МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ПрАТ «ПВНЗ «ЗАПОРІЗЬКИЙ ІНСТИТУТ ЕКОНОМІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»

Кафедра інформаційних технологій

ДО ЗАХИСТУ ДОПУЩЕНА

Зав. кафедри _____

д.е.н., доц. С.І. Левицький

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

ПІДВИЩЕННЯ НАДІЙНОСТІ РОБОТИ КОМП'ЮТЕРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ТА ОБЛАДНАННЯ MIKROTIK

Виконав

ст.гр. КІ–112м _____ В.В. Глущенко

Науковий керівник

професор _____ А.В. Переверзєв

Запоріжжя

2024 р.

ПРАТ «ПВНЗ «ЗАПОРІЗЬКИЙ ІНСТИТУТ ЕКОНОМІКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»
Кафедра інформаційних технологій

ЗАТВЕРДЖУЮ
Зав. кафедри
д.е.н., доцент Левицький С.І.
_____
20.10.2023 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ МАГІСТЕРСЬКУ РОБОТУ
студента гр.КІ–112м, спеціальності 123 «Комп'ютерна інженерія»
ОП «Комп'ютерна інженерія»
Глущенка Віталія Володимировича

1.Тема: Підвищення надійності роботи комп'ютерної мережі з використанням технологій та обладнання MIKROTIK
затверджена наказом по інституту (№ 02-25 від 05.12.2022 р.)
2. Термін здачі студентом закінченої роботи: 16.01.2024 р.
3. Перелік питань, що підлягають розробці
1. Огляд актуальних підходів до розвитку комп'ютерних мереж
2. Розглянути існуючі методи покращень комп'ютерних мереж
3. Ознайомитись з вразливостями мереж
4. Підбір обладнанням та додатків MIKROTIK
5. Виявлення корисних конфігурацій обладнання MIKROTIK
6. Налаштування мережі для підвищення надійності
7. Оформити звіт за результатами роботи

4. Календарний графік підготовки кваліфікаційної магістерської роботи

№ етапу	Зміст	Терміни виконання	Готовність по графіку %, підпис керівника	Підпис керівника про повну готовність етапу, дата
1.	Корегування теми кваліфікаційної магістерської роботи, збір практичного матеріалу за темою кваліфікаційної магістерської роботи	17.10.23		
2.	І атестація І розділ кваліфікаційної магістерської роботи	28.10.23		
3.	ІІ атестація ІІ розділ кваліфікаційної магістерської роботи	25.11.23		
4.	ІІІ атестація ІІІ розділ кваліфікаційної магістерської роботи, висновки та рекомендації, додатки, реферат, перевірка програмою «Антиплагіат»	23.12.23		
5.	Доопрацювання кваліфікаційної магістерської роботи, підготовка презентації, отримання відгуку керівника і рецензії	06.01.24		
6.	Попередній захист кваліфікаційної магістерської роботи	10.01.24		
7.	Подача кваліфікаційної магістерської роботи на кафедру	за 3 дні до захисту		
8.	Захист кваліфікаційної магістерської роботи	18.01.24		

Дата видачі завдання: 23.10.2023 р.

Керівник магістерської роботи _____ А.В. Переверзєв
(підпис) (прізвище та ініціали)

Завдання отримав до виконання _____ В.В. Глущенко
(підпис студента) (прізвище та ініціали)

РЕФЕРАТ

Магістерська робота складається: 74 сторінок, включає 9 малюнків, 14 посилань на первинні джерела.

Об'єктом вивчення є впровадження технологій та обладнання MikroTik для підвищення надійності комп'ютерних мереж. Дослідження охоплює розгляд продуктивності та надійності рішень MikroTik в умовах як стабільного, так і менш надійного мережевого з'єднання.

Метою роботи є проведення глибокого розгляду та порівняння ефективності сучасних технологій MikroTik у забезпеченні надійності мережі, що в результаті призведе до розробки обґрунтованих рекомендацій для вибору оптимального рішення.

Для досягнення цієї мети було поставлено конкретні завдання: вивчення проблем вибору протоколу для віртуальної приватної мережі; складання списку протоколів для порівняльного аналізу; визначення метрик та інструментів для вимірювання продуктивності; визначення результатів роботи та порівняння ефективності різних рішень в різних умовах застосування; обґрунтування рекомендацій щодо вибору найбільш надійного протоколу.

Методи, використані в дослідженні, включали практичні підходи, вимірювання та порівняння з аналогічними ресурсами. Отримані висновки можуть стати цінним ресурсом для мережевих адміністраторів, які працюють над підвищенням надійності мережі, особливо в умовах динамічно змінюючихся умов.

MIKROTIK, НАДІЙНІСТЬ, КОМП’ЮТЕРНА МЕРЕЖА, ПРОДУКТИВНІСТЬ, СТАБІЛЬНІСТЬ МЕРЕЖІ, МЕРЕЖЕВІ РІШЕННЯ, ПРОТОКОЛ

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Слово / словосполучення	Скорочення	Умови використання
C		
Center for the Study of Intelligence	CSI	В тексті
E		
Enhanced Interior Gateway Routing Protocol	EIGRP	В тексті
O		
Operating system	OS	В тексті
I		
Internet Protocol	IP	В тексті
Internet of Things	IoT	В тексті
T		
Transmission Control Protocol	TCP	В тексті
V		
Virtual Private Protocol	VPN	В тексті
W		
Wirelless Local Area Network	WLAN	В тексті
Wirelless mesh networks	MESH	В тексті

ВСТУП

У світі стрімкого технологічного розвитку комп'ютерні мережі стають визначальною складовою сучасного підприємництва та індустрії. Надійність і стійкість мережевих інфраструктур є критичними аспектами для забезпечення безперебійної роботи підприємств, надання послуг та ефективного обміну інформацією. У цьому контексті, технології Mikrotik визначають себе як важливий гравець у сегменті розробки та управління мережевим обладнанням.

Ця магістерська дипломна робота ставить перед собою завдання глибокого вивчення можливостей підвищення надійності комп'ютерних мереж з використанням технологій та обладнання Mikrotik. Зростаюча складність мереж, швидкі темпи технологічних змін та постійно зростаючі вимоги до продуктивності накладають великі виклики на адміністраторів мереж і вимагають нових підходів до забезпечення їх надійності.

Розгляд зосереджується на практичному використання можливостей конфігурації, резервуванні каналів та розробці методів моніторингу та відновлення після збоїв з використанням технологій Mikrotik. А саме для того, щоб при необхідності винекнення проблеми, була можливість підвищення надійності. Робота має велике значення для практичного застосування у сферах бізнесу, телекомунікацій, та інших галузях, де надійність мереж визначає успіх та стабільність функціонування.

У контексті постійної необхідності підвищення ефективності мереж та забезпечення стійкості до невідомих викликів, ця робота ставить за мету розширити знання та надати конкретні практичні рекомендації для професіоналів у сфері мережевого адміністрування.

1 АКТУАЛЬНІСТЬ ТЕМИ

У сучасному цифровому епохальному віці, де комп’ютерні мережі виступають як стовп життєвого функціонування підприємств та організацій, питання забезпечення надійності і безперебійності мережевого зв’язку стають критичними.

В умовах ростучої конкуренції, глобалізації та залежності від інформаційних технологій, недостатність ефективності чи надійності мережі може призвести до серйозних фінансових втрат і втрати репутації.[5]

Вибір теми «Підвищення надійності роботи комп’ютерної мережі з використанням технологій та обладнання Mikrotik» базується на кількох ключових обставинах.

По-перше, Mikrotik визнаний як провідний постачальник обладнання для мережевого управління, і його технології здатні забезпечити високий рівень функціональності та гнучкості. Це робить його привабливим кандидатом для вивчення, як засобу забезпечення надійності.

По-друге, зростання об’ємів даних та вимог до швидкодії передачі відображається у необхідності удосконалення мережевих технологій. При цьому Mikrotik володіє рядом функцій, які можуть оптимізувати та забезпечити високий рівень надійності в умовах інтенсивного мережевого трафіку.

Також слід враховувати стрімкий розвиток мережевих технологій та збільшення загроз кібербезпеки, що вимагає від адміністраторів мереж вдосконалених інструментів для забезпечення безпеки та високої надійності.

Отже, обрана тема відображає актуальні виклики, перед якими стоїть галузь мережевого адміністрування, та спрямована на розробку практичних рекомендацій щодо вдосконалення стабільності та ефективності комп’ютерних мереж з використанням передових технологій Mikrotik.

1.1 Загальна характеристика розвитку комп'ютерних мереж

Розвиток комп'ютерних мереж у XXI столітті визначається стрімкістю та несподіваністю змін, що відбуваються в інформаційному суспільстві. Комп'ютерні мережі стали основою для обміну даними, комунікації та доступу до інформації в реальному часі. [5]

Цей розділ роботи розглядає загальну характеристику розвитку комп'ютерних мереж, починаючи від їхнього виникнення та закінчуючи сучасними тенденціями. Початки комп'ютерних мереж можна відстежити до середини XX століття, коли виникла необхідність в обміні даними між великими обчислювальними машинами.

З появою ARPANET у 1969 році відбулося практичне втілення ідеї комп'ютерної мережі. Протягом наступних десятиліть відбувалися значущі події, такі як створення TCP/IP протоколів, що лягли в основу Інтернету, та комерціалізація мережевих послуг у 1990-х роках.

1.1.1 Роль комп'ютерних мереж у сучасному світі

Комп'ютерні мережі стали необхідною складовою сучасного суспільства, вони підтримують економіку, науку, освіту, забезпечують комунікацію та обмін інформацією в усіх сферах життя. Їхнє значення трудно переоцінити, і тому дослідження та вдосконалення їх надійності є важливим завданням для забезпечення стабільності та продуктивності інформаційного суспільства.

У цьому розділі роботи ми провели огляд історії розвитку комп'ютерних мереж, виділили ключові етапи їхнього розвитку, розглянули сучасні тенденції та визначили роль, яку вони відіграють у сучасному суспільстві. Далі буде проведено аналіз літературних джерел та поглиблено дослідження аспектів підвищення надійності комп'ютерних мереж. Комп'ютерні мережі

відіграють ключову роль у сучасному світі і є невід'ємною частиною практично всіх аспектів нашого життя.

Ось деякі з найважливіших ролей комп'ютерних мереж у сучасному світі:

— Зв'язок і Комунікація: Комп'ютерні мережі дозволяють спілкуватися і обмінюватися інформацією незалежно від відстані між користувачами. Це важливо для бізнесу, освіти, наукових досліджень та особистого спілкування.

— Інтернет: Інтернет є найбільшою глобальною комп'ютерною мережею. Він забезпечує доступ до різноманітної інформації, електронної комерції, соціальних мереж, онлайн-освіти та багато іншого.

— Бізнес і Торгівля: Комп'ютерні мережі дозволяють підприємствам здійснювати глобальні операції, співпрацювати з партнерами та клієнтами, обмінюватися інформацією та автоматизувати багато бізнес-процесів.

— Наука і Дослідження: Вчені використовують комп'ютерні мережі для обміну даними, співпраці над дослідженнями та отримання доступу до розширених обчислювальних ресурсів.

— Освіта: Комп'ютерні мережі грають важливу роль у сучасній освіті, дозволяючи студентам і викладачам спілкуватися, обмінюватися матеріалами та здійснювати дистанційне навчання.

— Медицина: Комп'ютерні мережі допомагають обмінюватися медичною інформацією, забезпечують доступ до електронних медичних записів і сприяють розвитку телемедицини.

— Інтернет речей (IoT): Комп'ютерні мережі забезпечують зв'язок для великої кількості підключених пристроїв у сферах таких як автомобільна промисловість, домашня автоматизація, охорона здоров'я та інше.

— Безпека: Комп'ютерні мережі грають важливу роль у забезпеченні безпеки даних і інформації. Мережеві технології допомагають виявляти і запобігати кіберзагрозам.

— Розваги: Споживачі використовують комп'ютерні мережі для стрімінгу відео, музики, гри та інших форм розваг.

— Комп'ютерні мережи стали невід'ємною складовою сучасного суспільства, і їх роль продовжує зростати в контексті швидкого технологічного розвитку.

1.1.2 Проблеми та виклики, пов'язані із забезпеченням надійності мереж

Важливість теми дослідження нерозривно пов'язана з роллю комп'ютерних мереж у функціонуванні інформаційних систем у різних сегментах бізнес-діяльності. Комп'ютерні мережі не лише використовуються для передачі даних і комунікації між автоматизованими вузлами підприємства, але також впливають на управління правами доступу до інформаційних ресурсів, що визначає ефективну імплементацію і застосування інформаційних технологій. Проектування інфраструктури стає критично важливим для забезпечення надійності та захищеності процесів передачі даних, як в межах організації, так і поза нею, а також для їх централізованого зберігання та управління.

У цьому контексті, важливими етапами є розробка критеріїв, які сприятимуть ефективному відображенню реальних бізнес-процесів підприємства на віртуальні, зокрема архітектури, логічної та фізичної топології, типу використовуваного обладнання, засобів захисту та підвищення надійності комп'ютерних мереж. Науково-практична задача включає дослідження методів і засобів забезпечення надійності і захищеності, які б

оцінювали локальні і глобальні критерії, а також надавали рекомендації щодо оптимізації.

Під час проектування, модернізації та супроводу комп'ютерних мереж обов'язково слід враховувати вимоги до забезпечення надійності апаратних засобів, їх продуктивності, фізичного і програмного захисту, а також розмежування прав доступу. Відомі методи, що дозволяють розробляти оптимальні рішення, мають свої обмеження, зокрема узгодженість локальних критеріїв надійності і захищеності, що робить актуальними завдання забезпечення надійності і захищеності, включаючи апаратні та програмні аспекти.

Науково-практичне дослідження вже отримало віддзеркалення в роботах українських та закордонних вчених, але існують проблеми, що потребують подальшого уточнення і розв'язання. Такі завдання включають вивчення методів побудови та забезпечення надійності комп'ютерних мереж, зокрема апаратних і програмних компонентів, з урахуванням потреб сучасного бізнесу.

1.2 Мета та завдання дослідження

У сучасному цифровому епохальному віці, де комп’ютерні мережі виступають як стовп життєвого функціонування підприємств та організацій, питання забезпечення надійності і безперебійності мережевого зв’язку стають критичними. В умовах ростучої конкуренції, глобалізації та залежності від інформаційних технологій, недостатність ефективності чи надійності мережі може призвести до серйозних фінансових втрат і втрати репутації.

Вибір теми «Підвищення надійності роботи комп’ютерної мережі з використанням технологій та обладнання Mikrotik» базується на кількох ключових обставинах.

По-перше, Mikrotik визнаний як провідний постачальник обладнання для мережевого управління, і його технології здатні забезпечити високий

рівень функціональності та гнучкості. Це робить його привабливим кандидатом для вивчення, як засобу забезпечення надійності.

По-друге, зростання об’ємів даних та вимог до швидкодії передачі відображається у необхідності удосконалення мережевих технологій. При цьому Mikrotik володіє рядом функцій, які можуть оптимізувати та забезпечити високий рівень надійності в умовах інтенсивного мережевого трафіку.

Також слід враховувати стрімкий розвиток мережевих технологій та збільшення загроз кібербезпеки, що вимагає від адміністраторів мереж вдосконалених інструментів для забезпечення безпеки та високої надійності.

Отже, обрана тема відображає актуальні виклики, перед якими стоїть галузь мережевого адміністрування, та спрямована на розробку практичних рекомендацій щодо вдосконалення стабільності та ефективності комп’ютерних мереж з використанням передових технологій Mikrotik.

1.3 Формулювання цілей підвищення надійності мережі

Підвищення надійності мережі є критично важливою метою в динамічному світі, де інформаційні технології стають основою практично кожної галузі. Це не просто технічний аспект, але і стратегічна необхідність, яка впливає на ефективність та стійкість різноманітних сфер діяльності.

Головна мета - забезпечити постійний доступ до мережі, навіть у випадку виникнення збоїв чи небезпек для її функціонування. Це може включати планування резервних шляхів, використання механізмів автоматичного відновлення та запобігання однопунктовим точкам відмов.

Ціль - створити мережну інфраструктуру, яка здатна витримувати велику кількість різноманітних викликів, включаючи кібератаки, технічні неполадки та природні катастрофи. Використання декількох різних методів захисту може бути ключовим елементом.

Дуже важливо досягти оптимального балансу між надійністю та швидкодією мережі. Це може включати вдосконалення архітектури, використання швидких комунікаційних технологій та оптимізацію маршрутизації для забезпечення ефективного використання ресурсів.

Комп'ютерні мережі в сучасному світі стали не лише складовою інформаційних технологій, але й основною інфраструктурою для бізнесу, освіти, медицини та громадянського життя. У цьому контексті, підвищення надійності мереж стає важливим завданням, яке визначає стабільність і продуктивність різноманітних сфер діяльності. Розглядаючи цю тему, варто звернутися до ключових аспектів підвищення надійності, сучасних викликів та стратегій, які допомагають забезпечити стійкі та ефективні мережеві системи.

Надійні комп'ютерні мережі визначаються як основний елемент інфраструктури, який забезпечує передачу даних, комунікацію та обмін інформацією. Для бізнесу, це є гарантом безперервності операцій та взаємодії з клієнтами. У сфері науки і освіти, надійні мережі є базовим елементом для дистанційного навчання та досліджень. Для громадянського життя, це забезпечує надійний доступ до інформації та глобальної комунікації.

З плином часу зростає складність та обсяги передаваних даних, що створює нові виклики для надійності мереж. Кіберзагрози, такі як віруси, атаки замахів та кіберпреступність, стають все більш вибагливими та вдосконаленими. Природні катастрофи та технічні збої також можуть викликати серйозні перерви в роботі мереж. Такі виклики вимагають комплексних підходів до забезпечення надійності.

1.3.1 Огляд і аналіз існуючих методів підвищення надійності

В умовах зростаючої залежності від комп'ютерних мереж, питання надійності стає надзвичайно актуальним. З метою забезпечення безперебійного функціонування систем та попередження можливих відмов, було розроблено та впроваджено різноманітні методи та стратегії. Огляд і аналіз існуючих методів підвищення надійності комп'ютерних мереж включає в себе розгляд технологічних рішень, їхні переваги та недоліки, а саме:

1. Резервне Забезпечення (Redundancy):

Резервне забезпечення — це один з основних методів, який включає в себе дублювання ключових елементів мережі, таких як сервери, маршрутизатори, інтерфейси, тощо. У випадку відмови одного компонента, резервний елемент автоматично вступає в роботу.

— Переваги: Забезпечення безперебійного функціонування при відмові. Можливість вдосконалення продуктивності через балансування навантаження.
— Недоліки: Збільшення витрат на обладнання та енергоспоживання та складність у керуванні та обслуговуванні дубльованих систем.

2. Протоколи Динамічного Маршрутизування:

Використання протоколів, таких як OSPA або EIGRP, які автоматично переналаштовують маршрути в разі відмови або змін в мережі.

— Переваги: Адаптивність до змін у мережі та можливість швидкого відновлення маршрутів.
— Недоліки: Значний обсяг ресурсів, необхідних для обчислень та підтримки.

3. Методи Захисту від Кіберзагроз:

— Використання систем виявлення вторгнень, антивірусного захисту та інших засобів кібербезпеки для запобігання відмовам, викликаним кіберзагрозами.

— Переваги: Захист від різноманітних кібератак та програм шкідливого коду. І також дуже важливий фактор, це забезпечення конфіденційності та цілісності даних.
— Недоліки: Потреба в постійному оновленні та адаптації до нових загроз.

4. Методи Моніторингу та Аналізу:

Застосування систем моніторингу, які надають реального часу або післяподійний аналіз подій в мережі для виявлення аномалій та потенційних проблем.

— Переваги: Виявлення відхилень в роботі системи перед виникненням серйозних проблем. А також, можливість оптимізації роботи системи на основі зібраних даних.
— Недоліки: Потреба у великому обсязі обробки та аналізу даних.

Огляд і аналіз існуючих методів підвищення надійності комп'ютерних мереж підкреслює необхідність комплексного підходу. Використання резервного забезпечення, протоколів динамічного маршрутизування, методів кіберзахисту та моніторингу дозволяє створити високонадійні мережі, які відповідають вимогам сучасного інформаційного середовища. Однак ефективність заходів залежить від конкретного випадку використання та врахування специфіки мережі.

1.3 Висновки за розділом

Розділ 1 магістерської дипломної роботи глибоко досліджує актуальність теми розвитку комп'ютерних мереж. Подробиці загальної характеристики розвитку цих мереж визначають необхідний контекст для подальшого розгляду у роботі. Детальне вивчення ролі комп'ютерних мереж в світі розкриває перед нами не лише великий вплив на технологічний прогрес, а й значення для суспільства у цілому.

Сформульовані мета та завдання дослідження чітко визначають шлях подальших наукових розробок та підвищення надійності на практиці

Зазначений у розділі 1 керівний фреймворк стає основою для подальшого розгляду проблем та ефективних стратегій у наступних частинах дипломної роботи. Доповнюючи та уточнюючи інформацію, наведену в цьому розділі, ми забезпечимо більш повний обзор теми та запропонуємо конкретні та обґрунтовані рекомендації для вирішення проблем, пов'язаних з надійністю комп'ютерних мереж.

2 ТЕОРЕТИЧНІ АСПЕКТИ ПІДВИЩЕННЯ НАДІЙНОСТІ МЕРЕЖ

Забезпечення стабільності комп’ютерних систем можна розглядати в контексті двох основних аспектів. У першому випадку, надійність визначається відсутністю відмов, помилок та несправностей. Другий аспект орієнтований на швидке відновлення апаратури та обчислювального процесу в разі виникнення проблем. Термін "надійність" можна розглядати як властивість об'єкта утримувати визначені значення параметрів визначений час, враховуючи його здатність виконувати функції в умовах експлуатації, технічного обслуговування та інших аспектів. Ця властивість об'єднує безвідмовність, довговічність, ремонтопридатність та збереженість.

Надійність визначається як здатність об'єкта утримувати працездатний стан протягом певного періоду часу або наробітку. Наробіток представляє обсяг часу або роботи, що визначається, наприклад, у кількості вирішених задач або циклів роботи.

Відмова - це подія, що викликає порушення працездатності об'єкта, зазвичай пов'язана з фізичним руйнуванням елементів чи поступовим погіршенням їхніх характеристик. Збій визначається як короткочасне порушення роботи обчислювального пристрою або його елемента, яке не потребує ремонту для відновлення працездатності.

Відновлення комп'ютерних систем передбачає відновлення апаратури до працездатного стану за допомогою заміни непрацюючих елементів. Покращення надійності вимагає додаткових витрат на розробку, виробництво та обслуговування систем, а визначення рівня надійності повинно враховувати різноманітні витрати та можливі наслідки відмов. Якщо відмова може призвести до небезпеки або аварії, рівень надійності визначається з урахуванням найвищих стандартів безпеки.

2.1 Огляд технологій Mikrotik

MikroTik - це компанія із Латвії, яка була заснована у 1996 році з метою розробки маршрутизаторів та систем бездротового Інтернет-провайдера. В даний момент MikroTik постачає обладнання та програмне забезпечення для забезпечення доступу до Інтернету в більшості країн світу.

Досвід використання стандартного комп'ютерного обладнання і комплексних систем маршрутизації дозволив компанії у 1997 році створити програмну систему RouterOS, яка забезпечує високу стабільність, контроль і гнучкість для всіх видів інтерфейсів даних і маршрутизації. У 2002 році компанія вирішили виробляти власне обладнання, і народився бренд RouterBOARD. [11]

Огляд їхнього продукту розкриває широкий асортимент пристроїв, відповідних різним потребам – від домашніх маршрутизаторів до складних корпоративних комутаторів.

Ключовими характеристиками обладнання Mikrotik є його висока продуктивність, гнучкість та розширювані можливості. Пристрої виробника відзначаються ефективним використанням ресурсів, що робить їх економічно вигідними та привабливими для різних категорій користувачів.

Важливою особливістю є операційна система RouterOS, яка вбудована в пристрої Mikrotik. Вона базується на ядрі Linux та надає широкі можливості для налаштування та управління мережею. RouterOS підтримує різноманітні мережеві протоколи, VPN, VLAN, а також інші функціональні можливості [9].

Крім того, обладнання Mikrotik вражає своєю апаратною базою. Відмінні характеристики процесорів, кількість та тип портів, можливість встановлення додаткових модулів – все це враховано в розробці пристроїв для забезпечення їхньої найвищої ефективності.

Обладнання Mikrotik легко інтегрується в різноманітні мережеві сценарії завдяки своїм конфігураційним можливостям. Від базових задач, таких як маршрутизація та комутація, до більш складних, таких як

налаштування VPN або контроль пропускної здатності, Mikrotik дозволяє адміністраторам втілювати різноманітні концепції мережевого управління.

Окрім цього, екосистема Mikrotik включає в себе різноманітні інструменти та додатки, які доповнюють функціональність пристроїв. Магазин додатків MikroTik є центром, де користувачі можуть знаходити та встановлювати додатки, які відповідають їхнім конкретним потребам.

Загальний огляд обладнання Mikrotik дозволяє визначити його сильні сторони та виявити можливості для оптимізації та підвищення надійності комп'ютерних мереж. [11]

Надійність операцій технологічних об'єктів є ключовим показником, який визначає престиж компаній-операторів зв'язку. Комп'ютерні мережі, які використовуються такими компаніями, служать ілюстрацією технологічного об'єкта, який потребує постійного підвищення надійності.

На цьому етапі розвитку комп'ютерних інформаційних технологій акцент зроблено на максимальних швидкостях передачі даних на великі відстані корпоративних мереж і використанні резервування елементів будь-якої мережі. У контексті швидкостей передачі даних, використання хмарних технологій і передача великого обсягу інформації від кінцевих користувачів підштовхує до підвищення швидкостей принаймні до 100 Мбіт/с від будь-якого хосту до хосту в інформаційно-комп'ютерних мережах.

На всіх етапах розвитку IT-інфраструктури залишається актуальним питання про надійність технологічних об'єктів, що є складовими частинами корпоративних мереж. Забезпечення надійності роботи всіх елементів та систем зв'язку досягається наближенням коефіцієнта надійності роботи до 0,99, що є важливим як для комутаційних вузлів, так і для кінцевих користувачів.

Одним з ефективних методів підвищення надійності технологічних об'єктів є використання резервування. На відміну від інших видів резервування, часто увага не приділяється обладнанню, яке виступає у ролі

перемикача, але важливо враховувати його надійність при розрахунках надійності системи.

Для підвищення надійності роботи кінцевих користувачів використовуються проекти резервування каналів зв'язку. Наприклад, застосовується радіопідключення як резервування для будь-якої сучасної технології підключення кабелем. Компанія використовує обладнання MikroTik, яке демонструє високий коефіцієнт надійності, щоб забезпечити автоматичне перемикання каналів передачі даних.

Основні фактори, які впливають на надійність корпоративних мереж, включають резервування та його якість, вибір обладнання та його типу для побудови мережі, а також модернізацію мережі за допомогою новітнього обладнання та технологій.

2.2 Використання Mikrotik у сучасних мережевих рішеннях

MikroTik вирізняється в сучасних мережевих рішеннях завдяки широкому спектру можливостей та високій надійності. Його продукція включає в себе різноманітні маршрутизатори, точки доступу та обладнання для створення ефективних бездротових мереж.

Це робить MikroTik важливим гравцем для підприємств, які прагнуть налаштувати стабільні та безпечні мережеві з'єднання. Операційна система RouterOS, яка використовується у пристроях MikroTik, забезпечує адміністраторам широкий функціонал для конфігурації та управління мережею. Це включає в себе можливості налаштування VPN, належний контроль мережевого трафіку, а також засоби для віддаленого моніторингу та управління.

Міцність MikroTik полягає не лише у його технічних характеристиках, але і в ефективному співробітництві з клієнтами. Відзначається тим, що компанія вивчає статистичні дані щодо надійності свого обладнання та

взаємодіє зі спільнотою та партнерами для постійного вдосконалення продукції.

Загалом, MikroTik продовжує залишатися високою якістю рішенням для розвинених мереж, надаючи надійні та інноваційні технології для вимогливих клієнтів у всьому світі. MikroTik використовується в сучасних мережевих рішеннях завдяки своїм передовим технологіям та функціональності. Деякі з основних переваг MikroTik у сучасних мережевих рішеннях включають:

Маршрутизація та Airewall: MikroTik пропонує потужні функції маршрутизації та міжмережевого екрану (airewall), що дозволяє налаштовувати складні мережеві сценарії та забезпечувати безпеку мережі.

Бездротові технології: Продукція MikroTik включає в себе бездротові маршрутизатори та точки доступу, що дозволяє створювати надійні та потужні мережі Wi-Ai для різних застосувань.

Широкі можливості налаштувань: RouterOS, операційна система MikroTik, надає широкі можливості налаштувань, що дозволяє адміністраторам використовувати різні протоколи та сервіси відповідно до вимог мережі.

VPN та безпека: MikroTik підтримує різні протоколи VPN, забезпечуючи безпечний зв'язок між різними точками мережі.

Моніторинг та управління мережею: RouterOS має вбудовані інструменти моніторингу та засоби віддаленого управління, що полегшує ведення мережі та вирішення проблем.

Загалом, MikroTik заслужено користується популярністю в сучасних мережевих рішеннях завдяки своїй надійності, гнучкості та розширеним можливостям налаштувань [9].

2.3 Аналіз проблем та вразливостей комп'ютерних мереж

Аналіз проблем та вразливостей комп'ютерних мереж є важливою складовою стратегії забезпечення безпеки і надійності інформаційно-комунікаційних систем.

Цей процес спрямований на виявлення потенційних небезпек та слабких місць у мережевій інфраструктурі, що можуть стати об'єктом атак та порушень безпеки. Ретельний аналіз дозволяє розібратися в різноманітних аспектах забезпечення безпеки мережі та вжити заходів для їх вирішення.

Однією з ключових задач є визначення різноманітних загроз, які можуть виникнути у вигляді вірусів, хакерських атак, фішингових атак, атак типу DDoS тощо. Проведення такого аналізу дозволяє виявити можливі джерела загроз та розробити ефективні стратегії захисту.

Далі, аналіз вразливостей систем полягає в ретельному перегляді програмного та апаратного забезпечення, а також конфігурації компонентів мережі. Це спрямовано на виявлення слабких місць, які можуть стати лакмусовим папірцем для потенційних атак і несанкціонованого доступу.

Додатково, проведення аудиту безпеки дозволяє виявити можливі порушення політик безпеки та виявити будь-які прояви несанкціонованого доступу. Такий аудит є необхідним для забезпечення високого рівня внутрішньої безпеки [8].

Окрім того, моніторинг мережевого трафіку використовується для виявлення аномалій та підозрілих активностей, що може свідчити про потенційні атаки або несанкціонований доступ. Після завершення аналізу можна розробити та впровадити стратегії для підвищення безпеки мережі та ефективного захисту інформації від потенційних загроз.

Існують чотири дії, пов'язані з інформацією, які можуть представляти загрозу: збір, модифікація, витік і знищення. Ці етапи є основою для подальшого аналізу. Згідно з прийнятою класифікацією, всі загрози

поділяються на внутрішні та зовнішні. Внутрішні загрози охоплюють співробітників організації, програмне забезпечення та апаратні засоби.

Загрози можуть приймати форму помилок користувачів і системних адміністраторів, порушень регламентів збору, обробки, передачі та знищення інформації співробітниками, помилок у роботі програмного забезпечення та відмов комп'ютерного обладнання.

До зовнішніх джерел загроз відносяться комп'ютерні віруси, шкідливі програми, організації, окремі особи та стихійні лиха. Ці загрози можуть призводити до зараження комп'ютерів вірусами, несанкціонованого доступу до конфіденційної інформації, інформаційного моніторингу конкуруючими структурами, дій державних служб із збирання, модифікації, вилучення та знищення інформації, а також аварій, пожеж і техногенних катастроф.Усі наведені види загроз можна поділити на свідомі та несвідомі [8].

За даними Інституту захисту комп'ютерів (CSI) і ФБР, понад 50% вторгнень припадає на дії власних співробітників компаній. Щодо частоти вторгнень, то 21% опитаних повідомили про повторні "напади". Найпоширенішою формою атаки було несанкціоноване змінення даних, особливо у медичних і фінансових установах. Понад 50% респондентів вважають конкурентів можливими джерелами атак.

Особливу увагу приділяють фактам підслуховування, вторгненням в інформаційні системи та атакам, при яких зловмисники фальсифікують зворотню адресу для перенаправлення слідств на невинних осіб. Такі атаки часто здійснюються співробітниками, які порушили закони, та конкурентами.

Аналіз проблем та вразливостей комп'ютерних мереж – це важливий етап у забезпеченні безпеки і надійності інформаційно-комунікаційних систем. Зазначене дослідження дозволяє виявити та розібратися в потенційних ризиках, що можуть виникнути в процесі експлуатації мережі.

Нижче представлено деякі аспекти аналізу проблем та вразливостей комп'ютерних мереж:

— Відомості про загрози: Систематичний аналіз різноманітних загроз, таких як віруси, хакерські атаки, фішингові атаки, DDoS-атаки тощо. Важливо визначити потенційні джерела загроз та їхні методи дії.

— Визначення вразливостей систем: Аналіз програмного та апаратного забезпечення, а також конфігурацій мережевих компонентів для визначення слабких місць, які можуть стати об'єктом атак.

— Аудит безпеки: Проведення систематичного аудиту безпеки для виявлення можливих порушень політик безпеки, недоліків в конфігурації та виявлення неавторизованого доступу.

— Моніторинг мережевого трафіку: Аналіз трафіку для виявлення аномалій та підозрілих активностей, що може вказувати на атаки або несанкціоноаний доступ.

— Оцінка політик безпеки: Перегляд і оцінка ефективності наявних політик безпеки, визначення слабких місць та нестачі заходів безпеки.

— Аналіз соціальної інженерії: Оцінка рівня свідомості та підготовленості персоналу до атак, що базуються на соціальній інженерії.

— Внутрішні загрози: Аналіз внутрішніх загроз, таких як дії невірних працівників або нещасних випадків.

— Оновлення та патчі: Визначення рівня актуальності програмного забезпечення та наявність встановлених патчів для усунення відомих вразливостей.

Після проведення аналізу проблем та вразливостей, можна розробити та впровадити стратегії для підвищення безпеки мережі та захисту інформації.

2.4 Типові несправності та відмови

Комп'ютерні мережі можуть стикатися з різноманітними несправностями та відмовами, які впливають на їхню надійність та ефективність.

Розглянемо деякі типові несправності та можливі відмови в комп'ютерних мережах:

— Втрата з'єднання (Link Aailure): Причина: Пошкодження або від'єднання кабелів, несправні роз'єми, проблеми з мережевим обладнанням.

Можливі заходи: Перевірка фізичного стану кабелів, заміна пошкоджених роз'ємів, перезавантаження мережевого обладнання.

— Проблеми з IP-адресацією: Головною причиною, можуть бути конфлікти IP-адрес, неправильні налаштування DHCP, невірно налаштовані IP-адреси.

Можливі заходи: Перевірка налаштувань DHCP, виправлення конфліктів IP-адрес, перевірка правильності налаштувань маршрутизаторів.

— Атаки та віруси: Причина: Атаки ззовні або внутрішні вторгнення, віруси, шкідливе програмне забезпечення.

Можливі заходи: Встановлення файрволів, антивірусного програмного забезпечення, регулярне оновлення програм та систем.

— Надмірне навантаження (Overload): Причина: Надмірний обсяг даних, велика кількість запитів, неправильне використання ресурсів.

Можливі заходи: Оптимізація мережевого трафіку, впровадження механізмів контролю навантаження, розширення ресурсів.

— Проблеми з безпекою: Причина: Несанкціонований доступ, виток чутливої інформації, незахищені точки доступу.

Можливі заходи: Використання шифрування, встановлення прав доступу, використання віртуальних приватних мереж (VPN).

— Проблеми з маршрутизацією: Причина: Неправильні записи в таблиці маршрутизації, відмови в роботі маршрутизаторів.

Можливі заходи: Перевірка налаштувань маршрутизаторів, виправлення помилок в таблицях маршрутизації.

— Несправні апаратні елементи: Причина: Відмови в роботі комутаторів, маршрутизаторів, мережевих карт та іншого обладнання.

Можливі заходи: Тестування та діагностика обладнання, заміна несправних елементів.

— Проблеми з електропостачанням: Причина: Перебої в електропостачанні, напругові скачки, вимкнення живлення з причино поломки, чи блек-ауту.

Можливі заходи: Використання джерел живлення з резервним електроживленням, застосування стабілізаторів напруги.

Постійний моніторинг та вчасна реакція на несправності є ключовими для забезпечення надійності і безпеки комп'ютерних мереж.

2.5 Методи підвищення надійності мережі

Кожен невдача в роботі комп'ютерної мережі становить серйозні виклики не лише для працівників підприємства та мережних адміністраторів, а й може мати значущий вплив на фінансовий стан організацій. Сучасний розвиток технологій електронних платежів та "безпаперового" документообігу робить локальні мережі ключовим елементом функціонування корпорацій і банків.

Статистика від фірми Inaonetics свідчить, що середньостатистична північноамериканська локальна мережа зазнає близько 23.6 відмов на рік, і витрати на їх усунення становлять у середньому приблизно 5 годин. Вартість цих відмов для власників мережі може сягати від однієї до п'ятдесяти тисяч доларів на годину, враховуючи не лише прямі витрати на ремонт, але й втрати доходу, втрату робочого часу та інші негативні наслідки.

Щодо іноземних компаній, інформації про їхні втрати від відмов у роботі локальних мереж наразі немає відомостей. Проте ймовірно, що проблема відмовостійкості мережі та захисту даних є актуальною і для них. Зазначимо, що деякі російські компанії на початкових етапах свого розвитку можуть віддавати перевагу більш доступним, але менш надійним мережевим рішенням.

За результатами опитування 100 адміністраторів локальних мереж, проведеного фірмою IT у січні цього року, стало відомо, що серйозні збої у мережевому обладнанні та програмному забезпеченні в більшості російських фірм відбуваються щомісяця. Зрозуміло, що захист даних в комп'ютерних мережах наразі стоїть як одна з найбільш гострих проблем в інформатиці.

Сучасна інформаційна безпека ґрунтується на трьох основних принципах:

— Цілісність даних: захист від збоїв, які можуть призвести до втрати інформації, а також від несанкціонованого створення або знищення даних;

— Конфіденційність інформації: забезпечення захисту конфіденційної інформації від несанкціонованого доступу;

— Доступність інформації: забезпечення можливості доступу до інформації для всіх авторизованих користувачів.

Необхідно відзначити, що конкретні галузі, такі як банківські та фінансові установи, інформаційні мережі, системи державного управління, а також оборонні та спеціальні структури, вимагають спеціальних заходів безпеки даних та мають підвищені вимоги до надійності функціонування інформаційних систем, оскільки вони вирішують завдання важливого характеру [6].

У даній ситуації не буде розглядатися проблема спеціальних систем безпеки; ми зосередимося на загальних аспектах захисту інформації в комп'ютерних мережах.

При аналізі питань забезпечення захисту даних в мережі виникає необхідність класифікації відмов та порушень прав доступу, які можуть вести до небажаної модифікації або знищення даних. Серед потенційних "загроз" можна виділити:

1. Збій обладнання:

— Збої в кабельній системі;

— Перебої в електропостачанні;

— Збої в дискових системах;

Неполадки у функціонуванні систем архівації даних.

2. Втрати інформації внаслідок некоректної роботи програмного забезпечення:

— Завада в роботі серверів, робочих станцій, мережевих карт і т. д.;

— Втрата або зміна даних при помилках програмного забезпечення.

3. Втрати, пов'язані з несанкціонованим доступом:

— Втрати внаслідок зараження комп'ютерними вірусами та неправомірного копіювання, знищення або підробки інформації.

— Втрати даних, пов'язані з некоректним зберіганням архівних даних.

4. Помилки персоналу та користувачів при обслуговуванні:

— Ознайомлення з конфіденційною інформацією осіб, не маючих до цього відношення;

— Непередбачене знищення чи зміна даних.

Залежно від можливих порушень роботи мережі, включаючи несанкціонований доступ, різні аспекти захисту інформації можна розділити на два основні класи:

— Засоби фізичного захисту включають заходи для захисту кабельних систем, систем електропостачання, архівації, дисків, та інше.

— Програмні засоби захисту включають антивірусні програми, системи розмежування повноважень, програмні засоби контролю доступу.

— Адміністративні заходи захисту включають контроль доступу до приміщень, розробку стратегії безпеки фірми, плани дій у надзвичайних ситуаціях і т.д.

Важливо зауважити, що цей розподіл є умовним, оскільки сучасні технології спрямовані на поєднання програмних і апаратних засобів захисту. Програмно-апаратні засоби, зокрема, широко використовуються в галузі контролю доступу і захисту від вірусів.

2.6 Резервне керування

Резервне керування є системою або процессом, який використовується для забезпечення продовження роботи або відновлення управління в разі відмови основного управління.

Це стратегічно важлива складова для забезпечення неперервності бізнес-процесів та функціонування систем в умовах виникнення непередбачених ситуацій чи аварій.

Основна мета резервного керування - це зменшити час простою та вплив на продуктивність в разі виникнення проблем у системі. Це може бути досягнуто за допомогою резервування ключових елементів, розподілу навантаження між різними системами або застосування інших стратегій відновлення.

Ключові аспекти резервного керування включають:

— Резервування обладнання: Використання дублюючого обладнання або систем, що готові взяти на себе функції основних елементів при їхній відмові.

— Резервування даних: Збереження копій важливих даних на віддалених серверах чи в інших безпечних місцях для подальшого відновлення.

— Резервування програмного забезпечення: Застосування різних програмних рішень для виконання тих самих завдань, що дозволяє переключатися між ними у разі необхідності.

— Автоматизоване виявлення відмов та відновлення: Використання систем, які можуть автоматично визначати відмови та переходити до резервного варіанту управління.

— Тестування та вдосконалення: Регулярне тестування систем резервного керування для переконання в їхній ефективності та вдосконалення заходів відновлення.

— Плани невідкладних заходів (DRP) та плани відновлення бізнесу (BCP): Розробка та впровадження стратегій та процедур для відновлення бізнес-процесів у найбільш ефективний спосіб.

— Системи моніторингу та аналізу: Використання систем, які надають інформацію щодо стану системи та можливих проблем для швидкого реагування.

Загалом, резервне керування є ключовою частиною стратегії управління ризиками та забезпечення стабільності функціонування систем у будь-яких умовах.

2.7 Методи балансування навантаження

Зі зростанням обсягів інформації виникає нестабільність у поведінці трафіку, що призводить до неочікуваних змін інтенсивності передачі та обмежень у пропускній спроможності каналів. Оскільки завдання балансування навантаження стають важливішими у зв'язку з постійним зростанням навантаження на інформаційні ресурси, їх вирішення стає ключовим для підвищення ефективності використання інформаційних систем.

Широко використовувані технології схильні до збільшення кількості користувачів. Зростання обсягів масового та неконтрольованого мережевого трафіку може викликати непередбачувані об'єми, що призводять до виникнення вузьких місць в деяких каналах та недостатнього використання інших, що може призвести до нерівномірного розподілу навантаження та порушення умов якості обслуговування (QoS). Відтак, існує необхідність в розробці ефективного механізму обробки та передачі трафіку без втрат, що супроводжується підвищенням швидкості передачі за допомогою рівномірного розподілу навантаження (балансування) [4].

Існують два основних типи концептуальних схем балансування навантаження: статичні і динамічні. У статичних схемах розподілу навантаження визначається на етапі проектування розподіленої програми [1]. Статичне балансування навантаження виявляється менш ефективним у забезпеченні оптимальної продуктивності системи через функціональні зміни в мережі, такі як втрата працездатності вузла або ланки та перевантаження попередньо незавантаженого вузла або ланки.

Динамічне балансування навантаження - це процес автоматизованого перерозподілу навантаження системи між обчислювальними ресурсами, враховуючи параметри, такі як масштабованість, продуктивність та відмовостійкість мережевих комплексів для попередження перевантажень. Технологія балансування навантаження використовує автоматизований процес перерозподілу потоків між мережевими ресурсами з метою уникнення перевантажень частини маршрутів та обладнання, забезпечуючи при цьому незавантажені інші.

Однією з основних цілей цього процесу є уникнення зниження працездатності мережі, проте головною метою балансування навантаження є підвищення ефективності роботи мережі. У контексті напрямків досліджень проведено аналіз протоколів динамічної маршрутизації, таких як RIP, EIGRP, OSPA [2].

З урахуванням усіх переваг та недоліків було обрано протокол OSPA для подальшої реалізації механізму балансування навантаження. Цей протокол є найбільш поширеним відкритим протоколом маршрутизації і може бути налаштований на пристроях різних виробників.

Хоча OSPA має деякі недоліки у порівнянні з EIGRP, такі як менша гнучкість та відсутність чіткого опису механізму підрахунку метрики, він також має численні переваги. Серед цих переваг можна відзначити ієрархічний дизайн мережі за допомогою зон, зручність налаштування та підтримку різних вимог IP-пакетів щодо якості обслуговування.

Головною особливістю OSPA є використання метрики пропускної здатності складової мережі для вибору маршруту, де передача даних відбувається по найбільш швидкісних каналах зв'язку. Протокол також може підтримувати різні вимоги стандартів за допомогою окремих таблиць маршрутизації для кожного показника.

Для простого балансування навантаження може використовуватися встановлення однакових метрик на декілька кращих каналів зв'язку. Однак,

важливим недоліком OSPA є висока обчислювальна складність, яка зростає зі збільшенням розміру мережі та вимагає додаткових ресурсів маршрутизатора.

Заради розширення масштабованості протоколу використовується розділення мережі на логічні області, з'єднані магістральною областю. OSPA дозволяє здійснювати ефективне управління мережею шляхом зміни метрик маршрутизаторів, при цьому залишаючи завдання визначення нових метрик важливим завданням. Формула OSPA для розрахунку вартості маршруту використовує параметри пропускної здатності і визначається як стала, залежна від пропускної здатності та швидкості передачі даних (рис. 2.0).

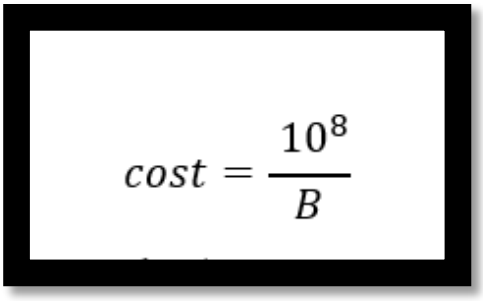

Рисунок 2.0 — Розрахунок пропускної здатності та швидкості передачі даних.

де B – (в бітах на секунду, bps) - це величина, що визначає пропускну здатність інтерфейсу в бітах на секунду.

Для впровадження механізму балансування та управління комп'ютерною мережею за допомогою контролера маршрутизації необхідно розглянути основні аспекти:

— Способи зміни обраних маршрутів.

— Інформація про стан мережі, яку необхідно зібрати для аналізу та вибору маршрутів передачі трафіку.

— Методи отримання даних для аналізу.

— Реакція системи на виникнення раптових або передбачуваних подій. З метою визначення способу зміни обраних

маршрутів розглянемо мережу з двома рівнозначними маршрутами на рис. 1

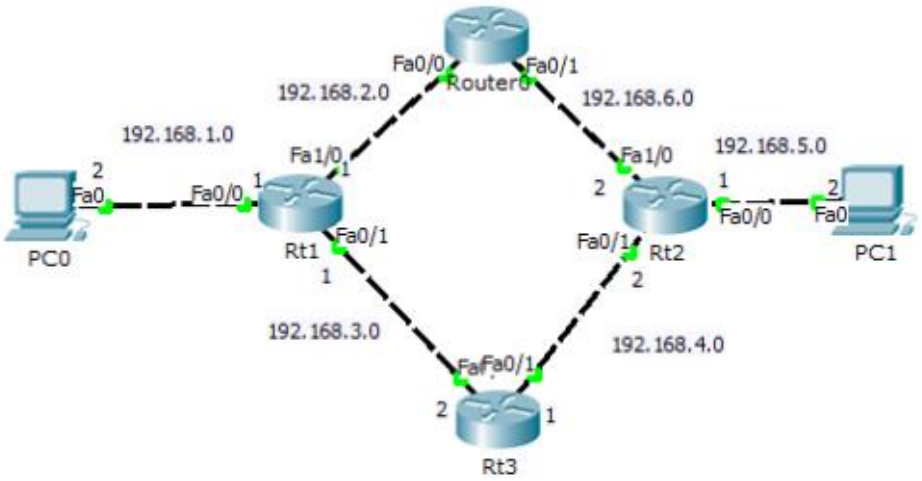

Рисунок 2.1 — Мережа, де налаштований протокол маршрутизації OSPA.

Після налаштування IP-адреси та роботи протоколу OSPA в мережі, функціонування мережі виглядало наступним чином. Усі пакети, що надсилалися з PC0 на PC1, слідували маршрутом PC0-Rt1-Rt3-Rt2-PC1 [10].

Аналізуючи методи визначення маршрутів в OSPA, з урахуванням того, що пропускна здатність інтерфейсу встановлюється за замовчуванням, можна зробити висновок, що вплив на значення маршрутів OSPA можна здійснити двома способами (Рис. 2):

Модифікуючи значення маршруту шляхом зміни параметра "cost" на певному інтерфейсі:

Router(conaig)#interaace aastEthernet 0/1

Router(conaig-ia)#ip ospa cost 100

Змінюючи значення вихідної смуги пропускання - B за допомогою команди інтерфейсу маршрутизатора – bandwith:

Router(conaig)# interaace aastEthernet 0/1

Router(conaig-ia)#bandwidth 1000000

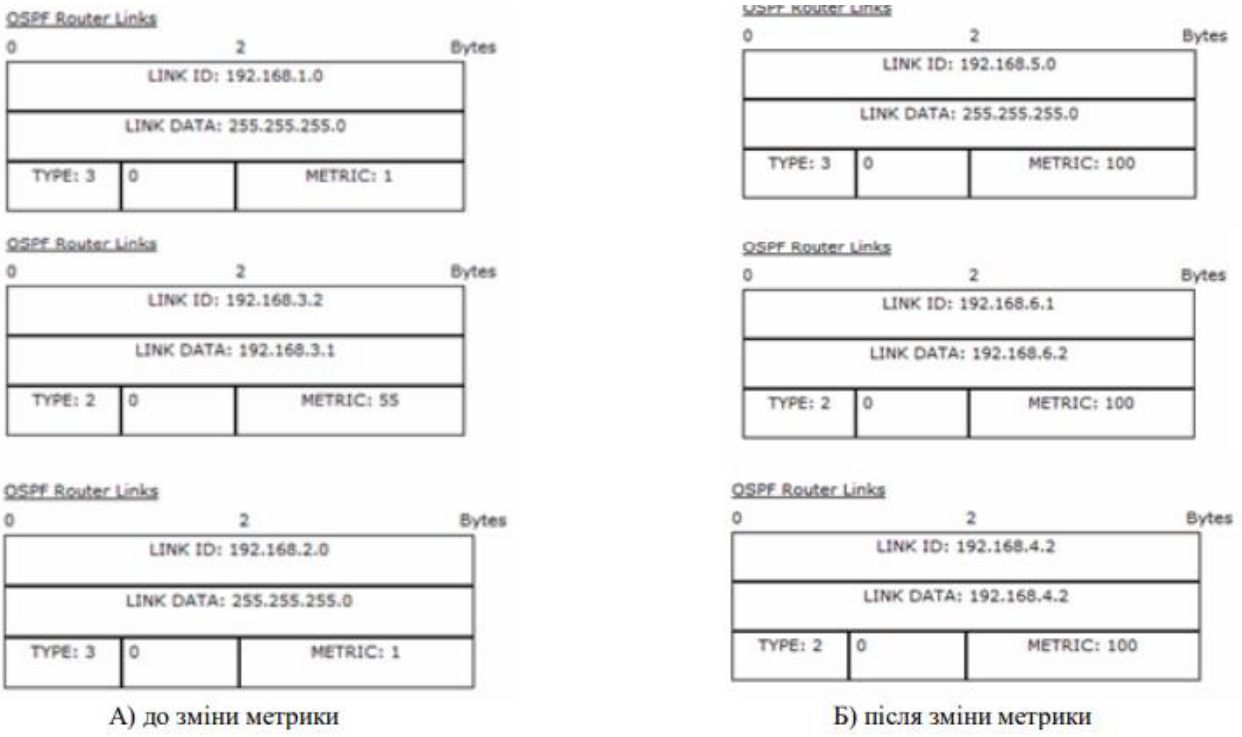

Рисунок 2.3 — Інформаційні пакети.

Після налаштувань, маршрутизатори взаємодіють, обмінюючись інформацією про зміни у мережі та перебудову маршрутів. Таким чином, визначено, як можна змінити вибрані маршрути та впливати на динамічну маршрутизацію протоколу OSPA. На даному етапі необхідно встановити параметри, які будуть характеризувати стан мережі для подальшого аналізу:

— пропускна здатність каналу;

— затримка (час розповсюдження пакету);

— кількість дейтаграм, що очікують у черзі,

— завантаженість каналів та буферів;

— завантаженість центрального процесора маршрутизатора.

Після отримання даних параметрів і їх розрахунку можна визначити загальний комбінований показник, який впливатиме на вибір маршрутів. Система балансування навантаження складається з мережевих пристроїв, контролера та модуля керування.

У цьому контексті контролер повинен отримувати інформацію про обсяг трафіку, що передається в мережі, рівень завантаженості каналів і пристроїв,

дані про черги, завантаженість буфера, а також інші параметри, такі як можливі альтернативні маршрути. Для моніторингу трафіку у мережі може бути використаний власний відкритий протокол NetAlow, розроблений компанією Cisco. NetAlow надає можливість аналізу мережевого трафіку на рівні сесій, реєструючи кожну транзакцію TCP/IP.

Архітектура системи базується на сенсорі, колекторі та аналізаторі:

— Сенсор, розташований на граничних маршрутизаторах сегментів мережі, збирає статистику щодо трафіку, який проходить через нього.
— Колектор виконує збір інформації від сенсорів, а після цього зберігає отримані дані у файл для подальшого аналізу.
— Аналізатор, або система обробки, зчитує ці файли та створює звіти у більш зручному форматі.

Усі маршрутизатори реагують на SNMP-запити контролера, щоб останній міг додавати статичні записи для певних підмереж, змінювати метрику та перенаправляти трафік іншим маршрутом, розділяючи його відповідно до можливої кількості передаваного трафіку без перевантаження альтернативного маршруту. Оскільки контролер періодично відсилає SNMP-запити для отримання поточних станів завантаженості мережевих пристроїв, може виникнути ситуація, на яку треба негайно реагувати на виникнені раптові зміни.

Особливості протоколу маршрутизації OSPA передбачають вбудовані механізми повідомлень для інших маршрутизаторів про зміни в топології мережі, і в такому випадку робота контролера може взяти за основу принципи дії протоколу OSPA. Крім того, важливо передбачити та уникнути максимального завантаження окремих каналів, встановивши порогові рівні завантаження від 60% до 80%, залежно від типу трафіку.

При досягненні відносного порогового значення завантаженості каналів, контролер повинен врахувати виникнення події та перенаправити частину трафіку на альтернативний маршрут.

2.8 Заходи забезпечення безпеки мережі

Система балансування навантаження складається з мережевих пристроїв, контролера та модуля керування. В даному контексті контролер повинен отримувати інформацію про обсяг трафіку, що передається в мережі, рівень завантаженості каналів і пристроїв, дані про черги, завантаженість буфера, а також інші параметри, такі як можливі альтернативні маршрути. Для моніторингу трафіку в мережі може бути використаний власний відкритий протокол NetAlow, розроблений компанією Cisco. NetAlow надає можливість аналізу мережевого трафіку на рівні сесій, реєструючи кожну транзакцію TCP/IP.

Архітектура системи базується на сенсорі, колекторі та аналізаторі. Сенсор (розміщується на граничних маршрутизаторах сегментів мережі) збирає статистику щодо трафіку, який проходить через нього. Колектор здійснює збір інформації від сенсорів, а потім зберігає отримані дані у файл для подальшого аналізу. Аналізатор, або система обробки, читає ці файли та генерує звіти у більш зручному форматі.

Всі маршрутизатори реагують на SNMP-запити контролера, щоб останній міг додавати статичні записи для певних підмереж, змінювати метрику і перенаправляти трафік іншим маршрутом, розділяючи його відповідно до можливої кількості передаваного трафіку без перевантаження альтернативного маршруту. Оскільки контролер періодично висилає SNMP-запити для отримання поточних станів завантаженості мережевих пристроїв, може виникнути ситуація, на яку треба невідкладно реагувати на виникнені раптові зміни.

Особливості протоколу маршрутизації OSPA передбачають вбудовані механізми повідомлення для інших маршрутизаторів про зміни в топології мережі, і в такому випадку робота контролера може взяти за основу принципи дії протоколу OSPA.

Крім того, важливо передбачити та уникнути максимального завантаження окремих каналів, встановивши порогові рівні завантаження від 60% до 80%, в залежності від типу трафіку. При досягненні відносного порогового значення завантаженості каналів, контролер повинен врахувати виникнення події та переспрямувати частину трафіку на альтернативний маршрут [12].

2.9 Висновки за розділом

Розділ 2 "ТЕОРЕТИЧНІ АСПЕКТИ ПІДВИЩЕННЯ НАДІЙНОСТІ МЕРЕЖ" глибоко розглядає технології Mikrotik та їх вплив на підвищення надійності комп'ютерних мереж. Загальний огляд технологій Mikrotik введе нас у світ їхніх основних характеристик та можливостей, а також розгляне їх застосування в сучасних мережевих рішеннях.

У розділі визначено, що Mikrotik відіграє важливу роль у вирішенні завдань комп'ютерних мереж. Зокрема, розглянуто їхню роль у сучасних мережевих рішеннях, визначено переваги та недоліки використання Mikrotik у цих рішеннях. Це надає ключовий внесок у розуміння того, як технології Mikrotik можуть бути використані для забезпечення надійності мереж.

Аналіз проблем та вразливостей комп'ютерних мереж дозволяє нам глибше розуміти потенційні загрози для стабільності мережевого середовища. Це важливо при визначенні стратегій підвищення надійності, оскільки можливі вразливості визначають, на які аспекти слід звернути увагу при впровадженні заходів.

Аналіз типових несправностей та відмов дозволяє ідентифікувати ситуації, які можуть призвести до непрогнозованих проблем. Це допомагає у визначенні конкретних методів підвищення надійності мережі. Перегляд резервних каналів та методів відновлення стає важливим етапом для

гарантії безперебійності роботи мережі під час виникнення непередбачуваних ситуацій.

Розгляд резервного керування та методів балансування навантажень вказує на те, як Mikrotik може бути використаний для забезпечення стійкості та ефективності мереж. Резервне керування виявляється ключовим аспектом стратегій підвищення надійності, а балансування навантажень робить роботу мережі більш оптимальною та ефективною.

На останньому етапі розділу розглядаються заходи забезпечення безпеки мережі. Це важливий аспект, оскільки безпека є невід'ємною частиною надійності. Огляд загроз та використання Mikrotik для забезпечення безпеки надає повніший погляд на заходи, які можна прийняти для збереження цілісності та конфіденційності мережі.

У цілому, розділ 2 ставить основу для подальших досліджень з питань підвищення надійності мереж. Розглянуті аспекти технологій Mikrotik, аналіз проблем та методи підвищення надійності, які висвітлені в цьому розділі, формують теоретичну базу для практичних рекомендацій, які будуть представлені в подальших розділах дипломної роботи.

3 ВИБІР КОНФІГУРАЦІЇ ТА ОБЛАДНАННЯ MIKROTIK

MikroTik пропонує широкий спектр обладнання для мережевих потреб. Вибір конкретної моделі зазвичай залежить від різноманітних факторів, таких як розмір мережі, типи з'єднань, потужність, функціональні можливості та бюджет.

Було підібрано, декілька моделей MikroTik, які можуть бути корисними:

MikroTik hAP ac³ (RB4011 series) (Рис.3) - це багатофункціональний маршрутизатор, який підходить для середніх та великих мереж. Він має вбудований бездротовий модуль, який підтримує стандарти Wi-Ai 5 (802.11ac), що забезпечує швидкі та стабільні бездротові підключення (Рис. 3.0).

Завдяки потужному процесору і оптимізованій архітектурі може ефективно обробляти великий обсяг даних, забезпечуючи стабільну роботу мережі.

Рисунок 3.0 — MikroTik hAP ac³ (RB4011 series)

MikroTik CRS328-24P-4S+RM - це комутатор з 24 портами, з яких 4 порти підтримують SAP+ (10G) з'єднання, що може бути корисним для швидкісного підключення між пристроями або серверами. Має підтримку Power over Ethernet (PoE), що означає, що ви можете живити пристрої через екіпірувані порти, такі як веб-камери або точки доступу Wi-Ai, без додаткових блоків живлення. (Рис. 3.1).

Рисунок 3.1 — MikroTik CRS328-24P-4S+RM

MikroTik RB1100AHx4 - це маршрутизатор, який підходить для великих мереж або сценаріїв з високим обсягом даних. Має потужний чотирьохядерний процесор, який забезпечує високу продуктивність обробки даних. Підтримує різноманітні функції маршрутизації та керування мережею, що дозволяє гнучко налаштовувати його під різні потреби (рис.3.2).

Рисунок 3.2 — MikroTik RB1100AHx4

Крім вибору конкретного обладнання, налаштування програмного забезпечення MikroTik, такого як RouterOS, грає важливу роль у покращенні мережі. Це програмне забезпечення дозволяє налаштовувати маршрутизацію, мережеву безпеку, контроль пропускної здатності, VPN та багато іншого.

Обираючи обладнання MikroTik, важливо врахувати різні фактори, такі як розмір мережі, потреби у пропускній здатності, безпека та бюджет, для забезпечення оптимальної працездатності мережі.

Операційна система RouterOS, розроблена компанією MikroTik для їхнього мережевого обладнання. Вона є важливою частиною функціональності пристроїв MikroTik і надає багато можливостей для налаштування та управління мережею [10].

Ключові аспекти RouterOS:

- Маршрутизація: RouterOS надає широкі можливості для налаштування маршрутизації. Це включає стандартні протоколи маршрутизації, такі як OSPA, BGP, RIP, а також можливості VLAN та маршрутизації на рівні 2 і 3.
- Безпека: Однією з ключових особливостей є широкий спектр засобів захисту мережі, таких як файервол, VPN, фільтрація пакетів, захист від DDoS-атак, IPSec та інші.
- Керування пропускною здатністю: RouterOS дає можливість контролювати промопускну здатність за допомогою QoS (якості обслуговування), що дозволяє пріоритизувати різні типи трафіку для забезпечення оптимальної швидкості та продуктивності для конкретних додатків або сервісів.
- Бездротові технології: RouterOS підтримує бездротові мережі (Wi-Ai) та може бути налаштований як точка доступу, клієнт, мост або репітер, що розширює можливості побудови бездротової інфраструктури.
- Управління і моніторинг: ОС RouterOS має вбудовані інструменти для моніторингу та управління мережею, такі як командний рядок (CLI), графічний інтерфейс користувача (GUI), можливості ведення журналів, SNMP та інші.
- Різноманітність функцій: RouterOS має великий набір функцій, які можна використовувати для налаштування та оптимізації мережі відповідно до конкретних потреб користувача.

ОС RouterOS є передовим засобом для налаштування й управління мережевим обладнанням MikroTik. Вона забезпечує високий рівень контролю та гнучкість налаштувань для різних потреб в мережевому середовищі.

3.1. Вибір оптимальної конфігурації для підвищення надійності

Підвищення надійності комп'ютерної мережі є критично важливим для забезпечення безперебійної роботи та продуктивності. Для досягнення цієї мети існують кілька ключових стратегій, які ми застосуємо:

- Дублювання обладнання: Використання резервних пристроїв (резервні маршрутизатори, комутатори) або резервних компонентів в мережі дозволяє автоматично переходити на резервне обладнання у разі відмови основного.
- Запасні джерела живлення: Встановлення UPS або генераторів дозволяє уникнути відмов у живленні та забезпечити безперебійну роботу мережі навіть під час перебоїв в електропостачанні.
- Застосування резервних каналів: Використання альтернативних шляхів передачі даних або резервних ліній зв'язку знижує ризик відмови мережі через пошкодження або відключення основного каналу.
- Стратегія дублювання даних: Використання RAID-масивів для сховищ даних дозволяє зберігати дані на декількох дисках, зменшуючи ймовірність втрати даних в разі відмови одного з них.
- Стратегія дублювання маршрутизації: Використання протоколів, таких як VRRP (Virtual Router Redundancy Protocol) або HSRP (Hot Standby Router Protocol), дозволяє автоматично переключатися на резервний маршрутизатор у разі відмови основного.
- Регулярне резервне копіювання та тестування: Регулярне створення резервних копій конфігурацій та тестування резервних процедур дозволяє переконатися в готовності мережі до відновлення у разі відмови.

Ці стратегії допомагають підвищити стійкість та надійність комп'ютерної мережі, забезпечуючи безперебійну роботу у випадку відмов або проблем. Налаштування різноманітних резервних систем і процедур дозволяє

забезпечити більш високий рівень доступності та захисту мережі від виникнення непередбачуваних ситуацій.

3.2 Налаштування резервного керування

Резервне управління та підвищення надійності мережі - це не лише опціональні функції, але й критично важливі аспекти для будь-якої комп'ютерної інфраструктури. Ось чому це так важливо:

- Безперебійна продуктивність бізнесу: Недоступність мережі може призвести до припинення роботи бізнесу, що призведе до втрати продуктивності, обмеження доступу до ресурсів та втрати потенційного доходу.
- Збереження даних інформаційних систем: Резервне збереження даних і надійність управління мережею відіграють важливу роль у запобіганні втрати важливої інформації, яка може бути вирішальною для функціонування бізнесу.
- Збільшення доступності та зручності для користувачів: Надійні мережі забезпечують безперервний доступ до ресурсів і послуг для користувачів без перерв або відмов.
- Зменшення витрат: Втрати через відмови мережі можуть бути значними, як у вигляді втрати бізнесу, так і витрат на відновлення систем та відновлення даних. Резервне керування допомагає зменшити ці ризики та витрати.
- Захист від непередбачуваних ситуацій: Резервне управління дозволяє підготуватися до непередбачуваних ситуацій, таких як припинення роботи обладнання, перебої в живленні або природні катастрофи.

Отже, підвищення надійності мережі та налаштування резервного керування є критично важливими для забезпечення стійкості бізнесу та зменшення ризиків у випадку відмов або проблем з мережею. Це дає

можливість підтримувати безперебійну роботу системи та забезпечити високий рівень доступності для користувачів і бізнес-процесів.

3.3 Використання протоколів VRRP та HSRP

VRRP (Virtual Router Redundancy Protocol) та HSRP (Hot Standby Router Protocol) є протоколами, які використовуються для забезпечення високої доступності в комп'ютерних мережах. Обидва протоколи дозволяють створювати віртуальний IP-адресу, яка буде доступна в разі відмови основного маршрутизатора або пристрою.

Отже, основна мета цих протоколів полягає в забезпеченні резервування мережевих пристроїв, таких як маршрутизатори, щоб у разі відмови одного з пристроїв інший можна було автоматично призначити віртуальну IP-адресу і продовжити обробку мережевого трафіку без втрати з'єднання.

Основні відмінності між VRRP та HSRP:

- Власники стандарту: HSRP був розроблений компанією Cisco, тоді як VRRP є стандартом, що був розроблений Інтернет-інженерною робочою групою.
- Номери портів: HSRP використовує порт 1985, тоді як VRRP використовує 112.
- Підтримка вендорами: VRRP є більш універсальним і підтримується різними вендорами мережевого обладнання, тоді як HSRP в основному підтримується тільки пристроями Cisco.
- Як правило, обирають протокол відповідно до вендора обладнання, що використовується в конкретній мережі. Обидва ці протоколи мають схожий функціонал та призначені для однієї мети — забезпечення високої доступності мережі.

Протокол VRRP (Virtual Router Redundancy Protocol) є стандартом, розробленим Інтернет-інженерною робочою групою (IETA), і

використовується для забезпечення високої доступності в комп'ютерних мережах. Основна ідея полягає в створенні віртуального IP-адресу та віртуального маршрутизатора, які використовуються як основні для обробки мережевого трафіку в разі відмови основного маршрутизатора.

Основні принципи роботи VRRP такі:

— Вибір майстра (Master) та стендбай (Standby): Група маршрутизаторів працює разом, один з яких є активним (має статус "майстра"), інший же перебуває в режимі очікування (має статус "стендбая"). Активний маршрутизатор обробляє мережевий трафік, а стендбай очікує на випадок відмови основного.

— Віртуальна IP-адреса: Група маршрутизаторів використовує одну IP-адресу, яка відома як віртуальна. Ця адреса використовується для редиректу мережевого трафіку від користувачів до активного маршрутизатора.

— Обмін повідомленнями: Маршрутизатори в групі постійно обмінюються повідомленнями, щоб визначити, який з них має бути активним. Якщо активний маршрутизатор вийде з ладу або перестане відповідати, стендбай може автоматично стати активним.

— Перехід до нового майстра: У випадку відмови активного маршрутизатора, стендбай автоматично приймає його роль і продовжує обробку мережевого трафіку без перерви.

Використання VRRP дозволяє підвищити доступність мережі шляхом запобігання відмові маршрутизаторів та мінімізації впливу відмов на продуктивність мережі. Цей протокол широко використовується для побудови надійних мережевих інфраструктур у підприємствах та провайдерів послуг.

Протокол HSRP (Hot Standby Router Protocol) також спрямований на забезпечення високої доступності в комп'ютерних мережах, але він був розроблений компанією Cisco і є пропрієтарним протоколом, у порівнянні з більш універсальним стандартом VRRP.

Основні принципи роботи HSRP схожі на VRRP:

— Майстер і стендбай маршрутизатори: Група маршрутизаторів працює разом, один з яких є активним (має статус "майстра"), а інший - в режимі очікування (має статус "стендбая"). Активний маршрутизатор обробляє мережевий трафік, а стендбай очікує на випадок відмови основного.
— Віртуальна IP-адреса: Група маршрутизаторів використовує одну IP-адресу, яка відома як віртуальна. Ця адреса використовується для редиректу мережевого трафіку від користувачів до активного маршрутизатора.
— Обмін повідомленнями: Маршрутизатори в групі постійно обмінюються повідомленнями, щоб визначити, який з них має бути активним. Якщо активний маршрутизатор вийде з ладу або перестане відповідати, стендбай може автоматично стати активним.
— Перехід до нового майстра: У випадку відмови активного маршрутизатора, стендбай може автоматично прийняти його роль і продовжити обробку мережевого трафіку без перерви.

Головна відмінність полягає в тому, що HSRP є пропрієтарним протоколом Cisco, тому він частіше використовується в мережах, де застосовуються пристрої Cisco. В інших випадках, коли важлива взаємодія з пристроями різних вендорів, VRRP може бути більш популярним варіантом через свою універсальність.

3.4 Імплементація бекап-з'єднань та aailover-режимів

Імплементація бекап-з'єднань та режимів aailover є важливими аспектами для забезпечення надійності та високої доступності в мережевих середовищах. Тут є декілька стратегій, які можна використовувати для цього:

1. Redundant Connections (Резервні з'єднання):

— Multiple Physical Links: Використання кількох фізичних з'єднань між двома пристроями або маршрутизаторами для створення резервних шляхів. Це може включати в себе підключення через різні мережеві картки, комутатори або провайдерів.

— Diverse Routing Paths: Використання різних маршрутів або технологій маршрутизації для створення альтернативних шляхів для трафіку.

2. Aailover Modes (Режими aailover):

— Hardware Redundancy: Використання резервних компонентів на апаратному рівні, таких як резервні блоки живлення, дискові масиви, модулі мережевих карток тощо.

— Soatware Aailover: Використання програмних засобів для автоматичного перемикання на резервний пристрій або шлях в разі виявлення відмови або проблеми з основним пристроєм.

3. Протоколи високої доступності (High Availability Protocols):

— Як у попередніх відповідях згадувалося, протоколи, такі як VRRP або HSRP, можуть використовуватись для створення віртуальних маршрутизаторів з можливістю автоматичного переходу до резервного маршрутизатора у разі відмови основного.

4. Monitoring and Detection (Моніторинг та виявлення):

— Використання систем моніторингу для постійного відстеження працездатності мережі та пристроїв.

— Виявлення відмов та автоматична реакція на них, зокрема, автоматичний перехід на резервні пристрої або з'єднання.

5. Конфігурація устаткування:

— Налаштування обладнання для автоматичного переключення на резервні засоби при виявленні відмови основного обладнання.

Імплементація бекап-з'єднань та aailover-режимів варіюється в залежності від конкретних потреб мережі та рівня доступності, який потрібно досягти. Зазвичай, це комбінація фізичних, програмних та мережевих засобів, які працюють разом для забезпечення стабільності та надійності мережі.

3.4 Балансування навантажень та оптимізація ресурсів

Балансування навантажень та оптимізація ресурсів в мережах інформаційних технологій - це ключові практики для ефективності, продуктивності та надійності мережевих систем. Ось деякі стратегії для цього:

1. Load Balancing (Балансування навантажень):

— Трафікове балансування: Розподіл трафіку між різними серверами або маршрутизаторами для запобігання перевантаження одного пристрою та оптимізації ресурсів. Це може бути реалізовано за допомогою різних алгоритмів, таких як Round Robin, Least Connections, або IP Hashing.

— Мережеве балансування: Розподіл навантаження між різними мережевими шляхами для забезпечення ефективного використання доступних ресурсів та підвищення доступності мережі.

2. Content Delivery Networks (CDN - мережі доставки контенту):

— Використання CDN для розподілу контенту (зображення, відео, статичні файли) на різних серверах у різних регіонах для швидшого доступу та зменшення навантаження на основний сервер.

3. Resource Optimization (Оптимізація ресурсів):

— Віртуалізація: Використання віртуалізації для оптимізації використання фізичних серверів та ресурсів.

— Cloud Services (Хмарні сервіси): Використання хмарних рішень для масштабування та оптимізації ресурсів згідно з потребами.

4. Network Monitoring (Моніторинг мережі):

— Постійний моніторинг мережі для виявлення проблем, надання метрик про продуктивність, використання ресурсів та попередження про можливі перевантаження.

5. Application Optimization (Оптимізація програм):

— Покращення ефективності програмного забезпечення для зменшення навантаження на мережу та сервери, використання кешування, оптимізація запитів та обробки даних.

6. Quality oa Service (QoS - Якість обслуговування):

— Встановлення пріоритетів та обмежень на різні типи трафіку для забезпечення найважливіших послуг і призначення ресурсів відповідно.

Ці стратегії можуть використовуватися окремо або в поєднанні, залежно від потреб та характеристик конкретної мережі. Оптимізація ресурсів та балансування навантажень допомагають забезпечити ефективну та стабільну роботу мережі, особливо в умовах високого навантаження чи ризику відмов [7].

3.4.1 Використання технологій балансування навантажень MIKROTIK

MIKROTIK пропонує різноманітні можливості балансування навантажень для мереж на основі своїх пристроїв та програмного забезпечення RouterOS. Ось деякі з основних технологій, що використовуються для балансування навантажень на пристроях MIKROTIK:

1. Load Balancing на основі різних методів:

— PCC (Per Connection Classiaier): Розподіл трафіку на основі хешування параметрів з'єднання, таких як IP-адреса джерела та призначення, порти тощо.

— ECMP (Equal Cost Multi-Path): Розподіл трафіку по різних шляхах з однаковою вартістю для пакетів.
— NTH (Next-Hop-Treshold): Вибір шляху для пакета на основі порядкового номера.

2. Балансування навантажень на рівні шляху (Link Level):

— Підтримка балансування навантажень на рівні шляху для керування розподілом трафіку між різними з'єднаннями, наприклад, між двома або більше інтернет-каналами.

3. Aailover і резервування з'єднань:

— Підтримка автоматичного переходу на резервний з'єднання або шлях в разі відмови основного з'єднання.

4. QoS (Quality oa Service):

— Можливість встановлення пріоритетів та обмежень на різні типи трафіку для забезпечення якості обслуговування.

5. Інтеграція з іншими функціями маршрутизації:

Використання балансування навантажень у поєднанні з іншими можливостями маршрутизації, такими як мережеві фаерволи, VPN, VLAN тощо.

6. Web Proxy та Cache:

— Використання вбудованого проксі-сервера та кешування для зменшення навантаження на зовнішні мережі.

7. Системи моніторингу:

— Можливості моніторингу та журналювання для відстеження продуктивності та використання ресурсів.

MIKROTIK дозволяє налаштовувати різні методи балансування навантажень залежно від потреб конкретної мережі. Це дозволяє оптимізувати роботу мережі та забезпечувати стабільність під час роботи з великим обсягом трафіку.

3.4.2 Оптимізація шляхів маршрутизації

Оптимізація шляхів маршрутизації - це ключовий аспект для забезпечення ефективної та оптимальної передачі даних у мережі. Тут декілька стратегій для оптимізації шляхів маршрутизації:

1. Динамічна маршрутизація: Використання протоколів динамічної маршрутизації, наприклад, OSPA (Open Shortest Path Airst), RIP (Routing Inaormation Protocol), або BGP (Border Gateway Protocol), для автоматичного визначення та вибору оптимальних маршрутів у мережі.

Ці протоколи можуть адаптуватися до змін у мережі та автоматично підбирати оптимальні шляхи.

2. Статична маршрутизація: Вручне визначення маршрутів для конкретних сегментів мережі. Це може бути корисним для фіксованих маршрутів або для обходу певних проблем у мережі.

3. Маршрутизація за політикою: Використання різних маршрутів в залежності від політики та потреб. Наприклад, встановлення пріоритетів маршрутизації для різних типів трафіку або сервісів.

4. ECMP (Equal-Cost Multi-Path): Використання ECMP для розподілу трафіку по різних шляхах з однаковою вартістю.

Це дозволяє маршрутизатору вибирати найкращий шлях для кожного пакету.

5. Технології віртуалізації мережі: Використання технологій віртуалізації мережі, таких як VPN (Virtual Private Network) або VRA (Virtual Routing and Aorwarding), для створення окремих віртуальних мереж з власними шляхами маршрутизації.

6. Monitoring (Моніторинг): Постійний моніторинг мережі для виявлення проблем у шляхах маршрутизації та вчасного реагування на них.

Це допомагає виявляти перегрузки, проблеми у підключеннях чи відмови маршрутизаторів та шукати оптимальні рішення для усунення проблем.

Оптимізація шляхів маршрутизації важлива для забезпечення надійності та ефективності мережі. Це дозволяє підтримувати стабільну та швидку передачу даних у мережі навіть при змінних умовах та навантаженнях.

3.5 Заходи забезпечення безпеки мережі

Мережна безпека - це комплекс заходів, спрямованих на захист інформаційної мережі від несанкціонованого доступу, випадкових або умисних втручань у її роботу та спроб руйнування компонентів. Це включає захист обладнання, програмного забезпечення, даних та персоналу. Політика мережевої безпеки визначає правила та заходи, призначені для запобігання та контролювання несанкціонованого доступу, недопущення неправильного використання, змін чи відмов у роботі мережі. Користувачі отримують доступ до даних через авторизацію - ID, пароль або інші методи перевірки, що визначають їхні повноваження.

Мережева безпека охоплює різні види мереж - від державних до приватних, які використовуються для угод між підприємствами та особами. Вона застосовується у всіх сферах, від корпорацій до особистих мереж. Одним з найбільш поширених методів захисту ресурсів мережі є призначення унікальних імен і відповідних паролів.

Заходи забезпечення безпеки мережі включають широкий спектр стратегій та практик, спрямованих на захист інформації, обладнання та користувачів від потенційних загроз.

Ось кілька ключових заходів:

1. Airewalls (міжмережеві брандмауери): Керування трафіком, фільтрація пакетів та застосування правил доступу для запобігання несанкціонованому входу та вихідним даним.

2. Шифрування даних: Використання шифрування для захисту конфіденційної інформації під час передачі через мережу.

3. Аутентифікація і авторизація:

Встановлення процедур перевірки ідентичності користувачів та призначення прав доступу на основі їхніх ролей у мережі.

4. Оновлення та патчі: Регулярне оновлення програмного забезпечення та оперативних систем для усунення вразливостей та захисту від вторгнень.

5. Моніторинг та журналювання: Системи моніторингу для виявлення незвичайної активності та журналювання для запису подій для подальшого аналізу.

6. Фізична безпека: Заходи безпеки для фізичного обладнання, такі як захищені приміщення, контроль доступу до серверних приміщень тощо.

7. Освіта та навчання користувачів: Навчання користувачів правилам безпеки, створення паролів, виявлення шахраїв та фішингу.

8. Бекапи та відновлення: Регулярне створення бекапів даних та процедури відновлення в разі втрати чи вторгнень.

Ці заходи спільно створюють ефективну систему захисту мережі, запобігають потенційним загрозам та забезпечують стійкість та безпеку інформаційних ресурсів.Заходи забезпечення безпеки мережі включають широкий спектр стратегій та практик, спрямованих на захист інформації, обладнання та користувачів від потенційних загроз [1].

Ось кілька ключових заходів:

1. Airewalls (міжмережеві брандмауери): Керування трафіком, фільтрація пакетів та застосування правил доступу для запобігання несанкціонованому входу та вихідним даним.

2. Шифрування даних: Використання шифрування для захисту конфіденційної інформації під час передачі через мережу.

3. Аутентифікація і авторизація: Встановлення процедур перевірки ідентичності користувачів та призначення прав доступу на основі їхніх ролей у мережі.

4. Оновлення та патчі: Регулярне оновлення програмного забезпечення та оперативних систем для усунення вразливостей та захисту від вторгнень.

5. Моніторинг та журналювання: Системи моніторингу для виявлення незвичайної активності та журналювання для запису подій для подальшого аналізу.

6. Фізична безпека: Заходи безпеки для фізичного обладнання, такі як захищені приміщення, контроль доступу до серверних приміщень тощо.

7. Освіта та навчання користувачів: Навчання користувачів правилам безпеки, створення паролів, виявлення шахраїв та фішингу.

8. Бекапи та відновлення: Регулярне створення бекапів даних та процедури відновлення в разі втрати чи вторгнень.

Ці заходи спільно створюють ефективну систему захисту мережі, запобігають потенційним загрозам та забезпечують стійкість та безпеку інформаційних ресурсів.

3.6 Виявлення та усунення потенційних загроз

Виявлення та усунення потенційних загроз - це критичний аспект забезпечення безпеки мережі. Цей процес включає в себе кілька ключових кроків:

1. Моніторинг та виявлення: Використання систем моніторингу, інструментів аналізу трафіку та спеціалізованого програмного забезпечення для постійного контролю за активністю мережі. Це допомагає виявляти аномалії, незвичайну активність або вторгнення.

2. Інтелектуальні системи виявлення загроз (IDS) та системи захисту від вторгнень (IPS): Використання спеціальних систем, які автоматично виявляють атаки або надзвичайну активність у мережі та реагують на ці загрози шляхом блокування або виконання інших захисних дій.

3. Аналіз та відповідь на інциденти: Реагування на виявлені загрози шляхом аналізу їхньої природи, масштабів та потенційного впливу на мережу. Після цього приймаються заходи для їхнього врегулювання.

4. Удосконалення систем безпеки: Постійне оновлення та удосконалення систем безпеки, включаючи встановлення оновлень програмного забезпечення, конфігураційні зміни та розгортання нових захисних засобів.

5. Планування та навчання персоналу: Створення планів відповіді на інциденти, тренування персоналу щодо виявлення та реагування на загрози безпеки.

6. Аудит безпеки: Проведення регулярних аудитів безпеки для оцінки систем, виявлення слабких місць та розробки стратегій їх усунення.

Ці заходи у поєднанні допомагають виявляти потенційні загрози, надають можливість реагувати на них та покращують загальний рівень захисту мережі від вторгнень та інших небезпечних ситуацій.

3.7 Захист мережевої інфраструктури Mikrotik від атак

Захист мережевої інфраструктури MIKROTIK від атак вимагає комплексного підходу та налаштувань. Ось кілька кроків, які можна вжити для захисту мережі на пристроях MIKROTIK:

Ми блокуємо відповідь на запит PING з WAN портів. Відповідь на PING-запит значно підвищує ймовірність потрапити під приціл хакерів. За статистикою, якщо немає відповіді на PING-запит, то подальші спроби увійти за IP-адресою швидко зменшуються на 40%. Необхідно організувати заборону відповіді з WAN-портів для PING-запитів по опції "echo reply" і запитів по MAC-адресі [2].

Мережа Інтернет становить ключову небезпеку для корпоративної мережі, оскільки через відкриті порти постійно відбуваються спроби підключення до стандартних портів популярних протоколів і служб. Рішенням цієї проблеми є виявлення та блокування всіх IP-адрес, з яких здійснюються спроби це зробити.

/ip airewall ailter add chain=inputaction=add-src-to-address-list in-interaacelist=

WAN src-address-list="!Not_Drops_IP" protocol=tcp dstport=22, 23, 53, 389,

445, 3389, 4569, 5060, 5061, 8291 connection-nat-state=!dstnat address-list=

Drop_Address address-list-timeout=3d comment="Drop TCP traaic"

Також робимо і для трафіку UDP.

63/ip airewall ailter add chain=input action=add-src-to-address-list in-interaacelist=

WAN src-address-list="!Not_Drops_IP" protocol=tcp dstport=53, 161, 389, 4569,

5060 connection-nat-state=!dstnat address-list=Drop_Address

Шляхом використання Airewall Raw ми блокуємо всі виявлені IP-адреси. Додаємо їх до списку "Drop_Address". Це дозволяє нам знизити навантаження

процесора в разі DOS-атак, оскільки Raw-таблиці справляються з цим завданням, роблячи роутер значно стійкішим до атак типу "відмова в обслуговуванні".

Мережа постійно піддається масовому скануванню портів, і спеціальне програмне забезпечення зловмисників шукає слабкі місця у пристроях глобальної мережі, після чого вони приступають до злому (рис.3.0). Це може становити ризик для уразливого пристрою, що може стати частиною якої-небудь нейромережі. Щоб запобігти цій проблемі, необхідно встановити правило для виявлення сканування та подальшого блокування IP-адрес джерела запитів. (рис.3.1-3.2).

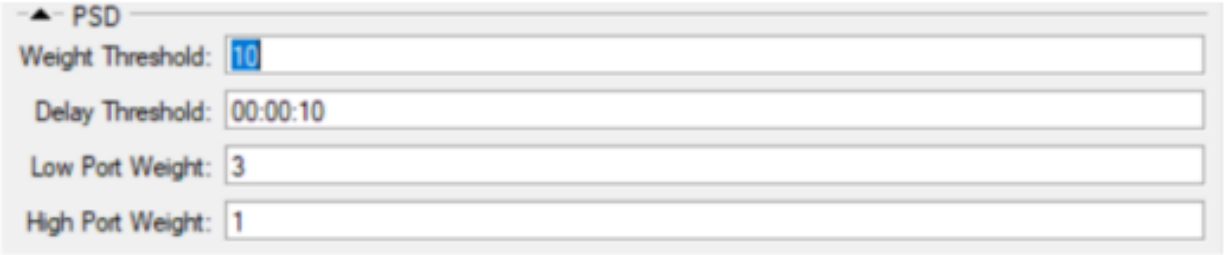

Рисунок 3.0 — Налаштування правила «Чорного списку».

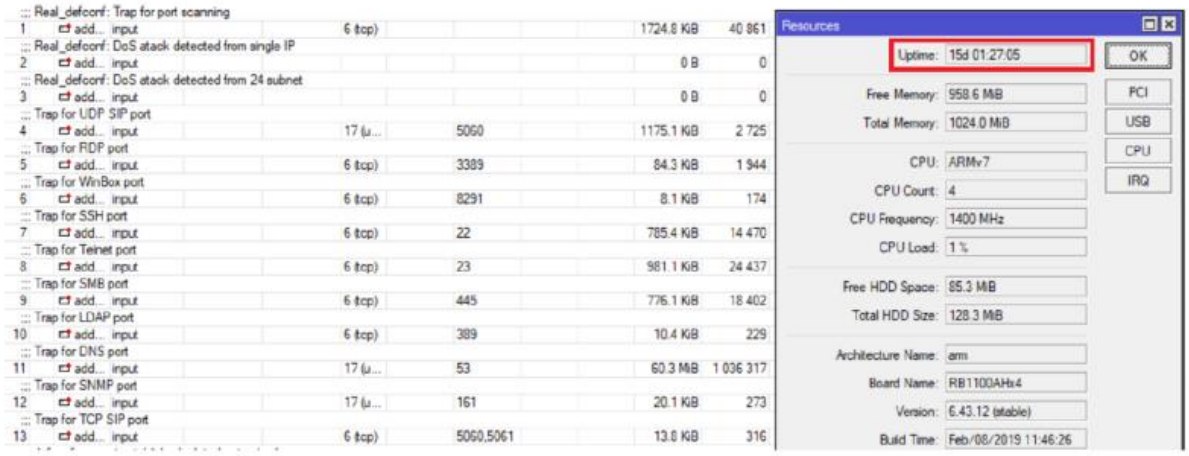

Рисунок 3.1 — Результати налаштування «Чорного списку».

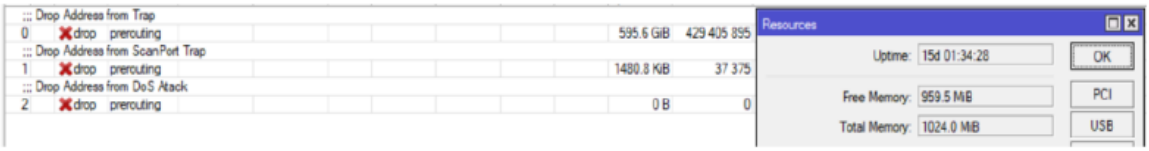

Рисунок 3.3 — Результати налаштування «Raw-таблиць».

Виключаємо можливість розсилки спама з нашої мережі. Щоб виключити варіанти, коли заражені наші пристрої в мережі і спроби ними розсилати запити_ в зовнішню мережу, необхідно виявляти і заблокувати вірусну активність з внутрішньої мережі в мережу Інтернет, щоб не стати джерелом небезпеки для зовнішнього світу.

Для цього необхідно налаштувати блокування найбільш популярних для сканування портів з зовнішньої мережі (наприклад, порти 25, 587, 465), за винятком довірених хостів. Далі додаємо довірені адреси зовнішніх SMTP серверів, через які ми будемо надсилати листи. /ip airewall address-list add address=smtp.gmail.com list=SMTP-External-Servers /ip airewall address-list add address="mail.domain.com" list=SMTP-ExternalServers А також адреси внутрішніх SMTP серверів і клієнтів, які будуть мати право відправляти листи в світ. /ip airewall address-list add address=192.168.0.4 list=SMTP-Internal-ServerClients

Захист від атак типу «відмова в обслуговуванні». Так само необхідно встановити додатковий захист своїх зовнішніх сервісів від атак типу DoS. Для цього ми будемо відловлювати і блокувати ip-адреси, які генерують занадто велику кількість з'єднань, для додавання блокуючого правила в airewall прописуємо наступні команди в консолі RouterOS.

Проблема немаршрутизованого трафіку. У комп'ютерних мережах передається величезна кількість різних запитів, і не завжди вони позначені якоюсь конкретного адресою, тобто ми говоримо зараз про не маршрутизований трафік, так званих Bogon networks. З одного боку, за замовчуванням, маршрутизатор пропускає всі вихідні запити в світ, і якщо ви

є великою компанією з величезною інфраструктурою, то ви можете пристойно засмічувати мережу провайдеру нікому не призначеними запитами, що не є добре. 66 А з іншого боку Bogon networks часто зловмисно використовується хакерами для своїх шкідливих атак. На цю проблему відреагувала організація Internet Engineering Task Aorce (IETA, укр. Інженерний рада Інтернету) і зробила список ip-адрес, рекомендованих до закриття на зовнішні інтерфейси приватних мереж.

Організація резервних копій. Необхідно завжди мати резервні_ копії конфігурації обладнання, а також відправляти ці бекапи на сторонній ресурс, наприклад, файлосховище або на електронну пошту. Ми розглянемо варіант з поштою, тому що atp-сервера може не бути, а електронна пошта є у всіх.

Ні в якому разі не можна використовувати одну і ту ж пошту для відправки та отримання листів, необхідно щоб відправляючий поштовий ящик був створений саме для цієї мети і обов'язково автоматизуємо процес. 67 Для відправки електронної пошти потрібно налаштувати поштову скриньку, як зазвичай рекомендую використовувати командний рядок.

Налаштування системи керування трафіком (QoS). У невеликих комерційних організаціях не так важливо обмежити швидкість, а більше пріоритезувати важливий трафік і мінімізувати вплив на нього другорядного трафіку. Але даний механізм привілейованості будуть діяти тільки для симетричних каналів.

Налаштування VPN-сервера. Для VPN-сервера на MikroTik обираємо протокол L2TP over IPSec, тому що він є одним з найбезпечніших протоколів VPN, досить простий в налаштуванні і VPN-клієнт вже є майже у всіх сучасних системах, як наслідок, немає необхідності встановлювати або налаштовувати якесь додаткове ПЗ, а просто потрібно згенерувати конфігураційний файл, наприклад, для генерації в ОС Windows використовуємо Connection Manager Administration Kit (CMAK), а для MacOS використовуємо Apple Conaigurator 2 і підключаємось.

Налаштування безкоштовного роумінгу за допомогою технології CAPsMAN. Так як у кожного користувача в офісі є одне і більше пристроїв, що працюють з Wi-Ai, а якщо ці користувачі пересуваються по офісу, буде незручно перемикатися від точки до точки вручну, виходом з цієї проблеми буде налаштування технології CAPsMAN. Система CAPsMAN призначена для централізованого управління декількома Wi-F і точками доступу MikroTik. З її допомогою можна налаштувати для Wi-F і точок одне ім'я мережі, пароль для підключення і реалізувати роумінг [13].

Після внесення змін до налаштування CAPsMAN, вони автоматично застосовуються до всіх Wi-Ai точок. CAPsMAN налаштовується на будь-якому роутері MikroTik. Тобто роутер виступає в ролі контролера, а Wi-Ai точки підключаються до нього і отримують налаштування. Повноцінний безшовний роумінг з відсутністю втрат переданих даних є тільки в дуже дорогому обладнанні з застосуванням апаратних контролерів. Однак в будинок, кафе, готель або невеликий офіс таке обладнання можуть дозволити собі далеко не всі.

У недорогих рішеннях як у MikroTik, роумінг відбувається з не великими затримками і втратами даних. Наприклад, при розмові по Skype або Viber при переході від точки до точки на 1-2 секунди може зависнути звук. Якщо ви качаєте файл з сайту, який не підтримує докачку, то при переході станеться обрив, і закачування доведеться виконати заново. При перегляді відео з Youtube перемикання буде непомітно, оскільки дані кешуються. При серфінгу в браузері перемикання так само непомітно.

Налаштування гостьової точки доступа. Не всім Wi-Ai користувачам необхідний доступ до корпоративної мережі, багатьом достатньо простої наявності мережі Інтернет, не кажучи вже щодо можливих гостей компанії, їм доступ в мережу необхідно заборонити. Для цього створимо нову підмережу з доступом тільки в Інтернет. Налаштуємо на вже створеному CAPsMAN гостьову WiAi мережу з доступом тільки в Інтернет.

3.8 Висновок до розділу

Вибір конфігурацій та обладнання є ключовим етапом у нашій роботі, оскільки він фокусується на виборі оптимальних конфігурацій та обладнання для підвищення надійності мережі. Цей розділ розглядає широкий спектр аспектів, починаючи від конфігураційного вибору та закінчуючи заходами забезпечення безпеки та балансуванням навантажень.

Налаштування резервного керування включає в себе використання протоколів VRRP та HSRP.

Імплементація бекап-з'єднань та failover-режимів є необхідною для забезпечення роботи мережі у випадку виникнення проблем з основними з'єднаннями. Це дозволяє мережі швидко переключатися на альтернативні шляхи та мінімізувати вплив можливих відмов.

Балансування навантажень та оптимізація ресурсів стає ключовою стратегією для забезпечення рівномірного розподілу трафіку та використання ресурсів. Використання технологій балансування навантажень Mikrotik, а також оптимізація шляхів маршрутизації, сприяє підтримці стабільності та ефективності мережі.

Заходи забезпечення безпеки мережі включають аспекти захисту від несанкціонованого доступу та мережевих атак. Огляд методів та стратегій захисту допомагає побудувати мережеву інфраструктуру.

Враховуючи заходи забезпечення безпеки, ми створюємо інфраструктуру, яка не тільки оптимізує використання ресурсів, але й максимально ефективно реагує на непередбачені ситуації.

Цей розділ визначає теоретичні основи для подальших практичних застосувань, покращень та рекомендацій, що допоможуть побудувати мережу майбутнього - стійку, швидку та надійну.

4 ПІДСУМКИ ВИВЧЕННЯ ТА ЗАСТОСУВАННЯ НА ПРАКТИЦІ

Покращення надійності комп'ютерної мережі завдяки обладнанню MIKROTIK відображає значний вплив на її ефективність. Мінімізація відмов – це лише один із аспектів, який допомагає створити стійкішу систему. Підвищення швидкості передачі даних, сприятливе впливає на продуктивність мережі, забезпечуючи швидкий та безперебійний обмін інформацією. Оптимізація алгоритмів маршрутизації створює можливість більш ефективно розподіляти дані та знижує час відповіді системи.

Ці зміни не лише поліпшують внутрішні процеси мережі, а й підвищують загальний рівень безпеки. MIKROTIK пропонує різноманітні інструменти для захисту від зовнішніх загроз, включаючи брандмауери, VPN та інші засоби контролю доступу. Це допомагає уникнути атак та зберегти конфіденційність даних. Інтеграція обладнання MIKROTIK може відобразити неабиякі переваги для підприємства чи організації. Вона сприяє покращенню ефективності та продуктивності, зниженню витрат на обслуговування та ремонт мережі, а також робить її менш вразливою до можливих проблем.

Зазначені покращення свідчать про те, що управління мережею за допомогою MIKROTIK може стати ключовим чинником у створенні стабільної, швидкої та безпечної інфраструктури, що відповідає вимогам сучасного світу технологій та забезпечує надійне функціонування мережі у будь-яких умовах.

4.1 Важливість використання технологій MIKROTIK для підвищення надійності мереж

Важливість використання технологій MIKROTIK для підвищення надійності мереж полягає в їхньому потенціалі оптимізувати та покращувати функціональність інфраструктури. Мережі, які використовують обладнання

MIKROTIK, мають можливість бути більш гнучкими та ефективними у керуванні та розподілі ресурсів.

Однією з ключових переваг є зниження відмов. Це особливо важливо для бізнесу, оскільки навіть коротка відмова в мережі може призвести до значних фінансових втрат та втрати репутації. MIKROTIK дозволяє створювати мережі з вищим рівнем надійності через вбудовані механізми резервування, що забезпечує неперервний доступ до даних та сервісів.

Технології MIKROTIK також відіграють важливу роль у підвищенні швидкості передачі даних та оптимізації алгоритмів маршрутизації. Вони дозволяють управляти трафіком мережі більш ефективно, забезпечуючи швидкий обмін інформацією та оптимальний розподіл даних між пристроями.

Крім того, забезпечення безпеки є невід'ємною частиною роботи будь-якої мережі. MIKROTIK надає інструменти для створення брандмауерів, впровадження VPN та контролю доступу, що робить мережу менш вразливою до потенційних загроз зовнішніх атак або несанкціонованого доступу.

У цілому, використання технологій MIKROTIK дозволяє підприємствам та організаціям будувати стійкі, ефективні та безпечні мережі, що є важливим аспектом сучасного бізнесу та розвитку технологій.

Використання технологій MIKROTIK в сфері підвищення надійності мереж є ключовим фактором у забезпеченні ефективності та стабільності інформаційних систем. Ось чому це так важливо:

— Мінімізація відмов та підвищення доступності: Технології MIKROTIK дозволяють розробляти мережі з високим рівнем доступності, які мінімізують відмови і забезпечують постійний доступ до ресурсів.

— Швидкість і продуктивність: MIKROTIK дозволяє оптимізувати швидкість передачі даних та маршрутизацію, підвищуючи продуктивність мережі і забезпечуючи швидкий обмін інформацією.

— Безпека: Ці технології також включають інструменти для забезпечення безпеки мережі, від брандмауерів до VPN, допомагаючи захистити систему від зовнішніх загроз.
— Ефективне управління ресурсами: MIKROTIK надає засоби для ефективного управління ресурсами мережі, що дозволяє оптимізувати їх використання та підтримувати баланс у навантаженні.
— Скорочення витрат: Використання цих технологій може також призвести до зменшення витрат на обслуговування та ремонт мережі, оскільки вона стає менш вразливою до проблем.

4.2 Перспективи подальших вдосконалень

Розвиток технологій у сфері мережевих систем постійно відкриває нові горизонти для дослідження та вдосконалення. У контексті використання технологій MIKROTIK, можливості для майбутніх досліджень безмежні.

Одним із напрямків є пошук оптимальних рішень у сфері маршрутизації. Робота у цьому напрямку спрямована на вдосконалення алгоритмів маршрутизації, що дозволить мережі забезпечувати найбільш оптимальний та швидкий шлях передачі даних, зменшуючи час відповіді та оптимізуючи використання ресурсів.

Далі, розгляду можуть зосередитися на підвищенні рівня безпеки. Це може включати аналіз нових потенційних загроз для мережі та розробку відповідних інструментів для їх запобігання. Інноваційні методи виявлення та блокування загроз, спрямовані на захист від новітніх кібератак, стають ключовими у сучасному цифровому середовищі. Окрім цього, дослідження можуть охоплювати розвиток автоматизованих систем моніторингу та управління мережею. Інтелектуальні алгоритми, що базуються на штучному інтелекті та машинному навчанні, можуть спростити та оптимізувати процеси

управління мережею, реагуючи на проблеми в реальному часі та надаючи прогнозовані рішення.

І нарешті, у сфері розгляду можливий розвиток адаптивних систем, здатних пристосовуватися до змінних умов мережі. Робота над розширенням масштабованості мережі, зокрема її здатності працювати з великим обсягом даних та у високонавантажених умовах, стає актуальною у зв'язку зі зростанням потреб та розвитком технологій.

Ці напрямки вивчення та застосування на практиці можуть відкрити нові можливості для покращення ефективності, надійності та безпеки мережевих систем, забезпечуючи стійку та ефективну інфраструктуру для сучасного цифрового світу.

4.3 Напрямки подальшого вдосконалення технологій MIKROTIK для підвищення надійності мереж

Розвиток технологій MIKROTIK для підвищення надійності мережі є постійним процесом, що має низку перспектив для подальшого вдосконалення. Один з напрямків - це створення адаптивних систем, здатних автоматично реагувати на зміни в мережі. Розробка алгоритмів, які адаптуються до нових умов та забезпечують ефективну роботу мережі навіть у змінних умовах, може бути ключовою для підвищення її стабільності.

Крім того, значна увага приділяється розширенню засобів моніторингу та управління мережею. Розвиток інтелектуальних систем, які не лише виявляють потенційні проблеми, а й роблять прогнози для запобігання виникненню таких ситуацій, може забезпечити більш високий рівень доступності мережі.

Значний акцент також робиться на збільшенні безпеки. В умовах зростаючого кількості кіберзагроз, розробка більш ефективних інструментів виявлення, аналізу та усунення можливих атак стає важливим аспектом для збереження цілісності та захисту даних мережі.

Такі напрямки вдосконалення є ключовими для забезпечення надійності, безпеки та ефективності мережі. Подальший розвиток цих аспектів може допомогти створити мережі, що будуть готові відповідати вимогам майбутнього та працювати навіть у складних умовах, забезпечуючи безперебійний обмін даними та захист інформації.

Звичайно, технології MIKROTIK постійно розвиваються для забезпечення ще більшої надійності комп'ютерних мереж. Ось деякі напрямки, які можуть бути вдосконалені:

— Автоматизація та оптимізація маршрутизації: Подальше вдосконалення алгоритмів маршрутизації для автоматичного вибору оптимальних маршрутів, враховуючи різні параметри мережі та умови, для забезпечення швидкості та ефективності передачі даних.

— Резервне керування та відновлення після відмов: Розробка ще більш ефективних методів резервування, які дозволяють автоматично переключати трафік у разі відмови основного каналу для мінімізації перерв у роботі мережі.

— Інтелектуальна система моніторингу та прогнозування проблем: Розробка систем, які за допомогою аналізу даних можуть передбачати можливі несправності або проблеми в мережі та надавати рекомендації для їх запобігання.

— Розширення засобів безпеки: Подальший розвиток систем захисту мережі від нових загроз, включаючи розробку більш інтелектуальних інструментів виявлення потенційних загроз та систем управління доступом.

— Підвищення масштабованості та швидкості роботи: Розробка технологій, які дозволять мережі більш ефективно працювати з великим обсягом даних та високим рівнем навантаження, забезпечуючи при цьому швидку передачу даних.

4.4 Можливості розширення дослідження в інших сферах інформаційних технологій

Розширення досліджень у сферах інформаційних технологій є нескінченним процесом, оскільки вони застосовуються у різних сферах життя.

Ось кілька можливих напрямків:

— Медицина та охорона здоров'я: Розвиток систем штучного інтелекту для аналізу медичних даних та підтримки в прийнятті рішень лікарями. Використання сенсорів та пристроїв для збору даних про здоров'я пацієнтів у реальному часі.

— Енергетика та екологія: Розробка технологій для збереження енергії та створення нових джерел чистої енергії. Використання даних для прогнозування екологічних змін та управління ресурсами.

— Транспорт і логістика: Впровадження систем автономних автомобілів та оптимізація логістичних процесів за допомогою алгоритмів штучного інтелекту.

— Фінанси та банківська справа: Використання блокчейн-технологій для забезпечення безпеки транзакцій та розвитку нових фінансових інструментів.

— Педагогіка та навчання: Розвиток онлайн-платформ для навчання з використанням інтерактивних методик та адаптивного навчання з врахуванням потреб кожного учня.

Ці напрямки досліджень у сферах інформаційних технологій не лише показують широкий спектр можливостей, але й відображають суттєвий вплив на суспільний розвиток. Подальше розширення досліджень у цих галузях може призвести до виникнення нових інновацій, що стануть важливими для вирішення глобальних проблем.

Продовження досліджень у медицині може призвести до винайдення нових методів лікування та діагностики хвороб, покращуючи якість життя

людей. Розвиток енергетики та екології забезпечить більш сталий та ефективний використання ресурсів, сприяючи збереженню природних екосистем.

Технологічний прогрес у різних сферах, від транспорту до фінансів, відкриває можливості для створення більш зручного та безпечного світу.

Продовження наукових досліджень та впровадження нових рішень може мати значний вплив на наше життя та сприяти загальному просуванню суспільства.

4.5 Висновки за розділом

Підсумки вивчення є завершальним етапом нашої роботи, де ми аналізуємо отримані результати, визначаємо важливість використання технологій MikroTik для підвищення надійності мереж та розглядаємо перспективи подальших досліджень.

Важливість використання технологій MIKROTIK для підвищення надійності мереж засвідчується на основі проведених досліджень. Використання MikroTik дозволяє не лише підвищити стійкість мережі, але й оптимізувати ресурси, забезпечуючи ефективне управління трафіком та роботою обладнання.

Перспективи подальших досліджень вказують на необхідність розвитку та вдосконалення існуючих технологій MikroTik. Однією з перспектив є глибше дослідження можливостей балансування навантажень та резервного керування, щоб досягти максимальної ефективності в умовах різноманітних сценаріїв використання.

Напрямки подальшого вдосконалення технологій MIKROTIK для підвищення надійності мереж включають в себе оптимізацію алгоритмів балансування, підвищення безпеки та розширення можливостей конфігурацій для різних типів мереж та умов використання.

Можливості розширення дослідження в інших сферах інформаційних технологій вказують на перспективи використання здобутих знань в інших областях, таких як розробка програмного забезпечення, виробництво мережевого обладнання та розгортання комплексних мережевих інфраструктур.

У цілому, розділ 4 закріплює ключові висновки дослідження. Використання технологій MikroTik виявилося важливим чинником для забезпечення стійкості та надійності мереж. Подальші дослідження та вдосконалення цих технологій відкривають шлях для побудови ще більш ефективних та стійких мереж майбутнього.

ВИСНОВОК

Магістерська робота ретельно дослідила питання підвищення надійності роботи комп'ютерної мережі з використанням технологій та обладнання MikroTik. В процесі дослідження були вивчені та розглянуті різноманітні аспекти, пов'язані з функціональністю, налаштуваннями та можливостями, які надає вказане обладнання.

Застосування технологій MikroTik виявилося важливим кроком у підвищенні ефективності та надійності комп'ютерних мереж. Серія рішень, що пропонує MikroTik, дозволяє ефективно керувати та контролювати мережевий трафік, забезпечуючи високий рівень безпеки, стабільності та доступності.

У процесі виконання поставлених завдань було проведено розгляд актуальних проблем та викликів у сфері комп'ютерних мереж. Огляд сучасних підходів надав можливість визначити стратегічні напрямки розвитку, зокрема звертаючи увагу на технології, які домінують у галузі, такі як SDN (Software-Defined Networking) та використання хмарних рішень для оптимізації ресурсів.

Аналіз існуючих методів покращень комп'ютерних мереж дозволив ідентифікувати ефективні та інноваційні підходи. Зокрема, акцент був зроблений на використанні алгоритмів маршрутизації, удосконаленні технік QoS (Quality of Service) та впровадженні механізмів моніторингу трафіку для виявлення проблем.

Детальний огляд вразливостей мереж дозволив зосередитися на аспектах безпеки. Були визначені загрози, пов'язані зі зловживанням протоколів, атаками на рівні даних та можливими прослуховуваннями. Це дозволило розробити стратегію забезпечення мережевої безпеки та план заходів для запобігання можливим атакам.

Підбір обладнання та додатків від MIKROTIK виявився ключовим етапом, оскільки це вирішення забезпечує високий рівень функціональності та надійності. Вивчення корисних конфігурацій обладнання дозволило визначити оптимальні налаштування для досягнення максимальної продуктивності.

На основі отриманих даних було проведено налаштування мережі, спрямоване на підвищення її надійності та оптимізацію роботи. Це включало в себе балансування навантаження, резервне копіювання даних та впровадження механізмів автоматичного відновлення підключень.

Завершальним етапом було складання звіту, в якому були представлені детальні висновки щодо кожного етапу роботи, а також рекомендації для подальшого розвитку та підтримки мережевої інфраструктури. Звіт відображав виконані завдання, виявлені труднощі та запропоновані шляхи вирішення проблем, що дало повністю обґрунтований підхід до розвитку комп'ютерних мереж.

Таким чином, результати цієї магістерської роботи підтверджують актуальність та ефективність використання технологій MikroTik у практичній діяльності для підвищення надійності та ефективності комп'ютерних мереж. Вони можуть бути корисними для фахівців у галузі інформаційних технологій та мережевого адміністрування для подальших досліджень та впровадження нових технологій у роботу мереж.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Оглтрі Т.В. Airewalls. Практичні застосування міжмережевих екранів. «ДМК», М., 2008. - 109 с .;

2. Бірюков А.А. Інформаційна безпека: захист і напад. 2-ге вид. «ДМКПресс», М., 2017. – 347 с.

3. Аудит інформаційної безпеки навч. посібник для вузів / В.І. Аверченков. – 3-те вид. – М.: ФЛІНТА, 2016. – 269 с.

4. Біячуев Т.А. Безпека корпоративних мереж. СПб., 2008. - 327 с.;

5. Щеглов А.Ю. Захист комп'ютерної мережі від несанкціонованого доступу. «НиТ», СПб., 2009. - 202 с.;

6. Зіглер Р. Брандмауери в Linux. «Вільямс», М., 2009. - 74 с .; 7. Яковлєв В.Ю. Міжмережеві екрани, Спб., 2009. - 32 с .;

8. Ubiquiti vs Mikrotik: веб-сайт. URL: https://aorum.mikrotik.com/viewtopic.php?t=82501#p415257;

9. Mikrotik Router OS - описание и возможности: веб-сайт. URL: https://lanmarket.ua/stats/mikrotik-router-os-opisanie-i-vozmozhnosti;

10. За что я люблю и ненавижу MIKROTIK: веб-сайт. URL: https://mum.mikrotik.com/presentations/MD19/presentation_7212_1568363147.pda;

11. Спецификация MikroTik RB4011iGS+RM: веб-сайт. URL: https://mikrotik.com/product/rb4011igs_rm#andtn-speciaications

12. Ubiquiti EdgeRouter 12P (ER-12P) Маршрутизатор: веб-сайт. URL: (openarchive.nure.ua) http://ubiquiti.net.ua/ubiquiti-edgerouter-12p-er12p?keyword=Ubiquiti%20EdgeRouter%2012;

13. CVE's aor routeros: веб-сайт. URL: http://cve.circl.lu/search/mikrotik/routeros (дата звернення: 15.12.2019); (openarchive.nure.ua) 90

14. Немаршрутизируемые в Интернет адреса (bogon networks) и безопасность: веб-сайт. URL: https://www.securitylab.ru/blog/personal/aodugin/305208.php