Фильтрованный доступ к данным для тестирования, оценки и защиты сети

По мере усложнения сетей администраторы и инженеры придают все большее значение их работе, безопасности и соответствию нормам. Устройства для тестирования, оценки и защиты, используемые при мониторинге и обслуживании сетей, сегодня должны видеть всю информацию в распределенной сети. Рост корпоративных сетей и объем обрабатываемой ими информации требует разработки новых стратегий по защите и оценке использования пропускной способности сетей. Агрегация линий и фильтрующие устройства обеспечивают улучшенное видение сети, необходимое для ее защиты и анализа.

Содержание

FLUKE networks

landata
ТОЧКА ОПОРЫ

Введение

Компьютерные сети стали важнейшей частью инфраструктуры любых компаний, и вопросы их диагностики усложнились. Коммутируемые инфраструктуры, архитектуры SAN и распределенные сети, использующие такие приложения, как VoIP, могут создать проблемы даже для опытных специалистов. Структура сети становится все более неоднородной и включает разнообразные компоненты от целого ряда производителей. Если происходит сбой, все труднее устранить ситуацию, когда производители разных компонентов и сотрудники разных отделов постоянно «переводят стрелки» и обвиняют друг друга в случившемся. Сетевые администраторы сегодня нуждаются в точнейшей информации. Им необходима верная и своевременная информация о состоянии сети и ее безопасности. Только так можно гарантировать непрерывную оптимизацию сети, создание внутренних отчетов, планирование сетевого бюджета и создание статистики для проверки соответствия сети нормам законодательства.

Безопасность

Защита сети ранее была направлена на защиту от внешних врагов с помощью межсетевых экранов. Теперь, хотя этот аспект сохраняет большое значение, все больший акцент делается на безопасность внутреннего трафика. Зараженные вирусами ноутбуки, несанкционированные беспроводные сети и сотрудники – все это увеличивает важность внутреннего анализа работы сети.

В наше время модели глубинной защиты способны распознавать и предотвращать сетевые атаки, использовать внутренние межсетевые экраны и системы контроля доступа к сетям. Системы защиты часто внедряются на важнейших устройствах и каналах или рядом с ними. Такими устройствами могут быть серверы, основные коммутаторы, демилитаризованные зоны (DMZ) и межсетевые экраны. Асимметричные маршруты трафика позволяют ему следовать от источника и обратно по разным путям. Такие маршруты (с резервированием) заставляют сотрудников отдела защиты сети внедрять все новые приборы для анализа трафика и посвящать больше времени выявлению и решению проблем безопасности. К сожалению, данные, предоставляемые этими приборами, зачастую ограничены характеристиками SPAN-порта или чрезмерным объемом посылаемого на прибор трафика. Приборы для защиты сетей не могут видеть 100% сетевых данных, и специалисты по безопасности вынуждены определять на глазок, что включено или не включено в проводимый ими анализ.

Мониторинг

Мониторинг компьютерных сетей развивался аналогично безопасности сетей. Процесс мониторинга стал сегментированным, охватывая все большие области – и порождая все больше вопросов в области отслеживания работы сети и устранения сбоев. Мест накопления информации о сетях становится все больше, а следовательно, увеличивается и число приборов, используемых для получения доступа к этой информации. Улучшение видения сетей означает дальнейший рост устройств, необходимых для получения доступа к сетям с целью мониторинга, защиты, обслуживания или диагностики. Процессы диагностики и обнаружения и устранения неисправностей требуют видения сетей, работающих на различных платформах. Каждая из этих систем требует извлечения данных из целого ряда сетевых устройств, маршрутизаторов, коммутаторов, серверов и зондов. Очень часто необходимо видеть одни и те же данные в конкретном сегменте сети. Чтобы диагностировать и устранять проблемы с сетью, ИТ-специалисты вынуждены применять множество приборов и связанных с ними приложений.

Новые нормы, требующие от компаний хранения данных о работе сети и создания на базе этих данных отчетности, еще больше увеличивают потребность в отслеживании состояния сетей. CALEA, Sarbanes-Oxley, GLBA, HIPAA, SB1386 и PCI – вот лишь несколько из этих многочисленных норм.

SPAN-порты

SPAN-порты стали обычным средством сбора информации о сети. Они встроены в большинство промышленных коммутаторов и маршрутизаторов. Порты позволяют сетевому администратору копировать проходящий через конкретные сетевые порты трафик и отправлять эти копии на другой порт. SPAN-соединения легко создавать: для этого нет необходимости отключать сетевое соединение. Одно из преимуществ SPAN-портов в том, что они позволяют видеть пакеты, адрес отправителя и получателя которых непосредственно связаны с портом коммутатора, на котором применяются SPAN. Этот трафик никогда не идет по uplink-порту к другому коммутатору или маршрутизатору, и его было бы трудно зафиксировать без прямого захвата пакетов в канале, соединяющем отправителя и получателя трафика. SPAN-порты очень эффективны для задач срочного выявления и устранения проблем с приложениями, где объем трафика относительно невелик.

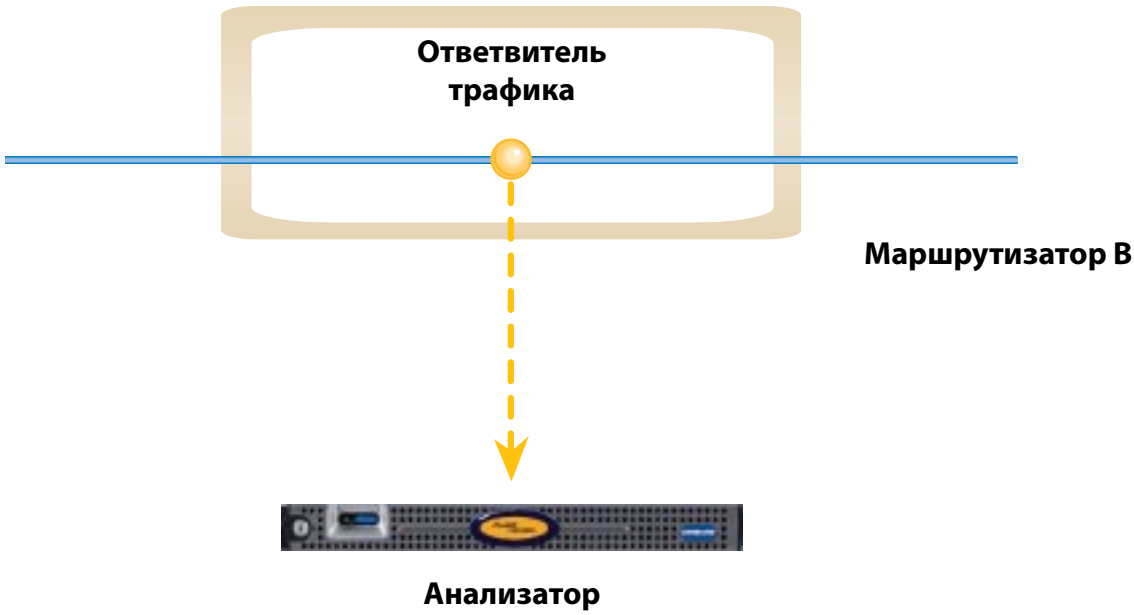
Однако их применение связано с определенными условиями и ограничениями. Если несколько SPAN-портов копируют трафик на один конечный порт, то объем генерируемого трафика может быстро перегрузить SPAN-порт-получатель. Трафик, пропущенный из-за перегрузки SPAN-порта-получателя, не будет ретранслирован отправитель трафика. Проблема в том, что, если ресурсы сетевого устройства исчерпаны, SPAN-порты часто имеют низкий приоритет. При использовании этих портов есть риск, что часть трафика не достигнет порта-получателя. Приборы для мониторинга и защиты могут пропустить трафик, если SPAN-порт не сможет его передать. Для приборов, осуществляющих анализ безопасности сети, это может стать серьезной проблемой.

SPAN-порты также занимают сетевой порт на устройстве, где могут быть подключены другие средства для анализа и защиты сетей. Если свободные порты коммутатора отсутствуют, SPAN-порты для мониторинга сети использовать нельзя. Число SPAN-портов для большинства сетевых устройств ограничено, и у каждого производителя есть свои ограничения по тому, что SPAN-порт способен или не способен видеть.

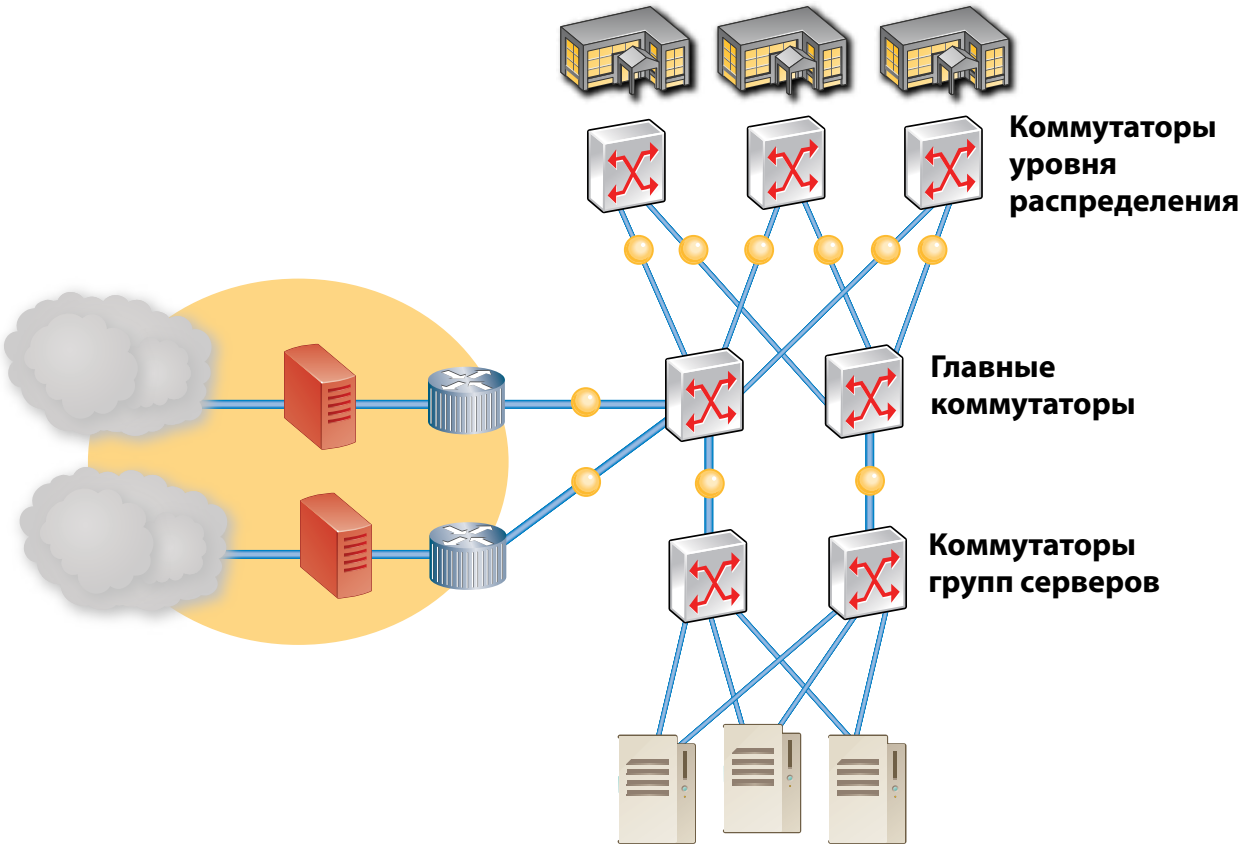
Для устранения серьезных сбоев в работе сети приходится привлекать множество ИТ-специалистов. Зачастую SPAN-порт создается для диагностики возникшей проблемы или сбора информации. В этот трудный период важно верно настроить SPAN-порт, иначе он создаст дополнительные сложности или перегрузит сетевое устройство, на котором установлен. Из-за всего этого – а также необходимости видеть 100% данных – SPAN-порты все реже используются для сбора данных на важнейших участках сети. Эта тенденция вызвана также ограничениями в настройках, установке, агрегации и пропускной способности SPAN-портов.

Ответвители сетевого трафика

Ответвители сетевого трафика – альтернатива SPAN-портам в области сбора трафика. Ответвители – это устройства, подключенные в разрыв между коммутаторами, межсетевыми экранами и серверами. Ответвители имеют преимущества над SPAN-портами, в особенности потому, что позволяют трафику беспрепятственно перемещаться между сетевыми устройствами, пока они копируют его для целей мониторинга или защиты сети. Ответвители – это постоянная точка видения сетевого трафика и будут обеспечивать целостность соединения, даже если питание на ответвителе будет отключено. Ответвитель копирует видимый им сетевой трафик без существенной задержки или потери пакетов между сетевыми устройствами. Поскольку ответвители подключаются последовательно, им не нужен порт на коммутаторе или маршрутизаторе. Хотя ответвители трафика способны видеть больше информации, чем SPAN-порты, они не видят внутренний трафик коммутаторов. Большинство ответвителей не требуют настройки – они просто постоянно работают. Некоторые ответвители могут делать множество копий сетевого трафика; таким образом разные приборы видят один и тот же набор данных.



Ответвитель трафика



В типичной сети ответвители устанавливаются в каналах, по которым передается наиболее важная информация для обеспечения быстрого и эффективного подключенияанализатора.

Ответвители сетевого трафика бывают разными и работают на разных скоростях. Если необходимо предоставить нескольким приборам доступ к каналу, неудобно для каждого прибора использовать отдельный ответвитель. Это слишком удорожит процесс. Намного практичнее иметь один ответвитель, воспроизводящий трафик на несколько портов для подключения устройств для мониторинга по необходимости или желанию. В этом случае копии трафика поступают в канал один раз, минимизируя потерю оптического сигнала (если это волоконно-оптический ответвитель) и позволяя предоставить каждому прибору точную копию данных.

Сегодня, когда безопасность сетей имеет важнейшее значение, сетевые ответвители оказываются надежнее SPAN-портов, поскольку порты мониторинга могут быть однонаправленными и невидимыми для других сетевых компонентов. Syslog-сервер или устройство для записи сетевых данных, получающие данные от направленного ответвителя трафика, могут не бояться удаления данных хакером, получившим доступ через ответвитель и пытающимся замести следы своего посещения.

При установке ответвителей соединение между сетевыми устройствами необходимо прервать (отключить), но после установки оно может работать непрерывно. Одно устройство для анализа сети может видеть множество сетевых сегментов, используя ответвитель трафика, агрегирующий данные из этих сегментов. Экономия, связанная с необходимостью в меньшем количестве зондов для анализа сети, позволит быстро окупить затраты на ответвитель сетевого трафика. Ответвители трафика используются в любых сетях, где необходима 100% видимость и работоспособность – от самых важных и крупных до самых небольших.

Фильтрующие канальные агрегационные ответвители трафика

Такие правовые нормы, как закон Sarbanes-Oxley, вынудили многие компании внедрить сложные решения по мониторингу и аудиту финансовых операций и сетей, в которых они производятся.

Многие приборы для анализа сетей захватывают данные из сети и хранят их в буфере или на жестком диске. Этот анализ чаще всего производится постфактум, а не в режиме реального времени. Аппаратные ограничения, связанные с картой NIC и буфером (памятью), ограничивают объем данных, которые можно просматривать в режиме реального времени. Объем хранимых прибором данных ограничен размером буфера. Долгосрочный анализ обычно не осуществляется, поскольку буфер и память слишком быстро заполняются и делают такой анализ нерациональным.

Способность записывать и анализировать крупные объемы сетевого трафика на качество сервисов (QoS) и защиты приобрела особую важность с появлением VoIP. Вместо того чтобы использовать более сложные приборы для анализа сети, более объемные устройства для записи данных или их защиты, многие ИТ-специалисты пытаются сократить нежелательный трафик с помощью аппаратных фильтрующих ответвителей трафика.

Эти ответвители обладают многими из преимуществ, характерных для традиционных сетевых ответвителей, а также позволяют отфильтровывать ненужные пакеты. Фильтрация производится по разным критериям: IP-адресам, VLAN, портам приложений, MAC-адресам и разнообразной информации в заголовках. Сочетание фильтров позволяет тщательно отбирать только самую необходимую сетевую информацию. Это новый явный плюс для процессов анализа приложений и обеспечения безопасности или тестирования нагрузки на сеть.

Фильтрующие канальные ответвители трафика позволяют объединять сетевые потоки, выявлять шаблоны данных и отправлять на анализ только нужные данные. Используя эту тактику, становится возможным получать полное видение происходящего в сети (даже в разных ее сегментах) с помощью всего одного прибора. Фильтрация позволяет аналитическим приложениям обрабатывать только нужные данные, таким образом освобождая место для хранения информации и вычислительные мощности для увеличения эффективности выявления и устранения неисправностей и анализа работы сети. Фильтрующие канальные агрегационные ответвители трафика дополнительно улучшают анализ работы приложений, позволяя ИТ-специалистам видеть трафик, поступающий с конкретных адресов или VLAN, с конкретных портов диапазона портов.

Использование большого количества сетевых устройств – большая нагрузка на ИТ-бюджет. Один из способов удешевления анализа и защиты сетей – преобразование среды передачи с помощью ответвителей трафика. Преобразование среды передачи с помощью фильтрующих канальных агрегационных ответвителей трафика позволяет прибору для анализа медных сетей видеть трафик, скопированный с волоконно-оптической линии. Вместе с фильтрацией этот метод позволяет прибору, работающему на небольшой скорости, анализировать скоростную сеть – это продлевает срок работы прибора. Фильтрующие канальные ответвители трафика помогают преодолеть разрыв между скоростными каналами и «медленными» приборами для анализа и защиты сети.

Фильтрующие канальные ответвители трафика – пример использования

Крупная компания использует прибор для записи данных, чтобы защитить сеть и обеспечить ее соответствие нормам CALEA и Sarbanes-Oxley. Этот прибор способен записать примерно трехдневный трафик конкретной линии. Отдел защиты сети решил не использовать SPAN-порт, поскольку он не обеспечивает 100% передачу трафика записывающему устройству и в принципе может быть отключен хакерами, получающими доступ к сети – или случайным действием ИТ-специалиста. Было принято решение использовать фильтрующий канальный агрегационный ответвитель трафика, поскольку он обеспечивает передачу 100% сетевого трафика на записывающее устройство. Этот ответвитель полностью пассивен (он копирует данные с волоконно-оптической линии) и не допускает потери пакетов на пути от устройства к устройству, даже в случае катастрофического сбоя. Ответвитель может преобразовывать оптический сигнал волоконно-оптической сети в электрический: на записывающем устройстве используется более дешевый медный интерфейс. ИТ-специалисты знали, что каждую ночь выполнялось резервирование данных с нескольких серверов через данное соединение. После того как ответвитель скопировал этот трафик, он был подвергнут фильтрации перед отправкой на записывающее устройство. Эта тактика сократила объем сохраненных данных и почти удвоила объем записываемой информации: теперь это уже шесть дней.

Фильтрующие SPAN-решения

Для клиентов, предпочитающих работать со SPAN-портами, тот же уровень аппаратной фильтрации может использоваться для улучшения видения сети сетевыми устройствами и приборами для обеспечения безопасности. Фильтрующие канальные агрегационные SPAN ответвители трафика получают трафик со SPAN-порта и производят фильтрацию, агрегацию и преобразование среды передачи. Это не последовательно подключенные устройства, и они не копируют трафик, передаваемый по каналу. Фильтрующие канальные агрегационные ответвители трафика SPAN идеальны для ситуаций, когда инженеру необходимо взглянуть на трафик с разных портов сетевого коммутатора. Ответвитель SPAN имеет несколько выходов. Если у сетевого коммутатора мало SPAN-портов, то трафик с этого SPAN-порта, отправленный через фильтрующий канальный агрегационный SPAN ответвитель трафика, способен теперь предоставлять данные нескольким приборам.

Аналитические данные о сети необходимы многим отделам компании, поэтому фильтрующее устройство идеально подходит для таких случаев. Поскольку каждое фильтрующее устройство позволяет фильтровать каждый порт в отдельности, любой отдел может получать необходимые именно ему данные. Конкретные IP-адреса и VLAN могут исключаться из записи или анализа информации для некоторых отделов. Вы можете предоставлять в отдел защиты сети только сетевой трафик, без трафика VoIP, чтобы исключить подслушивание разговоров по VoIP. Для этого нужно просто использовать подключение к фильтрующему канальному агрегационному ответвителю трафика как к SPAN-порту-получателю. При необходимости можно создать SPAN-порт

из любого сетевого порта коммутатора – и отправить трафика на фильтрующий канальный агрегационный ответвитель трафика SPAN. Фильтрация на аппаратном уровне может ограничить трафик, чтобы прибор видел только интересующие его данные. Как правило, клиенты ограничивают широковещательный, групповой и другой не требующий анализа трафик.

Фильтрующие ответвители SPAN – пример использования

Некая компания включает в себя ряд отделов с различными приборами, которым необходимо получать информацию о сетевом трафике. Сетевой коммутатор располагает ограниченным числом SPAN-портов: их недостаточно для всех приборов, зондов и средств мониторинга защиты сети.

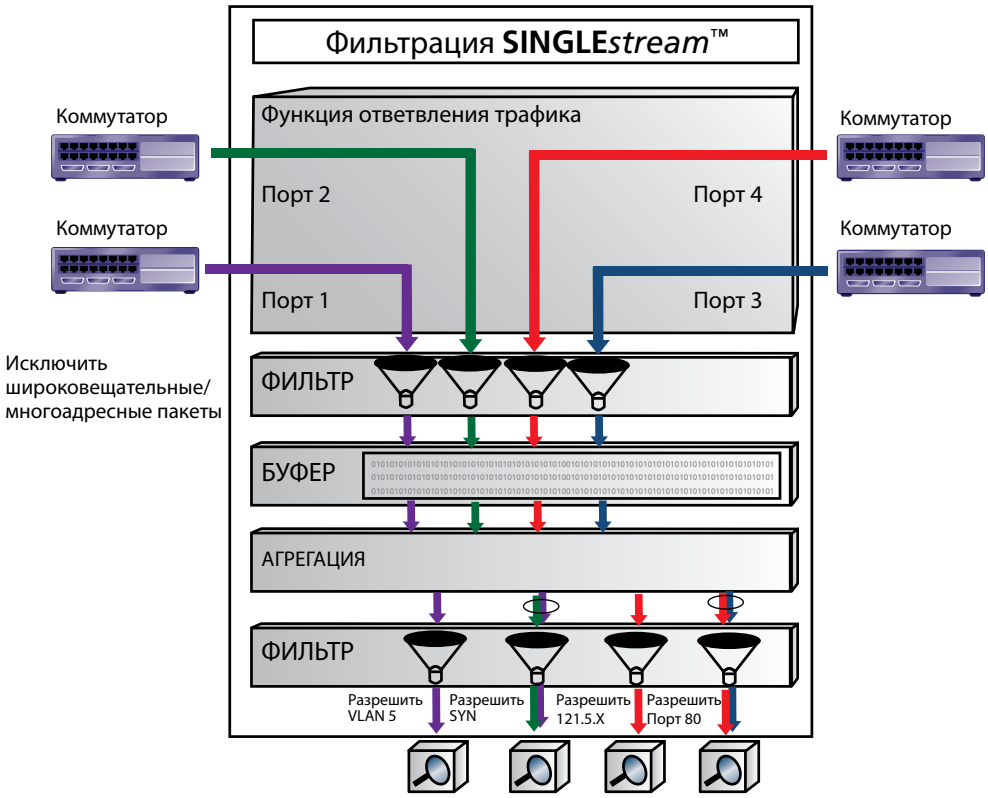
Сетевой отдел имеет доступ к коммутаторам и устанавливает SPAN-порты, но не желает, чтобы к ним имели доступ другие отделы.

Каждый отдел желает видеть сетевой трафик. Однако в сетевой группе основной акцент сделан на анализ трафика VoIP, отделу аудита нужен исходящий и входящий трафик бухгалтерской сети (VLAN), а отделу безопасности требуются все данные сразу.

Идеальное решение – фильтрующий канальный агрегационный ответвитель трафика. Сетевой отдел настраивает SPAN на просмотр конкретного uplink-порта. Этот конкретный SPAN-порткопирует трафик на фильтрующий канальный агрегационный ответвитель трафика, который делает копии для каждого порта мониторинга, который присваивается в зависимости от нужд конкретных отделов. Каждый отдел получает свою информацию. Фильтрация по отдельным портам на агрегационном ответвителе позволяет каждому отделу видеть только необходимый ему трафик: трафик VoIP, трафик бухгалтерской сети или весь трафик целиком. Нагрузка на сетевой отдел снижается, поскольку SPAN-порт не приходится перенастраивать. Если сетевой отдел решит проанализировать другой трафик, кроме VoIP, они могут просто поменять настройки фильтра порта, к которого подключен их прибор. Они не влияют на работу других отделов и не должны настраивать SPAN.

Фильтрующие канальные агрегационные ответвители трафика SPAN могут принимать трафик со SPAN-портов и фильтровать данные для различных портов мониторинга на основе запросов или критериев отделов.

Фильтрующие канальные агрегационные ответвители трафика SPAN



SPAN-вход со специальными фильтрами для каждого подразделения.

Заключение

Анализ сетей находится на такой стадии развития, когда особое значение приобретает тщательный контроль информации, предоставляемой решениям для анализа и защиты сетей. Потребность в улучшении методов сбора сетевого трафика без отключения сети привело к популяризации ответвителей сетевого трафика. С появлением аппаратных ответвителей трафика, фильтрующих и агрегирующих трафик на конкретных линиях, для анализа скоростных каналов стало возможно использовать уже имеющиеся средства.

Фильтрующие канальные ответвители трафика позволяют создавать передовые решения по защите, анализу и нормированию сетей в компаниях, стремящихся к поддержанию своих вычислительных сетей на самом высшем уровне.

О компании Fluke Networks

Компания Fluke Networks является лидером по поставке решений для управления производительностью сетей и приложений. Технологии компании позволяют предприятиям надежно и безопасно управлять распределенными критически-важными корпоративными приложениями по всей инфраструктуре. Продукты компании Fluke Networks увеличивают доступность приложений и сетей, оптимизируют производительность и уменьшают стоимость эксплуатации, как традиционных сетей, так и инфраструктур на основе использования IP протокола. Для получения дополнительной информации о полном перечне наших решений на основе ответвителей и коммутаторов, посетите страницу в Интернете по адресу www.fluke-networks.ru