ИССЛЕДОВАНИЕ И РАЗРАБОТКА ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ МОНИТОРИНГА ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ НА ОСНОВЕ ОТКРЫТЫХ СТАНДАРТОВ И ТЕХНОЛОГИЙ[1]

А.А. Сорокин, С.П. Королёв, А.Г. Тарасов, А.Л. Верхотуров
ВЦ ДВО РАН
e-mail: <alsor@febras.net>
ВЦ ДВО РАН
e-mail: <serejk@febras.net>
ВЦ ДВО РАН
e-mail: <taleks@as.khb.ru>
ВЦ ДВО РАН
e-mail: <andrey@ccfebras.ru>

Аннотация

С развитием телекоммуникационных сетей, информационных сервисов и лавинообразным ростом числа их пользователей, у операторов связи возникает проблема обеспечения качества представляемых услуг и бесперебойного доступа к ресурсам сети.

Выявление аномальных событий в работе сети позволяет своевременно устранить или минимизировать проблему, тем самым обеспечить надлежащий уровень сервиса, как для работы конечных потребителей, использующих стандартные пользовательские приложения, так и информационных систем (Grid, системы видеоконферецсвязи и др.), для работы которых требуется телекоммуникационный ресурс с гарантированной пропускной способностью или особенными параметрами.

Несмотря на многообразие информационных систем, до настоящего времени нет готовых решений, которые бы интегрировали на одной программной платформе инструменты для работы с протоколами SNMP и NetFlow с возможностью централизованного контроля и обработки данных, получаемых от всех средств управления сетью. В статье рассматриваются вопросы создания автоматизированной информационной системы для комплексного мониторинга телекоммуникационных сетей на основе открытых стандартов и технологий.

С развитием телекоммуникационных сетей, информационных сервисов и лавинообразным ростом числа их пользователей, у операторов связи возникает проблема обеспечения качества представляемых услуг и бесперебойного доступа к ресурсам сети. Она решается за счет внедрения систем мониторинга и управления сетью, которые должны информировать администраторов сети о проблемных ситуациях (событиях), возникающих вследствие различных ошибок, связанных с работой средств связи, использованием различного рода информационных сервисов, генерирующих большое количество соединений, проблем в области информационной безопасности и т.п. Указанные системы должны обладать инструментами для проведения качественного и количественного анализа трафика сети, определения состояния работы компонентов информационно-телекоммуникационной инфраструктуры.

Выявление аномальных событий в работе сети позволяет своевременно устранить или минимизировать проблему, тем самым обеспечить надлежащий уровень сервиса, как для работы конечных потребителей, использующих стандартные пользовательские приложения, так и информационных систем (Grid, системы видеоконферецсвязи и др.), для работы

[1] Работа проводится при поддержке Гранта РФФИ № 12-07-31149

которых требуется телекоммуникационный ресурс с гарантированной пропускной способностью или особыми параметрами. Решение вышеперечисленных задач связано с проведением не только технических (например, сбор показаний с сенсоров сети), но и исследовательских работ, таких как анализ потоков данных, разработка или адаптация алгоритмов их обработки и т.п. При этом важным исходным материалом для выполнения этих работ, является инструментальная информация, получаемая в результате оценки работы сети с использованием специализированных сетевых протоколов, среди которых наиболее используемыми являются SNMP [1] и NetFlow [2]. Первый представляет собой иерархическую систему оценки состояния различных счетчиков и средства управления устройствами, второй - протокол, для учета качественных и количественных показателей трафика сети. На базе этих и других протоколов работают многочисленные системы мониторинга информационно-телекоммуникационной инфраструктуры (Ganglia, Nagios, Zabbix, Netams и др.), которые помимо средств учета и визуализации состояния сети, позволяют создавать шаблоны поведения и реакции на различные события.

Как правило, системы мониторинга достаточно эффективно решают задачи сбора и обработки данных в своей узкоспециализированной области (например, Ganglia ориентирована на работу в сети вычислительного кластера), но не обладают возможностью взаимодействия друг с другом, что исключает использование в работе всего набора возможных первичных данных и средств их интерпретации. Таким образом, для поддержки и оценки функционирования сети и её ресурсов необходимо поддерживать и работать со множеством различных специализированных информационных систем. Это создает очевидные ограничения и неудобства, которые приводят к снижению скорости реакции на возникающие инциденты и увеличения вероятности возникновения ошибки администратора при работе с большим числом инструментов.

Несмотря на многообразие информационных систем, до настоящего времени нет готовых решений, которые бы интегрировали на одной программной платформе инструменты для работы с протоколами SNMP и NetFlow с возможностью централизованного контроля и обработки данных, получаемых от всех средств управления сетью. Совместный анализ данных как минимум этих двух протоколов, позволит получать качественные и количественные показатели состояния сети, как в режиме реального времени, так и за определенный промежуток прошедшего времени. Это позволит быстро и эффективно выявлять как единичные случаи нарушения нормального функционирования сети, так и системные долговременные попытки воздействия на нее, что приведет к повышению надежности её функционирования и как следствие предоставление информационным сервисам, ресурсам и пользователям необходимых телекоммуникационных ресурсов.

В ВЦ ДВО РАН начаты работы по созданию автоматизированной информационной системы (далее - АИС), направленной на решение задач мониторинга телекоммуникационной сети, обеспечивающей сбор информации со средств передачи данных и управления сетью по протоколам Syslog[3], SNMP, NetFlow, её комплексный анализ и хранение. АИС обеспечит решение следующих основных задач:

- сбор данных с различных сенсоров сети, передача их по каналам связи в коллектор, обеспечение защиты передаваемой информации от модификации и несанкционированного доступа;

- анализ и совместная обработка инструментальных данных, корреляция значений всех имеющихся метрик с возможностью получения как комплексной оценки состояния сети в целом, так и статуса отдельно наблюдаемого объекта;
- разработка и адаптация средств визуализации и оповещения о событиях в сети, сокращающих время на их оценку и принятие управленческих решений;
- формирование открытой, расширяемой и масштабируемой программной архитектуры, позволяющей добавлять в информационную систему новые алгоритмы анализа, и учитывать изменение конфигурации в топологии сети.

АИС будет реализована в виде набора взаимосвязанных информационных подсистем в составе:

1. Коллекторы данных мониторинга.

Указанные компоненты будут обеспечивать непрерывный прием информации от сенсоров сетевых устройств сети. Для этой подсистемы будут разработаны или адаптированы существующие технологии взаимодействия с устройствами передачи данных и специализированных компонент сети посредством различных протоколов. После сбора данных они могут быть переданы по запросу другим программным приложениям. Клиентские приложения могут обращаться к коллектору данных для получения новой информации от всех подсистем мониторинга в едином формате.

2. Модуль агрегации и архивации измеряемых величин.

Он определяет структуру и способ хранения значений метрик с необходимым уровнем детализации, осуществляет архивацию данных и обеспечивает доступ к накопленным базам данных. Многие процессы в сети невозможно корректно идентифицировать по данным за короткий промежуток времени или по одномоментному снимку всех метрик сети. Данная подсистема обеспечит надежное хранение данных за выбранное время работы с необходимым уровнем детализации.

3. Модуль анализа и обработки данных мониторинга.

Модуль предназначен для анализа полученных данных с целью выявления таких событий как критические значения метрик, потери на каналах связи при передачи информации, вирусная активность, DDoS-атаки на периметр сети и др. На основе комплексных триггеров модуль будет формировать уведомления о возникающих в сети проблемах и передавать их используя различные средства связи и оповещения.

4. Интерфейс пользователя.

Подсистема будет отвечать за формирование и функционирование набора пользовательских web-интерфейсов для работы с модулями АИС. Разработанные и адаптированные алгоритмы и технологии, положенные в основу АИС будут реализованы на основе открытой программной платформы Zabbix [4]. Она предоставляет средства мониторинга сети по протоколам SNMP и IPMI, а также интерфейс программирования приложений (API) для разработки виджетов визуализации и работы с архивом инструментальных данных.

Все созданные программные подсистемы будут апробированы и внедрены на базе Региональной компьютерной сети передачи данных ДВО РАН [5], построенной с использованием различных технологий и каналов связи.

ЛИТЕРАТУРА

[1]. Мауро Д., Шмидт К. Основы SNMP. – М.: Символ, Санкт-Петербург, 2012, 520 с.

[2]. Cisco IOS NetFlow / http://www.cisco.com/go/netflow.
[3]. A. Deveriya. Network administrators survival guide. – M.: Cisco Press, 2006, 552 p.
[4]. R. Olups. Zabbix 1.8 Network Monitoring. – M.: Packt Publishing, 2010, 428 p.
[5]. Ханчук А.И.,Наумова В.В., Сорокин А.А. Корпоративная сеть ДВО РАН: высокотехнологичная интеграция научных подразделений // Вестник РАН, 2008, №4, с.298-303