

网络维护与诊断

一般的网络硬件故障大多处于网络的最底层——物理层。排除这些故障离不开一些仪表及 PC 辅助工具，否则就只有望网兴叹，无从下手。而本章主要是针对用户所见到的网络故障的诊断与维护，需要一定的网络理论分析能力。本章以局域网的网络环境为基础，以对网络中可能出现的问题展开详细讨论。

【实训内容】检查网络故障的原因，了解常见的网络端口以及 ARP 病毒攻击与预防。并熟练掌握以下 windows 网络命令

◎Ping

◎Netstat

◎IPconfig

◎ARP

◎Tracert

【提示】如果是单机用户，建议读者学习本次实训前先掌握 VM 虚拟机的使用，有关虚拟机的使用教程请见本书附录一。

.1 准备知识

很多读者会问一个问题“同一个网络环境中，为什么别能上网，而我不能？”造成不能上网的原因很多，不能上网的情况也很多，不能笼统称为不能上网。例如可以访问外网但是不能访问内网，或者能够访问内网而不能访问外网，又或者在访问外网的同时，某些网络软件可以使用，如 QQ 可以使用，但是某些软件不能正常使用，诸如 IE 等。

不同的网络故障需要不同的方法进行检查、诊断。下面我们在动手实践这个环节通过服务、端口、病毒几个方面展开讨论。

.2 动手实践

.2.1 如何检查网络故障

实验目的：熟练掌握用以下 windows 网络命令检查网络故障发生的原因。

◎Ping

◎IPconfig

◎Tracert

实验环境：设备要求：装配 windows 2003（XP 亦可，截图以 windows2003 为标准，下同）操作系统的联网 PC 机若干台。

实验步骤：

判断网络故障是非常重要的。有时候我们会出现一个问题，当把网卡的驱动反复检查没有问题，系统重装之后都解决不了问题，最好发现网线没有插好。这种状况时有发生，所以我们在诊断网络故障的时候，第一步就是要判断网络故障的位置。

网络一旦出现故障，首先就应该想到使用“ping”。该命令是专业人员经常用来查找故障原因的基本命令，用以确认能否通过 IP 网络与通信对象交换信息。该命令在每当出现无法接入目标服务器的故障时，对于了解故障情况非常重要。下面将结合 ping 命令的用法对此加以介绍。

ping 是一条用于分析能否通过 IP 网络与特定计算机进行通信的命令。向 IP 地址所指定的对象发送信息，然后等待对方的应答。

如果能够正常地收到应答，就说明对方的计算机以及中间的线路是正常的。如果没有收到应答，或者收到应答所需的时间太长，就能推断网络的某个地方存在问题。

ping 命令的基本用法非常简单。在 Windows NT/2000/XP/VISTA 系统中打开命令提示符，只需在 ping 提示符后面输入想要调查的能否进行通信的计算机的地址即可。

1 · Ping 命令介绍

Ping 是个使用频率极高的实用程序，用于确定本地主机是否能与另一台主机交换（发送与接收）数据报。根据返回的信息，我们就可以推断 TCP/IP 参数是否设置得正确以及运行是否正常。需要注意的是：成功地与另一台主机进行一次或两次数据报交换并不表示 TCP/IP 配置就是正确的，我们必须执行大量的本地主机与远程主机的数据报交换，才能确信 TCP/IP 的正确性。

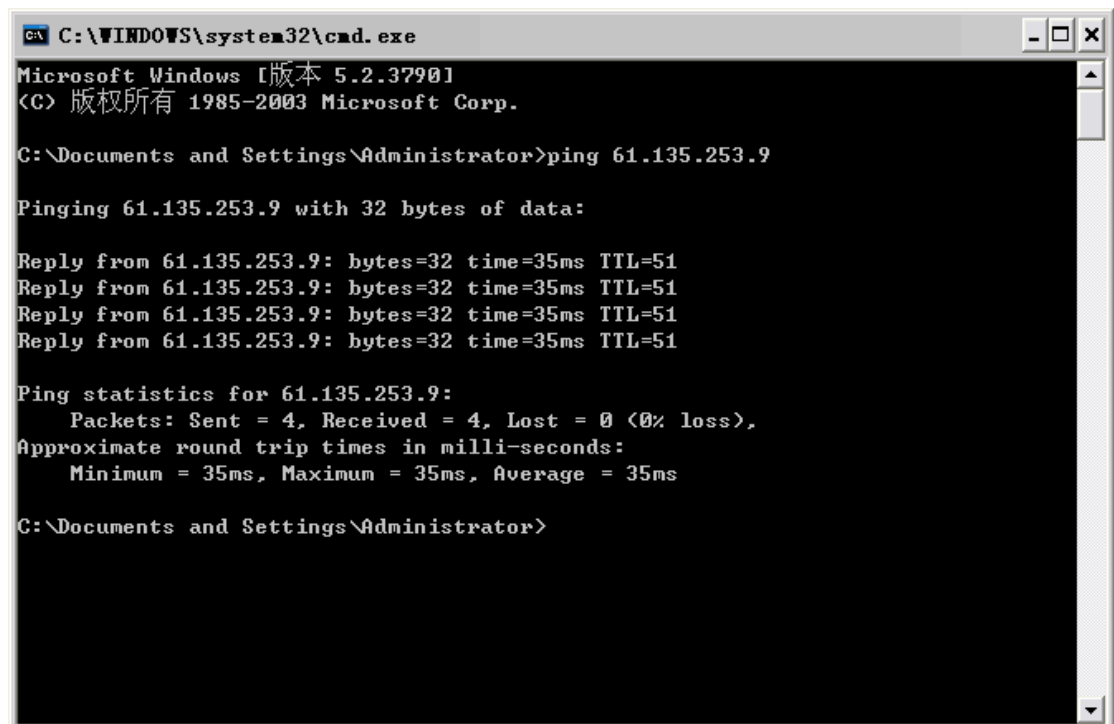
简单的说，Ping 就是一个测试程序，如果 Ping 运行正确，我们大体上就可以排除网络访问层、网卡、MODEM 的输入输出线路、电缆和路由器等存在的故障，从而减小了问题的范围。但由于可以自定义所发数据报的大小及无休止的高速发送，Ping 也被某些别有用心的人作为 DDOS（拒绝服务攻击）的工具，例如许多大型的网站就是被黑客利用数百台可以高速接入互联网的电脑连续发送大量 Ping 数据报而瘫痪的。

按照缺省设置，Windows 上运行的 Ping 命令发送 4 个 ICMP（网间控制报文协议）回送请求，每个 32 字节数据，如果一切正常，我们应能得到 4 个回送应答，如图所示。Ping 能够以毫秒为单位显示发送回送请求到返回回送应答之间的时间量。如果应答时间短，表示数据报不必通过太多的路由器或网络连接速度比较快。

Ping 还能显示 TTL（Time To Live 存在时间）值，TTL 是 IP 协议包中的一个值，它告诉网络路由器包在网络中的时间是否太长而应被丢弃。有很多原因使包在一定时间内不能被传递到目的地。例如，不正确的路由表可能导致包的无限循环。所以需要在包中设置这样一个值，包在每经过一个节点，将这个值减 1，反复这样操作，最终可能造成两个结果：包在这个值还为正数的时候到达了目的地，或者是在经过一定数量的节点后，这个值减为了 0。前者代表完成了一次正常的传输，后者代表包可能选择了一条非常长的路径甚至是进入了环路，这显然不是我们期望的，所以在这个值为 0 的时候，网络设备将不会再传递这个包而是直接将他抛弃，并发送一个通知给包的源地址，说这个包已死。第二个问题，通过 TTL 值我们能得到什么 其实 TTL 值这个东西本身并代表不了什么，对于使

用者来说，关心的问题应该是包是否到达了目的地而不是经过了几个节点后到达。但是 TTL 值还是可以得到有意思的信息的。每个操作系统对 TTL 值得定义都不同，这个值甚至可以通过修改某些系统的网络参数来修改，不同的操作系统，它的 TTL 值默认值是不相同的。默认情况下，Linux 系统的 TTL 值为 64 或 255，Windows NT/2000/XP 系统的 TTL 值为 128，Windows 98 系统的 TTL 值为 32，UNIX 主机的 TTL 值为 255。

我们可以通过 TTL 值推算一下数据包已经通过了多少个路由器：源地点 TTL 起始值一返回时 TTL 值。例如，返回 TTL 值为 51，那么可以推算数据报离开源地址的 TTL 起始值为 64（查看对应的操作系统，一般情况下，比返回 TTL 略大的一个 2 的乘方数）则源地点到目标地点要通过 13 个路由器网段（64-51），如图 5-1 所示；如果返回 TTL 值为 119，TTL 起始值就是 128，源地点到目标地点要通过 9 个路由器网段（128-119）。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 61.135.253.9

Pinging 61.135.253.9 with 32 bytes of data:

Reply from 61.135.253.9: bytes=32 time=35ms TTL=51
Reply from 61.135.253.9: bytes=32 time=35ms TTL=51
Reply from 61.135.253.9: bytes=32 time=35ms TTL=51
Reply from 61.135.253.9: bytes=32 time=35ms TTL=51

Ping statistics for 61.135.253.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 35ms, Average = 35ms

C:\Documents and Settings\Administrator>
```

图 5-1

输入 ping 命令后，就会显示出相应的结果。所显示的结果共有 3 种。

如果显示为“Relay from.....”，说明对方的计算机工作正常，中间的线路也正常。显示结果共有 4 行，后面显示的是测试结果的统计信息。在标准情况下使用 ping 命令，将反复 4 次发送 IP 信息并显示应答结果。

如果显示为“Request timed out.”，表示在规定时间内因某种原因没有返回 ping 命令的应答。这种情况说明很可能是对方的计算机没有运行，或者中间线路不通致使信息没有到达对方那里。大多数情况下是企业防火墙等阻挡了 ping 命令中使用的 ICMP 信息。在这种情况下即便通信对象正在工作，ping 命令的结果也会显示“Request timed out.”的结果。

有时在执行 ping 命令后，也会显示“Destination host unreachable.”。此错误信息表明执行命令的计算机没能将信息发送到对方那里。大多数情况是自己一方的计算机 LAN 连接线掉线，或者由于 IP 设置不对，而无法进行正常通信。

仅依靠这 3 种结果，就可一定程度上了解网络信息，如果进一步使用 ping 命令选项，还能够用于解决网络故障。用户可用命令帮助选项“? ”，列表显示可在 ping 命令中使用那些命令选项。操作方法是“ping-?”或“ping/?”。

图 5-2 显示的对 XP 下的 ping 命令参数解释，5-2 显示 2003 下的命令选项，加多了 IPv4 和 IPv6 选项

选项	意义
-t	连续发送和接收回送请求和应答 ICMP 报文直到手动停止(Ctr-Break: 查看统计信息, Ctr-C: 停止 ping 命令)
-a	将 IP 地址解析为主机名
-n count	发送回送请求 ICMP 报文的次数(缺省值为 4)
-l size	发送探测数据包的大小(缺省值为 32 字节)
-f	不允许分片(缺省为允许分片)
-i TTL	指定生存周期
-v TOS	指定要求的 service 类型
-r count	记录路由
-s count	使用时间戳选项
-j host-list	使用松散源路由选项
-k host-list	使用严格源路由选项
-w timeout	指定等待每个回送应答的超时时间(以毫秒为单位, 缺省值为 1,000)

图 5-2

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>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.
  
```

图 5-3

2 · IPconfig 命令介绍

IPConfig 通常使用它显示计算机中网络适配器的 IP 地址、子网掩码及默认网关。这些信息一般用来检验人工配置的 TCP/IP 设置是否正确。但是，如果我们的计算机和所在的局域网使用了动态主机配置协议 (DHCP)，这个程序所显示的信息也许更加实用。这时，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、子网掩码和缺省网关实际上是进行测试和故障分析的必要项目。

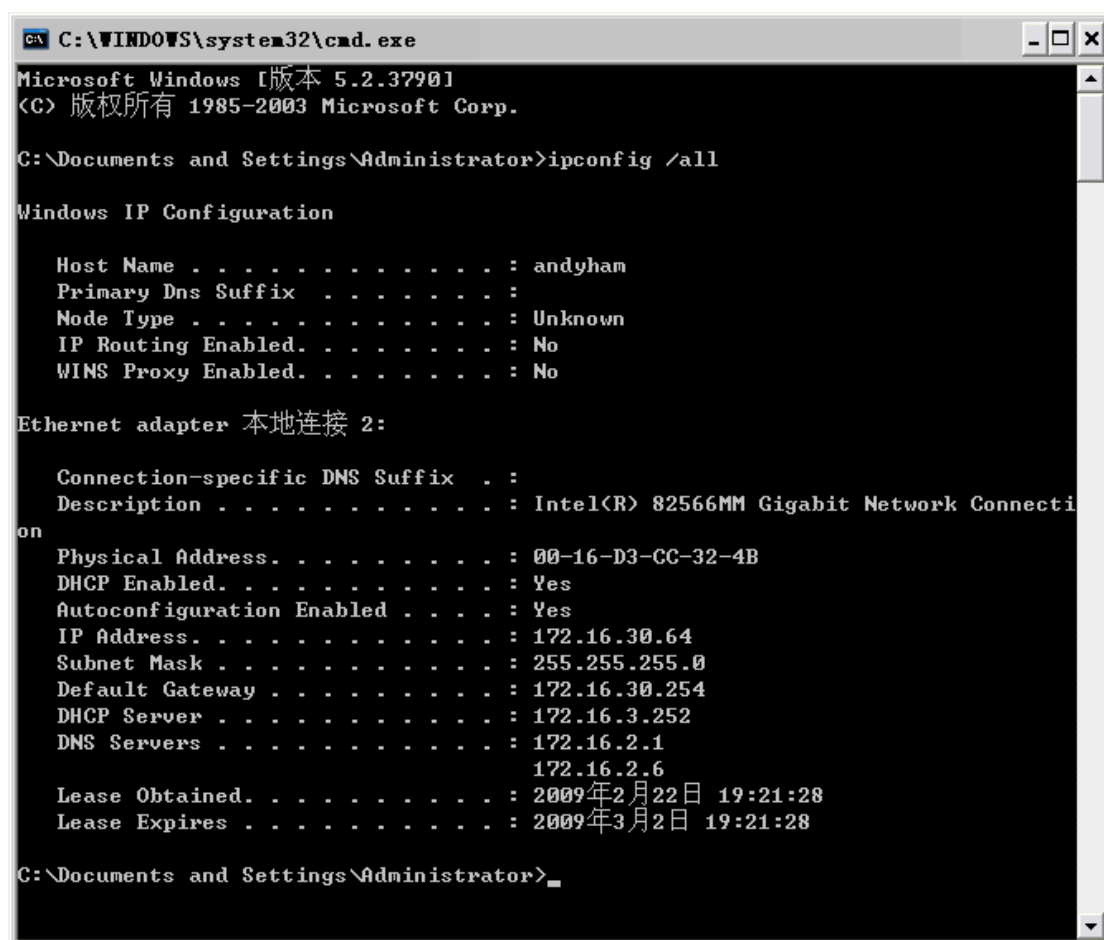
总的参数简介(也可以在 DOS 方式下输入 IPconfig /? 进行参数查询)

1) IPconfig

当不带任何参数时，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。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

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

Ethernet adapter 本地连接 2:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82566MM Gigabit Network Connection
Physical Address. . . . . : 00-16-D3-CC-32-4B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 172.16.30.64
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.30.254
DHCP Server . . . . . : 172.16.3.252
DNS Servers . . . . . : 172.16.2.1
                        172.16.2.6
Lease Obtained. . . . . : 2009年2月22日 19:21:28
Lease Expires . . . . . : 2009年3月2日 19:21:28

C:\Documents and Settings\Administrator>
```

图 5-4

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。

4) IPconfig /flushdns

清除本地 DNS 缓存内容；

5) IPconfig /displaydns

显示本地 DNS 内容；

6) IPconfig /registerdns

DNS 客户端手工向服务器进行注册；

7) IPconfig /showclassid

显示网络适配器的 DHCP 类别信息；

8) IPconfig /setclassid

设置网络适配器的 DHCP 类别。

3 · 检测网络故障的典型次序

正常情况下，当我们使用 Ping 命令来查找问题所在或检验网络运行情况时，我们需要使用许多 Ping 命令，如果所有都运行正确，我们就可以相信基本的连通性和配置参数没有问题；如果某些 Ping 命令出现运行故障，它也可以指明到何处去查找问题。下面就给出一个典型的检测次序及对应的可能故障：

1) 检查计算机之间的物理连接

网卡是网络连接的基本设备，在桌面计算机中，每个网卡后面的指示灯应该是亮的，这表示连接是正常的。如果不亮，请检查集线器或交换机是打开的，而且每个客户端连接的指示灯都是亮的，这表示链接是正常的。接下来检查网线的水晶头是否接触良好。

2) ping 127.0.0.1

这个 Ping 命令被送到本地计算机的 IP 软件，该命令永不退出该计算机。如果没有做到这一点，就表示 TCP/IP 的安装或运行存在某些最基本的问题。

3) ping 本机 IP

这个命令被送到我们计算机所配置的 IP 地址，我们的计算机始终都应该对该 Ping 命令作出应答，如果没有，则表示本地配置或安装存在问题。出现此问

题时，局域网用户请断开网络电缆，然后重新发送该命令。如果网线断开后本命令正确，则表示另一台计算机可能配置了相同的 IP 地址。

4) ping 局域网内其他 IP

这个命令应该离开我们的计算机，经过网卡及网络电缆到达其他计算机，再返回。收到回送应答表明本地网络中的网卡和载体运行正确。但如果收到 0 个回送应答，那么表示子网掩码（进行子网分割时，将 IP 地址的网络部分与主机部分分开的代码）不正确或网卡配置错误或电缆系统有问题。

5) ping 网关 IP

应答正确，表示局域网中的网关路由器正在运行并能够作出应答。

6) ping 远程 IP

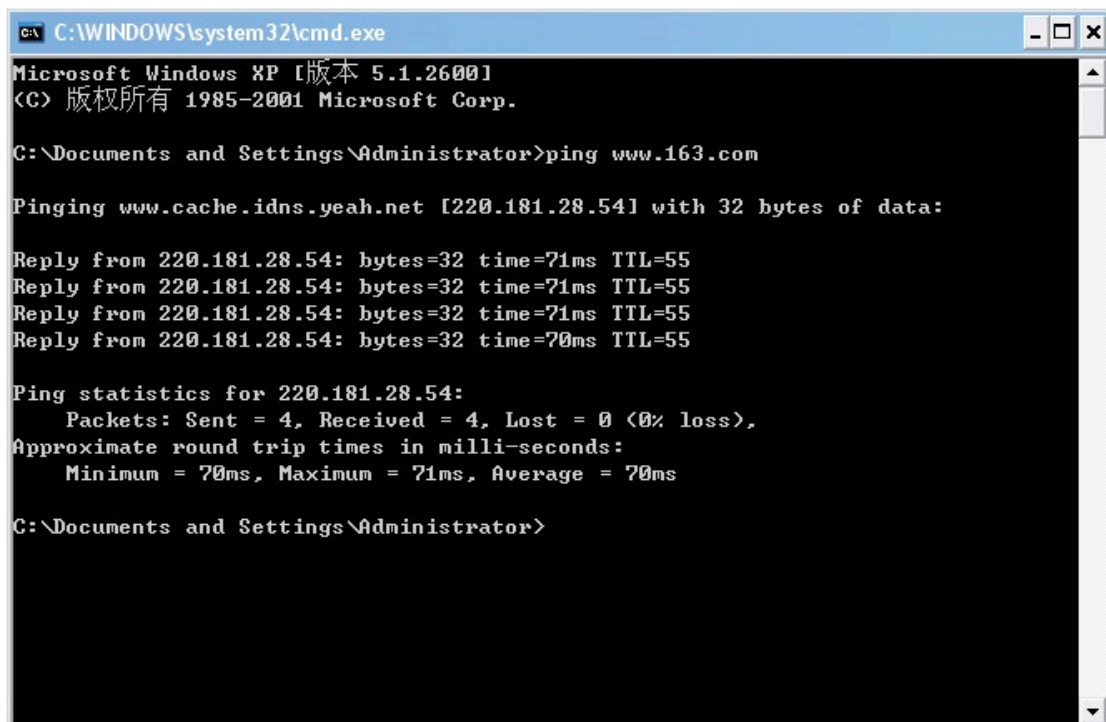
如果收到 4 个应答，表示成功的使用了缺省网关。对于拨号上网用户则表示能够成功的访问 Internet（但不排除 ISP 的 DNS 会有问题）。

7) ping localhost

localhost 是个作系统的网络保留名，它是 127.0.0.1 的别名，每台计算机都应该能够将该名字转换成该地址。如果没有做到这一带内，则表示主机文件（/Windows/host）中存在问题。

8) ping www.xxx.com

对这个域名执行 Ping www.xxx.com 地址，通常是通过 DNS 服务器 如果这里出现故障，则表示 DNS 服务器的 IP 地址配置不正确或 DNS 服务器有故障（对于拨号上网用户，某些 ISP 已经不需要设置 DNS 服务器了）。顺便说一句：我们也可以利用该命令实现域名对 IP 地址的转换功能，从下图我们了解到从本地到 www.163.com 共经过了 9 个路由器的网段（TTL=55）。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping www.163.com

Pinging www.cache.idns.yeah.net [220.181.28.54] with 32 bytes of data:

Reply from 220.181.28.54: bytes=32 time=71ms TTL=55
Reply from 220.181.28.54: bytes=32 time=71ms TTL=55
Reply from 220.181.28.54: bytes=32 time=71ms TTL=55
Reply from 220.181.28.54: bytes=32 time=70ms TTL=55

Ping statistics for 220.181.28.54:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 70ms, Maximum = 71ms, Average = 70ms

C:\Documents and Settings\Administrator>
```

图 5-5

9) Tracert

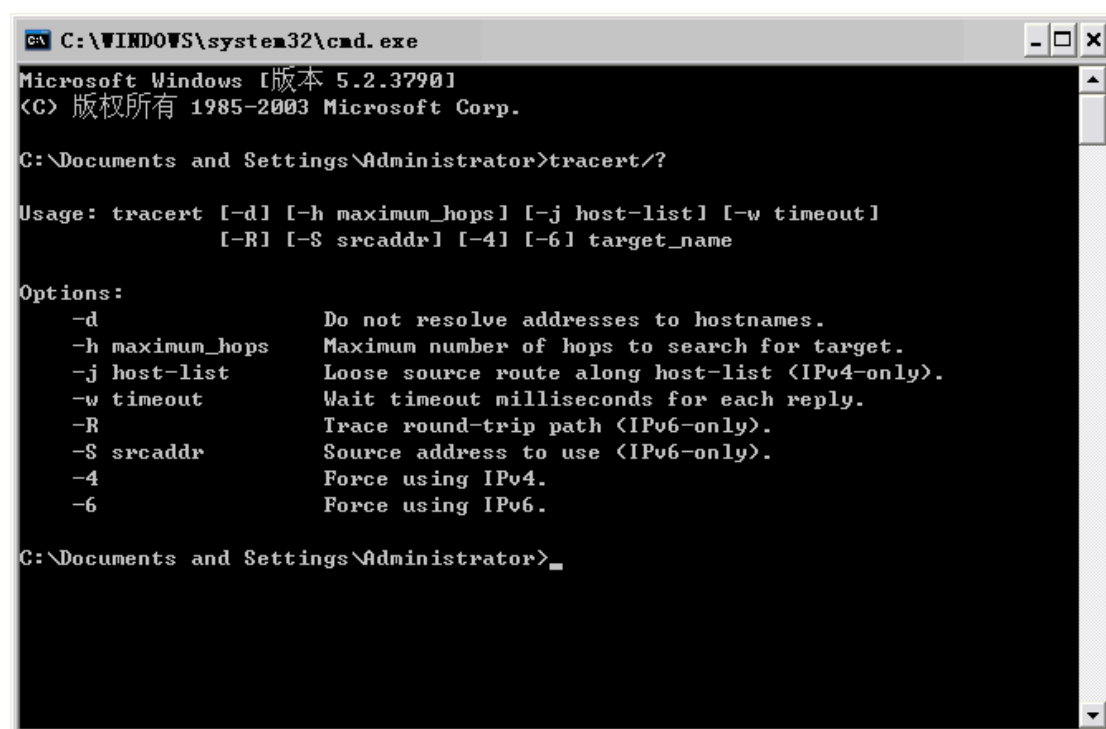
如果网络连通仍有问题，想了解具体在哪个环境出了状况，探测网络故障的位置。我们可以用 **Tracert** 命令。虽然 **Tracert** 命令不能分析问题的状况，但是至少可以检测问题所在的位置。

Tracert 命令用来检查到达的目标 IP 地址的路径并记录结果。**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。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。当数据报从你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）。该实用程序跟踪的路径是源计算机到目的地的一条路径，不能保证或认为数据报总遵循这个路径。如果你的配置使用 **DNS**，那么你常常会从所产生的应答中得到城市、地址和常见通信公司的名字。**Tracert** 是一个运行得比较慢的命令（如果你指定的目标地址比较远），每个路由器你大约需要给它 15 秒钟。

该诊断实用程序将包含不同生存时间（**TTL**）值的 **Internet** 控制消息协议（**ICMP**）回显数据包发送到目标，以决定到达目标采用的路由。要在转发数据包上的 **TTL** 之前至少递减 1，必需路径上的每个路由器，所以 **TTL** 是有效的跃点计数。数据包上的 **TTL** 到达 0 时，路由器应该将“**ICMP** 已超时”的消息发送回源系统。**Tracert** 先发送 **TTL** 为 1 的回显数据包，并在随后的每次发送过程将 **TTL** 递增 1，直到目标响应或 **TTL** 达到最大值，从而确定路由。路由通过检查中级路由器发送回的“**ICMP** 已超时”的消息来确定路由。不过，有些路由器悄悄地下传包含过期 **TTL** 值的数据包，而 **tracert** 看不到。

Tracert 的使用很简单，只需要在 **tracert** 后面跟一个 IP 地址或 URL，**Tracert** 会进行相应的域名转换的。

tracert 最常见的用法:



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

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

C:\Documents and Settings\Administrator>
```

图 5-6

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

参数

-d : 指定不将地址解析为计算机名(将更快地显示路由器路径, 因为 tracert 不会尝试解析路径中路由器的名称)。

-h maximum_hops : 指定搜索目标的最大跃点数。

-j computer-list : 指定沿 computer-list 的稀疏源路由。

-w timeout : 每次应答等待 timeout 指定的微秒数。

【注意】-R -S srcaddr -4 -6 参数涉及到 IPv6, 暂不讨论。

其实, Tracert 也可以不带任何参数, 例如本例中想了解从本地到从本地到 www.163.com (IP 地址为: 220.181.28.52) 的网络状况, 图 5-7 中共经历了 9 个路由器的网段, 与上图 ping 命令中加入对域名解析图 5-5 中所显示的 TTL 值相吻合。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>tracert www.163.com

Tracing route to www.cache.idns.yeah.net [220.181.28.52]
over a maximum of 30 hops:

  1    40 ms    39 ms    39 ms  116.28.208.1
  2    30 ms    31 ms    30 ms  61.146.21.201
  3    30 ms    30 ms    29 ms  193.26.146.61.broad.zj.gd.dynamic.163data.com.cn
[61.146.26.193]
  4    38 ms    37 ms    37 ms  202.97.64.250
  5    69 ms    70 ms    69 ms  202.97.34.117
  6    71 ms    72 ms    71 ms  202.97.37.25
  7    70 ms    70 ms    70 ms  220.181.16.149
  8    74 ms    72 ms    79 ms  220.181.16.10
  9    79 ms    71 ms    72 ms  220.181.17.54
 10    69 ms    70 ms    69 ms  220.181.28.52

Trace complete.

C:\Documents and Settings\Administrator>
```

图 5-7

如果上面所列出的所有网络命令都能正常运行，那么我们对自已的计算机进行本地和远程通信的功能基本上就可以放心了。但是，这些命令的成功并不表示我们所有的网络配置都没有问题，例如，某些子网掩码错误就可能无法用这些方法检测到。

2.2 常见的端口

实验目的：熟练掌握用 windows 的 Netstat 网络命令查看常见的端口

实验环境：设备要求：装配 windows 2003 (XP 亦可，截图以 windows2003 为标准，下同) 操作系统的联网 PC 机若干台。

实验步骤：

我们经常在生活中出现这样类似的网络问题，例如：为什么访问 Internet 一切正常而不能访问局域网内其他人的共享文件夹或者 FTP 服务器；又或者为什么能上 QQ 而不能使用 IE。除开病毒的影响之外，另一个直接的原因就是端口。

无论是 windows 还是 linux 操作系统，提供的网络服务都对应着相应的网络端口号。下面我们来了解一下端口的作用和如何利用端口对网络进行诊断

1. 什么是端口

计算机“端口”是英文 port 的义译，可以认为是计算机与外界通讯交流的出口。其中硬件领域的端口又称接口，如：USB 端口、串行端口等。软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和 I/O（基本输入输出）缓冲区。

按端口号可分为 3 大类：

1) 公认端口 (Well Known Ports)

从 0 到 1023, 它们紧密绑定 (binding) 于一些服务。通常这些端口的通讯明确表明了某种服务的协议。例如: 80 端口实际上总是 HTTP 通讯。

2) 注册端口 (Registered Ports)

从 1024 到 49151。它们松散地绑定于一些服务。也就是说有许多服务绑定于这些端口, 这些端口同样用于许多其它目的。例如: 许多系统处理动态端口从 1024 左右开始。

3) 动态和/或私有端口 (Dynamic and/or Private Ports)

从 49152 到 65535。理论上, 不应为服务分配这些端口。实际上, 机器通常从 1024 起分配动态端口。但也有例外: SUN 的 RPC 端口从 32768 开始。

2 · 常见的端口

一些端口常常会被黑客利用, 还会被一些木马病毒利用, 所以很多防火墙将这些端口对应的服务给关掉了, 以此来预防对计算机系统进行攻击。以下是 windows 计算机公认端口的介绍以及防止被黑客攻击的简要办法。

【试一试】由于操作系统的常见端口比较多, 不可能在此书中一一罗列, 建议搜索关键字: 计算机 端口。

1) 端口: 21 服务: FTP

说明: FTP 服务器所开放的端口, 用于上传、下载。最常见的攻击者用于寻找打开 anonymous 的 FTP 服务器的方法。这些服务器带有可读写的目录。木马 Doly Trojan、Fore、Invisible FTP、WebEx、WinCrash 和 Blade Runner 所开放的端口。

2) 端口: 25 服务: SMTP

说明: SMTP 服务器所开放的端口, 用于发送邮件。入侵者寻找 SMTP 服务器是为了传递他们的 SPAM。入侵者的帐户被关闭, 他们需要连接到高带宽的 E-MAIL 服务器上, 将简单的信息传递到不同的地址。木马 Antigen、Email Password Sender、Haebu Coceda、Shtrilitz Stealth、WinPC、WinSpy 都开放这个端口。

3) 端口: 80 服务: HTTP

说明: 用于网页浏览。木马 Executor 开放此端口。

4) 端口: 135 服务: Location Service

说明: 135 端口主要用于使用 RPC (Remote Procedure Call, 远程过程调用)

端口漏洞: 相信早 2 年很多 Windows 2000 和 Windows XP 用户都中了“冲击波”病毒, 该病毒就是通过 135 端口入侵, 利用 RPC 漏洞来攻击计算机的。目前也有非常多的木马后门通过 135 端口进行上传, 当然, 如果严格保密有关 IP

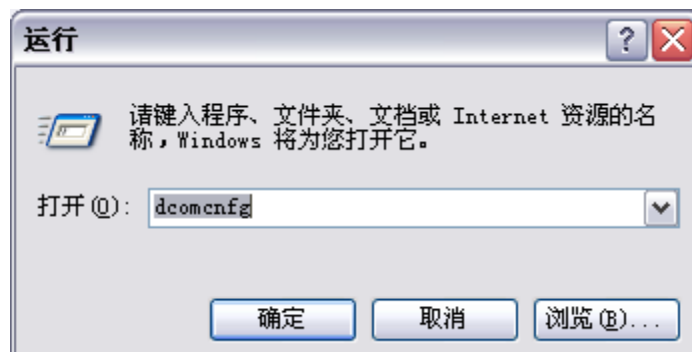
地址、系统登录名和密码，被攻击的可能性几乎不存在。

协议并提供 DCOM（分布式组件对象模型）服务，通过 RPC 可以保证在一台计算机上运行的程序可以顺利地执行远程计算机上的代码；使用 DCOM 可以通过网络直接进行通信，能够跨包括 HTTP 协议在内的多种网络传输。

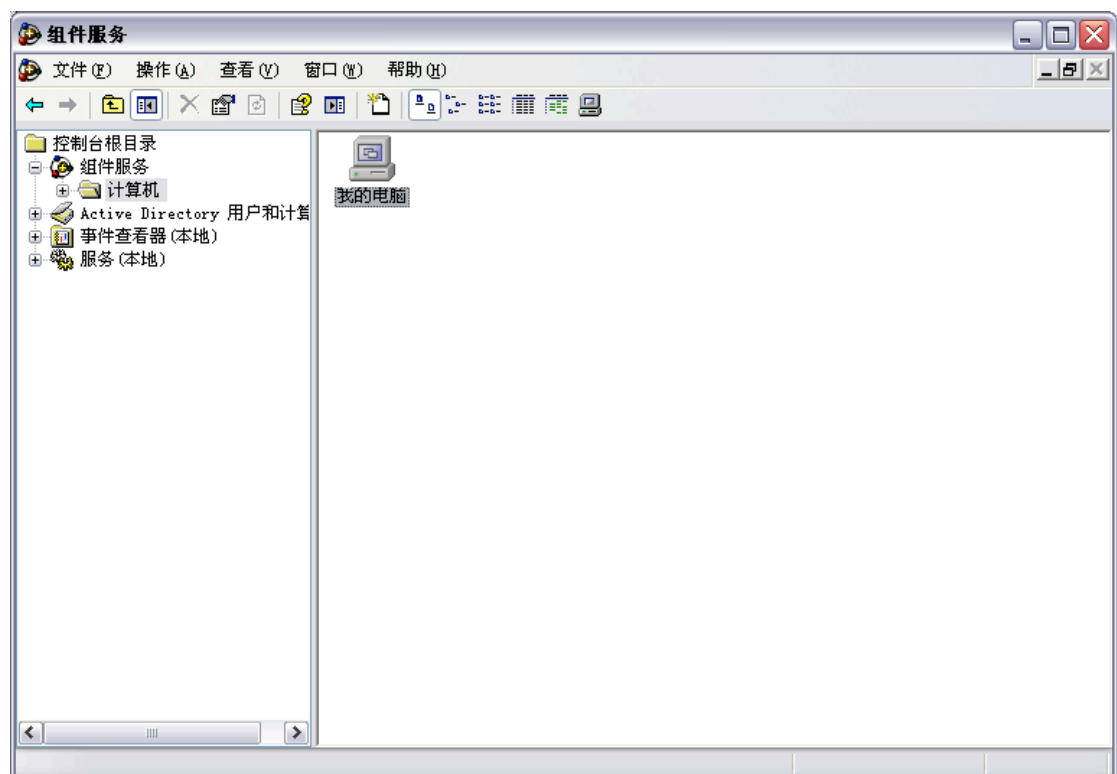
RPC 本身在处理通过 TCP/IP 的消息交换部分有一个漏洞，该漏洞是由于错误地处理格式不正确的消息造成的。该漏洞会影响到 RPC 与 DCOM 之间的一个接口，该接口侦听的端口就是 135。说简单一点，135 端口就是 RPC 通信中的桥梁。

关闭 135 端口方法：

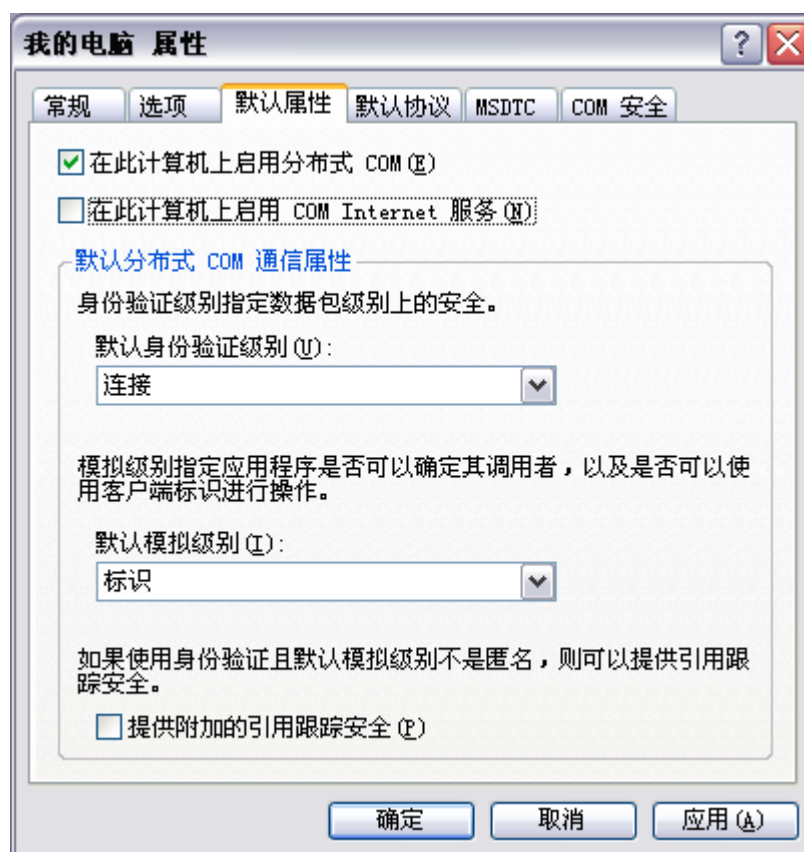
第一步：单击“开始”——“运行”，输入“dcomcnfg”，单击“确定”，打开组件服务。



第二步：在弹出的“组件服务”对话框中，选择“计算机”选项。



第三步：在“计算机”选项右边，右键单击“我的电脑”，选择“属性”。在出现的“我的电脑属性”对话框“默认属性”选项卡中，去掉“在此计算机上启用分布式 COM”前的勾。



5) 端口：137、138、139 服务：NETBIOS Name Service

说明：当开启远程桌面 RDP 服务的时候，总是能在后台看到启用的这几个端口。如果防火墙关掉这几个窗口，就无法在网络邻居上看到其他计算机，其他机也无法看到你，换句话说，无法享受共享服务。

137 端口的主要作用是在局域网中提供计算机的名字或 IP 地址查询服务，一般安装了 NetBIOS 协议后，该端口会自动处于开放状态。

要是非法入侵者知道目标主机的 IP 地址，并向该地址的 **137** 端口发送一个连接请求时，就可能获得目标主机的相关名称信息。例如目标主机的计算机名称，注册该目标主机的用户信息，目标主机本次开机、关机时间等。此外非法入侵者还能知道目标主机是否是作为文件服务器或主域控制器来使用。

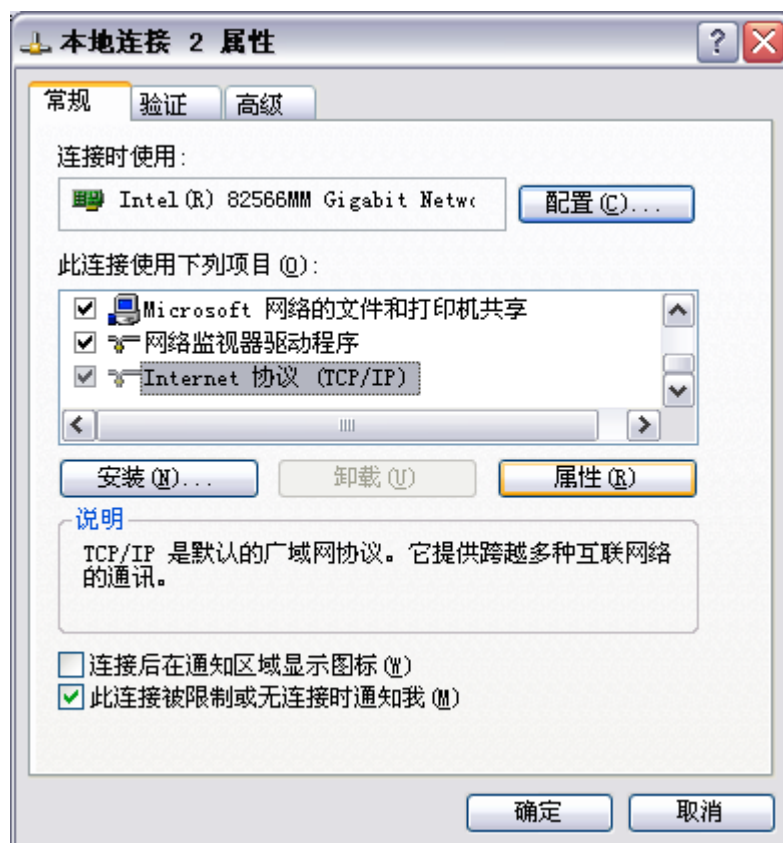
138 端口

137、**138** 端口都属于 UDP 端口，它们在局域网中相互传输文件信息时，就会发生作用。而 **138** 端口的主要作用就是提供 NetBIOS 环境下的计算机名浏览功能。

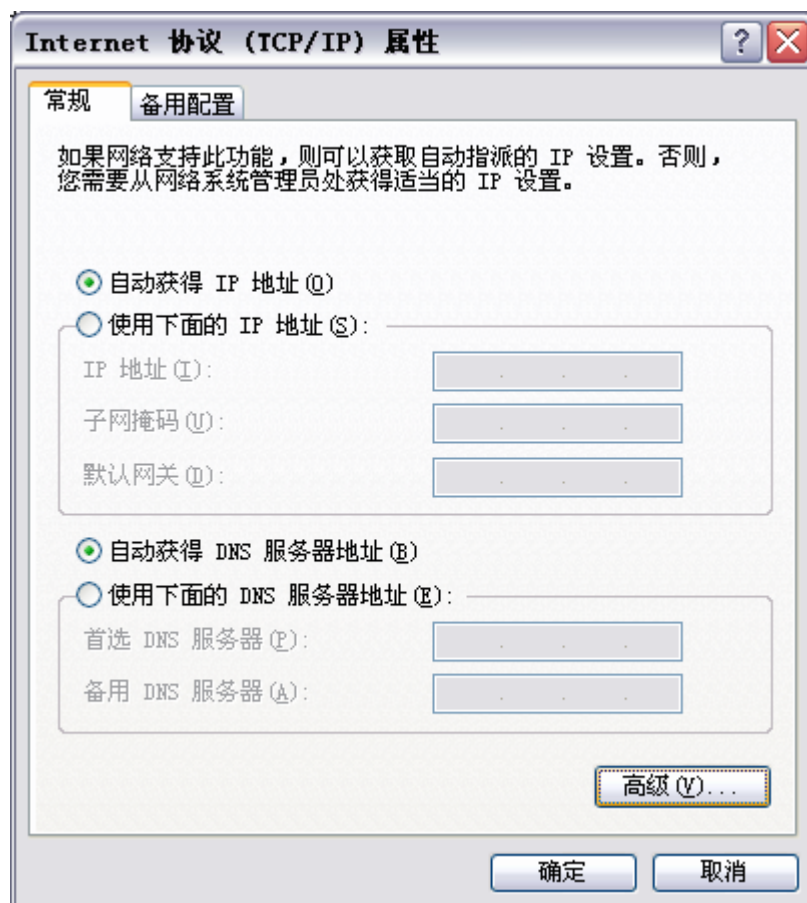
非法入侵者要是与目标主机的 **138** 端口建立连接请求的话，就能轻松获得目标主机所处的局域网网络名称以及目标主机的计算机名称。有了计算机名称，其对应的 IP 地址也就能轻松获得。如此一来，就为黑客进一步攻击系统带来了便利。

关闭 137、138 端口方法：

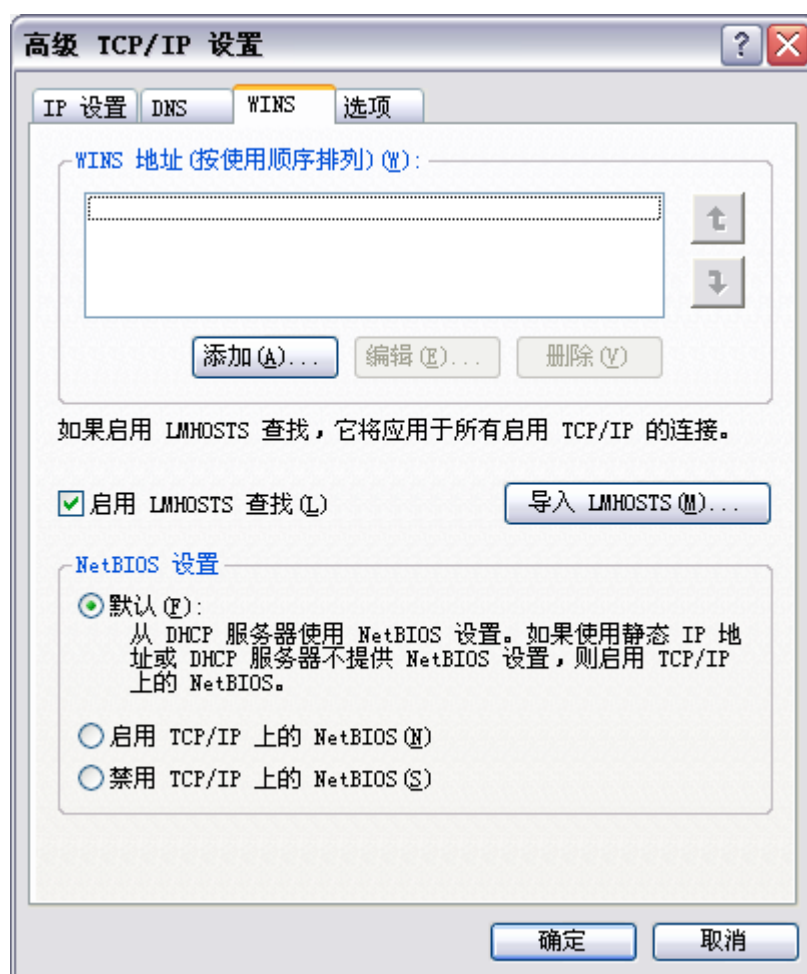
第一步：右击“网络邻居”——“本地连接”，选择“Internet 协议（TCP/IP）”，单击“属性”。



第二步：选择”高级”选项



第三步：选择“WINS”选项卡，选择”禁用 TCP/IP”上的 NetBIOS，即可。



139 端口

139 端口是一种 TCP 端口，该端口在你通过网上邻居访问局域网中的共享文件或共享打印机时就能发挥作用。

139 端口一旦被 Internet 上的某个攻击者利用的话，就能成为一个危害极大的安全漏洞。因为黑客要是与目标主机的 139 端口建立连接的话，就很有可能浏览到指定网段内所有工作站中的全部共享信息，甚至可以对目标主机中的共享文件夹进行各种编辑、删除操作，倘若攻击者还知道目标主机的 IP 地址和登录帐号的话，还能轻而易举地查看到目标主机中的隐藏共享信息。

445 端口(仅 WIN2K 及以后的操作系统)

445 端口也是一种 TCP 端口，该端口在 Windows 2000 Server 或 Windows Server 2003 系统中发挥的作用与 139 端口是完全相同的。具体地说，它也是提供局域网中文件或打印机共享服务。不过该端口是基于 CIFS 协议 (Common Internet File System) 工作的，而 139 端口是基于 SMB 协议 (服务器协议族) 对外提供共享服务。同样地，攻击者与 445 端口建立请求连接，也能获得指定局域网内的各种共享信息。

3 · 如何查看本机开放的端口

Netstat 用于显示协议统计信息和当前 TCP/IP 网络连接，一般用于检验本机各端口的网络连接情况。

如果我们的计算机有时候接受到的数据报会导致出错数据删除或故障，我们不必感到奇怪，**TCP/IP** 可以容许这些类型的错误，并能够自动重发数据报。但如果累计的出错情况数目占到所接收的 **IP** 数据报相当大的百分比，或者它的数目正迅速增加，那么我们就应该使用 **Netstat** 查一查为什么会出现这些情况了。

其格式如下：

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

下面简单说明各个参数的含义：

1) **netstat -a**

本选项显示一个所有的有效连接信息列表，包括已建立的连接（**ESTABLISHED**），也包括监听连接请求（**LISTENING**）的那些连接。

2) **netstat -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。

3) **netstat -e**

本选项用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。这个选项可以用来统计一些基本的网络流量）。

4) **netstat -n**

显示所有已建立的有效连接。

5) **netstat -o**

显示与每个连接相关的所属进程 **ID**。

6) **netstat -p**

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**。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -p tcp

Active Connections

Proto Local Address          Foreign Address         State
TCP   PC-200903281817:2042    bogon:3389             ESTABLISHED

C:\Documents and Settings\Administrator>
```

7) netstat -r

本选项可以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。

8) netstat -s

本选项能够按照各个协议分别显示其统计数据。如果我们的应用程序（如 **Web** 浏览器）运行速度比较慢，或者不能显示 **Web** 页之类的数据，那么我们就可以用本选项来查看一下所显示的信息。我们需要仔细查看统计数据的各行，找到出错的关键字，进而确定问题所在。

9) netstat -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。

10) 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)。

`netstat` 的参数可同时使用，例如 `netstat -ano:`

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -ano

Active Connections

    Proto Local Address           Foreign Address         State               PID
    TCP    0.0.0.0:80              0.0.0.0:0              LISTENING           4
    TCP    0.0.0.0:135             0.0.0.0:0              LISTENING           708
    TCP    0.0.0.0:445             0.0.0.0:0              LISTENING           4
    TCP    0.0.0.0:1025            0.0.0.0:0              LISTENING           476
    TCP    0.0.0.0:1026            0.0.0.0:0              LISTENING           976
    TCP    0.0.0.0:6059            0.0.0.0:0              LISTENING           1008
    TCP    127.0.0.1:1027          0.0.0.0:0              LISTENING           2464
    TCP    127.0.0.1:6396          127.0.0.1:1026         CLOSE_WAIT          3404
    TCP    172.16.30.64:139        0.0.0.0:0              LISTENING           4
    UDP    0.0.0.0:445             *:*:                    4
    UDP    0.0.0.0:500             *:*:                    476
    UDP    0.0.0.0:1032            *:*:                    1584
    UDP    0.0.0.0:1071            *:*:                    216
    UDP    0.0.0.0:1169            *:*:                    1612
    UDP    0.0.0.0:1170            *:*:                    1612
    UDP    0.0.0.0:1215            *:*:                    1612
    UDP    0.0.0.0:1216            *:*:                    1612
    UDP    0.0.0.0:1217            *:*:                    1612
    UDP    0.0.0.0:1307            *:*:                    1612
    UDP    0.0.0.0:1310            *:*:                    1612
    UDP    0.0.0.0:1311            *:*:                    1612
    UDP    0.0.0.0:3848            *:*:                    216
    UDP    0.0.0.0:4000            *:*:                    1612
    UDP    0.0.0.0:4500            *:*:                    476
    UDP    0.0.0.0:4999            *:*:                    216
    UDP    0.0.0.0:5354            *:*:                    1584
    UDP    0.0.0.0:5357            *:*:                    1584
    UDP    127.0.0.1:123           *:*:                    920
    UDP    127.0.0.1:1336          *:*:                    1612
    UDP    127.0.0.1:2279          *:*:                    832
    UDP    127.0.0.1:5779          *:*:                    1284
    UDP    127.0.0.1:5963          *:*:                    3528
    UDP    172.16.30.64:123        *:*:                    920
    UDP    172.16.30.64:137        *:*:                    4
    UDP    172.16.30.64:138        *:*:                    4

C:\Documents and Settings\Administrator>
```

2.3 ARP 病毒的影响

实验目的：熟练掌握用 windows 的 ARP 网络命令操作本机的 ARP 信息。

实验环境：设备要求：装配 windows 2003 (XP 亦可，截图以 windows2003 为标准，下同) 操作系统的联网 PC 机若干台。

实验步骤：

除了端口对网络影响之外，病毒造成的网络故障也非常常见。造成网络故障的病毒也很多，这里我们选取一种有代表性，影响范围大的病毒作为分析。

近期国内很多单位和学校的局域网爆发名为“ARP 欺骗”木马病毒，病毒发作时其症状表现为计算机网络连接正常，但电脑主机频繁掉线或是断网，极大地影响了校园网用户的正常使用。

1 · 什么是 ARP

我们知道，当我们在浏览器里面输入网址时，DNS 服务器会自动把它解析为 IP 地址，浏览器实际上查找的是 IP 地址而不是网址。那么 IP 地址是如何转换为第二层物理地址（即 MAC 地址）的呢？在局域网中，这是通过 ARP 协议来完成的。

ARP 协议是“Address Resolution Protocol”（地址解析协议）的缩写，是一个重要的 TCP/IP 协议。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的 MAC 地址。但这个目标 MAC 地址是如何获得的呢？它就是通过地址解析协议获得的。所谓“地址解析”就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

【知识点】为什么要将 IP 转化成 MAC 呢？

简单的说，这是因为在 TCP 网络环境下，一个 IP 包走到哪里，要怎么走是靠路由表定义。但是，当 IP 包到达该网络后，哪台机器响应这个 IP 包却是靠该 IP 包中所包含的 MAC 地址来识别。也就是说，只有机器的 MAC 地址和该 IP 包中的 MAC 地址相同的机器才会应答这个 IP 包。因为在网络中，每一台主机都会有发送 IP 包的时候。所以，在每台主机的内存中，都有一个 ARP--> MAC 的转换表。通常是动态的转换表（注意在路由中，该 ARP 表可以被设置成静态）。也就是说，该对应表会被主机在需要的时候刷新。这是由于以太网在子网层上的传输是靠 48 位的 MAC 地址而决定的。

2 · ARP 命令介绍

使用 ARP 命令，我们能够查看本地计算机或另一台计算机的 ARP 高速缓存中的当前内容。此外，使用 ARP 命令，也可以用人工方式输入 MAC/IP 地址对，我们可能会使用这种方式为缺省网关和本地服务器等常用主机进行这项作，有助于减少网络上的信息量。

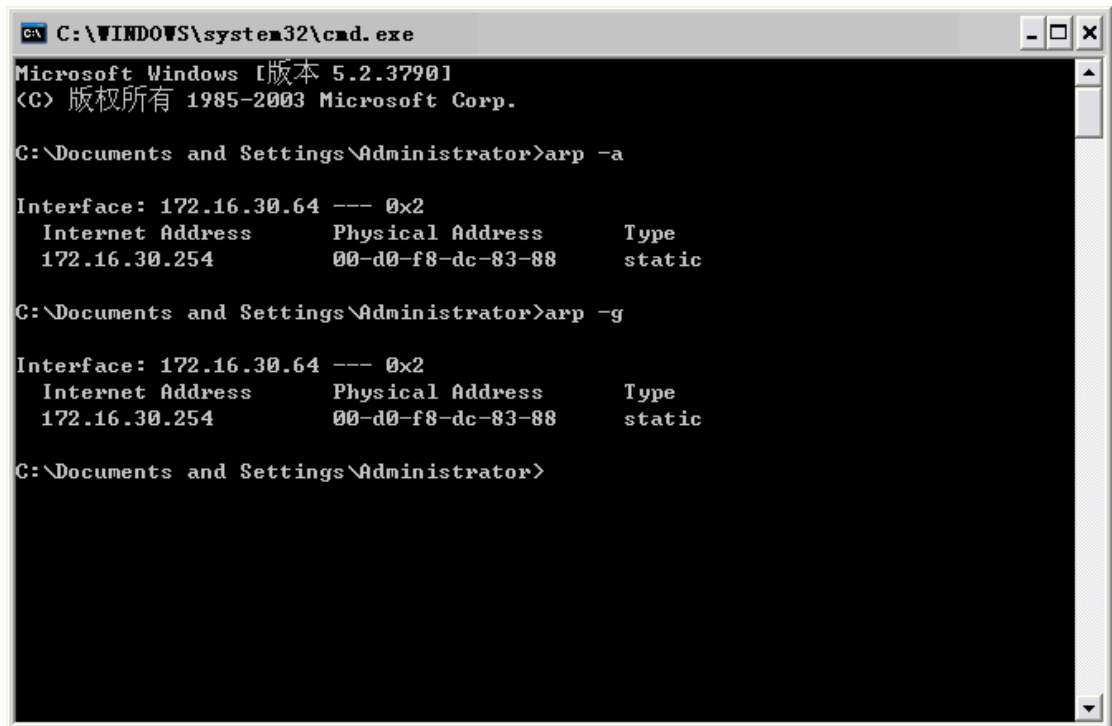
按照缺省设置，ARP 高速缓存中的表项是动态的，每当发送一个指定地点的数据报且高速缓存中不存在当前表项时，ARP 便会自动添加该表项。一旦高速缓存的表项被输入，它们就已经开始走向失效状态。例如，在 Windows 2003 网络中，如果输入表项后不进一步使用，MAC/IP 地址对就会在 2 至 10 分钟内失效。因此，如果 ARP 高速缓存中项目很少或根本没有时，请不要奇怪，通过另一台计算机或路由器的 ping 命令即可添加。所以，需要通过 ARP 命令查看高速缓存

中的内容时，请最好先 ping 此台计算机（不能是本机发送 ping 命令）。

ARP 常用命令选项（试验中 A 机的 IP 地址为：172.16.30.64，MAC 地址为：00-16-D3-CC-32-4B；B 机的 IP 为 172.16.30.86，MAC 地址为：00-04-61-7B-DD-2B）

1) ARP -a

用于查看高速缓存中的所有项目。-a 和 -g 参数的结果是一样的，多年来 -g 一直是 UNIX 平台上用来显示 ARP 高速缓存中所有项目的选项，而 Windows 用的是 ARP -a（-a 可被视为 all，即全部的意思），但它也可以接受比较传统的 -g 选项。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>arp -a

Interface: 172.16.30.64 --- 0x2
    Internet Address      Physical Address      Type
    172.16.30.254         00-d0-f8-dc-83-88    static

C:\Documents and Settings\Administrator>arp -g

Interface: 172.16.30.64 --- 0x2
    Internet Address      Physical Address      Type
    172.16.30.254         00-d0-f8-dc-83-88    static

C:\Documents and Settings\Administrator>
```

2) 添加 ARP 表项

动态表项

通过 B 机 ping A 机的 IP 地址，可以在 A 机器的高速缓存中添加 B 机的 IP 地址与 MAC 地址的映射关系加入到 A 机的 ARP 表中，图中显示 B 机使用“ping 172.16.30.64”之后，在 A 机中使用“arp-a”ARP 表项变化情况，请注意 Type 显示为：dynamic（动态）

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>arp -a

Interface: 172.16.30.64 --- 0x2
    Internet Address      Physical Address      Type
    172.16.30.86          00-04-61-7b-dd-2b    dynamic
    172.16.30.254         00-d0-f8-dc-83-88    static

C:\Documents and Settings\Administrator>_
```

静态添加

存储在 ARP 高速缓存中的 ARP 表，既可以有动态表项，也可以有静态表项。通过 ARP -s IP 物理地址，可以向 ARP 高速缓存中人工输入一个静态表项。该表项在计算机系统不会自动将它从 ARP 表中删除，知道人为删除或关机。如图所示，请注意与上图动态添加表项相比 Type 显示为：static（静态）

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

C:\Documents and Settings\Administrator>arp -s 172.16.30.86 00-04-61-7b-dd-2b

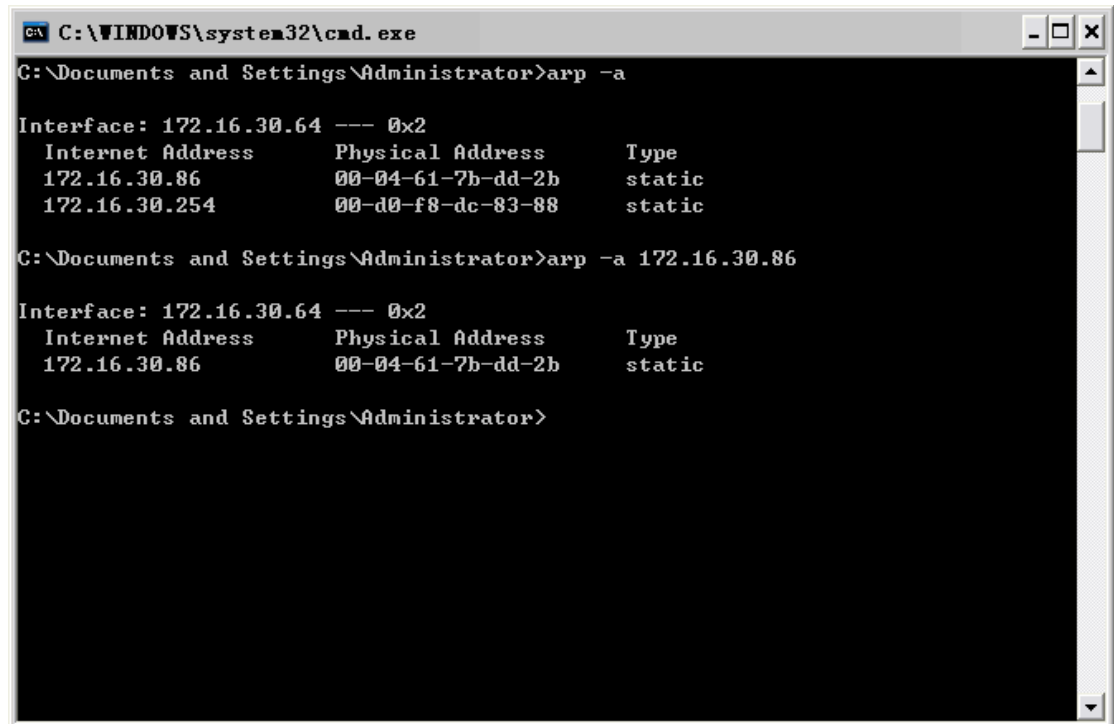
C:\Documents and Settings\Administrator>arp -a

Interface: 172.16.30.64 --- 0x2
    Internet Address      Physical Address      Type
    172.16.30.86          00-04-61-7b-dd-2b    static
    172.16.30.254         00-d0-f8-dc-83-88    static

C:\Documents and Settings\Administrator>_
```


3) ARP -a IP

如果我们有多个网卡，那么使用 ARP -a 加上接口的 IP 地址，就可以只显示与该接口相关的 ARP 缓存项目。



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>arp -a

Interface: 172.16.30.64 --- 0x2
    Internet Address      Physical Address        Type
    172.16.30.86          00-04-61-7b-dd-2b      static
    172.16.30.254         00-d0-f8-dc-83-88      static

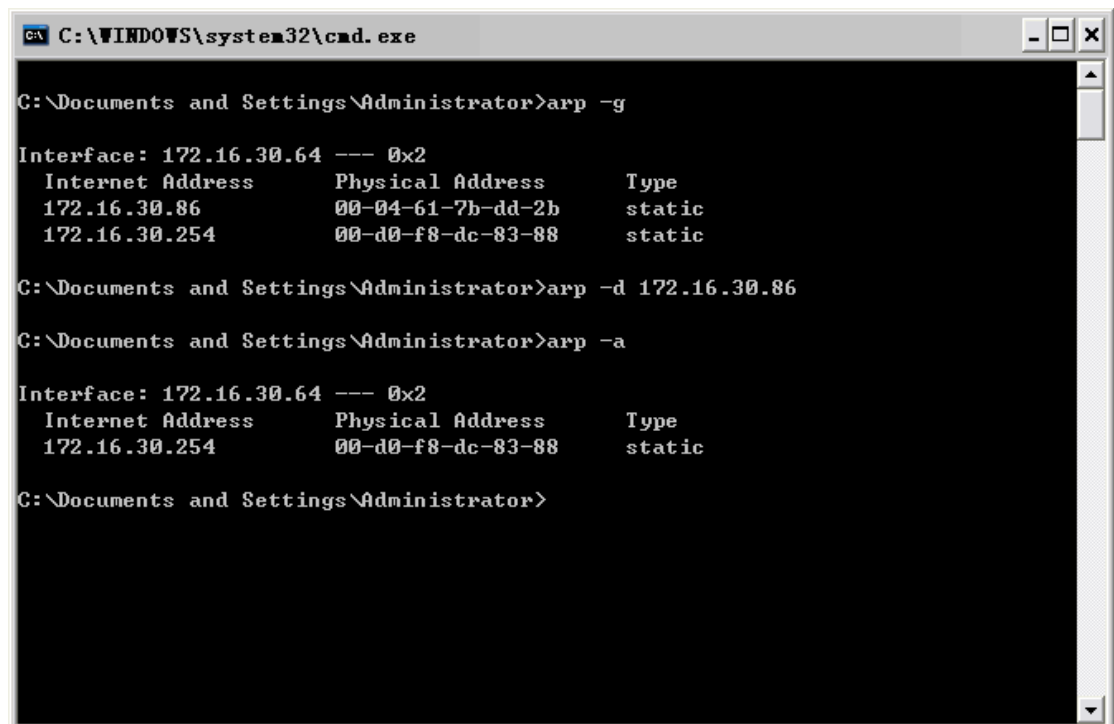
C:\Documents and Settings\Administrator>arp -a 172.16.30.86

Interface: 172.16.30.64 --- 0x2
    Internet Address      Physical Address        Type
    172.16.30.86          00-04-61-7b-dd-2b      static

C:\Documents and Settings\Administrator>
```

4) ARP -d IP

无论是动态表项还是静态表项，都可以通过 ARP -d IP 命令删除。如果要删除 ARP 表中所有的表项，也可以使用“*”代替具体的 IP 地址。



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>arp -g

Interface: 172.16.30.64 --- 0x2
    Internet Address      Physical Address        Type
    172.16.30.86          00-04-61-7b-dd-2b      static
    172.16.30.254         00-d0-f8-dc-83-88      static

C:\Documents and Settings\Administrator>arp -d 172.16.30.86

C:\Documents and Settings\Administrator>arp -a

Interface: 172.16.30.64 --- 0x2
    Internet Address      Physical Address        Type
    172.16.30.254         00-d0-f8-dc-83-88      static

C:\Documents and Settings\Administrator>
```

3 · 什么是 ARP 攻击

当初 ARP 方式的设计没有考虑到过多的安全问题。给 ARP 留下很多的隐患，ARP 欺骗就是其中一个例子。

网内的任何一台机器都可以轻松的发送 ARP 广播，来宣称自己的 IP 和自己的 MAC。这样收到的机器都会在自己的 ARP 表格中建立一个他的 ARP 项，记录他的 IP 和 MAC 地址。即使这个广播是错误的其他机器也会接受，这样就造成网络不能进行正常的网络通信。

例如：B 机本来的 IP 地址为 172.16.30.86，MAC 是：00-04-61-7B-DD-2B，但它却在内网广播自己的 IP 地址为：172.16.30.254(路由器的 IP)，MAC 地址是 00-04-61-7B-DD-2B（B 机的 MAC 地址）。这样大家会把发给路由器 172.16.30.254 的信息(信息必须通过路由器转发)，便发给 00-04-61-7B-DD-2B，也就是 172.16.30.86。

简单来说：在没有 ARP 欺骗之前，数据流向是这样的：网关<->本机。ARP 欺骗之后，数据流向是这样的：网关<->攻击者（“伪网关”）<->本机，本机与网关之间的所有通讯数据都将流经攻击者（“伪网关”）。因为这种攻击是利用 ARP 请求报文进行“欺骗”的，所以防火墙会误以为是正常的请求数据包，不予拦截。因此普通的防火墙很难抵挡这种攻击。

从影响网络连接通畅的方式来看，ARP 欺骗有两种攻击可能，一种是对路由器 ARP 表的欺骗（可导致此起彼伏的瞬间掉线或大面积的网络中断的症状）；另一种是对内网电脑 ARP 表的欺骗（主动攻击具体某台机，不断弹出“本机的 XXX 段硬件地址与网络中的 XXX 段地址冲突”的对话框，达到窃取信息的目的），当然也可能两种攻击同时进行。不管怎么样，欺骗发送后，电脑和路由器之间发送的数据可能就被送到错误的 MAC 地址上，从表面上来看，就是“上不了网”，“访问不了路由器”，“路由器死机了”，因为一重启路由器，ARP 表会重建正确的对应关系，如果 ARP 攻击不是一直存在，就会表现为网络正常，所以网络管理员会觉得是路由器“死机”了，而不会想到其他原因。为此，宽带路由器背了不少“黑锅”，但实际上应该 ARP 协议本身的问题。

4 · 防范 ARP 攻击

当我们了解了 ARP 攻击的原理之后，我们就可以彻底解决局域网的 ARP 攻击。

1) 双向绑定

现在最常用的基本对治方法是“ARP 双向绑定”。

所谓“双向绑定”，就是再路由器上绑定 ARP 表的同时，在每台电脑上也绑定一些路由器（网关）的 MAC 地址表项。

在 PC 上绑定路由器（网关）的 IP 和 MAC 地址

当获取到正确的路由器（网关）的 IP 和 MAC 地址之后，可以采用“arp -s”静态的添加到每台计算机 ARP 缓存表中，当每次计算机重启之后，都需要重新添加。我们可以写一个批处理文件，让计算机每次重启自动加载，这样的小软件，网上也很多。

【试一试】建议搜索关键字：“arp 攻击 批处理”

在路由器上绑定用户主机的 IP 和 MAC 地址

基本上路由器软件版本都支持：一般是在路由器管理界面--高级配置--用户管理中将局域网每台主机均作绑定。

“ARP 双向绑定”能够防御轻微的、手段不高明的 ARP 攻击。ARP 攻击程序如果没有试图去更改绑定的 ARP 表项，那么 ARP 攻击就不会成功；如果攻击手段不剧烈，也欺骗不了路由器，这样我们就能够防住 50%ARP 攻击。

2) ARP 防火墙

在现在 ARP 双向绑定流行起来之后，攻击程序的作者也提高了攻击手段，攻击的方法更综合，另外攻击非常频密，仅仅进行双向绑定已经不能够应付凶狠的 ARP 攻击了，仍然很容易出现掉线。

于是很多防火墙专门增加了“ARP 攻击主动防御”功能。原理是：当网内受到错误的 ARP 广播包攻击时，防火墙立即广播正确的 ARP 包去修正和消除攻击包的影响。这样就解决了掉线的问题，但是在最凶悍的 ARP 攻击发生时，仍然发生了问题----当 ARP 攻击很频密的时候，就需要防火墙发送更频密的正确包去消除影响。虽然不掉线了，但是却给网络带来了一些负载，出现了上网“卡”的问题。

所以，依靠“ARP 攻击主动防御”，也只能够解决 80%的问题。为了彻底消除 ARP 攻击，在此基础上有增加了“ARP 攻击源攻击跟踪”的功能。对于剩下的强悍的 ARP 攻击，采用“日志”功能，提供信息方便用户跟踪攻击源，这样用户通过临时切断攻击电脑或者封杀发出攻击的程序，根本能够解决问题。

.3 课后总结

.3.1 Ping 命令为什么可以检查网络故障

PING 命令是 OSI / RM 开放体系结构的最高层即应用层的命令。全称是 Packet Inter Net Groper 分组网间探测。但它实际的原理是：使用的是 OSI / RM 开放体系结构的第三层即网络层的 ICMP 协议中的回送请求与回送回答报文的这个功能达到检查网络故障的目的。

统计发送到哪个机器（IP 地址），发送的、收到的和丢失的分组数。往返时间的最小值、最大值和平均值。

.3.2 端口的范围以及分类

理论上，一个 IP 的端口范围可以从 1~65535 之间都可以使用。这些端口可细分为：

公认端口（0 到 1023）紧密绑定（binding）于一些 TCP/IP 的系统服务。

注册端口（从 1024 到 49151）松散地绑定于一些服务。也就是说有许多服务绑定于这些端口，这些端口同样用于许多其它目的。

动态或私有端口（从 49152 到 65535）留给客户网络进程暂时使用的端口范围。

.3.3 ARP 病毒的原理

ARP 是主机在发送数据包前将目标主机 IP 地址转换成目标主机 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

这时就涉及到一个问题，一个局域网中的电脑少则几台，多则上百台，这么多的电脑之间，如何能准确的记住对方电脑网卡的 MAC 地址，以便数据的发送呢？这就涉及到了另外一个概念，ARP 缓存表。

在局域网的任何一台主机中，都有一个 ARP 缓存表，该表中保存这网络中各个电脑的 IP 地址和 MAC 地址的对照关系。当这台主机向同局域网中另外的主机发送数据的时候，会根据 ARP 缓存表里的对应关系进行发送。

局域网内的主机如果需要访问网络，则必须借助网关转发数据。网关其实也可以看做一台主机，同样也有 IP 地址和 MAC 地址，如果别有用心的主机想截取该网络中所有需要上网的主机的信息，那么它可以伪装成网关的 MAC 地址，因为网内的任何一台机器都可以轻松的发送 ARP 广播，来宣称自己的 IP 和自己的 MAC（即使它是错误的对应关系），然后自己在连上网关，那么其他主机需要上网则需要先经过它，以此达到窃取信息的目的。

了解原理之后，解决方便也很简单，局域网的主机上网前将自己的 MAC 地址和网关的 MAC 地址绑定即可。

.4 思考讨论

.4.1 既然在网络链路上传送的帧最终是按照硬件地址（MAC 地址）找到目的主机的，那么为什么我们不直接使用 MAC 地址进行通信，而是要使用抽象的 IP 地址并调用 ARP 来寻找出相应的硬件地址呢？

由于全世界存在各式各样的网络，它们使用不同的硬件地址。要使用这些异构网络能够互相通信就必须进行非常复杂的硬件地址转换工作，因此由用户或用户主机来完成这项工作几乎是不可能的事。但统一的 IP 地址把这个复杂的问题解决了。连接到因特网的主机只需要拥有统一的 IP 地址，它们之间的通信就像连接在同一个网络上那样简单方便，因为上述的调用 ARP 的复杂过程都是由计算机软件自动进行的，对用户来说看不见这种调用过程的。

因此，在虚拟的 IP 网络上用 IP 地址进行通信给广大的计算机用户带来很大的方便。

.4.2 【扩展搜索】

操作系统（无论是 windows 还是 Linux）的端口不光只是上面罗列常用端口，有兴趣的读者可以通过搜索引擎了解一下端口的作用。建议搜索关键字“操作系统 端口”

