Г. Д. Мянник, А. А. Лазутин, М. С. Воробьева, А. А. Оленников
Тюменский государственный университет, г. Тюмень

УДК 004.457

ПРОГРАММНОЕ РЕШЕНИЕ ДЛЯ ДИАГНОСТИКИ ПРОБЛЕМНЫХ УЗЛОВ В ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

Аннотация. Рассматривается подход оперативного выявления неполадок в телекоммуникационной сети интернет-провайдера для обеспечения стабильности в работе путем мониторинга и анализа состояния управляемых коммутаторов. В случае выявления отклонений производится диагностика параметров проблемных телекоммуникационных узлов.

Ключевые слова: телекоммуникационная сеть, коммутатор, Zabbix, SNMP, мониторинг, анализ, ряды динамики, статистический анализ.

Введение. В настоящее время обеспечение доступа в интернет является неотъемлемой частью получения информации и взаимодействия. Вместе с растущим числом пользователей интернета, растет и масштаб телекоммуникационных сетей, предназначенных для обеспечения доступа в интернет. Такие системы требуют регулярный мониторинг и обслуживание, так как на стабильность работы может влиять множество случайных как внешних, так и внутренних факторов. Чем масштабнее становится телекоммуникационная сеть, тем сложнее проводить мониторинг, выявлять возникающие неполадки, поддерживать стабильность агрегатных узлов.

Данная тема является актуальной, что подтверждают исследования, проведенные специалистами в этой области. В частности, решения вопросов мониторинга и анализа состояния работы телекоммуникационной сети представлены авторами В.В. Аллакиным, Н.П. Будко, Н.В. Васильевым в работе [1], которые делают обзор программных решений для мониторинга сетевых систем, таких как Zabbix, Nagios и др, но главным недостатком таких решений является констатация факта наличия неполадки без выявления самой проблемы.

Авторы в статье [2] рассматривают диагностику сети при обнаружении неполадки, особое внимание уделяя сопоставлению характеристик маршрутов сети определенному набору условий. В случае

отклонения от эталона, производится диагностика проблемных участков (CRC и Reset на физических интерфейсах, скорость и пропускная способность MTU, наличие беспроводной сети РРЛ на трассе, загрузка ЦПУ и процессы на оборудовании на трассе). Такой подход направлен на обеспечение стабильной работы физических интерфейсов и трасс (маршрутов) телекоммуникационной сети, но данное решение направлено на мониторинг сетей телефонии, а не коммутаторов.

В сети могут возникать неполадки, решить которые можно различными способами. Для примера возьмем потребность в выявлении петель маршрутизации:1) J.Sommers и P. Barford предлагают анализ трассировки пакетов [3]; 2) Авторы статьи [4] рассматривают другое решение: разработка алгоритмов перемаршрутизации; 3) А. Мерсни предлагает модель маршрутизации, которая исключает появление петлей [5].

Одной из сторон мониторинга состояния сетей являются задачи прогнозирования их трафика, которые представили в работе [6] Митрохин В.Е., Рингенблюм П.Г., Башков И.Н.

Таким образом, одной из проблем для обеспечения стабильной работы телекоммуникационной сети является оперативная диагностика SNMP-ловушек и Zabbix-триггеров с целью выявления различных неполадок. Одним из решений данного вопроса служит исследование подхода для оперативного выявления нестабильности работы сети на основе анализа данных о состояниях коммутаторов и их связей.

Постановка задачи. Пусть есть телекоммуникационная сеть, в которой имеется N коммутаторов, связанных между собой определенным образом. Исходное работоспособное состояние сети W зависит от активных управляемых коммутаторов и связей. Каждое устройство сети имеет перечень параметров (состояние, загрузка центрального процессора, загруженности ОЗУ, температура внутренней среды коммутатора, набор интерфейсов и др.) и допустимый диапазон рабочих значений.

Для проведения исследования были введены три понятия: отклонение, первичное событие и сетевая неполадка. Первичным событием

будем называть выход за диапазон нормы значений параметров устройств. Отклонением называется набор первичных событий, удовлетворяющих некоторому условию. Сетевой неполадкой будем считать такое состояние участка сети, имеющее некоторое отклонение и алгоритм ее диагностики.

Необходимо выявить неполадки и провести диагностику проблемных узлов.

Сетевые неполадки. В ходе опытной эксплуатации сети и обсуждения с экспертами вопросов о возникающих в сети неисправностях были выявлены следующие группы неполадок (одиночные и множественные, внутренние и внешние), определены неполадки и предложены алгоритмы диагностики.

Рассмотрим внешнюю множественную сетевую неполадку № 1: «Повреждение кабеля или проблема с затуханием его оптического сигнала», для которой определено отклонение: «Существуют два первичных события о падении линка, при этом коммутаторы проблемного линка активны». Алгоритм диагностики заключается в следующем:

1) производится сбор значений параметра «Статус интерфейса» с периодом в 5 минут в течение 3 дней;

2) на собранных данных рассчитывается количество изменений значения параметра «Статус интерфейса»;

3) если значение параметра не меньше P1, то считается, что в сети имеется данная проблема, где P1 — минимальное количество изменений относительно данных состояний интерфейсов, имеющих данное отклонение за определенный период.

Рассмотрим внутреннюю одиночную сетевую неполадку №2: «Утечка оперативной памяти коммутатора», для которой определено отклонение: «Существует коммутатор, значение параметра “Использовано ОЗУ” которого не меньше 50%». Для данной неполадки алгоритм диагностики включает следующие этапы:

1) сбор значений параметра «Использовано ОЗУ» с периодом в 15 минут в течение 24 часов;

2) выборка собранных значений проверяется на условие: если все базисные показатели рядов динамики данной переменной поло-

жительны и все цепные показатели рядов динамики данной переменной не отрицательны, то считается, что в сети имеется данная проблема.

Рассмотрим внешнюю одиночную (или внешнюю множественную) сетевую неполадку №3: «Проблемы с климатом помещения» для которой определено отклонение: существует параметр «Температура» коммутатора (или нескольких коммутаторов с одинаковым географическим положением), для которого значение не меньше 45 °C. Алгоритм диагностики заключается в следующем:

1) производится сбор значений параметра «Температура» с проблемных коммутаторов с периодом в 15 минут в течение 12 часов;

2) производится проверка на соответствие условию: если последнее полученное значение переменной больше P2, то диагностика прерывается и считается, что в сети имеется данная проблема (где P2 — предпороговое значение критических значений температуры коммутаторов согласно условиям эксплуатации);

3) в ином случае, после проведения сбора выборка подвергается проверке условию: если все базисные изменения параметра “Температура” положительны, а цепные абсолютные изменения неотрицательны, то считается, что в сети имеется данная проблема.

Функциональные элементы архитектуры. Архитектура приложения для работы с ядром конкретной телекоммуникационной сети включает несколько частей (ядро сети, сетевой мониторинг, модули, диагностика неполадок) (см. рис. 1).

Модуль синхронизации получает актуальную информацию об адресах, моделях, географическом положении и связях коммутаторов из выходных файлов дампа телекоммуникационной сети, используя для этого как статичные парсеры, так и регулярные выражения. Полученная информация сопоставляется с данными хостов Zabbix-сервера и затем производится процесс актуализации IP адресов, списка активных управляемых коммутаторов, а также отслеживаемых первичных событий с использованием Zabbix API.

Zabbix занимается мониторингом состояния коммутаторов по SNMP и генерацией списка первичных событий, проверка которого на набор условий какой-либо неполадки периодически производится модулем анализа. В случае соответствия списка первичных

событий некоторому набору условий производится запуск скрипта, реализующего алгоритм диагностики сетевой неполадки.

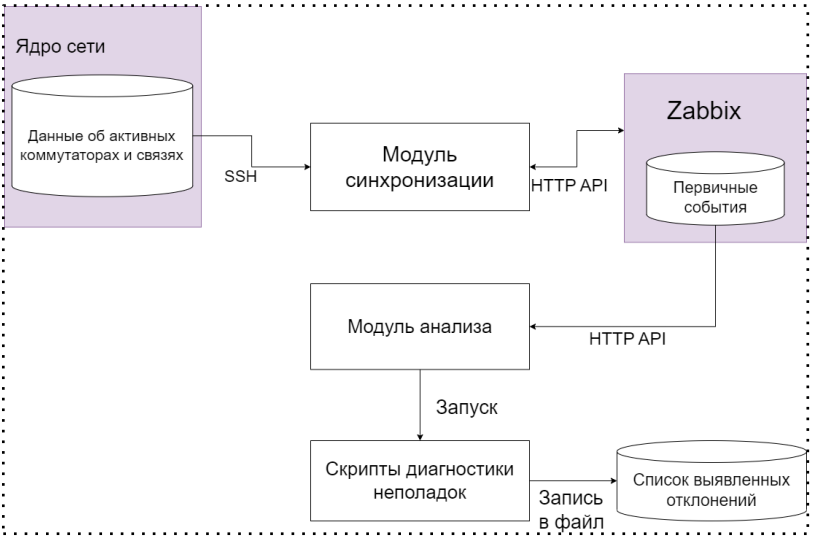

Рис. 1. Архитектура приложения

Выявленные неисправности записываются в файл json формата, который считывается web-сервером после получения HTTP-запроса (рис. 2). Пользователю выдается таблица, состоящая из трех столбцов: «Время», «Выявленные сетевые неполадки», «Номера проблемных коммутаторов».

Не защищено | switchmanager.deozal/

Время	Выявленные сетевые неполадки	Набор проблемных узлов
2023-05-28 15:42:41	Повреждение кабеля или проблема с затуханием его оптического сигнала	1901, 3041
2023-04-26 7:42:41	Повреждение кабеля или проблема с затуханием его оптического сигнала	1508, 2706

Рис. 2. Вывод выявленных сетевых неполадок

Результаты. Апробация программного решения была осуществлена на телекоммуникационной сети интернет-провайдера, имеющей 584 активных коммутатора с 538 связями. В табл. 1 представлены выявленные сетевые неполадки за май 2023 года.

Таблица 1

Выявленные сетевые неполадки

Дата и время	*Тип неполадки*	*Подтверждено диагностикой*
2023-05-07 7:42:41	Повреждение кабеля или проблема с затуханием его оптического сигнала	Да
2023-05-11 12:20:33	Проблемы с климатом помещения	Нет
2023-05-26 7:31:20	Повреждение кабеля или проблема с затуханием его оптического сигнала	Нет
2023-05-28 15:42:41	Повреждение кабеля или проблема с затуханием его оптического сигнала	Да

Заключение. Предложенный подход позволил специалистам обеспечить оперативное выявление проблем. В перспективе планируется сформировать расширенный реестр новых сетевых неполадок, а также провести исследование подхода прогнозирования сетевых неисправностей и выявления превентивных мероприятий противодействия их возникновению.

СПИСОК ЛИТЕРАТУРЫ

1. Общий подход к построению перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей / В. В. Аллакин, Н. П. Будко, Н. В. Васильев. — Текст: электронный // Системы управления, связи и безопасности. — 2021. — № 4. — С. 125-227. — URL: https://elibrary.ru/download/elibrary_46616109_42527444.pdf (Дата обращения: 30.04.2023)
2. Разработка мониторинга качества в телекоммуникационной сети с использованием машинного обучения / А.Р. Жунусов, А.С. Байкенов,

Т.Ж. Желтаев, Т.А. Зиекенов. — Текст : непосредственный // Энергетика, инфокоммуникационные технологии и высшее образование: Междунар. науч.-техн. конф. 20-21 окт. 2022 г. — Казань, 2023. Т. 1. — С. 445-456.
3. Detection and analysis of routing loops in packet traces / U. Hengartner, S. Moon, R. Mortier, C. Diot — URL: https://dl.acm.org/doi/abs/10.1145/637201.637217 (дата обращения: 01.05.2023). — Текст: электронный.
4. A Novel Loop-Free IP Fast Reroute Algorithm / G. Enyedi, G. Rétvári, T. Cinkler — URL: https://link.springer.com/chapter/10.1007/978-3-540-73530-4_14 (дата обращения: 01.05.2023). — Текст: электронный.
5. Модель маршрутизации многоадресных потоков с поддержкой общего явного резервирования канального ресурса / А. Мерсни. — Текст : электронный // Телекоммуникационные и информационные технологии. — 2017. — № 1(54). — С. 117-124. — URL: https://elibrary.ru/download/elibrary_35691214_94079415.pdf (Дата обращения: 02.05.2023)
6. Анализ методов прогнозирования трафика в телекоммуникационных сетях / В.Е. Митрохин, П.Г. Рингенблюм, И.Н. Башков. — Текст : непосредственный // Надежность функционирования и информационная безопасность инфокоммуникационных, телекоммуникационных и радиотехнических сетей и систем: Всерос. науч.-техн. конф. 25 окт. 2019 г. — Омск, 2019. — С. 38-45.