УДК 621.398:621.317:519.5

СРЕДСТВА МОНИТОРИНГА В СОВРЕМЕННЫХ СЕТЯХ СВЯЗИ: ОБЕСПЕЧЕНИЕ ПОЛНОЦЕННОГО ДОСТУПА К ТРАФИКУ

Ю.А. Демурджян, региональный директор компании Gigamon по региону РФ/СНГ/Северная Европа; julian.demurjian@gigamon.com

Ключевые слова: *мониторинг производительности сети, инфраструктура доступа, фильтрация трафика, СОРМ, универсальная выделенная шина.*

Введение. Управление большой и распределенной сетевой инфраструктурой требует столь же сложной системы управления и мониторинга. Доступность в режиме 24×7 и приемлемый уровень производительности имеют решающее значение для предоставления качественных услуг связи и дальнейшего их развития. Дополнительные требования на проектирование и управление сетями в области специализированных средств мониторинга (систем оперативно-розыскных мероприятий, СОРМ) накладывают также регулирующие органы.

Уже многие годы технические сотрудники и сетевые инженеры полагаются на традиционные инструменты, такие как анализаторы для мониторинга производительности сети, подключенные к портам активного коммутирующего оборудования с функцией SPAN. Однако рост трафика и увеличение скорости передачи данных в сети привели к тому, что мощности стандартных SPAN-решений явно не удовлетворяют современным требованиям по мониторингу и управлению трафиком. Новые решения в области DPI (Deep Packet Inspection), APM (Applications Performance Monitoring), IPS, QoS, а также возросшие объемы задач, связанных с обеспечением требований по СОРМ, заставляют искать более гибкие и производительные решения в этой области.

Ряд задач по доступу к трафику решался и до сих пор решается при помощи пассивных или активных сплиттеров, или, как их называют, TAP-устройств. Но практика показывает, что далеко не всегда для выделенной системы требуется полная копия трафика, которую снимает сплиттер, поэтому фильтрация все равно необходима. Естественно, операторы озабочены тем, как эффективно выстроить систему доступа к трафику и при этом выполнить следующие условия:

- обеспечить доступ к полному объему передаваемого трафика в рамках всей территориально распределенной сети без потери ее производительности;
- минимизировать нагрузку на активное коммутирующее оборудование;
- сохранить качество оптического и электрического сигналов в каналах;
- обеспечить эффективную фильтрацию снятого трафика в соответствии с задачами выделенных систем мониторинга;
- сохранить и продлить использование уже внедренных систем мониторинга в условиях непрерывного роста объема передаваемого трафика и увеличения пропускной способности каналов вплоть до 100 Гбит/с;
- и, что самое главное, уложиться в рамках оптимальных бюджетных параметров.

Традиционные технологии. Большинство производителей сетевого оборудования считают, что нескольких встроенных функций будет вполне достаточно для решения любых задач, связанных с мониторингом и доступом к трафику. Такими традиционными технологиями являются SPAN, RSPAN, ERSPAN, VACL.

Cisco SPAN. Функция SPAN (Switch Port ANalyzer) или ее аналог доступна во многих современных коммутаторах. Порт SPAN копирует данные из одного или нескольких портов-источников или VLAN. Работу SPAN иллюстрирует рис. 1, где данные внутри коммутаторов Cisco копируются из одного или нескольких порталов (в данном примере

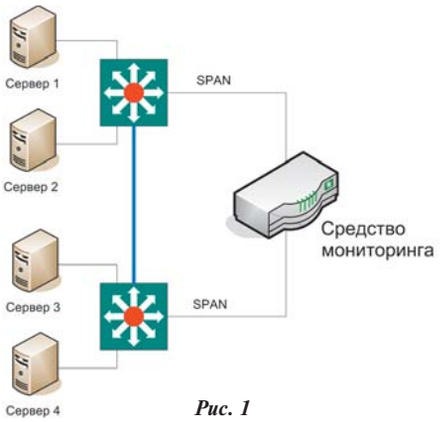

Рис. 1

это порты, в которые подключены серверы) в SPAN-порты, куда подключены средства мониторинга.

Коммутаторы Cisco могут поддерживать две SPAN-сессии на одном устройстве – для крупных инфраструктурных решений этого недостаточно. Таким образом, различные подразделения, отвечающие за разные задачи и использующие в своей постоянной работе специализированные средства мониторинга, конкурируют за доступ к таким портам практически на каждом узле, что создает дополнительную нагрузку на службы эксплуатации и ИТ.

Функция SPAN имеет и ряд ограничений. В частности, трафик, отобранный с одного порта, нельзя одновременно перенаправить на две разные SPAN-сессии или, например, нельзя одновременно собрать в одной SPAN-сессии трафик с VLAN-метками и без них. Однако же главным ограничением является производительность. Практика показывает, что коммутатор с перегруженными SPAN-сессиями может нестабильно работать вплоть до сбоя по основным задачам коммутации. Таким образом, SPAN-сессии хороши для точечного анализа в малых и средних системах, где потребности мониторинга невелики, но не годятся для применения в крупных телекоммуникационных сетях.

Cisco RSPAN. Функция RSPAN (Remote Switch Port ANalyzer) работает почти так же, как SPAN. Единственное дополнение – данные могут быть отправлены в порты на удаленных коммутаторах по коммутируемой среде с использованием VTP. На рис. 2 показано, что данные отбираются на коммутаторе и передаются через специализированный Reflector Port по RSPAN VLAN на удаленный узел, где расположена система мониторинга.

Существующие ограничения RSPAN позволяют организовать только два направления передачи снятого

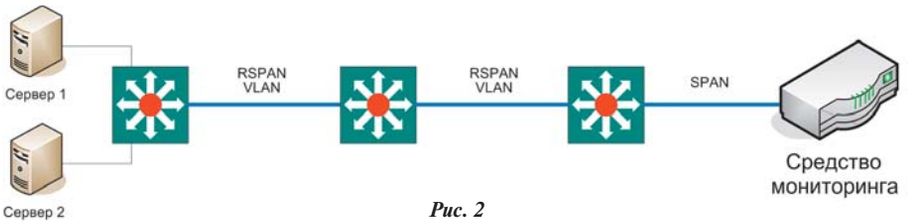

Рис. 2

трафика. Так же, как в SPAN, данные из одного источника (порта или VLAN) не могут быть разделены между двумя сессиями.

Cisco ERSPAN. Функция ERSPAN (Encapsulated Remote Switch Port ANalyzer) позволяет передавать данные с удаленных коммутаторов на средства мониторинга через IP-сеть. Для этого используется GRE-туннели, настроенные на соответствующих коммутаторах. ERSPAN поддерживается на коммутаторах Cisco только с Supervisor Engine 720 с PFC3A. Это означает, что данная функция доступна лишь на ряде моделей Catalyst 6500. Также эта функция еще не переведена на новую платформу Nexus.

Пакеты ERSPAN с пересчитанным CRC помечены 50-байт заголовком. Необходимо помнить, что ERSPAN не поддерживает фрагментированные кадры, поэтому все коммутаторы, участвующие в ERSPAN, должны быть настроены для поддержки Jumbo Frames, в противном случае все кадры размером более 1500 байт будут удалены. Как в других технологиях SPAN, в ERSPAN можно создать только два направления ERSPAN на одном коммутаторе.

Cisco VACL фактически является списком доступа (access-list) в инфраструктуре VLAN. VACL помогает преодолеть часть ограничений SPAN и дополнительно к этому позволяет отбирать трафик по таким критериям, как порт TCP или IP-адрес. VACL как списки доступа применяются только к данным в конкретном VLAN; они отделены от обычных ACL, которые используются в конфигурации маршрутизатора. Максимальное количество VACL всегда определяется текущим количеством настроенных VLAN на данном коммутаторе. Например, если настроено только пять VLAN, то можно создать только пять портов захвата VACL (VACL Capture Port).

Как правило, VACL используется для того, чтобы освободить ресурсы SPAN и тем самым обеспечить более полную систему мониторинга. Настройка VACL требует более подготовленных специалистов, так как основана на знаниях технологии Cisco Network Visibility.

Gigamon GigaVUE & Traffic Visibility Nodes. Gigamon предлагает решение, позволяющее более эффективно выстроить систему доступа к трафику. Gigamon GigaVUE & Traffic Visibility Nodes (узлы доступа к трафику) представляет собой специально разработанную технологию для создания полностью независимой инфраструктуры доступа к трафику. Ее назначение – обеспечить улучшенную видимость данных для всех задач мониторинга, включая также средства информационной безопасности, подключаемые в режиме in-line.

Решение позволяет подключаться к множеству сетевых соединений, агрегировать и отфильтровывать необходимые данные в точном соответствии с планом расположения систем мониторинга и их техническим назначением. Важно отметить, что вся обработка трафика в решениях Gigamon осуществляется на скоростях соединения. Максимальные задержки, которые не зависят от условий и сложности фильтрации, не превышают нескольких микросекунд.

Пользователи могут подключаться к SPAN, RSPAN, VACL, ERSPAN, а

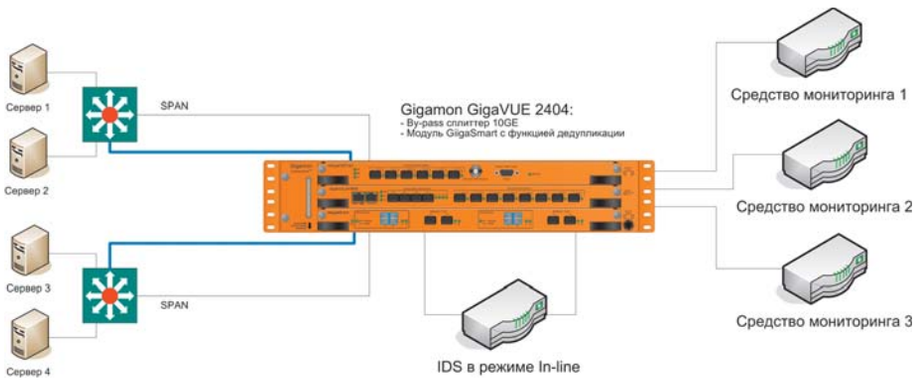

Рис. 3

также к существующей системе сплиттеров и тем самым обеспечить полную агрегацию технических средств доступа к трафику в единую не зависимую от транспортной сети систему. На рис. 3 представлено решение Gigamon GigaVUE 2404 со встроенным сплиттером 10GE.

Gigamon GigaVUE & Traffic Visibility Nodes можно считать основным компонентом инфраструктуры мониторинга в новых сетях – 1, 10, 40 Гбит/с, а в скором времени и 100 Гбит/с. Назовем основные преимущества решения:

- Устранение конкуренции при подключении к SPAN, RSPAN, ERSPAN. Решения Gigamon позволяют эффективно масштабировать одно подключение к этим ресурсам на множество исходящих сессий, форсированных дополнительной балансировкой.
- Обеспечение безопасного доступа к данным для мониторинга. Единожды снятый трафик более не влияет на производительность транспортной сети. Обработка, фильтрация, агрегация происходят на выделенных устройствах, обрабатывающих только копию первоначально снятого трафика.
- Сохранение доступа в сетях 10 Гбит/с для систем мониторинга, рассчитанных на скорость 1 Гбит/с. Возможно использования нескольких 1G-систем для анализа подключения 10 Гбит/с.
- Обеспечение полной прозрачности данных по асимметричной связи.
- Фильтрация любой области на уровнях 1–4, а также на основе определяемых пользователем специальных бинарных фильтров.
- Консолидация управления всей инфраструктурой доступа к трафику в единую систему. Все устройства могут быть соединены в общий стек и управляться с одной центральной консоли.
- Доступность расширенных функций, таких как Time Stamping, удаление ненужных заголовков, сокрытие пользовательских данных (пароли, данные кредитных карт и т.п.).

Flow Mapping. Ключевой технологией, которая позволяет реализовать указанные преимущества GigaVUE, является запатентованный Gigamon механизм обработки потоков Flow Mapping, обеспечивающий распределение трафика с любого входящего порта на любое количество исходящих портов на линейной скорости без потери данных. Данная технология существенно отличается от классической фильтрации, которая также доступна в решениях Gigamon.

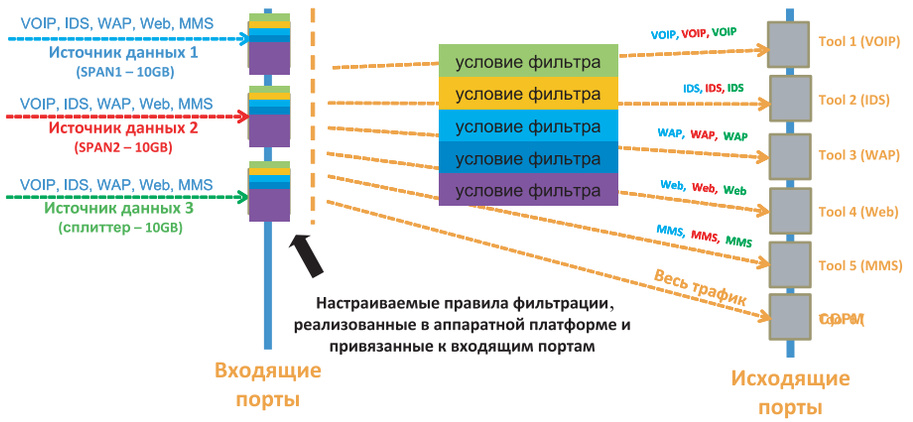

Рис. 4

Как только правило Flow Mapping создано, оно может быть привязано к одному или нескольким входящим портам. Это дает возможность для последующего динамического изменения потоков данных в соответствии с задачами мониторинга. При использовании классических порт-фильтров любое изменение правил фильтрации требует обновления настроек фильтров для каждого порта в отдельности. Дополнительно даже при наличии правила Flow Ping, привязанного к группе портов, возможно использование уникальных механизмов, таких как порт-коллектор (Port Collector) и полный проброс (Pass All). Каждое правило Gigamon Flow Mapping может быть снабжено дополнительным условием для коллектора. Этот механизм позволяет снять трафик, не попавший под все множество условий данного правила, и перенаправить его на любой другой порт для независимого анализа. Данная функция обеспечивает более точную подстройку правил или поиск трафика, по какой-то причине не попавшего в условия основного правила.

Механизм Pass All поддерживает параллельный съем полного объема трафика на входящем порту в обход привязанных к порту правил отбора Flow Mapping. Эта функция очень удобна при необходимости параллельного исследования исходного трафика разными системами мониторинга (например, при поиске неисправностей).

При планировании инфраструктуры доступа к трафику с использованием решений Gigamon достаточно определить ключевые места, где съем трафика даст максимально полную картину передаваемых данных. Решив эту задачу один раз, Gigamon GigaVUE & Traffic Visibility Node обеспечит полную обработку трафика, в том числе его многократное копирование, перераспределение, агрегацию и фильтрацию. Данная технология применима также в крупных территориально распределенных сетях, позволяя агрегировать необходимые средства контроля и мониторинга трафика в удобных центрах обработки данных, одновременно реализуя съем трафика в различных участках сети. Так как технология Flow Mapping осуществляет фильтрацию на входящих портах, то потребность в каналах связи при агрегации будет существенно оптимизирована.

Заключение. Объединяемые в централизованно управляемый стек решения Gigamon позволяют применять технологию Flow Mapping на всем множестве распределенных устройств. Правило может быть распространено на входящие порты, расположенные на разных физических устройствах, равно как и исходящие порты в одном правиле могут быть физически разрознены.

Построенная на базе решений Gigamon система доступа к трафику снимает существенную нагрузку с транспортных коммутаторов, предоставляя последним возможность решать задачи, для которых они и были спроектированы – передавать и коммутировать трафик.

Кроме того, различные подразделения оператора могут использовать систему Gigamon GigaVUE & Traffic Visibility Node для различных уникальных и порой не пересекающихся задач. Удобная система разграничения прав доступа к управлению системой позволяет ограничить выделенных пользователей до настройки конфигурации лишь тех портов, в которые непосредственно подключены их средства мониторинга и иные инструменты. Таким образом, решение Gigamon можно использовать как универсальную выделенную шину, не влияющую на работоспособность самой сети и скорость передачи трафика в ней.

Получено 13.03.12