КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій

_____

(факультет)

інформаційних технологій

_____

(кафедра)

ПОЯСНЮВАЛЬНА ЗАПИСКА

ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ

НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЮ «БАКАЛАВР»

на тему: «Розробка захищеної бази даних інтернет провайдера»

ВОРОНКОВ АРТЕМ СЕРГІЙОВИЧ

(прізвище, ім’я та по батькові студента повністю)

Київ 2023 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

БУДІВНИЦТВА І АРХІТЕКТУРИ

автоматизації і інформаційних технологій

_____

(факультет)

інформаційних технологій

_____

(кафедра)

ЗАТВЕРДЖУЮ

Завідувач кафедри ІТ

д.т.н., професор Цюцюра С.В.

_____

„___” _____2023 року

ПОЯСНЮВАЛЬНА ЗАПИСКА

ДО АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ

НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЮ «БАКАЛАВР»

на тему: "Розробка захищеної бази даних інтернет провайдера"

Виконав: Студент спеціальності

122 «Комп`ютерні науки .

(шифр і назва напряму підготовки, спеціальності)

Воронков А.С. .

(прізвище та ініціали)

Керівник __д.т.н., проф. Терентьєв О.О. ____

(прізвище та ініціали)

Рецензент __к.т.н., доц. Шабала Є.Є. .

(прізвище та ініціали)

Київ, 2023 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: __автоматизації і інформаційних технологій .

Кафедра:___інформаційних технологій .

Освітній рівень: «бакалавр» за ОП .

Спеціальність: 122 «Комп`ютерні науки» .

ЗАТВЕРДЖУЮ

Завідувач кафедри ІТ

д.т.н., професор Цюцюра С.В.

_____

„___” _____2023 року

З А В Д А Н Н Я

ДО ВИКОНАННЯ АТЕСТАЦІЙНОЇ ВИПУСКНОЇ РОБОТИ

НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЮ «БАКАЛАВР»

Воронков Артем Сергійович

(прізвище, ім’я та по батькові студента)

1. Тема роботи: Розробка захищеної бази даних інтернет провайдера .

затверджена наказом ректора КНУБА № _____ від « » листопад 2022 р.

2. Керівник роботи: Терентьєв Олександр Олександрович, д.т.н, професор кафедри ІТППМ .

3. Строк подання студентом роботи до захисту: червень 2023 р. .

4. Зміст пояснювальної записки за розділами:

Р. 1. Аналіз предметної області .

Р. 2. Проектування бази даних системи .

Р. 3. Тестування роботи інформаційної технології .

Р. 4. Ергономіка інформаційних технологій .

5. Інформаійні слайди:

С. 1. Діаграма дерево цілей .

С. 2. Модель багатоканальної систсеми прийому замовлень .

С. 3. Модель процесу обробки змовлень .

С. 4. Граф станів .

С. 5. Модель архітектурного шаблону програмного забезпечення системи.

С. 6. _Структура модулів системи .

6. Календарний план виконання атестаційної випускної роботи

Види робіт та їх зміст	Дата виконання
Р. 1. Аналіз предметної області	Травень 2023 р.
Р. 2. Проектування бази даних системи	Травень 2023 р.
Р. 3. Тестування роботи інформаційної технології	Травень 2023 р.
Р. 4. Ергономіка інформаційних технологій	Травень 2023 р.
Остаточне оформлення роботи	Червень 2023 р.
Направлення роботи на рецензування	Червень 2023 р.
Попередній захист роботи на кафедрі	Червень 2023 р.

7. Консультанти розділів атестаційної випускної роботи

Розділ	Прізвище, ініціали та посада консультанта, представника комісії	дата	підпис
Ергономіка інформаційних технологій	д.т.н. проф. Терентьєв О.О.		
Прийом програмного продукту	к.т.н. доц. Шабала Є.Є.		

8. Дата видачі завдання: 11 листопада 2022 року

Керівник Терентьєв О.О.

(підпис) (прізвище та ініціали)

Бакалавр Воронков А.С.

(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Воронков А.С. «Розробка захищеної бази даних інтернет провайдера».

Атестаційна випускова робота бакалавра за спеціальністю: 122 «Комп'ютерні науки». – Київський національний університет будівництва та архітектури. – Київ, 2023.

Інформаційна технологія управління Інтернет - магазином як складова системи управління інтернет - магазином у цілому забезпечує автоматизацію продажу товарів, прийому замовлень, а також автоматизує: процесс вибору товару, оплати, формування рахунків, управління ассортиментом магазину, оптимізацію процесса прийому замовлень.

Ключові слова: моделі, засоби, інформаційна технологія, інтернет - магазин, управління, проектування баз даних.

SUMMARY

Voronkov A.S. "Development of a secure Internet provider database."

Attestation thesis of the bachelor in the specialty: 122 "Computer science". - Kyiv National University of Construction and Architecture. - Kyiv, 2023.

Information technology of Internet - shop management as a component of the Internet - shop management system in general provides automation of sales of goods, acceptance of orders, and also automates: the process of product selection, payment, billing, assortment management, optimization of the process of ordering.

Keywords: models, means, information technology, internet shop, management, database designing.

ЗМІСТ

ВСТУП 8
1.ОГЛЯД ІСНУЮЧИХ МЕРЕЖЕВИХ МОДЕЛЕЙ 10
1.1. Модель OSI 11
1.2. Протоколи TCP/IP 14
1.3. Маршрутизація 17
1.4. Рівні комутаторів 22
2.ОГЛЯД ТОПОЛОГІЙ ТА АНАЛІЗ ПРОБЛЕМ, ЩО ВИНИКАЮТЬ. 25
2.1. Топології мереж 26
2.2. Vlan 34
2.3. Spanning Tree Protocol та його специфікації 37
2.4. flowcontrol 42
2.5. Speed and Duplex 43
2.6. Опис відомих проблем 46
3.РОЗРОБКА КОМП'ЮТЕРНОЇ МЕРЕЖІ INTERNET-ПРОВАЙДЕРА. 51
4. ЕРГОНОМІКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ……..64
ВИСНОВКИ 62
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 77
ДОДАТКИ ..... **Ошибка! Закладка не определена.**

ВСТУП

Раніше, коли люди не мали іншої можливості розповсюджувати і зберігати інформацію аніж на фізичних носіях даних, таких як жорсткі диски, дискети, USB-накопичувачі, CD та DVD диски, користувачі не сильно задумувалися над необхідністю доступу до інтернету, такий доступ не був річчю, без якої людина не могла би уявити свого життя. Інтернет в той час надавав простим користувачам не більше, ніж просту можливість переглядати певний перелік сторінок, наповнених інформацією. Але на теперішній час, ситуація, що стосується інтернету швидко змінюється і набирає нових, непритаманних йому раніше рис. Так, ніхто досі й подумати не міг про те, що у людей буде можливість зберігати будь-яку інформацію десь в одному місці, та отримувати доступ до власного сховища даних звідусіль, де б власник не знаходився. Також слід зазначити, що з таким розвитком можливостей зберігання даних, було життєво необхідно забезпечити цілісність та захищеність таких даних. Коли такі можливості для зберігання даних тільки входили повсякденне життя людей, про захист думали досить недбало. Настільки, що поцупити дані у користувача без його відома було простіше, аніж отримати доступ до даних, що зберігалися деінде безпосередньо у користувача. Але з плином часу ця проблема також знаходить свої шляхи вирішення, але досягнути абсолютної безпеки підключення все ще не вдається. Оскільки зі збільшенням захищеності даних та підключення, зростає і жага да цих даних тими, хто мати доступ до них не повинен. Так і буде продовжуватися ця боротьба між тими, хто захищає, та тими, хто бажає не по праву власності заволодіти всім.

На сьогоднішній день для простого користувача вже не є можливим навіть уявити своє існування без інтернет-підключення. Все більше і більше

речей переноситься в мережу інтернет, вона продовжує розповсюджувати свій вплив на всі сфери людського життя. Зараз люди не тільки отримують інформацію з інтернету, посередництвом інтернет-ресурсів, таких як «вікіпедія», наприклад, а ще й отримали можливість виконувати досить великий спектр дій та операцій: зберігання, завантаження, викладання інформації будь куди. Зараз, більша частина провідних компаній також зав'язана на інтернет-підключенні, через що вона виявляється досить щільно пов'язана з необхідністю надання стабільного, безперебійного підключення, що буде працювати 24/7 без необхідності постійного за ним нагляду.

Чим далі йде у своєму розвитку людство – тим більше функцій бере на себе віддалене керування, таким чином, наприклад, вже можна оплачувати рахунки через інтернет, користуючись одним тільки телефоном, з наявним на ньому інтернет-підключенням. Інтернет на даний момент – це основна площа, де люди з усіх куточків земної кулі можуть зустрітися, навіть якщо це не має відношення до фізичного прояву світу, але це має дуже високе значення для інших аспектів людського життя. Уявити, що люди в якийсь момент можуть втратити доступ до інтернету, та будуть змушень повертатися до «дідівських» методів зберігання та отримання даних – для більшості така альтернатива розвитку з наявним доступом до мережі інтернет може бути гіршою за пекло. До чого тільки може призвести така подія - втрата інтернет-підключення на декілька діб. Більшість молодого покоління може розцінити це як клінічну смерть людини, з якою вони спілкувалися от ще декілька миттів тому. Саме через такі дрібні проблеми у житті простих людей, а також підвищений рівень комфорту, якого вдалося досягти завдяки інтернету, спонукає спеціалістів до забезпечення якомога стабільнішого та надійнішого інтернет-підключення, щоб користувачі даної мережі могли отримати доступ до бажаного її елементу у будь-який проміжок часу, будь то вдень чи вночі. В дипломній роботі розробляється рішення відомих проблем, що трапляються в роботі мереж інтернет-провайдерів.

1. ОГЛЯД ІСНУЮЧИХ МЕРЕЖЕВИХ МОДЕЛЕЙ

Сам по собі, інтернет являє собою всесвітню систему сполучених комп'ютерних мереж, що базуються на комплекті Інтернет-протоколів. Інтернет також називають мережею мереж, що складається з мільйонів локальних і глобальних приватних, публічних, академічних, ділових і урядових мереж, пов'язаних між собою з використанням різноманітних дротових, оптичних і бездротових технологій. Інтернет становить фізичну основу для розміщення величезної кількості інформаційних ресурсів і послуг, таких як взаємопов'язані гіпертекстові документи Всесвітньої павутини (World Wide Web — WWW) та електронна пошта.

Інтернет не має централізованого управління, правил використання чи доступу. Кожна складова мережа встановлює свої власні стандарти. Централізовано визначаються правила використання адресного простору Інтернет-протоколу та Системи доменних імен. Керує цим Інтернет-корпорація з присвоєння імен та номерів (англ. Internet Corporation for Assigned Names and Numbers, або ICANN), міжнародна некомерційна організація з головним офісом у США. Технічне обґрунтування і стандартизацію основних протоколів (IPv4 та IPv6) проводить Internet Engineering Task Force (IETF) — некомерційна організація, відкрита міжнародна спільнота проектувальників, учених, мережевих операторів і постачальників послуг.

Інтернет складається з багатьох тисяч корпоративних, наукових, урядових та домашніх мереж. Об'єднання різнорідних за архітектурою мереж стало можливо завдяки протоколу IP (англ. Internet Protocol) і принципу

маршрутизації пакетів даних. Протокол IP був спеціально створений агностичним у відношенні до фізичних каналів зв'язку. Тобто будь-яка мережа передачі цифрових даних може передавати інтернет-трафік. На стиках мереж спеціальні маршрутизатори займаються сортуванням та перенаправленням пакетів даних, базуючись на IP-адресах одержувачів цих пакетів. Протокол IP утворює єдиний адресний простір у масштабах всього світу, але в кожній окремо взятій мережі може існувати свій власний адресний підпростір. Така організація IP-адрес дозволяє маршрутизаторам однозначно визначати подальший напрямок для кожного, навіть найменшого, пакету даних. У результаті між різними мережами Інтернету не виникає конфліктів і дані точно і без перешкод передаються від мережі до мережі по всій планеті.

Також, для більш детального опису, для повноти розуміння має місце зазначити так досить суттєву деталь, як модель OSI, завдяки якій процес інтернет-підключення, маршрутизації та обміну даними стає більш прозорим і зрозумілим для користувача.

1.1. Модель OSI

Модель OSI (базова еталонна модель взаємодії відкритих систем) — абстрактна мережева модель для комунікацій і розробки мережевих протоколів. Представляє рівневий підхід до мережі. Кожен рівень обслуговує свою частину процесу взаємодії. Завдяки такій структурі спільна робота мережевого обладнання й програмного забезпечення стає набагато простішою, прозорішою й зрозумілішою.

	Единица данных	Уровень	Функция	Примеры протоколов
ОС	Поток	Прикладной	Прикладная задача	HTTP, SMTP, DNS, etc.
		Представления	Представление данных, шифрование, etc.	MIME, SSL
		Сеансовый	Взаимодействие хостов (на уровне ОС)	NetBIOS, именов. пайпы
	Сегмент	Транспортный	Соединение конец-в-конец, контроль передачи данных	TCP, UDP
Сеть	Пакет	Сетевой	Логическая адресация и маршрутизация пакетов	IP, ICMP
	Фрейм	Канальный	Физическая адресация	IEEE 802.3, ARP, DHCP
	Бит	Физический	Кодирование и передача данных по физическому каналу	IEEE 802.3

Рисунок 1.1 – Рівні моделі OSI

Відлік рівнів моделі проводиться знизу догори: від фізичного рівня закінчуючи прикладним рівнем.

Фізичний рівень - Найнижчий рівень моделі, призначений безпосередньо для передачі потоку даних. Здійснює передачу електричних або оптичних сигналів у кабель і відповідно їхній прийом і перетворення в біти даних відповідно до методів кодування цифрових сигналів. Інакше кажучи, здійснює інтерфейс між мережним носієм і мережним пристроєм. На цьому рівні працюють концентратори й повторювачі (ретранслятори) сигналу. Фізичний рівень визначає електричні, процедурні і функціональні специфікації для середовища передачі даних, в тому числі роз'єми, розпаювання і призначення контактів, рівні напруги, синхронізацію зміни напруги, кодування сигналу.

Цей рівень приймає кадр даних від канального рівня, кодує його в послідовність сигналів, які потім передаються у лінію зв'язку. Передача кадру даних через лінію зв'язку вимагає від фізичного рівня визначення таких елементів: тип середовища передавання (дротовий або бездротовий, мідний кабель або оптичне волокно) і відповідних конекторів; як повинні бути представлені біти даних у середовищі передавання; як кодувати дані; якими повинні бути схеми приймача і передавача.

Канальний рівень - Цей рівень призначений для забезпечення взаємодії мереж на фізичному рівні й контролю за помилками, які можуть виникнути. Отримані з фізичного рівня дані він упаковує в кадри даних, перевіряє на цілісність, якщо потрібно виправляє помилки й відправляє на мережний рівень. Канальний рівень може взаємодіяти з одним або декількома фізичними рівнями, контролюючи й управляючи цією взаємодією. Специфікація IEEE 802 розділяє цей рівень на 2 підрівня — MAC (Media Access Control) регулює доступ до поділюваного фізичного середовища, LLC (Logical Link Control) забезпечує обслуговування мережного рівня. На цьому рівні працюють комутатори, мости й мережні адаптери.

Мережевий рівень - 3-й рівень мережної моделі OSI, призначений для визначення шляху передачі даних. Відповідає за трансляцію логічних адрес й імен у фізичні, визначення найкоротших маршрутів, комутацію й маршрутизацію пакетів, відстеження неполадок і заторів у мережі. На цьому рівні працює такий мережний пристрій, як маршрутизатор.

Транспортний рівень - 4-й рівень моделі OSI, призначений для доставлення даних без помилок, втрат і дублювання в тій послідовності, у якій вони були передані. При цьому немає значення, які дані передаються, звідки й куди, тобто він визначає сам механізм передачі. Блоки даних він розділяє на фрагменти, розмір яких залежить від протоколу, короткі об'єднує в один, довгі розбиває. Протоколи цього рівня призначені для взаємодії типу «точка-точка».

Сеансовий рівень - Відповідає за підтримку сеансу зв'язку, дозволяючи додаткам взаємодіяти між собою тривалий час. Рівень керує створенням/завершенням сеансу, обміном інформацією, синхронізацією завдань, визначенням права на передачу даних і підтримкою сеансу в періоди неактивності додатків. Синхронізація передачі забезпечується розміщенням у потік даних контрольних точок, починаючи з яких відновлюється процес при порушенні взаємодії.

Рівень представлень - цей рівень відповідає за перетворення протоколів і кодування/декодування даних. Запити додатків, отримані з прикладного рівня, він перетворить у формат для передачі по мережі, а отримані з мережі дані перетворить у формат, зрозумілий додаткам. На цьому рівні може здійснюватися стиснення/розпакування або кодування/декодування даних, а також перенапрямок запитів іншому мережевому ресурсу, якщо вони не можуть бути оброблені локально.

Прикладний рівень - верхній (7-й) рівень моделі, забезпечує взаємодію мережі й користувача. Рівень дозволяє додаткам користувача доступ до мережних служб, таким як обробник запитів до баз даних, доступ до файлів, пересиланню електронної пошти. Також відповідає за передачу службової інформації, надає додаткам інформацію про помилки й формує запити до рівня подання.

На даний час основним використовуваним стеком протоколів є TCP/IP, розробка якого не була пов'язана з моделлю OSI і до того ж була здійснена до її прийняття. За увесь час існування моделі OSI вона не була реалізована, і, очевидно, не буде реалізована ніколи. Сьогодні використовується тільки деяка підмножина моделі OSI. Вважається, що модель занадто складна, а її реалізація займе занадто багато часу.

1.2. Протоколи TCP/IP

Стек протоколів TCP/IP – набір протоколів для роботи з мережею Інтернет. Назва утворилася завдяки двом основним протоколам стеку: IP – internet protocol – мережевий протокол; TCP – transmission control protocol – протокол керування передаванням. Даний стек протоколів поділяється на чотири рівні (Прикладний, Транспортний, Мережевий, Рівень доступу до середовища передачі), що були сформовані завдяки впливу еталонної моделі OSI.

Прикладний рівень - Протоколи прикладного рівня TCP/IP визначають процедури організації взаємодії прикладних процесів (програм) різних мережевих комп'ютерів і форми подання інформації за такої взаємодії. За ознаками взаємодії прикладних процесів виділяють два типи прикладного програмного забезпечення: програма-клієнт та програма-сервер. Протоколи прикладного рівня зорієнтовано на конкретні прикладні завдання. Серед традиційних послуг, котрі забезпечують протоколи прикладного рівня з сімейства TCP/IP, сьогодні найпопулярнішими є електронна пошта — протоколи SMTP та POP3, передача файлів — FTP та TFTP, емуляція віддаленого терміналу — TELNET чи SSH.

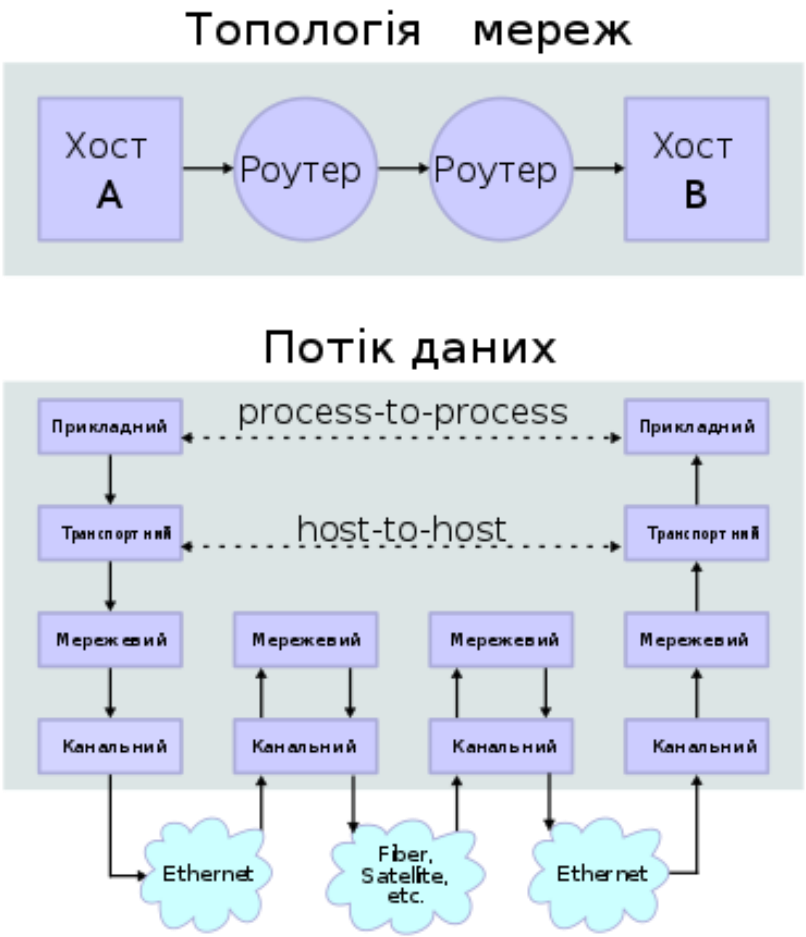


Рисунок 1.2 – Рівні стеку TCP/IP та взаємодія між ними

Транспортний рівень - Протоколи транспортного рівня TCP/IP-моделі надають транспортні послуги прикладним процесам. Основними протоколами транспортного рівня TCP/IP є протокол керування передавання TCP і протокол користувальницьких дейтаграм UDP. Транспортні послуги цих протоколів суттєво відрізняються. Протокол UDP доставляє дейтаграми без установлення з'єднання. При цьому він не гарантує їхнього доставляння. Протокол TCP забезпечує надійне доставляння байтових потоків (сегментів) із попереднім встановленням транспортного дуплексного з'єднання (віртуального каналу) між модулями TCP мережевих комп'ютерів. Для розв'язання транспортних завдань протоколи TCP та UDP під час передавання даних формують і додають до даних свої заголовки обсягом 20 байт та 8 байт відповідно.

Мережевий рівень - Протоколи мережевого рівня TCP/IP забезпечують взаємодію мереж різної архітектури тощо. Основним протоколом мережного рівня технології TCP/IP є мережевий протокол IP та його допоміжні протоколи: адресний протокол ARP; реверсний адресний протокол RARP (Reverse ARP); протокол діагностичних повідомлень ICMP (Internet Control Message Protocol), який надсилає повідомлення вузлам мережі про помилки на маршруті, які виникають при передачі пакетів тощо.

Рівень доступу до середовища передачі –

Функції:

- відображення IP-адреси в фізичні адреси мережі (MAC-адреси);
- інкапсуляція IP-датаграм в кадри для передачі по фізичному каналу і передачі кадрів.
- На цьому рівні працює протокол ARP[12], який здійснює відображення адреси IP-> MAC.

Для формування підключення від одного комп’ютера до іншого, чи від однієї мережу до іншої знайшла своє застосування така технологія, як маршрутизація.

1.3. Маршрутизація

Маршрутиза́ція — процес визначення маршруту прямування інформації між мережами. Маршрутизатор (або роутер) приймає рішення, що базується на IP-адресі отримувача пакету. Для того, щоб переслати пакет далі, всі пристрої на шляху слідування використовують IP-адресу отримувача. Для прийняття правильного рішення маршрутизатор має знати напрямки і маршрути до віддалених мереж.

Схеми маршрутизації:

Anycast - Метод розсилання пакетів, що дозволяє пристроям посилати дані найближчому з групи отримувачів. Даний тип маршрутизації, наприклад, реалізовано в протоколі IPv6. В протоколі IP anycast реалізований шляхом публікації однакового маршруту з різних точок мережі посередництвом протоколу BGP. Одним з основних критеріїв вибору маршруту в BGP є AS-Path – набор(список) номерів автономних систем, через які повинен пройти пакет: обирається маршрут з найкоротшим AS-Path. При отриманні опису маршруту із двох чи більше точок, буде обраний найкоротший шлях[46]

Через особливості топологій мережі чи її політики найближчий вузол не обов’язково буде географічно найближчим.

На сьогоднішній день схема anycast застосовується в мережі інтернет для зменшення часу відповіді і балансування навантаження на корінних DNS-серверах.

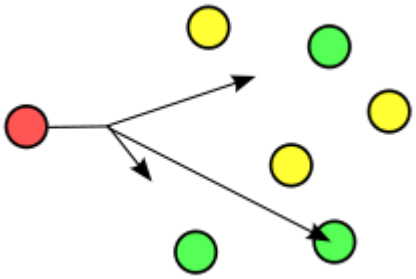


Рисунок 1.3 - Схема маршрутизації anycast

Broadcast - Метод передачі даних в комп'ютерних мережах, при котрому потік даних(кожний пересланий пакет у випадку пакетної передачі) призначений для прийому всіма учасниками мережі.

У стеку протоколів TCP/IP широкомовний канал можливий до реалызації тільки в межах одного сегменту мережі(Л2 чи Л3). Однак, пакети даних можуть бути передані ззовні визначеного сегменту, в якому буде виконано широкомовний запит(Наприклад, передача пакету на широкомовну IP-адресу через маршрутизатор з-за меж мережі). Навантаження на мережу у випадку використання широкомовного каналу не відрізняється від звичайної передачі даних одному адресату, оскільки пакети не розмножуються(на відміну від unicast).

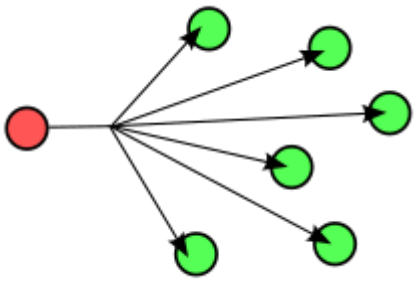


Рисунок 1.4 - Схема маршрутизації broadcast

Multicast – спеціальна форма телевізійного чи іншого мовлення, при якій копії пакетів надсилаються певній підмножині адресатів. Термін multicast найбільш часто застосовується, коли мова йде про надання відео потоку або IP телефонії через інтернет. Окремі випадки Multicast, це unicast - потік даних йде певному вузлу, і broadcast - широкомовна розсилка, коли потік даних йде до всіх вузлів мережі без вибору.

Дана технологія використовує адреси з 224.0.0.0 по 239.255.255.255. Підтримується статична та динамічна адресація. Прикладом статичних адрес є 224.0.0.1 — адреса групи, що включає в себе всі вузли локальної мережі, 224.0.0.2 — всі маршрутизатори локальної мережі. Діапазон адрес з 224.0.0.0 по 224.0.0.255 зарезервований для протоколів маршрутизації. Інші адреси використовуються додатками.

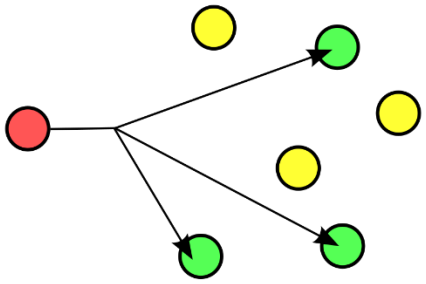


Рисунок 1.5 - Схема маршрутизації multicast

Unicast - Однонапрямлена(одностороння) передача даних, під якою мається на увазі передача пакетів єдиному адресату. Дана схема пакетної маршрутизації даних являється прямим протиставленням широкомовній схемі маршрутизації(Broadcast).

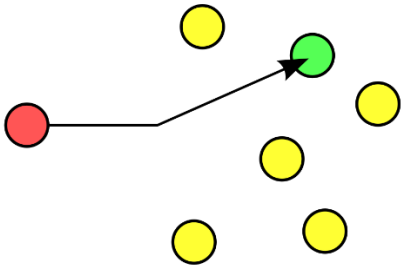


Рисунок 1.6 - Схема маршрутизації Unicast

Існує два типи маршрутизації:

- Статична маршрутизація — маршрути задаються вручну адміністратором.
- Динамічна маршрутизація — маршрути обчислюються автоматично за допомогою протоколів динамічної маршрутизації — RIP, OSPF, EIGRP, IS-IS, BGP, HSRP та ін, які отримують інформацію про топологію і стан каналів зв'язку від інших маршрутизаторів у мережі.

Оскільки статичні маршрути конфігуруються вручну, будь-які зміни мережної топології вимагають участі адміністратора для додавання і видалення статичних маршрутів відповідно до змін. У великих мережах підтримка таблиць маршрутизації вручну може вимагати величезних витрат часу адміністратора. У невеликих мережах це робити легше. Статична маршрутизація не має можливості масштабування, яку має динамічна маршрутизація через додаткові вимоги до налаштування і втручання адміністратора. Але і у великих мережах часто конфігуруються статичні маршрути для спеціальних цілей у комбінації з протоколами динамічної маршрутизації, оскільки статична маршрутизація є стабільнішою і вимагає мінімум апаратних ресурсів маршрутизатора для обслуговування таблиці.

Таблиця маршрутизації[2] — електронна таблиця (файл) або база даних, що зберігається на маршрутизаторі або мережевому комп'ютері, що описує відповідність між адресами призначення і інтерфейсами, через які слід відправити пакет даних до наступного маршрутизатора. Є найпростішою формою правил маршрутизації.

Таблиця маршрутизації зазвичай містить:

- Адресу мережі або вузла призначення, або вказівку, що маршрут є маршрутом за замовченням.
- Маску мережі призначення (для IPv4-мереж маска / 32 (255.255.255.255) дозволяє вказати одиничний вузол мережі)

- Шлюз, що позначає адресу маршрутизатора в мережі, на яку необхідно надіслати пакет, що прямує до вказаної адреси призначення
- Інтерфейс (залежно від системи це може бути порядковий номер, GUID або символьне ім'я пристрою)
- Метрику — числовий показник, що задає перевагу маршруту. Чим менше число, тим кращий маршрут (інтуїтивно представляється як відстань).

У таблиці може бути один, а в деяких операційних системах і кілька шлюзів за замовченням. Такий шлюз використовується для мереж для яких немає більш конкретних маршрутів в таблиці маршрутизації.

Динамічні маршрути виставляються іншим чином. Після того, як адміністратор активізував і налаштував динамічну маршрутизацію за одним з протоколів, інформація про маршрути оновлюється автоматично в процесі маршрутизації після кожного отримання з мережі нової інформації про маршрути. Маршрутизатори обмінюються повідомленнями про зміни у топології мережі в процесі динамічної маршрутизації.

Динамічна маршрутизація[10] – вид маршрутизації, при якому таблиця маршрутизації редагується на вручну, а програмно. У випадку систем на базі ядра UNIX – демонами маршрутизації, в інших системах – службовими програмами, що виконують ту саму роль.

Демони маршрутизації обмінюються між собою інформацією, котра дозволяє їм заповнити таблиці маршрутизації найбільш оптимальними маршрутами. Протоколи, за допомогою котрих виконується обмін інформацією між демонами, називаються протоколами динамічної маршрутизації.

В стеці протоколів TCP/IP[28] передбачено два демони, підтримуючих динамічну маршрутизацію: routed та gated. Демон gated підтримує одночасно Протокол інформації щодо маршрутизації (RIP – Routing Information Protocol), протокол інформації щодо маршрутизації наступного

покоління(RIPng – Routing Information Protocol next generation), протокол зовнішніх шлюзів(EGP – External Gateway Protocol), протокол граничних шлюзів (BGP – Border Gateway Protocol, BGP4+), та протокол HELLO(Протокол, за допомогою якого між обладнанням підтримуються сусідські стосунки), протокол найкоротшого шляху(OSPF – Open Shortest Path First), протоколи IS-IS(Intermediate System to Intermediate System), ICMP(Internet Control Message Protocol)та ICMPv6/Router Discovery. Окрім цього демон gated підтримує простий протокол керування мережею(SNMP – Simple Network Management protocol).

Демон routed підтримує тільки RIP-протокол. Залежності від опцій, вказаних при запусканні демона маршрутизації, він може працювати в одному з двох режимів – пасивному або активному. В активному режимі демон маршрутизації періодично відправляє шлюзам і хостам оповіщення , що містить інформацію щодо маршрутизації їх локальних мереж, а також отримує інформацію щодо маршрутизації від інших хостів та шлюзів. В пасивному режимі демон маршрутизації тільки отримує інформацію щодо маршрутизації і не намагається оновити інформацію щодо маршрутизації віддалених шлюзів (тобто він не розповсюджує свою інформацію щодо маршрутизації)[18].

Два описані типи маршрутизації застосовуються не тільки шлюзами, а й хостами мереж. Статична маршрутизація застосовується для шлюзів так само, як і для інших хостів. Проте, демони динамічної маршрутизації, котрі виконуються не на шлюзах, можуть працювати тільки в пасивному(тихому) режимі.

1.4. Рівні комутаторів

Для виконання поставлених задач у організації стабільного і безперебійного підключення застосовується обладнання різних рівнів обробки інформації. У даному контексті визначення «рівень» має на увазі рівень моделі OSI на якому працює обладнання, що буде застосоване. Нижче

приведено детальний аналіз та короткий огляд пристроїв кожного з рівнів та принципи його роботи:

Пристрої першого рівня(L1) – це пристрої, що працюють на фізичному рівні моделі OSI, дане обладнання взагалі не можуть оброблювати дані, що передають. Вони працюють на рівні електронних сигналів: сигнал було отримано – його необхідно передати далі. До таких пристроїв відносяться так звані «хаби»(hub) котрі здобули свою популярність в епоху зародження Ethernet-мереж, які застосовуються ще й досі. Також до даного рівня відносяться різноманітні повторювачі та підсилювачі. Пристрої такого типу зазвичай називають концентраторами.

Пристрої другого рівня(L2)- пристрої, що працюють на канальному рівні та виконують фізичну адресацію. Робота на даному рівні виконується над кадрами, чи так званими «фреймами»(frame). На даному рівні відсутні будь-які ip-адреси, прилади ідентифікують отримувача та відправника тільки по MAC-адресі і передають кадри між ними. Такі прилади, як правило, називають комутаторами, іноді уточнюючи, що це комутатор другого рівня, чи L2 комутатор[15].

Пристрої третього рівня(L3) – працюють на мережевому рівні, котрий призначений для визначення шляху передачі даних. Таке обладнання розуміє, що таке ip-адреса приладів. Обладнання даного тип визначає найкоротші маршрути для транспортування даних, використовуючи алгоритм Дейкстри. Даний алгоритм, відкритий нідерландським науковцем, покликаний знаходити найкоротший шлях від однієї вершини графа до всіх інших вершин. Даний алгоритм знайшов своє місце у протоколі OSPF, що зав'язаний на знаходженні найкоротшого шляху.

Пристрої даного рівня відповідають за встанолення різного типу з’єднань(Наприклад, PPPoE та його аналоги). Даний тип обладнання зазвичай називають маршрутизаторами, хоча іноді його називають і комутатором третього рівня чи L3 комутатором.

Пристрої четвертого рівня(L4) – відповідають за забезпечення надійності передачі даних. Це, так звані «передові» комутатори, що на основі інформації, отриманої з заголовку пакету, розуміють приналежність трафіку різним додаткам та можуть приймати рішення щодо перенаправлення такого трафіку на основі даної інформації. Назва для даного типу обладнання конкретно визначена не була, так їх іноді називають «інтелектуальними» комутаторами чи L4 комутаторами[33].

В більшості випадків організації мереж інтернет провайдерами застосовуються переважно комутатори Другого та Третього рівнів. У дрібних провайдерів також застосування знаходить обладнання Першого рівня. Нижче приведено для чого даний тип обладнання застосований:

Комутатор другого рівня покликаний для з'єднання декількох пристроїв локальної обчислюваної мережі(LAN) чи декількох сегментів даної мережі. L2 комутатор оброблює і реєструє MAC-адреси фреймів, що поступають, виконує фізичну адресацію та керування потоком даних (застосування технологій VLAN – Virtual Local Area Network, мультикаст фільтрування, QoS – набір методів для керування ресурсами пакетних мереж)

Комутатори третього рівня чи L3 комутатори фактично є маршрутизаторами, що реалізують механізми маршрутизації(логічна адресація і обирання шляху доставки даних(даних) з використанням протоколів маршрутизації (RIPv1 та RIPv2, OSPF, BGP, проприетарні протоколи маршрутизації)) не з використанням програмного забезпечення пристроїв, а за допомогою спеціалізованих апаратних засобів(мікросхем). В результаті прилад стає менш гнучким, оскільки для модернізації засобів реалізації застосовуємих протоколів маршрутизації потребується заміна апаратного забезпечення, а не просто оновлення програмного. Прикладом можуть слугувати пристрої, в котрих підтримка різноманітних протоколів маршрутизації виконується різних моделях. Традиційно комутатори третього рівня використовувалися у локальних та територіальних мережах

для забезпечення швидкодії передачі даних в інтересах великої кількості підключених до них приладів у відмінності від маршрутизаторів, традиційно виконуючих низькошвидкісний доступ до розподіленної мережі (WAN – World Area Network)[30]. Як правило, сьогодні маршрутизатори застосовуються при організації зовнішнього зв'язку між різними точками, такими як центри керування мережами, диспетчерськими центрами, простими користувачами, для забезпечення зв'язку між маршрутизаторами та іншою периферією.

У великих і досить розвинених провайдерів інтернет-доступу у переважній більшості застосовуються комутатори другого та третього рівнів, через свій функціонал та більшу надійність, з можливістю здійснення контролю за станом зв'язку. Але у дрібних інтернет-провайдерів, так званих «локальних», може не вистачати коштів на придбання обладнання такого типу, чи спеціалістів для його обслуговування. Тому провайдери такого типу надають перевагу підключенню абонентів через більш дешеві – що в лексиці даної галузі іноді можуть називатися «тупарями» (через те що даний тип комутаторів не має можливостей до керування трафіком, що проходить), що просто збирають інформацію про підключені пристрої (переважно їх MAC-адреси) та адресує їх до керованого комутатора другого рівня. Такі прилади відрізняються своєю дешевизною у порівнянні із комутаторами другого чи третього рівня. Також має місце зазначити, що даний тип організації мережі та підключення абонентів дозволяє таким дрібним провайдерам «розкрутитися», набрати клієнтську базу та отримати необхідний дохід для покращення обслуговування та режиму роботи мережі, що була ним організована і відмовитися від використання даного типу приладів та обладнання, якщо не повністю, то хоча б частково.

2. ОГЛЯД ТОПОЛОГІЙ ТА АНАЛІЗ ПРОБЛЕМ, ЩО ВИНИКАЮТЬ.

Для детального вирішення проблеми, що пов’язана з організацією комп’ютерної мережі, спочатку необхідно зазначити перелік визначних технологій та функцій, що покликані вирішити вже відомі проблеми та забезпечити якнайякісніше підключення:

2.1. Топології мереж

Не останню роль в організації мереж займає її топологія. Під топологією (компонуванням, конфігурацією, структурою) комп'ютерної мережі звичайно розуміється фізичне розташування комп'ютерів мережі один щодо іншого та спосіб їх з'єднання лініями зв'язку. Важливо відзначити, що поняття топології ставиться, насамперед, до локальних мереж, у яких структуру зв'язків можна легко простежити. У глобальних мережах структура зв'язків звичайно схована від користувачів і не надто важлива, тому що кожний сеанс зв'язку може виконуватися по своєму власному шляху.

Топологія комп'ютерної мережі відображає структуру зв'язків між її основними функціональними елементами. В залежності від компонентів, що розглядаються, розрізняють фізичну і логічну структури локальних мереж. Фізична структура визначає топологію фізичних з'єднань між комп'ютерами. Логічна структура визначає логічну організацію взаємодії комп'ютерів між собою. Доповнюючи одна одну, фізична та логічна структури дають найповніше уявлення про комп'ютерну мережу.

Топологія мережі спричиняється її характеристиками. Зокрема, вибір тієї або іншої топології впливає на:

- склад необхідного мережного встаткування;
- характеристики мережного встаткування;
- можливості розширення мережі;
- спосіб керування мережею.

Щоб спільно використати ресурси або виконувати інші мережні завдання, комп'ютери повинні бути підключені один до одного. Для цієї мети в більшості випадків використається кабель (рідше — бездротові мережі — інфрачервоне встаткування Input/Output). Однак, просто підключити комп'ютер до кабелю, що з'єднує інші комп'ютери, недостатньо. Різні типи кабелів у сполученні з різними мережевими платами, мережними операційними системами й іншими компонентами вимагають і різного взаєморозташування комп'ютерів[1].

Кожна топологія мережі накладає ряд умов. Наприклад, вона може диктувати не тільки тип кабелю але й спосіб його прокладки.

Існує безліч способів з'єднання мережевих пристроїв. Виділяють 3 базових топології[1]:

- шина (bus)
- зірка (star)
- кільце (ring)

І додаткові (похідні):

- подвійне кільце
- сотова топологія
- решітка
- дерево
- Fat Tree
- сніжинка
- повнозв'язна

Додаткові способи є комбінаціями базових. У загальному випадку такі топології називаються змішаними або гібридними, але деякі з них мають власні назви, наприклад «Дерево»[34].

Топологія мережі визначає не тільки фізичне розташування комп'ютерів, але, що набагато важливіше, характер зв'язків між ними,

особливості поширення сигналів мережею. Саме характер зв'язків визначає ступінь відмовостійкості мережі, необхідну складність мережної апаратури, найбільш підходящий метод керування обміном, можливі типи середовищ передачі (каналів зв'язку), припустимий розмір мережі (довжина ліній зв'язку й кількість абонентів), необхідність електричного узгодження й багато чого іншого.

Коли в літературі згадується про топологію мережі, то можуть мати на увазі чотири зовсім різних поняття, що ставляться до різних рівнів мережної архітектури:

1. Фізична топологія (тобто схема розташування комп'ютерів і прокладки кабелів). У цьому змісті, наприклад, пасивна зірка нічим не відрізняється від активної зірки, тому її нерідко називають просто «зіркою».

2. Логічна топологія (тобто структура зв'язків, характер поширення сигналів мережею). Це, напевно, найправильніше визначення топології.

3. Топологія керування обміном (тобто принцип і послідовність передачі права на захват мережі між окремими комп'ютерами).

4. Інформаційна топологія (тобто напрямок потоків інформації, переданої мережею).

Найпоширеніші прості топології[1]:

- Топологія шини

В цьому випадку комп'ютери з'єднуються один з одним коаксіальним кабелем. Інформація, що передається від одного комп'ютера мережі іншому, розповсюджується, як правило, в обидві сторони. Основними перевагами такої схеми є дешевизна й простота розводки кабелю приміщеннями, можливість майже миттєвого широкомовного звертання до всіх станцій мережі. Головний недолік спільної шини полягає в її низькій надійності: будь-який дефект кабелю чи якого-небудь із численних роз'ємів повністю паралізує всю мережу. Іншим недоліком спільної шини є її невисока продуктивність, так як при такому способі з'єднання в кожний момент часу

тільки один комп'ютер може передавати дані в мережу. Тому пропускна здатність каналу зв'язку завжди поділяється тут між усіма станціями мережі.

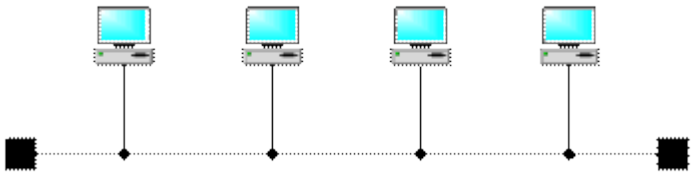


Рисунок 2.1 - Мережна топологія «шина»

- Кільцева топологія

В мережах із кільцевою конфігурацією дані передаються по кільцю від одного комп'ютера до іншого, як правило, в одному напрямку (рис. 1d). Це мережева топологія, в якій кожна станція має точно два зв'язки з іншими станціями. Якщо комп'ютер розпізнає дані як «свої», то він копіює їх у свій внутрішній буфер. Оскільки у випадку виходу з ладу мережевого адаптера будь-якої станції переривається канал зв'язку між іншими станціями мережі, даний вид топології використовується як логічна топологія.

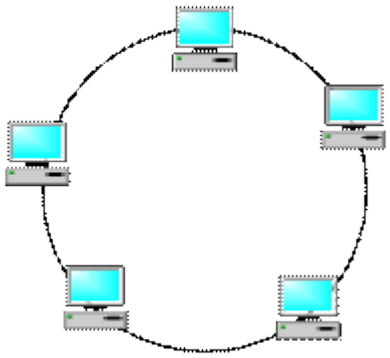


Рисунок 2.2 - Мережна топологія «кільце»

- Топологія зірка

це єдина топологія мережі з явно виділеним центром, до якого підключаються всі інші абоненти. Обмін інформацією йде винятково через центральний комп'ютер, на який лягає більше навантаження, тому нічим

іншим, крім мережі, він, як правило, займатися не може. Зрозуміло, що мережне устаткування центрального абонента повинно бути істотно складнішим, чим устаткування периферійних абонентів. Про рівноправність всіх абонентів (як у шині) у цьому випадку говорити не доводиться. Звичайно центральний комп'ютер найпотужніший, саме на нього покладають всі функції по керуванню обміном. Ніякі конфлікти в мережі з топологією зірка в принципі неможливі, тому що керування повністю централізоване[32].

Якщо говорити про стійкість зірки до відмов комп'ютерів, то вихід з ладу периферійного комп'ютера або його мережного встаткування ніяк не відбивається на функціонуванні мережі, зате будь-яка відмова центрального комп'ютера робить мережу повністю непрацездатною. У зв'язку із цим повинні прийматися спеціальні заходи щодо підвищення надійності центрального комп'ютера і його мережної апаратури.

Обрив кабелю або коротке замикання в ньому при топології зірка порушує обмін тільки з одним комп'ютером, а всі інші комп'ютери можуть нормально продовжувати роботу.

На відміну від шини, у зірці на кожній лінії зв'язку перебувають тільки два абоненти: центральний й один з периферійних. Найчастіше для їхнього з'єднання використовується дві лінії зв'язку, кожна з яких передає інформацію в одному напрямку, тобто на кожній лінії зв'язку є тільки один приймач й один передавач. Це так звана передача точка-точка. Все це істотно спрощує мережне встаткування в порівнянні із шиною й рятує від необхідності застосування додаткових, зовнішніх термінаторів[35].

Велика перевага зірки (як активної, так і пасивної) полягає в тому, що всі точки підключення зібрані в одному місці. Це дозволяє легко контролювати роботу мережі, локалізувати несправності шляхом простого відключення від центра тих або інших абонентів (що неможливо, наприклад, у випадку шинної топології), а також обмежувати доступ сторонніх осіб до життєво важливих для мережі точок підключення. До периферійного

абонента у випадку зірки може підходити як один кабель (по якому йде передача в обох напрямках), так і два (кожний кабель передає в одному із двох зустрічних напрямків), причому останнє зустрічається набагато частіше.

Загальним недоліком для всіх топологій типу зірка (як активної, так і пасивної) є значно більша, ніж при інших топологіях, витрата кабелю. Наприклад, якщо комп'ютери розташовані в одну лінію, то при виборі топології зірка знадобиться в кілька разів більше кабелю, ніж при топології шина[31]. Це істотно впливає на вартість мережі в цілому й помітно ускладнює прокладку кабелю.

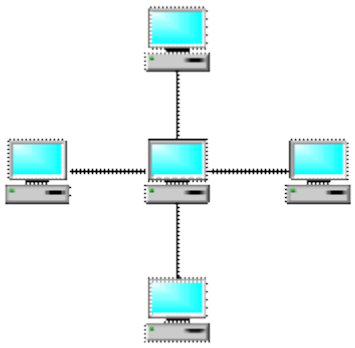


Рисунок 2.3 - Мережна топологія «зірка»

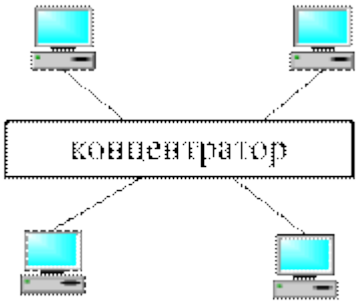


Рисунок - Топологія «пасивна зірка»

- Топологія дерева

Ця мережева топологія з чисто топологічної точки зору схожа на зіркову, в якій окремі периферійні мережеві пристрої можуть передавати до або приймати від тільки одного іншого мережевого пристрою в напрямку до центрального мережевого пристрою (рис. 1e). Як і в класичній зірковій топології, окремі мережеві пристрої можуть бути ізольовані від мережі внаслідок ліквідації одного зв'язку (гілки), наприклад, внаслідок аварії на лінії. У мережі з топологією дерева існує один виділений мережевий пристрій, який є коренем дерева[38].

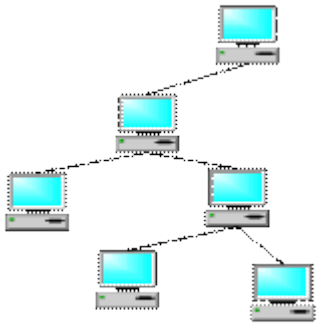


Рисунок 2.5 - Топологія «активне дерево»

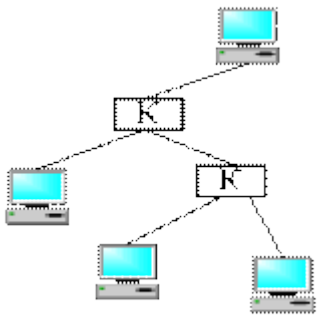


Рисунок 2.6 - Топологія «пасивне дерево». К – концентратори

- Топологія сітки

Цей вид топології дістають із топології повного з'єднання шляхом видалення деяких можливих зв'язків (рис. 1f). Це мережева топологія, в якій існують щонайменше два комп'ютери з двома або більше шляхами між ними

- Змішана (гібридна) топологія

Це поєднання двох або більшої кількості мережевих топологій (рис. 1g). Можна навести приклади, коли дві об'єднані основні мережеві топології не змінюють характеру топології мережі і тому не створюють гібридної мережі. Наприклад, сполучення мереж із топологією дерева дає мережу з такою ж топологією. Тому гібридна топологія мережі виникає тільки тоді, коли сполучені дві мережі з основними топологіями дають у результаті мережу, топологія якої не відповідає жодному з означень основних топологій. Наприклад, дві мережі із зірковою топологією при об'єднанні утворюють мережу з гібридною топологією. Гібридна топологія мережі виникає також при сполученні мереж із різними видами топологій.

- Топологія подвійного кільця

Мережами з такою конфігурацією є мережі FDDI. Вони відрізняються вбудованою надлишковістю, яка забезпечує захист від системних відмов: основне кільце служить для передавання даних, а допоміжне кільце — для передавання управляючих сигналів. Існує можливість передавання даних по обох кільцях у протилежних напрямках у випадку відсутності обривів кабелю. Якщо ж трапляється обрив кабелю або одна зі станцій виходить із ладу основне кільце об'єднується з допоміжним, знову утворюючи єдине кільце. Цей режим роботи мережі називається завертанням кілець.

- Лінійна (ланцюгова) топологія

Це топологія, у якій кожний комп'ютер з'єднаний із попереднім та наступним відносно себе (рис. 1i). Виникає з кільцевої при видаленні однієї гілки. Часом трактується як ідентично до шини.

- Повнозв'язна топологія

Повнозв'язна топологія містить n*(n-1)/2 каналів зв'язку, де n — кількість вузлів. Мережі з повнозв'язною топологією відрізняються високою надійністю, оперативністю і можливістю прихованої передачі. Однак їх

створення потребує великих вкладень. Ця топологія властива системам зв'язку на геостаціонарних орбітах.

2.2. Vlan

VLAN (Virtual Local Area Network)[5] – група пристроїв, що мають можливість взаємодіяти між собою безпосередньо на канальному рівні, при цьому вони можуть бути підключені до різних мережевих комутаторів. Та навпаки, прилади, що знаходяться у різних VLAN не ідентифікуються один одним на канальному рівні, навіть якщо вони підключені до одного комутатору. Такому разі, зв’язок між цим обладнанням буде можливим тільки починаючи з мережевого рівня.

В сучасних мережах VLAN потрібен для:

- гнучкого розділення обладнання на групи;

Як правило, одному VLAN відповідає одна підмережа. Пристрої, що знаходяться у різних VLAN, будуть знаходитися у різних підмережах. Але в той самий час, VLAN не прив’язаний до фізичного місцезнаходження обладнання і саме тому, обладнання що фізично знаходиться досить далеко одне від одного може знаходитися в одному VLAN незалежно від місцезнаходження.

- Зменшення широкомовного трафіку в мережі;

Фактично, один VLAN це окремий широкомовний домен. Наприклад, комутатор – пристрій другого рівня – всі порти на комутаторі з одним VLAN знаходяться в одному широкомовному домені. Створення додаткових VLAN призведе до розділення комутатора на декілька широкомовних доменів. Якщо один і той самий VLAN буде налаштований на різних комутаторах, порти що знаходяться в одному VLAN будуть утворювати один широкомовний домен.

- Підвищення безпеки та керованості мережі.

Коли мережа розбита на VLAN, зпрощується задача застосування політик та правил безпеки. З VLAN політики можна застосовувати до цілих підмереж, а не окремих пристроїв та обладнання.

Окрім того, перехід з одного VLAN в інший потребує такої передумови, як проходження трафіку через пристрій третього рівня на котрому, зазвичай, і застосовуються політики, що дозволяють чи забороняють доступ з одного VLAN до іншого.

Комп'ютер при відправленні трафіку в мережу навіть не здогадується про те, в якому VLAN він знаходиться. Про це думає комутатор: він знає, що комп'ютер, підключений до певного порту, знаходиться у відповідному даному порту VLAN. Трафік, що поступає на порт визначеного VLAN нічим не відрізняється від трафіку, що поступає на інший VLAN. Таким чином вдалося з'ясувати, що інформації про приналежність трафіку визначеному VLAN у самому трафіку немає.

Однак, якщо через порт може пройти трафік різних VLAN, комутатор повинен його розрізняти. Для цього кожний кадр(або «фрейм») трафіку повинен бути поміченим особливим способом. Примітка повинна повідомлять про те, котрому з налаштованих VLAN належить трафік що проходить.

Найбільш розповсюджений зараз спосіб робити таку помітку описаний у відкритому стандарті IEEE 802.1Q. Існують схожі за принципом дії протоколи, що вирішують схожі задачі, наприклад протокол ISL від Cisco Systems, але вони не здобули такої популярності.

IEEE 802.1Q або VLAN Tagging — мережевий стандарт, запропонований робочою групою IEEE 802.1, для сумісного використання фізичної мережі Ethernet багатьма логічними (віртуальними) мережами.

IEEE 802.1Q визначає віртуальну мережу (virtual LAN або VLAN) відповідно до моделі комутації пакетів на рівні MAC та протоколу IEEE 802.1D (spanning tree protocol). Протокол забезпечує обмін даними між об'єктами

мережі, підключеними до різних VLAN'ів, крізь комутатори мережевого рівня (Network Layer/Layer 3) або маршрутизатори. Shortest Path Bridging (IEEE 802.1aq) включається в IEEE 802.1Q-2014.

Формат кадру

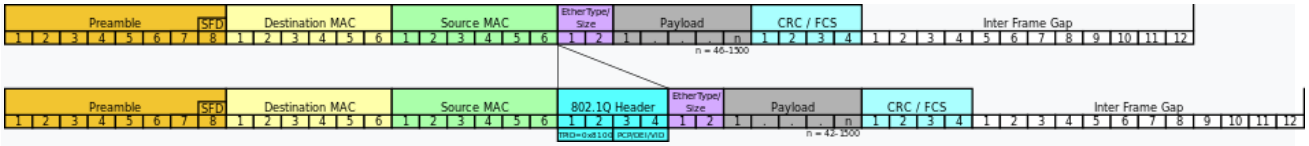


Рисунок 2.7 - Додавання 802.1Q Tag в кадр Ethernet

Насправді 802.1Q не енкапсулює в собі початковий кадр. Замість цього всередину Ethernet II frames додається 32-бітне поле між MAC'ом передаючої сторони й полями типу та розміру кадру (EtherType/Length) оригінального кадру. Два байти використовуються як ідентифікатор протоколу тегування (tag protocol identifier — TPID), інші два байти — управляюча інформація (tag control information — TCI). Поле TCI містить в собі поля PCP, CFI та VID.

1	3		1
6 біт	**біта**	**біт**	**2 біт**
T	P		V
PID	CP	FI	ID

Рисунок 2.8 - Розміри сегментів поля TCI

- Ідентифікатор протоколу тегування (Tag Protocol Identifier, TPID): 16-бітне поле, що містить значення 0x8100, є ідентифікатором IEEE 802.1Q кадру з встановленим tag'ом. Це поле розміщено в тій самій позиції Ethernet-кадру, що і EtherType/Size в звичайному кадрі і використовується для розрізнення кадрів з додатковим тегом (tagged), і звичайних (untagged) кадрів.

- Код пріорітету (Priority Code Point, PCP): 3-бітне поле, що інтерпретується згідно зі стандартом IEEE 802.1p[20]. Вказує пріоритет кадру. Допустимі значення від 0 (у разі можливості) до 7 (найвищий); 1 — найнижчий пріоритет. Ці значення застосовуються для пріоритезації трафіку (передача голосу, відео, даних, та ін.).
- Ідентифікатор канонічного формату (Canonical Format Indicator, CFI): а 1-бітне поле. Якщо це поле встановлено в 1, MAC-адреса передається не в канонічному форматі. Значення 0 свідчить про те, що MAC-адреса передається відповідно до канонічного формату. Завжди встановлений в 0 для комутаторів Ethernet. CFI використовується для забезпечення сумісності між мережами Ethernet та Token Ring. Якщо кадр з CFI встановленим в 1 потрапляє в порт Ethernet, він не має потрапити в порт без тегування.
- Ідентифікатор VLAN (VLAN Identifier, VID): 12-бітний ідентифікатор VLAN, до якого належить кадр. Значення 0 вказує на те, що кадр не належить до жодного VLAN; у цьому разі тег 802.1Q вказує тільки пріоритет. Значення 0xFFF зарезервовано. Решта значень можуть використовуватись як ідентифікатори VLAN'ів. Всього їх може бути до 4094. Зазвичай на комутаторах VLAN 1 є зарезервованим. Також у багатьох комутаторів VLAN 1 — це так званий Default VLAN (або Native VLAN), що за замовчуванням використовується для нетегованих кадрів. Ще у деяких комутаторів зарезервованим є VLAN 4094[25].

2.3. Spanning Tree Protocol та його специфікації

Spanning Tree Protocol (STP)[14] (протокол кістякового дерева) — мережевий протокол, що працює на другому рівні моделі OSI. Заснований на однойменному алгоритмі, розробником якого є Радья Перлман.

Основним завданням STP є приведення мережі Ethernet з множинними зв'язками до деревоподібної топології (кістякове дерево), що виключає

передачу пакетів по колу. Відбувається це шляхом автоматичного блокування надлишкових в цей час зв'язків для повної зв'язності портів. Протокол описаний в стандарті IEEE 802.1D.

Принцип дії полягаэ у тому, що у мережі вибирається один кореневий міст (англ. Root Bridge). Далі кожен, відмінний від кореневого, міст прораховує найкоротший шлях до кореневого порту. Відповідний порт називається кореневим портом (англ. Root Port). У будь-якого не кореневого комутатора може бути тільки один кореневий порт.

Після цього для кожного сегмента мережі прораховується найкоротший шлях до кореневого порту. Міст, через який проходить цей шлях, стає призначеним для цієї мережі (англ. Designated Bridge). Безпосередньо підключений до мережі порт моста — призначеним портом.

Далі на всіх мостах блокуються всі порти, які не є кореневими та призначеними. У підсумку виходить деревоподібна структура (математичний граф) з вершиною у вигляді кореневого комутатора.

Основні поняття та визначення, що допоможуть у розумінні принципу дії даного протоколу:

- Pathcost- вартість лінка в STP;
- Bpduguard- BPDU-фільтр;
- Rootguard- root-фільтр;
- Bridge ID= Bridge priority + MAC;
- Bridge priority= vlan xxx + 32 768 (default cost);
- Cost- «вартість портів». За замовчуванням дорівнює 32 768 (2 в 15 степені);
- Hello BPDU пакет= root ID + bridge ID + cost;
- Root port(кореневий порт) — це порт, який має найкоротшу відстань до будь-якого порту кореневого комутатора.
- Designated port(призначений порт) — це порт, який має найкоротшу відстань від призначеного комутатора до кореневого комутатора.

Швидкість передачі та вартість шляху

Таблиця знизу показує вартість інтерфейсу в залежності від швидкості передачі.

Швидкість передачі	Вартість (802.1D-1998)	Вартість (802.1t-2001)
4 Mbit/s	250	5000000
10 Mbit/s	100	2000000
16 Mbit/s	62	1250000
100 Mbit/s	19	200000
1 Gbit/s	4	20000
2 Gbit/s	3	10000
10 Gbit/s	2	2000

Рисунок 2.9 - Таблиця співвідношення швидкості та вартості інтерфейсу

Важливі правила

Кореневим (root-овим) комутатором призначається комутатор з найнижчим BID (Bridge ID)

Можливі випадки, коли пріоритет у двох і більше комутаторів буде однаковий, тоді вибір кореневого комутатора (root-а) буде відбувається на підставі MAC-адреси комутатора, де кореневим (root) комутатором стане комутатор з найменшою MAC-адресою.

Комутатори, за замовчуванням, не вимірюють стан мережі, а мають заздалегідь прописані налаштування.

Кожен порт має свою вартість (cost) з'єднання, встановлену або на заводі-виробнику (за замовчуванням), або вручну.

Алгоритм дії STP (Spanning Tree Protocol)

1. Після включення комутаторів в мережу, за замовчуванням кожен Комутатор вважає себе кореневим (root).
2. Потім комутатор починає посилати по всіх портах конфігураційні Hello BPDU пакети раз на 2 секунди.
3. Виходячи з даних Hello BPDU пакетів, той чи інший комутатор набуває статусу root, тобто кореня.
4. Після цього всі порти крім root port і designated port блокуються.
5. Відбувається посилка Hello-пакетів раз на 2 секунди, з метою перешкоджання появи петель в мережі.

Портам можуть бути присвоєні такі типи(они можуть перебвати у таких станах в залежності від налаштуваннь):

- Root Port
- Designated Port
- Non-designated Port
- Disabled Port

З перебігом часу даний протокол здобув продовження у своїх модифікаціях та специфікаціях, таких як:

- Rapid Spanning Tree Protocol (RSTP)

Rapid STP (RSTP) характеризується значними вдосконаленнями STP, серед яких зменшення часу збіжності і вища стійкість. Описаний в стандарті IEEE 802.1w (згодом включено до 802.1D-2004).

- Per-VLAN Spanning Tree Protocol (PVSTP)

Per-VLAN STP (PVSTP) відповідно до назви розширює функціонал STP для використання VLAN. У рамках даного протоколу в кожному VLAN працює окремий екземпляр STP. Є пропрієтарним розширенням Cisco, згодом став з незначними обмеженнями підтримуватися іншими виробниками (Juniper, Extreme Networks). Споконвічно протокол PVST працював тільки через ISL-транки, потім було розроблено розширення PVST +, яке дозволяло працювати через набагато поширеніші 802.1Q-транки[23].

Існують реалізації, об'єднуючі властивості PVST + і RSTP, оскільки ці розширення зачіпають незалежні частини протоколу, в результаті виходить (в термінології Cisco) rapid-pvst.

PVST не сумісно з MSTP і при одночасній роботі пристроїв Cisco з цими протоколами викликає проблеми в мережі, зокрема, відключення downlink'ового порту root'ового MSTP-пристрою.

Для блокування PVST на більшості мережевих пристроях інших виробників доводиться створювати MAC фільтр, оскільки в їх BPDU фільтрах пакети PVST невідомі і можуть проходити через ці пристрої навіть при відключених STP.

- Multiple Spanning Tree Protocol (MSTP)[13]

Multiple STP (MSTP) є найсучаснішою стандартною реалізацією STP, що враховує всі переваги і недоліки попередніх рішень. Описана в стандарті IEEE 802.1s (згодом включено до 802.1Q-2003). На відміну від PVST +, в якому число примірників сполучного дерева (spanning tree) дорівнює кількості віртуальних мереж, MSTP передбачає конфігурування необхідної кількості примірників незалежно від числа віртуальних мереж (VLAN) на комутаторі. В один примірник MST можуть входити декілька віртуальних мереж. Проте, всі комутатори, які беруть участь у MST, повинні мати однаково сконфігуровані групи VLAN (MST instances), що обмежує гнучкість при зміні конфігурації мережі.

- Shortest Path Bridging

Shortest Path Bridging (SPB)або IEEE 802.1aq долає обмеження блокування.

Shortest Path Bridging є сучасною альтернативою старому сімейству протоколів Spanning Tree (IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP), які вміють використовувати тільки один маршрут пересилання трафіку до кореневого комутатора (root bridge) і блокують будь-які альтернативні шляхи, оскільки це може призвести до утворення мережевої

петлі на 2-му рівні. SPB активно використовує всі наявні маршрути пересилання з однаковою вартістю(equal cost multipathing), і дозволяє будувати більш масштабні топології на 2-му рівні (до 16 мільйонів сервісів, що набагато більше традиційного обмеження IEEE 802.1Q на 4,096 віртуальних мереж VLANs). Він так само має дуже швидкий час збіжності, і збільшує ефективність багатозв'язних (Mesh мережі) топологій шляхом використання більшої смуги пропускання між усіма пристроями і більшою відмовостійкістю, оскільки трафік використовує і балансується між усіма доступними шляхами пересилання в багатозв'язній Mesh мережі. Для підвищеної надійності рівень доступу SPB може використовувати технології агрегації ліній, такі як стандарт IEEE 802.1AX або пропрієтарні реалізації механізмів MC-LAG.

SPB дозволяє розгортати логічні мережі Ethernet поверх фізичної Ethernet інфраструктури, використовуючи протокол станів сполук (link state protocol) для оголошення фізичної топології, так і членства в логічних/віртуальних мережах. Пакети інкапсулюються на кордоні або у кадр MAC-in-MAC IEEE 802.1ah або у теговані фрейми IEEE 802.1Q/IEEE 802.1ad і передаються тільки іншим членам тієї ж логічної мережі. Підтримуються одноадресне, багатоадресне, і широкомовне пересилання і вся маршрутизація здійснюється за симетричними (в прямому і зворотному напрямках) найкоротшими шляхами. Керування (control plane) базується на протоколі Intermediate System to Intermediate System (IS-IS), і використовує невелику кількість розширень, визначених у стандарті RFC 6329.

2.4.flowcontrol

Управлі́ння пото́ком переда́чі да́них (англ. Flow Control) - в комп'ютерних мережах, механізм, який пригальмовує передавач даних при неготовності приймача.

Існує два підходи до вирішення цієї проблеми[6]:

▪ Керування потоком зі зворотнім зв’язком (англ. feedback-based flow control)

коли отримувач відсилає передавачу інформацію що дозволяє йому продовжити передачу, чи повідомляє як загалом йдуть справи.

▪ Керування потоком з обмеженням(англ. rate-based flow control)

коли передавачі обмежуються в швидкості передачі даних, а зворотній зв’язок з приймачем відсутній.

Розрізняють три основних способи вирішення цієї проблеми:

- Апаратний, при якому сигнали «готовий /зайнятий» передаються по окремих фізичних лініях зв'язку. Найбільш відома така реалізація в інтерфейсі RS-232.
- Програмний, при якому програмний прапорець «готовий /зайнятий» зводиться і скидається вставкою в потік даних спеціальної унікальної послідовності (XOn / XOff). Застосовується в програмних драйверах інтерфейсу RS-232 як альтернатива апаратному контролю потоку у випадках неповного з'єднувального кабелю.
- Протокольний, при якому програмний прапорець «готовий /зайнятий» зводиться і скидається спеціальними угодами в рамках протоколу обміну даними. На сьогодні є практично єдиним застосовуваним способом контролю потоку. Найбільш відомий приклад - реалізація контролю потоку в протоколі TCP методом ковзного вікна.

2.5. Speed and Duplex

За замовчуванням, кожен порт налаштований таким чином, що пристрій сам визначає які налаштування на якому порту використовувати, яку швидкість обирати, який режим передачі даних обирати. Така технологія називається «Auto-negotiation» чи «Автоузгодження»(Автовизначення).

Також ці параметри є можливість задати «вручну», на кожному порту пристрою.

Комутатори визначають автоматично швидкість між мережевими пристроями(наприклад між портом комутатору та мережевою картою комп'ютера), використовуючи деякі методи. Комутатори використовують для визначення швидкості Fast Link Pulse(FLP), це деякий електронний імпульс, по котрому прилади можуть зрозуміти на котрих оптимальних швидкостях може встановлюватися з'єднання між даними сітьовими пристроями.

Якщо швидкості виставлені вручну і вони співпадають, то прилади зможуть встановити з'єднання використовуючи електричні сигнали.

Якщо на комутаторі і на мережевому приладі комп'ютера, встановлені вручну швидкості і вони не співпадають, то з'єднання не буде встановлено.

Наприклад, так само трапляється й визначення режиму роботи з'єднання: half-duplex чи full-duplex.

Якщо обидка прилади працюють у режимі автовизначення і прилади можуть працювати у duplex режимі, то цей режим і встановиться.

Якщо на пристроях автоузгодження вимкнено, то режим буде присвоєно деяким параметром «за замовчуванням». Для 10 та 100 мегабітних інтерфейсів встановиться режим half-duplex, для 1000 мегабітних буде встановлено full-duplex.

Для відключення автовизначення дуплексності необхідно вручну вказати налаштування режиму.

Ethernet пристрої можуть працювати у режимі Full-Duplex тільки тоді, коли відсутні колізії у передаючій середі.

Колізії трапляються тільки там, де наявна середа передачі даних, що розділяється. Наприклад при топології шина чи при застосування такого пристрою як «хаб»(на сьогоднішній день хаби майже вийшли з використання).

Для боротьби з колізіями в таких мережах передачі даних використовується алгоритм, що називається CSMA/CD (Carrier Sense Multiple Access/ Collision Detection), що означає чисельний доступ з контролем носія та детекцією коллізій.

Коллізія це накладання сигналу, тобто коли одночасно декілька мережевих пристроїв починають передачу даних по середі що розділяється, два ці сигнали перетинаються, накладаються один на одного і утворюється коллізія(тобто дані спотворені і не несуть в собі ніякого корисного навантаження)

Даний алгоритм працює наступним чином:

- Пристрій, що бажає відправити кадр(фрейм) спочатку слухає, чи вільна лінія зв'язку.
- Коли лінія зв'язку не зайнята, даний пристрій починає відправляти кадри(фрейми) в Ethernet.
- Пристрій «чує», що колізія не відбувається, це означає що все добре.
- Якщо за збігом обставин, колізія все ж таки трапилася – а така ситуація може скластися через те, що на етапі прослуховування лінії на наявність вільного каналу, декілька пристроїв одночасно відправили кадри, через це і відбулося накладання одного кадру на інший. Як тільки приладам, що відправили кадри(«фрейми») стає відомо, що трапилася колізія, вони посилають так званий jam signal, що сигналізує іншим пристроям у мережі про те, що зараз передача даних неможлива, через те що виникла колізія і зараз необхідно зачекати.

- Після jam сигналу, у кожного пристрою, що відправляє дані випадковим чином визначається деякий час, що можна назвати «часом простою», коли пристрій не може відправляти жодних даних по мережі.

- Після того, як час, відведений таймером, добігає кінця, алгоритм знову починається з першого кроку.

2.6. Опис відомих проблем

Спираючись на власний досвід у роботі з мережевим обладнанням, та маючи доступ до спостережень своїх співробітників у цій справі, було виявлено проблеми такого характеру та видів:

Проблеми фізичного характеру:

- Проблема обрання топології підключення.
- Належна обжимка кабелів(пряма обжимка, кросс-обжимка).
- Обрання обладнання та його виробників.
- Належна організація підключення(обирання тип кабелів, якими підключається обладнання).
- Відсутність підключення до DHCP-серверу(при динамічних налаштуваннях підключення).
- Не реалізовані можливості для забезпечення безперебійного підключення(генератори, UPS-и та інші елементи живлення та забезпечення безперебійного живлення).

Проблеми логічного (програмного характеру):

- Налаштування не співпадають з сторони користувача/провайдера.
- Конфігурація порту не відповідає заданим стандартам.
- Заблоковані порти, за якими відбуваються звернення до інтернету(наприклад 80 чи 8080).
- Неправильно налаштоване підключення(наприклад при статичних налаштуваннях не прописані дані для маршрутизації, при динамічній – не налаштований DHCP -сервер).
- Програмно відключений доступ користувачеві до інтернету.

- Не налаштовані резервні шляхи для підключення або повна їх відсутність.

Вирішення даних проблем досить просте – достатньо перед тим, як братися за налаштовування підключення та обладнання, ознайомитися з його специфікацією, принципами його роботи, технологіями та методами, що використовуються при його роботі, або які були вшиті у програмну оболонку обладнання.

Якщо підходити до даного питання з розумом та розумінням, то можна отримати цілком робочу, адекватну модель комп'ютерної мережі, що може не втратити роботоздатність навіть в умовах відсутності електроживлення по місцю розміщення обладнання, що призведе до забезпечення безперебійного доступу до інтернет мережі, якщо у користувача буде чим його використовувати в умовах відсутності електромережі.

Також є необхідність зазначити перелік особливостей та проблем, пов'язаних зі специфікацією використовуваного обладнання:

Комутатори виробництва D-link:

- Мають можливість працювати з прив'язками, що дозволяють обмежувати проходження трафіку через задані порти чи порт.
- Є як оптичні версії комутаторів від даного виробника, так і мідні.
- У наявності також є функція блокування фізичних адрес, що дозволяє здійснювати жорсткий контроль за тим, що відбувається на портах, але зазвичай дана функція перешкоджає нормальному використанню доступу до інтернету.
- Прив'язки можуть бути створені як для роботи по статичним налаштуванням, так і по динамічним.
- Присутня деяка проблем з командами, оскільки одні й ті самі слова в командах, але у різних часах та однині/множині відносяться до абсолютно різних команд, що може ускладнити налаштування.

- Є можливість налаштовувати всі параметри портів однією командою, але якщо допустити помилку хоча б в одному місці даної команди, вона не буде виконана зовсім.

Комутатори виробництва ZTE[3]:

- Мають унікальну серед перерахованого обладнання функцію – налаштування ACL(Access Control List), що дозволяє виконувати досить тонке налаштування проходження трафіку через порт, на якому активовано задані правила ACL.
- Є досить корисна можливість перевіряти, як саме налаштований порт і які налаштування до нього застосовуються – динамічні чи статичні.
- Є можливість прописувати на порту статичну мак адресу, це буває корисно, коли фізична адреса від користувача надходить досить довго, чи не надходить через те, що їй необхідно пройти всі етапи верифікації та автентифікації.

Комутатори виробництва Linksys:

- Мають досить корисну можливість перевіряти, що саме отримує абонент: IP-адресу, його MAC, VLAN, час на який було видано дану IP-адресу та номер порту на який надходить дана інформація.
- Досить чутливі до погодних умов, траплялися випадки, коли при перевірці роботоспроможності портів, у грозу, на даному типі комутаторів частина з них ставала непридатна до використання, і їх надальше використання призводило до відмови цілого комутатора.
- Редагувати параметри speed та duplex на даному типі комутаторів досить складно через те, що для вимикання автоузгодження на порті необхідно знати окрему команду що його вимикає.
- Є можливість спостерігати за перебігом подій на таких комутаторах у режимі реального часу.

Комутатори виробництва BDCOM(OLT)[7]:

- Підключення на даному типі комутаторів реалізується посередництвом технології PON(Passive Optical Network) та додаткового обладнання, що називається ONU(Optical Network Unit)чи ONT(Optical Network Terminal), оскільки підключення проходить через оптично-волоконний кабель,
- ONU необхідні для конвертування світлового сигналу в електричний та подальшу його передачу до обладнання користувачів.
- Підключення поділяються на так звані «гілки» прив'язки до яких робляться по позиції гілки у нумерації портів
- Кожна ONU має бути підключена, зареєстрована і повинна отримати налаштування окремо. Якщо у файлах конфігурації будуть відсутні налаштування для відповідної ONU – вона не буде працювати належним чином.
- На деяких видах OLT(Optical Line Terminal) можна підключити більше аніж 64 ONU, але тільки 64 може бути зареєстровано та налаштовано на одній гілці. Інші не будуть працювати.
- Реалізована можливість перевіряти затухання оптичного сигналу від OLT до ONU та навпаки.

Комутатори виробництва Raisecom[4]:

- Можуть працювати як з мідним типом обладнання так із оптичним.
- Всі порти за замовченням налаштовані на швидкісне обмеження до 1ГБ/с (якщо це оптичний тип комутатора)
- Перевести порт з підключення 1ГБ/с до 100МБ/с досить складно через те, що для цього може знадобитися одна команда, що за це відповідає, але про неї мало хто знає.

Комутатори виробництва Foxgate:

- Коли даних комутаторів виявляється у кільці більше аніж сім – виникають проблеми з передачею даних між ними. Пакети починають втрачатися та відкидатися.

- Є можливість працювати з прив’язками, як на статичних налаштуваннях так і на динамічних.
- Можна отримувати основну інформацію про стан підключення на порту, використовуючи команду «sh interface brief 0/0/№-порту»(для портів після 24-го: 0/1/№-порту)
- Працюють з оптичними видами обладнання, для підключення через даний тип комутаторів потребується медіаконвертор, що буде налаштований на довжину та частоту хвилі, що задана виробником на комутаторі.

3. РОЗРОБКА КОМП'ЮТЕРНОЇ МЕРЕЖІ INTERNET-ПРОВАЙДЕРА

Спираючись на власні спостереження у роботі обладнання, було розроблено рішення, яке наочно демонструє як повинна працювати мережа, в якій ризик виникнення відомих проблем зведено до мінімуму.

Почати роботу зі створення комп'ютерної мережі було необхідно з етапу планування самої мережі. До роботи на даному етапі входять розрахунки розмірів мережі, виділяються VLAN-и, проводиться планування по виділеним підмережам, складається IP-план, виводиться таблиця щодо підключень по портам на обладнанні. Для більшого розуміння та читабельності кожному комутатору, маршрутизатору та кінцевому обладнанню було присвоєно індивідуальні імена, що покращують читабельність коду.

№VLAN	Имя VLAN	Примечание
1	default	not using
2	Managemen	For managing of devices
3	Servers	For Servers
4	Obolon	Link to Obolon
5	Pechersk	Link to Pechersk
6-100		Reserved
101	PTO	For PTO
102	FEO	FOR FEO
103	Accounting	FOR ACCOUNTING
104	Other	For Other Needs

Рисунок 3.1 - План на використання vlan-ів

Як видно з вищезазначеного рисунка, для потреб кожної окремої віртуальної мережі було створено окремий vlan, що дозволить зменшити навантаження на обладнання, посередництвом розмежування широкомовних доменів. Також це забезпечить значну можливість у підвищенні безпеки мережі, оскільки взаємодіяти між собою користувачам різних vlan-ах буде досить складно. Але для забезпечення доступності мережі для налаштовування та взаємодії між районами міста Києва, в якому було розгорнуто даного інтернет-провайдера, було налаштовано intervlan routing, що дозволяє здійснювати обмін даними між різними підмережами, організованими посередництвом vlan-ів.

Наступним кроком було сформовано таблицю ip-адрес, які будуть присвоєні різному мережевому обладнанні та інтерфейсам.

IP-адрес	Примечание	VLAN
172.16.0.0/16		
172.16.0.0/20	**Kyiv**	
172.16.0.0/24	**Servers**	3
172.16.0.1	Gateway	
172.16.0.2	Web	
172.16.0.3	File	
172.16.0.4	Mail	
172.16.0.5-172.16.0.254	Reserved	
172.16.1.0/24	**Managing**	2
172.16.1.1	Gateway	
172.16.1.2	kyiv-poznyaki-dsw1	
172.16.1.3	kyiv-poznyaki-asw1	
172.16.1.4	kyiv-poznyaki-asw2	
172.16.1.5	kyiv-poznyaki-asw3	
172.16.1.6	kyiv-darnytsya-asw1	
172.16.1.6-172.16.1.254	Зарезервировано	

Рисунок 3.2 - Ip-план на мережу для відділів інтернет-провайдера

172.16.2.0/24	**Point-to-Point Net**	
172.16.2.0/28	**Obolon**	
172.16.2.0/30	**Obolon-Dnipro Heroes**	4
172.16.2.1	Kyev-poznyaki-gw1	
172.16.2.2	obl-dnh-gw1	
172.16.2.4/30	**Obolon-Stalingrad Heroes**	
172.16.2.5	obl-dnh-gw1	
172.16.2.6	obl-stlh-gw1	
172.16.2.8-172.16.2.15	Reserved	
172.16.2.16/30	**Pechersk**	5
172.16.2.17	kyev-poznyaki-gw1	
172.16.2.18	pchr-boichyka-gw1	
172.16.2.20-172.16.2.254	reserved	

Рисунок 3.3 -IP-план на мережу для районів Києва

172.16.3.0/24	**PTO**	101
172.16.3.1	Gateway	
172.16.3.2-172.16.3.254	Users pool	
172.16.4.0/24	**FEO**	102
172.16.4.1	Gateway	
172.16.4.2-172.16.4.254	Users pool	
172.16.5.0/24	**Accounting**	103
172.16.5.1	Gateway	
172.16.5.2-172.16.5.254	Users pool	
172.16.6.0/24	**Other needs**	104
172.16.6.1	Gateway	
172.16.6.2-172.16.6.254	Users pool	
172.16.7.0- 172.16.15.254	Reserved	

Рисунок 3.4 - IP-план на відділи що працюють у мережі

172.16.16.0/21	**Obolon**	
172.16.16.0/24	**Dnipro Heroes**	
172.16.16.1	obl-dnh-gw1	
172.16.16.2	obl-dnh-dsw1	
172.16.16.20-172.16.16.254	Users	
172.16.17.0/24	**Stalingrad Heroes**	
172.16.17.1	obl-stlh-gw1	
172.16.17.20-172.16.17.254	Users	2
172.16.18.0-172.16.23.255	Reserved	
172.16.24.0/22	**Pechersk**	
172.16.24.0/24	**Boichyka**	
172.16.24.1	pchr-boichyka-gw1	
172.16.24.2	pchr-boichyka-dsw1	
172.16.24.2-172.16.24.254	Users	2
172.16.25.0-172.16.255.254	Reserved	

Рисунок 3.5 - IP-план на райони міста Києва

Як зазначено на рисунках від 3.2 до 3.5 - такі ip-адреси будуть використовуватися для налаштування зв'язку та підключення між обладнанням. Також на даних рисунках зазначено пул ip-адрес для користувачів, що будуть підключатися й надалі. Також слід звернути увагу на те, що цифрами після символу «/» зазначено яку маску підмережі матиме дана підмережа. Макса визначає, яку кількість хостів(з урахуванням зарезервованих широкомовних ip-адрес) матиме дана підмережа, а число, яким маска визначається вказує на те, скільки бітів(чи одиниць у бінарній системі зчислення) матиме дана маска. Так, наприклад, маска підмережі «/24» має вигляд : 255.255.255.0, що означає, що у даній підмережі може бути визначено 254 хости, без урахування зарезервованої широкомовної адреси.

172.16.x.1	Gateway
172.16.x.2-172.16.x.12	Network devices
172.16.x.13-172.16.x.24	Servers
172.16.x.25-172.16.x.220	Computers
172.16.x.221-172.16.x.254	Printers

Рисунок 3.6 - Регламент щодо використання IP-адрес у всіх підмережах інтернет-провайдера

Рисунок 3.6 наочно демонструє як і які ip-адреси будуть використовуватися і для чого будуть використовуватись зазначені адреси.

Згідно рисунку 3.7 можемо побачити що і куди буде підключено, через які порти, з використанням якого саме vlan-у, та до якої частини мережі належить той чи інший порт[34]. З даної таблиці можна виділити такі деталі:

- У назві обладнання виділена така інформація: регіон(місто або район), до чого саме належить дане облднання(район або вулиця) та тип обладнання(gw – gateway чи шлюз, маршрутизатор; dsw – distribution switch чи комутатор рівня надання послуг, куди підключається інше мережеве обладнання; asw – access switch чи комутатор доступу, куди підключаються кінцеві хости).
- Визначається у який порт(порти) буде виконано підключення, та тип порту. Так, наприклад FA0/24 – це порт під номером 24 типу fastethernet – тобто до 100 мбіт/с. А порт GI0/1 – gigabitethernet №1 – з обмеженням швидкості до 1Гбіт/с.
- Визначається що саме через цей порт буде підключене, визначається його назва, що була вказана у першому стовбці[46]. Також тут визначається формування так званих port-channel-ів(об’єднань декількох портів для підвищення пропускної здатності).

- У стовпці VLAN визначається який саме влан буде використовуватися на порту, якщо порт працюватиме у режимі access(куди підключаються кінцеві хости), чи перелік ланів, що будуть проходити через порт, якщо це буде режим trunk(посередництвом якого реалізується підключення між обладнанням, та передача кадрів з різними vlan-мітками).

Имя устройства	Порт	Название	VLAN	
			Access	Trunk
kyiv-poznyaki-gw1	FE0/1	UpLink		
	FE0/0	kyiv-poznyaki-dsw1		2,3,101,102,103,104
kyiv-poznyaki-dsw1	FE0/24	kyiv-poznyaki-gw1		
	GE1/1	kyiv-poznyaki-asw1		2,3
	GE1/2	kyiv-poznyaki-asw2		2,3
	FE0/1	kyiv-darnytsya-asw1		2,101,104
	FE0/19-FE0/23	port-channel 1 (asw3)		2,101,102,103,104
kyiv-poznyaki-asw1	GE1/1	kyiv-poznyaki-dsw1		2,3
	GE1/2	kyiv-poznyaki-asw2		2,3
	FE0/1	Web-server	3	
	FE0/2	File-server	3	
kyiv-poznyaki-asw2	GE1/1	kyiv-poznyaki-asw1		2,3
	Ge1/2	kyiv-poznyaki-dsw1		
	FE0/1	Mail-Server	3	
kyiv-poznyaki-asw3	GE1/1	kyiv-poznyaki-dsw1		
	FE0/1-FE0/5	PTO	101	
	FE0/6-FE0/10	FEO	102	
	FE0/11-FE0/15	Accounting	103	
	FE0/16-FE0/19	Other		
	FE0/20-FE0/24	port-channel 1 (dsw1)		
kyiv-darnytsya-asw1	FE0/24	kyiv-poznyaki-dsw1		2,104
	FE0/1-FE0/15	PTO	1	
	FE0/20	administrator	104	

Рисунок 3.7 - Регламент щодо портів, куди буде виконано підключення і що саме буде туди підключено для відділів провайдера

Имя устройства	Порт	Название	VLAN	
			Access	Trunk
obl-dnh-gw1	FE0/0	LAN		
	FE1/0	Kyev		4
	FE1/1	stalingrad heroes		
obl-dnh-sw1	FE0/24	obl-dnh-gw1		
obl-stlh-gw1	FE0/24	obl-dnh-gw1		

Рисунок 3.8 - Регламент щодо портів, куди буде виконано підключення і що саме буде туди підключено для користувачів

Имя устройства	Порт	Название	VLAN	
			Access	Trunk
pchr-boichyka-gw1	FE0/0	LAN and UpLink		2,5
pchr-boichyka-ds1	FE0/24	Kiev-poznyaki		5
	FE0/23	pchr-boichyka-gw1		2

Рисунок 3.9 - Регламент щодо портів, куди буде виконано підключення і що саме буде туди підключено для користувачів

По завершенню складання плану можна переходити до реалізації поставлених задач. Для початку необхідно було побудувати макет майбутньої мережі і для цього було обрано найдоступніший симулятор Cisco Packet Tracer версії 7.1.1.0137. Після цього було обрано обладнання яким було реалізовано макет робочої мережі та оформлені з’єднання між ними.

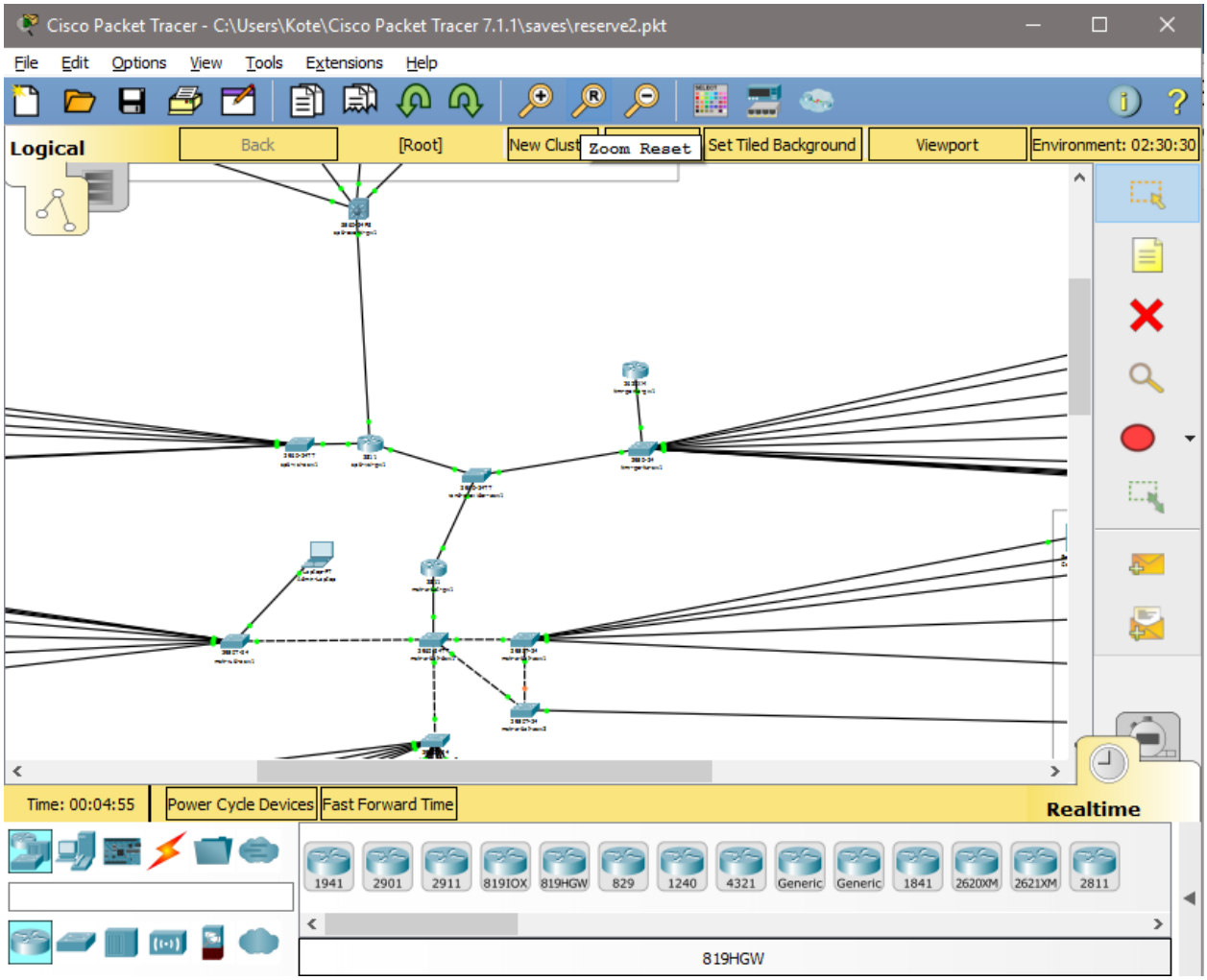


Рисунок 3.10 – Результат додавання мережевого обладнання до проекту, та оформлення його підключення

Підключення було виконано згідно правил по правильному підключенню, а саме – однаковий тип обладнання підключається кросс-кабелем(перехресним кабелем), різні типи обладнання підключаються прямим кабелем.

Тепер необхідно додати кінцеві хости: користувачів і персонал що буде обслуговувати мережу.

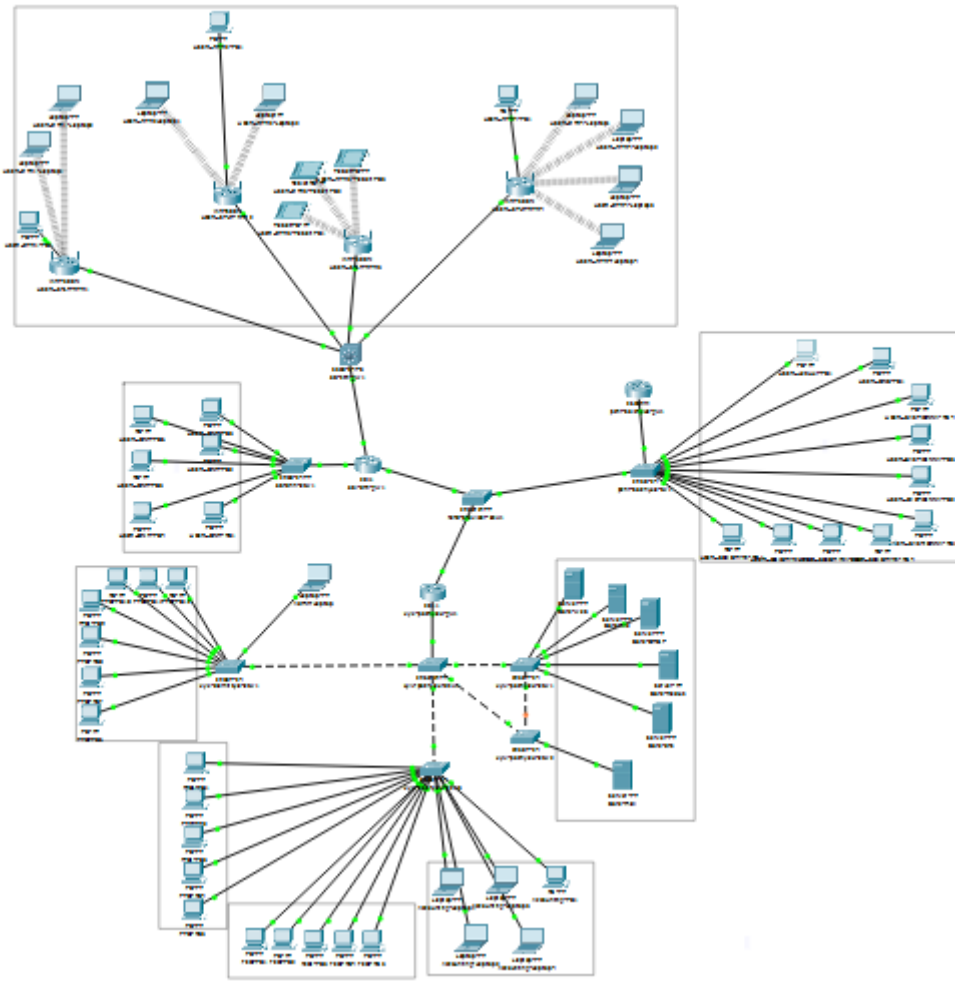


Рисунок 3.11 – Результат додання кінцевих хостів(користувачів, серверів та персоналу)

Прямокутниками виділені різні зони(Київ район Позняків, Дарниця, Оболонь(вулиці Герої Дніпра та Героїв Сталінграду)) та відділи(Фінансово-Економічний, Бухгалтерія, технічний відділ та підтримка).

Для забезпечення відмовостійкості серверів, було створено додаткове з’єднання між комутаторами Kyiv-poznyaki-dsw1, Kyiv-poznyaki-asw1 та kyiv-poznyaki-asw2. За допомогою протоколу STP у місці підключенні серверів було забезпечено безперебійне з’єднання і навіть якщо одно зі з’єднань буде втрачено, то зв’язок буде встановлено по іншому шляху за декілька секунд[29].

Також було імітоване транспортне підключення між нашою мережею та іншим місцевим «інтернет-провайдером», що люб’язно надав нам доступ до свого обладнання через яке ми змогли розповсюдити свою мережу, за символічну платню.

В даній мережі було реалізовано декілька методів підключеня кінцевих хостів і застосовано декілька методів маршрутизації. Наприклад, частина мережі підключена через L3-комутатор, який за замовченням працює як маршрутизатор, але його можна перелаштувати у режим L2-комутатора і підключати пристрої як зазвичай. Завдяки тому, що порти працюють, як на маршрутизаторі, через нього можливо підключити користувачів і організувати підключення мережевого обладнання. Це дозволяє значно зберегти кошти, що могли бути витрачені на закупівлю більшої кількості обладнання(окремо маршрутизатора, окремо комутаторів).

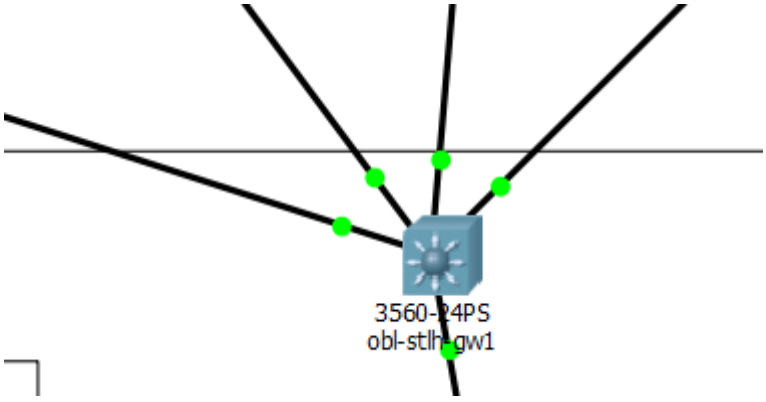


Рисунок 3.12 - L3-комутатор у Cisco Packet Tracer

Також продемонстровано метод підключення маршрутизатора як так званий «маршрутизатор на паличці», що також дозволяє заощадити кошти на обладнанні і організації підключення[44]. Назву свою цей метод отримав через те, що комутатор має тільки одне підключення, і тому виглядає як «на паличці».

За застосуванням такого методу трафік проходить через маршрутизатор «в один бік» і це не впливає на можливості маршрутизатору виконувати свої функції.

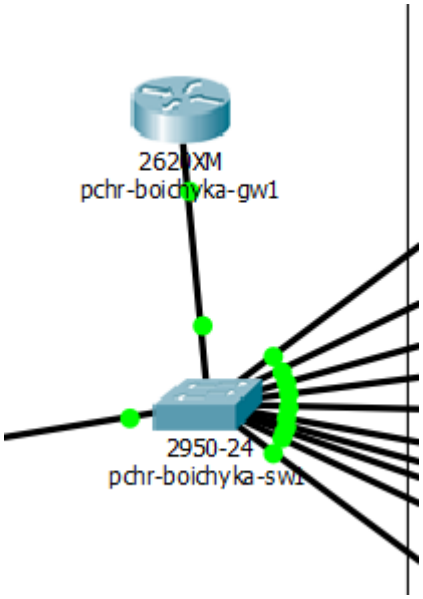


Рисунок 3.13 – Реалізація методу маршрутизатор «на паличці»(router-on-the-stick)

Мережа була налаштована у режимі статичного підключення, що дозволяє отримати наочні результати щодо того, як працює мережа і які процеси в ній відбуваються і яким чином. Більш детальний опис того, як було налаштовано мережеве обладнання для сприяння ліпшій взаємодії та фільтруванню трафіку.

4. ЕРГНОНОМІКА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

4.1 Розрахунок часу евакуації людей при пожежі в приміщенні

Підприємство є одноповерховою будівлею, що відображена на рис. 4.1 розмірами 10 м. на 20м.; кількість робочих кімнат 8; кількість працюючих 13; кількість виходів 1.

Для розрахунку загального часу евакуації необхідно розрахувати час на кожній ділянці руху людей, починаючи від максимально віддаленої точки.

Рух людей під час процесу евакуації є вимушеним, тобто пов’язаним із необхідністю покинути приміщення чи будівлю через виниклу небезпеку. Вимушений рух людей має свої специфічні особливості, вже на початковій стадії, людині погрожує небезпека в результаті того, що пожежа супроводжується виділенням теплоти, продуктів повного й неповного згорання, токсичних речовин, обвалення конструкцій, що так чи інакше погрожує людині. Із цього слід зробити висновок, що при плануванні будівлі і устрої приміщень в них необхідно прийняти заходи, щоб процес евакуації міг закінчитися безпечно і в необхідний час.

Друга особливість полягає у тому, що в силу погрожуючої людині небезпеки рух інстинктивно починається одночасно в один і той же напрям – у сторону виходів. Це призводить до того, що проходи швидко заповнюються людьми при визначеній щільності потоків. Із збільшенням щільності потоків швидкість руху зменшується, що створює певний визначений ритм руху. В цій ситуації з’являється погроза утворення затору, і дуже важко запобігти їй.

Показником ефективності процесу вимушеної евакуації є час, на протязі якого люди можуть при необхідності покинути окремі приміщення і

будівлю в цілому. Безпечність, досягнута тоді, коли цей час менший, ніж тривалість пожежі. Короткочасність процесу евакуації повинна досягатися не тільки конструктивно-планувальними рішеннями, на які звертали увагу раніше, але й організаційними рішеннями.

Процес евакуації людей можна поділити на три етапи :

- рух людей від найбільш віддаленої точки приміщення до евакуаційних виходів;
- рух людей від евакуаційних виходів до виходів на зовні ;
- рух людей від виходів із будівлі та їх розсіювання.

При евакуації основними параметрами, які характеризують процес руху людей є :

1) щільність людського потоку – D, люд/м2;

2) швидкість руху людського потоку – v, м/хв;

3) пропускна спроможність шляху (виходів) - Q ;

4) інтенсивність руху людського потоку - q ;

1) Щільність людського потоку D, яка складається з N людей, дорівнює:

$$D_1 = \frac{N_1 f}{A}, \text{ м}^2/\text{м}^2 \qquad (4.1),$$

де $A = g \cdot l$ – площа шляху евакуаційної ділянки [м²];

l – довжина ділянки; g- ширина ділянки;

f – площа горизонтальної проекції людини.

Якщо $D < 0.05$ людина має повну свободу пересування;

Якщо $0.05<D<0.15$ людина не може вільно змінювати напрямок свого руху;

Якщо $0.15<D<=0.92$ люди рухаються вкупі. Величина 0.92 є верхньою межею, коли люди рухаються вкупі, та нею обмежується щільність при проектуванні евакуаційних шляхів.

2) Швидкість руху людського потоку *v* залежить від його щільності *D* та виду шляху (горизонтальні чи похилі). Значення швидкості v , а також інтенсивності руху людського потоку q в залежності від його цільності D приведено в табл. 4.1.

Таблиця 4.1 Значення швидкості v і інтенсивності q руху людського потоку залежно від його щільності D

Щільність потоку $м^2/м^2$, Д	Горизонтальний шлях		Дверний проем	Сходи вниз		Сходи вверх	
	Швидкість м/хв. v	Інтенсивність, q м/хв.	Інтенсивність, q м/хв.	Швидкість м/хв. v	Інтенсивність, q м/хв.	Швидкість м/хв. v	Інтенсивність, q м/хв.
0,01	100	1	1	100	1	60	0,6
0,05	100	5	5	100	5	60	3
0,1	80	8	8,7	95	9,5	53	5,3
0,2	60	12	13,4	68	13,6	40	8
0,4	40	16	18,4	40	16	26	10,4
0,6	27	16,2	19	24	14,4	18	10,8
0,8	19	15,2	17,3	13	10,4	13	10,4
0,9 и більше	15	13,5	8,5	8	7,2	11	9,9

3) Пропускна спроможність шляху *Q* (м/хв чи люд/хв)

$$Q = D \cdot v \cdot \delta \text{ , м}^2\text{/хв.} \quad (4.2)$$

4) Інтенсивністю руху людського потоку *q* (м/хв чи люд/хв)

$$q = D \cdot v \quad (4.3)$$

Інтенсивність руху не залежить від ширини шляху і являється характеристикою потоку. Інтенсивністю руху людського потоку на кожному відрізку дорівнює:

$$q_i = \frac{q_{i-1}\delta_{i-1}}{\delta_i}, \text{ м/хв.} \qquad (4.4)$$

де: δ_I, δ_{i-1} – ширина розглядаючого і-го і перед ним (і – 1) відрізків шляху, м;

q_i, q_{i-1} – значення інтенсивності руху потоку на розглядаючому і-му і перед ним (і - 1) відрізках шляху, м/хв.

Якщо q_i менше чи рівно q_{max}, то час руху на відрізку можні визначити по формулі:

$$t_1 = \frac{l_1}{v_1}, \qquad (4.5)$$

при цьому значение q_{max} треба приниймати рівним, м/хв.:

- для горизонтальних шляхів 16,5
- для дверних проємів 19,6
- для сходів вниз 16
- для сходів вверх 11

Розрахунковий час евакуації людей із приміщення й будівлі *tp* встановлюється по розрахунку часу руху людських потоків від найбільш віддалених місць розташування. При розрахунку весь шлях руху людського потоку поділяється на ділянки (прохід, коридор, сходинковий марш, дверний проріз, тамбур) довжиною l_i і шириною g_i.

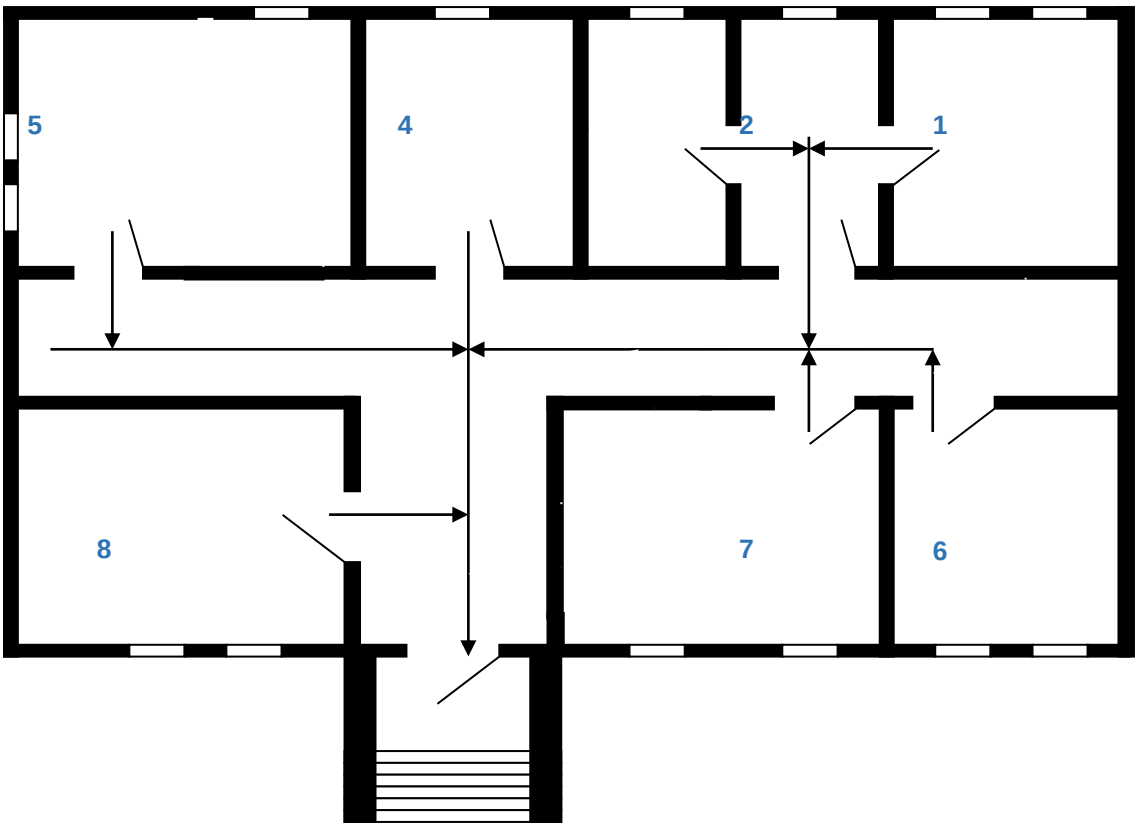
Початковими ділянками являються проходи між робочими місцями.

Розрахунковий час евакуації дорівнює :

$$t_p = t_1 + t_2 + t_3 + \ldots + t_i = t \ [\text{хв}], \qquad t_i = l_i / v_i \ [\text{хв}].$$

де t_i – час руху людського потоку на кожній окремій ділянці.

Умова безпечної евакуації характеризується виразом $t_p <= t_{нб}$, тобто розрахункова тривалість вимушеної евакуації на різноманітних ділянках при розрахункових швидкостях людей і розрахунковій пропускній спроможності



евакуаційних дверей повинна бути рівна або менша необхідного часу тривалості евакуації. Необхідний час евакуації $t_{нб}$ визначається по таблиці.

Використовуючи вище зазначений опис, за винятком таких ділянок як дверний проріз та тамбур (не передбачена у будівлі), проведемо розрахунок часу евакуації людей для прийнятого приміщення.

Маршрут евакуації розбивається на дев'ять етапів (ділянок). Для проведення розрахунку задамося планом евакуації людей (рис. 4.1).

Рисунок 4.1 План евакуації людей

Перша ділянка.

Час руху людського потоку – вихід людей з кімнати № 1:

де l= 13 м – довжина ділянки ; v – швидкість руху на ділянці.

f = 0.113 м^2 – середня площа горизонтальної проекції людини ;

N = 2 – кількість людей ; S = 3 м – ширина ділянки .

$D_1 = 2\left(\frac{0.113}{3 \cdot 13}\right) = 0.006$ [м^2/м^2], тоді v_1 = 100 м/хв ; q_1= 1 м/хв.

t_1 = 13/100 =0,13 хв.

Друга ділянка.

Час руху людського потоку – вихід людей з кімнати № 2:

$D = 3\left(\frac{0.113}{11 \cdot 3}\right) = 0.01$ [м^2/м^2], тоді v_3 = 100 м/хв ; q_3= 1 м/хв.

t_2 = 11/100 =0,11 хв.

де l = 11 м; f = 0.113 м^2; N = 3; S = 3 м.

Третя ділянка.

Час руху людського потоку – вихід людей з кімнати № 3:

$D = 1\left(\frac{0.113}{12 \cdot 3}\right) = 0.003$ [м^2/м^2], тоді v_2 = 100 м/хв; q_2= 1 м/хв.

t = 12/100 =0,12 хв.

де l = 12 м; f = 0.113 м^2; N = 1; S = 3 м.

Четверта ділянка.

Час руху людського потоку – вихід людей з кімнати № 4:

$D = 2\left(\frac{0.113}{5 \cdot 3}\right) = 0.01$ [м^2/м^2], тоді v_4 = 100 м/хв; q_4= 1 м/хв.

t = 5/100 =0,05 хв.

де l = 5 м; f = 0.113 м^2; N = 2; S = 3 м.

П’ята ділянка.

Час руху людського потоку – вихід людей з кімнати № 5:

$D = 2\left(\frac{0.113}{12 \cdot 3}\right) = 0.007$ [м^2/м^2], тоді v_5 = 100 м/хв ; q_5= 1 м/хв.

t = 12/100 =0,12 хв.

де l = 12 м; f = 0.113 м^2; N = 2; S = 3 м.

Шоста ділянка.

Час руху людського потоку – вихід людей з кімнати № 6:

$D = 2\left(\frac{0.113}{12 \cdot 3}\right) = 0.007$ [м^2/м^2], тоді v_6 = 100 м/хв; q_6= 1 м/хв.

t = 12/100 =0,12 хв.

де l = 12 м; f = 0.113 м^2; N = 2; S = 3 м.

Сьома ділянка.

Час руху людського потоку – вихід людей з кімнати № 7:

$D = 2\left(\frac{0.113}{9 \cdot 3}\right) = 0.008$ [м^2/м^2], тоді v_7 = 100 м/хв; q_7= 1 м/68в..

Т = 9/100 =0,09 хв.

Де l = 9 м; f = 0.113 м^2; N = 2; S = 3 м.

Восьма ділянка.

Час руху людського потоку – вихід людей з кімнати № 8:

$D = 2\left(\frac{0.113}{3 \cdot 3}\right) = 0.02$ [м^2/м^2], тоді v_8 = 100 м/хв; q_8= 1 м/хв.

t = 3/100 =0,03 хв.

де l = 3 м; f = 0.113 м^2; N = 2; S = 3 м.

Дев'ята ділянка.

Час руху людського потоку – вихід людей з кімнати № 9:

$D = 7\left(\frac{0.113}{9 \cdot 3}\right) = 0.03$ [м^2/м^2], тоді v_9 = 100 м/хв; q_9= 1 м/хв.

t = 9/100 =0,09 хв.

де l = 9 м; f = 0.113 м^2; N = 7; S = 3 м.

Десята ділянка.

Час руху людського потоку – вихід людей з кімнати № 10:

$D = 11\left(\frac{0.113}{5 \cdot 3}\right) = 0.08$ [м^2/м^2], тоді v_{10} = 100 м/хв; q_{10}= 1 м/68в..

T = 5/100 =0,05 хв.

Де l = 5 м; f = 0.113 м^2 ; N = 11; S = 3 м.

Одинадцята ділянка.

Час руху людського потоку – вихід людей з кімнати № 11:

$D = 13\left(\frac{0.113}{3 \cdot 3}\right) = 0.1632$ [м^2/м^2], тоді v_{11} = 60 м/хв; q_{11} = 12 м/хв.

t = 3/60 =0,05 хв.

де l = 3 м; f = 0.113 м^2 ; N = 13; S = 3 м.

Загальний час евакуації : $t = t_1 + t_2 + \ldots + t_{18}$ = 1,01 [хв].

$t_{нб}$ = 2,5 хвилин для одноповерхового будинку (з СНиП 2.01.02-85, табл. 12)

t = 1,01 < $t_{нб}$ = 2,5 хв, тобто вимоги пожежної безпеки виконуються.

В зв'язку з можливістю виникнення пожежі на території будівлі внаслідок несправної роботи комп'ютернрї техніки, яка підключена до електромережі, я вирішив вибрати вуглекислотні вогнегасники моделі ОУ-8 та порошкові – моделі ОП-8Б. Розмістити їх необхідно на пожежних щитах в вестибюлі та біля пожежного, по одному екземпляру кожного типу.

За допомогою вогнегасника ОУ-8 можна гасити різні речовини, крім тих, які можуть горіти без доступу повітря. Також їм можна тушити пожежу в пристроях під напругою до 1000V, при умові приближення по струмопровідних частин не ближче одного метру.

Механізм припинення горіння за допомогою використання вуглекислого газу базується на його властивостях шляхом розбавлення знижувати концентрацію реагуючих речовин до рівня, при якому горіння становиться неможливим.

За допомогою вогнегасника ОП-8Б можна тушити палаюче електрообладнання під напругою до 1000V, легкозаймисті рідини, тліючі матеріали (навіть ті що горять без доступу повітря) праці в робочому приміщенні.

4.2 Ергономічні вимоги до організації і обладнання робочих місць з комп`ютерною технікою

Оператор обробки інформації при виконанні своєї роботи майже весь робочий час знаходиться в сидячому положенні за робочим столом, на якому розташоване його робоче обладнання. Для запобігання виникнення, пов`язаних з таким видом робіт, хвороб (скаліоз, хвороби очей та ін.), а також для усунення загального дискомфорту, зменшення втомлюваності працівника, підвищенню його продуктивності необхілно правильно організувати робоче місце.

Організація робочого місця передбачає:

- правильне розміщення робочого місця у виробничому приміщенні;
- вибір ергономічного обгрунтованого робочого положення, виробничих меблів з урахуванням антропометричних характеристик людини;
- раціональну компановку обладнання на робочих місцях;
- урахування характеру та особливостей трудової діяльності;
- ДНАОП 0.00-1.31-99, ГОСТ 12.2.032-78, ДСанПІН 3.3.2.007-98 регламентує такі вимоги до організації робочого місця користувача ВДТ (візуальний дисплейний термінал):

1) Конструкція робочого столу має відповідати сучасним вимогам ергономіки і забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання (дисплея, клавіатури, принтера) і документів. Рекомендовані розміри столу: висота – 725 мм, ширина – 600-1400 мм, глибина – 80-1000 мм. Робочий стіл повинен мати простір для ніг висотою не менше ніж 450 мм, на рівні витягнутої ноги не менше 650 мм.

Робоче місце має бути обладнане підставкою для ніг шириною не менше ніж 300 мм, глибиною не менше ніж 400 мм, з можливістю регулювання по висоті в межах 150 мм та кута нахилу опорної поверхні – в межах 20°. Підставка повина мати рифлену поверхню і бортик по передньому краю заввишки 10 мм.

2) Робочий стілець користувача ВДТ повинен мати такі основні елементи: сидіння, спинку та стаціонарні або знімні підлокітники. Робочий стілець має бути підйомно – поворотним, регульованим за висотою, за кутом нахилу сидіння та спинки і за відстанню від спинки до попереднього краю сидіння. Поверхня сидіння має бути плоскою, передній край заокругленим.

Висота поверхні сидіння має регулюватися в межах 400…500 мм, а ширина і глибина становити не менше ніж 400 мм. Кут нахилу сидіння – до 15° вперед і до 5° назад.

Висота спинки має становити (300 ± 20) мм, ширина – не менше ніж 380 мм, радіус кривизни горизонтальної площини – 400 мм. Кут нахилу спинки має регулюватися в межах 0…30° від вертикального положення. Відстань від спинки до переднього краю сидіння має регулюватися в межах 260…400 мм.

Для зниження статичного навантаження м`язів верхніх кінцівок слід використовувати стаціонарні або знімні підлокітники довжиною не менше ніж 250 мм, шириною не менше ніж 50…70 мм. що регулюються за висотою над сидінням у межах 230…260 мм і відстанню між підлокітниками в межах 350…500 мм.

Поверхня сидіння і спинки стільця має бути напівм`якою з нековзним, повітронепроникненим покриттям, що легко чиститься і не електризується.

Конструкція виробничих меблів для користувача ВДТ має бути такою, щоб забезпечувати йому підтримання оптимальної робочої пози з

такими ергономічними характеристиками: ступні ніг – на підлозі або на підставці для ніг; стегна – в горизонтальній площині; верхні частини рук – вертикальні; кут ліктьового суглоба (між плечем та передпліччям) – 70 -90°; зап`ястки зігнуті під кутом не більше 20° відносно горизонтальної площини, нахил голови вперед в межах 15-20° до вертикалі.

3) Дисплей має розташуватися на столі на відстані від очей користувача не більше 700 мм (оптиальна відстань 450 – 500 мм). Розташування екрану має забезпечувати зручність зорового спостереження у вертикальній площині під кутом + 30° до нормальної лінії погляду працюючого. В горизонтальній площині кут спостереження екрану не повинен перевищувати 60°.

4) Клавіатуру слід розташувати на поверхні столу на відстані 100…300 мм від краю, звернутого до працюючого. У конструкції клавіатури має передбачитися опорний пристрій, який дає змогу зиінювати кут нахилу поверхні клавіатури у межах 5…10°. Висота середнього рядка клавіш має не перевищувати 30 мм. Поверхня клавіатури має бути матовою з коефіцієнтом відбиття 0,4.

5) Документ для вводу даних розташовується на відстані 450…500 мм від очей працівника, переважно зліва, кут між екраном дисплея та документом в горизонтальній площині має бути 30 - 40°.

6) Розміщення принтера або іншого пристрою введення – виведення інформації на робочому місці має забезпечувати добру видимість екрана ВДТ, зручність ручного керування пристроєм введення – виведення інформації в зоні досяжності: по висоті 900 – 1300 мм, по глибині 400 – 500 мм. Під принтери ударної дії потрібно підкладати вібраційні килимки для гасіння вібрації та шуму.

На рис. 4.2 зображено вид робочого місця з ВДТ:

А-принтер.

В-монітор.

C-системний блок.

D-клавіатура.

E-папка для документів.

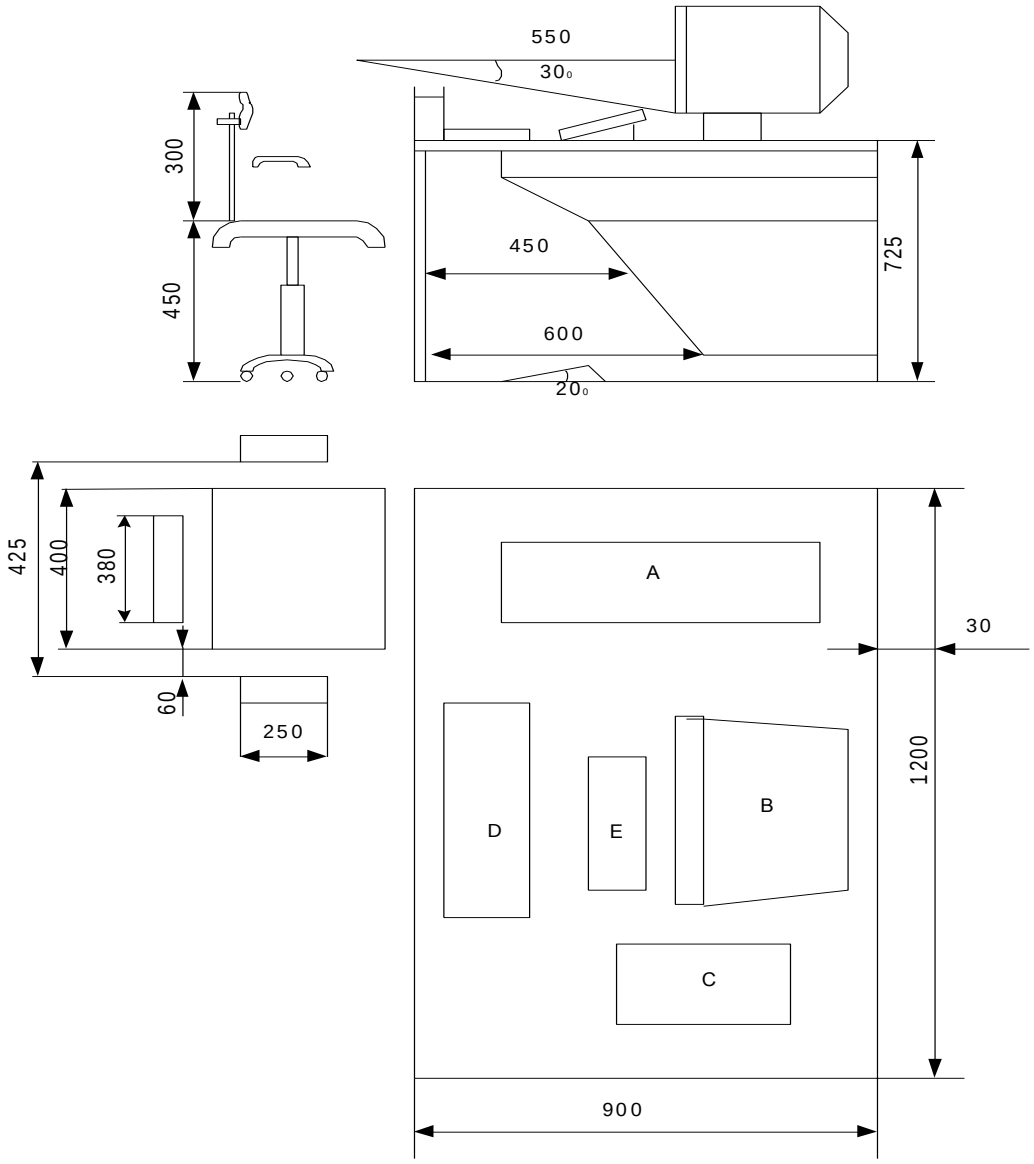


Рисунок 4.2 Вид робочого місця з ВДТ

ВИСНОВКИ

В результаті проведених досліджень було встановлено, що існують не тільки відомі проблеми з організацією комп'ютерних мереж, та доступу до мережі інтернет, а і деякі з невиявлених чи неоголошених особливостей обладнання, з яким працюють користувачі, також велику значимість має однорідність обладнання, оскільки при послідовному підключенні на одному й тому ж самому рівні обладнання, що розроблюється різними компаніями може призвести до непередбачуваних наслідків: від простої неспроможності надати стабільний доступ до мережі інтернет, чи обмін даними між двома чи більше кінцевими пристроями до абсолютної втрати роботоспроможності обладнанням без можливості подальшого відновлення.

Необхідно також зазначити, що для організації зазначеного інтернет-підключення є перелік вимог, що мають бути обов'язково виконанні і без яких доступ до всесвітньої мережі не буде можливим. В першу чергу має бути визначеним тип підключення. У цьому випадку мова йде про метод, за яким будуть надаватися налаштування[46]. На сьогоднішній день найвідоміші й найпоширеніші такі типи підключення як:

1. *Dynamic (DHCP)* – тип підключення, при якому прописувати налаштування на обладнанні користувача немає потреби.
2. *Static* – тип підключення, при якому всі налаштування прописуються вручну.

Головною вимогою до типу підключення є відповідність його як на обладнанні користувача, так і на обладнанні, до якого користувач

підключений, у випадку, коли тип підключення у користувача виставлено не той, що встановлено на обладнанні, наприклад, провайдера, то доступу до мережі не буде взагалі. Також, якщо тип підключення є статичним, то необхідна відповідність налаштуванням, за якими обладнання користувача ідентифікується в мережі. Ідентифікація користувача у мережі провайдера, та знаходження тих самих, необхідних йому налаштувань у таблиці відповідності знаходиться по відповідності зазначеної *IP-адреси* та відповідної *MAC-адреси*.

MAC-адреса – унікальний ідентифікатор обладнання, що бажає підключитися до мережі.

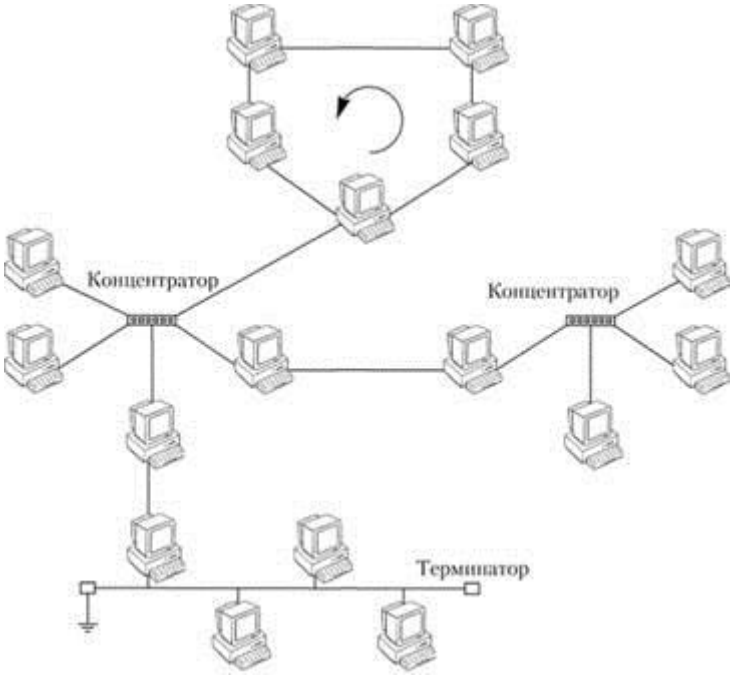
IP-адреса – адреса за якою обладнання ідентифікується в мережі.

Це єдина вимога, що безпосередньо стосується користувача. Всі наступні вимоги можуть змінюватися, в залежності від того, яке обладнання виступає провідником у наданні доступу, яким методом виконується підключення: по витій парі, оптоволоконним кабелем, бездротово, чи коаксіальним кабелем[48]. Від цього критерію може залежати стабільність підключення та якість вхідного/вихідного сигналу.

Також вважаю за потрібне зазначити, що вирішальну роль може мати навіть топологія мережі, що організовується на місці використання. У більшості випадків в наш час застосовується змішана топологія, на основі топологій кільце, зірка та шина. Кільцем підключаються комутатори, до яких підключають кінцеве обладнання, а зіркою – обладнання сполучення.

Також необхідно зазначити перелік вимог, що стосуються безпосередньо обладнання, через яке підключається користувач, у цьому випадку – комутатори. Для здійснення стабільного якісного підключення, мають бути сконфігуровані порти належним чином, як на фізичному рівні, так і на логічному. Не зайвим буде трохи більше уваги приділити логічному рівню. Для забезпечення роботоспроможності підключення, порт має бути сконфігурований, як порт типу *access*, що відповідає конфігурації порту в

режимі роботи з кінцевим обладнанням[41]. Існує також конфігурація в режимі *trunk,* що використовується зазвичай для підключення комутаторів між собою. Оскільки у комутаторів також є свій максимально допустимий поріг роботи, бажано також створити та сконфігурувати *vlan*-и для роботи з кінцевими користувачами та що будуть застосовуватися для роботи обслуговуючого персоналу. Для простоти їх можна назвати абонентським *vlan*-ом та *vlan* менеджменту.



Приклад змішаної топології на основі топологій: зірка, кільце та шина

Перший відповідає за роботу з кінцевими користувачами, їх можна створити декілька, наприклад для розмежування всіх користувачів на окремі групи, в яких вони не «бачити» один одного.

Другий відповідає за наявність доступу до налаштувань комутатора без застосування абонентських vlan-ів, створюється для зручності використання та підвищення рівню захищеності.

Для викоистання vlan-ів було створено межу, тому допстимий діапазон для творення вланів відповідає від 1-го до 4096-го. Частина з них може бути зарезервована виробником, ще на стадії прогрмування, зазвичай перший

встановлюється як стандартний *vlan* повсюди[42]. Тому коли обладнання починають конфігурувати вже на місці використання, то з більшості портів за необхідністю його видаляють. Таким чином отримуємо досить великий перелік речей, що будучи налаштовані неправильно чи, без належного розуміння суті проблеми, можуть призвести до відсутності з'єднання без явних на те причин, повну втрату доступу до обладнання, поки воно не буде «занулено» чи абсолютну відмову обладнання від здатності до справної роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комп'ютерні мережі – топологія комп'ютерних мереж [Електронний ресурс]. – Режим доступу :

http://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6

2. Про MAC-таблицы в коммутаторах/ Хабр [Електронний ресурс]. – Режим доступу : https://habr.com/post/254183/

3. ZXR10 2900E Series Easy-maintenance Secure Switch Configuration Guide [Електронний ресурс]. – Режим доступу : http://zte.by/manuals/29e/Configuration_Guide.pdf

4. Manual P3310 Rus 22022013 [Електронний ресурс]. – Режим доступу : http://doc.pavlabor.net/HARD/PON/BDCOM/Manual_P3310_Rus_22022013.pdf

5. VLAN [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/VLAN

6. Flow control [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/Flow_control

7. Raisecom ISCOM Series Switch Configuration Guide [Електронний ресурс]. – Режим доступу : http://www.svpro.ru/pdf/bib/Raisecom%20Switch%20Software%20Configuration%20Guide.pdf

8. Еще раз про IP-адреса, маски подсетей и вообще/ Хабр [Електронний ресурс]. – Режим доступу : https://habr.com/post/129664/

9. Zeroconf [Електронний ресурс]. – Режим доступу : https://ru.wikipedia.org/wiki/Zeroconf

10. DHCP [Електронний ресурс]. – Режим доступу : https://ru.wikipedia.org/wiki/DHCP

11. RFC 3171 [Електронний ресурс]. – Режим доступу : http://www.faqs.org/rfcs/rfc3171.html

12. http://www.rfc-editor.org/rfc/rfc3330.txt [Електронний ресурс]. – Режим доступу : http://www.rfc-editor.org/rfc/rfc3330.txt

13. Understanding MSTP [Електронний ресурс]. – Режим доступу : http://blog.ine.com/2010/02/22/understanding-mstp/

14. STP [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/STP

15. Безопасность канального уровня [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/l2security

16. ARP-spoofing [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/ARP-spoofing

17. arpwatch [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/arpwatch

18. Агрегирование каналов [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/link_aggregation

19. LACP [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/LACP

20. IEEE 802.3ad Link Bundling [Електронний ресурс]. – Режим доступу : https://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/sbcelacp.html

21. DHCP snooping [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/DHCP_snooping

22. The Debian Administrator’s Handbook [Електронний ресурс]. – Режим доступу : https://debian-handbook.info/browse/stable/

23. 802.1Q [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/802.1Q

24. GVRP [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/GVRP

25. VLAN ID [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/VLAN_ID

26. ISL [Електронний ресурс]. – Режим доступу : http://xgu.ru/wiki/ISL

27. HTTP Strict Transport Security Cheat Sheet [Електронний ресурс]. – Режим доступу : https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet

28. TCP/IP [Електронний ресурс]. – Режим доступу : https://ru.wikipedia.org/wiki/TCP/IP

29. UDP [Електронний ресурс]. – Режим доступу : https://ru.wikipedia.org/wiki/UDP

30. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. — СПб.: Питер, 2016. — 992 с

31. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с. (2016)

32. Д. Куроуз, К. Росс Компьютерные сети: Нисходящий подход(6-е издание) – Москва: Издательство «Э», 2016. – 912 с.

33. Сергеев А. Н. Основы локальных компьютерных сетей: Учебное пособие. — СПб.: Издательство «Лань», 2016. — 184 с.

34. Робачевский А. Интернет изнутри. Экосистема глобальной Сети. - 2-е изд., перераб. и доп. - М.: Альпина Паблишер, 2017. - 271 с

35. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация, акад. изд.: Пер. с англ. - М.: ООО "И.Д. Вильяме", 2015. - 736 с

36. Bash. Карманный справочник системного администратора Арнольд Роббинс; Издательство: Вильямс; ISBN: 978-5-9909445-4-1; Год издания: 2017 г.; Страниц: 152

37. CCNP Self-Study CCNP BCRAN Exam Certification Guide Second Edition [Електронний ресурс]. – Режим доступу : https://docstore.mik.ua/cisco/pdf/routing/Cisco%20Press%20-%20CCNP%20BCRAN%20Certification%20Guide.pdf

38. Hierarchical internetworking model [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/Hierarchical_internetworking_model

39. Ethernet [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/Ethernet

40. Frame (networking) [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/Frame_(networking)

41. Frame synchronization [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/Frame_synchronization

42. CRC-based framing [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/CRC-based_framing

43. Asynchronous transfer mode (ATM) [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/Asynchronous_transfer_mode_(ATM)

44. Octet (computing) [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/Octet_(computing)

45. Broadband Integrated Services Digital Network [Електронний ресурс]. – Режим доступу : https://en.wikipedia.org/wiki/Broadband_Integrated_Services_Digital_Network

46. BPDU [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/BPDU

47. IEEE 802 [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/IEEE_802

48. LMSC, LAN/MAN Standards Comitee (Project 802) [Електронний ресурс]. – Режим доступу : http://www.ieee802.org/