблене компанією Huawei, яке використовується для моделювання та симуляції комп'ютерних мереж.

Прогнозні припущення щодо розвитку об'єктів розроблення – модернізація та розширення комп'ютерної мережі.

Матеріали кваліфікаційної роботи рекомендується використовувати для оновлення та удосконалення існуючої мережевої інфраструктури, впровадження нових рішень та розробки стратегії розвитку мережі, а також, можуть бути корисні адміністраторам, які відповідають за планування, розгортання та управління локальною комп'ютерною мережею навчального закладу.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

LAN	-	Local Area Network
WAN	-	Wide Area Network
MAN	-	Metropolitan Area Network
UTP	-	Unshielded Twisted Pair
FDDI	-	Fiber Distributed Data Interface
CSMA/CD	-	Carrier Sense Multiple Access with Collision Detection
IP	-	Internet Protocol
NAT	-	Network Address Translation
DDoS	-	Distributed Denial of Service
SSL	-	Secure Sockets Layer
eNSP	-	Enterprise Network Simulation Platform
OSPF	-	Open Shortest Path First
BGP	-	Border Gateway Protocol
MPLS	-	Multiprotocol Label Switching
VLAN	-	Virtual Local Area Network
DHCP	-	Dynamic Host Configuration Protocol
Wi-Fi	-	Wireless Fidelity
WPA	-	Wi-Fi Protected Access
AES	-	Advanced Encryption Standard
IDS	-	Intrusion Detection System
IPS	-	Intrusion Prevention System
VPN	-	Virtual Private Network
SSID	-	Service Set Identifier
ВВП	-	Валовий Внутрішній Продукт

ВСТУП

Актуальність теми. В даній роботі буде спроба розробити проект локальної комп'ютерної мережі, навчального закладу. Навчальний заклад в цьому випадку це – звичайна школа I-III ступенів. За рахунок правильного проектування і налагодження комп’ютерної мережі, в класах інформатики покращиться працездатність і підвищиться надійність мережі. Відповідно це поліпшить освітній процес для школярів і роботу для вчителів, буде налагоджена передача даних між комп’ютерами в класах, що значно вплине на зручність та правильність роботи.

Локальна комп'ютерна мережа (LAN - Local Area Network) - це мережа, яка охоплює обмежену територію, таку як будівля, офіс, школа або кампус. У локальній мережі можуть бути підключені різні пристрої, такі як комп'ютери, принтери, маршрутизатори, комутатори, маршрутизатори, медіаплеєри та інші.

Кожен пристрій в мережі має свою власну адресу, відому як IP-адреса. За допомогою мережевих протоколів, таких як TCP/IP, пристрої можуть взаємодіяти між собою, обмінюватися даними та ресурсами, такими як файли, друк, доступ до Інтернету та інші.

Зв’язок роботи з науковими програмами, планами, темами.

Мета і завдання дослідження. – створити комп’ютерну мережу для начального закладу.

Для досягнення поставленої мети вирішуються такі наукові завдання:

– вибір топології локальної мережі;

– вибір способу управління мережею;

– конфігурація мережевого обладнання;

– вибір технологій з’єднань;

– проектування комп’ютерної мережі в кабінетах;

– розрахунок витрат на створення мережі.

Об’єктом дослідження – є комп’ютерна мережа навчального закладу.

Предметом дослідження – є локальна комп’ютерна мережа.

Методи досліджень. проєктування мереж, методи обчислення, методи аналізу комп’ютерних мереж.

Практичне значення отриманих результатів.

Матеріали роботи даної рекомендується використовувати для оновлення та удосконалення існуючої мережевої інфраструктури, впровадження нових рішень та розробки стратегії розвитку мережі, а також, можуть бути корисні адміністраторам, які відповідають за планування, розгортання та управління локальною комп'ютерною мережею навчального закладу.

РОЗДІЛ 1
ОСНОВНІ ПОНЯТТЯ КОМП'ЮТЕРНИХ МЕРЕЖ ТА ЇХ ТЕХНОЛОГІЙ

1.1. Комп'ютерні мережі

Комп'ютерні мережі - це сукупність комп'ютерів, розподілених на деякій території і об'єднаних для спільного використання ресурсів (даних, програм і апаратних компонентів).

Головна мета, яка обґрунтовує об'єднання комп'ютерів у мережу це - надання користувачам доступу до різних інформаційних ресурсів (наприклад, документам, програмам, базам даних і т.д.), які розподілені по цих комп'ютерам. Найважливішою характеристикою будь-якої комп'ютерної мережі є площа території, яку вона охоплює. Площа охоплення визначається взаємною віддаленістю комп'ютерів, які утворюють мережу і відповідно визначає тип мережі, отже, впливає на технологічні рішення, технології побудови і обладнання які були обрані при проектуванні.

Комп'ютерні мережі, створенні для передачі даних чи обміну інформації є результатом інформаційної революції. Всесвітня тенденція до об'єднання комп'ютерів у мережу обумовлена прискоренням передачі інформаційних повідомлень, можливістю швидкого обміну інформацією між користувачами, одержанням і передачею повідомлень (наприклад, e-mail-листів, електронних конференцій і т.д.), не відходячи від робочого місця, а також можливістю миттєвого одержання будь-якої інформації з будь-якої точки земної кулі.

На сьогоднішній день існуючі мережі ділять в першу чергу за територіальною ознакою. Простими словами - яка відстань між комп'ютерами в тій чи інший мережі.

Основні типи комп'ютерних мереж:

1. Локальна мережа (LAN - Local Area Network). До локальних комп'ютерних мереж відносять ті мережі, комп'ютери яких зосереджені на відносно невеликих територіях (менше 2000 м) [1]. Прикладом локальної мережі є мережа будь-якого навчального закладу (школи, університету і т.д.), яка розташована в межах однієї

лише будівлі і не має відносно великої відстані між комп’ютерами, невеликого офісу, який розташовано в одному або декількох будівлях. За рахунок невеликого розміру локальних мереж можна використовувати для їх побудови досить дорогі і високоякісні технології, що забезпечує високу швидкість обміну інформацією між комп'ютерами. Це і є головною перевагою локальної мережі цього типу.

2. Глобальна мережа (WAN - Wide Area Network – це комп’ютерна мережа, яка побудована на основі комутованих або виділених каналах існуючих мереж [2]. До терміну глобальних відносять мережі, призначені для об'єднання окремих комп'ютерів і локальних мереж, розташованих на значній відстані (сотні і тисячі кілометрів) один від одного. Прикладом глобальної комп’ютерної мережі є підприємство, яке має філіали чи офіси, в різних містах, чи може навіть країнах. Враховуючи велику відстань між комп’ютерами в глобальній мережі, дійшли висновку, що, організація спеціальних та якісних каналів зв'язку великої протяжності є досить дорогою, тому в мережах такого типу нерідко можна зустріти вже існуючі і спочатку не призначені для побудови комп'ютерних мереж лінії (наприклад, телефонні або телеграфні). Це і є причиною істотно нижчої швидкості передачі даних, порівняно з локальною мережею.

3. Регіональна мережа (MAN - Metropoliten Area Network) – це комп’ютерна мережа, яка працює в межах певного регіону, міста, району [3]. Кожна така мережа є частиною деякої глобальної мережі і має особливу специфіку. Однак, при досить великих відстанях між вузлами, для побудови використовують якісні лінії зв’язку, що дає високу швидкість обміну даними, а існуючі лінії не використовуються на відміну від глобальних мереж. Міські комп’ютерні мережі з’явились порівняно нещодавно, проте займають проміжне положення між локальними і глобальними мережами, та слугують для об’єднання цих мереж.

1.2. Локальна комп’ютерна мережа

У зв'язку з тим що, метою дипломного проєкту є розробка локальної комп'ютерної мережі навчального закладу, більш детально розглянемо саме локальну.

Локальна мережа (Local Area Network, LAN) — це комп’ютерна мережа, яка об’єднує комп’ютери в одне ціле на маленькій відстані, це можуть бути сусідні кімнати, або одна будівля, де відстань між приміщеннями невелика і всі вони мають бути під одним адміністративним контролем [4]. Локальна мережа на прикладі школи (Рис 1.1):

Рис 1.1 Приклад локальної мережі школи

За визначенням, основним призначенням всіх комп’ютерних мереж є — спільний доступ до мережних ресурсів (апаратного забезпечення комп’ютерів, периферійних пристроїв), спільне використання даних і швидкий обмін ними, спільне використання програмного забезпечення.

Робота в середині мережі передбачає віддалений доступ до мережних ресурсів та компонентів за певною технологією.

Відповідно до наданих повноважень, комп’ютери мережі розділяють на сервери й клієнти:

- Клієнт — це комп’ютер звичайного користувача мережі, який здійснює запит.
- Сервер — це комп’ютер, який обробляє здійснений клієнтом запит і відповідає на нього. (Рис. 1.2).

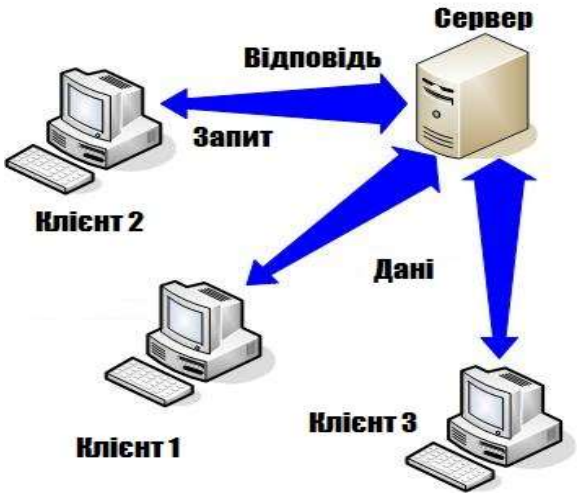

Рис. 1.2 Функції клієнта та сервера

Також мережі поділяють на централізовані та децентралізовані (однорангові). Розберемо кожну з них:

Централізована мережа — це комп'ютерна мережа, яка має один виділений комп'ютер — виділений сервер, що виконує основні функції з організації роботи мережі. Всі клієнти в централізованій мережі отримують доступ до ресурсів мережі через сервер (Рис. 1.3).

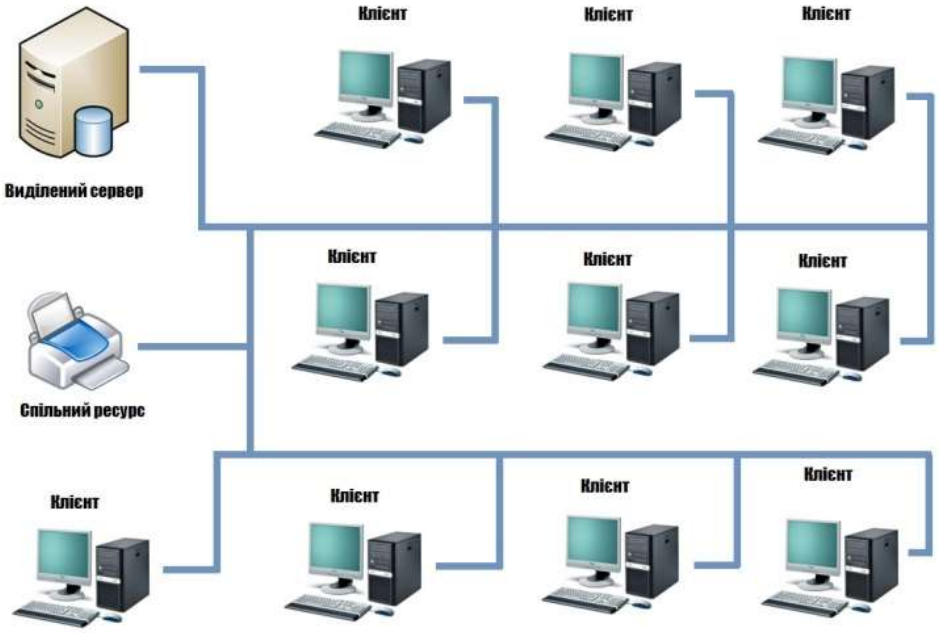

Рис. 1.3 Централізована мережа - «клієнт-виділений сервер»

Для правильної роботи такої мережі на сервері необхідно встановити спеціальну операційну систему, яка відкриває можливості організації і контролю роботи комп’ютерів і користувачів у мережі, а також надає кожному користувачеві певні повноваження чи права доступу до ресурсів і даних всередині цієї мережі.

Кожному користувачу надається «ім'я користувача» (логін) та пароль для входу до мережі. Прикладами такої мережі можуть бути комп’ютерні мережі банків, корпорацій, навчальних закладів.

До основних переваг централізованої комп’ютерною мережі відносять:

- висока швидкість обміну даними;
- наявність можливості розподіляти права доступу користувачів у ній.

Істотним недоліком вважають те, що при виході з ладу сервера вся мережа перестає працювати.

Децентралізована мережа — це комп’ютерна мережа, у якій відсутній виділений сервер, а будь-який комп’ютер в мережі може виступати в ролі сервера чи клієнта. Такі мережі ще називають одноранговими (Рис. 1.4).

Як клієнт, комп’ютери в одноранговій мережі мають змогу здійснювати запити щодо доступу до ресурсів інших комп’ютерів, які знаходяться в цій мережі. Як сервер, комп’ютер повинен опрацювати запити від інших комп’ютерів мережі й надавати потрібні дані.

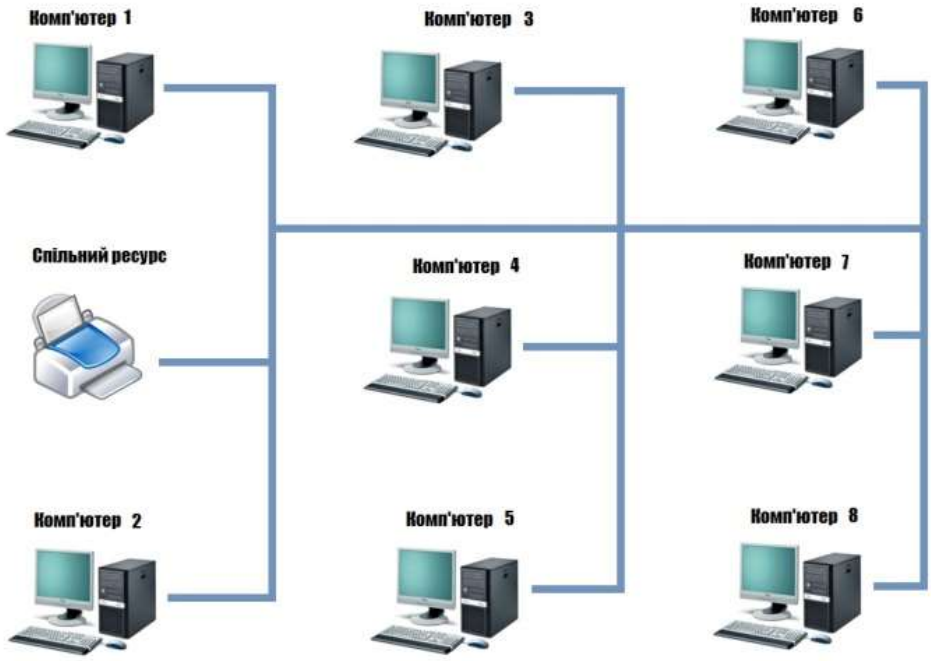

Рис. 1.4 Децентралізована мережа – «однорангова»

В одноранговій комп’ютерній мережі всі комп’ютери мають однакові повноваження (ранги) щодо доступу до ресурсів кожного й до периферійних пристроїв. Кожен користувач мережі має можливість визначити теки і окремі файли на своєму жорсткому диску, які він надає для загального користування. У таких мережах на всі комп’ютери встановлюють операційні системи, які забезпечують їм рівні можливості.

До переваг однорангової комп’ютерної мережі відносять — працездатність мережі при виході з ладу будь-якого з комп’ютерів, а недоліком вважають — неможливість розподіляти права клієнтів щодо роботи у мережі.

1.3. Види з’єднання

Для коректної роботи і можливості взаємодіяти, комп’ютерам необхідне середовище, яке надає можливість передачі сигналів на фізичному рівні. Це середовище передачі сигналів може являти собою кабельну інфраструктуру, тобто набір дротів різних типів, з’єднувальних роз’ємів (конекторів) і пристроїв зв’язку [5]. Проте воно може бути також просто атмосферою, ба більше, безповітряним

простором, - аби тільки за допомогою цього була можливість якимось чином передати сигнал від одного комп’ютера до іншого.

1.3.1. Кабельні з’єднання

Найчастіше при побудові комп’ютерної мережі використовують кабельне з’єднання. Таке з’єднання виступає в якості середовища передачі електричних або оптичних сигналів між комп’ютерами та іншими мережевими пристроями в мережі. Для виконання цих задач, найбільш поширеними є такі типи кабелів:

- коаксіальний кабель (coaxial cable);
- кручена пара (twisted pair):
- неекранована (unshielded, UTP),
- екранована (shielded);
- волоконно-оптичний, або оптоволоконний кабель (fiber optic).

Близько десяти-п’ятнадцяти років тому при створенні комп’ютерних мереж найчастіше застосовували саме коаксіальний кабель (Рис. 1.5). Він складається з мідної або алюмінієвої жили, яка передає сигнал, шару ізоляції, екрануючого обплетення з мідних дротів або алюмінієвої фольги та захисної зовнішньої оболонки. Для досконалої передачі сигналу у коаксіальному кабелі використовувалася центральна жила, в той час як обплетення заземляється, виступаючи в ролі «електричного нуля».

Рис. 1.5. Коаксіальний кабель

1.3.2. Бездротові мережі

Основні проблеми які характерні для всіх комп'ютерних дротових мереж це - їхня низька мобільність, досить великі витрати та мала дальність передачі сигналу. У випадку з бездротовим з'єднанням, цього майже немає, тому вони все частіше і швидше входять в наше життя.

Існує декілька способів передачі даних в бездротових мережах:

- Технології радіозв'язку пересилають дані на радіочастотах і практично не мають обмежень за дальністю. Найчастіше їх використовуються не тільки у локальних мережах, але і для мережевих з'єднань на великих відстанях. З урахуванням того, що радіосигнали легко перехопити, необхідно забезпечити обов'язковий захист даних кодуванням та/або шифруванням.
- Передача даних в мікрохвильовому діапазоні використовує більш високі частоти і застосовується як на не великих відстанях (об'єднання локальних мереж), так і у глобальних мережах – за допомогою супутників та наземних супутникових антен. Одне з головних обмеження такого типу зв'язку є те, що і передавач, і приймач повинні бути в зоні прямої видимості один одного.
- Технології, в яких використовують інфрачервоне випромінювання для передачі сигналів, часто застосовуються для двосторонньої або широкомовної передачі на близьких відстанях. Передачу даних за допомогою інфрачервоного випромінювання, зазвичай використовують у складських і офісних приміщеннях, найчастіше для взаємодії з портативними пристроями. Хоча швидкість і зручність використання інфрачервоних мереж досить привабливі, можуть виникати труднощі під час передачі сигналів на відстань більше 30 метрів.
- Для бездротових мереж також досить часто застосовують світлове випромінювання у видимому діапазоні (наприклад, за допомогою лазерів), хоча цей спосіб передачі використовується рідко. Проте цей спосіб з'єднання може бути зручний для зв'язку між висотними будівлями.

Під час розробки локальної комп'ютерної мережі навчального закладу я використовуватиму кабельне з'єднання.

1.4 Топології локальних мереж

Збільшення кількості комп'ютерів у мережі зростає і це призводить до можливих конфігурацій, в результаті цього постає питання вибору конфігурації фізичних зв'язків. У випадку, якщо три комп'ютери можна об’єднати в два способи (Рис. 1.5), то з чотирма комп'ютерами можна запропонувати вже шість різних конфігурацій (Рис.1.6).

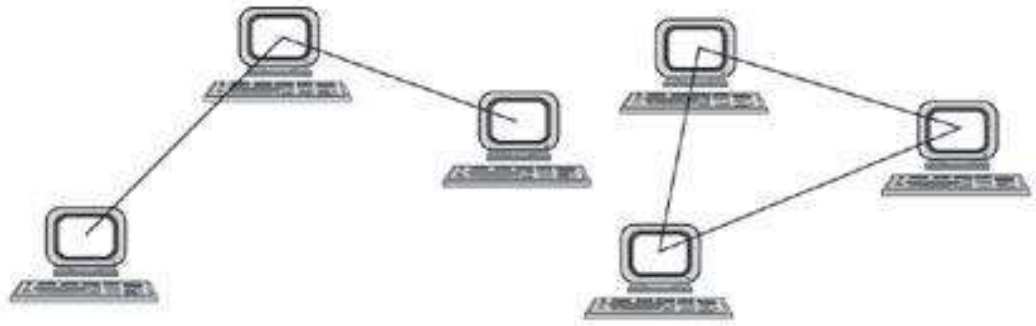

Рис. 1.5. Об'єднання трьох комп'ютерів

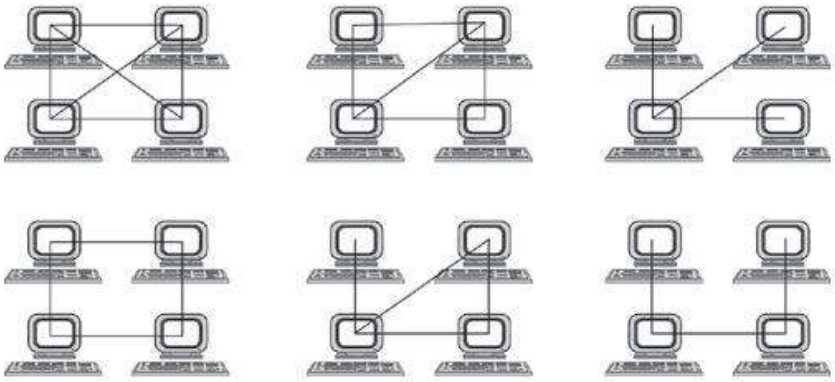

Рис. 1.6. Об'єднання чотирьох комп'ютерів

Топологією (компонуванням, конфігурацією, структурою) комп'ютерної мережі називають фізичне розташування комп'ютерів, а також їх об'єднання лініями зв'язку [6]. Це як конфігурація графа, вершинам якого відповідають кінцеві вузли мережі (наприклад, комп'ютери) або комунікаційне устаткування (наприклад, маршрутизатори), а ребрам — електричні чи інформаційні зв'язки між ними.

Мережна топологія визначає вимоги до обладнання, тип використаного кабелю, методи керування обміном даними, надійність роботи, можливості розширення мережі.

Від вибору топології зв'язків залежать багато інших характеристик мережі. Тобто, наявність між вузлами кількох каналів підвищує надійність мережі і рівномірне завантаження окремих каналів. Простота під’єднання нових вузлів, яка властива певним топологіям, робить мережу легко розширюваною. Економічні міркування часто приводять до вибору топологій, для яких характерною є мінімальна сумарна довжина ліній зв'язку.

Поняття топології зв’язків відноситься, перш за все, до локальних мереж, в яких структуру зв'язків можна легко прослідкувати. В глобальних мережах структура зв'язків зазвичай прихована від користувачів і не є дуже важливою, оскільки кожен сеанс передачі даних може відбуватися за іншим шляхом.

Рис. 1.7. Типи мережних топологій

За повнозв'язної топології кожний комп'ютер мережі є безпосередньо під'єднаним до решти комп’ютерів (Рис. 1.8).

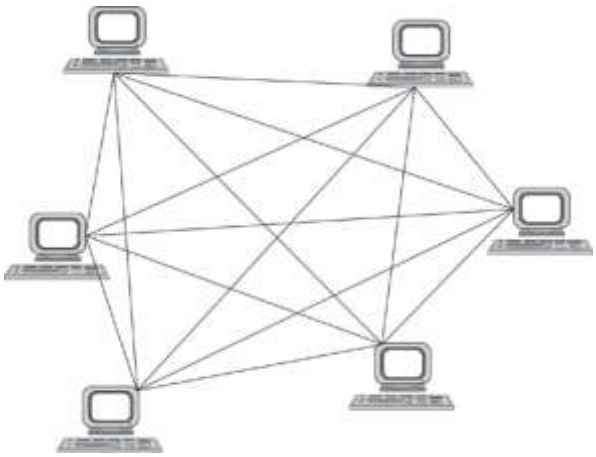

Рис. 1.8. Повнозв’язна топологія

Незважаючи на логічну простоту, цей варіант є громіздким і неефективним. Кожний комп'ютер в мережі повинен мати велику кількість комунікаційних портів для зв'язку з кожним з решти комп'ютерів. Для кожної пари комп'ютерів повинна бути відведена окрема фізична лінія зв'язку, в деяких випадках навіть дві, якщо неможливе використання цієї лінії для двосторонньої передачі.

Повнозв'язні топології у великих мережах застосовуються рідко. Зазвичай, така топологія використовується в багатомашинних комплексах або в мережах, що об'єднують невелику кількість комп'ютерів.

Всі інші варіанти з’єднань засновано на неповнозв’язних топологіях, коли для обміну даними між двома комп'ютерами існує проміжна передача даних через інші вузли мережі.

1.4.1. Топологія «шина»

Топологія «загальна шина» своєю структурою регламентує рівноправність всіх абонентів у доступі до мережі та ідентичність мережного устаткування комп'ютерів (рис. 1.9).

В топології «загальна шина» реалізовано режим напівдуплексного обміну даними, тобто в обох напрямах, але по черзі. Якщо кілька комп'ютерів передаватимуть інформацію одночасно, вона буде спотворена в результаті накладання сигналів (конфлікту, колізії) [7].

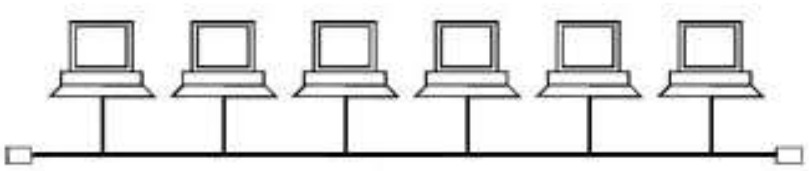

Рис. 1.9. Топологія «загальна шина»

В топології «загальна шина» немає явно вираженого центрального абонента, через який передається вся інформація, що збільшує її надійність. Додавання нових абонентів до «загальної шини» є досить простим і це можна зробити навіть під час роботи мережі. Для використання «загальної шини» потрібно мінімальну кількість кабелю у порівнянні з іншими топологіями.

Оскільки центрального абонента в такій топології не передбачено, то вирішення можливих конфліктів в даному випадку перекладається на мережне устаткування кожного окремого абонента. Тому мережне устаткування комп’ютерів при топології «загальна шина» є складнішим, ніж в інших топологіях.

Із-за особливостей поширення електричних сигналів по довгих лініях зв'язку на кінцях «загальної шини» розташовують спеціальні пристрої - термінатори. Без наявності термінаторів сигнал відбивається від кінця лінії і спотворюється так, що зв'язок по мережі стає неможливим.

При відмові будь-якого з комп'ютерів мережі справні машини можуть нормально продовжувати обмін.

У разі розриву або пошкодження кабелю порушується цілісність лінії зв'язку, і припиняється обмін навіть між тими комп'ютерами, які залишилися сполученими між собою. Коротке замикання в будь-якій точці кабелю «загальної шини» виводить з ладу всю мережу (Рис. 1.10).

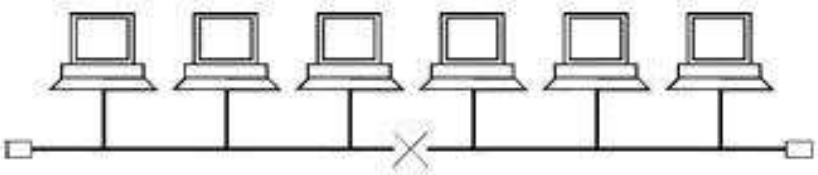

Рис. 1.10. Обрив кабелю в мережі

При проходженні по лінії зв'язку мережі з топологією «загальна шина» інформаційні сигнали згасають, що накладає жорсткі обмеження на сумарну довжину ліній зв'язку. Для збільшення довжини мережі за топологією «загальна шина» часто використовують кілька сегментів (частини мережі, кожна з яких є «загальною шиною»), що сполучені між собою за допомогою спеціальних підсилювачів і відновників сигналів — повторювачів.

1.4.2. Топологія «зірка»

Топологія «зірка» — це топологія мережі з явно виділеним центральним елементом, до якого під’єднується решта абонентів [8]. Обмін інформацією відбувається виключно через центральний пристрій, на який припадає більше навантаження, тому він зазвичай використовується для виконання суто мережних функцій. Зрозуміло, що мережне устаткування центрального абонента повинно бути істотно складнішим, ніж устаткування периферійних абонентів. Жодні конфлікти у мережі з топологією «зірка» в принципі є неможливими, оскільки управління цілком централізоване.

Якщо говорити про стійкість «зірки» до відмов комп'ютерів, то вихід з ладу периферійного комп'ютера або його мережного устаткування жодним чином не відбивається на функціонуванні мережі, проте будь-яка відмова центрального пристрою робить мережу цілком непрацездатною.

Обрив кабелю або коротке замикання в топології «зірка» порушує обмін лише з одним комп'ютером, решта комп'ютерів може нормально продовжувати роботу.

На відміну від «загальної шини», в «зірці» кожна лінія зв'язку з’єднує лише два абоненти: центральний та один з периферійних. Зазвичай, для їх з'єднання використовують дві лінії зв'язку, кожна з яких передає інформацію в одному напрямку, тобто кожна лінія зв'язку містить лише один приймач і один передавач, так звана передача «точка-точка». Це істотно спрощує мережне устаткування у порівнянні з «загальною шиною» і позбавляє від необхідності застосування додаткових, зовнішніх термінаторів.

Проблема загасання сигналів в лінії зв'язку вирішується в «зірці» простіше, ніж в топології «загальна шина», оскільки кожен приймач завжди отримує сигнал одного рівня. Гранична довжина мережі з топологією «зірка» може бути вдвічі більшою, ніж в «загальній шині».

Серйозний недолік топології «зірка» полягає в жорсткому обмеженні кількості абонентів. Зазвичай, центральний абонент може обслуговувати не більше 16 – 32 периферійних абонентів.

Розрізняють топології «пасивна зірка» та «активна зірка». В топології «пасивна зірка» в центрі мережі знаходиться спеціальний пристрій - концентратор або хаб (hub), який відновлює сигнали, що надійшли і пересилає їх у всі інші лінії зв'язку (рис. 1.11). В топології "активна зірка" центральним елементом мережі є комп’ютер (рис.1.12).

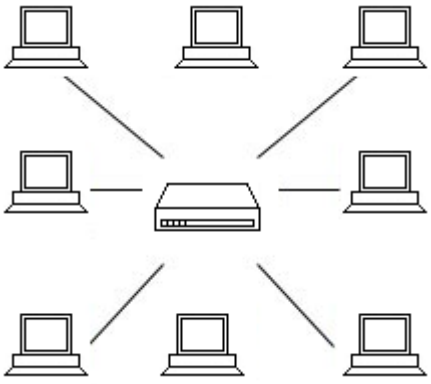

Рис. 1.11. Топологія «пасивна зірка»

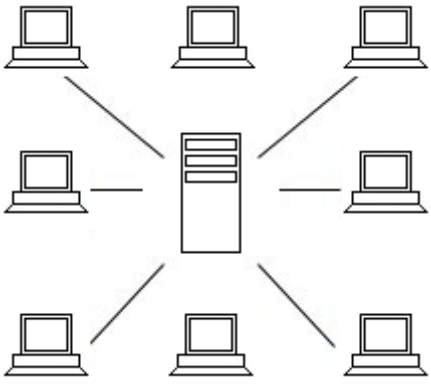

Рис. 1.12. Топологія «активна зірка»

Суттєвою перевагою "зірки" (як активної, так і пасивної) є те, що всі точки під’єднання зібрано в одному місці. Це дозволяє легко контролювати роботу мережі, локалізувати несправності шляхом простого вимикання від центру тих або інших абонентів (що є неможливим, наприклад, у топології "загальна шина"), а також обмежувати доступ сторонніх осіб до важливих для мережі точок під’єднання [9].

Загальним недоліком для всіх топологій типу "зірка" (як активної, так і пасивної) є значно більша, ніж в інших топологіях, витрата кабелю, що істотно впливає на вартість мережі в цілому і ускладнює прокладання кабелю.

1.4.3. Топологія «кільце»

Топологія "кільце" — це топологія, в якій кожен комп'ютер з’єднано лініями зв'язку з двома іншими: від одного він отримує інформацію, а іншому передає. Кожна лінія зв'язку, як і у разі "зірки", має лише один передавач і один приймач (зв'язок типу "точка-точка"). Це дозволяє відмовитися від застосування зовнішніх термінаторів (Рис.1.13).

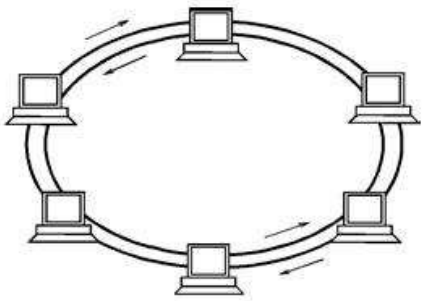

Рис.1.13. Топологія «кільце»

Важливою особливістю "кільця" є те, що кожен комп'ютер відновлює (ретранслює, підсилює) сигнал, що надходить до нього, тобто виступає в ролі повторювача. Згасання сигналу у всьому "кільці" є не таким важливим, як згасання між сусідніми комп'ютерами "кільця". Розміри кільцевих мереж сягають десятків кілометрів, що істотно перевершує інші топології.

Чітко виділеного центру у топології "кільце" немає, всі комп'ютери можуть бути однаковими і рівноправними. Проте часто в "кільці" виділяється спеціальний комп’ютер, який керує обміном або контролює його. Зрозуміло, що наявність єдиного керуючого абонента зменшує надійність мережі, оскільки його вихід з ладу відразу ж паралізує весь обмін.

Під’єднання нових комп’ютерів до "кільця" відбувається досить просто, хоч і вимагає обов'язкового припинення роботи всієї мережі на час під’єднання. Як і у топології "загальна шина", максимальна кількість абонентів в "кільці" може бути достатньо великою (до тисячі і більше).

Топологія "кільце" зазвичай має високу стійкість до перевантажень, забезпечує надійну роботу з великими потоками інформації, що передається по мережі, в ній,

зазвичай, немає конфліктів (на відміну від "загальної шини"), а також не є обов’язковим центральний абонент (на відміну від "зірки"), який може бути перевантажений великими потоками інформації.

Сигнал в "кільці" проходить послідовно через всі комп'ютери мережі, тому вихід з ладу хоча б одного з них (або ж його мережного устаткування) порушує роботу мережі в цілому. Обрив або коротке замикання в будь-якому з кабелів "кільця" також робить роботу всієї мережі неможливою.

З трьох розглянутих топологій "кільце" є самим вразливим до пошкоджень кабелю, тому у топології "кільце" зазвичай передбачають прокладку двох (або більше) паралельних ліній зв'язку, одна з яких знаходиться в резерві.

Іноді мережа з топологією "кільце" виконується на основі двох паралельних кільцевих ліній зв'язку, що передають інформацію в протилежних напрямках. Метою подібного рішення є збільшення вдвічі швидкості передачі інформації по мережі. При пошкодженні одного з кабелів мережа може працювати з іншим кабелем, хоча гранична швидкість буде меншою.

Ознайомившись детально з різними топологіями побудови локальних комп’ютерних мереж, дізнавшись про переваги та недоліки кожної з них, я вирішив що для побудови локальної комп’ютерної мережі навчального закладу я використовуватиму топологію «зірка». На мою думку, для виконання обраної задачі і з точки зору надійності, цей тип топології є найкращим. Комп’ютерна мережа вийде з ладу лише у випадку несправності центрального елементу.

1.5. Мережеві технології локальних мереж

В локальних мережах, як правило, використовується середовище передачі даних, що розділяється, і основна роль відводиться протоколам фізичного і канального рівнів, оскільки ці рівні найбільшою мірою відображають специфіку локальних мереж.

Мережева технологія — це погоджений набір стандартних протоколів та програмно-апаратних засобів, які їх реалізовують, достатній для побудови локальної

обчислювальної мережі [10]. Мережеві технології називають базовими технологіями або мережевою архітектурою локальних мереж. Мережева технологія або архітектура визначає топологію і метод доступу до середовища передачі даних, кабельну систему або середовище передачі даних, формат мережевих кадрів тип кодування сигналів, швидкість передачі в локальній мережі. У сучасних локальних обчислювальних мережах широкого поширення набули такі технології або мережева архітектура, як: Ethernet, Token-ring, Arcnet, FDDI.

Мережеві технології локальних мереж Ieee802.3/Ethernet

В даний час ця мережна технологія найпопулярніша у світі. Популярність забезпечується простими, надійними і недорогими технологіями. У класичній локальній мережі Ethernet застосовується стандартний коаксіальний кабель двох видів (товстий і тонкий). Проте найбільшого поширення набула версія Ethernet, яка використовує як середовище передачі виті пари, оскільки монтаж і обслуговування їх набагато простіший.

У локальних мережах Ethernet застосовуються топології типу «шина» і типу «пасивна зірка», а метод доступу CSMA/CD.

Стандарт Ieee802.3 залежно від типу середовища передачі даних має модифікації:

- 10BASE5 (товстий коаксіальний кабель) — забезпечує швидкість передачі даних 10 Мбіт/с і довжину сегменту до 500м;
- 10BASE2 (тонкий коаксіальний кабель) — забезпечує швидкість передачі даних 10 Мбіт/с і довжину сегменту до 200м;
- 10base-t (неекранована вита пара) — дозволяє створювати мережу топології «зірка». Відстань від концентратора до кінцевого вузла до 100м. Загальна кількість вузлів не повинна перевищувати 1024;
- 10base-f (оптоволоконний кабель) — дозволяє створювати мережу топології «зірка». Відстань від концентратора до кінцевого вузла до 2000м.

У розвиток мережної технології Ethernet створені високошвидкісні варіанти: Ieee802.3u/Fast Ethernet і Ieee802.3z/Gigabit Ethernet. Основна топологія, яка використовується в локальних мережах Fast Ethernet і Gigabit Ethernet — пасивна зірка.

Мережева технологія Fast Ethernet забезпечує швидкість передачі 100 Мбіт/с і має три модифікації:

- 100BASE-T4 — використовується неекранована вита пара. Відстань від концентратора до кінцевого вузла до 100м;
- 100base-tx — використовуються дві виті пари (неекранована і екранована). Відстань від концентратора до кінцевого вузла до 100м;
- 100base-fx — використовується оптоволоконний кабель (два волокна в кабелі). Відстань від концентратора до кінцевого вузла до 2000м;.

Мережна технологія локальних мереж Gigabit Ethernet — забезпечує швидкість передачі 1000 Мбіт/с. Існують такі модифікації стандарту:

- 1000base-sx — застосовується оптоволоконний кабель з довжиною хвилі світлового сигналу 850 нм.
- 1000base-lx — використовується оптоволоконний кабель з довжиною хвилі світлового сигналу 1300 нм.
- 1000base-cx — використовується екранована вита пара.
- 1000base-t — застосовується неекранована вита пара.

Локальні мережі Fast Ethernet і Gigabit Ethernet сумісні з локальними мережами, виконаними за технологією (стандарту) Ethernet, тому легко і просто сполучати сегменти Ethernet, Fast Ethernet і Gigabit Ethernet в єдину обчислювальну мережу.

Мережеві технології локальних мереж Ieee802.5/Token-ring передбачає використання середовища передачі даних, яке утворюється об'єднанням всіх вузлів в кільце, що розділяється. Мережа Token-ring має зоряно-кільцеву топологію (основна кільцева і зоряна додаткова топологія). Для доступу до середовища передачі даних використовується маркерний метод (детермінований маркерний метод). Стандарт підтримує виту пару (екрановану і неекрановану) і оптоволоконний кабель. Максимальне число вузлів на кільці — 260, максимальна довжина кільця — 4000 м. Швидкість передачі даних до 16 Мбіт/с.

Мережеві технології локальних мереж Ieee802.4/Arcnet як топологію локальна мережа Arcnet використовує «шину» і «пасивну зірку». Підтримує екрановану і неекрановану виту пару і оптоволоконний кабель.

У мережі Arcnet для доступу до середовища передачі даних використовується метод передачі повноважень. Локальна мережа Arcnet — це одна із старих мереж і користувалася великою популярністю. Серед основних переваг локальної мережі Arcnet можна назвати високу надійність, низьку вартість адаптерів та гнучкість. Основним недолікам мережі є низька швидкість передачі інформації (2,5 Мбіт/с). Максимальна кількість абонентів — 255. Максимальна довжина мережі — 6000 метрів.

Мережеві технології локальних мережі FDDI (Fiber Distributed Data Interface) — стандартизована специфікація для мережевої архітектури високошвидкісної передачі даних по оптоволоконних лініях [11]. Швидкість передачі — 100 Мбіт/с. Ця технологія багато в чому базується на архітектурі Token-ring і використовується детермінований маркерний доступ до середовища передачі даних. Максимальна протяжність кільця мережі — 100 км. Максимальна кількість абонентів мережі — 500. Мережа FDDI — це дуже високонадійна мережа, яка створюється на основі двох оптоволоконних кілець, створючих основну і резервну дороги передачі даних між вузлами.

1.6. IP-адреси та їх класифікації

IP-адреси (Internet Protocol address) — це ідентифікатор (унікальний числовий номер) мережевого рівня, який використовується для адресації комп'ютерів чи пристроїв у мережах, які побудовані з використанням стеку протоколів TCP/IP [12]. У мережі Інтернет потрібна глобальна унікальність адрес, у разі роботи в локальній мережі — в межах мережі.

У версії протоколу IPv4 IP-адреса має 4 байти, а у версії IPv6 — 16 байтів. Процес перетворення доменного імені на IP-адресу виконується DNS-сервером.

IP-адресу називають статичною (постійною, незмінною), якщо вона задається користувачем у налаштуваннях пристрою, або якщо надається автоматично при підключенні пристрою до мережі та не може бути присвоєна іншому пристрою.

IP-адресу називають динамічною (непостійною, змінною), якщо вона надається автоматично при підключенні пристрою до мережі і використовується протягом обмеженого проміжку години, зазначеної у службі, яка надала IP-адресу (DHCP).

Динамічні адреси IP також є віртуальними. Обслуговування уявної адреси IP проводитиметься за технологією NAT: користувачам надається можливість безперешкодно отримувати інформацію з мережі Інтернет, при цьому втрачається будь-яка можливість іншого доступу до комп'ютера з мережі, наприклад, комп'ютер з такою адресою IP не може використовуватися як вебсервер. Не уявні адреси IP називають реальними, прямими, зовнішніми, громадськими чи громадськими, «білими», всі такі адреси IP є статичними.

В протоколі IPv4 існує п'ять класів IP-адрес: A, B, C, D і E. Клас визначає, які байти (октети) IP-адреси відносяться до ідентифікатора мережі, а які - до ідентифікатора вузла. Клас також визначає максимально можливе число вузлів у даній мережі.

Класи IP-адрес розрізняють за значенням четвертого октету адреси. Адреси класу A назначаються хостам великих по розміру мереж. Старший біт в цих адресах завжди рівний "0". Перший октет IP-адреси цього класу виділяється під ідентифікатор мережі, присвоюється організацією InterNIC і модифікації не підлягає. Решта три октети містять ідентифікатор вузла.

Адреси класу B назначаються хостам середніх по числу комп’ютерів мереж. Два старші біти в цих адресах завжди рівні двійковому значенню "10". Два перші октети IP-мережі класу B виділяються під ідентифікатор мережі і присвоюються організацією InterNIC. Два останні октети містять ідентифікатор вузла.

Адреси класу C застосовуються в невеликих по розміру мережах. Три старші біти в цих адресах завжди рівні двійковому значенню "110". Три перші октети адреси класу C становлять ідентифікатор мережі і присвоюються організацією InterNIC. Четвертий октет є ідентифікатором вузла.

IP-адреси класу D призначені для групових повідомлень. Чотири старші біти в цих адресах завжди рівні "1110". Решта біт означають конкретну групу отримувачів і не діляться на частини. Цей клас призначений для економного розсилання за

допомогою спеціального протоколу Internet Group Management Protocol (IGMP) мультимедійної інформації вибраній групі хостів в об’єднаній мережі.

Клас E зарезервований для майбутнього використання і наразі не використовується. Старші біти в IP- адресах цього класу завжди рівні значенню "11110".

Користувачами реально використовуються IP-адреси класів A, B і C. При цьому адміністратор мережі присвоює всім вузлам фізичної мережі IP-адреси, які складаються з виділеного провайдером ідентифікатора мережі та вибраного адміністратором з діапазону даного класу ідентифікатора вузла.

Таблиця 1.1.

Структура IP- адрес класів A, B, C

№ Байта	4-ий байт	3-ий байт	2-ий байт	1-ий байт
Клас A	Ідентифікатор мережі		Ідентифікатор вузла	
Клас B	Ідентифікатор мережі		Ідентифікатор вузла	
Клас C	Ідентифікатор мережі			Ідентифікатор вузла

Протокол IPv4 передбачає цілий ряд IP-адрес, які не присвоюються вузлам мережі і вважаються виділеними адресами. Розрізняють наступні виділені адреси:

- 0.0.0.0 - даний вузол у даній мережі;
- 255.255.255.255 - всі вузли мережі, в якій знаходиться відправник пакету (обмежена широкомовна адреса-limited broadcast);
- номер мережі / всі нулі - IP-мережа за вказаним номером (ідентифікатор мережі);
- всі нулі / номер хоста - хост в даній IP-мережі (ідентифікатор хоста);
- номер мережі / всі одиниці - всі хости в IP-мережі за вказаним номером (ширококомовна адреса-broadcast).

Таблиця 1.2.

Характеристики IP-мереж класів A, B, C

Клас IP-адреси	Старші біти 4-го байта	Кількість мереж	Найменший ідентифікатор мережі	Найбільший ідентифікатор мережі	Число вузлів
A	0	126	1.0.0.0	127.0.0.0	2^{24}-2
B	10	16384	128.0.0.0	191.255.0.0	2^{16}-2
C	110	2097152	192.0.0.0	223.255.255.0	2^{8}-2

ВИСНОВКИ ДО РОЗДІЛУ 1

В першому розділі дипломного проєкту були розглянуті основні поняття комп’ютерних мереж, види з’єднань, топології мереж, мережеві технології та класифікації IP-адрес.

Комп'ютерні мережі - це сукупність ПК, розподілених на деякій території і об'єднаних для спільного використання ресурсів (даних, програм і апаратних компонентів)

Основною їх задачею є доступ користувачів до різних інформаційних джерел розподіленими по цих комп’ютерах та полегшення їх роботи. Характеристика за якою розрізняють комп’ютерні мережі є широта території, яку вона охоплює.

Ознайомившись з усім матеріалом, в цьому дипломному проєкті буде використана топологія «зірка». На мою думку, для виконання обраної задачі і з точки зору надійності, цей тип топології є найкращим. Комп’ютерна мережа вийде з ладу лише у випадку несправності центрального елементу.

Опрацювавши матеріал на тему «Мережеві технології локальних мереж», дійшов висновку, що в даному проекті буде використана технологія Gigabit Ethernet 1000Base-T. На мою думку цей варіант є найкращим для виконання поставленої задачі, адже швидкість передачі даних становить – 1000 Мбит/с і ця технологія є подальшим розвитком мережі Ethernet.

РОЗДІЛ 2
БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ

2.1. Основні поняття безпеки

У цьому розділі буде розглянуто основні поняття безпеки комп'ютерних мереж, загрози які можуть виникнути, забезпечення надійності, цілісності даних та запобігання атак чи помилок при роботі.

Розділ на цю тему є невід'ємною частиною комп'ютерних мереж, їх проєктування та побудови, адже це забезпечує правильність роботи і уникнення помилок чи атак. У випадку з локальними мережами все простіше, так як вони не є великими, тому відповідно мають менше клопоту з контролем і безпекою, можна обійтись мінімальними заходами, такими як: встановлення антивірусу та системи контролю і управління доступом. З більш масштабними, ситуація зовсім інша, якщо розглянути глобальну комп'ютерну мережу якоїсь міжнародної компанії, то зазвичай вони мають декілька філіалів чи офісів по світу, у зв'язку з цим постає проблема з ускладненим контролем і забезпеченням безпеки, так як кількість комп'ютерів і вузлів більше, відстань протяжності також зростає, відповідно вразливість такої мережі значно вища. В такому випадку використовують вже більше надійні методи захисту - резервування, використання шифрувального програмного забезпечення, системи виявлення вторгнення. Всі ці, та інші проблеми і варіанти їх вирішення і будуть розглянуті в цьому розділі.

Безпека комп'ютерної мережі – це сукупність заходів, які забезпечують захист мережі від несанкціонованого доступу, випадкового чи навмисного втручання в роботу мережі, а також спроб руйнування компонентів (Рис. 2.1).

Рис. 2.1. Безпека комп’ютерних мереж

Саме поняття «безпека інформаційної мережі» включає в себе захист обладнання, програмного забезпечення, даних і персоналу які є частино певної мережі. Основна складова мережевої безпеки складається з положення і політики, прийнятої адміністратором мережі, для блокування та контролю несанкціонованим доступом, неправильним використанням, зміни або відмови в комп’ютерній мережі та доступних ресурсах [14]. Мережева безпека містить у собі дозвіл на доступ до даних у мережі. Користувачі мають змогу обрати або їм призначається ідентифікатор і пароль, які дозволяють їм здійснювати доступ до інформації і програм в рамках своїх повноважень.

Мережева безпека охоплює різні комп'ютерні мережі включаючи державні і приватні, які використовуються у повсюдних робочих місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами. Найбільш поширеним і простим способом захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного пароля.

2.2. Типи атак і небезпек для мережі

Комп’ютерні мережі вразливі до атак з різних джерел. Самі атаки діляться на дві категорії: «пасивні», так їх називають в тому випадку коли злочинець перехоплює дані, які проходять через мережу, і «активні», це коли злочинець може ініціювати команди які порушують нормальну роботу мережі або здійснює моніторинг, метою якого є отримання доступу до даних.

2.2.1. Атака «відмова в обслуговуванні»

Тип атаки, яку називають «відмова в обслуговуванні», призначена для того, щоб зробити мережевий ресурс чи будь-який комп’ютер недоступним для його користувача. Найпростішими прикладами і шляхами, якими користуються зловмисники, для досягнення результату є багаторазове введення не правильного паролю при вході в систему, що веде за собою блокування облікового запису. Іншим популярним методом є масове перенавантаження комп’ютерів чи самої мережі, в результаті чого відбувається блокування всіх користувачів одночасно. Якщо така атака відбуватиметься з одного пристрою, боротись з нею легше, проте можливі форми атак, коли сигнали поступають від великої кількості IP-адрес (DDos).

DDoS-атаки є одними з найбільш складних і руйнівних загроз безпеці комп'ютерних мереж (Рис. 2.2). Під час таких атак зловмисники використовують багато комп'ютерів або пристроїв для надсилання великої кількості запитів до цільового сервера або мережі. Це призводить до перевантаження ресурсів та зниження пропускної здатності, що призводить до відмови в обслуговуванні для легітимних користувачів.

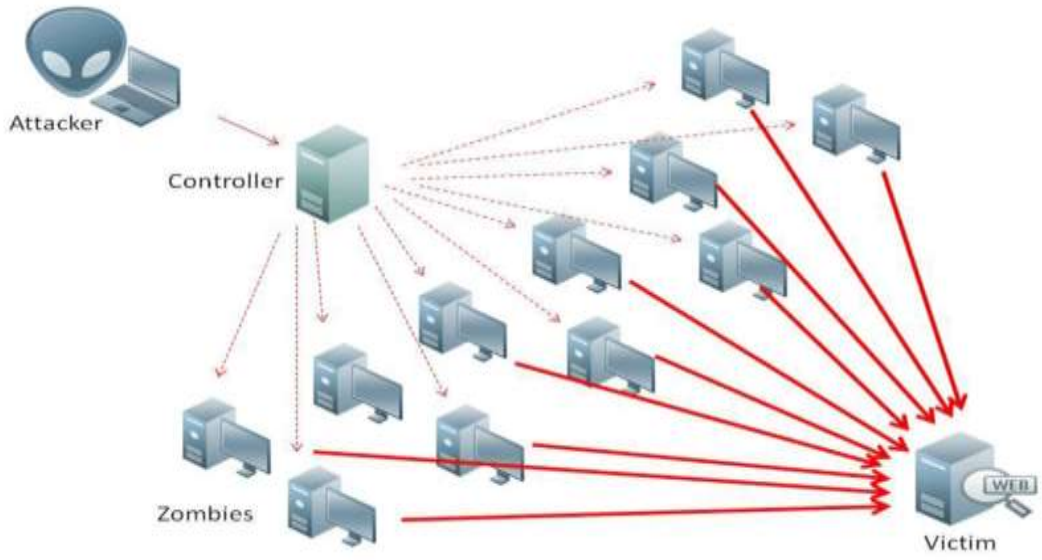

Рис. 2.2 Схема DDoS-атаки

Для запобігання DDoS-атакам необхідно використовувати спеціальне програмне та апаратне забезпечення, яке виявляє та фільтрує незвичайний трафік, а

також мережеві протоколи, які можуть виділяти та обмежувати ресурси для запитів, що надходять до системи.

2.2.2. Атака прямого доступу

Після отримання фізичного доступу до комп'ютера, зловмисник має змогу скопіювати, видалити, викрасти та пошкодити інформацію. Ці недоброзичливі користувачі можуть також поставити під загрозу питання безпеки всієї комп'ютерної мережі шляхом внесення змін в операційну систему, встановленням вірусних файлів, програмних черв'яків, клавіатурних шпигунів та навіть пристроїв для слідкування чи прослуховування [15]. Зменшити ризик такої атаки на ваші пристрої можна методом шифрування диску.

Шкідливі програми, такі як віруси, черви та інші є однією з найбільш поширених загроз, які ставлять від питання безпеку цілої мережі. Ці програми здаються незначними, проте наслідки можуть бути жахливими. Вони мають можливість пошкодити та навіть знищити дані, які знаходяться на пристрої, значно сповільнити роботу мережі та поширюватись на інші комп'ютери. Убезпечити себе від таких програм можна встановленням та регулярним оновленням якісних антивірусних програм або програмного забезпечення, а також надавати інструкції користувачам щодо безпеки використання комп'ютерів та мережі.

2.2.3. Фішинг та соціальний інжиніринг

Фішинг та соціальний інжиніринг є методами, за допомогою яких зловмисники намагаються отримати конфіденційну інформацію, таку як паролі чи дані банківських карток, шляхом обману користувачів. Атаки такого плану зазвичай проводяться через електрону пошту, соціальні мережі, або будь-які інші комунікаційні канали.

Працює такий тип небезпеки досить просто, злочинці маскуються під установи чи органи, яким довіряє людина. Це може бути співробітник вашого банку, мобільний оператор чи представник органів влади. Вони надсилають повідомлення чи лист на вашу електрону пошту з текстом, в якому просять вас ввести ваші конфіденційні дані,

під виглядом перевірки чи якоїсь помилки. Також є варіант з телефонним дзвінком в якому може відбуватися все те саме.

На такий «гачок» може потрапити будь-хто, навіть професіонали в цій галузі можуть помилитись, адже можливості і технології з кожним днем тільки ростуть і способи таких атак тільки збільшуються.

Даний спосіб обману може використовуватись не лише для отримання персональних даних, ваших грошей, але і для доступу до комп’ютерів чи комп’ютерних мереж. Бути впевненим у своїй безпеці на 100 відсотків майже не можливо, проте можна зменшити ризики використовуючи антивірусні програми, вони добре допомагають у виявленні фішингу, та якісною інформаційною гігєною і поповнювати кожного дня свої знання в цій галузі.

2.2.4. Витік інформації

Витік інформації є серйозною загрозою для безпеки комп'ютерних мереж навчального закладу. Це може статися через недостатньо захищений доступ до файлів та баз даних, недостатній контроль доступу до конфіденційної інформації або недбалість користувачів. Для запобігання витоку інформації, необхідно встановлювати строгий контроль доступу до конфіденційних даних, шифрувати важливу інформацію та забезпечувати навчання користувачів щодо правил та процедур безпеки.

2.3 Заходи безпеки в комп'ютерних мережах

Ознайомившись з вище наведеною інформацією, постає питання захисту комп'ютерів та комп'ютерних мереж, саме про них наступна інформація.

2.3.1. Встановлення фаєрвола

Брандмауер або ж фаєрвол – це програма для комп'ютера, яка здійснює захист від вірусів і хакерських атак. Фаєрвол має змогу відстежувати трафік, що надходить в операційну систему, та допомагає зупинити шкідливі програми, які хочуть отримати

доступ до особистої інформації. Фаєрвол являється першим рівнем захисту від несанкціонованого доступу та шкідливого трафіку.

2.3.2. Антивірусні програми

Встановлення та слідкування за оновленням якісного антивірусного програмного забезпечення на всіх комп'ютерах в мережі є важливим кроком до захисту від вірусів та всіх шкідливих програм.

2.3.3. Використання ключів

В процесі ліцензування програмного забезпечення використовують USB – ключі, проте їх також можна розглянути як спосіб запобігання несанкціонованого доступу до комп’ютера чи мережі. Цей самий ключ може створити безпечний зашифрований тунель. Принцип роботи такого методу полягає в тому схема шифрування яка використовується, може забезпечити більш високу ступінь безпеки в комп’ютерних мережах, так як злочинцю буде набагато важче зламати цей ключ, ніж скопіювати власне програмне забезпечення на інший пристрій і користуватись цим.

2.3.4. Шифрування даних

Шифрування – це технічний процес, за допомогою якого інформація перетворюється на секретний код, який маскує дані при обміну, отриманні чи зберіганні.

Важлива конфіденційна інформація, така як дані студентів та викладачів, повинна бути зашифрована для запобігання несанкціонованого доступу до неї. Використання шифрування даних допоможе зберегти конфіденційність та цілісність інформації.

Варто також зазначити, що шифрування відіграє важливу роль у гарантуванні безпеки під час перегляду вебсторінок. Багато вебсайтів використовують протокол захищених сокетів (SSL), який шифрує дані, що надсилаються на вебсайт і отримуються з нього, перешкоджаючи доступу хакерів до даних під час їх

передавання. Однак в останні роки SSL замінив стандартний протокол шифрування TLS (захист на транспортному рівні), який використовувався для автентифікації серверів походження вебсайтів і дотримання безпеки запитів та відповідей HTTP.

Розшифрувати інформацію можна за допомогою ключа дешифрування, проте звісно, є можливість декодувати зашифровані файли без ключа, але для виконання цього, щоб якісно зламати розроблену схему, знадобиться величезний обсяг обчислювальних ресурсів.

2.3.5. Резервне копіювання даних

Резервне копіювання даних – це процес створення хмарної копії з носія, призначений для відновлення цих даних у разі пошкодження чи видалення.

Розділяються три основні типи резервного копіювання:

Повне копіювання – це повна резервна копія даних, яка у разі помилки чи атаки зможе відновити повний працездатний стан системи до події яка спричинила збій (Рис. 2.3). Недоліками такого типу є час, необхідний для створення і дисковий простір, який він займатиме.

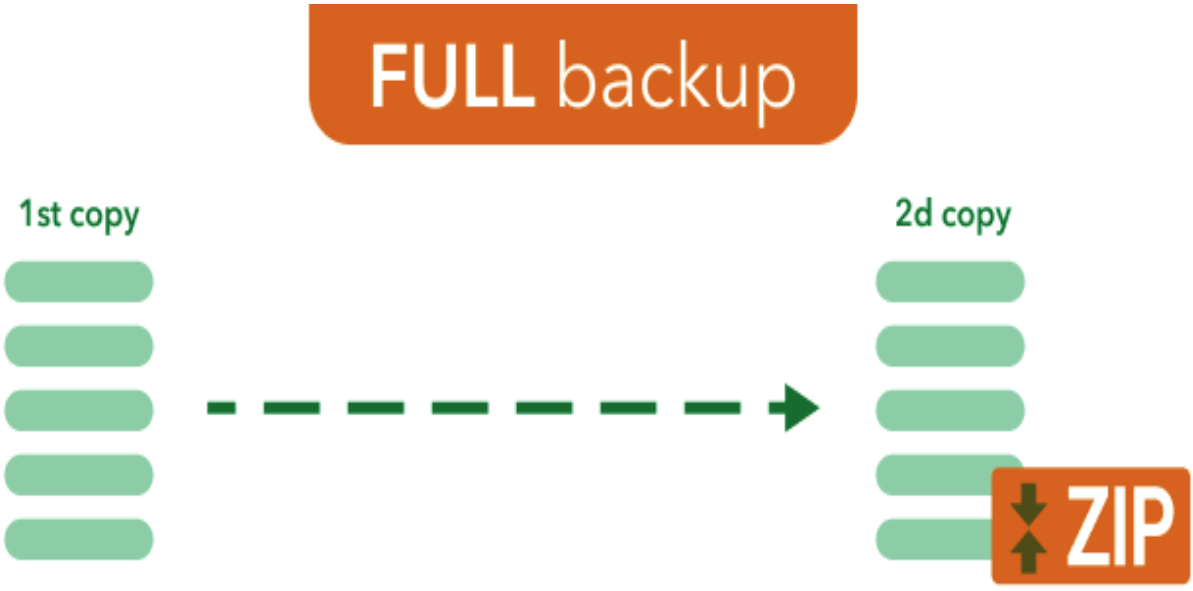

Рис. 2.3. Повне резервне копіювання

Диференційне копіювання відрізняється тим, що копія створюється з інформації які була додана або змінена після повного резервного копіювання (Рис. 2.4.). Незважаючи на те, що такий тип займає відносно мало місця, для відновлення повного стану системи необхідні дані з останньої повної та накопичувальної резервної копії.

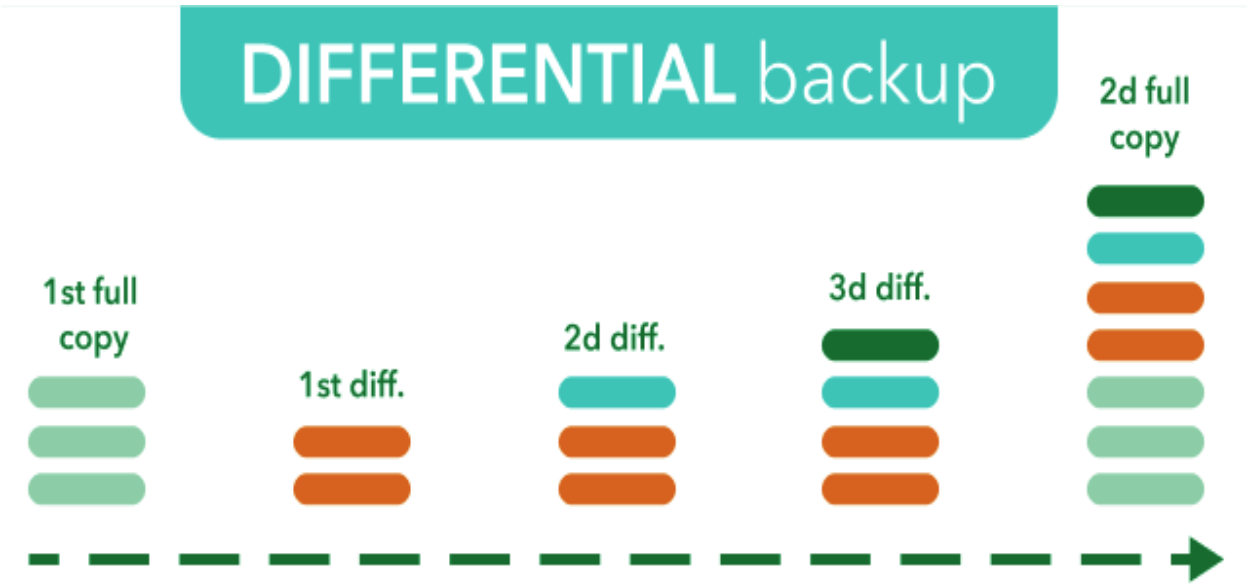

Рис. 2.4. Диференційне резервне копіювання

Інкрементне копіювання є найпростішим способом резервування (Рис. 2.5.). Використовуючи цей метод, копіюються лише файли, які понесли зміни з часу попереднього резервного копіювання. Проте, в разі атаки, для відновлення знадобиться не лише остання копія повного резервування, але й усі інші. У такому випадку, цей процес може призвести до відновлення системи з кількох десятків копій, а це може зайняти багато часу.

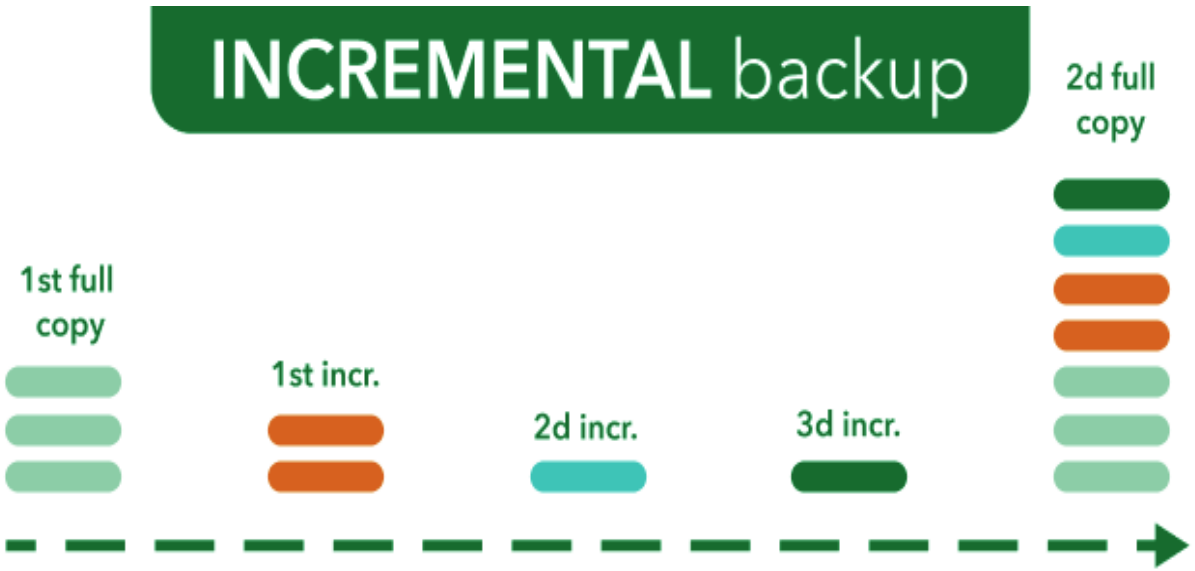

Рис. 2.5. Інкрементне резервне копіювання

Також в питанні резервування даних не менш важливим кроком є створення плану боротьби з масштабним збоєм, де значну увагу варто приділити процедурі плану аварійного відновлення (DRP). Він визначає, як ми захищаємо себе від втрати інформації і систематизує весь процес.

Ця процедура включає кілька важливих етапів:

- Надайте пріоритет важливості. Визначте стратегічно важливу інформацію, від втрати якої може зупинитися робота бізнесу та ту, втрата якої не призведе до “краху”.
- Встановіть частоту резервного копіювання та швидкість відновлення. Незалежно від того, чи хочете ви створювати резервні копії раз на день, раз на тиждень або раз на місяць, ця інформація має вирішальне значення під час вибору методу резервного копіювання. Можливе географічне розташування резервної копії та використовувані технології також залежать від запланованої швидкості відновлення.
- Визначте політику та процедури безпеки даних. Потрібно знати, як часто потрібно створювати резервні копії кожної категорії інформації, скільки копій потрібно зробити та де вони будуть розташовані.

- Підготуйте бюджет. Будуючи складну IT-інфраструктуру, ми часто забуваємо виділити бюджет на резервне копіювання, що є великою помилкою. Варто порахувати втрати, спричинені втратою даних і перервою в роботі.
- Захистіть дані, які ви обробляєте поза центром обробки даних. Буває, що наша система використовує гібридні рішення. Деякі дані обробляються за межами наших серверів, наприклад, у хмарі, або наші сервери розташовані в кількох дата-центрах. У цьому випадку кожне з цих місць має мати власну резервну копію.

2.4 Фізичний захист мережевого обладанання

Фізичний захист мережевого обладнання є так само важливим, як і захист від електронних загроз. Нижче наведені деякі аспекти, які слід враховувати для забезпечення фізичної безпеки комп'ютерної мережі:

1. *Захищений фізичний доступ до серверних кімнат та приміщень мережевого обладнання*. Важливо забезпечити обмежений та контрольований фізичний доступ до серверних кімнат та приміщень, де розташоване мережеве обладнання. Це може включати використання карт доступу, систем відеоспостереження, а також фізичну охорону.

2. *Розміщення мережевого обладнання*. Мережеве обладнання, таке як комутатори, маршрутизатори та сервери, повинні бути розміщені в безпечних розподільчих шафах або кабельних каналах. Це дозволяє запобігти несанкціонованому доступу до обладнання та зменшити його вразливість до фізичних пошкоджень.

3. *Захист фізичних кабелів мережі*. Фізичні кабелі, які використовуються для підключення комп'ютерів та мережевого обладнання, повинні бути захищені від несанкціонованого доступу. Використання захищених кабельних каналів, замків на розподільчих шафах та фізичне маркування кабелів може допомогти уникнути фізичного підключення до мережі без дозволу.

4. *Резервне живлення та захист від перенапруги*. Для забезпечення надійності мережевого обладнання і запобігання втрати даних у разі перебоїв електропостачання важливо використовувати резервне живлення, таке як UPS, а також захист від перенапруги. Це дозволяє уникнути можливих пошкоджень обладнання та зберегти його працездатність.

5. *Регулярне фізичне обслуговування та оновлення обладнання*. Регулярне фізичне обслуговування мережевого обладнання, таке як перевірка на наявність оновлень програмного забезпечення, перевірка на наявність фізичних пошкоджень та заміна застарілого обладнання, допомагає забезпечити його надійну роботу та підвищити загальний рівень безпеки мережі.

Ці заходи фізичного захисту допомагають забезпечити надійну та безпечну роботу комп'ютерної мережі навчального закладу, запобігти несанкціонованому доступу до обладнання та зберегти цілісність даних та ресурсів мережі.

ВИСНОВКИ ДО РОЗДІЛУ 2

В цьому розділі було описано та опрацьовано тему безпеки комп’ютерних мереж, різновиди атак і методи їх запобігання.

Ця тема є невід’ємною частиною наших пристроїв, домашніх комп’ютерів і комп’ютерних мереж незалежно від їх типу. На це варто звертати увагу ще на самому початку, при проєктуванні, адже це впливає, навіть, елементарно розміщення технічного обладнання, яке буде використовуватися. Треба виділити певну частину бюджету, адже якщо брали великі мережі, такі як глобальні, там місць уражень значно більше, тому і безпека має бути відповідною. Від цих кроків і того як люди до цього поставляться залежить працездатність мережі і безпека, як особистих даних, так і робочих. Навіть мінімальний вірус може зробити велику проблему і зупинити всю роботу.

У випадку з комп’ютерною мережею навчального закладу трошки простіше, на мою думку, буде достатньо правильного налаштування зв’язків, використання

якісного антивірусного програмного забезпечення, інформаційної гігієни і надання учням інструкції щодо правильного користування комп’ютерами.

……

РОЗДІЛ 3
МОДЕЛЮВАННЯ МЕРЕЖІ НАВЧАЛЬНОГО ЗАКЛАДУ В ПРОГРАМНОМУ ПАКЕТІ HUAWEI ENSP

3.1. Загальні відомості про програмний пакет Huawei eNSP

Huawei eNSP (Enterprise Network Simulation Platform) - це програмне забезпечення, розроблене компанією Huawei, яке використовується для моделювання та симуляції комп'ютерних мереж [16]. Воно дозволяє інженерам з мережевого адміністрування віртуально будувати та тестувати мережеві топології без необхідності фізичного обладнання.

Основні можливості Huawei eNSP включають:

Моделювання мережевих топологій: eNSP надає можливість створювати віртуальні мережі, включаючи роутери, комутатори, мережеві пристрої та інші елементи інфраструктури. Користувачі можуть встановлювати параметри пристроїв, налаштовувати мережеві інтерфейси та робити інші необхідні налаштування.

Симуляція мережевого трафіку: eNSP дозволяє генерувати різні типи мережевого трафіку і тестувати його в мережевій топології. Це допомагає інженерам оцінити продуктивність мережі, ідентифікувати можливі проблеми та розробляти ефективні стратегії маршрутизації.

Стеження за мережевим трафіком: eNSP надає можливість переглядати та аналізувати мережевий трафік в реальному часі. Інженери можуть відстежувати дані про передачу пакетів, пропускну здатність мережі, затримки та інші метрики продуктивності.

Відлагодження мережевих протоколів: eNSP підтримує ряд мережевих протоколів, таких як OSPF, BGP, MPLS, VLAN та інші. Інженери можуть налаштовувати та відлагоджувати ці протоколи у віртуальному середовищі, перевіряти їх роботу та реагувати на можливі проблеми.

Інтеграція з реальним обладнанням: eNSP може бути підключений до реальних мережевих пристроїв Huawei для тестування та налаштування їх параметрів. Це дозволяє інженерам експериментувати з реальним обладнанням та виконувати різні тести без впливу на живу мережу.

Huawei eNSP є корисним інструментом для інженерів з мережевого адміністрування, оскільки воно дозволяє їм віртуально тестувати, моделювати та налаштовувати мережеві топології перед їх реалізацією у реальному світі [17]. Використання eNSP допомагає зменшити час і витрати на встановлення та налагодження мереж та сприяє покращенню якості мережевих рішень.

Рис. 3.1. Умовні позначення пристроїв в програмному пакеті Huawei eNSP

3.2. Проєкт мережі навчального закладу

Комунікаційні мережі є повсюдними в інформаційному суспільстві, а мережі кампусів завжди є основною частиною. Кампуси є скрізь, включаючи заводи, урядові будівлі та споруди, торгові центри, адміністративні будівлі, шкільні містечка та парки. Згідно зі статистичними даними, 90% міських жителів працюють і живуть в кампусах, 80% валового внутрішнього продукту (ВВП) створюється в кампусах, і кожна людина перебуває в кампусах по 18 годин щодня. Мережі кампусів, як інфраструктура для підключення кампусів до цифрового світу, є невід'ємною

частиною будівництва кампусу і відіграють все більшу роль у щоденній роботі, науково-дослідних роботах, виробництві та управлінні експлуатацією.

Побудова мережі для навчального закладу (кампусу) є важливим завданням, оскільки забезпечує зв'язок та обмін даними між всіма пристроями та користувачами в закладі. Ось кілька ключових причин, чому побудова мережі є необхідною:

Зв'язок та спільний доступ до ресурсів: мережа дозволяє студентам, викладачам та адміністраторам спілкуватися та спільно використовувати ресурси, такі як файли, друк, електронна пошта, веб-сайти, бібліотеки тощо. Це сприяє покращенню комунікації та співпраці всередині навчального закладу.

Доступ до Інтернету: мережа надає доступ до Інтернету для студентів та викладачів, що дозволяє отримувати інформацію, проводити дослідження, отримувати онлайн-освіту та використовувати різноманітні веб-приклади.

Електронна система навчання: багато навчальних закладів використовують електронні системи навчання, такі як платформи для онлайн-курсів, електронні бібліотеки, веб-сайти для навчальних матеріалів тощо. Мережа дозволяє студентам та викладачам отримати доступ до цих систем та зручно користуватися ними.

Безпека та контроль: мережа дозволяє встановити системи безпеки, такі як брандмауери, системи виявлення вторгнень та антивірусні програми, для захисту мережі та інформації від несанкціонованого доступу та кібератак.

Управління та моніторинг: мережа дозволяє адміністраторам моніторити та управляти всіма пристроями в мережі централізовано. Це забезпечує ефективне виявлення проблем, налаштування пристроїв та забезпечення безперебійної роботи мережі.

Масштабованість: мережа надає можливість розширювати та розгортати нові сервіси та пристрої в майбутньому. Навчальні заклади постійно зростають та змінюються, тому мережа повинна бути гнучкою та готовою до масштабування.

Загалом, побудова мережі для навчального закладу дозволяє забезпечити зручний та безперебійний зв'язок, доступ до ресурсів та сприяє ефективному навчанню та управлінню.

Мережева топологія. Потрібно побудувати мережу Навчального закладу. Будівля навчального закладу має шість поверхів. В даний час введено в експлуатацію три поверхи: зал прийому на першому поверсі, адміністративний відділ та кабінет директора на другому поверсі, навчально-наукові лабораторії та лекційні аудиторії на третьому поверсі. Кімната основного обладнання розміщена на першому поверсі, а маленька кімната для розміщення мережевих пристроїв розміщена на кожному з інших поверхів.

Вибір пристроїв та проєктування фізичної топології. У таблиці 3.1 наведено загальну кількість терміналів у мережі.

Таблиця 3.1

Загальна кількість терміналів у мережі навчального закладу

Поверхи будівлі навчального закладу	**Перший поверх**	**Другий поверх**	**Третій поверх**	**Інші поверхи (зарезервоване обладнання)**
Провідні термінали	10	200	200	500
Безпровідні термінали	100	50	50	200
Зауваження	Гостьові бездротові термінали + сервери	Комп’ютери + мобільні телефони		

Трафік від бездротових терміналів - це трафік доступу в Інтернет. Кожен клієнт має швидкість не меншу за 2 Мбіт/с.

Швидкість з'єднання комп'ютерів становить 100 Мбіт/с, а серверів - 1000 Мбіт/с.

Для поліпшення якості бездротового доступу на кожному поверсі потрібні принаймні три дводіапазонних точки доступу.

На рисунку 3.2. представлено проєкт фізичної топології телекомунікаційної мережі навчального закладу.

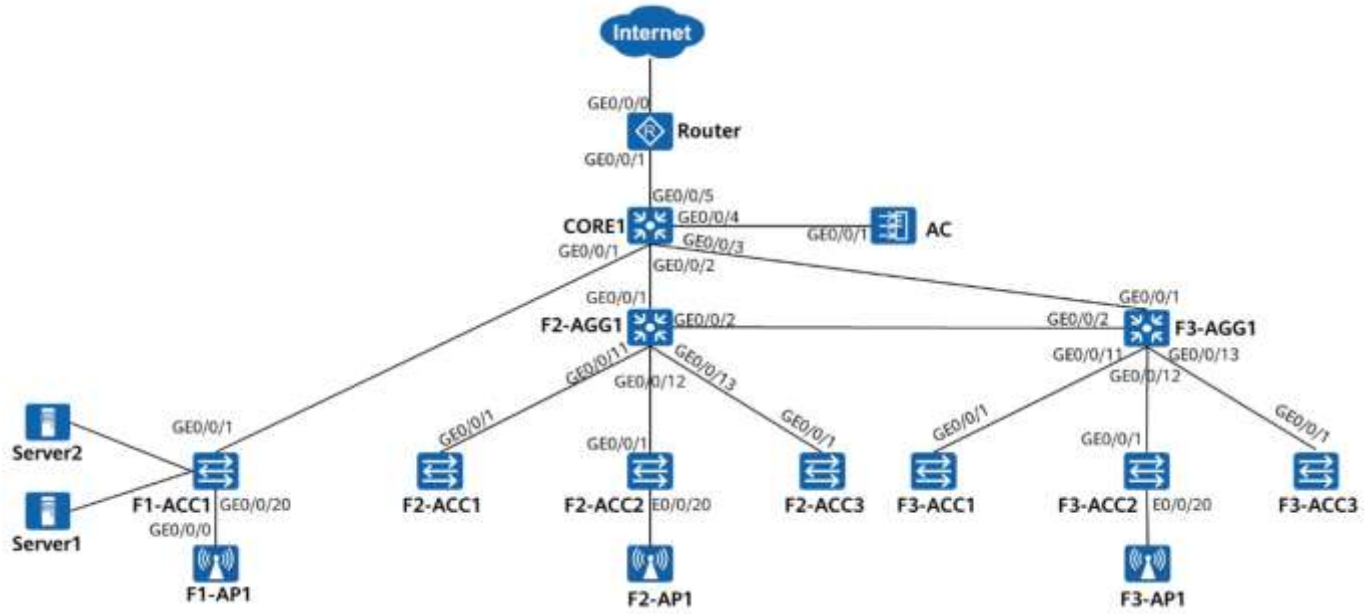

Рис. 3.2. Проєкт фізичної топології телекомунікаційної мережі навчального закладу

В таблиці 3.2 представлені номери інтерфейсів, що з'єднують компоненти запропонованої мережі.

Таблиця 3.2

Номери інтерфейсів

Пристрій	Номер інтерфейсу
F2-ACC1, F2-ACC2, F2-ACC3, F3-ACC1, F3-ACC2, та F3-ACC	E0/0/1~E0/0/222 GE0/0/1~GE0/0/2
F1-ACC1, F2-AGG1, F3-AGG1, та CORE1	GE0/0/1~GE0/0/24
AC	GE0/0/1~GE0/0/8
F1-AP1, F2-AP1, та F3-AP1	GE0/0/0~GE0/0/1
Router	GE0/0/0~GE0/0/2

Передумови для створення мережі. Створення VLAN у дротовій мережі:

− Порти комутатора доступу GE 0/0/1 до GE 0/0/10 у приміщенні основного обладнання підключаються до серверів і присвоюються одній і тій же VLAN.

− На другому поверсі F2-ACC2 підключений до кабінету директора, а інші комутатори - до адміністративного відділу. Два відділи належать до різних VLAN.

− На третьому поверсі E0/0/1 до E0/0/10 F3-ACC1 та F3-ACC3 належать до лекційних аудиторій, а E0/0/11 до E0/0/20 належать до навчально-наукових лабораторій.

− E0/0/1 до E0/0/19 з F3-ACC2 належать до лекційних аудиторій.

Створення VLAN у бездротовій мережі:

− Бездротові термінали на різних поверхах повинні бути призначені різним VLAN.

− Управління бездротовою мережею VLAN на кожному поверсі відрізняється.

В таблиці 3.3 представлені ідентифікатори VLAN для дротової мережі навчального закладу.

Таблиця 3.3

Ідентифікатори VLAN для дротової мережі

VLAN ID	**Description**
1	Рівень 2 управління пристроями VLAN на першому поверсі
2	Рівень 2 управління пристроями VLAN на другому поверсі
3	Рівень 2 управління пристроями VLAN на третьому поверсі
100	VLAN для серверів
101	VLAN для офісу директора
102	VLAN для адміністративного відділу
103	VLAN для лекційних аудиторій
104	VLAN для навчально-наукових лабораторій
105	VLAN для бездротових терміналів на першому поверсі
106	VLAN для бездротових терміналів на другому поверсі

Закінчення таблиці 3.3

107	VLAN для бездротових терміналів на третьому поверсі
201	VLAN для взаємозв'язку між F2-AGG1 і CORE1
202	VLAN для взаємозв'язку між F3-AGG1 і CORE1
203	VLAN для взаємозв'язку між F2-AGG1 і F3-AGG1
204	VLAN для взаємозв'язку між CORE1 та маршрутизатором
205	Управління бездротовою мережею VLAN на першому поверсі
206	Управління бездротовою мережею VLAN на другому поверсі
207	Управління бездротовою мережею VLAN на третьому поверсі

Створення мережі. Діапазон адрес - мережа 192.168.0.0/16. Вимоги такі:

− Перший поверх: сервери використовують статичні IP-адреси. IP-адреси бездротових станцій та точки доступу призначаються CORE1 через DHCP. Шлюз знаходиться на CORE1. IP-адреси управління комутаторами доступу є статичними IP-адресами, а шлюз знаходиться на CORE1.

− Другий і третій поверхи: IP-адреси всіх дротових терміналів, бездротових терміналів та бездротових точок доступу призначаються комутатором агрегування відповідного поверху через DHCP. Шлюз розгортається на агрегаційних комутаторах. IP-адреси управління комутаторами доступу є статичними IP-адресами, а шлюз знаходиться на комутаторі агрегації відповідного поверху. OSPF використовується у всій мережі, щоб забезпечити зв'язок між сервісними мережами. Всі термінали отримують доступ до Інтернету через маршрутизатор.

У таблиці 3.4 представлено планування мережі з розподіленням адресного простору.

Таблиця 3.4

Розподіл простору IP адрес в мережі та маршрутизація

IP мережа	**Метод призначення адреси та шлюз**	**Конфігурація маршрутизації**	**Опис мережі**
192.168.1.0/24	Статична адреса; CORE1	Маршрут за замовчуванням вказує на CORE1	Мережа керування пристроями рівня 2 на першому поверсі
192.168.2.0/24	Статична адреса; F2-AGG1	Маршрут за замовчуванням вказує на F2-AGG1	Мережа керування пристроями рівня 2 на другому поверсі
192.168.3.0/24	Статична адреса; F3-AGG	Маршрут за замовчуванням вказує на F3-AGG	Мережа керування пристроями рівня 2 на третьому поверсі
192.168.100.0/24	Статична адреса; CORE1	Оголошується в OSPF через пристрої-шлюзи	Мережа серверів
192.168.101.0/24	Присвоєно F2-AGG1 за допомогою DHCP; F2-AGG1		Мережа офісу директора
192.168.102.0/24			Мережа адміністративного відділу
192.168.103.0/24	Присвоєно F3-AGG1 за допомогою DHCP; F3-AGG1		Мережа лекційних аудиторій

Продовження таблиці 3.4

192.168.104.0/24			Мережа навчально-наукових лабораторій
192.168.105.0/24	Присвоєно CORE1 за допомогою DHCP; CORE1		Мережа бездротових терміналів на першому поверсі
192.168.106.0/24	Присвоєно F2-AGG1 за допомогою DHCP; F2-AGG1		Мережа бездротових терміналів на другому поверсі
192.168.107.0/24	Присвоєно F3-AGG1 за допомогою DHCP; F3-AGG1		Мережа бездротових терміналів на третьому поверсі
192.168.201.0/30	Статична адреса; не потребує використання шлюзу	OSPF увімкнено, сусідські відносини встановлені, і маршрут за замовчуванням оголошується маршрутизатором	Мережа для з'єднання між F2-AGG1 і CORE1
192.168.202.0/30			Мережа для з'єднання між F3-AGG1 і CORE1
192.168.203.0/30			Мережа для з'єднання між F2-AGG1 і F3-AGG1
192.168.204.0/30			Мережа для з'єднання між CORE1 і маршрутизатором

Закінчення таблиці 3.4

192.168.205.0/24	Присвоєно CORE1 за допомогою DHCP; CORE1	Оголошується в OSPF через пристрої-шлюзи	Мережа управління бездротовою мережею на першому поверсі
192.168.206.0/24	Присвоєно F2-AGG1 through DHCP; F2-AGG1		Мережа керування бездротовою мережею на другому поверсі
192.168.207.0/24	Присвоєно F3-AGG1 t за допомогою DHCP; F3-AGG1		Бездротова мережа управління мережею на третьому поверсі

Вимоги до бездротової мережі. Усі точки доступу управляються AC уніфіковано, і AC має обмежену ефективність переадресації.

- Точки доступу на першому поверсі зареєстровані на рівні 2.
- Усі точки доступу на другому та третьому поверхах реєструються в AC на рівні 3. Шлюз AC є CORE1.

SSID для кожного поверху.

- Використовується політика безпеки WPA2-WPA3 + PSK + AES.
- Кожен поверх має різні SSID та пароль.

Таблиця 3.5

Планування бездротової мережі навчального закладу

Пункт	**WLAN на першому поверсі**	**WLAN на другому поверсі**	**WLAN на третьому поверсі**
VLAN керування точкою доступу	VLAN205	VLAN206	VLAN207

Продовження таблиці 3.5

Служба VLAN	VLAN105	VLAN106	VLAN107
DHCP scepвер	CORE1 призначає IP адреси до AP і STA.	F2-AGG1 призначає IP-адреси AP і STA.	F3-AGG1 призначає IP-адреси AP і STA.
IP-адреса вихідного інтерфейсу AC	VLANIF205: 192.168.205.253/24		
група AP	Назва: WLAN-F1 Профіль VAP: WLAN-F1 Регуляторний профіль домену: за замовчуванням	Назва: WLAN-F2. Профіль VAP: WLAN-F2 Регуляторний профіль домену: за замовчуванням	Назва: WLAN-F3 Профіль VAP: WLAN-F3 Регуляторний профіль домену: за замовчуванням
Регуляторний профіль домену	Ім'я: за замовчуванням Код країни: UA		
Профіль SSID	Назва: WLAN-F1 Назва SSID: WLAN-F1	Назва профілю: WLAN-F2 Назва SSID: WLAN-F2	Назва профілю: WLAN-F3 Назва SSID: WLAN-F3
Security profile	Назва: WLAN-F1 Політика безпеки: WPA2-WPA3+PSK+AES Пароль: WLAN@Guest123	Назва: WLAN-F2 Політика безпеки: WPA-WPA2+PSK+AES Пароль: WLAN@Employee2	Назва: WLAN-F3 Політика безпеки: WPA2-WPA3+PSK+AES Пароль: WLAN@Employee3

Закінчення таблиці 3.5

VAP профіль	Назва: WLAN-F1 Режим переадресації: пряма переадресація VLAN служби: VLAN: 105 Профілі: Профіль SSID: WLAN-F1; Профіль безпеки: WLAN-F1	Назва: WLAN-F2 Режим переадресації: пряма переадресація Служба VLAN: 106 Профілі: Профіль SSID: WLAN-F2 Профіль безпеки: WLAN-F2	Назва: WLAN-F3 Режим переадресації: пряма переадресація VLAN служби: VLAN: 107 Профілі: Профіль SSID: WLAN-F3 Профіль безпеки: WLAN-F3

Вимоги до налаштування бездротової мережі:

Ідентифікатор гостя SSID не має доступу до інтрамережі компанії.

− Доступ до інтернету можуть мати лише бездротові термінали.

− Маршрутизатор використовує статичну IP-адресу для доступу до Інтернету. Оператор призначає маршрутизатору IP-адреси з 1.1.1.1 до 1.1.1.10 (з 24-бітовою маскою). next-hop IP-адреса маршрутизатора для доступу до Інтернету - 1.1.1.254

− Веб-сервер на підприємстві повинен надавати послуги для зовнішніх користувачів. Приватна IP-адреса веб-сервера - 192.168.100.1, а номер порту - 80. Щоб забезпечити безпеку сервера, відображення NAT надається лише для веб-служб.

Проєктування мережевого управління:

− SNMPv3 використовується для зв’язку з новою системою управління, а аутентифікація та шифрування налаштовані для підвищення безпеки.

– Усі пристрої, крім маршрутизатора та AC, взаємодіють з NMS за адресою 192.168.100.2/24 через управління VLAN.

– Маршрутизатори взаємодіють з NMS через GE0/0/1.

– AC з'єднується з NMS через VLANIF 205.

– Усі пристрої повинні мати можливість повідомляти NMS про тривоги SNMP.

3.3. Проєктування телекомунікаційної мережі навчального закладу в програмному пакеті Huawei eNSP

Враховуючи всі необхідні вимоги до телекомунікаційної мережі навчального закладу, побудуємо її фізичне втілення в програмному пакеті Huawei eNSP.

На рисунку 3.3 представлена телекомунікаційна мережа навчального закладу, що включає в себе: зал прийому на першому поверсі, адміністративний відділ та кабінет директора на другому поверсі, навчально-наукові лабораторії та лекційні аудиторії на третьому поверсі.

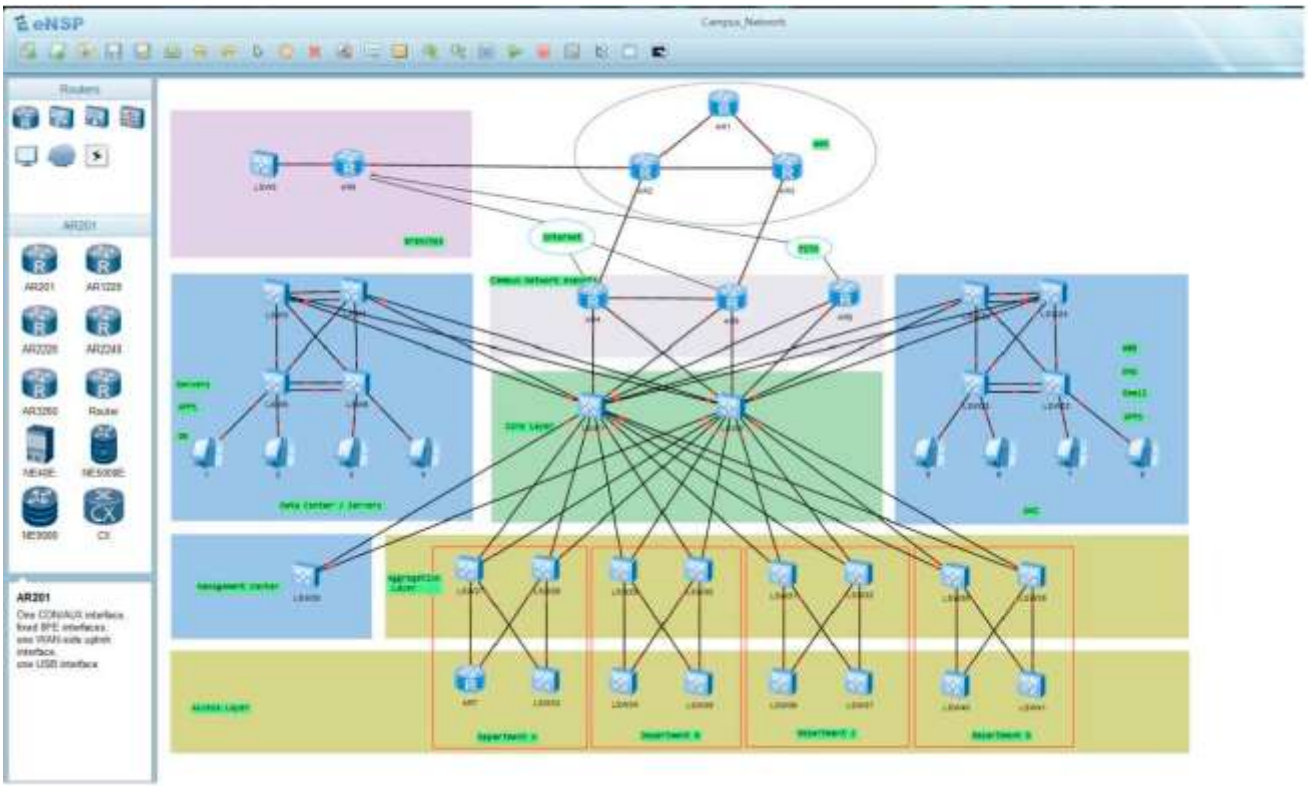

Рис. 3.3. Мережа навчального закладу в програмному пакеті Huawei eNSP

Приклад налаштування маршрутизації між компонентами мережі AR1 – AR3 за допомогою командного рядка представлено на рисунку 3.4.

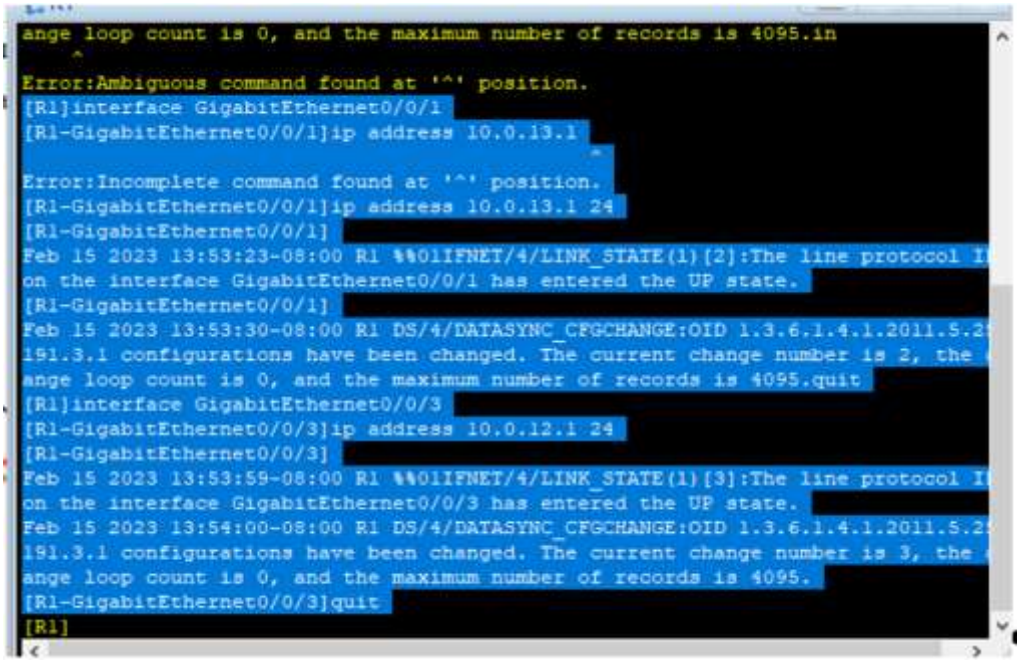

Рис. 3.4. Налаштування за допомогою командного рядка

Для перевірки вірності з’єднання використовуємо команду PING. Приклад використання команди в мережі навчального закладу представлено на рисунку 3.5.

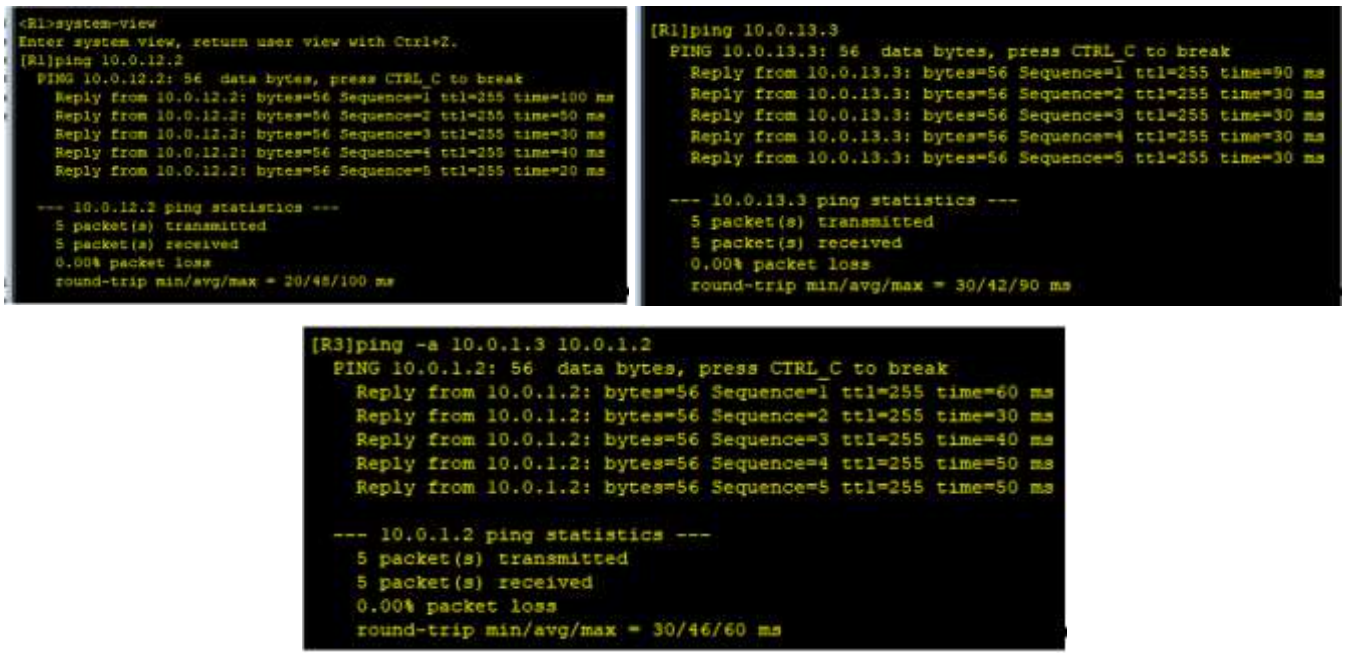

Рис. 3.5. Приклад використання команди PING для перевірки вірності налаштування з’єднання мережевого устаткування

Налаштування DHCP за допомогою веб-інтерфейсу комунікаційного обладнання представлено на рисунку 3.6.

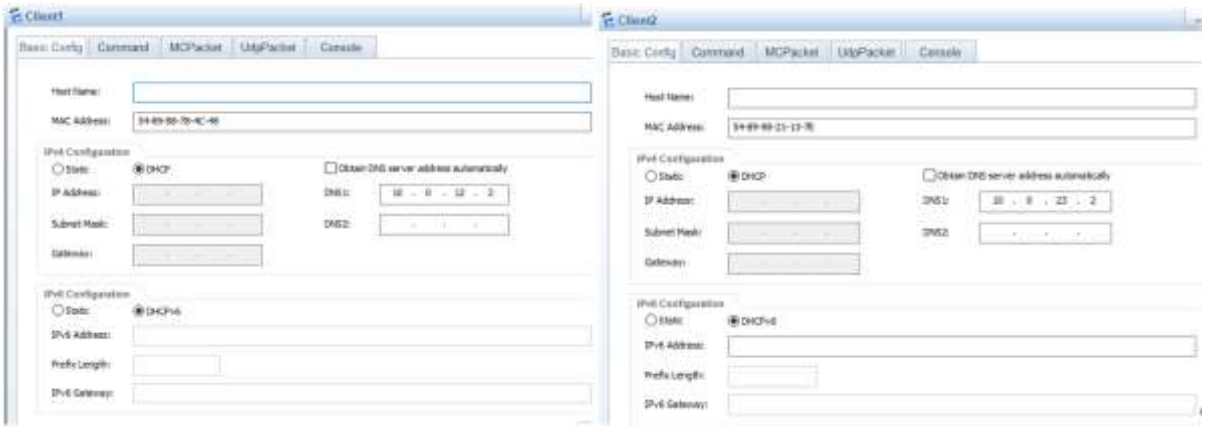

Рис. 3.6. Налаштування DHCP за допомогою веб-інтерфейсу

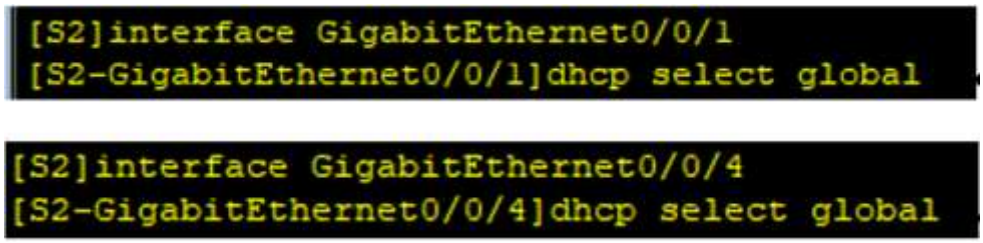

Рис. 3.7. Активація DHCP серверу за допомогою командного рядка

Повний перелік налаштувань телекомунікаційної мережі навчального закладу за на базі програмного пакету Huawei eNSP представлено в Додатку А до кваліфікаційної роботи.

ВИСНОВКИ ДО РОЗДІЛУ 3

В даному розділі кваліфікаційної роботи представлено проєкт телекомунікаційної мережі навчального закладу в програмному продуктів Huawei eNSP, що включає в себе: зал прийому на першому поверсі, адміністративний відділ та кабінет директора на другому поверсі, навчально-наукові лабораторії та лекційні аудиторії на третьому поверсі. Кімната основного обладнання розміщена на першому поверсі, а маленька кімната для розміщення мережевих пристроїв розміщена на кожному з інших поверхів.

Загалом, побудова телекомунікаційної мережі для навчального закладу вимагає детального планування та врахування специфічних потреб навчального закладу. Важливо забезпечити ефективну комунікацію, надійність, безпеку та масштабованість мережі, щоб задовольнити потреби користувачів та сприяти ефективному навчанню та управлінню.

ВИСНОВКИ

В рамках даної дипломної роботи було проведено детальне дослідження та аналіз локальної комп'ютерної мережі навчального закладу. Робота складалась з трьох розділів, в кожному з яких досліджувалися певні аспекти комп'ютерних мереж.

У першому розділі були розглянуті основні терміни і поняття, які відіграють важливу роль у розумінні комп'ютерних мереж. Було детально розглянуто такі терміни, як топологія мережі, протоколи передачі даних, мережеве обладнання та мережеві пристрої. Крім того, у розділі були представлені різні технології, які використовуються для побудови локальних мереж. Зокрема, було оглянуто Ethernet, який є одним з найпоширеніших стандартів для передачі даних у локальних мережах. Також були розглянуті бездротові технології, зокрема Wi-Fi, які дозволяють безпроводову передачу даних у межах комп'ютерної мережі.

Дослідження цих технологій дозволяє розуміти принципи їх роботи, переваги та недоліки, а також правильно обирати відповідну технологію залежно від потреб і вимог локальної мережі навчального закладу. Розуміння основних термінів та понять допомагає забезпечити ефективну роботу мережі, забезпечити надійну передачу даних та забезпечити безпеку.

Таким чином, перший розділ дипломної роботи надає необхідні знання та базову основу для подальшого розгляду та дослідження локальної комп'ютерної мережі навчального закладу.

Другий розділ - виявився надзвичайно важливим для забезпечення безпеки локальної комп'ютерної мережі навчального закладу. У цьому розділі було проведено грунтовне дослідження загроз та ризиків, які можуть виникати у комп'ютерних мережах, а також висвітлено різні методи та технології для ефективного захисту мережі від несанкціонованого доступу та атак. Під час дослідження було виявлено, що комп'ютерні мережі стикаються з різноманітними загрозами, такими як віруси, зловмисні програми, хакерські атаки та перехоплення даних. Ці загрози можуть

призвести до порушення конфіденційності, цілісності та доступності даних, а також до втрати важливої інформації.

Для захисту мережі було розглянуто різні методи і технології, такі як використання брандмауерів, систем виявлення вторгнень (IDS), систем захисту від вторгнень (IPS), аутентифікація та авторизація користувачів, шифрування даних та використання віртуальних приватних мереж (VPN). Враховуючи зростаючу кількість загроз у комп'ютерних мережах, розділ про безпеку мережі набуває особливого значення. Забезпечення безпеки мережі є необхідним для захисту конфіденційної інформації, запобігання витоку даних, забезпечення безперебійної роботи мережі та збереження репутації навчального закладу.

Таким чином, другий розділ дипломної роботи надає глибоке розуміння загроз та ризиків у комп'ютерних мережах та пропонує ефективні методи і технології для забезпечення безпеки локальної комп'ютерної мережі навчального закладу.

Третій розділ пропонує конкретний підхід до проектування та налаштування локальної комп'ютерної мережі навчального закладу. Застосування програмного обладнання Huawei eNSP дозволяє виконати оптимальне проектування та налаштування компонентів мережі з метою забезпечення її ефективної роботи та безпеки. У цьому розділі було розглянуто процес проектування мережі, включаючи визначення топології, вибір необхідного мережевого обладнання, а також розподіл IP-адрес та налаштування мережевих пристроїв. Використання програмного обладнання Huawei eNSP спрощує цей процес і дозволяє здійснити віртуальне моделювання мережі для перевірки її працездатності та ефективності. Окрім того, у розділі була приділена особлива увага безпеці мережі. Було розглянуто методи та налаштування для забезпечення безпеки мережевого трафіку, виявлення та запобігання потенційним загрозам, а також контролю доступу до ресурсів мережі.

В результаті дослідження та застосування програмного обладнання Huawei eNSP, вдалося створити оптимальну мережеву інфраструктуру для навчального закладу, забезпечивши ефективну передачу даних, високу доступність та безпеку мережі.

Тому, можна відмітити, що дослідження та розробка локальної комп'ютерної мережі навчального закладу є важливим завданням для забезпечення якісної освіти та комунікації у навчальному середовищі. Правильне проектування, налаштування та забезпечення безпеки мережі відіграють критичну роль у забезпеченні безперебійної та ефективної роботи навчального закладу. Використання програмного обладнання Huawei eNSP може сприяти оптимальному проектуванню та налаштуванню мережі, а використання проаналізованих даних дає основу для подальших досліджень та вдосконалення локальних комп'ютерних мереж у навчальних закладах з метою покращення якості освітнього процесу та задоволення потреб учасників навчального середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Таненбаум, Е. Комп'ютерні мережі / Ендрю Таненбаум, Девід Везеролл. – 5-те видання. – Київ: Видавництво "Дія", 2012. – 960 с.

2. Comer, D. E. Computer Networks and Internets / Douglas E. Comer. – 6th edition. – Upper Saddle River, NJ: Prentice Hall, 2014. – 672 p.

3. Peterson, L. L. Computer Networks: A Systems Approach / Larry L. Peterson, Bruce S. Davie. – 5th edition. – Burlington, MA: Morgan Kaufmann, 2011. – 920 p.

4. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

5. Stallings, W. Data and Computer Communications / William Stallings. – 10th edition. – Boston, MA: Pearson, 2013. – 912 p.

6. Kurose, J. F. Computer Networking: A Top-Down Approach / James F. Kurose, Keith W. Ross. – 7th edition. – Boston, MA: Pearson, 2016. – 864 p.

7. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

8. Tanenbaum, A. S. Computer Networks / Andrew S. Tanenbaum, David J. Wetherall. – 5th edition. – Upper Saddle River, NJ: Pearson, 2010. – 960 p.

9. Cisco Networking Academy. CCNA Routing and Switching: Introduction to Networks Companion Guide / Cisco Networking Academy. – 6th edition. – Indianapolis, IN: Cisco Press, 2016. – 736 p.

10. Клименко, О. О. Основи цифрової обробки сигналів: навчальний посібник / О. О. Клименко, О. Л. Букрєєва, А. А. Клименко. – Київ: Видавничий дім "Києво-Могилянська академія", 2018. – 336 с.

11. Mitchell, B. Local Area Networks: A Complete Guide to Design, Implementation, and Management / Brian Mitchell. – 1st edition. – New York, NY: CRC Press, 2019. – 258 p.

12. Hunt, C. TCP/IP Network Administration / Craig Hunt. – 3rd edition. – Sebastopol, CA: O'Reilly Media, 2002. – 746 p.

13. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

14. Goleniewski, L. Network+ Guide to Networks / Tamara Dean, Jean Andrews, Lawrence Goleniewski. – 8th edition. – Boston, MA: Cengage Learning, 2015. – 912 p.

15. Голобородько, В. О. Основи комп'ютерних мереж: навчальний посібник / В. О. Голобородько, Ю. О. Клименко. – Київ: НУ "Львівська політехніка", 2017. – 296 с.

16. Fitzgerald, J. Computer Networking Basics: An Introductory Guide for Complete Beginners / James Fitzgerald. – 2nd edition. – CreateSpace Independent Publishing Platform, 2017. – 84 p.

17. Василенко, М. М. Комп'ютерні мережі: навчальний посібник / М. М. Василенко, С. В. Коляда. – Київ: Ліра-К, 2018. – 304 с.