Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування вищого навчального закладу)
Навчально-науковий інститут інформаційних технологій та робототехніки
(повне найменування інституту, назва факультету (відділення))
Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи
бакалавр
(освітній рівень)
на тему **Розробка проєкту локальної обчислювальної мережі приміщень Національного університету "Полтавська політехніка імені Юрія Кондратюка**

Виконав: студент 4 курсу, групи 401-ТТ
спеціальність 172 «Телекомунікації та радіотехніка»
(шифр і назва напрямку підготовки, спеціальності)
Фенько В.В.
(прізвище та ініціали)
Керівник Лактіонов О.І.
(прізвище та ініціали)
Рецезент Обіход Я.Я.
(прізвище та ініціали)

Полтава – 2021 рік

РЕФЕРАТ

Обсяг пояснювальної записки складає 66 сторінок. Робота містить 16 ілюстрацій, 9 таблиць, 13 бібліографічних посилань та 4 додатків.

Метою роботи є розробка проекту локальної обчислювальної мережі першого, другого та третього поверхів «Ф» корпусу Національного університету "Полтавська політехніка імені Юрія Кондратюка». Вибір оптимального апаратного забезпечення та налаштування мережі, для забезпечення масштабованості та максимальної продуктивності мережі в рамках даної мережі та окремих її сегментів.

Результатами даної роботи є вибір оптимальної топології мережі, оцінка можливості масштабування мережі та вибір відповідного активного обладнання, а також приклад оптимального налаштування апаратного забезпечення для отримання кращих якісних характеристик.

При обраній конфігурації мережі передбачається спрощення адміністрування мережі, зниження широкомовного трафіку та створення можливості масштабування мережі в подальшому.

Ключові слова: топологія, ієрархічна модель, сегмент, віртуальна мережа, трафік, пропускна здатність.

ABSTRACT

The explanatory note is 66 pages long. The work contains 16 illustrations, 9 tables, 13 bibliographic references and 4 appendices. The purpose of the work is to develop a project for a local computer network of the first, second and third floors of the «F» building of the National University "Yuri Kondratyuk Poltava Polytechnic". The results of this work are the selection of the optimal network topology, the assessment of the scalability of the network and the selection of the appropriate hardware, as well as an example of the optimal configuration of the hardware to obtain the best quality characteristics. With the chosen network configuration, it is planned to simplify network administration, reduce broadcast traffic and create the ability to scale the network in the future. Key words: topology, hierarchical model, segment, virtual area network, traffic, bandwidth.

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій та робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Освітньо-кваліфікаційний рівень Бакалавр
Спеціальність 172 «Електроенергетика, електротехніка та електромеханіка»

ЗАТВЕРДЖУЮ

Завідувач кафедри
автоматики, електроніки та
телекомунікацій

_____О.В.Шефер
“ 11 ” травня 2021 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Феньку Валентину Володимировичу

1. Тема роботи «Розробка проєкту локальної обчислювальної мережі приміщень Національного університету "Полтавська політехніка імені Юрія Кондратюка»
керівник роботи Лактіонов Олександр Ігорович, к.т.н., доцент
затверджена наказом вищого навчального закладу від 15.06.2021 року №_____

2. Строк подання студентом проекту (роботи) 15.06.2021 р.

3. Вихідні дані до проекту (роботи) розміри та план будівлі

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Технології та стандарти при побудові сучасних обчислювальних мереж. Розрахунок та вибір архітектури мережі. Моделювання роботи мережі.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):
   1) Оцінка масштабованості мережі
   2) Топологія на основі обраної мережевої моделі та апаратне забезпечення
   3) Сегментація мережі та схема підключення активного обладнання
   4) Розподіл IP адрес. Налаштування пулу адрес на маршрутизаторі за протоколом DHCP
   5) Перевірка налаштування модельованої мережі
6. Дата видачі завдання 11.05.2021 р.

ЗМІСТ

ВСТУП

З самого початку розвитку обчислювальної техніки, зокрема комп'ютерів, існувала задача поєднання останніх у єдиний інформаційний простір, з метою обміну повідомленнями між віддаленими пристроями. З урахуванням існуючого на той час принципу універсального (однорідного) принципу представлення даних, рішення поставленої задачі відкривало багато нових можливостей у подальшому. Дана концепція розвивалась досить стрімко, що сприяло розробці перших моделей мережевої взаємодії, які майже у своєму первісному виді зберіглися до сьогодення, та апаратного забезпечення для реалізації необхідних функції згідно поставленої задачі.

На сьогоднішній день інформаційні технології стали невід'ємною частиною суспільства. Ці зміни стосуються майже усіх аспектів нашого життя, в тому числі й роботи та навчання, зокрема при підготовці спеціалістів (актуально для будь-якої спеціальності). Якщо на початку розвитку комп'ютерних систем, локальні мережі можна було зустріти лише в державних установах та у провідних вищих навчальних закладах, то сьогодні дана привілея доступна для шкіл, приміщень малого та середнього бізнесу та навіть в межах власної квартири.

З розвитком інформаційних технологій з'являлося все більше нових стандартів апаратного та програмного забезпечення для побудови мереж. На сьогоднішній день існує безліч пристроїв, що виконують одну функції але мають різний набір технічних характеристик. Таким чином, існує завдання вибору оптимального апаратного забезпечення. Крім того, необхідно правильно організувати фізичну та логічну топології мережі, та провести налаштування обладнання таким чином, щоб забезпечити максимальну продуктивність роботи мережі.

У рамках даної кваліфікаційної роботи бакалавра розглядається розробка проекту локальної обчислювальної мережі приміщень декількох поверхів начального закладу. На момент написання роботи, представлена мережа налічує деяку кількість комп'ютерів, що мають доступ до глобальної мережі, але план мережі відсутній.

Беручи до уваги вищесказане поставлена задача включає наступні етапи розробки проекту:

- розглянути можливості масштабування мережі;
- провести вибір мережевої архітектури для побудови фізичної топології мережі;
- Здійснити вибір апаратного забезпечення;
- Провести оцінку ефективності обраної топології та активного обладнання з точки зору пропускної здатності;
- здійснити вибір оптимального варіанту налаштування обладнання;
- провести моделювання мережі для перевірки роботи обраної конфігурації.

Таким чином, у даному проекту мережі передбачається раціональне використання пропускної здатності мережі (зменшення кількості широкомовного трафіку) та можливість забезпечення масштабування мережі у подальшому.

1. ТЕХНОЛОГІЇ ТА СТАНДАРТИ ПРИ ПОБУДОВІ СУЧАСНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

Еталонні моделі OSI та TCP/IP – це дві важливі мережеві архітектури, що поділяють мережеву взаємодію на рівні абстракції для спрощення аналізу роботи мережі в цілому. Протоколи, що прив'язані до відповідних рівнів моделі OSI на даний час не використовуються, але сама теоретична модель актуальна, а властивості, що притаманні кожному з її рівнів є важливими. І навпаки – протоколи мережевої моделі TCP/IP активно використовуються (дана мережева модель тісно зв'язана з технологією Ethernet), але сама модель майже не використовуються [1].

Ще одна вагома причина, чому протоколи архітектури OSI не знайшли практичного застосування – це значний час її розробки. У свою чергу модель TCP/IP з самого початку передбачала прикладне застосування та набувала розвитку у подальшому. Таким чином, модель OSI не застосовується безпосередньо, але слугує базовою моделлю, на основі якої будується усі сучасні стеки протоколів, що застосовуються у реальних комп'ютерних мережах. Тому дану архітектури іноді називають «довідковою моделлю» [2].

1.1. Еталонна мережева модель OSI

Еталонна модель OSI – це перший крок у спробі розробки міжнародного стандарту протоколів. Міжнародна організація по стандартизації (International Organization for Standardization, ISO) розробила дану модель в 1983 на основі вже існуючих напрацювань. Дана модель отримала назву ISO/OSI – модель взаємодії відкритих систем (OSI Open Systems Interconnection)[3].

Модель включає сім рівнів. Така структура обумовлена наступними міркуваннями:

1) Існування кожного рівня повинно бути обумовлено необхідністю окремого рівня абстракції.
2) Кожен рівень повинен виконувати строго фіксовану низку функцій.
3) Вибір функцій для кожного рівня повинен враховувати необхідність створення стандартизованих міжнародних протоколів, що йому відповідатимуть.
4) Границі розподілу рівнів повинні обиратися таким чином, щоб передача даних між інтерфейсами різних рівнів була мінімальна.
5) Кількість рівнів повинна бути достатньою великою для того щоб різні функції не перетиналися на одному рівні абстракції, але не занадто великою, щоб не нагромаджувати архітектуру в цілому [1].

Таким чином у даній мережевій архітектурі кожен рівень взаємодії має свої стандартні назви та набір притаманних йому функцій.

Згідно з попередніми міркуваннями щодо структури даної архітектури, кожен рівень працює лише з однією, чітко визначеною частиною мережевої взаємодії. У стеку протоколів OSI визначається сім рівнів (шарів) абстракції. Кожен рівень моделі має інтерфейси для з'єднання з рівнями, що лежать вище або нижче. Кожен рівень працює із своїм типом даних (рис. 1.1).

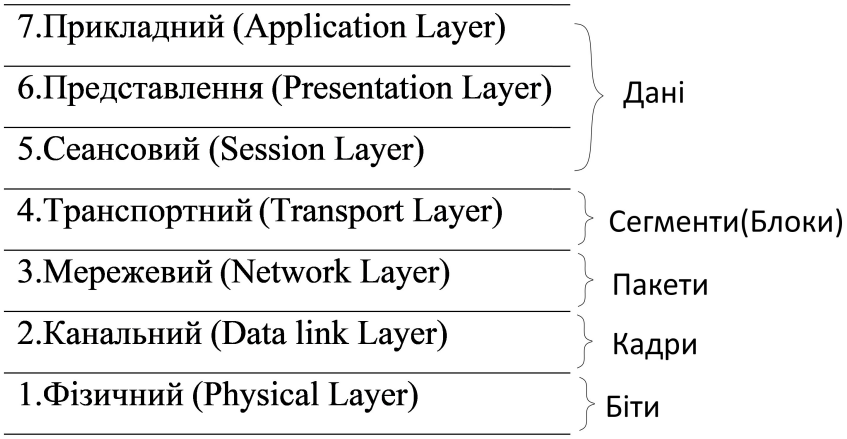


Рисунок 1.1 –Типи даних за рівнями мережевої архітектури OSI

Повідомлення від комп’ютера А до комп’ютера Б послідовно передається від вищого рівня до нижчого і в зворотному напрямку (рис. 1.2).

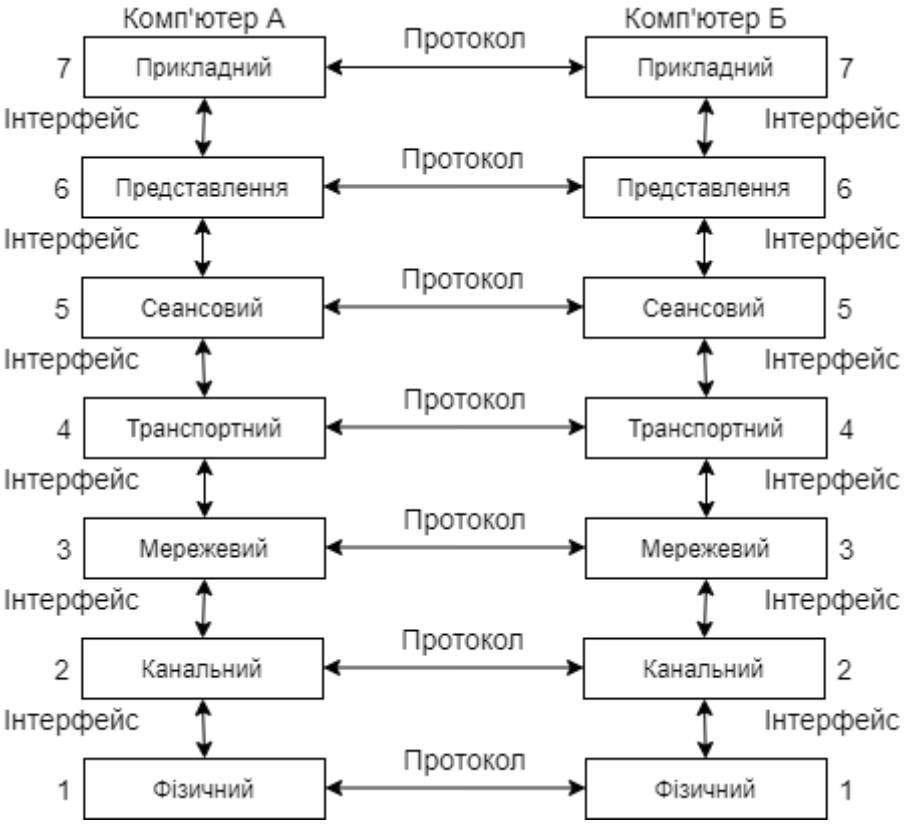


Рисунок 1.2 - Схема взаємодії двох комп’ютерів по моделі OSI/ISO

На кожному рівні надлишкова службова інформація обробляється на видаляється для передачі корисного навантаження на наступний рівень. Таким чином, поки не досягне прикладного рівня [2].

Більш детально про кожний з рівнів:

Фізичний рівень встановлює, підтримує та розриває безпосереднє з’єднання з фізичним каналом зв’язку (вита пара, оптоволокно або коаксіальний кабель тощо). Біти інформації необхідно передати на відповідну відстань та відтворити на прийомній стороні з заданим рівнем достовірності відповідно до заданих характеристик середовища поширення сигналу.

Канальний рівень встановлює логічне з’єднання між взаємодіючими вузлами мережі. Визначається швидкість прийом-передачі, встановлюється

надійне з’єднання за допомогою виявлення та виправлення помилок. Канальний рівень ділиться на два локальних підрівня:

- Логічної передачі даних (LLC, Logical Link Control).
- Управління доступом до мережі (MAC, Media Access Control)

Як було зазначено раніше, дані на канальному рівні представлені кадрами. Вхідні дані фізичного рівня (біти) групуються в кадри, розмір яких варіюється від сотень до тисяч байт (1 байт = 8 біт). Кадр формується відповідно до стандартів канального рівня використовуваної технології (Ethernet,Token Ring FDDI). Як правила кадр включає у собі контрольну суму (FCS – Frame Check Sequence) для перевірки послідовності бітів на помилки.

Мережевий рівень виконує логічну адресацію, комутацію (каналів, повідомлень, пакетів) та маршрутизацію при передачі даних від джерела до адресата. Функції мережевого рівня реалізуються групою протоколів (Наприклад IP протокол). Таким чином основна задача мережевого рівня є розрахунок оптимального маршруту для передачі даних, представлених пакетами.

Транспортний рівень необхідний для надійної передачі даних від джерела до адресата. Модель OSI пропонує п’ять класів транспортного сервісу (від нижчого 0 до вищого 5). До протоколів транспортного рівня відносять протоколи UDP (User Datagram Protocol) и TCP (Transmission Control Protocol). Основною відміною двох даних протоколів є перевірка наявності встановлення з’єднання (Таким чином створюється компроміс між надійністю та швидкістю передачі даних).

Сеансові рівень. Даний рівень відповідає за створення сеансу, його підтримку деякий значний проміжок часу та завершення. Також даний рівень виконує задачу синхронізації, визначає права на передачі даних у мережі й таке інше. Як правило, функції даного рівня поєднуються с функціями інших рівнів моделі OSI.

Рівень представлення. Даний рівень займається перетворенням інформації, що передається у мережі, але не змінює її початковий зміст. Сюди можна віднести алгоритми шифрування / дешифрування даних, стиск та розпакування даних, приведення їх до необхідного формату, переклад з рівних мов і таке інше. Як приклад, криптографічний протокол SSL (Secure Socket Layer).

Прикладний рівень. На прикладному рівні прикладні процеси користувача мережі (програмні додатки) отримують безпосередній доступ до ресурсів мережі. Також даний рівень організує передачу файлів, обмін електронними повідомленнями, управління мережею і таке інше. Як приклад, можна привести протокол передачі гіпертекстових файлів HTTP, що може бути прочитаний браузером, а також протокол передачі файлів FTP та протокол передачі пошти SMTP [3].

1.2. Мережева модель передачі даних TCP/IP

За весь час існування комп'ютерних мереж було представлено багато різних протоколів обміну даними, але найбільше розповсюдження отримав стек протоколів TCP/IP. До складу даного стеку протоколів входять протоколи TCP та IP. Серед інших протоколів даної моделі слід визначити службу доменних імен DNS, що займається перетворенням логічних адрес у зручний для кінцевого користувача вигляд та навпаки, зазначений раніше протокол передачі файлів FTP, який займається передачею файлів та набір протоколів NFS, що забезпечує доступ до віддалених файлових систем.

Протоколи TCP/IP використовувались у комп'ютерній мережі ARPANET, що можна назвати прототипом сучасного інтернету. Існування багатьох технологій починається з ініціативи військових, і ARPANET не є виключенням. ARPANET була дослідницькою мережею Міністерства оборони США. З часом

дана мережа поєднувала у собі сотні університетів та державних установ за допомогою виділених телефонних ліній. Таким чином мережа ускладнювалася, збільшуючись в масштабах, і почали формуватися інші мережі з іншими принципами передачі трафіку.

При появі нових способів передачі сигналів (супутник, радіо) з'явилися великі проблеми в узгодженні нових та існуючих мереж, за допомогою існуючих протоколів. Можливість поєднувати різні мережі в єдиний інформаційний простір була проблемою с самого початку існування мереж. Архітектура, що використовувалась у ARPANET пізніше отримала назву TCP/IP відповідно до двох основних протоколів, що в ній використовуються. У книзі Cerf и Kahn (1974) з'явився перший опис даною мережевої архітектури, а пізніше TCP/IP становиться стандартом (Braden, 1989).

Міністерство оборони США турбувала можливість виходу з ладу окремих частин мережі (Кінцеве обладнання, маршрутизатори, міжмережеві шлюзи). Таким чином архітектура мережі отримала вимогу до того, щоб зберегти працездатність (можливість передачі трафіку від одного хоста до іншого), при виході з ладу проміжного обладнання. Іншими словами, необхідно обрати найбільш оптимальну архітектуру мережі при якій з'єднання буде існувати до тих пір, поки залишається робочими приймаюча та передаючі машини та деяка частина проміжного, комутуючого та маршрутизуючого обладнання. Крім того, архітектурі повинна бути притаманна гнучкість, адже передбачалось використання різного роду додатків зі специфічними вимогами (перенос файлів, передача мови в реальному часі тощо).

Таким чином протоколи TCP та IP в сукупності з іншими протоколами утворюють однойменну модель мережевого обміну даними TCP/IP.

Модель TCP/IP ієрархічна і на відміну від еталонної моделі OSI/ISO має лише чотири рівні (рис. 1.3) у порівнянні із сімома. Це обумовлено тим, що в даній мережевій моделі у порівнянні із OSI відсутні рівень представлення,

сеансовий рівень на фізичний рівень (фізичний и канальний рівень представлені одним єдиним рівнем). В свою чергу відсутність двох вищих рівнів аргументується тим, що прикладні додатки включають усі необхідні функції двох даних рівнів і таким чином в них немає необхідності.

4 Прикладний рівень
3 Транспортний рівень
2 Міжмережевий рівень
1 Канальний рівень

Рисунок 1.3 –Рівні мережевої моделі TCP/IP

Більш детально про кожний рівень та його функції:

Прикладний рівень. Даний рівень визначає спосіб у який здійснюється обмін даними між користувацькими прикладними додатками. Інакше, у системах «клієнт-сервер» додаток-клієнт повинен знати, як формувати запит на передачу, а в свою чергу додаток-сервер повинен знати як даний запит обробити. Дану функцію реалізують такі протоколи як HTTP, FTP , Telnet. Також сюди входять такі протоколи як DNS, RTP, SMTP.

Транспортний рівень. Даний рівень виконує ту ж саму функцію, що й транспортний рівень моделі OSI. Тобто він виконує задачу підтримки зв’язку між двома хостами одного рангу в режимі прийом-передача. Даний рівень реалізується протоколами, які вже вище згадувались у моделі OSI, а саме протоколи TCP та UTP.

Протокол управління передачею TCP, як це було зазначено раніше є надійним протоколом з встановленням з’єднання, що в свою чергу дозволяє без помилок розшифрувати повідомлення від одного хоста до іншого в межах однієї об’єднаної мережі. Даний протокол розбиває потік байт, що передаються на

окремі повідомлення, для передачі по міжмережевому рівню. На приймаючій стороні за допомогою TCP – процесу виконується зворотна операція по поєднанню окремих повідомлень у єдиний потік. Також даний протокол управляє вихідним потоком для уникнення перенавантаження вузьких місць мережі (якщо передача виконується швидше за прийом).

Інший протокол транспортного рівня – це протокол датаграм користувача. Даний протокол на відміну від TCP не встановлює з'єднання та не має послідовного управління потоком як у TCP, що робить даний протокол ненадійним. Іншими словами передача буде виконуватися «наосліп», тобто без підтвердження факту прийому повідомлення. Це може бути корисним коли швидкість потрібна більша за надійність. Наприклад для одноразових запитів по типу «клієнт-сервер», зокрема відео та звуки. Адже при втраті деякої частини повідомлення (частини слова, або кадру) людський мозок здатний доповнити відсутню інформацію.

Співвідношення протоколів IP ,TCP та UDP представлено у (табл. 1.1).

Таблиця 1.1 - Протоколи мережевої моделі TCP/IP

Рівень	Протоколи
Прикладний	HTTP, SMTP, RTP , DNS
Транспортний	TCP, UDP
Міжмережевий	IP, ICMP
Канальний	DLS, SONET, 802.11(WIFI),Ethernet

Міжмережевий рівень, або інакше інтернет рівень. По суті даний рівень є основою всієї архітектури. Основна задача міжмережевого рівня - це пошук оптимального маршруту для передачі пакету від одного хоста мережі до іншого по незалежному шляху. Тобто передача та прийом не обов'язково можуть здійснюватися в одному напрямку. Більш того частини одного повідомлення

відправлені одночасно можуть бути отримані на прийомній стороні в довільному порядку (тобто окремі пакети можуть рухатися різними шляхами). Якщо необхідно дотримуватися вихідного порядку передачі, то дана задача виконується протоколами вищих рівнів. Також міжмережевий рівень визначає формат пакету та протокол IP, а також службовий протокол ICMP.

Канальний рівень. Це найнижчий рівень даної архітектури. Від поєднує у собі апаратне, програмне забезпечення та параметри для передачі сигналу по визначеному середовищу. Тобто канальний рівень визначається стандартами технології канального рівня, що використовуються (Ethernet, 802.11 тощо). В загальному випадку, це скоріш не рівень, а інтерфейс між середовищем поширення сигналу та інтернет рівнем. Іншими словами, для рівнів вище не важливо, яким чином розповсюджується сигнал, адже його абстрактне представлення залишається однаковим [1, 4].

1.3. Технологія Ethernet

Сама розповсюджена на сьогоднішній день технологія Ethernet і перші її стандарти були розроблені в 1970 році компанією Xerox Corporation. Таким чином, з самого початку це був стандарт яким користується лише дана фірма, що займається виробництвом мережевого обладнання. Через деякий час (в 1980) схожий стандарт був прийнятий інститутом IEEE (комітет IEEE 802).

Даний комітет включає в собі декілька робочих груп. Для розробки стандартів та правил функціонування мереж безпосередньо для стандарту Ethernet була виділена група 802.3. Дана група стандартів визначає фізичне середовище розповсюдження сигналу та формат кадру [5].

Існує декілька загальних для даної групи стандартів форматов кадру Ethernet, але на практиці мережеве обладнання працює лише с одним форматом

кадру Ethernet DIX (табл. 1.2). Також зустрічається назва Ethernet II, за номером останнього стандарту DIX.

Таблиця 1.2 –Формат кадру Ethernet DIX(II)

6 байтів	6 байтів	2 байти	46-1500 байт	4 байти
MAC-адресата	MAC-відправника	Код протоколу інтернет рівня (0x0800 для IPv4)	Дані	FCS

На сьогоднішній день найбільш розповсюдженою технологією при побудові локальних обчислювальних мереж є технологія (набір стандартів) Fast Ethernet (зокрема 100Base-T, загальна назва для стандартів зі швидкістю передачі 100 Мбіт/с по витій парі), що є похідною від технології Ethernet [6].

1.4. Набір стандартів передачі Fast Ethernet

Специфікація Fast Ethernet була першою із швидкісних версій Ethernet, тому й отримала назву «Fast» (100 Мбіт/с проти 10 Мбіт/с).

Фізично Fast Ethernet використовує топологію зірка, але логічно працює як шинна мережа в силу методів доступу до мережі, які вона успадкувала від Ethernet. Формат кадрів технології Fast Ethernet не відрізняється формату кадрів Ethernet DIX(II).

Fast Ethernet підтримує три варіанті фізичного середовища поширення:

- Багатомодовий оптоволоконний кабель (два волокна);
- Вита пара категорії 5 (дві пари);
- Вита пара категорії 3 (чотири пари).

Коаксіальний кабель, навколо якого будувалась перша мережа Ethernet в даний стандарт не входить. Таким чином офіційний стандарт 802.3 включає у собі три різних специфікації для фізичного рівня Fast Ethernet:

- 100Base-TX – для двох пар кабелю неекранованої витої пари (UTP) категорії 5;
- 100Base-T4 – для двох пар по чотири кабелю неекранованої витої пари (UTP) категорії 3,4 або 5.
- 100Base-FX – для багатомодового оптоволоконного кабелю с двома волокнами

Наряду із технологією Ethernet, технологія Fast Ethernet використовує метод множинного доступу з контролем несучою та виявленням колізій. Кожен із типу кабелю технології Fast Ethernet має фізичні обмеження на довжину кабелю, які обумовлені затуханням сигналу та виникненням колізій (передача відбувається від двох хостів одночасно і кількість колізій, як не складно здогадатися залежить від кількості хостів та навантаження мережі, а при великій довжині кабелю зростають затримки), і для витої пари становить 90-100 м, а для оптичного кабелю 100 Base-FX приблизно 400 м.

На сьогоднішній день для з’єднання комп’ютерів локальної обчислювальної мережі із комутаційним обладнанням, зазвичай, використовують неекрановану виту пару категорії 5E. Це обумовлено відносно низькою вартістю та задовільною пропускною здатністю [6,7].

1.5. Протокол DHCP

Так як технологія Fast Ethernet тісно пов’язана із протоколами мережевої моделі TCP/IP, зокрема з двома однойменними даній архітектурі протоколами, то необхідно, щоб для кожного комп’ютера чи іншого пристрою, що підтримують дані протоколи (смартфони, ноутбуки, планшети, телевізори тощо) і підключені до локальної мережі виділялася унікальна IP адреса. Таким чином, зі збільшенням кількості пристроїв підключених одночасно до такої мережі ускладнюється задача видачі системним адміністратором кожному з них

унікальної IP адреси. Більш того, для тимчасових пристроїв це зробити неможливо.

З точки зору безпеки, кращим варіантом буде записати для кожного пристрою IP адресу вручну. Але мережа може налічувати десяток комутаторів до яких підключено сотні комп'ютерів та десяток принтерів. Це досить типова кількість обладнання для корпоративної локальної мережі представленою декількома поверхами. Тут на допомогу приходить протокол DHCP.

Протокол DHCP працює за принципом «клієнт-сервер». При старті ОС комп'ютер, який є DHCP - клієнтом (встановлений відповідний флаг у налаштуваннях адаптера) робить широкомовний запит на отримання IP адреси. DHCP сервер відповідає на запит и надсилає параметри необідні для роботи пристрою у мережі, зокрема його IP адресу. DHCP сервер може працювати у трьох режимах:

- ручне встановлення статичних адрес
- автоматичне встановлення статичних адрес
- автоматичний розподіл динамічних адрес

При будь-якому режимі роботи системний адміністратор при налаштуванні DHCP сервера на маршрутизаторі вводить деякий діапазон IP-адрес (або декілька), таким чином, що всі дані адреса відносяться до однієї мережі (усі хости мають однаковий адрес мережі, розмір якого визначає маска).

В ручному режимі необхідно окрім діапазону доступних логічних адрес (IP адрес) вказати у відповідність перелік фізичних адрес (MAC-адрес) хостів. В такому випадку DHCP сервер при кожному запуску буде видавати заздалегідь визначені IP адреси у відповідністю з фізичною адресою кожного хоста.

В напівавтоматичному режимі (автоматичне встановлення статичних адрес) DHCP сервер визначає фізичну адресу хостів та прив'язує до неї IP адресу на постійній основі, як і в випадку із ручним встановленням.

В автоматичному режиму DHCP сервер видає кожному хосту адресу в «оренду», на обмежений період часу, тобто до того часу як пристрій не видалиться із мережі. Це особливо корисно у випадку підключення мережі таких пристроїв як смартфон, планшет або ноутбук (За допомогою пачт-корду RJ-45, або безпровідне з'єднання 802.11(WIFI)).

Для динамічної видачі IP адресів зазвичай використовують маршрутизатор (роутер). Як приклад, домашній WIFI роутер, що поєднує у собі функціонал комутуючого обладнання, маршрутизатора та точки доступу. Також може бути використаний окремий DHCP сервер, або комутатор рівня L3 моделі OSI з підтримкою динамічної адресації.

При використанні технології віртуальних локальних мереж (VLAN) можливо зазначити окремі діапазони IP адрес для кожного VLAN. Наприклад в корпоративній мережі відокремити гостьовий WIFI у окрему віртуальну мережі та призначити для неї деякий діапазон IP адрес для видачі тимчасовим пристроям мережі (ноутбуки, смартфони, планшети и таке інше), що підключається за допомогою WIFI (стандарт 802.11) [5,6].

Таким чином у даному розділі були представлені основні технології, стандарти та протоколи, що використовується у сучасних локальних обчислювальних мережах. Представлена семирівнева еталона модель OSI використовується для аналізу роботи мережі та розподіл мережевої взаємодії на рівні абстракції (як правило останні три рівні поєднується в один). Стек протоколів TCP/IP та технологія Ethernet є основою сучасних комп'ютерних мереж. Протокол DHCP дозволяє спростити налаштування та адміністрування відносно великих за обсягом локальних мереж.

2. РОЗРАХУНОК ТА ВИБІР АРХІТЕКТУРИ МЕРЕЖІ

2.1. Вибір топології та оцінка масштабованості мережі

Необхідно виконати розрахунок локальної обчислювальної мережі для приміщень Національного Університету «Полтавської політехніки імені Юрія Кондратюка», зокрема перший, другий та третій поверхи «Ф» корпусу.

Станом на 2021 рік мережа вже налічує деяку кількість комп'ютерів та мережевого обладнання. Структурована кабельна система відсутня, в тому плані що немає документації або планів монтованої мережі. Більшість навчальних аудиторій не адаптовані під облаштування робочих місць.

Підключенню до глобальної мережі інтернет у «Ф» корпусі підведено до другого поверху.

В якості середовища поширення сигналу використовується вита пара, як правило неекранована, категорії 5е (для з'єднання інформаційних розеток с патч-панеллю та для патч-корду).

Поставлена задача включає розрахунок елементів локальної обчислювальної мережі (розрахункова кількість робочих місць, кількість та характеристики обладнання, що може використовуватися при побудові мережі тощо) для навчальних аудиторій та інших приміщень, де очікується розташування користувачів та створення проекту мережі з дотриманням вимог і претензією на масштабованість, що включає документацію та плани мережі.

Розробка проекту локальної обчислювальної мережі проводитися на першому, другому та третьому поверсі «Ф» корпусу. До складу приміщень, що припускають розміщення комп'ютерів входять приміщення кафедри, навчальні аудиторії, викладацькі і таке інше за виключенням великих лекційних аудиторій (215Ф, 217Ф та 219Ф), невеликих службових приміщень, малої актової зали, музикального класу і т.і.

Створювана локальна обчислювальна мережа в першу чергу передбачає забезпечення кожного комп’ютеру мережі, або тимчасового пристрою (ноутбуки, смартфони тощо) доступом до глобальної мережі інтернет та поєднання їх у єдиний інформаційний простір між собою у навчальних цілях та створення єдиного інформаційно-телекомунікаційного простору даної мережі та єдиної корпоративної мережі усього навчального закладу.

Висота міжповерхового перекриття різна для 2 та 3 поверхів, але приблизно рівна 3 м. Тобто довжина кабелю необхідна для прокладання вертикальною кабельної системи між двома поверхами з урахуванням міжповерхового перекриття (приблизно 50 см) становить 3.5м плюс запас на підключення між поверховими комутаторами.

Підвісні стелі та фальшполи відсутні, а значить прокладання кабельних ліній буде здійснюватися за допомогою звичайного пластикового короба у коридорах та в приміщеннях.

При прокладанні короба потрібно враховувати можливі джерела електромагнітних завад, зокрема лінії електроживлення, особливо при використанні у якості середовища поширення сигналу неекранованої витої пари (при цьому можливе прокладання кабелю передачі даних перпендикулярно лінії електроживлення).

Згідно з ДСанПІН 3.3.2.007-98 відстань між бічними поверхнями візуальними дисплейними терміналами (або інакше екран монітору комп’ютера) електронно-обчислювальних машин повинна бути 1,2 м (для рідкокристалічних матриць), а відстань від тильною поверхні одного екрану монітора до іншого повинна бути 2.5м.

Площа на одне робоче місце с використанням рідкокристалічних моніторів в свою чергу повинна складати не менше ніж 6 квадратних метри.

На кожне робоче місце повинна приходитися як мінімум одна інформаційна розетка.

Усе вище сказане задає вектор при побудові горизонтальної та вертикальної кабельних систем, але реалізація може відрізнятися, адже існують різні архітектурні моделі побудови фізичної топології мережі.

До таких моделей відносять централізовану архітектуру мережі та ієрархічну модель архітектури мережі, розроблену компанію Cisco.

Основним недоліком централізованої архітектури є відсутність ієрархічних рівнів і безпосереднє підключення всіх користувачів мережі до комутаційного активного обладнання в одному місці. Це не дуже зручно при проектування структурованої кабельною системи на декількох поверхах.

Ієрархічна модель Cisco позбавлена зазначених вище недоліків. Основними перевагами даної моделі є:

- Спрошує аналіз роботи мережі у цілому
- Спрощує пошук та усунення проблем у мережі
- За рахунок ієрархічної структури легше додавати нові елементи
- Спрошує монтаж та обслуговування

Ієрархічна модель включає три рівні:

- рівень ядра (Core layer), який має забезпечувати високу продуктивність, надійність і відмовостійкість;
- рівень дистрибуції (Distribution layer), який має забезпечувати взаємодію між ядром мережі та рівнем доступу, розподіл типів трафіку, обмеження доступу, маршрутизацію;
- рівень доступу (Access layer), на якому має забезпечуватись:

1) підключення користувачів до мережі;
2) висока щільність портів за невеликої ціни за порт;
3) наявність швидкісних каналів для підключення до комутаторів рівня дистрибуції;
4) контроль доступу на канальному рівні;
5) підтримка VLAN;

6) класифікація трафіку.

Ієрархічна модель архітектури компанії Cisco в першу чергу передбачає використання активного обладнання саме цієї компанії. Але з огляду на вищеперераховані вимоги до активного обладнання, можливе використання будь-якого обладнання, що відповідає даним вимогам.

На рівні доступу використовується такий пристрій, як комутатор (або switch). Це може буде керований комутатор, некерований або смарт комутатор (в даному випадку налаштування відбувається в більш прозорому з точки зору адміністратора мережі вигляді). У такій спосіб комп'ютери або інші пристрої (точки доступу, принтери, ноутбуки і т.і) під'єднані до одного комутуючого пристрою утворюють сегмент мережі.

На рівні дистрибуцію (рівень агрегації, поєднання сегментів) сегменти мережі поєднуються у єдину мережу. Для цього використовуються керовані комутатори L2 або L2/L3. Точка доступу, при необхідності підключається само на цьому рівні.

Прикладом рівня доступу при побудові мережі багатоповерхового будинку буде поєднання комутаторів окремих поверхів у один єдиний сегмент мережі.

Основна функція рівня ядра – це забезпечення маршрутизації усіх сегментів мережі. Дану функція може бути реалізована за допомогою маршрутизатора, або комутатор L3, що поєднує у собі функції комутатора та протоколи маршрутизації (але комутатор L3 не замінює повністю маршрутизатор, для виходу у глобальну мережу все одно потрібен шлюз).

На рівні ядра може бути реалізований файловий сервер, фаервол для шлюзу, DHCP сервер, DNS сервер и таке інше.

На (рис. 2.1) представлена загальна схема сегменту ієрархічної моделі побудови мережі за версію Cisco.

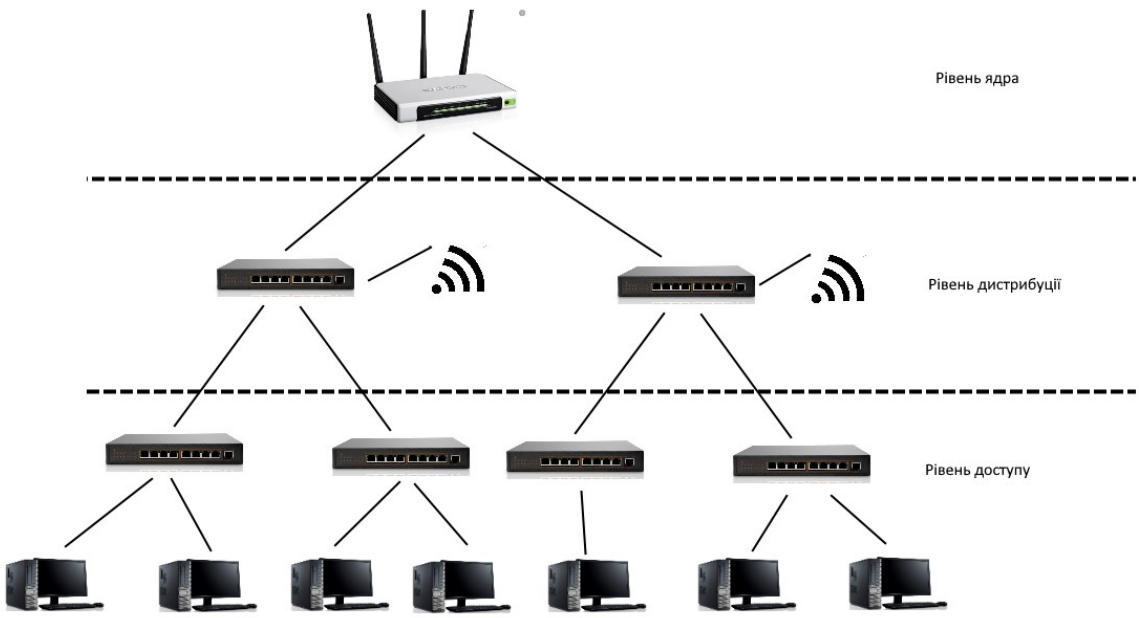


Рисунок 2.1 –Приклад сегменту мережі ієрархічної моделі

При дотриманні ієрархічної моделі при побудові мережі у будівлі необхідно для кожного поверху відокремити поверховий розподільчий комутатор типу L2, L2+ або L3 для поєднання горизонтальних сегментів мережі, тобто поєднання усіх комутаторів на одному поверсі в одному вузлі і в подальшому поєднання даних вузлів у центральному комутаторі будівлі. Дотримання даної моделі дозволяє побудувати максимально структуровану і продуктивну кабельну систему.

Як правило, на практиці класична ієрархічна модель розглядається лише при проектуванні великих корпоративних мереж із складною топологічною структурою (наявність серверів, телефонної лінії, декількох шлюзів для виходу у глобальні мережі і т.і.) , а для реалізації більше простої топології використовується сегмент даної моделі (рівень доступу та рівень агрегації сегментів мережі). Це особливо актуально при побудові невеликих локальних мереж з обмеженим бюджетом.

Таким чином, можливий варіант підключення сегментів одного поверху послідовно (послідовне включення комутаторів) в цілях заощадження. Тобто вертикальна кабельна система буде представлена звичайними L2 або L2+ комутаторами до яких у свою чергу послідовно підключається інші комутатори на поверху (або безпосередньо хости, якщо їх кількість невелика). При використанні такого способу має місце наявність вузьких ділянок мережі, але це не завжди є критичною проблемою (наприклад, навантаження на мережу рознесено у часі або в загальному не велике) і цілком та повністю залежить від призначення мережі.

Таким чином, з огляду на вище сказане доцільно, при побудові локальної обчислювальної мережі, що орієнтується на забезпечення доступу до інтернету та поєднанні користувачів у єдиний інформаційний простір зупинитися на варіанті побудови мережі з мінімальною кількістю активного обладнання, що дозволить забезпечити необхідну швидкодію та можливість масштабування мережі у подальшому [8,9,10].

На другому поверсі «Ф» корпусу знаходяться кафедральні приміщення, викладацькі, бухгалтерія, навчальні аудиторії.

Таким чином загальна кількість приміщень призначена для розміщення користувальницьких робочих місць, а саме інформаційних розеток для підключення персональних комп’ютерів, принтерів, WIFI роутерів і т.і становить 15 приміщень для другого поверху.

На першому та третьому поверсі кількість таких приміщень також становить 15.

Також на другому поверсі передбачається розташування точок доступу WIFI для підключення користувачів.

З урахуванням норми на 6 квадратних метри для одного робочого місця при використанні рідкокристалічного монітору та за умови, що на кожне робоче місце приходиться одна інформаційна розетка маємо, що кількість

інформаційних розеток повинна бути рівна кількості робочих місць, тобто відношенню площі приміщення до 6 м^2.

Остаточне значення кількості робочих місць береться із відношення площі приміщення до норми площі на одне робоче місце з округленням до меншого (відкиданням дробової частини), а також із особливостей конкретного приміщення.

У таблиці 2.1 наведені результати розрахунку кількості робочих місць для другого поверху «Ф» корпусу, тобто мінімально необхідну кількість портів на комутаторі (або, відповідно кількості інформаційних розеток для робочих місць, де розташовується персональний комп’ютер) для підключення кінцевого обладнання та точок доступу з урахуванням норм на площу для одного робочого місця, особливостей розташування робочих місць у приміщенні та відстані між робочими місцями.

Розташування активного обладнання, інформаційних розеток, місць підключення точок доступу та маршруту прокладання кабелю витої пари зазначено на загальній структурній схемі мережі у Додатку Б.1-3 відповідно для кожного поверху.

Розташування комутаторів на структурній схемі кожного поверху обумовлено забезпеченням можливості поєднання їх у вертикальну кабельну систему та забезпеченням мінімально необхідної довжини маршруту прокладання кабелю до розеток.

Розташування розеток на схемі в першу чергу відображає їх кількість на одне приміщення згідно вище зазначених ДСТУ. Тобто, їх розташування може бути змінено виходячі із особливостей приміщення.

Таблиця 2.1 – «Площа приміщень другого поверху «Ф» корпусу та розрахункова кількість робочих місць»

№	Аудиторія	Площа за планом будівлі, $м^2$	Розрахункова кількість робочих місць
1	214-Ф	31.2	4
2	207-Ф	48.2	8
3	206-Ф	20	3
4	212-Ф	51.6	8
5	211-Ф	28.32	4
6	210-Ф	18.9	3
7	209-Ф	48.1	6
8	208-Ф	16.4	2
9	205-Ф.1	16.1	2
10	205-Ф.2	17.7	2
11	205-Ф.3	15.8	2
12	205-Ф.4	16.5	2
13	205-Ф.5	14.8	2
14	204-Ф	45.5	7
15	208-А	55.6	9

Аналогічним чином розраховуємо кількість робочих місць для приміщень першого та третього поверхів. Дані представлені у (табл. 2.2.) для першого поверху та у (табл. 2.3) для третього поверху відповідно.

Порядок слідування аудиторій у таблицях 2.1..2.3 відповідає їх розміщенню на плані зліва-направо, зверху-вниз. Для комутатора кожного поверху інформаційні розетки нумеруються починаючи з 1.

Нумерація розеток на плані мережі проводиться згідно з планом пікдлючення останніх до комутаційного обладання на кожному з поверхів.

Кожен с поверхів налічує багато закритих аудиторій, що перешкоджатиме проходженю WIFI сигналу між користувачем та точкою доступа. Таким чином на кожному поверсі передбачається розміщення як мінімум чотирьох точок доступу.

Таблиця 2.2 – Площа приміщень першого поверху «Ф» корпусу та розрахункова кількість робочих місць

№	Аудиторія	Площа за планом будівлі, $м^2$	Розрахункова кількість робочих місць
1	102-Ф	47.9	7
2	126-Ф	32.2	5
3	113-Ф	67.9	11
4	114-Ф	51.3	8
5	115-Ф	34.6	5
6	116-Ф	19.1	3
7	100-Ф	15.3	2
8	118-Ф	50.5	8
9	125-Ф	31.3	5
10	124-Ф	17.7	2
11	123-Ф	18	3
12	119-Ф	16.3	2
13	122-Ф	16.5	2
14	120-Ф	45.2	7
15	121-Ф	31.1/14.1	7

Кількість інформаційних розеток вираховується з претензією на максимальну можливу кількість робочих місць (можливість масштабувати мережу), за умови, що на кожне робоче місце приходиться хоча б одна інформаційна розетка.

Максимальна довжина кабелю від робочого місця до комутаційного обладнання (або до патч-панелі) повинна бути не більше ніж 90 м. В свою чергу, максимальна загальна довжина з'єднуючого кабелю на обох кінцях кабелю має бути не більше 10 м. Кабелі і розетки мають бути узгоджені за категорією.

Більшість сучасних пристроїв, що реалізують інтерфейс 8P8C (RJ-45) мають функції автоматичного розпізнавання прямого та перехресний типу кабелю MDI/MDIX. В такому випадку схеми обтиску витої пари T568A та T568B, як правило, будуть взаємно узгодженими.

Таблиця 2.3 – Площа приміщень третього поверху «Ф» корпусу та розрахункова кількість робочих місць

№	Аудиторія	Площа за планом будівлі, $м^2$	Розрахункова кількість робочих місць
1	302-Ф	31.4	5
2	301-Ф	49	8
3	312-Ф	28.9	4
4	313-Ф	17.1	2
5	314-Ф	52	8
6	315-Ф	33.2	5
7	316-Ф	18.2	3
8	317-Ф	66.8	11
10	319-Ф	16.9/18.7	4
11	320-Ф	30.8	4
12	324-Ф	49.7	8
13	325-Ф	14.6	2
14	323-Ф.1	10.3	1

Таким чином для 44 - рьох приміщень, що припускають розміщення користувачів, маємо максимально можливу розрахункову загальну кількість робочих місць, рівну 77-ти для першого поверху, 64 для другого поверху (та 6 точок доступу WIFI) і 65 робочих місця для третього поверху «Ф» корпусу. Загальна кількість інформаційних розеток відповідає кількості робочих місць та точок доступу (по 1 розетці на кожне робоче місце без урахування принтерів і т.п.).

Реалізації рівня доступу на кожному поверсі, тобто поєднання комп’ютерів у сегменти мережі, доцільно виконувати за допомогою двох керованих (смарт) 48-ми портових комутаторів (тобто мінімальна кількість активного обладнання), а поєднання сегментів за допомогою 24-портового керованого комутатора

Використання смарт комутатора дає можливість налаштування VLAN для сегментації мережі.

Згідно цього у (табл. 2.4) зведені дані про необхідну кількість комутуючого активного обладнання для кожного поверху будівлі, а також інформацію про використання портів [8].

Таблиця 2.4 – Необхідна кількість комутуючого обладнання

Поверх	Робочі місця	Точки доступу	Розрахункова кількість портів	Обладнання
1	77	4	81	Switch 48 ports L2 x2, Acces Point x4
2	64	4	68	Switch 48 ports L2 x2, Switch 24 ports L2, Acces Point x4
3	65	4	69	Switch 48 ports L2 x2, Acces Point x4

2.2. Специфікація обладнання

Для поєднання комп'ютерів мережі у сегменти на рівні доступу та агрегації доцільно використовувати керовані комутатори компанії D-Link (одні з кращих по відношенню ціна/якість) . У випадку із точками доступу по даному критерію зарекомендували себе безпровідні пристрої компанії MikroTik.

Обладнання даних виробника зарекомендував себе як непогане рішення за свою ціну (Комутатори та точки компанії Cisco з схожими характеристиками коштує на порядок дорожче).

Таким чином, необхідно обрати керований L2 комутатор з 48 портами та підтримкою усіх основних протоколів канального рівня, що відповідає основним вимогам технічного завдання. Досить популярним рішенням довго залишався комутатор DES 3200-52 та його модифікації, але він був знятий з виробництва. Більш сучасною заміною є комутатори серії WebSmart DGS-1210.

Комутатор WebSmart DGS-1210-52. Необхідна його модифікація WebSmart DGS-1210-52/F1 на 48 основних портів та 4 комбо порти зображена на Рисунку 2.2 [11].

Рисунок 2.2 – Комутатор WebSmart DGS-1210 – 52/F

Даний керований комутатор має 48 портів 10/100/1000 Base – T та 4 комбінованих порти 100/1000Base-T/SFP. Наявна підтримка технології D-Link Green та розширені функції управління та безпеки. Забезпечує високу продуктивність и можливість масштабування мережі. Функції управління включають SNMP, можливість налаштування за допомогою Web-інтерфейсу, утиліту D-Link Network Assistant і спрощений інтерфейс командного рядка (CLI) через Telnet.

Модель DGS-1210-52 / F оснащена пасивною системою охолодження, яка забезпечує безшумну роботу і дозволяє продовжити термін експлуатації пристрою.

Технологія D-Link Green. Дана технологія дозволяє заощадити за рахунок зниження споживаної електроенергії без втрат продуктивності або функціональних можливостей. Комутатор визначає статус з’єднання для кожного порту та здійснює перехід у режим сну, якщо порт виявляється неактивним.

Даний пристрій реалізує функції L2 рівня еталонної моделі OSI, зокрема IGMP Snooping, Port Mirroring, Spanning Tree Protocol (STP) та Link Aggregation

Control Protocol (LACP). Оптимізація навантаження на комутатор та підвищення надійності передачі даних реалізується за рахунок управління потоком IEEE 802.3x. Наявна підтримка повного дуплексу на швидкості 2000 Мбіт/с на кожному з портів, що забезпечує необхідну продуктивність на кожному з робочих місць.

Комутатор має функцію діагностики кабелю, що дозволяє визначити стан витої пари на будь якому з портів комутатора та дозволяє діагностувати несправність та її тип.

Функції Loop Back Detection виконує перевірку портів на наявність замкнутої петлі. Якщо на якомусь з портів комутатора буде виявлена петля, даний порт буде вимкнутий в автоматичному режимі.

Комутатори даної серії підтримують Auto Surveillance VLAN (ASV) та Auto Voice VLAN. Таким чином дані пристрої можуть бути використані для побудови систем відеоспостереження та IP – телефонії. Дві дані технології дозволяють автоматично виділяти системи відеоспостереження та пристрої VoIP для подальшого групування їх у окрему віртуальну мережу. Для відео та аудіо трафіку в рамках даного VLAN задається найвищий пріоритет. Таким чином, за рахунок даних технологій забезпечується стабільна робота систем відеоспостереження та IP – телефонії. Також Web – інтерфейс комутатора включає режим для роботи із системами відеоспостереження.

Функція D-Link Safeguard Engine забезпечує ефективний механізм захисту комутатора від вірусів та шкідливого трафіку. Наявна можливість використання зовнішнього сервера RADIUS для авторизації користувачів за рахунок автентифікації на основі порту 802.1X. Також, функції списку управління доступом (ACL) дозволяє збільшити захищеність мережі за рахунок фільтрації трафіку, що надходить від несанкціонованих MAC/IP – адрес. Наявна функції, що дозволяє попередити ARP Spoofing, за рахунок відстеження хибних ARP запитів, які в свою чергу можуть викликати затримку або змінити трафік. Даний

захист також реалізується за рахунок списку управління доступом, блокуючи пакети, що включають хибні ARP – запити. DHCP Server Screening дозволяє збільшити рівень безпеки за рахунок обмеження доступу неавторизованим DHCP – серверам.

Налаштування комутаторів даної серії можливе за допомогою Web – інтерфейсу та утиліти D-Link Network Assistant. Дане програмне забезпечення дозволяє автоматично виявляти та відображати на моніторі усі комутатори серії D-Link Smart, що відносяться до одного L2 сегменту мережі. За рахунок цього системний адміністратор має змогу не змінювати IP адресу свого комп'ютера для налаштування комутатору. Також, адміністратору доступні налаштування в розширеному режимі та основні налаштування виявлених пристроїв, наприклад, зміна паролю та оновлення програмного забезпечення. Комутатор DGS-1210-52 / F також підтримує програму D-View 7, та спрощений інтерфейс командного рядку CLI через протокол Telnet. Програма D-View 7 - це система мережевого управління, що дозволяє здійснювати контроль над важливими параметрами, зокрема працездатність, надійність, гнучкість та захищеність.

До апаратного забезпечення комутатора DGS-1210-52 / F відноситься процесор, що працює на частоті 700 МГц, 128 МБ оперативної пам'яті та 32 МБ Flash пам'яті.

Підтримка стандартів витої пари IEEE 802.3 10Base-T, IEEE 802.3u 100Base-Tx (Fast Ethernet), IEEE 802.3ab 1000 Base-T. Підтримка технології IEEE 802.3az Energy Efficient Ethernet. Автоматичне узгодження швидкості та режиму дуплекса. Управління потоком IEEE 802.3x. Підтримка стандарту передачі по оптичному кабелю IEEE 802.3z 1000Base-X. Наявна функція автоматичного визначення MDI/MDIX (типу кабелю витої пари , прямого або кросового) на усіх портах комутатора. Підтримка повного дуплекса для швидкостей 10/100/1000 Мбіт/с та напівдуплексного режиму роботи для швидкостей 10 та

100 Мбіт/с. Наявні кнопки Power та Reset. На кожному з портів наявні три індикатори: з’єднання (Link), статусу активності (Activity) та швидкості (Speed).

Швидкість комутаційної матриці становить 104 Гбіт/с. Метод комутації Store-and-Forward (зі збереженням кадрів). Буфер пакетів при цьому 1.5 МБ Розмір таблиці комутації 16000 записів. Максимальна швидкість перенаправлення 64-байтних пакетів становить 77.4 Mpps (Millions of packets per second). Підтримує Jumbo – фрейми розміром до 10000 байт.

VLAN. Стандарт 802.1q (тегування трафіку), максимальна кількість статичних VLAN-груп становить 256. Діапазон VID (1-4094). Підтримка Asymmetric VLAN та Auto Voice VLAN, Auto Surveillance VLAN.

Реалізує деякі функції рівня L3. Наявність 4-рьох IP інтерфейсів, IPv6 Neighbor Discovery (ND), статична маршрутизація, підтримка статичних маршрутів (124 для IPv4 та 50 для IPv6).

Максимальна споживана потужність 34.85 Вт. Споживана потужність в режимі очікування складає 13.9 Вт. Тепловиділення 118.92 BTU/год. MTBF 400667 год. Рівень шуму 0 дБ (пасивна система охолодження). Робоча температура від -5 до 50 градусів Цельсія, збереження від -20 до 70 градусів Цельсія. Вологість повинна бути в межах від 0 до 95 відсотків без конденсату.

Комутатор DGS-1210 – 24/F1. Комутатор серії WebSmart DGS-1210-28 (рис 2.3 [11]).

Рисунок 2.3 – Комутатор WebSmart DGS-1210-28

Підтримка технологій та протоколів аналогічна з попередньо розглянутим комутатором WebSmart DGS-1210-52/F. Відрізняється лише кількістю портів та відповідно технічними характеристиками, які представлені нижче.

Оснащений 24 портами 10/100/1000 Base – T та 4 комбо-портами 100/1000 Base – T/SPF.

Має процесор з тактовою частотою 500 МГц, 128 МБ оперативної пам’яті та 32 МБ Flash – пам’яті.

Швидкість комутаційної матриці 56 ГБіт/с. Метод комутації Store-and-forward. Розмір таблиці комутації становить 8000 записів. Максимальна швидкість перенаправлення 64-байтних пакетів 41,7 Mpps. Розмір буферу пакетів складає 512 кБ. Розмір Jumbo – фрейму 10000 байт[11].

Точка доступу MicroTik cAp (RBcAP2nD). Безпровідна точка доступа з можливістю встановлення на стіну або стелю у приміщенні. Зовнішній вигляд пристрою представлений на рисунку 2.4 [12].

Рисунок 2.4 – Точка доступу MicroTik cAp (RBcAP2nD)

Діаметр пристрою складає 185 мм, висота 31 мм.

Має вбудований одноядерний процесор з тактовою частотою 650 МГц, об’єм оперативної пам’яті складає 64 МБ, об’єм постійної флеш пам’яті 16 МБ.

MTBF 100000 годин при експлуатації за температури 25 градусів Цельсія. При цьому допустима температура експлуатації пристрою лежить в межах від -40 до 70 градусів Цельсія. Система охолодження пасивна.

Налічує один порт Ethernet 10/100 Base – T з підтримкою технології PoE (стандарти 802.3af/at). Максимальна споживана потужність 4 Вт. Вхідна напруга 11-57 В.

Швидкість передачі даних на частоту 2.4 ГГц становить 300 Мбіт/с. Максимальна вихідна потужність 22 dBm (158 мВт)[12].

2.3. Схема підключення та документація мережі

При побудові відносно великих локальних мереж (більше 100 робочих місць) встає проблема широкомовного трафіку у мережі (ARP, DHCP запити тощо). Рішенням є сегментація мережі на канальному рівні, тобто для груп користувачів необхідно визначити свої віртуальні сегменти (VLAN-ни).

В рамках проекту для кожної групи користувачів обмежених одним комутатором, а також для точок доступу доцільно відокремити свій VLAN. Згідно цього перелік усіх VLAN наведений у (табл 2.5).

Таблиця 2.5. – Перелік та призначення VLAN проекту

VID	Name	Призначення
11	vlan11_asw11	Сегмент asw1.1
12	vlan12_asw12	Сегмент asw1.2
21	vlan21_asw21	Сегмент asw2.1
22	vlan22_asw22	Сегмент asw2.2
31	vlan31_asw31	Сегмент asw3.1
32	vlan32_asw32	Сегмент asw3.2
100	vlan100_APs	Точки доступу

При цьому native VLAN не використовується, так як для кожного сегменту визначено більше одного VLAN.

Схему підключення активного обладнання доцільно здійснювати за топологією зірка. Таким чином, уся пропускна здатність окремих комутаторів доступу буде залежати лише від швидкості uplink з'єднання. У випадку із послідовним включенням комутаторів, пропускна здатність усієї конструкції буде обмежуватись швидкістю лише одного, крайового uplink з'єднання.

Схема підключення активного обладання (роутеру, комутаторів та точок доступу) представлена у (табл 2.6).

Оцінка навантаження на мережу. Для оцінки навантаження на комутатор доступу (при умові, що задіяні усі порти комутатора) необхідно визначити сумарну пропускну здатність його портів у режими повного дуплексу та порівняти із швидкістю комутуючої матриці та швидкістю uplink з'єднання.

Комутатори доступу у проекту представлені обладннаням DGS 1210-52/F. Максимальна швидкість кожного порта складає 1000 МБіт/с за умови використання на кінцевому обладнанні мережевого адаптера, що підтримує дану швидкість. Таким чином маємо 48 ГБіт/с для полу дуплексного режиму роботи та 96 ГБіт/с для повно дуплексного режиму. Швидкість комутаційної матриці згідно специфікації складає 104 ГБіт/с. Таким чином, в рамках одного сегменту мережі забезпечується максимальна швидкість передачі даних.

Сумарна швидкість усіх uplink портів даного комутатора складає 4 ГБіт/с. Реальний трафік між маршрутизатором та будь-яким із сегментів мережі значно менше, через те, що на момент написання роботи у мережі присутній лише один маршрутизатор на усю мережу (тобто лише одна зовнішня адреса для виході у глобальну мережу). З оглядом на поставлену задачу, оціночне навантаження на одного користувача складає 20 МБіт/с (в середньому 5 Мбіт/с). В свою чергу, пропускної 4 Гбіт/с достатньо для забезпечення кожного користувача каналом 4Гбіт/с : 48 = 83 Мбіт/с.

Навантаження на uplink порт агрегуючого комутатора dsw1 складається із суми навантажень його портів, тобто 24Гбіт/с. В режимі повного дуплексі 48

Гбіт/с. Швидкість комутаційної матриці даного комутатора становить 56 Гбіт/с. Тобто даний комутатор є неблокуємим. Однак, вузьким місцем даної мережі є один маршрутизатор та лише одне з'єднання (router-dsw1) швидкістю 1 Гбіт/с.

Таким чином логічним удосконаленням буде встановлення додаткового маршрутизатора та двох додаткових з'єднань з сумарною пропускною здатністю 4 Гбіт/с.

Таблиця 2.6. – Схема підключення активного обладнання

Uplink	Порт	Downlink	Порт	Trunk/A
Router	Gigabit 0/0/0	dsw1	Gigabit 0/0/1	11-12,21-22,31-32,100
dsw1	Gigabit 0/1-Gigabit 0/4	asw1.1	Gigabit 0/0/1-Gigabit 0/0/4	11,100
	Gigabit 0/5-Gigabit 0/8	asw1.2	Gigabit 0/0/1-Gigabit 0/0/4	12,100
	Gigabit 0/9-Gigabit 0/12	asw2.1	Gigabit 0/0/1-Gigabit 0/0/4	21,100
	Gigabit 0/13-Gigabit 0/16	asw2.2	Gigabit 0/0/1-Gigabit 0/0/4	22,100
	Gigabit 0/17-Gigabit 0/20	asw3.1	Gigabit 0/0/1-Gigabit 0/0/4	31,100
	Gigabit 0/21-Gigabit 0/24	asw3.2	Gigabit 0/0/1-Gigabit 0/0/4	32,100
asw1.1	Gigabit 0/1	AP1.1	FastEthernet0	100
	Gigabit 0/2	AP1.2	FastEthernet0	100
asw1.2	Gigabit 0/1	AP1.3	FastEthernet0	100
	Gigabit 0/2	AP1.4	FastEthernet0	100

Таблиця 2.6. – Схема підключення активного обладнання(продовження)

asw2.1	Gigabit 0/1	AP2.1	FastEthernet0	100
	Gigabit 0/2	AP2.2	FastEthernet0	100
asw2.2	Gigabit 0/1	AP2.3	FastEthernet0	100
	Gigabit 0/2	AP2.4	FastEthernet0	100
asw3.1	Gigabit 0/1	AP3.1	FastEthernet0	100
	Gigabit 0/2	AP3.2	FastEthernet0	100
asw3.2	Gigabit 0/1	AP3.3	FastEthernet0	100
	Gigabit 0/2	AP3.4	FastEthernet0	100

Схема IP-адресації. Отримання IP адрес у мережі передбачає використання протоколу DHCP. Відповідно, для кожного сегменту (VLAN) мережі свій діапазон. При адресації доцільно використовувати 24-бітну маску (для спрощення адміністрування мережі). На один такий діапазон приходиться 256 адрес (адреса шлюзу та широкомовна зарезервовані). Точки доступу винесені в окремий діапазон и використовують маску 21 біт (254 адрес може бути не достатньо для 12 точок доступу на трьох поверхах). Згідно цього схема IP-адресації представлена у (табл 2.7).

Таблиця 2.7. – Схема розподілу IP адрес

IP адреса/маска	Діапазон	VLAN
192.168.11.1/24	192.168.11.2-192.168.11.254	11
192.168.11.1/24	192.168.11.2-192.168.11.254	12
192.168.11.1/24	192.168.11.2-192.168.11.254	21
192.168.11.1/24	192.168.11.2-192.168.11.254	22
192.168.11.1/24	192.168.11.2-192.168.11.254	31
192.168.11.1/24	192.168.11.2-192.168.11.254	32
192.168.100/21	192.168.96.2-192.168.103.254	100

Таким чином проект мережі включає шість комутаторів рівня доступу (D-Link DGS 1210-52/F1). Один комутатор рівня розподілення (D-Link DGS 1210-28/F1. Дванадцять точок доступу (MicroTik cAP, по чотири на кожен поверх).

Обрана топологія реалізує сегмент ієрархічної моделі. Даний підхід дозволяє заощадити за рахунок зменшення кількості активного обладнання та спрощує адміністрування мережі, хоча класична ієрархічна модель дозволяє отримати максимально продуктивну мережу за рахунок надлишковості.

Розрахункові значення навантаження для комутаторів доступу та розподільчого комутатора показує, що технічних параметрів комутаторів, зокрема швидкості комутуючої матриці (104 Гбіт/с та 56 Гбіт/с для комутаторів доступу та агрегуючого відповідно) та сумарної пропускної здатності uplink портів (4Гбіт для обох моделей) достатньо для забезпечення передачі трафіку в мережі.

Вузьким місцем мережі є наявність лише одного маршрутизатора. Для реалізації пропускної здатності мережі у повній мірі, необхідно встановити додатковий маршрутизатор та додаткові з’єднання з розподільчим комутатором (максимум 4 з’єднання).

Сегментація мережі дозволяє знизити кількість широкомовного трафіку. Представлена схема поділу на віртуальні підмережі і схема IP-адресації також дозволяють спросити адміністрування мережі [10, 11].

3. МОДЕЛЮВАННЯ РОБОТИ МЕРЕЖІ

У якості програмного забезпечення для моделювання роботи локальної розрахованої обчислювальної мережі будемо використовувати Cisco Packet Tracer.

Даний програмний комплекс дозволяє моделювати мережі будь якої складності та розміру, в тому числі у локальні. Є можливість організації та налаштування логічної та фізичної топології мережі. Для організації фізичної топології в редакторі передбачені контейнери, для розмежування сегментів мережі, та шаблони. Також є можливість завантажити план будівлі у якості фону для шаблону поверху будівлі або контейнеру. На ряду із є можна розмістити комутаційну стійку де буде наочно видно задіяні порти активного обладнання та їх статус у реальному часі.

До складу апаратного забезпечення, що моделюється, входять маршрутизатори, комутатори, персональні комп'ютери, смартфони, ноутбуки, принтери, IP телефони і т.і., а також різні побудові Bluetooth,WIFI та USB пристрої.

Мережеве обладнання представлено продуктами компанії Cisco (у разі використання реального обладнання даної компанії, є можливість синхронізації налаштувань мережі у програмі та реального обладнання). Вибір апаратного забезпечення досить великий, що дозволяє проводити моделювання мережі для довільного обладнання (налаштування VLAN, DHCP пулів на роутері та інші загальні параметри).

У програмі присутні два режими роботи мережі: у реальному часі та режим симуляції. Дана функція дозволяє відстежити трафіку у мережі, окремі байти, кадри та пакети. Симуляція приближена до поведінки реального апаратного та програмного забезпечення, що дозволяє приблизно оцінити поведінку мережі при заданих параметрах.

3.1. Підготовка проекту

Проект мережі складається із трьох поверхів. На кожному поверсі п’ятнадцять приміщень, що передбачають розміщення користувачів, два комутатори (48 портів + 4 комбо порти) та чотири точки доступу.

Для більшою наочності доцільно кожен поверх представити у вигляді окремого сегменту мережі (контейнеру) та завантажити плани поверху для розміщення обладнання, як представлено на (рис. 3.1 [13]).

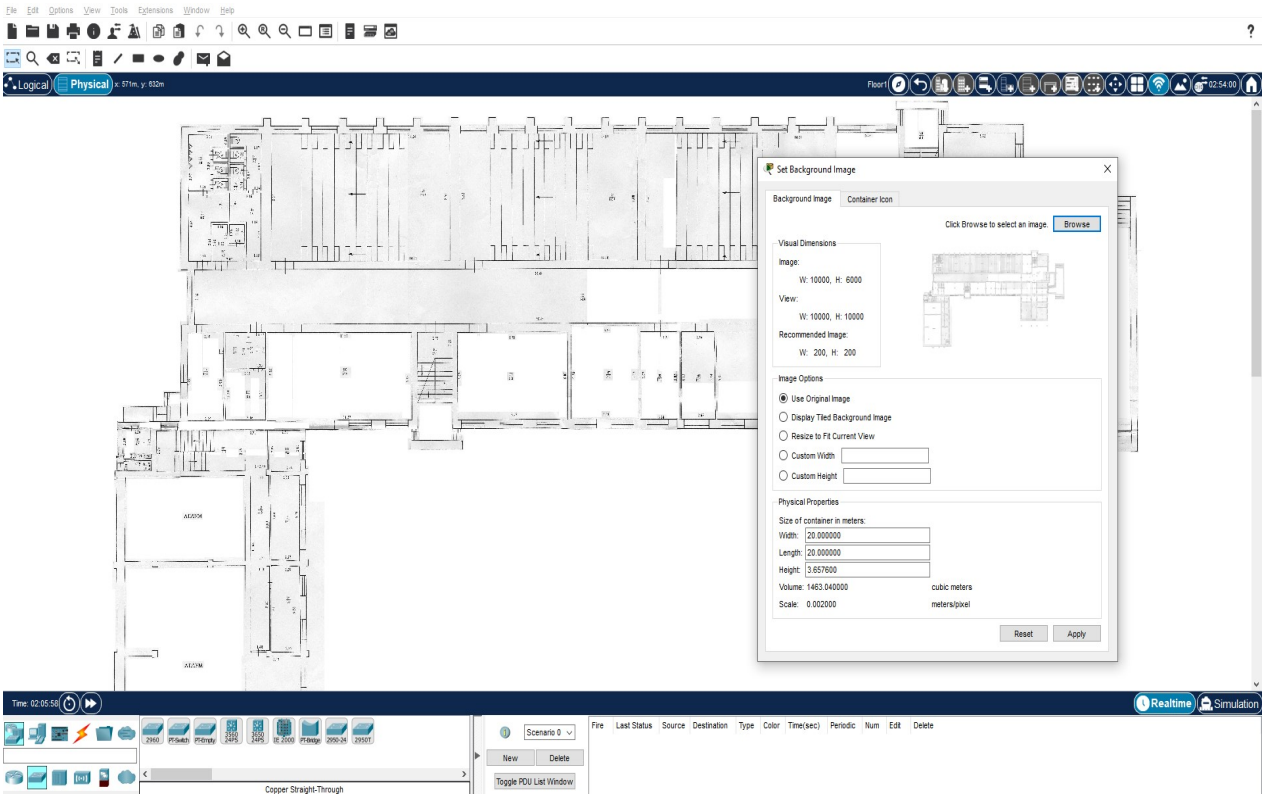


Рисунок 3.1. – Налаштування плану будівлі у редакторі на прикладі 1-го поверху

Аналогічним чином завантажуємо у редактор плани приміщень вдох інших поверхів.

Можливе налаштування розміру контейнеру у метрах. Це може знадобитися для відстеження зони покриття без врахування перешкод для точки доступу або WIFI роутеру.

Розміщення обладнання в редакторі фізичної топології автоматично дублює його у вікно логічної топології.

При поєднанні декількох поверхів у один сегмент , за допомогою агрегуючого комутатора, у вікні фізичної топології можна спостерігати статус з'єднання(рис. 3.2 [13]).

Рисунок 3.2. – Поєднання декількох поверхів у один сегмент мережі

Таким чином можливо створити повноцінний план/проект мережі з можливістю редагування та налаштування активного обладнання, що до нього входить.

В програмі присутні лише 24-портові керовані комутатори. Так як в проекті мережі використовується 48-портовий комутатор D-Link, у якості активного обладнання будемо використовувати комутатор Cisco 2960 (Кількість комп'ютерів підключених до одного комутатора на рівні доступу відрізняється від плану проекту, але для оцінки роботи мережі та налаштувань достатньо і декількох комп'ютерів).

Таким чином логічна топологія проектованої мережі у Packet Tracer з урахуванням вищесказаного представлена на (Рисунку 3.3 [13]).

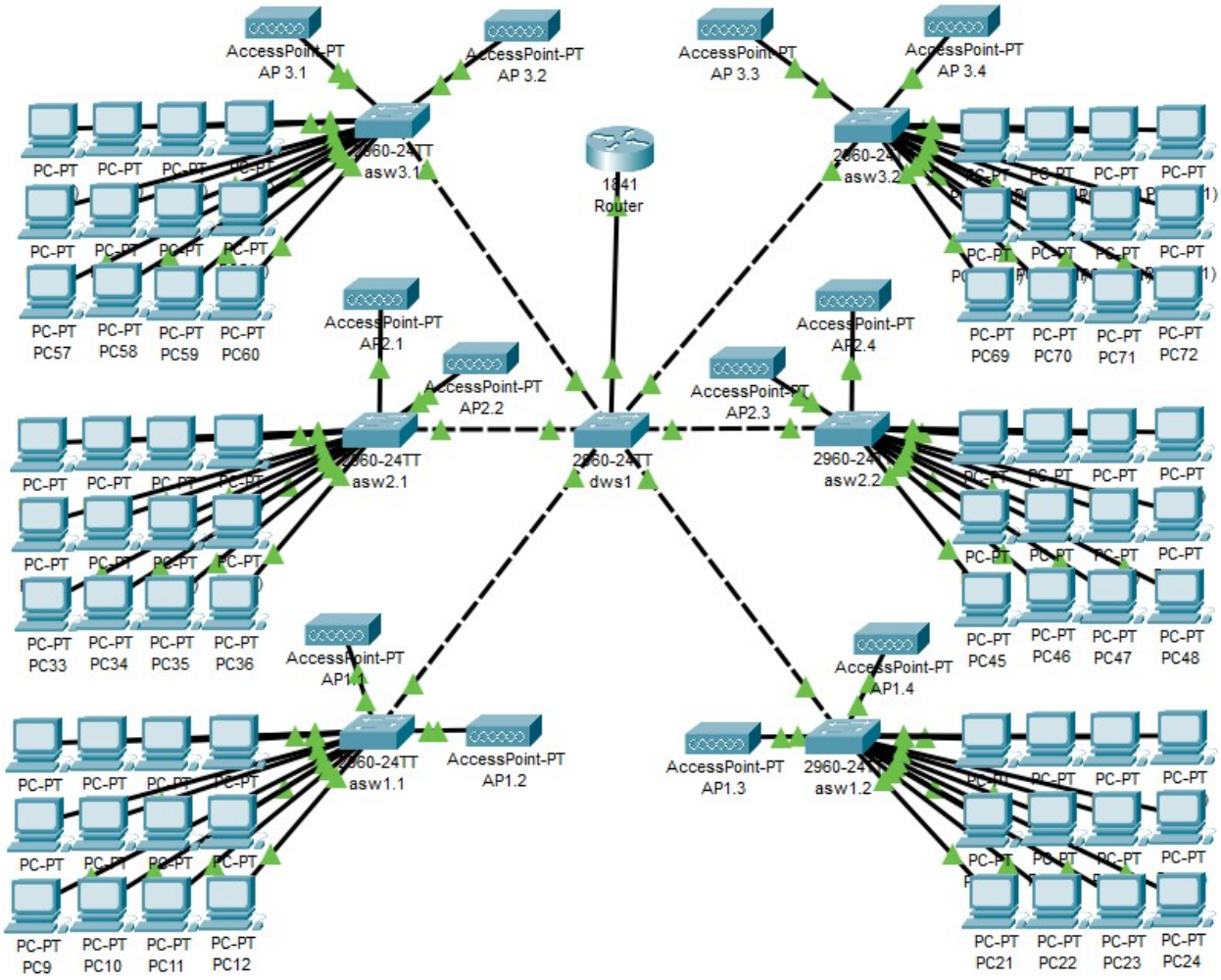


Рисунок 3.3. – Загальна логічна топологія мережі

3.2. Налаштування VLAN та Trunk на комутаторах

Налаштування агрегуючого комутатора dsw1. Згідно проекту мережа поділяється на 7 сегментів (або інакше доменів або VLAN) з метою зменшення широкомовного трафіку та збільшення стабільності роботи мережі. Тобто необхідно визначити 7 VLAN-ів, назначити транк порти (згідно схеми підключення активного обладання) та визначити допустимі VLAN-ни для кожного порту.

Лістинг команд для виконання представлений на (Рисунку 3.4 [13]).

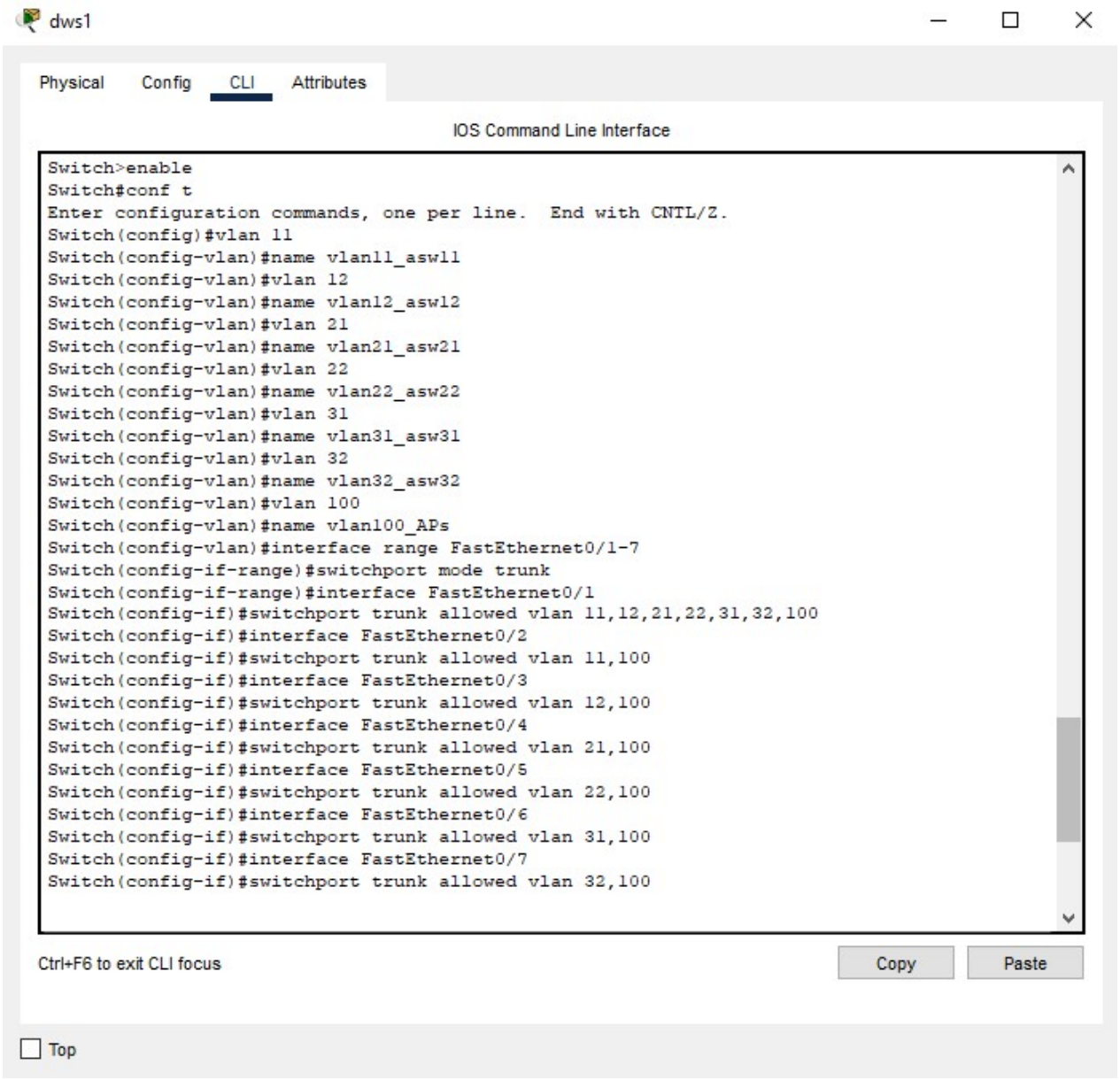


Рисунок 3.4. – Налаштування комутатора dw1

Налаштування комутаторів рівня доступу. Для налаштування комутаторів рівня доступу (asw1.1,asw1.2..asw.3.2) необхідно таким же чином визначити VLAN-ни і призначити транкові та порти доступу (access ports), а також налаштувати VLAN-ни для кожного з них.

Налаштування та лістинг команд представлений на (Рисунку 3.5 [13]) на прикладі комутатора asw2.2.

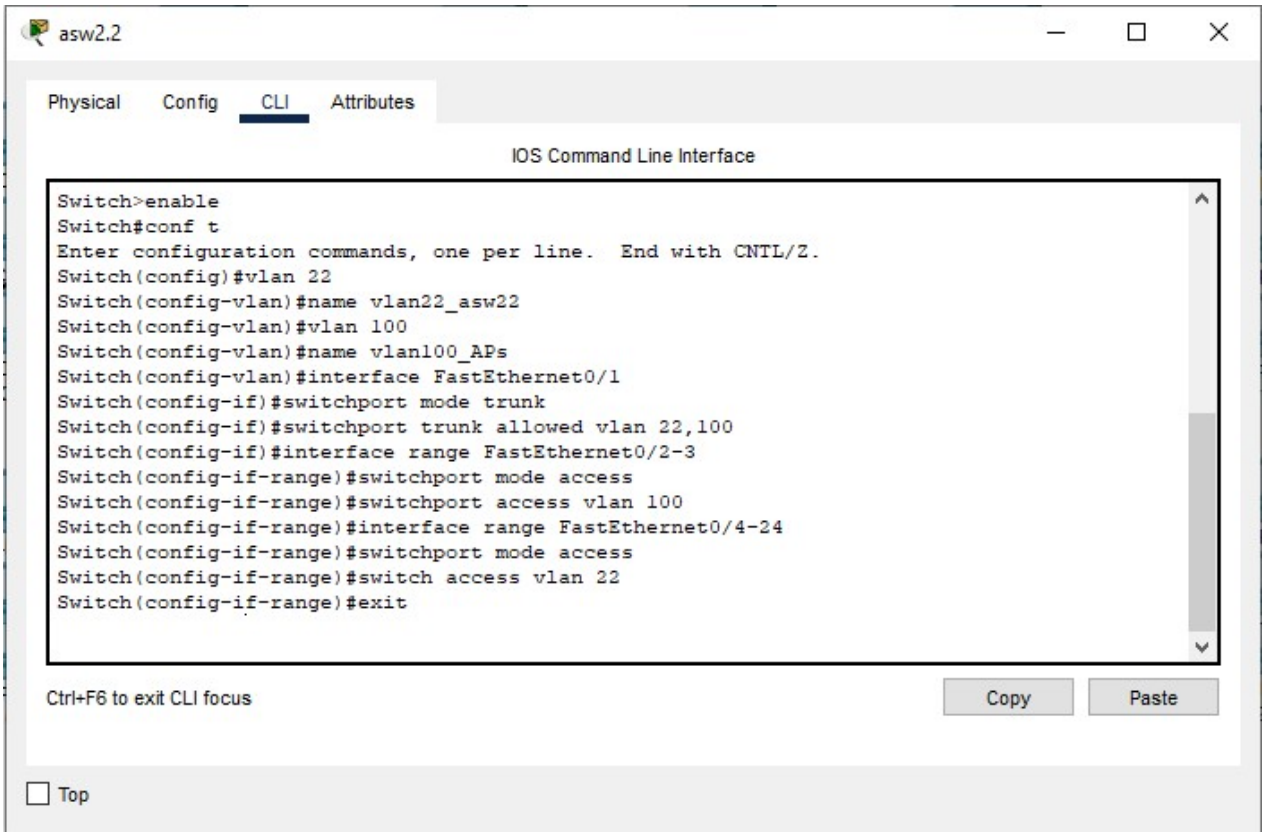


Рисунок 3.5. – Налаштування комутатора рівня доступу на прикладі asw2.2.

Налаштування інших комутаторів доступу виконується аналогічним чином згідно плану підключення обладнання.

При передачі тегованого трафіку через транк порт, назва VLAN-нів не зберігається (Стандарт 801.1Q включає лише числовий ідентифікатор). Вони необхідні для спрощення адміністрування, але ініціалізація VLAN-нів, що використовуються в даному сегменті потрібна в будь якому випадку.

3.3. Налаштування для VLAN пулу DHCP

Для кожного сегменту мережі необхідно визначити пул адрес, що отримають пристрої у відповідь на DHCP запис. Для цього, в свою чергу, необхідно визначити VLAN, створити віртуальні інтерфейси для кожного із

сегментів мережі (на основі фізичного інтерфейсу підключення роутера до агрегуючого комутатора), визначити для кожного з них метод інкапсуляції та ідентифікатор VLAN.

Лістинг команд для налаштування роутеру у відповідності з вищесказаним представлений на (рис. 3.6 [13]) та (рис. 3.7 [13]).

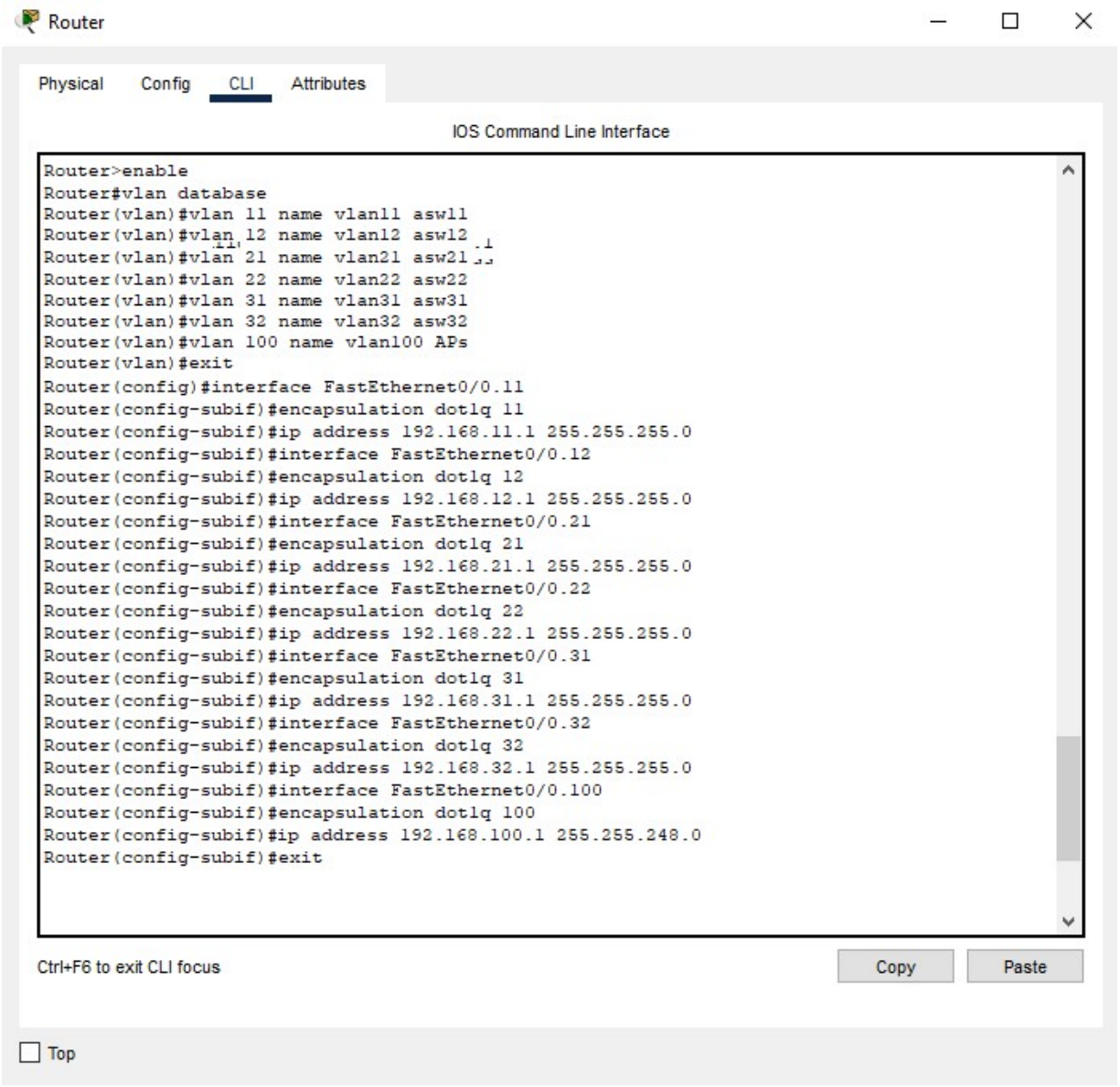


Рисунок 3.6. – Ініціалізація віртуальних інтерфейсів маршрутизатора

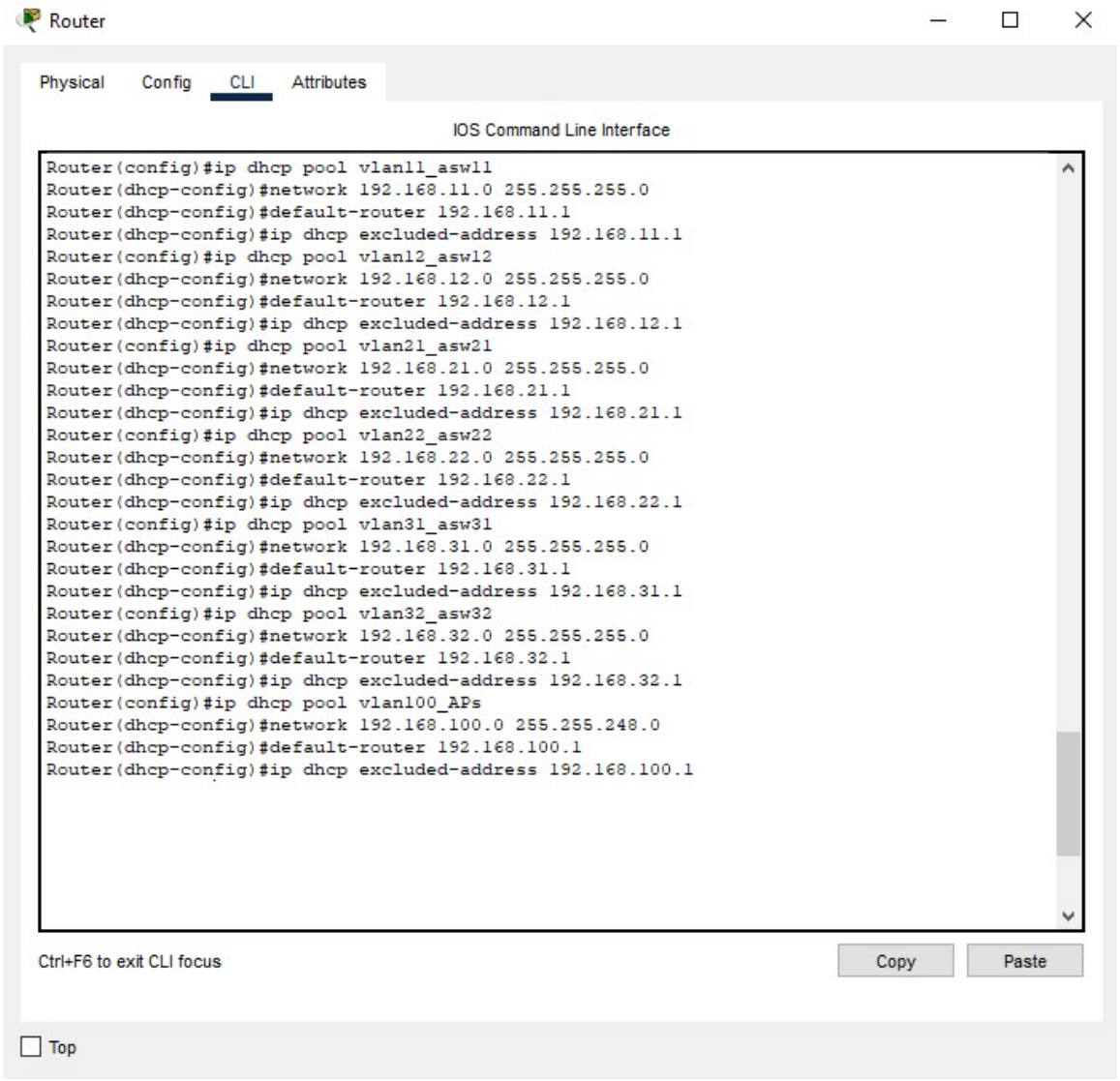


Рисунок 3.7. – Налаштування пулу DHCP адрес на маршрутизаторі

Для перевірки правильності налаштування пулу DHCP та транк портів необхідно на двох будь-яких комп’ютерах у рамках одного сегменту обрати динамічний режим отримання адрес та провести ping запит (рис 3.8). За рахунок сегментації мережі DHCP запит повинен оброблятися значно швидше у порівнянні з плоскою мережею.

Аналогічним чином перевіряється правильність налаштування мережі для точок доступу. Для перевірки доцільно додати до плану мережі два ноутбуки для здійнення ping запиту та перевірки DHCP (рис. 3.9 [13]) [13].

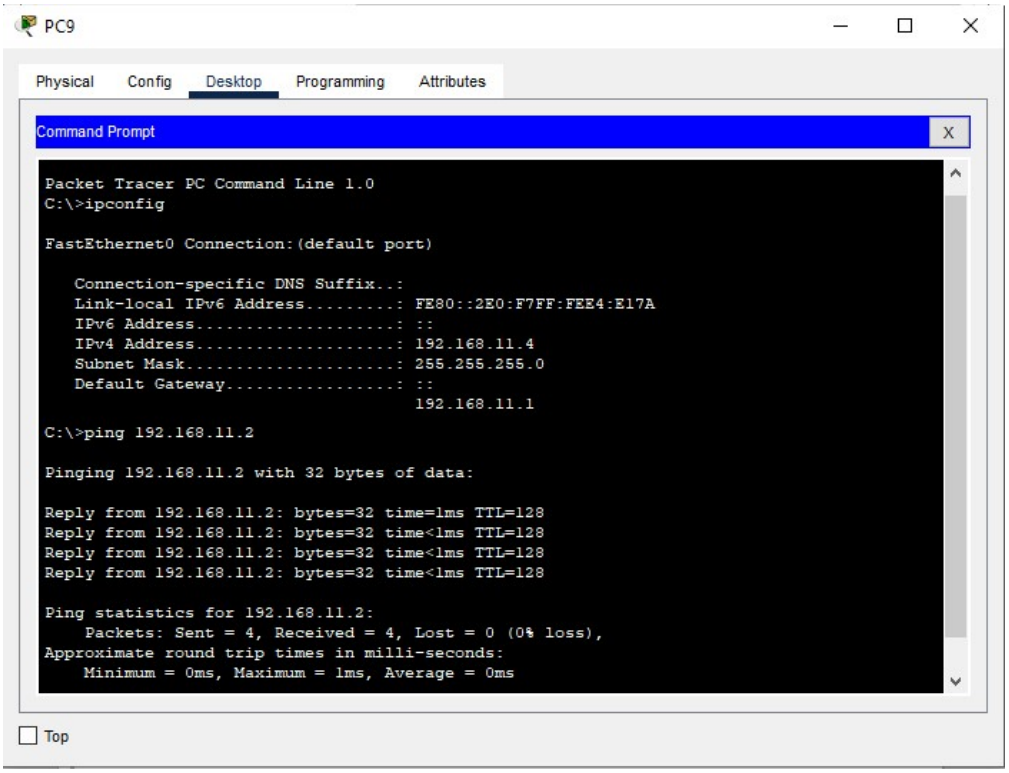


Рисунок 3.8. – Виконання команди ping всередині одного сегменту

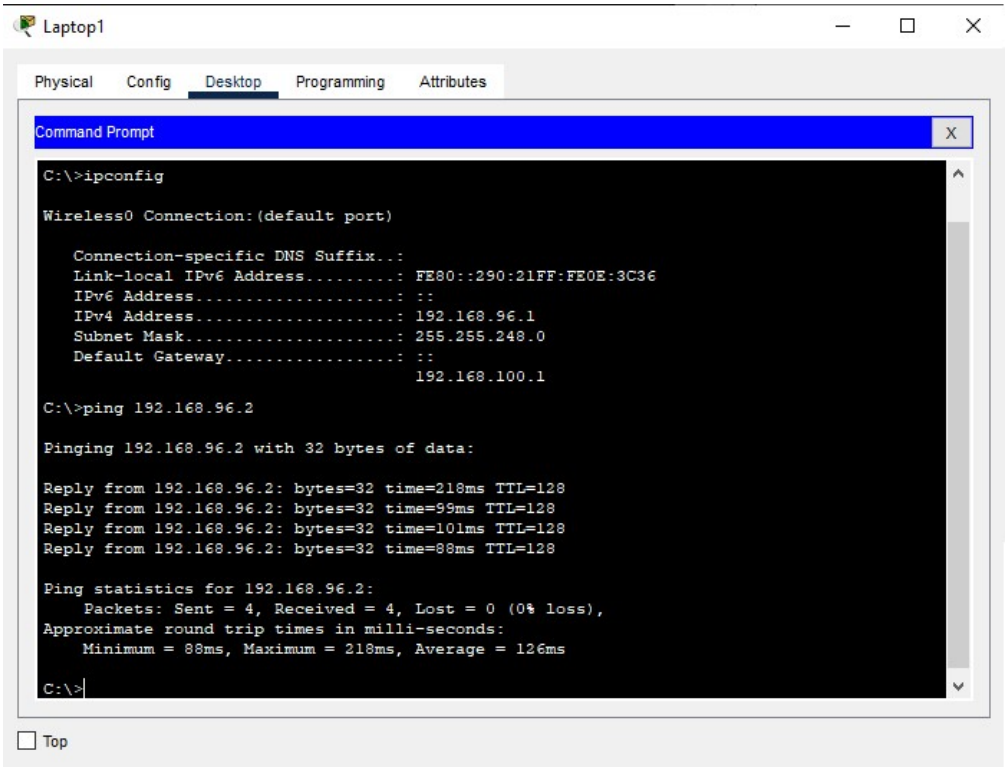


Рисунок 3.9. – Виконання команди ping для ноутбуків підключених до однієї точки доступу

ВИСНОВКИ

У даній роботі були представлені етапи розробки проекту локальної обчислювальної мережі для трьох поверхів корпусу навчального закладу.

Були розглянути технології та стандарти при побудові локальних мереж. На першому етапі було розраховано оціночну можливу кількість робочих місць, з урахуванням норм ДСТУ на розміщення користувачів та призначення кожного з приміщень. На основі отриманих даних було обране відповідне активне обладнання (комутатори доступу, представлені смарт комутаторами компанії D-Link DGS 1210-52/F1), для поєднання користувачів у один сегмент мережі.

Для поєднання сегментів мережі була обрана зіркоподібна топологія, що базується на сегменті ієрахічної моделі побудови. У ролі агрегуючого комутатора D-Link DGS 1210-28/F1. Для забезпечення бездротового з'єднання запропоновано використання точок доступу (чотири на кожен поверх). Точки доступа представлені обладнанням MicroTik Cap (RBcAP2Nd).

Було розраховане теоретичне навантаження в рамках одного сегменту, на рівні розподілення та на порту маршрутизатора. Згідно цього, для поліпшення Інтернет-з'єднання було запропоновано встановлення додаткового маршрутизатора.

З метою зменшення широкомовного трафіку та спрощення адміністрування, мережа була розбита на сім сегментів (кожен комутатор представлений окремим сегментом мережі). Для точок доступу був виділений окремий VLAN. Побудований план IP адресації.

Виконане моделювання роботи мережі у Cisco Packet Tracer. Налаштування обладнання проводилося згідно проекту (налаштування доступу портів комутатора згідно схеми підключення, налаштування віртуальних інтерфейсів та пулу DHCP адрес згідно плану IP-адресації).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Таненбаум Эндрю С, Уэзеролл Дэвид. Компьютерные сети. 5-е изд. – Питер, 2019. – 960 с.
2. А. Н. Цуриков. Компьютерные системы и сети: учебное пособие. – Scientific magazine «Kontsep», 2016. – 64 с.
3. Н. Д. Москин. Вычислительные системы, сети и телекоммуникации. – Петрозаводск, 2019. – 66 с.
4. С. С. Арбузов. Инфокоммуникационные системы и сети: Учебное пособие. – Екатеринбург, 2019. – 112 с.
5. Ватаманюк А.И. Создание, обслуживание и администрирование сетей на 100%. – Питер, 2010. – 288 с.
6. Олифер В.Г. Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – Питер, 2020 – 1008 с.
7. Лаем Куин Ричард Рассел. Fast Ethernet – Киев, 1998. – 448 с.
8. І.М. Журавлівська. Проектування та монтаж локальних комп’ютерних мереж. – Миколаїв, 2016. – 360 с.
9. А.Б. Семенев. Проектирование и расчет структурированных кабельных систем и их компонентов. – Москва, 2010 – 416 с.
10. Ю. А. Тарнавський, І. М. Кузьменко. Організація комп’ютерних мереж. – Київ , КПІ ім. Ігоря Сікорського, 2018. – 259 с.
11. D – LINK. – Режим доступу: https://www.dlink.ru/
12. MicroTik. – Режим доступу: https://mikrotik.com/
13. Cisco Packet Traces - Networking Simulation Tool. - Режим –оступу: https://www.netacad.com/ru/courses/packet-tracer

ДОДАТОК А. Перший розділ (анг.)

BUILDING MODERN NETWORKS. TECHNOLOGIES AND STANDARDS

The OSI and TCP / IP conceptual models are two important network architectures that separate networking into abstraction layers to simplify network analysis. The protocols of the OSI model are not currently used, but the theoretical model is still actual, and the properties of its layers are important. In turn, the protocols of the TCP / IP network model are actively used (especially in Ethernet technology), but the model itself is almost never used.

Another reason why the protocols of the OSI architecture are not used in practice is the long development time. In turn, the TCP / IP c model was used in a real network and evolved in the future. Thus, the OSI model is not used directly, but serves as a basic model for building protocol stacks that are used in real computer networks. This architecture is also called the "reference model".

1.1. OSI conceptual network model

The OSI Reference Model is the first step in the development of an international protocol standard. The International Organization for Standardization (ISO) had created this model in 1983 based on existing developments. This model is called ISO / OSI - Open Systems Interconnection.

The OSI model includes seven layers. This structure is due to the following requirements:

1) The presence of each layer is due to the need to create a separate layer of abstraction
2) Each layer performs a strictly assigned function
3) The functions of each layer must follow standardized protocols
4) Data transfer between interfaces of different layers should be minimal

5) The number of layers should be as small as possible so that the model is not too large.

According to the above about the structure of this network architecture, each layer works with only one specific part of the network interaction. The OSI protocol stack defines seven layers of abstraction. Each layer of the OSI model has interfaces for connecting to layers above or below. Each level works with its own data type (Fig.1.1).

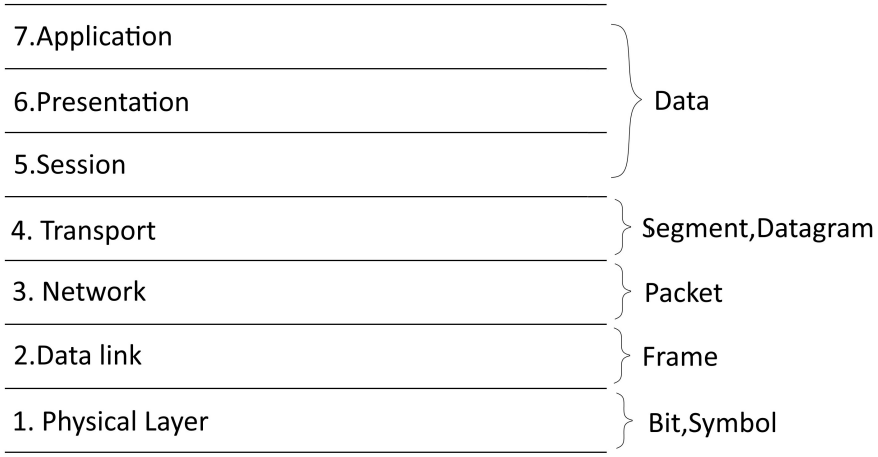


Figure 1.1 – Data types for each layer of the OSI model

The message from computer A to computer B is sequentially transmitted from the highest level to the lowest and vice versa (Fig. 1.2).

Service information at each layer is removed before transferring the payload to the next layer, until we reach the application level.

More detail about each layer:

The physical layer establishes, maintains and breaks a direct connection to the physical communication channel (twisted pair or coaxial cable). Bits of information must be transmitted at a certain distance and reproduced on the receiving side with a given level of confidence in accordance with the characteristics of the signal propagation medium.

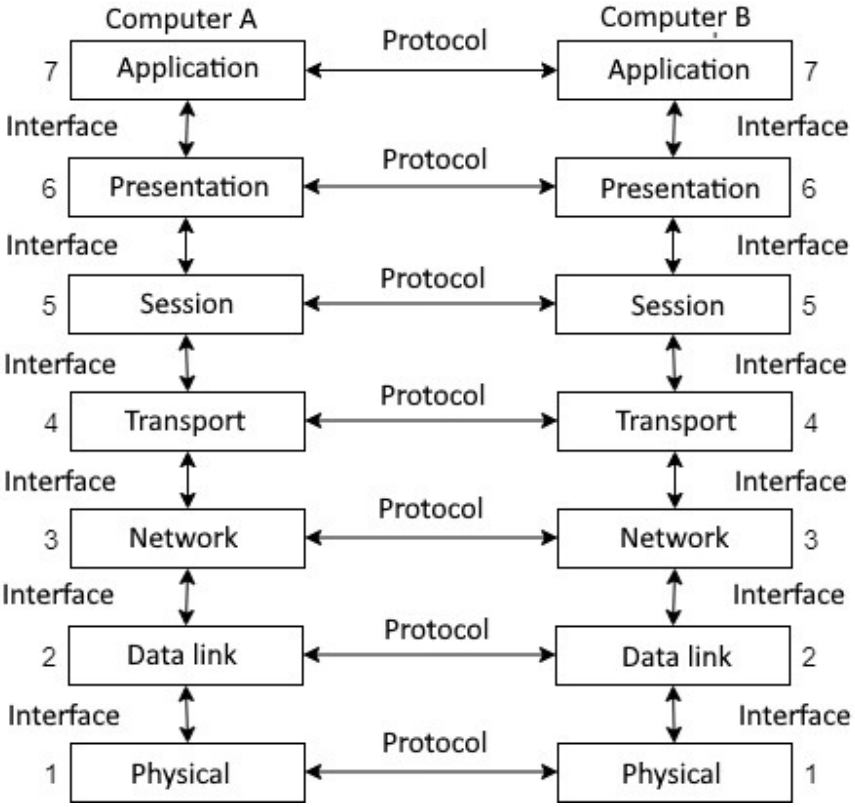


Figure 1.2 – Interaction of two computers according to the OSI / ISO model

The link layer establishes a logical connection between network nodes. Determines the speed of transmission and reception, establishes a reliable connection by detecting and correcting errors. The link layer is divided into two local sublevels:

- LLC, Logical Link Control.
- MAC, Media Access Control

As mentioned earlier, data at the link layer is represented by frames. Physical layer input data (bits) are grouped into frames that range in size from hundreds to thousands of bytes (1 byte = 8 bits). The frame is formed in accordance with the data link layer standards of the technology used (Ethernet, Token Ring FDDI). As a rule, the frame includes a checksum (FCS - Frame Check Sequence) to check the sequence of bits for errors.

The network layer performs logical addressing, switching (channels, messages, packets) and routing when transferring data from source to destination. Network layer functions are implemented by a group of protocols (for example, IP protocol). Thus,

the main task of the network layer is to calculate the optimal route for transmitting data represented by packets.

The transport layer is designed to reliably transfer data from source to destination. The OSI model offers five classes of transport protocol (from lowest 0 to highest 5). Transport layer protocols include UDP (User Datagram Protocol) and TCP (Transmission Control Protocol). The main difference between these two protocols is the verification of the connection establishment (a compromise between reliability and data transfer rate).

Presentation layer. This layer transforms the information that is transmitted on the network, but does not change its content. This includes encryption / decryption algorithms, compressing and decompressing data, converting them into the required format, translating from different languages, and so on. As an example, the cryptographic protocol SSL (Secure Socket Layer).

Session layer. This layer is responsible for creating a session, maintaining it for a significant period of time and ending it. Also, this level performs the task of synchronization, determines the priority of data transmission in the network, and so on. Usually, the functions of this layer are combined with the functions of other layers of the OSI model.

Application layer. At the application layer, network user application processes (software) gain access to network resources. Also, this layer organizes file transfer, e-mail exchange, network management, and so on. For example, HTTP (Hypertext File Transfer Protocol) that can be read by a web browser, FTP (File Transfer Protocol) and SMTP (Simple Mail Transfer Protocol).

1.2. TCP/IP conceptual network model

During the development of computer networks, many different network protocols have been presented, but the most popular of them is the TCP / IP protocol

stack. This protocol stack includes the TCP and IP protocols. This model also includes other protocols, such as the domain name system (DNS), which converts logical addresses to textual form for the end user, and vice versa, and the previously mentioned file transfer protocol (FTP), which organizes file transfers, and also versions of the NFS protocol, which provide access to remote file systems.

The TCP / IP protocols were used in the ARPANET computer network, which can be called the prototype of the modern Internet. Many technologies start with the military and the ARPANET is no exception. ARPANET was the research network of the US Department of Defense. Over time, this network connected hundreds of universities and government buildings using telephone lines. This network grew and after that new ways of transferring data appeared.

When new ways of transmitting traffic (satellite, radio) appeared, problems arose when trying to combine existing networks and new ones using existing protocols. The ability to combine different networks into a single information space has been a problem since the beginning of networks. The network architecture that was used in the ARPANET was later named TCP / IP in accordance with the two main protocols of this architecture. Cerf and Kahn (1974) was the first to describe this network architecture, and later TCP / IP became the standard (Braden, 1989).

The US Department of Defense was concerned about the possibility of failure of certain parts of the network (hosts, routers, gateways). Therefore, this architecture was required to keep the network functioning (the ability to transfer traffic from one host to another) even if a certain amount of hardware fails. In other words, it is necessary to choose the most optimal network architecture where the connection remains until the receiving and transmitting machines and some part of the switching and routing hardware remain working. In addition, the architecture should be flexible, because it was supposed to use various kinds of applications with specific requirements (file transfer, real-time voice transmission, etc.).

The TCP / IP model is hierarchical and unlike the OSI / ISO reference model, it has only four layers compared to seven (Fig. 1.3). This is due to the fact that in this network model, compared to OSI, there is no presentation layer, session layer and physical layer (the physical and data link layers are represented by one single layer). In turn, the absence of a session layer and a presentation layer is explained by the fact that applications include all the necessary functions of these two layers and therefore they are not needed.

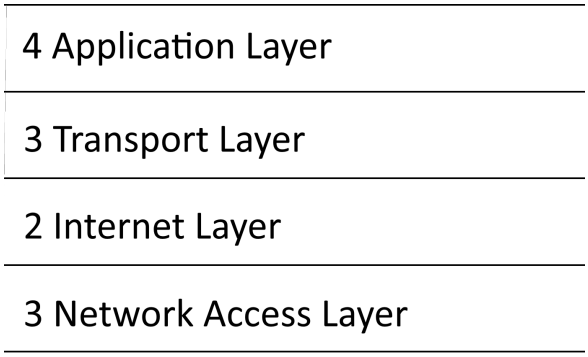


Figure 1.3 – TCP / IP network model levels

Details about each layer and its functions:

Application level. This level defines the way of data exchange between user applications. In client-server systems, the client application must know how to form a transfer request, and in turn, the server application must know how to process this request. This function is implemented by the protocols HTTP, FTP, Telnet. It also includes protocols like DNS, RTP, SMTP.

Transport layer. This layer performs the same function as the transport layer of the OSI model. That is, it establishes a connection between two hosts of the same rank in the transmit-receive mode. This layer is implemented by the protocols that were already mentioned above in the OSI model, specifically the TCP and UTP protocols.

Transmission Control Protocol TCP, as mentioned earlier, is a reliable connection protocol. This means that he must make sure that data is transferred from one host to another without errors. This protocol splits the transmitted stream of bytes

into separate messages for transmission over the Internet layer. On the receiving side, using the TCP process, the individual messages are combined into one stream of bytes. It also controls the output stream to avoid overloading network bottlenecks (if transmission is faster than reception).

Another transport layer protocol is the user datagram protocol. This protocol, unlike TCP, does not establish a reliable connection and does not control the flow as in TCP, which makes this protocol unreliable. In other words, the transfer will be performed "blindly", that is, without confirmation of the fact of data reception. This can be useful when speed is needed more than reliability. For example, for one-time client-server requests, such as video and audio. In this case, if a small part of the message (part of a word, or frame) is lost, the human brain is able to supplement the missing information.

Some of the protocols of the TCP / IP model are shown in Figure 1.4.

Figure 1.4 – Protocols of the TCP/IP model

Layer	Protocols
Application	HTTP, SMTP, RTP , DNS
Transport	TCP, UDP
Internet	IP, ICMP
Network Access	DLS, SONET, 802.11(WIFI),Ethernet

Internet layer. This level is the basis of the TCP / IP model. The main task of the internetwork layer is to find the optimal route for transmitting a packet from one host on the network to another along an independent path. That is, when receiving and transmitting, packets do not necessarily have to go through the same path. Moreover, parts of one message sent simultaneously can be received on the receiving side in an arbitrary sequence (if the packets were transmitted in different ways). If it is necessary to adhere to the original sequence, then higher-level protocols are used. Also, the gateway defines the packet format and the Internet protocol.

Link layer. This is the lowest layer of this architecture. It combines hardware, software and signal transmission parameters for a specific signal propagation medium. Tre link layer is determined by the standards of the link layer technology that is used (Ethernet, 802.11, etc.). In general, it is not a layer, but an interface between the signal propagation medium and the Internet layer. In other words, for the layers above it does not matter how the signal propagates, because the data remains the same.

1.3. Ethernet technology

The most common Ethernet technology and its first standards were developed in 1970 by the Xerox Corporation. This was the standard used by only one company. sometime later (in 1980) a similar technology was adopted by the IEEE (IEEE 802 committee).

This committee includes several working groups. To develop standards and rules for the operation of networks for the Ethernet standard, the 802.3 group was formed. This group of standards defines the physical medium of the signal propagation and the frame format.

There are several common Ethernet frame formats for this group of standards, but in practice the network hardware only works with one frame format, namely the Ethernet DIX (Fig. 1.5). This format is also called Ethernet II, because of the number of the latest DIX standard.

Today, the most common technology in the construction of local area networks is Fast Ethernet technology (group of standards), which comes from Ethernet technology. In particular, the widespread standard is 100Base-T, a common name for standards with a transmission rate of 100 Mbps over twisted pair.

Figure 1.5 – Ethernet DIX (II) frame format

6 byte	6 byte	2 byte	46-1500 byte	4 byte
Destination MAC	Source MAC	Internet layer protocol code (0x0800 for IPv4)	Data	FCS

1.4. Fast Ethernet

The Fast Ethernet specification was the first of the high-speed versions of Ethernet, so it was called "Fast" (100 Mbps vs. 10 Mbps).

The physical topology of Fast Ethernet is a star, but logically works like a bus network due to the network access methods it inherited from Ethernet technology. The frame format of Fast Ethernet technology is no different from the frame format of Ethernet DIX (II).

Fast Ethernet supports three physical signal propagation medium:

- Multi-mode fiber optic cable (two fibers);
- Category 5 cable of twisted pair (two pair);
- Category 3 cable of twisted pair (four fibers).

Coaxial cable used in Ethernet technology is not included in this standard. Thus, the official 802.3 standard includes three different specifications for the physical layer of Fast Ethernet:100Base-TX:

- 100Base-TX – two pairs of four unshielded category 5 cable of twisted pair
- 100Base-T4 – two pairs of four unshielded category 3,4 and 5 cable of twisted pair
- 100Base-FX – multy-mode fiber optic cable with two fibers

Fast Ethernet technology uses a multi-access method with carrier control and collision detection, like an Ethernet technology. Each type of Fast Ethernet cable has physical limitations on cable length due to signal attenuation and collisions

(transmission starts from two hosts at the same time and the number of collisions increases with the number of hosts and network load, and delays increase with long cable lengths). The limit for twisted pair is 90-100 m, and for 100 Base-FX optical cable approximately 400 m.

Category 5E unshielded twisted pair is typically used to connect LAN computers to switching hardware. This cable is used due to its low cost and good bandwidth.

1.5. DHCP

Fast Ethernet technology uses TCP / IP network model protocols, including the Internet protocol. Each computer or other device that supports these protocols (smartphones, laptops, tablets, printers, etc.) and is connected to a local network must have a unique IP address. as the number of devices connected to the network increases, it becomes more difficult for the system administrator to record a unique IP address for each of them. From a security point of view, the best option is to write down the IP address manually for each device. But a network can have dozens of switches that connect hundreds of computers and dozens of printers. This is a fairly typical amount of hardware for a corporate LAN. There is DHCP to solve this problem. DHCP works as a "client-server". When the OS starts, the computer that is the DHCP client (the flag is enabled in the adapter settings) makes a broadcast request for an IP address. The DHCP server responds to the request and sends the parameters necessary for the operation of the device on the network, including its IP address. The DHCP server can operate in three modes:

- Manual mode
- Automatic mode
- Dynamic mode

In any mode, when configuring a DHCP server on a router, the administrator enters a range of IP addresses (or multiple ranges) so that all of these addresses belong to the same network (have the same network address).

In manual mode, in addition to the range of available logical addresses (IP addresses), the administrator must specify a list of physical addresses (MAC addresses) of hosts. In this case, the DHCP server will distribute predefined IP addresses at each startup according to the physical address of each host.

In automatic mode (automatic installation of static addresses), the DHCP server determines the physical address of the hosts and binds the IP address to it, as in manual mode.

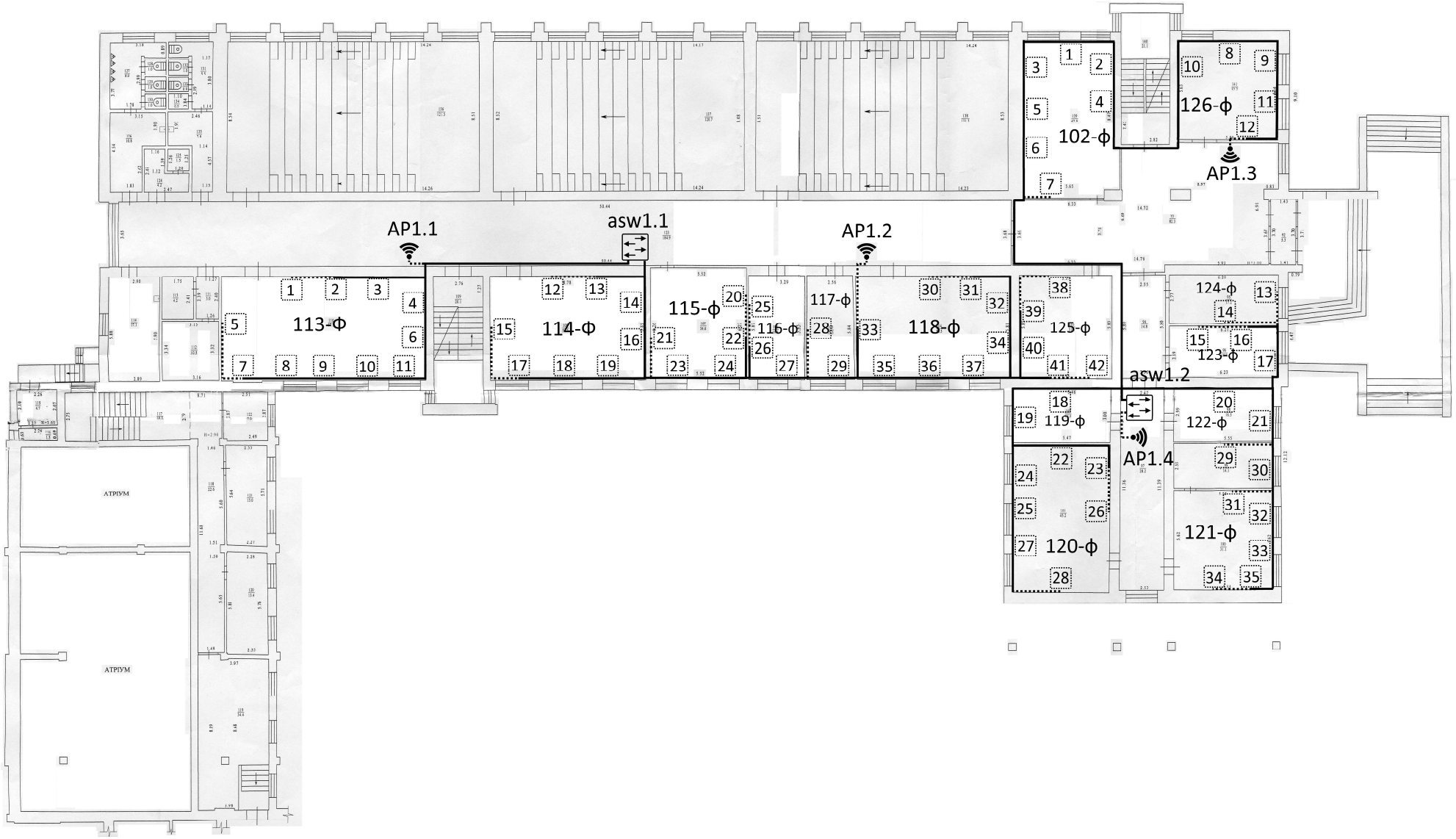
In automatic DHCP mode, the server gives each host an address for "lease" for a limited period of time, i.e. until the device is removed from the network. This is especially useful when connecting a network of devices such as a smartphone, tablet, or laptop (using an RJ-45 postcard, or a wireless connection).

A router is usually used to dynamically distribute IP addresses. As an example, a home WIFI router that combines the functionality of switching hardware, router and access point. A separate DHCP server or OSI model L3 level switch with dynamic addressing support can also be used.

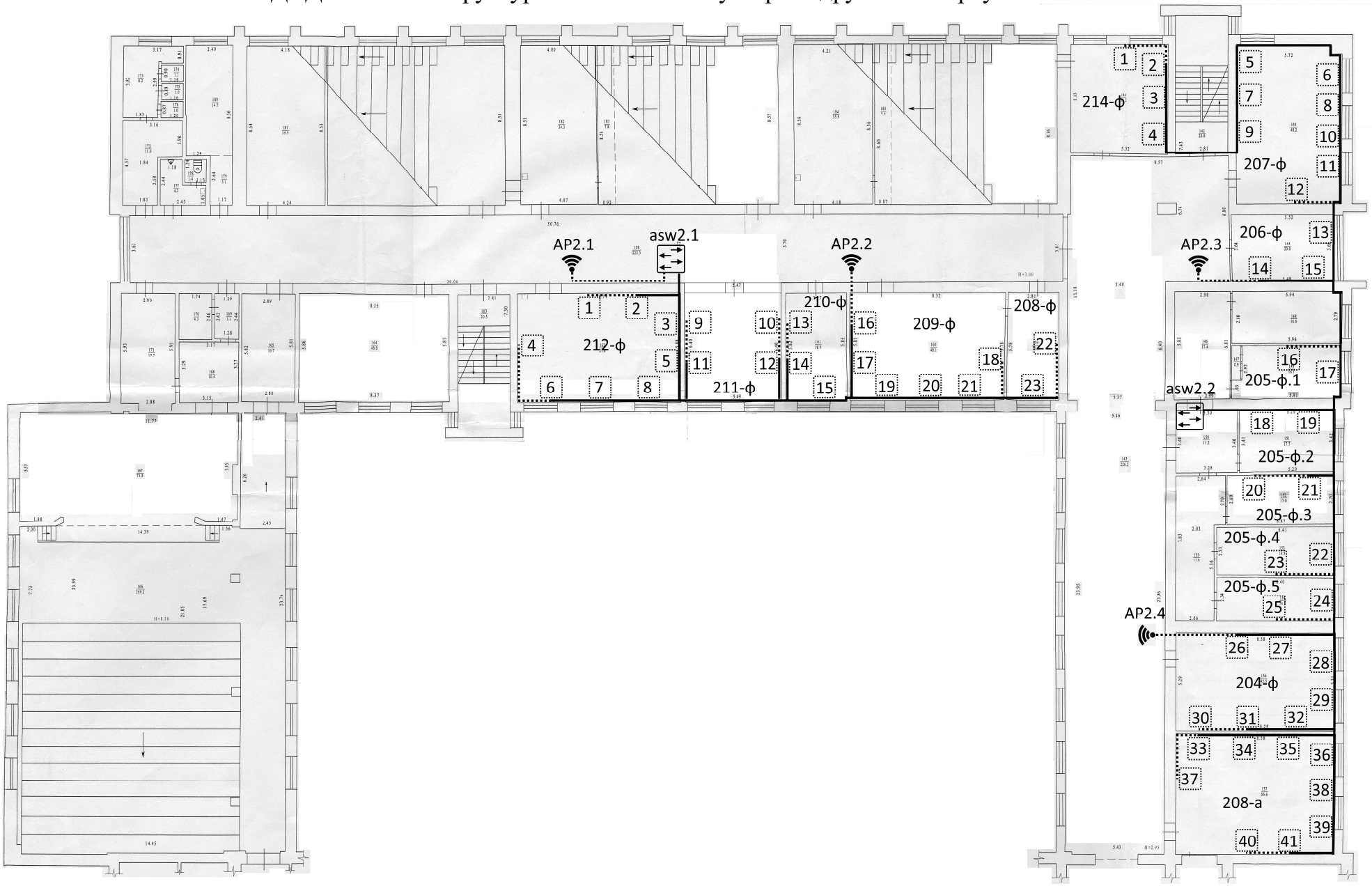
When using virtual local area network (VLAN) technology, it is possible to specify separate IP address ranges for each VLAN. For example, in a corporate network, separate guest WIFI into a separate virtual network and assign it a range of IP addresses for issuing temporary network devices (laptops, smartphones, tablets, etc.) that connect via WIFI (802.11 standard).

ДОДАТОК Б. Структурна схема мережі

Б.1 Структурна схема сегменту мережі першого поверху



ДОДАТОК Б.2 Структурна схема сегменту мережі другого поверху



ДОДАТОК Б.3 Структурна схема сегменту мережі третього поверху