Юрий Кравцов

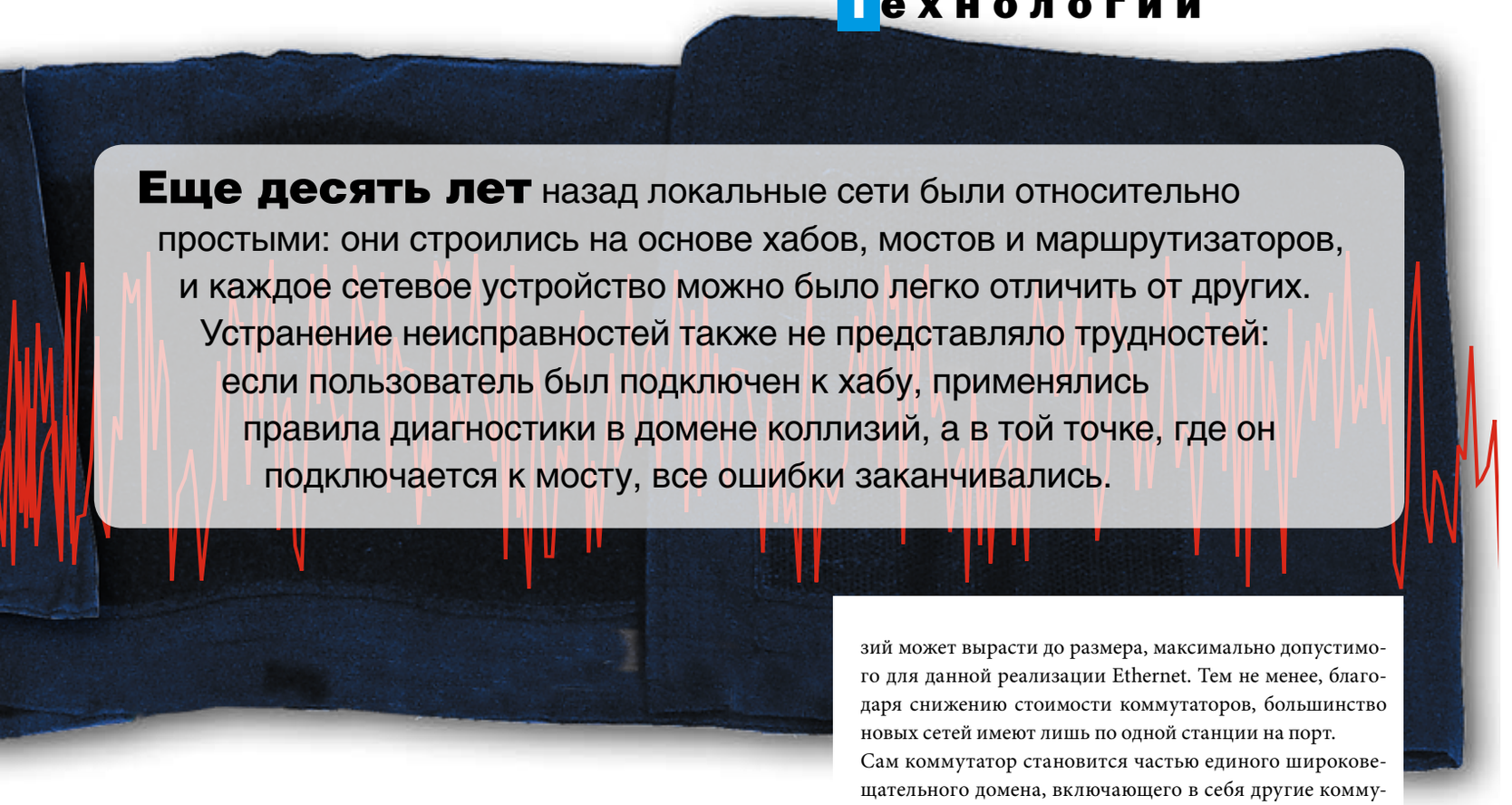
Диагностика коммутируемых сетей

Диагностика с помощью анализатора протоколов была вполне эффективна, поскольку большинство сетевых администраторов знали основы сети и используемых протоколов. Затем в сетях появились коммутаторы. Проблемы, связанные с коммутируемой средой, в целом аналогичны сложностям при работе с разделяемыми ресурсами: трудно понять, какой именно сбой произошел, что послужило источником проблемы и насколько это по- влияло на работу смежных компонентов. В коммутируемых сетях ответы на эти вопросы должны относиться к конкретному порту.

Общие рекомендации по конфигурации сети

Проблемы обнаружения неисправностей начинаются с того, что коммутатор выполняет функции моста 2-го уровня, и усложняются необходимостью поддержки VLAN, а также других функций и правил коммутации 3-го и более высоких уровней сетевой модели OSI. Поиск ошибок в работе функций, использующих информацию 4-го уровня (например, распределение нагрузки), требует отличного знания настроек коммутатора.

При установке коммутатора отдельный домен коллизий создается на каждом полудуплексном порту – такова природа коммутатора. Если к порту коммутатора подключен хаб, домен колли-



Еще десять лет назад локальные сети были относительно простыми: они строились на основе хабов, мостов и маршрутизаторов, и каждое сетевое устройство можно было легко отличить от других. Устранение неисправностей также не представляло трудностей: если пользователь был подключен к хабу, применялись правила диагностики в домене коллизий, а в той точке, где он подключается к мосту, все ошибки заканчивались.

зий может вырасти до размера, максимально допустимого для данной реализации Ethernet. Тем не менее, благодаря снижению стоимости коммутаторов, большинство новых сетей имеют лишь по одной станции на порт.

Сам коммутатор становится частью единого широковещательного домена, включающего в себя другие коммутаторы. Если в сети используются функции 3-го уровня, то создается множество широковещательных доменов, равное количеству сетей VLAN. В предельном случае (если позволяют параметры коммутатора) каждый порт может быть сконфигурирован как отдельный широковещательный домен, и это очень ограничивает возможности для диагностики. Кроме того, при такой конфигурации в коммутаторе должна поддерживаться функция маршрутизации, обычно требующая значительных ресурсов центрального процессора коммутатора для управления трафиком. Трудно предположить, что маршрутизация в сети каждого отдельного запроса и ответа может оказаться целесообразной, поэтому подобной конфигурации следует избегать. К сожалению, она встречается очень часто (хотя и в менее очевидном варианте) в тех сетях, где все серверы относятся к одной подсети или широковещательному домену, а все пользователи находятся в нескольких других подсетях или доменах. На практике при такой конфигурации сети все запросы все равно должны быть маршрутизированы.

Если работы по обслуживанию сети должны ограничиваться только одной серверной комнатой, рекомендуется размещать серверы в различных сетях VLAN. Такая конфигурация позволит коммутационной матрице работать в качестве моста 2-го уровня для обычного трафика, а маршрутизации будут подлежать только необычные или редкие запросы. Если сервер обслуживает не одну, а несколько групп пользователей, следует установить дополнительные сетевые адаптеры в сервере, чтобы сохранить связь с пользователями на 2-м уровне.

Вот типичные вопросы, которые возникают при использовании коммутируемой среды:
Насколько загружен каждый порт? Как найти источник ошибок? Что является источником широковещательного шторма (размножения некорректно сформированных широковещательных сообщений)? Правильно ли работают таблицы MAC-адресов? Какие станции подключены к данному порту? Ограничивает ли коммутатор скорость работы какого-либо протокола или порта? Находится ли данный порт в виртуальной локальной сети (VLAN)? Если да, то находится ли сервер в этой же самой VLAN?

Пять методов диагностики коммутируемых сетей

Существует пять основных методов, позволяющих определить, что происходит в коммутаторе. Каждый метод предполагает собственный подход и имеет как положительные, так и отрицательные стороны. Как и во множестве других ситуаций, связанных с сетями, здесь нет единственно правильного ответа. Наиболее подходящее решение определяется, с одной стороны, наличием нужного инструментария, а с другой – возможностью прерывания связи при использовании данного метода диагностики.

Даже если скомбинировать все возможные методы, они не смогут обеспечить такой же уровень контроля коммутируемой сети, как в случае применения в сети хабов. Весь трафик, идущий через коммутатор, просмотреть почти невозможно. В большинстве случаев при поиске неисправности предполагается, что трафик проходит между компьютером и сервером или через линию связи с другим узлом (Uplink). Если две рабочие станции обмениваются информацией напрямую, трафик не будет проходить че-

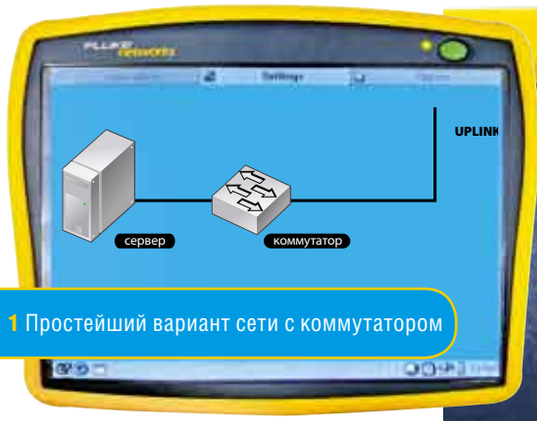


Рис. 1 Простейший вариант сети с коммутатором

Рис. 2 Использование консольного порта

Рис.3 Мониторинг с любого свободного порта

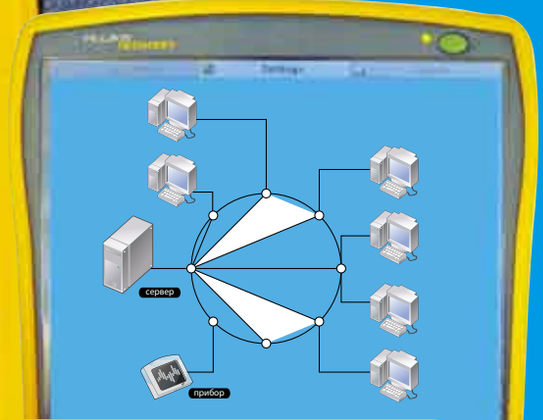


Рис.4 Анализатор "видит" только широковещательный трафик

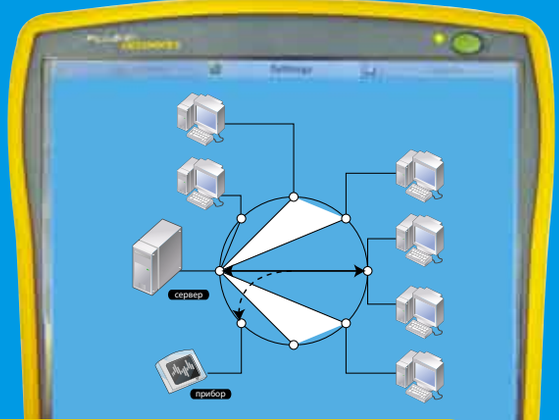


Рис.5 Коммутаторы направляют поток данных от передающего порта в порт назначения

рез Uplink, как впрочем, и через любой другой порт коммутатора. И если специально не проверить трафик между этими двумя компьютерами, то можно и не обнаружить проблему.

Для простоты рассмотрим одну из типичных конфигураций сети – сервер, подключенный к коммутатору (рис. 1). Пользователь (пользователи), у которого возникают проблемы, может быть подключен к тому же коммутатору или получать доступ к серверу через Uplink – линию связи, ведущую к другому коммутатору или маршрутизатору. При этом жалоба пользователя будет звучать примерно так: "Связь с сервером слишком медленная". Такая формулировка, к сожалению, не говорит сетевому администратору почти ничего.

Метод 1. Настройка коммутатора через Telnet или последовательный порт

В процессе поиска неисправности сетевой администратор (если у него есть пароль доступа) может проверить правильность настроек коммутатора путем подключения к консольному порту RS-232 (рис. 2) или с помощью Telnet-сессии.

Однако полученные в результате данные о конфигурации коммутатора сами по себе малоинформативны. Чтобы понять, корректны они или нет, придется использовать один или несколько других методов поиска неисправностей.

Некоторые коммутаторы снабжены дополнительными средствами диагностики, однако диапазон их возможностей различен в зависимости от производителя и модели коммутатора. В любом случае, чтобы воспользоваться этими инструментами, требуются немалый опыт и глубокие теоретические знания.

Метод 2. Подключение анализатора к свободному порту коммутатора

Самый простой метод обнаружения неполадок – подключение прибора с функцией мониторинга (например, анализатора протоколов) к любому неиспользуемому порту на коммутаторе (рис. 3). Подключенный таким образом прибор получает доступ в широковещательный домен как обычная рабочая станция, не нарушая работы других пользователей. К сожалению, коммутатор (который мы считаем многопортовым мостом) будет направлять на контролируемый порт лишь незначительную часть трафика. Это нормальное поведение моста, поскольку его назначение – предотвращать попадание трафика в те порты, которым он не предназначен. А анализатор протоколов в этом случае не запрашивал никакого трафика и, скорее всего, не передавал ни одного фрейма (рис. 4). Прибор "увидит" лишь несколько фреймов в минуту вместо нескольких тысяч в секунду, которые могут передаваться между станциями и сервером.

Трафик, приходящий на порт мониторинга, будет почти полностью состоять из широковещательных фреймов. Возможно, там окажется еще несколько случайных фреймов, пришедших от неизвестных отправителей. Такие фреймы могут появляться из-за старения таблицы MAC. Некоторые невнимательные сетевые администраторы в таких случаях решают, что в сети действительно почти 100% пакетов – широковещательные, и при этом не замечают, что уровень использования (утилизации) сетевых ресурсов очень низкий. В результате делается некорректный вывод о наличии в сети широковещательного шторма. А если жалоб от пользователей не поступало, то администратор вообще может решить, что такая ситуация – часть нормального процесса функционирования сети.

Поскольку описанный подход к диагностике сети практически бесполезен, прибор должен сам запрашивать трафик. "Опрос" широковещательного домена полезен для обследования сети и поиска других проблем, однако он не поможет продвинуться в решении проблемы медленного соединения, о которой сообщил пользователь.

Более содержательные результаты могут быть получены при использовании так называемого зеркального копирования (зеркалирования) портов: большинство коммутаторов разрешают копировать трафик из выбранного порта или портов на другой порт, к которому и подключается анализатор (рис. 5). Зеркалирование позволяет прибору "видеть" трафик между сервером и "проблемным" компьютером, пользователь которого жалуется на низкую производительность. У старых моделей коммутаторов в качестве порта для мониторинга можно сконфигурировать специально выделенный порт; на новых коммутаторах для этого подходит любой порт.

Способ реализации данного метода варьируется у различных производителей, но имеется несколько общепринятых способов зеркалирования. Отметим, что в большинстве случаев пакеты, перенаправленные в порт мониторинга, будут отфильтрованы так же, как и пакеты, посылаемые на все остальные порты. Это означает, что все ошибки будут отфильтрованы коммутатором и не достигнут порта мониторинга. Тогда зеркалирование трафика на порт мониторинга может оказаться неэффективным для целей диагностики, поскольку при таком подходе коммутатор скрывает целый класс проблем. Кроме того, чтобы правильно настроить порт мониторинга, нужно подключиться к нему либо с консоли (порт RS-232 на коммутаторе), либо через Telnet-сессию – следовательно, помимо анализатора потребуется еще и компьютер.

"Зеркальный" порт мониторинга часто бывает только принимающим, хотя некоторые производители коммутаторов делают его двунаправленным. На него может поступать копия трафика от любого другого порта – одного или нескольких. И чем больше портов в коммутаторе "прослушивает" порт мониторинга, тем выше вероятность того, что ему не хватит пропускной способности и анализатор протоколов получит не все фреймы.

Пропускная способность порта мониторинга – серьезная проблема. Дело в том, что порт имеет приемную (Rx) и передающую (Tx) части. Передающая часть порта мониторинга может быть заблокирована на коммутаторе, но независимо от этого пропускная способность приемного канала (от порта коммутатора к анализатору) все равно ограничена. Если зеркалируется полнодуплексный порт, работающий с той же скоростью, что и порт мониторинга, коммутатор может просто отбросить часть трафика, не выдав об этом никакого сообщения. И неважно, подключен прибор по полу- или полнодуплексному каналу – ограничение скорости работы приемника все равно будет одним и тем же.

Предположим, возникла необходимость проанализировать трафик сервера, подключенного к коммутатору на скорости 100 Мбит/с по полнодуплексному каналу (рис. 6). При полном дуплексе приемная и передающая части могут соответственно передавать и принимать по 100 Мбит/с трафика каждая. Таким образом, суммарная пропускная способность канала составляет 200 Мбит/с. Для зеркалирования трафика, идущего от сервера, может использоваться только приемник (Rx). Следовательно, размер контролируемого трафика ограничен максимумом в 100 Мбит/с. Любой трафик сервера, превышающий 50% емкости данной линии (200 Мбит/с), будет потерян.

Если на порт мониторинга поступает трафик с нескольких портов, проблема соответственно усложняется. Впрочем, поскольку большинство коммутаторов работает далеко не на 100% своей пропускной способности, данная проблема может и не коснуться вашей сети, но потенциально она существует. Для большинства пользователей сети загруженность соединений не превышает 10%, и изредка происходит кратковременный, но большой по амплитуде всплеск трафика.

Пользователь, у которого возникают проблемы, может быть подключен к тому же коммутатору или получать доступ к серверу через Uplink. При этом жалоба пользователя будет звучать примерно так: "Связь с сервером слишком медленная". Такая формулировка, к сожалению, не говорит сетевому администратору почти ничего

Очевидное решение проблемы – подключить прибор к высокоскоростному порту, который может принять весь "зеркальный" трафик. Если бы пропускная способность порта мониторинга (рис. 6) составляла 1 Гбит/с вместо 100 Мбит/с, совокупный трафик в 200 Мбит/с был бы с легкостью принят и проанализирован.

Метод 3. Установка хаба в тестируемый сегмент

Во многих сетях большую часть трафика создают совместно используемые ресурсы (например, файловые серверы). Если установить хаб между файлсервером и коммутатором и подключить к нему анализатор (рис. 7), то последний окажется в том же широковещательном домене, что и сервер.

При такой схеме подключения анализатор "видит" весь входящий и исходящий трафик сервера, благодаря чему сетевой администратор может узнать о неудачных попытках подключения зарегистрированных пользователей к серверу, а также определить, не приводит ли низкая производительность канала к сбросу соединений.

Такой метод, к сожалению, неприменим в сетях с несколькими серверами. Размещать хаб рядом с каждым сервером нецелесообразно, а если переносить хаб от сервера к серверу, то придется останавливать сеть на время, требуемое для подключения хаба. Конечно, установить хаб – дело нескольких минут, но текущие соединения при этом будут сброшены. Кроме того, нет гарантии, что анализатор сможет работать на скорости канала, по которому подключен сервер. Тем не менее использование хаба полезно для решения ряда задач мониторинга трафика и поиска ошибок. В частности, это почти единственный способ разобраться в ошибках MAC-уровня в коммутируемой среде. Конечно, такие ошибки можно отследить и с помощью SNMP-клиента, но для полноценного анализа ошибок значительно лучше "увидеть" их напрямую на тестирующем устройстве.

У данного метода есть два существенных недостатка. Во-первых, серверная линия связи не может быть полнодуплексной, в противном случае несоответствие режимов передачи приведет к большему количеству ошибок, чем сможет обнаружит администратор. Во-вторых, для реализации этого метода необходим хаб, а большинство современных хабов на самом деле являются мостами, "замаскированными" под хаб. Установить такое устройство, не являющееся настоящим хабом с разделяемой пропускной способностью, – все равно что установить еще один коммутатор, и в результате увидеть искомый трафик будет невозможно.

Двухскоростные хабы 10/100 на самом деле представляют собой два хаба – на 10 и 100 Мбит/с, соединенных между собой мостом. Такой хаб использовать можно, только следует убедиться, что сервер и анализатор работают на одной скорости.

Также встречаются дешевые коммутаторы, у которых от настоящих хабов осталось только название и низкая цена. Производители стремятся унифицировать производство, и им выгоднее снизить цены на коммутаторы, чем сохранять производство хабов. Такие "хабы" для описанного выше метода совершенно непригодны.

Метод 4. Использование разветвителя кабеля

Этот метод аналогичен предыдущему с установкой хаба, за исключением того, что анализатор сможет только принимать, но не передавать данные (рис. 8). Существуют разветвители для медных и для волоконно-оптических кабелей.

Оптические разветвители (сплиттеры) являются пассивными устройствами и не требуют электропитания. Сплиттер характеризуется процентом отводимой оптической мощности (например, разветвитель 80:20 отводит 20% мощности). Очевидно, что добавление сплиттера в линию связи приводит к уменьшению мощности сигнала, поступающего на приемник. А если бюджет по затуханию на этой линии практически исчерпан, то добавление сплиттера неизбежно приведет к нарушению связи. Впрочем, некоторые оптические передатчики более устойчивы к внесению затухания, так что можно попробовать установить сплиттер на другой стороне линии.

Медные разветвители также вносят в линию дополнительное затухание и приводят к потере связи, если линия уже работает на пределе своих возможностей. Медным разветвителям требуется электропитание, так как они принимают, восстанавливают и передают полученный сигнал. Впрочем, при пропадании питания сама линия все равно будет работать – отключится только порт мониторинга (конечно, при условии, что разветвитель установлен правильно).

Удобство использования разветвителей заключается в том, что они невидимы для остального сетевого оборудования. Достаточно установить разветвитель один раз на контролируемом соединении и использовать его при необходимости. К сожалению, для его установки придется резать кабель. Надо сказать, что это не единственный недостаток. Разветвитель работает отдельно с каждым направлением передачи, следовательно, порт мониторинга состоит из двух физических соединений (рис. 9).

Поэтому для одновременного мониторинга обоих направлений в тестирующем приборе должно быть два входа. Обычно приборы с двумя входами могут объединять оба потока и анализировать их одновременно. Можно, конечно, анализировать каждое направление по отдельности, но это значительно сложнее. Эффективность данного метода одинакова для полу- или полнодуплексных соединений.

Метод 5. Сбор данных по протоколу SNMP

Самый эффективный метод диагностики коммутируемой сети – запросить информацию о ситуации в сети у самого коммутатора. Это делается удаленно с помощью протокола SNMP (рис. 10) или путем непосредственного подключения к консольному порту коммутатора. Использование SNMP удобнее, поскольку администратору не нужно ходить с ноутбуком от коммутатора к коммутатору – вся информация будет поступать на его рабочее место. Если реализована система управления сетью,

В реальной жизни чаще всего используется такой метод диагностики – дождаться жалоб от пользователей. И не следует его отбрасывать из-за слишком очевидной простоты – на самом деле он очень эффективен

Рис.6 Ограничение пропускной способности порта мониторинга

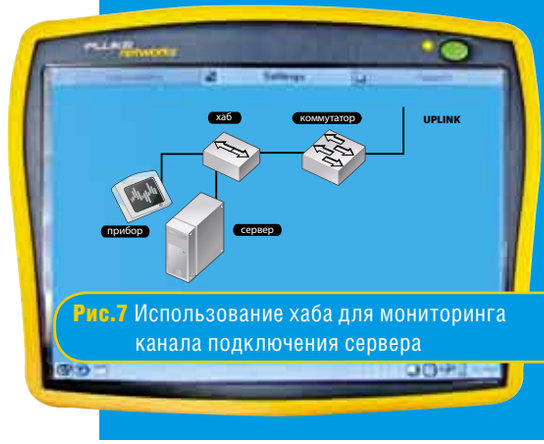


Рис.7 Использование хаба для мониторинга канала подключения сервера

можно настроить коммутатор на автоматическую отправку сообщений о событиях, проходящих в сети (SNMP trap), например, об ошибке или выходе значения какого-либо параметра за пределы заданных пороговых значений. Сетевому администратору останется лишь с помощью тестирующего устройства выяснить, почему это нежелательное событие произошло.

Буквально все коммутаторы (кроме самых дешевых) оснащены функцией SNMP-управления. Разница лишь в том, насколько детализирована информация, предоставляемая коммутатором. Некоторые коммутаторы имеют средства SNMP, предлагающие только информацию об устройстве в целом, другие (более дорогие) предоставляют подробную информацию по каждому порту в отдельности.

SNMP, пожалуй, самый удобный и наименее разрушительный метод мониторинга коммутируемой сети. SNMP-клиент может располагаться в любом месте сети, а доступ ко всей диагностической информации защищен паролем (community string). К одному и тому же коммутатору может быть несколько паролей с различными правами доступа. Ограничения доступа также могут касаться подсетей и даже отдельных IP-адресов. В отношении защищенного доступа к коммутатору необходимо обратить внимание на следующее. Большинство коммутаторов поставляется с паролем “public”, и просто поразительно, как много сетевых администраторов не меняют его! Еще одна угроза безопасности связана с тем, что пароли передаются по сети в открытом виде. Шифрование предусмотрено в версии SNMPv3, но она пока не получила широкого распространения.

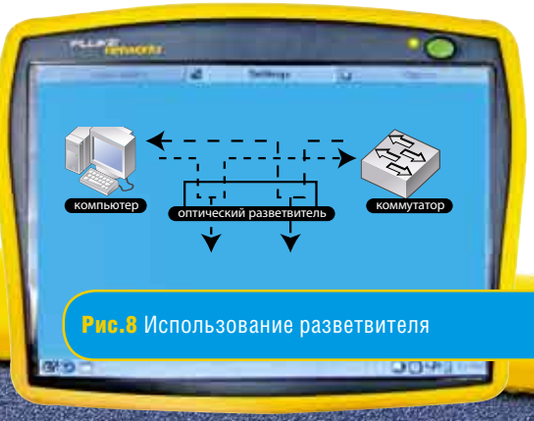


Рис.8 Использование разветвителя

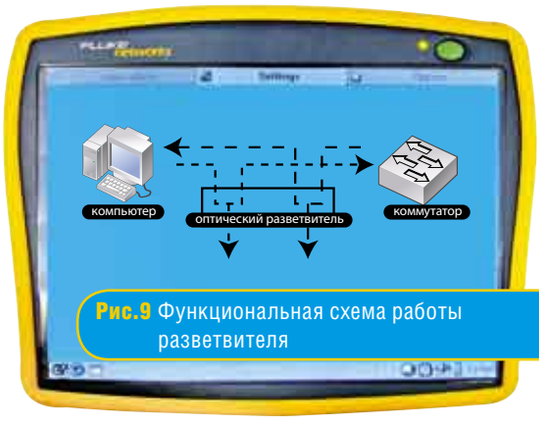


Рис.9 Функциональная схема работы разветвителя

Рис.10 Использование протокола SNMP для мониторинга коммутатора

Перечень контролируемых параметров зависит от используемой базы MIB. Большинство производителей коммутаторов предлагают MIB-базы собственной разработки, но можно воспользоваться и стандартной (MIB II, Ethernet-Like Interface MIB, RMON Ethernet, RMON 2, SMON и т.д.).

Маршрутизаторы, через которые проходят SNMP-пакеты, могут накладывать на них различные ограничения, а межсетевые экраны (firewall) могут полностью блокировать SNMP. Кроме того, SNMP-агенты могут работать с ошибками, что приводит к ложным срабатываниям. Тем не менее SNMP в целом является очень полезным средством диагностики.

Заключение

В реальной жизни чаще всего используется такой метод диагностики – дождаться жалоб от пользователей. И не следует его отбрасывать из-за слишком очевидной простоты – на самом деле он очень эффективен. Сообщество пользователей имеет обостренное чутье на то, как должна вести себя сеть. Любое отклонение от нормального хода вещей будет доведено до сведения службы технической поддержки. После жалобы пользователя сетевой администратор может начать процесс диагностики с соответствующего порта подключения. Однако такой подход можно сравнить с тушением пожара, а ведь всем известно, что пожары лучше предотвращать, чтобы потом не пришлось их тушить. Для предотвращения проблем следует организовать регулярный мониторинг – собирать информацию с каждого коммутатора и отслеживать загруженность каждого порта, и это избавит службу технической поддержки от большинства жалоб пользователей. **Обсудим?**

fnet@icsgroup.ru