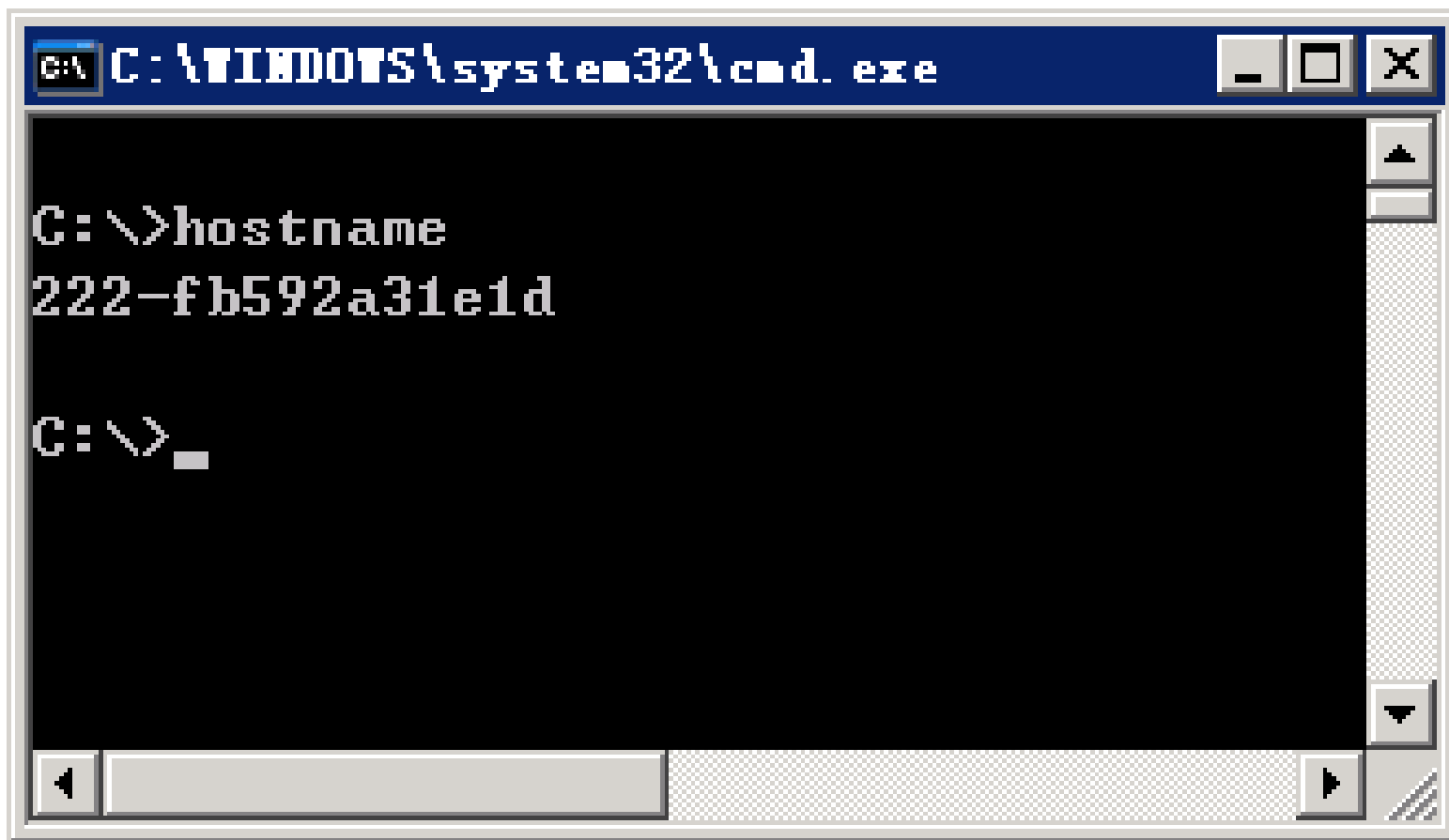


第6章 网络诊断命令

宣江华
宁波工程学院

1、hostname

- n **hostname**诊断程序用于显示当前的主机名。该命令不带任何参数

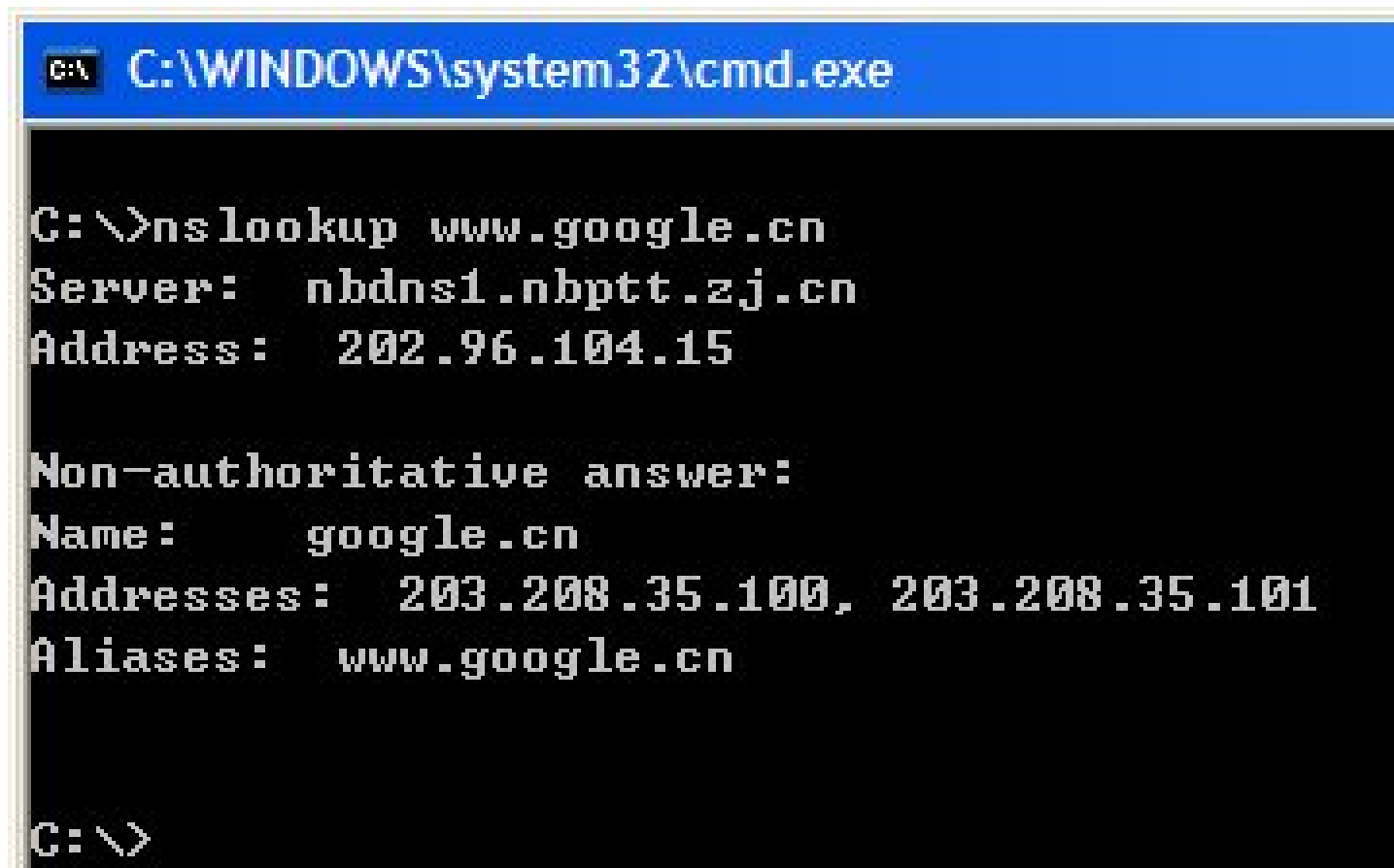


A screenshot of a Windows command prompt window. The title bar at the top reads "C:\WINDOWS\system32\cmd.exe". The command prompt shows the command "hostname" being entered and executed, resulting in the output "222-fb592a31e1d". The prompt "C:\>" is visible on the line below the output. The window has standard Windows XP-style window controls (minimize, maximize, close) in the top right corner and a scroll bar on the right side.

```
C:\>hostname
222-fb592a31e1d
C:\>_
```

2、nslookup

- n **nslookup**命令用于显示网络中**DNS**服务器的名字。
- n 交互模式和非交互模式、指定**DNS**服务器



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

C:\>nslookup www.google.cn
Server:  nbdns1.nbptt.zj.cn
Address:  202.96.104.15

Non-authoritative answer:
Name:     google.cn
Addresses: 203.208.35.100, 203.208.35.101
Aliases:  www.google.cn

C:\>
```

3、ipconfig (1)

- n **ipconfig**诊断程序用于显示当前**TCP/IP**协议的配置情况，并对其更新或释放。当不带任何参数时，**ipconfig**命令可以显示当前**TCP/IP**协议的基本配置情况，包括**IP地址（IP Address）**、子网掩码（**Subnet Mask**）和默认网关（**Default Gateway**）等。

3、ipconfig (2)

- n 可用于显示当前的**TCP/IP**配置的设置值。
- n 这些信息一般用来检验人工配置的**TCP/IP**设置是否正确。
- n 如果使用了**DHCP**，**IPConfig**可以让我们了解自己的计算机是否成功的租用到一个**IP**地址，如果租用到则可以了解它目前分配到的是什么地址。了解计算机当前的**IP**地址、子网掩码、缺省网关、**DNS**服务器实际上是进行测试和故障分析的必要项目。

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

C:\>ipconfig -?

USAGE:
    ipconfig [/? : /all : /renew [adapter] : /release [adapter] :
        /flushdns : /displaydns : /registerdns :
        /showclassid adapter :
        /setclassid adapter [classid] ]

where
    adapter          Connection name
                     (wildcard characters * and ? allowed, see examples)

Options:
    /?              Display this help message
    /all            Display full configuration information.
    /release        Release the IP address for the specified adapter.
    /renew          Renew the IP address for the specified adapter.
    /flushdns       Purges the DNS Resolver cache.
    /registerdns    Refreshes all DHCP leases and re-registers DNS names
    /displaydns     Display the contents of the DNS Resolver Cache.
    /showclassid    Displays all the dhcp class IDs allowed for adapter.
    /setclassid     Modifies the dhcp class id.
```

3、ipconfig (3)

n **ipconfig**命令的语法为:

n **ipconfig** [/? | /all | /release [adapter] | /renew [adapter] | /flushdns | /registerdns | /showclassid adapter [classidtoreset]]

n 其中主要参数的功能如下:

n **/?** : 显示参数项及其功能。

n **/all**: 显示TCP/IP协议的全部配置信息, 包括主机名 (Host Name)、节点类型 (Node Type)、是否启动IP路由 (IP Routing Enabled) 和是否启动WINS代理 (WINS Proxy Enabled) 等。

n **/release**: 释放指定给网卡的IP地址。

n **/renew**: 更新指定给网卡的IP地址。

3、ipconfig (4)

- n **/flushdns**: 清除DNS解析缓冲。
- n **/registerdns**: 刷新所有的DHCP租用并重新注册DNS名。
- n **/displaydns**: 显示DNS解析器高速缓存的内容。
- n **/showclassid**: 显示所有的DHCP类ID。
- n **/setclassid**: 设置DHCP类ID。


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

C:\>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.100
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

C:\>
```

C:\WINDOWS\system32\cmd.exe

C:\>ipconfig /all

Windows IP Configuration

Host Name : 222-fb592a31e1d
Primary Dns Suffix :
Node Type : Unknown
IP Routing Enabled. : No
WINS Proxy Enabled. : No

Ethernet adapter 本地连接:

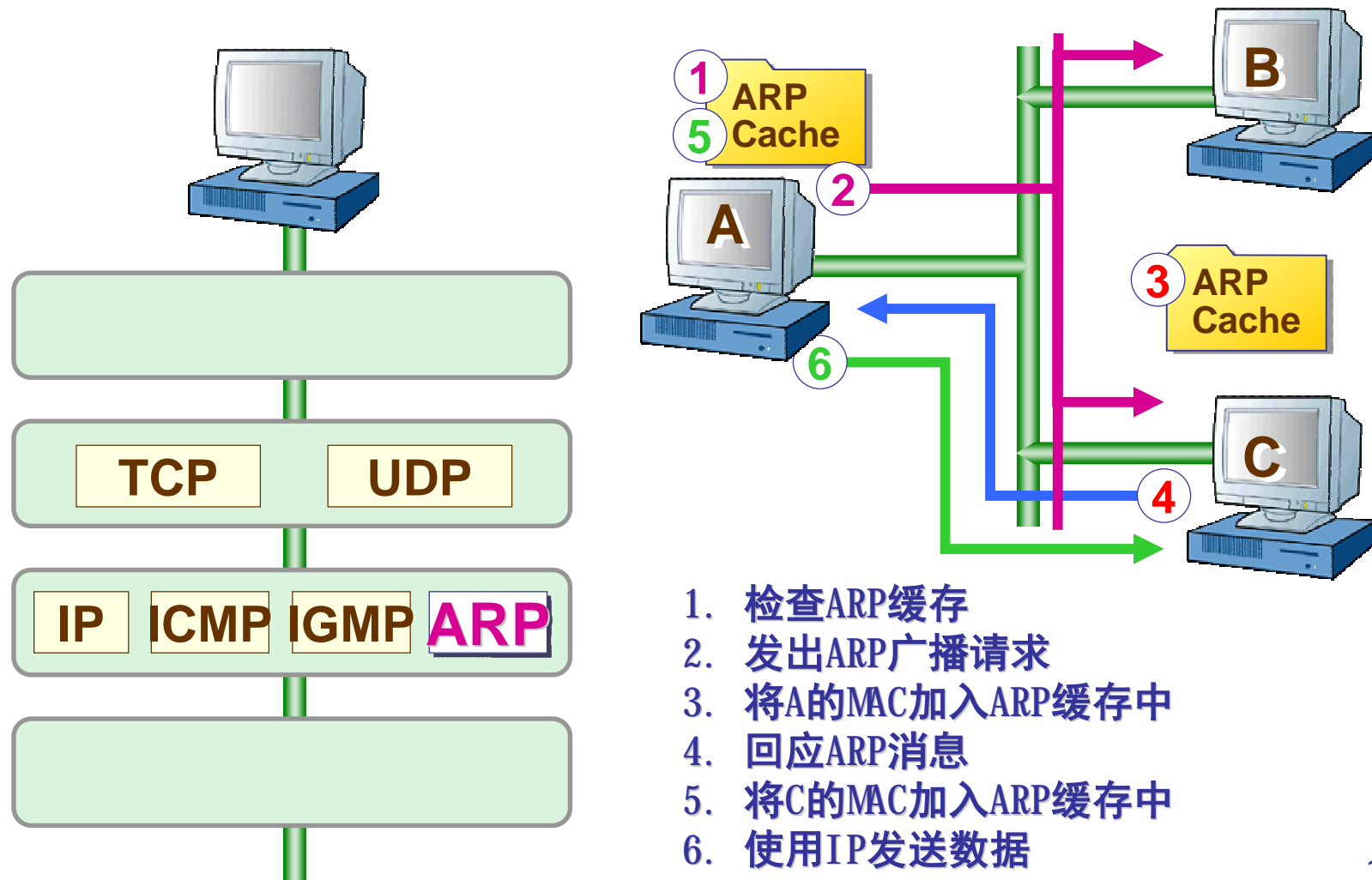
Connection-specific DNS Suffix . :
Description : AMD PCNET Family PCI Ethernet Adapter
Physical Address. : 00-0C-29-3C-64-9C
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes
IP Address. : 192.168.1.20
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1
DHCP Server : 192.168.1.1
DNS Servers : 202.96.104.15
 202.96.104.25
Lease Obtained. : 2009年2月7日 17:48:51
Lease Expires : 2009年2月9日 17:48:51

C:\>

4、ARP（1）

- n **ARP**(地址解析协议, **Address Resolution Protocol**)的作用就是根据目标主机的**IP**地址来解析其**MAC**地址, 并将解析过的**IP**地址和**MAC**地址的对应关系保存在**ARP**缓存中。

ARP协议的解析过程



4、ARP（2）

- n **arp**是Windows2003中用于查看和修改本地计算机的**ARP**（地址解析协议）所使用的地址转换表的一个诊断程序，其语法格式为：

- n **ARP -s int_addr eth_addr[if_addr]**

- n **ARP -d int_addr [if_addr]**

- n **ARP -a [inet_addr] [-N if_addr]**

- n 其中主要参数的功能如下：

- n **-a**：通过查询当前的协议数据来显示当前**ARP**项。如果已指定**int_addr**参数项，则只显示指定主机的**IP**地址和物理地址。如果有一个以上的网络接口使用**ARP**，将显示名**ARP**表项的内容。

- n **inet_addr**：指定一个Internet地址。

- n **-N if_addr**：被**if_addr**指定的网络接口显示**ARP**的输入项。

4、ARP (3)

- n **-d:** 删除被**inet_addr**指定的主机。或者删除全部。
- n **-s:** 添加**ARP**缓冲中的项，以便将**Internet**地址：**inet_addr**与物理地址**ether_addr**进行关联。该物理地址为由连字符分隔的个十六进制字节。输入项是静态的，即超时终止后不从缓冲中自动删除，重新引导计算机后该输入项丢失。
 - n **ether_addr:** 指定物理地址。
 - n **If_addr:** 指定现有接口的**IP**地址，该接口地址转换表需要修改。现有接口不存在时，则使用第1个可用接口的**IP**地址。

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

C:\>arp -s 192.168.1.1 cc-cc-cc-cc-cc-cc

C:\>arp -a

Interface: 192.168.1.100 --- 0x10003
    Internet Address      Physical Address      Type
    192.168.1.1           cc-cc-cc-cc-cc-cc     static
    192.168.1.11          00-16-36-29-8f-75     dynamic

C:\>arp -d

C:\>arp -a

Interface: 192.168.1.100 --- 0x10003
    Internet Address      Physical Address      Type
    192.168.1.11          00-16-36-29-8f-75     dynamic

C:\>
```

5、netstat (1)

- n **netstat**诊断程序用于显示协议的统计信息及当前**TCP/IP**网络的连接状态。**Netstat**命令的语法格式为:
 - n **netstat [-a] [-b] [-e] [-n] [-s] [-p proto] [-r][interval]**
- n 其中主要参数的功能如下:
 - n **-a**: 显示所有的连接 (**ESTABLISHED**) 及监听端口 (**LISTENING**) 。
 - n **-b**: 显示包含于创建每个连接或监听端口的可执行组件。
 - n **-e**: 显示**Ethernet** (以太网) 的统计信息, 可与**-s**参数结合使用。
 - n **-n**: 用数字形式表示地址和端口号。

5、netstat (2)

- n **-p proto**: 显示**proto**指定协议的连接信息。**Proto**可以是**TCP**或**UCP**子协议。如果和**-s**参数共同使用可以显示每个协议（可以是**TCP**协议、**UDP**协议或**IP**协议）的统计信息。
- n **-r**: 显示关于路由表的信息，类似于后面所讲使用**route print**命令时看到的 信息。除了显示有效路由外，还显示当前有效的连接。
- n **-s**: 显示每个协议的统计信息。默认时显示**TCP**、**UDP**和**IP**子协议的统计信息；如果与**-p**参数结合使用，可以指定默认子网。

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

C:\>netstat -?

显示协议统计信息和当前 TCP/IP 网络连接。

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

-a          显示所有连接和监听端口。
-b          显示包含于创建每个连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下包含于创建连接或监听端口的组件序列被显示。这种情况下，可执行组件名在底部的 [ ] 中，顶部是其调用的组件，等等，直到 TCP/IP 部分。注意此选项可能需要很长时间，如果没有足够权限可能失败。
-e          显示以太网统计信息。此选项可以与 -s 选项组合使用。
-n          以数字形式显示地址和端口号。
-o          显示与每个连接相关的所属进程 ID。
-p proto    显示 proto 指定的协议的连接；proto 可以是下列协议之一：TCP、UDP、TCPv6 或 UDPv6。
            如果与 -s 选项一起使用以显示按协议统计信息，proto 可以是下列协议之一：
            IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6。
-r          显示路由表。
-s          显示按协议统计信息。默认地，显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息；-p 选项用于指定默认情况的子集。
-t          显示当前连接卸载状态。
-v          与 -b 选项一起使用时将显示包含于为所有可执行组件创建连接或监听端口的组件。
interval    重新显示选定统计信息，每次显示之间暂停时间间隔<以秒计>。按 CTRL+C 停止重新显示统计信息。如果省略，netstat 显示当前配置信息<只显示一次>

C:\>
```

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

C:\>netstat

Active Connections

    Proto Local Address          Foreign Address         State
    TCP    222-fb592a31e1d:2121   USER-2E5F1F7500:activesync ESTABLISHED
    TCP    222-fb592a31e1d:ms-wbt-server USER-2E5F1F7500:1032 ESTABLISHED

C:\>netstat -an

Active Connections

    Proto Local Address          Foreign Address         State
    TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
    TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
    TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
    TCP    0.0.0.0:2121           0.0.0.0:0              LISTENING
    TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
    TCP    192.168.1.100:139      0.0.0.0:0              LISTENING
    TCP    192.168.1.100:2121     192.168.1.11:1034      ESTABLISHED
    TCP    192.168.1.100:3389     192.168.1.11:1032      ESTABLISHED
    UDP    0.0.0.0:445            *:*
    UDP    0.0.0.0:500            *:*
    UDP    0.0.0.0:1049           *:*
    UDP    0.0.0.0:4500           *:*
    UDP    127.0.0.1:123          *:*
    UDP    192.168.1.100:123      *:*
    UDP    192.168.1.100:137      *:*
    UDP    192.168.1.100:138      *:*
```

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

C:\>netstat -anb

Active Connections

  Proto  Local Address          Foreign Address        State               PID
  TCP    0.0.0.0:135             0.0.0.0:0              LISTENING           656
  RpcSs
  [svchost.exe]

  TCP    0.0.0.0:445             0.0.0.0:0              LISTENING           4
  [System]

  TCP    0.0.0.0:1025            0.0.0.0:0              LISTENING           384
  [lsass.exe]

  TCP    0.0.0.0:2121            0.0.0.0:0              LISTENING           1772
  [ftpserv.exe]

  TCP    0.0.0.0:3389            0.0.0.0:0              LISTENING           1308
  TermService
  [svchost.exe]

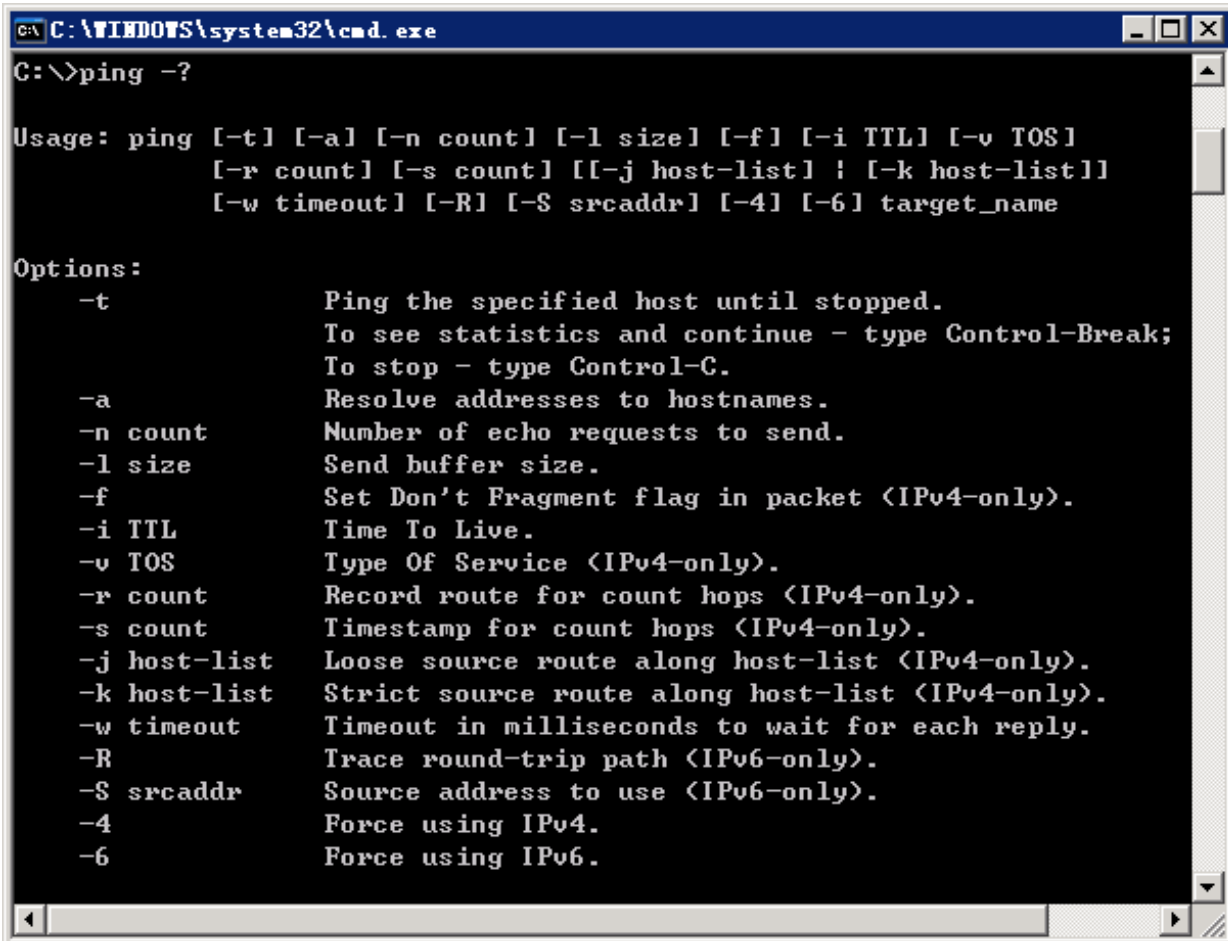
  TCP    192.168.1.100:139       0.0.0.0:0              LISTENING           4
  [System]

  TCP    192.168.1.100:2121      192.168.1.11:1034      ESTABLISHED         1772
  [ftpserv.exe]

  TCP    192.168.1.100:3389      192.168.1.11:1032      ESTABLISHED         1308
  TermService
  [svchost.exe]
```

6、ping (1)

- n ping是使用TCP/IP协议的网络中最常使用和最为重要的一个诊断程序，它可以查看TCP/IP协议的配置状态，以及远程计算机之间的连接情况。



```
C:\WINDOWS\system32\cmd.exe
C:\>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] [-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).
    -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          Trace round-trip path (IPv6-only).
    -S srcaddr  Source address to use (IPv6-only).
    -4          Force using IPv4.
    -6          Force using IPv6.
```

6、ping (2)

n ping命令的语法格式为:

```
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
```

n 其中主参数的功能如下:

- n **-t**: 不停止的ping指定的主机。使用**Ctrl+c**组合键结束操作。
- n **-a**: 解析主机的地址。
- n **-n count**: 发送数据包次数 (n默认为4)

- n **-l size:** 发送缓冲区的大小。
- n **-f:** 在数据包中设置不分段标志，从而该数据包在以过路由网关进不再分段。
- n **-v TTL:** 设置生存时间字段为TTL指定的值。
- n **-v TOS:** 设置服务字段类型为TOS指定的值。
- n **-s count:** 由 指定的时间戳。
- n **-j host-list:** 通过由 指定各主机传递数据包，连接的主机可以由中间的网关隔开。
- n **-k nost-list:** 通过 指定和各主机传数据包，连接的主机不能由中间的网关隔开。
- n **-w timeout:** 指定等待每次响应的超时时间间隔，以ms单位。

C:\WINDOWS\system32\cmd.exe

C:\>ping www.google.cn

Pinging google.cn [203.208.35.100] with 32 bytes of data:

Reply from 203.208.35.100: bytes=32 time=61ms TTL=247

Reply from 203.208.35.100: bytes=32 time=61ms TTL=247

Reply from 203.208.35.100: bytes=32 time=61ms TTL=247

Reply from 203.208.35.100: bytes=32 time=61ms TTL=247

Ping statistics for 203.208.35.100:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 61ms, Maximum = 61ms, Average = 61ms

C:\>ping 222.222.222.222

Pinging 222.222.222.222 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 222.222.222.222:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>

6、ping (3)

n 利用ping诊断网络:

- n ping 127.0.0.1 ping localhost
- n ping 本机IP
- n ping 网关IP
- n ping 远程IP
- n ping www.xxx.com

使用ping命令排除简单网络故障

- n (1) **ping** 环回地址（127.0.0.1）
 - n 以验证本地计算机上是否正确地配置了 **TCP/IP**
 - n 执行失败，说明**TCP/IP**协议安装不正确
- n (2) **ping** 本地计算机的 **IP** 地址
 - n 验证其是否已正确地添加到网络中
 - n 执行失败，说明**IP**地址配置不正确，或没有连接到网络中
- n (3) **ping** 默认网关的 **IP** 地址
 - n 验证默认网关是否正常工作以及是否可以与本地网络上的本地主机进行通信
 - n 执行失败，需要验证默认网关 **IP** 地址是否正确以及网关（路由器）是否运行
- n (4) **ping** 远程主机的 **IP** 地址
 - n 验证到远程主机（不同子网上的主机） **IP** 地址的连通性
 - n 命令失败，需要验证远程主机的 **IP** 地址是否正确，远程主机是否运行，以及该计算机和远程主机之间的所有网关（路由器）是否运行。
- n (5) **ping** 远程主机的计算机名
 - n 如果 **ping IP** 地址已成功，但**ping** 命令失败，名称解析问题所致，需要验证 **DNS** 服务器的 **IP** 地址是否正确，**DNS** 服务器是否运行，以及该计算机和 **DNS** 服务器之间的网关（路由器）是否运行。

7、nbtstat

- n **nbtstat**诊断程序用于显示当前使用**NET（NetBIOS over TCP/IP）**连接**TCP/IP**协议的状态信息及统计信息等。**Nbtstat**命令的语法格式为（注意参数的大小写）：
- n **nbtstat [[-a RemoteName][-A IP address][-c][-n][-r][-R][-RR][-s][-S][interval]]**
- n 其中主要参数的功能如下：
- n **-a RemoteName**：用计算机名显示远程计算机名表。
- n **-A IP address**：用计算机IP地址显示远程计算机列表。
- n **-c**：显示过程计算机名的**NBT（NetBIOS over TCP/IP）**缓存内容和IP地址。
- n **-n**：显示本地计算机的**NetBIOS**名。

7、nbtstat

- n **-r:** 列出通过广播或**WINS**解析的名字。
- n **-R:** 清除和重新装载远程缓冲名表。
- n **-S:** 显示带有目的的**IP**地址的会话表。
- n **-s:** 显示将目的**IP**地址转化为计算机名后的会话表。
- n **--RR:** 将名字释放包发送给**WINS**服务器，然后进行刷新操作。
- n **RemoteName:** 远程主机名。
- n **IP address:** **IP**地址的加点十进制表示。
- n **Interval:** 重新显示在两面次之间的所选统计信息和暂停间隔秒数。
按**Ctrl+C**组合键终止重新显示统计信息。

8、route (1)

- n **route**诊断程序用于对**IP**路由表进行增删、打印等操作。其中命令格式为:
- n **route [-f][-p][command[destination][MASK netmask][geteway][METRIC metric][IF interface]**
- n 其中主要参数的功能如下:
 - n **-f**: 清除所有网关的路由表。如果该参数与其他的命令共同使用, 则路由表在命令运行之前消除。
 - n **-p**: 当该参数与**ADD**命令一起使用时, 计算机重新启动后路由将保持不变。默认情况下, 计算机重新启动后原来的路由信息不会保存。

8、route (2)

- n **Command:** 指定以太4个命令中的一个:
 - n **PRINT:** 打印一个路由。
 - n **ADD:** 添加一个路由。
 - n **DELETE:** 删除一个路由。
 - n **CHANGE:** 更改现有的路由。
- n **Destination:** 指定发送命令的主机。
- n **MASK:** 指定一个参数为netmask卷。
- n **Netmask:** 指定子网掩码与该路由项建立关联。如果未指定，系统默认的子网掩码为**255. 255. 255. 255**,
- n **Gateway:** 指定网关。
- n **Interface:** 指定路由的接口号。
- n **METRIC:** 指定要目的主机的路由量度。

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

Examples:

> route PRINT
> route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
           destination^      ^mask      ^gateway      metric^      ^
                                   Interface^

    If IF is not given, it tries to find the best interface for a given
    gateway.
> route PRINT
> route PRINT 157*      .... Only prints those matching 157*
> route CHANGE 157.0.0.0 MASK 255.0.0.0 157.55.80.5 METRIC 2 IF 2

    CHANGE is used to modify gateway and/or metric only.
> route PRINT
> route DELETE 157.0.0.0
> route PRINT
```

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

C:\>route print

IPv4 Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x10003 ...00 0c 29 3c 64 9c ..... AMD PCNET Family PCI Ethernet Adapter
=====

Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1      192.168.1.100    30
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1        1
192.168.1.0                255.255.255.0    192.168.1.100    192.168.1.100    30
192.168.1.100              255.255.255.255  127.0.0.1        127.0.0.1        30
192.168.1.255              255.255.255.255  192.168.1.100    192.168.1.100    30
224.0.0.0                  240.0.0.0        192.168.1.100    192.168.1.100    30
255.255.255.255            255.255.255.255  192.168.1.100    192.168.1.100    1
Default Gateway:          192.168.1.1
=====

Persistent Routes:
None

C:\>
```


C:\WINDOWS\system32\cmd.exe

C:\> route ADD 10.10.10.0 MASK 255.255.255.0 192.168.1.2

C:\>route change 10.10.10.0 MASK 255.255.255.0 192.168.1.5

C:\>route print

IPv4 Route Table

Interface List

0x1 MS TCP Loopback interface

0x10003 ...00 0c 29 3c 64 9c AMD PCNET Family PCI Ethernet Adapter

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.100	30
10.10.10.0	255.255.255.0	192.168.1.5	192.168.1.100	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.100	192.168.1.100	30
192.168.1.100	255.255.255.255	127.0.0.1	127.0.0.1	30
192.168.1.255	255.255.255.255	192.168.1.100	192.168.1.100	30
224.0.0.0	240.0.0.0	192.168.1.100	192.168.1.100	30
255.255.255.255	255.255.255.255	192.168.1.100	192.168.1.100	1

Default Gateway: 192.168.1.1

Persistent Routes:

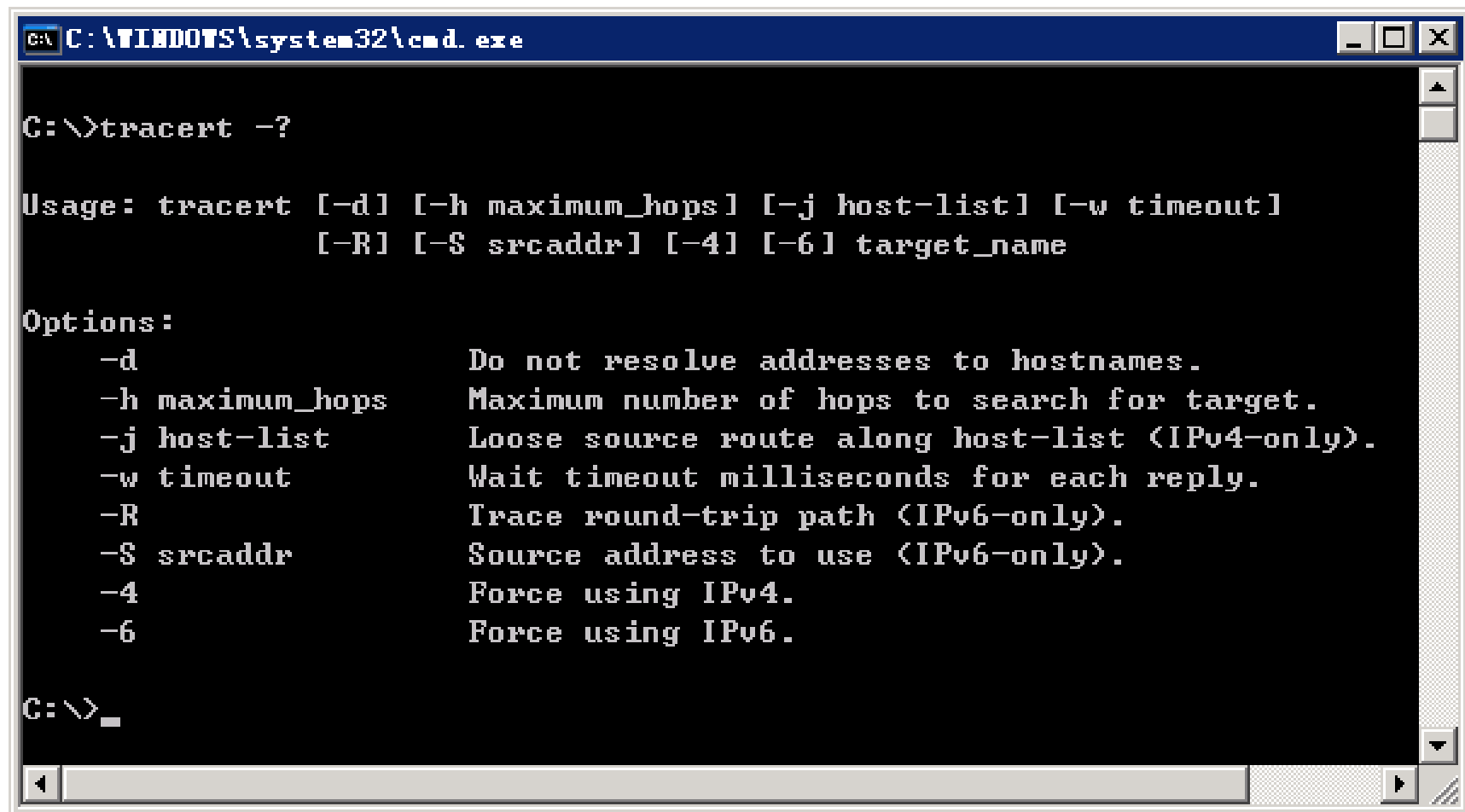
None

9、tracert（1）

- n **tracert**诊断程序可以用于检查通过向远程系统的路由，一般用来检测故障的位置。
 - n **tracert** 命令显示用于将数据包从计算机传递到目标位置的一组 **IP** 路由器，以及每个跃点所需的时间。
 - n 如果数据包不能传递到目标，**tracert** 命令将显示成功转发数据包的最后一个路由器。
 - n 当数据报从我们的计算机经过多个网关传送到目的地时，**Tracert** 命令可以用来跟踪数据报使用的路由（路径）。
 - n 对于解决大型网络问题非常有用，可以确定数据包在网络上的停止位置、路由环路等问题

9、tracert (2)

- n 在Windows 提示符下运行tracert -?命令，可以显示所有的参数及其说明。



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

C:\>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 round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                Force using IPv4.
    -6                Force using IPv6.

C:\>
```

9、tracert (3)

- n 其中主要的参数及其功能如下：
- n **-d**: 不解析主机名的地址。
- n **-h maximum_hops**: 设定寻找目标过程的最大中转数。

```
C:\>tracert 10.23.1.101

Tracing route to dns.nbut.cn [10.23.1.101]
over a maximum of 30 hops:

  1    <1 ms    1 ms    1 ms    10.20.18.1
  2    <1 ms    1 ms    1 ms    192.168.31.1
  3     1 ms    1 ms    1 ms    192.168.13.1
  4    <1 ms    1 ms    1 ms    192.168.14.2
  5     1 ms    1 ms    1 ms    dns.nbut.cn [10.23.1.101]

Trace complete.
```

10、telnet

- n 远程登录命令
- n 现在一般使用**SSH**
- n **SSH和VPN区别**

11、ftp命令

n 访问ftp服务器的命令

ftp> help

Commands may be abbreviated. Commands are:

!	delete	literal	prompt	send
?	debug	ls	put	status
append	dir	mdelete	pwd	trace
ascii	disconnect	mdir	quit	type
bell	get	mget	quote	user
binary	glob	mkdir	recv	verbose
bye	hash	mls	remotehelp	
cd	help	mput	rename	
close	lcd	open	rmdir	

pathping

- n 使用**pathping**跟踪数据包的路径
 - n 一个路由跟踪工具
 - n 将 **ping** 和 **tracert** 命令的功能及这两个命令所不提供的其他信息结合起来
- n **pathping**命令的格式:
 - n **pathping** [<命令选项>] <目标主机的名称或 IP 地址>

表2-3 pathping 命令选项

选项	功能
-n	不将地址解析成主机名。
-h maximum_hops	搜索目标的最大跃点数。
-g host-list	沿着主机列表释放源路由。
-p period	在 ping 之间等待的毫秒数。
-q num_queries	每个跃点的查询数。
-w timeout	每次等待回复的毫秒数。
-i address	使用指定的源地址。
-4	强制 pathping 使用 IPv4。
-6	强制 pathping 使用 IPv6。


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

C:\>pathping -n ns.ahhfptt.net.cn

通过最多 30 个跃点跟踪
到 ns.ahhfptt.net.cn [202.102.192.68] 的路由:
 0 172.16.18.6
 1 172.16.18.1
 2 172.16.99.2
 3 218.22.0.17
 4 61.190.246.169
 5 61.190.246.10
 6 202.102.192.68

正在计算统计信息, 已耗时 150 秒...
指向此处的源 此节点/链接
跃点 RTT 已丢失/已发送 = Pct 已丢失/已发送 = Pct 地址
 0 0/ 100 = 0% 0/ 100 = 0% 172.16.18.6
 1 0ms 0/ 100 = 0% 0/ 100 = 0% 172.16.18.1
 2 5ms 0/ 100 = 0% 0/ 100 = 0% 172.16.99.2
 3 5ms 1/ 100 = 1% 0/ 100 = 0% 218.22.0.17
 4 4ms 1/ 100 = 1% 0/ 100 = 0% 61.190.246.169
 5 5ms 1/ 100 = 1% 0/ 100 = 0% 61.190.246.10
 6 7ms 1/ 100 = 1% 0/ 100 = 0% 202.102.192.68

跟踪完成。
```