

Анализ сетевого трафика с помощью NetFlow

Говорите умно. Враг подслушивает.
©Ежи Лец.

Разное.

Как трудно приходит понимание, что, сами не желая того, производители "считалок" оснастили полмира весьма совершенными коммуникаторами. Осталось только научиться их использовать.

Передача голоса (да уже и видео) по IP идет превосходно, разговор через Skype ([Sipnet](#), Yahoo, ICQ,...) как правило качественнее, чем по телефону. Вопросы масштабирования, продолжающие ограничивать корпоративный VoIP, в распределенных системах практически отсутствуют. Легкость настройки пользовательского софта немного пугает, а количество удобных "мелочей" вызывает легкий шок. Взять хотя бы мобильный, привязанный только к паролю номер-ник, видео, конференции, параллельную разговору пересылку текстов и файлов...

В сущности, скоро не удивит трансконтинентальная IP-пьянка "на троих". Забавно будет видеть, как последняя российская незыблемая и вечная ценность обретет новую жизнь в киберпространстве.

Но очень узок круг, страшно далеки такие способы коммуникации от народа. Даже при наличии технической возможности (что само по себе привилегия крупных городов) мешает психологический барьер неодолимой высоты.

Что говорить, если в весьма "продвинутом на телекоммуникациях" круге общения реальная эксплуатация "компьютера как телефона" только делает первые шаги. Страшная сил привычка заставляет тянуться к трубке.

Процесс освоения затрудняет и сложность шлюзования обычной телефонии в IP. В теории с компьютера можно позвонить на любой Российский телефон через полдюжины разных программ. Даже относительно не дорого - рублей от 3-6 в минуту. Но качество оставляет желать лучшего. Это если говорить мягко. А реально - при звонке на мобилку слова разобрать сложно. На обычный телефон - вспоминаются времена первых "карточных" провайдеров.

И будет только хуже. Отраслевое правительство ухватилось за контроль шлюзов как утопающий за соломинку, и не выпустит их пока не задушит совсем. Оно бы и сам Skype закрыло - да не может. Хорошо, что остальные аналогичные программы не так сильно известны, а то бы им то же "досталось" с министерского плеча. Но суть от этого не меняется - коммуникации типа компьютер-компьютер в России (а так же Китае и некоторых других странах) продолжают жить своей жизнью, мало пересекаясь с законодательством.

Ну не нравится правительству развивать Российский бизнес, надо вытеснить новые, высокотехнологичные его части из страны вместе с налогами и специалистами. Генералы готовятся к прошлой войне...

На первый взгляд, хорошего в этом мало. Но с другой стороны, не все ли равно... Последнее время начинает казаться, что пакетная передача голоса не сможет победить в образе обычного на вид телефона с "другим" кабелем. **Она придет как новый, недоступный прежде набор услуг**. То, что происходит в отрасли сейчас, похоже скорее на ходунки у быстро растущего ребенка. Вырастет, и отбросит надоевший девайс.

Локомотивами, по всей вероятности, станут мобильные телефоны с поддержкой Wi-Fi (по сути, те же компьютеры в маленьком корпусе), на которые наложится видео и дешевизна услуг (идиома "он-лайн" расширит свое значение). Не зря же Google и Skype что-то мутят с хот-спотами. Решение этого же вопроса через технологии ОПСОСов (3G и т.п.) на сегодня кажется менее вероятным, да и суть проблемы от этого не изменится.

Каких-нибудь 2-3 года, и окажется, что система цифровой нумерации и шлюзование в ТФОП не очень-то и нужны. Ну примерно как ICQ живет параллельно с e-mail или IRC. Набор инструментов будет под рукой, и пользователь сможет выбирать наиболее удобный, а то и разговаривать параллельно по несколькими "через удержание".

Под давлением экономики межгород будет смещаться на "межкомпьютерные" способы, туда же за дополнительными возможностями пойдет коммуникабельная продвинутая молодежь. При этом низкое качество стыков технологий заставит пользоваться для выхода в ТФОП обычный телефон (сотовый, в крайнем случае стационарный).

Период мирного сосуществования двух систем может быть довольно длительным. Примерно лет 5-7, пока миниатюризация не загонит полноценные компьютеры в гаджеты и мобилки. После этого

вопрос стыка и шлюзования отпадет сам собой. Собственно, средний пользователь даже не заметит, что его "трубка" превратилась в многопротокольный компьютер-коммуникатор.

Конечно, стационарные проводные телефоны какое-то время будут применяться, но тут уж о шлюзовании в "большой мир" придется думать в основном владельцам кабельной инфраструктуры времен развитого социализма.

Впрочем, Ethernet-провайдерам от этих процессов ни холодно, и ни жарко. Оптика до дома все равно будет более чем востребована (даже Verizon последнее время не жалеет сил и средств на развертывание оптоволокон). И для высокоскоростного включения абонентов компьютерные голосовые программы только лишний повод.

А так как заработать на карточной IP-телефонии правительство не дает, - так пусть на международном/междугороднем трафике не заработает и Связьинвест...

Фотография "в тему". Импровизированный переговорный пункт собран на куске деревянного ящика от телевизора "Рекорд".



Прислал **Anton** (Казань).

Ссылки:

[Разъяснения Правил оказания услуг связи](#). В связи с тем, что "Правила оказания услуг связи по передаче данных" подписанные Правительством России 23 января 2006 г. в широких массах были истолкованы неверно, 1 февраля 2006 г. Мининформсвязи выступило с разъяснением сферы регулирования этого документа...

В общем, "хороший" получился документ, смешной и забавный. Жаль, цирк подчиняется другому ведомству.

Телеграф умер. На прошлой неделе Western Union отправил последнюю телеграмму. Технология передачи сообщений, просуществовавшая больше 150 лет, теперь навсегда ушла в прошлое. В прошлом году Western Union было передано всего 20 тыс. телеграмм (по 55 в день), а в эпоху расцвета передавалось по 550 тыс. сообщений ежедневно.

Кстати, в Екатеринбурге осталось только одно место, где принимают телеграммы...

[Конвертер потока sflow в netflow](#). Причем бесплатный и в сорцах.

[Полтора года за FTP](#). Приговор не бесспорный, но, к сожалению, вполне реальный.

И еще один документ из под пера чиновников: Мининформсвязи утвердило требования к защите от несанкционированного доступа к программам цифрового спутникового телевидения стандарта DVB

Админ - опасная профессия, или история как директор оператора связи избил своего клиента. Такого

еще видеть в сети не приходилось.

Морозы не прошли бесследно:



Прислал **Виталий**

Маршрутизатор на одном из чердаков. Температура -25°C.



- [Фото 1](#)
- [Фото 2](#)
- [Фото 3](#)

Прислал **Zalex**, г. Мариуполь

Цены Немецкой Научной Сети на интернет (X-WIN):

Сама сеть, это 43 города соединённые через (как это у них сказано) мульти-гигабит, к ним подключены все университеты Германии и почти все другие научные учреждения (линии от 2 Mbit до 10 Gbit). Почти все школы включены через DSL/ISDN.

Трафик теперь никому не считают. На счёт линии не совсем понятно, написано только что заказывать её надо самому у кого хочешь. Подключиться может каждый, кто хоть как-то связан с наукой.

А вот цены на Cluster, т.е. когда несколько клиентов используют одну линию/одно подключение

(цена каждому конечно).

Я подключён к ним вот так: местный телефонист даёт DSL линию (у меня 4300/725 Kb) до моего университета, а тот подключён к сети (X-WIN) через 1 Gigabit. Стоит 35 евро в месяц (DSL 4000 и 2 ISDN-канала для телефона).

Andreas Werschbowski

Обновление в разделах

- Дополнены в [Фотографии сетевого оборудования](#) - [3Com 4900](#).
- В оглавлении выложен архив обзоров за 2005 год. Так как общий объем - около 400 Мб, он разделен на четыре части "поквартильно".
- В разделе [shop.nag.ru](#) можно просто посмотреть **новые поступления**. Обновлено примерно 1/4 ассортимента, цены заметно снижены на едва ли не на половину позиций...

Анализ сетевого трафика с помощью NetFlow.

Автор [Эдуард Афонцев](#)

4.2. Flow-tools

Наиболее развитые средства анализа NetFlow данных обеспечивают соответствующие утилиты из комплекта flow-tools. Рассмотрим их подробнее.

Просмотр данных обеспечивает flow-print (дополнительно можно форматировать вывод опцией -f):

UNIX # cat /netflow/* | flow-print | less

srcIP	dstIP	prot	srcPort	dstPort	octets	packets
212.162.137.27	195.209.163.99	6	1646	25	598	12
192.93.0.4	195.12.66.65	17	53	2666	133	1
194.187.251.2	195.209.191.1	17	64217	53	60	1
81.84.242.5	195.12.66.65	17	53	2666	128	1
72.36.190.2	195.12.66.1	17	58155	53	74	1

Более гибкой является комбинация flow-print и flow-cat.

Просмотр информации до указанного времени:

UNIX # flow-cat -t "15:00" /netflow/2005/2005-02/2005-02-18/ | flow-print | less

UNIX # flow-cat -t "2005-02-18 15:00" /netflow/2005/2005-02/2005-02-18/ | flow-print | less

srcIP	dstIP	prot	srcPort	dstPort	octets	packets
212.220.196.244	195.12.65.194	1	0	0	140	5
82.209.198.42	195.12.85.114	17	500	500	112	1
217.24.189.58	195.12.65.194	1	0	0	140	5
80.78.96.1	195.12.66.1	17	53	53	202	3
212.220.235.6	195.12.65.194	1	0	0	140	5
85.37.61.43	195.12.66.65	17	53799	53	59	1

Просмотр информации после указанного времени:

UNIX # flow-cat -T "15:00" /netflow/2005/2005-02/2005-02-18/ | flow-print | less

UNIX # flow-cat -T "2005-02-18 15:00" /netflow/2005/2005-02/2005-02-18/ | flow-print | less

srcIP	dstIP	prot	srcPort	dstPort	octets	packets
205.188.189.196	195.12.66.97	1	0	2048	84	1

203.130.159.21	195.12.87.50	17	24449	53	52	1
18.7.14.168	195.209.163.98	17	32788	33435	320	10
65.4.73.172	195.12.81.116	1	0	771	112	1
194.190.200.132	195.12.69.18	6	4588	25	60	1
205.188.1.144	195.12.71.6	6	5190	1280	40	1

Анализ данных некоторого временного интервала:

UNIX # flow-cat -t "14:00" -T "15:00" /netflow/2005/2005-02/2005-02-18/ | flow-print | less
UNIX # flow-cat -t "03/23/05 9:00" -T "03/23/05 8:00" /netflow

srcIP	dstIP	prot	srcPort	dstPort	octets	packets
81.91.43.214	195.12.69.203	6	1156	44313	593	5
81.91.43.214	195.12.69.203	6	1157	44313	648	5
194.67.45.10	195.12.67.61	6	80	3517	1106	4
86.200.58.92	195.12.87.50	6	2533	25	80	2
217.16.19.237	195.12.67.61	6	80	1463	460	4
81.19.66.19	195.12.67.61	6	80	2428	1121	5

Некоторую статистику можно получить, используя flow-stat. Утилита позволяет форматировать данные по IP адресам (-f FORMAT) и сортировать (-s, -S).

Пример построения суммарного отчета:

UNIX # cat /netflow/2005/2005-02/2005-02-18/ft-v05.2005-02-18.124221+0500 | flow-stat -f 0 | less

--- ---- ---- Report Information --- --- ---

#

Fields: Total

Symbols: Disabled

Sorting: None

Name: Overall Summary

#

Args: flow-stat -f 0

#

Total Flows : 24371

Total Octets : 55501363

Total Packets : 184670

Total Time (1/1000 secs) (flows): 55133888

Duration of data (realtime) : 303

Duration of data (1/1000 secs) : 1619965508

Average flow time (1/1000 secs) : 2262.0000

Average packet size (octets) : 300.0000

Average flow size (octets) : 2277.0000

Average packets per flow : 7.0000

Average flows / second (flow) : 0.0150

Average flows / second (real) : 80.4323

Average Kbits / second (flow) : 0.2741

Average Kbits / second (real) : 1465.3825

IP packet size distribution: 1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480

.004 .338 .269 .088 .064 .030 .028 .014 .009 .006 .005 .009 .016 .025 .001

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608

.049 .002 .002 .020 .020 .000 .000 .000 .000 .000 .000

Packets per flow distribution: 1 2 4 8 12 16 20 24 28 32 36 40 44 48 52

.423 .078 .087 .157 .187 .019 .011 .008 .008 .005 .002 .003 .003 .001 .001

60 100 200 300 400 500 600 700 800 900 >900

.001 .003 .001 .000 .000 .000 .000 .000 .000 .000 .001

Octets per flow distribution: 32 64 128 256 512 1280 2048 2816 3584 4352 5120 5888 6656 7424 8192

.002 .205 .115 .095 .193 .298 .032 .010 .007 .003 .004 .003 .003 .002 .001

8960 9728 10496 11264 12032 12800 13568 14336 15104 15872 >15872
.001 .003 .001 .001 .001 .001 .001 .000 .001 .001 .017

Flow time distribution: 10 50 100 200 500 1000 2000 3000 4000 5000 6000 7000 8000 9000 10000
.449 .019 .051 .058 .070 .067 .145 .031 .030 .009 .008 .005 .004 .012 .008

12000 14000 16000 18000 20000 22000 24000 26000 28000 30000 >30000
.007 .004 .005 .003 .002 .003 .001 .001 .001 .001 .008

Выявление активных генераторов трафика:

UNIX # cat /netflow/2005/2005-02/2005-02-18/ft-v05.2005-02-18.124221+0500 | flow-stat -f 9 -S 2 | less

--- ---- ---- Report Information --- --- ---

Fields: Total
Symbols: Disabled
Sorting: Descending Field 2
Name: Source IP

Args: flow-stat -f 9 -S 2

#

IPAddr	flows	octets	packets
193.108.94.9	1	11899545	7937
195.134.59.84	3705	4239728	44506
83.219.9.30	35	2735485	2133
81.176.67.67	210	2468914	2283
213.180.204.9	280	2038394	2291
84.254.220.174	6	1603649	1567
195.58.6.10	7	1292947	8757
195.58.1.117	1	1019593	7648
195.161.200.130	43	907820	807

Выявление активных потоков:

UNIX # cat /netflow/2005/2005-02/2005-02-18/ft-v05.2005-02-18.124221+0500 | flow-stat -f 10 -S 3 | less

--- ---- ---- Report Information --- --- ---

Fields: Total
Symbols: Disabled
Sorting: Descending Field 3
Name: Source/Destination IP

Args: flow-stat -f 10 -S 3

#

src IPAddr	dst IPAddr	flows	octets	packets
193.108.94.9	195.12.81.39	1	11899545	7937
83.219.9.30	195.12.67.37	35	2735485	2133
81.176.67.67	195.12.82.242	202	2384076	2190
213.180.204.9	195.12.76.103	280	2038394	2291
84.254.220.174	195.12.67.55	6	1603649	1567
195.58.6.10	195.12.85.45	7	1292947	8757
195.58.1.117	195.12.71.171	1	1019593	7648

195.161.200.130	195.12.85.137	27	898215	749
194.67.27.125	195.12.82.146	12	625005	455
81.176.69.122	195.12.72.82	16	622661	460

Для гибкой фильтрации можно использовать утилиты flow-filter и flow-nfilter. Последняя является более продвинутой и обеспечивает расширенные возможности.

Для использования flow-nfilter необходимо создать конфигурационный файл с описанием фильтров - **filter.acl**:

```
filter-primitive client-ip
type ip-address
permit 195.12.69.199
default deny
```

```
filter-primitive www
type ip-port
permit 80
default deny
```

```
filter-definition all-from-client
match ip-source-address client-ip
```

```
filter-definition all-to-client
match ip-destination-address client-ip
```

```
filter-definition www-to-client
match ip-destination-address client-ip
match ip-source-port www
```

Далее можно использовать фильтрацию. Например, для анализа всего трафика к клиенту:

```
UNIX # flow-cat -t "9:00" -T "12:00" /netflow/2006/2006-01/2006-01-06/ | flow-nfilter -f filter.acl
-F all-to-client | flow-print | less
```

srcIP	dstIP	prot	srcPort	dstPort	octets	packets
221.208.208.2	195.12.69.199	17	41593	1026	485	1
195.95.85.206	195.12.69.199	6	4666	139	96	2
202.96.87.35	195.12.69.199	17	58686	1026	501	1
216.40.238.207	195.12.69.199	6	57924	22	60	1
212.118.50.140	195.12.69.199	1	0	2048	28	1
212.118.50.140	195.12.69.199	6	52274	80	40	1

Или для анализа только www трафика клиента.

```
UNIX # flow-cat -t "9:00" -T "12:00" /netflow/2006/2006-01/2006-01-06/ | flow-nfilter -f filter.acl
-F www-to-client | flow-print | less
```

srcIP	dstIP	prot	srcPort	dstPort	octets	packets
207.126.111.225	195.12.69.199	6	80	1043	811	5
212.58.226.19	195.12.69.199	6	80	1044	17106	16
207.126.111.225	195.12.69.199	6	80	1047	811	5
207.126.111.225	195.12.69.199	6	80	1046	811	5
212.58.226.19	195.12.69.199	6	80	1048	17106	16
212.58.226.19	195.12.69.199	6	80	1049	17106	16
212.58.226.19	195.12.69.199	6	80	1044	40	1

Для выявления фактов сканирования или заражения рекомендуется использование утилиты flow-dscan.

Приведем простейший пример детектирования источников сканирования по 135 порту:

UNIX # touch dscan.suppress.src

UNIX # touch dscan.suppress.dst

UNIX # flow-cat -t "9:00" -T "12:00" /netflow/2006/2006-01/2006-01-06/ | flow-filter -P 135 | flow-dscan -b | less

flow-dscan: load_suppress 0

flow-dscan: load_suppress 1

flow-dscan: host scan: ip=219.161.100.213 ts=1136524997 start=0106.10:23:17.726

flow-dscan: host scan: ip=213.168.117.86 ts=1136529053 start=0106.11:30:53.162

В заключении приведем примеры детектирования сетевых аномалий с помощью flow-tools.

Выявление активных генераторов пакетов на 135 порт:

UNIX # flow-cat -t "9:00" -T "12:00" /netflow/2006/2006-01/2006-01-06/ | flow-filter -P 135 | flow-stat -f 9 -S 2 | less

--- ---- ---- Report Information --- --- ---

#

Fields: Total

Symbols: Disabled

Sorting: Descending Field 2

Name: Source IP

#

Args: flow-stat -f 9 -S 2

#

#

IPAddr	flows	octets	packets
219.161.100.213	1619	94080	1960
213.168.117.86	237	24544	472
195.115.9.24	166	16512	344
195.241.159.181	142	12672	264
195.162.171.15	102	9120	190
195.207.152.209	91	8832	184
195.87.209.64	79	6672	139
195.46.177.188	76	6624	138
195.128.136.113	63	6000	125
212.220.57.192	12	5712	72

Выявление сканирования 445 порта (или вирусной активности):

UNIX # flow-cat -t "9:00" -T "12:00" /netflow/2006/2006-01/2006-01-06/ | flow-filter -P 445 | flow-dscan -b -S 2000

flow-dscan: load_suppress 0

flow-dscan: load_suppress 1

flow-dscan: host scan: ip=195.146.34.156 ts=1136520666 start=0106.09:11:06.250

flow-dscan: host scan: ip=217.36.205.230 ts=1136520870 start=0106.09:14:30.387

flow-dscan: host scan: ip=58.93.7.15 ts=1136522170 start=0106.09:36:10.113

flow-dscan: host scan: ip=64.108.214.217 ts=1136522220 start=0106.09:37:00.770

flow-dscan: host scan: ip=209.136.9.176 ts=1136523394 start=0106.09:56:34.950

flow-dscan: host scan: ip=60.20.220.247 ts=1136525268 start=0106.10:27:48.357

flow-dscan: host scan: ip=195.52.201.172 ts=1136527136 start=0106.10:58:56.120

flow-dscan: host scan: ip=71.241.68.118 ts=1136527305 start=0106.11:01:45.140

flow-dscan: host scan: ip=195.161.147.148 ts=1136527980 start=0106.11:13:00.352

4.3. Flowscan.

Среди множества утилит, работающих с NetFlow, невозможно не отметить flowscan [3]. С ее помощью можно получать подробную визуализацию потоков с распределением по протоколам, что облегчает задачу мониторинга и выявления нестандартных ситуаций.

Анонс

- Вслед за США диапазон 71-76/81-86 ГГц принят для коммерческого использования в Европе. Россия на очереди?
- Магистральная дедовщина;
- Письма про ADSL (анлимит в US);
- Абонентский вынос в Новосибирске, серверная в РГРТА, кабель на лестничной площадке, и другие зарисовки узлов разных провайдеров. Вечная тема (много фотографий гарантировано);
- Традиционный пункт - ссылки на интересные места Сети. Присылайте письма - они очень нужны для обзоров. Обязательно сообщайте, нужна ли Ваша подпись, ссылка, или лучше обойтись без нее;
- В "ужастиках" - кабельная прокладка в Евпатории.

Долгострой:

- Послегрозовой ремонт управляемых коммутаторов (надеюсь дойдут руки);
- Не все Vlan'ы одинаково полезны;
- Публичный проект сети в небольшом городе (именно они выходят на первый, авангардный план интернатизации России, в мегаполисах "уже все давно ясно"). Т.е. еженедельные отчеты о строительстве и работе "с нуля".