ВОЗДЕЙСТВИЕ ШИРОКОВЕЩАТЕЛЬНОГО ШТОРМА НА ПРОЦЕСС МОНИТОРИНГА ЛОКАЛЬНЫХ СЕТЕЙ

Шушпанников Александр Николаевич
Студент Московского политехнического университета

Логачёв Максим Сергеевич
Кандидат технических наук, доцент кафедры «Инфокогнитивные технологии» и руководитель образовательной программы «Корпоративные информационные системы» Московского политехнического университета

Аннотация: Широковещательный шторм является одной из основных причин сбоя в работе локально вычислительной сети (ЛВС) организации, который может принести убыток в десятки, а то и сотни тысяч рублей предприятию, если его не предотвратить на уровне мониторинга сетевых ресурсов или на уровне настроек сетевого оборудования. В работе подробно представлены средства и механизмы по выявлению, устранению, предотвращению и распространению шторма. Результаты представлены в виде формальных моделей, отображающие ход выполнения бизнес-процессов на предприятии при организации мониторинга (BPMN-диаграммы) и отображающие систему планирования и использования ресурсов при реализации соответствующего процесса (EPC-диаграммы). Полученные результаты могут быть использованы при проектировании и разработки универсальной системы прогнозирования сбоев или мониторинга ЛВС организации.

Ключевые слова: сеть, модель процесса, сетевые протоколы, мониторинг сети, локально вычислительная сеть, сегментирование сети, VLAN

Abstract: A broadcast storm is one of the main reasons for the failure of an organization's local area network (LAN), which can cause losses of tens or even hundreds of thousands of rubles to an enterprise if it is not prevented at the level of monitoring network resources or at the level of network equipment settings. The work presents in detail the means and mechanisms for identifying, eliminating, preventing and spreading the storm. The results are presented in the form of formal models that display the progress of business processes in the enterprise during monitoring (BPMN) and display the planning and use of resources when implementing the corresponding process (EPC). The results can be used in the design and development of a universal system for predicting failures or monitoring the LAN of an organization.

Keywords: network, process model, network protocols, network monitoring, local area network, network segmentation, VLAN

Введение

Для бесперебойной работы предприятий требуется IT-инфраструктура, обеспечивающая не только передачу данных, но и возможность управления принятием решений. Объединение такой инфраструктуры в единую сеть позволяет разделить ресурсы, предоставляя доступ множеству конченых пользователей к одному и тому же устройству; разделить данные, предоставляя доступ пользователям в соответствие с их должностными обязанностями и уровнями доступа; разделить программные средства для организации эффективной работы каждого из сотрудников организации [4].

В такой сети маршрутизация может быть статической и динамической. При организации статической маршрутизации сети возможно обеспечить быструю и простую настройку только в малых сетях за счет невысокой нагрузки на процессор сетевого оборудования [3, 5]. При динамической маршрутизации устанавливается высокий показатель отказоустойчивости, осуществляется относительно несложная настройка резервных каналов и имеется возможность автоматической балансировки трафика. Все это увеличивает нагрузку на процессоры сетевого оборудования, и при отладке

такой сети могут возникнуть непредсказуемые результаты [7].

При проектировании сети следует учитывать все возможные риски, которые могут возникнуть в дальнейшем при работе сети. Чаще всего, уже на этапе проектирования не учитываются нагрузки на будущую сеть и не закладывается возможность дальнейшего масштабирования. Но и во время работы сети следует осуществлять постоянный контроль всех объектов, входящих в ее состав. Для эксплуатации должен быть использован достаточно широкий спектр современных и научно обоснованных технических и технологических решений их анализа и мониторинга [7].

На сегодняшний момент системы контроля функционирования сети имеют некоторые недостатки. Так, масштабирование сети приводит к тому, что контроль над работой сети уменьшается и не соответствует изначально заложенным параметрам, в том числе по такому важному параметру, как максимальное время обнаружение ошибки [8]. Это объясняется тем, что увеличивается интервал между опросами сетевого оборудования. Имеющиеся в данный момент программные продукты не оптимально используют свободные ресурсы и не адаптируются к разным сетям. В большинстве случаев для работы системы мониторинга используются те ресурсы, которые уже задействованы в данный момент времени другими приложениями [6].

Аналитическая часть

Для определения проблем, возникающих в корпоративной сети организации, используют специализированные программные продукты: [9]

1. Cacti — open-source программа, позволяющая построить графики нагрузки сети на основе выбранных статистических данных.
2. Nagios — программа для системных и сетевых администраторов, разработка которой поддерживается пользователями и сторонними разработчиками. Позволяет осуществлять широкий набор функций по мониторингу сети (например, имеется возможность контроля использования дискового пространства на сервере, проверки загруженности оперативной памяти и процессора).
3. Zabbix — программа с веб-интерфейсом для сетевого и системного мониторинга сети. Функционирует с помощью программных агентов, запускаемых на контролируемых точках, или с использованием протокола SNMP. Узлы для проверки добавляются вручную или автоматически.
4. 10-Страйк Мониторинг Сети Pro — система мониторинга удаленных сетей, осуществляющая проверку доступности хостов, серверов с последующим оповещением о сбое или обрывах в виде отчета (имеется возможность настроить отправку уведомлений о неполадках на электронную почту).

Анализ используемых программных продуктов для мониторинга локальной сети показал, что их функциональные возможности схожи. Приведем в табл. 1 результаты данного анализа (рассматриваются программы только в базовой комплектации без установки дополнительных плагинов).

Использование того или иного программного продукта зависит от характеристик локально вычислительной сети организации и задач, которые должен решить ее мониторинг [2]. Но при этом существенным недостатком всех перечисленных программ (и большинства других, не вошедших в анализ) является отсутствие возможности отследить и предотвратить широковещательный шторм (broadcast storm).

Широковещательный шторм в считанные секунды парализует передачу полезного трафика во всей сети и «забивает» пакетами данных полосу пропускания портов экспоненциальным ростом их количества [3]. Причиной возникновения таких ситуаций могут быть, как и хакерские атаки, так и ошибки при настройке оборудования или сбое протоколов.

Обычно, для выявления причин широковещательного шторма проверяется активное сетевое оборудование [1]. В данном процессе участвуют, как минимум два специалиста. Модель процесса проверки всего активного оборудования выглядит таким образом, как показано на рис. 1.

Таблица 1

Характеристика программ мониторинга ЛВС

	Cacti	Nagios	Zabbix	10-Страйк Мониторинг Сети Pro
Тип	Open source	Open source	Open source	Платная
Веб-интерфейс	+	+	+	+
Реагирование на события сети	–	+	+	+
Шаблоны	+	+	+	–
Мониторинг показателей «железа»	–	+	+	+
Уведомления	E-mail	E-mail, SMS	E-mail, SMS	E-mail, SMS
Анализ сетевого трафика	–	–	–	+
Система длительного хранения данных	+	–	+	+
Графический интерфейс	+	–	+	+

Рис. 1. BPMN-диаграмма процесса проверки активного сетевого оборудования для обнаружения широковещательного шторма

Проектная часть

Существует ряд методик, позволяющих устранить в локальной вычислительной сети широковещательные штормы. К таким можно отнести следующие [11]:

1. Ограничение широковещательного трафика до 10% (или 1%). Показатель зависит от модели активного сетевого оборудования. Данный способ является простым и менее действенным.
2. Включение на коммутаторах loopback detection. В результате применения метода в сеть отправляется специальный кадр, при возвращении которого считается, что порт подключен к «штормящему» участку. Недостатком данного метода являются частые перебои, так как при масштабных «штормах» сеть становится полностью парализованной.
3. Сегментирование сети. На рис. 2 представлена модель процесса сегментирования сети, которая позволит создать изолированные виртуальные сегменты.

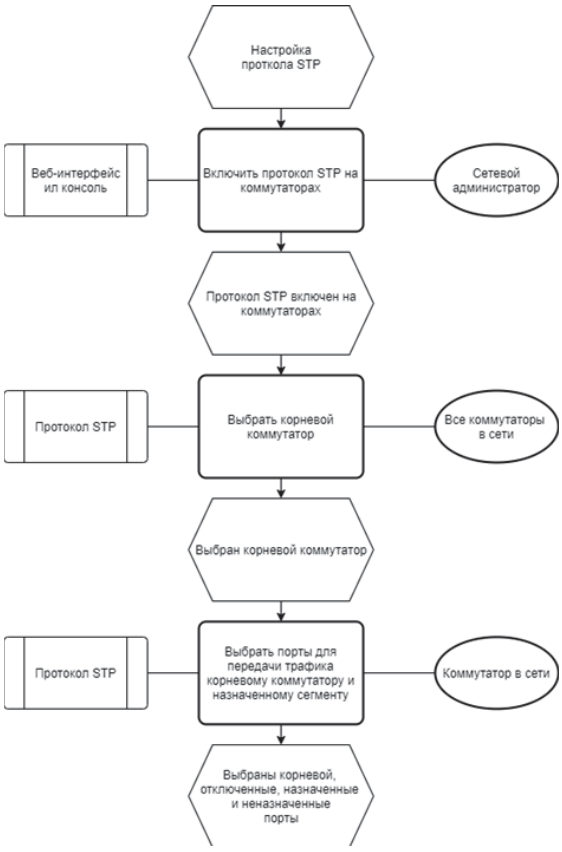

Рис. 2. Модель процесса сегментирования сети с использованием U-образной топологии

Повышение уровня безопасности можно добиться путем использования протоколов FHRP и U-образной топологии на уровне доступа. В некоторых случаях от «закольцованности» достаточно сложно отказаться, так как требуется развернуть отказоустойчивую инфраструктуру, например, с подключением к облаку. Клиентские виртуальные сети проходят внутри облачной инфраструктуры между всеми хо-

стами кластера виртуализации, получая полное дублирование всех сетевых элементов [2].

При реализации процесса устранения шторма может использоваться протокол RSTP, позволяющий находить и «разбивать» бродкастовые петли [2]. Такой вариант предпочтительнее для дата-центров, но не для организаций с постоянно растущим числом клиентов. Для таких организаций может быть использован протокол MSTP, позволяющий объединить несколько VLAN в один STP-процесс (для администрирования требуется дополнительный сотрудник с соответствующей квалификацией) [10].

Альтернативой MSTP может выступать, например, FlexLinks, позволяющий резервировать линки коммутатора или стек под единым управлением. Модель процесса использования такого средства представлена на рис. 3.

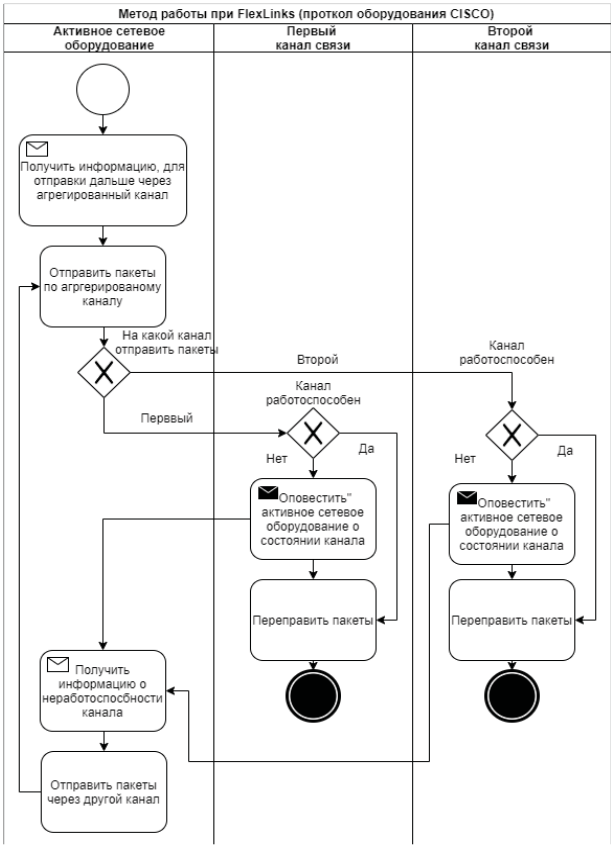

Рис. 3. Модели процессов объединения линков с использованием FlexLinks

Таким образом, модель процесса мониторинга параметров локально вычислительной сети для организации можно представить в виде модели, представленной на рис. 4.

Заключение

Система мониторинга должна обеспечивать максимально возможный уровень точности анализа состояния входящих в состав сети узлов и не оказывать влияния на состояние функционирующих в ней информационных систем. Таким образом, минимизировать влияние на интенсивность обмена служебным трафиком.

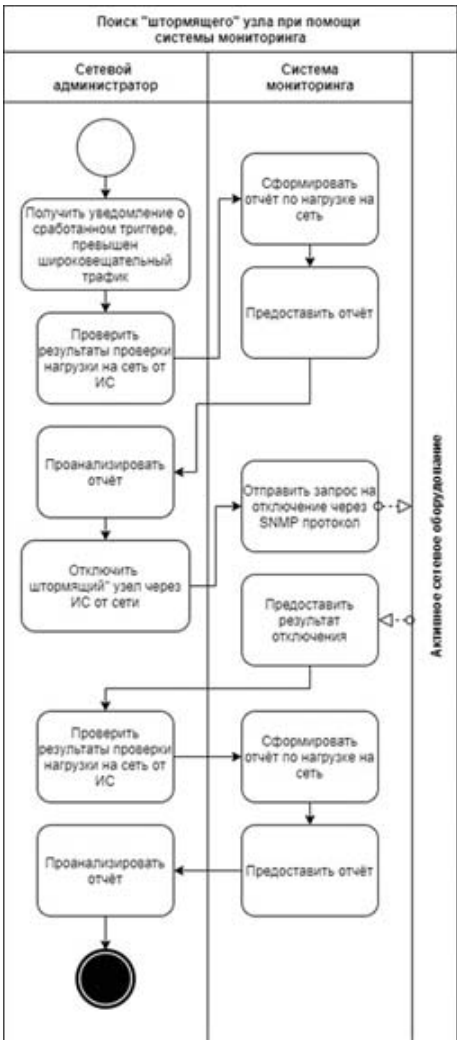

Рис. 4. Модель процесса мониторинга ЛВС с учетом определения широковещательного шторма

На рынке программ, позволяющих осуществлять мониторинг ЛВС, имеется множество систем, большая часть которых осуществляет контроль коммутаторов, серверов, баз данных и т.д. Это позволяет оперативно получать информацию о разрывах соединения, повреждении каналов связи, остановке процессов и устранять проблему до того момента, как она станет критической.

Изучение процессов показало, что имеется потенциальная возможность интеграции такого большого количества средств для мониторинга сети и производительности в консолидированной системе является востребованной.

Объединение инструментов в одном программном продукте позволит не только осуществлять контроль за производительностью сети, но и позволит создать единое хранилище данных, для которого отчеты и интеллектуальные решения станут основой для дальнейшего бесперебойного функционирования системы организации.

Список литературы

1. **Богоявленская О.Ю.** Распределенная многоагентная система мониторинга и прогнозирования производительности транспортного уровня сетей передачи данных / О.Ю. Богоявленская // Программная инженерия. – 2019. – Т9, №1. – С. 11–21. – DOI: 10.17587/prin.9.11-21.
2. «Идеальный шторм» и как это лечится [Электрон. ресурс]. – Режим доступа: https://habr.com/ru/company/dataline/blog/253609 (дата обращения: 15.04.2020). – Загл. с экрана.
3. **Изосимова Т.Н.** Разработка автоматизированной системы мониторинга оборудования и программного обеспечения компьютерной сети / Т.Н. Изосимова, Ч.О. Бочко // Инновационное развитие науки и образования: сб. ст. Междунар. науч.-практ. конф. (15 февраля 2018 г., Пенза). – Пенза: Наука и Просвещение, 2018. – С. 80–82.
4. **Лавров А.А.** Метод и алгоритмы мониторинга вычислительных сетей на основе совместного анализа временных и функциональных характеристик стека протоколов TCP/IP: автореф. дисс. ... канд. техн. наук: 05.13.11 / А.А. Лавров. – СПб., 2013. – 18 с.
5. **Лавров А.А.** Мониторинг и администрирование в корпоративных вычислительных сетях: моногр. / А.А. Лавров, А.Р. Лисс, В.В. Яновский. – СПб.: СПбГЭТУ «ЛЭТИ», 2013. – 160 с.
6. **Логачёв М.С.** Информационные системы и программирование. Администратор баз данных. Выпускная квалификационная работа: учеб. / М.С. Логачёв. – М.: Инфра-М, 2020. – 439 с. – (Среднее профессиональное образование).
7. **Логачёв М.С.** Информационные системы и программирование. Специалист по информационным системам. Выпускная квалификационная работа: учеб. / М.С. Логачёв. – М.: Инфра-М, 2020. – 576 с. – (Среднее профессиональное образование). – DOI: 10.12737/1069178.
8. **Олифер В.Г.** Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2020. – 1008 с. – (Учебник для вузов).
9. **Степанова И.В.** Использование перспективных технологий для развития распределенных корпоративных сетей связи / И.В. Степанова, М.О.А. Абдулвасеа // T-Comm. – 2017. – №6. – С. 10–15.
10. **Сторожук Д.О.** Методы и алгоритмы для систем мониторинга локальных сетей: дисс. ... канд. техн. наук: 05.13.13 / Д.О. Сторожук. – М., 2008. – 120 с.
11. **Таненбаум Э.** Компьютерные сети / Э. Таненбаум, Д. Уэзеролл; пер. Ю. Гребеньков. – 5-е изд. – СПб: Питер, 2019. – 960с. – (Классика computer science).