УДК 681.3

А. Л. Моисеев, Р. Р. Моисеева, В. В. Шаров,
Ю. Н. Зацаринная

МЕТОДЫ ТЕСТИРОВАНИЯ И ДИАГНОСТИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Ключевые слова: локальная сеть, диагностика, тестирование.

В данной статье рассмотрены основные методы тестирования и диагностирования компьютерных сетей. Благодаря своевременному выявлению ошибок в работе сети можно значительно повысить эффективность работы компьютерных сетей, а также увеличить эксплуатационный срок.

Keywords: local network, diagnostics, testing.

In this article the main methods of testing and diagnosing of computer networks are considered. Thanks to timely identification of mistakes in network functioning it is possible to increase considerably overall performance of computer networks, and also to increase operational term.

На протяжении ряда лет большинство вопросов повышения производительности и надежности сетей решалось закупкой новой техники. Не всегда подобное решение было технически и экономически обоснованно, но почти всегда оно позволяло достигнуть желаемой цели — сеть начинала работать быстрее и лучше. При наличии 200% запаса пропускной способности практически все "узкие места" можно без труда "расширить", а приобретая только самое дорогое оборудование лидеров сетевых технологий, вы можете с большой степенью вероятности обезопасить себя от "скрытых дефектов". Сегодня ситуация изменилась, и экономическое обоснование проектов по модернизации сетей становится актуальным. Мировой опыт показывает, что инвестиции в профессионализм специалистов дают большую отдачу, чем инвестиции в "железо", даже очень хорошее. Необходимую пропускную способность сети или ее надежность нельзя оценить без детального анализа ее нынешнего состояния. Это можно сделать только посредством диагностических средств и методов тестирования компьютерных сетей.

Диагностические средства, предназначенные для компьютерных сетей, можно классифицировать по двум основным признакам:

- средство предназначенное для диагностики сети или для тестирования сети;
- средство предназначенное для реактивной диагностики или для упреждающей диагностики.

Под диагностикой сети принято понимать измерение характеристик работы сети в процессе ее эксплуатации (без остановки работы операторов). Диагностикой сети является, в частности, измерение числа ошибок передачи данных, степени загрузки (утилизации) ресурсов сети или времени реакции прикладного ПО, которую администратор сети должен осуществлять ежедневно.

Диагностика бывает двух типов: упреждающая (proactive) и реактивная (reactive). Упреждающая диагностика должна проводиться в процессе эксплуатации сети ежедневно. Основная цель упреждающей диагностики — предотвращение сбоев в работе сети. Реактивная диагностика выполняется, когда в сети уже произошел сбой и надо быстро локализовать источник и выявить причину.

Для того чтобы проверить соответствие качества кабельной системы требованиям стандартов, определить максимальную пропускную способность сети или оценить время реакции прикладного программного обеспечения (ПО) при изменении параметров настройки коммутатора или операционной системы (ОС), то такие измерения можно сделать только при отсутствии в сети работающих пользователей. В этом случае правильно употреблять термин "тестирование" сети. Таким образом, тестирование сети — это процесс активного воздействия на сеть с целью проверки ее работоспособности и определения потенциальных возможностей по передаче сетевого трафика.

Тестирование можно условно разделить на несколько видов в зависимости от цели, ради которой оно проводится. Это тестирование кабельной системы сети на соответствие стандартам TIA/EIA TSB-67; стрессовое тестирование конкретных сетевых устройств с целью проверки устойчивости их работы при различных уровнях нагрузок и различных типах сетевого трафика; тестирование ПО, в частности для определения его требований к пропускной способности сетевых ресурсов (к характеристикам канала связи, сервера и т. п.); стрессовое тестирование сети (конкретных сетевых конфигураций) с целью выявления "скрытых дефектов" в оборудовании и "узких мест" в архитектуре сети, а также с целью определения пороговых значений трафика, допустимых в данной сети.

Тестирование прикладного ПО с целью определения требований к пропускной способности сетевых ресурсов проводят компании-разработчики ПО. Такое тестирование осуществляется в рамках комплексной проверки ПО перед выпуском его на рынок и называется тестированием на соответствие качеству (Quality Assurance Test, QAT

Стрессовое тестирование сетевых устройств обычно проводится независимыми специализированными лабораториями. Примерами таких лабораторий являются организации LANQuest и Data Communications. Чаще всего стрессовое тестирование устройств проводится с целью проверки заявленных технических характеристик и выявления различного рода дефектов.

Средства, предназначенные для диагностики сетей, можно условно разделить на две категории в зависимости от принципа их работы: средства мониторинга и управления работой сети (далее средства мониторинга — monitoring software) и анализаторы сетевых протоколов (далее анализаторы протоколов — analyzers).

Принцип работы средств мониторинга основан на взаимодействии консоли оператора с так называемыми агентами, которые, собственно, и занимаются мониторингом и управлением работой устройств сети. Примерами средств мониторинга являются программы Transcend компании 3Com, Optivity компании Bay Networks (ныне Nortel), HP OpenView Net Metrix. Агенты могут быть встроены в оборудование или загружены программным образом. Поскольку наиболее распространенным протоколом общения консоли оператора и агентов является SNMP, такие агенты часто называют SNMP-агентами. SNMP-агенты могут выполнять самые различные функции в зависимости от типа баз управляющей информации (Management Information Base, MIB), которые они поддерживают. Эти функции могут включать в себя управление конфигурацией устройства, в которое агенты встроены (configuration management), управление контролем доступа к информации (security management), анализ производительности устройства (perfomance management), измерение числа ошибок при передаче данных (fault management) и другие.

При реактивной диагностике сети с помощью средств мониторинга измерительным прибором является SNMP-агент самого диагностируемого устройства. Однако при появлении сбоев показания SNMP-агента нельзя считать достоверными. Это особенно актуально, когда сбои происходят в самом устройстве с установленным SNMP-агентом. В таких случаях наблюдатель должен быть "независим" от диагностируемого устройства. SNMP-агент устройства наблюдает за коллизионным доменом сети всегда только из одной точки и, что особенно важно для реактивной диагностики, не имеет возможности производить генерацию тестового трафика. В результате если не все оборудование имеет встроенные агенты, то часть ошибок канального уровня в домене сети может не фиксироваться.

С точки зрения реактивной диагностики, т. е. возможности быстрой локализации дефектов в сети, применение анализаторов сетевых протоколов оказывается предпочтительным. Они представляют собой значительно более мощное средство по сравнению со средствами мониторинга сети, так как лишены всех перечисленных выше недостатков. Именно возможность эффективного проведения реактивной диагностики является сегодня актуальной задачей для администраторов сетей Принцип работы анализатора протоколов отличается от принципа работы средства мониторинга сети. Анализатор сетевых протоколов исследует весь проходящий мимо него сетевой трафик. Локальные сети по своей природе являются широковещательными, т. е. каждый кадр от любой станции в пределах коллизионного домена видят все станции этого домена сети. Подключая анализатор к любой точке коллизионного домена сети, вы будете видеть весь трафик в этом домене.

Анализаторы протоколов предоставляют возможность собирать данные о работе протоколов всех уровней сети и, в большинстве случаев, способны производить генерацию тестового трафика в сеть. Имея большой буфер для сбора пакетов, анализаторы протоколов позволяют быстро локализовать причину сбоя в сети: например, обнаружить факт перегрузки конкретного сервера, бесследное исчезновение пакетов транспортного уровня на неисправных сетевых платах, коммутаторах и маршрутизаторах, IP-пакеты с неправильной контрольной суммой, дубликаты IP-адресов и многое другое.

Анализаторы протоколов можно разделить на две категории: программные и аппаратные (или программно-аппаратные). Программный анализатор — это программа, которая устанавливается на компьютер с обычной сетевой платой. Анализатор протоколов переводит сетевую плату компьютера в режим приема всех пакетов (promiscous mode). Примерами программных анализаторов протоколов являются Observer и Distributed Observer компании Network Instruments, NetXray компании Network Associates, LANalyzer for Windows компании Novell и многие другие.

Использование всевозможных методов тестирования и диагностирования компьютерных сетей позволяет своевременно выявить ошибки в работе сети, что позволит значительно повысить эффективность работы компьютерных сетей, а также увеличить эксплуатационный срок.

Литература

1. Скотт Хогдал Дж. Анализ и диагностика компьютерных сетей – М: Лори, 2001 -353 с.
2. Моисеев А.Л., Шаров В.В., Моисеева Р.Р., Зацаринная Ю.Н. Автоматизированная система контроля электрических параметров питания узлов компьютерных сетей// Вестник Казанского технологического университета. – 2013. – №11 – С. 240-242.
3. Староверова Н.А., Фадхкал З. Анализ существующих методов оценки рисков корпоративных информационных систем /Н.А. Староверова// Вестник Казанского технологического университета. – 2013. – №9 – С. 282-288.

© **А. Л. Моисеев –** асп. каф. информатики и информационно-управляющих систем КГЭУ, leha.mos@mail.ru; **Р. Р. Моисеева –** асс. каф. электрических станций КГЭУ, milawka-86@mail.ru; **В. В. Шаров** - канд. тех. наук, доц. информатики и информационно-управляющих систем КГЭУ, shw24@mail.ru; **Ю. Н. Зацаринная** - канд. тех. наук, доц. каф. электрических станций КГЭУ, доц. каф. автоматизированных систем сбора и обработки информации КНИТУ, zac_jul@mail.ru.