

CS305B Lab1 Report

11812418 樊青远 Fan Qingyuan

Q1

Use the ipconfig command to query the local ip, subnet mask, gateway, MAC address, and screenshot instructions.

```
>ifconfig
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 38:f9:d3:75:70:88
    inet6 fe80::472:9e7f:3642:1950%en0 prefixlen 64 secured scopeid 0xa
    inet 10.17.120.246 netmask 0xfffff8000 broadcast 10.17.127.255
    inet6 2001:da8:201d:1109::f762 prefixlen 128 dynamic
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
```

```

cyf@LAPTOP-TMBP81 ~ - zsh - 90x36
[ 10021 23:22:31 ]
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC20: flags=0<> mtu 0
XHC0: flags=0<> mtu 0
XHC1: flags=0<> mtu 0
VHC128: flags=0<> mtu 0
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether ac:de:48:00:11:22
    inet6 fe80::aede:48ff:fe00:1122%en5 prefixlen 64 scopeid 0x8
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (100baseTX <full-duplex>)
        status: active
ap1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 3a:f9:d3:75:70:88
        media: autoselect
        status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=400<CHANNEL_IO>
    ether 38:f9:d3:75:70:88
    inet6 fe80::472:9e7f:3642:1950%en0 prefixlen 64 secured scopeid 0xa
        inet 10.17.120.246 netmask 0xffff8000 broadcast 10.17.127.255
        inet6 2001:da8:201d:1109::f762 prefixlen 128 dynamic
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
feth5391: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    ether 66:65:74:68:15:0f
    peer: feth391

```

Result

Parameters	Value
Local IP	10.17.120.246
Subnet mask	0xffff8000 (255.255.128.0)
Gateway	10.17.127.255
MAC address	38:f9:d3:75:70:88

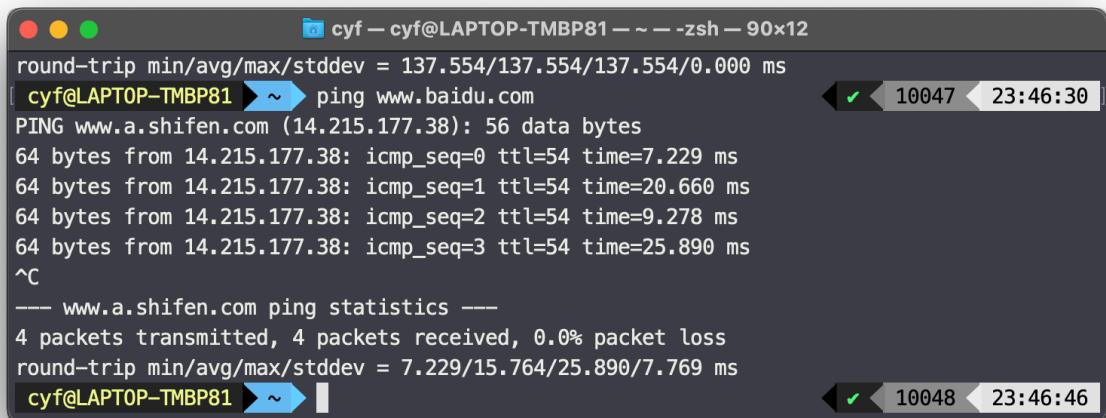
Q2

Ping www.baidu.com and ping www.sustc.edu.cn, the screenshot gives a brief description of the echo message (whether the destination host is reachable, the communication duration, the TTL value)

ping www.baidu.com

```
>ping www.baidu.com
PING www.a.shifen.com (14.215.177.38): 56 data bytes
64 bytes from 14.215.177.38: icmp_seq=0 ttl=54 time=7.229 ms
64 bytes from 14.215.177.38: icmp_seq=1 ttl=54 time=20.660 ms
64 bytes from 14.215.177.38: icmp_seq=2 ttl=54 time=9.278 ms
64 bytes from 14.215.177.38: icmp_seq=3 ttl=54 time=25.890 ms
^C
--- www.a.shifen.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 7.229/15.764/25.890/7.769 ms
```

Screenshot



```
cyf@LAPTOP-TMBP81 ~ zsh 90x12
round-trip min/avg/max/stddev = 137.554/137.554/137.554/0.000 ms
[ cyf@LAPTOP-TMBP81 ~ ] ping www.baidu.com
PING www.a.shifen.com (14.215.177.38): 56 data bytes
64 bytes from 14.215.177.38: icmp_seq=0 ttl=54 time=7.229 ms
64 bytes from 14.215.177.38: icmp_seq=1 ttl=54 time=20.660 ms
64 bytes from 14.215.177.38: icmp_seq=2 ttl=54 time=9.278 ms
64 bytes from 14.215.177.38: icmp_seq=3 ttl=54 time=25.890 ms
^C
--- www.a.shifen.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 7.229/15.764/25.890/7.769 ms
cyf@LAPTOP-TMBP81 ~ ]
```

ping www.sustc.edu.cn

```
>ping www.sustc.edu.cn
PING www.sustc.edu.cn (172.18.8.244): 56 data bytes
64 bytes from 172.18.8.244: icmp_seq=0 ttl=62 time=2.850 ms
64 bytes from 172.18.8.244: icmp_seq=1 ttl=62 time=21.632 ms
64 bytes from 172.18.8.244: icmp_seq=2 ttl=62 time=21.563 ms
64 bytes from 172.18.8.244: icmp_seq=3 ttl=62 time=10.690 ms
^C
--- www.sustc.edu.cn ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.850/14.184/21.632/7.915 ms
```

Screenshot

```
cyf@LAPTOP-TMBP81: ~ round-trip min/avg/max/stddev = 7.229/15.764/25.890/7.769 ms
PING www.sustc.edu.cn (172.18.8.244): 56 data bytes
64 bytes from 172.18.8.244: icmp_seq=0 ttl=62 time=2.850 ms
64 bytes from 172.18.8.244: icmp_seq=1 ttl=62 time=21.632 ms
64 bytes from 172.18.8.244: icmp_seq=2 ttl=62 time=21.563 ms
64 bytes from 172.18.8.244: icmp_seq=3 ttl=62 time=10.690 ms
^C
--- www.sustc.edu.cn ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.850/14.184/21.632/7.915 ms
cyf@LAPTOP-TMBP81: ~
```

Q3

Use the netstat command to check the traffic statistics on the local Ethernet card and take a screenshot

```
cyf@LAPTOP-TMBP81: ~ netstat -a
Active Internet connections
Proto Recv-Q Send-Q Local Address        Foreign Address      (state)
tcp4   0      0    10.17.120.246.53293  196.55.215.129.https  SYN_SENT
tcp4   0      0    10.17.120.246.53276  40.70.161.102.https  ESTABLISHED
tcp6   0      0    2001:da8:201d:11.53269  2001::68f4:2eb9.https  SYN_SENT
tcp4   0      0    10.17.120.246.53268  ec2-54-234-18-20.https  SYN_SENT
tcp4   0      0    10.17.120.246.53251  tr.sn.sparktour..28007  ESTABLISHED
tcp4   0      0    localhost.7891       localhost.53250       ESTABLISHED
tcp4   0      0    localhost.53250       localhost.7891       ESTABLISHED
tcp4   0      0    10.17.120.246.53210  101.230.204.226.https  ESTABLISHED
tcp4   0      0    10.17.120.246.53195  17.141.128.198.https  ESTABLISHED
tcp4   0      0    10.17.120.246.53187  17.141.128.198.https  ESTABLISHED
tcp4   0      0    10.17.120.246.53186  101.230.204.226.https  ESTABLISHED
tcp4   0      0    10.17.120.246.53183  17.141.128.198.https  ESTABLISHED
tcp4   0      0    10.17.120.246.53115  159.240.178.107..https ESTABLISHED
tcp4   0      0    10.17.120.246.52996  tr.sn.sparktour..28007  ESTABLISHED
tcp4   0      0    localhost.7891       localhost.52995       ESTABLISHED
tcp4   0      0    localhost.52995       localhost.7891       ESTABLISHED
tcp4   0      0    10.17.120.246.52994  tr.sn.sparktour..28007  ESTABLISHED
tcp4   0      0    localhost.7891       localhost.52993       ESTABLISHED
tcp4   0      0    localhost.52993       localhost.7891       ESTABLISHED
```

Q4

Use the tracert command to access www.baidu.com and take a screenshot analysis to mark the total number of hops from the host to the destination host, whether there is any icmp packet loss, and the ip address of the server where www.baidu.com is located.

```
cyf - cyf@LAPTOP-TMBP81 -- -zsh - 94x23
tcp4      31      0  10.17.120.246.60470    172.18.1.222.https    CLOSE_WAIT
tcp4      31      0  10.17.120.246.60469    172.18.1.222.https    CLOSE_WAIT
tcp4      31      0  10.17.120.246.60467    172.18.1.222.https    CLOSE_WAIT
^C
[ cyf@LAPTOP-TMBP81 ~ ] traceroute www.baidu.com          SIGINT(2) ↵ 10050 23:48:52 ]
traceroute: Warning: www.baidu.com has multiple addresses; using 14.215.177.38
traceroute to www.a.shifen.com (14.215.177.38), 64 hops max, 52 byte packets
 1  10.10.10.11 (10.10.10.11)  2.856 ms  2.745 ms  3.201 ms
 2  10.23.255.83 (10.23.255.83)  2.234 ms  2.151 ms  2.164 ms
 3  group01.its.sustc.edu.cn (116.7.234.1)  4.955 ms  3.040 ms  4.223 ms
 4  183.56.64.1 (183.56.64.1)  14.984 ms  12.452 ms  6.378 ms
 5  125.176.37.59.broad.dg.dynamic.163data.com.cn (59.37.176.125)  4.065 ms
   117.176.37.59.broad.dg.dynamic.163data.com.cn (59.37.176.117)  3.946 ms  2.704 ms
 6  * * 202.105.106.49 (202.105.106.49)  4.759 ms
 7  113.96.4.246 (113.96.4.246)  31.929 ms
   113.96.4.250 (113.96.4.250)  19.932 ms
   113.96.5.102 (113.96.5.102)  22.084 ms
 8  * * 86.96.135.219.broad.fs.gd.dynamic.163data.com.cn (219.135.96.86)  10.370 ms
 9  86.96.135.219.broad.fs.gd.dynamic.163data.com.cn (219.135.96.86)  10.171 ms  12.806 ms
   14.29.117.234 (14.29.117.234)  7.341 ms
10  * 14.215.32.94 (14.215.32.94)  36.946 ms *
11  * * *
12  * * *
```

```
cyf - sudo mtr 14.215.177.38 -n - mtr - mtr - sudo - 90x19
My traceroute [v0.93]
LAPTOP-TMBP81.local (10.17.120.246) 2021-01-14T11:10:59+0800
Keys: Help  Display mode  Restart statistics  Order of fields  quit
          Packets                      Pings
Host        Loss%     Snt   Last    Avg   Best Wrst StDev
1. 10.10.10.11          0.0%    16   4.1  30.1   2.2 284.2  70.8
2. 10.23.255.83          0.0%    16   5.4  16.7   2.6 197.3  48.3
3. 116.7.234.1           0.0%    15  15.5 101.7  13.7 232.6  97.9
4. 183.56.64.9            0.0%    15  32.0 114.4  15.8 218.4  72.1
5. 59.37.176.117          14.3%   15 225.6  67.5  11.6 225.6  66.9
6. 59.38.107.177          0.0%    15 172.7  40.1  11.2 172.7  51.8
7. 113.96.4.250           42.9%   15  18.7  23.9  18.2  40.9   7.5
8. 219.135.96.94          0.0%    15  19.9  56.0  13.0 295.3  89.9
9. 14.29.121.186          0.0%    15  19.6 104.5  16.3 237.7  95.9
10. (waiting for reply)
11. (waiting for reply)
12. 14.215.177.38          0.0%    15  58.2  44.9  14.8 367.1  89.9
```

The total number of hops from the host to the destination host is 12. (The traceroute program always indicates that the packet was lost at the 12th hop, so the result is obtained from mtr)

There are packet loss at the 6th, 6th, 10th of the hops from the traceroute result.

The IP address of the baidu server is `14.215.177.38`.

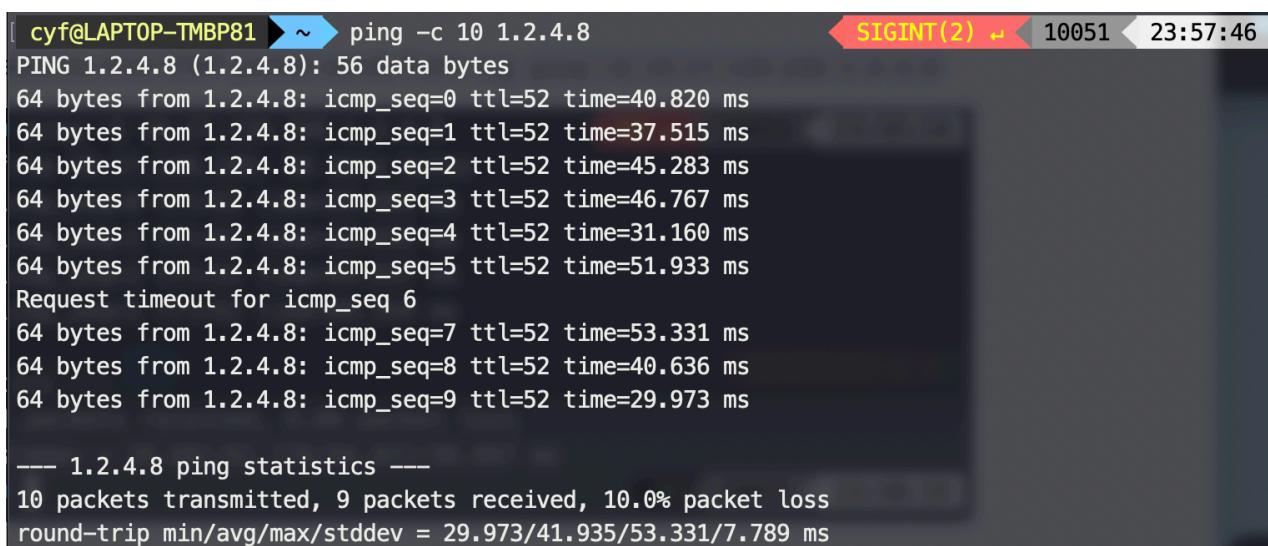
Q5

In this lab class, list the commands that requires addition parameters to run. Use these commands and parameters (each command chooses 2 or 3 of them to experiment), take a screenshot and explain its function.

ping

```
usage: ping [-AaDdfnoQqRrv] [-c count] [-G sweepmaxsize]
            [-g sweepminsize] [-h sweepincrsize] [-i wait]
            [-l preload] [-M mask | time] [-m ttl] [-p pattern]
            [-S src_addr] [-s packetsize] [-t timeout][ -W waittime]
            [-z tos] host
ping [-AaDdfLnoQqRrv] [-c count] [-I iface] [-i wait]
      [-l preload] [-M mask | time] [-m ttl] [-p pattern] [-S src_addr]
      [-s packetsize] [-T ttl] [-t timeout] [-W waittime]
      [-z tos] mcast-group
Apple specific options (to be specified before mcast-group or host like all
options)
      -b boundif          # bind the socket to the interface
      -k traffic_class    # set traffic class socket option
      -K net_service_type # set traffic class socket options
      -apple-connect      # call connect(2) in the socket
      -apple-time         # display current time
```

`ping -c` means the count the `ping` command runs. e.g. `ping -c 10 1.2.4.8`



```
| cyf@LAPTOP-TMBP81 ~ ping -c 10 1.2.4.8           SIGINT(2) ↵ 10051 23:57:46
PING 1.2.4.8 (1.2.4.8): 56 data bytes
64 bytes from 1.2.4.8: icmp_seq=0 ttl=52 time=40.820 ms
64 bytes from 1.2.4.8: icmp_seq=1 ttl=52 time=37.515 ms
64 bytes from 1.2.4.8: icmp_seq=2 ttl=52 time=45.283 ms
64 bytes from 1.2.4.8: icmp_seq=3 ttl=52 time=46.767 ms
64 bytes from 1.2.4.8: icmp_seq=4 ttl=52 time=31.160 ms
64 bytes from 1.2.4.8: icmp_seq=5 ttl=52 time=51.933 ms
Request timeout for icmp_seq 6
64 bytes from 1.2.4.8: icmp_seq=7 ttl=52 time=53.331 ms
64 bytes from 1.2.4.8: icmp_seq=8 ttl=52 time=40.636 ms
64 bytes from 1.2.4.8: icmp_seq=9 ttl=52 time=29.973 ms

--- 1.2.4.8 ping statistics ---
10 packets transmitted, 9 packets received, 10.0% packet loss
round-trip min/avg/max/stddev = 29.973/41.935/53.331/7.789 ms
```

`ping -s` means specific the address that ICMP packet sends from. e.g. `ping -s 10.17.120.246 1.2.4.8`

```

cyf@LAPTOP-TMBP81 ~ ping -S 10.17.120.246 1.2.4.8
PING 1.2.4.8 (1.2.4.8) from 10.17.120.246: 56 data bytes
64 bytes from 1.2.4.8: icmp_seq=0 ttl=52 time=29.681 ms
64 bytes from 1.2.4.8: icmp_seq=1 ttl=52 time=33.832 ms
64 bytes from 1.2.4.8: icmp_seq=2 ttl=52 time=94.037 ms
64 bytes from 1.2.4.8: icmp_seq=3 ttl=52 time=89.554 ms
^C
--- 1.2.4.8 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 29.681/61.776/94.037/30.097 ms
cyf@LAPTOP-TMBP81 ~

```

Traceroute

```

Version 1.4a12+Darwin
Usage: traceroute [-adDefInrSvx] [-A as_server] [-f first_ttl] [-g gateway] [-i
iface]
[-M first_ttl] [-m max_ttl] [-p port] [-P proto] [-q nqueries] [-s src_addr]
[-t tos] [-w waittime] [-z pausemsecs] host [packetlen]

```

`traceroute -i` means traceroute using the specific interface. e.g. `traceroute -i en0 1.0.0.1`

```

cyf@LAPTOP-TMBP81 ~ traceroute -i en0 1.0.0.1
traceroute to 1.0.0.1 (1.0.0.1), 64 hops max, 52 byte packets
 1  10.10.10.11 (10.10.10.11)  2.604 ms  2.210 ms  2.138 ms
 2  10.23.255.83 (10.23.255.83)  2.110 ms  3.756 ms  2.132 ms
 3  116.6.234.129 (116.6.234.129)  7.828 ms  5.735 ms  6.665 ms
 4  17.186.37.59.broad.dg.gd.dynamic.163data.com.cn (59.37.186.17)  3.611 ms  5.213 ms
   21.186.37.59.broad.dg.gd.dynamic.163data.com.cn (59.37.186.21)  4.238 ms
  5  * 125.176.37.59.broad.dg.gd.dynamic.163data.com.cn (59.37.176.125)  11.891 ms *
  6  113.104.38.59.broad.fs.gd.dynamic.163data.com.cn (59.38.104.113)  11.758 ms
   105.104.38.59.broad.fs.gd.dynamic.163data.com.cn (59.38.104.105)  6.707 ms
   109.104.38.59.broad.fs.gd.dynamic.163data.com.cn (59.38.104.109)  4.899 ms
  7  59.43.132.125 (59.43.132.125)  16.932 ms  8.420 ms  19.230 ms
  8  59.43.130.146 (59.43.130.146)  19.858 ms
   59.43.130.122 (59.43.130.122)  19.067 ms
   59.43.130.126 (59.43.130.126)  13.926 ms
  9  59.43.187.110 (59.43.187.110)  19.328 ms
   59.43.187.114 (59.43.187.114)  18.761 ms  28.732 ms
 10  59.43.250.82 (59.43.250.82)  19.408 ms
   59.43.188.122 (59.43.188.122)  20.418 ms
   59.43.188.126 (59.43.188.126)  18.941 ms
 11  xe-0-0-21-2.a01.chwahk02.hk.bb.gin.ntt.net (203.131.241.69)  18.271 ms  19.314 ms  17.036
ms
 12  ae-15.r03.tkokhk01.hk.bb.gin.ntt.net (129.250.5.162)  18.594 ms
   ae-14.r03.tkokhk01.hk.bb.gin.ntt.net (129.250.5.178)  15.040 ms
   ae-15.r03.tkokhk01.hk.bb.gin.ntt.net (129.250.5.162)  15.256 ms
 13  203.131.253.202 (203.131.253.202)  16.153 ms  19.592 ms  17.211 ms
 14  one.one.one (1.0.0.1)  15.040 ms  15.258 ms  16.396 ms

```

`traceroute -m` specific the max TTL (Time To Live) for the packet. e.g. `traceroute -m 3 1.0.0.1`

```
[ cyf@LAPTOP-TMBP81 ~ ] traceroute -m 3 1.0.0.1
traceroute to 1.0.0.1 (1.0.0.1), 3 hops max, 52 byte packets
 1  10.10.10.11 (10.10.10.11)  2.962 ms  1.887 ms  5.323 ms
 2  10.23.255.83 (10.23.255.83)  2.440 ms  2.071 ms  2.099 ms
 3  116.6.234.129 (116.6.234.129)  6.593 ms  4.053 ms  5.277 ms
[ cyf@LAPTOP-TMBP81 ~ ]
```

Nslookup

`nslookup -query=AAAA www.cloudflare.com 172.18.1.92` means query the `AAAA` record of `www.cloudflare.com` from DNS server `172.18.1.92`.

```
[ cyf@LAPTOP-TMBP81 ~ ] nslookup -query=AAAA www.cloudflare.com 172.18.1.92
Server:      172.18.1.92
Address:     172.18.1.92#53

Non-authoritative answer:
www.cloudflare.com      has AAAA address 2606:4700::6810:7c60
www.cloudflare.com      has AAAA address 2606:4700::6810:7b60
```

`nslookup -query=TXT xn--g28h.hack.ustclug.org 172.18.1.92` means query the `AAAA` record of `xn--g28h.hack.ustclug.org` from DNS server `172.18.1.92`.

```
[ cyf@LAPTOP-TMBP81 ~ ] nslookup -query=TXT xn--g28h.hack.ustclug.org 172.18.1.92
Server:      172.18.1.92
Address:     172.18.1.92#53

Non-authoritative answer:
xn--g28h.hack.ustclug.org      text = "flag{DN5_C4N_H4VE_em0ji_haha}"
```

Q6

Download and install Wireshark: <https://www.wireshark.org/>

