Network Working Group B. Claise, Ed.
Request for Comments: 3954 Cisco Systems
Category: Informational October 2004

Протокол экспорта NetFlow версии 9

Cisco Systems NetFlow Services Export Version 9

Статус документа

В этом документе содержится информация для сообщества Internet. Документ не задает каких-либо стандартов Internet. Документ может распространяться без ограничений.

Авторские права

Примечание IESG

В этом RFC документирован протокол экспорта NetFlow версии 9 в том виде, как он был представлен IETF в качестве основы для работы IPFIX WG.

Данный RFC сам по себе не рассматривается как возможный стандарт Internet. IETF не несет ответственности за возможность использования протокола с теми или иными целями и специально отмечает, что данный протокол не рассматривался полностью IETF на предмет безопасности, контроля насыщения и некорректного взаимодействия с другими протоколами. Редактор RFC принимал решение о публикации документа по своему усмотрению.

Тезисы

В этом документе содержится спецификация формата экспорта данных NetFlow версии 9 компании Cisco Systems для использования в реализациях сетевых элементов и/или программах сбора данных мониторинга. Формат экспорта NetFlow версии 9 использует шаблоны для предоставления доступа к информации о потоках пакетов IP с высоким уровнем гибкости и расширяемости. Шаблон определяет набор полей с соответствующими описаниями структуры и семантики.

Оглавление

1. Введение

Сервис NetFlow компании Cisco Systems обеспечивает администраторам доступ к информации о потоках IP в сети передачи данных. Элементы сети (маршрутизаторы и коммутаторы) собирают данные о потоках и экспортируют их в коллекторы[1]. Собранные данные обеспечивают точное измерение параметров использования ресурсов с хорошей детализацией и гибким выбором параметров мониторинга.

Поток данных определяется как однонаправленная последовательность пакетов с неким общим набором свойств, проходящих через сетевое устройство. Собранная информация о потоках экспортируется на внешнее устройство, называемое коллектором NetFlow. Информация о потоках включает большой набор параметров — в частности, адреса IP, счетчики пакетов и байтов, временные метки, значения ToS[2], номера портов приложений, входные и выходные интерфейсы и т. п.

Экспортированные данные NetFlow используются для разных целей, включая учет передачи данных в масштабе предприятия и по отдельным подразделениям, учет потоков данных в сеть ISP[3], использование хранилищ данных, мониторинг сети, перспективное планирование сети, мониторинг и профилирование приложений и пользователей, анализ защищенности, сбор данных для маркетинга.

В этом документе содержится спецификация протокола экспорта NetFlow версии 9. Документ рассматривает спецификацию для реализаций протокола с точки зрения как сетевых элементов, так и коллекторов NetFlow. Эта спецификация должна помочь разработчикам реализаций NetFlow v.9 для различных платформ и различных производителей, снижая риск утраты интероперабельности. Формат экспорта NetFlow версии 9 использует шаблоны для предоставления доступа к информации о потоках пакетов IP с высоким уровнем гибкости и расширяемости.

Шаблон определяет набор полей с соответствующими описаниями структуры и семантики.

Основанная на шаблонах модель обеспечивает ряд преимуществ:

- Новые поля могут добавляться в записи NetFlow о потоках без изменения структуры формата экспорта записей. В предыдущих версиях NetFlow добавление нового поля в запись для потока приводило к необходимости создания новой версии протокола экспорта и разработки новой версии коллектора NetFlow, которая позволила бы разбирать новый формат протокола экспорта.
- Шаблоны, передаваемые коллектору NetFlow, содержат структурную информацию о полях экспортируемых записей, следовательно коллектор NetFlow, не понимающий семантику новых полей, сохраняет возможность интерпретации записи о потоке.
- Гибкость механизма шаблонов позволяет экспортировать из потока коллектору NetFlow только требуемые поля. Это обеспечивает снижение объема передаваемой информации и может также снижать потребности в памяти при экспорте данных и на коллекторе NetFlow. Снижение объема передаваемой информации позволяет также уменьшить нагрузку на сеть.

Рабочая группа IETF IPFIX (IP Flow Information eXport[4]) разрабатывает новый протокол на основе версии 9 протокола NetFlow. Новый протокол IPFIX будет обеспечивать преимущества в ряде областей (устойчивый к перегрузкам траспорт, встроенная защита и т. п.). Более подробно узнать об этом протоколе можно из материалов рабочей группы IPFIX.

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе используются для обозначения уровня требований и интерпретируются в соответствии с BCP 14, RFC 2119 [RFC2119].

2. Терминология

В этом разделе приведены определения терминов, используемых в документе. Отметим, что в таблице параграфа 2.1 приведен список используемых терминов и показаны связи между ними.

Observation Point — точка наблюдения

Observation Point представляет собой место в сети, где можно отслеживать пакеты IP (например, один или несколько интерфейсов маршрутизатора или другого сетевого устройства). Каждая точка наблюдения связана с областью (доменом) наблюдения — Observation Domain.

Observation Domain — область (домен) наблюдения

Множество точек наблюдения, обеспечивающее наибольший агрегируемый набор информации о потоках на сетевом устройстве с поддержкой NetFlow, называется областью наблюдения. Например, интерфейсный модуль маршрутизатора является областью наблюдения, в которой каждый интерфейс является точкой наблюдения.

IP Flow или Flow — поток IP или поток

Поток IP (или просто поток) определяется как множество пакетов IP, проходящих через точку наблюдения в течение некоторого времени. Все пакеты конкретного потока обладают общим набором свойств, связанным с содержащимися в пакетах данными или трактовкой пакетов в точке наблюдения.

Flow Record — запись о потоке

Записи о потоках обеспечивают информацию о потоках IP в точке наблюдения. В этом документе используется также термин «запись для данных о потоке» (Flow Data Record) для обозначения данных NetFlow.

Exporter — экспортер

[1] Сборщики информации. *Прим. перев.*
[2] Type of Service — тип обслуживания пакетов.
[3] Internet Service Provider – поставщик услуг Internet. *Прим. перев.*
[4] Экспорт информации о потоках IP.

Устройство (например, маршрутизатор) со включенным сервисом NetFlow, обеспечивающее мониторинг пакетов в точке наблюдения и создание потоков из этих пакетов. Информация из созданных потоков экспортируется в форме записей о потоке коллектору NetFlow.

NetFlow Collector — коллектор NetFlow

Коллектор NetFlow получает записи о потоках от одного или множества экспортеров и обрабатывает полученные пакеты экспорта, разбирая и сохраняя информацию из записей о потоках. Записи о потоках могут агрегироваться перед их записью на диск. Коллекторы NetFlow в этом документе также могут сокращенно называться коллекторами.

Export Packet — пакет экспорта

Пакет экспорта представляет собой исходящий от экспортера пакет, содержащий записи о потоках от данного экспортера и адресованный коллектору NetFlow.

Packet Header — заголовок пакета

Заголовок пакета представляет собой первую часть пакета экспорта. Заголовок пакета содержит базовую информацию о пакете, включая номер версии NetFlow, число записей в данном пакете и порядковый номер.

Template Record — шаблон

Шаблон определяет структуру и интерпретацию полей записи данных о потоке.

Flow Data Record — запись данных о потоке

Запись данных о потоке представляет собой запись, содержащую параметры пакета в соответствии с шаблоном.

Options Template Record — шаблон опций

Шаблон опций определяет структуру и интерпретацию полей в записи данных опций, включая определение границ применимости записи данных опций.

Options Data Record — запись данных опций

Запись, содержащая значения и информацию о границах данных в параметрах измерения потока, соответствующие шаблону записи опций.

FlowSet — набор потоков

FlowSet — базовый термин для набора записей о потоках, имеющих похожую структуру. В пакетах экспорта после заголовка следует один или множество наборов FlowSet. Существует три разных типа наборов FlowSet: Template FlowSet, Options Template FlowSet и Data FlowSet.

Template FlowSet — набор шаблонов

Набор из одного или множества шаблонов, сгруппированных в пакете экспорта.

Options Template FlowSet — набор шаблонов опций

Набор из одной или множества записей шаблонов опций, сгруппированных в пакете экспорта.

Data FlowSet — набор данных

Набор из одной или множества однотипных записей, сгруппированных в пакете экспорта. Каждая запись имеет тип Flow Data или Options Data, как определено в шаблоне или шаблоне опций.

2.1. Таблица терминов

	Содержимое	
FlowSet	Template Record	Data Record
Data FlowSet	/	Запись (записи) Flow Data или Options Data
Template FlowSet	Шаблон(ы)	/
Options Template FlowSet	Шаблон(ы) опций	/

Набор Data FlowSet состоит из записей данных опций или данных о потоке без включения шаблона. Шаблон определяет запись данных о потоке, а шаблон опций — запись данных опции.

Набор Template FlowSet состоит из шаблонов без включения данных о потоке или опциях.

Набор Options Template FlowSet состоит из шаблонов опций без включения данных о потоке или опциях.

3. Картина NetFlow на стороне экспортера

3.1. Процесс NetFlow у экспортера

Процесс NetFlow на стороне экспортера отвечает за создание потоков (Flow) из наблюдаемых пакетов IP. Детали этого процесса выходят за рамки данного документа.

3.2. Окончание срока действия потока

Покток считается неактивным, если в точке наблюдения в течение заданного интервала времени не было отмечено относящихся к потоку пакетов. При появлении любого пакета, относящемуся к потоку, в течение заданного интервала поток рассматривается, как активный. Поток может экспортироваться при следующих условиях:

1. Экспортер может детектировать окончание потока. Например, при обнаружении в потоке TCP [RFC793] пакета с флагом FIN или RST запись о потоке экспортируется.

2. Поток неактивен в течение заданного времени. Значение тайм-аута **следует** делать настраиваемым на стороне экспортера с возможностью задания нулевого тайм-аута для немедленного завершения.

3. Для долгосрочных потоков экспортеру **следует** экспортировать записи о потоке на регулярной основе. Значение периода экспорта **следует** делать настраиваемым на стороне экспортера.

4. Если у экспортера возникают внутренние ограничения, **возможно** досрочное завершение (экспорт) потока. Причиной такого досрочного завершения может явиться достижение верхней ганицы счетчиков или нехватка памяти.

3.3. Транспортный протокол

Для обеспечения эффективной обработки на уровне экспортеров с учетом большого объема пакетов экспорта в протоколе NetFlow используется инкапсуляция этих пакетов в дейтаграммы транспортного протокола UDP [RFC768] для передачи коллектору NetFlow. Однако NetFlow версии 9 обеспечивает независимость от транспортного протокола. Следовательно, обеспечивается возможность работы на базе протоколов с контролем насыщения, таких, как SCTP [RFC2960].

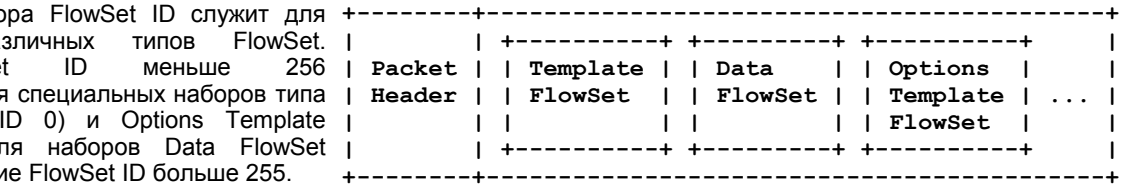
Отметим, что экспортер может работать со множеством коллекторов, независимо выбирая для них транспортный протокол.

Протокол UDP [RFC768] не поддерживает контроля насыщения, поэтому при развертывании NetFlow версии 9 в чувствительной к перегрузкам среде соединение между экспортером и коллектором осуществляется по выделенному каналу. Это обеспечивает воздействие выбросов трафика NetFlow исключительно на выделенный канал без негативного влияния на работу сети. Когда коллектор NetFlow невозможно разместить в одном интервале маршрутизации (one-hop distance) от экспортера или путь между экспортером и коллектором используется не только для передачи данных мониторинга, путь экспорта данных следует строить так, чтобы на нем обеспечивалась устойчивость к максимальным пикам трафика NetFlow от экспортера. Отметим, что при использовании слишком медленного канала экспортер может входить в насыщение.

4. Структура пакета

Пакет экспорта состоит из заголовка, за которым следует по крайней мере один набор данных FlowSet. В качестве FlowSet могут использоваться три типа наборов данных: шаблон (Template), данные (Data), шаблон опций (Options Template).

Идентификатор набора FlowSet ID служит для идентификации различных типов FlowSet. Значения FlowSet ID меньше 256 зарезервированы для специальных наборов типа Template FlowSet (ID 0) и Options Template FlowSet (ID 1). Для наборов Data FlowSet используется значение FlowSet ID больше 255.

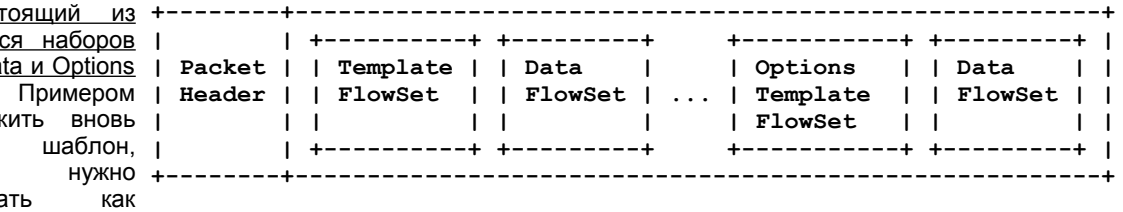


Пакет экспорта

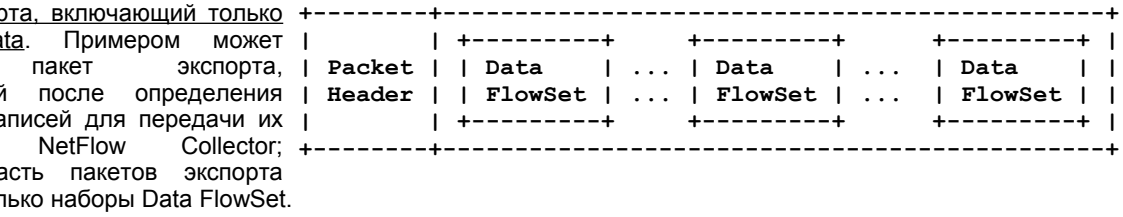
Формат наборов Template, Data и Options Template обсуждается ниже. Экспортер **должен** использовать для всех двоичных целых чисел в заголовке и наборах FlowSet сетевой порядок байтов (его также называют big-endian).

Ниже приведено несколько примеров пакетов экспорта.

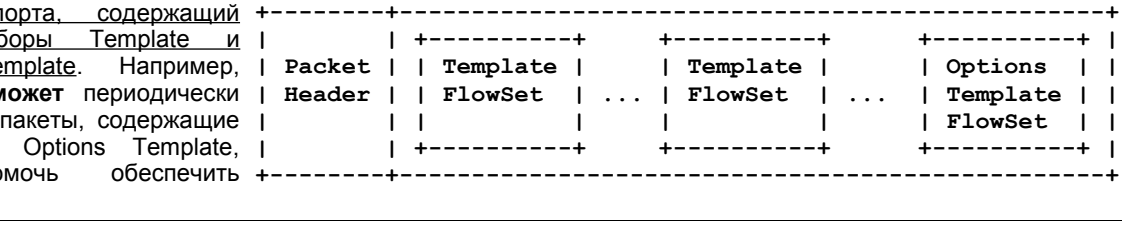
1. Пакет, состоящий из чередующихся наборов Template, Data и Options Template. Примером может служить вновь созданный шаблон, который нужно экспортировать как можно скорей. Поэтому, если уже есть пакет экспорта с Data FlowSet, подготавливаемый к экспорту, в него включают наборы Template и Option Template, чередуя их с данными, как показано на рисунке с учетом доступного в пакете пространства.



2. Пакет экспорта, включающий только наборы Data. Примером может служить пакет экспорта, создаваемый после определения шаблонов записей для передачи их коллектору NetFlow Collector; большая часть пакетов экспорта включает только наборы Data FlowSet.



3. Пакет экспорта, содержащий только наборы Template и Options Template. Например, экспортер **может** периодически передавать пакеты, содержащие Template и Options Template, чтобы помочь обеспечить

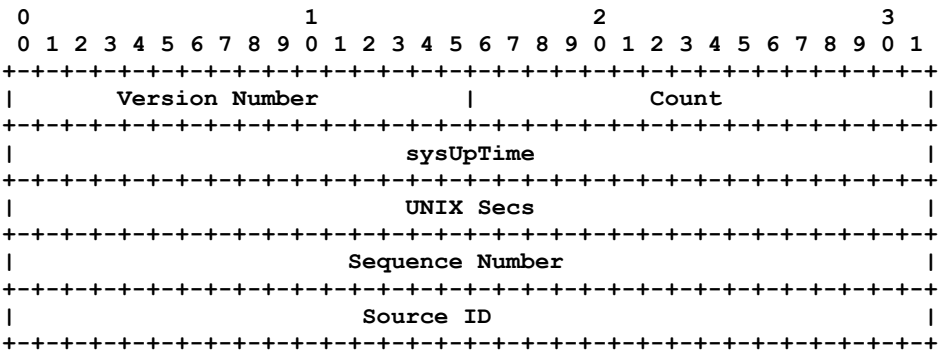


коллектору корректность записей Template и Options Template при получении соответствующих записей Flow Data.

5. Формат пакета экспорта

5.1. Формат заголовка

Формат заголовка пакета показан на рисунке.



Ниже приведено описание полей заголовка.

Version - версия

Версия формата Flow Record, экспортируемого в данном пакете. Для текущей версии значение этого поля равно 9.

Count - счетчик

Общее число записей в пакете экспорта, равное сумме числа записей Options FlowSet, Template FlowSet и Data FlowSet.

sysUpTime

Время, прошедшее с момента загрузки системы (в миллисекундах).

UNIX Secs

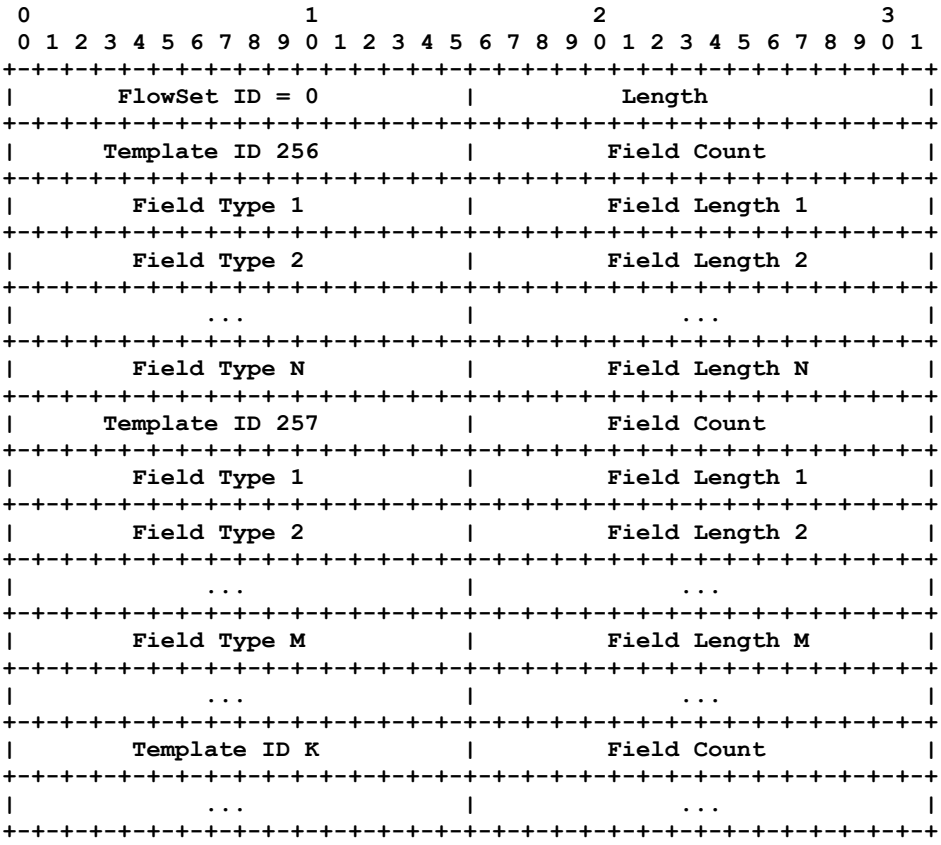
Число секунд, прошедших с момента 0000 UTC 1970 до момента отправки экспортером пакета экспорта.

Sequence Number — порядковый номер

Нарастающий счетчик числа пакетов экспорта, переданных экспортером из данной точки наблюдения. Это значение **должно** быть накопительным и колекторам **следует** использовать его для детектирования потерь пакетов экспорта.

Source ID

32-битовое значение, идентифицирующее область наблюдения экспортера. Коллекторам NetFlow **следует** использовать IP-адрес отправителя в комбинации с Source ID для идентификации различных потоков экспорта от одного экспортера.



5.2. Формат шаблона FlowSet

Одним из существенных элементов NetFlow является Template FlowSet. Шаблоны существенно повышают уровень гибкости формата записей о потоках, поскольку они позволяют коллекторам обрабатывать записи о потоках даже при отсутствии возможности интерпретации всех содержащихся в записи данных. Формат Template FlowSet показан на рисунке.

Ниже приводится описание полей шаблона.

FlowSet ID — идентификатор набора

Для Template FlowSet зарезервировано значение FlowSet ID = 0.

Length — размер

Общий размер данного набора FlowSet. Поскольку Template FlowSet **может** включать множество записей Template Record, для определения позиции следующей записи FlowSet, которая может иметь любой тип FlowSet, **должно** использоваться значение поля Length. Размер представляет собой сумму размеров полей FlowSet ID, Length, а также всех записей Template Record в данном наборе FlowSet.

Template ID — идентификатор шаблона

Каждой из вновь генерируемых записей Template присваивается уникальное значение Template ID. Уникальность должна обеспечиваться в масштабе области наблюдения, генерирующей Template ID. Значения Template ID от 0 до 255 зарезервированы для наборов Template FlowSet, Options FlowSet и других зарезервированных наборов FlowSet, которые будут создаваться. Template ID для наборов Data FlowSets принимают значения от 256 до 65535.

Field Count — счетчик полей

Число полей в данной записи Template. Поскольку набор Template FlowSet обычно содержит множество записей Template, значение этого поля позволяет коллектору определить завершение текущей записи Template и начало следующей.

Field Type — тип поля

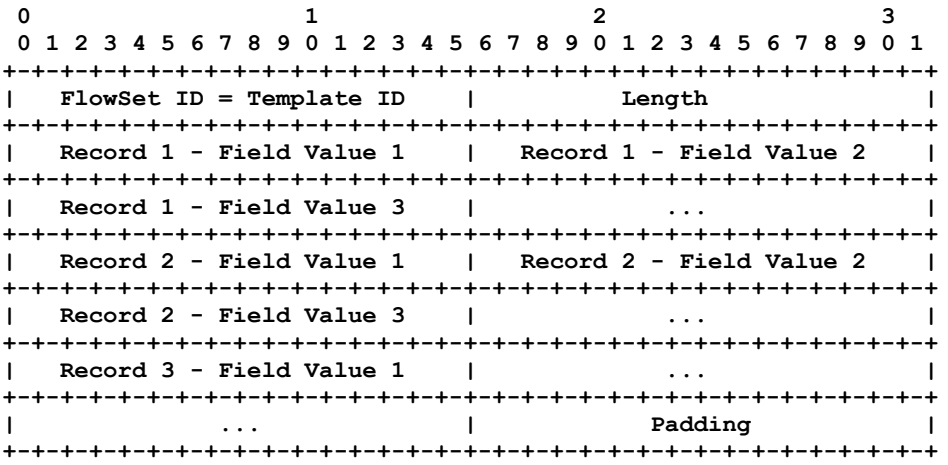
Числовой идентификатор типа поля. Идентификаторы описаны в параграфе «Определения типов полей».

Field Length — размер поля

Размер соответствующего Field Type в байтах (см. параграф «Определения типов полей»).

5.3. Формат Data FlowSet

Формат набора Data FlowSet показан на рисунке.



Ниже приведены описания полей Data FlowSet.

FlowSet ID = Template ID

Каждый набор Data FlowSet имеет свой идентификатор FlowSet ID. Значение FlowSet ID совпадает с созданным ранее идентификатором Template ID. Коллектор **должен** использовать значение FlowSet ID для нахождения соответствующей записи Template и декодирования записей о потоках из набора FlowSet.

Length — размер

Размер данного набора FlowSet, определяемый суммой размеров полей FlowSet ID, Length, всех записей Flow Record в данном наборе FlowSet и байтов заполнения, если они используются.

Record N - Field Value M — запись N - значение поля M

Оставшаяся часть Data FlowSet представляет собой набор записей Flow Data, каждая из которых является набором значений полей. Поля Type и Length заранее определяются в записи Template Record, указанной полем FlowSet ID или Template ID.

Padding – заполнение

Экспортеру **следует** использовать байты заполнения для выравнивания наборов FlowSet по 4-байтовой границе. Важно отметить, что значение поля Length учитывает байты заполнения. Для заполнения **следует** использовать значения 0.

Интерпретация формата Data FlowSet возможна только в тех случаях, когда коллектору доступен шаблон Template FlowSet, соответствующий значению Template ID.

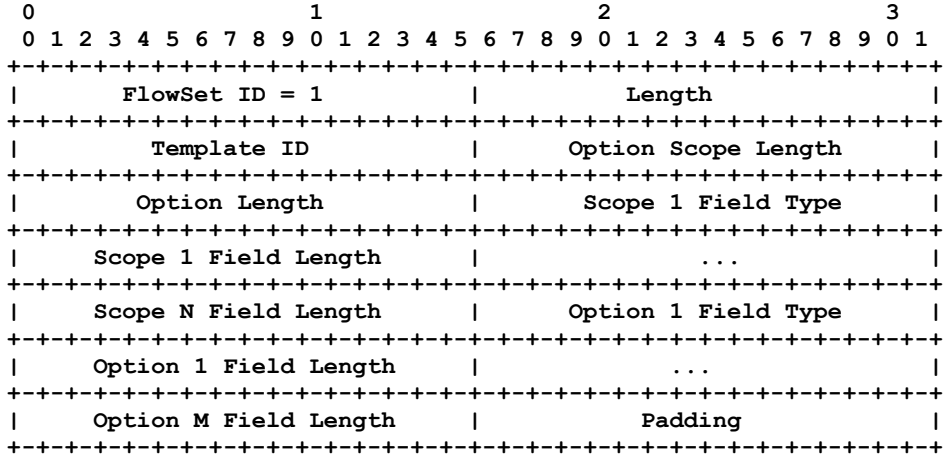
6. Опции

6.1. Формат шаблона опций

Записи Options Template (и соответствующие записи Options Data) используются для передачи данных о конфигурации процесса NetFlow или специфических для процесса данных, а не информации о потоке IP.

Например, Options Template FlowSet может показывать частоту выборки для конкретного интерфейса и используемый метод выборки информации.

Формат набора Options Template FlowSet показан на рисунке.



Ниже описаны поля Options Template FlowSet.

FlowSet ID = 1

Значение FlowSet ID = 1 соответствует шаблону опций (Options Template).

Length — размер

Общий размер данного набора FlowSet. Каждый набор шаблонов опций **может** включать множество записей Options Template. Следовательно, поле Length **должно** использоваться для определения начала следующей записи FlowSet, которая может представлять собой Template FlowSet или Data FlowSet.

Значения поля Length равно сумме размеров полей FlowSet ID и Length, а также всех записей Options Template в данном FlowSet Template ID.

Template ID — идентификатор шаблона

Идентификатор данного шаблона опций. Значение этого поля больше 255.

Option Scope Length — размер определений поля Scope

Размер (в байтах) всех определений поля Scope, содержащегося в записи Options Template (использование поля Scope рассматривается ниже).

Option Length — размер опций

Размер (в байтах) всех полей определения опций, содержащихся в данной записи Options Template.

Scope 1 Field Type — тип поля Scope 1

Часть процесса Exporter/NetFlow, на которую указывает запись Options Template. В настоящее время определены значения:

1 System - система;

2 Interface - интерфейс;

3 Line Card - линейная плата;

4 Cache - кэш;

5 Template - шаблон.

Например, процесс NetFlow может быть реализован для каждого интерфейса и запись Options Template будет говорить о конфигурации интерфейса, если в качестве типа поля Scope будет указано значение 2 (интерфейс). Соответствующий идентификатор интерфейса будет в этом случае передаваться в связанном наборе Options Data. Возможна дополнительная конкретизация Scope путем указания множества типов, которым соответствует процесс. Отметим, что поля Scope всегда предшествуют полям Option.

Scope 1 Field Length — размер поля Scope 1

Размер (в байтах) поля Scope в записи Options Data.

Option 1 Field Type — тип поля Option 1

Числовой идентификатор типа поля, которое будет появляться в записи Options Template. Значения идентификаторов приведены в параграфе «Определения типов полей».

Option 1 Field Length — размер поля Option 1

Размер поля Option в байтах.

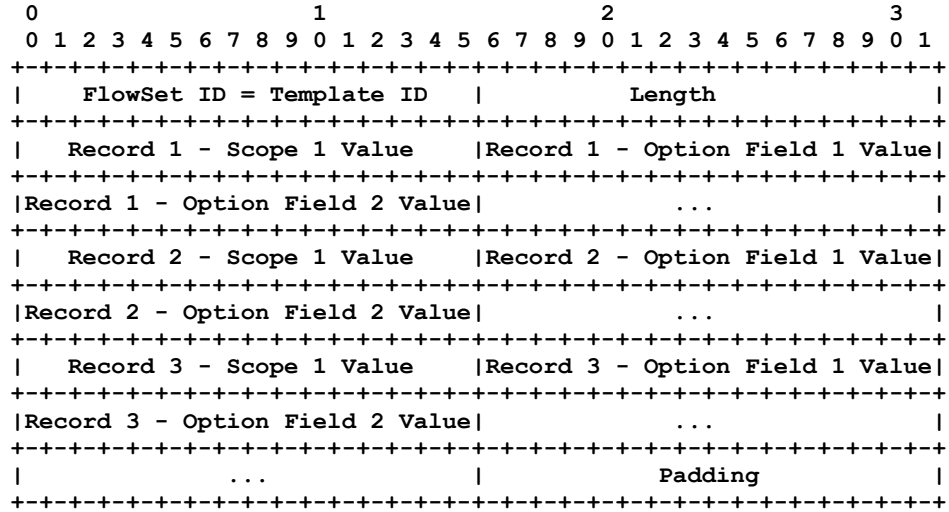
Padding — заполнение

Экспортеру **следует** использовать байты заполнения для выравнивания начала следующего набора FlowSet по 4-байтовой границе. Важно отметить, что байты заполнения учитываются в поле Length. Для заполнения **следует** использовать значение 0.

6.2. Формат данных опций

Записи Options Data передаются в наборах Data FlowSets регулярно, но не с каждой записью Flow Data. Частота отправки записей Options Data задается в конфигурации (см. параграф «Управление шаблонами»).

Формат набора Data FlowSet с записями Options Data показан на рисунке.



Ниже приводится описание полей записей Options Data в наборе Data FlowSet.

FlowSet ID = Template ID

Идентификатор FlowSet ID предшествует каждой группе записей Options Data в наборе Data FlowSet. Значение FlowSet

ID совпадает с созданным ранее идентификатором Template ID соответствующей записи Options Template. Коллектор **должен** использовать FlowSet ID для отображения подходящего типа и размера значений всех последующих полей.

Length — размер

Размер данного набора FlowSet, определяемый суммой размеров полей FlowSet ID и Length, всех записей Options Data в данном наборе FlowSet и байтов заполнения, если они используются.

Record N - Option Field M Value — запись N - значение поля опции M

Оставшаяся часть Data FlowSet представляет собой набор записей о потоках, каждая из которых содержит область охвата и значения полей. Тип и размер полей определяются записью Options Template, указанной идентификатором FlowSet ID или Template ID.

Padding — заполнение

Экспортеру **следует** использовать байты заполнения для выравнивания начала следующего набора FlowSet по 4-байтовой границе. Важно отметить, что байты заполнения учитываются в поле Length. Для заполнения **следует** использовать значение 0.

Формат Data FlowSet может интерпретироваться только при доступности для коллектора набора Options Template FlowSet, соответствующего идентификатору Template ID.

7. Управление шаблонами

Записи Flow Data, соответствующие Template Record, **могут** появляться в том же или последующих пакетах. Записи Template не обязательно передавать в каждом пакете экспорта. Поэтому коллектор NetFlow **должен** сохранять запись Template для интерпретации соответствующих записей Flow Data, которые будут получены в последующих пакетах.

Коллектор NetFlow, получающий пакеты экспорта от одного экспортера для нескольких областей наблюдения, **должен** принимать во внимание отсутствие гарантии уникальности Template ID в разных областях наблюдения.

Значения Template ID должны сохраняться в течение всего срока жизни процесса NetFlow на стороне экспортера. Если экспортер или процесс NetFlow по той или иной причине запускается заново (перезагрузка), вся информация о шаблонах теряется и значения Template ID создаются заново. Таким образом, согласованность идентификаторов Template ID после рестарта экспортера или процесса NetFlow не гарантируется.

Вновь созданной записи Template экспортером присваивается неиспользуемое значение Template ID. Если конфигурация шаблона изменяется, текущее значение Template ID «закрывается» и его **не следует** использовать до перезапуска экспортера или процесса NetFlow. Если коллектор получает новое определение для уже существующего идентификатора Template ID, он **должен** отбросить предыдущее определение шаблона и использовать взамен новое.

Если настроенный на экспортере шаблон удаляется и создается вновь с такими же параметрами конфигурации, **можно** повторно использовать тот же идентификатор Template ID.

Экспортер передает наборы данных Template FlowSet и Options Template FlowSet в следующих случаях:

1. После перезапуска процесса NetFlow экспортеру **недопустимо** передавать какие-либо Data FlowSet без отправки соответствующего Template FlowSet и требуемого Options Template FlowSet в предыдущем пакете экспорта или включения этих наборов в тот же пакет. **Можно** передавать Template FlowSet и Options Template FlowSet заранее, без каких-либо Data FlowSets для того, чтобы обеспечить гарантию наличия у коллектора корректного шаблона до получения первой записи Flow или Options Data.
2. В случае смены конфигурации экспортеру **следует** в ускоренном режиме передать новые определения шаблона. В таких случаях экспортер **может** передать измененные записи Template и Options Template без каких-либо данных заранее, чтобы обеспечить гарантию наличия у коллектора корректного шаблона до получения данных.
3. В регулярном режиме экспортер **должен** передать все записи Template и Options Template для обновления коллектора. Срок жизни идентификаторов Template ID на коллекторе ограничен и эти идентификаторы **должны** периодически обновляться. Существует два варианта обновления шаблонов на стороне коллектора:
   - обновление через каждые N пакетов экспорта;
   - обновление по времени — через каждые N минут.

   Обе опции **должны** быть настраиваемыми пользователем на стороне экспортера. При выполнении одного из условий экспортер **должен** передать Template FlowSet и Options Template.
4. При изменении конфигурации таймера на стороне экспортера последнему **следует** в ускоренном режиме передать определения шаблонов.

8. Определения типов полей

В приведенной ниже таблице даны определения всех полей, которые экспортер **может** поддерживать. Поля могут быть выборкой полей заголовков пакетов, результатами просмотра (например, номерами автономных систем или масками подсетей) и свойствами пакетов (например, размером).

Тип поля	*Код*	*Размер в байтах*	*Описание*
IN_BYTES	1	N	Счетчик входящих данных с размерностью N x 8 битов для подсчета числа байтов, связанных с потоком IP. По умолчанию N = 4.

Тип поля	*Код*	*Размер в байтах*	*Описание*
IN_PKTS	2	N	Счетчик входящих данных с размерностью N x 8 битов для подсчета числа пакетов, связанных с потоком IP. По умолчанию N = 4.
FLOWS	3	N	Число агрегированных потоков; по умолчанию N = 4.
PROTOCOL	4	1	Тип протокола IP.
TOS	5	1	Байт типа обслуживания, задаваемый на входном интерфейсе.
TCP_FLAGS	6	1	Флаги TCP; объединение всех флагов TCP, замеченных в данном потоке.
L4_SRC_PORT	7	2	Номер порта TCP/UDP на стороне отправителя (например, FTP, Telnet и т. п.).
IPV4_SRC_ADDR	8	4	Адрес IPv4 на стороне отправителя.
SRC_MASK	9	1	Число непрерывных битов в маске подсети на стороне отправителя (значение маски в нотации /).
INPUT_SNMP	10	N	Индекс входного интерфейса. По умолчанию N = 2, но могут использоваться большие значения.
L4_DST_PORT	11	2	Номер порта TCP/UDP на стороне получателя (например, FTP, Telnet и т. п.).
IPV4_DST_ADDR	12	4	Адрес IPv4 на стороне получателя.
DST_MASK	13	1	Число непрерывных битов в маске подсети на стороне получателя (значение маски в нотации /).
OUTPUT_SNMP	14	N	Индекс выходного интерфейса. По умолчанию N = 2, но могут использоваться большие значения.
IPV4_NEXT_HOP	15	4	Адрес IPv4 для следующего маршрутизатора.
SRC_AS	16	N	Номер автономной системы BGP на стороне отправителя. N может принимать значения 2 или 4. По умолчанию N = 2.
DST_AS	17	N	Номер автономной системы BGP на стороне получателя. N может принимать значения 2 или 4. По умолчанию N = 2.
BGP_IPV4_NEXT_HOP	18	4	IP-адрес следующего маршрутизатора в домене BGP.
MUL_DST_PKTS	19	N	Счетчик исходящих пакетов IP с групповой адресацией с размерностью N x 8 битов для учета пакетов, связанных с потоком IP. По умолчанию N = 4.
MUL_DST_BYTES	20	N	Счетчик исходящих октетов (байтов) с групповой адресацией с размерностью N x 8 битов для учета байтов, связанных с потоком IP. По умолчанию N = 4.
LAST_SWITCHED	21	4	Значение sysUptime в миллисекундах на момент коммутации последнего пакета в данном потоке.
FIRST_SWITCHED	22	4	Значение sysUptime в миллисекундах на момент коммутации первого пакета в данном потоке.
OUT_BYTES	23	N	Счетчик исходящих данных с размерностью N x 8 битов для подсчета числа байтов, связанных с потоком IP. По умолчанию N = 4.
OUT_PKTS	24	N	Счетчик исходящих данных с размерностью N x 8 битов для подсчета числа пакетов, связанных с потоком IP. По умолчанию N = 4.
IPV6_SRC_ADDR	27	16	Адрес IPv6 на стороне отправителя.
IPV6_DST_ADDR	28	16	Адрес IPv6 на стороне получателя.
IPV6_SRC_MASK	29	1	Число непрерывных битов в маске IPv6 на стороне отправителя.
IPV6_DST_MASK	30	1	Число непрерывных битов в маске IPv6 на стороне получателя.
IPV6_FLOW_LABEL	31	3	Метка потока IPv6 в соответствии с RFC 2460.
ICMP_TYPE	32	2	Тип пакета ICMP[1]; в отчете указывается, как ICMP Type * 256 + ICMP code.
MUL_IGMP_TYPE	33	1	Тип пакета IGMP[2].

[1]Internet Control Message Protocol — протокол управляющих сообщений Internet.
[2]Internet Group Management Protocol — протокол управления группами Internet.

Тип поля	*Код*	*Размер в байтах*	*Описание*
SAMPLING_INTERVAL	34	4	При использовании выборки NetFlow этот параметр определяет скорость выборки; например, значение 100 показывает, что отбирается каждый сотый пакет.
SAMPLING_ALGORITHM	35	1	Задает на уровне платформы алгоритм выборки NetFlow: 0x01 — детерминированная выборка; 0x02 — случайная выборка. Используется вместе с SAMPLING_INTERVAL.
FLOW_ACTIVE_TIMEOUT	36	2	Тайм-аут (в секундах) для активных потоков в кэше NetFlow.
FLOW_INACTIVE_TIMEOUT	37	2	Тайм-аут (в секундах) для неактивных потоков в кэше NetFlow.
ENGINE_TYPE	38	1	Тип машины коммутации потоков (маршрутный процессор, интерфейсная плата и т. п.).
ENGINE_ID	39	1	Числовой идентификатор машины коммутации потоков.
TOTAL_BYTES_EXP	40	N	Счетчик с размерностью N x 8 битов для подсчета байтов, экспортированных областью наблюдения. По умолчанию N = 4.
TOTAL_PKTS_EXP	41	N	Счетчик с размерностью N x 8 битов для подсчета пакетов, экспортированных областью наблюдения. По умолчанию N = 4.
TOTAL_FLOWS_EXP	42	N	Счетчик с размерностью N x 8 битов для подсчета потоков, экспортированных областью наблюдения. По умолчанию N = 4.
MPLS_TOP_LABEL_TYPE	46	1	Тип метки MPLS: 0x00 UNKNOWN 0x01 TE-MIDPT 0x02 ATOM 0x03 VPN 0x04 BGP 0x05 LDP
MPLS_TOP_LABEL_IP_ADDR	47	4	Класс эквивалента пересылки[1], соответствующий метке MPLS.
FLOW_SAMPLER_ID	48	1	Идентификатор, показываемый в «show flow-sampler».
FLOW_SAMPLER_MODE	49	1	Тип алгоритма, используемого для выборки данных: 0x02 — случайная выборка. Используется вместе с FLOW_SAMPLER_RANDOM_INTERVAL[2]
FLOW_SAMPLER_RANDOM_INTERVAL	50	4	Интервал выборки (в пакетах). Используется вместе с FLOW_SAMPLER_MODE
DST_TOS	55	1	Байт типа обслуживания, задаваемый на выходном интерфейсе.
SRC_MAC	56	6	MAC-адрес на стороне отправителя.
DST_MAC	57	6	MAC-адрес на стороне получателя.
SRC_VLAN	58	2	Идентификатор виртуальной ЛВС (VLAN), связанной со входным интерфейсом.
DST_VLAN	59	2	Идентификатор виртуальной ЛВС (VLAN), связанной с выходным интерфейсом.
IP_PROTOCOL_VERSION	60	1	Номер версии протокола IP (4 для IPv4, 6 для IPv6). При отсутствии в шаблоне предполагается версия 4.
DIRECTION	61	1	Направление потока: 0 — входной; 1 — выходной.
IPV6_NEXT_HOP	62	16	Адрес IPv6 для следующего маршрутизатора.
BGP_IPV6_NEXT_HOP	63	16	Следующий маршрутизатор в домене BGP.
IPV6_OPTION_HEADERS	64	4	Битовое поле, показывающее заголовки опций IPv6, обнаруженные в потоке.
MPLS_LABEL_1	70	3	Метка MPLS на позиции 1 в стеке.
MPLS_LABEL_2	71	3	Метка MPLS на позиции 2 в стеке.
MPLS_LABEL_3	72	3	Метка MPLS на позиции 3 в стеке.

[1]Forwarding Equivalent Class
[2]В оригинале ошибочно указано FLOW_SAMPLER_MODE. *Прим. перев.*

Тип поля	*Код*	*Размер в байтах*	*Описание*
MPLS_LABEL_4	73	3	Метка MPLS на позиции 4 в стеке.
MPLS_LABEL_5	74	3	Метка MPLS на позиции 5 в стеке.
MPLS_LABEL_6	75	3	Метка MPLS на позиции 6 в стеке.
MPLS_LABEL_7	76	3	Метка MPLS на позиции 7 в стеке.
MPLS_LABEL_8	77	3	Метка MPLS на позиции 8 в стеке.
MPLS_LABEL_9	78	3	Метка MPLS на позиции 9 в стеке.
MPLS_LABEL_10	79	3	Метка MPLS на позиции 10 в стеке.

Значение поля является числовым идентификатором данного типа. Для фирменных полей зарезервированы значения: 25, 26, 43 - 45, 51 - 54 и 65 - 69.

При необходимости расширения в список будут добавляться новые типы полей. Новые типы учитываются на стороне экспортера и коллектора, но формат экспорта NetFlow при этом не меняется. Список обновлений типов полей доступен на сайте http://www.cisco.com.

В некоторых случаях размер поля фиксирован по определению (например, для полей PROTOCOL и IPV4_SRC_ADDR). Однако часть типов имеет переменный размер. Это повышает эффективность использования памяти на коллекторе и снижает загрузку сети, по которой осуществляется обмен данными между экспортером и коллектором. Например, для поля IN_BYTES маршрутизатору доступа может быть достаточно 32-битового счетчика (N = 4), а магистральному маршрутизатору потребуется 64 бита (N = 8).

Все счетчики и другие числовые объекты выражаются бесзнаковыми целыми числами размерностью N * 8 битов.

9. Коллектор

Коллектор получает записи Template от экспортера (обычно до получения записей Flow Data или Options Data). Записи Flow Data (или Options Data) в этом случае могут декодироваться и сохраняться на локальных устройствах. Если записи Template не были получены к моменту приема Flow Data (или Options Data), коллектору **следует** сохранять записи Flow Data (или Options Data) и декодировать их после приема Template. Для коллектора **недопустимо** предполагать, что Data FlowSet и связанный с ним Template FlowSet (или Options Template FlowSet) экспортируются в одном пакете.

Для коллектора **недопустимо** предполагать, что в пакете экспорта содержится один и только один набор Template FlowSet.

Срок жизни шаблона в коллекторе ограничен фиксированным тайм-аутом обновления. Срок существования шаблонов, не обновленных экспортером до тайм-аута, истекает. Для коллектора **недопустимы** попытки декодирования записей Flow или Options Data с истекшим сроком существования шаблона. В любой момент времени коллектору **следует** поддерживать для всех текущих записей Template и Options Template информацию об экспортере, области наблюдения, последнем полученном пакете экспорта, а также Template ID и определение шаблона.

Отметим, что область наблюдения идентифицируется полем Source ID из пакета экспорта.

При изменении конфигурации часов на стороне экспортера коллектору **следует** отбросить все записи Template и Options Template, связанные с этим экспортером, чтобы коллектор получил новый набор значений Exporter, Observation Domain, Template ID, Template Definition, Last Received.

Значение Template ID уникально для экспортера и области наблюдения.

Если коллектор получает новую запись Template (например, при перезапуске экспортера), он **должен** незамедлительно переписать существующую запись Template.

В заключение отметим, что коллектор **должен** принимать байты заполнения в наборах Data FlowSet и Options Template FlowSet, которые могут использоваться для записей Flow Data, Options Data и Template. Информация о типах записей приведена в таблице параграфа 2.1.

10. Вопросы безопасности

Протокол NetFlow версии 9 был разработан в предположении, что экспортер и коллектор находятся в одной приватной сети. Однако этот протокол может использоваться для передачи записей о потоках через публичную сеть Internet, что подвергает записи Flow различным угрозам. Например, атакующий может захватывать, менять или вставлять пакеты экспорта. Следовательно, существует риск перехвата или подмены информации IP Flow в целях атаки на коллектор NetFlow.

Разработчики NetFlow версии 9 не предъявляли каких-либо требований по конфиденциальности, целостности или аутентификации, поскольку это вело бы к снижению эффективности протокола, а на момент основных работ по созданию протокола предполагалось, что экспортер и коллектор будут размещаться в одной частной сети в достаточной близости один от другого.

Протокол IPFIX, использующий NetFlow версии 9 в качестве базового протокола, снимает описанные здесь проблемы безопасности. Дополнительную информацию можно найти в проекте требований IPFIX по безопасности [RFC3917].

10.1. Раскрытие данных из потока

Поскольку пакеты экспорта NetFlow версии 9 не шифруются, просмотр записей Flow может дать атакующему информацию об активных потоках в сети, конечных точках обмена данными и картине трафика. Эта информация может использоваться для шпионажа за пользователями и планирования будущих атак.

Информация, которую атакующий может получить при перехвате записей Flow, зависит от определения потоков. Например, запись о потоке, содержащая IP-адреса отправителя и получателя может раскрывать приватные данные о действиях конечных пользователей, тогда как запись Flow, содержащая лишь информацию о сетях отправителя и получателя, будет раскрывать меньше данных.

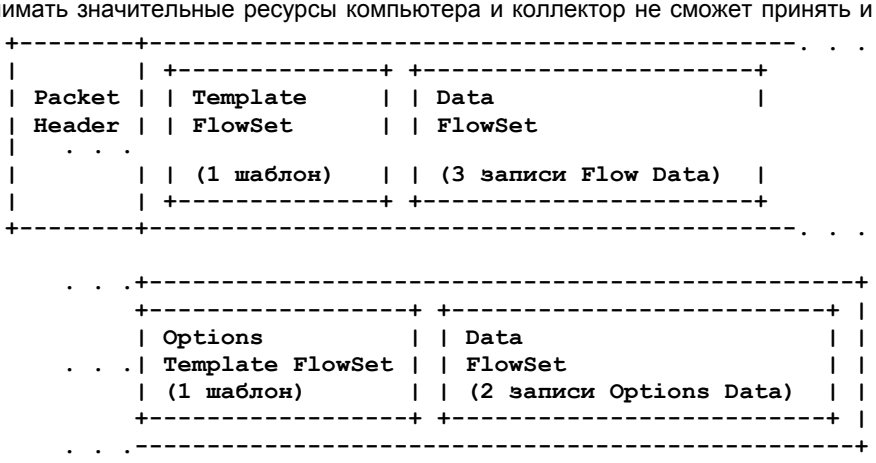
10.2. Фальшивые записи для потоков и шаблонов

Если записи Flow используются в приложениях по учету трафика и/или в защитных приложениях, для атакующих может оказаться весьма привлекательной подмена таких записей (например, для обмана поставщика услуг или сокрытия атаки). Подмена записей Flow может осуществляться путем изменения записей на пути между наблюдателем и коллектором или путем вставки фальшивых записей Flow, как будто они созданы экспортером.

Атакующий может подменить шаблоны и/или шаблоны опций, чтобы таким образом попытаться ввести в заблуждение коллектор NetFlow, убеждая его в неспособности декодировать пакеты экспорта.

10.3. Атаки на коллектор NetFlow

DoS-атаки на коллектор NetFlow могут отнимать значительные ресурсы компьютера и коллектор не сможет принять и декодировать некоторые пакеты экспорта NetFlow. Эта опасность не является специфической для NetFlow версии 9 и для снижения вредного влияния могут применяться существующие методы смягчения DoS-атак.



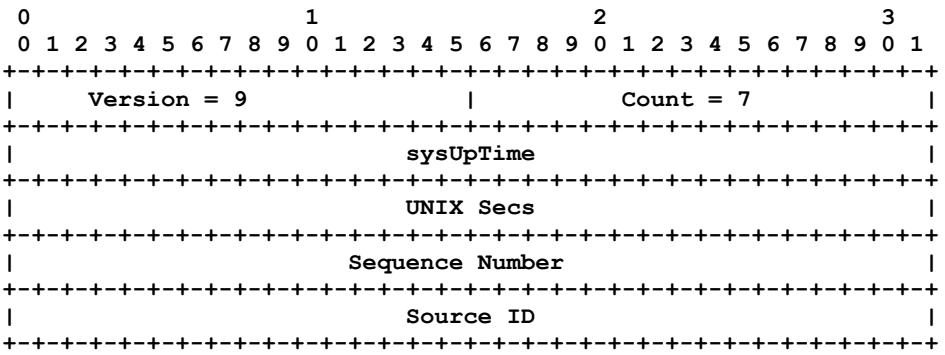
11. Примеры

Рассмотрим пакет экспорта, включающий Template FlowSet, Data FlowSet (с тремя записями Flow Data), Options Template FlowSet и Data FlowSet (с 2 записями Options Data).

Формат пакета показан на рисунке.

11.1. Пример заголовка пакета

Заголовок пакета показан на рисунке.

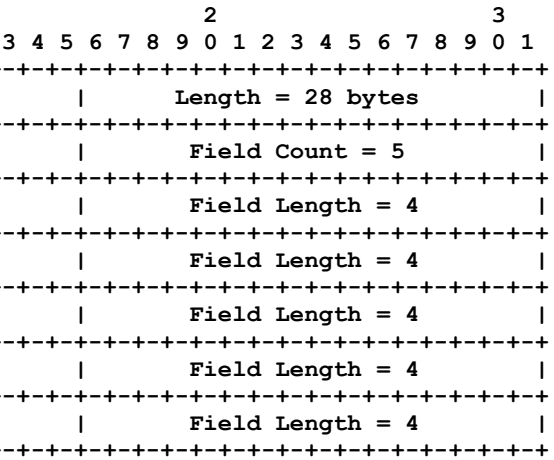


11.2. Пример шаблона FlowSet

Мы хоти включить в отчет следующие типы полей:

- IP-адрес отправителя (IPv4), размером 4 байта;
- IP-адрес получателя (IPv4), размером 4 байта;
- IP-адрес следующего маршрутизатора (IPv4), размером 4 байта;
- число байтов в потоке;
- число пакетов в потоке.

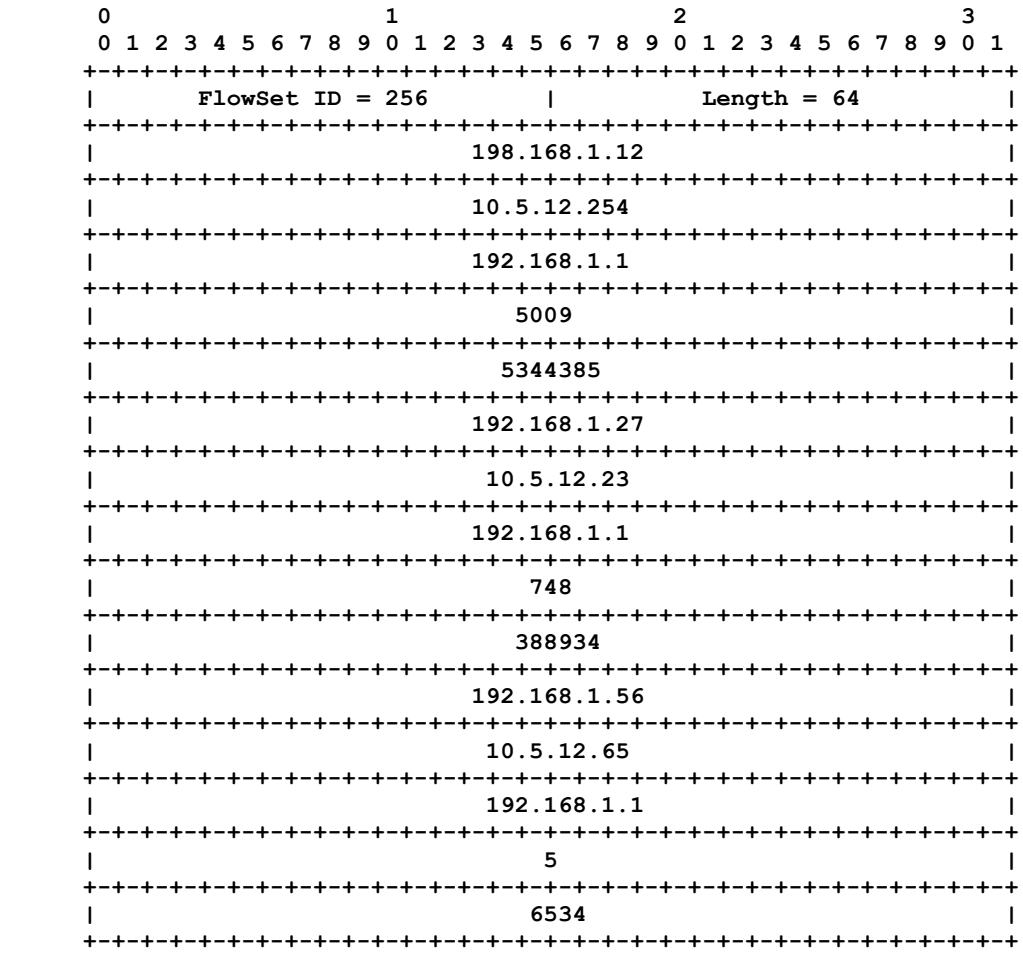
Следовательно, набор Template FlowSet будет иметь вид:



11.3. Пример Data FlowSet

В этом примере отчет включает три записи о потоках:

IP-адрес отправителя	IP-адрес получателя	Адрес следующего маршрутизатора	Число пакетов	Число байтов
198.168.1.12	10.5.12.254	192.168.1.1	5009	5344385
192.168.1.27	10.5.12.23	192.168.1.1	748	388934
192.168.1.56	10.5.12.65	192.168.1.1	5	6534



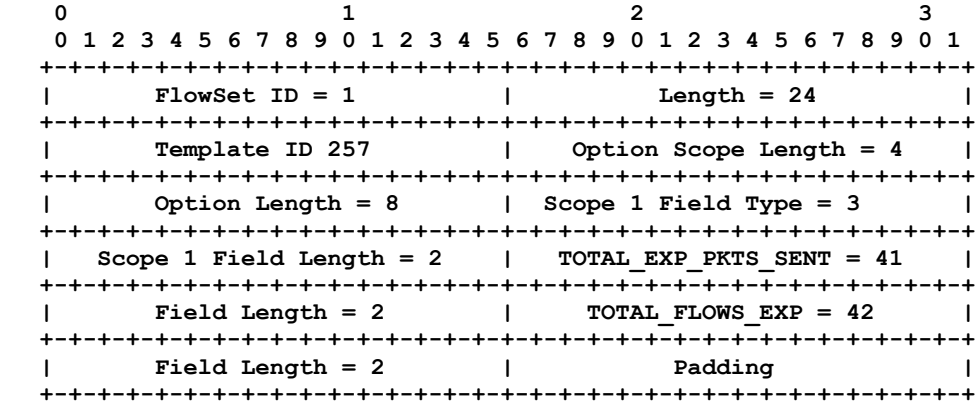
Отметим, что заполнение в этом примере не требуется.

11.4. Пример Options Template FlowSet

Для каждой из двух линейных плат, с которыми связан экспортер, в отчет включаются следующие типы полей:

- общее число пакетов экспорта;
- общее число экспортируемых потоков;

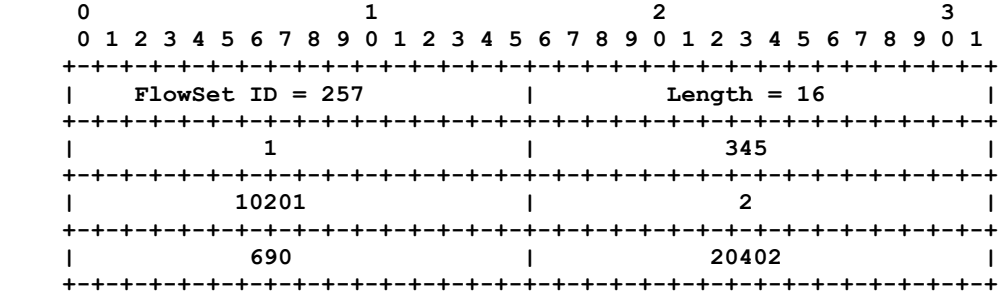
Формат Options Template FlowSet показан на рисунке.



11.5. Пример Data FlowSet с записями Options Data

В этом примере отчет включает две записи.

Идентификатор линейной платы	Пакет экспорта	Поток экспорта
1	345	10201
2	690	20402



12. Литература

12.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119[1], March 1997.

12.2. Дополнительная литература

[RFC768] Postel, J., "User Datagram Protocol", STD 6, RFC 768[1], August 1980.

[RFC793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793[1], September 1981.

[RFC2960] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L., and V. Paxson, "Stream Control Transmission Protocol", RFC 2960[1], October 2000.

[RFC3917] Quittek, J., Zseby, T., Claise, B., and S. Zander, "Requirements for IP Flow Information Export (IPFIX)", RFC 3917, October 2004.

13. Авторы

Этот документ совместно написали Vamsidhar Valluri, Martin Djernaes, Ganesh Sadasivan и Benoit Claise.

14. Благодарности

Авторы благодарны Pritam Shah, Paul Kohler, Dmitri Bouianovski и Stewart Bryant за их ценные технические замечания.

15. Адреса авторов

Benoit Claise (Editor)

Cisco Systems

De Kleetlaan 6a b1

1831 Diegem

Belgium

Phone: +32 2 704 5622

EMail: bclaise@cisco.com

Ganesh Sadasivan

Cisco Systems, Inc.

3750 Cisco Way

San Jose, CA 95134

USA

Phone: +1 408 527-0251

EMail: gsadasiv@cisco.com

Vamsi Valluri

Cisco Systems, Inc.

510 McCarthy Blvd.

San Jose, CA 95035

USA

Phone: +1 408 525-1835

EMail: vvalluri@cisco.com

[1]Перевод этого документа имеется на сайте www.protocols.ru. *Прим. перев.*

Martin Djernaes

Cisco Systems, Inc.

510 McCarthy Blvd.

San Jose, CA 95035

USA

Phone: +1 408 853-1676

EMail: djernaes@cisco.com

Перевод на русский язык
Николай Малых
nmalykh@gmail.com

16. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor в настоящее время обеспечивается Internet Society.