CS 305 Lab1 Tutorial
Commands for network detection and diagnosis

Dept. Computer Science and Engineering
Southern University of Science and Technology

SUSTech
Southern University
of Science and Technology

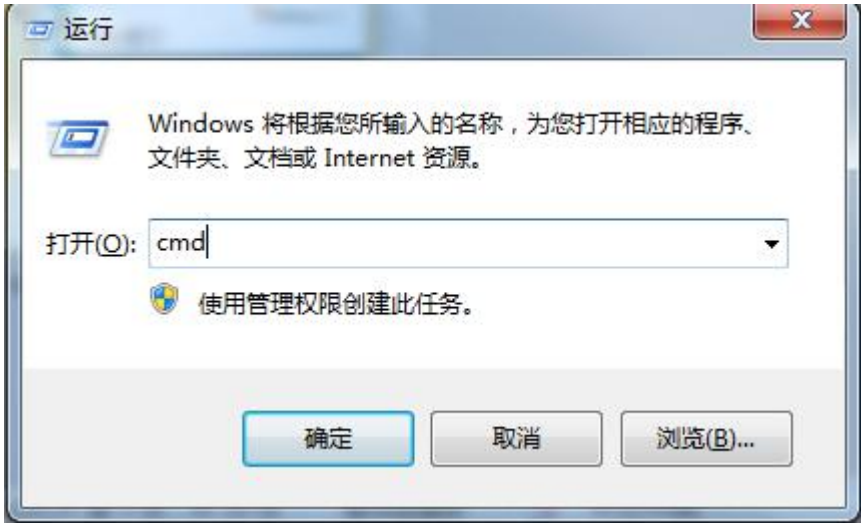
Topics

- Learn the usage of network commands. Learn how to use them to conduct network testing,troubleshooting and event detection.
  - ipconfig
  - ping
  - netstat
  - Tracert
  - arp
  - net
  - Nslookup

- 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



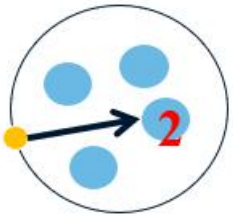
1. ipconfig

- Check the configuration in TCP/IP, such as IP address, gateway, network mask etc.
- Tips: use '?' or '-help' following the commands to get its help infomation.

管理员: 命令提示符

```
C:\windows\system32>ipconfig

Windows IP 配置


以太网适配器 以太网 2:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 本地连接* 3:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::a119:ae60:6b10:8050%18
   IPv4 地址 . . . . . . . . . . . . : 192.168.0.102
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.0.1

以太网适配器 蓝牙网络连接:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
```

Thinking …



IP range: 192.168.1.1~192. 168.1.254

Subnet mask: 255.255.255.0

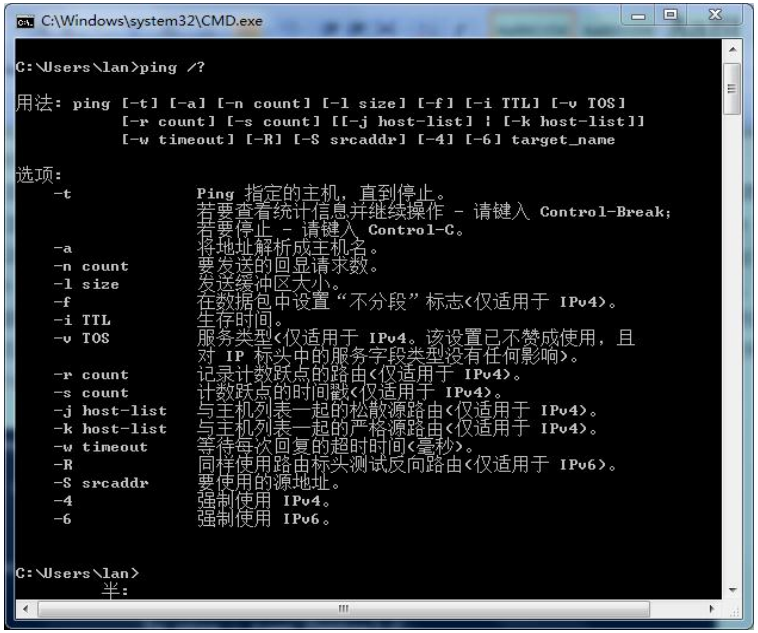
IP range: 192.168.2.1~192.168.2.254

Subnet mask: 255.255.255.0

- What is the gateway?
- How many subnets are there, what's the network ID？
- How many hosts in each subnet?
- Practice on ipconfig with option '/all' , what info will be shown by running this command?

2. ping (1)

- Help to check the network connectivity



- Options:
  - -t
  - -i
  - -n
- Try:

‘ ping www.sustech.edu.cn –t –n -3’
‘ ping www.sustech.edu.cn –n 3 -t’
respectively, is there any difference?

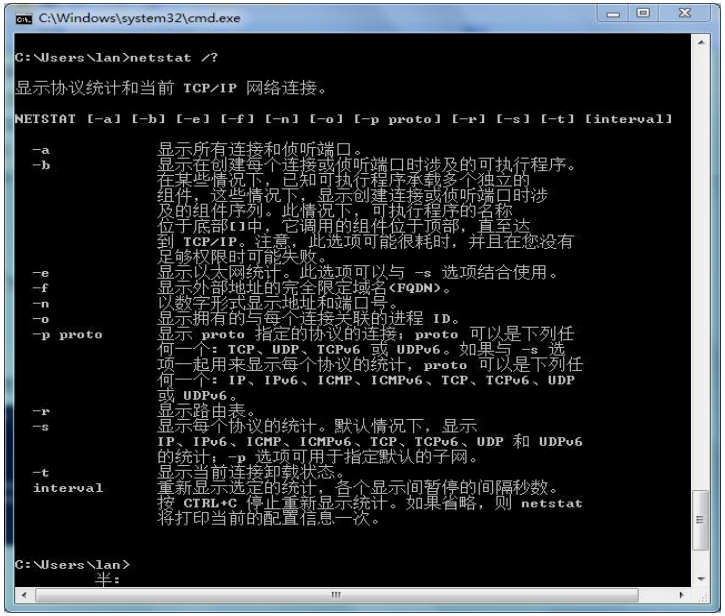
2. ping (2)

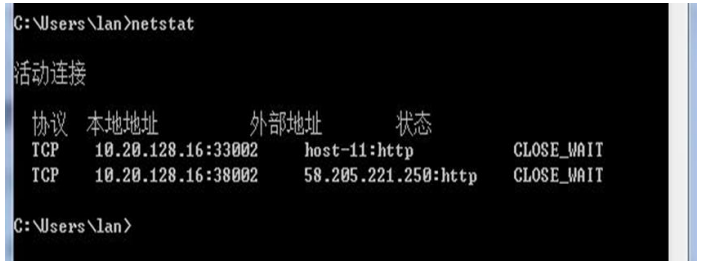
```
C:\windows\system32>ping www.sustc.edu.cn

正在 Ping www.sustc.edu.cn [116.7.234.3] 具有 32 字节的数据:
来自 116.7.234.3 的回复: 字节=32 时间=16ms TTL=55
来自 116.7.234.3 的回复: 字节=32 时间=16ms TTL=55
来自 116.7.234.3 的回复: 字节=32 时间=14ms TTL=55
来自 116.7.234.3 的回复: 字节=32 时间=16ms TTL=55

116.7.234.3 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 14ms，最长 = 16ms，平均 = 15ms
```

- What does time=16ms mean?
- What does TTL mean? Does the initial value of TTL keep the same for different OS?

3. netstat (1)

- Display protocol statistics on current TCP/IP network connections





3. netstat (2)

- Options:
  - netstat –a
    - Display a list of all valid connection information, including established connections (ESTABLISHED), as well as those that listen for connection requests (LISTENING).
  - netstat –n
    - List IP addresses in dot decimal format, rather than symbolic hostnames and network names
  - netstat –e
    - Display statistics about Ethernet
  - netstat –r
    - Display the routing info
  - 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.

3. netstat (3)

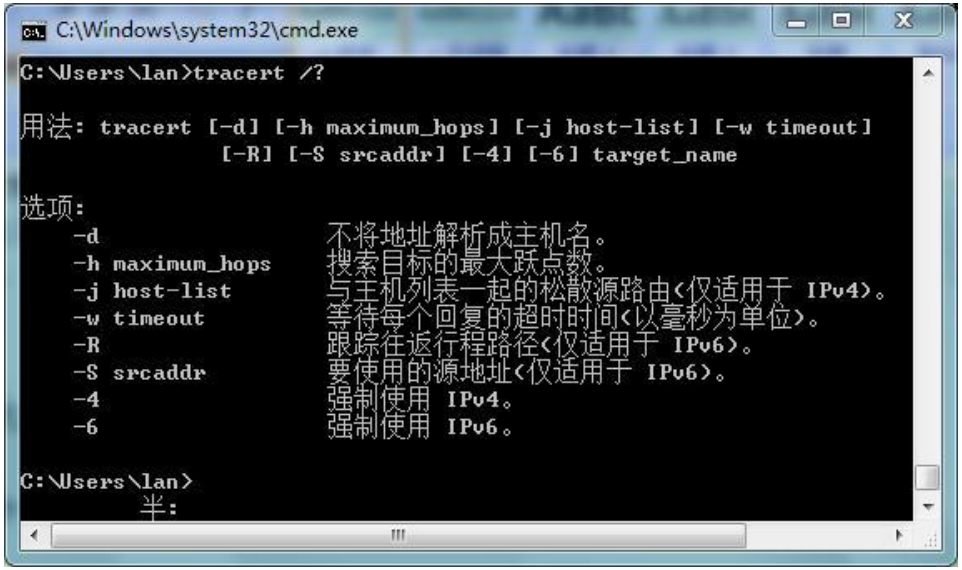
- LISTEN
  - Listening for connection requests from remote TCP ports
- SYN-SENT
  - Waiting for a matching connection request after sending a connection request
- SYN-RECEIVED
  - Waiting for confirmation of a connection request after receiving and sending a connection request
- ESTABLISHED
  - Represents an open connection
- FIN-WAIT-1
  - Waiting for confirmation of remote TCP connection interrupt request or previous connection interrupt request
- FIN-WAIT-2
  - Waiting for connection interrupt requests from remote TCP

3. netstat (4)

- CLOSE-WAIT
  - Waiting for connection interruption requests from local users
- CLOSING
  - Waiting for confirmation of connection interruption by remote TCP
- LAST-ASK
  - Waiting for the confirmation of the original connection interrupt request sent to remote TCP
- TIME-WAIT
  - Wait for enough time to ensure that remote TCP receives confirmation of connection interrupt requests
- CLOSED
  - No connection status

4. tracert (1)

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



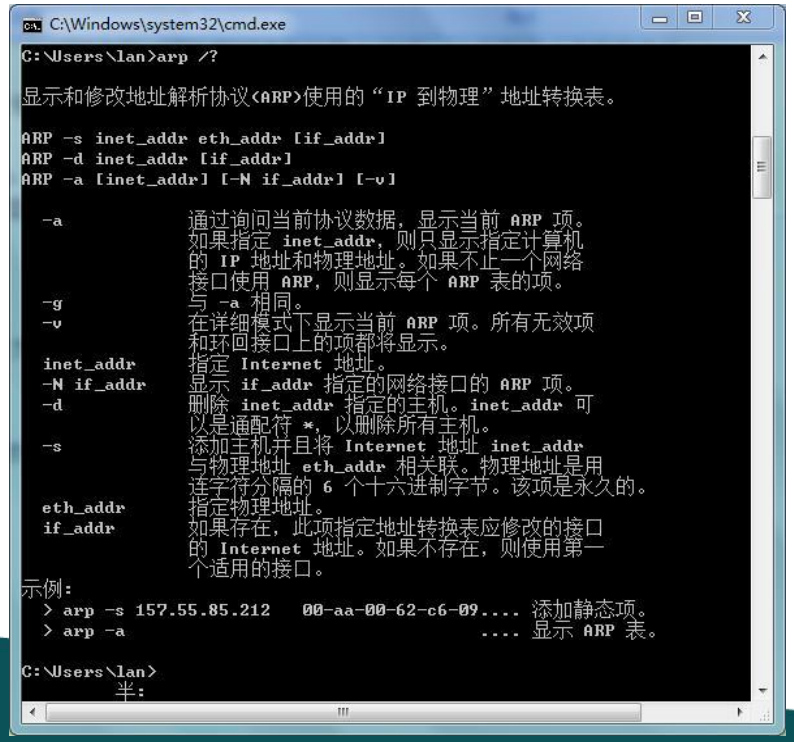
4. tracert (2)

```
C:\Windows\system32\cmd.exe
C:\Users\lan>tracert www.sustc.edu.cn

通过最多 30 个跃点跟踪
到 www.sustc.edu.cn [172.18.1.3] 的路由:

  1    <1 毫秒   <1 毫秒   <1 毫秒 10.10.10.10
  2    <1 毫秒   <1 毫秒   <1 毫秒 172.18.1.3

跟踪完成。

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

通过最多 30 个跃点跟踪
到 www.a.shifen.com [119.75.217.56] 的路由:

  1    <1 毫秒   <1 毫秒    1 ms  10.10.10.10
  2     *         *         *     请求超时。
  3     1 ms      1 ms      1 ms  218.192.243.209
  4    26 ms      2 ms      1 ms  218.192.242.229
  5     1 ms      3 ms      1 ms  101.4.112.222
  6     9 ms      4 ms      4 ms  101.4.117.93
  7    51 ms     55 ms     55 ms  101.4.117.33
  8    20 ms     20 ms     25 ms  101.4.112.38
  9    41 ms     39 ms     39 ms  101.4.117.38
 10    49 ms     49 ms     49 ms  101.4.112.1
 11    50 ms     50 ms     51 ms  101.4.116.194
 12    92 ms    211 ms    210 ms  219.224.103.10
 13    39 ms     39 ms     39 ms  192.168.0.5
 14    51 ms     51 ms     51 ms  10.65.190.130
 15    40 ms     39 ms     39 ms  119.75.217.56

跟踪完成。

C:\Users\lan>
        半:
```

- 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).

5. arp (1)

- To display / modify the address translation table (ARP cache, with the IP and MAC address pairs in it) which is used by ARP protocol.



SUSTech
Southern University
of Science and Technology

5. 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

5. arp (3)

- Enter the ARP - a command in the DOS window 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.

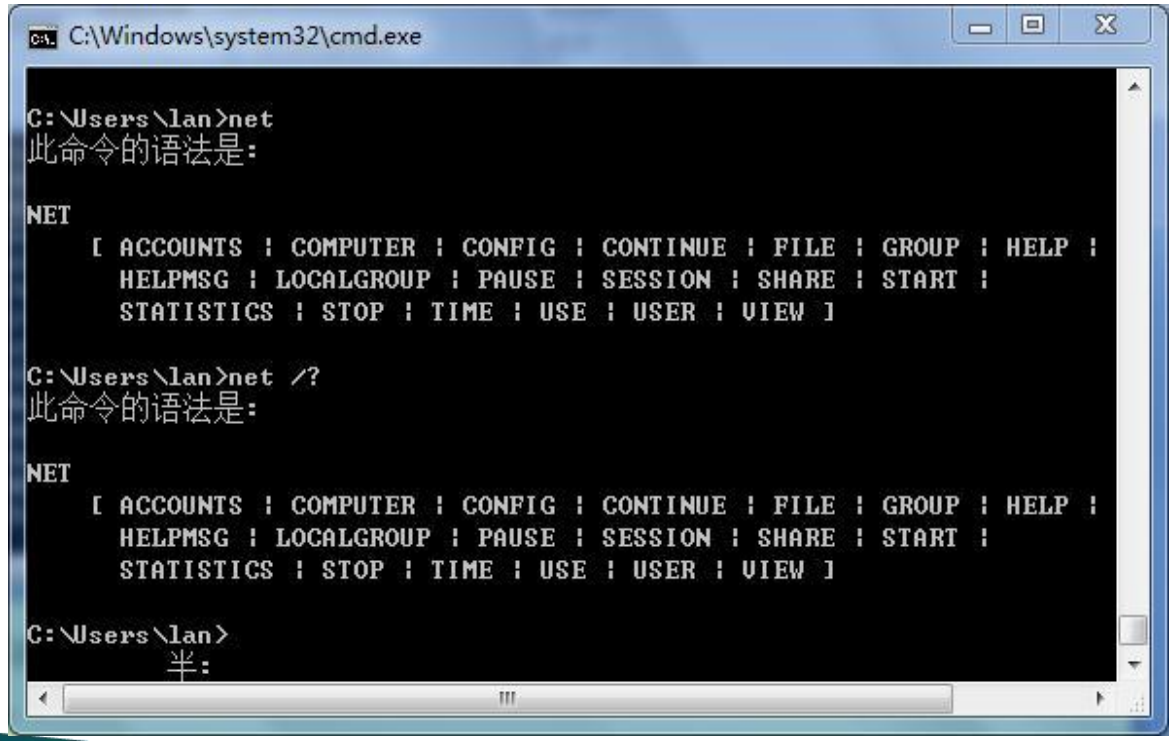
```
C:\windows\system32>arp -a

接口: 10.21.3.80 --- 0x12
  Internet 地址         物理地址              类型
  10.21.127.254         2c-21-31-aa-6d-c3     动态
  10.21.127.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

6. net (1)

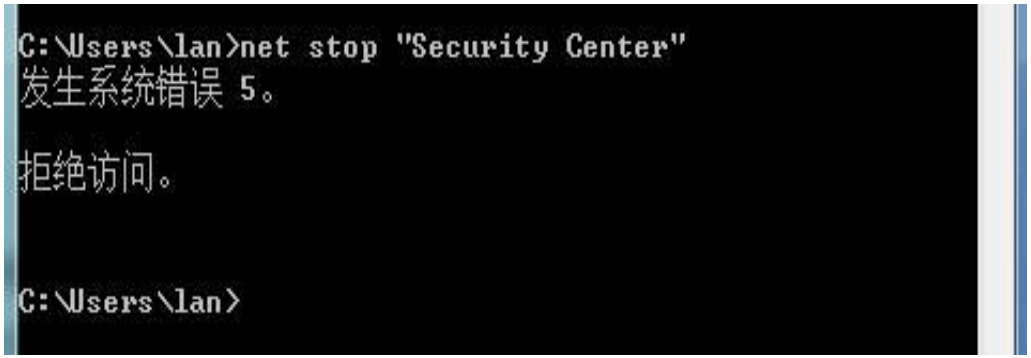
- ‘net’ is a powerful command, including the management of network environment, services, users and other important management functions.
- ‘net’ is usually used to obtain the local or remote computer network environment and the operation and configuration of various service programs

6. net (2)

- Using ‘net start’ to display the net service which is started



6. net (3)



- Running ‘net stop’ requires administrator privileges, otherwise access is denied as shown in the following figure

7. nslookup

- To find the corresponding IP through the host name, or find the corresponding host by specifying the IP

Assignment

Query the relevant network information by commands, please give a screenshot of command and execution result and explain the result accordingly.

1. Query the ip address, subnet mask and MAC address of host.

Please check whether the IP address of host is allocated statically or dynamically through DHCP. If the address is allocated dynamically, what's the IP address of host's DHCP server, how long is the lease time of the current IP ?

2. DNS provides the corresponding relationship between domain name and IP address. Please query 1) IP address of host's DNS server 2) DNS information cached in host 3) IP address of www.cernet.edu.cn

3. Statistical analysis on the traffic on ICMP protocols, please list how many destination unreachable, echo reply, request timeout message are received on host?

4. What's the default value of max hops while process 'tracert' command, can this value be changed? Use the 'tracert' to access 'www.bilibili.com', find out the total number of hops from the local host to the target. Are there any ICMP messages lost during the tracert process? what's the IP address of the your PC's gateway.

5. Find a web site with IPv6 address, use command to check if it is reachable or not. what's the IPv6 address of the host, is '::1' a legal or illegal IPv6 address.

Requirements on reports

1. please submit practical report by pdf file to sakai site (submit by QQ or email is NOT allowed)

2. practical report should includes:
   - Brief description on the practical topic, background, and the content of the lab.
   - Clear description on Steps by words and screen shot if necessary.
   - Clear description on practical result: screen shot is MUST with detailed description and analysis.
   - summary: describe the problem and the method you met in this lab, suggestion on the lab is also welcomed
   - notes: every picture should be labelled with ‘Fig.index’ (such as Fig.1),