

数据的发送目的地。这样看到的转发路径其实是相反的，那我们就干脆来看一下诸位的计算机到 GrapeCity 的 Web 服务器的路径吧。请在命令提示符窗口中执行如下命令（执行结果如图 9.8 所示）。

```
tracert www.grapecity.com
```

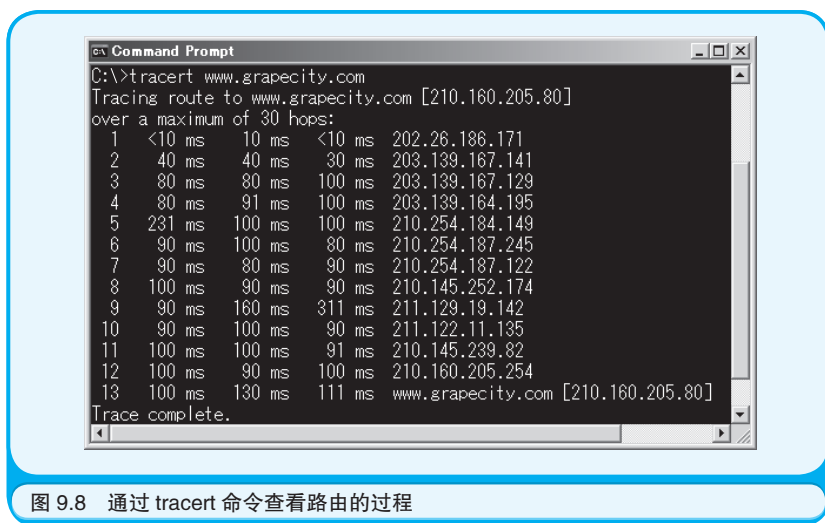


图 9.8 通过 tracert 命令查看路由的过程

诸位难道不认为这回的实验结果非常有意思吗？左侧按照 1~13 的顺序列出了数据前进道路上途经的 IP 地址。第 1 行的 202.26.186.171 是作为实验对象的 LAN 内的路由器。第 2 行的 203.139.167.141 是笔者所租用的互联网服务提供商的路由器。从第 3 到第 11 行，是其他服务提供商的路由器。其中第 11 行的 210.145.239.82 是 GrapeCity 所租用的服务提供商的路由器。第 12 行的 210.160.205.254 是 GrapeCity 的路由器。最后，第 13 行的 210.160.205.80 是 Grape City 的 Web 服务器。可以看到，从笔者公司内的 LAN 出发，通过 13 次路由才终于到达了 GrapeCity。

9.7 实验 6: DNS 服务器可以把主机名解析成 IP 地址

笔者希望诸位在刚刚的实验中注意到了这样一个问题：在互联网的世界中，本应使用 IP 地址这样的数字来标识计算机才是，而刚刚却可能使用一串字符 `www.grapecity.com` 来标识 Grape City 的 Web 服务器。实际上，在互联网中还存在一种叫作 DNS（Domain Name System，域名系统）的服务器。正是该服务器为我们把 `www.grapecity.com` 这样的域名解析为了 `210.160.205.80` 这样的 IP 地址。

诸位的计算机都有一个主机名，每个 LAN 也都有一个域名。举例来说，笔者所使用的计算机的主机名是 `ma50j`（源于这台计算机的型号），所在的 LAN 的域名是 `yzw.co.jp`。把主机名和域名组合起来所形成的 `ma50j.yze.co.jp`，就是能够标识笔者这台计算机的一个世界范围内独一无二的名字，这个名字与 IP 地址的作用是等价的。通常把这种由主机名和域名组合起来形成的名字称作 FQDN（Fully Qualified Domain Name，完整限定域名）。

在互联网中，难以记忆的 IP 地址使用起来很麻烦。于是人们就发明出了 DNS 服务器，这样只需要使用 FQDN，DNS 服务器就可以自动地把它解析为 IP 地址了（这个过程叫作“域名解析”）。DNS 服务器通常被部署在各个 LAN 中，里面记录着 FQDN 和 IP 地址的对应关系表。世界范围内的 DNS 服务器是通过相互合作运转起来的。如果一台 DNS 服务器无法解析域名，它就会去询问其他的 DNS 服务器。这套流程是自动进行的，诸位并不会意识到。

下面我们就进入实验阶段吧。首先，查一查各自计算机的主机名。在命令提示符窗口执行 `hostname` 这条命令。结果中只会显示主机名，并没有 FQDN（如图 9.9 所示）。虽然有些啰嗦，但还是要说明一下在

其他版本的 Windows 中，这条命令的输出结果可能会有差异。这里没能列出其他版本上的执行结果，还望诸位见谅。

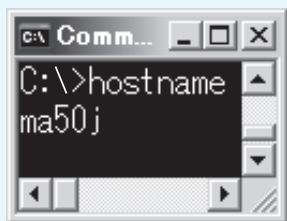


图 9.9 用 hostname 命令确认主机名

接下来想要查看 FQDN 的话，则需要执行之前使用过的 `ipconfig /all` 命令。结果画面中，Host Name 后面显示的是主机名，而 DNS Suffix Search List 后面显示的就是域名。将这两者组合起来就能得到 FQDN。于是可以确认笔者计算机的 FQDN 确实是 `ma50j.yzw.co.jp`（如图 9.10 所示）。

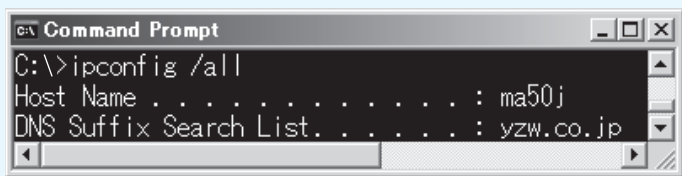
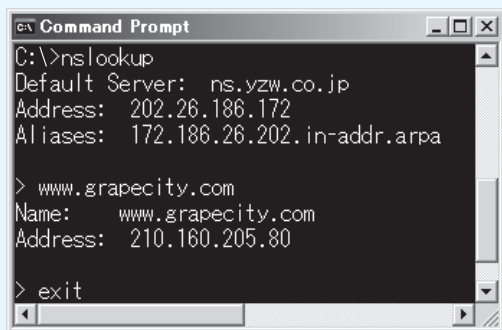


图 9.10 用 ipconfig /all 命令确认主机名和域名

下面再来操作一下 DNS 服务器。在命令提示符窗口中执行 `nslookup`，屏幕上就会显示出一个提示符“>”，表示现在可以询问 DNS 服务器了。而提示符上面的 `ns.yze.co.jp` 和 `202.26.186.35`，则是笔者公

司 LAN 内的 DNS 服务器的 FQDN 和 IP 地址。试着输入 `www.grapecity.com`，然后按下 Enter 键。结果输出了 210.160.205.80，这正是 GrapeCity 的 Web 服务器的 IP 地址。`www.grapecity.com` 和 210.160.205.80 的对应关系，是通过询问其他互联网上的 DNS 服务器才得知的，并没有被事先录入到笔者公司内 LAN 中的 DNS 服务器上。要想退出 `nslookup`，请输入 `exit`，然后按下 Enter 键（如图 9.11 所示）。



```
c:\>nslookup
Default Server: ns.vzw.co.jp
Address: 202.26.186.172
Aliases: 172.186.26.202.in-addr.arpa

> www.grapecity.com
Name: www.grapecity.com
Address: 210.160.205.80

> exit
```

图 9.11 使用 `nslookup` 进行域名解析

9.8 实验 7：查看 IP 地址和 MAC 地址的对应关系

在互联网的世界中，到处传输的都是附带了 IP 地址的数据。但是能够标识作为数据最终接收者的网卡的，还是 MAC 地址。于是在计算机中就加入了一种程序，用于实现由 IP 地址到 MAC 地址的转换，这种功能被称作 ARP（Address Resolution Protocol，地址解析协议）。

ARP 的工作方式很有意思。它会对 LAN 中的所有计算机提问：“有谁的 IP 地址是 210.160.205.80 吗？有的话请把你的 MAC 地址告诉我。”通常把这种同时向所有 LAN 内的计算机发送数据的过程称作“广

播”(Broadcast)。通过广播询问,如果有某台计算机回复了MAC地址,那么这台计算机的IP地址和MAC地址的对应关系也就明确了。ARP的工作流程也是自动进行的,诸位并不会意识到。

如果为了查询MAC地址,每回都要进行广播询问,那么查询的效率就会降低。于是ARP还提供了缓存的功能,当向各个计算机都询问完一轮之后,就会把得到的MAC地址和IP地址的对应关系缓存起来(临时保存在内存中)。存起来的这些对应关系信息称作“ARP缓存表”。只要在命令提示符窗口中执行`arp -a`命令,就可以查看当前ARP缓存表中的内容。那么,作为最后的实验,我们就来查看一下ARP缓存表吧。

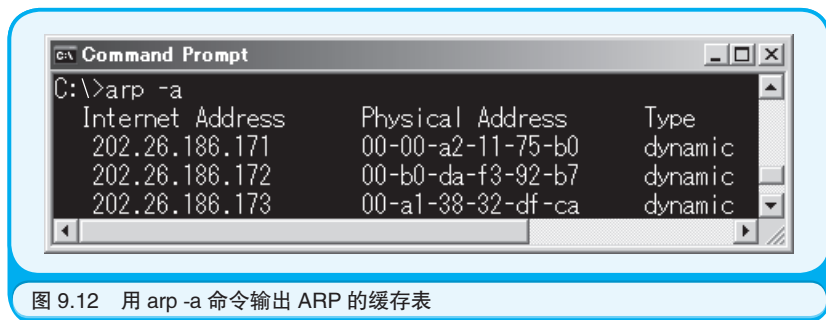


图 9.12 用 `arp -a` 命令输出 ARP 的缓存表

9.9 TCP 的作用及 TCP/IP 网络的层级模型

最后请允许笔者补充说明一些内容。TCP/IP 这个词表示在网络上同时使用了 TCP 和 IP 这两种协议。正如前面所讲解的那样,IP 协议用于指定数据发送目的地的 IP 地址以及通过路由器转发数据。而 TCP 协议则用于通过数据发送者和接收者相互回应对方发来的确认信号,可靠地传输数据。通常把像这样的数据传送方式称作“握手”

(Handshake)(如图 9.13 所示)。TCP 协议中还规定,发送者要先把原始的大数据分割成以“包”(Packet)为单位的数据单元,然后再发送,而接收者要把收到的包拼装在一起还原出原始数据。

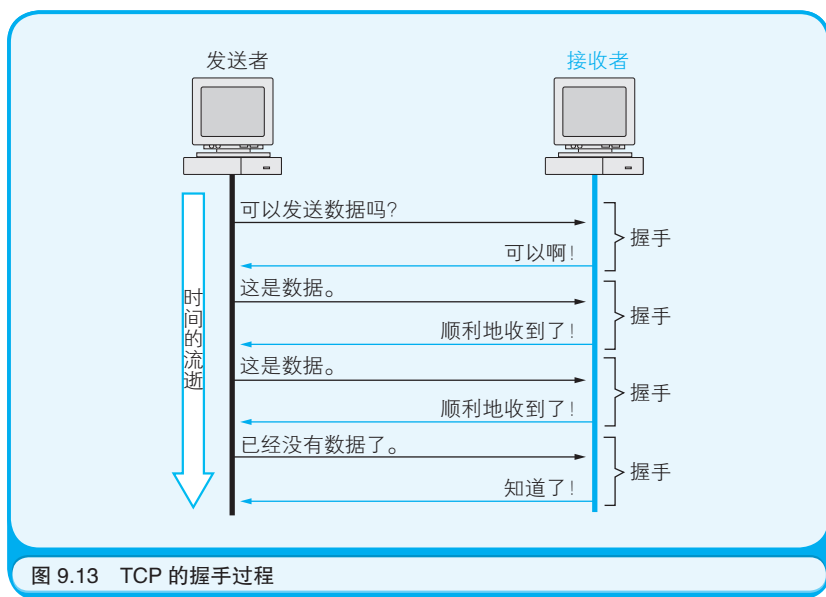


图 9.13 TCP 的握手过程

在之前的讲解中,一直把协议和约束等同起来,但恐怕还是会有人觉得协议这个词难以理解吧。正因为发送者和接收者都遵循了相同的约束,双方才能相互发送数据。为了能够在约束下收发数据,操作系统将实现了 TCP 和 IP 等协议的程序作为自身的一部分功能提供。遵循约束表现在统一数据的格式上。例如,诸位敲打键盘输入的电子邮件正文等数据,并不是原封不动地发送出去的,而是先通过实现了 TCP 协议的程序附加上遵守 TCP 约束所需的信息,然后再通过实现了 IP 协议的程序,进一步附加上遵守 IP 约束所需的信息。实际上计算机发送的是以包为单位的、附加了各种各样信息的数据(如图 9.14 所示)。



图 9.14 附加了各种各样信息的数据包

硬件上发送数据的是网卡。在网卡之上是设备驱动程序（用于控制网卡这类硬件的程序），设备驱动程序之上是实现了 IP 协议的程序，IP 程序之上则是实现了 TCP 协议的程序，而再往上才是应用程序，比如 Web 或电子邮件。这样就构成了一幅在硬件之上堆叠了若干个软件层的示意图（如图 9.15 所示）。TCP 协议使用被称作“TCP 端口号”的数字识别上层的应用程序。TCP 端口号中有一些是预先定义好的，比如 Web 使用 80 端口，电子邮件使用 25 端口（用于发送）和 110 端口（用于接收）。

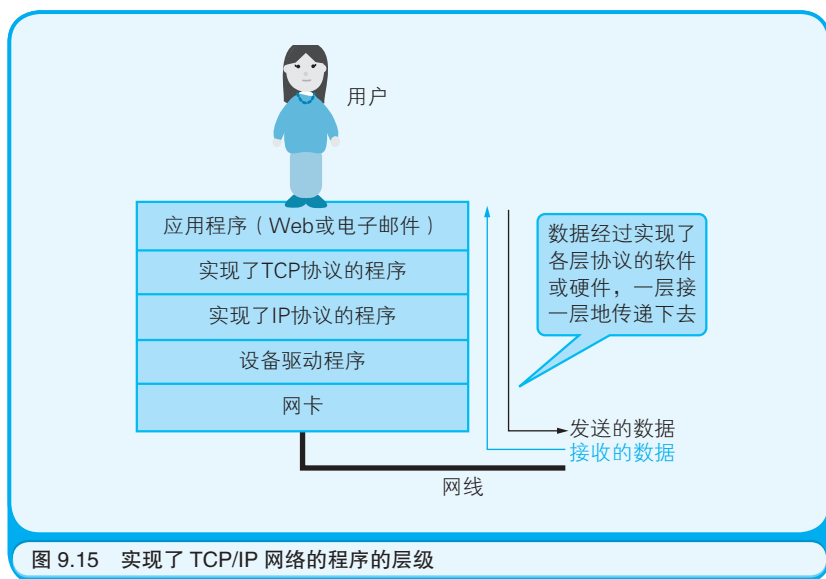


图 9.15 实现了 TCP/IP 网络的程序的层级

☆ ☆ ☆

怎么样？对于至今为止一直在使用却不知其所以然的网络，一旦了解了其中的原理，就会很有成就感吧？但是，目前为止我们通过实验所掌握的只不过是 TCP/IP 网络的基础知识。如果想要了解得更加深入，笔者建议诸位去学习有关 TCP/IP 的专业书籍。只要掌握了本章所讲解的基础知识，即便在这之前还觉得那些书难以理解，现在也应该可以轻松地看懂了。在深入学习的阶段，如果有条件进行实验，那么请务必动手做一做。因为通过实验学到的知识，人们往往会掌握得更扎实、记忆得更牢靠。

在接下来的第 10 章中，笔者将讲解与网络安全相关的加密技术和身份认证机制。敬请期待！

第 10 章

试着加密数据吧

热身问答

在阅读本章内容前，让我们先回答下面的几个问题来热热身吧。



问题

初级问题

通常把还原加密过的文件这一操作叫作什么？

中级问题

在字母 A 的字符编码上加上 3，可以得到哪个字母？

高级问题

在数字签名中使用的信息摘要是什么？

怎么样？被这么一问，是不是发现有一些问题无法简单地解释清楚呢？下面，笔者就公布答案并解释。

答案

初级问题：叫作解密。

中级问题：可以得到字母 D。

高级问题：信息摘要是指从作为数字签名对象的文件整体中计算出的数值。

解释

初级问题：本章将会介绍加密和解密的具体例子。

中级问题：因为字母表中的字母编码是按字母顺序排列的，所以在字母 A 的编码上加 3，即 $A \rightarrow B \rightarrow C \rightarrow D$ ，所以可以得到 D。

高级问题：对比由文件整体计算出的信息摘要，可以证明文件的内容有没有被篡改。加密处理过的信息摘要就是数字签名。