Министерство науки и высшего образования
Российской Федерации

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Новосибирский государственный технический университет»

НГТУ НЭТИ

Кафедра теоретической и прикладной информатики

Практическая работа № 2
по дисциплине «Сетевые информационные технологии»

Анализ трафика компьютерной сети

Факультет:	ПМИ
Группа:	ПМИМ-01
Студенты:	Наи Сора Орлов М. В.
Бригада:	3
Преподаватель:	Кобылянский В.Г.

Новосибирск
2021

1. Цель работы

Целями работы является изучение программного обеспечения, предназначенного для контроля и анализа сетевого трафика, а также получение практических навыков работы с программой WireShark.

2. Указания к выполнению работы

С помощью программы WireShark осуществить мониторинг и перехват потребляемого трафика сети Интернет, затем проанализировать полученные данные.

3. Ход работы

1. Запустить захват сетевого трафика в WireShark, проходящего через интерфейс, подключенный к локальной или внешней сети. Эмулировать сетевую активность в течение 10 минут выполнением указанных действий:

- посетить различные сайты, просмотреть текстовый и видеоконтент;
- выполнить пинг и трассировку любых узлов сети Интернет;
- с помощью браузера подключиться к серверу ftp.nstu.ru и скачать из корневого каталога файлы INDEX и NEW-THIS-WEEK;
- отключить перехват и сохранить сеанс в файле с расширением .pcapng.

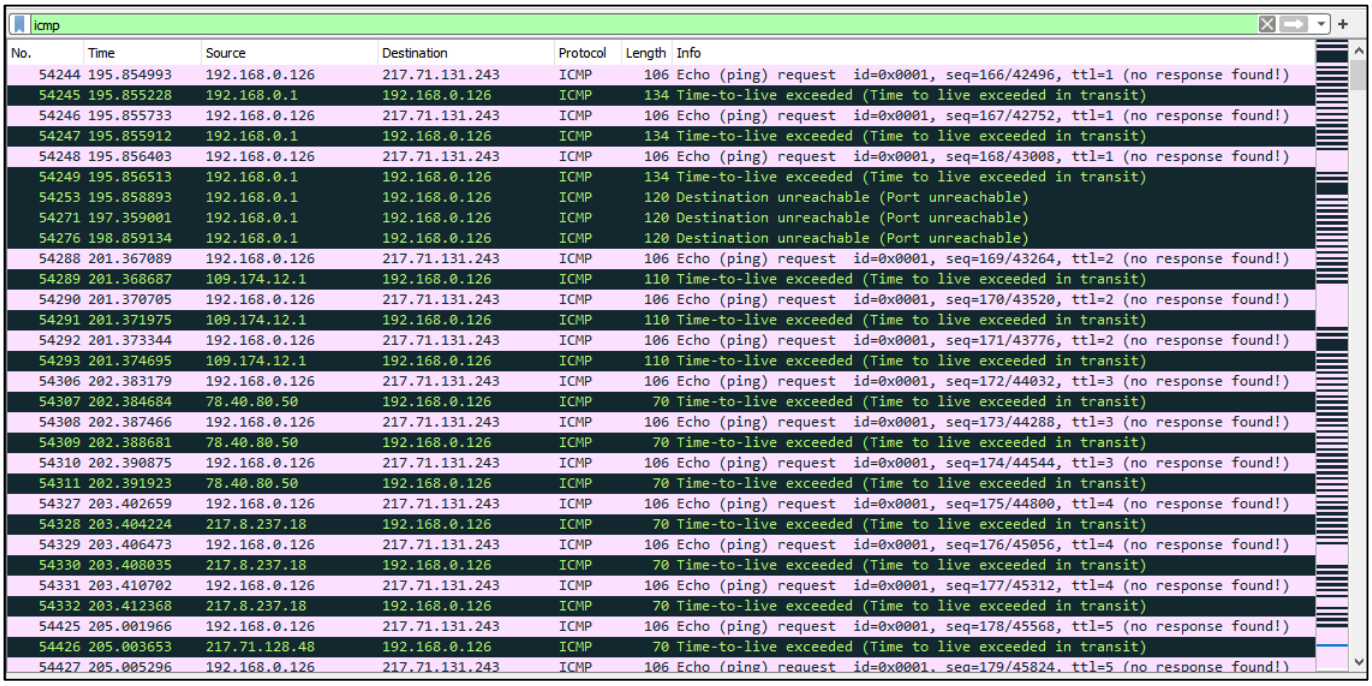
2. Выполнить фильтрацию трафика по протоколам HTTP, ICMP, ARP, FTP. Для FTP выполнить перехват команд и данных.

Фильтр по протоколу HTTP:

http

No.	Time	Source	Destination	Protocol	Length	Info
64643	437.661330	192.168.0.126	64.233.165.102	HTTP	408	GET / HTTP/1.1
64646	437.734143	64.233.165.102	192.168.0.126	HTTP	582	HTTP/1.1 301 Moved Permanently (text/html)
64653	437.801768	192.168.0.126	74.125.131.99	HTTP	201	GET / HTTP/1.1
64663	437.906298	74.125.131.99	192.168.0.126	HTTP	1217	HTTP/1.1 200 OK (text/html)
64798	452.836359	192.168.0.126	217.71.131.242	HTTP	194	GET / HTTP/1.1
64800	452.837956	217.71.131.242	192.168.0.126	HTTP	376	HTTP/1.1 302 Moved Temporarily (text/html)
77163	571.837812	192.168.0.126	2.19.115.138	HTTP	281	GET / HTTP/1.1
77167	571.913051	2.19.115.138	192.168.0.126	HTTP	317	HTTP/1.1 304 Not Modified
77173	571.935014	192.168.0.126	212.188.32.96	HTTP	307	GET /DSTROOTCAX3CRL.crl HTTP/1.1
77175	571.937387	212.188.32.96	192.168.0.126	HTTP	322	HTTP/1.1 304 Not Modified
77182	571.960417	192.168.0.126	212.188.32.16	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?9d7d8ccd0c31f9c4 HT…
77184	571.962742	212.188.32.16	192.168.0.126	HTTP	322	HTTP/1.1 304 Not Modified
77192	572.046536	192.168.0.126	88.221.216.106	HTTP	253	GET /ca.crl HTTP/1.1
77194	572.121166	88.221.216.106	192.168.0.126	HTTP	261	HTTP/1.1 304 Not Modified
1171…	784.949070	192.168.0.126	116.203.96.213	HTTP	574	GET /internet/ftp/ftpusage.shtml HTTP/1.1
1172…	785.121406	192.168.0.126	116.203.96.213	HTTP	453	GET /css/main-2.css HTTP/1.1
1172…	785.130474	116.203.96.213	192.168.0.126	HTTP	1341	HTTP/1.1 200 OK (text/html)
1172…	785.131218	192.168.0.126	116.203.96.213	HTTP	487	GET /pictures/logos/citlogo8.gif HTTP/1.1
1173…	785.208675	116.203.96.213	192.168.0.126	HTTP	878	HTTP/1.1 200 OK (text/css)
1173…	785.209953	192.168.0.126	116.203.96.213	HTTP	480	GET /pictures/xml_rss.gif HTTP/1.1
1173…	785.210992	192.168.0.126	116.203.96.213	HTTP	509	GET /pictures/logos/banner-88x31-rambler-darkblue2.gif HTTP/1.1
1173…	785.222414	116.203.96.213	192.168.0.126	HTTP	1223	HTTP/1.1 200 OK (GIF89a)
1173…	785.296994	116.203.96.213	192.168.0.126	HTTP	767	HTTP/1.1 200 OK (GIF89a)
1173…	785.299661	116.203.96.213	192.168.0.126	HTTP	1289	HTTP/1.1 200 OK (GIF89a)
1177…	785.895644	192.168.0.126	142.250.150.138	HTTP	715	GET /generate_204 HTTP/1.1
1178…	785.958252	142.250.150.138	192.168.0.126	HTTP	137	HTTP/1.1 204 No Content
1178…	786.074631	192.168.0.126	116.203.96.213	HTTP	471	GET /favicon.ico HTTP/1.1
1178…	786.163341	116.203.96.213	192.168.0.126	HTTP	349	HTTP/1.1 200 OK

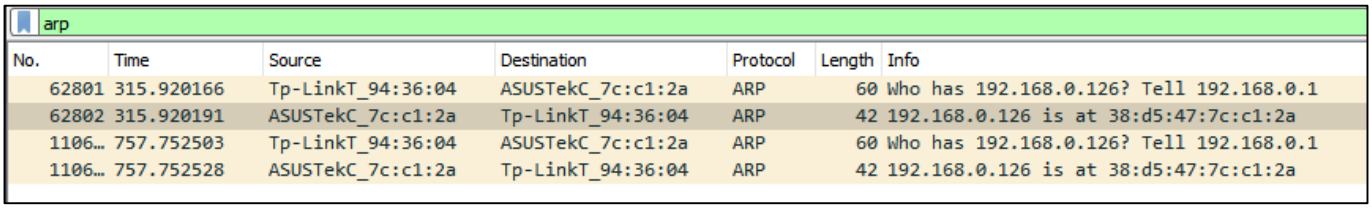
Фильтр по протоколу ICMP:



icmp

No.	Time	Source	Destination	Protocol	Length	Info
54244	195.854993	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=166/42496, ttl=1 (no response found!)
54245	195.855228	192.168.0.1	192.168.0.126	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
54246	195.855733	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=167/42752, ttl=1 (no response found!)
54247	195.855912	192.168.0.1	192.168.0.126	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
54248	195.856403	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=168/43008, ttl=1 (no response found!)
54249	195.856513	192.168.0.1	192.168.0.126	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
54253	195.858893	192.168.0.1	192.168.0.126	ICMP	120	Destination unreachable (Port unreachable)
54271	197.359001	192.168.0.1	192.168.0.126	ICMP	120	Destination unreachable (Port unreachable)
54276	198.859134	192.168.0.1	192.168.0.126	ICMP	120	Destination unreachable (Port unreachable)
54288	201.367089	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=169/43264, ttl=2 (no response found!)
54289	201.368687	109.174.12.1	192.168.0.126	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
54290	201.370705	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=170/43520, ttl=2 (no response found!)
54291	201.371975	109.174.12.1	192.168.0.126	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
54292	201.373344	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=171/43776, ttl=2 (no response found!)
54293	201.374695	109.174.12.1	192.168.0.126	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
54306	202.383179	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=172/44032, ttl=3 (no response found!)
54307	202.384684	78.40.80.50	192.168.0.126	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
54308	202.387466	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=173/44288, ttl=3 (no response found!)
54309	202.388681	78.40.80.50	192.168.0.126	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
54310	202.390875	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=174/44544, ttl=3 (no response found!)
54311	202.391923	78.40.80.50	192.168.0.126	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
54327	203.402659	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=175/44800, ttl=4 (no response found!)
54328	203.404224	217.8.237.18	192.168.0.126	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
54329	203.406473	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=176/45056, ttl=4 (no response found!)
54330	203.408035	217.8.237.18	192.168.0.126	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
54331	203.410702	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=177/45312, ttl=4 (no response found!)
54332	203.412368	217.8.237.18	192.168.0.126	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
54425	205.001966	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=178/45568, ttl=5 (no response found!)
54426	205.003653	217.71.128.48	192.168.0.126	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
54427	205.005296	192.168.0.126	217.71.131.243	ICMP	106	Echo (ping) request id=0x0001, seq=179/45824, ttl=5 (no response found!)

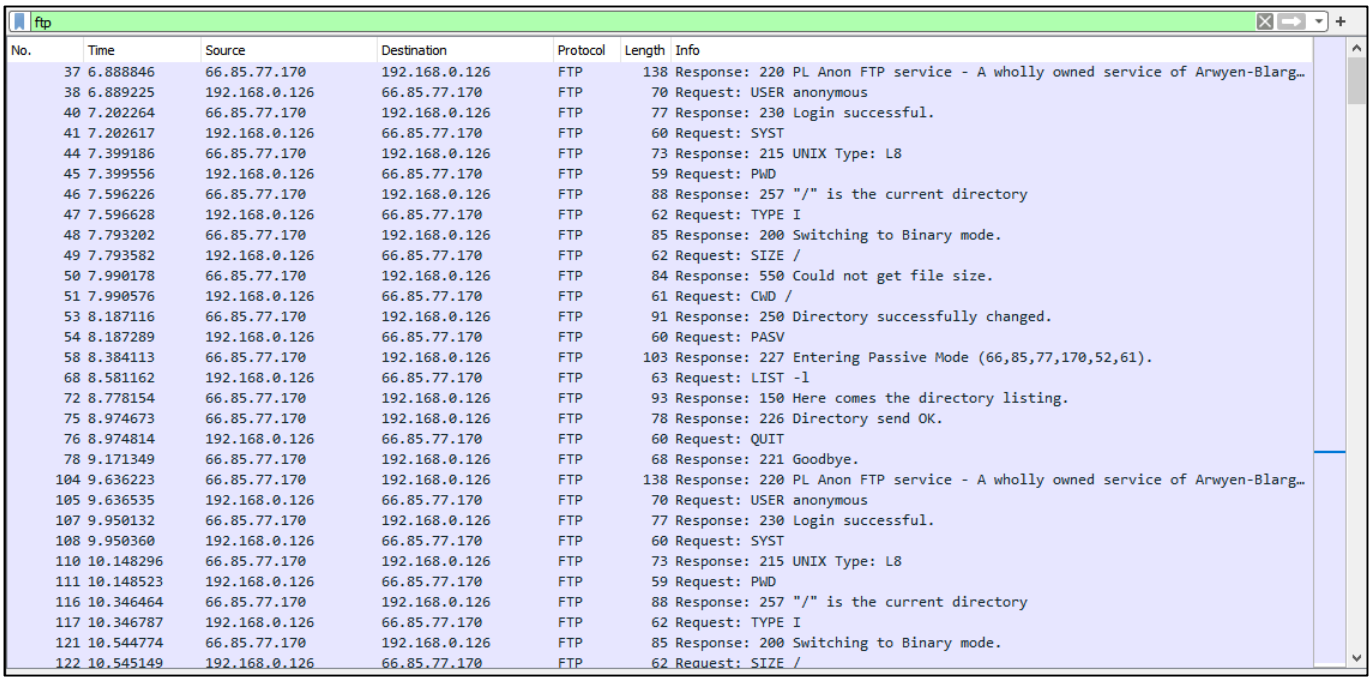
Фильтр по протоколу ARP:



arp

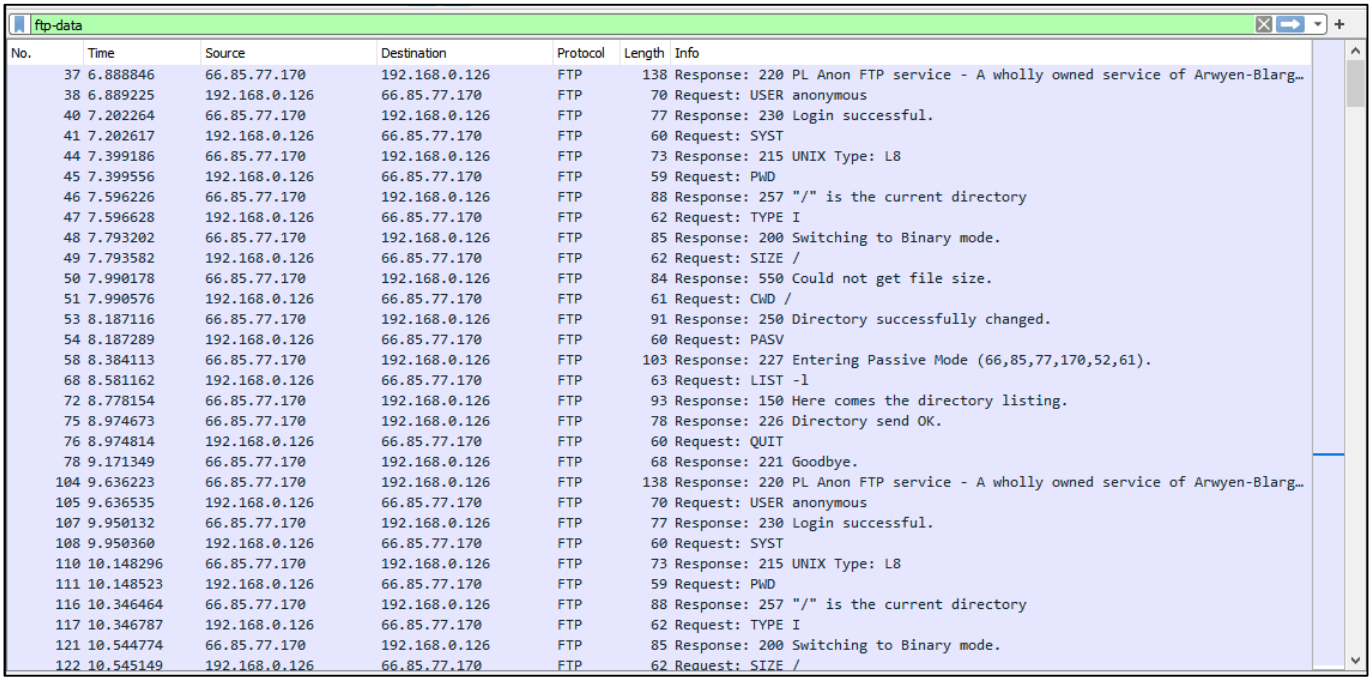
No.	Time	Source	Destination	Protocol	Length	Info
62801	315.920166	Tp-LinkT_94:36:04	ASUSTekC_7c:c1:2a	ARP	60	Who has 192.168.0.126? Tell 192.168.0.1
62802	315.920191	ASUSTekC_7c:c1:2a	Tp-LinkT_94:36:04	ARP	42	192.168.0.126 is at 38:d5:47:7c:c1:2a
1106…	757.752503	Tp-LinkT_94:36:04	ASUSTekC_7c:c1:2a	ARP	60	Who has 192.168.0.126? Tell 192.168.0.1
1106…	757.752528	ASUSTekC_7c:c1:2a	Tp-LinkT_94:36:04	ARP	42	192.168.0.126 is at 38:d5:47:7c:c1:2a

Фильтр по протоколу FTP:



ftp

No.	Time	Source	Destination	Protocol	Length	Info
37	6.888846	66.85.77.170	192.168.0.126	FTP	138	Response: 220 PL Anon FTP service - A wholly owned service of Arwyen-Blarg…
38	6.889225	192.168.0.126	66.85.77.170	FTP	70	Request: USER anonymous
40	7.202264	66.85.77.170	192.168.0.126	FTP	77	Response: 230 Login successful.
41	7.202617	192.168.0.126	66.85.77.170	FTP	60	Request: SYST
44	7.399186	66.85.77.170	192.168.0.126	FTP	73	Response: 215 UNIX Type: L8
45	7.399556	192.168.0.126	66.85.77.170	FTP	59	Request: PWD
46	7.596226	66.85.77.170	192.168.0.126	FTP	88	Response: 257 "/" is the current directory
47	7.596628	192.168.0.126	66.85.77.170	FTP	62	Request: TYPE I
48	7.793202	66.85.77.170	192.168.0.126	FTP	85	Response: 200 Switching to Binary mode.
49	7.793582	192.168.0.126	66.85.77.170	FTP	62	Request: SIZE /
50	7.990178	66.85.77.170	192.168.0.126	FTP	84	Response: 550 Could not get file size.
51	7.990576	192.168.0.126	66.85.77.170	FTP	61	Request: CWD /
53	8.187116	66.85.77.170	192.168.0.126	FTP	91	Response: 250 Directory successfully changed.
54	8.187289	192.168.0.126	66.85.77.170	FTP	60	Request: PASV
58	8.384113	66.85.77.170	192.168.0.126	FTP	103	Response: 227 Entering Passive Mode (66,85,77,170,52,61).
68	8.581162	192.168.0.126	66.85.77.170	FTP	63	Request: LIST -l
72	8.778154	66.85.77.170	192.168.0.126	FTP	93	Response: 150 Here comes the directory listing.
75	8.974673	66.85.77.170	192.168.0.126	FTP	78	Response: 226 Directory send OK.
76	8.974814	192.168.0.126	66.85.77.170	FTP	60	Request: QUIT
78	9.171349	66.85.77.170	192.168.0.126	FTP	68	Response: 221 Goodbye.
104	9.636223	66.85.77.170	192.168.0.126	FTP	138	Response: 220 PL Anon FTP service - A wholly owned service of Arwyen-Blarg…
105	9.636535	192.168.0.126	66.85.77.170	FTP	70	Request: USER anonymous
107	9.950132	66.85.77.170	192.168.0.126	FTP	77	Response: 230 Login successful.
108	9.950360	192.168.0.126	66.85.77.170	FTP	60	Request: SYST
110	10.148296	66.85.77.170	192.168.0.126	FTP	73	Response: 215 UNIX Type: L8
111	10.148523	192.168.0.126	66.85.77.170	FTP	59	Request: PWD
116	10.346464	66.85.77.170	192.168.0.126	FTP	88	Response: 257 "/" is the current directory
117	10.346787	192.168.0.126	66.85.77.170	FTP	62	Request: TYPE I
121	10.544774	66.85.77.170	192.168.0.126	FTP	85	Response: 200 Switching to Binary mode.
122	10.545149	192.168.0.126	66.85.77.170	FTP	62	Request: SIZE /



3. Заполнить таблицу, используя данные из отчета Статистика/Свойства файла. При заполнении таблицы обратите внимание на соблюдение размерности величин (Кбайт, Мбайт, Мбит).

Параметр	Значение
Время захвата, мин	16:27
Время захвата, сек	987
К-во захваченных пакетов	180722
Объем трафика, Мбайт	146.53
Средний размер пакета, Кбайт	0.83
Средняя скорость, пакетов/сек	182.9
Средняя скорость, Мбит/сек	1.19

4. По данным отчета Статистика/Иерархия Протоколов заполнить таблицу 2.3 распределения трафика по протоколам и сделать выводы о соотношении прикладных и служебных протоколов.

Протокол	Трафик, Мбайт	Трафик, %
HTTP	0,0351	0,02
FTP	0,0039	0
FTP-DATA	0,0898	0,06
GQUIC	95,9979	65,54
DNS	0,0406	0,03
MDNS	0,0018	0
TLS	48,2349	32,93
SSDP	0,1917	0,13
IGMP	0,0003	0
ICMP	0,0149	0,01
ARP	0,0001	0
NetBIOS	0,0098	0,01
LLC	0,0194	0,01
OData	1,8385	1,26
Итого	146,53	100

5. Заполнить таблицу распределения Ethernet-трафика по узлам сети. Исходные данные для заполнения таблицы получить из отчета Статистика/Конечные точки. Определить, какие из узлов наиболее загружены с учетом направления трафика (исходящий, входящий, общий).

MAC-адрес	Разрешенное имя	Трафик				
		входящий		исходящий		общий
		Мбайт	%	Мбайт	%	Мбайт
ff:ff:ff:ff:ff:ff	Broadcast	0,0802	0,054734052	0	0	0,0802
a8:9c:ed:fc:71:e8	XiaomiCo_fc:71:e8	0	0	0,0002	0,000136494	0,0002
38:d5:47:7c:c1:2a	ASUSTekC_7c:c1:2a	140,3141	95,76009014	5,8859	4,016949823	146,2001
33:33:00:01:00:03	IPv6mcast_01:00:03	0,0006	0,000409482	0	0	0,0006
33:33:00:00:00:fb	IPv6mcast_fb	0,0027	0,001842668	0	0	0,0027
10:fe:ed:94:36:04	Tp-LinkT_94:36:04	5,8786	4,011965055	140,5993	95,95479592	146,4779
10:fe:ed:94:36:02	Tp-LinkT_94:36:02	0	0	0,0283	0,019313899	0,0283
01:80:c2:00:00:0e	LLDP_Multicast	0,0001	6,82469E-05	0	0	0,0001
01:80:c2:00:00:00	Spanning-tree-(for-bridges)_00	0,0283	0,019313886	0	0	0,0283
01:00:5e:7f:ff:fa	IPv4mcast_7f:ff:fa	0,218	0,148778346	0	0	0,218
01:00:5e:00:00:fc	IPv4mcast_fc	0,0008	0,000545976	0	0	0,0008
01:00:5e:00:00:fb	IPv4mcast_fb	0,0028	0,001910915	0	0	0,0028
01:00:5e:00:00:01	IPv4mcast_01	0,0005	0,000341235	0	0	0,0005
00:00:b4:d4:15:69	EdimaxTe_d4:15:69	0	0	0,0129	0,008803862	0,0129

6. По данным таблицы из п.3 определить относительную загрузку сети (в %) за контрольный период времени по формуле:

$$\text{Загрузка} = \frac{(\text{Трафик, Мбит} \,/\, \text{Время, сек}) \cdot 100}{(\text{Пропускная способность, Мбит/сек})} = \frac{(146.53 \cdot 8 \,/\, 987) \cdot 100}{(86.5)} = 1.37\%$$

По данным сервиса https://2ip.ru/speed пропускная способность: 86.5 Мбит / сек