УДК 004.7:004.72

О. П. Кліменко

РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ПІДВИЩЕННЯ СТІЙКОСТІ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ ЗА РАХУНОК ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SELF-HEALING NETWORK

Анотація. *У роботі розглянуто проблему забезпечення стійкості мереж передачі даних у разі відмов мережевого обладнання, пошкодження каналів зв'язку та перевантаження окремих ділянок мережі. Проаналізовано принципи побудови самовідновлюваних мереж (Self-Healing Network), що передбачають автоматичне виявлення несправностей, визначення доступних альтернативних маршрутів і відновлення передавання інформації з мінімальним втручанням адміністратора. Запропоновано комплекс технічних заходів на основі резервування каналів, динамічної маршрутизації OSPF, швидкого виявлення відмов за допомогою BFD, резервування шлюзів VRRP та моніторингу стану мережевих вузлів. Визначено показники для оцінювання ефективності запропонованих рішень: час відновлення зв'язку, втрати пакетів, доступність мережі та затримка передавання даних.*

Ключові слова: *Self-Healing Network, самовідновлювана мережа, стійкість мережі, відмовостійкість, OSPF, BFD, VRRP, резервування каналів.*

Abstract. *The paper examines the problem of maintaining the resilience of data transmission networks in the event of network equipment failures, communication link outages, and congestion. The principles of Self-Healing Networks are analyzed, including automatic fault detection, selection of available alternative routes, and restoration of data transmission with minimal administrator intervention. A set of technical measures is proposed based on link redundancy, OSPF dynamic routing, BFD fast failure detection, VRRP gateway redundancy, and network node monitoring. The effectiveness of the proposed solutions is to be evaluated using recovery time, packet loss, network availability, and data transmission latency.*

Keywords: *Self-Healing Network, network resilience, fault tolerance, OSPF, BFD, VRRP, link redundancy.*

Вступ

Сучасні інформаційно-телекомунікаційні системи залежать від безперервного обміну даними між робочими станціями, серверами, маршрутизаторами та іншими мережевими пристроями. Порушення працездатності навіть одного важливого вузла або каналу може призвести до втрати доступу до мережевих ресурсів, затримки передавання інформації та зниження ефективності роботи всієї системи. Особливо критичними такі наслідки є для систем управління, диспетчеризації та мереж спеціального призначення, у яких важливими вимогами є безперервність і передбачуваність обміну даними.

Одним із перспективних напрямів підвищення надійності є використання концепції Self-Healing Network - самовідновлюваної мережі. Її сутність полягає в тому, що мережа здатна автоматично виявляти порушення, визначати працездатні альтернативні шляхи та відновлювати передавання трафіку. При цьому Self-Healing Network не є окремим протоколом: це архітектурний підхід, який реалізується за допомогою сукупності механізмів резервування, маршрутизації, контролю стану та автоматизованого управління.

Мета роботи - розробити та обґрунтувати пропозиції щодо підвищення стійкості мереж передачі даних шляхом упровадження механізмів самовідновлення. Для досягнення мети необхідно проаналізувати типові причини відмов, визначити функціональні вимоги до самовідновлюваної мережі, обрати відповідні мережеві технології та запропонувати методику перевірки їх ефективності.

Аналіз проблеми та принципів побудови Self-Healing Network

Основними причинами порушення працездатності мереж передачі даних є фізичне пошкодження кабельних ліній, відмова портів і мережевих пристроїв, збої електроживлення, помилки конфігурації, перевантаження каналів та програмні несправності. У мережах із єдиним маршрутом між вузлами відмова будь-якого проміжного елемента може спричинити повну втрату зв'язку між сегментами. Тому першою умовою самовідновлення є усунення одиничних точок відмови шляхом створення альтернативних шляхів передавання.

Функціонування Self-Healing Network доцільно розглядати як послідовність взаємопов'язаних етапів: постійний контроль стану каналів і вузлів; виявлення ознак відмови; локалізація проблемної ділянки; вибір резервного маршруту; перенаправлення трафіку; перевірка відновлення зв'язку та реєстрація події. Чим швидше мережа виявляє несправність і запускає процедуру перемикання, тим меншими є перерва в обміні даними та кількість втрачених пакетів.

Важливо розрізняти резервування та самовідновлення. Наявність двох фізичних каналів сама по собі не гарантує автоматичного відновлення: мережеве обладнання має своєчасно визначити недоступність основного шляху й виконати перемикання на резервний. Так само динамічна маршрутизація без продуманої топології та контролю стану може забезпечувати відновлення із затримкою, неприйнятною для чутливих до часу сервісів.

Пропозиції щодо підвищення стійкості мережі

Для реалізації концепції Self-Healing Network пропонується побудувати мережу з надлишковою топологією, у якій ключові вузли з'єднані щонайменше двома незалежними шляхами. Резервні канали бажано прокладати різними фізичними трасами або організовувати через різні середовища передавання, щоб зменшити ймовірність одночасного пошкодження основного та резервного з'єднань. Для критичних вузлів доцільно передбачити резервне живлення та дублювання мережевих пристроїв.

Основним механізмом автоматичного вибору маршрутів пропонується використати протокол OSPF. Він дає змогу маршрутизаторам обмінюватися інформацією про топологію та самостійно перераховувати маршрути після зміни стану мережі. За наявності кількох доступних шляхів OSPF обирає маршрут відповідно до розрахованої вартості. Налаштування вартості інтерфейсів має враховувати пропускну спроможність і призначення каналів, а резервний шлях повинен залишатися працездатним та мати коректну IP-адресацію.

Для скорочення часу виявлення відмов пропонується застосувати протокол BFD (Bidirectional Forwarding Detection). Він забезпечує швидку перевірку доступності сусіднього мережевого вузла та може взаємодіяти з протоколом маршрутизації, ініціюючи швидше оновлення маршрутної інформації. Параметри інтервалів BFD необхідно підбирати з урахуванням характеристик обладнання та каналів, оскільки надто агресивні значення можуть спричинити хибне оголошення відмови в мережах із нестабільною затримкою.

Для підвищення доступності локального шлюзу доцільно використати VRRP. У такій схемі декілька маршрутизаторів утворюють групу резервування та спільно надають віртуальну IP-адресу шлюзу. У штатному режимі трафік обробляє активний маршрутизатор, а в разі його відмови роль шлюзу переходить до резервного пристрою. Це дозволяє зберегти для кінцевих вузлів незмінні параметри шлюзу за замовчуванням.

На канальному рівні Ethernet для запобігання петлям і забезпечення резервних з'єднань можуть застосовуватися RSTP або спеціалізовані механізми захисту кільцевих топологій, зокрема ERPS відповідно до рекомендації ITU-T G.8032. Вибір технології

залежить від типу комутаторів, структури мережі та вимог до часу перемикання. Одночасне застосування декількох механізмів резервування має бути узгоджене, щоб уникнути конфліктів і непередбачуваних змін топології.

Окремою складовою самовідновлення має стати централізований моніторинг. Система моніторингу повинна збирати відомості про стан інтерфейсів, завантаження каналів, затримку, втрати пакетів і доступність вузлів. За визначеними порогами вона може формувати повідомлення адміністратору або запускати заздалегідь перевірені сценарії автоматизації. Автоматичні зміни конфігурації необхідно супроводжувати журналюванням, контролем прав доступу та можливістю повернення до попереднього стану.

Оцінювання ефективності запропонованих рішень

Практичну перевірку запропонованої архітектури доцільно виконати в середовищі GNS3 або EVE-NG, а для базової демонстрації-у Cisco Packet Tracer. Модель повинна містити декілька маршрутизаторів, комутатори, кінцеві вузли, основні та резервні канали. На маршрутизаторах налаштовуються адресація, OSPF і, за підтримки обраного обладнання, BFD; для резервування шлюзу конфігурується VRRP.

Під час експерименту необхідно зафіксувати початкову працездатність мережі, виконати безперервну передачу тестових пакетів між віддаленими вузлами, після чого по черзі імітувати відмову основного каналу, маршрутизатора та шлюзу. Для кожного сценарію вимірюються час від моменту виникнення відмови до відновлення зв’язку, кількість втрачених пакетів, середня затримка та доступність мережевих сервісів. Отримані результати слід порівняти з базовою мережею без резервних маршрутів.

Для об’єктивного оцінювання експерименти потрібно повторювати за однакових умов і фіксувати конфігурацію обладнання, параметри протоколів та характеристики тестового трафіку. Це дасть змогу визначити, який саме механізм найбільше впливає на швидкість відновлення, а також виявити можливі побічні ефекти - короткочасні петлі, асиметричну маршрутизацію або надмірне навантаження на пристрої. Кількісні висновки щодо покращення показників слід формувати лише за результатами проведених вимірювань.

Висновки

У роботі розглянуто підхід до підвищення стійкості мереж передачі даних на основі концепції Self-Healing Network. Визначено, що самовідновлення забезпечується не одним окремим протоколом, а комплексом узгоджених засобів: фізичним і логічним резервуванням, автоматичним виявленням несправностей, динамічною маршрутизацією, резервуванням шлюзів та моніторингом стану мережі.

Як основні технічні пропозиції визначено використання OSPF для перебудови маршрутів, BFD для прискореного виявлення відмов, VRRP для збереження доступності шлюзу, а також RSTP або ERPS для резервування на канальному рівні. Запропоновано методику моделювання аварійних ситуацій у GNS3, EVE-NG або Cisco Packet Tracer та систему показників для порівняння роботи мережі до і після впровадження зазначених механізмів.

Практична цінність запропонованого підходу полягає у можливості зменшити тривалість перерв зв’язку та обсяг втрат даних у разі типових відмов мережевої інфраструктури. Остаточна оцінка ефективності має ґрунтуватися на експериментальних вимірюваннях для конкретної топології й обладнання. Подальші дослідження доцільно спрямувати на автоматизацію діагностики несправностей, аналіз стану каналів за телеметрією та впровадження політик відновлення з урахуванням пріоритетності трафіку.

Список використаних джерел:

1. Moy J. OSPF Version 2. RFC 2328. Internet Engineering Task Force, 1998. URL: https://www.rfc-editor.org/rfc/rfc2328.

2. Katz D., Ward D. Bidirectional Forwarding Detection (BFD). RFC 5880. Internet Engineering Task Force, 2010. URL: https://www.rfc-editor.org/rfc/rfc5880.

3. Nadas S. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. RFC 5798. Internet Engineering Task Force, 2010. URL: https://www.rfc-editor.org/rfc/rfc5798.

4. ITU-T. Recommendation G.8032/Y.1344: Ethernet ring protection switching. International Telecommunication Union. URL: https://www.itu.int/rec/T-REC-G.8032.

5. IEEE. IEEE Std 802.1Q: Bridges and Bridged Networks. Institute of Electrical and Electronics Engineers. URL: https://standards.ieee.org/standard/802_1Q-2022.html.

6. Cisco. OSPF Design Guide. Cisco Systems. URL: https://www.cisco.com/.

Кліменко Олександр Павлович *– курсант Харківського національного університету Повітряних Сил імені Івана Кожедуба, м. Харків, e-mail: sashaklimenko307@gmail.com*

Klimenko *Oleksandr Pavlovich – Cadet of Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, e-mail: sashaklimenko307@gmail.com*