

РЕФЕРАТ

Пояснювальна записка: 61 с., 26 рис., 6 табл., 2 додатки, 9 джерел.

КОМП'ЮТЕРНА СИСТЕМА, МАРШРУТИЗАТОР, КОРПОРАТИВНА МЕРЕЖА, SNMP, ICMP, MIB, CISCO PACKET TRACER.

Об'єктом розробки є комп'ютерна система для геймінг-кафе «Joy-стік».

Мета роботи полягає в розробці та побудові мережевої інфраструктури, що відповідає вимогам компанії до забезпечення високої пропускної здатності мережі, безпеки передачі даних, можливості моніторингу стану мережевого обладнання та готовності мережі до інтегрування різнотипних кінцевих пристроїв, таких як комп'ютери та різноманітне відеоігрове приладдя.

Було здійснено розробку мережі на базі детального аналізу вимог, побудову її моделі та проведено тестування. Дослідження проводилось із врахуванням сучасних практик у побудові мережевих інфраструктур та з використанням програмного забезпечення для моделювання роботи мережевих пристроїв. Випробування мережі свідчать про її високу продуктивність та відповідність вимогам сучасності.

Можливо проведення модернізації розробленої комп'ютерної системи шляхом масштабування мережі та впровадження більшої кількості засобів забезпечення безпеки.

Результат роботи може бути задіяним у багатьох інших видах закладів, які будуть зацікавлені у впровадженні мережі для надання клієнтам послуг у вигляді доступу до мережі інтернет, або комп'ютерного обладнання.

ЗМІСТ

Перелік скорочень, умовних познач, одиниць і термінів	6
Вступ.....	7
1 Стан питання і постановка завдання.....	8
1.1 Стисла характеристика сфери та умов застосування комп'ютерної системи.....	8
1.2 Характеристика та організаційна структура ГК JS.....	9
1.3 Стислі відомості про топологічне розміщення структурних підрозділів ГК JS	12
1.4 Особливості та проблеми функціонування комп'ютерної мережі ГК JS	14
1.5 Визначення можливих напрямків рішення завдання з моніторингу та керування мережею в ГК JS	15
1.6 Обґрунтування вибраного напрямку інженерного рішення	17
1.7 Завдання і мета роботи	17
2 Розробка апаратної частини комп'ютерної системи.....	19
2.1 Технічні вимоги до комп'ютерної системи ГК JS.....	19
2.1.1 Вимоги до системи в цілому.....	19
2.1.1.1 Вимоги до структури і функціонуванню системи	19
2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики.....	19
2.1.1.1.2 Вимоги до способів і засобів зв'язку між компонентами комп'ютерної системи	20
2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної системи із суміжними системами.....	20
2.1.1.1.4 Вимоги до режимів функціонування системи	20
2.1.1.1.5 Вимоги до діагностування системи	21
2.1.1.1.6 Перспективи розвитку, модернізації системи	21
2.1.1.2 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему, і режиму його роботи.	22

2.1.1.3	Вимоги щодо надійності	23
2.1.1.4	Вимоги до показників призначення	23
2.1.1.5	Вимоги до патентної чистоти	24
2.1.1.6	Додаткові вимоги	24
2.1.2	Вимоги до видів забезпечення КС.....	24
2.1.2.1	Вимоги до технічного забезпечення	24
2.1.2.2	Вимоги до програмного забезпечення	24
2.1.2.3	Вимоги до інформаційного забезпечення.....	25
2.1.2.4	Вимоги до лінгвістичного забезпечення	25
2.2	Розробка апаратної частини комп'ютерної системи.....	25
2.2.3	Розробка структурної схеми мережі.....	25
2.2.4	Розробка специфікації апаратних засобів КС.....	27
2.2.5	Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства	31
3	Розробка корпоративної мережі.....	33
3.1	Розрахунок схеми адресації корпоративної мережі.....	33
3.2	Розробка моделі мережі в Packet Tracer	36
3.3	Вибір та налаштування способу маршрутизації та доступу до Інтернет	38
3.4	Налаштування мереж VLAN, маршрутизації між VLAN	40
3.5	Захист від несанкціонованого доступу	43
4	Налаштування протоколу snmp.....	44
4.1	Архітектура та функції протоколу SNMP.....	44
4.2	Management Information Base	47
4.3	Налаштування протоколу SNMP на мережевих пристроях.....	49
4.4	Тестування роботи протоколу SNMP	50
	Висновки	53
	Перелік посилань.....	54

**ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І
ТЕРМІНІВ**

ГК JS	геймінг-кафе Joy-стік
ГК	геймінг-кафе
КМ	комп'ютерна мережа
КС	комп'ютерна система
SNMP	простий протокол керування мережею (англ. Simple Network Management Protocol)
MIB	Management Information Base
OSPF	Open Shortest Path First – відкритий протокол пошуку найкоротшого шляху
RFC	Request for Comments – запит коментарів

ВСТУП

Розвиток в сфері інтернет-геймінгу став одним із найбільш швидкозростаючих і перспективних напрямків індустрії розваг. З кожним днем кількість гравців, які обирають віртуальні світи для відпочинку та розваг, постійно зростає. У такому контексті важливо правильно підібрати та впровадити систему моніторингу та керування мережею в інтернет-геймінг кафе.

Ця робота присвячена дослідженню призначення спеціалістів-системних адміністраторів в умовах сьогодення, коли комп'ютерні мережі сягають надзвичайно великих масштабів у всіх сферах функціонування сучасного світу. В якості прикладу, в цій роботі розглядається функціонал і призначення комп'ютерних мереж у корпоративному середовищі, та які завдання стоять перед системними адміністраторами в таких умовах.

Також в роботі детально розглянуті деякі засоби системного адміністрування, та для чого вони призначені разом із принципом їх функціонування. Було створено модель корпоративної мережі, для якої було проведено детальне налаштування, разом із впровадженням засобів системної адміністрації розглянутих у роботі.

Було проведено практичне дослідження та випробування роботи протоколів мережі інтернет які були розроблені для моніторингу, налаштування, та загального адміністрування компонентів сучасних комп'ютерних мереж, як і для загального використання, так і для потреб корпорацій та бізнесу.

Ця робота виділяє ключові елементи функцій що виконують спеціалісти системного адміністрування телекомунікаційних мереж у цьому полі, зокрема визначаючи які саме цілі та завдання розвитку цієї галузі диктує як сучасне корпоративне середовище, так і розвиток загальних комп'ютерних мереж у світі в цілому.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика сфери та умов застосування комп'ютерної системи

Інтернет-кафе, або кібер-кафе – це кафе, яке надає клієнтам доступ до комп'ютерів із швидкісним доступом до мережі інтернет на основі погодинної оплати. Зазвичай такі установи також пропонують різні напої та закуски, як звичайні кафе. З поширенням мобільного доступу до інтернету та персональних комп'ютерів, у розвинених країнах популярність таких закладів почала падати, залишаючись популярними лише серед мандрівників та туристів. В країнах що розвиваються, це популярний спосіб отримати до інтернету заради серфінгу або дзвінків.

Для того щоб привабити більше клієнтів, багато інтернет-кафе почали надавати не лише доступ до мережі інтернет, а й до потужних персональних комп'ютерів зокрема для геймінгу, такого рівня який не кожна людина може дозволити собі придбати. Такі заклади почали називатись геймінг-кафе, або інтернет геймінг-кафе, але в Україні вони більш відомі під назвою комп'ютерні клуби.

В геймінг-кафе можна отримати доступ не лише до потужних ігрових персональних комп'ютерів, а й до ігрових консолей та обладнаних зон з шоломами віртуальної реальності. Деякі кафе проводять внутрішні любительські турніри по кіберспорту із врученням призів та промокодів.

Сучасні інтернет-геймінг кафе повинні забезпечувати надійну та швидку мережеву інфраструктуру для забезпечення зручності та комфорту клієнтів.

Однією з ключових складових успіху інтернет-геймінг кафе є надійна робота комп'ютерної системи, яка повинна забезпечувати стабільну роботу мережі та моніторинг її компонентів.

Розробка підсистема моніторингу та керування дозволить адміністратору віддалено моніторити та керувати мережею. Це дозволить адміністраторам виявляти проблеми в мережі та швидко реагувати на них, що

зменшує ризики простою мережі та негативного впливу на роботу кафе. Очікується, що така система моніторингу та керування мережею буде ефективною для інших інтернет-геймінг кафе в Україні.

1.2 Характеристика та організаційна структура ГК JS

Інтернет-геймінг кафе Joy-стік (ГК JS) – це сучасний заклад, орієнтований на любителів онлайн відеоігор та кіберспорту. Головним завданням закладу є надання клієнтам високоякісного середовища для геймінгу, соціалізації та участі в кіберспортивних заходах. Основними характеристиками та послугами кафе є:

- ігрові зони кафе Joy-стік обладнані сучасними ігровими комп'ютерами з потужними процесорами і відеокартами, та швидкісним підключенням до інтернету, що дає змогу відвідувачам насолоджуватись великою бібліотекою сучасних відеоігор з відмінним ігровим досвідом;

- окрім настільних комп'ютерів, кафе пропонує також ігрові консолі як останнього покоління, так і ретро консолі, що дає гравцям доступ до ексклюзивних ігор сьогодення та минулих років на автентичному обладнанні;

- Joy-стік є майданчиком для проведення кіберспортивних турнірів від спонсорів та кіберспортивних компаній, забезпечуючи професійне суддівство та призові фонди;

- кафе має комфортні місця для сидіння, ергономічні крісла, просторі ігрові стійки а також окремі VIP-кімнати для приватних ігор або групових заходів;

- облаштований соціальний простір де геймери можуть спілкуватися, обмінюватися досвідом та знаходити нових друзів;

- меню кафе включає в себе широкий вибір напоїв таких як кава, чай, енергетичні напої а також легкі закуски та десерти, що дозволяє гравцям перекусити під час гри;

- персонал кафе – це досвідчені геймери, які можуть допомогти з налаштуванням обладнання, порадити цікаві ігри або надати технічну

підтримку;

– для постійних клієнтів Joy-стік існують членські програми з привілеями, такими як знижки на час гри, спеціальні заходи та дочасний доступ до нових ігор.

В таких умовах комп'ютерна систем кафе має бути готовою до підтримки великої кількості одночасних користувачів та підтримання якісної роботи усіх компонентів.

Організаційна структура кафе побудована таким чином, щоб забезпечити ефективну роботу персоналу, задоволення потреб клієнтів та збереження високого рівня сервісу. Схематично корпоративну структуру інтернет-геймінг кафе Joy-стік наведено на рисунку 1.1.



Рисунок 1.1 – Організаційна структура геймінг-кафе

Управління:

– директор (1 особа): відповідає за стратегічне планування;

Відділ маркетингу: –

– менеджери (2 особи): відповідають за просування геймінг-кафе на ринку, пошуку нових клієнтів, утримання лояльності та управління соціальними мережами.

Відділ обслуговування клієнтів:

– адміністратор (2 особи): відповідає за загальне управління закладом, планування та контроль роботи персоналу, взаємодію з постачальниками, контроль фінансових потоків та ведення документації;

– кухар (1 особа): готує страви для клієнтів;

– офіціант (2 особи): обслуговує клієнтів, приймає замовлення, подає страви та напої, розраховує клієнтів.

– бармен (2 особи): готує напої, контролює наявність алкоголю та безалкогольних напоїв, забезпечує підтримання чистоти в барній зоні.

Відділ технічного обслуговування:

– системний адміністратор (1 особа): відповідає за технічне обслуговування комп'ютерів та мережі, налагодження та підтримку програмного забезпечення, забезпечення безперебійної роботи ігрових станцій;

– технік (1 особа): здійснює дрібний ремонт комп'ютерної техніки, надає технічну підтримку користувачам, займається підключенням та налаштуванням периферійних пристроїв, підтримку програмного забезпечення.

Загалом в геймінг-кафе працює 12 осіб, включаючи керівництво, менеджерів, адміністраторів, офіціантів, барменів та техніків.

Кількість клієнтів, які можуть одночасно перебувати в кафе, становить 50 осіб. Для них надається 30 комп'ютерів, обладнаних усіма необхідними для геймінгу програмами та пристроями.

Ефективна організація роботи геймінг кафе Joy-стік забезпечується завдяки розділенню на функціональні підрозділи, кожен з яких відповідає за свою певну функцію. Це дозволяє впевнено керувати всіма аспектами роботи кафе, забезпечити якісне обслуговування клієнтів та досягти успіху в своїй галузі.

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

Таблиця 1.1 – Комп'ютеризовані робочі місця підприємства

Структурний підрозділ	Кількість		
	Користувачі	ПК	Принтери
Управління	1	1	1
Відділ маркетингу	2	2	1

Відділ обслуговування клієнтів	7	1	-
Відділ технічної підтримки + сервер	2	3	1
Робочі місця для клієнтів	50	30	
Загалом ПК		37	3

1.3 Стислі відомості про топологічне розміщення структурних підрозділів ГК JS

Кафе знаходиться м. Житомир, Житомирська область, 10002, вулиця Приміщення кафе розділено на чотири зони: зону адміністративного відділу, зону обслуговування клієнтів, зону технічного забезпечення та зону кухні та бару. Загальна площа геймінг-кафе: 350 м².

Топологічне розміщення підрозділів організаційної структури у будівлі організовано наступним чином (рис. 1.2):

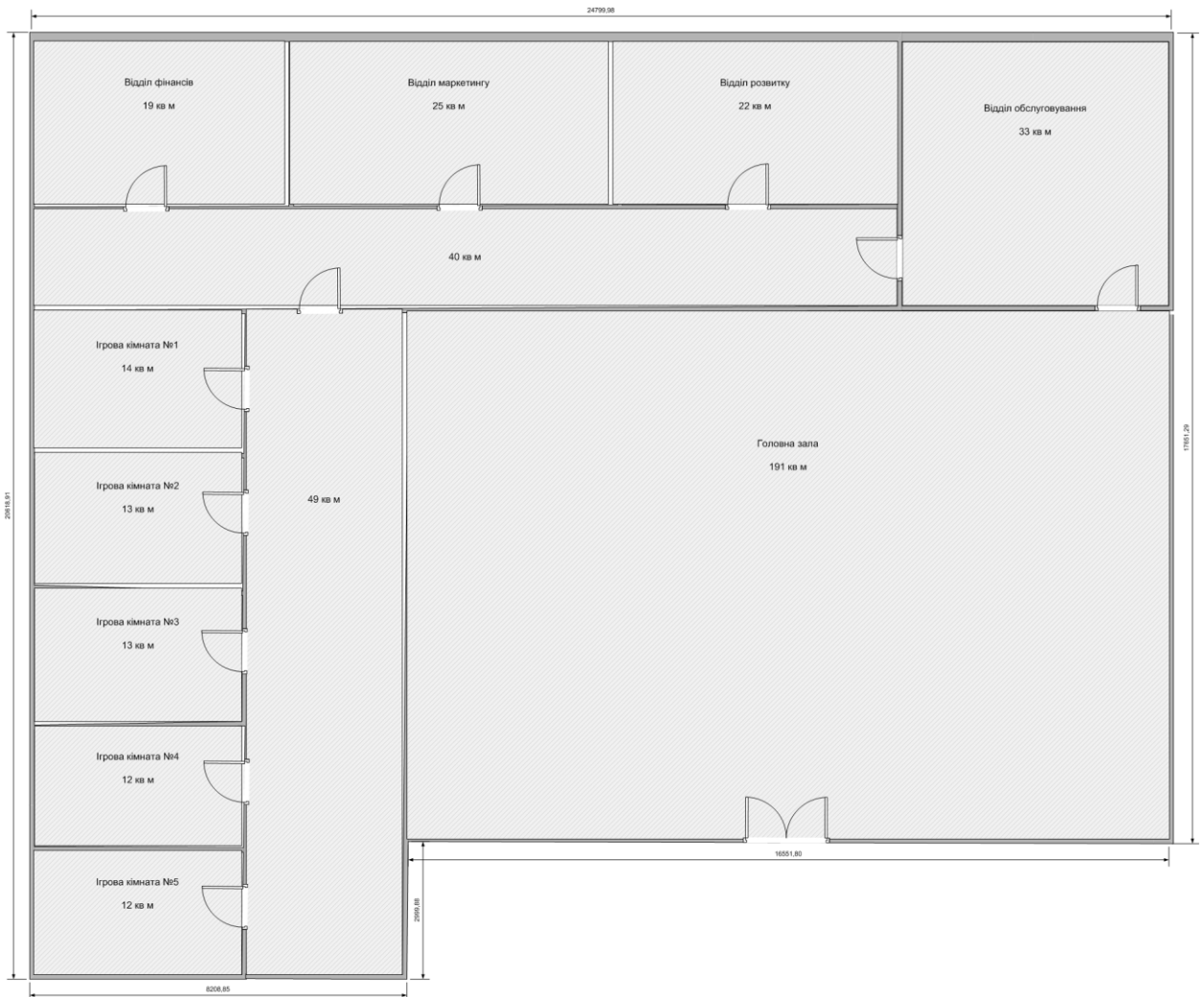


Рисунок 1.2 – План першого поверху закладу

- РС-зона: розташована в центрі будівлі, займає більшу частину площі. Містить 20 сучасних ігрових комп'ютерів з високопродуктивними комплектуючими та ергономічними ігровими кріслами;
- консольна зона: з комфортабельними диванами та великими телевізорами для любителів консольних ігор;
- бар: розташований поруч з ігровим залом, з легким доступом для клієнтів та забезпечує обслуговування напоями та закусками;
- адміністраторська: розміщена в окремому кабінеті, що дозволяє адміністратору вести документацію та контролювати роботу персоналу;
- технічне приміщення: для розміщення серверного обладнання, комунікацій та інженерних систем.
- VIP-зона: обладнана комфортабельними ігровими станціями, забезпечує приватність та комфорт для VIP-клієнтів;

- окремі зони відпочинку: з диванами, телевізором та можливістю замовити кальян;
- кімната для трансляцій: оснащена великим екраном, проектором та зручними місцями для перегляду ігрових трансляцій.

1.4 Особливості та проблеми функціонування комп'ютерної мережі ГК JS

Комп'ютерні ігрові кафе стали популярними місцями для геймерів, які хочуть зіграти у свої улюблені ігри з друзями або спільнотою. Проте, призвести така популярність також до ряду особливостей та проблем у функціонуванні комп'ютерної мережі в геймінг-кафе.

Особливості функціонування комп'ютерної мережі ГК JS.

а) Інтенсивний трафік:

- геймінг-кафе потребує високошвидкісного інтернет-з'єднання для забезпечення безперервної гри;
- високий обсяг даних, що передається, вимагає ефективного управління трафіком.

б) Безпека мережі:

- необхідність захисту від кібератак та шкідливого програмного забезпечення;
- забезпечення конфіденційності даних користувачів.

в) Різноманітність підключених пристроїв:

- велика кількість ігрових комп'ютерів та іншого обладнання вимагає надійної інфраструктури.

г) Постійний моніторинг і управління:

- використання програмного забезпечення для відслідковування стану мережі та управління пристроями;
- збір статистики про використання ресурсів мережі кожним користувачем.

Однією з основних проблем функціонування комп'ютерної мережі

геймінг-кафе є недостатня пропускна здатність, особливо у години пік, коли кафе заповнені гравцями. Це може спричинити зависання гри або низьку швидкість Інтернету, що негативно впливає на геймплей.

Ще однією проблемою є забрудненість та перегрів комп'ютерного обладнання через постійне його використання. Це може призвести до зниження продуктивності обладнання та витрат на його обслуговування.

Третью проблемою є необхідність моніторингу працездатності мережного обладнання та геймерських ПК з метою вчасного ремонту та інформування про збої та неполадки.

Важливо вирішувати ці проблеми для забезпечення ефективного функціонування закладу.

1.5 Визначення можливих напрямків рішення завдання з моніторингу та керування мережею в ГК JS

Для ефективного функціонування геймінг-кафе необхідно забезпечити високу швидкість та стабільність інтернет-з'єднання, надійний захист від кібератак, управління мережевими ресурсами та постійний моніторинг стану мережі.

Розглянемо можливі напрями рішення з управління мережевими ресурсами та постійного моніторингу стану мережі для ГК JS.

Першим можливим напрямком розв'язання цього завдання може бути створення програмного забезпечення, яке дозволить моніторити та керувати всіма аспектами мережі кафе. Це може включати в себе контроль швидкості інтернет-з'єднання, обмеження доступу до певних веб-сайтів або онлайн-ігор, а також ведення статистики щодо використання ресурсів мережі кожним з користувачів.

Переваги:

- контроль швидкості інтернет-з'єднання, обмеження доступу до певних веб-сайтів або онлайн-ігор;

- ведення статистики щодо використання ресурсів мережі кожним з

користувачів.

Недоліки:

– необхідність розробки або налаштування спеціалізованого програмного забезпечення.

– можливі витрати на підтримку та оновлення ПЗ.

Другим можливим напрямком є встановлення спеціалізованого обладнання для моніторингу мережі та керування нею. Наприклад, це може бути використання маршрутизаторів з підтримкою програмного забезпечення для управління мережею чи використання спеціальних комутаторів з можливістю відслідковування трафіку та обмеження швидкості передачі даних.

Переваги:

– використання маршрутизаторів з підтримкою програмного забезпечення для управління мережею;

– спеціальні комутатори з можливістю відслідковування трафіку та обмеження швидкості передачі даних.

Недоліки:

– висока вартість обладнання;

– складність налаштування та технічного обслуговування.

Також, третім можливим напрямком розв'язання завдання може бути використання хмарних технологій для моніторингу та керування мережею. Це дозволить зберігати всю необхідну інформацію про мережу кафе в онлайн-режимі і надавати доступ до неї з будь-якої точки земної кулі.

Переваги:

– збереження всієї необхідної інформації про мережу в онлайн-режимі;

– доступ до даних з будь-якої точки світу.

Недоліки:

– залежність від стабільного інтернет-з'єднання;

– можливі проблеми з безпекою даних в хмарі.

1.6 Обґрунтування вибраного напрямку інженерного рішення

Для забезпечення функціонування інтернет-геймінг кафе необхідно мати систему моніторингу та керування мережею.

Одним із можливих напрямків рішення цієї задачі є застосування протоколу SNMP (Simple Network Management Protocol). Цей протокол визнаний стандартом для управління мережевими обладнаннями у широкому спектрі відомих підприємств та організацій. З його допомогою можна забезпечити збір інформації з комп'ютерів та мережевого обладнання, а також віддалене керування ними [2].

Застосування протоколу SNMP в інтернет-геймінг кафе Joy-стік може мати декілька переваг. Перш за все, він дозволить системному адміністратору керувати мережними пристроями з централізованої точки, що спростить процес управління мережею. Крім того, за допомогою SNMP можна моніторити стан мережі, виявляти і усувати можливі проблеми та вчасно реагувати на них.

1.7 Завдання і мета роботи

Робота ставить на меті розробку потужної комп'ютерної системи для інтернет-геймінг кафе "Joy-стік" що включає в себе детальний розгляд побудови архітектури мережі та виконання відповідних налаштувань пристроїв для впровадження розробленої комп'ютерної мережі. Також важливим є забезпечення можливості модифікувати та адаптовувати мережеву інфраструктуру, зберігаючи її надійність та ефективність роботи.

Для досягнення цього необхідно засновувати мережеву інфраструктуру на сучасних та передових технологічних рішеннях, провести комплексну роботу з реалізацією таких етапів:

– визначити архітектуру створюваної мережі, та підібрати мережеве обладнання. Важливо обґрунтувати вибір обладнання що підтримує тривалу безперебійну роботу, гарантує безпеку даних та відкрите до масштабування мережі відповідно до зростаючих потреб кафе;

– організувати засоби моніторингу мережі для відстежування її функціонування та системи контролю для усунення проблем, що можуть виникати під час роботи обладнання або нештатних випадків, використовуючи протокол SNMP;

– провести тестування функціонування створеної комп'ютерної мережі, випробування компонентів мережі для затвердження працездатності.

Результатом виконання роботи має стати комп'ютерна мережа, що відповідає вимогам постійного моніторингу та управління мережею інтернет-геймінг кафе “Joy-стік”, є надійною та забезпечує безпечне інформаційне середовище. Така мережа дозволить закладу добре зарекомендувати себе на ринку, надати клієнтам якісне обслуговування та сервіс що задовольнить їх потребам у розвагах та цікавому проведенні вільного часу.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до комп'ютерної системи ГК JS

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонуванню системи

2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики

Об'єктом розробки є комп'ютерна система (надалі КС) для геймінг-інтернет кафе "Joy-стік" (надалі просто ГК JS). Основним призначенням КС є надання послуги тимчасової оренди комп'ютерів та ігрових пристроїв для клієнтів, а також для забезпечення корпоративних процесів функціонування закладу.

КС має складатися з наступних функціональних блоків:

Мережа клієнтів: дана частина КС виконує функцію надання послуг клієнтам, вона має містити в собі комп'ютери, ігрові консолі, установки віртуальної реальності, та ігрове приладдя таке як специфічні ігрові контролери (танцювальні килими, контролери у вигляді музичних інструментів, тощо). Також до цього функціонального мають входити бездротові точки доступу до мережі інтернет призначені для використання відвідувачами закладу.

Мережа обслуговування: ця частина КС має складатися з комп'ютерів призначених до використання персоналом, Із цього функціонального блоку має здійснюватись моніторинг роботи всієї мережі. Також через цей функціональний блок має здійснюватись обмін даними з інтернет провайдером.

Мережа відділу маркетингу: має складатися з обладнаних комп'ютерами робочими місцями, призначених для фахівців аналізу та розробки інновацій.

Також необхідно впровадити підсистему для моніторингу та керування мережею ГК JS на основі мережевого протоколу SNMP.

Підсистема має складатися з наступних з трьох основних компонентів:

- агентів моніторингу;
- сервера моніторингу;
- інтерфейсу адміністратора.

Агенти моніторингу встановлюються на кожному пристрої мережі та збирають дані про стан пристрою та мережі. Сервер моніторингу збирає дані від агентів моніторингу та будує карту мережі, що дозволяє адміністратору бачити стан мережі в режимі реального часу. Інтерфейс адміністратора забезпечує керування мережею та налаштування параметрів моніторингу.

2.1.1.1.2 Вимоги до способів і засобів зв'язку між компонентами комп'ютерної системи

Для створення каналів зв'язку в КС між мережевими пристроями необхідно використовувати кабелі вита пара категорії 6а для забезпечення пропускної здатності каналу до 1 Гбіт/с на відстані до 100 метрів. Також треба додати до мережі точки доступу Wi-Fi для надання доступу до мережі мобільним пристроям клієнтів.

2.1.1.1.3 Вимоги до характеристик взаємозв'язків створюваної системи із суміжними системами

Має бути створений швидкісний та захищений канал обміну даних між КС та компанією, що виступає надавачем доступу до мережі інтернет. У якості лінії підключення до надавача виступає оптоволоконний кабель з пропускною здатністю каналу до 1 Гбіт/с.

2.1.1.1.4 Вимоги до режимів функціонування системи

КС повинна працювати в декількох різних режимах роботи:

Режим повного функціонування: цей режим застосовується в робочі години закладу щодня протягом тижня, з 6:00 до 23:00. Він передбачає одночасну роботу всіх функціональних блоків КС.

Режим часткового функціонування: у цей режим мережа переводиться у

неробочі години закладу, з 23:00 до 6:00. У цьому режимі працюють лише ті функціональні блоки КС, які використовуються для внутрішніх процесів функціонування закладу, тобто без блоків що призначені для використання клієнтами.

Режим технічного обслуговування: може застосовуватись замість режиму часткової роботи у неробочі години закладу в тому випадку коли виникає необхідність проведення технічного обслуговування вузлів всередині функціональних блоків, або коли проводиться планове технічне обслуговування один раз на тиждень.

2.1.1.1.5 Вимоги до діагностування системи

Під час всіх режимів функціонування КС, має проводитись постійний моніторинг мережевих пристроїв, таких як маршрутизатори та комутатори за допомогою використання SNMP, для відстеження навантаження на певних ділянках мережі та вчасного виявлення будь яких помилок в роботі цих пристроїв.

2.1.1.1.6 Перспективи розвитку, модернізації системи

Необхідно мережу розділити на чотири підмережі відповідно до організаційної структури за допомогою VLAN.

Комутатори з'єднати в кільце щоб покращити надійність мережі шляхом зменшення точок відмов та забезпечення резервних маршрутів для передачі даних.

У процесі розвитку важливою є питання ефективності та надійності мережевої інфраструктури. Одним із ключових напрямків у цьому аспекті є модернізація мережі, що полягає у розширенні її функціоналу. Для досягнення цієї мети можна розглянути можливість додання чотирьох підмереж нових закладів геймінг-кафе та їх з'єднання через множинні маршрутизатори.

Розширити мережу шляхом додавання 4 підмереж організації та їх з'єднання через множинні маршрутизатори, налаштування маршрутизації.

IP-адресацію мереж потрібно використовувати із запропонованого завдання та відповідно до варіанту (рис. 2.1) [1]. Завданий адресний простір мережі – 172.25.114.0/21.

Кількість вузлів в певному сегменті мережі:

- LAN1 – 40;
- LAN2 – 70;
- LAN3 – 35;
- LAN4 – 121.

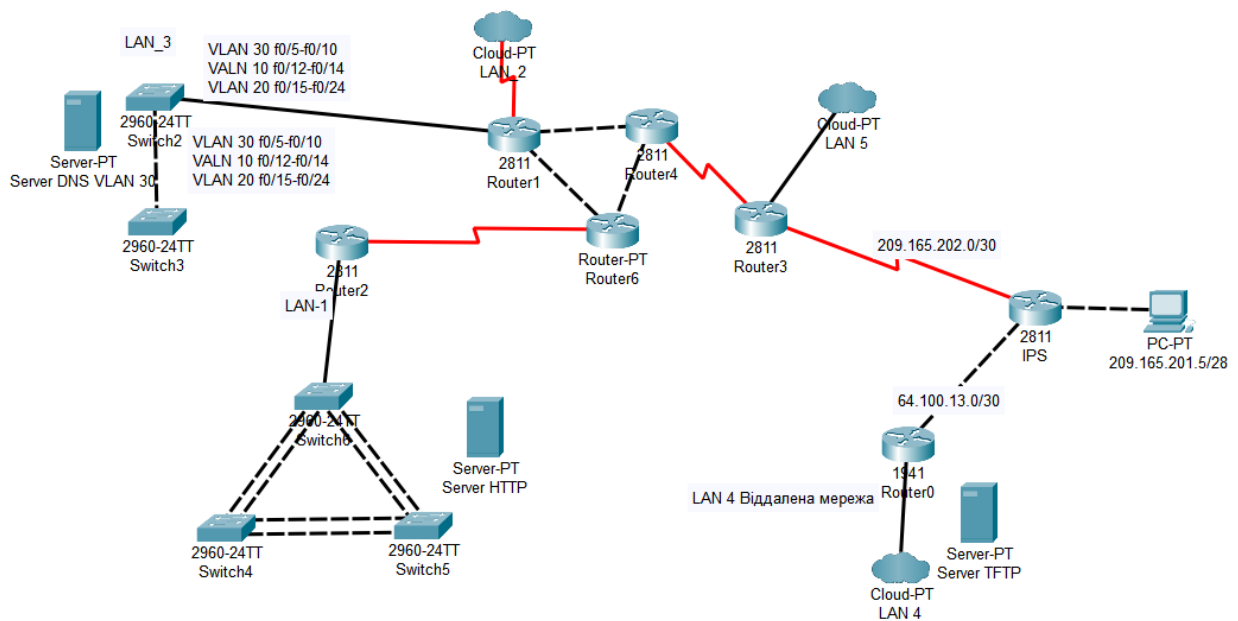


Рисунок 2.1 – Топологія мереж геймін-кафе

Для ефективного функціонування мережі важливо правильно налаштувати маршрутизатори, щоб забезпечити оптимальний шлях для передачі даних між підмережами та зовнішніми мережами.

2.1.1.2 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:

– системні адміністратори є молодшими спеціалістами в галузі "Комп'ютерна інженерія", відповідають за підтримку роботи комп'ютерів та ігрових консолей, вирішення технічних проблем та неполадок;

– технік має бакалаврську або молодшу освіту в галузі «Електроніка, автоматизація та електронні комунікації» та відповідають за ремонт та обслуговування геймінгового обладнання.

Всі працівники 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.

2.1.1.3 Вимоги щодо надійності

Для забезпечення стабільної та надійної роботи геймінг-кафе, необхідно дотримуватися певних вимог до апаратного та програмного забезпечення.

Надійне обладнання з показником MTBF не менше 100,000 годин для серверів та 50,000 годин для мережевого обладнання.

Резервування важливих компонентів (серверів, мережевих комутаторів, джерел живлення) для досягнення вірогідності безвідмовної роботи 99.99%.

Використовувати сучасне антивірусне ПЗ, оновлювати ОС і програмне забезпечення регулярно, налаштувати моніторинг системи для виявлення та виправлення помилок в режимі реального часу.

Використовувати інструменти моніторингу, такі як SNMP, для постійного контролю стану мережі та серверів, а також автоматизованих сповіщень у випадку виявлення проблем.

2.1.1.4 Вимоги до показників призначення

Перевірка показників зібраних за допомогою використання SNMP що свідчать про підтримання високої пропускної здатності мережі має відбуватись щогодинно під час робочих годин закладу, коли мережа перебуває у режимі повного функціонування.

2.1.1.5 Вимоги до патентної чистоти

Має бути забезпечена патентна чистота програмного та апаратного забезпечення на території України.

2.1.1.6 Додаткові вимоги

Додаткові вимоги до КС не висуваються.

2.1.2 Вимоги до видів забезпечення КС

2.1.2.1 Вимоги до технічного забезпечення

Мережеві пристрої, такі як маршрутизатори та комутатори повинні забезпечувати наступне:

- високу пропускну здатність каналу;
- підтримку протоколу SNMP для забезпечення збирання даних про стан мережі та віддаленого управління.

Потужний сервер моніторингу для обробки великої кількості даних, що надходять від мережевих пристроїв пристроїв:

- багатоядерний процесор (не менше 4 ядер);
- RAM мінімум 16 ГБ;
- мінімум 1 Тб жорстких дисків (рекомендується SSD);
- пропускну здатність: мінімум 1 Гбіт/с;
- підтримка протоколів шифрування, таких як SSH або SSL/TLS;
- підтримка протоколу SNMP.

Комутатори повинні забезпечувати наступні вимоги:

- 24 порти гігабітної мережі;
- швидкість передачі даних до 16 Гбіт/с.;
- стандарт 100BASE-TX;

2.1.2.2 Вимоги до програмного забезпечення

На сервері встановлений SNMP-менеджер для збору і аналізу даних від SNMP-агентів. Це може бути спеціалізоване ПЗ, як-от Nagios, Zabbix або

PRTG.

Підтримка різних версій SNMP, включаючи SNMPv1, SNMPv2c і SNMPv3 для забезпечення сумісності з різним обладнанням і рівнями безпеки.

SNMP-агенти повинні бути встановлені на кожному мережевому пристрої для збору і передачі даних на SNMP-менеджер.

2.1.2.3 Вимоги до інформаційного забезпечення

Мають бути розроблені нормативні документи з експлуатації та обслуговування компонентів мережі та робочих місць, розроблений документ правил техніки безпеки при використанні компонентів мережі.

Також, має бути створена пояснювальна записка для клієнтів закладу з експлуатації пристроїв до яких їм надається доступ під час надання послуг.

2.1.2.4 Вимоги до лінгвістичного забезпечення

Всі лінгвістичні елементи мережі мають переважно надаватися українською мовою, або англійською мовою у разі відсутності української альтернативи.

2.2 Розробка апаратної частини комп'ютерної системи

2.2.3 Розробка структурної схеми мережі

На основі загальної характеристики компанії, її організаційної структури, кількості підмереж та поставлених завдань була створена структурна схема технічних засобів комп'ютерної системи ГК JS (рисунок 2.1):

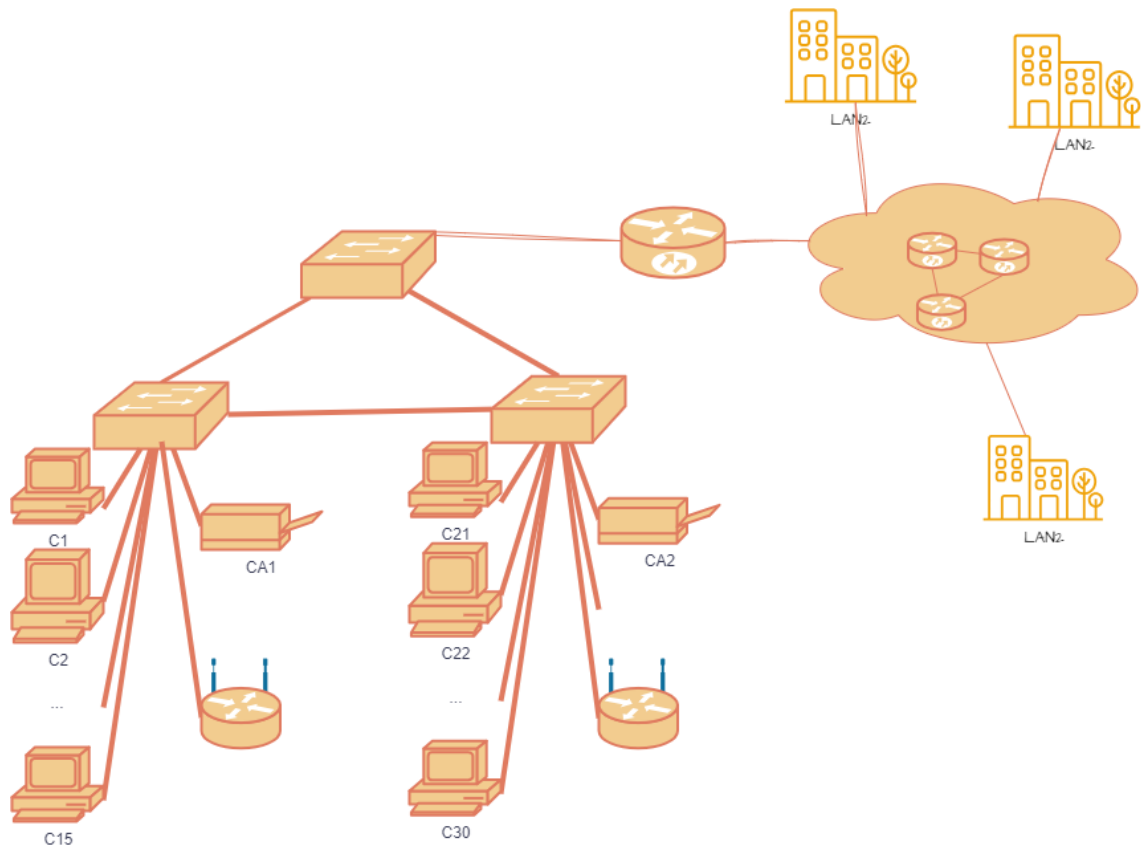


Рисунок 2.2 – Структурна схема комплексу технічних засобів КС

Розроблена схема включає в себе:

Використання маршрутизаторів та комутаторів: розташування маршрутизаторів та комутаторів дозволяє ефективно керувати мережевим трафіком, забезпечуючи високу доступність, розподіл навантаження між вузлами мережі, та забезпечення високої пропускнуої здатності.

Сегментація мережі за допомогою Virtual LAN: використання VLAN допомагає ізолювати трафік всередині мережі, що дозволяє підвищити захищеність мережі, та дозволяє більш ефективно нею керувати.

Головна мережа закладу має розділитись на декілька віртуальних мереж, згідно функціоналу для якого призначені кінцеві вузли (комп'ютери та інші пристрої) для полегшення керування мережею та моніторингу:

VLAN10 – віртуальна мережа призначена для клієнтів закладу. Складається з 30 комп'ютерів та ігрових пристроїв, а також містить бездротові точки доступу.

VLAN20 – призначена для комп'ютерів що використовуються

персоналом обслуговування. Складається з 15 робочих станцій.

VLAN30 – призначена для робочих станцій фінансового відділу, налічує 10 комп'ютерів.

VLAN40 – віртуальна мережа виділена для потреб відділу розвитку, налічує 5 постійних робочих станцій у вигляді комп'ютерів, з можливістю додавання до неї пристроїв які випробовуються та тестуються;

VLAN100 – призначена для адміністрування мережним обладнанням.

2.2.4 Розробка специфікації апаратних засобів КС

У комп'ютерній мережі передбачено використання 3-х шістнадцяти портових комутаторів.

Виконуючи вимоги до апаратного забезпечення мережі, було розроблено специфікацію пристроїв для забезпечення швидкості 1Гб/с та безпеки мережі.

Для з'єднання кінцевих вузлів геймінг-кафе буде використовуватися комутатори, а для об'єднання підрозділів в єдину локальну мережу - маршрутизатори. Вибір комутаторів та маршрутизаторів ґрунтується на вимогах проекту.

Комутатори Catalyst 2960 та маршрутизатори Cisco 2911 були обрані для реалізації проекту (рис.2.3–2.4). Комутатор Catalyst 2960 є високопродуктивним пристроєм, який може підключатися до різних типів пристроїв, таких як робочі станції, бездротові точки доступу Cisco, сервери, маршрутизатори та інші комутатори.

Комутатор Cisco Catalyst 2960 – це серія комутаторів Ethernet, які широко використовуються в бізнес-мережах для забезпечення швидкого і надійного підключення різних пристроїв до мережі. Вони мають різні моделі з різними характеристиками, але загалом Catalyst 2960 відомий своєю надійністю, продуктивністю і простотою управління. На рисунку 2.3 продемонстрований зовнішній вигляд комутатора Cisco Catalyst 2960.



Рисунок 2.3 – Зовнішній вигляд комутатора Cisco Catalyst 2960

Ключові характеристики Catalyst 2960:

– швидкість і пропускну здатність: Catalyst 2960 підтримує швидкість передачі даних до 10/100/1000 Мбіт/с на порт, залежно від моделі. Деякі моделі також можуть мати підтримку Gigabit Ethernet SFP портів;

– управління: Catalyst 2960 має різні можливості управління, включаючи Cisco IOS Software, яке дозволяє адміністраторам конфігурувати та моніторити мережеві параметри;

– підтримка безпеки: вони також забезпечують різні функції безпеки, такі як ACL (Access Control Lists), VLAN (Virtual LAN) і портова безпека;

– енергозбереження: деякі моделі Catalyst 2960 мають функції енергозбереження, які дозволяють ефективно використовувати електроенергію;

– стійкість і надійність: Catalyst 2960 відомий своєю стійкістю і надійністю, що робить їх популярними в бізнес-середовищах, де доступність мережі є критичною.

Маршрутизатор Cisco 2911 є популярним вибором для мереж інтернет-кафе завдяки своїм надійним технічним характеристикам та можливостям.

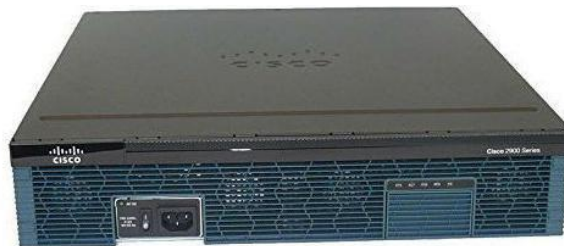


Рисунок 2.4 – Вигляд маршрутизаторів Cisco 2911

Основні характеристики цього пристрою включають [6]:

– процесор: підтримка багатоядерного процесора;

- пам'ять: 512 MB DRAM (максимум 2 GB), 256 MB Flash (максимум 4 GB) [4];
- порти: 3 порти 10/100/1000 Gigabit Ethernet для швидкого та надійного з'єднання [5];
- слоти розширення: підтримка EHWIC слотів для розширення функціональності;
- безпека: Інтегровані функції безпеки, такі як VPN, брандмауер та IPS (Intrusion Prevention System);
- QoS (Quality of Service): підтримка для управління трафіком та забезпечення високої якості обслуговування;
- VoIP: підтримка голосового зв'язку через інтернет (VoIP) для підключення телефонних ліній;
- SFP-роз'єми: можливість переходу на оптичні з'єднання для підвищення швидкості та надійності мережі;
- форм-фактор: компактний дизайн для зручного розміщення в серверних стійках.

Підключення ПК геймерів до комутаторів відбувається за допомогою кабелю категорії 5e. Між комутаторами за допомогою мінімум двох лінків FastEthernet для надійності та збільшення пропускної здатності за рахунок агрегування каналів.

Бездротовий маршрутизатор Asus RT-AX1800U є перспективним рішенням для геймінг-кафе, що прагнуть забезпечити своїх відвідувачів високоякісним інтернет-з'єднанням. Цей маршрутизатор поєднує в собі передові технології Wi-Fi 6, що забезпечують швидкий та надійний бездротовий доступ до мережі [4].

Ключовими перевагами моделі Asus RT-AX1800U є її надзвичайна пропускна здатність, що сягає 1800 Мбіт/с, та підтримка технології OFDMA. Ці характеристики дозволяють ефективно обслуговувати велику кількість одночасних підключень, що є критично важливим для геймінг-кафе, де одночасно працюють численні комп'ютери та мобільні пристрої.

В таблиці 2.1 надано специфікацію апаратних засобів КС.

Таблиця 2.1 – Специфікація обладнання комп'ютерної системи

Позиція	Найменування та технічна характеристика	Тип, марка, позначення документа	Од. виміру	Кількість
1	Комп'ютер: AMD 8-core Ryzen 7 5700G 3.8-4.6GHz ; Radeon Vega 8 ; 8GB DDR4-3200 ; 240GB SSD ;	ARTLINE Business B47v09	шт.	30
2	Монітор 27" Samsung Curved LS27C366 частота оновлення 75 Гц, 1920x1080 (FullHD), Flicker-Free, вигнутий екран, кут огляду горизонтальний 178°	Curved LS27C366	шт	35
3	Комп'ютер: Intel (8p+16e)-Core i9 13900KF 3.0-5.8GHz ; GeForce RTX 4090 24GB ; 64GB DDR5-6000 Gaming ; 1TB NVMe Gen4 ;	ARTLINE HYPERIONv12	шт.	1
4	Маршрутизатор: Crypto, 4 built-in GE, Dual P/S, 20Gbit, 6x1000Base-X (SFP), 2x10G SFP+ інтегровані RP, SIP та ESP, 1xNIM, 1xSPA, RAM 8Gb, 2xAC	Cisco 2911	шт.	1
5	Маршрутизатор Wi-Fi Asus RT-AX1800U, 5 ГГц + 2.4 ГГц (дводіапазонний), швидкість LAN портів 1 Гбіт/с. Стандарт зв'язку Wi-Fi: 802.11a/b/g/n, Wi-Fi 5 (802.11ac), Wi-Fi 6 (802.11ax). Швидкість Wi-Fi, Мбіт/с. 1800 Мбіт/сек	Asus RT-AX1800U	шт.	2
6	Комутатор: Ethernet 10/100/1000 Мбіт/сек, RIP v1, RIP v2, OSPF, USB-порт, LAN Base, 4 SFP слоти	Cisco Catalyst 2960	шт.	23
7	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)	шт	1
8	Кабель витая пара ОК-Net UTP кат.5е КПВ-ВП (350) 4*2*0,51, 305м	КПВ-ВП (350) 4*2*0,5	шт.	1

2.2.5 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

В підмережі ГК JS встановлений комутатор Cisco2960, що об'єднує 70 ПК. Вихідний трафік з комутатора надсилається до роутера 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 $\mu=86$ (кадрів/с), а середня довжина повідомлення – 1150 байт.

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

$$P_{p.p.} = \mu * L_{пов} * N * 8 = 86 * 1150 * 70 * 8 = 55.39 \text{ Мбіт/с} \quad (2.1)$$

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

$$\mu_{вих} = 10^9 / (1150 * 8) = 108\,696 \text{ пакетів/с} \quad (2.2)$$

Оскільки в середньому, кожне джерело виробляє 86 пакетів/с, то маршрутизатор обмежений кількістю приєднань, яку ми можемо дізнатись наступним чином:

$$N = \mu_{вих} / \mu = 108\,696 / 86 \approx 1264 \text{ джерела} \quad (2.3)$$

Ця кількість задовольняє кількості вузлів у найбільшій нашій локальній мережі, до якої входить 70 ПК.

Кожен з 70 ПК посилає потік заявок з інтенсивністю у 86 кадрів/с. Звідси, можемо розрахувати інтенсивність вихідного трафіку:

$$\lambda = N * \mu = 70 * 86 = 6020 \text{ пакетів/с.} \quad (2.4)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu_{\text{вих}}} = \frac{6020}{108696} = 0,055 \quad (2.5)$$

Коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0,055}{1-0,055} = 0,058 \quad (2.6)$$

Середня затримка кадру, пов'язана з чергою М/М/1, дорівнює:

$$T = \frac{1}{(\mu-\lambda)} = \frac{1}{(108696-6020)} = 9,73 \text{ мкс} \quad (2.7)$$

Середня довжина черги:

$$L_{\text{чер}} = \frac{\rho^2}{1-\rho} = \frac{0,055^2}{1-0,055} = 0,0032 \quad (2.8)$$

Середній час перебування пакета у черзі:

$$T_{\text{оч}} = \frac{L_{\text{чер}}}{\lambda} = \frac{0,0032}{6020} = 0,5 \text{ мкс} \quad (2.9)$$

Це значення задовольняє вимогам до затримки в ЛМ.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

Згідно з розділом 2.1.1.1.6 перспективи розвитку для адресації для 5 мереж закладів використовується блок адрес 172.25.112.0/21. В таблиці 3.1 наведено результат розрахунку адрес мереж методом VLSM. Важливо, щоб не було перекриття між підмережами і всі адреси використовувалися оптимально.

Для розбиття мережі 172.25.112.0/21 на 5 підмереж методом VLSM, виконано чином:

ГКЗ (182 вузлів):

- необхідно: $182 + 2$ (адреси мережі та широкомовлення) = 184 адреси;
- найближче більше значення: 256 адрес (8 біт для хостів);
- маска підмережі: /24;
- діапазон: 172.25.112.0 - 172.25.112.255;

ГК 5 (121 вузол):

- необхідно: $121 + 2 = 123$ адреси;
- найближче більше значення: 128 адрес (7 біт для хостів);
- маска підмережі: /25;
- діапазон: 172.25.113.0 - 172.25.113.127.

ГК 2 (75 вузлів):

- необхідно: $75 + 2 = 77$ адрес;
- найближче більше значення: 128 адрес (7 біт для хостів);
- маска підмережі: /25;
- діапазон: 172.25.113.128 - 172.25.113.255.

ГК JS (40 вузлів):

- необхідно: $40 + 2 = 42$ адреси;
- найближче більше значення: 64 адреси (6 біт для хостів);
- маска підмережі: /26;
- діапазон: 172.25.114.0 - 172.25.114.63.

Підмережа 4 (35 вузлів):

- необхідно: $35 + 2 = 37$ адрес;
- найближче більше значення: 64 адреси (6 біт для хостів);
- маска підмережі: /26;
- діапазон: 172.25.114.64 - 172.25.114.127;

Таким чином, усі підмережі розподілено без перекриття відповідно до їхніх вимог за кількістю вузлів. Результати підрахунків адрес підмереж наведено на таблиці 3.1.

Таблиця 3.1 – Схема адресації мереж

Назва підмережі	Необхідна кіл-ть вузлів	Адреса підмережі	Діапазон допустимих IP-адрес вузлів
ГК3	182	172.25.112.0/24	172.25.112.1 – 172.25.112.254
ГК5	121	172.25.113.0/25	172.25.113.1 – 172.25.113.126
ГК2	75	172.25.113.128/25	172.25.113.129 – 172.25.113.254
ГК JS	40	172.25.114.0/26	172.25.114.1 – 172.25.114.62
ГК4	35	172.25.114.64/26	172.25.114.65 – 172.25.114.126

В мережі ГК JS щоб зменшити навантаження та покращити безпеку буде застосовано технологію віртуальних локальних мереж (VLAN). Для цього мережу потрібно розділити на окремі віртуальні підмережі, за межами яких не буде виходити ширококомовний трафік. Згідно з 2.2.3 таких підмереж буде організовано 5: VLAN10, VLAN20, VLAN30, VLAN40, VLAN100. В таблиці 3.2 наведені відомості про ці мережі.

Таблиця 3.2 – VLAN в мережі ГК JS

VLAN	Name	IP-address	Примітка
10	Customer	172.25.114.0/26	клієнти закладу ГК JS
20	Service	172.25.114.64/26	персонал обслуговування
30	Finance	172.25.114.128/26	фінансовий відділу
40	Develop	172.25.114.192/26	відділ розвитку
100	Admin	192.168.100.0/24	адміністрування мережним обладнанням

На рисунку 3.1 представлена L3-схема реалізацію концепції VLAN у геймінг-кафе, де показано логічно розділені сегменти в єдиній фізичній мережі. Такий підхід дозволяє забезпечити високий рівень безпеки, продуктивності та керованості мережевої інфраструктури закладу.

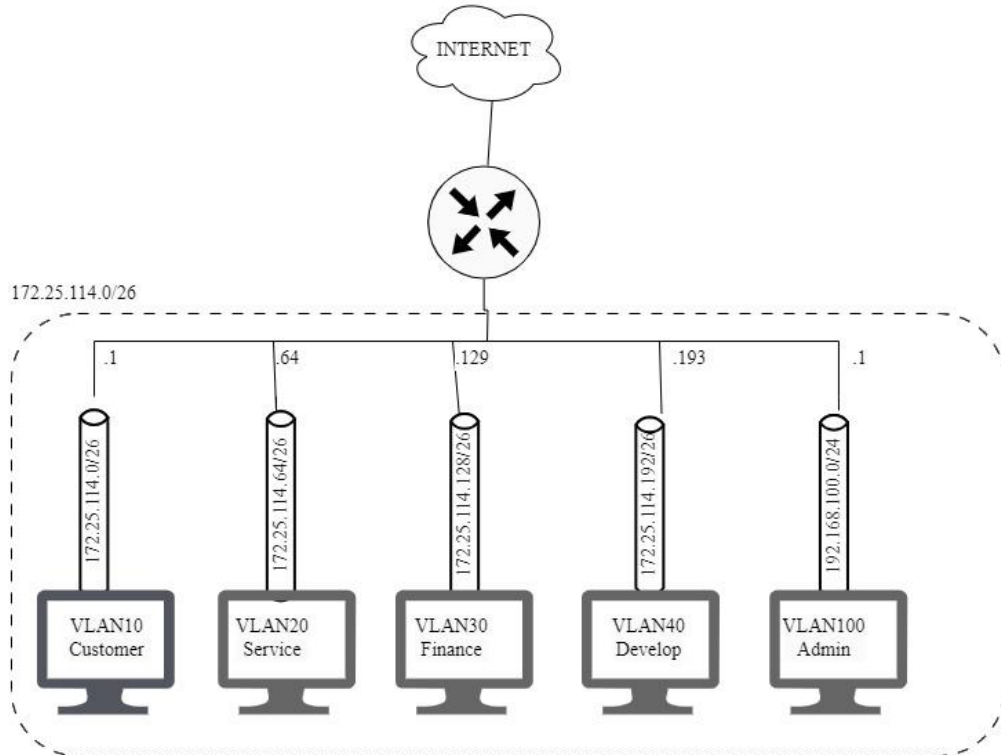


Рисунок 3.1 – L3-схема мережі ГК JS

В таблиці 3.3 наведено адресація мережного обладнання. Перша адреса призначається маршрутизатору і використовується в якості шлюза на ПК.

Таблиця 3.3 – Адресація пристроїв

Пристрій	Інтерфейс	IP-адреса	Шлюз	VLAN
R_JS	f0/0.10	172.25.114.1/26	-	10
	f0/0.20	172.25.114.65/26	-	20
	f0/0.30	172.25.114.129/26	-	30
	f0/0.40	172.25.114.192/26	-	40
	f0/0.100	192.168.100.1/24	-	10
Sw_JS1	Vlan100	192.168.100.10	f0/0.100	100
Sw_JS2	Vlan100	192.168.100.11	f0/0.100	100
Sw_JS3	Vlan100	192.168.100.12	f0/0.100	100

3.2 Розробка моделі мережі в Packet Tracer

Згідно з вимогами до КС було розроблено модель мережі в Cisco Packet Tracer, наведену на рисунку 3.2. Packet Tracer – це інструмент від компанії Cisco, який дозволяє моделювати реальні комп'ютерні мережі логічну топологію мережі.

Геймерські ПК та ПК співробітників закладу об'єднані в одну локальну мережу за допомогою 3-х 24-портових комутаторів Cisco 2960. 2 комутатори (Sw_JS1 та Sw_JS2) для під'єднання ПК з різних VLAN, третій (Sw_JS3) для їх об'єднання та для підключення до маршрутизатора. Маршрутизатор підключено до Інтернет по волокну оптичному кабелю.

Комутатори з'єднані в кільце, щоб покращити надійність мережі шляхом зменшення точок відмов та забезпечення резервних маршрутів для передачі даних. По 2 лінки між ним для збільшення пропускної здатності в 2 рази та надійності. В разі обриву одного з кабелів, пропускна здатність зменшиться, але лінк буде працювати.

Встановлено 2 бездротових маршрутизатори, тому всі клієнти закладу матимуть доступ до мережі незалежно від їхнього місця розташування.

Потрібно налаштувати мережеві пристрої, а саме:

- налаштувати паролі для приватного режиму, консолі і vty;
- усі відкриті паролі зашифровані;
- встановлено банер MOTD;
- налаштований на усіх лініях vty використання протоколу ssh;
- для шифрування даних створено ключ RSA завдовжки 1024 біт;
- на DCE-інтерфейсах маршрутизаторів значення тактової частоти – 128000;
- в якості імені домена використовувати ім'я KRYVOSHEIEV.

В Додатку А наведено конфігураційний файл з налаштуваннями на маршрутизаторі R_JS.

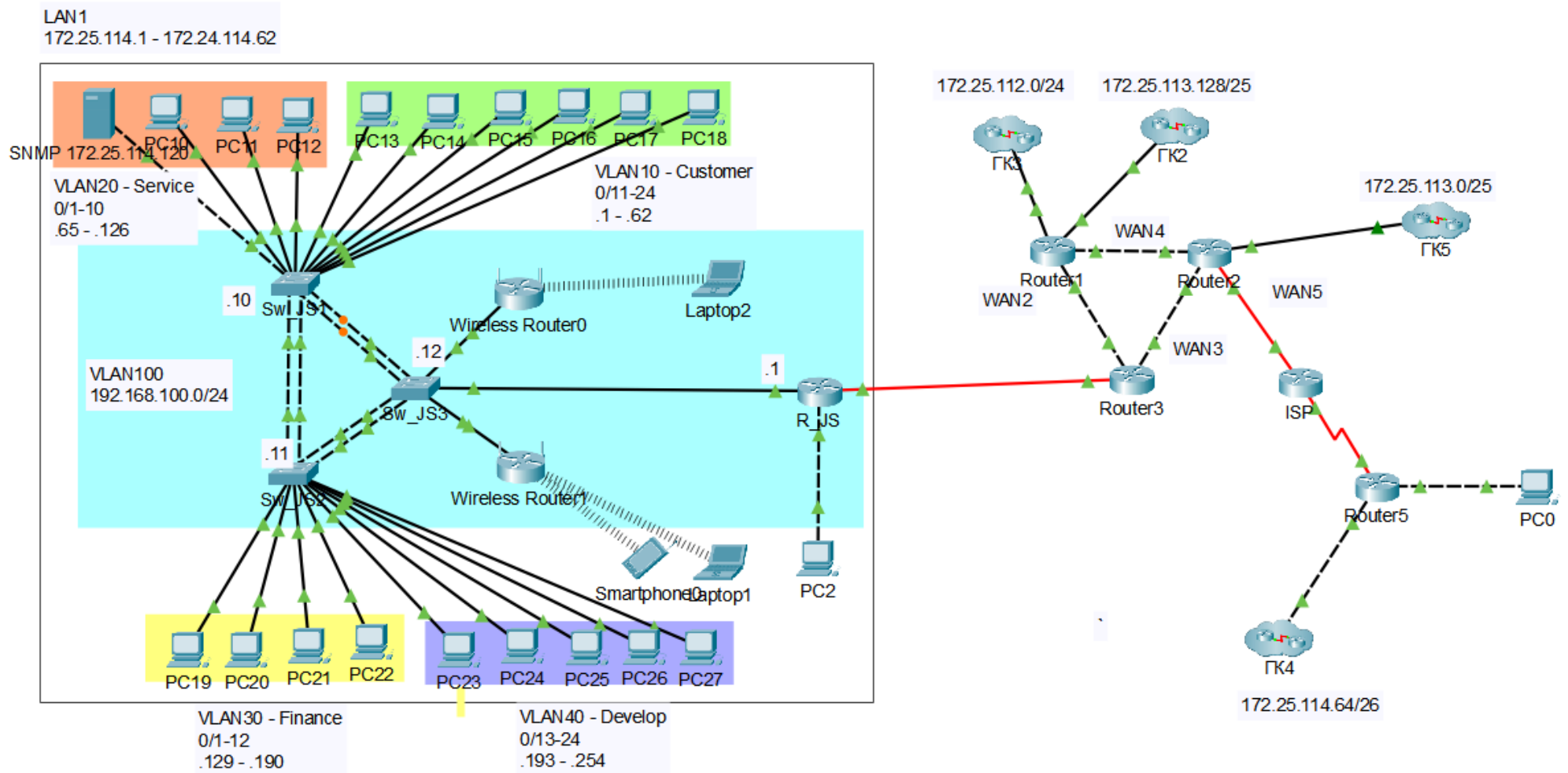


Рисунок 3.2 – Модель мережі в Packet Tracer

3.3 Вибір та налаштування способу маршрутизації та доступу до Інтернет

Організація ефективної та стабільної мережі в геймінг-кафе є ключовим фактором для успіху. Для цього необхідно обрати спосіб маршрутизації та забезпечити надійний доступ до Інтернету.

OSPF (Open Shortest Path First) – це протокол маршрутизації внутрішнього домену, який використовується для створення маршрутної таблиці на основі найкоротшого шляху.

Переваги OSPF:

- швидке конвергування: OSPF швидко адаптується до змін у мережі, що забезпечує мінімальні перебої в роботі;
- масштабованість: протокол може масштабуватись для великих мереж, що особливо важливо для геймінг-кафе з великою кількістю користувачів;
- надійність: OSPF забезпечує надійну маршрутизацію завдяки механізму виявлення помилок та резервування.

У цьому контексті протокол маршрутизації OSPF (Open Shortest Path First) є надійним та ефективним рішенням. OSPF дозволяє динамічно адаптувати маршрути передачі даних відповідно до змін у мережі, забезпечуючи оптимальний шлях для пакетів. Це особливо важливо в середовищі геймінг-кафе, де мережа може зазнавати значного навантаження та змін.

Поряд із маршрутизацією, важливим аспектом є організація доступу до Інтернету. Геймінг-кафе потребують надійного та швидкого Інтернет-з'єднання, яке здатне впоратися з високим трафіком та різноманітними онлайн-активностями відвідувачів. Тут варто розглянути можливість використання швидких оптичних або кабельних технологій, а також балансування навантаження між декількома Інтернет-провайдерами для підвищення відмовостійкості.

На рисунку 3.3 наведено код з налаштування OSPF на маршрутизаторі R_JS. Конфігурація передбачає, що маршрутизатор має інтерфейси,

підключені до мереж 10.0.0.0/24 і 172.25.0.0/16.

```
R_JS(config)#router ospf 9
R_JS(config-router)#auto-cost reference-bandwidth 1000
R_JS(config-router)#net 10.0.0.0 0.0.0.255 a 0
R_JS(config-router)#net 172.25.0.0 0.0.255.255 a 0
```

Рисунок 3.3 – Налаштування OSPF на маршрутизаторі R_JS

Ця конфігурація налаштовує маршрутизатор OSPF із такими параметрами:

- ID протоколу 9;
- еталонна смуга пропускання: 1000 (це визначає базову смугу пропускання, яка використовується для розрахунку вартості інтерфейсів. Чим нижча еталонна смуга пропускання, тим вища вартість інтерфейсів із меншою смугою пропускання).

- мережа 10.0.0.0 0.0.0.255 area 0: цей рядок рекламує мережу 10.0.0.0/24 як мережу OSPF;

- мережа 172.25.0.0 0.0.255.255 area 0: цей рядок рекламує мережу 172.25.0.0/16 як мережу OSPF.

OSPF використовуватиме ці оператори мережі для створення своєї таблиці маршрутизації та обміну цією інформацією з іншими маршрутизаторами OSPF у тій самій зоні.

Аналогічно було виконано налаштування і на інших маршрутизаторах мереж геймінг-кафе. Після обміну інформацією в таблиці маршрутизації повинні відобразитися записи з IP-адресам віддалених мереж з символом «O» на початку. На рисунку 3.4 таблиця маршрутизації на R_JS відображає всі відомі йому мережі.

```

R_JS
Physical Config CLI Attributes
IOS Command Line Interface
i - IS-IS, LI - IS-IS level-1, LZ - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

 10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C   10.0.0.0/30 is directly connected, GigabitEthernet0/3/0
L   10.0.0.2/32 is directly connected, GigabitEthernet0/3/0
O   10.0.0.4/30 [110/11] via 10.0.0.1, 00:48:01, GigabitEthernet0/3/0
O   10.0.0.8/30 [110/11] via 10.0.0.1, 00:48:01, GigabitEthernet0/3/0
O   10.0.0.12/30 [110/21] via 10.0.0.1, 00:48:01, GigabitEthernet0/3/0
 172.25.0.0/16 is variably subnetted, 11 subnets, 4 masks
O   172.25.112.0/24 [110/21] via 10.0.0.1, 00:48:01, GigabitEthernet0/3/0
O   172.25.113.0/25 [110/21] via 10.0.0.1, 00:48:01, GigabitEthernet0/3/0
O   172.25.113.128/25 [110/21] via 10.0.0.1, 00:48:01, GigabitEthernet0/3/0
C   172.25.114.0/26 is directly connected, FastEthernet0/0.10
L   172.25.114.1/32 is directly connected, FastEthernet0/0.10
C   172.25.114.64/26 is directly connected, FastEthernet0/0.20
L   172.25.114.65/32 is directly connected, FastEthernet0/0.20
C   172.25.114.128/26 is directly connected, FastEthernet0/0.30
L   172.25.114.129/32 is directly connected, FastEthernet0/0.30
C   172.25.114.192/26 is directly connected, FastEthernet0/0.40
L   172.25.114.193/32 is directly connected, FastEthernet0/0.40
 192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.100.0/24 is directly connected, FastEthernet0/0.100
L   192.168.100.1/32 is directly connected, FastEthernet0/0.100
O*E2 0.0.0.0/0 [110/1] via 10.0.0.1, 00:48:01, GigabitEthernet0/3/0

R_JS# |

```

Рисунок 3.4 – Таблиця маршрутизації на R_JS

Виконаємо трасування маршруту для того, щоб упевнитись у правильних налаштуваннях мережі та в тому, що мережі можуть обмінюватись даними без перешкод. Отримані результати нас задовольняють, тому можна сказати, що налаштування та побудова мережі пансіонатів завершена успішно.

```

R_JS#traceroute 172.25.113.1
Type escape sequence to abort.
Tracing the route to 172.25.113.1

 0  10.0.0.1          0 msec    0 msec    0 msec
 1  10.0.0.1          0 msec    0 msec    0 msec
 2  10.0.0.10         0 msec    0 msec    0 msec
R_JS#

```

Рисунок 3.5 – Трасування до мережі ГК5

3.4 Налаштування мереж VLAN, маршрутизації між VLAN

Створення VLAN відбувається у налаштуваннях комутаторів мережі.

Потри на комутаторах розподілені між VLAN наступним чином:

- Sw_JS1: f0/1-10 VLAN20;
- Sw_JS1: f0/11-20 VLAN10;
- Sw_JS1: f0/21-24, g0/1-2 trunk;

- Sw_JS2: f0/1-10 VLAN30;
- Sw_JS2: f0/1-10 VLAN40;
- Sw_JS1: f0/21-24, g0/1-2 trunk;
- Sw_JS3: f0/21-24, g0/1-2 trunk

Далі наведено приклад налаштувань на комутаторі Sw_JS1:

```
interface range fa0/11-20 //вибір портів для призначення їм VLAN
switchport mode access //зміна режиму роботи портів
switchport access vlan 10 //призначення обраним портам VLAN
vlan 10 //налаштування VLAN
name Customer //зміна назви VLAN для зручності адміністрування
interface range fa0/1-10
switchport mode access
switchport access vlan 20
vlan 20
name Service
interface range f0/21-24, gig0/1-2
switchport mode trunk //переведення портів у режим транкування
```

Командою `show vlan brief` перевіримо правильність налаштувань та розподілень портів між VLAN. На рисунку 3.6 маємо результат відповідний до налаштувань.

```
Sw_JS1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Gig0/1, Gig0/2
10	Customer	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20
20	Service	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10
30	Finance	active	
40	Develop	active	
90	Native	active	
100	Admin	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
Sw_JS1#
```

Рисунок 3.6 – Перевірка VLAN на Sw-JS1

Для обміну інформацією між ПК в різних VLAN на маршрутизаторі R_JS створюються підінтерфейси до кожної VLAN (рис. 3.7).

```
R_JS#show ip interface brief | include 0/0
FastEthernet0/0          unassigned      YES NVRAM      up
FastEthernet0/0.10      172.25.114.1   YES manual    up
FastEthernet0/0.20      172.25.114.65  YES manual    up
FastEthernet0/0.30      172.25.114.129 YES manual    up
FastEthernet0/0.40      172.25.114.193 YES manual    up
FastEthernet0/0.100     192.168.100.1  YES manual    up
R_JS#
```

Рисунок 3.7 – Підінтерфейси на R_JS

Для перевірки, що вузли в різних VLAN можуть обмінюватися інформацією між собою, виконаємо ping та tracert з ПК в VLAN20 на ПК в VLAN10 (рис. 3.8).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:42FF:FE8E:2704
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 172.25.114.67
    Subnet Mask . . . . .: 255.255.255.192
    Default Gateway . . . . .: ::
                                172.25.114.65

C:\>ping 172.25.114.4

Pinging 172.25.114.4 with 32 bytes of data:

Request timed out.
Reply from 172.25.114.4: bytes=32 time<1ms TTL=127
Reply from 172.25.114.4: bytes=32 time<1ms TTL=127
Reply from 172.25.114.4: bytes=32 time<1ms TTL=127

Ping statistics for 172.25.114.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>tracert 172.25.114.4

Tracing route to 172.25.114.4 over a maximum of 30 hops:

  0  0 ms    0 ms    1 ms    172.25.114.65
  1  0 ms    0 ms   14 ms    172.25.114.4

Trace complete.

C:\>
```

Рисунок 3.8 – Перевірка доступу з VLAN20 до VLAN10

Як видно, результати успішні і вузли досяжні між собою. Трасування показує, що пакет проходить через створені підінтерфейси на R_JS.

3.5 Захист від несанкціонованого доступу

Зв'язок між головною мережею та рештою КС відбувається за допомогою маршрутизатора R_JS. На ньому виконані базові налаштування з безпеки. Конфігурація на рисунку встановлює наступне:

1. Логін «Kryvosheiev» із секретним паролем «net24J@y».
2. Увімкнено секретний пароль «NetP@ss24».
3. Доступ до консолі з паролем «net@4Joy» і включеним входом.
4. Лінії VTY (від 0 до 4) з увімкненим локальним входом.
5. Шифрування паролів увімкнено для всіх паролів.

Ця конфігурація забезпечує основні заходи безпеки, такі як автентифікація користувача та захист паролем для інтерфейсів керування маршрутизатора. Важливо зберігати ці паролі в безпеці, а також регулярно переглядати й оновлювати їх за потреби з міркувань безпеки.

```
R_JS(config)#username Kryvosheiev secret net24J@y
R_JS(config)#enable secret NetP@ss24
R_JS(config)#line console 0
R_JS(config-line)#password net@4Joy
R_JS(config-line)#login
R_JS(config-line)#line vty 0 4
R_JS(config-line)#login local
R_JS(config-line)#service password-encryption
R_JS(config)#
```

Рисунок 3.9 – Базові налаштування безпеки на маршрутизаторі R_JS

4 НАЛАШТУВАННЯ ПРОТОКОЛУ SNMP

4.1 Архітектура та функції протоколу SNMP

Simple Network Management Protocol (SNMP) це протокол інтернету для збору та організації інформації щодо пристроїв у мережах IP, а також модифікації цієї інформації для зміни поведінки пристроїв. Типовими пристроями що підтримують роботу протоколу SNMP є комутатори, сервери, роутери, кабельні модеми та робочі станції. У моделі OSI цей протокол працює на прикладному рівні. Існує три основні версії протоколу, що є лінійними версіями розвитку протоколу.

SNMP широко застосовується для адміністрування та моніторингу мереж, в яких при застосуванні протоколу виділяються кілька компонентів:

Керуючі пристрої – виконують застосунки які виконують моніторинг та управління керованими пристроями та надають сховище для даних які відстежуються за допомогою протоколу;

Керовані пристрої – різноманітні пристрої у мережі, такі як, наприклад, роутери, сервери, комутатори, кабельні модеми, пристрої IP телефонії, відеокамери, комп'ютери, тощо. Вони передають та зчитують інформацію що відстежується протоколом;

Агент – програмний додаток, що виконується на керованих пристроях, який володіє локальною інформацією та виконує її відправку та отримання.

SNMP сам по собі не диктує тип даних що відстежуються, а надає можливість обмінюватись потрібними адміністратору даними у вигляді змінних. Також протокол надає можливість віддалено виконувати операції адміністрування, таких як, до прикладу, зміна конфігурації мережевих пристроїв. Дані що передаються організовуються за заданими ієрархіями, та описуються базами керованої інформації (management information bases, MIB).

Усі повідомлення SNMP передаються через протокол датаграм користувача (User Datagram Protocol, UDP). Побудова кожного пакету PDU наведена на табл. 4.1:

Таблиця 4.1 – Структура PDU

IP заголовок	UDP заголовок	Версія	Спільнота	Тип PDU	Id запити	Статус помилок	Індекс помилок	Прив'язки змінних
--------------	---------------	--------	-----------	---------	-----------	----------------	----------------	-------------------

SNMPv1 та v2 використовують поле спільноти для встановлення довіри між менеджерами та агентами, являють собою по суті паролі груп.

SNMPv1 визначає п'ять основних типів протоколу об'єктів інформації (Protocol Data Units, PDU), у подальших версіях були додані ще два типи. Загалом, у полі типу пакета визначаються сім типів:

– GetRequest – запит від менеджера до агента на отримання значення або списку значень. Потрібні значення вказуються в полі прив'язки змінних. У відповідь повертається PDU типу Response;

– SetRequest – запит менеджера до агента на заміну значення змінної або списку змінних. У відповідь надсилається Response у якому містяться поточні нові значення змінних;

– GetNextRequest – запит менеджера до агента на знаходження доступних змінних та їх значень;

– GetBulkRequest – запит на декілька ітерацій GetNextRequest, є по суті більш оптимізованою версією цього запиту;

– Response – повертає значення та підтвердження від агента до менеджера. Повідомлення у випадку виникнення помилок подається у полях статус помилки та індекс помилки;

– Trap – асинхронне сповіщення від агента до менеджера, на яке не було запиту від менеджера. Використовується для повідомлення про важливі події та показники;

– InformRequest – підтвержене асинхронне повідомлення призначене для обміну інформацією між менеджерами. В пізніших версіях протоколу дали можливість використовувати так само як і Trap, це дало змогу гарантувати доставку повідомлення через UDP так як повертає підтвердження при отриманні пакету.

SNMP може бути використана зловмисниками для проникнення в мережу, так як протокол часто використовується системними адміністраторами для віддаленого налаштування мережевих пристроїв. Внаслідок цього, рекомендується деактивувати SNMP у мережах де він не використовується для запобігання атак зловмисників.

Архітектура протоколу SNMP складається з чотирьох шарів:

- мережеві диспетчери SNMP – програмний додаток, що запитує інформацію від агентів та виводить її для користувача. В більшості таких додатків можна селективно відображати потрібну інформацію та задавати форму в якій вона буде виводитись;

- мастер агент – це додаток що надає інтерфейс взаємодії між диспетчером та субагентами;

- субагенти – це програма що надає інформацію мастер агенту;

- контрольовані компоненти – це апаратна частина чи програмний додаток, яка створює та підтримує роботу субагента.

Мережа може містити в собі декілька диспетчерів SNMP. Контрольований пристрій може мати лише одного мастер агента, та декілька субагентів і MIB для компонентів пристрою що контролюються. SNMP не визначає протокол за яким взаємодіють мастер агенти та субагенти.

Схематичне відображення архітектури SNMP наведено на рисунку 4.1:

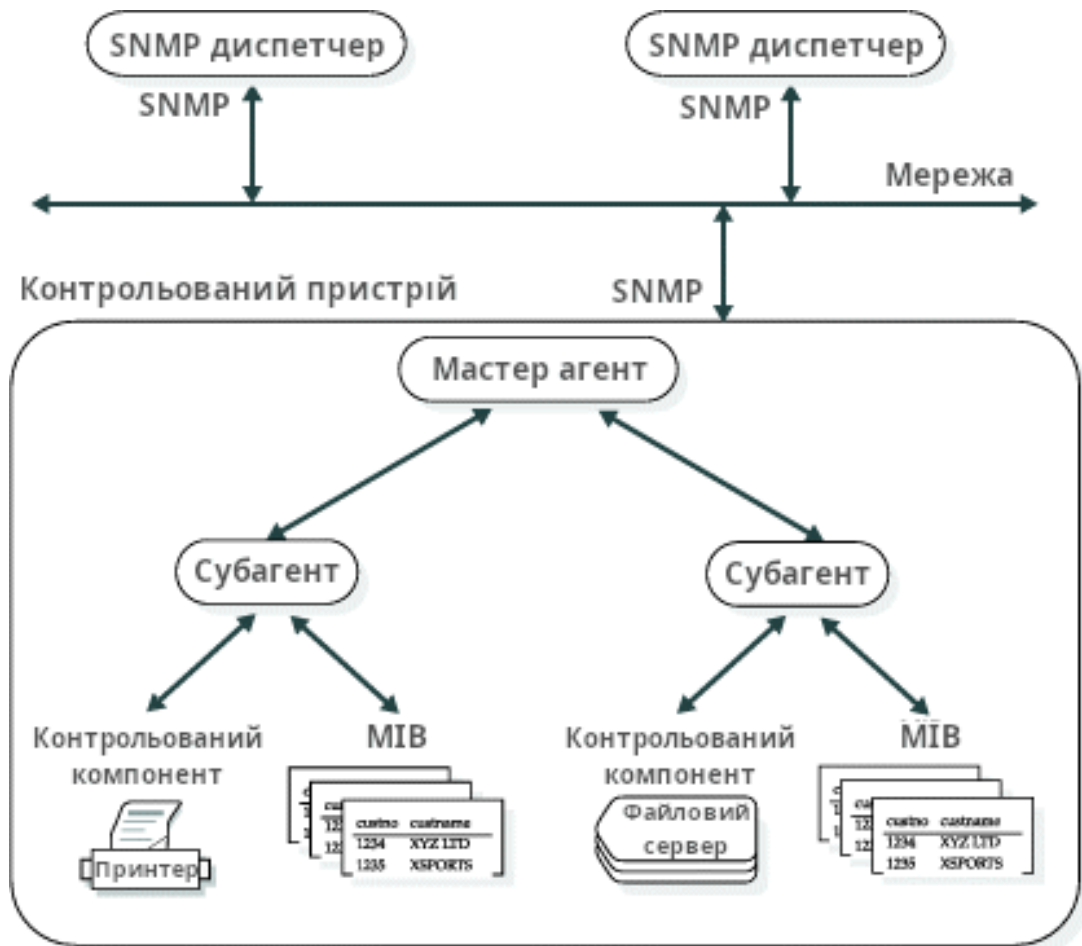


Рисунок 4.1 – Архітектура протоколу SNMP

4.2 Management Information Base

Management Information Base (MIB) це віртуальна база даних що використовується для управління об'єктами в комунікаційних мережах, хоча найчастіше асоціюється саме з протоколом SNMP. Ця база даних є ієрархічною, використовує деревоподібну структуру в якій корінь не має імені (рисунок 4.2). Дані записуються в базу мовою опису даних Structure of Management Information (SMI) яка є адаптованою для SNMP частиною ASN. 1. Керований MIB-об'єкт є будь-якою однією характеристикою керованого пристрою, їх існує два види: скалярні (визначають один екземпляр об'єкта) та табличні (кілька пов'язаних примірників об'єктів згрупованих у таблиці).

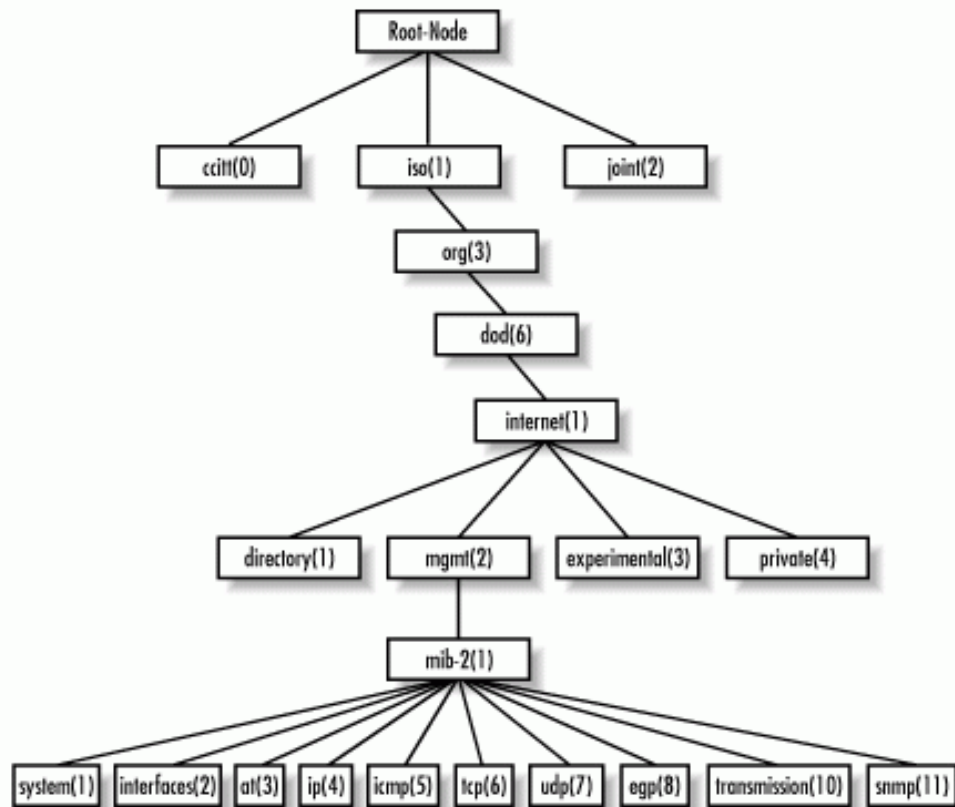


Рисунок 4.2 – Приклад ієрархії стандартної MIB

Типи даних які використовуються в SNMP MIB поділяються на два види: прості типи даних та application-wide типи даних.

До простих типів даних належать:

- цілочисельний тип даних (integer data type);
- рядки октетів (octet strings) – впорядковані послідовності октетів;
- Object ID (OID, ідентифікатори об'єктів).

Існують наступні типи даних application-wide:

– мережеві адреси (Network Addresses) – представляють собою адреси певного сімейства протоколів. SNMPv1 підтримує лише IPv4 адреси, в той час як в SNMPv2 для запису адрес використовують рядки октетів;

– лічильники (Counters) – цілі невід'ємні числа що збільшуються до заданого максимуму, після чого скидаються до нуля;

– датчики (Gauges) – цілі невід'ємні числа що можуть збільшуватись та зменшуватись в заданих межах значень;

– відмітка часу (Time ticks) – представляє кількість часу що пройшла від певної події, вимірюється в мілісекундах;

– Opaques – довільний тип даних який використовується для передачі інформації що не визначена в SMI;

– цілі числа (Integers) – тип даних який передає інформацію у вигляді цілих чисел зі знаком, він перевизначає відповідний тип даних в ASN 1, для того щоб задати обмежену точність в SMI;

– цілі числа без знаків (Unsigned Integers) – передає інформацію у вигляді цілих чисел без знаку, використовується коли знаки не релевантні для даних.

У SNMP версії 2 також додатково визначаються модулі інформації які задають групу пов'язаних значень. Існує три таких модулі:

– MIB-модулі містять визначення взаємопов'язаних керованих об'єктів;
– заяви про відповідність – надають систематичний спосіб опису групи керованих об'єктів, які повинні бути реалізовані відповідно до стандарту;

– заяви про можливість – використовуються для вказівки точного рівня підтримки, який вимагає агент по відношенню до групи MIB.

4.3 Налаштування протоколу SNMP на мережевих пристроях

Налаштування SNMP в мережі складається з двох етапів: налаштування агента SNMP на пристрої який буде контролюватися протоколом, та диспетчера за допомогою якого системний адміністратор буде взаємодіяти із контрольованими пристроями.

У спроектованій мережі в якості контрольованого пристрою буде виступати маршрутизатор R_JS. Для того щоб запустити та провести налаштування SNMP агента необхідно перейти до режиму конфігурації терміналу.

Для того щоб можна було контролювати роботу пристрою за допомогою SNMP, необхідно на даному пристрої активувати SNMP агента.

В даній мережі буде відбуватись моніторинг стану комутаторів та маршрутизатора. Активація агенту виконується командою snmp-server

community, в якості аргументу для якої виступає текстовий рядок що позначатиме спільноту якій буде надано доступ до параметрів пристрою.

Повна команда для активації SNMP на пристроях виглядає наступним чином: `snmp-server community AdminC0mmun1ty rw`, де останній запис RW означає що цій спільноті буде дозволено отримувати та перезаписувати дані на пристрої. Також створено спільноту якій надається право лише на читання записів MIB використовуючи аргумент команди RO, під назвою `Re@dCommunity`.

Таким чином SNMP був налаштований на маршрутизаторі Central (рисунок 4.3), та аналогічно комутаторах Sw_JS1, Sw_JS2 та Sw_JS3.

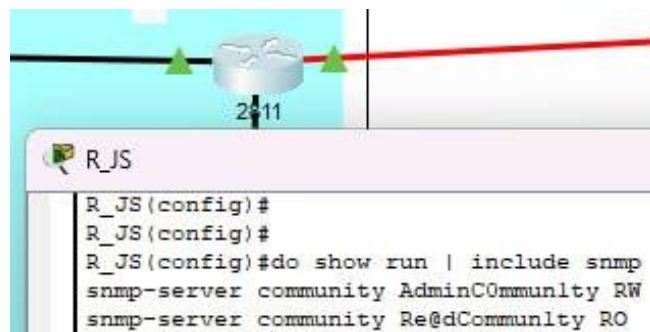


Рисунок 4.3 – Фрагмент файлу конфігурації маршрутизатора R_JS про SNMP

4.4 Тестування роботи протоколу SNMP

Контроль стану пристроїв відбувається з SNMP серверу, який знаходиться у підмережі VLAN20 з адресою 172.25.114.120, за допомогою додатку MIB Browser. В додатку введено IP адресу маршрутизатора та відповідний йому запис спільноти для запису та читання (`AdminC0mmun1ty`). В якості версії протоколу для здійснення запитів обрано SNMPv3 (рисунок 4.4)

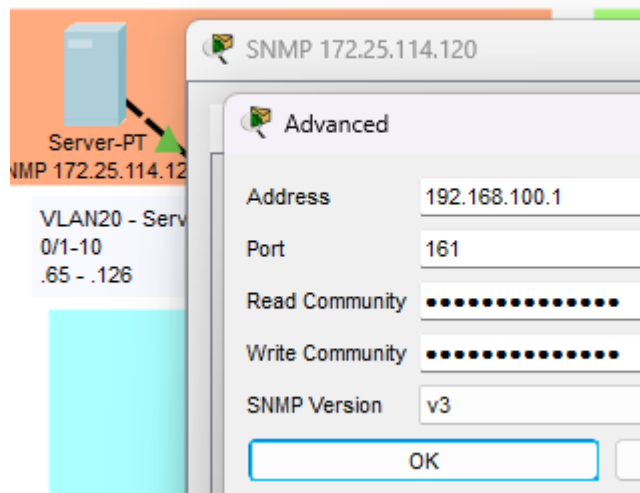


Рисунок 4.4 – параметри MIB Browser на сервері SNMP

Вказавши IP адресу маршрутизатора мережі та текстовий рядок спільноти, було створено запит GET для отримання назви пристрою, яка була виконана успішно (рисунок 4.5), що свідчить про працездатність протоколу.



Рисунок 4.5 – Виконання команди отримання даних про назву пристрою

Далі, виконано перевірку доступності комутатора Sw_JS3. До MIB Browser введено його адресу та виконано запит GET на отримання статусу портів цього комутатора. Запит було виконано успішно, і можна побачити що порти до яких під'єднані комп'ютери активні (рисунок 4.6):

Result Table	
Name/OID	
.1.3.6.1.2.1.2.2.1.8.2 (iso.org.dod.internet.mgmt.mib-2.interfac...	up
.1.3.6.1.2.1.2.2.1.8.3 (iso.org.dod.internet.mgmt.mib-2.interfac...	up
.1.3.6.1.2.1.2.2.1.8.4 (iso.org.dod.internet.mgmt.mib-2.interfac...	up
.1.3.6.1.2.1.2.2.1.8.5 (iso.org.dod.internet.mgmt.mib-2.interfac...	up

Рисунок 4.6 – Статус інтерфейсів комутатора Sw_JS3 які знаходяться у VLAN30

Щоб було зручніше орієнтуватись до яких підмереж під'єднані комутатори, за допомогою SNMP клієнта на сервері командою SET (рисунок 4.7) додано запис до MIB таблиці кожного комутатора інформація в поле .sysLocation у вигляді текстового рядку CustomerAndService_VLAN10-20 – для комутатора Sw_JS2 (рисунок 4.8-4.9), та FinancesAndDev_VLAN30-40 — для комутатора Sw_JS3.

192.168.100.10

SNMP Set ?

OID: .1.3.6.1.2.1.1.6.0

Data Type: OctetString

Value: CustomerAndService_VLAN10-20

OK Cancel

Рисунок 4.7 – Створення запиту на запис інформації в MIB таблиці комутатора Sw_JS2

192.168.100.11

OID: .1.3.6.1.2.1.1.6.0

Operations: Get

Result Table	
Name/OID	Value
.1.3.6.1.2.1.1.6.0 (.iso.org.dod.internet.mgmt.mib-2.system....	

Рисунок 4.8 – Вміст MIB Sw_JS2 до виконання запиту на запис інформації

Result Table	
Name/OID	Value
.1.3.6.1.2.1.1.6.0 (.iso.org.dod.internet.mgmt.mib-2.system....	CustomerAndService_VLAN10-20

Рисунок 4.9 – Результат виконання запиту на запис інформації до MIB Sw_JS2

ВИСНОВКИ

В результаті виконання завдань поставлених у даній кваліфікаційній роботі присвяченій розробці, побудові та налаштуванню комп'ютерної системи для геймінг-кафе «Joy-стік», було досягнуто позитивного результату, який відповідає сучасному рівню технологічного забезпечення у сфері інформаційних технологій.

Комп'ютерна система, що була створена під час виконання роботи відповідає всім вимогам які були висунуті, є продуктивною, надійною та підтримує високий рівень інформаційної безпеки. Розроблена модель може використовуватись не лише для геймінг-кафе, а також може бути адаптованою для потреб компаній, що потребують комп'ютерних мереж загального призначення.

Комп'ютерна мережа була детально налаштована з дотриманням важливих та необхідних практик системного адміністрування. Для ефективної побудови мережі закладу було виконано розділення підмережі на віртуальні підмережі та проведено налаштування маршрутизації між ними. Структура мережі була побудована на основі системи комутаторів, лінії зв'язку між якими були агреговані для утворення каналів даних що мають високу пропускну здатність та відмовостійкість.

Окремо треба визначити впровадження системи моніторингу стану мережевих пристроїв з використанням широко поширеного у сучасних комп'ютерних мережах протоколу SNMP, для забезпечення високої продуктивності шляхом своєчасного виявлення, швидкої діагностики та виправлення збоїв що можливі під час роботи мережі.

Значущість роботи в науковому та науково-технологічному напрямках полягає у розробці та впровадженні засобів та практик мережевого адміністрування, що відповідають новітнім стандартам галузі інформаційних технологій.

ПЕРЕЛІК ПОСИЛАНЬ

- 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 Simple Network Management Protocol (SNMP) [Електронний ресурс]. – Режим доступу: <https://tools.ietf.org/html/rfc1157>
- 3 Мережа cisco – [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/site/us/en/products/networking/access-networking/index.html>
- 4 Маршрутизатор Cisco 2911 (CISCO2911/K9). stack-systems.com.ua - Мережеве обладнання. URL: <https://stack-systems.com.ua/marshrutizator-cisco-2911-k9> (дата звернення: 15.06.2024).
- 5 Роутер ASUS RT-AX1800U Black 802.11ax. [Електронний ресурс]. – Режим доступу: <https://allo.ua/ua/wi-fi-routery/router-asus-rt-ax1800u-black-802-11ax-90ig06p0-mo3530-rt-ax1800u.html>
- 6 Технології моніторингу та трафік-інжинірингу в телекомунікаційних мережах [Електронний ресурс] : підручник для студ. спеціальності 172 «Телекомунікації та радіотехніка» / П. В. Кучернюк; КПІ ім. Ігоря Сікорського. – Електронні текстові данні (1 файл: 5,2 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 257 с.
- 7 Management Information Base for Network Management of TCP/IP-based internets: MIB-II [Електронний ресурс]. – Режим доступу: <https://tools.ietf.org/html/rfc1213>
- 8 A Convention for Defining Traps for use with the SNMP [Електронний ресурс]. – Режим доступу: <https://tools.ietf.org/html/rfc1215>
- 9 Remote Network Monitoring Management Information Base [Електронний ресурс]. – Режим доступу: <https://tools.ietf.org/html/rfc1757>

Додаток А

Текст програми налаштування мережного обладнання в ГК JS

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ
НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ

Текст програми налаштування мережного обладнання

804.02070743.23004-08 12 01

Листів

АНОТАЦІЯ

Дана програма містить зміст конфігураційного файлу маршрутизатора R_JS в геймінг-кафе. Виконується налаштуваннями SSH, параметри домену, IP-адресація інтерфейсів, DHCP та оголошено SNMP.

містить конфігураційний файл комутатора Sw_JS1. Виконується налаштуваннями SSH, параметри домену, IP-адресація VLAN100, налаштування портів доступу та транкових портів, агрегування каналів та оголошено SNMP.

3MICT

1 R_JS_startup-config.txt 3
2 Sw_JS1_startup-config.txt 5

1 R_JS_startup-config.txt

```

!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R_JS
enable secret 5
$1$mERr$NcRNzdORqaj7CP8IRoy47/
!
!
ip dhcp excluded-address 172.25.114.1
ip dhcp excluded-address 172.25.114.65
ip dhcp excluded-address 172.25.114.129
ip dhcp excluded-address 172.25.114.193
!
ip dhcp pool VLAN10
network 172.25.114.0 255.255.255.192
default-router 172.25.114.1
ip dhcp pool VLAN20
network 172.25.114.64 255.255.255.192
default-router 172.25.114.65
ip dhcp pool VLAN30
network 172.25.114.128 255.255.255.192
default-router 172.25.114.129
ip dhcp pool VLAN40
network 172.25.114.192 255.255.255.192
default-router 172.25.114.193
!
!
!
no ip cef
no ipv6 cef
!
!
!
username Kryvosheiev secret 5
$1$mERr$Mo7KLC0.MQWpA9NKVFkKv0
!
!
license udi pid CISCO2811/K9 sn
FTX10173XF0-
!
no ip domain-lookup
!
!
spanning-tree mode pvst
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
encapsulation dot1Q 10
ip address 172.25.114.1 255.255.255.192
!
interface FastEthernet0/0.20
encapsulation dot1Q 20
ip address 172.25.114.65 255.255.255.192
!
interface FastEthernet0/0.30
encapsulation dot1Q 30
ip address 172.25.114.129 255.255.255.192
!
interface FastEthernet0/0.40
encapsulation dot1Q 40
ip address 172.25.114.193 255.255.255.192
!
interface FastEthernet0/0.100
encapsulation dot1Q 100
ip address 192.168.100.1 255.255.255.0
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/3/0
ip address 10.0.0.2 255.255.255.252
!
interface Serial1/0
no ip address
clock rate 2000000
!
interface Serial1/1
no ip address
clock rate 2000000
shutdown
!
interface Serial1/2
no ip address
clock rate 2000000
shutdown
!
interface Serial1/3

```

```
no ip address
clock rate 2000000
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 9
log-adjacency-changes
auto-cost reference-bandwidth 1000
network 10.0.0.0 0.0.0.255 area 0
network 172.25.0.0 0.0.255.255 area 0
!
router rip
!
ip classless
!
ip flow-export version 9
!
snmp-server community AdminC0mmun1ty
RO
!
line con 0
password 7 082F495A294D2F180B
login
!
line aux 0
!
line vty 0 4
login local
transport input ssh
!
!
!
end
```

2 Sw_JS1_startup-config.txt

```

!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime
msec
no service password-encryption
!
hostname Sw_JS1
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface Port-channel1
switchport access vlan 10
switchport mode trunk
!
interface Port-channel2
switchport access vlan 10
switchport mode trunk
!
interface FastEthernet0/1
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/2
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/5
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 20

```

```

switchport mode access
!
interface FastEthernet0/7
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 10
switchport mode access

```

```

!
interface FastEthernet0/19
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/20
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/21
  switchport access vlan 10
  switchport mode trunk
  channel-group 2 mode active
!
interface FastEthernet0/22
  switchport access vlan 10
  switchport mode trunk
  channel-group 2 mode active
!
interface FastEthernet0/23
  switchport access vlan 10
  switchport mode trunk
  channel-group 1 mode active
!
interface FastEthernet0/24
  switchport access vlan 10
  switchport mode trunk
  channel-group 1 mode active
!
interface GigabitEthernet0/1
  switchport trunk native vlan 90
  switchport mode trunk
!
interface GigabitEthernet0/2
  switchport trunk native vlan 90
  switchport mode trunk
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan100
  ip address 192.168.100.10 255.255.255.0
!
ip default-gateway 192.168.100.1
!
!
!
snmp-server community AdminC0mmun1ty
RW
!
line con 0
!
line vty 0 4
  login
line vty 5 15
  login
!
!
!
!
end

```