网管手册

（下）

王继刚 主编

目录

个人 Internet 网站创建过程详解

本文通过创建 Internet 示范网站——自由网络（Webfree）的实例，详细叙述了 Windows NT 安装、WWW 服务、FTP 服务的配置、邮件服务、新闻讨论组服务的 DNS 设置、IP 地址分配等网站的安装、设置过程。

在 Internet 日益红火的今天，相信你早已加入了网迷的队伍，整天泡在网上了。你可能还租了个“门面”，在网上精心侍弄着自己的免费个人主页。可是，你有没有想过有朝一日安个“家”，拥有属于自己的 Internet 网站呢？其实这并不难，我就有一个。不太相信？那好办：点亮你的电脑，叫醒你的猫，建立一个拨号网络连接，连接位置：自由网络（Webfree）；电话号码：0429－7129081；用户名：guest；口令：guest。拨号连接……嘿！通了！！！快运行你的网页浏览器，敲入这个网址：http:•www.webfree.com，看到了吧？这就是我的自由网络！Web 网页浏览、FTP 文件传输、E－mail 收发、NEWS 讨论、在线讨论、免费邮箱、免费个人主页，应有尽有！而这一切除了电脑＋猫＋电话，并不需要任何额外设备。怎么？就这么容易？看完本文，你会说：真这么容易！好吧！变心动为行动，Do it yourself。

一、Windows NT Server 4.0 中文版的安装

上面所说的这一切，都要以 Windows NT Server 操作系统为运行平台。所以，对你的电脑的要求就是能够跑 Windows NT。基本配置要求：486 以上 CPU；16 兆以上内存；500 兆以上硬盘空间。不过，要是没有一颗奔腾的“心”和 32 兆以上的内存，可别想跑得轻松。

1.安装前准备

我的硬盘分成 C:、D：两个分区。C：FAT 格式，2047MB，MS－DOS 主分区,已装 MS－DOS/Windows 95，配成多重启动；D：FAT 格式，2047MB，MS－DOS 扩展分区,预留 Windows NT 空间。光驱盘符为 E:。在 MS－DOS 环境或 Windows 95 的 MS－DOS 命令窗口下，进入光盘 Windows NT Server 4.0 中文版的安装主目录 I386，键入 WINNT/B 后回车，即开始基于 MS－DOS 部分的安装，然后重新启动计算机。

2.基本系统安装

重新启动时，启动过程已被 Windows NT 的操作系统管理器 OS Loader 4.0 所控制。OS Loader 自动选择“Windows NT 4.0 Installation/Upgrade”项目，继续进行后续安装工作。保持 Windows NT 默认的安装目录“\WINNT”不变，安装程序将复制 Windows NT 基本系统文件到 D:\WINNT 目录。复制完成后，按回车键启动计算机。

3.网络向导安装

再次启动计算机时，应在 OS Loader 处选择第一项“Windows NT Server Version 4.00”。稍后出现 Windows NT 图形安装界面，继续复制 Windows NT 系统安装向导文件。然后，Windows NT 安装向导开始运行。本例计算机名称输入“DAMUGE”（自动变大写）；服务器类型为“主域控制器”；勾选“用线路连接到网络”、“安装 Microsoft Internet Information Server”；在网络适配器选择界面，点选“从列表中选择”，并从弹出的网络适配器选择窗口中选取“MS Loopback 卡”；在服务安装选择窗口中，除已有的服务外，点取“从列表中选择”，然后在弹出的网络服务窗口中分两次选取“Microsoft DNS 服务器”和“远程访问

服务”，然后在安装 MS Loopback 卡和安装 TCP/IP 窗口中，分别取默认值，并进行调制解调器的检测、安装。在 Microsoft TCP/IP 属性设置窗口中，在 IP 地址选项卡下点取“指定 IP 地址”，并输入本服务器指定的 IP 地址（注意：如果你的服务器是与 Internet 实际连接的，IP 地址是由上级结点指定给你的，固定不变；如果你的服务器是独立运行的，所有的 IP 地址资源都是可以使用的，你可以任意指定自己服务器的 IP 地址），例如：202.96.34.88。在主域控制器域名输入窗口去掉默认的域名“DOMAIN”，输入指定的域名，如“COM”。一段时间后，完成 Windows NT 网络部分的安装，自动开始 Microsoft Internet Information Server 2.0 的安装。Windows NT 的 IIS 包括 WWW、FTP、Gopher 三项基本 Internet 服务。除在选项窗口点选安装全部选项之外，其余全部取默认项即可。最后，单击“重新启动计算机”，整个安装过程结束。

二、安装后的调整、补充

Windows NT Server 4.0 全部安装完毕之后，启动计算机，在 Windows NT 登录窗口，确认用户名为管理员（Administrator），输入管理员密码（安装时建立的密码）回车，即可登录到 Windows NT 桌面，进行进一步的调整、维护工作了。

1.远程访问配置

顺序选取“控制面板”·“网络”·“服务”·“远程访问服务”·“属性”。点取“配置”，在“配置端口用法”窗口中将“端口用法”点选为“拨出和接收”，单击“确定”，再点取“网络”，在“允许远程客户运行”的三种协议中只保留“TCP/IP”一项的勾选，并点取 TCP/IP 后面的“配置”，然后点选“使用静态地址集”，在“起始”IP 地址栏输入 202.96.0.1,

在“结束”IP 地址栏输入 202.96.255.255,顺序单击“确定”、“确定”、“继续”完成设置。

2.添加 IP 地址

顺序选取“控制面板”·“网络”·“协议”·“TCP/IP 通讯协议”·“属性”，在 IP 地址选项卡下点取“高级”，重复点取“添加”，添加如下 IP 地址资源备用：

202.96.34.168（准备用于 WWW 主页 www.webfree.com 及 FTP 服务 ftp.webfree.com）；

202.96.34.169（准备用于 NEWS 新闻服务 news.webfree.com）；

202.96.34.170（准备用于 MAIL 邮件服务 mail.webfree.com）；

202.96.34.188（准备用于 HOME 主机 WWW 远程管理服务 home.webfree.com）；

202.96.34.189（准备用于以后扩充其他服务）；

202.96.34.190（准备用于以后扩充其他服务）。

以上 IP 地址添加完毕后，单击“确定”返回；再点击“DNS”选项卡，在“DNS 服务器搜索顺序”处单击“添加”，然后输入主机 DAMUGE 的 IP 地址 202.96.34.88,单击“添加”，再点击“WINS 地址”选项卡，在“主 WINS 服务器”处输入主机 DAMUGE 的 IP 地址 202.96.34.88,然后单击“确定”，再单击“关闭”退出网络属性窗口，重新启动计算机。

三、DNS 服务器及 WWW、FTP 服务设置

1.DNS 服务器设置

重新启动 Windows NT，以管理员（Administrator）身份登录，在桌面依次单击“开始”·“程序”·“管理工具（公用）”·“DNS 管理器”，进入 DNS 服务器设置。

单击“DNS”•“新建服务器”，在 DNS 服务器处输入主机名字 DAMUGE 后单击确定，即建立了 DNS 服务器。在服务器清单下点选“DAMUGE”，然后单击“DNS”•“新建区域”，在区域类型处点选“主要”，并在“区域”处输入“COM”，点击“服务器”输入栏自动出现“COM.DNS”文件名，再单击“下一步”、“完成”，即建立了 COM 区域。

点选新建的区域 COM，然后单击“DNS”•“新建域”，在域名处输入“WEBFREE”后单击“确定”，即建立了区域 COM 下的 WEBFREE 域。

点选新建的域 WEBFREE，然后单击“DNS”•“新建主机”，分别输入以下主机名、IP 地址并单击“添加主机”，建立所有需要的域名映射：

主机名：WWW　主机 IP 地址：202.96.34.168；

主机名：FTP 主机 IP 地址：202.96.34.168；

主机名：NEWS　主机 IP 地址：202.96.34.169；

主机名：MAIL　主机 IP 地址：202.96.34.170；

主机名：HOME　主机 IP 地址：202.96.34.188；

完成后，屏幕如下图所示。最后退出 DNS 服务管理，结束 DNS 服务器的设置。

2.WWW 服务的设置

在桌面依次单击“开始”•“程序”•“Microsoft Internet Server（公用）”•“Internet 服务管理器”，进入 Internet 服务设置。

双击 DAMUGE 的 WWW 服务，点选“目录”选项卡，双击“D:\InetPub\wwwroot”项，勾选“虚拟服务器”，输入 IP 地址：202.96.34.188，勾选“执行”后单击“确定”回到目录选项卡。单击“添加”，输入 WWW 网页目录 D:\InetPub\wwwroot\webfree（须事先建好此目录并将相应网页

文件拷贝到此目录下），点选“主目录”，勾选“虚拟服务器”，输入 IP 地址：202.96.34.168，然后单击“确定”回到目录选项卡。单击“确定”返回。

3.FTP 服务的设置

在桌面依次单击“开始”·“程序”·“Microsoft Internet Server（公用）”·“Internet 服务管理器”，进入 Internet 服务设置。

双击 DAMUGE 的 FTP 服务，点选“信息”选项卡，在欢迎信息窗口输入欢迎信息，再点选“目录”选项卡，单击“添加”，输入 FTP 文件上传目录 D:\InetPub\ftproot\upload（须事先建好此目录，主要供用户上传文件），点选“虚拟目录”，勾选“可写”，输入虚拟目录别名：/upload，然后单击“确定”回到目录选项卡。单击“确定”返回。

四、域用户设置管理

在桌面依次单击“开始”·“程序”·“管理工具（公用）”·“域用户管理器”，进入域用户管理器。

要建立新的一般用户，可单击“用户”·“新用户”建立新的用户，输入此用户的有关信息，单击“拨入”，勾选“给予用户拨入的权限”，单击“确定”、“添加”，即完成了一个新用户的拨号访问账号的建立。重复该过程可以建立另外的用户账号。新增加的账号默认为隶属于“Domain users”组。建立用户时最好勾选“用户不得更改密码”选项，并且注意不随意赋予客户和一般用户较高的访问权限，以减少安全漏洞。

对于已经存在的用户，如管理员（Administrator）、客户（Guest）等，应该分别赋予其“拨入”的权限，并且将客户（Guest）的口令改为“guest”。对于新建的网络管理员账号，还要单击“组”图标，添加其到“Administrator

s”组，才可以在服务器上或以远程拨号连接的方式管理服务器资源。为了安全，应把管理员账号的口令设置为大小写字母和数字混合的、长度尽量长的，还要不定期更换口令。这样做虽然麻烦，但对于网络资源安全来说是有益的。

五、远程访问测试和远程 HTML 方式管理

完成以上步骤后，基本的 Internet 服务就设置完毕，可以开始测试了。分别在远程以客户（Guest）、一般用户和管理员的身份拨号入网，拨号连通之后，可以进行基本 Internet 功能和远程 HTML 管理方式的测试。

在网页浏览器中输入网址 http:•www.webfree.com，即可浏览 WWW 网页，默认的 WWW 主页文件名为 Default.htm，如果不是此文件名，应改为此文件名，也可以在 WWW 服务管理器里将默认的 WWW 主页文件名由原来的 Default.htm 改为你希望的文件名。

在网页浏览器或 FTP 软件的地址栏输入网址 ftp:•ftp.webfree.com，应该可以出现 FTP 服务器的文件资源，点取某一个文件，可以下载这个文件。

Windows NT 的 IIS 提供了远程访问方式的管理，可以很方便地进行 WWW、FTP、Gopher 服务的远程管理。以管理员身份拨号上网，在网页浏览器中输入网址 http:•home.webfree.com，即可进入远程 HTML 方式的管理界面。在弹出的身份验证窗口输入管理员账号和口令，即可方便地进行以上三种服务的远程设置，操作基本与 Windows NT 桌面方式的管理相同。

好了，你现在已经拥有了一个基本的 Internet 服务器。你可以尽情地体会一下“家”的感觉了。更进一步的功能，如：E－mail 服务、Newsgroups、在线讨论等，

可以在 Internet 网（或我的自由网络）上下载相应的软件，在 Windows NT 桌面上安装这些软件，并进行各自的设置即可。

内网 IP 建 ftp 服务器教程

很多朋友想建 ftp 服务器在 Internet 上共享自己的资源，苦于没有公网 IP，无法实现。其实，内网 IP 也可以建 ftp 服务器的。

第一步：

首先当然要安装 d2g client,申请一个动态域名解析了，你可以到它的官方网站下载到

http://www.deerfield.com/download/dns2go/

下载后你可以把它安装在你的局域网服务器或者客户机上都可以。

一路回车安装完后，按提示，注册一个新的域名：**.dns2go.com

注册好后，如果一切正常，你的 d2g 客户端便已经工作了，可以对你的静态或动态 IP 地址解析了。

其实，申请动态域名解析不仅仅 dns2go 一种方法，其它还有花生壳、动态主机等等。如果有静态 IP，则可以不用申请动态域名解析，直接用 IP 地址即可。

第二步：

但是，现在的 d2g 只能映射你局域网服务器的 IP，外部并不能访问你的机器。

现在你需要一个端口映射软件。

推荐一个小巧实用的工具：portTunnel

配合在局域网内架设网站的利器 --- PortTunnel 介

绍

这里向大家推荐一款工具，可以帮助大家轻松搞定“端口映射”。这款工具叫“PortTunnel”（中文意思叫“端口通道”），由 SteelBytes 出品，目前已经完全免费了！它的设置极其简单，可以运行在所有的 Windows 平台上。

好了，让我们来实际 x 作一番：

假设我是一个局域网用户，我的内部 IP 地址是 10.10.10.10，我是通过指定网关 10.10.10.1 上网的，我在自己的计算机上安装了“动态 IP 解析”软件和 WEB 服务器还有 FTP 服务器准备开一个网站和 FTP 服务器。以下是我的设置过程：

1. 到我的网关（代理）服务器 10.10.10.1 上安装“PortTunnel”软件（拷贝即可）

这是软件的界面：

2. 针对我需要的 WEB 服务进行配置，点击“Add”按钮，

点击“OK”按钮保存

注意：

Port In 填的端口号是 80，这样填的前提是网关（代理服务器）上没有 WEB 服务器在运行，否则请更换其它端口，例如“8080”（在这种情况下，用户必须通过 http://<你的域名>:8080 来访问你的网站。）

3. 针对我需要的 FTP 服务进行配置，点击“Add”按钮

点击“OK”按钮保存

注意：

Port In 填的端口号是 21，这样填的前提是网关（代理服务器）上没有 FTP 服务器在运行，否则请更换其它

端口，例如“2100”（在这种情况下，用户必须通过 ftp://<你的域名>:2100 来访问你的 FTP 服务器。）

4. 设置成功后的正常运行界面（平时这个界面可以关掉，不会影响使用）

注意：

正常运行时，你设置的通道的状态应当是“Active”，如果是“Failed”那很可能你设置的“Port In”端口号和网关（代理服务器）上的现有端口冲突。

5. 测试一下：

如果通过 http://<你的域名>能访问你的网站或 FTP://<你的域名>能访问你的 FTP 服务器，那就成功了。

重要提示：

如果局域网内有多个用户想架设网站，那么注意在设置的时候，一个“Port In”端口只能为一个用户服务，例如，usera 使用了“80”作“Port In“，那么他的网站就可以通过“http://”来访问，而 userb 就只能使用其它“Port In”端口了，例如“8080”，他的网站只能通过“http://:8080”来访问了。FTP 服务器的道理也是一样。

附：

PortTunnel 的下载地址：

http://www.steelbytes.com/download/PortTunnel_CH.zip (中文)

http://www.steelbytes.com/download/PortTunnel_ENGUK.zip (English)

这里，Port In 是要监听的端口，port out 是要映射的端口。比如你想监听服务器的 88 端口，映射到你的机器的 80 端口，这里的 port in 便是 88，port out 便是 80。默认的 FTP 端口是 21，如果想开 FTP 服务器，这里可

以是 21。

添加后，点"start"，服务器开始。程序自动加入系统服务，每次开机便会自动启动。

以上两步完成，一切 OK！

好了，现在可以用你申请的“d2g 域名:监听端口”来访问你的机器了。

透过局域网架网站

如今宽带已经不再是一个新鲜名词了，很多朋友也希望能够为丰富网络资源贡献一些自己的力量，而通过宽带架设 Web 网站或者是提供 FTP 下载服务则是最佳的选择。不过现在很多宽带用户都是使用电信、长城、聚友等一些城域网，也就是说整个公司在 Internet 上只有一个真正的 IP 地址，然后公司局域网内部的计算机通过服务器共享上网，对于这种情况如何建造自己的 FTP 站点就是一件令人头痛不已的事情。其实局域网内部的计算机也可以架设 FTP 服务器的，不过这需要一个端口映射软件的帮助，如果你也想在局域网中架设 FTP 网站的话，不妨一起来看看吧。

由于整个局域网在 Internet 上只有一个真正的 IP 地址，而这个 IP 地址是属于局域网中服务器独有的，即使我们在其它计算机中通过 Ser-U 等软件架设了 FTP 站点，但是无法让 Internet 上的朋友使用。这是为什么呢？打个比方说，如果你仅仅知道朋友在某幢写字楼上班，但是不知道它具体的房间，你就无法找到他。同样的道理，如果直接在局域网中架设 FTP，那么 Internet 上的朋友登录的时候仅仅可以找到局域网中的服务器，但是

至于怎样才能连接到你的计算机上就是一个问号了。为了解决这个问题，我们在局域网中建造自己 FTP 站点的时候需要一个端口映射软件来帮助，在此推荐一个小巧实用的工具－PortTunnel，它可以帮助大家轻松搞定这一切。顾名思义，PortTunnel 的中文意思就是“端口通道”，它的作用就是在服务器上为你的计算机指定一条通道，使得 Internet 上的朋友可以顺利的与你建立连接。

在使用 PortTunnel 之前有一点需要强调，就是它必须运行在服务器端，这样才能够实现端口映射的目的。这时点击下部的“增加”按钮进行相关的设置。这里有几个比较重要的项目重点介绍一下：

1、名称：在此中填写你的名称，这在局域网中有多台计算机需要端口映射的时候能够区分出每一台计算机。

2、输入端口：如果服务器端没有运行 FTP 服务，则可以采用默认的“21”作为端口，否则不能使用“21”，因为端口号重复将会导致系统冲突。

3、输出端口：这里填写的是你计算机中的 FTP 服务端口，通常采用默认的“21”，除非你另行指定了特殊的端口。

4、输出地址：这里填写你的计算机在整个局域网中的 IP 地址，比如此处是“129.156.0.21”。

点击下部的“确定”按钮保存之后，服务器端的端口映射就完成了，这时会发现原先的主窗口中多出了一项记录，按下“开始”就可以激活 PortTunnel 的端口映射服务了。此时你可以通过其他网友通过 ftp://129.156.0.21:21 来访问你的 FTP 服务器，如果能够顺利登录就说明已经全部搞定了。：

怎么样，PortTunnel 的设置与使用都非常简单吧，而且通过端口映射还可以实现在局域网内的计算机上架设 Web 服务器和 SMTP 服务器的功能，它们的设置与上面介绍的差不多，在此就不详述了，有兴趣的朋友不妨自行尝试一下。

说到这里，最后再提醒大家一下：PortTunnel 需要在服务器端才可以运行，至于怎样才能让网络管理员为你开通端口映射就要看各位的本事了，大家就各显神通吧。

远程分析 IIS 设置

提起微软公司 IIS web 服务器的安全问题,很多人立刻就会联想到那些为人们所称颂的致命

漏洞: UNICODE ，CGI 解析，.ida,idq, .Printer 远程溢出等. 这些伟大的漏洞恐怕是我等 scripts

远程确定目录权限

让我们打开一个 IIS 服务器来看看。在 IIS 服务管理器中，选择一个目录，看他的属性

在目录属性项有有这么一些选项（日志访问和索引此资源不计）：

脚本资源访问： 对网站的脚本可以读取原文件。

读取 读取目录里面的静态资源。

写入 用户可以建立以及删除资源

目录浏览 用户可以浏览目录内容。

应用程序设置的执行许可中有三个选项：

无 只能访问静态页面

纯脚本只允许允许脚本 如 ASP 脚本

脚本和可执行程序　可以访问和执行各种文件类型

那么，如何确定服务器上面的这些开关设置呢？别着急，一个一个来。

执行权限

如何确定某个目录是否开了执行权限呢？很简单，向服务器发送一个下面得请求：

http://iis-server/dir/no-such-file.dll

/dir/为要判断得目录，no-such-file.dll 是随便取得一个名字，服务器上面没有这个文件。

服务器对我们得请求会返回一个信息。如果返回的是一个 500 错误：

HTTP 500 - 内部服务器错误 （Internal Server error）

那么就说明这个目录的执行权限是开着的。对于服务器，能不开执行权限的就不要开。特别是虚拟目录的执行权限，大家想一想 UNICODE 和二次解码漏洞的利用过程就明白了。

如果服务器返回的是一个 404 错误：

HTTP 404 - 未找到文件

那么就说明这个目录的执行权限没有开。

写权限

测试一个目录对于 web 用户是否具有写权限，采用如下方法：

telnet 到服务器的 web 端口(80)并发送一个如下请求：

PUT /dir/my_file.txt HTTP/1.1

Host: iis-server

Content-Length: 10 <enter><enter>

这时服务器会返回一个 100(继续)的信息：

HTTP/1.1 100 Continue

Server: Microsoft-IIS/5.0

Date: Thu, 28 Feb 2002 15:56:00 GMT

接着，我们输入 10 个字母：

AAAAAAAAAA

送出这个请求后，看服务器的返回信息，如果是一个 201 Created 响应：

HTTP/1.1 201 Created

Server: Microsoft-IIS/5.0

Date: Thu, 28 Feb 2002 15:56:08 GMT

Location: http://iis-server/dir/my_file.txt

Content-Length: 0

Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, COPY, MOVE, PROPFIND,

PROPPATCH, SEARCH, LOCK, UNLOCK

那么就说明这个目录的写权限是开着的，反之，如果返回的是一个 403 错误，那么写权限就是

没有开起来，如果需要你认证，并且返回一个 401 (权限禁止) 的响应的话，说明是开了写权限，但是匿名用户不允许。如果一个目录同时开了”写”和“脚本和可执行程序”的话，那么 web 用户就可以上传一个程序并且执行它，恐怖哦%^#$!~

纯脚本执行权限

这样的目录就太多了。很多不需要给执行权限的