

Wireshark

Ping

1. Адрес моего хоста 192.168.1.40, адрес хоста назначения 171.67.215.200
2. Номера портов есть у транспортных протоколов (TCP и UDP), а ICMP – протокол сетевого уровня, поэтому порта у него нет.
3. Type: 8 (Echo (ping) request)
Code: 0

Другие поля: контрольная сумма, идентификатор, порядковый номер.

По 2 байта на контрольную сумму, идентификатор и порядковый номер.

4. Type: 0 (Echo (ping) reply)
Code: 0

Другие поля: контрольная сумма, идентификатор, порядковый номер.
По 2 байта на контрольную сумму, идентификатор и порядковый номер.

icmp									
No.	Time	Source	Destination	Protocol	Length	Info			
1639	7.544738804	192.168.1.40	171.67.215.200	ICMP	98	Echo (ping) request	id=0x86e9, seq=1/256, ttl=64 (reply in 1677)		
1677	7.734495188	171.67.215.200	192.168.1.40	ICMP	98	Echo (ping) reply	id=0x86e9, seq=1/256, ttl=241 (request in 1639)		
1840	8.545761510	192.168.1.40	171.67.215.200	ICMP	98	Echo (ping) request	id=0x86e9, seq=2/512, ttl=64 (reply in 1884)		
1884	8.735436685	171.67.215.200	192.168.1.40	ICMP	98	Echo (ping) reply	id=0x86e9, seq=2/512, ttl=241 (request in 1840)		
2077	9.547044745	192.168.1.40	171.67.215.200	ICMP	98	Echo (ping) request	id=0x86e9, seq=3/768, ttl=64 (reply in 2132)		
2132	9.736338415	171.67.215.200	192.168.1.40	ICMP	98	Echo (ping) reply	id=0x86e9, seq=3/768, ttl=241 (request in 2077)		
2335	10.5488988...	192.168.1.40	171.67.215.200	ICMP	98	Echo (ping) request	id=0x86e9, seq=4/1024, ttl=64 (reply in 2386)		
2386	10.7385257...	171.67.215.200	192.168.1.40	ICMP	98	Echo (ping) reply	id=0x86e9, seq=4/1024, ttl=241 (request in 2335)		
2703	11.5500010...	192.168.1.40	171.67.215.200	ICMP	98	Echo (ping) request	id=0x86e9, seq=5/1280, ttl=64 (reply in 2751)		
2751	11.7401995...	171.67.215.200	192.168.1.40	ICMP	98	Echo (ping) reply	id=0x86e9, seq=5/1280, ttl=241 (request in 2703)		
2993	12.5516853...	192.168.1.40	171.67.215.200	ICMP	98	Echo (ping) request	id=0x86e9, seq=6/1536, ttl=64 (reply in 3035)		
3035	12.7414424...	171.67.215.200	192.168.1.40	ICMP	98	Echo (ping) reply	id=0x86e9, seq=6/1536, ttl=241 (request in 2993)		
3205	13.5529292...	192.168.1.40	171.67.215.200	ICMP	98	Echo (ping) request	id=0x86e9, seq=7/1792, ttl=64 (reply in 3253)		
3253	13.7425158...	171.67.215.200	192.168.1.40	ICMP	98	Echo (ping) reply	id=0x86e9, seq=7/1792, ttl=241 (request in 3205)		
3445	14.5539993...	192.168.1.40	171.67.215.200	ICMP	98	Echo (ping) request	id=0x86e9, seq=8/2048, ttl=64 (reply in 3494)		
3494	14.7433877...	171.67.215.200	192.168.1.40	ICMP	98	Echo (ping) reply	id=0x86e9, seq=8/2048, ttl=241 (request in 3445)		
3712	15.5556514...	192.168.1.40	171.67.215.200	ICMP	98	Echo (ping) request	id=0x86e9, seq=9/2304, ttl=64 (reply in 3769)		
3769	15.7455156...	171.67.215.200	192.168.1.40	ICMP	98	Echo (ping) reply	id=0x86e9, seq=9/2304, ttl=241 (request in 3712)		
3936	16.5574305...	192.168.1.40	171.67.215.200	ICMP	98	Echo (ping) request	id=0x86e9, seq=10/2560, ttl=64 (reply in 3970)		
Ethernet II, Src: ZyxelCom_cb:ba:54 (5c:f4:ab:cb:ba:54), Dst: IntelCor_b1:db:95 (88:78:73:b1:db:95)									
Internet Protocol Version 4, Src: 171.67.215.200, Dst: 192.168.1.40									
Internet Control Message Protocol									
Type: 0 (Echo (ping) reply)									
Code: 0									
Checksum: 0x336a [correct]									
[Checksum Status: Good]									
Identifier (BE): 34537 (0x86e9)									
Identifier (LE): 59782 (0xe986)									
Sequence Number (BE): 1 (0x0001)									
Sequence Number (LE): 256 (0x0100)									
[Request frame: 1639]									
[Response time: 189,756 ms]									
Timestamp from icmp data: Apr 21, 2022 17:23:14.000000000 MSK									
[Timestamp from icmp data (relative): 0.848534363 seconds]									
Data (48 bytes)									
0000	88 78 73 b1 db 95 5c f4	ab cb ba 54 08 00 45 00	.xs... \. . . . T . E .						
0010	00 54 c8 f8 40 00 f1 01	7b d3 ab 43 d7 c8 c0 a8	.T . @ . . . { . C . . .						
0020	01 28 00 00 35 6a 86 e9	00 01 d2 68 61 62 00 00	.(. 5) . . . hab . .						
0030	00 00 49 0d 0a 00 00 00	00 00 10 11 12 13 14 15	. . I						
0040	16 17 18 19 1a 1b 1c 1d	1e 1f 20 21 22 23 24 25 ! "# \$ %						
0050	26 27 28 29 2a 2b 2c 2d	2e 2f 30 31 32 33 34 35	&' () * + , - . / 0 1 2 3 4 5						
0060	36 37	67							

Traceroute

1. Нет поля Timestamp from icmp data. Кроме того у первых запросов есть пометка [Expert Info (Warning/Sequence): No response seen to ICMP request]
2. Появились подразделы Internet Protocol Version 4 и Internet Control Message Protocol с информацией об эхо-запросе (см. скриншот)
3. У последних пакетов есть поля Sequence Number и Identifier, а также время ответа. В отличие от пакетов с ошибками, эти пакеты отправил хост, для которого запускался traceroute.

4. Наибольшая задержка была между mskix.he.net (зарегистрирован в Москве) и ve951.core1.ewr5.he.net (Фримонт, США). Ниже скриншоты работы traceroute и обращений к whois.

```
margo@laptop:~$ sudo traceroute -I stanford.edu
traceroute to stanford.edu (171.67.215.200), 30 hops max, 60 byte packets
 1  gateway (192.168.1.1)  2.571 ms  2.495 ms  2.474 ms
 2  5x19x0x194.static-business.spb.ertelecom.ru (5.19.0.194)  19.904 ms  19.892 ms  19.880 ms
 3  5x19x0x197.static-business.spb.ertelecom.ru (5.19.0.197)  6.364 ms  6.354 ms  6.343 ms
 4  msk-ix.ertelecom.ru (195.208.209.132)  21.757 ms  22.753 ms  22.740 ms
 5  mskix.he.net (195.208.210.40)  38.846 ms  38.832 ms  38.818 ms
 6  * * *
 7  * * *
 8  ve951.core1.ewr5.he.net (184.104.196.98)  174.780 ms  174.763 ms  174.747 ms
 9  * * *
10  100ge13-1.core4.fmt2.he.net (184.105.81.61)  205.469 ms  205.456 ms  205.443 ms
11  100ge9-1.core1.pao1.he.net (184.105.222.90)  205.426 ms  205.412 ms *
12  stanford-university.100gigabitethernet5-1.core1.pao1.he.net (184.105.177.238)  307.052 ms  307.007 ms  276.322 ms
13  woa-west-rtr-vl3.SUNet (171.66.255.132)  276.220 ms *  276.159 ms
14  * * *
15  web.stanford.edu (171.67.215.200)  307.377 ms  307.363 ms  307.351 ms
```

IP: 195.208.210.40

```
% Information related to '195.208.208.0 - 195.208.215.255'
% Abuse contact for '195.208.208.0 - 195.208.215.255' is 'ip@msk-ix.ru'
inetnum:          195.208.208.0 - 195.208.215.255
netname:          RU-MSK-IX-19960419
country:         RU
org:              ORG-JCE1-RIPE
admin-c:          EV3802-RIPE
tech-c:           IA5224-RIPE
status:           ALLOCATED PA
mnt-by:           RUIX-MNT
mnt-by:           RIPE-NCC-HM-MNT
created:          2019-02-21T12:05:25Z
last-modified:    2019-02-21T12:05:25Z
source:           RIPE
organisation:     ORG-JCE1-RIPE
org-name:         Joint-stock company "Internet Exchange "MSK-IX"
country:         RU
org-type:         LIR
address:          8 Marta Street 1, bld. 12, office XXXV, room 19
address:          127083
address:          Moscow
address:          RUSSIAN FEDERATION
```

IP: 184.104.196.98

```
#
NetRange:         184.104.0.0 - 184.105.255.255
CIDR:             184.104.0.0/15
NetName:          HURRICANE-11
NetHandle:        NET-184-104-0-0-1
Parent:           NET184 (NET-184-0-0-0-0)
NetType:          Direct Allocation
OriginAS:         AS6939
Organization:     Hurricane Electric LLC (HURC)
RegDate:          2010-05-10
Updated:          2012-02-24
Ref:              https://rdap.arin.net/registry/ip/184.104.0.0
OrgName:          Hurricane Electric LLC
OrgId:            HURC
Address:          760 Mission Court
City:             Fremont
StateProv:        CA
PostalCode:       94539
Country:          US
```

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
1381	4.486221747	192.168.1.40	171.67.215.200	ICMP	74	Echo (ping) request id=0x242d, seq=46/11776, ttl=16 (reply in 1455)
1382	4.487000710	171.66.255.132	192.168.1.40	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1383	4.487161564	192.168.1.40	171.67.215.200	ICMP	74	Echo (ping) request id=0x242d, seq=47/12032, ttl=16 (reply in 1456)
1408	4.551545247	171.66.255.132	192.168.1.40	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1409	4.551651724	192.168.1.40	171.67.215.200	ICMP	74	Echo (ping) request id=0x242d, seq=48/12288, ttl=16 (reply in 1477)
1415	4.570784259	171.66.255.132	192.168.1.40	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1416	4.570967011	192.168.1.40	171.67.215.200	ICMP	74	Echo (ping) request id=0x242d, seq=49/12544, ttl=17 (reply in 1481)
1440	4.663137003	171.67.215.200	192.168.1.40	ICMP	74	Echo (ping) reply id=0x242d, seq=43/11000, ttl=241 (request in 1367)
1449	4.663854124	171.67.215.200	192.168.1.40	ICMP	74	Echo (ping) reply id=0x242d, seq=44/11264, ttl=241 (request in 1369)
1452	4.665397712	171.67.215.200	192.168.1.40	ICMP	74	Echo (ping) reply id=0x242d, seq=45/11520, ttl=241 (request in 1372)
1455	4.675741003	171.67.215.200	192.168.1.40	ICMP	74	Echo (ping) reply id=0x242d, seq=46/11776, ttl=241 (request in 1381)
1456	4.676336051	171.67.215.200	192.168.1.40	ICMP	74	Echo (ping) reply id=0x242d, seq=47/12032, ttl=241 (request in 1383)
1477	4.740863540	171.67.215.200	192.168.1.40	ICMP	74	Echo (ping) reply id=0x242d, seq=48/12288, ttl=241 (request in 1409)
1481	4.760275760	171.67.215.200	192.168.1.40	ICMP	74	Echo (ping) reply id=0x242d, seq=49/12544, ttl=241 (request in 1416)

Internet Protocol Version 4, Src: 171.66.255.132, Dst: 192.168.1.40
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0x6a85 [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 192.168.1.40, Dst: 171.67.215.200
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 60
Identification: 0x6236 (25142)
Flags: 0x00
Fragment Offset: 0
Time to Live: 1
Protocol: ICMP (1)
Header Checksum: 0x12af [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.40
Destination Address: 171.67.215.200
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x5e26 [unverified] [in ICMP error packet]
[Checksum Status: Unverified]
Identifier (BE): 9261 (0x242d)
Identifier (LE): 11556 (0x2d24)
Sequence Number (BE): 39 (0x0027)

Программирование

1. IP-адрес и маска сети

Результат работы ifconfig:

```
wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.40 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::7610:128a:c2b5:3037 prefixlen 64 scopeid 0x20<link>
    ether 88:78:73:b1:db:95 txqueuelen 1000 (Ethernet)
    RX packets 489863 bytes 237982521 (226.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 175560 bytes 26490236 (25.2 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2. Доступные порты

С помощью утилиты

`nmap -p <range> host`

можно узнать занятые порты в данном диапазоне. Свободные – все остальные.

```
margo@laptop:~$ sudo nmap -p10-200 localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-22 17:48 MSK
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000090s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 188 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
139/tcp   open  netbios-ssn

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

Задачи

Задача 1

- 1) Количество отправленных пакетов =

$$\frac{W}{2} + \dots + W - 1 + W = \frac{\frac{W}{2} + W}{2} \left(\frac{W}{2} + 1 \right) = \frac{3}{8}W^2 + \frac{3}{4}W$$

Из этих пакетов 1 потерян, значит частота потерь $L = \frac{1}{\frac{3}{8}W^2 + \frac{3}{4}W}$

- 2) По предыдущему пункту $L = \frac{1}{\frac{3}{8}W^2 + \frac{3}{4}W} \approx \frac{1}{\frac{3}{8}W^2}$ (считаем, что W мало по

сравнению с W^2). Откуда $W = \sqrt{\frac{8}{3L}}$. Средняя скорость передачи данных равна

$$\frac{3}{4}W \text{ MSS} / RTT = \frac{3}{4} \sqrt{\frac{8}{3}} \frac{\text{MSS}}{RTT \sqrt{L}} \approx \frac{1,22 \text{ MSS}}{RTT \sqrt{L}}$$

Задача 2

- 1) Размер окна будет увеличиваться $W/2, \alpha W/2, \dots, \alpha^{n-1}W/2, \alpha^n W/2 = W$

Из последнего равенства $n = \ln 2 / \ln \alpha$

То есть время t увеличения окна с $W/2$ до W вычисляется как

$$t = (n + 1)RTT = (\ln 2 / \ln \alpha + 1)RTT$$

Видно, что t зависит только от α .

- 2) Пакеты теряются при последнем увеличении окна, то есть количество

$$\text{потерянных пакетов} \alpha^n W/2 - \alpha^{n-1} W/2 = W - W/\alpha = W(\alpha - 1)/\alpha$$

То есть частота потерь (количество потерянных пакетов за RTT времени)

$$W(\alpha - 1)/\alpha n = W \frac{\alpha - 1}{\alpha} \frac{\ln \alpha}{\ln 2} = W \frac{\alpha - 1}{\alpha} \log_2 \alpha - \text{линейная зависимость от длины}$$

окна.

Если же под частотой потерь подразумевается доля потерянных пакетов, то вычислить ее можно как

$$W(\alpha - 1)/\alpha / (W/2 + \alpha W/2 + \dots + \alpha^{n-1} W/2 + \alpha^n W/2) =$$

$$2(\alpha - 1)/\alpha/(1 + \alpha + \dots + \alpha^{n-1} + \alpha^n) = 2(\alpha - 1)^2/\alpha(2\alpha - 1)$$

Даже если не проводить вычисления до конца, видно, что доля потерянных пакетов не зависит от размера окна.