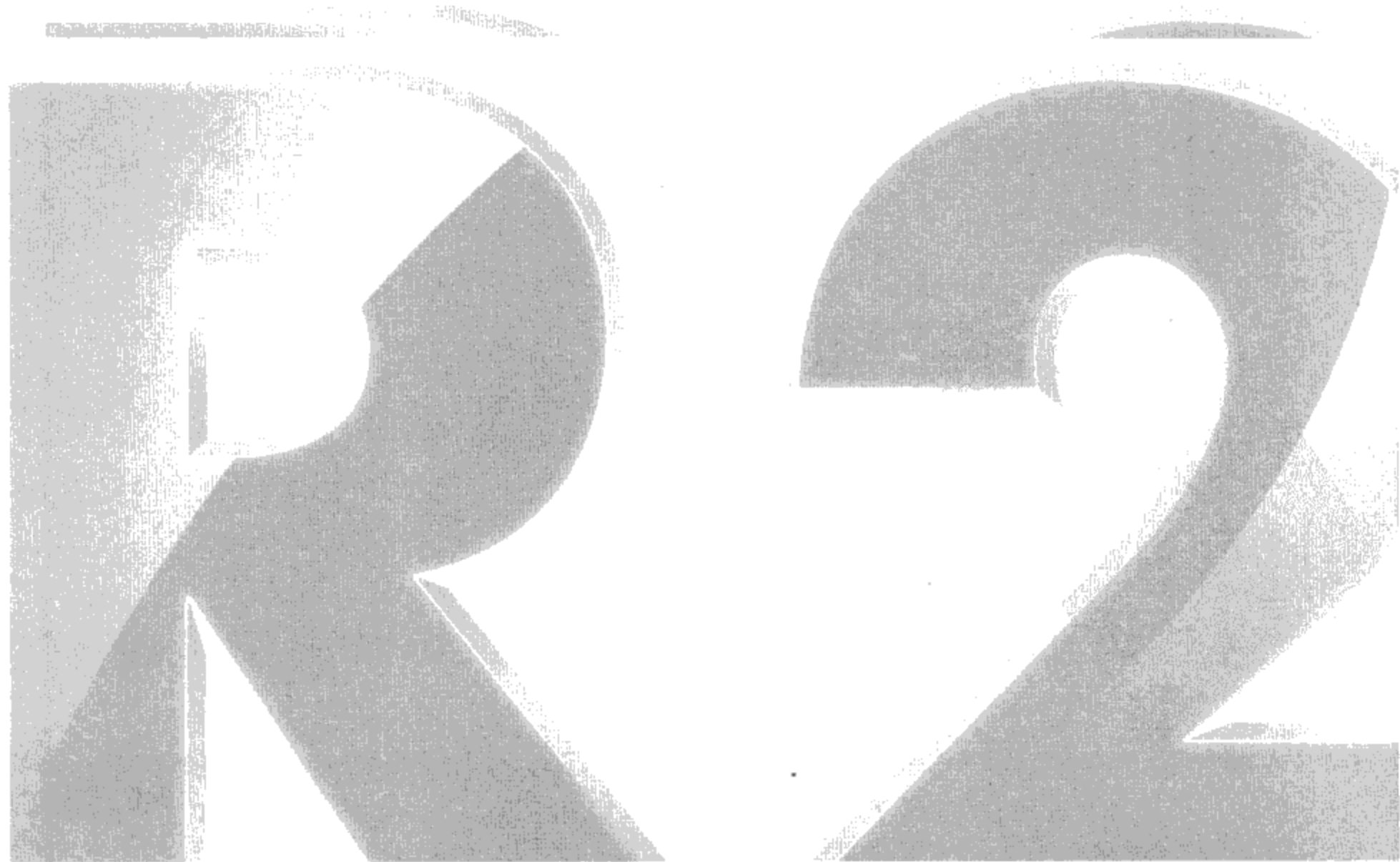


# 第 9 章

## FTP服务器的架设

FTP（File Transfer Protocol，文件传输协议）是一个用来在两台计算机之间传送文件的协议，这两台计算机中，一台是FTP服务器，一台是FTP客户端。FTP客户端可以从FTP服务器下载文件，也可以将文件上传到FTP服务器。

- ✎ 安装FTP服务器
- ✎ FTP站点的基本设置
- ✎ 物理目录与虚拟目录
- ✎ FTP站点的用户隔离设置
- ✎ 具备安全连接功能的FTP over SSL
- ✎ 防火墙的FTP设置
- ✎ 虚拟主机名



## 9-1 安装FTP服务器

Windows Server 2008 R2内置的是增强功能的新版本FTP服务器，它支持以下的新功能：

- 与Windows Server 2008 R2的IIS充分集成，因此您可以通过IIS全新的管理界面来管理FTP服务器。而且您可以将FTP服务器集成到现有的站点内，也就是一个站点内同时包含着网站与FTP服务器。
- 支持最新的因特网标准，例如支持FTP over SSL (FTPS)、IPv6与UTF8。
- 支持虚拟主机名 (virtual host name)。
- 更强的用户隔离功能。
- 更强的记录功能，让您更容易掌控FTP服务器的运行情况。

### 9-1-1 测试环境的创建

我们将通过图 9-1来解说与练习本章内容。为了方便练习，因此图中的域名并没有经过申请程序，而是随意设置的，当然也没有对外注册图中的DNS服务器。请先自行架设好图中的3台计算机，然后按照以下说明来设置：

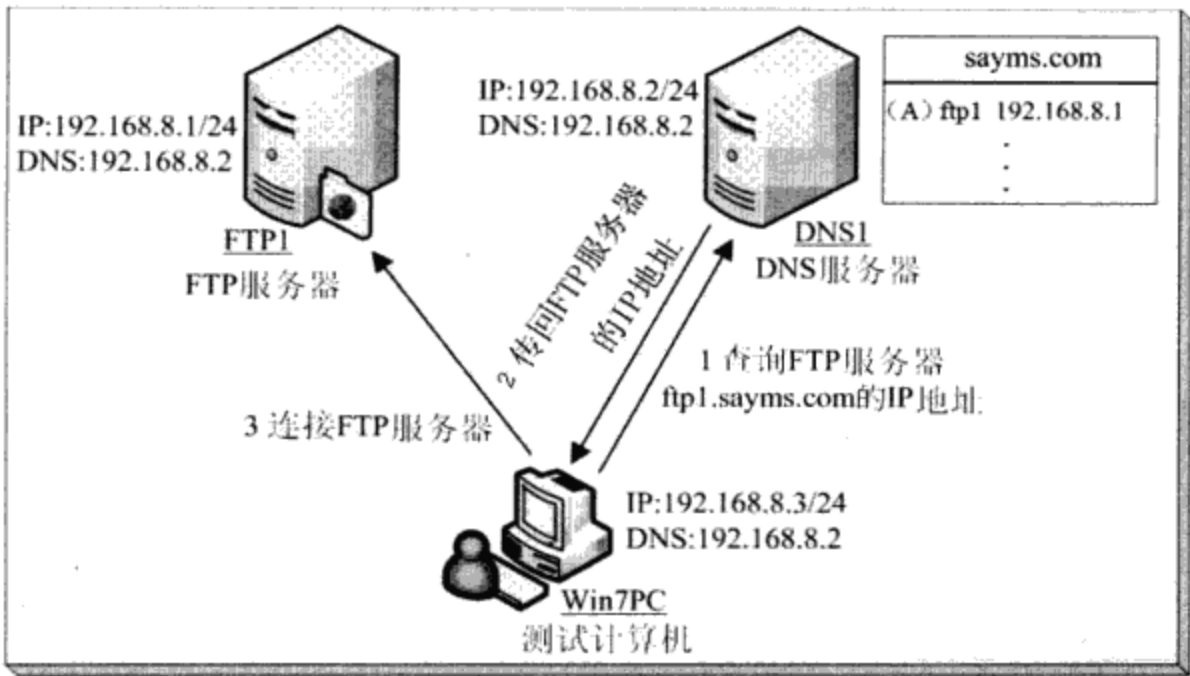




图 9-1



#### 提示

若要简化测试环境的话，可以将FTP与DNS服务器都架设到同一台计算机。若要再简化的话，可以撤销DNS服务器，然后将FTP服务器的网址与IP地址输入到测试计算机Win7PC的Hosts文件内（见第4章的说明）。

- **FTP服务器FTP1的设置：**它是Windows Server 2008 R2，请按照图 9-1来设置其IP地址与首选DNS服务器的IP地址（图中采用TCP/IPv4）。

- **DNS服务器DNS1的设置:** 它是Windows Server 2008 R2, 请按照图 9-1来设置其IP地址、首选DNS服务器的IP地址, 然后通过【单击左下角**服务器管理器**图标  角色  添加角色】的方法安装好DNS服务器, 并在其内新建一个名为sayms.com的正向查找区域, 然后在此区域内新建FTP服务器的主机记录, 如图 9-2中的ftp1.sayms.com、其IP地址为192.168.8.1。

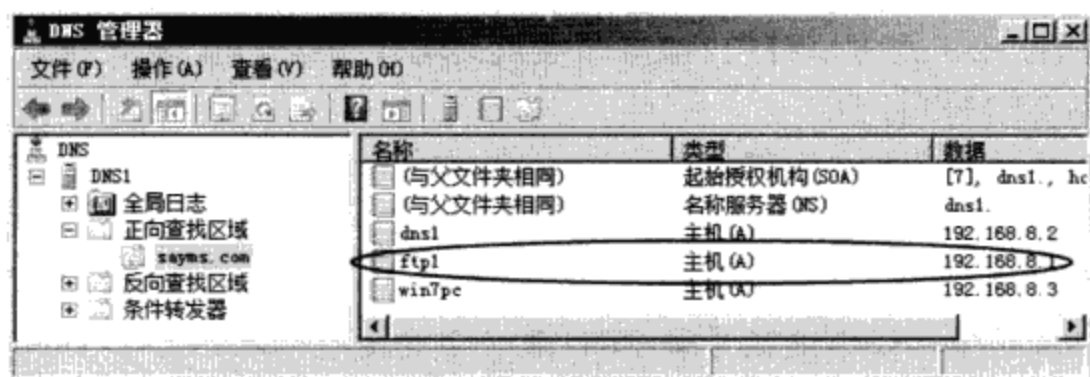




图 9-2

- **测试计算机Win7PC的设置:** 请按照图 9-1来设置其IP地址、首选DNS服务器的IP地址。图中为了让此计算机能够解析到FTP服务器ftp1.sayms.com的IP地址, 因此将其首选DNS服务器直接指定到DNS服务器192.168.8.2。请在此计算机上【按 **Windows** + **R** 键  输入CMD后按 **Enter** 键  如图 9-3所示用ping命令来测试是否可以解析到ftp1.sayms.com的IP地址】, 图中为成功解析到IP地址的界面。

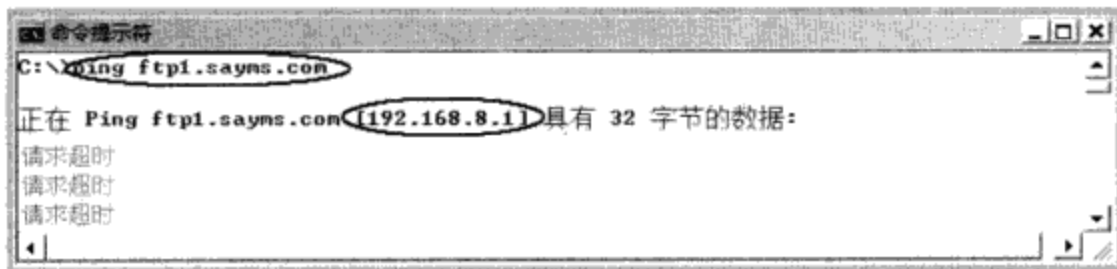


图 9-3



#### 提示

因Windows Server 2008 R2计算机默认已经打开**Windows防火墙**, 它会阻止ping命令的数据包, 故会出现界面中**请求超时**的信息。

## 9-1-2 安装FTP服务与新建FTP站点







我们要通过以下方法来安装FTP服务器角色服务: 【单击左下角**服务器管理器**图标  单击**角色**界面右边的**添加角色**  单击**下一步**  如图 9-4所示选择**网页服务器 (IIS)**  单击**下一步**  如图 9-5所示选择**FTP服务器**  ...】。



图 9-4

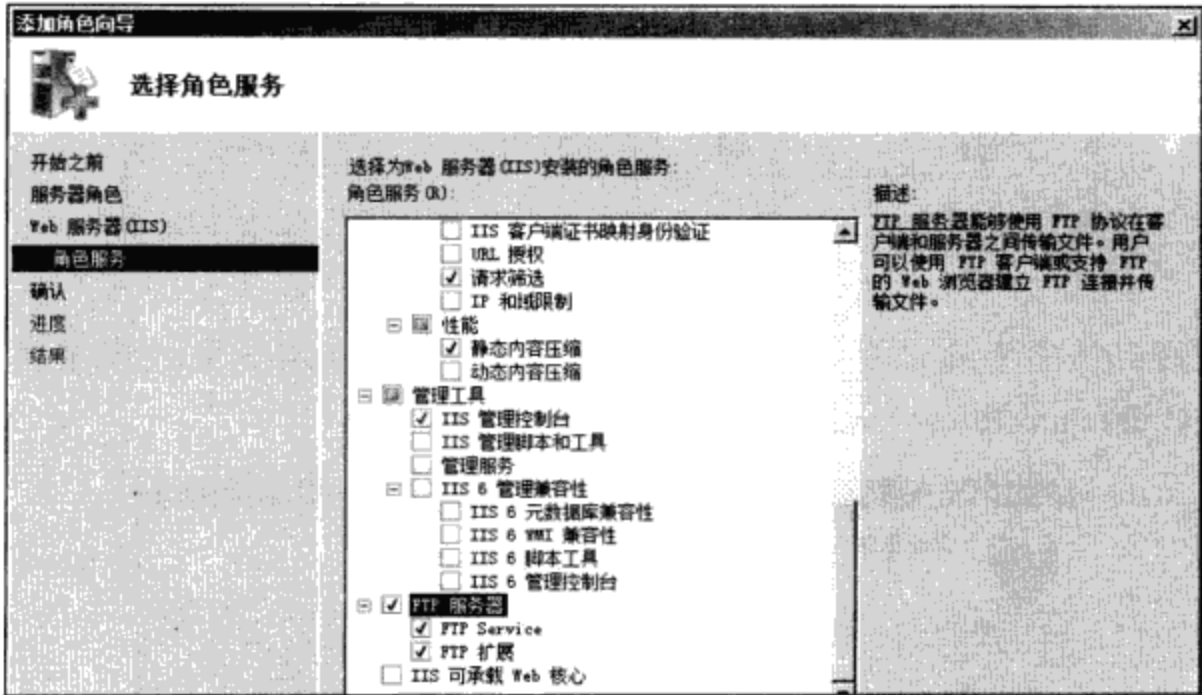


图 9-5

### 新建新的FTP站点

我们即将新建第1个FTP站点，站点需要一个用来存储文件的文件夹，也就是需要一个主目录（home directory），此处我们将利用内置的C:\inetpub\ftproot文件夹来作为站点的主目录，请随意复制几个文件到此文件夹内，以供测试时使用，如图 9-6所示。

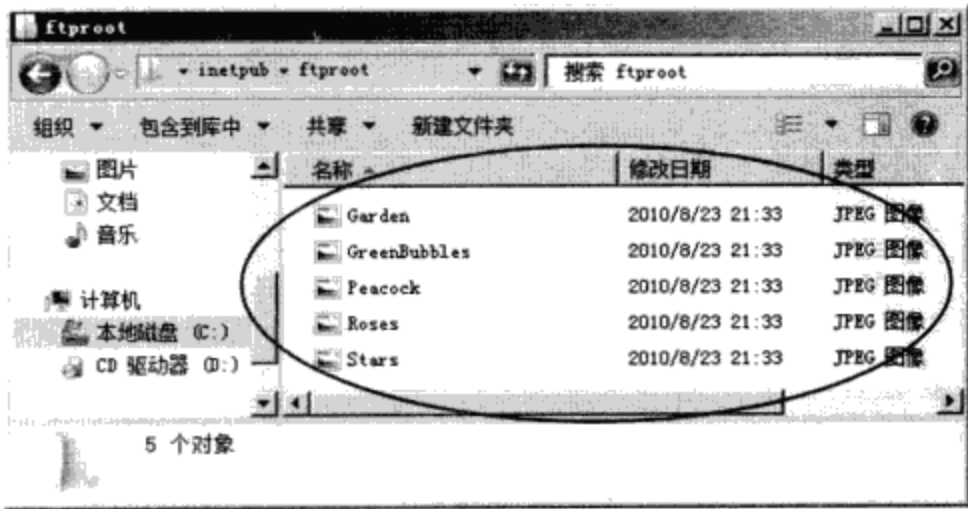


图 9-6



### 提示

此文件夹默认是赋与Users组**读取**的权限，有需要的话，请自行更改权限设置。

新建FTP站点的步骤如下所示：

**STEP 1** 开始 管理工具 Internet 信息服务 (IIS) 管理器。

**STEP 2** 如图 9-7所示单击**网站**右边的**添加FTP站点...**。



图 9-7

**STEP 3** 在图 9-8中为此站点取一个友好的名称、输入或浏览到代表主目录的文件夹（C:\inetpub\ftproot）后单击**下一步**。

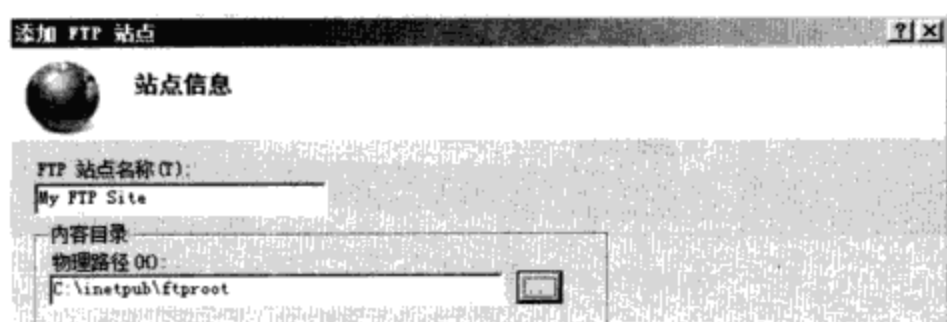


图 9-8

**STEP 4** 在图 9-9中将最下方**SSL**选项改为选择**无**后单击**下一步**。图中并未指派特定IP地址给此站点、端口号为默认的21、让FTP站点自动启动。由于FTP站点尚未拥有SSL证书，故最后一个选项选择**无**。

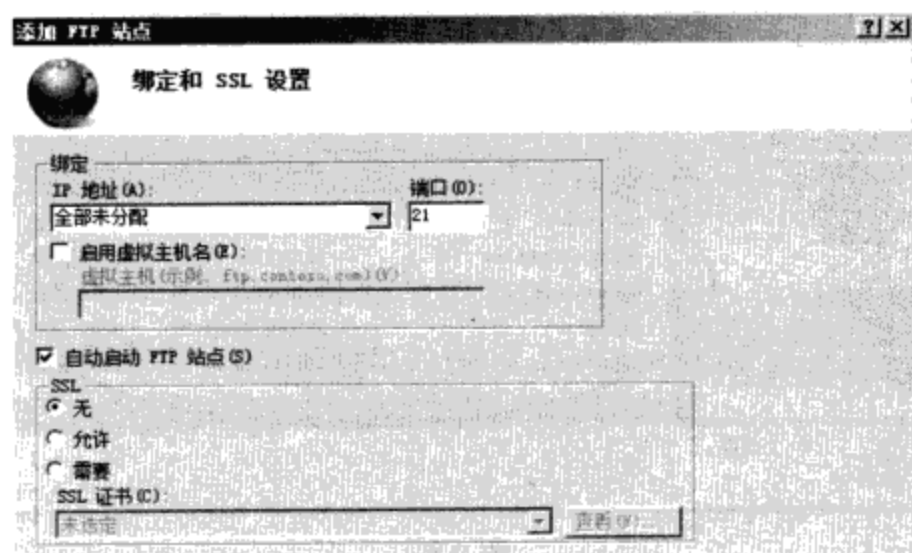


图 9-9

**STEP 5** 在图 9-10中假设同时选择匿名与基本身份验证方式、开放所有用户拥有读取权限后单击**完成**。

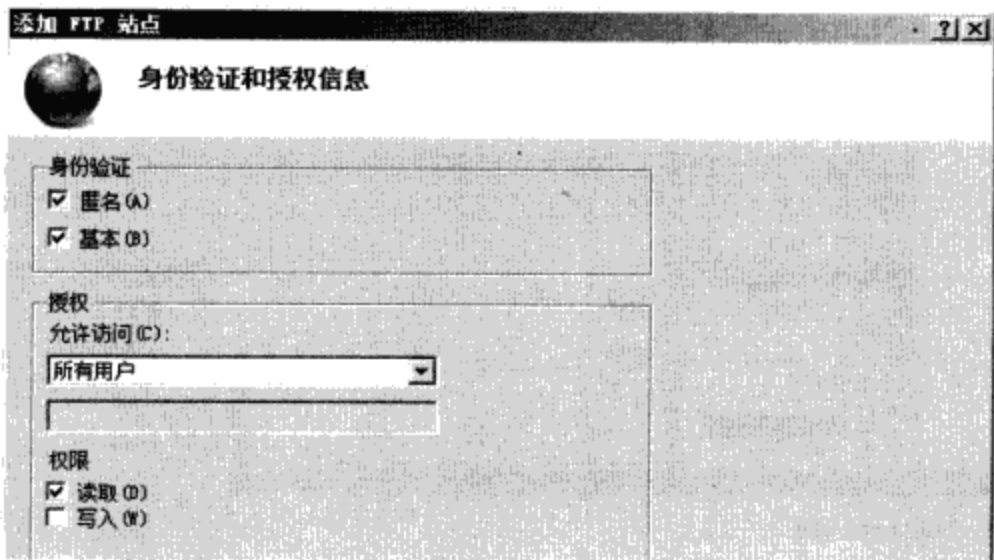


图 9-10

**STEP 6** 图 9-11为完成后的界面。您可以通过单击下方的**内容视图**或右边的**浏览**来查看主目录内的文件；您还可以通过右边的**重新启动**、**启动**、**停止**来更改FTP站点的启动状态。



图 9-11

### 新建集成到网站的FTP站点

您也可以新建一个集成到网站的FTP站点，这个FTP站点的主目录就是网站的主目录，此时您只需要通过同一个站点来同时管理网站与FTP站点。例如若要新建一个被集成到网站 Default Web Site 的新FTP站点的话，则其方法为单击图 9-12后图中**Default Web Site**右边的**添加 FTP发布...**，接下来大致上都跟之前新建My FTP Site站点的步骤相同，不过并不需要指定FTP

站点的主目录，因为它与**Default Web Site**相同（一般是C:\inetpub\wwwroot），还有因为之前我们已经新建了My FTP Site站点（端口号为21），因此图 9-12中的IP地址、端口号（Port）与虚拟主机名（Virtual Host Name）等3个设置值至少要有一个与My FTP Site不同，否则此新FTP站点无法被启动，故图 9-12中我们将其端口号由默认的21改为21222。

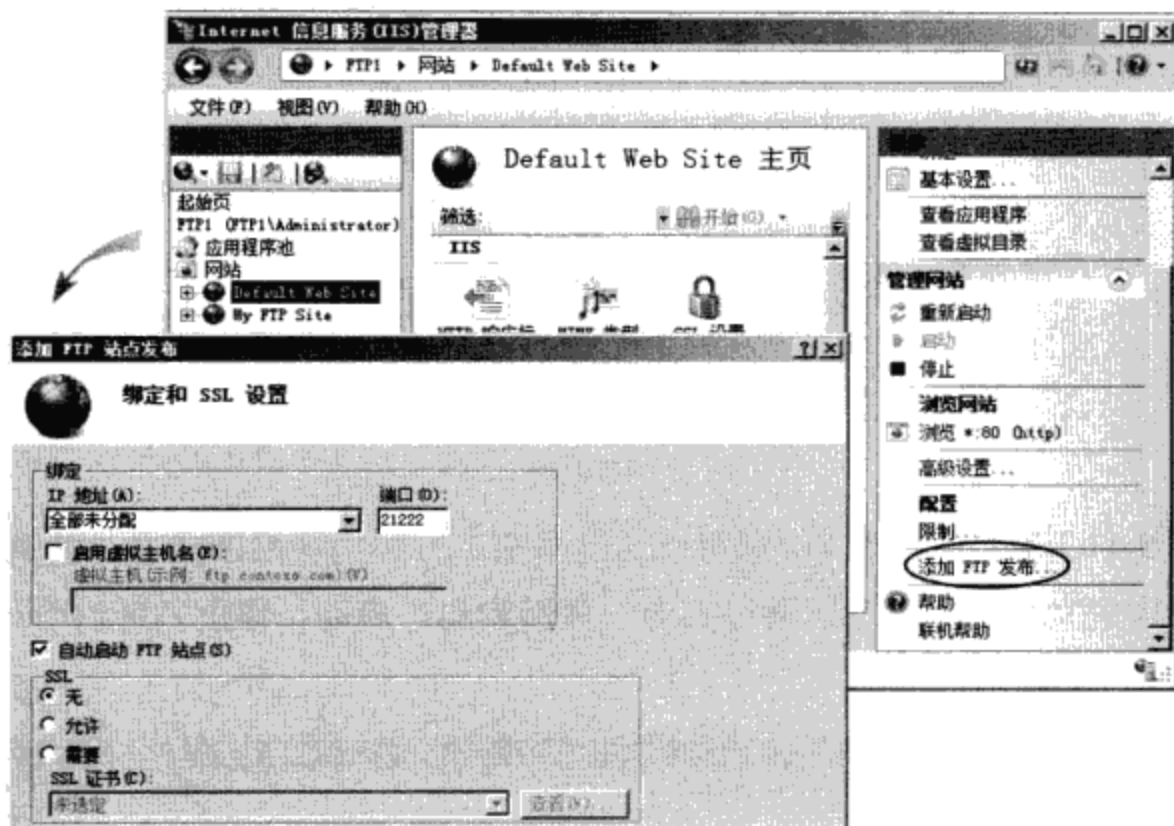


图 9-12

图 9-13后图为集成完成后的界面，由图中可看出我们可以通过**Default Web Site**来同时管理FTP站点与IIS网站。在单击右边的**绑定**后，可从前图看到它同时绑定到端口80(网站)与21222 (FTP服务器)。



图 9-13



### 9-1-3 测试FTP站点是否架设成功

我们即将到测试计算机Win7PC上来连接FTP站点My FTP Site, 不过因为FTP服务器的Windows防火墙会阻挡FTP的相关流量, 因此请先将Windows防火墙关闭: 到FTP服务器上选择【开始→控制面板→系统和安全→Windows防火墙→单击打开或关闭Windows防火墙→根据所在网络位置来选择关闭Windows防火墙(不推荐)后单击**确定**】。您可以到测试计算机Win7PC上利用以下所介绍的三种方式来连接FTP站点。



#### 提示

虽然FTP服务器安装完成后, 系统默认会在Windows防火墙内自动新建规则来开放与FTP有关的流量, 但这些规则实际上并没有发挥作用(除非这台FTP服务器有加入Active Directory域), 因此我们必须另外新建规则来开放, 不过因为FTP的运行过程较复杂, 因此Windows防火墙的设置也比较麻烦, 故此处请暂时将Windows防火墙完全关闭, 章节9-6内会对其做详细的分析, 到时再来对Windows防火墙做适当的设置。

#### 利用内置的FTP客户端连接程序ftp.exe

请打开**命令提示符**, 然后通过以下三种方式之一来连接FTP站点:

- 运行ftp ftp1.sayms.com
- 运行ftp 192.168.8.1
- 运行ftp ftp1

其中ftp1.sayms.com是FTP站点注册在DNS服务器内的网址、192.168.8.1是其IP地址、ftp1是其计算机名。图 9-14中我们利用ftp ftp1.sayms.com来连接FTP站点, 在**用户**处输入匿名账户anonymous, **密码**处随意输入即可(建议输入您的电子邮件账号)或直接按**Enter**键。进入ftp提示符的环境后(ftp>), 如图所示可以利用dir命令来查看FTP主目录内的文件, 这些文件是之前随意从其他地方复制过来的。

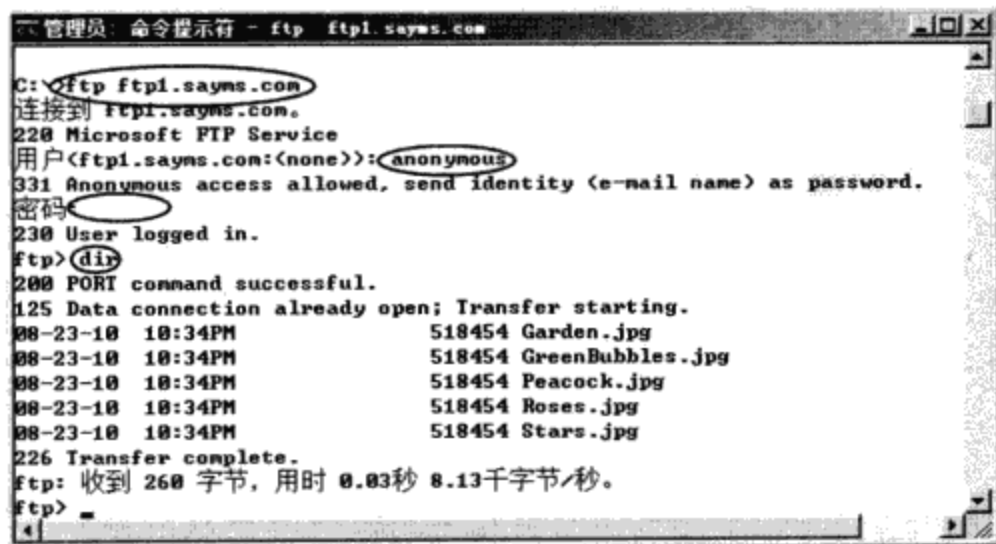


图 9-14



您也可以利用FTP服务器的本地用户账户或Active Directory用户账户（若FTP服务器有加入Active Directory域的话）来连接FTP站点。

在ftp提示符下可以利用?命令来查看可供使用的命令。若要中断与FTP站点的连接的话，请利用bye或quit命令。

### 利用Windows资源管理器

您可以直接通过**Windows 资源管理器**来连接FTP站点，而连接时可以利用网址、IP地址或计算机名，例如通过【开始 单击**计算机** 在图 9-15中输入ftp://ftp1.sayms.com】的方法，它会自动利用匿名来连接FTP站点。从界面中可看到位于FTP站点主目录内的文件。

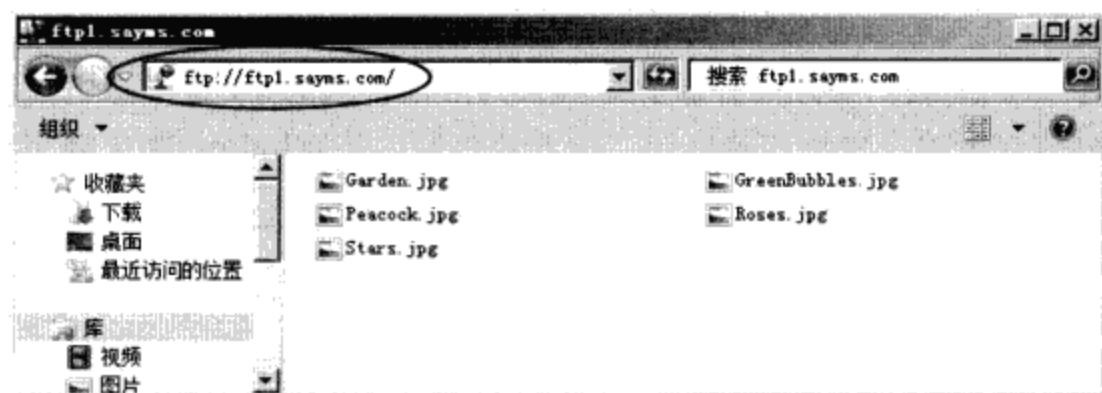


图 9-15

### 利用浏览器Internet Explorer

您也可以通过浏览器Internet Explorer来连接FTP站点，而连接时可以利用网址、IP地址或计算机名，例如图 9-16中是利用网址ftp://ftp1.sayms.com/来连接FTP站点，而且它是自动利用匿名来连接FTP站点。从界面中可看到位于FTP站点主目录内的文件。



图 9-16

您也可以在图 9-17中【选择**网页菜单** 选择在**Windows资源管理器**中打开FTP站点】，以便改用**Windows 资源管理器**来查看FTP站点内的文件。



注意

若未关闭FTP服务器的Windows 防火墙的话，将无法连接FTP站点。

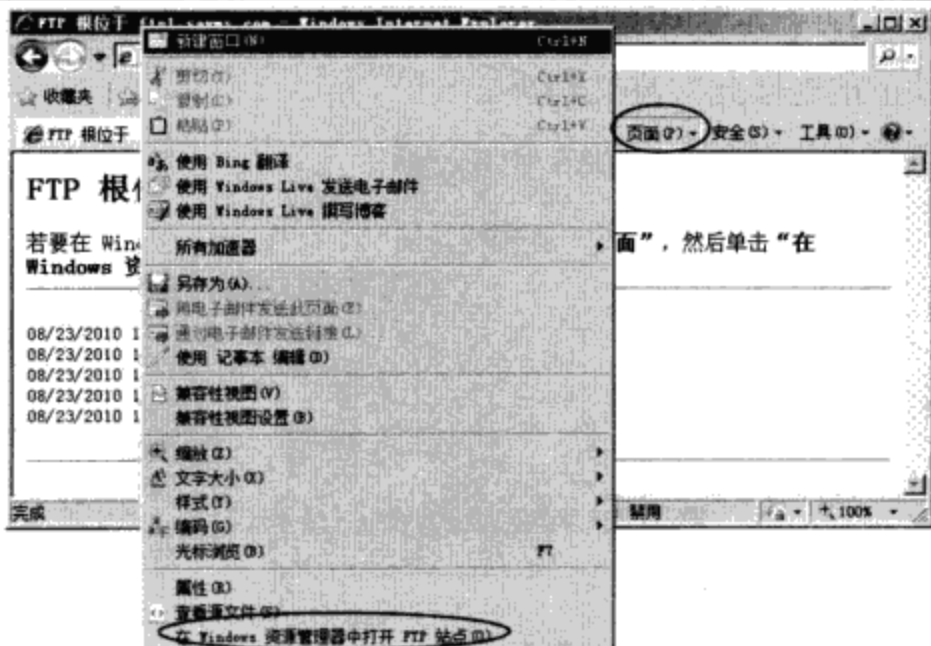


图 9-17

## 9-2 FTP站点的基本设置

本节将介绍以下的主题：主目录与目录列表样式、站点绑定、站点信息、验证设置、授权设置、查看当前连接的用户、通过IP地址与域名来限制连接等。

### 9-2-1 文件存储地点

当用户使用ftp://ftp1.sayms.com/来连接FTP站点时，他将被导向到FTP站点的主目录，也就是用户所看到的文件是存储在主目录内的文件。要查看FTP站点主目录的话，请【如图 9-18 所示单击My FTP Site右边的基本设置...通过前图中物理路径来查看】。

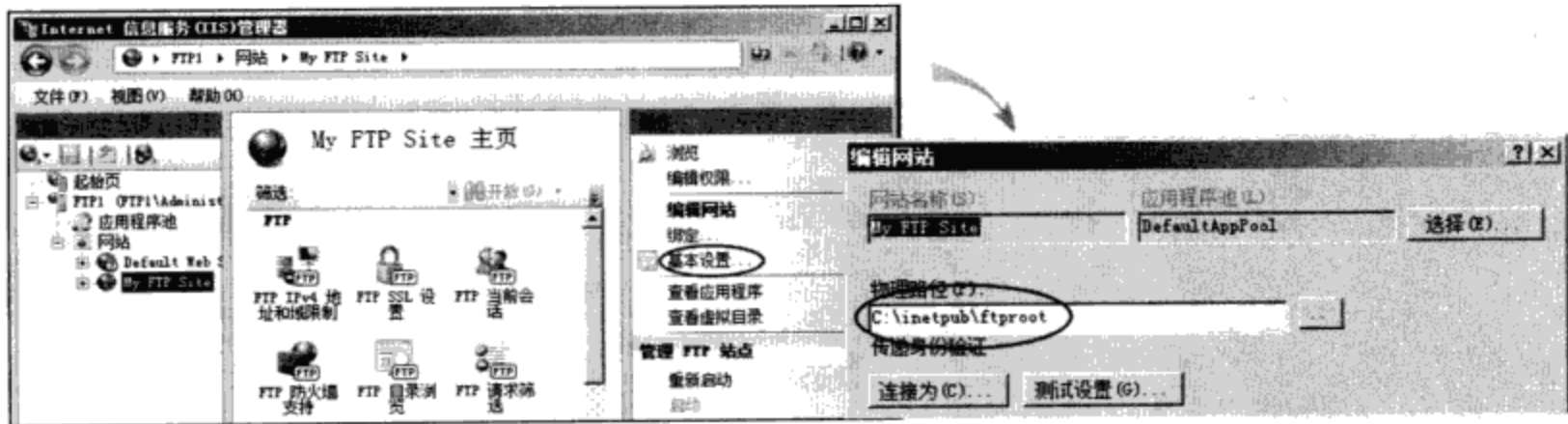


图 9-18

您可以将主目录的物理路径更改到本地计算机的其他文件夹。您也可以将它设置到网络上

其他计算机的共享文件夹内，不过FTP站点必须提供有权限访问此共享文件夹的用户名与密码：【如图 9-19所示在**物理路径**处输入网络共享文件夹，单击**连接为**，单击**设置**，输入网络计算机内的用户名与密码】，例如图中的用户名为administrator。完成后建议通过后图中的**测试设置**来测试是否可以正常连接此共享文件夹。

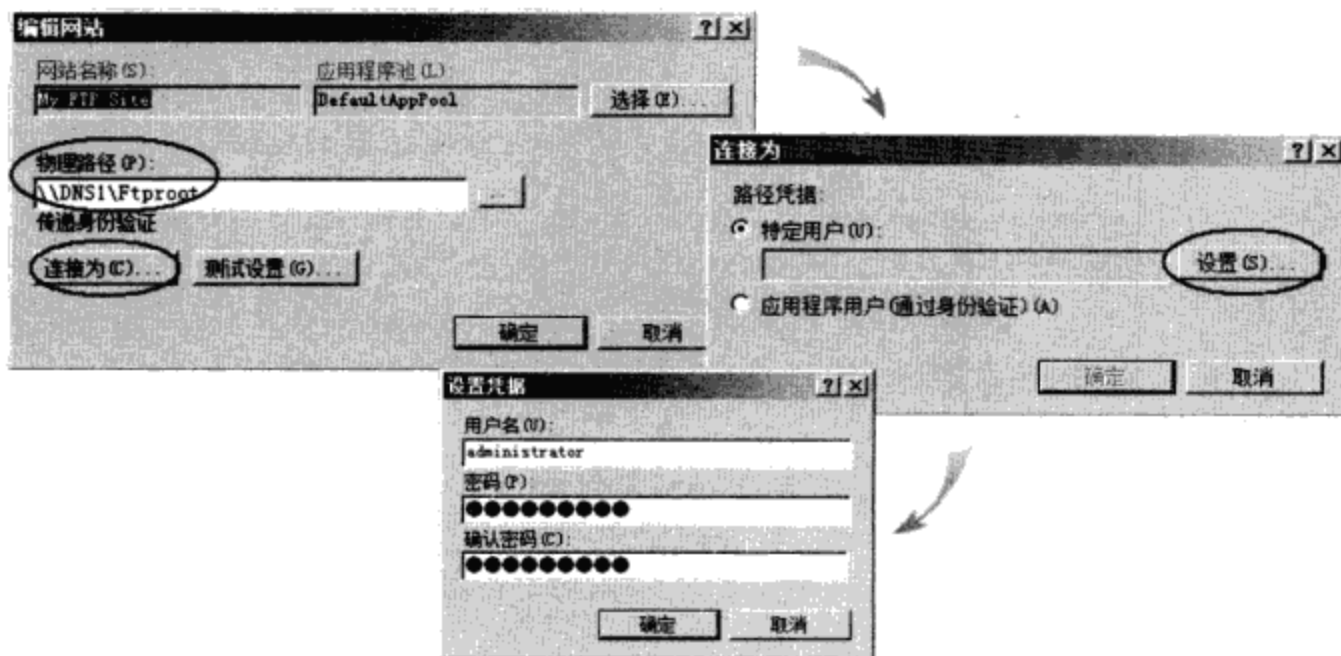


图 9-19



#### 提示

您也可以通过【单击My FTP Site右边的高级设置...，物理路径】来设置主目录。

## 9-2-2 目录列表样式

用户在查看FTP站点内的文件时，其界面上所显示的文件列表格式分为MS-DOS与UNIX两种格式，可通过【单击图 9-20中的My FTP Site中的FTP目录浏览，在目录列表样式中】来选择：



图 9-20

➤ **MS-DOS格式**: 这是默认值, 如图 9-21所示是利用ftp.exe的dir命令所看到的示例界面。

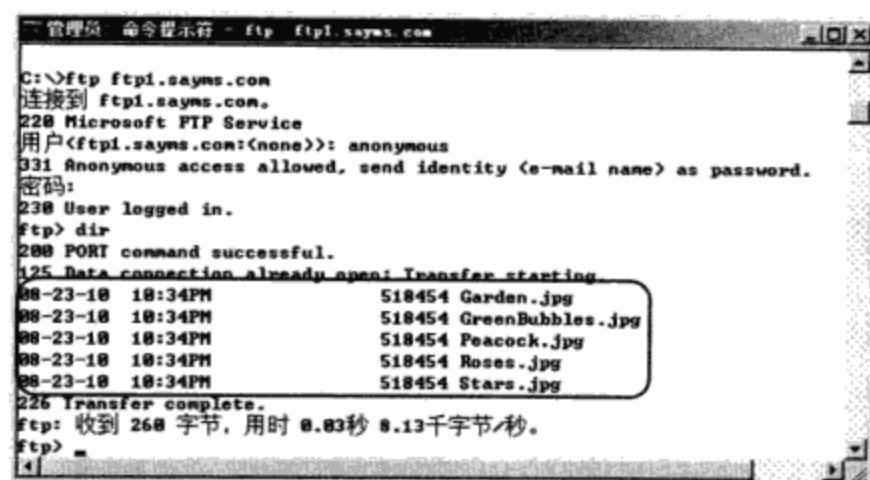


图 9-21

➤ **UNIX格式**: 如图 9-22所示。



图 9-22



**提示**

用户若使用浏览器Internet Explorer或Windows资源管理器来连接的话, 则其显示文件的方式并不会受到目录列表样式设置的影响。

另外图 9-20中还可以通过目录列表选项来设置是否要显示虚拟目录、FTP站点的磁盘剩余可用空间 (参见图 9-23) 与是否用4个字符来显示公元年 (例如2010年)。



图 9-23



## 提示

若使用浏览器Internet Explorer或Windows资源管理器来连接的话，则公元年一律自动用4个字符来显示，不受上述设置的影响。

### 9-2-3 FTP站点的绑定设置

您可以在一台计算机内建立多个FTP站点，为了能够正确区分出这些FTP站点，必须给予每一个站点唯一的识别信息，可用来识别站点的识别信息有**虚拟主机名**、**IP地址**与**TCP端口号**，即这台计算机内所有FTP站点的这3个识别信息不可以完全相同。

若要更改FTP站点的这3个设置值的话，可如图9-24所示【单击FTP站点右边的**绑定...**单击**编辑**通过前图来设置】，由图中可看出FTP站点默认的端口号为21。

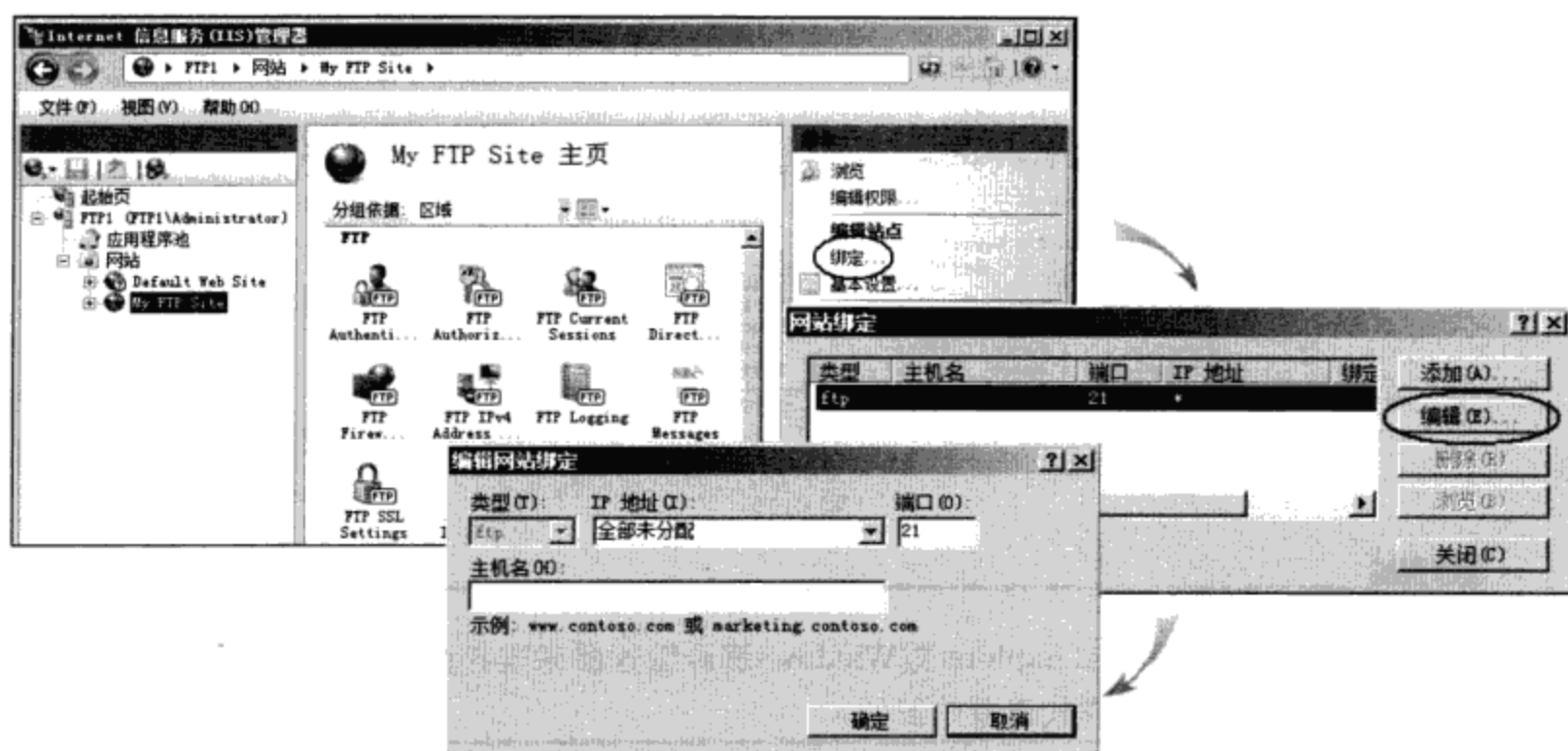


图 9-24

您可以更改默认端口号，那么用户若要连接此站点就必须自行输入对应端口号，例如若将端口号改为2121的话，假设用户通过ftp.exe程序来连接此FTP站点的话，需在ftp>提示符下执行**open ftp1.sayms.com 2121**命令，如图9-25所示。

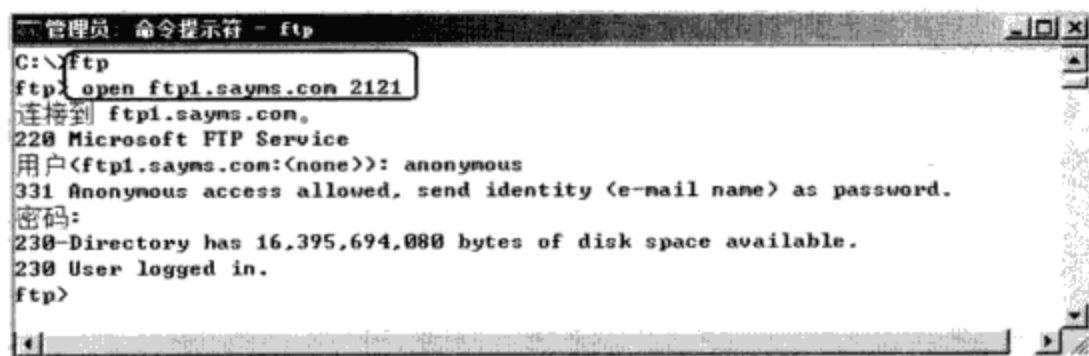


图 9-25

如果用户是利用浏览器Internet Explorer（或Windows资源管理器）来连接FTP站点的话，则请如图 9-26所示输入ftp://ftp1.sayms.com:2121/。完成练习后，请将端口号恢复为21。

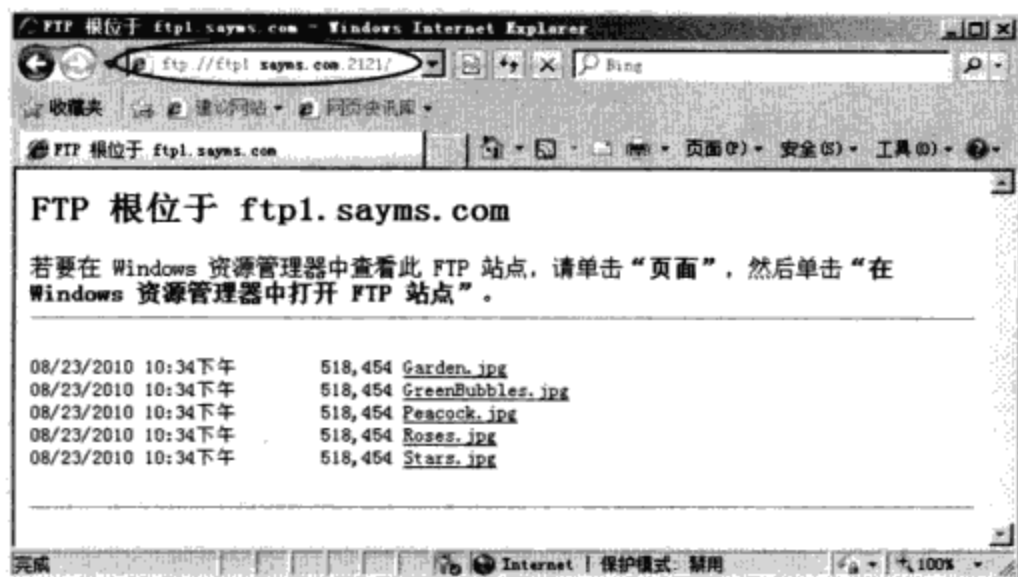


图 9-26

若要连接之前我们所新建的另外一个FTP站点的话（与Default Web Site集成的站点，端口号为21222），则连接方法也是一样，但是需将端口号改为21222。

#### 9-2-4 FTP站点的信息设置

我们可以为FTP站点设置一些显示信息，用户连接FTP站点时就会看到这些信息，以My FTP Site来说，其设置方法为【如图 9-27所示单击My FTP Site中间的FTP消息在FTP消息页面中输入相应消息正文后单击应用】：

##### ┇ 横幅

用户连接FTP站点时，会先看到此处的文字。

##### ┇ 欢迎使用

当用户登录到FTP站点后，会看到这些欢迎词。

##### ┇ 退出

当用户注销时会看到这些欢送词。

##### ┇ 最大连接数

若FTP站点有连接数量限制，而且目前连接的数目已经到达限制值的话，则其后连接FTP站点的用户，将看到此处所设置的信息。

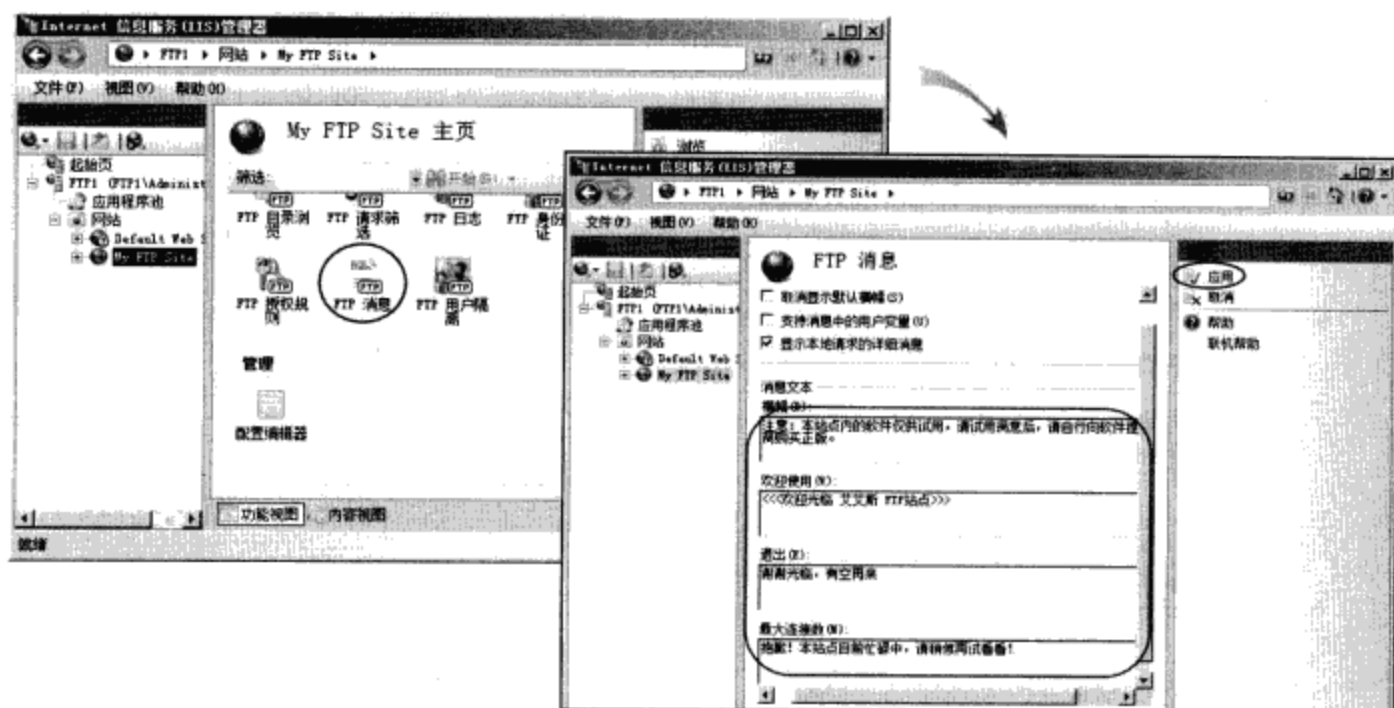


图 9-27

完成以上设置后，用户利用ftp.exe程序来连接时，将看到类似图 9-28所示的界面。



#### 提示

如果利用浏览器Internet Explorer来连接此FTP站点的话，并不会看到以上信息；若利用颇受欢迎的CuteFTP或SmartFTP等软件来连接此FTP站点的话，就可以看到这些消息。

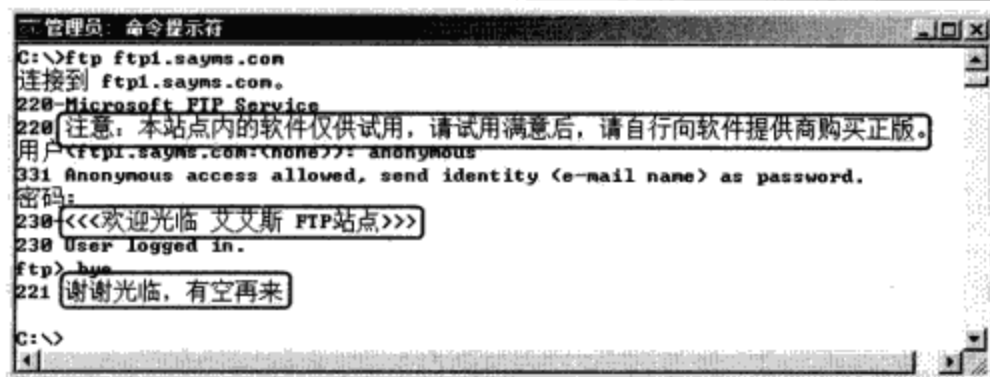


图 9-28

若FTP站点的连接数目已经达到最大数目的话，此时用户来连接此FTP站点，将看到如图 9-29所示的界面。

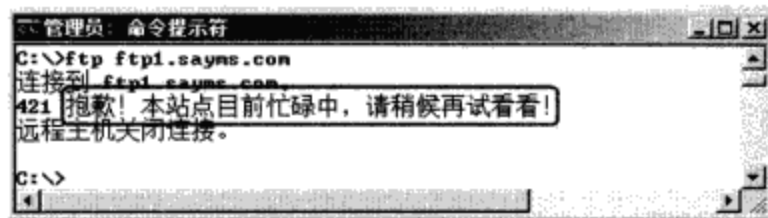


图 9-29



#### 提示

如果利用浏览器Internet Explorer来连接此FTP站点的话，并不会看到以上信息，而会出现要求输入用户名与密码的界面。



如果您要练习看到图 9-29界面的话，可以先将连接到FTP站点的最大连接数量限制为1，然后同时开启两个**命令提示符**窗口来连接FTP站点，就可以看到此界面。限制连接数量的设置方法为：**【如图 9-30所示单击My FTP Site右边的高级设置...展开前图中的连接将最大连接数设置为1】**。练习完后，将此数值改回原设置值或适当值。

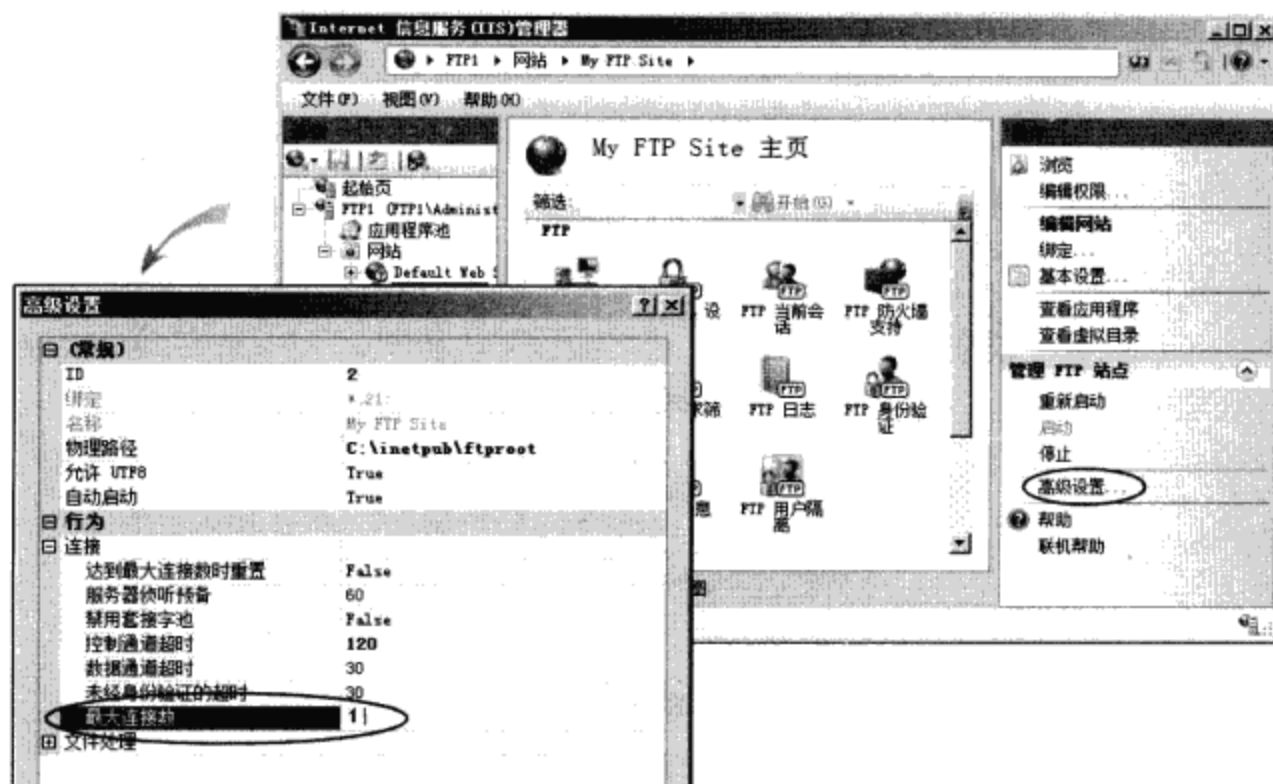


图 9-30

FTP消息页面上方还有以下三个选项（见图9-31）：

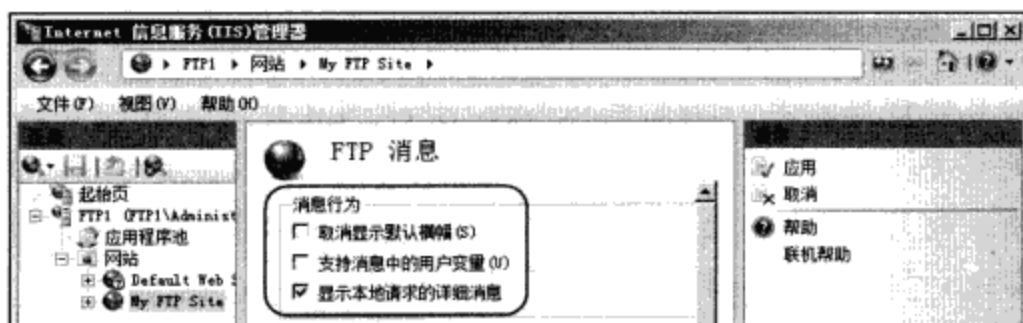


图 9-31

✎ 取消显示默认横幅：也就是不显示图 9-32中 Microsoft FTP Service文字。

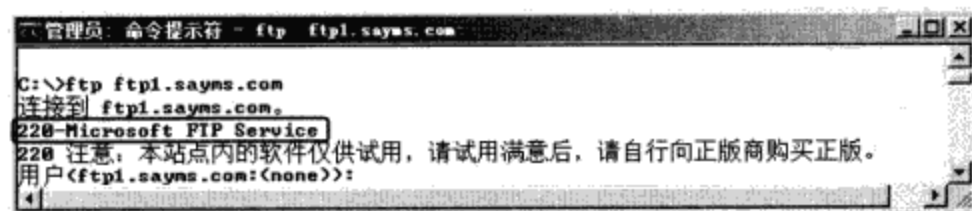


图 9-32

✎ 支持消息中的用户变量：支持在消息中使用变量，这些变量包含：

- %BytesReceived%：此次连接中，从服务器传给客户端的字节数。
- %BytesSent%：此次连接中，从客户端传给服务器的字节数。

- %SessionID%: 此次连接的标识符。
- %SiteName%: FTP站点的名称。
- %UserName%: 用户名称。

例如若FTP站点的消息设置是如图 9-33所示, 则用户 george连接到FTP站点时, 其所看到的界面将如图 9-34所示。



图 9-33

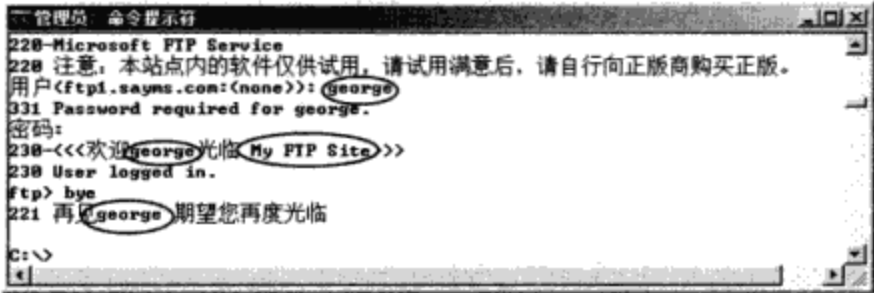


图 9-34

➤ **显示本地请求的详细信息:** 设置当从本地 (FTP站点自己这台计算机) 来连接FTP站点有误时, 是否要显示详细的错误信息。举例来说, 假设FTP站点的主目录因故无法访问 (例如被误删), 则从本地连接FTP站点时, 会有如图 9-35所示的的详细信息。注意若您是从其他计算机来连接FTP站点的话, 就不会看到这些信息。

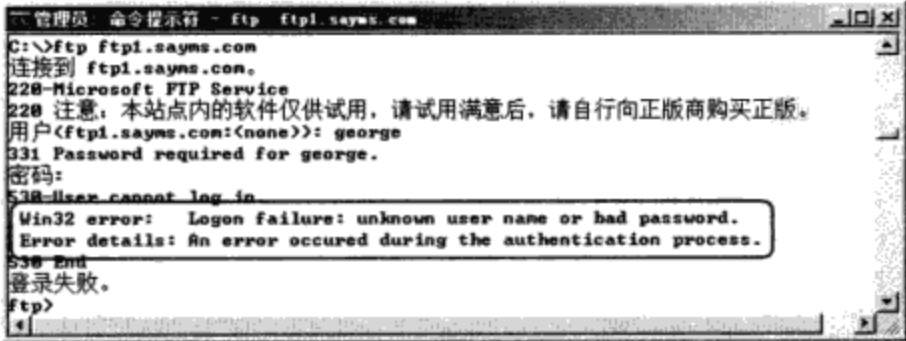


图 9-35

### 9-2-5 验证用户名与权限设置

您可以如图 9-36所示单击My FTP Site中间的FTP身份验证, 以便来设置如何验证用户的身

份，图中启用匿名身份验证与基本身份验证，它们是在新增此FTP站点时就已经选择的方法（参见前面图 9-10），关于它们的介绍与网站相同，因此请参考第5章的说明，此处不再重复。

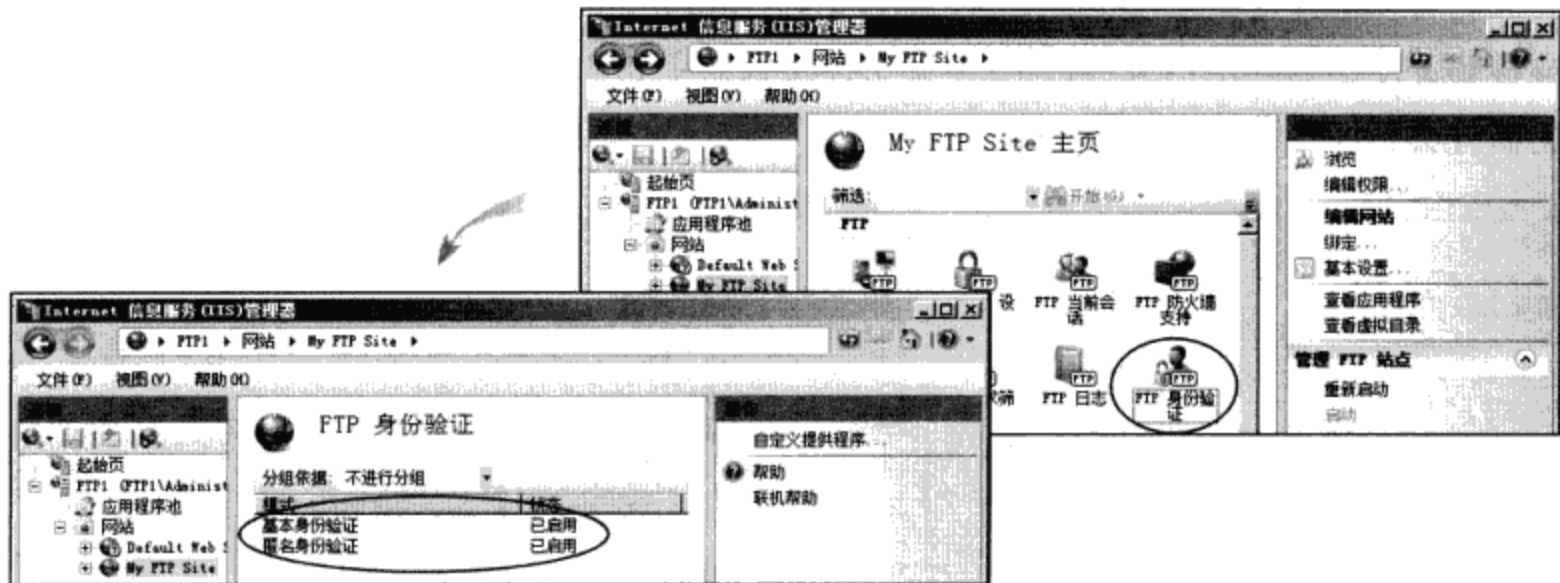


图 9-36

我们之前新建FTP站点时已经设置所有用户对FTP站点的访问权限为**读取**（参见前面图 9-10），若您要更改此权限的话，请【如图 9-37所示单击My FTP Site中间的FTP授权规则选择中间的授权规则单击右边的**编辑...**通过图 9-38来设置】。



图 9-37

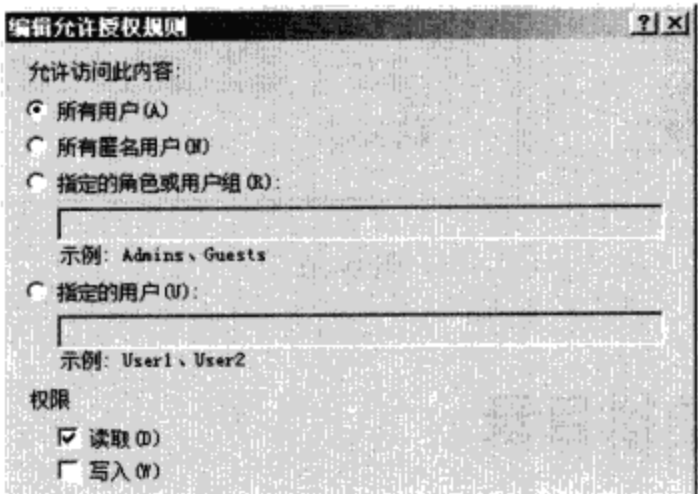


图 9-38

## 9-2-6 查看当前连接的用户

您可以选择【如图 9-39所示单击My FTP Site中间的FTP当前会话通过前图来查看目前连接到 FTP站点的用户】，若您要将某个连接强制中断的话，只要选择该连接后，再单击右边的断开会话即可。

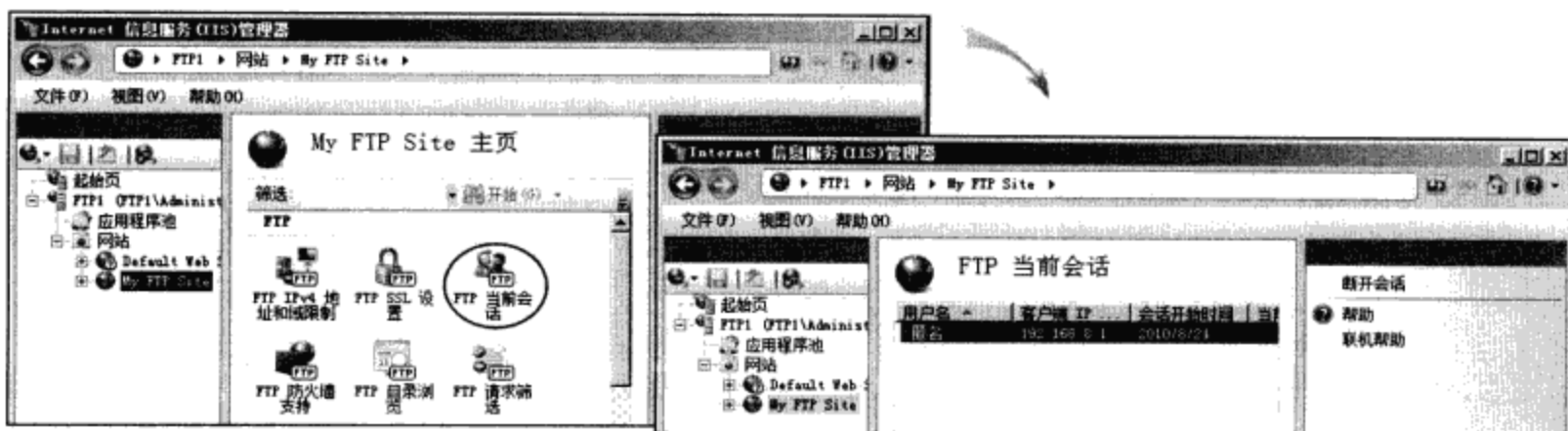


图 9-39



### 提示

一个已没有任何操作的连接，默认会在120秒后被自动中断，若要更改此默认值的话，可通过图 9-30前图中的控制通道超时来设置。

## 9-2-7 通过IP地址来限制连接

您可以让FTP站点允许或拒绝某台特定计算机或某一群计算机的连接，其设置方法为【如图 9-40所示单击My FTP Site中间的FTP IPv4地址和域限制通过前图来设置】，其设置原理与网站类似（见第5章的说明）。

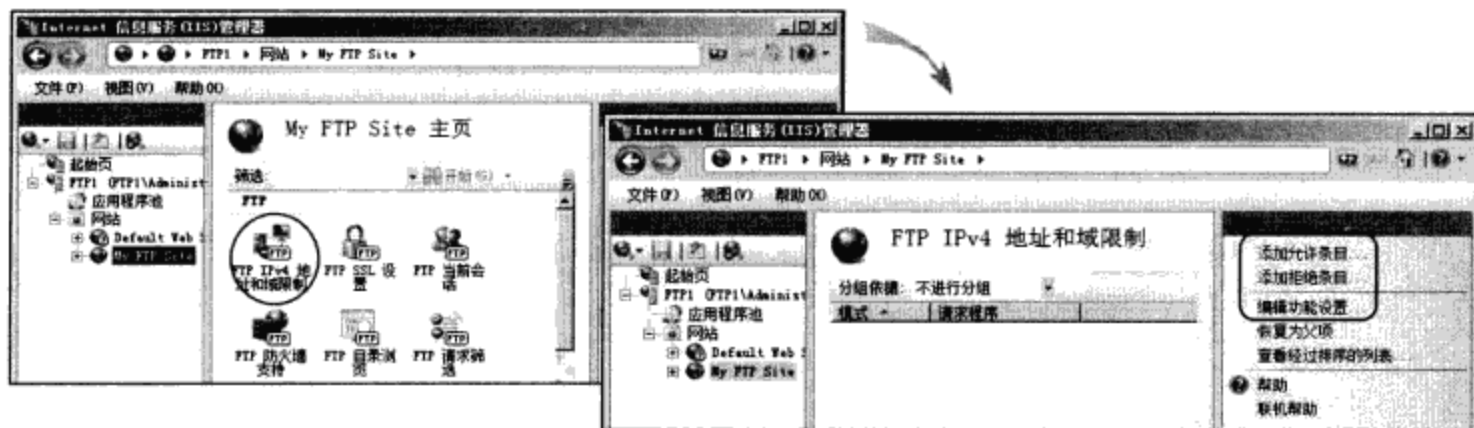


图 9-40

## 9-3 物理目录与虚拟目录

您可能需要在FTP站点的主目录下新建多个子文件夹，然后将文件存储到主目录与这些子

文件夹内，这些子文件夹被称为**物理目录**。

您也可以将文件存储到其他地点，例如本地计算机其他磁盘驱动器内的文件夹，或是其他计算机的共享文件夹，然后通过**虚拟目录**（virtual directory）来对应到这个文件夹。每一个虚拟目录都有一个**别名**（alias），用户通过别名来访问这个文件夹内的文件。虚拟目录的好处是：无论您将文件的实际存储地点更改到何处，只要别名不变，用户都仍然可以通过相同的别名来访问到文件。

### 9-3-1 物理目录实例演练

假设我们如图 9-41 所示在主目录下（C:\inetpub\ftproot），新建一个名称为**工具程序**的子文件夹，然后复制一些文件到此文件夹内以便测试，之后我们便可以如图 9-42 所示【单击**My FTP Site**⇨单击**工具程序**⇨单击**内容视图**】来看到这些文件。



图 9-41

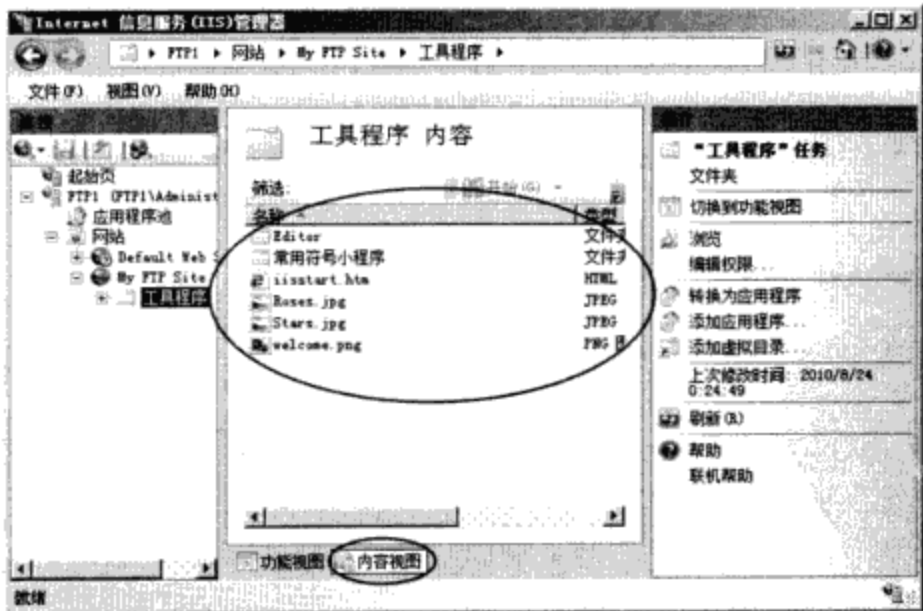


图 9-42

用户利用Internet Explorer连接到FTP站点后将看到如图 9-43 所示的界面。

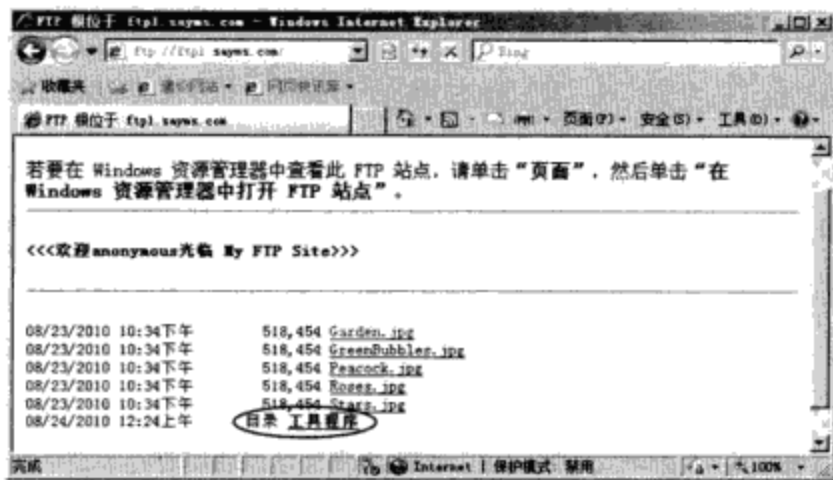


图 9-43

### 9-3-2 虚拟目录实例演练

如图 9-44所示我们在FTP站点计算机的C:\下新建一个名称为**儿童读物**的文件夹，然后复制一些文件到此文件夹内以便测试，将此文件夹设置为FTP站点的虚拟目录。

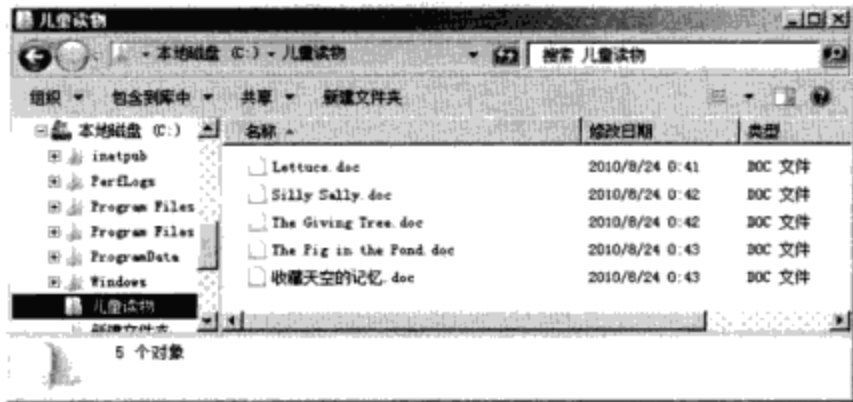


图 9-44

通过以下步骤来新建虚拟目录:【如图 9-45所示单击**My FTP Site**下方的**内容视图** 单击右方的**添加虚拟目录...** 在前图中输入别名（例如**儿童读物**） 输入或浏览到物理路径**C:\儿童读物** 单击**确定**】。



图 9-45



我们可以从图 9-46 的界面中看到 **My FTP Site** 下多了一个虚拟目录 **儿童读物**，同时在单击下方的 **内容视图** 后，便可以在图中间看到其内的文件。



图 9-46

您还需【单击 **My FTP Site** 下方的 **功能视图** 如图 9-47 所示单击 **FTP 目录浏览** 在前图中选择 **虚拟目录** 后单击 **应用**】，之后客户端才看得到此虚拟目录。

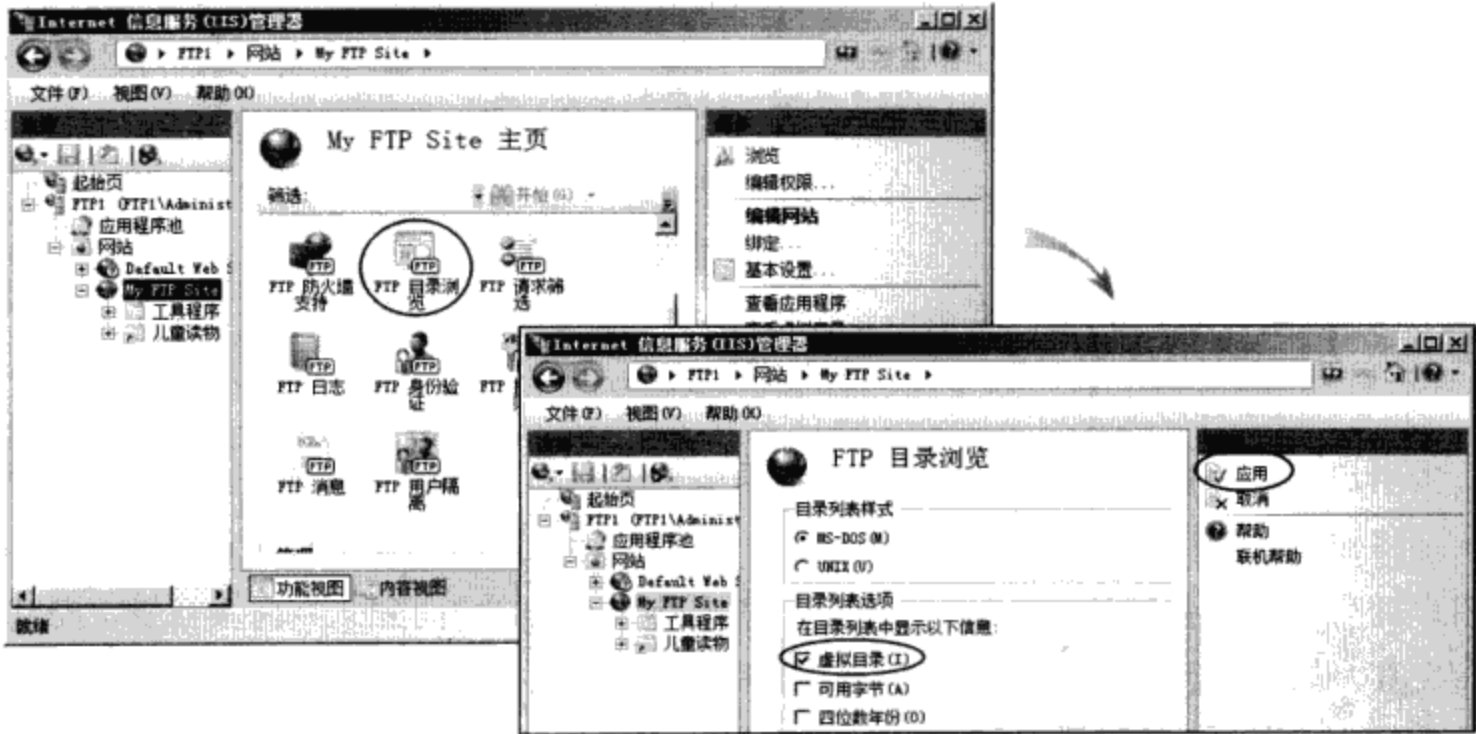


图 9-47

完成以上设置后，请到测试计算机 Win7 PC 上来连接 FTP 站点，此时应该可以如图 9-48 所示看到虚拟目录 **儿童读物**。



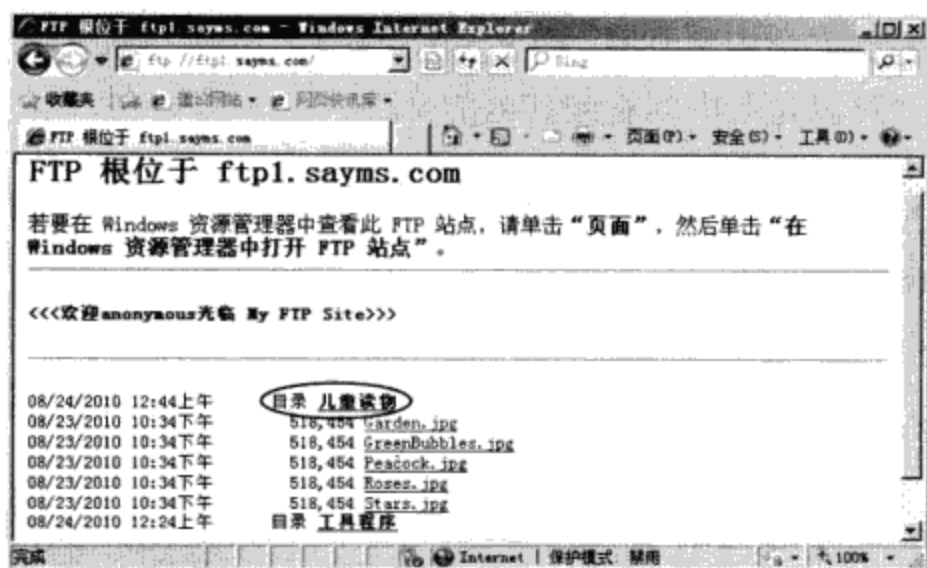


图 9-48

您可以通过单击图 9-49中虚拟目录**儿童读物**右边的**基本设置**来更改虚拟目录的物理路径，这些相关说明都与网站相同，请自行参考第5章的内容。

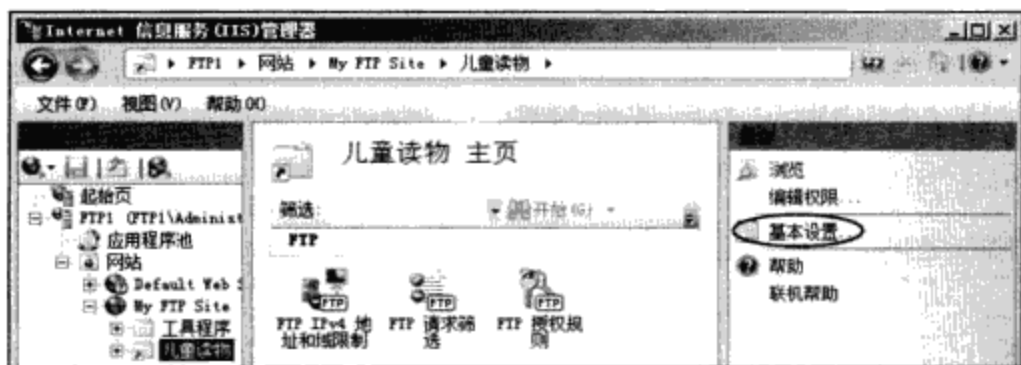


图 9-49

## 9-4 FTP站点的用户隔离设置

当用户连接FTP站点时，无论他们是利用匿名账户、还是利用一般账户来登录FTP站点，默认都将被导向到FTP站点的主目录，不过您可以利用**FTP用户隔离**（FTP user isolation）功能，让用户拥有其专属主目录，此时用户登录FTP站点后，会被导向到此专属主目录，而且可以被限制在其专属主目录内，也就是无法切换到其他用户主目录，因此无法查看或修改其他用户主目录内的文件。

**FTP用户隔离**的设置可通过如图 9-50所示【单击My FTP Site中间的**FTP 用户隔离**通过前图设置】的方法。



图 9-50

- **不隔离用户。**在以下目录中启动用户会话：它不会隔离用户，不过用户登录后的主目录并不相同：
  - **FTP根目录：**所有用户都会被导向到FTP站点的主目录（默认值）。
  - **用户名目录：**用户拥有自己的主目录，不过并不隔离用户，也就是只要拥有适当的权限，用户便可以切换到其他用户的主目录，因而可能可以查看、修改其内的文件。它所采用的方法是在FTP站点内建立目录名称与用户名相同的物理或虚拟目录，用户连接到FTP站点后，便会被导向到目录名称与用户名相同的目录。
- **隔离用户。**将用户局限于以下目录：它会隔离用户，用户拥有其专属主目录，而且会被限制在其专属主目录内，因此无法查看或修改其他用户的主目录内的文件。
  - **用户名目录（禁用全局虚拟目录）：**它所采用的方法也是在FTP站点内建立目录名称与用户名相同的物理或虚拟目录，用户连接到FTP站点后，便会被导向到目录名称与用户名相同的目录。用户无法访问FTP站点内的全局虚拟目录（后述）。
  - **用户名物理目录（启用全局虚拟目录）：**它所采用的方法是在FTP站点内建立目录名称与用户名称相同的物理目录，用户连接到FTP站点后，便会被导向到目录名称与用户名相同的目录。用户可以访问FTP站点内的全局虚拟目录。
  - **在Active Directory中配置的FTP主目录：**用户必须利用域用户账户来连接FTP站点。您需要在域用户的账户内指定其专属主目录。

### 9-4-1 不隔离用户，但是用户有自己的主目录

用户拥有自己的主目录，但并不隔离用户，因此只要用户拥有适当的权限（例如NTFS权限），他便可以切换到其他用户的主目录、查看或修改其内的文件。要让您的FTP站点启用这

种模式的话，请如图 9-51所示在图中间点选择用户名目录。

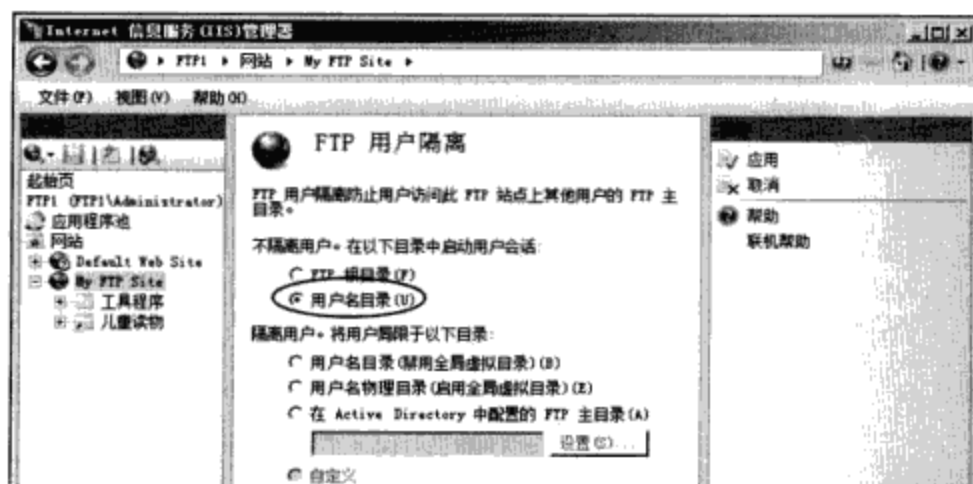


图 9-51

接下来需要新建目录名称与用户名相同的物理或虚拟目录，此处我们采用物理目录。假设我们要让用户George与Mary登录时被导向到自己的主目录，因此请如图 9-52所示在My FTP Site的主目录C:\inetpub\ftproot之下新建名称为george与mary两个子文件夹，并建议在这两个文件夹内分别放置一些文件，以便于测试。图中还新建了一个子文件夹default，利用匿名身份连接FTP站点的用户会被导向到此文件夹。

用户 George 与 Mary 登录 FTP 站点时会分别被导向到 C:\inetpub\ftproot\george 与 C:\inetpub\ftproot\mary 文件夹。

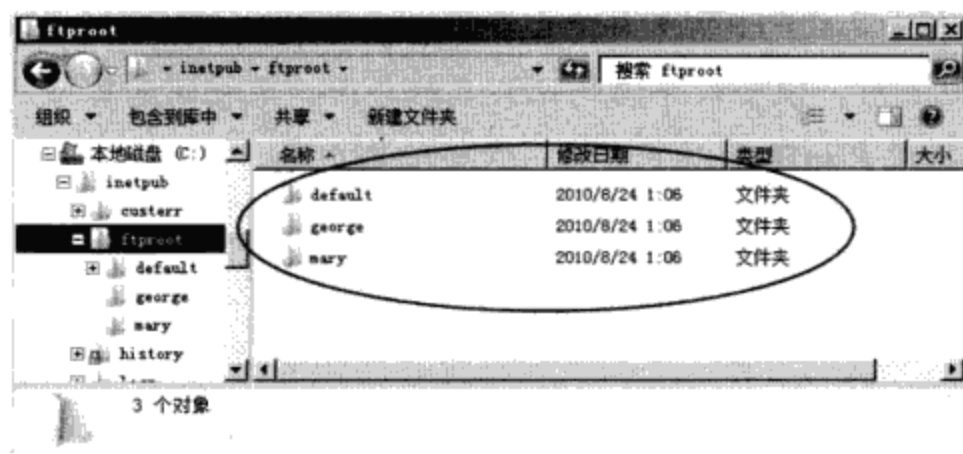


图 9-52



#### 提示

用户对其主目录的默认权限为**读取**，若要更改的话，请通过【单击图 9-53中的目录（例如george）➡单击中间的**FTP授权规则**】的方法。您可能还需要更改该目录所对应的文件夹的NTFS权限，此时可通过**Windows资源管理器**来更改，或直接通过图 9-53右边的**编辑权限...**。

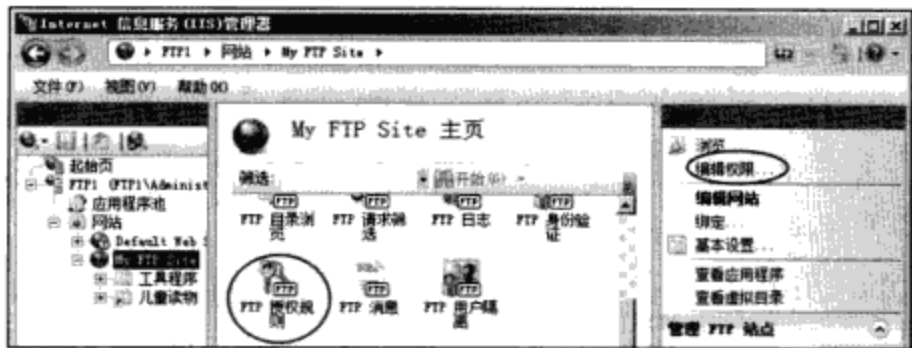


图 9-53

完成上述设置后，请到客户端利用ftp.exe命令或Windows资源管理器来测试。例如图 9-54 中以用户George的身份登录，然后利用dir命令可看到其主目录（C:\inetpub\ftproot\george）内的文件。可是因为并不隔离用户，故我们可以轻易地利用cd ../mary命令来切换到mary的主目录。



图 9-54



#### 注意

若要使用Windows资源管理器或Internet Explorer(IE)来连接FTP站点的话，请输入ftp://george@ftp1.sayms.com/，其中george为用户账号（IE需要重复输入一次账号与密码）。不过请用IE 7.0 以前的旧版本，因为IE 7.0（含）以后的版本连接FTP站点的方式已改变，无法被导向到用户的主目录，而只会被导向FTP站点的主目录。

### 9-4-2 隔离用户、有专属主目录，但无法访问全局虚拟目录

用户拥有自己的专属主目录，而且会隔离用户，也就是用户登录后会被导向到其专属主目录内，且被限制在此主目录内、无法切换到其他用户的主目录，因此无法查看或修改其他用户主目录内的文件。用户也无法访问FTP站点内的全局虚拟目录。

我们需要建立目录名称与用户名相同的物理或虚拟目录，此处我们采用物理目录。您需要在FTP站点主目录之下新建以下的文件夹结构：

- **LocalUser\用户名**: LocalUser文件夹是本地用户专属的文件夹，而**用户名**是本地用户名称。请在LocalUser文件夹之下为每一位需要登录FTP站点的本地用户各新建一个专属子文件夹，文件夹名称需与用户名称相同。当用户登录FTP站点时，他会被导向到与其用户名称同名的文件夹。
- **LocalUser\Public** 用户利用匿名账户(anonymous)登录FTP站点时，他会被导向到Public文件夹。
- **域名\用户名**: 若用户是利用Active Directory域用户账户来登录FTP站点的话，则请为该域新建一个专属文件夹，此文件夹名称需与NetBIOS域名相同；然后在此文件夹之下为每一位需要登录FTP站点的域用户，各新建一个专属的子文件夹，此文件夹名称需与用户名称相同。当域用户登录FTP站点时，他就会被导向到与用户名同名的文件夹。

举例来说，若FTP站点的主目录位于C:\inetpub\ftproot，而您要让匿名账户、本地用户George与Mary、域SAYMS用户Jackie与Alice等来登录FTP站点，且要让他们都有专属主目录的话，则在FTP站点主目录之下的文件夹结构将是如表 9-1所示。

表 9-1

用户	文件夹
匿名账户	C:\inetpub\ftproot\LocalUser\Public
本地用户George	C:\inetpub\ftproot\LocalUser\George
本地用户Mary	C:\inetpub\ftproot\LocalUser\Mary
域SAYMS用户Jackie	C:\inetpub\ftproot\SAYMS\Jackie
域SAYMS用户Alice	C:\inetpub\ftproot\SAYMS\Alice

要让您的FTP站点启用这种模式的话，请如图 9-55所示在图中间选择**用户名目录**（禁用全局虚拟目录）。

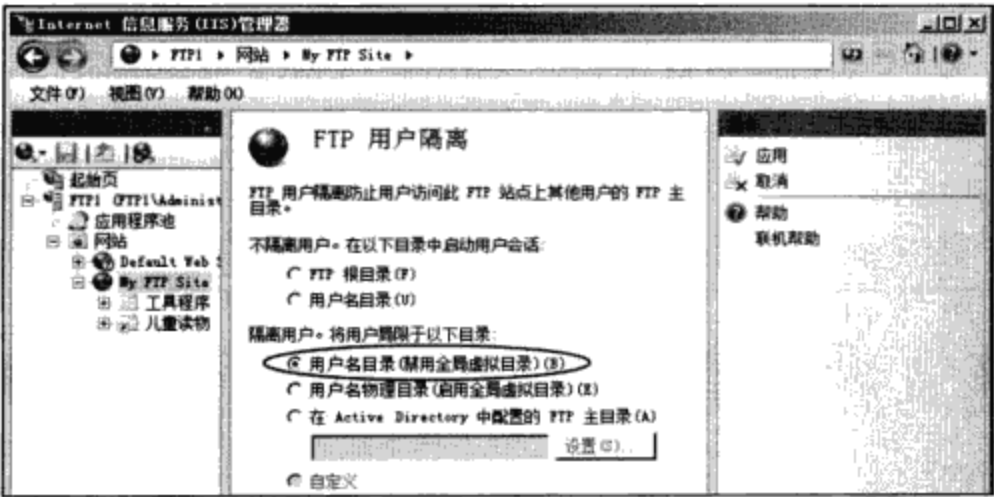


图 9-55

假设我们要让本地用户George与Mary登录时被导向到自己的主目录，而匿名用户会被导向到public文件夹，则请如图 9-56所示在**My FTP Site**的主目录C:\inetpub\ftproot下新建一个名称为LocalUser的文件夹，然后在其下分别新建george、mary与public三个子文件夹，并建议在这三个文件夹内分别放置一些文件，以便于测试时使用。

用户 George、Mary 与匿名者登录 FTP 站点时，会分别被导向到 C:\inetpub\ftproot\LocalUser\george、C:\inetpub\ftproot\LocalUser\mary 与 C:\inetpub\ftproot\LocalUser\public 文件夹。

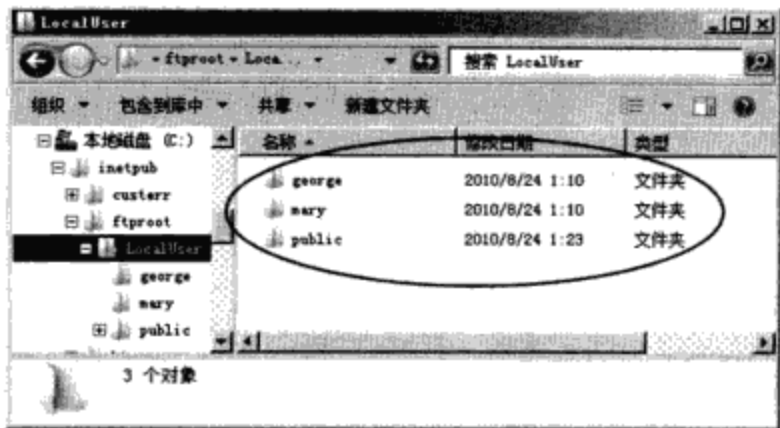


图 9-56



提示

用户对其主目录的默认权限为**读取**，若要更改的话，请通过【单击图 9-57 中的目录（例如 george）→单击中间的**FTP 授权规则**】的方法。您可能还需要更改该目录所对应的文件夹的 NTFS 权限，此时可通过**Windows 资源管理器**来更改，或直接通过图 9-57 中右边的**编辑权限...**。

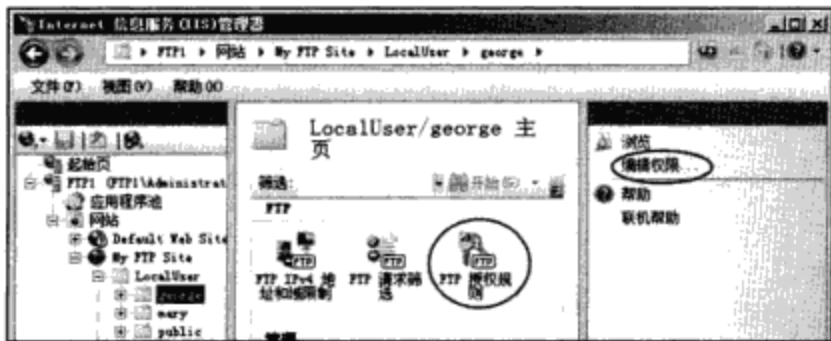


图 9-57

完成上述设置后，请到客户端利用 **ftp.exe** 命令或**Windows 资源管理器**来测试。例如图 9-58 中以用户 George 的身份登录，然后利用 **dir** 命令可看到其主目录（C:\inetpub\ftproot\LocalUser\george）内的文件。因为会隔离用户，因此无法利用图中的 **cd ../mary** 命令来切换到 mary 的主目录。



图 9-58

用户无法访问这种模式的FTP站点之下的全局虚拟目录，但是可以查看其专属主目录下的虚拟目录，例如用户George可以访问自己主目录下的虚拟目录Database，如图9-59所示，但是无法访问My FTP Site站点之下的虚拟目录（全局虚拟目录）儿童读物。



图 9-59

您可以先启用显示虚拟目录功能后再来测试是否可以访问虚拟目录。启用显示虚拟目录功能的方法为如图9-60所示【单击My FTP Site中间的FTP 目录浏览选择虚拟目录】。



图 9-60

然后如图9-61所示利用ftp.exe命令来连接FTP站点，图中利用用户George身份登录、运行dir命令后，可以看到George主目录内的虚拟目录Database，但是看不到FTP站点下的全局虚拟目录儿童读物，同时也无法利用cd 儿童读物命令切换到此虚拟目录。



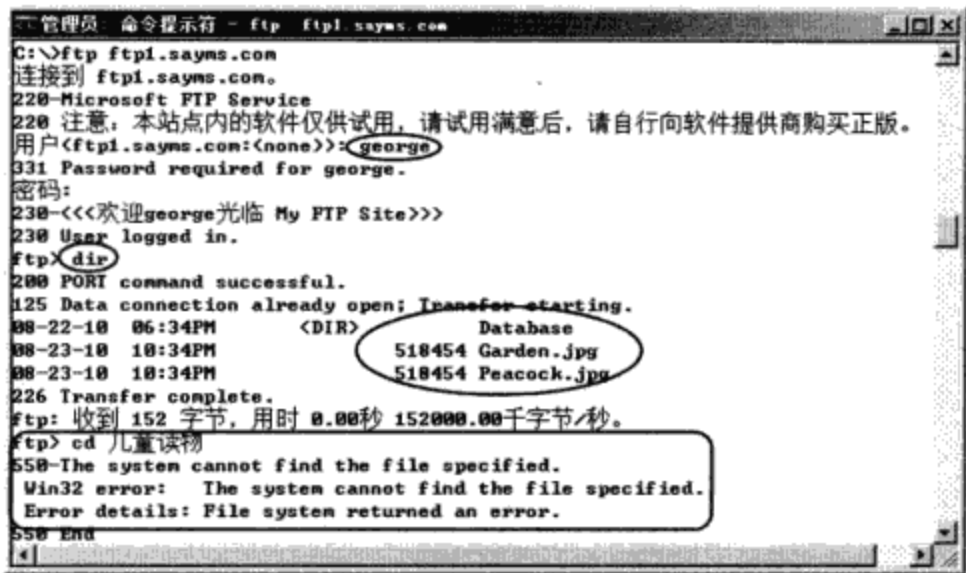


图 9-61

### 9-4-3 隔离用户、有专属主目录，可以访问全局虚拟目录

其启用方法为选择图 9-62 中间的用户名称物理目录（启用全局虚拟目录），它与前一小节的用户名称目录（禁用全局虚拟目录）几乎完全相同，不过此处选择**用户名称物理目录（启用全局虚拟目录）**的 FTP 站点具备以下特性：

- 用户专属的主目录必须是物理目录，不可以是虚拟目录。
- 用户可以访问 FTP 站点内的全局虚拟目录，例如图 9-62 中左边的虚拟目录**儿童读物**，但是却无法访问用户专属主目录内的虚拟目录，例如图中的虚拟目录**Database**。

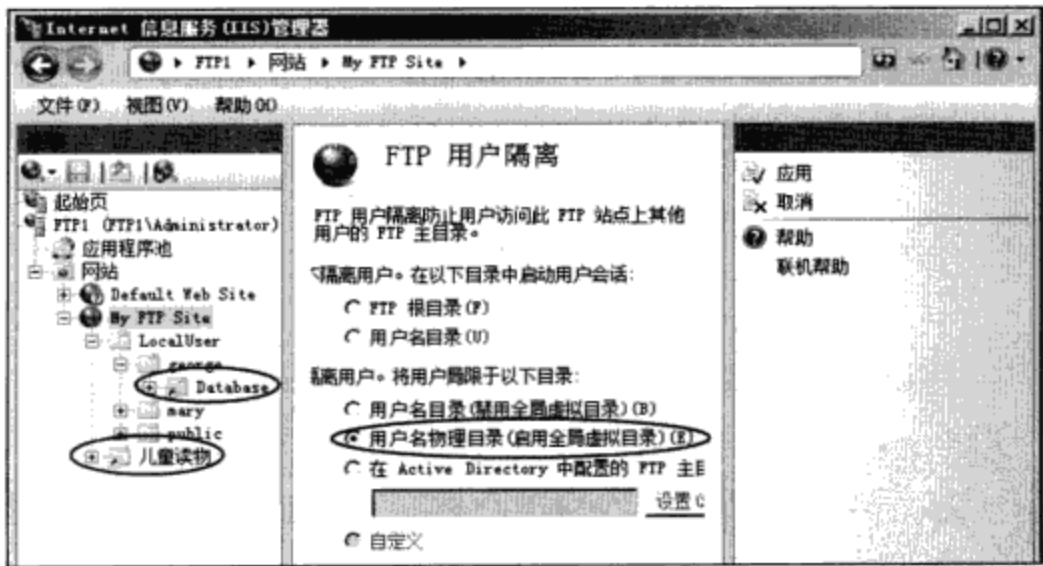


图 9-62

若您如图 9-63 所示通过 ftp.exe 命令来连接 FTP 站点，然后利用用户 George 身份登录、执行 dir 命令后，可以看到 FTP 站点之下的全局虚拟目录**儿童读物**，但是看不到用户专属主目录内的虚拟目录**Database**，同时也无法利用 **cd Database** 命令切换到此虚拟目录。

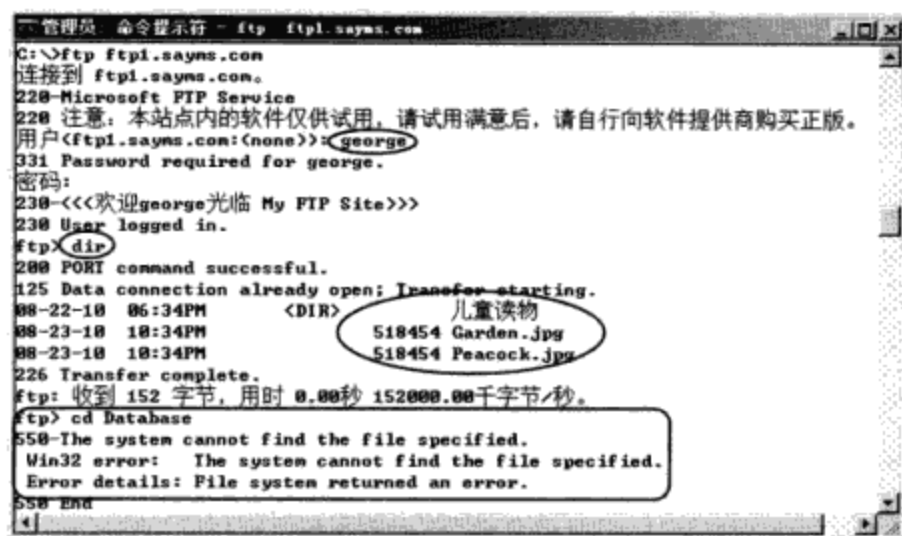


图 9-63

## 9-4-4 通过Active Directory来隔离用户

此模式只适合于Active Directory域用户。用户拥有专属主目录，而且会隔离用户，也就是用户登录后会被导向到其专属主目录内，且被限制在此主目录、无法切换到其他用户的主目录，因此无法查看或修改其他用户主目录内的文件。以下将通过图 9-64来说明，图中的DC为域控制器兼DNS服务器、FTP1为FTP服务器（成员服务器）、Win7PC为测试计算机。

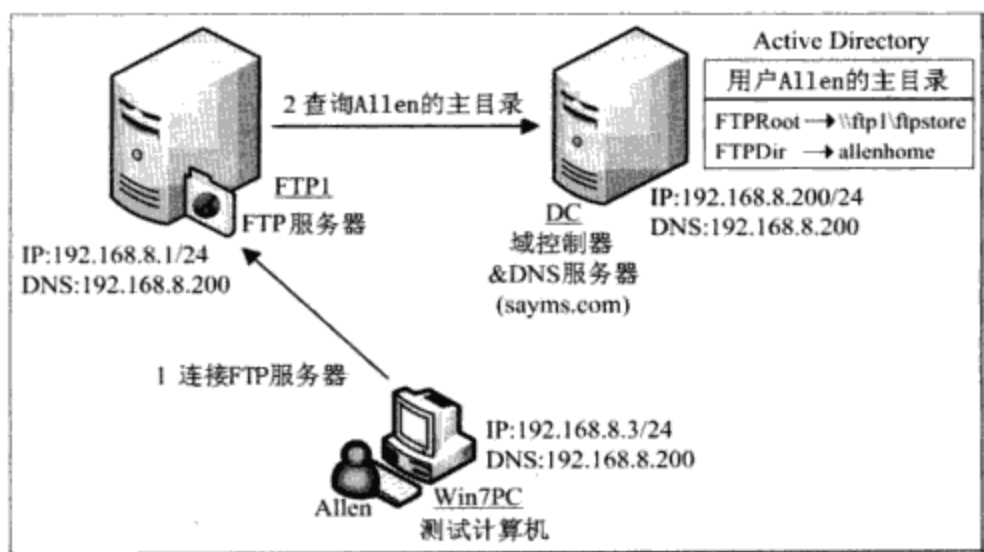


图 9-64

用户主目录的实际文件夹是被设置在域用户账户内，域用户连接FTP站点时，FTP站点会到Active Directory数据库来读取用户的主目录存储地点（文件夹），以便将用户导向到此文件夹。

### 新建域用户的主目录

您必须为每一位需要连接到FTP站点的域用户，分别新建一个专属的用户主目录，下面我们利用域用户Allen来练习，并且将其主目录指定到服务器FTP1的共享文件夹\\ftp1\ftpstore内的子文件夹allenhome。

请先在Active Directory数据库内新建用户账户Allen，假设我们将其新建在Users容器内。接着如图 9-65所示在服务器FTP1中新建文件夹ftpstore，将其设置为共享文件夹，并开放适当的共享权限（例如**读取/写入**）给Allen，然后在此文件夹下新建一个子文件夹allenhme，此文件夹\\ftp1\ftpstore\allenhme将作为用户Allen的主目录，而为了方便验证练习的结果，图中我们顺便复制了一些文件到此文件夹内。

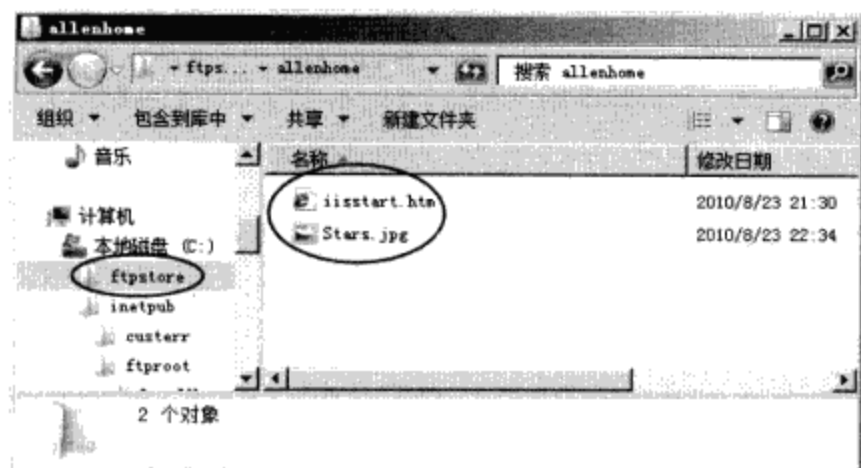


图 9-65

### 在Active Directory数据库中设置用户的主目录

在Active Directory数据库的用户账户内有两个属性用来支持**通过Active Directory来隔离**用户的FTP站点，它们分别是msIIS-FTPRoot与msIIS-FTPDir，其中msIIS-FTPRoot用来设置主目录的UNC网络路径、而msIIS-FTPDir用来指定UNC下的子文件夹，例如若要将用户Allen的主目录指定到\\ftp1\ftpstore\allenhme的话，则这两个属性的设置值为：

- msIIS-FTPRoot需被设置为\\ftp1\ftpstore
- msIIS-FTPDir需被设置为allenhme

请到域控制器DC上利用**ADSI编辑器**来设置用户账户的msIIS-FTPRoot与msIIS-FTPDir属性。



#### 注意

若要在服务器FTP1上来执行以下步骤的话，必须先在此服务器上安装**AD DS及AD LDS工具**、然后利用域系统管理员的身份登录。安装此工具的方法为：**【单击左下角服务器管理器图标 ➤ 功能 ➤ 添加功能 ➤ 展开远程服务器管理工具 ➤ 角色管理工具 ➤ 选择AD DS及AD LDS工具】**。

**STEP 1** 选择 **【开始 ➤ 运行 ➤ 输入ADSIEDIT.MSC后单击确定】**。

**STEP 2** 如图 9-66所示 **【对着ADSI编辑器单击右键 ➤ 连接到 ➤ 在前图中直接单击确定】**。

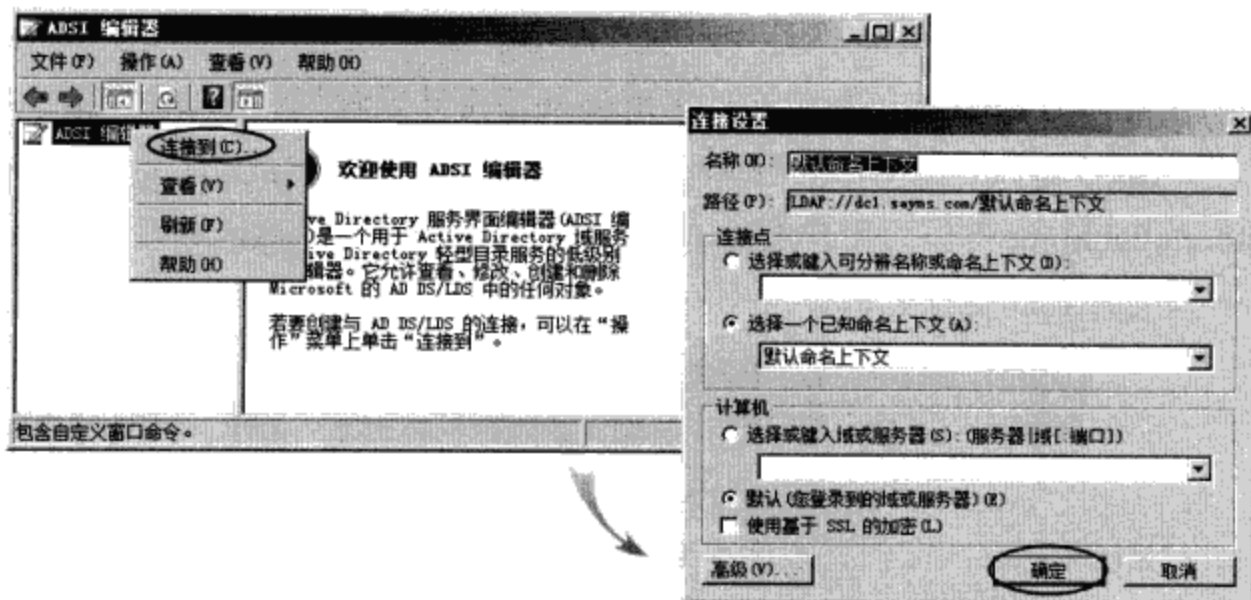


图 9-66

**STEP 3** 在图 9-67中【展开到用户账户所在的Users容器，对着用户allen单击右键，属性】。



图 9-67

**STEP 4** 在图 9-68通过编辑来将msIIS-FTPRoot与msIIS-FTPDDir这两个属性分别改为图中的\\ftp1\ftpstore与allenshome后单击确定。

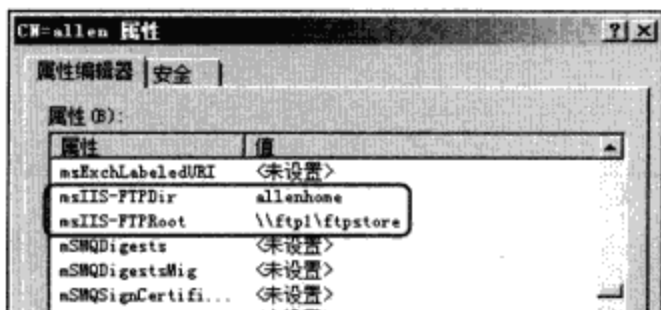


图 9-68

### 新建一个让FTP站点可以读取用户属性的域用户账户

域用户登录到FTP站点时，FTP站点需从Active Directory数据库来读取该登录者的msIIS-FTPRoot与msIIS-FTPDDir属性，以便得知其主目录的位置。不过FTP站点需提供有效的用户账户与密码，才可以读取这两个属性：我们将另外新建一个域用户账户，并开放让此账户有权利读取登录者的这两个属性，然后设置让FTP站点通过此账户来读取登录者的这两个属性。

**STEP 1** 请在域控制器上通过【开始☞管理工具☞Active Directory用户和计算机】来新建一个用户账户，例如图 9-69中我们在Users容器内新建了用户ftpuser。新建账户时请取消选择用户在下次登录时须更改密码、改选择密码永不过期。

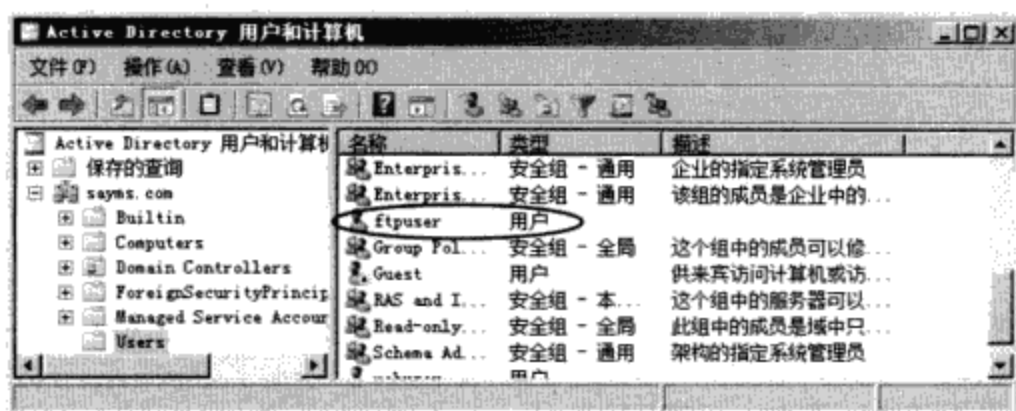


图 9-69

**STEP 2** 由于要登录FTP站点的用户Allen，其用户账户是位于Users容器内，因此我们需要开放让ftpuser可以来读取Users容器内的用户的msIIS-FTPRoot与msIIS-FTPDDir属性：请【如图 9-70所示对着Users容器单击右键☞委派控制】。



图 9-70

**STEP 3** 出现欢迎使用委派控制向导界面时单击下一步。

**STEP 4** 在图 9-71中单击添加来选择用户账户ftpuser，之后单击下一步。

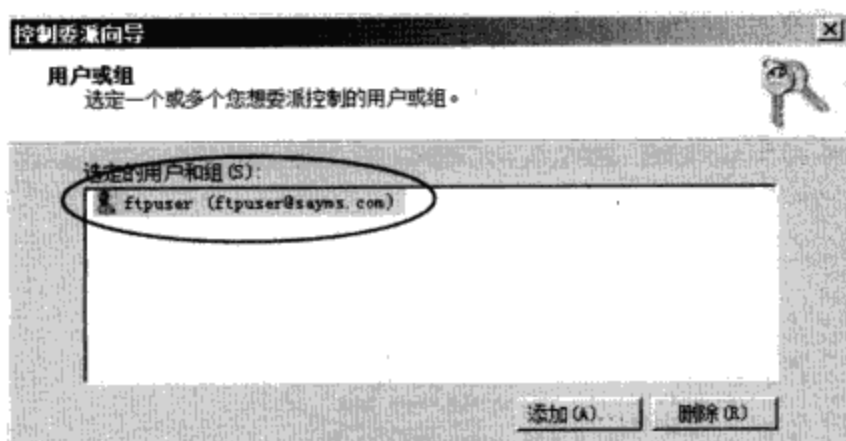


图 9-71

**STEP 5** 在图 9-72中选择读取所有用户信息后单击下一步。

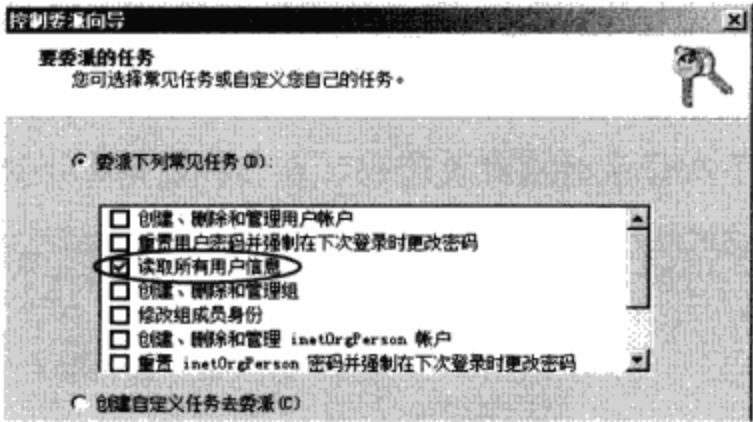


图 9-72

**STEP 6** 出现完成委派控制向导界面时单击**完成**。

FTP站点的设置与连接FTP站点的测试

我们需要让FTP站点利用域用户ftpuser来读取域用户Allen的msIIS-FTPRoot与msIIS-FTPDDir属性：请如图 9-73所示【选择My FTP Site界面中间的在Active Directory中配置的FTP主目录单击**设置**在前图中输入SAYMS\ftpuser与其密码单击**确定**单击右边的应用】。

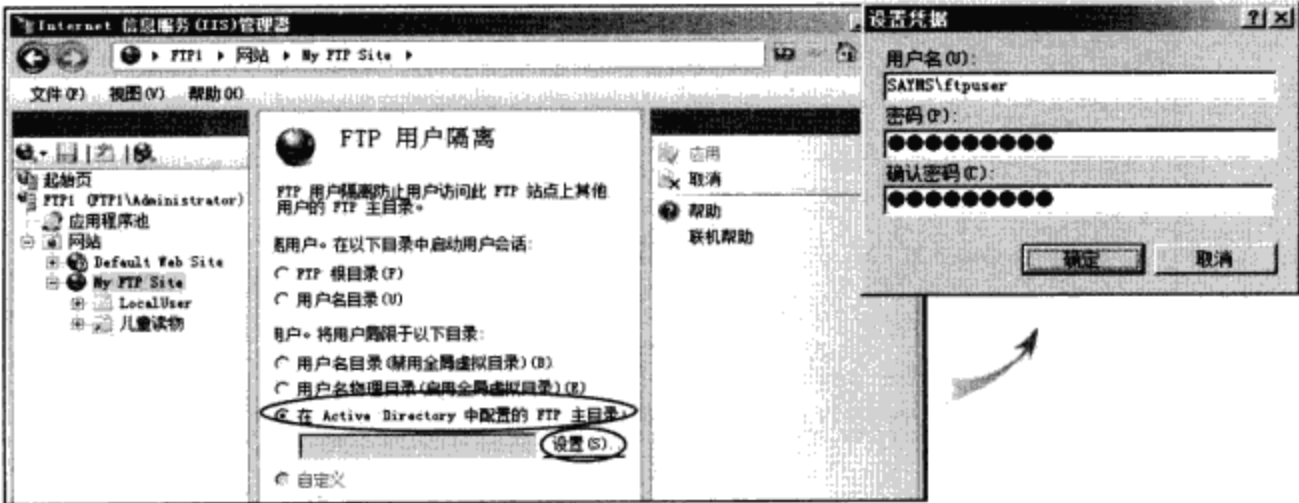


图 9-73

完成后请如图 9-74所示利用用户账户Allen来连接这个通过Active Directory隔离用户的FTP站点，图中我们利用dir命令所看到的文件是位于\\ftp1\ftpstore\allenhome的文件，因此可以确认其主目录为\\ftp1\ftpstore\allenhome。

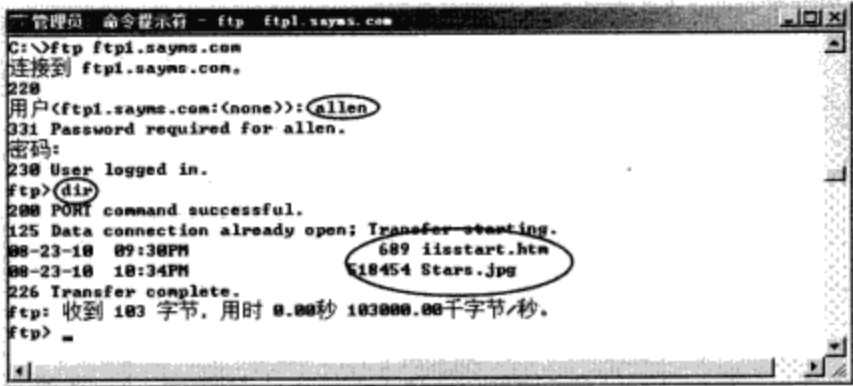


图 9-74

## 9-5 具备安全连接功能的FTP over SSL

Windows Server 2008 R2的FTP服务支持FTP over SSL (FTPS)，它让FTP客户端可以利用SSL安全连接来与FTP服务器通信，不过您必须为FTP服务器申请SSL安全连接证书与安装证书，这些概念与步骤都跟网站的SSL类似，在此我们仅列其重要步骤（有需要时再参考章节6-3的说明）：

- **新建证书申请文件：**选择【开始☞管理工具☞Internet 信息服务 (IIS)管理器☞单击服务器名称☞双击中间的服务器证书☞单击右边的新建证书申请...】。
- **申请与下载证书：**在浏览器内输入http://CA的IP或网址/certsrv/，以便将证书申请文件的内容发送到CA，并下载证书文件。
- **安装证书：**选择【开始☞管理工具☞Internet Information Services (IIS)管理器☞单击服务器名称☞双击中间的服务器证书☞单击右边的完成证书申请...】安装证书时请选择刚才所下载的证书，并为此证书设置一个好记的名称（例如My FTP SSL）。完成后，不需要做绑定操作。
- **选择证书：**如图 9-75所示【单击My FTP Site中间的FTP SSL设置☞在前图的SSL证书处选择前一个步骤所安装的SSL证书（My FTP SSL）☞单击应用】。

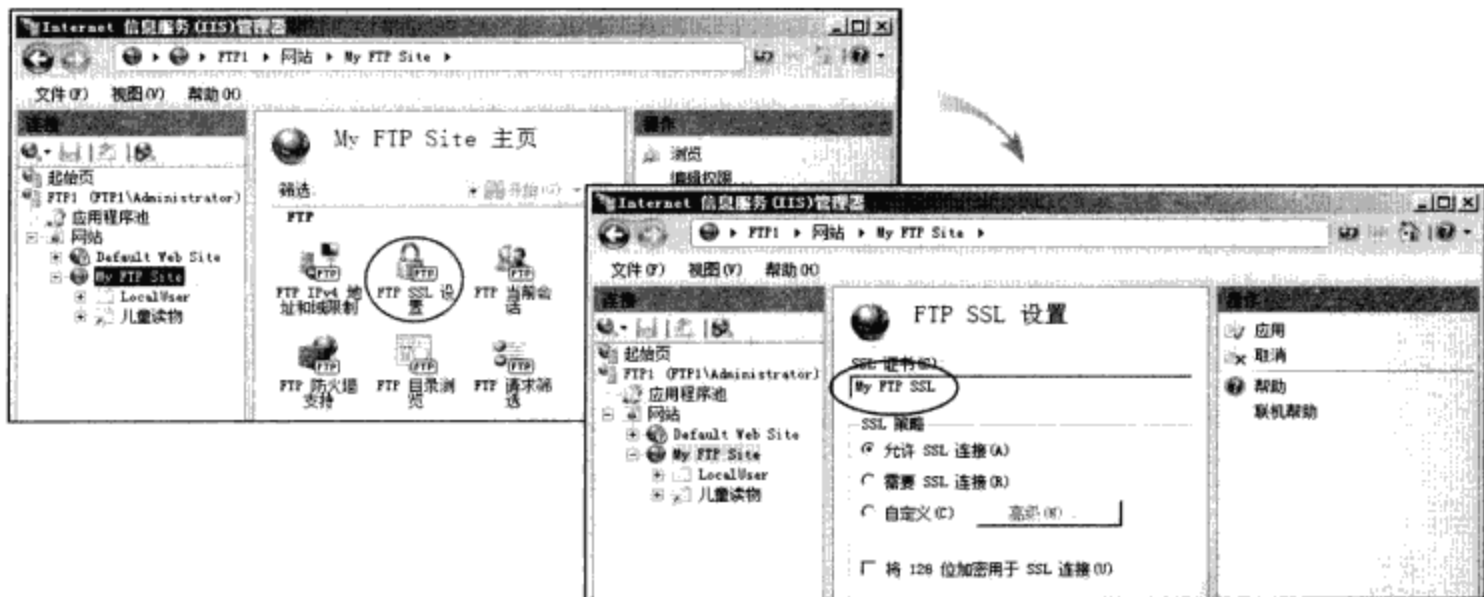


图 9-75

图 9-75中最下方的**将128位加密用于SSL连接**表示要求客户端必须采用128位加密方式。另外图中的**允许SSL连接**表示允许客户端利用SSL来连接，**需要SSL连接**表示客户端必须利用SSL方式来连接。

您也可以单击自定义处的**高级**，然后通过图 9-76进一步分别针对**控制通道**（Control Channel）与**数据通道**（Data Channel）做不同的设置，其中的**允许**表示允许使用SSL、**要求**表示必须使用SSL、**拒绝**表示拒绝SSL连接，而**控制通道**中的**只有凭据才需要**表示只有在传送用户名与密码时才使用SSL加密。通道说明请参考下一节。



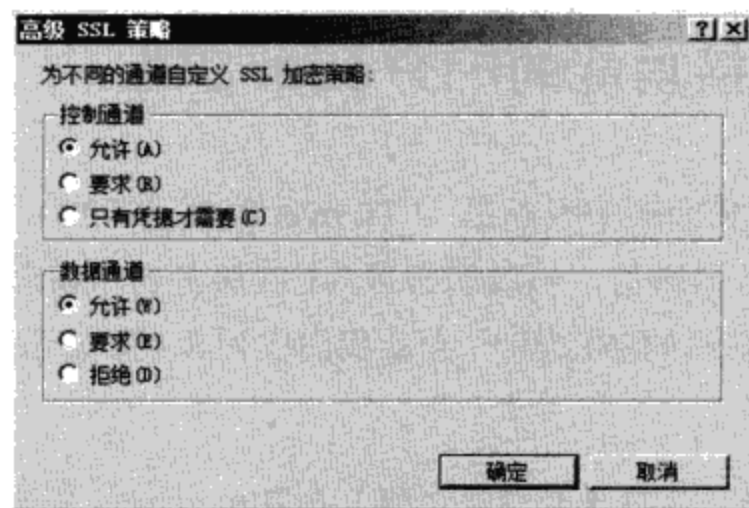


图 9-76

完成以上设置后，客户端便可以利用SSL安全连接方式来连接SSL FTP服务器，不过客户端的FTP软件必须支持SSL（FTPS），而Windows系统内置的ftp.exe、IE 7、IE 8与Windows资源管理等目前都不支持FTPS，因此客户端需采用其他供应商的软件，例如SmartFTP、CuteFTP等。

FTPS的运作又分为以下两种模式：

- **Explicit SSL**：若您将FTP服务器控制通道的端口号设置为21的话，它就是以**Explicit SSL**的模式在运行。

在此模式之下，客户端通过控制通道（端口21）连接服务器后，若希望在接下来的连接中使用SSL的话，需由客户端发指令给服务器，来“明确地（explicitly）”请求与服务器使用SSL连接。至于服务器是否接受SSL连接，要看图 9-75或图 9-76的设置来决定。Windows Server 2008 R2的FTPS默认是Explicit SSL模式。

- **Implicit SSL**：若您将FTP服务器的控制通道端口号设置为990的话，它就是以**Implicit SSL**的模式在运行。

在此模式之下，客户端与服务器必须使用SSL连接：当客户端通过控制通道（端口990）连接服务器后，客户端就立刻会与服务器来进行SSL的协商，以便使用SSL连接。

## 9-6 防火墙的FTP设置

若FTP客户端与服务器之间被防火墙隔离的话，由于客户端与服务器之间需要通过两个连接来新建两个通道（channel），因而增加了防火墙设置的复杂度。其中一个通道是用来发送命令的**控制通道**（control channel），另一个是用来发送数据的**数据通道**（data channel）。**控制通道**在服务器端所使用的端口为21，而**数据通道**则视FTP的运作模式而定。FTP的运行模式分为**主动模式**（Active Mode）与**被动模式**（Passive Mode）。

## 9-6-1 FTP主动模式

**主动模式**又称为**标准模式**或**PORT模式**，此时FTP客户端与服务器之间的通信过程如下所示（以图 9-77为例）：

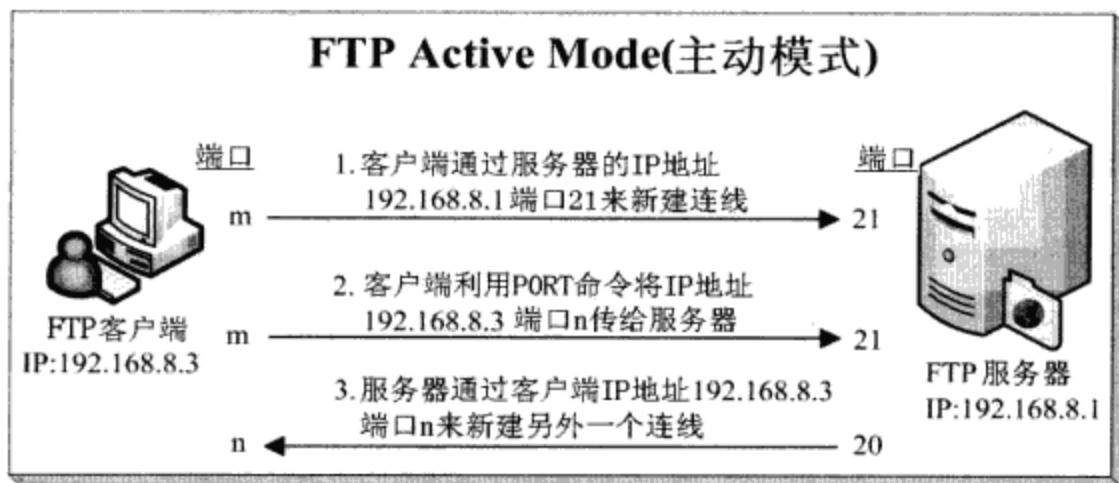


图 9-77

1. 客户端新建与服务器之间的**控制通道**连接：建立连接时服务器端的IP地址为192.168.8.1、端口号为标准的21；客户端的IP地址为192.168.8.3、端口号为动态生成（假设为m）。
2. 当客户端需要下载（或上传）文件时，客户端会通过**控制通道**来发送PORT命令给服务器，此命令包含客户端的IP地址与另外一个端口号（假设为n）。客户端利用PORT命令通知服务器通过此IP地址与端口号来发送文件给客户端。
3. 服务器新建与客户端之间的**数据通道**连接：创建连接时客户端的IP地址为192.168.8.3，端口号为n；服务器的IP地址为192.168.8.1，端口号为标准的20。



### 提示

主动模式FTP over SSL（FTPS）的Explicit SSL的**控制通道**端口号为21、**数据通道**端口号为20；Implicit SSL的**控制通道**端口号为990、**数据通道**端口号为989。

### 客户端与服务器被防火墙隔离

若FTP客户端与FTP服务器之间被防火墙隔离的话：

- ✎ 客户端在新建图（9-77）中1号箭头的**控制通道**连接时，必然会被防火墙阻挡，除非在防火墙开放端口号21，且其开放方向是客户端往服务器。
- ✎ 服务器在新建图中3号箭头的**数据通道**连接时，也必然会被防火墙阻挡，除非在防火墙开放端口号n，其开放方向是服务器往客户端。然而此端口n是动态生成，因此难以在防火墙针对这个不固定的端口来开放，此时您可以利用以下方法来解决此问题：
  - 在客户端改用**被动模式**来连接服务器。
  - 采用功能较强的防火墙，例如Microsoft ISA Server或Microsoft Forefront Threat

Management Gateway，它会监视客户端的PORT命令，以便得知客户端要使用的IP地址与端口号，然后自动开放此IP地址与端口。

### FTP服务器的Windows防火墙与主动模式

如果您是将FTP服务器架设在Windows Server 2008 R2计算机上的话，由于它内置**Windows防火墙**，而且默认已经开启，故客户端连接这台FTP服务器的连接会被阻挡，此时的解决方法如下（参考图 9-78）：

- 针对图 9-78中1号箭头的控制通道传入连接（incoming connection）来说，请在Windows防火墙开放端口号21。
- 针对图 9-78中3号箭头的数据通道连出连接（outgoing connection）来说，您并不需要做额外的开放设置，因为Windows防火墙默认并不会阻挡此连出连接。

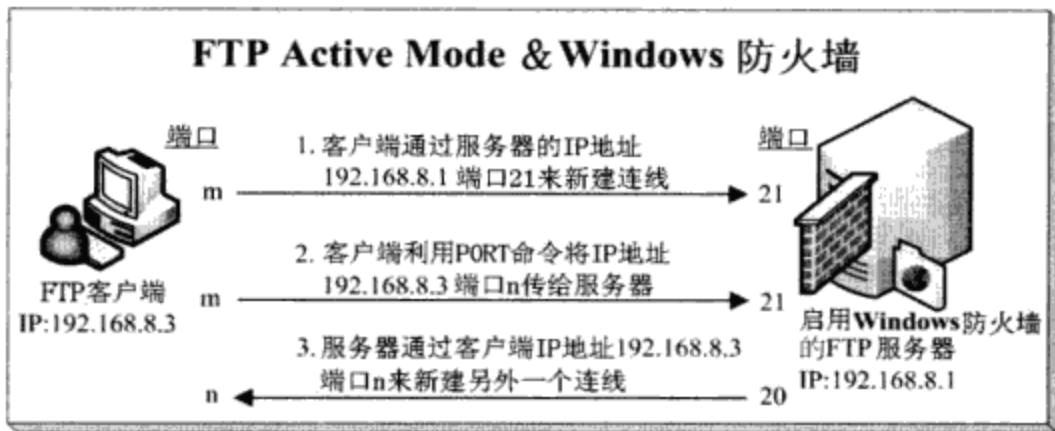


图 9-78

在**Windows防火墙**开放端口号21的传入连接的步骤如下所示：

- STEP 1** 请到FTP服务器上选择【开始➤控制面板➤系统和安全➤Windows防火墙➤单击左边的高级设置】（或选择【开始➤管理工具➤高级安全Windows防火墙】）。
- STEP 2** 如图 9-79所示单击入站规则右方的新建规则。

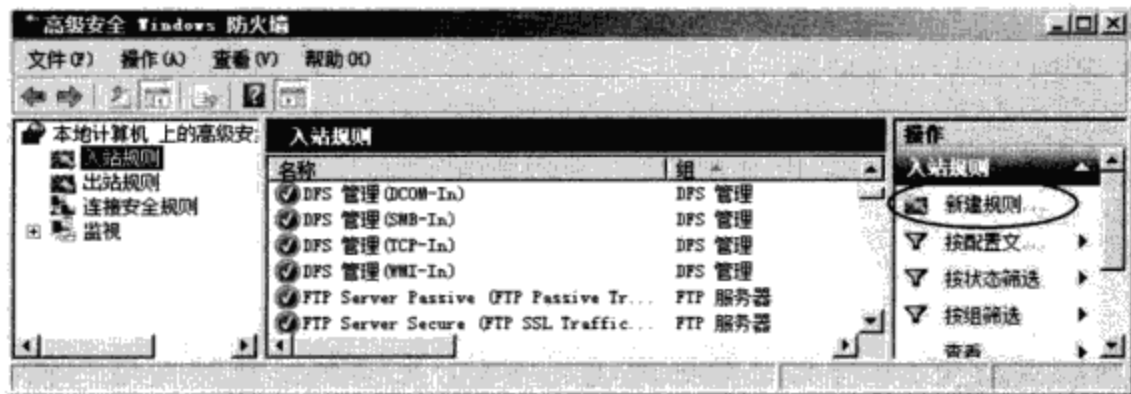


图 9-79

- STEP 3** 在图 9-80中选择端口后单击**下一步**。

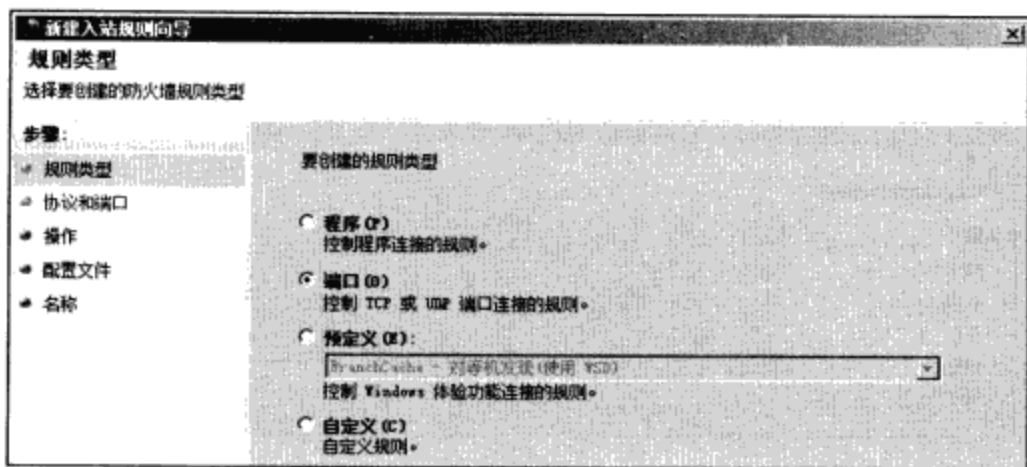


图 9-80

**STEP 4** 在图 9-81 中选择 TCP、在特定本地端口处输入 21。

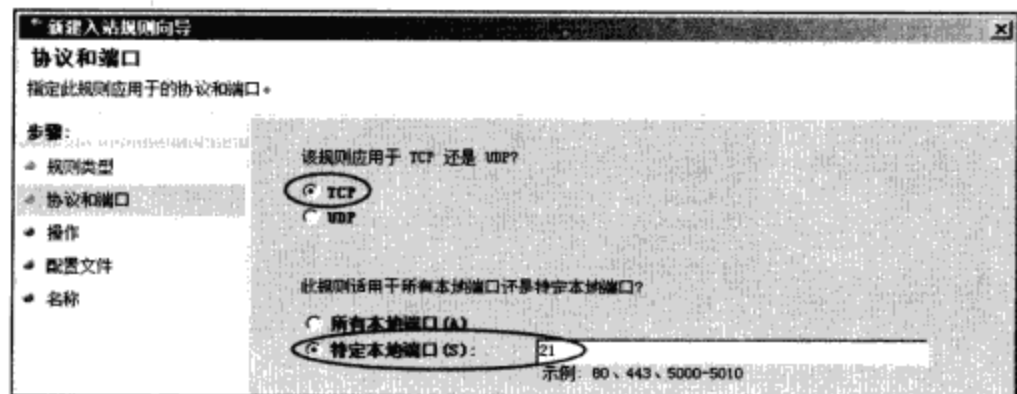


图 9-81

**STEP 5** 在图 9-82 中采用默认的允许连接后单击 **下一步**。

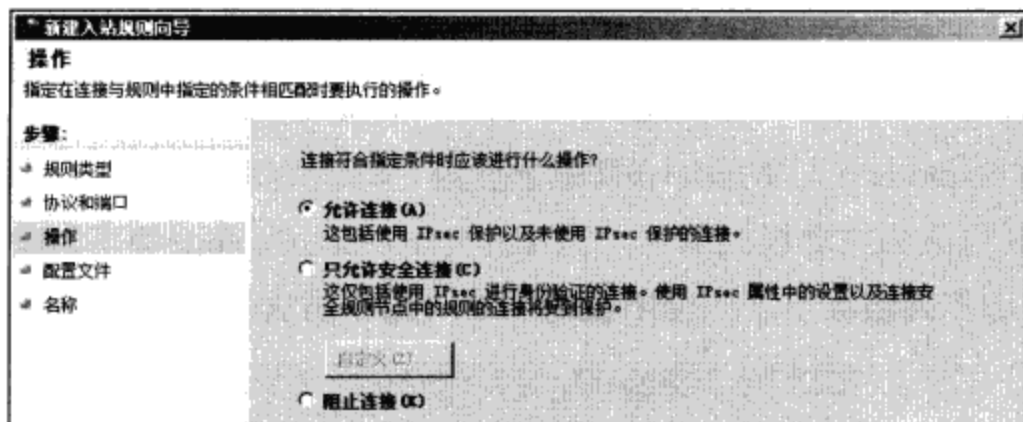


图 9-82

**STEP 6** 在图 9-83 中直接单击 **下一步**，它会将此规则应用到所有网络。

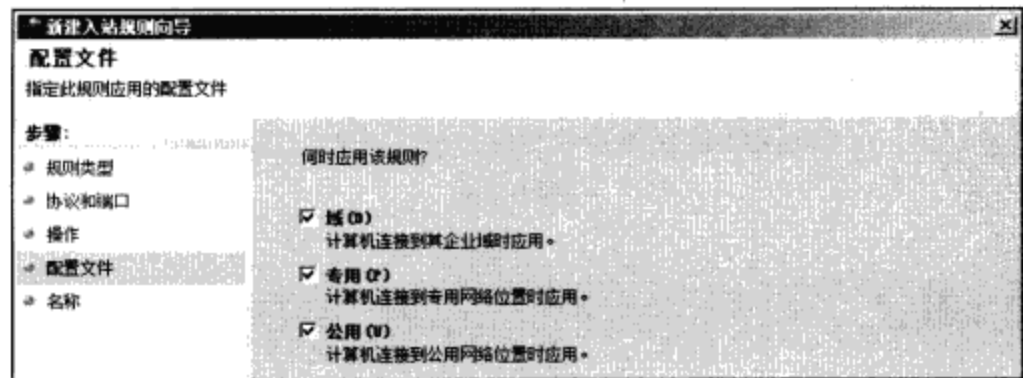


图 9-83

**STEP 7** 在图 9-84中设置此规则的名称后单击**完成**。

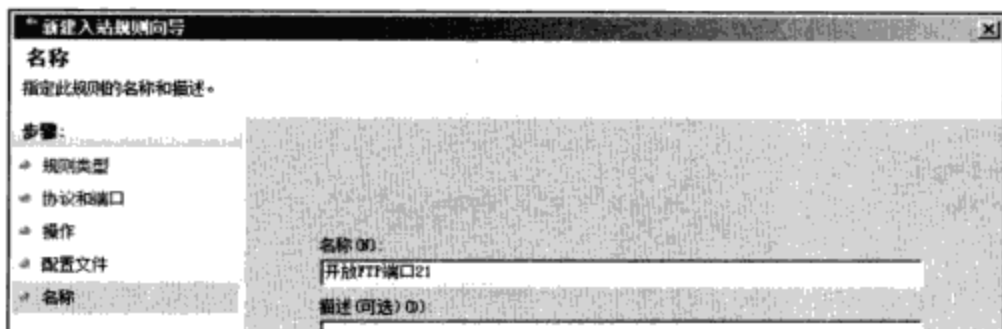


图 9-84

**STEP 8** 图 9-85为完成后的界面。

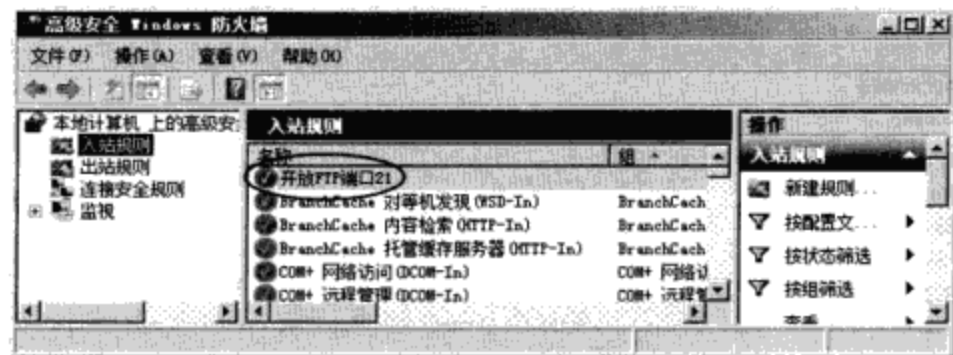


图 9-85

### FTP客户端主动模式连接测试

完成以上设置后，客户端就可以利用主动模式来连接FTP服务器。Windows系统内置的FTP客户端程序ftp.exe默认是采用主动模式，因此您可以利用它来连接我们所架设的FTP服务器My FTP Site（它是已经启用**Windows防火墙**的Windows Server 2008 R2计算机）。

浏览器Internet Explorer（与**Windows资源管理器**）默认是采用被动模式，因此无法连接My FTP Site，若要将其更改为主动模式的话，请【打开Internet Explorer☞工具菜单☞Internet选项☞如图 9-86所示取消选择**高级**标签下的**使用被动FTP（用于防火墙和DSL调制解调器的兼容）**】。

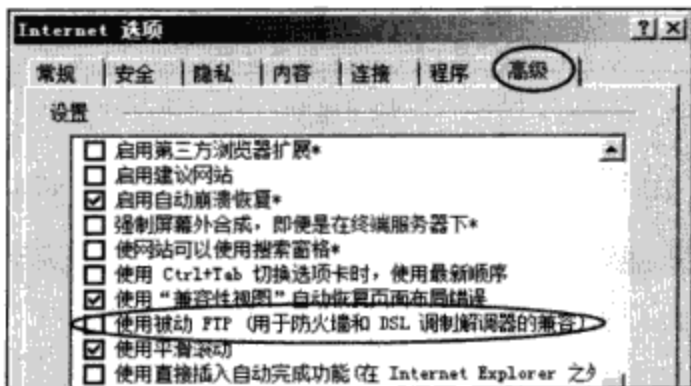


图 9-86

## 9-6-2 FTP被动模式

被动模式又称为**PASV模式**，此时FTP客户端与服务端之间的通信过程如下所示（以图 9-87

为例):

1. 客户端新建与服务器之间的**控制通道**连接: 新建连接时服务器的IP地址为192.168.8.1、端口号为标准的21; 客户端的IP地址为192.168.8.3、端口号为动态生成(假设为m)。
2. 客户端通过**控制通道**发送PASV命令给服务器, 表示要利用被动模式来与服务器通信。
3. 服务器通过**控制通道**将用来接听客户端请求的IP地址与端口号(假设为x)发给客户端, 此端口号为动态生成。
4. 客户端建立与服务器之间的**数据通道**连接: 建立连接时服务器的IP地址为192.168.8.1、端口号为x; 客户端的IP地址为192.168.8.3、端口号为动态生成(假设为n)。

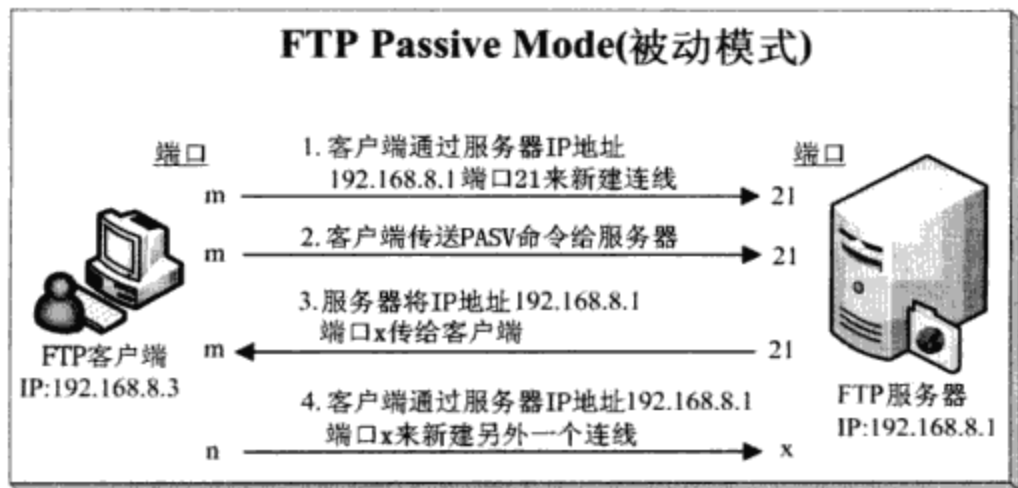


图 9-87



提示

被动模式FTP over SSL (FTPS) 的Explicit SSL的**控制通道**端口号为21、**数据通道**端口号为随机值; Implicit SSL的**控制通道**端口号为990、**数据通道**端口号为随机值。

#### 客户端与服务器被防火墙隔离

若FTP客户端与FTP服务器之间被防火墙隔离的话:

- ✎ 客户端在建立图 9-87中1号箭头的**控制通道**连接时, 必然会被防火墙阻挡, 除非在防火墙开放端口号21, 其开放方向是客户端往服务器。
- ✎ 客户端在创建图中4号箭头的**数据通道**连接时, 也必然会被防火墙阻挡, 除非在防火墙开放端口号x, 其开放方向是客户端往服务器。同样然而此端口x是动态产生, 因此难以在防火墙针对这个不固定的端口来开放, 此时您可以利用以下方法来解决此问题:
  - 将FTP服务器所使用的端口固定在一段范围内, 然后在防火墙开放这一段范围的端口 (参考后面图 9-91的相关说明)。
  - 也可采用功能较强的防火墙, 例如Microsoft ISA Server或Microsoft Forefront Threat Management Gateway, 它会监视客户端与服务器之间利用PASV命令通信的数据包 (图 9-87中2与3号箭头), 以便得知服务器要使用的IP地址与端口号, 然后自动开放此IP地址与端口。

## FTP服务器位于NAT之后

若FTP服务器是位于NAT（Network Address Translation，例如IP分享器或是以NAT模式运作的防火墙）设备之后，例如图 9-88中的FTP服务器位于防火墙（NAT模式）之后，则此时由于图中FTP服务器所使用的IP地址是私有IP（private IP）192.168.8.1，因此第3号箭头中FTP服务器的响应数据包内的IP地址，将使得客户端无法与服务器建立第4号箭头的**数据通道**连接，因为外部客户端无法连接仅限内部网络使用的私有IP地址。

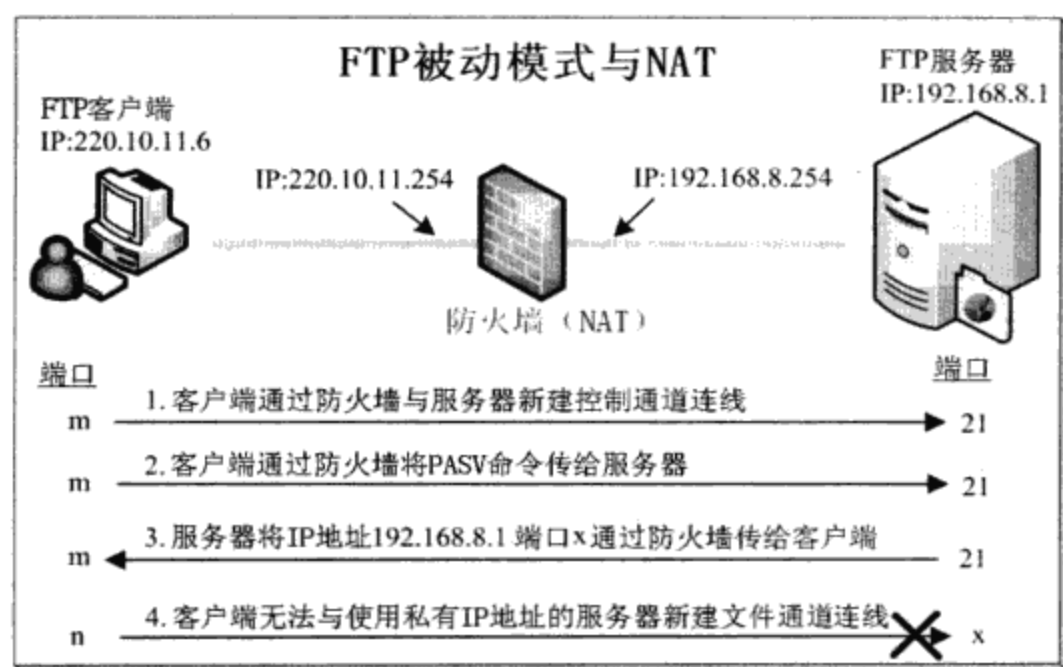


图 9-88

您可以采用功能较强的防火墙来解决上述问题，例如具备NAT功能的Microsoft ISA Server或Microsoft Forefront Threat Management Gateway，它会监视客户端与服务器之间利用PASV命令通信的数据包（图 9-88中2与3号箭头），并将第3号箭头中FTP服务器回应数据包中的私有IP地址192.168.8.1，替换成防火墙外部IP地址（图中的220.10.11.254），因此第4号箭头中客户端便会要求与防火墙新建**数据通道**连接，再由防火墙将其转到内部FTP服务器。

如果防火墙不具备上述功能的话，Windows Server 2008 R2 FTP服务器也提供另外一种方法来解决此问题：请事先在FTP服务器内指定防火墙的外部IP地址（220.10.11.254），之后当FTP服务器要将图中3号箭头的数据包通过防火墙传给客户端之前，会自行先将数据包内的服务器IP地址192.168.8.1替换成防火墙外部IP地址220.10.11.254。在FTP服务器内指定防火墙外部IP地址220.10.11.254的方法为：**【如图 9-89所示单击My FTP Site中的FTP防火墙支持在前图防火墙的外部IP地址中输入防火墙外部网卡的IP地址220.10.11.254单击右边的应用】。**





图 9-89

### FTP服务器的Windows防火墙与被动模式

如果您是将FTP服务器架设在Windows Server 2008 R2计算机上的话, 由于它内含**Windows 防火墙**, 而且默认已经打开, 故客户端连接这台FTP服务器的连接会被阻挡, 此时的解决方法如下 (参考图 9-90):

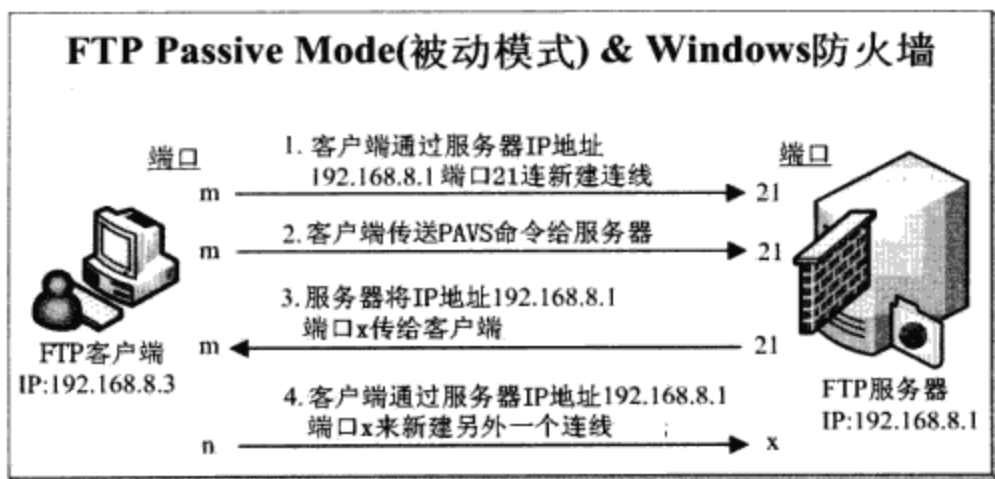


图 9-90

- 针对图 9-90 中 1 号箭头的控制通道传入连接 (incoming connection) 来说, 请在**Windows 防火墙**开放端口号 21。
- 针对图 9-90 中 4 号箭头的数据通道传入连接来说, 端口 x 是动态的 (此处说明也适用于 FTPS), 而 Windows Server 2008 R2 系统默认的动态端口范围是位于 49152~65535 之间, 因此您可以在**Windows 防火墙**来开放这一段范围的端口。

若觉得开放这么一大段范围的端口, 并不是很安全的话, Windows Server 2008 R2 FTP 服务器允许您将 FTP 服务器所使用的端口号固定在自行指定的一小段范围内, 此时您只要开放这一段范围即可: 【如图 9-91 所示单击 FTP 服务器的计算机名称 ➤ 单击 **FTP 防火墙支持** ➤ 在前图的数据通道端口范围处设置端口号范围 (例如图中的 50000~50100) ➤ 单击 **应用**】接下来通过【开始 ➤ 管理工具 ➤ 高级安全 Windows 防火墙】来开放这一段端口 (可能需要重新启动计算机)。



#### 提示

若在数据通道端口范围处输入0 - 0的话，表示采用Windows Server 2008 R2默认的动态端口范围，也就49152~65535。



图 9-91

### FTP客户端被动模式连接测试

完成以上设置后，客户端就可以利用被动模式来连接FTP服务器。浏览器Internet Explorer（与Windows资源管理器）默认是采用被动模式，因此您可以利用它来连接我们所架设的FTP服务器My FTP Site，已经启用Windows防火墙的Windows Server 2008 R2计算机。若您在前面曾经将浏览器Internet Explorer更改为主动模式的话，请先将其改回被动模式（参见前面的图9-86）。



#### 提示

Windows系统内置的FTP客户端程序ftp.exe默认是采用主动模式，但您可以在连接到FTP服务器后，通过literal pasv命令来切换到被动模式。

若您想要查看FTP客户端与FTP服务器之间的通信过程的话，可以利用CuteFTP或SmartFTP等软件来连接FTP站点，如图9-92所示为通过CuteFTP以PASV模式来连接FTP站点的界面，所使用的数据通道端口为50000。图中Entering Passive Mode (192,168,8,1,195,80)中的数字表示服务器的IP地址为192.168.8.1，端口为 $195 * 256 + 80 = 50000$ 。

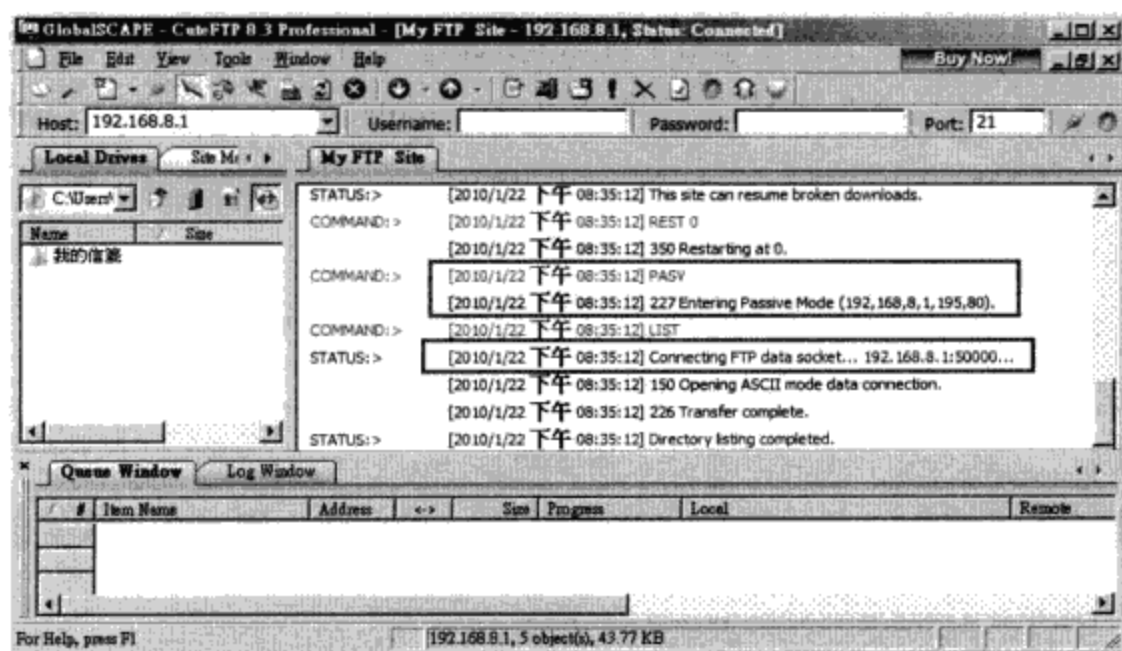


图 9-92

## 9-7 虚拟主机名

您可以在一台计算机内创建多个FTP站点，为了能够正确地区分出这些FTP站点，因此必须给予每一个站点唯一的识别信息，而用来识别站点的识别信息有**虚拟主机名**、**IP地址**与**TCP端口号**，这台计算机内所有FTP站点的这三个识别信息不可以完全相同。

其中虚拟主机名（virtual host name）主要的使用场合是：这台计算机只有一个IP地址，但您却要在其内架设多个FTP站点。此处我们并不介绍如何来架设多个FTP站点，只说明如何设置FTP站点的虚拟主机名与客户端要如何连接拥有虚拟主机名的FTP站点。

举例来说，若您要将My FTP Site的虚拟主机名设置为ftp1.sayms.com的话，请如图 9-93所示【单击My FTP Site右边的**绑定**，单击要更改的绑定后单击**编辑**，在主机名处输入ftp1.sayms.com，单击**确定**、**关闭**】。

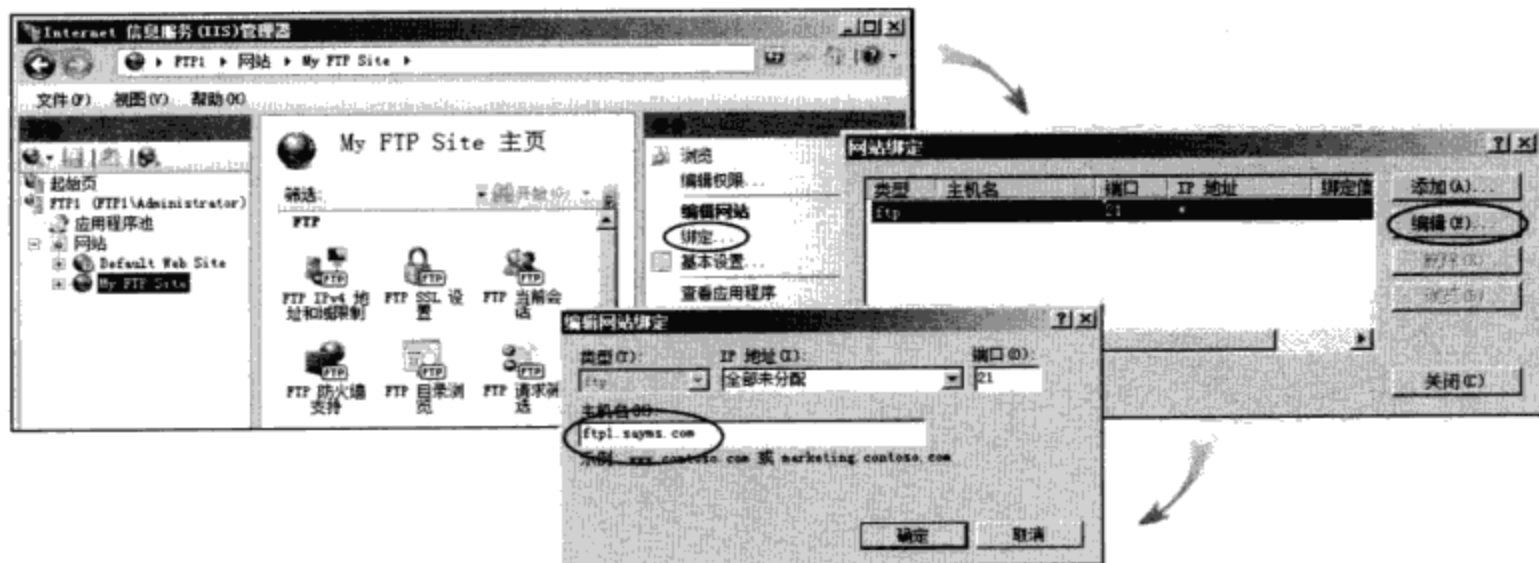


图 9-93

完成后，客户端要连接这个拥有虚拟主机名的FTP站点时，必须如图 9-94所示在登录账户前加上主机名ftp1.sayms.com与“|”符号，例如ftp1.sayms.com|anonymous或ftp1.sayms.com|George。

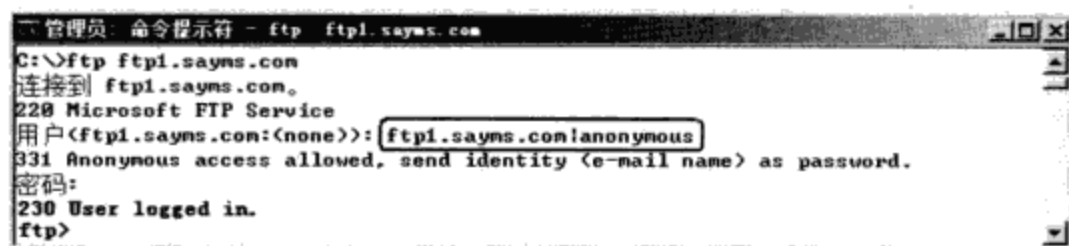


图 9-94

若连接时未输入虚拟主机名的话，将无法连接此FTP站点，同时会出现类似图 9-95所示的警示信息。

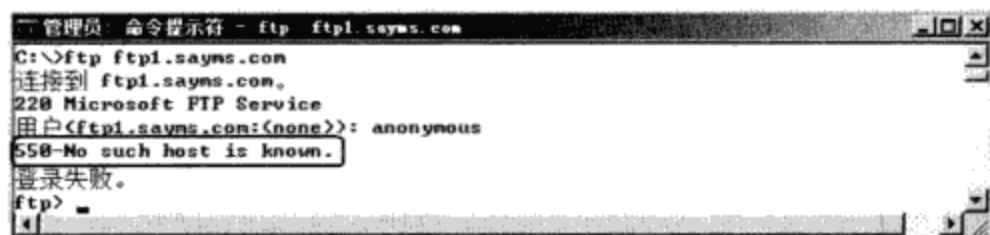


图 9-95



#### 提示

若要使用 **Windows 资源管理器** 或 Internet Explorer(IE)来连接FTP站点的话，请输入 **ftp://ftp1.sayms.com|anonymous@ftp1.sayms.com/**，其中anonymous为用户账号（可改用其他账户。IE需要重复输入一次账号与密码）。

如果这台服务器上还有另外一个FTP站点，而且它的IP地址与端口都与第1个站点相同，但是虚拟主机名不相同，例如为ftp2.sayms.com，则客户端要连接此FTP站点的话，同样需要在登录账户前加上主机名ftp2.sayms.com与“|”符号，例如ftp2.sayms.com|Anonymous或ftp2.sayms.com|George。