# 第七章常用网络命令

# 本章主要内容

1. ping
2. ARP
3. Tracert
4. Route
5. ipconfig
6. Netstat
7. Nbtstat
8. Pathping
9. Netsh
10. net

# Ping简介

- **原理：**源站点向目的站点发送ICMP request报文,目的主机收到后回icmp repaly 报文.这样就验证了两个接点之间IP的可达性.

- **功能：**用ping 来判断两个接点在网络层的连通性.

# Ping使用方法

**其他参数:**

Ping –n 连续ping N个包

Ping –t 持续地Ping直到人为地中断,ctrl+breack暂时终止Ping命令查看当前的统计结果,而ctrl+c则是中断命令的执行

Ping –l 指定每个ping 报文的所携带的数据部分字节 0-65500数

```
C:\>ping -l 3000 -n 2 10.15.50.1

Pinging 10.15.50.1 with 3000 bytes of data

Reply from 10.15.50.1: bytes=3000 time=321ms TTL=123

Reply from 10.15.50.1: bytes=3000 time=297ms TTL=123

Ping statistics for 10.15.50.1:

    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 297ms, Maximum =  321ms, Average =  309ms
```

# Ping出错信息

**unkonw host**

主机名不可以解析为IP地址，故障原因可能是DNS server

**Network unreacheble**

表示本地系统没有到达远程主机的路由。检查路由表的配置

netstat –r或是route print

**No answer**

表示本地系统有到达远程主机的路由，但接受不到远程主机返回报文

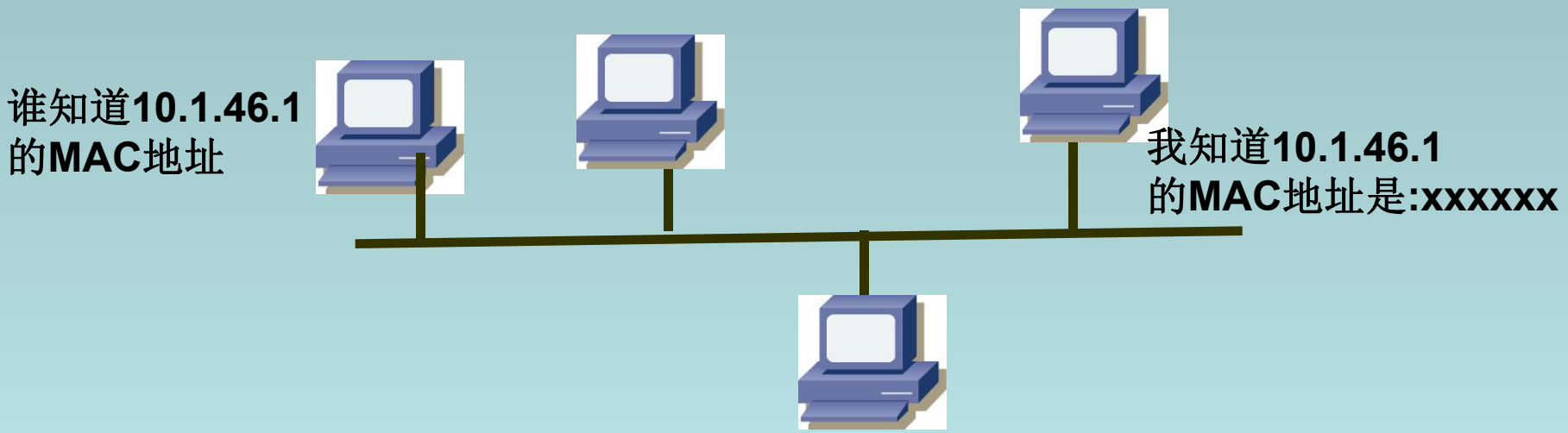
**Request timed out**

可能原因远程主机禁止了ICMP报文或是硬件连接问题

# ARP 地址解析协议

- **原理:**arp即地址解析协议,在常用以太网或令牌LAN上,用于实现第三层到第二层地址的转换IP → MAC

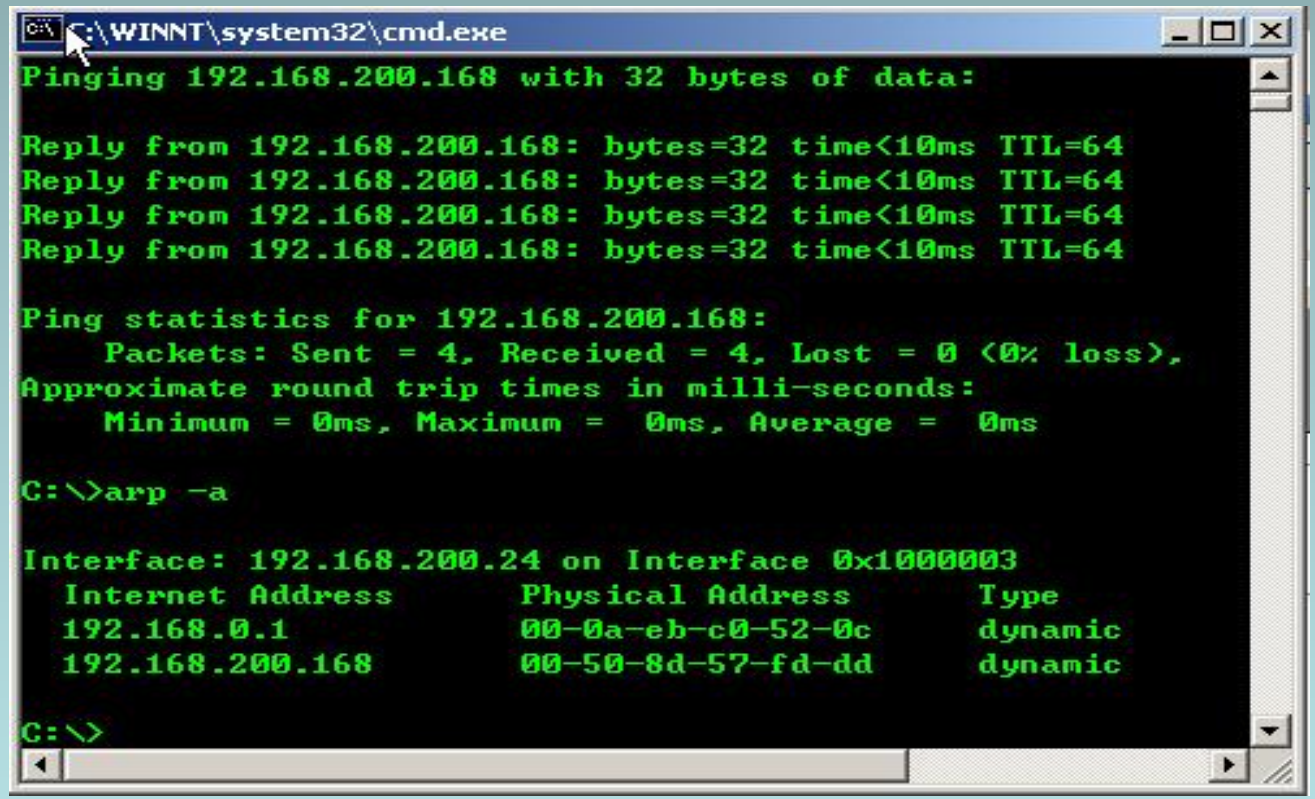
- **功能:**显示和修改IP地址与MAC地址的之间映射.



# ARP使用方法

常用参数:

Arp –a :显示所有的ARP表项. 例



# ARP使用方法

**其他参数:**

Arp -s:在ARP缓存中添加一条记录.

C:\>Arp -s 126.13.156.2 02-e0-fc-fe-01-b9

Arp -d:在ARP缓存中删除一条记录.

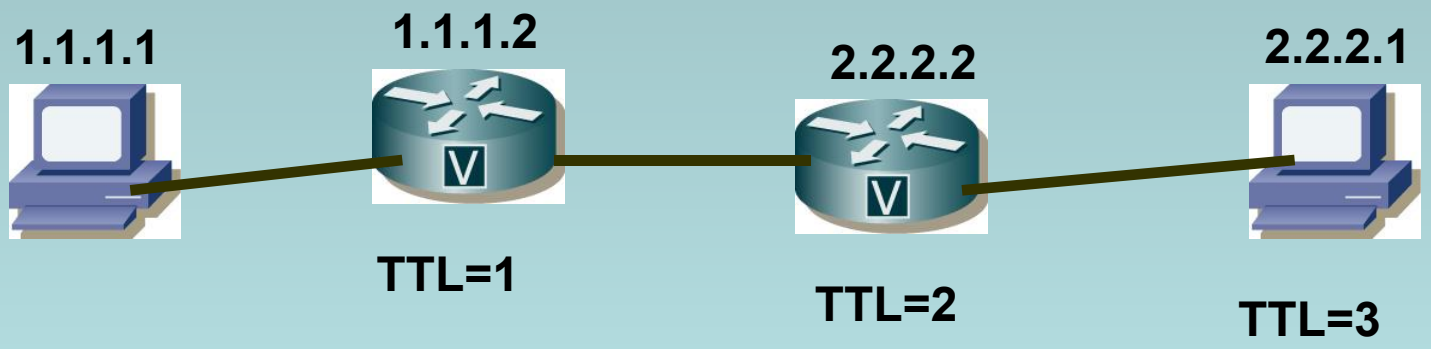
C:\>Arp -d 126.13.156.2

Arp -g:显示所有的表项

C:\>Arp -g

# Tracert 简介

- **原理:**tracert 是为了探测源节点到目的节点之间数据报文经过的路径.利用IP报文的TTL域在每个经过一个路由器的转发后减一,如果此时TTL=0则向源节点报告TTL超时这个特性,从一开始逐一增加TTL,直到到达目的站点或TTL达到最大值255.
- **功能:**探索两个节点的路由.



# Tracert使用方法

常用参数

c:\>tracert ip_adress

```
C:\>tracert 10.15.50.1

Tracing route to 10.15.50.1
over a maximum of 30 hops:

  1     3 ms     2 ms     2 ms  10.110.40.1
  2    14 ms     6 ms     3 ms  10.110.0.64
  3     3 ms     4 ms     5 ms  10.110.7.254
  4   157 ms   219 ms   209 ms  10.3.0.177
  5   222 ms   204 ms   128 ms  129.9.181.254
  6   151 ms   194 ms   167 ms  KJY-FS [10.15.50.1]

Trace complete.
```

# Tracert使用方法

**其他参数:**

Tracert -h N　设置TTL最大为N.

```
C:\>tracert -h 2 kjy-fs

Tracing route to kjy-fs.huawei.com.cn [10.15.50.1]
over a maximum of 2 hops:

  1    3 ms    2 ms    2 ms  10.110.40.1
  2    5 ms    3 ms    2 ms  10.110.0.64

Trace complete.
```

# Route简介

- **原理:** 路由是IP层的核心问题,路由表是TCP/IP协议栈所必须的核心数据结构,是IP选路的唯一依据.

- **功能:**route命令是操作，维护路由表的重要工具.

# route 使用方法

常用参数:

Route print 查看路由表.

```
C:\>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 0d 61 94 b8 33 ...... NDIS 5.0 driver

===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1  192.168.200.24       1
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
      192.168.0.0      255.255.0.0  192.168.200.24  192.168.200.24       1
   192.168.200.24  255.255.255.255        127.0.0.1        127.0.0.1       1
  192.168.200.255  255.255.255.255  192.168.200.24  192.168.200.24       1
        224.0.0.0        224.0.0.0  192.168.200.24  192.168.200.24       1
  255.255.255.255  255.255.255.255  192.168.200.24  192.168.200.24       1
Default Gateway:       192.168.0.1
===========================================================================
Persistent Routes:
  None
```

# route 使用方法

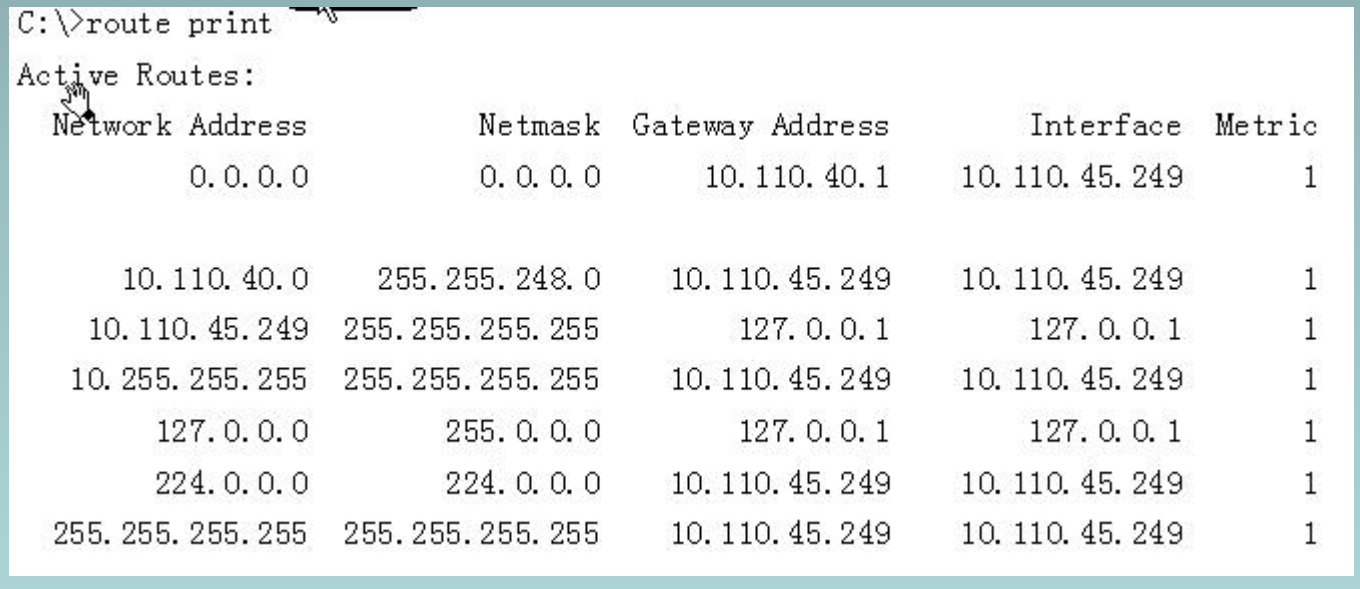
Route add 增加一条路由记录.

```
C:\>route add 1.1.0.0 mask 255.255.0.0 10.110.41.20 metric 3
C:\>route print
Active Routes:
  Network Address          Netmask  Gateway Address       Interface  Metric
          0.0.0.0          0.0.0.0     10.110.40.1   10.110.45.249       1
          1.1.0.0      255.255.0.0    10.110.41.20   10.110.45.249       3
       10.110.40.0    255.255.248.0   10.110.45.249   10.110.45.249       1
      10.110.45.249  255.255.255.255       127.0.0.1       127.0.0.1       1
     10.255.255.255  255.255.255.255   10.110.45.249   10.110.45.249       1
          127.0.0.0        255.0.0.0       127.0.0.1       127.0.0.1       1
          224.0.0.0        224.0.0.0   10.110.45.249   10.110.45.249       1
    255.255.255.255  255.255.255.255   10.110.45.249   10.110.45.249       1
```

# route 使用方法

Route delete　删除一条路由记录.

C:\> route delete 1.1.0.0



```
C:\>route print
Active Routes:
  Network Address          Netmask  Gateway Address       Interface  Metric
          0.0.0.0          0.0.0.0      10.110.40.1   10.110.45.249       1

       10.110.40.0    255.255.248.0   10.110.45.249   10.110.45.249       1
     10.110.45.249  255.255.255.255      127.0.0.1       127.0.0.1       1
    10.255.255.255  255.255.255.255   10.110.45.249   10.110.45.249       1
          127.0.0.0        255.0.0.0      127.0.0.1       127.0.0.1       1
          224.0.0.0        224.0.0.0   10.110.45.249   10.110.45.249       1
    255.255.255.255  255.255.255.255   10.110.45.249   10.110.45.249       1
```

# route 使用方法

Route –p add 永久地增加一条路由记录(重起后不丢失NT)

```
C:\>route -p add 1.1.1.1 mask 255.255.255.255 10.110.41.20 metric 4
C:\>route print
Active Routes:
  Network Address          Netmask  Gateway Address        Interface  Metric
        0.0.0.0          0.0.0.0      10.110.40.1    10.110.45.249       1
        1.1.1.1  255.255.255.255     10.110.41.20    10.110.45.249       4
     10.110.40.0    255.255.248.0    10.110.45.249    10.110.45.249       1
   10.110.45.249  255.255.255.255        127.0.0.1        127.0.0.1       1
  10.255.255.255  255.255.255.255    10.110.45.249    10.110.45.249       1
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
        224.0.0.0        224.0.0.0    10.110.45.249    10.110.45.249       1
  255.255.255.255  255.255.255.255    10.110.45.249    10.110.45.249       1
```

# Netstat 命令介绍

**netstat** 命令显示协议统计信息和当前的 TCP/IP 连接。该命令只有在安

装了 TCP/IP 协议后才可以使用

```
D:\>netstat /help

Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]

  -a            Displays all connections and listening ports.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -n            Displays addresses and port numbers in numerical form.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be TCP or UDP.  If used with the -s option to display
                per-protocol statistics, proto may be TCP, UDP, or IP.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for TCP, UDP and IP; the -p option may be used to specify
                a subset of the default.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
```

# Netstat 参数使用之一

**Netstat** [**-a**] [**-e**] [**-n**] [**-s**] [**-p** *protocol*] [**-r**] [*interval*]

**- a** 显示所有连接和侦听端口。服务器连接通常不显示。

```
C:\>netstat -a

Active Connections

Proto Local Address          Foreign Address        State
TCP   CORP1:1572       172.16.48.10:nbsession   ESTABLISHED
TCP   CORP1:1589       172.16.48.10:nbsession   ESTABLISHED
TCP   CORP1:1606       172.16.105.245:nbsession ESTABLISHED
TCP   CORP1:1632       172.16.48.213:nbsession  ESTABLISHED
TCP   CORP1:1659       172.16.48.169:nbsession  ESTABLISHED
TCP   CORP1:1714       172.16.48.203:nbsession  ESTABLISHED
TCP   CORP1:1719       172.16.48.36:nbsession   ESTABLISHED
TCP   CORP1:1241       172.16.48.101:nbsession  ESTABLISHED
UDP   CORP1:1025       *:*
UDP   CORP1:snmp       *:*
UDP   CORP1:nbname     *:*
UDP   CORP1:nbdatagram *:*
UDP   CORP1:nbname     *:*
UDP   CORP1:nbdatagram *:*
```

# Netstat 参数使用之二

**-e** 显示以太网统计。该参数可以与 **-s** 选项结合使用。

```
C:\>netstat -s
IP Statistics

Packets Received                   = 5378528
Received Header Errors             = 738854
Received Address Errors            = 23150
Datagrams Forwarded                = 0
Unknown Protocols Received         = 0
Received Packets Discarded         = 0
Received Packets Delivered         = 4616524
Output Requests                    = 132702
Routing Discards                   = 157
Discarded Output Packets           = 0
Output Packet No Route             = 0
Reassembly Required                = 0
Reassembly Successful                 = 0
Reassembly Failures                   =
Datagrams Successfully Fragmented  = 0
Datagrams Failing Fragmentation    = 0
Fragments Created                     = 0
```

```
ICMP Statistics
Received  Sent
Messages                693         4
Errors                  0           0
Destination Unreachable 685         0
Time Exceeded           0           0
Parameter Problems      0           0
Source Quenches         0           0
Redirects               0           0
Echoes                  4           0
Echo Replies            0           4
Timestamps              0           0
Timestamp Replies       0           0
Address Masks           0           0
Address Mask Replies    0           0
```

```
TCP Statistics

Active Opens                       = 597
Passive Opens                      = 135
Failed Connection Attempts         = 107
Reset Connections                  = 91
Current Connections                = 8
Segments Received                  = 106770
Segments Sent                      = 118431
Segments Retransmitted             = 461

UDP Statistics

Datagrams Received    = 4157136
No Ports              = 351928
Receive  Errors        = 2
 Datagrams Sent        = 13809
```

# Netstat 参数使用之三

**-n** 以数字格式显示IP地址和端口号（而不是尝试查找名称）。

```
D:\>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.200.1:1230     192.168.200.247:139    ESTABLISHED
  TCP    192.168.200.1:1236     211.196.154.198:80     ESTABLISHED
  TCP    192.168.200.1:1238     61.233.40.99:80        ESTABLISHED
  TCP    192.168.200.1:1239     61.233.40.99:80        ESTABLISHED
  TCP    192.168.200.1:1240     61.233.40.99:80        ESTABLISHED
  TCP    192.168.200.1:1241     61.233.40.99:80        ESTABLISHED
  TCP    192.168.200.1:1243     61.141.32.89:80        ESTABLISHED
  TCP    192.168.200.1:1246     218.22.10.251:80       ESTABLISHED
  TCP    192.168.200.1:1247     218.22.10.251:80       ESTABLISHED
  TCP    192.168.200.1:1251     210.78.148.25:80       ESTABLISHED
  TCP    192.168.200.1:1257     211.196.154.182:80     ESTABLISHED
  TCP    192.168.200.1:1259     61.152.94.134:80       ESTABLISHED
  TCP    192.168.200.1:1260     61.152.94.134:80       ESTABLISHED
```

# Netstat 参数使用之四

**-r**
显示路由表的内容。

**interval**
重新显示所选的统计，在每次显示之间暂停 interval 秒。按 CTRL+B 停止重新显示统计。如果省略该参数，netstat 将打印一次当前的配置信息。

# Netstat 参数使用之五

**-s**
显示每个协议的统计。默认情况下，显示 TCP、UDP、ICMP 和 IP 的统计。-p 选项可以用来指定默认的子集。

**-p protocol**
显示由 protocol 指定的协议的连接；protocol 可以是 tcp 或 udp。如果与 -s 选项一同使用显示每个协议的统计，protocol 可以是 tcp、udp、icmp 或 ip。

# Nbtstat 命令介绍

**Nbtstat**：是解决 NetBIOS 名称解析问题的有用工具。可以使用 **nbtstat** 命令删除或更正预加载的项目

**NETBIOS名字分两种类型：**

唯一名(UNIQUE)和组名(GROUP)。唯一名很好理解，就是说在同一子网上要独一为二；而组名的作用是可以实现多播数据通讯。

**NETBIOS结构：字符串和ScopeID**

字符串 就是我们给自己的计算机、工作组起的名字，而且对所能使用的字符及其长度都有限制

ScopeID域 它占用NETBIOS名的最后一个字节，最大的作用莫过于可以标识不同的Microsoft网络服务因为它是NETBIOS名的一部分

因此UNIQUEname允许两台computername相同但scopeID不同的计算机在同一子网上存在。

# Nbtstat参数使用之一

**nbtstat -n** 显示由服务器或重定向器之类的程序在系统上本地注册的名称。
“已注册”表明该名称已被广播 (Bnode) 或者 WINS（其他节点类型）注册

Node IpAddress: [192.168.200.1] Scope Id: [ ]

NetBIOS Local Name Table

| Name | Type | Status |
|---|---|---|
| XHWL-SERVER | <00> UNIQUE | Registered |
| XHWL-SERVER | <03> UNIQUE | Registered |
| WORKGROUP | <00> GROUP | Registered |
| WORKGROUP | <1E> GROUP | Registered |
| XHWL-SERVER | <20> UNIQUE | Registered |

# Nbtstat参数使用之二

**Nbtstat [-a remotename] [-A IP address] [-c] [-n] [-R] [-r] [-S] [-s]**

**nbtstat –A** 使用远程计算机的 **IP** 地址并列出名称表。

**nbtstat –a** 对指定***name***的计算机执行 **NetBIOS** 适配器状态命令。适配器状态命令将返回计算机的本地 **NetBIOS** 名称表，以及适配器的媒体访问控制地址。

# 例子 nbtstat -A

例子：Nbtstat [-a remotename] [-A IP address]

c:\>nbtstat –A 192.168.12.27

本地连接 2:

Node IpAddress: [192.168.12.1] Scope Id: [ ]

NetBIOS Remote Machine Name Table

| Name | Type | Status |
|---|---|---|
| SDXH-11 | <00> | UNIQUE Registered |
| SDXH-11 | <20> | UNIQUE Registered |
| WORKGROUP | <00> | GROUP Registered |
| WORKGROUP | <1E> | GROUP Registered |
| SDXH-11 | <03> | UNIQUE Registered |
| INet~Services | <1C> | GROUP Registered |
| IS~SDXH-11..... | <00> | UNIQUE Registered |

MAC Address = 00-E0-4C-61-4F-BC

# Nbtstat参数使用之三

**nbtstat -c** 显示 **NetBIOS** 名称缓存，包含其他计算机的名称对地址映射

**Nbtstat –r** 列出 **Windows** 网络名称解析的名称解析统计。在配置使用 **WINS** 的 **Windows 2000** 计算机上，此选项返回要通过广播或 **WINS** 来解析和注册的名称数。

**nbtstat -R** 清除名称缓存，然后从 **Lmhosts** 文件重新加载。

**nbtstat -RR** 释放在 **WINS** 服务器上注册的 **NetBIOS** 名称，然后刷新它们的注册

# 例子nbtstat - r

NetBIOS Names Resolution and Registration Statistics

---

Resolved By Broadcast = 6

Resolved By Name Server = 0

Registered By Broadcast = 22

Registered By Name Server = 0

NetBIOS Names Resolved By Broadcast

---

SDXH-15
SDXH-15
SDXH-11 <00>
SDXH-07
SDXH-15
SDXH-15

# Nbtstat参数使用之四

**Nbtstat –s** 显示客户端和服务器会话。尝试将远程计算机 **IP** 地址转换成使用主机文件的名称。

**nbtstat -S** 列出当前的 **NetBIOS** 会话及其状态（包括统计）
只通过 **IP** 地址列出远程计算机。

# ipconfig 命令介绍

**ipconfig** 命令获得主机配置信息，包括 IP 地址、子网掩码和默认网关。

对于 Windows 95 和 Windows 98 的客户机，
请使用 **winipcfg** 命令而不是 **ipconfig** 命令。

# ipconfig参数使用

**1 ipconfig**

当使用IPConfig时不带任何参数选项，那么它为每个已经配置了的接口显示IP地址、子网掩码和缺省网关值。

**2 ipconfig /all**

当使用all选项时，IPConfig能为DNS和WINS服务器显示它已配置且所要使用的附加信息（如IP地址等），并且显示内置于本地网卡中的物理地址（MAC）。如果IP地址是从DHCP服务器租用的，IPConfig将显示DHCP服务器的IP地址和 租用地址预计失效的日期。

**3 ipconfig /release和ipconfig /renew**

这是两个附加选项，只能在向DHCP服务器租用其IP地址的计算机上起作用。如果我们输入ipconfig /release，那么所有接口的租用IP地址便重新交付给DHCP服务器（归还IP地址）。如果我们输入ipconfig /renew，那么本地计算机便设法与DHCP服务器取得联系，并租用一个IP地址。请注意，大多数情况下网卡将被重新赋予和以前所赋予的相同的IP地址。

# Pathping命令介绍

pathping 命令是一个路由跟踪工具，它将 ping 和 tracert 命令的功能和这两个工具所不提供的其他信息结合起来。pathping 命令在一段时间内将数据包发送到到达最终目标的路径上的每个路由器，然后基于数据包的计算机结果从每个跃点返回。
由于命令显示数据包在任何给定路由器或链接上丢失的程度，因此可以很容易地确定可能导致网络问题的路由器或链接。

# Pathping参数选项

pathping [-n] [-h maximum_hops] [-g host-list] [-p period]

[-q num_queries] [-w timeout] [-t] [-R] [-r] target_name

Options:

-n Do not resolve addresses to hostnames.

-h maximum_hops Maximum number of hops to search for target.

-g host-list Loose source route along host-list.

-p period Wait period milliseconds between pings.

-q num_queries Number of queries per hop.

-w timeout Wait timeout milliseconds for each reply.

-T Test connectivity to each hop with Layer-2 priority tags.

-R Test if each hop is RSVP aware.

# Pathping命令参数使用

**-n** 不将地址解析为主机名.

**-h** maximum_hops:指定搜索目标的最大越点数,默认值为30

**-g** host-list:允许沿着host-list将一系列计算机按中间网关分隔开来.

**-p** period:指定两个连续的探测(ping)之间的时间间隔(以毫秒单位)
默认值是250毫秒

**-q** num_queries:指定对路由所经过的每个计算机的查询次数,默认值为100

**-w** timeout:指定等待应答的时间,默认值是3000

**-t** 在向路由所经过的每个网络设备发送的探测数据包上附加一个2级优先级标记.该参数必须大写,例如 802.1q.

# Pathping例子

D:\>pathping -n msw
Tracing route to msw [7.54.1.196]

over a maximum of 30 hops:

**0** 172.16.87.35

**1** 172.16.87.218

**2** 192.68.52.1

**3** 192.68.80.1

**4** 7.54.247.14

**5** 7.54.1.196

# Pathping例子

Computing statistics for 125 seconds...

| Source to Here | | | This Node/Link | |
|---|---|---|---|---|
| **Hop** | **RTT** | **Lost/Sent = Pct** | **Lost/Sent = Pct** | **Address** |
| 0 | 1 | | | 72.16.87.35 |
| | | | 0/ 100 = 0% | |
| 1 | 41ms | 0/ 100 = 0% | 0/ 100 = 0% | 172.16.87.218 |
| | | | **13/ 100 = 13%** | |
| 2 | 22ms | 16/ 100 = 16% | 3/ 100 = 3% | 192.68.52.1 |
| | | | 0/ 100 = 0% | |
| 3 | 24ms | 13/ 100 = 13% | 0/ 100 = 0% | 192.68.80.1 |
| | | | 0/ 100 = 0% | |
| 4 | 21ms | 14/ 100 = 14% | **1/ 100 = 1%** | 10.54.247.14 |
| | | | 0/ 100 = 0% | |
| 5 | 24ms | 13/ 100 = 13% | 0/ 100 = 0% | 10.54.1.196 |

Trace complete.

# Netsh 命令介绍

给用户提供一种交互方式操作的办法
Windows 2000 的 cmd shell 下，输入 netsh
就出来：netsh> 提示符，
输入 int ip 就显示：
interface ip>
例：输入 dump ，我们就可以看到当前系统的网络配置：

# interface ip>dump

```
# ------------------------------
# Interface IP Configuration
# ------------------------------
pushd interface ip
# Interface IP Configuration for "Local Area Connection"
set address name = "Local Area Connection" source = static
addr = 192.168.1.168
mask = 255.255.255.0
add address name = "Local Area Connection" addr = 192.1.1.111
mask = 255.255.255.0
set address name = "Local Area Connection" gateway =192.168.1.100
gwmetric = 1
set dns name = "Local Area Connection" source = static addr = 202.96.209.5
set wins name = "Local Area Connection" source = static addr = none
popd
# End of interface IP configuration
```

# interface ip>add

Interface ip>add ?
Interfaec ip>address
Interface ip>dns
Interface ip>wins

例：给网络接口指定一个IP地址和默认网关：

Netsh>
Netsh>interface ip
Interface ip>add address “Local Area connection” 192.168.200.1 255.255.255.0
Interface ip>add address “Local Area connection” gateway=192.168.0.1
gwmetirc=1

# Net命令介绍

**NET** 命令是一个命令行命令，Net 命令有很多函数用于实用和核查计算机之间的NetBIOS连接，可以查看我们的管理网络环境、服务、用户、登陆等信息内容

# 1、 Net view命令

作 用：显示域列表、计算机列表或指定计算机的共享资源列表。
命令格式：Net view [\\computername | /domain[:domainname]]
有关参数说明：

- 键入不带参数的Net view显示当前域的计算机列表
- \\computername 指定要查看其共享资源的计算机
- /domain[:domainname]指定要查看其可用计算机的域

例如：Net view \\xhwl-server查看xhwl-server计算机的共享资源列表。
Net view /domain:XYZ 查看XYZ域中的机器列表

# 2、Net User命令

**作 用：**添加或更改用户帐号或显示用户帐号信息。
**命令格式：**Net user [username [password | *] [options]] [/domain]
**有关参数说明：**

- 键入不带参数的Net user查看计算机上的用户帐号列表
- username添加、删除、更改或查看用户帐号名
- password为用户帐号分配或更改密码
- 提示输入密码
- /domain在计算机主域的主域控制器中执行操作。该参数仅在 Windows NT Server 域成员的 Windows NT Workstation 计算机上可用。默认情况下，Windows NT Server 计算机在主域控制器中执行操作。注意：在计算机主域的主域控制器发生该动作。它可能不是登录域。

**例如：**Net user test 查看用户test的信息。

# 3、Net Use

作 用：连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。

命令格式：Net use [devicename | *]
[\\computername\sharename[\volume]]
[password|*]]
[/user:[domainname\]username]
[[/delete]] [/persistent:{yes | no}]]

。

例如：Net use f: \\GHQ\TEMP 将**\\GHQ\TEMP**目录建立为**F**盘
Net use f: \GHQ\TEMP /delete 断开连接

# Net use有关参数说明

·键入不带参数的Net use列出网络连接
·devicename指定要连接到的资源名称或要断开的设备名称
·\\computername\sharename服务器及共享资源的名称
·password访问共享资源的密码
·*提示键入密码
·/user指定进行连接的另外一个用户
·domainname指定另一个域
·username指定登录的用户名
·/home将用户连接到其宿主目录
·/delete取消指定网络连接
·/persistent控制永久网络连接的使用。

# 4、Net Time

作 用：使计算机的时钟与另一台计算机或域的时间同步。
命令格式：Net time [\\computername | /domain[:name]] [/set]
有关参数说明：

- \\computername要检查或同步的服务器名
- /domain[:name]指定要与其时间同步的域
- /set使本计算机时钟与指定计算机或域的时钟同步。

# 5、启动 、暂停、 激活服务命令

**5、Net Start**

作 用：启动服务，或显示已启动服务的列表。

命令格式：Net start service

**6、Net Pause**

作 用：暂停正在运行的服务。

命令格式：Net pause service

**7、Net Continue**

作 用：重新激活挂起的服务。

命令格式：Net continue service

**8、Net Stop**

作 用：停止 Windows NT/2000/2003 网络服务。

命令格式：Net stop service

# 包含服务之一

(1)alerter(警报)；
(2)client service for Netware(Netware 客户端服务)
(3)clipbook server(剪贴簿服务器)
(4)computer browser(计算机浏览器)
(5)directory replicator(目录复制器)
(6)ftp publishing service (ftp )(ftp 发行服务)
(7)lpdsvc
(8)Net logon(网络登录)
(9)Network dde(网络 dde)
(10)Network dde dsdm(网络 dde dsdm)
(11)Network monitor agent(网络监控代理)
(12)ole(对象链接与嵌入)
(13)remote access connection manager(远程访问连接管理器)
(14)remote access isnsap service(远程访问 isnsap 服务)
(15)remote access server(远程访问服务器)

# 包含服务之二

(16)remote procedure call (rpc) locator(远程过程调用定位器)
(17)remote procedure call (rpc) service(远程过程调用服务)
(18)schedule(调度)
(19)server(服务器)
(20)simple tcp/ip services(简单 TCP/IP 服务)
(21)snmp
(22)spooler(后台打印程序)
(23)tcp/ip Netbios helper(TCP/IP NETBIOS 辅助工具)
(24)ups
(25)workstation(工作站)
(26)messenger(信使)
(27)dhcp client

# 9、Net Statistics

**作 用：**显示本地工作站或服务器服务的统计记录。
**命令格式：**Net statistics [workstation | server]
**有关参数说明：**

- 键入不带参数的Net statistics列出其统计信息可用的运行服务
- workstation显示本地工作站服务的统计信息
- server显示本地服务器服务的统计信息

**例如：**Net statistics server | more显示服务器服务的统计信息。

# 10、Net Share

**作 用：**创建、删除或显示共享资源。
**命令格式：**Net share sharename=drive:path
[/users:number | /unlimited] [/remark:"text"]
**有关参数说明：**

- 不带参数的Net share显示本地计算机上所有共享资源的信息
- sharename是共享资源的网络名称
- drive:path指定共享目录的绝对路径
- /users:number设置可同时访问共享资源的最大用户数
- /unlimited不限制同时访问共享资源的用户数
- /remark:"text "添加关于资源的注释，注释文字用引号引住

例如：Net share yesky=c:\temp /remark:“my first share”
以**yesky**为共享名共享**C:\temp**
Net share yesky /delete停止共享**yesky**目录

# 11、Net Session

**作 用：**列出或断开本地计算机和与之连接的客户端的会话。
**命令格式：**Net session [\\computername] [/delete]
**有关参数说明：**

·不带参数的Net session显示所有与本地计算机的会话的信息。
·\\computername标识要列出或断开会话的计算机。
·/delete结束与 \computername 计算机会话并关闭本次会话期间计算机的所有打开文件。如果省略\computername 参数，将取消与本地计算机的所有会话。

**例如：**Net session \\GHQ
要显示计算机名为GHQ的客户端会话信息列表。

# 12、Net Send

作 用：向网络的其他用户、计算机或通信名发送消息。
命令格式：Net send {name | * | /domain[:name] | /users}
message
有关参数说明：

- name要接收发送消息的用户名、计算机名或通信名
- * 将消息发送到组中所有名称
- /domain[:name]将消息发送到计算机域中的所有名称
- /users将消息发送到与服务器连接的所有用户
- message作为消息发送的文本

例如：**Net send** /users server will shutdown in 10 minutes.
给所有连接到服务器的用户发送消息。

# 13、Net Print

作 用：显示或控制打印作业及打印队列。
命令格式：Net print [\\computername ]
job# [/hold | /release | /delete]
有关参数说明：

- computername共享打印机队列的计算机名
- sharename打印队列名称
- job#在打印机队列中分配给打印作业的标识号
- /hold使用 job# 时，在打印机队列中使打印作业等待
- /release释放保留的打印作业
- /delete从打印机队列中删除打印作业

例如：Net print \\GHQ\HP8000
列出\\GHQ计算机上HP8000打印机队列的目录。

# 14、Net Name

**作 用：**添加或删除消息名（有时也称别名），或显示计算机接收消息的名称列表。

**命令格式：**Net name [name [/add | /delete]]

**有关参数说明：**

- 键入不带参数的Net name列出当前使用的名称
- name指定接收消息的名称
- /add将名称添加到计算机中
- /delete从计算机中删除名称

# 15、Net Localgroup

**作 用：**添加、显示或更改本地组。

**命令格式：**Net localgroup groupname
{/add [/comment:“text ”] | /delete} [/domain]

**有关参数说明：**

- ·不带参数的Net localgroup显示服务器名称和计算机的本地组名称
- ·groupname要添加、扩充或删除的本地组名称
- ·/comment: “text ”为新建或现有组添加注释
- ·/domain在当前域的主域控制器中执行操作，否则仅在本地计算机上执行操作
- ·/add将全局组名或用户名添加到本地组中
- ·/delete从本地组中删除组名或用户名

**例如：Net localgroup ggg /add**
将名为ggg的本地组添加到本地用户帐号数据库；
**Net localgroup ggg** 显示ggg本地组中的用户。

# 16、Net Group

作 用：在 Windows NT/2000/2003 Server 域中添加、显示或更改全局组。
命令格式：Net group groupname {/add [/comment:"text "] | /delete} [/domain]
有关参数说明：

- ·键入不带参数的Net group显示服务器名称及服务器的组名称
- ·groupname要添加、扩展或删除的组
- ·/comment:"text "为新建组或现有组添加注释
- ·/domain当前域的主域控制器中执行该操作，否则在本地计算机上执行操作
- ·username[ ...]列表显示要添加到组或从组中删除的一个或多个用户
- ·/add添加组或在组中添加用户名
- ·/delete删除组或从组中删除用户名

例：Net group ggg GHQ1 GHQ2 /add
将现有用户帐号GHQ1和GHQ2添加到本地计算机的ggg组。

# 17、Net File

**作 用：**显示某服务器上所有打开的共享文件名及锁定文件数。
**命令格式：**Net file [id [/close]]
**有关参数说明：**

- 键入不带参数的Net file获得服务器上打开文件的列表
- id文件标识号
- /close关闭打开的文件并释放锁定记录

# 18、Net Config

**作 用：**显示当前运行的可配置服务，或显示并更改某项服务的设置。
**命令格式：**Net config [service [options]]
**有关参数说明：**

- 键入不带参数的Net config显示可配置服务的列表
- service通过Net config命令进行配置的服务(server或workstation)
- options服务的特定选项

# 19、Net Computer

作 用：从域数据库中添加或删除计算机。
命令格式：Net computer \\computername {/add | /del}
有关参数说明：

·\\computername指定要添加到域或从域中删除的计算机
·/add将指定计算机添加到域
·/del将指定计算机从域中删除

例如：Net computer \\js /add将计算机js 添加到登录域。

# 20、Net Accounts

作 用：更新用户帐号数据库、更改密码及所有帐号的登录要求。

命令格式：Net accounts [/forcelogoff:{minutes | no}] [/minpwlen:length]
[/maxpwage:{days | unlimited}] [/minpwage:days]
[/uniquepw:number] [/domain]

有关参数说明：

·键入不带参数的Net accounts显示当前密码设置、登录时限及域信息

·/forcelogoff:{minutes | no}设置当用户帐号或有效登录时间过期时

·/minpwlen:length设置用户帐号密码的最少字符数

·/maxpwage:{days | unlimited}设置用户帐号密码有效的最大天数

·/minpwage:days设置用户必须保持原密码的最小天数

·/uniquepw:number要求用户更改密码时，必须在经过number次后才能重复使用与之相同的密码

·/domain在当前域的主域控制器上执行该操作

·/sync当用于主域控制器时，该命令使域中所有备份域控制器同步

例如：**Net accounts /minpwlen:8**

将用户帐号密码的最少字符数设置为8。