П. А. Давыдов, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.732, 004.722

ОРГАНИЗАЦИЯ БЕЗОПАСНОГО МОНИТОРИНГА КОМПЬЮТЕРНОЙ СЕТИ И АВТОМАТИЧЕСКОЕ ПОСТРОЕНИЕ ЕЕ ТОПОЛОГИИ

Аннотация. В работе проанализированы различные протоколы, предназначенные для взаимодействия с сетевыми устройствами. Рассмотрены варианты систем для автоматического мониторинга сетевых устройств. Результатом работы стала безопасная реализация системы мониторинга компьютерной сети на предприятии и разработка скрипта для построения и визуализации топологии.
Ключевые слова: автоматизация, мониторинг, SNMP, топология сети.

Введение. Сегодня компьютерные сети являются неотъемлемой частью бизнес-процессов в большинстве организаций. От надежности и безопасности сетевых устройств зависит эффективность работы компании и защита ее конфиденциальных данных. Именно поэтому мониторинг сетевых устройств является критически важным элементом в современном бизнесе [1]. Одной из основных проблем, связанных с организацией безопасного мониторинга, является сложность и масштабность самой сети. Современные компьютерные сети могут включать в себя сотни и даже тысячи устройств, каждое из которых может быть настроено индивидуально и иметь уникальную конфигурацию. Это делает процесс мониторинга крайне сложным и требует использования специальных инструментов и технологий [2; 3]. Кроме того, важным аспектом является безопасность мониторинга, так как в процессе сбора информации могут существовать уязвимости, которые могут быть использованы злоумышленниками для атаки на сеть [4]. Все эти факторы требуют тщательного планирования и реализации мер безопасности и контроля, чтобы обеспечить эффективный мониторинг и защиту компьютерной сети [5].

Проблема исследования. Обеспечение безопасного мониторинга сетевых устройств является комплексным и сложным процессов, поэтому были выделены следующие задачи:

1) рассмотреть протоколы взаимодействия с сетевыми устройствами;

2) сравнить и выбрать систему мониторинга;

3) изучить методы формирования и визуализации топологии сети;

4) установить систему мониторинга и реализовать визуализацию топологии устройств.

Материалы и методы. Методами данного исследования стали: сравнение, изучение, эксперимент. Опыты проводились с использованием сетевых устройств, функционирующих в действующей сети предприятия.

Результаты. Существует большое количество программных интерфейсов для связи с сетевыми устройствами. Главное требование к нему — универсальность в гетерогенных сетях. Интерфейс командной строки не соответствует этому критерию, так как у устройств разных производителей синтаксис может отличаться не только в зависимости от вендора, но и от разной версии операционной системы.

Netconf является на данный момент наиболее перспективным интерфейсом: у него есть множество стандартизированных модулей от сторонних производителей, однако не все существующие устройства его поддерживают.

Наиболее подходящим интерфейсом является SNMP, который является одним из фундаментальных протоколов и поддерживается практически всеми сетевыми устройствами. На сегодняшний день актуальными являются две версии: SNMPv2c и SNMPv3. Главное отличие — подход к безопасности. Во второй версии протокола безопасность реализована по подходу «все или ничего» — нельзя настроить список параметров, с которыми может взаимодействовать пользователь, а аутентификация производится с помощью строки *community*, которая хранится в виде открытого текста и не шифруется. В третьей версии разработчики добавили дополнительные функции безопасности — возможность ролевого управления доступом, а также шифрование тела SNMP-запроса.

Для работы с протоколом была выбрана система мониторинга Zabbix, которая является полностью свободной, настраиваемой, в ней присутствует возможность построение карт сети и отсутствует ограничение на количество устройств. Сравнительная таблица популярных систем мониторинга приведена на рис. 1.

	Zabbix	Prometheus	SolarWinds
Удобная визуализация	Есть	Со сторонними модулями	Есть
Возможности кастомизации	Полноценная кастомизация	Отдельные модули	Частичная кастомизация
Количество поддерживаемых устройств	Без ограничения	Без ограничения	3000 без потери производительности
Построение карт	Да	Нет	Да
Стоимость	Бесплатно	Бесплатно	1700$+

Рис. 1. Сравнение систем мониторинга

В Zabbix карту компьютерной сети можно создать двумя способами: ручным добавлением устройств и с использованием встроенного API. Для автоматизации данной задачи необходимо получить информацию о топологии, а затем добавить устройство и информацию о соединениях на карту. Для получения информации о топологии была использована схема, представленная на рис. 2.

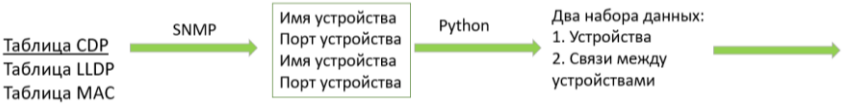

Рис. 2. Схема получения информации о топологии

Существует несколько источников, из которых можно взять информацию о соседних устройствах. Таблица CDP — таблица с информацией, полученной от проприетарного протокола CDP второго уровня, разработанного компанией Cisco. Протокол является наиболее стабильным и информативным, но не поддерживается на устройствах

других производителей. Таблица LLDP — аналог протокола CDP, но открытый, и направленный на взаимодействие между устройствами различных вендоров. Таблица MAC — список соответствий между MAC-адресами устройств и портами коммутатора, в ней отсутствует дополнительная информация о подключенном устройстве.

В качестве источника установления соседства была выбрана таблица CDP, так как компьютерная сеть построена на оборудовании Cisco. С помощью скрипта на Python, используя протокол SNMPv3, с каждого устройства собирается информация в виде набора данных: «имя», «локальный порт», «имя соседа», «порт соседа». Далее эти данные преобразуются в два списка: список устройств и список связей между устройствами. Визуализация топологии происходит с использованием Zabbix API. В POST-запрос на создание карты добавляются следующие параметры: название карты, размер в пикселях, идентификаторы устройств, связи между устройствами и другие дополнительные параметры. В результате работы скрипта была визуализирована топология сети одного из офисов предприятия (рис. 3).

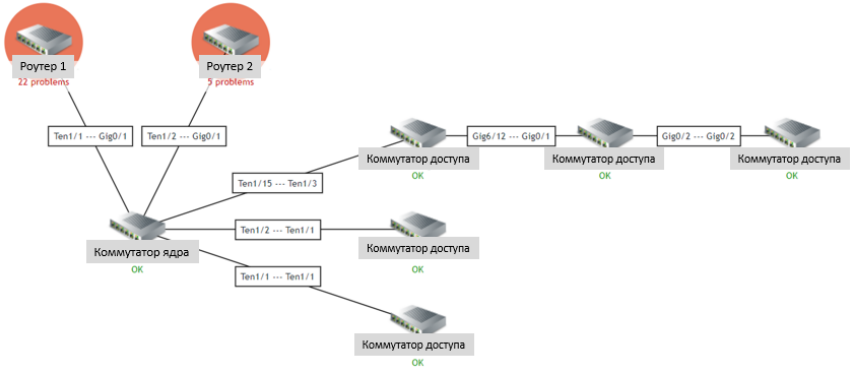

Рис. 3. Полученная топология сети одного из офисов

Заключение. В результате исследования были проведены сравнение протоколов сетевого взаимодействия с устройствами и систем мониторинга. Данный анализ позволил выбрать оптимальные решения для организации мониторинга компьютерной сети. Также была

реализована автоматическая визуализация топологии сети, что значительно ускорило время реакции на неполадки, и уменьшает возможности ошибки в результате человеческого фактора.

СПИСОК ЛИТЕРАТУРЫ

1. Строганов В. В. Электронный бизнес: использование предприятиями компьютерных сетей в бизнес-процессах / В. В. Строганов, М. А. Юревич. Москва: Информационное общество. — 2006. — № 2-3. — С. 92-102. — EDN KVSUMD. URL: https://elibrary.ru/item.asp?id=12874046
2. Угренинов А. И. Автоматизация сетевых сервисов предприятия средствами SDN / А. И. Угренинов, А. М. Шабалин // Математическое и информационное моделирование : материалы Всероссийской конференции молодых ученых, Тюмень, 18–23 мая 2022 года. — Тюмень: ТюмГУ-Press, 2022. — С. 339-344. — EDN OUAAUQ. URL: https://elibrary.ru/item.asp?id=49518848
3. Исаев А. Л. Проблема взаимодействия с телекоммуникационным оборудованием при мониторинге сетевых устройств / А. Л. Исаев, И. А. Опарин. Москва: Modern Science. — 2023. — № 1-1. — С. 260-268. — EDN TUPVRV. URL: https://elibrary.ru/item.asp?id=50119998
4. Жаркова М. С. Использование протокола SNMP для контроля параметров безопасности компьютерной сети / М. С. Жаркова, А. И. Козачок, А. В. Тезин. Москва: Инновации. Наука. Образование. — 2021. — № 46. — С. 651-656. — EDN IFFXTN. URL: https://elibrary.ru/item.asp?id=47415676
5. Лукинова О. В. Вопросы построения системы защиты компьютерной сети / О. В. Лукинова // Когнитивный анализ и управление развитием ситуаций: Международная научно-практическая мультиконференция «Управление большими системами — 2009»: Труды международной конференции, Москва, 17–19 ноября 2009 года. — Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2009. — С. 247-250. — EDN SNSETR. URL: https://elibrary.ru/item.asp?id=22012504