УДК 004

МОНИТОРИНГ ТРАФИКА ЛОКАЛЬНЫХ СЕТЕЙ

Ениватов Андрей Александрович

магистрант

Мордовский государственный университет им. Н.П. Огарева, Саранск

author@apriori-journal.ru

Аннотация. В данной статье рассматривается процесс мониторинга трафика в локальных сетях, описываются схемы процесса мониторинга трафика, средства мониторинга трафика и инструменты программной реализации.

Ключевые слова: мониторинг, локальная сеть, системы массового обслуживания, распределенные сети, программирование, база данных, C, СУБД, MySQL.

LOCAL NETWORK TRAFFIC MONITORING

Enivatov Andrey Alexandrovitch

undergraduate

Mordovian state university of N.P. Ogaryov, Saransk

Abstract. This article describes the process of monitoring traffic in local area networks, described the scheme of traffic monitoring, traffic monitoring tools and program realization.

Key words: monitoring, LAN, queuing systems, distributed networks, programming, data base, C, DBMS, MySQL.

Информационная инфраструктура современной компании представляет собой сложнейший конгломерат разномасштабных и разнородных сетей и систем. Чтобы обеспечить их слаженную и эффективную работу, необходима управляющая платформа с интегрированными инструментальными средствами. Однако до недавнего времени сама структура индустрии сетевого управления препятствовала созданию таких систем – «игроки» этого рынка стремились к лидерству, выпуская продукты ограниченной области действия, использующие средства и технологии, не совместимые с системами других поставщиков.

Сегодня ситуация меняется к лучшему – появляются продукты, претендующие на универсальность управления всем разнообразием корпоративных информационных ресурсов, от настольных систем до мэйнфреймов и от локальных сетей до ресурсов Сети. Одновременно приходит осознание того, что управляющие приложения должны быть открыты для решений всех поставщиков.

Актуальность данной работы обусловлена тем, что в связи с развитием компьютерных систем возросло значение локальных сетей (ЛВС), трафик которых и является объектом исследования. Целью исследования является создание системы мониторинга современных компьютерных сетей.

Мониторинг локальной сети - процесс (непрерывного) анализа входящего и исходящего трафика информационной системы. Проблемы в работе сети, являющейся распределенной системой массового обслуживания [4; 5] могут значительно ухудшать качество обслуживания пользователей, снижая степень их удовлетворенности сетевыми сервисами и порождая недовольство теми, кто предоставляет эти сервисы. Поэтому крайне важно максимально быстро обнаруживать, диагностировать и устранять проблемы. Различные системы сетевого мониторинга и диагностические средства ускоряют обнаружение и анализ проблем и тем самым способствуют сокращению периода времени между появ-

лением проблемы и ее устранением. Более того, собирая и анализируя информацию о работе сети, средства мониторинга позволяют выявлять возможные проблемы и не допускать их возникновения.

Предприятия заинтересованы в полном контроле работы своих сетей. При этом собирается и анализируется информация об объемах передаваемого трафика, порождающих наибольший трафик узлах, задержках в работе сети и приложений, потреблении полосы пропускания сети различными приложениями и клиентами и др. Эти сведения помогают выявлять те узлы, которые более всего нагружают сеть и устранять проблемы в работе приложений. Также с помощью средств мониторинга контролируются транзакции в приложениях и действия пользователей на предмет выявления возможных нарушений ими должностных инструкций (например, пользователи могут передавать вовне конфиденциальные данные и посещать запрещенные корпоративной политикой веб-сайты).

Сетевой администратор, на которого чаще всего ложатся функции по проведению мониторинга, должен знать особенности своей сети уже на фазе ее формирования, т.е. знать схему сети и подробное описание конфигурации программного обеспечения с указанием всех параметров и интерфейсов.

Сетевому администратору следует помнить, что с точки зрения пользователей качество работы прикладного программного обеспечения в сети оказывается определяющим. Все прочие критерии, такие как число ошибок передачи данных, степень загруженности сетевых ресурсов, производительность оборудования и т.п., являются вторичными. «Хорошая сеть» – это такая сеть, пользователи которой не замечают, как она работает.

Постоянный контроль над работой локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль – это необходимый первый этап,

который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и собственно управления полезно для небольших и средних сетей, для которых установка интегрированной системы управления экономически нецелесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети. Процесс контроля работы сети обычно делят на два этапа - мониторинг и анализ.

На этапе мониторинга выполняется процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т.п.

Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются программными и аппаратными измерителями, тестерами, сетевыми анализаторами, встроенными средствами мониторинга коммуникационных устройств, а также агентами систем управления. Задача анализа сети как распределенной системы массового обслуживания [4; 5] требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Все многообразие средств, применяемых для мониторинга вычислительных сетей, можно разделить на несколько крупных классов.

– агенты систем управления, поддерживающие функции одной из стандартных MIB (Management Information Base) – база данных информации управления [3], используемая в процессе управления сетью в ка-

честве модели управляемого объекта в архитектуре агент-менеджер, и поставляющие информацию по протоколу SNMP или CMIP. Для получения данных от агентов обычно требуется наличие системы управления, собирающей данные от агентов в автоматическом режиме.

– встроенные системы диагностики и управления (Embedded systems). Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления. Примером средств этого класса может служить модуль управления многосегментным повторителем Ethernet, реализующий функции автосегментации портов при обнаружении неисправностей, приписывания портов внутренним сегментам повторителя и некоторые другие. Как правило, встроенные модули управления «по совместительству» выполняют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления.

– анализаторы протоколов (Protocol analyzers). Представляют собой программные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями мониторинга и анализа трафика в сетях. Хороший анализатор протоколов может захватывать и декодировать пакеты большого количества протоколов, применяемых в сетях, обычно несколько десятков. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, то есть показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.

– экспертные системы. Этот вид систем аккумулирует знания технических специалистов о выявлении причин аномальной работы сетей и

возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая система помощи. Более сложные экспертные системы представляют собой, так называемые базы знаний, обладающие элементами искусственного интеллекта. Примерами таких систем являются экспертные системы, встроенные в систему управления Spectrum компании Cabletron и анализатора протоколов Sniffer компании Network General. Работа экспертных систем состоит в анализе большого числа событий для выдачи пользователю краткого диагноза о причине неисправности сети.

– оборудование для диагностики и сертификации кабельных систем. Условно это оборудование можно поделить на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

При анализе существующих программных средств мониторинга сетей были выявлены следующие недостатки:

– коммерческая лицензия – в свободном скачивании существуют только демо-версии.
– трудность настройки – процесс установки и настройки программ сильно зависит от опыта системного администратора.

Большинство коммерческих программ хорошо оптимизированы и обладают достаточным быстродействием для работы с подавляющим большинством локальных сетей. Однако, помимо них существует множество некоммерческих программ, разработанных под специфичные строения сетей, обладающих различным функционалом и, зачастую, написанных на языках высокого уровня, что ухудшает быстродействие всей системы. Учитывая этот фактор, в нашем случае для написания наиболее часто запрашиваемых (критичных по времени) модулей про-

граммы будет использован язык C [1; 2; 6], за счет чего будет достигнуто преимущество в быстродействии перед модулями, написанными на языках высокого уровня.

Программное средство мониторинга трафика в сети в нашем случае будет являться распределенной системой массового обслуживания [4; 5], схема ее представлена на рисунке 1.

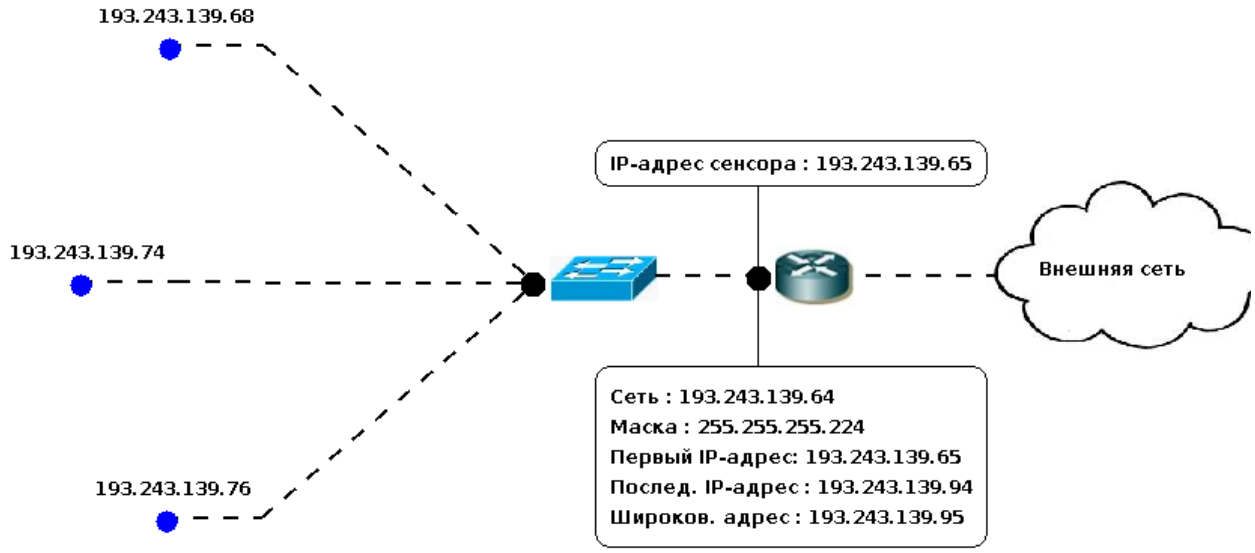

Рис. 1. Схема системы мониторинга трафика в локальной сети

Данная система состоит из следующих компонентов:

Сенсор – устройство или программное обеспечение, формирующее и экспортирующее записи об информационных потоках.

Коллектор – программное обеспечение, принимающее записи об информационных потоках от сенсора и помещающее их в хранилище.

Анализатор – программное обеспечение, обрабатывающее записи об информационных потоках из хранилища.

Сервер центра сбора данных – сервер, на котором расположен коллектор.

Визуализатор – программное обеспечение, представляющее данные хранилища в графическом виде

Процесс анализа и мониторинга трафика в локальной сети подразумевает продолжительный сбор и хранение информации о транспортировке данных в сети, времени выполнения транзакций, нагрузке узловых точек сети и статистике осуществляемых запросов каждого узла в отдельности. Постоянное накопление подобной информации требует значительных объемов памяти для запоминания, а устройства-анализаторы должны иметь возможность оперативного получения этих данных в любой момент времени. Для этих целей в составе программного продукта должна присутствовать база данных под управлением СУБД MySQL [3].

Для разработки пользовательских интерфейсов и средств генерации отчетов должны использоваться: языка программирования высокого уровня (C#, Java), встроенные возможности SQL.

Для написания критичного ко времени выполнения программного кода, который в процессе работы программы выполняется большое количество раз, должен использоваться язык низкого уровня C [1; 2; 6].

Список использованных источников

1. Александров Э.Э. Программирование на языке С в Microsoft Visual Studio 2010 / Э.Э. Александров, В.В. Афонин. Саранск: Изд-во Мордов. ун-та, 2010. 424 с.
2. Александров Э.Э., Афонин В.В., Программирование на языке С в Microsoft Visual Studio 2010 [Электронный ресурс]. Режим доступа: http://www.intuit.ru/department/pl/prcmsvs2010
3. Аббакумов А.А., Акимов В.Л., Егунова А.И., Лещанкин К.А., Таланов В.М. Базы данных (MS ACCESS, MYSQL). Саранск: Изд-во Средне-волжского математического общества, 2011. 112 с.
4. Резниченко А.Д., Аббакумов А.А., Панфилов С.А. Создание информационных систем на базе распределенных сетей сайтов // Научно-технический вестник Поволжья. 2015. № 3. С. 205-209.
5. Афонин В.В., Мурюмин С.М., Федосин С.А. Основы анализа систем массового обслуживания / В.В. Афонин, С.М. Мурюмин, С.А. Федосин. Саранск: Изд-во Мордов. ун-та. 2003. 236 с.
6. Александров Э.Э., Афонин В.В. Введение в программирование на языке С. Саранск: изд-во Мордов. Ун-та, 2009. 316 с.