

ОБЗОР ИНСТРУМЕНТОВ МОНИТОРИНГА ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Ган-Ловкис В. С.

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Зацепин Е.Н – кандидат технических наук, доцент

Рассмотрены средства, применяемые для мониторинга и анализа вычислительных сетей.

Системы управления сетью (NetworkManagementSystems) - централизованные программные системы, которые собирают данные о состоянии узлов и коммуникационных устройств сети, а также данные о трафике, циркулирующем в сети. Эти системы не только осуществляют мониторинг и анализ сети, но и выполняют в автоматическом или полуавтоматическом режиме действия по управлению сетью - включение и отключение портов устройств, изменение параметров мостов адресных таблиц мостов, коммутаторов и маршрутизаторов и т.п. Примерами систем управления могут служить популярные системы HPOpenView, SunNetManager, IBMNetView.

Средства управления системой (SystemManagement). Средства управления системой часто выполняют функции, аналогичные функциям систем управления, но по отношению к другим объектам. В первом случае объектом управления является программное и аппаратное обеспечение компьютеров сети, а во втором - коммуникационное оборудование. Вместе с тем, некоторые функции этих двух видов систем управления могут дублироваться, например, средства управления системой могут выполнять простейший анализ сетевого трафика.

Встроенные системы диагностики и управления (Embeddedsystems). 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 концентратором Distrebuted 5000, реализующий функции автосегментации портов при обнаружении неисправностей, приписывания портов внутренним сегментам концентратора и некоторые другие. Как правило, встроенные модули управления "по совместительству" выполняют роль SNMP-агентов, поставляющих данные о состоянии устройства для систем управления.

Анализаторы протоколов (Protocolanalyzers). 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.

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 (мультиметры).

- *Сетевые мониторы* (называемые также *сетевыми анализаторами*) предназначены для тестирования кабелей различных категорий. Следует различать сетевые мониторы и анализаторы протоколов. Сетевые мониторы собирают данные только о статистических показателях трафика - средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т.п.

- Назначение *устройств для сертификации кабельных систем*, непосредственно следует из их названия. Сертификация выполняется в соответствии с требованиями одного из международных стандартов на кабельные системы.

- *Кабельные сканеры* используются для диагностики медных кабельных систем.

- *Тестеры* предназначены для проверки кабелей на отсутствие физического разрыва.

Экспертные системы. Этот вид систем аккумулирует человеческие знания 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 help-система. Более сложные экспертные системы представляют собой так называемые базы знаний, обладающие элементами искусственного интеллекта. Примером такой системы является экспертная система, встроенная в систему управления Spectrum компании Cabletron.

Многофункциональные устройства анализа и диагностики. В последние годы, в связи с повсеместным распространением локальных сетей возникла необходимость разработки недорогих

портативных приборов, совмещающих функции нескольких устройств: анализаторов протоколов, кабельных сканеров и, даже, некоторых возможностей ПО сетевого управления. В качестве примера такого рода устройств можно привести Compas компании MicrotestInc. или 675 LANMeter компании FlukeCorp.

В соответствии с рекомендациями ISO можно выделить следующие функции *средств управления сетью*:

- *Управление конфигурацией сети и именованием* - состоит в конфигурировании компонентов сети, включая их местоположение, сетевые адреса и идентификаторы, управление параметрами сетевых операционных систем, поддержание схемы сети: также эти функции используются для именованя объектов.

- *Обработка ошибок* - это выявление, определение и устранение последствий сбоев и отказов в работе сети.

- *Анализ производительности* - помогает на основе накопленной статистической информации оценивать время ответа системы и величину трафика, а также планировать развитие сети.

- *Управление безопасностью* - включает в себя контроль доступа и сохранение целостности данных. В функции входит процедура аутентификации, проверки привилегий, поддержка ключей шифрования, управления полномочиями. К этой же группе можно отнести важные механизмы управления паролями, внешним доступом, соединения с другими сетями.

- *Учет работы сети* - включает регистрацию и управление используемыми ресурсами и устройствами. Эта функция оперирует такими понятиями как время использования и плата за ресурсы.

Из приведенного списка видно, что системы управления выполняют не только функции мониторинга и анализа работы сети, необходимые для получения исходных данных для настройки сети, но и включают функции активного воздействия на сеть - управления конфигурацией и безопасностью, которые нужны для отработки выработанного плана настройки и оптимизации сети. Сам этап создания плана настройки сети обычно остается за пределами функций системы управления, хотя некоторые системы управления имеют в своем составе экспертные подсистемы, помогающие администратору или интегратору определить необходимые меры по настройке сети.

Средства управления системой обычно выполняют следующие функции:

- *Учет используемых аппаратных и программных средств*. Система автоматически собирает информацию об обследованных компьютерах и создает записи в базе данных об аппаратных и программных ресурсах. После этого администратор может быстро выяснить, чем он располагает и где это находится. Например, узнать о том, на каких компьютерах нужно обновить драйверы принтеров, какие ПК обладают достаточным количеством памяти и дискового пространства и т. п.

- *Распределение и установка программного обеспечения*. После завершения обследования администратор может создать пакеты рассылки программного обеспечения - очень эффективный способ для уменьшения стоимости такой процедуры. Система может также позволять централизованно устанавливать и администрировать приложения, которые запускаются с файловых серверов, а также дать возможность конечным пользователям запускать такие приложения с любой рабочей станции сети.

- *Удаленный анализ производительности и возникающих проблем*. Администратор может удаленно управлять мышью, клавиатурой и видеть экран любого ПК, работающего в сети под управлением той или иной сетевой операционной системы. База данных системы управления обычно хранит детальную информацию о конфигурации всех компьютеров в сети для того, чтобы можно было выполнять удаленный анализ возникающих проблем.

Примерами средств управления системой являются такие продукты, как SystemManagementServer компании Microsoft или LANDeskManager фирмы Intel, а типичными представителями средств управления сетями являются системы HPOpenView, SunNetManager и IBMNetView.

Список использованных источников

1. *Высокоскоростные ЛКС [Электронный ресурс]*. – Электронные данные. – Режим доступа: <http://citforum.ru>.
2. *Кабельные системы Fast Ethernet [Электронный ресурс]*. – Электронные данные. – Режим доступа: <http://citforum.ru>.
3. Кеннет, Г. *Основы сетей Windows / Г. Кеннет*. – М. : Диалектика 1999, – 237 с.
4. *Коммутаторы Ethernet. Начальные сведения [Электронный ресурс]*. – Электронные данные. – Режим доступа: <http://citforum.ru>.