

IP Address { IPv4: 32位, 8位一组 在网络层中。网络中端系统的名字。  
IPv6 可以重复(在不同局域网中), 可以修改。

MAC Address: 在物理层中网卡地址, 每个都是独一无二的。出厂时就设置好了, 不可修改。(也称为physical address)

Domain Name: www.sustech.edu.cn

常用命令:

## ① ipconfig

- "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] ]
```

- 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. . . . . : 90-61-80-00-00-00  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::...::...::... (Preferred)  
IPv4 Address. . . . . : 192.168.2.104 (Preferred)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained. . . . . : 2021/9/31 21:36:09  
Lease Expires . . . . . : 2021/9/31 8:01:29  
Default Gateway . . . . . : 192.168.2.1  
DHCP Server . . . . . : 192.168.2.1  
DHCPv6 IAD . . . . . : 27897646  
DHCPv6 Client DUID. . . . . : 00-01-00-01-...-00-01-00-01-...-00-01-00-01-...  
DNS Servers . . . . . : 116.77.76.234  
NetBIOS over Tcpip. . . . . : Enabled
```

- In the following pictures, PC1 and PC2 are in two different 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



默认网关: 发出去的信息的第一跳的路由地址  
(Default Gateway) ↓ (router)

子网掩码: 用于划分子网  
(Subnet Mask) → 32位10进制

物理地址: 48位16进制

IPv4: 点号分4组10进制, 每组8bit

IPv6: 冒号分8组16进制, 每组16bit

(IPv6中若有连续的冒号, 中间全0, 但只能出现一次)

IP地址和子网掩码按位相与后可得到子网号, 同一个子网可直接交换信息, 不同的要通过路由交换。

## ② arp

- “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.
            Same as "a".
-h          Displays current ARP entries in verbose mode. All invalid
            entries and entries on the loopback interface will be shown.
            Specifies an internet address.
-i 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.
            Specifies a physical address.
            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-00-02-cd-09 .... Add a static entry.
> arp -a .... Displays the arp table.
```

- 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

ARP Protocol: 地址解析协议

ARP缓存表: 看与本机交互过的IP和MAC的映射关系.

## 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
```

可以解析域名. 查找域名和IP的对应关系.

## 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] [-s size] [-f] [-i TTL] [-v TOS]
           [-c count] [-q count] [-l host-list] [-k host-list]
           [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
           [-q] [-G] target_name

Options:
-t          Ping the specified host until stopped.
-i          To see statistics and continue - type Control-Break;
-a          To stop - type Control-C.
-n count   Resolve addresses to hostnames.
-s size    Number of echo requests to send.
-f          Send buffer size.
-i TTL     Set Don't Fragment flag in packet (IPv4-only).
-v TOS     Time To Live.
-R          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).
-q count   Timestamp for count hops (IPv4-only).
-l 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.
-S          Use routing header to test reverse route also (IPv6-only).
           Per RFC 3095 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.
-q          Force using IPv4.
-G          Force using IPv6.
```

检查网络连通性.



- 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 above? Check the value of IP address, TTL and time, explain why they are not all the same.

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

Pinging www.sustech.edu.cn [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=9ms 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 = 9ms, Maximum = 12ms, Average = 9ms
```

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

## ⑤ tracert

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

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

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 roundtrip path (IPv6-only).
  -S srcaddr  Source address to use (IPv6-only).
  -4          Force using IPv4.
  -6          Force using IPv6.
```

## 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).

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

Tracing route to www.sustech.edu.cn [103.78.127.222]
over a maximum of 30 hops:
  0  1 ms  1 ms  <1 ms  192.168.2.1
  1  10 ms  14 ms  10 ms  10.245.100.1
  2  21 ms  34 ms  10 ms  10.21.238.254
  3  11 ms  13 ms  9 ms  10.234.77.85
  4  *  *  *  10.254.46.90
  5  *  *  *  Request timed out.
  6  *  *  *  Request timed out.
  7  *  *  *  Request timed out.
  8  *  *  *  Request timed out.
  9  10 ms  0 ms  10 ms  103.78.127.222

Trace complete.

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

Tracing route to www.baidu.com [163.177.151.110]
over a maximum of 30 hops:
  0  1 ms  1 ms  2 ms  192.168.2.1
  1  33 ms  40 ms  17 ms  10.245.100.1
  2  11 ms  11 ms  9 ms  10.21.238.254
  3  11 ms  10 ms  9 ms  10.234.77.85
  4  9 ms  10 ms  9 ms  10.254.46.90
  5  *  *  *  Request timed out.
  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.
```

(Time-to-live 这个Time指跳数)

TTL会限制转发次数, 每次转发TTL值都会减1, 为0时不再转发, 以避免占用过多网络资源.

ping会总共发4个包来检查是否连通

能查看路由信息.

TTL依次加1, 每次发3个包.

## ⑥ netstat

- “**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	1384048	1071760
Non-unicast packets	13234544	42138
Discards	0	0
Errors	0	0
Unknown protocols	0	0

SUSTech  
Shenzhen University  
of Science and Technology

- 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 -ano tcp
Active Connections


```

Proto	Local Address	Foreign Address	State	PID
TCP	127.0.0.1:20860	127.0.0.1:61495	ESTABLISHED	10900
TCP	127.0.0.1:30001	127.0.0.1:63612	TIME_WAIT	0
TCP	127.0.0.1:30001	127.0.0.1:63613	TIME_WAIT	0
TCP	127.0.0.1:30001	127.0.0.1:63614	TIME_WAIT	0
TCP	127.0.0.1:30001	127.0.0.1:63615	TIME_WAIT	0
TCP	127.0.0.1:30001	127.0.0.1:59693	ESTABLISHED	14984
TCP	127.0.0.1:50061	127.0.0.1:34832	ESTABLISHED	14984
TCP	127.0.0.1:50061	127.0.0.1:69285	ESTABLISHED	14984
TCP	127.0.0.1:50063	127.0.0.1:50061	ESTABLISHED	21738
TCP	127.0.0.1:50062	127.0.0.1:50061	ESTABLISHED	16205
TCP	127.0.0.1:61495	127.0.0.1:20860	ESTABLISHED	21602
TCP	127.0.0.1:63285	127.0.0.1:50061	ESTABLISHED	4004
TCP	192.168.2.104:49197	180.163.131.166:443	ESTABLISHED	8836
TCP	192.168.2.104:49542	142.251.42.234:443	SYN_SENT	8836
TCP	192.168.2.104:49543	163.177.131.110:443	FIN_WAIT_1	14436
TCP	192.168.2.104:49558	183.78.126.107:443	ESTABLISHED	8836
TCP	192.168.2.104:49561	149.206.78.14:80	ESTABLISHED	11684

SUSTech