Гибкий доступ к сетевому трафику с помощью комбинированных ответвителей сетевого трафика

Изменение среды передачи данных (медь или волокно), увеличение загрузки сети и потребность в подключении к сети различных устройств для ее анализа требуют повышения гибкости и возможностей настройки ответвителей сетевого трафика. Данное техническое описание покажет, как улучшенные функционал и управляемость нового поколения комбинированных ответвителей сетевого трафика компании Fluke Networks помогут обеспечить гибкость, повысить экономическую эффективность и совершенствовать процедуру подключения решений для тестирования, мониторинга и обеспечения безопасности сети в соответствии с требованиями рынка.

Содержание

FLUKE networks

Введение

Внедрение ответвителей сетевого трафика, решений для агрегации трафика с нескольких сетевых интерфейсов и его регенерации становится стандартом для обеспечения доступа к данным в современных сетях. Эти устройства заменяют Mirror или SPAN-порты, предоставляя доступ к трафику устройствам для обеспечения безопасности, анализа протоколов и приложений, контроля за доступом в Интернет и т.д.

Факторами, влияющими на внедрение широкого спектра решений для мониторинга и обеспечения безопасности, являются, сокращение времени простоя сети (MTTR) и соответствие требованиям нормативных документов, в том числе CALEA, Sarbanes-Oxley и др.

Типы ответвителей сетевого трафика, решений для агрегации и регенерации трафика, которые были выбраны и внедрены в определённых проектах, продиктованы рядом условий. Это – определенное количество требуемых входов и выходов, тип интерфейса сетевой карты (медный или оптический) в устройствах для мониторинга и анализа сети, а также скорость или тип сетевого соединения. В случаях реализации долгосрочных проектов или изменении потребностей в видении сети, данные устройства могут не соответствовать целям некоторых пользователей, что вызывает ограничение гибкости и повышение затрат на приобретение новых решений для анализа.

Изменение среды передачи данных (медь или волокно), увеличение загрузки сети и потребность в подключении к сети решений для ее анализа требуют повышения гибкости и возможностей настройки ответвителей сетевого трафика. Данное техническое описание покажет, как улучшенные функционал и управляемость нового поколения комбинированных ответвителей сетевого трафика компании Fluke Networks помогут обеспечить гибкость, повысить экономическую эффективность и совершенствовать процедуры внедрения решений для тестирования, мониторинга и обеспечения безопасности сети в соответствии с требованиям рынка.

Сеть: доступ к сетевому трафику для тестирования, оценки и обеспечения безопасности

Процесс доступа к трафику для их последующего анализа значительно усложнился со времён появления первых сетей передачи данных. Простота подключения решений для мониторинга и захвата данных к концентратору Ethernet или к модулю многостанционного доступа (MAU) Token Ring претерпела изменение в середине 90-х в связи с переходом на использование коммутаторов и необходимостью обеспечения видения и контроля за работой коммутируемых сетей.

В связи с усложнением структуры сетей производители устройств начали предлагать Mirror/SPAN порты, которые обеспечивали непосредственное дублирование кадров с определенных портов на порт, к которому подключалось устройство для мониторинга и анализа трафика. За несколько лет эти порты были значительно модернизированы – сначала они обеспечивали возможность контроля за трафиком, передаваемым в одном направлении через один порт. Впоследствии с их помощью можно было получать информацию о трафике, передаваемом в двух направлениях через один порт, группу портов или даже во всей VLAN.

Несмотря на эти преимущества, Mirror/SPAN-порты имеют ряд недостатков:

- Настройка SPAN-сессии ставит под угрозу работу сети.
- Возможное снижение производительности коммутатора во время запуска SPAN-сессии.
- Возможность избыточного трафика, направленного на SPAN-порт, и ограниченное количество доступных портов.

Ответвители сетевого трафика и агрегационные ответвители: альтернативные решения для доступа к трафику для тестирования, оценки и обеспечения безопасности сети

Развитие ответвителей сетевого трафика обеспечило пассивный последовательный (in-line)-доступ к определенным физическим каналам, что позволяет снизить риски, связанные с неправильной настройкой SPAN-портов или негативным влиянием на производительность коммутаторов. Многопортовые агрегационные ответвители трафика, объединяют данные, передаваемые по нескольким каналам или SPAN-портам, и воспроизводят его, предоставляя возможность контролировать трафик с нескольких каналов или точек наблюдения, используя одно устройство для анализа трафика.

Полнодуплексные ответвители сетевого трафика, которые предоставляют отдельные копии Rx (входящий) и Tx (исходящий) трафика из ответвлённых линий, могут использоваться дополнительно с агрегационными ответвителями – решение, агрегирующее Rx и Tx трафик перед их передачей устройству для анализа трафика. Многопортовые агрегационные ответвители также стали включать возможность регенерации трафика – копирование трафика с одного или двух портов и создание большого количества идентичных копий.

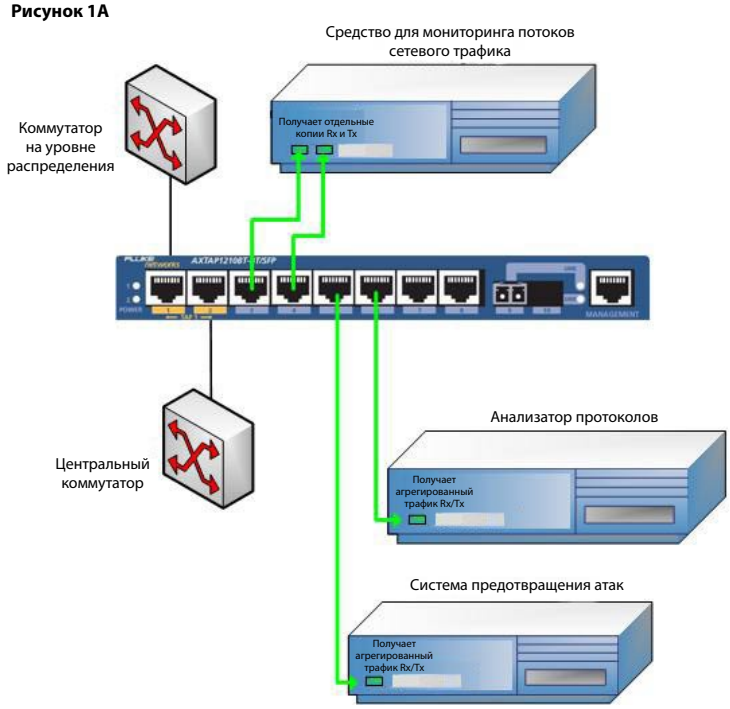
Все три категории ответвителей трафика, как правило, имеют возможность преобразовать среду передачи – например, к волоконно-оптическому сегменту или порту может быть подключено устройство для анализа трафика с медным интерфейсом и наоборот.

Мониторинг сетевого трафика, передаваемого в двух направлениях: баланс потребностей различных решений для анализа сети

Большая часть решений для анализа сети, включая большинство анализаторов протоколов и систем предотвращения сетевых атак, обычно имеют только один интерфейсный сетевой адаптер для захвата и анализа данных. Несмотря на ряд преимуществ традиционных полнодуплексных ответвителей по сравнению с Mirror/SPAN-портами, они не позволяют пользователю одновременно захватывать и просматривать обе стороны полнодуплексного сеанса обмена данными до тех пор, пока решение для анализа трафика не будет иметь два синхронизированных между собой интерфейса.

Агрегационные ответвители, объединяющие копии Rx (входящего) и Tx (исходящего) трафика позволяют решить данную проблему. Новое поколение продуктов обеспечивает статистический анализ трафика на основе двунаправленного потока обмена данными. В таких устройствах требуются отдельные копии Rx и Tx для нескольких интерфейсных адаптеров для мониторинга, а это вызывает конфликт при использовании существующих решений для мониторинга, которые имеют один интерфейс и требуют агрегацию Rx и Tx трафика.

Рисунок 1A

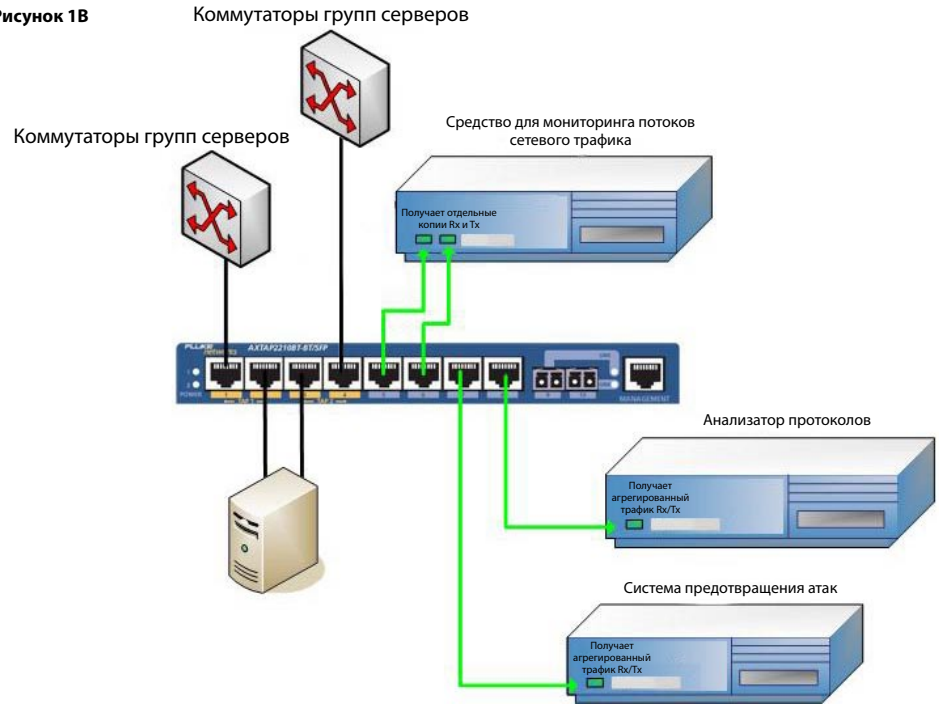


На рисунке 1A, комбинированный ответвитель передаёт отдельные копии Rx и Tx трафика устройству для анализа, контролирующему трафик, передаваемый в обоих направлениях. Анализатор протокола и IDS получают агрегированный трафик, так как эти решения поддерживают только один интерфейс и не могут анализазровать отдельно Rx и Tx.

Разные потребности этих неодинаковых решений становятся дилеммой, которую невозможно разрешить при помощи Mirror/SPAN-портов или обычных агрегационных ответвителей. Как просматривать, как сгруппированный, так и не сгруппированный трафик, передаваемый по одному или двум ответвленным каналам.

Решением проблемы являются комбинированные ответвители сетевого трафика. Изображённые на рисунке устройства могут ответвлять трафик как на один канал, так и на два канала. Их можно сконфигурировать для копирования Rx и Tx-трафика, передаваемого в канале, как на агрегированный порт, так и для передачи в виде двух отдельных не агрегированных потока данных. Пользователь по своему желанию может также регенерировать данные неограниченное количество раз.

Рисунок 1B



Двухканальный комбинированный ответвитель, изображённый на рисунке 1B, обеспечивает многократное копирование Rx и Tx трафика для агрегации и передачи на разные порты если это необходимо. В данном случае Rx обоих ответвлённых каналов передаётся из одного порта мониторинга, а агрегированныый Tx трафик передается через другой порт. В этом примере общая загрузка сети невысока, что позволяет агрегировать трафик из обоих каналов.

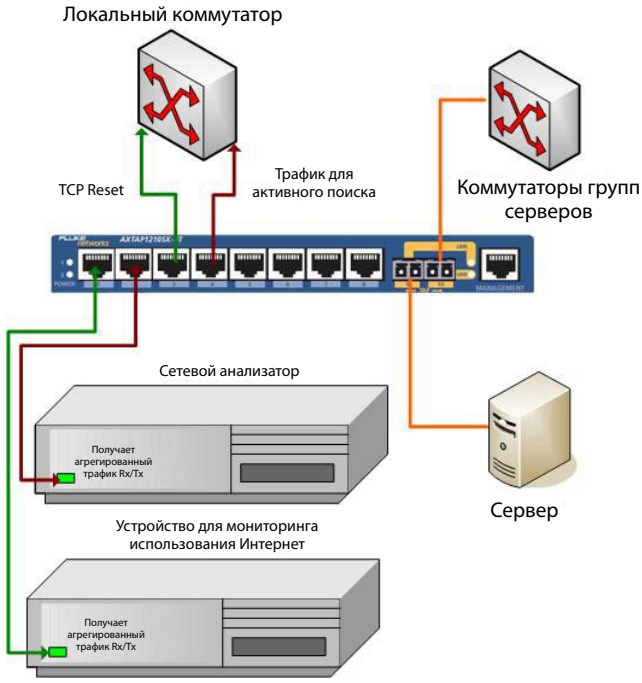
Передача трафика: Активный поиск и TCP reset в волоконно-оптических соединениях с одним сетевым адаптером

Ряд решений для анализа и мониторинга сетей имеет ценные функции, которые используют единственный интерфейсный адаптер и для отправки трафика в сеть и для анализа данных. Например, сетевой анализатор может создавать визуальную карту Visio подсети на основе трафика, полученного из ответвлённой линии, или устройство мониторинга использования Интернет может прервать сессию командой «TCP reset» и отправить ICMP сообщение нарушающему правила пользователю.

Это не возможно выполнить через большинство Mirror/SPAN-портов, которые не позволяют передавать трафик в сеть, несмотря на то, что данную возможность имели медные ответвители сетевого трафика с активированной передачей двунаправленного трафика. Волоконно-оптические линии ответвляются при помощи оптического разветвителя, характеристики которого позволяют передавать трафик обратно в ответвлённый канал непосредственно с интерфейса для мониторинга через ответвитель.

Комбинированные ответвители можно назвать удобным решением этой проблемы: теперь трафик может передаваться через единственный интерфейс через порт для мониторинга в ответвителе непосредственно локальному коммутатору. Входящий трафик на порту для мониторинга может быть заблокирован – таким образом, мы получаем надёжное решение, которое обеспечивает необходимую функциональность, но делает решение для мониторинга невидимым в сети для обеспечения необходимых мер безопасности.

Рис. 2



При высокой загрузке сети настройка комбинированных ответвителей для работы в режиме полногодуплексного подключения позволяет осуществлять анализ трафика на скорости канала.

Увеличение загрузки каналов: подбор ответвителей для обеспечения условий роста сетевого трафика

Анализ тенденций подтверждает – уровень загрузки каналов продолжает расти. Факторы, влияющие на эти тенденции – добавление новых пользователей, серверов, использование приложений, которые требуют больше пропускной способности.

Агрегационные ответвители, объединяющие копии Rx (входящего) и Tx (исходящего) трафика, являются приемлемым решением для мониторинга полнодуплексных каналов для использования с существующими решениями, которые имеют один интерфейс для мониторинга и требуют агрегированную копию Rx- и Tx-трафика.

Так как всё больше решений для тестирования, мониторинга и обеспечения безопасности сети имеют несколько интерфейсов для анализа в одном шасси, и загрузка полнодуплексных каналов начинает превышать 50%, в агрегационных ответвителях может наблюдаться потеря пакетов, что не делает данное решение непригодным для использования в данной ситуации.

Комбинированные ответвители обеспечивают новый подход сразу по нескольким направлениям – все достигается путем изменения функционала ответвителя трафика для соответствия возрастающей загруженности каналов без дополнительного инвестирования в оборудование для анализа. На рисунке 3A все подключенные устройства для анализа трафика получают агрегированный Rx- и Tx-трафик. На рисунке 3B показан ответвитель трафика, который был настроен для работы в сети с более высоким уровнем загрузки путем подключения дополнительного интерфейсного адаптера в одном из устройств для анализа сети. Ответвитель трафика работает в режиме без агрегации трафика и передает Rx- и Tx-трафик отдельно на каждый из интерфейсов устройства для мониторинга.

Потребность в информации и используемые решения для анализа сети: соответствие изменяющимся средам передачи данных

Увеличивающееся количество внедрённых в сети решений для анализа трафика и разные потребности ИТ групп, которым необходим доступ к сетевому трафику, стали причиной «борьбы» за SPAN-порты. Это способствовало появлению ответвителей трафика с несколькими выходными портами и многопортовыми регенераторами трафика, которые могут копировать трафик, передаваемый из ответвителей трафика или из SPAN-портов.

Рис. 3A – «до»

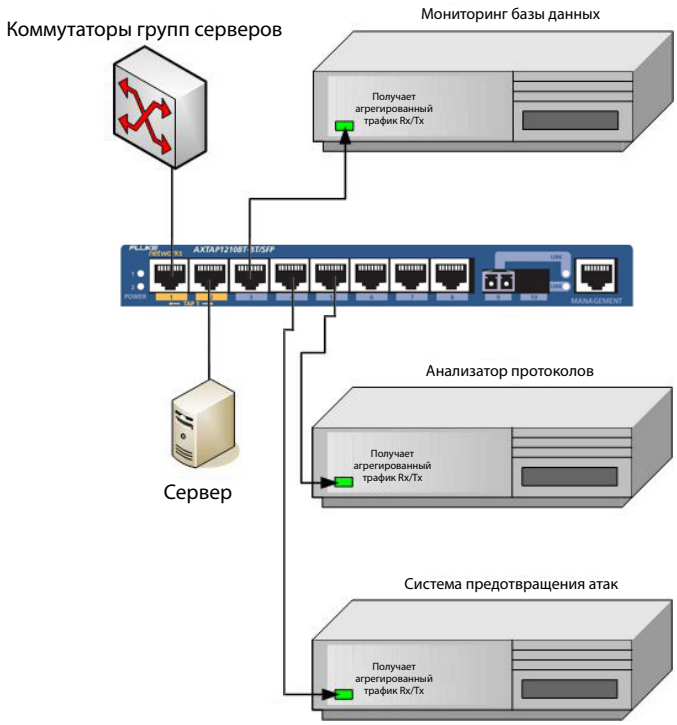
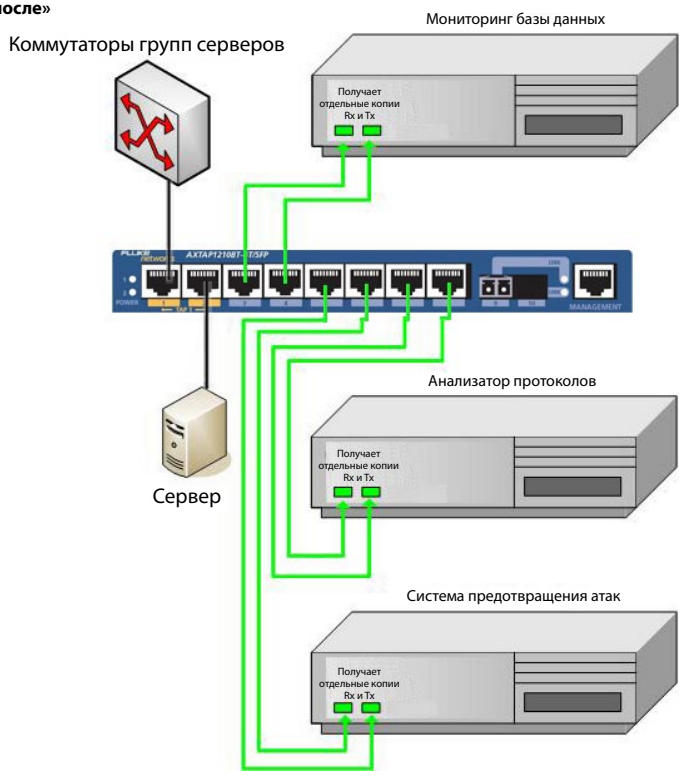


Рис. 3A – «после»



Данное решение эффективно, но оно имеет свои недостатки. Такие устройства предлагаются в определенной конфигурации с предустановленными входами, портами мониторинга и фиксированными типами среды передачи.

Комбинированные ответвители имеют специальные порты, предназначенные только для работы в качестве портов для последовательного подключения (in-line) к сети, и дополнительные порты, гибко настраиваемые как для работы в качестве портов ввода, так и в качестве портов для мониторинга. Дополнительная гибкость достигается благодаря двум SFP модулям, устанавливаемым на каждом комбинированном ответвителе, – что позволяет воспользоваться этими двумя портами для подключения к сети как на основе волоконно-оптического кабеля, так и медного кабеля.

Выводы

Доступ к сетевому трафику является растущей потребностью для различных ИТгрупп, которые полагаются на устройства для тестирования, мониторинга и безопасности для обеспечения высокой работоспособности и безотказной работы сети передачи данных. Использование гибких методов для доступа к трафику в условиях необходимости принятия решений, связанных с различным технологическим оборудованием, позволяет быть готовым к непредвиденным изменениям, которые возникают практически во всех ИТ инфраструктурах и архитектурах. Комбинированные ответвители сетевого трафика серии 1210 и 2210 от компании Fluke Networks отвечают растущим потребностям в доступе к передаваемому по сети трафику, и обеспечивают возможность снижения рисков, связанных с изменениями в сети. Во время оценки качества установки новых точек подключения к сети учтите потребность в переходе от агрегированных потоков данных к полнодуплексным. Кроме того, увеличение количества устройств для анализа влечёт за собой необходимость использования большего количества портов-повторителей, что является простой конфигурацией для этих устройств.

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.flukenetworks.com/taps**.

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks работает более чем в 50 странах мира. Чтобы найти ближайшее к вам представительство, зайдите на веб-сайт **www.flukenetworks.com/contact**.

Напечатано в США. 5/2007 3065162 D-RUS-N Ред. A