К ВОПРОСУ ОРГАНИЗАЦИИ МОНИТОРИНГА И АНАЛИЗА КОМПЬЮТЕРНЫХ СЕТЕЙ

А.Н. Курбацкий, С.А. Харевич
Беларусь, г. Минск

При эксплуатации компьютерных сетей часто возникают проблемы, связанные, либо с ухудшением их эксплуатационных характеристик, либо с потерей работоспособности. Данная ситуация показывает необходимость создания стратегии мониторинга и анализа компьютерной сети с комбинированным использованием аппаратурных и программных средств. Суть стратегии должна заключаться в следующем: в функционирующей компьютерной сети необходимо регулярно проводить многоуровневый мониторинг. Степень регулярности и выбор уровня мониторинга зависят от размера и топологии сети, а так же от ее прикладного значения. Уровень мониторинга может быть полный и частичный. Чем больше размер сети и ее прикладное значение, тем более регулярный (вплоть до постоянного) и более полный мониторинг следует проводить.

При частичном мониторинге в первую очередь проверке подлежат самые критичные узлы, потеря работоспособности которых может привести к отказу в работе значительного сегмента сети. Мониторинг таких узлов следует производить наиболее часто. На примере сети, структурная модель которой приведена на рис.1 можно сказать, что наиболее жесткому контролю должны подвергаться коммутаторы, концентраторы и маршрутизаторы, которые являются центральными объектами сети. Далее внимание можно уделить контроллерам домена, серверам, где находятся общие ресурсы, а уж затем рабочим станциям.

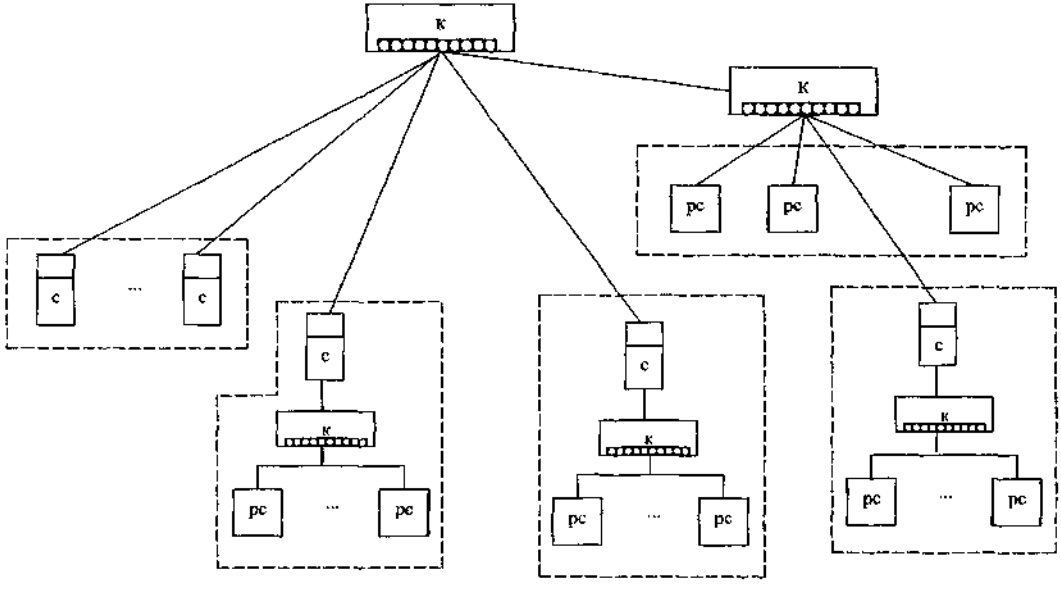
При полном мониторинге сети проверке подлежат все узлы, включая кабельные соединения между ними. При возможности он должен проходить постоянно.

Алгоритм полного мониторинга сети можно разделить на семь этапов согласно семиуровневой модели OSI [1,2].

На первом этапе, которому соответствует физический уровень, мониторингу подвергаются:

- концентраторы, хабы и повторители, регенерирующие электрические сигналы;

- соединительные разъемы среды передачи, обеспечивающие механический интерфейс для связи устройства со средой передачи;



Условные обозначения:
с-сервер, рс – рабочая станция, к-коммутатор.

Рис.1.Структурная модель компьютерной локальной сети

- модемы и различные преобразующие устройства, выполняющие цифровые и аналоговые преобразования.

На втором этапе, которому соответствует канальный уровень, мониторингу подвергаются:

-мосты;

- интеллектуальные концентраторы;

- коммутаторы;

- сетевые интерфейсные платы (сетевые интерфейсные карты, адаптеры и т.д.).

На третьем этапе - сетевом уровне, мониторингу подвергаются маршрутизаторы и некоторые виды интеллектуальных коммутаторов.

На четвертом этапе - транспортном уровне, мониторингу подвергается контроль доставки данных.

На пятом этапе – сеансовом уровне, мониторингу подвергается взаимодействие между устройствами, запрашивающими и поставляющими сетевые услуги.

На шестом этапе - уровне представления данных, мониторингу подвергается преобразование данных во взаимно согласованные форматы, понятные всем сетевым приложениям и компьютерам, на которых работают приложения.

На седьмом этапе, которому соответствует прикладной уровень, мониторингу подвергаются протоколы, необходимые для выполнения конкретных функций сетевого сервиса.

Для анализа и диагностики компьютерных сетей применяются различные аппаратные и программные средства [3], которые можно разделить на несколько классов:

- агенты систем управления, поддерживающие функции одной из стандартных баз данных управляющей информации 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 так же 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;

- сетевые мониторы (называемые также сетевыми анализаторами) предназначены для тестирования кабелей различных категорий. Сетевые мониторы собирают также данные о статистических показателях трафика: средней интенсивности общего трафика сети, средней интенсивности потока пакетов с определенным типом ошибки и т. п. Эти устройства являются наиболее интеллектуальными устройствами из всех четырех

групп устройств данного класса, так как работают не только на физическом, но и на канальном, а иногда и на сетевом уровнях;

- устройства для сертификации кабельных систем выполняют сертификацию 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.

В тех местах, где необходимо обеспечить особую отказоустойчивость в работе сети, необходимо, производить постоянный мониторинг сети.

Как один из вариантов обеспечения мониторинга можно рассмотреть программный комплекс, реализующий в себе функции анализатора протоколов. Данные исследований будут храниться на Microsoft SQL сервере, который содержит средства для возможности корректной одновременной работы нескольких пользователей. Данные должны быть представлены в трех разделах: первый из них будет ориентирован на менеджмент – персонал организаций – т.е. на людей, принимающих решения в сфере информационной структуры предприятия. В этом разделе будут содержаться визуальные интуитивно-понятные выводы работы компьютерной сети предприятия (организации) - схемы, графики, чертежи и т. д. Данный раздел должен обеспечивать:

1) Сбор статистики простоя классов (должны быть исследованы причины простоя классов, возникших ошибок);

2) Показ результатов загрузки отделов (классов);

3) Показ производительности по узлам и по всей компьютерной сети в целом;

4) Сохранение журналов контроля.

Второй раздел должен представлять сведения о работе сети, которые будут интересны инженерно – техническому персоналу предприятия. На основании этих данных специалисты могут сделать обоснованные выводы о работе сетевой инфраструктуры. Третий раздел должен представлять математические исследования и анализ полученных данных.

После сбора информации в каждом из разделов данные будут обработаны и будет осуществлен их экспертный анализ для подачи рекомендаций по дальнейшей эксплуатации сети. Так же должен быть задействован математический аппарат в области математической статистики в це-

лях получения статистических данных о работе компьютерной сети предприятия (организации).

Литература

1. Отлри Терри. Модернизация и ремонт сетей. – М.: Издательский дом "Вильямс", 2005.-1240с.

2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник.-СПб.: Питер, 2003. – 863с.

3. Татенбаум Э. Компьютерные сети.- СПб.:Питер, 2002. – 848с.