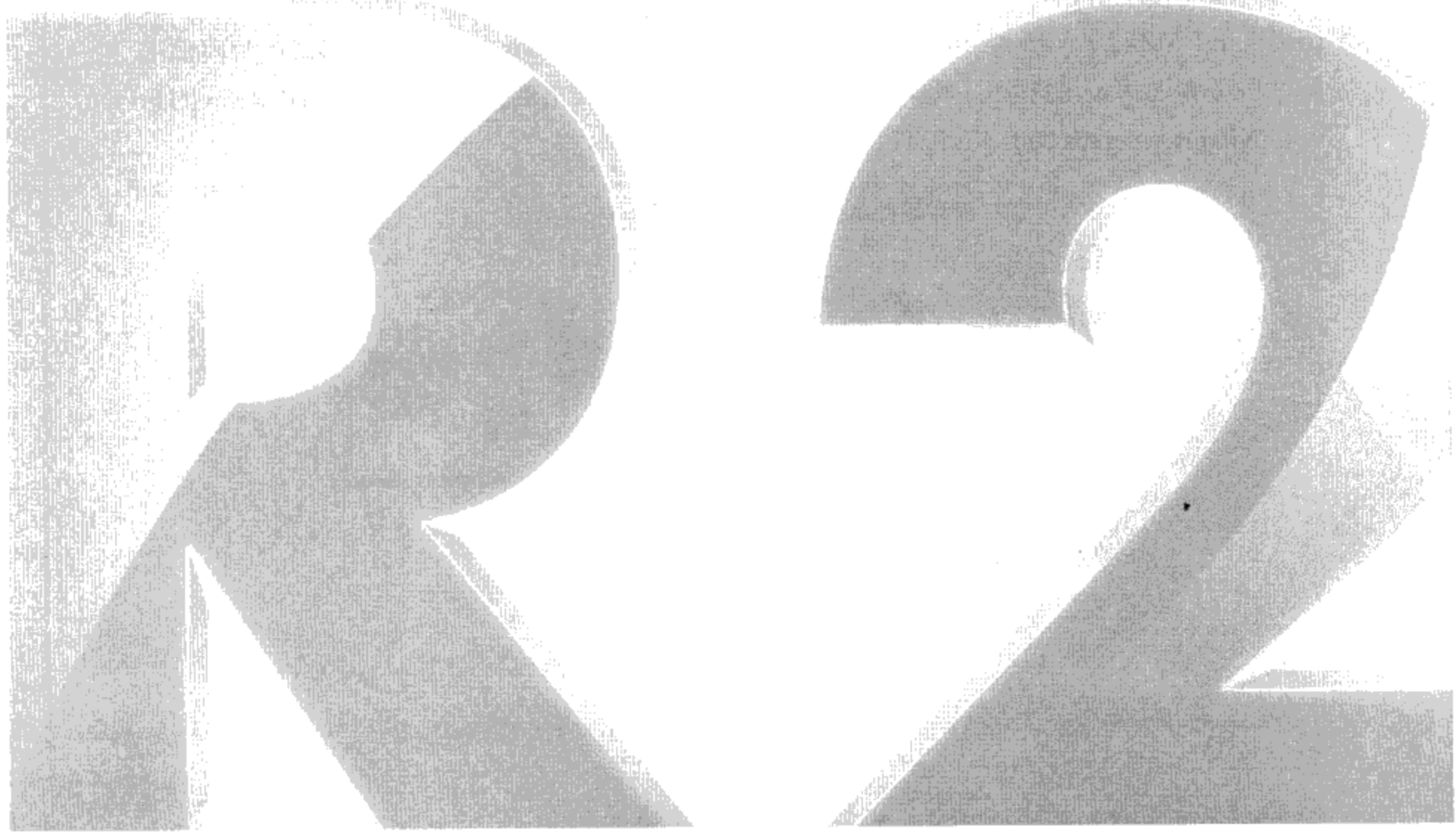
第8章

SMTP服务器的架设

SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）是用来发送与接收电子邮件的协议。Windows Server 2008 R2已内置SMTP服务器，因此您可以让IIS网站内的ASP.NET应用程序通过SMTP服务器来发送邮件，也可以让SMTP服务器扮演SMTP Relay（中转站）的角色来接收传入邮件或发送待发邮件。

- SMTP服务器概述
- 安装SMTP服务器与基本管理工作
- SMTP虚拟服务器的安全设置
- SMTP虚拟服务器的工作流程
- 邮件传递设置
- 邮件的管理
- SMTP域的管理
- SMTP Relay的设置



8-1 SMTP服务器概述

SMTP服务器主要的工作是提供电子邮件发送与接收的服务：

- **发送待发邮件**：发件人可以利用邮件软件（例如Windows Live Mail）将邮件发送给SMTP服务器，再由它将邮件发送给目的地的SMTP服务器。
- **接收传入邮件**：SMTP服务器也负责接收由其他SMTP服务器送来的邮件。

我们可以利用Windows Server 2008 R2的 SMTP服务器来支持IIS 7网页服务器内的ASP .NET应用程序，也就是在IIS网页服务器内指定一台Windows Server 2008 R2 SMTP服务器（见第5章），让使用System.Net.Mail API的ASP .NET应用程序可以利用这台SMTP服务器来发送邮件，如图 8-1所示。

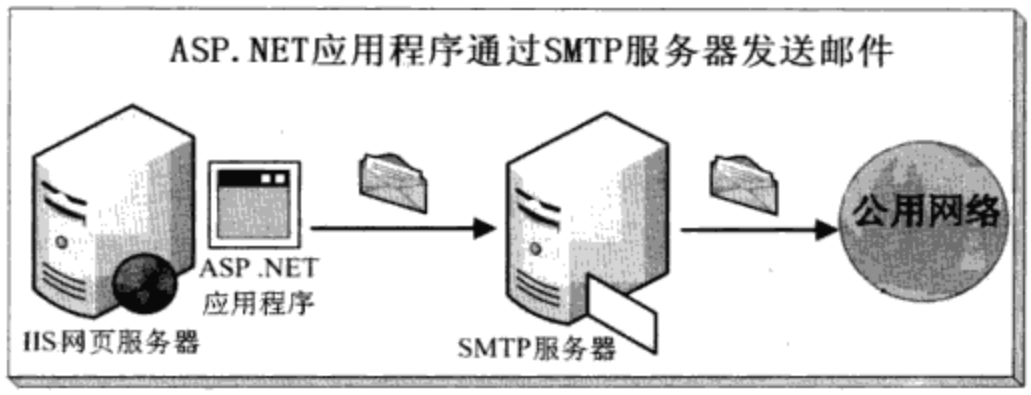


图 8-1

由于SMTP协议所使用的命令，可能会被入侵者用来作为攻击的途径，因此很多企业会通过SMTP Relay（中转站）来转寄邮件，例如图 8-2中的SMTP Relay被架设在外部因特网与内部网络之间的DMZ网络，所有外寄与传入的邮件都通过SMTP Relay，以避免外部直接与内部电子邮件服务器通信，这样可以减少内部电子邮件服务器被攻击的机会。这台SMTP Relay的角色可由Windows Server 2008 R2 SMTP服务器来扮演。

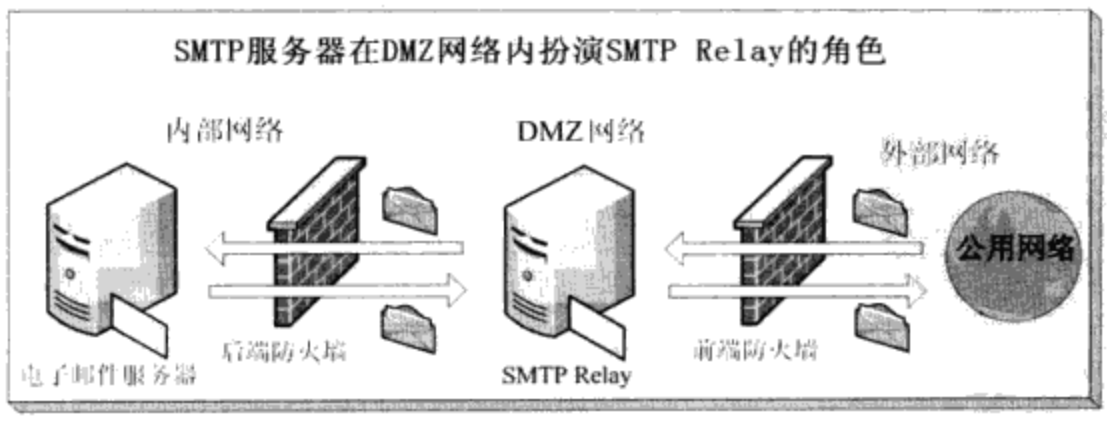


图 8-2

8-2 安装SMTP服务器与基本管理工作

我们需要通过添加**SMTP服务器**功能的方式来将SMTP服务器安装到Windows Server 2008 R2计算机上：【单击左下角**服务器管理器**图标➲功能➲添加功能➲如图 8-3所示选择**SMTP服务器**➲单击添加必需的角色服务➲依次单击下一步➲单击安装】。

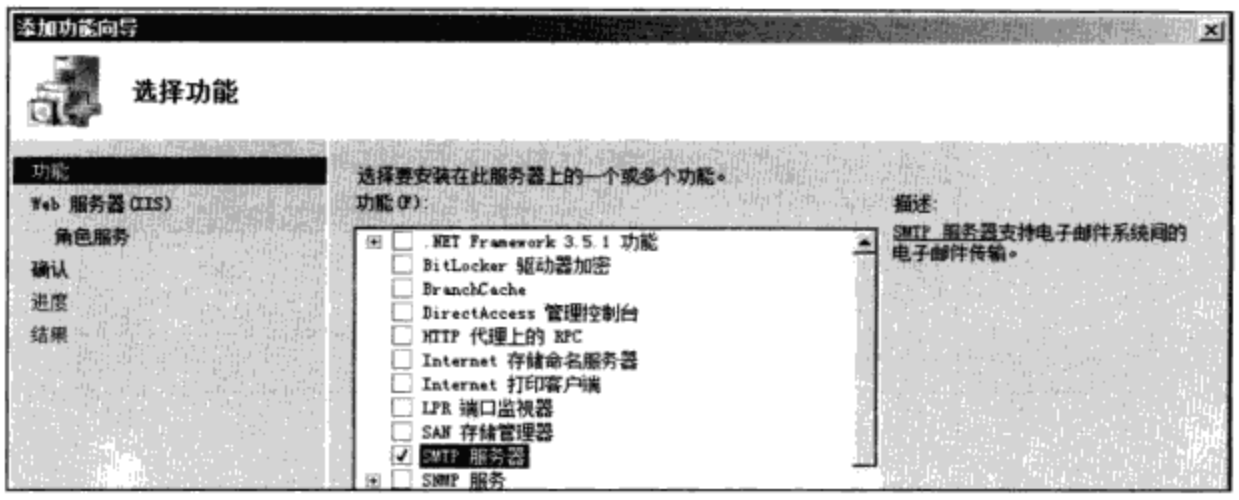


图 8-3

完成安装后会内置一个名为**SMTP Virtual Server #1**的SMTP虚拟服务器，而您可以通过【开始➲管理工具➲Internet 信息服务 (IIS) 6.0管理器】来管理SMTP服务器。

8-2-1 启动、停止与暂停SMTP虚拟服务器

系统默认会将**SMTP Virtual Server #1**启动，而您可以在单击图 8-4中的**SMTP Virtual Server #1**后，通过上方3 个图标来启动、停止与暂停它。

如果您需要对SMTP服务器进行设置更改或维护作业的话，此时可以将SMTP服务器暂停或停止：

- **暂停**：不再接受客户端新的连接请求，但是会继续服务现有的连接，同时已经收到、正在等待发送的电子邮件还是会继续发送。
- **停止**：现有连接都将中断、也不再接受新的连接、也不再发送电子邮件。

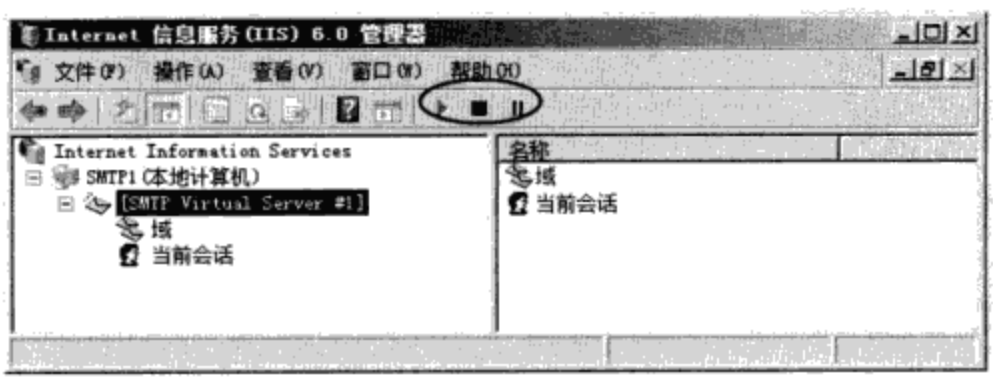


图 8-4

8-2-2 启动、停止与暂停SMTP服务

一台计算机内可以有多个SMTP虚拟服务器，而它们都是通过SMTP服务来运行。若您要启动、停止或暂停SMTP服务的话，可通过【开始➲管理工具➲服务➲ 简单邮件传输协议(SMTP)】的方法，如图 8-5所示。当停止或暂停此服务时，则所有的SMTP虚拟服务器都会被停止或暂停。

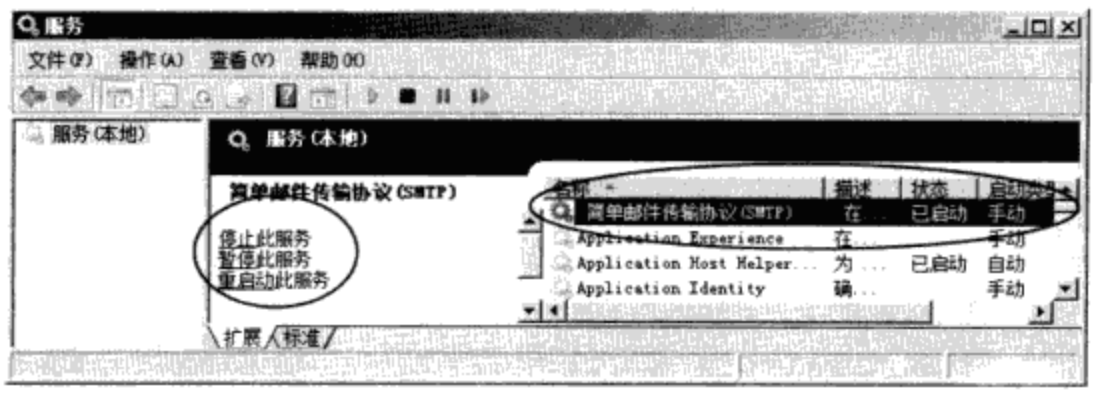


图 8-5

虽然SMTP服务在安装**SMTP服务器**功能时已被启动，不过它的启动类型为**手动**，因此以后计算机重新启动时都需自行手动启动。可将启动类型改为**自动**，请双击此服务，然后在图 8-6中选择**自动**。

提示

服务**启动类型**为**自动**表示系统在启动过程中（boot sequence）就会自动启动此服务，若要避免启动此服务而影响到系统启动效率的话，可以选择**自动（延迟启动）**，表示等完成系统启动程序后再启动此服务。

图 8-6

8-2-3 IP地址与TCP端口号的设置

若SMTP服务器这台计算机拥有多个IP地址的话，则您可以选择一个来提供SMTP服务，

此时SMTP服务器只接受通过此IP地址传来的电子邮件。

端口号是用来识别计算机内的TCP/UDP服务，而内置的**SMTP Virtual Server #1**的TCP端口号是标准的25。如果您要在一台计算机内架设多台SMTP虚拟服务器的话，则它们所使用的IP地址与端口号两者之中至少要有一个是不相同的。

若要更改SMTP Virtual Server #1的IP地址或端口号的话，请【在图 8-7选择SMTP Virtual Server #1➲单击上方的属性图标➲通过属性对话框来设置】。

若要同时更改IP地址与端口号的话，请【单击图 8-7前图右方的高级➲在图 8-8中单击编辑➲打开标识对话框来更改IP地址与TCP端口】。

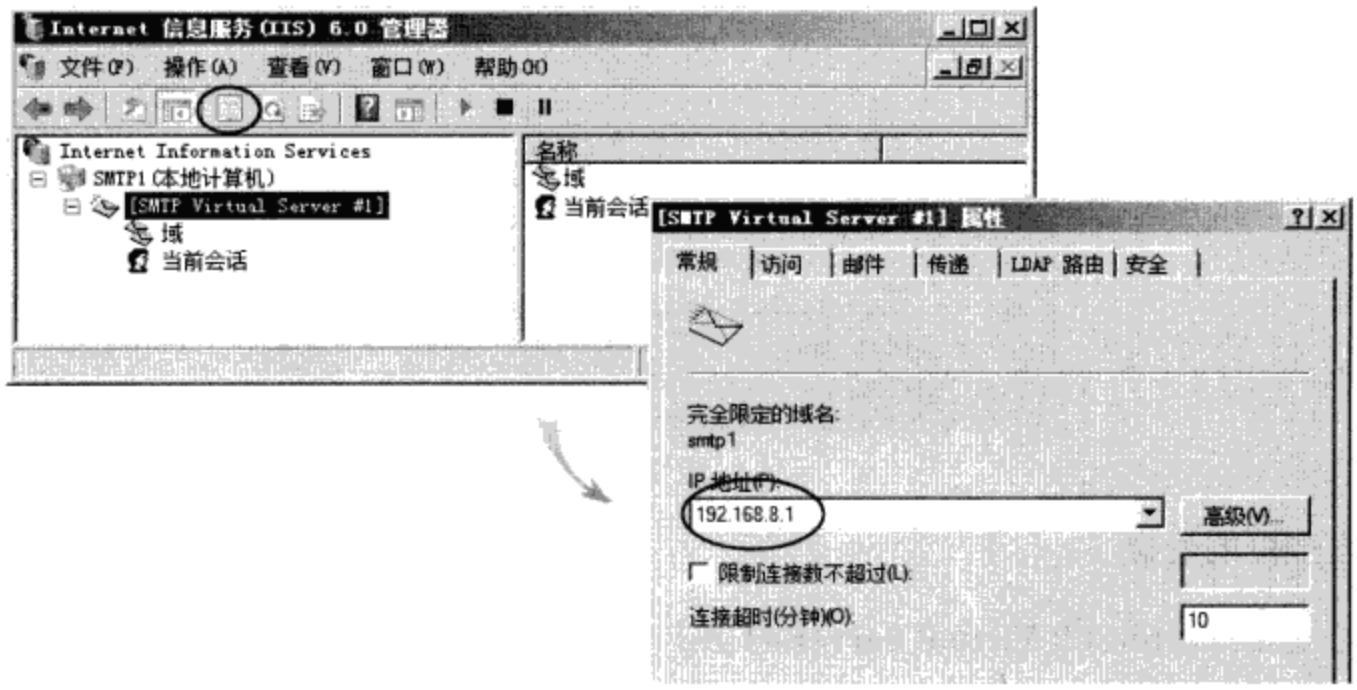


图 8-7

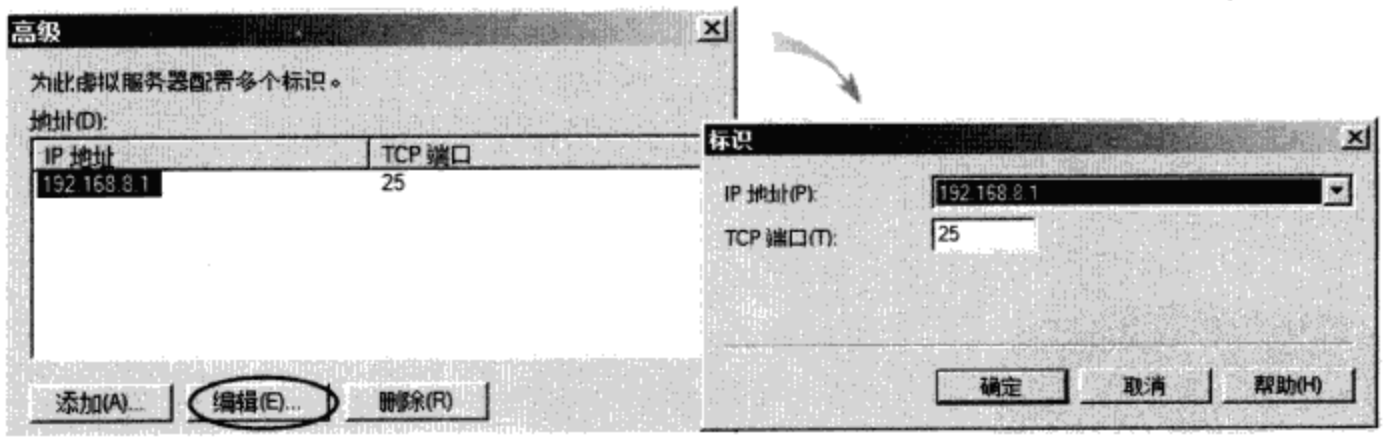


图 8-8

8-2-4 连接设置

当用户或其他SMTP服务器发送邮件给您的SMTP虚拟服务器时，两者之间就新建起一个连接（connection），或是您的SMTP虚拟服务器发送电子邮件给其他SMTP服务器时，两者之间也会新建一个连接。

您可以限制SMTP虚拟服务器的连接数量，以免服务器的负担太重，影响运行效率，同时也可以让入侵者攻击SMTP服务器的行为（例如Denial of Service，DoS）更为困难。

连入连接的设置

请选择【对着**SMTP Virtual Server #1**单击右键➲属性➲如图 8-9所示】：

- **限制连接数不超过**：用来设置同一时间内最大允许的连入数量。
- **连接超时（分钟）**：一个已经没有任何操作的连接，在这段时间过后就会被自动中断。

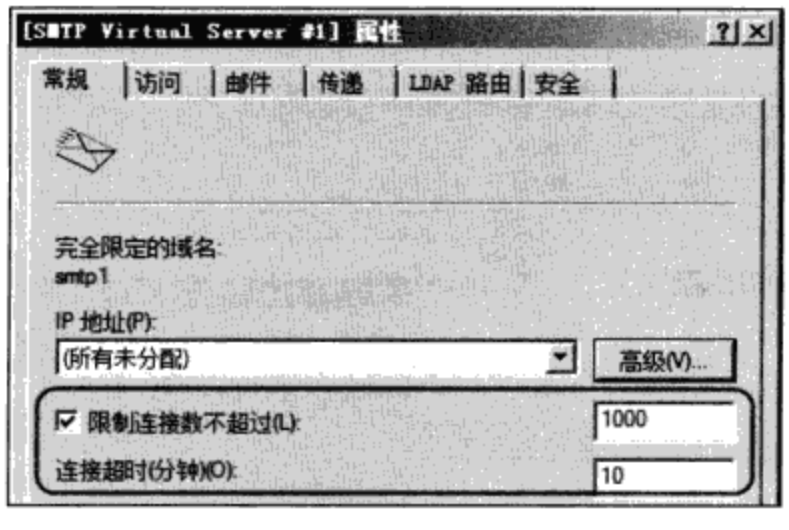


图 8-9

连出连接的设置

请通过【对着**SMTP Virtual Server #1**单击右键➲属性➲单击图 8-10中**传递**标签下的出站连接】的方法来设置：

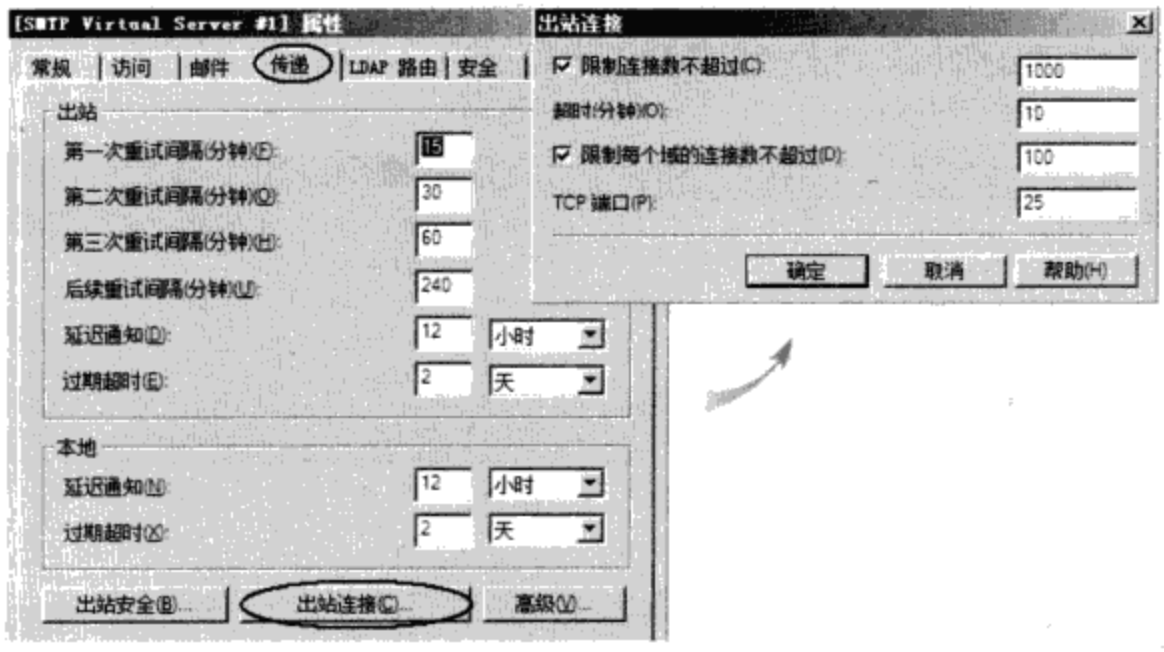


图 8-10

- **限制连接数不超过**：用来设置最大的连出数量。
- **超时（分钟）**：一个已没有任何操作的连接，在这段时间过后就会被自动中断。

- **限制每个域的连接数不超过**：用来设置每一个远程域（非此SMTP虚拟服务器所管辖的域）最多的连出数量，这个数值应该要少于或等于前面的**限制连接数不超过**。
- **TCP端口**：用来指定远程服务器的TCP端口号，默认值为25，表示要与远程服务器内支持端口号为25的SMTP服务来连接。

8-2-5 新建SMTP虚拟服务器

您可以在一台计算机内同时架设多个SMTP虚拟服务器，但是它们之间所使用的IP地址或端口号两者之中至少要有一个是不相同的。SMTP虚拟服务器的新建途径为【如图 8-11所示对着服务器名称单击右键➲新建➲虚拟服务器】，然后按照界面指示来操作即可。

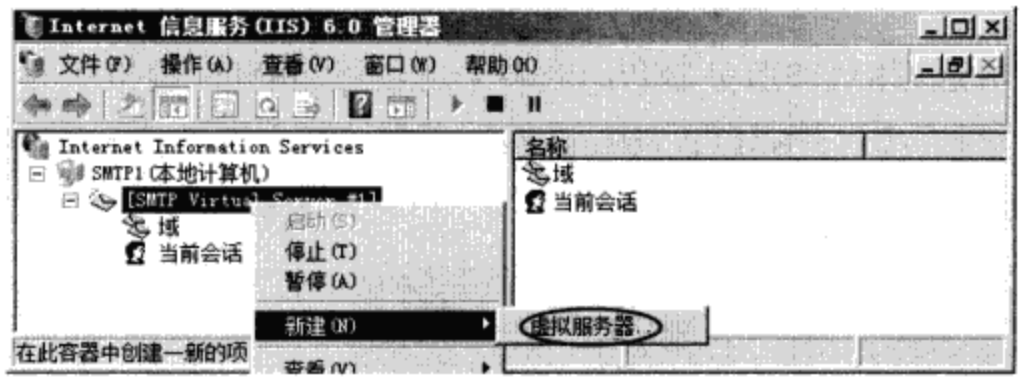


图 8-11

8-2-6 启用连接日志

您可以在前面图 8-7中选择**启用日志**，以便记录SMTP虚拟服务器的运行状况，例如利用它来检查是否有未经授权的用户尝试访问这台虚拟服务器。

8-3 SMTP虚拟服务器的安全设置

本节将介绍如何来指定SMTP虚拟服务器的操作员、连入/连出验证设置、利用IP地址来限制连接、中继限制与TLS安全连接设置等。

8-3-1 指定操作员

操作员有权限来访问与更改SMTP虚拟服务器的设置，指定操作员的途径为【对着**SMTP Virtual Server #1**单击右键➲属性➲单击图 8-12的**安全**标签➲单击添加】。

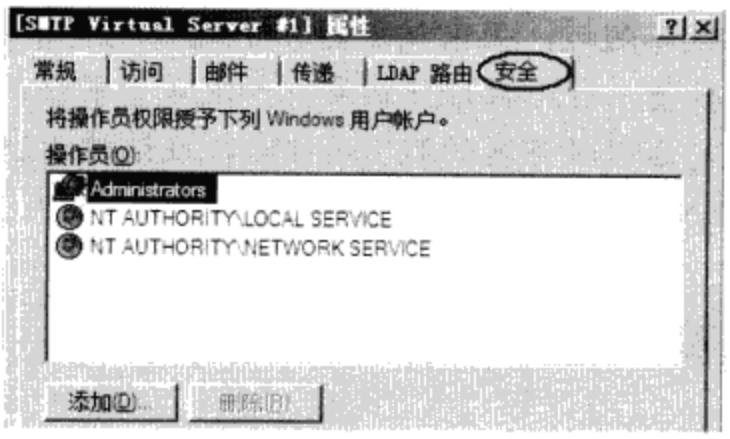


图 8-12

8-3-2 连入连接的验证设置

您可以让用户或远程SMTP服务器利用匿名来连接您的SMTP虚拟服务器，或要求他们提供用户名与密码来连接：【对着**SMTP Virtual Server #1**单击右键➲属性➲如图 8-13所示选择**访问**标签➲单击身份验证➲通过前图来设置】：

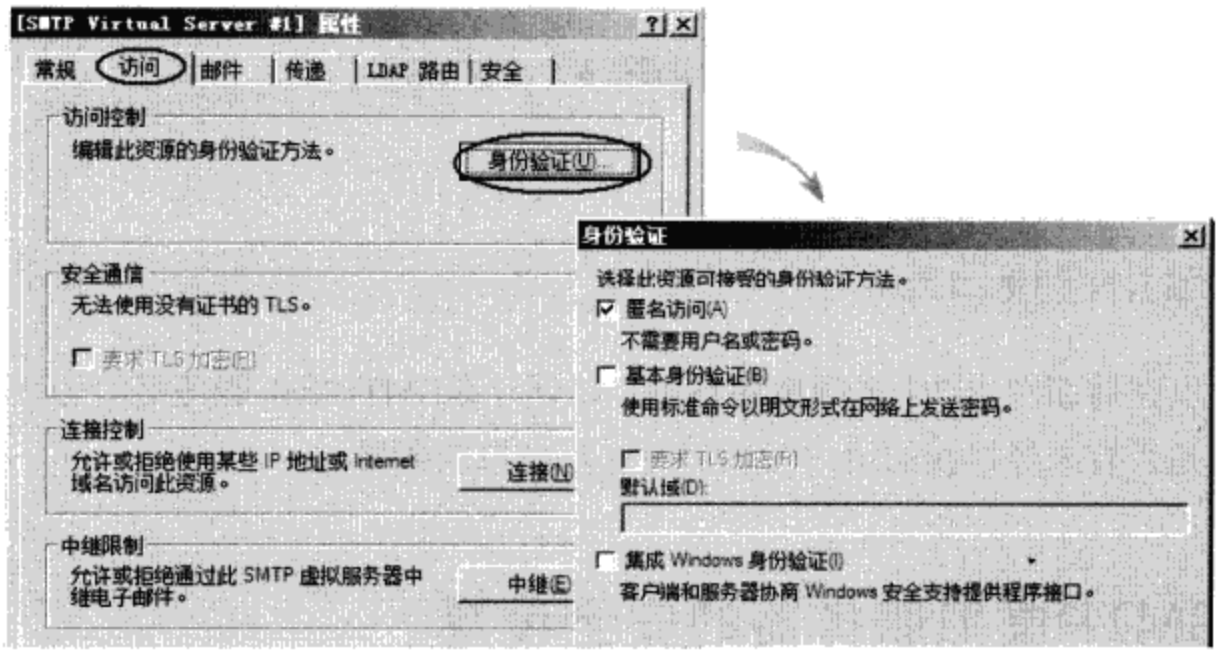


图 8-13

- **匿名访问**（Anonymous access）：表示用户或其他SMTP服务器，可以不需要提供用户名与密码来连接您的SMTP虚拟服务器。
- **基本身份验证**（Basic authentication）：表示需要用户或其他SMTP服务器提供用户名与密码来连接您的SMTP虚拟服务器，不过密码是以不加密的明文（cleartext）来发送，因此最好搭配图中的**要求TLS加密**（后述）。
- **集成Windows身份验证**：表示用户或其他SMTP服务器需要提供用户名与密码来连接您的SMTP虚拟服务器，而且密码会被加密。

以上验证方法与网站安全类似，请参考第5章内关于网站安全性的说明。

注意

若用户是利用匿名方式来连接SMTP服务器的话，则SMTP服务器默认仅接收入站的邮件，不接受外寄的邮件。

8-3-3 连出连接的验证设置

当您的SMTP服务器要将邮件转发到其他SMTP服务器时，您必须视对方的验证要求来选择适当的验证方法：【对着**SMTP Virtual Server #1**单击右键➲属性➲如图 8-14所示单击**传递**标签下的出站安全➲通过前图来设置】：

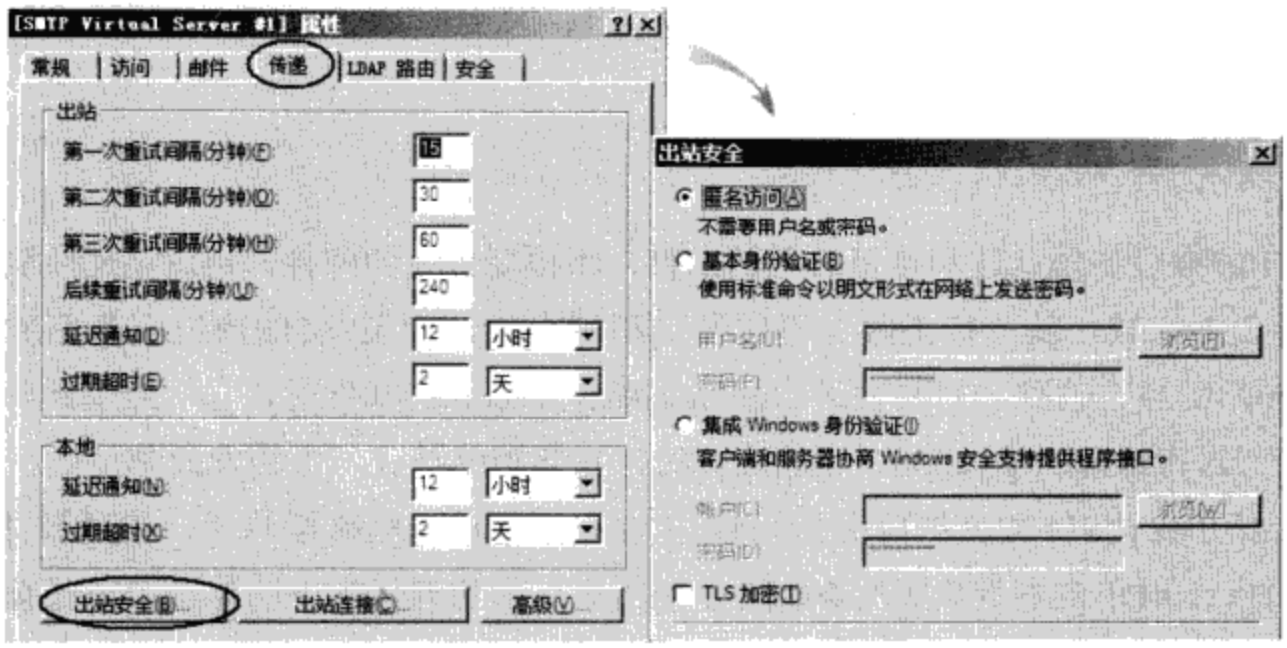


图 8-14

- **匿名访问**：表示利用匿名的方式来连接其他的SMTP服务器。
- **基本身份验证**：表示需提供用户名称与密码来连接其他SMTP服务器，其密码是以不加密的明文（cleartext）来发送。
- **集成Windows 验证**：表示需提供用户名与密码来连接其他SMTP服务器，其密码会加密。
- **TLS加密**：若对方要求采用TLS方式来将连接加密的话，请选择图中的**TLS加密**。

8-3-4 利用IP地址来限制连接

您可以允许或拒绝某台特定计算机、某一群计算机来连接您的SMTP虚拟服务器：【对着**SMTP Virtual Server #1**单击右键➲属性➲如图 8-15所示单击**访问**标签下的连接➲通过前图来设置】，默认是允许所有的计算机来连接。这些设置与第5章网站安全的设置相同。

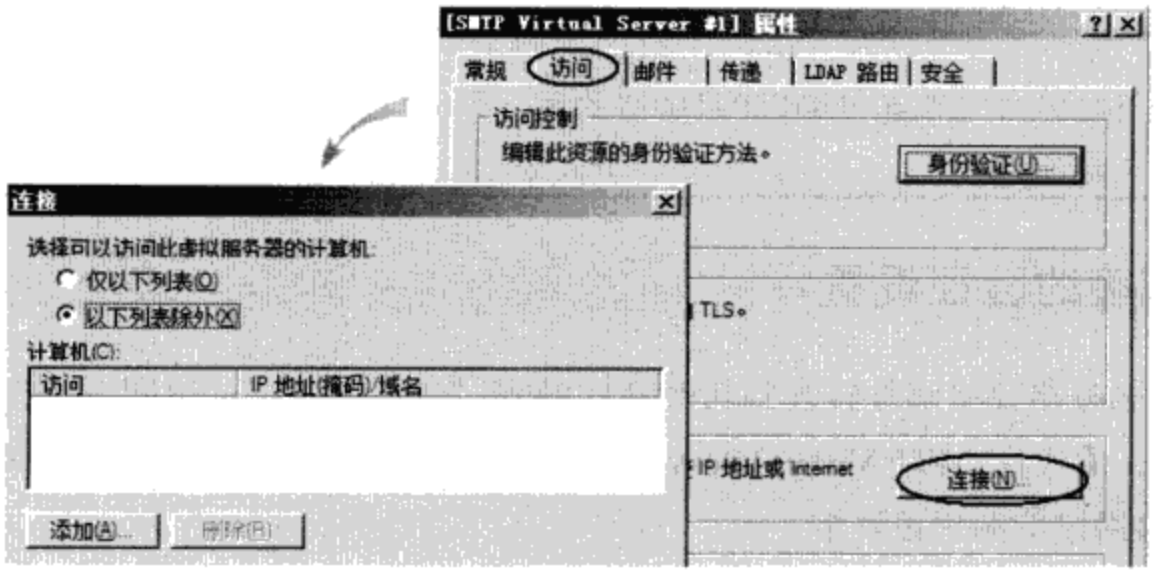


图 8-15

8-3-5 设置或删除中继限制

SMTP虚拟服务器默认只接受传入的邮件，不接受外寄的邮件，也就是所收到的邮件，若不是它所负责的域，就一律拒收、不转发。举例来说，如果SMTP虚拟服务器所管辖的域为sayms.com，则当它收到一封要发送给george@sayms.com的邮件时，它会接受此邮件，可是如果它收到一封寄给mary@yahoo.com的邮件时，它会拒绝接收、不转发此邮件。

如果要开放让SMTP虚拟服务器可以中继（relay）待发邮件的话，请通过【对着**SMTP Virtual Server #1**单击右键➲属性➲如图 8-16所示单击**访问**标签下的中继➲通过前图来设置】的方法，图中您可以通过单击添加来选择要为哪一些计算机转发外寄的邮件。

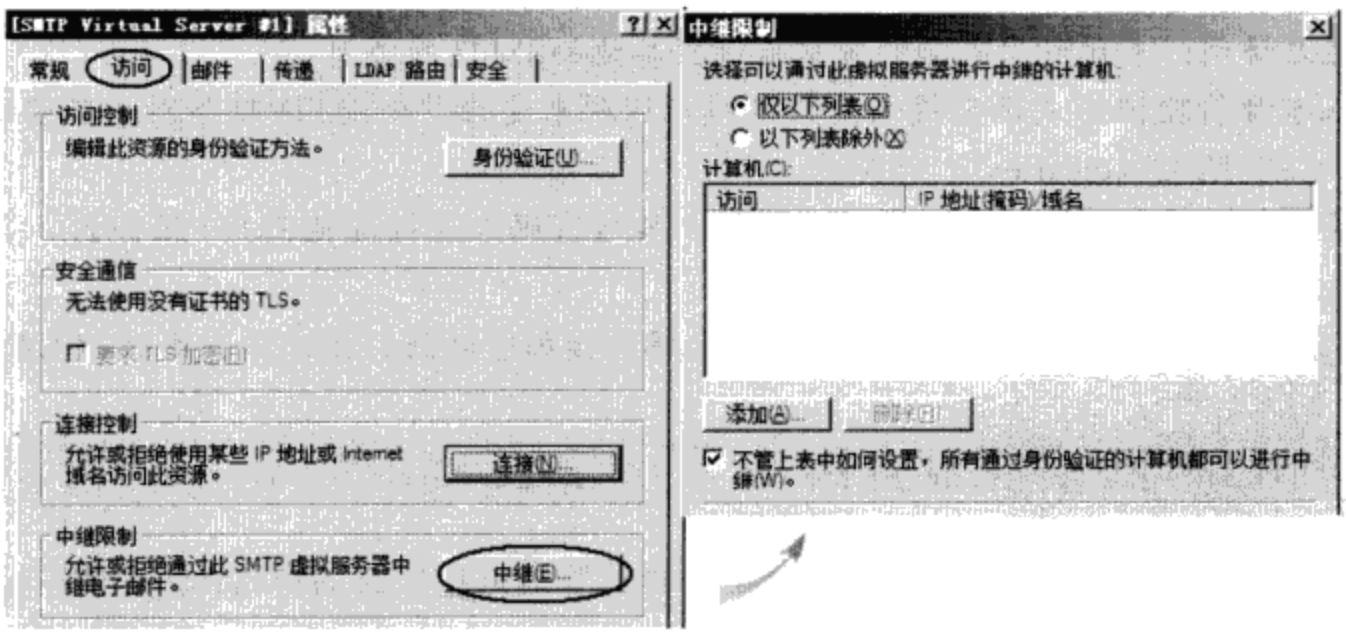


图 8-16

另外图中默认已经选择**不管上表中如何设置，所有通过身份验证的计算机都可以进行中继**，表示只要发件人能够提供有效的用户名与密码，就为他们转发外寄的邮件，不论他们所使用的计算机是否列在上述列表内。不过您还必须在这个SMTP虚拟服务器内添加验证方法，

也就是在前面的图 8-13中增加选择**基本身份验证**或**集成Windows身份验证**。

8-3-6 TLS安全连接设置

用户或远程SMTP服务器可以采用TLS（Transport Layer Security）安全连接来连接到您的SMTP虚拟服务器 也就是将所有发送的数据经过TLS加密。TLS是一种类似SSL（Secure Sockets Layer）的安全协议。

如果SMTP虚拟服务器的验证方法是选择**基本身份验证**的话，发件人所发送的用户名与密码都是以不加密的方式来发送，此时可以采用TLS加密来增加其发送的安全性。

启用SMTP虚拟服务器的TLS

若要启用TLS功能的话，就需为SMTP虚拟服务器申请证书与安装证书，这些概念与步骤都与网站的SSL类似（可参考第6章），此处仅列其重要步骤：

- **安装与网站有关的角色服务**：由于新建证书申请文件、完成证书安装等步骤需要通过**Internet信息服务(IIS)管理器**来完成，故您需要先暂时在这台SMTP服务器计算机上新建与IIS网站有关的角色服务：【单击左下角**服务器管理器**图标➲展开**角色**➲单击**Web服务器(IIS)**➲单击右方的**添加角色服务**➲选择**一般HTTP功能**与**IIS管理控制台**➲...】。
- **创建证书文件申请**：请通过【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**创建证书申请...**】的方法来创建证书申请文件，注意输入数据时，在**通用名称**处必须输入SMTP服务器的FQDN。
- **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。若SMTP虚拟服务器这台计算机尚未信任CA的话，请先执行信任CA的步骤。
- **安装证书**：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**完成证书申请...**】安装时请选择刚才所下载的证书。

提示

如果SMTP服务器是隶属于Active Directory域，而且企业CA在线的话，则您可以通过以下步骤来申请与安装证书【开始➲运行➲输入**MMC**后按Enter键➲**文件**菜单➲添加/删除管理单元➲在列表中选择**证书**后单击添加➲选择**计算机账户**➲单击下一步、完成、确定➲展开**证书**➲对着**个人**单击右键➲所有任务➲申请新证书➲单击两次下一步➲选择**计算机**➲单击**详细信息**右边的图标➲单击属性➲在**常规**标签下输入友好的名称➲单击**用户**标签➲在**用户名称**的**类型**处选择**公用名**、在**值**处输入SMTP虚拟服务器的FQDN后按添加➲在**备用名称**的**类型**处选择**DNS**、在**值**处输入SMTP虚拟服务器的FQDN后按添加➲单击**扩展信息**标签➲单击**扩展的密钥用法（应用程序策略）**右边的图标、确认**服务器身份验证**已被选择➲单击**证书颁发机构**标签、确认已选择发放证书的CA➲单击确定、注册、完成】。执行以上步骤前，请确认SMTP服务器已经信任该企业CA，否则请先运行gpupdate来应用组策略。

完成证书安装后，默认并不会强迫发件人使用TLS加密方式将邮件寄给此台SMTP虚拟服务器，而是由发件人自行决定是否要使用TLS加密。

如果SMTP虚拟服务器的验证方法是**基本身份验证**，同时您要强迫发件人使用TLS加密来连接SMTP虚拟服务器的话，请【对着**SMTP Virtual Server #1**单击右键➲属性➲单击图 8-17中**访问**标签下的身份验证➲选择前图**基本身份验证**处的**要求TLS加密**】。

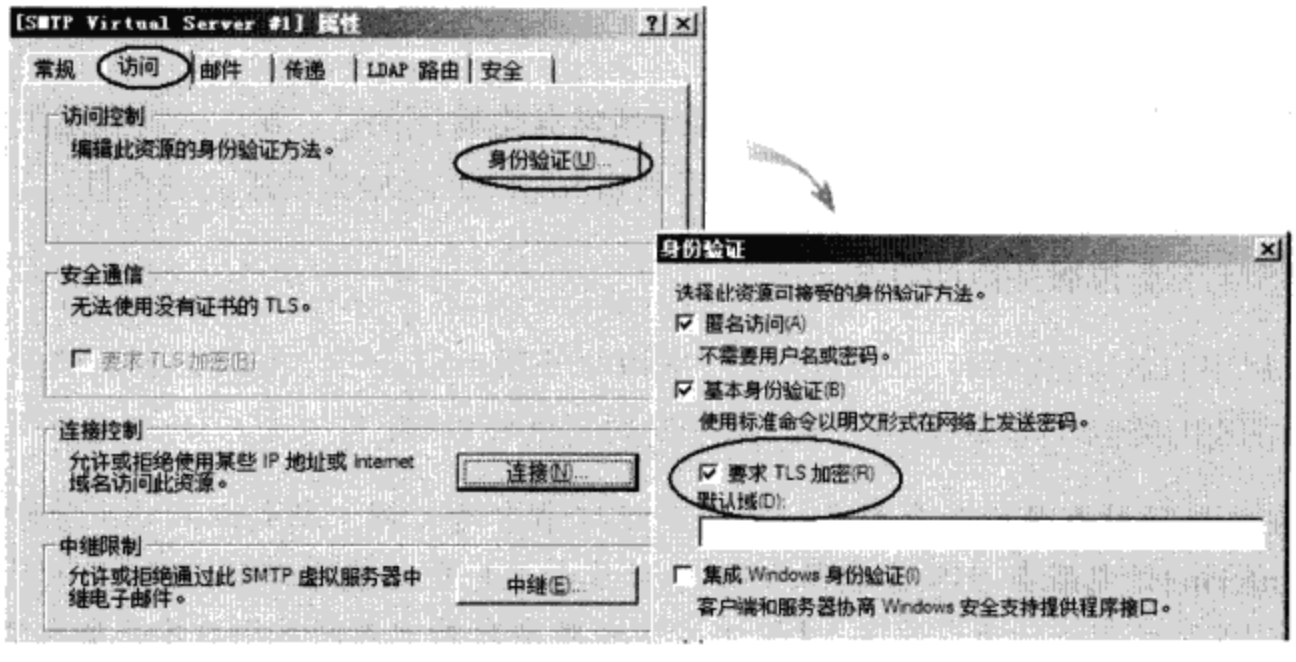


图 8-17

您可以要求发件人不论采用哪一种验证方法都需使用TLS加密：【对着**SMTP Virtual Server #1**单击右键➲**属性**➲单击图 8-18中的**访问**标签➲选择**要求TLS加密**】。若SMTP虚拟服务器没有安装证书的话，将无法选择此选项。

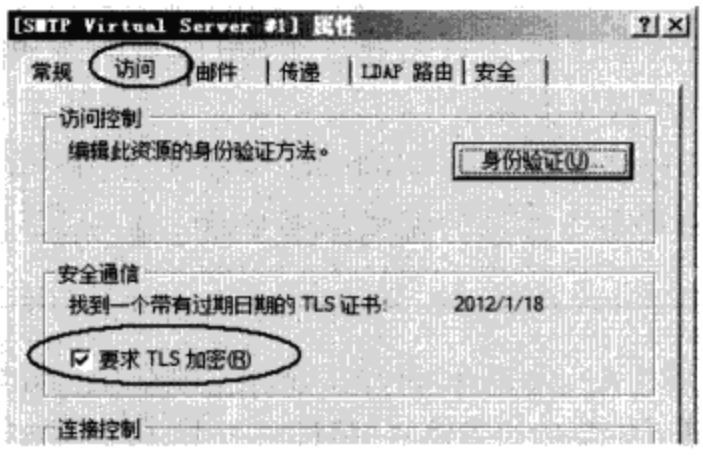


图 8-18

客户端的设置

假设用户的计算机是Windows 7，且是通过Windows Live Mail来收发电子邮件，则其启用TLS安全连接的方法为：【运行Windows Live Mail➲按Alt键➲**工具**菜单➲账户➲选择邮件账户➲单击属性➲如图 8-19所示在**服务器**标签下的**待发邮件（SMTP）**处输入SMTP虚拟服务器的FQDN】，注意此FQDN必须与当初替SMTP虚拟服务器申请证书时，在**通用名称**处所输入的FQDN相同，不可以输入IP地址。

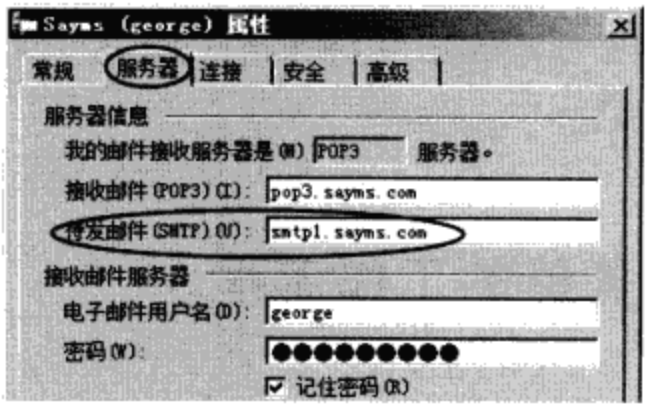


图 8-19

还有需在图 8-20中**高级**标签下选择**此服务器要求安全连接（SSL）**。

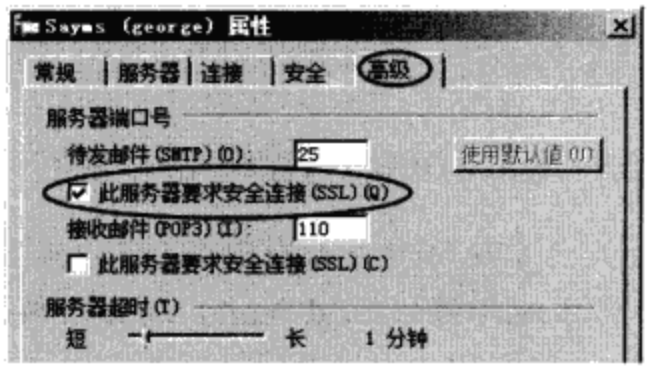


图 8-20

提示

若用户的计算机尚未信任CA的话，则应该还要执行信任CA的程序（参阅第6章的说明）。

远程SMTP服务器的设置

若远程SMTP服务器也是Windows Server 2008 R2 SMTP虚拟服务器的话，则其启用安全连接来连接您的SMTP虚拟服务器的途径为:【在这台SMTP服务器上对着**SMTP Virtual Server #1**单击右键➲属性➲在图 8-21中单击**传递**标签下的出站安全➲选择**TLS加密**】。

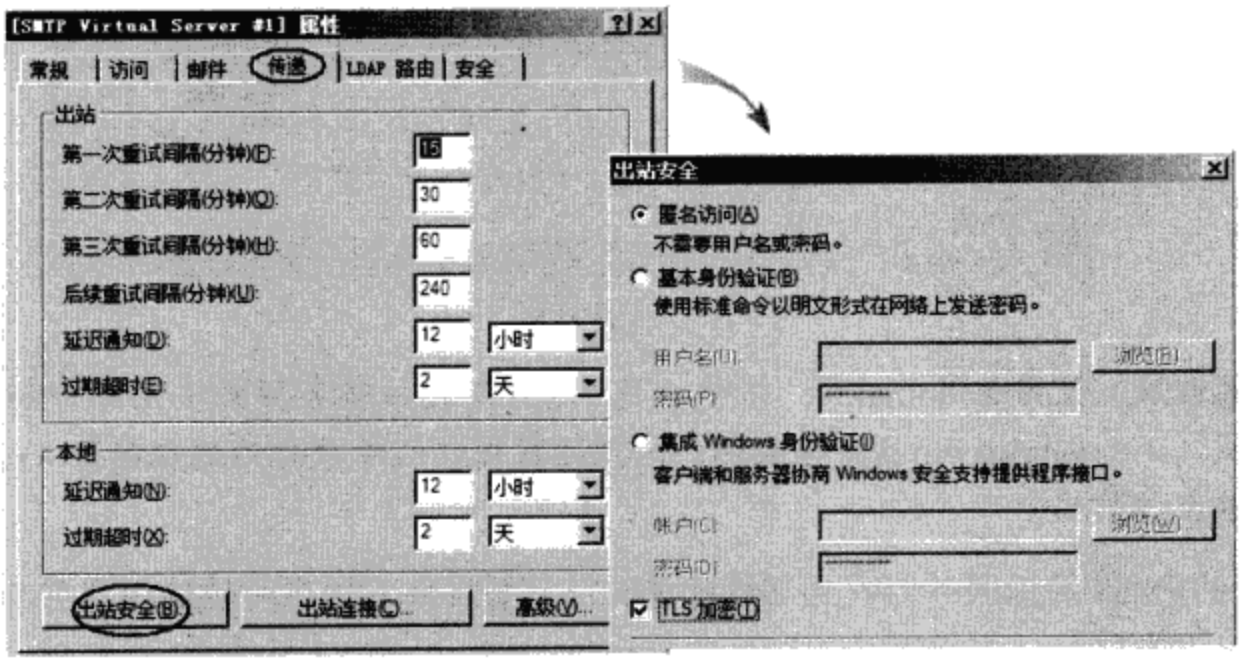


图 8-21

同理，若您的SMTP虚拟服务器要利用TLS来连接远程SMTP服务器的话，则您的SMTP服务器也必须如图 8-21所示来设置。

8-4 SMTP虚拟服务器的工作流程

本节将介绍SMTP域、SMTP的文件夹结构与SMTP工作流程，这些信息可以协助您找出SMTP虚拟服务器无法正常发送邮件的原因。

8-4-1 SMTP域类型

SMTP域用来组织邮件，它与Active Directory域不相同。我们可以将SMTP域分为以下两种：

- **本地域**（local domain）：本地域就是此台SMTP虚拟服务器所管辖的域，所有要发送到此域的邮件都被称为**本地邮件**（local mail）或**传入邮件**，当SMTP虚拟服务器收到本地邮件时，会将此邮件储存到指定的文件夹。本地域又分为以下两种（参见图 8-22）：
  - **本地默认域**：例如图 8-22中的SMTP1.sayms.com就是本地默认域，此域的默认名称为这台服务器的FQDN，您可以通过【开始➲对着**计算机**单击右键➲属性➲计算机全名】来查看此名称。此域不可以被删除，但是可以更改其域名。
  - **本地别名域**：您可以替本地默认域另外设置一个别名（alias），所有要发送到本地别名域的邮件就等于是要发送给本地默认域。图 8-22中的sayms.com就是本地别名域。

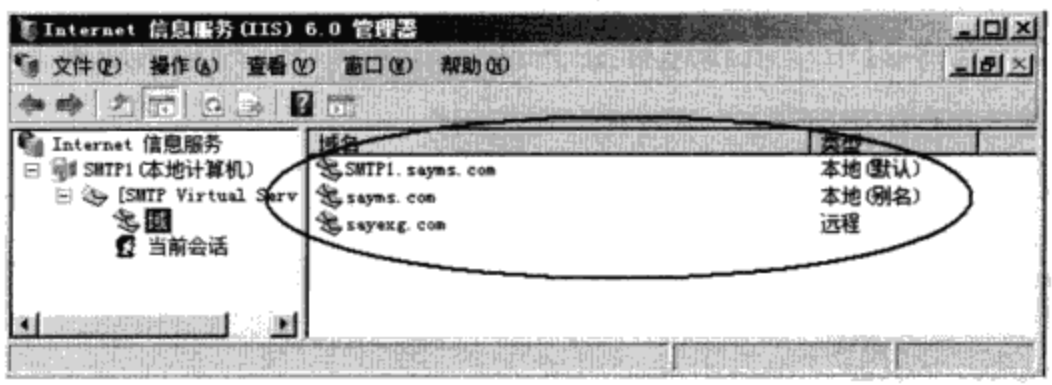


图 8-22

- **远程域**（remote domain）：不是由您的SMTP虚拟服务器来提供服务的域就称为远程域，例如yahoo.com就是远程域，送到远程域的邮件被称为**远程邮件**（remote mail）或**待发邮件**。

当您的SMTP虚拟服务器收到远程邮件时，只要发件人提供有效的用户名与密码，它便可以通过DNS服务器（MX资源日志，参见第4章）来查找远程域的SMTP服务器，并将邮件送到此SMTP服务器。

您可以针对某个特定远程域进行不同的发送设置，不过您需要添加该远程域（例如图 8-22中的sayexg.com），然后再做适当的设置，例如设置当SMTP虚拟服务器接收到发往sayexg.com域的邮件时，便将它转发给指定的另一台SMTP服务器来处理，而不是通过DNS服务器来查找该域的SMTP服务器。

8-4-2 SMTP服务器的文件夹结构与发送流程

SMTP服务器安装好后，系统会在**%*systemdrive*%\inetpub\mailroot**文件夹内新建多个子文件夹，如图 8-23所示，这些文件夹与SMTP虚拟服务器发送邮件的流程有着密切的关系。

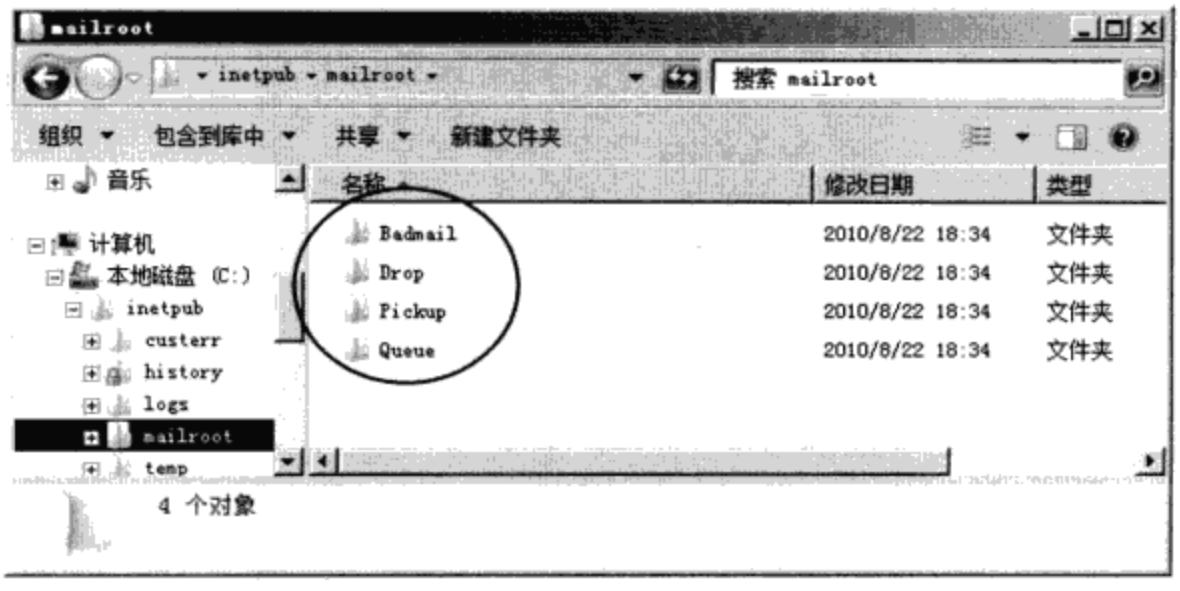


图 8-23

要发送到SMTP虚拟服务器的邮件，可以通过TCP端口（默认为25）传进来或直接将符合邮件格式的文件复制到**Pickup**文件夹内，无论是通过哪一个途径，当SMTP虚拟服务器收到这些邮件后，都会将它们放置到**Queue**文件夹内，然后再视邮件为本地邮件或远程邮件而有不同的处理方式：

- **本地邮件**：若所收到的邮件是属于本地默认域或本地别名域的话，就会将它们从**Queue**文件夹转移到**Drop**文件夹内。
- **远程邮件**：若所收到的邮件是属于远程邮件的话，它的处理步骤如下：
  - 邮件仍然是被放置在**Queue**文件夹内，不过会经过分类、排序，以便提高发送的效率。
  - 与远程SMTP服务器通信，如果远程SMTP服务器已经准备好接收邮件，就开始将邮件发送出去；如果尚未准备妥当，则邮件仍然放置在**Queue**文件夹内等待下一次的发送。
  - 如果邮件本身有问题，例如格式有误，则该邮件会被转移到**Badmail**文件夹内。
  - 如果邮件无法被发送到目的地，则这封邮件将被退回给用户，并附上**未送达报告**（non-delivery report，NDR）。NDR会被放置到**Queue**文件夹内按照邮件发送的程

序来处理。

■ 如果NDR无法被发送出去的话，它会被转移到**Badmail**文件夹内。

8-5 邮件传递设置

本节我们将介绍邮件传递设置选项，例如重试间隔时间、跃点计数、FQDN、智能主机与反向DNS查询等，这些设置都可通过【对着**SMTP Virtual Server #1**单击右键➲属性➲如图 8-24所示的**传递**标签】的方法来设置。

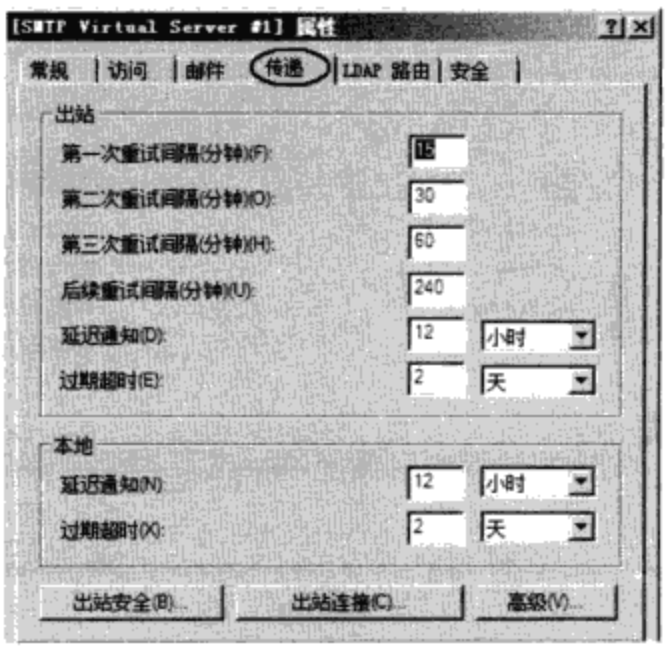


图 8-24

8-5-1 重试与间隔时间设置

当SMTP虚拟服务器传递邮件失败时，它会间隔一段时间后再尝试重试，这些间隔时间的相关设置如图 8-24所示，图中您可以分别设置前三次的间隔时间与第三次以后的间隔时间（后续重试间隔）。除此之外，不论是外寄的远程邮件或传入的本地邮件，都还可以有以下两个设置：

- **延迟通知**（Delay notification）：如果发件人的邮件一直没有被成功发送出的话，则在过了**延迟通知**时间后，SMTP虚拟服务器会寄一封邮件通知发件人其邮件尚未发出。
- **过期超时**（Expiration timeout）：如果过了这段时间后，邮件还是没有被成功寄出的话，则这封邮件会退回给发件人，并附上**未送达报告**（NDR）。NDR会被放置到**Queue**文件夹内按照邮件发送的程序来处理。

8-5-2 邮件跃点计数设置

邮件在传递过程中，在尚未到达目的地之前，途中可能会经过多台SMTP服务器来转发，

每一台SMTP服务器被称为一个**跳跃点**（hop）。您可以设置SMTP虚拟服务器所能够接受的最大跳跃点数，设置的途径为单击前面图 8-24右下方的高级，然后通过图 8-25中的**最大跃点计数**来设置。

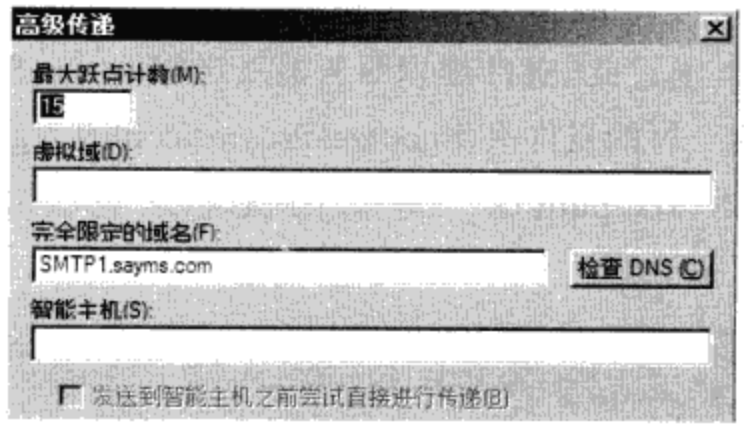


图 8-25

图中默认值为15，表示当SMTP虚拟服务器接收到邮件后，它会检查邮件头（header）中有几行Received字段，以便计算总共经过了多少台SMTP服务器，如果已经超过了15台，它就会退回此邮件，例如图 8-26中总共有两行Received，表示总共经过两台SMTP服务器。

图 8-26

提示

想要自行做实验来得到上述界面吗？您可以采用以下步骤：【架设两台SMTP服务器➲分别在这两台服务器上将本地默认域改名为sayms.com与sayexg.com➲在sayms.com这台服务器上另外新建远程域（参见章节8-7）、将此远程域的邮件转给第2台服务器（sayexg.com）➲运行Windows Live Mail➲利用george@sayms.com的身份寄送一封邮件给mary@sayexg.com➲到第2台服务器的C:\inetput\mailroot\Drop文件夹查找此封邮件、利用**记事本**打开它】。

8-5-3 虚拟域设置

您可以利用**虚似域**来替代邮件中的本地域名，例如SMTP服务器的本地域名为sayms.com，而在图 8-27中**将虚似域**设置为123.com，若发件人的电子邮件信箱为george@sayms.com，则当其通过此SMTP虚拟服务器发送邮件时，SMTP虚拟服务器会将邮件头（header）内的**x-sender**这一行的发件人由george@sayms.com改为george@123.com，如图 8-28所示；同时邮件头内**Return-path**这一行的回复地址也会由george@sayms.com改为george@123.com。

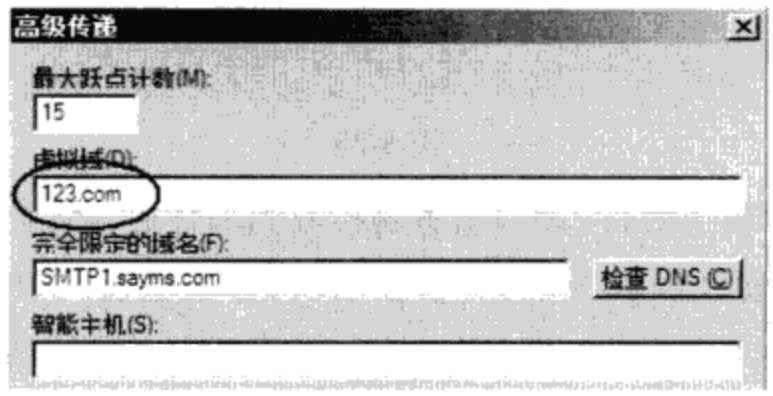


图 8-27

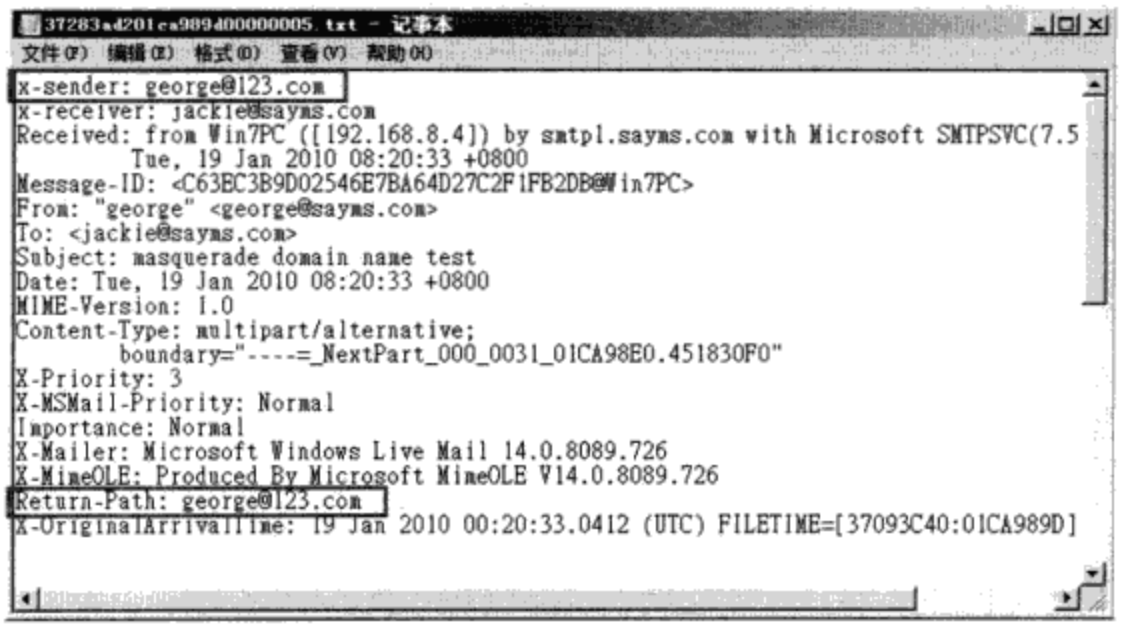


图 8-28

提示

由上图可看出**From**这一行的域名并没有改变，还是维持原来的george@sayms.com。如果邮件寄送过程中会经过多台的SMTP服务器的话，则只有第1台SMTP服务器会通过**虚拟域**来更改上述字段内的域名。

8-5-4 Fully Qualified Domain Name(FQDN)设置

SMTP虚拟服务器**SMTP Virtual Server #1**的FQDN默认就是这台计算机的**计算机全名**（full

computer name），例如smtp1.sayms.com，因此只要是通过这台SMTP虚拟服务器所送出的邮件，其报头（header）内就会记载着这个名称，表示邮件是由这台SMTP服务器送出。当您通过【开始➲对着**计算机**单击右键➲属性➲更改设置】的途径来更改**计算机全名**后，此台SMTP虚拟服务器的FQDN也会自动改变。

您也可以通过图 8-29中的**完全限定的域名**来设置这台SMTP虚拟服务器的FQDN，此处的设置优先于计算机的**计算机全名**。

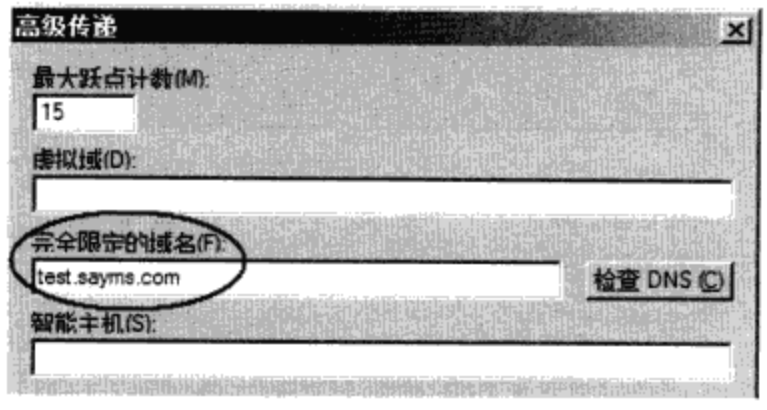


图 8-29

举例来说，若您如图中所示将**完全限定的域名**改为test.sayms.com后（应该要按检查DNS来确定找得到其IP地址），则所有通过这台SMTP虚拟服务器所寄出的邮件，其报头内所记载的SMTP服务器名称将是test.sayms.com，如图 8-30所示，图中的test.sayms.com原本应该是smtp1.sayms.com。

图 8-30

8-5-5 智能主机设置

当您的SMTP虚拟服务器要发送远程邮件时，它会通过DNS服务器（MX资源日志）来查找这封远程邮件所属的SMTP服务器，然后将邮件发送给此台SMTP服务器。不过您的SMTP

服务器也可以不需要通过DNS服务器，而是直接将邮件转发给特定的SMTP服务器，然后由这台SMTP服务器来负责发送邮件，这台特定的SMTP服务器被称为**智能主机**（smart host）。

智能主机可通过图 8-31来设置，您可以输入智能主机的FQDN或IP地址，若输入IP地址的话，需在IP地址前后加方括号，例如[192.168.8.83]。

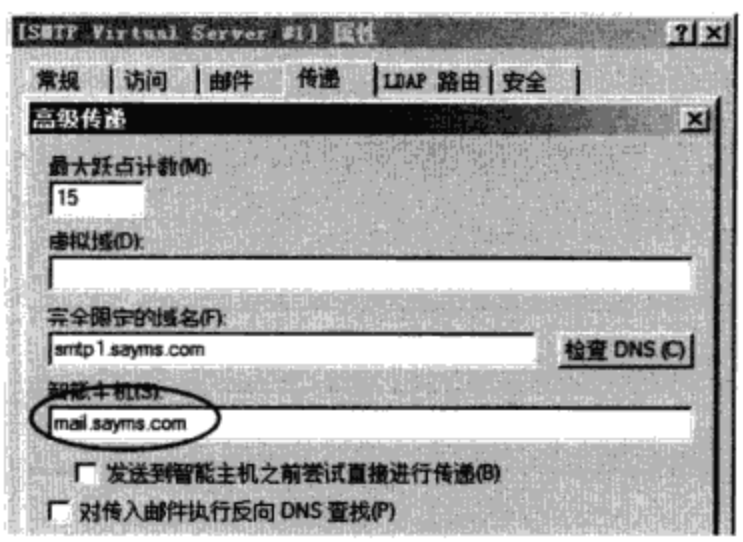


图 8-31

如果您选择图中的**发送到智能主机之前尝试直接进行传递**的话，则SMTP虚拟服务器会先通过DNS服务器来查找远程SMTP服务器的IP地址，以便直接将邮件发送给它；若失败，再改通过智能主机来发送。

提示

若您有另外新建远程域的话（后述），则您可以针对这个域来单独设置不同的智能主机，该域的智能主机设置优先于本处的设置。

8-5-6 反向DNS查询设置

当客户端计算机发送邮件给您的SMTP虚拟服务器时，客户端计算机会通过HELO/EHLO命令来与SMTP虚拟服务器通信，这个命令内包含着客户端计算机的FQDN。您可以让SMTP虚拟服务器来检查客户端计算机的IP地址是否与这个FQDN相符合，也就是该IP地址是否为这台计算机所拥有，此功能可用来检查邮件是否为垃圾邮件。

启用此功能的方法为选择前图 8-31下方的**对传入邮件执行反向DNS查找**，它会通过DNS服务器的反向对应区域来查询，如果检查出此FQDN并不是此IP地址所拥有的话，则它会在邮件中**Received**这一行的IP地址后加上**unverified**的字样，如图 8-32所示。

图 8-32

如果反向查询失败的话，它会加上**RDNS failed**的字样，如图 8-33所示。

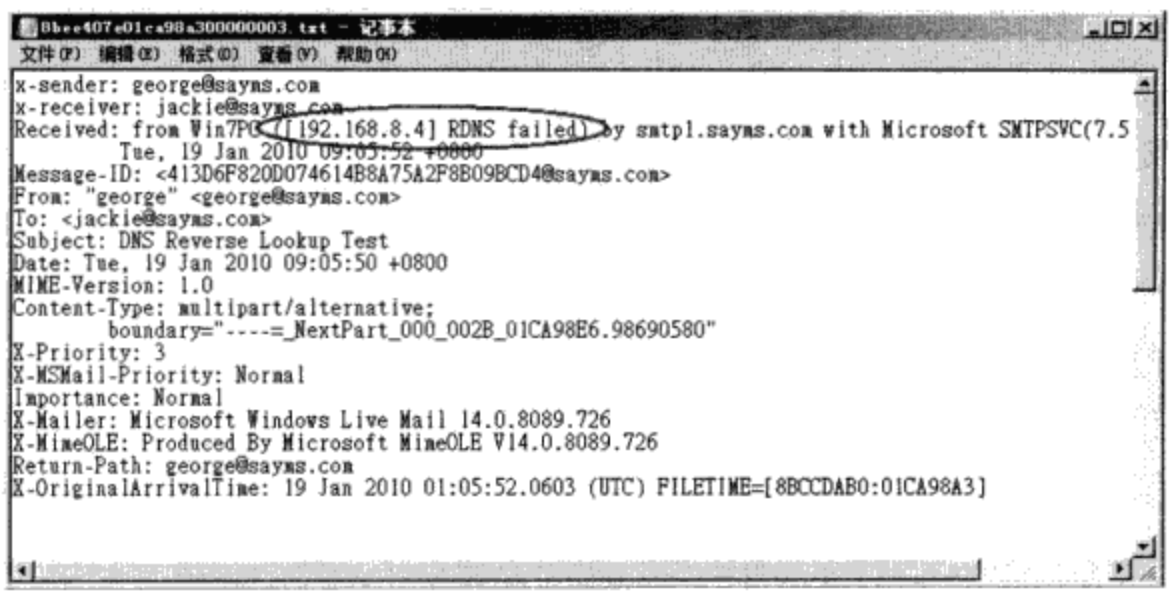


图 8-33

提示

启用**对传入邮件执行反向DNS查找**的话，会影响SMTP虚拟服务器的运行效率，请自行斟酌是否要启用此功能。

8-6 邮件的管理

本节将介绍如何来设置连接限制、邮件大小限制、收件人数限制与如何处理无法传递的邮件等，这些设置可通过【对着**SMTP Virtual Server #1**单击右键➲**属性**➲**邮件**标签】的方法，如图 8-34所示。

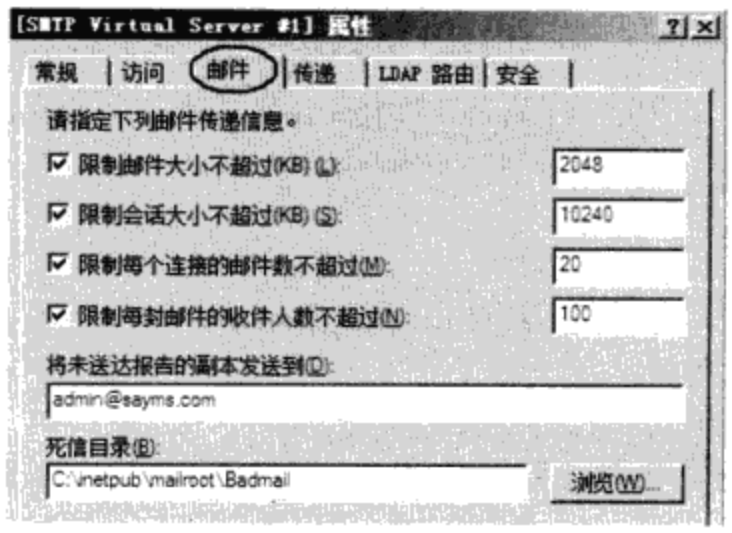


图 8-34

- **限制邮件大小不超过、限制会话大小不超过**：这两个设置可用来避免用户发送大型邮件。
  - **限制邮件大小不超过**：发件人所发来的邮件大小如果超过此处的限制值，邮件将被拒收。
  - **限制会话大小不超过**：用来限制发件人在一个连接中，所有发送邮件的总容量，此处的设置值应该要大于或等于**限制邮件大小不超过**的设置值。某些发件人的邮件软件为了避开邮件大小的限制，会将一封大型邮件拆成数个较小的邮件，然后通过同一个连接来发送。如果在一个连接中所有邮件的总容量超过在**限制会话大小不超过**的设置，则SMTP虚拟服务器会将此连接中断。

    这两个限制不仅对连接到SMTP虚拟服务器的用户有效，也对连接到SMTP虚拟服务器的远程SMTP服务器有效，而这些远程SMTP服务器经常是通过一个连接来同时发送许多封邮件，所以很可能总容量会超过**限制会话大小不超过**的限制，因此在设置时必须非常谨慎，因为这些远程SMTP服务器在超过限制而被中断连接后，会自动重新连接来重送这些邮件，这个步骤可能会持续一段时间，一直到发送成功或超过它自己的重试次数为止，因此可能会影响到您的SMTP虚拟服务器的效率。

提示

有些远程SMTP服务器支持进阶的EHLO命令，当它们要连接您的SMTP虚拟服务器时，会先侦测邮件大小限制，若要传递的邮件大小超过限制的话，就会将邮件退回给用户，并附上NDR。

- **限制每个连接的邮件数不超过**：这个设置也会影响到SMTP虚拟服务器的运行效率，默认值为20。例如当SMTP虚拟服务器要发送100封邮件给远程域时，它会每20封邮件通过一个单一连接来发送，因此总共同时会有5个连接，这种作法会比利用单一连接发送100封邮件有效率。
- **限制每封邮件的收件人数不超过**：用来限制在单一连接中，同一封邮件最多可以发送给多少位收件者。图中默认值为100人，这也是RFC 2821中规定的最小值。当SMTP虚拟服务器要发送一封收件者超过100人的邮件时，它会为第100位以后的收件者另外新

建一个连接。

> 提示
>
> 有些SMTP服务器收到由远程SMTP服务器传来超过限制的错误信息时，会直接发送NDR给发件人，并不会自动创建另一个新连接来将邮件发送给其余的收件者。

- **将未送达报告的副本发送到**：如果邮件无法传递，SMTP虚拟服务器会将邮件退还给发件人并附上**未送达报告**(NDR)。您也可以设置将NDR副本发送一份给一个指定电子邮件信箱，例如图8-33中的admin@sayms.com。
- **死信目录**：错误的邮件（例如格式不符）会被转移到**Badmail**文件夹。如果NDR无法被发送出去的话，它也会被转移到**Badmail**文件夹。此文件夹默认是位于%*systemdrive*%\inetpub\mailroot\Badmail路径，而您可以通过图 8-33中的**死信目录**来更改路径。

8-7 SMTP域的管理

我们在章节8-4内已经介绍过SMTP域，本节将做进一步的设置。在图 8-35中已经有一个本地默认域，域名就是此SMTP服务器的**计算机全名**SMTP1.sayms.com，也就是FQDN。您可以通过【对着此域单击右键➲重新命名】的途径来更改此名称。

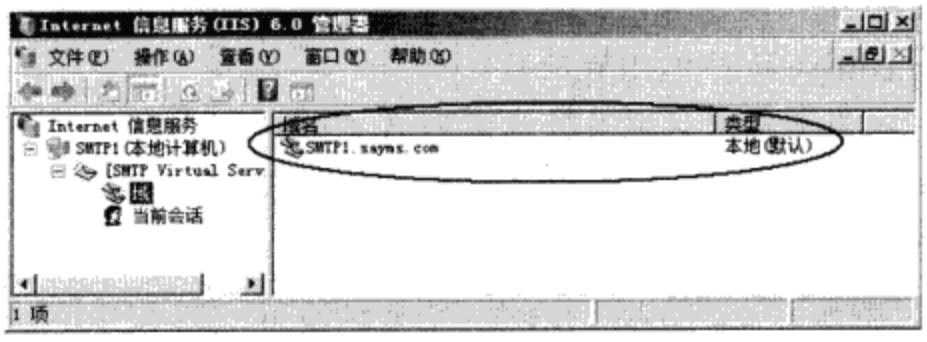


图 8-35

当SMTP虚拟服务器收到属于本地域的邮件时，会将它们保存到%*systemdrive*%\inetpub\mailroot\Drop文件夹内，如果您要更改此文件夹路径的话，请【对着本地域单击右键➲属性➲通过图 8-36中的**投递目录**来更改】。

图 8-36

图中若选择**启用投递目录配额**的话，系统会将此文件夹的容量限制为前面图 8-33中**限制邮件大小不超过**的设置值的10倍。

8-7-1 新建SMTP域

若要新建域的话，请如图 8-37所示【对着**域**右键单击➲新建➲域➲选择**远程**或**别名**域】:

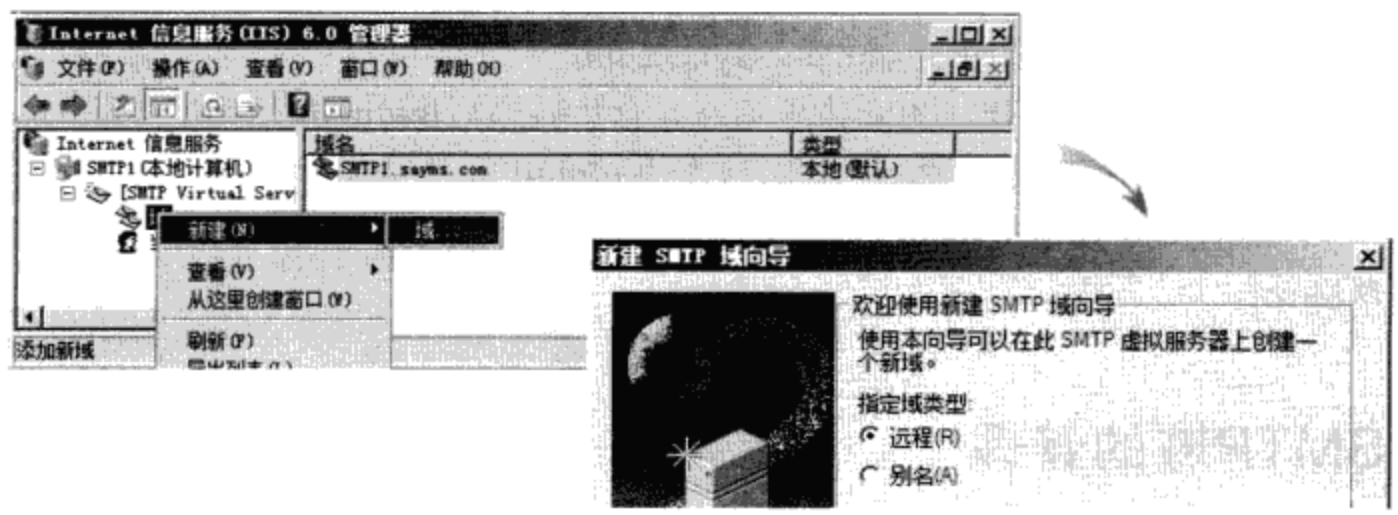


图 8-37

- **远程域**：不是由您的SMTP虚拟服务器所管辖的域就称为远程域。SMTP虚拟服务器在转发邮件给远程域时，它与所有远程域的互动方法默认是相同的，但如果您在此处新建了特定的远程域，则您可以让这个远程域有着不同的设置值。假设我们新建了一个远程域sayexg.com（如图 8-38所示）。
- **别名域**：您可以为本地默认域另外设置别名（alias），所有要发送到本地别名域的邮件就等于要发送给本地默认域。假设我们替本地默认域新建了一个别名域sayms.com（如图 8-38所示）。

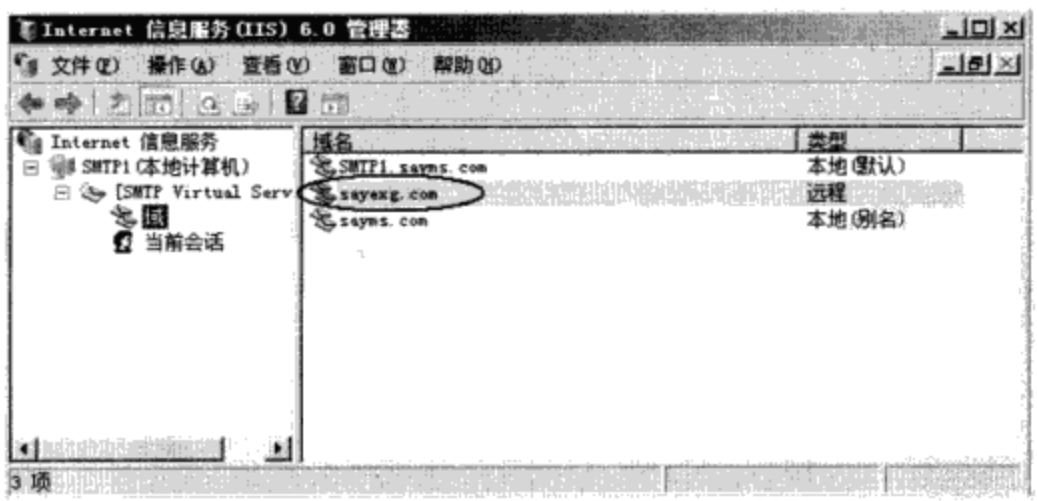


图 8-38

远程域新建完成后，可能还需要针对远程域做更进一步的设置：【双击图 8-38中的远程域sayexg.com➲通过图 8-39来设置】:

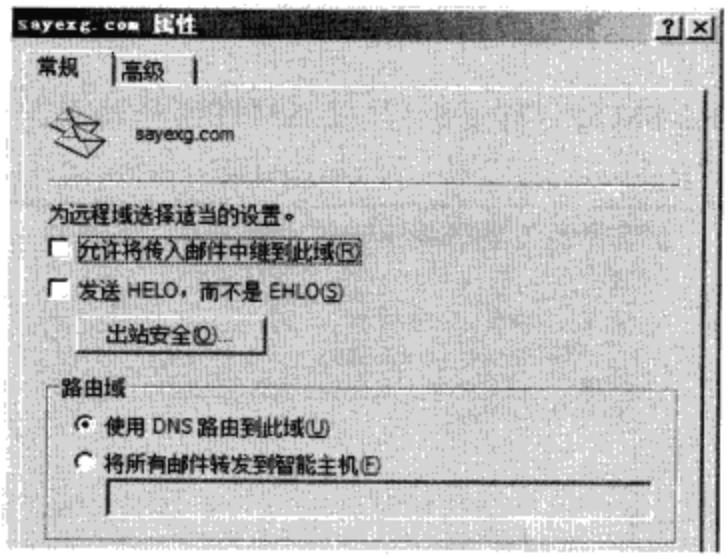


图 8-39

- **允许将传入邮件中继到此域**：选择此选项表示会将邮件中继此域，否则会封锁此域的邮件。
- **发送HELO，而不是EHLO**：若远程SMTP服务器并不支持SMTP高级规格ESMTP的话，则请选择此选项，以便利用HELO来与这台远程SMTP服务器通信。
  - **出站安全**：通过出站安全可以设置与远程SMTP服务器通信所用的验证方法，这些验证方法我们在前面都已经介绍过。
- 路由域
  - **使用DNS路由到此域**：表示SMTP虚拟服务器将自行通过DNS服务器（MX记录）来查找远程域（sayexg.com）的SMTP服务器。
  - **将所有邮件转发到智能主机**：表示SMTP虚拟服务器会将要送到远程域sayexg.com的邮件直接转发到智能主机来发送。请输入智能主机的FQDN或IP地址，若输入IP地址的话，需在IP地址前后加方括号，例如[192.168.8.83]。

8-7-2 为远程域启用ATRN功能

单击图 8-40中的**高级**标签后，可以选择**排列邮件以便进行远程触发传递**（Queue message for remoting trigged delivery），表示当SMTP虚拟服务器收到要发送到远程域sayexg.com的邮件后，会将这些邮件送到队列（queue）等待，而不会主动将它们发送到远程SMTP服务器。等到远程域的SMTP服务器自行利用ATRN（Authenticated TURN）命令提出索取邮件的要求后，再将邮件传给此SMTP服务器。这个功能特别适合于需要定期来下载邮件的远程域。

远程域的SMTP服务器利用ATRN命令来索取邮件时，必须提供有效的用户名与密码，这个用户必须是**授权使用ATRN的账户**列表中的用户，因此请将要供远程域来使用的用户账户加入到列表内：【单击图中的添加➲选择本地或Active Directory域内的用户账户】。

提示

Windows Server 2008 R2 SMTP只接受远程域的SMTP服务器发送出ATRN命令给您的SMTP虚拟服务器，不支持您的SMTP虚拟服务器送出ATRN命令给远程域的SMTP服务器。

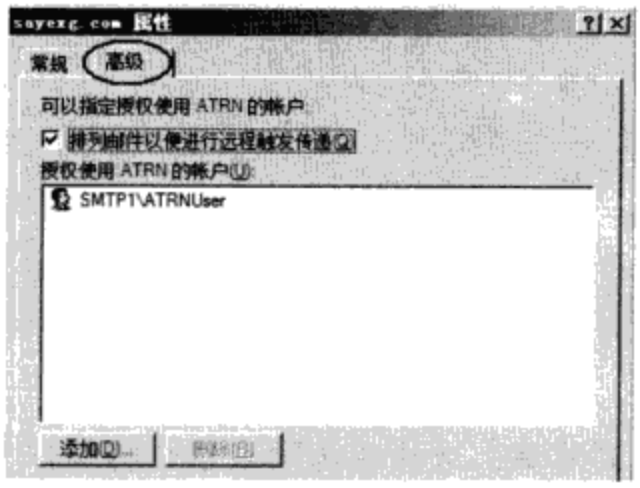


图 8-40

8-8 SMTP Relay的设置

通过SMTP Relay（中转站）来寄送邮件，可以避免内部电子邮件服务器直接与外部网络通信、减少内部电子邮件服务器被攻击的机会。我们将利用图 8-41来说明如何设置SMTP Relay，图中SMTP Relay为Windows Server 2008 R2计算机，而内部电子邮件服务器假设是Exchange Server 2003或Exchange Server 2007，其所管辖的域名为sayexg.com。

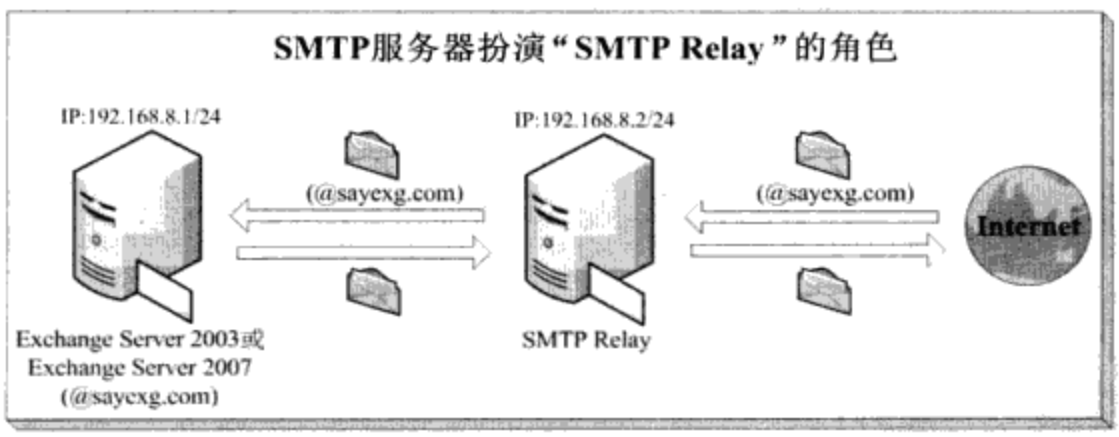


图 8-41

提示

在Exchange Server 2007环境内可以使用**边缘传输服务器**（Edge Transport Server）来扮演SMTP Relay的角色。

8-8-1 传入SMTP Relay的设置

图 8-41中Exchange Server所管辖的域名为sayexg.com，若邮件收件者的域名也是

sayexg.com的话，例如george@sayexg.com，则这封邮件就是**传入邮件**，SMTP Relay会将所收到的**传入邮件**转送给Exchange Server。

SMTP Relay的设置

SMTP Relay并不需要验证用户名称与密码就可以接受**传入邮件**，也就是远程SMTP服务器只需利用匿名方式，就可以发送**传入邮件**给SMTP Relay。

STEP 1 请选择【开始➲管理工具➲Internet 信息服务 (IIS) 6.0管理器➲展开本地计算机➲对着 **SMTP Virtual Server #1**单击右键➲属性➲选择图 8-42中**访问**标签下的身份验证➲确认**匿名访问**已经选择】。

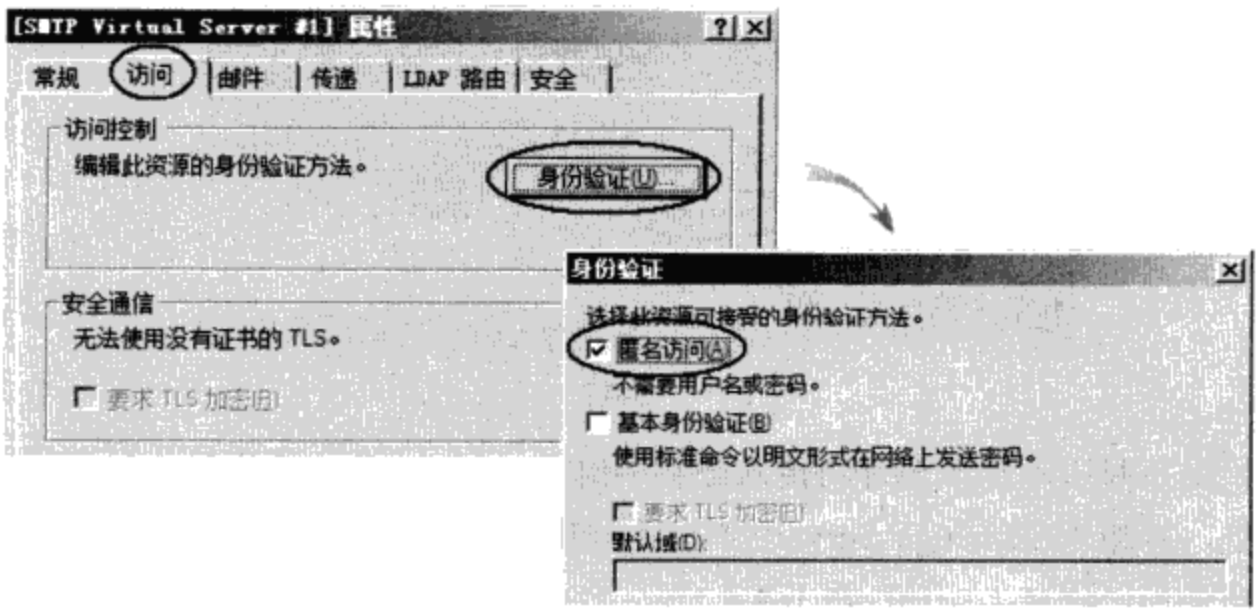


图 8-42

STEP 2 如图 8-43所示【对着**域**单击右键➲新建➲域】。

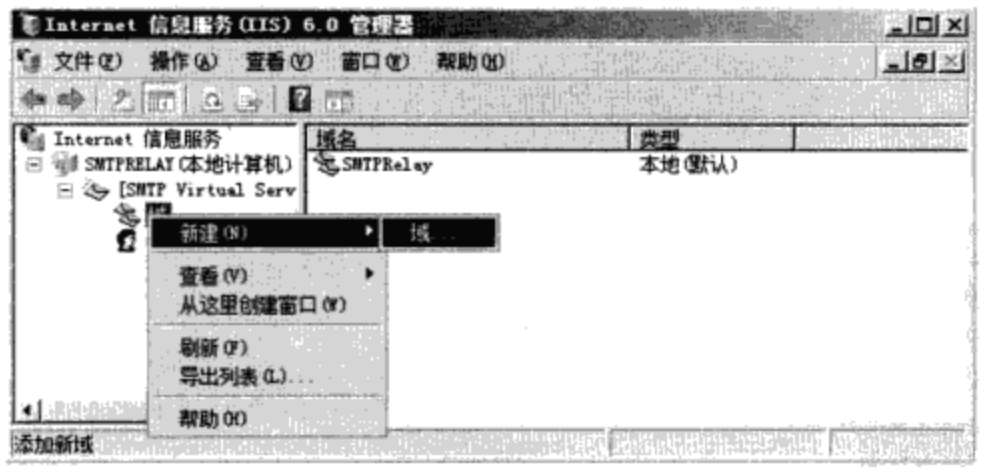


图 8-43

STEP 3 在图 8-44中选择**远程**后单击下一步、输入域名sayexg.com后单击完成。

图 8-44

STEP 4 双击图 8-45中刚才所新建的远程域sayexg.com。

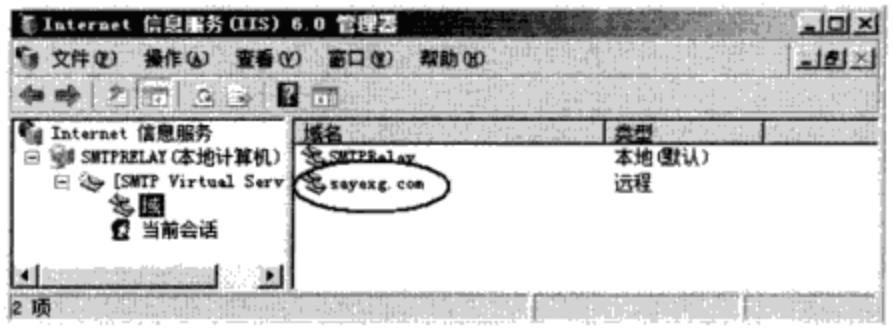


图 8-45

STEP 5 如图 8-46所示选择**允许将传入邮件中继到此域**，然后选择**将所有邮件转发到智能主机**，并输入Exchange Server的FQDN或IP地址，图中我们输入IP地址，但IP地址前后需加方括号，例如[192.168.8.1]。

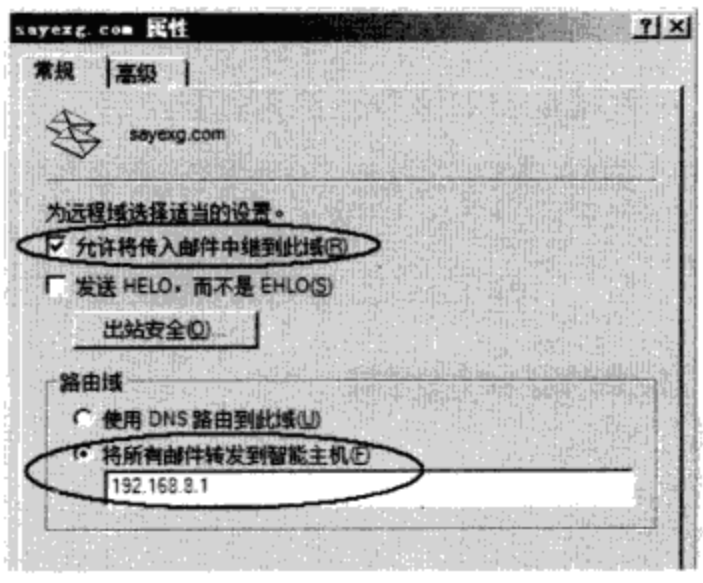


图 8-46

Exchange Server的设置

SMTP Relay默认是利用匿名方式将传入邮件转送给Exchange Server，而 Exchange Server 2003默认也不需要验证传入邮件的发件人的用户名与密码(匿名访问)，因此在Exchange Server 2003不需要额外的设置。

若SMTP Relay是将传入邮件发送给扮演**边缘传输服务器**角色（Edge Transport Server role）的Exchange Server 2007，此时因为**边缘传输服务器**默认已经启用匿名访问，故也不需要额外的设置。

若SMTP Relay是将传入邮件发送给扮演**集线传输服务器**角色（Hub Transport Server role）的Exchange Server 2007的话，就必须另外启用匿名访问（默认为禁用）：到**集线传输服务器**上选择【开始➲所有程序➲Microsoft Exchange Server 2007➲Exchange管理控制台➲如图 8-47展开**服务器配置➲集线器传输**➲对着图中Default的接收连接器（Receive Connector）单击右键➲属性➲如前图所示选择**权限组**标签下的**匿名用户**】。

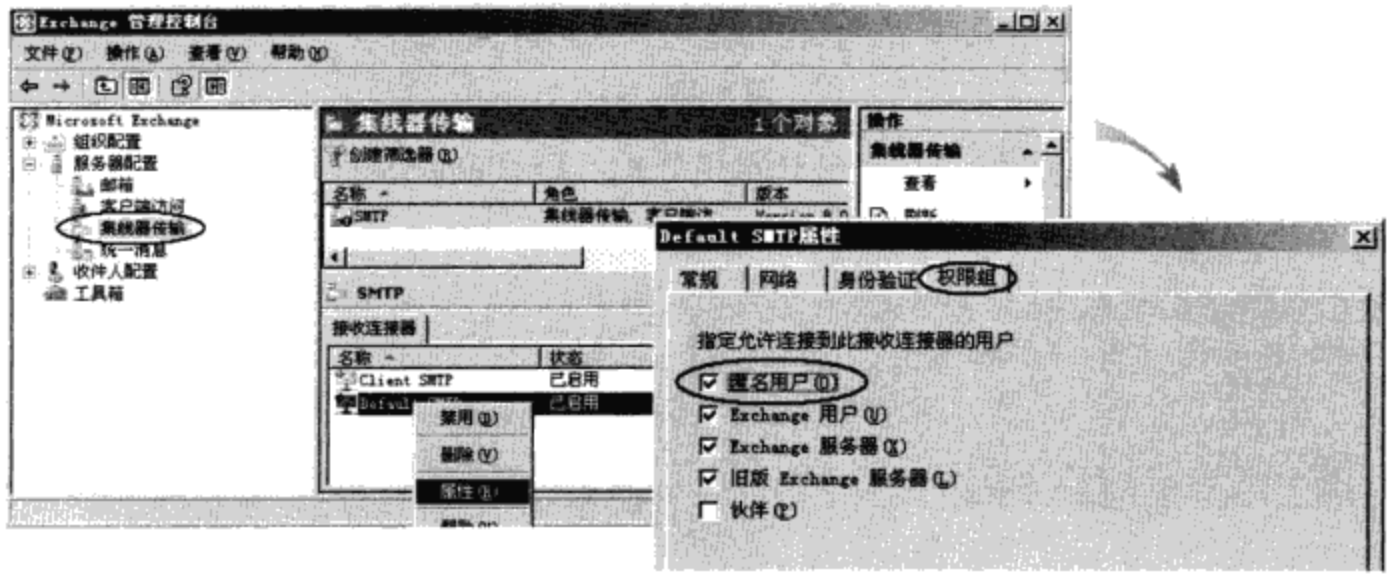


图 8-47

8-8-2 外寄SMTP Relay的设置

当SMTP Relay接收到待发邮件（不是@sayexg.com的邮件）时，它是否应该将此邮件寄送出去呢？

- 如果是从Exchange Server所转来的待发邮件，则应该将邮件寄送出去。
- 如果是从外部SMTP服务器所转来的待发邮件，则应该拒绝转送此邮件，否则SMTP Relay有可能成为替别人发送**垃圾邮件**（spam）的中转站。

SMTP Relay的设置

我们需要在SMTP Relay这台服务器上设置让它接受从Exchange Server所转来的待发邮件，并将此邮件发送出去。设置方法如下：

STEP 1 请【对着 **SMTP Virtual Server #1**单击右键➲属性➲选择图 8-48中**访问**标签下的中继】。

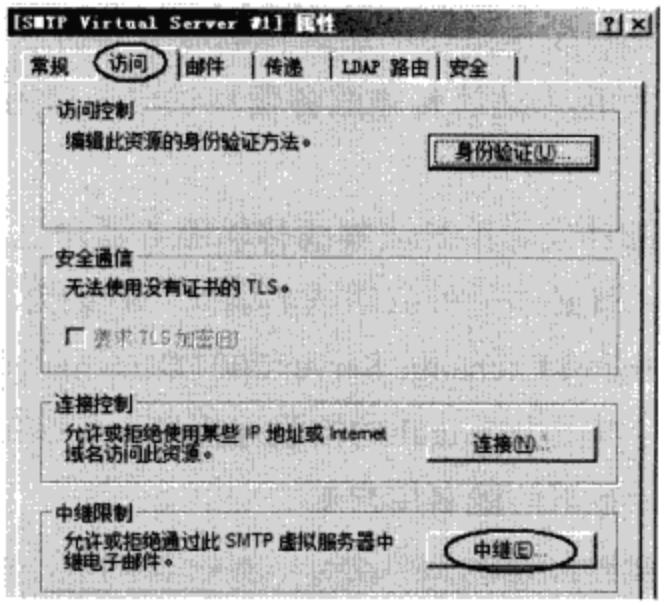


图 8-48

STEP 2 在图 8-49中单击添加、在**一台计算机**处输入Exchange Server的IP地址192.168.8.1后单击确定。

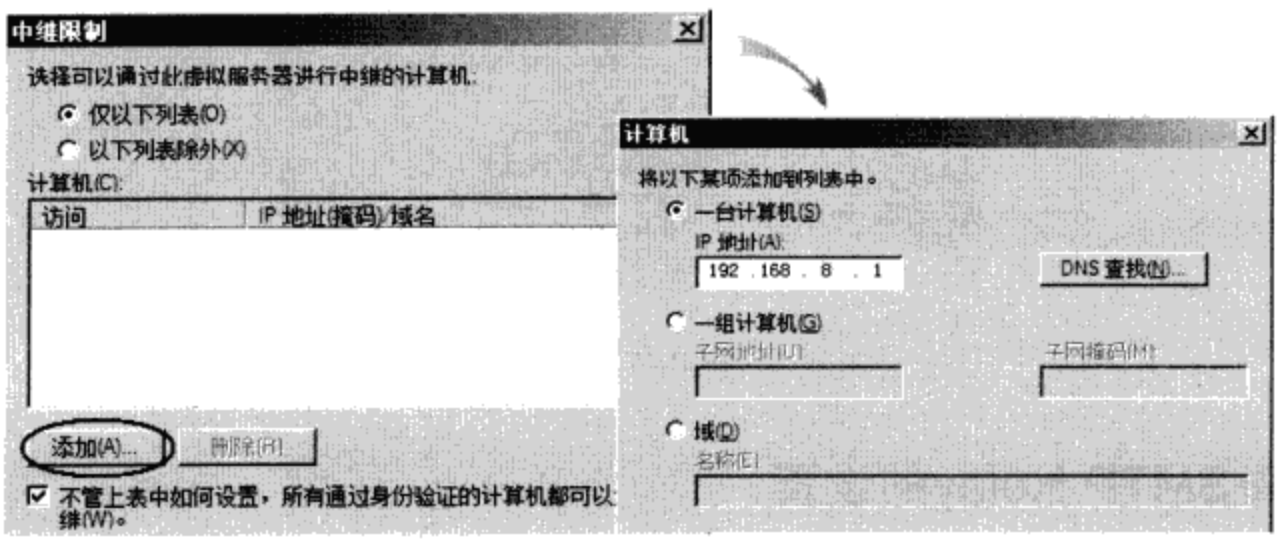


图 8-49

STEP 3 图 8-50为完成后的界面，它表示SMTP Relay已经可以接受由IP地址是192.168.8.1的Exchange Server所发来的待发邮件。

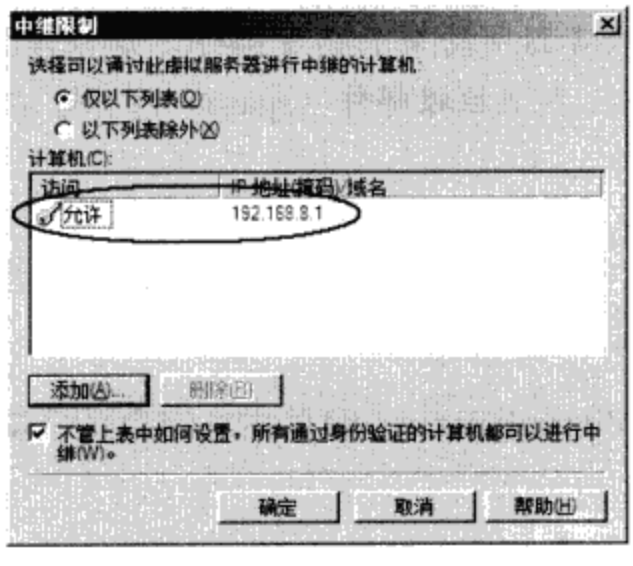


图 8-50

不是列于图 8-50列表中的服务器所传来的待发邮件会被拒绝，若选择图中的**不管上表中如何设置，所有通过身份验证的计算机都可以进行中继**，只要这些服务器能够提供有效用户名与密码，则SMTP Relay仍然会接受它们所发来的待发邮件，不过SMTP Relay的验证方法需增加**基本身份验证**或 **集成Windows身份验证**。

注意

请不要如图 8-51所示来选择，否则SMTP Relay会变成**Open Relay**（开放式中转站），它会接受与转发所有待发邮件，如此它有可能成为为别人发送**垃圾邮件**的中转站。有一些业者会提供Open Relay名单，拥有此名单的公司，可能会拒绝接收此名单内的服务器所送来的邮件。

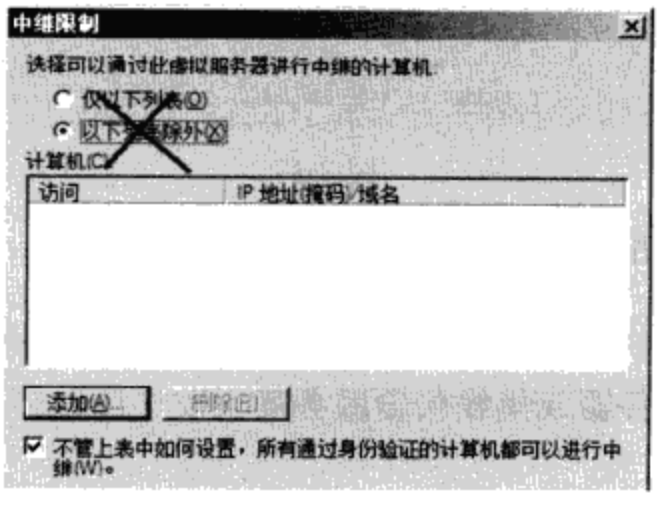


图 8-51

Exchange Server 2003的设置

您需要在Exchange Server 2003上设置将所有待发邮件转发给SMTP Relay来寄送，其设置方法为：

STEP 1 选择【开始➲所有程序➲Microsoft Exchange➲系统管理器➲如图 8-52所示展开到SMTP协议的**默认SMTP虚拟服务器处**➲单击上方的**属性**图标】。

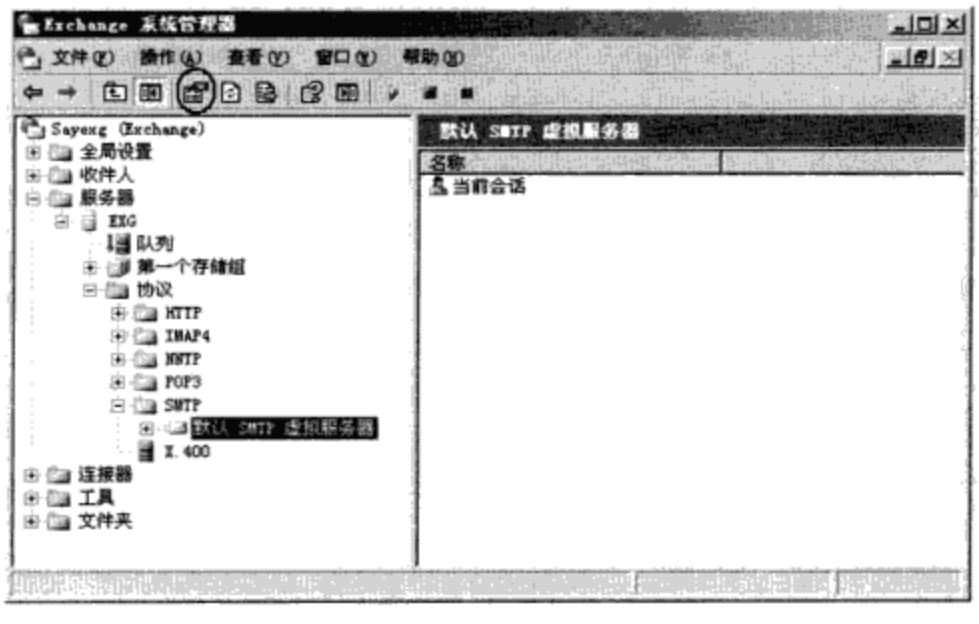


图 8-52

STEP 2 单击图 8-53中**传递**标签下的高级、在前图中的**智能主机**处输入SMTP Relay的FQDN或IP地址，图中我们输入IP地址，例如[192.168.8.2]。

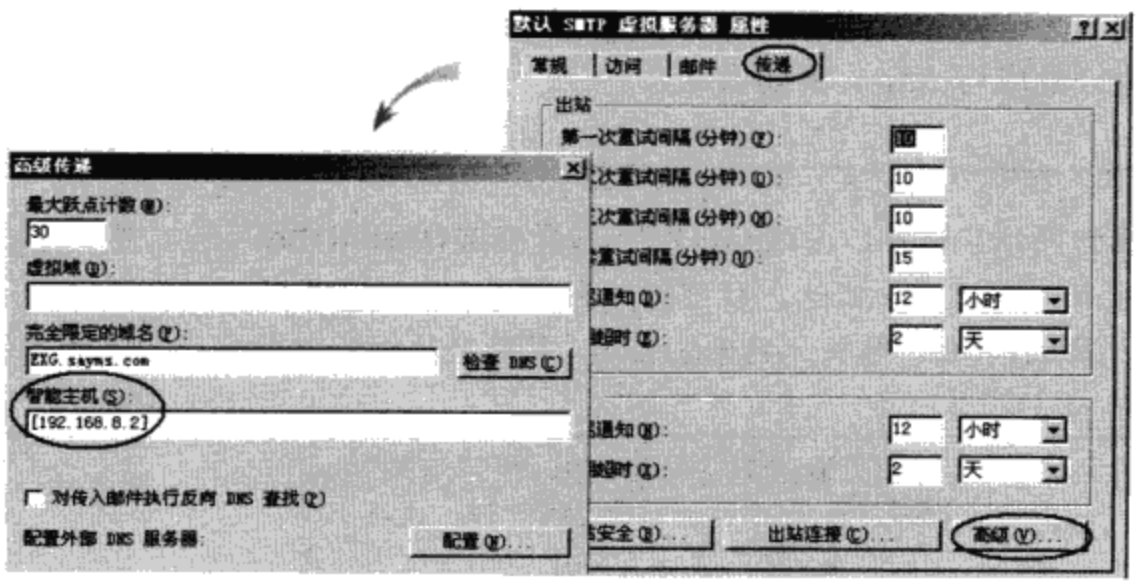


图 8-53

Exchange Server 2007的设置

您需要在Exchange Server 2007上设置将所有待发邮件转给SMTP Relay来寄送，此时需视企业内部是利用**边缘传输服务器**或**集线传输服务器**来发送待发邮件而有不同的设置。

边缘传输服务器

请到扮演**边缘传输服务器**角色的Exchange Server 2007上更改负责外送的**发送连接器**(Send Connector)：【如图 8-54所示单击**发送连接器**标签下的发送连接器（假设其名称为**连接外部网络**）➲属性➲单击**网络**标签➲将图中的智能主机设置到SMTP Relay（192.168.8.2）、同时确认智能主机的验证方式为**无**】，您可以通过图中的添加、编辑与更改来设置。

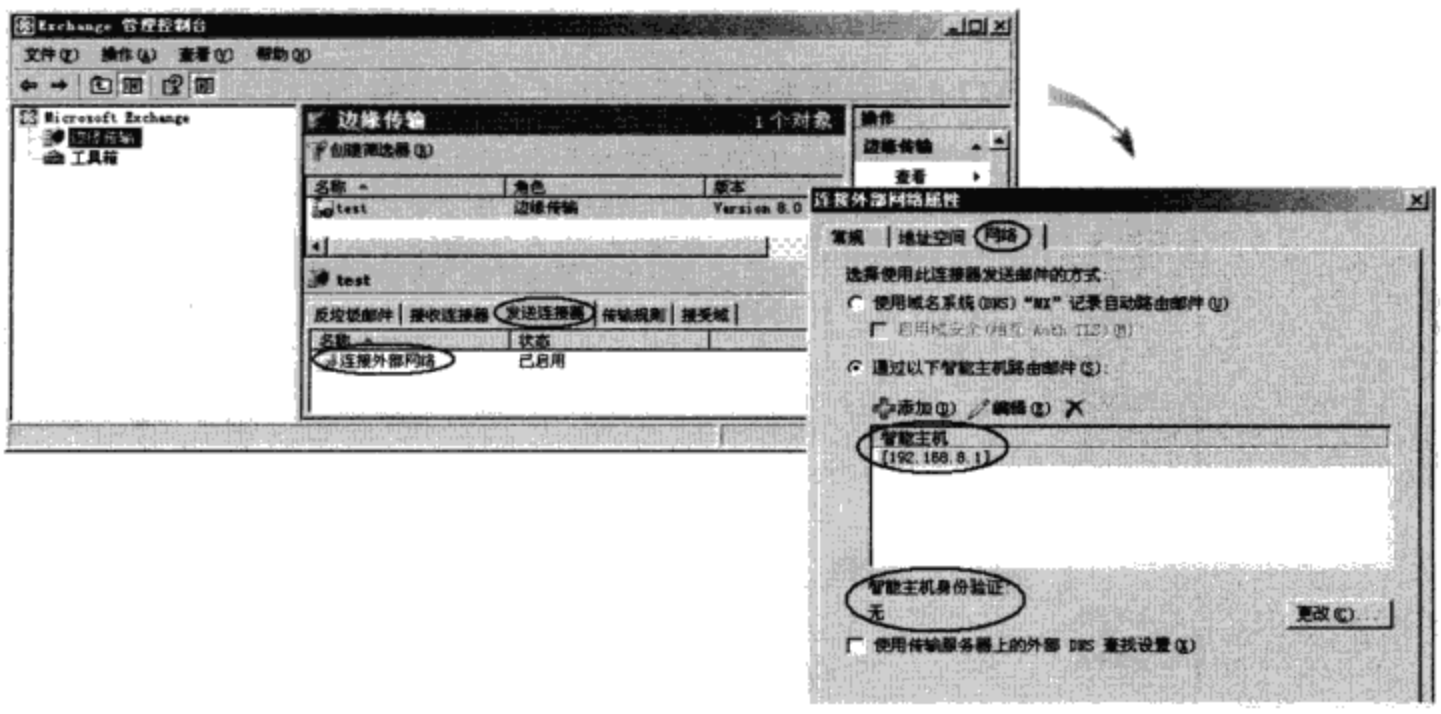


图 8-54

集线传输服务器

请到扮演**集线传输服务器**角色的Exchange Server 2007上更改负责外送的**发送连接器**：【如图 8-55所示单击**发送连接器**标签下的传出连接器（图中假设其名称为**连接到外部网络**）➲属性➲单击**网络**标签➲将图中的智能主机设置到SMTP Relay（192.168.8.2）、同时确认智能主机的验证方式为**无**】，您可以通过图中的添加、编辑与更改来设置。

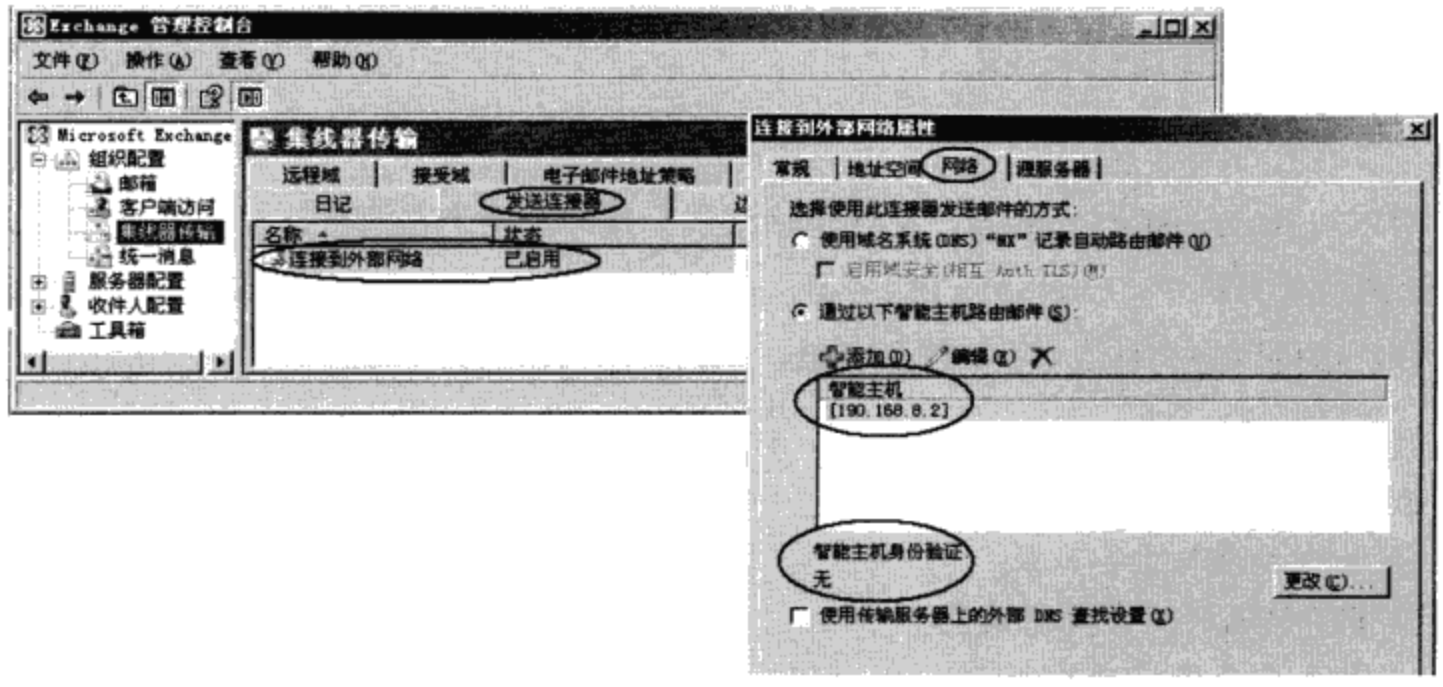


图 8-55