Міністерство освіти і науки України
Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»
(повне найменування вищого навчального закладу)

Відділення телекомунікацій та електронних систем
(назва відділення)
Циклова комісія комп'ютерної інженерії
(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи бакалавра

(освітньо-кваліфікаційний рівень)

на тему: **Розробка проекту комп'ютерної мережі ТОВ «ЕКС-простір»**

Виконав: студент VI курсу, групи КІб-602

Спеціальності:
123 «Комп'ютерна інженерія
(шифр і назва спеціальності)

_____Андрій КІТ_____
(підпис) (ім'я та прізвище)

Керівник _____ Василь ПИЖ
(підпис) (ім'я та прізвище)

Рецензент _____
(підпис) (ім'я та прізвище)

Тернопіль – 2023

Відокремлений структурний підрозділ
«Тернопільський фаховий коледж
Тернопільського національного технічного університету імені Івана Пулюя»

Відділення телекомунікацій та електронних систем
Циклова комісія комп'ютерної інженерії
Освітньо-кваліфікаційний рівень бакалавр
Спеціальність 123 «Комп'ютерна інженерія»
(шифр і назва)

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"01" травня 2023 року

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

Кіт Андрію Володимировичу
(прізвище, ім'я, по батькові студента)

1. Тема роботи: **Розробка проекту комп'ютерної мережі ТОВ «ЕКС-простір»**

керівник роботи: Пиж Василь Степанович
(прізвище, ім'я, по батькові)

затверджені наказом вищого навчального закладу від 1.05.2023р. № 4/9-173

2. Строк подання студентом кваліфікаційної роботи 21.06.2023р.

3. Вихідні дані до роботи: плани приміщень, завдання на проектування, стандарти побудови СКС, документація на мережеве обладнання і сервери

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

Перелік термінів і скорочень

Вступ

АНОТАЦІЯ

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

4.7 Обчислення накладних витрат

4.8 Складання кошторису витрат та визначення собівартості НДР.

4.9 Розрахунок ціни НДР

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

5. ОХОРОНА ПРАЦІ, ТЕХНІКИ БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Електромагнітні випромінювання (ЕМП)

5.2 Пожежна безпека на підприємстві

ВИСНОВКИ

ПЕРЕЛІК ПОСИЛАНЬ

Висновки: навести результати роботи по кожному розділу зокрема і загальний висновок по кваліфікаційній роботі

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

План приміщень

Логічна топологія

Фізична топологія

Таблиця IP-адрес

Таблиця техніко-економічних показників

Модель мережі

6. Консультанти розділів кваліфікаційної роботи бакалавра

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Оксана РЕДЬКВА викладач		
Охорона праці, техніка безпеки та екологічні вимоги	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	02.05	
2	Збір і узагальнення інформації по роботі	15.05	
3	Написання першого розділу	24.05	
4	Розробка технічного та робочого проекту	29.05	
5	Написання спеціального розділу	2.06	
6	Розрахунок економічної частини	5.06	
7	Написання розділу охорони праці	7.06	
8	Виконання графічної частини	12.06	
9	Оформлення проекту	16.06	
10	Проходження нормоконтролю	19.06	
11	Попередній захист роботи	21.06	
12	Захист роботи		

7. Дата видачі завдання 2.05.2023р.

Студент _____ Андрій КІТ_
(підпис) (ім'я та прізвище)

Керівник кваліфікаційної роботи _____ Василь ПИЖ
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Кіт А В. Розробка проекту комп’ютерної мережі ТОВ «ЕКС-простір» : кваліфікаційна робота на здобуття освітнього ступеня бакалавр, за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2023. 90с.

Кваліфікаційна робота описує головні етапи створення компютерної мережі. В роботі приводиться структура підприємства, опис та вибір топології та технології мережі, проводиться підбір та налаштування обладнання мережі.

Проводиться обґрунтування вибору програмного забезпечення та способи його налаштування. В роботі розроблено модель мережі.

Описано методику розрахунку вартості робіт та описані питання з техніки безпеки та охорони праці.

Ключові слова: компютерна мережа, топологія, технологія, сервер, вита пара.

ANNOTATION

Kit A. V. Development of the computer network project of "EKS-prostir" LLC : qualifying work for obtaining a bachelor's degree, specialty 123 Computer engineering. Ternopil: Separate Structural Subdivision "Ternopil Professional College of Ternopil Ivan Puluj National Technical University", 2023, 2023. 90p.

The qualification work describes the main stages of creating a computer network. The work presents the structure of the enterprise, description and selection of network topology and technology, selection and configuration of network equipment.

The justification of the choice of the software and the methods of its adjustment are carried out. A network model is developed in the paper.

The methodology for calculating the cost of works is described, as well as issues related to safety and occupational health and safety.

Key words: computer network, topology, technology, server, twisted pair.

Зміст

ВСТУП

Протягом останнього десятиліття дедалі ширший розвиток отримують глобальні обчислювальні й інформаційні мережі – унікальний симбіоз комп'ютерів і комунікацій. Відбувається активне приєднання всіх країн до всесвітніх мережних структур. [22]

Світовою системою комп'ютерних комунікацій щодня користуються більш як 300 млн. людей. Зростає потреба в засобах структурування, накопичення, збереження, пошуку і передачі інформації. Задоволенню цих потреб служать інформаційні мережі та їхні ресурси.

Спільне використання ресурсів мереж (бібліотек програм, баз даних, обчислювальних потужностей) забезпечується технологічним комплексом і засобами доступу.

Глобальні мережі (WideArea Network, WAN) – це телекомунікаційні структури, що об'єднують локальні комп'ютерні мережі, які мають загальний протокол зв'язку, методи підключення і протоколи обміну даними. Кожна з глобальних мереж (INTERNET, BITNET, DECNET і ін.) організовувалася для певних цілей, а надалі розширювалася завдяки підключенню локальних мереж, що використовують її послуги і ресурси.

Найбільшою глобальною інформаційною мережею є Internet, яка об'єднує кілька мільйонів людей із всіх країн світу за допомогою сучасних і зручних засобів зв'язку.

Архітектура мережі Internet розроблена на основі концепції взаємопоєднуваності або міжмережевого поєднання різнорідних мереж, побудованих на базі різних фізичних систем зв'язку і комунікаційних технологій.

Таким чином, Internet- це сукупність технічних засобів, стандартів і домовленостей, яка дає змогу підтримувати зв'язок між різними комп'ютерними мережами у світі.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Темою кваліфікаційної роботи бакалавра є розробка проекту комп'ютерної мережі для компанії "ЕКС-простір".

Перед мережею ставляться такі вимоги:

– Об'єднання ПК, що входять до різних структурних одиниць.

– Спільне використання одного підключення до мережі Інтернет.

– Використання в своїй роботі служб локальної мережі та мережі Інтернет.

– Дешевий засіб обміну інформацією.

1.1.2 Призначенння розробки

Дана комп'ютерна мережа призначена для організації ефективної роботи працівників компанії "ЕКС-простір".

Дане підприємство займається продажем автозапчастин.

Проектована мережа повинна забезпечити швидкий доступ до файлів, службової інформації та інших ресурсів загального використання, забезпечити вихід в Інтернет.

Дана мережа буде використовуватися для документообігу, а також для обміну інформацією між структурними підрозділами підприємства, для доступу до Інтернет, для мережевого друку.

Для зберігання інформації в мережі має бути використано сервер.

Швидкість мережі має бути 1000 Мбс.

Дана мережа повинна мати доступ до Internet.

1.1.3 Вимоги до апаратного та програмного забезпечення

Мережа яку ми проектуємо в даній роботі має бути побудована на:

- базі сучасних програмних та апаратних засобів,
- використовувати сучасні протоколи обміну,
- сучасні технології та топологію,
- бути поділена на робочі групи,
- швидкість мережі має бути 100/1000 Мбіт/с.

Апаратне забезпечення нашої мережі має бути:

- загальновживане,
- недороге,
- підтримувати вказану швидкість передачі даних,
- мати можливість швидкої заміни, ремонту,
- мати можливість адміністрування.

Програмне забезпечення мережі – це сукупність операційних систем, що встановленні на комп'ютерах працівників підприємства.

В даному випадку операційні системи, які планується використовувати- Windows 10.

Безпровідні точки доступу мають підтримувати протоколи wpa-psk, wpa2-psk і відповідати стандарту 802.11n.

1.1.4 Стадії та етапи розробки

При проектуванні мережі необхідно вивчити таке:

- Чим займається підприємство,
- Чи планується його зростання.
- Чи є існуюча комп'ютерна мережа.
- Яке програмне забезпечення буде використано в мережі.

– Визначити тип мережі, топологію, провідники та інше обладнання першого рівня.

– Визначити тип та необхідну кількість комутаторів для робочих груп.

– Визначити потребу головного комутатора,

– Визначити необхідність встановлення маршрутизаторів та підключення до мережі Інтернет.

1.1.5 Вимоги до документації

В результаті проектування потрібно створити наступну документацію:

– Логічна топологія

– Фізична топологія

– Помічені виходи кабелю

– Помічені траси кабелю

Після виконання вищевказаних робіт можна приступити до монтажу системи.

1.1.6 Техніко-економічні показники

Розроблена мережа повинна бути:

– сучасною,

– недорогою,

– масштабованою

– швидкість передачі інформації — 100\1000 Мбіт\с,

– мати доступ до мережі Інтернет

– мережа повинна мати безпровідний сегмент,

– в мережі повинен бути сервер для бухгалтерії та WEB сервер.

1.1.7 Порядок контролю та прийому

При прийомці мережі необхідно виконати

– перевірку функціонування усіх мережевих вузлів.

– кабелі мають бути промаркованими.

– перевірка функціонування мережі виконується за допомогою прикладних утиліт або пакетів, здатних замінити дані утиліти.

Здача в експлуатацію мережі – досить важливий етап, який певною мірою визначає якісне функціонування мережі протягом всього терміну експлуатації.

Замовник, який одержав повідомлення підрядника про завершення робіт та комплект документів, повинен приступити до комплексної перевірки функціональних характеристик мережі та прийняття її в експлуатацію спеціально створеною приймальною комісією.

1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі

Мета дипломного проекту - створення комп’ютерної мережі компанії "ЕКС-простір".

Основним видом діяльності є імпорт та реалізація якісних автозапчастин та автохімії. Систематичний аналіз потреб ринку, постійне розширення асортименту та спектру послуг сприяло успішному розвитку компанії. На сьогодні була виконана величезна робота над удосконаленням усіх етапів робочого процесу від підбору автозапчастини до отримання її клієнтом.

Якісна консультація клієнта стоїть у пріоритеті компанії. Широкий асортимент магазину дозволяє нашим клієнтам вибрати найвигіднішу пропозицію.

За допомогою сучасного системного забезпечення нашого ресурсу клієнтам надано: максимально зручний інтерфейс для підбору запчастин, оптимізована форма прийому замовлень, можливість відстеження стану замовлень на кожному етапі постачання, SMS інформування, онлайн комунікація з клієнтом протягом усієї угоди, детальна інформація про товар, зручні способи оплати тощо.

Персональні комп'ютери будуть розміщуватись у таких приміщеннях:

– Бухгалтерія — розміщено мережевий принтер, три ПК, сервер, комутуюче обладнання;

– конференц приміщення — 5 ПК, мережевий принтер, точка доступу, комутатор,

– два кабінети менеджерів — 10 пк,

– технічний відділ — все обладнання для створення мережі (центральний комутатор , доступ до інтернету, сервер)

– Керівник та заступник керівника - два комп'ютера;

– виставковий зал - 4 ПК.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Розробка та обґрунтування логічної та фізичної схем мережі [23,24]

Під топологією (компонуванням, конфігурацією, структурою) комп'ютерної мережі звичайно розуміється фізичне розташування комп'ютерів мережі друг щодо друга й спосіб з'єднання їхніми лініями зв'язку. Важливо відзначити, що поняття топології ставиться, насамперед, до локальних мереж, у яких структуру зв'язків можна легко простежити.

Топологія визначає вимоги до устаткування, тип використовуваного кабелю, можливі й найбільш зручні методи керування обміном, надійність роботи, можливості розширення мережі. Типи топологій комп'ютерних мереж зображено на рисунку. 2.1.

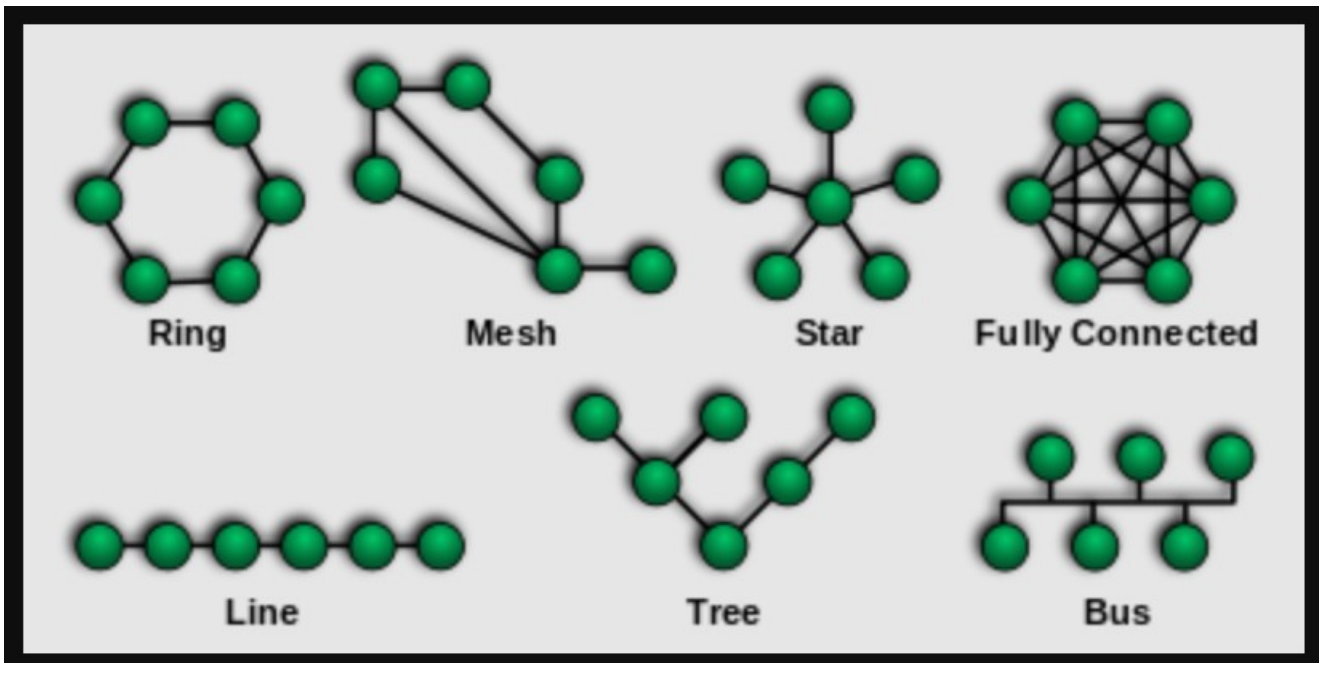


Рисунок 2.1 - Типи топологій комп'ютерних мереж, де:
верхній ряд зліва направо — кільце, комірчаста, зіркова, повнозв'язна;
нижній ряд зліва направо — лінійна, деревоподібна, шина.

Існує три основних топології мережі:

1. зірка (star), при якій до одного центрального комп'ютера приєднуються інші периферійні комп'ютери, причому кожний з них використовує свою окрему лінію зв'язку ;
2. кільце (ring), при якій кожний комп'ютер передає інформацію завжди тільки одному комп'ютеру, наступному в ланцюжку, а одержує інформацію тільки від попереднього комп'ютера в ланцюжку, і цей ланцюжок замкнутий в «кільце»;
3. шина (bus), при якій всі комп'ютери паралельно підключаються до однієї лінії зв'язку й інформація від кожного комп'ютера одночасно передається всім іншим комп'ютерам .

Топологія "Зірка"

Топологія «Зірка» - це топологія з явно виділеним центром, до якого підключаються всі інші абоненти. Весь обмін інформацією йде винятково через центральний вузол, на який у такий спосіб лягає дуже більше навантаження, тому нічим іншим, крім мережі, воно займатися не може. Зрозуміло, що мережне устаткування центрального абонента повинне бути істотно більше складним, чим устаткування периферійних абонентів. Про рівноправність абонентів у цьому випадку говорити не доводиться. Як правило, саме центральний вузол є самим потужним, і саме на нього покладають всі функції по керуванню обміном. Ніякі конфлікти в мережі з топологією «зірка» у принципі неможливі, тому що керування повністю централізоване, конфліктувати нема чому.

Якщо говорити про стійкість зірки до відмов комп'ютерів, то вихід з ладу периферійного комп'ютера ніяк не відбивається на функціонуванні частини мережі, що залишилася, зате будь-яка відмова центрального комп'ютера робить мережу повністю непрацездатною. Тому повинні прийматися спеціальні заходи щодо підвищення надійності центрального комп'ютера і його мережної апаратури. Обрив будь-якого кабелю або коротке замикання в ньому

при топології «зірка» порушує обмін тільки з одним комп'ютером, а всі інші комп'ютери можуть нормально продовжувати роботу.

На відміну від шини, у зірці на кожній лінії зв'язку перебувають тільки два абоненти: центральний і один з периферійних. Найчастіше для їхнього з'єднання використовується дві лінії зв'язку, кожна з яких передає інформацію тільки в одному напрямку. Таким чином, на кожній лінії зв'язку є тільки один приймач і один передавач. Все це істотно спрощує мережне встаткування в порівнянні із шиною й рятує від необхідності застосування додаткових зовнішніх термінаторів. Проблема загасання сигналів у лінії зв'язку також вирішується в «зірці» простіше, ніж в «шині», адже кожний приймач завжди одержує сигнал одного рівня. Серйозний недолік топології «зірка» складається у жорсткому обмеженні кількості абонентів. Звичайно центральний абонент може обслуговувати не більше 8-16 периферійних абонентів. Якщо в цих межах підключення нових абонентів досить просто, то при їхньому перевищенні воно просто неможливо. Правда, іноді в зірці передбачається можливість нарощування, тобто підключення замість одного з периферійних абонентів ще одного центрального абонента (у результаті виходить топологія з декількох з'єднаних між собою зірок).

Існує топологія зірки, що зветься активною, або справжньою зіркою.

Кільце найбільш уразливе до ушкоджень кабелю, тому в цій топології звичайно передбачають прокладку двох (або більше) паралельних ліній зв'язку, одна з яких перебуває в резерві.

У той же час велика перевага кільця полягає в тому, що ретрансляція сигналів кожним абонентом дозволяє істотно збільшити розміри всієї мережі в цілому (часом до декількох десятків кілометрів). Кільце щодо цього істотно перевершує будь-які інші топології.

Недоліком кільця (у порівнянні із зіркою) можна вважати те, що до кожного комп'ютера мережі необхідно підвести два кабелі.

Іноді топологія «кільце» виконується на основі двох кільцевих ліній

зв’язку, що передають інформацію в протилежних напрямках. Мета подібного рішення – збільшення (в ідеалі удвічі) швидкості передачі інформації. До того ж при ушкодженні одного з кабелів мережа може працювати з іншим кабелем (правда, гранична швидкість зменшиться).

Коміркова топологія

Коміркова топологія (mesh) утворюється з повнозв’язної шляхом видалення деяких можливих зв'язків. У мережі з комірковою топологією безпосередньо зв'язуються тільки ті вузли, між якими відбувається інтенсивний обмін даними, а для обміну даними між вузлами, не сполученими прямими зв'язками, використовуються транзитні передачі через проміжні вузли. Коміркова топологія припускає з'єднання великої кількості вузлів і характерна, як правило, для глобальних мереж.

Топологія "Шина"

Топологія «шина» (або, як її ще називають, «загальна шина») самою своєю структурою припускає ідентичність мережного устаткування комп’ютерів, а також рівноправність всіх абонентів. При такому з’єднанні комп’ютери можуть передавати тільки по черзі, тому що лінія зв’язку єдина. У іншому випадку передана інформація буде спотворюватися в результаті накладення (конфлікту, колізії). Таким чином, у шині реалізується режим напівдуплексного (half duplex) обміну (в обох напрямках, але по черзі, а не одночасно).

У топології «шина» відсутній центральний абонент, через який передається вся інформація, що збільшує її надійність (адже при відмові будь-якого центра перестає функціонувати вся керована цим центром система). Додавання нових абонентів у шину досить просте й звичайно можливе навіть під час роботи мережі. У більшості випадків при використанні шини потрібна мінімальна кількість сполучного кабелю в порівнянні з іншими топологіями. Правда, треба врахувати, що до кожного комп’ютера (крім двох крайніх) підходить два кабелі, що не завжди зручно. Тому що дозвіл можливих конфліктів у цьому випадку лягає на мережне устаткування кожного окремого абонента,

апаратура мережного адаптера при топології «шина» виходить складніше, ніж при інших топологіях. Однак через широке поширення мереж з топологією «шина» (Ethernet, Arcnet) вартість мережного устаткування виходить не занадто високою.

Залежно від властивостей та функцій мережевого обладнання одна й та ж сама фізична топологія може ставати зовсім іншою логічною топологією.

Комутатор (світч) – пристрій, призначений для з'єднання вузлів мережі у межах одного або декількох сегментів. Світч використовує другий рівень моделі OSI. Вхідний пакет, що надходить до комутатора, буде переданим тільки одержувачу, що підвищує безпеку, а також продуктивність на відміну від концентратора. Принцип роботи полягає в зберіганні таблиці комутації, в якій міститься список відповідностей MAC-адрес вузлів до портів комутатора. Комутатор реалізує топологію логіної зірки.

Маршрутизатор (роутер) – пристрій, що служить для зв'язку різних мереж. Роутер працює на третьому рівні мережевої моделі OSI і для доставки пакетів використовує типологію мережі і правила задані адміністратором. Маршрутизатор може виконувати трансляцію адрес одержувача і відправника. Також може здійснювати фільтрацію потоку пакетів для обмеження або шифрування чи дешифрування даних. Важливою відмінністю між мережами, що використовують комутатори і маршрутизатори, є те, що мережі з комутаторами не блокують радіопередачі. В результаті комутатори можуть бути зіпсовані потоками пакетів радіопередач. Маршрутизатори блокують радіопередачі по локальній мережі, таким чином, потік радіопередач зачіпає тільки той домен, з якого він виходить.

Мости – пристрої мережі, які з'єднують два окремих сегмента, обмежених своєю фізичною довжиною, і передають трафік між ними. Мости також можуть підсилювати і конвертувати сигнали.

Порівняльні характеристики топологій

Топологія «Зірка»

Переваги:

– висока швидкодія мережі, так як загальна продуктивність мережі залежить тільки від продуктивності центрального вузла;

– легкість підключення нового вузла;

– при виході з ладу одного з вузлів мережі, це не позначиться на роботі мережі в цілому;

– відсутність зіткнення переданих даних, так як дані між робочою станцією і центральним вузлом передаються по окремому каналу, не зачіпаючи інші комп'ютери;

– висока продуктивність і зручність адміністрування;

– легкість знаходження несправності в мережі.

Недоліки:

– вартість реалізації, в якій має бути центральний вузол та більша ніж у шинній топології кількість кабелю;

– відмова центрального вузла призводить до відмови працездатності мережі;

– обмежена кількість з’єднань з центральним вузлом, яка залежить від кількості роз’ємів.

Топологія «Кільце»

Переваги:

– контроль процесу доставки даних адресату;

– ефективне пересилання повідомлень, тому що можна відправляти кілька повідомлень один за одним по кільцю;

– легкість відстеження вузлів, що некоректно працюють;

– протяжність мережі може бути значною, тобто комп'ютери можуть підключатися один до одного на значних відстанях, без використання спеціальних підсилювачів сигналу.

Недоліки:

– при великій кількості клієнтів швидкість роботи в мережі сповільнюється, так як вся інформація проходить через кожний вузол;

– низька надійність мережі, оскільки відмова будь-якого вузла тягне за собою відмову всієї системи;

– для підключення нового клієнта необхідно відключити роботу мережі.

Топологія «Шина»

Переваги:

– вся інформація знаходиться в мережі і доступна кожному комп'ютеру;

– низька вартість реалізації, простота налаштувань і установки;

– робочі станції можна підключати незалежно одну від одного, тобто при підключенні нового абонента немає необхідності зупиняти передачу інформації в мережі;

– втрата працездатності одного з пристроїв не позначається на працездатності мережі.

Недоліки:

– низька безпека, тому що інформація на кожному комп'ютері може бути доступна з будь-якого іншого комп'ютера;

– низька швидкість передачі даних;

– будь-який дефект кабелю або якого-небудь з численних роз'ємів повністю паралізує всю мережу;

– важко визначити дефекти з'єднань;

– швидкодія мережі залежить від числа підключених комп'ютерів (чим більше комп'ютерів підключено до мережі, тим повільніше йде передача інформації від одного комп'ютера до іншого).

Коміркова топологія

Переваги:

– розрив кабелю не відбивається на працездатності мережі;

– ефективніша порівняно з повнозв’язною, так як безпосередньо зв'язуються тільки ті вузли, між якими відбувається інтенсивний обмін даними.

Недоліки:

– великі витрати кабелю.

Топологія «Дерево»

Переваги:

– ієрархічна структура;

– мережа може розташовуватись на великих відстанях;

– легкість відстеження мережевих зв’язків.

Недоліки:

– при великих обсягах передачі даних між несуміжними вузлами топологія недостатньо ефективна, тому що потрібно проходити через проміжні ланки.

Для своєї мережі я обираю топологію зірка та комірчата.

При виборі типу кабелю враховують наступні їх характеристики:

– вартість установки і подальшого обслуговування;

– швидкість передачі даних;

– максимальна дальність передачі інформації, тобто відстань, на якій гарантується якісний зв'язок без застосування спеціальних підсилювачів-повторювачів (репітерів);

– безпеку передачі даних, у тому числі перешкодозахищеність.

Типи кабелів

Основна складність при виборі відповідного типу кабелю полягає в тому, що важко одночасно забезпечити найкращі значення всіх вищеперелічених характеристик кабелю.

Вита пара (TP - Twisted Pair) - це кабель, виконаний у вигляді скрученої

пари проводів. Він може бути екранованим і неекранованим.

Екранований кабель більш стійкий до електромагнітних перешкод. Вита пара найкращим чином підходить для малих установ. Недоліками даного кабелю є високий коефіцієнт загасання сигналу і висока чутливість до електромагнітних перешкод, тому максимальна відстань між активними пристроями в локальної обчислювальної мережі (ЛОМ) при використанні витої пари повинно бути не більше 100 м.

Коаксіальний кабель складається з одного цільного або крученого центрального провідника, який оточений шаром діелектрика.

Провідний шар алюмінієвої фольги, металевого обплетення або їх комбінації оточує діелектрик і служить одночасно як екран проти наведень.

Загальний ізолюючий шар утворює зовнішню оболонку кабелю.

Коаксіальний кабель може використовуватися у двох різних системах передачі даних: без модуляції сигналу і з модуляцією.

У першому випадку цифровий сигнал використовується в такому вигляді, в якому він надходить з ПК, і відразу ж передається по кабелю на приймну станцію. Кабель має один канал передачі зі швидкістю до 10 Мбіт/с і максимальний радіус дії 4000 м.

У другому випадку цифровий сигнал перетворюють в аналоговий і направляють його на прийомну станцію, де він знову перетворюється на цифровий.

Операція перетворення сигналу виконується модемом; кожна станція повинна мати свій модем. Цей спосіб передачі є багатоканальним (забезпечує передачу по десяткам каналів, використовуючи для цього всього лише один кабель). Таким способом можна передавати звуки, відеосигнали та інші дані. Довжина кабелю може досягати 50 км.

Оптоволоконний кабель є більш новою технологією, використовуваної в мережах.

Носієм інформації є світловий промінь, який модулюється мережею і

приймає форму сигналу. Така система стійка до зовнішніх електричних перешкод, і, таким чином, можлива дуже швидка, секретна і безпомилкова передача даних зі швидкістю до 40 Гбіт / с.

Кількість каналів в таких кабелях величезне.

Передача даних виконується тільки в симплексному режимі (передача і прийом даних можливі черзі в кожному з двох напрямків), тому для організації обміну даними пристрою необхідно з'єднувати двома оптичними волокнами (на практиці оптоволоконний кабель завжди має парне, парне кількість волокон). До недоліків оптоволоконного кабелю можна віднести велику вартість, а також складність під'єднання.

Типи ліній зв'язку представлені на рисунку 2.2.

Коаксіальний кабель

Кручена пара

Оптоволоконний кабель

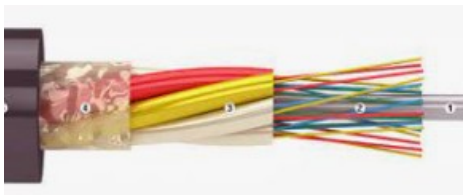


Рисунок 2.2 - Типи кабелів комп’ютерних мереж

Радіохвилі використовуються як передавальної середовища в бездротових локальних мережах або для зв'язку між локальними мережами.

У першому випадку максимальна відстань між станціями складає 200-300 м, у другому - це відстань прямої видимості. Швидкість передачі даних - до 2 Мбіт / с.

Бездротові локальні мережі вважаються перспективним напрямком розвитку комп'ютерних мереж. Їх перевага - простота і мобільність.

Також зникають проблеми, пов'язані з прокладкою і монтажем кабельних з'єднань, - досить встановити інтерфейсні плати на робочі станції, і мережа готова до роботи.

Порівняльні характеристики ліній зв'язку представлені в таблиці 2.1.

Таблиця 2.1 - Порівняльні характеристики ліній зв'язку

Тип лінії зв'язку	Швидкість, Мбіт / с	Завадостійкість
1	2	3
Радіохвилі	До 2	Низька
Коаксіальний кабель	До 10	Висока
Кручена пара	10-100	Низька
Оптоволоконний кабель	Більше 200	Найкраща

Для нашої мережі, на основі таблиці 2.1 я обираю кабель вита пара 5Е.

Отже, після вибору топології мережі, вибору кабелів варто описати яким чином буде створена логічна структура мережі.

В мережі використано шість шістнадцятипортових комутаторів, котрі є некерованими.

Від них протягнуті лінки до головного комутатора, котрий є комутатором 3 рівня.

Така схема дає можливість утворити робочі групи, котрі будуть не залежними одна від одної оскільки будуть поділені на Vlan-и.

До комутатора під'єднаємо лінк на точку доступу, включимо її в окремий Vlan.

Все описане відображено в таблицях 2.2. та 2.3.

Таблиця 2.2 – Логічна адресація в мережі

Позначення вузлів	Робоча група/ Кількість вузлів		Назва кабінету	Номер VLAN	Адреса підмережі/ Маска
1	2	3	4	5	6
WS_1—WS_2	MENEJERS	2	Керівник та його заступник	10	192.168.10.0/24
WS_3—WS_7	MENEJERS	5	менеджери	10	192.168.10.0/24
WS_8-WS_11, PR_1	MENEJERS	4	менеджери	10	192.168.10.0/24
WS_12—WS_17	MENEJERS	8	менеджер3	10	192.168.10.0/24
WS_18—WS_22, PR_2	MENEJERS	5	конференц-зал	10	192.168.10.0/24
WS_23—WS_25, PR_3, S_2	BUCH	3	бухгалтерія	30	192.168.30.0/24
WS_26	MENEJERS	1	охорона	10	192.168.10.0/24
S_1	MENEJERS		Технічний відділ	10	192.168.10.0/24
Ap_1	MENEJERS		Конференц приміщення	20	192.168.20.0/24

Таблиця 2.3 - Таблиця конфігурування VLAN

№ п/п	Познач. вузла	Номер порту	Тип порту	Назва мереж. пр-ю	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
2	SW_4	10	Провайдер інтернет				
3	SW_4	12	Access	S_1	-	Access	-
4	SW_4	1	Access	SW_1	16	Access	10
5	SW_4	2	Access	SW_2	16	Access	10
6	SW_4	3	Access	SW_3	16	Access	10
7	SW_4	4	Access	SW_5	16	Access	10
8	SW_4	5	Access	SW_6	16	Access	10
9	SW_4	6	Access	SW_7	16	Access	30
	SW_4	10	Access	WS_26		Access	10
18	SW_4	12	Access	AP_1	WAN	Access	20

2.2 Обґрунтування вибору комунікаційного обладнання

У комп'ютерній мережі передбачено використання головного комутатора. Для створення надійної та відмовостійкої мережі, для можливості керування мережею, її захисту ми повинні обрати комутатор третього рівня. Виробників на даний час є багато, а також їх асортимент надто широкий, є можливість в одному пристрої об'єднати кілька пристроїв, тому проведемо вибір комутатора.

Пристрій 1:

Planet GS-4210-24P2S

Вартість - 20 500,00 грн.

Тип - Керований комутатор

Кількість портів - 24

Швидкість портів - 10/100/1000T 802.3at PoE + 2-а порта 100/1000X SFP

Керування - Layer 2/2+

Пристрій 2:

Код продукту RB1100x4

Архітектура ARM 32 біт

Порти 13 шт

Швидкість портів 100\1000 Ethernet

Вартість 9500 грн

Пристрій 3:

Назва EdgeRouter 12 (ER-12)

Вартість 10000 грн

Порти Gigabit Ethernet: 10 x 10/100/1000Mbps

Порти SFP: 2 x 100/1000 Mbps

Підтримка PoE: PoE In

Якщо глянути на приведені вище моделі, то на мою думку варто обрати виріб фірми Mikrotik RB1100x4 (див. рис. 2.3). Даний комутатор поєднує в собі ще і маршрутизатор, VPN, фаєрвол та багато чого ще.

Даний маршрутизатор оснащено 13 гігабітними портами Ethernet, що працюють на базі процесора Annapurna Alpine AL21400 із чотирма ядрами Cortex A15, що працюють на частоті 1,4 ГГц кожне, для максимальної пропускної здатності до 7,5 Гбіт. Пристрій підтримує апаратне прискорення IPsec (до 2,2 Гбіт/с з AES128).

Пристрій поставляється з корпусом для монтажу в стійку 1U, послідовним портом RS232 і подвійними резервними джерелами живлення (з -48 В постійного струму для телекомунікаційного живлення та підтримкою 802.3at/

af).

RB1100AHx4 обладнаний двома вбудованими блоками живлення на 100-240 V та роз'ємом для під'єднання зовнішнього блока живлення постійного струму 12-57 V, що дуже зручно для користувача, оскільки дозволяє застосовувати різні схеми резервування живлення.

Порти 11 та 12 підтримують функцію байпас (bypass), що дає можливість на апаратному рівні здійснювати резервування ядра мережної інфраструктури. Таким чином, навіть у разі відмови маршрутизатора або відсутності живлення, функціонал байпас автоматично скомутує все на інший порт, який можна з'єднати з резервним пристроєм.

Рисунок 2.3 – Зовнішній вигляд комутатора Mikrotik RB1100x4

У комп’ютерній мережі необхідно використати шість шістнадцятипортових комутаторів.

Для вибору комутатора складемо порівняльну таблицю популярних комутаторів.

Таблиця 2.4 – Порівняльна характеристика шістнадцятипортових комутаторів

Марка	Cisco CBS110-16T-EU	TP-LINK TL-SG1016PE	Netgear JGS516v2
1	2	3	4
тип	Некерований	Некерований	Некерований

Продовження таблиці 2.4

1	2	3	4
Порти	16 портів 10/100/1000 Мбіт/ сек	16 x RJ45 10/100/1000 Мбіт/ сек	16 x Gigabit Ethernet (10/100/1000 Мбит/
Підтримка PoE	Нема	є	Нема
Габарити і вага	279 x 170 x 44 мм, 0.97 кг	294 x 180 x 44 мм, 2.2 кг	1328 x 169 x 43 мм 1.47 кг
Гарантія	60 місяців	60 місяців	12 місяців
Ціна, грн	5900 грн	5999 грн	4900 грн

Виходячи з таблиці 2.4, враховуючи співвідношення ціни до технічних характеристик пристрою для мережі вибрано комутатор Cisco CBS110-16T-EU, зовнішній вигляд якого зображено на рисунку 2.4.

Рисунок 2.4 – Зовнішній вигляд комутатора Cisco CBS110-16T-EU

У мережі використовується безпровідна точка доступу. На сучасному ринку представлено дуже багато моделей пристроїв різних виробників, але ми

для мережі вибрали безпровідну точку доступу MikroTik cAP AC RBcAPGi-5acD2nD, зовнішній вигляд якої зображено на рисунку 2.4. Основний критерій вибору саме такої точки — можливість працювати в парі з головним комутатором в плані організації керованої безпровідної мережі. Її вартість — 2600 грн. Зовнішній вигляд показаний на рисунку 2.5.

Рисунок 2.5 – Зовнішній вигляд безпровідної точки доступу MikroTik cAP AC RBcAPGi-5acD2nD

В точку доступу cAP 2nD закладений функціонал для підтримки стандарту 802.11b / g / n. Подача живлення відбувається по PoE.

Ідеально підходить для CAPsMAN, спеціальної системи з управління керованими точками доступу, що виконує функції на будь-якому пристрої RouterBOARD в мережі. З такою точкою доступу вам не потрібно шукати ПО і тим більше немає необхідності в окремому ПК.

У комп'ютерній мережі передбачено використання серверного комп'ютера.

Він має бути встановлений в стійці чи комутаційній шафі, і виконувати роль WEB сервера.

Сервер ARTLINE Business R37 v32 має мінімальне споживання енергії

і високу продуктивність.

Сервер ARTLINE Business стане надійним фундаментом у виконанні офісних та виробничих завдань, він втілює в себе: надійність, довговічність, продуктивність, економічність, простоту експлуатації.

Ретельно підібрана конфігурація ARTLINE Business R37v32 містить:

– Форм-фактор заввишки 2U, який дав змогу зібрати цю модель у досить компактному корпусі. Розташування компонентів усередині R37v32 оптимізоване під охолодження під час встановлення в серверну шафу або відкриту стійку — це дуже зручно та може бути суттєвою перевагою для максимально зручної інтеграції в корпоративну структуру. У результаті, сервер легко встановити, під'єднати й обслуговувати упродовж усього терміну експлуатації.

– Сучасний серверний процесор Intel Xeon E-2388G з 8 фізичними ядрами та 16 потоками (наявність Intel Hyper-Threading — додаткова перевага для максимально швидкого виконання завдань у багатопотокових програмах), що має чудову продуктивність, енергоефективність та безпечність. Завдяки вбудованим фірмовим технологіям (Intel Turbo Boost, Intel VT-x, Intel vPro, Enhanced Intel SpeedStep і іншим) ця апаратна платформа дає змогу розгорнути кілька віртуальних серверів; має набір функцій безпеки, стійкість проти шкідливого ПЗ і захист конфіденційних даних; дає змогу інтелектуально моніторити й керувати навантаженням для оптимального розподілу ресурсів у конкретний момент часу. Ну й може похвалитися привабливою ціною на одиницю потужності.

– Материнська серверна плата P12R-M від виробника ASUS. Компанія ASUS є лідером на ринку материнських плат упродовж багатьох років, а це означає, що ця плата забезпечить гарантовано тривалий термін експлуатації сервера ARTLINE. З особливостей: технологія Intel Platform Firmware Resilience (Intel PFR) для забезпечення відмови стійкості мікропрограм і запобігання доступу хакерів до інфраструктури, підтримка

Trusted Platform Module 2.0 (TPM 2.0) для захисту обладнання за допомогою вбудованих криптографічних ключів з регулярним оновленням прошивки для усунення уразливостей

– Декілька накопичувачів SSD, що мають запас міцності навіть в експлуатації за постійного навантаження.

– Встановлений блок живлення потужністю 600 Вт гарантує безпроблемну роботу сервера довгі роки.

Однією з особливостей сервера ARTLINE Business R37v32 є рішення для організації віддаленої роботи за стандартом IPMI 2.0. Віддалене під'єднання через локальну мережу через Ethernet-інтерфейс (технологія KVM-over-IP) дає змогу уникнути прямої присутності адміністратора безпосередньо поруч з апаратною та програмною частиною сервера — це допомагає неабияк знизити операційні витрати. Програмна оболонка забезпечує необхідний контроль та відстеження цілої низки параметрів (показників напруги силових ланцюгів, температурних датчиків, роботи системи охолодження, під'єднаної периферії тощо).). Зручний вебінтерфейс працює незалежно від операційної системи сервера, що дає змогу організувати периферійний контроль роботи останнього: ввімкнення/вимикання, моніторинг апаратних елементів, інсталяція ОС, налаштування, оновлення, відеозапис, реєстрація критичних помилок із веденням журналу логування.

Характеристики серверного ПК ARTLINE

Материнська плата P12R-M

Форм-фактор 2U Rackmount

Тактова частота процесора 3.2 ГГц

Характеристики оперативної пам'яті ECC DDR4-3200 МГц

Кількість ЦП в комплекті 1

Кількість БЖ в комплекті 1

Кількість дискових накопичувачів в комплекті 4

Процесор Восьмиядерний Intel Xeon E-2388G (3.2 – 5.1 ГГц)

Обсяг встановленої оперативної пам'яті 128 ГБ

Жорсткий диск SSD: 2 x 500 ГБ, SSD: 2 x 1 ТБ

Корпус 2U Rackmount

Контролер віддаленого доступу ASMB10-iKVM

Кількість LAN (RJ-45) 3

Швидкість LAN 1 Гбіт/с

Гарантія 38 місяців

Тип дискових систем SSD

Сокет LGA 1200

Типи підтримуваних ОЗП DDR4 UDIMM

Максимальна кількість дискових слотів

Вартість 99 000 грн

Зовнішній вигляд зображено на рисунку 2.6.

Рисунок 2.6 – Зовнішній вигляд ARTLINE Business R37v32

Зведемо все вибране нами обладнання в одну таблицю 2.5.

Таблиця 2.5 — Перелік обладнання мережі

№ п.п	назва	Кількість	ціна
1	2	3	4
1	комутатор Cisco CBS110-16T-EU	6	5900,00 грн.
2	комутатор Mikrotik RB1100x4	1	9500,00 грн.
3	точка доступу MikroTik cAP AC RBcAPGi-5acD2nD	1	2600,00 грн.
4	Сервер ARTLINE Business R37v32	1	99 000,00 грн.
5	Комутаційна шафа	1	16860,00 грн.
6	Кабель мережевий	4	3 400,00 грн.
7	Короб 20x40x2000	45	69,00 грн.

2.3 Особливості монтажу мережі

Найбільш поширеним середовищем передачі даних в структурованих кабельних системах (СКС) залишається кабель з мідними провідниками. Хоча в магістральних каналах першого і другого рівня все частіше використовують оптоволоконні кабелі, здатні забезпечити великі швидкості передачі даних.

Від того, наскільки правильно в ході монтажу СКС були протягнуті і закріплені кабелі, багато в чому залежать стабільність, швидкість і довговічність роботи системи.

Загальні вимоги до прокладення і кріплення кабелів викладаються в стандартах монтажу СКС, таких як ISO/IEC IS 11801 або ГОСТ Р 53246.

Дуже важливо, щоб кабельні траси проходили на достатньому видаленні від джерел електромагнітних завад.

До джерел електромагнітних завад відносяться силова електропроводка, трансформаторне устаткування, великі електродвигуни або електро-

генератори, радіопередавачі і потужна копіювальна техніка. Ще на етапі проектування необхідно врахувати взаємне місце розташування телекомунікаційних кабелів і джерел перешкод.

Проте на практиці далеко не завжди вдається дотримати достатню відстань. В цьому випадку використовуються захищені і екрановані кабелі або екрановані короби і кабель-каналы.

Для зниження дії електромагнітних завад кабельні канали, по яких прокладаються телекомунікаційні кабелі, в процесі монтажу СКС необхідно заземляти. Це відноситься до усіх типів металевих кабельних трас, як екранованих, так і звичайних.

Нерідко кабелі СКС прокладаються паралельно силовим кабелям електроживлення :

В цьому випадку слід дотримувати мінімальну відстань, яка залежить від потужності силового кабелю. Стандарт EIA/TIA 569 визначає цю відстань в 127 мм для кабелів до 2 кВт, не менше 305 мм - від силового кабелю 2-5 кВт, і не менше 610 мм - від кабелів більше 5 кВт. Якщо телекомунікаційний кабель розміщений в заземленому металевому кабельному каналі, то ця відстань зменшується удвічі. Якщо в заземлених металевих кабельних каналах розташовуються і силовий, і телекомунікаційний кабелі, то вимоги до мінімальної відстані знижуються в чотири рази.

Кабельні траси при монтажі СКС бажано не прокладати впритул до труб і радіаторів системи опалювання, а також інших нагрівальних приладів.

При монтажі кабелів необхідно уникати утворення механічної напруги, яка може утворитися в результаті скручування, натягнення або занадто різкого вигину кабелю.

Мінімальний радіус вигину кабелю визначений в стандартах монтажу СКС.

Слід зазначити, що ця вимога істотно розрізняється для кабелів:

- складових магістральну,

- горизонтальну підсистеми СКС

- для комутаційних

- апаратних шнурів

При цьому існує обмеження, що якщо у виробника кабелю жорсткіші вимоги до мінімального кута повороту, то слід застосовувати їх. Ситуація з менш жорсткими вимогами не розглядається, тому при розбіжності вимог стандарту і виробника кабелю рекомендується використовувати строгіші. Кабельні траси різних типів повинні мати спеціалізовані пристосування, які перешкоджають перегину і перекрученню кабелів як в процесі монтажу СКС, так і в ході експлуатації.

Кабель в процесі монтажу СКС, а також в процесі експлуатації може випробовувати механічні навантаження, при цьому необхідно, щоб вони не перевищували максимально допустимої сили натягнення. Інакше цілісність і працездатність кабелю можуть бути порушена.

Максимально допустима сила натягнення залежить від типу кабелю і зазвичай встановлюється виробником. Стандарт висуває вимогу тільки відносно чотирипарних кабелів на основі витої пари усіх типів, для них максимальне натягнення встановлене в 110 Н.

В обов'язковому порядку при монтажі СКС слід залишати запас кабелю в телекомунікаційних приміщеннях.

Для телекомунікаційної, апаратної і міського застосування стандарт рекомендує залишати не менше трьох метрів кабелю витої пари. На робочому місці, біля розетки RJ - 45, також необхідно залишати запас в 30 см

Це необхідно для того, щоб була можливість здійснити перестановку устаткування без необхідності міняти кабель цілком. Крім того, запас кабелю може знадобитися при необхідності ремонту, наприклад, в результаті обриву кабелю або ушкодження модульної розетки.

При укладанні запасів кабелю слід віддавати перевагу U -подібним петлям або бухтам у вигляді цифри 8 з великим радіусом кіл. Дуже небажане

укладання витої пари в бухти з невеликим діаметром кілець, оскільки кабель, укладений таким чином, стає джерелом сильних електромагнітних завад.

Для кріплення кабелю і формування його в бухти широко використовуються: різного роду хомути, бандажі, стяжки.

Хомути при монтажі СКС використовуються не лише для фіксації кабелю в лотках і кабельних каналах, але і для кріплення окремих кабелів і пучків на стіні при прокладенні відкритим способом або на приладові стійки.

Стандарти вимагають, щоб після затягування хомута він зберігав рухливість і в подовжньому і поперечному напрямі. Подібна вимога пояснюється прагненням уникнути передавлювання і деформації кабелю в процесі монтажу СКС.

Один з досить поширених способів кріплення відкритої проводки, широко використовуваний при прокладенні силових кабелів і телефонії, це застосування скоб і спеціалізованих степлерів. На практиці вони нерідко застосовуються і для кріплення витої пари при монтажі СКС. При цьому використання скоб для кріплення телекомунікаційних кабелів усіх типів вітчизняний стандарт категорично не рекомендує.

Суворе дотримання правил прокладення кабелів багато в чому визначає якість монтажу СКС в цілому.

Кабелі мережі будуть проведені попід стелею, понад підвісною стелею. Спуски виконані в порожнинах гіпсокартону.

2.4 Тестування мережі [25]

Протягом кількох років більшість питань підвищення продуктивності та надійність мереж вирішувалося закупівлею нової техніки.

Не завжди подібне рішення було технічно та економічно обґрунтовано, але майже завжди воно дозволяло досягти бажаної мети - мережа починала працювати швидше та краще. За наявності 200% запасу пропускної спромож-

ності практично всі "вузькі місця" можна легко "розширити", а купуючи тільки найдорожче обладнання лідерів мережевих технологій, ви можете з великим ступенем ймовірності убезпечити себе від "прихованих дефектів".

Сьогодні ситуація змінилася, та економічне обґрунтування проектів з модернізації мереж стає актуальним. Світовий досвід показує, що інвестиції у професіоналізм фахівців дають більшу віддачу, ніж інвестиції в "залізо", навіть дуже гарне. Необхідну пропускну здатність мережі чи її надійність не можна оцінити без детального аналізу її поточного стану. Це можна зробити тільки за допомогою діагностичних засобів та методів тестування комп'ютерних мереж.

Діагностичні засоби, призначені для комп'ютерних мереж, можна класифікувати за двом основним ознакам:

– засіб призначений для діагностики мережі або для тестування мережі;

– засіб призначений для реактивної діагностики або попереджувальної діагностики.

Під діагностикою мережі прийнято розуміти вимірювання характеристик роботи мережі у процесі її експлуатації (без зупинення роботи операторів).

Діагностикою мережі є, зокрема, вимір числа помилок передачі даних, ступеня завантаження (утилізації) ресурсів мережі чи часу реакції прикладного ПЗ, яку адміністратор мережі повинен здійснювати щоденно.

Діагностика буває двох типів: попереджувальна (proactive) та реактивна (reactive).

Випереджальна діагностика повинна проводитись у процесі експлуатації мережі щодня, основна ціль попереджувальної діагностики - запобігання збоям у роботи мережі. Реактивна діагностика виконується, коли в мережі вже стався збій і треба швидко локалізувати джерело та виявити причину.

Для того, щоб перевірити відповідність якості кабельної системи вимо-

гам стандартів, визначити максимальну пропускну здатність мережі або оцінити час реакції прикладного програмного забезпечення (ПЗ) при зміни параметрів налаштування комутатора або операційної системи (ОС), то такі виміри можна зробити лише за відсутності в мережі працюючих користувачів. В цьому випадку правильно вживати термін "тестування" мережі.

Таким чином, тестування мережі – це процес активної дії на мережу з метою перевірки її працездатності та визначення потенційних можливостей щодо передачі мережевого трафіку.

Тестування можна умовно поділити на кілька видів в залежності від мети, заради якою воно проводиться. Це:

– тестування кабельної системи мережі на відповідність стандартам TIA/EIA TSB-67;

– стресове тестування конкретних мережевих пристроїв з метою перевірки стійкості їх роботи за різних рівнів навантажень та різних типах мережевого трафіку;

– тестування ПЗ, зокрема визначення його вимог до пропускної спроможності мережевих ресурсів (до характеристик каналу зв'язку, сервера та т. п.);

– стресове тестування мережі (конкретних мережевих конфігурацій) з метою виявлення "прихованих дефектів" в обладнанні та "вузьких місць" в архітектурі мережі, а також з метою визначення порогових значень трафіку, допустимих у даній мережі.

Тестування прикладного програмного забезпечення з метою визначення вимог до пропускної спроможності мережевих ресурсів проводять компанії-розробники ПЗ. Таке тестування здійснюється в рамках комплексної перевірки ПЗ перед випуском його на ринок і називається тестуванням на відповідність якості (Quality Assurance Test, QAT)

Стресове тестування мережевих пристроїв зазвичай проводиться незалежними спеціалізованими лабораторіями. Прикладами таких лабораторій

є організації LANQuest та Data Communications. Найчастіше стресове тестування пристроїв проводиться з метою перевірки заявлених технічних характеристик та виявлення різноманітних дефектів.

Кошти, призначені для діагностики мереж, можна умовно розділити на дві категорії залежно від принципу їх роботи: засоби моніторингу та управління роботою мережі (далі засоби моніторингу — monitoring software) та аналізатори мережевих протоколів (далі аналізатори протоколів — analyzers). Принцип роботи засобів моніторингу заснований на взаємодії консолі оператора з так званими агентами, які, власне, займаються моніторингом та управлінням роботою пристроїв мережі.

Прикладами засобів моніторингу є програми Transcend компанії 3Com, Optivity компанії Bay Networks (нині Nortel), HP OpenView Net Metrix. Агенти можуть бути вбудовані в обладнання або завантажені програмним чином. Оскільки найпоширенішим протоколом спілкування консолі оператора та агентів є SNMP, такі агенти часто називають SNMP-агентами. SNMPагенти можуть виконувати різні функції в залежності від типу баз керуючої інформації (Management Information Base, MIB), які вони підтримують. Ці функції можуть включати управління конфігурацією пристрою, в яке агенти вбудовані (configuration management), управління контролем доступу до інформації (security management), аналіз продуктивності пристрою (perfomance management), вимірювання числа помилок при передачі даних (fault management) та інші. При реактивній діагностиці мережі за допомогою засобів моніторингу вимірювальним приладом є SNMP-агент самого пристрою, що діагностується. Однак у разі збоїв показання SNMP-агента не можна вважати достовірними. Це особливо актуально, коли збої відбуваються у пристрої з встановленим SNMP-агентом. У таких випадках спостерігач повинен бути "незалежним" від діагностованого пристрою. SNMP-агент пристрою спостерігає за колізійним доменом мережі завжди тільки з однієї точки і, що особливо важливо для реактивної діагностики, не має змоги генерувати

тестовий трафік. В результаті, якщо не все обладнання має вбудовані агенти, то частина помилок канального рівня в домені мережі може не фіксуватися. З погляду реактивної діагностики, т. е. можливості швидкої локалізації дефектів у мережі, застосування аналізаторів мережевих протоколів виявляється кращим. Вони є значно більш потужний засіб у порівнянні із засобами моніторингу мережі, оскільки позбавлені всіх перерахованих вище недоліків. Саме можливість ефективного проведення реактивної діагностики є сьогодні актуальним завданням для адміністраторів мереж. Принцип роботи аналізатора протоколів відрізняється від принципу роботи засобу моніторингу мережі. Аналізатор мережевих протоколів досліджує весь мережний трафік, що проходить повз нього.

Локальні мережі за своєю природою є широкомовними, тобто кожен кадр від будь-якої станції межах колізійного домену бачать все станції цього домену мережі. Підключаючи аналізатор до будь-якої точки колізійного домену мережі, ви будете бачити весь трафік у цьому домену. Аналізатори протоколів надають можливість збирати дані про роботу протоколів всіх рівнів мережі та, як правило, здатні проводити генерацію тестового трафіку в мережу. Маючи великий буфер для збору пакетів, аналізатори протоколів дозволяють швидко локалізувати причину збою в мережі: наприклад, виявити факт перевантаження конкретного сервера, безслідне зникнення пакетів транспортного рівня на несправних мережних платах, комутаторах та маршрутизаторах, IP-пакети з неправильною контрольною сумою, дублікати IPадрес багато іншого.

Аналізатори протоколів можна розділити на дві категорії: програмні та апаратні (або програмно-апаратні).

Програмний аналізатор – це програма, яка встановлюється на комп'ютер із звичайною мережевою платою. Аналізатор протоколів переводить мережну плату комп'ютера режим прийому всіх пакетів (promiscous mode).

Прикладами програмних аналізаторів протоколів є Observer та Distributed Observer компанії Network Instruments, NetXray компанії Network Associates, LANalyzer for Windows компанії Novell та багато інших. Використання всіляких методів тестування та діагностування комп'ютерних мереж дозволяє своєчасно виявити помилки в роботі мережі, що дозволить значно підвищити ефективність роботи комп'ютерних мереж, а також збільшити експлуатаційний строк.

2.5 Захист комп’ютерної мережі

Безпека мережі — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів. Мережева безпека включає в себе дозвіл на доступ до даних в мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ID і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформації і програм у рамках своїх повноважень. Мережева безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами. Мережі можуть бути приватними, такими як всередині компанії або відкритими, для публічного доступу. Мережева безпека бере участь в організаціях, підприємствах та інших типів закладів. Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю.

Мережева безпека починається з аутентифікації, що зазвичай включає в себе ім'я користувача і пароль. Коли для цього потрібно тільки одна деталь аутентифікації (ім'я користувача), то це називають однофакторною аутентифікацією. При двофакторній аутентифікації, користувач ще повинен використати маркер безпеки або 'ключ', кредитну картку або мобільний телефон, при трьохфакторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.

Після перевірки дійсності, брандмауер забезпечує доступ до послуг користувачам мережі. Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (IPS).

Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційність.

Система безпеки мережі не ґрунтується на одному методі, а використовує комплекс засобів захисту. Навіть якщо частина обладнання виходить з ладу, решта продовжує захищати дані Вашої компанії від можливих атак.

Встановлення рівнів безпеки мережі надає Вам можливість доступу до цінної ділової інформації з будь-якого місця, де є доступ до мережі Інтернет, а також захищає її від загроз.

Система безпеки мережі:

– Захищає від внутрішніх та зовнішніх мережних атак. Небезпека, що загрожує підприємству, може мати як внутрішнє, так і зовнішнє походження. Ефективна система безпеки стежить за активністю в мережі, сигналізує про аномалії та реагує відповідним чином.

– Забезпечує конфіденційність обміну інформацією з будь-якого місця та в будь-який час. Працівники можуть увійти до мережі, працюючи вдома або в дорозі, та бути впевненими у захисті передачі інформації.

– Контролює доступ до інформації, ідентифікуючи користувачів та їхні системи. Ви маєте можливість встановлювати власні правила доступу

до даних. Доступ може надаватися залежно від ідентифікаційної інформації користувача, робочих функцій, а також за іншими важливими критеріями.

– Забезпечує надійність системи. Технології безпеки дозволяють системі запобігти як вже відомим атакам, так і новим небезпечним вторгненням. Працівники, замовники та ділові партнери можуть бути впевненими у надійному захисті їхньої інформації.

Засоби захисту комп’ютерних мереж:

Брандмауери. Централізовані брандмауери та брандмауери окремих комп’ютерів можуть запобігати проникненню зловмисного мережного трафіку до мережі, яка підтримує діяльність компанії.

Антивірусні засоби.

Більш захищена мережа може виявляти загрози, що створюють віруси, хробаки та інше зловмисне програмне забезпечення, і боротися з ним попереджувальними методами, перш ніж вони зможуть заподіяти шкоду.

Знаряддя, які відстежують стан мережі, грають важливу роль під час визначення мережних загроз.

Захищений віддалений доступ і обмін даними.

Безпечний доступ для всіх типів клієнтів із використанням різноманітних механізмів доступу грає важливу роль для забезпечення доступу користувачів до потрібних даних, незалежно від їх місцезнаходження та використовуваних пристроїв.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція з інсталяції програмного забезпечення серверів та активного комутаційного обладнання

Налаштування маршрутизатора Mikrotik RB1100x4

називаємо роутер

```
system identity set name=router-sw4
```

Позначимо фізичні порти по тим мережам, яким вони належать. Позначимо маркуванням lan фізичні порти, які будуть належати мережі підприємства, а маркуванням wifi фізичні порти, які будуть належати мережі (класу С).

```
interface ethernet set [ find default-name=ether1 ] name=ether1-lan
interface ethernet set [ find default-name=ether2 ] name=ether2-lan
interface ethernet set [ find default-name=ether3 ] name=ether3-lan
interface ethernet set [ find default-name=ether4 ] name=ether4-lan
interface ethernet set [ find default-name=ether5 ] name=ether5-lan
interface ethernet set [ find default-name=ether6 ] name=ether6-lan
interface ethernet set [ find default-name=ether7 ] name=ether7-lan
interface ethernet set [ find default-name=ether8 ] name=ether8-lan
interface ethernet set [ find default-name=ether9 ] name=ether9-lan
interface ethernet set [ find default-name=ether10 ] name=ether10-wan
interface ethernet set [ find default-name=ether11 ] name=ether11-lan
interface ethernet set [ find default-name=ether12 ] name=ether12-lan
interface ethernet set [ find default-name=ether13 ] name=ether13-lan

interface ethernet set [ find default-name=sfp-sfpplus1 ] disabled=yes
interface ethernet set [ find default-name=sfp-sfpplus2 ] disabled=yes
```

Створимо віртуальні інтерфейси у вкладці bridge, для об'єднання LAN портів.

```
interface bridge add name=br1-lan
interface bridge add name=br10-lan
interface bridge add name=br20-lan
interface bridge add name=br30-lan
```

Призначаємо LAN порти маршрутизатора віртуальним інтерфейсам (bridge) відповідно до таблиці 2.4.

```
interface bridge port add bridge=br10-lan interface=ether2-lan
interface bridge port add bridge=br10-lan interface=ether3-lan
interface bridge port add bridge=br10-lan interface=ether4-lan
interface bridge port add bridge=br10-lan interface=ether5-lan
interface bridge port add bridge=br10-lan interface=ether6-lan
interface bridge port add bridge=br30-lan interface=ether7-lan
interface bridge port add bridge=br10-lan interface=ether8-lan
interface bridge port add bridge=br10-lan interface=ether9-lan

interface bridge port add bridge=br10-lan interface=ether11-lan
interface bridge port add bridge=br20-lan interface=ether12-lan
```

Призначаємо мережі віртуальним інтерфейсам

```
ip address add address=192.168.10.1/24 interface=br10-lan network=192.168.10.0
ip address add address=192.168.20.1/24 interface=br20-lan network=192.168.20.0
ip address add address=192.168.30.1/24 interface=br30-lan network=192.168.30.0
ip address add address=192.168.1.1/24 interface=br1-lan network=192.168.1.0

ip address add address=15.16.17.0/0 interface=ether10-wan network=15.16.17.0
```

Налаштуємо пул адрес мережі wi-fi, налаштуємо dhcp

```
ip pool add name=pool-wifi ranges=192.168.20.50-192.168.20.220

ip dhcp-server add address-pool=pool-wifi disabled=no interface=br20-wifi name=dhcp-wifi

ip dhcp-server network add address=192.168.20.0/24 dns-server=8.8.8.8,8.8.4.4 domain=wifi.local gateway=192.168.20.1
```

Включимо NAT, щоб пристрої, що знаходяться в мережах мали вихід в

інтернет.

```
ip firewall nat add action=masquerade chain=srcnat out-interface=ether1-wan src-address=192.168.0.0/24
ip firewall nat add action=masquerade chain=srcnat out-interface=ether1-wan src-address=192.168.1.0/24
```

Ізолюємо підмережі, щоб пристрої з мережі 192.168.10.0/24 не бачили і не використовували пристрої, що знаходяться в мережі 192.168.20.0/24.

```
ip firewall filter add action=drop chain=forward disabled=yes dst-address=192.168.10.0/24 in-interface=br1-lan
```

3.2 Налаштування точки доступу

Для створення мережі WI-FI настроїмо контролер capsman. Перед цим необхідно налаштувати та активувати wireless-cm2.

Щоб активувати функцію контролера бездротової мережі, переходим до розділу CAPsMAN, натискаємо на Менеджер і ставимо галочку Enabled.

Отже ми включимо контролер контроллер управління точками доступу. До нього можна підключити окремі Wi-Fi точки які отримують з нього настройки.

Кожна підключена точка доступу формує віртуальний інтерфейс wifi на контроллері. Це дозволяє стандартними засобами керувати трафіком на контроллері.

Набори налаштувань на контролері можуть бути об'єднані в іменовані конфігурації. Це дозволяє легко контролювати і призначати різні конфігурації різними точками.

Наприклад, можна створити групу з глобальними настройками для всіх точок доступу, але при цьому окремим точкам можна задавати додаткові налаштування, які будуть перезаписувати глобальні.

Після підключення керованої точки до мережі, всі локальні бездротові

настройки на клієнті перестають діяти. Вони заменяються настройками capsman v2.

Створюємо новий радіоканал та вказуємо його параметри. Переходимо на вкладку Канали, натискаємо на плюсик і вказуємо параметри. (див. рис. 3.1)

На рисунку 3.1 позначено:

Name	Ім'я каналу
Frequency	Частота частота в МГц, вона же номер канала
Width	полоса в MHz
Band	режим роботи
Extension Channel	настройки extension channel
Tx. Power	Потужність сигналу в Dbm

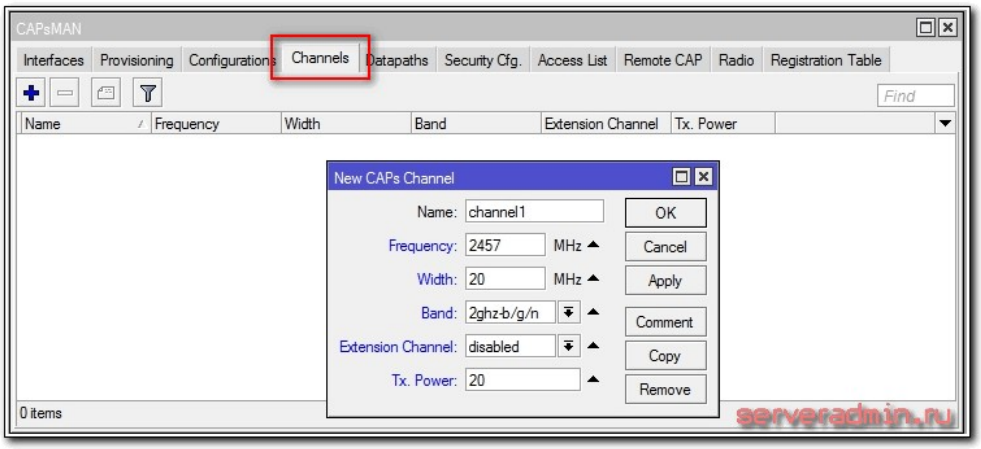


Рисунок 3.1 – Створюємо новий радіоканал та вказуємо його параметри

Переходимо на вкладку Datapaths. Натискаємо плюсик і задаємо параметри. (див. рис. 3.2)

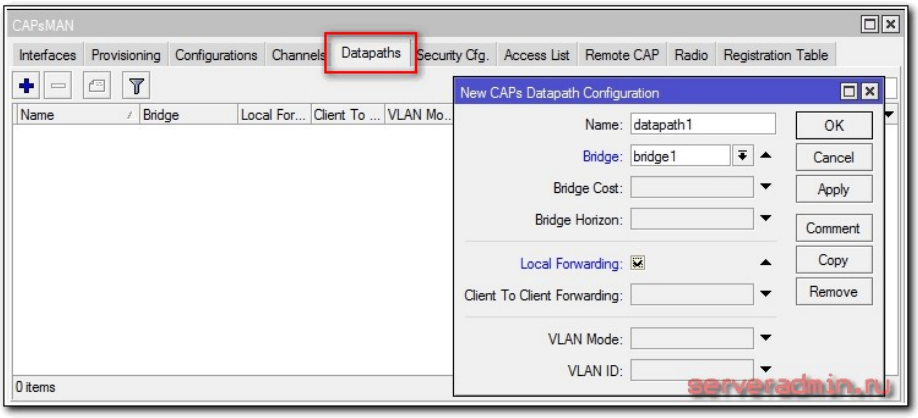


Рисунок 3.2 – Створюємо новий Datapaths

На рисунку 3.2 позначено:

Bridge	в який бридж буде додано інтерфейс як порт
Bridge Cost	значення bridge port cost, використовується тільки якщо актвний параметр bridge
Bridge Horizon	значення bridge horizon, , використовується тільки якщо актвний параметр bridge
Local Forwarding	Керування параметром режиму переадресації
Client To Client Forwarding	Керує параметром client-to-client forwarding між клієнтами керує точкою доступу, якщо активний параметр local-forwarding , цим параметром керує сама точка доступу, в іншому випадку - контроллер
Vlan Mode	Керує призначенням VLAN tag для інтерфейсу
Vlan Id	який VLAN ID буде призначено інтерфейсу, якщо vlan-mode встановлено в use tag

Переходимо до налаштувань безпеки. Відкриваємо вкладку Security Cfg. І натискаємо плюсик. (див. рис. 3.3)

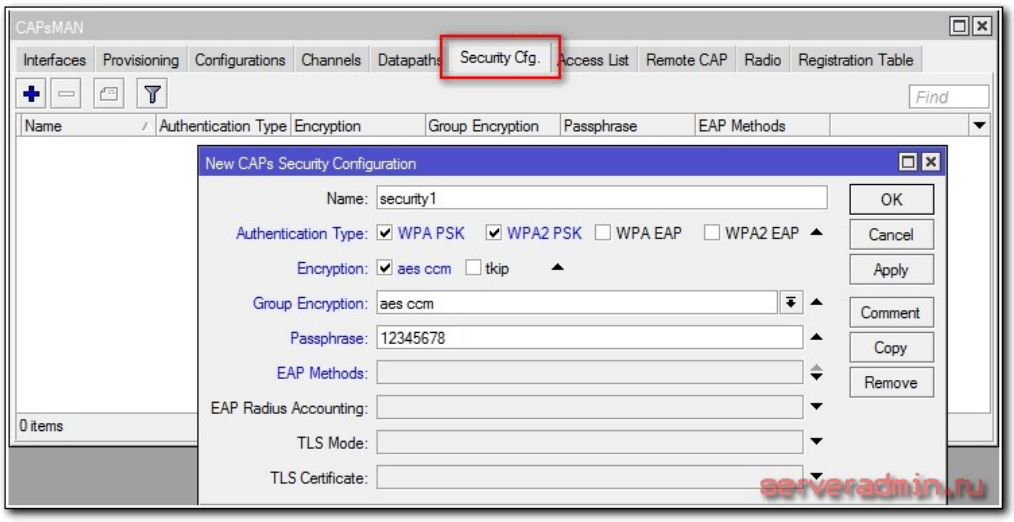


Рисунок 3.3 – Налаштовуємо параметр безпеки

На рисунку 3.3 позначено:

name	ім'я конфігурації
Authentication type	Вибір типу авторизації
Encryption	вибір алгоритму unicast encryption
Group Encryption	вибір алгоритму group encryption
Passphrase	WPA or WPA2 pre-shared key
Eap Methods	Вибір типу авторизації
Eap Radius Accounting	використання авторизації Radius
TLS Mode	Керування використанням сертифікату
TLS Certificate	Вибір сертифікату, якщо його використання активоване в попередньому параметрі

З’єднуємо всі налаштування в єдине. Таких конфігурацій може бути декілька з різними настройками.

Перехдимо на вкладку Configurations и плюсик.(див. Рис. 3.4)

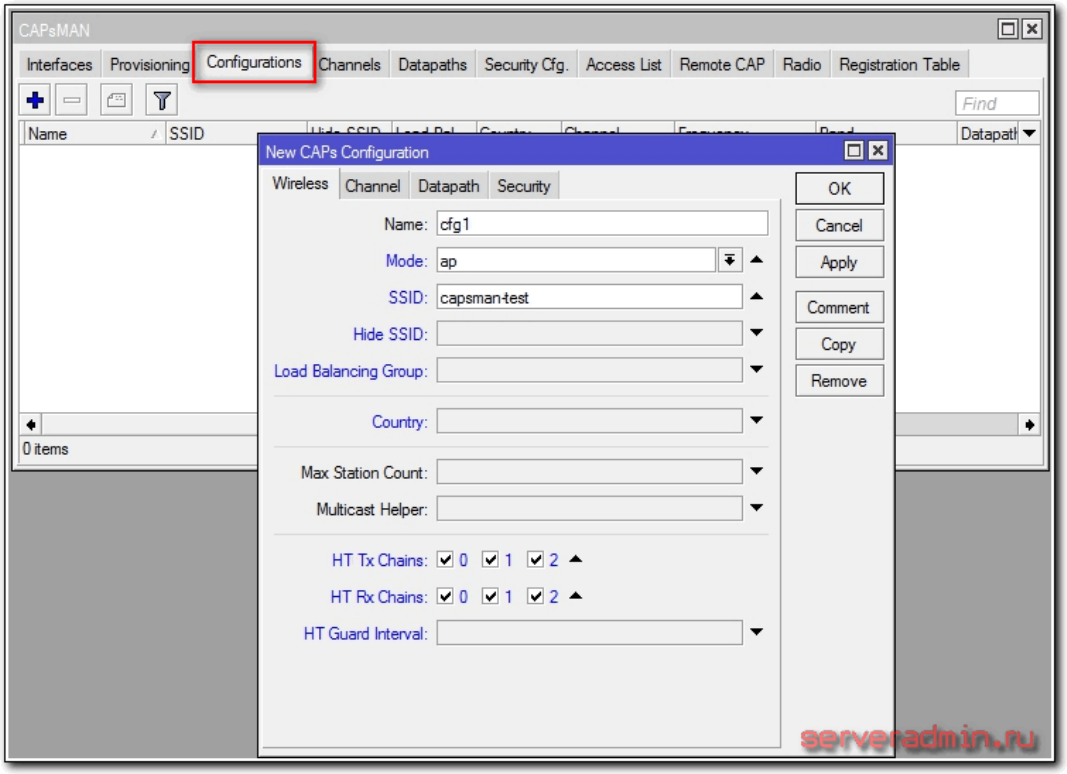


Рисунок 3.4 – Об’єднання конгфігурацій

На першій вкладці Wireless вказуємо ім’я конгфігурації, режим ap і ім’я SSID майбутньої бесшовної Wi-Fi мережі.

На інших вкладках просто вибираємо створені раніше налаштування.

Основні настройки mikrotik контроллера capsman v2 закінчені.

Тепер потрібно створити правила розповсюдження цих налаштувань.

Переходимо на вкладку Provisioning і плюсик (див. рис. 3.5).

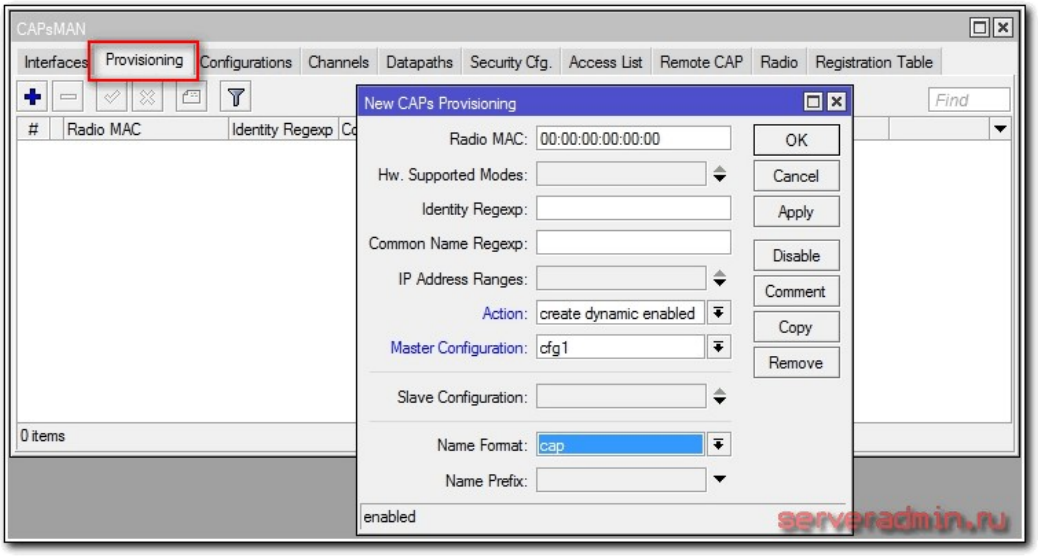


Рисунок 3.5 – Створення правил розповсюдження цих налаштувань

На цьому налаштуванні контролера capsman v2 завершено, можна підключити wifi точку доступу до нього.

3.3 Початкове налаштування сервера Ubuntu 20.04 [26]

На сервері S_1 будуть встановлені Linux сервіси, тому ми опишемо налаштування даної ОС, яка попередньо вже встановлена на ньому.

Після встановлення операційної системи необхідно виконати ряд важливих кроків у конфігурації в рамках базових налаштувань. Ці кроки допомагають підвищити рівень безпеки та полегшити роботу з сервером і послужити надійною основою для наступних дій.

Крок 1 — Вхід з привілегіями root

Щоб увійти на сервер, вам потрібно знати публічну IP-адресу вашого сервера . Також вам потрібен пароль або, якщо ви встановили ключ SSH для аутентифікації, приватний ключ для облікового запису користувача root .

Якщо ви ще не підключилися до сервера, зробіть вхід в систему як користувач root , використовуючи наступну команду:

ssh root@your_server_ip

Зверніть увагу на автентичність хоста, якщо він з'явиться на екрані. Якщо ви використовуєте аутентифікацію за паролем, введіть пароль root для входу в систему. Якщо ви використовуєте ключ SSH із захистом за фразою-паролем, вам може бути запропоновано ввести фразу-пароль у перший раз під час використання ключа в кожному сеансі. Якщо ви перший раз виконуєте вхід на сервер за допомогою пароля, вам також можна запропонувати змінити пароль root .

Детальніше про root

root user — це користувач із правами адміністратора в середовищі Linux, який має дуже широкий набір привілеїв. Із-за такого широкого набору привілеїв облікового запису root *не рекомендується* використовувати її на регулярній основі. Це пов'язано з тим, що частина можливостей, отриманих за допомогою root , включає можливість внесення дуже руйнівних змін, навіть якщо це відбувається непередбачено.

У наступному кроці буде створено новий обліковий запис користувача з обмеженими привілеями для щоденного використання.

Крок 2 — Створення нового користувача.

Після входу в систему з правами root ми готові додати новий обліковий запис користувача. У майбутньому ми виконаємо вхід за допомогою цього нового облікового запису, а не з правами root .

adduser admin

Вам буде запропоновано відповісти на кілька питань, починаючи з пароля облікового запису.

Введіть надійний пароль і введіть за бажанням будь-яку додаткову інформацію. Це робити необов'язково, і можна натиснути ENTER в будь-якому полі, яке ви хочете пропустити.

Крок 3 — Надання адміністративних прав

Тепер у нас є новий обліковий запис користувача зі стандартними правами. Однак іноді може знадобитися виконання адміністративних завдань.

Щоб не здійснювати вихід із стандартного облікового запису та виконати вхід до системи з облікового запису root , ми налаштуємо так званого *суперкористувача* або додамо привілегії root для стандартного облікового запису. Це дозволить нашому звичайному користувачеві запускати команди з правами адміністратора, вказавши слово sudo перед кожною командою.

Щоб додати ці права для нового користувача, нам потрібно додати користувача в групу sudo . За замовчуванням в Ubuntu 20.04 користувачі, що входять до групи sudo , можуть використовувати команду sudo.

Використовуючи права root , запустіть цю команду, щоб додати нового користувача в групу sudo:

usermod -aG sudo admin

Тепер, коли ви ввійдете в систему зі стандартним користувачем, ви можете ввійти sudo перед командами для виконання дій з правами суперкористувача.

Крок 4 — Налаштування базового брандмауера

Сервери Ubuntu 20.04 можуть використовувати Brandmauer UFW для перевірки, щоб надати дозволи лише до певних служб. Ми можемо легко створити базовий брандмауер за допомогою додатків.

Рекомендовано використовувати тільки один брандмауер в один момент часу, щоб уникнути конфліктів, які можуть затруднити проведення відладки.

Додатки можуть зареєструвати свої профілі в UFW після встановлення. Ці профілі дозволяють UFW керувати цими додатками по імені. OpenSSH, служба, що дозволяє підключитися до нашого сервера зараз, має профіль, зареєстрований в UFW.

Щоб побачити це, можна ввести наступну команду:

ufw app list

Нам потрібно переконатися в тому, що брандмауер дозволяє підключення SSH, щоб ми могли зайти на сервер в наступний раз. Щоб відключити ці підключення, можна ввести наступне:

ufw allow OpenSSH

Після цього ми можемо активувати брандмауер за допомогою наступної команди:

ufw enable

Введіть YES, натисніть ENTER, щоб продовжити. Щоб побачити, що підключення SSH дозволено, введіть наступне:

ufw status

Оскільки брандмауер в даний час блокує всі підключення, крім SSH , якщо ви встановите і налаштуєте додаткові служби, потрібно змінити налаштування брандмауера, щоб дозволити вхідний трафік.

Крок 5 — Активація зовнішнього доступу для стандартного користувача.

Тепер, коли у нас є стандартний обліковий запис для щоденного використання, необхідно переконатися, що ми можемо ввести SSH безпосередньо в обліковий запис.

Процес налаштувань доступу SSH для нового користувача залежить від того, чи використовує обліковий запис із правами root пароль входу на сервер чи ключі SSH для автентифікації.

Якщо root використовує аутентифікацію за паролем:

Якщо ви заповнили вхід в обліковий запис root *за допомогою пароля* ,

тоді для SSH активована *аутентифікація* за паролем. Ви можете використовувати SSH для нового користувача, запустивши новий сеанс-термінал і використовуючи SSH з новим іменем:

ssh admin@your_server_ip

Після введення пароля для звичайного користувача можна виконати вхід. Якщо вам потрібно запустити команду з правами адміністратора, введіть sudo перед командою таким чином:

sudo command_to_run

Вам буде запропоновано використовувати пароль звичайного користувача під час використання sudo в перший раз для кожного сеансу (і періодично після цього).

Щоб підвищити рівень безпеки вашого сервера, ми обов’язково рекомендуємо встановити ключі SSH замість використання аутентифікації за паролем.

Якщо root використовує аутентифікацію за ключем SSH:

Якщо ви заповнили вхід в обліковий запис root за допомогою ключів SSH , тоді аутентифікація за паролем для SSH відключена . Вам потрібно додати копію локального відкритого ключа у файл ~/.ssh/authorized_keys нового користувача для успішного входу.

Якщо ваш відкритий ключ уже включено в кореневий ~/.ssh/ authorized_keys файл на сервері, ми можемо скопіювати структуру цього файлу та каталоги для нашого нового користувача в існуючому сеансі.

Самий простий спосіб копіювання файлів з правами володіння та дозволами — скористатися командою rsync. Вона копіюватиме директорію .ssh-користувача root , збереже дозволи та змінить файли власників, усе в одній команді. Обов'язково змініть виділені нижче частини відповідно до імені вашого стандартного користувача:

rsync --archive --chown=admin:admin ~/.ssh /home/admin

Тепер відкрийте новий сеанс-термінал на локальному комп'ютері та використовуйте SSH з новим іменем користувача:

ssh admin@your_server_ip

Ви повинні зайти в обліковий запис без використання пароля. Якщо вам потрібно запустити команду з правами адміністратора, введіть sudo перед командою таким чином:

sudo command_to_run

Тепер у вас є основа для вашого сервера. Ви можете перейти до установки програмного забезпечення, яка потрібна на вашому сервері.

3.4 Тестування мережі

Захист комп'ютерних мереж та тестування має дуже велике значення. Тому ми опишемо команди з допомогою яких можна протестувати мережу.

Синтаксис команди в операційних системах сімейства Windows має наступний вигляд:

ping [ключі] адреса (ім'я) вузла

Ключі:

– t – продовжує відправку запитів , доки робота не буде перервана командою Ctrl-C;

– a – дозволяє використовувати імена вузлів замість IP-адрес;

– n число – вказує кількість exo запитів для відправки ;

– l довжина – вказує довжину exo – запитів;

– f – забороняє фрагментування пакету, визначає, чи пристрій змінював розмір пакету;

– i час – встановлює час життя пакету (Time to Live -TTL) відправляємих пакетів;

– v тип – встановлює тип обслуговування (TOS)

– r число – відображає шляхи для заданого числа переприйомів;

– s число – відмічає час для вказаного числа переприйомів;

– j список вузлів – маршрутизація пакетів через вказані вузли. Послідовні вузли можуть бути розділені шлюзами;

– k список вузлів - маршрутизація пакетів через вказані вузли. Послідовні вузли не можуть бути розділені шлюзами.

– w час – встановлює час очікування відповіді в мілісекундах.

Команда TRACERT також використовує протокол ICMP для визначення всіх пристроїв, через які проходить пакет на шляху до вузла призначення. Приклад застосування команди зображено на рисунку 3.6.

За допомогою цієї команди, можна отримати досить обширну інформацію про те, як функціонує мережа.

Має наступний синтаксис :

tracert [ключі] ім’я вузла

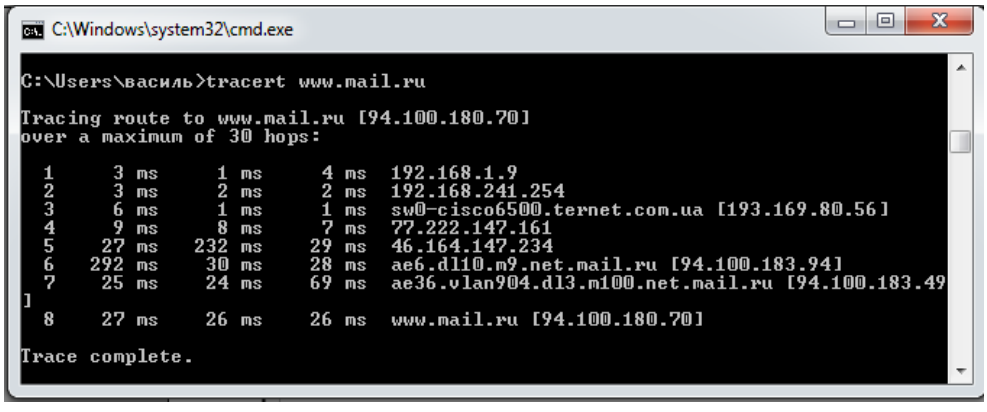


Рисунок 3.6 – Застосування команди TRACERT

Ключі :

– d – використовувати імена вузлів замість IP адрес;

3.5 Моделювання мережі

Cisco Packet Tracer є дуже зручним засобом моделювання мереж передачі даних. Дозволяє робити працездатні моделі мережі, налаштовувати (командами Cisco IOS) маршрутизатори і комутатори, взаємодіяти між декількома користувачами (через хмару). Успішно дозволяє створювати навіть складні макети мереж, перевіряти на працездатність топології. Однак, варто зауважити, що реалізована функціональність пристроїв обмежена і не надає всіх можливостей реального обладнання. Cisco Packet Tracer доступний безкоштовно для учасників Програми Мережевий Академії Cisco.

Інтерфейс (див.рис. 3.7)

Основне вікно програми складається з шести меню, 4 з яких використовуються найбільш часто. На малюнку відзначені найбільш часто використовувані меню програми Cisco Packet Tracer.

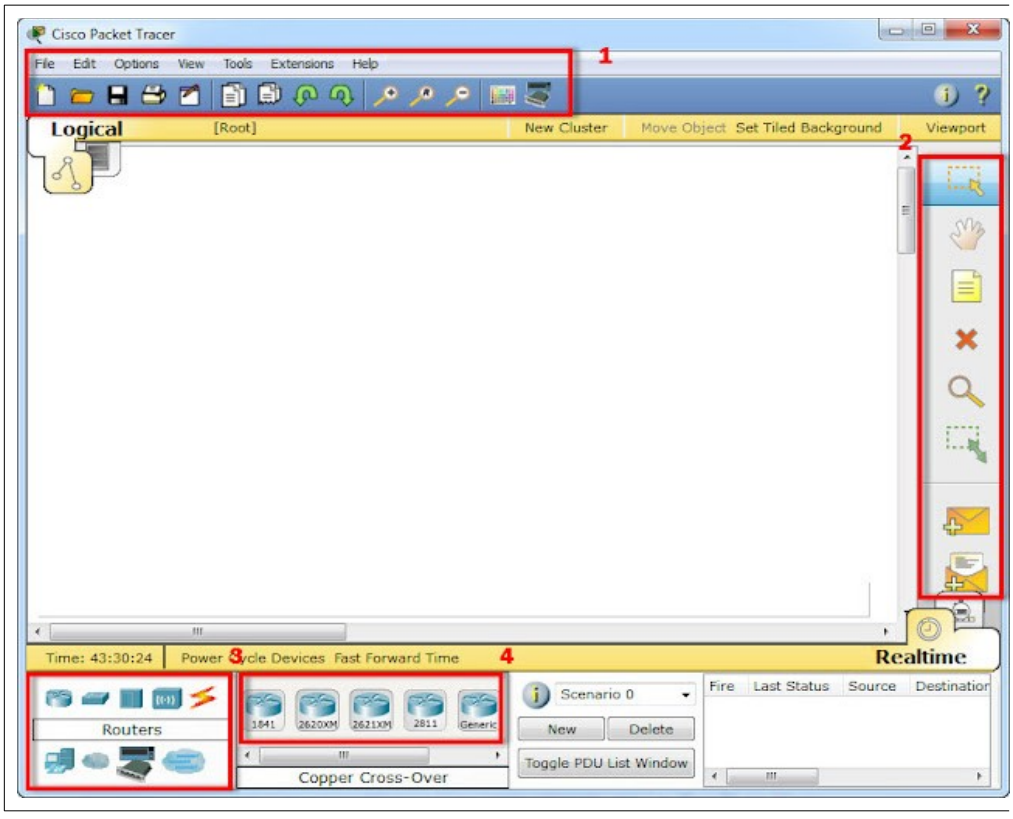


Рисунок 3.7 - Основне вікно програми Cisco Packet Tracer

Стандартне програмне меню (1) мало чим відрізняється від подібного меню в інших прорамах операційної системи Windows. Виняток становлять два інструменти на графічній панелі: Drawing Palette і Custom Device Dialog.

Праве графічне меню (див.рис. 3.8) (2) містить досить впізнавані піктограми інструментів для роботи з проектом і об'єктами проекту. Кожен з розташованих в даному меню інструментів активується кліком мишки на відповідній піктограмі, а також, для більш швидкого доступу, відповідної клавіші.

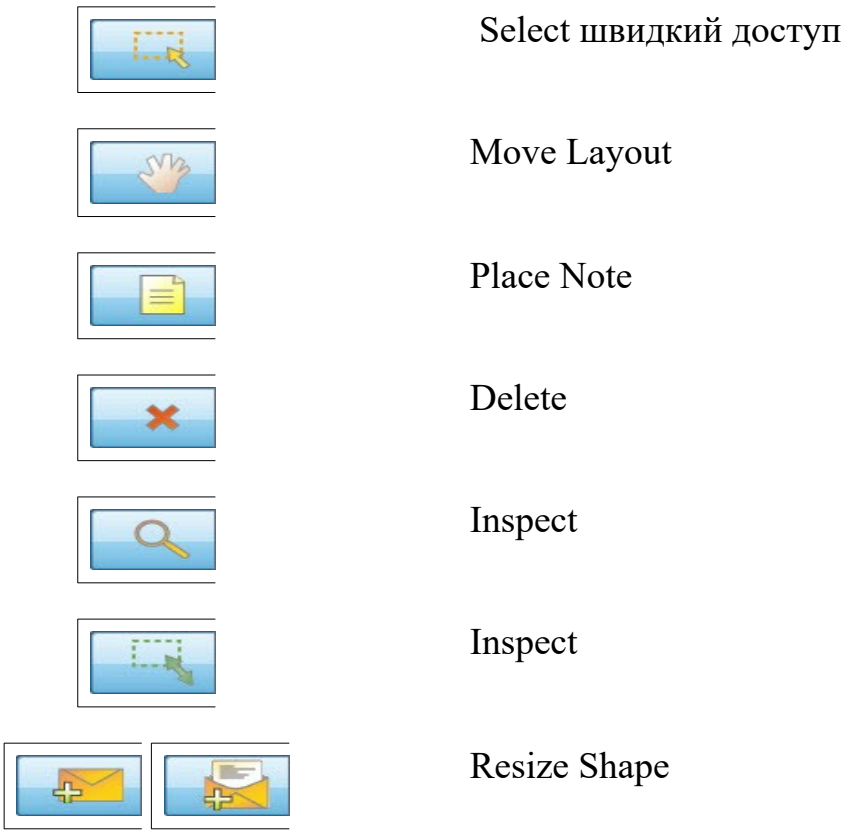


Рисунок 3.8 - Піктограми інструментів для роботи з проектом і об'єктами проекту

Перший інструмент меню (з верху в низ) Select (швидкий доступ - [Esc]).

Як і в більшості інших програм використовується для виділення одного або більше об'єктів. Як правило для подальшого переміщення, копіювання або

видалення.

Наступний інструмент даного графічного меню Move Layout ([M]) використовується для прокрутки більших проектів.

Незважаючи на те що основне вікно програми, що використовується для побудови проекту. має смуги прокрутки, наявність додаткового інструменту з подібною функцією, який активується натисненням однієї клавіші, може бути дуже зручним при роботі з великими топологіями.

Інструмент Place Note ([N]) додає підпис в будь-якій частині проекту. Зручно використовувати для коментарів або ж для розміщення основної інформації сценарію безпосередньо в проекті для подальшої роботи.

Інструмент Delete ([Del]) видаляє об'єкт або групу об'єктів.

Інструмент Inspect ([I]) не взираючи на зовнішній вигляд, що нагадує лупу, не використовується для збільшення об'єктів проекту.

Даний інструмент дозволяє, в залежності від типу пристрою, переглядати вміст таблиці ARP, таблиці маршрутизації, таблиці NAT і т.д.

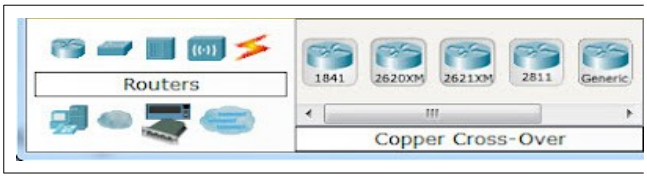
Постійно виключають з більшої частини описів інструмент Resize Shape ([Alt] + [R]) призначений для зміни розмірів мальованих об'єктів (чотирикутників і кіл).

Так як інструмент малювання не дуже зручний в Cisco Packet Tracer, то і Resize Shape мало ким використовується.

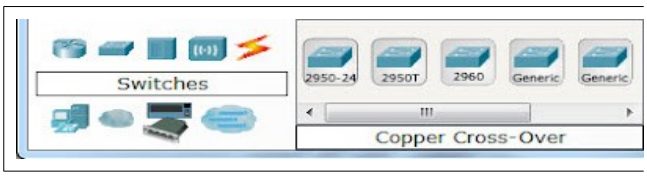
Знаходяться в самому низу даного меню інструменти Add Simple PDU ([P]) і Add Complex PDU ([C]) призначені для емуляції відправки з подальшим відстеженням довільного пакету даних всередині проекту.

Дана можливість сприяє кращому розумінню модельованих технологій. Відмінності двох даних інструментів полягають в більшій кількості можливих параметрів при використанні Add Complex PDU, в той час як Add Simple PDU дозволяє це зробити простіше і швидше.

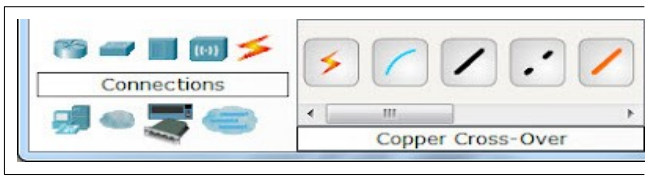
Меню 3 дозволяє вибрати тип пристроїв, а меню 4 безпосередньо сам пристрій. Найбільш використовуваними є (див.рис. 3.9):



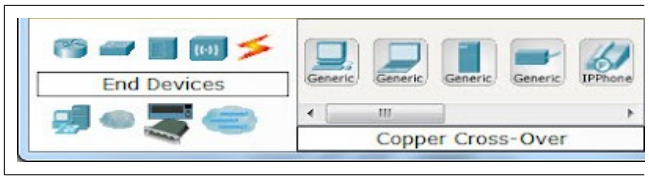
Routers



Switches



Connections



End devices

Рисунок 3.9 — Типи пристроїв для Cisco Packet Tracer

Routers - дозволяє додавати в проект маршрутизатори Cisco. В Cisco Packet Tracer 5.3.3 доступні Cisco 1841 Cisco 2820 XM, Cisco 2821 XM, Cisco 2811.

Switches - використовується для додавання комутаторів L2. Доступні наступні моделі Cisco Catalyst WS-C2950-24, Cisco Catalyst WS-C2950T-24, Cisco Catalyst WS-C2960-24TT

Connections - вибір типу підключення для об'єктів топології проекту.

End devices - вибір кінцевих пристроїв. Персональні комп'ютери, ле-птопи, IP-телефони.і сервера.

Додавання об'єктів топології проводиться прості перетягуванням. При з'єднанні різних пристроїв в єдину топологію, використовуючи Connections,

буде надаватися вибір фізичного порту підключення.

Для того щоб додати маршрутизатор в проект мережі, необхідно вибрати лівим кліком миші даний тип обладнання, також вибрати модель і додати в проект, клікнувши на робочому полі програми. Весь процес додавання нового юніта робиться в три кліка.

Після того як обладнання додано в проект, можна відкрити вікно параметрів даного пристрою яке надає можливість доступу до апаратної конфігурації даного юніта (див.рис. 3.10).

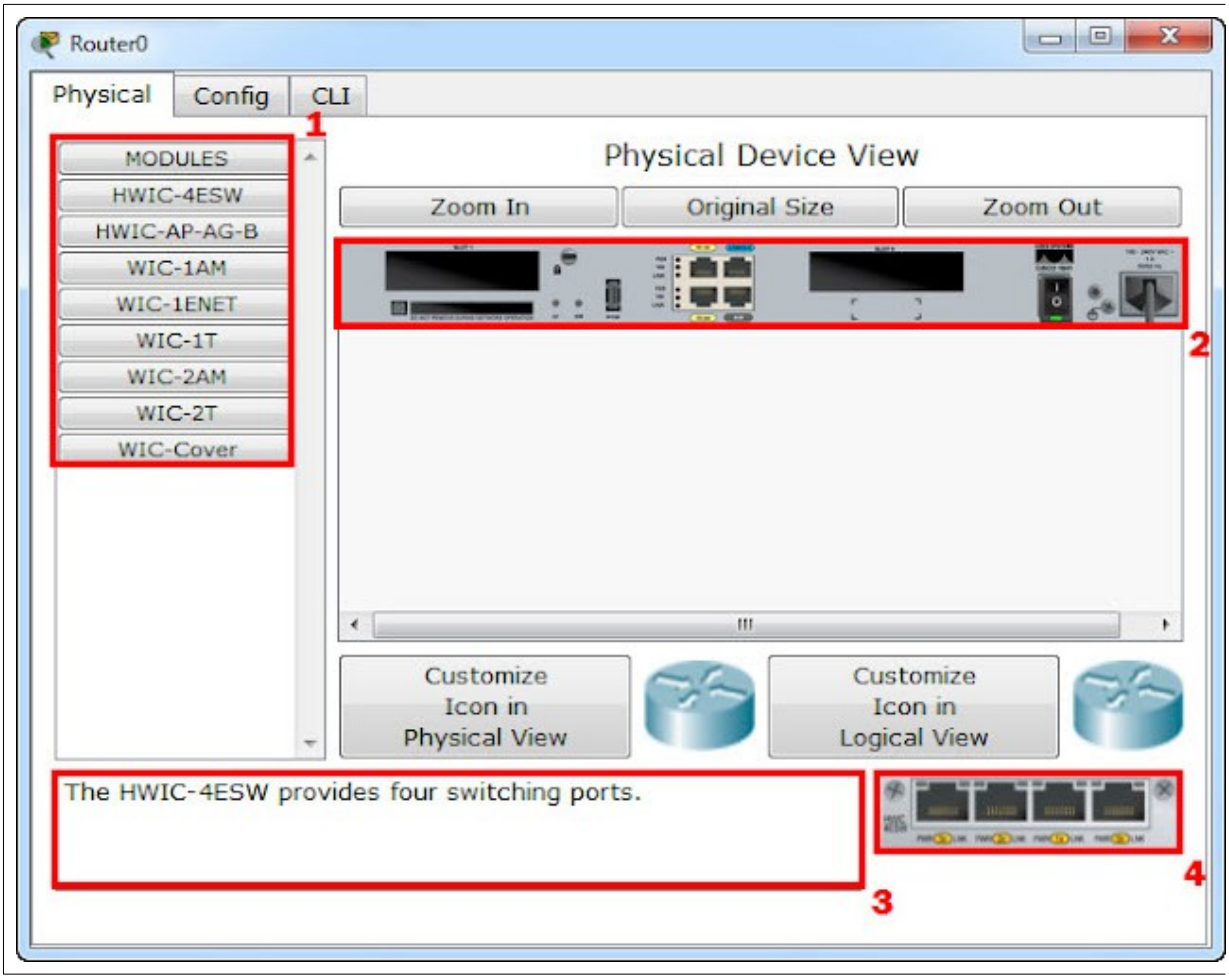


Рисунок 3.10 — Вікно параметрів пристрою Cisco Packet Tracer

У тих випадках, коли для виконання роботи потрібен, відсутній за замовчуванням, інтерфейс, дана вкладка дозволяє додати будь-який з доступних. Крім того, вільні слоти можуть бути закриті фальш панелями (WIC-

Cover). Будь-які операції по додаванню або видалення модулів проводяться тільки на вимкненому обладнання. У зв'язку з цим, віртуальне обладнання повинно бути відключено від мережі кнопкою живлення перед установкою або видаленням мережевого модуля.

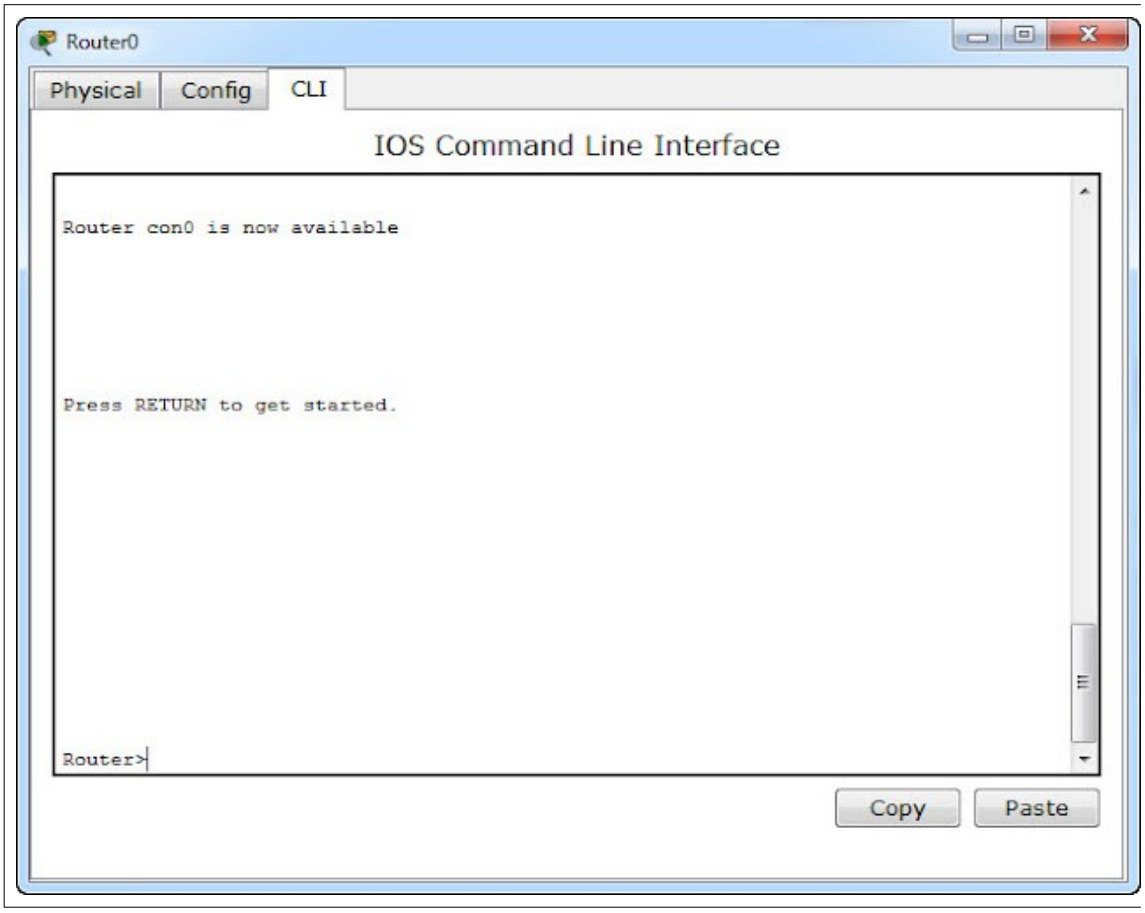


Рисунок 3.11 - Вкладка CLI Cisco Packet Tracer

Вкладка CLI надає доступ до консолі Console 0 маршрутизатора. За замовчуванням на доступ до консолі пароль не встановлено (див.рис. 3.11).

Кінцеві вузли мережі, такі як сервера, робочі станції додаються в топологію ідентично іншим пристроям проекту.

Параметри мережевих інтерфейсів для даного виду пристроїв встановлюються через меню на вкладці Config. Дана вкладка практично ідентична для перерахованих вище пристроїв (див.рис. 3.12).

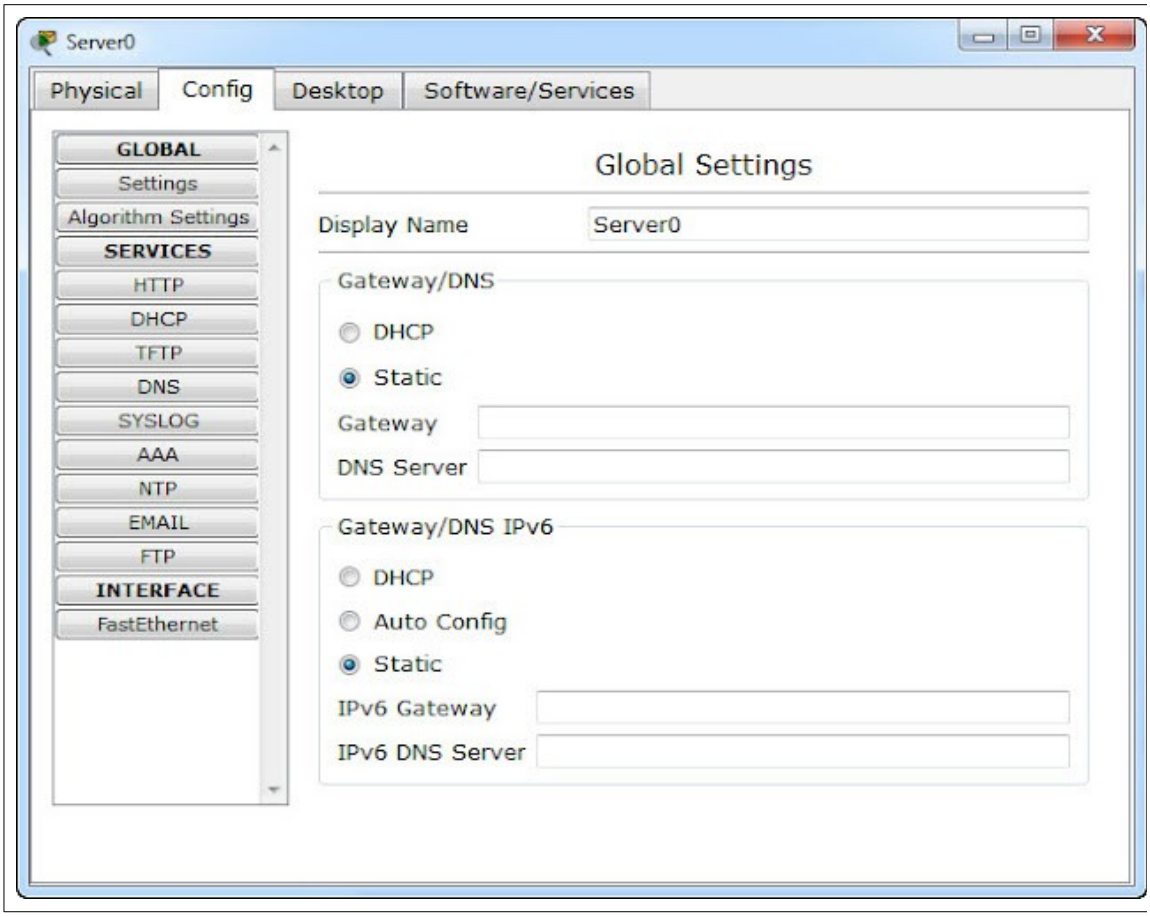


Рисунок 3.12 — Зміна параметрів мережі пристрою в Cisco Packet Tracer

Виняток становить наявність додаткових меню налаштування мережевих сервісів (HTTP, DHCP, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP) у пристрої сервіс. Дані сервіси далекі за своєю функціональністю від реальних, але забезпечують базову функціональність, необхідну для тестування.

Мережеві параметри вказуються в меню Settings і меню властивостей мережевого інтерфейсу (FastEthernet) вкладки Config.

Після того як всі необхідні для обраного сценарію роботи пристрою додані в проект, необхідно всі одиниці обладнання з'єднати між собою відповідно до сценарію. Для цього використовується меню Conenctions.

Вибір кабелю залежить від обладнання, що підключається і технології підключення. У цьому конкретному випадку це будет Copper Cross-Over. Ко-

жен раз при з'єднанні обладнання буде пропонуватися вибір інтерфейсу, якщо такі є в наявності і не беруть участь в іншому підключенні. В кінцевому підсумку виходить наступний проект мережі (див.рис. 3.13).

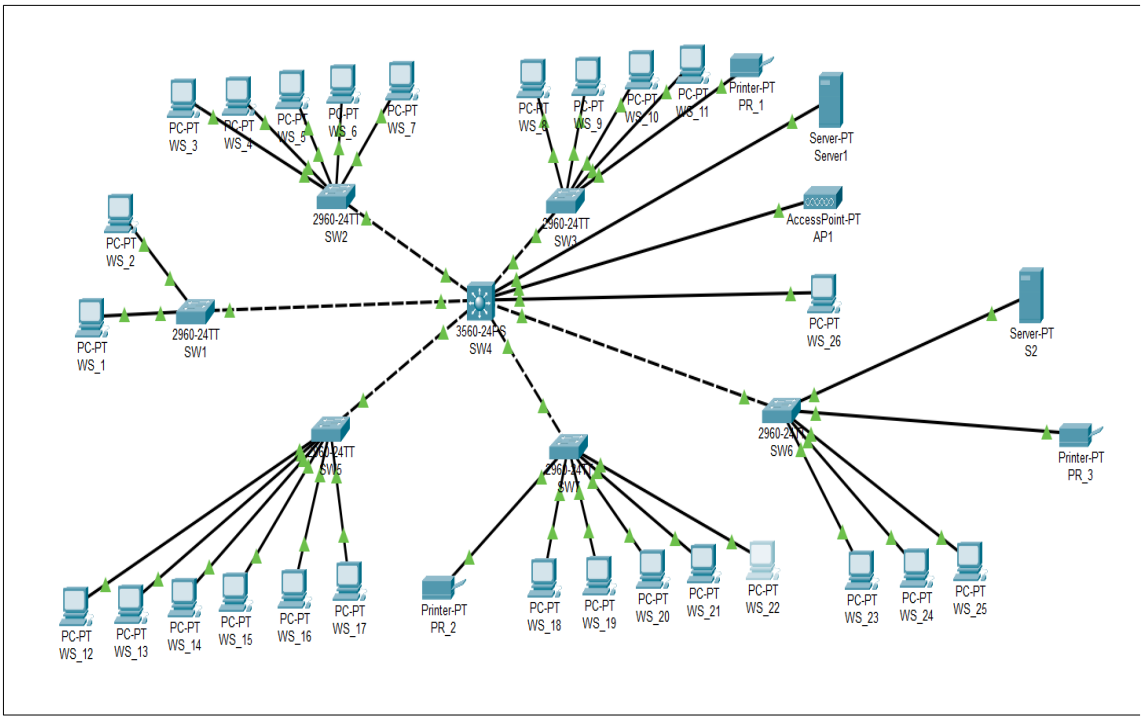


Рисунок 3.13 — Готовий проект в Cisco Packet Tracer

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини дипломного проекту є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп’ютерної мережі для ТОВ "ЕКС-простір" і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР дані витрат часу по окремих операціях технологічного процесу зводяться у таблицю 4.1.

Таблиця 4.1 - Середній час виконання НДР та стадій технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1	Розробка логічної та фізичної топологій мережі.	Керівник проекту	14
2	Монтаж кабельних каналів	Технік	30
3	Монтаж активного та пасивного мережевого обладнання	Технік	10
4	Тестування мережі. Моніторинг основних параметрів (кільк. переданих та прийнятих пакетів та їх тип).	Інженер	18

Продовження таблиці 4.1

1	2	3	4
5	Налагодження мережі та створення технічної документації	Інженер	10
Разом		-	82

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі складає 82 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Оплата праці - грошовий вираз вартості і ціни робочої сили, який виступає у формі будь-якого заробітку, виплаченого власником підприємства працівникові за виконану роботу.

Заробітна плата працівника залежить від кінцевих результатів роботи підприємства, регулюється податками і максимальними розмірами не обмежується.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців.

Основна заробітна плата розраховується за формулою:

$$Зосн.=Тс \cdot Кг , \quad (4.1)$$

де Тс – тарифна ставка, грн.;

Кг – кількість відпрацьованих годин.

Отже, основна заробітна плата для:

- керівника проекту: Зосн1 = 14· 80 = 1120,00 грн.
- інженера: Зосн2 = 28 · 70 = 1960,00 грн.
- техніка: Зосн3 = 40 · 60 = 2400,00 грн.

Сумарна основна заробітна плата становить:

Зосн = 1120,00 + 1960,00 + 2400,00 = 5480,00 грн

Додаткова заробітна плата становить 10-15 % від суми основної заробітної плати:

$$Здод.=Зосн. \cdot Кдопл , \quad (4.2)$$

де Кдопл. – коефіцієнт додаткових виплат працівникам: 0,1 – 0,15.

Отже, додаткова заробітна плата по категоріях працівників становить:

1. керівника проекту: Здод1= 1120,00 · 0,14 = 156,8 грн.
2. інженера: Здод2= 1960,00 · 0,14 = 274,4 грн.
3. техніка: Здод3= 2400,00 · 0,14 = 336,00 грн.

Загальна додаткова заробітна плата становить:

Здод = 156,8 + 274,4 + 336,00 = 767,2 грн.

Звідси загальні витрати на оплату праці (Во.п.) визначаються за формулою:

$$Во.п.=Зосн.+Здод , \quad (4.3)$$

Во.п = 5480,00 0 + 767,2= 6247,20 грн

Крім того, слід врахувати суму нарахування на заробітну плату:

- фонд страхування на випадок безробіття – 1,6 %;
- фонд по тимчасовій втраті працездатності – 1,4 %;
- пенсійний фонд – 33,2 %;

- внески на страхування від нещасного випадку на виробництві та професійного захворювання - 1,4%.

Загальна сума зазначених відрахувань становить 37,6 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = ФОП \cdot 0,376, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з.} = 6247,20 \cdot 0,376 = 8596,15 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додатк. заробл. плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. Ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	80	14	1120,00	156,8	-	-
2	Інженер	70	28	1960,00	274,4		
3	Технік	60	40	2400,00	336,00	-	-
Разом				5480,00	767,20	2348,95	8596,15

Отже, загальні витрати на оплату праці становлять 5678,48 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$MBi = qi \cdot pi \quad (4.5)$$

де qi – кількість витраченого матеріалу і-го виду;

pi – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$Зм.в. = \sum MBi \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. вим.	Факт. витрачено матеріалів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	Cisco CBS110-16T-EU	шт	6	5900,00	35400,00
2	Mikrotik RB1100x4	шт	1	9500,00	9500,00
3	MikroTik cAP AC RBcAPGi-5acD2nD	шт	1	2600,00	2600,00
4	Сервер ARTLINE	шт	1	99000,00	99000,00
5	Комутаційна шафа	шт	1	16860,00	16860,00
6	Кабель мережевий	шт	4	3 400,00	13600,00
7	Короб 20x40x2000	шт	45	69,00	3105,00
Разом					180065,00

Отже, загальна сума матеріальних витрат дорівнюють Зм.в = 180065,00 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$Зе=W \cdot T \cdot S, \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 14 годин, споживана потужність - 0,5 кВт/год, вартість електроенергії 6,50 грн.

Тому:

$Зе = 0,5 \cdot 14 \cdot 6,5 = 45,5$ грн.

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8 - 10 % від загальної суми матеріальних затрат:

$$Тв = Зм.в. \cdot 0,08...0,1, \quad (4.8)$$

де Тв – транспортні витрати.

Отже,

$Тв = 180065,00 \cdot 0,8 = 14405,20$ грн.

4.6 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі ви-

робництва є їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів.

Мінімально допустимі строки їх використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{100\%} \cdot T, \quad (4.9)$$

де А – амортизаційні відрахування за звітний період, грн.

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %;

Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 14 год., балансова вартість ПК – 99000,00 грн., тому:

А = 99000,00 · 0,04 /150 · 14 = 462,00 грн

4.7 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створення необхідних умов праці.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20 – 60 % від суми

основної та додаткової заробітної плати працівників.

$$Нв = Во.п. \cdot 0,2...0,6, \quad (4.10)$$

де Нв – накладні витрати.

Нв = 6247,20 · 0,3 = 1874,16 грн.

4.8 Складання кошторису витрат та визначення собівартості НДР.

Результати проведених вище розрахунків зведемо у таблиці 4.4.

Таблиця 4.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	6247,2,8	3,04
Відрахування на соціальні заходи	2348,95	1,14
Матеріальні витрати	180065,00	87,65
Витрати на електроенергію	45,50	0,02
Транспортні витрати	14405,20	7,01
Амортизаційні відрахування	462,00	0,22
Накладні витрати	1874,16	0,91
Собівартість	205448,01	100

Собівартість (Св) НДР розрахуємо за формулою:

$$Св = Во.п.+Вс.з.+Зм.в.+Зв+Тв+А+Нв \quad (4.11)$$

Отже, собівартість дорівнює

Св = 205448,01 грн

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = Св \cdot (1+Ррен) \cdot (1+ПДВ), \quad (4.12)$$

де Св – собівартість виконання НДР;

Ррен. – рівень рентабельності,

ПДВ – ставка податку на додану вартість,

Ц = 205448,01· (1+0,3) · (1+0,2) = 320498,89 грн.

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва - категорія, яка характеризує результативність виробництва. Вона свідчить не лише про приріст обсягів виробництва, а й про те, якими витратами ресурсів досягається цей приріст, тобто свідчить про якість економічного зростання.

Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

$$П = 320498,89 - 205448,01 = 115050,88 \text{ грн.}$$

Економічна ефективність ($Е_р$) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою 4.14.

$$Е_р = П / С_в, \quad (4.14)$$

де П – прибуток;

$С_в$ – собівартість.

$Е_р$ = 115050,88 / 205448,01 = 0,56

Поряд із економічною ефективністю розраховують (формула 4.15) термін окупності капітальних вкладень ($T_р$):

$$T_р = 1 / E_р \qquad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку $T_р=1/0,56=1,79$.

Всі дані розрахунків внесемо в зведену таблицю 4.5 техніко-економічних показників.

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1.	Собівартість, грн.	205448,01
2.	Плановий прибуток, грн.	115050,88
3.	Ціна, грн.	320498,89
4.	Термін окупності, рік	1,79

Загальна вартість розробленої комп’ютерної мережі ТОВ "ЕКС-простір" становить 320498,89 грн. Термін окупності становить 1,79 роки.

5. ОХОРОНА ПРАЦІ, ТЕХНІКИ БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Електромагнітні випромінювання (ЕМП)

Електромагнітні поля (ЕМП) – це змінні електричні та магнітні поля, що поширюються у просторі у формі хвиль зі швидкістю світла.

Що таке електромагнітний смог?

За останні 50-60 років сформувався фактор довкілля – електромагнітний смог або ЕМП антропогенного походження. ЕМП антропогенного походження – це радіо- та теле- станції, мобільні телефони, радіолокаційні установки, фізіотерапевтичні апарати, електроплити, електронагрівачі, холодильники, телевізори, тощо. Діапазон частот електромагнітних коливань, які використовуються в різних сферах – від десятків герц (промислова частота) до 1014 Гц, джерела випромінювання в такому широкому спектрі характеризуються середніми потужностями – від 106 до 10-2 Вт.

Кількість осіб, які контактують із надмірними рівнями енергії ЕМП, постійно зростає. Проблема заключається не в наявності радіохвиль, а в зростанні їх інтенсивності та зміні характеру випромінювання.

Глобальне електромагнітне забруднення довкілля

У 1995 році Всесвітньою Організацією Охорони Здоров'я (ВООЗ) офіційно запроваджений термін "глобальне електромагнітне забруднення довкілля". ВООЗ включила проблему електромагнітного забруднення навколишнього середовища в перелік пріоритетних проблем людства. Слід звернути увагу, що рівень цього забруднення кожні десять років зростає в 10–15 разів.

Живі організми у процесі еволюції пристосувалися до певного природного рівня інтенсивності електромагнітного поля і значні відхилення від

нього в більшу чи меншу сторону (за межі оптимальної життєдіяльності живих організмів) є стресовим фактором. Електромагнітні поля антропогенного походження, маючи інші характеристики, ніж геомагнітне поле, призводять до десинхронізації міжклітинних і міжорганних взаємодій у біологічній системі, яка налаштована в унісон із природним електромагнітним фоном. Сьогоднішній рівень електромагнітного фону Землі перевищує природній рівень в 200000 разів.

Найчутливішими до ЕМП є нейродинамічні процеси, які прямо чи побічно перемикають хронобіологічні процеси організму на патологічний або стресовий режим функціонування. Ще в 1928 р О.Л.Чижевський назвав сонячну активність “фактором, який сприяє виникненню та поширенню психозів”. Серед людей, які працюють у зоні промислових частот ЕМП, або проживають поблизу ліній високовольтних електропередач, поширені депресивні стани. Серед осіб, що проживають у місцях, де інтенсивність електромагнітного поля з частотою 50 Гц перевищує 0,15 мкТл, збільшується число самогубств.

Встановлено, що під впливом слабких ЕМП в організмі людини змінюється амплітуда та фаза ритмів біологічних показників. Як відомо, десинхроноз є загальною ознакою розладнання здоров’я на початкових етапах.

Ступінь впливу ЕМП на організм людини

Ступінь впливу ЕМП на організм людини залежить від діапазону частот, інтенсивності та характеру випромінювання (неперервного чи модульованого), режиму опромінювання, розміру поверхні тіла, що зазнає опромінювання, індивідуальних особливостей організму.

Тривалий та інтенсивний вплив ЕМП призводить, в першу чергу, до функціональних змін в серцево- судинній і центральній нервовій системах. Внаслідок переходу електромагнітної енергії в теплову при дії ЕМП спостерігається підвищення температури тіла та селективне нагрівання органів і

тканин організму. Таке нагрівання особливо небезпечне для органів із слабкою терморегуляцією (головний мозок, очі, нирки, шлунок тощо).

Перевищення електромагнітного навантаження від нормативного на 50 % призводить до збільшення захворюваності населення на 17 %, а при збільшенні на 150 % – на 37 % (найчастіше це захворювання органів дихання, алергічні захворювання, хвороби нервової системи). Електромагнітне опромінення впливає на репродуктивну функцію людини (спостерігається порушення дозрівання сперматозоїдів та яйцеклітин, що призводить до безпліддя). Серед населення, яке проживає в умовах дії електромагнітного випромінювання, у 1,5-2 рази вища захворюваність на хронічну патологію в порівнянні з населенням, яке живе на “чистій” території. Так, напруженість поля 1000 В/м спричинює головний біль, сильну втому, більші значення зумовлюють розвиток неврозів, безсоння. У 2004 році працівники Малагського університету (Іспанія) встановили, що мікрохвилі великої інтенсивності збільшують шанси розвитку депресії в 40 разів, а також пригнічують синтез мелатоніну, особливо в людей із хронічними захворюваннями та ослабленим імунітетом.

Дія електромагнітного випромінювання на людину вивчена недостатньо. Відомо, що зі збільшенням довжини хвилі знижується негативна дія ЕМП.

Вже не перший рік ведуться розмови про шкідливість мобільних телефонів

Це питання хвилює всіх користувачів мобільного зв’язку (2% з них не чули про небезпеку, а 52% вважають використання телефонів небезпечним). Мозок людини – органічний комп’ютер, всередині якого є рухомі електричні заряди, на які діють електричні та магнітні поля.

Питомий коефіцієнт поглинання електромагнітної енергії (SAR – Specific Absorbtion Rate) – показник, що свідчить про максимальну питому по-

тужність, яка поглинається людським тілом при розмові з використанням мобільного телефона (безпечний рівень – 2,0 Вт/кг). Більшість телефонів мають SAR від 0,5 до 1,0 Вт/кг, тобто немає достатньої потужності для перегріву мозку або хрусталика, що вказує на безпечність використання мобільних телефонів. Водночас з'ясовано, що мобільний телефон під час роботи генерує електромагнітне поле (ЕМП) не лише на основних (робочих) частотах. Крім основного сигналу (0.3 – 3 ГГц), мобільний телефон у режимі "дзвінок" і "розмова" генерує змінне електричне поле в діапазоні 5 – 2000 Гц і змінне магнітне поле в діапазоні 5 – 500 Гц.

При використанні мобільного телефона розглядається теплова і нетеплова (специфічна) дії ЕМП, які залежать від потужності випромінювання, виду тканин, часу та частоти. Відомо, що електромагнітне випромінювання частотою > 1МГц розігріває тканини організму. Перегрівання тканин призводить до руйнування білків у клітинах, що викликає відмирання клітин, виникнення пухлин тощо. Всі ці процеси носять ймовірнісний характер (потенціал терморегуляції захищає їх). В організмі існують тканини, які не омиваються кров'ю (наприклад, хрусталик ока) і при значному нагріванні руйнуються.

Нетермічний вплив ЕМП проявляється зміною біоелектричної активності головного мозку, порушеннями проникності клітинних мембран для іонів кальцію і т.п.

Незважаючи на літературні дані у вітчизняних та закордонних виданнях, що присвячені проблемі дії мікрохвильового випромінювання мобільного телефона, у них немає конкретної та чіткої відповіді на питання – шкідливе чи нешкідливе це випромінювання для людини та які критерії "нешкідливості".

Водночас експерти радять дітям і підліткам обмежувати тривалість використання телефонів, так як мозок і нервова система у них знаходяться у процесі формування.

Деякі країни законодавчо обмежили використання дітьми мобільних телефонів. Наприклад:

Франція. Розглянуто законопроект, за яким учні молодших і середніх класів не можуть носити та використовувати телефони у навчальних закладах.

Великобританія. У 2001 році в країні заборонено використання сотових телефонів у школах, при їх продажі в коробку вкладають інформаційні брошури про можливі наслідки спілкування мобільними телефонами.

Росія. Санітарними правилами і нормами (СанПиН 2.1.8/2.2.4.1190-03, пункт 6.9) рекомендовано обмеження можливості використання мобільних телефонів особами, які не досягли 18 років.

Показовим є той факт, що у Швеції при укладанні договорів страхування страхові агенти часто вводять у договір застереження "… за винятком шкоди, спричиненої електромагнітним полем".

Безперечно, ніякі залякування не призведуть до того, що люди перестануть користуватися мобільним зв'язком, це просто нереально в умовах науково-технічного прогресу. Однак, слід застерегти від надмірної тривалості розмов мобільними телефонами. Особливо це стосується людей з ослабленою імунною системою, дітей і вагітних жінок.

Спеціалісти із ВООЗ рекомендують утриматися від використання системи безпровідного доступу до Інтернету Wi-Fi в навчальних закладах для дітей, тому що електромагнітне випромінювання створює додаткове навантаження на організм дитини. У США, Великобританії та Німеччини все частіше відмовляються від Wi-Fi в школах, лікарнях, університетах. ВООЗ відзначає, що поки що володіє недостатнім об'ємом даних, які дозволяють робити однозначні висновки про шкідливість Wi-Fi для дитячого організму. Тому організація відносить використання цієї системи та мобільних телефонів до факторів недоведеного ризику. Крім цього, згідно офіційних даних, приблизно 3%

населення Землі страждають на гіперелектрочутливість – випромінювання довільного походження може здійснювати негативний вплив на їх організм.

5.2 Пожежна безпека на підприємстві [26]

Співробітники не часто замислюються, чи добре захищений офіс, в якому вони працюють, від пожеж, поки не станеться найгірше. А чи безпечно працювати у вашій компанії?

Метою пожежної безпеки будь-якого об’єкта є запобігання пожежі на визначеному чинними нормативами рівні, а в разі виникнення пожежі – обмеження її розповсюдження, своєчасне виявлення, гасіння пожежі, захист людей і матеріальних цінностей.

Для працівників важливо виконувати елементарні правила пожежної безпеки під час перебування на робочому місці. Адже безвідповідальне ставлення до таких, здавалося б, дрібниць, як недопалок чи залишений без нагляду електрообігрівач, може спричинити пожежу. Часто займання стається через неправильне зберігання в приміщенні легкозаймистих речовин, спалах електропроводки через перевантаження електромережі, неакуратне поводження з вогнем у місцях приготування їжі.

Вимоги протипожежного режиму

1. Куріння. Куріння у приміщеннях заборонено. Для куріння на територіях об'єктів обладнані спеціальні місця, які облаштовані урнами для недопалків. На території об'єктів заборонено застосування відкритого вогню (розігрівання замерзлих труб опалення, спалювання відходів виробництва, сміття, сухого листя, тощо).

2. Користування електронагрівальними приладами. Приготування кип'ятку, розігрівання та приготування їжі здійснюється в спеціально

обладнаних для цього місцях із застосуванням електрочайників та інших приладів з автоматичними пристроями відключення електронагрівальних елементів.

3. Робота з електроприладами. Забороняється залишати без нагляду увімкнені в електромережу електроприлади та оргтехніку – персональні комп'ютери, оргтехніку, радіоприймачі, електронагрівальні прилади, вентилятори, кондиціонери.

4. Вогненебезпечні роботи. Проведення вогневих та інших пожежонебезпечних робіт (газоелектрозварювальних, газорізальних, розігрів бітумів та смоли) дозволяється проводити після підготовки місця проведення цих робіт, узгодження з інженером з пожежної безпеки та виконання усіх передбачених заходів з пожежної безпеки.

5. На підприємстві має бути план евакуації. Тільки досвідчений фахівець може розробити план евакуації на вищому рівні. Дуже важливо заздалегідь подбати про евакуацію людей в момент загоряння і початку пожежі. У приміщенні повинні залишатися вільними евакуаційні шляхи і коридори, а вказівники повинні бути розташовані так, щоб було зрозуміло, де вихід. Має бути система оповіщення, яка подасть сигнал у разі пожежі

6. Порядок на робочих місцях. Як не дивно, акуратність теж важлива для пожежної безпеки. Папір – легкозаймистий матеріал. Не давайте йому розмножуватися і розповзатися по столу і підвіконню. Зберігайте його в папках і спеціальних боксах.

Інакше є небезпека, що одного разу папірець доповзе до подовжувача або до обігрівача, який раптово заіскрив. Пильнуйте, щоб колеса офісних крісел не їздили по проводах, які лежать на підлозі. Це може нашкодити як внутрішній частині провода, так і його ізоляції. А далі – удар струмом і загоряння.

7. Пожежна сигналізація – це один з найважливіших пристроїв для забезпечення безпеки в приміщеннях.

8. Перевірка робочих місць та приміщень наприкінці робочого дня. Перед закінченням роботи та закриттям приміщень особа, відповідальна за протипожежний стан приміщення, зобов'язана перевірити протипожежний стан приміщень, вимкнути напругу з усіх електроустановок та електроприладів (вимірювальних, електронно-обчислювальних, паяльників, кондиціонерів, вентиляторів, радіоприймачів, комп'ютерів тощо), а також з мереж їх живлення.

Закрити вікна, кватирки.

Виявлені порушення правил пожежної безпеки потрібно усунути до зачинення приміщень.

9. Навчання. На будь-якому підприємстві потрібно регулярно проводити інструктажі з пожежної безпеки та практичні тренування.

Загальний порядок дій працівників у разі пожежі.

– негайно повідомити пожежну охорону за телефоном 101;

– вжити заходів щодо евакуації людей та збереження матеріальних цінностей, гасіння пожежі з використанням вогнегасників та інших наявних засобів пожежогасіння;

– повідомити про пожежу керівника чи відповідну компетентну посадову особу;

– вимкнути, за потреби, струмоприймачі та вентиляцію;

– за потреби викликати інші аварійно-рятувальні служби (медичну, газорятувальну тощо).

На рисунку 5.1 приведено план приміщення та поставлені на ньому знаки пожежної безпеки

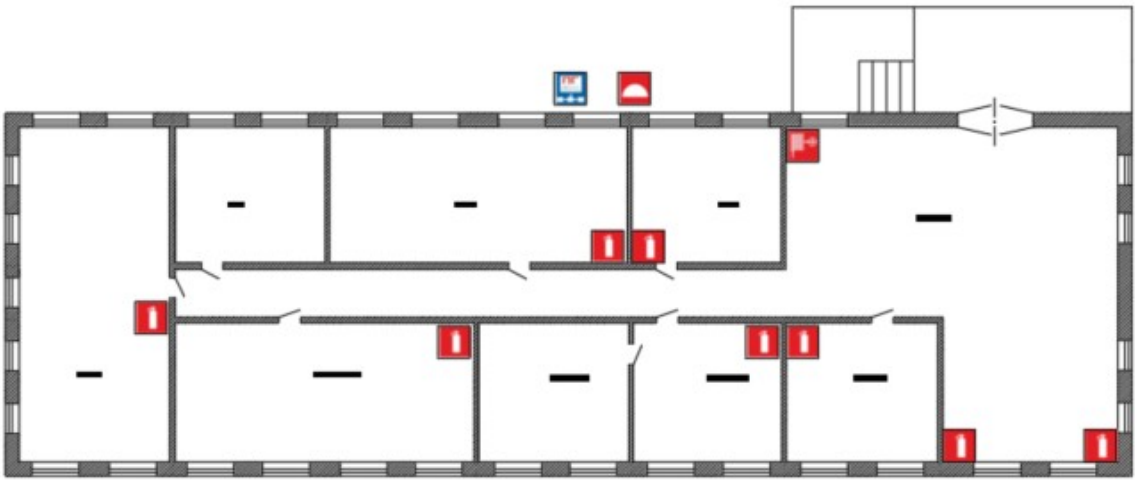


Рисунок 5.1 — Знаки пожежної безпеки на підприємстві

ВИСНОВКИ

В ході роботи над кваліфікаційною роботою бакалавра спроектовано комп’ютерну мережу підприємства "ЕКС-простір". Зроблено аналітичний огляд літератури та існуючих рішень, та на його основі спроектовано логічну та фізичну топологію мережі. Вибрано пасивне та активне комутаційне обладнання, сервер, точку доступу та програмне забезпечення.

Робота містить повністю завершену логічну і фізичну топології мережі, таблицю IP-адресації та техніко-економічних показників які подано в графічній частині.

В економічному розділі розраховано собівартість мережі, її економічну ефективність, термін окупності та інші показники.

Останній розділ кваліфікаційної роботи описує питання охорони праці, та техніки безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1.
2. Альваро Ретана, Дон Слайс, Расс Уайт. Принципы проектирования корпоративных IP-сетей. - М.: АБФ, 2003. – 435с.
3. Антонов В.М. Сучасні комп'ютерні мережі. Підручник — К.: "МК-Прес", 2005. — 480 с.
4. Буров Є. Комп'ютерні мережі, 2-е видання. - БаК, 2004. – 584 с.: іл.
5. Жуков І.А., Дрововозов В.І., Махновський Б.Г. Експлуатація комп’ютерних систем та мереж. Київ: НАУ. 2007. 361с.
6. Контроль та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології: навч. посіб. / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. Харків: СМІТ. 2014. 544 с
7. Додонов О. Г., Ланде Д. В., Путятін В. Г. Інформаційні потоки в глобальних комп’ютерних мережах. — К.: Наук, думка, 2009. — 295 с
8. Горбатий І.В., Бондарєв А.В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи. Львів: Львівська політехніка. 2016. 336с.
9. Царьов Р.Ю. Структуровані кабельні системи: навч. посіб. для студентів вищих навчальних закладів. Одеса: ОНАЗ ім. О.С. Попова, 2013. 260 с.
10. Навакатікян О. О., Кальниш В. В., Стрюков С. М.. Охорона праці користувачів комп'ютерних відеодисплейних терміналів. Київ, 1997. 400 с.
11. І.В Шудренко. Основи охорони праці: навч. посібник. Житомир: Видавець ОО Євенок, 2016. 214 с.
12. Журавська І. М. Проектування та монтаж локальних комп’ютерних мереж: навчальний посібник. Миколаїв: Видавництво ЧДУ ім. Петра Могили, 2016. 396 с.
13. Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. Комп’ютерні мережі: навчальний посібник. Київ: Компрінт, 2017. 821с.

14. Горбатий І.В., Бондарєв А.В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи. Львів: Львівська політехніка. 2016. 336с.
15. Рамський Ю.С., Олексюк В.П., Балик А.В. Р21 Адміністрування комп'ютерних мереж і систем: Навч. пос. — Тернопіль: Навчальна книга – Богдан, 2010. — 196 с.
16. КОМП'ЮТЕРНІ МЕРЕЖІ Частина 1 НАВЧАЛЬНИЙ ПОСІБНИК [Електронний ресурс]: навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем» та «Інформаційне забезпечення робототехнічних систем»/ Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 8,6 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.
17. Комп'ютерні мережі. Принципи, технології, протоколи. Ювілейне видання. Оліфер В. Г.Оліфер Н. А.
18. Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп'ютерних систем. Монографія. - К.: ДУПСТ, 2011. - с.257.
19. Business Products [Електронний ресурс] – Режим доступу до ресурсу: http://www.trendnet.com/products/business/category/switches – Дата доступу: 11.04.2017.
20. Комутатори [Електронний ресурс] – Режим доступу до ресурсу: http://hotline.ua/computer/kommutatory/ – Дата доступу: 11.04.2017.
21. Охорона праці – Москальова В.М. [Електронний ресурс] – Режим доступу до ресурсу: http://studentbooks.com.ua/content/view/1327/76/ – Дата доступу: 11.04.2023.
22. Глобальні компютерні мережі URL:https://pidru4niki.com/74236/informatika/globalni_kompyuterni_merezhi

(дата звернення: 18.04.2023.

23. Організація компютерних мереж URL:http://nickshevtsov.blogspot.com/2017/10/blog-post.html (дата звернення: 22.04.2023.
24. Мережеве устаткування компютерних мереж URL:https://stud.com.ua/53330/informatika/merezheve_ustatkuvannya_programni_komponenti_upravlinnya_merezheyu (дата звернення: 11.05.2023.
25. Методи тестування та діагностики компютерних мереж URL:file:///C:/Users/vaste/Downloads/metody-testirovaniya-i-diagnostirovaniya-kompyuternyh-setey.pdf (дата звернення: 3.05.2023).
26. Встановлення Ubuntu 20.04 URL:https://www.digitalocean.com/community/tutorials/initial-server-setup-with-ubuntu-20-04-ru (дата звернення: 13.05.2023).
27. Пожежна безпека на робочому місці. URL:https://ohoronapraci.kiev.ua/article/news/pozezna-bezpeka-na-robocomu-misci (дата звернення: 23.05.2023).
28. Ознайомлення з Cisco Packet Tracer URL:http://organizationofcomputernetworks.blogspot.com/2017/10/cisco-packet-tracer-cisco-packet-tracer.html (дата звернення: 13.05.2023).