Санкт-Петербургский национальный исследовательский университет

Информационных технологий механики и оптики

Факультет информационных технологий и программирования

Лабораторная работа №2

По предмету Администрирование в информационных системах

«Работа с адресами IP сетей и мониторинг сетевого трафика»

Исполнитель: Трофимов В.А.

Руководитель: Береснев А.Д.

Группа: 3511

Санкт-Петербург

2014

# Цель работы

* Получить практические навыки по работе с пространством IP-адресов, масками и управления адресацией в IP сетях;
* Получить практические навыки по работе с анализаторами сетевого трафика.
* На практике ознакомиться с различиями в принципах работы активного сетевого оборудования.
* Уяснить особенности взаимодействия сетевого и канального уровней на примере стека TCP/IP.
* Выяснить отличия форматов кадров Ethernet.
* Познакомиться с консольными утилитами диагностики и анализа сетевых соединений.

# Расчет сетей



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Вар. | IP-адрес из сети маска | Количество компьютеров в сети | | | | |
| Сеть 1 | Сеть 2 | Сеть 3 | Сеть 4 | Сеть 5 |
| 1 | 194.85.32.19 255.255.255.0 | 10 | 6 | 1 | 18 | 100 |
| 2 | 10.12.12.15  255.255.254.0 | 25 | 16 | 240 | 117 | 1 |
| 3 | 212.24.15.199  255.255.255.192 | 7 | 0 | 0 | 11 | 10 |
| 4 | 120.13.120.120  255.255.255.224 | 5 | 2 | 2 | 1 | 1 |

## Вариант 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 | Сеть 4 | Сеть 5 |
| IP-адрес сети, маска | 194.85.32.64/28 | 194.85.32.80/28 | 194.85.32.8 /29 | 194.85.32.32/27 | 194.85.32.128/25 |
| Количество IP-адресов в сети | 16 | 16 | 8 | 32 | 128 |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров | 194.85.32.65  194.85.32.78 | 194.85.32.81  194.85.32.94 | 194.85.32.9  194.85.32.14 | 194.85.32.33  194.85.32.62 | 194.85.32.129  194.85.32.254 |

## Вариант 2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 | Сеть 4 | Сеть 5 |
| IP-адрес сети, маска | 10.12.12.32 /27 | 10.12.12.64 /27 | 10.12.13.0 /24 | 10.12.12.128/25 | 10.12.12.4/30 |
| Количество IP-адресов в сети | 32 | 32 | 256 | 128 | 4 |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров | 10.12.12.33  10.12.12.62 | 10.12.12.65  10.12.12.94 | 10.12.13.1  10.12.13.254 | 10.12.12.129  10.12.12.254 | 10.12.12.5  10.12.12.6 |

## Вариант 3

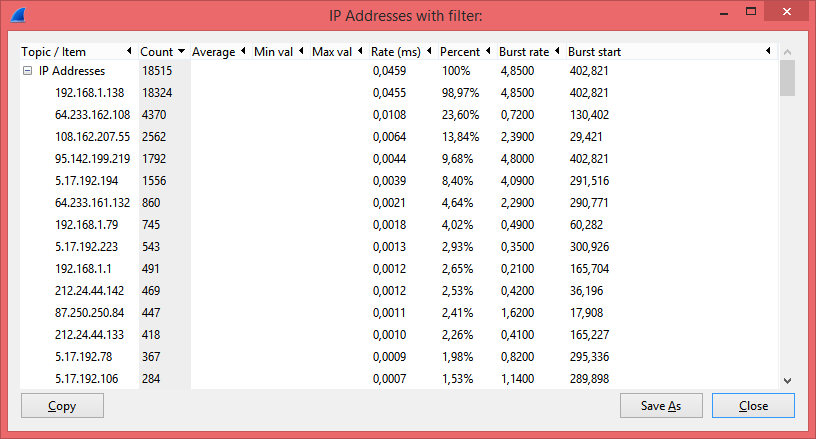
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 | Сеть 4 | Сеть 5 |
| IP-адрес сети, маска | 212.24.15.240/28 | 212.24.15.200/30 | 212.24.15.196/30 | 212.24.15.224/28 | 212.24.15.208/28 |
| Количество IP-адресов в сети | 16 | 4 | 4 | 16 | 16 |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров | 212.24.15.241  212.24.15.254 | 212.24.15.201  212.24.15.202 | 212.24.15.197  212.24.15.198 | 212.24.15.225  212.24.15.238 | 212.24.15.209  212.24.15.222 |

## Вариант 4

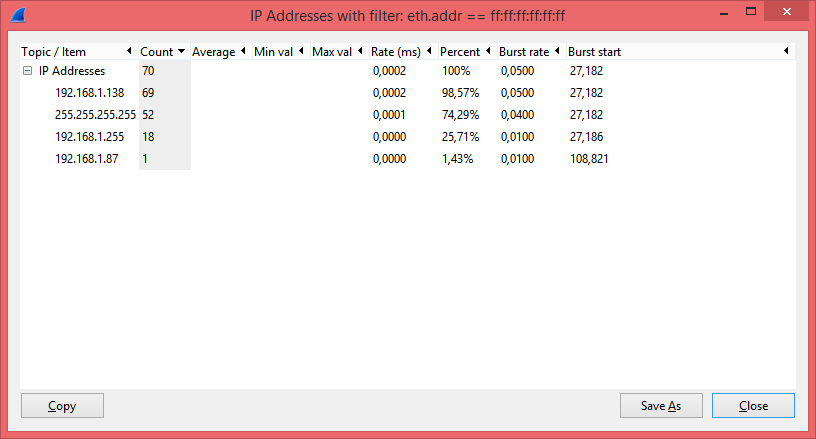
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Сеть | Сеть 1 | Сеть 2 | Сеть 3 | Сеть 4 | Сеть 5 |
| IP-адрес сети, маска | 120.13.120.104/29 | 120.13.120.112/29 | 120.13.120.120/29 | 120.13.120.96/30 | 120.13.120.100/30 |
| Количество IP-адресов в сети | 8 | 8 | 8 | 4 | 4 |
| Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров | 120.13.120.105  120.13.120.110 | 120.13.120.113  120.13.120.118 | 120.13.120.121  120.13.120.126 | 120.13.120.97  120.13.120.98 | 120.13.120.101  120.13.120.102 |

# Мониторинг сетевого трафика

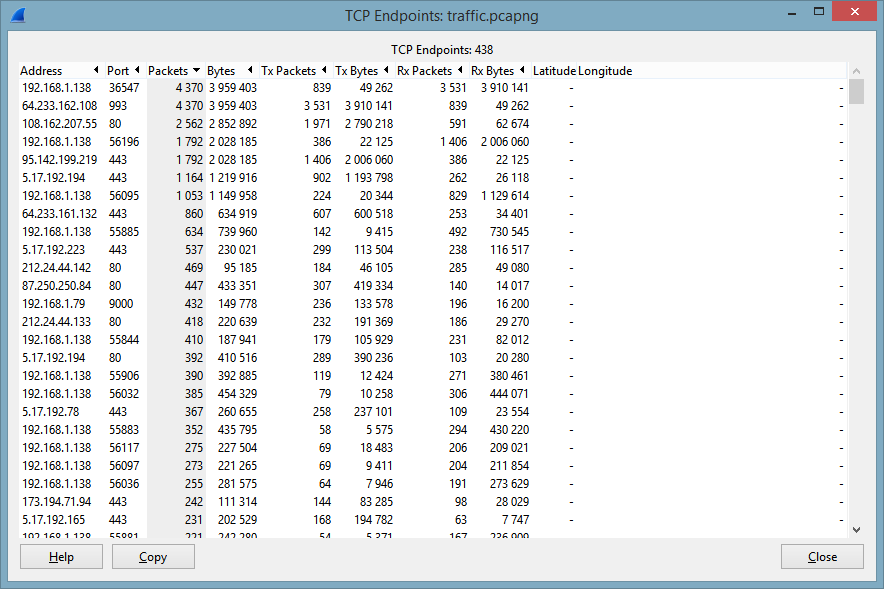
## Узел с максимальной активностью (по объему переданных данных)



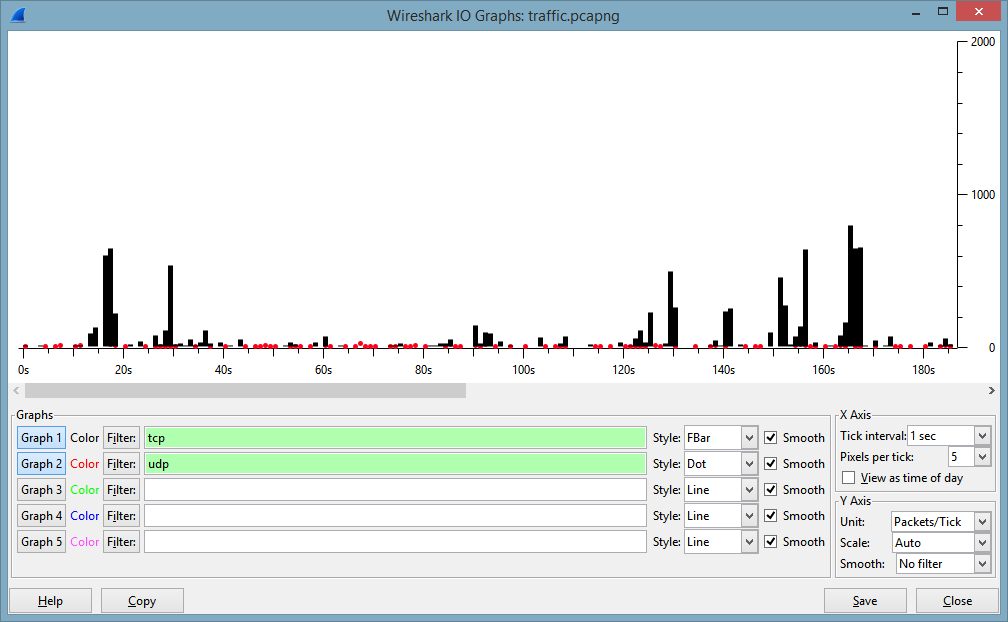
## Узел, осуществивший наибольшее количество широковещательных рассылок



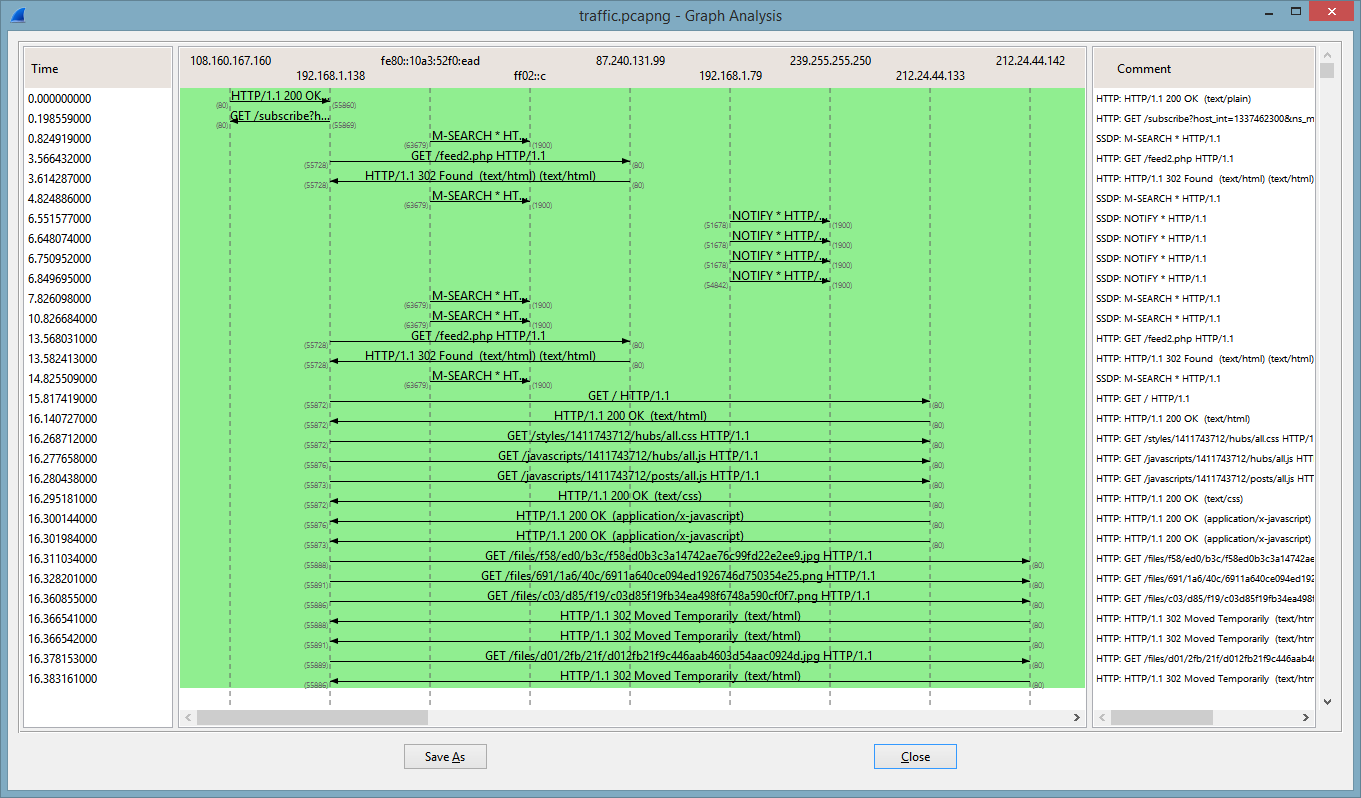
## Самый активный TCP-порт на хосте (по количеству переданных пакетов)



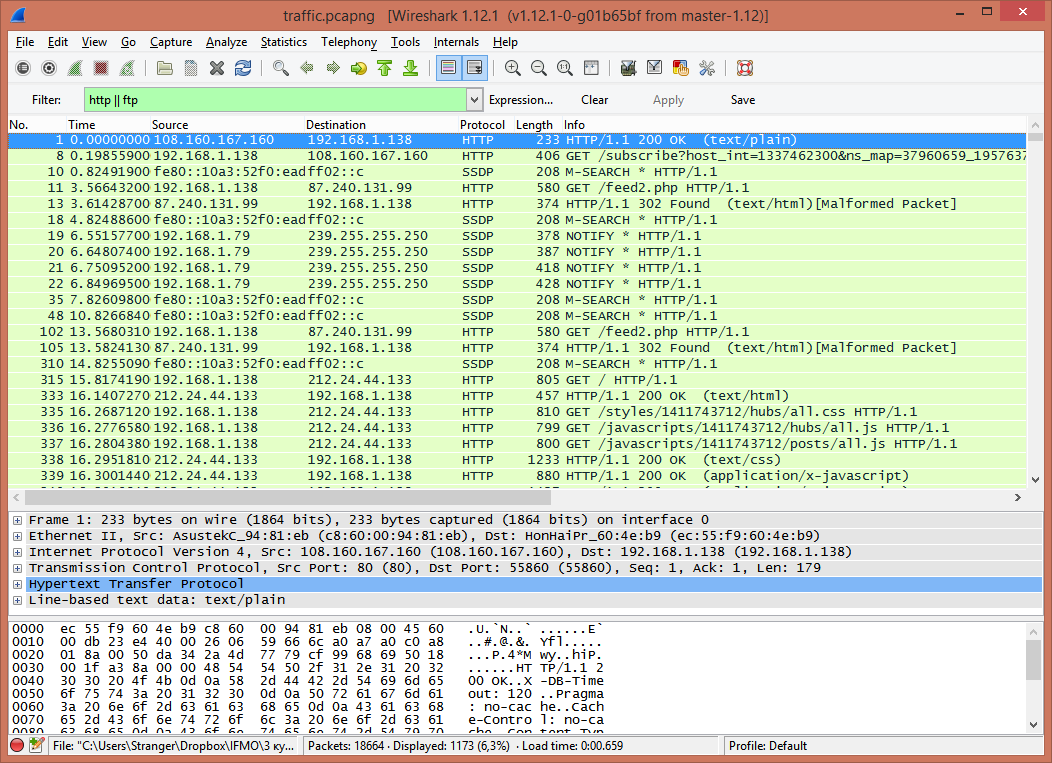
## Графики интенсивности TCP и UDP трафика



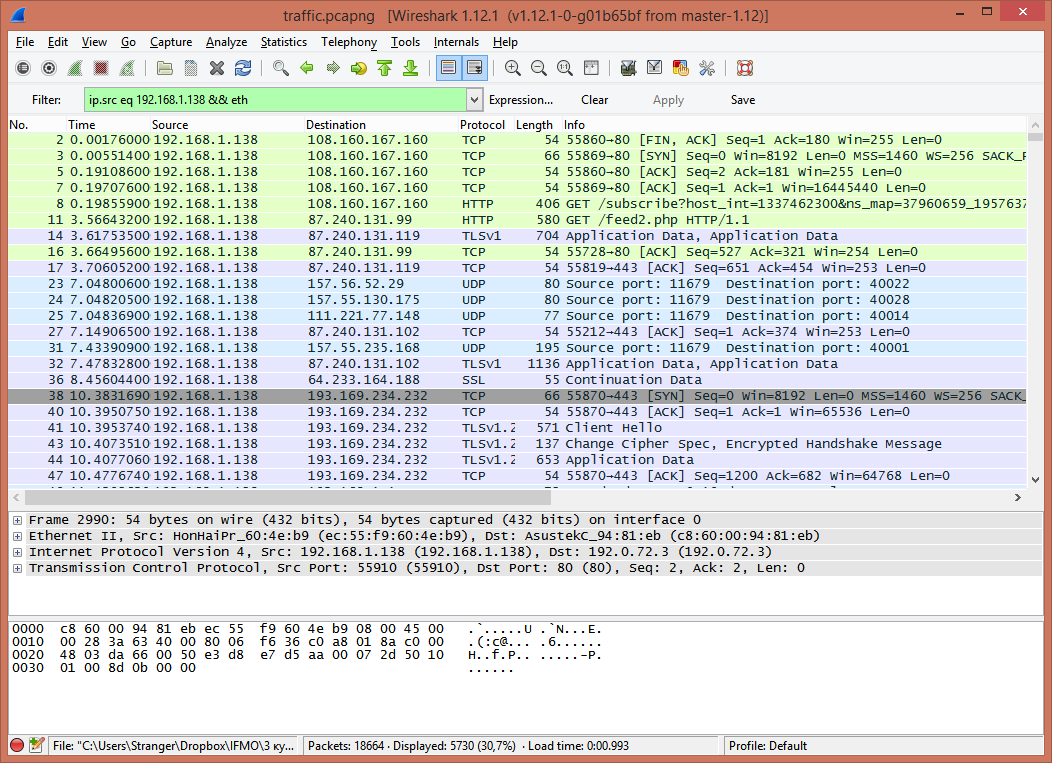
## Граф связей только для пакетов, содержащих сообщения протокола HTTP



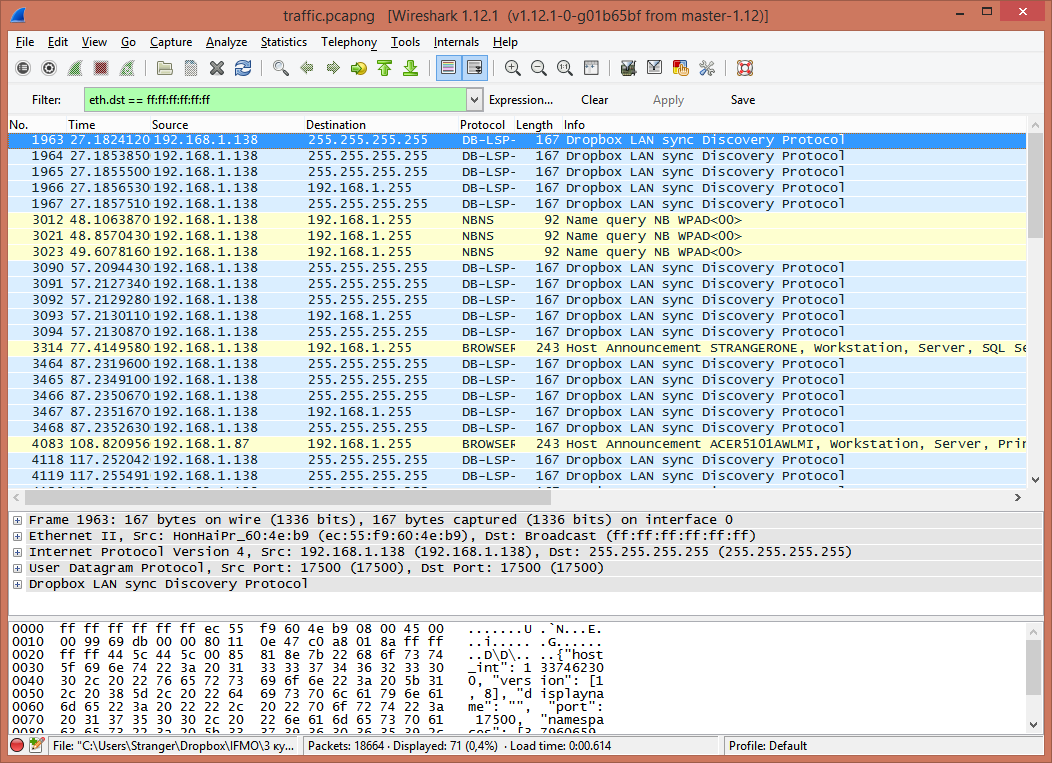
## Относящиеся к работе протоколов HTTP и FTP



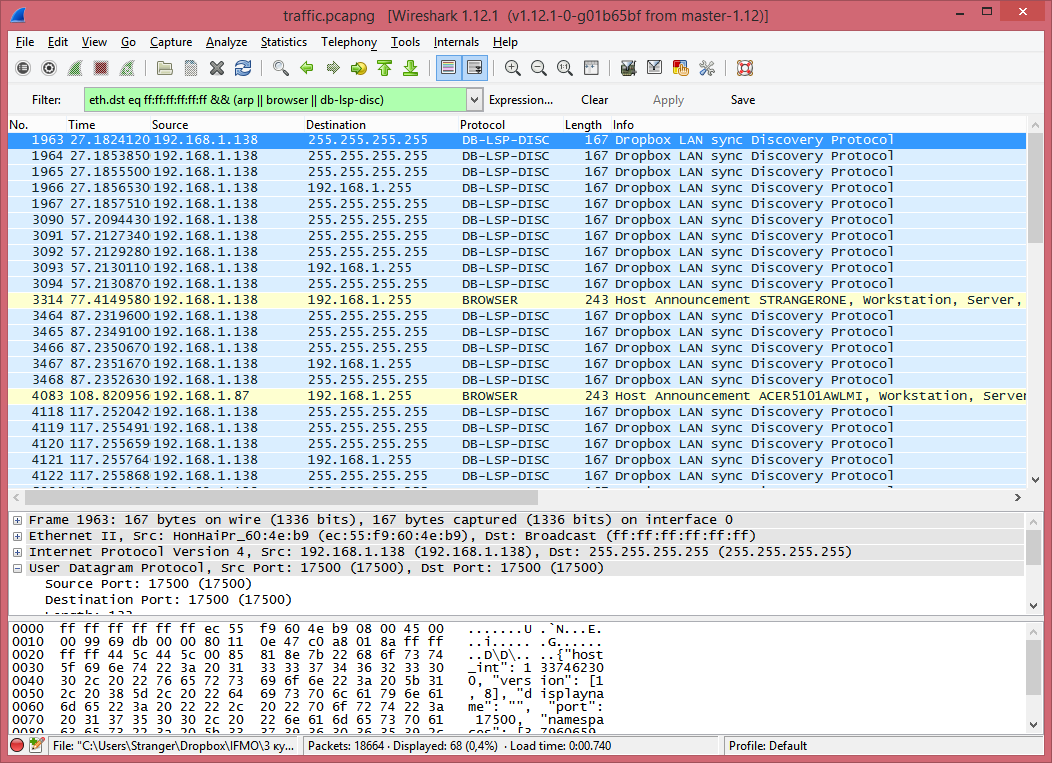
## Все кадры Ethernet, отправленные с сетевого интерфейса хоста



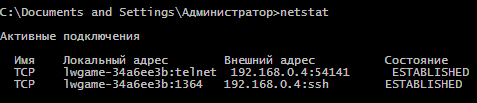
## Только широковещательные сообщения. Определите назначение как минимум 3-х широковещательных рассылок разных протоколов



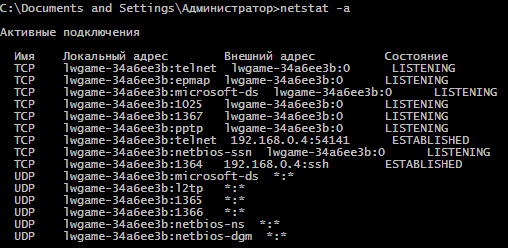
## Фильтры для каждой из выбранных трех широковещательных рассылок



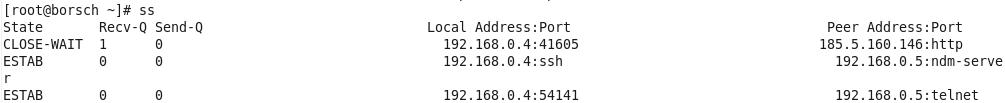
## Список соединений на Windows хосте



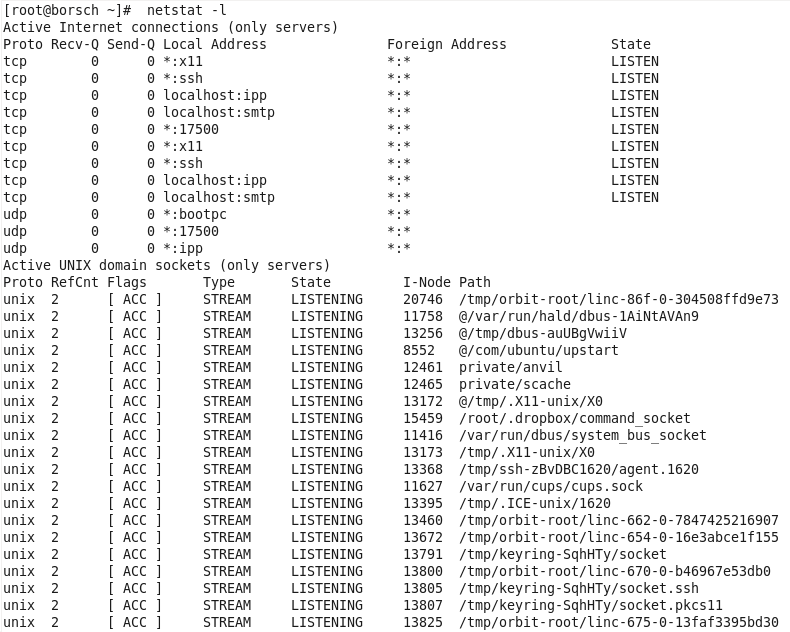
## Список активных портов на Windows хосте



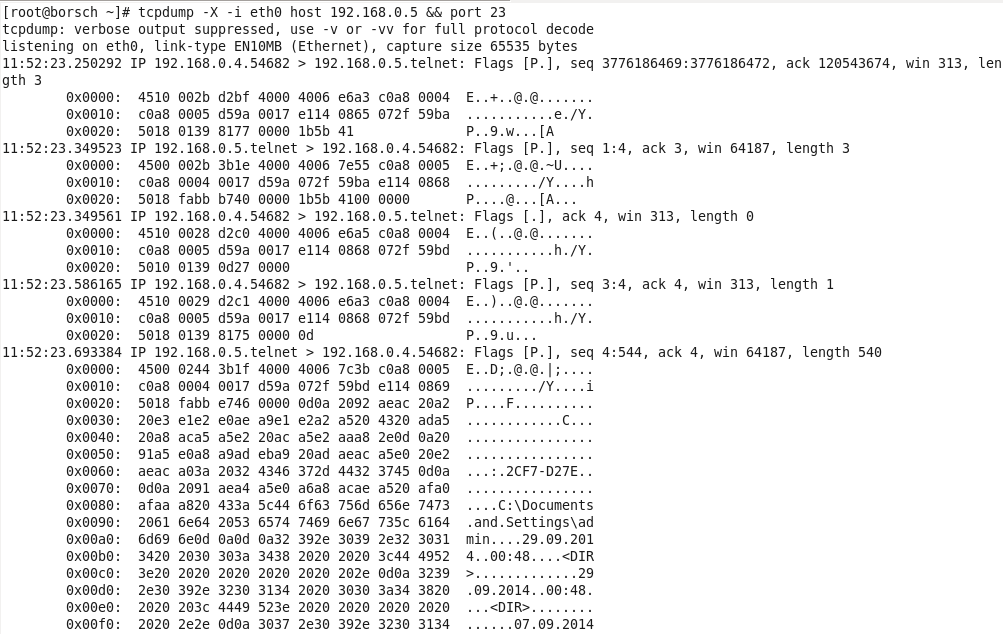
## Список соединений на Linux хосте



## Список активных портов на Linux хосте

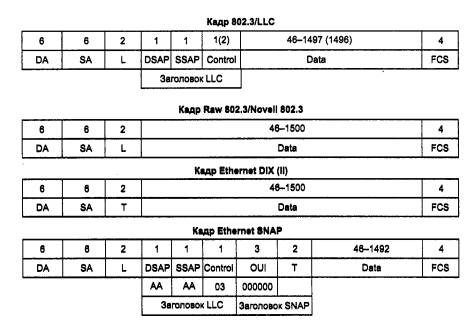


## Вывод на экран содержимого пакетов от Windows-хоста по протоколу telnet



# Ответы на вопросы

## Какие типы кадров Ethernet бывают, в чем их отличия?



## Какой тип кадров Ethernet используется в анализируемой сети? Почему именно он?

В анализируемой сети используются кадры Ethernet II, данный формат кадров является самым распространенным.

## Как можно определить тип используемого коммутационного оборудования, используя сетевую статистику? Какой тип коммутационного оборудования использовался в сети?

Используя описание источников и адреса назначения, а так же используемые при передаче протоколы. Роутер переупаковывает пакеты в кадры, к которых в качестве MAC-адреса источника указывается адрес интерфейса шлюза. Коммутатор же не изменяет кадры, а просто пересылает их требуемому адресату. Хаб пересылает кадры всем устройствам сети.

## На какие адреса сетевого уровня осуществляются широковещательные рассылки?

Используются широковещательные адреса, вид которых зависит от протокола. Так, в IP-сетях широковещательные адреса формируются следующим образом: к адресу подсети прибавляется побитовая инверсия маски подсети (то есть все биты адреса подсети, соответствующие нулям в маске, устанавливаются в «1»). Например, если адрес сети равен 192.168.0.0, маска подсети 255.255.255.0, то широковещательный адрес будет 192.168.0.255.

## На какой канальный адрес осуществляются широковещательные рассылки?

Используется широковещательный MAC-адрес FF:FF:FF:FF:FF:FF для передачи служебных дейтаграмм (например, ARP-запросов). Дейтаграммы, отправленные на такой адрес, принимаются всеми сетевыми устройствами локальной сети.

## Для чего применяются перехваченные широковещательные рассылки?

Для отслеживания с сети источников, забивающих канал мусорной информацией с целью нарушения работоспособности сети.

## Как с помощью утилиты arp просмотреть arp-кэш и как его очистить? В каких случаях может понадобиться последняя операция?

Просмотр: arp –a

Очистка: netsh interface ip delete arpcache

Очистка кэша может понадобиться, например, при внесении в него неверного статического сопоставления сетевого адреса физическому, вследствие чего могут быть недоступны некоторые ресурсы.