Аудит «здоровья» сети своими силами

Методика аудита качества работы ИТ-Инфраструктуры с использованием бесплатного программного продукта ProLAN QuTester Plus.

Есть хорошая английская пословица: «Everything is difficult before it is easy». Всё сложно пока не просто. Аудит «здоровья» ИТ-Инфраструктуры - это сложная задача пока не знаешь, как ее решать. В этой статье мы расскажем о том, как быстро и эффективно локализовать дефектное сетевое оборудование, выявить «узкие места» сети, оценить качество работы арендуемых каналов связи, узнать мнение пользователей о производительности бизнес-приложений и даже измерить индекс «здоровья» своей сети. Предлагаемая методика не только эффективна, но и доступна. Для проведения аудита вам понадобится только бесплатный программный продукт QuTester Plus (www.prolan.ru/qutester) и немного терпения.

Сначала о терминах. Под ИТ-Инфраструктурой будем понимать сетевое оборудование, кабельную систему, серверы, каналы связи и т.п. Термины ИТ-Инфраструктура и сеть употребляются нами как синонимы. Под аудитом «здоровья» ИТ-Инфраструктуры будем понимать измерение и оценку качества работы ИТ-Инфраструктуры во время её эксплуатации.

В этой статье мы не будем рассматривать методику проведения инвентаризации оборудования, построение схемы информационных потоков, оценку информационной безопасности и отказоустойчивости ИТ-Инфраструктуры. Это важные вопросы, но в рамках аудита «здоровья» сети они не решаются.

Целью аудита является получение информации, необходимой и достаточной для оценки текущего «здоровья» ИТ-Инфраструктуры и, если необходимо, выработки аргументированных рекомендаций по его улучшению. Для этого необходимо решить следующие задачи: выявить и локализовать явные дефекты и «узкие места» ИТ-Инфраструктуры (далее – явные проблемы), выявить и локализовать скрытые дефекты ИТ-Инфраструктуры (далее – скрытые проблемы), провести оценку качества работы арендуемых каналов связи.

Явными будем называть дефекты, которые вызывают появление прогнозируемых ошибок. Дефекты, которые таких ошибок не вызывают, будем называть скрытыми. Явными являются, например, дефекты кабельной системы сети, вызывающие ошибки типа CRC error, Alignment error и т.д., фиксируемые сетевым оборудованием. Скрытым является, например, дефект firmware маршрутизатора, вызывающий бесследное исчезновение сетевых пакетов.

Явными «узкими местами» будем называть такие компоненты ИТ-Инфраструктуры, утилизация которых в течение длительных периодов времени составляет 100 %. Скрытыми «узкими местами» будем называть компоненты ИТ-Инфраструктуры, которые ограничивают загруженность других компонент, но при этом загруженность их самих измерить нельзя. Например, если утилизация процессора сервера в течение длительных промежутков времени составляет 100%, то процессор сервера является явным «узким местом» сети. Скрытым «узким местом» является, например, маршрутизатор, процессор которого загружен на 100% (и это ограничивает загрузку канала связи), если маршрутизатор этой информации не предоставляет. Можно привести следующую аналогию. Если в автомобиле глохнет мотор и при этом загорается индикатор бензонасоса, то это явная проблема. Если мотор глохнет, но никакие индикаторы не загораются, то это скрытая проблема.

Выявление явных проблем сети

Методика выявления явных проблем относительно проста. Поскольку явные проблемы всегда «оставляют следы», то чтобы их локализовать, достаточно иметь средство мониторинга, позволяющее «увидеть эти следы». «Увидеть следы» - это найти метрики, значения которых больше или меньше рекомендуемых (пороговых) значений. Это является признаком наличия проблемы.

Если сетевое оборудования поддерживает SNMP, то для его мониторинга чаще всего используют SNMP-консоль (SNMP, Simple Network Management Protocol). Это специальная программа, которая периодически обращается к агенту (SNMP-агенту), встроенному в оборудование, и забирает значения метрик, которые этот агент измеряет. Использование SNMP-консоли позволяет выявить множество явных сетевых проблем. К ним относятся, например, ошибки передачи данных, вызываемые дефектами кабельной системы сети и/или неправильной настройкой коммутаторов (на одном конце линка - full duplex, на другом конце – half duplex). Широковещательные штормы, блокирующие работу портов сетевого устройства. Высокая утилизация портов коммутатора, переполнение таблиц коммутации, утечка памяти на маршрутизаторах и многое другое. Большинство SNMP-консолей можно эффективно использовать также для мониторинга Linux-серверов, периферийного оборудования, источников бесперебойного питания, баз данных и много другого.

Для мониторинга серверов MS Windows обычно используют утилиту MS Performance Monitor или WMI-консоли других производителей (WMI – Windows Management Interface). Подобные средства позволяют выявить большинство явных проблем, связанных с работой Windows-серверов. Чаше всего это высокая утилизация процессоров, низкий процент кэшируемых данных, очереди в дисковой системе, утечка ОЗУ и т.п. Кроме этого, многие бизнес-приложения добавляют свои счетчики в MS Performance Monitor, поэтому с помощью этих средств можно контролировать еще и работу бизнес-приложений.

Если нужно провести аудит «здоровья» небольшой сети (10-50 компьютеров), то возможностей обычного средства мониторинга для этого, как правило, вполне достаточно. Если же необходимо провести аудит сети, состоящей из ста и более компьютеров, то использование обычных средств мониторинга сопряжено с рядом сложностей.

Первой сложностью является необходимость одновременного измерения большого числа метрик. Например, чтобы измерить качество работы сети, состоящей только из одного 48-портового коммутатора, нужно измерить, как минимум, значения 144 метрик (48 метрик – ошибки по портам, 48 метрик – процент широковещательных пакетов, 48 метрик – утилизация портов). Если сеть состоит из пяти таких коммутаторов, то нужно будет измерить уже 720 метрик. Но кроме коммутаторов в сети есть еще серверы, маршрутизаторы, сетевые экраны и другие устройства, качество работы которых нужно измерять. С помощью обычных средств мониторинга это сложно сделать по двум причинам. Во-первых, нужно знать, какие метрики нужно измерять в каждом конкретном случае. Во-вторых, нужно проделать большую работу, чтобы настроить средство мониторинга на автоматическое получение всех этих метрик.

Вторая сложность заключается в том, что значения всех метрик нужно не только получить, но и правильно оценить. Если оценить метрики, характеризующие работу простейшего коммутатора Ethernet относительно несложно, то оценить метрики, характеризующие работу серверов, баз данных, маршрутизаторов, сетевых экранов и т.п. значительно сложнее. Обычно, чем качественнее сетевое оборудование, тем больше информации о себе оно предоставляет. В этом, кстати, одно из различий дорогого и дешевого оборудования. Если дорогой коммутатор позволяет узнать о себе практически все (начиная с исправности вентилятора и заканчивая утилизацией таблицы коммутации),

то дешевый коммутатор в лучшем случае предоставляет информацию об интенсивности трафика и числе ошибок на портах, а иногда и этого не делает.

Для проведения аудита «здоровья» больших сетей нужно использовать специализированный инструментарий. Только в этом случае получение данных, на основе которых можно сделать достоверные выводы о «здоровье» ИТ-Инфраструктуры, является выполнимой задачей. Примером такого инструментария, является бесплатный программный продукт QuTester Plus. Этот продукт отличается от обычных средств мониторинга наличием встроенных Оценочных Тестов (ProLAN-Тестов), позволяющих существенно упростить процесс сбора и оценки метрик «здоровья» ИТ-Инфраструктуры. ProLAN-Тесты - это программы на скриптовом языке, в которых предустановленно, какие метрики и как должны измеряться для оценки качества работы различных компонент сети (коммутаторов, маршрутизаторов, серверов, каналов связи и т.д.), а также пороговые значения для каждой измеряемой метрики. ProLAN-тест является упрощенной экспертной системой, предназначенной для оценки «здоровья» различных компонент ИТ-Инфраструктуры.

Всего компанией ProLAN разработано более 40 ProLAN-Тестов, из них более 20 являются бесплатными продуктами и поставляются в составе QuTester Plus. В данной статье мы будем рассматривать только такие тесты.

Для выявления явных дефектов и «узких мест» ИТ-Инфраструктуры рекомендуется использовать тесты, перечисленные в Таблице 1. Эти тесты мы называем пассивными, т.к. они не измеряют значения метрик, а получают их от контролируемых устройств.

Таблица 1.

Объекты аудита	**Рекомендуемые ProLAN-тесты**
Коммутаторы и любое сетевое оборудование, поддерживающее SNMP MIB II (маршрутизаторы, сетевые карты, сетевые экраны, Linux-серверы и т.п.)	Профессиональный тест оценки «здоровья» коммутаторов, поддерживающих MIB II.
Коммутаторы	Профессиональный тест оценки «здоровья» коммутаторов, поддерживающих MIB II. Тест контроля утилизации таблиц коммутации (802.1D)
Серверы MS Windows	Тест оценки «здоровья» сервера NT4/2000/XP. Тест оценки «здоровья» сервера MS SQL. Тест оценки «здоровья» сервера MS DNS.
Маршрутизаторы Cisco Systems	Тест оценки «здоровья» маршрутизаторов Cisco.

Описания этих тестов можно найти на сайте компании ProLAN в разделе ProLAN-Тесты или в бесплатно распространяемом справочнике Test IT; см. раздел: «За Качество IP-Сетей». Методику работы с оценочными тестами рассмотрим на примере использования профессионального теста оценки «здоровья» коммутаторов, поддерживающих MIB II (см. Рисунок 1).

На любой (не обязательно выделенный) компьютер сети установите программный пакет QuTester Plus и стартуйте его в режиме ProLAN-Administrator (Demo). Из предложенного списка запустите профессиональный тест оценки «здоровья» коммутаторов, поддерживающих MIB II. Этот тест находится в группе, которая называется: «Тесты

оценки здоровья оборудования, поддерживающего SNMP». Вам будет предложено задать IP-адрес тестируемого коммутатора и пароль (community string) для доступа по чтению. Дальше все делается автоматически. Тест сам подключится к коммутатору, определит его модель, число портов, производительность портов, проверит, поддерживает ли коммутатор MIB II и т.п. После окончания проверок тест начнет получать SNMP-данные, характеризующие работу сети (число принятых байт, число переданных байт, число широковещательных пакетов, число ошибок и т.д.).

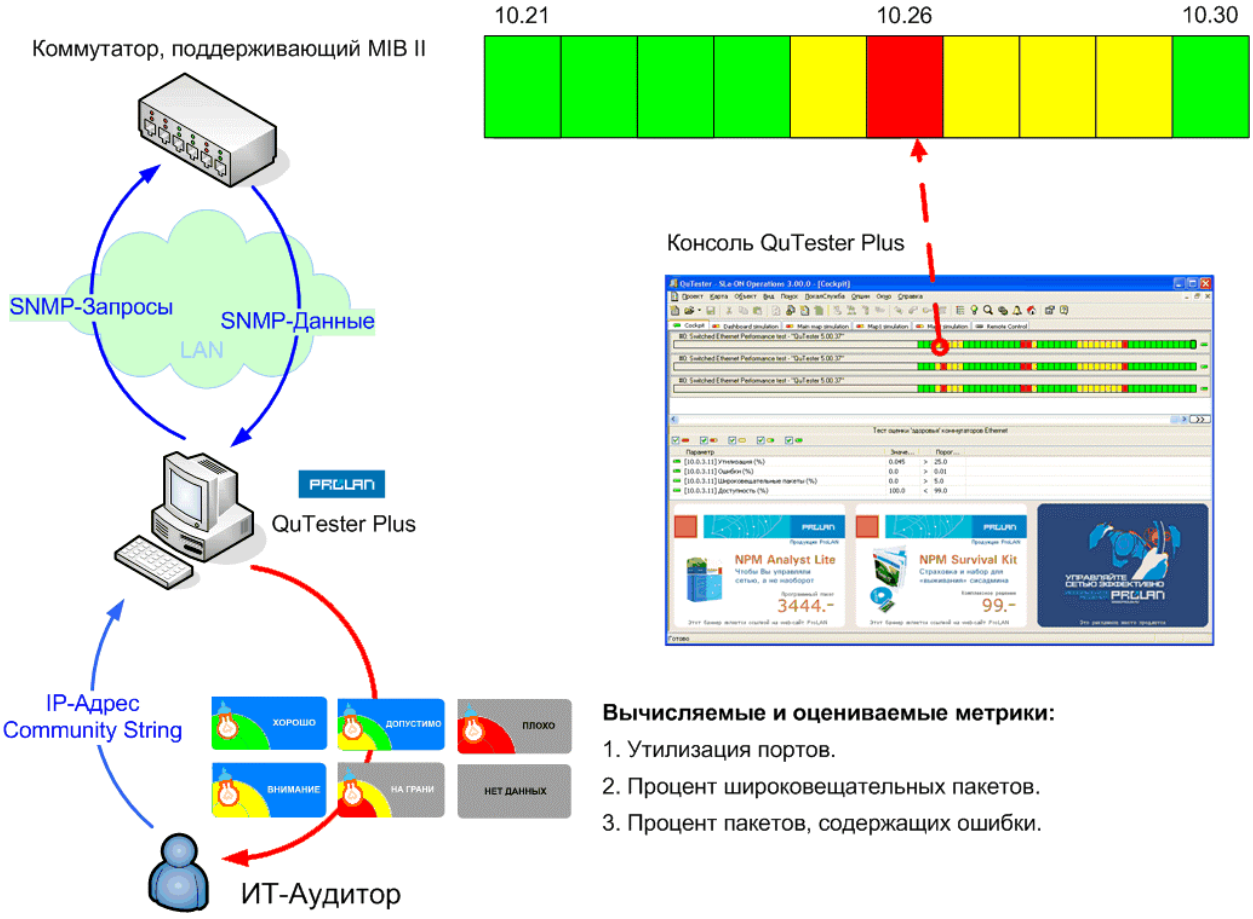

Рисунок 1. Тест оценки «здоровья» коммутаторов, поддерживающих MIB II.

Каждую минуту для каждого порта коммутатора тест будет автоматически вычислять значения трех метрик: утилизация порта, процент широковещательных пакетов, процент ошибок. Все эти метрики каждую минуту будут автоматически сравниваться с предустановленными пороговыми значениями, и оцениваться по пятибалльной шкале (пороговые значения можно изменять). В результате каждую минуту тест будет формировать набор цветных индикаторов, характеризующих текущее «здоровье» сети. Наихудшее значение индикатора выводится на ленточную диаграмму, которая называется светофором. Если ни одна метрика в течение данной минуты не превысила пороговое значение, то светофор будет зеленым. Если хотя бы одна метрика превысит пороговое значение, то светофор изменит свой цвет. Под светофором отображается его расшифровка, представляющая собой список метрик, из которых состоит светофор и результаты их оценки (см. Рисунок 2).

Поскольку тест должен работать в течение длительного периода времени, вам следует настроить систему оповещения о сбоях. Если это сделать, то тест будет автоматически посылать электронные письма всякий раз, когда цвет светофора изменится. При этом можно задать цвета светофоров и сколько раз подряд такое изменение должно произойти, прежде чем будет отправлено письмо. В письме содержится информация о том, какой светофор изменил свой цвет, когда это произошло, какие метрики при этом

изменились и насколько. Каждое такое письмо является тем самым «следом», который оставляет явный дефект или «узкое место» сети. Множество таких писем будем называть *логом явных проблем*.

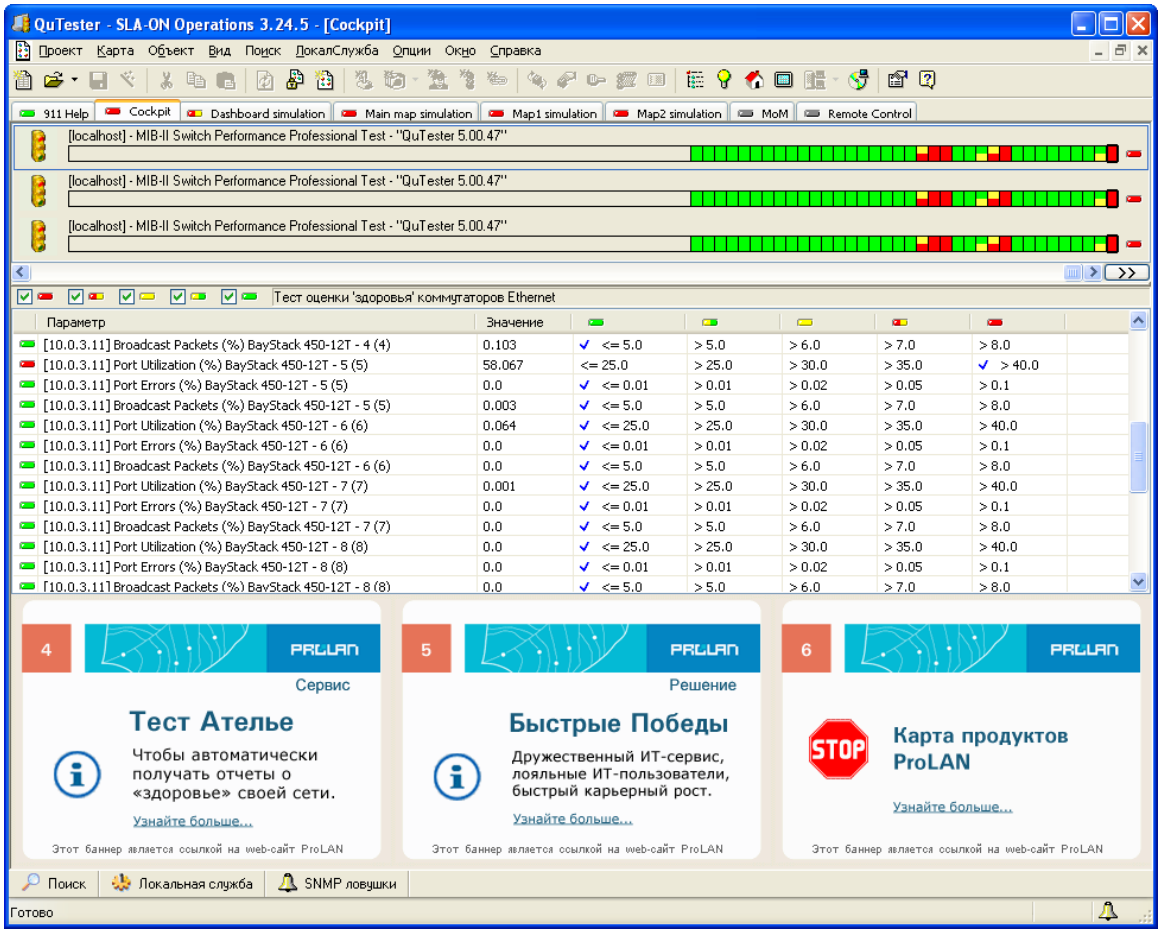

Рисунок 2 . Отображение светофора, характеризующего «здоровье» коммутируемой сети.

Анализировать лог явных дефектов не сложно, т.к. в описании каждой метрики, как правило, содержится информация о возможных причинах дефекта. Например, причинами большого числа ошибок передачи данных в 100% коммутируемой сети обычно являются: дефекты кабельной системы, дефекты приемо-передающего оборудования, неправильная настройка портов коммутаторов (на одном конце линка - full duplex, на другом конце – half duplex). Причиной высокой утилизации порта может быть неудачная топология сети, использование в сети большого числа ресурсоемких приложений (передача живого видео), неправильная настройка порта коммутатора. Наличие большого числа широковещательных пакетов, как правило, объясняется использованием в сети соответствующих приложений. Если что-то из перечисленного не является, по вашему мнению, проблемой, то вы можете уменьшить число оцениваемых метрик (например, не оценивать процент широковещательных пакетов), или изменить пороговые значения.

Выявление скрытых проблем сети

Если явных проблем не выявлено, а пользователи продолжают жаловаться на плохую работу бизнес-приложений, то это означает одно из двух. Либо вам не удалось выявить все явные проблемы, либо в сети есть скрытые проблемы. Скрытая проблема – это то, что вызывает сбои или замедление работы бизнес-приложений, но при этом не сопровождается появлением прогнозируемых ошибок. Локализовать скрытую проблему означает найти компонент ИТ-Инфраструктуры (коммутатор, дисковый контроллер,

драйвер сетевой карты и т.п.), который негативно влияет на производительность или доступность сети.

Найти можно только то, что можно увидеть. Поскольку скрытые проблемы не оставляют «обычных следов», необходимо найти другие способы определения их наличия. Признаками наличия скрытых проблем обычно считаются низкие значения скорости выполнения сетевых операций и/или большое число повторных передач на транспортном уровне сети (TCP). Признаки первого типа обычно используются в активных (генерирующих трафик) системах мониторинга. Признаки второго типа – в анализаторах сетевых протоколов. Пакет QuTester Plus относится к категории активных систем мониторинга.

Измерение скорости выполнения сетевых операций является очень эффективным способом определить наличие скрытой проблемы. Например, если коммутатор «глотает» сетевые пакеты, то это обязательно скажется на скорости выполнения файловых операций. Если «тормозит» дисковая система сервера, то это обязательно скажется на скорости выполнения SQL-запросов или хранимых процедур. Если периодически «зависает» из-за перегрева маршрутизатор, то это обязательно скажется на доступности всех приложений, трафик которых проходит через этот маршрутизатор. Поэтому для выявления скрытых проблем достаточно иметь средство, позволяющее измерять скорость выполнения различных сетевых операций. Такими средствами являются, например, активные оценочные тесты, представленные в таблице 2. Эти тесты мы называем активными, т.к. они сами измеряют значения метрик, характеризующих «здоровье» сети.

Таблица 2.

Измеряемые метрики	**Рекомендуемые ProLAN-тесты**
Скорость и доступность сети при выполнении файловых операций.	Базовый тест оценки производительности файлового сервиса сети. Тест оценки производительности файлового сервиса для программ 1С.
Скорость и доступность сети при выполнении SQL-запросов и/или хранимых процедур.	Базовый SQL-тест

Технологию выявления скрытых проблем продемонстрируем на примере использования теста оценки производительности файлового сервиса (см. Рисунок 3). Установите QuTester Plus на выделенный компьютер и подключите его к тому коммутатору, к которому подключены компьютеры пользователей сети, часто жалующиеся на плохую работу бизнес-приложения. Запустите тест оценки файлового сервиса сети и настройте его на выполнение файловых операций с сервером, где установлено плохо работающее бизнес-приложение. Укажите UNC путь до сервера, тип сети, тип ОС на сервере, стартуйте тест. Тест начнет автоматически выполнять файловые операции и измерять скорость их выполнения (скорость чтения, скорость записи, доступность). Каждую минуту тест будет выполнять операции чтения/записи блоков данных размером 2 KB из файла размером 16 KB; 50% составляют операции чтения, 50%-операции записи. Интенсивность выполнения файловых операций составляет ~ 50 Кбайт/с, что соответствует ~ 0.2% дополнительной утилизации сети Fast Ethernet FD. Размер файла полностью попадает в кэш память сервера, поэтому скорость выполнения файловых операций будет зависеть в основном от качества канала передачи данных между компьютером и сервером (производительность дисковой системы сервера на скорость практически не влияет).

Если какой-то коммутатор, расположенный в канале передачи данных между компьютером и сервером, перегревшись, начинает «глотать» сетевые пакеты, то в те

моменты времени, когда это происходит, скорость выполнения сетевых операций значительно снижается. Поскольку файловые операции выполняются непрерывно, неадекватная работа сети может быть быстро обнаружена. Если в канале передачи данных расположено несколько коммутаторов, то чтобы локализовать «злоумышленника», достаточно запустить тест на компьютере, подключенном к другому коммутатору (который ближе к серверу). Если в этом случае скорость будет нормальной, то виноват первый коммутатор. Если нет, то второй коммутатор или сетевая система сервера. Таким образом, перемещая тест по сети, вы сможете быстро локализовать все дефектные компоненты ИТ-Инфраструктуры или убедиться в их отсутствии.

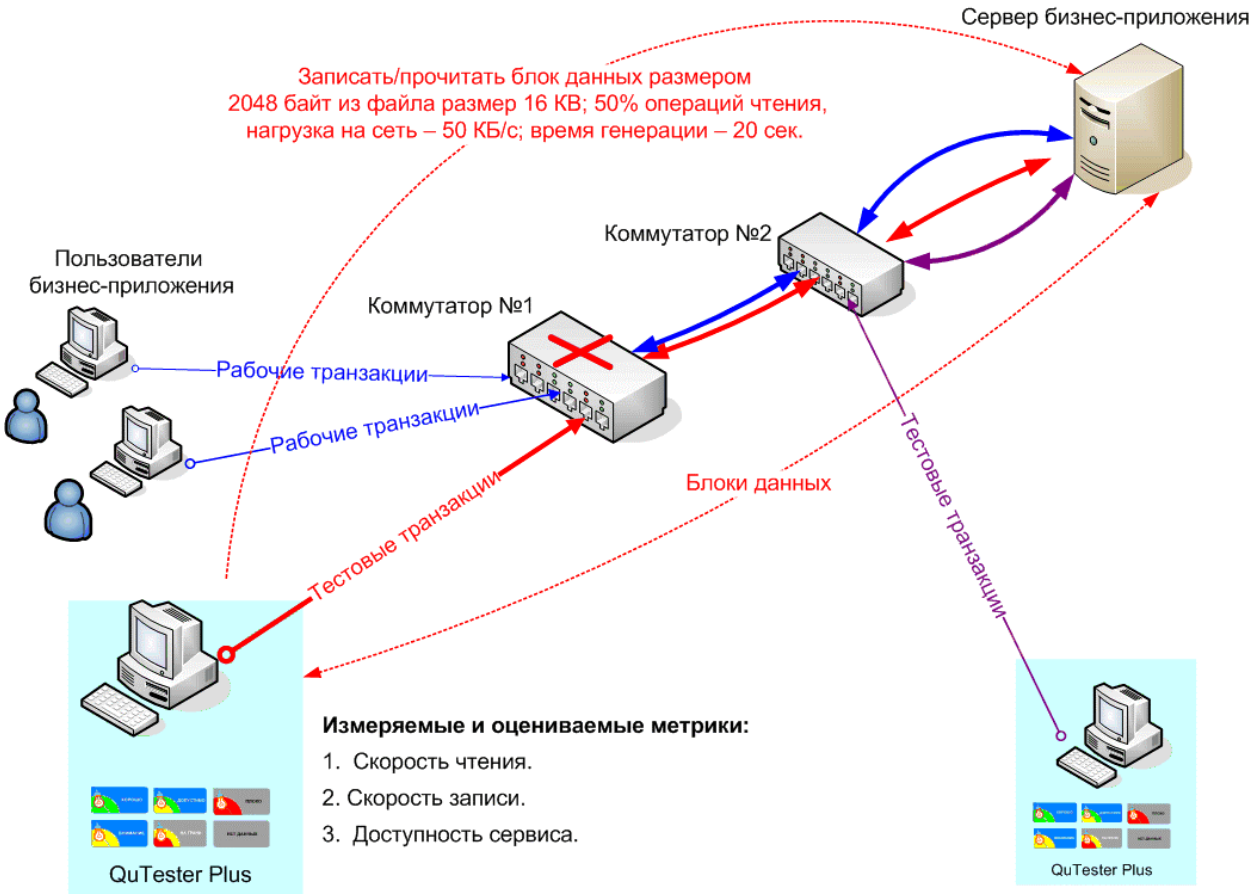

Рисунок 3. Выявление скрытых дефектов.

При анализе результатов активных тестов нужно понимать, что при отсутствии явных проблем скорость выполнения сетевых операций может снижаться не только из-за наличия скрытых проблем, но и вследствие повышения загруженности сети. Поэтому активные сетевые тесты рекомендуется выполнять одновременно с пассивными тестами, используемыми для выявления явных проблем. Чтобы избежать влияния пассивных тестов на работу активных тестов, желательно, чтобы активные и пассивные тесты выполнялись на разных компьютерах сети.

Поскольку скорость выполнения файловых операций автоматически оценивается по пятибалльной шкале, то, настроив систему оповещения, вы будете автоматически получать электронные письма всякий раз, когда скорость выполнения файловых операций или доступность файлового сервиса будут ниже установленного порога. В письмах будет содержаться информация о том, какой светофор изменил свой цвет, когда это произошло, какие метрики при этом изменились и насколько. Множество этих электронных писем будем называть *логом низкой производительности сети*.

Градуировка оценочных тестов

Достоверность оценочных тестов сильно зависит от правильности установки пороговых значений. Несмотря на то, что предустановленные пороговые значения в большинстве случаев позволяют адекватно оценить «здоровье» сети, полностью полагаться на них не рекомендуется. В наибольшей степени это относится к пороговым значениям активных тестов, т.к. скорость выполнения сетевых операций очень сильно зависит от архитектуры и топологии сети. Чтобы гарантировано выявить все скрытые проблемы сети, необходимо градуировать оценочные тесты, т.е. определить пороговые значения именно для вашей сети. Это можно сделать разными способами, с разной точностью. Ниже мы расскажем о наиболее точном, хотя и не самом простом способе. Он заключается в сопоставлении друг с другом метрик, характеризующих скорость сети, и метрик, характеризующих удовлетворенность пользователей бизнес-приложений качеством их работы. Этот метод называется: «Найти Точку Опоры».

В качестве метрики, характеризующей удовлетворенность пользователей, предлагаем использовать метрику СОКС (Субъективная Оценка Качества Сервиса), которая вычисляется следующим образом. Если в данный момент времени (по умолчанию – одна минута) существует хотя бы один пользователь, который недоволен производительностью бизнес-приложения, то значение СОКС принимает значение 0, если таких пользователей нет, то значение СОКС равно единице. Измерить СОКС можно следующим способом.

Из числа пользователей бизнес-приложения сформируйте фокус группу, в состав которой должны войти наиболее опытные, и при этом, наиболее активные пользователи (~ 10%-20% от общего числа пользователей). Для этого вам может потребоваться помощь руководителя ИТ-Службы. Обычно руководители поддерживают такие инициативы, т.к. они повышают престиж ИТ-службы. (Вы изучаете мнение пользователей, целью которого является улучшение работы ИТ-Инфраструктуры.)

Установите на компьютеры членов фокус группы 30-ти дневную версию программы ProLAN HelpMe, входящую в дистрибутив QuTester Plus. Попросите этих пользователей сделать следующее. Как только они обнаружат замедление в работе бизнес-приложения, которое длится дольше психологически допустимого порога (например, 3-х секунд), они должны нажать определенную комбинацию клавиш на своем компьютере, например, Ctrl+F2+F2. В этом случае программа HelpMe автоматически отправит SNMP-Трап, который будет принят программой SLA-ON Operations, входящей в состав QuTester Plus. Если в данный момент времени (данную минуту) был получен хотя бы один такой SNMP-трап, то в данную минуту значение СОКС равно нулю. Если SNMP-трапов получено не было, то единице.

Градуировка тестов – это такой подбор пороговых значений, чтобы каждому нулевому значению СОКС соответствовал красный цвет светофора метрики, характеризующей скорость сети. Если большинство нулевых значений СОКС попали в красную зону значений скорости сети, то пороговые значения подобраны правильно. Если это не удается сделать, то это означает одно из трех. Либо пока неправильно заданы пороговые значения, и нужно продолжить подбор. Либо неправильно выбрана сетевая операция, скорость которой измеряется тестом. Либо проблема находится вне ИТ-Инфраструктуры, например, это дефект самого приложения. В последнем случае вместо скорости работы сети нужно найти метрику, характеризующую работу приложения и коррелирующую с жалобами пользователей. Это может быть, например, число одновременно работающих пользователей или запуск определенной хранимой процедуры на сервере.

Подбор пороговых значений можно автоматизировать, но для этого требуются специальный инструментарий, который не входит в состав бесплатного продукта

QuTester Plus. Подробнее о технологии подбора пороговых значений можно прочесть в документе: «Найти Точку Опоры».

Оценка качества арендуемых каналов связи

Для оценки качества арендуемых каналов можно использовать генераторы трафика (одновременно измеряющие его качество) и анализаторы сетевых протоколов, захватывающие и оценивающие качество рабочего трафика. Достоинствами генераторов трафика являются высокая точность результатов и возможность оценивать качество каналов связи при отсутствии рабочего трафика. Недостатком – создание дополнительной нагрузки на сеть. Достоинством анализатора протоколов является отсутствие дополнительного трафика, а недостатками – невозможность оценивать качество сети при отсутствии рабочего трафика и плохая масштабируемость. Поэтому для мониторинга сети чаще используют анализаторы сетевых протоколов, а для аудита – генераторы трафика.

Для оценки качества каналов связи «точка-точка» обычно используют четыре метрики. Задержку передачи данных (delay), которая может быть круговой (round trip) или однонаправленной (one way). Вариацию задержки (jitter). Процент потерянных пакетов (packet loss). Доступность (availability). Качество Internet-каналов обычно оценивают с помощью двух метрик: доступность и пропускная способностью на уровне HTTP или FTP. Технология измерения этих метрик определяется видом канала (точка-точка или Internet-канал) и типом каналообразующего оборудования на стороне клиента; см. Рисунок 4. В таблице 3 приведены ProLAN-тесты, которые рекомендуется использовать в каждом из этих случаев.

Таблица 3.

Вид канала	Тип оборудования	Рекомендуемые ProLAN-тесты
«точка-точка»	Cisco Systems	Тесты оценки качества IP-канала на основе Cisco SAA (IP SLA).
«точка-точка»	Любое	Тесты производительности TCP-канала Тесты производительности UDP-канала
Internet	Любое	Базовый тест производительности WEB-серверов

Проще всего оценить качество канала связи «точка-точка», на обоих концах которого установлены маршрутизаторы Cisco Systems. Это объясняется поддержкой операционной системой Cisco (IOS) технологии SAA (новое название - IP SLA). Суть этой технологии в том, что маршрутизатор Cisco можно настроить на генерацию тестового трафика, который будет «подмешиваться» в рабочий трафик. При этом маршрутизатор, который передает тестовый трафик, одновременно оценивает его качество (вычисляет значения метрик delay, jitter, packet loss и т.д.).

Настройку и запуск SAA-тестов можно делать вручную, из командной строки. Но это не очень удобно. Кроме этого, результаты измерений нужно оценивать. Поэтому компания ProLAN разработала набор оценочных тестов, позволяющих автоматизировать этот процесс. Эти тесты объединены в группу: «Тесты оценки качества IP-канала на основе Cisco SAA (IP SLA)». Каждый тест представляет собой специальную SNMP-консоль, предназначенную для тестирования каналов связи на базе оборудования Cisco. Тесты различаются типом генерируемого трафика (эмулируется голосовой трафик с различным типом кодеков) и пороговыми значениями. Поэтому, чтобы провести аудит канала связи от вас потребуется только разрешить на маршрутизаторах поддержку SAA, запустить соответствующий тест и указать параметры маршрутизаторов, образующих канал связи (IP-адреса, community string.). Все остальное тест сделает сам аналогично тому, как это делает профессиональный тест оценки здоровья коммутаторов, описанный выше. В результате вы получите набор индикаторов и светофоров, характеризующих качество арендуемого канала связи. Тест должен работать долго, поэтому настройте оповещение

о сбоях. В результате вы получите *лог сбоев арендуемого канала связи*, который может быть частью *лога низкой производительности сети*.

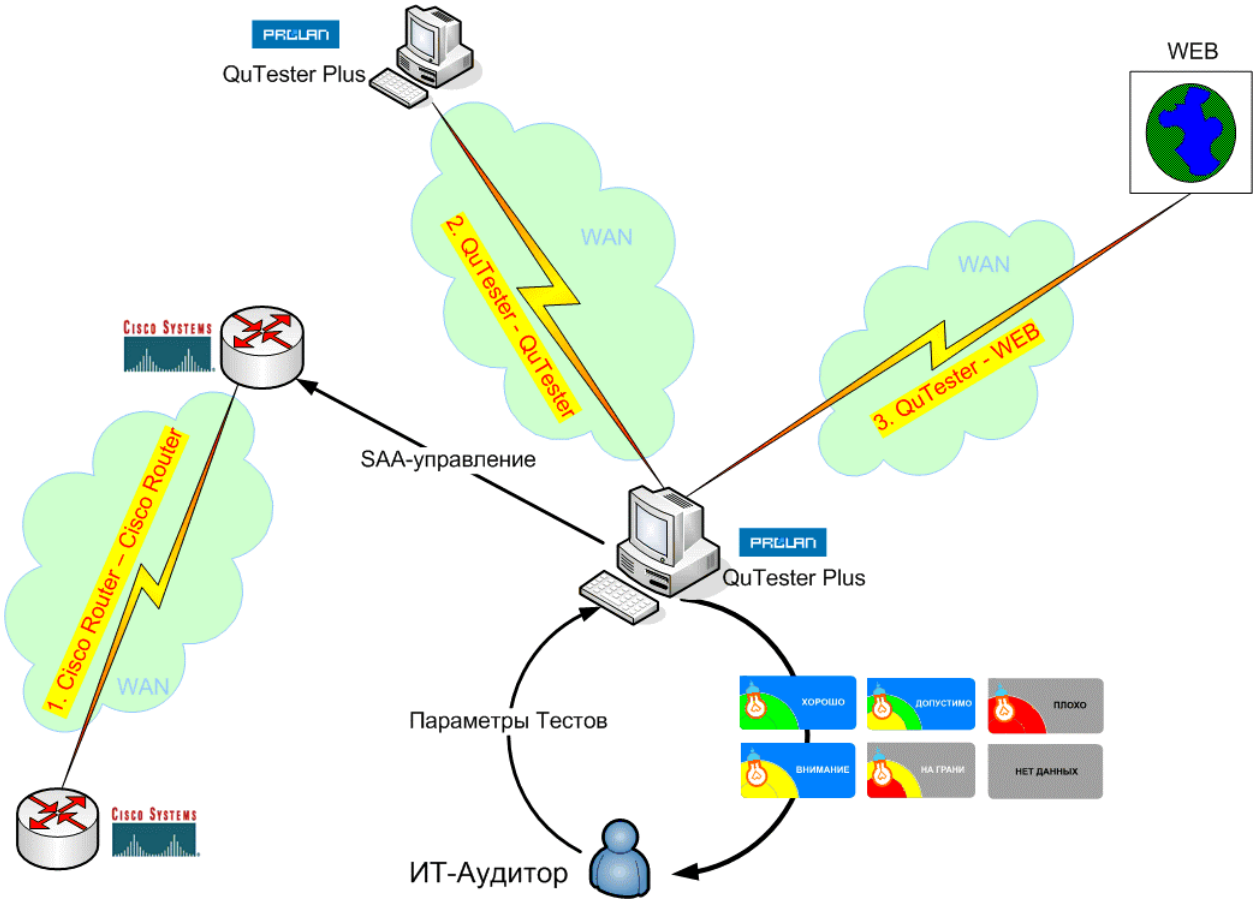

Рисунок 4. Оценка качества арендуемых каналов связи.

Оценка качества каналов связи «точка-точка», построенных на основе оборудования других производителей (не Cisco Systems), практически не отличается от описанной выше. Отличие заключается только в том, что тестовый трафик создается не самими маршрутизаторами, а программой QuTester Plus, которая для этого должна быть установлена на обеих сторонах тестируемого канала связи. При этом можно использовать тесты двух категорий: «Тесты производительности TCP-канала» и «Тесты производительности UDP-канала». Тесты первой категории эмулируют трафик бизнес-приложений (MS Axapta, Citrix и т.п.). Тесты второй категории эмулируют голосовой трафик.

При оценке качества каналов «точка-точка», как правило, не нужно производить градуировку оценочных тестов. Это объясняется тем, что пороговые значения, используемые в этих тестах, основаны на рекомендациях TIA/EIA, рекомендациях Microsoft, Citrix, и даже на рекомендациях руководящих документов Министерства информационных технологий и связи Российской Федерации. Все эти документы регламентируют, каковы должны быть значения метрик (delay, jitter, packet loss и др.) для хорошей работы различных приложений. Особенно хорошо эти вопросы проработаны для голосовых приложений (VoIP).

Если вы планируете обсудить полученные результаты с оператором связи, то их лучше всего представить в виде набора Базовых Линий: «Типовой Рабочий День». Подробнее об этом читайте ниже в главе: «Документирование здоровья сети». При этом следует понимать, что использовать полученные результаты в качестве свидетельства невыполнения оператором связи своих обязательств, вам, скорое всего, не удастся.

Сегодня большинство операторов связи не включают в Соглашение об Уровне Обслуживания гарантируемые значения приведенных выше метрик качества.

Методика оценки качества Internet-канала отличается от методики оценки качества канала «точка-точка». Поскольку на стороне Internet-провайдера нельзя установить SAA-ответчик или программу QuTester Plus, то невозможно измерить значения задержки, вариации задержки, числа потерянных пакетов и т.п. Поэтому нужно измерять «производную» от этих метрик, например, скорость загрузки web-страниц. Эта задача решается с помощью базового теста производительности web-серверов, который автоматически загружает web-страницы и измеряет скорость их загрузки. Адреса web-страниц задаются в параметрах теста.

Зная размер web-страницы и время ее загрузки, можно легко измерить скорость Internet-канала на уровне HTTP. Основной интерес представляет не абсолютное значения скорости, а динамика ее изменения. Например, насколько скорость днем ниже скорости ночью, как скорость в рабочие дни отличается от скорости в выходные дни и т.п.

Документирование «здоровья» сети

Прежде чем документировать результаты аудита и приступить к выработке рекомендаций, нужно убедиться в полноте собранных данных и правильности их оценки. Сделать это можно следующим образом. Сопоставьте *лог явных проблем* и *лог низкой производительности сети* со значениями метрики СОКС. Если время появления красных значений светофоров в логах совпадает по времени с нулевыми значениями СОКС, то данные полны и оценены правильно. Это будет означать, что установлено соответствие между жалобами пользователей бизнес-приложений и «здоровьем» сети. Если полного соответствия не будет, то результаты недостоверны. Степень достоверности легко оценить в процентах.

В ходе аудита собирается множество данных, характеризующих «здоровье» сети. Чтобы превратить эти данные в информацию, их нужно статистически обработать и представить в удобном для анализа виде. Таким видом является Базовая Линия. Обычно используют три вида Базовых Линий. Простейшей Базовой Линией является среднее арифметическое значение метрики за все время аудита. Как и средняя температура по больнице, такая оценка мало информативна. Вторым видом Базовой Линии является диапазон наиболее вероятных значений метрики за все время аудита. В данном случае вычисляется не среднее арифметическое значение, а перцентиль, например, перцентиль 75 (диапазон наиболее вероятных значений с вероятностью 75%). Этот показатель более информативен и мы рекомендуем его использовать для не очень значимых метрик.

Наибольший интерес для анализа представляет Базовая Линия, которая называется: «Типовой Рабочий День». Она представляет собой множество наиболее вероятных значений метрики в каждый момент времени (минуту ,15 минут и т.д.) в течение рабочего дня. Используя Типовой Рабочий День, можно легко выявить причинно-следственные связи в работе ИТ-Инфраструктуры, оценить «запас устойчивости» сети и многое другое. Кроме этого, Типовой Рабочий День используется в качестве параметра ProLAN-тестов, предназначенных для обнаружения аномалий в работе сети, например, в тесте обнаружения аномалий в работе коммутируемой сети. Обычно Типовой Рабочий День рассчитывают для наиболее значимых метрик, например, утилизации сервера, утилизации магистрального канала связи и т.п.

Чтобы построить Типовой Рабочий День, данные, полученные в понедельник, нужно «статистически наложить» на данные вторника, среды и т.д. В результате будут получены два графика, «перцентиль >» и «перцентиль <», образующих «вероятностную трубу», характеризующую наиболее вероятные значения метрики в каждый момент времени в течение дня. К сожалению, статистическая обработка данных требует наличия

специального инструментария, который не входит в состав бесплатного продукта QuTester Plus.

Для макроанализа «здоровья» сети очень удобно иметь одну интегральную оценку «здоровья» сети. Такую оценку мы называем индексом «здоровья» сети и рассчитываем следующим образом. Это доля времени, выраженная в процентах, в течение которого в *логе явных проблем* и *логе низкой производительности сети* не фиксировались красные значения светофоров. При этом важно, чтобы данные, на основе которых вычисляется индекс «здоровья» сети были полны и достоверны (в соответствии с описанным выше алгоритмом). Например, если в течение рабочего дня (10 часов или 600 минут) было зафиксировано 90 красных светофоров, то индекс «здоровья» сети составит: 100% - 90/600*100% = 85%. Индекс «здоровья» сети удобно использовать не только для оценки текущего «здоровья» сети, но и для оценки эффективности проведенной модернизации сети. Например, сравнив значения индекса «здоровья» сети до и после замены сервера, можно легко оценить эффективность сделанной замены.

Часто задаваемые вопросы

Может ли процесс сбора данных о «здоровье» сети негативно отразиться на работе пользователей сети?
В этом вопросе содержатся два вопроса. Первый вопрос – может ли дополнительный трафик, создаваемый тестами, повлиять на работу пользователей сети. Интенсивность создаваемого трафика регулируется параметрами теста, поэтому, если параметры заданы правильно, то не может. Даже если используются параметры по умолчанию и данные собираются с интервалом усреднения – 1 минута, то трафик настолько мал, что обычно он не оказывает заметного влияние на работу пользователей сети.

Второй вопрос – может ли выполнение, например, SNMP-запросов негативно повлиять на работу сетевого оборудования. Да, но только в том случае, если в оборудовании есть дефект. Мы иногда встречаемся с подобными случаями, и обычно проблема решается заменой firmware.

Можно ли ограничиться оценкой «здоровья» только некоторых, наиболее значимых компонент сети?
Нет, этого делать не следует, т.к. это может привести к неверным выводам о «здоровье» сети. Выборочный аудит сети, когда оцениваются не все компоненты ИТ-Инфраструктуры или измеряются не все метрики, является распространенной ошибкой. Например, часто оценивается работа только центральных серверов и сетевого оборудования. Это неправильно, т.к. дефект порта периферийного коммутатора или дефект сетевой карты в компьютере пользователя, работающего с каким-то приложением, могут вызвать замедление работы всех пользователей этого приложения. (Пользователи ждут, пока освободится критический ресурс, а он долго не освобождается из-за большого числа повторных передач, вызванных дефектом.) Это, в свою очередь, может быть причиной низкой загруженности сетевых ресурсов. Поэтому может показаться, что в сети проблем нет и в медленной работе пользователей «виновато» само приложение. На самом же деле это может быть не так.

Сколько времени должны собираться данные о «здоровье» сети для получения достоверных результатов?
Для достоверного выявления сетевых проблем сбор данных должен производиться в течение, минимум, 5 дней. Часто «здоровье» сети измеряется только в течение одного рабочего дня. Это неправильно, т.к. в течение одного дня обычно проявляются только наиболее заметные проблемы, например дефекты кабельной системы сети. Более сложные проблемы, например, связанные с температурным режимом работы оборудования, широковещательными штормами, переполнением ОЗУ сетевых устройств за один день могут не проявится.

Пользователи жалуются на плохую работу бизнес-приложений. Поможет ли нам проведение аудита определить причину проблемы?
Да, но только в том случае, если причиной проблемы являются дефекты или «узкие места» ИТ-Инфраструктуры. Если причина в плохом качестве бизнес-приложения, то вы сможете аргументировано доказать это программистам, что часто эквивалентно решению проблемы.

Можно ли с помощь аудита проверить кабельную систему сети?
Можно убедиться, что кабельная система исправна. Например, если в ходе аудита не будет зафиксировано ошибок передачи данных, то это именно так. Если же в ходе аудита будет выявлено наличие ошибок, то установить их причину будет сложно. Поэтому для проверки кабельной системы рекомендуется использовать специальные приборы – кабельные сканеры.

Каковы основные ограничения бесплатного продукта QuTester Plus?
Основных ограничений, важных для аудита, два. Первое ограничение - вы не сможете представить результаты аудита в виде красивых отчетов, содержащих Базовые Линии, таблицы, графики и т.п. Если аудит делается для себя, то, как правило, это и не нужно. Второе ограничение – аудит займет больше времени, чем при использовании наших коммерческих продуктов, и трудоемкость работ будет выше. Это объясняется тем, что QuTester Plus в одно время с одного компьютера позволяет запускать только один оценочный тест, который оценивает «здоровье» только одного компонента сети (коммутатора, маршрутизатора, канала связи и т.п.). Если сеть не очень большая, то это ограничение также не очень существенно.

Вместо заключения

Возможно, кому-то предлагаемая методика покажется слишком сложной или избыточной. Действительно, столь тщательная проверка «здоровья» сети требуется не всегда. В ряде случаев можно ограничиться выявлением только явных дефектов сети, не градуировать тесты, не оценивать достоверность и полноту собранных данных, не вычислять индекс «здоровья» сети и т.п.

Но существует как минимум два случая, когда тщательный аудит «здоровья» сети не только экономически целесообразен, но и необходим. Первый случай – это внедрение нового, критически важного бизнес-приложения. Аудит позволит отделить дефекты внедряемого приложения от дефектов ИТ-Инфраструктуры. Это сэкономит много сил и времени, т.к. выполнить набор заранее определенных проверок проще и быстрее, чем «решать одно уравнение с двумя неизвестными», пытаясь определить, почему бизнес-приложение не работает как нужно. Второй случай – это внедрение технологии ITSM, в частности, внедрение Service Desk, процессов управления инцидентами, проблемами и т.п. Попытка формализовать работу ИТ-Службы в условиях, когда сеть работает плохо, и у технических специалистов нет эффективных средств мониторинга её «здоровья», часто оканчивается неудачей.

Если вы хотите высказать свое мнение о предлагаемой методике или задать свои вопросы, то можете написать нам по адресу expert@prolan.ru или посетить бесплатный технический семинар: «Чай с Экспертом» (подробнее см. http://www.prolan.ru/).