Что такое NetFlow?

Понятие **NetFlow** состоит из 2-х слов: Net – сеть и Flow – поток. Соответственно, NetFlow означает Сетевой Поток. Это понятие применила компания **Cisco Systems** для своей технологии, используемой в операционной системе **Cisco IOS**. В соответствии с NetFlow протоколом выполняется анализ пакетов, проходящих через определенный интерфейс сетевого устройства, на основе чего формируется информация в определенном формате о параметрах различных сетевых потоков, проходящих через этот интерфейс, и эта информация передается по IP сети специальной программе, называемой NetFlow коллектором (NetFlow collector). Программа NetFlow коллектор, устанавливается на каком-то компьютере (сервере) сети, и занимается сбором и первичной обработкой информации от одного или группы сетевых устройств, передающих данные в формате NetFlow. Далее уже используются программы, анализирующие собранные данные и предоставляющие пользователю требуемые ему отчеты о работе сети.

Чем же характерен сетевой поток? Сетевой поток идентифицируется, как однонаправленный поток пакетов между определенным источником и приемником данных, которые характеризуются IP адресами и используемыми портами. Если же быть точнее, то для уникальной идентификации потока используется 7 полей:

- IP адрес источника данных;
- IP адрес приемника данных;
- Номер порта источника данных;
- Номер порта приемника данных;
- Тип протокола 3-го уровня;
- Тип сервиса IP пакетов (ToS);
- Входной логический интерфейс.

Рисунок 1

Пример сетевого потока через сетевой интерфейс Inf1(127.0.0.1) из IP порта 61418 с IP адресом 10.10.5.24 на IP порт 5060 сетевого устройства с IP адресом 195.5.0.116 с использованием протокола UDP и типом сервиса, равным 0, показан на рисунке 1. В большинстве случаев, как правило, присутствует и обратный сетевой поток с аналогичными параметрами (иногда может отличаться Тип сервиса - ToS). Обратный сетевой поток с аналогичными параметрами будет отсутствовать для группой и широковещательных рассылок, так как приемниками данных в этих случаях выступают специальные (групповые или широковещательные) IP адреса. Перечень таких IP адресов можно найти в RFC 3330 [1].

Перечисленные выше поля являются ключевыми в протоколе NetFlow всех версий.

Рассмотрим, какие версии протокола NetFlow существуют. **Версия 1** протокола NetFlow

на сегодняшний день уже устарела и не используется. **Версии 2-4**, а также **версия 6** никогда не включались в Cisco IOS, и, соответственно, не поддерживаются. Одной из наиболее популярных стала **версия 5**, в который была добавлена информация об номерах автономных систем, используемых в протоколе граничного шлюза (Border Gateway Protocol — BGP), и номер потока. Эта версия до сих пор используется, если нет потребности в дополнительной информации, которая предоставляется более поздними версиями протокола. **Версия 7** стала развитием версии 5 и она стала поддерживаться в серии коммутаторов Cisco Catalyst. В **версии 8** была введена возможность агрегации данных, что актуально при больших объемах данных протокола NetFlow. И, наконец, в последней **версии, 9-й**, протокола NetFlow количество полей существенно увеличилось по сравнению с версией 5. Эти дополнительные поля позволяют расширить и уточнить информацию, проходящую в сетевом потоке. Например, версия 9 включает информацию 2-го уровня сетевой модели: поддержка IPv6, групповых (Muticast) рассылок, параметры протоколов MPLS, BGP и другое. Но основное новшество версии 9 — это использование шаблонов, что обеспечивает легкое расширение протокола за счет использования новых типов шаблонов данных. Более подробное описание протокола NetFlow версий 5 и 9 будет приведено ниже.

Поскольку компания Cisco Systems применила протокол NetFlow в операционной системе Cisco IOS, то, соответственно, он использовался в устройствах этой компании, в частности, в маршрутизаторах, серверах доступа. В настоящее время, благодаря своей успешности и дальнейшему усовершенствованию, этот протокол применяется и в других сетевых устройствах (коммутаторах, точках доступа и т.п.) этой компании. На базе NetFlow версии 9 сообществом IETF был принят стандарт **IPFIX** (**IP F**low **I**nformation e**X**port), который применяется рядом производителей сетевого оборудования, в частности, Avaya-Nortel и другими. Были также созданы подобные NetFlow протоколы другими компаниями - производителями сетевого оборудования:

- Flow (Foundry Networks),
- NetStream (HP - 3Com, H3C, Huawei),
- Cflowd (Alcatel, Lucent),
- Jflow & cflowd (JunIPer Networks),
- и другие.

Существуют также программы - сенсоры NetFlow или подобных ему протоколов для компьютеров с различными операционными системами, которые позволяют формировать информацию о сетевых потоках, проходящих через интерфейсы компьютера.

Информация, полученная с помощью NetFlow протокола, может использоваться в целом ряде приложений:

- **Мониторинг сети**.
  Данные NetFlow протокола позволяют осуществлять мониторинг состояния сети. С помощью программ, обрабатывающих накопленные данные от NetFlow коллекторов, можно оценить трафик по отдельным сетевым устройствам (пиковый, усредненный, по определенному интерфейсу и т.п.), выявлять проблемы, возникающие в сети (перегрузка или отказ каких-то сетевых устройств, несанкционированные действия в сети и т.п.) и соответственно быстро принимать решения по устранению этих проблем.
- **Мониторинг приложений**.
  Данные NetFlow протокола позволяют сетевым администраторам иметь точную информацию том, какие приложение в какое время используются в сети, выявлять, какие из приложении наибольшим образом нагружают сеть. Это может использоваться для планирования новых сервисов, таких как передача голоса через IP (VoIP), IPTV, видео по запросу и т.п., и распределения программных приложений в сети.
- **Мониторинг пользователей**.
  Данные NetFlow протокола позволяют собирать детальную информацию по каждому пользователю сети, о том какие сетевые ресурсы им используются в конкретный момент

времени, какие используются приложения, с какими IP адресами работает и тому подобное. Эта информация может использоваться для эффективного планирования сети и распределения доступа пользователей к сетевым ресурсам, определения требуемой для них полосы пропускания, а также обнаружения возможных проблем с безопасностью.

- **Планирование развития сети**.
  Если обеспечить сбор и анализ данных NetFlow протокола за длительный период времени, то можно выявить тенденции по росту сети и на основе этих данных заблаговременно спланировать необходимое ее развитие, за счет увеличения числа или производительности маршрутизаторов, расширения полосы пропускания, изменения в политике маршрутизации сетевых потоков. NetFlow протокол позволяет минимизировать общую стоимость сетевых операций и в тоже время увеличить производительность сети, ее возможности и надежность. NetFlow позволяет обнаружить нежелательный внешний трафик, контролировать качество сервиса (QOS) и анализировать последствия внедрения в сеть новых сетевых приложений.
- **Анализ безопасности в сети**.
  Используя NetFlow протокол можно идентифицировать и классифицировать атаки по отказу в обслуживании (DDOS атаки), выявлять трафик, генерируемый вирусами и троянскими программами в реальном времени. Анализируя сетевое проведение, можно оперативно выявить аномалии в сети и принять меры для их устранения.
- **Учет используемых сетевых ресурсов. Биллинг**.
  Существует несколько механизмов для учета используемых пользователями сетевых ресурсов. Один из них, который широко используется, это на основе данных NetFlow протокола. Он обеспечивает точной информацией о переданном/принятом трафике, на какие или с каких IP адресов, по каким портам и какие конкретно время. На основании чего можно выставлять пользователям счета, если пользователем не используется безлимитный пакет.

NetFlow кэширование и экспорт

Рассмотрим механизм, того, как происходит сбор информации о сетевых потоках и их экспортирование в оборудовании Cisco Systems. Программный модуль на сетевом устройстве просматривает пакеты, проходящие через сетевой интерфейс, и на основании их анализа формирует данные по каждому сетевому потоку, проходящему через этот интерфейс в формате NetFlow протокола. Эти данные в виде отдельных записей по каждому сетевому потоку временно складываются в кэш (кэшируются). Каждая запись о потоке имеет уникальный идентификатор. Периодически данные из кэша пересылаются через сетевой интерфейс на компьютер (сервер), на котором установлена программа NetFlow коллектора (рисунок 2).

Таким образом, использование NetFlow протокола несколько дополнительно загружает сетевой интерфейс. Однако, благодаря очень высокой эффективности протокола, передаваемые с помощью него данные занимают всего около 1,5% от трафика коммутатора или маршрутизатора [2]. NetFlow протокол подсчитывает практически все пакеты и обеспечивает сжатый, но достаточно информативный обзор о всем сетевом трафике по заданному сетевому интерфейсу. Экспортирование данных из кэша выполняется по определенным правилам:

- Записи о сетевых потоках хранятся в кэше заданный промежуток времени. По истечению этого времени они удаляются. По умолчанию в устройствах Cisco Systems записи могут храниться 30 минут.
- Если кэш полностью заполняется, то часть записей удаляется.
- TCP соединения, у которых прекратился поток (FIN) или к которым применена

перезагрузка (RST), будут считаться утратившими силу.

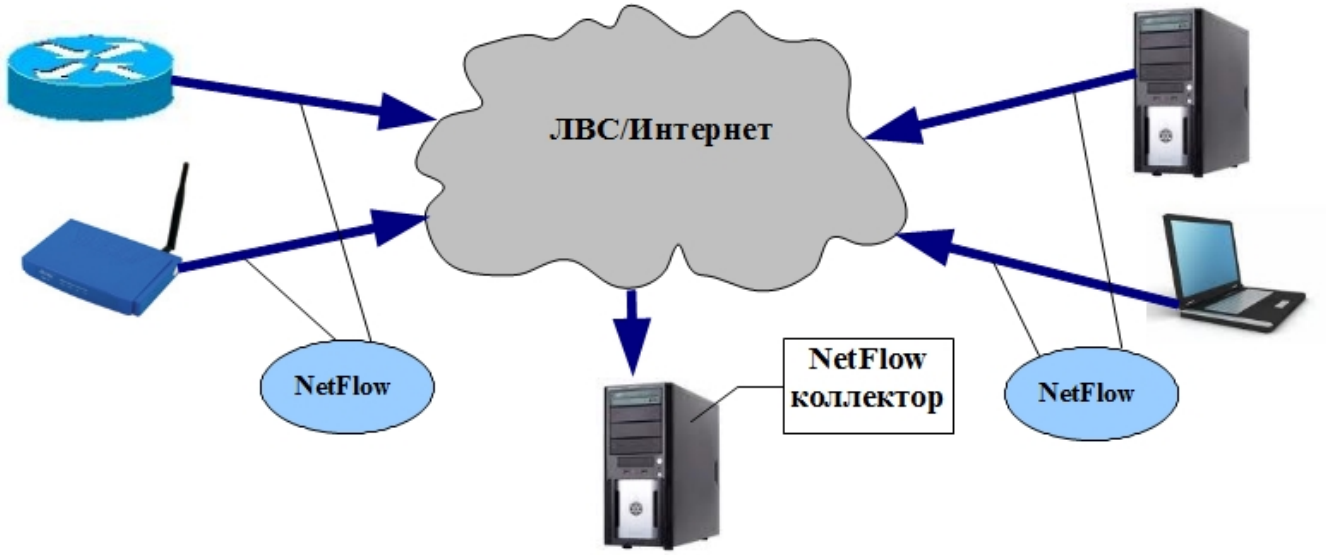

Рисунок 2

Записи о сетевых потоках, которые утратили силу группируются в "NetFlow Export" дейтаграммы и экспортируются на сетевое устройство (компьютер), с установленным NetFlow коллектором. Такие дейтаграммы могут содержать до 30 записей для NetFlow протоколов версий 5 или 9. Настройка NetFlow протокола выполняется для каждого интерфейса сетевого устройства. Для экспорта информации требуется указать IP адрес и номер порта устройства, где будет работать NetFlow коллектор.

NetFlow агрегация

Как упоминалось выше, начиная с версии 8, протокол NetFlow поддерживает агрегацию данных. Использовать агрегацию рекомендуется, если ожидается большой объем данных по этому протоколу от множества сетевых устройств с большим количеством интерфейсов. Применение агрегации позволяет снизит ширину полосы пропускания, необходимую для передачи NetFlow данных, снизить нагрузку на компьютер с NetFlow коллектором и сэкономить объем жесткого диска, необходимый для хранения обработанных коллектором NetFlow данных. Хотя, естественно, при этом часть информации будет утеряна. Компанией Cisco Systems предлагается 11 вариантов схем агрегации: шесть, основанных, на параметре Тип сервиса (ToS) и пять, которые не используют этот параметр.

Схемы агрегации без ToS:

- по автономным системам;
- по префиксу приемника данных;
- по префиксу;
- на основе протокол — порт;
- по префиксу источника данных.

Схемы агрегации на основе ToS:

- автономная система — ToS;
- префикс приемника данных — ToS;
- префикс — ToS;

- протокол — порт — ToS;
- префикс источника данных — ToS;
- префикс — порт.

Поля NetFlow версии 5

Краткое описание полей, которые содержатся в NetFlow протоколе версии 5, приведено в таблице 1.

Таблица 1

Наименование	Описание
srcaddr	IP адрес источника данных
dstaddr	IP адрес приемника данных
nexthop	IP адрес следующего сетевого устройства (маршрутизатора), через которых будут пересылаться пакеты данных
input	Входной интерфейс
output	Выходной интерфейс
dPkts	Количество пакетов в потоке
dOctets	Количество байт в потоке
first	Время начала потока в системе SysUptime
last	Время SysUptime, когда последний пакет потока был получен
scrport	Номер порта источника данных (4-го уровня сетевой модели)
dstport	Номер порта приемника данных (4-го уровня сетевой модели)
pad1	неиспользуемый байт
tcp_flags	TCP флаги
prot	Протокол 4-го уровня (например, 6=TCP, 17=UDP и т.п.)
tos	Тип сервиса IP протокола
scr_as	Номер автономной системы источника данных
dst_as	Номер автономной системы приемника данных
scr_mask	Маска адреса источника данных
dst_mask	Маска адреса приемника данных
pad2	неиспользуемый байт

Для большинства задач, которые решаются администратором сети и которые перечислялись в начале статьи, указанных выше полей достаточно для проведение детального анализа работы сети.

Поля NetFlow версии 9

Краткое описание полей, которые содержатся в NetFlow протоколе версии 9 [3], приведено в таблице 2.

Таблица 2

Наименование	Описание
IN_BYTES	Входящий счетчик с длиной N x 8 бит для количества байт, связанных с IP потоком.
IN_PKTS	Входящий счетчик с длиной N x 8 бит для количества пакетов, связанных с IP потоком.
FLOWS	Количество потоков, которое агрегируется. По умолчанию 4.
PROTOCOL	IP протокол
SRC_TOS	Тип Сервиса для входящего интерфейса
TCP_FLAGS	Совокупность всех TCP флагов для этого потока
L4_SRC_PORT	Номер порта TCP/UDP источника: FTP, Telnet и т.п.
IPV4_SRC_ADDR	Адрес источника данных IP протокола версии 4
SRC_MASK	Маска источника данных
INPUT_SNMP	Индекс входящего интерфейса; по умолчанию 2, но могут использоваться и более высокие значения.
L4_DST_PORT	Номер порта TCP/UDP приемника: FTP, Telnet и т.п.
PV4_DST_ADDR	Адрес приемника данных протокола IP версии 4
DST_MASK	Маска приемника данных
OUTPUT_SNMP	Индекс исходящего интерфейса; по умолчанию 2, но могут использоваться более высокие значения.
IPV4_NEXT_HOP	IPv4 адрес следующего маршрутизатора (next-hop router)
SRC_AS	Номер автономной системы BGP источника. Значение по умолчанию: 2. Также может быть и 4
DST_AS	Номер автономной системы BGP приемника. Значение по умолчанию: 2. Также может быть и 4
BGP_IPV4_NEXT_HOP	IP адрес следующего маршрутизатора в BGP домене
MUL_DST_PKTS	Счетчик групповых исходящих IP пакетов с длиной N x 8 бит для пакетов, связанных с IP потоком
MUL_DST_BYTES	Счетчик групповых исходящих IP байт с длиной N x 8 бит для байтов, связанных с IP потоком
LAST_SWITCHED	Системное время работы, при котором последний пакет в этом потоке был скоммутирован.
FIRST_SWITCHED	Системное время работы, при котором первый пакет в этом потоке был скоммутирован.
OUT_BYTES	Исходящий счетчик с длиной N x 8 бит для количества байт, связанных с IP потоком
OUT_PKTS	Исходящий счетчик с длиной N x 8 бит для числа пакетов, связанных с IP потоком.
MIN_PKT_LNGTH	Минимальная длина IP пакета для входящих пакетов потока
MAX_PKT_LNGTH	Максимальная длина IP пакета для входящих пакетов потока
IPV6_SRC_ADDR	IPv6 адрес источника данных

IPV6_DST_ADDR	IPv6 адрес приемника данных
IPV6_SRC_MASK	Длина маски IPv6 источника данных
IPV6_DST_MASK	Длина маски IPv6 приемника данных
IPV6_FLOW_LABEL	Ярлык потока IPv6, как определено в RFC 2460
ICMP_TYPE	Тип пакета межсетевого протокола управляющих сообщений (Internet Control Message Protocol - ICMP); выводятся как: ((ICMP Type*256) + ICMP code)
MUL_IGMP_TYPE	Тип пакета протокола управления группами Интернет (Internet Group Management Protocol - IGMP)
SAMPLING_INTERVAL	Используется для выборочного потока NetFlow. Частота, с которой выбираются пакеты. Т.е. 100 будет означать, что выбирается каждый 100-й пакет.
SAMPLING_ALGORITHM	Тип алгоритма, используемого для выборки NetFlow: 0x01 — детерминированная выборка; 0x02 — случайная выборка.
FLOW_ACTIVE_TIMEOUT	Величина таймаута (в секундах) для записей неактивного потока в кэш NetFlow.
FLOW_INACTIVE_TIMEOUT	Величина таймаута (в секундах) для записей неактивного потока в NetFlow кэше.
ENGINE_TYPE	Тип потока коммутационной машины: RP=0, VIP/Linecard=1
ENGINE_ID	Идентификатор коммутационной машины
TOTAL_BYTES_EXP	Счетчик с длиной N x 8 бит для байт для количества байт экспортируемых Доменом Наблюдения
TOTAL_PKTS_EXP	Счетчик с длиной N x 8 бит для байт для количества пакетов экспортируемых Доменом Наблюдения
TOTAL_FLOWS_EXP	Счетчик с длиной N x 8 бит для байт для количества потоков экспортируемых Доменом Наблюдения
IPV4_SRC_PREFIX	Префикс адреса IPv4 источника (специально для архитектуры Catalyst)
IPV4_DST_PREFIX	Префикс адреса IPv4 приемника (специально для архитектуры Catalyst)
MPLS_TOP_LABEL_TYPE	MPLS Top Label Type: 0x00 UNKNOWN 0x01 TE-MIDPT 0x02 ATOM 0x03 VPN 0x04 BGP 0x05 LDP
MPLS_TOP_LABEL_IP_ADDR	Переадресуемый Эквивалентный Класс (Forwarding Equivalent Class) соответствующий верхней метки MPLS
FLOW_SAMPLER_ID	Идентификатор, показанный в “show flow-sampler”
FLOW_SAMPLER_MODE	Тип алгоритма, используемого для выборочных данных: 0x02 случайный выбор. Используется совместно с FLOW_SAMPLER_MODE
FLOW_SAMPLER_RANDOM_INTERVAL	Пакетный интервал, с которым осуществляется выборка. Используется совместно с FLOW_SAMPLER_MODE
MIN_TTL	Минимальное время жизни пакетов (TTL) для входящего потока.
MAX_TTL	Максимальное время жизни пакетов (TTL) для исходящего потока.
IPV4_IDENT	Идентификационное поле IPv4.
DST_TOS	Байт типа сервиса, устанавливаемый для исходящего интерфейса.
IN_SRC_MAC	MAC адрес входящего источника
OUT_DST_MAC	MAC адрес исходящего приемника
SRC_VLAN	Идентификатор виртуальной ЛВС, связанный с входящим интерфейсом
DST_VLAN	Идентификатор виртуальной ЛВС, связанный с исходящим интерфейсом
IP_PROTOCOL_VERS	Версия Интернет Протокола. Значение 4 — для IPv4, и 6 — для IPv6. Если

ION	отсутствует в шаблоне, значит, используется версия 4.
DIRECTION	Направление потока: 0 — входящий поток, 1 — исходящий поток.
IPV6_NEXT_HOP	IPv6 адрес для маршрутизатора следующего перехода (скачка).
BPG_IPV6_NEXT_HOP	Ipv6 адрес маршрутизатора следующего перехода в BGP домене.
IPV6_OPTION_HEADERS	Битово-кодируемое поле, идентифицирующее дополнительные заголовки IPv6, обнаруженные в потоке.
MPLS_LABEL_1	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).
MPLS_LABEL_2	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).
MPLS_LABEL_3	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).
MPLS_LABEL_4	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).
MPLS_LABEL_5	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).
MPLS_LABEL_6	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).
MPLS_LABEL_7	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).
MPLS_LABEL_8	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).
MPLS_LABEL_9	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).
MPLS_LABEL_10	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).
IN_DST_MAC	MAC адрес входящего приемника
OUT_SRC_MAC	MAC адрес исходящего источника
IF_NAME	Сокращенное имя интерфейса, например: “FE1/0”
IF_DESC	Полное имя интерфейса, например: “"FastEthernet 1/0”
SAMPLER_NAME	Имя выборки потока
IN_ PERMANENT _BYTES	Счетчик текущего байта для постоянного потока
IN_ PERMANENT _PKTS	Счетчик текущего пакета для постоянного потока
FRAGMENT_OFFSET	Величина фрагментного смещения для фрагментируемых IP пакетов
FORWARDING STATUS	Состояние переадресации, которое кодируется 2-я левыми битами в байте, а остальные 6 бит — указывают код причины переадресации.

Как видно из таблицы 2, число полей в протоколе NetFlow версии 9 существенно расширено по сравнению с версией 5, но это расширение в первую очередь связано с параметрами маршрутизации протокола BGP и протокола мультипротокольной коммутации MPLS. Также включается информация по MAC адресам, что может быть в ряде случаев интересно для анализа. Если пользователь не заинтересован в подобных полях, то он может ограничиться использованием NetFlow прокола версии 5.

NetFlow коллекторы и программы анализа

В настоящее время существует целый ряд программ, которые выполняют сбор и обработку NetFlow информации.

Наша компания, **"Софт Пи Ай"**, готова предложить пользователям ряд своих программных решений для NetFlow протокола.

1. **SoftPI NetFlow Collector**.
   Система SoftPI NetFlow Collector предназначена для сбора информации о сетевых потоках в форматах NetFlow версий 5 или 9(Cisco Systems) и IPFIX (RFC 5101, 5102), а также гибкой агрегации собранной информации с последующим сохранением в хранилище одного из трёх типов: база данных Microsoft SQL, база данных MySQL или текстовый файл, расположенных на копьютерах с операционными системами Windows 2000/XP/2003/Vista/2008/7 (Microsoft). Для обработки информации из хранилища пользователь может использовать любые доступные ему средства, обеспечивающие работу с соответствующим хранилищем данных.
2. **Flansys**.
   Система Flansys предназначена для анализа трафика в сети и может использоваться:
   - администраторами сети — для мониторинга различных параметров сетевых устройств и оптимизации работы сети;
   - сотрудниками службы безопасности — для своевременного обнаружения нежелательного трафика и контроля за состоянием сетевых устройств;
   - обычными пользователями — для анализа сетевого трафика собственного компьютера и выявления аномалий.

   Система Flansys содержит в себе:
   - NetFlow коллектор,
   - хранилище NetFlow информации на базе Microsoft SQL Server,
   - программу Flansys, обеспечивающую мониторинг и анализ как информации в реальном времени, так и ранее накопленной,
   - служба Flansys Alarm предназначена для анализа информации о сетевых потоках в режиме реального времени и оповещения о заданных сетевых события или выполнения пользовательского сценария.
3. **Биллинговая система Tariscope**.
   Обеспечивает учет услуг, оказанных в IP сетях на основании данных протокола NetFlow (включает в себя NetFlow коллектор), ведение данных по абонентам, выставление счетов и других документов, учет карточек предварительной оплаты и другие услуги.
4. **fSonar**.
   Программа fSonar является NetFlow сенсором и предназначена для генерации потока данных в формате протокола NetFlow версии 5 о сетевой активности на одном или группе сетевых интерфейсов компьютера, работающего под управлением операционной системы Windows (Microsoft).

Литература

1. RFC3330 - Special-Use IPv4 Addresses.
2. NetFlow Services Solutions Guide.
3. Cisco IOS NetFlow Version 9 Flow-Record Format.