Программное обеспечение «Система мониторинга транспортных сетей передачи данных "Topolograph"»

Руководство пользователя

Оглавление

Глоссарий терминов 3
1. Введение и назначение системы 4
1.1. Назначение Topolograph 4
1.2. Решаемые задачи 4
2. Архитектура и компоненты 5
2.1. Логическая архитектура и подсистемы 5
2.2. Основные принципы работы 7
3. Сценарии использования 7
3.1. Примеры использования 7
3.2. Использование AI 8
4. Практическая эксплуатация 9
4.1. Модель представления данных 9
4.2. Обзор WEB-интерфейса 10
4.3. Слой IGP 11
4.4. Слой Netflow 12
5. Интеграции и обмен данными 12
6. Кооперация в развитии Topolograph 12

Глоссарий терминов

Топология сети
Схема взаимного расположения узлов сети (сетевого оборудования) и способов их соединения линиями связи. В контексте Topolograph топология сети представлена графом, узлами которого являются маршрутизаторы, а связями — сетевые линки.

Связь (Link)
Соединение между двумя узлами, позволяющее передавать данные. В графе связи представлены рёбрами.

Узел (Node)
Элемент графа топологии сети, обычно сетевое оборудование (маршрутизатор).

IGP (Interior Gateway Protocol)
Обобщённое название протоколов маршрутизации, основанных на парадигме мониторинга состояния каналов. К семейству IGP относятся протоколы OSPF и IS-IS. Альтернативная парадигма — дистанционно-векторная маршрутизация, к которой относятся протоколы семейства EGP (Exterior Gateway Protocol).

IS-IS (Intermediate System to Intermediate System)
Протокол динамической маршрутизации, основанный на парадигме состояния канала, который позволяет строить карты сети и оптимизировать маршрутизацию. Широко используется в крупных сетях провайдеров.

OSPF (Open Shortest Path First)
Протокол динамической маршрутизации, использующий алгоритм вычисления кратчайшего пути (Dijkstra) для определения наилучшего маршрута передачи данных. Разделяет сеть на области, упрощая управление крупными сетями.

AS (Autonomous System)
Набор IP-сетей и маршрутизаторов, контролируемых одной организацией или административной единицей и действующих под одним номером автономной системы. Является сущностью протокола BGP, который управляет маршрутизацией между AS.

BGP (Border Gateway Protocol)
Протокол динамической маршрутизации, использующий дистанционно-векторную парадигму для выбора маршрута.

Элементы графа
В терминах Topolograph это узлы и связи. Элементы имеют атрибуты, которые бывают обязательными и опциональными.

Атрибуты элементов графа
Пары key-value в строковом представлении, определяющие свойства (характеристики) узлов и связей. Примеры атрибутов — имя узла и метрика cost связи.

Моментальный граф
Графовое представление топологии сети, построенное для конкретного момента времени. Фактически граф отражает состояние топологии сети на указанный момент времени.

Дифференциальный граф
Графовое представление топологии сети, отражающее изменения в топологии за некоторый промежуток времени. Представляет собой комбинацию моментального графа на момент начала интервала времени и всех изменений до окончания интервала.
Метрика (cost)
Сущность протоколов IGP, числовой показатель линка, используемый для расчёта кратчайшего маршрута по алгоритму Dijkstra.
События
Информация об изменениях в топологии сети или в других наблюдаемых сущностях. Представлены набором пар key:value и доступны для просмотра в WEB-интерфейсе.

1. Введение и назначение системы

Транспортные сети провайдерского уровня являются сложными распределёнными системами, которые автоматически управляют маршрутизацией нагрузки в них. Информационная система Topolograph предназначена для мониторинга маршрутизации в таких сетях.

1.1. Назначение Topolograph

Комплекс предназначен для непрерывного мониторинга сетевой топологии транспортных сетей операторов связи, хранения данных о состоянии сети в исторической глубине и анализа её динамики.
Topolograph получает данные из сообщений протоколов IGP: он «видит» сеть так же, как любой маршрутизатор в её составе, воспроизводит и анализирует LSDB (Link State Database). По результатам анализа комплекс строит граф состояния сети на любой момент времени, определяет изменения в топологии сети за заданный промежуток времени и позволяет анализировать динамику сетевой топологии.

1.2. Решаемые задачи

Данные, собираемые комплексом, позволяют решать ряд повседневных задач, связанных с эксплуатацией сетевой инфраструктуры:

- инвентаризация сущностей сети: маршрутизаторов, линков, подсетей, пространства метрик, идентификаторов устройств (RID), адресов интерфейсов и пр.;
- оценка степени конвергентности сети: flapping, flood, связность, доступность;
- оценка уровня резервирования сетевых путей, степени рисков и потерь в случае аварий;
- оценка степени достижения расчётного эффекта от изменения конфигураций оборудования;

- контроль фактического адресного плана, поля метрик и пространства имён идентификаторов;
- контроль маршрутов по умолчанию;
- диагностика аварий и аномалий.

2. Архитектура и компоненты

2.1. Логическая архитектура и подсистемы

На рисунке 1 представлена логическая архитектура комплекса Topolograph, в которой можно выделить следующие подсистемы:

- Подсистема сбора данных схематически представлена на рисунке 2. Она реализована устройствами, которые включаются в контролируемую сеть как обычные маршрутизаторы с установлением IGP-соседства. Пример такого устройства представлен на рисунке 3. Устройства получают данные из протоколов маршрутизации и передают их на сервер. Устройства настраиваются на основании технических условий подключения, которые вырабатываются совместно представителями разработчика и провайдера в ходе подготовки к развёртыванию Topolograph. Пользователь не имеет доступа к устройствам подсистемы сбора.
- Серверная часть получает данные от устройств подсистемы сбора и сохраняет их в СУБД ClickHouse. Она разработана в архитектуре микросервисов и управляется Docker. Браузер пользователя обращается к серверной части для получения контента. Серверная часть реализует модель хранения данных, обеспечивающую различные способы представления сети — так называемые слои. Модель послойного представления сетевых данных описана в последующих разделах.
- Аналитическая подсистема представлена AI-агентом совместно с локальной LLM. Она доступна пользователю через чат с ИИ-ботом, который отвечает на вопросы о состоянии сети на естественном языке.

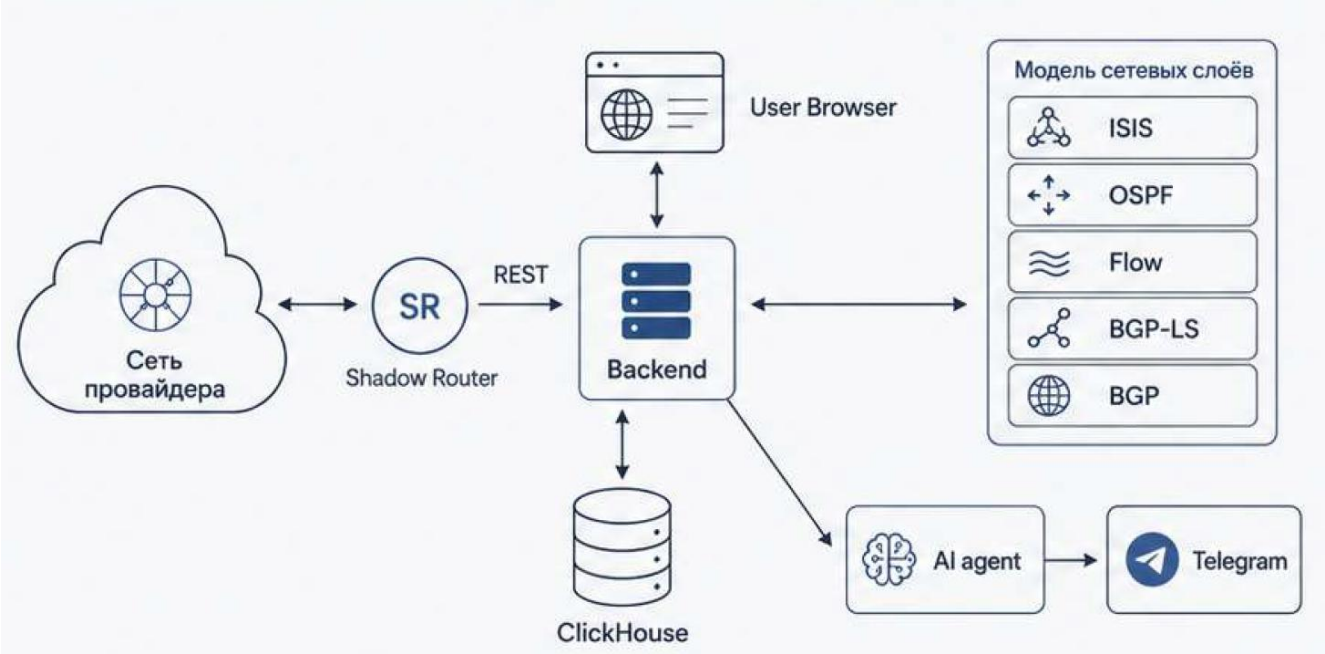

Рисунок 1. Логическая архитектура Topolograph

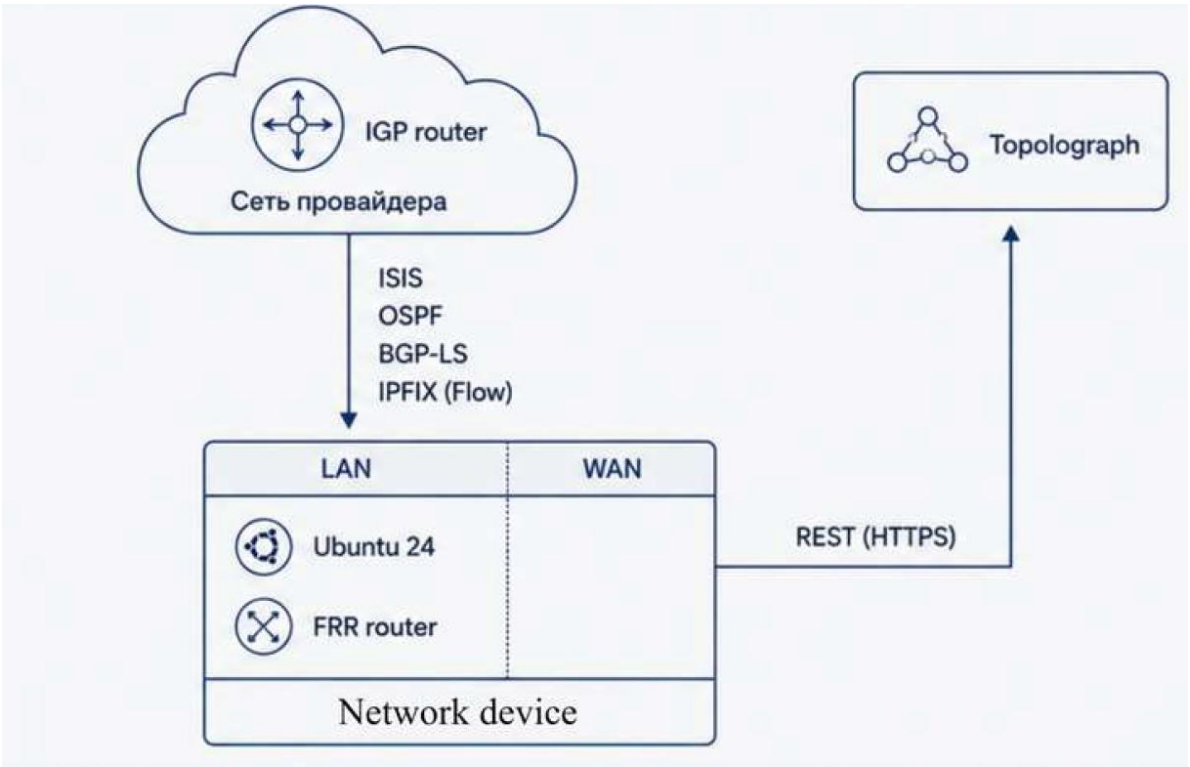

Рисунок 2. Подсистема сбора данных Рисунок 2. Подсистема сбора данных

Рисунок 3. Пример устройства для работы в подсистеме сбора данных NanoPi R2S

2.2. Основные принципы работы

Принципиальная особенность работы Topolograph — представление данных в виде графа. Эта математическая конструкция с узлами и связями позволяет очень информативно передать состояние сети, обеспечивая лёгкое восприятие и понимание её функционирования.
Графом можно представить не только топологию сети, но и целый ряд иных сущностей: классификацию Netflow-трафика по глобальному адресному пространству, статические маршруты и VPN L2/L3-конструкции, динамику в виде дифференциального графа. Также граф можно размещать разными способами на плоскости, в том числе на географической.
Все важные данные и свойства наблюдаемых сущностей закрепляются за элементами графа в виде атрибутов — пар key:value, доступных для поиска и навигации.
Для удобства поиска и навигации предусмотрено также классическое табличное представление элементов графа — оно описано далее, в разделе о пользовательском интерфейсе.

3. Сценарии использования

Визуализация сетевой топологии в виде графа позволяет решать множество прикладных задач, примеры которых представлены в этом разделе.

3.1. Примеры использования

- Авария широковещательного домена. 15 маршрутизаторов в полносвязной топологии, связность через broadcast-домен из 3 коммутаторов. Grafana показала аномально высокую нагрузку на одном из интерфейсов. На графе

Topolograph видна одновременная потеря нескольких IGP-соседств при сохранении остальных интерфейсов в состоянии UP. Дифференциальный граф показал сбойные узлы. Выявлен отказ блока питания одного из коммутаторов. Сеть продолжала работать, но риск перегрузки вырос — аварию локализовали вовремя.

- Флаппинг маршрута. После ночного окна изменений IGP оставался конвергентным, связность не нарушалась. Zabbix и Grafana отклонений не выявили. Topolograph зафиксировал аномально большое число событий по одной пользовательской подсети; фильтр по источнику выявил флаппинг маршрута. Причиной оказалась некорректная настройка, ухудшавшая доступ к подсети и заметная только по истории событий.
- Управление маршрутами по умолчанию. Default route меняется при плановых работах, резервировании или аварийном переключении, из-за чего возникают нерасчётные эффекты: смена точки выхода, асимметрия, перегрузка каналов. Topolograph фиксирует появление или исчезновение маршрута 0.0.0.0/0, источник изменения и затронутые узлы. Это позволяет проверять изменения маршрутов по умолчанию по истории топологии, а не по догадкам.

3.2. Использование AI

Локальная модель LLM в составе комплекса Topolograph способна анализировать состояние сети и её изменения, выполнять подсчёты и поиск, значительно ускоряя анализ причин сбойных ситуаций. Примеры чата и наиболее частых вопросов представлены на рисунке 4.

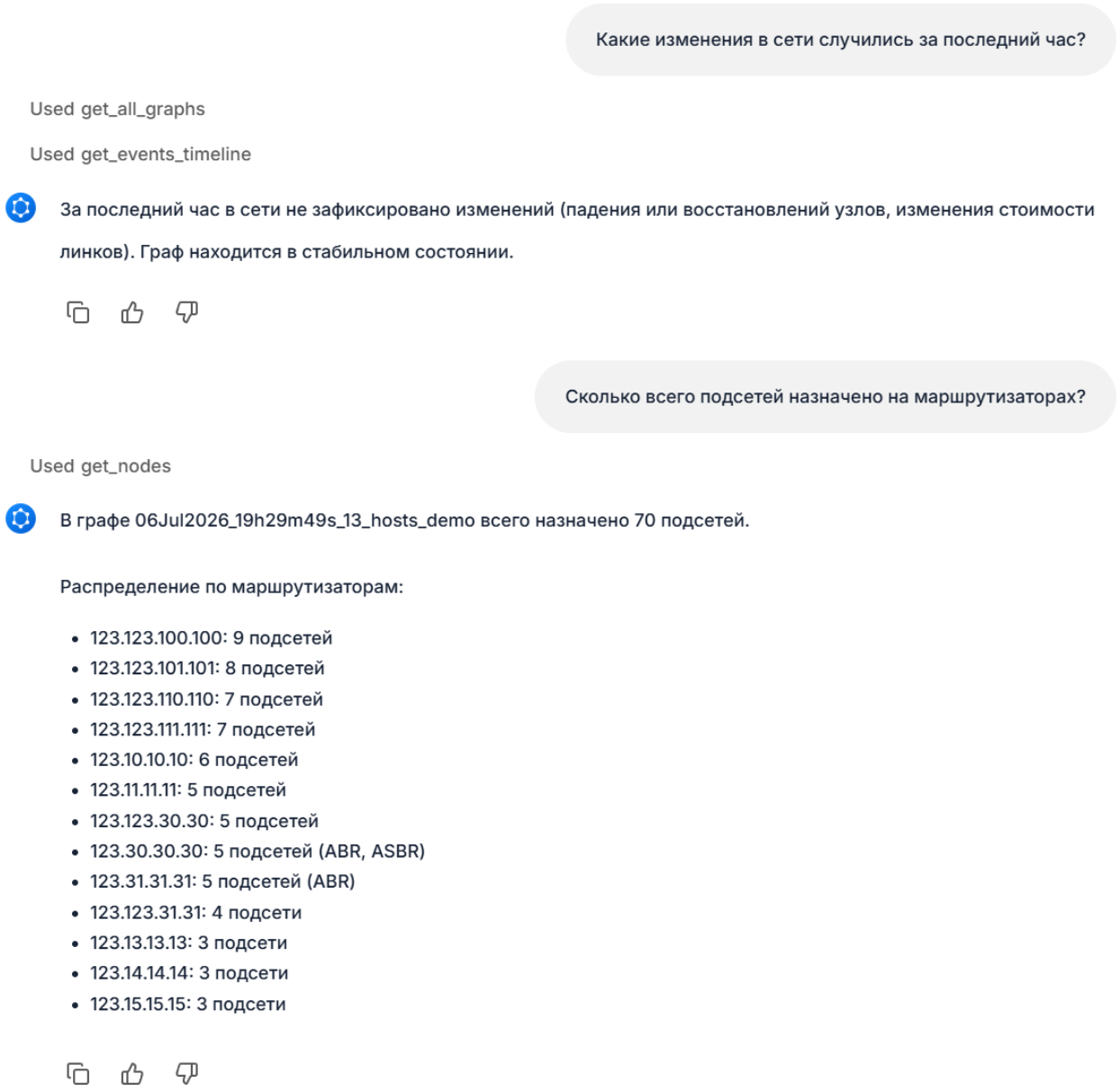

Рисунок 4. Использование AI-инструмента для анализа

4. Практическая эксплуатация

4.1. Модель представления данных

Удобно представлять контент как абстрактные графовые данные любой природы, без привязки к конкретному объекту. Эти данные подчиняются единым правилам визуализации.

Графовые данные изначально генерируются из потока событий, содержащих сведения о появлении и удалении элементов графа и изменении их атрибутов. Для построения моментального графа из СУБД поднимаются все события за всю историю хранения для запрошенного источника в подсистеме сбора. Результатом такой генерации становится сам моментальный граф и всё множество

формирующих его событий. Это целостный (консистентный) контент, который сохраняется в кэше на серверной стороне и доступен с высокой скоростью повторной выдачи — как полностью, так и частями (страницами событий). Дифференциальный граф генерируется в два этапа. Сначала поднимается моментальный граф на момент начала запрошенного интервала, а затем собираются все события изменений за этот интервал, в соответствии с которыми на графе отмечаются элементы с релевантными изменениями (включение, выключение, изменение атрибутов). На серверной стороне в кэш помещается консистентный дифференциальный граф с событиями запрошенного интервала времени. Весь контент в кэше хранится около 3 часов и в течение этого периода доступен с высокой скоростью выгрузки.
Модель моментального и дифференциального графов применяется ко всем источникам и данным любой природы. Это позволяет представить разные аспекты сетевых данных в виде слоёв, например:

- слои отдельных OSPF-area;
- слои Netflow каждого коллектора или интерфейса;
- слои VPN L2/L3-конструкций;
- слой междоменной связности BGP и др.

Единообразное представление слоёв позволяет выполнять их слияние и отображать, например, на одном графе несколько IGP-доменов.

4.2. Обзор WEB-интерфейса

Для пользователя данные доступны через WEB-интерфейс, представленный на рисунке 5. Окно браузера разделено на три части:

- область отображения контента в виде графа, где представлен интерактивный граф IGP-домена;
- область отображения контента в виде таблицы с возможностью поиска, сортировки и перехода на граф;
- область отображения сетевых событий с временной гистограммой и группировкой по источникам.

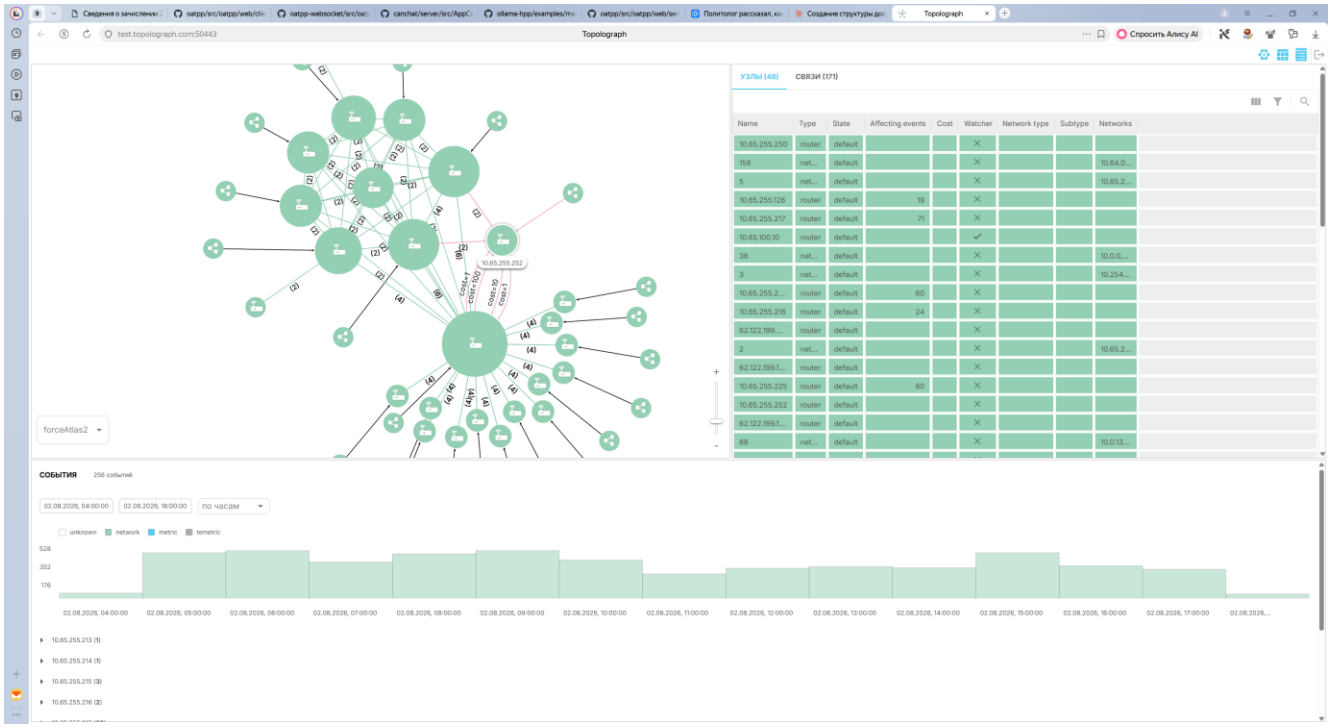

Рисунок 5. Скриншот WEB-интерфейса

При первом подключении на интерфейс выводится моментальный граф сети по состоянию на момент времени последнего события в СУБД. Если подсистема сбора активна, отображается граф на текущий момент времени.
Дифференциальный граф доступен по клику на временной интервал на гистограмме, шаг которой может быть выбран часовым или минутным.
События на моментальном графе составляют полное множество от момента установления соседства до момента построения графа. События разбиты на страницы и сгруппированы по источникам.
События на дифференциальном графе представлены только для интервала времени этого графа и также разбиты на страницы и сгруппированы по источникам.
В целом WEB-интерфейс интуитивно понятен и позволяет быстро разобраться в происходящих в сети процессах.

4.3. Слой IGP

Для пользователя слой IGP представлен топологией домена маршрутизации вне зависимости от протокола, по которому получены данные в подсистеме сбора (IS-IS, OSPF, BGP-LS). Этот слой полностью отражает состояние и динамику домена так, как его видят маршрутизаторы сети. Узлами графа являются маршрутизаторы, рёбра представляют сетевые линки с атрибутом cost.
Кроме маршрутизаторов граф содержит искусственные узлы, в которые объединены подсети. Такие узлы имеют собственную иконку на графе, вместо имени содержат счётчик всех входящих в них подсетей и связаны логической связью с тем узлом-маршрутизатором, на котором эти подсети настроены. Все

подсети перечислены в атрибутах такого узла и доступны для поиска в табличном представлении.
Дифференциальный граф выделяет в отдельные узлы подсети, которые включались или выключались за запрошенный период.

4.4. Слой Netflow

Слой Netflow может быть представлен графом двумя способами: как дополнение к IGP-слою с атрибутами загруженности линков и как граф классификации адресного пространства назначения трафика. В текущем релизе реализован только второй вариант.
Узлами графа являются IP-адреса источника и назначения каждой сессии Flow, а также искусственные узлы классификации IP-адреса назначения (страны, отраслевая классификация, провайдеры). На таком графе хорошо видно, куда именно передавался трафик от конкретного пользователя (интерфейса) в небольшой сети или даже с единственного интерфейса. Для такого представления моментальный граф не имеет смысла — при запросе возвращается граф за последние 12 часов от текущего момента.

5. Интеграции и обмен данными

Микросервисы Topolograph взаимодействуют по REST API и могут быть интегрированы в информационные системы заказчика. Документация по этим интерфейсам предоставляется по отдельному запросу.

6. Кооперация в развитии Topolograph

Команда разработчиков высоко ценит вовлечённость пользователей в развитие Topolograph. Предложения и замечания по функциональности комплекса приветствуются.