

# CS 305 Lab1 Tutorial

## Commands for network detection and diagnosis

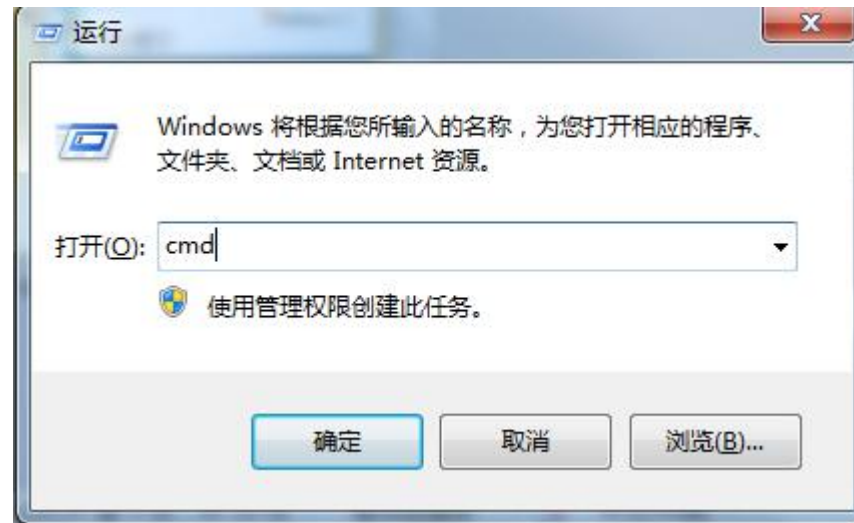
Dept. Computer Science and Engineering  
Southern University of Science and Technology

# 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 information.

```
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 . . . . . :

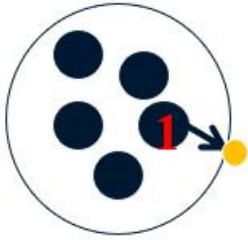
无线局域网适配器 WLAN:

    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:

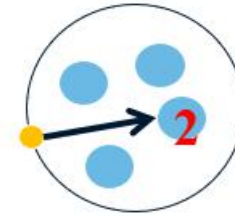
    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :
```

# Thinking ...



IP range: 192.168.1.1~192.168.1.254

Subnet mask: 255.255.255.0



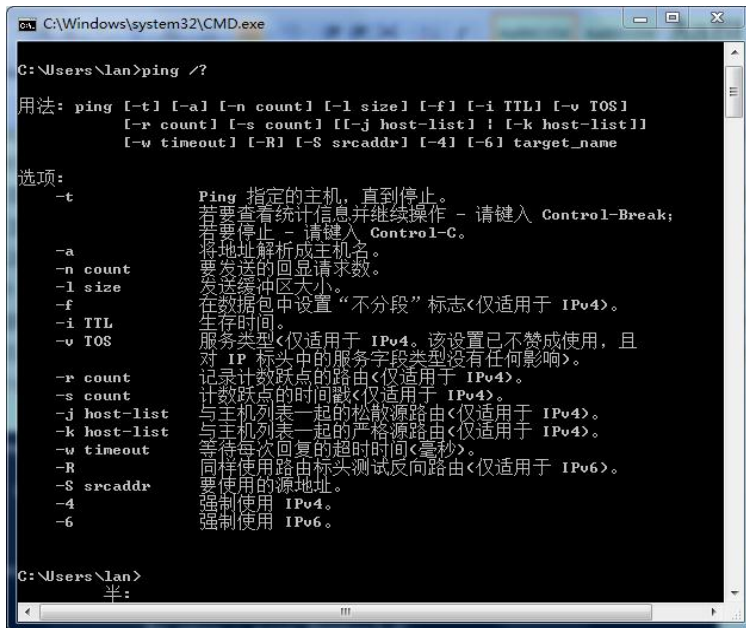
IP range: 192.168.2.1~192.168.2.254

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



```
C:\Windows\system32\CMD.exe

C:\Users\lan>ping /?

用法: 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] [-4] [-6] target_name

选项:
-t          Ping 指定的主机, 直到停止。
            若要查看统计信息并继续操作 - 请键入 Control-Break;
            若要停止 - 请键入 Control-C。
-a          将地址解析成主机名。
-n count    要发送的回显请求数。
-l size      发送缓冲区大小。
-f          在数据包中设置“不分段”标志<仅适用于 IPv4>。
-i TTL      生存时间。
-v TOS      服务类型<仅适用于 IPv4。该设置已不赞成使用, 且
            对 IP 标头中的服务字段类型没有任何影响>。
-r count    记录计数跃点的路由<仅适用于 IPv4>。
-s count    计数跃点的时间戳<仅适用于 IPv4>。
-j host-list 与主机列表一起的松散源路由<仅适用于 IPv4>。
-k host-list 与主机列表一起的严格源路由<仅适用于 IPv4>。
-w timeout  等待每次回复的超时时间<毫秒>。
-R          同样使用路由标头测试反向路由<仅适用于 IPv6>。
-S srcaddr  要使用的源地址。
-4          强制使用 IPv4。
-6          强制使用 IPv6。

C:\Users\lan>
```

- Options:

— -t

— -i

— -n

- Try:

‘ping [www.sustech.edu.cn](http://www.sustech.edu.cn) -t -n -3’

‘ping [www.sustech.edu.cn](http://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

```
C:\Windows\system32\cmd.exe

C:\Users\lan>netstat /?

显示协议统计和当前 TCP/IP 网络连接。

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]

-a          显示所有连接和侦听端口。
-b          显示在创建每个连接或侦听端口时涉及的可执行程序。
             在某些情况下，已知可执行程序承载多个独立的
             组件，这些情况下，显示创建连接或侦听端口时涉
             及的组件序列。此情况下，可执行程序名称位于
             底部[]中，它调用的组件位于顶部，直至达到
             TCP/IP。注意，此选项可能很耗时，并且在您没有
             足够权限时可能失败。
-e          显示以太网统计。此选项可以与 -s 选项结合使用。
-f          显示外部地址的完全限定域名(FQDN)。
-n          以数字形式显示地址和端口号。
-o          显示拥有的与每个连接关联的进程 ID。
-p proto    显示 proto 指定的协议的连接；proto 可以是下列任
             何一个：TCP、UDP、TCPv6 或 UDPv6。如果与 -s 选
             项一起用来显示每个协议的统计，proto 可以是下列任
             何一个：IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP
             或 UDPv6。
-r          显示路由表。
-s          显示每个协议的统计。默认情况下，显示
             IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6
             的统计；-p 选项可用于指定默认的子网。
-t          显示当前连接就绪状态。
interval    重新显示选定的统计，各个显示间隔的间隔秒数。
             按 CTRL+C 停止重新显示统计。如果省略，则 netstat
             将打印当前的配置信息一次。

C:\Users\lan>
```

```
C:\Users\lan>netstat

活动连接

协议 本地地址 外部地址 状态
TCP 10.20.128.16:33002 host-11:http CLOSE_WAIT
TCP 10.20.128.16:38002 58.205.221.250:http CLOSE_WAIT

C:\Users\lan>
```



# 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)

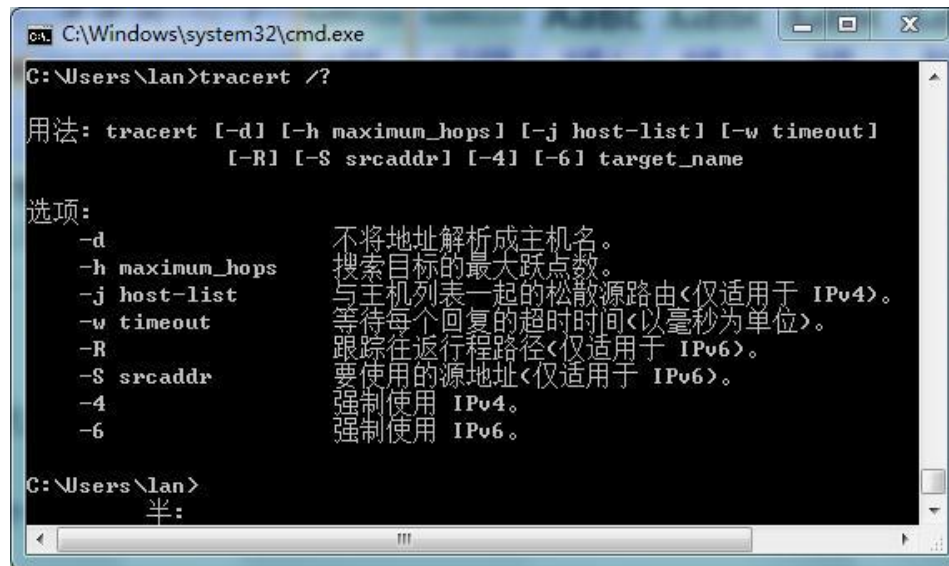
- LISTEN
  - Listening for connection requests from remote TCP ports
- SYN-SENT
  - Waiting for a matching connection request after sending a connection request
- SYN-RECEIVED
  - Waiting for confirmation of a connection request after receiving and sending a connection request
- ESTABLISHED
  - Represents 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.



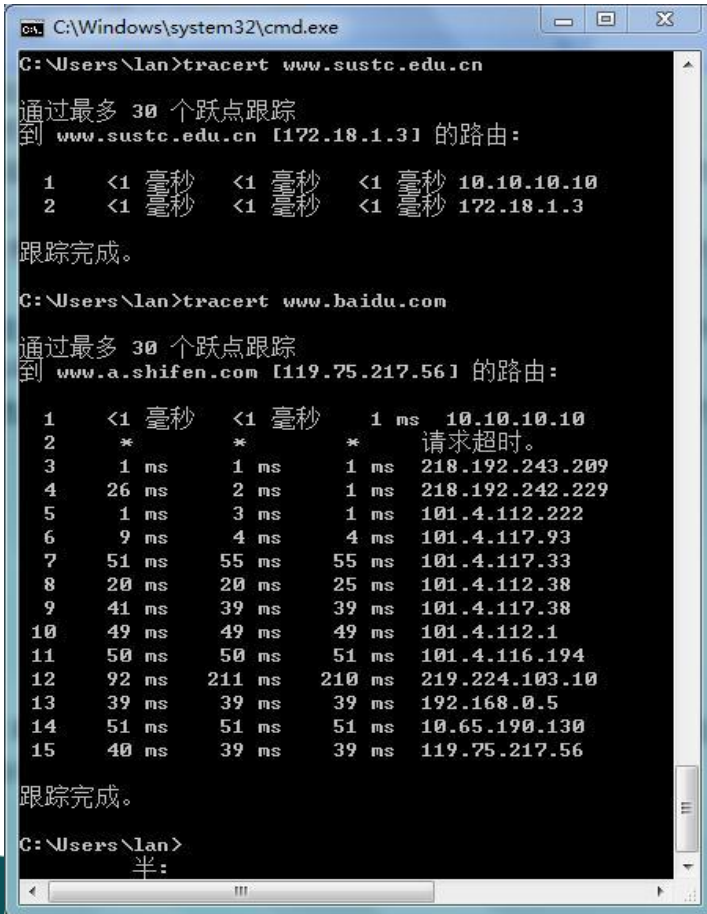
```
C:\Windows\system32\cmd.exe
C:\Users\lan>tracert /?

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

选项:
    -d          不将地址解析成主机名。
    -h maximum_hops  搜索目标的最大跃点数。
    -j host-list  与主机列表一起的松散源路由<仅适用于 IPv4>。
    -w timeout    等待每个回复的超时时间<以毫秒为单位>。
    -R          跟踪往返行程路径<仅适用于 IPv6>。
    -S srcaddr    要使用的源地址<仅适用于 IPv6>。
    -4          强制使用 IPv4。
    -6          强制使用 IPv6。

C:\Users\lan>
```

## 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

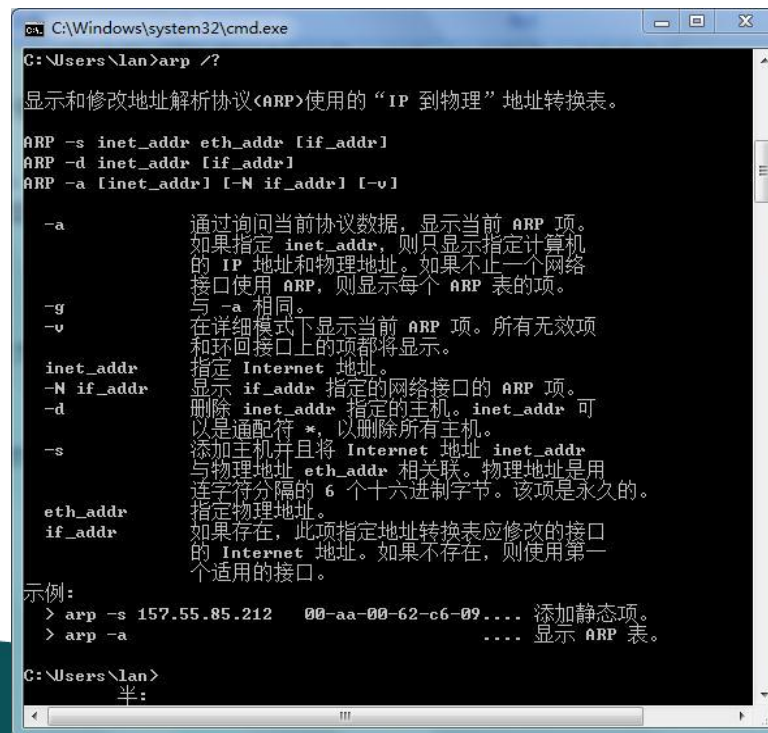
跟踪完成。

C:\Users\lan>
```

- 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.



```
C:\Windows\system32\cmd.exe
C:\Users\lan>arp /?

显示和修改地址解析协议<ARP>使用的“IP 到物理”地址转换表。

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

-a          通过询问当前协议数据，显示当前 ARP 项。
             如果指定 inet_addr，则只显示指定计算机
             的 IP 地址和物理地址。如果不止一个网络
             接口使用 ARP，则显示每个 ARP 表的项。
-g          与 -a 相同。
-v          在详细模式下显示当前 ARP 项。所有无效项
             和环回接口上的项都将显示。
inet_addr   指定 Internet 地址。
-N if_addr  显示 if_addr 指定的网络接口的 ARP 项。
-d          删除 inet_addr 指定的主机。inet_addr 可
             以是通配符 *，以删除所有主机。
-s          添加主机并且将 Internet 地址 inet_addr
             与物理地址 eth_addr 相关联。物理地址是用
             连字符分隔的 6 个十六进制字节。该项是永久的。
eth_addr    指定物理地址。
if_addr     如果存在，此项指定地址转换表应修改的接口
             的 Internet 地址。如果不存在，则使用第一
             个适用的接口。

示例：
> arp -s 157.55.85.212 00-aa-00-62-c6-09.... 添加静态项。
> arp -a          .... 显示 ARP 表。

C:\Users\lan>
```

## 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

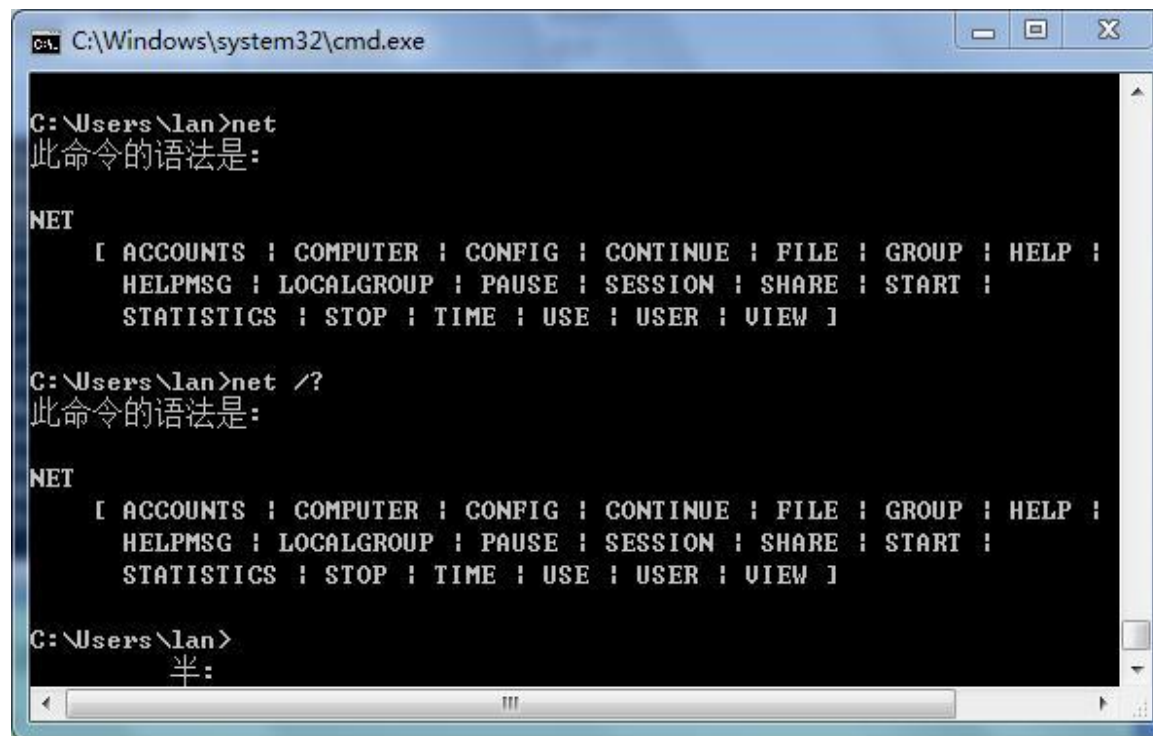


## 6. net (1)

- '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



```
C:\Windows\system32\cmd.exe

C:\Users\lan>net
此命令的语法是:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\lan>net /?
此命令的语法是:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\lan>
```

## 6. net (3)

```
C:\Users\lan>net stop "Security Center"
发生系统错误 5。

拒绝访问。

C:\Users\lan>
```

```
管理员: C:\Windows\System32\cmd.exe

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>net stop "Security Center"
Security Center 服务正在停止。
Security Center 服务已成功停止。

C:\Windows\system32>net start "Security Center"
Security Center 服务正在启动。
Security Center 服务已经启动成功。

C:\Windows\system32>
```

- 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



```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>nslookup www.baidu.com
服务器:  dnspai-public-dns.dnspai.com
Address:  140.207.198.6

非权威应答:
名称:     www.a.shifen.com
Addresses: 14.215.177.38
          14.215.177.39
Aliases:  www.baidu.com

C:\Users\Administrator>nslookup 140.207.198.6
服务器:  dnspai-public-dns.dnspai.com
Address:  140.207.198.6

名称:     dnspai-public-dns.dnspai.com
Address:  140.207.198.6

C:\Users\Administrator>
```

# 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](http://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),