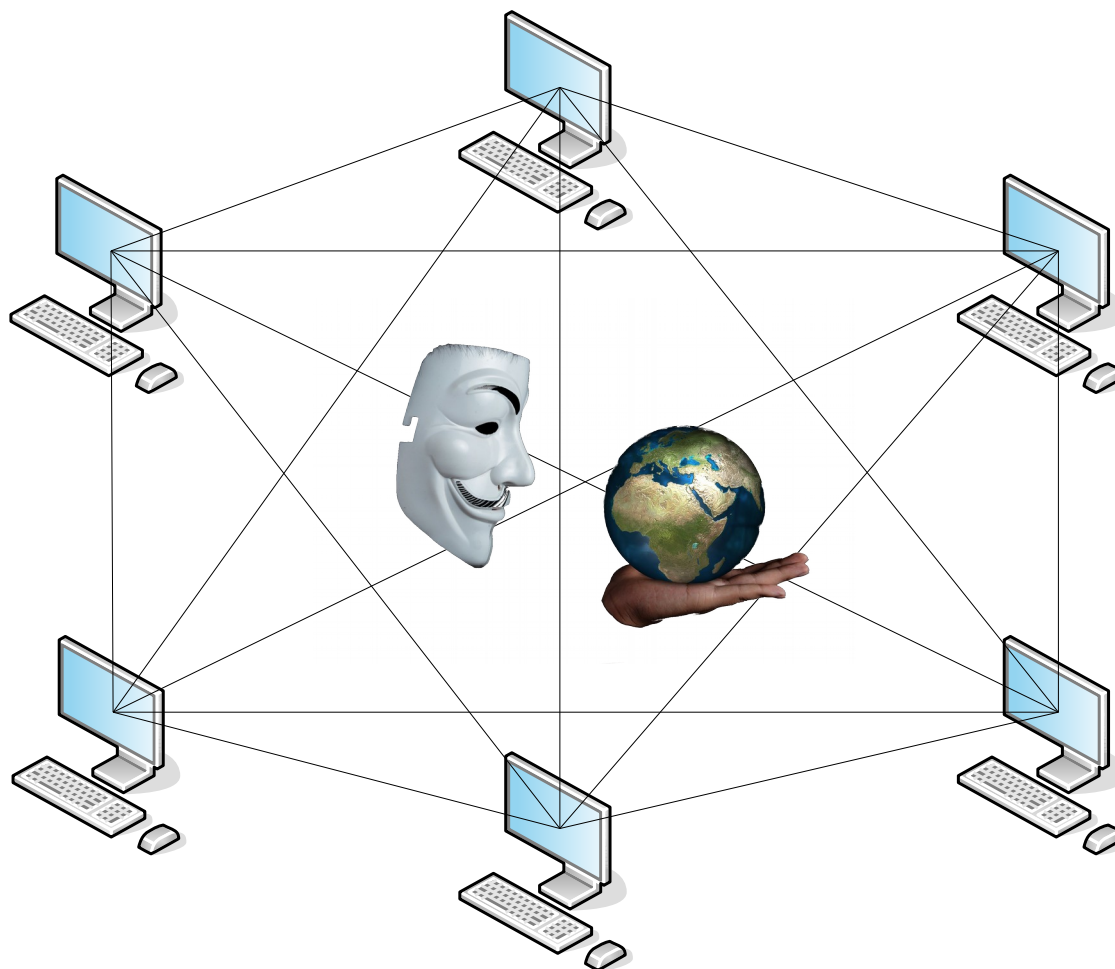


Ограничение использования файлообменных сетей P2P на примере протокола BitTorrent



Об авторе

- Антон Тарасов, г. Алматы, Казахстан
- Сертификаты MikroTik: МТСНА, МТСРЕ, МТСВЕ, МТСТСЕ
- Сертифицированный тренер MikroTik TR0416
- WWW: <http://routeros.kz>
- Skype: a_tarassov
- E-mail: a.tarassov@gmail.com

Цель презентации

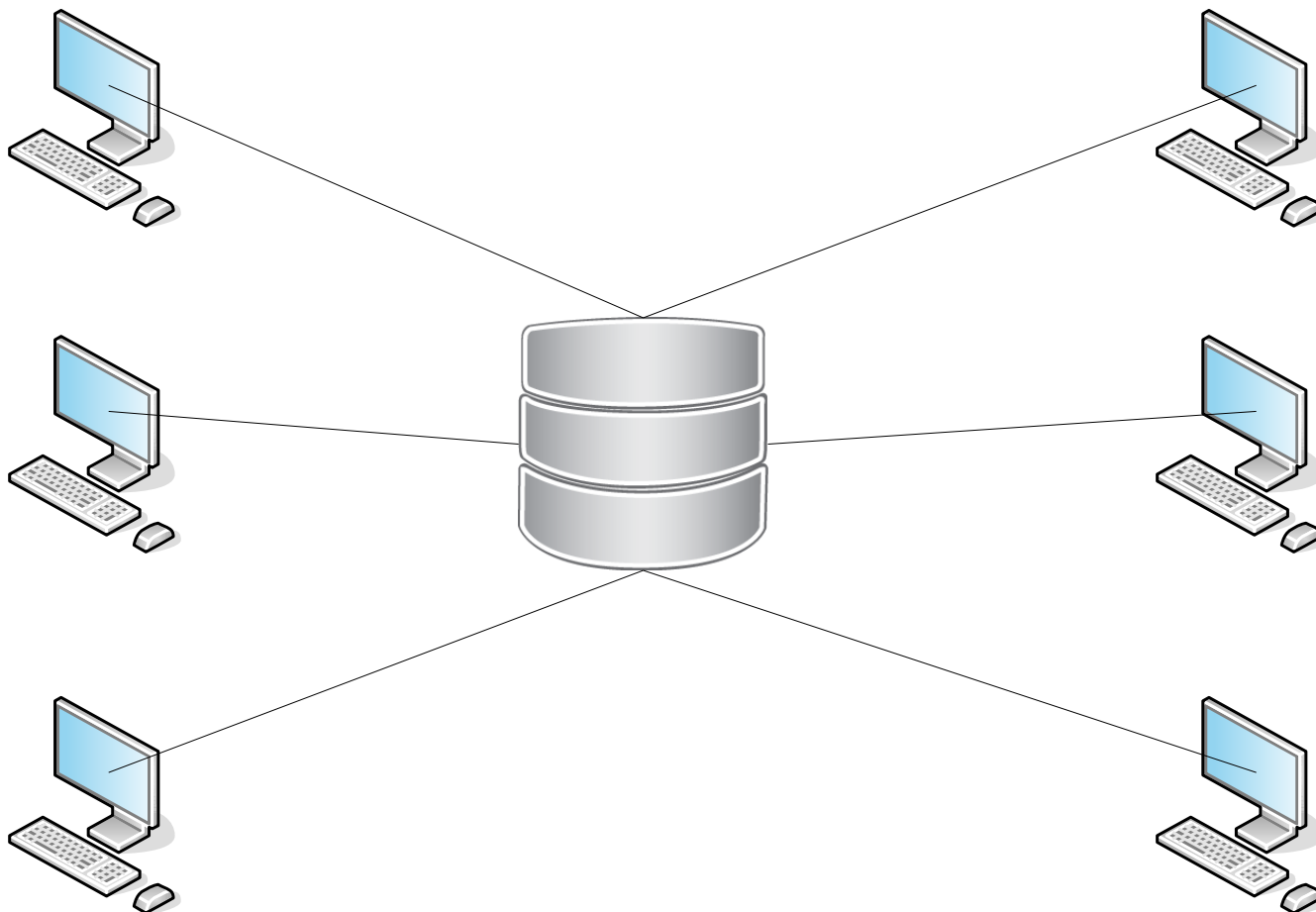
- Исследовать протокол BitTorrent и его расширения согласно официальной документации и при помощи Wireshark
- Показать возможности использования Layer7 фильтров на RouterOS
- Ограничить скорость скачивания файлов из сети BitTorrent
- Реальный опыт эксплуатации

Основная задача

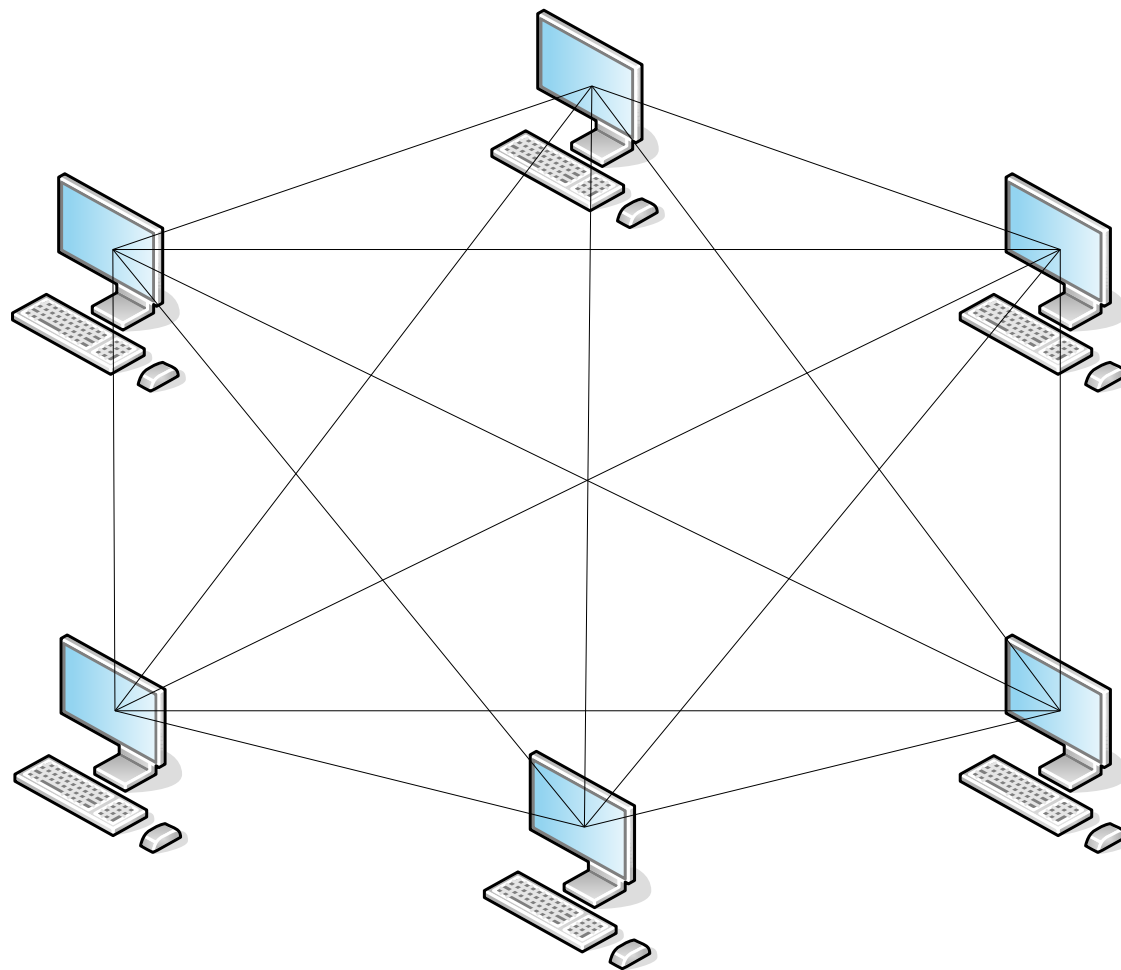
- НЕ запретить, НО ограничить



Модель сети «клиент-сервер»



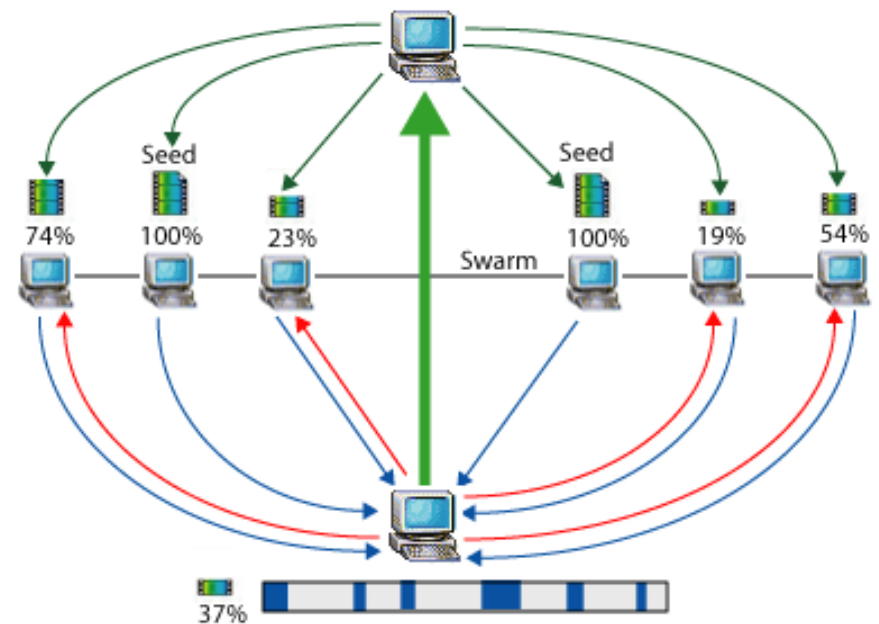
Одноранговая или пиринговая сеть



Пиринговая (P2P) сеть

- BitTorrent - P2P-протокол, предназначенный для обмена файлами через Интернет
- Торрент-трекер координирует действия скачивающего и раздающих (сидеров)

BitTorrent-трекер идентифицирует рой и сопровождает обмен файлами



Компьютер при помощи BitTorrent-клиента одновременно получает и отправляет множество частей файлов

Плюсы и минусы P2P сетей

Плюсы:

- отсутствие очередей на загрузку
- высокая скорость (чем больше раздающих, тем выше скорость)
- докачка файлов (в любое время можно продолжить загрузку)
- много трекеров без регистрации

Минусы:

- не слабо загружает канал, если не ограничивать, иногда даже страничку открыть сложно
- требуется установка сторонней программы (bittorrent, utorrent, transmission и т. д.)

Политики разрешения

Запрещено все, что не разрешено:

- Обычно применяется в корпоративных сетях
- Большой набор разрешающих правил
- Более высокая нагрузка на CPU

Разрешено все, что не запрещено:

- Обычно применяется в сетях сервис провайдера при пропуске трафика к абонентам
- Несколько запрещающих правил
- Менее высокая нагрузка на CPU

Порядок определения и ограничения P2P трафика

- Создание адресного листа (/ip firewall address-list), для хранения IP адресов раздающих – „p2p-seeds“
- Добавление FQDN трекеров в адресный лист – „p2p-seeds“
- Создание списка Layer7 протоколов (/ip firewall layer7-protocol)
- Создание правил обнаружения P2P соединений
- Добавление обнаруженных IP адресов в адресный лист
- Маркировка соединений и пакетов с IP адресами из адресного листа
- Ограничение скорости (/simple queues или /queue tree)

Создание адресного листа и добавление FQDN трекеров

Нр.	Название	Ссылка	Посетители	Регистрация	Статус
1.	Rutracker		83M	Да	●
2.	LostFilm		29M	Да	●
3.	PornoLab (18+)		19.7M	Да	●
..	таронс	онек.net		да	
12.	HDClub		3.4M	Да	●
13.	HDReactor		2.9M	Нет	●
14.	Torrent Baza		2.8M	Нет	●
15.	RiperAM		2.7M	Нет	●
16.	PiratBit		2.5M	Нет	●
17.	Katushka		2.4M	Нет	●

Создание адресного листа и добавление FQDN трекеров

v6.36 changes

...

*) firewall - allow to add domain name to address-lists (dynamic entries for resolved addresses will be added to specified list);

...

A terminal window titled "Terminal" with a blue header bar. The terminal shows a series of commands to add addresses to a list named "p2p-seeds". The commands are:

```
/ip firewall address-list  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
[antoxa@BT] >
```

 The terminal output shows the commands being executed, with the list name "p2p-seeds" highlighted in green. The prompt is "[antoxa@BT] >".

```
Terminal  
/ip firewall address-list  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
add address=[redacted] list=p2p-seeds  
[antoxa@BT] >
```

Создание адресного листа и добавление FQDN трекеров

Name	Address	Timeout	Creation Time
p2p-seeds			Sep/22/2017 22:51:23
D p2p-seeds			Sep/22/2017 22:51:23
p2p-seeds			Sep/22/2017 22:51:23
D p2p-seeds			Sep/22/2017 22:51:23
p2p-seeds			Sep/22/2017 22:51:23
D p2p-seeds			Sep/22/2017 22:51:24
p2p-seeds			Sep/22/2017 22:51:23
D p2p-seeds			Sep/22/2017 22:51:24
p2p-seeds			Sep/22/2017 22:51:24
D p2p-seeds			Sep/22/2017 22:51:24
p2p-seeds			Sep/22/2017 22:51:24
D p2p-seeds			Sep/22/2017 22:51:24
p2p-seeds			Sep/22/2017 22:51:24
D p2p-seeds			Sep/22/2017 22:51:24
p2p-seeds			Sep/22/2017 22:51:24
D p2p-seeds			Sep/22/2017 22:51:24
p2p-seeds			Sep/22/2017 22:51:24
D p2p-seeds			Sep/22/2017 22:51:24
p2p-seeds			Sep/22/2017 22:51:24
D p2p-seeds			Sep/22/2017 22:51:24
p2p-seeds			Sep/22/2017 22:51:24
D p2p-seeds			Sep/22/2017 22:51:24
p2p-seeds			Sep/22/2017 22:51:24
D p2p-seeds			Sep/22/2017 22:51:24
p2p-seeds			Sep/22/2017 22:51:24
D p2p-seeds			Sep/22/2017 22:51:24
p2p-seeds			Sep/22/2017 22:51:24
D p2p-seeds			Sep/22/2017 22:51:24

25 items

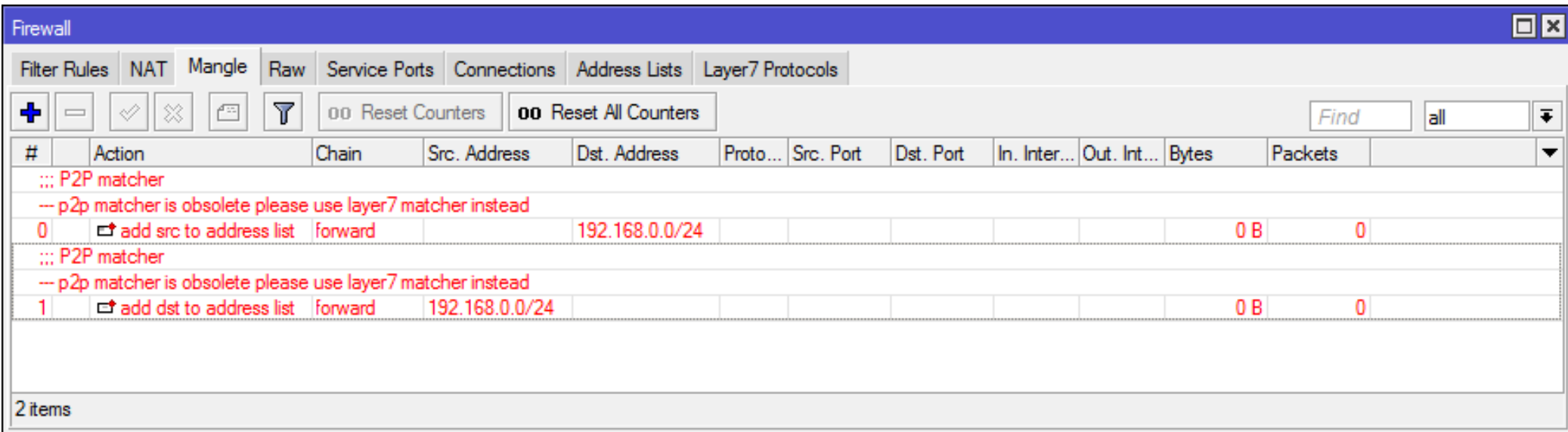
Встроенный P2P matcher

v6.39 changes

...

!) firewall - discontinued support for p2p matcher (old rules will become invalid);

...



The screenshot shows the Firewall configuration window in RouterOS. The 'Filter Rules' tab is active. The table below shows two rules, both of which are marked as obsolete due to the discontinued support for P2P matchers.

#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	add src to address list	forward		192.168.0.0/24						0 B	0
1	add dst to address list	forward	192.168.0.0/24							0 B	0

2 items

RouterOS Layer7

- Метод поиска данных по шаблону в ICMP/TCP/UDP потоках
- L7 matcher анализирует первые 10 пакетов или первые 2КБ соединения
- L7 matcher должен видеть и входящий и исходящий трафик, т. е. находиться в цепочке forward, или обязательно в prerouting+postrouting
- L7 это ресурсоемкий процесс
- L7 шаблоны независимы от регистра

RouterOS Layer7

- RouterOS L7 шаблоны совместимы с шаблонами проекта L7-filter

The pattern *name* is what you must use when issuing l7-filter commands. The names below link to the pattern files. Select column headings to sort

bad third line in replaytv-ivs.pat

wiki	name	speed	quality	group	notes	description
	100bao	○○○	■			100bao - a Chinese P2P protocol/program - http://www.100bao.com
	aim	●○○	■	L ₀ L \$		AIM - AOL instant messenger (OSCAR and TOC)
	aimwebcontent	●○○	■	L ₀ L	\$	AIM web content - ads/news content downloaded by AOL Instant Messenger
	applejuice	○○○	■			Apple Juice - P2P filesharing - http://www.applejuicenet.de
	ares	○○○	■	055	-	Ares - P2P filesharing - http://aresgalaxy.sf.net
	armagetron	●○○	■	055		Armagetron Advanced - open source Tron/snake based multiplayer game
	battlefield1942	○○○	■	\$		Battlefield 1942 - An EA game
	battlefield2	●○○	■	\$		Battlefield 2 - An EA game.
	battlefield2142	○○○	■	\$		Battlefield 2142 - An EA game.
	bgp	○○○	■			BGP - Border Gateway Protocol - RFC 1771
	biff	○○○	■		- +	Biff - new mail notification
	bittorrent	●○○	■	055	-	Bittorrent - P2P filesharing / publishing tool - http://www.bittorrent.com
	chikka	○○○	■	\$ L ₀ L	●	Chikka - SMS service which can be used without phones - http://chikka.com

RouterOS Layer7

```
← ⓘ | 17-filter.sourceforge.net/layer7-protocols/protocols/bittorrent | 🔍 Поиск | ☆ | 📁 | 🛡️ | ⬇️ | 🏠 | ☰
```

```
# Bittorrent - P2P filesharing / publishing tool - http://www.bittorrent.com
# Pattern attributes: good slow notsofast undermatch
# Protocol groups: p2p open_source
# Wiki: http://www.protocolinfo.org/wiki/Bittorrent
# Copyright (C) 2008 Matthew Strait, Ethan Sommer; See ../LICENSE
#
# This pattern has been tested and is believed to work well.
# It will, however, not work on bittorrent streams that are encrypted, since
# it's impossible to match (well) encrypted data.

bittorrent

# Does not attempt to match the HTTP download of the tracker
# 0x13 is the length of "bittorrent protocol"
# Second two bits match UDP wierdness
# Next bit matches something Azureus does
# Ditto on the next bit. Could also match on "user-agent: azureus", but that's in the next
# packet and perhaps this will match multiple clients.
# bitcomet-specific strings contributed by liangjun.

# This is not a valid GNU basic regular expression (but that's ok).
^(\\x13bittorrent protocol|azver\\x01$|get /scrape\\?info_hash=get /announce\\?info_hash=|get /client/bitcomet/|GET
/data\\?fid=)|d1:ad2:id20:|\\x08'7P\\) [RP]

# This pattern is "fast", but won't catch as much
#^(\\x13bittorrent protocol|azver\\x01$|get /scrape\\?info_hash=)
```

RouterOS Layer7

The image shows a screenshot of the RouterOS Firewall configuration interface, specifically the Layer7 Protocols tab. A table lists a single protocol named 'l7-filter' with a complex regular expression. Below the table is a terminal window showing the command used to create this protocol.

Firewall Layer7 Protocols Configuration:

Name	Regex
l7-filter	^(\x13bittorrent protocol azver\x01\$ get /scrape\?info_hash=get /announce\?info_hash=get /client/bitcomet/GET /data\?fid=) d1:ad2:id20: \x08'7P\)[RP]

1 item

Terminal Output:

```
/ip firewall layer7-protocol
add name=l7-filter regex="^(\x13bittorrent protocol|azver\x01$|get /scrape\\?info_hash=get /announce\\?info_hash=get /\
client/bitcomet/|GET /data\\?fid=)|d1:ad2:id20:|\x08'7P\)[RP]"
[antoxa@BT] >
```

Определение P2P соединений и маркировка пакетов

The image shows the Mikrotik WinBox Firewall configuration interface and a terminal window. The Firewall configuration is for the 'Mangle' tab, showing five rules. Red boxes and arrows highlight the flow of connection and packet marking: Rule 2 marks connections to 'p2p-cmark', Rule 3 marks connections to 'p2p-cmark', and Rule 4 marks packets to 'p2p-pmark' based on the 'p2p-cmark' connection mark.

#	Action	Chain	Src. Address	Dst. Address	Connection Mark	Src. Address List	Dst. Address List	Layer7 Protocol	New Packet Mark	New Connection Mark	Bytes	Packets
0	add src to address list	forward		192.168.0.0/24		p2p-seeds		l7-filter			0 B	0
1	add dst to address list	forward	192.168.0.0/24				p2p-seeds	l7-filter			0 B	0
2	mark connection	forward				p2p-seeds				p2p-cmark	0 B	0
3	mark connection	forward					p2p-seeds			p2p-cmark	0 B	0
4	mark packet	forward			p2p-cmark					p2p-pmark	0 B	0

5 items

```
Terminal
/ip firewall mangle
add action=add-src-to-address-list address-list=p2p-seeds address-list-timeout=none-dynamic chain=forward dst-address=192.168.0.0/24 \
layer7-protocol=l7-filter src-address-list=!p2p-seeds
add action=add-dst-to-address-list address-list=p2p-seeds address-list-timeout=none-dynamic chain=forward dst-address-list=!p2p-seeds \
layer7-protocol=l7-filter src-address=192.168.0.0/24
add action=mark-connection chain=forward new-connection-mark=p2p-cmark passthrough=yes src-address-list=p2p-seeds
add action=mark-connection chain=forward dst-address-list=p2p-seeds new-connection-mark=p2p-cmark passthrough=yes
add action=mark-packet chain=forward connection-mark=p2p-cmark new-packet-mark=p2p-pmark passthrough=no
[antoxa@BT] >
```

Ограничение скорости P2P

The image shows the RouterOS Queue List and the configuration for a Simple Queue named 'P2P'. The Queue List table is as follows:

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit (bi...
0	P2P	192.168.0.0/24	512k	512k	p2p-pmark	

The configuration for the Simple Queue 'P2P' is shown in the 'General' tab:

- Packet Marks: p2p-pmark
- Target Upload Limit At: unlimited
- Target Download Limit At: unlimited bits/s
- Priority: 8
- Bucket Size: 0.100 ratio
- Queue Type: default-small
- Parent: none

Buttons on the right side of the configuration window include: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters, and Torch. The status at the bottom is 'enabled'.

Тестирование конфигурации

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Find p2p-seeds

Name	Address	Timeout	Creation Time
D p2p-seeds			Sep/23/2017 00:21:51
D p2p-seeds			Sep/23/2017 00:21:06
D p2p-seeds			Sep/23/2017 00:23:56
D p2p-seeds			Sep/23/2017 00:23:40
D p2p-seeds			Sep/23/2017 00:21:17
D p2p-seeds			Sep/23/2017 00:23:39

1522 items

Queue List

Simple Queues Interface Queues Queue Tree Queue Types

Reset Counters Reset All Counters

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks
0	P2P	192.168.0.0/24	512k	512k	p2p-mark

1 item (1 selected) 0 B queued 0 packets queued

Simple Queue <P2P>

General Advanced Statistics Traffic Total Total Statistics

Target Upload Target Download

Rate: 35.3 kbps 521.6 kbps

Packet Rate: 74 p/s 54 p/s

Upload: 35.3 kbps
Download: 521.6 kbps

Upload Packets: 74 p/s
Download Packets: 54 p/s

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
Torch

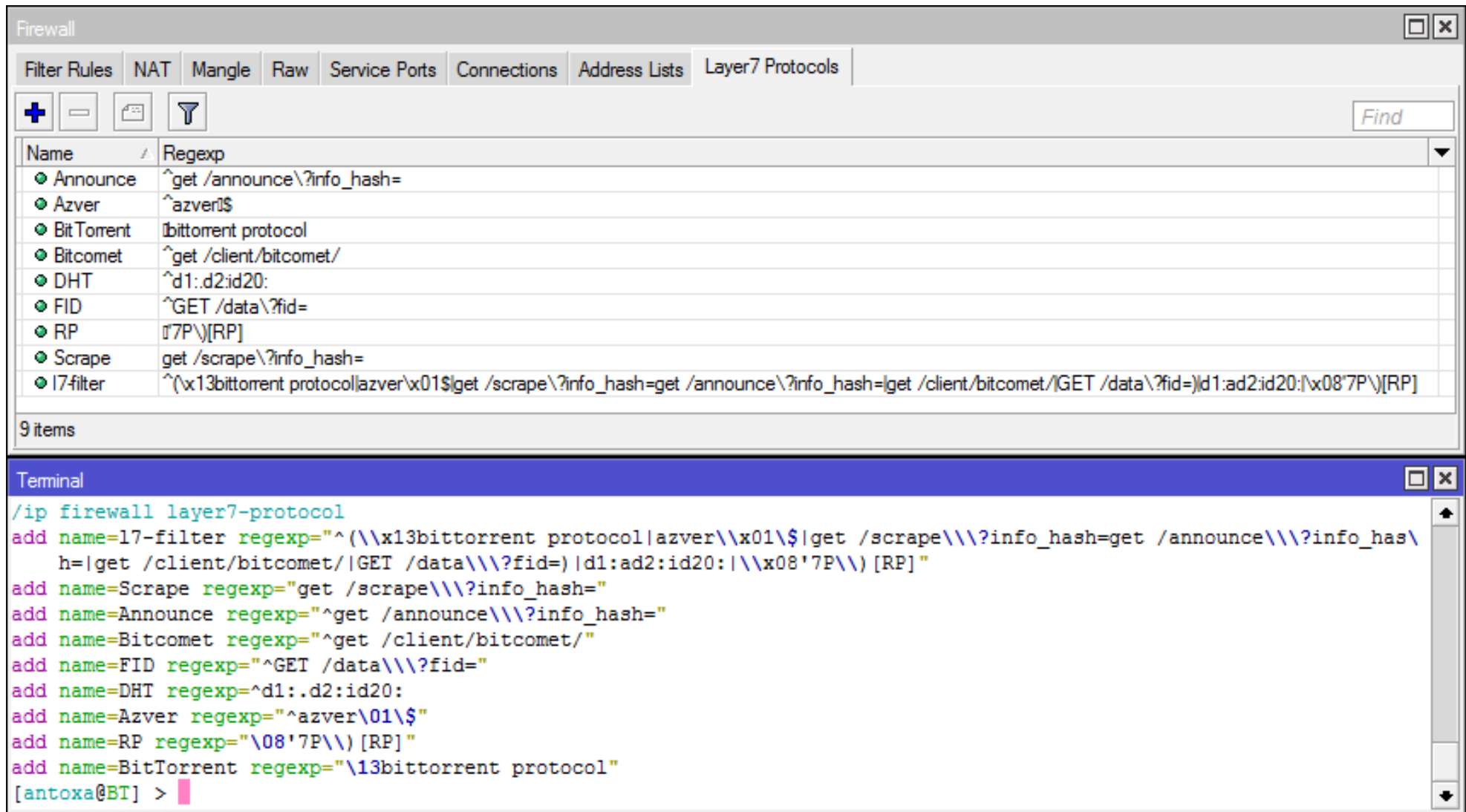
Тестирование конфигурации

№	Имя	Размер	Состояние	Дост...	Загрузка	Отдача	Время	Воспрои
1		1.45 ГБ	Загрузка 13.4 %		1021.2 КБ/s	1.2 КБ/s	21 ми...	
2		1.45 ГБ	Загрузка 7.1 %		994.9 КБ/s	1.1 КБ/s	25 ми...	
3		1.36 ГБ	Загрузка 3.1 %		353.5 КБ/s	0.7 КБ/s	55 ми...	
4		1.44 ГБ	Загрузка 3.5 %		68.6 КБ/s	25.7 КБ/s	8 ч 54 ...	
5		1.36 ГБ	Загрузка 8.4 %		694.6 КБ/s	2.9 КБ/s	33 ми...	

IP	Клиент	Флаги	%	Загрузка	Отдача	Запр...	Отдано	Загружено
[uTP]	MediaGet2 2.01.3673	d EP	100.0	135.6 КБ/s		71 0		4.57 МБ
[uTP]	MediaGet2 2.01.3731	D EP	100.0	106.8 КБ/s	0.0 КБ/s	101 0		15.6 МБ
[uTP]	MediaGet2 2.01.3673	D EP	100.0	71.4 КБ/s		94 0		2.53 МБ
[uTP]	MediaGet2 2.01.3673	D EP	100.0	70.6 КБ/s	0.1 КБ/s	127 0		23.4 МБ
	µTorrent 3.4.9	D E	100.0	58.8 КБ/s		61 0		10.1 МБ
[uTP]	µTorrent 3.5	D EP	100.0	57.7 КБ/s		50 0		3.21 МБ
[uTP]	µTorrent 3.5	D EP	100.0	52.9 КБ/s		99 0		4.34 МБ
[uTP]	µTorrent 3.5	D NEP	100.0	48.6 КБ/s		81 0		18.3 МБ
[uTP]	MediaGet2 2.01.3673	D EP	100.0	45.7 КБ/s		34 0		16.0 МБ
[uTP]	µTorrent 3.5	D EP	100.0	45.7 КБ/s		42 0		1.34 МБ
[uTP]	µTorrent 3.5	D NEP	100.0	45.6 КБ/s		11 0		6.54 МБ
[uTP]	MediaGet2 2.01.3673	D EP	100.0	34.1 КБ/s		65 0		6.62 МБ
[uTP]	MediaGet2 2.01.3727	D EP	100.0	32.8 КБ/s		70 0		9.28 МБ

DHT: 719 узлов (обновление) П: 3.3 МБ/с В: 534.0 МБ О: 37.8 КБ/с В: 7.6 МБ

RouterOS Layer7



The image shows the RouterOS Firewall configuration interface for Layer7 Protocols. The top window displays a list of 9 protocols with their respective Regexp patterns. The bottom window shows the terminal output of the configuration commands.

Name	Regexp
Announce	^get /announce\?info_hash=
Azver	^azver!\$
BitTorrent	!bittorrent protocol
Bitcomet	^get /client/bitcomet/
DHT	^d1:.d2:id20:
FID	^GET /data\?fid=
RP	!7P\)[RP]
Scrape	get /scrape\?info_hash=
l7-filter	^(\\x13bittorrent protocol azver\\x01!\$ get /scrape\?info_hash=get /announce\?info_hash= get /client/bitcomet/ GET /data\?fid=) d1:ad2:id20: \\x08'7P\)[RP]

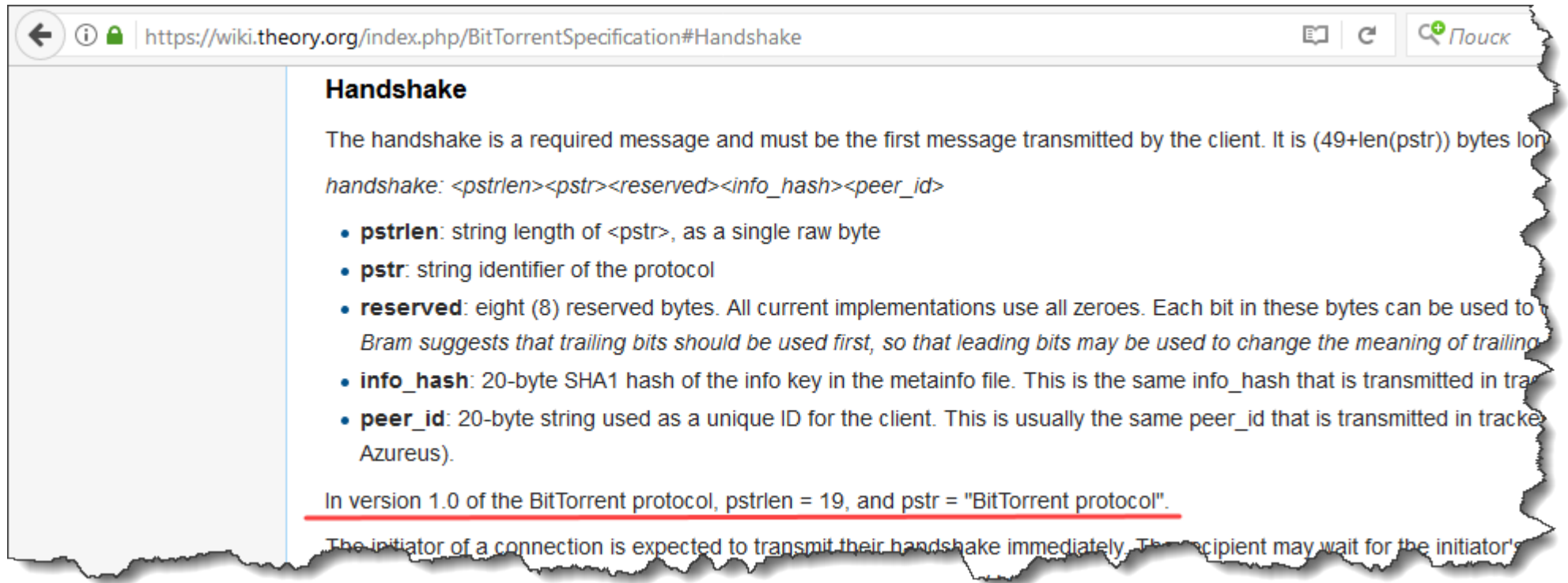
```
/ip firewall layer7-protocol
add name=l7-filter regexp="^(\\x13bittorrent protocol|azver\\x01!$|get /scrape\\?info_hash=get /announce\\?info_has
h=|get /client/bitcomet/|GET /data\\?fid=)|d1:ad2:id20:|\\x08'7P\)[RP]"
add name=Scrape regexp="get /scrape\\?info_hash="
add name=Announce regexp="^get /announce\\?info_hash="
add name=Bitcomet regexp="^get /client/bitcomet/"
add name=FID regexp="^GET /data\\?fid="
add name=DHT regexp="^d1:.d2:id20:"
add name=Azver regexp="^azver!$"
add name=RP regexp="\\x08'7P\)[RP]"
add name=BitTorrent regexp="!13bittorrent protocol"
[antoxa@BT] >
```

Определение P2P соединений и маркировка пакетов

Firewall												
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols												
#	Action	Chain	Src. Address	Dst. Address	Connection Mark	Src. Address List	Dst. Address List	Layer7 Protocol	New Packet Mark	New Connection Mark	Bytes	Packets
0	add src to address list	forward		192.168.0.0/24		lp2p-seeds		Announce			0 B	0
1	add src to address list	forward		192.168.0.0/24		lp2p-seeds		Azver			0 B	0
2	add src to address list	forward		192.168.0.0/24		lp2p-seeds		BitTorrent			1114 B	2
3	add src to address list	forward		192.168.0.0/24		lp2p-seeds		Bitcomet			0 B	0
4	add src to address list	forward		192.168.0.0/24		lp2p-seeds		DHT			314 B	2
5	add src to address list	forward		192.168.0.0/24		lp2p-seeds		FID			0 B	0
6	add src to address list	forward		192.168.0.0/24		lp2p-seeds		RP			0 B	0
7	add src to address list	forward		192.168.0.0/24		lp2p-seeds		Scrape			0 B	0
8	add dst to address list	forward	192.168.0.0/24				lp2p-seeds	Announce			0 B	0
9	add dst to address list	forward	192.168.0.0/24				lp2p-seeds	Azver			0 B	0
10	add dst to address list	forward	192.168.0.0/24				lp2p-seeds	BitTorrent			8.1 KiB	76
11	add dst to address list	forward	192.168.0.0/24				lp2p-seeds	Bitcomet			0 B	0
12	add dst to address list	forward	192.168.0.0/24				lp2p-seeds	DHT			37.3 KiB	290
13	add dst to address list	forward	192.168.0.0/24				lp2p-seeds	FID			0 B	0
14	add dst to address list	forward	192.168.0.0/24				lp2p-seeds	RP			0 B	0
15	add dst to address list	forward	192.168.0.0/24				lp2p-seeds	Scrape			0 B	0
16	mark connection	forward				p2p-seeds				p2p-cmark	22.2 MiB	24 482
17	mark connection	forward					p2p-seeds			p2p-cmark	3351.0 KiB	22 663
18	mark packet	forward			p2p-cmark				p2p-pmark		25.4 MiB	47 103

19 items

Спецификация BitTorrent



The screenshot shows a web browser window with the address bar containing the URL `https://wiki.theory.org/index.php/BitTorrentSpecification#Handshake`. The page content is titled "Handshake" and describes the handshake process in the BitTorrent protocol. It includes a list of fields in the handshake message and a note about the protocol version 1.0.

Handshake

The handshake is a required message and must be the first message transmitted by the client. It is $(49 + \text{len}(\text{pstr}))$ bytes long.

handshake: <pstrlen><pstr><reserved><info_hash><peer_id>

- **pstrlen**: string length of <pstr>, as a single raw byte
- **pstr**: string identifier of the protocol
- **reserved**: eight (8) reserved bytes. All current implementations use all zeroes. Each bit in these bytes can be used to *Bram suggests that trailing bits should be used first, so that leading bits may be used to change the meaning of trailing*
- **info_hash**: 20-byte SHA1 hash of the info key in the metainfo file. This is the same info_hash that is transmitted in tracker
- **peer_id**: 20-byte string used as a unique ID for the client. This is usually the same peer_id that is transmitted in tracker (e.g. Azureus).

In version 1.0 of the BitTorrent protocol, pstrlen = 19, and pstr = "BitTorrent protocol".

The initiator of a connection is expected to transmit their handshake immediately. The recipient may wait for the initiator's

Wireshark BitTorrent

bittorrent

No.	Time	Source	Destination	Protocol	Length	Info
145...	2017-09-23 01:11:25,685529	192.168.0.254		BitTorrent	122	Handshake
249...	2017-09-23 01:11:45,479171	192.168.0.254		BitTorrent	122	Handshake
272...	2017-09-23 01:11:49,533868	192.168.0.254		BitTorrent	122	Handshake
526...	2017-09-23 01:12:31,533770	192.168.0.254		BitTorrent	122	Handshake
636...	2017-09-23 01:12:47,656471	192.168.0.254		BitTorrent	122	Handshake

<

> Frame 14579: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
> Ethernet II, Src: QuantaCo_5d:e2:aa (08:9e:01:5d:e2:aa), Dst: Routerbo_b0:3a:7b (4c:5e:0c:b0:3a:7b)
> Internet Protocol Version 4, Src: 192.168.0.254, Dst:
> Transmission Control Protocol, Src Port: 53370, Dst Port: 6881, Seq: 1, Ack: 1, Len: 68

▼ BitTorrent

Protocol Name Length: 19
Protocol Name: BitTorrent protocol
Reserved Extension Bytes: 0000000000100005
SHA1 Hash of info dictionary: 789ad8e4a8bd69065516f16081bbec57a6a428e1
Peer ID: 2d5554333530302d8cab96267825c2a3f61ee15e

0000	4c 5e 0c b0 3a 7b 08 9e 01 5d e2 aa 08 00 45 00	L^...:{... .]....E.
0010	00 6c 57 90 40 00 80 06 00 00 c0 a8 00 fe	.lW.@...\.
0020	d0 7a 1a e1 9e 5f f1 69 d3 a9 dc 61 50 18	...z... .i...aP.
0030	01 04 c3 f6 00 00 13 42 69 74 54 6f 72 72 65 6eB itTorren
0040	74 20 70 72 6f 74 6f 63 6f 6c 00 00 00 00 00 10	t protoc ol.....
0050	00 05 78 9a d8 e4 a8 bd 69 06 55 16 f1 60 81 bb	..x..... i.U..`..
0060	ee 57 a6 a4 28 e1 2d 55 54 33 35 30 30 2d 8c ab	.W..(-U T3500-...
0070	96 26 78 25 c2 a3 f6 1e e1 5e	.&x%.... .^

DHT

- DHT (Distributed hash table – распределенная хэш-таблица) – это протокол, позволяющий битторрент-клиентам находить друг друга без использования трекера
- Клиенты с поддержкой DHT образуют общую DHT-сеть и помогают друг другу найти участников одних и тех же раздач

Спецификация DHT

- DHT запросы (Queries)
 - ping
 - find_node
 - get_peers
 - announce_peer

http://www.bittorrent.org/beps/bep_0005.html

Спецификация DHT

ping

The most basic query is a ping. "q" = "ping" A ping query has a single argument, "id" the value is a 20-byte string containing the senders node ID in network byte order. The appropriate response to a ping has a single key "id" containing the node ID of the responding node.

```
arguments: {"id" : "<querying nodes id>"}
```

```
response: {"id" : "<queried nodes id>"}
```

Example Packets

```
ping Query = {"t":"aa", "y":"q", "q":"ping", "a":{"id":"abcdefghij0123456789"}}
```

```
bencoded = d1:ad2:id20:abcdefghij0123456789e1:q4:ping1:t2:aa1:y1:qe
```

```
Response = {"t":"aa", "y":"r", "r": {"id":"mnopqrstuvwxyz123456"}}
```

```
bencoded = d1:rd2:id20:mnopqrstuvwxyz123456e1:t2:aa1:y1:re
```

Спецификация DHT

find_node

Find node is used to find the contact information for a node given its ID. "q" == "find_node" A find_node query has two arguments, "id" containing the node ID of the querying node, and "target" containing the ID of the node sought by the querier. When a node receives a find_node query, it should respond with a key "nodes" and value of a string containing the compact node info for the target node or the K (8) closest good nodes in its own routing table.

```
arguments: {"id" : "<querying nodes id>", "target" : "<id of target node>"}
```

```
response: {"id" : "<queried nodes id>", "nodes" : "<compact node info>"}
```

Example Packets

```
find_node Query = {"t":"aa", "y":"q", "q":"find_node", "a": {"id":"abcdefghij0123456789", "target":"mnopqrstuvwxyz123456789"},  
bencoded = d1:ad2:id20:abcdefghij01234567896:target20:mnopqrstuvwxyz123456e1:q9:find_node1:t2:aa1:y1:qe
```

```
Response = {"t":"aa", "y":"r", "r": {"id":"0123456789abcdefghij", "nodes": "def456..."}}
```

```
bencoded = d1:rd2:id20:0123456789abcdefghij5:nodes9:def456...e1:t2:aa1:y1:re
```

get_peers

Спецификация DHT

get_peers

Get peers associated with a torrent infohash. "q" = "get_peers" A get_peers query has two arguments, "id" containing the node ID of the querying node, and "info_hash" containing the infohash of the torrent. If the queried node has peers for the infohash, they are returned in a key "values" as a list of strings. Each string containing "compact" format peer information for a single peer. If the queried node has no peers for the infohash, a key "nodes" is returned containing the K nodes in the queried nodes routing table closest to the infohash supplied in the query. In either case a "token" key is also included in the return value. The token value is a required argument for a future announce_peer query. The token value should be a short binary string.

```
arguments: {"id" : "<querying nodes id>", "info_hash" : "<20-byte infohash of target torrent>"}
```

```
response: {"id" : "<queried nodes id>", "token" : "<opaque write token>", "values" : ["<peer 1 info string>", "<peer 2 info string>"]}
```

```
or: {"id" : "<queried nodes id>", "token" : "<opaque write token>", "nodes" : "<compact node info>"}
```

Example Packets:

```
get_peers Query = {"t":"aa", "y":"q", "q":"get_peers", "a": {"id":"abcdefghij0123456789", "info_hash":"mnopqrstuvwxyz1234567890"}, "token":"a"}  
bencoded = d1:ad2:id20:abcdefghij01234567899:info_hash20:mnopqrstuvwxyz123456e1:q9:get_peers1:t2:aa1:y1:qe
```

```
Response with peers = {"t":"aa", "y":"r", "r": {"id":"abcdefghij0123456789", "token":"a", "values": ["axje.u", "axje.u"]}, "token":"a"}  
bencoded = d1:rd2:id20:abcdefghij01234567895:token8:a:values16:axje.u6:axje.u6:token8:a
```

```
Response with closest nodes = {"t":"aa", "y":"r", "r": {"id":"abcdefghij0123456789", "token":"a", "nodes": "def456...5"}, "token":"a"}  
bencoded = d1:rd2:id20:abcdefghij01234567895:nodes9:def456...5:token8:a
```

Спецификация DHT

announce_peer

Announce that the peer, controlling the querying node, is downloading a torrent on a port. announce_peer has four arguments: "id" containing the node ID of the querying node, "info_hash" containing the infohash of the torrent, "port" containing the port as an integer, and the "token" received in response to a previous announce_peer query. The queried

port argument should be ignored and the source port of the UDP packet should be used as the peer port instead. This is useful for peers behind a NAT that may not know their external port, and supporting uTP, they accept incoming connections on the same port as the DHT port.

```
arguments: {"id" : "<querying nodes id>",
            "implied_port": <0 or 1>,
            "info_hash" : "<20-byte infohash of target torrent>",
            "port" : <port number>,
            "token" : "<opaque token>"}

response: {"id" : "<queried nodes id>"}
```

Example Packets:

```
announce_peers Query = {"t":"aa", "y":"q", "q":"announce_peer", "a": {"id":"abcdefghij0123456789", "implied_port": 1},
                        "i": "info_hash20:", "p": "port16:", "t": "token8:"}
bencoded = d1:ad2:id20:abcdefghij01234567899:info_hash20:  
mnopqrstuvwxyz1234564:port16881e5:token8:aoeusnthel:q13:announce_peer1:t2:aa1:y1:qe

Response = {"t":"aa", "y":"r", "r": {"id":"mnopqrstuvwxyz123456"}}
bencoded = d1:rd2:id20:mnopqrstuvwxyz123456e1:t2:aa1:y1:re
```


Wireshark DHT

bt-dht

No.	Time	Source	Destination	Protocol	Length	Info
246	2017-09-23 01:59:15,544592	192.168.0.254		BT-DHT	145	BitTorrent DHT Protocol
249	2017-09-23 01:59:15,700258		192.168.0.254	BT-DHT	145	BitTorrent DHT Protocol
250	2017-09-23 01:59:15,732819	192.168.0.254		BT-DHT	121	BitTorrent DHT Protocol reply=0 nodes
251	2017-09-23 01:59:15,870670		192.168.0.254	BT-DHT	121	BitTorrent DHT Protocol reply=0 nodes
307	2017-09-23 01:59:22,560497	192.168.0.254		BT-DHT	145	BitTorrent DHT Protocol
371	2017-09-23 01:59:29,553829	192.168.0.254		BT-DHT	145	BitTorrent DHT Protocol

> Frame 249: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
> Ethernet II, Src: Routerbo_b0:3a:7b (4c:5e:0c:b0:3a:7b), Dst: QuantaCo_5d:e2:aa (08:9e:01:5d:e2:aa)
> Internet Protocol Version 4, Src: , Dst: 192.168.0.254
> User Datagram Protocol, Src Port: 52525, Dst Port: 8080
▼ BitTorrent DHT Protocol
 > Request arguments: Dictionary...
 > Request type: find_node
 > Transaction ID: bc050000
 > Version: 5554ab8c
 > Message type: Request

```
0000 08 9e 01 5d e2 aa 4c 5e 0c b0 3a 7b 08 00 45 00  ...]..L^ ...{..E.  
0010 00 83 7f ea 00 00 64 11 f1 b8 c0 a8  ....d. ..."M...  
0020 00 fe cd 2d 1f 90 00 6f f7 d4 64 31 3a 61 64 32  ...-...o .d1:ad2  
0030 3a 69 64 32 30 3a dc 29 f9 ba a2 ef 2d 73 50 9a  :id20:.) .....sP.  
0040 4e eb 98 f6 d7 b3 51 d3 6d 4d 36 3a 74 61 72 67  N.....Q. mM6:targ  
0050 65 74 32 30 3a dc 29 ff 94 00 00 6c 70 00 00 5d  et20:.) ...lp..]  
0060 f2 00 00 28 61 00 00 60 60 65 31 3a 71 39 3a 66  ...(a..` `e1:q9:f  
0070 69 6e 64 5f 6e 6f 64 65 31 3a 74 34 3a bc 05 00  ind_node 1:t4:...  
0080 00 31 3a 76 34 3a 55 54 ab 8c 31 3a 79 31 3a 71  .1:v4:UT ..1:y1:q  
0090 65 e
```

Тестирование конфигурации

№	Имя	Размер	Состояние	Дост...	Загрузка	Отдача	Время	Воспров
1		1.45 ГБ	Загрузка 26.4 %		820.3 КБ/s	1.3 КБ/s	25 ми...	
2		1.45 ГБ	Загрузка 18.3 %		1.1 МБ/s	2.6 КБ/s	18 ми...	
3		1.36 ГБ	Загрузка 12.9 %		563.9 КБ/s	0.8 КБ/s	33 ми...	
4		1.44 ГБ	Загрузка 9.1 %		230.6 КБ/s	12.2 КБ/s	9 ч 21 ...	
5		1.36 ГБ	Загрузка 21.1 %		921.6 КБ/s	2.0 КБ/s	21 ми...	

IP	Клиент	Флаги	%	Загрузка	Отдача	Запр...	Отдано	Загружено
[uTP]	MediaGet2 2.01.3731	D XEP	100.0	184.7 КБ/s	0.3 КБ/s	64 0		1.85 МБ
[uTP]	MediaGet2 2.01.3725	D HXEP	100.0	28.7 КБ/s		17 0		480 КБ
	µTorrent 3.1.3	D HXE	100.0	13.1 КБ/s		4 0		144 КБ
	µTorrent 3.4.2	D HE	100.0	2.5 КБ/s		4 0		16.0 КБ
[uTP]	µTorrent 3.5	D HXEP	100.0	0.6 КБ/s		2 0		48.0 КБ
	µTorrent 3.5	d HXE	100.0	0.1 КБ/s	0.1 КБ/s			144 КБ
[uTP]	µTorrent 3.5	d EP	100.0					
[uTP]	µTorrent 3.5	d HXEP	100.0					
	µTorrent 3.4.1	d HXE	100.0					
[uTP]	µTorrent 3.5	d HXEP	100.0					
[uTP]	µTorrent 3.0	d XEP	100.0					
[uTP]	µTorrent 3.5	d XEP	100.0					176 КБ
[uTP]	µTorrent 3.5	d HEP	100.0					16.0 КБ

DHT: 733 узлов	П: 3.6 МБ/с В: 644.1 МБ	О: 22.8 КБ/с В: 7.6 МБ
----------------	-------------------------	------------------------

Флаги µTorrent

- D – В данный момент скачивается (заинтересован и доступен)
- d – Ваш клиент хочет скачать, но пир не хочет отдавать (заинтересован, но занят)
- U – В данный момент отдается (заинтересован и доступен)
- u – Пир хочет у Вас скачать, но Вы еще не отдаете (заинтересован, но занят)
- E – Пир использует шифрование протокола (весь трафик)
- e – Пир использует шифрование протокола (при соединении)
- X – Пир был добавлен через обмен пирами (Peer Exchange, PEX)
- H – Пир был добавлен через DHT-сеть
- h – Пир подключился с использованием UDP-hole punching
- P – Пир подключился через uTP
- I – Входящее подключение
- S – Пир "уснул" (нулевая активность)
- O – Пир освобождается и скоро будет готов раздавать
- K – Пир хочет Вам отдать, но Вы не хотите скачивать
- ? – Ваш клиент готов отдать, но пир не хочет получать
- L – Локальный пир (был найден через "Поиск локальных пиров")
- F – Пир был замечен в передаче "битого" куска (не обязательно плохой пир, просто был вовлечен)

BEP – BitTorrent Enhancement Proposal

- DHT – Distributed Hash Table – распределённая хеш-таблица
- PEX – Peer EXchange – расширение BitTorrent-протокола для обмена списками участников
- μ TP – Micro Transport Protocol – транспортный протокол с контролем доставки (подобно TCP) на основе протокола UDP

http://www.bittorrent.org/beps/bep_0000.html

Спецификация PEX

← ⓘ bittorrent.org/beps/bep_0010.html

handshake message

The payload of the handshake message is a bencoded dictionary. All items in the dictionary are optional. Names should be ignored by the client. All parts of the dictionary are case sensitive. This is the defined dictionary:

name	description
m	Dictionary of supported extension messages which maps names of extensions to their extended message ID for each extension message. The only required extension is the peer ID extension.
p	Peer ID
v	Version

and in the encoded form:

```
d1:md11:LT_metadata1e6:uT_PEXi2ee1:pi6881e1:v13:\xc2\x5Torrent 1.2e
```

To make sure the extension names do not collide by mistake, they should be prefixed with the two (or one) characters that is used to identify the client that introduced the extension. This applies to both the name

Wireshark PEX

Apply a display filter ... <Ctrl-/>

Packet bytes ▾ Narrow & Wide ▾ Case sensitive String ▾ ut_pex

No.	Time	Source	Destination	Protocol	Length	Info
2207	2017-09-23 11:27:08,595350	192.168.0.1	192.168.0.254	TCP	1032	8291 → 49861 [PSH,
2208	2017-09-23 11:27:08,595362	192.168.0.254	192.168.0.1	TCP	54	49861 → 8291 [ACK]
2209	2017-09-23 11:27:08,595489		192.168.0.254	TCP	585	61384 → 57659 [PSH,
2210	2017-09-23 11:27:08,595521	192.168.0.254		TCP	312	57659 → 61384 [PSH,
2211	2017-09-23 11:27:08,595826		192.168.0.254	BT-uTP	62	uTorrent Transport
2212	2017-09-23 11:27:08,596155	192.168.0.254		UDP	138	8080 → 2710 Len=96

<

> Internet Protocol Version 4, Src: , Dst: 192.168.0.254

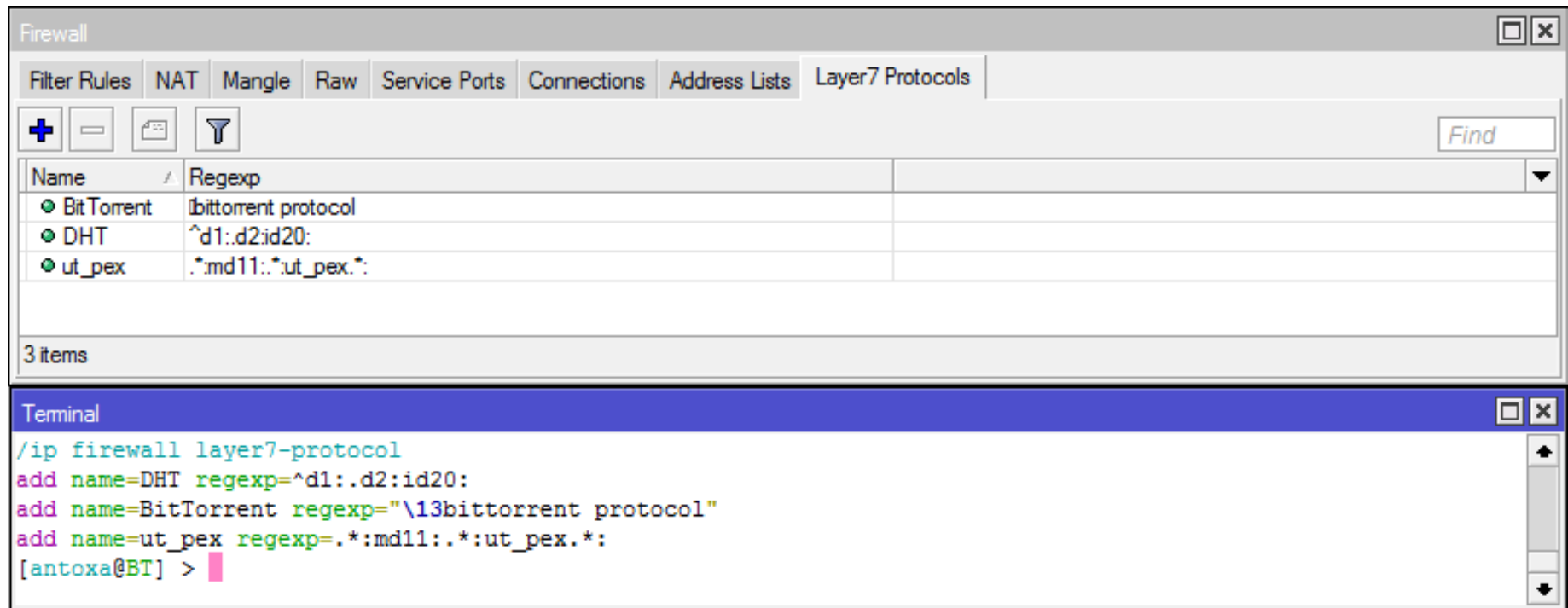
▼ Transmission Control Protocol, Src Port: 61384, Dst Port: 57659, Seq: 110, Ack: 188, Len: 531

Source Port: 61384

Destination Port: 57659

```
0020  00 fe ef c8 e1 3b 15 75 a4 b1 01 9f 08 c3 50 18  .....;.u .....P.
0030  01 02 a8 05 00 00 bd 30 f9 0b 9e d1 9d c1 93 31  .....0 .....1
0040  32 3a 63 6f 6d 70 6c 65 74 65 5f 61 67 6f 69 32  2:complete_agoi2
0050  65 31 3a 6d 64 31 31 3a 75 70 6c 6f 61 64 5f 6f  el:md11:upload_o
0060  6e 6c 79 69 33 65 31 31 3a 6c 74 5f 64 6f 6e 74  nlyi3e11 :lt_dont
0070  68 61 76 65 69 37 65 31 32 3a 75 74 5f 68 6f 6c  havei7e1 2:ut_hol
0080  65 70 75 6e 63 68 69 34 65 31 31 3a 75 74 5f 6d  epunchi4 e11:ut_m
0090  65 74 61 64 61 74 61 69 32 65 36 3a 75 74 5f 70  etadatai 2e6:ut_p
00a0  65 78 69 31 65 31 30 3a 75 74 5f 63 6f 6d 6d 65  ex:le10: ut_comme
00b0  6e 74 69 36 65 65 31 33 3a 6d 65 74 61 64 61 74  nti6ee13 :metadat
00c0  61 5f 73 69 7a 65 69 31 34 39 35 32 65 31 3a 70  a_sizei1 4952e1:p
00d0  69 36 31 33 38 34 65 34 3a 72 65 71 71 69 32 35  i61384e4 :reqqi25
00e0  35 65 31 3a 76 31 33 3a ce bc 54 6f 72 72 65 6e  5e1:v13: ..Torren
00f0  74 20 33 2e 35 32 3a 79 70 69 35 37 36 35 39 65  t 3.52:ypi57659e
0100  36 3a 79 6f 75 72 69 70 34 3a 5b 87 c0 d7 65 00  6:yourip 4:[...e.
```

RouterOS Layer7



The image shows two windows from the RouterOS interface. The top window is titled "Firewall" and has tabs for "Filter Rules", "NAT", "Mangle", "Raw", "Service Ports", "Connections", "Address Lists", and "Layer7 Protocols". The "Layer7 Protocols" tab is active, showing a table with three entries:

Name	Regexp
Bit Torrent	bittorrent protocol
DHT	^d1:.d2:id20:
ut_pex	.*:md11:.*:ut_pex.*:

Below the table, it says "3 items". The bottom window is titled "Terminal" and shows the following commands being executed:

```
/ip firewall layer7-protocol
add name=DHT regexp=^d1:.d2:id20:
add name=BitTorrent regexp="\13bittorrent protocol"
add name=ut_pex regexp=.*:md11:.*:ut_pex.*:
[antoxa@BT] >
```

Определение P2P соединений и маркировка пакетов

Src. Address	Dst. Address	Protocol	Connection Mark	Src. Address List	Dst. Address List	Layer7 Protocol	New Packet Mark	New Connection Mark	Bytes	Packets
192.168.0.0/24	192.168.0.0/24	6 (tcp)		!p2p-seeds		ut_pex			8.6 KB	13
192.168.0.0/24	192.168.0.0/24	6 (tcp)		!p2p-seeds		BitTorrent			625 B	10
192.168.0.0/24	192.168.0.0/24	17 (udp)		!p2p-seeds		DHT			0 B	0
192.168.0.0/24		6 (tcp)			!p2p-seeds	ut_pex			1081 B	3
192.168.0.0/24		6 (tcp)			!p2p-seeds	BitTorrent			4104 B	38
192.168.0.0/24		17 (udp)			!p2p-seeds	DHT			16.9 KB	132
				p2p-seeds				p2p-cmark	2686.2 ...	3 098
					p2p-seeds			p2p-cmark	207.9 KB	2 842
			p2p-cmark				p2p-pmark		2894.9 ...	5 945

Тестирование конфигурации

№	Имя	Размер	Состояние	Дост...	Загрузка	Отдача	Время	Воспро
1		1.45 ГБ	Загрузка 29.3 %		446.1 КБ/с	0.6 КБ/с	2 ч 3 ...	
2		1.45 ГБ	Загрузка 21.3 %		8.2 КБ/с	0.2 КБ/с	1 д 6 ч	
3		1.36 ГБ	Загрузка 15.7 %		601.4 КБ/с	1.1 КБ/с	53 ми...	
4		1.44 ГБ	Загрузка 11.5 %		801.3 КБ/с	1.7 КБ/с	1 ч 56 ...	
5		1.36 ГБ	Загрузка 24.2 %		15.4 КБ/с	0.3 КБ/с	22 ч 4...	

IP	Клиент	Флаги	%	Загрузка	Отдача	Запр...	Отдано	Загружено
8 [uTP]	µTorrent 3.5	D EP	100.0	304.5 КБ/с	0.3 КБ/с	55 0		4.26 МБ
1 [uTP]	Transmission 2.92	D EP	100.0	217.8 КБ/с	0.1 КБ/с	25 0		4.28 МБ
13 [uTP]	µTorrent Mac 1.8.7	D P	100.0	71.8 КБ/с	0.1 КБ/с	158 0		6.71 МБ
188 [uTP]	MediaGet2 2.01.3725	D P	100.0	2.8 КБ/с		75 0		144 КБ
172 [uTP]	Zona 2.0.0.6	D P	100.0	1.7 КБ/с		88 0		256 КБ
10 [uTP]	Zona 2.0.0.6	D P	100.0	0.9 КБ/с		14 0		48.0 КБ
25 [uTP]	Zona 2.0.0.6	D P	100.0	0.6 КБ/с		18 0		
8	Zona 2.0.0.6	D	100.0	0.5 КБ/с	0.1 КБ/с	121 0		
34 [uTP]	Zona 2.0.0.6	D P	100.0	0.1 КБ/с		126 0		
226 [uTP]	µTorrent 3.5	D P	100.0	0.0 КБ/с		2 0		32.0 КБ
	Zona 2.0.0.6	d	100.0					32.0 КБ
	Zona 2.0.0.6	D	100.0			2 0		
	MediaGet2 2.01.3684	d	100.0					2.71 МБ

DHT: 743 узлов П: 1.7 МБ/с В: 856.0 МБ О: 5.3 КБ/с В: 9.3 МБ

μTP – Micro Transport Protocol

- транспортный протокол с контролем доставки (подобно TCP) на основе протокола UDP
- предназначен для более быстрого скачивания, так как работает по протоколу UDP
- ускорение достигается за счёт того, что торрент-клиент берёт на себя выполнение нужных функций, отсутствующих в UDP, например, клиент перепроверяет целостность данных и, если блок неверен, скачивает его заново

Спецификация μ TP

← ⓘ | bittorrent.org/beps/bep_0029.html

header format

version 1 header:

0	4	8	16	24	32
type	ver	extension	connection_id		
timestamp_microseconds					
timestamp_difference_microseconds					
wnd_size					
seq_nr			ack_nr		

All fields are in network byte order (big endian).

version

This is the protocol version. The current version is 1.

connection_id

Спецификация μTP

← ⓘ bittorrent.org/beps/bep_0029.html

type

The type field describes the type of packet.

It can be one of:

- ST_DATA = 0**
regular data packet. Socket is in connected state and has data to send. An ST_DATA p
- ST_FIN = 1**
Finalize the connection. This is the last packet. It closes the connection, similar to T
never have a sequence number greater than the sequence number in this packet. The
number as eof_pkt. This lets the socket wait for packets that might still be missing an
receiving the ST_FIN packet.
- ST_STATE = 2**
State packet. Used to transmit an ACK with no data. Packets that don't include any pay
seq_nr.
- ST_RESET = 3**
Terminate connection forcefully. Similar to TCP RST flag. The remote host does not h
connection. It is stale and should be terminated.
- ST_SYN = 4**
Connect SYN. Similar to TCP SYN flag, this packet initiates a connection. The sequenc
connection ID is initialized to a random number. The syn packet is special, all subsequ
connection (except for re-sends of the ST_SYN) are sent with the connection ID

Wireshark μTP

bt-utp

No.	Time	Source	Destination	Protocol	Length	Info
94	2017-09-23 12:21:41,458560	192.168.0.254		BT-uTP	62	uTorrent Transport Protocol Type: Syn
100	2017-09-23 12:21:41,460202	192.168.0.254		BT-uTP	62	uTorrent Transport Protocol Type: Syn
102	2017-09-23 12:21:41,460770	192.168.0.254		BT-uTP	62	uTorrent Transport Protocol Type: Syn
133	2017-09-23 12:21:41,586982			BT-uTP	62	uTorrent Transport Protocol Type: State
135	2017-09-23 12:21:41,587442	192.168.0.254		BT-uTP	130	uTorrent Transport Protocol Type: Data
199	2017-09-23 12:21:42,478502	192.168.0.254		BT-uTP	62	uTorrent Transport Protocol Type: Syn

> Frame 102: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
> Ethernet II, Src: QuantaCo_5d:e2:aa (08:9e:01:5d:e2:aa), Dst: Routerbo_b0:3a:7b (4c:5e:0c:b0:3a:7b)
> Internet Protocol Version 4, Src: 192.168.0.254, Dst: .182
> User Datagram Protocol, Src Port: 8080, Dst Port: 63581
v uTorrent Transport Protocol V1 (20 bytes)
.... 0001 = Version: 1
0100 = Type: Syn (4)
Next Extension Type: No Extension (0)
Connection ID: 15275
Timestamp Microseconds: 3054226039
Timestamp Difference Microseconds: 0
Windows Size: 1048576
Sequence number: 24050
ACK number: 0

```
0000 4c 5e 0c b0 3a 7b 08 9e 01 5d e2 aa 08 00 45 00  L^.:{. .]....E.  
0010 00 30 35 67 00 00 80 11 00 00 00 a8 00 fe d4 4a  .05g.... .J  
0020 ca b6 1f 90 f8 5d 00 1c 60 d5 41 00 3b ab b6 0b  ....].. ^.A.;...  
0030 ca 77 00 00 00 00 10 00 00 5d f2 00 00  .w..... .]...
```

RouterOS Layer7

The image shows a screenshot of the RouterOS Firewall configuration interface, specifically the Layer7 Protocols tab. The window displays a list of 7 items, each with a Name and a Regexp. Below the list, a terminal window shows the commands used to create these protocols.

Name	Regexp
μTP_FIN	^f .{2}.{4}.{4}.{4}.{2}.{2}
μTP_RESET	^r .{2}.{4}.{4}.{4}.{2}.{2}
μTP_STATE	^s .{2}.{4}.{4}.{4}.{2}.{2}
μTP_SYN	^A .{2}.{4}.{4}.{4}.{2}.{2}
BitTorrent	!bittorrent protocol
DHT	^d1:.d2:id20:
ut_pex	.*:md11:.*:ut_pex.*:

```
/ip firewall layer7-protocol
add name=DHT regexp=^d1:.d2:id20:
add name=BitTorrent regexp="!bittorrent protocol"
add name=ut_pex regexp=.*:md11:.*:ut_pex.*:
add name="\B5TP_FIN" regexp="^f\00.{2}.{4}.{4}.{4}.{2}.{2}"
add name="\B5TP_STATE" regexp="^s\00.{2}.{4}.{4}.{4}.{2}.{2}"
add name="\B5TP_RESET" regexp="^r\00.{2}.{4}.{4}.{4}.{2}.{2}"
add name="\B5TP_SYN" regexp="^A\00.{2}.{4}.{4}.{4}.{2}.{2}"
[antoxa@BT] >
```

Определение Р2Р соединений и маркировка пакетов

Reset Counters

Src. Address	Dst. Address	Protocol	Connection Mark	Src. Address List	Dst. Address List	Layer7 Protocol	New Packet Mark	New Connection Mark	Bytes	Packets
	192.168.0.0/24	6 (tcp)		!p2p-seeds		ut_pex			0 B	0
	192.168.0.0/24	6 (tcp)		!p2p-seeds		BitTorrent			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		DHT			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		μTP_FIN			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		μTP_RESET			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		μTP_STATE			0 B	0
	192.168.0.0/24	17 (udp)		!p2p-seeds		μTP_SYN			0 B	0
192.168.0.0/24		6 (tcp)			!p2p-seeds	ut_pex			0 B	0
192.168.0.0/24		6 (tcp)			!p2p-seeds	BitTorrent			108 B	1
192.168.0.0/24		17 (udp)			!p2p-seeds	DHT			739.5 KiB	5 771
192.168.0.0/24		17 (udp)			!p2p-seeds	μTP_FIN			0 B	0
192.168.0.0/24		17 (udp)			!p2p-seeds	μTP_SYN			151.5 KiB	3 232
192.168.0.0/24		17 (udp)			!p2p-seeds	μTP_STATE			0 B	0
192.168.0.0/24		17 (udp)			!p2p-seeds	μTP_RESET			0 B	0
				p2p-seeds				p2p-cmark	234.3 ...	331 640
					p2p-seeds			p2p-cmark	33.1 MiB	317 270
			p2p-cmark				p2p-pmark		267.1 ...	646 558

Тестирование конфигурации

№	Имя	Размер	Состояние	Дост...	Загрузка	Отдача	Время	Воспро
1		1.45 ГБ	Загрузка 34.2 %		18.3 КБ/с	0.5 КБ/с	1 д 6 ч	
2		1.45 ГБ	Загрузка 27.4 %		10.0 КБ/с	0.3 КБ/с	1 д 1 ч	
3		1.36 ГБ	Загрузка 22.4 %		16.5 КБ/с	0.1 КБ/с	20 ч 1...	
4		1.44 ГБ	Загрузка 21.1 %		271.6 КБ/с	5.9 КБ/с	2 ч 6 ...	
5		1.36 ГБ	Загрузка 32.1 %		8.0 КБ/с	0.1 КБ/с	1 д 6 ч	

IP	Клиент	Флаги	%	Загрузка	Отдача	Запр...	Отдано	Загружено
...:35de [uTP]	Torrent 2.2.1	D IeP	100.0	270.0 КБ/с	0.3 КБ/с	67 0		59.0 МБ
	µTorrent 1.8.2	D X	100.0	0.2 КБ/с		2 0	32.0 КБ	16.0 КБ
	Vuze 5.7.5.0	D XP	100.0	0.2 КБ/с		2 0		240 КБ
	µTorrent 3.5	DS HXP	100.0	0.2 КБ/с		1 0		880 КБ
	Transmission 2.84	D XE	100.0	0.2 КБ/с		2 0		176 КБ
	Zona 2.0.0.6	D HX	100.0	0.1 КБ/с		4 0		496 КБ
	µTorrent 3.5	d XeP	100.0	0.1 КБ/с				
	µTorrent 3.2	D H	100.0	0.1 КБ/с		2 0		32.0 КБ
	µTorrent 3.5	d IXP	100.0					64.0 КБ
	µTorrent 3.5	d IXeP	100.0					512 КБ
	µTorrent 3.5	d IXP	100.0					64.0 КБ
	µTorrent 3.5	d IP	100.0					
	µTorrent/3.5.0.0	I	0.0					

DHT: 731 узлов (обновление) П: 309.0 КБ/с В: 1.3 ГБ О: 12.9 КБ/с В: 21.2 МБ

Teredo

- Teredo – сетевой протокол, предназначенный для передачи IPv6 пакетов через сети IPv4, путём их инкапсуляции в UDP-дейтаграммы
- Использует UDP порт 3544

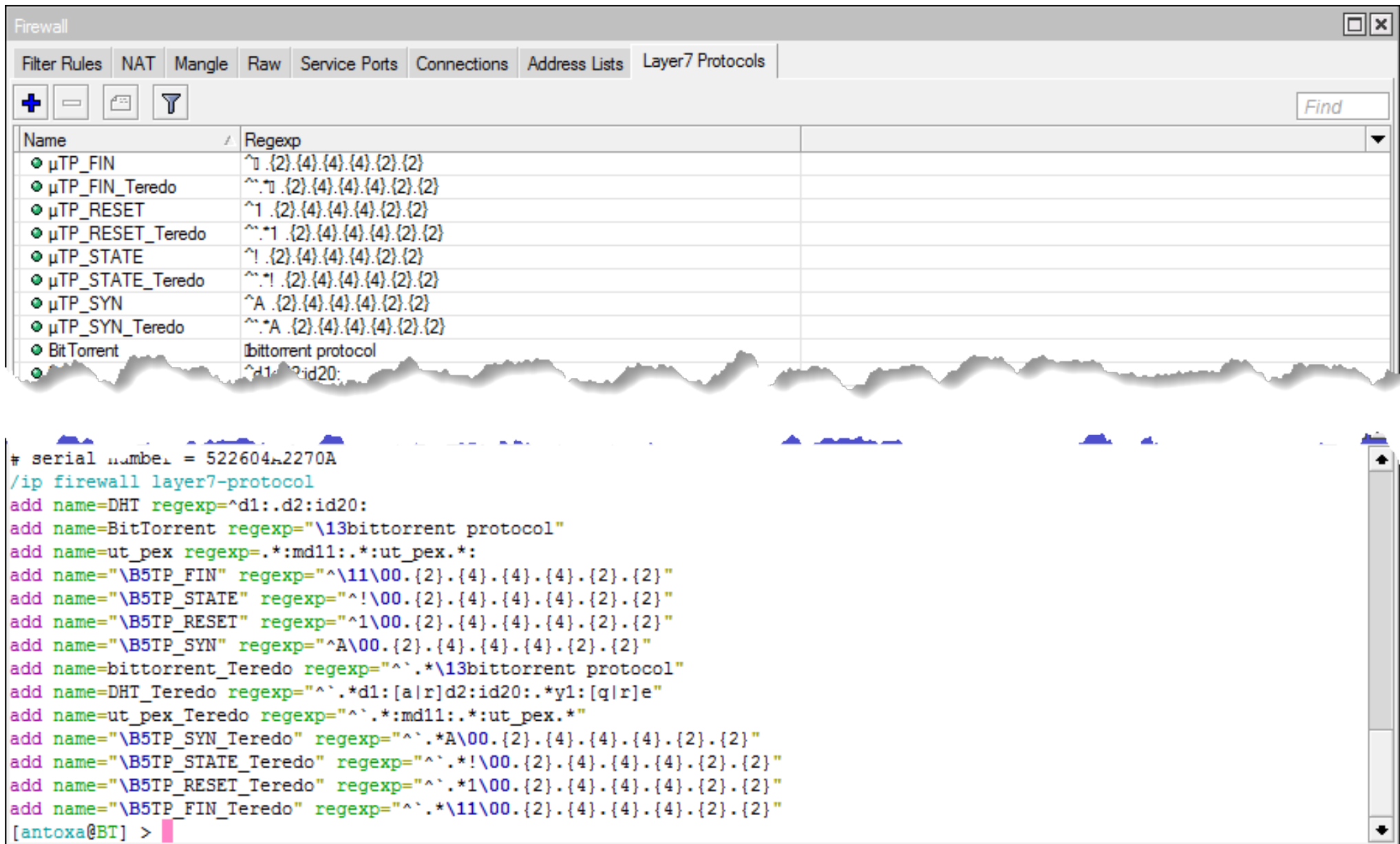
Wireshark Teredo

No.	Time	Source	Destination	Protocol	Length	Info
7985	2017-09-23 13:54:10,384082	...	2001:0:4137:9e76:382...	BT-uTP	120	uTorrent Transport Protocol Type: Syn
7986	2017-09-23 13:54:10,384436	2001:0:4137:9e76:382...	...	BT-uTP	110	uTorrent Transport Protocol Type: State
7990	2017-09-23 13:54:10,390710	...	2001:0:4137:9e76:382...	TCP	114	14434 → 8080 [SYN] Seq=0 Win=8192 Len=0 MSS=144
7991	2017-09-23 13:54:10,391020	2001:0:4137:9e76:382...	...	TCP	114	8080 → 14434 [SYN, ACK] Seq=0 Ack=1 Win=8192
8034	2017-09-23 13:54:10,576081	...	2001:0:4137:9e76:382...	TCP	102	14434 → 8080 [ACK] Seq=1 Ack=1 Win=65792 Len=0
8039	2017-09-23 13:54:10,578168	...	2001:0:4137:9e76:382...	TCP	205	14434 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=65792

> Frame 7985: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
> Ethernet II, Src: Routerbo_b0:3a:7b (4c:5e:0c:b0:3a:7b), Dst: QuantaCo_5d:e2:aa (08:9e:01:5d:e2:aa)
> Internet Protocol Version 4, Src: ..., Dst: 192.168.0.254
> User Datagram Protocol, Src Port: 3545, Dst Port: 49340
Teredo IPv6 over UDP tunneling
> Internet Protocol Version 6, Src: ..., Dst: 2001:0:4137:9e76:3829:fbfc:a478:3f28
> User Datagram Protocol, Src Port: 14232, Dst Port: 8080
uTorrent Transport Protocol V1 (30 bytes)
.... 0001 = Version: 1
0100 = Type: **Syn (4)**

```
0000 08 9e 01 5d e2 aa 4c 9e 0c b0 3a 7b 08 00 45 00 ...].L^ ...{..E.  
0010 00 6a 69 8c 00 00 34 11 2e 20 d8 42 54 ee c0 a8 .ji...4. . .BT...  
0020 00 fe 0d d9 c0 bc 00 56 d0 6d 60 00 00 00 26 .....V .m`....&  
0030 11 78 )00 d1 67 ee cc .x*.s.$ . .g....  
0040 35 de 20 01 00 00 41 37 9e 76 38 29 fb fc a4 78 5. ...A7 .v8)...x  
0050 3f 28 37 98 1f 90 00 26 96 60 41 02 50 86 52 f9 ?(7....& .`A.P.R.  
0060 84 a0 00 00 00 00 00 38 00 00 64 17 00 00 08 .....8 ..d....  
0070 00 00 00 00 00 00 00 00 .....
```

RouterOS Layer7



The image shows the RouterOS Firewall configuration interface for Layer7 Protocols. The top part is a graphical view with a table of protocols, and the bottom part is a terminal window showing the configuration commands.

Name	Regexp
μTP_FIN	^!\{2}\{4}\{4}\{4}\{2}\{2}
μTP_FIN_Teredo	^^!\{2}\{4}\{4}\{4}\{2}\{2}
μTP_RESET	^!\{2}\{4}\{4}\{4}\{2}\{2}
μTP_RESET_Teredo	^^!\{2}\{4}\{4}\{4}\{2}\{2}
μTP_STATE	^!\{2}\{4}\{4}\{4}\{2}\{2}
μTP_STATE_Teredo	^^!\{2}\{4}\{4}\{4}\{2}\{2}
μTP_SYN	^A\{2}\{4}\{4}\{4}\{2}\{2}
μTP_SYN_Teredo	^^A\{2}\{4}\{4}\{4}\{2}\{2}
BitTorrent	bittorrent protocol
DHT	^d1:.d2:id20:

```
# serial number = 522604A2270A
/ip firewall layer7-protocol
add name=DHT regexp=^d1:.d2:id20:
add name=BitTorrent regexp="\|bittorrent protocol"
add name=ut_pex regexp=.*:md11:.*:ut_pex.*:
add name="\B5TP_FIN" regexp="^!\1\00.\{2}\{4}\{4}\{4}\{2}\{2}"
add name="\B5TP_STATE" regexp="^!\00.\{2}\{4}\{4}\{4}\{2}\{2}"
add name="\B5TP_RESET" regexp="^!\00.\{2}\{4}\{4}\{4}\{2}\{2}"
add name="\B5TP_SYN" regexp="^A\00.\{2}\{4}\{4}\{4}\{2}\{2}"
add name=bittorrent_Teredo regexp="^^.*\|bittorrent protocol"
add name=DHT_Teredo regexp="^^.*d1:[a|r]d2:id20:.*y1:[q|r]e"
add name=ut_pex_Teredo regexp="^^.*:md11:.*:ut_pex.*"
add name="\B5TP_SYN_Teredo" regexp="^^.*A\00.\{2}\{4}\{4}\{4}\{2}\{2}"
add name="\B5TP_STATE_Teredo" regexp="^^.*!\00.\{2}\{4}\{4}\{4}\{2}\{2}"
add name="\B5TP_RESET_Teredo" regexp="^^.*!\00.\{2}\{4}\{4}\{4}\{2}\{2}"
add name="\B5TP_FIN_Teredo" regexp="^^.*!\1\00.\{2}\{4}\{4}\{4}\{2}\{2}"
[antoxa@BT] >
```

Определение P2P соединений и маркировка пакетов

Src. Address	Dst. Address	Protocol	Connection Mark	Src. Address List	Dst. Address List	Layer7 Protocol	New Packet Mark	New Connection Mark	Bytes	Packets
	192.168.0.0/24	6 (tcp)		lp2p-seeds		ut_pex			0 B	0
	192.168.0.0/24	17 (udp)		lp2p-seeds		ut_pex_Teredo			0 B	0
	192.168.0.0/24	6 (tcp)		lp2p-seeds		BitTorrent			0 B	0
	192.168.0.0/24	17 (udp)		lp2p-seeds		μTP_STATE			0 B	0
	192.168.0.0/24	17 (udp)		lp2p-seeds		μTP_STATE_Teredo			0 B	0
	192.168.0.0/24	17 (udp)		lp2p-seeds		μTP_SYN			1110 B	23
	192.168.0.0/24	17 (udp)		lp2p-seeds		μTP_SYN_Teredo			80 B	1
192.168.0.0/24		6 (tcp)			lp2p-seeds	ut_pex			0 B	0
192.168.0.0/24		17 (udp)			lp2p-seeds	ut_pex_Teredo			0 B	0
192.168.0.0/24		6 (tcp)			lp2p-seeds	BitTorrent			756 B	7
192.168.0.0/24		17 (udp)			lp2p-seeds	BitTorrent_Teredo			0 B	0
192.168.0.0/24		17 (udp)			lp2p-seeds	DHT			2838.2 ...	22 140
192.168.0.0/24		17 (udp)			lp2p-seeds	DHT_Teredo			0 B	0
192.168.0.0/24		17 (udp)			lp2p-seeds	μTP_FIN			0 B	0
192.168.0.0/24		17 (udp)			lp2p-seeds	μTP_FIN_Teredo			572 B	7
192.168.0.0/24		17 (udp)			lp2p-seeds	μTP_SYN			333.5 KiB	7 115
192.168.0.0/24		17 (udp)			lp2p-seeds	μTP_SYN_Teredo			5.3 KiB	68
192.168.0.0/24		17 (udp)			lp2p-seeds	μTP_STATE			96 B	2
192.168.0.0/24		17 (udp)			lp2p-seeds	μTP_STATE_Teredo			0 B	0
192.168.0.0/24		17 (udp)			lp2p-seeds	μTP_RESET			0 B	0
192.168.0.0/24		17 (udp)			lp2p-seeds	μTP_RESET_Teredo			0 B	0
				p2p-seeds				p2p-cmark	1725.6 ...	3 595 5...
					p2p-seeds			p2p-cmark	1700.7 ...	3 612 7...
			p2p-cmark				p2p-pmark		1732.6 ...	3 640 2...

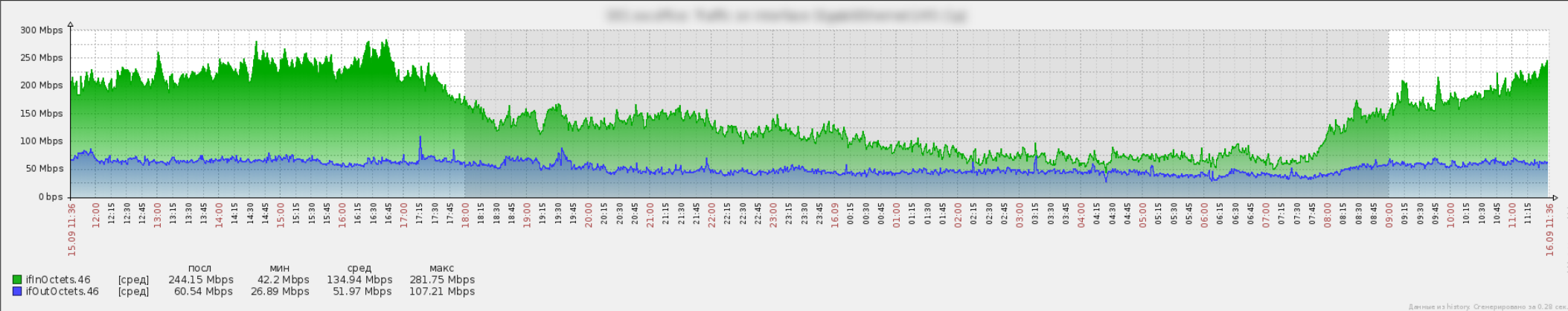
Тестирование конфигурации

№	Имя	Размер	Состояние	Дост...	Загрузка	Отдача	Время	Воспро...
1		1.45 ГБ	Загрузка 37.1 %		7.4 КБ/с	0.7 КБ/с	1 д 10 ч	
2		1.45 ГБ	Загрузка 33.1 %		6.9 КБ/с	0.4 КБ/с	1 д 5 ч	
3		1.36 ГБ	Загрузка 26.1 %		17.0 КБ/с	0.2 КБ/с	16 ч 5...	
4		1.44 ГБ	Загрузка 23.5 %		8.9 КБ/с	0.3 КБ/с	2 д 22 ч	
5		1.36 ГБ	Загрузка 42.6 %		11.5 КБ/с	2.0 КБ/с	23 ч 2...	

IP	Клиент	Флаги	%	Загрузка	Отдача	Запр...	Отдано	Загружено
	Transmission 2.84	D XE	100.0	1.6 КБ/с		4 0		1.28 МБ
	µTorrent 3.4.2	DS HX	100.0	1.1 КБ/с		1 0		128 КБ
	µTorrent Mac 1.8.7	D H	100.0	0.7 КБ/с		3 0		560 КБ
	µTorrent Mac 1.8.7	D HXE	100.0	0.5 КБ/с		3 0		1.25 МБ
	µTorrent 3.5	D HEP	100.0	0.4 КБ/с		2 0		112 КБ
	MediaGet2 2.01.3726	D HEP	100.0	0.4 КБ/с		2 0		64.0 КБ
	µTorrent 3.5	D HEP	100.0	0.4 КБ/с		2 0		
	Zona 2.0.0.6	D HXE	100.0	0.3 КБ/с		5 0		448 КБ
	µTorrent 3.5	D H	100.0	0.2 КБ/с		4 0		16.0 КБ
	MediaGet2 2.01.3680	d HE	100.0	0.1 КБ/с	0.1 КБ/с			
	MediaGet2 2.01.3673	d HE	100.0	0.1 КБ/с				
	µTorrent 3.5	DS H	100.0	0.1 КБ/с		1 0		112 КБ
	MediaGet2 2.01.3731	d HP	100.0	0.1 КБ/с				

DHT: 705 узлов (обновление) П: 54.8 КБ/с В: 519.5 МБ О: 5.8 КБ/с В: 60.6 МБ

Опыт эксплуатации



Time: 14:11:31 Date: Oct/12/2017 CPU: 6% Memory: 10.7 GiB Uptime: 66d 14:34:23

Firewall

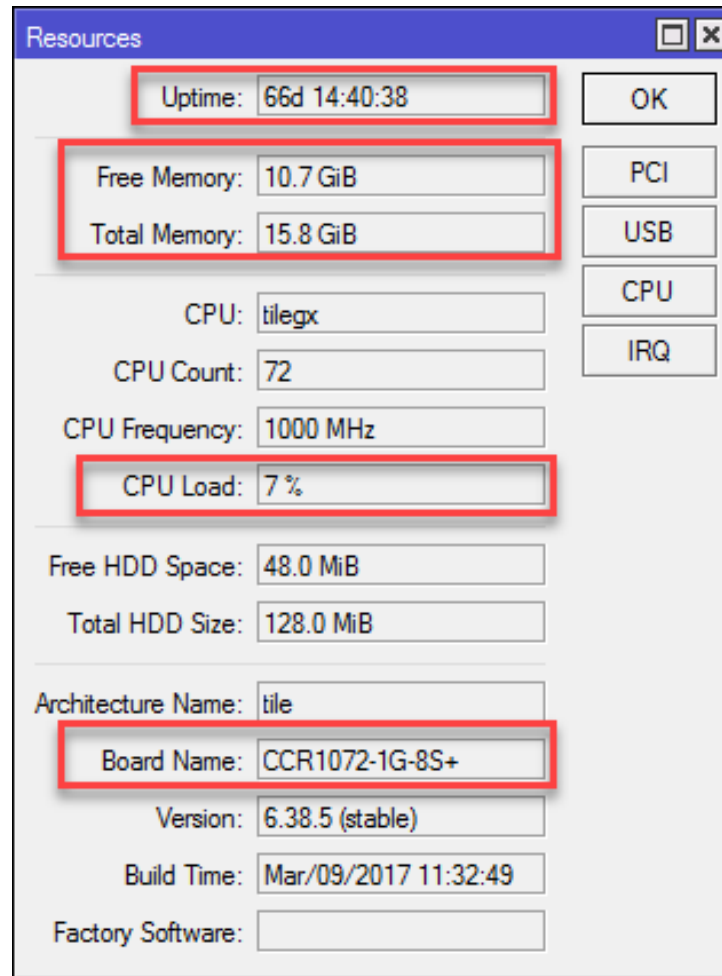
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Find p2p-seeds

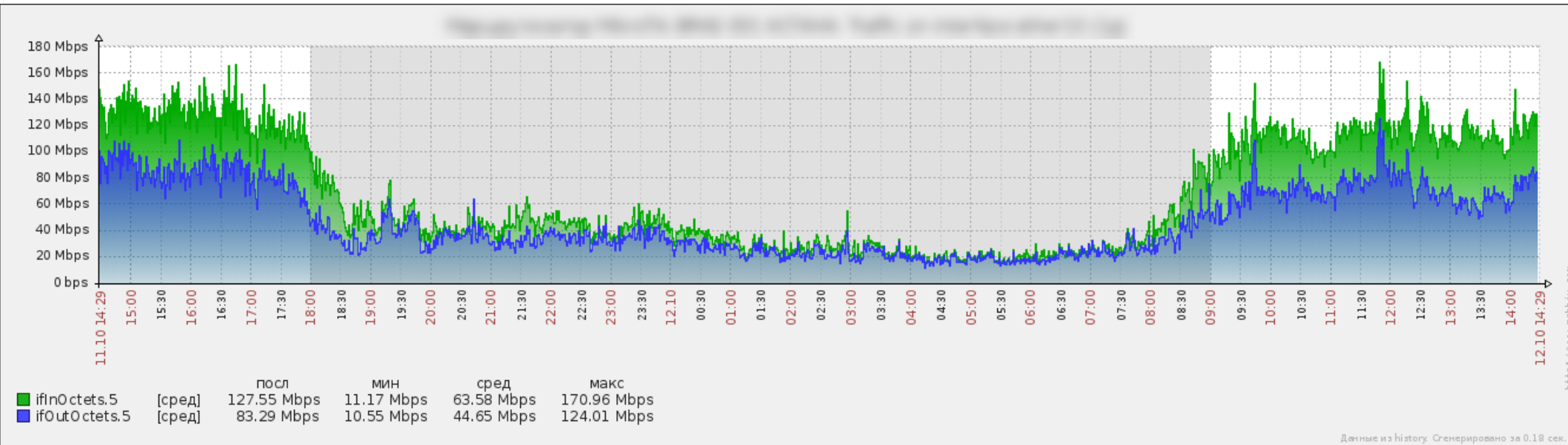
Name	Address	Timeout	Creation Time
D p2p-seeds			Sep/23/2017 17:18:34
D p2p-seeds			Sep/23/2017 16:47:18
D p2p-seeds			Sep/23/2017 17:14:19
D p2p-seeds			Sep/23/2017 17:03:36
D p2p-seeds			Sep/23/2017 16:49:31
D p2p-seeds			Sep/23/2017 16:56:22
D p2p-seeds			Sep/23/2017 16:45:34
D p2p-seeds			Sep/23/2017 16:51:58
D p2p-seeds			Sep/23/2017 16:58:40

102717 items out of 16193949

Опыт эксплуатации



Опыт эксплуатации



Time: 02:39:22 Date: Oct/12/2017 CPU: 39% Memory: 694.2 MiB Uptime: 4d 23:57:46

Firewall

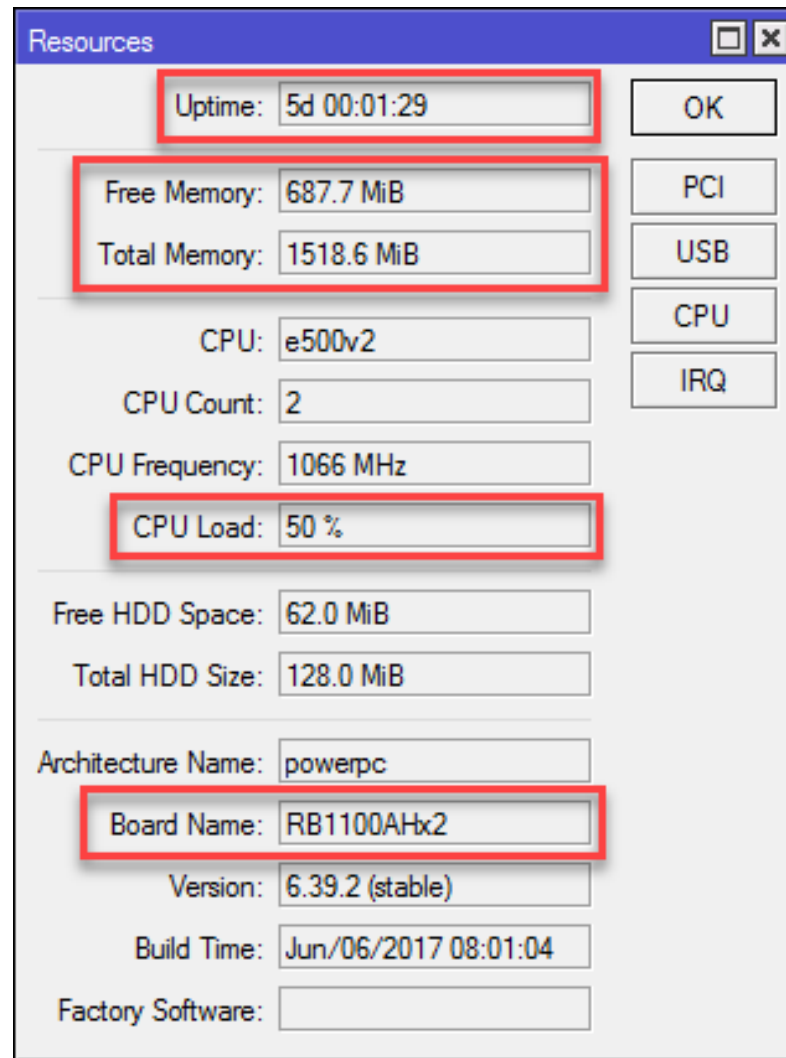
Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Find p2p-seeds

Name	Address	Timeout	Creation Time
D p2p-seeds			Oct/07/2017 03:...
D p2p-seeds			Oct/07/2017 02:...
D p2p-seeds			Oct/07/2017 03:...
D p2p-seeds			Oct/07/2017 02:...
D p2p-seeds			Oct/07/2017 03:...
D p2p-seeds			Oct/07/2017 02:...
D p2p-seeds			Oct/07/2017 03:...
D p2p-seeds			Oct/07/2017 03:...
D p2p-seeds			Oct/07/2017 03:...
D p2p-seeds			Oct/07/2017 03:...
D p2p-seeds			Oct/07/2017 03:...

65826 items out of 2984417

Опыт эксплуатации



Спасибо за внимание!