ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Розробка корпоративної комп'ютерної мережі на базі технології FHRP для підприємства»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Владислав ДІДОВЕЦЬ*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-41
Владислав ДІДОВЕЦЬ
Ім'я, ПРІЗВИЩЕ

Керівник: Ігор БУЧЕНКО
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедрою Наталія ЛАЩЕВСЬКА
_____Ім'я, ПРІЗВИЩЕ
«_____» _____ 2024р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дідовець Владислав Максимович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Розробка корпоративної комп'ютерної мережі на базі технології FHRP для підприємства
керівник кваліфікаційної роботи Ігор БУЧЕНКО,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024р. № 36
2. Строк подання кваліфікаційної роботи «3» червня 2024р.
3. Вихідні дані до кваліфікаційної роботи: протоколи технології FHRP: HSRP, VRRP, GLBP; хмарні технології: IaaS, SaaS, PaaS; топологія мережі, логічна топологія (Layer 3), фізична топологія (Layer 2), одноранговa мережа (P2P), клієнт-серверна мережа; IPv4/IPv6; технологія PoE; модулі SFP; мережеві протоколи: TCP, UDP, DHCP;
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Поняття корпоративної комп'ютерної мережі. віртуалізація та FHRP
2. Інфраструктура корпоративної комп'ютерної мережі
3. Провадження та підтримка корпоративної мережі
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання «27» лютого 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	28.02-24.03.2024	Виконано
2	Обробка матеріалу	23.03-05.04.2024	Виконано
3	Розробка теоретичної частини	06.04-10.04.2024	Виконано
4	Розробка моделі мережі	11.04-20.04.2024	Виконано
5	Висновки за результатами аналізу	21.04-06.05.2024	Виконано
6	Оформлення пояснювальної записки	07.05-08.05.2024	Виконано
7	Розробка презентації	09.05-11.05.2024	Виконано
8	Передзахист	14.05-17.05.2024	Виконано
9	Здача в деканат	27.05-3.06.2024	Виконано

Здобувач вищої освіти _____ Владислав ДІДОВЕЦЬ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ігор БУЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 45 стор., 29 рис., 4 табл., 30 джерел.

Мета роботи – Розробка корпоративної комп'ютерної мережі на базі технології FHRP для підприємства

Об'єкт дослідження – Корпоративна комп'ютерна мережа на базі технології FHRP для підприємства

Предмет дослідження – Комп'ютерна мережа на базі технології FHRP

Короткий зміст роботи: Існуючі корпоративні комп'ютерні мережі є доволі різноманітними. Кожна з них потребує індивідуального підходу при проєктуванні та має свої особливості. В сучасному світі все є прив'язаним до мережі Інтернет. Тож коли зникає Інтернет чи з ним є проблеми це перешкоджає нормальній роботі та може приносити збитки. Тож постає питання, як з боку компанії забезпечити постійний Інтернет навіть при виході якогось обладнання з ладу. Це досягається використанням надійного обладнання, резервними шляхами та використанням двох чи більше маршрутизаторів. Таку можливість надає технологія FHRP. Вона забезпечить доступ до Інтернету у випадку виходу маршрутизатора з ладу бо резервний маршрутизатор одразу включиться в роботу. Проте для того аби правильно обрати потрібний варіант FHRP варто розглянути, що таке корпоративна комп'ютерна мережа її особливості побудови та вимоги.

На основі проведеного дослідження було з'ясовано актуальність використання FHRP в корпоративній комп'ютерній мережі, особливості її побудови, етапи та приклад компанії, що потребуватиме її використання.

КЛЮЧОВІ СЛОВА: ТЕХНОЛОГІЯ FHRP, ТЕХНОЛОГІЯ КОРПОРАТИВНА КОМП'ЮТЕРНА МЕРЕЖА, HSRP, VRRP, GLBP, IAAS, SAAS, PAAS, IPV4/IPV6, POE

ЗМІСТ

ВСТУП

В наш час комп’ютерні мережі є невід’ємною складовою нашого життя. Вони присутні всюди де є людина та її діяльність. Комп’ютерні мережі відрізняються одна від одної через сферу їх застосування, масштаби та покладенні на них завдання. Найпростішим прикладом є домашня мережа, а найскладнішим - мережі в великому офісі з різноманітними підрозділами у світі. Вихід до мережі Інтернет забезпечується інтернет-провайдером, а вдома та офісі для цього існує маршрутизатор (роутер). У випадку домашньої мережі є недорогий та простий роутер, що здатен забезпечити доступ до мережі Інтернет та хорошу швидкість інтернету до 1 Гб/с. В корпоративній комп’ютерній мережі потрібні вищі швидкості та різноманітні сервіси. При використанні домашнього роутера в корпоративній мережі він не забезпечить нормальної швидкості та не зможе надати необхідні сервіси. Тому для корпоративних комп’ютерних мереж використовують потужні роутери, що забезпечують високу швидкість та відповідні сервіси. Проте, у випадку використання одного роутера мережа може бути вразливою. Оскільки один роутер може стати вузьким місцем (bottleneck) в мережі через його недостатню пропускну здатність або вихід з ладу. Для того, щоб компанія мала стабільний доступ до мережі Інтернет, у випадку виходу з ладу основного роутера, можна мати два або більше маршрутизаторів, що братимуть участь у роботі або виконуватимуть функцію резервних. Це в свою чергу усуває недостатню пропускну здатність в мережі та створює надлишковість та відмовостійкість. В такому випадку потрібно правильно налаштувати та змусити працювати їх як одне ціле. Саме таку можливість надає технологія FHRP, завдяки якій можна налаштувати маршрутизатори, як резервні на випадок виходу основного з ладу так і будуть працювати в режимі балансування.

РОЗДІЛ 1. ПОНЯТТЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ. ВІРТУАЛІЗАЦІЯ ТА FHRP

1.1 Корпоративна комп'ютерна мережа

Комп'ютерна мережа – це система з двох чи більше взаємопов'язаних пристроїв, що можуть обмінюватися інформацією[1].

Корпоративна комп'ютерна мережа – це система, що складається з двох та більше комп'ютерів, принтерів, серверів, іншої офісної техніки, які знаходяться в одній компанії й поєднані між собою різноманітними каналами зв'язку(рис. 1.1). Ця мережа використовується для обміну даними, ресурсами та послугами серед компанії чи з зовнішніми користувачами. В сучасному світі існує безліч прикладів застосування корпоративних комп'ютерних мереж. Їх ми можемо зустріти в: фінансових установах, освітніх і дослідницьких центрах, в середньому або великому бізнесі (регіональному або міжнародному). Отже, у цих випадках ми будемо мати не схожі між собою мережі, бо у кожної компанії є своя сфера діяльності та вимоги. І підхід до побудови мережі буде індивідуальний з великим різноманіттям технологій та архітектур.

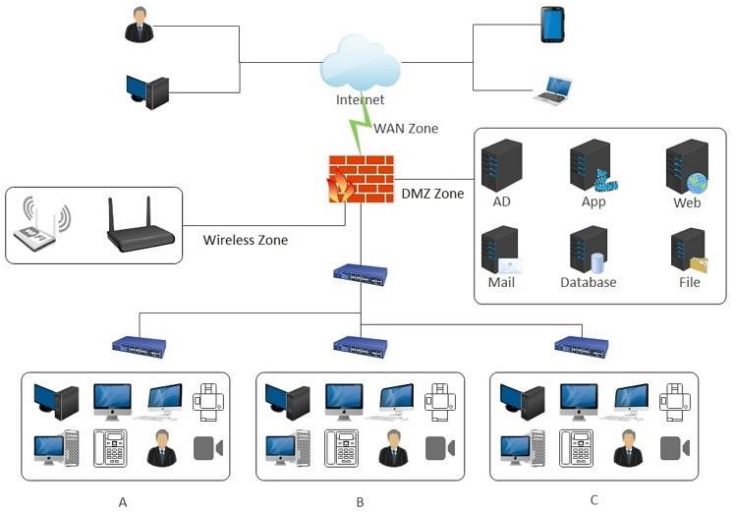


Рисунок 1.1 – Приклад корпоративної комп'ютерної мережі

Вимоги до корпоративної комп'ютерної мережі. Вимоги до корпоративної комп'ютерної мережі будуть відрізнятися в залежності від сфери діяльності компанії. Тому наведемо загальні вимоги для побудови будь-якої корпоративної комп'ютерної мережі:

1. достатня пропускна здатність – це кількісна характеристика мережі, яка визначає, скільки даних може бути передано через неї за одиницю часу. Вона вимірюється в бітах на секунду (біт/с), мегабітах на секунду (Мбіт/с), гігабітах на секунду (Гбіт/с) або терабітах на секунду (Тбіт/с). Корпоративна комп'ютерна мережа повинна мати достатню пропускну здатність для опрацювання трафіку, що генерується користувачами, пристроями та програмами. Це важливо аби забезпечити нормальне функціонування мережі, якісне обслуговування користувачів й уникати затримок. Вона має розраховуватися при піковому навантаженні на мережу, оскільки для нас важливо її функціонування при максимальному навантаженні;

2. надійність мережі – це здатність мережі функціонувати без перебоїв у роботі та відмов обладнання, забезпечуючи доступ користувачів до мережі Інтернет та сервісів, що надає компанія. Надійність мережі досягається шляхом створення надлишковості та відмовостійкості. Це включає в себе наявність резервних шляхів доставки інформації, резервного обладнання та використання хмарних технологій для частини завдань. Також це здатність швидко відновлювати свою роботу після перевантаження та/або відмови;

Безпека мережі – це комплекс заходів направлених на забезпечення безпеки в корпоративній комп'ютерній мережі. В цей комплекс заходів входить встановлення системи контролю доступу (СКД), використання антивірусного програмного забезпечення (ПЗ), брандмауера, впровадження спеціальних політик доступу, забезпечення резервного копіювання тощо. Використання окремої спеціальної кімнати для встановлення важливого мережевого обладнання (маршрутизатори, комутатори, сервери, фаєрволи тощо). В цій системі доступ може надаватися за допомогою карток, паролів біометрії тощо. Її використання допоможе запобігти фізичному втручанню сторонніх осіб в інші відділи та

обладнання. Наприклад, коли прибиральник може випадково зачепити той чи інших пристрій або провід. Також встановлення брандмауера є обов'язковим. Брандмауер, Firewall чи міжмережевий екран – один із інструментів для захисту комп'ютера від кібератак та інших загроз із мережі Інтернет. Він забезпечує фільтрацію мережевого трафіку, що проходить в мережу через нього й на основі налаштованих політик безпеки приймає рішення про блокування цього трафіку чи пропуску. Також він блокує несанкціонований доступ до обладнання та ресурсів, налаштовуючи права доступу. Забезпечує захист від DDoS атак, вірусів, троянських програм, шкідливого програмного забезпечення й інших видів мережевих атак. Спеціальні політики доступу – це політики доступу користувачів до різних сегментів в мережі та її ресурсів. Вони забезпечуються різним програмним забезпеченням для надання, контролю та обліку тих хто має доступ до різних сегментів чи ресурсів в мережі. Забезпечення резервного копіювання з одної сторони це питання надійності та відмовостійкості, але також це питання й безпеки. Оскільки завдяки цим діям у випадку збою в системі чи цілеспрямованої атаки ми можемо безпечно відновити конфігурацію та данні;

3. масштабованість – це вимога до мережі та її здатність масштабуватися в залежності від спадаючих чи зростаючих потреб компанії без необхідності значних витрат на її перебудову чи розширення. Це виражається у наявності запасних або вільних портів для підключення нових пристроїв чи налаштування нового робочого місця. Також це може виражатися в запасі пропускної здатності, сервісах або обладнанні. Оскільки при розширенні мережі в компанії нам може знадобитися створення нового відділу для працівників, впровадження нових периферійних пристроїв;

4. керованість – це можливість ефективного та зручного керування налаштуванням чи моніторингом мережі. Воно виражається у використанні спеціального програмного забезпечення та вебсервісів. Вони представляють собою програми для моделювання мережі, радіопланування, моніторингу стану обладнання, трафіку та продуктивності мережі. Прикладами таких програм є: Cisco Packet Tracer, Wireshark, tcpdump, Ekahau AI Pro тощо;

5. резервування важливих даних – це резервне копіювання даних користувачів, конфігурацій обладнання, створення копій віртуальних машин для їх швидкого розгортання та відновлення. Резервування даних важливо робити, щоб уникнути непередбачуваних ситуацій. Наприклад, втрата даних на робочому місці, хакерська атака, яка націлена на знищення важливих даних, зміни в конфігурації, що призводять до збоїв в обладнанні або вихід з ладу обладнання, в тому числі у випадку короткого замикання;

6. підтримка периферійного обладнання – це можливість підключення у мережу таких пристроїв: принтери, сканери, аудіо-/відеообладнання, проєктори, IoT-пристрої.

1.2 Віртуалізація в корпоративних комп'ютерних мережах

Віртуалізація – це технологія, яка дає можливість створювати віртуальні версії когось або чогось. Віртуалізація дозволяє нам на одному фізичному робочому місці розгортати декілька віртуальних робочих місць(рис. 1.3)[2]. Це забезпечує гнучкість та безпеку для роботи користувачів. Ми можемо зробити віртуальне робоче місце на базі існуючих операційних систем (ОС) чи на одному фізичному сервері розгорнути декілька віртуальних серверів, що будуть надавати різні сервіси. Як наслідок нам не треба витрачати багато коштів на розгортання робочих місць/серверів на великій кількості фізичного обладнання. Варто зазначити, що завдяки віртуалізації з'явилися та розвиваються хмарні технології[3].

Хмарні технології – це технології, які надають користувачу доступ до певних послуг або ресурсів через мережу Інтернет. Користувач лише сплачує кошти за підписку на певний сервіс. Самі хмарні технології ми можемо поділити на три типи(рис.1.2):

1. інфраструктура як послуга (IaaS) — це надання хмарним провайдером обчислювальних ресурсів, таких як віртуальні сервери, мережі та сховища у вигляду онлайн-сервісу. Користувачі можуть використовувати надані IaaS-ресурси для запуску своїх власних програм, мереж та інших систем;

2. програмне забезпечення як послуга (SaaS) – це надання хмарним провайдером програмного забезпечення як онлайн-сервісу. Користувачі можуть використовувати програмне забезпечення без необхідності купівлі, встановлення та підтримки на своєму власному комп'ютері чи сервері;

3. платформа як послуга (PaaS) — це надання платформи або інструментів для розробки та розгортання програм. Користувачі можуть використовувати PaaS-платформи для створення, тесту та запуску власних програм без необхідності володіння та управління інфраструктурою[4].

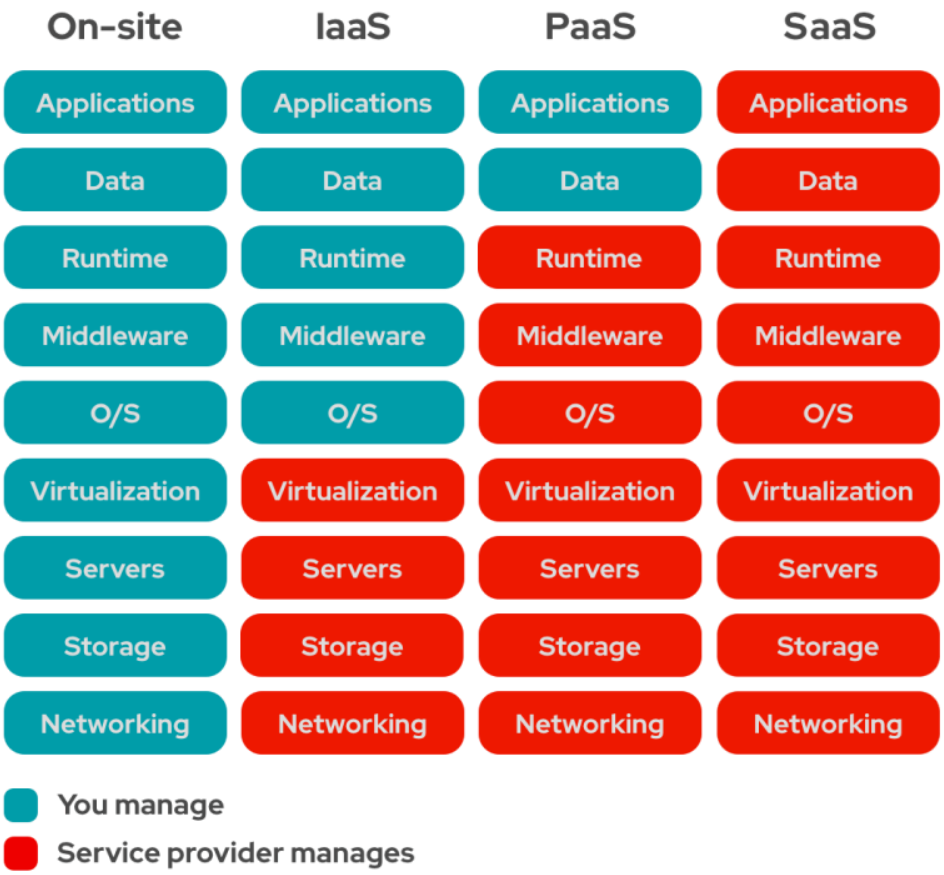


Рисунок 1.2 – Типи хмарних технологій PaaS, SaaS, IaaS[5]

У випадку з апаратною частиною мережі можна використовувати технологію

FHRP (First-hop redundancy protocol). Простими словами це створення одного віртуального маршрутизатора на базі декількох маршрутизаторів. Існують різні варіанти її реалізації, про них буде описано в наступних розділах роботи.

Рисунок 1.3 – «Звичайна» віртуалізація

1.3 Технологія FHRP для побудови надійної корпоративної мережі

Технологія FHRP (First-hop redundancy protocol) – це технологія резервування першого переходу, розроблена для захисту шлюзу за замовчуванням, що використовується в підмережі, дозволяючи двом або більше маршрутизаторам забезпечувати резервне копіювання цієї адреси у разі виходу з ладу активного маршрутизатора[1][13]. Використання цієї технології є гарним варіантом для забезпечення надійного з’єднання з мережею Інтернет в корпоративній комп’ютерній мережі. Оскільки в сучасних мережах маршрутизатори

використовуються для під’єднання користувачів до мережі Інтернет. Тож він може стати ймовірною точкою відмови в мережі й при його виході з ладу користувачі втрачають доступ до мережі Інтернет. В залежності від роду діяльності компанії це може спричинити фінансові, репутаційні збитки або зупинити її роботу. Це спонукає компанію мати резервний маршрутизатор в мережі для його використання в разі виходу з ладу основного. Проте шлюз за замовчуванням може мати тільки одну адресу. Таку проблему може вирішити технологія FHRP. Вона дозволяє налаштувати маршрутизатори на одну адресу, що в свою чергу забезпечить функціонування мережі при виході одного з маршрутизаторів з ладу.

РОЗДІЛ 2. ІНФРАСТРУКТУРА КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Архітектура корпоративної комп'ютерної мережі

Архітектура мережі – це структурний та організаційний план, що визначає фізичну, логічну топологію, схеми під'єднання пристроїв, вид комп'ютерної мережі, протоколи, сервіси, систему безпеки та безпосереднє розташування обладнання[6]. Вона описує взаємозв'язок між різними компонентами мережі: комутаторами, маршрутизаторами, серверами, комп'ютерами, периферійними та IoT пристроями, що використовуються для обміну даними.

Топологія мережі – це фізична та логічна структура з'єднання пристроїв у комп'ютерній мережі. Вона описує спосіб з'єднання користувачів та пристроїв у мережі й визначає, як данні передаються між пристроями[8].

Логічна топологія (Layer 3) – це опис з'єднань, що визначають та показують шляхи для обміну даними між різними вузлами в мережі незалежно від їх фізичного розташування(рис. 2.1-2.2).

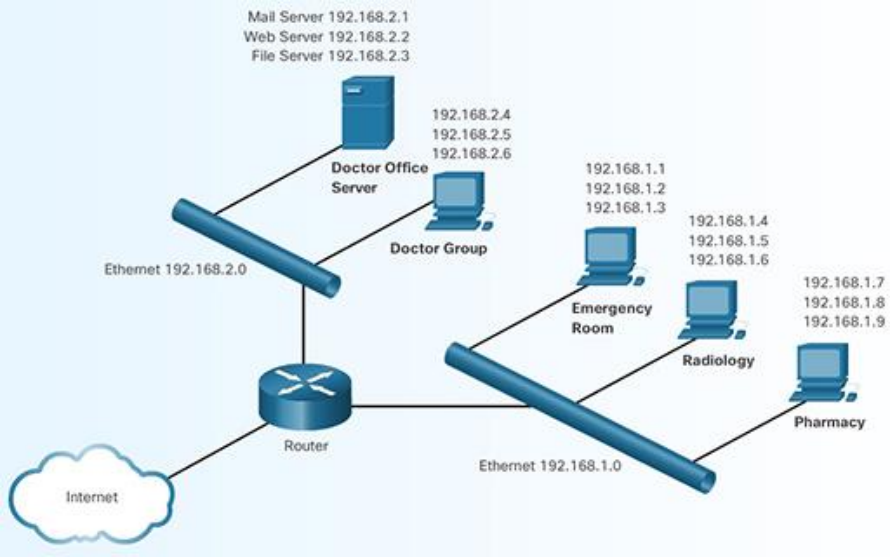


Рисунок 2.1 – «Проста» логічна топологія мережі

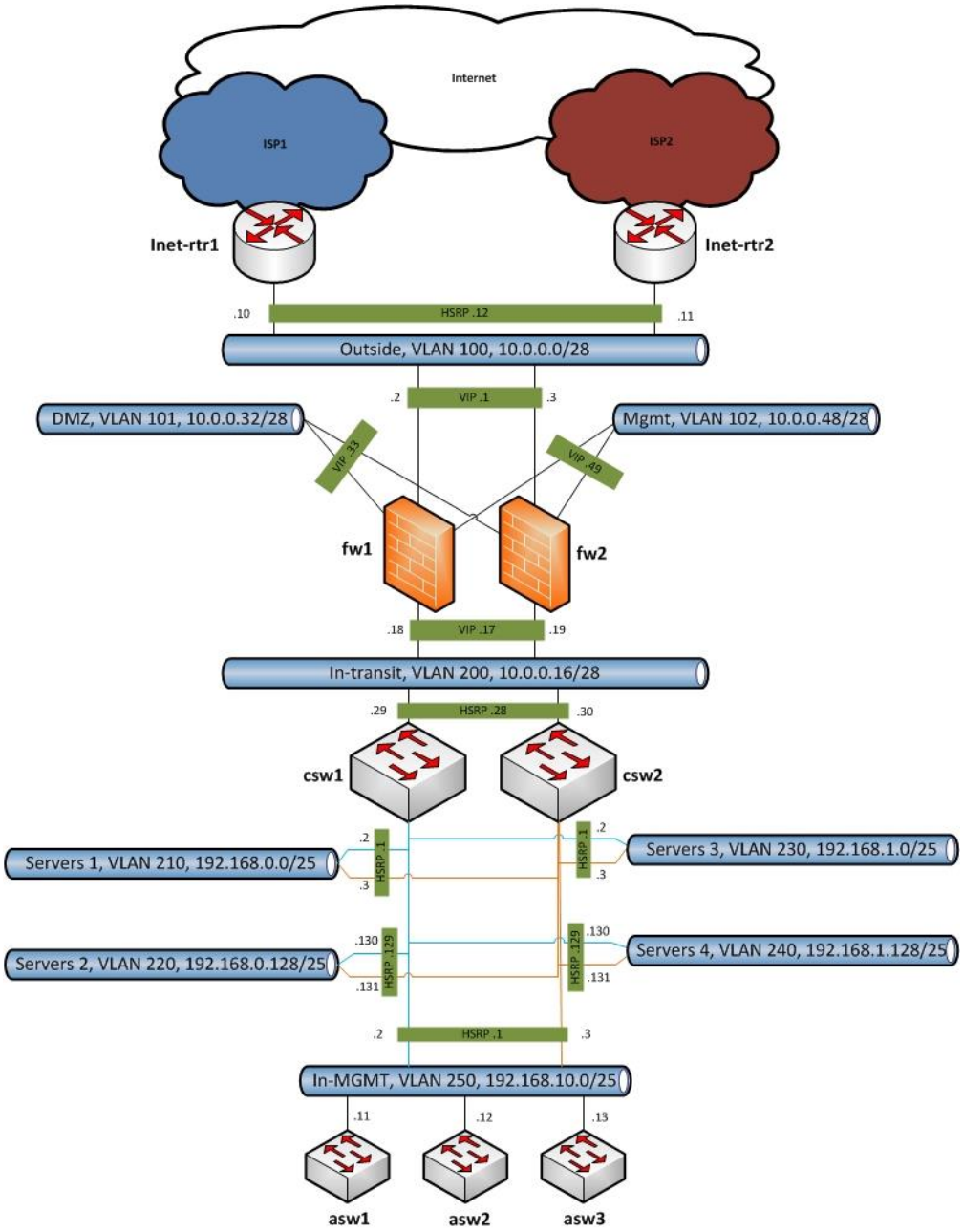


Рисунок 2.2 – «Складна» логічна топологія мережі

Фізична топологія (Layer 2) – це схема, що показує розташування різних елементів мережі та їх підключення між собою(рис. 2.3-2.4)[9]. Тобто з фізичної топології ми бачимо, як комп'ютер взаємодіє з принтером, сервером, іншими комп'ютерами чи з роутером задля виходу в Інтернет. Ми безпосередньо бачимо як відбувається підключення, комунікація та якими кабелями це реалізується.

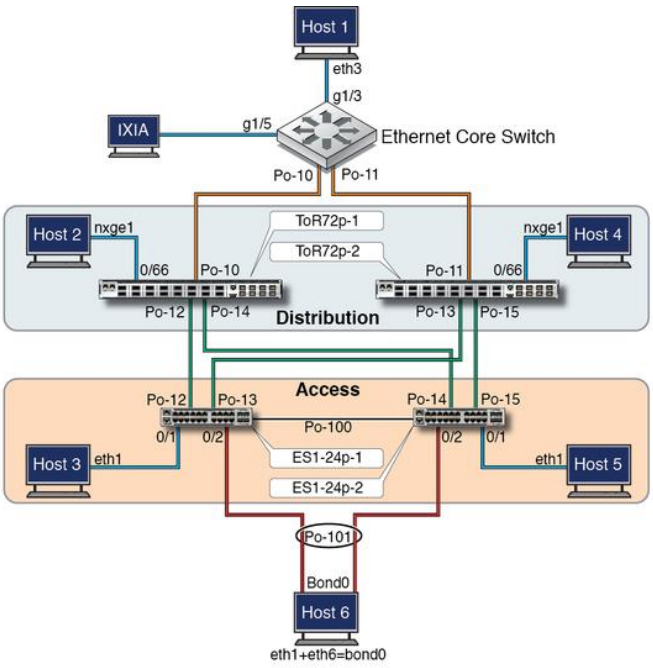


Рисунок 2.3 – «Проста» фізична топологія

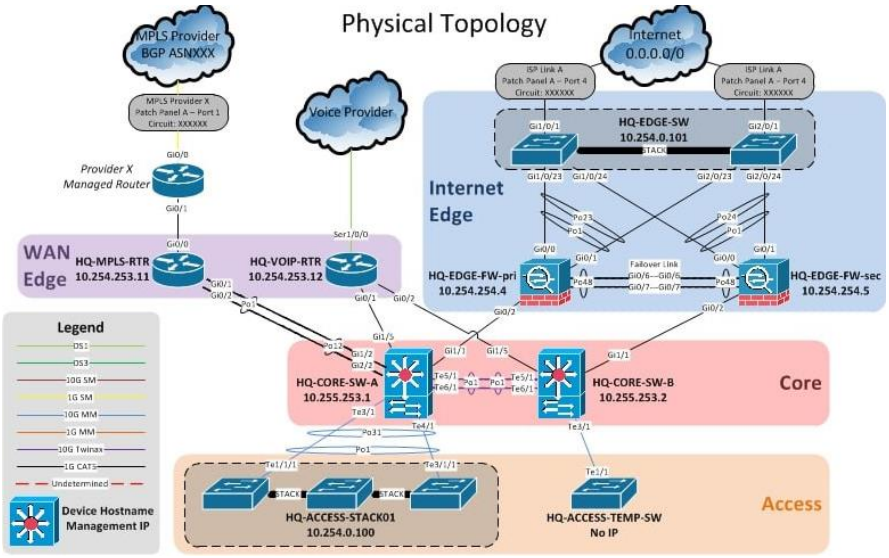


Рисунок 2.4 – «Складна» фізична топологія

Також варто згадати схематичне зображення розташування пристроїв в стійках, шафах та безпосереднє підключення кабелів в порти пристроїв (рис. 2.5-2.6). Ці схеми дають розуміння, які пристрої де розташовані й зображення схеми використання портів забезпечує просте та зручне керування та виправлення неполадок. Оскільки в такому випадку адміністратор мережі має розуміння, як розташовані пристрої, що необхідні, та в який саме порт вони підключені. Тож йому не доводиться вгадувати й створювати проблеми в мережі своїм пошуком

випадково вимкнувши не той лінк.

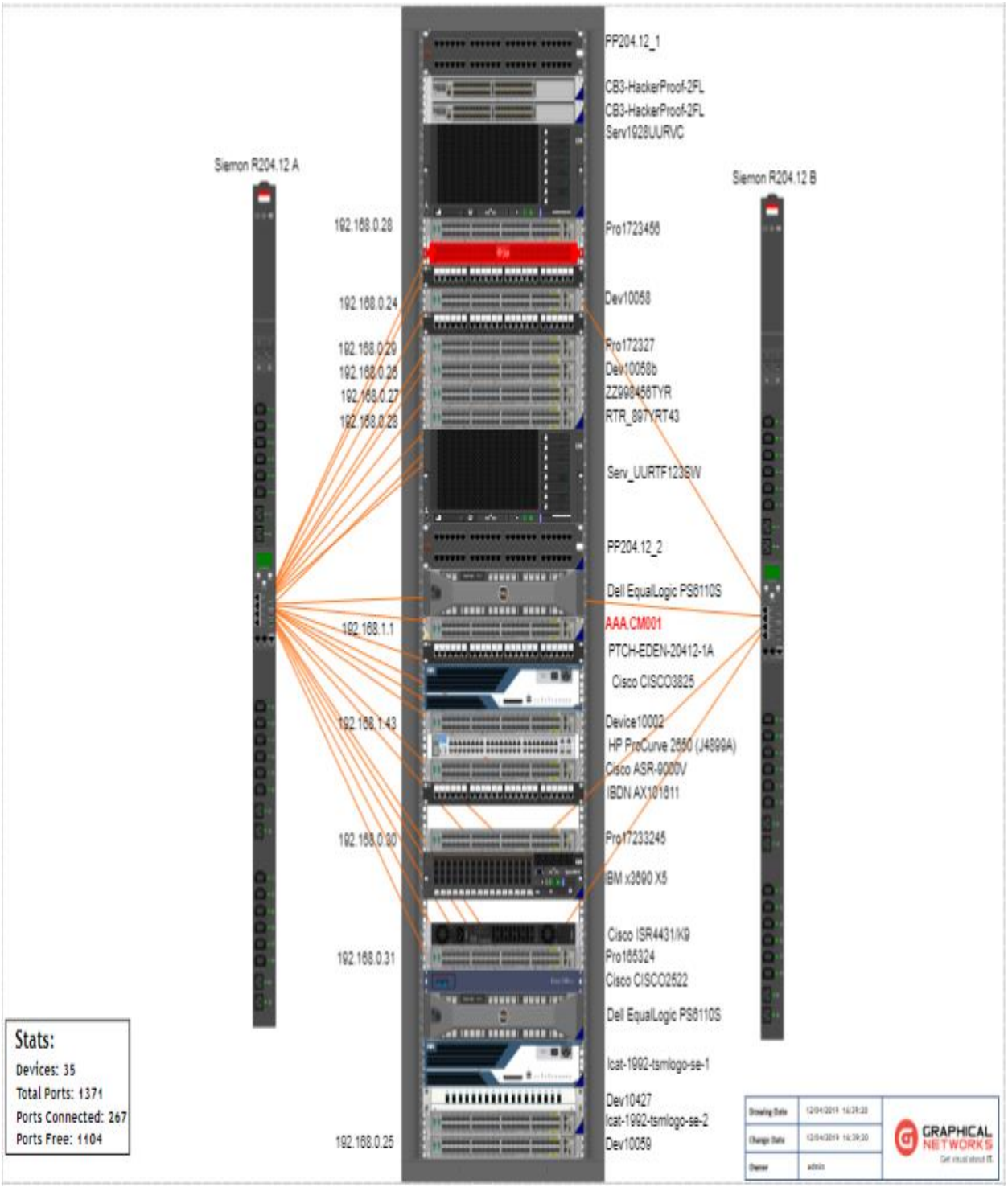


Рисунок 2.5 – Комутаційний шафа

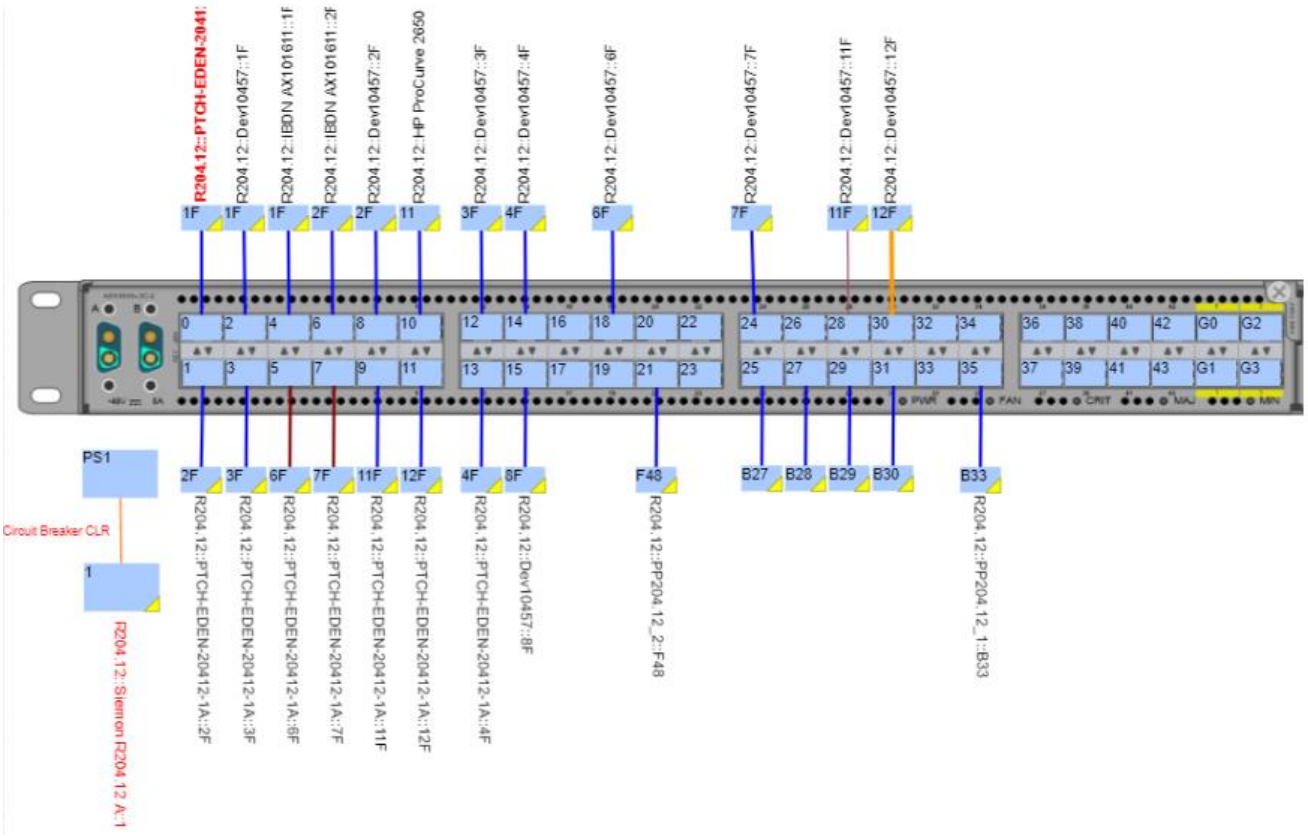


Рисунок 2.6 – Схема фізичного під’єднання обладнання

Типи архітектури мережі. В сучасному світі існує безліч мереж, що відрізняються між собою за розмірами, сферою застосування й складністю побудови. Будь-яка мережа будується в залежності від поставлених їй вимог, що визначають її модель та складність побудови. Вона може бути побудована, як за визначеним типом так бути гібридною. Існує два основних типи мереж, на які орієнтуються при побудові[7]:

– однорангова мережа;

– клієнт-серверна мережа.

Однорангова мережа (Peer-to-peer, P2P) – це мережа, в якій всі пристрої є рівноправними та можуть взаємодіяти один з одним без ієрархічної системи(рис. 2.7). Це означає, що файли, які знаходяться на одному комп’ютері є доступними для будь-якого іншого комп’ютера в мережі. Якщо принтер під’єднаний до одного пристрою, то він є видимим для усіх інших пристроїв у мережі. Зазвичай однорангові мережі можуть використовуватися в навчальних закладах задля

зручності роботи, навчання та дослідження. Також однорангову мережу використовують всілякі торренти, де завантаження файлів здійснюється з пристроїв користувачів.

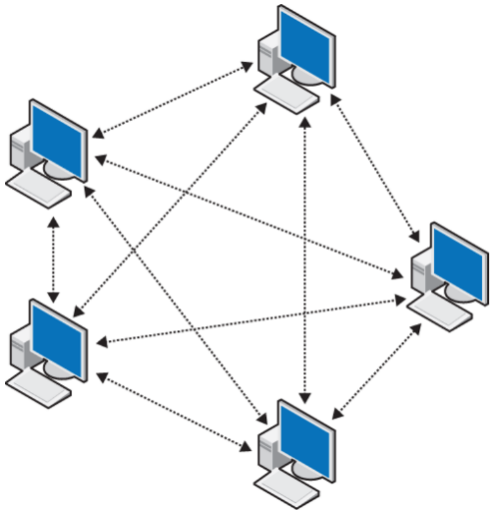


Рисунок 2.7 – Однорангова мережа

Переваги однорангової мережі:

1. спільний доступ до ресурсів. В такій мережі нам немає необхідності мати виділений сервер оскільки кожен комп’ютер виступає в ролі клієнта та сервера одночасно. Тобто дані зберігаються на кожному комп’ютері й за потреби він ці дані надає всім або сам бере з іншого комп’ютера;

2. відмовостійкість. Відмовостійкість даної мережі виражається наступним чином: якщо будь-який комп’ютер виходить з ладу, то в нас лише зникає доступ до файлів на цьому комп’ютері, але інші комп’ютери продовжують працювати й обмінюватися даними.

3. економія коштів. Оскільки немає потреби у дорогих виділених серверах або централізованій інфраструктурі, вартість налаштування та підтримки мережі однорангової мережі може бути нижчою, ніж використання мережі з спеціалізованим мережевим обладнанням та залучення спеціалістів.

Недоліки однорангової мережі:

1. складність в керуванні. Такою мережею складніше керувати, оскільки всі учасники мають рівні права та можливості. Це в свою чергу вимагає додаткової

координації з користувачами задля роз’яснення правил зберігання даних. Тому, що кожен користувач може встановити на своєму комп’ютері свою систему зберігання файлів, яка може бути незрозумілою для інших, що сповільнить продуктивність;

2. залежність від доступності однорангових пристроїв. Це залежність від постійного підключення в мережу кожного учасника задля доступу до даних чи ресурсів. Тобто, якщо користувач вимикає комп’ютер чи він ламається, то інші користувачі не можуть отримати доступ до нього, що негативно вплине на їх роботу. Також може бути втрачена цілісність даних;

3. безпека. Дана мережа має підвищені ризики, оскільки відповідальність за безпечні файли, програмне забезпечення (ПЗ), відсутність вірусів несе відповідальність лише користувач;

4. порушення авторських прав. Оскільки всі дані в мережі є доступними для кожного користувача, то кожен може їх переглядати за допомогою різноманітних програм. Такий підхід не забезпечує безпеку інтелектуальної власності та захищеність авторських прав.

Клієнт-серверна мережа – це модель мережі, де доступ кінцевих користувачів до різних ресурсів здійснюється за допомогою виділеного сервера з різними правами доступу для користувачів(рис. 2.8). Ця модель використовується вебсерверами, файловими серверами, поштовими серверами та базами даних.

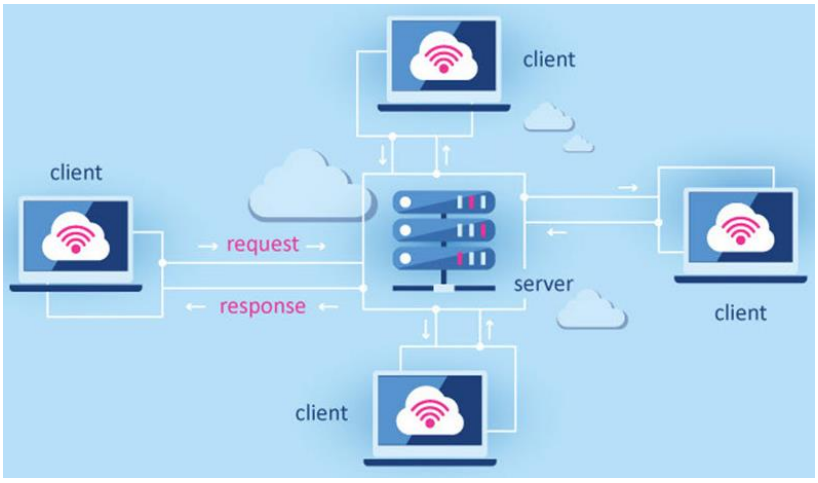


Рисунок 2.8 – Клієнт-серверна модель мережі

Працює ця модель доступу наступним чином:

1. клієнт надсилає запит до серверу з проханням надати доступ до ресурсів чи інформації;

2. сервер запитує дані користувача для з'ясування, які права є у даного користувача;

3. користувач надсилає свій логін та пароль на перевірку серверу;

4. сервер приймає ці дані та обробляє їх;

5. у випадку відсутності прав чи відсутності такого користувача сервер запросить дані знову;

6. якщо логін та пароль підійшли, тоді користувачу надається доступ до ресурсів або даних, які він запитував;

7. користувач починає використовувати дані чи ресурси.

Тобто процедура доступу в скороченому вигляді складається в 3 дії:

1. клієнтський запит;

2. обробка запиту сервером;

3. передача даних.

Переваги мережі клієнт-сервер:

1. масштабованість: клієнт-серверна модель легко масштабується для підтримки великої кількості користувачів і ресурсів;

2. надійність: сервери можуть бути більш потужними та надійними, ніж клієнти, що робить мережу більш стійкою до збоїв;

3. безпека: сервери можуть бути краще захищені від несанкціонованого доступу, ніж клієнти;

4. централізоване управління: ресурсами мережі можна легко управляти з центрального сервера.

Недоліки мережі клієнт-сервер:

1. залежність від сервера: клієнти залежать від серверів для надання ресурсів. Якщо сервер виходить з ладу, клієнти не можуть працювати;

2. вартість: клієнт-серверні мережі можуть бути дорогими для впровадження та обслуговування;

3. складність: клієнт-серверні мережі можуть бути складними для налаштування та обслуговування.

2.2 Протоколи та сервіси

Одною з складових архітектури корпоративної комп’ютерної мережі будуть протоколи та сервіси, що використовуються в мережі. Мережеві протоколи відіграють важливу роль у функціонуванні корпоративних комп’ютерних мереж. Вони забезпечують зв’язок, доступ до ресурсів, безпеку й впливають на вибір мережевого обладнання. Протоколи – це система правил, яка дозволяє двом або більше об'єктам системи зв'язку передавати інформацію. Розглянемо деякі з основних:

IPv4/IPv6 – це дві версії протоколу IP (Internet Protocol), що використовуються для адресації пристроїв в Інтернет. Завдяки цим протоколам пристрої мають свої унікальні адреси у мережі, які забезпечують між ними спілкування. IPv4 використовує 32-бітові адреси, що надає до 4,3 мільярда адрес. Ця версія була прийнята у 1981 році. Проте з часом вільні адреси цієї версії почали вичерпуватися. Тоді на заміну прийшов IPv6, що прийнятий у 1998 році але активне розповсюдження цієї версії почалося у другій половині 2000-х років і продовжується зараз. IPv6 використовує 128-бітові адреси, що 340 секстильйонів унікальних адрес(табл. 2.1)[10]. Така кількість доступних адрес вирішує проблему вичерпання адрес IPv4. Від розуміння версії Internet Protocol буде залежати, яка обладнання та технології варто використовувати.

Таблиця 2.1 – Порівняння протоколів IPv4 та IPv6

IPv4	IPv6
Випущений 1981	Випущений 1998
32-bit IP address	128-bit IP address
4.3 міліарди адрес	7.9x1028 адрес
Числовий крапково-десятковий запис 192.168.5.18	Алфавітно-цифровий шістнадцятковий запис 50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified – 50b2:6400::6c3a:b17d:0:10a9)
DHCP або ручна конфігурація	DHCP або автоконфігурація

TCP (Transmission Control Protocol) – це протокол, що забезпечує надійну передачу даних між пристроями у мережі. Він розбиває дані на пакети та надсилає їх через мережу, впорядковуючи їх при доставці для забезпечення доставки без помилок та в правильному порядку. Кожному пакету присвоюється номер для правильного впорядкування даних при отриманні. Під час роботи TCP встановлює та зберігає з'єднання між відправником і отримувачем до завершення передачі даних[11].

UDP (User Datagram Protocol) – це протокол, що забезпечує передачу даних між пристроями в мережі, проте без встановлення з’єднання. Він використовується для передавання трафіку, що чутливий до затримок, такого як відео, аудіо або запити DNS. У порівнянні з TCP, UDP не гарантує надійне з'єднання, що може призвести до втрати частини даних, але він працює швидше за TCP (рис. 2.9).

DHCP (Dynamic Host Configuration Protocol) – це протокол динамічної конфігурації вузла, що дозволяє пристроям автоматично отримувати IP-адресу, адресу шлюзу, DNS-серверу, що необхідні для роботи в мережі. Цей протокол є в двох версіях для IPv4/IPv6. Він розгортається на маршрутизаторі чи сервері в залежності від потреб кожної мережі[12].

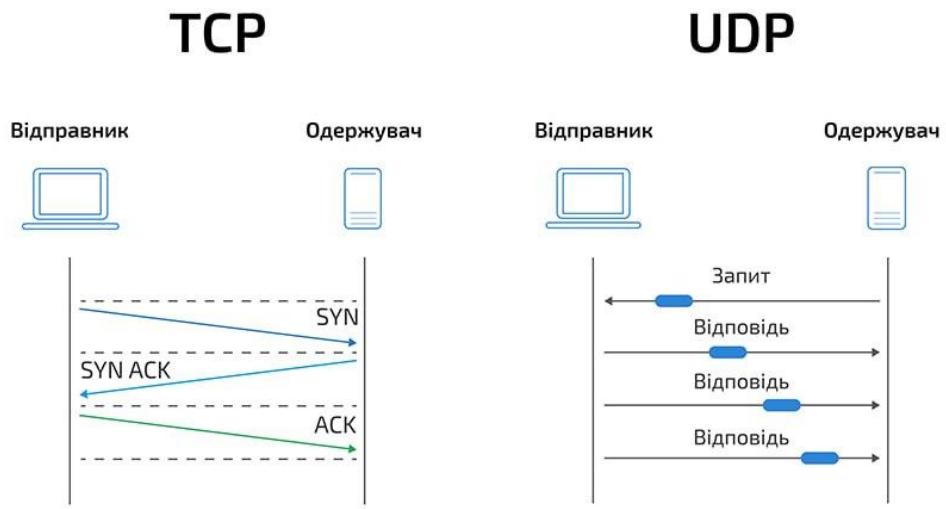


Рисунок 2.9 – Порівняння UDP та TCP

HTTP (Hypertext Transfer Protocol) – це протокол, що використовується для передачі вебсторінок та інших мультимедійних вмістів через Інтернет. HTTPS (HTTP Secure) – це версія протоколу HTTP, що використовує шифрування для забезпечення безпеки передачі даних(рис. 2.10)[14].

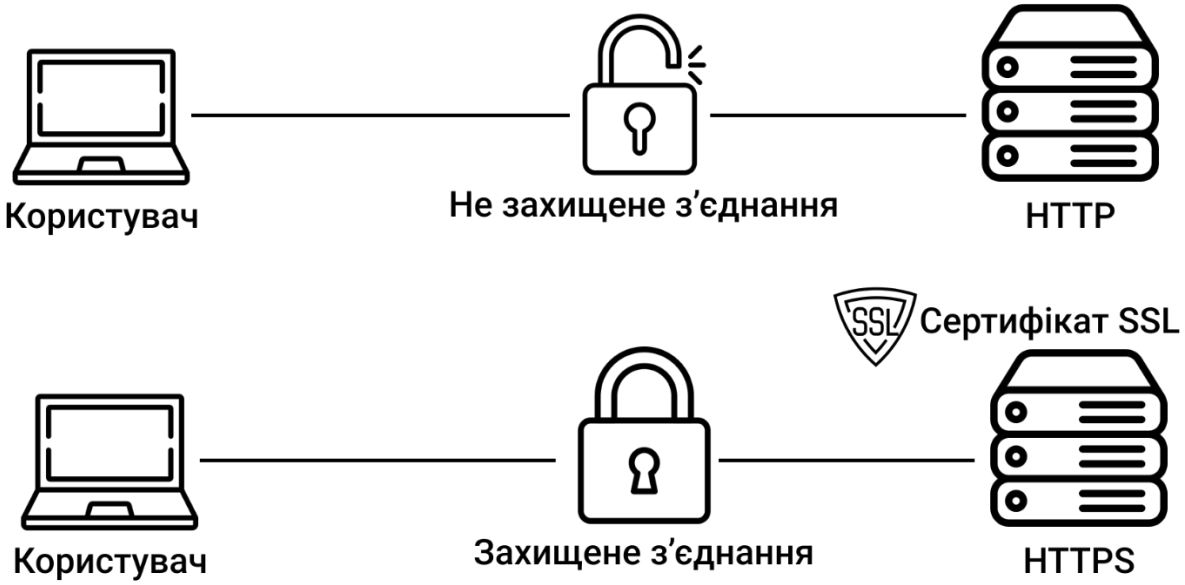


Рисунок 2.10 – Порівняння HTTP та HTTPS

AAA (Authentication, Authorization, Accounting) – це опис процесів, що використовуються для централізованого керування доступом користувачів до мережевих ресурсів[15]. Існує два протоколи, що це забезпечують: RADIUS, TACACS+(табл. 2.2). RADIUS (Remote Authentication Dial-In User Service) – це

протокол передачі даних, що використовується в комп'ютерних мережах для автентифікації, авторизації та обліку різноманітних сервісів[16]. TACACS+ – це протокол безпеки, що використовується в рамках AAA для забезпечення централізованої автентифікації користувачів, що хочуть отримати доступ до мережі чи ресурсів[17].

Таблиця 2.2 – Різниця між RADIUS та TACACS+

RADIUS	TACACS+
Поєднує автентифікацію та авторизацію.	Розділяє всі 3 елементи AAA, роблячи його більш гнучким.
Менш безпечний виконує лише хешування пароля.	Більш безпечний – шифрує весь пакет, включаючи ім’я користувача, пароль і атрибути.
Вимагає, щоб кожен мережевий пристрій містив конфігурацію авторизації.	Центральне керування конфігурацією авторизації.
Немає журналу команд.	Повне журналювання команд.
Мінімальна підтримка постачальника для авторизації.	Підтримується більшістю основних постачальників.
UDP – порти UDP без підключення 1645/1646, 1812/1813	TCP – Орієнтований на підключення TCP-порт 49
Розрахований на абонента AAA	Призначений для адміністратора AAA

Корпоративна комп’ютерна мережа може використовувати різноманітні сервіси й розгортати їх в своїй мережі або використовувати хмарні сервіси. Популярними сервісами є файлові сервіси, поштові та хмарні. Розгортання сервісів в локальній мережі компанії є доволі витратною справою тому це доцільно робити в тому випадку, якщо на цьому наполягають фахівці з безпеки, данні є конфіденційними та на це є виділений бюджет. Це можуть бути певні конфігурації, програми, дослідницька інформація тощо. Проте, якщо специфіка даних дозволяє використовувати хмарні сервіси то варто надавати перевагу їм. Оскільки компанії потрібно лише оформити підписку на хмарний сервіс й вона миттєво отримає доступ до нього. Хмарні сервіси є досить гнучкими тож з ними зручно працювати для компанії, бо сервіси доступні з будь-якого місця світу де у вас є інтернет. Проте остаточний вибір протоколів та сервісів буде залежати від сфери діяльності

компанії, її бюджету та вимог безпеки.

2.3 Фізичне розташування обладнання

Фізичне розташування обладнання. Питання фізичного розташування мережі є дуже важливим, оскільки від цього залежить зручність керування та безпека. Наприклад, в невеликих фірмах чи навчальних закладах можна побачити, як мережеве обладнання(комутатори, маршрутизатори, міжмережевий екран, тощо) розкидане по різним кімнатам та коридорам. У випадку, якщо це патч-панель чи інтернет-розетки це – припустимо, але якщо ми бачимо як комутатор або маршрутизатор знаходиться в кабінеті чи коридорі без простого захисту, у вигляді маленької шафки, це – неправильно. В такому випадку обладнання може бути несвідомо чи свідомо пошкоджене або постраждає від пилу та бруду. Коридори доступні для всіх, як і більшість кімнат, що створює загрозу безпеці та погіршує управління. Тому гарним рішенням буде виділити спеціальну кімнату із системою контролю доступу, де все обладнання буде зібрано. Таке приміщення буде мати систему клімат-контролю, для підтримки нормальної вологості, та температури для нормальної роботи обладнання. Там будуть розташовані спеціальні стійки та шафи для монтування обладнання та кабель-менеджменту. Отже, маючи таке приміщення зі встановленою СКД забезпечується фізична безпека обладнання, доступ до якого будуть мати лише системні адміністратори(рис. 2.11). Проте варто зазначити, що не завжди буде можливість зосередити все в одній кімнаті чи кімнатах. Але варто зазначити, що не завжди усе обладнання буде в одному приміщені. Наприклад, комутатори доступу можуть бути розташовані на поверхах й потребувати нормального встановлення. У такому випадку

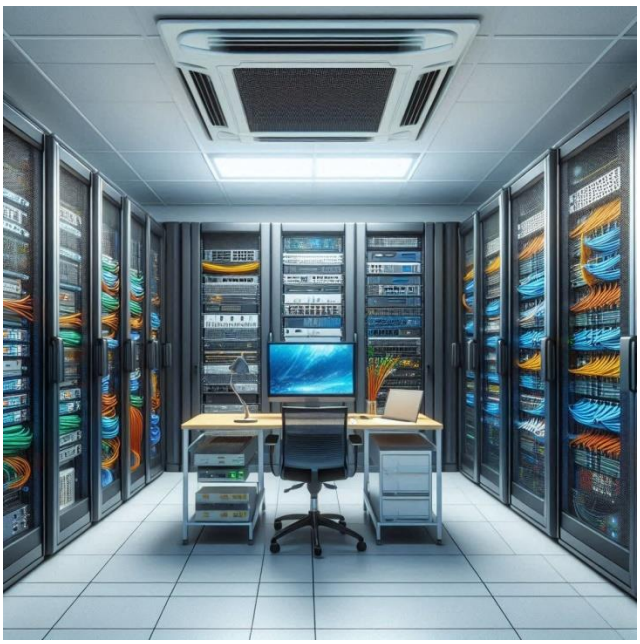


Рисунок 2.11 – Приклад кімнати з мережевим обладнанням

2.4 Критерії вибору мережевого обладнання

Під час розробки корпоративної комп’ютерної мережі одним із завдань є вибір мережевого обладнання. Підбір обладнання проводиться на етапі коли є розробленні топології мережі, відома кількість користувачів та пристроїв, визначені необхідні сервіси та ресурси у цій мережі згідно з побажаннями замовника. Тож при наявності цієї інформації можна приступати до вибору мережевого обладнання в корпоративну комп’ютерну мережу. Наведемо критерії, на які варто звертати увагу при підборі обладнання:

1. *розмір мережі*. Для того, щоб почати підбір обладнання необхідно розуміти її масштаби корпоративної комп’ютерної. Оскільки обладнання для кав’ярні, коворкінг-центру чи бізнес-центру будуть відрізнятися й неможна встановлювати однакове всюди. По-перше, потрібно знати на якій території будується мережа та для якого замовника. Тобто потрібно мати план будівлі (рис. 2.12) чи приміщення (рис. 2.13) й розуміти в якій сфері працює компанія. По-друге, необхідно знати кількість працівників, що максимально розрахована по штату,

оскільки саме під них розраховується максимальна кількість пристроїв в мережі. По-третє, необхідно мати планування робочого простору офісу від дизайнера та комунікувати з ним задля нормально розміщення пристроїв й уникнення кабельного жаху. Кабельний жах – це відсутність компактного та продуманого підключення, що призводить до наявності на підлозі чи навколо робочих місць кабелів живлення та інформаційних кабелів, які починають заважати нормальному переміщенню персоналу. Адже в такому випадку кабелі заплутуються один в одному та є великі ризики їх зачепити при пересуванні. Володіючи цією інформацією можна переходити до інших критеріїв;

Рисунок 2.12 – План будівлі

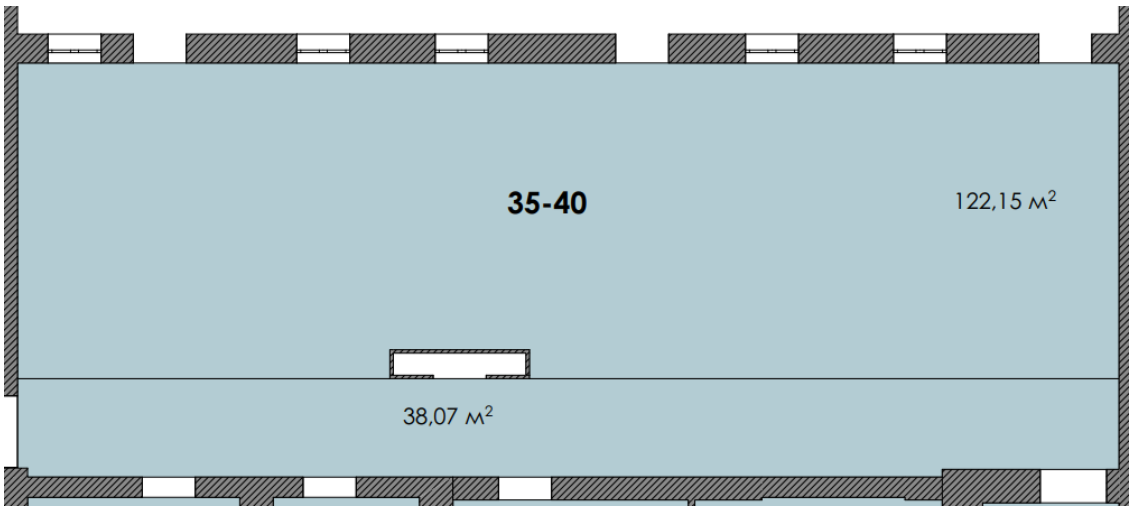


Рисунок 2.13 – Кількість працівників в кімнаті

2. *масштабування мережі*. Треба розуміти, що при побудованій мережі її розширення може бути проблематичним та дорогим. Пов’язано це з тим, що при розробці мережі в неї вже закладають максимально можливе підключення користувачів й пристроїв виходячи з планів компанії та її бюджету. Звісно масштабування мережі можливе, але потрібно враховувати шляхи як це забезпечити. Можна передбачити появу нових відділів та певної кількості нових працівників шляхом закладання їх у початкові розрахунки мережі. Або у випадку майбутнього розширення будівлі, шляхом добудови нового корпусу, можна закласти запасні магістральні лінії й взяти більш потужне обладнання або збільшити кількість існуючого. Проте обидва цих випадки мають прораховуватися заздалегідь, оскільки розширення існуючої мережі може стати невигідним з економічної точки зору, ніж створення нової на новій ділянці.

3. *кількість користувачів*. Під час планування необхідно знати кількість користувачів, які передбачаються штатом. Оскільки на кожного користувача або групу користувачів розраховують кількість пристроїв на робочому місці. Кількість користувачів має розраховуватися замовником з запасом на можливе розширення.;

4. *пропускна здатність*. Розрахунок пропускної здатності відбувається з урахуванням кількості користувачів, сервісів, що використовуються, типу діяльності користувача та можливого пікового навантаження. Якщо користувачі у мережі потребують одномоментно пропускної здатності від 2 до 5 Гб/с, а в нас є

тільки 1 Гб/с, то це створить затримку, що погіршить ефективність роботи та якість обслуговування клієнтів чи в найгіршому випадку виведе з ладу мережу; Також варто враховувати тип трафіку, що курсуватиме у мережі. Оскільки в компанії може бути великий внутрішній трафік, проте назовні буде виходити лише невелика його частина, або буде навпаки. Тож важливо розуміти де й яка пропускна здатність є необхідна;

5. *надійність мережі.* Цей критерій є важливим для побудови мережі та вибору обладнання, оскільки він передбачає надійне з'єднання, забезпечення тимчасового джерела живлення на випадок аварійного завершення роботи, резервні шляхи, резервне копіювання та наявність резервного обладнання;

6. *розуміння типу підключення пристроїв.* При підборі обладнання для корпоративної комп'ютерної мережі необхідно враховувати різні варіанти підключення мережевого обладнання та кінцевих користувачів до мережі. Існує два варіанти підключення до мережі: дротове та бездротове[18]. Дротовий варіант зазвичай використовується для підключення настільних комп'ютерів, а також IP-телефонії, телевізорів, проєкторів, багатофункціональних пристроїв (БФП) тощо. Дротове з'єднання є більш безпечним та надійним, оскільки воно менш вразливе. Також воно здатне забезпечувати високу пропускну здатність й стабільну швидкість. Бездротовий варіант (Wi-Fi) використовується для підключення телефонів, планшетів, ноутбуків та різноманітних IoT-пристроїв. Цей варіант підключення є гнучким та дозволяє користувачу переміщуватися в різні місця в межах діапазону дії роутера чи точки доступу (Access Point). В такому випадку користувач не залежить від дротів й можна підключити не один пристрій до Інтернету. Це зручно впроваджувати у кав'ярнях, парках, заправних станціях чи торгових центрах для забезпечення клієнтам доступу до мережі Інтернет. Проте недоліком цього варіанту є послаблення сигналу за стінами будівель чи накладання сигналів один на одного. Також при використанні Wi-Fi варто використовувати високий ступінь захисту й не користуватися відкритим Wi-Fi, оскільки це може призвести до хакерської атаки на пристрій. Варто зазначити, що бездротовий варіант підключення останнім часом доступний майже для всіх девайсів.

Наприклад, настільний ПК можна під’єднати за допомогою Wi-Fi, якщо той має спеціальну мережеву карту(рис. 2.15) чи адаптер в материнській платі(рис.2.14).

Рисунок 2.14 – Wi-Fi адаптер на материнській платі Asus ROG MAXIMUS Z790 APEX

Рисунок 2.15 – Wi-Fi-адаптер Asus PCE-AX1800

Проте, в наш час багатофункціональні пристрої (БФП), проєктори, телевізори тощо підтримують з’єднання за допомогою Wi-Fi. Тож враховуючи переваги та недоліки обох варіантів можна перейти до визначення варіанту підключення

пристроїв. Оскільки мова йде про корпоративну комп’ютерну мережу, то з цього випливає, що мережа розрахована на велику кількість користувачів. Розглянемо це на прикладі великої ігрової компанії, що має власний великий офіс. Для підключення настільних комп’ютерів краще використовувати дротовий варіант, оскільки він забезпечить стабільне з’єднання та високу швидкість. Цілком ймовірно, що компанія буде мати власний бездротовий інтернет для працівників та гостей компанії. В такому випадку в приміщеннях будуть встановленні точки доступу. Тож варто розглянути які пристрої можуть бути підключені до точок доступу Wi-Fi. Перш за все до Wi-Fi будуть підключені телефони, планшети та ноутбуки. Даними пристроями можуть користуватися, як працівники для можливості вільно пересуватися з робочими девайсами по території компанії так і гості компанії в спеціальних кімнатах для демонстрації або гостьових зонах.

Розглядаючи відділ з наявністю до 30 працівників, слід врахувати наявність пристроїв, які потребують підключення до мережі, таких як принтер, сканер, IoT-пристрої, проєктор або телевізор. Кожен з цих пристроїв потребує доступу до Інтернету. Якщо ми вирішимо забезпечити підключення за допомогою дротового з'єднання, це може вимагати відводу додаткових портів та кабелів для кожного з них, що, в свою чергу, може призвести до затрат на додаткове мережне обладнання та встановлення захисних кожухів для дротів. У великих компаніях, де може бути декілька таких відділів, це може створити значне навантаження на мережеву інфраструктуру та збільшити кількість потрібних з'єднань. Проте, цю ситуацію можна уникнути, використовуючи бездротове підключення. Воно дозволить уникнути складнощів з проведенням додаткових кабелів та портів і зменшить витрати на обслуговування мережі. Оскільки раніше було сказано про використання точок доступу, можна використовувати їх для підключення даних пристроїв. Сучасних можливостей бездротового з’єднання цілком вистачить для покриття цих потреб. Оскільки ці пристрої, крім IoT-пристроїв, будуть використовуватися лише час від часу й не створюватимуть дуже великого навантаження на мережу. IoT-пристрої можуть функціонувати постійно в залежності від їх завдання. IoT-пристроєм може бути датчик температури,

вологості, вуглекислого газу тощо. При використанні IoT-пристроїв та Access Point варто враховувати підтримку технології Power over Ethernet (PoE). Power over Ethernet (PoE) – це технологія передачі електроенергії та даних за допомогою «витої пари»(рис. 2.16)[19]. Це наддасть змогу зручніше розміщувати ці пристрої не прив'язуючись до розеток й використання подовжувачів. Отже під час вибору мережевого обладнання для корпоративної комп'ютерної мережі варто також враховувати варіанти під'єднання їх до мережі Інтернет та електромережі, бо це дозволяє позбутися зайвих витрат та краще розмістити їх в компанії.

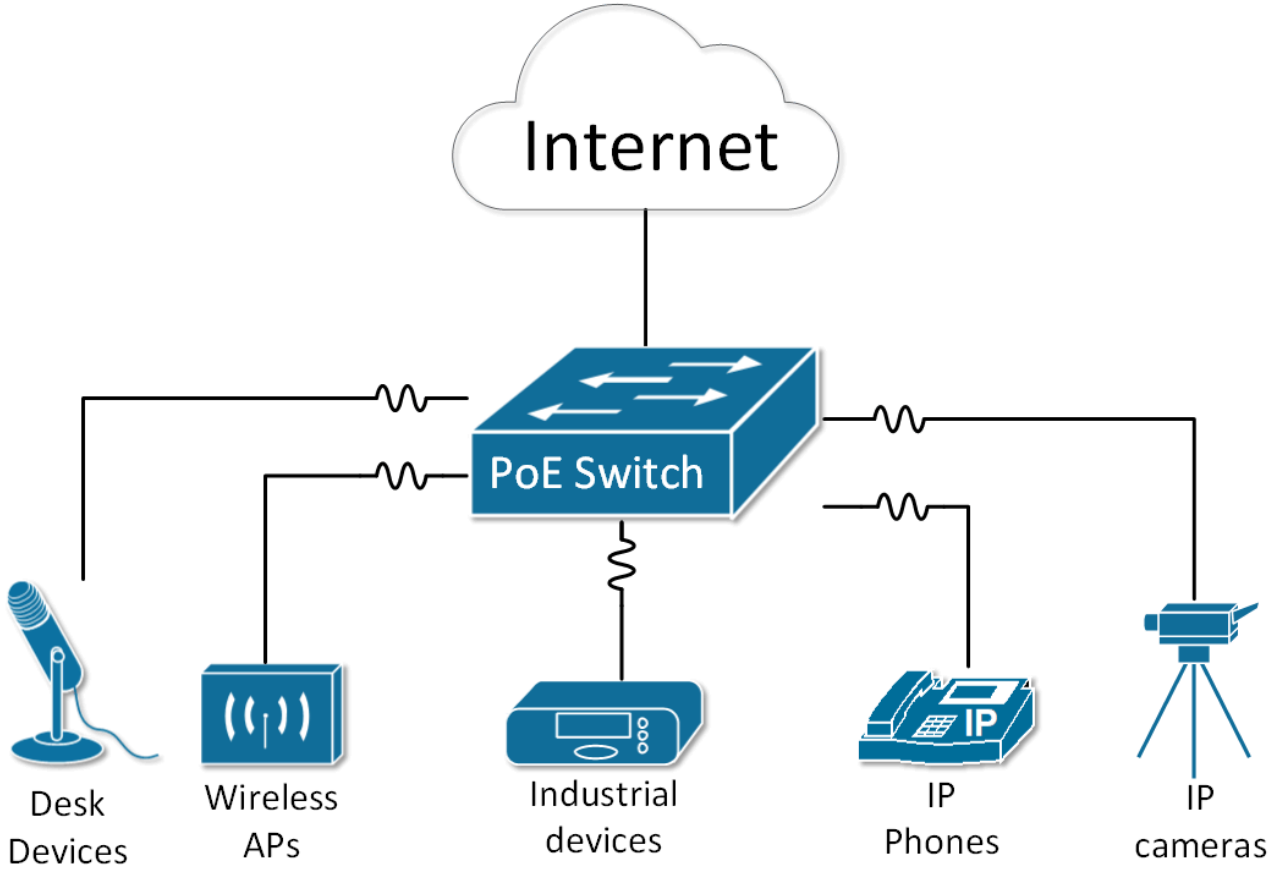


Рисунок 2.16 – Технологія PoE

7. *бюджет*. Бюджет – це кількість грошей розрахована та виділена на ту чи іншу справу людиною або компанією. Він завжди має бути фіксованим і повинен мати певний запас для маневру. Тому при розробці корпоративної комп'ютерної мережі потрібно знати всі деталі описані раніше задля розрахунку витрат і надання фінальної суми на обговорення замовнику.

Врахувавши ці критерії, можна приступати до вибору мережевого обладнання для корпоративної комп’ютерної мережі звертаючи увагу на поставлені вимоги до мережі та особливості мережевого обладнання.

Патч-панель – це одна із складових частин структурованої кабельної системи призначеної для з’єднання між собою пристроїв й оперативного перемикання обладнання[20]. За кількістю портів існують від 4 до 48 портів(рис. 2.17) й мають різні типи портів за швидкістю. Типи портів за швидкістю передачі даних зображені в таблиці 2.3[21].

Таблиця 2.3 – Ethernet Cable Categories

Категорія	Швидкість	Частота
CAT 1	Передає тільки голос	1MHz
CAT 2	4Mbps	4MHz
CAT 3	10Mbps	16MHz
CAT 4	16Mbps	20MHz
CAT 5	100Mbps	100MHz
CAT 5e	1000Mbps	100MHz
CAT 6	1000Mbps	250MHz
CAT 7	10Gbps	600MHz
CAT 7a	10Gbps	1000Gbps
CAT 8	25Gbps	2000Mhz

Також додатковими факторами є матеріал з якого вони зроблені та вид монтажу. Вони бувають виготовленні з металу чи пластику й бувають настінного чи стійкового монтажу, тому при виборі варто враховувати ці фактори. Розрахунок кількості необхідних патч-панелей – це кількість пристроїв у корпоративній комп’ютерній мережі поділена на кількість портів в обраній патч-панелі.

Рисунок 2.17 – Патч-панель на 48 портів

Комутатор – це мережевий пристрій, що забезпечує з’єднання різноманітних пристроїв в мережі та передає пакети даних з одного пристрою до іншого використовуючи таблиці MAC-адрес[23]. Існує багато варіантів мережевих комутаторів. Вони відрізняються між собою портами, керованістю, додатковими функціями, кріпленням та живленням, що визначає в яких мережах вони можуть застосовуватися. Також вибір їх характеристик та кількості виходить з максимально розрахованої кількості пристроїв в мережі. Тож при виборі комутатора необхідно спиратися на наступні критерії вибору:

1. кількість підключених пристроїв в корпоративній комп’ютерній мережі; Цей критерій показує максимально можливу кількість пристроїв, що будуть у мережі. До таких пристроїв входять: стаціонарні комп’ютери, ноутбуки, принтери, сканери, проєктори, телевізори, камери, IoT-пристрої тощо. Тож необхідна кількість комутаторів визначається поділом суми усіх пристроїв на кількість портів в комутаторі;

Рисунок 2.18 – Види комутаторів

2. порти. Комутатори мають різну кількість портів в залежності від сфери застосування або кількості пристроїв. Вони бувають на 5, 8, 16, 24 або 48 порти(рис. 2.18). Окрім кількості порти комутаторів відрізняється за швидкістю передачі даних, яка забезпечується різними SFP модулями[25]. SFP (Small Form-factor Pluggable) — промисловий стандарт модульних компактних приймачів (трансиверів), використовуваних для передачі даних в телекомунікаціях. Вони можуть бути вбудовані в комутатор або є можливість доставити потрібні модулі. В залежності від того який модуль буде використовуватися(мідний чи оптичний) буде доступна різна швидкість передавання даних(рис. 2.19). При підборі обладнання на офіційному сайті виробника зазвичай ця інформація вказується;

Рисунок 2.19 – Оптичний(справа) та мідний(зліва) модулі SFP

3. властивості портів. Цей критерій показує чи можливо використання частини або усіх портів для живлення пристрою та передачі даних. Це

забезпечується технологією PoE (Power over Ethernet), яка дозволяє наприклад: підключити точку доступу надавши їй живлення через кабель Ethernet(табл. 2.4)[24];

Таблиця 2.4 – Cisco Catalyst 9300 Series switch configurations

Модель	Total 10/100/1000, Multigigabit copper or SFP Fiber	Конфігурація Uplink	Джерело живлення за замовчуванням
Варіанти портів			
C9300X-48HX	48 port Cisco UPOE+, 48x 10G Multigigabit (10G/5G/2.5G/1G/100M) with 90W UPOE+	Modular Uplinks	1100W AC
C9300X-48TX	48 port Data, 48x 10G Multigigabit (10G/5G/2.5G/1G/100M)	Modular Uplinks	715W AC
C9300X-48HXN	48 port Cisco UPOE+, 8x 10G Multigigabit (10G/5G/2.5G/1G/100M) + 40x 5G Multigigabit (5G/2.5G/1G/100M)	Modular Uplinks	1100W AC
C9300X-24HX	24 port Cisco UPOE+, 24x 10G Multigigabit (10G/5G/2.5G/1G/100M)	Modular Uplinks	1100W AC
C9300X-12Y	12 port 25G/10G/1G SFP28	Modular Uplinks	715W AC
C9300-24P	24 port PoE+	Modular Uplinks	715W AC
C9300-48P2	48 port PoE+	Modular Uplinks	715W AC

4. керований чи некерований[23]. Існує керований та некерований комутатор. Керований комутатор надає більше можливостей до налаштування портів, сегментування, агрегації трафіку, пріоритетності трафіку та аналізу. Також ці комутатори можуть мати графічний або вебінтерфейс для зручності та простоти налаштування. Некерований комутатор має фіксовану конфігурацію, яку неможна змінити. Такі комутатори є дешевшими, але в тай час вони є специфічними. Оскільки вони вже є налаштованими й там немає змоги змінювати конфігурацію,

це може спричинити проблеми при налаштуванні та виправлені неполадок в мережі. Їх рекомендується використовувати лише в специфічних завданнях, під які вони можуть бути налаштовані, або невеликих мережах, де необхідно просто під'єднати пристрої;

5. видом монтажу. Існує декілька видів кріплення комутаторів в залежності від потреб: Настінний монтаж використовується для комутаторів коли є потреба прикріпити його на стіну. Цей метод є популярним в домашніх середовищах чи невеликих офісах. Монтаж у стійку використовується у великих компаніях при наявності стійки чи шафи й в центрах обробки даних (ЦОД). Настільний монтаж використовують для невеликих комутаторів, що встановлюються на робочих місцях. Тож в залежності від мережі буде використовуватися різний вид монтажу;

6. живлення. Враховуючи можливість використання технології PoE потрібно розраховувати необхідну потужність блоку живлення комутатора врахувавши потребу в живленні пристроїв, що використовуватимуть PoE. Також можливий варіант коли один комутатор має потужний блок живлення, а сусідній комутатор живиться від нього.

Маршрутизатор (router) – це мережевий пристрій, що використовується для поєднання двох та більше мереж й приймає рішення про маршрутизацію на підставі встановлених правил маршрутизації та інформації про топологію мережі[26]. Вибір маршрутизатора для корпоративної комп'ютерної мережі залежить від наступних критеріїв:

1. масштаби мережі. Розуміння масштабу корпоративної мережі дозволяє розрахувати під, яку кількість користувачів та архітектуру потрібно здійснювати вибір маршрутизатора. Оскільки важливо розуміти, що саме користувачі будуть потребувати й це одна мережа чи підключення різних філіалів;

2. пропускна здатність. Цей критерій важливий при виборі, оскільки він визначає тип та ціну маршрутизатора. При розрахунку необхідної пропускної здатності потрібно розуміти тип трафіку, що буде курсувати по мережі. Оскільки компанія може мати встановленні внутрішні сервери то й великий відсоток трафіку

може буде локальним. Тобто він не буде виходити за межі корпоративної комп’ютерної мережі. У випадку ігрової компанії це можуть бути конфігурації гри, програми, моделі, графіка тощо, що генеруються працівниками. У випадку активного використання хмарних технологій, трансляцій, серфінгу в інтернеті працівниками то більшість трафіку можу бути зовнішнім. Оскільки працівники генеруватимуть запити до сайтів, відділених робочих місць, ресурсів, сервісів. Тож для обрання достатньої пропускної здатності потрібно розуміти тип трафіку в внутрішній мережі та після цього приймати рішення про купівлю відповідного за характеристикою та портами маршрутизатора;

3. безпека. Безпека на маршрутизаторі забезпечується використанням вбудованого брандмауера, наявністю VPN, контролю доступу тощо. Це забезпечить фільтрацію трафіку ззовні та всередині, шифрування даних, захист від різноманітних мережевих атак та несанкціонованого доступу;

4. розширений функціонал та ліцензії. Цей критерій звертає увагу на необхідність купівлі ліцензії на це обладнання у випадку використання розширеного функціоналу, наприклад: використання вбудованого VPN, розблокування обмеження пропускної здатності, агрегація портів, використання програмного забезпечення тощо. Кожен виробник може встановлювати такі обмеження на розширенні послуги керуючись його політикою в компанії. Тому при остаточному виборі маршрутизатора варто переглянути обмеження та ліцензії.

РОЗДІЛ 3. ВПРОВАДЖЕННЯ ТА ПІДТРИМКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Приклад компанії, яка потребує надійної корпоративної комп’ютерної мережі

Змоделюємо ситуацію, в якій вигадана мною українська ігрова компанія “Віртуальні мандрівники” – це професійна та амбітна ігрова компанія, яка прагне створювати високоякісні, високобюджетні ігри, що будуть захоплювати гравців по всьому світу своїм сюжетом, графікою, механіками, увагою до деталей й дарувати гравцям приємні враження при проходженні гри. Майбутній проєкт компанії має назву: "Епічні легенди: Володарі перснів та Хоббіта" – це нова відеогра, яка поєднує в собі два культові світи: "Володар перснів" та "Хоббіт". Гравці матимуть змогу пройти цю гру в одиночному варіанті та в кооперативі з друзями. Гра надає два варіанти сюжету, а саме: Проходження канонічного сюжету описаного в книгах або альтернативний, що буде залежати від вибору варіанту дій гравців під час проходження. Тож дана компанія переїжджає в збудований для них великий кількаповерховий офіс й потребує мережі, що забезпечить постійний доступ до інтернету. За штатом передбачено 1100 працівників поділених на відділи: Програмісти, Game дизайнери, Тестувальники, Дизайнери, Cybersecurity, Бугалтерія, Відділ кадрів, Відділ продажу та реклами, Аналітики, Системні адміністратори, Керівництво, Охорона праці, HR, Sound дизайнери. Також передбачений Wi-Fi для працівників та відвідувачів. Компанія передбачає виділення конференц залу. Планується розгортання невеликої серверної інфраструктури для власних потреб та використання хмарних сервісів для кращого функціонування компанії. На кожному поверсі є виділена кімната для правильного встановлення й забезпечення контролю доступу до мережевого обладнання. Враховуючи використання хмарних сервісів ігровою компанією для роботи вона

потребує надійного та стабільного з’єднання з мережею Інтернет. Це Тож враховуючи наданий стислий опис ігрової компанії використання FHRP для постійного доступу в мережу Інтернет є необхідним. Варіанти використання FHRP та етапи проєктування й впровадження мережі будуть описані в наступних розділах.

3.2 Варіанти використання FHRP в корпоративної комп'ютерній мережі

З опису компанії в попередньому пункті випливає необхідність побудови великої корпоративної комп’ютерної мережі, що повинна мати постійний доступ до мережі Інтернет. Це можна забезпечити шляхом використання двох чи більше маршрутизаторів на випадок виходу з ладу одного з них. Таку можливість нам надає технологія FHRP[27]. Вона забезпечує створення одного логічного маршрутизатор з двох або більше фізичних шляхом використання одної віртуальної IP-адреси (рис. 3.1).

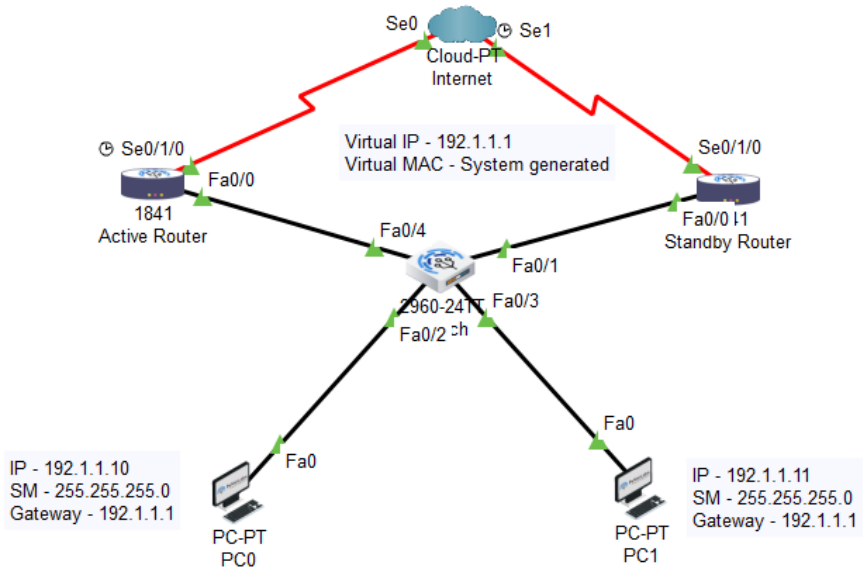


Рисунок 3.1 – Використання двох роутерів, як одного логічного

В такому випадку один маршрутизатор обирається головним а інші

резервними на випадок виходу основного з ладу, проте є варіант коли всі маршрутизатори будуть працювати разом в режимі балансування навантаження. Розберемо варіанти FHRP:

1. HSRP – це Cisco-пропрієтарний FHRP, що призначений для забезпечення відмовостійкості IPv4-пристрою першого переходу тобто маршрутизатора[28]. Він використовується в групі маршрутизаторів для вибору активного та резервного пристрою. Маршрутизатор з найвищим пріоритетом стає головним та виконує усю роботу. Інші маршрутизатори знаходяться в режимі очікування поки основний не вийде з ладу. При виході основного з ладу резервний маршрутизатор, що має більший пріоритет включається у роботу(рис. 3.5). Цей протокол існує в варіанті для IPv4 та для IPv6. Існує декілька станів HSRP:

1.1. Initial (початковий) – цей стан виникає при зміні конфігурації, або у випадку, коли інтерфейс вперше стає доступним;

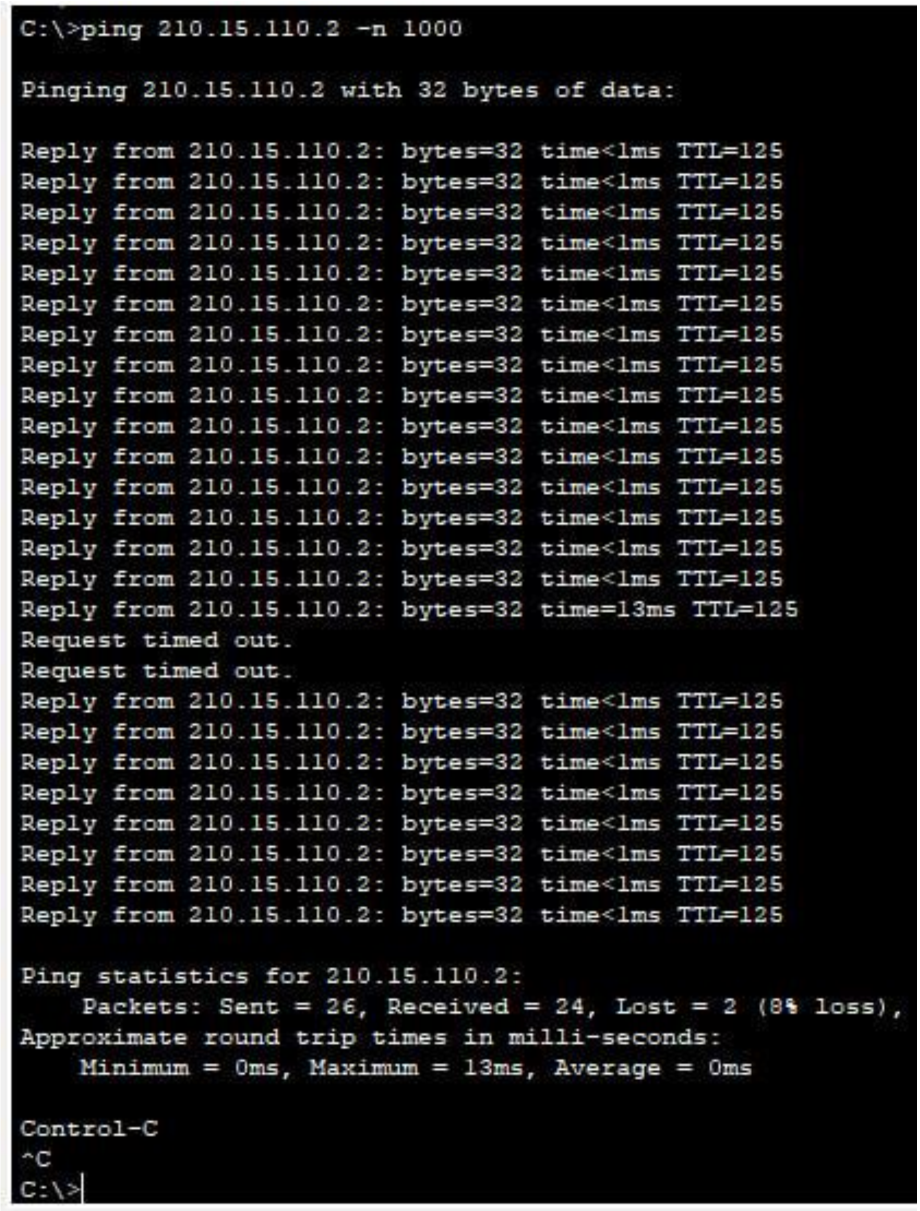
1.2. Learn (навчальний) – це стан під час якого маршрутизатор не визначив віртуальну IP-адресу й не отримав привітального повідомлення від активного маршрутизатора. В такому випадку він очікує на привітальне повідомлення;

1.3. Listen (прослуховування) – це стан в якому маршрутизатор знає віртуальну IP-адресу проте досі не є активним чи резервним. Він прослуховує привітальні повідомлення від інших маршрутизаторів;

1.4. Speak (розмовний) – це стан під час якого маршрутизатор періодично відправляє привітальні повідомлення і бере активну участь у виборі активного і/або резервного маршрутизатора;

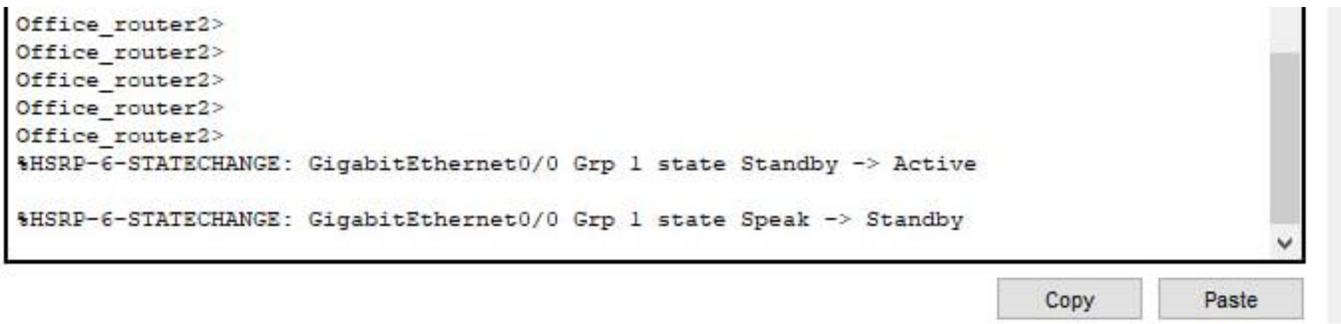
1.5. Standby (резервний) – це стан коли маршрутизатор є кандидатом на роль наступного активного маршрутизатора і періодично відправляє привітальні повідомлення.

Приклад роботи протоколу HSRP при відмові основного маршрутизатора(рис. 3.2-3.4).



```
C:\>ping 210.15.110.2 -n 1000

Pinging 210.15.110.2 with 32 bytes of data:

Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time=13ms TTL=125
Request timed out.
Request timed out.
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125
Reply from 210.15.110.2: bytes=32 time<1ms TTL=125

Ping statistics for 210.15.110.2:
    Packets: Sent = 26, Received = 24, Lost = 2 (8% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 13ms, Average = 0ms

Control-C
^C
C:\>
```

Рисунок 3.2 – Здійснюється пінг сервера, що знаходиться в мережі Інтернет



```
Office_router2>
Office_router2>
Office_router2>
Office_router2>
Office_router2>
%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 1 state Standby -> Active

%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 1 state Speak -> Standby
```


Рисунок 3.3 – Включення в роботу резервного маршрутизатора при відмові основного та після відновлення основного маршрутизатора перехід до резервного

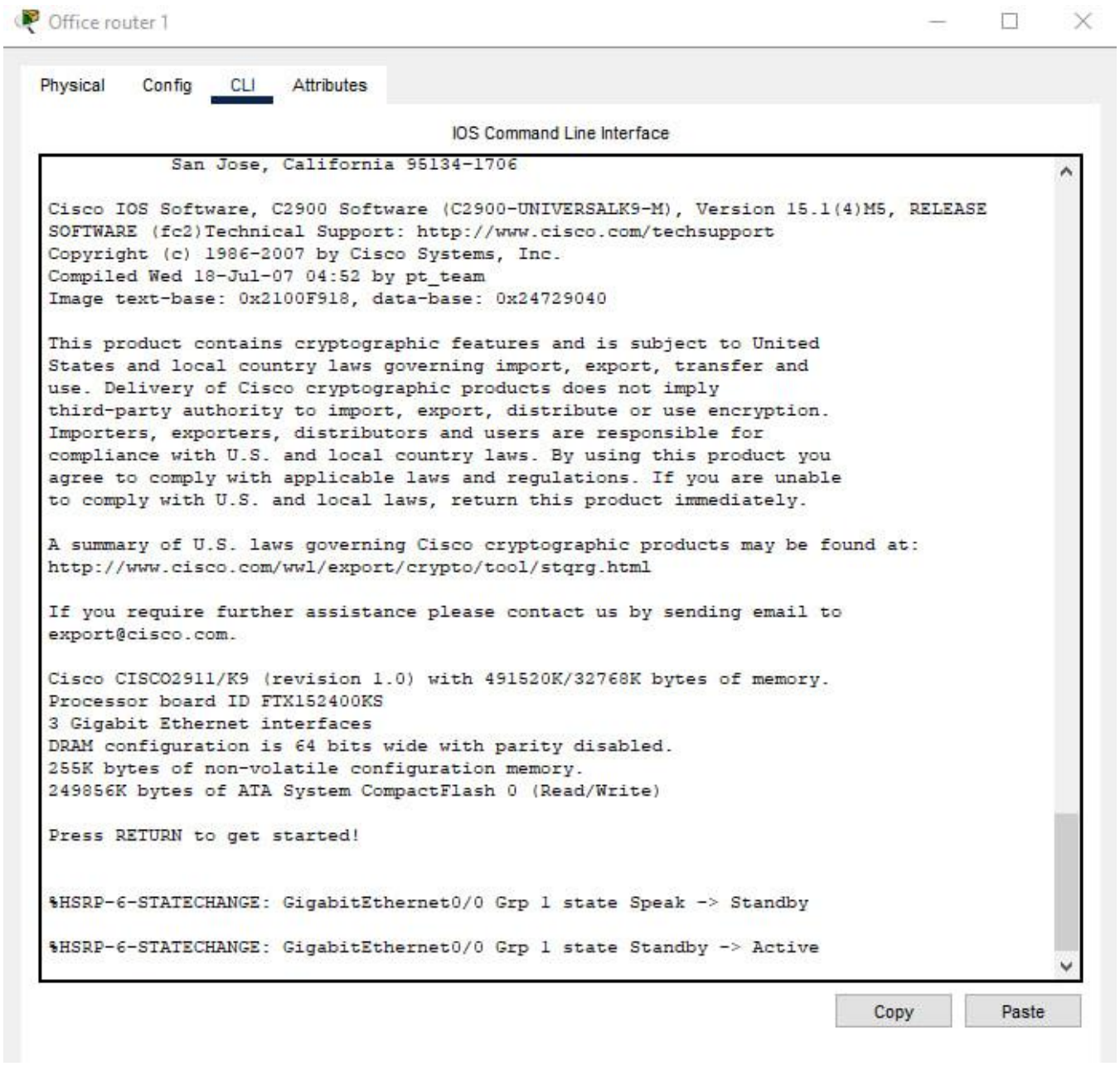


Рисунок 3.4 – Включення в роботу основного маршрутизатора після несправності

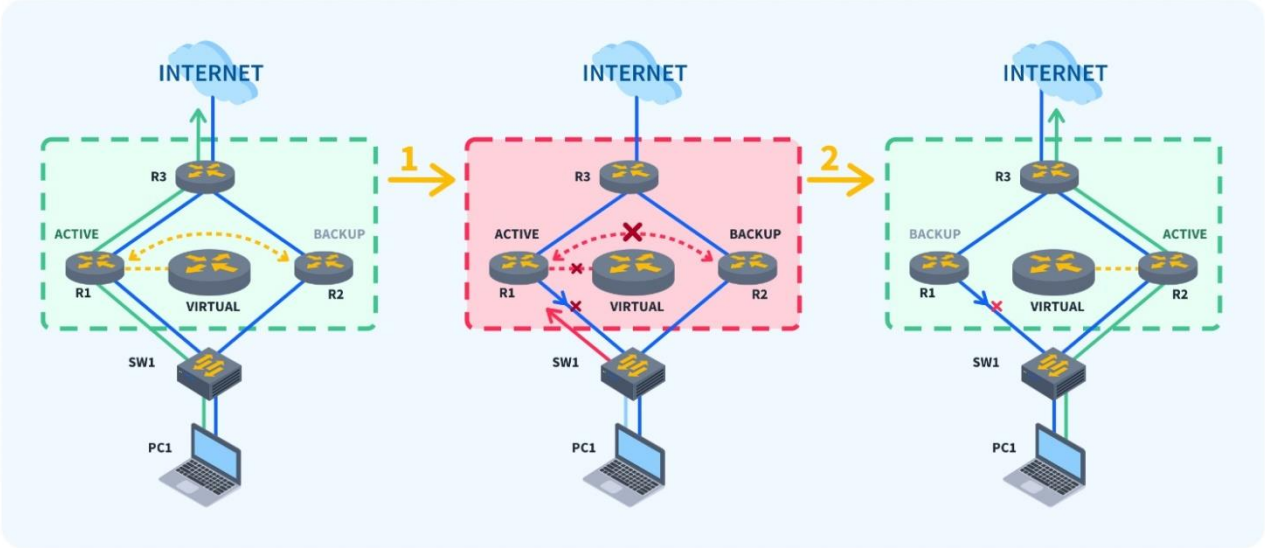


Рисунок 3.5 – Принцип роботи HSRP

2. VRRP – це протокол з відкритим стандартом, що динамічно призначає маршрутизатори в роль активного чи резервного. Оскільки він є відкритим стандартом то його підтримують інші вендори. Це зручно для тих хто не використовує обладнання Cisco або є мультивендорним. Він підтримує стандарти IPv4 та IPv6. VRRPv3 здатен працювати в середовищі де присутня мультивендорність і є більш масштабованим.;

3. GLBP – це Cisco-пропрієтарний FHRP, який захищає трафік даних від відмов маршрутизатора забезпечуючи балансування навантаження одночасно дозволяючи працювати декільком маршрутизаторам. Існує версія GLBP для IPv6, яка працює з адресами IPv6.;

Тож в враховуючи різні потреби компаній та різних виробників маршрутизаторів обирається необхідний варіант FHRP. Якщо є потреба мати запасний маршрутизатор на випадок виходу основного з ладу варто використовувати HSRP або VRRP в залежності від виробника маршрутизатора. Якщо є потреба у розвантаженні основного маршрутизатора або балансуванні трафіку при наявності запасного маршрутизатора варто використовувати GLBP, оскільки він буде забезпечує балансування навантаження й це покращить роботу мережі.

3.3 Етапи розробки та впровадження проєкту

Впровадження проєкту є комплексним та складним процесом, що вимагає залучення великої кількості спеціалістів та проходження певних етапів проєктування й розробки корпоративної комп'ютерної мережі. Розберемо ці етапи впровадження проєкту:

1. отримання завдання. Перш за все компанія, що розроблятиме корпоративну комп'ютерну мережу отримує від замовника завдання на розробку корпоративної комп'ютерної мережі. В цьому завданні зазначаються вимоги, та побажання до мережі зі сторони замовника. Тобто визначаються під яку сферу діяльності компанії будується мережа, які сервіси та програмне забезпечення будуть використовуватись, надлишковість та відмовостійкість мережі, передбачений штат працівників та пристроїв, що будуть використовуватися працівниками. Разом з цим надається план будівлі, схема прокладення електродротів й дизайнерський план, щоб мати уявлення про розташування робочих місць, кімнат тощо. Це важливо аби під час етапів розробки були правильно розраховані потреби в обладнанні та підключенні, зроблені схеми та налаштована мережа.

2. проєктування мережі. Отримавши відомості зазначенні в попередньому пункті починається робота над проєктуванням мережі. На основі плану будівлі вводяться записи про кількість пристроїв та необхідних підключень на кожну кімнату. Створюється таблиця потреб в мережевому обладнанні розбита по поверхам чи частинам будівлі. Туди включають потребу в комутаторах, маршрутизаторах, патч-панелях точках доступу й іншого необхідного мережевого обладжнання (дод.А). Далі відбувається розробка фізичної та логічної топології мережі. На яких зазначають способи з'єднання, структуру, типи каналів зв'язку, сегменти мережі, пристрої тощо. (дод.Б,В) Для прокладення кабелів залучаються спеціалісти, що проєктують схему прокладення інтернет кабелів враховуючи схему прокладення електродротів, особливості кожного типу кабелю та вразливостей, що

спотворюють чи глушать сигнал. Після цього ця схема передається на виконання монтажному відділу. Проводиться розробка IP-плану мережі де відбувається сегментація на VLAN різних відділів в компанії та визначають пули адрес.(дод Г) В кінці етапу проєктування та розробки мережі підбирається мережеве обладнання відповідно до визначених вимог та потреб й подається у вигляді таблиці з найменуванням пристроїв, кількістю, вендором, моделлю та ліцензіями чи програмним забезпеченням (Додаток Д(приклади обладнаня)). При розроблені моделі мережі використовуються програми, що надають можливість створення працюючої моделі в емуляторі та радіопланування при побудові бездротових мереж. Такими програмами є Ekahau AI Pro (рис. 3.6)[29], Cisco packet tracer (рис. 3.7), GNS3 тощо.

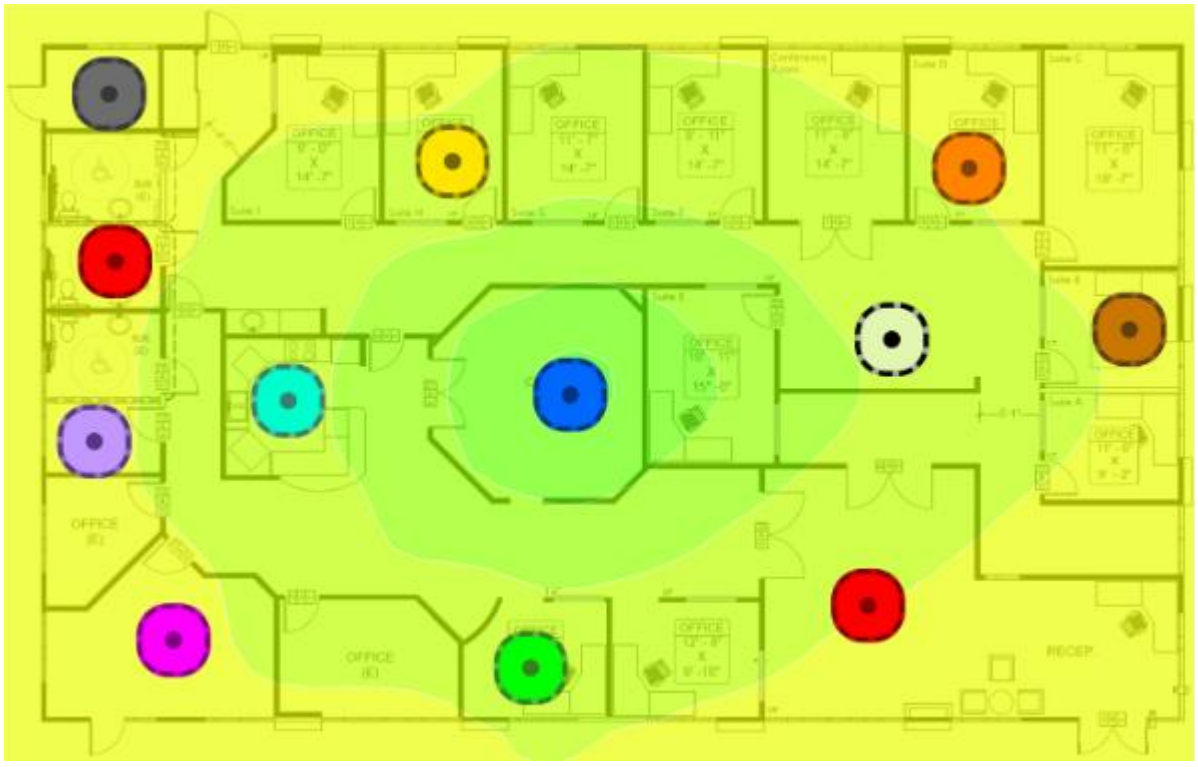


Рисунок 3.6 – Радіопланування в програмі Ekahau AI Pro

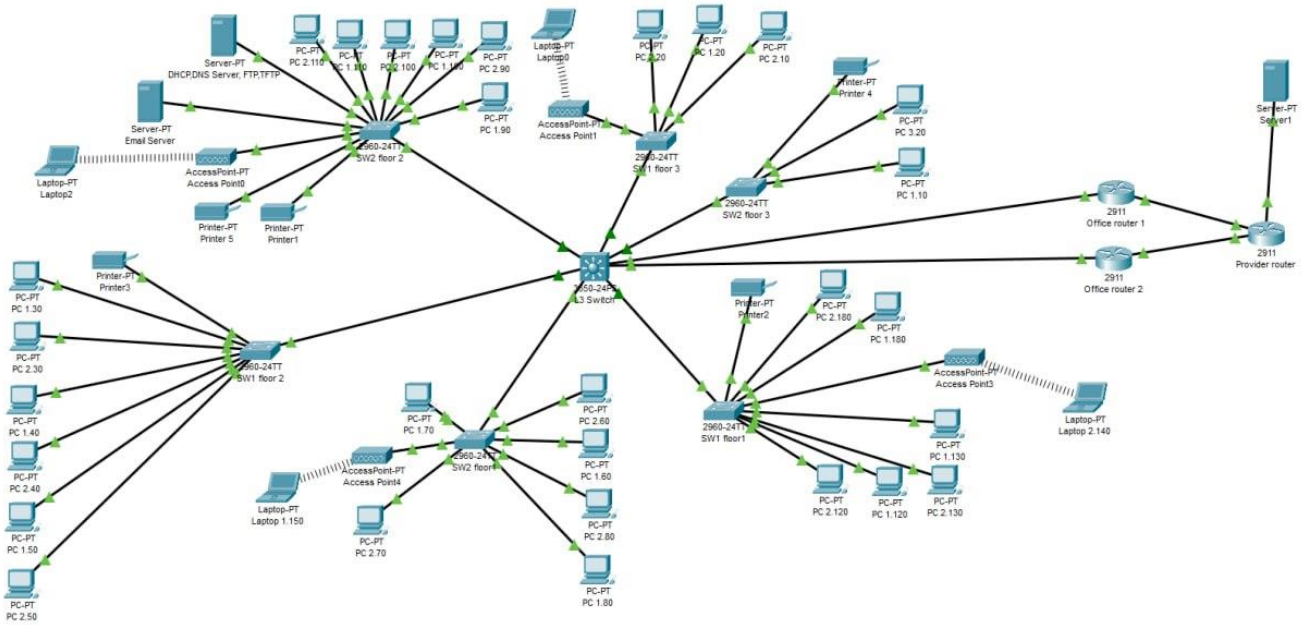


Рисунок 3.7 – Приклад спроєктованої мережі в програмі Cisco Packet Tracer для ігрової компанії

3. закупівля обладнання. Закупівля обладнання відбувається коли готові схеми мережі, дротів та складено перелік необхідного обладнання виходячи з потреб й виділення коштів. Під час його вибору враховується необхідна пропускна здатність, типи підключень, типи кабелів, технології, що використовуються, кількість та ліцензії

4. кофігурація обладнання та підключення. Конфігурація обладнання відбувається після виконання попередніх етапів й проводиться безпосередньо на об’єкті або конфігурується на фірмі й потім тільки підключається на об’єкті. Під час конфігурації відбувається сегментація мережі, налаштування сервісів, політик доступу, впроваджується захист на кожному девайсі й налаштовується брандмауер. Після конфігурації обладнання встановлюється в визначених місцях й документується його розташування й підключення пристроїв до нього. (дод Е,Ж)

5. тестування мережі. Тестування мережі відбувається на завершальному етапі й проводиться тими, хто розробляв мережу або з залученням спеціальних фахівців. При тестуванні перевіряється якість бездротового та дротового з’єднання за допомогою спеціальних пристроїв, безпека мережі, доступність та правильність налаштування, відмовостійкість тощо. Здійснюється перевірка рівня захисту

портів, роботи брандмауера, системи контролю доступу. По закінченню тестування надається висновок про проходження тестування й зауваження.

Під час будь-якого з цих етапів здійснюється комунікація із замовником та різноманітними фахівцями для усунення проблемних питань чи своєчасного внесення змін. Дотримання цих етапів допоможе зробити мережу більш якісною та зрозумілою в обслуговуванні. Оскільки наявність озвучених схем, таблиць та документів дозволяє якісніше та швидше виправляти неполадки й підтримувати мережу в робочому стані. Тому, що системному адміністратору не потрібно буде самому складати ці схеми й шукати потрібні пристрої та підключення навмання.

3.4 Безпека та моніторинг мережі

Безпека та моніторинг мережі це комплекс заходів спрямованих на забезпечення безпеки корпоративної комп’ютерної мережі та моніторингу її стану. Безпека забезпечується використанням різноманітних програм, пристроїв сервісів, відеонагляду та систем контролю доступу. Питаннями безпеки займається системний адміністратор або виділений відділ безпеки. Приклади інструментів безпеки:

1. Cisco ASA – це лінійка мережевих пристроїв безпеки Cisco, що виконують функції брандмауера та системи запобігання вторгненням(рис. 3.8);

Рисунок 3.8 – Міжмережевий екран Cisco ASA5506-K8

Брандмауер запобігає проникненню в мережу хакерів, шкідливого програмного забезпечення, фільтрацію трафіку, виявлення та блокування загроз, захист від DDoS-атак тощо.

2. для захисту кінцевих користувачів можуть використовуватися різні антивірусні програми. Одною з популярних та хороших програм є Avast Antivirus. Це антивірусна програма для ПК на базі операційних систем Microsoft Windows, macOS та Linux. Вона здатна перевіряти ПК на наявність вірусів, шпигунських програм, троянів, шкідливих скриптів тощо. Також має вбудований бранмауер та різноманітні екрани безпеки, що відстежують дії з файлами, поштою, роботу скриптів тощо. Вона пропонує захист для домашніх користувачів та бізнесу;

3. система контролю доступу існує, як фізична так і за допомогою програм чи служб. Система контролю доступу обмежує фізичний доступ працівників до приміщень за для уникнення несанкціонованого доступу в інші відділи або в серверні кімнати. Також можуть використовуватися Active Directory (AD). Active Directory (AD) – це служба каталогу доменів, розробленою компанією Microsoft для управління користувачами, комп'ютерами та різноманітними ресурсами в мережі. Вона забезпечує централізоване управління доступом до ресурсів, аутентифікацію користувачів, установку політик безпеки тощо.

Моніторинг мережі забезпечується шляхом використання спеціального програмного забезпечення або спеціальних платформ. Такими інструментами є Observium, PRTG, Wireshark, Zabbix тощо. Вони надають змогу відстежувати трафік, стан обладнання, помилки, інформацію про порти маючи лише ноутбук при собі. Це дозволяє в реальному часі аналізувати й контролювати мережу аби попередити чи оперативно усунути неполадки (дод К,Л). В залежності від бюджету та потреб можна використовувати різні інструменти.

ВИСНОВКИ

Будь-яка мережа використовує маршрутизатори для доступу в Інтернет. У випадку корпоративних комп'ютерних мереж використовуються потужні маршрутизатори. Проте, використання одного роутера створює єдину точку відмови і це може спровокувати збої в роботі мережі. Оскільки один роутер може стати вузьким місцем (bottleneck) в мережі через його недостатню пропускну здатність або вихід з ладу, то є необхідність в резервному маршрутизаторі, що дає можливість працювати в режимі балансування одночасно з основним. Таку можливість надає технологія FHRP.

Аналізуючи вище сказане та дослідивши корпоративну комп'ютерну мережу, вимоги до її розгортання, налаштування та подальшої роботи, віртуалізацію та використання в ній протоколів технології FHRP можна дійти висновку, що корпоративні комп'ютерні мережі є дуже поширеними й в залежності від виду діяльності компанії мають різні вимоги та особливості.

Використання протоколів технології FHRP роблять корпоративну комп'ютерну мережу відмовостійкою та надійною. Її протоколи забезпечують стабільний доступ до мережі Інтернет, що є важливим для будь-якого бізнесу.

Досліджено поняття архітектури мережі та її складових. Наведено два основних типи мереж, на які орієнтуються при побудові корпоративної комп'ютерної мережі. Визначено їх переваги та недоліки. Наведено протоколи та можливі сервіси, які можуть бути використані в корпоративній мережі. Виділено рекомендації правильного розташування фізичного обладнання та критерії вибору обладнання для корпоративної комп'ютерної мережі.

Приведено приклад компанії, що може потребувати надійної корпоративної комп'ютерної мережі з використанням різних протоколів резервування шлюзу за замовчуванням. Описано ці протоколи та продемонстровано приклад роботи одного з них. Визначено етапи впровадження проєкту з послідовністю розробки корпоративної комп'ютерної мережі, документуванням та засобами, що

використовуються в роботі. Розглянуто питання безпеки й моніторингу для постійного контролю та підтримки корпоративної комп’ютерної мережі.

Інвестиції в розробку аналогічних технологій та протоколів, подальший їх розвиток є актуальним й необхідним, оскільки вони забезпечують надійність та доступність мережі у випадку непередбачуваних ситуацій. Їх розвиток разом з розвитком корпоративної комп’ютерної мережі дозволить покращити існуючі мережеві інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. CCNA: Switching, Routing, and Wireless Essentials | Networking Academy. Networking Academy. URL: https://www.netacad.com/courses/networking/ccna-switching-routing-wireless-essentials (дата звернення: 06.05.2024).
2. What is Virtualization? - Cloud Computing Virtualization Explained - AWS. Amazon Web Services, Inc. URL: https://aws.amazon.com/what-is/virtualization/?nc1=h_ls (дата звернення: 16.04.2024).
3. What Are Computer Networks & How Do They Work for Business? - We Are Your IT. IT Help, Support, Services & Solutions in York | We Are Your IT. URL: https://www.weareyourit.co.uk/learning-hub/introduction-to-computer-networking-network-services-for-business (дата звернення: 16.04.2024).
4. . Дата-центр United DC. Дата центр у Києві | Надійний ЦОД рівня TIER-III в Україні. URL: https://uniteddc.net.ua/news/i/scho-take-hmarni-tehnologiyi/ (дата звернення: 16.04.2024).
5. IaaS vs. PaaS vs. SaaS. Red Hat - We make open source technologies for the enterprise. URL: https://www.redhat.com/en/topics/cloud-computing/iaas-vs-paas-vs-saas (дата звернення: 16.04.2024).
6. Fusion Connect. What is Network Architecture? And, How Does It Work?. Fusion Connect. URL: https://www.fusionconnect.com/blog/what-is-network-architecture (дата звернення: 16.04.2024).
7. What is network architecture? Everything you need to know. NordVPN. URL: https://nordvpn.com/uk/blog/network-architecture/ (дата звернення: 17.04.2024).
8. Logical vs. Physical Network Diagrams - Graphical Networks - DCIM, Network Documentation, OSP Software. Graphical Networks - DCIM, Network Documentation, OSP Software. URL: https://graphicalnetworks.com/blog-logical-vs-physical-network-diagrams/ (дата звернення: 17.04.2024)

9. L2 and L3 Topology - Oracle Ethernet Switches. Moved. URL: https://docs.oracle.com/cd/E19285-01/html/E41457/z400378d1870238.html (дата звернення: 17.04.2024).

10. IPv4 vs IPv6: What's The Difference Between the Two Protocols?. Kinsta®. URL: https://kinsta.com/blog/ipv4-vs-ipv6/ (дата звернення: 17.04.2024).

11. What is Transmission Control Protocol (TCP)? - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/ (дата звернення: 17.04.2024).

12. What Is User Datagram Protocol (UDP)? | Fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/user-datagram-protocol-udp (дата звернення: 17.04.2024).

13. Understanding First Hop Redundancy Protocols (FHRP) – Expert Network Consultant. Expert Network Consultant – Networking | Cloud | DevOps | IaC. URL: https://www.expertnetworkconsultant.com/installing-and-configuring-network-devices/understanding-first-hop-redundancy-protocols-fhrp/ (дата звернення: 18.04.2024).

14. Why is HTTP not secure? | HTTP vs. HTTPS: URL: https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/ (дата звернення: 16.04.2024).

15. Magnusson A. What is AAA Security? Authentication, Authorization, and Accounting. StrongDM: Your Partner in Zero Trust Privileged Access. URL: https://www.strongdm.com/blog/aaa-security (дата звернення: 18.04.2024).

16. What Is the RADIUS Protocol? | Fortinet. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/radius-protocol (дата звернення: 18.04.2024).

17. TACACS+ Protocol - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/tacacs-protocol/ (дата звернення: 18.04.2024).

18. Messink B. Ethernet vs. Wi-Fi: Is It Really Better to Go Wireless?. HighSpeedInternet.com. URL: https://www.highspeedinternet.com/resources/ethernet-vs-wifi (дата звернення: 19.04.2024).

19. PoE vs. PoE+: What's the Difference?. Twinstate Blog - Cloud Communications, Cybersecurity, and Business Productivity Content. URL: https://blog.twinstate.com/poe-vs-poe-plus (дата звернення: 19.04.2024).

20. Що таке патч-панелі і навіщо вони потрібні: типи і види патч-панелей. OmniLink. URL: https://omnilink.ua/dlya-choho-potribni-patch-paneli/ (дата звернення: 19.04.2024).

21. Ethernet Cable Categories Explained in Tabular Form (Cat1, Cat2, Cat3, Cat4, Cat5, Cat5e, Cat6, Cat7 and Cat8) - LEARNABHI.COM. LEARNABHI.COM -. URL: https://www.learnabhi.com/ethernet-cable-categories-cat1-cat2-cat3-cat4-cat5-cat5e-cat6-cat7-cat8/ (дата звернення: 19.04.2024).

22. How to choose the best switch for your network!. TRENDnet | Networks People Trust. URL: https://www.trendnet.com/products/features/default?featureid=56 (дата звернення: 19.04.2024).

23. Difference between Managed Vs Unmanaged switch and which one to buy?. https://www.hdv-fiber.com/. URL: https://www.hdv-fiber.com/uk/news/difference-between-managed-vs-unmanaged-switch-and-which-one-to-buy/ (дата звернення: 19.04.2024).

24. Cisco Catalyst 9300 Series Switches Data Sheet. Cisco. URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html (дата звернення: 19.04.2024).

25. What Are SFP Modules? | Types & Advantages Explained. Versitron. URL: https://www.versitron.com/blogs/post/everything-you-should-know-about-the-sfp-module (дата звернення: 19.04.2024).

26. How to Choose the Right Router for Your Business. URL: https://worldwidesupply.net/blog/choose-right-router-business/ (дата звернення: 20.04.2024).

27. Understanding First Hop Redundancy Protocols (FHRP) – Expert Network Consultant. Expert Network Consultant – Networking | Cloud | DevOps | IaC. URL: https://www.expertnetworkconsultant.com/installing-and-configuring-network-devices/understanding-first-hop-redundancy-protocols-fhrp/ (дата звернення: 20.04.2024).

28. HSRP vs VRRP vs GLBP Protocols - GeeksforGeeks. GeeksforGeeks. URL: https://www.geeksforgeeks.org/hsrp-vs-vrrp-vs-glbp-protocols/ (дата звернення: 20.04.2024).

29. Ekahau AI Pro | Wi-Fi Design, Survey & WLAN Troubleshooting Software. Ekahau. URL: https://www.ekahau.com/products/ekahau-connect/ai-pro/ (дата звернення: 20.04.2024).

30. The Team at CXtec. What Is CISCO Adaptive Security Appliance (ASA)? - CXtec. Best IT Infrastructure Solutions | IT Infrastructure Hardware - CXtec. URL: https://www.cxtec.com/blog/what-is-cisco-asa-security-appliance/ (дата звернення: 20.04.2024).

Додаток А

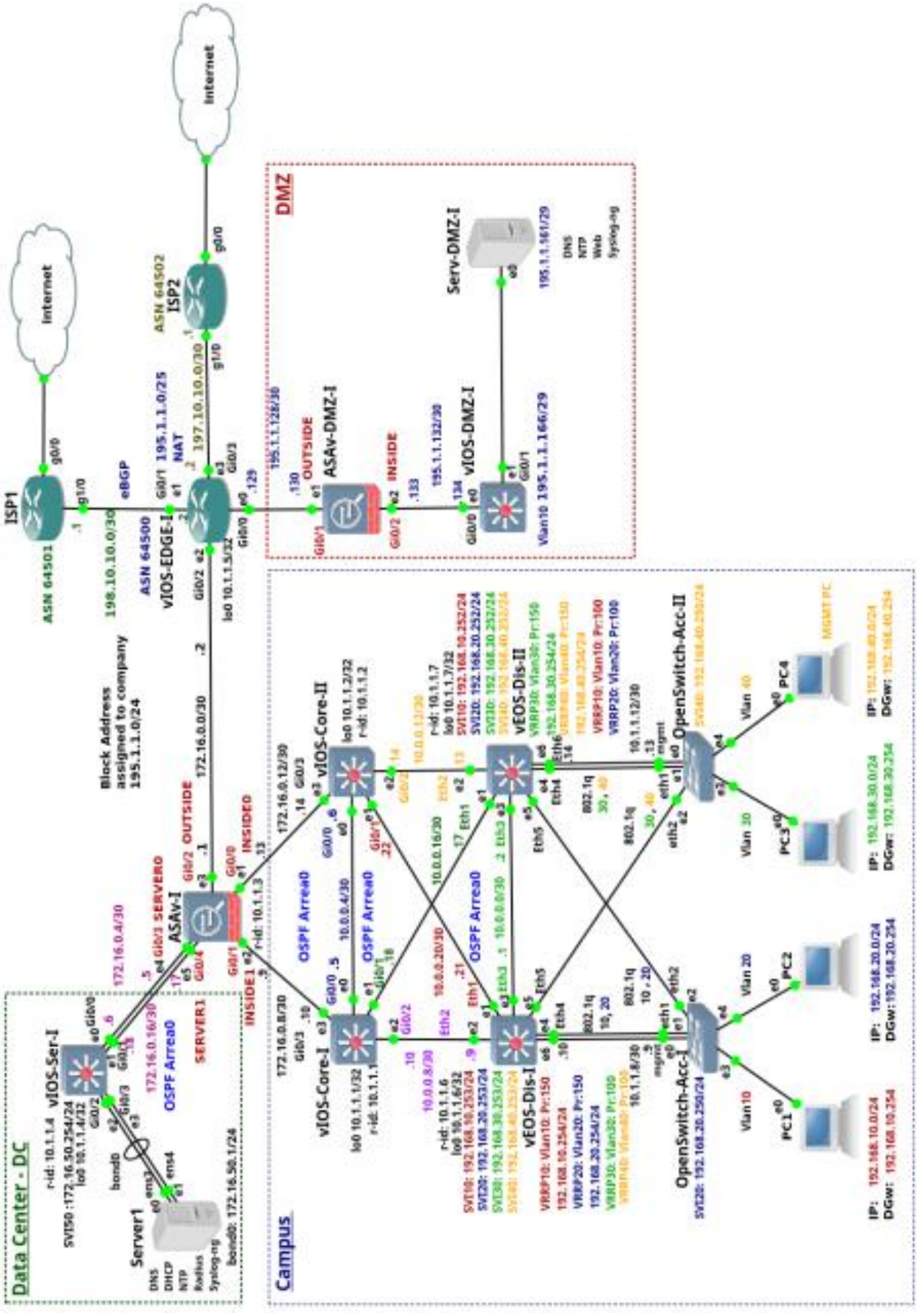
Приклад потреб в обладнанні

Потреба в обладнанні на поверх

Поверх	Switch L2 (24-ports)	Switch L3 (24-ports)	Patch-panel (24-ports)	Switch L2 (48-ports)	Switch L3 (48-ports)	Patch-panel (48-ports)	Router	AP(access point)
1	13,41666667	2	13,41666667	6,708333333	2	6,708333333	2	21,46666667
2	15,83333333		15,83333333	7,916666667		7,916666667		25,33333333
3	13,29166667		13,29166667	6,645833333		6,645833333		21,26666667
4	13,29166667		13,29166667	6,645833333		6,645833333		21,26666667
Підсумок	55,833333		55,8333333	27,9166667		27,91666667		89,33333333

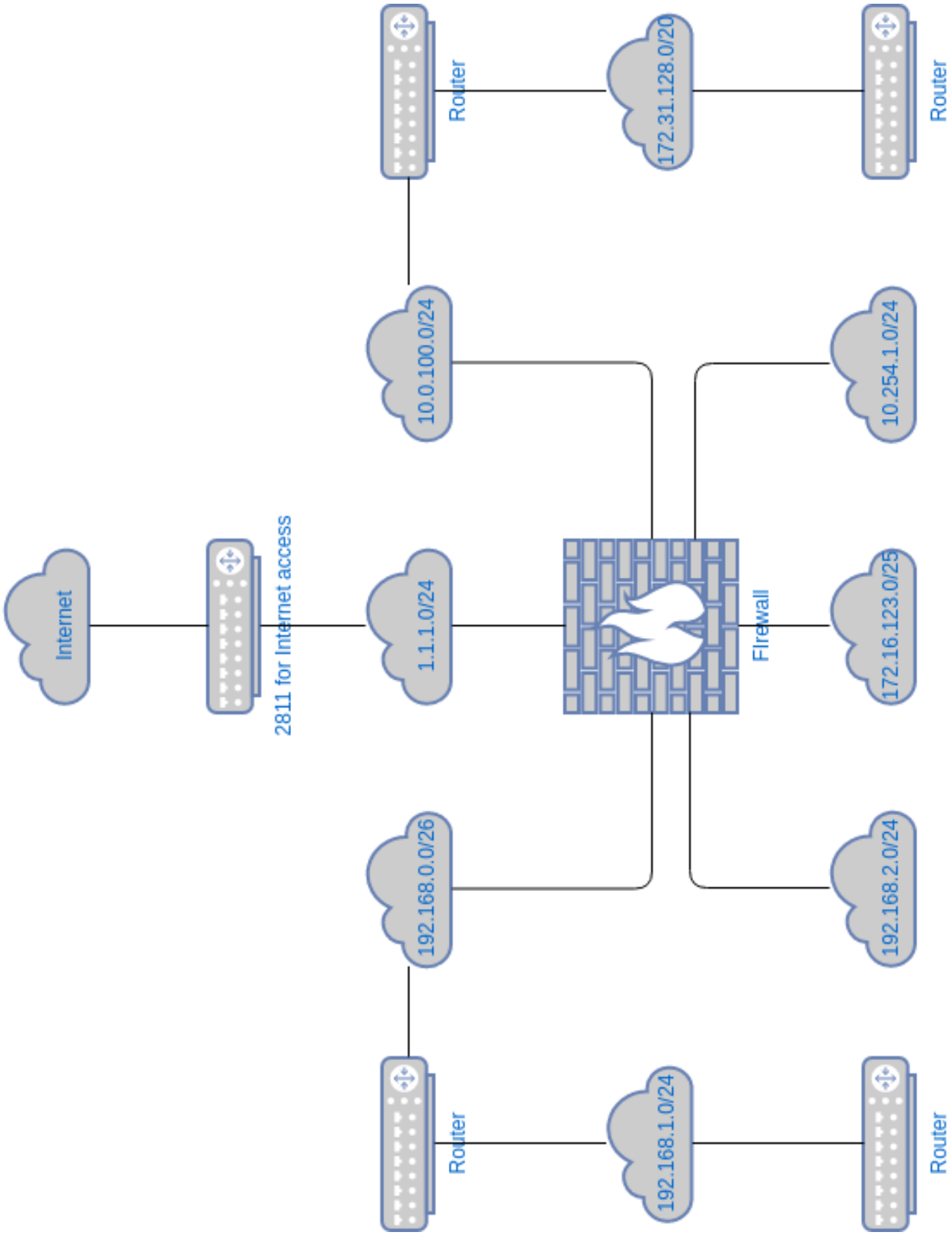
Додаток Б

Приклад фізичної топології мережі



Додаток В

Приклад логічної топології мережі



Додаток Г

IP-план мережі

Відділ	VLAN	Кількість хостів	Надано адрес	IP-мережі	Маска	Префікс мережі	Шлюз	IP-адреса початкова	IP-адреса кінцева	Діапазон наданих IP- address
Програмісти	10	500	512	172.16.10.0	255.255.254.0	/23	172.16.10.1	172.16.10.1	172.16.10.254	172.16.10.2 - 172.16.10.254
Гейм-дизайнери	20	160	254	172.16.20.0	255.255.255.0	/24	172.16.20.1	172.16.20.1	172.16.20.254	172.16.20.2 - 172.16.20.254
Тестувальники	30	100	126	172.16.30.0	255.255.255.128	/25	172.16.30.1	172.16.30.1	172.16.30.126	172.16.30.2 - 172.16.30.126
Графічні дизайнери	40	100	126	172.16.40.0	255.255.255.128	/25	172.16.40.1	172.16.40.1	172.16.40.126	172.16.40.2 - 172.16.40.126
Cybersecurity	50	24	30	172.16.50.0	255.255.255.224	/27	172.16.50.1	172.16.50.1	172.16.50.254	172.16.50.2 - 172.16.50.30
Бухгалтерія	60	12	14	172.16.60.0	255.255.255.240	/28	172.16.60.1	172.16.60.1	172.16.60.14	172.16.60.2 - 172.16.60.14
Відділ кадрів	70	20	30	172.16.70.0	255.255.255.224	/27	172.16.70.1	172.16.70.1	172.16.70.30	172.16.70.2 - 172.16.70.29
Відділ продажу та реклами	80	50	62	172.16.80.0	255.255.255.192	/26	172.16.80.1	172.16.80.1	172.16.80.62	172.16.80.2 - 172.16.80.62
Аналітики	90	20	30	172.16.90.0	255.255.255.224	/27	172.16.90.1	172.16.90.1	172.16.90.30	172.16.90.2 - 172.16.90.30
Системні адміністратори	100	20	30	172.16.100.0	255.255.255.224	/27	172.16.100.1	172.16.100.1	172.16.100.30	172.16.100.2 - 172.16.100.30
Керівництво	110	10	14	172.16.110.0	255.255.255.240	/28	172.16.110.1	172.16.110.1	172.16.110.14	172.16.110.2 - 172.16.110.14
Охорона праці	120	7	14	172.16.120.0	255.255.255.240	/28	172.16.120.1	172.16.120.1	172.16.120.14	172.16.120.2 - 172.16.120.14
HR	130	20	30	172.16.130.0	255.255.255.224	/27	172.16.130.1	172.16.130.1	172.16.130.30	172.16.130.2 - 172.16.130.30
Wi-Fi для працівників	140	1100	2046	172.16.140.0	255.255.252.0	/21	172.16.140.1	172.16.140.1	172.16.143.254	172.16.140.2 - 172.16.143.254
Wi-Fi для гостей	150	50	62	172.16.150.0	255.255.255.192	/26	172.16.150.1	172.16.150.1	172.16.150.62	172.16.150.2 - 172.16.150.62
Printers	160	23	32	172.16.160.0	255.255.255.224	/27	172.16.160.1	172.16.160.1	172.16.160.30	172.16.160.1-172.16.160.30
Servers	170	4	6	172.16.170.0	255.255.255.248	/29	172.16.170.1	172.16.170.1	172.16.170.6	172.16.170.1-172.16.170.6
Sound Engineers	180	20	30	172.16.180.0	255.255.255.224	/27	172.16.180.1	172.16.180.1	172.16.180.30	172.16.180.1-172.16.180.30

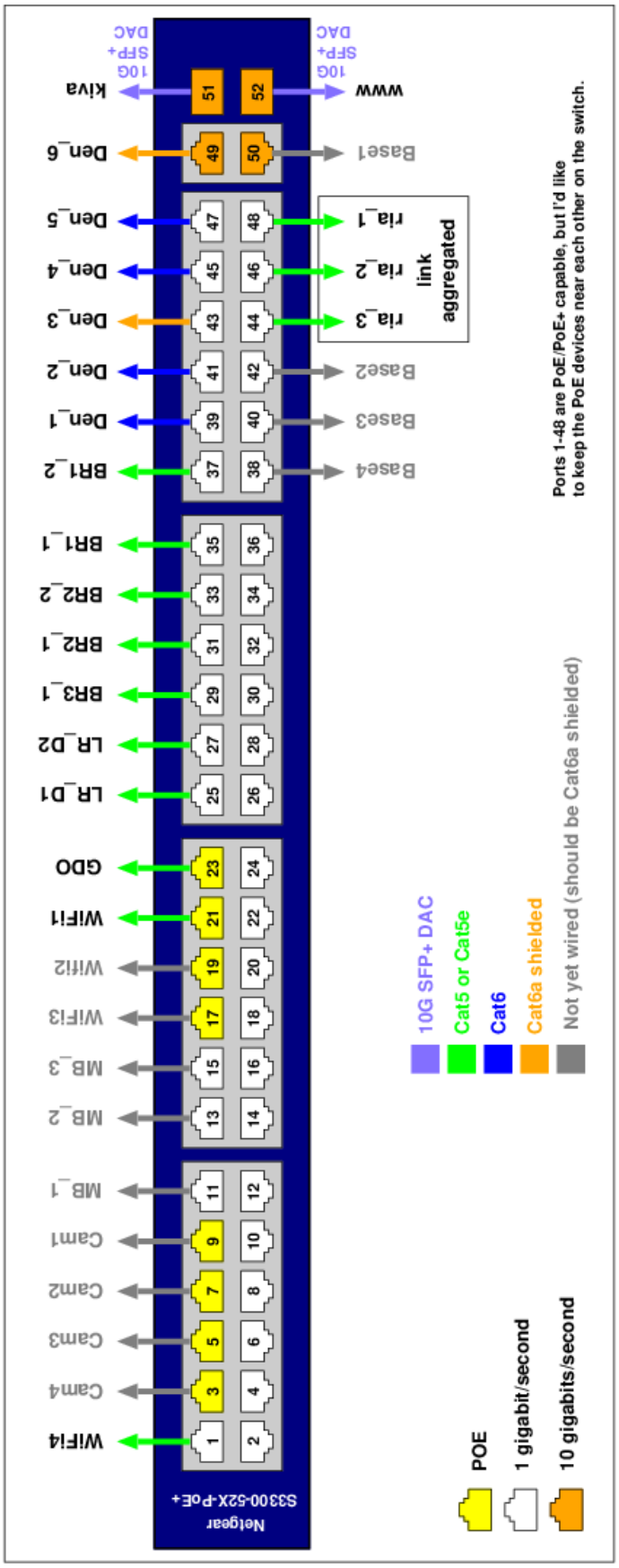
Додаток Д

Приклади обладнання

№	Пристрій	Виробник	Модель	Порти	Кількість	Примітка
1	Switch	Cisco	C9500-48Y4C	48-port 1/10/25G Gigabit Ethernet switch with SFP28	2	Layer 3 Switch
2	Switch	Cisco	C9300X-48HX	48 port Cisco UPOE+, 48x 10G Multigigabit (10G/5G/2.5G/1G/100M) with 90W UPOE+	28	Layer 2 Switch
3	Router	Cisco	C8500-12X4QC	12-port 1/10GE, 2-port 40/100GE, 2-port 40GE	2	Gateway
4	access point	Ubiquiti	UniFi AP U7 Pro	Ethernet (RJ45) PoE	90	PoE
5	patch-panel	Alantec	Alantec 19" 1U 48 портів Cat 5e STP Black	48 портів Cat 5e STP	28	patch-panel
6	patch-panel	Corning	Corning на 48 портів з модулями S500 FutureCom CAT 6A 1U	48 портів з модулями S500 FutureCom CAT 6A	2	patch-panel

Додаток Е

Схема підключення на комутаторі

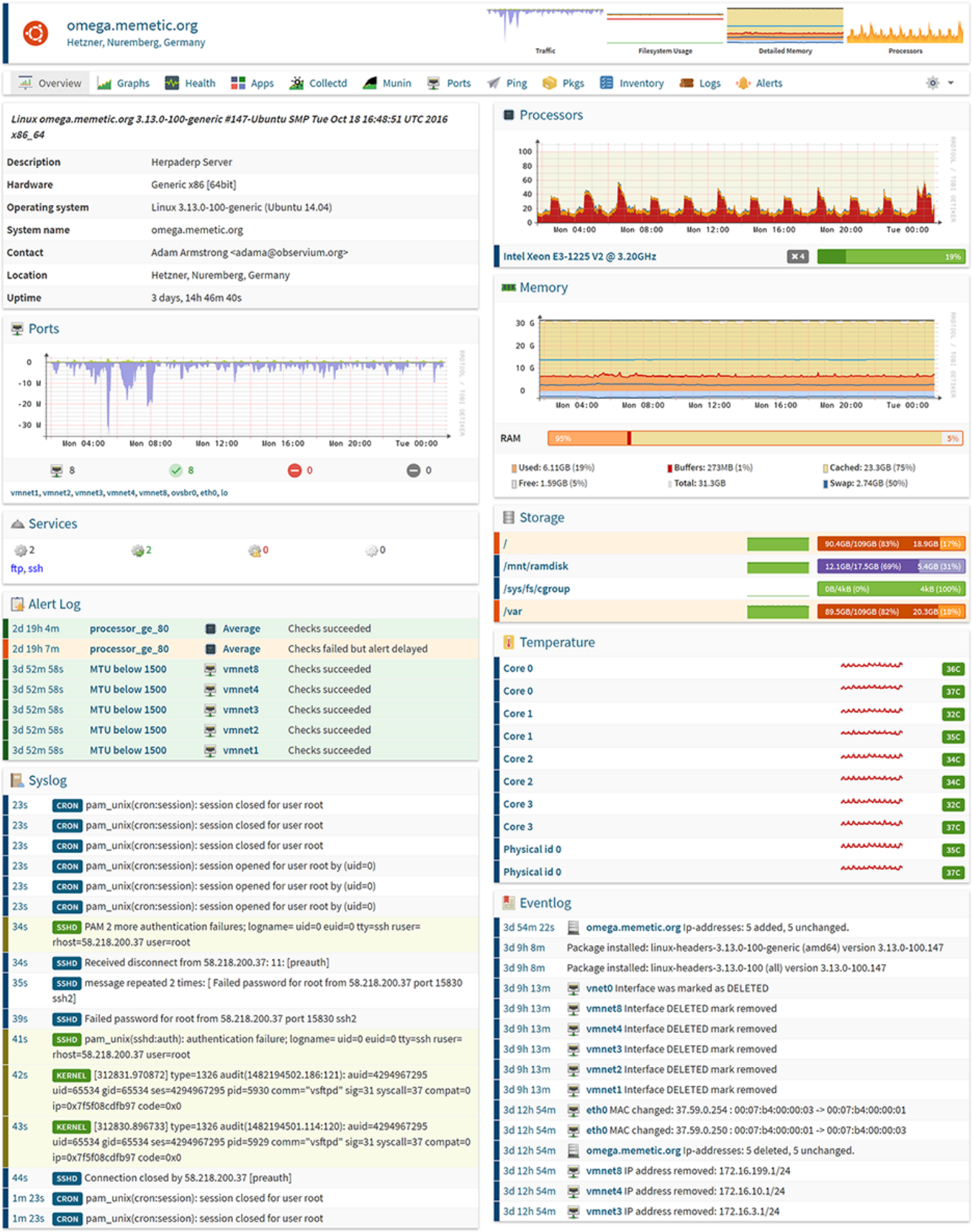


Додаток Ж

Встановлене обладнання в комутаційній шафі

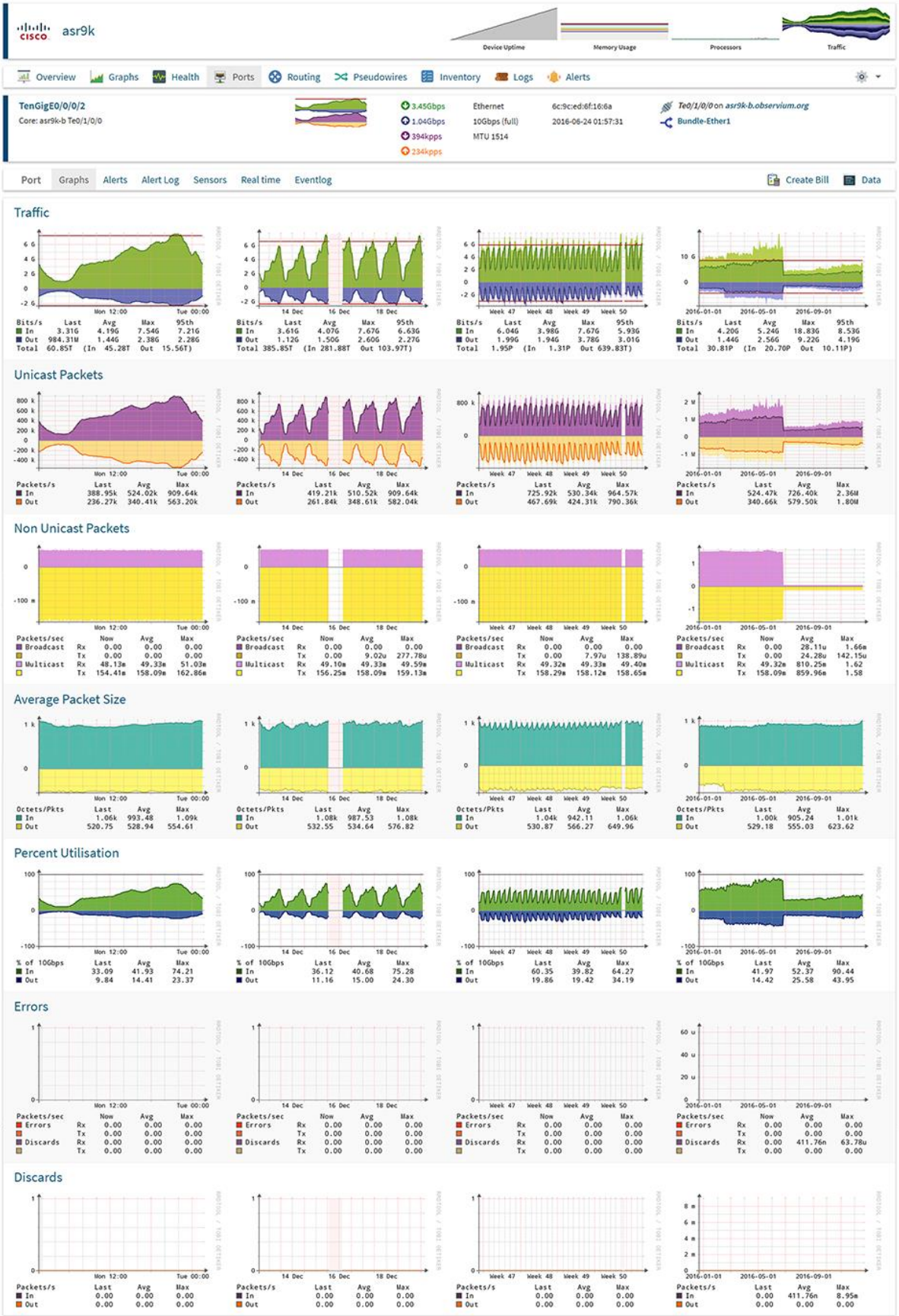
Додаток К

Контроль стану пристрою в Observium



Додаток Л

Дані про трафік в Observium



Додаток М

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА

на тему: «Розробка корпоративної комп'ютерної мережі на базі технології FHRP для підприємства»

Виконав студент групи КІД-41
Дідовець Владислав Максимович
Керівник кваліфікаційної роботи:
Бученко Ігор Анатолійович,
старший викладач кафедри КІ

Київ – 2024

Мета роботи – Розробка корпоративної комп'ютерної мережі на базі технології FHRP для підприємства

Об`єкт дослідження – Корпоративна комп'ютерна мережа на базі технології FHRP для підприємства

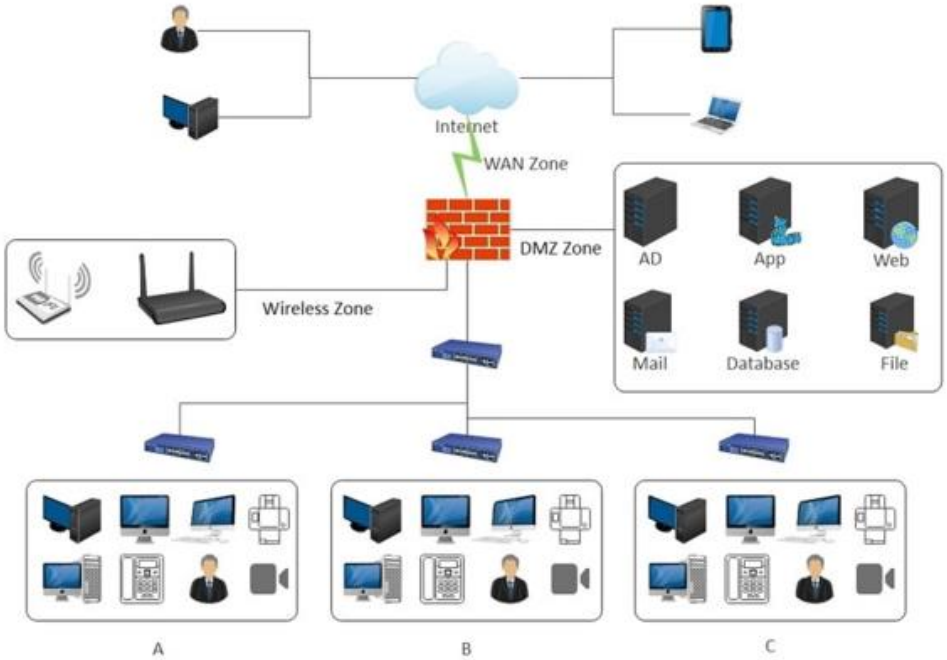
Предмет дослідження – Комп'ютерна мережа на базі технології FHRP

Актуальність обраної теми

В наш час комп’ютерні мережі є невід’ємною складовою нашого життя. Вони присутні всюди де є людина та її діяльність та відрізняються за сферою діяльності. Корпоративні комп'ютерні мережі потребують постійного доступу до мережі Інтернет за для роботи компанії. Проте, якщо маршрутизатор в такій мережі виходить з ладу компанія втрачає доступ до Інтернету. В цьому випадку можна застосувати технологію FHRP за умови використання декількох маршрутизаторів. Вона забезпечить резервування основного маршрутизатора або роботу декількох у режимі балансування.

3

Приклад корпоративної комп’ютерної мережі



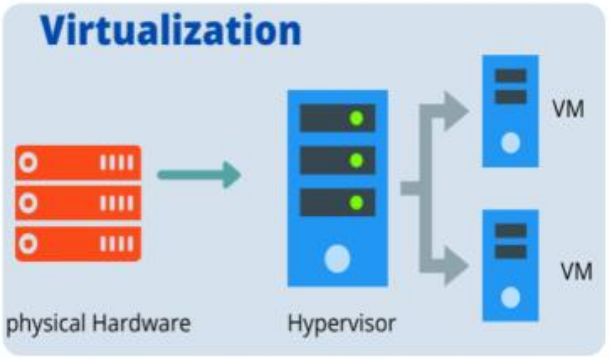
4

Характеристики та вимоги до корпоративної комп'ютерної мережі:

1. достатня пропускна здатність;
2. надійність мережі;
3. масштабованість;
4. керованість;
5. резервування важливих даних;
6. підтримка периферійного обладнання.

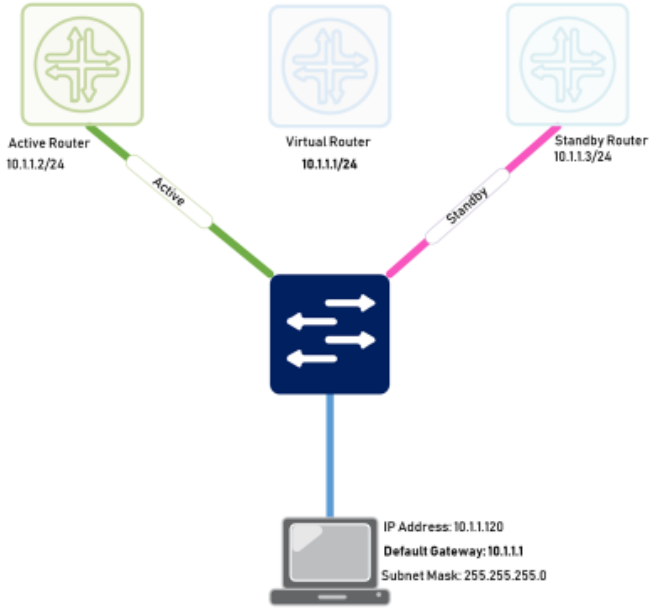
5

Віртуалізація в корпоративних комп'ютерних мережах:



6

Технологія FHRP для побудови надійної корпоративної мережі:

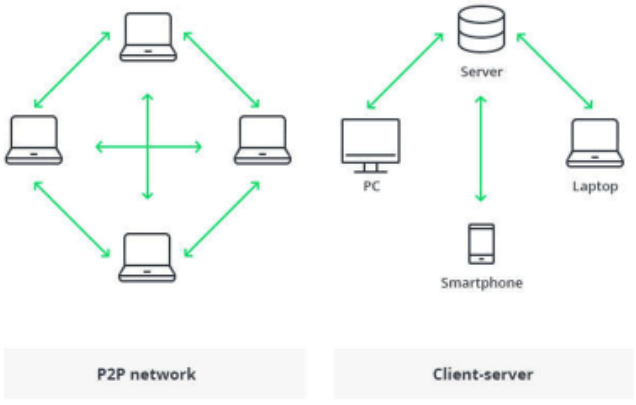


Технологія FHRP (First-hop redundancy protocol) – це технологія резервування першого переходу, розроблена для захисту шлюзу за замовчуванням, що використовується в підмережі, дозволяючи двом або більше маршрутизаторам забезпечувати резервне копіювання цієї адреси у разі виходу з ладу активного маршрутизатора

7

Вид мережі

1. однорангова мережа (Peer-to-peer, P2P) – це мережа, в якій всі пристрої є рівноправними та можуть взаємодіяти один з одним без ієрархічної системи;
2. клієнт-серверна мережа – це модель мережі, де доступ кінцевих користувачів до різних ресурсів здійснюється за допомогою виділеного сервера з різними правами доступу для користувачів.

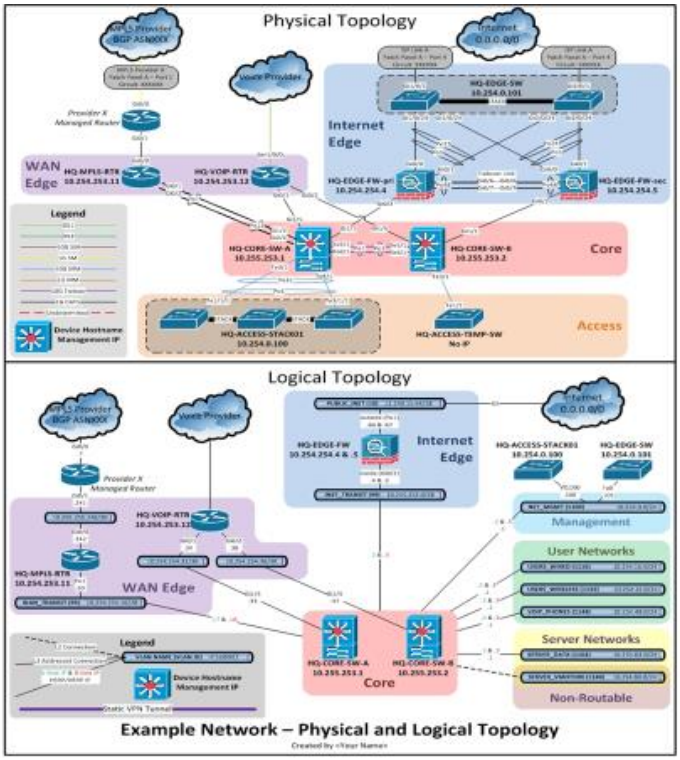


8

Топології

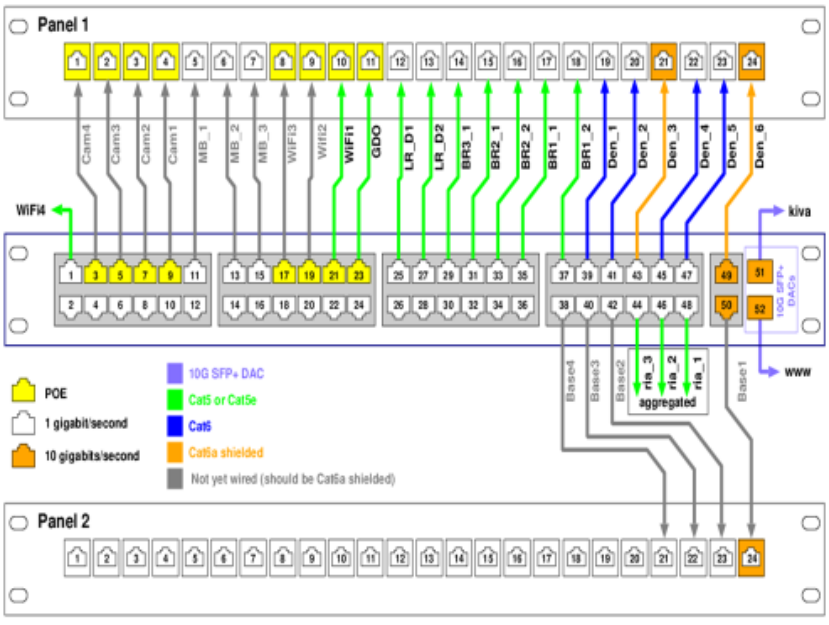
1. Логічна топологія (Layer 3) – це опис з’єднань, що визначають та показують шляхи для обміну даними між різними вузлами в мережі незалежно від їх фізичного розташуваннявисока міра гетерогенності типів комп'ютерів, комунікаційного обладнання, різні операційних систем і додатки;

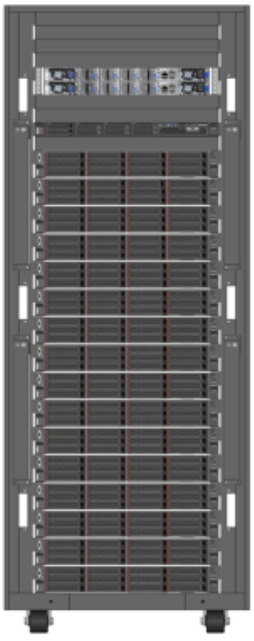
2. Фізична топологія (Layer 2) – це схема, що показує розташування різних елементів мережі та їх підключення між собою.



9

Схеми підключення та розташування



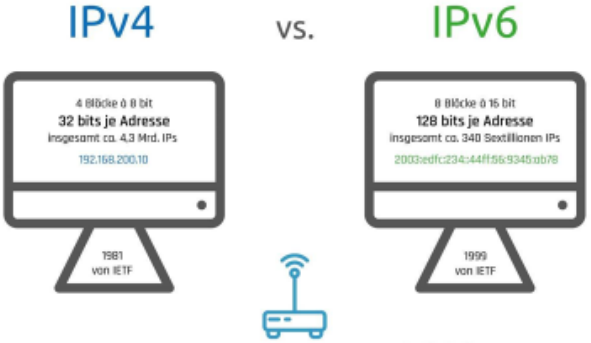


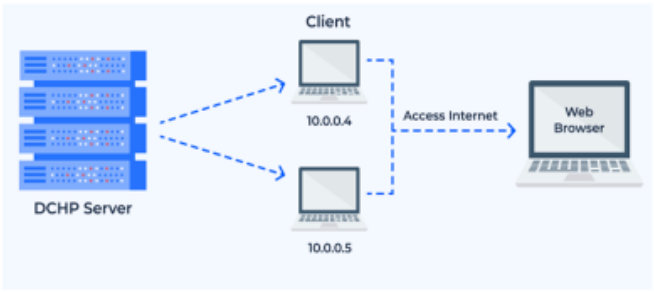
Mellanox SN2410 "TOR-2" Switch
Mellanox SN2410 "TOR-1" Switch

SR630 V3 "HLH" management system
SR650 V3 "Node16"
SR650 V3 "Node15"
SR650 V3 "Node14"
SR650 V3 "Node13"
SR650 V3 "Node12"
SR650 V3 "Node11"
SR650 V3 "Node10"
SR650 V3 "Node09"
SR650 V3 "Node08"
SR650 V3 "Node07"
SR650 V3 "Node06"
SR650 V3 "Node05"
SR650 V3 "Node04"
SR650 V3 "Node03"
SR650 V3 "Node02"
SR650 V3 "Node01"

10

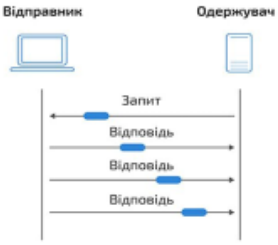
Протоколи та сервіси:





TCP

UDP



11

Розташування обладнання

Модулі SFP

Fiber SFP Module

Copper SFP Module

Критерії вибору мережевого обладнання:

1. розмір мережі;
2. маштабування;
3. кількість користувачів та пристроїв;
4. пропускна здатність;
5. надійність мережі;
6. типи підключення пристроїв;
7. бюджет.

12

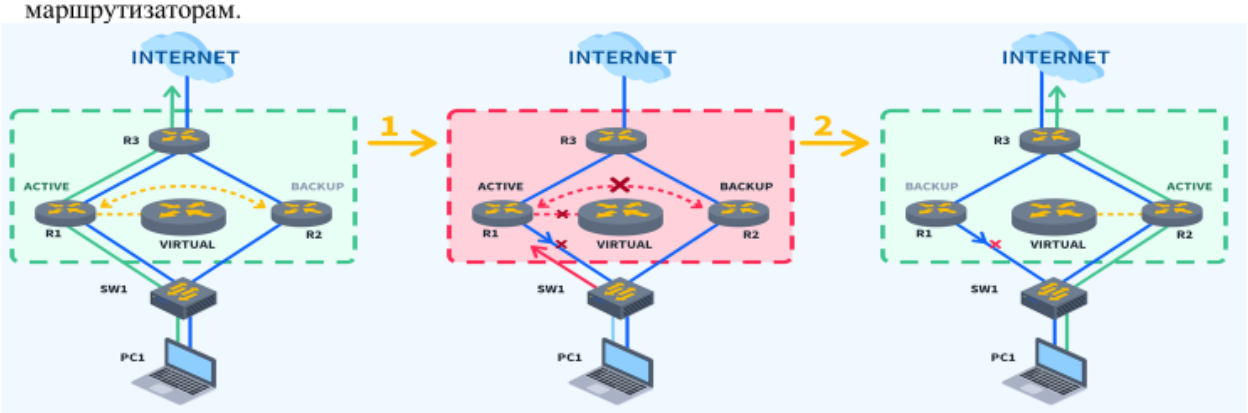
Приклад компанії:

Українська ігрова компанія “Віртуальні мандрівники” – це професійна та амбітна ігрова компанія, яка прагне створювати високоякісні, високобюджетні ігри, що будуть захоплювати гравців по всьому світу своїм сюжетом, графікою, механіками, увагою до деталей й дарувати гравцям приємні враження при проходженні гри. Майбутній проєкт компанії має назву: "Епічні легенди: Володарі перснів та Хоббіта" – це нова відеогра, яка поєднує в собі два культові світи: "Володар перснів" та "Хоббіт".

13

Варіанти використання FHRP в корпоративній комп'ютерній мережі:

1. HSRP – це Cisco-пропрієтарний FHRP, що призначений для забезпечення відмовостійкості IPv4-пристрою першого переходу тобто маршрутизатора;
2. VRRP – це протокол з відкритим стандартом, що динамічно призначає маршрутизатори в роль активного чи резервного;
3. GLBP – це Cisco-пропрієтарний FHRP, який захищає трафік даних від відмов маршрутизатора забезпечуючи балансування навантаження одночасно дозволяючи працювати декільком маршрутизаторам.



Принцип роботи протоколів HSRP та VRRP

14

Етапи розробки та впровадження проєкту:

1. отримання завдання. Від замовника отримується завдання з вимогами на розробку мережі під певну компанію. Замовник надає дизайнерські схеми, плани приміщення, інформацію про штат тощо;

2. проєктування мережі. Розраховують кількість пристроїв в кожному приміщені, рисують топології, схеми прокладанні дротів, розробляють IP-план та список необхідного облодання;

3. закупівля обладнання. Проводиться закупівля обладнання та ліцензій;

4. конфігурація обладнання: Відбувається конфігурація обладнання відповідно до вимог мережі;

5. тестування мережі. Проводиться тестування безпеки, з'єднань та доступності сервісів;

6. підтримка мережі. Це заходи з контролю стану обладнання та мережі за допомогою сервісів та програм Observium, PRTG, Wireshark, Zabbix тощо;

15

ВИСНОВКИ

Дослідивши корпоративну комп'ютерну мережу, вимоги до її розгортання, налаштування та подальшої роботи, віртуалізацію та використання в ній протоколів технології FHRP можна дійти висновку, що корпоративні комп'ютерні мережі є дуже поширеними й в залежності від виду діяльності компанії мають різні вимоги та особливості. Використання протоколів технології FHRP роблять корпоративну комп'ютерну мережу відмовостійкою та надійною. Її протоколи забезпечують стабільний доступ до мережі Інтернет, що є важливим для будь-якого бізнесу.

Досліджено поняття архітектури мережі та її складових. Наведено два основних типи мереж, на які орієнтуються при побудові корпоративної комп'ютерної мережі. Визначено їх переваги та недоліки. Наведено протоколи та можливі сервіси, які можуть бути використані в корпоративній мережі. Виділено рекомендації правильного розташування фізичного обладнання та критерії вибору обладнання для корпоративної комп'ютерної мережі.

16

ПРОДОВЖЕННЯ ВИСНОВКІВ

Приведено приклад компанії, що може потребувати надійної корпоративної комп'ютерної мережі з використанням різних протоколів резервування шлюзу за замовчуванням. Описано ці протоколи та продемонстровано приклад роботи одного з них. Визначено етапи впровадження проєкту з послідовністю розробки корпоративної комп'ютерної мережі, документуванням та засобами, що використовуються в роботі. Розглянуто питання безпеки й моніторингу для постійного контролю та підтримки корпоративної комп'ютерної мережі.

Інвестиції в розробку аналогічних технологій та протоколів, подальший їх розвиток є актуальним й необхідним, оскільки вони забезпечують надійність та доступність мережі у випадку непередбачуваних ситуацій.

17

РЕЗУЛЬТАТИ ВПРОВАДЖЕННЯ

1. Бученко І. А., Дідовець В. М. Огляд сучасних протоколів маршрутизації. «Проблеми комп'ютерної інженерії» : IV науково-практ. конф., м. Київ, 1 груд. 2023 р. С. 94–96. URL: https://duikt.edu.ua/uploads/p_2626_33497568.pdf.

2. Бученко І. А., Дідовець В. М. Відмовостійкість мережі. «Проблеми комп'ютерної інженерії» : IV науково-практ. конф., м. Київ, 1 груд. 2023 р. С. 96–98. URL: https://duikt.edu.ua/uploads/p_2626_33497568.pdf.

18