9.2 实验 1：查看网卡的 MAC 地址

计算机是硬件和软件的集合体，网络也不例外。那么首先，我们就从构成网络的硬件开始探索吧。在组建公司内部的网络时，笔者购买了如下 4 种硬件：1. 安装到每台计算机上的网卡（NIC，Network Interface Card）；2. 插到网卡上的网线；3. 把网线汇集起来连接到一处的集线器；4. 用于接入到互联网的路由器。需要注意的是这些硬件的规格只有相互匹配了才能连接在一起。网卡选择的是规格极其普通的以太网（Ethernet）网卡。因为现在以太网已经成为了主流的选择，所以也就无需再考虑其他方案了。网卡的种类一旦确定下来，网线、集线器和路由器的规格也就确定了。既然硬件的规格一致了，就意味着其中传输的电信号的形式也是一致的。这样的话无论是 Linux 的计算机，还是 Windows 的计算机，它们在硬件上已经是连通的了。

以太网使用了一种略显粗糙的方法连接 LAN 内的计算机（如图 9.2 所示）。以太网中的每台计算机都需要先确认一件事：在网线上有没有其他的计算机正在传输电信号，也就是说要先确保没有人在占用网络，然后才能发送自己想传输的电信号。谁先抢到了网线的使用权，谁就先发送。万一遇到了多台计算机同时都想发送电信号的情况，只需要让这些计算机等待一段长度随机的时间后再重新发送相同的电信号即可。这套机制叫作 CSMA/CD（Career Sense Multiple Access with Collision Detection，带冲突检测的载波监听多路访问）。所谓载波监听（Career Sense），指的是这套机制会去监听（Sense）表示网络是否正在使用的电信号（Career）。而多路复用（Multiple Access）指的是多个（Multiple）设备可以同时访问（Access）传输介质。带冲突检测（with Collision Detection）则表示这套机制会去检测（Detection）因同一时刻

的传输而导致的电信号冲突（Collision）。在小规模的 LAN 中，像这样略显粗躁的 CSMA/CD 机制是可以正常运转的。因为 CSMA/CD 归根结底也只是一种适用于 LAN 的机制。

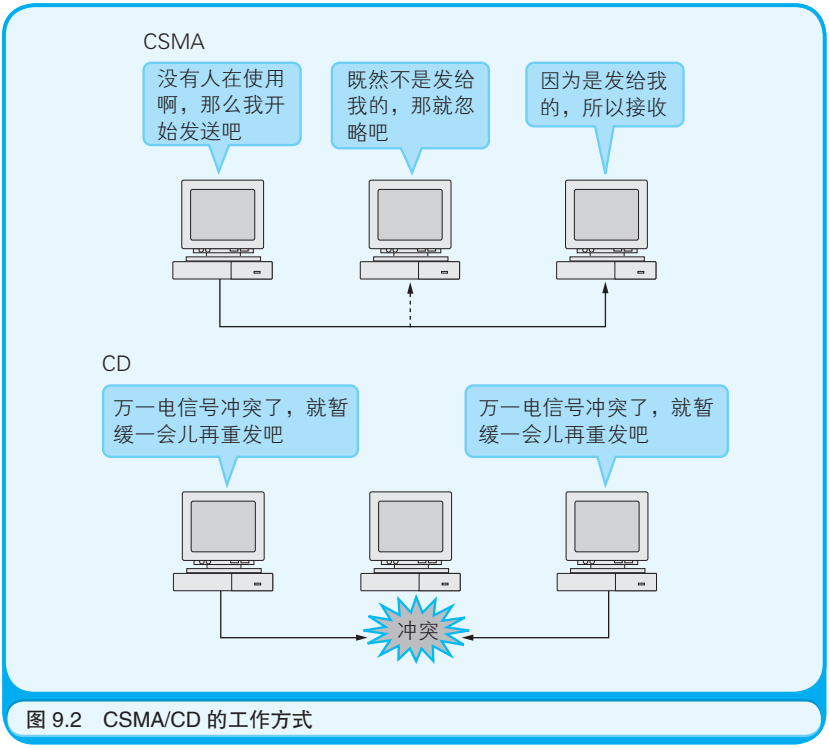

图 9.2　CSMA/CD 的工作方式

在以太网中，发送给一台计算机的电信号也可以被其他所有的计算机收到。一台计算机收到了电信号以后会先做判断，如果是发送给自己的则选择接收，反之则选择忽略。可以用被称作 MAC（Media Access Control）地址的编号来指定电信号的接收者。在每一块网卡所带有的 ROM（Read Only Memory，只读存储器）中，都预先烧录了一个唯一的 MAC 地址。网卡的制造厂商负责确定这个 MAC 地址是什

么。因为 MAC 地址是由制造厂商的编号和产品编号两部分组成的，所以世界上的每一个 MAC 地址都是独一无二的。

接下来我们就进入第一个实验吧——查看各自计算机中网卡的 MAC 地址。请先从 Windows 的开始菜单中选择“命令提示符”。由于 Windows 的版本不同，有的版本会把命令提示符叫作 MS-DOS 提示符。选中后会弹出一个背景全黑的窗口，这就是命令提示符窗口，用户可以在这里用键盘输入由字符串构成的命令。输入完一串字符后按下回车键，这串字符所表示的命令就会被执行。

打开命令提示符后，请试着输入如下命令。

```
ipconfig /all
```

在 Windows 中内置了各种各样的用于查看网络信息或网络连接状态的命令。Windows 有多个版本，在本实验中使用的是 Windows 2000 Professional。请注意，如果使用的是其他版本，命令的名称或输出的结果可能或多或少会有些差异。此外，还有一点需要大家注意的是，在我们的实验结果画面中显示的 MAC 地址和 IP 地址都是虚拟的。因为从安全的角度来说，网络的配置信息不应该随便暴露。

下面我们回到实验中。通过 ipconfig /all 这条命令，可以显示出各种信息。实验结果的画面中只显示了笔者希望诸位关注的部分（如图 9.3 所示）。画面中显示在 Physical Address 后面的、用“-”分隔的 6 个十六进制数（每个数占 8 比特）00-00-5D-B8-39-B0 就是 MAC 地址。其中 00-00-5D 代表制造商，B8-39-B0 代表产品的编号。

图 9.3　使用 ipconfig /all 命令查看 MAC 地址

9.3　实验 2：查看计算机的 IP 地址

MAC 地址虽然可以在硬件层面上标识网卡，可是如果只有 MAC 地址也很不方便。因为企业或组织需要对计算机分组管理，但是他们却没有办法把 MAC 地址前面的若干位统一起来。而且在互联网那种把全世界的计算机都连接在一起的大型网络中，又必须要有一种机制能够把数据的发送目的地像邮政编码那样整理并标识出来。假如在互联网中只能使用 MAC 地址，那么会发生什么呢？在接入互联网的数量众多的计算机中，只有尚未进行任何分组处理的编号（MAC 地址）。这样的话，仅仅是寻找信息的发送目的地就要花费大量的时间。

因此，在 TCP/IP 网络中，除了硬件上的 MAC 地址，还需要为每台计算机设定一个软件上的编号。这个编号就是众所周知的 IP 地址。

通常把设定了 IP 地址的计算机称为“主机”（Host）。因为路由器也算是计算机的一种，所以它们也有 IP 地址。在 TCP/IP 网络中，传输的数据都会携带 MAC 地址和 IP 地址两个地址。

IP 地址是一个 32 比特的整数，每 8 比特为一组，组间用“.”分隔，分成 4 段表示。8 比特所表示的整数换算成十进制后范围是 0～255，因此可用作 IP 地址的整数是 0.0.0.0～255.255.255.255，共计

4294967296 个。

通过 IP 地址就可以轻松地对计算机进行分组管理了。比如用 IP 地址中第 1 段到第 3 段的数值代表公司，用第 4 段的数值代表公司内部的计算机。例如，在 AAA.BBB.CCC 这个公司内，如果有一台计算机的编号是 ×××，那么它的 IP 地址就是 AAA.BBB.CCC.XXX。而看到了 AAA.BBB.CCC.YYY 这样一个 IP 地址，就能知道它是这个公司内的另一台计算机。通常把 IP 地址中表示分组（即 LAN）的部分称作“网络地址”、表示各台计算机（即主机）的部分称为“主机地址”。在本例中，AAA.BBB.CCC 这一部分是网络地址，而 XXX 或 YYY 的部分是主机地址。

下面进入实验，请诸位查看各自计算机上配置的 IP 地址。与之前相同，还是使用如下的命令。

```
ipconfig /all
```

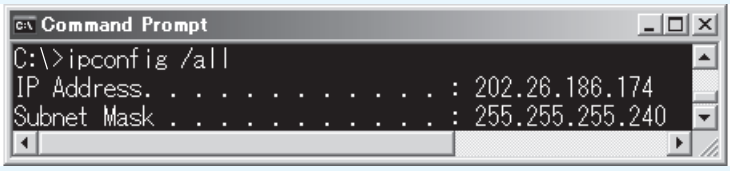

图 9.4　使用 ipconfig /all 命令查看 IP 地址

如图 9.4 所示，显示在 IP Address 后面的 202.26.186.174 就是 IP 地址。请诸位再留意一下显示在 Subnet Mask 后面的 255.255.255.240。这一串数字是“子网掩码”。子网掩码的作用是标识出在 32 比特的 IP 地址中，从哪一位到哪一位是网络地址，从哪一位到哪一位是主机地址。

把 255.255.255.240 用二进制表示的话，结果如下所示。

11111111.11111111.11111111.11110000

子网掩码中，值为 1 的那些位对应着 IP 地址中的网络地址，后面值为 0 的那些位则对应着主机地址。因此 255.255.255.240 这个子网掩码就表示，其所对应的 IP 地址前 28 比特是网络地址，后 4 比特是主机地址。

4 个二进制数可以表示的范围是从 0000 到 1111，共 16 个数。而因为最开始的 0000 和最后的 1111 具有特殊的用途，所以笔者的办公室内最多可以配置 14 台计算机，它们的主机地址范围是从 0001 到 1110。但是这其中又有一台路由器，所以实际上最多只能放置 13 台计算机。与 MAC 地址一样，每个 IP 地址的值也都是独一无二的。

9.4　实验 3：了解 DHCP 服务器的作用

IP 地址和子网掩码都是在软件上设置的参数。请先打开控制面板中的“网络连接”，然后用鼠标右键单击“本地连接”并选择“属性”菜单项，接着在打开的窗口中选择“Internet 协议（TCP/IP）”，最后单击“属性”按钮[①]。这样就打开了设定 IP 地址和子网掩码的对话框（如图 9.5 所示）。

① 如果您使用的是 Windows 7 或 8，请先打开控制面板中的“查看网络状态和任务”，然后单击左侧边栏中的“更改适配器设置”，接着用鼠标右键单击“本地连接”并选择“属性”菜单项，在打开的窗口中选择“Internet 协议版本 4（TCP/IPv4）”，最后单击“属性”按钮。

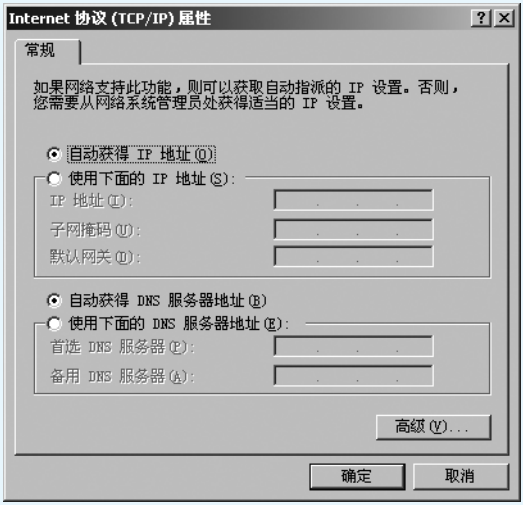

图 9.5 设置 IP 地址和子网掩码的对话框

虽然在这个对话框中可以手动设置 IP 地址和子网掩码，但是大多数情况下选择的还是“自动获得 IP 地址”这个选项。这个选项使得计算机在启动时会去从 DHCP 服务器获取 IP 地址和子网掩码，并自动地配置它们。

DHCP 的全称是 Dynamic Host Configuration Protocol（动态主机设置协议）。在笔者搭建的 LAN 中，使用了一台装有 Linux 的计算机充当 DHCP 服务器的角色。因为 Windows 的计算机也同样支持 DHCP 的协议，所以即使服务器上装的是 Linux，而客户端装的是 Windows，也没有关系。

DHCP 服务器上记录着可以被分配到 LAN 内计算机的 IP 地址范围和子网掩码的值。作为 DHCP 客户端的计算机在启动时，就可以从中

知道哪些 IP 地址还没有分配给其他计算机。

请再看一次图 9.5。虽然文字是灰色的也许有些难以辨认，但是还是可以看到有一个叫作“默认网关”的配置项。通常会把路由器的 IP 地址设置在这里。也就是说路由器就是从 LAN 通往互联网世界的入口（Gateway）。路由器的 IP 地址也可以从 DHCP 服务器获取。最后再请诸位注意一点，这里选择了“自动获得 DNS 服务器地址”这一选项。也就是说，DNS 服务器的 IP 地址也可以从 DHCP 服务器获取。DNS 服务器的作用将在稍后的章节中介绍。

9.5　实验 4：路由器是数据传输过程中的指路人

在分组管理下，IP 地址中的网络地址部分可以代表一个组中的全部计算机，即一个 LAN 中的计算机全体。互联网就是用路由器把多个 LAN 连接起来所形成的一张大网。从以上这两点，是不是就能慢慢看出路由器所扮演的角色了？

路由器正如其名，就是决定数据传输路径的设备。在本实验环境中，与 LAN 内的其他计算机一样，路由器也是连接在集线器上的。因为 LAN 内采用了 CSMA/CD 机制，所以所有发送出去的数据也都会发到路由器上。当从公司内的计算机向另一家公司的计算机发送数据时会发生什么呢？首先，一个不属于 LAN 内计算机的 IP 地址会被附加到数据的发送目的地字段上。这样的数据虽然会被 LAN 内的计算机所忽略，但是不会被路由器忽略。因为路由器的工作原理就是查看附加到数据上的 IP 地址中的网络地址部分，只要发现这个数据不是发送给 LAN 内计算机的，就把它发送到 LAN 外，即互联网的世界中。

路由器虽然看起来就是个小盒子，可实际上是一台神奇的计算机。分布在世界各地的 LAN 中的路由器相互交换着信息，互联网正是由于这种信息的交换才得以联通。这种信息被称作“路由表”，用来记录应该把数据转发到哪里。在像互联网这样的网络中，传输路径错综复杂，而路由器就是站在各个岔路口的指路人（如图 9.6 所示）。在一台路由器的路由表中，只会记录通往与之相邻的路由器的路径，而并不会记录世界范围内的所有传输路径。

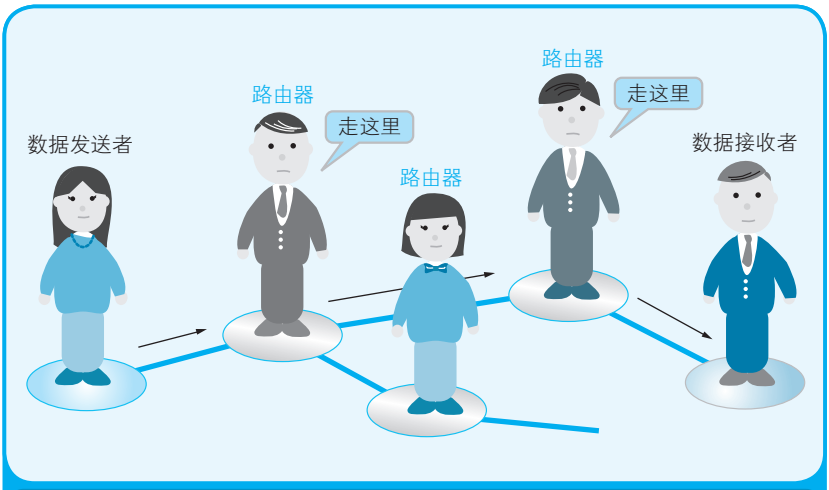

图 9.6 路由器是互联网中的指路人

下面就实际观察一下路由表吧。为此需要在命令提示符窗口中执行如下命令（执行结果如图 9.7 所示）。

```
route print
```

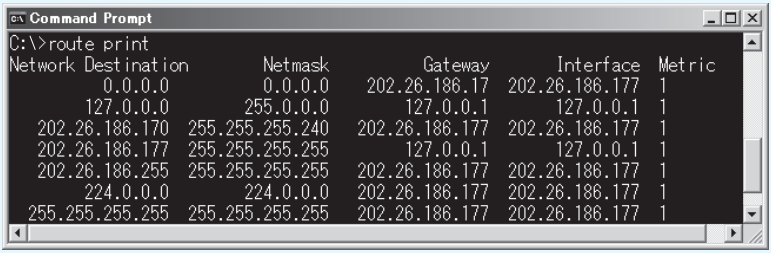

图 9.7　通过 route print 命令列出路由表

路由表由 5 列构成。Network Destination、Netmask、Gateway、Interface 这四列记录着数据发送的目的地和路由器的 IP 地址等信息。Metric 这一列记录着路径的权重，这个值由某种算法决定，比如数据传输过程中经过的路由器的数量。如果遇到有多条候选路径都可以通往目的地的情况，路由器就会选择 Metric 值较小的那条路径。在路由表中还有如下的规则：如果数据的发送目的地就在本 LAN 中，则可以直接发送数据而无需经过路由器转发；反之如果在 LAN 外（或发送目的地的 IP 地址不在路由表中），则需要经过路由器转发。细节虽然有些复杂，但是只要了解了大体上的规则就可以了。

9.6　实验 5：查看路由器的路由过程

假设诸位正在浏览笔者目前就职的公司 GrapeCity 的主页（http://www.grapecity.com/）。GrapeCity 的 Web 服务器中的数据，要经过若干个路由器的转发才能达到诸位的计算机上。通常把这种数据经过路由器转发的过程称为“路由”（Routing）。

在命令提示符窗口中执行 tracert 命令后，就可以查看路由的过程了。执行时需要在 tracert 的后面指定一个主机名（或计算机名），作为