常用网络命令

V 1.3

客服部 -2013

深圳磊科实业有限公司

版本控制

版本号	修改说明	修改人	时间
V1.1	新建文档结构以及基本内容	Wy	2013.3.4
V1.2	增加第四章 DNS 内容	Wy	2013.3.6
V1.3	增加第五章其他 cmd	Wy	2013.3.8

目　录

第1章 Ping 详解

1.1 Ping 的原理

ping 不仅仅是 windows 下的命令，在 unix 和 linux 下也有这个命令，ping 只是一个通信协议,是 ip 协议的一部分,tcp/ip 协议的一部分,Ping 在 Windows 系下是自带的一个可执行命令。利用它可以检查网络是否能够连通，用好它可以很好地帮助我们分析判定网络故障。应用格式：Ping IP 地址。该命令还可以加许多参数使用。

使用 Ping 检查连通性有六个步骤：

1. 使用 ipconfig /all 观察本地网络设置是否正确；

2. Ping 127.0.0.1，127.0.0.1 回送地址 Ping 回送地址是为了检查本地的 TCP/IP 协议有没有设置好；

3. Ping 本机 IP 地址，这样是为了检查本机的 IP 地址是否设置有误；

4. Ping 本网网关或本网 IP 地址,这样的是为了检查硬件设备是否有问题，也可以检查本机与本地网络连接是否正常；（在非局域网中这一步骤可以忽略）

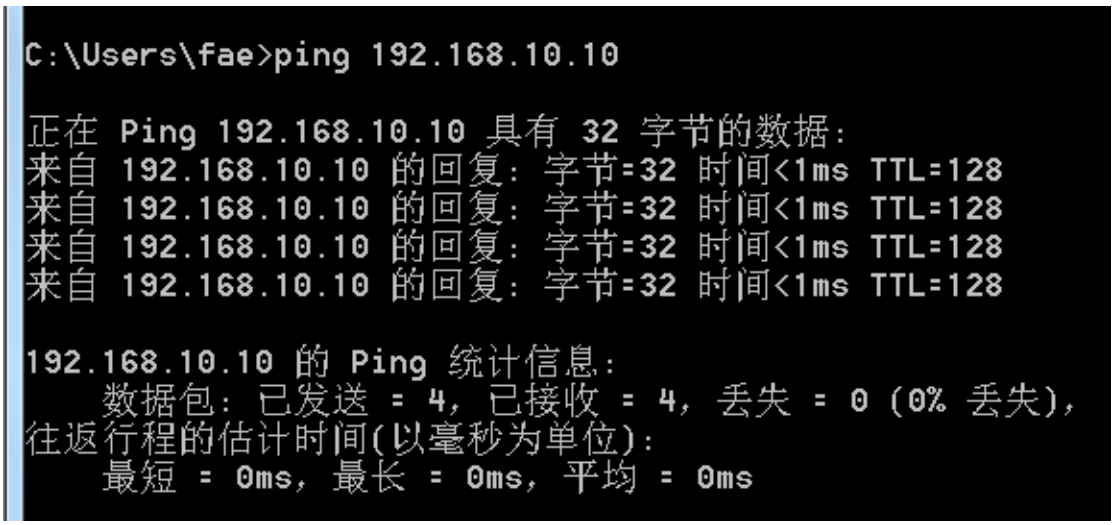
5. Ping 本地 DNS 地址，这样做是为了检查 DNS 是否能够将 IP。

6. Ping 远程 IP 地址，这主要是检查本网或本机与外部的连接是否正常。

1.2 Ping 的使用

1.2.1 Ping 本机 IP

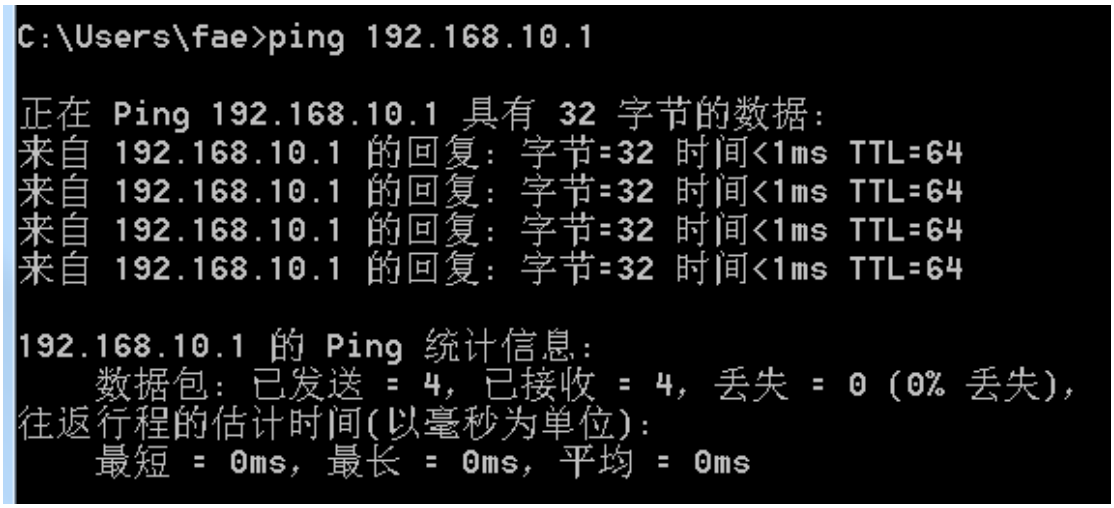
例如本机 IP 为 192.168.10.10，则执行命令 Ping192.168.10.10。如果网卡安装配置没有问题，则应有类似下列显示：



若此命令显示内容为：Request timed out，则表明网卡安装或配置有问题。将网线断开再次执行此命令，如果显示正常，则说明本机使用的 IP 地址可能与另一台正在使用的机器 IP 地址重复了。如 果仍然不正常，则表明本机网卡安装或配置有问题，需继续检查相关网络配置。

1.2.2 Ping 网关 IP

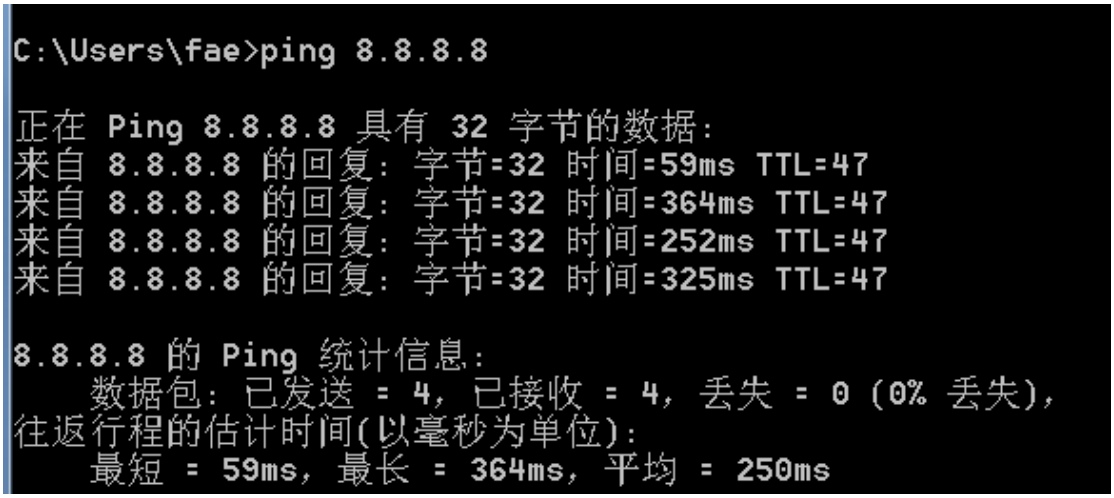
假定网关 IP 为：192.168.10.1，则执行命令 Ping192.168.10.1。在 MS-DOS 方式下执行此命令，如果显示类似以下信息：



则表明局域网中的网关路由器正在正常运行。反之，则说明网关有问题。

1.2.3 Ping 远程 IP

这一命令可以检测本机能否正常访问 Internet。比如本地电信运营商的 IP 地址为：8.8.8.8。在 MS-DOS 方式下执行命令：Ping 8.8.8.8，如果屏幕显示：



则表明运行正常，能够正常接入互联网。反之，则表明主机文件（windows/host）存在问题。

1.3 Ping 命令参数

-t ： 一直 Ping 指定的计算机，直到从键盘按下 Ctrl+C 中断。

-l ：发送指定数据量的 ECHO 数据包。默认为 32 字节;最大值是 65500byte。

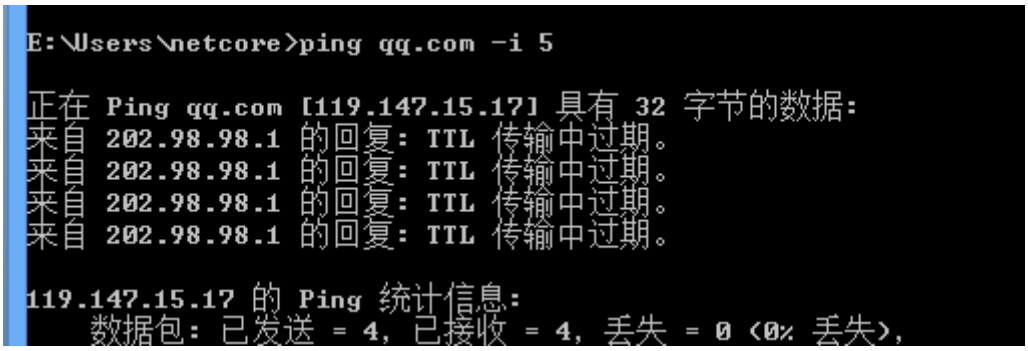
```
^C
E:\Users\netcore>ping qq.com -l 1460

正在 Ping qq.com [119.147.15.13] 具有 1460 字节的数据:
来自 119.147.15.13 的回复: 字节=1460 时间=357ms TTL=55
来自 119.147.15.13 的回复: 字节=1460 时间=366ms TTL=55
来自 119.147.15.13 的回复: 字节=1460 时间=325ms TTL=55
来自 119.147.15.13 的回复: 字节=1460 时间=430ms TTL=55

119.147.15.13 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 = 325ms, 最长 = 430ms, 平均 = 369ms
```

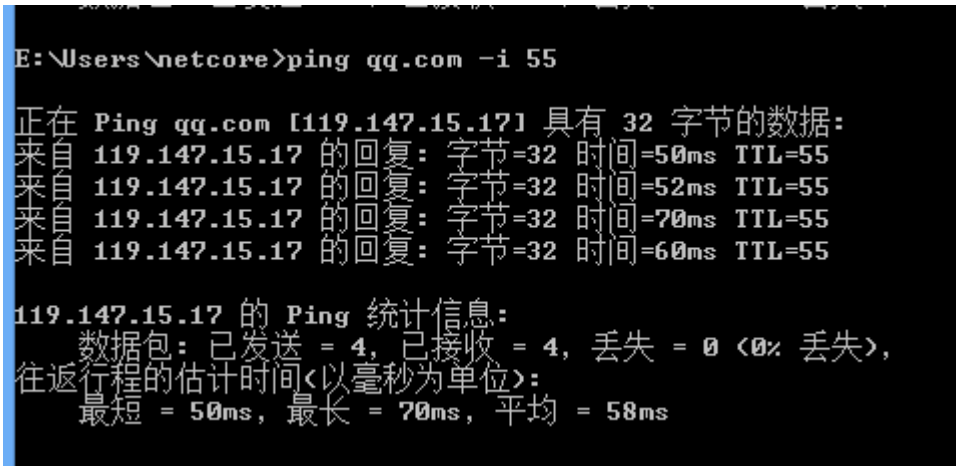
-f ：在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段。通常你所发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。

```
E:\Users\netcore>ping qq.com -f

正在 Ping qq.com [119.147.15.17] 具有 32 字节的数据:
来自 119.147.15.17 的回复: 字节=32 时间=46ms TTL=55
来自 119.147.15.17 的回复: 字节=32 时间=71ms TTL=55
来自 119.147.15.17 的回复: 字节=32 时间=62ms TTL=55
来自 119.147.15.17 的回复: 字节=32 时间=59ms TTL=55

119.147.15.17 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 = 46ms, 最长 = 71ms, 平均 = 59ms
```

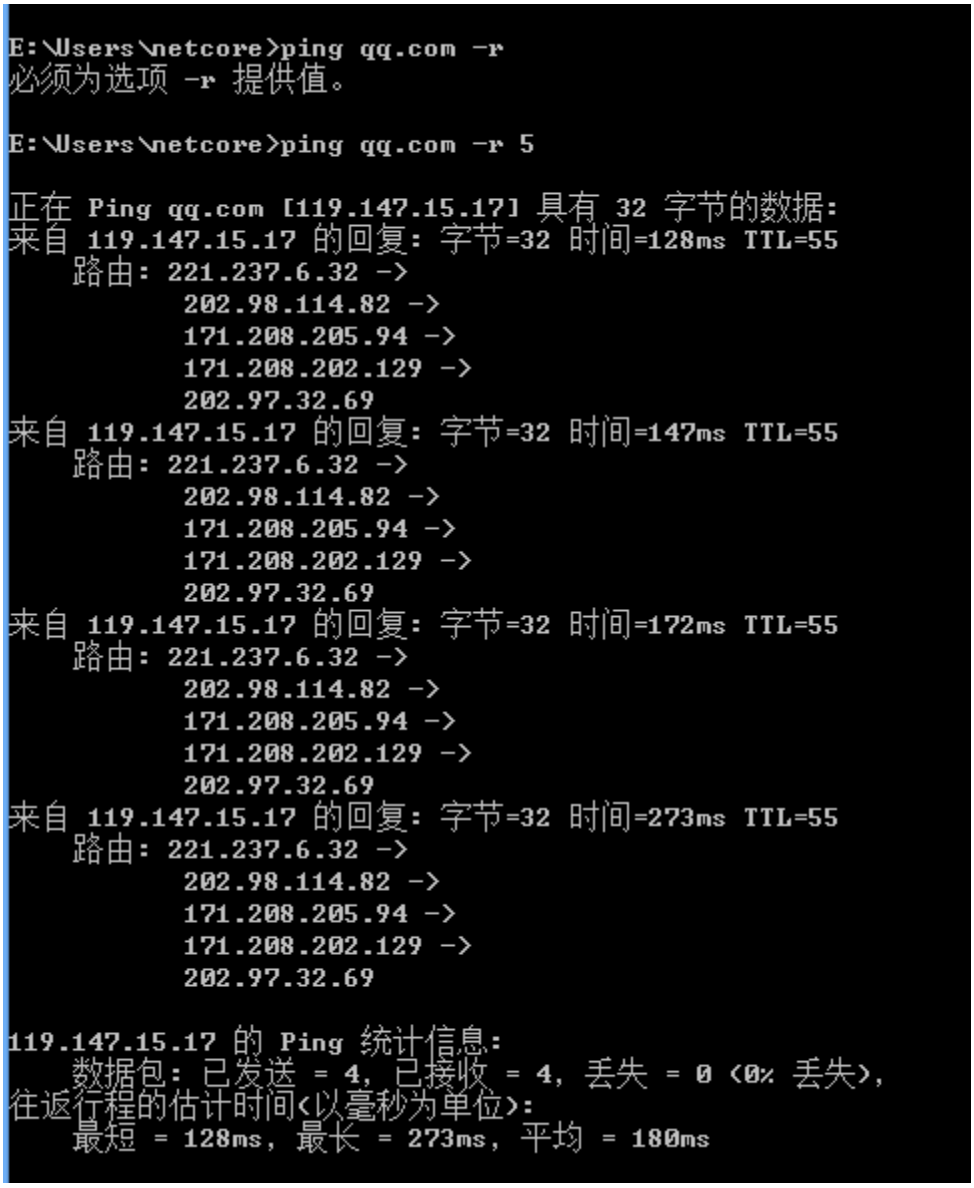
```
E:\Users\netcore>ping qq.com -f -l 14664

正在 Ping qq.com [119.147.15.17] 具有 14664 字节的数据:
需要拆分数据包但是设置 DF。
需要拆分数据包但是设置 DF。
需要拆分数据包但是设置 DF。
需要拆分数据包但是设置 DF。

119.147.15.17 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

-i ：将“生存时间”字段设置为 TTL 指定的值。指定 TTL 值在对方的系统里停留的时间。同时检查网络运转情况的。





-r ：在“记录路由”字段中记录传出和返回数据包的路由。通常情况下，发送的数据包是通过一系列路由才到达目标地址的，通过此参数可以设定，想探测经过路由的个数。限定能跟踪到 9 个路由。



Tracert 路由追踪

1.4 Ping 的结果

1.Request timed out

这是大家经常碰到的提示信息，很多文章中说这是对方机器置了过滤 ICMP 数据包，从上面工作过程来看，这是不完全正确的，至少有下几种情况。

（1） 对方已关机，或者网络上根本没有这个地址：比如在上图中主机 A 中 PING 192.168.0.7 ，或者主机 B 关机了，在主机 A 中 PING 192.168.0.5 都会得到超时的信息。

（2）对方与自己不在同一网段内，通过路由也无法找到对方，但有时对方确实是存在的，当然不存在也是返回超时的信息。

（3）对方确实存在，但设置了 ICMP 数据包过滤（比如防火墙设置）。

怎样知道对方是存在，还是不存在呢，可以用带参数 -a 的 Ping 命令探测对方，如果能得到对方的 NETBIOS 名称，则说明对方是存在的，是有防火墙设置，如果得不到，多半是对方不存在或关机，或不在同一网段内。

（4）错误设置 IP 地址

正常情况下，一台主机应该有一个网卡，一个 IP 地址，或多个网卡，多个 IP 地址（这些地址一定要处于不同的 IP 子网）。但如果一台电脑的“拨号网络适配器”（相当于一块软网卡）的 TCP/IP 设置中，设置了一个与网卡 IP 地址处于同一子网的 IP 地址，这样，在 IP 层协议看来，这台主机就有两个不同的接口

处于同一网段内。当从这台主机 Ping 其他的机器时，会存在这样的问题：

A.主机不知道将数据包发到哪个网络接口，因为有两个网络接口都连接在同一网段。

B.主机不知道用哪个地址作为数据包的源地址。因此，从这台主机去 Ping 其他机器，IP 层协议会无法处理，超时后，Ping 就会给出一个“超时无应答”的错误信息提示。但从其他主机 Ping 这台主机时，请求包从特定的网卡来，ICMP 只须简单地将目的、源地址互换，并更改一些标志即可，ICMP 应答包能顺利发出，其他主机也就能成功 Ping 通这台机器了。

2.Destination host Unreachable

（1） 对方与自己不在同一网段内，而自己又未设置默认的路由，比如上例中 A 机中不设定默认的路由，运行 Ping 192.168.0.1.4 就会出现“Destination host Unreachable”。

（2）网线出了故障

这里要说明一下“destination host unreachable”和 “time out”的区别，如果所经过的路由器的路由表中具有到达目标的路由，而目标因为其他原因不可到达，这时候会出现“time out”，如果路由表中连到达目标的路由都没有，那就会出现“destination host unreachable”。

3.Bad IP address

这个信息表示您可能没有连接到 DNS 服务器，所以无法解析这个 IP 地址，也可能是 IP 地址不存在。

4.Source quench received

这个信息比较特殊，它出现的机率很少。它表示对方或中途的服务器繁忙无法回应。

5.Unknown host——不知名主机

这种出错信息的意思是，该远程主机的名字不能被域名服务器（DNS）转换成 IP 地址。故障原因可能是域名服务器有故障，或者其名字不正确，或者网络管理员的系统与远程主机之间的通信线路有故障。

6.No answer——无响应

这种故障说明本地系统有一条通向中心主机的路由，但却接收不到它发给该

中心主机的任何信息。故障原因可能是下列之一：中心主机没有工作；本地或中心主机网络配置不正确；本地或中心的路由器没有工作；通信线路有故障；中心主机存在路由选择问题。

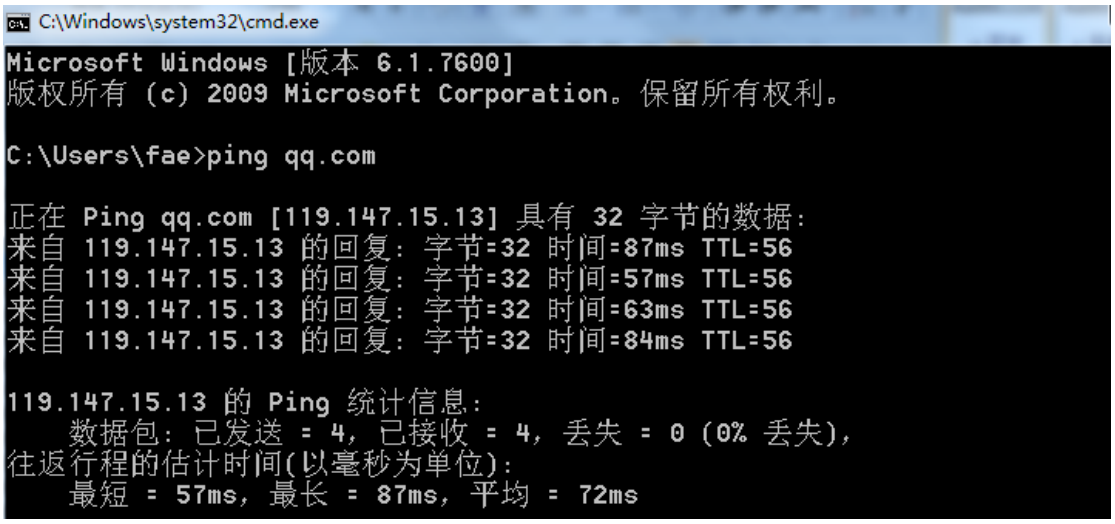
7.Ping 127.0.0.1：127.0.0.1 是本地循环地址

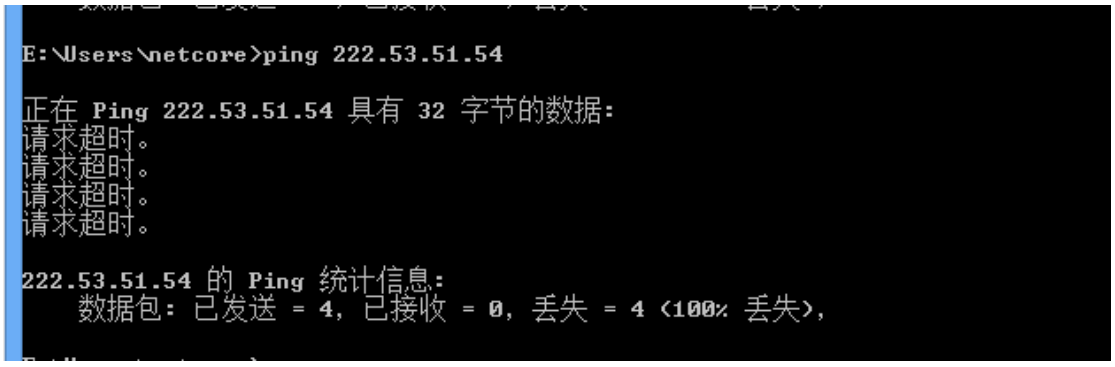
如果本地址无法 Ping 通，则表明本地机 TCP/IP 协议不能正常工作。

8.no rout to host：网卡工作不正常。

9.transmit failed，error code：10043 网卡驱动不正常。

10.unknown host name：DNS 配置不正确。





第2章 Mtu 详解

2.1 Mtu 的定义

通信术语 最大传输单元（Maximum Transmission Unit，MTU）是指一种通

信协议的某一层上面所能通过的最大数据包大小（以字节为单位）

2.2 Mtu 的影响

在因特网协议中，一条因特网传输路径的“路径最大传输单元”被定义为从源地址到目的地址所经过“路径”上的所有 IP 跳的最大传输单元的最小值。或者从另外一个角度来看，就是无需进一步分片就能穿过这条“路径”的传输单元的最大值。

如果本地路由器的 mtu 值高于上端路由的 mtu，本地电脑会以最大传输值传输数据，当数据到达上端路由时会因为高于上端路由的 MTU，从而导致数据无法通过。现象为部分网站或游戏运行不了，视频或图片打不开等。

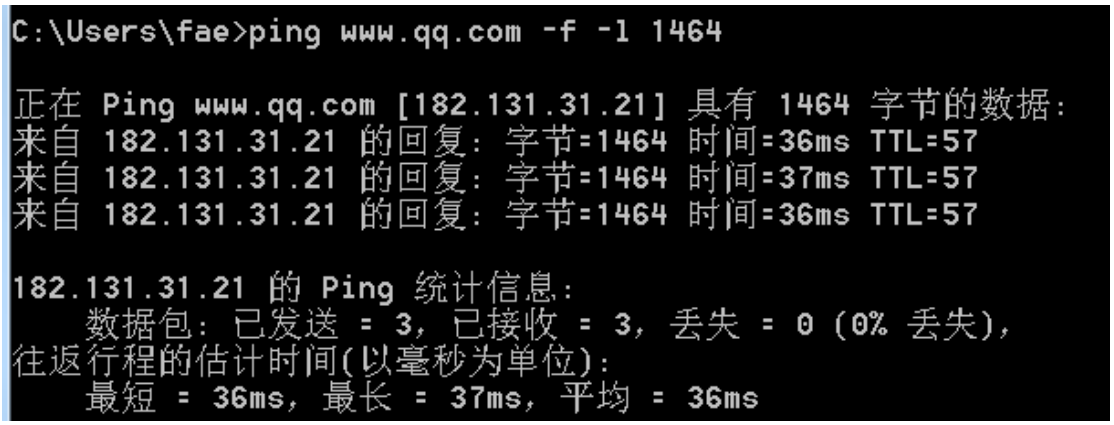
2.3 如何检测 Mtu

通过 ping 命令检测 mtu：ping 任意网站且不允许数据分片，通过改变数据包的大小检测数据包能否正常通过上端路由。

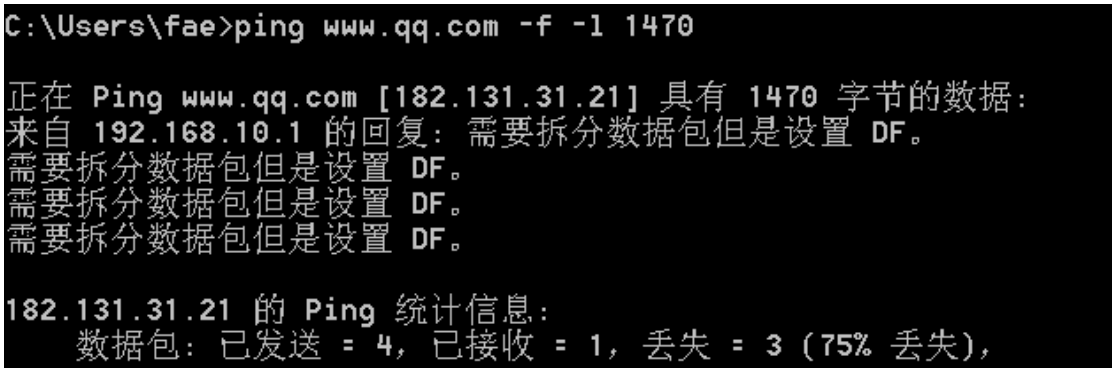
具体操作如下：

在不接路由器的情况下，单机上网使用如下命令：

Ping www.qq.com -f -l 1464



如果数据能通过，则增加数据大小，



如果不通则减小数据大小。直到找到数据包大小的临界值。

从上图可以看出，数据包大小的临界值是 1464。再加上 28 则可推算出 MTU。即 MTU=1464+28=1492。

第3章 Arp 详解

3.1 Arp 的定义

地址解析协议（Address Resolution Protocol，ARP）是在仅知道主机的 IP 地址时确定其物理地址的一种协议。

3.2 Arp 的原理

在 TCP/IP 协议中，A 给 B 发送 IP 包，在报头中需要填写 B 的 IP 为目标地址，但这个 IP 包在以太网上传输的时候，还需要进行一次以太包的封装，在这个以太包中，目标地址就是 B 的 MAC 地址。

计算机 A 是如何得知 B 的 MAC 地址的呢？解决问题的关键就在于 ARP 协议。

在 A 不知道 B 的 MAC 地址的情况下，A 就广播一个 ARP 请求包，请求包中填有 B 的 IP(192.168.1.2)，以太网中的所有计算机都会接收这个请求，而正常的情况下只有 B 会给出 ARP 应答包，包中就填充上了 B 的 MAC 地址，并回复给 A。

A 得到 ARP 应答后，将 B 的 MAC 地址放入本机缓存，便于下次使用。

本机 MAC 缓存是有生存期的，生存期结束后，将再次重复上面的过程。

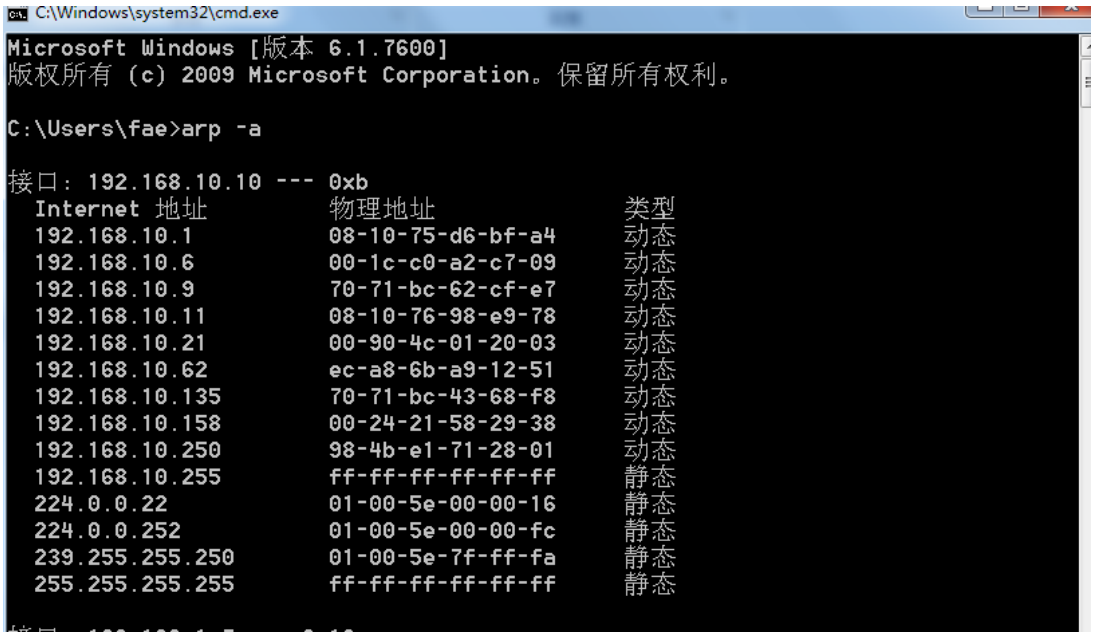
ARP 协议并不只在发送了 ARP 请求才接收 ARP 应答。当计算机接收到 ARP 应答数据包的时候，就会对本地的 ARP 缓存进行更新，将应答中的 IP 和 MAC 地址存储在 ARP 缓存中。因此，当局域网中的某台机器 B 向 A 发送一个自己伪造的 ARP 应答，而如果这个应答是 B 冒充 C 伪造来的，即 IP 地址为 C 的 IP，而 MAC 地址是伪造的，则当 A 接收到 B 伪造的 ARP 应答后，就会更新本地的 ARP 缓存，这样在 A 看来 C 的 IP 地址没有变，而它的 MAC 地址已经不是原来那个了。由于局域网的网络流通不是根据 IP 地址进行，而是按照 MAC 地址进行传输。所以，那个伪造出来的 MAC 地址在 A 上被改变成一个不存在的 MAC 地址，这样就会造成网络不通，导致 A 不能 Ping 通 C！这就是一个简单的 ARP 欺骗。

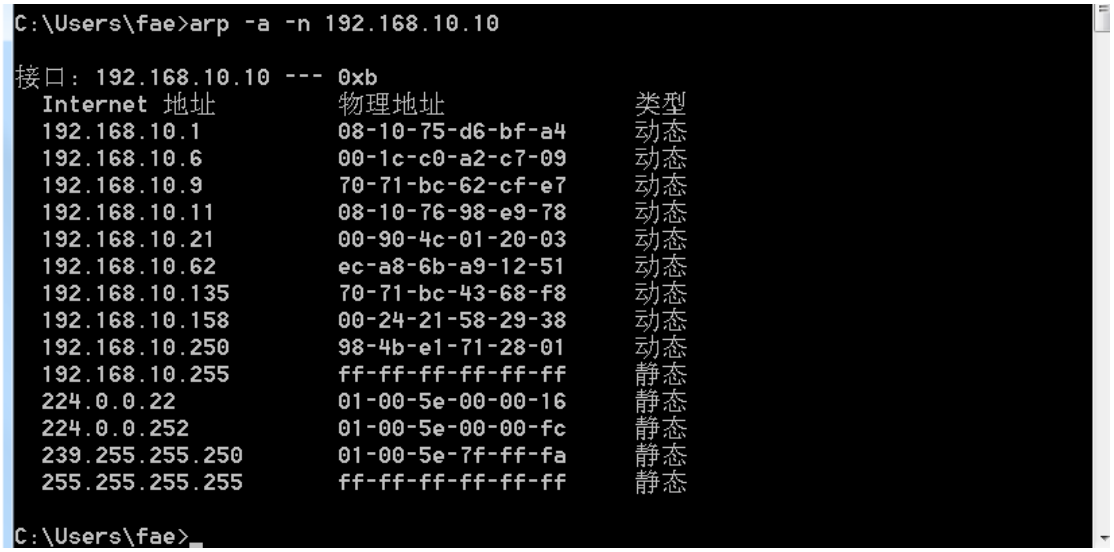
3.3 如何查看 arp

windows 中 arp 命令详解：

arp -a

显示所有接口的当前 ARP 缓存表。要显示特定 IP 地址的 ARP 缓存项，请使用带有 InetAddr 参数的 arp -a，此处的 InetAddr 代表 IP 地址。如果未指定 InetAddr，则使用第一个适用的接口。





arp -d

删除指定的 IP 地址项，此处的 InetAddr 代表 IP 地址。对于指定的接口，要删除表中的某项，请使用 IfaceAddr 参数，此处的 IfaceAddr 代表指派给该接口的 IP 地址。要删除所有项，请使用星号 (*) 通配符代替 InetAddr。

arp -s

向 ARP 缓存添加可将 IP 地址 InetAddr 解析成物理地址 EtherAddr 的静态项。要向指定接口的表添加静态 ARP 缓存项，请使用 IfaceAddr 参数，此

处的 IfaceAddr 代表指派给该接口的 IP 地址。

3.4 Arp 欺骗

ARP 欺骗分为二种，一种是对路由器 ARP 表的欺骗；另一种是对内网 PC 的网关欺骗。

第一种 ARP 欺骗的原理是——截获网关数据。它通知路由器一 系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址， 造成正常 PC 无法收到信息。第二种 ARP 欺骗的原理是——伪造网关。它的原理是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的路由器途径上网。在 PC 看来，就是上不了网了，“网络掉线了”。

3.5 局域网 ARP 欺骗的应对

3.5.1 故障现象及原因分析

情况一、当局域网内某台主机感染了 ARP 病毒时，会向本局域网内（指某一网段，比如：10.10.75.0 这一段）所有主机发送 ARP 欺骗攻击谎称自己是这个网端的网关设备，让原本流向网关的流量改道流向病毒主机，造成受害者不能正常上网。

情况二、局域网内有某些用户使用了 ARP 欺骗程序（如：网络执法官,QQ 盗号软件等）发送 ARP 欺骗数据包，致使被攻击的电脑出现突然不能上网，过一段时间又能上网，反复掉线的现象。

3.5.2 故障诊断

如果用户发现以上疑似情况，可以通过如下操作进行诊断：

点击“开始”按钮->选择“运行”->输入“arp－d”->点击“确定”按钮，然后重新尝试上网，如果能恢复正常，则说明此次掉线可能是受 ARP 欺骗所致。

注：arp-d 命令用于清除并重建本机 arp 表。arp－d 命令并不能抵御 ARP

欺骗，执行后仍有可能再次遭受 ARP 攻击。

3.5.3 故障处理

1、中毒者：建议使用趋势科技 SysClean 工具或其他杀毒软件清除病毒。

2、被害者：(1)绑定网关 mac 地址。具体方法如下：

1）首先，获得路由器的内网的 MAC 地址（例如网关地址 10.10.75.254 的 MAC 地址为 0022aa0022aa)。2）编写一个批处理文件 AntiArp.bat 内容如下：@echooffarp-darp-s10.10.75.25400-22-aa-00-22-aa

将文件中的网关 IP 地址和 MAC 地址更改为您自己的网关 IP 地址和 MAC 地址即可，计算机重新启动后需要重新进行绑定，因此我们可以将该批处理文件 AntiArp.bat 文件拖到“windows--开始--程序--启动”中。这样开机时这个批处理就被执行了。

(2)使用 ARP 防火墙(例如 AntiArp)软件抵御 ARP 攻击。

AntiArp 软件会在提示框内出现病毒主机的 MAC 地址

3.5.4 找出 ARP 病毒源

第一招：使用 Sniffer 抓包

在网络内任意一台主机上运行抓包软件，捕获所有到达本机的数据包。如果发现有某个 IP 不断发送

ARP Request 请求包，那么这台电脑一般就是病毒源。原理：无论何种 ARP 病毒变种，行为方式有两种，一是欺骗网关，二是欺骗网内的所有主机。最终的结果是，在网关的 ARP 缓存表中，网内所有活动主机的 MAC 地址均为中毒主机的 MAC 地址;网内所有主机的 ARP 缓存表中,网关的 MAC 地址也成为中毒主机的 MAC 地址。前者保证了从网关到网内主机的数据包被发到中毒主机，后者相反，使得主机发往网关的数据包均发送到中毒主机。

第二招：使用 arp-a 命令任意选两台不能上网的主机，在 DOS 命令窗口下运行 arp-a 命令。例如在结果中，两台电脑除了网关的 IP，MAC 地址对应项，都包含了 192.168.0.186 的这个 IP，则可以断定 192.168.0.186 这台主机就是病毒源。原理：一般情况下，网内的主机只和网关通信。正常情况下，一台主机的

ARP 缓存中应该只有网关的 MAC 地址。如果有其他主机的 MAC 地址，说明本地主机和这台主机最后有过数据通信发生。如果某台主机（例如上面的 192.168.0.186)既不是网关也不是服务器,但和网内的其他主机都有通信活动，且此时又是 ARP 病毒发作时期，那么，病毒源也就是它了。

第三招：使用 tracert 命令在任意一台受影响的主机上，在 DOS 命令窗口下运行如下命令：tracert61.135.179.148。假定设置的缺省网关为 10.8.6.1，在跟踪一个外网地址时，第一跳却是 10.8.6.186，那么，10.8.6.186 就是病毒源。原理：中毒主机在受影响主机和网关之间，扮演了“中间人”的角色。所有本应该到达网关的数据包，由于错误的 MAC 地址，均被发到了中毒主机。此时，中毒主机越俎代庖，起了缺省网关的作用。

第4章 DNS 详解

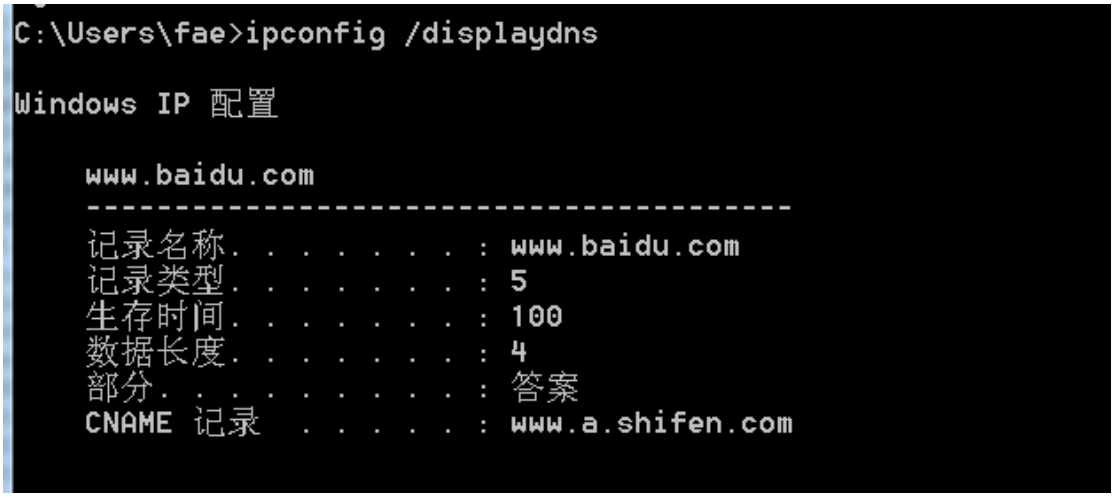
4.1 DNS 的定义

DNS 是计算机域名系统 (Domain Name System 或 Domain Name Service) 的缩写，它是由解析器以及域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应 IP 地址，并具有将域名转换为 IP 地址功能的服务器。DNS 使用 TCP 与 UDP 端口号都是 53，主要使用 UDP，服务器之间备份使用 TCP。

4.2 Dns 常用命令

4.2.1 查看主机 dns 缓存

使用命令 ipconfig –displaydns



4.2.2 清空主机 dns 缓存

使用命令 ipconfig /flushdns

第5章 其他 cmd 命令

1. gpedit.msc-----组策略
2. sndrec32-------录音机
3. Nslookup-------IP 地址侦测器
4. explorer-------打开资源管理器
5. logoff---------注销命令
6. tsshutdn-------60 秒倒计时关机命令
7. lusrmgr.msc----本机用户和组
8. services.msc---本地服务设置

9. oobe/msoobe /a----检查 XP 是否激活
10. notepad--------打开记事本
11. cleanmgr-------垃圾整理
12. net start messenger----开始信使服务
13. compmgmt.msc---计算机管理
14. net stop messenger-----停止信使服务
15. conf----------启动 netmeeting
16. dvdplay--------DVD 播放器
17. charmap--------启动字符映射表
18. diskmgmt.msc---磁盘管理实用程序
19. calc----------启动计算器
20. dfrg.msc-------磁盘碎片整理程序
21. chkdsk.exe-----Chkdsk 磁盘检查
22. devmgmt.msc--- 设备管理器
23. regsvr32 /u *.dll----停止 dll 文件运行
24. drwtsn32------ 系统医生
25. rononce -p ----15 秒关机
26. dxdiag---------检查 DirectX 信息
27. regedit-------注册表编辑器
28. Msconfig.exe---系统配置实用程序
29. rsop.msc-------组策略结果集
30. mem.exe--------显示内存使用情况
31. regedit.exe----注册表
32. winchat--------XP 自带局域网聊天
33. progman--------程序管理器
34. winmsd---------系统信息
35. perfmon.msc----计算机性能监测程序
36. sfc /scannow-----扫描错误并复原
37. taskmgr-----任务管理器（2000/xp/2003

38. winver---------检查 Windows 版本

39. wmimgmt.msc----打开 windows 管理体系结构(WMI)

40. wupdmgr--------windows 更新程序

41. wscript--------windows 脚本宿主设置

42. write----------写字板

43. wiaacmgr-------扫描仪和照相机向导

44. . Msconfig.exe---系统配置实用程序

45. mplayer2-------简易 widnows media player (媒体播放机)

46. mspaint--------画图板

47. mstsc----------远程桌面连接

48. magnify--------放大镜实用程序

49. mmc------------打开控制台

50. mobsync--------同步命令

51. dcomcnfg-------打开系统组件服务

52. ddeshare-------打开 DDE 共享设置

53. nslookup-------网络管理的工具向导

54. ntbackup-------系统备份和还原

55. narrator-------屏幕“讲述人”

56. ntmsmgr.msc----移动存储管理器

57. ntmsoprq.msc---移动存储管理员操作请求

58. netstat -an----(TC)命令检查接口

59. syncapp--------创建一个公文包

60. sysedit--------系统配置编辑器

61. sigverif-------文件签名验证程序

62. shrpubw--------创建共享文件夹

63. secpol.msc-----本地安全策略

64. syskey---------系统加密，一旦加密就不能解开，保护 windows xp 系统的双重密码

65. services.msc---本地服务设置

66. Sndvol32-------音量控制程序
67. sfc.exe--------系统文件检查器
68. tourstart------xp 简介（安装完成后出现的漫游 xp 程序）
69. eventvwr-------事件查看器
70. eudcedit-------造字程序
71. packager-------对象包装程序
72. regedit.exe----注册表
73. regsvr32 /u zipfldr.dll------取消 ZIP 支持
74. cmd.exe--------CMD 命令提示符
75. chkdsk.exe-----Chkdsk 磁盘检查
76. certmgr.msc----证书管理实用程序
77. cliconfg-------SQL SERVER 客户端网络实用程序
78. Clipbrd--------剪贴板查看器
79. ciadv.msc------索引服务程序
80. osk------------打开屏幕键盘
81. odbcad32-------ODBC 数据源管理器
82. iexpress-------木马捆绑工具，系统自带
83. fsmgmt.msc-----共享文件夹管理器
84. utilman--------辅助工具管理器