УДК: 654.078

А.В. Березин

РАЗРАБОТКА МУЛЬТИАГЕНТНОЙ СИСТЕМЫ МОНИТОРИНГА СЕТЕВОГО ОБОРУДОВАНИЯ

Нижегородский государственный технический университет им. Р.Е. Алексеева

Статья посвящена разработке мультиагентной системы мониторинга сетевого оборудования, описаны методы и принципы, которые были использованы при работе над системой мониторинга, представлено описание создаваемой системы.

Ключевые слова: мультиагентный, мониторинг, сеть, гетерогенный.

Вендоры сетевого оборудования стараются сделать свой продукт уникальным, даже если функционал у устройств разных производителей один и тот же, у них различается система команд и идентификаторы OID. Развитие информационных технологий подразумевает под собой не только возможность собирать и накапливать информацию, но и осуществлять ее анализ, делая на основании его результатов конкретные выводы, полезные для соответствующей отрасли, чего не могут дать большинство из существующих сейчас на рынке систем мониторинга [1], что, в свою очередь, переходит в обязанности сетевых инженеров и системных администраторов, делая их труд напряженным, однообразным и утомительным.

Гетерогенная сеть, т.е. сеть, где используется оборудование различных вендоров, является типичной для среднего и крупного бизнеса в России. Проблемой является то, что ни одна из существующих сегодня систем мониторинга (NMS) не может дать рекомендаций по возможной проблемной ситуации, поэтому требуется их интеллектуализировать.

Теоретический анализ

Типовые задачи, решаемые системой мониторинга:

- сбор информации с сетевого оборудования;
- обработка и хранение собранных данных;
- анализ данных на наличие отклонений;
- выдача рекомендаций при наличии зафиксированных отклонений.

Для их решения предлагается использовать средства интеллектуальной поддержки принятия решения, а для описания предметной области - универсальный аппарат фреймов, который совместно с протоколом SNMP позволяет автоматизировать синтез средств интеллектуальной поддержки.

Фреймовая модель для системы мониторинга имеет следующий вид (рис. 1).

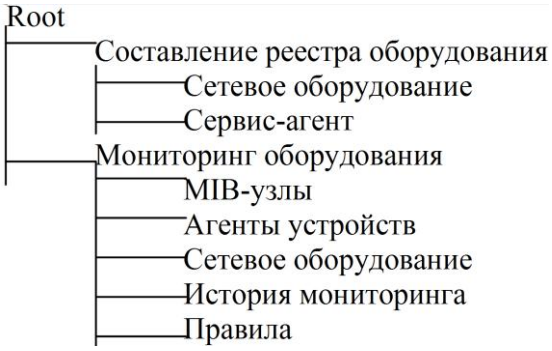

Рис. 1. Иерархия фреймов

В табл. 1 представлен пример структуры фрейма.

Таблица 1

Структура фрейма «Опрос оборудования»

Имя слота	**Значение слота**	**Домен**	**Дескриптор**
Имя фрейма: **Опрос оборудования**			
Слот 1: IP адрес устройства	сетевой адрес устройства	автоматический опрос устройства на предмет наличия его IP адреса	при выполнении этого условия передается управление во 2 слот
Слот 2: DNS имя устройств	имя, присвоенное устройству	автоматический опрос устройства на предмет наличия его DNS имени	при получении данного значения выполняется слот 3
Слот 3: ID устройства	идентификатор устройства	автоматические назначение идентификатора	после выполнения этого условия передается управление слоту 4
Слот 4: ID модели устройства	идентификатор модели устройства	автоматическое присвоение сетевому оборудования идентификатора модели	
Дескриптор: собрать информацию об устройстве			

При возникновении ситуации, когда невозможно получить данные по слоту 1, управление передается другому фрейму – поиск оборудования.

Фреймовая модель описывает типовые ситуации, возникающие при решении типовых задач мониторинга, которые описаны с помощью сценариев.

Противоречия, характерные для систем мониторинга сети:

- неуниверсальность систем мониторинга: каждая компания создает свой собственный программный продукт, который не может быть перенесен в другую корпоративную среду [2];
- отсутствие стандарта в контролируемых параметрах: есть некоторый небольшой повторяющийся во всех системах мониторинга набор параметров, который дополнительно расширяется другими параметрами, которые добавляются по желанию разработчиков или заказчиков [3];
- пассивный сбор данных: система мониторинга формирует определенную статистику, но не может указать на причину, по которой возникают сбои, а также не может дать рекомендаций по их устранению.

Данная работа посвящена проблеме создания основы, базы для интеллектуализации систем мониторинга сетей.

Система мониторинга подразумевает зависимость от человека, который может не только следить за ней, но и вмешиваться в ее работу. Такое вмешательство не всегда производится квалифицированным или уполномоченным на то персоналом, что может нарушить работу самой системы. Чтобы этого избежать, необходимо, чтобы система мониторинга могла работать в полуавтономном режиме как экспертная система, могла сама давать необходимые рекомендации.

При построении систем управления и мониторинга в режиме реального времени каждый практик неизбежно сталкивается с проблемой построения аппарата ситуационного опи-

сания [4] и интерфейса, который наглядно отображает ситуации в предметной области функционирования АС.

Свойства корпоративных компьютерных сетей:

- гетерогенность [5];
- изменчивость параметров во времени;
- изменчивость каталога установленных устройств;
- модифицируемость и расширяемость.

В данной работе предложена модель фреймового представления объектов при проектировании информационного обеспечения системы мониторинга процессов корпоративной IP-сети, отличающаяся легкой расширяемостью и модифицируемостью, подстраиваясь таким образом под различные условия использования.

Как показали исследования, данная модель характеризуется высоким уровнем универсальности и легко переносима с одной предметной области на другую. Система мониторинга состоит из двух частей: статическое ядро, переносимое с одной NMS на другую, и подсистемы взаимодействия с окружающей средой, которая требует адаптации для каждой конкретной сетевой структуры. Такого типа адаптация заключается в том, что система мониторинга настраивается на конкретные модели и параметры оборудования. В ядро входит вся логика работы программы: экспертная система, система управления агентами, база знаний, база данных, фреймовая подсистема, «скелеты» агентов.

Фрейм любого вида – это та минимально необходимая структурированная информация, которая однозначно определяет данный класс объектов. Наличие фрейма позволяет относить объект к тому классу, который им определяется [6].

Фрейм является структурой данных для представления стереотипной ситуации. С каждым фреймом ассоциирована информация разных видов. Одна ее часть указывает, каким образом следует использовать данный фрейм, другая – что предположительно может повлечь за собой его выполнение, третья – что следует предпринять, если эти ожидания не подтвердятся [6].

Фреймовая модель – инструментарий концептуального проектирования БД – информационного обеспечения: фрейм с именем «Опрос оборудования» определяет состав таблицы «Устройство»; «Сбор csv лог-файлов» – «Правила csv агента», «SNMP» – «Модель устройства», «Конкретизация вендора» – «MIB устройства», «Настройка агента» – «Агент устройства», «Выделение необходимой информации» – «MIB модели устройства», «Анализ значений» – «История параметров устройства», «Обращение к БЗ для поиска соответствующего решения» – «Правила для агентов», «Запись истории мониторинга» – история мониторинга.

Методика

Для мониторинга и управления сетями для стека TCP/IP создано два протокола: SNMP (Simple Network Management Protocol) [7, 8, 9, 10] и CMOT (Common Management information protocol Over TCP) [11]. В последнее время применение протокола CMOT ограничено [12]. Обычно управляющая прикладная программа воздействует на сеть по цепочке SNMP-UDP-IP-Ethernet [12].

Основной концепцией протокола SNMP является то, что вся необходимая для управления устройством информация хранится па самом устройстве – коммутаторе, маршрутизаторе и т.п. – в так называемой базе данных информации управления (MIB – Management Information Base).

Существует несколько стандартов на базы данных управляющей информации для протокола SNMP. Основные – стандарты MIB-I [13], MIB-II [14] и версия базы данных для удаленного управления RMON MIB [15]. Кроме этого существуют стандарты для специальных устройств MIB конкретного типа (например, MIB для концентраторов или MIB для модемов), а также частные MIB конкретных фирм-производителей оборудования.

Спецификация MIB-I определяла только операции чтения значений переменных. Операции изменения или установки значений объекта являются частью спецификаций MIB-II. Версия MIB-I определяет 114 объектов, которые подразделяются на 8 групп.

В версии MIB-II был существенно (до 185) расширен набор стандартных объектов, а число групп увеличилось до десяти.

База данных MIB-II не дает легальной статистики по характерным ошибкам кадров Ethernet, что впоследствии было реализовано в новом стандарте RMON MIB [15], который специально ориентирован на сбор детальной статистики по протоколу Ethernet.

Основной элемент любой системы управления сетью – схема взаимодействия «менеджер–агент–управляемый объект» [16]. Агент наполняет MIB управляемого объекта текущими значениями его характеристик, а менеджер извлекает данные из MIB. Таким образом, агент является посредником между управляемым объектом и менеджером располагающимся, обычно, на отдельной станции сетевого управления (NMS – Network Management Station). Агент поставляет менеджеру только те данные, которые предусматриваются MIB. Узнать MIB, поддерживаемые устройством, можно из его документации.

SNMP, как непосредственно сетевой протокол, предоставляет только набор команд для работы с переменными MIB.

Для именования переменных базы MIB и однозначного определения их форматов используется дополнительная спецификация, называемая SMI – Structure of Management Information.

При описании переменных MIB и форматов протокола SNMP спецификация SMI опирается на формальный язык ASN.1, принятый ISO в качестве нотации для описания терминов коммуникационных протоколов. Имена переменных MIB могут быть записаны как в символьном, так и в числовом форматах. Символьный формат используется для представления переменных в текстовых документах и на экране дисплея, а числовые имена – в сообщениях протокола SNMP.

Составное числовое имя объекта SNMP MIB соответствует полному имени этого объекта в дереве регистрации объектов стандартизации ISO (объекты баз MIB SNMP зарегистрированы во всемирном дереве регистрации стандартов ISO).

Пространство имен объектов ISO имеет древовидную иерархическую структуру. От корня этого дерева отходят три ветви, соответствующие стандартам, контролируемым ISO, ITU и совместно ISO-ITU. В свою очередь, организация ISO создала ветвь для стандартов, создаваемых национальными и международными организациями (ветвь org). Стандарты сети Интернет создавались под руководством министерства обороны США (Department of Defense, DoD), поэтому стандарты MIB попали в поддерево dod-internet, а далее – в группу стандартов управления сетью – ветвь mgmt.

Объекты любых стандартов, создаваемых под покровительством ISO, однозначно идентифицируются составными символьными именами, начинающимися от корня этого дерева. В сообщениях протоколов применяются однозначно соответствующие им составные числовые имена (Object Identifier – OID). Каждая ветвь дерева имен объектов нумеруется в дереве целыми числами слева направо, начиная с единицы; эти числа и заменяют символьные имена. Поэтому полное символьное имя объекта MIB имеет вид: iso.org.dod.internet.mgmt.mib, а полное числовое имя: 1.3.6.1.2.1.

Как видно, базы MIB в сочетании с протоколом SNMP представляют собой основу для мониторинга и управления сетями, позволяющую оперировать параметрами сетевых устройств на различных уровнях модели OSI/ISO. Именно значения MIB-переменных, получаемых непосредственно с наблюдаемых сетевых устройств с помощью протокола SNMP, предлагается использовать в данной работе для мониторинга состояния компьютерной сети.

Преимущества использования MIB-переменных заключаются в следующем:

- охват различных уровней сетевого взаимодействия;
- считывание данных непосредственно с наблюдаемого сетевого устройства;

– отсутствие необходимости захвата (сниффинга) и анализа трафика, что необходимо в случае использования данных, извлекаемых из пакетов, и что проблематично в случае мониторинга высокоскоростных магистралей.

Экспериментальная часть

Выясним, какая архитектура сети максимально упростит управление ею. В самой простой архитектуре (рис. 2) одна станция управления отвечает за всю сеть. Когда сеть расширяется до размера, когда одна NMS больше не может всем управлять, необходимо будет переходить на более распределенную архитектуру. Ее идея: использовать две или более станций управления и расположить их максимально близко к управляемым ими узлам.

В обеих архитектурах для отправки и получения трафика управления используется Интернет. Это вызывает проблемы, связанные с безопасностью и общей надежностью. Наилучшим решением будет использование для выполнения всех функций по управлению сетью частных каналов (VPN), которые, в основном, выделены для трафика управления, хотя их можно использовать и в других целях. Использование частных каналов имеет преимущество: строки «сообщество» никогда не отправляются через Интернет. Использование частных каналов также подходит для архитектуры с одной NMS. Если корпоративная сеть состоит исключительно из частных каналов, а интернет-подключения выделены только для внешнего трафика, использование частных каналов для трафика управления становится очевидным.

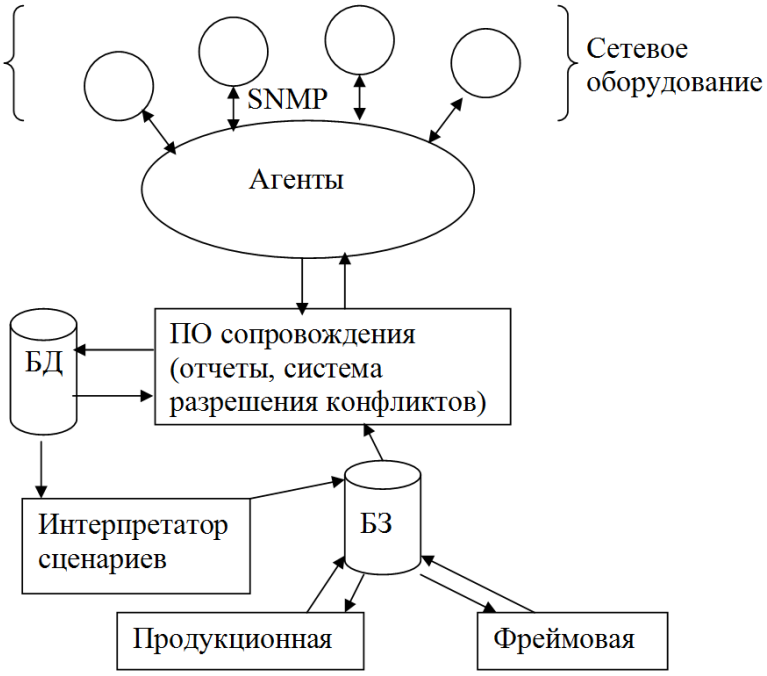

Рис. 2. Архитектура системы мониторинга

Результаты

В ходе работы созданы модель и программный комплекс, позволяющие повысить эффективность мониторинга компьютерной сети предприятия. Это осуществляется за счет выдачи рекомендаций по сложившимся ситуациям.

В работе получены следующие основные теоретические и практические результаты:

1. Предложена модель фреймов для построения программы сетевого мониторинга;
2. Разработана структура специального программного обеспечения мониторинга компьютерной сети, позволяющего давать рекомендации по сложившейся ситуации;

3. Произведена апробация программы на данных реально действующей сети НГТУ кафедры «Менеджмент».

Библиографический список

1. **Олифер, В.Г.** Средства анализа и оптимизации локальных сетей / В.Г. Олифер, Н.А. Олифер // Центр Информационных Технологий CITFORUM, 1998. URL: http://citforum.ru/nets/optimize/ (дата обращения: 30.01.2014).
2. Полный мониторинг сети. Кто как мониторит свою сеть… URL: http://forum.nag.ru/forum/index.php?showtopic=45571&st=80 (дата обращения: 30.01.2014).
3. Полезные SNMP MIB object (OID) для Cisco URL: http://www.opennet.ru/base/net/cisco_snmp.txt.html (дата обращения: 30.01.2014).
4. **Мисевич, П.В.** Сценарно-ситуационный подход к проектированию средств интеллектуальной поддержки процесса функционирования автоматизированных систем // Системы управления и информационные технологии. 2007. N2.1(28). С. 166–171.
5. **Олифер, В.Г.** Транспортная подсистема неоднородных сетей / В.Г. Олифер, Н.А. Олифер // Центр Информационных Технологий CITFORUM, 1998. URL: http://citforum.ru/nets/tpns/contents.shtml (дата обращения: 30.01.2014).
6. **Минский, М.** Фреймы для представления знаний / М. Минский. – М.: Мир, 1979. – 152 с.
7. Case J., Fedor M., Schoffstall M., Davin J. A Simple Network Management Protocol (SNMP), RFC 1157, SNMP Research Inc., 1990.
8. Rose M. Bulk. A Convention for Defining Traps for use with the SNMP, RFC 1215, 1991.
9. Rose M., McCloghrie K., Davin J. Bulk Table Retrieval with the SNMP, RFC 1187, 1990.
10. Schoffstall M., Davin J., Fedor M., Case J. SNMP over Ethernet, RFC 1089, 1989.
11. Waldbusser S. Remote network monitoring management information base, RFC 1271, 1991.
12. **Семенов, Ю.А.** Телекоммуникационные технологии. // ИТЭФ-МФТИ. 2013. URL: http://book.itep.ru/1/intro1.htm (дата обращения: 30.01.2014).
13. McCloghrie K. Management Information Base for Network Management of TCP/IP-based internets. RFC 1156, 1990.
14. McCloghrie K., Rose M. Management information base for network management of TCP/IP-based internets: MIB-II, RFC 1213, 1991.
15. Thottan M. J. Anomaly detection in IP Networks // IEEE Transactions on signal processings, vol.51, no.8, 2003, University of California Berkeley.
16. **Олифер, В.Г.** Основы компьютерных сетей / В.Г. Олифер, Н.А. Олифер.– Питер, 2009. – 352 с.

Дата поступления
в редакцию 27.06.2014

A.V. Berezin

DEVELOPMENT OF NETWORK EQUIPMENT MULTI-AGENT MONITORING SYSTEM

Nizhny Novgorod state technical university n.a. R.E. Alexeev

Purpose: tools creation on the basis of frames. It automates multi-agent system monitoring construction and supports all network equipment of heterogeneous networks.

Design/methodology/approach. Proposed theoretical framework is based on three mutually complementary perspectives: frames, multi-agency and expert systems.

Findings. It is possible, for example, to apply findings in companies with large network.

Research limitations/implications. The present study provides a starting-point for further researches in the international industrial sector.

Originality/value. Frame model representation of objects is offered while designing aids of monitoring system intellectual support.

Key words: multi-agency, monitoring, network, heterogeneity.