Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(інститут)

Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Турта Дмитро Володимирович
(П.І.Б.)
академічної групи 123-20ск-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)
на тему Комп'ютерна система ТОВ «Українські інформаційні технології» з опрацюванням побудови та налаштування корпоративної мережі
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
кваліфікаційної роботи	доц. Кожевников А.В.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

"___" _____ 2023 року.

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Турта Д.В. **академічної групи** 123-20ск-1
(прізвище, ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему Комп'ютерна система ТОВ «Українські інформаційні технології» з опрацюванням побудови та налаштування корпоративної мережі
(назва за наказом ректора)

затверджена наказом ректора НТУ «Дніпровська політехніка» від . .20223 №___-Л

Розділ	Зміст завдання	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2023
Розробка апаратної частини	На основі аналізу підприємства сформулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	25.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	05.06.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	10.06.2023

Завдання видано _____ доц. Кожевников А.В.
(підпис керівника) (прізвище та ініціали)

Дата видачі 01.04.2023 р.

Дата подання до атестаційної комісії 15.06.2023 р.

Прийнято до виконання _____ Турта Д.В.
(підпис студента) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 93 с., 30 рис., 10 табл., 2 дод., 5 джерел.

СИСТЕМА, МЕРЕЖА, ЛОКАЛЬНА МЕРЕЖА, МЕРЕЖЕВІ ЗАСОБИ

Об’єкт розробки: комп’ютерна система ТОВ «Українські інформаційні технології» з опрацюванням побудови та налаштування корпоративної мережі.

Мета: створення комп’ютерної система ТОВ «Українські інформаційні технології» з опрацюванням побудови та налаштування корпоративної мережі.

Розроблена комп’ютерна система ТОВ «Українські інформаційні технології» з опрацюванням побудови та налаштування корпоративної мережі.

Розроблено систему з урахуванням можливості швидкої зміни конфігурацій і здійснення технічної і програмної модернізації системи, яка забезпечує збір та обробку, накопичення інформації у базах даних; комунікацію між кінцевими споживачами у різних підрозділах та доступ до загальних ресурсів.

Комп’ютерн система ТОВ «Українські інформаційні технології» виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці або додатках.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ЕОМ – Електронна обчислювальна машина

КС – Комп’ютерна система;

ПК – Персональний комп’ютер;

Ethernet – Технологія передачі даних по мережі;

Wi-Fi – технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11;

ВСТУП

Початок XXI століття характеризується впровадженням нових інформаційних систем і технологій у всі сфери діяльності суспільства, використанням сучасних комп’ютерних і комунікаційних засобів. В даний час мобільні технології розвиваються швидше. За оцінками, кількість комп'ютерів у світі наближається до 500-600 мільйонів.

Кожна обчислювальна система також унікальна по-своєму. Тому знайти дві системи з однаковою апаратною та програмною конфігурацією не дуже просто. Тому фахівець, який займається експлуатацією обчислювальної техніки, повинен мати широкий спектр знань і досвіду. Найпримітивніша комп'ютерна мережа створюється шляхом фізичного з'єднання двох і більше комп'ютерів. Для створення комп’ютерної мережі важливо мати спеціальне мережеве обладнання та спеціальне мережеве програмне забезпечення. Усі комп’ютерні мережі мають одну мету – спільне використання спільних мережевих ресурсів.

ТОВ «Українські інформаційні технології» забезпечує організації будь-якого розміру найкращими та найнадійнішими IT-рішеннями, на ринку технологій, що постійно розвивається. ТОВ «Українські інформаційні технології» забезпечує є надійним союзником, який може допомогти іншім компаніям у вирішенні викликів, які супроводжують технологічний розвиток.

Заснована в 2003 році, ТОВ «Українські інформаційні технології» є однією з провідних IT-компаній України. Тісно співпрацюючи з провідними міжнародними компаніями, яка пропонує широкий спектр продуктів і послуг, в тому числі хмарні технології, послуги безпеки та мобільності, які включають системну інтеграцію, рішення для центрів обробки даних, мережеві рішення, електропостачання, системи охолодження, розробку програмного забезпечення, IT-консалтингові послуги, а також послуги з розподілу. Роки професійного підходу до бізнесу привели

компанію до досягнення високого рівня задоволеності клієнтів і, як наслідок, зробили її однією з провідних IT-компаній сьогодні.

ТОВ «Українські інформаційні технології» є партнером відомих брендів: Bestcomp Group Hewlett Packard Enterprise, Aruba Networks, Hewlett Packard Incorporated, Thales, Entrust, Intel, Fortinet і Snom, Master Security, Cisco, Schneider Electric, дистриб'ютор Microsoft, Acer, Lenovo, Dell, Juniper, Micro Focus, Radware, VMware, Schneider Electric, Eaton, Tripplite та ще понад 50 інших провідних виробників світу.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика галузі та умови застосування комп’ютерних систем

1.1.1 Загальні відомості

Комп'ютер, на відміну від інших пристроїв, - це пристрій, який працює за підготовленою для нього програмою і виконує будь-які операції, пов'язані з аналізом введеної в нього інформації. Тому для комп’ютера має бути розроблена детальна послідовність дій, тобто програма, зрозумілою йому мовою.

Рисунок 1.1 – Вигляд сучасних комп’ютерів

Програма - це список інструкцій або команд, які машина виконуватиме крок за кроком. Щоб використовувати комп'ютер і розширити область його застосування, вони повинні мати програмне забезпечення. Програмне забезпечення - це такий комплекс програм, без якого неможливо уявити роботу комп'ютера. Програма призначена не тільки для вирішення конкретної задачі, а й для створення зв'язку між користувачем і комп'ютером, управління процесом обробки інформації, допомоги програмісту у вирішенні проблеми, навіювання помилок і донесення до нього і т. д. необхідні для Програмне забезпечення — це набір програм, які вирішують проблеми та проблеми, які досліджує користувач комп’ютера.

За способом роботи програми, що входять до складу ПЗ, діляться на три категорії:

1. Системні програми. Такі програми завжди готові до роботи і зберігаються в пам'яті. Їх основне завдання - встановити зв'язок між пристроями і апаратним забезпеченням комп'ютера та іншими програмами, які використовуються в процесі роботи. До таких програм належать програмне забезпечення BIOS;

2. Прикладні програми. Це найпоширеніша категорія програм. За допомогою цих програм можна вирішити будь-які проблеми на комп’ютері. Після закінчення роботи цих програм пам'ять звільняється і управління передається іншим програмам.

3. Резидентні програми. Такі програми, на відміну від звичайних програм, не видаляються з основної пам'яті, коли вони передають керування іншим програмам, а переймають керування після завершення виконання програм.

За функціональним призначенням програмне забезпечення, що використовується в комп’ютері, поділяється на три групи:

- системне програмне забезпечення, що виконує управлінські та різні допоміжні функції. Наприклад, копіювання використаної інформації, перевірка працездатності пристрою на комп’ютері тощо.
- системи програмування або інструментальні системи, що забезпечують створення нових програм на ЕОМ;
- прикладні програми, які виконують певні завдання користувача, наприклад, текстові редактори, малювання картинок і графіки тощо.

Системне програмне забезпечення:

Системне програмне забезпечення організовує процес обробки інформації на комп’ютері. Системними програмами є:

- операційні системи;
- мережеві системи;
- комунальні послуги та ін.

Через системні програми можна форматувати диски, задавати параметри зовнішніх пристроїв, підключених до комп’ютера, перевіряти практичну пам’ять та інші пристрої, організовувати друк, встановлювати з’єднання з локальними та глобальними мережами.

Основою системного програмного забезпечення є операційні системи. Операційні системи є одним з важливих елементів персонального комп'ютера. Операційна система - це програмна система, яка запускається при підключенні комп'ютера, забезпечує роботу всіх частин комп'ютера та керує інформацією. Операційна система має інтерфейс для користувача на додаток до управління зберіганням і обробкою даних.

Мережеві операційні системи забезпечують доступ до всіх ресурсів комп'ютерної мережі користувача за рахунок формування локальних і глобальних комп'ютерних мереж.

Мережеве програмне забезпечення керує загальними ресурсами розподіленої обчислювальної мережі. Загальні ресурси включають пристрої пам’яті, периферійні пристрої, спільне програмне забезпечення тощо, а мережеве програмне забезпечення включає Windows 2000 для сервера, Windows NT Server, Netware, Windows для робочої групи тощо. належить до.

До складу операційної системи входять службові програми, які виконують ряд завдань. Ці програми значно покращують використання комп’ютера та його технічні характеристики. Ці програми контролюють роботу апаратної частини комп'ютера, виявляють помилки, визначають місце їх виникнення, отримують доступ до ядра операційної системи, завантажують програми із зовнішніх накопичувачів (дисків і флешок) в практичну пам'ять, виправляють помилки під час роботи. , встановлення зв'язку між програмними модулями, форматування дисків тощо.

Сервісні програми включають наступне:

- інтерфейсні програми;

- програми для роботи з файлами, каталогами та папками;
- антивіруси;
- програми-архіватори;
- програмні накладки;
- програми, що перевіряють працездатність пристроїв;
- програми, що керують роботою пристроїв - драйвери;
- службові програми.

Під час роботи комп’ютера службові програми виконують такі допоміжні функції:

- проводить діагностику комп’ютера, виявляє несправності та по можливості усуває їх;
- програми-архіватори стискають файли та зменшують їх розмір (ARJ, ZIP, WINZIP? WINRAR);
- антивірусні програми запобігають перевірці комп’ютера на віруси та видаляють нові віруси (NOD32, ESET тощо).

Інструментальні програми (системи програмування):

1. Інструментальні програми або системи програмування використовуються для створення нових програмних засобів (систем і додатків). Системи програмування забезпечують роботу на мовах програмування, які зручніші для користувача, ніж на машинній мові.
2. Машинна мова працює з кодами, які може безпосередньо зрозуміти комп’ютер і складаються з кількох послідовностей команд. Однак багатьом користувачам не зручно працювати цією мовою. Тому використовуються символічні мови, близькі до природної мови. Такі мови називаються мовами програмування. Програми, написані на мові програмування, перетворюються на машинні мови та виконуються.
3. Алгоритмічні мови вважаються мовами високого рівня. Програми, написані на таких мовах, працюють на будь-якому комп'ютері, з ними

зручно і легко працювати. Недоліками є те, що неможливо врахувати технічні характеристики комп'ютера і витрачається більше часу на виконання.

Алгоритмічні мови діляться на такі групи:

- для розв'язування логічних задач;
- для програмування науково-технічних та економічних питань;
- з питань програмування управління технологічними процесами та моделювання.

Перед виконанням програми, написаної на мові програмування, вона перетворюється на машинну мову за допомогою набору програм, який називається транслятором.

Перекладачі можуть бути організовані двома способами: інтерпретація та компіляція. Тому транслятор доречно називати інтерпретатором або компілятором.

Інтерпретатор аналізує оператори програми один за одним і завантажує його в пам'ять як єдине ціле. З цієї причини час роботи програми подовжується.

Компілятор перетворює всю програму в машинний код і вчасно передає інформацію про помилку користувачеві. Тут аналіз операторів і перетворення в машинний код виконується один раз. Тому швидкодія комп'ютера зростає і виконання програми не залежить від процесу. У результаті немає необхідності завантажувати програму у віртуальну пам'ять, а віртуальне ім'я можна використовувати для інших цілей.

1.1.2 Захист інформації

Немає потреби спеціально обґрунтовувати важливість збереження проблеми інформаційної безпеки в центрі уваги в сучасний час і вжиття необхідних додаткових заходів для її усунення. Сьогодні дуже велика частина населення планети користується можливостями інформаційних технологій, комп'ютерних систем і мереж, у тому числі Інтернету. Звичайно, кожна людина, яка так чи інакше

використовує комп’ютер і користується послугами мережі Інтернет, стикалася з проблемами інформаційної безпеки, включаючи звичайне «зникнення» файлів і збій системи, зараження комп’ютера вірусами, файли, комп’ютер, система та/або різні серйозні проблеми аж до несанкціонованого доступу до мережі. Зокрема, до цих проблем відноситься незаконне втручання в роботу комп'ютерів, комп'ютерних систем і мереж, їх порушення, викрадення комп'ютерної інформації, розтрата, захоплення, поширення, знищення тощо. такі небезпечні нові соціальні прояви можна віднести.

Рисунок 1.2 – Зображення-нагадування про захист інформації

У зв'язку з цим мережа Інтернет відіграє роль одного з головних факторів, що сприяють подальшому загостренню проблеми інформаційної безпеки. Кількість людей, які ним користуються, астрономічно зростає. Сьогодні Інтернет охоплює понад 160 країн світу. У 1998 році до Інтернету було підключено приблизно 143 мільйони користувачів, а в 2010 році їх кількість досягла 1 мільярда 600 мільйонів. Зараз кількість користувачів Інтернету перевищила 426 мільйонів в Європі, 765 в Азії, 260 в Північній Америці, 187 в Латинській Америці, 86 в Африці і 21 мільйон в Австралії. Першу десятку країн світу за чисельністю займають Китай (298 млн), США (227 млн), Японія (94 млн), Індія (81 млн), Бразилія (67,5 млн), Німеччина (55 млн), Велика Британія. користувачів Інтернету (43,8 млн), Франції (40,9 млн), Росії

(38 млн) і Південної Кореї (36,8 млн). Число користувачів Інтернету в Азербайджані вже перевищило 4 мільйони (45% населення). Інтернет надає абсолютно однакові можливості всім, хто користується його послугами, включаючи хакерів, злочинців і терористів, для реалізації своїх злочинних намірів.

З цієї точки зору основну загрозу комп'ютерним системам становлять люди, які грають роль зловмисників і професійні фахівці в області інформаційних технологій - хакери. Хакери, як правило, знають тонкощі комп’ютерних систем і мереж, телекомунікаційних пристроїв та інформаційних систем, а також систем безпеки, включаючи їх слабкі місця, вони мають доступ до всіх необхідних програмних і технічних баз для аналізу, злому, створення та поширювати механізми безпеки, і вони мають можливості. Комп'ютерні віруси є одним з найважливіших факторів, що вимагає підвищеної уваги до проблеми інформаційної безпеки. Подібно до природних вірусів, комп’ютерні віруси з різними функціями поширюються шляхом таємного додавання (запису) до програм, пристроїв пам’яті та файлів. Пізніше він автоматично перенесеться в інші програми, файли тощо. передаються комп’ютерні віруси від відображення будь-якої інформації на екрані, пошкодження інформаційних ресурсів, вихід з ладу дисководів тощо. може призвести до тяжких наслідків та інших дуже серйозних проблем.

Для запобігання вищезгаданим загрозам використовуються різні методи та засоби. Оскільки більш серйозні загрози, які виникають або реалізуються, базуються на сучасних технологіях, методи та засоби їх запобігання повинні реалізовуватися на основі найсучасніших технологій. В останні роки екран захисту мережі, системи виявлення атак і технології віртуальної приватної мережі використовуються для більш серйозного забезпечення безпеки інформації в комп'ютерних системах і мережах. Важливо вивчати і застосовувати ці технології на практиці. Втручання в роботу системи, її збій, а також витік, модифікація, знищення інформації тощо. для забезпечення усунення загроз систематично

проводити боротьбу зі шкідливими програмами, впроваджувати методи та засоби їх своєчасного виявлення та запобігання.

Загалом, для більш цілеспрямованого забезпечення вирішення проблеми інформаційної безпеки, включаючи вибір необхідних методів і засобів, встановлення ефективної політики безпеки, усунення можливих слабких місць у системі чи мережі, методи оцінки рівень безпеки в комп'ютерних системах і мережах і засоби аналізу ситуації, які необхідно реалізувати. З урахуванням викладеного в навчальному посібнику викладено методи та засоби забезпечення інформаційної безпеки в комп’ютерних системах і мережах на основі сучасних технологій [3].

1.2 Характеристика ТОВ "Українські інформаційні технології"

1.2.1 Геолокація розташування

Компанія ТОВ "Українські інформаційні технології" зареєстрована за юридичним адресом Україна, 79017, львівська обл., місто Львів, вул. Водогінна, 2.

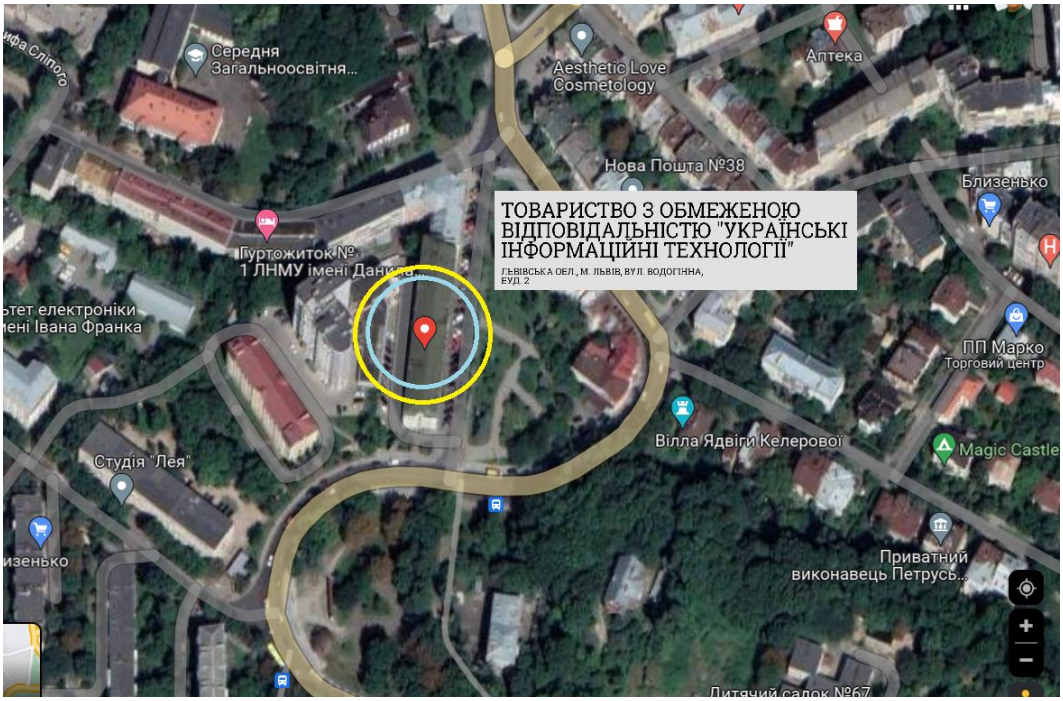


Рисунок 1.3 – Геолокація розташування ТОВ "Українські інформаційні технології"

1.2.2 Загальна інформація

Ukrainian Business Award (UBA) розробила методику визначення кращих компаній шляхом комплексного аналізу їх позиції на ринку країни. Класифікація створена на основі аналізу відкритих даних, у тому числі з використанням системи YouControl. Методологія включає кілька ключових аспектів, які були враховані при оцінці компаній:

- фінансовий аналіз: оцінка фінансової стійкості компанії, включаючи ліквідність, платоспроможність і прибутковість, а також аналіз імпортно-експортних операцій;
- ситуація на ринку: аналіз частки ринку компанії, темпів зростання, присутності в Інтернеті (сайт, соціальні мережі) та відгуків клієнтів;
- фактори ризику: оцінка ризиків, пов'язаних з компанією, включаючи відносини, судові справи, розслідування, борги, податкову інформацію, ліцензії, сертифікати та дозволи.

На наступному етапі компанії класифікувалися за такими ознаками:

- види діяльності: компанії були розділені на 99 кодів і підкодів КВЕД з урахуванням більш ніж в три рази більше підкодів;
- бізнес-сектор: класифікація компаній за розміром бізнесу, включаючи мікро-, малі, середні та великі підприємства;
- категорії: компанії класифікуються як A, B, C та D на основі їх ефективності та фінансових показників.

На заключному етапі для визначення оцінок використовувалася математична формула оцінювання, яка відображає загальну оцінку кожної компанії. Після цього було сформовано рейтинг, у якому компанії ранжуються в порядку їх балів, що вказує на їх позицію в топ-100 компаній України у 2023 році.

ТОВ "Українські інформаційні технології" є лідером ТОП-100 компаній України 2023 р.

Таблиця 1.1 – Перша десятка найкращих компаній України 2023 року [2]

ЄДРПОУ	Назва компанії	Розмір	Категорія	Оцінка	ФК	РП	ФР
32568891	ТОВ «УКРАЇНСЬКІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ» (SoftServe)	XL	A	100,0	4	4	X/3
32108814	ТОВ «РЕХАУ»	XL	A	100,0	4	4	X/3
34307795	ТОВ «ВЕДЕРСТАД»	XL	A	100,0	4	4	X/2
31170127	ТОВ «ШНЕЙДЕР ЕЛЕКТРІК УКРАЇНА»	XL	A	100,0	4	4	X/3
32424407	ТОВ «ФЕРРЕРО УКРАЇНА»	XL	A	100,0	4	4	X/3
21638055	ТОВ «МАРС УКРАЇНА»	XL	A	100,0	4	4	X/3
32638227	ТОВ «АНТОНІВСЬКИЙ М’ЯСОКОМБІНАТ»	XL	A	100,0	4	4	X/4
31489175	ТОВ «ДАНОН ДНІПРО»	XL	A	100,0	4	4	X/2
31273402	ТОВ «ЗБАРАЗЬКИЙ КОМБІНАТ ХЛІБОПРОДУКТІВ»	XL	A	100,0	4	4	X/2
30176505	ТОВ З ІНОЗЕМНИМИ ІНВЕСТИЦІЯМИ «ВОЛЬВО УКРАЇНА»	XL	A	100,0	4	4	X/1

Основні види діяльності ТОВ "Українські інформаційні технології":

- комп'ютерне програмування;
- видавництво комп'ютерних ігор;
- розгортання інших програм;
- консультації з питань інформатики;
- інша діяльність у сфері інформаційних технологій та комп'ютерних систем;
- обробка даних та поширення інформації на веб-сайтах та пов'язана з ними діяльність;

– оренда та експлуатація приватної або орендованої нерухомості [1].

1.2.3 IT-послуги з кіберзахисту інформації

Нагальна необхідність забезпечення кіберзахисту інформації, комунікацій та автоматизованих систем в контексті реалізації існуючих заходів з протидії сучасним кіберзагрозам є невід'ємною частиною політики інформаційної безпеки підприємств та відомств усіх форм власності. Основою реалізації будь-якої політики інформаційної безпеки є побудова комплексної системи захисту інформації. Комплексний підхід до проектування, розробки, впровадження та обслуговування комплексної системи захисту інформації є запорукою надійного захисту інформації з обмеженим доступом.

ТОВ "Українські інформаційні технології" має ліцензію на провадження господарської діяльності з надання послуг у галузі технічного захисту інформації, за переліком, що визначається Кабінетом Міністрів України: п. II.1 «Оцінювання захищеності інформації, що не становить державної таємниці», які дозволяють надавати послуги з інформаційної безпеки.

1.3 Принципи, технічні способи та математичні методи інформаційного забезпечення підприємства

ТОВ "Українські інформаційні технології" освоює новий напрямок свого розвитку - створення комплексних програмних комплексів, призначених для автоматизації банківських, фінансових та інших структур, проектування, побудови телекомунікаційних мереж і надання послуг передачі даних (передачі даних), побудова та впровадження систем VoIP та відеоспостереження по оптичних каналах і WiFi technology, займається системною інтеграцією, продажом та установкою комунікаційного обладнання, наданням послуг широкосмугового інтернет-провайдера та ADSL.

Компанія успішно продовжує впровадження та експлуатацію програмних продуктів АСУ «Смарт-Банк» та АСУ «Смарт-Фінанс».

ТОВ "Українські інформаційні технології", окрім побудови корпоративних мереж, є партенром з послуг передачі даних, побудови та впровадження систем відеоспостереження по оптичних каналах та технологіям «WiFi», системна інтеграція, продаж та встановлення комп'ютерне та комунікаційне обладнання.

Рисунок 1.4 - Комп'ютерне та комунікаційне обладнання

Волоконна-оптичний зв'язок полягає в передачі інформації з однієї точки в іншу за допомогою електромагнітних хвиль світлових імпульсів. В основному ця система використовується в місцях з важкими природними умовами (вогкість, сирість, місця проходження високовольтних кабелів), коли необхідно передати інформацію на високій швидкості на відстань 20…80 км. Іноді необхідно передати інформаційні кабелі, такі як CCTV, CAT5-6-7, телефонний тощо на відстань більше 500 м або такі кабелі в суворих природних умовах, поблизу ліній високої напруги. Волоконна-оптичні мережі для цього є незамінними.

Компанія пропонує розробку систем відеоспостереження, IT, телефонних ліній з ВОЛЗ щоб забезпечити велику кількість людей якісним Інтернетом, проектує відповідну інфраструктуру за технологією ADSL.

Рисунок 1.5 - Обладнання для послуг SMART VOICE

Компанія розроблює і впроваджує послугу телефонної розмови з будь-якою країною світу у своїй базі послуг SMART VOICE.

IP-телефонія останнім часом є засобом зв'язку, що швидко розвивається. Розвиток сучасних технологій створив чудові можливості для спілкування. Це або стаціонарні домашні пристрої, або мобільні телефони.

В IP-телефонії немає таких понять, як виклик абонента мережі і «роумінг». При використанні IP-телефону тарифи фіксовані і не залежать від того, в яку країну ви телефонуєте.

Перше, що привертає увагу споживача, це ціна хвилини розмови - у будь-який момент можна користуватися IP-телефоном, отримуючи переваги сучасних технологій за найнижчою ціною в порівнянні з іншими варіантами дзвінків. Економія в 1,5…2 рази, ця послуга працює вже кілька років і дає можливість абонентам телефонувати в будь-яку точку світу.

Технологія IPTV (Internet Protocol Television) (IPTV, IP-телебачення) - цифрове інтерактивне телебачення в мережах передачі даних на основі протоколу IP, телебачення нового покоління.

Рисунок 1.6 - Обладнання для IP-телебачення

Кожен інтернет-користувач зможе дивитися багато вітчизняних та іноземних телеканалів через послугу IPTV.

1.4 Огляд рішень для впровадження комп’ютерних систем

1.4.1 Навчання персоналу

З метою забезпечення безпеки, безперервності, регулярності та ефективності, які вважаються основними елементами забезпечення діяльності комп’ютерних систем, належне налагодження роботи існуючою структури мережевого забезпечення в IT компаніях завжди було актуальним як один із основних пріоритетні питання. Зі збільшенням обсягу та інтенсивності трафіку мережі збільшується пропускна здатність комп’ютерних систем, і водночас це збільшення також створює багато серйозних і негативних проблем. Для цього необхідно систематизувати та оновити підготовку спеціалістів інженерного обслуговування комп’ютерних систем з метою подальшого підвищення якості роботи з технічного супроводу та завчасного запобігання негативним ситуаціям, які можуть виникнути,

шляхом використання найсучасніших технологій, які є можливими завдяки розвитку техніки.

У центрі процесу відбору та підготовки фахівця, що виконує технічне забезпечення, знаходиться врахування інструкторів і стандартизованих інструкцій, знань і, в більшості випадків, практичних навичок. У будь-якому випадку якість вирішення технічної проблеми в кінцевому підсумку багато в чому залежить від людського фактору. З проведених досліджень зрозуміло, що існуючі методи та інструменти, які використовуються для відбору, оцінки та навчання фахівців з інженерного забезпечення, на даний момент мають достатні недоліки. Це в першу чергу проявляється у створенні сприятливих умов для партнерства та різноманітних психологічних навантажень.

У процесі подальшої підготовки та роботи, оскільки база даних процедур технічної підтримки, необхідних для вирішення проблеми, систематично науково не аналізується, необхідно використовувати окремі шаблони навіть для найменших технічних збоїв тощо.

При оцінці критеріїв методик, призначених для відбору та навчання спеціаліста з реалізації технічної підтримки, стає зрозуміло, що вимоги до вихідних даних бази, нормативних та керівних документів, оцінка наданої інформації щодо організації повні та несуперечливі процедури в готовому робочому пакеті та застосований для цього механізм оцінки, втрати часу, витраченого на технічну підтримку, налагодження відносин між фахівцем технічного персоналу та інструктором, оцінка якості процедур, застосованих для вирішення різноманітних проблем і т. д., велика кількість ознак дозволяє охарактеризувати ці системи за допомогою мультиагентних технологій.

1.4.2 Системи штучного інтелекту

Мультиагентні системи були створені для вирішення різноманітних задач штучного інтелекту. У цих системах весь спектр вирішення проблем розподіляється

між агентами, кожен з яких є членом певної групи або організації, відповідно до набору правил. Розподіл і складність завдань змінюється в залежності від здатності кожного агенту їх виконувати.

Враховуючи вищевикладене можна стверджувати, що ефективність і якість роботи підрозділів інженерного забезпечення комп'ютерних систем для IT-компаній залежить від великої кількості різноманітних характерних факторів - людського фактору, технічної та інформаційної забезпеченості, ступеня важливості технічної проблеми, що вирішується, тощо. залежить від факторів, кожен з цих факторів викликає різні характеристики в розглянутому процесі. Для того, щоб оцінити вплив цих ознак на показники якості та ефективність роботи, необхідно розглянути питання побудови моделі вибору альтернативних процедурних правил, що відповідають найкращим критеріям обраних ознак якості для вирішення проблеми обслуговування з використанням мультиагентних технологій.

Для побудови моделі даної проблеми та більш точної оцінки доцільно використати методологію IDEF0-функціонального моделювання діяльності підрозділів інженерного забезпечення IT-компаній. Ця методологічна теорія в даний час використовується в наукових дослідженнях, виробництві, соціології і т. д.

Підготовлені пакети робіт, які будуть виконуватися в IT-компанії у відділі інженерної підтримки, безпосередньо від системних адміністраторів, інформації з діагностичних приладів, мережевого обладнаних.

Готовий комплекс робіт планується та направляється бригаді технічного обслуговування комп'ютерних мереж, кількості та впливу наявних і відсутніх технічних засобів. Технічний персонал, у свою чергу, використовуючи наявні ресурси, виконує надіслане завдання, або завдання, яке не може бути виконане, повертається до планового відділу для перевірки, виконання та архівації. Невиконані завдання повертаються до відділу інженерного забезпечення для перевірки та передаються до планового відділу для повторного виконання після з'ясування та усунення причин, які могли перешкодити виконанню завдання [4].

1.5 Структури ТОВ "Українські інформаційні технології"

1.5.1 Організаційна структура

Однією з переваг ТОВ "Українські інформаційні технології" є ефективна організаційна структура управління, яка представлена на рис. 1.7.

Перед ІТ-компаніями в сучасній економічній системі одним із найважливіших завдань є правильне і доцільне здійснення управління. Сучасний економічний розвиток і тренд здорової конкуренції на підприємстві з застосуванням прогресивних форм і методів господарювання, діяльності на світовому ринку і ефективній інтеграції створює ширші можливості для менеджменту компанії. Для цього треба мати практичні навички і глибоке володіння наукою знаннями. Зазначені відносини є рушійним фактором економічного розвитку високих технологій у господарських суб'єктах, виступає важливим фактором її реалізації. Ось чому крім характеру та змістом управління інформаційними системами в сучасну епоху є параметри впливу цієї галузі на суб’єктів господарювання, їх регулятивна та стимулююча дія, а інформацію цих відносин необхідно вивчати, так як вона впливає на розвиток ІТ-технології.

Оцінка ефективності використання інформаційних ресурсів є дуже важливою, а її реалізація потребує підготовки спеціалістів з достатньо високими управлінськими навичками [5].

Організаційні структури підрозділів ТОВ "Українські інформаційні технології" побудовані за принципом чіткого розмежування підрозділів за сегментами ринку. При цьому сегментація ринку може ґрунтуватися на таких ознаках, як:

- характеристика ІТ-послуг;
- регіональні особливості ІТ-послуг (географічна сегментація) і потреби споживачів (споживчі характеристики).

Передача влади і управління компанією в цьому випадку здійснюється менеджером, який відповідає за взаємодію з певним сегментом ринку.

Ці організаційні структури відносяться до типу лінійного функціоналізму. Функціональна лінійна структура поєднує в собі переваги лінійних і функціональних структур і в даний час набула широкого поширення. У цій структурі разом з виконавчим управлінням створюються спеціалізовані підрозділи на кожному рівні управління, які, на відміну від штабів, мають певні права по відношенню до підлеглих підрозділів.

Лінійні керівники координують діяльність функціональних підрозділів, розробляють рішення для підлеглих підрозділів. При цьому спираються в основному на управлінський вплив - накази і розпорядження. Функціональні служби управляють по лінії функціонального підпорядкування за допомогою інструкцій, правил, рекомендацій, норм, стандартів і т. Д. При цьому афілійовані служби повинні вважати свої вказівки обов'язковими. Тому лінійна функціональна структура має чітку ієрархічну структуру, в якій ланки управління об'єднані вертикально, при цьому існують чітко виражені функціональні ознаки діяльності менеджерів певного управлінського рівня в результаті горизонтального поділу праці.

Лінійні функціональні структури мають свої позитивні сторони: вони стимулюють спеціалізацію, покращують координацію дій у функціональних підрозділах. У компаніях, побудованих за таким принципом, більш ефективний контроль витрат (можливо ефективне використання функціонального аналізу витрат в обліку витрат), вони більш гнучка підлаштовуються під вимоги ринку, в таких структурах полегшується координація дій в підрозділах (рис. 1.7).

Недоліком цієї структури є захоплення функціональних служб прямими вказівками, наказами, збільшення їх кількості, крім того, може виникнути конкуренція всередині організації через конфлікт інтересів окремих підрозділів.

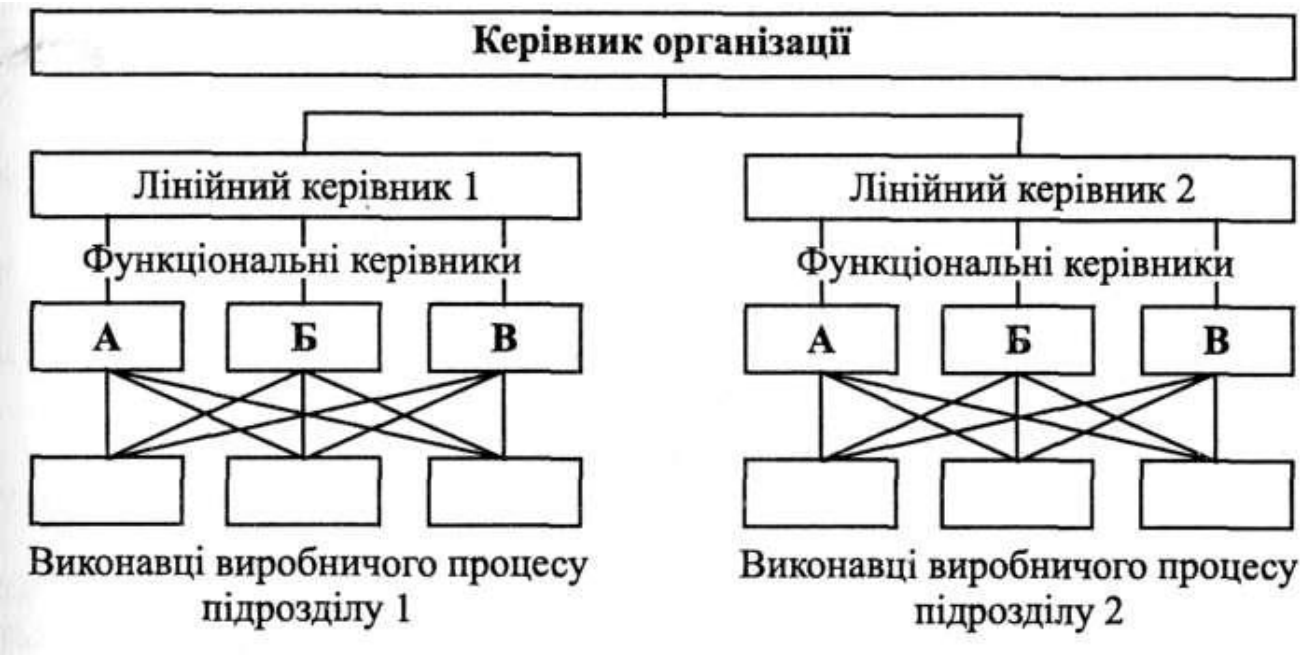


Рисунок 1.7 – Організаційна структура ТОВ "Українські інформаційні технології"

Основною причиною появи лінійних функціональних організаційних структур стало зростання розмірів організацій і спроба розширення в тому випадку, коли компанія орієнтована на випуск однорідної продукції, яку вона пропонує різним географічним сегментам ринку.

1.5.1 Параметри мережі ТОВ «Українські інформаційні технології»

Для вдалого використання організаційної структура слід поєднати команду фахівців ТОВ "Українські інформаційні технології" за допомогою комп’ютерної мережі.

Як визначено завданням до кваліфікаційної роботи для синтезу комп’ютерної системи ТОВ "Українські інформаційні технології" з детальним опрацюванням побудови та налаштування корпоративної мережі маємо наступні початкові дані:

- блок адрес для виділення підмереж: 172.23.IPn.0/21;
- значення IPn блоку адрес виділення підмереж IPn: 192;
- кількості вузлів для мережі LAN1: 45;
- кількості вузлів для мережі LAN2, од.: 25;

– кількості вузлів для мережі LAN3, од.: 88;

– кількості вузлів для мережі LAN4, од.: 9;

– кількості вузлів для мережі LAN5, од.: 44;

– інтенсивність трафіку найбільшої мережі, μ (кадрів/с) : 111.

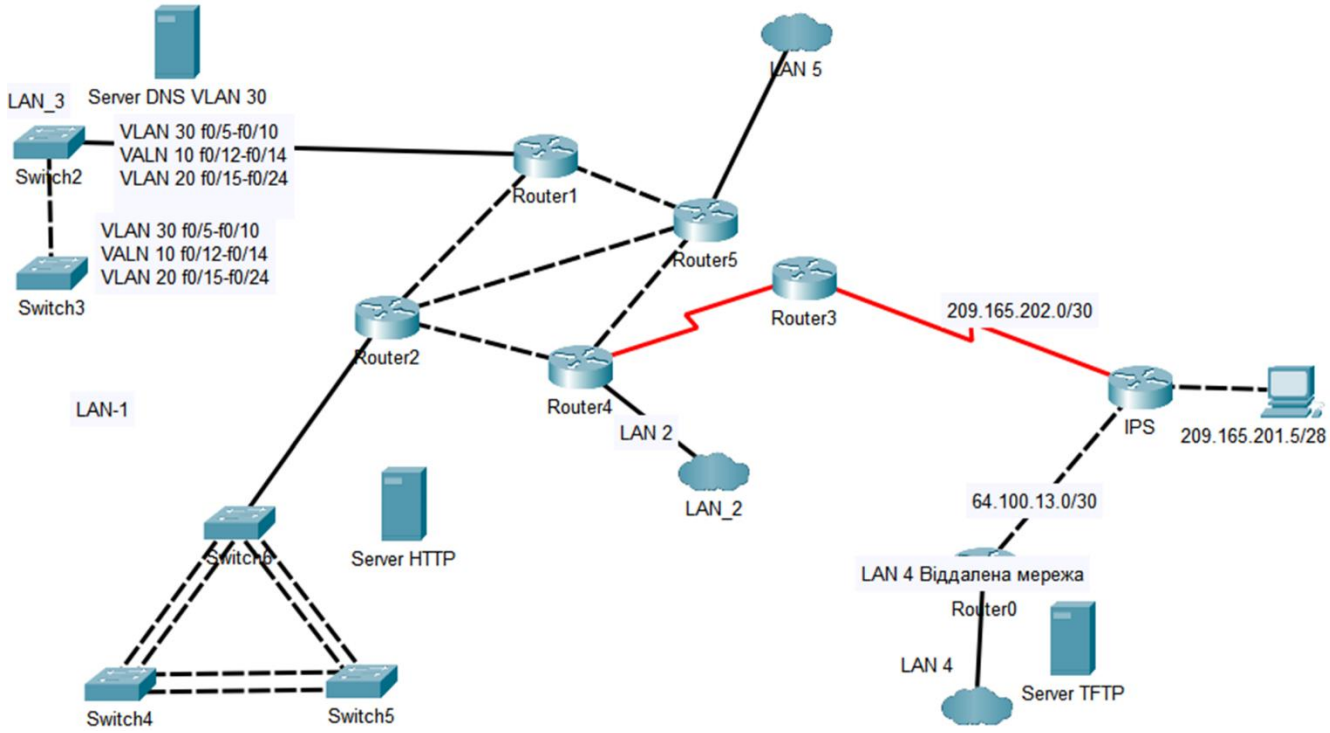


Рисунок 1.8 – Топологія мережі ТОВ «Українські інформаційні технології»

1.6 Постановка завдання

Завданням даної кваліфікаційної роботи є розробка комп'ютерної системи ТОВ «Українські інформаційні технології» з опрацюванням побудови та налаштування корпоративної мережі.

Враховуючи визначену для ТОВ «Українські інформаційні технології» архітектуру мережі, а також кількість підмереж та взаємозв'язки, рекомендовану кількість комп'ютерів та мережевого обладнанням необхідно виконати розрахунок мережі та здійснити налаштування, провести необхідні розрахунки, а також виконати подальше моделювання і перевірку роботи комп'ютерної системи.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП’ЮТЕРНОЇ СИСТЕМИ

2.1 Технічне завдання

2.1.1 Загальні відомості

Замовник (ТОВ "Українські інформаційні технології") доручає Виконавцю (автору кваліфікаційної роботи ступеня бакалавра Турті Дмитру Володимировичу) розробку Проекту СКС ЛОМ (структурована кабельна система локальної обчислювальної мережі), активного та пасивного обладнання.

За запитом Замовника Виконавець надає на погодження спільно зі специфікацією на обладнання та кошторисними розрахунками вартості монтажних та проектних робіт попередній Робочий проект СКС у форматі передбачених норм на таку проектну документацію.

Матеріали та обладнання, що застосовуються, повинні забезпечувати вимоги нормативно-технічних документів з вогнестійкості та пожежної та електротехнічної безпеки, а також електромагнітної сумісності.

Проектування необхідно виконати згідно з чинними документами, нормативами та вимогами, які передбачає законодавство Республіки Білорусь у галузі проектної документації.

Проектування ЛОМ та СКС необхідно здійснювати з урахуванням можливості використання сучасних протоколів зв'язку, можливого розвитку технологій, а також при визначенні кількості автоматизованих робочих місць можливість їх збільшення у зв'язку з розвитком підприємства чи зміни призначення приміщення.

2.1.2 Опис об'єкта проектування

Об'єктом проектування для комп’ютерної системи ТОВ «Українські інформаційні технології» з опрацюванням побудови та налаштування

корпоративної мережі є адміністративна будівля, розташована за юридичним адресом Україна, 79017, львівська обл., місто Львів, вул. Водогінна, 2.

На об'єкті вже існує СКС за попереднім проектом, що підлягає демонтажу силами підрядних організацій і не має враховуватись у поточному проекті.

2.1.3 Структурована кабельна система

Призначення та цілі створення СКС

Структурована кабельна система створюється для забезпечення офісу Замовника слабо-точною кабельною інфраструктурою, на основі якої будується:

- локальна обчислювальна мережа для взаємодії засобів обчислювальної техніки, телекомунікаційних та периферійних пристроїв (ip-телефонів, мережевих принтерів, Wi-Fi точок доступу)
- мережа зв'язку пристроїв відео спостереження
- мережу зв'язку контрольних та виконавчих пристроїв системи контролю доступу.

Вимоги щодо розподілу комунікаційних портів: Кількість портів доступу визначиться затвердженим планом розташування робочих місць, а також кількістю мережевих пристроїв (мережеві принтери, веб-камери, точки доступу Wi-Fi , пристрої контролю доступу, ТБ) Замовника.

2.1.4 Вимоги до горизонтальної підсистеми:

- проект монтажу кабельної системи СКС до робочих місць провести з урахуванням обмежень щодо взаємного розташування силових та інформаційних кабелів пожежної системи безпеки;
- технологія прокладання кабелю повинна забезпечувати збереження естетичного виду приміщень після виконання будівельних та монтажних робіт;

- кабельні траси в приміщеннях повинні прокладатися за фальщ-стелі в металевих лотках сітчастого типу, застосування інших видів кріплення кабельних трас – за погодженням із Замовником;
- топологію розташування кабельних трас узгодити із Замовником на етапі проектування. Визначальними вимогами розробки топології є вимоги щодо забезпечення параметрів СКС. (обмеження робочих довжин);
- кожне робоче місце локальної мережі, позначене як стаціонарне, з боку користувача кінець подвійною розеткою RJ45 Cat.5e, що забезпечує підключення. З боку комутаційного вузла – патч-панеллю RJ45.Cat 5e;
- під час проектування слід враховувати створення додаткових портів для підключення додаткових периферійних пристроїв до локальної мережі (принтерів, ноутбуків, систем зберігання даних, пристроїв доступу, IP-камер).
- довжина сегментів СКС, що виконуються по кабелю типу кручена пара, повинна бути не більше 100 м;
- необхідно дотримуватись умов прокладання кабелів СКС з урахуванням стандартів для конкретних видів кабелів;
- перетин кабельних трас СКС та електроживлення виконувати під кутом 90 град., інакше - узгодити з представником Замовника;
- місце для підключення бездротової точки доступу повинно включати 1 порт локальної мережі з підтримкою POE (Power over Ethernet) і розташоване вище за рівень фальшстелі.

2.1.5 Вимоги до вертикальної підсистеми:

- врахувати у проекті, що з'єднання центрального оптичного кросу (у серверній кімнаті) та вузлів комутації здійснюватимуться за допомогою волоконна-оптичного кабелю;

- термінінація всіх оптичних ліній буде на оптичних патч-панелях 19”, що монтуються у стійку. Тип оптичних роз'ємів узгодити із Замовником на етапі проектування.

2.1.6 Ядро мережі

Розташування центральних оптичних кросів зробити в приміщенні, позначеному Замовником як Серверне (комутаційне), його з'єднання з вузлами комутації виконати за топологією «зірка» оптоволоконними лініями зв'язку. Для резервування кожного вузла комутації має бути протягнуто щонайменше 4 оптичних волокон.

2.1.7 Вузли комутації

При проектуванні місця вузлів комутації погодити із замовником.

Вузли комутації розташувати в спеціалізованих телекомунікаційних настінних шафах, що замикаються. Шафа повинна бути обладнана бічними панелями, профілями, кріпленнями, вентиляторами, розведенням живлення та органайзерами для розведення проводів від патч-панелей до комутатора, з достатнім запасом між напрямними та дверями. Розмірність та комплектація шаф розраховується з можливістю 20% запасу на збільшення портів СКС.

Кабелі від робочих місць термінують на патч-панелі. Панелі потрібно комплектувати органайзерами.

Передбачити 1U місце у настінних шафах для встановлення джерел безперебійного живлення.

2.1.7 Зовнішні підключення

Підключення постачальника інтернет послуг та телефонії до корпоративної мережі передачі даних виконати одномодовим волоконна-оптичним кабелем, що

забезпечує роботу на швидкості 10 Гб/с і має не менше 8 волокон. Тип конекторів узгодити із замовником.

2.2 Вибір апаратних засобів КС

2.2.1 Загальні відомості

Більшість із нас щодня користуються послугами комп’ютерних мереж. Особливо це стосується Інтернету - ми добре знаємо, наскільки він допомагає в навчанні, роботі та спілкуванні з іншими людьми. Глобальна мережа також може дати багато розваг.

Кожен користувач мережі знає, як підключитися до неї, а фахівець знає які пристрої, необхідні для роботи самої мережі. Наведемо огляд матеріалу для вибору на обладнання, необхідного для побудови комп’ютерної мережі, пристроїв, необхідних для керування такою структурою.

Електронні пристрої, що утворюють комп'ютерну мережу, можна розділити на дві групи:

- мережеві пристрої - це ті елементи, які дозволяють пересилати дані через комп'ютерну мережу (комутатори, маршрутизатори тощо),
- кінцеві пристрої - усі пристрої, які спілкуються з мережевими пристроями, тобто використовують мережу або надають її послуги іншим кінцевим пристроям; до цієї групи входять комп’ютери, які виконують роль клієнтів, серверів, ігрових консолей, смартфонів, смарт-телевізорів, принтерів тощо.

Мережева карта (Network Interface Card - NIC) - це елемент мережі або термінальний пристрій, що дозволяє підключати її до комп'ютерної мережі. У випадку з комп’ютерами він має форму плати розширення, яка встановлюється у відповідний роз’єм на материнській платі, або є електронною системою, постійно встановленою на материнській платі.

Рисунок 2.1 - Гігабітна стандартна дротова мережева карта Ethernet

За типом середовища передачі мережеві карти можна розділити на дві групи:

– дротові карти - зазвичай використовуються в настільних комп'ютерах; підключення до мережі здійснюється через виту пару або оптоволокно, якщо мережева карта сумісна зі стандартом Gigabit Ethernet, для підключення використовується кабель вита пара і штекери RJ45;
– бездротові карти - зазвичай використовуються в ноутбуках, телевізорах, ігрових приставках і в смартфонах; дані надсилаються для

Дротовий мережевий адаптер Gigabit Ethernet через радіохвилі з використанням одного зі стандартів Wi-Fi; картки бездротові пристрої можна постійно встановити в пристрій або підключити до нього через порт USB.

Кожна мережева карта, як встановлена на материнській платі, так і підключена до пристрою, має унікальний ідентифікатор - MAC-адрес. Його також називають фізичною адресою пристрою. Такий ідентифікатор присвоюється виробником картки. Завдяки MAC-адресам можна розрізнити підключені до мережі пристрої (ідентифікатор виконує ту ж функцію, що й номер телефону або номер PESEL).

Мережевий комутатор є основним пристроєм, який зазвичай використовується в локальних комп'ютерних мережах. Мережевий комутатор відповідає за виконання багатьох завдань, найважливішою з яких є з'єднання комп'ютерів та інших кінцевих пристроїв в мережі LAN. Якщо ви хочете запустити мережу, що складається з кількох чи дюжини комп’ютерів, ви повинні використовувати комутатор.

Рисунок 2.2 - Мережевий комутатор

Кінцеві пристрої, включені в мережу LAN, підключаються до комутатора через порти. У мережах, побудованих за допомогою витої пари, порти найчастіше мають форму роз'ємів RJ45. Комутатор використовує MAC-адреси підключених мережевих карт для передачі даних між відповідними пристроями.

При виборі комутатора слід враховувати використовуване середовище передачі в Інтернеті. Якщо ви використовуєте кабель типу вита пара, то варто придбати комутатор, адаптований для цього типу підключення (таких моделей у продажу найбільше). Якщо передача даних здійснюється за допомогою оптоволокна, необхідно придбати комутатор, адаптований для роботи з таким середовищем. У цьому випадку слід враховувати збільшені витрати на будівництво мережі - як мережеві карти, так і комутатори, що працюють з оптичними волокнами, однозначно дорожчі, ніж моделі, адаптовані для підключення мідними проводами.

Міст використовується для з’єднання різних сегментів (областей) мережі LAN. Спочатку мости використовувалися, наприклад, для з'єднання двох окремих мереж з різними протоколами передачі, різними середовищами передачі даних і т. д. В даний час пристрої такого типу замінені мережевими комутаторами.

Точка доступу, як і мережевий комутатор, дозволяє кінцевим пристроям підключатися до локальної мережі. Різниця між комутатором і точкою доступу зводиться до використовуваного середовища передачі. Кінцеві пристрої спілкуються з точкою доступу за допомогою радіохвиль.

Рисунок 2.3 - Точка доступу

Після встановлення точки доступу у локальній мережі, ми зможемо підключити до нього кінцеві пристрої за допомогою з технологією Wi-Fi.

Маршрутизатор - це мережевий пристрій, який виконує багато завдань. Дві найважливіші функції:

– підключення різних комп'ютерних мереж;
– вибір маршруту передачі пакетів даних.

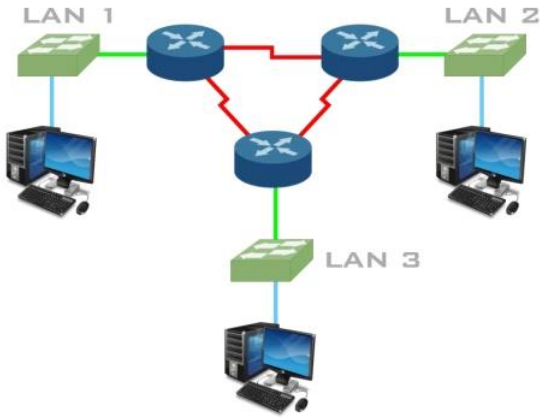


Рисунок 2.4 – Маршрутизатори

Маршрутизатори з’єднують локальні мережі один з одним і можуть передавати дані між пристроями на основі IP-адрес (логічних адрес пристроїв, що працюють у комп’ютерній мережі) між різними комп’ютерними мережами. Якщо ми хочемо з’єднати дві (чи більше) локальні комп’ютерні мережі разом, ми використовуємо маршрутизатор. Це забезпечує передачу даних між кінцевими пристроями, які є частиною різних структур локальної мережі.

Ми також використовуємо роутери вдома: через цей пристрій ми підключаємо власну локальну мережу до Інтернету.

Рисунок 2.5 – Підключення через роутер власної домашньої локальної мережі до Інтернету

Локальна комп’ютерна мережа, підключена до Інтернету через домашній маршрутизатор. Маршрутизатори також утворюють магістраль глобальних мереж. Весь Інтернет побудований прямо зараз від маршрутизаторів. Кожен маршрутизатор зберігає в пам'яті так звану таблицю маршрутизації, яка містить адреси інших мереж (шляхи, що з'єднують його власну мережу з іншими мережами). На основі цих даних маршрутизатор вирішує, яким маршрутом пересилати пакети з мережі джерела в мережу призначення.

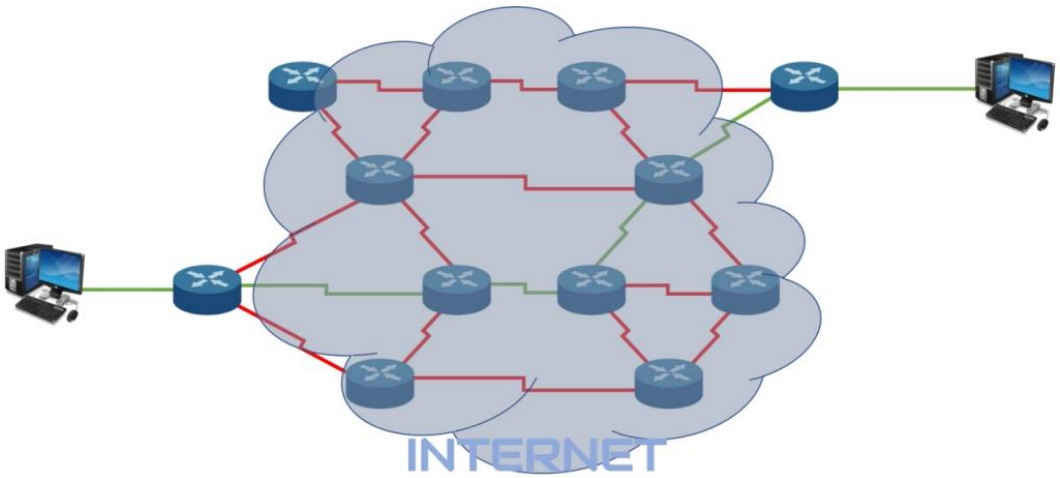


Рисунок 2.6 – Приклад вибору маршруту передачі даних через Інтернет

Брандмауер - це елемент, який захищає комп'ютерну мережу від атак. Брандмауер може блокувати дані, надіслані в мережу ззовні (наприклад, з Інтернету) і таким чином може запобігти хакерським атакам. Брандмауер також може блокувати вихідний трафік з мережі в Інтернет - таким чином ви можете, наприклад, заборонити відвідування вибраних веб-сайтів. Брандмауери мають форму окремих пристроїв або є частиною програмного забезпечення, встановленого на маршрутизаторі чи сервері.

Модем - це пристрій, який перетворює цифровий сигнал в аналоговий і навпаки. Це дозволяє надсилати дані, оброблені комп’ютером або іншим цифровим пристроєм, через аналогові стаціонарні телефонні лінії.

Якщо оператор, у якого ми придбали послугу доступу до Інтернету, має мережеву інфраструктуру на основі аналогових каналів зв’язку, для обміну даними з глобальною мережею доведеться використовувати модем. Коли ми підписуємо договір з оператором, ми зазвичай отримуємо модем – вона здається нам в оренду або продається.

Модем також потрібен, коли ми підключаємося до Інтернету через мобільну мережу (4G або 5G). Цей тип пристрою зазвичай оснащений інтерфейсом USB,

тому його можна підключити безпосередньо до комп’ютера або маршрутизатора, який підтримує модеми мобільних телефонів.

Модеми є автономними пристроями або частиною більш складних мережевих пристроїв.

Рисунок 2.6 – Модем

Багатофункціональні маршрутизатори - це одночасно маршрутизатор, мережевий комутатор і точка доступу (іноді модем). Зазвичай пристрої цього типу називають маршрутизаторами Wi-Fi, оскільки вони виконують кілька завдань, але, перш за все, вони дозволяють підключити вашу локальну мережу до Інтернету.

Рисунок 2.7 – Багатофункціональний маршрутизатор

Адаптер PowerLine - це пристрій, який дозволяє передавати дані між комп’ютерами або іншими кінцевими пристроями через електроустановку. Для роботи такої системи необхідно як мінімум два перехідника. Один з них підключається до розетки живлення і до роутера, який з'єднує локальну мережу з

Інтернетом (адаптер зв'язується з роутером по кабелю типу кручена пара). Другий адаптер підключається до електричної розетки поруч із комп’ютером.

Рисунок 2.8 - Адаптер PowerLine

Підсилювачі також підключаються до адаптера за допомогою витої пари.

Описана система ідеально підходить для великих будівель, наприклад, будинків односімейні будинки, якщо ми не хочемо використовувати мережу Wi-Fi або прокладати мережеві кабелі. Варто зазначити, що до такої мережі можна підключити максимум 16 пристроїв, а сама мережа працюватиме лише на т.зв. одна фаза.

Повторювач використовується для розширення зони дії мережі Wi-Fi в будівлі. Зазвичай такий пристрій підключається безпосередньо до електричної розетки. Репітер бездротовим способом зв'язується з Wi-Fi-роутером, що працює в локальній мережі, і передає свій сигнал. Таким чином ми збільшуємо радіус дії мережі - сам повторювач виконує роль точки доступу для кінцевих пристроїв.

Домашні мережі MESH Домашня мережа MESH складається з пристроїв, які утворюють бездротову «мережу» підключень. Все це нагадує роботу Wi-Fi роутера з підсилювачем - завдання окремих елементів - забезпечити потужний стабільний радіосигнал на всій території обслуговування. Проте мережа MESH - це велика

структура, що складається щонайменше з двох передавачів і програмного забезпечення. Така система в основному використовується, коли місцева радіомережа повинна охоплювати велику територію (наприклад, односімейний будинок або квартиру площею 100 квадратних метрів і більше).

2.2.2 Апаратні засоби комп’ютерної система ТОВ «Українські інформаційні технології»

Відповідно до конкретної задачі розробки комп'ютерної системи ТОВ «Українські інформаційні технології» з детальним вивченням побудови та налаштування корпоративної мережі були обрані наступні апаратні рішення.

Конфігурація цього пристрою буде використана при розробці мережевого проекту для комп'ютерної системи ТОВ «Українські інформаційні технології» в програмному забезпеченні Cisco Packet Tracer.

Для підключення користувачів комп'ютерної системи ТОВ «Українські інформаційні технології» обрано наступні основні компоненти - адаптери, роутери та робочі станції на базі стаціонарних комп’ютерів.

З мережевого обладнання будуть використанні комутатори Catalyst 2960.

Рисунок 2.9 – Вигляд комутаторів Catalyst 2960

Технічні характеристики:

- 24 порти гігабітної мережі Ethernet;
- 64 Мб флеш-пам'яті;
- швидкість передачі даних до 16 Гбіт / с.;
- стандарт 100BASE-TX;

- універсальний порт Ethernet 2 x SFP.

З мережевого обладнання будуть використанні маршрутизатори Cisco 2811 з двома слотами HWIC-2T.

Рисунок 2.10 – Вигляд маршрутизаторів Cisco 2911

До технічних характеристик відносять:

- 3 x інтерфейс Ethernet 10Base-T / 100Base-TX / 1000Base-T, роз'єм RJ-45;
- 1 x гігабітний WAN (RJ-45);
- 1 x гігабітний DMZ (RJ-45);
- швидкість передачі 1 Гбіт / с.;
- протокол Ethernet, Fast Ethernet, Gigabit Ethernet.

В якості робочих станцій обрано HP Z1 G8 TWR/Intel i7-11700/16/512F/NVD RTX3070-8/kbm/W10P.

Рисунок 2.3 – Вигляд робочої станції HP Z1 G8 TWR/Intel i7-11700/16/512F/NVD RTX3070-8/kbm/W10P

Основні показники:

процесор - Intel Core i7;

вага - 5,95 кг;

комплектація - USB клавіатура та USB миша, монітор 27’’;

габарити (ВхШхГ) - 168 х 370 х 308;

звук - HD audio.

2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Для розрахунку ключових характеристик вихідного трафіку, треба щоб мережа ТОВ «Українські інформаційні технології» була завантажена на близько до 100 %.

Вхідні дані наступні:

- найбільша кількість комп’ютерів (хостів) дорівнює Nl = 88, які розташовані у мережі LAN3;
- середній показник інтенсивності трафіку: μ = 111 (кадрів/с);
- розмір повідомлення в середньому: l = 650 байт;
- передача пакету не повинна перевищувати ≤5 мс;
- кількість портів в комутаторі рівня доступу n = 8;
- загальна кількість користувачів (хостів) N = 210.

Вихідний трафік перенаправляється на маршрутизатор по лінії з пропускною здатністю 1000 Мбіт/с.

Пропускна здатність всієї мережі розраховується з урахуванням того, що мережею одночасно користується 100 % користувачів і обчислюється наступним чином:

Пропускна здатність мережі L3 на рівні доступу:

Рр.д= Nl * l * n * 8 = 88 * 650 * 24 * 8 = 10,99 Мбіт/с,

Пропускна здатність мережі на рівні розподілу обчислюється наступним чином. З комутаторами рівня доступу, придатними для одного комутатора рівня розподілу та загалом Nl користувачів, пропускна здатність мережі на рівні розподілу така:

Pp.p = μ * l * Nl *8 = 111 * 650 * 88 * 8 = 50,8 Мбіт/с,

Результати, отримані під час розрахунку, не перевищують зазначених параметрів мережі, тому обране обладнання не буде перевантаженим.

Перемикач рівня розподілу перенаправляє трафік до маршрутизатора через вихідну лінію з пропускною здатністю 1 000 Мбіт/с.

μвих = 1 000 000 000 / (650 * 8) = 192 310 пакетів/с.

Кожне джерело виробляє в середньому 200 пакетів на секунду, що обмежує його до підключення до максимального розподілу на рівні комутації.

Ns = 192 310 / 200 = 961 джерел.

Він заповнює мережу з Nl ПК. Кожен з Nl ПК посилає потік заявок з інтенсивністю 200 кадрів / с.

Інтенсивність вихідного трафіку від всіх користувачів:

λ = N * μ = 88 * 200 = 17 600 (пакетів/с).

Коефіцієнт затримки на рівні розподілу, показник навантаження на вихідний канал зв'язку, що впливає на затримку черги.

ρ= λ / μвих = 17 600/ 192 310 = 0,091

Коефіцієнт зайнятості комутатора рівня розподілу:

r = ρ / (1 – ρ) = 0,076 / (1 - 0,076) = 0,082

Середня затримка кадру, пов’язана з чергою M/M/1, становить:

T=1 / (μ - λ) = 1 / (192 310 - 17 600) = 5,72 мкс.

Середня довжина черги:

L_чер=ρ^2/(1-ρ)=0,076 * 0,076/(1-0,076)=0,0062

Ця цифра корисна під час черги пристрою. В апаратному забезпеченні можна вказати максимальний розмір черги пакетів.

Середній час пакетів у черзі:

$T\_чер = L\_чер / \lambda = 0,0062 / 17\ 600 = 0,35$ мкс.

Це значення менше необхідного значення ≤ 5 мс, що відповідає вимогам.

Пропускна здатність каналу:

λ = (пропускна здатність) / (довжина кадру) = b / l.

$b = \lambda * l = 17\ 600*650*8 = 91,52$ Мбіт/с.

Середнє значення пропускної здатності каналу розраховано та відповідає пропускній здатності вихідного каналу 1 000 Мбіт/с.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Адресація в корпоративній мережі

3.1.1 Завдання

Згідно з завданням до теми кваліфікаційної роботи бакалавра «комп'ютерна система ТОВ «Українські інформаційні технології» з опрацюванням побудови та налаштування корпоративної мережі» слід використати наступні початкові дані для синтезу мережі:

- блок адрес для виділення підмереж: 172.23.IPn.0/21;
- значення IPn блоку адрес виділення підмереж IPn: 192;
- кількості вузлів для мережі LAN1: 45;
- кількості вузлів для мережі LAN2, од.: 25;
- кількості вузлів для мережі LAN3, од.: 88;
- кількості вузлів для мережі LAN4, од.: 9;
- кількості вузлів для мережі LAN5, од.: 44;
- інтенсивність трафіку найбільшої мережі, μ (кадрів/с) : 111.

Розподіл мереж між маршрутизаторами (WAN):

- блок адрес для каналів між маршрутизаторами 172.23.IPn.0/21;
- номер варіанту № 18;
- перші IP-адреси призначати інтерфейсам і під-інтерфейсам маршрутизаторів у LAN;
- інші IP-адрес призначати комутаторам у LAN;
- адреса серверів: останній можливий адресу у мережі.
- адреса вузлів: інші з використаних;
- в мережах VLAN використовувати адресацію кінцевих пристроїв за протоколом DHCP.

Враховуючи визначену для комп’ютерної системи ТОВ «Українські інформаційні технології» архітектуру мережі, а також кількість підмереж та взаємозв’язки, рекомендовану кількість комп’ютерів та мережевого обладнанням необхідно виконати розрахунок мережі та здійснити налаштування, провести необхідні розрахунки, а також виконати подальше моделювання і перевірку роботи комп’ютерної системи. Для заданих мереж треба розрахувати діапазони можливих IP-адресів.

3.1.2. Структурована кабельна система

Структурована кабельна система (СКС) – система, призначена для об'єднання інформаційних потоків за допомогою кабельних трас та телекомунікаційного обладнання.

Структурована кабельна система (СКС) – закінчена сукупність кабелів зв'язку та комутаційного обладнання, що відповідає вимогам відповідних нормативних документів. Включає набір кабелів і комутаційних елементів та методику їх спільного використання.

Мережі СКС та ЛОМ, кабельні мережі дозволяють об'єднати багато інформаційних систем:

- телефонію;
- локальні обчислювальні мережі (зокрема і Wi-Fi мережі);
- відеоспостереження;
- системи контролю доступу, обліку робочого часу та домофонію;
- системи охоронної та пожежної сигналізації;
- мультимедійні системи;
- системи озвучування.

Універсальність, масштабованість, простата обслуговування та ремонту - основні переваги структурованої кабельної системи (СКС мережу).

Локальна обчислювальна мережа (ЛВС, Local Area Network, LAN) - найпоширеніша комп'ютерна мережу, що у більшості компаній.

Завдання організації ЛОМ:

- збереження та резервування інформації;
- оперативний обмін даними між користувачами та комутаційними вузлами;
- підключення до робочих комп'ютерів периферійних пристроїв (МФУ, принтери, факси та інше обладнання);
- централізоване використання системних програм всім користувачів;
- захист даних від несанкціонованого доступу до ЛОМ, захист самої локальної мережі від злому.

Найпоширеніші категорії СКС, ЛОМ:

- CAT 5e - найпоширеніший варіант у корпоративному сегменті; частота - 125 MHz. Швидкість - 100 Мб/с (2 пари) та 1000 Мб/с (4 пари); підходить для об'єктів, де не планується зростання трафіку та швидкості (системи відеоспостереження, IP-телефонія, «розумний дім», комп'ютерна мережа невеликого офісу.

CAT 6 - найпопулярніша категорія при будівництві нових об'єктів; частота передачі даних – 250 МГц; Швидкість передачі до 10 Гб/с на відстань до 55 м;

CAT 6a -покращена версія CAT 6; швидкість інфопотоку – 10 Гб/с на смузі частот 500 МГц. дальність передачі – до 100 метрів; використовується на об'єктах з високою концентрацією трафіку: ЦОД (центри обробки даних), міських мережах та магістралях.

Насправді, кабельні системи локальних комп'ютерних мереж можна розділити різні групи. Існують кручена пара, екранована та неекранована кручена пара (часто звана STP і UTP або також lOBaseT) та оптоволоконні кабелі. Вибір правильної кабельної системи зазвичай визначається типом створюваної мережі та умовами, встановленими користувачами.

Бездротові (Wi-Fi) мережі.

Позитивні сторони:

- відсутні будь-які кабелі;
- монтажних робіт майже немає;
- зручно використовувати там, де важко прокласти кабель;
- легкість перенесення мережі до іншого приміщення;
- є можливість підключення мобільних пристроїв.

Негативні сторони:

Дороге обладнання;

- можливі завади, якщо сигнал проходить через вулицю;
- є ймовірність зламування мережі, якщо безпека буде налаштована погано.

3.1.3 IP-Адресація в комп'ютерній мережі

IP-адреса - це унікальний числовий ідентифікатор, який призначається кожному пристрою, підключеному до комп'ютерної мережі, яка використовує для зв'язку Інтернет-протокол.

IP-адреса – це унікальний набір чисел, який ідентифікує пристрій у мережі, наприклад телефон або комп'ютер. Це як номер телефону, який дозволяє пристроям спілкуватися один з одним через комп'ютерну мережу.

IP-адреса - це унікальний ідентифікатор, який призначається кожному пристрою, підключеному до комп'ютерної мережі. Він служить цифровою адресою, яка дозволяє пристроям спілкуватися один з одним через комп'ютерну мережу. Абревіатура IP означає Інтернет-протокол, набір правил і процедур, які регулюють передачу даних через Інтернет.

Кожному пристрою, підключеному до комп'ютерної мережі, будь то комп'ютер, смартфон або пристрій IoT, призначається IP-адреса. Ця адреса використовується для ідентифікації пристрою та маршрутизації інформації до та від

нього. IP-адреси є важливими для спілкування через комп’ютерну мережу, оскільки вони дозволяють пристроям надсилати та отримувати пакети даних від інших пристроїв у мережі. Без IP-адрес пристрої не могли б спілкуватися один з одним через комп’ютерну мережу.

IP-адреса або адреса Інтернет-протоколу – це унікальний ідентифікатор, призначений кожному пристрою, підключеному до мережі за допомогою протоколу TCP/IP. Це 32- або 128-розрядний номер, який використовується для ідентифікації пристрою в мережі та полегшення зв’язку між пристроями. IP-адреси представлені у двійковому або десятковому форматі.

Існує два типи IP-адрес: загальнодоступні та приватні. Загальнодоступні IP-адреси призначаються Управлінням розподілення номерів в Інтернеті (IANA) і використовуються для ідентифікації пристроїв у загальнодоступному Інтернеті. Приватні IP-адреси використовуються для ідентифікації пристроїв у приватній мережі, і до них неможливо отримати доступ із загальнодоступного пристрою комп’ютерної мережі.

Загальнодоступні IP-адреси є унікальними та розпізнаються у всьому світі, тоді як приватні IP-адреси унікальні лише в межах певної мережі та не розпізнаються у всьому світі. Загальнодоступні IP-адреси використовуються для доступу до Інтернету, тоді як приватні IP-адреси використовуються для полегшення зв’язку між пристроями в приватній мережі.

Статичні IP-адреси призначаються пристрою вручну та залишаються фіксованими, а динамічні IP-адреси призначаються сервером DHCP і можуть змінюватися з часом. Статичні IP-адреси зазвичай використовуються для серверів та інших пристроїв, яким потрібна постійна адреса, тоді як динамічні IP-адреси використовуються для пристроїв, яким не потрібна постійна адреса.

IP-адреси є важливим компонентом комп’ютерної мережі. Вони дозволяють пристроям спілкуватися один з одним і підключатися до комп’ютерної мережі.

Маршрутизація - це процес пересилання пакетів даних з однієї мережі в іншу. IP-адреси відіграють важливу роль у маршрутизації, визначаючи джерело та призначення пакетів даних. Кожен пристрій, підключений до мережі, має унікальну IP-адресу, яка допомагає маршрутизаторам визначати, куди надсилати пакети даних.

Постачальники послуг Інтернету (ISP) і сервери відіграють важливу роль у роботі IP-адрес. Інтернет-провайдери призначають IP-адреси пристроям, підключеним до їхньої мережі, тоді як сервери використовують IP-адреси для зв'язку з іншими пристроями в Інтернеті. Наприклад, DNS-сервери використовують IP-адреси для перетворення доменних імен на IP-адреси.

IP-адреси полегшують зв'язок між пристроями в комп'ютерній мережі. Коли пристрій хоче зв'язатися з іншим пристроєм, він надсилає пакет даних, що містить IP-адресу призначення. Маршрутизатори використовують цю IP-адресу для визначення найефективнішого маршруту для досягнення пакетом даних місця призначення.

IP-адреси також відіграють важливу роль у встановленні з'єднань між пристроями за допомогою протоколу TCP/IP. Протокол TCP використовує IP-адреси для визначення джерела та призначення пакетів даних і забезпечення їх надійної передачі.

У результаті IP-адреси є важливим компонентом комп'ютерної мережі та відіграють важливу роль у маршрутизації, Інтернет-провайдерах і серверах, а також у зв'язку. Вони дозволяють пристроям спілкуватися один з одним і підключатися до Інтернету, перетворюючи Інтернет на глобальну мережу взаємопов'язаних пристроїв.

Коли справа доходить до налаштування IP-адреси, існує два основних типи: динамічна та статична. У цьому розділі ми розглянемо обидва типи конфігурацій і те, як їх налаштувати за допомогою різних методів.

Динамічні IP-адреси автоматично призначаються сервером DHCP, коли пристрій підключається до мережі. Це найпоширеніший тип конфігурації IP-адреси, оскільки його легко налаштувати та керувати ним. Коли пристрій підключається до мережі, він надсилає запит на IP-адресу на сервер DHCP. Потім сервер призначає доступну IP-адресу пристрою.

Динамічні IP-адреси корисні для мереж із великою кількістю пристроїв, оскільки вони дозволяють ефективно використовувати доступні IP-адреси. Вони також корисні для пристроїв, які часто переміщуються між мережами, таких як ноутбуки та смартфони.

Статичні IP-адреси призначаються пристрою вручну. Цей тип конфігурації є менш поширеним, оскільки вимагає більше зусиль для налаштування та керування. Однак статичні IP-адреси корисні для пристроїв, яким потрібна фіксована IP-адреса, наприклад серверів і принтерів.

Щоб налаштувати статичну IP-адресу, вам потрібно знати IP-адресу, маску підмережі, шлюз за замовчуванням і адресу DNS-сервера для вашої мережі. Потім ви можете вручну ввести ці значення в налаштування мережі пристрою.

Операційні системи Windows і Linux забезпечують інтерфейси командного рядка, які дозволяють налаштовувати IP-адреси за допомогою командного рядка або терміналу. Ви можете використовувати команду ipconfig для перегляду та налаштування IP-адрес у Windows. У Linux ви можете використовувати команду ifconfig для тієї ж мети.

Настільні та мобільні операційні системи також забезпечують графічний інтерфейс користувача для налаштування IP-адрес. У Windows ви можете отримати доступ до параметрів мережі, клацнувши піктограму мережі на панелі завдань і вибравши «Параметри мережі та Інтернету». У macOS ви можете отримати доступ до мережевих налаштувань, відкривши Системні налаштування та натиснувши Мережа.

Смартфони, планшети та смарт-телевізори також мають графічний інтерфейс для налаштування параметрів мережі. Зазвичай ці налаштування можна знайти в меню пристрою «Налаштування».

Таким чином, налаштування IP-адреси можна виконувати динамічно або статично за допомогою різних методів, таких як командний рядок, термінал або графічний інтерфейс користувача. Динамічні IP-адреси призначаються автоматично сервером DHCP, тоді як статичні IP-адреси призначаються вручну. Обидва типи конфігурації мають свої переваги та недоліки залежно від вимог пристрою та мережі.

IP-адреса може використовуватися як ідентифікатор для кіберзлочинців для відстеження та націлювання на окремих осіб. Кіберзлочинці можуть використовувати IP-адреси для здійснення таких атак, як DDoS (розподілена відмова в обслуговуванні), фішинг і розповсюдження шкідливого програмного забезпечення. Кіберзлочинці також можуть використовувати IP-адреси для доступу до особистої інформації, крадіжки даних і крадіжки особистих даних.

IP-адреси можуть розкривати багато інформації про онлайн-діяльність людини, зокрема веб-сайти, які вони відвідують, їхнє місцезнаходження та пристрої, якими вони користуються. Це може бути серйозною проблемою щодо конфіденційності, особливо коли IP-адреса пов’язана з конфіденційною особистою інформацією.

Для захисту конфіденційності можна використовувати такі інструменти, як віртуальні приватні мережі (VPN) і проксі-сервери. Ці інструменти можуть маскувати вашу IP-адресу та шифрувати вашу онлайн-діяльність, що ускладнює для кіберзлочинців відстеження та націлювання на вас.

Є кілька інструментів і ресурсів, доступних для перевірки вашої IP-адреси та захисту вашої конфіденційності. Деякі популярні інструменти включають IP Chicken і WhatIsMyIPAddress.com, які дозволяють перевірити вашу IP-адресу та місцезнаходження.

Якщо ви турбуєтеся про свою конфіденційність в Інтернеті, ви також можете скористатися такими інструментами, як браузер Tor, який шифрує вашу онлайн-діяльність і направляє її через мережу серверів, щоб захистити вашу особу та місцезнаходження.

Крім того, важливо знати різницю між спільними IP-адресами та приватними IP-адресами. Спільні IP-адреси використовуються кількома користувачами, що може ускладнити відстеження окремих користувачів. Приватні IP-адреси використовуються одним користувачем, і їх легше пов’язати з особистою інформацією.

Загалом, важливо знати про ризики для безпеки та конфіденційності, пов’язані з IP-адресами, і вживати заходів для захисту своєї діяльності в Інтернеті.

3.1.4 Маска IP-адресів в комп’ютерній мережі

Підмережі — це метод поділу великої мережі на менші мережі. З іншого боку, супермережі - це техніка, яка використовується для з’єднання менших діапазонів адрес у більший. Надмережа розроблена, щоб зробити процес маршрутизації більш зручним. Крім того, стискання зменшує розмір даних таблиці маршрутизації, щоб вона могла займати менше місця в пам’яті. Чітко визначений метод створення підмереж - це FLSM і VLSM із використанням CIDR для масштабування.

Маски CIDR і VLSM - це чітко визначені терміни, що використовуються під час проектування мережі, де CIDR використовується для об'єднання шляхів для зменшення кількості інформації про маршрутизацію, що надсилається базовими маршрутизаторами. Навпаки, VLSM полегшує оптимізацію доступного адресного простору.

CIDR є прямою протилежністю VLSM, описуючи правила довідки для мереж, які використовують однопрохідний оператор. Замість цього VLSM встановлює правила розділення мереж.

CIDR (Non-Class Domain Routing) не використовує мережеві ідентифікатори на основі класів, оскільки, як ми знаємо, класичні адреси мали обмеження: публічні IP-адреси менші, ніж суспільний попит на публічні адреси (для використання в Інтернеті). Спочатку він був розроблений, щоб дозволити провайдерам виділяти менші або більші блоки IP-адрес замість класів. Він також відомий як короткий зміст треку.

VLSM (Hide Variable Length Subnet) - це метод ідентифікації хост-області різного розміру між мережами шляхом розбиття мережі на кілька підмереж. В основному він призначений для забезпечення більшої гнучкості в налаштуванні сітки за допомогою різних масок.

Підмережі та супермережі - це методи, винайдені для вирішення проблеми вичерпання адрес. Хоча цей метод не вирішив проблему, він зменшив швидкість вичерпання адреси. Надмережа - процес, зворотний до підмережі.

Таблиця 3.1 - Порівняльна таблиця

Показник порівняння	Підмережа	Супермережа
Головна	Процес поділу мережі на підмережі.	Процес об'єднання малих мереж у більшу мережу.
Процедура	Збільшується кількість біт в мережевих адресах.	Розрядність адрес хостів збільшується.
Біти маски переміщено правильно	Права частина маски за замовчуванням.	Зліва від маски за замовчуванням.
додаток	VLSM (маскування підмережі змінної довжини).	CIDR (безкласова міждоменна маршрутизація).
призначення	Використовується для зменшення вичерпання адреси.	Спростіть і закрийте процес маршрутизації.

3.1.5 Розрахунок комп’ютерної мережі

Виконаємо розподіл адресів в мережі для комп’ютерної системи ТОВ «Українські інформаційні технології» з застосуванням маскування підмережі зі

змінною довжиною (VLSM), що є більш ефективним способом розподілу мережі. на підмережі.

Використовуючи VLSM калькулятор можна швидко та ефективно налаштувати мережу.

Кількість вузлів в підмережах початкових даних наведено табл. 3.1.

Таблиця 3.1 – Кількість вузлів в підмережах

LAN1	LAN2	LAN3	LAN4	LAN5
45	25	88	9	44

Результат розрахунку для мережі з використанням блоку адрес 172.23.192.0/21 для каналів між маршрутизаторами показав, що максимальна кількість можливих хостів становить 2046, а для нашого варіанту підмережі потрібно лише 211 хостів. Результат розподілу підмереж LAN1…LAN5 представлено в табл. 3.3.

Розрахуємо адресацію між маршрутизаторами. Враховуючі максимальну кількість вузлів в підмережі WAN, яка дорівнює. 2, можна застосувати замість блока адрес 172.23.18.0/21 блок адрес 172.23.18.0/30. Визначення підмереж між маршрутизаторами наведено на рис. 3.1. Результат розподілу підмереж WAN1…WAN7 представлено в табл. 3.3.

Розрахуємо адресацію LAN3 для в підмережі VLAN з 88 комп’ютером із застосуванням заданого блоку адрес 172.23.0.0/25.

Результат розподілу для 4 підмереж VLAN10, VLAN20, VLAN30 та VLAN40 представлено в табл. 3.3.

Схема адресації пристроїв мережі наведена в табл. 3.4.

3.2 Розробка топологічної схеми корпоративної мережі

Розроблена топологічна схема ТОВ «Українські інформаційні технології» представлена на рис. 3.1.

Таблиця 3.2 – Розподіл адресів для підмереж LAN1…LAN5

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast
LAN3	88	126	38	172.23.0.0	/25	255.255.255.128	172.23.0.1 - 172.23.0.126	172.23.0.127
LAN1	45	62	17	172.23.0.128	/26	255.255.255.192	172.23.0.129 - 172.23.0.190	172.23.0.191
LAN5	44	62	18	172.23.0.192	/26	255.255.255.192	172.23.0.193 - 172.23.0.254	172.23.0.255
LAN2	25	30	5	172.23.1.0	/27	255.255.255.224	172.23.1.1 - 172.23.1.30	172.23.1.31
LAN4	9	14	5	172.23.1.32	/28	255.255.255.240	172.23.1.33 - 172.23.1.46	172.23.1.47

Таблиця 3.3 – Розподіл адресів для підмереж WAN1…WAN5

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast
WAN1	2	2	0	172.23.18.0	/30	255.255.255.252	172.23.18.1 - 172.23.18.2	172.23.18.3
WAN2	2	2	0	172.23.18.4	/30	255.255.255.252	172.23.18.5 - 172.23.18.6	172.23.18.7
WAN3	2	2	0	172.23.18.8	/30	255.255.255.252	172.23.18.9 - 172.23.18.10	172.23.18.11
WAN4	2	2	0	172.23.18.12	/30	255.255.255.252	172.23.18.13 - 172.23.18.14	172.23.18.15
WAN5	2	2	0	172.23.18.16	/30	255.255.255.252	172.23.18.17 - 172.23.18.18	172.23.18.19
WAN6	2	2	0	172.23.18.20	/30	255.255.255.252	172.23.18.21 - 172.23.18.22	172.23.18.23
WAN7	2	2	0	209.165.202.0	/30	255.255.255.252	209.165.202.1 - 209.165.202.2	209.165.202.3
WAN7	2	2	0	64.100.13.0	/30	255.255.255.252	64.100.13.1 - 64.100.13.2	64.100.13.3

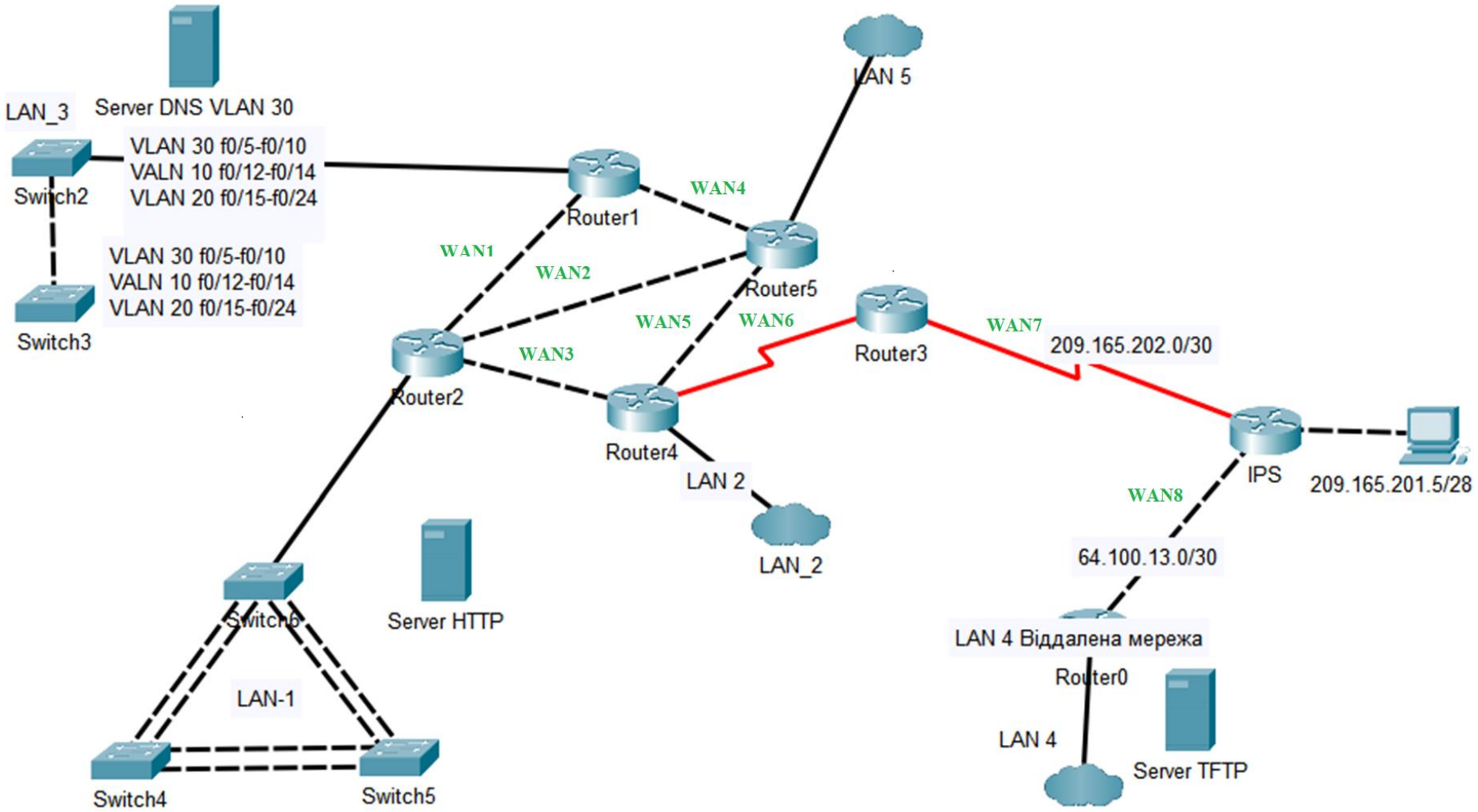


Рисунок 3.1 – Визначення підмереж WAN між маршрутизаторами

Таблиця 3.4 – Схема адресації підмережі мережі VLAN

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast
VLAN20	30	30	0	172.23.0.0	/27	255.255.255.224	172.23.0.1 - 172.23.0.30	172.23.0.31
VLAN10	29	30	1	172.23.0.32	/27	255.255.255.224	172.23.0.33 - 172.23.0.62	172.23.0.63
VLAN30	29	30	1	172.23.0.64	/27	255.255.255.224	172.23.0.65 - 172.23.0.94	172.23.0.95
VLAN40	22	30	8	172.23.0.96	/27	255.255.255.224	172.23.0.97 - 172.23.0.126	172.23.0.127

Таблиця 3.4 – Схема адресації підмережі мережі IPS

Name	Hosts Needed	Hosts Available	Unused Hosts	Network Address	Slash	Mask	Usable Range	Broadcast
IPS	20	28	8	209.165.201.0	/28	255.255.255.240	209.165.201.1 - 209.165.201.30	209.165.201.31

Таблиця 3.5 – Схема адресації пристроїв мережі

Ім'я пристрою	Інтерфейс	IP-адреса	Маска	Шлюз
Маршрутизатори				
Turta_R0	Fa0/0	172.23.1.33	/28	-
	Se0/1/0	64.100.13.1	/30	-
Turta_R1	Fa0/0	172.23.0.1	/25	-
	Se0/1/0	172.23.18.2	/30	-
	Se0/1/1	172.23.18.13	/30	-
Turta_R2	Fa0/0	172.23.0.129	/26	-
	Se0/1/0	172.23.18.1	/30	-
	Se0/1/1	172.23.18.9	/30	-
	Se0/3/0	172.23.18.5	/30	-
Turta_R3	Se0/1/0	172.23.18.22	/30	-
	Se0/1/1	209.165.202.1	/30	-
Turta_R4	Fa0/0	172.23.1.1	/27	-
	Se0/1/0	172.23.18.17	/30	-
	Se0/3/0	172.23.18.21	/30	-
Turta_R5	Fa0/0	172.23.0.193	/26	-
	Se0/1/0	172.23.18.14	/30	-
	Se0/1/1	172.23.18.17	/30	-
	Se0/3/0	172.23.18.6	/30	-
Turta_SPS	Fa0/0	209.165.201.1	/28	-
	Se0/1/0	209.165.202.2	/30	-
	Se0/1/1	64.100.13.2	/30	-
LAN1				
L1PC0	Fa0	172.23.0.130	/26	172.23.0.128
L1PC1	Fa0	172.23.0.131	/26	172.23.0.128
L1PC2	Fa0	172.23.0.132	/26	172.23.0.128
Server_HTTP	Fa0	172.23.0.90	/26	172.23.0.128
LAN2				
L2PC0	Fa0	172.23.1.2	/27	172.23.1.0
L2PC1	Fa0	172.23.1.3	/27	172.23.1.0

Продовження таблиці 3.5

L2PC1	Fa0	172.23.1.04	/27	172.23.1.0
LAN3				
L3PC0	Fa0	172.23.0.34	/27	172.23.0.32
L3PC1	Fa0	172.23.0.35	/27	172.23.0.32
L3PC2	Fa0	172.23.0.2	/27	172.23.0.0
L3PC3	Fa0	172.23.0.3	/27	172.23.0.0
L3PC4	Fa0	172.23.0.66	/27	172.23.0.64
L3PC5	Fa0	172.23.0.67	/27	172.23.0.64
L3PC6	Fa0	172.23.0.98	/27	172.23.0.96
L3PC7	Fa0	172.23.0.99	/27	172.23.0.96
Server_DNS	Fa0	172.23.0.126	/27	172.23.0.96
LAN4				
L4PC0	Fa0	172.23.1.34	/28	172.23.1.32
L4PC1	Fa0	172.23.1.35	/28	172.23.1.32
L4PC2	Fa0	172.23.1.36	/28	172.23.1.32
Server_TFTP	Fa0	172.23.1.46	/28	172.23.1.32
LAN5				
L5PC0	Fa0	172.23.0.194	/26	172.23.0.192
L5PC1	Fa0	172.23.0.195	/26	172.23.0.192
L5PC2	Fa0	172.23.0.196	/26	172.23.0.192
Provider				
LIPS_PC0	Fa0	209.165.201.2	/28	209.165.201.0
LIPS_PC1	Fa0	209.165.201.3	/28	209.165.201.0
LIPS_PC2	Fa0	209.165.201.4	/28	209.165.201.0
LIPS_PC2	Fa0	209.165.201.5	/28	209.165.201.0

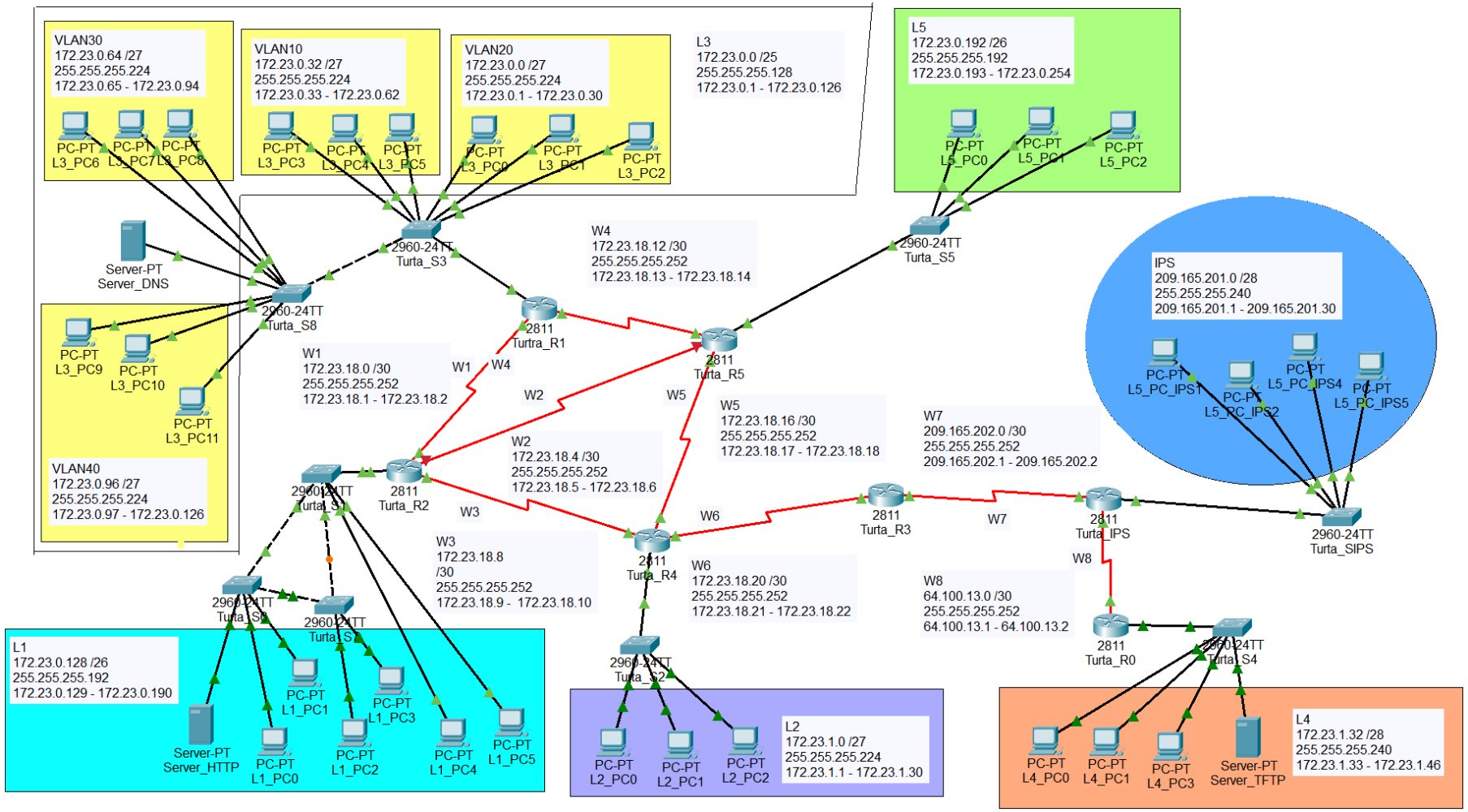


Рисунок 3.2 – Мережа комп’ютерної система ТОВ «Українські інформаційні технології»

3.3 Розрахунок налаштувань маршрутизації корпоративної мережі

3.3.1 Загальні відомості про протоколи маршрутизації

EIGRP і OSPF - це внутрішні протоколи маршрутизації комутатора, які допомагають вибирати маршрути для передачі або розподілу даних шляхом взаємодії з маршрутизаторами. Перший протокол, EIGRP, використовує протокол дистанційної векторної маршрутизації, а другий, OSPF, використовує протокол пересилання за станом зв'язку.

Однак здатність EIGRP і OSPF вивчати динамічні маршрути для мережі функціонально еквівалентна, але між ними є кілька відмінностей. Спеціальний IGP Cisco, наприклад EIGRP, популярний лише в мережах Cisco. З іншого боку, OSPF є відкритими стандартами IGP для корпоративної мережі.

Таблиця 3.6 – Порівняння протоколів маршрутизації для комутатора

Основа для порівняння	EIGRP	OSPF
Це означає	Розширений протокол внутрішнього шлюзу	Спочатку відкрийте найкоротший шлях
На основі стандартів	Власність Cisco	Відкритий стандарт IETF
Тип протоколу	Гібрид	Статус підключення
Вимірювання маршруту	Поєднання пропускної здатності, надійності, навантаження та затримки.	Пропускна здатність інтерфейсу
Адміністративна дистанція	90 (внутрішній) 170 (зовнішній)	110
Вимоги до ЦП	Низькі вимоги до ЦП і пам'яті	Потрібні потужні процесор і пам'ять
Алгоритм	Попарний вектор відстані	Стан підключення Дейкстри
Ієрархічний дизайн	ні	Так
Підтримка IPX і AppleTalk	Так	ні
Оновлення	Оновлення та запити за потреби для багатоадресної адреси	За потреби періодично передавати на кілька широкомовних адрес
Простота застосування	Легко, але без автоматичного підсумку	Це складно
Запобігання петлям	Роздвоєний горизонт і ДУАЛ	Повна інформація про топологію
Фільтрування та підсумовування	Доступно будь-де в мережі	Тільки на ASBR або ABR

EIGRP (Advanced Gateway Routing Protocol) - це дистанційний векторний протокол на основі Cisco, який працює на DUAL (алгоритм оновлення) . Він використовується для пересилання інформації на сусідні маршрутизатори, які знаходяться в тій самій зоні. Хоча це складний протокол, ми можемо легко налаштувати та запустити його в малих і великих мережах. Він був розроблений, щоб подолати недоліки класичних протоколів дистанційної векторної маршрутизації, таких як IGRP і RIP, які важко масштабувати відповідно до потреб мережі.

EIGRP вважається гібридом, оскільки він поєднує функції дистанційної векторної маршрутизації та протоколу пересилання стану зв’язку. Подібно до протоколу дистанційної векторної маршрутизації, EIGRP отримує оновлення від своїх сусідів. Подібним чином EIGRP підтримує топологічну таблицю оголошених маршрутів і використовує алгоритм дифузійного оновлення (DUAL), щоб вибрати шлях без розривів як протокол стану з’єднання.

Перш ніж зрозуміти конвергенцію в EIGRP, нам потрібно зрозуміти, що таке конвергенція. Час конвергенції мережі – це час, який потрібен усім маршрутизаторам у мережі, щоб прийняти зміну мережі. Якщо час конвергенції невеликий, маршрутизатор може швидко адаптуватися до зміни топології мережі. EIGRP не надсилає повні періодичні оновлення маршруту, тому він має швидкий час конвергенції. Оскільки EIGRP не знає про всі мережеві підключення, він покладається на оголошення сусідів.

OSPF (Open Shortest Path First) також є протоколом маршрутизації, як EIGRP, але є відкритим стандартом IETF, який можна використовувати та розгортати в різних мережах. Основною ідеєю розробки протоколу OSPF є розробка протоколу стану зв’язку, який може забезпечити більшу ефективність і масштабованість, ніж RIP. OSPF використовує протокол номер 89 під час роботи через IP, подібно до TCP, що працює через IP, який використовує протокол номер

6. Замість транспортного протоколу, такого як TCP, він має надійний механізм транспортування.

OSPF — це безкласовий протокол маршрутизації, який також підтримує маскування підмережі змінної довжини (VLSM) і роз'єднані мережі. Групові адреси використовуються для надсилання привітів і оновлень - 224.0.0.5 і 224.0.0.6. Також доступна перевірка, два типи – простий тест і алгоритм дайджесту повідомлення 5.

Дерево найкоротших шляхів (SPT) для обчислення маршрутів генерує алгоритм Дейкстри OSPF. В оголошеннях про підключення кожен маршрутизатор представляє себе та свої відносини з сусідами в чіткій і зрозумілій формі, щоб OSPF міг налаштувати топологію мережі на основі інформації з дерева найкоротших шляхів.

Тип інформації, якою обмінюються маршрутизатори, - це тип підключення до інших маршрутизаторів і мережева інформація, і це відомо як процес. Біржа LSA (реклама стану посилання) .

При вибір метрики та шляху протоколу EIGRP існують різні фактори, які визначають загальну метрику для конкретного призначення, наприклад пропускна здатність, затримка, навантаження, надійність, кількість переходів і MTU. Однак для обчислення стандартної метрики використовуються лише пропускна здатність і затримка.

Щоб вибрати шлях, EIGRP використовує поняття наступника, можливого наступника, зареєстрованої відстані та можливої відстані. На першому етапі наступний маршрутизатор вважається найкращим наступним маршрутизатором для певного пункту призначення. Маршрутизатор наступного стрибка відповідає за повідомлення про конкретну відстань призначення як повідомлену відстань. Приймаючий маршрутизатор EIGRP отримує відстань отриманих даних і додає відповідний розмір інтерфейсу, щоб отримати можливу відстань. Усі шляхи до місця призначення перевіряються та порівнюються між собою, з яких

вибирається найкращий шлях. Можливий наступник тут вказує на найкращий наступний маршрутизатор як альтернативу даному пункту призначення.

На відміну від EIGRP, OSFP переважно враховує вартість простого шляху для визначення метрики для заданого призначення префіксу. Щоб обчислити вартість шляху, базова пропускна здатність ділиться на пропускну здатність інтерфейсу. Процес вибору маршруту починається з вибору найдешевшого шляху як найкращого шляху до пункту призначення. Хоча поля OSPF також впливають на процес маршрутизації. Отже, виконайте наведений нижче приклад, щоб вибрати маршрут OSPF:

Маршрути в полі: це маршрути, вивчені в полі. Міжрегіональний маршрут включає маршрути, вивчені за межами регіону. Зовнішні маршрути - маршрути, яких немає в автономній системі OSPF і вивчаються ззовні.

Порівняння протоколів EIGRP і OSPF, EIGRP є досить складним, тоді як OSPF є простішим, оскільки він використовує лише вартість метрики. Основна відмінність між цими протоколами полягає в тому, що EIGRP обмінюється повною інформацією про маршрут лише тоді, коли сусідні маршрути відстежуються на наявність змін після їх встановлення. Натомість OSPF послідовно відстежує всю топологічну базу даних усіх посилань у базі даних.

3.3.1 Розрахунок налаштувань протоколу маршрутизації

В комп’ютерній системі ТОВ «Українські інформаційні технології» , згідно технічних вимог, застосований протокол динамічної маршрутизації EIGRP, який є дистанційно-векторним протоколом, з номером автономної системи 9.

При налаштуванні маршрутизації на роутерах даної КС, на serial-інтерфейсах, відповідно до технічних умов, встановлено пропускну спроможність 128 кб/с , вартість метрики 7’500 та швидкість каналу 128’000.

Turta_R5(config)#interface s0/1/0

Turta_R5(config-if)#bandwidth 128

Turta_R5(config-if)# clock rate 128000

Для маршрутизаторів використовувати перші можливі IP-адреси із діапазону допустимих адрес, призначати інтерфейсам і під інтерфейсам маршрутизаторів у LAN. В мережах VLAN та LAN використовувати адресацію кінцевих пристроїв за протоколом DHCP.

3.5 Налаштування та перевірка роботи комп'ютерної системи

3.5.1 Базове налаштування конфігурації пристроїв

Процес базового налаштування конфігурації активних мережних пристроїв включає:

– застосування сервісу шифрування паролів;

– захист привілейованого режиму ОС, консольного порту та ліній vty;

– призначення банера MOTD *#123-20ck Turta. There is protection router ARIA#*;

– для віддаленого доступу до пристрою на лініях vty застосований протокол SSH;

– створено локальні облікові записи (username 12320ck_Turta) з паролем admincisco;

– створено доменне ім'я пристрою (ip domain-name Turta_R1);

– створено ключ RSA завдовжки 1024 біт для шифрування даних.

Приклад базових налаштувань на роутері R1.

Заборонено пошук DNS на маршрутизаторі:

Router(config)#no ip domain-lookup

Задання пристрою унікального імені:

Router(config)#hostname Turta_R1

Зашифровано всі паролі, що зберігаються у відкритому вигляді:

Turta_R1(config)#service password-encryption

Встановлення паролю на вхід до привілейованого режиму:

Turta_R1(config)#enable secret class123

Встановлено парою на вхід до консольної лінії:

Turta_R1(config)#line console 0

Turta_R1(config-line)#password cisco123

Налаштування запиту пароля при вході:

Turta_R1(config-line)#login

Turta_R1(config-line)#exit

Налаштування банера MOTD:

Turta_R1(config)#banner motd #123-20ck Turta. There is protection router#

Налаштування протоколу SSH, Створення користувача:

Turta_R1(config)#username 12320ck_Turta password admincisco;

Створення домену:

Turta_R1(config)#ip domain-name Turta_R1

Для шифрування даних створено ключ RSA довжиною 1024 біт:

Turta_R1(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Налаштування лінії VTY:

Turta_R1(config)#line vty 0 4

Встановлення необхідності введення логіну та пароля для входу лінії:

Turta_R1(config-line)#login local

Встановлення входу на лінію тільки по протоколу SSH:

Turta_R1(config-line)#transport input ssh

Встановлення IPv4-адрес відповідно до таблиці 3.3:

Turta_R1(config)#interface g0/1

Turta_R1 (config-if)# ip address 10.22.185.1 255.255.255.0

Для запуску інтерфейсу до роботи слід його обов’язково увімкнути:

Turta_R1(config-if)#no shutdown

3.5.2 Налаштування маршрутизаторів корпоративної мережі

Приклад налаштування маршрутизації на Turta_R2:

Включити протокол EIGRP на маршрутизаторі:

Turta_R2(config)#router eigrp 9

Turta_R2(config-router)#)#eigrp router-id 19.19.19.19

Об’явлені мережі, підключені до маршрутизатора:

Turta_R2(config-router)#network 10.22.184.0

Turta_R2(config-router)#network 10.0.9.0. 0.0.0.3

Turta_R2(config-router)#network 209.165.202.0 0.0.0.255

Задано інтерфейси, на які не надсилаються оновлення таблиці маршрутизації:

Turta_R5(config-router) #passive-interface G0/1

Маршрут за замовчуванням на Turta_R2:

ip route 0.0.0.0 0.0.0.0 209.165.202.2

Файл конфігурації роутера зберігається в в енерго-незалежну пам'ять.

Turta_R2#copy running-config startup-config

Перевірити таблицю маршрутизації роутера можна командою:

Turta_R5#show ip route

Перевірку таблиці маршрутизації роутера Turta_R2 наведено на рис. 3.3. Таблиці маршрутизації інших роутерів КС наведено в додатку А.

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 22 subnets, 6 masks
C       10.0.9.0/30 is directly connected, Serial0/2/0
L       10.0.9.1/32 is directly connected, Serial0/2/0
C       10.0.9.4/30 is directly connected, Serial0/2/1
L       10.0.9.5/32 is directly connected, Serial0/2/1
D       10.0.9.8/30 [90/21024000] via 10.0.9.2, 00:26:57, Serial0/2/0
                    [90/21024000] via 10.0.9.6, 00:22:18, Serial0/2/1
D       10.0.9.12/30 [90/21024000] via 10.0.9.2, 00:18:23, Serial0/2/0
                     [90/21024000] via 10.0.9.18, 00:16:31, Serial0/0/0
C       10.0.9.16/30 is directly connected, Serial0/0/0
L       10.0.9.17/32 is directly connected, Serial0/0/0
D       10.0.9.20/30 [90/21024000] via 10.0.9.6, 00:18:43, Serial0/2/1
                     [90/21024000] via 10.0.9.18, 00:16:31, Serial0/0/0
D       10.22.184.0/24 [90/20512256] via 10.0.9.6, 00:20:44, Serial0/2/1
D       10.22.185.0/24 [90/20512256] via 10.0.9.2, 00:28:52, Serial0/2/0
C       10.22.186.0/25 is directly connected, GigabitEthernet0/2
L       10.22.186.1/32 is directly connected, GigabitEthernet0/2
D       10.22.186.128/25 [90/20517376] via 10.0.9.18, 00:06:53, Serial0/0/0
C       10.22.187.0/27 is directly connected, GigabitEthernet0/1.19
L       10.22.187.1/32 is directly connected, GigabitEthernet0/1.19
C       10.22.187.32/27 is directly connected, GigabitEthernet0/1.29
L       10.22.187.33/32 is directly connected, GigabitEthernet0/1.29
C       10.22.187.64/27 is directly connected, GigabitEthernet0/1.39
L       10.22.187.65/32 is directly connected, GigabitEthernet0/1.39
C       10.22.187.96/28 is directly connected, GigabitEthernet0/1.99
L       10.22.187.97/32 is directly connected, GigabitEthernet0/1.99
D    53.0.0.0/8 [90/20517120] via 10.0.9.18, 00:12:16, Serial0/0/0
D    64.0.0.0/8 [90/20517120] via 10.0.9.18, 00:06:57, Serial0/0/0
D    209.165.202.0/24 [90/20514560] via 10.0.9.18, 00:12:28, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 3.3 – Таблиця маршрутизації на Turta_R2

3.5.3 Налаштування роботи Інтернет

Протокол NAT (Network Address Translation) – цей протокол полягає в перетворенні мережевих адрес. Це дозволяє багатьом пристроям, найчастіше підключеним через локальну мережу, використовувати одну публічну IP-адресу. Протокол був створений зростаючою проблемою перспективи зайняти всі адреси IPv4 в Інтернеті. Щоб подолати це, локальні комп'ютерні мережі, які використовують приватні адреси, можна підключити до Інтернету через один маршрутизатор, який має менше Інтернет-адрес, ніж комп'ютери в мережі. Цей маршрутизатор динамічна перетворює приватні адреси на зовнішні, коли комп'ютери в локальній мережі спілкуються із зовнішнім світом, дозволяючи

більшій кількості комп’ютерів використовувати Інтернет, ніж у вас є зовнішні адреси.

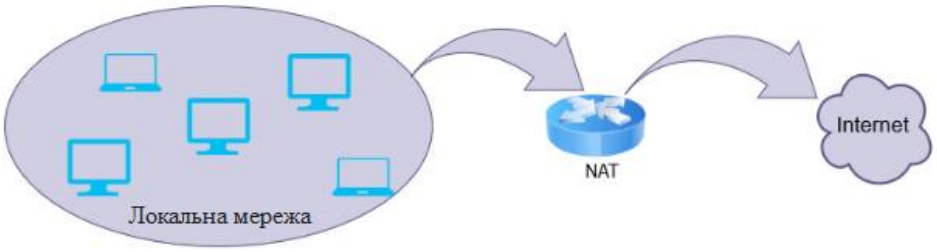


Рисунок 3.4 – Взаємодія локальної мережі та мережі Інтернет

Існує два основних типи протоколу NAT:

– SNAT (Source Network Address Translation) – змінює адресу джерела IP-пакету

– DNAT (Destination Network Address Translation) – змінює адресу призначення IP- пакету

Перевагою протоколу NAT є підвищена анонімність через неможливість ідентифікації конкретного хоста лише за IP-адресою та можливість доступу до Інтернету для більшої кількості комп’ютерів, ніж кількість доступних загальнодоступних IPv4-адрес.

NAT також має кілька недоліків. Комп’ютер не може запустити доступний в Інтернеті сервер без змін, які потребують втручання адміністратора, а також перешкоджає використанню мереж P2P і прямому завантаженню файлів,

NAT на прикордонному маршрутизаторі налаштовано згідно з вимогами:

- пул адрес 209.165.201.1 - 209.165.201.30 ;
- 172.23.0.190 – адреса Server HTTP;
- номер списку доступу: 9;
- ім'я пулу: Internet.

Приклад налаштування NAT на Turta_R3:

Список контролю доступу, що дозволяє всі адреси внутрішньої мережі:

Turta_R3(config)# access-list 9 permit 10.22.184.0 0.0.7.255

Пул для динамічного виділення інтернет адрес:

Turta_R3(config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.185

Підміна адреси внутрішньої мережі на інтернет адреси згідно з списком контролю доступу:

Turta_R3(config)#ip nat inside source list 9 pool Internet

Адреса статичного NAT для серверу HTTP:

Turta_R3(config)#i ip nat inside source static 10.22.186.10 209.165.200.5

Призначення інтерфейсу в якості вихідного для трафіку з мережі приватних адрес:

Turta_R3(config)#interface F4/0

Turta_R3(config-if)#ip nat outside

Призначення інтерфейсу в якості вхідного для трафіку з мережі приватних адрес:

Turta_R3(config-if)#interface Serial3/0

Turta_R3(config-if)#ip nat inside

Для перевірки роботи NAT отримаємо таблицю перетворювань.

Pro	Inside global	Inside local	Outside local	Outside global
icmp	209.165.202.5:6	10.22.185.17:6	53.1.9.10:6	53.1.9.10:6
icmp	209.165.202.5:7	10.22.185.17:7	53.1.9.10:7	53.1.9.10:7
icmp	209.165.202.5:8	10.22.185.17:8	53.1.9.10:8	53.1.9.10:8
icmp	209.165.202.6:4	10.22.186.18:4	53.1.9.10:4	53.1.9.10:4
icmp	209.165.202.6:5	10.22.186.18:5	53.1.9.10:5	53.1.9.10:5
icmp	209.165.202.7:1	10.22.186.19:1	53.1.9.10:1	53.1.9.10:1
icmp	209.165.202.7:2	10.22.186.19:2	53.1.9.10:2	53.1.9.10:2
---	209.165.202.3	10.22.186.10	---	---

Рисунок 3.5 – Таблиця перетворювань NAT на Turta_R3

3.5.4 Перевірка роботи комп’ютерної системи

Виконання команди Ping між хостами з підмереж LAN2 та LAN5.

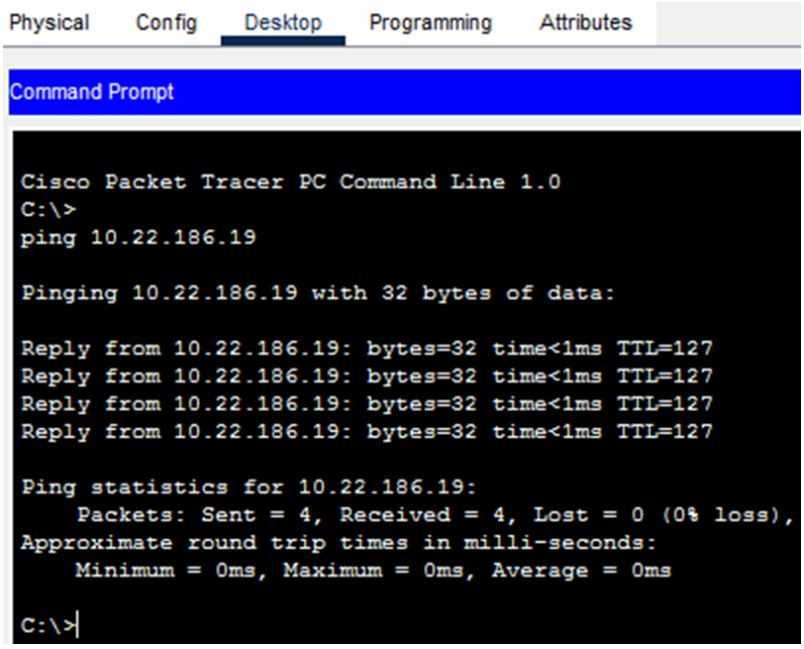


Рисунок 3.6 – Результат команди «ping» між підмережами КС

Для перевірки працездатність мережі також перевіряється, налаштування безпечного віддаленого доступу до активних мережних пристроїв, перевірку зв'язку між вузлами з різних VLAN, автоматичне призначення адрес при використанні протоколу DHCP.

Для перевірки SSH зробимо підключення з командного рядка PCF1 з підмережі «LAN4» до маршрутизатора Turta_R1 від користувача 12320ck_Turta з паролем admincisco.

В підмережах комп’ютерної системи ТОВ «Українські інформаційні технології» хости отримують мережні налаштування за протоколом DHCP.

Приклад налаштування DHCP на Turta_R2.

Turta_R1(config)#interface g0/1

Активовано протокол DHCP:

Turta_R2(config-if)#service DHCP

Створений пул DHCP з ім’ям Pool_VLAN19:

Turta_R2(config-if)#ip dhc pool VLAN19

Вилучено з пулу перші 10 адрес:

Turta_R2(config-if)#ip dhc ex 10.22.187.1 10.22.187.10

Зазначена мережа і шлюз за замовчуванням:

Turta_R2(config-if)#net 10.22.187.0 255.255.255.224

Turta_R2(config-if)#def 10.22.187.1

Turta_R2(config-if)#dns 10.22.186.10

IP address	Client-ID/ Hardware address	Lease expiration	Type
10.22.187.11	0030.A320.EA8A	--	Automatic
10.22.187.12	0002.4AA1.D28D	--	Automatic
10.22.187.13	000C.CF86.656C	--	Automatic
10.22.187.44	0040.0BAE.A501	--	Automatic
10.22.187.45	0001.97C8.5C05	--	Automatic
10.22.187.46	00E0.F73D.5391	--	Automatic
10.22.187.47	00D0.FF28.2607	--	Automatic
10.22.187.48	0009.7C11.B06D	--	Automatic
10.22.187.76	0003.E468.78BB	--	Automatic
10.22.187.77	0006.2A40.DD5D	--	Automatic
10.22.187.79	0060.5C08.C371	--	Automatic
10.22.187.78	000A.41D2.AB7A	--	Automatic
10.22.187.80	0000.0CDC.2CAC	--	Automatic
10.22.186.11	0004.9A26.63A4	--	Automatic
10.22.186.12	0040.0BDD.EDA6	--	Automatic
10.22.186.14	0001.437E.02E4	--	Automatic
10.22.186.13	0001.63A4.C101	--	Automatic
10.22.186.15	00D0.BCE8.B519	--	Automatic
10.22.186.16	0090.21B6.73E2	--	Automatic
10.22.186.17	0090.0CD5.329D	--	Automatic

Рисунок 3.7 − Таблиця призначення IP-адрес вузлам за протоколом DHCP

Агрегування каналів виконане із застосуванням протоколу управління агрегацією каналів (LACP).

LACP - це протокол для колективної обробки кількох фізичних портів, який можна як один канал з метою мережного трафіку. Це є загальним принципом агрегації каналів, який описує зусилля з налаштування паралельних мережевих структур забезпечення надмірності чи підвищення продуктивності.

Etherchannel - це технологія, що дозволяє об'єднувати (агрегувати) кілька фізичних проводів (каналів, портів) у єдиний логічний інтерфейс. Як правило, це використовується для підвищення стійкості до відмови і збільшення пропускної здатності каналу. Зазвичай, для з'єднання критично важливих вузлів (комутатор-комутатор, комутатор-сервер та ін.). Саме слово Etherchannel введене компанією Cisco і все, що пов'язане з агрегуванням, вона містить його. Інші вендори

агрегування називають по-різному. Huawei називає це Link Aggregation, D-Link називає LAG і так далі. Але сутність від цього не змінюється.

На комутаторах Turta_S1, Turta_S6 та Turta_S7 виконане агрегування каналів, що дозволяє об’єднати декілька фізичних каналів в один логічний для збільшення пропускної спроможності та надійності каналу.

```
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------

1      Po1(SU)           PAgP   Fa0/1(P) Fa0/2(P)
3      Po3(SD)           PAgP   Fa0/3(I) Fa0/4(I)
```

Рисунок 3.8 – Перевірка налаштування агрегування каналів

3.6 Захист інформації в комп’ютерній системі від несанкціонованого доступу

3.6.1 Розробка методів для захисту інформації в комп’ютерній системі

Проблема забезпечення інформаційної безпеки потребує комплексного підходу. Основними напрямками розвитку політики інформаційної безпеки є:

- визначення того, які дані повинні бути захищені та з якою серйозністю;
- визначення того, хто і в якому обсязі може завдати підприємству інформаційної шкоди;
- розрахунок ризиків і визначення схеми їх зниження до допустимого рівня;
- опис усіх запланованих технічних та адміністративних заходів;

- розрахунок економічної ціни програми, що розглядається;
- погодження та оформлення документів керівництвом підприємства;
- реалізація.

Крім того, що організаційні заходи є одним із ефективних засобів захисту інформації, вони складають основу всіх створених систем захисту. Організаційні заходи охоплюють такі теми:

- управління персоналом;
- фізичний захист;
- підтримка працездатності системи;
- реагування на порушення безпеки;
- планування відновлення.

Найпоширенішим типом аутентифікації є пароль. Введений пароль порівнюється з паролем, призначеним раніше користувачеві. Коли вони збігаються, користувач вважається автентифікованим.

Основним недоліком паролів є їх електронне перехоплення. Практично єдиний вихід - це криптографічне шифрування паролів перед їх передачею по лініях зв'язку. Значно підвищити надійність захисту паролем можуть такі заходи:

- встановлення технічних обмежень (пароль не повинен бути занадто коротким, пароль повинен містити літери, цифри, знаки пунктуації тощо);
- управління терміном дії паролів, їх періодична зміна;
- обмеження доступу до файлу паролів;
- обмеження невдалих спроб входу в систему;
- інструктування користувачів;
- використання програм-генераторів паролів.

Проблеми автентифікації бездротового клієнта є однією з найскладніших проблем, з якою стикаються інженери бездротових мереж. Щоб усунути

несправності, часто потрібно отримати проблемний клієнт, працювати з кінцевими користувачами, які не мають найкращих знань про бездротові мережі, а також збирати дані про налагодження та захоплення. У все більш критичній бездротовій мережі це може спричинити значні простої.

Досі не було простого способу визначити, чи збій автентифікації був спричинений радіус-сервером, який відхиляє клієнта, чи просто проблемою доступності. Команда test aaa radius дозволяє зробити саме це. Можна віддалено перевірити, чи відбувається збій зв'язку з сервером WLC-Radius або чи облікові дані для клієнта призводять до пройденої чи невдалої автентифікації.

Базовий робочий процес при використанні команди test aaa radius показано на рис. 9.

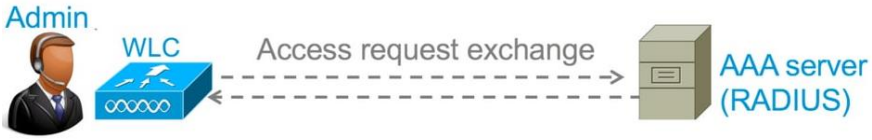


Рисунок 3.9 - Базовий робочий процес при використанні команди test aaa radius

Крок 1. WLC надсилає повідомлення із запитом на доступ радіус-серверу разом із параметрами, згаданими в тестовій команді radius aaa .

Наприклад: test aaa radius ім'я користувача пароль адміністратора cisco123 wlan-id 1 група груп за замовчуванням індекс сервера 2

Крок 2. Радіус-сервер перевіряє надані облікові дані та надає результати запиту автентифікації.

3.6.2 Налаштування маршрутизаторів на підтримку служби AAA

Приклад налаштування сервісу AAA та сереверу RADIUS.

Запуск служби AAA:

Turta_R2(config)#aaa new-model

Налаштування методу аутентифікації з використання локальної бази користувачів:

Turta_R2(config)#aaa authentication login default local

Налаштування методу аутентифікації Login на серевері RADIUS, а якщо він недоступний, то з використанням локальної бази користувачів:

Turta_R2(config)#aaa authentication login Login group radius local

Застосування методу аутентифікайфії Login на консольній лінії та vty:

Turta_R2(config)#line console 0

Turta_R2(config-line)#login authentication Login

Turta_R2(config)#line vty 0 4

Turta_R2(config-line)#login authentication default

Налаштування RADIUS-серверу:

Turta_R2(config)#radius-server host 10.22.186.10 auth-port 1645

Turta_R2(config)#radius-server key radiusKovalev

Для доступу використовується доменне ім’я пристрою Turta_R2 з паролем radius12318, що був налаштований на сервері RADIUS.

3.6.3 Налаштування мережах VLAN та параметрів безпеки комутаторів

Згідно до технічних вимог в підмережі LAN3 створено 4 підмережі VLAN.

Таблиця 3.7 – Назви VLAN для підмережі

Номер VLAN	Ім’я VLAN	Примітка
VLAN9	Default	Не використовується
VLAN29	Service	Служба розпорядників
VLAN39	Control	Відділ аналітики
VLAN49	Management	Управління пристроями

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/3, Fa0/4, Gig0/2
19   vlan19                            active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9
29   vlan29                            active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14
39   vlan39                            active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
99   Management                        active
100  Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 3.9 – Налаштування VLAN на Turta_S2

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/3, Fa0/4, Gig0/1
                                                 Gig0/2
19   vlan19                            active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9
29   vlan29                            active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14
39   vlan39                            active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
99   Management                        active
100  Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 3.10 – Налаштування VLAN на Turta_S3

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Gig0/1
                                                 Gig0/2
19   vlan19                            active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9
29   vlan29                            active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14
39   vlan39                            active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
99   Management                        active
100  Native                            active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 3.11 – Налаштування VLAN на Turta_S1

На рисунках наведено розподіл портів комутаторів за віртуальнимм мережами, які було створено.

Для здійснення передачі трафіку між VLAN необхідно налаштувати порт GigabitEthernet0/1 маршрутизатора Turta_R2 на підтримку технології інкапсуляції 802.1Q.

Turta_R2(config)#interface g0/1

Turta_R2(config-if)#no shutdown

Налаштування підінтерфейсу для маршрутизації трафіку між VLAN.

Turta_R2(config)#interface g0/0.19

Тегування пакетів для данного підінтерфейсу.

Turta_R2(config-subif)#encapsulation dot1Q 19 //

Turta_R2(config-subif)#ip address 10.22.187.1 255.255.255.224

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Down	--	<not set>	<not set>	0001.C942.2195
GigabitEthernet0/1	Up	--	<not set>	<not set>	00D0.BC6E.3ED8
GigabitEthernet0/1.19	Up	--	10.22.187.1/27	<not set>	00D0.BC6E.3ED8
GigabitEthernet0/1.29	Up	--	10.22.187.33/27	<not set>	00D0.BC6E.3ED8
GigabitEthernet0/1.39	Up	--	10.22.187.65/27	<not set>	00D0.BC6E.3ED8
GigabitEthernet0/1.99	Up	--	10.22.187.97/28	<not set>	00D0.BC6E.3ED8
GigabitEthernet0/2	Up	--	10.22.186.1/25	<not set>	0005.5E8D.E9D3
Serial0/0/0	Down	--	<not set>	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>	<not set>
FastEthernet0/1/0	Up	1	--	<not set>	0060.7099.0133
FastEthernet0/1/1	Up	1	--	<not set>	0060.3E98.52CD
FastEthernet0/1/2	Up	1	--	<not set>	0003.E459.3E4D
FastEthernet0/1/3	Up	1	--	<not set>	0030.A38B.5EC7
Serial0/2/0	Down	--	10.0.9.17/30	<not set>	<not set>
Serial0/2/1	Down	--	10.0.9.5/30	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	00E0.F97E.A8B2

Рисунок 3.12 – Перевірка налаштування 802. 1Q на Turta_R2

Інкапсуляція 802. 1Q Rout1_Radabank на налаштована.

На портах комутатора Turta_S5, де встановлені сервери КС фірми «Megamart», налаштовані засоби безпеки: тільки одному вузлу дозволений доступ до порту; MAC-адреса пристрою додається статично в поточну конфігурацію; при порушенні системи безпеки порт виключається.

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
-----------------------------------------------------------------------
       Fa0/23        2           0                0         Restrict
       Fa0/24        2           0                0         Restrict
-----------------------------------------------------------------------
```

Рисунок 3.13 – Перевірка безпеки портів Turta_S5

3.6.4 Налаштування віртуальної приватної мережі VPN

В КС мережею VPN передається трафік між підмережею «LAN3» та підмережою «LAN1».

Для перевірки створеного VPN тунелю передачі трафіку між підмережами застосовується команда *show crypto ipsec sa*.

```
interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.0.9.21

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.22.184.0/255.255.255.30/0/0)
   remote  ident (addr/mask/prot/port): (10.22.186.128/255.255.255.128/0/0)
   current_peer 64.100.13.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.0.9.21, remote crypto endpt.:64.100.13.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)

     inbound esp sas:
      spi: 0x430ECD00(1125043456)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3576)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

Рисунок 3.14 – Перевірка стану IPSec SA на роутері Turta_R5

```
interface: GigabitEthernet0/0
    Crypto map tag: VPN-MAP, local addr 64.100.13.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.22.186.128/255.255.255.128/0/0
   remote  ident (addr/mask/prot/port): (10.22.184.0/255.255.255.30/0/0)
   current_peer 10.0.9.21 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 64.100.13.2, remote crypto endpt.:10.0.9.21
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x0(0)

     inbound esp sas:
      spi: 0x430ECD00(1125043456)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: FPGA:1, crypto map: VPN-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/3576)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

Рисунок 3.15 – Перевірка стану IPSec SA на роутері Turta_R0

4 БАЗА ДАНИХ

4.1 Загальна інформація

База даних - це сукупність даних, яка відповідає певній закономірності та порядку. Це сукупність інформації, якою можна керувати, змінювати, переносити з одного місця в інше, а між собою можна встановлювати певні відносини. База даних — це система, створена для підготовки, зберігання та опису великої колекції взаємопов’язаних даних багатьма користувачами. База даних — це можливість використання інформації з єдиного центру в деяких організаціях.

Програми, які використовуються для створення бази даних, керування нею, введення нових даних (даних), видалення, зміни тощо, називаються системами керування базами даних. Англійською мовою це скорочено називається СУБД (DataBase Management System).

Існує багато типів баз даних. Прикладами таких є розподілені бази даних, об’єктно-орієнтовані бази даних, гіпермедійні бази даних та інші. Але є інший тип бази даних, який є найпоширенішим і найбільш використовуваним типом бази даних. Ця база даних називається реляційною базою даних. Майже всі сучасні бази даних сьогодні зберігають і обробляють дані за допомогою моделі реляційної бази даних. У реляційній базі даних дані зберігаються в таблицях. У таблицях зберігається лише інформація, що стосується однієї теми. Для прикладу опишемо бібліотеку. Як ви думаєте, якою може бути інформація про цю бібліотеку? Назви книг у бібліотеці, автор книги, Ці книги, розміщені на полицях, можуть мати серійні номери та іншу інформацію. Ці дані можна розмістити в одній або кількох таблицях. Хоча ці дані розташовані в інших таблицях, ми можемо об’єднати потрібну інформацію з цих таблиць і описати її у вигляді таблиці.

Системи керування реляційними базами даних (РСУБД) доступні для керування реляційними базами даних. Через РСУБД ми можемо швидко

отримувати доступ до даних і запитувати потрібну інформацію. Системи управління реляційними базами даних (РСУБД) повністю здатні описувати, маніпулювати та обмінюватися даними з іншими користувачами. Система дозволяє каталогізувати велику кількість даних у багатьох таблицях, спростити керування та використовувати багато її функцій. РСУБД має 3 основні функції: опис даних, управління даними та контроль даних.

Опис даних – Ви можете визначити, які дані зберігаються в базі даних, типи цих даних (наприклад, char, число, дата тощо) і як дані пов’язані.

Керування даними – з даними можна працювати різними способами. Там можна вибрати потрібний стовпець даних, відсортувати їх, видаливши непотрібні дані. Ви можете видалити та змінити дані, які вам не потрібні, або ви можете помістити їх у нову таблицю. Поєднавши та об’єднавши дві таблиці, ви можете створити іншу таблицю з потрібних вам даних.

Контроль даних – ви можете обмежити або дозволити, які користувачі можуть читати дані в базі даних, які можуть вставляти нові дані, які можуть видаляти дані, які користувачі можуть змінювати дані чи ні. Ви навіть можете дозволити або заборонити їм ділитися цими даними з іншими.

Наразі жодні прикладні програми для керування базою даних не використовуються. Для управління базою даних тепер використовуються системи управління базами даних (RDBMS). Можна перерахувати назви деяких із цих систем. Наприклад, Microsoft Access, Microsoft SQL Server, Oracle, Sybase тощо.

4.2 Розробка бази даних

4.2.1 Постановка завдання для реалізації бази даних

Для співробітників ТОВ «Українські інформаційні технології» розробимо базу даних для зберігання параметрів орендованих офісних приміщень та їх власників.

База даних, що розробляється повинна зберігати таку інформацію:

- інформацію про спрацьовування сигналізації;
- інформацію про охорону;
- інформацію про облік спожитих ресурсів;
- інформацію про власників;
- інформацію про обслуговування;
- інформацію про обладнання.

4.2.2 Обґрунтування вибору СУБД

Для реалізації бази даних (БД) у кваліфікаційні роботі бакалавра обрана реляційна модель (РМ). В основі РМ лежать прості таблиці, які задовольняють певним обмеженням і можуть розглядатися як математичні відносини. Відносно (таблиці) виділяється декілька атрибутів, однозначно ідентифікують кортежі і званих ключами.

Особливість реляційної моделі полягає в тому, що на відміну від мережевої та ієрархічної моделей реальні об'єкти і взаємозв'язки між ними представляються в базі даних однаково в вигляді нормалізованих відносин.

Переваги реляційної моделі:

– РМ БД є звичним для користувача набором таблиць;

– автоматизований доступ до даних і алгоритми і процедури обробки запитів;

– реляційні мови легкі для вивчення і освоєння;

– реляційне уявлення дає ясну картину взаємозв'язків атрибутів з різних відносин;

– спрямовані зв'язку в реляційної БД відсутні.

– операції проекції і об'єднання дозволяють розрізати і склеювати відносини, що служить для отримання різноманітних файлів в потрібній формі;

– для кожного відносини є можливість завдання правомірності доступу, засекречені показники виділяються в окремі відносини з перевіркою прав доступу.

– фізичне розміщення однорідних файлів набагато простіше, ніж розміщення ієрархічних і мережевих структур.

– БД допускає можливість розширення.

Для управління базою даних в цьому дипломному проекті обрана система керування базами даних Access.

Access сприймає велику кількість форматів даних, включаючи файлові структури інших СУБД. Тому додаток в Access може імпортувати з текстових файлів або електронних таблиць і експорт в них: надавати прямий доступ і оновлювати файли Paradox, FoxPro і інших БД. Можна також імпортувати дані з цих файлів в таблиці Access.

Перевагою Access так само є наявність засобів проектування програми БД без знання мови програмування. Робота в Access починається з визначення реляційних таблиць і полів, призначених для зберігання даних. Відразу після цього за допомогою форм, звітів, макросів і VBA можна визначати дії над цими даними. Форми і звіти використовуються для виведення на екран і додаткових обчислень при роботі з таблицями. У разі розробки більш складного додатка можна використовувати мову Visual Basic.

Вбудована мова запитів SQL дозволяє максимально гнучка працювати з даними і значно прискорює доступ до зовнішніх даних. Крім того, дана СУБД оптимально підходить під операційну систему, встановлену на автоматизоване робоче місце оператора АРМ оператора, а саме Microsoft Windows 10.

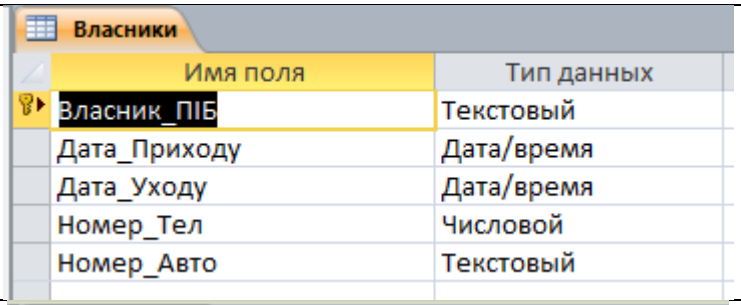
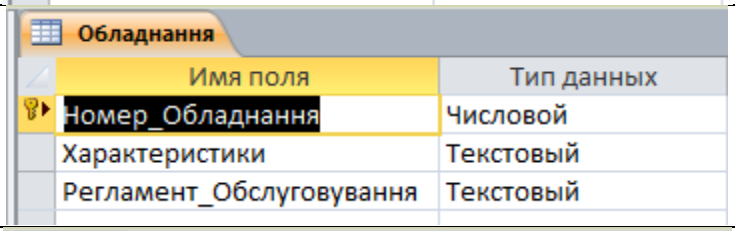
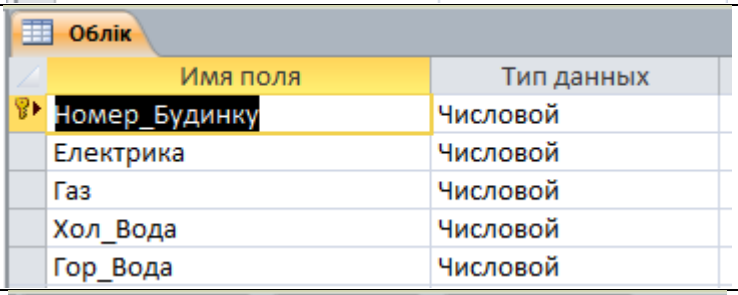
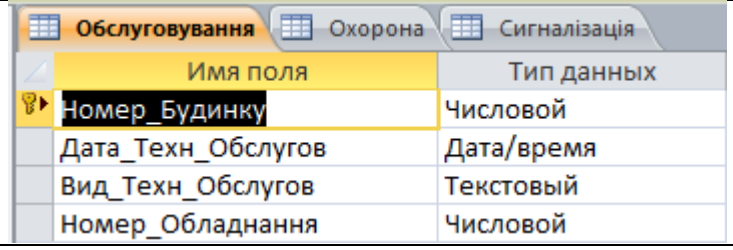
4.2.3 Розробка логічної структури БД

База даних у кваліфікаційні роботі представлена у вигляді шести таблиць: **Охорона** - містить інформацію про охоронців; **Сигналізація** - містить

інформацію про спрацьовування сигналізації та час; **Облік** - містить інформацію про спожиті ресурси з прив'язкою до будинку; **Обслуговування** - містить дані про вид та дату технічного обслуговування; **Власники** - містить інформацію про власників; **Обладнання** - містить інформацію про обладнання, яке встановлено в будинках, та підлягає періодичному обслуговуванню.

Структура таблиць представлена в табл. 4.1.

Таблиця 4.1 - структура таблиць БД

Назва таблиці	Вигляд структури таблиці у середовищі Access
1	2
Власники	
Обладнання	
Облік	
Обслуговування	

Продовження таблиці 4.1

1	2
Охорона	Обслуговування | Охорона | Сигналізація Имя поля: Охоронник_ПІБ (Текстовый); Дата_Зміни (Дата/время); Час_Зміни (Дата/время)
Сигналізація	Обслуговування | Охорона | Сигналізація Имя поля: Тип_Сигналізації (Текстовый); Дата_Спрацьовування (Дата/время); Час_Спрацьовування (Дата/время); Номер_Будинку (Числовой)

Логічна модель бази даних, розроблена в середовищі Access приведена на рис 4.1.

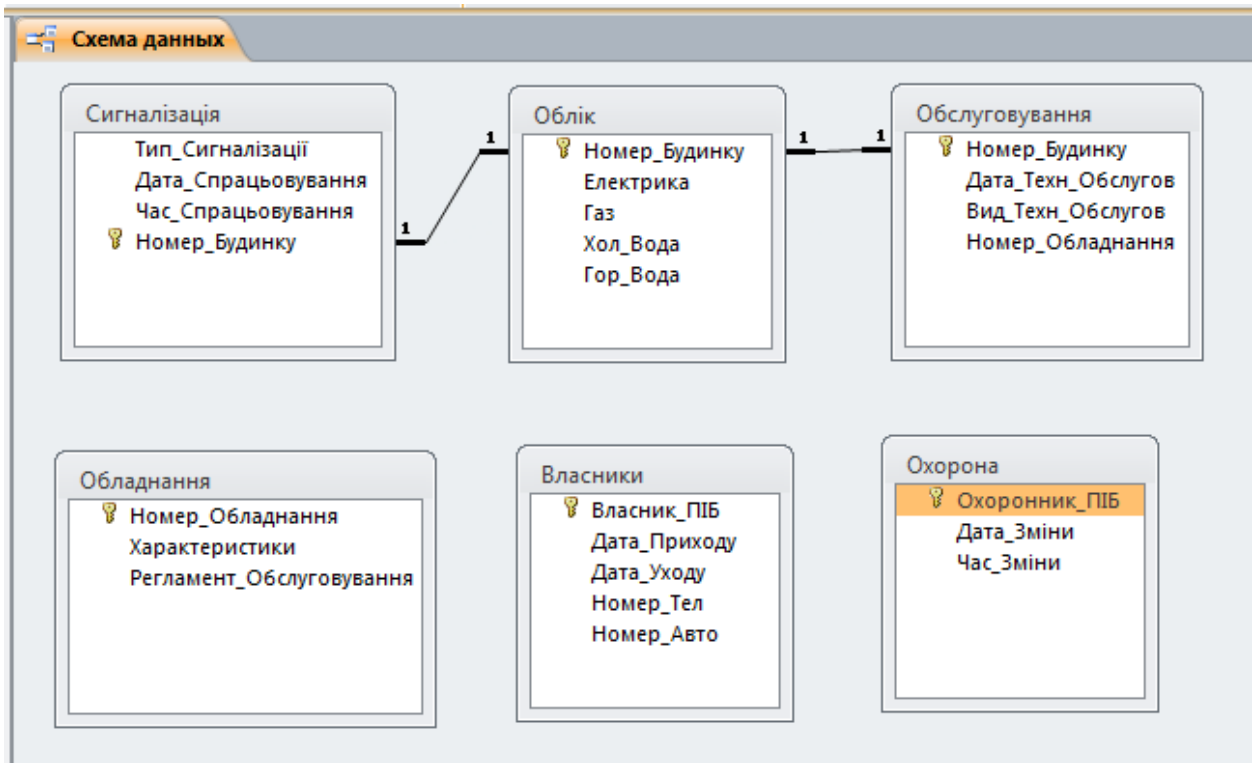


Рисунок 4.1 - Логічна модель бази даних

4.2.4 Створення об'єктів БД

Запит на вибірку інформації про обслуговування будинку 12 на рис. 4.2.

Даному запиту відповідає наступний код на мові SQL:

SELECT Обслуговування.Номер_Будинку, Обслуговування.Дата_Техн_Обслугов, Обслуговування.Номер_Обладнання

FROM Обслуговування

WHERE (((Обслуговування.Номер_Будинку)=12));

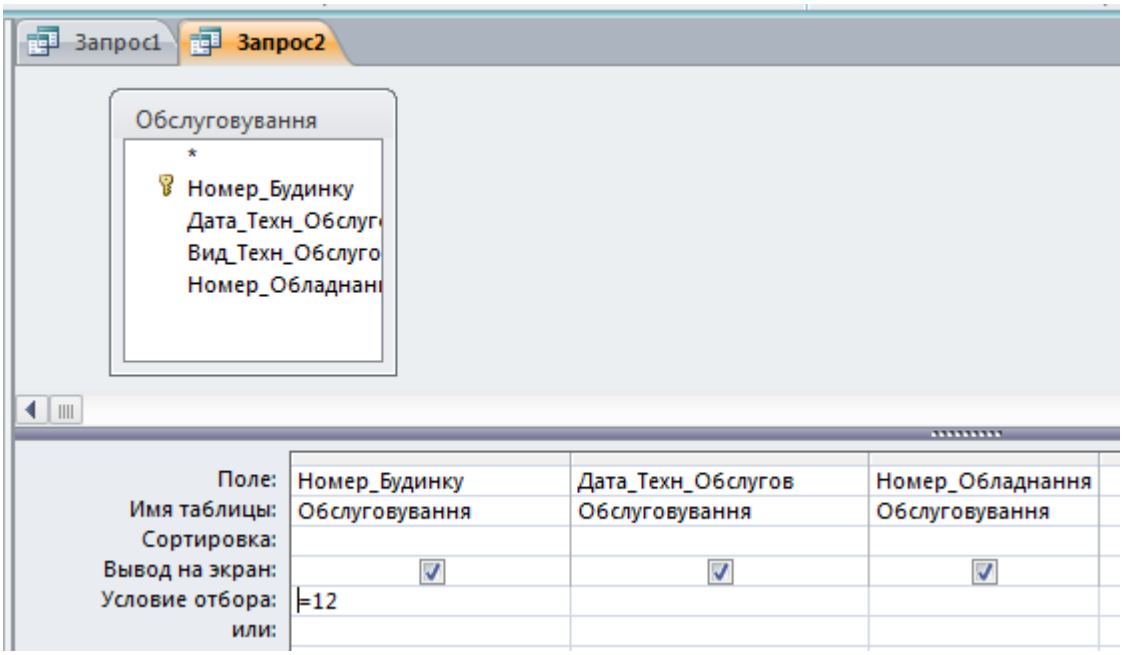


Рисунок 4.2 - Реалізація запиту на вибірку в середовищі Access

Результатом вибірки служить таблиця з інформацією про обслуговування будинку 12, як зображено на рис. 4.3.

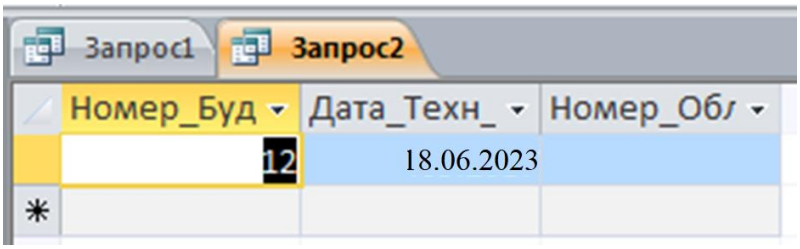


Рисунок 4.3 - Таблиця результату вибірки

Запит на вибірку інформації про споживання ресурсів на рис. 4.4.

Даному запиту відповідає наступний код на мові SQL:

SELECT Облік.Номер_Будинку, Облік.Електрика, Облік.Газ, Облік.Хол_Вода, Облік.Гор_Вода

FROM Облік;

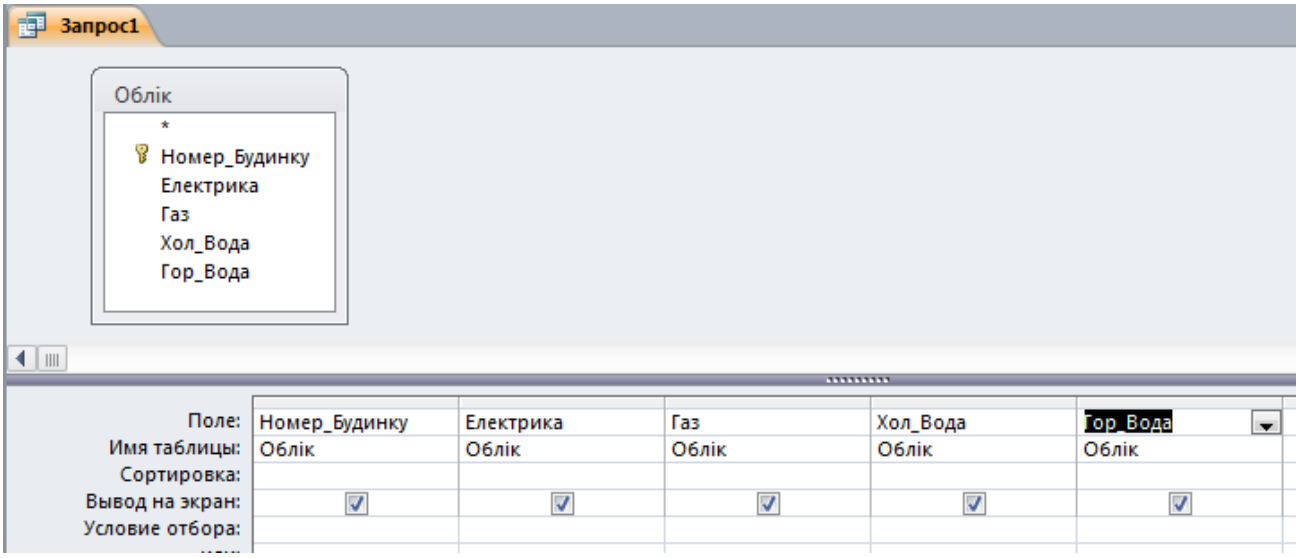


Рисунок 4.4 - Реалізація запиту на вибірку в середовищі Access

Результатом вибірки служить таблиця з інформацією про споживання ресурсів, як зображено на рис. 4.5.

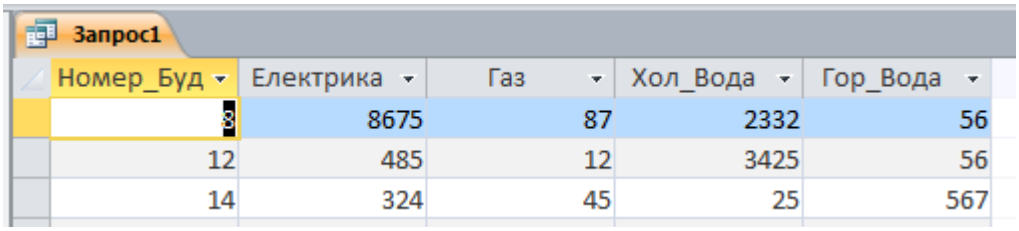


Рисунок 4.5 - Таблиця результату вибірки

ВИСНОВКИ

Завданням даної кваліфікаційної роботи є розробка комп’ютерної системи ТОВ «Українські інформаційні технології» з детальним опрацюванням побудови та налаштування корпоративної мережі.

Враховуючи визначену для ТОВ «Українські інформаційні технології» архітектуру мережі, а також кількість підмереж та взаємозв’язки, рекомендовану кількість комп’ютерів та мережевого обладнанням необхідно виконано розрахунок мережі та здійснене налаштування, проведені необхідні розрахунки, а також виконати подальше моделювання і перевірку роботи комп’ютерної системи.

В розділі розробка апаратної частини комп’ютерної системи розроблено технічне завдання для проектування комп’ютерної системи ТОВ «Українські інформаційні технології» з детальним опрацюванням побудови та налаштування корпоративної мережі, у будинку розташованому за адресом: Україна, 79017, львівська обл., місто Львів, вул. Водогінна, 2.

Також зроблено вибір апаратних засобів створення комп’ютерної мережі, зроблено розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства.

Виконано розрахунок налаштувань для заданої топології мережі, обрано інтерфейси каналів зв’язку та протоколи обміну, розрахована топологічна схема комп’ютерної системи, розраховані налаштування маршрутизації комп’ютерної мережі, а також виконане подальше моделювання і перевірка роботи комп’ютерної системи.

Розроблено комплект документації для програмного забезпечення комп’ютерної мережі

ПЕРЕЛІК ПОСИЛАНЬ

1. Товариство з обмеженою відповідальністю "Українські інформаційні технології". Режим доступу: https://clarity-project.info/edr/32568891

2. Топ-100 компаній України 2023 . Режим доступу: https://uba.top/top-100/

3. Гасімов В.А. Сучасні технології захисту інформації. Підручник. Баку. Видавництво Академії Гейдара Алієва НАНУ. 2011, - 112 с.

4. Н.В. Агаєв, Г.М. Хамідова. Системи інженерного забезпечення в компаніях. Нечіткий мультиагент для оцінки роботи. Національна авіаційна академія. Наукові збірники т. 21, № 1-2019, 149 стор.

5. М.К. Рамазанов «Управління інформаційними системами». Навчальний посібник, Баку, 2017 --- стор.187. . Режим доступу:

Додаток А

Текст програми

Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.23018-01 12 01

Листів 7

2023

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп’ютерної системи третього апеляційного адміністративного суду. Програма призначена для забезпечення налаштування динамічної маршрутизації, DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену и SSH комп’ютерної системи.

ЗМІСТ

1 Налаштування роутера Turta_R2

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Turta_R2
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 10.22.187.1 10.22.187.10
ip dhcp excluded-address 10.22.187.33 10.22.187.43
ip dhcp excluded-address 10.22.187.65 10.22.187.75
ip dhcp excluded-address 10.22.186.1 10.22.186.10
!
ip dhcp pool POOL_VLAN19
 network 10.22.187.0 255.255.255.224
 default-router 10.22.187.1
 dns-server 10.22.186.10
ip dhcp pool POOL_VLAN29
 network 10.22.187.32 255.255.255.224
 default-router 10.22.187.33
 dns-server 10.22.186.10
ip dhcp pool POOL_VLAN39
 network 10.22.187.64 255.255.255.224
 default-router 10.22.187.65
 dns-server 10.22.186.10
ip dhcp pool POOL_lan5
 network 10.22.186.0 255.255.255.128
 default-router 10.22.186.1
 dns-server 10.22.186.10
!
!
aaa new-model
!
aaa authentication login Login group radius local
aaa authentication login SSH-LOGIN local
aaa authentication login default group radius local
!
username 12320ck_Turta password 7 0822455D0A16
!
license udi pid CISCO2911/K9 sn FTX1524F1CX-
license boot module c2900 technology-package securityk9
!
no ip domain-lookup
ip domain-name Turta_R2
!
!
spanning-tree mode pvst
interface GigabitEthernet0/1.19
 encapsulation dot1Q 19
 ip address 10.22.187.1 255.255.255.224
!
interface GigabitEthernet0/1.29
 encapsulation dot1Q 29
 ip address 10.22.187.33 255.255.255.224
!
interface GigabitEthernet0/1.39
 encapsulation dot1Q 39
 ip address 10.22.187.65 255.255.255.224
!
interface GigabitEthernet0/1.99
 encapsulation dot1Q 99
 ip address 10.22.187.97 255.255.255.240
```

```
!
interface GigabitEthernet0/2
 ip address 10.22.186.1
255.255.255.128
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.0.9.17 255.255.255.252
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Serial0/2/0
 description to R3
 bandwidth 128
 ip address 10.0.9.1 255.255.255.252
!
interface Serial0/2/1
 description to R4
 bandwidth 128
 ip address 10.0.9.5 255.255.255.252
 clock rate 128000
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 9
 redistribute static
 passive-interface GigabitEthernet0/2
 passive-interface
GigabitEthernet0/1.19
 passive-interface
GigabitEthernet0/1.29
 passive-interface
GigabitEthernet0/1.39
 passive-interface
GigabitEthernet0/1.99
 network 10.0.9.0 0.0.0.3
 network 10.0.9.4 0.0.0.3
 network 10.0.9.16 0.0.0.3
 network 10.22.187.0 0.0.0.31
 network 10.22.187.32 0.0.0.31
 network 10.22.187.64 0.0.0.31
 network 10.22.187.96 0.0.0.15
 network 10.22.186.0 0.0.0.127
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.2
!
ip flow-export version 9
!
banner motd #123-20ck Turta. There is
protection router ARIA#
!
radius-server host 10.22.186.10 auth-
port 1645
radius-server key zzz
!
radius server 10.22.186.10
 address ipv4 10.22.186.10 auth-port
1645
line con 0
 password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
 password 7 0822455D0A16
 login authentication SSH-LOGIN
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 transport input ssh
end
```

2 Налаштування комутатора Turta_S2

```
!
version 15.0
```

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Turta_S2
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip domain-name Turta_S2
!
username 12320ck_Turta privilege 1 password 7 0822455D0A16
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1

 switchport trunk native vlan 100
 switchport trunk allowed vlan 19,29,39,99-100
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 100
 switchport trunk allowed vlan 19,29,39,99-100
 switchport mode trunk
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 19
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 19
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 19
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 19
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 19
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 29
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 29
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 29
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 29
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/17
```

```
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 39
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 39
 switchport mode access
!
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan
19,29,39,99-100
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
interface Vlan99
 description LAN Vnutr_99
 ip address 10.22.187.98
255.255.255.240
!
ip default-gateway 10.22.187.97
!
banner motd #123-20ck Turta. There is
protection router ARIA#
!
line con 0
 password 7 0822455D0A16
 login
!
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
end
```

Додаток Б

Таблиці маршрутизації

Таблиця маршрутизації на Turta_R1

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 18 subnets, 6 masks
C       10.0.9.0/30 is directly connected, Serial0/2/0
L       10.0.9.2/32 is directly connected, Serial0/2/0
D       10.0.9.4/30 [90/21024000] via 10.0.9.10, 00:32:56, Serial0/2/1
                    [90/21024000] via 10.0.9.1, 00:32:55, Serial0/2/0
C       10.0.9.8/30 is directly connected, Serial0/2/1
L       10.0.9.9/32 is directly connected, Serial0/2/1
C       10.0.9.12/30 is directly connected, Serial0/0/0
L       10.0.9.13/32 is directly connected, Serial0/0/0
D       10.0.9.16/30 [90/21024000] via 10.0.9.14, 00:32:56, Serial0/0/0
                     [90/21024000] via 10.0.9.1, 00:32:55, Serial0/2/0
D       10.0.9.20/30 [90/21024000] via 10.0.9.10, 00:32:56, Serial0/2/1
                     [90/21024000] via 10.0.9.14, 00:32:56, Serial0/0/0
D       10.22.184.0/24 [90/20512256] via 10.0.9.10, 00:32:56, Serial0/2/1
C       10.22.185.0/24 is directly connected, GigabitEthernet0/1
L       10.22.185.1/32 is directly connected, GigabitEthernet0/1
D       10.22.186.0/25 [90/20512256] via 10.0.9.1, 00:32:55, Serial0/2/0
D       10.22.186.128/25 [90/20517376] via 10.0.9.14, 00:32:56, Serial0/0/0
D       10.22.187.0/27 [90/20514560] via 10.0.9.1, 00:32:55, Serial0/2/0
D       10.22.187.32/27 [90/20514560] via 10.0.9.1, 00:32:55, Serial0/2/0
D       10.22.187.64/27 [90/20514560] via 10.0.9.1, 00:32:55, Serial0/2/0
D       10.22.187.96/28 [90/20514560] via 10.0.9.1, 00:32:55, Serial0/2/0
D    53.0.0.0/8 [90/20517120] via 10.0.9.14, 00:32:56, Serial0/0/0
D    64.0.0.0/8 [90/20517120] via 10.0.9.14, 00:32:56, Serial0/0/0
D    209.165.202.0/24 [90/20514560] via 10.0.9.14, 00:32:56, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Таблиця маршрутизації на Turta_R2

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 22 subnets, 6 masks
C       10.0.9.0/30 is directly connected, Serial0/2/0
L       10.0.9.1/32 is directly connected, Serial0/2/0
C       10.0.9.4/30 is directly connected, Serial0/2/1
L       10.0.9.5/32 is directly connected, Serial0/2/1
D       10.0.9.8/30 [90/21024000] via 10.0.9.2, 00:26:57, Serial0/2/0
                    [90/21024000] via 10.0.9.6, 00:22:18, Serial0/2/1
D       10.0.9.12/30 [90/21024000] via 10.0.9.2, 00:18:23, Serial0/2/0
                     [90/21024000] via 10.0.9.18, 00:16:31, Serial0/0/0
C       10.0.9.16/30 is directly connected, Serial0/0/0
L       10.0.9.17/32 is directly connected, Serial0/0/0
D       10.0.9.20/30 [90/21024000] via 10.0.9.6, 00:18:43, Serial0/2/1
                     [90/21024000] via 10.0.9.18, 00:16:31, Serial0/0/0
D       10.22.184.0/24 [90/20512256] via 10.0.9.6, 00:20:44, Serial0/2/1
D       10.22.185.0/24 [90/20512256] via 10.0.9.2, 00:28:52, Serial0/2/0
C       10.22.186.0/25 is directly connected, GigabitEthernet0/2
L       10.22.186.1/32 is directly connected, GigabitEthernet0/2
D       10.22.186.128/25 [90/20517376] via 10.0.9.18, 00:06:53, Serial0/0/0
C       10.22.187.0/27 is directly connected, GigabitEthernet0/1.19
L       10.22.187.1/32 is directly connected, GigabitEthernet0/1.19
C       10.22.187.32/27 is directly connected, GigabitEthernet0/1.29
L       10.22.187.33/32 is directly connected, GigabitEthernet0/1.29
C       10.22.187.64/27 is directly connected, GigabitEthernet0/1.39
L       10.22.187.65/32 is directly connected, GigabitEthernet0/1.39
C       10.22.187.96/28 is directly connected, GigabitEthernet0/1.99
L       10.22.187.97/32 is directly connected, GigabitEthernet0/1.99
D    53.0.0.0/8 [90/20517120] via 10.0.9.18, 00:12:16, Serial0/0/0
D    64.0.0.0/8 [90/20517120] via 10.0.9.18, 00:06:57, Serial0/0/0
D    209.165.202.0/24 [90/20514560] via 10.0.9.18, 00:12:28, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Таблиця маршрутизації на Turta_R3

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 16 subnets, 7 masks
D       10.0.0.0/8 is a summary, 00:33:34, Null0
D       10.0.9.0/30 [90/21024000] via 10.0.9.17, 00:33:30, Serial3/0
                    [90/21024000] via 10.0.9.13, 00:33:29, Serial2/0
D       10.0.9.4/30 [90/21024000] via 10.0.9.17, 00:33:31, Serial3/0
                    [90/21024000] via 10.0.9.21, 00:33:30, Serial6/0
D       10.0.9.8/30 [90/21024000] via 10.0.9.21, 00:33:30, Serial6/0
                    [90/21024000] via 10.0.9.13, 00:33:29, Serial2/0
C       10.0.9.12/30 is directly connected, Serial2/0
C       10.0.9.16/30 is directly connected, Serial3/0
C       10.0.9.20/30 is directly connected, Serial6/0
S       10.22.184.0/21 is directly connected, FastEthernet4/0
D       10.22.184.0/24 [90/20512256] via 10.0.9.21, 00:33:34, Serial6/0
D       10.22.185.0/24 [90/20512256] via 10.0.9.13, 00:33:29, Serial2/0
D       10.22.186.0/25 [90/20512256] via 10.0.9.17, 00:33:31, Serial3/0
D       10.22.186.128/25 [90/20005376] via 209.165.202.2, 00:33:38, FastEthernet4/0
D       10.22.187.0/27 [90/20514560] via 10.0.9.17, 00:33:31, Serial3/0
D       10.22.187.32/27 [90/20514560] via 10.0.9.17, 00:33:31, Serial3/0
D       10.22.187.64/27 [90/20514560] via 10.0.9.17, 00:33:31, Serial3/0
D       10.22.187.96/28 [90/20514560] via 10.0.9.17, 00:33:31, Serial3/0
D    53.0.0.0/8 [90/20005120] via 209.165.202.2, 00:33:38, FastEthernet4/0
D    64.0.0.0/8 [90/20005120] via 209.165.202.2, 00:33:38, FastEthernet4/0
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
D       209.165.202.0/24 is a summary, 00:33:39, Null0
C       209.165.202.0/27 is directly connected, FastEthernet4/0
S*   0.0.0.0/0 is directly connected, FastEthernet4/0
               [1/0] via 209.165.202.2
D    64.0.0.0/8 [90/20517120] via 10.0.9.18, 00:06:57, Serial0/0/0
D    209.165.202.0/24 [90/20514560] via 10.0.9.18, 00:12:28, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Таблиця маршрутизації на Turta_R5

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.0.9.9 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 18 subnets, 6 masks
D       10.0.9.0/30 [90/21024000] via 10.0.9.9, 00:33:09, Serial0/2/1
                    [90/21024000] via 10.0.9.5, 00:33:08, Serial0/2/0
C       10.0.9.4/30 is directly connected, Serial0/2/0
L       10.0.9.6/32 is directly connected, Serial0/2/0
C       10.0.9.8/30 is directly connected, Serial0/2/1
L       10.0.9.10/32 is directly connected, Serial0/2/1
D       10.0.9.12/30 [90/21024000] via 10.0.9.9, 00:33:09, Serial0/2/1
                     [90/21024000] via 10.0.9.22, 00:33:09, Serial0/0/0
D       10.0.9.16/30 [90/21024000] via 10.0.9.22, 00:33:13, Serial0/0/0
                     [90/21024000] via 10.0.9.5, 00:33:08, Serial0/2/0
C       10.0.9.20/30 is directly connected, Serial0/0/0
L       10.0.9.21/32 is directly connected, Serial0/0/0
C       10.22.184.0/24 is directly connected, GigabitEthernet0/1
L       10.22.184.1/32 is directly connected, GigabitEthernet0/1
D       10.22.185.0/24 [90/20512256] via 10.0.9.9, 00:33:09, Serial0/2/1
D       10.22.186.0/25 [90/20512256] via 10.0.9.5, 00:33:08, Serial0/2/0
D       10.22.186.128/25 [90/20517376] via 10.0.9.22, 00:33:13, Serial0/0/0
D       10.22.187.0/27 [90/20514560] via 10.0.9.5, 00:33:08, Serial0/2/0
D       10.22.187.32/27 [90/20514560] via 10.0.9.5, 00:33:08, Serial0/2/0
D       10.22.187.64/27 [90/20514560] via 10.0.9.5, 00:33:08, Serial0/2/0
D       10.22.187.96/28 [90/20514560] via 10.0.9.5, 00:33:08, Serial0/2/0
D    53.0.0.0/8 [90/20517120] via 10.0.9.22, 00:33:13, Serial0/0/0
D    64.0.0.0/8 [90/20517120] via 10.0.9.22, 00:33:13, Serial0/0/0
D    209.165.202.0/24 [90/20514560] via 10.0.9.22, 00:33:13, Serial0/0/0
D*EX 0.0.0.0/0 [170/25632000] via 10.0.9.9, 00:33:09, Serial0/2/1
               [170/25632000] via 10.0.9.5, 00:33:08, Serial0/2/0
```

Таблиця маршрутизації на Turta_R0

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 64.100.13.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
D       10.0.0.0/8 [90/20010496] via 64.100.13.1, 00:34:05, GigabitEthernet0/0
C       10.22.186.128/25 is directly connected, GigabitEthernet0/1
L       10.22.186.129/32 is directly connected, GigabitEthernet0/1
D    53.0.0.0/8 [90/30720] via 64.100.13.1, 00:34:09, GigabitEthernet0/0
     64.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       64.100.13.0/30 is directly connected, GigabitEthernet0/0
L       64.100.13.2/32 is directly connected, GigabitEthernet0/0
D    209.165.202.0/24 [90/30720] via 64.100.13.1, 00:34:09, GigabitEthernet0/0
D*EX 0.0.0.0/0 [170/25637120] via 64.100.13.1, 00:34:02, GigabitEthernet0/0
```