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

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Потік Дениса Дмитровича
(ПІБ)

академічної групи 123-21ск-1
(шифр)

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

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

на тему «Комп'ютерна система комунального закладу "Дніпропетровський геріатричний пансіонат" з детальним опрацюванням налаштування безпечного віддаленого доступу до мережних пристроїв через термінальний сервер»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Ткаченко С.М.			
спеціальної частини	доц. Ткаченко С.М.			
розділів:				
розробка апаратної частини	доц. Бешта Д.А.			
розробка корпоративної мережі	ас. Панферова Я.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
« » _____ 2024 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Потік Д.Д. **академічної групи** 123-21ск-1
(прізвище та ініціали) (шифр)

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

на тему «Комп'ютерна система комунального закладу "Дніпропетровський геріатричний пансіонат" з детальним опрацюванням налаштування безпечного віддаленого доступу до мережних пристроїв через термінальний сервер»
затверджену наказом ректора НТУ «Дніпровська політехніка» від 29.04.2024 № 375-с

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел розглянути призначення та завдання термінального сервера в комп'ютерній системі геріатричного пансіонату.	05.05.2024
Розробка апаратної частини	Розробити вимоги до функцій, виконуваними системою, розробити структурну схему та специфікацію обладнання.	12.05.2024
Розробка корпоративної мереж	Побудувати в Packet Tracer модель корпоративної мережі пансіонату, виконати налаштування та перевірку роботи системи.	26.05.2024
Розробка компонента системи	Реалізувати та налаштувати безпечний віддалений доступ до мережних пристроїв через термінальний сервер.	09.06.2024

Завдання видано _____ доц. Ткаченко С.М.
(підпис керівника) (прізвище, ініціали)

Дата видачі 06.02.2024

Дата подання до екзаменаційної комісії 14.06.2024

Прийнято до виконання _____ Потік Д.Д,
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 79 с., 37 рис., 5 табл., 2 додатки, 12 джерел.

CISCO, CONSOLE, LAN, PACKET TRACER, SSH, TERMINAL SERVER, VLAN. КОМУТАТОР

Об’єкт розробки – комп’ютерна система "Дніпропетровський геріатричний пансіонат" з реалізацією побудови та налаштування корпоративної мережі.

Мета роботи – побудова комп'ютерної системи комунального закладу "Дніпропетровський геріатричний пансіонат" з детальним опрацюванням налаштування безпечного віддаленого доступу до мережних пристроїв через термінальний сервер.

Ця робота присвячена детальному вивченню та налаштуванню комп'ютерної системи комунального закладу "Дніпропетровський геріатричний пансіонат" з фокусом на створенні безпечного віддаленого доступу до мережних пристроїв через термінальний сервер.

Побудована модель мережі пансіонату в середовищі Packet Tracer. Мережа включає в себе маршрутизатори, комутатори, клієнтські пристрої та термінальний сервер. Ця модель відображає типову корпоративну мережу з необхідними зонами безпеки та сегментами мережі.

Виконано налаштування термінального сервера для забезпечення безпеки та ефективності віддаленого доступу до маршрутизаторів та комутаторів. Це включає в себе налаштування аутентифікації, шифрування з'єднань, управління доступом та інші заходи безпеки. Після налаштування термінального сервера проведено перевірка його роботи, щоб переконатися в його коректній роботі та відповідності вимогам безпеки. Це включає в себе перевірку з'єднання, аутентифікації, авторизації та шифрування даних.

Виконання цих завдань дозволило створити безпечне та ефективне середовище для віддаленого керування мережними пристроями в мережі закладу через термінальний сервер.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

ІТ	– інформаційні технології
КЗ ДГП	– комунальний заклад "Дніпропетровський геріатричний пансіонат"
КМ	– комп’ютерна мережа
КС	– комп’ютерна система
ПК	– персональний комп’ютер
DNS	– Domain Name System;
HTTP	– Hypertext Transfer Protocol
LAN	– Local Area Network
NAT	– Network Address Translation
OSPF	– Open Shortest Path First
SSH	– Secure Shell
TS	– Terminal Server
VLAN	– Virtual Local Area Network
WAN	– Wide Area Network

ВСТУП

У сучасному світі інформаційних технологій (ІТ), використання комп'ютерних систем у сфері охорони здоров'я стає не лише потребою, але й вимогою ефективного та безпечного функціонування закладів. Комунальні заклади, зокрема геріатричні пансіонати, не виключені із цього процесу, оскільки забезпечення якісної медичної та соціальної допомоги потребує оптимізації процесів управління та обміну даними.

Важливим аспектом роботи геріатричного пансіонату є забезпечення високої якості медичної допомоги та догляду за клієнтами. Для досягнення цієї мети, комп'ютерні системи відіграють ключову роль. Вони дозволяють збирати, зберігати та організовувати медичну інформацію, забезпечують контроль доступу до даних, спрощують процеси адміністрування та планування ресурсів, а також забезпечують можливість віддаленої консультації з лікарем. Таким чином, комп'ютерні системи відіграють важливу роль у забезпеченні ефективної роботи геріатричного пансіонату та покращенні якості медичної допомоги.

Одним із ключових напрямків удосконалення функціонування комп'ютерних систем є забезпечення надійного та безпечного віддаленого доступу до мережних пристроїв.

Налаштування безпечного віддаленого доступу до мережного обладнання через термінальний сервер стає важливою складовою для забезпечення конфіденційності, цілісності та доступності мережевих ресурсів. Ця техніка дозволяє інженерам та адміністраторам мережі віддалено керувати обладнанням, забезпечуючи при цьому захищений канал зв'язку та контроль доступу до системи.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп’ютерної системи, що проектується.

Галузь геріатрії, або лікування проблем старіння, є однією з найважливіших галузей в медицині, оскільки населення світу старіє, і з цим пов'язані різноманітні медичні та соціальні виклики. Геріатричні пансіонати - це спеціалізовані медичні заклади, які надають комплексну медичну, психологічну та соціальну допомогу літнім людям, забезпечуючи їм підтримку та догляд у їхній повсякденній діяльності [2].

Умови застосування комп'ютерної системи в геріатричних пансіонатах включають в себе:

а) Управління медичними даними. Комп'ютерні системи дозволяють збирати, зберігати та організовувати інформацію про пацієнтів, їхні медичні записи, лікування та рецепти. Це дозволяє медичному персоналу швидко отримувати доступ до необхідної інформації та забезпечувати координацію медичної допомоги.

б) Системи контролю доступу. Забезпечення безпеки даних та конфіденційності медичної інформації через належний контроль доступу до комп'ютерних систем.

в) Телемедицина. Можливість використання відеоконференцій та інших технологій для віддаленої консультації з лікарем, що дозволяє зменшити потребу у відвідуванні лікарні та забезпечує швидкий доступ до медичної допомоги.

г) Управління ресурсами. Комп'ютерні системи дозволяють ефективно керувати ресурсами пансіонату, включаючи запаси медикаментів, облік пацієнтів та планування персоналу.

д) Навчання та підтримка персоналу. Використання комп'ютерних систем для навчання та підтримки медичного персоналу, що дозволяє підтримувати високий рівень професійної компетентності та покращувати якість надання медичної допомоги.

Сучасне суспільство стрімко крокує до цифровізації всіх сфер життя, і медична галузь не є виключенням. Запровадження технологій віддаленого доступу до мережних пристроїв у медичних закладах набуває особливої актуальності в умовах сьогодення.

Віддалений доступ до мережного обладнання уможливлює здійснення технічної підтримки та налаштувань без безпосереднього втручання в роботу медичного закладу, що є запорукою збереження здоров'я як пацієнтів, так і обслуговуючого персоналу.

Таким чином, впровадження технологій віддаленого доступу до мережних пристроїв медичного закладу є актуальним та затребуваним кроком у напрямі цифровізації галузі охорони здоров'я та забезпечення безперебійної роботи критично важливої інфраструктури.

1.2 Характеристика і структура компанії

Геріатричні пансіонати, такі як "Дніпропетровський", відіграють ключову роль у наданні догляду та підтримки літнім людям, забезпечуючи їм якісну медичну допомогу та соціальну інтеграцію. У зв'язку з цим, розгляд характеристики і структури компанії "Геріатричний пансіонат "Дніпропетровський"" дозволяє краще зрозуміти контекст, в якому впроваджується комп'ютерна система та її важливість для оптимізації роботи закладу.

Передусім, "Геріатричний пансіонат "Дніпропетровський"" є комунальним закладом, який спеціалізується на наданні послуг стаціонарного догляду та лікування літніх людей. Метою пансіонату є забезпечення літніх людей комфортним та безпечним проживанням, а також надання їм комплексної медичної та соціальної допомоги. У зв'язку зі специфікою клієнтської аудиторії, геріатричний пансіонат має велику команду медичного та адміністративного персоналу, яка забезпечує повний спектр послуг та догляду.

Структура компанії включає адміністративний відділ, медичний відділ, відділ соціальної роботи та технічний відділ (рис.1.1).

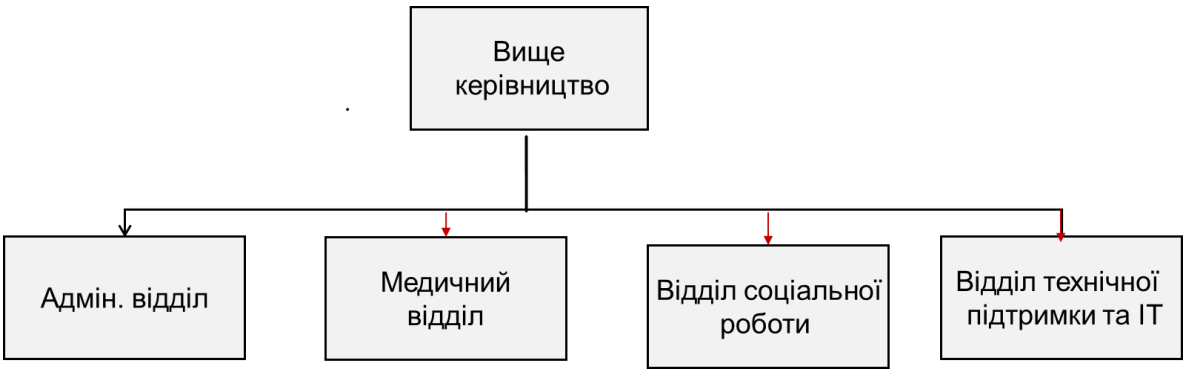


Рисунок 1.1 – Схема організаційної структури пансіонату

Адміністративний відділ відповідає за управління пансіонатом та забезпечення ефективної діяльності, включаючи фінансові, кадрові та логістичні аспекти.

Медичний відділ забезпечує медичну допомогу пацієнтам, включаючи лікарів, медичних сестер та психологічну службу.

Відділ соціальної роботи займається соціальною інтеграцією та психосоціальною підтримкою клієнтів.

Технічний відділ відповідає за технічне забезпечення пансіонату, включаючи IT-інфраструктуру та технічне обслуговування (рис.1.1).

Кожна служба виконує свої функції, забезпечуючи комплексний підхід до догляду за людьми похилого віку, включаючи медичну допомогу, соціальну підтримку, організацію дозвілля та підтримання комфортних умов проживання.

1.3 Стислі відомості про топологічне розміщення структурних підрозділів компанії

Топографічне розміщення структурних підрозділів скається з однієї 3-типоверхової будівлі. Знаходиться заклад за адресою: м. Дніпро, вул. Гаванська, 15) [3]. Топографічна схема розміщення структурних підрозділів показана на рис. 1.2.

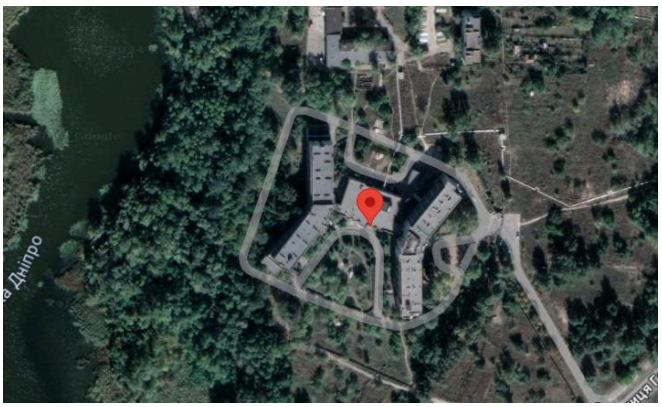


Рисунок 1.2 – Топографічна схема розміщення структурних підрозділів

Пансіонат – триповерховий будинок в якому розташовується персонал та клієнти. В серверній на 1 поверсі розміщено мережне обладнання, яке забезпечує вихід в Інтернет та підключення ПК користувачів адміністративного відділу, медичного + відділ соціальної роботи, сервер та клієнтів та медичного обладнання в локальну мережу закладу.

На першому поверсі розташовується медперсонал з кабінетами для надання медичних послуг пенсіонерам. На поверсі налічується 20 хостів. Вони розміщені в умовній локації, яка має 9 приміщень, одне з яких це серверна кімната.

Вигляд першого поверху можна побачити на рисунку 1.3.

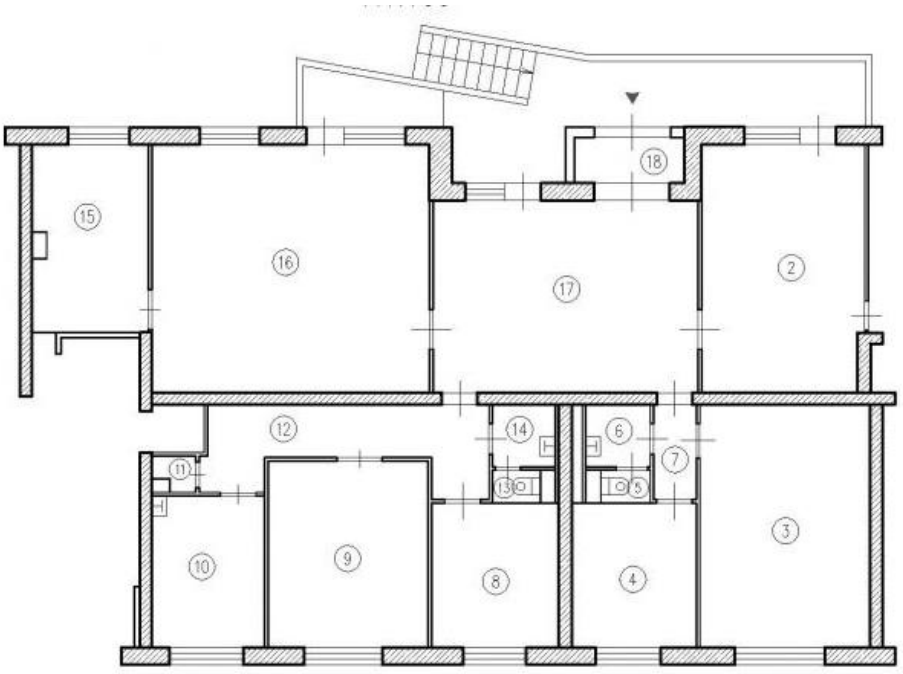


Рисунок 1.3 – Схема першого поверху КЗ ДГП

На другому та 3 поверхах знаходяться кімнати, де проживають люди похилого віку. На рисунку 4.3 представлено план другого поверху. Аналогічно виглядає третій поверх.

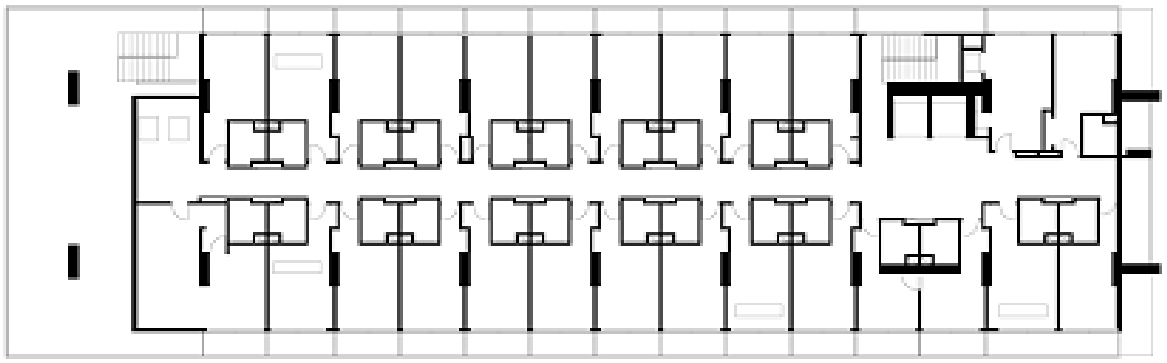


Рисунок 1.4 – План другого поверху

Оскільки комп'ютерна мережа охоплює невелику територію, розташовану в одній будівлі, вона є локальною.

У всіх кабінетах, де здійснюється прийом підопічних, встановлено щонайменше по одному ПК, який використовується для автоматизації роботи пансіоната.

В кожній кімнаті є мінімум 1 настінна розетка RJ45 для фізичного закінчення (термінування) кабелю. Загалом в будівлі на кожному поверсі є по 30 розеток RJ-45.

Ступінь комп'ютеризації робочих місць КЗ ДГП приведена в табл.1.1.

Таблиця 1.1 – Комп'ютеризовані робочі місця підприємства

Структурний підрозділ	Кількість		
	Працівники	ПК	Принтери
Керівництво	2	2	1
Адміністративний відділ	3	3	1
Фінансовий відділ	4	3	1
Відділ соціальної роботи	4	4	1
Медичний відділ	30	20	6
Відділ технічної підтримки + сервер	2	2	1
Робочі місця для клієнтів	90	90	
Загалом ПК		108	11

Комп'ютери з'єднані між собою мідними провідниками (кручена пара) – це вид кабелю зв'язку, що являє собою одну або кілька пар ізольованих провідників, скручених між собою (з невеликою кількістю витків на одиницю довжини) та покритих пластиковою оболонкою. Наразі, завдяки своїй дешевизні та легкості в монтажі, кручена пара є найпоширенішим рішенням для побудови дротових (кабельних) локальних мереж.

1.4 Особливості та проблеми функціонування комп'ютерної мережі геріатричного пансіонату

Комп'ютерна мережа геріатричного пансіонату є складовою частиною сучасної інфраструктури таких закладів. Вона забезпечує ефективну комунікацію між співробітниками, лікарями, пацієнтами та їхніми родичами, а також надає доступ до необхідної інформації та ресурсів. Однак, функціонування комп'ютерної мережі в геріатричному пансіонаті має свої особливості та проблеми, які потрібно враховувати при її створенні та експлуатації.

Однією з особливостей комп'ютерної мережі геріатричного пансіонату є необхідність забезпечення безпеки та конфіденційності даних про пацієнтів. Геріатричні пансіонати працюють з конфіденційною інформацією про здоров'я та особисте життя пацієнтів, тому мережа повинна бути захищена від несанкціонованого доступу та кібератак. Крім того, мережа повинна бути спроектована з урахуванням специфічних потреб геріатричних пансіонатів, таких як забезпечення доступу до медичної інформації, комунікації між лікарями та пацієнтами, а також забезпечення комфортного проживання пацієнтів.

Іншою проблемою є забезпечення доступу до мережі для пацієнтів з обмеженими можливостями. Геріатричні пансіонати повинні забезпечити доступ до мережі для пацієнтів з обмеженими можливостями, таких як інваліди або люди з порушеннями зору. Це може потребувати спеціальних рішень, таких як адаптивні інтерфейси або спеціальні пристрої для доступу до мережі.

Однак, функціонування комп'ютерної мережі геріатричного пансіонату також пов'язане з рядом проблем. Одна з них – це обмежені ресурси, такі як

фінансування та кваліфіковані кадри. Геріатричні пансіонати, як правило, не мають великих бюджетів на розвиток інфраструктури, тому вони можуть не мати можливості інвестувати в сучасні технології та кваліфіковані кадри. Крім того, геріатричні пансіонати можуть зіткнутися з проблемами старіння обладнання та програмного забезпечення, що може призвести до порушення роботи мережі. Тому застосування термінального сервера вирішить задачу централізованого моніторингу та керування обладнанням, що дозволяє IT-персоналу пансіонату швидко виявляти та вирішувати технічні проблеми. Це дозволяє адміністраторам мережі легко керувати доступом до ресурсів, налаштовувати політику безпеки та відслідковувати діяльність користувачів.

Віддалений доступ до мережного обладнання уможливлює здійснення технічної підтримки та налаштувань без безпосереднього втручання в роботу медичного закладу, що є запорукою збереження здоров'я як пацієнтів, так і обслуговуючого персоналу.

Таким чином, впровадження технологій віддаленого доступу до мережних пристроїв медичного закладу КЗ ДГП є важливим елементом інфраструктури геріатричного пансіонату, що дозволяє забезпечити комфортне та безпечне проживання пенсіонерів.

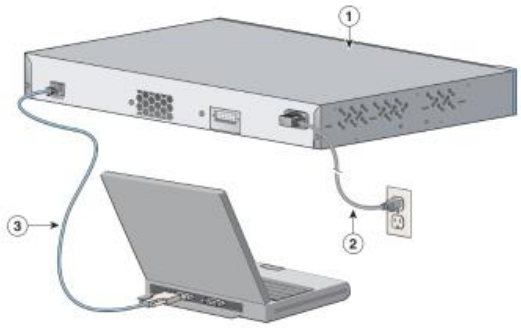
1.5 Визначення можливих напрямків рішення поставлених завдань

Отримання доступу до маршрутизаторів і комутаторів є дуже важливим для адміністраторів мережі, оскільки це дозволяє їм налаштовувати, моніторити і керувати мережевими пристроями. Отримання доступу до маршрутизаторів і комутаторів через мережу дозволяє адміністраторам віддалено керувати мережею, що особливо корисно для великих або розподілених мереж, забезпечуючи їх надійність, безпеку і ефективність роботи.

Розглянемо найпопулярніші методи доступу: пряме консольне підключення, віддалене по SSH та через термінальний сервер.

1.5.1 Пряме консольне підключення

Консольне підключення (Console Connection) – це пряме підключення послідовного порту комп'ютера до консольного порту комутатора за допомогою спеціального консольного кабелю (див. рисунок 1.5) [5].



1 – Комутатор Cisco 2960; 2 – кабель живлення; 3 – консольний кабель

Рисунок 1.5 – Консольне підключення

Це підключення також позначається як Console Out-of-Band Connection. Консольне підключення є основним типом підключення для початкового налагодження комутатора.

Консольне підключення реалізовується з використанням або послідовних інтерфейсів RS-232 (EIA/TIA-232), або інтерфейсу USB.

Консольне підключення виконується наступним чином:

– для прямого консольного підключення використовується консольний кабель, який зазвичай має спеціальний роз'єм (наприклад, RJ45 або DB9) на одному кінці для підключення до консольного порту пристрою і стандартний RS-232 або USB роз'єм на іншому кінці для підключення до комп'ютера або термінала;

– після підключення консольного кабелю до пристрою і комп'ютера встановлюється термінальна програма (наприклад, PuTTY на Windows або Terminal на macOS або Linux), яка використовується для взаємодії з пристроєм через консольний порт;

– після запуску термінальної програми користувач повинен вибрати правильний комунікаційний порт і встановити налаштування зв'язку, такі як швидкість передачі даних та парітет;

– після успішного підключення до пристрою користувач може ввести

інструкції та команди для управління маршрутизатором або комутатором через консольний інтерфейс.

Пряме консольне підключення найчастіше використовується для управління та налагодження мережного обладнання, особливо у випадках, коли немає можливості здійснити доступ через мережу або вона недоступна.

Цей метод також може бути використаний для відновлення маршрутизатора або комутатора у випадку, якщо налаштування мережі заблоковано або виникли проблеми з мережевим з'єднанням, або забутий пароль.

Пряме консольне підключення є надійним та ефективним методом отримання доступу до мережного обладнання і забезпечує можливість управління пристроями, навіть якщо немає доступу до мережі. Але воно потребує фізичного доступу до пристрою та обмежено у віддаленому керуванні.

1.5.2 Підключення по локальній мережі через SSH

SSH (Secure Shell) – це захищений мережевий протокол, що дає змогу здійснювати віддалене під'єднання до сервера з використанням імені користувача та пароля. Тому це підключення вимагає наявність чинного SSH-сервера, правильного налаштування і конфігурації доступу по SSH, та налаштування облікових записів користувачів із відповідними правами.

Підключення по SSH виконується наступним чином (рис. 1.6) [4]:

– для підключення до маршрутизатора або комутатора по локальній мережі через SSH, спочатку потрібно встановити SSH-сервер на пристрої;

– потім, використовуючи SSH-клієнт (наприклад, PuTTY на Windows або Terminal на macOS або Linux), користувач може підключитися до маршрутизатора або комутатора, використовуючи його IP-адресу або доменне ім'я та правильні облікові дані;

– після встановлення з'єднання за допомогою SSH користувач може ввести свій пароль або використовувати інші методи аутентифікації, які були налаштовані на пристрої.

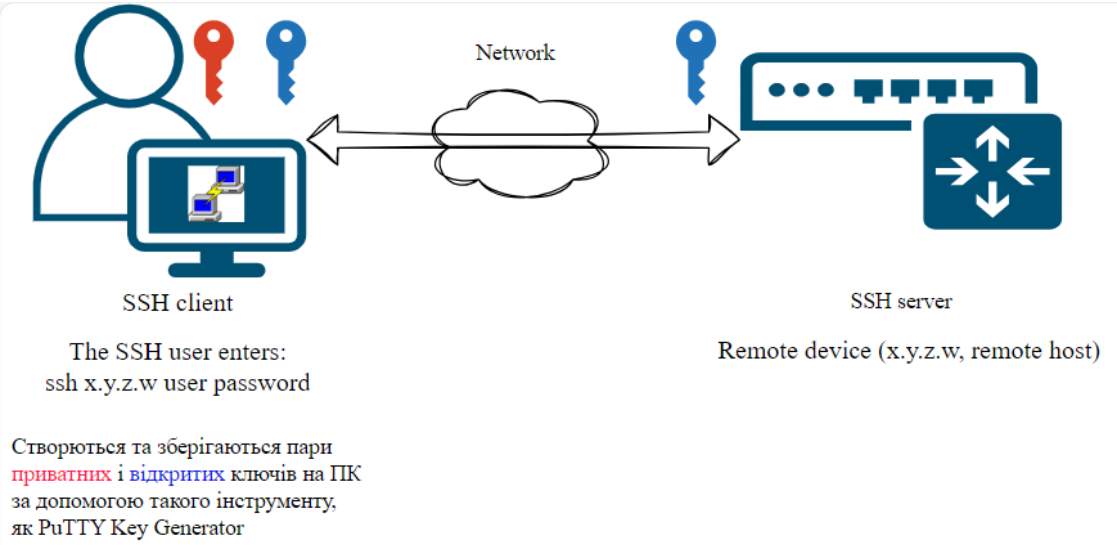


Рисунок 1.6 – SSH з’єднання

Підключення через SSH є безпечним методом, оскільки всі дані, що передаються між клієнтом і сервером, шифруються.

Цей метод часто використовується для віддаленого управління та налагодження маршрутизаторів і комутаторів, особливо у великих мереж, де доступ до пристроїв по локальній консолі не завжди зручний.

SSH також може використовуватися для автоматизації задач адміністрування та віддаленого моніторингу мережевого обладнання за допомогою скриптів та програмного забезпечення керування мережею.

Підключення по локальній мережі через SSH є потужним та безпечним методом отримання доступу до мережного обладнання і використовується адміністраторами мереж для управління та налагодження пристроїв. Але вимагає налаштування SSH на пристрої та можливі атаки на SSH, якщо не налаштовано належні заходи безпеки.

1.5.3 Підключення через термінальний сервер

Підключення через термінальний сервер – це метод, за якого адміністратор може отримати доступ до маршрутизаторів і комутаторів шляхом підключення до термінального сервера, а потім віддаленого управління цими пристроями через термінальне з'єднання.

Термінальний сервер – це пристрій, який служить посередником між

адміністратором і віддаленими мережевими пристроями. Він може мати багато портів для підключення до різних пристроїв.

Підключення через термінальний сервер виконується наступним чином (рис. 1.7) [5]:

– адміністратор підключається до термінального сервера через мережу, використовуючи протоколи, такі як SSH або Telnet;

– після успішного підключення до термінального сервера адміністратор може використовувати термінальне з'єднання для віддаленого управління маршрутизаторами і комутаторами, підключеними до термінального сервера. Це може включати введення команд для конфігурації, моніторинг або діагностику пристроїв.

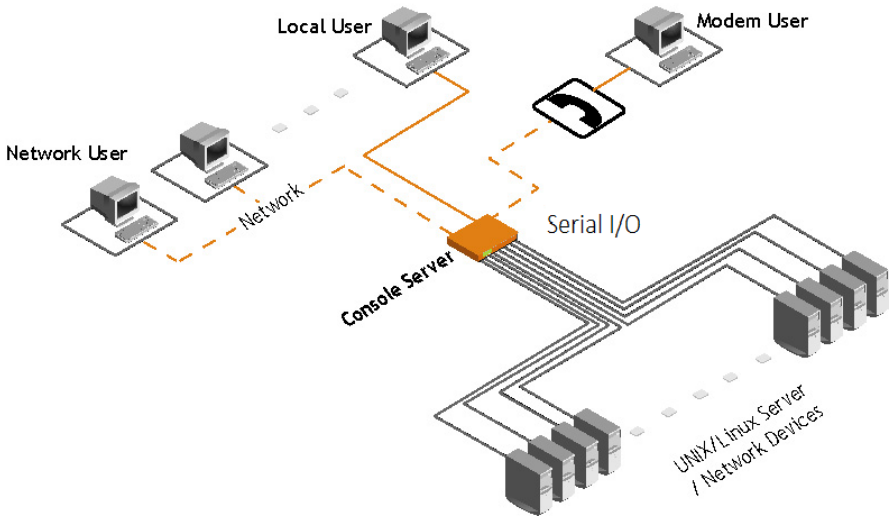


Рисунок 1.7 – Підключення через термінальний сервер

Термінальні сервери можуть мати різні можливості конфігурації, такі як управління портами, автоматичне підключення до пристроїв при їх перезавантаженні, аутентифікація користувачів тощо.

Підключення через термінальний сервер дозволяє керувати декількома пристроями через одне з'єднання, забезпечуючи централізований доступ до пристроїв у великих мережах, але вимагає додаткового обладнання.

1.6 Обґрунтування вибраного напрямку інженерного рішення

Кожен метод отримання доступу до маршрутизаторів і комутаторів має свої

власні варіанти використання залежно від потреб адміністратора мережі. Найчастіше адміністратори використовують комбінацію цих методів для забезпечення надійного та безпечного доступу до мережевих пристроїв.

Для виконання практичної частини проекту було вирішено використовувати термінальний сервер з доступом по SSH. Виконавши це завдання, ми зможемо маневрувати від сервера терміналів до кожного окремого мережного пристрою, а потім назад до сервера терміналів.

Для моделювання мережі пансіонату було вирішено обрати топологію на рис.1.8. Для цього проекту потрібно створити п’ять локальних мереж. Мережа LAN1 є мережею "Дніпропетровського геріатричного пансіонату", інші 4 мережі представляють можливі пансіонати в інших містах та додані для виконання учбового завдання з реалізації маршрутизації між підмережами. Кожна з підмереж повинна мати можливість доступу до Інтернет.

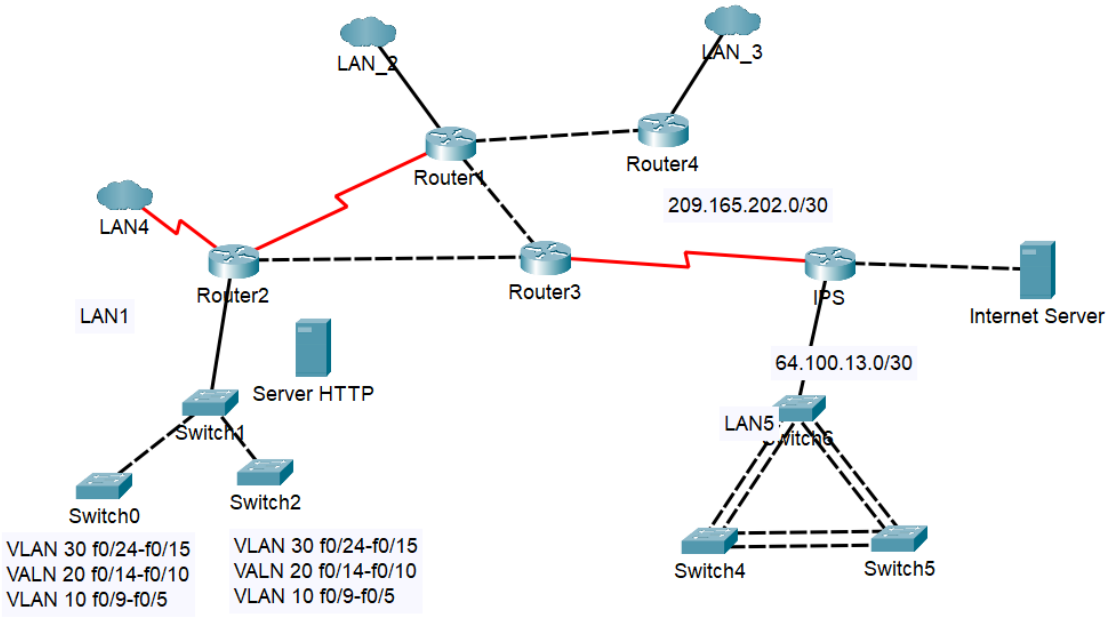


Рисунок 1.8 – Загальна топологія мереж геріатричних пансіонатів

Підмережа геріатричного пансіонату буде розділена на підмережі відповідного до організаційної структури, не змінюючи фізичного топології та не існуючому обладнання з застосуванням VLAN на комутаторах. Виходячи із структури пансіонату таких підмереж буде 4 і додатково ще для керування пристроями. Використання технології VLAN (Virtual Local Area Network) є

поширеною практикою у сучасних комп'ютерних мережах. VLAN є логічною сегментацією фізичної мережі, що дозволяє створювати незалежні групи пристроїв, які можуть взаємодіяти одна з одною, начебто вони знаходилися в одній фізичній мережі.

Також, VLAN-технологія забезпечує більш ефективне використання ресурсів мережі, оскільки дозволяє розподіляти доступ до ресурсів мережі відповідно до потреб окремих груп користувачів.

В цілому, використання технології VLAN є необхідною умовою для створення надійної та ефективної локальної мережі, яка може відповідати постійно зростаючим вимогам організації.

1.7 Завдання і мета роботи

Метою роботи є побудова комп'ютерної системи комунального закладу "Дніпропетровський геріатричний пансіонат" з детальним опрацюванням налаштування безпечного віддаленого доступу до мережних пристроїв через термінальний сервер.

Основні етапи завдання наступні:

– аналіз потреб компанії та її інфраструктури;

– формулювання технічних вимог до мережі;

– вибір мережевої архітектури та обладнання;

– розробка специфікації апаратних засобів;

– конфігурування мережевого обладнання;

– методи отримання доступу до маршрутизаторів і комутаторів;

– огляд і вибір термінального сервера;

– налаштування серверу терміналів для надання доступу до мережного обладнання в Packet Tracer;

– тестування роботи термінального сервера;

– тестування мережі та її компонентів.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до комп'ютерної системи КЗ ДГП

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціоналу систем

2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики

Комп'ютерна система «Дніпропетровського геріатричного пансіонату» призначена для комунікації між співробітниками, лікарями, пацієнтами та їхніми родичами, а також надає доступ до необхідної інформації та ресурсів.

Структура комп'ютерної системи має складатись з наступних підмереж згідно організаційної структури:

– адміністративна область для реєстраційни й пункт, фінансовий відділ тощо, 6 вузлів;

– медична область для медичних працівників, лікарів, медсестер та іншого медичного персоналу, 20 вузлів;

– пацієнтська область для пацієнтів з доступом до Інтернету та розважальних ресурсів, 90 вузлів;

– серверна область для серверів та мережного обладнання, 4 вузли.

Для цього проекту потрібно створити п'ять локальних мереж, що представляють собою мережу пансіонату в м.Дніпро та в інших містах:

– LAN1 – це мережа КЗ ДГП, яка повинна забезпечувати об'єднання в локальну мережу ПК та медичне обладнання медичних робітників та обладнання закладу, то доступ клієнтів до мережі Інтернет:

– LAN2, LAN3, LAN4 та LAN5 – мережі пансіонатів в інших містах.

Підмережу геріатричного пансіонату потрібно розділити на підмережі відповідного до організаційної структури, не змінюючи фізичного топології та не існуючому обладнання з застосуванням VLAN на комутаторах. Виходячи із структури пансіонату таких підмереж буде 4 і додатково ще для керування пристроями.

Для відповідності вимогам потрібно використовувати приватний IP-блок-адрес 172.20.40.0/21 для призначення підмереж, враховуючи кількість вузлів.

Для забезпечення надійності та майбутнього розширення мережі, рекомендується мати приблизно 10% запасних портів на випадок відмови портів або для майбутнього розширення та вдосконалення мережі.

Налаштувати сервер терміналів для надання віддаленого захищеного доступу до мережного обладнання в мережі КЗ "Дніпропетровського геріатричного пансіонату".

2.1.1.1.2 Вимоги до способів та засобів зв'язку для інформаційного обміну між компонентами системи

В LAN1 мережі КЗ ДГП повинна використовуватися технологія логічного розділення фізичної мережі на окремі віртуальні мережі VLAN.

В LAN5 повинна використовуватися технологія EtherChannel, що дозволяє об'єднати декілька фізичних з'єднань між комутаторами в одне логічне. Це дозволяє підвищити пропускну здатність та надійність мережі.

В мережі повинен використовується протокол динамічної маршрутизації OSPF для виявлення та прокладання маршрутів між різними підмережами.

Мережа повинна бути підключена до Інтернету через постачальника послуг за допомогою технології NAT. Для внутрішньої мережі основної мережі та віддаленої повинна бути використана вита пара, а для об'єднання мереж – оптичне волокно.

Сервер терміналів повинен забезпечувати позасмуговий доступ через консольний порт інших маршрутизаторів або комутаторів.

2.1.1.1.3 Вимоги до режимів функціонування систем

Система повинна забезпечувати неперервний доступ до основних функцій навіть у випадку виникнення тимчасових збоїв або відмов обладнання.

В разі виникнення неполадок система повинна мати можливість швидко і відновлюватися до нормального режиму роботи без значного впливу на

продуктивність.

Система має бути гнучкою і здатною пристосовуватися до змін у вимогах і потребах користувачів без значного переривання роботи.

Режими функціонування системи повинні забезпечувати високий рівень захисту від несанкціонованого доступу.

Система повинна бути здатною масштабуватися для врахування зростаючих потреб користувачів і обсягів даних без втрати продуктивності.

2.1.1.1.4 Вимоги щодо діагностування системи

Персонал повинен мати здатність ручно виявляти можливі проблеми та помилки в роботі системи шляхом аналізу доступної інформації та спостереження за роботою.

Працівники повинні періодично проводити моніторинг стану компонентів, ресурсів та процесів в системі для вчасного виявлення проблем.

Персонал повинен мати доступ до відповідних інструментів для аналізу виниклих помилок та аномалій, щоб зрозуміти їх причини та вирішити їх.

Система повинна вести детальний журнал подій.

2.1.1.2 Вимоги до показників призначення

Комунікація. Система має забезпечувати спілкування між персоналом клініки шляхом використання миттєвих повідомлень, електронної пошти та відеоконференцій.

Обмін даними та доступ. Система повинна надавати лікарям можливість доступу до медичних даних пацієнтів, включаючи аналізи, медичні зображення та записи пацієнтів.

Централізоване зберігання даних. Система повинна мати можливість централізованого зберігання даних на серверах та можливість відновлення даних за допомогою резервного збереження в хмарі.

Безпека. Система повинна захищати дані від несанкціонованого доступу та вірусів, впроваджуючи різноманітні механізми безпеки.

Доступ до Інтернету. Система повинна надавати можливість доступу до мережі Інтернет.

Віддалене підключення. Система має забезпечувати можливість віддаленого підключення через використання термінального сервера.

2.1.1.3 Вимоги до експлуатації, технічного обслуговування, ремонту і зберігання компонентів системи

Для кожного компонента системи повинні бути розроблені докладні інструкції з експлуатації, які включають у себе правила використання, обмеження і рекомендації з їх використання.

Функціонування системи сплановане для неперервної роботи, з вимкненням відповідних сегментів для профілактичних робіт не частіше одного разу на рік.

У наявності повинно бути достатня кількість запасних частин для швидкого заміщення у випадку виникнення поломок або несправностей.

Копії програмного забезпечення та ліцензійні ключі в потрібно зберігати у безпечному місці, щоб забезпечити їх доступність у разі потреби.

Мають бути розроблені місця де компоненти системи в безпечних, сухих та чистих приміщеннях, щоб запобігти пошкодженню від вологи, пилу або інших зовнішніх факторів.

2.1.1.4 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему, і режиму його роботи.

Для забезпечення якісного обслуговування комп’ютерної системи, були сформовані такі вимоги до кваліфікації персоналу:

– керівник відділу технічної підтримки є магістром галузі "Комп’ютерна інженерія" з робочим досвідом від 2-3 років на даній посаді;

– адміністратори мережі є молодшими спеціалістами в галузі "Комп’ютерна інженерія", відповідають за налагодження та підтримку працездатності мережі, зокрема, ремонт та налаштування мережевого

обладнання;

– механіки обслуговування обладнання мають бакалаврську або молодшу спеціалістську освіту в галузі "Автоматизація та комп’ютерно-інтегровані технології" та відповідають за моніторинг стану обладнання у цехах та, в разі несправності, проводять ремонт або заміну.

Всі працівник повинні пройти медогляд та первинний інструктаж. Періодичний інструктаж з техніки безпеки - не рідше 1 разу на рік. Періодичний медогляд - не рідше 2 разів на рік.

2.1.1.5 Вимоги до надійності

Система повинна бути стійкою до відмов обладнання, програмних систем та електропостачання. Для забезпечення надійності комплексу необхідно використовувати високонадійні апаратні компоненти, які повинні відповідати наступним критеріям:

– напрацювання на відмову - не менше 20000 годин;

– вірогідність безвідмовної роботи на період 100 годин має становити не менше 99,5%.

У нормальному режимі роботи мережа повинна забезпечувати швидкий обмін інформацією між кінцевими пристроями зі швидкістю не менше 10 Мб/с.

Вимоги до надійності системи повинні бути визначені для таких аварійних ситуацій:

– вихід з ладу апаратних компонентів системи, наприклад, маршрутизаторів і комутаторів, на період до 6 годин;

– відсутність електропостачання на період до 6 годин.

Для забезпечення надійності роботи програмного забезпечення необхідно використовувати лише програмні продукти з відповідною ліцензією.

2.1.1.6 Вимоги до патентної чистоти

Обладнання та ПЗ, яке використовується в комп'ютерній системі, має забезпечувати вимоги до патентної чистоти на території України.

2.1.1.7 Додаткові вимоги

Налаштувати сервер терміналів для надання віддаленого захищеного доступу до мережного обладнання в LAN1 мережі "Дніпропетровського геріатричного пансіонату".

Структура термінального сервера має бути модульною, щоб забезпечувати стійкість і масштабованість. Вона повинна складатися з наступних компонентів: процесор, пам'ять, пристрій зберігання даних, мережевий інтерфейс та пристрій введення-виводу. Крім того, термінальний сервер повинен мати надійну систему безпеки, щоб запобігти несанкціонованому доступу до ресурсів мережі.

Функціонал термінального сервера повинен включати засоби автентифікації та авторизації користувачів, інструменти моніторингу та управління ресурсами, а також засоби забезпечення безпеки та резервного копіювання даних.

При налаштуванні сервера терміналів необхідно враховувати наступні вимоги:

– сервер має підтримувати протокол SSH для безпечного термінального обслуговування;

– граничний маршрутизатор в КЗ ДГП налаштувати як сервер терміналів;

– сервер терміналів підключається до консольного порту кожного пристрою;

– призначення портів за таким правилом: Р№ – 200№, де № – номер лінії.

2.1.2 Вимоги до задач (налаштувань), які виконує КС

Під час розробки адресації підмережі необхідно враховувати наступні вимоги:

– LAN1 – це мережа «Дніпропетровського геріатричного пансіонату, яка повинна забезпечувати 119 хостів та до неї входить HTTP сервер для надання вебсторінок;

– LAN2, LAN3, LAN4 та LAN5 – мережі пансіонатів в інших містах, які повинні забезпечувати 68, 179, 54 та 53 хостів відповідно.

Загалом підсистема повинна налічувати 354 IP-адреси для хостів.

Блок адрес для виділення підмереж повинен бути 172.20.40.0/21.

Для каналів між маршрутизаторами застосувати блок адрес 10.0.13.0/24.

Середня інтенсивність вихідного трафіку, середня довжина вихідного повідомлення та затримка передачі пакету в найбільшій мережі повинні відповідати заданим параметрам: μ =108 кадрів/с.

Для виконання базового налаштування конфігурації пристроїв потрібно враховувати наступні вимоги:

– назви пристроям за наступним правилом: Potik_тип пристрою_номер пристрою;

– на всіх пристроях повинен бути назначений пароль *cisco* до консолі і vty;

– на всіх пристроях повинен бути назначений пароль *class* до привілейованого режиму;

– усі паролі, що зберігаються у відкритому вигляді, потрібно зашифрувати;

– потрібно назначити на усіх лініях vty використання протоколу SSH;

– потрібно призначити ім’я користувача та пароль на всіх пристроях за правилом: група_прізвище з паролем *admincisco*;

– в якості імені домена потрібно використати ім'я пристрою;

– для шифрування даних потрібно створювати ключ RSA завдовжки 1024 біт;

– на DCE-інтерфейсах маршрутизаторів потрібно призначити встановлення значення тактової частоти – 128000;

– потрібно налаштувати аудит і відправку повідомлень про початок і завершення процесу exec, з використанням локальної бази;

– з метою збільшення пропускної здатності і надійності каналів в мережі LAN5 на комутаторах потрібно виконати агрегування каналів.

На маршрутизаторах потрібно використовувати протокол динамічної маршрутизації OSPF, що підтримує множинні шляхи, має малий час збіжності та реагування та створює мінімальний службовий трафік. Під час налаштування маршрутизаторів потрібно враховувати наступні вимоги:

– потрібно оголосити безпосередньо підключені мережі і відключити поширення оновлень маршрутизації на інтерфейси в локальні мережі;

– для VLAN мереж потрібно налаштувати сумарний маршрут і оголосити його іншим маршрутизаторам;

– потрібно налаштувати маршрут за умовчанням на маршрутизаторі з прямим підключенням до інтернет-провайдера (ISP) і розповсюдити його через оновлення маршрутизації.

При налаштуванні роботи Інтернет в Системі необхідно враховувати наступні вимоги:

– потрібно встановити одного провайдера послуг доступу до Інтернет (ISP);

– для виходу робочих станцій в Інтернет необхідно настроїти пограничний маршрутизатор з динамічним NAT за такими даними: ім’я пула: Internet, пул адресів: 209.165.200.5 по 209.165.200.30, номер списку доступу 12.

Під час налаштування мереж VLAN і маршрутизації між ними потрібно враховувати наступні вимоги:

– налаштувати транкові порти і порти доступу, а також вимкнути усі невикористовувані фізичні порти комутаторів;

– налаштувати SVI-інтерфейси на комутаторах, призначивши IPv4- адреси з мережі Management VLAN;

– налаштувати маршрутизацію між мережами VLAN. [5]

При налаштуванні адресації ПК в мережах VLAN необхідно враховувати наступні вимоги:

– налаштувати маршрутизатор, що здійснює маршрутизацію між VLAN, в якості сервера DHCP для мереж VLAN;

– створити пули DHCP під назвою pollvlan№, де № − номер VLAN;

– виключити з пулу перші 10 адрес і для кожного пулу вказати адресу DNS-сервера і шлюз за замовчуванням. [1]

2.1.3 Вимоги до видів забезпечення КС

2.1.3.1 Вимоги до технічного забезпечення

Для ефективної роботи кожне робоче місце повинно бути оснащене комп'ютером з такою конфігурацією:

– процесор з мінімум чотирма ядрами з тактовою частотою не нижче 2 Ггц;

– об'єм опертивної пам'яті не нижче 8 Гб;

– дискретний відеоадаптер;

– об'єм пам'яті не менше 256 Гб;

– операційна система Windows 10 або Windows 11.

Термінальний сервер повинен відповідати вимогам:

– процесор мінімум 1 ГГц;

– -мінімум 4 ГБ ОЗП (рекомендується 8 ГБ або більше);

– мінімум 250 ГБ жорстких дисків (рекомендується SSD);

– підтримка протоколів: SSH, FTP, HTTP

– підтримка протоколів шифрування, таких як SSH або SSL/TLS

– пропускна здатність: мінімум 100 Мбіт/с (рекомендується 1 Гбіт/с або більше)

Комутатор повинен відповідати вимогам:

– 24 порти FastEthernet та порт GigabitEthernet;

– підтримка Etherchannel, VLAN.

Маршрутизатор повинен відповідати вимогам:

– мінімум 2 порти GigabitEthernet, 4 EHWIC слоти;

– модуль HWSC-8A для забезпечення до восьми асинхронних підключень EIA-232 до консольних портів;

– підтримка DHCP, NAT, VPN та AAA протоколів.

2.1.3.2 Вимоги до організаційного забезпечення

Працівники IT-відділу повинні мати доступ до технічного приміщення за допомогою ключ-карток.

2.1.3.3 Вимоги до лінгвістичного забезпечення системи

Все лінгвістичне забезпечення системи для організації взаємодії з користувачем повинно використовувати в переважно українську мову або англійську мову.

Усі написи інтерфейсу керування повинні бути викладені українською або англійською мовами.

2.2 Розробка апаратної частини комп'ютерної системи

2.2.1 Опису апаратних засобів комп'ютерної системи

2.2.1.1 Мережне обладнання

Вибір апаратної частини корпоративної мережі є важливим кроком для забезпечення надійності та продуктивності системи.

В якості мережного обладнання було обрано маршрутизатор Cisco 2911, комутатор Cisco Catalyst 2960 та Wi-Fi роутер Linksys WRT-300N.

Модульний маршрутизатор Cisco 2911/K9 – це пристрій нового покоління, що відноситься до сімейства ISR G2. Модель дозволяє створювати безпечне широкосмугове підключення до мережі, проводити передачу мультимедійних даних, відео, здійснювати бездротовий зв'язок, а також застосовувати безліч додаткових функцій при мінімальному рівні витрат на придбання та утримання. На рис. 2.2 наведено зображення маршрутизатора Cisco 2911в Packet Tracer.

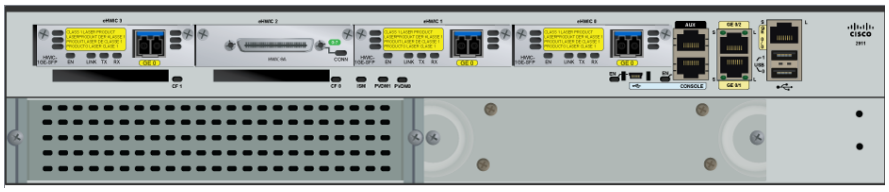


Рисунок 2.1 – Маршрутизатор Cisco 2911

Основні характеристики [5]:

– процесор: 1.8 GHz dual-core processor;

– оперативна пам'ять: 1 GB (макс. 4 GB);

– флеш-пам'ять: 256 MB (макс. 4 GB);

– інтерфейси:

– 2 x Gigabit Ethernet (RJ-45);

– 2 x WAN (RJ-45);

– 1 x AUX (RJ-45);

– 1 x Console (RJ-45);

– 1 x USB 2.0;

– підтримка протоколів: IPv4, IPv6, OSPF, EIGRP, BGP, RIP, HSRP, VRRP

– безпека: Firewall, VPN, ACL, IPS

Функціональні можливості:

– маршрутизація пакетів між мережами;

– підтримка до 1000 VPN-тунелів;

– підтримка до 1000 користувачів;

– підтримка Quality of Service (QoS);

– підтримка Voice over IP (VoIP);

– підтримка відеоконференцзв'язку;

– підтримка мережевих сервісів, таких як DNS, DHCP, NTP;

– підтримка моніторингу та управління мережею за допомогою SNMP, Syslog, NetFlow;

– підтримка безпекових функцій, таких як інтрusion prevention, URL-фільтрація, антивірусна перевірка.

Комутатори Cisco Catalyst 2960 серії (рис. 2.3) є лінійкою комутаторів з фіксованою конфігурацією і портами Fast Ethernet і Gigabit Ethernet, що мають розширені LAN сервіси для підприємств початкового рівня і мереж віддаленого офісу [6].

Рисунок 2.2 – Вигляд комутаторів Catalyst 2960

Основні характеристики:

– тип: Layer 2 Managed Switch (комутатор 2-го рівня з управлінням);

– кількість портів: 24 x 10/100BASE-T (RJ-45);

– 2 x 10/100BASE-T (RJ-45) SFP (Small Form-Factor Pluggable) ports for uplinks;

– максимальна пропускна здатність: 128 Gbps;

– пам'ять: 128 MB RAM, 32 MB Flash;

– оперативна система: Cisco IOS Software.

Функціональні можливості:

– підтримка до 4094 VLAN, з можливістю настройки VLAN по портах, MAC-адресах та інших критеріях;

– підтримка STP для запобігання петель в мережі та забезпечення високої доступності;

– підтримка link aggregation (EtherChannel) для збільшення пропускної здатності та надійності зв'язку між комутаторами;

– підтримка QoS для управління трафіком та забезпечення пріоритету для критичних застосунків;

– підтримка функцій безпеки, таких як ACL (Access Control Lists), 802.1x, SSH, SSL, та інших;

– підтримка різних протоколів управління, таких як SNMP, HTTP, HTTPS, Telnet, та інших;

– підтримка функцій моніторингу, таких як syslog, RMON, та інших;

– підтримка PoE для живлення пристроїв, таких як IP-телефони, камери спостереження, та інших;

– підтримка до 255 комутаторів в стеці для збільшення масштабу мережі.

Комутатор Cisco 2960-24TT є популярним вибором для будівництва мереж в офісах, школах, університетах та інших організаціях, де необхідна надійна та масштабована мережева інфраструктура.

Wi-Fi router Linksys WRT-300N.

Linksys WRT300N – це бездротовий для невеликих домашніх мереж.

Функціональні можливості:

– підтримка стандартів Wi-Fi 802.11b/g/n;

– швидкість бездротового з'єднання до 300 Мбіт/с;

– порти Ethernet Gigabit LAN;

– 1 порт WAN для підключення до інтернет-провайдера;

– 1 порт USB 2.0 для підключення зовнішніх пристроїв;

– підтримка QoS (Quality of Service) для пріорітизації трафіку;

– вбудований сервер DHCP;

– підтримка VPN-тунелювання;

– батьківський контроль та фільтрація веб-контенту;

– підтримка шифрування WEP, WPA та WPA2;

– вбудований міжмережевий екран.

2.2.1.2 Термінальний сервер

Мати прямий послідовний доступ до мережевих пристроїв, включаючи доступ до завантажувача, службової ОС тощо, можна за допомогою виділеного сервера терміналів. Але можна надати практично ті самі функції, використовуючи один із маршрутизаторів Cisco і відповідні асинхронні послідовні порти.

Сервер терміналів забезпечує позасмуговий доступ для кількох пристроїв. Позадіапазонний доступ здійснюється через консоль маршрутизатора або допоміжний порт у порівнянні з внутрішньосмуговим доступом, який здійснюється через мережу за допомогою зворотнього Telnet. Загалом сервер терміналів – це маршрутизатор із декількома асинхронними портами, підключеними до інших пристроїв, таких як консольний порт інших маршрутизаторів або комутаторів [7].

Найвідомішими серверами доступу Cisco є 2509 і 2511. Хоча ці моделі зняті з виробництва, вони ще використовуються в багатьох компаніях як сервери доступу для мережевого обладнання. Ці пристрої мають 8 і 16 асинхронних послідовних портів відповідно. Це означає, що можна до 8 або 16 пристроїв підключити їхні консольні порти до сервера доступу та керувати цими пристроями, перейшовши до консольного порту або підключившись до сервера доступу Telnet. Для їх підключення необхідно під’єднати асинхронний вісімковий кабель до 68-контактного інтерфейсу SCSI 2511 (рис. 2.4) [8].

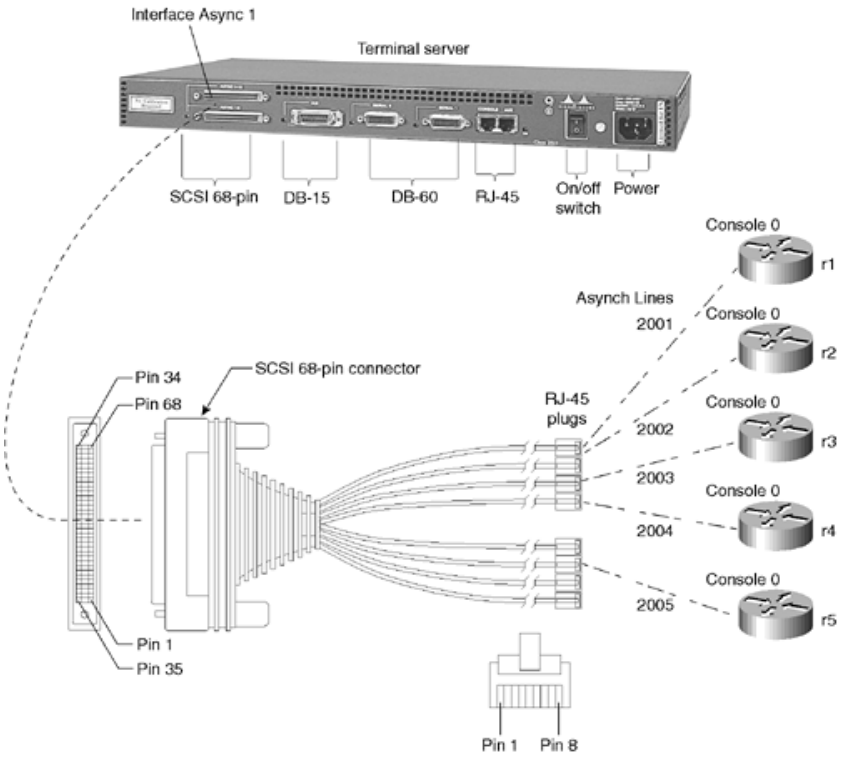


Рисунок 2.3 – Підключення Cisco 2511 до мережних пристроїв

Іншим варіантом є асинхронний мережевий модуль HWIC-8A/S-RS232 (рис.2.5). Цей модуль може встановлюватися в маршрутизатор Cisco 2911, що задовольняє нашим вимогам та обраному нами пристрою.

Рисунок 2.4 – Модуль HWIC-8A/S-RS232

Для цього модуля потрібен кабель CAB-HD8-ASYNC. З одного боку він має такий же роз’єм же SCSI-68 pin male, а з іншого – 8 проводів з RJ-45 на кінці (рис.2.6).

Рисунок 2.5 – Кабель CAB-OCTAL-ASYNC

Він забезпечує вісім асинхронних (асинхронних) портів згорнутого кабелю RJ-45 на кожному 68-контактному роз'ємі. 68-контактний роз'єм підключений до Interface Async сервера терміналів. Кожен згорнутий кабель RJ-45 підключається до консольного порту кожного мережного пристрою. Для цілей конфігурації кожен згорнутий кабель у конфігурації називається асинхронною лінією. Кожен рядок має нумерацію, починаючи з 2001 до 2008 (рис.2.4).

Встановлення підключення від маршрутизатора до одного з портів консолі називається зворотним telnet.

Зворотний Telnet – це спосіб здійснення з'єднання з клієнтського пристрою до сервера через протокол Telnet, але з використанням власного сервера, який надає цю можливість. У зворотньому Telnet сервер відкриває порт і чекає на з'єднання від клієнта.

Основна ідея полягає в тому, що сервер чекає на з'єднання, а клієнтські пристрої ініціюють це з'єднання. Це відмінно від класичного Telnet, де клієнтські пристрої запитують сервер про з'єднання. У зворотньому Telnet роль ініціювання з'єднання відіграється клієнтом.

Це може бути корисним в таких сценаріях, де сервер розташований за файрволом або NAT, який забороняє зовнішнім пристроям ініціювати з'єднання. Зворотній Telnet дозволяє обійти ці обмеження, оскільки з'єднання ініціюється від клієнта, який знаходиться за файрволом або NAT, і сервер лише чекає на це з'єднання.

Проте, варто зауважити, що використання Telnet, взагалі, може бути

небезпечним через його відкритий текстовий формат, що робить передачу даних небезпечною у відкритих мережах. Тому, зазвичай, рекомендується використовувати більш безпечні альтернативи, такі як SSH (Secure Shell).

2.2.2 Розробка специфікації папаратних засобів

Для виконання поставленої задачі було розроблено специфікацію апаратних засобів комп'ютерної системи, у тому числі засобів збору та передачі інформації, інформації про які наведена в таблиці 2.1 та інформація про автоматизоване робоче місце працівника охорони здоров'я.

Таблиця 2.1 – Специфікація обладнання в КЗ ДГП

Позиція	Найменування і технічна характеристика	Тип, марка	Одиниці виміру	Кількість
1.	Маршрутизатор Cisco 2911 (2xGE, 2xWAN,1xSFP)	Cisco 2911-SEC/K9	од.	2
2.	Коммутатор Cisco 2960 24xLAN(10/100 Мбіт/с + 2SFP)	Cisco WS-C2960-TT	од.	7
3.	Wi-Fi router Linksys WRT-300N. Стандарт: 802.11b/g/n Максимальна швидкість з'єднання: 300 Мбіт/с	Linksys WRT-300N	од.	3
4.	Асинхронний мережевий модуль HWIC-8A	HWIC-8A/S-RS232	од.	1
5.	Кабель Lead Octal Cable (68 pin to 8 Male RJ-45s)	CAB-OCTAL-ASYNC	од.	1
6.	Сервер: 1 шт HP ProLiant DL380P Gen8 Intel Xeon E5-2609 v0x2 16 RAM 72HDD, 8 GB DDR3, 2x порта 1 Gb Ethernet	HP ProLiant DL380P	од.	1
7.	Комп'ютер: ПК HP EliteDesk 705 G4 Mini AMD A10 8/128Gb, Windows 10Pro	HP EliteDesk 705 G4	од.	20
8.	БФП кольорового друку Canon PIXMA G2430, технологія друку струменева	Canon PIXMA G2430	од.	8
9.	Кабель вита пара КПВ-ВП (250) 4*2*0,54 (U/UTP-cat.6), 305 м	КПВ-ВП (250) 4*2*0,54 (U/UTP-cat.6)	од	1
10.	Кабельний канал 40x25 мм	Елекор м	м.	300
11.	Розетка комп'ютерна RJ-45 Electric Asfora	Schneider	од.	100

2.2.3 Розробка структурної схеми мережі

Організація комп'ютерної мережі в геріатричному пансіонаті є одним з ключових елементів ефективної роботи медичного персоналу та забезпечення високоякісної медичної допомоги. Комплекс технічних засобів комп'ютерної мережі лікувального закладу складається з кількох компонентів, які працюють разом для забезпечення надійної та швидкої передачі даних.

Структурна схема мережі, часто перший документ у мережевому проекті, надає уявлення високого рівня про архітектуру мережі та основні функціональні модулі.

Загальні елементи, зображені на структурній схемі, включають комутатори (як L2, так і L3), брандмауери, сервери, комп’ютери та ключові сегменти мережі, такі як з’єднання провайдера, локальні мережі та Wi-Fi.

На рис. 2.1 зображена узагальнена структурна схема локальної мережі пансіонату. Хости об’єднуються в локальну мережу комутаторам другого рівня. Комутатори доступу сходяться в одну єдину точку до комутатора ядра. Він є один з головних елементів сегментації саме локальних мереж, як правило це комутатор третього рівня, який вміє амортизувати трафік між локальними сегментами, там де потрібна висока швидкість. Далі іде периметр мережі, який реалізований або маршрутизатором, який забезпечує захист мережі. Маршрутизатор під'єднаний до мережі інтернет-провайдера.

Для забезпечення всіх вузлів у підмережі, буде встановлено відповідну кількість комутаторів. Так як у комутатора Cisco 2960 кількість портів 24 Fast + 2 Gigabit, на третьому та другому поверхах для 30 підключень та запас 10% достатньо 2 комутатори. На першому поверху буде встановлено 3 комутатори, для кожного сегменту відділу окремий. Комутатор ядра з’єднується з маршрутизатором для доступу в Інтернет. На кожному поверсі передбачено Wi-Fi-маршрутизатор для безпровідного під’єднання через мобільні пристрої.

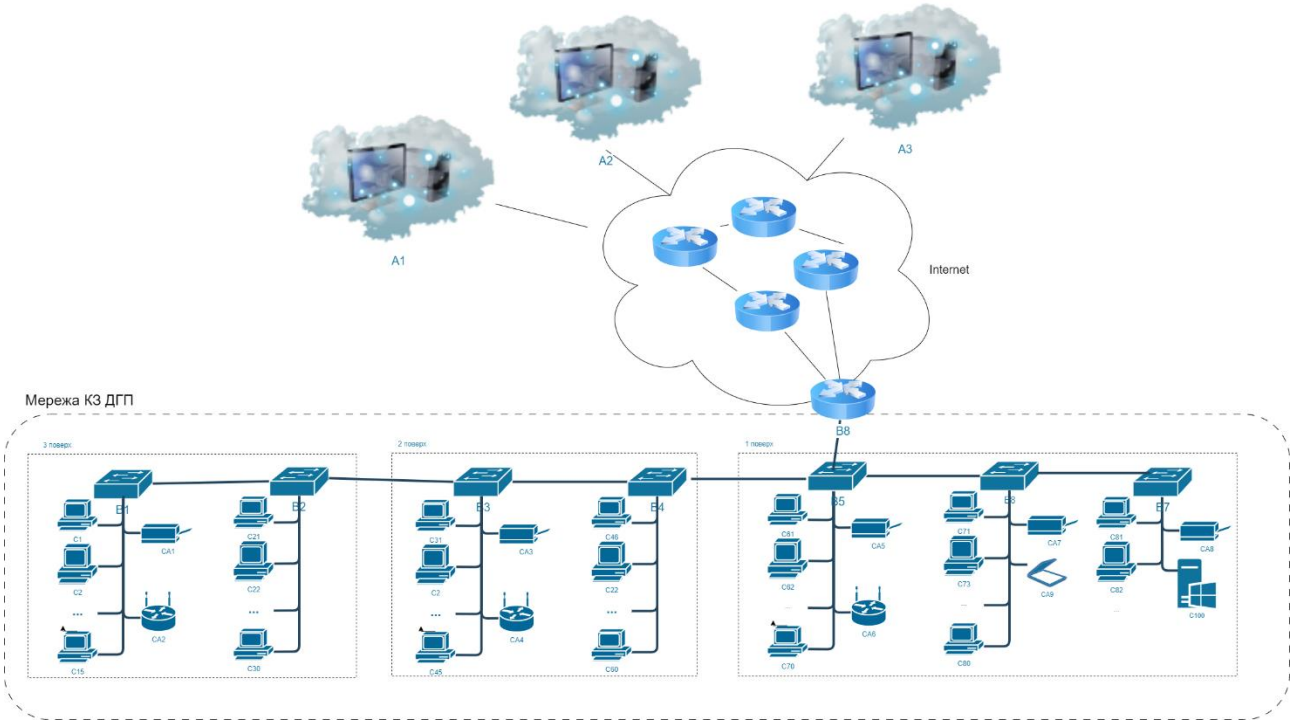


Рисунок 2.6 – Структурна схема мережі

2.3 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

Швидкість надходження пакетів повинна бути менше, ніж швидкість відправлення для того, щоб не перевантажувати канал.

В підмережі LAN1 пансіонату встановлений комутатор ядра Cisco2960, що об'єднує 119 хостів. Вихідний трафік з комутатора Fl1_SW0_Potik надсилається до роутера R1_LAN1_Potik В в лінію з пропускною здатністю, що становить 1000 Мбіт/с.

Для того, щоб комутатор не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку μ=108 кадрів/с, а середня довжина повідомлення складає 850 байт.

Теоретично припустимо, що всі користувачі найбільшої підмережі LAN1 одночасно використовують мережу. В такому разі, пропускна здатність на рівні доступу буде дорівнювати:

$$P_{р.р.} = \mu L_{пов} * N * 8 = 108*850*119*8 = 87 \text{ Мбіт/с} \qquad (3.1)$$

де $L_{пов}$ – середня довжина повідомлення;

N – кількість вузлів в мережі.

Отриманий результат не перевищуватиме заданих параметрів мережі по вихідному каналу, отже перенавантажень не трапиться.

Комутатор Fl1_SW0_Potik також передає трафік до маршрутизатора зі швидкістю 1000 Мбіт/с. Отже, загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих} = 10^9 / (850 * 8) = 147\ 058 \text{ пакетів/с} \quad (3.2)$$

Оскільки в середньому, кожне джерело виробляє 108 пакетів/с, то маршрутизатор обмежений кількістю приєднань, яку ми можемо дізнатись наступним чином:

$$N = \mu_{вих} / \mu = 147058/ 108 \approx 1362 \text{ джерела} \quad (3.3)$$

Ця кількість задовольняє кількості вузлів у найбільшій нашій локальній мережі, до якої входить 119 ПК.

Кожен з 119 ПК посилає потік заявок з інтенсивністю у 108 кадрів/с. Звідси, можем розрахувати інтенсивність вихідного трафіку:

$$\lambda = N\ \mu = 119*108 = 12852 \text{ пакетів/с.} \quad (3.4)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu вих} = \frac{12852}{147\ 058} = 0{,}087 \quad (3.5)$$

Коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0{,}087}{1-0{,}087} = 0{,}095 \quad (3.6)$$

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

$$T = \frac{1}{(\mu-\lambda)} = \frac{1}{(147\ 058 - 12852\ )} = 7.45 \text{ мкс} \quad (3.7)$$

Середня довжина черги:

$$L_{чер} = \frac{\rho^2}{1-\rho} = \frac{0{,}087^2}{1-0.087} = 0.0083 \quad (3.8)$$

Середній час перебування пакета у черзі:

$$T_{оч} = \frac{Lчер}{\lambda} = \frac{0{,}083}{12852} = 6.45 \text{ мкс} \quad (3.9)$$

Це значення задовольняє вимогам до затримки в ЛМ.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розробка схеми фізичної топології мережі пансіонату

Розробка схеми фізичної топології корпоративної мережі – це процес планування та проектування фізичної структури мережі, що включає в себе розміщення пристроїв, кабелів, комутаторів, маршрутизаторів та інших компонентів мережі.

Для підключення пристроїв до мережі зі швидкістю 100 Мбіт/с найбільш підходящим типом кабелю буде Category 5e (Cat5e) або Category 6 (Cat6).

Кабель категорії 5e (Cat5e) підтримує швидкість передачі даних до 1 Гбіт/с, широко використовується в сучасних локальних мережах, забезпечує достатню пропускну здатність для мережі зі швидкістю 100 Мбіт/с. Має хороше співвідношення ціна/якість та підтримує стандарти Ethernet 10/100/1000 Мбіт/с.

Кабель категорії 6 (Cat6) підтримує швидкість передачі даних до 10 Гбіт/с, забезпечує більшу пропускну здатність та краще екранування, ніж Cat5e, може бути доцільним вибором, якщо в майбутньому планується модернізація мережі до вищих швидкостей, але має дещо вищу вартість, ніж Cat5e.

Для локальної мережі з майбутньою її модернізацією найбільш оптимальним вибором буде Category 6e (Cate) кабель. Він забезпечить необхідну продуктивність з перспективою на майбутнє.

Загалом, найбільш оптимальними місцями для розташування комутаторів та маршрутизаторів у локальній мережі є центральні, легкодоступні та добре вентильовані приміщення, такі як серверні кімнати або спеціально обладнані комунікаційні шафи. Це дозволить забезпечити ефективне підключення кінцевих пристроїв, надійність та масштабованість мережі.

Перед тим як приступити до побудови мережі треба визначити деякі правила підключення обладнання між собою, які будуть завжди однаковими для моделювання:

– підключення обладнання до комутаторів виконується за допомогою прямого кабелю Cat6, вони приєднуються до портів FastEthernet;

– підключення комутаторів між собою виконується за допомогою перехресного кабелю. Вони приєднуються виключно до портів GigabitEthernet з метою забезпечення швидкісної передачі даних;

– підключення комутатора до маршрутизатора виконується за допомогою прямого кабелю, вони приєднуються до портів GigabitEthernet;

– підключення маршрутизатора до глобальної мережі, тобто назовні, виконується також за допомогою прямого кабелю. Він приєднується до порту GigabitEthernet.

Ці правила використовують з метою забезпечення безперебійної роботи мережі.

При створені проекту було використано топологію "дерево" (об'єднання декількох топологій "зірка").

Відповідно до вимог (розділ.2.3.2) мережа пансіонатів складаються з 5 мереж LAN1-LAN5.

LAN1 – це мережа «Дніпропетровського геріатричного пансіонату, яка повинна забезпечувати 119 хостів та до неї входить HTTP сервер для надання веб-сторінок. В LAN1 повинна використовуватися технологія логічного розділення фізичної мережі на окремі віртуальні мережі VLAN, а граничний маршрутизатор в LAN1 буде виконувати роль термінального сервера.

Пансіонат – триповерховий будинок в якому розташовується 119 персоналу та клієнтів загалом. В серверній на 1 поверсі буде розміщено 1 маршрутизатор, який буде керувати трафіком та 4 комутатори, які будуть об’єднувати користувачів адміністративного відділу, медичного + відділ соціальної роботи, серверів та клієнтів.

З самого початку для моделювання мережі пансіонату в Packet Tracer в вкладці фізичної топологогії створено 3 поверхи, які мають назви “Поверх1”, “Поверх2” та “Поверх3”. Переглянути їх розташування можна на рисунку 3.1.

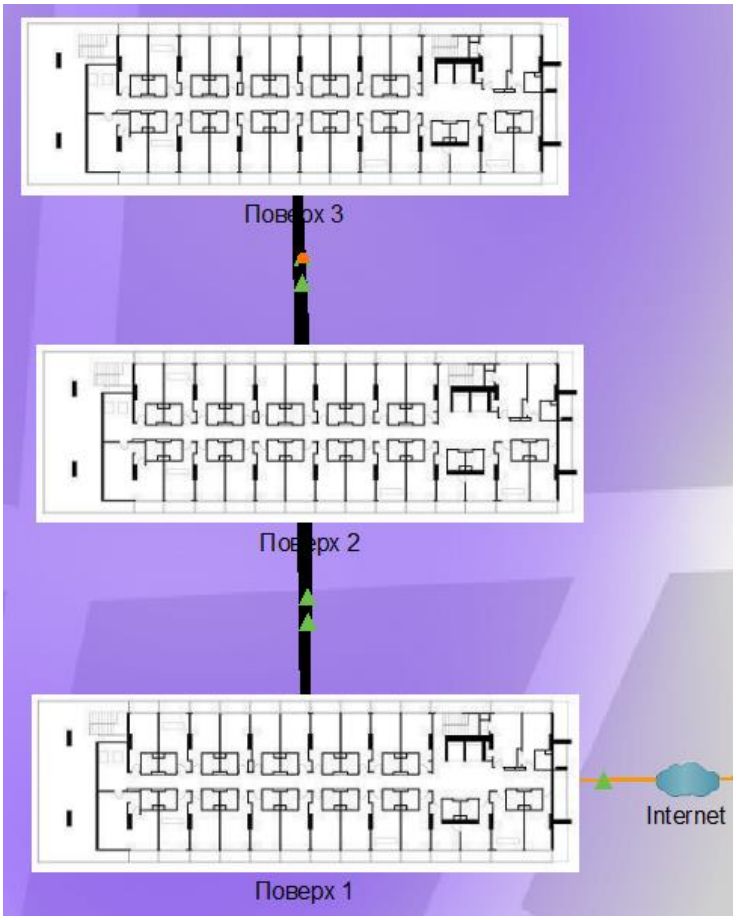


Рисунок 3.1 – Загальна фізична топологія пансіонату

Почнемо з першого поверху – головного. На ньому розташувався медперсонал з кабінетами для надання медичних послуг пенсіонерам. На поверсі налічується 20 хостів. Вони розміщені в умовній локації, яка має 9 приміщень, одне з яких це серверна кімната, яка є на кожному поверсі. Усі підключені кабелі розміщені в коробах, розташування комп'ютерів має умовний характер для відображення дійсності. Вигляд побудованого першого поверху можна побачити на рисунку 4.2. Зелений кабель, який йде через стіну на рисунку – прямий, ним підключені комп'ютери до комутаторів. Назви комп'ютерів на схемі відповідають поверху, на якому вони розташовані. Усі кабелі з комп'ютерів йдуть до серверної кімнати, у якій розташовані комутатори, до яких вони підключені.

Маршрутизація для виходу в Інтернет буде статичною. В якості мережного обладнання обрано маршрутизатор 2911, оскільки він має високу продуктивність та включає GigabitEthernet порти, що мають пропускну здатність 1 гігабіт на секунду, та комутатори Cisco Catalyst 2960, які включають 24 FastEthernet порти

з пропускною здатністю 100 мегабіт на секунду та 2 GigabitEthernet порти, також підтримує технологію VLAN, має покращену безпеку, додаткові функції контролю доступу та і.н.

Для того, щоб поверх відповідав усім заданим нормам потрібно влаштувати серверну кімнату, у якій для належної роботи знаходяться 2 сервери (приватний та піблічний HTTP), 4 комутатори, у яких в наявності є 24 інтерфейси для підключення усіх комп'ютерів на поверсі та маршрутизатор, за допомогою якого заклад матиме змогу виходу у глобальну мережу. На рисунку 3.2 представлено перший поверх в програмі Packet Tracer.

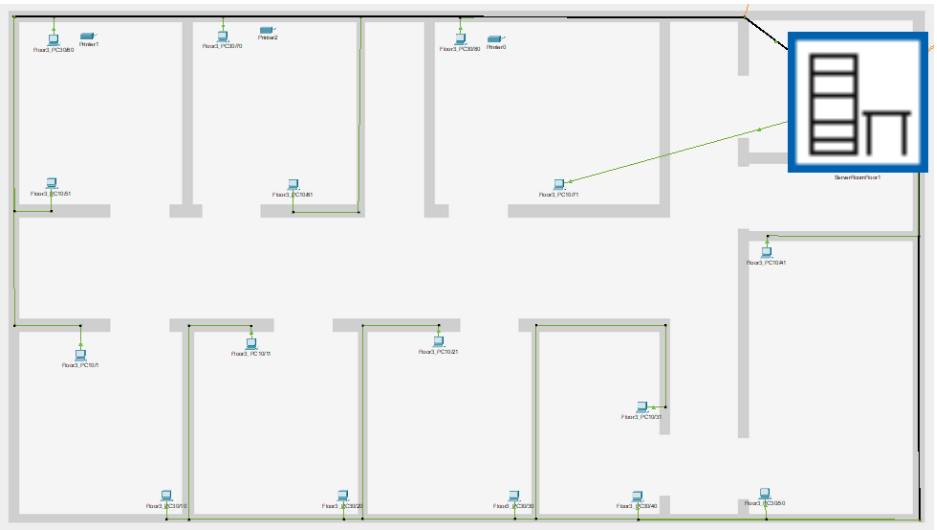


Рисунок 3.2 – Фізична топологія першого поверху

Після об'єднання обладнання між собою отримуємо готовий перший поверх, який служить каркасом для нашої подальшої роботи з побудови мережі пансіонату. Тому переходимо до моделювання наступного поверху.

На другому та 3 поверхах знаходяться кімнати, де проживають люди похилого віку. Так само все починається з розташування розеток у приміщеннях та їх підключеннях до комутаторів. Слід зазначити, що окрім зеленого кабелю можна побачити ще один – помаранчевий. Він є перехрестним та відповідає за з'єднання комутаторів між собою. Вони підключені в порти GigabitEthernet з метою збільшення можливостей підмережі. Методика побудови поверху така сама, як і на попередньому. На рисунку 4.3 представлено другий поверх в програмі Packet Tracer. Аналогічно виглядає третій поверх.

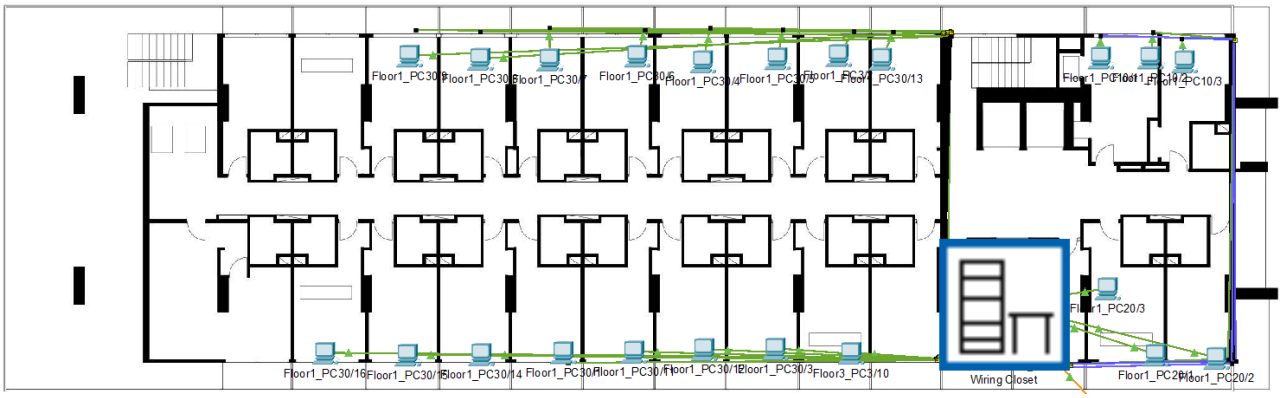


Рисунок 3.3 – Фізичне розташування другого поверху

На рис. 3.4 представлено L2-схему пансіонату в м. Дніпро.

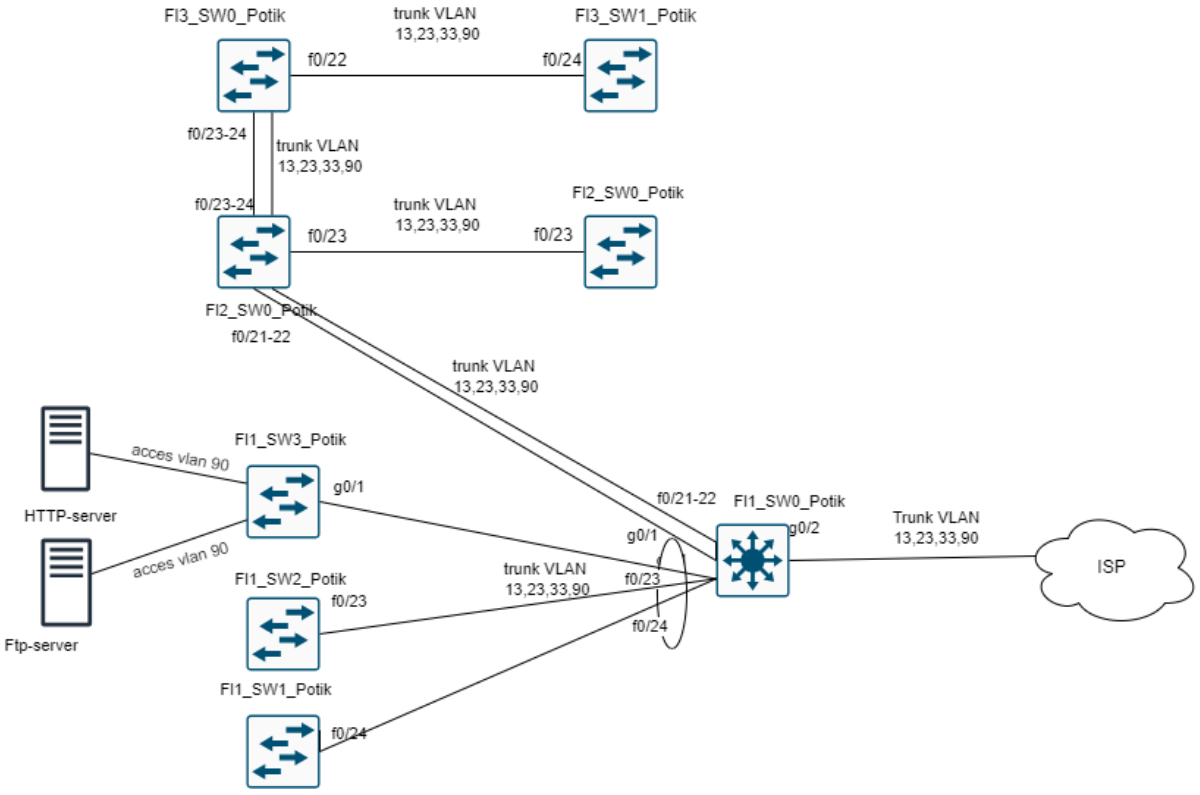


Рисунок 3.4 – L2-схема пансіонату в м. Дніпро

3.2 Розрахунок схеми адресації корпоративної мережі

Відповідно до вимог (розділ.2.3.2) мережа пансіонатів складаються з 5 мереж LAN1-LAN5, з конкретною кількістю вузлів в кожній з них: 119, 68, 197, 54 та 53 відповідно. Блок адрес для виділення підмереж повинен бути 172.20.40.0/21, а для каналів між маршрутизаторами застосувати блок адрес 10.0.13.0/24.

Щоб зменшити навантаження та підвищити безпеку в мережі LAN1 пансіонату м. Дніпро буде використано технологію віртуальних локальних мереж (VLAN). Для цього мережу буде розділено на окремі віртуальні підмережі, за межі яких не буде виходити широкомовний трафік. Виходячи із організаційної структури (рис.1.1) таких підмереж буде організовано 4: VLAN13, VLAN23, VLAN33, VLAN90. Таким чином, можна буде розділити користувачів на 4 підрозділи, а також розвантажити трафік, оскільки комутатор буде відправляти пакети тільки до тих користувачів, які знаходяться у відповідній VLAN. Користувачі в різних VLAN зможуть обмінюватися пакетами між собою через маршрутизатор, а в одній, напряму через комутатор.

Метод VLSM (Variable Length Subnet Masking) дозволяє розподіляти IP-адреси більш ефективно, використовуючи підмережі різних розмірів в одній мережі. Алгоритм виконання розрахунку IP-адресації за допомогою VLSM наступний:

1. Визначається кількість хостів для кожної підмережі.
2. Підмережі сортуються за кількістю хостів у порядку спадання.
3. Обирається початковий блок IP-адрес, який буде використовуватися для розділення на підмережі.
4. Для кожної підмережі обчислюється необхідна маска підмереж за формулою:

$$2^n \geq (\text{Кількість хостів} + 2) \qquad (4.1)$$

де n – кількість біт, відведених під частину хоста.

5. Починаючи з найбільшої підмережі призначаються їй IP-адреси, дотримуючись правил маскування.
6. За описаною вище схемою розраховується адреса для наступної підмережі.

В таблиці 3.1 наведено результат розрахунку адрес мереж методом VLSM. Важливо, щоб не було перекриття між підмережами і всі адреси використовувалися оптимально.

Таблиця 3.1 – Схема адресації мережі

Назва підмережі	Кіл. вузлів	Адреса підмережі	Маска підмережі	Діапазон допустимих IP-адрес вузлів
LAN1_Dnipro	119	172.20.41.0	255.255.255.128	172.20.41.1 - 172.20.41.126
VLAN 33	60	172.20.41.0	255.255.255.192	172.20.41.1 - 172.20.41.62
VLAN 23	30	172.20.41.64	255.255.255.224	172.20.41.65 - 172.20.41.94
VLAN 13	14	172.20.41.96	255.255.255.240	172.20.41.97 - 172.20.41.110
VLAN 90	6	172.20.41.112	255.255.255.248	172.20.41.113 - 172.20.41.118
LAN2_X	68	172.20.41.128	255.255.255.128	172.20.41.129 - 172.20.41.254
LAN3_Y	197	172.20.40.0	255.255.255.0	172.20.40.1 - 172.20.40.254
LAN4_Z	54	172.20.42.0	255.255.255.192	172.20.42.1 - 172.20.42.62
LAN5_W	53	172.20.42.64	255.255.255.192	172.20.42.65 - 172.20.42.126
WAN1	2	10.0.13.0	255.255.255.252	10.0.13.1 – 10.0.13.2
WAN2	2	10.0.13.4	255.255.255.252	10.0.13.5 – 10.0.13.6
WAN3	2	10.0.13.8	255.255.255.252	10.0.13.9 – 10.0.13.10

3.3 Розробка логічної схеми мережі

Розробка логічної топології комп'ютерної мережі пансіонату включає в себе розподіл мережі на логічні сегменти та визначення способів комунікації між цими сегментами.

Основні сегменти мережі пансіонату:

– адміністративна область для реєстраційний пункт, фінансовий відділ тощо;

– медична область для медичних працівників, лікарів, медсестер та іншого медичного персоналу;

– пацієнтська область для пацієнтів з доступом до Інтернету та розважальних ресурсів;

– серверна область для серверів та мережного обладнання.

Розробка логічної топології комп'ютерної мережі для лікарні потребує детального планування та налаштувань, щоб забезпечити надійну та безпечну мережу, яка відповідає потребам медичного закладу.

На рис. 3.5 представлено L3-схему LAN1. Також, варто зазначити, що на L3-схемі один порт на маршрутизаторі містить декілька IP-адрес, це пов’язано з розділенням інтерфейсу на підінтерфеси (віртуальні інтерфейси), необхідно для маршрутизації між VLAN.

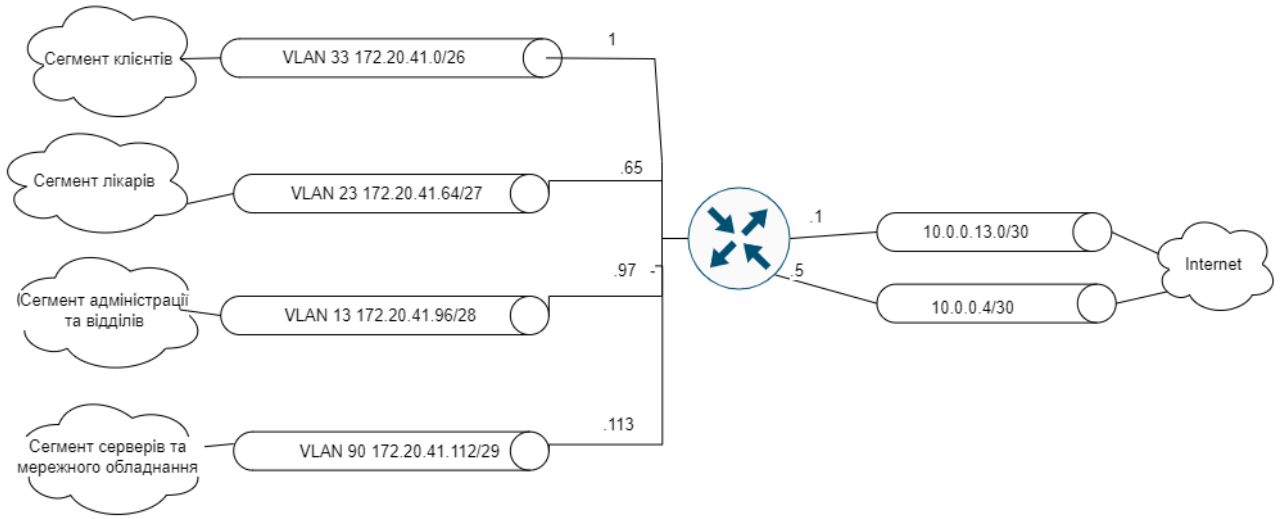


Рисунок 3.5 – L2-схема мережі пансіонату в м.Дніпро

На рис. 3.6, відповідно до завдання, представлено побудовану логічну топологію всієї мережі пансіонатів в програмі Packet Tracer. В мережах LAN2-LAN5 схема L3 може також бути реалізованою як в мережі LAN1 Дніпровського пансіонату.

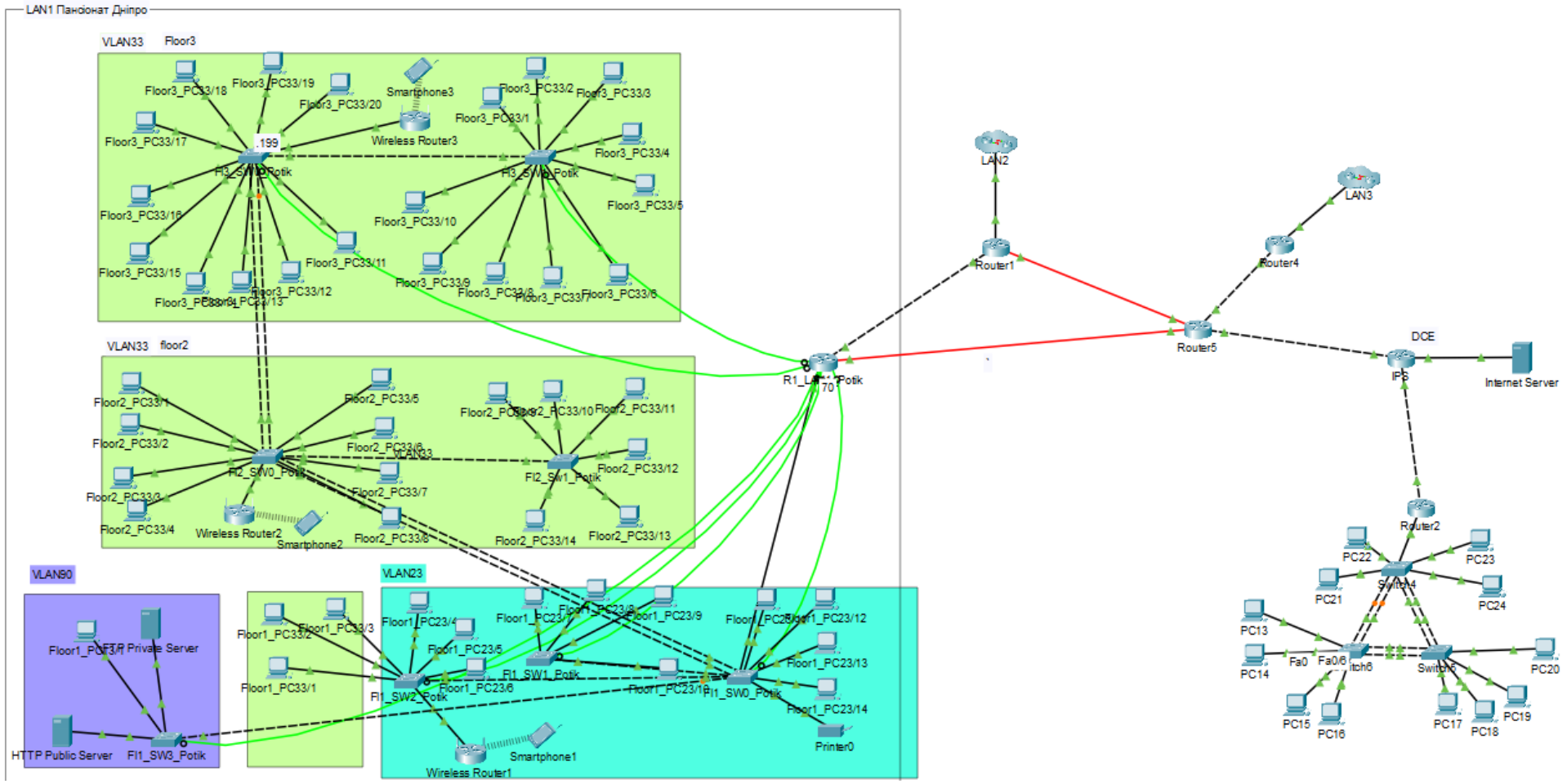


Рисунок 3.6 – Логічна топологія мережі пансіонатів

3.5 Розрахунок схеми адресації пристроїв

Відповідно до вимог мережі, мережу потрібно створювати за допомогою таких принципів:

– перші доступні IP-адреси повинні бути призначені на інтерфейсі маршрутизатора та нижче інтерфейсу LAN;

– кожному комутатору локальної мережі повинна бути призначена друга можлива IP-адреса;

– серверам, як правило, надаються налаштовані IP-адреси, які також починаються з першої можливої адреси у мережі;

– остання використана IP-адреса буде призначена останньому пристрою у мережі;

– VLAN використовує адресацію кінцевих пристроїв через DHCP.

Детальна адресація пристроїв в мережі LAN1, як у фізичній, так і в логічній топології, наведена у таблиці 3.2.

Таблиця 3.2 – Схема адресації пристроїв мережі LAN1

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN
R1_LAN1_Potik	g0/0	10.0.0.1	/30	-	-
	g0/3/0	10.0.4.1	/30	-	-
	g0/1.13	172.20.40.1	/25	-	13
	g0/1.23	172.20.40.129	/27	-	23
	g0/1.33	172.20.40.161	/27	-	33
	g0/1.43	172.20.40.193	/28	-	43
Fl1Sw1_Potik	Vlan1	172.20.40.194	/28	172.20.40.193	-
Fl1Sw2_Potik	Vlan1	172.20.40.195	/28	172.20.40.193	-
Fl2Sw1_Potik	Vlan1	172.20.40.196	/28	172.20.40.193	-
Fl2Sw2_Potik	Vlan1	172.20.40.197	/28	172.20.40.193	-
Fl3Sw1_Potik	Vlan1	172.20.40.198	/28	172.20.40.193	-
Fl3Sw2_Potik	Vlan1	172.20.40.199	/28	172.20.40.193	-

3.6 Налаштування та перевірка роботи комп’ютерної системи

Після виконання підрахунку адресації йдемо далі та починаємо налаштування маршрутизатору та комутаторів, на яких маємо виконати

динамічне розподілення адрес, VLAN, NAT та присвоєння адрес комутаторам, серверам та маршрутизатору.

Розпочнемо з найголовнішого – маршрутизатора. Спочатку треба створити на кабелі, який веде до нашої мережі підінтерфейси, які будуть використовуватися в подальшому для наших віртуальних мереж та увімкнути його. Не забуваємо привласнити їм першу адресу мереж відповідних VLAN. Одразу привласнимо адресу інтерфейсу, який веде назовні. Для зручного користування маршрутизатором змінюємо його назву. Команди, використані під час цих налаштувань, можна побачити нижче.

Лістинг 3.1 – Налаштування IP-адрес на роутері

```
hostname R1_LAN1_Potik
interface GigabitEthernet0/1.13
encapsulation dot1Q 13
ip address 172.20.41.1 255.255.255.192
!
interface GigabitEthernet0/1.23
encapsulation dot1Q 23
ip address 172.20.41.65 255.255.255.224
!
interface GigabitEthernet0/1.33
encapsulation dot1Q 33
ip address 172.20.41.97 255.255.255.240
!
interface GigabitEthernet0/1.43
encapsulation dot1Q 43
ip address 172.20.41.113 255.255.255.248
```

Наступним завданням було виділення пулу адресів з підмереж на свій розсуд (тобто кількість, яку забажаємо). У першій підмережі це 10 адрес, у другій одна та у третій дві. Далі ми створюємо об’єднаний резерв для VLAN, вказуючи адресу мережі, її маску, шлюз та DNS-сервер. Далі це нам знадобиться для динамічного розподілу адрес та налаштування DHCP-сервісу.

Лістинг 3.2 – Налаштування DHCP

```
ip dhcp excluded-address 172.20.40.1 172.20.40.10
ip dhcp excluded-address 172.20.40.129
no ip dhcp excluded-address 172.20.41.97
no ip dhcp excluded-address 172.20.41.113
!
```

```
ip dhcp pool pool_VLAN13
 network 172.20.41.0 255.255.255.192
 default-router 172.20.41.1
 dns-server 172.20.41.10
ip dhcp pool pool_VLAN23
 network 172.20.41.64 255.255.255.224
 default-router 172.20.41.65
 dns-server 172.20.41.10
ip dhcp pool pool_VLAN33
 network 172.20.41.96 255.255.255.240
 default-router 172.20.41.97
 dns-server 172.20.41.10
ip dhcp pool pool_VLAN43
 network 172.20.41.112 255.255.255.248
 default-router 172.20.41.113
 dns-server 172.20.41.10
```

Після виконання усіх потрібних налаштувань потрібно переконатися у правильності їх написання, тому за допомогою команди do show ip int brief перевіряємо результат наших налаштувань. Отриманий результат можна переглянути на рисунку 3.7.

```
R1_LAN1_Potik#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     10.0.13.1       YES manual up                    up
GigabitEthernet0/1     unassigned      YES NVRAM  up                    up
GigabitEthernet0/1.13  172.20.41.1     YES manual up                    up
GigabitEthernet0/1.23  172.20.41.65    YES manual up                    up
GigabitEthernet0/1.33  172.20.41.97    YES manual up                    up
GigabitEthernet0/1.43  172.20.41.113   YES manual up                    up
GigabitEthernet0/2     unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0/0   unassigned      YES unset  down                  down
GigabitEthernet0/1/0   unassigned      YES unset  down                  down
GigabitEthernet0/3/0   10.0.13.5       YES manual up                    up
Loopback1              10.10.10.1      YES manual up                    up
```

Рисунок 3.7 – Перевірка правильності налаштувань на маршрутизаторі R1_LAN1_Potik

Бачимо, що команди, які ми використовували, налаштовані вірно, тому маємо змогу переходи до налаштувань комутаторів, яких у нас в 6 штук.

Виконаємо стандартне налаштування комутаторів. Налаштуємо VLAN і привласнимо інтерфейс для них. Змінемо назву пристрою на зручну для нас. Після цього створюємо інтерфейс vlan90 та надаємо йому IP-адресу з нашої додаткової четвертої підмережі. Вмикаємо інтерфейс та додаємо комутатору шлюз за замовчуванням. Для налаштування кожного з комутаторів

відрізнятись буде лише IP-адреса. Використані команди налаштування наведені далі.

Лістинг 3.3 – Налаштування IP-адреси на коммуаторах

```
host Fl3_SW1_Potik
int vlan90
ip add 172.20.40.194 255.255.255.240
no shut
ip default-gat 172.20.40.193
```

Після стандартного налаштування комутаторів перейдемо до створення VLAN на комутаторах та надання їм назви для подальшого керування створеною віртуальною мережею. Ці команди використовуються для налаштування кожного з комутаторів без змін. Приклад такого налаштування за допомогою відповідних команд продемонстрований нижче.

Лістинг 3.4 – Оголошення VLAN

```
vlan 13
name Accounting
vlan 23
name Doctor
vlan 33
name Pacienty
vlan 90
name Management
```

VLAN ми створили, залишилось присвоїти на комутаторі інтерфейси відповідно до підрозділів, у яких знаходяться наші пристрої.

Для цього треба визначити та вказати довжину адрес, які будуть підходити для певної віртуальної мережі. Ось на цьому етапі налаштування на комутаторах може відрізнятись, тому треба бути уважними і не допустити помилок. Варіант мого завдання виявився не дуже складним для цього, адже лише на одному комутаторі в мене є два підрозділи, а на всіх інших лише по одному. Є сенс уважно перевіряти інтерфейси, до яких підключені комп’ютери того чи іншого підрозділу, адже від цього залежить працездатність мережі між собою. Після визначення діапазону певних підрозділів треба вказати метод доступу в залежності від наших потреб (Access – на шляху до мережевих пристроїв, Trunk – на шляху інтерфейсів, якими з’єднані комутатори між собою). Ще треба виконати налаштування інтерфейсів підключення

комутаторів між собою для можливості обміну даними. Приклад такого налаштування показаний далі.

Лістинг 3.5 – Налаштування потів доступу та танкових каналів

```
interface range fa0/9-22
switchport mode access
switchport access vlan 21
interface range fa0/1-8
switchport mode access
switchport access vlan 31
int g0/1
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan all
interface range f0/21-24, g0/1-2
swi mode trunk
```

Таким чином ми налаштовуємо кожний комутатор відповідно до його потреб. Тепер маємо можливість заповнити таблицю 3.3 відповідність мереж VLAN і призначення її портів, їх опис. Побачити її можна на наступній сторінці.

Таблиця 3.3 – Мережі VLAN і призначення портів

Номер VLAN	Ім’я VLAN	Порт	Примітка
33	Pacienty	Fl2_SW1 Fa0/10-20 Fl2_SW2 Fa0/10-20 Fl3_SW1 Fa0/10-20 Fl3_SW2 Fa0/10-20 Fl1_SW2 Fa0/1-10	Для пацієнтів
23	Doctor	Fl1_SW2 Fa0/11-20 Fl1_SW1 Fa0/11-20	Для лікарів
13	Accounting	Fl1_SW0 Fa0/11-20	Для адміністрації
90	Management	Fl1_SW3 Fa0/1-10	Server

Після виконання налаштувань комутаторів вже маємо можливість призначити комп’ютерам за допомогою сервісу DHCP ip-адрес, маску, dns-сервер та шлюз. Відбувається це все автоматично. Також для зручності краще розподілити комп’ютери на логічній топології по нашим створеним підрозділам і виконати нотатки у вигляді назви мережі, її ip-адреси, маски, шлюзу та діапазону адрес.

Слід ще зазначити, що на кожній підмережі після її побудови та налаштування треба виконати перевірку. Спочатку перевіримо на комутаторі налаштовані VLAN. Для цього використаємо команду show vlan brief.

```
Fl1_SW2_Potik#sh vlan br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1, Gig0/2
13   Accounting                        active
23   Doctor                            active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20
33   Pacienty                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/21, Fa0/22
90   Management                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 3.8 – Перевірка налаштувань на комутаторі Fl1_SW2

Як ми можемо побачити на рисунку 3.8, усе працює, усі порти та налаштування відповідають заданим. Маємо 5 створених власноруч віртуальних мереж та одну за замовчуванням, на якій залишаються невикористані запасні порти.

3.7 Вибір та налаштування способу маршрутизації та доступу до Інтернет

Ефективна маршрутизація в мережі пансіонату є ключовим фактором для забезпечення надійного та безперебійного зв'язку між різними сегментами мережі. У цьому контексті протокол маршрутизації OSPF є одним із найбільш популярних і широко використовуваних рішень.

Мережа пансіонату є компактною та обмеженою за розміром, що складається з однієї будівлі та має один gateway, який з'єднує її з зовнішнім світом.

Оцінивши особливості мережі пансіонату, використовується протокол маршрутизації OSPF (Open Shortest Path First), оскільки він:

– має високу швидкість конвергенції після зміни топології мережі;

– підтримує обмін даними між маршрутизаторами в реальному часі.

При виборі та налаштуванні OSPF в мережі пансіонату необхідно

ретельно враховувати кілька важливих аспектів. По-перше, необхідно оцінити топологію мережі, кількість і розташування маршрутизаторів, а також характер трафіку, який буде передаватися в мережу. Ця інформація дозволить визначити оптимальну конфігурацію OSPF, включаючи розділення мережі на області, вибір параметрів корневого маршрутизатора та налаштування, такі як передача пакетів і пріоритети.

Використовуючи протокол OSPF, можна поширювати інформацію про мережі динамічно. При будь-яких змінах в мережі, маршрутизатори, автоматично змінять інформацію про маршрути. А також надається можливість маніпулювання маршрутами за допомогою алгоритма Дейкстри, з метою підвищення продуктивності роботи мережі.

Машрутизатор R5_Potik граничний маршрутизатор, через який забезпечується вихід до провайдера. На ньому слід назначити маршрут за-замовчуванням та розповсюдити його по OSPF.

Він задається командою ip route 0.0.0.0 0.0.0.0 g0/1. Цей інтерфейс прямує до нашого емульваного Інтернет-провайдера.

Виконаємо трасування маршруту для того, щоб упевнитись у правильних налаштуваннях мережі та в тому, що кінцеві пристрої можуть обмінюватись даними без перешкод. Також виконаємо пінгування з комп’ютера в LAN3 до ПК в межу пансіоната м. Дніпра (LAN1). Результат можемо побачити на рисунку 3.9. Отримані результати нас задовольняють, тому можна сказати, що налаштування та побудова мережі пансіонатів завершена успішно.

```
C:\>tracert 172.20.41.6

Tracing route to 172.20.41.6 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      172.20.40.1
  2    0 ms      0 ms      0 ms      10.0.13.13
  3    0 ms      0 ms      0 ms      10.0.13.5
  4    0 ms      0 ms      0 ms      172.20.41.6

Trace complete.
```

Рисунок 3.9 – Перевірка доступності LAN1 та LAN3

На рисунку 3.10 результат в режимі Simalation.

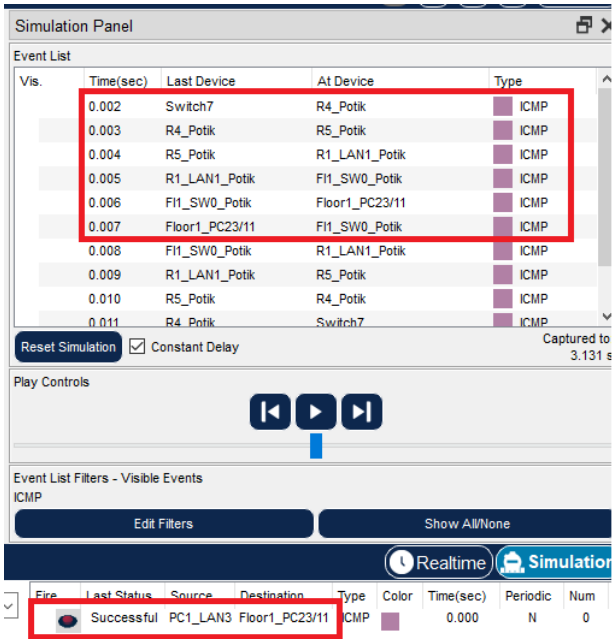
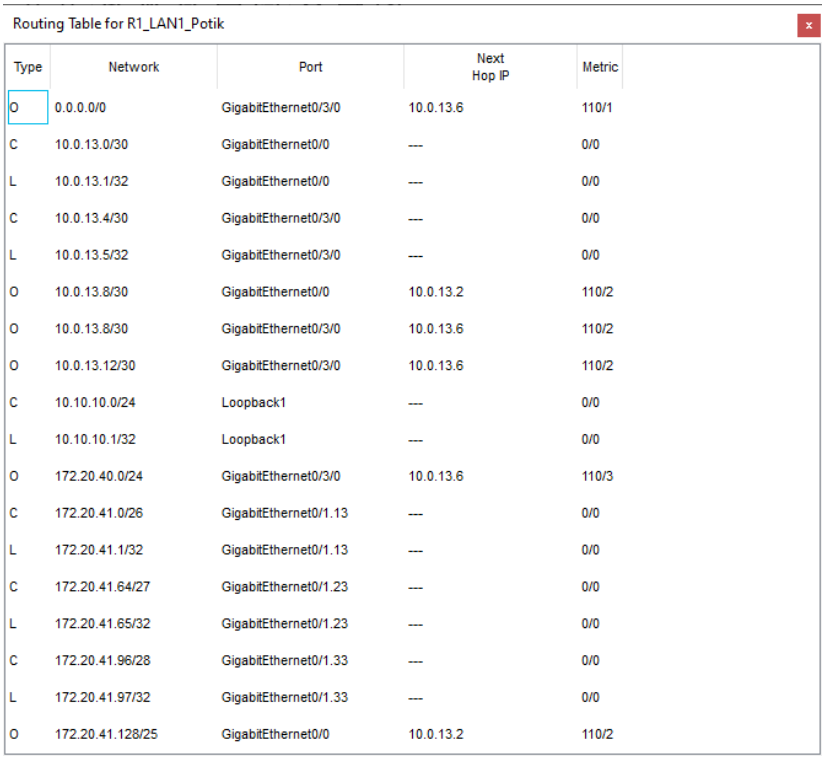


Рисунок 3.10 – Перевірка звязк в режимі Simalation

На рисунку 3.11 продемонстровано, як виглядає таблиця маршрутизації на R1_LAN1_Potik після налаштування OSPF. В таблиці літерою O розраховані маршрути до віддалених мереж.



Type	Network	Port	Next Hop IP	Metric
O	0.0.0.0/0	GigabitEthernet0/3/0	10.0.13.6	110/1
C	10.0.13.0/30	GigabitEthernet0/0	---	0/0
L	10.0.13.1/32	GigabitEthernet0/0	---	0/0
C	10.0.13.4/30	GigabitEthernet0/3/0	---	0/0
L	10.0.13.5/32	GigabitEthernet0/3/0	---	0/0
O	10.0.13.8/30	GigabitEthernet0/0	10.0.13.2	110/2
O	10.0.13.8/30	GigabitEthernet0/3/0	10.0.13.6	110/2
O	10.0.13.12/30	GigabitEthernet0/3/0	10.0.13.6	110/2
C	10.10.10.0/24	Loopback1	---	0/0
L	10.10.10.1/32	Loopback1	---	0/0
O	172.20.40.0/24	GigabitEthernet0/3/0	10.0.13.6	110/3
C	172.20.41.0/26	GigabitEthernet0/1.13	---	0/0
L	172.20.41.1/32	GigabitEthernet0/1.13	---	0/0
C	172.20.41.64/27	GigabitEthernet0/1.23	---	0/0
L	172.20.41.65/32	GigabitEthernet0/1.23	---	0/0
C	172.20.41.96/28	GigabitEthernet0/1.33	---	0/0
L	172.20.41.97/32	GigabitEthernet0/1.33	---	0/0
O	172.20.41.128/25	GigabitEthernet0/0	10.0.13.2	110/2

Рисунок 3.11 – Таблиця маршрутизації на R1_LAN1_Potik

Таким чином, можна зробити висновок, що налаштування виконано правильно.

4 НАЛАШТУВАННЯ ТЕРМІНАЛЬНОГО СЕРВЕРА

4.1 Захист інформації в комп'ютерній системі від несанкціонованого доступу

Для налагодження функціонування протоколів віддаленого доступу (зокрема, Telnet та SSH) на пристроях Cisco використовуються як деякі загальні для всіх протоколів команди, так і характерні лише для певного протоколу команди. До загальних команд належать такі команди: password, username, login, transport, autocommand, security authentication та похідні від них команди.

Команди login, password, username призначені для налагодження параметрів аутентифікації для певного мережевого підключення.

Для керування сеансами мережевих протоколів можуть використовуватися як певні комбінації клавіш (для призупинення сесії Ctrl+Shift+6), так і певні команди (повернення до сеансу – команда resume, завершення сеансу – команда disconnect).

Cisco VTY – віртуальний інтерфейс, за допомогою якого можна забезпечити віддалений доступ до пристрою. Обладнання Cisco підтримує не менше 16 одночасних підключень по віртуальному інтерфейсу. VTY – це лінія віртуального терміналу маршрутизатора, що використовується виключно для керування внутрішніми з'єднаннями Telnet, SSH та rlogin з маршрутизатором. Вони є віртуальними, функцією програмного забезпечення – немає обладнання, пов'язаного з ними. Вони відображаються в конфігураціях як vty 0 4.

Команди налагодження функціонування протоколу SSH:

– команда ip ssh authentication-retries призначена для встановлення кількості спроб аутентифікації, після якої SSH-клієнтові забороняється доступ;

– команда ip ssh time-out використовується для обмеження часу відповіді SSH-клієнта (SSH-сервер перериває з'єднання, якщо дані не передаються протягом часу очікування);

– команда ip ssh version призначена для вказування версії протоколу SSH, що буде використовуватися у процесі роботи;

– для роботи з ключами використовуються команди групи crypto key. Для генерації ключів застосовуються команди crypto key generate, crypto key generate rsa general-keys modulus.

Сценарій налагодження віддаленого підключення за протоколом SSH до маршрутизатора Cisco з використанням імені пристрою та імені домену та з використанням засобів локальної аутентифікації на базі механізму користувачів наведений на рисунку 4.1 .

```
R1_LAN1_Potik(config)#username admin privilege 15 secret cisco.
R1_LAN1_Potik(config)#enable secret class
R1_LAN1_Potik(config)#ip domain-name potik.com
R1_LAN1_Potik(config)#crypto key generate rsa
The name for the keys will be: R1_LAN1_Potik.potik.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

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

R1_LAN1_Potik(config)#ip ssh version 2
*Mar 2 1:57:53.89: %SSH-5-ENABLED: SSH 2 has been enabled
R1_LAN1_Potik(config)#ip ssh time-out 60
R1_LAN1_Potik(config)#line vty 0 4
R1_LAN1_Potik(config-line)#transport input ssh
R1 LAN1 Potik(config-line)#
```

Рисунок 4.1 – Налагодження віддаленого підключення за протоколом SSH

4.2 Налаштування роботи термінального сервера

Основна перевага термінального сервера полягає в тому, що він дає змогу отримати доступ до консольних портів багатьох пристроїв з однієї точки. Це корисно спочатку коли маршрутизатори не мають жодних параметрів конфігурації, таких як IP-адреси чи параметри Telnet. Без сервера терміналів налаштування виконувалось би через процес ручного перемикання між портами консолі кожного мережного обладнання для отримання доступу. Друга перевага полягає в тому, що термінальний сервер може забезпечити відмовостійкість у випадку, якщо маршрутизатори стають недоступними через збій мережі.

В кваліфікаційній роботі для керування мережними пристроями в

мережі LAN1 будемо застосувати граничний маршрутизатор Cisco з доданою платою HWIC-8A, яка забезпечить до восьми асинхронних підключень EIA-232 до консольних портів. Граничний маршрутизатор в LAN1 R1_LAN1_Fl1_Potik буде як сервер терміналів (рис. 4.2). Виконавши на маршрутизаторі додаткові налаштування, він таким чином буде виконувати роль термінального серверу, з якого зможемо отримати доступ до всіх інших маршрутизаторів через зворотний ssh.

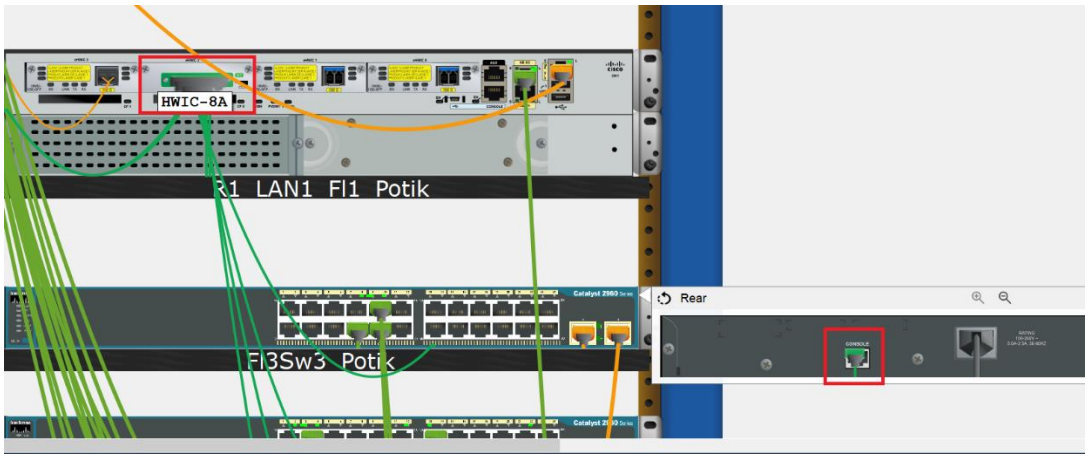


Рисунок 4.2 – Роутер Cisco 2911 з платою HWIC-8A

Встановлення підключення від маршрутизатора до одного з портів консолі називається зворотним ssh. Для цього нам потрібна IP-адреса для підключення. Ми можемо зробити це, створивши loopback-інтерфейс з IP-адресою на ньому.

Loopback адреси є кращими, оскільки вони є віртуальними і тому завжди доступні. Щоб зворотній SSH працював, інтерфейс, який використовується, має бути активним, а протокол лінії має працювати. Через це використання loopback-інтерфейсу є вигідним, оскільки він ніколи не виходить з ладу, на відміну від інтерфейсу Ethernet, який може вийти з ладу та перешкодити роботі зворотного Telnet.

Для налаштування термінального сервера необхідно виконати наступні кроки:

Крок 1. Створити loopback-інтерфейс.

Крок 2. Призначити IP-адресу інтерфейсу зворотного зв’язку.

Крок 3. Дозволити SSH як транспорт через асинхронні лінії з 1 по 16.

Крок 4. Створити таблицю хостів, яка зіставить ім'я хоста маршрутизатора (наприклад, R1, R2 і так далі) з асинхронною лінією, до якої він підключений на сервері терміналів (наприклад, 2001, 2002 і так далі).

Кроки 1 і 2: Створення інтерфейсу зворотного зв'язку та призначення IP-адреси

Створення loopback-інтерфейсу виконується в режимі глобальної конфігурації. Для виконання цієї задачі створимо інтерфейс loopback1 та призначимо йому IP-адресу 10.10.10.1/24 (рис. 4.3).

```
R1_LAN1_Potik(config)#interface loopback 1

R1_LAN1_Potik(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up

R1_LAN1_Potik(config-if)#ip add 10.10.10.1 255.255.255.0
```

Рисунок 4.3 – Створення інтерфейси зворотного зв'язку

Наш майбутній сервер терміналів постачається з деякими line, які посилаються на порти, які він має. Командою show line можна отримати відомості про них, щоб побачити, які номери рядків вона використовує (рис. 4.4). В даному випадку номери це 67-74.

```
R1_LAN1_Potik#show line
   Tty Line Typ     Tx/Rx    A Roty AccO AccI   Uses   Noise  Overruns   Int
*    0    0 CTY              -    -    -    -      0       0     0/0       -
     1    1 AUX    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/0   67 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/1   68 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/2   69 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/3   70 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/4   71 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/5   72 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/6   73 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/7   74 TTY    9600/9600 -    -    -    -      0       0     0/0       -
   388  388 VTY              -    -    -    -      0       0     0/0       -
   389  389 VTY              -    -    -    -      0       0     0/0       -
   390  390 VTY              -    -    -    -      0       0     0/0       -
   391  391 VTY              -    -    -    -      0       0     0/0       -
   392  392 VTY              -    -    -    -      0       0     0/0       -
Line(s) not in async mode -or- with no hardware support:
3-66, 75-387
R1_LAN1_Potik#
```

Рисунок 4.4 – Результат команди show line

Граничний маршрутизатор в LAN1 R1_LAN1_Potik буде як сервер терміналів. Сервер терміналів підключається до консольного порту кожного

пристрою через модуль HWIC-8A та кабель CAB-HD8-ASYNC. Даний модель забезпечує до 8 підключень. Призначення портів є такими (рис. 4.5):

– Fl1Sw0 – 67;

– Fl1Sw1 – 68;

– Fl2Sw0 – 69;

– Fl2Sw1 – 70;

– Fl3Sw0 – 71;

– Fl3Sw1 – 72;

– Fl3Sw2 – 73;

– Fl3Sw3 – 74.

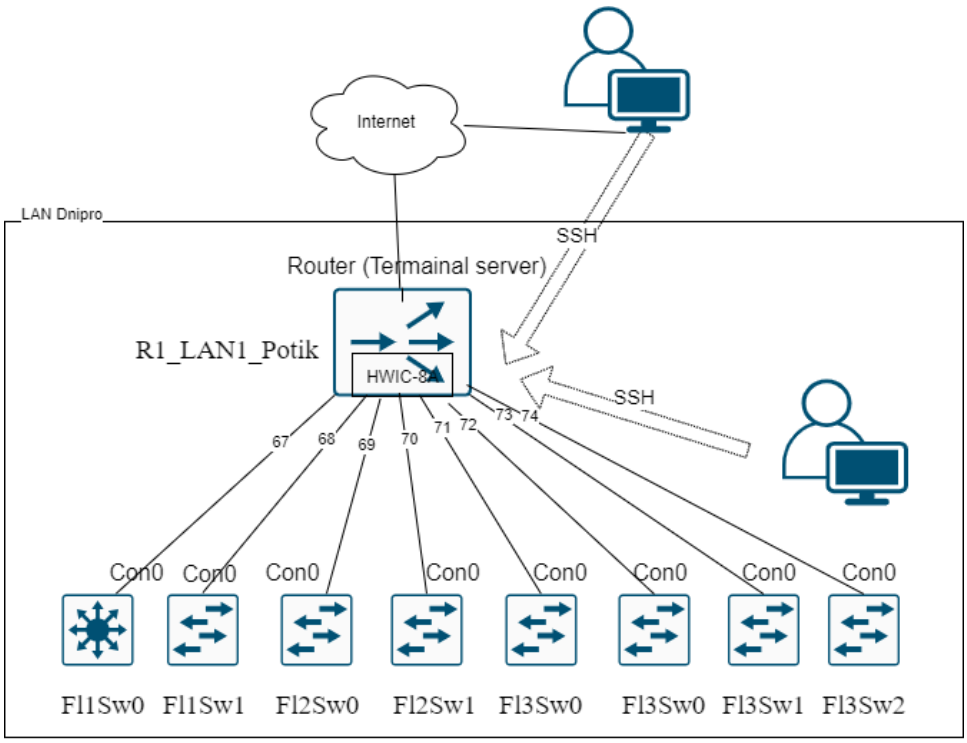


Рисунок 4.5 – Підключення термінального сервера

Крок 3: Дозвіл SSH через асинхронні лінії

Тепер, коли інтерфейс loopback 1 створено, потрібно переконатися, що асинхронні лінії дозволяють SSH-з'єднання.

Це робиться за допомогою команди transport input x, де x — це протокол, який потрібно дозволити, наприклад SSH. Команда дозволяє деталізувати лише певні протоколи для перетину асинхронних ліній (рис 4.6).

```
R1_LAN1_Potik(config)#line 0/2/0 0/2/7
R1_LAN1_Potik(config-line)#transport input ssh
R1_LAN1_Potik(config-line)#login local
```

Рисунок 4.6 – Дозвіл SSH як транспорту через асинхронні лінії

Крок 4. Створення таблиці хостів, яка відображає ім'я хоста маршрутизатора на асинхронну лінію, до якої він підключений на сервері терміналів

На цьому етапі сервер терміналів налаштований і повинен працювати; однак, щоб заощадити час, краще створите таблицю хостів, яка зіставляє ім'я маршрутизатора з інтерфейсом loopback 1, а потім буда вказано асинхронний порт, з якого ініціюватиме зворотній сеанс SSH. Це робиться за допомогою команди ip host . Команда ip host – це статичний запис DNS, який використовується маршрутизатором. Маршрутизатор перетворить «Fl1Sw0 » на порт 10.10.10.1:67. Після заповнення таблиці хостів ми отримаємо доступ до кожного пристрою, ввівши його ім'я. Наприклад, введення *Fl1Sw0* ініціює зворотний сеанс SSH з асинхронного рядка 2067 (67). На рис. 4.7 наведено створення таблиці хостів.

```
R1_LAN1_Potik(config)#ip host Fl1Sw0 2067 10.10.10.1
R1_LAN1_Potik(config)#ip host Fl1Sw1 2068 10.10.10.1
R1_LAN1_Potik(config)#ip host Fl2Sw0 2069 10.10.10.1
R1_LAN1_Potik(config)#ip host Fl2Sw1 2070 10.10.10.1
R1_LAN1_Potik(config)#ip host Fl3Sw0 2071 10.10.10.1
R1_LAN1_Potik(config)#ip host Fl3Sw1 2072 10.10.10.1
R1_LAN1_Potik(config)#ip host Fl3Sw2 2073 10.10.10.1
R1_LAN1_Potik(config)#ip host Fl3Sw3 2074 10.10.10.1
```

Рисунок 4.7 – Створення таблиці хостів

4.3 Тестування роботи термінального сервера

На будь-якому ПК в мережі пансіонату з командного рядка підключимся по SSH до комутатора Fl1Sw1 через IP-адресу термінального сервера і перевіримо зворотну функціональність SSH (рис.4.8).

```
C:\>ssh -l admin:67 10.10.10.1

Password:

Router of Hospital Dnipro (Potik)
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with
21039K bytes of memory.
2960-24TT starting...

Fl1_SW0_Potik>
```

Рисунок 4.8 – Підключення з ПК до комутатора Fl1Sw1 через TS

З рисунку можна побачити, що термінальний сервер ініціює підключення до роутера R1_LAN1_Potik. Це робиться шляхом підключення до адреси loopback1 10.10.10.1 (через SSH), а потім перенаправлення з'єднання з асинхронного порту 67. Оскільки з'єднання SSH є «переспрямованим», воно називається зворотним з'єднанням SSH. Потім натиснувши клавішу Enter бачимо підказку **Fl1_SW0_Potik>** .

Замість того, щоб вводити ці команди, ми можемо використовувати створену таблицю хостів. В режимі глобальної конфігурації перевіримо зворотну функціональність SSH, ввівши «Fl1Sw1» у режимі користувача EXEC або привілейованому режимі EXEC (рис. 4.9).

```
R1_LAN1_Potik#Fl1Sw1
Trying 10.10.10.1 ...OpenRouter of Hospital Dnipro (Potik)^

User Access Verification

Username:
```

Рисунок 4.9 – Підключення до комутатора Fl1Sw1 через термінальний сервер

Ми бачимо, це підключення працює, на ньому написано «OpenRouter», що означає підключення. Ми бачимо бачити консоль пристрою, до якого зараз підключено.

Командою show line при отримані відомостей про них, можна побачити, які номери рядків використовувались, вони позначені * та в стовбці Uses загальна кількість підключень (рис. 4.10).

```
R1_LAN1_Potik#show line
    Tty Line Typ     Tx/Rx    A Roty AccO AccI   Uses   Noise  Overruns   Int
*     0    0 CTY              -    -    -    -      0       0     0/0       -
      1    1 AUX    9600/9600 -    -    -    -      0       0     0/0       -
*0/2/0   67 TTY    9600/9600 -    -    -    -      1       0     0/0       -
*0/2/1   68 TTY    9600/9600 -    -    -    -      3       0     0/0       -
 0/2/2   69 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/3   70 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/4   71 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/5   72 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/6   73 TTY    9600/9600 -    -    -    -      0       0     0/0       -
 0/2/7   74 TTY    9600/9600 -    -    -    -      0       0     0/0       -
```

Рисунок 4.10 – Результат команди show line

Щоб повернутися до свого термінального сервера, потрібно натиснути , **CTRL+SHIFT+6** а потім **X**. Це не розриває з’єднання, але залишає його у фоновому режимі. Якщо необхідно розірвати його, доведеться скористатися командою clear line (рис.4.11):

```
R1_LAN1_Potik#clear line tty 68
[confirm]
 [OK]
R1_LAN1_Potik#
```

Рисунок 4.11 – Розірвання з’єднання

Щоб термінальний сервер був доступний звідусіль, слід надати йому зареєстрований загальнодоступний Інтернет-адресу та розмістити його за межами брандмауера, щоб проблеми з брандмауером не переривали з’єднання. Це гарантує, що завжди можна буде підтримувати зв'язок із сервером терміналів і мати доступ до підключених пристроїв. Якщо турбує додаткова безпека, слід налаштувати списки доступу, щоб дозволити доступ лише до серверу терміналів з певних адрес.

ВИСНОВКИ

У ході цієї роботи детально розглянуто комп'ютерну систему комунального закладу "Дніпропетровський геріатричний пансіонат" з фокусом налаштування безпечного віддаленого доступу до мережних пристроїв через термінальний сервер.

В результаті аналізу було встановлено, що впровадження комп'ютерної системи в геріатричному пансіонаті є критично важливим для забезпечення якісної медичної допомоги та догляду за пацієнтами. Враховуючи специфіку роботи закладу та потреби у захисті конфіденційності медичної інформації, було розроблено та налаштовано систему віддаленого доступу через термінальний сервер.

Застосування термінального сервера дозволило забезпечити безпечний віддалений доступ до мережних пристроїв для медичного персоналу та адміністративного персоналу пансіонату. Завдяки цьому, лікарі та інші фахівці можуть отримувати доступ до необхідної медичної інформації з будь-якого місця та в будь-який час, що сприяє підвищенню ефективності та якості надання медичних послуг.

Однак, для успішного функціонування комп'ютерної системи необхідно постійно вдосконалювати заходи забезпечення безпеки, включаючи захист від кібератак, забезпечення конфіденційності даних та забезпечення відмовостійкості. Також важливо забезпечити систему надійними засобами резервного копіювання та відновлення даних, щоб запобігти втраті інформації у випадку непередбачених ситуацій.

Комп'ютерна мережа була розроблена відповідно до завдань, поставлених для кваліфікаційної роботи бакалавра

СПИСОК ДЖЕРЕЛ ПОСИЛАННЯ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2023. – 62 с.
2. Про затвердження Типового положення про будинок-інтернат для громадян похилого віку та осіб з інвалідністю. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/772-2020-п#Text (дата звернення: 19.05.2024).
3. Дніпропетровський геріатричний пансіонат | Відгуки, ціни, адреса. *Будинки престарілих*. URL: https://doma-prestarelyh.com.ua/dnipropetrovskyj-geriatrychnyj-pansionat/ (дата звернення: 19.05.2024).
4. What is SSH? - ClouDNS Blog. *ClouDNS Blog*. URL: https://www.cloudns.net/blog/what-is-ssh/ (date of access: 02.06.2024).
5. Вступ до мереж версії 7.0 (ITN). Курс Cisco. URL: https://lms.netacad.com/course/view.php?id=2163011 (date of access: 19.05.2024).
6. Маршрутизатор Cisco 2911 (CISCO2911/K9). *stack-systems.com.ua - Мережеве обладнання*. URL: https://stack-systems.com.ua/marshrutizator-cisco-2911-k9 (дата звернення: 19.05.2024).
7. Комутоарор Cisco 2960 (Cisco WS-C2960-24LT-L). *stack-systems.com.ua - Мережеве обладнання*. URL: https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24lt-l (дата звернення: 19.05.2024).
8. How to Configure a Cisco Router as a Terminal Server - Petri IT Knowledgebase. *Petri IT Knowledgebase*. URL: https://petri.com/how-to-configure-cisco-router-as-terminal-server/ (date of access: 19.05.2024).
9. Configuring the Terminal Server > CCNA Practical Studies: Gaining Access to Routers and Switches | Cisco Press. *Cisco Press: Source for Cisco Technology, CCNA, CCNP, CCIE Self-Study | Cisco Press*. URL: https://www.ciscopress.com/articles/article.asp?p=27650&seqNum=5

(date of access: 19.05.2024).

10. ДСТУ 3008-2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – К.: Держстандарт, 2015. – 37с.

11. Положення про організацію атестації здобувачів вищої освіти НТУ «Дніпровська політехніка» / М-во освіти і науки України, Нац. техн. ун-т. – Д. : НТУ «ДП», 2018. – 40 с 3

12. ДСТУ ГОСТ 7.1:2006. Бібліографічний запис, бібліографічний опис. Загальні вимоги та правила складання: метод. рекомендації з впровадження / Уклали: Галевич О. К., Штогрин І. М. – Львів, 2008. – 20 с.

Додаток А

Текст програми налаштування термінального сервера

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ ТЕРМІНАЛЬНОГО СЕРВЕРА

Текст програми

804.02070743.24013-01 12 01

Листів 4

2024

АНОТАЦІЯ

Дана програма містить розділ конфігураційного файлу з налаштуваннями SSH, параметри домену, записи статичних хостів для різних комутаторів і налаштовується лінійний інтерфейс для можливих з’єднань.

ЗМІСТ

1. config_ts.txt

// ip ssh версії 2`: ця команда вказує, що маршрутизатор повинен використовувати SSH версії 2 для безпечного зв'язку.

//ip ssh time-out 60`: встановлює час очікування SSH на 60 секунд, що означає, що якщо протягом 60 секунд не буде активності, сеанс SSH буде припинено.

```
ip ssh version 2
ip ssh time-out 60
no ip domain-lookup
ip domain-name potik.com
```

// Команди `ip host` налаштовують записи статичних хостів для різних комутаторів Fl із відповідними IP-адресами петлі. Наприклад, «ip host Fl1Sw0 2067 10.10.10.1» встановлює для імені хоста «Fl1Sw0» IP-адресу «10.10.10.1» і вказує порт «2067».

```
ip host Fl1Sw0 2067 10.10.10.1
ip host Fl1Sw1 2068 10.10.10.1
ip host Fl2Sw0 2069 10.10.10.1
ip host Fl2Sw1 2070 10.10.10.1
ip host Fl3Sw0 2071 10.10.10.1
ip host Fl3Sw1 2072 10.10.10.1
ip host Fl3Sw2 2073 10.10.10.1
ip host Fl3Sw3 2074 10.10.10.1
!
```

//`line 0/2/0 0/2/7`: Ця команда вказує конфігурацію інтерфейсу лінії від 0/2/0 до 0/2/7.

//`transport input all`: вказує, що для транспортування можна використовувати всі протоколи.

```
line 0/2/0 0/2/7
 transport input all
 login local
```

Додаток Б

Текст програми налаштування граничного маршрутизатора КЗ ДГП

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ ГРАНИЧНОГО МАРШРУТИЗАТОРА КЗ ДГП

Текст програми

804.02070743.24013-01 12 01

Листів 5

2024

АННОТАЦІЯ

Код є конфігурацією Cisco граничного маршрутизатора в мережі пансіонату КЗ ДГП, який називається "R1_LAN1_Potik". Файл конфігурації визначає ім’я хоста маршрутизатора, увімкнути секрет, пули DHCP, конфігурації інтерфейсу, конфігурацію маршрутизації, VLAN та інші налаштування.

```
Current configuration : 2856 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1_LAN1_Potik
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 172.20.40.1 172.20.40.10
ip dhcp excluded-address 172.20.40.129
ip dhcp excluded-address 172.20.40.161 172.20.40.162
ip dhcp excluded-address 172.20.41.1 172.20.41.5
ip dhcp excluded-address 172.20.41.65 172.20.41.66
ip dhcp excluded-address 172.20.41.97
ip dhcp excluded-address 172.20.41.113
!
ip dhcp pool pool_VLAN13
 network 172.20.41.0 255.255.255.192
 default-router 172.20.41.1
 dns-server 172.20.41.10
ip dhcp pool pool_VLAN23
 network 172.20.41.64 255.255.255.224
 default-router 172.20.41.65
 dns-server 172.20.41.10
ip dhcp pool pool_VLAN33
 network 172.20.41.96 255.255.255.240
 default-router 172.20.41.97
 dns-server 172.20.41.10
ip dhcp pool pool_VLAN43
 network 172.20.41.112 255.255.255.248
 default-router 172.20.41.113
 dns-server 172.20.41.10
!
!
!
no ip cef
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
```

```
!
!
license udi pid CISCO2911/K9 sn FTX1524AV9S-
!
!
spanning-tree mode pvst
!
interface Loopback1
 ip address 10.10.10.1 255.255.255.0
!
interface GigabitEthernet0/0
 ip address 10.0.13.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.13
 encapsulation dot1Q 13
 ip address 172.20.41.1 255.255.255.192
!
interface GigabitEthernet0/1.23
 encapsulation dot1Q 23
 ip address 172.20.41.65 255.255.255.224
!
interface GigabitEthernet0/1.33
 encapsulation dot1Q 33
 ip address 172.20.41.97 255.255.255.240
!
interface GigabitEthernet0/1.90
 encapsulation dot1Q 90
 no ip address
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/0/0
 no ip address
!
interface GigabitEthernet0/1/0
 no ip address
!
interface GigabitEthernet0/3/0
```

```
 ip address 10.0.13.5 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 13
 log-adjacency-changes
 network 10.0.13.0 0.0.0.3 area 0
 network 10.0.13.4 0.0.0.3 area 0
 network 172.20.41.0 0.0.0.127 area 0
!
ip classless
!
ip flow-export version 9
!
!
no cdp run
!
banner motd ^CRouter of Hospital Dnipro (Potik)^C
!
!
line con 0
 password 7 0822455D0A16
 login
!
line aux 0
!

line vty 0 4
 login local
 transport input ssh
!
!
!
end
```