



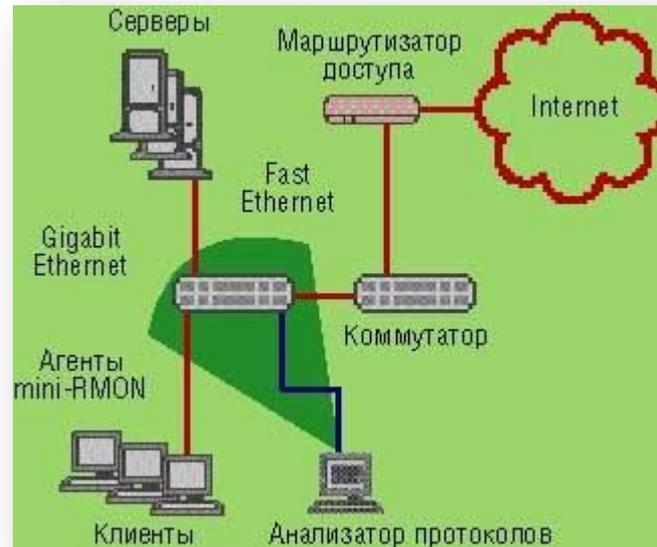
☞ +И



☞ 1 = H



- ▶ При диагностировании локальных сетей более длительным и трудоемким является процесс выявления **скрытых дефектов оборудования и программного обеспечения** (далее – ПО), а также оценка качества архитектурного решения сети.



Скрытые дефекты – это такие дефекты, которые проявляются нерегулярно.

Они имеют особенность проявляться в самые неподходящие моменты.

Пока сеть невелика, скрытые дефекты проявляются редко и на них не обращают особого внимания.

При расширении сети и увеличении ее загруженности вероятность проявления скрытых дефектов растет.

Существуют два основных подхода к выявлению скрытых дефектов и оценке качества архитектуры локальной сети:

- ▶ **пассивная диагностика**
- ▶ **стрессовое тестирование**

- ▶ **Метод пассивной диагностики** состоит в постоянном наблюдении за состоянием сети и регистрации изменений в ее поведении.
- ▶ Он основан на использовании специальных средств пассивного наблюдения за работой сети: анализаторов протоколов или программ на основе протокола SNMP.
- ▶ Этот метод получил очень широкое распространение, и сегодня уже существуют диагностические средства, содержащие встроенную экспертную систему, которая упрощает процесс диагностики.

- ▶ **Метод стрессового тестирования** состоит в создании в сети большой нагрузки и проверке ее работоспособности в этих экстремальных условиях.
- ▶ Метод стрессового тестирования дополняет метод пассивной диагностики.
- ▶ Он позволяет проверить сеть в экстремальных условиях эксплуатации и построить "систему координат", облегчающую интерпретацию данных, полученных в результате пассивной диагностики.
- ▶ Обычно метод стрессового тестирования используется на этапе пуско-наладки сети и после существенных модификаций ее архитектуры или топологии.

Организация процесса диагностики сети

- ▶ На качество работы сети значительное влияние оказывает **состояние активного оборудования** (сетевых плат, концентраторов, коммутаторов), **качество оборудования сервера и настройки сетевой операционной системы**. Кроме того, функционирование сети существенно зависит от алгоритмов работы эксплуатируемого в ней прикладного ПО.

- ▶ Основные **причин неудовлетворительной работы ППО** в сети :
 - повреждения кабельной системы
 - дефекты активного оборудования
 - перегруженность сетевых ресурсов (канала связи и сервера)
 - ошибки самого ППО.

- ▶ Часто одни дефекты сети маскируют другие. Таким образом, чтобы достоверно определить, в чем причина неудовлетворительной работы прикладного ПО, локальную сеть требуется подвергнуть **комплексной диагностике**.

Комплексная диагностика предполагает выполнение следующих этапов (работ):

- ▶ выявление дефектов физического уровня сети: кабельной системы, системы электропитания активного оборудования; наличия шума от внешних источников;
- ▶ измерение текущей загруженности канала связи сети и определение влияния величины загрузки канала связи на время реакции прикладного ПО;
- ▶ измерение числа коллизий в сети и выяснение причин их возникновения;

- ▶ измерение числа ошибок передачи данных на уровне канала связи и выяснение причин их возникновения;
- ▶ выявление дефектов архитектуры сети;
- ▶ измерение текущей загруженности сервера и определение влияния степени его загрузки на время реакции ППО;
- ▶ выявление дефектов ППО, следствием которых является неэффективное использование пропускной способности сервера и сети.

Измерение утилизации сети и установление корреляции между замедлением работы сети

Утилизация канала связи сети – это процент времени, в течение которого канал связи передает сигналы, или иначе – доля пропускной способности канала связи, занимаемой кадрами, коллизиями и помехами.

- ▶ Параметр "Утилизация канала связи" характеризует величину загруженности сети.
- ▶ Канал связи сети является общим сетевым ресурсом, поэтому его загруженность влияет на время реакции ППО. Первоочередная задача состоит в определении наличия взаимозависимости между плохой работой ППО и утилизацией канала связи сети.

Чтобы определить, какова же максимально допустимая утилизация канала связи в данном конкретном случае, рекомендуется следовать приведенным ниже правилам:

- ▶ **Правило 1** Если в сети Ethernet в любой момент времени обмен данными происходит не более чем между двумя компьютерами, то любая сколь угодно высокая утилизация сети является допустимой.
- ▶ **Правило 2** Высокая утилизация канала связи сети только в том случае замедляет работу конкретного ППО, когда именно канал связи является "узким местом" для работы данного конкретного ПО.
- ▶ **Правило 3** Максимально допустимая утилизация канала связи зависит от протяженности сети.
- ▶

Программные средства диагностики

- ▶ Команда NET DIAGS
- ▶ Утилита диагностики Personal NetWare (Network Diagnostics utility) позволяет отслеживать операции сети.
- ▶ Она позволяет просматривать и отслеживать другие группы в сети, сравнивать трафик клиентов и серверов, сравнивать использование серверов, информацию о диске клиента, просматривать информацию о конфигурации, статистику по серверам и клиентам, а также тестировать подключения сервера и клиента.

ScanLink

- ▶ Программа ScanLink предназначена для обработки информации, накопленной прибором в процессе тестирования кабельных сетей. Оно легко устанавливается на любую рабочую станцию. Передача данных из прибора осуществляется через последовательный порт, для чего он комплектуется соответствующим шнуром. Программа способна печатать на принтер табличные отчеты, и отчеты для сертификации сетей. Дополнительно ScanLink имеет возможность сохранять данные в стандарте CSV, для обработки информации в таких программах, как Excel, Access и Word, и создавать произвольные для них шаблоны.

Инструменты диагностики

- ▶ Для разрешения проблем на физическом уровне, а также в электрических или оптических средах передачи данных предназначены кабельные тестеры и такие специализированные инструменты, как временные рефлектометры (Time Domain Reflectometers, TDRs).

- ▶ Традиционным инструментом решения проблем канального, сетевого и транспортного уровней является анализатор протоколов. Недорогие анализаторы обычно создаются на основе серийно выпускаемых портативных ПК с использованием стандартных сетевых карт с поддержкой режима приема всех пакетов.

- ▶ Третьим основным диагностическим инструментом наряду с кабельными тестерами и анализаторами протоколов является зонд или монитор. Эти устройства обычно подключаются к сети на постоянной основе, а не только в случае возникновения проблемы и функционируют в соответствии со спецификациями удаленного мониторинга RMON и RMON II.