УДК 004.942

ОРГАНИЗАЦИЯ СЪЕМА СЕТЕВОГО ТРАФИКА ПО ТЕХНОЛОГИИ NETFLOW БЕЗ ИСПОЛЬЗОВАНИЯ ОБОРУДОВАНИЯ CISCO

Горелов Г.А., Тарасов В. Н.

В статье рассмотрен механизм съема трафика ЛВС нижнего уровня многосегментной сети вуза, основанный на технологии NetFlow, без использования оборудования Cisco. Описаны различные способы подключения оборудования при зеркалировании трафика на ПК-сенсор.

Ключевые слова: NetFlow, сенсор, коллектор, зеркалирование портов, трафик, promiscuous mode

Введение

Задача сбора и накопления статистики о проходящем трафике является одной из важнейших в комплексе мер по обеспечению всестороннего мониторинга и контроля сети любого масштаба.

Сбор информации о трафике осуществляется с помощью специальных библиотек. Средствами библиотечных функций реализуется взаимодействие с операционной системой и сетевым адаптером компьютера. Программные средства для сбора трафика опираются на функциональные возможности встраиваемых библиотек. Программа-демон, работая в фоновом режиме, «слушает» сетевой интерфейс и обрабатывает проходящие пакеты. Необходимые сведения извлекаются из заголовков пакетов (в том числе инкапсулированных в кадры более низкого уровня) и затем преобразуются (агрегируются). После этого агрегированная информация передается другому модулю программы для дальнейшей обработки.

Совершенно очевидно, что хранить и манипулировать настолько детализированной информацией о трафике крайне неудобно. За сутки через сетевой интерфейс могут проходить сотни тысяч пакетов. Данные об одном пакете могут насчитывать не один десяток значений в зависимости от того, насколько детально требуется анализировать заголовки вложенных (инкапсулированных) пакетов более высокого уровня. Самый простой способ как-то структурировать информацию – это суммировать данные по одному или нескольким критериям и хранить их в обработанном виде. Часто применяют группировку по значению адресов отправителя и получателя. Это решение позволяет упростить процесс формирования статистических отчетов о расходе трафика каждым узлом компьютерной сети за счет сужения области поиска. Более того, в целом, при таком подходе значительно уменьшается объем дискового пространства, занимаемый данными о трафике. Выбор критериев обусловлен конкретными задачами и ситуацией, ввиду которой возникает необходимость вести подсчет трафика.

Технология NetFlow

Комплексный подход к вопросу учета трафика предложила компания Cisco, разработав и реализовав в программном обеспечении для своих маршрутизаторов технологию, позволяющую гораздо более гибко работать с сетевым трафиком и распределять задачи по его обработке, сохраняя при этом высокую информативность полученных данных.

Подход к анализу сетевого трафика базируется на поиске общих характеристик у различных пакетов путем анализа значений полей их заголовков. Цель такого анализа – выявить в общем трафике отдельные уникальные потоки IP-пакетов. Поток состоит из некоторого числа пакетов со схожими характеристиками. Разумно, например, предположить, что логическое соединение между двумя компьютерами и передаваемый в его рамках трафик будет представлен в виде одного потока, пакеты которого будут иметь несколько общих значений служебных полей.

Для того чтобы сделать вывод о наличии потока, требуется установить сходство следующих полей IP-пакетов:

- IP-адрес источника;
- IP-адрес назначения;
- порт источника;
- порт назначения;
- тип протокола;
- тип сервиса (TOS);
- имя сетевого интерфейса, на который пришел пакет.

Таким образом, все пакеты, имеющие одинаковые значения вышеперечисленных полей, представляются в виде потока и начинают обрабатываться как части единого целого. В памяти обработчика хранятся постоянные значения полей для потока (см. список); помимо этого отдельно ведется подсчет числа пакетов и их размера для каждого отдельного потока.

При поступлении очередного пакета программа-сенсор, прослушивающая сетевой интерфейс, анализирует заголовки и пытается соотнести при-

шедший пакет с одним из имеющихся активных потоков. В случае когда принадлежность установить не удается, динамически создается запись о новом потоке на основании характеристик его первого пакета (см. рис. 1).

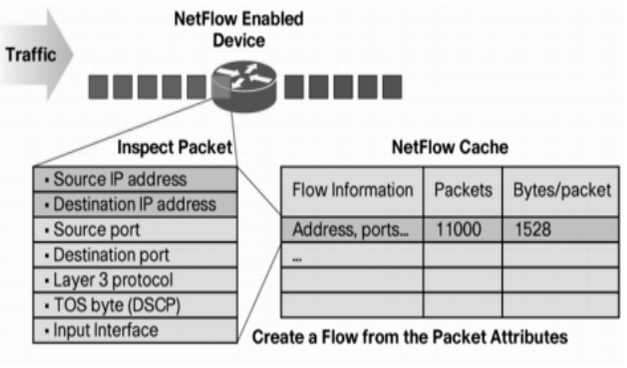


Рис. 1. Создание потока из атрибутов пакетов

Существует так называемый интервал ожидания, в течение которого должен прийти очередной пакет из того же потока. По истечении интервала ожидания поток считается неактивным, закрывается и сведения о нем удаляются из оперативной памяти. Информация о таких потоках передается программе-коллектору дейтаграммным способом (используется протокол UDP) на указанный IP-адрес и UDP порт. Коллектор захватывает дейтаграммы и сбрасывает полученные данные в файлы определенного формата, которые затем можно использовать в целях анализа трафика.

Архитектура NetFlow

NetFlow сетевой протокол, предназначенный для учета сетевого трафика, разработанный компанией Cisco Systems. Netflow имеет три основные компоненты, показанные на рис. 2:

- сенсор;
- коллектор;
- система обработки и предоставления данных.

Сенсор – это программа, которая слушает сеть и фиксирует данные сеанса. Так же как Snort или любая другая система обнаружения вторжений, сенсор должен иметь возможность подключиться к хабу, «зеркалированному» порту коммутатора или любому другому устройству для просмотра сетевого трафика.

Коллектор (collector) – это вторая программа, которая слушает UDP порт, указанный вами, и осуществляет сбор информации от сенсора. Полученные данные она сбрасывает в файл для дальнейшей обработки. Различные коллекторы сохраняют данные в различных форматах.

Наконец, система обработки читает эти файлы и генерирует отчеты в форме, более удобной для пользователя. Эта система должна быть совместима с форматом данных, предоставляемых коллектором.

Как было сказано, маршрутизаторы Cisco имеют в своем программном обеспечении средства, способные экспортировать NetFlow данные (netflow-сенсор), которые передаются на специальный узел, известный как netflow-коллектор. При необходимости получить сведения о трафике, используя технологию NetFlow, с оборудования, не поддерживающего экспорт NetFlow данных, нужно реализовать схему зеркалирования портов (трафика) с установкой и настройкой NetFlow-сенсора на персональном компьютере.

Мониторинг в неразборчивом («promiscuous») режиме

В компьютерных сетях режим promiscuous – это особый режим оборудования Ethernet, как правило, сетевых интерфейсных карт (NIC), который позволяет карте получать весь трафик сети, даже если этот трафик не адресован конкретно данной карте. По умолчанию NIC игнорирует весь не адресованный ему трафик путем сравнения адреса назначения Ethernet-пакета и аппаратного адреса принимающего устройства (MAC-адреса). Хотя такая схема работы вполне оправданна технически, не-promiscuous режим существенно затрудняет работу программ сетевого анализа и мониторинга, применяемых для диагностики сетевых проблем и учета трафика.

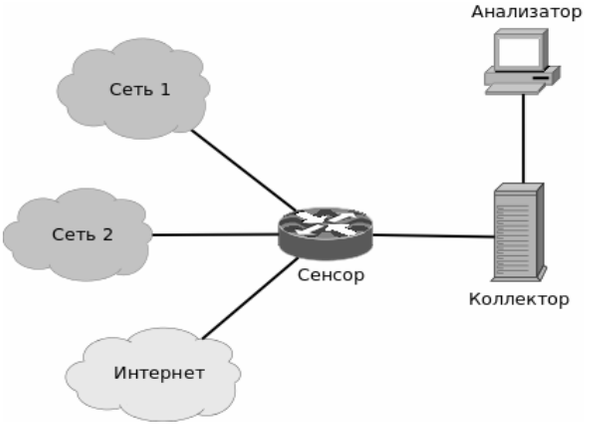


Рис.2. Архитектура NetFlow

Мониторинг с помощью коммутаторов

Управляемый (managed) коммутатор с поддержкой зеркалирования (mirroring) портов (функция, позволяющая перенаправлять трафик с од-

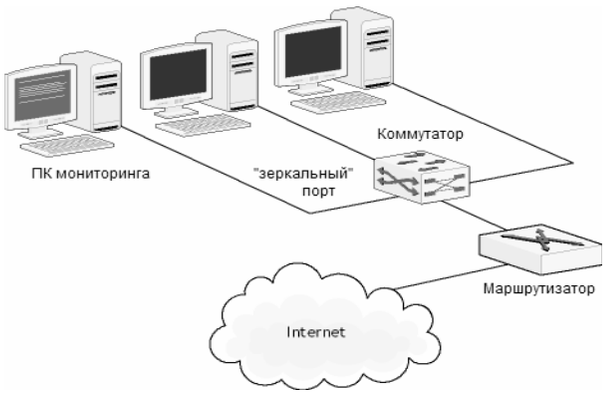


Рис. 3. Вариант 1: схема подключения с одним управляемым коммутатором

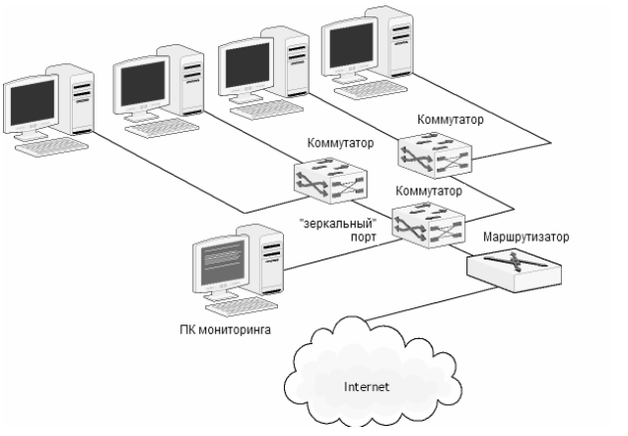


Рис.4. Вариант 2: схема подключения неуправляемых коммутаторов к управляемому коммутатору

них портов на определенный порт коммутатора) – идеальное устройство для сетевого мониторинга. Настройки зеркалирования портов зависят от модели и производителя.

Ниже показаны два типичных варианта с использованием зеркалирования портов (см. рис. 3 и рис. 4).

Во втором варианте главный коммутатор имеет функцию зеркалирования портов. ПК мониторинга подключен к «зеркальному» порту, на который переправляется весь трафик с локальных рабочих станций и маршрутизатора. Коммутатор можно настроить на перенаправление данных с одного или с нескольких портов.

Если в сегменте локальной сети используются неуправляемые (unmanaged) коммутаторы, не поддерживающие зеркалирование портов, то можно добавить управляемый коммутатор. Направляя Internet-трафик через коммутатор, поддерживающий зеркалирование портов, ПК мониторинга подключается к зеркальному порту и тем самым получает возможность перехватывать трафик между локальными рабочими станциями и маршрутизатором. При данном сетевом подключении не будет возможности наблюдать трафик между локальными рабочими станциями, поскольку он проходит через неуправляемые коммутаторы и, следовательно, не доходит до управляемого коммутатора.

В конкретном случае, на кафедре ПОУТС используется схема мониторинга сети, показанная на рис. 5. Между неуправляемыми коммутаторами подключен управляемый коммутатор, который перехватывает интернет-трафик и обращение рабочих станций кафедры к локальным ресурсам сети университета и зеркалирует его на персональный компьютер с настроенным NetFlow-сенсором, данные от которого передаются программам коллектору и анализатору.

В качестве netflow-сенсора был выбран fprobe (на Linux ПК), в качестве коллектора и анализатора – NetFlow Analizer (на отдельном виртуальном ПК).

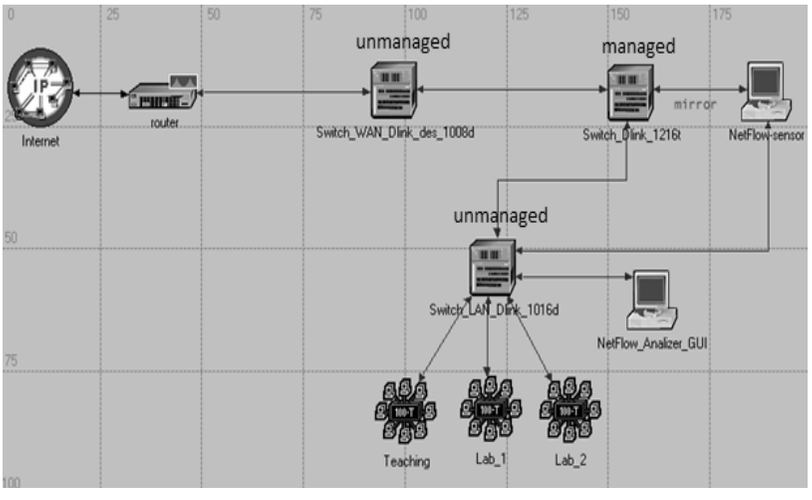


Рис. 5. Схема мониторинга сети кафедры ПОУТС

NetFlow-сенсор fprobe

Fprobe – это инструмент, основанный на библиотеке libpcap, при помощи которого можно собирать данные трафика и передавать их дальше коллектору. В число возможностей программы входит поддержка экспорта данных о трафике в формате NetFlow. Существует возможность экспорта потоков сразу нескольким программам-обработчикам (коллекторам). Синтаксис запуска программы выглядит следующим образом: fprobe [параметры] узел:порт…

Рассмотрим основные параметры запуска сенсора.

Ключ *-p* ставит запрет на использование promiscuous mode. Сетевой адаптер будет обрабатывать только те кадры, где в качестве узла назначения указан его физический адрес.

Ключ *-i <интерфейс>* определяет сетевой интерфейс, или перечень интерфейсов, которые будут прослушиваться сенсором. Параметр «any» указывает на то, что прослушиваться будут все сетевые интерфейсы в системе.

Ключ *-n <версия>* – версия NetFlow для использования (1, 5 или 7). [по умолчанию = 5].

Ключ *-f <выражение>* – фильтр, который выбирает, какие пакеты должны быть захвачены. Если не задано значение переменной, то будут захвачены все доступные пакеты. Для получения более детальной информации касаемо синтаксиса выражений следует читать документацию по *tcpdump*.

Узел:порт – параметры узел и порт определяют адрес и порт NetFlow коллектора. Можно указывать несколько коллекторов.

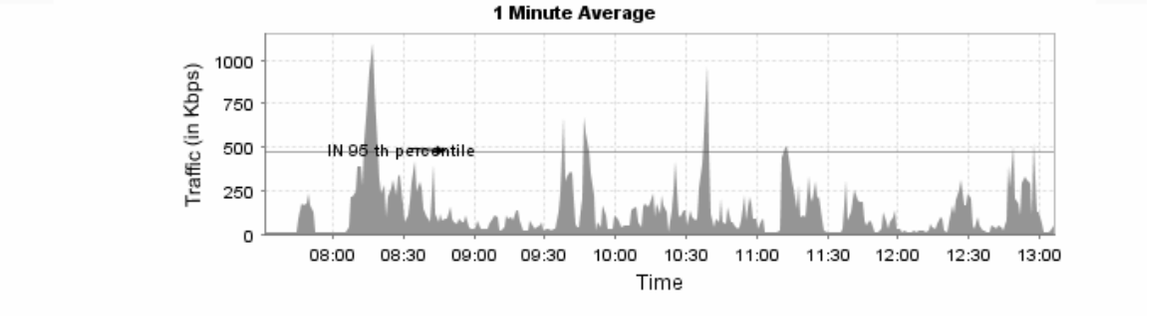
Результаты съема трафика сети кафедры

Так как входящий и исходящий трафик «зеркалируется» на один порт, то результирующая картина по трафику будет являться суммой входящего и исходящего трафика. Чтобы узнать, что приходится на входящий трафик, что на исходящий трафик, нужно открыть таблицы, содержащие IP-адреса источники и IP-адреса назначения для всего трафика в целом либо по конкретному приложению. В данной конкретной программе NetFlow Analizer можно выделять группы IP-адресов из общего потока, для которых статистика о трафике будет считаться отдельно. В этом случае трафик будет разделяться на входящий и исходящий.

Для получения всего входящего и исходящего трафика в отдельности следует подключать два управляемых коммутатора и настраивать зеркалирование портов на два сетевых интерфейса ПК-сенсора. С одного коммутатора зеркалируется входящий трафик, с другого исходящий трафик.

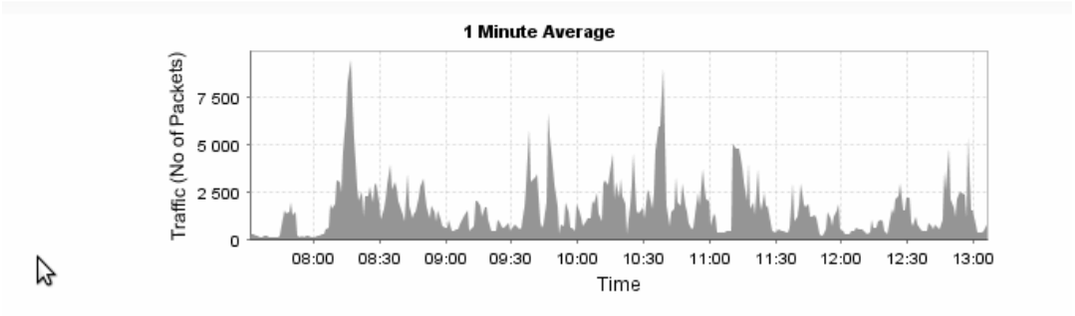
На рис. 6 представлен график интенсивности трафика в Кбит/С как целочисленного случайного процесса. Аналогичный график интенсивности трафика в пакетах в минуту представлен на рис. 7, где средняя длина пакета при максимальной интенсивности трафика составляет $(1{,}09 \cdot 1024 \cdot 1024)/(8 \cdot (9476/60)) \approx 904$ байта. В дальнейшем возникает задача исследования распределения интервалов времени между пакетами приведенного трафика, что является далеко не простой задачей.

На рис. 8 можно увидеть структуру трафика по протоколам. Из чего можно делать вывод о доле внутреннего и внешнего трафика. Около



Category	Total	Max	Min	Avg	Standard Deviation	95th Percentile
IN	341.02 MB	1.09 Mbps	4.58 Kbps	135.32 Kbps	164.37 Kbps	475.37 Kbps
OUT	0.00	0.00	0.00	0.00	0.00	-

Рис. 6. Отчет по интенсивности (Кбит/С)



Category	Total	Max	Min	Avg	Standard Deviation	95th Percentile
IN	540161.0	9476.0	45.0	1607,62	1499	-
OUT	0.0	0.0	0.0	0,00	0	-

Рис.7. Отчет по количеству пакетов в минуту

Application	Traffic(Total: 342.41 MB)	% of total traffic
proxy	128.03 MB	37%
TCP_App	83.98 MB	25%
http	65.05 MB	19%
dr.web	43.61 MB	13%
IP_App	11.68 MB	3%
genie	4.75 MB	1%
netbios-ssn	1.18 MB	<1%
UDP_App	650.87 KB	<1%

Рис.8. Отчет по используемым приложениям

70% трафика является внешним по отношению к сети кафедры, остальное – внутренний трафик.

Литература

1. http://www.cisco.com/en/US/tech/tk812/technolo gies_white_paper09186a008022bde8.shtml «Cisco IOS IPsec Accounting with Cisco IOS NetFlow»
2. http://ru.wikipedia.org/wiki/Netflow
3. http://www.tamos.ru/htmlhelp/monitoring/ Мониторинг локальных и беспроводных сетей – мМетодики, советы, топологии сетей.
4. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей. М.: ЛОРИ. – 350 с.

THE ORGANIZATION OF PICK-UP OF THE NETWORK TRAFFIC OF A SOFTWARE OF TECHNOLOGY NETFLOW WITHOUT MACHINE UTILIZATION CISCO

Gorelov G.A., Tarasov V.N.

In article the mechanism of pick-up of the traffic of a LAN of lower layer of a multisegment network of the HIGH SCHOOL, based on technology NetFlow, without Cisco machine utilization is considered. Various methods of connection of the equipment are described at traffic mirroring on a PC sensor control.

Keywords: *NetFlow, sensor control, collector, mirroring of ports, traffics, promiscuous mode.*

Горелов Глеб Александрович, аспирант Кафедры «Программное обеспечение и управление в технических системах» (ПОУТС) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. (8-846) 228-00-13, E-mail: gleb_fox@bk.ru

Тарасов Вениамин Николаевич, д.т.н, профессор, заведующий Кафедрой ПОУТС ПГУТИ. Тел. (8-846) 228-00-13, E-mail: vt@ist.psati.ru