НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет інформаційних технологій

УДК 004.94:339.3-025.12

«ПОГОДЖЕНО»	**«ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ»**
Декан факультету інформаційних технологій	Завідувач кафедри комп'ютерних систем і мереж
Глазунова О.Г., д.п.н., професор	Лахно В.А., д.т.н., професор
_____	_____
___ _____ **2021 р.**	___ _____ **2021 р.**

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему «Дослідження та проектування локально обчислювальної мережі торгівельної компанії»

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма «Комп'ютерні системи і мережі»

Орієнтація освітньої програми освітньо-професійна

Керівник магістерської кваліфікаційної роботи

к.пед.н., доцент _____ Касаткін Д.Ю.

Виконав Іващенко В.А. _____
(ПІБ студента)

КИЇВ-2021

НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Факультет інформаційних технологій

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних систем і мереж
Лахно В.А., д.т.н., доцент

_____
"____" _____20_____року

З А В Д А Н И Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ СТУДЕНТУ

Іващенко Володимир Анатолійович
(прізвище, ім'я, по батькові)

Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерні системи і мережі»
Орієнтація освітньої програми освітньо-професійна
Тема магістерської кваліфікаційної роботи «Дослідження та проектування локально обчислювальної мережі торгівельної компанії»

затверджена наказом ректора НУБіП України від "23" жовтня 2020р. № 1578 «С»
Термін подання завершеної роботи на кафедру 13.12.2021
Вихідні дані до магістерської кваліфікаційної роботи

Перелік питань, що підлягають дослідженню:

1. Дослідження алгоритмів проектування локально обчислювальної мережі
2. Аналіз вимог до функціональних можливостей локально обчислювальної мережі
3. Розробка та проектування локально обчислювальної мережі до заданих потреб

Дата видачі завдання "23" жовтня 2020р.

Керівник магістерської кваліфікаційної роботи _____ Касаткін Д.Ю
(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ Іващенко В.А.
(підпис) (прізвище та ініціали студента)

ЗМІСТ

Перелік скорочень та умовні позначки

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

IEEE – Institute of Electrical and Electronics Engineers

IP – Internet Protocol

IP – Internet Protocol

ISO – International Organization for Standardization

LAN – Local Arial Net (укр. «ЛОМ»)

MAC – Media Access Control

MAN – Metropolitan Area Network

NAT – Network Address Translation (укр. «трансляція мережевих адрес з публічних у локальні та навпаки»)

PAN – Private Arial Net

PAN – Personal Area Network

PoE – Power over Ethernet

SAN – Storage Area Network

TCP – Transmission Control Protocol

VPN – Virtual Private Network

WAN – Wide Area Network

Wi-Fi – Wireless Fidelity

ВСТУП

Планування та проектування локальної обчислювальної мережі є надзвичайно важливими. Найчастіше вони належать організаціям для власного користування, тобто приватні мережі. Це виключає дуже великі мережі, особливо загальнодоступні мережі, реалізовані постачальниками послуг зв'язку такі як телефонні компанії та великі постачальники послуг Інтернету. З іншого боку, магістерській роботі не розглядаються мережі, які настільки малі, щоб їх можна було придбати «з коробки» і для яких планування, проектування та впровадження здійснюється кількома людьми, можливо, лише одним.

На початку проектування потрібно дати чітку харктеристику ЛОМ. Цей опис має узагальнити результати різного вид стратегічного аналізу: масштабованість, керованість, продуктивність, довговічність. Деякі з питань, які необхідно розглянути: хто з ким спілкується? Чи проект, призначений для підтримки комунікацій всередині компанії, постачальників і клієнтів (бізнесбізнес), комунікації з клієнтами (роздрібна торгівля) чи їх комбінація?

Кінцевим результатом проектування ЛОМ є складання докладної схеми майбутньої мережі.

1) провести дослідження та аналіз предметної галузі;
2) вивчення основних топологій комп'ютерних мереж;
3) проаналізувати потреби кадрів у техніці;
4) створити логічну схему мережі та схему приміщень;
5) створити фізичну схему комп'ютерної мережі

організації;

1 ПЕРШИЙ РОЗДІЛ

1.1 Типи комп’ютерних мереж

Доступні різні типи комп'ютерних мереж. Класифікація мережі в комп'ютерах може бути здійснена за їх розміром, а також за призначенням. Розмір мережі повинен бути виражений географічною областю та кількістю комп'ютерів, які є частиною їхньої мережі. Він включає пристрої, розміщені в одній кімнаті, та мільйони пристроїв по всьому світу. Нижче наведено популярні типи комп'ютерних мереж.

- PAN (персональна мережа)
- LAN (локальна мережа)
- MAN (міська мережа)
- WAN (глобальна мережа)

1.2 Personal Area Network (PAN)

Personal Area Network – це комп'ютерна мережа, створена навколо людини. Зазвичай він складається із комп'ютера, мобільного телефону або персонального цифрового помічника. PAN може використовуватися для встановлення зв'язку між цими особистими пристроями для підключення до цифрової мережі та Інтернету.

Характеристики PAN:

- В основному це мережа персональних пристроїв, обладнаних на обмеженій території.

- Дозволяє керувати підключенням IT-пристроїв в оточенні одного користувача.
- PAN включає мобільні пристрої, планшети та ноутбуки.
- Він може бути підключений до Інтернету через бездротову мережу під назвою WPAN.
- Пристрої, що використовуються для PAN: бездротові миші, клавіатури та Bluetooth.

Переваги PAN:

- Мережі PAN щодо безпечні та безпечні
- Він пропонує лише рішення для малого радіусу дії до десяти метрів.
- Строго обмежено невеликою площею

1.3 Local Area Network (LAN)

Локальна мережа - являє собою групу комп'ютерів і периферійних пристроїв, які з'єднані в обмеженому просторі, наприклад, як школи, лабораторії, будинки та офісні будівлі. Це мережа, що широко використовується для обміну такими ресурсами, як файли, принтери, ігри та інші програми. Найпростіший тип мережі LAN - це з'єднання комп'ютерів та принтера в чиємусь будинку або офісі. Як правило, LAN буде використовуватися як один із типів середовища передачі. Це мережа, що складається з менш ніж 5000 взаємозалежних пристроїв у кількох будинках.

Характеристики LAN:

- Це приватна мережа, тому зовнішній регулюючий орган ніколи не контролює її.
- LAN працює на відносно вищій швидкості, порівняно з іншими системами WAN.
- Існують різні методи керування доступом до середовища передачі даних, такі як Token Ring та Ethernet.

Переваги LAN:

- Комп'ютерні ресурси, такі як жорсткі диски, DVDдиски та принтери можуть спільно використовувати локальні мережі. Це значно знижує вартість придбання обладнання.
- Ви можете використовувати одне й те саме програмне забезпечення по мережі замість того, щоб купувати ліцензійне програмне забезпечення для кожного клієнта в мережі.
- Всі користувачі мережі можуть зберігатися на одному жорсткому диску серверного комп'ютера.
- Ви можете легко надсилати дані та повідомлення через підключені до мережі комп'ютери.
- Керувати даними буде просто з одного місця, що зробить дані безпечнішими.
- Локальна мережа пропонує можливість спільного використання одного підключення до Інтернету серед усіх користувачів локальної мережі.

Недоліки LAN:

- LAN дійсно заощадить кошти через загальні комп'ютерні ресурси, але початкова вартість установки локальних мереж досить висока.
- Адміністратор локальної мережі може перевіряти файли особистих даних кожного користувача локальної мережі, тому це не забезпечує хорошої конфіденційності.
- Неавторизовані користувачі можуть отримати доступ до критично важливих даних організації, якщо адміністратор локальної мережі не може захистити централізоване сховище даних.
- Локальна мережа вимагає постійного адміністрування локальної мережі, оскільки виникають проблеми, пов'язані з налаштуванням програмного забезпечення та апаратними збоями.

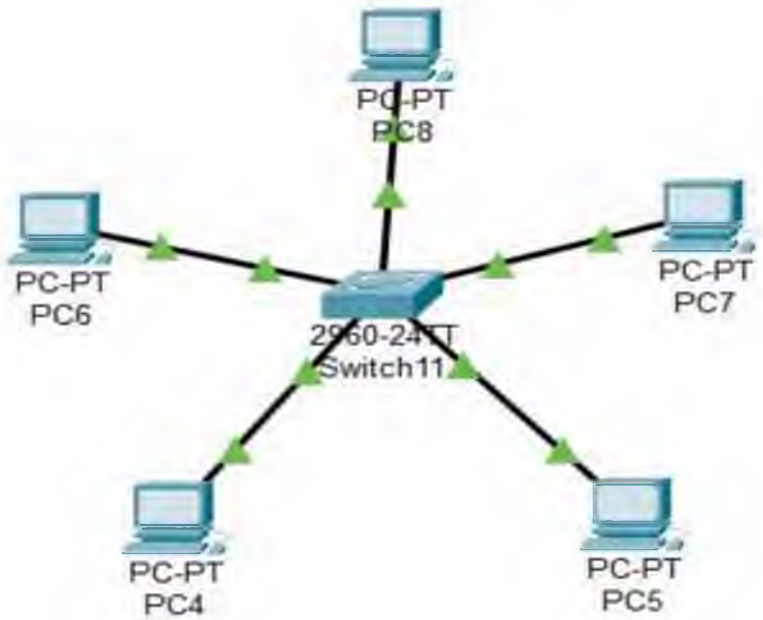


Рисунок 1.3.1 – Мережева топологія «Зірка»

1.4 Wide Area Network (WAN)

Глобальна мережа – ще одна важлива комп'ютерна мережа, яка розташована на великій географічній території. Мережева система WAN може являти собою з'єднання LAN, яке з'єднується з іншими LAN за допомогою телефонних ліній та радіохвиль. Здебільшого це обмежується підприємством чи організацією.

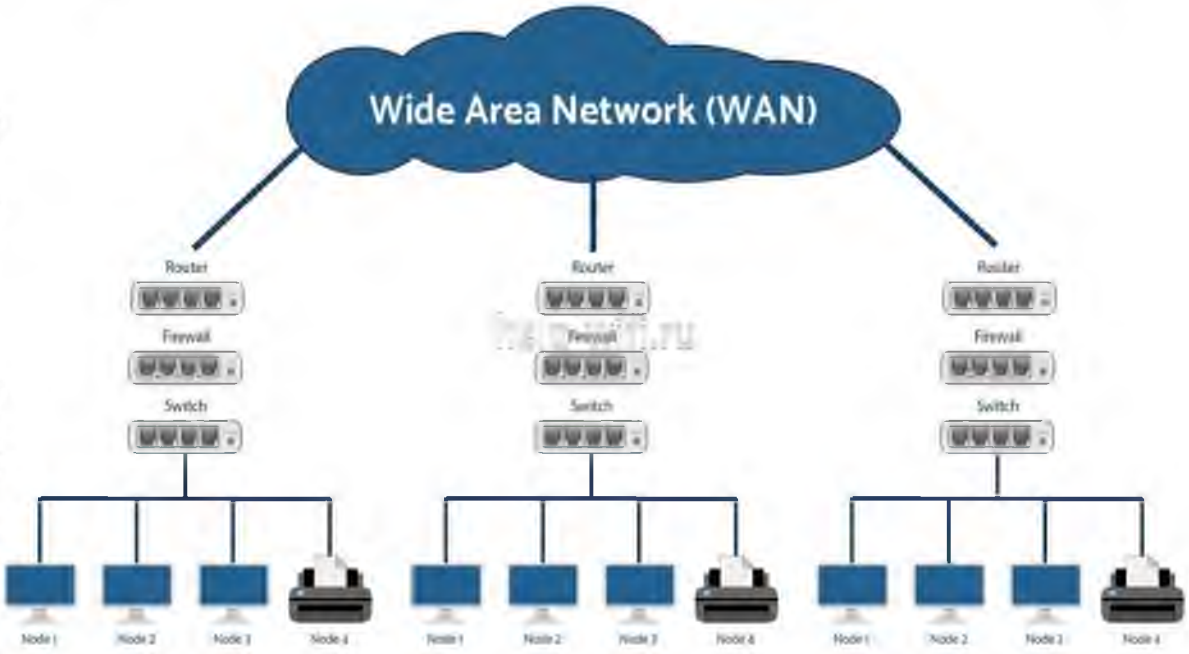


Рисунок 1.4.1 – Логічна побудова WAN мереж

Характеристики WAN:

Файли програмного забезпечення будуть доступні для всіх користувачів; тому всі можуть отримати доступ до останніх файлів.

Будь-яка організація може створити свою глобальну інтегровану мережу за допомогою WAN.

Переваги WAN:

- WAN допомагає вам покрити велику географічну зону. Таким чином, бізнес-офіси, які розташовані на великих відстанях, можуть легко спілкуватися.
- Містить такі пристрої, як мобільні телефони, ноутбуки, планшети, комп'ютери, ігрові консолі тощо. буд.
- З'єднання WLAN працюють із допомогою радіопередавачів і приймачів, вбудованих у клієнтські устрою.

Недоліки WAN:

- Вартість початкової установки дуже висока.
- Важко підтримувати мережу WAN. Вам потрібні кваліфіковані спеціалісти та мережеві адміністратори.
- Помилок і проблем стає більше через широке охоплення та використання різних технологій.
- Для вирішення проблем потрібно більше часу через залучення безлічі дротових та бездротових технологій.
- Пропонує нижчий рівень безпеки, ніж інші типи комп'ютерних мереж.

1.5 MAN

Metropolitan Area Network - складається з комп'ютерної мережі через все місто, кампус коледжу або невеликий регіон. Цей тип мережі більше, ніж локальна мережа, яка здебільшого обмежена одним будинком чи майданчиком. Залежно від типу конфігурації, цей тип мережі дозволяє вам покривати територію від кількох миль до десятків миль.

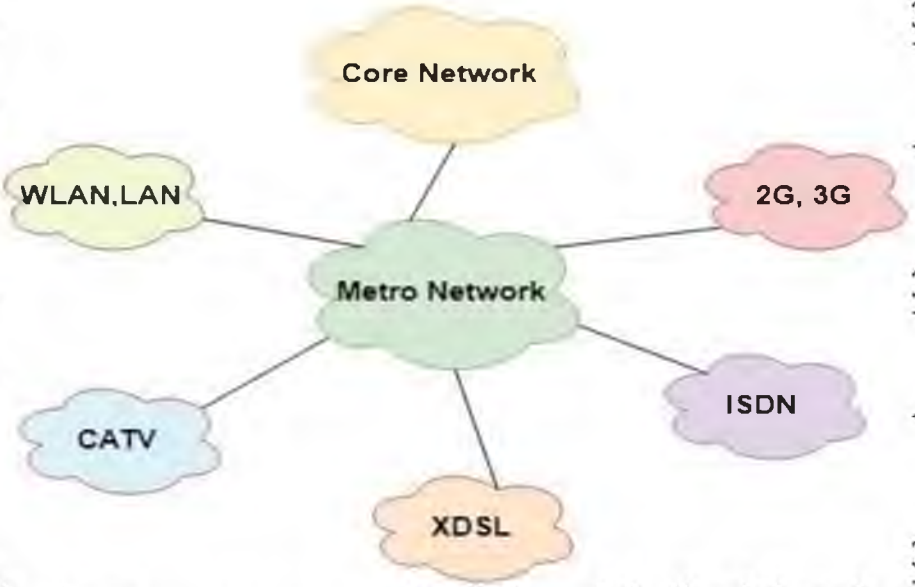


Рисунок 1.5 – Технології та типи мереж які охоплює MAN

Характеристики MAN:

- В основному, він охоплює міста з максимальною дальністю 50 км.
- Найчастіше використовуване середовище – це оптичні волокна, кабелі.
- Швидкість передачі даних адекватна додатків розподілених обчислень.

Переваги MAN:

- Він пропонує швидкий зв'язок із використанням високошвидкісних носіїв, таких як оптоволоконні кабелі.
- Він забезпечує відмінну підтримку мережі великого розміру та ширший доступ до глобальних мереж.
- Подвійна шина в мережі MAN забезпечує одночасну передачу даних в обох напрямках.
- Мережа MAN переважно включає деякі райони міста або ціле місто.

1.6 WLAN

WLAN (бездротова локальна мережа) допомагає зв'язати один або кілька пристроїв за допомогою бездротового зв'язку в межах обмеженої області, наприклад будинку, школи або офісної будівлі. Це дозволяє користувачам перемішатися в межах локальної зони покриття, яка може бути підключена до мережі. Сьогодні більшість сучасних систем WLAN базуються на стандартах IEEE 802.11.

1.7 SAN

Мережа зберігання даних – це тип мережі, яка дозволяє зберігати консолідовані дані на рівні блоків. Він переважно використовується для

виготовлення пристроїв зберігання, таких як дискові масиви, оптичні музичні автомати та стрічкові бібліотеки.

Системна мережа використовується локальної мережі. Він пропонує високошвидкісне з'єднання у міжсерверних та міжпроцесорних додатках. Комп'ютери підключені до мережі SAN працюють як єдина система з досить високою швидкістю.

Пасивна оптична локальна мережа POLAN – це мережна технологія, яка допомагає інтегруватися у структуровані кабелі. Це дозволяє вирішити питання підтримки протоколів Ethernet та мережевих програм. POLAN дозволяє використовувати оптичний розгалужувач, що допомагає відокремити оптичний сигнал від одномодового оптичного волокна. Він перетворює цей єдиний сигнал на кілька сигналів.

Домашня мережа (HAN): Домашня мережа завжди будується за допомогою двох або більше взаємозалежних комп'ютерів для формування локальної мережі (LAN) всередині будинку. Наприклад, у США близько 15 мільйонів будинків мають більше одного комп'ютера. Ці типи підключення до мережі допомагають власникам комп'ютерів підключатися до кількох комп'ютерів. Ця мережа дозволяє обмінюватися файлами, програмами, принтерами та іншими периферійними пристроями.

1.8 Virtual Private Network (VPN)

Віртуальна приватна мережа – це приватна мережа, яка використовує загальнодоступну мережу для з'єднання віддалених сайтів або користувачів. Мережа VPN використовує «віртуальні» з'єднання, що маршрутизуються через Інтернет із приватної мережі підприємства або сторонньої служби VPN на віддалений сайт. Це безкоштовна або платна послуга, яка забезпечує

безпеку та конфіденційність перегляду веб-сторінок через загальнодоступні точки доступу Wi-Fi.

1.9 Класифікаційна характеристики LAN

Локальні мережі - є основними будівельними блоками всіх об'єднаних мереж. Ці технології реалізуються на рівні каналу передачі даних моделі OS. Це пов'язано з тим, що ці мережеві технології значною мірою визначаються фізичними носіями, які вони спільно використовують, і тим, як управляють доступом до цього спільного середовища. Цей рівень каналу передачі також називається MAC - рівень доступу до середовища передачі даних. Основний формат трафіку на цьому рівні називається кадром. Таким чином, у локальних мережах зв'язок може мати справу лише з MAC-адресами, які є серійними номерами, такими як ідентифікатори пристроїв. Такі речі, як IP-адреси, потрібні лише при маршрутизації даних між сегментами LAN через об'єднану мережу. Ці технології 2-го рівня можуть підтримувати лише комутовані міжмережові операції. Вони підходять тільки для локальних областей або простих маршрутів на великі відстані, де не потрібно багато вказівок для доставки даних. Таким чином, локальні мережі можна поділити на дві основні категорії. Доступ до локальних мереж – вони приймають кабельне або бездротове з'єднання від пристроїв, зв'язують робочі групи разом та спільно використовують локальні ресурси, такі як принтери та сервери відділів. Ці сегменти формуються/фокусуються концентраторами чи комутаторами доступу. Зазвичай вони знаходяться у відділі чи на поверсі будівлі. Магістральні ЛОМ - вони пов'язують ЛОМ з доступом, наприклад, до серверів баз даних, поштових серверів та інших спільно використовуваних пристроїв з більшою зоною покриття. Вони формуються/фокусуються маршрутизаторами

чи комутаторами LAN. Зазвичай вони проходять через усю будівлю або офісне містечко.

Певні типи трафіку потребують передбачуваності більше, ніж інші. Наприклад, телефонні розмови не можуть терпіти затримок у передачі, тому що це порушить перебіг розмови. У потокового відео є дещо схожі вимоги, але ситуація гнучкіша. Чутливість до затримки - це термін, що використовується для характеристики чутливості до затримок передачі. Пріоритетна чутливість у чомусь схожа, але пов'язана з порядком отримання даних. Наприклад, при потоковій передачі відео допустимі деякі невеликі затримки, особливо під час буферизації, але якщо вони отримані не в правильному порядку, виникнуть серйозні проблеми. Широкомовне повідомлення йде до кожного приймального пристрою в межах певного домену. Очевидно, що всі ми отримуємо радіо та телетрансляції через різні ЗМІ. Мовлення в Інтернеті може призвести до величезних витрат на інфраструктуру і не є чимось зазвичай прийнятним. Багатоадресної передачі повідомлення проходить тільки з заздалегідь визначеними приймальними пристроями в межах широкомовного домену. Хоча змусити працювати багатоадресне розсилання належним чином - справжня проблема, вона все ж таки буде краще трансляції в Інтернеті. Ethernet - найпоширеніша форма LAN. Вперше він був розроблений Xerox у 1970 році. Потім Digital Equipment Company, Intel і Xerox випустили другу версію, часто звану DIX Ethernet, у 1982 році, щоб подолати багато труднощів оригіналу. Зв'язок з Ethernet працює за принципом порівняння. Пристрої, які спільно використовують Ethernet, прослуховують інший трафік і передають дані тільки в тому випадку, якщо LAN вільна. Якщо дві станції відправляють приблизно в один і той же час та їх повідомлення конфліктують, обидві передачі перериваються, і вони чекають протягом випадково згенерованого періоду перед повторною передачею. Ethernet використовує так званий CSMA/CD - протокол множинного доступу з контролем несучої та виявленням

колізій для регулювання трафіку. Крім того, оскільки середовище підключення є загальним, кожен пристрій в сегменті локальної мережі Ethernet отримує кожне повідомлення і перевіряє, чи адреса призначення збігається з його власним . Якщо є збіг, повідомлення приймається та обробляється. Якщо збігів не знайдено, повідомлення буде відкинуто. Все це створює враження, що Ethernet є дуже неефективним, і це так. Так більшість доступної лінії пропускання втрачається через перерваних передач, що теоретична ефективна пропускну здатність становить лише близько 37% від цього, що практично доступно. З іншого боку, обладнання, необхідне роботи з такими спрощеними протоколами, настільки недороге проти іншими підходами, що зазвичай виявляється найбільш рентабельним. Ethernet має досить багато варіантів реалізації. Три з найбільш відомих наведено в таблиці.

Таблиця 1.9.1 – Варіанти Ethernet реалізації

Опція Ethernet	Швидкість	Підключення
Оригінал	1 Мбіт/с	Коаксіальний кабель або вита пара 10BaseT
Швидкий	100 Мбіт/с	Вита пара 100BaseTX або оптоволокно 100BaseFX
Гігабіт	1000 Мбіт/с	Вита пара 1000BaseTX або оптоволокно 1000BaseFX

В даний час популярною конфігурацією є підключення до локальних мереж доступу Fast Ethernet через магістральну локальну мережу Gigabit Ethernet.

Token Ring раніше був основним конкурентом Ethernet. За власними стандартами він несумісний з Ethernet з точки зору мережевих адаптерів,

кабельних роз'ємів та програмного забезпечення, яке потрібно використовувати. Token Ring зазвичай найбільш широко використовується на підприємствах, де переважають обчислення на базі IBM. Token Ring отримало свою назву від того факту, що воно визначає підключені пристрої в логічне, хоч і малоймовірне, фізичне кільце. Ми називаємо це логічним кільцем, тому що воно передає сигнали, ніби пристрої були підключені одним замкнутим кабелем. Фізично вони цілком можуть бути в топології хаба та спиці, званої зіркоподібною топологією. Token Ring дозволяє уникнути конфліктів у сегменті LAN за рахунок використання протоколу передачі токенів. Тільки пристрій, що володіє токеном, може передавати, що усуває конфлікти. Такий підхід напевно збільшує ефективне використання доступної пропускної спроможності Token Ring. Тестування показує, що Token Rings може використовувати до 75% доступної пропускної спроможності. На жаль, витрати на використання Token Rings відносно вищі, ніж витрати на використання Ethernet. За розумними оцінками, у сегментах ЛОМ має бути не менше 40 користувачів, щоб стати рентабельними. Як тільки трафік у сегменті LAN збільшується до певного рівня, конфлікти, пов'язані з Ethernet, стають для користувачів більш дорогими.

Як з'ясовується, більшість локальних мереж дійсно досить малі, переважно тому, що переважна більшість людей зайнята в малому або середньому бізнесі. Але навіть ті, хто працює у великих компаніях, знаходяться в локальних мережах, які використовують Ethernet з усією його неефективністю.

Особливості розвитку технологій бездротового доступу З розвитком радіотехніки та електроніки поняття «бездротовий» використовувався для позначення радіозв'язку в найширшому сенсі цього слова, тобто у всіх випадках, коли інформація передавалася без кабелю спілкування. У наступний час інтерпретація «бездротовий» практично пішла адресу, а «бездротовий

(бездротовий)» почали використовувати як поняття термін «радіо» або «RF - радіочастота». Наразі терміни вважаються взаємозамінними, коли йдеться про частотні діапазони від 3 кГц до 300 ГГц. Тим не менш, термін «радіо» все частіше використовується для опису існуючі раніше технології (супутниковий зв'язок, мовлення, радіолокаційний, а також радіотелефонний зв'язок). Поняття терміна «бездротовим» сьогодні прийнято називати новітні технології радіозв'язок, такий як стільниковий зв'язок, пейджинг, абонентський доступ. Існують три типи бездротових мереж:

- WWAN (бездротова глобальна мережа);
- WLAN (бездротова локальна мережа);
- WPAN (бездротова персональна мережа);

2 Обґрунтування проблем LAN що досліджуються.

У бездротових локальних мережах немає кабелів та роз'ємів. Внаслідок цього усуваються витрати на встановлення мережі. Наприклад, для встановлення мережі не потрібно наймати спеціаліста з мережі. Це набагато економічніший спосіб порівняно із звичайними мідними кабелями.

Додавання або видалення нової робочої станції у WLAN стало простіше. Як і комп'ютер, мережа WLAN може бути розширена без будь-якого планування. Але користувачам необхідно стежити за тим, щоб кількість пристроїв не перевищувала певного рівня.

Ще одна перевага бездротової передачі у WLAN – це мобільність, яку вона пропонує. З пристроями користувачі можуть вільно переміщатися у межах зони покриття. А якщо працівникам потрібно змінити робоче місце, вони можуть зробити це зручно за допомогою WLAN.

Як згадувалося раніше, WLAN не використовує жодних фізичних дротів. Це означає, що всередині мережі не використовуються жодні дроти чи кабелі. Коли мережа розширюється, нові кабелі не потрібні. Це також значно заощаджує час на встановлення.

3 Типові проблеми при налаштуванні та проектуванні LAN або WLAN

Незважаючи на всі зусилля, спрямовані на те, щоб мережа працювала без збоїв є декілька поширених проблем.

3.1 IP-адреси, що повторюються.

Коли два пристрої намагаються спільно використовувати одну IPадресу, ви бачите жахливу помилку "Адреса вже використовується" - без можливості доступу до мережі.

Швидке виправлення: вина часто покладається на конфігурацію DHCP вашого маршрутизатора за замовчуванням. DHCP, ймовірно, намагається призначити вашому новому пристрою адресу на початку вашої підмережі, а інший пристрій може вже займати ці адреси з низьким номером зі статичними IP-адресами. Якщо ви додали до своєї мережі новий пристрій або сервер, у нього може бути власний DHCP-сервер. Просто відключіть DHCP-сервер на цьому пристрої, щоб відновити працездатність вашої мережі.

Профілактичний захід: ви можете зробити один простий крок, щоб уникнути конфліктів IP-адрес, змінивши конфігурацію вашого маршрутизатора, щоб почати призначати DHCP-адреси у верхній частині вашої підмережі, залишивши нижні адреси доступними для пристроїв, яким потрібні статичні IP-адреси.

3.2 Вичерпання IP-адреси

Щоб вирішити цю проблему, використовуйте ipconfig. Якщо робоча станція привласнила собі IP-адресу, що починається з 169.xxx, це означає, що IP-адреса не була доступна з DHCP-сервера.

Швидке рішення: у деяких користувачів кабельного Інтернету може не бути локального маршрутизатора, і в цьому випадку IP-адреси призначаються на обмеженій основі безпосередньо від вашого інтернет-провайдера. Ймовірно, у вашого інтернет-провайдера закінчилися дозволені IP-адреси. Рішенням є придбання автономного маршрутизатора або точки доступу Wi-Fi із вбудованим маршрутизатором. Це створює власний локальний пул внутрішніх адрес, гарантуючи, що ви не закінчите.

Якщо у вас вже є локальний маршрутизатор з DHCP, за замовчуванням пул адрес може бути занадто малим для вашої мережі. Отримавши доступ до налаштувань DHCP на маршрутизаторі, ви можете налаштувати розмір пула адрес відповідно до потреб вашої мережі.

Профілактичні заходи: важливо, щоб у будь-якій мережі, підключеній до Інтернету, був локальний маршрутизатор, що працює з NAT і DHCP, як з міркувань безпеки, так і для запобігання вичерпанню IP-адрес. Маршрутизатор повинен бути єдиним пристроєм, підключеним до модему, а решта пристроїв підключаються через маршрутизатор.

3.3 Проблеми з DNS

Помилки, такі як мережний шлях не може бути знайдено, IP-адреса не може бути знайдена або ім'я DNS не існує, зазвичай можуть бути пов'язані з проблемою конфігурації DNS . Утиліту командного рядка nslookup можна використовувати для швидкого відображення установок DNS робочої станції.

Швидке виправлення: робочі станції та інші мережні пристрої можна настроїти на використання власних DNS-серверів, ігноруючи сервер, призначений DHCP. Перевірка налаштувань «Протокол Інтернету версії 4 (TCP/IP)» для вашого адаптера покаже, чи вказано неправильний DNS-сервер, тому просто виберіть «Отримати адресу DNS-сервера автоматично».

Запобіжний захід: ваш локальний маршрутизатор може бути налаштований для роботи в якості DNS-сервера, створюючи наскрізну передачу DNS на сервери ваших інтернет-провайдерів. У завантажених мережах це може завантажити можливості маршрутизатора. Змініть налаштування DHCP вашої мережі, щоб отримати прямий доступ до ваших DNS-серверів.

3.4 Одиночна робоча станція не може підключитись до мережі.

Якщо тільки одна робоча станція відображає повідомлення «Немає Інтернету» при відкритті веб-браузера, ми зазвичай можемо припустити, що решта мережі справна, і звернути увагу на будь-яке обладнання та програмне забезпечення, що відноситься до цієї системи.

Швидке виправлення: Щоб вирішити цю проблему з мережею, почніть з усунення очевидних комунікаційних бар'єрів, таких як поганий кабель, поганий сигнал Wi-Fi, збій мережної карти або неправильні драйвери.

Переконайтеся, що мережний адаптер робочої станції налаштований з правильною IP-адресою, підмережею та DNS-серверами.

Якщо це не вирішить проблему, перевірте будь-яке програмне забезпечення брандмауера на пристрої, щоб переконатися, що порти відкриті для зовнішньої мережі. Загальні порти включають 80 та 443 для веб-трафіку, а також 25, 587, 465, 110 та 995 для електронної пошти.

Профілактичний захід: Зазвичай краще залишити для всіх налаштувань TCP/IP робочої станції значення «Автоматично призначається». Використовуйте DHCP-сервер, щоб роздати однакову конфігурацію всім пристроям у мережі. Якщо статична IP-адреса потрібна на конкретній робочій станції або сервері, більшість DHCP-серверів дозволяють створювати статичні зіставлення IP-адрес.

3.5 Неможливо підключитися до локальних файлів або загальних ресурсів принтера.

Проблеми спільного використання є одними з найскладніших для вирішення проблем мережі через кількість компонентів, які необхідно правильно налаштувати.

Найчастіше проблеми спільного використання виникають через конфлікти між змішаними безпековими середовищами. Навіть різні версії однієї і тієї ж операційної системи іноді використовують кілька різних моделей безпеки, що може ускладнити з'єднання робочих станцій.

Швидке рішення: ми можемо вирішити проблеми із спільним використанням найефективніше, вивчивши можливості у такому порядку:

Переконайтеся, що потрібні служби працюють. У системах Windows мають бути запущені сервер, TCP/IP NetBIOS Helper, робоча станція та комп'ютерні служби браузера. На машинах Linux Samba - це основний компонент, необхідний спільного використання із системами Windows.

Перевірте брандмауер (-и) . Брандмауер робочої станції часто налаштовується на блокування трафіку загального доступу до файлів і принтерів, особливо якщо встановлений новий антивірусний пакет з власним брандмауером. Проблеми з брандмауером можуть виникати на апаратному рівні, тому переконайтеся, що маршрутизатори або керовані комутатори пропускають загальний трафік усередині підмережі. До речі про підмережу.

Переконайтеся, що всі робочі станції розташовані в одній підмережі. Ця проблема зазвичай виникає лише у складних мережах, проте навіть прості мережі іноді мають обладнання статичного IP з неправильно налаштованою підмережею. В результаті зовнішній трафік рухатиметься нормально, тоді як внутрішній трафік зіткнеться з несподіваними перешкодами.

Для всіх мережних адаптерів Windows знадобиться спільний доступ до файлів та принтерів для мереж Microsoft, клієнт для мереж Microsoft та NetBIOS через TCP/IP.

Після того, як перераховані вище перевірки пройдені, настав час перевірити найбільш ймовірного винуватця - дозволу. Потрібно кілька рівнів доступу, кожен із своїм власним інтерфейсом в ОС. Перевірити:

Системи настроєно з неправильною робочою групою або доменом.

Неправильно настроєна домашня група.

Тип мережі встановлено на Public.

Неправильні дозволи NTFS.

3.6.Локальна мережа не може підключитися до Інтернету.

Ця ситуація може бути періодичною чи постійною. Часто найскладнішим аспектом вирішення будь-якої проблеми із зовнішньою мережею є пошук відповідальної компанії. А потім доручають їм вирішити проблему, особливо з періодичними збоями, які важко відстежити. Іноді може виникнути така проблема, що організаціям доведеться змінити інтернетпровайдера, щоб вирішити цю проблему.

Швидке рішення: перезавантаження маршрутизатора та модему – це перше, що потрібно зробити. Утиліту tracert then можна використовувати для виявлення розривів зв'язку. Очевидно, що на конкретному переході маршрутизатора, який викликає проблему, станеться збій. Зверніться до свого інтернет-провайдера та повідомте свої висновки, за необхідності надавши знімки екрана.

Профілактичний захід: щоб уникнути звинувачень, які можуть завадити швидкому вирішенню зовнішніх проблем, проведіть невелике дослідження, щоб переконатися, що ви забезпечуєте підключення тільки у місцевих постачальників рівня. 1, оскільки фактично не володіють інфраструктурою у вашому районі.

Мета полягає в тому, щоб видалити якнайбільше посередників, щоб, коли (а не якщо) ви зіткнетеся з проблемою, достатньо одного телефонного дзвінка, щоб виявити проблему і змусити технічних фахівців працювати над нею.

3.7.Повільна робота в Інтернеті.

Низька продуктивність зазвичай виникає через перевантаження або іноді через погану якість з'єднання іншим чином погіршилися. Перевантаження не може бути пов'язане безпосередньо з вичерпанням смуги пропускання, оскільки один перевантажений порт на комутаторі або маршрутизаторі може знизити продуктивність мережі.

Це може бути особливо вірним для виділених ліній, де очікується виділена смуга пропускання, але тести швидкості показують, що мережа не досягає свого номінального потенціалу.

Швидке рішення: використовуйте веб-сайти для перевірки швидкості, проводячи тести з географічно віддалених серверів. Це може точно визначити сфери навантаження в мережі інтернет-провайдера. У разі кабельного Інтернету локальна мережа використовується спільно вашими сусідами, що змушує вашого інтернет-провайдера виконувати дороге оновлення смуги пропускання у разі насичення. Повідомте свої висновки своєму інтернетпровайдеру, щоб він зробив кроки для вирішення проблеми.

DNS-сервери - це аспект продуктивності Інтернету, що часто не береться до уваги. Використання неправильних DNS-серверів може призвести до перевантаження маршрутизації або проблем із балансуванням навантаження. Хоча зазвичай вам слід використовувати налаштування DNS.

4 Центр обробки даних.

Підприємства масово вирішують використовувати автоматизоване рішення для численних завдань, що викликає необхідність розробки

обчислювальних систем високої доступності. Центральним елементом системи є Центр обробки даних.

Центр обробки даних (дата-центр) – це місце, де знаходиться різне електронне обладнання, особливо комп'ютери та телекомунікаційне обладнання. Як випливає з назви, він служить насамперед для обробки інформації, яка потрібна бізнесу. Наприклад, банк може використовувати такий центр, надаючи йому інформацію про своїх клієнтів під час обробки їх транзакцій. Насправді такий центр використовують практично всі середні компанії. Щодо великих компаній, то їх часто використовують десятки.

Бази даних часто мають вирішальне значення для бізнес-операцій, а також дуже чутливі до їхнього захисту. З цієї причини у цих центрах підтримується високий рівень безпеки та обслуговування, щоб гарантувати цілісність та роботу обладнання на місці.

Точне та стабільне повітря в центрі обробки даних. Точний контроль пилу, навколишнього середовища в центрі обробки даних. Блок енергії Аварійне джерело живлення та резервний блок у центрі обробки даних. Складна система пожежної сигналізації. Автоматичне гасіння пожежі краплями чи інертним газом. Труби для кабелів нижче та вище підлоги. Моніторинг за допомогою камер відеоспостереження у центрі обробки даних. Контроль доступу та фізична безпека. Спостереження 24/7 виділені сервери (комп'ютери).

Основні завдання центру – забезпечити гарне мережне з'єднання та високу доступність інформаційної системи. Відповідно, можна розгортати різні програмні продукти для критично важливих бізнес-завдань бізнесклієнтів. Ці програми включають менеджерів баз даних, файлових серверів та серверів програм.

Мережа зв'язок у центрі тепер здійснюється майже виключно за Інтернет-протоколом. Тому він містить маршрутизатори, комутатори та інше обладнання, що забезпечує зв'язок між серверами та зовнішнім світом. Надмірність іноді досягається за рахунок використання кількох мережних пристроїв різних виробників. Деякі сервери використовуються для надання користувачам інтрамережі та інтернету компанії сервісів, яких вони потребують: електронна пошта, проксі, DNS, файли тощо. З пристроїв мережевої безпеки також є: міжмережевий екран, VPN, системи виявлення вторгнень тощо. Є... і навіть системи моніторингу мережі та деяких додатків.

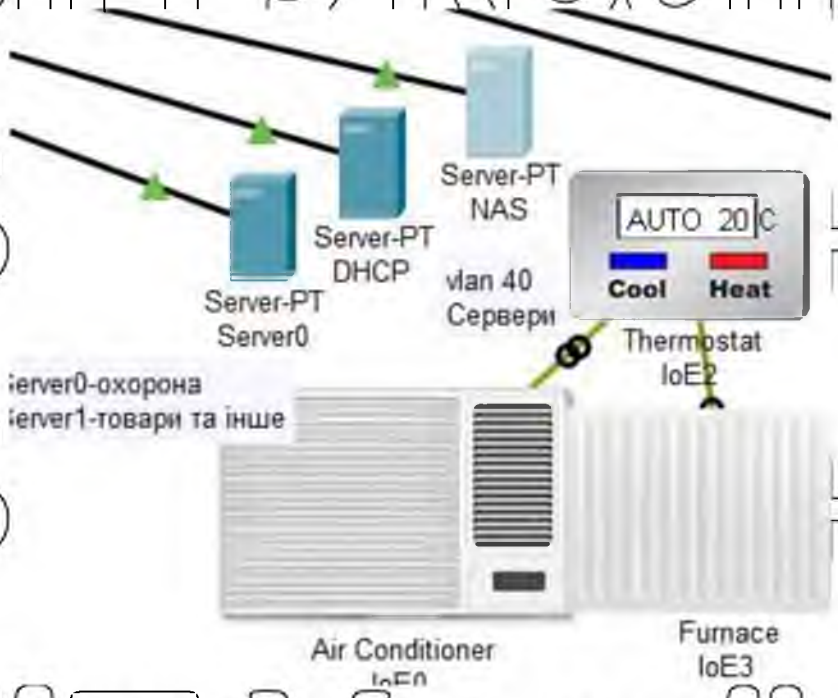


Рисунок 4.1 - ЦОТ локально обчислювальної мережі

Основна мета центру обробки даних (центру обробки даних) – запускати додатки, які обробляють дані, необхідні для функціонування суспільства. Ці програми можуть бути спроектовані та розроблені всередині компанії-клієнта або постачальником програмного забезпечення для керування. Це може бути типово для ERP та CRM. Часто ці програми

розподілені по кількох комп'ютерах, кожному з яких виконується певна частина завдання. Компоненти центру обробки даних - це найпоширеніша база даних управління системами, файлові сервери, сервери програм, проміжне ПЗ.

2 ДРУГИЙ РОЗДІЛ

5 Причини впровадження локально обчислювальної мережі

Роблячи обмін інформацією простим та швидким, мережі відкривають нові способи роботи та підвищують продуктивність. Вони забезпечують більш ефективне використання ресурсів, дозволяючи спілкуватися та співпрацювати на відстані. Завдяки обміну файлами всі співробітники, незалежно від місцезнаходження, мають доступ до однієї інформації. Загальні бази даних також унеможливлюють дублювання зусиль. Співробітники можуть "ділитися екраном" з комп'ютерними файлами, працюючи з даними, якби вони знаходилися в одній кімнаті. Їхні комп'ютери з'єднані телефонними або кабельними лініями, всі вони бачать те саме на своїх дисплеях, і будь-хто може вносити зміни, які бачать інші учасники. Співробітники також можуть використовувати мережі для відеоконференц-зв'язку. Мережі дозволяють компаніям запускати корпоративне програмне забезпечення, великі програми із вбудованими модулями, які керують усіма внутрішніми операціями корпорації. Системи планування ресурсів підприємства працюють у мережах. Типові підсистеми включають фінанси, людські ресурси, інжиніринг, продаж та розподіл замовлень, а також управління замовленнями та закупівлями. Ці модулі працюють незалежно, а потім автоматично обмінюються інформацією, створюючи систему в масштабах компанії, яка включає поточні дати постачання, стан запасів, контроль якості та іншу важливу інформацію.

Локальної мережі (LAN) дозволяє людям на одному сайті обміну даними та спільно використовувати апаратне та програмне забезпечення від різних виробників комп'ютерів. ЛОМ пропонують компаніям більш економічний спосіб з'єднання комп'ютерів, ніж з'єднання терміналів з мейнфреймом. Наприклад, найбільш поширені види використання локальних мереж на малих підприємствах – це автоматизація діловодства, бухгалтерський облік та управління інформацією. ЛОМ можуть допомогти компаніям скоротити штат, оптимізувати операції та скоротити витрати на обробку. ЛОМ можуть бути налаштовані з дротовими або бездротовими підключеннями.

У сучасному світі потреба в бездротовому мереж, у різних сферах діяльності, а особливо у сфері малого та великого бізнес та IT-технології. На підприємстві користувачі з бездротовим мережевим доступом до інформації, може виконувати роботу більш продуктивно й ефективно, ніж робітники, до яких прив'язані службові кабельні локальні мережі. Один із сучасних етапів розвитку бездротова технологія, це бездротова мережа Wi-Fi, найзручніша умови, що вимагають мобільності, зручності використання, а також економічно вигідний через недорогу вартість монтажу та обслуговування. Wi-Fi (від англ. wireless fidelity - бездротовий зв'язок) - широкосмуговий стандарт зв'язок сімейства бездротових 802.11.

IEEE 802.11 є початковим стандартом для бездротових локальних мереж на основі бездротової передачі даних 2,4 ГГц. Підтримує обмін даними зі швидкістю до 1 - 2 Мбіт/с. Прийнятий в 1997 році стандарт передбачав два види модуляції - DSSS і FHSS.

IEEE 802.11a — це стандарт бездротової локальної мережі, заснований на бездротовій передачі в діапазоні 5 ГГц. Діапазон розділений на три різнорідні піддіапазони. Максимальна швидкість передачі даних становить 54 Мбіт / с, також доступні швидкості 48, 36, 24, 18, 12, 9 і 6 Мбіт / с.

IEEE 802.11b — це стандарт бездротової локальної мережі, заснований на бездротовій передачі даних 2,4 ГГц. У всьому діапазоні є три різних канали, тобто три різні бездротові мережі можуть працювати в одній зоні, не впливаючи одна на одну. Цей стандарт використовує метод модуляції DSSS. Максимальна швидкість становить 11 Мбіт / с, також доступні швидкості 5,5, 2 і 1 Мбіт / с.

Стандарт IEEE 802.11b був прийнятий у 1999 році в рамках розробки раніше прийнятого стандарту IEEE 802.11. Він також передбачає використання діапазону частот 2,4 ГГц, але тільки з модуляцією DSSS. Продукти IEEE 802.11b від різних виробників були перевірені на сумісність і сертифіковані Альянсом Wireless Ethernet Compatibility Alliance (WECA), більш відомим як Wi-Fi Alliance. Сумісні бездротові продукти, які були протестовані в рамках Wi-Fi Alliance, можуть мати позначку Wi-Fi.

IEEE 802.11b + — це розширена версія стандарту 802.11b, реалізована окремими постачальниками, що забезпечує підвищену швидкість передачі даних. В інтерпретації Texas Instruments відрізняється від оригінальної версії модуляцією PBCC (Packet Binary Convolutional Coding), подвоєною максимальною швидкістю (до 22 Мбіт/с). Також були анонсовані рішення зі збільшеною продуктивністю до 44 Мбіт/с.

IEEE 802.11g — це стандарт бездротової локальної мережі, заснований на бездротовій передачі даних 2,4 ГГц. Діапазон розділений на три різні канали, тобто три різні бездротові мережі можуть працювати в одній зоні, не впливаючи одна на одну. Для збільшення швидкості передачі даних при ширині каналу, подібній до 802.11b, використовують метод модуляції з ортогональним частотним мультиплексуванням (OFDM, Ortogonal Frequency Division Multiplexing), а також метод двійкового згорткового кодування PBCC (Packet Binary Convolutional Coding).

IEEE 802.11e (QoS, Quality of service) - додатковий стандарт, що дозволяє забезпечити гарантовану якість обміну даними шляхом перестановки пріоритетів різних пакетів; необхідний для потокових послуг, таких як VoIP або IPTV.

IEEE 802.11i — це стандарт, який усуває недоліки безпеки попередніх стандартів. 802.11i вирішує захист даних на рівні даних і дозволяє створювати захищені бездротові мережі практично будь-якого масштабу.

IEEE 802.11n — це стандарт бездротової локальної мережі, який забезпечує бездротову передачу даних у діапазонах 2,4 ГГц і 5 ГГц. Стандарт 802.11n значно перевищує швидкість передачі даних попередніх стандартів, забезпечуючи швидкість на рівні Fast Ethernet; зворотна сумісність з 802.11a, 802.11b і 802.11g. Основною відмінністю від попередніх версій Wi-Fi є додавання підтримки MIMO (multiple-input multi-output) до фізичного рівня (PHY). Теоретична швидкість може становити 150 Мбіт/с

IEEE 802.11ac є стандартом для бездротових мереж Wi-Fi на частотах 5-6 ГГц. Якщо обидва пристрої підтримують цю технологію, швидкість передачі даних може перевищувати 1 Гбіт/с (до 6 Гбіт/с 8x MU-MIMO). Стандарт передбачає використання до 8 антен MU-MIMO і розширення каналів до 80 або 160 МГц. 20 січня 2011 року була прийнята перша версія 0.1, а 1 лютого 2013 року – версія 5.0.

IEEE 802.11ax – це новий стандарт бездротової локальної мережі, який має на меті забезпечити пропускну здатність близько 10 Гбіт/с. Робочі діапазони стандарту 5 ГГц і 2,4 ГГц (можуть включати додаткові діапазони частот в діапазоні від 1 до 7 ГГц). Стандарт був офіційно затверджений 9 лютого 2021 року.

5.1 Cisco Meraki

Cisco Meraki - це IT-компанія, штаб-квартира якого розташована в СанФранциско, штат Каліфорнія. Їх рішення включають в себе бесправодную передачу, комутацію, безпеку, управління мобільністю підприємства (EMM), комунікації та камери безпеки, все централізовано керовані з Інтернету. Meraki був придбаний компанія Cisco Systems в грудні 2012 року. Меракі заснували Санджит Бісвас, Джон Бікет і Ханс Робертсон. Компанія була заснована частково на проекті MIT Roofnet, експериментальної мережі 802.11b/g, розробленої Лабораторією компьютерных наук и искусственного интелекта в Институте технологий Массачусетса. Meraki був профінансований компанією Google і Sequoia Capital. Організація початку в Маунтин-Вью, штат Каліфорнія, в 2006 році, а потім переїхала в Сан-Франциско. Meraki занял людей, які працювали над проектом MIT Roofnet. 18 листопада 2012 компанія Cisco Systems об'явила, що придбав Meraki приблизно 1,2 мільярда доларів. За шість років після придбання Meraki нараховує 1590 співробітників Cisco, які працюють у всьому світі. Розділ має близько 250 000 унікальних клієнтів і більше 3500000 пристроїв в Інтернеті. Продукти розроблені Meraki слідують за принципом plug-and-play, з простим апаратним забезпеченням і легким для понімання програмним інтерфейсом, який означає, що компанія з малим і середнім розміром може створити безпровідну сеть, не наймаючи людей з особливою підготовкою і навиками. Продукція розробки Meraki також ділиться на різні серії, щодо їх призначення: MR серия Серія Meraki MR є першою в світі лінією доступу WLAN, управляємою через облако. Розроблені для складних бізнес-сред, точки доступу MR використовують удосконалені технології 802.11ac і 802.11n, включаючи MIMO, формування луча та зв'язування каналів для забезпечення пропускної здатності і надійного покриття, необхідного для требовательных бизнес-приложений. MS серія Cisco Meraki MS є першим у галузевому комутаторі управляємого доступу та агрегації, що поєднує переваги централізованого управління в області з потужною, надійною платформою доступа. Завдяки

управлінню через хмару, тисячі портів коммутатора можуть бути настроені і відслечені мгновенно через Інтернет. Предоставляет можливість вносити зміни в конфігурацію в мережі, а також легко управляти кампусом і розподільними мережами без навчання або спеціалізованого персоналу.

Meraki MX – це корпоративне пристрій безпеки та SD-WAN, призначене для розподілених розвертів, требуючих удаленного адміністрування. Воно ідеально підходить для сетевых адміністраторів, які вимагають як простоти розвертання, так і сучасного набору функцій.

Meraki MC є кінцевою точкою взаємодії, розробленої для зручності управління та видаленого адміністрування. Воно ідеально підходить для адміністраторів, які хочуть швидкого та легкого розвертання та управління розподільними телефонними системами.

Meraki MV – це лінійка мережевих камер для приміщення та вулиці, які є надзвичайно простими для розгортання і налаштування, завдяки їх інтеграції в інформаційну панель Meraki Dashboard та використання хмарних технологій. Семейство MV робить не потрібним використанням складних і дорогих апаратних засобів, необхідних для традиційних рішень, тим самим обмеження, які зазвичай виникають при розвертуванні відеонагляду. Також в Meraki є рішення для управління пристроями та наборами під назва системний менеджер. Одним із самих великих переваг Systems Менеджер є можливістю реєструвати, керувати та контролювати багато різних типів пристроїв. Оскільки кожна операционная система має унікальний набір функцій MDM, важливо ознайомитися с відповідною документацією пристроїв, якими планується керувати. Для цих служб рекомендується використовувати общий або організаційний ідентифікатор.

Системний менеджер включає в себе такі технології:

- керування мобільними пристроями (MDM)
- керування мобільними додатками (MAM)

- керування мобільним вмістом (MCM)
- керування мобільною ідентифікацією (MIM).

Незареєстровані кінцеві точки доступу до внутрішньої мережі будуть переспрямовано на хмарну сторінку реєстрації Cisco Meraki EMM для реєстрації на основі ролі користувача, типу пристрою тощо. Крім того, Meraki також може надати пристрої корпоративного призначення такі програми, як AnyConnect (VPN), Jabber (Спільна робота) тощо, щоб користувач мав безпечний доступ до корпоративних ресурсів, коли пристрій знаходиться на вулиці. Невідповідні кінцеві точки будуть надаватися обмежено доступ на основі статусу відповідності. Періодична перевірка відповідності хмарному серверу Cisco Meraki EMM. Можливість для адміністраторів ISE віддалено вносити зміни пристроїв через хмару Cisco Meraki EMM. Можливість кінцевого користувача використовувати порт ISE My для керування персональними пристроями. Наприклад, повне видалення, корпоративне видалення та блокування PIN-коду. Для віддаленого моніторингу мережі існує продукт Meraki Insight розроблено, щоб надати клієнтам Meraki легкий спосіб легко контролювати продуктивність веб-додатків у їхніх мережах визначення можливих проблем, викликаних мережею або програмою. Це інформація представлена у вигляді серії простих для розуміння графіків і діаграм, які чітко показують, де виникають проблеми з продуктивністю локальної мережі або якщо проблема з продуктивністю наслідком чогось на рівні програми або WAN. Існує два основних типи розпорядників інформації, панелі: організація та мережа. Адміністратори організації мають повний доступ до їх організація та всі її мережі. Цей тип облікового запису еквівалентний до адміністратора root або домену, тому важливо уважно відстежувати, хто отримує такий рівень контролю. Адміністратори мережі мають доступ до окремих мереж та їх пристроїв. Ці користувачі можуть мати повну або обмежену контролюють конфігурацію своєї мережі, але не мають

доступу до інформації на рівні організації (ліцензування, інвентаризація пристроїв тощо).

Гостьовий доступ: користувач може бачити список користувачів Аутентифікація Meraki, додавання користувачів, оновлення існуючих користувачів і авторизувати або видаляти користувачів за ідентифікатором SSID або VPN клієнт.

Монітор: користувач може переглядати лише підмножину розділ «Монітор» на панелі інструментів і не вносити жодних змін це заборонено.

Лише читання: користувач має доступ до більшості аспектів мережі, включаючи розділ «Налаштування», але не може вносити жодних змін.

Повний: користувач має доступ до налаштувань для всіх аспектів мережі та можна вносити в нього будь-які зміни.

5.2 Захист WLAN

Мережева стратегія Cisco Self Defending Network (SDN) пропонує механізм захисту від загроз безпеки, пов'язаних із впровадженням бездротових технологій, що базується на радикальному вдосконаленні здатність мережі автоматично виявляти, запобігати та адаптуватися до загроз безпеки. Який є У рамках цієї стратегії модель уніфікованої бездротової мережі Cisco надає комплексне рішення для захисту дротової мережі від бездротові загрози; і безпечний, конфіденційний зв'язок через авторизовану WLAN. Кожен мережевий пристрій - від клієнтів і точок доступу до бездротових контролерів і систем адміністрування - відіграє роль у забезпеченні безпеки інфраструктури бездротової мережі в межах розподілений механізм захисту. Мобільна природа бездротової мережі вимагає багатошарового підходу до безпеки. Щоб зменшити ризики безпеки мережі, пов’язані з

бездротовими загрозами, Cisco Systems рекомендує виконати дію п'ять кроків нижче: z Створіть політику безпеки для WLAN. z Забезпечте безпеку мережі WLAN. Захистіть дротову мережу (Ethernet) від бездротових загроз. z Захист організації від зовнішніх загроз. z Мобілізуйте працівників для захисту мережі. У цьому документі розглядаються найкращі методи захисту вашої мережі - як дротової, так і бездротовий - проти несанкціонованого використання через WLANз'єднання в контексті кожного з п'яти перерахованих точки. Ці методи повинні бути узгоджені з процесами управління ризиками в організації та доповнений ефективним практичним механізмом безпеки. Поєднання цих заходів дозволить убезпечити себе організації від нецільового використання ресурсів і крадіжки інформації, а також захистити репутацію своєї компанії перед клієнтами та партнерами. Якщо ви хочете отримати комплексну оцінку стану справ у сфері мережі безпеки для вашої організації, консультанти Cisco Advanced Services можуть проаналізувати рівень безпеки мережі відповідно до найкращих практик галузі та визначити вразливі місця, які можуть загрожувати. На основі результатів ретельного аналізу Cisco надасть рекомендації щодо покращення загального рівня мережі безпеки та надасть перелік дій, пріоритетних та призначених для виправлення ситуації у сфері безпеки. Звичайно, ці дії повинні бути доповнені жорсткою політикою управління контроль доступу та інші заходи безпеки в мережі.

За останнім часом масштаби інфраструктур WLAN значно зросли. Досить багато інфраструктур WLAN недостатньо безпечні що дає можливість зловмисникам втручатися в роботу мережі. Підтримувати безпеку WLAN не легке завдання. Після появи об'єднаної бездротової мережі Cisco зробили це завдання легше. Процес мережевої безпеки базується на розширенні стратегії Cisco Self Defending Network що має три основні елементи: безпечні комунікації, контроль та нейтралізацію загроз, дотримання політики та відповідність вимогам.

5.3 Переліку обладнання, що буде використано.

1 маршрутизатори, 3 комутаторів, 3 сервери, 2 точки доступу Wi-Fi Комутатори працюють на рівнях "доступу" та "розподілу", вони комутують пакети між користувачами як з однієї підмережі VLAN, так і з різних. Маршрутизатор забезпечує маршрутизацію пакетів між різними фізичними мережами, вихід до Інтернету, а також віддалений доступ для адміністратора. Сервер є високопродуктивною робочою станцією і налаштовується під потреби користувачів організації. Він може представляти як файлове сховище, центр обробки даних, DHCP-сервер, сервер камер відеоспостереження тощо.

Точка доступу Wi-Fi використовує ЕМВ певної частоти, щоб надати користувачам доступ до локальної мережі. Устаткування настроюється на IPv4 або IPv6. Ми налаштовуємо ваше обладнання для адресації протоколів IPv4, а також більш сучасного IPv6. Розбиття локальної мережі на віртуальні локальні підмережі VLAN Ця технологія дозволяє гнучко налаштувати використання мережевих ресурсів залежно від завдань користувачів конкретного VLAN.

Маршрутизація між мережами VLAN при введенні VLAN необхідно налаштувати маршрутизацію, щоб користувачі з різних підмереж могли взаємодіяти один з одним. У цьому бюджетному рішенні застосовується статична маршрутизація, що підходить для малих підприємств, у яких рідко з'являються та/або видаляються пристрої. Налаштування протоколу STP (зокрема, Rapid STP та PVST) STP - сімейство мережевих протоколів, призначених для автоматичного видалення циклів (петлі комутації) з топології мережі на канальному рівні в Ethernet-мережах. Ця технологія стає актуальною за умов наявності рекурсивних шляхів комутації лише на рівні розподілу. Такі ситуації притаманні середнім та великим підприємствам. Налаштування протоколу EtherChannel ця технологія

дозволяє збільшити пропускну здатність лінії лише на рівні розподілу шляхом агрегування кількох фізичних каналів на один віртуальний.

Налаштування протоколу SSHv2. Цей протокол використовується для забезпечення безпечного віддаленого доступу Налаштування безпеки від мережевих атак на рівні L2.

Динамічна маршрутизація між мережами Маршрутизація - процес визначення кращого шляху, яким пакет може бути доставлений одержувачу. Вибір протоколу маршрутизації стає актуальним середніх і великих підприємствах, адже неправильна конфігурація може позначитися якості обслуговування. У цьому рішенні застосовується протокол EIGRP – удосконалений дистанційно-векторний протокол динамічної маршрутизації, розроблений компанією Cisco динамічний протокол маршрутизації. Налаштування зв'язку з провайдером Для підприємства середніх та великих розмірів не підходить стандартне з'єднання з провайдером для забезпечення співробітникам та гостям доступу в інтернет, тому для нього також потрібне тонке налаштування. Налаштування віддаленого доступу адміністратора за протоколом SSHv2 У разі неполадок мережі мережному адміністратору не обов'язково знаходиться поруч із обладнанням - ви можете надати йому віддалений доступ за безпечним протоколом SSHv2.

Протокол DHCP дозволяє пристроям у мережі автоматично отримувати IPадресу та інші параметри, необхідні для роботи в цій мережі. Налаштування розширених списків контролю доступу ACL. Списки контролю доступу є список правил обробки мережного пакета, визначальний необхідні дії щодо його обробки. Списки контролю доступу корисні для фільтрації, пріорітизації інформації, а також її вибіркової обробки в залежності від необхідності. Перевага розширених ACL полягає в тому, що вони можуть перевіряти адреси джерел, а також адреси одержувачів, якщо IP ще тип протоколу і TCP/UDP порти, а не тільки адреси джерел Налаштування бездротової локальної мережі Wi-FI Гостьова локальна мережа

ізольована від внутрішньої мережі організації в окремому VLAN. Відвідувачі отримують ip-адресу, адресу сервера DNS і маршрут за замовчуванням від DHCP-сервера.

Протокол NAT забезпечує трансляцію мережевих адрес - змінює адрес в заголовках IP-пакетів при їх проходженні через маршрутизатор або інший пристрій. Зокрема замінює внутрішню IP адресу пристрою локальної мережі на одну єдину, видану провайдером, зовнішню IP адресу. Використання цього протоколу дозволяє виходити користувачам локальної мережі в Інтернет. Налагодження зв'язку між філіями. Проводиться об'єднання кількох філій у межах міста у масштабну локальну мережу - WAN. Для забезпечення надійності також налаштовується резервний канал зв'язку між IP-телефонія Дана технологія дозволяє використовувати голосовий зв'язок, трафік якого рівноцінний будь-якому іншому внутрішньому трафіку.

ТРЕТІЙ РОЗДІЛ

6 Логічна схема побудови мережі

Спроектовано логічну схему мережі. Логічна мережева схема ілюструє потік інформації через мережу та відображає комунікацію між пристроями.

Вона містить такі елементи, як підмережі, пристрої та об'єкти мережі, протоколи маршрутизації, голосові шлюзи, потоки трафіку та сегменти мережі.

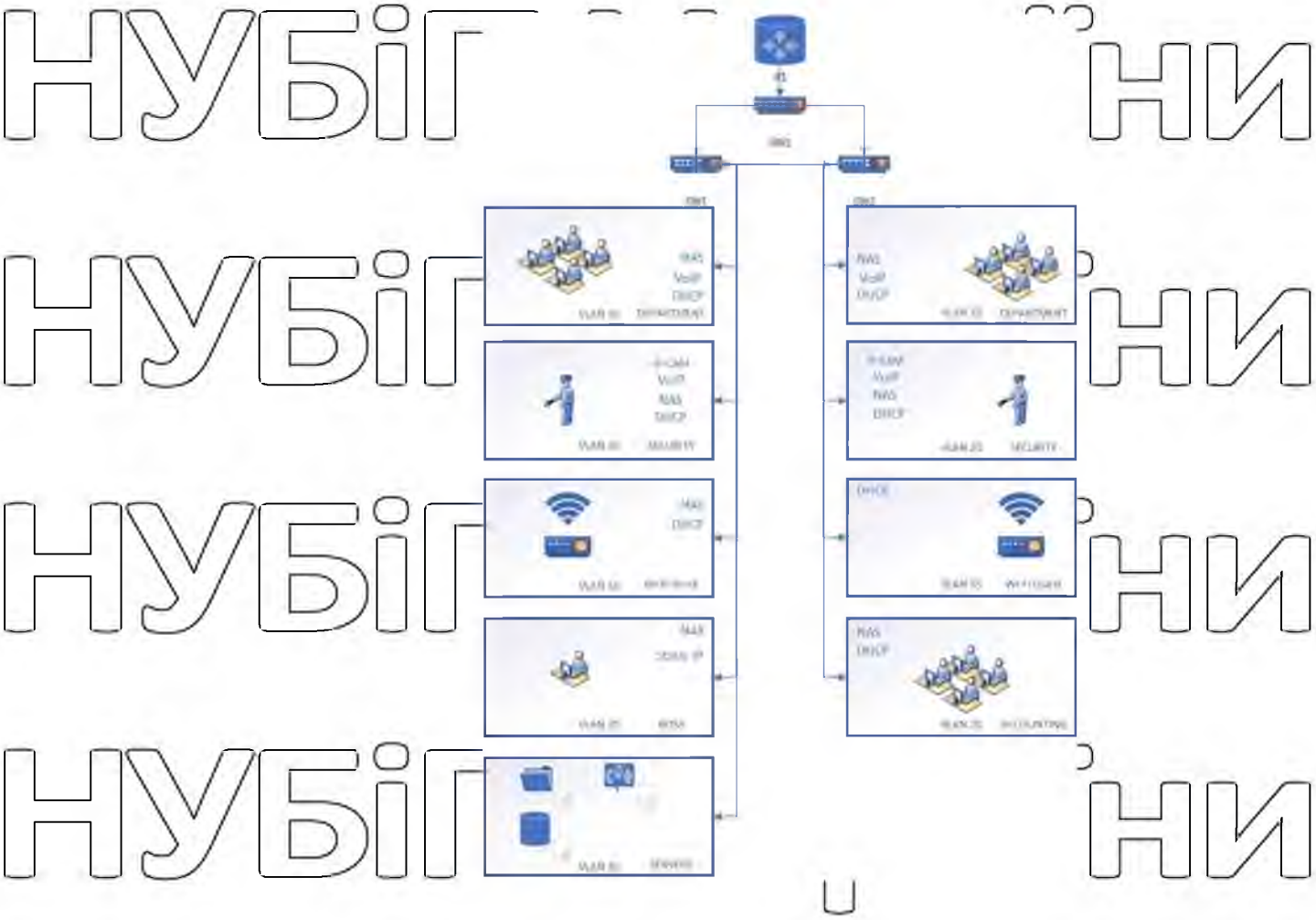


Рисунок 6.1 – Логічна схема мережі

Vlan 10 може пінгувати хости з vlan 10 даної будівлі та звертатись до Server1 через web browser хост 192.1.20.3/24/ Може звертатися до хостів 192.1.40.2/24 та 192.1.20.2/24 vlan55 має можливіть www та перегляд server1 у web browser vlan 30 не має доступу до Server3,Server4 у web browser.

Налаштування протоколу STP (зокрема, Rapid STP та PVST) STP - сімейство мережевих протоколів, призначених для автоматичного видалення циклів (петлі комутації) з топології мережі на канальному рівні в Ethernetмережах. Ця технологія стає актуальною за умов наявності рекурсивних шляхів комутації лише на рівні розподілу. Такі ситуації притаманні середнім та великим підприємствам.

Налаштування протоколу EtherChannel Дана технологія дозволяє збільшити пропускну здатність лінії на рівні розподілу шляхом агрегування кількох фізичних каналів на один віртуальний.

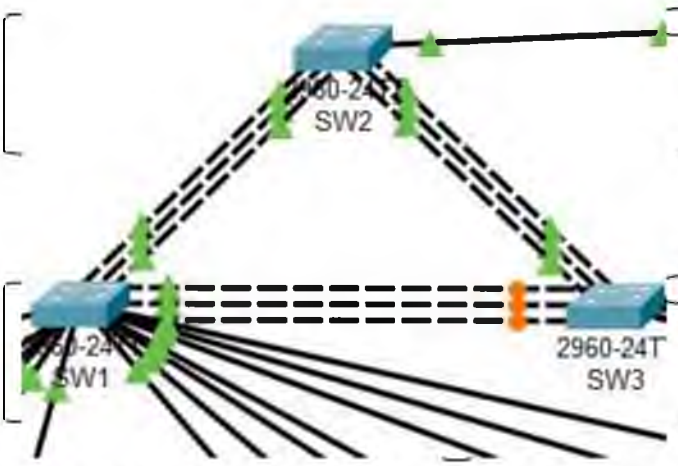


Рисунок 6.2 – агрегування каналів передачі даних

Налаштування протоколу SSH Цей протокол використовується для забезпечення безпечного віддаленого доступу.

Налаштування безпеки від мережевих атак на рівні L2 Перегляньте перелік загроз, від яких реалізується захист ви можете тут. Динамічна маршрутизація між мережами Маршрутизація - процес визначення кращого шляху, яким пакет може бути доставлений одержувачу. Вибір протоколу маршрутизації стає актуальним на середніх та великих підприємствах, адже неправильна конфігурація може позначитися на якості обслуговування. У цьому бюджетному рішенні застосовується протокол EIGRP – удосконалений дистанційно-векторний протокол динамічної маршрутизації, розроблений компанією Cisco динамічний протокол маршрутизації.

Налагодження зв'язку з провайдером для підприємства середніх та великих розмірів не підходить стандартне з'єднання з провайдером для

забезпечення співробітникам та гостям доступу в інтернет, тому для нього також потрібне тонке налаштування.

Налаштування віддаленого доступу адміністратора за протоколом SSH

У разі неполадок мережі мережному адміністратору не обов'язково знаходиться поруч із обладнанням - ви можете надати йому віддалений доступ за безпечним протоколом SSH.

Налаштування протоколу DHCP Протокол DHCP дозволяє пристроям у мережі автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в цій мережі.

Налаштування розширених списків контролю доступу ACL Списки контролю доступу являють собою список правил обробки мережного пакета, що визначає необхідні дії для його обробки. Списки контролю доступу корисні для фільтрації, пріорітизації інформації, а також її вибіркової обробки в залежності від необхідності. Перевага розширених ACL полягає в тому, що вони можуть перевіряти адреси джерел, а також адреси одержувачів, у разі IP ще тип протоколу та TCP/UDP порти, а не тільки адреси джерел.

Налаштування бездротової локальної мережі Wi-FI Гостьова локальна мережа ізольована від внутрішньої мережі організації в окремому VLAN'і. Відвідувачі отримують ip-адресу, адресу DNS сервера та маршрут за замовчуванням від DHCP-сервера.

Налаштування протоколу NAT Протокол NAT забезпечує трансляцію мережевих адрес - змінює адрес в заголовках IP-пакетів при їх проходженні через маршрутизатор або інший пристрій. Зокрема замінює внутрішню IP адресу пристрою локальної мережі на одну єдину, видану провайдером, зовнішню IP адресу. Використання цього протоколу дозволяє виходити користувачам локальної мережі в Інтернет.

Лістинг 6.1 – команди налаштування NAT протоколу

```
Router(config)# ip nat inside source static 192.168.1.5 208.165.100.5
Router(config)# interface serial0/0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)# interface serial0/1/0
Router(config-if)#ip nat outside
```

В результаті трансляції проходитимуть так:

Клієнт хоче відкрити з'єднання з веб-сервером. Клієнт відправляє пакет на веб-сервер, використовуючи загальнодоступну IPv4-адресу призначення 208.165.100.5. Це внутрішня глобальна адреса веб-сервера.

Перший пакет, який роутер отримує від клієнта зовнішньому інтерфейсі NAT, змушує його перевіряти свою таблицю NAT. Адреса IPv4 адресата знаходиться в таблиці NAT, він транслюється.

Роутер замінює внутрішній глобальний адрес призначення 208.165.100.5 внутрішнім локальним 192.168.1.5 і пересилає пакет до веб-сервера.

Веб-сервер отримує пакет і відповідає клієнту, використовуючи внутрішню локальну адресу джерела 192.168.1.5.

Роутер отримує пакет із веб-сервера на свій внутрішній інтерфейс NAT з адресою джерела внутрішньої локальної адреси веб-сервера, 192.168.1.5. Він перевіряє NAT таблицю для переведення внутрішньої локальної адреси у внутрішній глобальний, змінює адресу джерела з 192.168.1.5 на 208.165.100.5 та відправляє його з інтерфейсу Serial 0/1/0 у бік клієнта.

Клієнт отримує пакет і обмін пакетами триває. Роутер виконує попередні кроки кожного пакета.

Таблиця 6.1 – Довідкові термінали

Довідкові термінали					
Системні блоки					
№	Комплектуючі	Модель	Ціна	Кількість	Загальна вартість
	Процессор	Intel Celeron G1820 BOX 2,8Ghz	2500,00	8	20000
	Материнска плата	GIGABYTE GA-H81M-S1	3100,00	8	24800
	Оперативна память	Crucial [CT4G4DFS8213] 4 ГБ	1850,00	8	14800
	HDD	WD Caviar Blue [WD10EZEX] 1TB	3350,00	8	26800
	Відеоадаптер	Інтегрований	0,00	0	0
	Блок живлення	Aerocool Vx-350 [VX-350]	1400,00	8	11200
1.	Корпус	CaseCom CJ-39	1650,00	8	13200
	Ціна кофігурації				13850,0

Таблиці 6.2 - Вартість обладнання «Директор»

Директор					
ПК					
№	Комплектуючі	Модель	Ціна	К-л.	Вартість
	Процессор	Intel Pentium G4400 BOX 3	4200,00	1	4200
	Материнська плата	MSI H110M PRO-VD PLUS	3450,00	1	3450
	RAM	Crucial [CT4G4DFS8213] 4	1850,00	1	1850
	HDD	WD Caviar Blue [WD10EZEX]	3350,00	1	3350
1	Блок живлення	Aerocool Vx-350 [VX-350]	1400,00	1	1400
Периферия					
№	Назва	Модель	Ціна	Кількість	Загальна сума
1	Монітор	AOC E975SWDA 19"	5500	1	5500
2	Клавіатура	CBR KB 300M	370	1	370
3	Мишка	Oklick 115S	210	1	210
4	IP телефон	Cisco IP Phone CPV7942G	15500	1	15500

Ціна комплекту	34880
Загальна ціна	34880

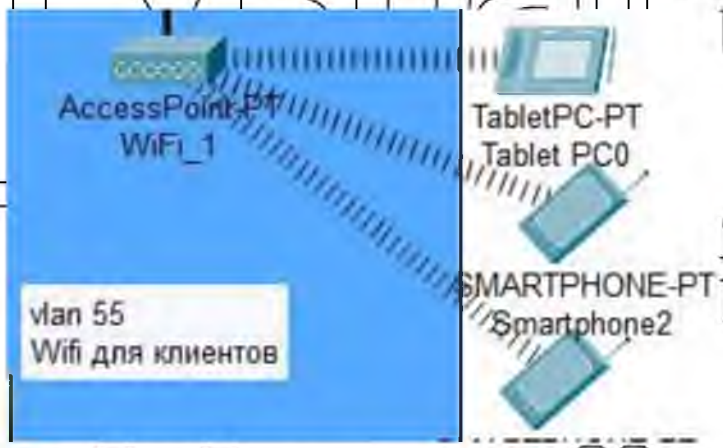


Рисунок 6.2 - Vlan 55 - це логічна побудова мережі з Wi-Fi точкою доступу для виходу в інтернет клієнтів проектованої мережі

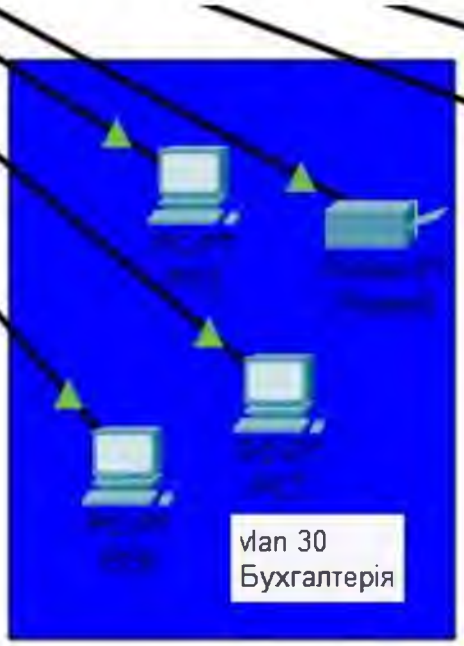


Рисунок 6.5 - Vlan 30 відділ бугалтерії

Таблиці 6.3 - Вартість обладнання «Бухгалтерія»

Бухгалтерія				
ПК				
Комплектуючі	Модель	Вартість	Кількість	Загальна вартість
Процессор	Intel Pentium G4400 BOX 3,3Ghz	4200,00	3	12600
Материнская плата	MSI H110M PRO-VD PLUS	3450,00	3	10350
RAM	Crucial [CT4G4DFS8213] 4 ГБ	1850,00	3	5550

HDD	WD Caviar Blue [WD10EZEX] 1TB	3350,00	3	1 0050
Відеоадаптер	Встроенное	0,00	3	0
Блок питания	Aerocool Vx-350 [VX-350]	1400,00	3	4 200
Корпус	CaseCom CJ-39	1650,00	3	4 950
Вартість одної конфігурації				1 5900,0
Загальна вартість				4 7700
Переферія				
Назва	Модель	Вартість	Кількість	Загальна вартість
Монітор	AOC E975SWDA 19"	5500	3	1 6500
Клавіатура	CBR KB 300M	370	3	1 110
Мишка	Oklick 115S	210	3	6 30
Мережевий принтер	Pantum M6550NW	8200	1	8 200
IP телефон	Cisco IP Phone CP-7942G	15500	3	4 6500
Вартість одного комплекту				2 9780

Загальна вартість					7 2940
Провода для подключения к сети					
	Местона хождение узла	Длина кабеля по ширине, М	Длина кабеля по высоте, М	Кабель в запас	Стоимость
	Принтер	6	4	0,5	1 57,5
	Первый увел	7,5	4	0,57 5	1 81,125
	Второй этаж зал	9,5	4	0,67 5	2 12,625
	Второй этаж склад	9,5	4	0,67 5	2 12,625
Общая стоимость кабелей					7 63,875
Итого					1 21403,875

Рисунок 6.6 зображує логічну топологію мережі таких елементів як Vlan 20 – пунк охорони. Містить ПК та IP телефон. Vlan 10 – кабінет для працівників з робочими машинами та відеонаглядом. Vlan 55 – точка доступу WiFi для клінтів компанії.

Таблиця 6.3 – Розрахунок вартості обладнання

Охорона

Системные блоки

№	Комплектующе	Модель	Ціна	Кількість	Сума
1	Процессор	Intel Pentium G4400 BOX 3,3Ghz	4200,00	1	4200
	Материнская плата	MSI H110M PRO-VD PLUS	3450,00	1	3450
	Сперативная память	Crucial [CT4G4DFS821 3] 4 ГБ	1850,00	1	1850
	HDD	WD Caviar Blue [WD10EZEX] 1TB	3350,00	1	3350
	Видеоадаптер	Встроенное	0,00	0	0
	Блок питания	Aerocool Vx-350 [VX-350]	1400,00	1	1400
	Корпус	CaseCom CJ-39	1650,00	1	1650
	Общая стоимость системных блоков			0	15900

Переферія					
№	Наименование	Модель	Стоимость	Количество	Общая стоимость
1	Монитор	AOC E975SWDA 19"	5500	1	5500
2	Клавиатура	CBR KB 300M	370	1	370
3	Мышь	Oklick 115S	210	1	210
4	IP телефон	Cisco IP Phone CP-7942G	15500	1	15500
Стоимость одного комплекта					21880
Полная стоимость перефирии					21580
Провода для подключения к сети					
№	Местонахождение узла	Длина кабеля по ширине, М	Длина кабеля по высоте, М	Кабель в запас	Стоимость
1	Узел охранника	12	4	0,8	252
Общая стоимость кабелей					252
Итого					37732

Сервер

Сервер на базе Asus ESC500 G4 SATA Для видеонаблюдения

№	Комплектующие	Модель	Стоимость	Количество	Общая стоимость
1	Процессор	Intel Xeon E5-2550 v5 2,6Ghz	50000,00	1	50000
	Материнская плата	Asus	40000,00	1	40000
	Оперативная память	ELPIDA 8 ГБ buffered	6800,00	1	6800
	HDD	WD NAS HDD 4 TB	5000,00	4	20000
					71800

Сервер на базе HP ProLiant ML10 Gen9

№	Комплектующие	Модель	Стоимость	Количество	Общая стоимость
2	Процессор	Intel Xeon E3-1225v5 3,3Ghz	34700,00	1	34700
	Материнская плата	MSI H110M PRO-VD PLUS	3450,00	1	3450

	Оперативная память	HP 8 ГБ buffered	8500,00	2	17000
	HDD	HP 2TB 6GB SATA	4500,00	4	18000
	Общая стоимость сервера				216750
	Переферія				
№	Наименование	Модель	Стоимость	Количество	Общая стоимость
1	Монитор	AOC E975SWDA 19"	5500	2	11000
2	Клавиатура	CBR KB 300M	370	2	740
3	Мышь	Oklick 115S	210	2	420
4	Датчик температуры	ESM-10	3800	1	3800
5	Нагреватель	FLH-150	6000	1	6000
6	Кондиционер	Electrolux EACS 09HG/N3	16000	1	16000
	Стоимость одного комплекта				31880

Полная стоимость периферии					3796
Провода для подключения к сети					
№	Местонахождение узла	Длина кабеля по ширине, М	Длина кабеля по высоте, М	Кабель в запас	Стоимость
1	Узел охранника	9,6	4	0,68	214,2
Общая стоимость кабелей					214,2
Итого					3267 24,2

Сетевое оборудование

№	Наименование	Модель	Стоимость	Количество	Общая стоимость
1	Маршрутизатор	Cisco 2811	80000	2	160000
2	Коммутатор	Cisco 2960v24	3700	3	11100
3	Платы расширения	Cisco nm-4e	1200	1	1200
4	Wi-fi точка доступа	Cisco WRT300N	2500	2	5000
Провода для подключения к сети					

№	Местонахождение узла	Длина кабеля по ширине, М	Длина кабеля по высоте, М	Кабель в запас	Стоимость
1	Серверная	85	10	4,75	1496,25
Общая стоимость кабелей					1496,25
Общая стоимость					27869 6,25

Прочие расходы

№	Наименование	Модель	Стоимость	Количество	Общая стоимость
1	Кабель-каналы	Элекс р 60*40мм*2м	150	80	12000
2	Шурупы и дюбеля	6x60	15	350	5250
3	Штекер RJ45	5E 8P8C	7	44	308
4	IP камера	TP-LINK NC200	2450	2	4900
5	Кофеварка	De'Longhi Dinamica ECAM 350.55	7800	1	7800
6	Кондиционер	Delfa ACM-12 IP	17800	1	17800

7	Нагреватель	ФЦН 015 IP 44		2500	1	2500
8	Провода для подключения камер	Витая пара		15	20	300
	Сумма прочих расходов				8	5085
	Итого					9855 34,275

7 Параметри захисту мережі

7.1 Захист віддаленого доступу

Якщо у в компанії вже налаштовано віддалений доступ, наприклад, за допомогою Telnet знадобиться захистити дані, що передаються через цей канал. Це можна реалізувати через протокол SSH, що забезпечує віддалений доступ, захищаючи дані, що передаються. Щоб продемонструвати цю технологію, візьмемо приклад мережі з технології Віддалений доступ На комутаторах у прикладі необхідно прописати ряд команд для налаштування протоколу SSH. На рисунку 7.1.1 можна переглянути приклад налаштування протоколу SSH для комутатора у програмі PacketTracer.

Спочатку необхідно перевірити, чи підтримується протокол на обладнанні. Це можна зробити командою: show ip ssh. Якщо ваше обладнання не підтримує криптографічні функції, а, отже, і протокол SSH, то дана команда не розпізнається.

Потім надаємо ім'я ip домену мережі за допомогою команди: Ip domainname ocsic У цій команді для прикладу вибрали ім'я ocsic. Потім створюємо пари ключів RSA командою: Crypto key generate rsa Потім нам

потрібно вибрати довжину блоку. Cisco рекомендує вибирати довжину блоку щонайменше 1024 біт. Більш довгий модуль безпечніший, але вимагає більше часу для його створення та використання, тому при виборі розміру враховуйте ваші умови, щоб вибрати найбільш відповідний блок. Потім необхідно увімкнути протокол SSH на каналах vty. Робиться це з допомогою наступних команд: line vty 0 15 – вибираються канали для налаштування, у цьому прикладі вибрано канали з 0 по 15 transport input ssh – включається протокол ssh на вибраних каналах Ця конфігурація дозволяє приймати підключення тільки по протоколу SSH та виключає інші протоколи (наприклад, Telnet). Потім необхідно увімкнути другу версію протоколу, щоб уникнути ряду відомих уразливостей першої версії. Друга версія протоколу включається наступною командою: IP ssh version 2.

```
SW1(config)#ip domain-name ocsic
SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.ocsic
Choose the size of the key modulus in the range of 360 to 2048
for your
  General Purpose Keys. Choosing a key modulus greater than 512
may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK]

SW1(config)#line vty 0 15
*??? 1 0:39:36.972:  %SSH-5-ENABLED: SSH 1.99 has been enabled
SW1(config-line)#transport input ssh
SW1(config-line)#login local
SW1(config-line)#exit
SW1(config)#ip ssh version 2
SW1(config)#exit
```

Рисунок 7.1

7.2 Атака MAC-Spoofing

Підміна MAC-адреси на мережній карті комп'ютера, що дозволяє йому перехоплювати пакети, адресовані іншому пристрою, що у тому ж широкомовному домені.

У таблиці MAC-адрес комутатора запис з атакованою MAC-адресою буде співвіднесений з інтерфейсом, на якому востаннє було ідентифіковано кадр з даною source MAC-адресою.

Як результат, до надходження кадру з пристрою, що атакується, всі дані комутатор, відповідно до своєї таблиці MAC-адрес, буде пересилати на атакуючий пристрій.

Захистити мережу від цієї атаки можна за допомогою налаштування портів комутатора, використовуючи такі команди:

- Switch(config-if)#switchport mode aecess
- Switch(config-if)#switchport port-security - увімкнення безпеки порту на інтерфейсі
- Switch(config-if)#switchport port-security mac-address 0000.1111.1111 - встановлення на інтерфейсі безпечної статичної MAC-адреси вручну.

7.3 DHCP starvation (виснаження ресурсів DHCP)

Атака, здійснювана з допомогою протоколу DHCP. DHCP-пул, з якого клієнти отримують IP-адреси, обмежений. Наприклад, це може бути 253 адреси (при масці 255.255.255.0).

Дії, які здійснюються при атаці: Атакуючий пристрій запитує IP-адресу у DHCP-сервера і отримує його; MAC-адреса атакуючого пристрою

змінюється і він запитує наступну, вже іншу IP-адресу, маскуючись під нового клієнта. Такі дії повторюються, поки весь пул IP-адрес на сервері не буде вичерпаний. Як результат цієї атаки можна виділити наступне: Відмова у обслуговуванні. Проведення атаки DHCP-spoofing із ймовірністю успіху 100%.

Методи захисту від цієї атаки. Захистити мережу від цієї атаки можна за допомогою налаштування портів комутатора, використовуючи такі команди: Switch(config-if)#switchport mode access

- Switch(config-if)# switchport port-security - увімкнення безпеки порту на інтерфейсі
- Switch(config-if)# switchport port-security maximum value - встановлення максимальної кількості безпечних MAC-адрес для інтерфейсу. Діапазон становить від 1 до 3072; за замовчуванням 1
- Switch(config-if)# switchport port-security mac-address sticky - включення навчання порту та збереження MAC-адрес у конфігураційний файл.
- Switch(config-if)# switchport port-security violation {restrict | shutdown} - встановлює дію, яку необхідно вжити при виявленні порушення безпеки. restrict - обмеження даних та виклик SecurityViolation для збільшення лічильника та надсилання повідомлення. shutdown - відключення інтерфейсу у разі порушення безпеки.
- Switch(config-if)# ip dhcp snooping limit rate <1-2048> - встановлює обмеження кількості пакетів порт, при перевищенні тимчасово вимикає порт. Таким чином можна виявити нелегітимний пристрій, який генерує та посилає безліч пакетів.

7.4 Атака з подвійним тегуванням (або подвійною інкапсуляцією)

Даний вид атаки ґрунтується на використанні принципів роботи апаратного забезпечення на більшості комутаторів. Більшість комутаторів виконують лише один рівень деінкапсуляції 802.1Q, що дозволяє зловмиснику вставляти у кадр приховану мітку 802.1Q. Мітка дозволяє пересилати кадр у мережу VLAN, яка не вказана початковою міткою 802.1Q. Важлива властивість атаки з подвійною інкапсуляцією полягає в тому, що вона діє, навіть якщо транкові порти відключені, оскільки вузол зазвичай відправляє кадр у сегменті, який не є транковим каналом.

Дії, які здійснюються при атаці. Зловмисник відправляє на комутатор кадр із подвійним тегуванням 802.1Q. Зовнішній заголовок містить мітку VLAN зловмисника, яка збігається з native VLAN транкового порту. Передбачається, що комутатор обробляє отриманий від зловмисника кадр, ніби він перебуває в транковом порту чи порті з голосової VLAN (комутатор ні отримувати тегований кадр Ethernet на порту доступа). Як приклад уявіть, що мережею native VLAN є VLAN 10. Внутрішній тег - це VLAN, яка піддається атаці. В даному випадку – VLAN 20.

Кадр прибуває на комутатор, який перевіряє перші 4 байти тега 802.1Q. Комутатор бачить, що кадр призначений для VLAN 10 яка є мережею native VLAN. Видавши мітку VLAN 10, комутатор пересилає пакет із усіх портів мережі VLAN 10. На транковому порті видаляється мітка мережі VLAN 10, але пакет не тегується заново, оскільки він є частиною native VLAN. У цей час мітка мережі VLAN 20, як і раніше, недоторкана і не перевіряється першим комутатором. Другий комутатор перевіряє лише внутрішній тег 802.1Q, відправлений зловмисником, і бачить, що кадр призначений для мережі VLAN 20, яка є метою зловмисника.

Другий комутатор відправляє кадр на атакований порт або наповнює його лавинною розсилкою залежно від того, чи є в таблиці MAC-адрес запис для вузла, що атакується. Цей вид атаки є односпрямованим і працює, тільки якщо зловмисник підключений до порту, який знаходиться в тій же VLAN, що і мережа native VLAN транкового порту. Запобігти такій атаці не так легко, як зупинити звичайні атаки VLAN hopping. Методи захисту від цієї атаки. Найкращий спосіб зниження шкоди від атак з подвійним тегуванням — переконатися, що мережа native VLAN транкових портів відрізняється від VLAN будь-яких портів користувача. Рекомендується використовувати фіксовану VLAN, яка відрізняється від всіх власних VLAN в комутованій мережі, як мережа native VLAN для всіх транкових каналів 802.1Q.

8 Алгоритм проектування локально обчислювальних мереж.

Вихідні дані. Важливість цього пункту пов'язана з необхідністю впорядкування вимог до створюваної ЛЗ та її окремих елементів для забезпечення можливості прийняття у майбутньому конкретних рішень. При створенні нової мережі для якогось підприємства необхідно враховувати:

- особливості інформації, що передається по мережі (дані, оцифрована мова, зображення), які позначається на потрібній швидкості передачі;
- технічні характеристики апаратного забезпечення (комп'ютерів, адаптерів, кабелів, репітерів, концентраторів, комутаторів) та його вартість;
- можливості прокладання кабельної системи у приміщеннях та між ними, а також заходи забезпечення її цілісності;
- способи обслуговування мережі та контролю її безвідмовності та безпеки;

– вимоги до програмних засобів за допустимим розміром мережі, швидкості, гнучкості, розмежування прав доступу, вартості, можливостей контролю обміну інформацією та ін;

– необхідність підключення до інших мереж, глобальних або локальних.

Мережа, порівняно з автономними, локальними комп'ютерами, породжує безліч додаткових проблем. Це і найпростіші механічні (комп'ютери, підключені до мережі, важче переміщати всередині приміщення), і складні інформаційні (необхідність контролювати ресурси, що спільно використовуються, запобігати зараженню мережі вірусами). Крім того, користувачі локальної мережі вже не такі незалежні, як користувачі автономних комп'ютерів, їм необхідно дотримуватися певних правил, підкорятися встановленим вимогам, яким їх потрібно навчити. Мережева взаємодія ставить питання про безпеку інформації, захист від несанкціонованого доступу, адже з будь-якого комп'ютера мережі можна використовувати дані із спільних мережних дисків. Захистити один або кілька одиночних комп'ютерів набагато простіше, ніж локальну мережу. Тому приступати до встановлення мережі доцільно лише тоді, коли без мережі робота стає непродуктивною чи зовсім неможливою.

На початку проектування мережі необхідно виконати інвентаризацію наявного апаратно-програмного комплексу, а також зовнішніх периферійних пристроїв (принтерів, сканерів тощо). Це дозволить при створенні мережі виключити непотрібне дублювання (апаратне та програмне забезпечення можливо використовувати як ресурси, що розділяються), а також поставити завдання модернізації (апгрейду) як апаратних, так і програмних засобів. Для більш точного визначення параметрів комп'ютерів доцільно використовувати спеціальні діагностичні програми.

8.1 Вибір розміру та структури мережі

Під розміром мережі випадку розуміється як кількість комп'ютерів, що об'єднуються в мережу, так і відстані між ними. Потрібно заздалегідь визначити, скільки комп'ютерів (мінімально та максимально) необхідно об'єднати у мережу. При цьому необхідно залишати можливість подальшого збільшення їх кількості в мережі на 20–50 відсотків.

Визначення необхідної довжини ліній зв'язку мережі відіграє при проектуванні мережі. Наприклад, якщо відстані між абонентами дуже великі, може знадобитися використання дорогого обладнання. До того ж зі збільшенням довжини ліній зв'язку різко зростає значущість їхнього захисту від зовнішніх електромагнітних перешкод. Від відстані залежить швидкість передачі інформації по мережі (вибір між Ethernet і Fast Ethernet). При виборі відстаней доцільно збільшувати їх на 10 відсотків для врахування непередбачуваних обставин. Подолати обмеження за довжиною можна шляхом вибору структури мережі та розбиття її на окремі частини. Локальна мережа підприємства може поєднувати робочі групи комп'ютерів, мережі підрозділів, опорні мережі, засоби зв'язку з іншими мережами. Для об'єднання частин мережі може використовуватись різне мережеве обладнання (репітери, концентратори, комутатори, мости, маршрутизатори). Вибір структури мережі дуже важливий, оскільки часом вартість цього об'єднувального устаткування може значно перевищити вартість комп'ютерів, мережевих адаптерів і кабелю. В ідеалі структура мережі повинна відповідати структурі будівлі (його поверховому плануванню) та всього комплексу будівель підприємства. Робочі місця групи співробітників, які займаються подібними завданнями (бухгалтерія, відділ продажу, інженерна група), повинні розміщуватися в

одному або поряд розташованих приміщеннях. Тоді комп'ютери цих співробітників можна об'єднати в один мережевий сегмент і встановити біля цих приміщень сервер, з яким вони працюватимуть, а також концентратор або комутатор, який об'єднує ці абоненти. Робочі місця працівників відділу, які займаються комплексом аналогічних завдань, краще розташувати на одному поверсі будівлі, що значно спростить їхнє об'єднання в сегмент та процес адміністрування. На цьому ж поверсі логічно розмістити комутатори, маршрутизатори та сервери, з якими працює цей підрозділ.

8.2 Вибір обладнання.

При виборі мережного обладнання необхідно враховувати:

- рівень уніфікації обладнання та його сумісність із найбільш поширеним програмним забезпеченням;
- швидкість передачі інформації та перспективи її подальшого збільшення;
- топології мережі та їх можливі комбінації;
- метод управління обміном даними у мережі (CSMA/CD, повний дуплекс або маркерний метод);
- типи кабелю мережі та його основні характеристики;
- технічні характеристики та вартість апаратних засобів (мережевих адаптерів, трансіверів, репітерів, концентраторів, комутаторів).

В даний час для обладнання локальних мереж найчастіше використовується некранована кручена пара UTP. Інші, більш витратні варіанти на основі екранованої кручені пари, оптоволоконного кабелю або бездротових з'єднань використовуються у випадках, коли в цьому дійсно існує

потреба. Наприклад, оптоволокно може використовуватися для поєднання віддалених сегментів мережі без втрати швидкості.

Не менш важливе завдання – це вибір комп'ютерів. Якщо для робочих станцій або невиділених серверів зазвичай використовують ті комп'ютери, які вже є, виділений сервер бажано купувати спеціально для мережі. Краще, якщо це буде швидкодіючий спеціалізований комп'ютер-сервер, спроектований з урахуванням специфічних потреб мережі (такі сервери випускаються всіма найбільшими виробниками комп'ютерів). Вимоги до сервера:

- Максимально швидкий процесор. Типова величина тактової частоти процесора для сервера становить 2 -4 ГГц. Для більших мереж використовують багатопроцесорні сервери (від 8 процесорів);
- Великий обсяг оперативної пам'яті. Типовий обсяг оперативної пам'яті сервера зараз становить 32-256 Гб. Великий обсяг оперативної пам'яті (RAM) сервера важливіше за швидкодію мікропроцесора, так як дозволяє ефективно використовувати кешування дискової інформації, зберігаючи в пам'яті копії тих областей диска, з якими виробляється інтенсивний обмін;
- Швидкі жорсткі диски великого об'єму. Типовий розмір диска сучасного сервера становить 10-50 Тбайт. Дисководи повинні бути сумісні з мережевою операційною системою (драйвери повинні входити до набору драйверів, що постачається з операційною системою). У серверах передбачається можливість заміни дисків без вимкнення живлення сервера («гаряча заміна»);

– Спеціалізовані сервери вже мають у своєму складі мережеві адаптери з оптимальними характеристиками. Якщо сервер використовується звичайний персональний комп'ютер, то мережевий адаптер для нього необхідно вибирати найбільш швидкодіючий;

– миші, клавіатури та відеомонітори не є обов'язковим приладдям сервера, оскільки він, як правило, не працює як звичайний ПК.

Якщо є можливість вибору комп'ютерів для робочих станцій, варто вивчити питання доцільності використання бездискових робочих станцій (із завантаженням операційної системи через мережу). Це значно знизить вартість мережі в цілому або дозволить за тих же витрат придбати робочі станції з кращими характеристиками.

Для будь-якої мережі дуже критична ситуація перебоїв її електроживлення. Незважаючи на те, що багато мережних програмних засобів застосовують спеціальні заходи проти цього, як і проти інших відмов апаратури (дублювання дисків, автозбереження), проблема досить серйозна. Вимкнення живлення може повністю вивести комп'ютерну мережу з ладу. Захищеними від відключення живлення повинні бути всі сервери мережі, а в ідеалі та робочі станції.

Перераховано лише частину проблем, крім яких проектувальнику мережі доводиться вирішувати завдання, пов'язані з вибором мережевих адаптерів, репітерів, концентраторів, комутаторів, маршрутизаторів та іншого обладнання. Варто відзначити, що продуктивність мережі та її надійність визначаються компонентом з найнижчою якістю, бажано, щоб усі вони максимально відповідали один одному.

При виборі мережного програмного забезпечення треба враховувати наступні фактори:

- яку мережу підтримує програмне забезпечення: однорангову, мережу на основі сервера або обидва ці типи;
- максимальна кількість абонентів (із запасом не менше ніж 20%);
- типи та кількість серверів;
- сумісність із різними апаратно-програмними платформами, а також з іншими мережевими засобами;
- Оптимальний рівень продуктивності ПЗ у різних режимах роботи;
- надійність роботи, режими доступу та ступінь захисту даних;
- вартість програмного забезпечення, його експлуатації, обслуговування та модернізації.

Ще до встановлення мережі необхідно вирішити питання щодо її керування. Навіть у разі одноранговоі мережі краще виділити для цього окремого спеціаліста (адміністратора), який матиме вичерпну інформацію про конфігурацію мережі та розподіл ресурсів, а також слідкувати за коректним її використанням усіма користувачами. Якщо мережа велика, то забезпечення її функціонування крім мережного адміністратора потрібна група високопрофесійних фахівців.

ВИСНОВКИ

Результати, отримані в магістерській роботі, є рішенням практичної задані підвищення ефективності алгоритмів проектування локально обчислювальної мережі торгівельної компанії. Отримано такі теоретичні та практичні результати:

1. Проведено аналіз алгоритмів проектування локально обчислювальних мереж;
2. На основі аналізу виявлено їх основні недоліки та напрями удосконалення;
3. Проведено дослідження, в результаті якого спроектовано локально обчислювальну мережу для торгової компанії відповідно до її потреб описаних в магістерській роботі;
4. Розроблено мережеву топологію, алгоритм роботи;
5. Візуально змодельовано та зімітовано комп'ютерну мережу, що демонструє основне застосування та характеристики алгоритму.

Таким чином, всі поставлені в роботі задачі виконані й мета досягнута.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2001. – 172 с.
2. Джеймс Челлис Основы построения сетей: Учебное пособие для специалистов MCSE 1.0. – СПб.: Питер, 1997. – 326 с.
3. IP Калькулятор [Электронный ресурс] – Режим доступа : URL : http://ip-calculator.ru/. – Загл. с экрана.

4. Li-Fi: световая замена Wi-Fi [Электронный ресурс] // Хакер. – 2011, 01 августа.

5. IP Video System Design Tool : програма проектування систем відеоспостереження [Електронний ресурс] // Інтернет-магазин софта «AllSoft». – Режим доступу : URL : http://allsoft.ua/program_page.php3grp=120862. – Загол. з екрану.

6. IP Калькулятор [Электронный ресурс] – Режим доступа : URL :http://ip-calculator.ru/. – Загл. с экрана.

7. Li-Fi: световая замена Wi-Fi [Электронный ресурс] // Хакер. – 2011, 01 августа. – Режим доступа : URL : http://www.xakep.ru/56357. –

8. Multi 9. Оборудование для распределительных сетей низкого напряжения на токи от 0,5 до 125 А [Электронный ресурс] // Каталог оборудования компании Schneider Electric в Украине (M9-CAT2002UA). – Режим доступа : URL : www.schneider-electric.com.ua. –Загл. с экрана.

9. Netgear представила двухпортовый наноадаптер Powerline XAVB2602 [Электронный ресурс] // Новостной портал «SiteUA». –Режим доступа : URL : http://goo.gl/ie0etm. – Загл. с экрана.

10. PowerLine – отличная замена перегруженной беспроводной связи [Электронный ресурс] // Веб-сайт фирмы D-Link. – Режим доступа : URL : http://dlink.ru/ru/faq/266/1203.html. – Загл. с экрана.

11. PLANET : сетевые решения для телекома [Электронный ресурс] // Веб-сайт фирмы PLANET Technology Corporation. – Режим доступа : URL : http://www.planet.com.tw/en/Application/Telecom.php. –Загл. с экрана.

12. RFC 1517. Applicability Statement for the Implementation of Classless

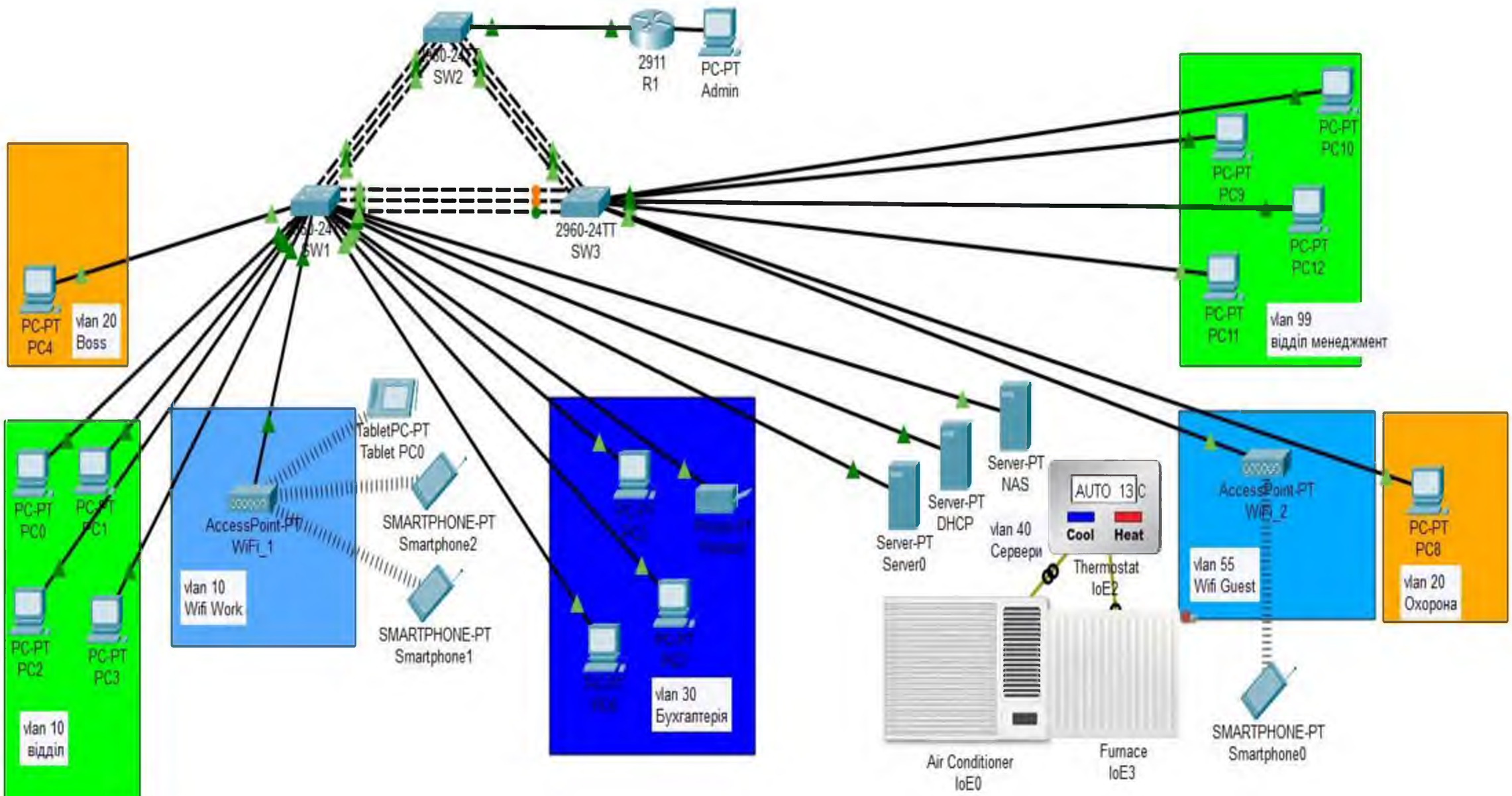
Inter-Domain Routing (CIDR) [Электронный ресурс] – Режим доступа : URL : www.ietf.org/rfc/rfc1517.txt. – Загл. с экрана.

13. RFC 1918. Address Allocation for Private Internets [Электронныйресурс]. – Режим доступа : URL : www.rfc editor.org/rfc/rfc1918.txt. –Загл. с экрана.

14. RFC 3330. Special-Use IPv4 Addresses [Электронный ресурс]. – Режим доступа : URL : www.rfc-editor.org/rfc/rfc3330.txt. – Загл. с экрана.

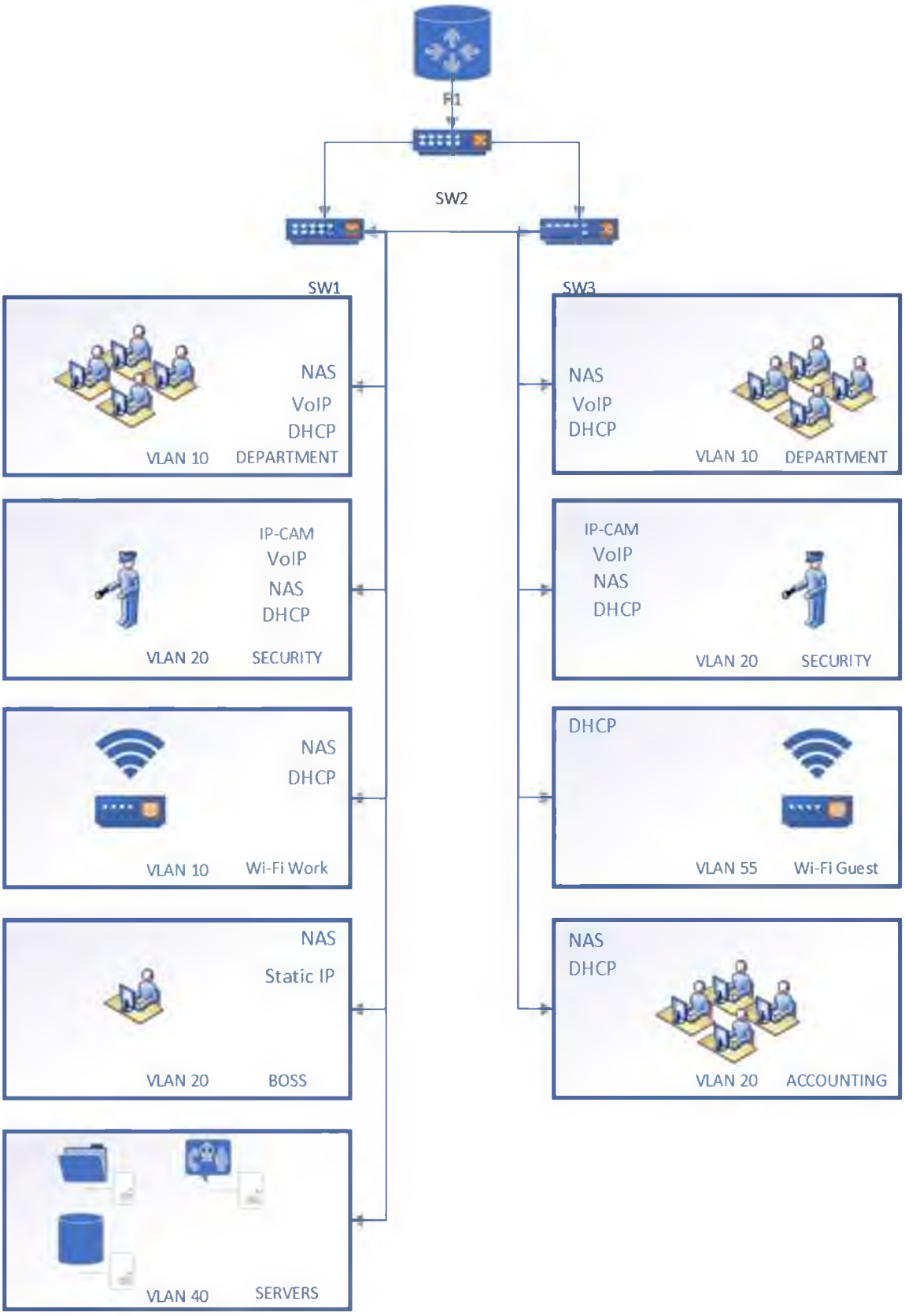
15. TIA-1179 and Beyond: Addressing Information Technology Needs for Evolving Healthcare Facilities [Электронный ресурс] // Belden. –Режим доступа:URL:http://belden.com/pdfs/Techpprs/Addressing_Info_Tech_for_Healthcare_Facilities.pdf. – Загл. с экрана

ДОДАТОК А



					15.04 – МР.1578 «С» 2020.10.23.0007. ПЗ			
Змн.	Арк.	№ Докум.	Підпис	Дата				
Розроб.		Іващенко В.А.			Дослідження та проектування локально обчислювальної мережі торгівельної компанії	Літ	Арк.	Аркушів
Перевір.		Касаткін Д.Ю.						
Реценз.						Аркуш 1	Аркушів 2	

ДОДАТОК Б



					15.04 – МР.1578 «С» 2020.10.23.0012. ПЗ			
Змн.	Арк.	№ Докум.	Підпис	Дата				
Розроб.		Іващенко В.А.			Дослідження та проектування локально обчислювальної мережі торгівельної компанії	Літ	Арк.	Аркушів
Перевір.		Касаткін Д.Ю.						
Реценз.						Аркуш 2	Аркушів 2	
Н. Контр.		Касаткін Д.Ю.			Логічна схема мережі	НУБіП України КІ-20005М		
Затверд.		Лахно В.А.						