### 一、显示和修改本地ARP列表——ARP

ARP（Address Resolution Protocol）是负责将IP地址解析成MAC地址的协议，对于网络中的高层应用程序，网络主机之间的通讯是靠IP地址来完成，但在TCP/IP协议的最低层，主机之间的信息交换则是通过MAC地址来定位的。每台装有网卡的主机中都有一个ARP表，保存着同一网络中IP到MAC之间的映射记录。ARP表并不是一成不变的，大约每2分钟更新一`次，这种纪录称为动态式（Dyanmi）记录。还有一种称为静态记录，也就是表中的记录不变，直到TCP/IP协议重启后才会消失。

ARP命令用于显示和修改“地址解析协议（ARP）”缓存中的项目。ARP缓存中包含一个或多个表，它们用于存储IP地址及其经过解析的以太网或令牌环网络适配器的物理地址。计算机上安装的每一个以太网或令牌环网络适配器都有自己单独的表。ARP命令可以对这个表中的记录进行添加和修改，实现对ARP表的维护。如果使用ARP命令时不带参数，则显示帮助信息。

实例1： 要查看本机的ARP表，可以在命令提示符下键入如下命令：

ARP –a

回车，命令运行结果显示如图1所示。

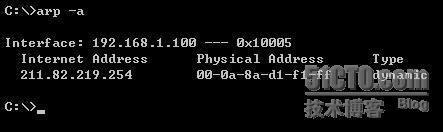


图1

这就是当前本机的ARP表中的记录，也就是近一段时间内与本机通讯的主机。如图中所示，Internet Address显示的是IP地址，而Physical Address显示的是该IP地址所对应的MAC地址。Type说明该记录是动态记录。

实例2：添加将IP地址192.168.0.9解析成物理地址00-50-BA-25-96-00的静态ARP缓存项。在命令提示符下，键入如下命令：

arp -s 192.168.0.9 00-50-BA-25-96-00

回车执行该命令，该静态项即添加完毕。然后执行arp -a命令查询ARP表，显示如图14所示的记录。

|  |
| --- |
| 动态记录 |

|  |
| --- |
| 静态记录 |

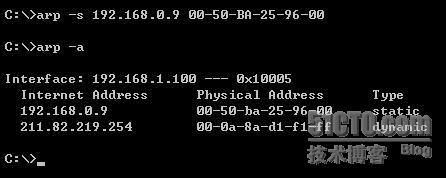


图2

ARP在添加静态记录之前，必须有一个MAC寻址的过程。当一个TCP/IP的包要发出时，会先查看本机ARP表中的记录是否有该IP的记录。如果有，则直接转换成该IP对应的MAC，如果没有，则将发一个ARP Request广播封包向对方查询MAC地址，这个广播包会被同一子网内的所有主机收到，但只有与该IP相同的主机接收，并回答一个ARP APPLY封包，该包有相应IP与MAC的信息，这样就可以找到相应的主机的MAC地址。

在ARP表中的记录一般是动态的，大约每2分钟刷新一次。如果本地主机有频繁的IP要访问时，比如网关、代理服务器、路由器等，为了减少发ARP Request广播包，可以在ARP表中创建静态记录。

### 二、查看网络配置信息命令——Ipconfig和Winipcfg

Ipconfig命令用于显示本地网卡的IP地址，使用该命令，可以查看当前所有的TCP/IP网络配置值、刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。该命令只能在Windows 98/Me/2000/XP的命令行窗口中运行，而不能在实模式DOS环境、或者Windows 2000/XP的故障恢复控制台下运行。而且Windows 98/Me与Windows 2000/XP系统下的Ipconfig命令之间也存在着一定的区别，下面分别以Windows XP和Windows 98为例进行比较和介绍。

通常，用户需要查看的仅仅是IP地址信息，使用不带参数的Ipconfig就可以显示所有适配器的 IP 地址、子网掩码和默认网关。在命令提示符下键入如下命令：

Ipconfig

回车，会显示如图3所示运行结果。

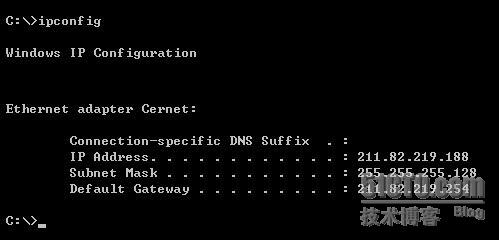


图3

该命令还可以查看主机的相关配置信息，如主机名、DNS服务器、节点类型、网络适配置器的物理地址等。其中网络适配器的物理地址在检测网络错误时非常有用，而且在远程唤醒网络上的某台计算机时，也必须先知道该计算机网卡的物理地址，即网卡的Mac地址。由于每个网卡的Mac地址是全球唯一的，这样就能很准确的定位到要唤醒的计算机。在Windows XP的命令提示符下，键入如下命令：

ipconfig /all

然后回车，运行结果显示如图4所示。

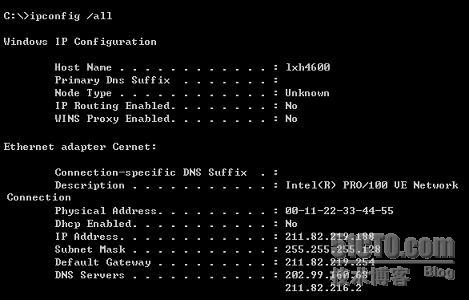


图4

在Windows98下执行Ipconfig /all命令的结果和Windows XP下略有不同。在Windows98下的执行结果显示如图5所示。

|  |
| --- |
| 配置信息有效期 |



图5

另外，在Windows 98/95操作系统中，查看网络配置信息还可以使用Winipcfg命令，执行后提供图形化界面。在Windows 98/95的MS-DOS窗口中键入如下命令：

Winipcfg

回车运行，显示如图6所示“IP配置”对话框，可以看到本机的网络配置信息。

|  |
| --- |
| 单击此处，可查看不同网络适配器的配置信息 |



图6

如果单击“详细信息”按钮，还可以查看有关主机信息、DNS服务器信息等，显示如图7所示对话框。



图7

### 三、显示NetBIOS协议的统计资料命令——Nbtstat

Nbtstat命令是Windows下自带的NetBIOS管理工具，用于显示本地计算机和远程计算机的基于TCP/IP协议的NetBIOS统计资料、NetBIOS名称表和NetBIOS名称缓存。Nbtstat可以刷新NetBIOS名称缓存和注册的Windows Internet名称服务（WINS）名称。如果使用不带参数的Nbtstat命令，将会显示有关该命令的帮助信息。

而NetBIOS（Network Basic Input Output System，网络基本输入输出系统），是局域网 (LAN) 上的程序可以使用的应用程序编程接口（API），几乎所有的局域网计算机都是在NetBIOS基础上工作的。NetBIOS为程序提供了请求低级服务的统一的命令集，这些服务是管理名称、执行会话和在网络节点之间发送数据报所要求的。

实例1：如果要显示计算机名为liusm的远程计算机的NetBIOS名称表，在命令提示符下键入下面命令：

nbtstat -a liusm

回车运行后的执行结果显示如图8所示。

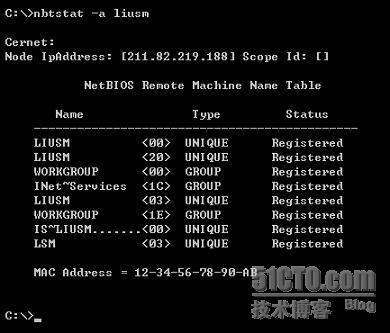


图8

由此可以知道，计算机名为liusm的远程计算机属于MSHOME工作组，同时能获得远程计算机的网络适配器的MAC地址（12-34-56-78-90-AB）。

实例2：显示IP地址为211.82.219.211的远程计算机的MAC地址和NetBIOS名称表，可以在命令提示符下键入如下命令行：

nbtstat -a 211.82.219.211

回车运行后的结果显示如图9所示。



图9

该命令的作用和实例1中的命令作用相同，这里不再赘述。

实例3：显示本地计算机的NetBIOS名称表，可以在命令提示符下键入如下命令：

nbtstat -n

回车，运行后的结果显示如图10所示。



图10

从执行结果中可以得知该计算机的NetBIOS名、所在域（或工作组）以及当前登录的用户等信息。

实例4：显示本地计算机NetBIOS名称缓存的内容，在命令提示符下键入如下命令：

nbtstat -c

回车运行后的结果显示如图11所示。

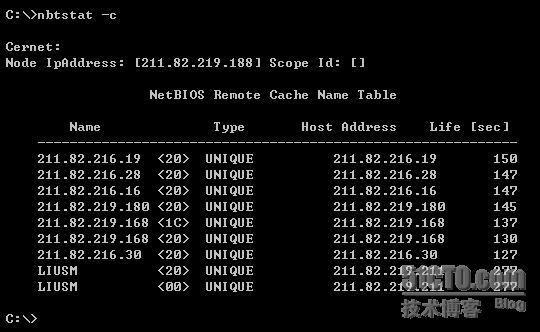


图11

从上面的运行结果中可以看出，本地计算机曾经与211.82.216.x和211.82.219.x网段的计算机连接过。因为NetBIOS的缓存里储存的IP是对方已经信任你的计算机IP，因而这也给网络安全带来了隐患。

### 四、显示网络连接信息——Netstat

在服务器与网络的管理中，需要经常查看服务器所开放的端口、当前的所有连接，以便随时了解网络状态。这时就要用Netstat命令。该命令可以让管理员轻松查看计算机系统服务是否正常，是否被“黑客”留下后门、木马等。Netstat同时也是一个实时的入侵检测工具，可以随时查看是否有不正常的连接。

Netstat命令用于显示活动的TCP连接、计算机侦听的端口、以太网统计信息、IP路由表、IPv4统计信息（对于IP、ICMP、TCP和UDP协议）。使用时如果不带任何参数，Netstat命令将显示活动的TCP连接。

实例1：显示本机所有活动的TCP连接以及计算机侦听的TCP和UDP端口。

在命令提示符下键入如下命令：

Netstat –a

回车，运行后的结果显示如图12所示：



图12

从运行结果可以知道计算机当前开放的TCP和UDP端口，并与蠕虫病毒和黑客程序的端口相对照，确认是否感染病毒或被恶意攻击。

实例2：显示当前活动的TCP/IP连接

在命令提示符下键入如下命令：

Netstat -n 或者 Netstat（不带任何参数）

回车，运行后的结果显示如图13所示：



图13

该图中显示计算机的当前连接情况，来访者的IP与连接端口一览无遗。该命令与使用-a参数不同的是，这里只以IP的形式来表示当前的所有连接，而不解析对方的NetBIOS名字。

实例3：显示以太网统计信息和所有协议的统计信息

在命令提示符下键入如下命令：

Netstat -s-e

回车，运行后的结果显示如图14所示。



图14

实例4：检查路由表确定路由配置情况

在命令提示符下键入如下命令，

Netstat -rn

回车，运行后的结果显示如图15所示。



图15

### 五、洞悉网络连通测试命令——Ping

在网络中，经常会出现网络不通等问题，这就需要网络管理员来检查并排除网络故障，包括检查网络配置信息，检查硬件连接，使用网络命令测试等，而在命令检测中，用得最多的就是Ping命令了。

Ping是使用最频繁的网络测试命令，主要用于确定网络的连通性。Ping程序使用ICMP协议来简单地发送一个网络包并请求应答，接收请求的目标主机再次使用ICMP返回与接收的数据一样的数据包，于是Ping便可根据每个包发送和接收报告的往返时间，报告无响应包的百分比，这可以判断网络是否正确连接，以及网络连接的状况（丢包率）。

#### 1. Ping命令的应用

Ping是Windows操作系统集成的TCP/IP应用程序之一，通常在命令提示符下运行。利用Ping命令可以有效地测试网络连通故障，并可确定网络故障发生的大致原因，下面就来看看该命令的简单应用。

##### （1）Ping本地地址或127.0.0.1

Ping本地计算机的IP地址或127.0.0.1，可以确认：

l         该计算机是否正确安装了网卡。如果测试不成功，应当在“设备管理器”中查看网卡是否有黄色的“！”。如果有，则删除该网卡或重新正确安装。如果没有，说明网卡安装正确。

l         该计算机是否正确安装了TCP/IP协议。如果测试不成功，应打开控制面板的“网络”属性查看是否安装TCP/IP协议。如果没有，则需安装TCP/IP协议并正确配置后，重新启动计算机并再次测试。如果已经安装，继续向下检查。

l         该计算机是否正确配置了IP地址和子网掩码。如果测试不成功，应打开控制面板的“网络”属性查看IP地址和子网掩码是否设置正确。如果不正确，需重新设置，重新启动计算机并再次测试。

##### （2）Ping同一VLAN中其它计算机的地址

Ping同一VLAN中其他计算机的地址，可以确认：

l         IP地址、子网掩码的设置是否正确。如果测试不成功，应打开控制面板的“网络”属性查看IP地址和子网掩码是否设置正确。如果设置不正确，需重新设置，重新启动计算机并再次测试。如果设置正确，继续向下检查。

l         网络连接是否正常。如果测试不成功，应当对网络设备和通讯介质逐段测试、检查和排除。

##### （3）Ping Internet中远程主机的地址

Ping Internet中远程主机的地址，可以确认：

l         网关的设置是否正确。如果测试不成功，应打开控制面板的“网络”属性查看默认网关设置是否正确。如果不正确，需重新设置，然后重新启动计算机并再次测试。如果设置正确，继续向下检查。

l         域名服务器设置是否正常。如果使用域名测试不成功，应打开控制面板的“网络”属性查看域名服务器（DNS）设置是否正确。如果正确，继续向下检查。

l         路由器的配置是否正确。如果该计算机被加入到禁止出站访问的IP控制列表中，那么，该用户将无法访问Internet。

l         Internet连接是否正常。如果到任何一个主机的连接都超时，或丢包率都非常高，则应当与ISP共同检查Internet连接，包括线路、Modem和路由器设置等诸多方面。

#### 2. 常见的出错信息

常见的出错信息通常分为四种情况：

● unknown host

unknown host（不知名主机）表示该远程主机名不能被命名服务器转换成IP地址。故障原因可能是命名服务器有故障，或者其名称不正确，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。

● Network unreachable

Network unreachable（网络不能到达）表示本地系统没有到达远程系统的路由，可用netstat –rn命令检查路由表来确定路由配置情况。

● No answer

No answer（无响应），远程系统没有响应。这种说明本地系统有一条到达远程主机的路由，但却接受不到它发给该远程主机的任何分组报文。故障原因可能是远程主机没有工作，或本地或远程主机网络配置不正确，或本地或远程的路由器没有工作，或通信线路有故障，或远程主机存在路由选择问题。

● timed out

timed out（超时），表示与远程主机的链接超时，数据包全部丢失。故障原因可能是到路由器的连接问题、路由器不能通过、也可能是远程主机已经当机。

#### 3. 应用实例

在“Ping命令的应用”一节，详细介绍了Ping命令的应用，当出现网络故障时，通常就是使用所介绍的顺序进行网络故障诊断与排除；在出现的Ping的结果中，分析网络的连通性，找出故障所在，从而在故障排除过程中做到有的放矢。下面就Ping命令的实际应用列举几个简单的例子。

实例1：以下范例显示Ping的输出：

在命令提示符下键入如下命令：

Ping [url]www.coolpen.org[/url]

回车执行，如果显示如图16所示的运行结果，则表明连接正常，所有发送的包均被成功接收，丢包率为0。

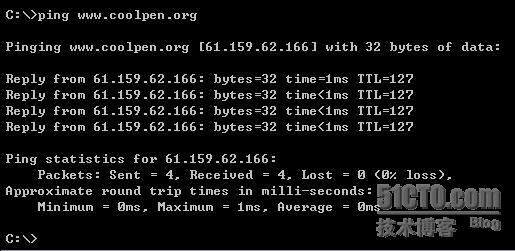


图16

这里对测试结果中的一些数据作简单解释：

Pinging [url]www.coolpen.org[/url] [61.159.62.166] with 32 bytes of data

这里的“32 bytes”中的“32”指的是发送的消息，及回响的消息数据字段值为32字节。

Reply from 61.159.62.166: bytes=32 time=44ms TTL=113

这里的“44ms”，指的是从发送数据到收到回响所经历的时间，该时间值一般有一定限制，当相应时间超过4000ms（即4s）时，将显示连接超时。

“TTL=113”，这里的TTL值默认为对方主机的TTL值，根据TTL值一般可以确定该计算机使用哪种操作系统。对于使用Windows XP/2000的计算机，该值一般为128；Windows 98计算机的TTL值一般为64，Unix计算机机的TTL值一般为255。不过在注册表中可以随意改变TTL值，所以利用该值来确定主机的操作系统并不一定准确。

如果执行如下命令：

Ping [url]www.coolpen.com[/url]

显示如图17所示测试消息，则表明网络连接不正常，或对方对ICMP包作了过滤，因此，所有发送的包均未被成功接收，丢包率为100%，目的主机不可到达。



图17

实例2：如果网络Ping不通，在设备或线路调试期间，可以使用“-t”参数一直进行测试。只要按下“Ctrl-C”组合键中止该命令为止。

Ping -t [url]www.coolpen.net[/url]

回车运行，命令执行结果显示如图18所示。



图18

实例3：

若欲测试代理服务器或路由器的性能，可以使用大字段的消息值，从而增加网络流量。需要注意的是，“数据”字段长度（以字节表示）默认值为 32，指定的数据包不能大于65527。

Ping –l 1024 [[url]www.coolpen.net[/url]](http://www.coolpen.net/" \t "http://blog.csdn.net/xumin07061133/article/details/_blank)

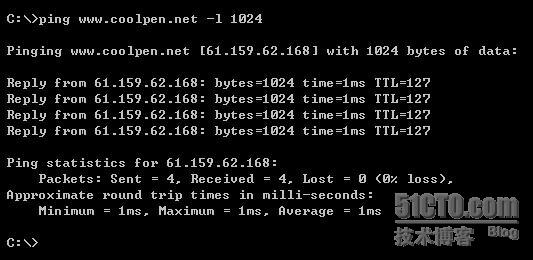


图19

实例3：验证到某个IP地址或域名的的连通性，并记录所经过的路由。该命令在使用上与tracert有类似之处，都可以追踪路由。

在命令提示符下，执行如下命令：

Ping -r 4 [url]www.hengshui.com[/url]

[可测试与](http://www.coolpen.net/" \t "http://blog.csdn.net/xumin07061133/article/details/_blank)[[url]www.hengshui.com[/url]的连通性，并记录所经过的4个路由。需要注意的是，最多可以记录9个路由。](http://www.hengshui.com/" \t "http://blog.csdn.net/xumin07061133/article/details/_blank)

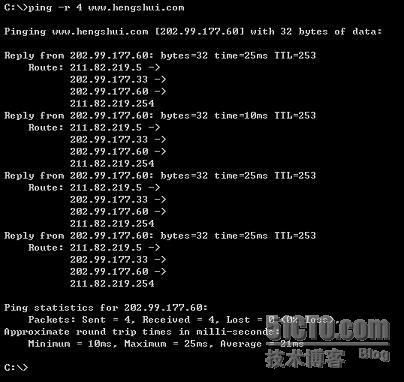


图20

### 六、数据包跟踪诊断——Tracert

当数据报从本地计算机经过多个网关传送到目的地时，它会寻找一条具体路径来传送，每次传送数据报，不能保证或认为总遵循唯一的一条路经。那么如何知道发送的数据报所经过的路径呢？这时就要用到Tracert命令。Tracert命令同样是内置于Windows的TCP/IP应用程序之一，可以对IP地址或URL进行相应的域名转换。Tracert一般用来检测故障的位置，通过追踪路由，可以判断发生故障的路由设备或网关，以及发生故障的区段，从而便于查找和排除故障。

Tracert诊断实用程序将包含不同生存时间（TTL）值的Internet消息控制协议（ICMP）回显数据包发送到目标，以决定到达目标使用的路由。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达到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返回的“ICMP 已超时”的消息来确定路由。不过，有些路由器下传包含过期TTL值的数据包，而Tracert看不到。

实例1：追踪到[url]www.hengshui.com[/url]的路由，测试局域网络和Internet连接是否正常，以及导致故障发生的路由器的位置。

在命令提示符下执行如下命令行：

Tracert [url]www.hengshui.com[/url]

命令执行结果显示如图21所示，从运行结果可知，局域网络和Internet连接均正常。



图21

### 七、显示和修改本地路由表命令——Route

大多数主机都驻留在只连接一台路由器的网段上，因此不存在使用哪一台路由器将数据报发表到远程计算机上的问题，该路由器的IP地址即是该网段上所有计算机的缺省网关。但是，当网络上拥有两个或多个路由器时，就不一定只依赖缺省网关了。可以让某些远程IP地址通过某个特定的路由器来传递，而其他的远程IP通过另一个路由器来传递。这时，需要相应的路由信息，这些信息储存在路由表中，每个主机和每个路由器都配有自己独一无二的路由表。大多数路由器使用专门的路由协议来交换和动态更新路由器之间的路由表。但在有些情况下，必须手动将项目添加到路由器和主机上的路由表中。这时就要用到Route命令，它用来显示、人工添加和修改路由表项目。

如果要查看Route命令的帮助信息，可在命令提示符下运行不带任何参数的Route命令。

下面就通过几个简单的实例，来具体看一看Route命令的简单应用。

实例1：显示路由表中的当前项目

在命令提示符下，键入如下命令行：

Route print

回车，命令的执行结果显示如图22所示。

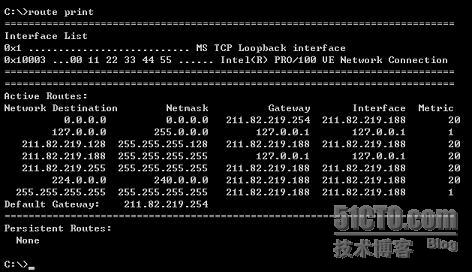


图22

由于用IP地址配置了网卡，因此所有的这些项目都是自动添加的。

实例2：显示IP路由表中以211开始的路由

在命令提示符下键入如下命令：

Route print 211.\*

回车，运行结果显示如图23所示。

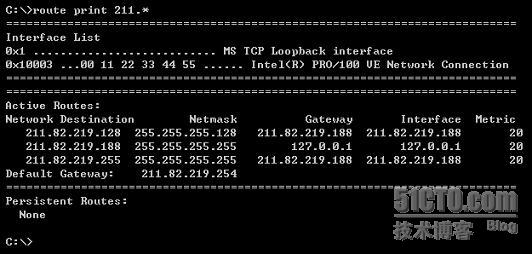


图23

实例3：利用route可以在计算机中设置多个默认网关。例如，对192.168.0.0网段的访问使用192.168.0.1网关，对其他网段的访问则使用192.168.1.1网关。那么，可以执行以下命令：

route add 192.168.0.0 mask 255.255.255.0 192.168.0.1

route add 0.0.0.0 mask 0.0.0.0 192.168.1.1