Описание технологии : sFlow

D-Link HQ, Июнь 2007

Бигаров Руслан, консультант по проектам

e-mail: rbigarov@dlink.ru

D-Link®
Building Networks for People

- Обзор sFlow
- Дейтаграмма sFlow
- Механизм выборки
- Настройка sFlow для DGS-3600
- Инструменты сбора данных sFlow

Обзор

- NetFlow – хорошо известный протокол анализа трафика, используемый компанией Cisco. Протокол sFlow аналогичен NetFlow компании Cisco. И кроме того, этот протокол стандартизирован.
- RFC 3176
- Технология использует механизм выборки для мониторинга трафика в сетях передачи данных, построенных с использованием маршрутизаторов и коммутаторов.
- sFlow (Netflow) обычно используется на уровне распределения и ядра коммутатора / маршрутизатора (Foundry Fast Iron/ Big Iron series, Cisco 45/6500).
- Коммутаторы DGS-3600 R2 D-Link серии xStack поддерживают sFlow.
- Коммутаторы DGS-3400 D-Link серии xStack будут поддерживать sFlow в будущем.

Обзор

- Цель разработки
  - Способность точного мониторинга трафика на скоростях Гигабит/с и выше
  - Позволяет осуществлять управление от 10 до 1000 агентов из единой точки
  - Очень низкая стоимость установки агентов
  - Устранение ограничений RMONv1
    - Mini-RMON: сегодня 95% коммутаторов поддерживают неполную версию RMONv1 - группы 1, 2, 3 и 9
    - Мониторинг сети только на MAC-уровне и ниже.
  - Устранение ограничений RMONv2
    - Расширение RMONv1 и фокусировка на более высоких уровнях трафика (выше MAC-уровня)
    - Поддержка RMONv2 существенно влияет на производительность коммутатора, поэтому сегодня почти нет коммутаторов, поддерживающих RMONv2.
    - Большинство реализаций пересылают копии RMON на порт зеркальный/SPAN для анализа трафика. Но это дорогое и плохо масштабируемое решение.

Обзор

- Преимущества sFlow
  - Стоимостная эффективность

    требуется минимум компьютерных ресурсов
  - Масштабируемый мониторинг трафика для всех сетевых портов, эффективный на скорости Гигабит/с и выше и не влияющий на производительность сети
  - Постоянный мониторинг сети
  - Визуальное представление сети

    Мониторинг трафика на уровнях от L2 до L7 для всех устройств, доступный как в реальном времени, так и в архиве в виде детализированного отчета.
  - Ведение учетных записей и выставление счетов за пользование сетью, предоставление детальных отчетов об использовании сети.
  - Начисление платы за дополнительные услуги (например, VoIP)

Обзор

- Коллектор данных:
  - Получает данные, отправленные агентом sFlow
- База управляющей информации sFlow MIB:
  - Позволяет управлять агентом sFlow Agent через SNMP
- Агент sFlow:
  - Позволяет осуществлять мониторинг трафика с помощью заданного механизма выборки
- Дейтаграмма sFlow:
  - Стандартный формат отправки данных выборки агента sFlow

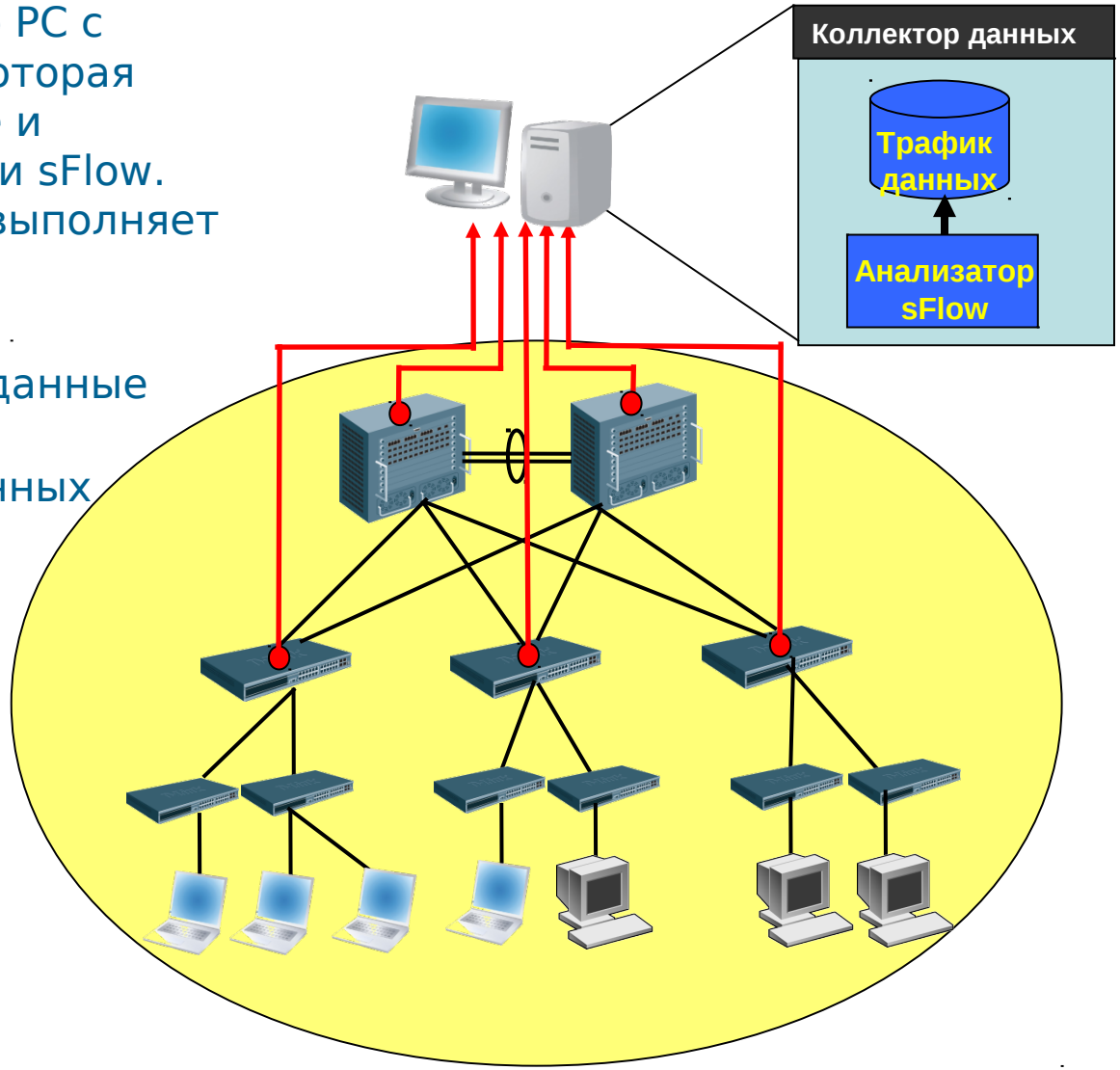
Система мониторинга sFlow

- Коллектор данных

  В большинстве случаев, это PC с запущенной программой, которая позволяет собирать данные и создавать отчеты с данными sFlow. Коллектор данных обычно выполняет 2 функции:
  - Анализатор sFlow

    Собирает/анализирует данные sFlow
  - Место для хранения данных

- Агент sFlow
  - Использует технологию выборки для снятия статистики трафика



Дейтаграмма sFlow

Агенты sFlow

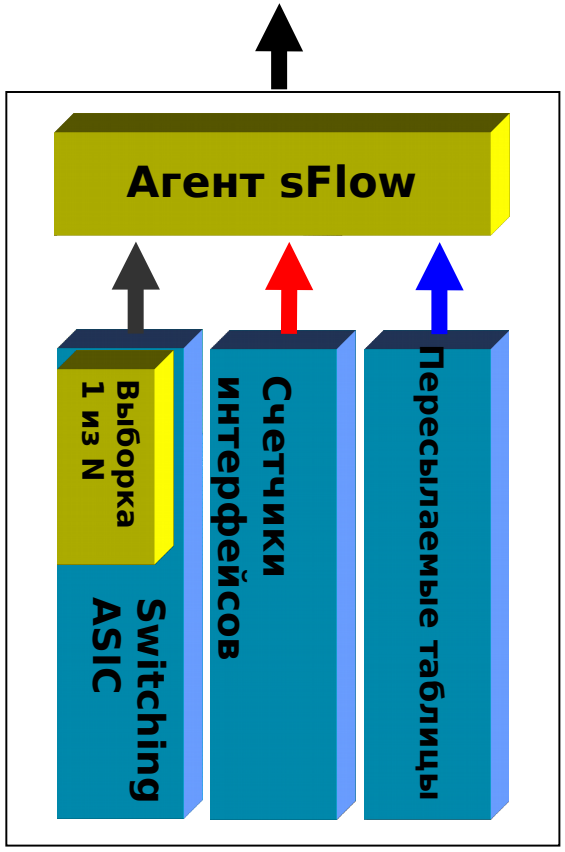
- Обзор sFlow
- Дейтаграмма sFlow
- Механизм выборки
- Настройка sFlow для DGS-3600
- Инструменты сбора данных sFlow

Дейтаграмма sFlow

- Определение
  - Позволяет задать стандартный формат отправки данных выборки агента sFlow на удаленный коллектор данных.
  - UDP-пакет
- Ненадежность UDP-пакета
  - Повторная отправка выборки с новым значением в следующем интервале опроса, если сделанная выборка утеряна.
  - Незначительное снижение эффективности выборки при потере пакетов
  - Сокращение загрузки буфера данных
  - Хорошее средство своевременной доставки информации о трафике в условиях интенсивного трафика.

Дейтаграмма sFlow

Дейтаграмма sFlow передается на UDP-порт 6343 (по умолчанию)



- Заголовок пакета (т.е. MAC,IPv4,IPv6,IPX,AppleTalk,TCP,UDP, ICMP)
- Образец параметров процесса (скорость, пул адресов и т.д.)
- Порты входа/выхода
- Приоритет (802.1p и TOS)
- VLAN (802.1Q)
- Префикс источника/назначения
- Адрес следующего хопа (Next hop)
- Источник AS, Source Peer AS
- Путь к назначению AS
- Сообщества (ccommunities), локальные приоритеты
- Идентификаторы пользователя (TACACS/RADIUS) для источника/назначения
- URL, соответствующие источнику/назначению
- Статистики интерфейсов (RFC 1573, RFC 2233 и RFC 2358)

Коммутатор / Маршрутизатор

Содержимое выборки

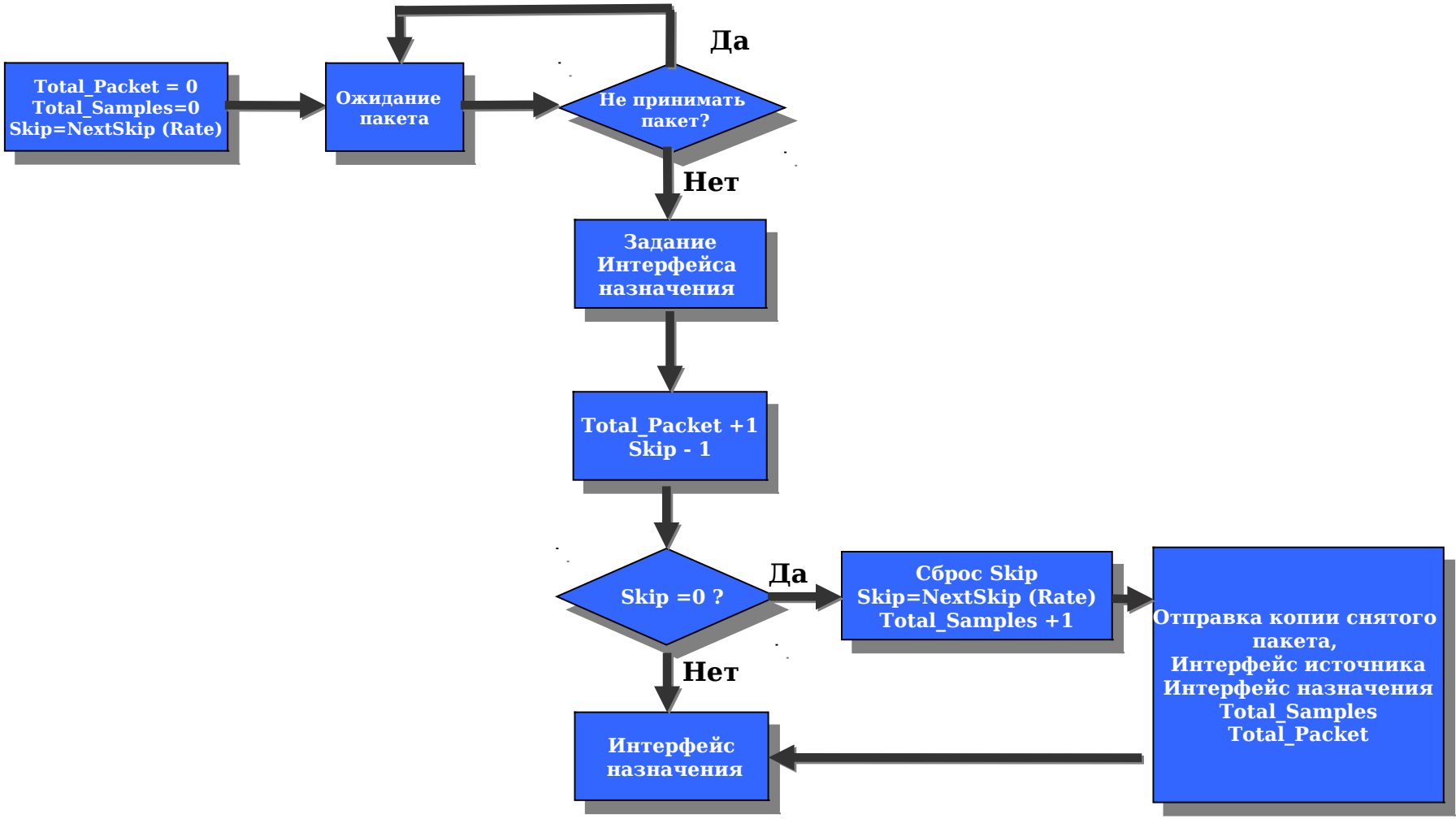
- Протокол
  - Заголовки пакетов
  - Ethernet/802.3
  - IP/ICMP/UDP/TCP
  - IPX
  - Appletalk
- Уровень 2
  - Интерфейс Входа/Выхода
  - Приоритет Входа/Выхода
  - VLAN Входа/Выхода
- Уровень 3
  - Подсеть/префикс источника
  - Подсеть/префикс назначения
  - Next Hop
- BGP4
  - Источник AS
  - Источник Peer AS
  - Назначение AS
  - Назначение Peer AS
  - Сообщества Communities
  - Пути AS

- Обзор sFlow
- Дейтаграмма sFlow
- Механизм выборки
- Настройка sFlow для DGS-3600
- Инструменты сбора данных sFlow

Механизм выборки

- Агент sFlow использует два механизма выборки
  - Статистический механизм выборки на основе пакетов в потоке
  - Выборка сетевой статистики интерфейса на основе времени
- Выборка потока
  - Поток:
    все пакеты, полученные на один интерфейс, вводятся в модуль коммутации/маршрутизации и отправляются на другой интерфейс.
  - Гарантируется, что все пакеты в потоке имеют одинаковые шансы попасть в выборку
  - Выборка статистики сетевых интерфейсов
  - sFlow имеет счетчики опроса для всех источников данных и может периодически выделять ключевую статистику (например, количество отправленных / полученных пакетов, отправленных/полученных байтов, ошибок .. на каждый интерфейс)

Процедура выборки



- Обзор sFlow
- Дейтаграмма sFlow
- Механизм выборки
- Настройка sFlow для DGS-3600
- Инструменты сбора данных sFlow

DGS-3600 Настройка sFlow

- Включение sFlow
  - Включите функцию sFlow на коммутаторе
  - Команда:
    enable sflow
- Создание сервера анализатора sFlow
  - Создает удаленный анализатор sFlow (коллектор) для сбора и анализа дейтаграмм sFlow, приходящих от коммутаторов. Параметр “owner” несет только информационную функцию
  - Команда:
    create sflow analyzer server 1 owner OwnerName
- Настройка IP-адреса сервера анализатора sFlow
  - Команда:
    config sflow analyzer_server collectoraddress 10.90.90.9
- Создание счетчиков опроса sFlow
  - Задает настройки для счетчиков опроса коммутатора. Этот механизм позволяет опрашивать счетчики IF коммутатора (интервал 20 означает 20сек)
  - Команда:
    create sflow counter_poller ports 1-27 analyzer_server_id 1 interval 20
- Создание портов выборки sFlow
  - Задает настройки портов выборки sFlow и решает, как выполнять выборку данных с помощью заданной длины начальных байт (максимальный размер заголовка может быть 1-256 байт).
  - Команда:
    create sflow flow_sampler ports 1:1 analyzer_server_id 1 rate 10000 maxheadersize 128

- Обзор sFlow
- Дейтаграмма sFlow
- Механизм выборки
- Настройка sFlow для DGS-3600
- Инструменты сбора данных sFlow

Инструменты sFlow

- Сейчас все больше и больше вендоров выпускают устройства с поддержкой технологии sFlow.
- В связи с возросшей потребностью в sFlow, многие организации и компании предлагают средства сбора данных sFlow.
- Вот несколько организаций, которые предлагают решения для мониторинга трафика sFlow:
  - Корпорация InMon является главной в продвижении стандарта sFlow
  - sflowtool корпорации InMon – бесплатный инструмент для сбора информации sFlow и получения данных, полезных для разработчиков программного обеспечения.
  - Организация ntop поставляет программное обеспечение “ntop” (бесплатно для платформы Unix и за плату для платформы Windows). Демонстрационная версия Windows рассчитана на 1000 пакетов.
  - ntop предоставляет дружественный пользователю графический интерфейс управления, позволяющий легко создавать Web-отчеты.

sflowtool компании inMon

- Введение в sflowtool
  - InMon Corp.
    - Фокусирует внимание на решениях по мониторингу трафика для высокоскоростных коммутируемых сетей
  - sflowtool будет собирать трафик sFlow на UDP-порту 6343 (по умолчанию)
  - Снимает дейтаграмму sFlow и выводит отчетные данные
  - Выведенные данные могут храниться в виде архива в специальной базе данных
  - Для доступа к базе данных используется PERL, C, C++, JAVA
  - Построение Web-интерфейса с помощью PHP

- Пример полученного отчета

unixSecondsUTC 991362247 (всегда первое поле новой дейтаграммы)
datagramVersion 2
agent 10.0.0.254 (Агент sFlow)
sysUpTime 10391000
packetSequenceNo 5219 (последовательный номер дейтаграммы от этого агента)
samplesInPacket 4
sampleSequenceNo 9466 (последовательный номер снятого пакета)
dropEvents 0
inputPort 14
outputPort 16
packetDataTag INMPACKETTYPE_HEADER
headerProtocol 1

sflowtool

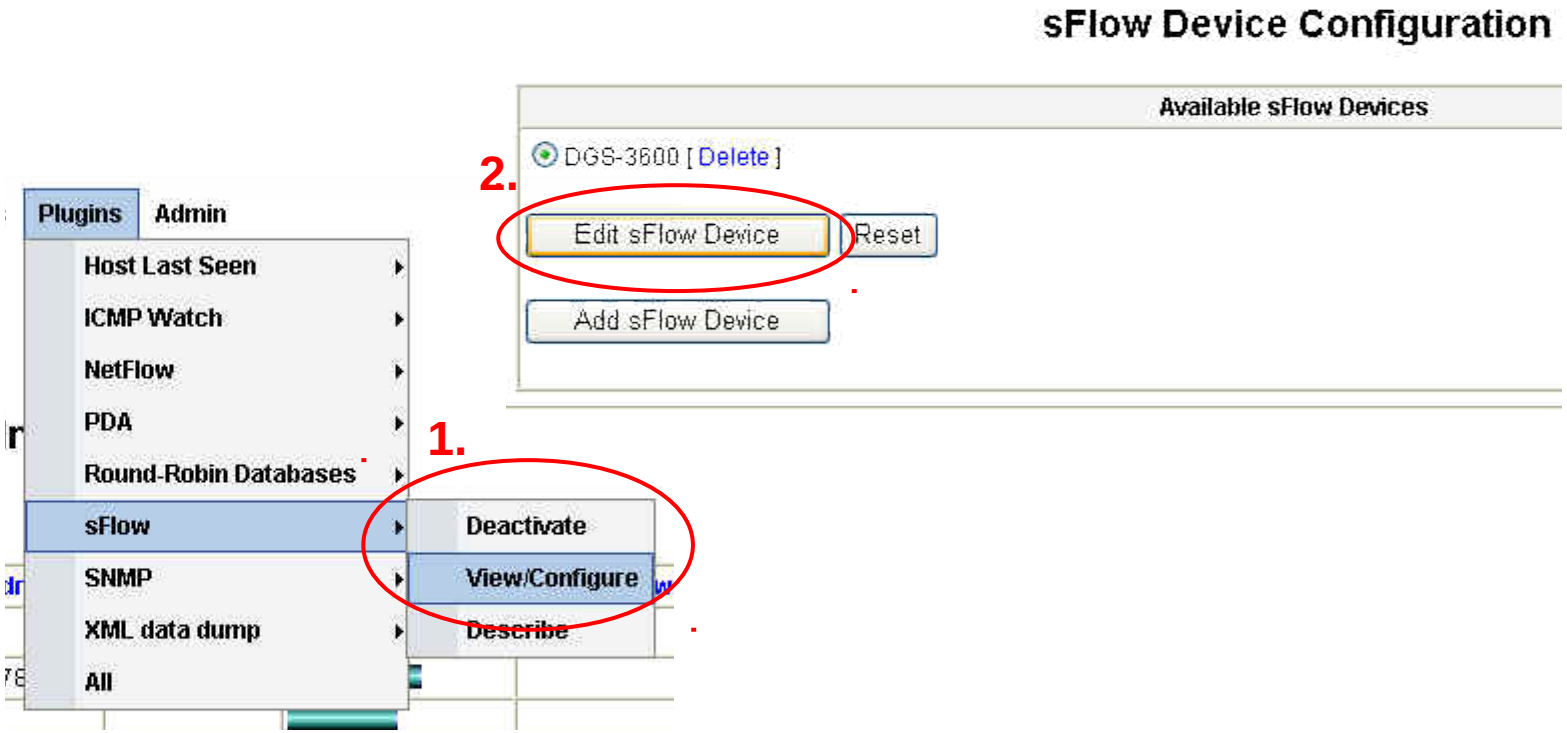
extendedType ROUTER (пересылаемая информация L3)
nextHop 129.250.28.33
srcSubnetMask 24
dstSubnetMask 24
sampleSequenceNo 346 (следующая выборка - выборка счетчика от 0:92)
sourceId 0:92
sampleType COUNTERSSAMPLE
statsSamplingInterval 20
counterBlockVersion 1
ifIndex 92
networkType 53
ifSpeed 0
ifDirection 0
ifStatus 0
ifInOctets 18176791
ifInUcastPkts 92270

- Что такое ntop?
  - Тестовый сетевой трафик, отображающий использование сети
  - Позволяет работать на базе Unix и платформы Win32
  - Пользователь с помощью Web-браузера может перемещаться по информации о трафике и получать информацию о статусе сети

ntop

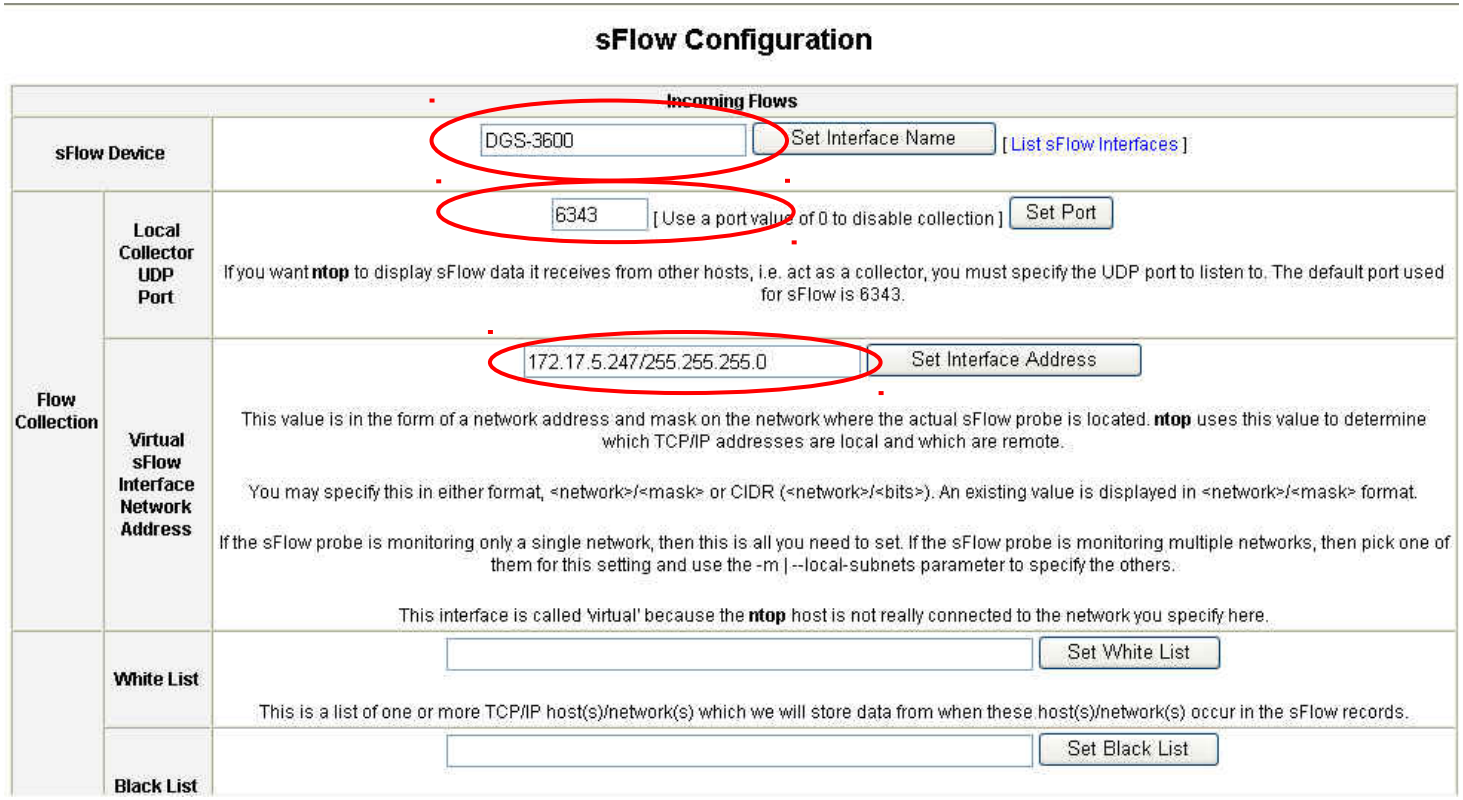
- Что позволяет сделать ntop?
  - Отображает сетевой трафик в соответствии с многими протоколами
  - Сортирует сетевой трафик в соответствии с различными критериями
  - Отображает статистику трафика
  - Идентифицирует подлинность компьютерных пользователей
  - Пассивная идентификация хоста OS (без отправки пробных пакетов)
  - Анализ IP-трафика и его сортировка по источнику / назначению
  - Отображает распределение IP-трафика между различными протоколами
  - Используется для сбора информации NetFlow/sFlow
  - Позволяет сформировать отчет об использовании IP-протокола, отсортированный по типу протокола

- Активизируйте sFlow plug-in
- Настройте sFlow plug-in: выберите пункт “View/Configure”
- Добавьте устройство sFlow: кликните по кнопке “Edit sFlow Device”.



ntop — как настроить ntop

- Введите название устройства с поддержкой sFlow
- Настройте UDP-порт (по умолчанию, 6343)
- Настройте IP-адрес коммутатора, поддерживающего sFlow



ntop — вывод данных ntop

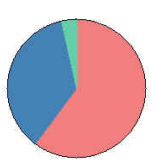
Host Information

Traffic Unit: [Bytes] [Packets]

Host	Domain	IP Address	MAC Address	Other Name(s)	Bandwidth	Nw Board Vendor
myfinux		172.17.98.7				
172.17.5.247		172.17.5.247				
172.17.98.254		172.17.98.254	00:0F:3D:78:6E:00			D-Link C
192.168.15.1		192.168.15.1				
239.255.255.250		239.255.255.250				LAA (Locally assigne
172.17.98.210		172.17.98.210	00:13:46:DA:E3:AD			
172.17.98.211		172.17.98.211	00:13:46:DA:E3:AE			
baym-tw1.msgr.hotmail.com		207.46.110.51				
netbios:00:00:01			03:00:00:00:00:01			
multicast:02:01:01			01:20:DA:02:01:01			
172.17.98.14		172.17.98.14	00:14:85:03:4A:0E			
172.17.98.88		172.17.98.88	00:05:5D:04:2C:20			D-Link Sy
172.17.98.44		172.17.98.44	00:0F:EA:89:54:90			Giga-Byte Technolog
172.17.98.29		172.17.98.29	00:50:BA:0A:F2:94			
0.0.0.0		172.17.98.36	00:02:3F:8B:2A:60			Compal Elect

Traffic Report for 'peth0' [switch]

	Dropped (libpcap)	0.0%	0
	Dropped (ntop)	0.0%	0
	Total Received (ntop)		1,301,564
	Total Packets Processed		1,301,564
	Unicast	36.2%	471,430
	Broadcast	60.4%	786,271
	Multicast	3.4%	43,863
Packets	Shortest		42 bytes
	Average Size		177 bytes
	Longest		8,231 bytes
	<= 64 bytes	43.7%	568,632

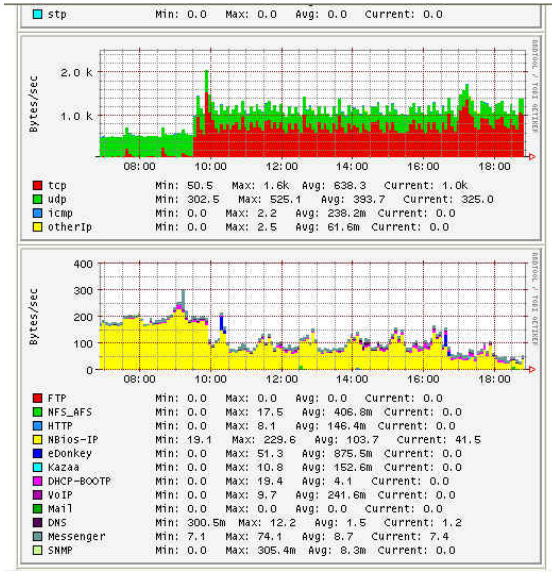


IP	249.6 MB	88.6%	UDP	79.7 MB	31.9%	
			ICMP	47.7 KB	0%	
			ICMPv6	3.4 KB	0%	
			IGMP	39.3 KB	0%	
			Other IP	7.0 KB	0%	
(R)ARP	21.1 MB	8.5%				
IPX	578.7 KB	0%				
NetBios	170.3 KB	0%				
IPv6	67.8 KB	0%				
STP	0.6 KB	0%				
Other	253.0 KB	0%				

TCP/UDP Traffic Port Distribution: Last Minute View

TCP/UDP Port		Total	Sent	Rcvd
sflow	6343	25.1 KB	12.5 KB	12.5 KB
hbci	3000	8.2 KB	6.3 KB	1.9 KB
giop	2481	4.5 KB	740	3.8 KB
ttc	2483	3.1 KB	695	2.4 KB
netbios-ns	137	2.0 KB	1012	1012
netbios-dgm	138	984	492	492
ttc-ssl	2484	674	558	116
41532	41532	422	274	148
msnp	1863	422	148	274
nss-routing	159	372	0	372
pcmail-srv	158	372	0	372
4905	4905	186	186	0
4904	4904	186	186	0
4910	4910	124	124	0
4909	4909	124	124	0
4903	4903	62	62	0
4902	4902	62	62	0

Notes:



Итоги

- sFlow – отраслевой стандарт, предоставляющий различные инструменты для мониторинга и анализа трафика.
- Коммутаторы D-Link семейства xStack, благодаря поддержке sFlow, могут передавать комплексную информацию о трафике. Будь то мониторинг сетевого трафика или информация биллинга для сетей предприятия, кампуса или телекоммуникационной компании.
- Коммутаторы D-Link семейства xStack поддерживают sFlow