УДК 004.7:004.056

ПОВЫШЕНИЕ ОТКАЗОУСТОЙЧИВОСТИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Скиб А.И., магистрант гр. 567001

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Лагутин А.Е. – канд. тех. наук, доцент

Аннотация. В статье рассматриваются основные способы повышения отказоустойчивости в компьютерных сетях. Описаны подходы, направленные на обеспечение непрерывности работы сетевой инфраструктуры при сбоях оборудования, каналов связи и программного обеспечения. Рассматриваются методы резервирования, кластеризации, балансировки нагрузки и динамической маршрутизации. Сделан вывод о необходимости комплексного подхода для обеспечения высокой доступности сети.

Ключевые слова: отказоустойчивость, сеть, резервирование, кластер, маршрутизация, балансировка нагрузки.

Введение

Современные компьютерные сети выступают фундаментом цифровой инфраструктуры любой организации [1–2]. От их стабильной работы зависит функционирование корпоративных информационных систем, облачных сервисов и критически важных бизнес-процессов. В условиях высоких требований к непрерывности предоставления услуг (SLA) даже кратковременные сетевые сбои приводят к существенным финансовым и репутационным потерям [3].

Современные корпоративные стандарты требуют обеспечения уровня доступности сети (High Availability) не ниже «четырех девяток» (99,99 %), что допускает простой не более 52,6 минут в год, а для критических систем 99,999 % (около 5 минут простоя в год) [4]. Одной из главных проблем при проектировании таких сетей является устранение «единых точек отказа» (Single Point of Failure, SPOF) узлов или каналов, выход из строя которых приводит к неработоспособности всей системы.

Цель данной статьи – систематизация и анализ методов повышения отказоустойчивости компьютерных сетей с оценкой их эффективности в современных инфраструктурах.

Методы

Исследование базируется на анализе научно-технической литературы, международных стандартов (RFC), а также рекомендаций ведущих производителей сетевого оборудования (Cisco Validated Design). В работе применен метод сравнительного анализа для оценки технических характеристик различных протоколов резервирования и архитектурных решений. Критериями оценки выступили время сходимости (восстановления связи), сложность внедрения и способность обеспечивать заданные метрики RTO (Recovery Time Objective).

Примечание. При подготовке текста использовался искусственный интеллект исключительно для улучшения стилистики и перевода аннотации на английский язык под строгим контролем автора.

Результаты анализа

Базовым подходом к устранению SPOF является аппаратное резервирование и мультихоминг (подключение к нескольким независимым провайдерам) [5]. Дублирование физических линков и узлов формирует основу для работы логических механизмов отказоустойчивости.

На сетевом уровне широкое применение находят протоколы резервирования первого шлюза (FHRP), в частности VRRP (Virtual Router Redundancy Protocol) [6].

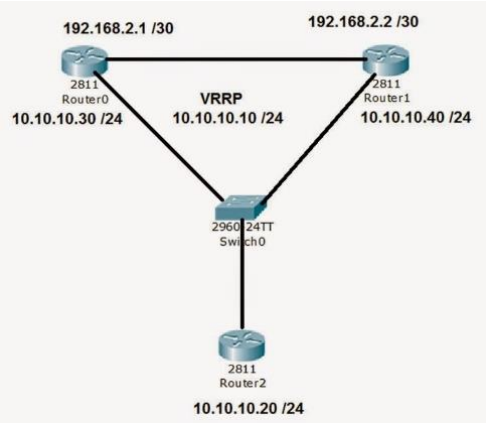

Рисунок 1 – Схема работы протокола VRRP

Архитектура VRRP (рис. 1) строится по принципу кластера «master-slave» (режим active/passive). Маршрутизаторы объединяются в логическую группу с общим виртуальным IP-адресом. Основной узел (Master) обрабатывает весь трафик, а резервный (Slave) находится в режиме ожидания, непрерывно получая служебные сообщения (heartbeat). При падении мастера резервный узел автоматически (обычно в течение 1–3 секунд) перехватывает виртуальный IP- и MAC-адрес, восстанавливая маршрутизацию незаметно для конечных узлов. Для серверов и межсетевых экранов применяется кластеризация.

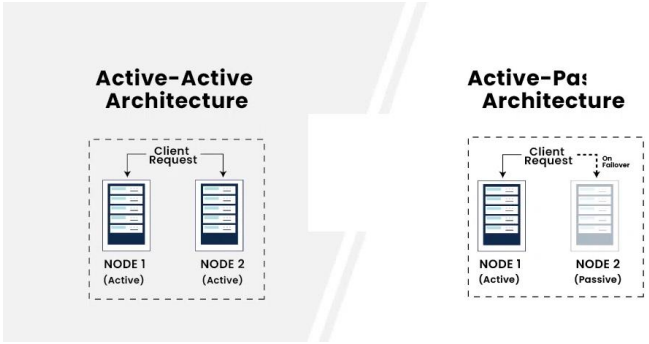

Рисунок 2 – Архитектура отказоустойчивых кластеров (Active-Passive и Active-Active)

В режиме Active-Passive логика аналогична VRRP, тогда как в режиме Active-Active (рис. 2) все узлы кластера одновременно обрабатывают трафик, что требует применения механизмов балансировки нагрузки (Load Balancing, например, HAProxy, Nginx или аппаратных ADC) [7]. Балансировщик распределяет запросы и автоматически исключает упавший узел из пула маршрутизации.

Особую роль играет динамическая маршрутизация (OSPF, BGP). В отличие от статических маршрутов, динамические протоколы способны автоматически перестраивать таблицу маршрутизации при падении линка [8–9]. Сходимость OSPF при правильной настройке таймеров может составлять менее секунды.

Для систематизации проанализированных подходов была составлена сравнительная таблица (Таблица 1).

Таблица 1 – Сравнительная характеристика методов повышения отказоустойчивости

Метод	Принцип действия	Преимущества	Недостатки	Среднее время восстановления
VRRP (Active/Passive)	Перехват виртуального IP резервным маршрутизатором при сбое основного	Простота настройки, прозрачность для хостов	Простаивание ресурсов резервного узла (Slave)	1–3 секунды
Кластер Active/Active	Распределение нагрузки между всеми узлами с автоматическим исключением сбойных	Максимальная утилизация ресурсов, высокая производительность	Сложность настройки синхронизации состояний (stateful)	Миллисекунды – секунды
Динамическая маршрутизация (OSPF)	Автоматический перерасчет метрик и путей при изменении топологии	Масштабируемость, учет состояния каналов на всей сети	Требует вычислительных ресурсов для работы алгоритма SPF	< 1 секунды (с BFD)
Мультихоминг + BGP	Подключение к разным ISP с анонсированием автономной системы	Защита от аварий на стороне провайдера	Высокая стоимость, сложная настройка политик маршрутизации	10–90 секунд

Анализ эффективности

Анализ показывает, что ни один из методов по отдельности не гарантирует доступность на уровне 99,99 %. Использование только динамической маршрутизации защищает сеть от обрыва оптики, но не спасет от падения шлюза по умолчанию на стороне локальных хостов (здесь необходим

VRRP). В свою очередь, VRRP не защитит от перегрузки сервиса (здесь нужен балансировщик и кластер Active/Active).

Современным трендом в повышении отказоустойчивости является внедрение программно-определяемых сетей (SDN) [10] и микросервисных архитектур (например, на базе Kubernetes) [11], где функции сетевого управления отделены от передачи данных. Это позволяет контроллеру SDN мгновенно перенаправлять потоки при обнаружении деградации каналов, снижая RTO практически до нуля.

Кроме того, при оценке эффективности выбранной стратегии необходимо учитывать не только скорость переключения (Failover Time), но и сохранение целостности сессий пользователей. В современных мультиоблачных и гибридных инфраструктурах классических методов резервирования становится недостаточно из-за задержек на трансграничных каналах связи. Внедрение интеллектуальных систем мониторинга, работающих в связке с протоколами BFD (Bidirectional Forwarding Detection), позволяет сократить время обнаружения обрыва линка до нескольких миллисекунд, что критически важно для передачи голоса (VoIP) и потокового видео. Также стоит отметить, что избыточность инфраструктуры неизбежно ведет к усложнению администрирования: увеличение числа активных узлов в кластере Active-Active повышает вероятность возникновения ошибок конфигурации. Таким образом, баланс между максимальной отказоустойчивостью и операционной простотой системы является основной задачей сетевого инженера при проектировании масштабируемых сетей.

Заключение

Таким образом, повышение отказоустойчивости компьютерных сетей требует комплексного подхода. Использование только одного метода не обеспечивает полной защиты от сбоев. Наиболее эффективным является сочетание резервирования, кластеризации, балансировки нагрузки и динамической маршрутизации.

Современные сети должны проектироваться с учетом возможных отказов и предусматривать механизмы автоматического восстановления. Это позволяет обеспечить непрерывность работы сервисов и повысить надежность всей информационной инфраструктуры.

Список литературы

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб.: Питер, 2012. 960 с.

2. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. 6-е изд. СПб.: Питер, 2020. 1008 с.

3. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th ed. Pearson, 2021. 864 p.

4. Cisco Systems. Enterprise Campus 3.0 Architecture: Overview and Framework. Cisco Validated Design (CVD), 2023. [Электронный ресурс]. URL: https://www.cisco.com (дата обращения: 26.03.2026).

5. Chen, M., et al. "BGP Multihoming and Fast Reroute Mechanisms for Enterprise Networks." IEEE Transactions on Network and Service Management, vol. 22, no. 2, 2025, pp. 210-225.

6. RFC 5798. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. Internet Engineering Task Force (IETF), 2010.

7. Smith, R., Jones, T. "Evaluating Load Balancing Algorithms in Active-Active High Availability Clusters." Springer Journal of Network and Systems Management, vol. 32, no. 4, 2024, pp. 55-78.

8. Дойл Дж., Кэрролл Д. Маршрутизация TCP/IP. Том 1. 2-е изд. М.: Вильямс, 2006. 800 с.

9. Иванов А. С., Петров В. В. Сравнительный анализ протоколов динамической маршрутизации при построении отказоустойчивых сетей // Вестник инфокоммуникационных технологий. 2025. Т. 12. № 2. С. 34-41.

10. Zhang, Y., et al. "High Availability in Software-Defined Networking: A Comprehensive Survey." IEEE Communications Surveys & Tutorials, vol. 25, no. 1, 2023, pp. 450-485.

11. Li, X., Wang, H. "Reliability Analysis of Kubernetes-based Microservice Architectures in Edge Computing." Elsevier Future Generation Computer Systems, vol. 142, 2024, pp. 112-125..

UDC 004.7:004.056

IMPROVING FAULT TOLERANCE IN COMPUTER NETWORKS

Skib A.I.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Lagutin A.E. – PhD in Technical Sciences, Associate Professor

Annotation. The article considers the main methods of improving fault tolerance in computer networks. The approaches aimed at ensuring continuous operation of network infrastructure in case of failures of equipment, communication channels and software are described. The methods of redundancy, clustering, load balancing and dynamic routing are analyzed. The result of the study is the conclusion that a comprehensive approach is required to achieve high availability and reliability of modern networks.

Keywords: fault tolerance, computer networks, redundancy, clustering, load balancing, routing