Міністерство освіти і науки України

Кам’янець-Подільський національний університет імені Івана Огієнка

Фізико-математичний факультет

Кафедра комп’ютерних наук

Кваліфікаційна робота магістра

з теми: **«Розробка проєкту телекомунікаційної мережі для Кам’янець-Подільської міської лікарні»**

Виконав: здобувач вищої освіти групи KN1-M23

спеціальності 122 Комп’ютерні науки

Басістий Міхаіл Юрійович

Керівник: Понеділок Вадим Віталійович, к.т.н., доцент кафедри комп’ютерних наук

Рецензент:_____

(прізвище, ім’я та по батькові, науковий ступінь, вчене звання рецензента)

м. Кам’янець-Подільський – 2024р.

АНОТАЦІЯ

Басістий М.Ю. «Розробка проєкту телекомунікаційної мережі для Кам’янець-Подільської міської лікарні»

Кваліфікаційна робота магістерського рівня присвячена розробці проєкту телекомунікаційної мережі для Кам’янець-Подільської міської лікарні. В роботі проаналізовано реалізацію телекомунікаційних мереж в лікарські установи, розглянуто різні аспекти при впровадженні таких мереж.

Проведено аналіз підприємства, розроблені схеми, моделі мережі, які ознайомлюють з проєктом. Надано приклади налаштування мережевого обладнання. Розроблені рекомендації щодо впровадження подібних мереж в лікарські установи.

Кваліфікаційна робота в повному обсязі складається з 82 сторінок. З них основна частина складає 57 сторінок, список використаної літератури і джерел – 4 сторінки, додатки – 18 сторінок.

В кваліфікаційній роботі використовуються:

Рисунків – 30.

Таблиць – 2.

Основна мета проєктування полягала у перебудові наявної мережі, яка на даний момент в багатьох місцях є аварійною, виконана недбало і порушує загальні правила безпеки для мережі, що є неприпустимим для об’єкту такого рівня.

Дослідження пов’язані з кваліфікаційною роботою були опубліковані в віснику 16 випуску Кам’янець-Подільського національного університету імені Івана Огієнка фізико-математичних наук.

Також окремі результати роботи були продемонстровані в квітні 2024 року на науковій конференції студентів і магістрантів за підсумками науково-дослідної роботи у 2023 році.

ABSTRACT

Basistyi M. «Development of a telecommunications network project for Kamianets-Podilskyi city hospital»

The master's level qualification work is devoted to the development of a telecommunications network project for Kamianets-Podilskyi city hospital. The work analyzes the implementation of telecommunications networks in medical institutions, considers various aspects of implementing such networks.

An analysis of the enterprise was carried out, schemes and network models were developed that introduce the project. Examples of network equipment configuration were provided. Recommendations for the implementation of such networks in medical institutions were developed.

The qualification work in full consists of 82 pages. Of these, the main part is 57 pages, the list of used literature and sources is 4 pages, and appendices are 18 pages. The qualification work uses:

Figures – 30.

Tables – 2.

The main purpose of the project was to rebuild the existing network, which is currently in a state of emergency in many places, was executed carelessly and violates general safety rules for the network, which is unacceptable for an object of this level.

Research related to the qualification work was published in the Bulletin of the 16th issue of the Ivan Ohienko Kamianets-Podilsky National University of Physical and Mathematical Sciences.

Also, some of the results of the work were demonstrated in April 2024 at a scientific conference of students and masters based on the results of scientific research work in 2023.

ЗМІСТ

ВСТУП 7
РОЗДІЛ І. ОСНОВНІ ЗАДАЧІ ТА КРИТЕРІЇ ВПРОВАДЖЕННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ В ДІЯЛЬНОСТІ ЗАКЛАДІВ ОХОРОНИ ЗДОРОВ'Я 11
1.1. Інформаційно-комунікаційні технології у медичних закладах. Основні нормативні документи застосування комунікаційних мереж у сфері охорони здоров'я 11
1.2. Вимоги до каналів зв'язку для організації обміну медичною та персональною інформацією пацієнтів закладів охорони здоров'я 14
1.3. Технічне та технологічне забезпечення користування мережею Інтернет у медичних закладах 16
РОЗДІЛ ІІ. ПРОДУКТИВНІСТЬ ТА ОЦІНЮВАННЯ СТАНУ КОМП'ЮТЕРНИХ МЕРЕЖ 21
2.1. Швидкість передачі даних у локальній мережі. Пропускна здатність TCP між серверами 21
2.2. Оцінювання поточного стану мережі. Оптимізація налаштувань мережевого обладнання 26
2.3. Якість мережевої інфраструктури. Керування трафіком і пріоритизація 28
2.4. Забезпечення безпеки даних 30
РОЗДІЛ ІІІ. ПРОЄКТУВАННЯ, РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ДЛЯ КОМУНАЛЬНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА «КАМ'ЯНЕЦЬ-ПОДІЛЬСЬКА МІСЬКА ЛІКАРНЯ КАМ'ЯНЕЦЬ-ПОДІЛЬСЬКОЇ МІСЬКОЇ РАДИ» 33
3.1. Розробка та розрахунок базових функціональних можливостей мережі медичного закладу 33

3.1.1. Характеристика підприємства для якого створюється проєкт мережі 33
3.1.2. Технічне завдання з розробки мережі 34
3.1.3. Топологія та використані технології телекомунікаційної мережі..... 35
3.1.4. Розрахунки продуктивності мережі 37
3.1.5. IP адресація в мережі 39
3.2. Реалізація функціональних можливостей комп'ютерної мережі Кам'янець-Подільської міської лікарні 41
3.2.1. Розробка схематичної мережі 41
3.2.2. Проєктування віртуальної моделі мережі 45
3.2.3. Логічна схема мережі 46
РОЗДІЛ IV. ДІАГНОСТИКА ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ТА МОЖЛИВОСТІ МОДЕРНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ КОМУНАЛЬНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА «КАМ'ЯНЕЦЬ-ПОДІЛЬСЬКА МІСЬКА ЛІКАРНЯ КАМ'ЯНЕЦЬ-ПОДІЛЬСЬКОЇ МІСЬКОЇ РАДИ» 48
4.1. Тестування комп'ютерної мережі Кам'янець-Подільської міської лікарні 48
4.2. Можливості модернізації телекомунікаційної мережі Кам'янець-Подільської міської лікарні 57
4.3 Рекомендації для впровадження мереж у медичних закладах 58
ВИСНОВКИ 60
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ 63
ДОДАТКИ 67

ВСТУП

Комп’ютерні технології поширені по всьому світу. Майже на будь-якому підприємстві є певний комп’ютерний відділ, який виконує різні види робіт. Сфера комп’ютерних технологій і пов’язаних разом з нею елементів розвивається ще з минулого століття, і справляє серйозний вплив на роботу різних установ. З кожним роком комп’ютерні технології стають більш поширенішими, компактнішими, потужнішими. Нині кожен день розробляється та впроваджується щось нове, що є кращим аналогом попередньої версії.

Проблемою багатьох установ, підприємств є необхідність модернізації або ж повної заміни свого старого комп’ютерного обладнання через певний час. З швидким рухом технологій це може викликати складнощі, адже те що сьогодні є гарним варіантом, завтра вже може вважатись застарілою технологією. Важливим моментом для підприємств є впровадження технологій, які будуть довго підтримуватися, або які буде легко модернізувати, щоб забезпечити потрібний рівень обчислювальної потужності. І хоч з певними видами комп’ютерного обладнання це зробити важко, є значна кількість технологій, які можна підтримувати довгий період часу.

Темою наукової роботи є розробка проєкту телекомунікаційної мережі для Кам’янець-Подільської міської лікарні, яка ставить собі за мету впровадження продуманої телекомунікаційної мережі, яка буде мати великий ресурс експлуатації та великий потенціал модернізації.

Питання функціонування телекомунікаційних мереж досліджували багато науковців, праці яких стали підґрунтям роботи: Андросов А.І., Є. В. Буров, С.В. Волошко, П. П. Воробієнко, В.М. Гаркуша, І. В. Горбатий, О. С. Городецька, І. М. Журавська, А. Г. Микитишин, С. І. Тарабаєв, Е. С. Таненбаум, Н. В. Фрідріхсон та інші.

Актуальність теми. В сучасному світі зі стрімким розвитком комп’ютерних технологій актуальність розвитку комп'ютерної мережі для медичних закладів надзвичайно висока. Користування мережею Інтернет відкриває безліч можливостей для закладів охорони здоров’я, які сприяють покращенню якості надання медичних послуг та підвищенню ефективності діяльності закладу в цілому, дозволяє поліпшити обмін даними між медичними працівниками, забезпечити більш швидкий доступ до медичних баз даних, телемедицини та моніторингу здоров’я пацієнтів.

Існуюча комп’ютерна мережа міської лікарні не відповідає сучасним вимогам. Часті аварійні ситуації, застаріле обладнання, хаотичні попередні модернізації значно знижують продуктивність роботи медичного персоналу. Окрім цього відкриття нових відділів і підключення їх до існуючої мережі вимагають кардинальних змін мережевої структури і обладнання.

Предметом дослідження є технічні особливості та методика створення телекомунікаційних мереж.

Об'єктом дослідження є мережа для міської лікарні, яка включає в себе планування, розгортання, налаштування та підтримку інфраструктури.

Гіпотезою дослідження є припущення, що розробка продуктивної комп’ютерної мережі, що відповідає сучасним технологічним вимогам допоможе покращити доступність медичних послуг та ефективність роботи лікарні.

Ідея полягає в тому, щоб створити інтегровану комп’ютерну мережу, яка забезпечить швидкий та безперебійний обмін медичною інформацією, забезпечить безпеку даних та покращить координацію роботи медичного персоналу.

Завданням дослідження є розробка архітектури мережі, вибір технологій, розгортання і налаштування обладнання, забезпечення продуктивності і стабільності роботи, забезпечення безпеки даних та розробка пропозицій для можливих майбутніх модернізацій мережі.

Наукова новизна: Наукова новизна полягатиме в розробці комплексного підходу до розвитку мережі для міської лікарні, враховуючи специфічні потреби медичної галузі, а саме:

1. Створено проєкт структурованої телекомунікаційної мережі для міської лікарні, яка передбачає використання сучасних технологій та підходів, які раніше не застосовувались для побудови та експлуатації мереж подібного характеру. Дана мережа буде стресостійкою до різних аварійних ситуацій, матиме стандартифіковану структуру, яка покращить експлуатацію мережі і закладе фундамент до наступних модернізацій, якщо виникне така необхідність.

2. Прокладання комунікацій між корпусами лікарні. Це необхідно з багатьох причин. Аварійний стан міжкорпусних з’єднань, приєднання до лікарні нових корпусів, які повинні бути задіяні і забезпеченні мережею, зв’язком, інтернетом. Також, згідно з нинішнім станом війни в країні держава зобов’язує об’єкти критичної інфраструктури мати резервні лінії зв’язку. Це означає, що в лікарні необхідно, як мінімум, мати двох різних провайдерів, які зможуть підмінити з’єднання в разі непередбачуваних подій, що вимагає нові міжкорпусні з’єднання.

3. Розроблений набір рекомендацій для проєктування мереж. Створення великих, розподілених мереж це завжди різні компромісні підходи, які не завжди є звичайними та стандартними. У випадку проєктування мережі в лікарні складність мережі виходить на додатковий рівень. Проєктування телекомунікаційної мережі з документуванням різних творчих підходів та широкого застосування технологій принесе велику користь в майбутніх розробках мереж в незвичайних установах.

Теоретичне значення: дослідження здійснює внесок у вивчення та практичне впровадження комп'ютерних мереж в медичних закладах, що може бути корисним для оптимізації процесів надання медичних послуг.

Практична цінність: результати дослідження можуть бути використані для поліпшення обслуговування пацієнтів та підвищення ефективності роботи лікарні.

РОЗДІЛ І. ОСНОВНІ ЗАДАЧІ ТА КРИТЕРІЇ ВПРОВАДЖЕННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ В ДІЯЛЬНОСТІ ЗАКЛАДІВ ОХОРОНИ ЗДОРОВ'Я

1.1. Інформаційно-комунікаційні технології у медичних закладах. Основні нормативні документи застосування комунікаційних мереж у сфері охорони здоров'я

Інтернет надає широкий спектр можливостей в охороні здоров'я, починаючи від полегшення доступу до інформації та послуг до сприяння самостійному контролю за своїм здоров'ям. Використання цих можливостей може значно покращити якість та ефективність охорони здоров'я.

За даними ВООЗ до 2030 року кожен шостий житель планети буде належати до людей похилого віку, а вже до 2050 їх кількість лише подвоїться. Тому підтримка зв'язку з пацієнтами та перевірка стану їхнього здоров'я на відстані стануть основою ефективного лікування та профілактики захворювань [19].

Користування мережею Інтернет відіграє важливу роль у діяльності закладів охорони здоров'я, зокрема, ключові аспекти використання мережі розширюють можливості в діяльності закладів охорони здоров'я, а саме:

- Доступ до медичної інформації: Інтернет забезпечує легкий та швидкий доступ до медичних досліджень, наукових публікацій, клінічних випробувань та актуальної медичної інформації. Це дозволяє медичним працівникам покращувати знання та навички, приймати обґрунтовані рішення та підвищувати якість надання медичної допомоги.
- Електронна медична документація: за допомогою Інтернету створюються та обробляються електронні медичні записи, що сприяє зручному зберіганню, обміну та доступу до медичної інформації. Це сприяє

ефективній співпраці різних підрозділів та медичних працівників, забезпечує кращу організацію та координацію медичної допомоги.

- Телемедицина: Інтернет дозволяє проводити віддалені консультації та надавати медичну допомогу. За допомогою відеозв'язку та спеціалізованих платформ лікарі можуть проводити прийоми, формувати попередні діагнози, надавати електронні рецепти та направлення, забезпечувати віртуальний моніторинг та проводити консультації з пацієнтами, що знаходяться віддалено. Це особливо корисно для пацієнтів, які проживають у віддалених регіонах або мають обмежені можливості пересування.
- Медична освіта та навчання: Інтернет надає доступ до навчальних ресурсів, онлайн-курсів, вебінарів та форумів, що сприяє постійному професійному розвитку медичних працівників, з'являється можливість поглиблювати свої знання, обмінюватися досвідом та взаємодіяти з колегами з усього світу.
- Комунікація та спілкування: Інтернет надає засоби для зручної комунікації між медичним персоналом, пацієнтами та іншими зацікавленими сторонами: електронна пошта, спільні робочі платформи, месенджери та соціальні мережі забезпечують швидкий обмін інформацією та співпрацю для поліпшення процесів надання медичної допомоги [17].

Електронна охорона здоров'я (е-здоров'я, eHealth) – система взаємоприйнятних інформаційних відносин усіх суб'єктів сфери охорони здоров'я, які базуються на використанні методів, заходів та технологій із застосуванням цифрового середовища, у тому числі інформаційно-комунікаційних технологій, спрямованих на підтримку сфери охорони здоров'я.

Медичні послуги з використання телемедичних технологій можна умовно розділити на дві категорії: «лікар – пацієнт» і «лікар – лікар». Перший тип дозволяє здійснювати віддалену консультацію, діагностику та моніторинг пацієнтів без прямого фізичного контакту, такі як відеоконференції з лікарем, обмін медичними даними, використання мобільних додатків для вимірювання

показників здоров'я, а також надання онлайн-рецептів та рекомендацій щодо лікування. Другий випадок – клінічна телемедична консультація між лікарями або консиліум застосовуються для вирішення питань оцінки стану здоров'я пацієнта, уточнення діагнозу, визначення прогнозу і тактики медичного обстеження і лікування, доцільності госпіталізації або медичної евакуації [19].

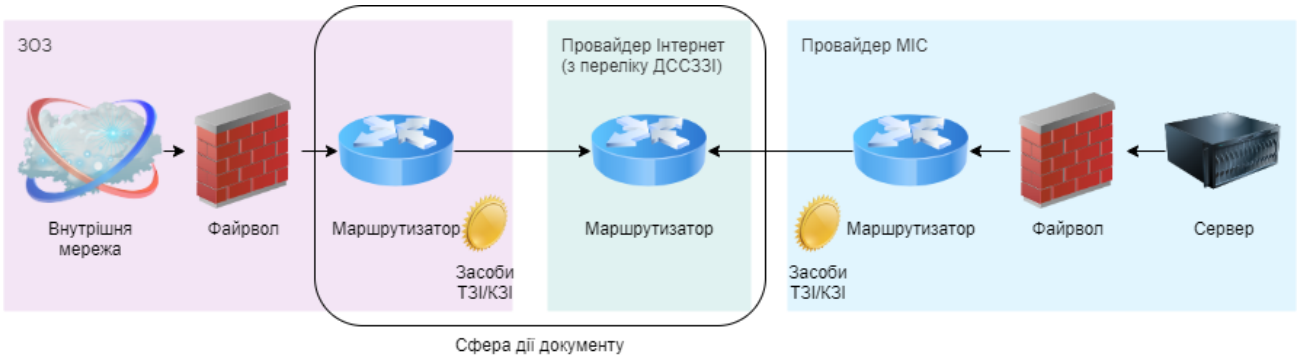
Наступні нормативні документи є правовим підґрунтям для застосування комунікаційних мереж у сфері охорони здоров’я:

1. Закон України «Про авторське право і суміжні права».
2. Розпорядження КМУ № 247-р від 15 травня 2002 р. «Про затвердження Концепції легалізації програмного забезпечення та боротьби з нелегальним його використанням».
3. Рекомендації Міністерства економіки України щодо забезпечення правомірності використання комп’ютерних програм у діяльності суб’єктів господарювання.
4. Наказ МОЗ № 797 від 08.04.2019 р. «Про внесення змін до Примірного табеля матеріально-технічного оснащення закладів охорони здоров’я та фізичних осіб-підприємців, які надають первинну медичну допомогу».
5. Наказ МОЗ № 142 від 14.03.2011 р. «Стандарти акредитації закладів охорони здоров’я».
6. Наказ МОЗ № 261 від 26.03.2010 р. «Про впровадження телемедицини в закладах охорони здоров’я».
7. Наказ МОЗ № 681 від 19.10.2015 р. «Про затвердження нормативних документів щодо застосування телемедицини у сфері охорони здоров’я».
8. ДСТУ ISO 17432:2009. Інформатика в охороні здоров’я. Повідомлення та пересилання даних.
9. ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги».

1.2. Вимоги до каналів зв’язку для організації обміну медичною та персональною інформацією пацієнтів закладів охорони здоров’я

Для забезпечення конфіденційності та цілісності, вся медична інформація та персональна ідентифікаційна інформація про особу передається у зашифрованому вигляді. Шифрування здійснюється за допомогою засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

Обмін медичною та персональною інформацією пацієнтів закладів охорони здоров’я (далі – ЗОЗ) між ЗОЗ та провайдером медичної інформаційної системи (далі – МІС), показано на Мал. 1.1.



Мал. 1.1. – Канал зв’язку між ЗОЗ та провайдером МІС

Для оброблення медичної інформації та персональної ідентифікаційної інформації про особу, використовуються пристрої зв’язку з переліку засобів технічного захисту інформації, відповідність яких вимогам нормативних документів засвідчено сертифікатом відповідності або позитивним експертним висновком.

Для забезпечення безпеки при передачі даних, пристрої зв’язку налаштовуються відповідно до наступних вимог:

1. Доступ до налаштувань мережевого обладнання обмежений та контрольований. Налаштування мережевого обладнання ззовні охоронюваного периметру мережі заборонене, та доступне виключно з середини мережі.

2. Вимоги до паролів облікових записів адміністраторів мережевого обладнання, включаючи їх складність та частоту змінення, описані у Політиці паролів.

3. Всі внутрішні та зовнішні порти, які не використовуються для роботи ІТ систем ЗОЗ адміністративно відключені.

4. Використовується лише те мережеве обладнання, до якого застосовані всі актуальні оновлення програмного забезпечення з боку виробника.

5. Мережі, через які передається інформація МІС відділені від мереж загального користування (наприклад, публічний Wi-Fi для пацієнтів та відвідувачів).

6. Фізичний доступ до пристроїв зв'язку обмежено авторизованим персоналом і контролюється відповідно до політики інформаційної безпеки.

Заклади охорони здоров'я, які перебувають у державній власності, закуповують послуги (укладають договори) з доступу до мережі Інтернет у операторів (провайдерів) телекомунікацій, які забезпечують Захищені вузли доступу до мережі Інтернет (ЗВІД). Перелік таких провайдерів розташований на сторінці ДССЗЗІ (**ДССЗЗІ** – Державна служба спеціального зв'язку та захисту інформації України) [18].

В закладі охорони здоров'я здійснюються спеціальні запобіжні заходи для блокування зовнішнього доступу через Інтернет до інформаційних ресурсів закладу, не призначених для публічного доступу, а також для захисту конфіденційної інформації ЗОЗ при її передачі через Інтернет.

Доступ до інформаційних ресурсів закладу через модеми, інші комунікаційні пристрої або відповідне програмне забезпечення підлягає авторизації та автентифікації системою контролю доступу. Зовнішній виклик чи комутація на внутрішній номер (кінцевий пристрій) без проходження через систему контролю доступу заборонений.

Всі комп'ютери закладу захищені від безпосереднього доступу з Інтернет та загроз із внутрішньої мережі за допомогою зовнішніх та

вбудованих брандмауерів. Політика брандмауерів за замовчанням, встановлена як «заборонено все, що явно не дозволено». Налаштування брандмауерів контролюється відповідальним з ІБ.

Таким чином захист інформації з обмеженим доступом і зокрема захист персональних даних є пріоритетною ціллю.

1.3. Технічне та технологічне забезпечення користування мережею Інтернет у медичних закладах

Доступ до мережі відкриває додаткові можливості для користувачів та вимагає дотримання певних вимог. Початок користування Інтернетом передбачає підготовку у тому числі технічного характеру, а саме:

- Підключення до Інтернету: основною вимогою є наявний доступ до мережі Інтернет, це може бути через провайдера Інтернету, який надає послуги з підключення, або через мобільного оператора, якщо ви плануєте користуватися мобільним Інтернетом. Підключення до Інтернету є невід'ємною передумовою для користування мережею. На сьогодні існують різні способи підключення, включаючи використання провайдера Інтернету або мобільного оператора. Провайдери Інтернету надають послуги підключення через кабель, оптичний кабель або безпровідний зв'язок, в той час як мобільні оператори забезпечують мобільний Інтернет через мережу мобільного зв'язку. Також доступ може бути забезпечений через бездротову мережу Wi-Fi, яку надають різні заклади. Вибір конкретного способу підключення залежить від індивідуальних потреб, доступності та уподобань користувача.
- Вибір пристрою: для забезпечення доступу до Інтернету важливим кроком є вибір пристрою, який відповідатиме вашим потребам та зручності. Наявність комп'ютера, смартфона або планшета дає можливість користуватися різноманітними функціями мережі. Основні аспекти, які варто враховувати при виборі пристрою, включають:

1. Функціональність: пристрій повинен мати необхідні функції для користування Інтернетом, такі як веб-браузер, можливість встановлення додатків або програм для доступу до різних сервісів.

2. Розмір та портативність: обов’язковим є врахування того, як планується використання пристрою, – стаціонарні комп’ютери забезпечують більше функцій, але можуть бути менш портативними, тоді як смартфони та планшети можуть бути зручнішими для використання в рухомому середовищі.

3. Операційна система: на вибраному пристрої повинна бути встановлена операційна система, яка буде зрозумілою для користувача та зручною у використанні.

4. Характеристики технічного обладнання: передбачають оцінку потужності пристрою (швидкість роботи процесора, обсяг оперативної пам'яті та обсяг внутрішнього сховища), що є важливим для забезпечення стабільної і оперативної роботи Інтернету та запуску програмних додатків.

5. Безпека: вибраний пристрій повинен мати вбудовані засоби безпеки та можливість оновлення програмного забезпечення для захисту від потенційних загроз Інтернету.

– Підключення до мережі: для забезпечення підключення до мережі Інтернету необхідно налаштувати доступ до мережі. Це можна зробити шляхом підключення комп’ютера до маршрутизатора або модему за допомогою екрана або Wi-Fi. Для підключення до провайдера Інтернету через маршрутизатор або модем необхідно сконфігурувати мережеві налаштування пристрою, включаючи введення інформації про мережу та налаштування безпеки, такі як пароль Wi-Fi. У разі використання мобільного Інтернету користувач повинен активувати функцію передачі даних на своєму смартфоні або планшеті, щоб забезпечити доступ до Інтернету через мобільну мережу оператора зв'язку.

– Встановлення веб-браузера: веб-браузер – це програмне забезпечення, що дозволяє переглядати веб-сторінки. На пристрої має бути завантажений та встановлений веб-браузер.

Робота з браузером є важливою частиною користування Інтернетом, оскільки він дозволяє користувачам переглядати веб-сторінки, взаємодіяти з веб-додатками та виконувати різноманітні операції в Інтернеті.

– Створення облікового запису та електронної пошти: цей крок потребує вибору провайдера електронної пошти. Після вибору провайдера необхідно перейти на офіційний веб-сайт провайдера та знайти опцію «Створити обліковий запис» або «Зареєструватися». Процес реєстрації облікового запису передбачає надання особистої інформації, такої як ім'я, прізвище, дата народження, обране ім'я користувача та пароль. Обліковий запис в Інтернеті відображає ідентифікаційні дані користувача та дозволяє отримати доступ до різних сервісів та ресурсів. Він забезпечує ідентифікацію та автентифікацію користувача, що дозволяє зберігати його персональні налаштування, збережені дані та історію взаємодії з різними платформами та послугами.

Робота з медичною інформаційною системою (МІС) також включає етапи реєстрації та входу до системи за допомогою необхідних персональних даних через обліковий запис.

Окрім означених можливостей доступ до мережі Інтернет дозволяє долучатися до електронної системи охорони здоров’я через функціональність медичних інформаційних систем та відкриває можливості для ефективного управління медичною інформацією, покращення якості надання медичних послуг та спрощення взаємодії між різними учасниками системи охорони здоров’я.

Виділяють два види комп’ютерного забезпечення: програмне і апаратне. Програмне забезпечення включає в себе системне і прикладне. У системне програмне забезпечення входить мережевий інтерфейс, який забезпечує доступ до даних на сервері. База даних управляється прикладною програмою управління (СКБД) і може містити, зокрема, історії хвороби, рентгенівські знімки в цифрованому вигляді, статистичну звітність по стаціонару, бухгалтерський облік. Прикладним забезпеченням є програми, що

забезпечують обчислення, обробку результатів досліджень, різного роду розрахунки, обмін інформацією між комп'ютерами [25].

В таблиці 1.1. наведено перелік програмного забезпечення для типового робочого місця закладу охорони здоров'я.

Таблиця 1.1.

Перелік програмного забезпечення для типового робочого місця закладу охорони здоров'я

з/п	Тип програмного забезпечення	Назва програмного забезпечення	Безкоштовно (Так/Ні)
1	Операційна система для персонального комп'ютера або ноутбука	Microsoft Windows	Ні
2	Антивірусне програмне забезпечення	Windows Defender	Поставляється разом з операційною системою
3	Програмне забезпечення для доступу в інтернет	Google Chrome	Так
4	Програмне забезпечення для багатофункціонального пристрою або принтера + сканера	Драйвер пристрою від виробника або з комплекту Microsoft Windows	Поставляється разом з пристроєм або з операційною системою
5	Програмне забезпечення для діловодства	Microsoft Office	Ні
6	Спеціальне (прикладне) програмне забезпечення для ПМСД, спеціалізованої допомоги та програмне забезпечення для доступу до бази даних щодо лікувального процесу	Відповідно до переліку медичних інформаційних систем, підключених до ЦБД eHealth (https://ehealth.gov.ua/pidklyucheni-do-ehealth-mis/)	Ні
7	Спеціальне програмне забезпечення для електронного обладнання, яке має можливість запису та (або) передачі отриманих результатів в електронному вигляді для використання, в тому числі в телемедицині	Драйвер пристрою від виробника, RadiAnt DICOM	Поставляється разом з пристроєм

Отже, значення телекомунікаційної мережі для сфери охорони здоров'я є надзвичайно важливим, оскільки ця технологія надає розширені можливості у зборі, обміні та використанні медичної інформації, покращує комунікацію між медичними працівниками та пацієнтами, сприяє підвищенню якості надання медичних послуг та ефективності управління охороною здоров'я. Інтернет забезпечує швидкий та зручний доступ до великого обсягу медичної інформації, включаючи наукові дослідження, клінічні протоколи, медичні журнали та бази даних. Це дозволяє медичним працівникам оновлювати свої знання та практику відповідно до найновіших рекомендацій. Також Інтернет забезпечує ефективну комунікацію та співпрацю між медичними працівниками, що дозволяє здійснювати консультації, обмін даними та взаємодію на відстані. Це особливо корисно у випадках віддалених комунікацій та спільного прийняття рішень.

В цьому розділі було розглянуто можливості та переваги застосування телекомунікаційних мереж в лікарських закладах, ознайомлення з нормативними документами, що корегують впровадження таких мереж в подібних закладах. Проведено ознайомлення з вимогами до організації каналів зв’язку для обміну інформацією пацієнтів всередині лікарської мережі. Було проаналізовано технічне та певне програмне забезпечення кінцевих пристроїв, які можуть використовуватись в телекомунікаційній мережі.

Таким чином, користування мережею Інтернет у сфері охорони здоров'я має велике значення для покращення доступу до інформації, підвищення ефективності комунікації та співпраці, вдосконалення управління та надання медичних послуг і підвищення медичної грамотності пацієнтів.

РОЗДІЛ ІІ. ПРОДУКТИВНІСТЬ ТА ОЦІНЮВАННЯ СТАНУ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1. Швидкість передачі даних у локальній мережі. Пропускна здатність TCP між серверами

Швидкість передавання даних у локальній мережі є важливим фактором, який визначає, наскільки швидко й ефективно комп'ютери можуть обмінюватися даними один з одним. Для сфери охорони здоров'я висока швидкість локальної мережі є критично важливою для багатьох додатків, як-от спільне використання файлів, віддалений доступ до робочих столів, потокове відео та VoIP[1].

Максимальна швидкість передачі даних у локальній мережі залежить від типу технології.

Існують чотири фундаментальні технології:

1. Fast Ethernet

Це був перший стандарт Ethernet, який надав користувачам швидкість передачі даних.

За технологією Fast Ethernet можна отримати максимальну швидкість 100 Мбіт/с. Зазвичай комутатори Fast Ethernet мають символ швидкості передачі даних 10/100 Мбіт/с, який є діапазоном швидкостей.

Якщо встановлено Fast Ethernet, то верхня межа швидкості передачі даних становитиме 100 Мбіт/с, а нижня –1 Мбіт/с. Залежно від швидкості мегабіт на секунду можна зрозуміти максимальну швидкість локальної мережі.

2. Gigabit Ethernet

В Gigabit Ethernet – нижній поріг 1 Мбіт/с, а максимальна швидкість передачі даних буде в гігабітах.

[1] Технологія передачі медіа-даних у реальному часі за допомогою сімейства протоколів TCP/IP

Зазвичай це:

- 1 Gigabit Ethernet
- 10 Gigabit Ethernet

1 Gigabit Ethernet може забезпечити максимальну швидкість 1000 Мбіт/с або 1 Гбіт/с. У випадку 10 Gigabit Ethernet максимальна швидкість передачі даних становить 10 гігабайт на секунду. Однак, залежно від гігабітної технології, можна отримати 25 Гбіт/с, 40 Гбіт/с, 100 Гбіт/с тощо.

Отже, локальна мережа, що містить комутатор 10 GbE, матиме максимальну швидкість близько 10,000 мегабіт на секунду. Подібна концепція застосовується до інших версій Gigabit Ethernet. Таким чином, можна отримати приблизну оцінку максимальної швидкості передачі даних.

3. PoE

Power Over Ethernet це технологія, яка забезпечує швидкість передачі даних і потужність через один порт Ethernet. Він має різні стандарти, запроваджені Інститутом електротехніки та електроніки.

Ось стандарти IEEE:

- IEEE 802.3af
- IEEE 802.3at
- IEEE 802.3bt

Від цих стандартів залежить максимальна потужність і швидкість мережі PoE. Якщо використовується IEEE 802.3bt – отримуємо 100 Вт, тоді як низька потужність стосується інших методів. Стандарт PoE також може дати уявлення про швидкість передачі даних і максимальну потужність.

Швидкість мережі залежить від живлення через Ethernet. Це залежить від типу комутатора, який використовується для своєї технології PoE. Наприклад, якщо використовується Fast Перемикач PoE, максимальна швидкість становитиме близько 100 Мбіт/с. Так само можна отримати швидкість передачі даних 100 Гбіт/с за допомогою комутатора PoE.

Однак, щоб побудувати мережу PoE, треба отримати свої пристрої та підключити їх до Ethernet-портів комутаторів.

4. Wi-Fi

Wi-Fi або бездротові точки доступу не використовують дроти, на відміну від систем PoE або Ethernet.

Якщо системи Wi-Fi мають стандарт 802.11a, максимальна швидкість буде близько 54 Мбіт/с. Так само швидкість буде вищою для інших стандартів.

Стандарт 802.11n забезпечує максимальну швидкість 450 Мбіт/с. Максимальна швидкість в секунду особливо помітна на пристроях Wi-Fi. Постачальники послуг пропонують нижчу швидкість вдома з невеликими мережами порівняно з офісами з розбудованими мережами. Залежно від вимог можна встановити систему та ефективно подолати проблеми з Інтернетом.

Найновіші стандарти Wi-Fi пропонують максимальну швидкість до 750 Мбіт/с наближену до Gigabit Ethernet [26].

Таким чином, сучасні технології, такі як Gigabit Ethernet і Wi-Fi 6, здатні значно збільшити швидкість локальної мережі.

Швидкість передавання даних локальною мережею залежить від кількох чинників, включно з типом технології, швидкістю мережевого обладнання, якістю мережевої інфраструктури та навантаженням мережі.

Фактори що визначають пропускну спроможність мережі:

1. Міжмережеві пристрої;
2. Тип даних які передаються;
3. Мережева топологія;
4. Кількість користувачів в мережі;
5. Користувацькі комп’ютери;
6. Сервера [22].

Для забезпечення з’єднання даних у локальній мережі потрібні:

- комутатори Ethernet або Wi-Fi для точок бездротового доступу;
- підключення пристроїв за допомогою комутатора або Wi-Fi;

– розгортання маршрутизаторів для покращення продуктивності мережі та контролювання трафіку.

Виділяють два найважливіші фактори для успішної передачі даних за протоколом TCP[2]:

– розмір TCP-вікна – кількість байт, яку одна із сторін готова прийняти без підтвердження;

– кругова затримка передачі-приймання – час, витрачений на відправку пакета та підтвердження його доставки.

За цими двома показниками розраховують максимально можливу пропускну здатність між двома хостами незалежно від ширини смуги пропускання.

Пропускна спроможність TCP розраховується за наступною формулою:

Пропускна здатність TCP (біт/с) = Розмір TCP-вікна (біт) / Кругова затримка (с) (2.1.)

Відповідно для того щоб зробити мережу швидше необхідно збільшити розмір TCP-вікна та/або скоротити затримку сигналу.

Для узгодження більшого розміру TCP-вікна, потрібне індивідуальне ручне налаштування кожного сервера. Щоб розрахувати оптимальний розмір TCP-вікна необхідно провести обчислення, спираючись на ширину смуги пропускання.

Для розрахунку оптимального розміру TCP-вікна використовуємо формулу:

Розмір TCP-вікна (байт) = Розмір TCP-вікна (біт) / 8 = Пропускна здатність (біт/с) * Кругова затримка (с) / 8 (2.2.)

[2] Протокол Transmission Control Protocol – призначений для керування передаванням даних у комп'ютерних мережах, працює на транспортному рівні моделі OSI.

Збільшення розміру TCP-вікна має свої недоліки.

По-перше, це вимагатиме більше пам’яті для буферизації серверів, яка потрібна для зберігання непідтверджених даних на випадок їх повторного відправлення.

По-друге, збільшений розмір TCP-вікна може спричинити більшу кількість втрачених пакетів, які, у свою чергу, вимагають повторної передачі всього вікна. Це може негативно позначитися на продуктивності. Для вирішення цієї проблеми у стеку TCP/IP сервера може бути активована опція «вибіркові підтвердження», яка за замовчуванням вимкнена.

Розміщення WAN-акселераторів – прискорювачів глобальної мережі на кожному кінці лінії є одним із варіантів вирішення проблеми, що дозволяє:

- відкрити збільшене вікно TCP;
- надати можливість тонкої оптимізації протоколу TCP (наприклад, вибіркові підтвердження лише між акселераторами);
- не вимагає спеціальної установки серверів або додаткової буферної пам'яті;
- може використовувати особливі функції прикладного рівня моделі OSI (Layer 7 – доступ до мережевих служб) для скорочення затримки.

Для зменшення затримки сигналу оптимальним способом оптимізації є також установка WAN-прискорювача на кожному кінці лінії, який передає отримані TCP-пакети локальному серверу, тим самим обманюючи його на предмет реальної швидкості трансферу даних. Локальний сервер приймає моментальні підтвердження прискорювача замість того, щоб чекати загальмований відгук віддаленого сервера. Це позбавляє необхідності коригування розміру TCP-вікна на самих серверах.

Пара WAAS[3]-пристроїв використовують збільшений розмір TCP-вікна та вибіркові підтвердження на всій ділянці лінії між ними.

[3] Система WAAS (Wide Area Augmentation System) служить для підвищення точності позиціювання навігаційних GPS систем

Крім того, WAAS ефективно очищають TCP-потік від надлишкових резервних даних, забезпечуючи надзвичайно високий рівень компресії (стиснення). Кожен акселератор запам’ятовує раніше переглянуті дані. Якщо дублюючий фрагмент виникає повторно, він видаляється і замінюється крихітною 2-байтовою міткою. Ця мініатюрна мітка розпізнається віддаленим прискорювачем, який замість неї вставляє оригінальний фрагмент даних перед відправкою трафіку на локальний сервер. Як результат більш висока пропускна спроможність лінії між серверами без спеціального TCP-налаштування локальних серверів.

Для розрахунку максимальної допустимої затримки для заданої пропускної спроможності використовуємо формулу:

Кругова затримка (мс) = Розмір TCP-вікна (біт) / (2.3.)
Необхідна пропускна здатність (біт/с)

Використовування каналу на 100% його пропускної спроможності можна добитись і без збільшення TCP-вікна і встановлення WAN-прискорювачів, просто використавши багатопоточність [23].

2.2. Оцінювання поточного стану мережі. Оптимізація налаштувань мережевого обладнання

Діагностика поточного стану мережі передбачає виявлення факторів, що сповільнюють роботу, і визначення вузьких місць, які потребують втручання.

Для оцінки поточної швидкості мережі дотримуються наступної послідовності дій:

1. тестування швидкості з’єднання за допомогою онлайн-інструментів і порівняння результатів з тарифним планом провайдера;
2. виявлення додатків або процесів, які використовують великі обсяги мережевих ресурсів через використання інструментів моніторингу ресурсів (Task Manager для Windows, Activity Monitor для macOS);

3. визначення проблем із затримкою, використовуючи команду ping для оцінки затримок (ping) між пристроями в мережі [12, с.236-237].

Для перевірки швидкості локальної мережі можна використати наступні програми:

- Speedtest by Ookla: онлайн-сервіс для точного тестування швидкості завантаження і вивантаження;
- iPerf: утиліта командного рядка, призначена для ретельнішого тестування пропускної здатності між пристроями;
- Wireshark: потужний аналізатор мережевого трафіку для виявлення проблем безпеки та детального аналізу мережевої взаємодії;
- NetSpot: інструмент для сканування Wi-Fi, який допомагає оптимізувати розташування маршрутизатора;
- Fing: мобільний застосунок для сканування мережі та виявлення під'єднаних пристроїв [10, с. 36].

Ці інструменти дають змогу також провести глибший аналіз для виявлення причин можливих проблем, таких як конфлікти IP-адрес, перевантаження мережі або неефективне використання ресурсів.

Оптимізація налаштувань мережевого обладнання відіграє ключову роль у підвищенні продуктивності локальної мережі і передбачає:

- регулярне оновлення прошивки маршрутизатора та комутатора є важливим кроком. Це – і поліпшення продуктивності, і виправлення помилок;
- налаштування каналів для мінімізації втручання від інших мереж при використанні Wi-Fi. Зокрема, увімкнення Quality of Service (QoS) дає змогу виділити пріоритетний трафік, що особливо корисно для часозатратних завдань:
- увімкнення опції WMM (Wi-Fi Multimedia) підтримує пріоритет для відео- та аудіотрафіку, покращуючи якість передавання даних;
- перехід на Wi-Fi 6 (802.11ax) для збільшення пропускної здатності при виборі бездротового стандарту;

- застосування протоколу IPv6 для забезпечення більш ефективного використання адрес і поліпшення стабільності мережі;
- використовування багатоканальності (Channel Bonding) і застосовування динамічного перенаправлення трафіку (Dynamic Routing) з протоколами типу OSPF або EIGRP для збільшення пропускної спроможності;
- використання VLAN (Virtual LAN) для поділу трафіку на логічні мережі управління і оптимізації передачі даних [14].

Ефективне налаштування мережевого обладнання з урахуванням цих інструкцій забезпечує оптимальну продуктивність мережі, роблячи її гнучкішою та такою, що відповідає вимогам бізнесу або домашнього використання.

2.3. Якість мережевої інфраструктури. Керування трафіком і пріоритизація

Стабільна та ефективна локальна мережа вимагає якісної інфраструктури. Вибір Cat6 або Cat6a кабелю забезпечує високу пропускну здатність, а в умовах електромагнітних завад рекомендується використовувати екрановані кабелі (FTP або STP).

Слід приділяти увагу якості ізоляції та уникати надлишкової довжини кабелю, щоб запобігти втраті сигналу.

Централізований розподіл обладнання та використання кабельних лотків спрощують управління структурою, а поділ мережі на зони – підвищує ефективність.

Розміщення обладнання в добре вентильованих місцях і правильний розподіл бездротових маршрутизаторів покращують продуктивність і стабільність мережі. Ці рекомендації створюють оптимальні умови для надійного передавання даних і мінімізують збої в мережевій інфраструктурі [2, с. 116].

Керування трафіком і пріоритизація дають змогу зробити так, щоб критично важливі додатки отримували пріоритет у мережі, навіть якщо

навантаження на неї високе. Це може підвищити продуктивність додатків (голосові та відеодзвінки), потокове відео та віддалений доступ до робочих столів.

Керування мережевим трафіком являє собою набір методів, які спрямовані на оптимізацію передавання даних у мережі. Ці методи включають контроль смуги пропускання, обмеження швидкості, блокування небажаного трафіку і пріоритизацію даних. Quality of Service (QoS) є технологією, яка надає пріоритет певним типам трафіку, забезпечуючи стабільність і мінімізацію затримок, особливо важливих для критично важливих застосунків.

Для налаштування пріоритетів в мережі для більш ефективної роботи необхідні наступні кроки.

1. У налаштуваннях маршрутизатора знайти розділ QoS і вказати, які види трафіку (відеодзвінки, стрімінг, передача файлів) повинні мати пріоритет.

2. Виділити додатки, яким потрібні низькі затримки і висока швидкість, як-от голосові та відеодзвінки, стримінг або віддалений доступ.

3. Створити віртуальні локальні мережі (VLAN) для критично важливого трафіку, такого як VoIP або відеоконференції. Налаштувати QoS для цих VLAN, щоб забезпечити їм пріоритет.

4. Встановити обмеження пропускної здатності для трафіку, який не є критично важливим, щоб уникнути його впливу на важливі потоки даних.

5. Налаштувати Wi-Fi роутер так, щоб різні канали використовувалися для різних видів трафіку, забезпечуючи пріоритет критично важливим потокам даних.

6. Регулярно стежити за роботою мережі та корегувати пріоритети застосунків залежно від мінливого завантаження [3].

Застосування цих кроків допоможе мережі більш ефективно обслуговувати різні потреби користувачів і додатків, водночас надаючи

пріоритет найважливішим завданням і мінімізуючи вплив менш критичних даних.

2.4. Безпека мережі та її вплив на швидкість

Мережева безпека також може вплинути на швидкість локальної мережі. Деякі заходи безпеки, як-от брандмауери й антивірусне програмне забезпечення, можуть споживати ресурси та знижувати швидкість. Атаки, як-от DDoS, віруси та шкідливі програми, не тільки можуть спричинити відмови в роботі, а й значно знизити пропускну спроможність і спричинити затримки в пересиланні даних. Отже, безпека мережі безпосередньо впливає на її здатність ефективно обслуговувати потреби користувачів і додатків.

Крім того, застосування шифрування для захисту даних, хоча і є необхідним кроком, може також вплинути на продуктивність. Складність алгоритмів шифрування та обсяг переданих даних можуть призвести до збільшення затримок, особливо на більш високих рівнях шифрування. Цей баланс між безпекою та продуктивністю вимагає уважного зважування залежно від конкретних потреб і рівня чутливості даних.

Критичним аспектом також є управління доступом. Впровадження суворих політик управління доступом може створити додаткові запити на аутентифікацію та авторизацію. Неоптимізоване управління доступом може знизити швидкість доступу до ресурсів, що впливає на загальну продуктивність мережі [7, с. 229]. Тому балансування між високим рівнем безпеки та оптимальною продуктивністю стає ключовим питанням для сучасних мереж.

Для забезпечення безпеки мережі без зниження швидкості доцільно здійснювати наступні інструкції.

1. Оновлювати ОС і ПЗ регулярно, щоб виправляти вразливості та запобігати атакам. Багато оновлень також включають оптимізації продуктивності.

2. Використовувати проксі-сервери та фаєрволи для контролю трафіку та запобігання вторгнень. Оптимізувати їхні налаштування, щоб знизити вплив на швидкість передавання даних.

3. Вибирати алгоритми шифрування, які забезпечують достатній рівень безпеки за мінімального впливу на продуктивність. Наприклад, використання апаратного прискорення шифрування може поліпшити ефективність.

4. При використанні віртуальної приватної мережі (VPN), обирати протоколи, які забезпечують хороший захист і водночас не надто знижують швидкість передавання даних.

5. Реалізувати ефективні методи управління доступом, мінімізуючи запити на автентифікацію та авторизацію. Використовувати групові політики для спрощення процесів.

6. Впровадити системи моніторингу безпеки, які можуть виявляти аномалії в реальному часі та реагувати на загрози, мінімізуючи їхній вплив на продуктивність [4].

Спільне забезпечення безпеки з високою продуктивністю вимагає балансу і ретельного налаштування. З правильними методами та інструментами, мережа може залишатися безпечною та ефективною одночасно.

Отже, швидкість локальної мережі є важливим фактором, який визначає, наскільки ефективно комп’ютери можуть обмінюватися даними один з одним. І існує безліч способів підвищити швидкість локальної мережі. Однак, мережева інфраструктура постійно розвивається, тому важливо стежити за новими технологіями і тенденціями. Це допоможе підтримувати мережу в актуальному стані та забезпечити максимальну продуктивність.

В цьому розділі було розглянуто швидкісні параметри у локальних мережах, обмін інформацією в ній, технології та обчислення, що застосовуються при побудові мереж. Проведення оцінювання поточного стану мережі, перелік засобів, якими можливо здійснити аналіз мережі. Поліпшення мережевої та безпекової інфраструктури телекомунікаційної мережі.

РОЗДІЛ ІІІ. ПРОЄКТУВАННЯ, РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ДЛЯ КОМУНАЛЬНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА «КАМ'ЯНЕЦЬ-ПОДІЛЬСЬКА МІСЬКА ЛІКАРНЯ КАМ'ЯНЕЦЬ-ПОДІЛЬСЬКОЇ МІСЬКОЇ РАДИ»

3.1. Розробка та розрахунок базових функціональних можливостей мережі медичного закладу

В цій кваліфікаційній роботі моделі мережі були модифіковані і є дещо неточними, це зроблено з метою міркувань безпеки для даного об’єкту.

3.1.1. Характеристика підприємства для якого створюється проєкт мережі

Повна назва закладу: Комунальне некомерційне підприємство Кам'янець-Подільська міська лікарня Кам'янець-Подільської міської ради.

Адреса: 32302, Україна, Кам'янець-Подільський р-н, Хмельницька обл., місто Кам'янець-Подільський, вулиця Мазепи Івана, будинок, 31

Кам'янець-Подільська міська лікарня має наступні відділення:

- Кардіологічне відділення
- Травматологічне відділення
- Інфекційне відділення
- Хірургічне відділення №1
- Хірургічне відділення №2
- Урологічне відділення
- Адміністрація лікарні
- Анестезіологічне відділення з палатами інтенсивної терапії
- Відділення гострого мозкового інсульту
- Клініко-діагностична лабораторія
- Отоларинтологічне-офтальмологічне відділення
- Терапевтичне відділення

– Приймальне відділення невідкладної медичної допомоги

– Рентгенологічне відділення та кабінети ультразвукової і функціональної діагностики

– Патологоанатомічне відділення

– Травмпункт

Лікарський заклад має багато різних відділень, які працюють по своїй специфіці, з своїм обладнанням. Кожне відділення має свою комп'ютерну техніку, робочі місця. В кожному відділенні має бути доступ до інтернету та до МІС для належної роботи з електронними документами та обміном потрібної інформації.

Система основних інформаційних потоків в лікувальному закладі виглядає наступним чином:

Мал. 3.1. - Система основних інформаційних потоків в лікувальному закладі

3.1.2. Технічне завдання з розробки мережі

На даний момент в лікарні існує комп'ютерна мережа, проте вже зараз з нею виникають аварійні інциденти. Застаріле обладнання, аварійний стан кабельних трас, релокація персоналу і устаткування, що потребує під'єднання

до мережі, відкриття нових відділів та модернізація нинішньої мережі декількома поколіннями мережевих інженерів, що робили надбудови, перебудови, модернізації без будь-яких відміток та нотаток приводить до висновку, що наявна мережа є хаотичною та заплутаною, недостатньо розвинутою в певних місцях і застарілою та без жодної мережевої карти, дописів, документації.

Модернізація та перебудова такої мережі є складним і часто марним процесом, що не надовго віддаляє необхідність заміни. Також до балансу лікарні недавно був переведений ще один корпус, з своїм обладнанням, що означає необхідність проєктування повністю нової мережевої гілки.

Найбільш сприятливим варіантом для установи буде частковий демонтаж наявної мережі, та побудова нової, структурно продуманої мережі.

Сформуємо технічні завдання, які необхідно втілити для досягнення мети роботи:

1. спроєктувати відділи лікарні, визначити приблизну кількість і розташування техніки яка потребує з’єднань з мережею;
2. розробка логічної схеми мережі;
3. проєктування телекомунікаційної мережі, позначення активного та пасивного обладнання в мережі, позначення робочих станцій;
4. розробка моделі мережі, її налаштування.

3.1.3. Топологія та використані технології телекомунікаційної мережі

Існує безліч способів з’єднання мережевих пристроїв. Багато з них вже є застарілими, зараз використовують такі топології:

- Зірка;
- Кільце;
- Сітка;
- Деревоподібна;
- Гібридна.

Часто окремі топології є комбінаціями базових. У загальному випадку такі топології називаються змішаними або гібридними, але деякі з них мають власні назви, наприклад «Дерево». Однак ці топології накладають певні обмеження на:

– довжину лінії зв’язку між двома вузлами;
– кількість вузлів в мережі;
– інтенсивність трафіку.

Для зняття цих обмежень використовуються спеціальні методи. Структурування мережі та спеціальне мережеве обладнання – повторювачі (ретранслятори), медіаконвертори, комутатори, маршрутизатори. Це обладнання називається комунікаційним, з його допомогою окремі сегменти мережі взаємодіють один з одним.

Ретранслятор – найпростіший пристрій зв'язку, використовується для фізичного з'єднання різних сегментів кабелю або радіозв’язку локальної мережі з метою збільшення загальної довжини мережі. Ретранслятор покращує якість переданого сигналу (відновлює потужність, амплітуду сигналу і т. д.).

Медіаконвертер – це пристрій, який використовується для перетворення сигналів між різними типами фізичних середовищ передачі даних. Найчастіше це перетворення між оптоволоконними та мідними кабелями

Мережевий комутатор або світч (switch) – пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента.

Маршрутизатор або роутер (router) – спеціалізований мережевий комп'ютер, який має два або більше мережних інтерфейсів та пересилає пакети даних між різними сегментами мережі. Маршрутизатор може зв'язувати неоднорідні мережі різної архітектури. Для прийняття рішень про пересилку пакетів він використовує інформацію про топологію мережі та правила, встановлені адміністратором [24].

В цьому проєкті буде застосовуватись топологія «Дерево».

При побудові телекомунікаційної мережі потрібно встановити потреби, які очікуються від користувачів, установи. В випадку лікарського закладу необхідно залучати декілька технологій в одну мережу, а саме:

– Ethernet
– Wi-Fi
– PoE

Ethernet. В лікарні є багато комп'ютерів, які використовуються в якості робочих станцій, ці станції необхідно залучити до мережі, більшість таких станцій буде підключена кабелем, для цього ідеально підходить технологія Ethernet.

Wi-Fi. Для лікарні є важливою функція безпровідного зв'язку. Деякі відділи облаштовані ноутбуками в якості робочих станцій, їх також необхідно залучити в мережу. Також персоналу є необхідною можливість підключатись до мережі Wi-Fi з інших пристроїв для обміну інформацією. В вимогах від МОЗ є також рішення про Wi-Fi покриття відділів, де є можливим перебування відвідувачів, або пацієнтів. Цю аудиторію необхідно забезпечити Wi-Fi зв'язком. Такі користувачі будуть підключатись до окремої «гостьової» Wi-Fi мережі.

PoE. В багатьох місцях розташування комутаційного обладнання будуть відсутні розетки електроживлення. В деяких місцях ці проблеми будуть вирішуватись встановленням окремих розеток живлення для мережі, але це не є можливим у всіх місцях. Технологія PoE дозволить використовувати звиту пару і як середовище передавання інформації, і як джерело живлення для комутаційного обладнання.

3.1.4. Розрахунки продуктивності мережі

Максимальна пропускна здатність не завжди дорівнює фактичній пропускній здатності мережі, особливо коли на неї впливають такі фактори мережі, як трафік.

Використовуючи формулу 2.1 наведену у розділі 2.1 розрахуємо необхідну пропускну здатність TCP (біт/с) для мережі медичного закладу.

Є гігабітний Ethernet-канал між серверами із круговою затримкою 30 мс. Наприклад, необхідно надіслати великий файл із одного сервера на інший сервер за протоколом FTP.

Розрахунок реальної пропускної здатності відбувається за наступним алгоритмом.

Спершу необхідно перевести розмір TCP-вікна з байтів у біти.

В даному випадку буде задіяно стандартне TCP-вікно Windows-машини розміром 64 КБ = 65536 Б = 65536 * 8 = 524288 біт.

Потім необхідно взяти розмір TCP-вікна в бітах і розділити його на кругову латентність каналу, виражену в секундах. Для цілей даних розрахунків 30 мс перетворюється на 0.030 с.

Максимальна пропускна спроможність TCP = 524 288 біт / 0.030 с = 17 476 266 біт/с = 17.4 Мбіт/с

Таким чином, незважаючи на те, що між двома серверами є гігабітний Ethernet-зв'язок, при передачі файлів не можна розраховувати більш ніж на 17 Мбіт/с.

Для розрахунку оптимального розміру TCP-вікна у нашій мережі для гігабітного Ethernet-маршруту між серверами з круговою затримкою 30 мс, використовуємо формулу 2.2. і отримуємо таке значення:

1 000 000 000 біт/с * 0.030 с = 30 000 000 біт/8 = 3 750 000 байтів.

Іншими словами, якщо налаштувати обидва сервери на TCP-вікно в 3750 КБ, FTP-з'єднання повністю заповнить смугу пропускання і досягне пропускної здатності в 1 Гбіт/с.

Для розрахунку кругової затримки (мс) використовуємо формулу 2.3.

Розрахуємо максимально допустиму затримку сигналу на ділянці між двома віддаленими серверами щоб гарантувати пропускну здатність FTP 10 Гбіт/с, використовуючи стандартний розмір TCP-вікна (64 КБ).

524 288 біт / 10 000 000 000 біт/с = 52.4 мікросекунди

3.1.5. IP адресація в мережі

IP адресація є важливим моментом в будь-якій мережі. В випадку лікарського закладу і додаткових рекомендаціях від МОЗ маємо вимогу про ділення адресного простору на підмережі, де відбувається розподіл між підмережею для персоналу та обміну чутливою інформацією, та з другої сторони мережі для пацієнтів та громадян, які перебувають в лікарні для доступу в мережу Інтернет.

Коротко розберемо IP адресацію та маски IP адрес і створимо приклад ділення на підмережу для певного відділення лікарні.

IP адреси поділяються на класи, їх є 5. Самі по собі вони вже поділені і кожен клас має свій діапазон:

Таблиця 3.1.

Класи IP-адрес

Клас	Маска	Початковий адрес мережі	Кінцевий адрес мережі	Максимальна кількість мереж	Максимальна кількість вузлів у мережі
A	255.0.0.0	0.0.0.0	127.255.255.255	128	16 777 216
B	255.255.0.0	128.0.0.0	191.255.255.255	16 384	65 536
C	255.255.255.0	192.0.0.0	223.255.255.255	2 097 152	256
D	Груповий адрес	224.0.0.0	239.255.255.255	-	Багатоадресний
E	Зарезервований	240.0.0.0	255.255.255.255	-	Зарезервований

Для більш гнучкого керування IP-адресами, їх діапазоном, використовують мережеві маски. Маска підмережі в IP-адресації використовується для визначення меж підмережі, тобто для розділення IP-адреси на частини, які представляють мережу та хост (пристрій у цій мережі). Вона допомагає визначити, які IP-адреси належать до однієї мережі, а які – до інших [15].

Маска дозволяє ділити мережі на підмережі. Це спрощує управління та підвищує безпеку. Наприклад, в лікарні можна поділити мережу на підмережі для різних відділів, щоб кожен відділ мав свій окремий сегмент.

Наведу приклад розподілення мережі на підмережі:

Припустимо, ми маємо мережу з адресою 10.0.0.0:

- Мережа: 10.0.0.0
- Маска: /24 або 255.255.255.0
- Кількість IP-адрес: 256 (254 для хостів)

Розділення на підмережі

Змінимо маску з 24 біт на 25 біт для створення двох підмереж. Це дозволить нам створити дві підмережі з 128 адресами в кожній.

Розрахунок.

1. Зміна маски з /24 на /25 означає, що перші 25 біт використовуються для частини мережі.

2. Оскільки маска /25 залишає 7 біт для хостів (32 - 25 = 7), у кожній підмережі буде 128 адрес (2^7 = 128), з яких 126 адрес доступні для хостів (мінус 1 мережна і 1 широкомовна адреса).

Таким чином, нові підмережі

Підмережа 1:

- Мережа: 10.0.0.0/25
- Діапазон IP-адрес для хостів: 10.0.0.1 – 10.0.0.126
- Широкомовна адреса: 10.0.0.127

Підмережа 2:

- Мережа: 10.0.0.128/25

- Діапазон IP-адрес для хостів: 10.0.0.129 – 10.0.0.254
- Широкомовна адреса: 10.0.0.255

3.2. Реалізація функціональних можливостей комп’ютерної мережі Кам'янець-Подільської міської лікарні

3.2.1. Розробка схематичної мережі

Головне мережеве обладнання та обчислювальна техніка розташована на другому поверсі головної будівлі, в якій нині розміщується друге відділення хірургії. Серед обладнання в серверній знаходиться:

- Маршрутизатор
- Комутатор
- Медіаконвертори
- Сервер для збереження даних
- Сервера – ПК для віддаленого доступу для лікарів

В серверну заходять оптоволоконні лінії від провайдерів, через медіаконвертори переходять в звиті пари, які вже надходять в головний маршрутизатор, який і є сполучником телекомунікаційної мережі лікарні і мережі Інтернет. Маршрутизатор сполучено з комутатором. До комутатора підключені решта обладнання серверної, а саме сервера і медіаконвертери. Медіаконвертери які під’єднані до комутатора є сполучниками серверної з відділами лікарні. Це необхідно через великі відстані між серверною і відділами. Оптоволоконні кабелі дозволяють передавати сигнал на 100 кілометрів, при 100 метрах звитої пари. Оптоволоконні лінії більш тонші і легші – це є перевагою в монтажі на великі відстані. Також оптоволокно передає дані набагато швидше через світлову технологію передачі сигналу. Все серверне обладнання підключено до ДБЖ (джерело безперебійного живлення). На випадок аварійних ситуацій ДБЖ підтримує живлення серверного обладнання, що дає час на підключення генераторної лінії персоналом, що заміняє централізоване постачання електроенергії. Серверна обладнана серверною стійкою, на які розставлено все комутаційне

обладнання. Важливим моментом є розташування обладнання з оптичним з’єднання. Таке обладнання ставиться вверху для забезпечення цілісності кабелів, та розподілення різних видів кабелів. В серверній також розташовано кондиціонер, який підтримує постійну температуру в кімнаті для сприятливого клімату роботи обладнання.

На другому поверсі головної будівлі в коридорі розташований ще один комутатор, який на пряму з’єднаний з серверним комутатор. На другому поверсі поки немає робочих станцій, цей комутатор є точкою масштабування для другого поверху.

Комутатор на другому поверсі є важливою ланкою, він з’єднує відділ хірургії №2, який базується на третьому поверсі, з’єднання відбувається по кабельній системі через стелю, звитою парою. На третьому поверсі окрім хірургії в сусідньому крилі розташоване лор-очне відділення. В хірургічному відділені розташовано 4 робочі станції і одна точка доступу. Все обладнання підключено звитою парою. Тут зони робочих станцій поділені на ординаторську, пост, що розташований в коридорі для прийому людей і окремий кабінет медичної сестри. Точка доступу використовується як вільне підключення до безпровідної мережі для відвідувачів та пацієнтів.

Комутатор з відділення хірургії №2 з’єднується напряму з комутатором в лор-очному відділенні. Тут розташовано 5 робочих станцій і одну точку доступу.

Загалом, кожне відділення має схожу структуру розташування робочих станцій:

- Ординаторська
- Пост
- Кабінет старшої медичної сестри
- Окремі станції в кабінетах лікарів.

Обладнання, що кріпиться в коридорах повинно мати фізичний захист від втручання сторонніх людей. Це гарантується висотою кріплення, таке обладнання розміщається високо, щоб не було можливості дістатись до

обладнання без додаткових засобів. Також на обраній висоті монтується спеціальний антивандальний ящик, в який заводяться мережеві кабелі та обладнання, яке необхідно розмістити на цій ділянці. Такі ящики виконані з металу і мають вбудовані замки, ключі залишаються у персонала з обслуговування мережі.

Клініко-діагностична лабораторія це невелика будівля. В ній проводяться різного роду експертизи. В цьому відділі лікарі, лаборанти працюють з різними медичними зразками без взаємодії з пацієнтами. Майже вся робота КДЛ відбувається на другому поверсі. Весь парк комп'ютерної техніки зосереджено там.

Корпус КДЛ знаходиться на одній території з серверною. Один з оптоволоконних кабелів серверної заведений до комутаційного обладнання, що розташований на другому поверсі. З сторони КДЛ розташований медіаконвертер, поряд з ним приймаючий комутатор та точка доступу для персоналу. З приймаючого комутатора проведено виту пару, яка виводиться в коридор, де на висоті встановлено комутатор, з якого направлена розводка кабелів до всієї комп'ютерної техніки. Також в коридорі є ще один комутатор, який обслуговує декілька окремих кімнат, де лаборанти працюють з специфічним технічним обладнанням. В цих кімнатах можуть проводитись зміни, масштабування. Цей комутатор має резервні місця підключення в випадку розширення комп'ютерної техніки.

Загалом в КДЛ розташовано 9 робочих станцій і одна точка доступу для персоналу.

Наступним відділом для опису буде відділ хірургії №1. В корпусі де розташовано цей відділ також знаходиться відділ невідкладної медичної допомоги.

Мережа в цьому корпусі починається з другого поверху. Оптоволокно заводиться з вулиці в антивандальний ящик на висоті в медіаконвертор, з медіаконвертора відбувається перехід в комутатор, звідки мережа починає

розгалужуватись по корпусі. На другому поверсі маємо пост з робочою станцією і точку доступу.

Далі в ординаторській маємо дві підключені робочі станції. Наступні підключення з комутатора розходяться на перший та третій поверх по кабельній системі.

Аналогічно до другого поверху на першому маємо комутатор і від нього розгалуження мережі по поверху. Різниця в тому, що на першому поверсі набагато більше підключень. Схематично перший поверх можна поділити на дві частини, де одну частину обслуговує комутатор, який приймає сигнал комутатора з другого поверху. Цей комутатор також під'єднано до комп'ютерів, які відносяться до відділу невідкладної медичної допомоги.

До першого роутера підключено:

- 9 робочих станцій
- 1 точка доступу

До другого комутатора, який підтримує другу частину першого поверху підключено:

- 4 робочі станції
- 1 точка доступу

На третьому поверсі розміщено один комутатор разом з точкою доступу.

Біля обладнання одразу знаходиться ординаторська з комп'ютерною технікою, куди прокладені кабелі витої пари. В другому крилі третього поверху в кімнаті підключено ще один комп'ютер. Також в другому крилі в коридорі встановлено точку доступу. Загалом 5 робочих місць і 2 точки доступу.

Останній корпус лікарні який розглядається в цій кваліфікаційній роботі охоплює відділи кардіології, терапії, неврології та отоларинтологічне-офтальмологічне відділення.

Мережа починається з другого поверху. Аналогічно до попередніх корпусів з вулиці заходить оптоволокно, з медіаконвертора переходить в виту пару і підключається в комутатор. Перший і другий поверх мають два крила.

Розташування обладнання було обрано так, щоб комутатори, які будуть обслуговувати третій і четвертий поверх були на одному рівні в розташуванні з приймаючим комутатором на другому поверсі і кабельна система не піддавалась змінам.

Перші два поверхи корпусу мають по два комутатори, кожен з яких відповідає за окреме крило.

До комутатора лівого крила першого поверху підключено:

- 6 робочих місць
- 2 точки доступу

До комутатора правого крила першого поверху підключено:

- 6 робочих місць
- 2 точки доступу

До комутатора лівого крила другого поверху підключено:

- 5 робочих місць
- 2 точки доступу

До комутатора правого крила другого поверху підключено:

- 8 робочих місць
- 4 точки доступу

Комутатор на третьому поверсі має такі підключення:

- 5 робочих місць
- 2 точки доступу

Комутатор на четвертому поверсі має такі підключення:

- 4 робочих місця
- 2 точки доступу

Всі схематичні моделі мережі, які пов’язані з даним розділом згадано в додатках (Додатки А-Г).

3.2.2 Проєктування віртуальної моделі мережі

Для кращого розуміння мережі, виявлення дефектів, спроби первинного тестового налаштування створена модель мережі. Віртуальна модель мережі

виконана в Cisco Packet Tracer. Ця модель розділена на кілька відокремлених один від одного частин, які в свою чергу окреслені зоною. Кожна частина мережі є моделлю мережі певного корпусу лікарні, який був спроєктований в редакторі. Кожна зона має назву, відповідну до назви корпусу, певні зони мають позначення поверхів корпусу.

Розшифровка деяких частин моделі:

Bridge-PT – Медіаконвертор (перехідник між оптоволокном і витою парою).

Fiber (Червоний кабель) – оптоволоконний кабель.

Copper Straight-Through (Чорний кабель) – вита пара.

Copper Cross-Over (Пунктирний чорний кабель) – Крос кабель, або ж перехресний. Має змінений обжим, змінює перестановку пінів в RJ45. Використовується для під'єднання однотипних пристроїв один до одного, наприклад: комп'ютер - комп'ютер, комутатор – комутатор.

AccessPoint-PT – точка доступу Wi-Fi підключення.

Всі віртуальні моделі мережі, які пов'язані з даним розділом згадано в додатках (Додатки Ґ-З).

3.2.3 Логічна схема мережі

Логічна модель описує роботу мережі на рівні взаємодії мережевих функцій та правил встановлення зв'язку між кінцевими системами, взаємодіючими через телекомунікаційну мережу [8, с. 42].

Логічна схема мережі відрізняється від моделі і мережевого плану розташування тим, що надає саму структуру побудови мережі, тобто концептуальний вигляд мережі, де зображено основні пристрої без нагромадження можливих підключень. Така схема дає зрозуміти працівникам суть роботи мережі, її головний функціонал, що допомагає скоординувати роботу для вирішення проблеми, налаштування, модернізації. Логічна схема мережі представлена у додатках.

Таким чином, в третьому розділі була здійснена розробка функціональних можливостей медичного закладу, де була надана структура закладу, його характеристика, було розроблене покрокове технічне завдання і наданий опис використаних технологій для реалізації задач, що були поставленні завданням. Представлені реалізація функціональних можливостей комп'ютерної мережі, опис функціонування мережі, проєктування віртуальної моделі та логічної схеми мережі.

Логічна модель мережі, яка пов'язані з даним розділом згадана в додатках (Додаток И).

РОЗДІЛ IV. ДІАГНОСТИКА ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ТА МОЖЛИВОСТІ МОДЕРНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ КОМУНАЛЬНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА «КАМ'ЯНЕЦЬ-ПОДІЛЬСЬКА МІСЬКА ЛІКАРНЯ КАМ'ЯНЕЦЬ-ПОДІЛЬСЬКОЇ МІСЬКОЇ РАДИ»

4.1. Тестування комп’ютерної мережі Кам'янець-Подільської міської лікарні

Приклади налаштування мережевих пристроїв:

1. Сегментування кінцевих пристроїв (VLAN)

VLAN – логічна «віртуальна» локальна комп’ютерна мережа, вона представляє собою групу кінцевих пристроїв з загальним набором потреб для всіх цих пристроїв. Вони взаємодіють так, ніби підключені до широкомовного домену, в незалежності їх фізичного розташування.

VLAN дає можливість розділяти направлені запити в мережі в розбиті групи користувачів, що покращує роботу мережі, запити надходять тільки певній групі хостів, а не всім кінцевим пристроям в мережі. Також VLAN відділяє одні кінцеві пристрої від інших посилюючи таким чином безпеку мережі, що в випадку мережі лікарні важливо.

Приклад налаштованого VLAN:

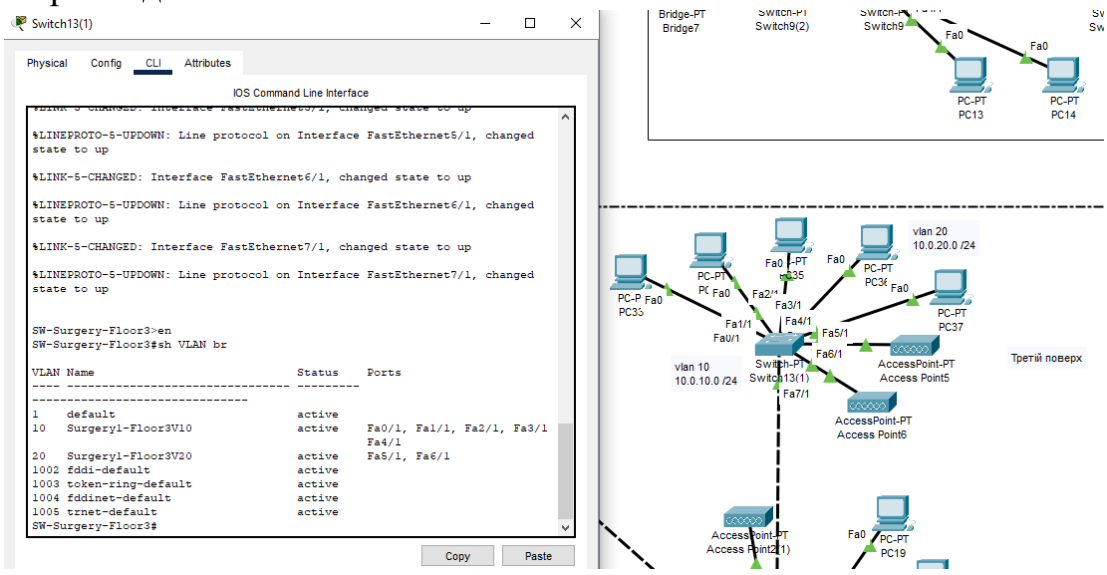


Рис. 4.1. – Налаштування VLAN

VLAN налаштовано на окремі порти комутатора, до якого підключаються відповідні пристрої.

Важливим моментом також є налаштування режиму портів. Їх є два:

- Access – Такий порт працює тільки для одного призначеного для нього VLAN
- Trunk – Порт вставляє в сегмент, який передається тег VLAN від якого йде повідомлення, це дає змогу обмінюватись кінцевим пристроям інформацією поза своїм VLAN

Приклад оголошення режиму Trunk для порта:

```
SW-Surgery-Floor3>en
SW-Surgery-Floor3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-Surgery-Floor3(config)#int f7/1
SW-Surgery-Floor3(config-if)#switchport mode trunk
```

Рис. 4.2. – Режим Trunk

Такий порт потрібно призначати на вихідний порт з іншим комутаційним обладнанням, для того, щоб інформацію могли отримувати кінцеві пристрої в VLAN.

Маючи багатоповерхові будівлі лікарні декілька комутаторів з’єднані один з одним, після чого один з них з’єднується з роутером для отримання IP адрес. Для цього комутатори та роутер повинні знати про існуючі VLAN в мережі.

Приклад налаштування передачі інформації про доступні VLAN іншим пристроям [27]:

- interface FastEthernet0/24 (порт до роутера або комутатора)
- switchport mode trunk (зміна налаштування порту)
- switchport trunk allowed vlan all (або перелік VLAN, які потрібні)
- exit

Далі, для розпізнавання VLAN мереж іншими комутаторами необхідно створити запис VLAN мереж в налаштуваннях:

- vlan [номер_VLAN]
- name [назва_VLAN]
- exit

Важливим є налаштування роутера для VLAN. Розрізняють два види підключень роутера для VLAN:

- Традиційний:

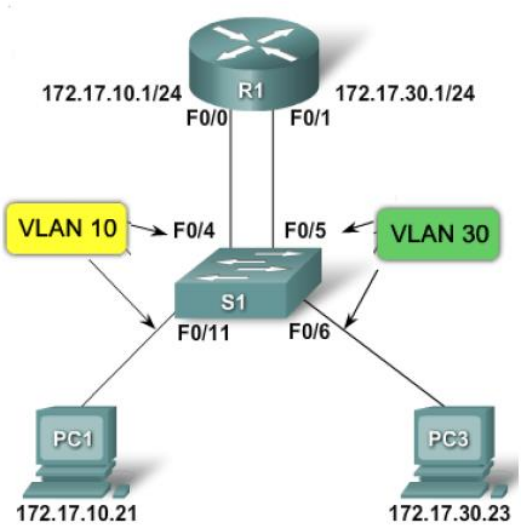


Рис. 4.3. – Традиційне налаштування VLAN для роутера

В даному випадку на кожен VLAN виділяється окремий порт.

- Router on stick:

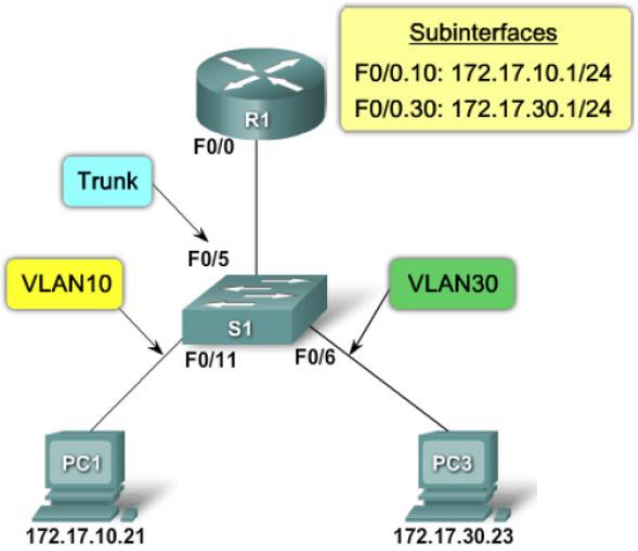


Рис. 4.4. – Налаштування роутера за технологією Router on stick

В даному випадку відбувається інкапсуляція одного порту. Він ділиться на підпорти, які налаштовуються для окремого VLAN.

В лікарні велика розподілена мережа, наш вибір метод «Router on stick».

Приклад налаштування:

- interface GigabitEthernet0/0.10 (або FastEthernet)
- encapsulation dot1Q 10 (номер VLAN)
- ip address 10.0.10.1 255.255.255.0 (адреса в підмережі VLAN)

Результат налаштування в конфігу роутера [28]:

```
Output_Router(config)#do sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     147.144.5.2     YES unset  up                    up
GigabitEthernet1/0     10.0.0.1        YES manual up                    up
GigabitEthernet1/0.10  10.0.10.1       YES manual up                    up
GigabitEthernet1/0.20  10.0.20.1       YES manual up                    up
Serial2/0              unassigned      YES unset  administratively down down
Serial3/0              unassigned      YES unset  administratively down down
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
Output_Router(config)#
```

Рис. 4.5. – Консольне меню налаштування роутера

2. DHCP

DHCP – це протокол прикладного рівня, який робить можливим автоматизовану роздачу IP адрес. DHCP може виконувати й інші важливі задачі. В цій мережі він відіграє важливу роль, адже комп’ютерної техніки в лікарні багато і вона розташована в різних місцях. Здійснювати статичну IP адресацію буде надважко і безрезультативно.

DHCP можна налаштовувати як на окремих серверах, так і на маршрутизаторах. В нашому випадку DHCP реалізовано на маршрутизаторі.

Приклад налаштування [29, 30, 31]:

- Ip dhcp excluded-address 10.0.10.1 10.0.10.10
- Ip dhcp excluded-address 10.0.20.1 10.0.20.10
- Ip dhcp pool vlan10Surgery1
- Default-router 10.0.10.1
- Network 10.0.10.0 255.255.255.0

- Exit
- Ip dhcp pool vlan20Surgery1
- Default-router 10.0.20.1
- Network 10.0.20.0 255.255.255.0

```
hostname Output_Router
!
!
!
!
ip dhcp excluded-address 10.0.10.1 10.0.10.10
ip dhcp excluded-address 10.0.20.1 10.0.20.10
!
ip dhcp pool vlan10Surgery1
 network 10.0.10.0 255.255.255.0
 default-router 10.0.10.1
ip dhcp pool vlan20Surgery1
 network 10.0.20.0 255.255.255.0
 default-router 10.0.20.1
!
```

Рис. 4.6. – Налаштування DHCP

3. Port Security

Технологія Port Security дозволяє обмежити перелік MAC-адрес на певному порту комутатора. При застосуванні Port Security комутатор не буде передавати через певний порт кадри від відправників, MAC-адреси яких відсутні у списку.

Такий тип захисту портів в мережі захищає від атак типу «MAC Address Flooding».

Для налаштування Port Security необхідно визначити тип його роботи, є три різновиди:

- Статичні адреси – адміністратор власноруч створює перелік дозволених MAC-адрес на певному порту.
- Динамічні адреси – комутатор динамічно створює перелік з числа MAC-адрес, що надходять з певного порту. При перезавантаженні комутатора інформація втрачається.
- Липкі (Sticky) адреси – адреси вивчаються динамічно, але існує можливість їх зафіксувати в конфігураційному файлі.

В випадку мережі для лікарні скористаємось «Sticky» режимом.

Додатковим в налаштуванні є реакція на загрозу, таких режимів також три:

- **protect** Security violation protect mode
- **restrict** Security violation restrict mode
- **shutdown** Security violation shutdown mode

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	Yes	No	Yes	Yes

Рис. 4.7. – Режими налаштування Port Security

- Приклад налаштування:
- int f 0/1
- switchport mode access
- switchport port-security
- switchport port-security maximum 10
- switchport port-security mac-address sticky
- switchport port-security violation restrict

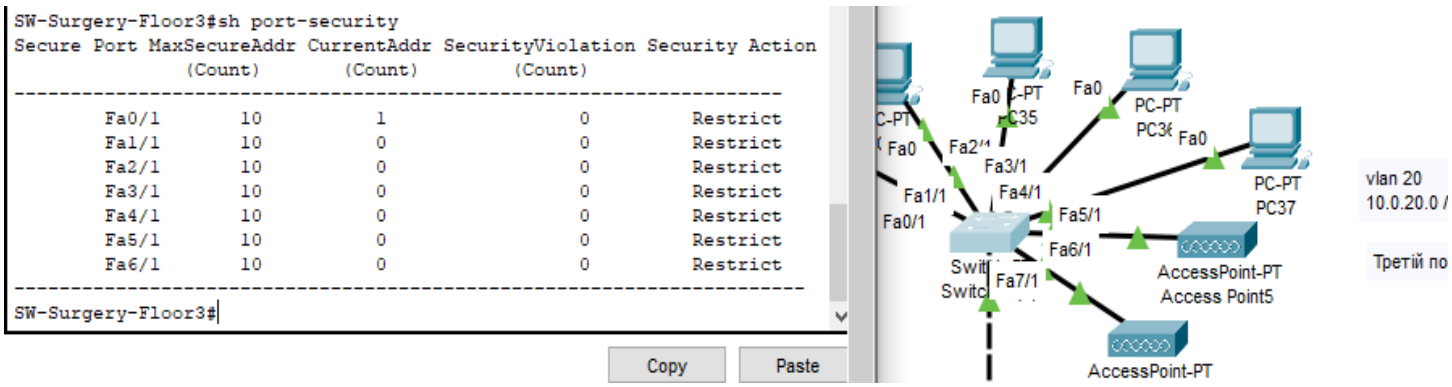


Рис. 4.8. – Налаштування Port Security

4. Статична адресація

Хоч в телекомунікаційній мережі застосовується технологія DHCP в деяких місцях варто використовувати статичні адреси, для звичайних користувачів це можуть бути мережеві принтери, або подібні технічні пристрої.

В мережі застосовуються декілька серверів, які виконують поставлені на них задачі, їм варто роздавати статичні адреси, які виділені для них з пулу динамічних і ніколи не змінюються. Це необхідно для стабільності роботи мережі, адже вони є головною частиною функціоналу, до них необхідно прокласти один постійний маршрут, який не буде змінюватись для робочих станцій, які обмінюються інформацією.

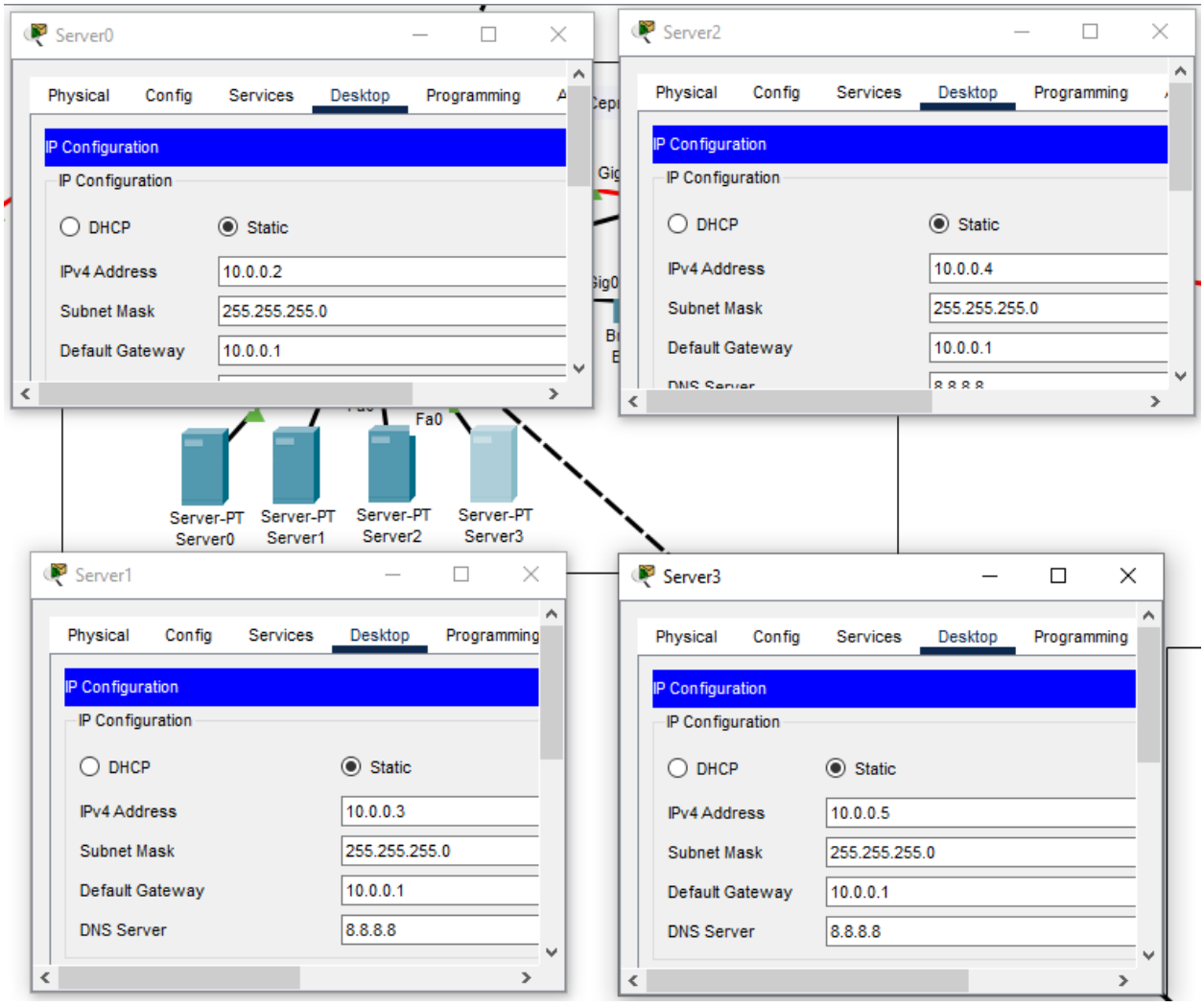


Рис. 4.9. – Налаштування статичної адресації

5. Перевірка зв’язку між пристроями

Здійснимо загальну перевірку комунікації між пристроями:

Відправимо з консолі комп’ютера, що приєднаний до комутатора в 10 VLAN на різні адреси команду PING:

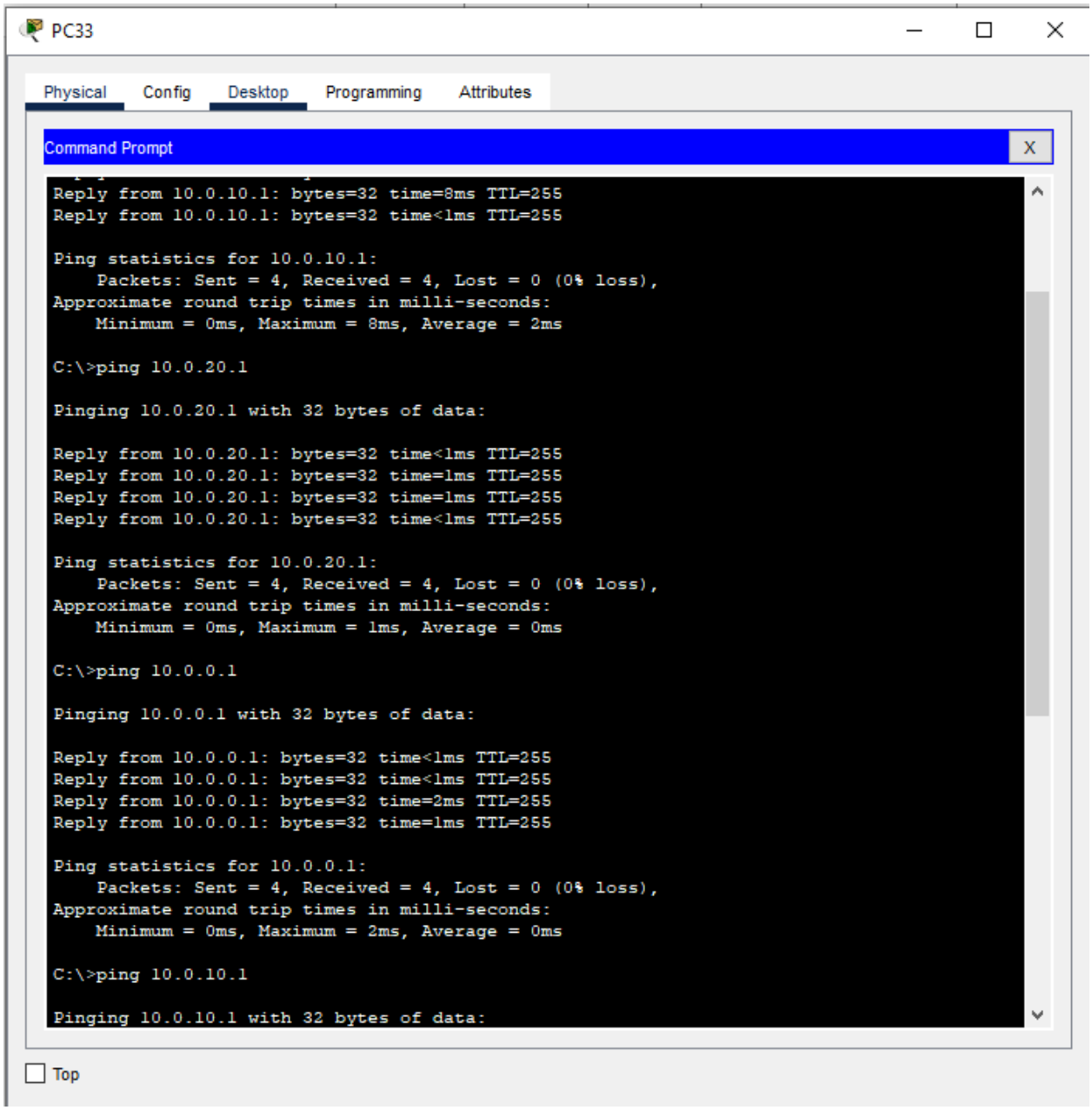


Рис. 4.10. – Перевірка зв’язку в мережі з кінцевого пристрою

Команда PING з сервера:

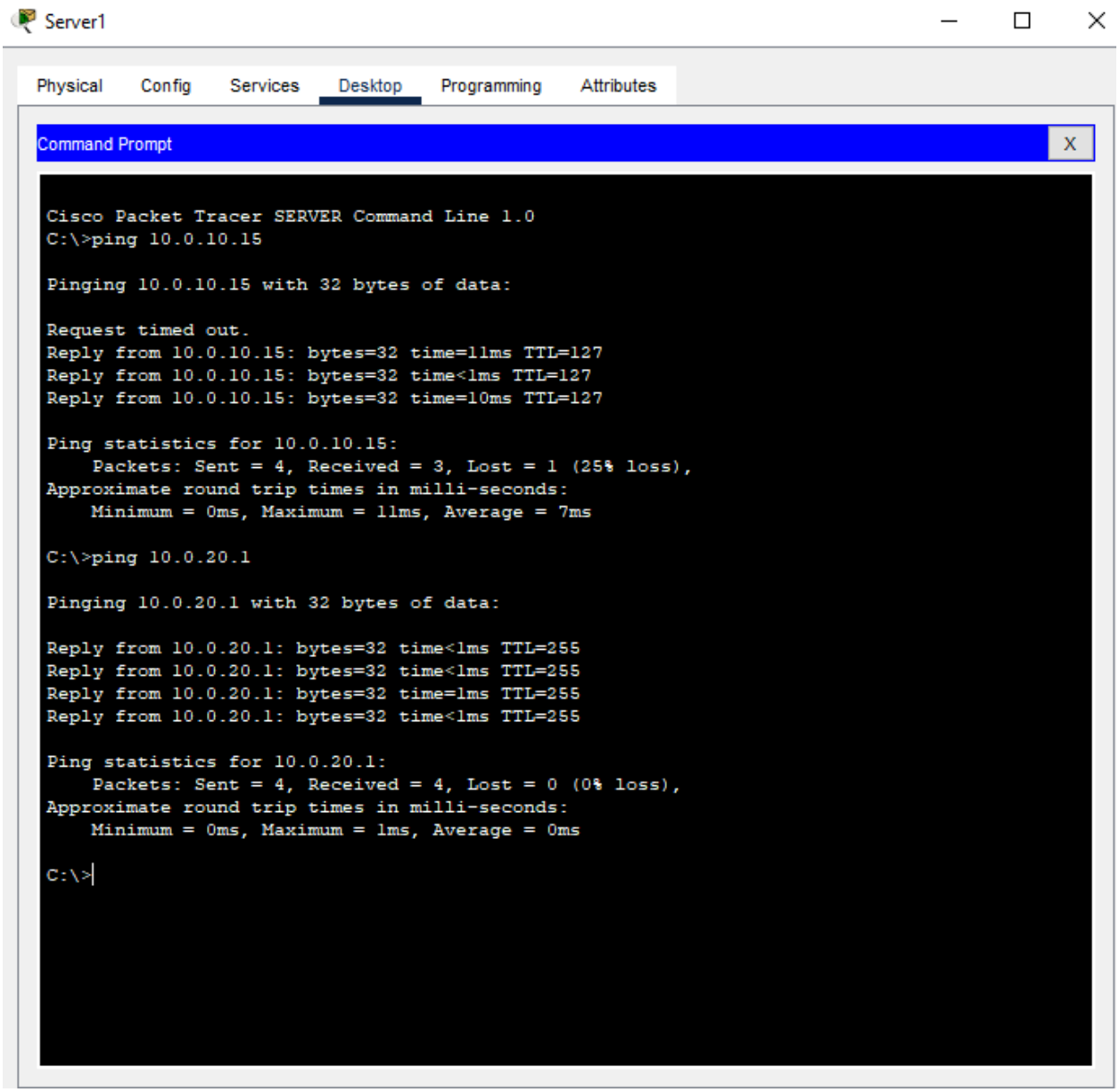


Рис. 4.11. – Перевірка зв’язку в мережі з сервера

При «пінгуванні» адреси 10.0.10.15 бачимо, що перший пакет не пройшов і отримав повідомлення «Request timed out». Це означає, що сервер не знав про існування цього пристрою в мережі. В його таблиці комутації, де є записи інших пристроїв до яких він може звертатись не було інформації про цей кінцевий пристрій. Перший пакет був розвідувальним, де кінцевий пристрій мав відкликнутись і надати інформацію про себе. Після чого наступні пакети пройшли без проблем.

4.2. Можливості модернізації телекомунікаційної мережі Кам'янець-Подільської міської лікарні

Час від часу мережа потребує обслуговування, різного, від ремонту і налаштувань до модернізацій. Різні установи та підприємства через деякий час змінюють комп’ютерну техніку, закуповують нові робочі станції.

Міська лікарня має багато можливостей для відкриття нових відділень, переформування, перерозподілу вже створених відділень. В таких випадках до підключеної в мережу техніки додаються нові робочі станції, які необхідно підключити в мережу. Також в лікарні є ще корпуса, які не обладнані, такі місця розглядаються для відкриття нових відділень, або розширень існуючих. В таких випадках частим питанням постає розширення мережі. Для міської лікарні є різні варіанти модернізації в залежності від поставленої цілі. Якщо це додавання певної техніки, яка вимагає підключення до мережі в вже готове відділення розглядається можливість підключення такої техніки до вже заведеної мережі. Майже в кожному відділенні розміщено комутатор, який відповідає за обмін даними в мережі, нову техніку можна підключити до вже існуючої гілки. Питання також може бути вирішене покупкою більш потужного комутатора, який розрахований на більшу кількість портів, якщо для нової техніки не вистачає місця.

Серверна облаштована серверною стійкою, що дозволяє при необхідності додавати обладнання, якщо воно буде потребуватись.

У випадку відкриття нового відділення в крилах корпусів, де немає заведеного мережевого обладнання модернізація буде проводитись схожим чином з заведенням окремої гілки з комутаційним обладнанням. Гілка може бути додана від сусідньої гілки, якщо поруч є відділення з розвинутим мережевим розгалуженням. В крайньому випадку є можливість створення нового підключення з вулиці, заведенням оптоволоконного кабелю для забезпечення мережі в корпусі.

Модернізація також полягає в оновленні програмного забезпечення. Загалом комутаційне обладнання має можливість самооновлення, що вирішує

дане питання, оновлення такого забезпечення відбувається вночі, коли працівники не користаються мережею.

4.3 Рекомендації для впровадження мереж в медичних закладах

Базуючись на нормативних документах та вимогах МОЗ складемо рекомендації для впровадження мереж в лікарські заклади:

1. Забезпечення конфіденційності та цілісності інформації

– Використовувати засоби криптографічного захисту інформації, що мають позитивний експертний висновок від державної експертизи.

– У разі передачі медичної інформації без підключення до ЦБД ЕСОЗ (Центральна база даних електронної системи охорони здоров'я), застосовувати відокремлені засоби криптографічного захисту.

– Передавати всі медичні дані та персональну інформацію у зашифрованому вигляді.

2. Вимоги до пристроїв зв'язку

– Забезпечити контроль доступу до налаштувань мережевого обладнання. Зовнішній доступ до налаштувань заборонено, налаштування доступне виключно з середини мережі.

– Адміністративно відключити всі внутрішні та зовнішні порти, які не використовуються.

– Використовувати мережеве обладнання з актуальними оновленнями ПЗ від виробника.

– Відокремлювати мережі МІС від загальнодоступних мереж, таких як Wi-Fi для пацієнтів.

– Обмежити фізичний доступ до пристроїв зв'язку лише авторизованим персоналом.

3. Вибір провайдера каналів зв'язку

– Обирати провайдерів з чинними атестатами відповідності системи захисту ЗВІД (Захищений вузол інтернет доступу).

Укладені угоди з провайдером повинні включати такі аспекти:

– Робочі години лікарського закладу.

– Узгоджені показники доступності послуг зв’язку (SLA).

– Максимально допустимий час недоступності.

– Механізми інформування відповідальних осіб про аварії чи перебої.

4. Організація мережевої безпеки

– Забезпечити належний рівень складності паролів для адміністраторів мережевого обладнання та їх регулярну зміну.

– Налаштувати доступ до мережевого обладнання відповідно до політики безпеки згідно з ДССЗЗІ (Державна служба спеціального зв’язку та захисту інформації України).

– Забезпечити постійний моніторинг безпеки мережевого середовища.

5. Дотримання нормативних вимог

– Орієнтуватися на вимоги ДССЗЗІ та використовувати лише затверджені технічні рішення.

– Дотримуватись переліку рекомендованих засобів крипто-графічного захисту та пристроїв зв’язку на офіційних ресурсах ДССЗЗІ.

Даний список рекомендацій допоможе створити або модернізувати мережу будь-якого лікарського закладу відповідно до необхідних критеріїв безпеки та експлуатації.

Отже, в четвертому розділі були надані приклади налаштування мережі на віртуальній моделі, тестування роботи цієї моделі з внутрішніми налаштуваннями мережі. Проведено опис можливостей майбутніх модернізацій телекомунікаційної мережі, при такій необхідності. Створення рекомендацій для впровадження мереж в лікарські установи.

ВИСНОВКИ

У процесі підготовки кваліфікаційної роботи були виконані наступні задачі:

- визначені критерії впровадження телекомунікаційних мереж в лікарські структури;
- здійснена оцінка продуктивності та працездатності мереж;
- розроблена телекомунікаційна мережа для Кам'янець-Подільської міської лікарні Кам'янець-Подільської міської ради;
- проведена діагностика мережі та розглянуті можливості модернізації мережі;
- сформовані ряд рекомендацій з впровадження комп’ютерних мереж у медичних закладах.

У першому розділі були проаналізовані нормативні документи, вимоги до обміну медичною інформацією в мережі, технічне та програмне забезпечення пристроїв, що підключені до мережі.

Впровадження медичних інформаційних систем у діяльність закладів охорони здоров’я дозволяють оптимізувати та покращувати якість надання медичної допомоги, підвищувати рівень координації та диференціації між структурними підрозділами, сприяють розвитку сфери охорони здоров’я в цілому.

У другому розділі висвітлено швидкість передачі даних в мережах. Було проведено оцінку поточного стану мережі, розглянуто можливості поліпшення якості мережевої інфраструктури.

Третій розділ присвячений розрахунку та проєктуванню мережі. В цьому розділі розроблено три види моделі мережі для Кам'янець-Подільської міської лікарні Кам'янець-Подільської міської ради, а саме: схематична, логічна і віртуальна. Середовищем проєктування було обрано дві програми: «Microsoft Visio 2016» та «Cisco Packet Tracer». За побудованими схемами орієнтуватись при впровадженні, модернізації, обслуговуванні мережі стає

набагато зручніше і легше, також це пришвидшує адаптацію нових мережевих працівників.

Основна мета проєктування полягала у переобладнанні наявної мережі, яка на даний момент в багатьох місцях є аварійною, виконана недбало і порушує загальні правила безпеки для мережі, що є неприпустимим для об’єкту такого рівня.

У результаті розробки комп’ютерної мережі підприємства «Кам'янець-Подільська міська лікарня Кам'янець-Подільської міської ради» було спроєктовано ефективну мережу, яка забезпечить більш високу якість надання послуг клієнтам та покращить робочі умови працівникам структури.

У четвертому розділі проведено тестування мережі в віртуальному режимі за допомогою віртуальної моделі мережі. На прикладі тестування віртуальної моделі було надано приклади налаштування мережевого обладнання та кінцевого, користувацького, обладнання. Також було розглянуто можливості майбутньої модернізації мережі, якщо це стане необхідним для об’єкта.

Використання засобів тестування і діагностування комп’ютерних мереж дозволяє своєчасно виявити помилки в роботі мережі, що дозволить значно підвищити ефективність роботи комп’ютерних мереж, а також збільшити експлуатаційний термін їх служби.

Крім основних завдань, пов’язаних із обміном, зберіганням та обробкою інформації, комп’ютерна мережа повинна задовольняти вимогам, щодо заощадження ресурсів на її обслуговування та експлуатацію. Для цього потрібно визначитися, які прилади в майбутній мережі найбільш ресурсоємні, спробувати мінімізувати їх кількість та продумати кабельну інфраструктуру так, аби навантажувати її щонайменше.

В мережу можуть інтегруватися також інші системи. Зокрема, IP-телефонія, відеоконференц-зв’язок, підсистеми бухгалтерського обліку й тайм-менеджменту, також системи безпеки та інше.

В електронній системі охорони здоров’я пріоритетним має бути захист даних. Для цього використовують наступні засоби: використання користувачами кваліфікованих електронних підписів (КЕП), реалізація архітектурних принципів GDPR (відокремлене зберігання медичних та персональних даних), blockchain-подібні алгоритми, що забезпечують цілісність даних та інші. Так, лише на вході в систему користувачі проходять двофакторну авторизацію. Серед основних заходів для захисту інформації на кожному робочому місці необхідно регулярно оновлювати програмне забезпечення; забезпечувати мережевий захист: фільтрацію та аналіз мережевого трафіку, виявлення і протидію мережевим атакам і т. д.; проводити резервування конфігураційних файлів та критично важливих системних файлів; забезпечувати антивірусний захист, перевірку на наявність шкідливого програмного коду всіх вкладень, що завантажуються користувачами тощо.

Отже, правильно спроєктована комп’ютерна мережа повинна відповідати таким основними вимогам: зниження витрат на інтернет та зв’язок, оптимізація трафіку, безпека мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Андросов А.І. Сучасні мережеві технології: навчально-методичний посібник для студентів провізорів очної, заочної та дистанційної форм навчання / Андросов А.І., Іванькова Н.А. Запоріжжя : ЗДМУ, 2016. 76 с.

2. Буров Є. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. Львів : «Магнолія 2006», 2010. 262 с.

3. Від чого залежить швидкість у локальній мережі. URL : https://foxminded.ua/shvydkist-u-lokalnii-merezhi/

4. Волошко С.В. Інформаційна безпека в безпроводових сенсорних мережах / С.В. Волошко, Д.О. Курца // Новітні інформаційні системи і технології. 2018. Випуск 9. URL : http://journals.pntu.edu.ua/mist/article/view/1039/869.

5. Воробієнко П. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П,П, Воробієнко, Л.А. Нікітюк, П.І. Резніченко. К. : САММІТ-Книга, 2010. 708 с. : іл. URL : https://studfile.net/preview/5207067/

6. Гаркуша І. М. Конспект лекцій з дисципліни «Комп'ютерні мережі» для студентів галузі знань 12 «Інформаційні технології» спеціальності 126 «Інформаційні системи та технології». Д. : НТУ «ДП», 2019. 75 с. URL : https://it.nmu.org.ua/ua/scientific_method_materials/lecture_notes/ Конспект_лекцій_КомпютерніМережі_2019.pdf

7. Горбатий І. В., Бондарєв А. П. Характеристики телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи / Горбатий І. В., Бондарєв А. П. Л : Видавництво Львівської політехніки, 2016. 336 с.

8. Комп'ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем» та

«Інформаційне забезпечення робототехнічних систем»/ Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.

9. Журавська І. М. Проектування та монтаж локальних комп'ютерних мереж. Навчальний посібник. / І. М. Журавська. Миколаїв : Видавництво ЧДУ ім. Петра Могили, 2016. 396 с.

10. Карпенко М. Ю. Конспект лекцій з курсу «Комп'ютерні мережі» (для студентів усіх форм навчання спеціальностей 122 – Комп'ютерні науки, 151 – Автоматизація та комп'ютерно-інтегровані технології, 126 – Інформаційні системи та технології) / М. Ю. Карпенко, Н. В. Макого н; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2019. 99 с.

11. Комплексні системи захисту інформації [Текст] : навч. посіб. / Яремчук Ю. Є. Павловський П. В., Катаєв В. С., Сінюгін В. В. ; Вінницький національний технічний університет. Вінниця : ВНТУ, 2018. 118 с

12. Комп'ютерні мережі: [Книга 1. Технології комп'ютерних мереж]: навчальний посібник / Євсеєв С.П., Дженюк Н.В., Толкачов М.Ю та ін. – Харків, Львів: Видавництво ПП «Новий Світ – 2000», 2024. 471 с.

13. Методичні вказівки з написання та оформлення магістерських робіт студентами спеціальності 122 комп'ютерні науки / уклад. В.А. Іванюк та ін. Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. 11 с.

14. Микитишин А.Г. Телекомунікаційні системи та мережі : навчальний посібник для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» / укл. : А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.

15. Модель TCP/IP та адресація в мережах. URL : https://uk.wikipedia.org/wiki/TCP/IP

16. Налаштування активного мережевого обладнання. URL : https://ittel.com.ua/nalashtuvannya-aktivnogo-merezhevogo-obladnannya/

17. Користування мережею інтернет. URL : https://moz.gov.ua/uk/ koristuvannya-merezheyu-internet

18. Захищені вузли доступу до мережі Інтернет. URL : https://cip.gov.ua/ua/news/zakhisheni-vuzli-dostupu-do-merezhi-internet.

19. Сучасний стан розвитку телездоров'я та телемедицини в світі. URL : https://moz.gov.ua/uk/suchasnij-stan-rozvitku-telezdorov-ya-ta-telemedicini-v-sviti.

20. Сергієнко О. М. Комп'ютерні мережі та захист даних. URL : https://kppk.com.ua/ELLIB/ebook/Segrienko/KM/ page6.html

21. Тарбаєв С. І., Домрачева К.О., Заїка В. Ф., Трембовецький М. П. Проектування інфокомунікаційних мереж. Навчальний посібник. Підготовлений для самостійної роботи студентів вищих навчальних закладів з кредитно-модульною організацією навчального процесу. Київ: НТІТІ ДУТ, 2019. 186 с.

22. Ширина каналу та пропускна спроможність. Підрахунок часу передачі даних. / Лекція 8. Комп'ютерні мережі. Тернопольский національний техничний університет ім. І. Пулюя. URL : https://studfile.net/preview/ 7825935/page:8

23. Як оцінити пропускну здатність TCP між серверами. URL : https://introserv.com/ua/blog/yak-ocziniti-propusknu-zdatnist-tcp-mizh-serverami

24. Таненбаум Е., Фімстер Н., Уезеролл Д. Комп'ютерні мережі. 6-е вид. [Електронний ресурс]. URL : http://flibusta.site/b/751435/read

25. Фрідріхсон Н. В. ІТ технології в медицині. [Електронний ресурс]. URL : https://naukam.triada.in.ua/index.php/konferentsiji/42-dvanadtsyata vseukrajinska-praktichno-piznavalna-internet-konferentsiya/462-it-tekhnologiji-v-meditsini

26. Яка максимальна швидкість локальної мережі? URL : https://howevision.com/uk/what-is-the-maximum-speed-of-lan

27. General vs Trunk Mode. URL : https://community.cisco.com/t5/switches-small-business/general-vs-trunk-mode/td-p/2281870

28. How to Configure DHCP Server For Multiple VLANS in Packet Tracer. URL : https://netizzan.com/how-to-configure-dhcp-server-for-multiple-vlans-in-packet-tracer/#google_vignette

29. Configuring DHCP for multiple VLANs and DHCP Routing. URL : https://www.youtube.com/watch?v=EVqnrKh4Mlw

30. How to Configure DHCP for Multiple VLAN in CISCO Packet tracer? | CCNA | DHCP URL : https://www.youtube.com/watch?v=Z9aU33gu87A&t=834s

31. How to Configure DHCP in CISCO router in Packet Tracer | DHCP Server in CCNA | DHCP Configuration. URL : https://www.youtube.com/watch?v=DsL_JEdMPXg