SoftPI

В.В. Питутин

Что такое IPFIX?

IP Flow Information Export можно перевести как «Экспорт информации по IP потоку». Далее для краткости будем использовать сокращение **IPFIX**.

Протокол IPFIX фактически является развитием NetFlow протокола версии 9 компании Cisco Systems. Об особенностях протокола NetFlow и его различных версиях можно прочитать в статье компании SoftPI: "Что такое NetFlow" [1].

Протокол IPFIX принят Специальной комиссией интернет-разработок (Internet Engineering Task Force, IETF) и опубликован в ряде RFC документов, перечень которых приведен в таблице 1.

Таблица 1

Документ	Название	Краткое описание
RFC 3917	Требования к IPFIX *Requirements for IP Flow Information Export (IPFIX)*	Даются основные определения, используемые для IPFIX протокола: IP поток, точка наблюдения, измерительный процесс, потоковая запись и другие. Рассматриваются приложения, которые могут использовать IPFIX: учет использования сетевых ресурсов, анализ трафика, обслуживание трафика, обнаружение сетевых атак и вторжений, мониторинг качества сервиса (QoS). Рассматриваются параметры, для выделения потоков, требования к процессам измерения, экспорта, конфигурации процессов и общие требования.
RFC 5101	Описание IPFIX протокола *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*	Описывается формат IPFIX сообщения, связи с информационной моделью, транспортные протоколы (SCTP, UDP, TCP), требования по защите.
RFC 5102	Информационная модель для IPFIX *Information Model for IP Flow Information Export*	Описываются типы используемых полей для информационных элементов IPIX, структура информационных элементов, и приводится описание каждого информационного элемента.
RFC 5103	Экспорт двунаправленного потока используя IPFIX. *Bidirectional Flow Export Using IP Flow Information Export (IPFIX)*	Рассматривается экспортный метод для IPFIX протокола, основанный на понятии двунаправленного потока.
RFC 5153	Рекомендации по внедрению IPFIX *IP Flow Information Export (IPFIX) Implementation Guidelines*	Даются рекомендации по управлению шаблонами, экспортным процессом, процессом сбора данных, по использованию транспортного протокола, рекомендации по безопасности и расширению информационной модели.
RFC 5470	Архитектура IPFIX *Architecture for IP Flow Information Export*	Определяется архитектура для мониторинга, измерения и экспорта информации по IP потокам. Описываются отдельные компоненты архитектуры и их функции.
RFC 5471	Рекомендации для тестированию IPFIX *Guidelines for IP Flow Information Export (IPFIX) Testing*	Указаны требования по тестированию системы сбора информации о IP потоках на базе протокола IPFIX.
RFC 5472	Применимость IPFIX	Описывается, как типовые приложения могут использовать IPFIX протокол, показаны возможности и ограничения этого

	IP Flow Information Export (IPFIX) Applicability	протокола. Также рассматриваются вопросы взаимосвязи IPFIX с другими протоколами (PSAMP, RMON, IPPM, AAA).
RFC 5473	Уменьшение избыточности IPFIX и выборка пакетов *Reducing Redundancy in IP Flow Information Export (IPFIX) and Packet Sampling (PSAMP) Reports*	Описывается протокол выборки пакетов для уменьшения полосы пропускания, необходимой для экспорта информации о потоках с использованием IPFIX протокола.
RFC 5474	Структура для выборки пакетов и отчетности *A Framework for Packet Selection and Reporting*	Описывается структура для протокола выборки пакетов (PSAMP). Функциями этого протокола являются выбор пакетов из потока в соответствии с стандартизированными фильтрами, формирование информации по отобранным пакетам и экспорт этой информации на коллектор.
RFC 5475	Технологии выборки и фильтрации для отбора IP пакетов *Sampling and Filtering Techniques for IP Packet Selection*	Описывается технологии выборки и фильтрации для IP пакетов. Дается классификация схем выборки и определяются параметры, для описания наиболее общих схем выборки пакетов.
RFC 5610	Экспорт типовой информации для информационных элементов IPFIX *Exporting Type Information for IP Flow Information Export (IPFIX) Information Elements*	Описывается общий механизм для кодирования полного набора параметров, доступных для определения информационных элементов внутри информационной модели IPFIX.
RFC 5655	Спецификация формата файла для IPFIX *Specification of the IP Flow Information Export (IPFIX) File Format*	Описывается формат файла для хранения потоковых данных IPFIX протокола.
RFC 5815	Определение управляемых объектов для IPFIX *Definitions of Managed Objects for IP Flow Information Export*	Описываются два MIB модуля для мониторинга IPFIX устройств, включая экспортеров и коллекторов, которые содержат стандартизируемые методы выборки пакетов.
RFC 5982	Посредник IPFIX: постановка задачи *IP Flow Information Export (IPFIX) Mediation: Problem Statement*	Информация IPFIX протокола может использоваться одновременно различными приложениями. Но эти приложения предъявляют различные требования к измерительному процессу. Для решения такой проблемы предлагается использование IPFIX посредника (Mediation), описание которого и приводится в данном документе.

В RFC 3917 дается определение IP потока:

IP поток *— это набор IP пакетов, проходящих через точку наблюдения в сети за определенный временной интервал. Все пакеты, принадлежащие к определенному потоку имеют перечень общих свойств. Каждое из свойств определятся как результат применения функции к значениям из:*

1. *одного или более пакетных полей заголовка (например, IP адрес приемника пакетов), поля транспортного заголовка (например, номер порта приемника пакетов) или поля заголовка приложения (например, поля заголовка RTP протокола).*
2. *одного или более параметра самого пакета (например, число MPLS меток и т.п.).*
3. *одного или более полей, извлеченных из тела пакета (например, IP адрес следующего маршрутизатора (hop), исходящий интерфейс и т.п.).*

Пакет считается принадлежащим к потоку, если он полностью соответствует всем параметрам потока.

Пример сетевого потока через сетевой интерфейс 1 из IP порта 61418 с IP адресом

10.10.5.24 на IP порт 5060 сетевого устройства с IP адресом 195.5.0.118 с использованием протокола UDP и типом сервиса, равным 0, показан на рисунке 1.

Приведем определения еще нескольких понятий из RFC 3917, которые часто встречаются в документах по IPFIX.

Точка наблюдения *- это место в сети, в которой происходит отслеживание IP пакетов. В качестве примеров можно привести: порт маршрутизатора, набор интерфейсов (физических или логических) маршрутизатора, сетевой интерфейс компьютера и т.п.*

Процесс измерения *генерирует потоковые записи. Входной информацией для этого процесса являются пакетные заголовки, наблюдаемые в точке наблюдения и тело (содержимое) пакета. Процесс измерения состоит из набора функций, которые включают захват, определение временных параметров, выборку, классификацию пакетных заголовков и администрирование потоковых записей. Администрирование потоковых записей может включать создание новых записей, обновление уже существующих, вычисление статистических параметров потока, извлечение дополнительных потоковых параметров, определение окончания потока, передача потоковых записей в экспортный процесс и удаление потоковых записей.*

Потоковая запись *содержит информацию о конкретном потоке, параметры которого определялись в точке наблюдения.*

Экспортный процесс *посылает потоковые записи на один или более коллекторных процессов.*

Коллекторный процесс *получает потоковые записи от одного или более экспортных процессов. Коллекторный процесс может сохранять полученные потоковые записи для их дальнейшей обработки.* Программы, которые выполняют коллекторный процесс называются коллекторами (IPFIX коллекторами или NetFlow коллекторами).

Рисунок 1

Сферы применения IPFIX

Основные сферы применения IPFIX протокола перечислены в RFC 3917 и более подробно рассматриваются в RFC 5472. Основными сферами применения этого протокола считаются:

- учет использования сетевых ресурсов,
- анализ трафика,
- администрирование трафика,
- обнаружение сетевых атак и вторжений,
- мониторинг качества сервиса (QoS).

Рассмотрим каждое из них более подробно.

Учет использования сетевых ресурсов

Использование IPFIX записей обеспечивает точную информацию по принятому и переданному сетевому трафику конкретным пользователем сетевых ресурсов. Однако, в большинстве случаев IPFIX протокол, как и NetFlow, не позволяют определить какое конкретно приложение использовалось пользователем. В тоже время у интернет провайдеров существует тенденция к предоставлению безлимитного доступа с применением дополнительных тарифов за

пользование какими-то специальными интернет-сервисами (IPTV, IP телефония, видео по запросу и т.п.). Поэтому использование IPFIX протокола в биллинговых целях актуально только при использовании тарифов за принятый/переданных объем данных.

Согласно RFC 5472 учет использованных сетевых ресурсов может основываться на потоках между IP адресами или на классифицируемых сервисах. В первом случае используются следующие информационные элементы (поля):

- IP адрес источника потока (sourceIPv4Address или sourceIPv6Address – при использовании, соответственно, IPv4 или IPv6)*,
- IP адрес приемника потока (destinationIPv4Address или destinationIPv6Address — при использовании, соответственно, IPv4 или IPv6)*,
- тип используемого протокола (protocolIdentifier),
- номера портов источника и приемника (udpSourcePort, udpDestinationPort)**.

* В RFC 5472 упоминаются только поля для IPv4, почему-то совершенно забыв об IPv6, который на момент опубликования этого стандарта (март 2009) уже использовался в ряде стран, особенно в азиатских.

** Для биллинговых целей информация о номерах портов, как правило, не актуальна, так как далеко не всегда однозначно можно точно определить по номеру порта приложение (сервис), которое его использует. Поэтому, как правило, биллинговыми системами используется общий трафик без его деления на потоки по признаку использования конкретного порта. И также странно, что авторы стандарта RFC 5472 предлагают использовать номера портов только UDP протокола, не упоминая, например, TCP протокол.

Во втором случае должны использоваться следующие информационные элементы:
точка кода дифференцированных услуг (Differentiated Services Code Point) — (ipDiffServCodePoint) и IP адреса источника и приемника (sourceIPv4Address, destinationIPv4Address).

Базовыми элементами, необходимыми для учета предоставленных сетевых ресурсов в обоих случаях являются количество переданных в потоке пакетов, которые отображаются в информационных элементах packetTotalCount, octetTotalCount.

Описание всех используемых информационных элементов в IPFIX протоколе смотрите далее в этой статье (таблицы 2 и 3).

Следует также заметить, что авторами RFC 5472 считается, что IPFIX протокол не обеспечивает достаточной надежности, которая определена для биллинговых систем в RFC 2975 [2] и он имеет ряд ограничений:

- **Возможность потери записей**. IPFIX протокол может использовать в качестве транспортного протокола: UDP, TCP, SCTP. Учитывая то, что в UDP протоколе отсутствует подтверждение доставки пакетов, рекомендуется использовать протоколы TCP или SCPT. В тоже время большинство известных производителей используют в своих устройствах для передачи IPFIX данных только UDP протокол. Например, в коммутаторах Ethernet Routing Switch 4500, 5000, 8300, 9600 (Avaya – Nortel) по состоянию на 2011 год для экспорта IPFIX данных используется UDP протокол через 9995 порт [3, 4].

Для справки заметим, что в соответствии с RFC 5101 передача IPFIX данных должна выполнять с помощью одного из протоколов: SCTP, TCP, UDP, используя порт 4739 или 4740 — для защищенного соединения. При этом, если для передачи данных используется UDP протокол, то он должен выполняться вместе с DTLS протоколом (Datagram Transport Layer Protocol). Если для передачи данных используется TCP протокол, то он должен выполняться вместе с TLS протоколом (Transport Layer Security).

- **Сетевые сбои**. IPFIX протокол позволяет использование нескольких Коллекторов для одного Экспортера, но не определяет никаких требований по использованию множества коллекторов для их устойчивой работы в случае сетевых сбоев.
- **Обнаружение и исключение дублирующих записей**. Подобная функция не поддерживается IPFIX протоколом.

- **Подтверждение о приеме на уровне приложений**. IPFIX протокол не поддерживает контроля за процессами измерения и экспорта приложениями высшего уровня. Подтверждение о приеме на уровне приложения является необходимым для информирования Экспортера в случае, когда приложение не может обработать данные, экспортируемые с использованием IPFIX протокола. Такая функциональность не поддерживается.

Анализ трафика

Информация, собранная с использованием IPFIX протокола за большой период времени может использоваться для отслеживания и прогнозирования роста сети и ее производительности. Это является необходимой для анализа тенденций в сети и сетевого планирования. Параметры, которые представляют интерес, определяются конкретным объектом анализа. В качестве таких параметров можно указать: продолжительность потока, объем переданной в потоке информации, используемые протоколы и сервисы (порты), количество пакетов определенного типа и другие.

Отдельный анализ используемых протоколов и сервисов может быть выполнен путем установки соответствующих Потоковых Ключей. Протоколы могут быть разделены с помощью информационного элемента (ИЭ): protocolIdentifier.

Информацию об используемых сервисах можно получить из номеров портов (destinationTransportPort, sourceTransportPort, udpSourcePort, udpDestinationPort, tcpSourcePort, tcpDestinationPort). Если номера порта недостаточно для определения используемого сервиса, то для его определения может потребоваться остальная часть пакета.

Пакетная загрузка может быть определена с использованием ИЭ ipPayloadPacketSection.

Продолжительность потока можно вычислить следующим образом:
flowEndMicroseconds - flowStartMicroseconds.
Вместо микросекунд могут использоваться аналогичные ИЭ с другими единицами измерения.

Число пакетов и число байт (октетов) в потоке можно определить на основании ИЭ: packetTotalCount, octetTotalCount.

Администрирование трафика

Целью администрирования трафика является оптимизация сетевых ресурсов и параметров трафика. Типовыми параметрами являются:

- пропускная способность канала,
- загрузка между определенными сетями, узлами;
- число, размеры и точки входа/выхода активных потоков;
- маршрутизирующая информация.

Объемы потоков в пакетах и байтах можно получить из ИЭ: packetTotalCount и octetTotalCount. Загрузка физического канала может быть получена благодаря использованию ИЭ (egressInterface или ingressInterface) и потоковых счетчиков packetTotalCount и octetTotalCount.

Загрузка между определенными сетевыми узлами может быть получена подобным путем, если интерфейс сетевого узла получает трафик только от одного соседнего узла. Если параметры входящего интерфейса являются недостаточными для однозначной идентификации соседнего узла, следует использовать поля заголовка IP пакета (например, sourceMacAddress), которые можно добавить в качестве потоковых ключей.

Информационный элемент observedFlowTotalCount обеспечивает информацией о количестве потоков для наблюдаемого домена с момента последней инициализации измерительного процесса. Если анализировать значение этого ИЭ через определенные промежутки времени, то фактически можно определить количество активных потоков в течение этих временных промежутков.

Обнаружение сетевых атак и вторжений

Одним из применений IPFIX протокола является обнаружение на основе его данных сетевых атак и вторжений. Однако, это достаточно сложный процесс, так как хакеры быстро подстраиваются под существующие системы обнаружения, пытаясь сделать свои атаки незаметными и более изощренными. В тоже время необычное изменение трафика не всегда является результатом злонамеренных действий. Трафик может резко измениться и в результате действия легитимных пользователей или ошибок в конфигурации сетевых устройств. Теоретически вся информация о трафике на IP уровне является доступной. Эти данные позволяют либо напрямую обнаруживать аномальные явления в сети или могут служить основой для создания более комплексных параметров, по которым можно обнаружит сетевые атаки.

В зависимости от типа атаки могут использоваться различный набор метрик. Внезапное резкое возрастание трафика может служить одном из признаков начала атаки. Весь объем трафика может отслеживаться с помощью ИЭ packetTotalCount или octetTotalCount. Число активных потоков можно определить с помощью параметра observedFlowTotalCount.

Внезапное увеличение потоков от различных источников на один из приемников пакетов может быть вызвано атакой на определенный хост или сетевой узел путем использования фальшивых адресов. Число потоков от или на определенную сеть (хосты) может быть выявлено за счет анализа адресов источников и приемников, принятых в качестве потоковых ключей, и числа активных потоков, как упоминалось выше. Множество потоков на один и тот же IP адрес, но различные порты, или множество потоков на один и тот же порт ряда сетевых устройств может быть индикатором вертикального или горизонтального сканирования портов. Число потоков на различные порты может определяться с помощью следующих ИЭ: udpSourcePort, udpDestinationPort, tcpSourcePort, tcpDestinationPort.

Необычное соотношение TCP-SYN к TCP-FIN пакетов может говорить о SYN флудинге (flooding). О числе SYN и FIN пакетов можно судить по ИЭ: tcpSynTotalCount и tcpFinTotalCount.

Сетевые "черви" могут быть обнаружены только путем детального изучения содержимого пакетов. И о них невозможно судить по параметрам трафика, а можно определить с использованием ИЭ ipPayloadPacketSection [5].

Следует учитывать, что количество ресурсов, необходимых для измерения, увеличивается с уровнем, требуемым для обнаружения атак. В данном случае могут быть полезны технологии многоступенчатого анализа, то есть применение более глубокого анализа, если сетевое поведение отличается от шаблонного. Для наблюдения за трафиком с целью обнаружения сетевых атак рекомендуется использовать методы фильтрации, которые описываются в RFC 5475.

Отнесение принадлежности IP адресов, участвующих в потоках, может быть полезным для определения корректности сетевого поведения. Корреляция данных из нескольких точек наблюдения позволяет оценить распространение атаки и помочь в локализации ее источника.

В тоже время сбор информации о потоках со всевозможных точек наблюдения часто является нереальным из-за ограничений на ресурсы. Следовательно, необходимо выбирать метрики, которые бы позволяли точно определять требуемые сетевые события при использовании минимальных ресурсов.

Во многих случаях использование только необработанных данных из IPFIX протокола недостаточно для выявления сетевых событий. Например, сравнение числа SYN и FIN пакетов за определенный интервал времени можно интерпретировать как непрерывную SYN атаку, но которая не очевидна из необработанных пакетов или потоковых данных. Дополнительные метрики, подобные коммулятивным суммам различных счетчиков, распределения пакетных атрибутов или спектр коэффициентов, должны использоваться для идентификации различных типов атак.

Для того чтобы обнаружить атаку на этапе ее зарождения полезно обрабатывать данные сразу же после их получения для формирования важных метрик, служащих для обнаружения атаки. Предварительная обработка "сырых" пакетов и данных потока уже в самом устройстве

может ускорить процесс обнаружения и уменьшить количество данных для экспорта. Кроме того, возможна непосредственная передача извлекаемых метрик путем определения соответствующих ИЭ. Желателен немедленный экспорт данных в случае потенциальной угрозы.

Эффективное обнаружение вторжений возможно при одновременном использовании функциональностей IPFIX и AAA (**А**вторизация, **А**утентификация, **А**ccounting – учет используемых ресурсов). Обычно функции AAA выполняют RADIUS сервера. Информацию по протоколу RADIUS можно посмотреть, например, в [6].

Мониторинг качества сервиса (QoS)

Мониторинг качества сервиса (quality of service) является одним из приложений IPFIX протокола. Типовыми параметрами качества сервиса являются потери, односторонняя и двусторонняя задержки (one-way и round-trip delay), вариация задержки (delay variation). Определение этих параметров требует обработки на уровне пакетов. Некоторые параметры качества сервиса требуют корреляции данных от нескольких точек наблюдения. Для этого необходима синхронизация по времени измерительных процессов в этих точках. Кроме этого необходимо распознавать, что один и тот же пакет наблюдался в различных точках наблюдения. Это может быть сделано путем сбора частей содержимого пакета (заголовок пакета или части тела пакета), которые не изменялись на пути к приемнику. Основываясь на содержимом пакета, возможно определить, когда один и тот же пакет поступил в другую точку наблюдения. Для уменьшения количества измеряемых данных возможно вычисление уникального пакетного идентификатора на основе содержимого пакета.

Информационные элементы IPFIX

Для IPFIX протокола информационные элементы с 1 по 127 в большинстве идентичны тем, которые используются в протоколе NetFlow версии 9 [7].

Дополнительный объем информационных элементов зарезервирован с 128 до 32767. Часть из них задействованы.

Перечень информационных элементов IPFIX протокола с 1 по 127 в соответствии RFC 5102 и соответствующих полей протокола NetFlow версии 9 приведены в таблице 2.

Таблица 2

ID	Информационный элемент в NetFlow v.9	Информационный элемент в IPFIX	Описание
1	IN_BYTES	octetDeltaCount	Входящий счетчик с длиной N x 8 бит для количества байт, связанных с IP потоком.
2	IN_PKTS	packetDeltaCount	Входящий счетчик с длиной N x 8 бит для количества пакетов, связанных с IP потоком.
3	FLOWS	RESERVED	Количество потоков, которое агрегируется. По умолчанию 4.
4	PROTOCOL	protocolIdentifier	IP протокол
5	TOS	ipClassOfService	Тип Сервиса для входящего интерфейса
6	TCP_FLAGS	tcpControlBits	Совокупность всех TCP флагов для этого потока
7	L4_SRC_PORT	sourceTransportPort	Номер порта TCP/UDP источника: FTP, Telnet и т.п.
8	IPV4_SRC_ADDR	sourceIPv4Address	Адрес источника данных IP протокола версии 4
9	SRC_MASK	sourceIPv4PrefixLength	Маска источника данных

10	INPUT_SNMP	ingressInterface	Индекс входящего интерфейса; по умолчанию 2, но могут использоваться и более высокие значения.
11	L4_DST_PORT	destinationTransportPort	Номер порта TCP/UDP приемника: FTP, Telnet и т.п.
12	IPV4_DST_ADDR	destinationIPv4Address	Адрес приемника данных протокола IP версии 4
13	DST_MASK	destinationIPv4PrefixLength	Маска приемника данных
14	OUTPUT_SNMP	egressInterface	Индекс исходящего интерфейса; по умолчанию 2, но могут использоваться более высокие значения.
15	IPV4_NEXT_HOP	ipNextHopIPv4Address	IPv4 адрес следующего маршрутизатора (next-hop router)
16	SRC_AS	bgpSourceAsNumber	Номер автономной системы BGP источника. Значение по умолчанию: 2. Также может быть и 4
17	DST_AS	bgpDestinationAsNumber	Номер автономной системы BGP приемника. Значение по умолчанию: 2. Также может быть и 4
18	BGP_IPV4_NEXT_HOP	bgpNexthopIPv4Address	IP адрес следующего маршрутизатора в BGP домене
19	MUL_DST_PKTS	postMCastPacketDeltaCount	Счетчик групповых исходящих IP пакетов с длиной N x 8 бит для пакетов, связанных с IP потоком
20	MUL_DST_BYTES	postMCastOctetDeltaCount	Счетчик групповых исходящих IP байт с длиной N x 8 бит для байтов, связанных с IP потоком
21	LAST_SWITCHED	flowEndSysUpTime	Системное время работы, при котором последний пакет в этом потоке был скоммутирован.
22	FIRST_SWITCHED	flowStartSysUpTime	Системное время работы, при котором первый пакет в этом потоке был скоммутирован.
23	OUT_BYTES	postOctetDeltaCount	Исходящий счетчик с длиной N x 8 бит для количества байт, связанных с IP потоком
24	OUT_PKTS	postPacketDeltaCount	Исходящий счетчик с длиной N x 8 бит для числа пакетов, связанных с IP потоком.
25	MIN_PKT_LNGTH	minimumIpTotalLength	Минимальная длина IP пакета для входящих пакетов потока
26	MAX_PKT_LNGTH	maximumIpTotalLength	Максимальная длина IP пакета для входящих пакетов потока
27	IPV6_SRC_ADDR	sourceIPv6Address	IPv6 адрес источника данных
28	IPV6_DST_ADDR	destinationIPv6Address	IPv6 адрес приемника данных
29	IPV6_SRC_MASK	sourceIPv6PrefixLength	Длина маски IPv6 источника данных
30	IPV6_DST_MASK	destinationIPv6PrefixLength	Длина маски IPv6 приемника данных
31	IPV6_FLOW_LABEL	flowLabelIPv6	Ярлык потока IPv6, как определено в RFC 2460
32	ICMP_TYPE	icmpTypeCodeIPv4	Тип пакета межсетевого протокола управляющих сообщений (Internet Control Message Protocol - ICMP); выводятся как: ((ICMP Type*256) + ICMP code)
33	MUL_IGMP_TYPE	igmpType	Тип пакета протокола управления группами Интернет (Internet Group Management Protocol - IGMP)
34	SAMPLING_INTERVAL	RESERVED	Используется для выборочного потока NetFlow. Частота, с которой выбираются пакеты. Т.е. 100 будет означать, что выбирается каждый 100-й пакет.
35	SAMPLING_ALGORITHM	RESERVED	Тип алгоритма, используемого для выборки NetFlow: 0x01 — детерминированная выборка; 0x02 — случайная выборка.

36	FLOW_ACTIVE_TIMEOUT	flowActiveTimeout	Величина таймаута (в секундах) для записей неактивного потока в кэш NetFlow.
37	FLOW_INACTIVE_TIMEOUT	flowIdleTimeout	Величина таймаута (в секундах) для записей неактивного потока в NetFlow кэше.
38	ENGINE_TYPE	RESERVED	Тип потока коммутационной машины: RP=0, VIP/Linecard=1
39	ENGINE_ID	RESERVED	Идентификатор коммутационной машины
40	TOTAL_BYTES_EXP	exportedOctetTotalCount	Счетчик с длиной N x 8 бит для байт для количества байт экспортируемых Доменом Наблюдения
41	TOTAL_PKTS_EXP	exportedMessageTotalCount	Счетчик с длиной N x 8 бит для байт для количества пакетов экспортируемых Доменом Наблюдения
42	TOTAL_FLOWS_EXP	exportedFlowRecordTotalCount	Счетчик с длиной N x 8 бит для байт для количества потоков экспортируемых Доменом Наблюдения
43	RESERVED		
44	IPV4_SRC_PREFIX	sourceIPv4Prefix	Префикс адреса IPv4 источника (специально для архитектуры Catalyst)
45	IPV4_DST_PREFIX	RESERVED	Префикс адреса IPv4 приемника (специально для архитектуры Catalyst)
46	MPLS_TOP_LABEL_TYPE	mplsTopLabelType	MPLS Top Label Type: 0x00 UNKNOWN; 0x01 TE-MIDPT; 0x02 ATOM; 0x03 VPN; 0x04 BGP; 0x05 LDP
47	MPLS_TOP_LABEL_IP_ADDR	mplsTopLabelIPv4Address	Переадресуемый Эквивалентный Класс (Forwarding Equivalent Class) соответствующий верхней метки MPLS
48	FLOW_SAMPLER_ID	RESERVED	Идентификатор, показанный в “show flow-sampler”
49	FLOW_SAMPLER_MODE	RESERVED	Тип алгоритма, используемого для выборочных данных: 0x02 случайный выбор. Используется совместно с FLOW_SAMPLER_MODE
50	FLOW_SAMPLER_RANDOM_INTERVAL	RESERVED	Пакетный интервал, с которым осуществляется выборка. Используется совместно с FLOW_SAMPLER_MODE
51	RESERVED	RESERVED	
52	MIN_TTL	minimumTTL	Минимальное время жизни пакетов (TTL) для входящего потока.
53	MAX_TTL	maximumTTL	Максимальное время жизни пакетов (TTL) для исходящего потока.
54	IPV4_IDENT	fragmentIdentification	Идентификационное поле IPv4.
55	DST_TOS	postIpClassOfService	Байт типа сервиса, устанавливаемый для исходящего интерфейса.
56	SRC_MAC	sourceMacAddress	MAC адрес исходящего источника
57	DST_MAC	postDestinationMacAddress	MAC адрес входящего приемника
58	SRC_VLAN	vlanId	Идентификатор виртуальной ЛВС, связанный с входящим интерфейсом
59	DST_VLAN	postVlanId	Идентификатор виртуальной ЛВС, связанный с исходящим интерфейсом
60	IP_PROTOCOL_VERSION	ipVersion	Версия Интернет Протокола. Значение 4 — для IPv4, и 6 — для IPv6. Если отсутствует в шаблоне, значит, используется версия 4.
61	DIRECTION	flowDirection	Направление потока: 0 — входящий поток, 1 — исходящий

			поток.
62	IPV6_NEXT_HOP	ipNextHopIPv6Address	IPv6 адрес для маршрутизатора следующего перехода (скачка).
63	BPG_IPV6_NEXT_HOP	bgpNexthopIPv6Address	Ipv6 адрес маршрутизатора следующего перехода в BGP домене.
64	IPV6_OPTION_HEADERS	ipv6ExtensionHeaders	Битово-кодируемое поле, идентифицирующее дополнительные заголовки IPv6, обнаруженные в потоке.
65	RESERVED	RESERVED	
66	RESERVED	RESERVED	
67	RESERVED	RESERVED	
68	RESERVED	RESERVED	
69	RESERVED	RESERVED	
70	MPLS_LABEL_1	mplsTopLabelStackSection	MPLS метка (ярлык) на 1-й позиции в стеке. Поле содержит в себе: 20 бит - MPLS метки, 3 EXP (экспериментальных) бита и 1 S бит (конец стека).
71	MPLS_LABEL_2	mplsLabelStackSection2	MPLS метка (ярлык) на 2-й позиции в стеке. Поле содержит в себе: 20 бит - MPLS метки, 3 EXP (экспериментальных) бита и 1 S бит (конец стека).
72	MPLS_LABEL_3	mplsLabelStackSection3	MPLS метка (ярлык) на 3-й позиции в стеке. Поле содержит в себе: 20 бит - MPLS метки, 3 EXP (экспериментальных) бита и 1 S бит (конец стека).
73	MPLS_LABEL_4	mplsLabelStackSection4	MPLS метка (ярлык) на 4-й позиции в стеке. Поле содержит в себе: 20 бит - MPLS метки, 3 EXP (экспериментальных) бита и 1 S бит (конец стека).
74	MPLS_LABEL_5	mplsLabelStackSection5	MPLS метка (ярлык) на 5-й позиции в стеке. Поле содержит в себе: 20 бит - MPLS метки, 3 EXP (экспериментальных) бита и 1 S бит (конец стека).
75	MPLS_LABEL_6	mplsLabelStackSection6	MPLS метка (ярлык) на 6-й позиции в стеке. Поле содержит в себе: 20 бит - MPLS метки, 3 EXP (экспериментальных) бита и 1 S бит (конец стека).
76	MPLS_LABEL_7	mplsLabelStackSection7	MPLS метка (ярлык) на 7-й позиции в стеке. Поле содержит в себе: 20 бит - MPLS метки, 3 EXP (экспериментальных) бита и 1 S бит (конец стека).
77	MPLS_LABEL_8	mplsLabelStackSection8	MPLS метка (ярлык) на 8-й позиции в стеке. Поле содержит в себе: 20 бит - MPLS метки, 3 EXP (экспериментальных) бита и 1 S бит (конец стека).
78	MPLS_LABEL_9	mplsLabelStackSection9	MPLS метка (ярлык) на 9-й позиции в стеке. Поле содержит в себе: 20 бит - MPLS метки, 3 EXP (экспериментальных) бита и 1 S бит (конец стека).
79	MPLS_LABEL_10	mplsLabelStackSection10	MPLS метка (ярлык) на 10-й позиции в стеке. Поле содержит в себе: 20 бит - MPLS метки, 3 EXP (экспериментальных) бита и 1 S бит (конец стека).
80	OUT_DST_MAC	destinationMacAddress	MAC адрес исходящего приемника
81	IN_SRC_MAC	postSourceMacAddress	MAC адрес входящего источника
82	IF_NAME	RESERVED	Сокращенное имя интерфейса, например: “FE1/0”
83	IF_DESC	RESERVED	Полное имя интерфейса, например: “"FastEthernet 1/0”
84	SAMPLER_NAME	RESERVED	Имя выборки потока
85	IN_PERMANENT	octetTotalCount	Счетчик текущего байта для постоянного потока

	_BYTES		
86	IN_ PERMANENT _PKTS	packetTotalCount	Счетчик текущего пакета для постоянного потока
87	RESERVED	RESERVED	
88	FRAGMENT_OFFSET	fragmentOffset	Величина фрагментного смещения для фрагментируемых IP пакетов
89	FORWARDING STATUS	RESERVED	Состояние переадресации, которое кодируется 2-я левыми битами в байте, а остальные 6 бит — указывают код причины переадресации.
90	RESERVED	mplsVpnRouteDistinguisher	Величина отличительного признака VPN маршрута соответствующей записи в таблице маршрутизации и переадресации VPN. Отличительный признак маршрута гарантирует, что подобный адрес может использоваться в нескольких различных MPLS VPN и что он может использоваться в BGP для передачи нескольких совершенно отличных маршрутов для этого адреса.
91-127		RESERVED	

Практически полное совпадение значений информационных элементов протокола IPFIX со значениями ИЭ протокола NetFlow версии 9 позволяет пользователям оборудования IPFIX использовать NetFlow коллекторы, которые поддерживают версию 9.

Перечень информационных элементов IPFIX протокола, начиная со 128 по 238 приведены в таблице 3.

Таблица 3

ID	Информационный элемент	Описание
128	BgpNextAdjacentAsNumber	Номер первой автономной системы (АС) на пути к IP адресу назначения. Путь определяется путем поиска IP адреса назначения потока в информационной базе маршрутизации BGP. Если информация о пути к автономной системе является доступной только для неупорядоченного набора АС, то величина данного информационного элемента равна 0.
229	BgpPrevAdjacentAsNumber	Номер последней автономной системы (АС) на пути от IP адреса источника. Путь определяется путем поиска IP адреса потока в информационной базе маршрутизации BGP. Если информация о пути для этого потока является доступной только для неупорядоченного набора АС (и не как упорядоченная последовательность АС), то величина информационного элемента будет 0. В случае асимметрии BGP, bgpPrevAdjacentAsNumber не может сообщать правильную величину.
130	ExporterIPv4Address	IP адрес v4, используемый процессом экспорта. Он используется коллектором для идентификации Экспортера в случаях, где идентификация Экспортера может быть скрыта за счет использования Прокси сервера.
131	ExporterIPv6Address	IP адрес v6, используемый процессом экспорта. Он используется коллектором для идентификации Экспортера в случаях, где идентификация Экспортера может быть скрыта за счет использования Прокси сервера.
132	DroppedOctetDeltaCount	Число байт (октетов) со времени предыдущего отчета в пакетах этого Потока, просмотренных обработчиком пакетов. Число байт включает IP заголовки и полезную информацию.
133	DroppedPacketDeltaCount	Число пакетов со времени предыдущего отчета в пакетах этого Потока, просмотренных обработчиком пакетов.
134	DroppedOctetTotalCount	Общее число байт в пакетах этого Потока, просмотренных обработчиком пакетов с момента инициализации процесса наблюдения до текущего момента. Число байт включает IP заголовки и полезную информацию.

135	DroppedPacketTotalCount	Общее число пакетов этого Потока, просмотренных обработчиком пакетов с момента инициализации процесса наблюдения до текущего момента.
136	FlowEndReason	Причина прерывания Потока.
137	CommonPropertiesId	Идентификатор набора общих свойств, который является уникальным для Наблюдаемого домена и транспортной сессии. Обычно этот информационный элемент используется для связи с информацией, получаемой в различных записях.
138	ObservationPointId	Идентификатор Точки наблюдения, который является уникальным для Наблюдаемого домена. Рекомендуется, чтобы этот идентификатор был также уникальным для IPFIX устройства. Обычно это информационный элемент используется для ограничения объема других информационных элементов.
139	IcmpTypeCodeIPv6	Тип и код сообщения IPv6 ICMP. Информация сообщается как: (ICMP*256)+ICMP код.
140	MplsTopLabelIPv6Address	IPv6 адрес системы, MPLS метка которой вызвала перенаправление Потока.
141	LineCardId	Идентификатор линейной платы, который является уникальным для IPFIX устройства в наблюдаемой точке. Обычно этот информационный элемент используется для ограничения объема информационных элементов.
142	PortId	Идентификатор линейного порта, который является уникальным для IPFIX устройства в точке наблюдения. Обычно этот информационный элемент используется для ограничения объема информационных элементов.
143	MeteringProcessId	Идентификатор процесса отслеживания потока, который является уникальным для IPFIX устройства. Обычно этот информационный элемент используется для ограничения других информационных элементов. Идентификаторы процесса обычно назначаются динамически. Отслеживаемый процесс может быть перезагружен с другим идентификатором.
144	ExportingProcessId	Идентификатор Экспортного процесса, который является уникальным для IPFIX устройства. Обычно этот информационный элемент используется для ограничения других информационных элементов. Идентификаторы процесса обычно назначаются динамически. Отслеживаемый процесс может быть перезагружен с другим идентификатором.
145	TemplateId	Идентификатор шаблона, который является локально уникальным внутри транспортной сессии и отслеживаемого домена. Идентификаторы шаблонов с 0 до 255 зарезервированы для набора Шаблонов, набора расширений шаблонов и других зарезервированных наборов еще до их создания. Идентификаторы шаблонов для наборов данных имеют номера с 256 до 65535.
146	WlanChannelId	Идентификатор канала протокола 802.11 (Wi-Fi).
147	WlanSSID	Сетевой идентификатор (SSID), используемый в сети 802.11 (Wi-Fi).
148	FlowId	Идентификатор потока, который является уникальным внутри отслеживаемого домена. Этот информационный элемент может использоваться для различия между Потоками, если ключи Потоков, такие как IP адреса и номера портов сообщаются в различных записях.
149	ObservationDomainId	Идентификатор отслеживаемого домена, который является локально уникальным в Экспортируемом процессе. Экспортируемый процесс использует идентификатор отслеживаемого домена для уникальной идентификации для процесса сбора отслеживаемого домена, где отслеживаются потоки. Рекомендуется, чтобы этот идентификатор был уникальным для IPFIX устройства. Величина 0 идентифицирует, что неопределенный отслеживаемый домен идентифицируется этим информационным элементом.
150	FlowStartSeconds	Абсолютная метка времени первого пакета в потоке, измеряемая в секундах.
151	FlowEndSeconds	Абсолютная метка времени последнего пакета в потоке, измеряемая в секундах.
152	FlowStartMilliseconds	Абсолютная метка времени первого пакета в потоке, измеряемая в миллисекундах.
153	FlowEndMilliseconds	Абсолютная метка времени последнего пакета в потоке, измеряемая в

		миллисекундах.
154	FlowStartMicroseconds	Абсолютная метка времени первого пакета в потоке, измеряемая в микросекундах.
155	FlowEndMicroseconds	Абсолютная метка времени последнего пакета в потоке, измеряемая в микросекундах.
156	FlowStartNanoseconds	Абсолютная метка времени первого пакета в потоке, измеряемая в наносекундах.
157	FlowEndNanoseconds	Абсолютная метка времени последнего пакета в потоке, измеряемая в наносекундах.
158	FlowStartDeltaMicroseconds	Это относительная метка времени действительная только внутри одного IPFIX сообщения. Она содержит отрицательный временной сдвиг относительно первого отслеживаемого пакета в этом Потоке относительно времени экспорта, определенного в заголовке IPFIX сообщения.
159	FlowEndDeltaMicroseconds	Это относительная метка времени, действительная внутри одного IPFIX сообщения. Она содержит отрицательный временной сдвиг последнего отслеживаемого пакета для этого Потока относительно к времени экспорта, определенного в заголовке IPFIX сообщения.
160	SystemInitTimeMilliseconds	Абсолютная метка времени в миллисекундах последней инициализации IPFIX устройства.
161	flowDurationMilliseconds	Определяет разницу во времени в миллисекундах между первым наблюдаемым пакетом в данном Потоке и последним наблюдаемым пакетом.
162	flowDurationMicroseconds	Определяет разницу во времени в микросекундах между первым наблюдаемым пакетом в данном Потоке и последним наблюдаемым пакетом.
163	observedFlowTotalCount	Общее число потоков наблюдаемых в Наблюдаемом Домене с момента инициализации (реининциализации) измерительного процесса для этой точки наблюдения.
164	ignoredPacketTotalCount	Общее число наблюдаемых IP пакетов, которое процесс изменения не обработал с момента инициализации (реинициализации) этого процесса.
165	ignoredOctetTotalCount	Общее число байт в наблюдаемых IP пакетах (включая и заголовок пакетов), которое процесс измерения не обработал с момента инициализации этого процесса.
166	notSentFlowTotalCount	Общее число потоковых записей, которое было сгенерировано процессом измерения и удалено процессом измерения или процессом экспорта вместо посылки их коллектору.
167	notSentPacketTotalCount	Общее число пакетов, которое было сгенерировано процессом измерения и удалено процессом измерения или процессом экспорта вместо посылки их коллектору. Существует несколько потенциальных причин для этого, включая дефицит ресурсов и специальные экспортные политики.
168	notSentOctetTotalCount	Общее число байтов, которое было сгенерировано процессом измерения и удалено процессом измерения или процессом экспорта вместо посылки их коллектору. Существует несколько потенциальных причин для этого, включая дефицит ресурсов и специальные экспортные политики.
169	destinationIPv6Prefix	Префикс IPv6 адреса приемника
170	sourceIPv6Prefix	Префикс IPv6 адреса
171	postOctetTotalCount	Определение этого информационного элемента является идентичным определению информационного элемента octetTotalCount, за исключением того, что он сообщает потенциально модифицируемую величину, которая осуществляется функцией промежуточного устройства (middlebox) после того, как пакет послан точкой наблюдения.

172	postPacketTotalCount	Определение этого информационного элемента является идентичным определению информационного элемента packetTotalCount, за исключением того, что он сообщает потенциально модифицируемую величину, которая осуществляется функцией промежуточного устройства (middlebox) после того, как пакет послан точкой наблюдения.
173	flowKeyIndicator	Этот набор битовых полей используется для пометки информационных элементов записей данных, которые служат Ключом Потока. Каждый бит представляет информационный элемент в записи данных с N-м битом, представляющим N-й информационных элемент. Бит, установленный, в 1 показывает, что соответствующий информационный элемент является Ключом Потока. Бит, установленный в 0, показывает, что он не используется. Если запись данных использует более чем 64 информационных элемента, соответствующий Шаблон должен быть создан так, чтобы все Ключи Потока находились среди первых 64 информационных элементов, поскольку flowKeyIndicator содержит только 64 бита. Если запись данных содержит меньше чем 64 информационных элемента, то биты в flowKeyIndicator, для которых нет информационных элементов, ДОЛЖНЫ иметь величину 0.
174	postMCastPacketTotalCount	Общее число исходящих групповых (multicast) пакетов посланных для пакетов этого Потока демоном (скрытым процессом) внутри наблюдаемого домена с момента инициализации измерительного процесса. Это свойство не обязательно должно наблюдаться в точке наблюдения, но может быть определено для других целей.
175	postMCastOctetTotalCount	Общее число байт в исходящих групповых (multicast) пакетах посланных для пакетов этого Потока групповым демоном (скрытым процессом) внутри наблюдаемого домена с момента инициализации измерительного процесса. Это свойство не обязательно должно наблюдаться в точке наблюдения, но может быть определено для других целей.
176	icmpTypeIPv4	Тип ICMP сообщения при IPv4 адресации
177	icmpCodeIPv4	Код ICMP сообщения при IPv4 адресации
178	icmpTypeIPv6	Тип ICMP сообщения при IPv6 адресации
179	icmpCodeIPv6	Код ICMP сообщения при IPv6 адресации
180	udpSourcePort	Идентификатор порта источника в UDP заголовке
181	udpDestinationPort	Идентификатор порта приемника в UDP заголовке
182	tcpSourcePort	Идентификатор порта источника в TCP заголовке
183	tcpDestinationPort	Идентификатор порта приемника в TCP заголовке
184	tcpSequenceNumber	Порядковый номер в TCP заголовке
185	tcpAcknowledgementNumber	Подтверждающий номер в TCP заголовке
186	tcpWindowSize	Поле размера окна в TCP заголовке. Если масштабирование TCP окна поддерживается, то это масштабирование должно быть известно для правильной интерпретации величины этой информации.
187	tcpUrgentPointer	Указатель срочности в TCP заголовке
188	tcpHeaderLength	Длина TCP заголовка. Следует заметить, что величина этого информационного элемента является различной в зависимости от величины поля Смещения Данных (Data Offset) в TCP заголовке. Поле Смещения Данных показывает длину TCP заголовка в единицах, равных 4 байтам. Этот информационных элемент определяет длину TCP заголовка в единицах байт.
189	ipHeaderLength	Длина IP заголовка. Для IPv6 величина этого информационного элемента равна 40.

190	totalLengthIPv4	Общая длина IPv4 пакета.
191	payloadLengthIPv6	Информационный элемент отображает величину поля Длина Данных (Payload Length) в заголовке IPv6.
192	ipTTL	Для IPv4 величина этого поля соответствует полю Время Жизни (Time to Live, TTL) в заголовке пакета. Для IPv6 — полю Ограничения Пересылок (Hop Limit) в заголовке пакета.
193	nextHeaderIPv6	Отображает поле Следующего Заголовка (Next Header) в заголовке IPv6 пакета.
194	mplsPayloadLength	Размер MPLS пакета без стека метки (label stack).
195	ipDiffServCodePoint	Величина Точки кода дифференцированных услуг (Differentiated Services Code Point (DSCP)) закодированная в поле Дифференцированных услуг (Differentiated Services). Поле Дифференцированных услуг определяет наиболее важные 6 бит поля Тип Сервиса (TOS) в IPv4 или поля Класс Трафика (Traffic Class) в IPv6. В этом элементе используется только 6 бит, поэтому значение элемента может быть в диапазоне 0 — 63.
196	ipPrecedence	Значение IP приоритета. Эта значение кодируется в первых трех битах поля Тип Сервиса (TOS) для IPv4 или поля Класс Трафика (Traffic Class) в IPv6
197	fragmentFlags	Фрагментация определяется флагами в заголовке пакета IPv4 или в заголовке фрагментации пакета IPv6
198	octetDeltaSumOfSquares	Сумма квадратов числа байт по входящему пакету с момента предыдущего отчета для этого Потока в Точке Наблюдения. Число байт включает IP заголовок и содержание пакета.
199	octetTotalSumOfSquares	Общая сумма квадратов числа байт по входящих пакетах для этого Потока в Точке Наблюдения с момента инициализации измерительного процесса. Число байт включает IP заголовок и содержание пакета.
200	mplsTopLabelTTL	Поле TTL (время жизни) из MPLS метки в верхушке стека, т.е. последней.
201	mplsLabelStackLength	Длина MPLS стека в байтах.
202	mplsLabelStackDepth	Число меток в стеке MPLS меток.
203	mplsTopLabelExp	Поле Exp из MPLS метки, находящейся в верхушке стека.
204	ipPayloadLength	Действительная длина тела IP пакета. Для пакетов IPv4 величина этого информационного элемента является отличной от длины пакета IPv4 (в totalLengthIPv4) и длиной заголовка пакета (headerLengthIPv4). Для IPv6 величина этого элемента в заголовке пакета отображается исключительно в случае, когда величина этого поля равна 0 и существует поле Большой длины (jumbo payload).
205	udpMessageLength	Значение длины поля в UDP заголовке.
206	isMulticast	Если IP адрес приемника не является зарезервированным групповым (multicast) адресом, то значение всех бит в байте (включая резервные) равно 0. Первый бит этого байта установлен в 1, если поле Версии в IP заголовке имеет значение 4 и если поле адреса приемника содержит зарезервированный групповой адрес в диапазоне 224.0.0.0 — 239.255.255.255. В противном случае этот бит равен 0. Второй и третий биты зарезервированы для будущего применения. Оставшиеся биты устанавливаются в значение отличное от 0, если IP адрес приемника является зарезервированным IPv6 групповым адресом. Тогда четвертый бит устанавливается в значение T флага в IPv6 группового адреса.
207	ipv4IHL	Значение поля длины заголовка (Internet Header Length (IHL) в заголовке Ipv4.
208	ipv4Options	IPv4 параметры в пакете этого Потока. Информация кодируется в набор битовых полей. Для каждого IPv4 типа параметра существует бит в этом наборе. Бит устанавливается в 1, если любой исследуемый пакет этого

		Потока содержит соответствующий параметр. В противном случае значение равно 0. Список параметров: http://www.iana.org/assignments/ip-parameters
209	tcpOptions	TCP параметры в пакетах этого Потока. Информация кодируется в набор битовых полей. Для каждого TCP типа параметра существует бит в этом наборе. Бит устанавливается в 1, если любой исследуемый пакет этого Потока содержит соответствующий параметр. В противном случае значение равно 0.
210	paddingOctets	Значением этого элемента является последовательность величин 0x00
211	collectorIPv4Address	IPv4 адрес, на который Экспортируемый Процесс посылает Поток информации.
212	collectorIPv6Address	IPv6 адрес, на который Экспортируемый Процесс посылает Поток информации.
213	exportInterface	Индекс интерфейса, с которого IPFIX сообщения посылаются Экспортируемым Процессом на Коллектор.
214	exportProtocolVersion	Версия протокола, используемая Экспортирующим Процессом для посылки Потоковой информации. Версия протокола задается значением поля Номер версии (Version Number) в заголовке сообщения. Для IPFIX — значение 10, для NetFlow версии 9 — 9.
215	exportTransportProtocol	Значение номера протокола, используемого Экспортируемым Процессом для посылки Потоковой информации. Номер протокола определяет тип IP пакета.
216	collectorTransportPort	Идентификатор порта приемника, на который Экспортный Процесс посылает Потоковую информацию. Для транспортных протоколов UDP, TCP и SCTP — это номер порта приемника.
217	exporterTransportPort	Идентификатор порта источника, с которого Экспортный Процесс посылает Потоковую информацию. Для транспортных протоколов UDP, TCP и SCTP — это номер порта источника.
218	tcpSynTotalCount	Общее число пакетов конкретного потока с TCP флагом "Synchronize sequence numbers" (SYN)
219	tcpFinTotalCount	Общее число пакетов конкретного потока с TCP флагом "No more data from sender" (FIN)
220	tcpRstTotalCount	Общее число пакетов конкретного потока с TCP флагом "Reset the connection" (RST)
221	tcpPshTotalCount	Общее число пакетов конкретного потока с TCP флагом "Push Function" (PSH)
222	tcpAckTotalCount	Общее число пакетов конкретного потока с TCP флагом "Acknowledgment field significant" (ACK)
223	tcpUrgTotalCount	Общее число пакетов конкретного потока с TCP флагом "Urgent Pointer field significant" (URG)
224	ipTotalLength	Общая длина IP пакета.
237	postMplsTopLabelExp	Определение этого информационного элемента идентично определению информационного элемента mplsTopLabelExp за исключением того, что он отображает потенциально модифицируемое значение функцией промежуточного устройства (middlebox function) после того, как пакет пройдет точку наблюдения.
238	tcpWindowScale	Масштабирование поля окна в TCP заголовке.

Информационные элементы в IPFIX протоколе разбиты на 12 групп:

1. Идентификаторы.
2. Конфигурация процессов измерения и экспорта.

3. Статистика процессов измерения и экспорта.
4. Поля IP заголовка.
5. Поля транспортного заголовка.
6. Поля подзаголовка.
7. Извлеченные пакетные свойства.
8. Минимальные/ максимальные свойства потока.
9. Временные параметры потока.
10. Счетчики по потоку.
11. Разносторонние свойства потока.
12. Дополнение.

Информационные элементы, которые извлекаются из полей пакетов или получаются в результате обработки пакетов, такие как элементы в группах 4-7, могут обычно применяться в качестве Потоковых ключей (Flow Keys), которые используются для привязки пакетов к Потокам.

Если они не используются, как Потоковые ключи, то их значения могут изменяться от пакета к пакету внутри одного Потока. Для информационных элементов со значениями, которые извлекаются из полей пакетов или получаются в результате обработки пакетов, и для которых значение может изменяться о пакета к пакету внутри одного Потока, информационная модель IPFIX считает, что их значение определяются первым пакетом, наблюдаемым в соответствующем Потоке, кроме описания информационного элемента напрямую определенного в различных семантиках. Это простое правило определяет запись всех информационных элементов, связанных с полями заголовка единожды тогда, когда наблюдается первый пакет Потока. Для исследуемых в дальнейшем пакетах этого же Потока, только те свойства Потока, которые зависят от более чем одного пакета, таких как информационных элементов в группах 8-11, необходимо будет добавить.

Идентификаторы

Информационные элементы, указанные ниже, являются идентификационными компонентами IPFIX архитектуры, IPFIX устройств или IPFIX протокола. Обычно, они используются для ограничения границ других информационных элементов (таблица 4).

Таблица 4

ID	**Наименование**	**ID**	**Наименование**
141	lineCardId	148	flowId
142	portId	145	templateId
10	ingressInterface	149	observationDomainId
14	egressInterface	138	observationPointId
143	meteringProcessId	137	commonPropertiesId
144	exportingProcessId		

Конфигурация процессов измерения и экспорта

Приведенные в таблице ниже перечень информационных элементов используются для конфигурации процессов измерения и экспорта.

Таблица 5

ID	Наименование	ID	Наименование
130	exporterIPv4Address	213	exportInterface
131	exporterIPv6Address	214	exportProtocolVersion
217	exporterTransportPort	215	exportTransportProtocol
211	collectorIPv4Address	216	collectorTransportPort
212	collectorIPv6Address	173	flowKeyIndicator

Статистика процессов измерения и экспорта

Информационные элементы этого сектора описывают статистику процессов измерения и экспорта. Перечень их приведен в таблице ниже.

Таблица 6

ID	Наименование	ID	Наименование
41	exportedMessageTotalCount	165	ignoredOctetTotalCount
40	exportedOctetTotalCount	166	notSentFlowTotalCount
42	exportedFlowRecordTotalCount	167	notSentPacketTotalCount
163	observedFlowTotalCount	168	notSentOctetTotalCount
164	ignoredPacketTotalCount		

Поля IP заголовка

Информационные поля этого раздела отображают значения полей IP заголовка или величины, извлеченные из IP заголовков.

Таблица 7

ID	Наименование	ID	Наименование
60	ipVersion	193	nextHeaderIPv6
8	sourceIPv4Address	195	ipDiffServCodePoint
27	sourceIPv6Address	196	ipPrecedence
9	sourceIPv4PrefixLength	5	ipClassOfService
29	sourceIPv6PrefixLength	55	postIpClassOfService
44	sourceIPv4Prefix	31	flowLabelIPv6
170	sourceIPv6Prefix	206	isMulticast
12	destinationIPv4Address	54	fragmentIdentification
28	destinationIPv6Address	88	fragmentOffset
13	destinationIPv4PrefixLength	197	fragmentFlags
30	destinationIPv6PrefixLength	189	ipHeaderLength

45	destinationIPv4Prefix	207	ipv4IHL
169	destinationIPv6Prefix	190	totalLengthIPv4
192	ipTTL	224	ipTotalLength
4	protocolIdentifier	191	payloadLengthIPv6

Поля транспортного заголовка

Набор информационных элементов относящихся к полям транспортного заголовка.

Таблица 8

ID	**Наименование**	**ID**	**Наименование**
7	sourceTransportPort	238	tcpWindowScale
11	destinationTransportPort	187	tcpUrgentPointer
180	udpSourcePort	188	tcpHeaderLength
181	udpDestinationPort	32	icmpTypeCodeIPv4
205	udpMessageLength	176	icmpTypeIPv4
182	tcpSourcePort	177	icmpCodeIPv4
183	tcpDestinationPort	139	icmpTypeCodeIPv6
184	tcpSequenceNumber	178	icmpTypeIPv6
185	tcpAcknowledgementNumber	179	icmpCodeIPv6
186	tcpWindowSize	33	igmpType

Поля подзаголовка

Перечень информационных элементов, входящих в этот набор приведен в таблице ниже.

Таблица 9

ID	**Наименование**	**ID**	**Наименование**
56	sourceMacAddress	201	mplsLabelStackLength
81	postSourceMacAddress	194	mplsPayloadLength
58	vlanId	70	mplsTopLabelStackSection
59	postVlanId	71	mplsLabelStackSection2
80	destinationMacAddress	72	mplsLabelStackSection3
57	postDestinationMacAddress	73	mplsLabelStackSection4
146	wlanChannelId	74	mplsLabelStackSection5
147	wlanSSID	75	mplsLabelStackSection6
200	mplsTopLabelTTL	76	mplsLabelStackSection7
203	mplsTopLabelExp	77	mplsLabelStackSection8
237	postMplsTopLabelExp	78	mplsLabelStackSection9

202	mplsLabelStackDepth	79	mplsLabelStackSection10

Извлеченные пакетные свойства

Набор информационных элементов, извлеченных из пакетных свойств (например, значения полей заголовка) включают элементы, перечисленные в таблице ниже.

Таблица 10

ID	Наименование	ID	Наименование
204	ipPayloadLength	18	bgpNextHopIPv4Address
15	ipNextHopIPv4Address	63	bgpNextHopIPv6Address
62	ipNextHopIPv6Address	46	mplsTopLabelType
16	bgpSourceAsNumber	47	mplsTopLabelIPv4Address
17	bgpDestinationAsNumber	140	mplsTopLabelIPv6Address
128	bgpNextAdjacentAsNumber	90	mplsVpnRouteDistinguisher
129	bgpPrevAdjacentAsNumber		

Минимальные/максимальные параметры потока

Таблица 11

ID	Наименование	ID	Наименование
25	minimumIpTotalLength	208	ipv4Options
26	maximumIpTotalLength	64	ipv6ExtensionHeaders
52	minimumTTL	6	tcpControlBits
53	maximumTTL	209	tcpOptions

Временные параметры потока

Информационные элементы flowStartSeconds, flowEndSeconds, flowStartMilliseconds, flowEndMilliseconds, flowStartMicroseconds, flowEndMicroseconds, flowStartNanoseconds, flowEndNanoseconds и systemInitTimeMilliseconds являются абсолютными и показывают время в секундах с 00:00 UTC 1 января 1970 года.

Информационные элементы flowStartDeltaMicroseconds и flowEndDeltaMicroseconds являются относительными и действительны только в рамках одного IPFIX сообщения. Они содержат время отрицательного смещения относительно времени экспорта, указанного в заголовке IPFIX сообщения. Максимальное значение смещения может быть 1 час 11 минут 34,967295 секунд.

Информационные элементы flowStartSysUpTime и flowEndSysUpTime представляют относительное время по отношению к последней инициализации IPFIX устройства.

Таблица 12

ID	Наименование	ID	Наименование
150	flowStartSeconds	156	flowStartNanoseconds

151	flowEndSeconds	157	flowEndNanoseconds
152	flowStartMilliseconds	158	flowStartDeltaMicroseconds
153	flowEndMilliseconds	159	flowEndDeltaMicroseconds
154	flowStartMicroseconds	160	systemInitTimeMilliseconds
155	flowEndMicroseconds	22	flowStartSysUpTime
		21	flowEndSysUpTime

Потоковые счетчики

Информационные элементы этого раздела являются счетчиками, которые содержат целые значения. Эти значение могут изменяться для каждого отчета, где они используются. Они не могут служить Потоковыми Ключами. Однако, потенциально они могут использоваться для выбора экспортируемых потоков, например, только потоков с числом переданных байт более определенного порога.

Существуют рабочие счетчики и изменяемые (delta) счетчики. Изменяемые счетчики сбрасываются в 0 каждый раз, когда их значение экспортируется. Рабочие счетчики накапливают значение постоянно, независимо от экспортируемого процесса.

Существуют потоковые счетчики (по потоку) и счетчики связанные с процессами измерения и экспорта. Потоковые счетчики отображают свойства потока и потенциально могут изменяться каждый раз, когда исследуется пакет, принадлежащий потоку.

Таблица 13

ID	**Наименование**	**ID**	**Наименование**
1	octetDeltaCount	134	droppedOctetTotalCount
23	postOctetDeltaCount	135	droppedPacketTotalCount
198	octetDeltaSumOfSquares	19	postMCastPacketDeltaCount
85	octetTotalCount	20	postMCastPacketDeltaCount
171	postOctetTotalCount	174	postMCastPacketTotalCount
199	octetTotalSumOfSquares	175	postMCastOctetTotalCount
2	packetDeltaCount	218	tcpSynTotalCount
24	postPacketDeltaCount	219	tcpFinTotalCount
86	packetTotalCount	220	tcpRstTotalCount
172	postPacketTotalCount	221	tcpPshTotalCount
132	droppedOctetDeltaCount	222	tcpAckTotalCount
133	droppedPacketDeltaCount	223	tcpUrgTotalCount

Разносторонние свойства потока

Информационные элементы этого раздела относятся к таким свойствам потока, как его начало, продолжительность, окончание, но они не являются временными метками.

Таблица 14

ID	Наименование	ID	Наименование
36	flowActiveTimeout	161	flowDurationMilliseconds
37	flowIdleTimeout	162	flowDurationMicroseconds
136	flowEndReason	61	flowDirection

Дополнение

Таблица 15

ID	Наименование	ID	Наименование
210	paddingOctets		

Как видно из приведенного выше материала в IPFIX протокол по сравнению с NetFlow версии 9 добавлено значительное число ИЭ. Но далеко не всегда пользователю нужны все эти ИЭ. И, естественно, что если оборудование будет для экспортных записей формировать весь возможный перечень ИЭ, тем большие нагрузки на процессор и память этого оборудования будут требоваться для этой цели. Кроме этого будут заниматься дополнительные сетевые ресурсы для передачи экспортных записей на коллектор. Поэтому, если оборудование позволяет выбрать необходимый перечень полей, то стоит воспользоваться этой возможность и задать только те, которые вам необходимы.

Существуют и другие способы уменьшить объем обрабатываемой информации о потоках и, соответственно, объем передаваемой по сети IPFIX информации. Такими способами являются выборки, фильтрация (описываемые в RFC 5473-5475) и агрегация. По агрегации существует пока лишь проект стандарта [8].

Приложения на основе IPFIX

Компания "Софт Пи Ай" может предложить свои программные продукты, построенные на основе IPFIX протокола:

1. ***Биллинговая система Tariscope***

Tariscope содержит NetFlow коллектор, обеспечивающий сбор информации о сетевых потоках на основе протоколов IPFIX, NetFlow и rFlow для учета используемых сетевых ресурсов. NetFlow коллектор работает, как служба операционной системы Windows. Экран настройки параметров этой службы показан на рисунке 2.

NetFlow коллектор работает только через UDP порт. Номер порта может настраиваться.

Имеется возможность записи "сырого" потока IPFIX данных в файл, что позволяет при необходимости повторно переобработать данные.

Для уменьшения объема базы данных, что является существенным при большом числе абонентов, коллектор позволяет агрерировать данные IPFIX протокола до уровня IP сетей.

В настройке коллектора имеется возможность задания режима тарификации: в режиме реального времени или по инициативе администратора системы.

Для учета работы NetFlow коллектора можно задать различные уровни протоколирования, что при необходимости может позволить выявить какие-либо проблемы.

Биллинговая система Tariscope обеспечивает ведение единого счета для абонента, как по

услугам доступа к интернет, так и за услуги телефонии или какие-либо другие услуги связи.

Более подробную информацию по биллинговому комплексу Tariscope, а также его триал-версию можно получить на сайте: http://www.tariscope.com

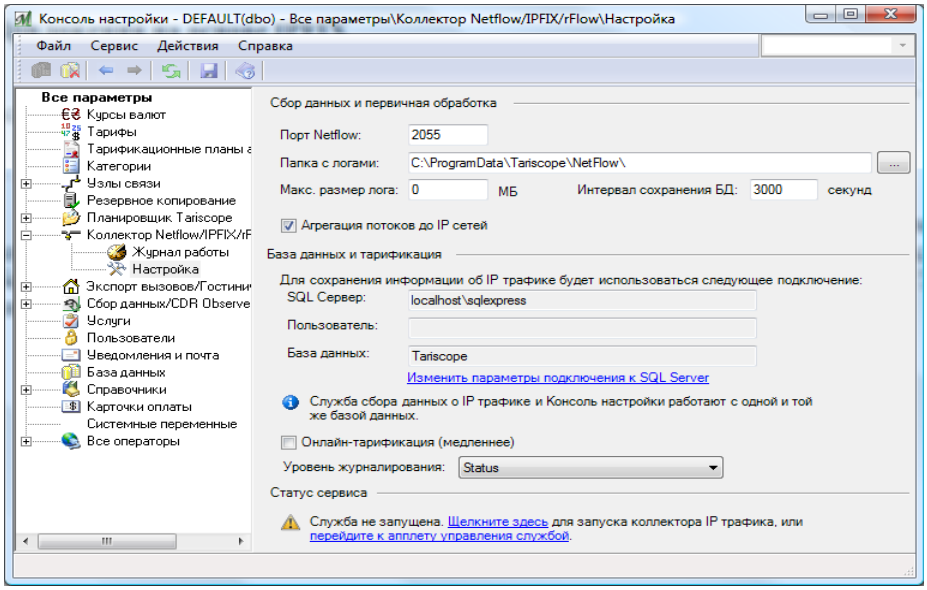

Рисунок 2

2. ***SoftPI NetFlow Collector***

SoftPI NetFlow Collector представляет собой коллектор, обеспечивающий сбор IPFIX или NetFlow (версии 5 или 9) протоколов в базу данный Miscosoft SQL или MySQL серверов (рисунок 3).

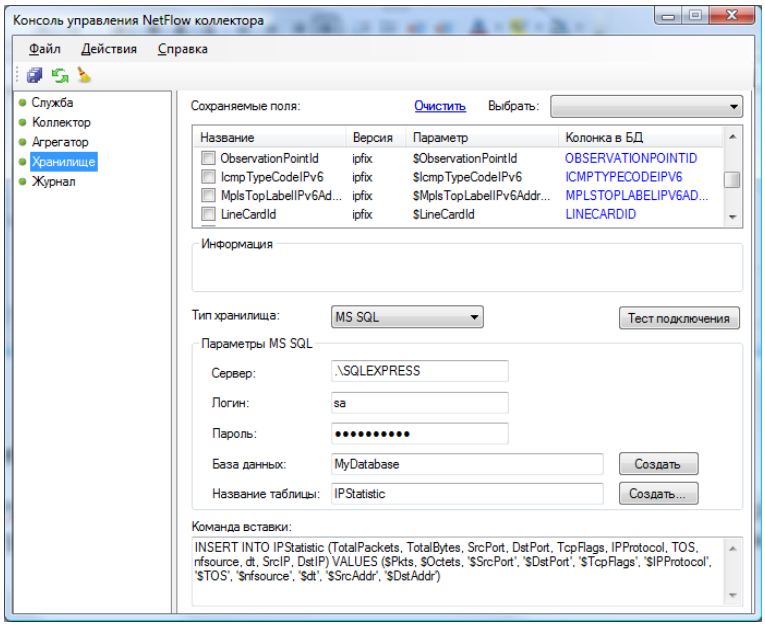

Рисунок 3

Для оптимального использования дискового пространства, используемого базой данных SoftPI NetFlowCollector, пользователь может указать для сохранения в этой базе данных, только необходимых ему полей. Кроме этого можно выбрать также агрегацию данных по целому ряду параметров. Подробную информацию по SoftPI NetFlowCollector можно получить на сайте: http://www.softpiua.com/ru/products/softpi/netflow-collector.html

Литература

1. Что такое NetFlow. http://softpi.com.ua/files/what_is_NetFlow.pdf
2. RFC 2975. B. Aboba, J. Arkko, D. Harrington. Introduction to Accounting Management.
3. NN48500-595. Avaya Ethernet Routing Switch 4500, 5000, 8300, 8600. IPFIX Technical Configuration Guide. 2010.
4. NN47200-505. Nortel Ethernet Routing Switch 5000 Series. Configuration — System Monitoring. Release 6.2. 2010
5. RFC 5477. T. Dietz, B. Claise, P. Aitken, F. Dressler, G. Carle. Information Model for Packet Sampling Exports.
6. Что такое RADIUS. http://www.softpi.com.ua/ru/softpi-radius/what-is-radius.html
7. RFC 3954. B. Claise, Ed. Cisco Systems NetFlow Services Export Version 9.
8. Internet-Draft. F. Dressler, C. Sommer, Univ. Erlangen, G. Muenz, Univ. Tuebingen, A. Kobayashi, NTT PF Lab. IPFIX Flow Aggregation.