CS 305 Lab1 Tutorial Commands for network detection and diagnosis

Dept. Computer Science and Engineering
Southern University of Science and Technology
tangm3@sustech.edu.cn
wangw6@sustech.edu.cn
wangq9@mail.sustech.edu.cn

SUSTech
Southern University
of Science and Technology

LAB information

- Lab website
  - Blackboard: Computer Networks Fall 2023
  - QQ group: 897669773
- Grading criteria
  - Attendance & practice(s) on each lab class
  - Lab programming assignments
  - Project
- regulations on plagiarism
  - The first time the score of the assignment will be 0
  - The second time the score of the course will be 0

wireshark抓包
eNSP仿真

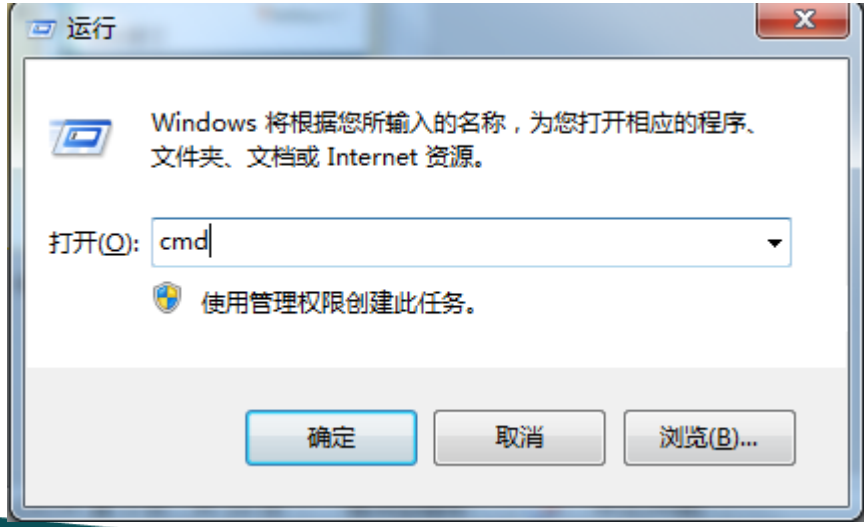
Topics

- Learn the usage of network commands. Learn how to use them to conduct network testing, troubleshooting and event detection.
  - **ipconfig**
  - **arp**
  - **nslookup**
  - **ping**
  - **tracert**
  - **netstat**

  TIPS: some commands may vary across different operating systems
- 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
  - Or Windows + R



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 .
  - Followed by different parameters can display different information.
  - "***ipconfig /all***" or "***ipconfig -all***" can display more information.
  - "***ipconfig /?***" or "***ipconfig -?***" can display its help information.

```
C:\Users\wq>ipconfig /?

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

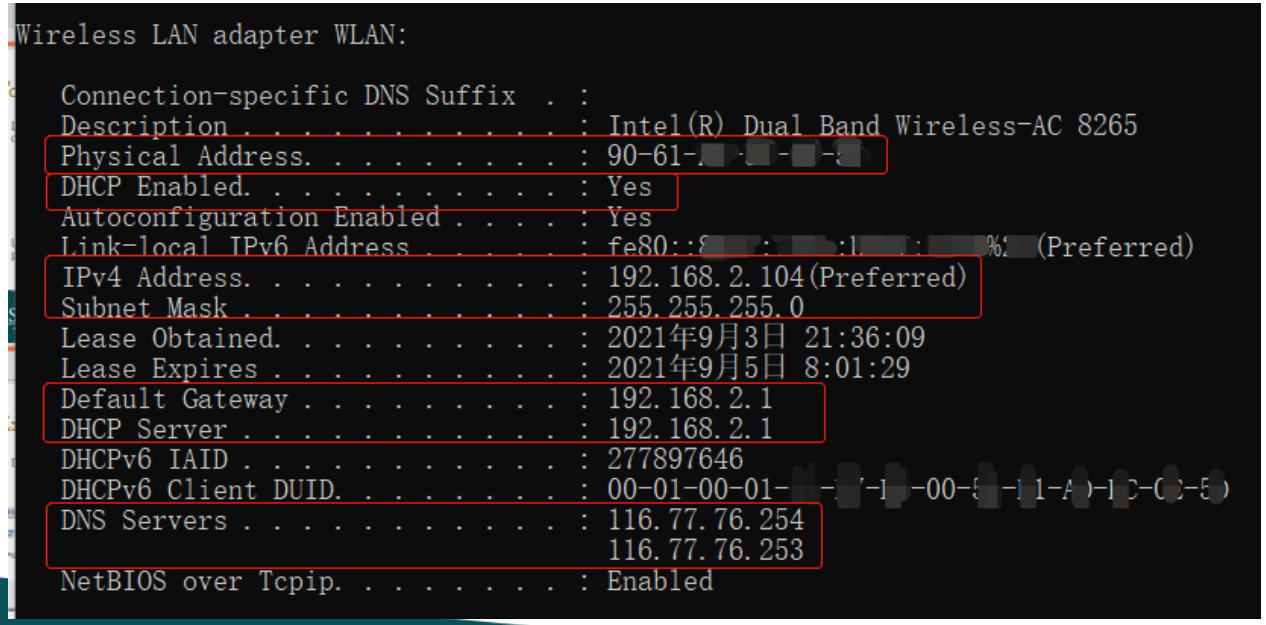
ipconfig /displaydns网址和ip地址的对应关系缓存
ipconfig /flushdns清除缓存

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



SUSTech
Southern University of Science and Technology

Practice 1.1

子网掩码：左侧连续的1（位数和网络号位数相等），右侧连续的0

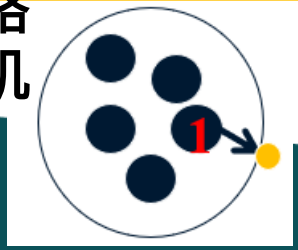
- Practise on "***ipconfig***" with option "***/all***", what info will be shown by running this command?
- Are the **IP address**, **subnet mask** and **default gateway** of your PC same as those of your classmates? What are **the same**, What are **different**? Are your PCs **in the same subnet**?
- In the following pictures, PC1 and PC2 are in two differnent subnets, if PC1 needs to communicate with PC2, what's the usage of default gateway? ip地址和子网掩码按位相与得到网络号

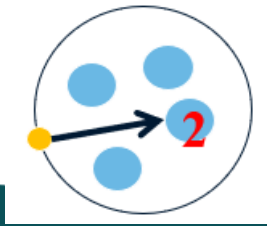
ip=网络号+主机号

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

大圆：网络
小圆：主机





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.

- "**arp /?**" or "**arp -?**" can display its help information.

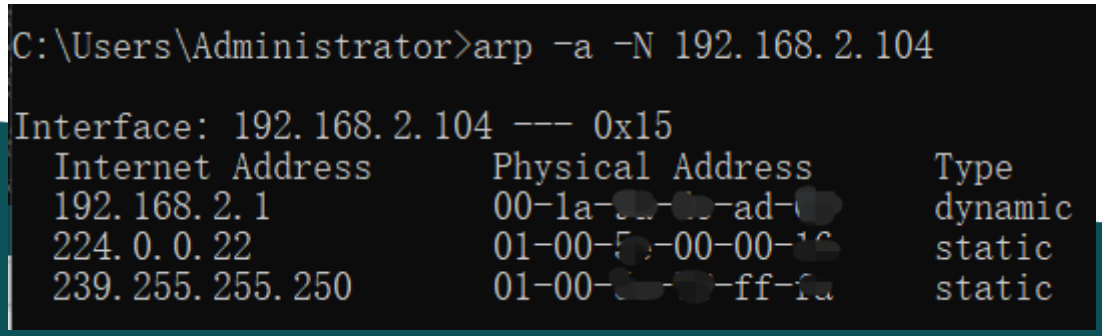
```
C:\Users\Administrator>arp /?

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

Practice 1.2

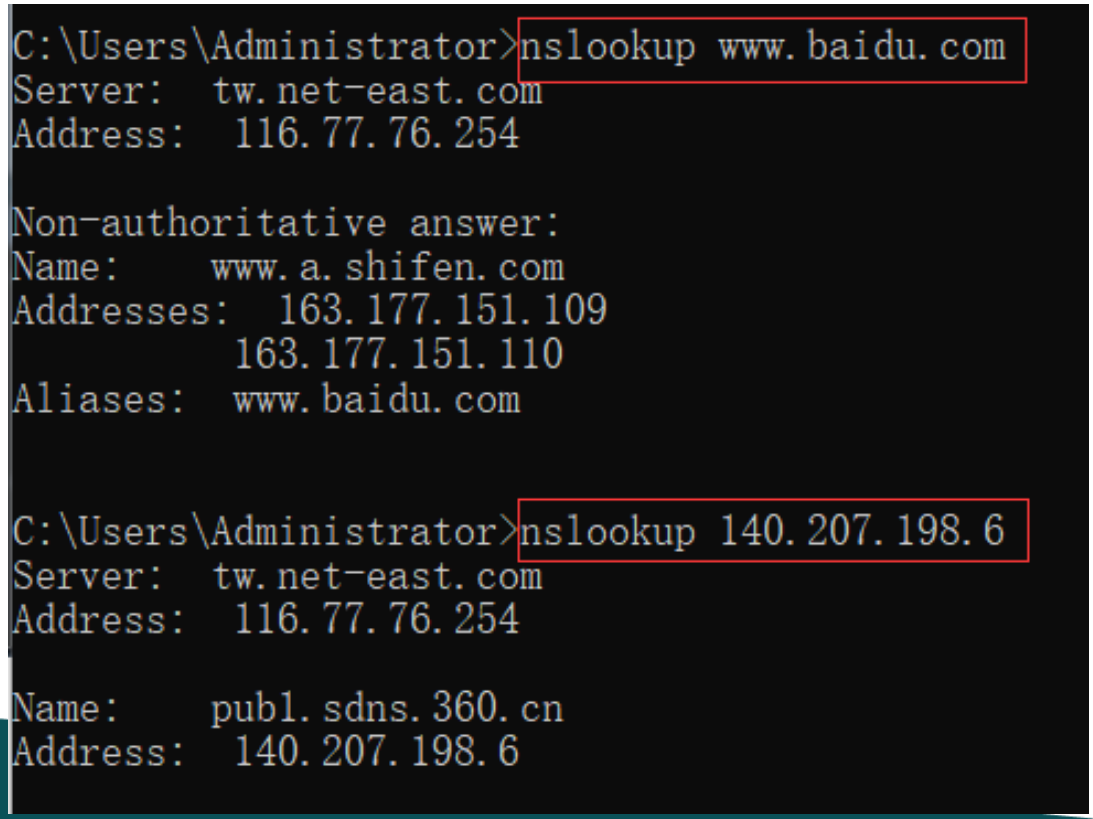
- Run the "***arp - a***" command to display all the corresponding relationships in the "IP address to physical address" address translation table (ARP cache).
- You can try to solve the problem of IP address embezzlement in LAN by using "***arp -s***" command according to the format, and bundle the 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***".
- Run the command "***arp -s 192.168.2.222 00-11-22-33-44-YY***", 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?



SUSTech
Southern University of Science and Technology

3. nslookup

- "**nslookup**" is usually used to find the corresponding IP through the host name, or find the corresponding host by specifying the IP. The former involves DNS services, while the latter involves reverse DNS (rDNS) services. Generally speaking, DNS services are available, but some websites may not support rDNS services.



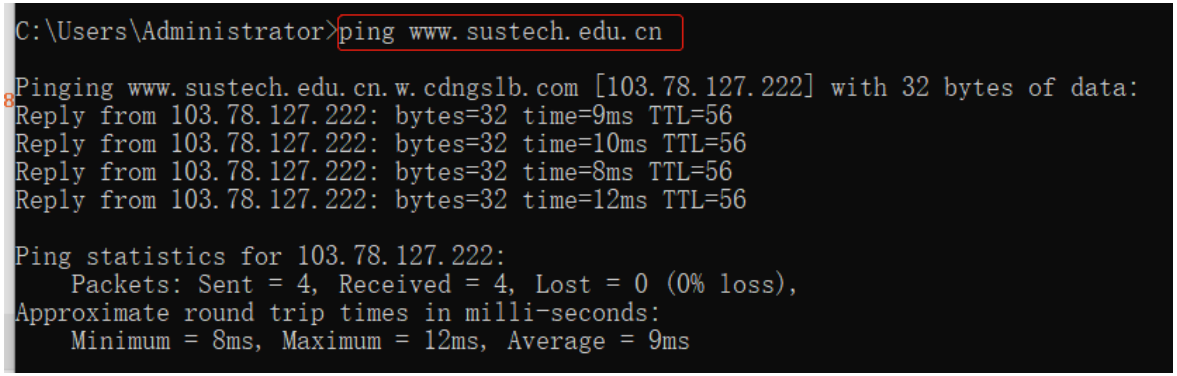
4. ping

- "ping" is usually used to check the network connectivity.
- Options
  - ping -t
  - ping -i
  - ping –n
  - ……

```
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.
```

Practice 1.3

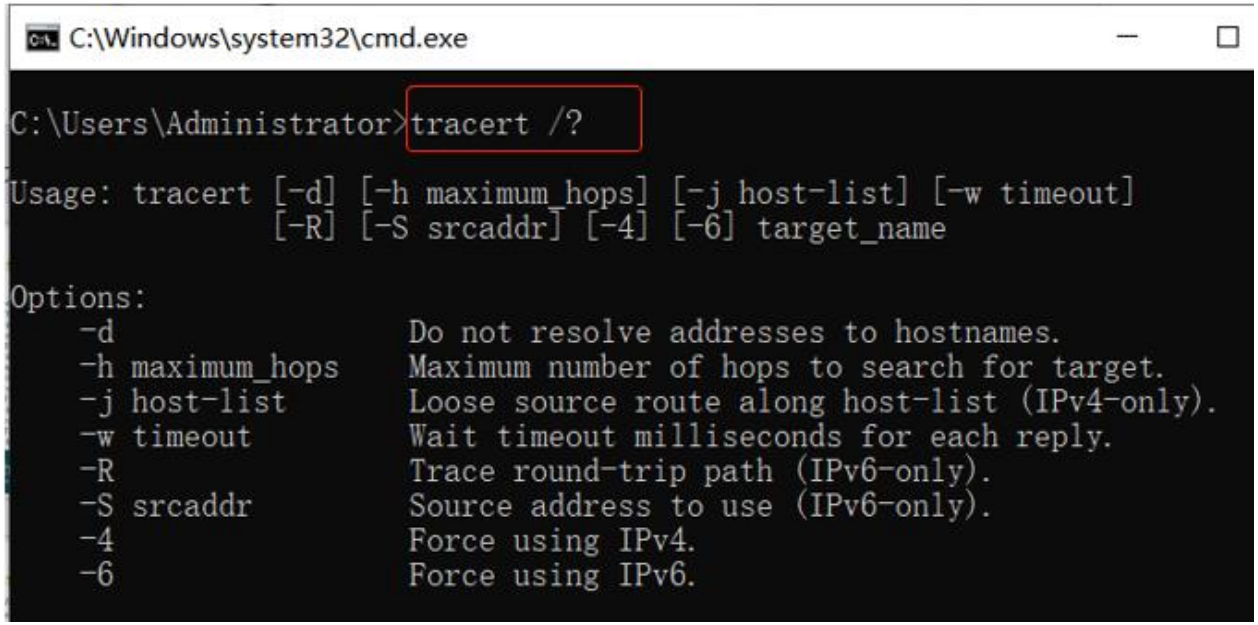
- Here using “ping” to test if the website “www.sustech.edu.cn” is reachable, as the information show, there is no packets lost, the website is reachable.
  - What does “time=9ms” mean?
  - What does TTL mean? Why all the “TTL”s based on reply keep same while the “time”s are different from each other?
  - Using your PC to run this command, is the testing result same with the picture below? Check the value of IP address, TTL and time, explain why they are not all the same.



- Use “ping www.sustech.edu.cn –4” and “ping www.sustech.edu.cn –6” respectively, is there any difference?

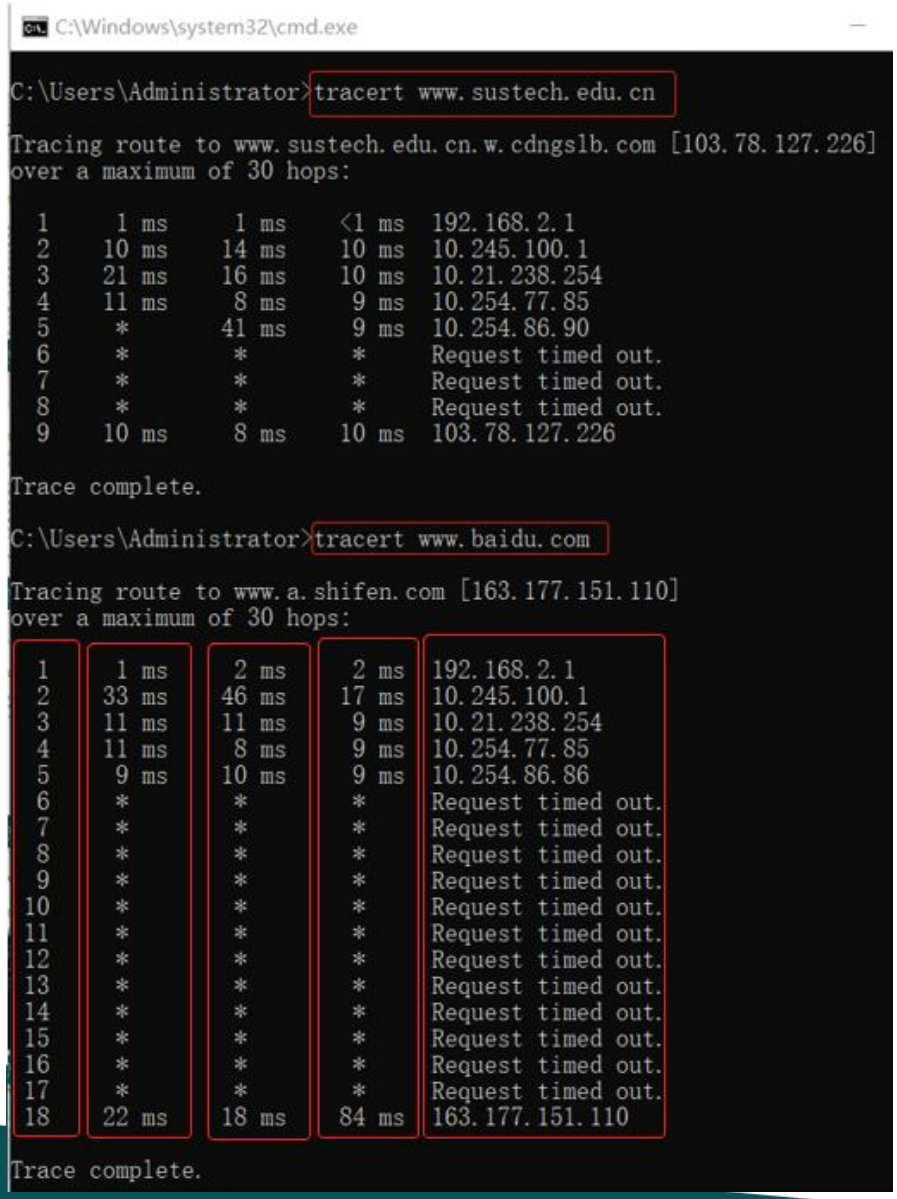
5. tracert (1)

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



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).



Practice 1.4

- Use “tracert www.baidu.com” command to check the information of each hop between your PC and Baidu server.
  - How many hops are there?
  - What does each column mean of each row?
  - What does * mean in some row?
- Run “tracert www.baidu.com” command again on your PC.
  - Does the result the same with the former? Which hops are same? And which hops are different? Try to speculate possible reasons to these results.
  - Are the first hops the same in these two results?
  - Are the destination hops the same in these two results?

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' arguments 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
```

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
```