Министерство образования Республики Беларусь
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Факультет прикладной математики и информатики

Бинцаровский Леонид Петрович

Аппаратные средства ПК и сетевое оборудование локальных компьютерных сетей

Отчет по лабораторной работе № 1,
(“Компьютерные сети”)
студента 3-го курса 3-ей группы

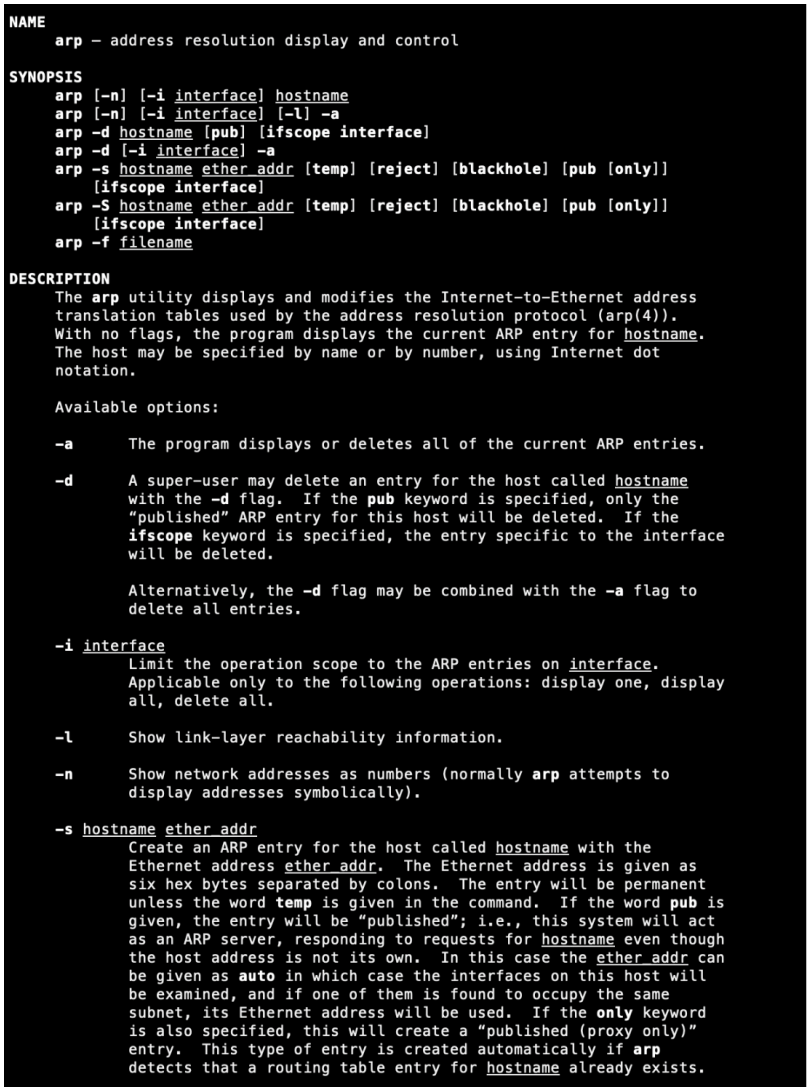
Преподаватель

Рафеенко Е.Д./
Рябый В.В.

2024

4.3.1 *Задание 1.* Получение справочной информации по командам

В отчет приложите скриншот получения справочной информации об одной из утилит на ваш выбор



```
NAME
     arp – address resolution display and control

SYNOPSIS
     arp [-n] [-i interface] hostname
     arp [-n] [-i interface] [-l] -a
     arp -d hostname [pub] [ifscope interface]
     arp -d [-i interface] -a
     arp -s hostname ether_addr [temp] [reject] [blackhole] [pub [only]]
         [ifscope interface]
     arp -S hostname ether_addr [temp] [reject] [blackhole] [pub [only]]
         [ifscope interface]
     arp -f filename

DESCRIPTION
     The arp utility displays and modifies the Internet-to-Ethernet address
     translation tables used by the address resolution protocol (arp(4)).
     With no flags, the program displays the current ARP entry for hostname.
     The host may be specified by name or by number, using Internet dot
     notation.

     Available options:

     -a      The program displays or deletes all of the current ARP entries.

     -d      A super-user may delete an entry for the host called hostname
             with the -d flag.  If the pub keyword is specified, only the
             "published" ARP entry for this host will be deleted.  If the
             ifscope keyword is specified, the entry specific to the interface
             will be deleted.

             Alternatively, the -d flag may be combined with the -a flag to
             delete all entries.

     -i interface
             Limit the operation scope to the ARP entries on interface.
             Applicable only to the following operations: display one, display
             all, delete all.

     -l      Show link-layer reachability information.

     -n      Show network addresses as numbers (normally arp attempts to
             display addresses symbolically).

     -s hostname ether_addr
             Create an ARP entry for the host called hostname with the
             Ethernet address ether_addr.  The Ethernet address is given as
             six hex bytes separated by colons.  The entry will be permanent
             unless the word temp is given in the command.  If the word pub is
             given, the entry will be "published"; i.e., this system will act
             as an ARP server, responding to requests for hostname even though
             the host address is not its own.  In this case the ether_addr can
             be given as auto in which case the interfaces on this host will
             be examined, and if one of them is found to occupy the same
             subnet, its Ethernet address will be used.  If the only keyword
             is also specified, this will create a "published (proxy only)"
             entry.  This type of entry is created automatically if arp
             detects that a routing table entry for hostname already exists.

             If the reject keyword is specified the entry will be marked so
             that traffic to the host will be discarded and the sender will be
             notified the host is unreachable.  The blackhole keyword is
             similar in that traffic is discarded but the sender is not
             notified.  These can be used to block external traffic to a host
             without using a firewall.

             If the ifscope keyword is specified, the entry will set with an
             additional property that strictly associate the entry to the
             interface. This allows for the presence of multiple entries with
             the same destination on different interfaces.

     -S hostname ether_addr
             Is just like -s except any existing ARP entry for this host will
             be deleted first.

     -f filename
             Cause the file filename to be read and multiple entries to be set
             in the ARP tables.  Entries in the file should be of the form

                   hostname ether_addr [temp] [pub [only]] [ifscope interface]

             with argument meanings as given above.  Leading whitespace and
             empty lines are ignored.  A '#' character will mark the rest of
             the line as a comment.

     -x      Show extended link-layer reachability information in addition to
             that shown by the -l flag.

SEE ALSO
     inet(3), arp(4), ifconfig(8), ndp(8)

HISTORY
     The arp utility appeared in 4.3BSD.

macOS 14.1                      March 18, 2008                      macOS 14.1
```

4.3.2. ***Задание 2.*** **Получение имени хоста**.
Выведите на экран и запишите имя локального хоста (желательно и личного компьютера), на котором вы работаете с помощью команды (какой?).

```
➜  ~ hostname
ilas-mbp
```

4.3.3. ***Задание 3.*** **Изучение утилиты ipconfig**
Проверьте конфигурацию TCP/IP с помощью утилиты ipconfig. Утилиту выполните на компьютере в дисплейном классе ФПМИ и на личном ноутбуке.

Заполните соответственно таблицу.
Обратите внимание на значения в последних двух справа столбцах.
Проанализируйте отличия в заполненных столбцах:

	ПК дисплейного класса	**Личный ноутбук в сети БГУ**	**Личный ноутбук в домашней сети**
Имя компьютера	Fpmi506-14	Ilas-mbp	Ilas-mbp
Описание адаптера	Realtek PCIe GbE Family Controller	Build-in Wi-Fi Apple adapter 802.11ax Wi-Fi 6 wireless networking IEEE 802.11a/b/g/n/ ac compatible	Build-in Wi-Fi Apple adapter 802.11ax Wi-Fi 6 wireless networking IEEE 802.11a/b/g/n/ ac compatible
Физический адрес	09-60-6E-D6-59-C5	A0-78-17-9B-D2-1F	

сетевого адаптера			
IP-адрес	10.150.5.86	192.168.100.3	
Маска подсети	255.255.255.0	255.255.128.0	
Основной шлюз	10.150.5.1	10.160.0.1	
Используется ли DHCP (адрес DHCP-сервера)	10.150.5.1	10.0.0.66	
Адрес DNS-сервера	10.0.0.66 10.0.0.67	10.0.0.66 10.0.0.67	
Адрес WINS-сервера	Основной: 10.0.0.67Дополнительный: 10.0.0.66	Основной: 10.0.0.67Дополнительный: 10.0.0.66	

4.3.4. ***Задание 4*****. Тестирование связи с помощью утилиты ping**.
Проверьте правильность установки и конфигурирования TCP/IP на

локальном компьютере. С помощью команды ping проверьте перечисленные ниже адреса и для каждого из них отметьте TTL (Time To Live) и время отклика.

10.150.1.3, 10.150.1.1, 10.0.0.20, 10.150.6.29, 10.150.3.30

Адрес	TTL	Время отклика
10.150.1.3	128	Минимальное = 29мсек, Максимальное = 92 мсек, Среднее = 45 мсек
10.150.1.1	Превышен интервал ожидания для запроса.	Превышен интервал ожидания для запроса.
10.0.0.20	63	Минимальное = 9мсек, Максимальное = 269 мсек, Среднее = 123 мсек
10.150.6.29	Превышен интервал ожидания для запроса.	Превышен интервал ожидания для запроса.
10.150.3.30	Превышен интервал ожидания для запроса.	Превышен интервал ожидания для запроса.

Попробуйте увеличить время отклика

Задайте различную длину посылаемых пакетов (можно только на любом одном из примеров выписать результат для отчета).

Выпишите ответы на следующие задания:

- Определите DNS-имя любого соседнего компьютера по его IP-адресу

```
PING 192.168.100.3 (192.168.100.3): 56 data bytes
64 bytes from 192.168.100.3: icmp_seq=0 ttl=64 time=0.146 ms
64 bytes from 192.168.100.3: icmp_seq=1 ttl=64 time=0.165 ms
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=0.203 ms
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=0.144 ms
64 bytes from 192.168.100.3: icmp_seq=4 ttl=64 time=0.147 ms

--- 192.168.100.3 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.144/0.161/0.203/0.022 ms
```

- Проверьте доступность сайта поисковой системы Yandex в сети Internet через две точки ya.ru и yandex.ru , а также узнайте их IP-адреса.

```
→  ~ ping -c 5 -i 1 ya.ru
PING ya.ru (77.88.55.242): 56 data bytes
64 bytes from 77.88.55.242: icmp_seq=0 ttl=51 time=76.780 ms
64 bytes from 77.88.55.242: icmp_seq=1 ttl=51 time=39.721 ms
64 bytes from 77.88.55.242: icmp_seq=2 ttl=51 time=75.699 ms
64 bytes from 77.88.55.242: icmp_seq=3 ttl=51 time=52.731 ms
64 bytes from 77.88.55.242: icmp_seq=4 ttl=51 time=81.522 ms

--- ya.ru ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 39.721/65.291/81.522/16.219 ms
→  ~ ping -c 5 -i 1 yandex.ru
PING yandex.ru (5.255.255.70): 56 data bytes
64 bytes from 5.255.255.70: icmp_seq=0 ttl=245 time=37.193 ms
64 bytes from 5.255.255.70: icmp_seq=1 ttl=245 time=33.969 ms
64 bytes from 5.255.255.70: icmp_seq=2 ttl=245 time=28.505 ms
64 bytes from 5.255.255.70: icmp_seq=3 ttl=245 time=32.582 ms
64 bytes from 5.255.255.70: icmp_seq=4 ttl=245 time=32.449 ms

--- yandex.ru ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 28.505/32.940/37.193/2.799 ms
```

- Пропинговать сетевой интерфейс локального компьютера

```
→  ~ nslookup
> 192.168.100.3
Server:         192.168.100.1
Address:        192.168.100.1#53

3.100.168.192.in-addr.arpa      name = ilas-mbp.
```

- Отправить на адрес согласно вашему варианту n сообщений (n-номер варианта) с эхо-запросом, каждое из которых имеет поле

данных из 1000 байт.

```
→  ~ ping -c 5 -i 1 rabota.by
PING rabota.by (178.172.250.174): 56 data bytes
64 bytes from 178.172.250.174: icmp_seq=0 ttl=56 time=25.524 ms
64 bytes from 178.172.250.174: icmp_seq=1 ttl=56 time=47.427 ms
64 bytes from 178.172.250.174: icmp_seq=2 ttl=56 time=21.105 ms
64 bytes from 178.172.250.174: icmp_seq=3 ttl=56 time=13.412 ms
64 bytes from 178.172.250.174: icmp_seq=4 ttl=56 time=13.914 ms

--- rabota.by ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 13.412/24.276/47.427/12.434 ms
→  ~ ping -c 5 -i 1 url.by
PING url.by (178.33.33.187): 56 data bytes
64 bytes from 178.33.33.187: icmp_seq=0 ttl=42 time=85.245 ms
64 bytes from 178.33.33.187: icmp_seq=1 ttl=42 time=86.800 ms
64 bytes from 178.33.33.187: icmp_seq=2 ttl=42 time=106.441 ms
64 bytes from 178.33.33.187: icmp_seq=3 ttl=42 time=96.149 ms
64 bytes from 178.33.33.187: icmp_seq=4 ttl=42 time=140.540 ms

--- url.by ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 85.245/103.035/140.540/20.227 ms
```

- Что такое TTL

  Time to live — время жизни пакета данных в протоколе IP (предельно допустимое время его пребывания в системе), время актуальности записей DNS.

4.3.5. *Задание 5.*

- Подключите Wi-Fi на личном ноутбуке и протестируйте ссылки согласно вашему варианту задания.

```
→  ~  ping -c 7 -i 1 rabota.by
PING rabota.by (178.172.250.173): 56 data bytes
64 bytes from 178.172.250.173: icmp_seq=0 ttl=56 time=20.229 ms
64 bytes from 178.172.250.173: icmp_seq=1 ttl=56 time=13.748 ms
64 bytes from 178.172.250.173: icmp_seq=2 ttl=56 time=13.657 ms
64 bytes from 178.172.250.173: icmp_seq=3 ttl=56 time=19.012 ms
64 bytes from 178.172.250.173: icmp_seq=4 ttl=56 time=27.416 ms
64 bytes from 178.172.250.173: icmp_seq=5 ttl=56 time=298.360 ms
64 bytes from 178.172.250.173: icmp_seq=6 ttl=56 time=17.650 ms

--- rabota.by ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 13.657/58.582/298.360/97.983 ms
→  ~  ping -c 7 -i 1 url.by
PING url.by (178.33.33.187): 56 data bytes
64 bytes from 178.33.33.187: icmp_seq=0 ttl=42 time=106.028 ms
64 bytes from 178.33.33.187: icmp_seq=1 ttl=42 time=101.850 ms
64 bytes from 178.33.33.187: icmp_seq=2 ttl=42 time=88.480 ms
64 bytes from 178.33.33.187: icmp_seq=3 ttl=42 time=91.771 ms
64 bytes from 178.33.33.187: icmp_seq=4 ttl=42 time=118.059 ms
64 bytes from 178.33.33.187: icmp_seq=5 ttl=42 time=108.899 ms
64 bytes from 178.33.33.187: icmp_seq=6 ttl=42 time=92.850 ms

--- url.by ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 88.480/101.134/118.059/9.911 ms
```

- Затем отключите Wi-Fi и протестируйте те же ссылки. Проанализируйте полученные результаты.

```
➜  ~  ping -c 5 -i 1 rabota.by
ping: cannot resolve rabota.by: Unknown host
➜  ~  ping -c 5 -i 1 url.by
ping: cannot resolve url.by: Unknown host
```

4.3.6. *Задание 6.* Утилита Tracert. Определение пути IP-пакета

- Определите список маршрутизаторов на пути следования пакетов от локального компьютера до адресов согласно вашему варианту без преобразования IP-адресов в имена DNS. (Выпишите команду с помощью которой это можно выполнить.)

```
➜  ~ traceroute url.by | head -n 30
traceroute to url.by (178.33.33.187), 64 hops max, 52 byte packets
 1  192.168.100.1 (192.168.100.1)  30.900 ms  4.136 ms  3.863 ms
 2  100.83.0.1 (100.83.0.1)  10.009 ms  9.484 ms  10.912 ms
 3  93.84.80.157 (93.84.80.157)  25.366 ms  11.369 ms  11.337 ms
 4  10.0.62.77 (10.0.62.77)  35.033 ms  11.928 ms  13.606 ms
 5  core1.net.belpak.by (93.85.253.197)  35.720 ms  22.696 ms  47.592 ms
 6  ie2.net.belpak.by (93.85.80.42)  15.473 ms  15.006 ms  16.292 ms
 7  asbr1.net.belpak.by (93.85.80.98)  15.997 ms  15.941 ms  14.744 ms
 8  * * *
 9  * * *
10  * * *
11  * * *
12  be104.ams-gsa1-sbb2-nc5.nl.eu (91.121.215.192)  81.362 ms
    be104.ams-gsa1-sbb1-nc5.nl.eu (91.121.215.190)  86.135 ms  80.392 ms
13  be104.gra-g2-nc5.fr.eu (213.251.128.66)  85.838 ms
    be104.gra-g1-nc5.fr.eu (213.186.32.210)  173.205 ms
    be104.gra-g2-nc5.fr.eu (213.251.128.66)  89.125 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
➜  ~ traceroute rabota.by | head -n 30
traceroute: Warning: rabota.by has multiple addresses; using 178.172.250.173
traceroute to rabota.by (178.172.250.173), 64 hops max, 52 byte packets
 1  192.168.100.1 (192.168.100.1)  4.893 ms  4.760 ms  4.461 ms
 2  100.83.0.1 (100.83.0.1)  9.957 ms  19.502 ms  17.053 ms
 3  93.84.80.157 (93.84.80.157)  10.462 ms  10.487 ms  11.823 ms
 4  10.0.62.77 (10.0.62.77)  14.354 ms  14.213 ms  14.936 ms
 5  core1.net.belpak.by (93.85.253.197)  22.617 ms  23.098 ms  24.590 ms
 6  93.84.125.189 (93.84.125.189)  13.770 ms  14.605 ms  14.654 ms
 7  10g.datacenter.beltelecom.by (178.124.134.53)  15.494 ms
    178.124.134.165 (178.124.134.165)  15.425 ms
    10g.datacenter.beltelecom.by (178.124.134.61)  14.036 ms
 8  93.85.86.50 (93.85.86.50)  19.353 ms  20.378 ms  20.979 ms
 9  * * *
```

- С помощью команды tracert проверьте, через какие промежуточные узлы идет сигнал. Выпишите ***первые три*** и ***последние два*** промежуточных узла на каждый из ваших вариантов заданий.

rabota.by	url.by
192.168.100.1	192.168.100.1
100.83.0.1	100.83.0.1
93.83.80.157	93.83.80.157

- Можно ли утилитой ***tracert*** задать максимальное число ретрансляций, если можно, то выпишите как.

  Можно. Нужно прописать дополнительный флаг -h. Пример: tracert -d -h 2 [hostname]

4.3.7. *Задание 7.* Просмотр ARP-кэша

- С помощью утилиты **arp** просмотрите и выпишите ARP-таблицу локального компьютера (несколько записей).

```
[→  ~ arp -a
192.168.100.1 (192.168.100.1) at f4:b8:a7:bc:46:de on en0 ifscope [ethernet]
ilas-mbp (192.168.100.3) at a0:78:17:9b:d2:1f on en0 ifscope permanent [ethernet]
192.168.100.8 (192.168.100.8) at 7c:e9:d3:56:1c:47 on en0 ifscope [ethernet]
192.168.100.55 (192.168.100.55) at 78:ab:bb:bd:c9:78 on en0 ifscope [ethernet]
192.168.100.255 (192.168.100.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
mdns.mcast.net (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

- Прокомментируйте какая информация хранится в ARP- таблице.

ARP — протокол сетевого уровня, предназначенный для преобразования IP- адресов (адресов сетевого уровня) в MAC-адреса (адреса канального уровня) в сетях TCP/IP. ARP-таблица отображает IP и MAC подключенных к серверу сетевых устройств.

4.3.8. ***Задание 8*****. Утилита netstat.** Получение информации о текущих сетевых соединениях и протоколах стека TCP/IP.

- Получите список активных TCP-соединений локального компьютера. (Выпишите команду с помощью которой это можно выполнить.)

```
→  ~ netstat
Active Internet connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  ilas-mbp.64854         86.57.191.25.https     ESTABLISHED
tcp4       0      0  ilas-mbp.64849         149.154.167.223.https  ESTABLISHED
tcp4       0      0  ilas-mbp.64848         149.154.167.223.https  ESTABLISHED
tcp4       0      0  ilas-mbp.64846         149.154.167.43.https   ESTABLISHED
tcp4       0      0  ilas-mbp.64838         149.154.167.223.https  ESTABLISHED
tcp4       0      0  ilas-mbp.64836         149.154.167.223.https  ESTABLISHED
tcp4       0      0  ilas-mbp.64730         149.154.167.51.https   ESTABLISHED
tcp4       0      0  ilas-mbp.64679         33.224.186.35.bc.https ESTABLISHED
tcp4       0      0  ilas-mbp.64677         lh-in-f188.1e100.https ESTABLISHED
tcp4       0      0  ilas-mbp.64657         149.154.167.41.https   ESTABLISHED
tcp4       0      0  ilas-mbp.64852         188.114.99.224.https   TIME_WAIT
tcp4       0      0  ilas-mbp.64853         25.224.186.35.bc.https TIME_WAIT
tcp4       0      0  ilas-mbp.65487         17.248.213.66.443      ESTABLISHED
tcp4       0      0  ilas-mbp.65486         lt-in-f207.1e100.443   ESTABLISHED
tcp4       0      0  ilas-mbp.65485         17.248.213.66.443      ESTABLISHED
tcp4       0      0  ilas-mbp.65484         17.248.213.68.443      TIME_WAIT
tcp4       0      0  ilas-mbp.65474         188.114.99.224.443     ESTABLISHED
tcp4       0      0  ilas-mbp.65472         188.114.98.224.443     TIME_WAIT
tcp4       0      0  ilas-mbp.65348         ec2-52-207-122-5.443   ESTABLISHED
tcp4       0      0  ilas-mbp.65290         ec2-52-70-125-53.443   ESTABLISHED
tcp4       0      0  ilas-mbp.65261         17.57.146.56.5223      ESTABLISHED
udp4       0      0  ilas-mbp.53521         25.224.186.35.bc.https
udp4       0      0  ilas-mbp.49484         25.224.186.35.bc.https
udp4       0      0  ilas-mbp.57850         25.224.186.35.bc.https
udp4       0      0  ilas-mbp.54513         18.224.186.35.bc.https
```

- Получите список активных TCP-соединений локального компьютера без преобразования IP-адресов в символьные имена DNS. (Выпишите команду с помощью которой это можно выполнить.)

```
→  ~ netstat -n
Active Internet connections
Proto Recv-Q Send-Q  Local Address          Foreign Address        (state)
tcp4       0      0  192.168.100.3.64889    149.154.167.223.443    ESTABLISHED
tcp4       0      0  192.168.100.3.64888    149.154.167.223.443    ESTABLISHED
tcp4       0      0  192.168.100.3.64883    149.154.167.223.443    ESTABLISHED
tcp4       0      0  192.168.100.3.64882    149.154.167.223.443    ESTABLISHED
tcp4       0      0  192.168.100.3.64879    149.154.167.43.443     ESTABLISHED
tcp4       0      0  192.168.100.3.64730    149.154.167.51.443     ESTABLISHED
tcp4       0      0  192.168.100.3.64679    35.186.224.33.443      ESTABLISHED
tcp4       0      0  192.168.100.3.64677    64.233.161.188.443     ESTABLISHED
tcp4       0      0  192.168.100.3.64657    149.154.167.41.443     ESTABLISHED
tcp4       0      0  192.168.100.3.64885    188.114.99.224.443     TIME_WAIT
tcp4       0      0  192.168.100.3.65494    17.248.213.70.443      TIME_WAIT
tcp4       0      0  192.168.100.3.65493    17.248.213.71.443      ESTABLISHED
tcp4       0      0  192.168.100.3.65492    142.251.1.207.443      TIME_WAIT
tcp4       0      0  192.168.100.3.65491    17.248.213.71.443      TIME_WAIT
tcp4       0      0  192.168.100.3.65490    2.20.28.26.443         ESTABLISHED
tcp4       0      0  192.168.100.3.65474    188.114.99.224.443     ESTABLISHED
tcp4       0      0  192.168.100.3.65348    52.207.122.56.443      ESTABLISHED
tcp4       0      0  192.168.100.3.65290    52.70.125.53.443       ESTABLISHED
tcp4       0      0  192.168.100.3.65261    17.57.146.56.5223      ESTABLISHED
```

- Какой результат выдаст утилита netstat с параметрами -a -s -r (три параметра одновременно)? Поясните полученный результат.

  -a отобразит все подключения и порты прослушивания.
  -r отобразит таблицы маршрутов.
  -s отобразит статистики по протоколам. По умолчанию для IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, UDPv6.

udp:
513263 datagrams received

0 with incomplete header
0 with bad data length field 0 with bad checksum
26 with no checksum
30 checksummed in software

20 datagrams (1850 bytes) over IPv4

10 datagrams (620 bytes) over IPv6

18547 dropped due to no socket

405 broadcast/multicast datagrams undelivered

0 time multicast source filter matched
46 dropped due to full socket buffers
0 not for hashed pcb

494265 delivered

235743 datagrams output

46979 checksummed in software
3319 datagrams (417334 bytes) over IPv4

43660 datagrams (20251666 bytes) over IPv6

ip:
2358077 total packets received

0 bad header checksum
450094 headers (9004808 bytes) checksummed in software

0 with size smaller than minimum
0 with data size < data length
273 with data size > data length

0 packet forced to software checksum

0 with ip length > max ip packet size
0 with header length < data size
0 with data length < header length
0 with bad options
0 with incorrect version number

0 fragment received
0 dropped (dup or out of space)

0 dropped after timeout

0 reassembled ok

2374564 packets for this host

2987 packets for unknown/unsupported protocol
0 packet forwarded (0 packet fast forwarded)

0 packet not forwardable
244 packets received for unknown multicast group

0 redirect sent

6535 input packets not chained due to collision
1400381 input packets processed in a chain
1278 input packets unable to chain
154391 input packet chains processed with length greater than 2

47656 input packet chains processed with length greater than 4

949883 input packets did not go through list processing path

0 input packet that passed the weak ES interface address match

362 input packets with no interface address match

2115809 packets sent from this host

390 packets sent with fabricated ip header
0 output packet dropped due to no bufs, etc.
48 output packets discarded due to no route
0 output datagram fragmented
0 fragment created
0 datagram that can't be fragmented
0 tunneling packet that can't find gif
0 datagram with bad address in header
20 packets dropped due to no bufs for control data
0 packet dropped due to NECP policy
2097871 headers (41969284 bytes) checksummed in software

icmp:

18547 calls to icmp_error

0 error not generated 'cuz old message was icmp

Output histogram:

echo reply: 14060

destination unreachable: 18547

0 message with bad code fields

0 message < minimum length
72 bad checksums
0 message with bad length
0 multicast echo requests ignored
0 multicast timestamp requests ignored

Input histogram:

echo reply: 16325
destination unreachable: 3167

echo: 14060
time exceeded: 99

14060 message responses generated

ICMP address mask responses are disabled

igmp:

555 messages received
0 message received with too few bytes
0 message received with wrong TTL
0 message received with bad checksum
308 V1/V2 membership queries received
0 V3 membership queries received

0 membership queries received with invalid field(s)
228 general queries received
80 group queries received
0 group-source queries received
0 group-source queries dropped
247 membership reports received
0 membership report received with invalid field(s)
247 membership reports received for groups to which we belong 0 V3 report received without Router Alert
2957 membership reports sent

ipsec:

0 inbound packet processed successfully
0 inbound packet violated process security policy 0 inbound packet with no SA available
0 invalid inbound packet
0 inbound packet failed due to insufficient memory 0 inbound packet failed getting SPI
0 inbound packet failed on AH replay check
0 inbound packet failed on ESP replay check
0 inbound packet considered authentic by AH
0 inbound packet failed on AH authentication
0 inbound packet considered authentic by ESP
0 inbound packet failed on ESP authentication
0 outbound packet processed successfully
0 outbound packet violated process security policy 0 outbound packet with no SA available
0 invalid outbound packet

0 outbound packet failed due to insufficient memory

0 outbound packet with no route

arp:

685 broadast ARP requests sent
8 unicast ARP requests sent
5177 ARP replies sent
0 ARP announcement sent
28708 ARP requests received 2166 ARP replies received
30915 total ARP packets received 0 ARP conflict probe sent

0 invalid ARP resolve request
0 total packet dropped due to lack of memory
0 total packet held awaiting ARP reply
1294 total packets dropped due to no ARP entry
127 total packets dropped during ARP entry removal 14 ARP entries timed out
0 Duplicate IP seen

mptcp:

0 data packet sent

0 data byte sent
0 data packet received
0 data byte received
0 packet with an invalid MPCAP option
0 packet with an invalid MPJOIN option
0 time primary subflow fell back to TCP
0 time secondary subflow fell back to TCP
0 DSS option drop
0 other invalid MPTCP option
0 time the MPTCP subflow window was reduced 0 bad DSS checksum
0 time received out of order data
0 subflow switch
0 subflow switch due to advisory
0 subflow switch due to rtt
0 subflow switch due to rto
0 subflow switch due to peer
0 number of subflow probe

ip6:

45649 total packets received

0 with size smaller than minimum 0 with data size < data length
4 with data size > data length

0 packet forced to software checksum

0 with bad options

0 with incorrect version number

0 fragment received

0 dropped (dup or out of space)

0 dropped after timeout
0 exceeded limit
0 reassembled ok

0 atomic fragments received

45319 packets for this host

0 input packet that passed the weak ES interface address match

0 input packet with no interface address match
0 packet forwarded
114 packets not forwardable

0 redirect sent
114 multicast packets which we didn't join
0 packet whose headers are not continuous
0 tunneling packet that can't find gif
0 packet discarded due to too may headers
0 forward cache hit
0 forward cache miss
0 packet dropped due to no bufs for control data
0 input packet dropped due to too short length
0 input packet dropped due to missing CLAT46 IPv6 address
0 input packet dropped due to missing CLAT46 IPv4 address
0 input packet dropped due to CLAT46 IPv4 address derivation failure

0 input packet dropped due to CLAT46 IP header translation failure
0 input packet dropped due to CLAT46 protocol translation failure
0 input packet dropped due to CLAT46 fragment translation failure
0 input packet dropped due to invalid pbuf
0 input IPv4 packet dropped on CLAT46 enabled interface
0 input packet dropped due to CLAT46 failures
0 input packet successfully translated from IPv6 to IPv4

46676 packets sent from this host

0 packet sent with fabricated ip header
0 output packet dropped due to no bufs, etc.

19356 output packets discarded due to no route

0 output datagram fragmented
0 fragment created
0 datagram that can't be fragmented

0 packet that violated scope rules
0 packet dropped due to NECP policy
0 output packet dropped due to missing CLAT46 IPv6 address
0 output packet dropped due to CLAT46 IPv6 address synthesis failure

0 output packet dropped due to CLAT46 IP header translation failure
0 output packet dropped due to CLAT46 protocol translation failure
0 output packet dropped due to CLAT46 fragment translation failure
0 output packet dropped due to invalid pbuf
0 output packet dropped due to CLAT46 failures
0 output packet successfully translated from IPv4 to IPv6

Input histogram:

hop by hop: 79

TCP: 2

UDP: 45162

ICMP6: 407

Mbuf statistics:

63 one mbuf

two or more mbuf:

lo0= 43527

(null)= 31

(null)= 7

2022 one ext mbuf

0 two or more ext mbuf
0 failure of source address selection

source addresses on an outgoing I/F

0 addresses scope=0

0 node-local
0 link-local
0 addresses scope=3

0 addresses scope=4

0 site-local

0 addresses scope=6

0 addresses scope=7

0 addresses scope=8

0 addresses scope=9

0 addresses scope=a

0 addresses scope=b

0 addresses scope=c

0 addresses scope=d

0 global

0 addresses scope=f

source addresses on a non-outgoing I/F

0 addresses scope=0

0 node-local
0 link-local
0 addresses scope=3

0 addresses scope=4

0 site-local

0 addresses scope=6

0 addresses scope=7

0 addresses scope=8

0 addresses scope=9

0 addresses scope=a

0 addresses scope=b

0 addresses scope=c

0 addresses scope=d

0 global

0 addresses scope=f

source addresses of same scope

0 addresses scope=0

0 node-local
0 link-local
0 addresses scope=3

0 addresses scope=4

0 site-local

0 addresses scope=6

0 addresses scope=7

0 addresses scope=8

0 addresses scope=9

0 addresses scope=a

0 addresses scope=b

0 addresses scope=c

0 addresses scope=d

0 global

0 addresses scope=f

source addresses of a different scope

0 addresses scope=0

0 node-local
0 link-local
0 addresses scope=3

0 addresses scope=4

0 site-local

0 addresses scope=6

0 addresses scope=7

0 addresses scope=8

0 addresses scope=9

0 addresses scope=a

0 addresses scope=b

0 addresses scope=c

0 addresses scope=d

0 global

0 addresses scope=f

deprecated source addresses

0 addresses scope=0

0 node-local
0 link-local
0 addresses scope=3

0 addresses scope=4

0 site-local

0 addresses scope=6

0 addresses scope=7

0 addresses scope=8

0 addresses scope=9

0 addresses scope=a

0 addresses scope=b

0 addresses scope=c

0 addresses scope=d

0 global

0 addresses scope=f

source address selection

21549 rules default

0 rule prefer same address

1 rule prefer appropriate scope

0 rule avoid deprecated addresses

0 rule prefer home addresses

0 rule prefer outgoing interface

0 rule prefer matching label

22773 rules prefer temporary addresses

0 rule prefer addresses on alive interfaces

0 rule use longest matching prefix

0 duplicate address detection collision

0 duplicate address detection NS loop

0 time ignored source on secondary expensive I/F

icmp6:

0 call to icmp_error

0 error not generated because old message was icmp error or so

0 error not generated because rate limitation
Output histogram:

router solicitation: 641

neighbor solicitation: 117

neighbor advertisement: 54 MLDv2

listener report: 2266

0 message with bad code fields

0 message < minimum length

0 bad checksum

0 message with bad length

Input histogram:

router advertisement: 161

neighbor solicitation: 54

neighbor advertisement: 159

Histogram of error messages to be generated:

0 no route

0 administratively prohibited 0 beyond scope
0 address unreachable
0 port unreachable

0 packet too big
0 time exceed transit
0 time exceed reassembly 0 erroneous header field
0 unrecognized next header 0 unrecognized option
0 redirect
0 unknown

0 message response generated
0 message with too many ND options

0 message with bad ND options
0 bad neighbor solicitation message
0 bad neighbor advertisement message

0 bad router solicitation message
0 bad router advertisement message
0 bad redirect message
0 path MTU change
0 dropped fragmented NDP message

ipsec6:

0 inbound packet processed successfully

0 inbound packet violated process security policy

0 inbound packet with no SA available
0 invalid inbound packet
0 inbound packet failed due to insufficient memory

0 inbound packet failed getting SPI

0 inbound packet failed on AH replay check
0 inbound packet failed on ESP replay check
0 inbound packet considered authentic by AH
0 inbound packet failed on AH authentication
0 inbound packet considered authentic by ESP
0 inbound packet failed on ESP authentication
0 outbound packet processed successfully
0 outbound packet violated process security policy

0 outbound packet with no SA available
0 invalid outbound packet
0 outbound packet failed due to insufficient memory

0 outbound packet with no route

rip6:

0 message received

0 checksum calculation on inbound
0 message with bad checksum
0 message dropped due to no socket
0 multicast message dropped due to no socket

0 message dropped due to full socket buffers

0 delivered

0 datagram output

pfkey:

0 request sent to userland
0 byte sent to userland
0 message with invalid length field
0 message with invalid version field
0 message with invalid message type field

0 message too short
0 message with memory allocation failure

0 message with duplicate extension
0 message with invalid extension type
0 message with invalid sa type
0 message with invalid address extension

0 request sent from userland
0 byte sent from userland
0 message toward single socket
0 message toward all sockets
0 message toward registered sockets
0 message with memory allocation failure

kevt:

12 current kernel control sockets

68 kernel control generation count 0 bad vendor failure
0 message too big failure
0 out of memory failure

0 message dropped due to full socket buffers

435413 messages posted

kctl:

0 total kernel control module registered
15 current kernel control modules registered
94 current kernel control sockets
3537 kernel control generation count
1808 connection attempts
0 connection failure

19 send failures
0 send list failure
134 enqueue failures
134 packets dropped due to full socket buffers
0 failure with bad kern_ctl_ref
0 register failure because of too many kern_ctl_ref
0 enqueuedata failure because could not allocate a packet

0 enqueuedata failure due to full socket buffers

nstat:

0 enqueue success message failure

0 enqueue source counts message failure

0 enqueue sysinfo message failure
6 enqueue source udpate message failures

0 enqueue description message failure

0 enqueue remove message failure
128 enqueue source added message failures

0 enqueue error message failure
0 copy descriptor failure
0 provider counts failure
0 control send description failure
6 control send goodbye failures
0 flush accumulated messages failure
0 accumulated message failure
0 control cleanup source failure

507211 handle message failures

xbkidle:

1 max per process
600 maximum time (seconds)

131072 high water mark
0 socket option not supported failure

0 too many sockets failure
0 total socket requested OK
0 extended bk idle socket
0 no cellular failure
0 no time failures
0 forced defunct socket
0 resumed socket
0 timeout expired failure
0 timer rescheduled
0 no delegated failure

net_api:

2 interface filters currently attached

2 interface filters currently attached by OS

5 interface filters attached since boot

5 interface filters attached since boot by OS

0 IP filter currently attached

0 interface filter currently attached by OS

0 IP filter attached since boot

0 IP filter attached since boot by OS

4 socket filters currently attached

4 socket filters currently attached by OS

4 socket filters attached since boot

4 socket filters attached since boot by OS

921719 sockets allocated since boot

199133 sockets allocated in-kernel since boot

199133 sockets allocated in-kernel by OS

202 sockets with NECP client UUID since boot

321563 local domain sockets allocated since boot

1963 route domain sockets allocated since boot

489098 inet domain sockets allocated since boot

53979 inet6 domain sockets allocated since boot

1848 system domain sockets allocated since boot

0 multipath domain socket allocated since boot

0 key domain socket allocated since boot

39 ndrv domain sockets allocated since boot

0 other domains socket allocated since boot

42982 IPv4 stream sockets created since boot

446116 IPv4 datagram sockets created since boot

14342 IPv4 datagram sockets connected

60271 IPv4 DNS sockets

389497 IPv4 datagram sockets without data

6126 IPv6 stream sockets created since boot

47853 IPv6 datagram sockets created since boot

10940 IPv6 datagram sockets connected

0 IPv6 DNS socket

47762 IPv6 datagram sockets without data

7336 socket multicast joins since boot

7336 socket multicast joins since boot by OS

0 IPv4 stream nexus flow added since boot

249 IPv4 datagram nexus flows added since boot

20621 IPv6 stream nexus flows added since boot

10641 IPv6 datagram nexus flows added since boot

18 interfaces currently allocated

23 interfaces allocated since boot

18 interfaces currently allocated by OS

23 extended interfaces allocated since boot by OS

28 PF addrule operations since boot

28 PF addrule operations since boot by OS

3 vmnet starts since boot

if_ports_used:

70 wakeuuid generations

93 offload port list queries with wakeuuid not set 10475 total offload port entries created since boot 28 current offload port entries
1274 max offload port entries

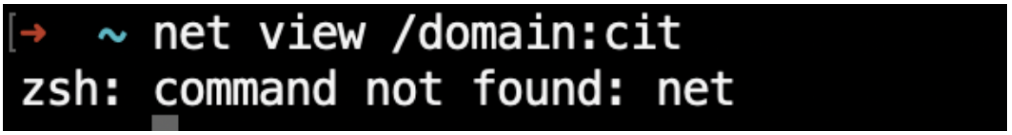
43067 duplicate offload port entries 280427 total table entry searches 51 max hash table entry searches
0 match so wake packet call

38 match ch wake packet calls 38 IPv4 wake packets
0 IPv6 wake packet
38 TCP wake packets

0 UDP wake packet
0 ISAKMP NAT traversal wake packet 0 ESP wake packet
0 bad protocol wake packet

0 bad family wake packet
8 wake packet events
30 duplicate wake packet events in same wake cycle
0 wake packet event undelivered
0 unattributed wake packet event
0 duplicate unattributed wake packet event in same wake cycle 0 unattributed wake packet event undelivered
0 unattributed wake packet received with null interface
0 bad packet without wake flag
0 pure fragment wake packet
0 packet with incomplete TCP header
0 packet with incomplete UDP header
0 port entry not added with wakeuuid not set
0 deferred matching of ISAKMP NAT traversal wake packet

4.3.9. ***Задание 9.*** **Утилита Net view.** Исследовать ресурсы доменов cit, fpmi или любого другого домена на ваше усмотрение с помощью команды net view.



4.3.10. ***Задание 10.*** Получите таблицу маршрутизации локального компьютера. Как это можно сделать.

```
➜  ~ netstat -nr
Routing tables

Internet:
Destination        Gateway            Flags               Netif Expire
default            192.168.100.1      UGScg                 en0
127                127.0.0.1          UCS                   lo0
127.0.0.1          127.0.0.1          UH                    lo0
169.254            link#11            UCS                   en0      !
192.168.100        link#11            UCS                   en0      !
192.168.100.1/32   link#11            UCS                   en0      !
192.168.100.1      f4:b8:a7:bc:46:de  UHLWIir               en0   1178
192.168.100.3/32   link#11            UCS                   en0      !
192.168.100.3      a0:78:17:9b:d2:1f  UHLWIi                lo0
192.168.100.8      7c:e9:d3:56:1c:47  UHLWI                 en0      !
192.168.100.54     dc:71:44:9c:54:a7  UHLWI                 en0   1198
192.168.100.55     78:ab:bb:bd:c9:78  UHLWI                 en0   1198
192.168.100.255    ff:ff:ff:ff:ff:ff  UHLWbI                en0      !
224.0.0/4          link#11            UmCS                  en0      !
224.0.0.251        1:0:5e:0:0:fb      UHmLWI                en0
239.255.255.250    1:0:5e:7f:ff:fa    UHmLWI                en0
255.255.255.255/32 link#11            UCS                   en0      !

Internet6:
Destination                             Gateway                                 Flags               Netif Expire
default                                 fe80::1%en0                             UGcIg                 en0
default                                 fe80::%utun0                            UGcIg               utun0
default                                 fe80::%utun1                            UGcIg               utun1
default                                 fe80::%utun2                            UGcIg               utun2
default                                 fe80::%utun3                            UGcIg               utun3
::1                                     ::1                                     UHL                   lo0
fe80::%lo0/64                           fe80::1%lo0                             UcI                   lo0
fe80::1%lo0                             link#1                                  UHLI                  lo0
fe80::%en0/64                           link#11                                 UCI                   en0
fe80::1%en0                             f4:b8:a7:bc:46:de                       UHLWIir               en0
fe80::1c80:feb1:9c11:f764%en0           a0:78:17:9b:d2:1f                       UHLI                  lo0
fe80::e464:63ff:fe84:3ae8%awdl0         e6:64:63:84:3a:e8                       UHLI                  lo0
fe80::e464:63ff:fe84:3ae8%llw0          e6:64:63:84:3a:e8                       UHLI                  lo0
fe80::%utun0/64                         fe80::a8c4:6a2f:3450:3a20%utun0         UcI                 utun0
fe80::a8c4:6a2f:3450:3a20%utun0         link#15                                 UHLI                  lo0
fe80::%utun1/64                         fe80::4f9c:eea4:912c:4137%utun1         UcI                 utun1
fe80::4f9c:eea4:912c:4137%utun1         link#16                                 UHLI                  lo0
fe80::%utun2/64                         fe80::ce81:b1c:bd2c:69e%utun2           UcI                 utun2
fe80::ce81:b1c:bd2c:69e%utun2           link#17                                 UHLI                  lo0
fe80::%utun3/64                         fe80::dcc4:31c5:90fe:5b70%utun3         UcI                 utun3
fe80::dcc4:31c5:90fe:5b70%utun3         link#18                                 UHLI                  lo0
ff00::/8                                ::1                                     UmCI                  lo0
ff00::/8                                link#11                                 UmCI                  en0
ff00::/8                                link#12                                 UmCI                awdl0
ff00::/8                                link#13                                 UmCI                llw0
ff00::/8                                fe80::a8c4:6a2f:3450:3a20%utun0         UmCI                utun0
ff00::/8                                fe80::4f9c:eea4:912c:4137%utun1         UmCI                utun1
ff00::/8                                fe80::ce81:b1c:bd2c:69e%utun2           UmCI                utun2
ff00::/8                                fe80::dcc4:31c5:90fe:5b70%utun3         UmCI                utun3
ff01::%lo0/32                           ::1                                     UmCI                  lo0
ff01::%en0/32                           link#11                                 UmCI                  en0
ff01::%utun0/32                         fe80::a8c4:6a2f:3450:3a20%utun0         UmCI                utun0
ff01::%utun1/32                         fe80::4f9c:eea4:912c:4137%utun1         UmCI                utun1
ff01::%utun2/32                         fe80::ce81:b1c:bd2c:69e%utun2           UmCI                utun2
ff01::%utun3/32                         fe80::dcc4:31c5:90fe:5b70%utun3         UmCI                utun3
ff02::%lo0/32                           ::1                                     UmCI                  lo0
ff02::%en0/32                           link#11                                 UmCI                  en0
ff02::%utun0/32                         fe80::a8c4:6a2f:3450:3a20%utun0         UmCI                utun0
ff02::%utun1/32                         fe80::4f9c:eea4:912c:4137%utun1         UmCI                utun1
ff02::%utun2/32                         fe80::ce81:b1c:bd2c:69e%utun2           UmCI                utun2
ff02::%utun3/32                         fe80::dcc4:31c5:90fe:5b70%utun3         UmCI                utun3
```

11. ***Задание 11.*** Приведите пример отправки сообщения соседу в дисплейном классе.

```
➜  ~ echo "Привет, мир!" | nc 10.150.1.3 1234

dquote>
```