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»

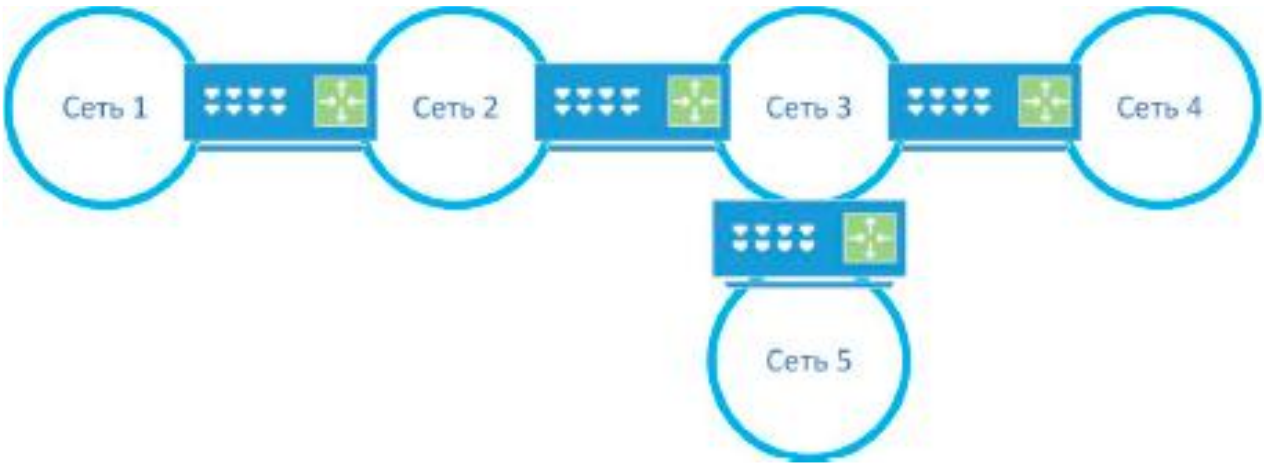
Исполнитель: Трофимов В.А.
Руководитель: Береснев А.Д.
Группа: 3511

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

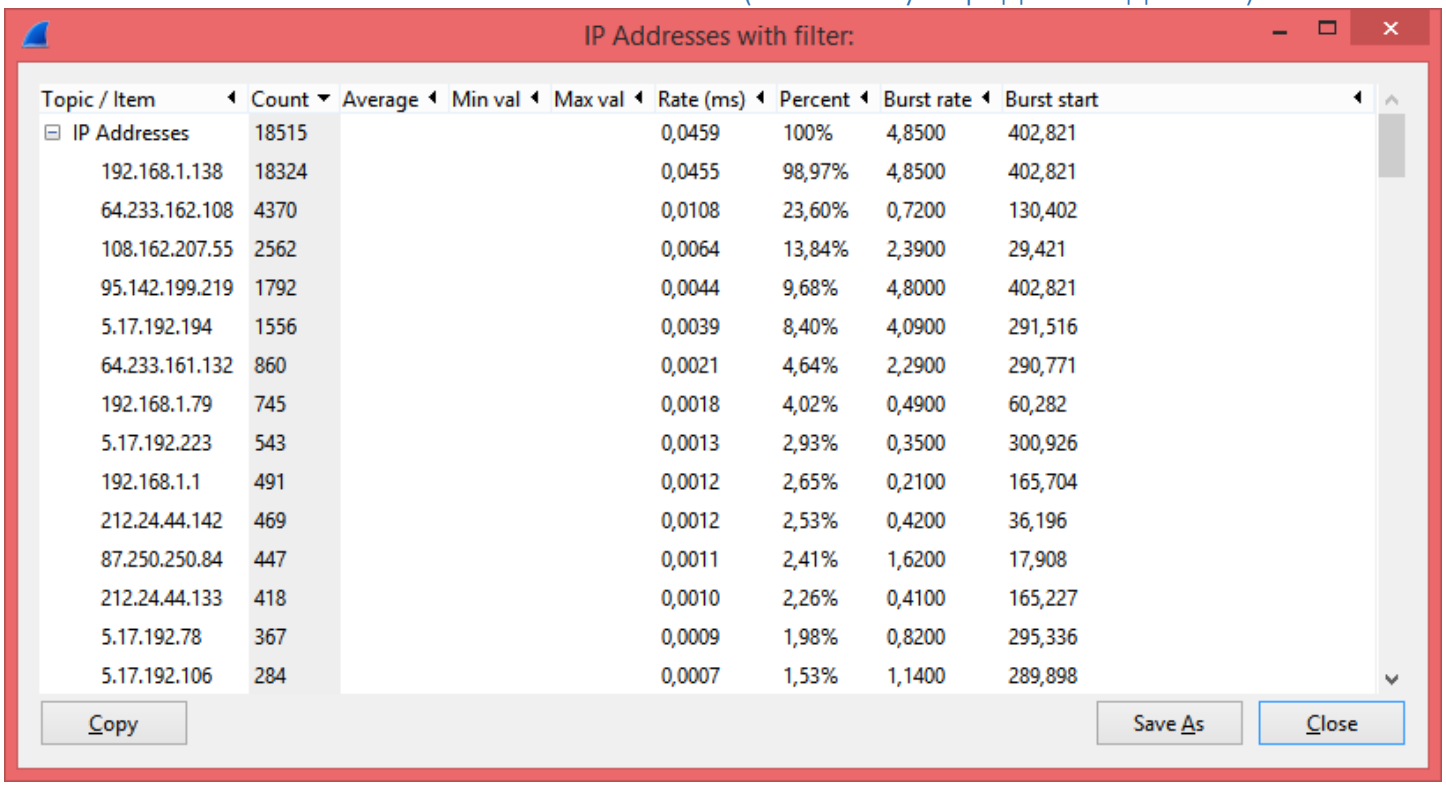
Сеть	Сеть 1	Сеть 2	Сеть 3	Сеть 4	Сеть 5
IP-адрес сети, маска	212.24.15.240 /28	212.24.15.200 /30	212.24.15.196 /30	212.24.15.224 /28	212.24.15.208 /28
Количество IP-адресов в сети	16	4	4	16	16
Начальный и конечный адреса сети, пригодные для адресации портов маршрутизаторов и компьютеров	212.24.15.241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

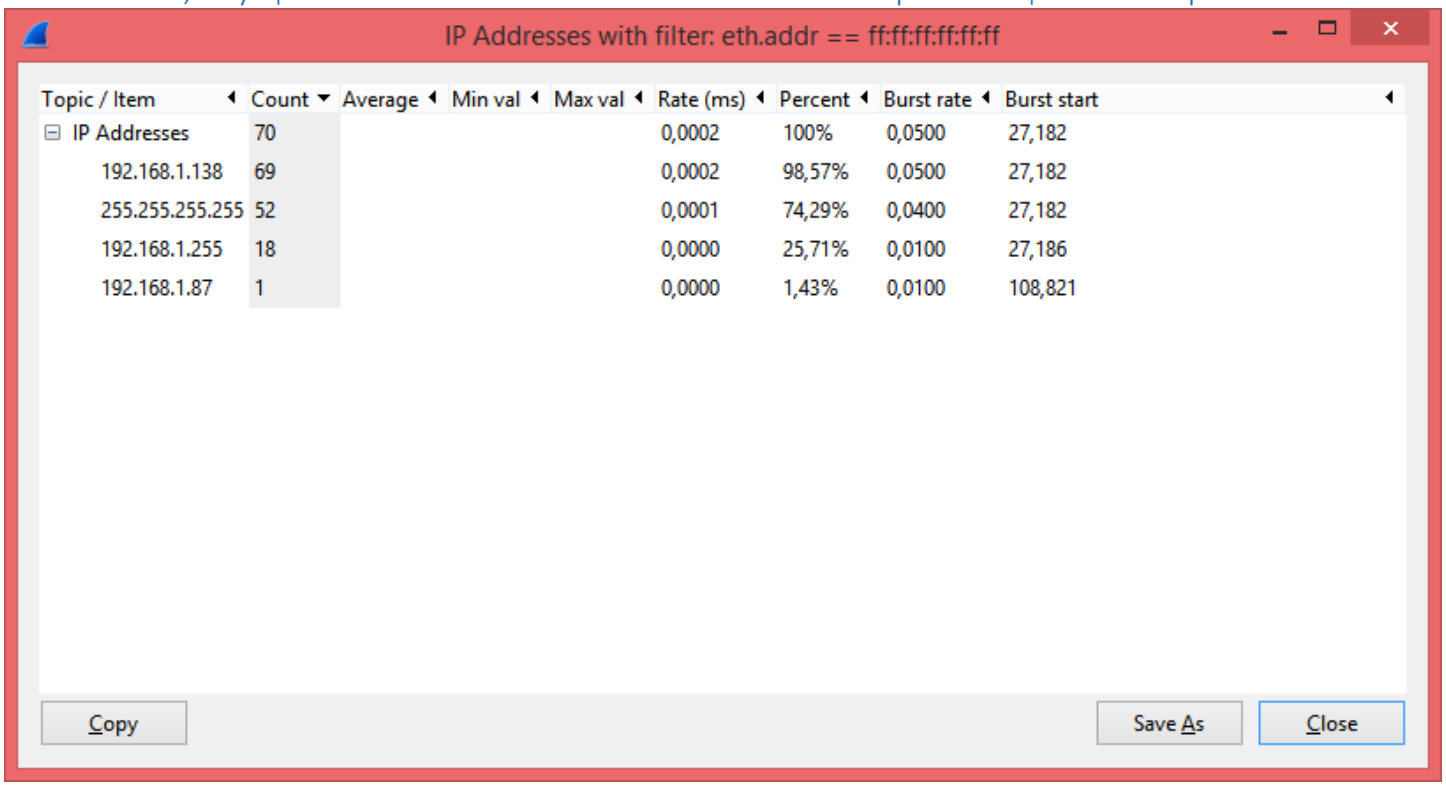
Узел с максимальной активностью (по объему переданных данных)



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
IP Addresses	18515				0,0459	100%	4,8500	402,821
192.168.1.138	18324				0,0455	98,97%	4,8500	402,821
64.233.162.108	4370				0,0108	23,60%	0,7200	130,402
108.162.207.55	2562				0,0064	13,84%	2,3900	29,421
95.142.199.219	1792				0,0044	9,68%	4,8000	402,821
5.17.192.194	1556				0,0039	8,40%	4,0900	291,516
64.233.161.132	860				0,0021	4,64%	2,2900	290,771
192.168.1.79	745				0,0018	4,02%	0,4900	60,282
5.17.192.223	543				0,0013	2,93%	0,3500	300,926
192.168.1.1	491				0,0012	2,65%	0,2100	165,704
212.24.44.142	469				0,0012	2,53%	0,4200	36,196
87.250.250.84	447				0,0011	2,41%	1,6200	17,908
212.24.44.133	418				0,0010	2,26%	0,4100	165,227
5.17.192.78	367				0,0009	1,98%	0,8200	295,336
5.17.192.106	284				0,0007	1,53%	1,1400	289,898

Copy Save As Close

Узел, осуществивший наибольшее количество широковещательных рассылок



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
IP Addresses	70				0,0002	100%	0,0500	27,182
192.168.1.138	69				0,0002	98,57%	0,0500	27,182
255.255.255.255	52				0,0001	74,29%	0,0400	27,182
192.168.1.255	18				0,0000	25,71%	0,0100	27,186
192.168.1.87	1				0,0000	1,43%	0,0100	108,821

Copy Save As Close

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

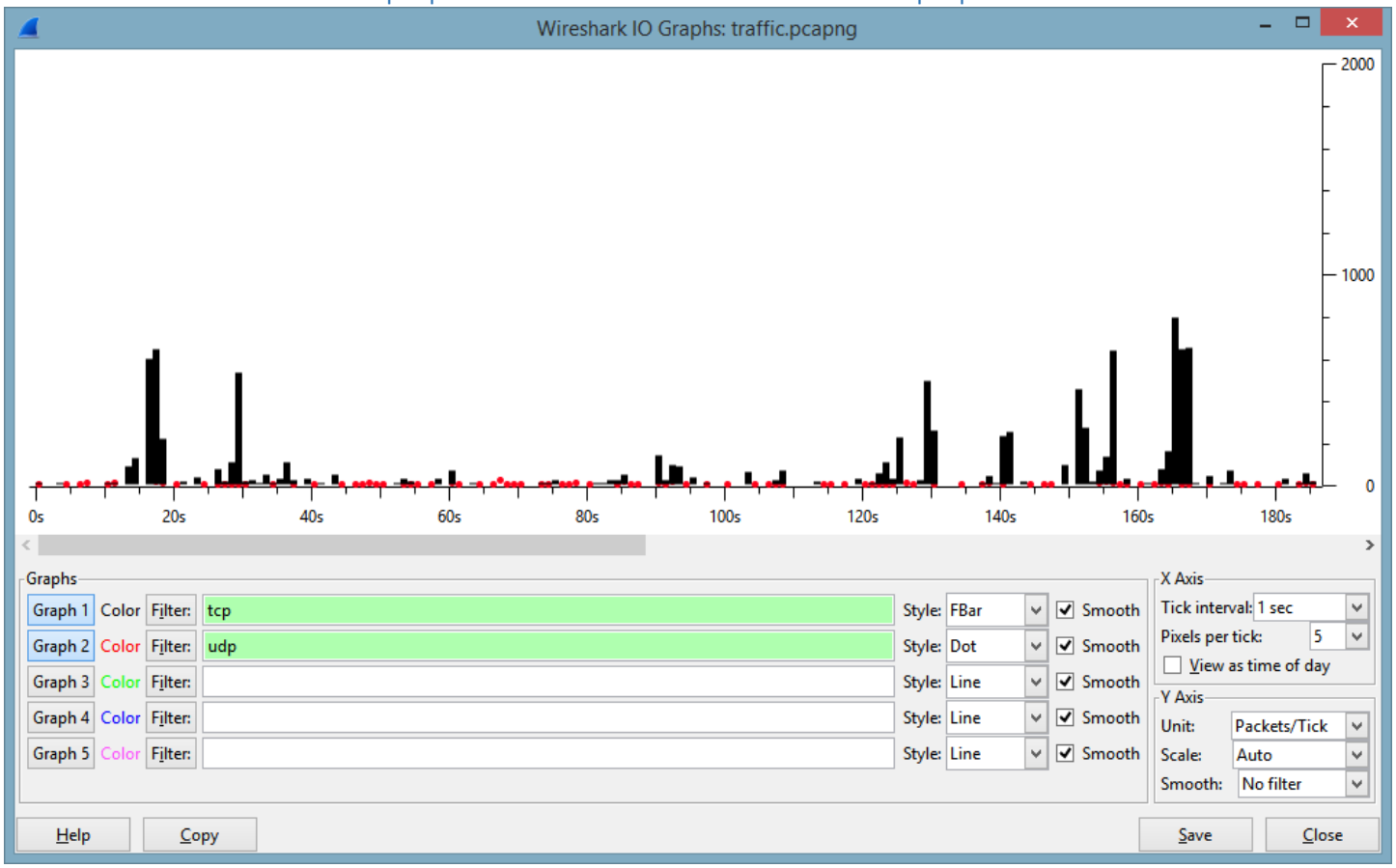
TCP Endpoints: traffic.pcapng

TCP Endpoints: 438

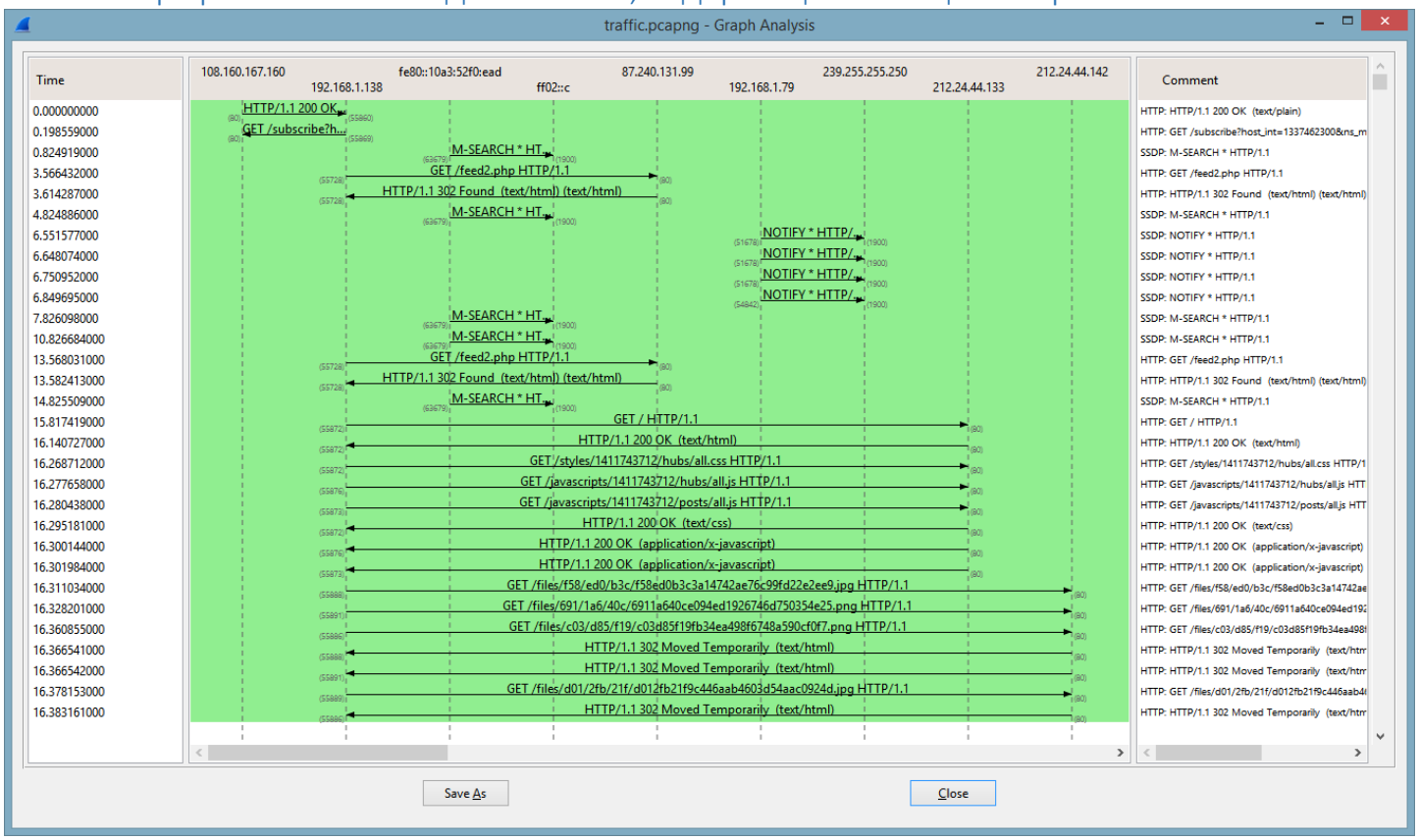
Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
192.168.1.138	36547	4 370	3 959 403	839	49 262	3 531	3 910 141	-	-
64.233.162.108	993	4 370	3 959 403	3 531	3 910 141	839	49 262	-	-
108.162.207.55	80	2 562	2 852 892	1 971	2 790 218	591	62 674	-	-
192.168.1.138	56196	1 792	2 028 185	386	22 125	1 406	2 006 060	-	-
95.142.199.219	443	1 792	2 028 185	1 406	2 006 060	386	22 125	-	-
5.17.192.194	443	1 164	1 219 916	902	1 193 798	262	26 118	-	-
192.168.1.138	56095	1 053	1 149 958	224	20 344	829	1 129 614	-	-
64.233.161.132	443	860	634 919	607	600 518	253	34 401	-	-
192.168.1.138	55885	634	739 960	142	9 415	492	730 545	-	-
5.17.192.223	443	537	230 021	299	113 504	238	116 517	-	-
212.24.44.142	80	469	95 185	184	46 105	285	49 080	-	-
87.250.250.84	80	447	433 351	307	419 334	140	14 017	-	-
192.168.1.79	9000	432	149 778	236	133 578	196	16 200	-	-
212.24.44.133	80	418	220 639	232	191 369	186	29 270	-	-
192.168.1.138	55844	410	187 941	179	105 929	231	82 012	-	-
5.17.192.194	80	392	410 516	289	390 236	103	20 280	-	-
192.168.1.138	55906	390	392 885	119	12 424	271	380 461	-	-
192.168.1.138	56032	385	454 329	79	10 258	306	444 071	-	-
5.17.192.78	443	367	260 655	258	237 101	109	23 554	-	-
192.168.1.138	55883	352	435 795	58	5 575	294	430 220	-	-
192.168.1.138	56117	275	227 504	69	18 483	206	209 021	-	-
192.168.1.138	56097	273	221 265	69	9 411	204	211 854	-	-
192.168.1.138	56036	255	281 575	64	7 946	191	273 629	-	-
173.194.71.94	443	242	111 314	144	83 285	98	28 029	-	-
5.17.192.165	443	231	202 529	168	194 782	63	7 747	-	-
192.168.1.138	55881	221	242 280	54	5 271	167	236 009	-	-

Help Copy Close

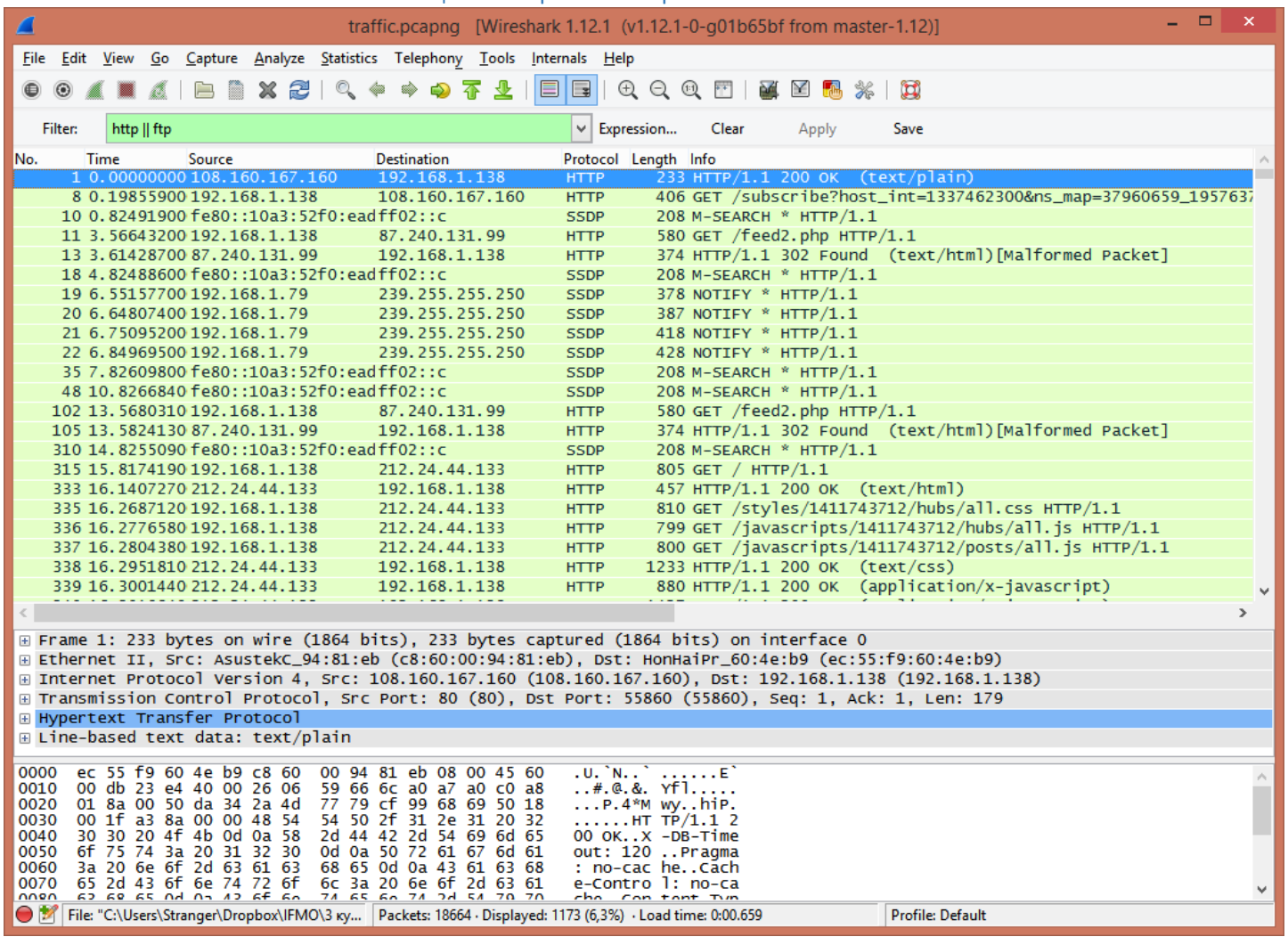
Графики интенсивности TCP и UDP трафика



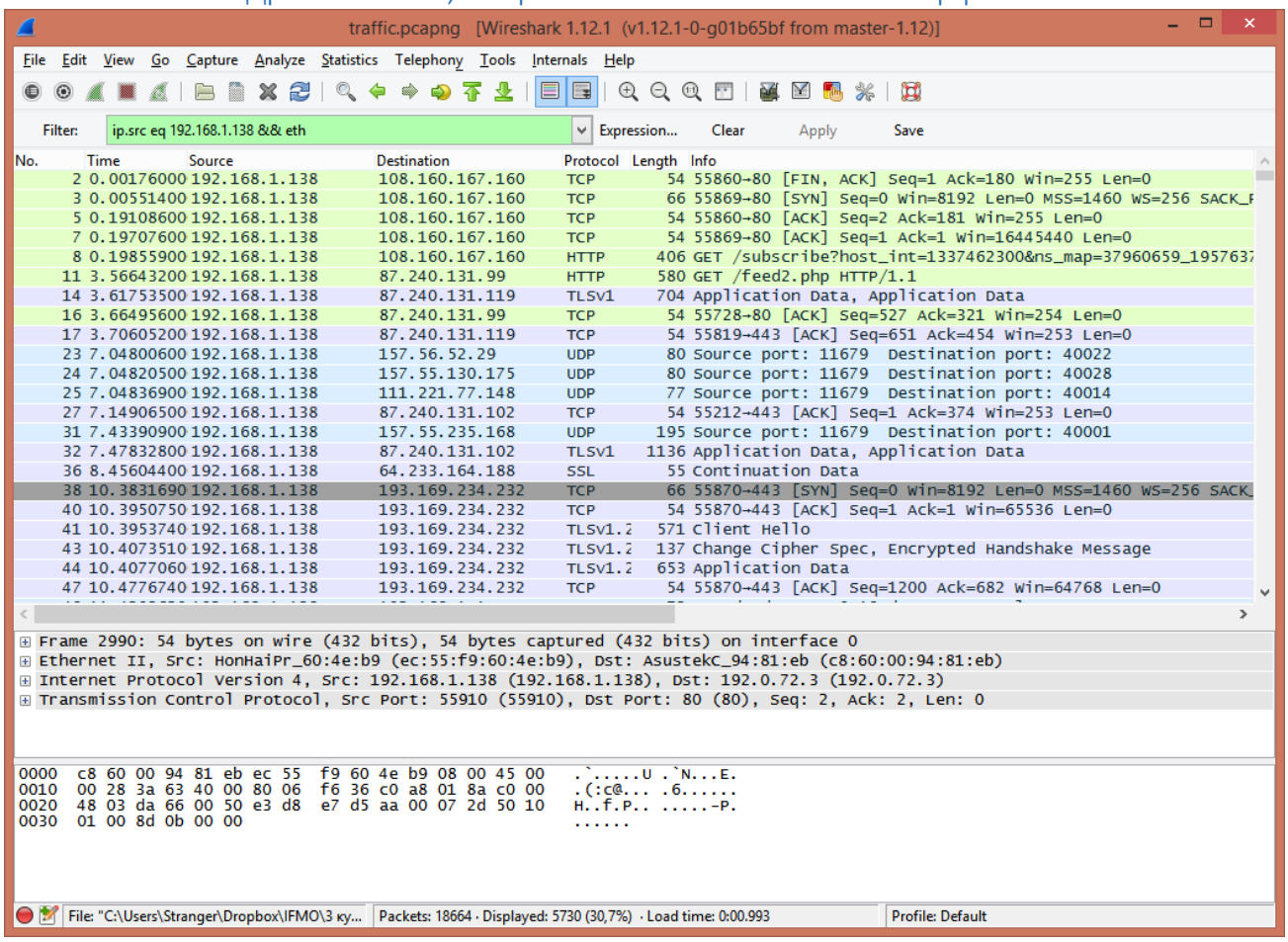
Граф связей только для пакетов, содержащих сообщения протокола HTTP



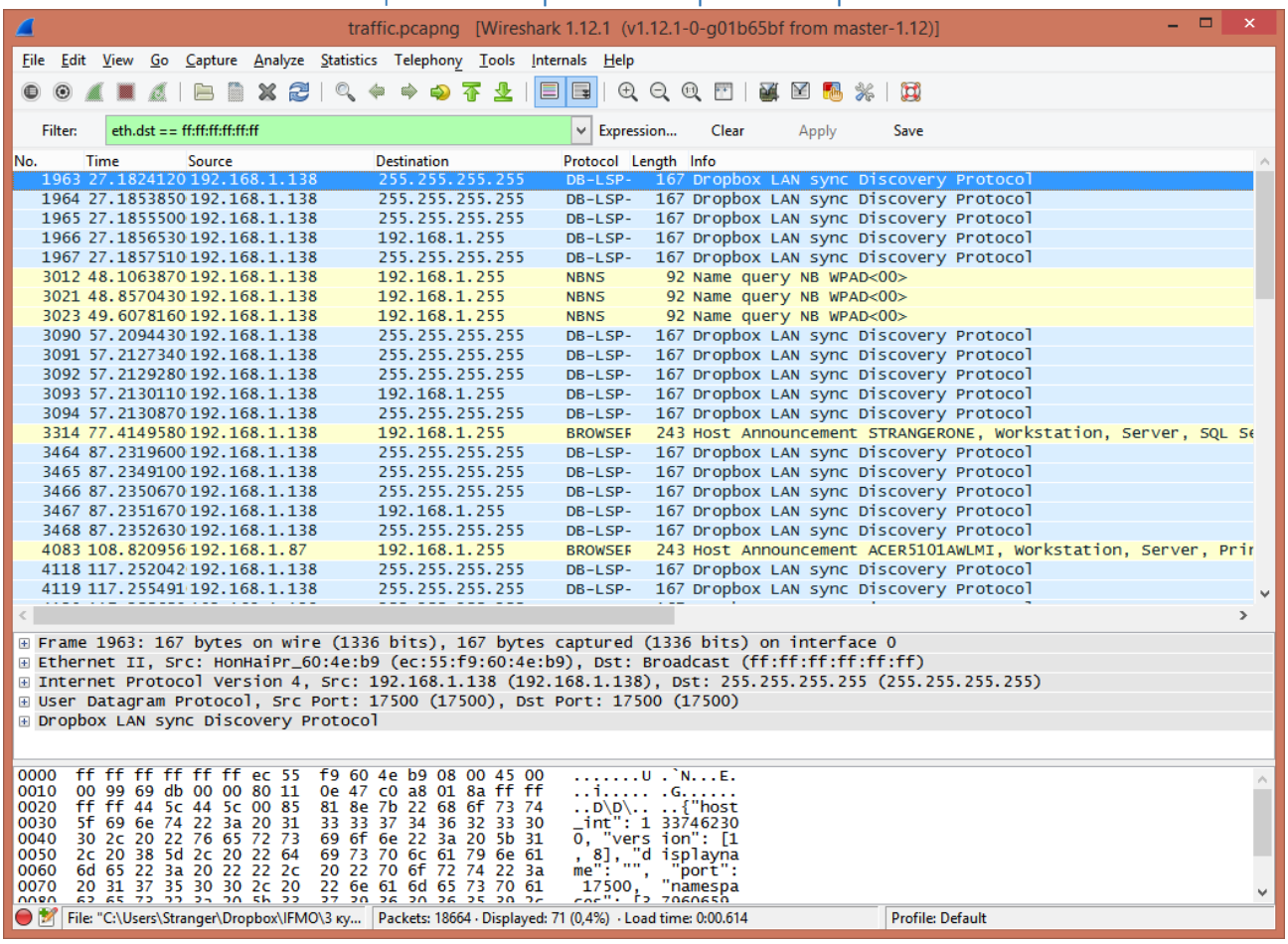
Относящиеся к работе протоколов HTTP и FTP



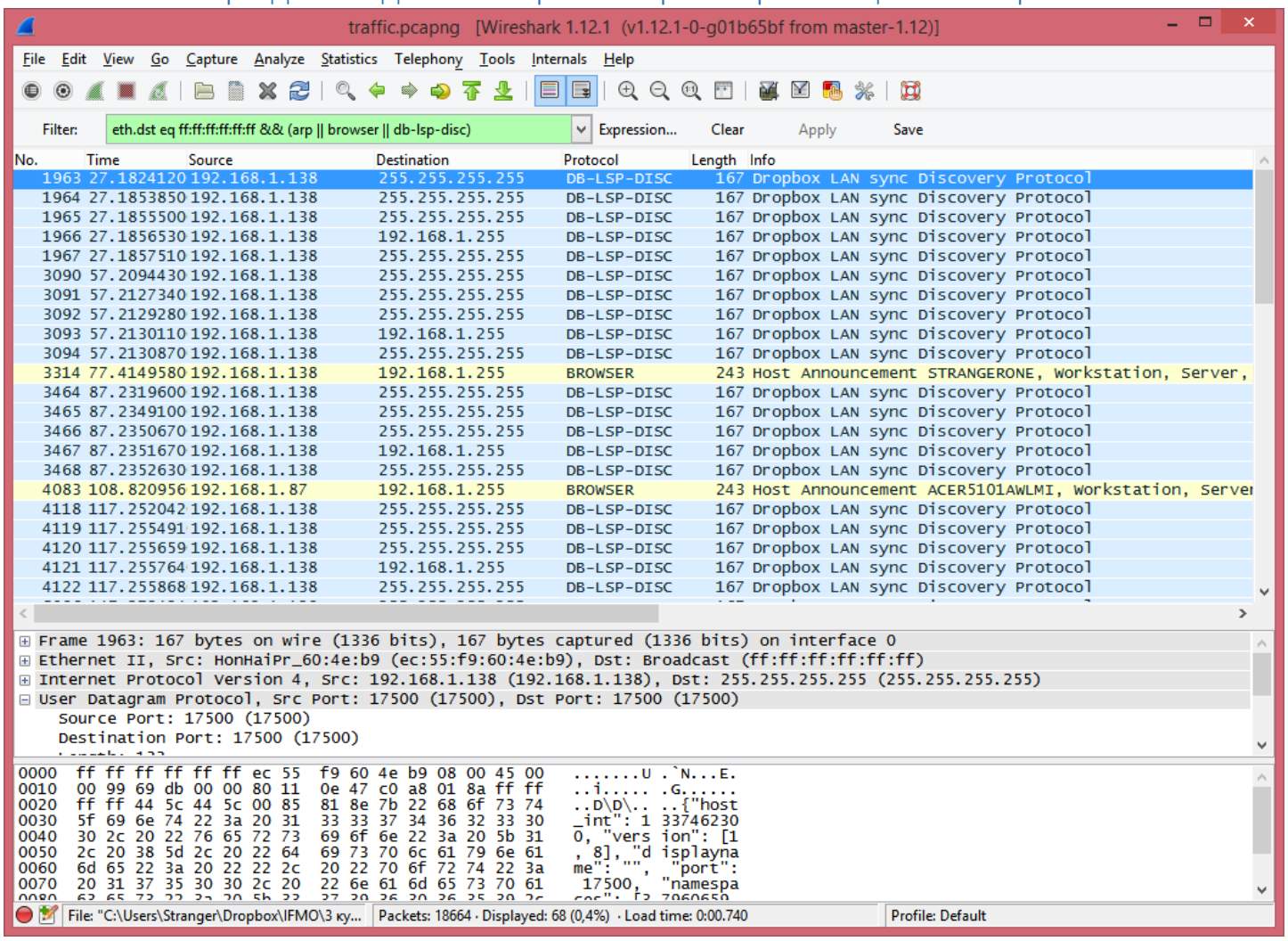
Все кадры Ethernet, отправленные с сетевого интерфейса хоста



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

```
C:\Documents and Settings\Администратор>netstat

Активные подключения

  Имя     Локальный адрес         Внешний адрес          Состояние
  TCP     lwgame-34a6ee3b:telnet  192.168.0.4:54141      ESTABLISHED
  TCP     lwgame-34a6ee3b:1364    192.168.0.4:ssh        ESTABLISHED
```

Список активных портов на Windows хосте

```
C:\Documents and Settings\Администратор>netstat -a

Активные подключения

  Имя     Локальный адрес         Внешний адрес          Состояние
  TCP     lwgame-34a6ee3b:telnet  lwgame-34a6ee3b:0      LISTENING
  TCP     lwgame-34a6ee3b:epmap   lwgame-34a6ee3b:0      LISTENING
  TCP     lwgame-34a6ee3b:microsoft-ds  lwgame-34a6ee3b:0      LISTENING
  TCP     lwgame-34a6ee3b:1025    lwgame-34a6ee3b:0      LISTENING
  TCP     lwgame-34a6ee3b:1367    lwgame-34a6ee3b:0      LISTENING
  TCP     lwgame-34a6ee3b:pptp    lwgame-34a6ee3b:0      LISTENING
  TCP     lwgame-34a6ee3b:telnet  192.168.0.4:54141      ESTABLISHED
  TCP     lwgame-34a6ee3b:netbios-ssn  lwgame-34a6ee3b:0      LISTENING
  TCP     lwgame-34a6ee3b:1364    192.168.0.4:ssh        ESTABLISHED
  UDP     lwgame-34a6ee3b:microsoft-ds  *:*
  UDP     lwgame-34a6ee3b:l2tp    *:*
  UDP     lwgame-34a6ee3b:1365    *:*
  UDP     lwgame-34a6ee3b:1366    *:*
  UDP     lwgame-34a6ee3b:netbios-ns  *:*
  UDP     lwgame-34a6ee3b:netbios-dgm  *:*
```

Список соединений на Linux хосте

```
[root@borsch ~]# ss
State       Recv-Q Send-Q                     Local Address:Port                      Peer Address:Port
CLOSE-WAIT  1      0                            192.168.0.4:41605                    185.5.160.146:http
ESTAB       0      0                            192.168.0.4:ssh                        192.168.0.5:ndm-serve
r
ESTAB       0      0                            192.168.0.4:54141                      192.168.0.5:telnet
```

Список активных портов на Linux хосте

```
[root@borsch ~]#  netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:x11                       *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 localhost:ipp               *:*                         LISTEN
tcp        0      0 localhost:smtp              *:*                         LISTEN
tcp        0      0 *:17500                     *:*                         LISTEN
tcp        0      0 *:x11                       *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 localhost:ipp               *:*                         LISTEN
tcp        0      0 localhost:smtp              *:*                         LISTEN
udp        0      0 *:bootpc                    *:*
udp        0      0 *:17500                     *:*
udp        0      0 *:ipp                       *:*
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     20746  /tmp/orbit-root/linc-86f-0-304508ffd9e73
unix  2      [ ACC ]     STREAM     LISTENING     11758  @/var/run/hald/dbus-1AiNtAVAn9
unix  2      [ ACC ]     STREAM     LISTENING     13256  @/tmp/dbus-auUBgVwiiV
unix  2      [ ACC ]     STREAM     LISTENING     8552   @/com/ubuntu/upstart
unix  2      [ ACC ]     STREAM     LISTENING     12461  private/anvil
unix  2      [ ACC ]     STREAM     LISTENING     12465  private/scache
unix  2      [ ACC ]     STREAM     LISTENING     13172  @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     15459  /root/.dropbox/command_socket
unix  2      [ ACC ]     STREAM     LISTENING     11416  /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     13173  /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     13368  /tmp/ssh-zBvDBC1620/agent.1620
unix  2      [ ACC ]     STREAM     LISTENING     11627  /var/run/cups/cups.sock
unix  2      [ ACC ]     STREAM     LISTENING     13395  /tmp/.ICE-unix/1620
unix  2      [ ACC ]     STREAM     LISTENING     13460  /tmp/orbit-root/linc-662-0-7847425216907
unix  2      [ ACC ]     STREAM     LISTENING     13672  /tmp/orbit-root/linc-654-0-16e3abce1f155
unix  2      [ ACC ]     STREAM     LISTENING     13791  /tmp/keyring-SqhHTy/socket
unix  2      [ ACC ]     STREAM     LISTENING     13800  /tmp/orbit-root/linc-670-0-b46967e53db0
unix  2      [ ACC ]     STREAM     LISTENING     13805  /tmp/keyring-SqhHTy/socket.ssh
unix  2      [ ACC ]     STREAM     LISTENING     13807  /tmp/keyring-SqhHTy/socket.pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     13825  /tmp/orbit-root/linc-675-0-13faf3395bd30
```

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

```
[root@borsch ~]# tcpdump -X -i eth0 host 192.168.0.5 && port 23
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:52:23.250292 IP 192.168.0.4.54682 > 192.168.0.5.telnet: Flags [P.], seq 3776186469:3776186472, ack 120543674, win 313, len
gth 3
        0x0000:  4510 002b d2bf 4000 4006 e6a3 c0a8 0004  E..+..@.@.......
        0x0010:  c0a8 0005 d59a 0017 e114 0865 072f 59ba  ...........e./Y.
        0x0020:  5018 0139 8177 0000 1b5b 41              P..9.w...[A
11:52:23.349523 IP 192.168.0.5.telnet > 192.168.0.4.54682: Flags [P.], seq 1:4, ack 3, win 64187, length 3
        0x0000:  4500 002b 3b1e 4000 4006 7e55 c0a8 0005  E..+;.@.@.~U....
        0x0010:  c0a8 0004 0017 d59a 072f 59ba e114 0868  ........./Y....h
        0x0020:  5018 fabb b740 0000 1b5b 4100 0000       P....@...[A...
11:52:23.349561 IP 192.168.0.4.54682 > 192.168.0.5.telnet: Flags [.], ack 4, win 313, length 0
        0x0000:  4510 0028 d2c0 4000 4006 e6a5 c0a8 0004  E..(..@.@.......
        0x0010:  c0a8 0005 d59a 0017 e114 0868 072f 59bd  ...........h./Y.
        0x0020:  5010 0139 0d27 0000                      P..9.'..
11:52:23.586165 IP 192.168.0.4.54682 > 192.168.0.5.telnet: Flags [P.], seq 3:4, ack 4, win 313, length 1
        0x0000:  4510 0029 d2c1 4000 4006 e6a3 c0a8 0004  E..)..@.@.......
        0x0010:  c0a8 0005 d59a 0017 e114 0868 072f 59bd  ...........h./Y.
        0x0020:  5018 0139 8175 0000 0d                   P..9.u...
11:52:23.693384 IP 192.168.0.5.telnet > 192.168.0.4.54682: Flags [P.], seq 4:544, ack 4, win 64187, length 540
        0x0000:  4500 0244 3b1f 4000 4006 7c3b c0a8 0005  E..D;.@.@.|;....
        0x0010:  c0a8 0004 0017 d59a 072f 59bd e114 0869  ........./Y....i
        0x0020:  5018 fabb e746 0000 0d0a 2092 aeac 20a2  P....F.........
        0x0030:  20e3 e1e2 e0ae a9e1 e2a2 a520 4320 ada5  ...........C...
        0x0040:  20a8 aca5 a5e2 20ac a5e2 aaa8 2e0d 0a20  ..............
        0x0050:  91a5 e0a8 a9ad eba9 20ad aeac a5e0 20e2  ..............
        0x0060:  aeac a03a 2032 4346 372d 4432 3745 0d0a  ...:.2CF7-D27E..
        0x0070:  0d0a 2091 aea4 a5e0 a6a8 acae a520 afa0  .............
        0x0080:  afaa a820 433a 5c44 6f63 756d 656e 7473  ....C:\Documents
        0x0090:  2061 6e64 2053 6574 7469 6e67 735c 6164  .and.Settings\ad
        0x00a0:  6d69 6e0d 0a0d 0a32 392e 3039 2e32 3031  min....29.09.201
        0x00b0:  3420 2030 303a 3438 2020 2020 3c44 4952  4..00:48....<DIR
        0x00c0:  3e20 2020 2020 2020 2020 202e 0d0a 3239  >.............29
        0x00d0:  2e30 392e 3230 3134 2020 3030 3a34 3820  .09.2014..00:48.
        0x00e0:  2020 203c 4449 523e 2020 2020 2020 2020  ...<DIR>........
        0x00f0:  2020 2e2e 0d0a 3037 2e30 392e 3230 3134  ......07.09.2014
```

Ответы на вопросы

Какие типы кадров Ethernet бывают, в чем их отличия?

Кадр 802.3/LLC

6	6	2	1	1	1(2)	46–1497 (1496)	4
DA	SA	L	DSAP	SSAP	Control	Data	FCS
			Заголовок LLC				

Кадр Raw 802.3/Novell 802.3

6	6	2	46–1500	4
DA	SA	L	Data	FCS

Кадр Ethernet DIX (II)

6	6	2	46–1500	4
DA	SA	T	Data	FCS

Кадр Ethernet SNAP

6	6	2	1	1	1	3	2	46–1492	4
DA	SA	L	DSAP	SSAP	Control	OUI	T	Data	FCS
			AA	AA	03	000000			
			Заголовок LLC			Заголовок SNAP			

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.