Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: Методи резервування та керування трафіком комп'ютерних мереж з використанням маршрутизатора MikroTik

Виконав: студент (ка) VI курсу, групи СІм-61
Спеціальності:
123 "Комп'ютерна інженерія"
(шифр і назва спеціальності)

Коцюк Н. М.
підпис (прізвище та ініціали)

Керівник Луцик Н. С.
підпис (прізвище та ініціали)

Нормоконтроль Тиш Є.В.
підпис (прізвище та ініціали)

Завідувач кафедри Осухівська Г. М.
підпис (прізвище та ініціали)

Рецензент Никитюк В. В.
підпис (прізвище та ініціали)

м. Тернопіль – 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г. М.*
(підпис) (прізвище та ініціали)
«__» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *магістр*
(назва освітнього ступеня)
за спеціальністю *123 Комп'ютерна інженерія*
(шифр і назва спеціальності)
Студенту *Коцюку Назару Мирославовичу*
(прізвище, ім'я, по батькові)
1. Тема роботи *Методи резервування та керування трафіком комп'ютерних мереж з використанням маршрутизатора MikroTik*

Керівник роботи *Луцик Надія Степанівна*
доктор філософії, доцент кафедри комп'ютерних систем та мереж
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджені наказом ректора *від « 01 » 12 2023 року № 4/7-1132*
2. Термін подання студентом завершеної роботи *22.12.2023*
3. Вихідні дані до роботи *Вимоги до системи резервування та керування трафіком, маршрутизатор MikroTik*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ.
1. Аналіз існуючих варіантів рішень та їх порівняння.
2. Засоби створення лабораторного середовища системи резервування.
3. Розробка системи резервування та керування трафіком.
4. Охорона праці та безпека в надзвичайних ситуаціях.
Висновки.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1 Актуальність теми, мета і завдання дослідження, об'єкт та предмет дослідження.
2 Методи дослідження, наукова новизна та практична цінність одержаних результатів.
3 Схема мережі лабораторного середовища на базі маршрутизатор MikroTik CHR.
4 Блок-схема алгоритму роботи системи резервування та керування трафіком.
5 Мережеві налаштування маршрутизатора MikroTik.
6 Лістинг фрагментів програмного коду системи резервування.
7 Приклади повідомлень про зміну маршрутизації.
8 Висновки.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	*Осухівська Г.М., к.т.н., доцент*		
Безпека в надзвичайних ситуаціях	*Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва*		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Вступ*		*Виконано*
2.	*Аналіз існуючих варіантів рішень та їх порівняння*		*Виконано*
3.	*Засоби створення лабораторного середовища системи резервування*		*Виконано*
4.	*Розробка системи резервування та керування трафіком*		*Виконано*
5.	*Охорона праці та безпека в надзвичайних ситуаціях*		*Виконано*
6.	*Висновки.*		*Виконано*
7.	*Оформлення пояснювальної записки*		*Виконано*
8.	*Оформлення графічної частини*		*Виконано*
9.	*Попередній захист кваліфікаційної роботи магістра*		*Виконано*
10.	*Захист кваліфікаційної роботи*		

Студент _____ *Коцюк Н.М.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Луцик Н.С.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи резервування та керування трафіком комп'ютерних мереж з використанням маршрутизатора MikroTik //Кваліфікаційна робота магістра // Коцюк Назар Мирославович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних систем та мереж, група СІм-61 // Тернопіль, 2023 // с. – 73, рис. – 32, аркушів А1 – 8, додат. – 3, бібліогр. – 14.

Ключові слова: MikroTik, резервування, зв'язок, трафік, надійність, скриптова мова, програмний код.

Кваліфікаційну роботу присвячено дослідженню методів керування та резервування каналів зв'язку для забезпечення надійності та високої доступності в комп'ютерних мережах. Проведено порівняльний аналіз можливостей Cisco, MikroTik, Juniper, Palo Alto та Fortinet щодо здатності автоматично переходити на альтернативний канал зв'язку. Досліджено можливості надсилання сповіщень через різні канали комунікації, такі як електронна пошта та SMS, про перехід на резервний канал. Вивчено мережеві можливості маршрутизатора MikroTik. Розроблено програмний код для автоматичного переходу на резервний канал з можливістю інформування за допомогою електронної пошти та SMS. Була оцінена здатність системи забезпечувати стабільність мережі, моніторинг, відновлення після збоїв і інформування в критичних сценаріях.

ABSTRACT

Methods of reserving and managing traffic in computer networks using MikroTik routers // Master's graduation thesis// Kotsiuk Nazar // Ivan Pulyu Ternopil National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Systems and Networks, group СІм-61 // Ternopil, 2023 // p. – 73, fig. - 32, sheets A1 - 8, add. – 3, bibliography - 14.

Keywords: MikroTik, redundancy, communication, traffic, reliability, script language, program code.

The master's thesis is devoted to the research of methods of switching to backup communication channels to ensure reliability and high availability in computer networks.

A comparative analysis of the capabilities of Cisco, MikroTik, Juniper, Palo Alto, and Fortinet regarding their ability to automatically switch to an alternative communication channel was conducted. The possibility of sending notifications via different communication channels, such as email and SMS, about switching to a backup channel has been explored. The network capabilities of the MikroTik router have been studied. A software code has been developed for automatic switching to a backup channel with the possibility of informing via email and SMS. The system's ability to provide network stability, monitoring, recovery after failures, and informing in critical scenarios was evaluated.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IOS	Internetwork Operating System
SLA	Service Level Agreement
RPM	Real-time Performance Monitoring
PBR	Policy-Based Routing
CHR	Cloud Hosted Router
VRRP	Virtual Router Redundancy Protocol
HSRP	Hot Standby Router Protocol
CARP	Common Address Redundancy Protocol
SNMP	Simple Network Management Protocol
QoS	Quality of Service
OSPF	Open Shortest Path First
BGP	Border Gateway Protocol
RIP	Routing Information Protocol
NAT	Network Address Translation
VPN	Virtual Private Network

ВСТУП

Актуальність теми. У сучасному світі інформаційних технологій, де забезпечення безперервного доступу до мережі Інтернет є важливою умовою для багатьох сфер діяльності, включаючи бізнес, освіту та побутове використання системи резервування та керування трафіком мають бути невід'ємною частиною інфраструктури. Швидкодія та надійність з'єднання з мережею Інтернет стають пріоритетними завданнями для користувачів та підприємств та забезпечують стабільності їхньої роботи.

Мета і завдання дослідження. Метою даного дослідження є розробка та впровадження системи резервування та керування трафіком на основі маршрутизаторів MikroTik з метою забезпечення безперервного доступу до Інтернету в умовах обмеженого або втраченого зв'язку.

Основні завдання дослідження:

- аналіз існуючих методів резервування трафіку;

- вивчення функціоналу та характеристик маршрутизаторів MikroTik;

- розробка та впровадження механізмів автоматичної перевірки якості зв'язку;

- розробка процедур автоматичного переключення між основним та резервним каналами зв’язку;

- апробування розробленого механізму шляхом розгортання та налаштування тестової інфраструктури;

Об’єкт дослідження. Об’єктом дослідження є процес резервування та керування трафіком в мережі Інтернет.

Предмет дослідження. Предметом дослідження є аналіз, розробка та впровадження методів забезпечення неперервного доступу до мережі Інтернет на базі маршрутизаторів MikroTik у ситуаціях обмеженого чи втраченого зв'язку.

Методи дослідження. Для досягнення поставленої мети та вирішення завдань були використані різноманітні методи наукового дослідження.

Серед них:

- аналіз існуючих варіантів рішень;

- емпіричні дослідження з проведенням практичних тестів на базі маршрутизаторів MikroTik для вивчення їхнього функціоналу та можливостей з резервування трафіку та практичного підтвердження розроблених методів на реальних об'єктах з подальшим аналізом результатів та оцінкою ефективності системи;

- метод моделювання з використання програмних засобів для моделювання аварійних ситуацій та перевірки працездатності розроблених методів автоматичного переключення трафіку.

Наукова новизна одержаних результатів кваліфікаційної роботи. Новизною даної роботи є вдосконалення та поєднання різноманітних методів та технологій для створення системи резервування та керування трафіком на базі маршрутизаторів MikroTik, що дозволяє автоматично переключати трафік для забезпечення безперервного доступу до Інтернету у ситуаціях погіршення якості або відсутності основного каналу зв'язку.

Практичне значення одержаних результатів. Результати даного дослідження мають практичне значення для підприємств та користувачів, що прагнуть забезпечити надійність свого Інтернет-з'єднання. Розроблені методи та технології можуть бути використані для створення стабільних мереж з автоматичним переключенням між каналами та мінімізацією впливу втрати зв'язку на виробничі процеси.

Публікації. Результати дослідження апробовано на II Міжнародній науковій конференції «Актуальні питання розвитку галузей науки», XII Міжнародна науково-технічна конференція молодих учених та студентів «Актуальні задачі сучасних технологій».

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається із вступу, 4 розділів, висновків, списку використаних джерел та додатків. Обсяг роботи: пояснювальна записка – 73 аркушів формату А4, графічна частина – 6 аркушів формату А1.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ ВАРІАНТІВ РІШЕНЬ ТА ЇХ ПОРІВНЯННЯ

1.1. Огляд предметної області у галузі резервування та керування трафіком

Резервування та керування трафіком - це важлива складова будь-якої мережі, яка спрямована на забезпечення неперервного доступу до мережі Інтернет та інших мережних ресурсів. Це особливо важливо для підприємств, постачальників послуг та організацій, які вимагають високої доступності та надійності мережі.

Основні аспекти в цій області включають надлишковість, балансування навантаження, автоматичний перехід на резервний канал, якість обслуговування, моніторинг і аналіз трафіку, системи сповіщення та реагування на відмови.

Надлишковість (Redundancy) - це створення дублюючих елементів у мережі або інфраструктурі з метою забезпечення неперервності роботи у випадку відмови основного компонента. Це одна з стратегій, яка допомагає знизити ризики відмов та забезпечити високу доступність мережі.

Основні концепції надлишковості у мережевому середовищі включають: дублювання обладнання, резервування мережних шляхів,

Дублювання обладнання означає створення резервних копій обладнання, які можуть автоматично або вручну брати на себе роботу у випадку відмови основного обладнання. Наприклад, налаштування двох маршрутизаторів, один з яких стає активним, а інший - резервним.

Резервування мережних шляхів означає наявність декількох фізичних або логічних шляхів з'єднання між вузлами мережі. У випадку відмови одного шляху трафік може автоматично перенаправлятися через інший, що забезпечує безперервність зв'язку.

Реалізація надлишковості в мережі варіюється в залежності від потреб користувача, розміру мережі та бюджетних обмежень. Однак вона є важливою

стратегією для забезпечення надійності та безперервності роботи мережі у випадку можливих відмов чи проблем.

Надлишковість може бути реалізована через різні технології, такі як VRRP, HSRP, CARP тощо.

Балансування навантаження (Load Balancing) - це стратегія розподілу трафіку між різними пристроями чи ресурсами мережі з метою оптимізації використання ресурсів та підвищення надійності та швидкості мережі.

Це може бути досягнуто за допомогою різних методів, таких як Round Robin (циклічний розподіл), Least Connections (розподіл за меншим навантаженням) або методів, що враховують поточний стан ресурсів.

Балансування навантаження дозволяє рівномірно розподіляти трафік між різними серверами або шляхами, що дозволяє уникнути перевантаження одного сервера або шляху та оптимізує використання ресурсів. Балансування навантаження дозволяє ефективно управляти пропускною здатністю мережі шляхом розподілу трафіку таким чином, щоб уникнути перевантаження та підвищити швидкість передачі даних.

Деякі системи балансування можуть враховувати географічне розташування клієнтів та серверів для кращого розподілу навантаження і оптимізації шляхів передачі даних.

Балансування навантаження є важливим елементом для підтримки високопродуктивної та високодоступної мережі.

Автоматичний перехід на резервний канал (Failover) - це процес автоматичного переключення трафіку на альтернативний канал зв'язку в разі відмови основного каналу, що дозволяє підтримувати безперервну роботу мережі та забезпечувати доступність сервісів для користувачів.

Ключові моменти автоматичного переходу на резервний канал включать: моніторинг стану основного каналу, виявлення відмови, тестування доступності резервного каналу, переключення на резервний канал, автоматичне переключення на основний канал.

Система моніторингу постійно перевіряє доступність основного каналу зв'язку. Це може бути здійснене шляхом періодичного пінгування ключових вузлів чи моніторингу рівня якості з'єднання через SNMP або інші інструменти.

Коли система моніторингу виявляє відмову основного каналу зв'язку (наприклад, відсутність відповіді на пінг, перевищення порогового значення затримки або перевищення порогового значення втрат), активується процес переходу на резервний канал з попереднім тестуванням його якості.

Автоматичний механізм переходу здійснюється шляхом перенаправлення трафіку на альтернативний канал зв'язку. Це може вимагати зміни таблиці маршрутизації мережевого обладнання для перенаправлення пакетів на резервний шлях.

Після переключення на резервний канал система може продовжувати моніторити стан цього каналу, щоб переконатися, що він працює нормально та забезпечує якісний зв’язок.

Після відновлення основного каналу зв'язку система може автоматично повернутися до нього та відновити передачу трафіку через основний шлях.

Ці процеси реалізуються за допомогою програмного забезпечення маршрутизаторів або мережевого обладнання, яке підтримує механізми автоматичного переходу на резервний канал. Автоматичний перехід на резервний канал є важливою складовою для забезпечення безперервності роботи мережі та надійності сервісів, особливо в ситуаціях, коли недоступність мережі може призвести до великих втрат чи проблем для бізнесу.

Технології такі як IP SLA дозволяють системам моніторити стан основного з'єднання та переходити на резервний канал автоматично.

Якість обслуговування (QoS) - це набір технічних механізмів і стратегій, що застосовуються в мережах для забезпечення певного рівня обслуговування для конкретних видів трафіку. Це дозволяє призначити пріоритети, керувати пропускною здатністю та забезпечити надійність передачі даних у мережі.

QoS дозволяє виділяти пріоритети для різних видів трафіку. Наприклад, голосовий чи відео трафік може мати вищий пріоритет, щоб забезпечити безперебійну передачу даних для VoIP дзвінків.

Технологія QoS дозволяє встановлювати обмеження на пропускну здатність для різних видів трафіку та може регулювати затримки та втрати пакетів, забезпечуючи оптимальну якість обслуговування для чутливих до затримок додатків. Використання різних алгоритмів черги дозволяє управляти трафіком у мережі, враховуючи його пріоритети та вимоги до якості обслуговування.

Використання QoS допомагає забезпечити оптимальне використання пропускної здатності мережі та забезпечити необхідний рівень обслуговування для різних типів трафіку. Це особливо важливо у сучасних мережевих середовищах, де різноманітність додатків та вимоги до якості обслуговування постійно зростають.

Моніторинг і аналіз трафіку - це процес виявлення, спостереження, збору та аналізу всіх даних, які пересилаються через мережу. Ця діяльність дозволяє адміністраторам мережі отримати інформацію про різні аспекти мережевого трафіку, включаючи його обсяг, джерела, призначення, протоколи, шляхи передачі та якість з'єднання. Ці процеси дозволяють виявляти аномалії у роботі мережі, передбачати можливі проблеми та реагувати на них. Інструменти моніторингу, такі як SNMP, NetFlow або спеціалізовані програмні рішення, грають ключову роль у цьому.

Системи сповіщення та реагування на відмови в мережі - це один з основних моментів для забезпечення безперервності роботи мережі та швидкого виявлення проблем. Системи сповіщення дозволяють оперативно отримувати інформацію про відмови, аномалії чи проблеми в мережі і швидко реагувати на них, щоб уникнути перерв у роботі мережі.

Системи моніторингу вимірюють і аналізують ключові параметри мережі, виявляючи відмови або аномалії у працездатності.

Дані системи можуть використовувати автоматизоване сповіщення адміністраторів чи відповідальних осіб про виявленні проблеми або відмови через різні канали зв'язку, такі як електронна пошта, SMS або пуш-сповіщення.

В даних система ключовим є налаштування автоматичних сценаріїв реагування на виявлені проблеми. Наприклад, автоматичне перенаправлення трафіку на резервний канал або відновлення працездатності сервісу без втручання оператора.

Важливо вести журнали подій для подальшого аналізу та удосконалення системи.

Системи сповіщення та реагування на відмови в мережі є критичними для підтримки неперервності роботи мережі та оперативного вирішення проблем. Їх ефективність визначається як швидкістю виявлення проблем, так і швидкістю реагування на них для мінімізації впливу на користувачів та бізнес-процеси.

Все це разом створює фундаментальні засади для забезпечення надійності та безперервності роботи мережі.

1.2. Огляд рішення Cisco у галузі резервування трафіку

Cisco - це технологічна компанія, що спеціалізується на розробці та виробництві мережевого обладнання, програмного забезпечення для підприємств, постачальників послуг інтернету та споживачів. Компанія виробляє широкий спектр мережевих пристроїв, включаючи маршрутизатори, комутатори, брандмауери, мережеві рішення Wi-Fi, пристрої для центрів обробки даних та інше. Крім апаратного забезпечення, Cisco розробляє програмне забезпечення для управління мережами, безпеки, аналізу даних та інші рішення для різних сегментів ринку.

Компанія пропонує рішення для захисту мережевої інфраструктури від кіберзагроз, включаючи брандмауери, системи виявлення вторгнень та інші заходи захисту.

Cisco пропонує різноманітні хмарні рішення для забезпечення мережевих послуг, віртуалізації та сховищ даних.

Cisco відома своїм впливом на розвиток мережевих технологій та інноваційними рішеннями у цій галузі. Вона є однією з провідних компаній у сфері мережевих технологій та відіграє ключову роль у побудові сучасного цифрового світу.

Cisco IOS є операційною системою, що використовується на маршрутизаторах та комутаторах Cisco. Вона є ключовою складовою для управління та керування мережевими пристроями Cisco.

Взаємодія з Cisco IOS зазвичай відбувається через командний рядок, що дозволяє адміністраторам налаштовувати та керувати пристроями за допомогою команд. Cisco IOS надає розширені можливості управління та налаштування маршрутизацією, комутацією та фільтрацією трафіку в мережах та має набір засобів безпеки для захисту мережі, таких як брандмауери, VPN, захист від DoS-атак, шифрування даних тощо.

Ця операційна система має різноманітні інструменти для керування мережею, моніторингу та діагностики, такі як SNMP, syslog, NetFlow, інструменти моніторингу пристроїв тощо.

Cisco IP SLA - це технологія вбудована в Cisco IOS, яка дозволяє виконувати тести та моніторинг мережевих параметрів для вимірювання рівня обслуговування (SLA) мережі [1]. Вона використовується для визначення та вимірювання пропускної здатності, затримок, втрати пакетів, які впливають на якість та доступність мережі.

IP SLA дозволяє виконувати різноманітні тести для моніторингу мережі. Це можуть бути тести Ping, UDP, TCP, HTTP, VoIP, і багато інших, які дозволяють вимірювати різні параметри мережі.

Система дозволяє моніторити якість мережі. Наприклад, воно може вимірювати затримки. IP SLA збирає дані та надає статистику про результати вимірювань. Це дозволяє адміністраторам мережі візуалізувати та аналізувати параметри мережі для прийняття рішень щодо вдосконалення мережі.

IP SLA може виконувати автоматичні дії на основі результатів тестів. Наприклад, при перевищенні певного порогу затримок в мережі, можна налаштувати автоматичне перенаправлення трафіку на інший шлях.

Ця технологія дозволяє постійно відстежувати стан мережі, що допомагає вчасно виявляти та вирішувати проблеми для запобігання перебоям у роботі.

Cisco IP SLA надає інструменти для активного моніторингу та управління мережевими ресурсами. Вона є корисним інструментом для адміністраторів мережі для виявлення проблем, планування мережі та вдосконалення рівня обслуговування мережі.

1.3. Огляд рішення MikroTik у галузі резервування трафіку

MikroTik - це компанія, що розробляє мережеве обладнання та програмне забезпечення для побудови та управління мережами. В їхньому асортименті є різноманітні пристрої, включаючи маршрутизатори, комутатори, точки доступу Wi-Fi та інше обладнання, які можуть бути використані для налаштування резервування трафіку в мережах [2].

MikroTik використовує власну операційну систему, яка називається RouterOS. Ця операційна система є спеціалізованою версією Linux, спеціально розробленою для роботи на маршрутизаторах, комутаторах та інших мережевих пристроях MikroTik.

MikroTik пропонує рішення для налаштування автоматичного переходу на резервний канал в разі відмови основного з'єднання, забезпечуючи неперервність роботи мережі [3]. Для цього можна скористатися різними технологіями та інструментами, такими як Netwatch або скриптами та планувальником завдань.

Функція Netwatch в MikroTik є корисним інструментом для моніторингу доступності віддалених серверів чи IP-адресів і може бути використана для автоматичного реагування на відмову основного з'єднання.

Але Netwatch є не ефективним рішенням при виявленні деяких типів проблем, таких як часткові втрати в каналі, коли цільовий пристрій моніторингу відповідає на пінги з певним відсотком втрат.

Скрипти та планувальники завдань (Scheduler) в MikroTik, - це потужні інструменти, які дозволяють автоматизувати та виконувати різні дії на мережевому обладнанні на основі розкладу або подій.

Скрипти в MikroTik - це послідовності команд, які можна створювати, редагувати та виконувати на пристроях MikroTik. Вони дозволяють автоматизувати різноманітні завдання, від налаштування мережі до автоматичного реагування на певні події. Скрипти можна створювати в інтерфейсі командного рядка (CLI) або через графічний інтерфейс (Winbox).

Планувальники завдань (Scheduler)в MikroTik дозволяють створювати розклади виконання певних дій в певний час або за певних умов. Вони дозволяють автоматизувати виконання скриптів, відновлення, перезавантаження, збереження конфігурацій, а також інші дії в заданий час або після виникнення певних подій.

Основні можливості та функції, що використовуються разом зі скриптами та планувальниками завдань MikroTik: автоматизація рутинних завдань, моніторинг та управління мережею, виконання складних операцій.

Скрипти можна використовувати для автоматизації рутинних операцій, таких як резервне копіювання конфігурацій, відновлення після відмови, моніторинг мережі та інше.

За допомогою скриптів та планувальників можна налаштовувати моніторинг різних параметрів мережі, виявлення проблем та автоматичне вирішення певних ситуацій. Скрипти можуть виконувати складні послідовності дій, що включають у себе різноманітні команди та умови виконання на основі програмованої логіки з надсиланням повідомлень на пошту чи за допомогою SMS про настання певних події.

1.4. Огляд рішення Juniper у галузі резервування трафіку

Juniper Networks — це відомий постачальник мережевого обладнання, програмного забезпечення для мережевої інфраструктури, рішень для безпеки та управління мережею. Компанія спеціалізується на розробці та виробництві різноманітних мережевих пристроїв, таких як маршрутизатори, комутатори, брандмауери, а також програмного забезпечення для управління цим обладнанням.

Маршрутизатори Juniper відомі своєю високою продуктивністю та масштабованістю. Кампанія випускає маршрутизатори для різних потреб, від підприємств до провайдерів інтернет-послуг.

Продукти для захисту мережі включають брандмауери, системи виявлення вторгнень, а також рішення для захисту від різного типу атак.

Програмне забезпечення включає в себе засоби для автоматизації управління мережею, аналізу даних, моніторингу та управління ресурсами.

Juniper пропонує також рішення для будівництва, управління та захисту хмарних середовищ.

Juniper використовує операційну систему Junos для свого мережевого обладнання, такого як маршрутизатори, комутатори та інші пристрої. Junos є власною операційною системою, розробленою Juniper Networks.

Операційна система Junos побудована на базі FreeBSD, яке є відкритою операційною системою Unix-подібної архітектури. Однак Junos має свою власну унікальну архітектуру, додаткові функції та інструменти, розроблені саме для мережевих потреб.

Операційна система Junos відома своєю надійністю, високою продуктивністю та масштабованістю. Вона надає широкий набір функцій для управління мережею, моніторингу, безпеки та управління ресурсами. Junos дозволяє виконувати широкий спектр завдань, включаючи маршрутизацію, комутацію, налаштування безпеки, аналіз мережі та багато іншого.

Ця операційна система має свою власну командну оболонку та інтерфейс для конфігурації та управління пристроями Juniper, що дозволяє інженерам мереж робити налаштування, моніторинг та управління мережею з використанням різних методів, включаючи командний рядок та графічний інтерфейс.

Juniper використовує RPM для виконання IP-моніторингу з можливістю Failover [4]. Ця технологія використовується для моніторингу та вимірювання різних параметрів мережевого зв'язку в реальному часі. RPM зазвичай використовується для вимірювання якості з'єднання, перевірки доступності вузлів та визначення продуктивності мережі.

RPM може використовувати проби (probe) для вимірювання параметрів мережі. Проба (probe) - це механізм, що використовується для виконання конкретних вимірювань чи тестів, таких як надсилання пакетів на певний IP-адрес, вимірювання затримки, втрат пакетів чи рівня пропускної здатності.

Таким чином, RPM проби - це інструмент для виконання вимірювань або тестів, що дозволяє моніторити мережеві параметри в реальному часі. Вони використовуються для збирання даних про стан мережі, які потім можуть використовуватися для аналізу продуктивності, виявлення відмов, налаштування мережі для оптимальної роботи та виявлення проблем в зв'язку для подальшого реагування.

Якщо тест RPM виявляє відмову, можна налаштувати автоматичне переключення на альтернативний шлях за допомогою PBR.

Juniper використовує RPM разом із системою маршрутизації для автоматичного реагування на проблеми мережі. Він дозволяє виявляти відмови та швидко переключати трафік на альтернативні шляхи, що забезпечує безперервність мережевого зв'язку.

1.5. Огляд рішення Palo Alto у галузі резервування трафіку

Palo Alto Networks - це відомий виробник обладнання та програмного забезпечення для кібербезпеки та мережевої безпеки. Вони спеціалізуються на розробці інтегрованих рішень для захисту мереж, даних і пристроїв від різних кіберзагроз.

Компанія виробляє та пропонує різноманітні продукти і рішення, спрямовані на захист корпоративних мереж, дата-центрів, хмарних середовищ та інших інфраструктур від кіберзагроз.

PAN-OS - це операційна система, що використовується на пристроях Palo Alto Networks, базується на спеціалізованій версії Linux. Компанія Palo Alto Networks розробляє цю операційну систему для своїх брандмауерів та мережевих пристроїв, і вона спеціально адаптована для забезпечення високої рівня безпеки мережі та виявлення кіберзагроз. Хоча PAN-OS базується на ядрі Linux, вона включає в себе велику кількість власних розробок, модифікацій і розширень, спеціально створених для вирішення завдань захисту мережі та боротьби з сучасними кіберзагрозами.

Palo Alto Networks пропонує функціонал, відомий як Path Monitoring (моніторинг шляху), який дозволяє налаштовувати моніторинг шляху та автоматичне переключення на резервний канал у випадку відмови або проблеми з доступністю мережевих шляхів [5]. Path Monitoring використовується для вимірювання доступності мережевих шляхів і автоматичного виконання переключення трафіку на альтернативні шляхи, якщо виявляється недоступність основного шляху. Адміністратор мережі вказує основний та резервний шляхи для моніторингу, встановлюючи параметри для вимірювання доступності (наприклад ICMP ping, HTTP, TCP). Встановлюються порогові значення, які вказують, коли слід вважати шлях недоступним або нездатним для передачі трафіку.

Якщо виявляється недоступність або проблема з основним шляхом, механізм автоматично перенаправляє трафік на резервний шлях без необхідності

втручання адміністратора. Після відновлення основного шляху пристрій повертається до нормальної роботи.

Цей механізм дозволяє Palo Alto Networks автоматично реагувати на проблеми з доступністю мережевих шляхів та забезпечити безперервність мережевого зв'язку через автоматичне перемикання на альтернативні шляхи в разі відмови основного шляху.

1.6. Огляд рішення Fortinet у галузі резервування трафіку

Fortinet - це провідний постачальник інтегрованих рішень з кібербезпеки, який пропонує широкий спектр продуктів та послуг для захисту мереж, пристроїв та даних від різноманітних кіберзагроз.

У компанії Fortinet є широка лінійка мережевих брандмауерів. Ці брандмауери забезпечують захист мережі, контроль доступу. Fortinet пропонує рішення для централізованого управління кібербезпекою та моніторингу заходів безпеки для всієї мережі. Рішення для захисту хмарних середовищ, включаючи різні послуги для контролю доступу та захисту від кіберзагроз.

В маршрутизаторах Fortinet використовується операційна система FortiOS. Ця операційна система розроблена компанією Fortinet спеціально для їхніх мережевих пристроїв, таких як брандмауери, мережеві точки доступу, маршрутизатори тощо. Fortinet використовує для своєї операційної системи FortiOS спеціалізовану версію операційної системи Linux. FortiOS базується на ядрі linux, яке відоме своєю надійністю та безпекою. Компанія Fortinet використовує цю основу для розробки своєї операційної системи з урахуванням потреб безпеки та захисту в мережі.

Link Monitor - це механізм, який використовується для постійного моніторингу стану з’єднань між мережевими пристроями, такими як маршрутизатори, брандмауери, комутатори тощо [6]. Цей механізм дозволяє Fortinet автоматично визначати недоступні або нестабільні з'єднання та при необхідності автоматично виконувати дії для відновлення роботи мережі.

Система постійно моніторить стан з'єднань між мережевими пристроями. Вона періодично відправляє тестові пакети до певних точок або IP-адрес для визначення доступності зв'язку.

Якщо статус з’єднання змінюється або не відповідає заданим критеріям доступності (наприклад, відсутність відповіді на запити або високий рівень втрат пакетів), то система класифікує це як відмову.

Коли виявляється відмова або недоступність основного з'єднання, відбувається автоматичне переключення трафік на альтернативний шлях для забезпечення неперервності послуги.

Адміністратор може налаштувати критерії та порогові значення для визначення відмови зв'язку. Це може включати час очікування відповіді, кількість втрачених пакетів тощо.

Ці функції дозволяють Fortinet виявляти недоступні або непрацюючі з'єднання та автоматично переключати трафік на альтернативні шляхи, що забезпечує безперервність мережевого зв'язку у випадку відмови основних з'єднань.

1.7. Порівняння рішення у галузі резервування трафіку

При порівнянні різних систем моніторингу та переходу на резервний канал, важливо враховувати їхні можливості, функціональність та ефективність у реальних умовах мережевого середовища. Cisco IP SLA, MikroTik скрипти та планувальники завдань, Juniper Real-time Performance Monitoring, Palo Alto Path Monitoring та Fortinet Link Monitor пропонують різні підходи до вимірювання метрик, моніторингу стану мережі та автоматизації переходу на альтернативний канал у випадку відмови.

Усі системи пропонують схожу функціональність що до можливості переключення на резервний канал, але можливості сповіщення про переключення відрізаються. Можливість сповіщення за допомогою електронної пошти є у всіх системах без застосування додаткових зовнішніх систем

моніторингу, але лише у MikroTik є можливість використання розширених алгоритмів в скриптах та сповіщення через різні канали, включно з надсиланням SMS через внутрішній засіб моніторингу [7].

У багатьох випадках, MikroTik є привабливим варіантом для малих та середніх підприємств. Ця система має низьку вартість в порівнянні з іншими рішеннями, пропонує широкий спектр функцій та може бути досить гнучкою для налаштування. MikroTik відомий широкими мережевими функціями та має різноманітні можливості для створення скриптів та автоматизації завдань.

1.8. Висновки до розділу

У розділі було проведено огляд сучасних систем управління мережею та моніторингу трафіку від провідних виробників, таких як Cisco, MikroTik, Juniper, Palo Alto та Fortinet. Здійснено порівняння їхніх можливостей для забезпечення надійності мережі, відслідковування трафіку та автоматичного переходу на резервний канал у разі відмови основного зв'язку.

Під час аналізу було розглянуто функціональність кожної системи, їхню здатність автоматично переходити на альтернативний канал зв’язку. Також було проаналізовано можливості автоматичного реагування на події у мережі та надсилання сповіщення про відмови через різні канали комунікації, такі як електронна пошта або SMS.

РОЗДІЛ 2
ЗАСОБИ СТВОРЕННЯ ЛАБОРАТОРНОГО СЕРЕДОВИЩА СИСТЕМИ РЕЗЕРВУВАННЯ

2.1. Огляд маршрутизатор MikroTik CHR

MikroTik CHR - це віртуальний маршрутизатор, який працює на базі операційної системи RouterOS, розробленій компанією MikroTik [8]. Цей віртуальний маршрутизатор розрахований на запуск у різних системах віртуалізації, такі як VMware, Hyper-V, KVM або XEN.

CHR надає можливість легко масштабувати мережеві рішення, що дозволяє адаптувати конфігурацію до потреб користувача. Даний маршрутизатор буде використано в лабораторному середовищі на базі гіпервізора VMware ESXi для створення системи резервування трафіку.

2.1.1. Системні вимоги

MikroTik CHR. Даний маршрутизатор підтримує архітектуру x86 64-біт [8].

Вимоги до системи для CHR:

- версія пакету RouterOS v6.34 або новіша;
- центральний процесор (CPU) хосту має бути 64-бітний з підтримкою віртуалізації;
- рекомендована оперативна пам'ять (RAM) становить1024 МБ або більше (мінімум 128 МБ , максимум 128 ГБ)
- мінімальний розмір диску 128 МБ для віртуального жорсткого диска CHR (максимум 16 ГБ)

Мінімальний обсяг оперативної пам'яті залежить від кількості інтерфейсів та процесорів. Щоб розрахувати орієнтовний мінімальний обсяг оперативної пам’яті можна використати наступну формулу:

$$RAM = ver + (8 \cdot (CPU\_C) \cdot (IF\_C - 1)), \quad (1.1)$$

де ver – коефіцієнт версії RouterOS (для v6 – 128, для v7 – 256);

CPU_C – кількість процесорів;

IF_C – кількість інтерфейсів.

2.1.2. Огляд можливостей MikroTik CHR. Віртуальний комутатор MikroTik CHR використовує ту ж операційну систему, що й фізичні маршрутизатори MikroTik, а саме RouterOS. Це надає широкий спектр мережевих функцій, включаючи маршрутизацію, VPN, мережевий брандмауер, QoS та інші.

CHR має повний функціонал RouterOS, але має іншу ліцензійну модель порівняно з решту версіями RouterOS.

Окрім статичної маршрутизації MikroTik CHR також підтримує різні протоколи маршрутизації, такі як OSPF, BGP, RIP і інші.

OSPF - це протокол маршрутизації, який використовує алгоритм Дейкстри для визначення найкоротших шляхів у мережі. Він враховує вартість кожного з'єднання та вибирає найефективніший шлях до кожного пункту призначення. OSPF автоматично створює топологічну карту мережі, використовуючи LSA (Link State Advertisements), що дозволяє кожному маршрутизатору мати повний огляд мережі та використовувати цю інформацію для прийняття рішень щодо маршрутизації. OSPF може бути розділений на логічні області, що дозволяє масштабувати мережу та зменшувати навантаження на маршрутизатори. Кожна область має свою топологічну карту, а маршрутизатори, які належать до однієї області, обмінюються лише суміжними LSA. OSPF реагує швидко на зміни в мережі. Якщо відбувається зміна топології, OSPF швидко оновлює свою топологічну карту та перераховує найкоротші шляхи, що дозволяє зберігати стабільність маршрутів у мережі.

OSPF не використовується в Інтернеті на рівні глобальної маршрутизації. Даний протокол широко використовується у внутрішніх мережах організацій, в

мережах провайдерів та у невеликих мережах, де вимагається внутрішній обмін маршрутами між маршрутизаторами однієї автономної системи (AS).

Хоча OSPF може використовуватися для будь-якого масштабу мережі, включаючи досить великі, проте в Інтернеті для маршрутизації застосовується BGP.

BGP - це протокол маршрутизації, який використовується у мережі Інтернеті для обміну інформацією між різними автономними системами (AS).

Даний протокол працює між різними автономними системами (AS). Кожна AS - це група мереж і маршрутизаторів, що управляються спільним адміністративним доменом. BGP обмінюється інформацією про маршрути між різними AS. Він передає інформацію про доступність мереж та найкращі шляхи до цих мереж між різними провайдерами Інтернету.

BGP дозволяє маршрутизаторам приймати рішення на основі політики мережі. Це означає, що адміністратори можуть використовувати різні критерії (наприклад, швидкість маршруту, пропускна здатність) для прийняття рішень щодо найкращого шляху. BGP - це дуже стабільний протокол маршрутизації, який дозволяє масштабувати глобальні мережі Інтернету. Він може працювати у складних середовищах, зберігаючи стабільність інтернет-підключення. Даний протокол надає адміністраторам гнучкий контроль над шляхами трафіку у мережі. Це дозволяє налаштовувати і маніпулювати трафіком для досягнення оптимальної швидкості та ефективності. BGP використовується провайдерами Інтернету та великими організаціями для обміну інформацією про маршрути для забезпечення надійного підключення до різних мереж в Інтернеті.

Брандмауер в MikroTik - це інструмент, який дозволяє контролювати та керувати трафіком в мережі. Брандмауер дозволяє створювати правила для фільтрації трафіку. Це може бути здійснено на основі IP-адрес, портів, протоколів або інших параметрів, щоб дозволити чи блокувати певний вид трафіку. Також MikroTik має підтримку Stateful Packet Inspection (SPI), що дозволяє аналізувати стан пакетів. Він може відстежувати стан кожного пакета

та приймати рішення щодо його пропуску чи блокування на основі інформації про попередні пакети в тій же сесії.

Брандмауер також підтримує NAT. Source NAT (SNAT) дозволяє змінювати IP-адреси джерела (вихідні IP-адреси) в пакетах, що проходять через маршрутизатор MikroTik. Це корисно, наприклад, при виході в Інтернет через одну публічну IP-адресу, яка є постійною з багатьох приватних IP-адрес.

Destination NAT (DNAT) використовується для переадресації пакетів, призначених для однієї IP-адреси та порту, на інші IP-адреси та порти. Це може бути корисним для направлення зовнішнього трафіку на конкретні пристрої чи сервери у внутрішній мережі.

Masquerade - це особливий тип NAT, який використовується для зміни IP-адреси джерела на публічну IP-адресу, яка присвоюється маршрутизатору MikroTik та не є постійною. Це зручно для надання доступу до Інтернету пристроям у внутрішній мережі.

Брандмауер MikroTik веде систему журналування, яка дозволяє відстежувати та аналізувати події, пов'язані з проходженням трафіку через брандмауер.

MikroTik пропонує різні можливості для налаштування VPN, що дозволяє створювати захищені тунелі для передачі даних через непублічні мережі. CHR підтримує IPsec для створення захищених тунелів між різними пристроями чи мережами. Це включає в себе можливість налаштування VPN тунелів з використанням різних алгоритмів шифрування та аутентифікації для забезпечення конфіденційності даних та безпеки тунелю. MikroTik також підтримує протокол OpenVPN, який є одним з популярних протоколів для створення VPN. OpenVPN забезпечує широкі можливості налаштування, включаючи шифрування, аутентифікацію.

MikroTik підтримує інші стандартні протоколи VPN, такі як PPTP та L2TP, які також можуть бути використані для налаштування VPN-тунелів між пристроями чи мережами.

QoS в MikroTik - це функціональність, яка дозволяє контролювати та управляти пріоритетами трафіку в мережі, забезпечуючи певний рівень обслуговування для різних типів даних. Це дозволяє класифікувати трафік на основі різних параметрів, таких як IP-адреси, порти, протоколи або типи послуг та відокремити різні види трафіку для подальшого управління його пріоритетами. Використовуючи QoS можна встановлювати правила для обмеження або формування обсягу трафіку для конкретних потоків даних. Це корисно для забезпечення рівномірного розподілу пропускної здатності та запобігання перевантаження мережі. QoS дозволяє встановлювати пріоритети для різних видів трафіку. Наприклад можна надавати високий пріоритет голосовому трафіку VoIP, щоб забезпечити якісну передачу голосової інформації навіть при великому обсязі інших даних.

Queue Management в MikroTik дозволяє створювати черги для різних видів трафіку та налаштовувати правила управління цими чергами, що дозволяє контролювати пропускну здатність для кожного виду трафіку.

QoS допомагає уникати заторів у мережі, розподіляючи пропускну здатність таким чином, щоб уникнути перенавантаження мережі та забезпечити кращий рівень обслуговування для критичних застосунків.

MikroTik RouterOS має вбудований механізм скриптів, який дозволяє автоматизувати різноманітні завдання в мережі. Можна створювати сценарії з використанням скриптів для виконання певних дій або послідовностей дій. Це може бути автоматизація рутинних завдань, налаштування параметрів, перевірка стану мережі тощо [2]. Використовуючи скрипти можна створювати автоматичні відповіді на певні події у мережі, наприклад, відключення або підключення певного пристрою чи виявлення помилки у роботі.

Скрипти можуть бути використані для пакетного налаштування параметрів різних пристроїв у мережі. Це дозволяє швидко та ефективно впроваджувати зміни в конфігурації. Скрипти можуть бути заплановані для виконання в певний час або через регулярні інтервали за допомогою планувальника завдань в MikroTik. Це корисно для автоматичного виконання певних дій у визначений час.

Можна використовувати скрипти для моніторингу певних параметрів в мережі та записувати результати в журнал для подальшого аналізу чи діагностики. Скрипти можуть додавати нові можливості та функції, які не включені в стандартні налаштування RouterOS.

MikroTik CHR є ефективним інструментом для віртуалізації мережевого середовища, надаючи різноманітні функції, які характерні для фізичних маршрутизаторів MikroTik, та відкриваючи можливості для ефективного управління мережами у віртуальних і хмарних середовищах.

2.2. Схема мережі лабораторного середовища

Для моделювання системи резервування та керування трафіком буде використано тестове середовище, схема якого представлена на рис.2.1.

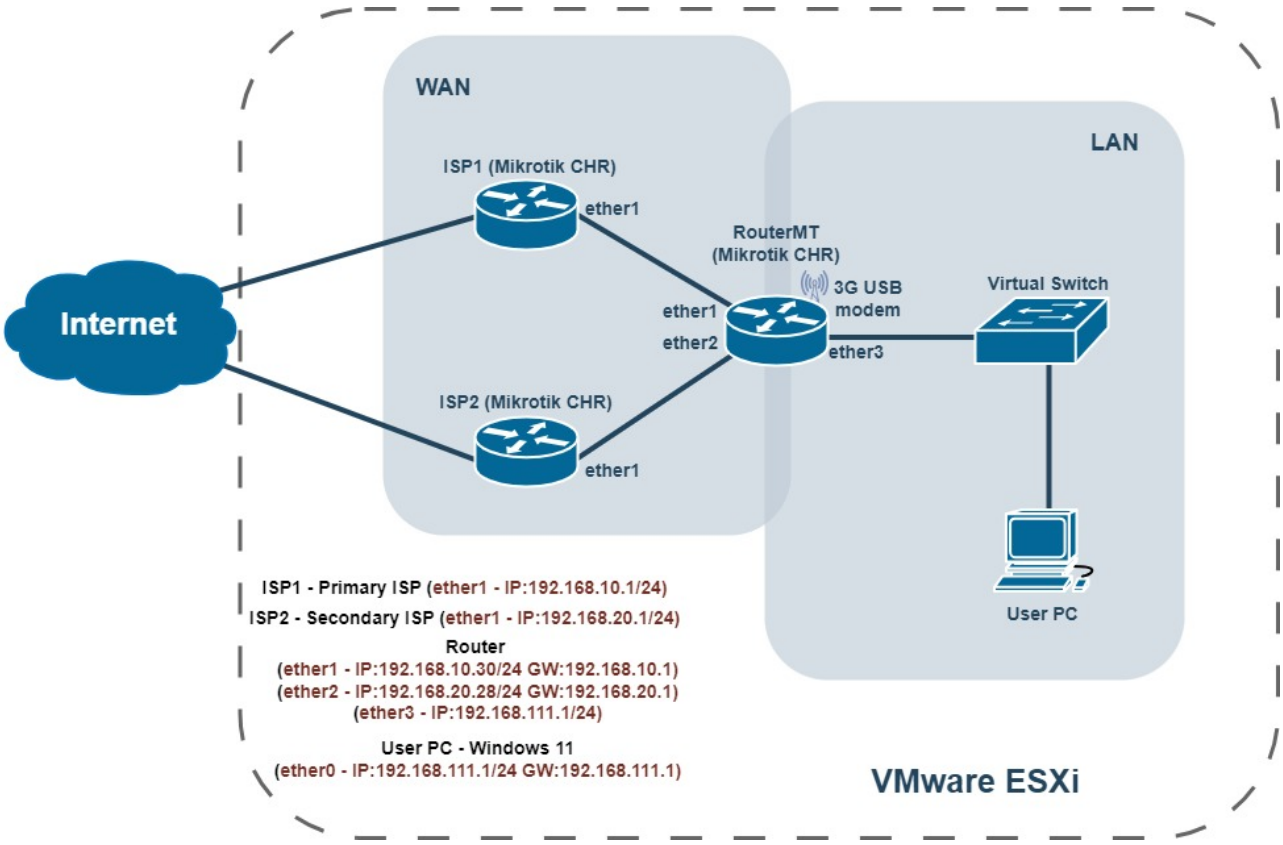


Рис. 2.1. Схема віртуальної лабораторної мережі

На схемі зображено тестове середовище для моделювання системи резервування та керування трафіком, яке складається з двох віртуальних мереж Wide Area Network (WAN) та Local Area Network (LAN).

Два інтернет-провайдери (ISP1 та ISP2) представлені як маршрутизатори MikroTik CHR. ISP1 підключений до локального маршрутизатора через інтерфейс ether1 з IP-адресою 192.168.10.1/24 та є основним інтернет-провайдером. ISP2 також підключений через інтерфейс ether1 до локального маршрутизатора, але має IP-адресу 192.168.20.1/24 і є резервним інтернет-провайдером.

Локальний маршрутизатор RouterMT, який з'єднує WAN і LAN, має інтерфейс ether1 з IP-адресою 192.168.10.30/24 та шлюзом 192.168.10.1 (ISP1) для підключення до основного ISP. Для підключення до резервного ISP використовується інтерфейс ether2 маршрутизатора, який має IP-адресу 192.168.20.20/24 з шлюзом 192.168.20.1 (ISP2). Інтерфейс ether3 має IP-адресу 192.168.111.1/24 і є шлюзом для локальної мережі (LAN). До локального маршрутизатора підключено 3G USB модем Huawei E1550, який використовується як канал зв’язку при аварійних ситуаціях з можливістю надсилання SMS.

LAN складається з віртуального комутатора (Virtual Switch) та користувацького ПК. Користувацький ПК з встановленою віртуальною машиною Windows 11 підключений до віртуального комутатора. Інтерфейс користувацького ПК (ether0) має IP-адресу 192.168.111.24/24 з шлюзом 192.168.111.1.

Все тестове середовище розгорнуто на платформі віртуалізації VMware ESXi, що дозволяє віртуалізувати мережеве обладнання та ПК.

2.3. Налаштування компонентів тестового середовища

2.3.1. Налаштування маршрутизаторів ISP1 та ISP2. Проведемо початкові налаштування MikroTik CHR, які використовуються як маршрутизатори ISP1 та ISP2.

На рис. 2.2 показано мережеві налаштування маршрутизатора ISP1.

```
[admin@ISP1] > /ip/address/print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#    ADDRESS            NETWORK        INTERFACE
0 D 192.168.0.114/24   192.168.0.0    ether0
1   192.168.10.1/24    192.168.10.0   ether1
[admin@ISP1] > /ip/route/print
Flags: D - DYNAMIC; A - ACTIVE; c, s, y - COPY
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#      DST-ADDRESS       GATEWAY       DISTANCE
0  As 0.0.0.0/0         192.168.0.1          1
  DAc 192.168.0.0/24    ether0               0
  DAc 192.168.10.0/24   ether1               0
[admin@ISP1] >
```

Рис. 2.2. Налаштування мережі маршрутизатора ISP1

IP-адреса 192.168.0.114/24 призначена для інтерфейсу ether0 за допомогою DHCP. IP-адреса 192.168.10.1/24 призначена для інтерфейсу ether1 статично.

Маршрутом за умовчанням є IP-адрес 192.168.0.1.

На рис. 2.3 показано налаштування DHCP сервера на маршрутизаторі ISP1.

```
[admin@ISP1] >  /ip/dhcp-server/print
Columns: NAME, INTERFACE, ADDRESS-POOL, LEASE-TIME
# NAME     INTERFACE  ADDRESS-POOL  LEASE-TIME
0 server1  ether1     DHCP-pool1    10m
[admin@ISP1] > /ip/pool/print
Columns: NAME, RANGES
#  NAME         RANGES
0  DHCP-pool1   192.168.10.20-192.168.10.30
[admin@ISP1] > /ip/dhcp-server/network/print
Columns: ADDRESS, GATEWAY, DNS-SERVER
# ADDRESS           GATEWAY       DNS-SERVER
0 192.168.10.0/24   192.168.10.1  192.168.10.1
[admin@ISP1] >
```

Рис. 2.3. Вивід параметрів налаштування DHCP сервера маршрутизатора ISP1

Вивід конфігурації DHCP сервера та пов'язаних з ним об'єктів показує що сервер з назвою server1 налаштований на інтерфейсі ether1. Цей сервер використовує адресний пул DHCP-pool1. Час оренди IP-адрес (lease time) становить 10 хвилин. Адресний пул DHCP-pool1 має діапазон IP-адрес від 192.168.10.20 до 192.168.10.30. DHCP сервер обслуговує мережу 192.168.10.0/24. Шлюзом для цієї мережі виступає IP-адреса 192.168.10.1. В якості DNS-сервера також використовується IP 192.168.10.1.

На рис. 2.4 показано налаштування NAT на маршрутизатора ISP1.

```
[admin@ISP1] > /ip/firewall/nat/print
Flags: X - disabled, I - invalid; D - dynamic
 0    chain=srcnat action=masquerade src-address=192.168.10.0/24
      out-interface=ether0 log=no log-prefix=""
[admin@ISP1] >
```

Рис. 2.4. Вивід параметрів налаштування NAT на маршрутизаторі ISP1

Правило NAT встановлене в ланцюгу srcnat з дією masquerade, яка використовується для зміни IP-адреси джерела на IP-адресу, яка присвоюється маршрутизатору MikroTik та не є постійною.

Ця конфігурація дозволяє пристроям з мережі 192.168.10.0/24 використовувати мережевий інтерфейс ether0 для виходу в Інтернет, приховуючи їхні оригінальні IP-адреси за адресою інтерфейсу ether0.

Налаштування MikroTik CHR, який використовуються як маршрутизатор ISP2 здійснимо аналогічно до налаштувань маршрутизатора ISP1 згідно IP-адресної схеми з рис. 2.1.

2.3.2. Налаштування локального маршрутизатора. Маршрутизатор на схемі представлений як MikroTik CHR з назвою RouterMT виконує ключову роль у керуванні та розподілі трафіку між LAN сегментам мережі та між ISP1та ISP2.

Проведемо початкове налаштування даного маршрутизатора.

На рис. 2.5 показано мережеві налаштування маршрутизатора RouterMT.

```
[admin@RouterMT] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.111.1/24   192.168.111.0   ether3
 1 D 192.168.10.30/24   192.168.10.0    ether1
 2 D 192.168.20.28/24   192.168.20.0    ether2
[admin@RouterMT] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADS  0.0.0.0/0                          192.168.10.1              1
 1  DS  0.0.0.0/0                          192.168.20.1              2
 2 ADC  192.168.10.0/24    192.168.10.30   ether1                    0
 3 ADC  192.168.20.0/24    192.168.20.28   ether2                    0
 4 ADC  192.168.111.0/24   192.168.111.1   bridge1                   0
```

Рис. 2.5. Налаштування мережі маршрутизатора RouterMT

В мережевих налаштування маршрутизатора RouterMT на інтерфейсі ether3 встановлено статичну IP-адресу 192.168.111.1/24. На інтерфейсі ether1 та ether2 динамічні IP-адреси 192.168.10.30/24 та 192.168.20.28/24 відповідно.

Є два маршрути за замовчуванням (0.0.0.0/0), що означає, що будь-який трафік, який не відповідає іншим правилам маршрутизації, буде відправлятись через вказані шлюзи.

Перший маршрут за замовчуванням (192.168.10.1) через інтерфейс ether1 з високим пріоритетом (distance = 1). Другий маршрут за замовчуванням (192.168.20.1) через інтерфейс ether2 з меншим пріоритетом (distance = 2). Активним є маршрут через інтерфейс ether1.

На рис. 2.6 показано налаштування DHCP сервера на маршрутизаторі RouterMT.

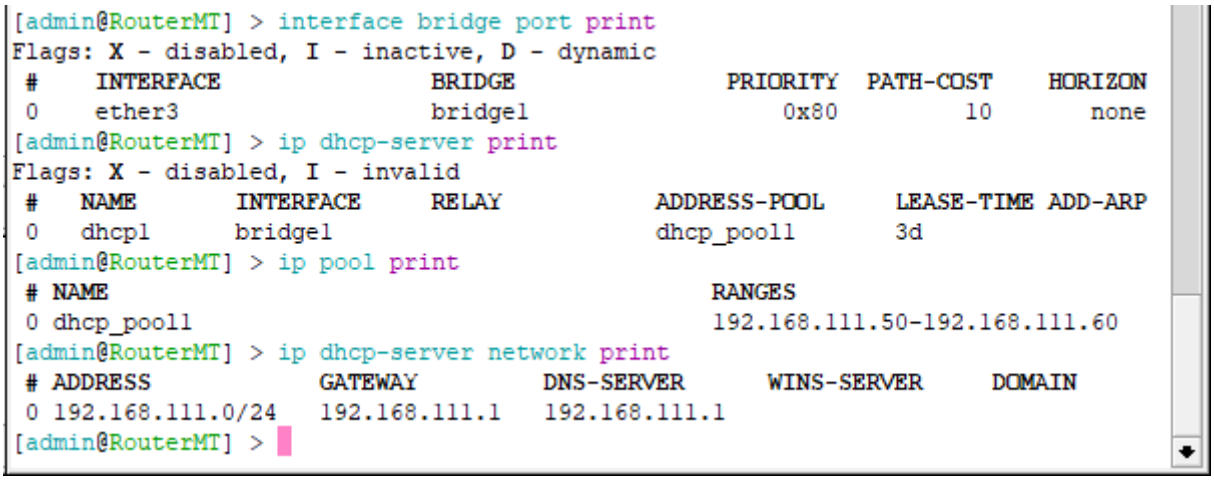


Рис. 2.6. Вивід параметрів налаштування DHCP сервера маршрутизатора RouterMT

Інтерфейс ether3 налаштований як порт мережевого моста bridge1 з пріоритетом 0x80 та вартістю шляху 10. DHCP-сервер з назвою dhcp1 налаштований на прослуховування інтерфейсу мосту bridge1. Цей сервер використовує адресний пул dhcp_pool1 з діапазоном IP-адрес від 192.168.111.50 до 192.168.111.60. Час оренди IP-адрес (lease time) сконфігурований на 3 дні. DHCP сервер видає IP-адреси з мережі 192.168.111.0/24, з шлюзом 192.168.111.1 та DNS-сервером 192.168.111.1.

Конфігурація DHCP сервера налаштована для динамічного виділення IP-адрес з діапазону 192.168.111.50-192.168.111.60 для пристроїв, що підключені до LAN мережі, а також надання їм відповідних додаткових налаштувань мережі [9].

На рис. 2.7 показано базові налаштування брандмауера на маршрутизаторі RouterMT.

#		Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
;;; accept established												
0		accept	input								23.4 MiB	369 898
;;; accept related												
1		accept	input								14.0 KiB	82
;;; drop invalid												
2		drop	input								614 B	13
;;; allow ICMP												
3		accept	input			1 (icmp)			ether1		0 B	0
4		accept	input			1 (icmp)			ether2		0 B	0
;;; allow Winbox												
5		accept	input			6 (tcp)			ether1		0 B	0
6		accept	input			6 (tcp)			ether2		0 B	0
;;; allow SSH												
7		accept	input			6 (tcp)			ether1		0 B	0
8		accept	input			6 (tcp)			ether2		0 B	0
;;; block everything else												
9		drop	input						ether1		389.9 KiB	2 631
10		drop	input						ether2		4472 B	31
;;; accept established												
11		accept	forward								511.3 MiB	513 022
;;; accept related												
12		accept	forward								959 B	11
;;; drop invalid												
13		drop	forward								7.5 KiB	188
;;; drop access to clients behind NAT from WAN												
14		drop	forward						ether1		0 B	0
15		drop	forward						ether2		0 B	0

Рис. 2.7. Вивід параметрів налаштування брандмауера на маршрутизаторі RouterMT

Правила для вхідного трафіку (input) виконують такі дії:

- правила 0-2 приймають з'єднання, пов'язані з уже існуючими;

- правила 3-4 дозволяють ICMP (ping) на інтерфейсах ether1 та ether2;

- правила 5-6 дозволяють доступ до Winbox (TCP port 8291) на інтерфейсах ether1 та ether2;

- правила 7-8 дозволяють доступ по протоколу SSH (TCP port 22) на інтерфейсах ether1 та ether2;

- правила 9-10 відкидають все інші вхідні підключення на інтерфейси ether1 та ether2.

Правила для пересилання трафіку (forward) виконують такі дії:

- правила 11-13 приймають з'єднання, пов'язані з уже існуючими встановленими;

- правила 14-15 відкидають новий трафік з вхідних інтерфейсів ether1 та ether2, що призначений для клієнтів за NAT.

На рис. 2.8 показано налаштування NAT на маршрутизатора RouterMT.

```
[admin@RouterMT] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=masquerade to-addresses=0.0.0.0
      src-address=192.168.111.0/24 out-interface=ether1

 1    chain=srcnat action=masquerade src-address=192.168.111.0/24
      out-interface=ether2
[admin@RouterMT] >
```

Рис. 2.8. Вивід параметрів налаштування NAT на маршрутизаторі RouterMT

Ці правила маскування IP-адрес в MikroTik призначені для приховування внутрішньої мережі (192.168.111.0/24) за однією зовнішньою IP-адресою. Основна відмінність між ними полягає у виборі активного маршруту за замовчуванням, через який відбувається маскування. Якщо активний маршрут до Інтернету через інтерфейс ether1, то правило маскування застосовуватиметься до пакетів, які виходять через цей інтерфейс. Якщо активний маршрут через інтерфейс ether2, то правило маскування буде виконуватися для пакетів, які виходять через цей інтерфейс. Таким чином, правила маскування налаштовані таким чином, щоб вони відповідали активному маршруту за замовчуванням для забезпечення приховування внутрішньої мережі за однією зовнішньою IP-адресою.

2.4. Перевірка працездатності лабораторного середовища

Здійснимо перевірку працездатності лабораторного середовища з операційної системи Windows 11, яка розміщена в локальній мережі (див. рис. 2.1).

На рис. 2.9 показано мережеві налаштування операційної системи Windows 11.

```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-74-C3-15
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::fcfb:f868:c738:9bc2%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.111.60(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 26 листопада 2023 р. 13:30:38
   Lease Expires . . . . . . . . . . : 29 листопада 2023 р. 13:30:37
   Default Gateway . . . . . . . . . : 192.168.111.1
   DHCP Server . . . . . . . . . . . : 192.168.111.1
   DHCPv6 IAID . . . . . . . . . . . : 100666409
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-6E-C6-39-00-0C-29-74-C3-15
   DNS Servers . . . . . . . . . . . : 192.168.111.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Рис. 2.9. Вивід команди ipconfig /all в Windows 11

Цей вивід свідчить про те, що Windows 11 отримав правильні мережеві налаштування за допомогою DHCP з маршрутизатора RouterMT.

На маршрутизаторі RouterMT також можна перевірити стан оренди IP-адрес в DHCP сервері та переконатись що Windows 11 отримав мережеві налаштування (див.рис.2.10).

```
[admin@RouterMT] > ip dhcp-server lease print
Flags: X - disabled, R - radius, D - dynamic, B - blocked
 #   ADDRESS                                MAC-ADDRESS       HOST-NAME              SERVER
 0 D 192.168.111.60                         00:0C:29:74:C3:15 WIN11EnterpriseEN      dhcp1
[admin@RouterMT] >
```

Рис. 2.10. Вивід команди ip dhcp-server lease print на маршрутизаторі RouterMT

Для перевірки якості зв'язку між Windows 11 і IP-адресою 8.8.8.8 використаємо програму WinMTR.

WinMTR - це програма для Windows, яка поєднує в собі функціональність утиліти traceroute і утиліти ping. Вона дозволяє виконувати трасування шляху пакетів до вказаної IP-адреси або доменного імені та вимірювати час затримки для кожного хосту на шляху.

На рис. 2.11 показано перевірку якості зв’язку до IP-адреси DNS сервера google.com.

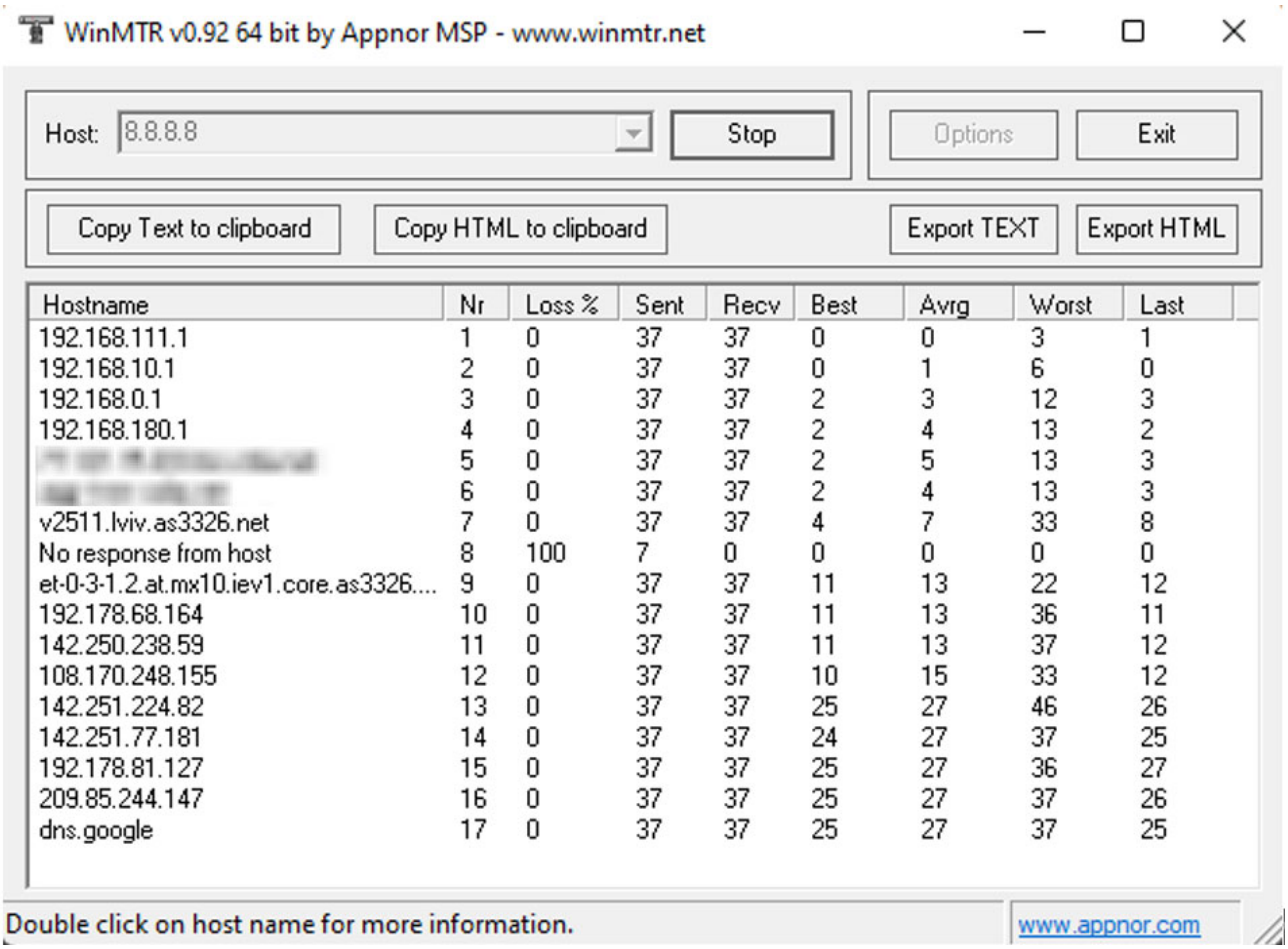


Рис. 2.11. Перевірки якості зв'язку до IP-адреси 8.8.8.8

Отже всі складові лабораторного середовища працюють коректно. Лабораторне середовище повністю готове до розробки та впровадження системи керування та резервування зв’язку.

2.5. Висновки до розділу

У цьому розділі було детально розглянуто засоби для створення лабораторного середовища системи резервування. Використання MikroTik CHR у лабораторному середовищі для системи резервування надає можливість використання всіх функціональних можливостей RouterOS в віртуальному середовищі. CHR підтримує архітектуру x86 64-біт і може бути запущений на більшості популярних гіпервізорах. Це дозволяє емулювати мережеве оточення, використовуючи різні протоколи маршрутизації, функції VPN, QoS та інші

функції, що притаманні RouterOS. Крім того, велика гнучкість налаштування CHR дозволяє створювати складні мережеві конфігурації та тестувати різні сценарії відновлення під час відмов та переключення трафіку на резервні канали зв’язку.

РОЗДІЛ 3
РОЗРОБКА СИСТЕМИ РЕЗЕРВУВАННЯ ТА КЕРУВАННЯ ТРАФІКОМ

3.1. Модифікування налаштувань локального маршрутизатора

Для забезпечення коректної роботи системи резервування трафіку потрібно провести зміни в конфігурації маршрутизатора RouterMT. На рис.3.1 показано додаткові налаштування, які є необхідними для наступних етапів впровадження системи резервування.

```
[admin@RouterMT] > /ip dhcp-client print
Flags: X - disabled, I - invalid
 #    INTERFACE          USE-PEER-DNS ADD-DEFAULT-ROUTE STATUS       ADDRESS
 0    ether2             yes          no                bound        192.168.20.28/24
 1    ether1             yes          no                bound        192.168.10.30/24
[admin@RouterMT] > /ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                          192.168.10.1              3
 1   S  0.0.0.0/0                          192.168.20.1              4
 2 A S  1.1.1.1/32                         192.168.10.1              1
 3 A S  1.1.1.2/32                         192.168.20.1              1
 4 A S  8.8.4.4/32                         192.168.20.1              1
 5 A S  8.8.8.8/32                         192.168.10.1              1
 6 ADC  192.168.10.0/24    192.168.10.30   ether1                    0
 7 ADC  192.168.20.0/24    192.168.20.28   ether2                    0
 8 ADC  192.168.111.0/24   192.168.111.1   bridge1                   0
[admin@RouterMT] >
```

Рис. 3.1. Вивід змінених налаштувань маршрутизатора RouterMT

У налаштуваннях DHCP-клієнтів можна побачити, що інтерфейси ether1 і ether2 мають налаштований DHCP-клієнт. Статус bound означає, що ці інтерфейси успішно отримали IP-адресу від DHCP-сервера.

Статус ADD-DEFAULT-ROUTE=no вказує на тещо DHCP-клієнт не використовує маршрут за замовчуванням від DHCP-сервера.

Щодо таблиці маршрутизації, маємо декілька статичних маршрутів (з прапорцем "S"). Маршрути для адрес 1.1.1.1, 1.1.1.2, 8.8.4.4, та 8.8.8.8 вказують на шлюзи 192.168.10.1 та 192.168.20.1 з відповідною вагою 1. Ці маршрути

будуть використовуються для розробки алгоритму роботи системи резервування трафіку.

Маршрути за замовчуванням 0.0.0.0/0 також встановлено як статичні і мають вагу 3 та 4 відповідно для шлюзів 192.168.10.1 та 192.168.20.1. Маршрут за замовчуванням з вагою 4 не активний в даний момент.

На рис.3.2 продемонстровано налаштування 3G USB модему Huawei E1550 з метою використання його як каналу зв'язку у випадку недоступності основного та резервного маршрутів.

```
[admin@RouterMT] > interface/ppp-client/print
Flags: X - disabled; R - running
 0 X  name="ppp-out1" max-mtu=1500 max-mru=1500 mrru=disabled port=usb3
      data-channel=0 info-channel=0 apn="internet" pin="" user="" password=""
      profile=default phone="" dial-command="ATDT" modem-init="" null-modem=no
      dial-on-demand=yes add-default-route=yes default-route-distance=1
      use-peer-dns=yes keepalive-timeout=30 allow=pap,chap,mschap1,mschap2
```

Рис. 3.2. Налаштування 3G USB модему Huawei E1550

Операційна система RouterOS має вбудовану підтримку даного типу модема. Модем призначений для доступу до Інтернету через мобільні мережі та підтримує роботу в мережах GSM/GPRS/EDGE/UMTS/HSPA. Це означає, що він може підключатися до різних типів мереж, включаючи 2G (GSM), 2.5G (GPRS/EDGE), та 3G (UMTS/HSPA).

Зазвичай, швидкість передачі даних модему E1550 в мережах 3G може сягати до 3.6 Mbps на вхід та до 384 kbps на вихід.

Також модем підтримує додаткові функції, такі як відправлення SMS-повідомлень.

Додатково потрібно налаштувати NAT для інтерфейсу ppp-out1 (див. рис.3.3) та дозволити вихід в Інтернет через 3G (див. рис.3.4) лише тим хостам в локальній мережі, яким це критично необхідно.

```
[admin@RouterMT] > ip firewall/nat/print
Flags: X - disabled, I - invalid; D - dynamic
 0    chain=srcnat action=masquerade src-address=192.168.111.0/24
      out-interface=ether1 log=no log-prefix=""

 1    chain=srcnat action=masquerade src-address=192.168.111.0/24
      out-interface=ether2 log=no log-prefix=""

 2 I  ;;; ppp-out1 not ready
      chain=srcnat action=masquerade src-address=192.168.111.0/24
      out-interface=ppp-out1 log=no log-prefix=""
[admin@RouterMT] >
```

Рис. 3.2. Налаштування NAT для інтерфейсу ppp-out1

Правило під номером 2 налаштовує NAT для інтерфейсу ppp-out1. Це правило буде спрацьовувати коли інтерфейс ppp-out1 перейде в активний стан.

```
16    ;;; 3G Internet
      chain=forward action=accept src-address=192.168.111.60
      in-interface=ppp-out1 log=no log-prefix=""

17    chain=forward action=drop in-interface=ppp-out1 log=no log-prefix=""

[admin@RouterMT] >
```

Рис. 3.3. Додаткові правила брандмауеру для інтерфейсу ppp-out1

Правило 16 в брандмауері відображає налаштування, що дозволяє трафік із IP-адреси 192.168.111.60, який прохоить через інтерфейс ppp-out1. Правило 17 блокує будь-який трафік, який проходить через інтерфейс ppp-out1.

3.2. Розробка програмного коду

Перед написання програмного коду для системи резервування трафіку була розроблена блок-схема, яка описує алгоритм роботи цієї системи. Вона міститься у додатку Б.

Згідно блок-схеми спочатку присвоюються змінні, які використовуються для подальшої роботи алгоритму. Далі здійснюється моніторинг доступності та якості зв’язку по основному та резервному каналах. В залежності від результатів моніторингу відбувається переключення на резервний канал зв’язку з надсиланням повідомлення електронною поштою, або на екстрений канал

зв’язку з використанням 3G та надсиланням SMS повідомлення про критичну ситуацію зі з’єднанням.

MikroTik RouterOS використовує мову сценаріїв, яка базується на власній реалізації shell-сценаріїв (скриптів) та підтримує ряд команд та функцій для автоматизації конфігурації, моніторингу та управління мережним обладнанням MikroTik [2].

Мова має зрозумілий і простий синтаксис, що спрощує розробку скриптів та автоматизацію задач. Підтримує широкий спектр вбудованих команд для роботи з інтерфейсами, IP-адресами, маршрутами, брандмауерами, DHCP, VPN, QoS та іншими аспектами мережевої конфігурації. Дозволяє використовувати змінні, розгалуження, цикли та інші конструкції для керування виконанням сценаріїв. Має можливість реагувати на певні події в мережі, такі як зміна стану інтерфейсів, отримання пакетів, зміни конфігурації тощо. Також є можливість виводити інформацію в консоль, журнал подій або відправляти сповіщення електронною поштою, SMS тощо.

Скрипти можуть виконуватися через командний рядок (CLI) або за розкладом через планувальник завдань (Scheduler).

Мова сценаріїв в RouterOS надає користувачам широкі можливості для автоматизації та налаштування мережевого обладнання MikroTik відповідно до їх потреб.

На початку скрипта встановлено ряд змінних для визначення параметрів мережі та інших налаштувань. Основні змінні включають імена інтерфейсів (ether1, ether2, ppp-out1), IP-адреси шлюзів (gw1 та gw2), IP-адреси хостів, які використовуються для тестування стану каналів (gw1host1, gw1host2, gw2host1, gw2host2), кількість спроб команди ping (pingCount), порогові значення стабільності підключення (ThresholdGw1, ThresholdGw2, ThresholdGw1to3G, ThresholdGw2to3G), маркер для журналювання подій (logmark) та бажані значення для налаштування відстаней маршрутизації (if1desiredDistance та if2desiredDistance) (див. рис. 3.4).

```
# Define variables
# First interface name
:local if1 "ether1";
# Second interface name
:local if2 "ether2";
#3G modem interface name
:local ifppp "ppp-out1";
# First gateway IP address
:local gw1 "192.168.10.1";
# Second gateway IP address
:local gw2 "192.168.20.1";
# First host to ping via gw1
:local gw1host1 "8.8.8.8";
# Second host to ping via gw1
:local gw1host2 "1.1.1.1";
# First host to ping via gw2
:local gw2host1 "8.8.4.4";
# Second host to ping via gw2
:local gw2host2 "1.1.1.2";
# Number of ping attempts
:local pingCount 10;
# Threshold for stable connection (%)
:local ThresholdGw1 90;
:local ThresholdGw2 95;
:local ThresholdGw1to3G 30;
:local ThresholdGw2to3G 30;
# Log marker for logging purposes
:local logmark "---> ";
# set distance
:local if1desiredDistance 3;
:local if2desiredDistance 4;
#
```

Рис. 3.4. Лістинг фрагменту коду встановлення змінних в скрипті

На рис. 3.5 показано лістинг фрагмент коду для перевірки та включення інтерфейсів, якщо вони вимкнені. Це забезпечує перевірку та встановлення вихідних умов для подальшої роботи скрипта.

```
# Check if interfaces are disabled, enable if needed
:if ([/interface ethernet get $if1 disabled] = true) do={
    /interface ethernet set $if1 disabled=no;
    :delay 5s;
} else={
    :put ("Interface $if1 is already enabled.");
    :log info ($logmark . "Interface $if1 is already enabled.");
}
#
:if ([/interface ethernet get $if2 disabled] = true) do={
    /interface ethernet set $if2 disabled=no;
    :delay 5s;
} else={
    :put ("Interface $if2 is already enabled.");
    :log info ($logmark . "Interface $if2 is already enabled.");
}
#
```

Рис. 3.5. Лістинг коду перевірки стану езернет інтерфейсів

Для перевірки якості зв’язку до тестових хостів використовується фрагмент коду наведений на рис.3.6. У цьому фрагменті коду виконуються тести за допомогою команди ping до вказаних хостів через основний та резервний канали зв’язку. Обчислюється відсоткове співвідношення успішних пінгів до хостів через кожен канал зв’язку зі збереженням результатів у змінних pingStatus1 та pingStatus2 відповідно.

```
#
# Perform ping tests on gateway hosts
:log info ($logmark . "start ping gw1  IP $gw1host1 and $gw1host2");
#
:local pingStatus1 \
    ((( [/ping $gw1host1 interface=$if1 count=$pingCount] + \
    [/ping $gw1host2 interface=$if1 count=$pingCount] ) / ($pingCount * 2)) * 100);
:put ("pingStatus1 $pingStatus1");
:log info ($logmark . "PingStatus1:  $pingStatus1 %");
:log info ($logmark . "ping stop gw1");
#
:log info ($logmark . "start ping gw2  IP $gw2host1 and $gw2host2");
#
:local pingStatus2 \
    ((( [/ping $gw2host1 interface=$if2 count=$pingCount] + \
    [/ping $gw2host2 interface=$if2 count=$pingCount] ) / ($pingCount * 2)) * 100);
:put ("pingStatus2 $pingStatus2");
:log info ($logmark . "PingStatus2:  $pingStatus2 %");
:log info ($logmark . "ping stop gw2");
```

Рис. 3.6. Лістинг коду перевірки якості зв’язку до тестових хостів

Для перевірки адміністративної відстані (пріоритету) основного та резервного каналу зв’язку використовується фрагмент коду наведений на рис.3.7. Цей фрагмент коду дозволяє перевіряти та змінювати адміністративні відстані маршрутизації для маршруті за замовчуванням, що допомагає контролювати коректність їх значення.

```
#
# Check and adjust route distances
:local if1Distance [/ip route get [find dst-address=0.0.0.0/0 gateway=$gw1] distance];
:local if2Distance [/ip route get [find dst-address=0.0.0.0/0 gateway=$gw2] distance];
#
:if ($if1Distance != $if1desiredDistance) do={
    /ip route set [find dst-address=0.0.0.0/0 gateway=$gw1] distance=$if1desiredDistance;
    :log warning  ($logmark . "Distance for 0.0.0.0/0 via gateway $gw1 set to \
    $if1desiredDistance");
} else={
    :log warning ($logmark . "Distance for 0.0.0.0/0 via gateway $gw1 is already \
    $if1desiredDistance");
    }
#
:if ($if2Distance != 2 && $if2Distance != 4) do={
    /ip route set [find dst-address=0.0.0.0/0 gateway=$gw2] distance=$if2desiredDistance;
    :log warning  ($logmark . "Distance for 0.0.0.0/0 via gateway $gw2 set to \
    $if2desiredDistance");
} else={
    :log warning ($logmark . "Distance for 0.0.0.0/0 via gateway $gw2 is OK");
    }
```

Рис. 3.7. Лістинг коду перевірки адміністративної відстані маршруту

На рис.3.8 наведено фрагмент коду, який використовує перевірку стабільності підключення до Інтернету через основний та резервний канали зв’язку для прийняття рішення про зміну маршрутизації за замовчуванням. Якщо якість зв’язку через основний шлюз падає нижче встановленого порогу, скрипт перевіряє якість зв’язку через резервний шлюз. Якщо стабільність роботи через резервний канал вище встановленого порогу і в даний момент цей канал не використовується (адміністративні відстань не рівна 2) відбувається зміна маршруту за замовчуванням з надсиланням повідомлення на електронну пошту про зміни в маршрутизації [10].

```
#
# Check internet connection stability and take action accordingly
:if ($pingStatus1 < $ThresholdGw1) do={
    :log error ($logmark . "main Internet channel problem");

    :if ($pingStatus2 > $ThresholdGw2) do={

        :if ($if2Distance  != 2) do={
        /interface/ppp-client/disable ppp-out1;
        /ip route set [find dst-address=0.0.0.0/0 gateway=$gw2] distance=2;
        :log warning ($logmark . "Distance for 0.0.0.0/0 via gateway $gw2 changed to 2");
        :delay 5s;
# Email notification
        /tool e-mail send server=mail.cs.networkacad.net port=25 \
        to=alert.router.cstntu@gmail.com from=mikrotik@cs.networkacad.net \
        subject="MikroTik: Alert $[/system clock get date], $[/system clock get time]" \
        body="switching to a backup Internet channel\nDate: $[/system clock get date]\nTime:
        $[/system clock get time]\nPingStatus:  $pingStatus1 %";
        :log warning ($logmark . "switching to a backup Internet channel. mail sent");
        } else={
        :put ("backup Internet channel is already in use");
        :log info ($logmark . "backup Internet channel is already in use");
            }
        }
```

Рис. 3.8. Лістинг коду переключення на резервний канал зв’язку

Фрагмент коду наведений рис.3.9 виконує перевірку стабільності підключення до Інтернету через основний та резервні канали зв’язку. Якщо якість зв’язку основного та резервного каналів виявляється недостатньою (нижче порогового значення), скрипт переходить до виконання альтернативних дій. У цьому випадку, якщо 3G інтерфейс є вимкненим, скрипт активує 3G підключення та надсилає SMS-повідомлення на вказаний номер телефону про проблеми з усіма каналами зв’язку [11].

Якщо 3G інтерфейс вже використовується, скрипт тільки реєструє цей факт. Такий механізм дозволяє системі автоматично активувати резервне 3G підключення в разі проблем з усіма каналами зв’язку.

```
# SMS notification and GSM backup enable
        :if ($pingStatus1 < $ThresholdGw1to3G && $pingStatus2 < $ThresholdGw2to3G) do={

        :if ([/interface ppp-client get $ifppp disabled] = true) do={

        :put ("sms send");
        :log info ($logmark . "sms send");
        /tool sms send usb3 channel=0 "+38097[illegible] message="RouterMT: \
        $[/system clock get date]: \
        $[/system clock get time]: Problem with all internet channels. Switch to 3G.  ";
        /interface/ppp-client/enable ppp-out1;

         } else={
        :put ("3G Internet is already in use");
        :log info ($logmark . "3G Internet is already in use");
                }
                    }
                }
```

Рис. 3.9. Лістинг коду переключення на 3G Інтернет

На рис.3.10 наведено фрагмент скрипта, що здійснює переключення на основний канал зв'язку при його задовільній якості. Фрагмент коду перевіряє, чи адміністративна відстань маршруту через резервний канал є коректною. Якщо значення не дорівнює 4, скрипт виправляє це шляхом встановлення відповідної відстані.

Після внесення змін у маршрут, скрипт відправляє повідомлення по електронній пошті на визначену адресу про переключення на основний канал зв'язку.

```
    :if ($if2Distance  != 4) do={
        /interface/ppp-client/disable ppp-out1;
        /ip route set [find dst-address=0.0.0.0/0 gateway=$gw2] distance=4;
        :log warning ($logmark . "Distance for 0.0.0.0/0 via gateway $gw2 changed to 4");
        :delay 5s;
# Email notification
        /tool e-mail send server=mail.cs.networkacad.net port=25 \
        to=alert.router.cstntu@gmail.com from=mikrotik@cs.networkacad.net \
        subject="MikroTik: Alert $[/system clock get date], $[/system clock get time]" \
        body="switching to the main Internet channel\nDate: $[/system clock get date]\nTime:
        $[/system clock get time]\nPingStatus:  $pingStatus1 %";
        :log warning ($logmark . "switching to the main Internet channel. mail sent");
        }
    }
```

Рис. 3.10. Лістинг коду переключення на основний канал зв'язку

Програмний код системи резервування та керування трафіком збережено в файловому сховищі маршрутизатора RouterMT під назвою channel-monitoring та наведено в додатку В.

3.3. Тестування системи резервування

Для виконання періодичних перевірок з'єднання використаємо планувальником завдань (Scheduler) в MikroTik RouterOS.

Планувальник завдань - це функція, яка дозволяє автоматизувати виконання різноманітних завдань у визначені моменти часу або за регулярними інтервалами. Він дозволяє налаштовувати певні дії на маршрутизаторі в певний час або з певною періодичністю без потреби постійного втручання адміністратора. Планувальник виконує задані дії або викликає певні команди в певний час або під час певних подій, наприклад, викликає скрипт, змінює налаштування інтерфейсів, створює резервні копії конфігурації тощо. Планувальник може відслідковувати кількість виконаних задач, що дозволяє контролювати час та частоту виконання певних дій.

На рис.3.11 показано налаштування планувальника завдань для періодичного запуску програмного коду системи резервування та керування трафіком.

```
[admin@RouterMT] > system/scheduler/print
Columns: NAME, START-DATE, START-TIME, INTERVAL, ON-EVENT, RUN-COUNT
# NAME                  START-DATE   START-TIME  INTERVAL  ON-EVENT           R
0 channel_monitoring_task  nov/20/2023  11:05:06    1m30s     channel-monitoring  8
[admin@RouterMT] >
```

Рис. 3.11. Налаштування планувальника завдань

У нашому випадку існує одне завдання планувальника з ім'ям channel_monitoring_task. Це завдання запускається кожні півтори хвилини з 20 листопада 2023 року. Кількість виконаних запусків цього завдання становить 8. Кожен раз, коли це завдання виконується, воно викликає подію channel-

monitoring. Ця подія є назвою скрипта системи резервування та керування трафіком.

Планувальник завдань дозволяє автоматизувати багато рутинних операцій на маршрутизаторі, що спрощує управління мережею та дозволяє зосередитися на більш складних завданнях адміністрування мережі.

Проведемо тестування коректності роботи системи резервування. На першому етапі змоделюємо ситуацію погіршення якості з'єднання через основний канал зв'язку.

На рис. 3.12 можна побачити, що було задіяно резервний канал зв'язку як маршрут за замовчуванням.

```
[admin@RouterMT] > ip route/print
Flags: D - DYNAMIC; A - ACTIVE; c, s, y - COPY
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#      DST-ADDRESS        GATEWAY         DISTANCE
0  As  0.0.0.0/0          192.168.20.1           2
1   s  0.0.0.0/0          192.168.10.1           3
2  As  1.1.1.1/32         192.168.10.1           1
3  As  1.1.1.2/32         192.168.20.1           1
4  As  8.8.4.4/32         192.168.20.1           1
5  As  8.8.8.8/32         192.168.10.1           1
   DAc 192.168.10.0/24    ether1                 0
   DAc 192.168.20.0/24    ether2                 0
   DAc 192.168.111.0/24   bridge1                0
[admin@RouterMT] >
```

Рис. 3.12. Таблиця маршрутизації при переключенні на резервний канал

Послідовність дій скрипта також можна відслідкувати в журналі подій MikroTik (див.рис.3.13).

Журнал подій MikroTik - це системний журнал, який зберігає інформацію про події, що відбуваються в маршрутизаторі MikroTik, такі як помилки, сповіщення, дії адміністраторів тощо. Цей журнал є важливим інструментом для аналізу та моніторингу пристрою та мережі в цілому.

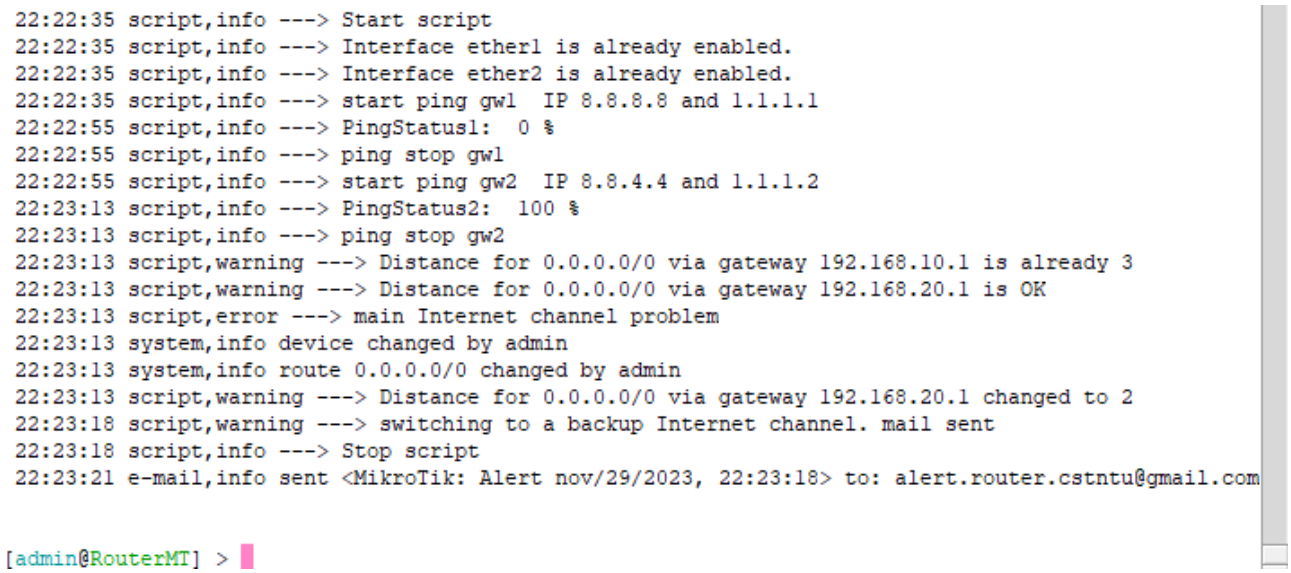


Рис. 3.13. Записи журналу MikroTik при переключенні на резервний канал

Події в журналі класифікуються за різними рівнями важливості, такими як інформаційні повідомлення, попередження, помилки та інші.

Журнал подій містить інформацію про різноманітні події, такі як зміни налаштувань, з'єднання або відключення, помилки маршрутизації, відновлення зв'язку, зміни конфігурації, спроби входу до системи, відмови в авторизації та інше. Є можливість фільтрувати події за різними критеріями, такими як рівень важливості, час, тип події та інші параметри для швидкого пошуку необхідної інформації.

Записи в журналі зберігаються пристроєм протягом визначеного періоду часу і можуть відображатися через веб-інтерфейс, CLI або інші інструменти адміністрування.

На рис. 3.14 показана перевірка якості зв'язку з Windows 11 через резервний канал. Маршрут проходить через IP-адресу 192.168.20.1, яка належить маршрутизатору ISP2.

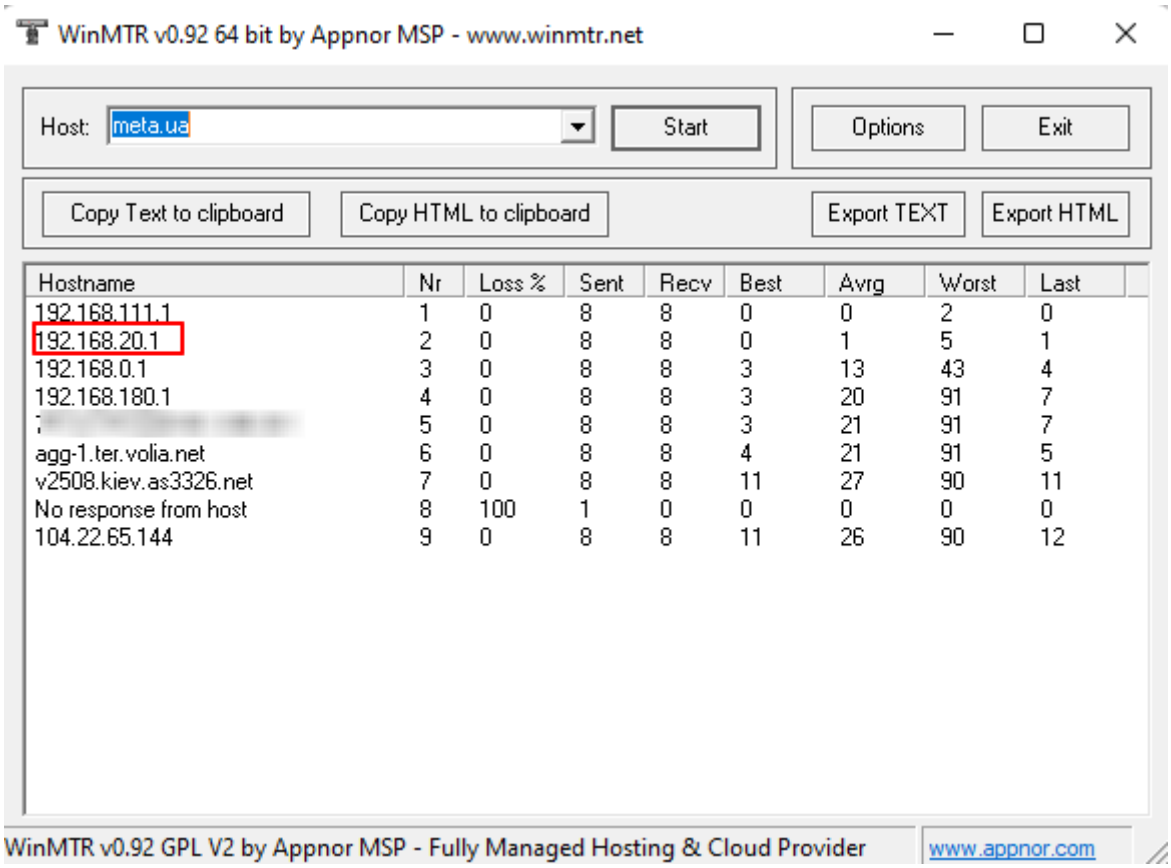


Рис. 3.14. Перевірка маршрутизації з Windows 11 при переключенні на резервний канал

Повідомлення про зміну маршрутизації, надіслане на електронну пошту після автоматичного переключення на резервний канал, це необхідна функція в системах мережевого управління. Це дозволяє адміністраторам мережі вчасно виявляти та реагувати на зміни в мережевому стані.

У нашому випадку, MikroTik автоматично відправив електронне повідомлення на вказану адресу електронної пошти про зміну маршрутизації (див.рис.3.15). Це важливо для адміністратора для відстеження змін у мережі, зокрема автоматичного переходу на резервний канал.

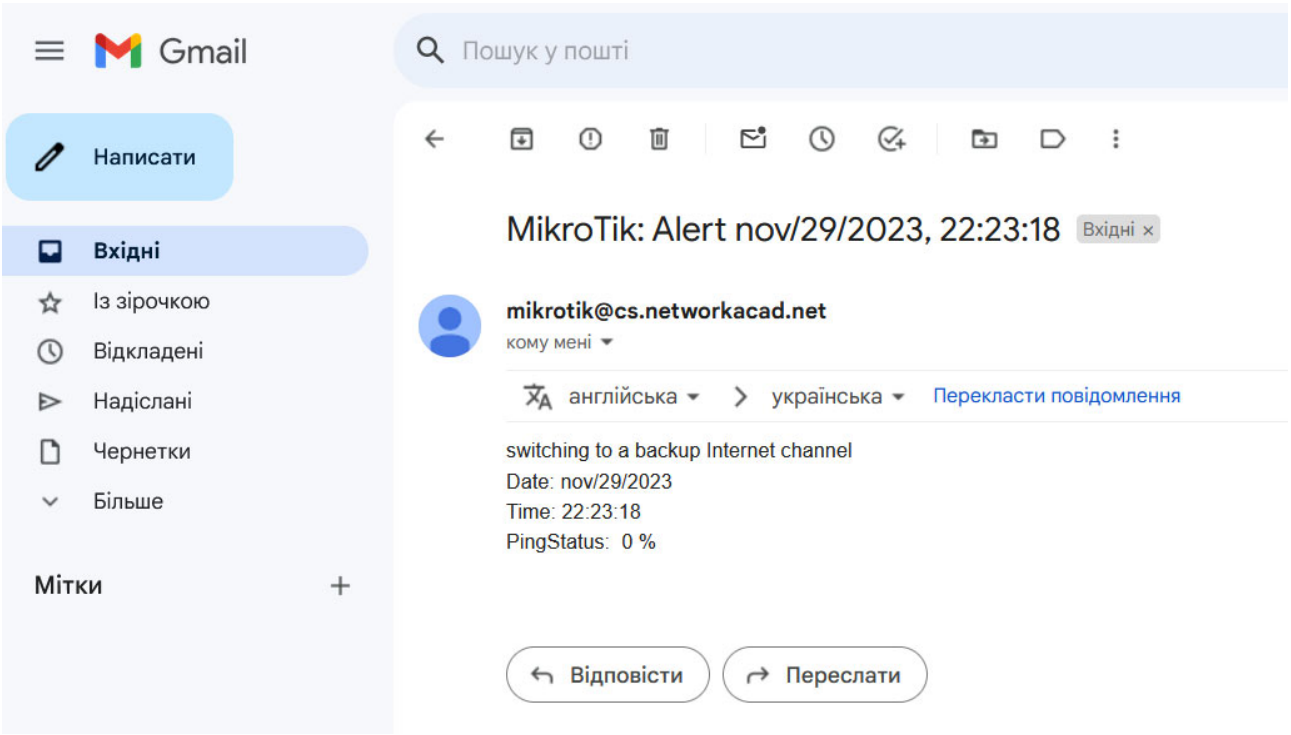


Рис. 3.15. Поштове повідомлення про переключення на резервний канал

Такі повідомлення дозволяють оперативно реагувати на ситуації, коли виникають проблеми з основним каналом і мережа автоматично переключається на резервний для забезпечення безперервності роботи.

На другому етапі змоделюємо ситуацію погіршення якості з'єднання через резервний канал зв'язку. На рис. 3.16 можна побачити, що було задіяно екстрений канал зв'язку з використанням 3G як маршрут за замовчуванням.

```
[admin@RouterMT] > ip route/print
Flags: D - DYNAMIC; A - ACTIVE; c, s, v, y - COPY
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#     DST-ADDRESS        GATEWAY         DISTANCE
  DAv 0.0.0.0/0          ppp-out1               1
0   s 0.0.0.0/0          192.168.20.1           2
1   s 0.0.0.0/0          192.168.10.1           3
2  As 1.1.1.1/32         192.168.10.1           1
3  As 1.1.1.2/32         192.168.20.1           1
4  As 8.8.4.4/32         192.168.20.1           1
5  As 8.8.8.8/32         192.168.10.1           1
  DAc 10.112.112.137/32  ppp-out1               0
  DAc 192.168.10.0/24    ether1                 0
  DAc 192.168.20.0/24    ether2                 0
  DAc 192.168.111.0/24   bridge1                0
[admin@RouterMT] >
```

Рис. 3.16. Таблиця маршрутизації при переключенні на екстрений канал

В таблиці маршрутизації з’явився динамічний маршрут до 0.0.0.0/0 через інтерфейс ppp-out1 з адміністративною відстанню 1. Цей маршрут використовується як основний.

На рис.3.17 показано журнал подій при переключенні на канал зв’язку з використанням 3G.

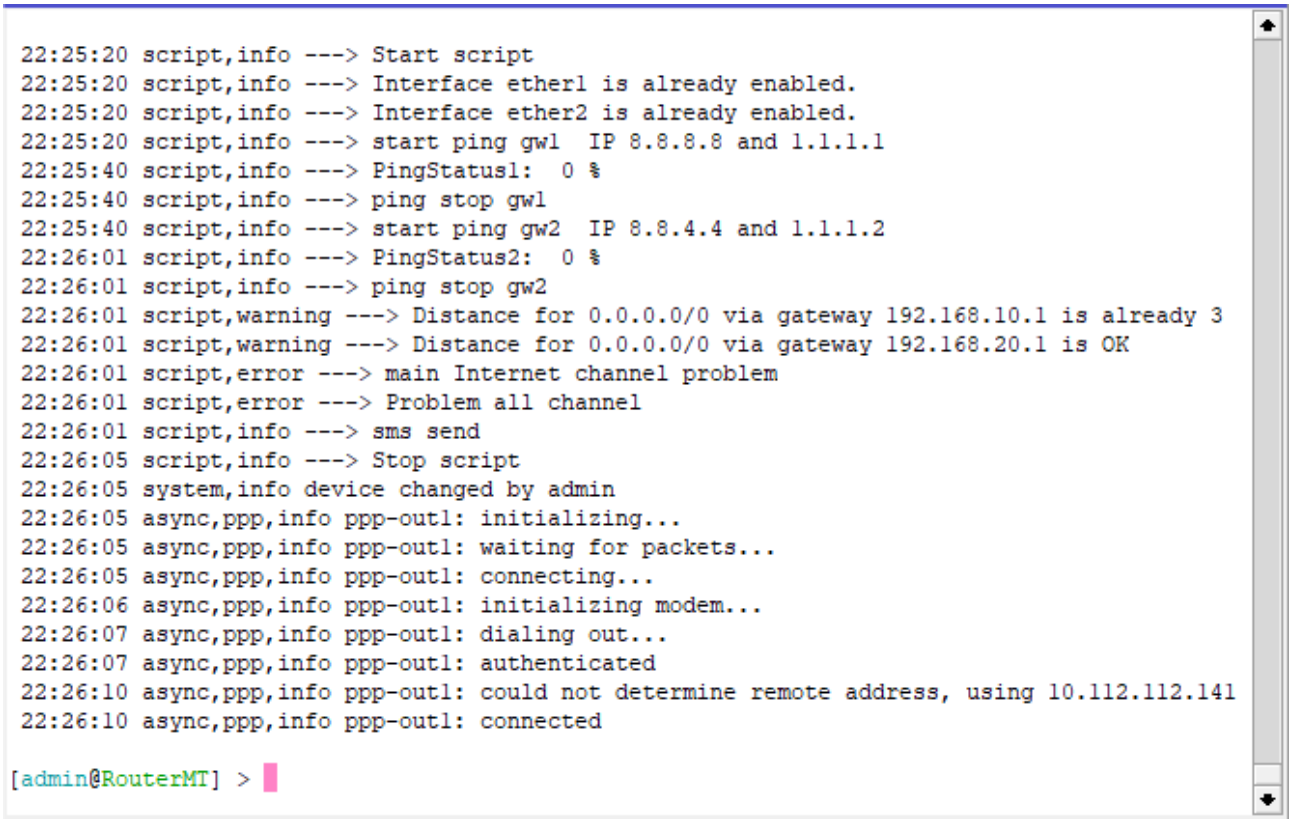


Рис. 3.17. Записи журналу MikroTik при переключенні на екстрений канал

При перевірці маршрутизації з Windows 11 за допомогою WinMTR можна побачити що шлях проходить через екстрений канал зв’язку з використанням 3G (див.рис.3.18).

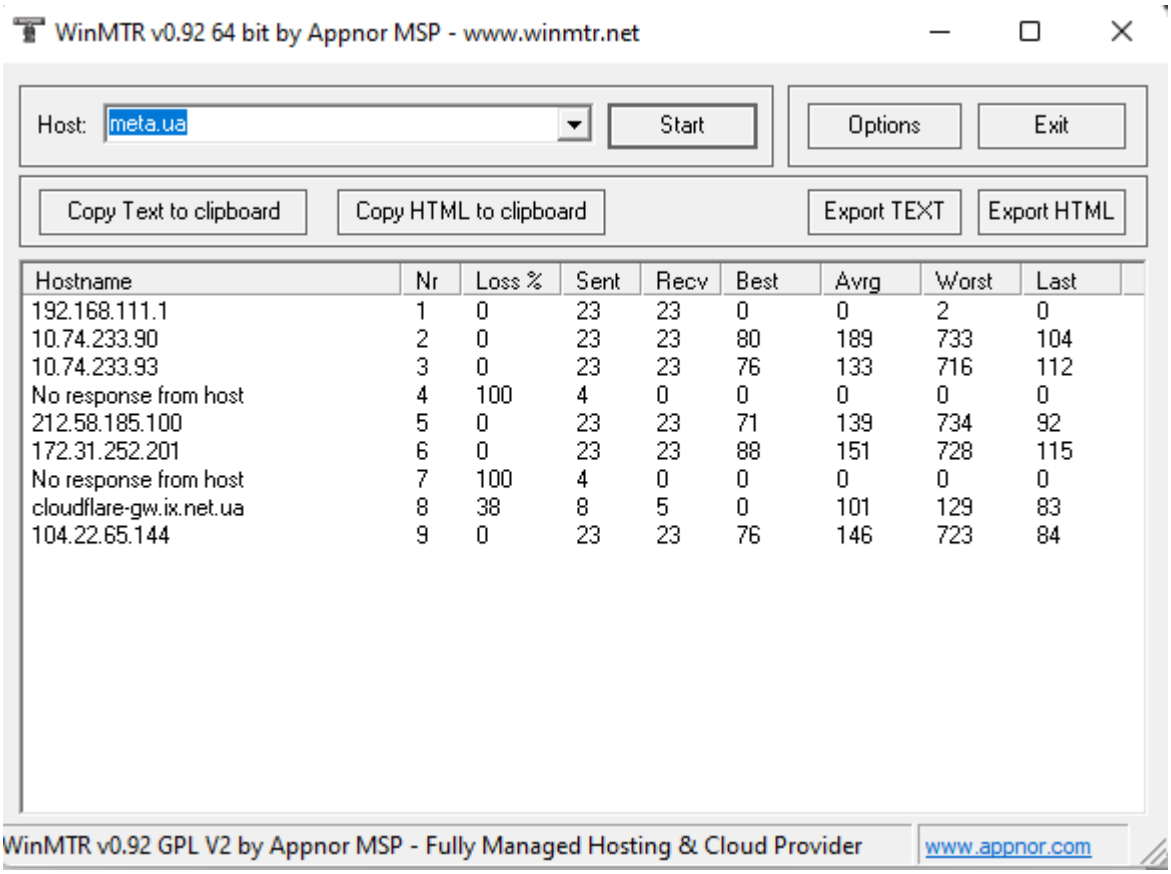


Рис. 3.18. Перевірка маршрутизації з Windows 11 при переключенні на 3G зв’язок

При переключенні на екстрений канал зв’язку з використанням 3G здійснюється надсиланням SMS повідомлення про критичну ситуацію зі з’єднанням.

На рис.3.19 показано SMS повідомлення, яке надійшло з маршрутизатора MikroTik після переключення на 3G з’єднання. SMS-інформування при відсутності з'єднання через основний та резервний канал зв'язку має критичне значення для швидкого реагування на аварійні ситуації.

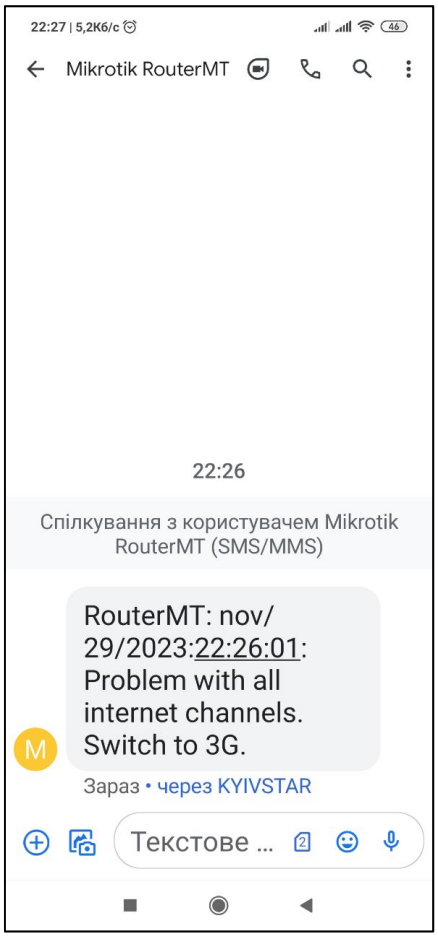


Рис. 3.19. SMS повідомлення про переключення на 3G зв’язок

SMS - це один з найшвидших способів сповіщення. Відправлення SMS зазвичай займає кілька секунд, і отримувач майже миттєво отримує повідомлення. Повідомлення за допомогою SMS зазвичай швидше читаються в порівнянні з іншими формами сповіщення, такими як електронна пошта.

При відновленні зв’язку через основний канал система повертається до початкового стану (див.рис.3.20).

```
[admin@RouterMT] > ip route/print
Flags: D - DYNAMIC; A - ACTIVE; c, s, y - COPY
Columns: DST-ADDRESS, GATEWAY, DISTANCE
#      DST-ADDRESS        GATEWAY        DISTANCE
0    s 0.0.0.0/0          192.168.20.1          4
1  As  0.0.0.0/0          192.168.10.1          3
2  As  1.1.1.1/32         192.168.10.1          1
3  As  1.1.1.2/32         192.168.20.1          1
4  As  8.8.4.4/32         192.168.20.1          1
5  As  8.8.8.8/32         192.168.10.1          1
   DAc 192.168.10.0/24    ether1                0
   DAc 192.168.20.0/24    ether2                0
   DAc 192.168.111.0/24   bridge1               0
[admin@RouterMT] >
```

Рис. 3.20. Таблиця маршрутизації при використанні основного каналу зв’язку

Після переключення на основний канал зв’язку також надсилається повідомлення на електронну пошту про відновлення основного каналу зв’язку (див.рис.3.21).

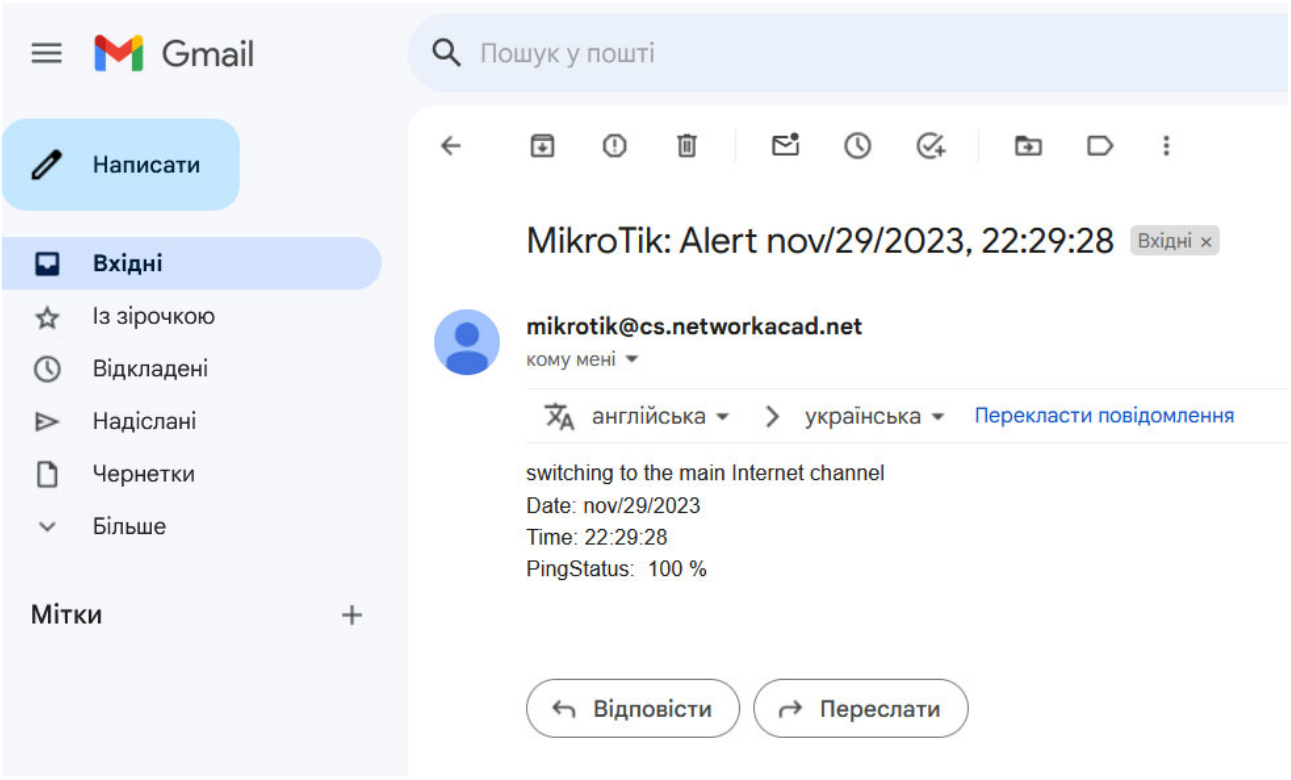


Рис. 3.21. Поштове повідомлення про переключення на основний канал

Успішне проходження всіх етапів тестування показує що система резервування та керування трафіком працює належним чином.

3.4. Висновки до розділу

У процесі створення системи керування та резервування каналів зв’язку було розроблено програмний код для моніторингу та переключення на резервний канал при відсутності зв’язку по основному каналу. Для написання програмного коду була використана вбудована в операційну систему RouterOS скриптова мова програмування. Було проведено процес тестування системи керування та резервування каналів зв’язку в різних аварійних ситуаціях. Також було підтверджено здатність системи виконувати моніторинг каналів зв’язку, здійснювати переключення та інформування за допомогою електронної пошти та SMS під час аварійних ситуацій.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Метою кваліфікаційної роботи є розробка та впровадження системи резервування та керування трафіком на основі маршрутизаторів MikroTik. Оскільки, проведення робіт з розробки та використання системи передбачає використання комп’ютерної техніки, зокрема ПК та периферійних пристроїв, то обов’язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників з розробки системи комп’ютерних систем, в тому числі і фахівців з підвищення ефективності контролю доступу в приміщення, необхідно організувати безпечні умови праці [12]. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями». Згідно Вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до цих вимог:

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

– Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду

України від 28.10.98 N 247 (далі - ДБН В.2.5-56:2014, з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, ДБН В.2.5-56:2010, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп’ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п’ять комп’ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп’ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз’єднання при відключенні має бути зворотним. Не допускається підключати комп’ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп’ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

Важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-7.15-18. Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги». Відстань від екрана до ока фахівців, які працюють за комп’ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп’ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Отже, у результаті аналізу вимог щодо охорони праці користувачів комп’ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи інженерів з розробки та впровадження системи резервування та керування трафіком.

4.2. Безпека в надзвичайних ситуаціях

4.2.1. Підвищення стійкості роботи об’єктів господарської діяльності у воєнний час.

Для покращення стійкості роботи об’єктів вивчають фактори, які впливають на стійкість та оцінюють стійкість елементів і галузей виробництва проти уражаючих факторів ядерної, хімічної і біологічної зброї, стихійних лих і виробничих аварій. Щоб підвищити стійкість необхідно завчасно організувати і провести організаційні, інженерно-технічні й технологічні заходи [13].

Здійснення організаційних заходів передбачає завчасну підготовку всіх структур цивільного захисту, служб і формувань до надзвичайних ситуацій, в тому числі і військових дій. Вжиттям технологічних заходів підвищується стійкість роботи об'єктів шляхом змінювання технологічних процесів, режимів, можливих в умовах різних надзвичайних ситуацій. Інженерно-технічні заходи мають забезпечити підвищену стійкість виробничих споруд, технологічних ліній, устаткування, комунікацій об'єкта до впливу уражаючих факторів під час військових дій. При проведенні цих заходів необхідно враховувати конкретні умови об'єкта народного господарства. Проте є загальні організаційні інженерно-технічні заходи, які мають проводитись на всіх об'єктах.

Одним з найбільш важливих завдань в умовах воєнного часу і надзвичайних ситуацій є забезпечення захисту людей та їх життєдіяльності.

Для підвищення стійкості об’єктів господарювання та захисту людей необхідно:

– створити на об'єкті надійну систему оповіщення про загрози нападу противника, радіоактивне забруднення, хімічне і біологічне зараження, загрозу стихійного лиха і виробничої аварії;

– організувати розвідку і спостереження за радіоактивним забрудненням, хімічним і біологічним зараженням;

– організувати гідрометеорологічне спостереження за рівнем води, напрямком і швидкістю вітру, рухом і поширенням хмари радіоактивного забруднення, сильнодіючих отруйних речовин і отруйних речовин;

– створити фонд захисних споруд ЦО, запасів засобів індивідуального захисту і забезпечення своєчасної видачі їх населенню;

– завчасно підготуватись до масової санітарної обробки населення і знезаражування одягу;

– організувати взаємодію з установами охорони здоров'я для медичного обслуговування населення в умовах воєнного часу.

Також в умовах воєнного часу необхідно провести підготовку до евакуації населення, розміщеного в зонах можливих руйнувань і катастрофічного затоплення. Це передбачає завчасну підготовку місць евакуації, організацію прийому евакуйованого населення на територію населених пунктів. Окрім цього, необхідно забезпечити постачання продуктів харчування, питної води, предметів першої необхідності та провести заходи щодо морально-психологічної підготовки населення до виживання в умовах воєнного часу, забезпечити процес чіткого інформування про обстановку та правила дій і поведінки населення в надзвичайних ситуаціях воєнного часу [13].

Для забезпечення стійкості роботи об'єктів повинні проводитись інженерно-технічні заходи на мережах комунального господарства з метою захисту джерел

тепла із заглибленням у ґрунт комунікацій. Котельні слід розміщувати в спеціальному окремо розміщеному приміщенні.

Якщо об'єкт одержує тепло з міської теплоцентралі, необхідно провести заходи для забезпечення стійкості трубопроводів і розподільних пристроїв, підведених до об'єкта. Теплова мережа має будуватися за кільцевою системою з прокладанням труб у спеціальних каналах зі з'єднанням паралельних ділянок. Для відключення пошкоджених ділянок мають бути встановлені запірно-регулюючі засувки, вентилі та ін. Ці пристосування необхідно розміщувати в оглядових колодязях, на території, що не завалюється при руйнуванні будівель.

Система каналізації має будуватись окремо: одна для дощових, друга для промислових і господарських вод. На об'єкті має бути не менше двох виводів з підключенням до міських каналізаційних колекторів, а також виводи і колодязі з аварійними засувками на об'єктових колекторах з інтервалом 50 м на території, що не завалюється, для аварійного скидання неочищеної води в найближчі штучні та природні заглиблення.

На деяких промислових об'єктах є системи для забезпечення технології виробництва: для подання кисню, аміаку, стиснутого повітря та інших рідких і газових реактивів. Для цих систем розробляють заходи для попередження виникнення вторинних факторів зброї, стихійних лих та виробничих аварій і катастроф.

Створення резерву енергетичних потужностей за рахунок автономних пересувних електростанцій, а також місцевих джерел електроенергії. Підготовка автономних електростанцій до роботи за спеціальним режимом (графіком) для забезпечення технологічних процесів виробництва, для яких неможливі тривалі перерви в електропостачанні. З метою попередження аварій на електричних мережах необхідно установити автоматичну систему відключення при виникненні перенапруги. Повітряні лінії електропостачання замінити на підземно-кабельні. Створення необхідних запасів (резервів) паливно-мастильних матеріалів та інших видів палива й організація їх безпечного зберігання.

Щоб не допустити зупинки підприємства через дефіцит палива, необхідно підготуватись для роботи на різних видах палива: нафта, вугілля, газ. Для підвищення стійкості забезпечення водою слід провести такі заходи.

Необхідно створити основні і резервні джерела водопостачання. Як резервне джерело краще мати артезіанську свердловину, яку необхідно підключити до системи водопостачання. Крім того, воду можна брати з близько розміщеної природної водойми або спорудити штучну водойму чи резервуари з обладнанням пристроїв для збору і перекачування води. Всі ділянки водопостачання повинні бути заглиблені в ґрунт з обладнанням пожежних гідрантів і пристроїв для відключення пошкоджених ділянок. Локальні мережі водопостачання окремих великих підприємств варто з'єднати із 80 загальноміською системою водопостачання в єдине кільце.

Підвищенню стійкості забезпечення водою сприяє подавання води безпосередньо в мережу поза водонапірними баштами, спорудження обвідних ліній для подання води поза пошкодженими спорудами.

Завчасне вжиття заходів захисту джерел водопостачання, водопровідних споруд, свердловин і шахтних колодязів від забруднення радіоактивними речовинами, зараження хімічними і біологічними засобами. Підготовка меліоративних, гідротехнічних та іригаційних споруд і систем до експлуатації в надзвичайних умовах.

Для забезпечення виробництва продукції необхідні електроенергія, паливо, мастила, засоби захисту рослин, міндобрива, профілактичні й лікувальні препарати ветеринарної медицини, запасні частини, сировина та інші матеріально-технічні засоби. Забезпечення об'єктів цими ресурсами дасть можливість випускати необхідну продукцію в надзвичайних умовах мирного і воєнного часу. Тому повинні проводитись такі заходи, які б забезпечили стійкість постачання і сприяли підвищенню захисту мережі електро-, водо-, газопостачання, транспортних комунікацій і джерел постачання всім необхідним для забезпечення функціонування галузей сільського господарства в надзвичайних умовах.

З метою попередження аварій на електричних мережах необхідно встановити автоматичну систему відключення перенапруги. Повітряні лінії електропостачання слід замінити на підземно-кабельні. Газ використовується як паливо і на хімічних підприємствах у технологічному процесі. Для безперебійного забезпечення газом, газові мережі необхідно підводити до об'єкта з двох напрямків, які мають бути з'єднані в єдине кільце з обладнанням для можливого дистанційного автоматичного управління й у разі необхідності відключення пошкоджених ділянок. На великих підприємствах необхідно мати підземні ємності із закачаним резервним газом.

На підприємствах, де використовується пара, необхідно захистити джерела його постачання, заглибити в ґрунт комунікації паропостачання і встановити запірні пристосування.

Запас резервних матеріалів необхідно розраховувати на такі строки роботи підприємства, за які можливе відновлення регулярного постачання.

Передбачити, на випадок перебоїв в постачанні підприємствами-суміжниками, створення місцевих матеріалів, сировини для виготовлення комплектуючих виробів і інструментів силами свого підприємства [13].

Для підвищення стійкості та забезпечення збереження (відновлення) будівель і споруд в умовах воєнного часу необхідно:

– провести оцінку можливих ступенів руйнування будівель і споруд господарства населеного пункту, визначити обсяг невідкладних ремонтних робіт, потреби в будівельних матеріалах;

– створити і підготувати спеціальні формування для ремонтно-відновних, будівельних та інших робіт на об'єкті;

– розробити комплекс протипожежних заходів, які виключали б можливість виникнення масових пожеж.

Для забезпечення надійності системи управління і зв'язку потрібно організувати захищений пункт управління, забезпечити його засобами зв'язку, які б дали можливість швидко доводити сигнали ЦЗ до всіх виробничих підрозділів і населення у місцях проживання. При цьому необхідно здійснити

планування збору даних про обстановку, передачу команд і розпоряджень в умовах впливу на об'єкт уражуючих факторів. Для підвищення стійкості системи управління і зв’язку в умовах воєнного часу необхідно організувати використання радіозасобів, засобів телефонного зв'язку а також забезпечити зв’язок із колонами евакуйованого населення, що перебувають у дорозі, і відповідальними особами, які супроводжують їх під час евакуації, забезпечити дублювання ліній і каналів зв'язку.

4.2.2. Запобігання наслідкам аварії на виробництвах із застосуванням аміаку. Вплив аміаку організм людини. Перша допомога. Профілактика уражень.

Для отримання низьких температур технологічними схемами компресорного цеху багатьох промислових підприємств харчової та переробної промисловості передбачено застосування токсичної речовини –аміаку [14].

Потенційна небезпека таких технологічних схем полягає у порушенні герметичності обладнання і трубопроводів, що містять аміак. Найбільшу небезпеку з цієї точки зору являють собою руйнування автоцистерн з рідким аміаком; руйнування напірних трубопроводів компресорів; порушення герметичності відокремлювачів рідини, лінійних та циркуляційних ресиверів, запірної арматури, батарей холодильних камер. Наслідком таких аварій є виникнення загазованості виробничого приміщення, відкритого майданчика цеху і підприємства в цілому, а також прилеглих житлових районів; утворення вибухонебезпечної суміші аміаку з повітрям в приміщеннях, внаслідок чого можливі вибухи і пожежі.

Джерелами локальних викидів аміаку можуть служити процеси стиснення газоподібного і нагнітання рідкого аміаку, а також інші операції.

Аварії на підприємствах, транспорті та продуктопроводах можуть супроводжуватися викидом (виливом) в атмосферу і на прилеглу територію небезпечних хімічних речовин (НХР), таких як хлор, аміак, синильна кислота, фосген, сірчаний ангідрид та інші. Це являє серйозну небезпеку для населення, заражене повітря уражає органи дихання, а також очі, шкіру та інші органи.

Фактори небезпеки викиду (розливу) хімічно небезпечних речовин: забруднення навколишнього середовища, небезпека для всього живого, що опинилося на забрудненій місцевості (загибель людей, тварин, знищення посівів та ін.), крім того, внаслідок можливого хімічного вибуху виникнення сильних руйнувань на значній території.

Аміак – безбарвний газ з характерним різким запахом і їдким смаком. Він майже у два рази легший від повітря. За звичайних умов аміак легко зріджується під тиском, а при випаровуванні поглинає тепло – сильно охолоджується. Ця властивість використовується у промислових та побутових холодильниках на м'ясокомбінатах, молокозаводах, овочевих базах, тобто там, де є необхідність в охолодженій продукції. Крім того, він є сировиною багатьох хімічних виробництв. Аміак зберігається і транспортується у зрідженому стані. Він один з найважливіших продуктів сучасної хімічної промисловості. Головною галуззю його застосування є виробництво нітратної кислоти і азотних добрив. Крім того, аміак використовують для виробництва багатьох інших хімічних продуктів. Останнім часом зріджений аміак і водний розчин аміаку стали широко застосовувати безпосередньо як азотне добриво. Як рідина, аміак легший за воду, має меншу густину і при виході на повітря утворює слабкий дим. Вогненебезпечний, створює вибухові суміші з повітрям, отруйний. Особливо небезпечний для очей. У випадку розливу рідкого аміаку і його концентрованих розчинів не можна доторкатися до розлитої рідини.

Ознаки отруєння аміаком:

- нежить, кашель, важке дихання, задуха;

- підвищене серцебиття, порушена частота пульсу;

- при контакті з рідким аміаком виникає обмороження, можливий опік з пухирями, виразки.

Перша допомога при отруєнні аміаком:

- одягніть протигаз і виведіть ураженого на свіже повітря;

- дайте подихати зволоженим повітрям (теплими водяними парами 10%-ного розчину ментолу в хлороформі);

- дайте потерпілому теплого молока з харчовою содою;

- при задусі необхідний кисень;

- при спазмі голосових щілин забезпечте тепло на ділянку шиї, теплі ванночки, інгаляцію;

- при зупинці дихання проведіть серцево-легеневу реанімацію;

- при потраплянні в очі − промийте водою;

- при уражені шкіри − обмийте чистою водою, зробіть примочки з 5%- ного розчину оцтової або лимонної кислоти.

При отруєнні аміаком винести потерпілого із зони зараження, шкіру, рот, ніс промити водою. В очі закапати по дві-три краплі 30% альбуциду, в ніс - оливкове масло. При необхідності відправити потерпілого до медичного закладу.

4.3. Висновки до розділу

Четвертий розділ кваліфікаційної роботи присвячений питанням охорони праці та безпеки у надзвичайних ситуаціях. У частині охорони праці розглянуто нормативні акти, що регламентують забезпечення охорони праці при роботі за ЕОМ. У частині безпеки в надзвичайних ситуаціях було розглянуто питання підвищення стійкості роботи об'єктів господарської діяльності у воєнний час шляхом організації та проведення сукупності заходів, які включають організаційні, інженерно-технічні й технологічні заходи. Також було розглянуто питання запобігання наслідкам аварії на виробництвах із застосуванням аміаку.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи магістра проведено дослідження методів керування та резервування каналів зв’язку. В результаті проведених теоретичних і практичних досліджень отримані наступні результати:

- проведено порівняння можливостей Cisco, MikroTik, Juniper, Palo Alto та Fortinet для забезпечення надійності мережі та автоматичного переходу на резервний канал у разі відмови основного зв'язку;

- проаналізовано можливості надсилання сповіщень про перехід на альтернативний канал зв’язку через різні системи комунікації, такі як електронна пошта та SMS;

- розглянуто мережеві можливості маршрутизатора MikroTik CHR для тестування різних сценаріїв відновлення під час відмов зв’язку;

- розроблено програмний код для автоматичного переходу на резервний канал зв’язку у разі відсутності зв’язку через основний канал з можливістю інформування за допомогою електронної пошти та SMS;

- проведено тестування розробленої системи в аварійних ситуаціях, включаючи переключення та інформування за допомогою електронної пошти та SMS про зміну маршрутизації за замовчуванням;

- проведено оцінку здатності системи забезпечувати стабільність мережі, виконувати моніторинг, переключення та інформування в аварійних ситуаціях;

- підтверджено успішність роботи розробленої системи резервування та керування трафіком на основі маршрутизатора MikroTik CHR у ситуаціях обмеженого чи втраченого зв'язку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IP SLA Fundamentals. URL: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKN0EAO/ip-sla-fundamentals (дата звернення: 27.11.2023).

2. RouterOS – Scripting. URL: https://help.mikrotik.com/docs/display/ROS/Scripting (дата звернення: 27.11.2023).

3. Коцюк Н.М., Тимощук В.Д., Момоток Ю.О., Луцик Н.С. Система резервування трафіку на основі MikroTik. Актуальні задачі сучасних технологій : збірник тез доповідей XII міжнародної науково-практичної конференції молодих учених та студентів (Тернопіль, 6–7 грудня 2023 року), Тернопіль: ТНТУ, 2023. С. 419.

4. Configuring Real-Time Performance Monitoring Probes. URL: https://www.juniper.net/documentation/us/en/software/nce/internet-protocol-srx-monitoring/topics/task/ip-monitoring-rpm-configuring.html (дата звернення: 27.11.2023).

5. Failover. URL: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/failover (дата звернення: 27.11.2023).

6. Link monitor. URL: https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/76624/link-monitor (дата звернення: 27.11.2023).

7. Коцюк Н.М., Тимощук В.Д., Луцик Н.С. Актуальні питання розвитку галузей науки: матеріали II міжнародної наукової конференції (Чернігів, 1 грудня 2023 року), Вінниця: ТОВ УКРЛОГОС Груп, 2023. С. 271.

8. Cloud Hosted Router. URL: https://help.mikrotik.com/docs/display/ROS/Cloud+Hosted+Router%2C+CHR-monitor (дата звернення: 27.11.2023).

9. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп’ютерні мережі. [навчальний посібник] Львів: «Магнолія 2006». 2013. 256с.

10. MikroTik Manual:Tools/email. URL: https://wiki.mikrotik.com/wiki/Manual:Tools/email (дата звернення: 27.11.2023).

11. MikroTik Manual:Tools/Sms. URL: https://wiki.mikrotik.com/wiki/Manual:Tools/Sms (дата звернення: 27.11.2023).

12. Лупенко С.А., Луцик Н.С., Луцків А.М., Осухівська Г.М., Тиш Є.В. Методичні вказівки до виконання кваліфікаційної роботи магістра для студентів спеціальності 123 «Комп'ютерна інженерія» другого (магістерського) рівня вищої освіти усіх форм навчання. Тернопіль, ТНТУ. 2021. 34 с.

13. Стручок В.С. Техноекологія та цивільна безпека. Частина «Цивільна безпека». Навчальний посібник. Тернопіль: ТНТУ. 2022. 150 с.

14. Желібо Є. П., Сагайдак І. С. Безпека життєдіяльності. Навчальний посібник для аудиторної та практичної роботи. К.:ЕКОМЕН. 2011. 200 с.

ДОДАТКИ

Додаток А Тези конференцій

СЕКЦІЯ XII.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

СЕКЦІЯ XIII.
ТРАНСПОРТ ТА ТРАНСПОРТНІ ТЕХНОЛОГІЇ

СЕКЦІЯ XIV.
ФІЛОЛОГІЯ ТА ЖУРНАЛІСТИКА

АНАЛІЗ РІШЕНЬ В ГАЛУЗІ РЕЗЕРВУВАННЯ ТА КЕРУВАННЯ ТРАФІКОМ

Коцюк Назар Мирославович
здобувач вищої освіти
факультету комп'ютерно-інформаційних систем і програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Тимощук Віталій Дмитрович
здобувач вищої освіти
факультету прикладних інформаційних технологій та електроінженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Науковий керівник: Луцик Надія Степанівна
доктор філософії, доцент кафедри комп'ютерних систем та мереж
Тернопільський національний технічний університет імені Івана Пулюя, Україна

У сучасному світі, де рівень використання мережевих технологій у всіх сферах стрімко зростає, важливість надійних рішень для резервування та керування трафіком є актуальною темою. Мережі, які забезпечують неперервний доступ до ресурсів Інтернету, потребують надійних рішень для ефективного керування трафіком та забезпечення безперервності зв'язку.

Аналіз рішень провідних виробників, таких як Cisco, MikroTik, Palo Alto, Juniper та Fortinet, показує, що кожен з них пропонує дещо відмінні методики та технології для резервування та керування мережевим трафіком.

Технологія Cisco IP SLA вбудована у Cisco IOS і дозволяє проводити тести та моніторинг мережевих параметрів для вимірювання рівня обслуговування. Ця система забезпечує виявлення затримок, втрати пакетів та інших факторів, що впливають на якість мережі [1]. Крім того, вона може автоматично перенаправляти трафік на інший шлях у разі виявлення проблем у роботі мережі.

Операційна система RouterOS в MikroTik дозволяє використовувати скрипти та планувальники завдань для автоматизації завдань, моніторингу та управління мережею. Це надає можливість налаштування автоматичного переходу на резервний канал при нестабільній роботі основного [2].

В маршрутизаторах Juniper використовується технологія RPM для моніторингу та вимірювання параметрів мережевого зв'язку в реальному часі [3]. Це включає в себе використання проб для вимірювання затримок, втрат пакетів та інших критичних параметрів. Також RPM може автоматично перенаправляти трафік на альтернативні шляхи у разі виявлення проблем у мережі.

Мережеве обладнання Palo Alto Networks пропонує функціонал Path Monitoring для моніторингу шляхів та автоматичного переключення на резервний канал у випадку відмови або проблеми з доступністю основного каналу зв’язку [4]. Це включає в себе визначення порогових значень для вимірювання доступності та автоматичне виконання переключення трафіку.

Fortinet використовує Link Monitor для постійного моніторингу стану зв'язку між мережевими пристроями [5]. Ця система дозволяє визначати недоступні або нестабільні з'єднання та при необхідності автоматично виконувати дії для відновлення роботи мережі з можливістю переключення на резервні канали.

Усі ці системи мають вбудовану можливість сповіщення про переключення на резервний канал через електронну пошту. Однак лише MikroTik надає можливість використання вбудованих засобів для надсилання SMS про відсутність зв'язку взагалі, без застосування зовнішніх систем моніторингу [6]. Маршрутизатор MikroTik є привабливим варіантом для малих та середніх підприємств завдяки своїй гнучкості та простоті налаштувань, широкому спектру функцій та доступності.

Список використаних джерел:

1. IP SLA Fundamentals [Електронний ресурс]. — URL: https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKN0EAO/ip-sla-fundamentals (дата звернення: 27.11.2023).
2. RouterOS – Scripting [Електронний ресурс]. — URL: https://help.mikrotik.com/docs/display/ROS/Scripting (дата звернення: 27.11.2023).
3. Configuring Real-Time Performance Monitoring Probes [Електронний ресурс]. — URL: https://www.juniper.net/documentation/us/en/software/nce/internet-protocol-srx-monitoring/topics/task/ip-monitoring-rpm-configuring.html (дата звернення: 27.11.2023).
4. Failover [Електронний ресурс]. — URL: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/failover (дата звернення: 27.11.2023).
5. Link monitor [Електронний ресурс]. — URL: https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/76624/link-monitor (дата звернення: 27.11.2023).
6. RouterOS – SMS [Електронний ресурс]. — URL: https://help.mikrotik.com/docs/display/ROS/SMS (дата звернення: 27.11.2023).

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

XII Міжнародної науково-практичної конференції молодих учених та студентів

6-7 грудня 2023 року

УКРАЇНА
ТЕРНОПІЛЬ – 2023

Матеріали XII Міжнародної науково-практичної конференції молодих учених та студентів «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль, 6-7 грудня 2023 року

УДК 004.77

Н. М. Коцюк, В. Д. Тимощук; Ю. О. Момоток,
Н. С. Луцик доктор філософії, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СИСТЕМА РЕЗЕРВУВАННЯ ТРАФІКУ НА ОСНОВІ MIKROTIK

N. Kotsiuk, V. Tymoshchuk, Yu. Momotok, N. Lutsyk Ph.D, Assoc. Prof.

BACKUP TRAFFIC SYSTEM BASED ON MIKROTIK

У світі комп'ютерних технологій резервування та керування трафіком у мережах є критичним елементом для забезпечення неперервності роботи інтернет-послуг, додатків та комунікацій загалом. Це особливо важливо у сферах, де великі обсяги даних пересилаються через мережі, а будь-який збій може призвести до серйозних фінансових втрат.

Мережеві пристрої, зокрема маршрутизатори MikroTik, надають широкі можливості для управління трафіком з метою забезпечення надійності зв'язку. Ці можливості охоплюють підключення резервних каналів зв'язку та автоматизацію процесу переходу на альтернативні маршрути в разі погіршення якості або відмови основного каналу.

Ефективне управління трафіком дозволяє оптимізувати пропускну здатність, раціонально використовувати ресурси мережі та забезпечувати користувачам прийнятний рівень сервісу. Цей підхід має важливе значення для забезпечення зв'язку як для сегменту B2B, так і для сегменту B2C.

Дослідницька робота була націлена на створення та впровадження системи управління та резервування трафіком на основі маршрутизаторів MikroTik з метою забезпечення постійного доступу до мережі Інтернет у ситуаціях обмеженого чи втраченого зв'язку.

У дослідженні були ретельно вивчені мережеві можливості маршрутизатора MikroTik для тестування сценаріїв відновлення у випадках погіршення якості або втрати зв'язку. В рамках цієї роботи був розроблений програмний код, що автоматизує перехід з основного каналу на резервний у разі погіршення якості зв’язку або його втрати. Крім того, цей код передбачає можливість отримання повідомлень через електронну пошту при переході на резервний канал зв’язку, а також SMS-повідомлень у випадках відсутності зв’язку по усіх каналах.

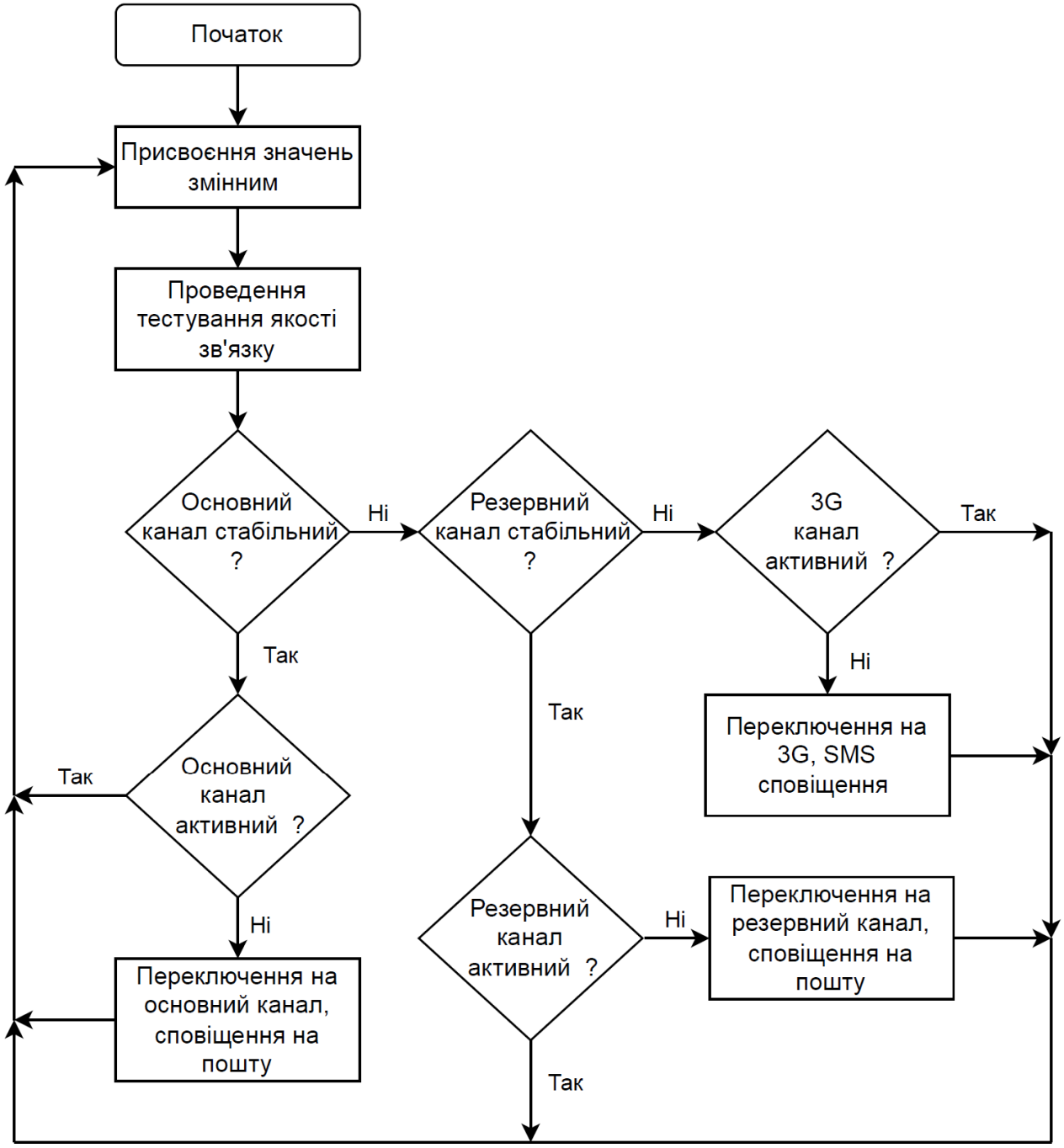
Після розробки системи було проведено комплексне тестування, що включало в себе моделювання ситуації аварійного переходу на резервний канал, інформування через електронну пошту про зміни у маршрутизації за замовчуванням, а також перевірку коректності роботи SMS-інформування в аварійних ситуаціях. Також проведена оцінка можливостей системи для виконання моніторингу інфраструктури.

Результати тестування підтвердили ефективність розробленої системи резервування та управління трафіком на базі маршрутизатора MikroTik в умовах обмеженого або втраченого зв'язку. Ця система є ефективним інструментом для забезпечення безперебійності та стабільності роботи мережі.

Література

1. RouterOS – Scripting [Електронний ресурс]. — URL: https://help.mikrotik.com/docs/display/ROS/Scripting (дата звернення: 27.11.2023).

Додаток Б Блок-схема алгоритму роботи



Додаток В Лістинг програмного коду

```
# Define variables
# First interface name
:local if1 "ether1";
# Second interface name
:local if2 "ether2";
#3G modem interface name
:local ifppp "ppp-out1";
# First gateway IP address
:local gw1 "192.168.10.1";
# Second gateway IP address
:local gw2 "192.168.20.1";
# First host to ping via gw1
:local gw1host1 "8.8.8.8";
# Second host to ping via gw1
:local gw1host2 "1.1.1.1";
# First host to ping via gw2
:local gw2host1 "8.8.4.4";
# Second host to ping via gw2
:local gw2host2 "1.1.1.2";
# Number of ping attempts
:local pingCount 10;
# Threshold for stable connection (%)
:local ThresholdGw1 90;
:local ThresholdGw2 95;
:local ThresholdGw1to3G 30;
:local ThresholdGw2to3G 30;
# Log marker for logging purposes
:local logmark "---> ";
# set distance
:local if1desiredDistance 3;
:local if2desiredDistance 4;
#
:log info ($logmark . "Start script");
#
# Check if interfaces are disabled, enable if needed
:if ([/interface ethernet get $if1 disabled] = true) do={
    /interface ethernet set $if1 disabled=no;
    :delay 5s;
} else={
    :put ("Interface $if1 is already enabled.");
    :log info ($logmark . "Interface $if1 is already enabled.");
}
#
:if ([/interface ethernet get $if2 disabled] = true) do={
    /interface ethernet set $if2 disabled=no;
    :delay 5s;
} else={
    :put ("Interface $if2 is already enabled.");
    :log info ($logmark . "Interface $if2 is already enabled.");
}
```

```
#
# Perform ping tests on gateway hosts
:log info ($logmark . "start ping gw1  IP $gw1host1 and $gw1host2");
#
:local pingStatus1 \
    ((( [/ping $gw1host1 interface=$if1 count=$pingCount] + \
    [/ping   $gw1host2   interface=$if1   count=$pingCount]   )   /
($pingCount * 2)) * 100);
:put ("pingStatus1 $pingStatus1");
:log info ($logmark . "PingStatus1:  $pingStatus1 %");
:log info ($logmark . "ping stop gw1");
#
:log info ($logmark . "start ping gw2  IP $gw2host1 and $gw2host2");
#
:local pingStatus2 \
    ((( [/ping $gw2host1 interface=$if2 count=$pingCount] + \
    [/ping   $gw2host2   interface=$if2   count=$pingCount]   )   /
($pingCount * 2)) * 100);
:put ("pingStatus2 $pingStatus2");
:log info ($logmark . "PingStatus2:  $pingStatus2 %");
:log info ($logmark . "ping stop gw2");
#
# Check and adjust route distances
:local  if1Distance  [/ip  route  get  [find  dst-address=0.0.0.0/0
gateway=$gw1] distance];
:local  if2Distance  [/ip  route  get  [find  dst-address=0.0.0.0/0
gateway=$gw2] distance];
#
:if ($if1Distance != $if1desiredDistance) do={
    /ip   route   set   [find   dst-address=0.0.0.0/0   gateway=$gw1]
distance=$if1desiredDistance;
    :log warning  ($logmark . "Distance for 0.0.0.0/0 via gateway
$gw1 set to \
     $if1desiredDistance");
} else={
    :log warning ($logmark . "Distance for 0.0.0.0/0 via gateway
$gw1 is already \
     $if1desiredDistance");
    }
#
:if ($if2Distance != 2 && $if2Distance != 4) do={
    /ip   route   set   [find   dst-address=0.0.0.0/0   gateway=$gw2]
distance=$if2desiredDistance;
    :log warning  ($logmark . "Distance for 0.0.0.0/0 via gateway
$gw2 set to \
     $if2desiredDistance");
} else={
    :log warning ($logmark . "Distance for 0.0.0.0/0 via gateway
$gw2 is OK");
    }
#
# Check internet connection stability and take action accordingly
:if ($pingStatus1 < $ThresholdGw1) do={
```

```
    :log error ($logmark . "main Internet channel problem");

    :if ($pingStatus2 > $ThresholdGw2) do={

         :if ($if2Distance  != 2) do={
          /interface/ppp-client/disable ppp-out1;
        /ip route set [find dst-address=0.0.0.0/0 gateway=$gw2]
distance=2;
        :log warning ($logmark . "Distance for 0.0.0.0/0 via gateway
$gw2 changed to 2");
          :delay 5s;
# Email notification
        /tool e-mail send server=mail.cs.networkacad.net port=25
to=alert.XXXX.YYYY@gmail.com \
          from=mikrotik@HH.LLLLLLLLL.net \
        subject="MikroTik: Alert $[/system clock get date],
$[/system clock get time]" \
        body="switching to a backup Internet channel\nDate:
$[/system clock get date]\nTime: \
         $[/system clock get time]\nPingStatus: $pingStatus1 %";
          :log warning ($logmark . "switching to a backup Internet
channel. mail sent");
        } else={
          :put ("backup Internet channel is already in use");
        :log info ($logmark . "backup Internet channel is already
in use");
                    }
        }
          else={
          :put ("Problem all channel");
        :log error ($logmark . "Problem all channel");
# SMS notification and GSM backup enable
          :if ($pingStatus1 < $ThresholdGw1to3G && $pingStatus2 <
$ThresholdGw2to3G) do={

          :if ([/interface ppp-client get $ifppp disabled] = true)
do={

     :put ("sms send");
          :log info ($logmark . "sms send");
          /tool sms send usb3 channel=0 "+380XXXXXXXXX"
message="RouteMT: \
          $[/system clock get date]: \
          $[/system clock get time]: Problem with all internet
channels. Switch to 3G.  ";
        /interface/ppp-client/enable ppp-out1;

         } else={
        :put ("3G Internet is already in use");
        :log info ($logmark . "3G Internet is already in use");
                }
                        }
                 }
```

```
} else={
    :log error ($logmark . "main Internet channel OK");

    :if ($if2Distance  != 4) do={
          /interface/ppp-client/disable ppp-out1;
        /ip route set [find dst-address=0.0.0.0/0 gateway=$gw2]
distance=4;
        :log warning ($logmark . "Distance for 0.0.0.0/0 via gateway
$gw2 changed to 4");
          :delay 5s;
# Email notification
        /tool e-mail send server= mail.cs.networkacad.net port=25
to=alert.XXXX.YYYY@gmail.com \
          from=mikrotik@HH.LLLLLLLLL.net \
        subject="MikroTik: Alert $[/system clock get date],
$[/system clock get time]" \
        body="switching to the main Internet channel\nDate:
$[/system clock get date]\nTime: \
          $[/system clock get time]\nPingStatus:  $pingStatus1 %";
          :log warning ($logmark . "switching to the main Internet
channel. mail sent");
        }
    }


:log info ($logmark . "Stop script");
```