CS 305 Lab1 Tutorial
Commands for network detection and diagnosis

Dept. Computer Science and Engineering

Southern University of Science and Technology

route -print

DHCP 服务：动态主机配置服务

网络号

↑

十进制

SUSTech
Southern University
of Science and Technology

IPV4 地址：172.18.5.155 32 bit. 网络号+主机号

子网掩码：255.255.255.0 IP & 子网

24

默认网关：172.18.5.254（路由器ip）

Topics

- Learn the usage of network commands. Learn how to use them to conduct network testing, troubleshooting and event detection.
  - ipconfig
  - arp
  - nslookup
  - ping 测试网络连通性 A → B
  - tracert 跟踪路由
  - netstat 收发报文的情况

识别主机标签

物理地址

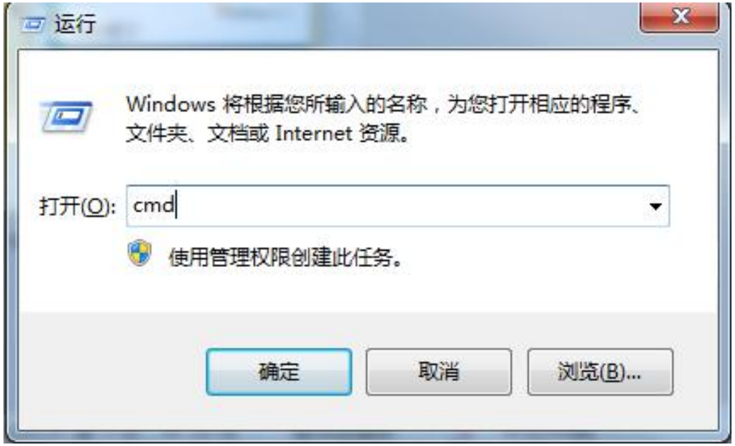
IP地址

域名（提供服务的服务器）

- Understand their working principle and underlying network protocols.

Experimental environment

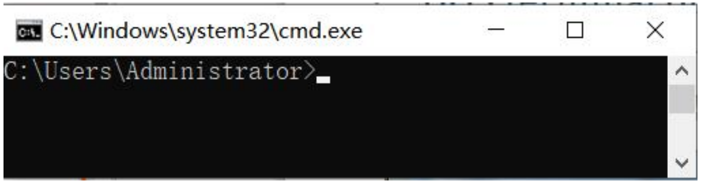
- DOS terminal on Windows 10
  - Click ‘start’ on desktop -> choose ‘run’ ->input ‘cmd’ to invoke the DOS terminal on windows



Windows 将根据您所输入的名称，为您打开相应的程序、文件夹、文档或 Internet 资源。

打开(O): cmd

使用管理权限创建此任务。

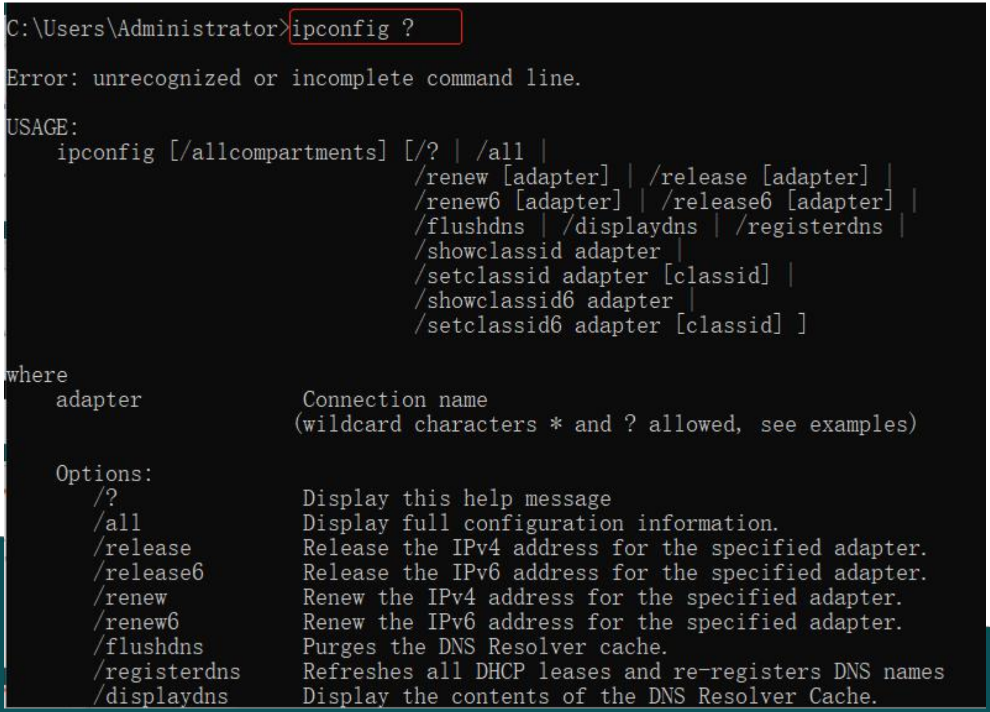


```
C:\Users\Administrator>_
```

1. ipconfig (1)

- “**ipconfig**” is usually used to show the configuration on network adapter.
  - “***ipconfig***” can display the IP address, gateway, network mask of network adapter . “***ipconfig -all***” can display more information.

Tips:
use ‘?’ or ‘-help’ following the commands to get its help information.



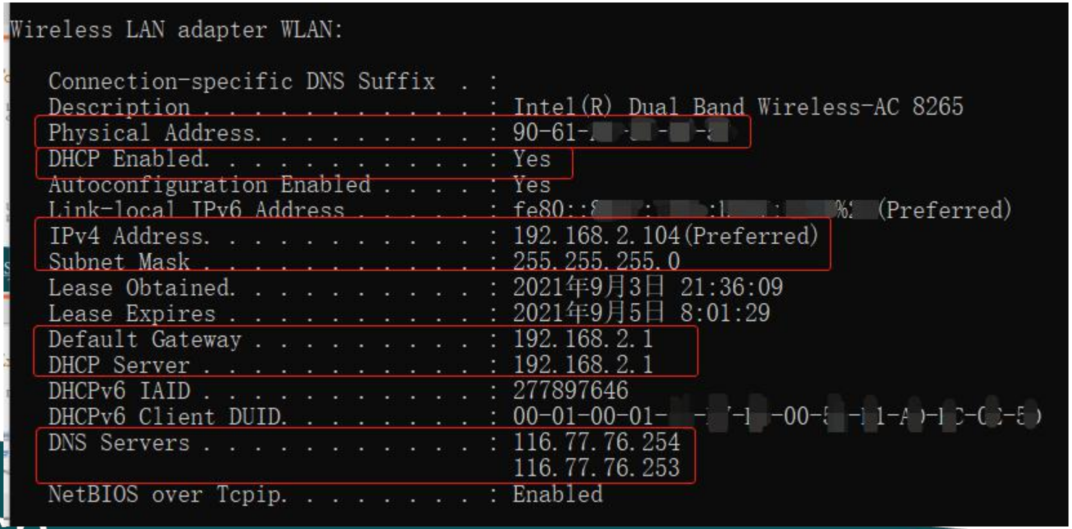
```
C:\Users\Administrator>ipconfig ?

Error: unrecognized or incomplete command line.

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
                       (wildcard characters * and ? allowed, see examples)

    Options:
       /?               Display this help message
       /all             Display full configuration information.
       /release         Release the IPv4 address for the specified adapter.
       /release6        Release the IPv6 address for the specified adapter.
       /renew           Renew the IPv4 address for the specified adapter.
       /renew6          Renew the IPv6 address for the specified adapter.
       /flushdns        Purges the DNS Resolver cache.
       /registerdns     Refreshes all DHCP leases and re-registers DNS names
       /displaydns      Display the contents of the DNS Resolver Cache.
```

1. ipconfig (2)

- Here is a part of information which is displayed while run the command“***ipconfig -all***”

Tips:

1. The Physical address has 48 bits, expressed in hexadecimal
2. IPv4 address and Subnet Mask has 32 bits, expressed in dotted decimal



```
Wireless LAN adapter WLAN:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : 90-61-[redacted]
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::[redacted](Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.2.104(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 2021年9月3日 21:36:09
   Lease Expires . . . . . . . . . . : 2021年9月5日 8:01:29
   Default Gateway . . . . . . . . . : 192.168.2.1
   DHCP Server . . . . . . . . . . . : 192.168.2.1
   DHCPv6 IAID . . . . . . . . . . . : 277897646
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-[redacted]
   DNS Servers . . . . . . . . . . . : 116.77.76.254
                                       116.77.76.253
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

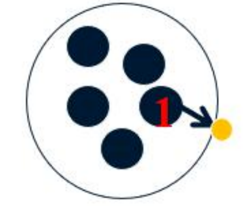
SUSTech
Southern University
of Science and Technology

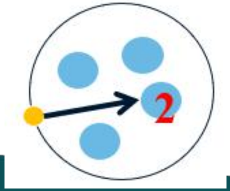
Thinking …

- Practise on “ ***ipconfig*** ” with option “***/all***’ , what info will be shown by running this command?
- Are the **IP address**, **subnet mask** and **default gateway** of your PC same as those of your deskmate? What are **same**, What are **different**? Are your PCs **in the same subnet**?
- In the following pictures, PC1 and PC2 are in the two differnent subnets, if PC1 needs to communicate with PC2, what's the usage of default gateway?

PC1
IP address: 192.168.**1**.104
Subnet mask: **255.255.255.0**
Default Gateway: 192.168.**1**.1

PC2
IP address: 192.168.**2**.104
Subnet mask: **255.255.255.0**
Default Gateway: 192.168.**2**.1

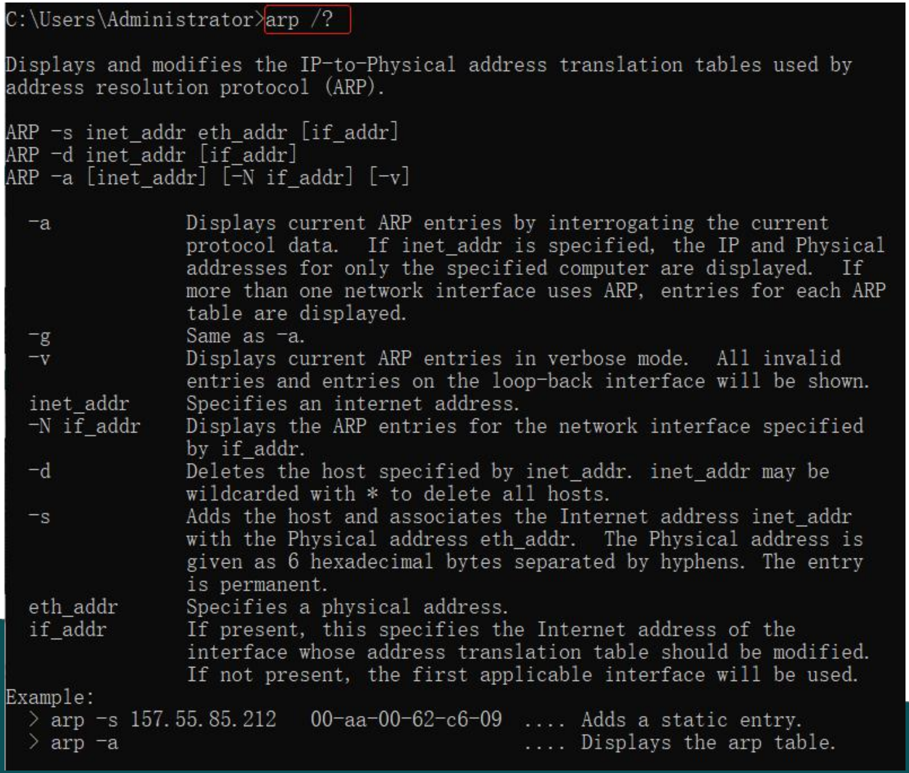




2. arp (1)

- “**arp**” is usually used to display or modify the address translation table (ARP cache, with the IP and MAC address pairs in it) which is used by ARP protocol.

Tips:
use ‘/?’ or ‘-help’ following the commands to get its help information.



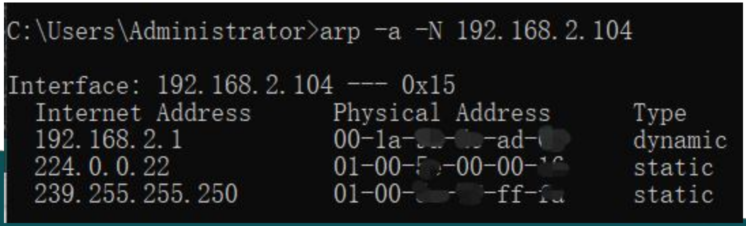
```
C:\Users\Administrator>arp /?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

2. arp (2)

- **arp –a**
  - **Display** all ARP information, that is, the corresponding relationship between all activated IP addresses and physical addresses
- **arp –d**
  - **Delete** all ARP cache contents.
  - If the IP address is specified in the command, only the ARP cache information of the IP address is deleted.
- **arp –s**
  - **Adding** the corresponding relationship between IP address and physical address to ARP cache

2. arp (3)

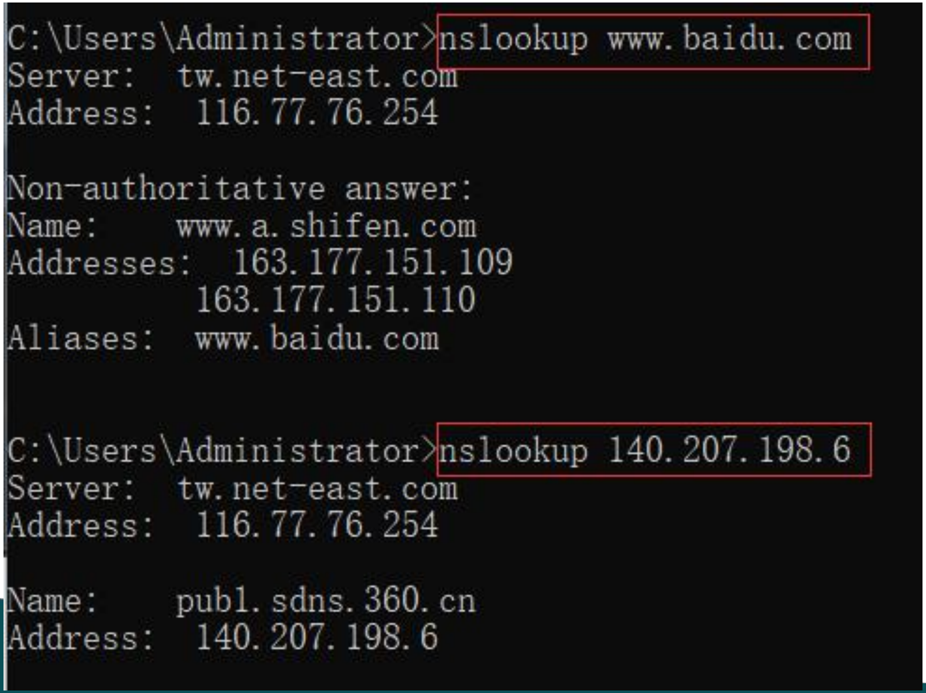
- Run the “***arp - a***” command to display all the corresponding relationships in the "IP address to physical address" address translation table (ARP cache).
- You can try to solve the problem of IP address embezzlement in LAN by using “***arp -s***” command according to the format, and bundle the static IP address with the physical address of the network card. For example, “***arp -s 172.16.0.19 00-10-5C-BE-11-CC***”.
- Practise:
  - Run the command “***arp -s 192.168.2.222 00-11-22-33-44-xx***”, could this mapping between two address be added to ARP cache? Why?
  - In the following picture, “192.168.2.104” is the IP address of a wirelesscard, “192.168.2.1” is its default gateway, could this arp item related to “192.168.2.1” be deleted or changed from ARP cache?



```
C:\Users\Administrator>arp -a -N 192.168.2.104

Interface: 192.168.2.104 --- 0x15
  Internet Address      Physical Address      Type
  192.168.2.1           00-1a-[redacted]-[redacted]-ad-[redacted]     dynamic
  224.0.0.22            01-00-[redacted]-00-00-[redacted]     static
  239.255.255.250       01-00-[redacted]-[redacted]-ff-[redacted]     static
```

3. nslookup

- "**nslookup**" is usually used to find the corresponding IP through the host name, or find the corresponding host by specifying the IP.



```
C:\Users\Administrator>nslookup www.baidu.com
Server:   tw.net-east.com
Address:   116.77.76.254

Non-authoritative answer:
Name:     www.a.shifen.com
Addresses:   163.177.151.109
           163.177.151.110
Aliases:   www.baidu.com


C:\Users\Administrator>nslookup 140.207.198.6
Server:   tw.net-east.com
Address:   116.77.76.254

Name:     publ.sdns.360.cn
Address:   140.207.198.6
```

4. ping (1)

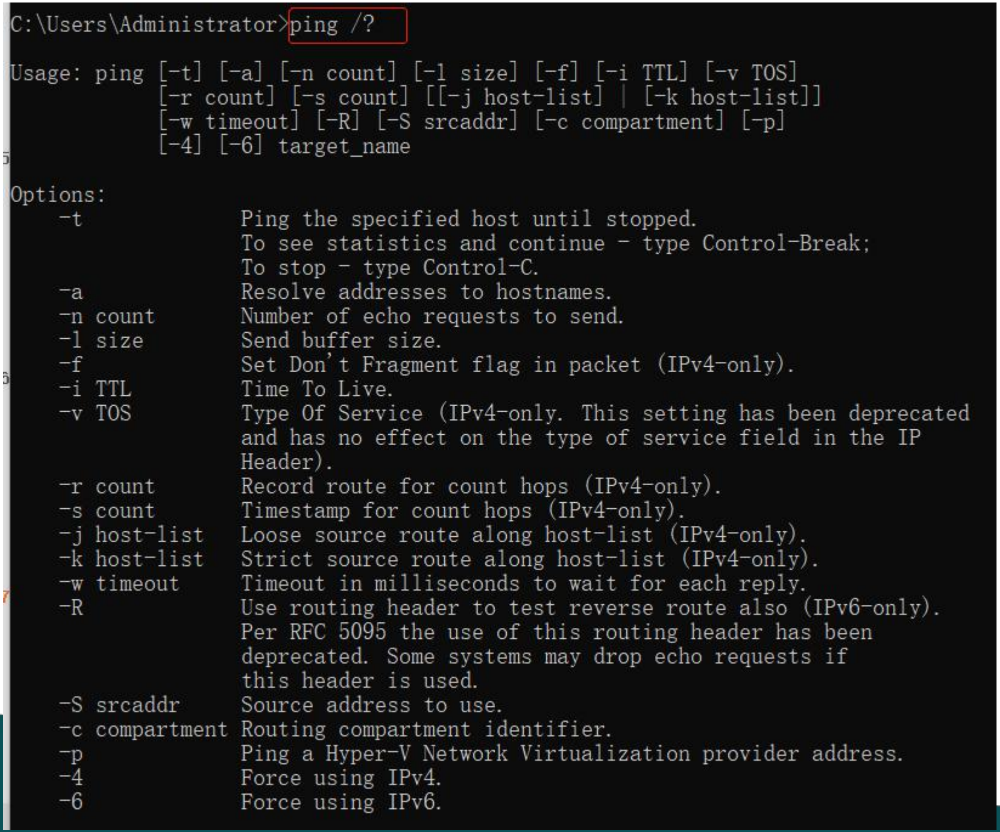
"**ping**" is usually used to check the network connectivity

- Options:
  - -t
  - -i
  - -n
- practise:

' ping www.sustech.edu.cn –4'

' ping www.sustech.edu.cn –6' ?

respectively, is there any difference?



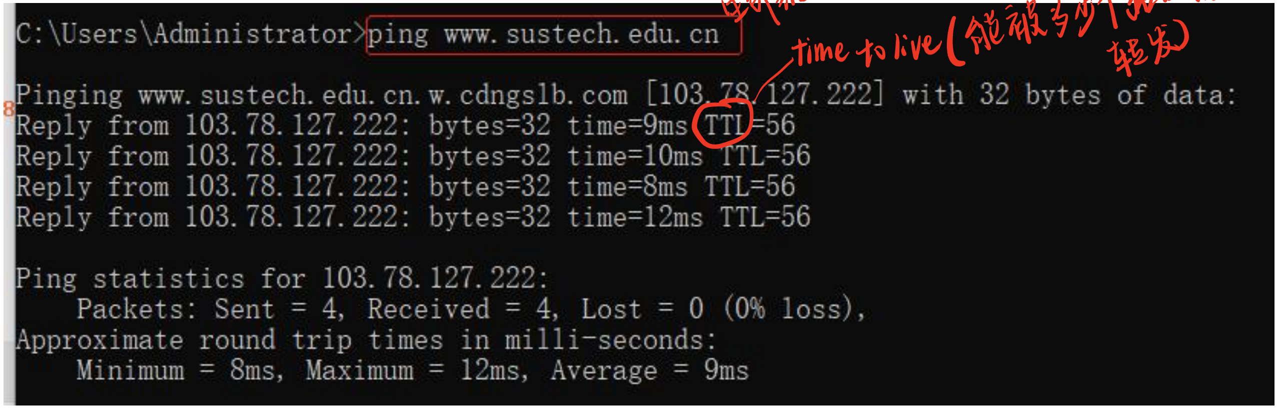
```
C:\Users\Administrator>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.
```

SUSTech
Southern University
of Science and Technology

4. ping (2)

生命期变0后将报文回转或丢弃（测试报文）

time to live（能被多少个路由器转发）



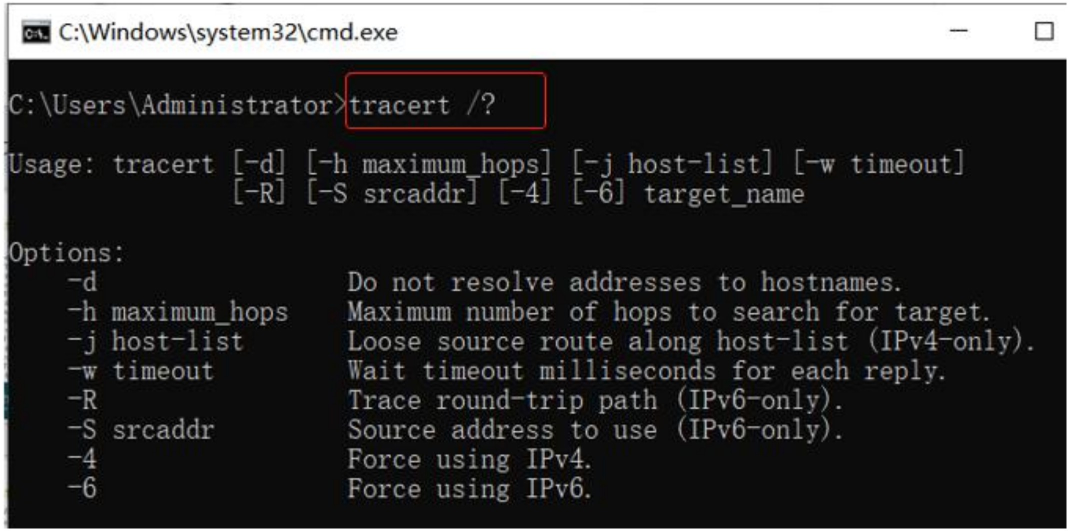
```
C:\Users\Administrator>ping www.sustech.edu.cn

Pinging www.sustech.edu.cn.w.cdngslb.com [103.78.127.222] with 32 bytes of data:
Reply from 103.78.127.222: bytes=32 time=9ms TTL=56
Reply from 103.78.127.222: bytes=32 time=10ms TTL=56
Reply from 103.78.127.222: bytes=32 time=8ms TTL=56
Reply from 103.78.127.222: bytes=32 time=12ms TTL=56

Ping statistics for 103.78.127.222:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 12ms, Average = 9ms
```

Here using “ping” to test if the website “www.sustech.edu.cn” is reachable, as the information show, there is no packets lost, the website is reachable.

- What does “time=9ms” mean?
- What does TTL mean? Why all the “TTL”s based on reply keep same while the “time”s are different from eachother?
- Using your PC to run this command, is the testing result same with the picture above? Check the value of IP address, TTL and time, explain why they are not all the same.

5. tracert (1)

- On the Internet, routing directly impact the network performance, it is necessary to track the routing to check the connectivity of the network.



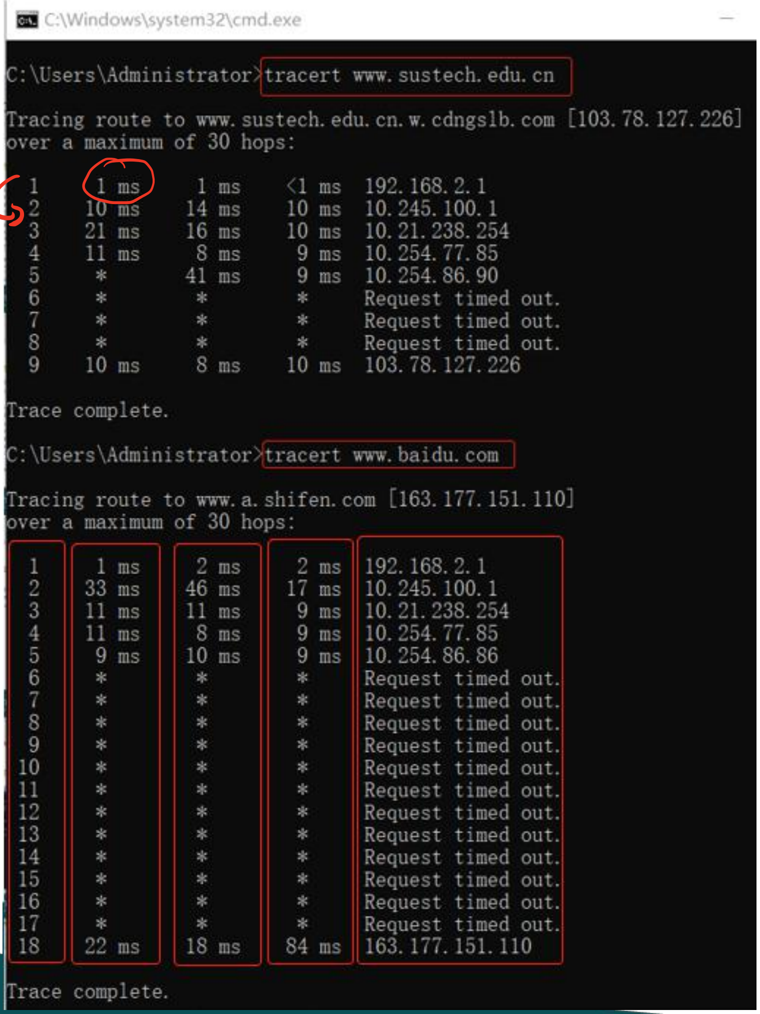
```
C:\Users\Administrator>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

学生机互ping?

5. tracert (2)

- The five parameters detected are represented from left to right respectively.
  - "Lifetime" (1 node per route)
  - "Return time of ICMP packets sent three times" (3 items in milliseconds)
  - "IP address through router" (IP address, if there is a host name, it will be included either).

TTL+1

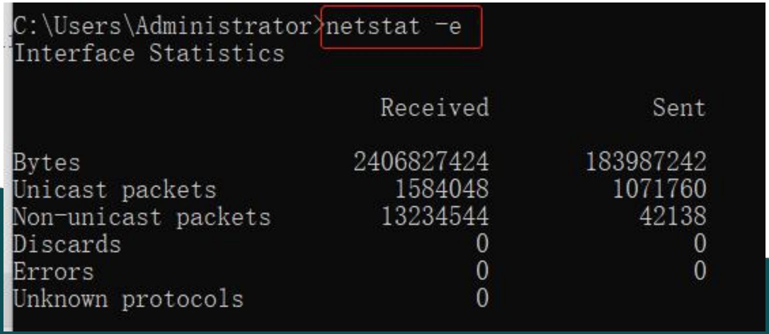


```
C:\Users\Administrator>tracert www.sustech.edu.cn

Tracing route to www.sustech.edu.cn.w.cdngslb.com [103.78.127.226]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  192.168.2.1
  2    10 ms    14 ms    10 ms  10.245.100.1
  3    21 ms    16 ms    10 ms  10.21.238.254
  4    11 ms     8 ms     9 ms  10.254.77.85
  5     *       41 ms     9 ms  10.254.86.90
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9    10 ms     8 ms    10 ms  103.78.127.226

Trace complete.

C:\Users\Administrator>tracert www.baidu.com

Tracing route to www.a.shifen.com [163.177.151.110]
over a maximum of 30 hops:

  1     1 ms     2 ms     2 ms  192.168.2.1
  2    33 ms    46 ms    17 ms  10.245.100.1
  3    11 ms    11 ms     9 ms  10.21.238.254
  4    11 ms     8 ms     9 ms  10.254.77.85
  5     9 ms    10 ms     9 ms  10.254.86.86
  6     *        *        *     Request timed out.
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18    22 ms    18 ms    84 ms  163.177.151.110

Trace complete.
```

6. netstat (1)

- "**netstat**" is usually used to display protocol statistics on current TCP/IP network connections.
- Options:
  - netstat –n
    - List IP addresses in dot decimal format, rather than symbolic hostnames and network names
  - netstat –e
    - Display statistics about Ethernet
  - netstat –s
    - The statistical data are displayed separately according to each protocol. In this way, we can see which connections exist in the current computer network, as well as the details of data packet sending and receiving, and so on.

Tips:
use '/?' or '-help' following the commands to get its help information.



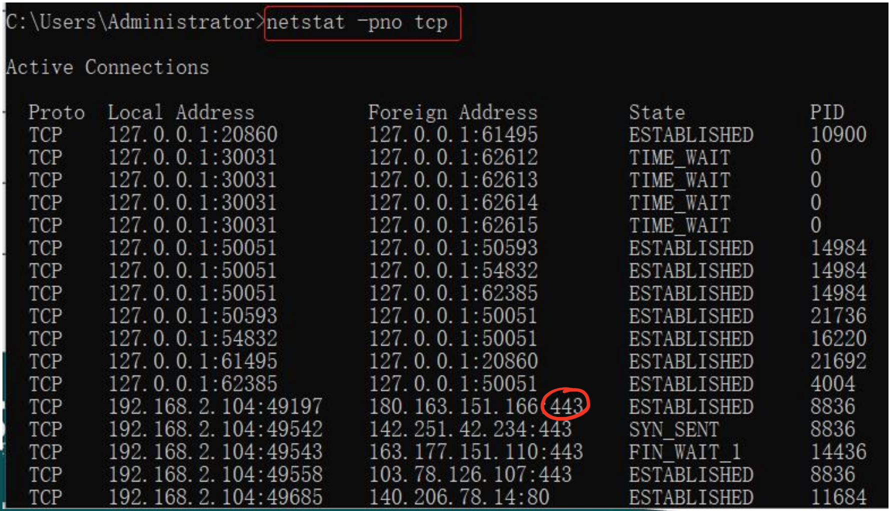
```
C:\Users\Administrator>netstat -e
Interface Statistics

                           Received            Sent

Bytes                    2406827424       183987242
Unicast packets             1584048         1071760
Non-unicast packets        13234544           42138
Discards                          0               0
Errors                            0               0
Unknown protocols                 0
```

SUSTech
Southern University
of Science and Technology

6. netstat (2)

- State of TCP connection
  - –**LISTEN:** Listening for connection requests from remote TCP ports
  - –**SYN-SENT:** Waiting for a matching connection request after sending a connection request
  - –**ESTABLISHED:** Represents an open connection
  - –**FIN-WAIT-1:** Waiting for confirmation of remote TCP connection interrupt request or previous connection interrupt request

- A connection can be uniquely determined by the protocol used by both sides of the communication, as well as the IP address and port number.
  - “127.0.0.1:20860”, “127.0.0.1” is an IP address, “20860” is the port number .
- “PID” is the ID number of the process.



```
C:\Users\Administrator>netstat -pno tcp

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127. 0. 0. 1:20860     127. 0. 0. 1:61495     ESTABLISHED     10900
  TCP    127. 0. 0. 1:30031     127. 0. 0. 1:62612     TIME_WAIT       0
  TCP    127. 0. 0. 1:30031     127. 0. 0. 1:62613     TIME_WAIT       0
  TCP    127. 0. 0. 1:30031     127. 0. 0. 1:62614     TIME_WAIT       0
  TCP    127. 0. 0. 1:30031     127. 0. 0. 1:62615     TIME_WAIT       0
  TCP    127. 0. 0. 1:50051     127. 0. 0. 1:50593     ESTABLISHED     14984
  TCP    127. 0. 0. 1:50051     127. 0. 0. 1:54832     ESTABLISHED     14984
  TCP    127. 0. 0. 1:50051     127. 0. 0. 1:62385     ESTABLISHED     14984
  TCP    127. 0. 0. 1:50593     127. 0. 0. 1:50051     ESTABLISHED     21736
  TCP    127. 0. 0. 1:54832     127. 0. 0. 1:50051     ESTABLISHED     16220
  TCP    127. 0. 0. 1:61495     127. 0. 0. 1:20860     ESTABLISHED     21692
  TCP    127. 0. 0. 1:62385     127. 0. 0. 1:50051     ESTABLISHED     4004
  TCP    192. 168. 2. 104:49197 180. 163. 151. 166:443 ESTABLISHED     8836
  TCP    192. 168. 2. 104:49542 142. 251. 42. 234:443  SYN_SENT        8836
  TCP    192. 168. 2. 104:49543 163. 177. 151. 110:443 FIN_WAIT_1      14436
  TCP    192. 168. 2. 104:49558 103. 78. 126. 107:443  ESTABLISHED     8836
  TCP    192. 168. 2. 104:49685 140. 206. 78. 14:80    ESTABLISHED     11684
```