SIEMENS

常问问题 8 月/2014 年

如何用 Windows Server 2008 配置 Radius Server 进行 802.1X 认证

Radius Server

http://support.automation.siemens.com/CN/view/zh/99858152

目录

1 简介

1.1 802.1X 介绍

IEEE 802.1X 是 IEEE 制定关于用户接入网络的认证标准，全称是“基于端口的网络接入控制”，属于 IEEE 802.1 网络协议组的一部分。于 2001 年标准化，之后为了配合无线网络的接入进行修订改版，于 2004 年完成。它为想要连接到 LAN 或 WLAN 的设备提供了一种认证机制。

802.1X 验证涉及到三个部分：申请者、验证者和验证服务器。申请者是一个需要连接到 LAN/WAN 的客户端设备，同时也可以指运行在客户端上，提供凭据给验证者的软件。验证者是一个网络设备，如以太网交换机或无线接入点。验证服务器通常是一个运行着支持 Radius 和 EAP 协议的主机。 验证者就像是一个受保护网络的警卫。申请者（如客户端设备）不允许通过验证者访问到受保护一侧的网络，直到申请者的身份被验证和授权。这就像是允许进入一个国家之前要在机场的入境处提供一个有效的签证一样。使用 802.1X 基于端口的验证，申请者向验证者提供凭据，如用户名/密码或者数字证书，验证者将凭据转发给验证服务器来进行验证。如果验证服务器认为凭据有效，则申请者（客户端设备）就被允许访问被保护侧网络的资源。

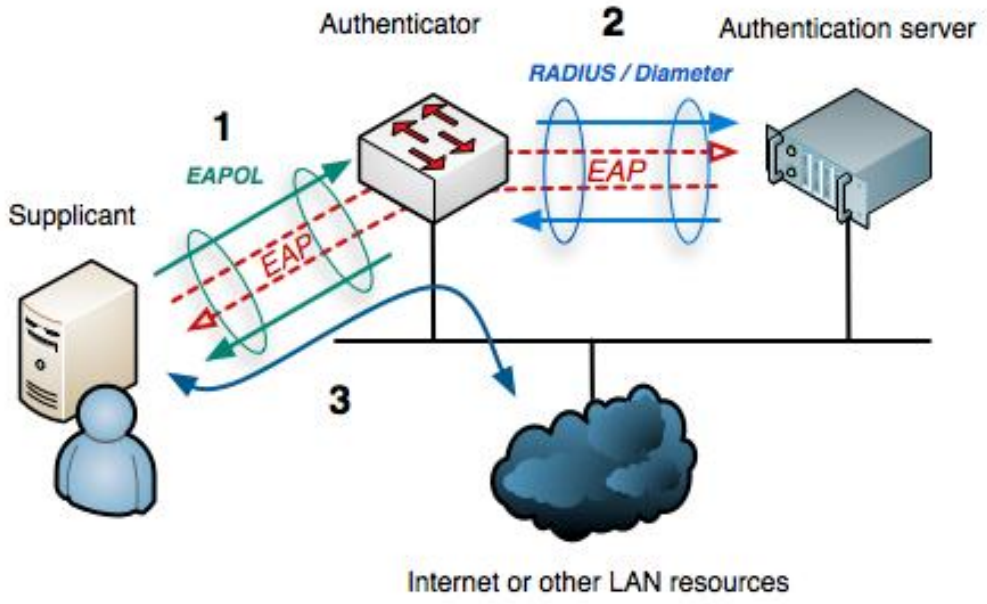

图 1-1 802.1X 的验证结构

EAP 数据首先被封装在 EAPOL 帧中，传输于申请者（Supplicant）和验证者（Authenticator）之间。随后又封装在 RADIUS 或 Diameter，传输于验证者和验证服务器（Authentication server）之间。

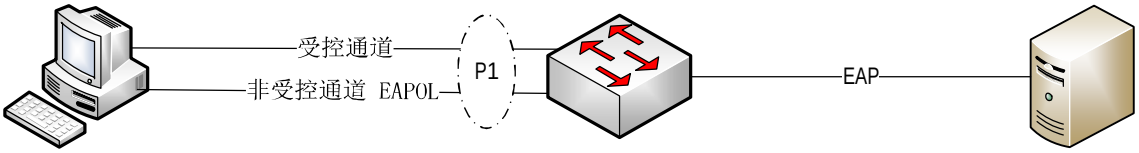

图 1-2 受控与非受控通道

802.1X 在验证者（Authenticator）端口（通常为连接申请者 PC 的交换机端口，如图 1-2 中 P1 端口）定义了两个逻辑端口实体，受控通道和非受控通道。受控通道是受 802.1X 端口访问保护的，进出受控通道的流量被 802.1X 端口访问实体允许或拒绝。非受控通道用于传输 EAPOL 报文，任何时候都是打开的。

验证过程：

1. 初始化：当交换机（验证者）检测到一个新的申请者时，交换机连接申请者的端口使能，设置为“未授权”状态。在该状态下，只有 802.1X 报文允许通过，其他报文被丢弃。
2. 启动：交换机（验证者）周期性的发送 EAP 请求身份报文到本地网段的特殊 2 层地址。申请者侦听该地址，当接收到 EAP 请求身份报文时，发送 EAP 响应身份报文，该报文包含申请者的身份信息，如用户 ID。交换机（验证者）将 EAP 响应身份报文包装成 Radius 访问请求报文，转发给验证服务器。
3. 协商：验证服务器发送响应（EAP 访问挑战报文）报文给交换机（验证者），该报文同时包含了希望申请者提供的 EAP 验证方法。交换机（验证者）将报文包装成为 EAPOL 报文后传输给申请者。
4. 验证：如果验证服务器和申请者都支持同样的 EAP 验证方式，EAP 请求和响应报文在申请者和验证服务器之间传输（由交换机负责翻译），如果验证成功，验证服务器响应 EAP 成功消息。然后交换机（验证者）将端口状态设置为“已授权”。当申请者退出时，发送 EAPOL-logoff 消息给验证服务器，交换机将端口重新设置为“未授权”状态，堵塞所有 non-EAP 报文。

1.2 EAP 认证方式

本节介绍 EAP 认证的几种常用方式：EAP_MD5，PEAP，EAP_TLS。

1.2.1 EAP_MD5 认证方式

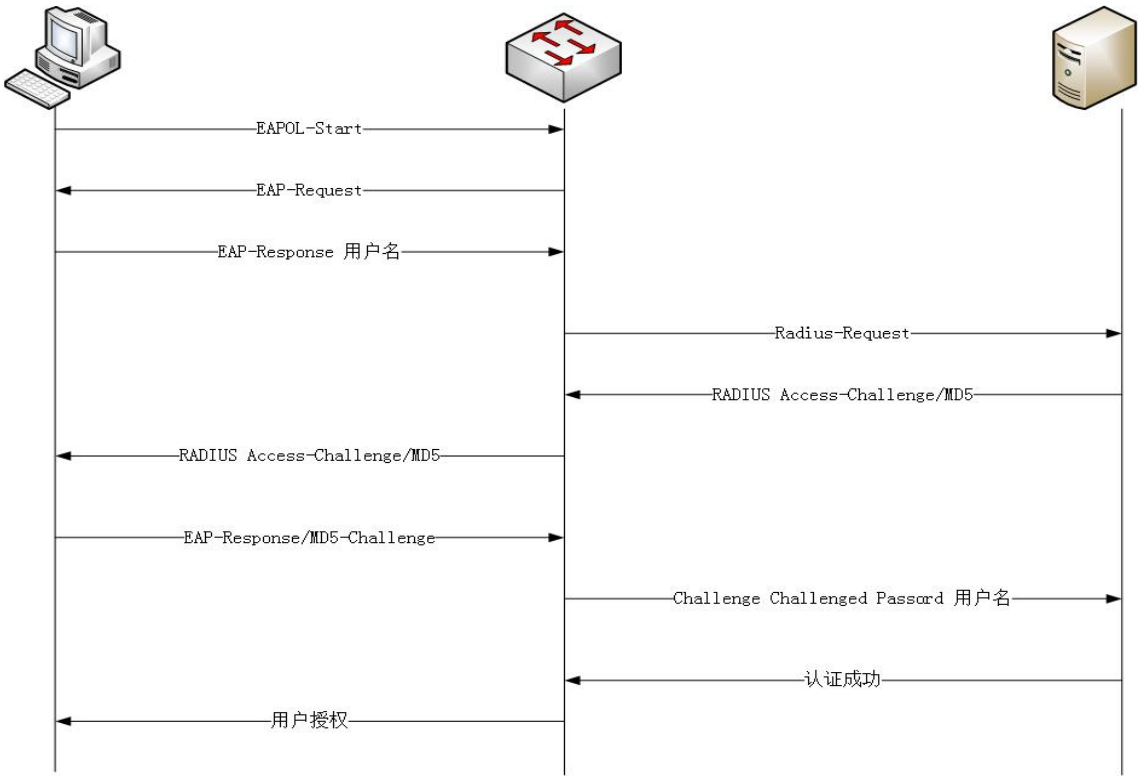

图 1-3 EAP_MD5 验证方式

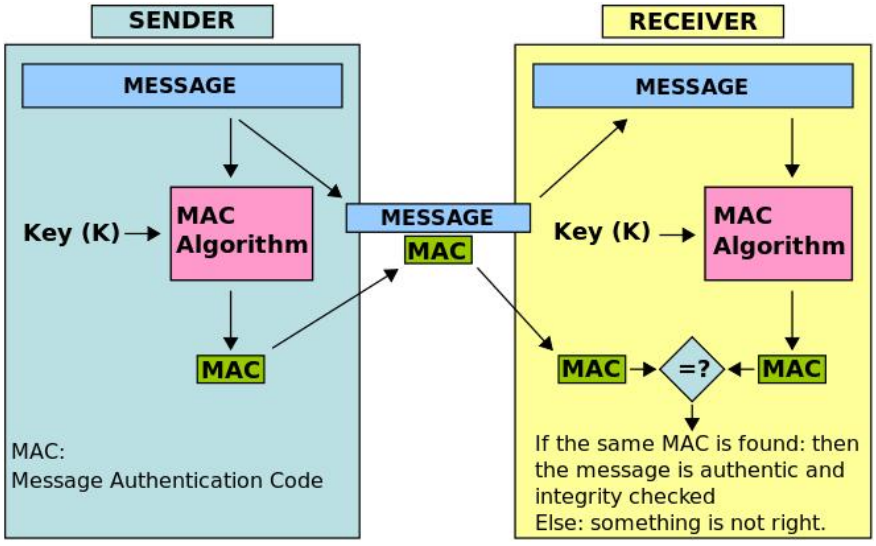

图 1-4 MD5 验证过程

EAP_MD5 验证方式是最简单，也是安全性最差的方式。

1. 申请者发送认证请求后，验证者（交换机）要求申请者提供用户身份。
2. 申请者将用户名提供给交换机后，交换机将包装后的用户名发送给 Radius Server。

3. Radius Server 收到申请者的用户名后，发出 Access-Challenge/MD5 请求报文，并附加一段随机字符串。
4. 申请者将用户名和密码和 Radius Server 发送的随机字符串进行 MD5 运算，得到的 MD5 运算结果发送给 Radius Server。
5. Radius Server 同样将用户名，密码，和随机字符串进行 MD5 运算，得到的结果与申请者的响应报文进行比较，如果相同，发送验证成功报文给交换机。
6. 交换机打开连接申请者的受控端口。

使用以上方式，用户名在网络传输，密码始终没有出现在网络上，只有密码，用户名，和随机字符串的 MD5 运算结果暴露在网络上，同时由于 MD5 运算的不可逆性，因此理论上避免了被网络攻击者窃取密码。但是由于 MD5 算法本身容易被破解，如果攻击者获取大量报文还是有可能破译出密码的。

1.2.2 PEAP 认证方式

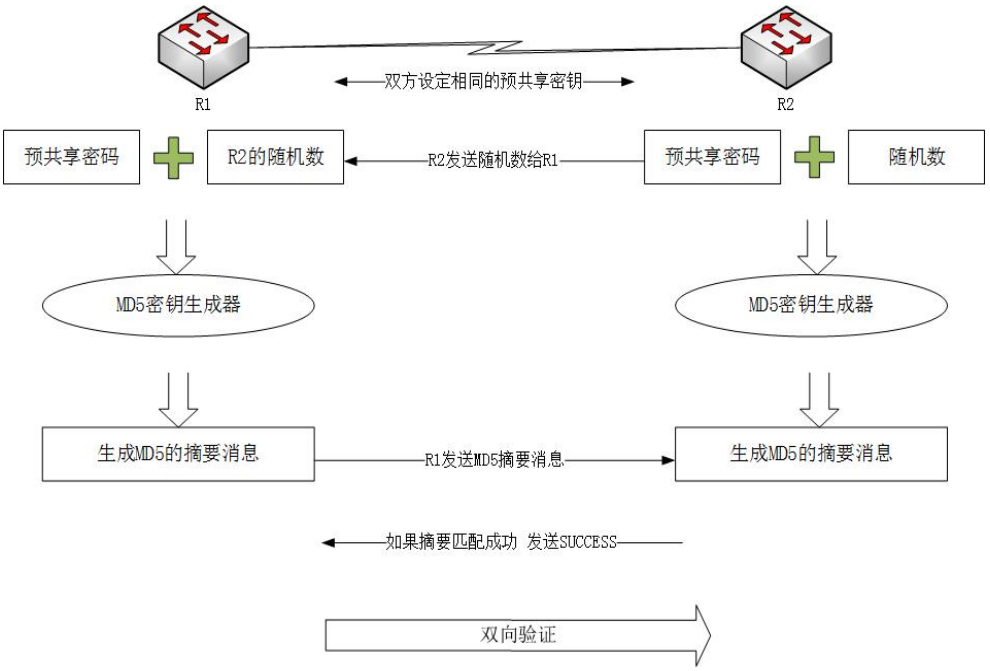

图 1-5 MSCHAP V2

PEAP 认证方式使用证书加密 MSCHAP V2 认证通道。下面首先介绍 MSCHAP V2 认证。MSCHAP V2 认证方式与前面的 EAP_MD5 类似。申请者与认证服务器使用相同的预共享密码和随机数进行 MD5 运算，计算出 MD5 摘要消息。然后申请者将计算出的摘要消息传输给认证服务器，认证服务器比较 MD5 摘要消息与自己计算的相同，发出认证成功消息。

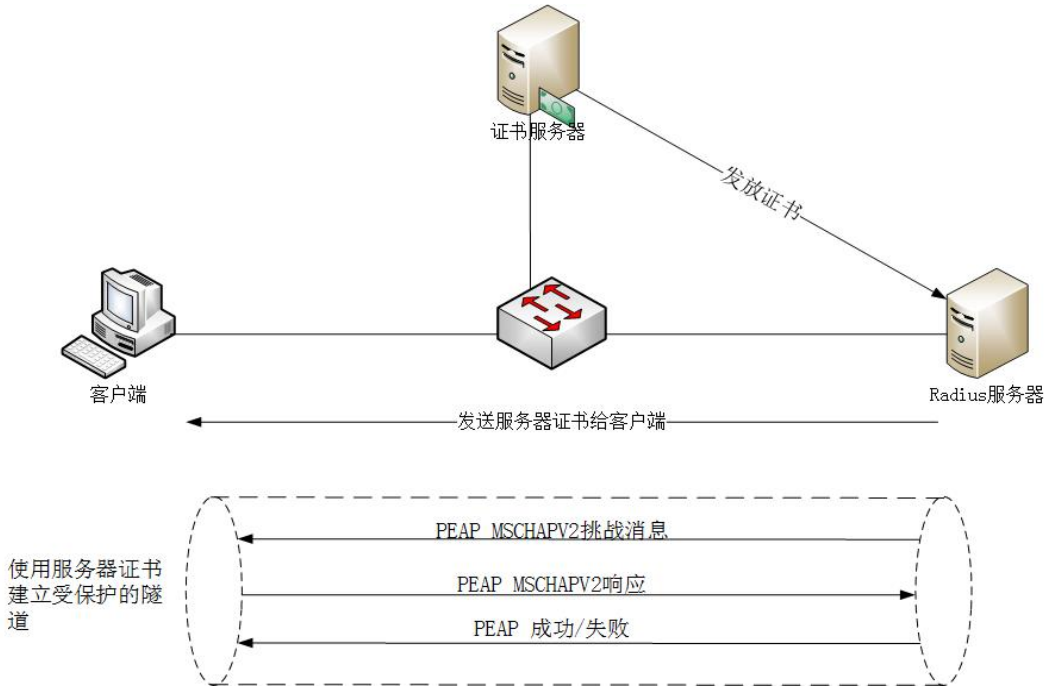

图 1-6 PEAP 认证方式

单独使用 MSCHAP V2 方式不够安全，PEAP 认证解决了这一缺点。PEAP 使用证书建立一个受保护的隧道来保证 MSCHAP V2 的安全性。攻击者要攻击 MSCHAP V2 认证首先需要攻击保护他的隧道，而证书加密方式目前看来安全性是非常高的。

在介绍 PEAP 之前先介绍一下对称密钥与非对称密钥。

非对称密钥是一个密钥对，分为公钥和私钥。公钥加密的数据只能通过私钥解密。优点是公钥可以方便的在网络上传输，不用担心被窃取，只要保护好自己的私钥不丢失就可以了。缺点是加密和解密的效率比较低。

对称密钥是加密和解密都用同一个密钥。缺点是如果密钥丢失，数据就可以被解密。优点是加密效率比较高。

PEAP 认证过程：

1. 首先需要有一个证书服务器，可以是客户自己搭建的内部证书服务器，也可以是公用的证书服务器。如果所有设备都在工厂内部，可以自己搭建证书服务器，否则需要使用大家都信任的公用证书服务器。
2. Radius 服务器向证书服务器申请一个数字证书，证书中包含一个密钥对（公钥和私钥），以及 Radius 服务器的描述信息。
3. Radius 服务器发送包含公钥的数字证书给客户端。

4. 客户端使用证书建立受保护的隧道。

下图描述了隧道建立的详细过程。

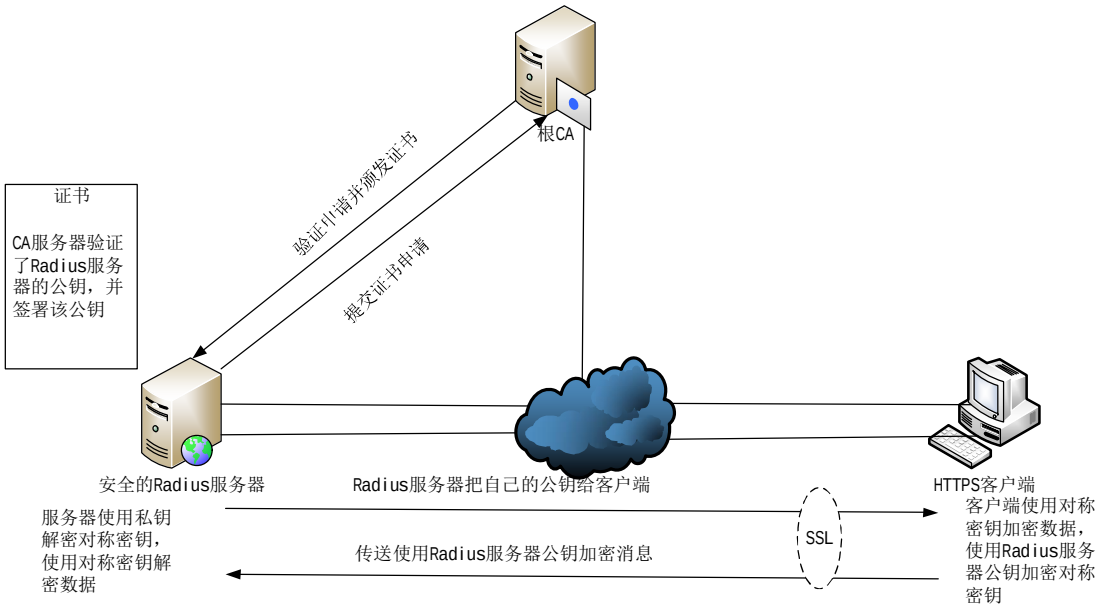

图 1-7 安全隧道建立过程

上图是安全隧道的建立过程。

1. 服务器将包含公钥的数字证书传递给客户端。
2. 客户端使用 CA 的公钥验证服务器的数字证书。
3. 客户端使用对称密钥加密双方交换的数据。由于客户端和服务器需要使用相同的对称密钥，为了将对称密钥传递给服务器，客户端用服务器的公钥加密对称密钥，然后将对称密钥传送给服务器。
4. 服务器获得加密的对称密钥后，用自己的私钥解密对称密钥。
5. 服务器获取了对称密钥，双方通过相同的密钥加密，解密数据，这样网络上传输的所有数据都是经过加密的，安全通道建立起来。

1.2.3 EAP_TLS 认证方式

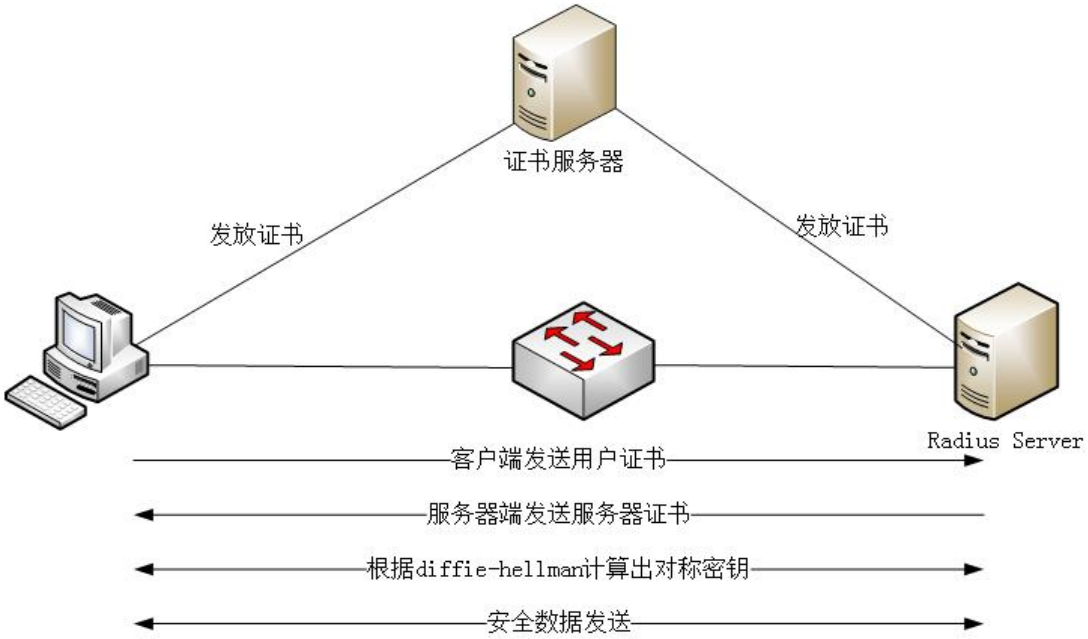

图 1-8 EAP_TLS 认证方式

PEAP 认证方式已经实现了比较安全的认证方式。但是缺点是建立安全隧道之前的认证是单向的。客户端验证了服务器的数字证书，服务器没有验证客户端。这样就有可能遭受中间人攻击。EAP_TLS 认证方式解决了该问题，客户端与服务器是双向认证的，只有双方都确认对方身份后，才建立起来安全隧道。

1. 服务器向 CA 申请数字证书，CA 验证后发放证书。证书包含服务器的公钥和私钥。
2. 客户端向 CA 申请数字证书，CA 验证后发送证书。证书包含客户端的公钥和私钥。
3. 客户端将包含自己公钥的证书发送给服务器，服务器将包含自己公钥的证书发送给客户端。
4. 由于客户端和服务器都信任同一个 CA，因此客户端和服务器都验证对方数字证书，确认对方身份合法。
5. 双方使用 Diffe-Hellman 密钥交换及对称密钥生成方法计算出对称密钥，并使用该对称密钥加密和解密数据。安全通信建立起来。

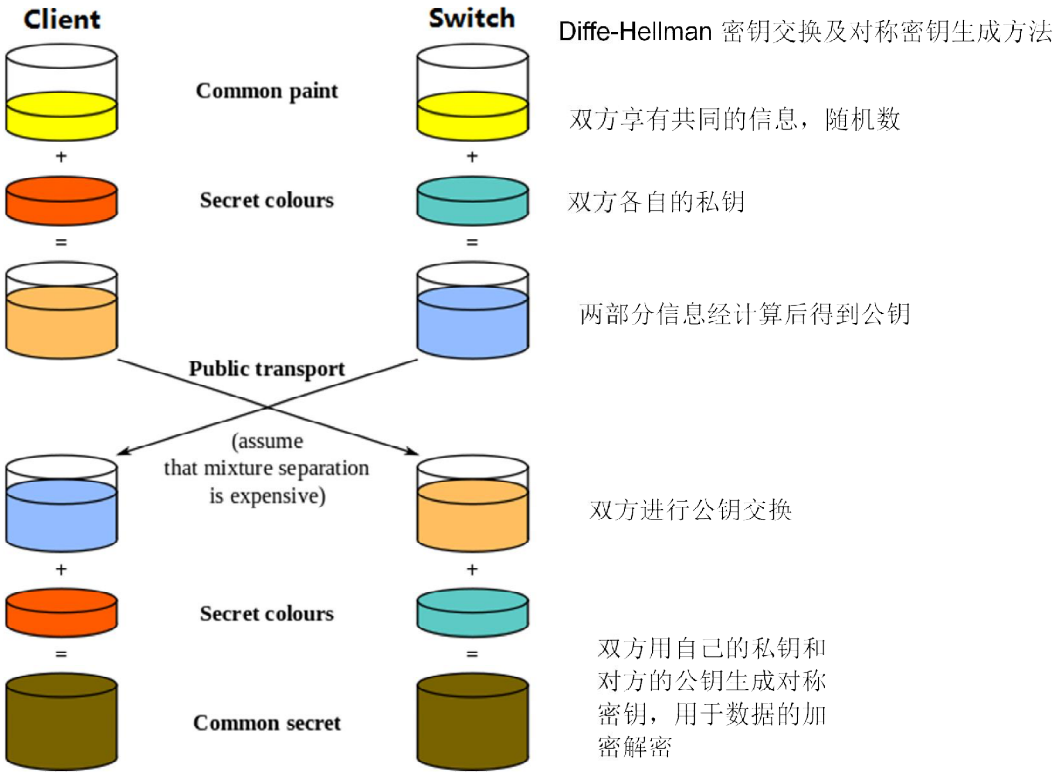

图 1-9 Diffe-Hellman 密钥交换

Diffe-Hellman 密钥交换及对称密钥生成方法如上图。

1. 首先双方交换随机数，双方共享同样的随机数。
2. 双方将随机数与各自的私钥经计算后得到一个公钥。
3. 双方将计算出的公钥传递给对方。
4. 双方用自己的私钥和对方的公钥生成完全相同的对称密钥。

由上述过程可以看到，EAP_TLS 方式没有用户名和密码的交换，只有包含公钥的数字证书交换就可以建立起来安全通信，是最安全的认证方式。但是由于需要为每个客户端和服务器都申请数字证书，需要工厂部署 CA 服务器，也是最复杂的方式。

1.3 硬件配置

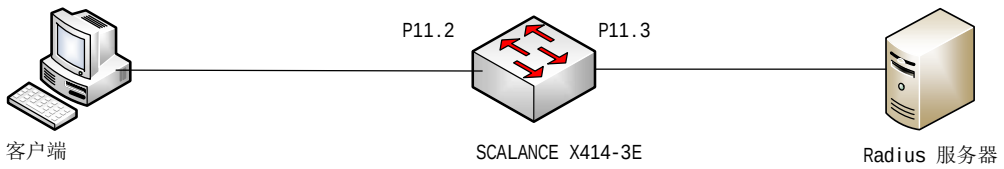

图 1-10 硬件配置图

本文中使用的硬件配置如上图。

- 1 台客户端电脑，运行 Windows XP 系统。
- 1 台 Scalance X 414-3E 交换机，订货号 6GK5414-3FC00-2AA2，固件版本号 V3.7.1。Port11.2 连接客户端电脑。IP 192.168.1.19。
- 1 台服务器，运行 Windows Server 2008 SP1，连接到交换机的 Port11.3，IP 192.168.1.125。

2 EAP_ MD5 认证方式配置

2.1 配置域服务

首先将 WINDOWS SERVER 2008 配置成为域服务器，域名为 office.siemens.com。

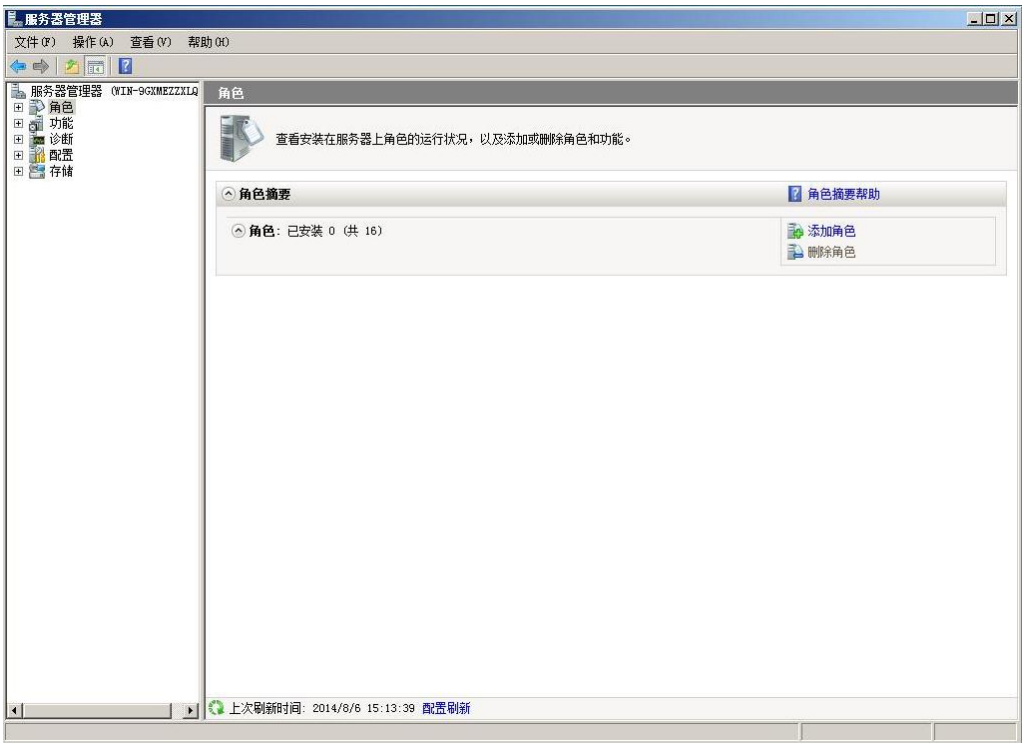

图 2-1 添加角色

打开“开始——服务器管理器”，打开如上图界面，可以看到，目前没有安装任何角色。点击“添加角色”。

图 2-2 添加角色

该页面提示管理员必须具有强密码，需要有静态 IP 等。首先检查管理员的密码是否符合强密码规则。然后设置本机的静态 IP 地址，如下图。设置 IP 为“ 192.168.1.125”。

图 2-3 IP 地址设置

注意：要正常使用域服务需要同时勾选 IPV4 地址和 IPV6 地址。否则域服务器无法联机。如下图。

图 2-4 本地连接属性设置

给 IPV6 地址也分配一个默认 IP 地址，这里不使用该地址。

图 2-5 安装域服务

图 2-6 安装域服务

如上图，勾选“ Active Directory”，然后点击下一步，准备安装域服务。

图 2-7 安装域服务

图 2-8 安装域服务

如上图，按照提示点击下一步，完成安装。安装完后需要重新启动计算机。点击“关闭该向导并启动 Active Directory 域服务安装向导”。或者直接在“开始”命令行中输入命令“ dcpromo.exe”启动域服务安装向导。

图 2-9 域服务配置向导

如上图，打开域服务安装向导，点击下一步，开始配置域服务。

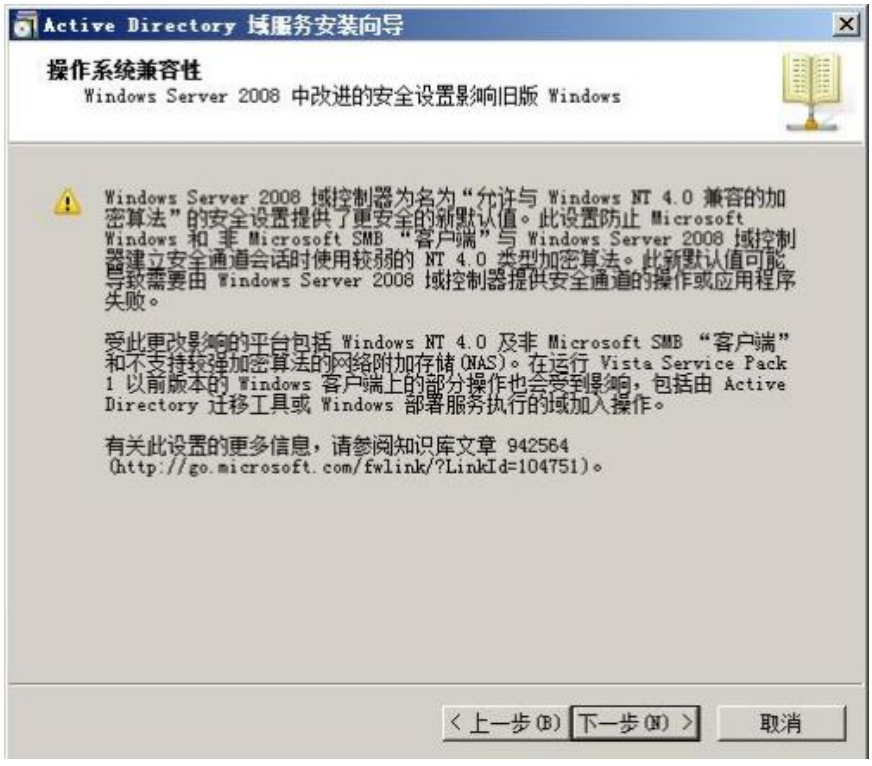

图 2-10 域服务配置向导

图 2-11 域服务配置向导

如上图，选中“在新林中新建域”，然后点击下一步。

图 2-12 域服务配置向导

图 2-13 域服务配置向导

图 2-14 域服务配置向导

勾选 DNS 服务器，会自动安装并配置 DNS 服务器。

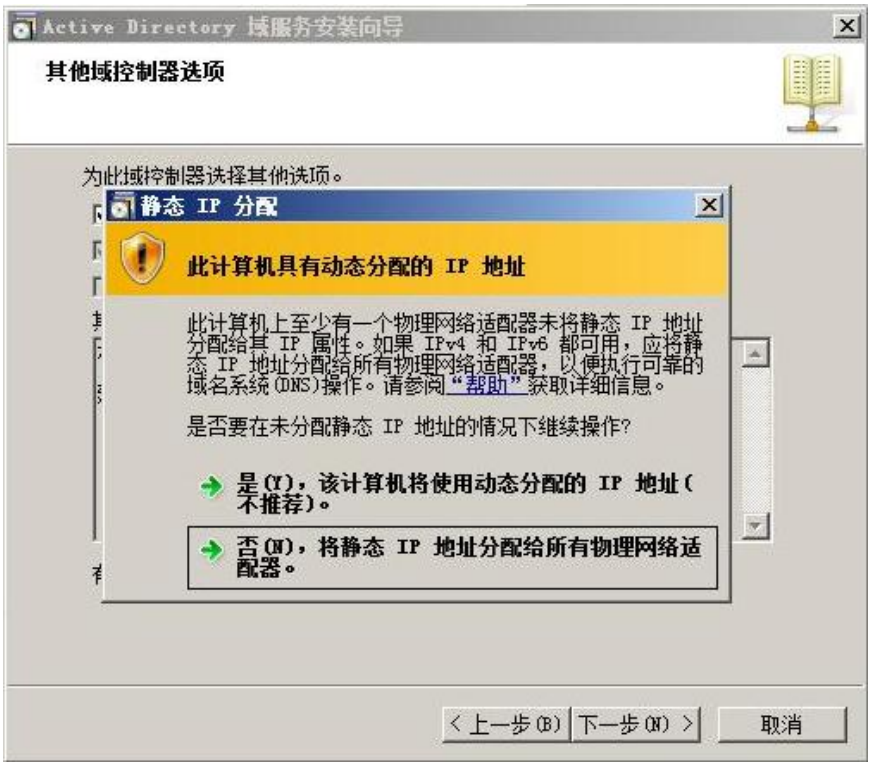

图 2-15 域服务配置向导

如果在图 2-4 步骤中已经给 IPV6 分配了默认的静态 IP，并且所有的网卡都有静态 IP 地址，这里选择“否，将静态 IP 地址分配给所有物理网络适配器”，否则选择“是，该计算机将使用动态分配的 IPV6 地址”。

图 2-16 域服务配置向导

在图 2-16 步骤中，会出现上述提示，点击“是”继续。

图 2-17 域服务配置向导

在图 2-17 步骤中选择数据库文件，日志文件，SYSVOL 文件存储的目录，这里用默认设置。

图 2-18 域服务配置向导

设置目录服务还原模式的管理员密码，这里需要设置一个符合强密码规则的密码。

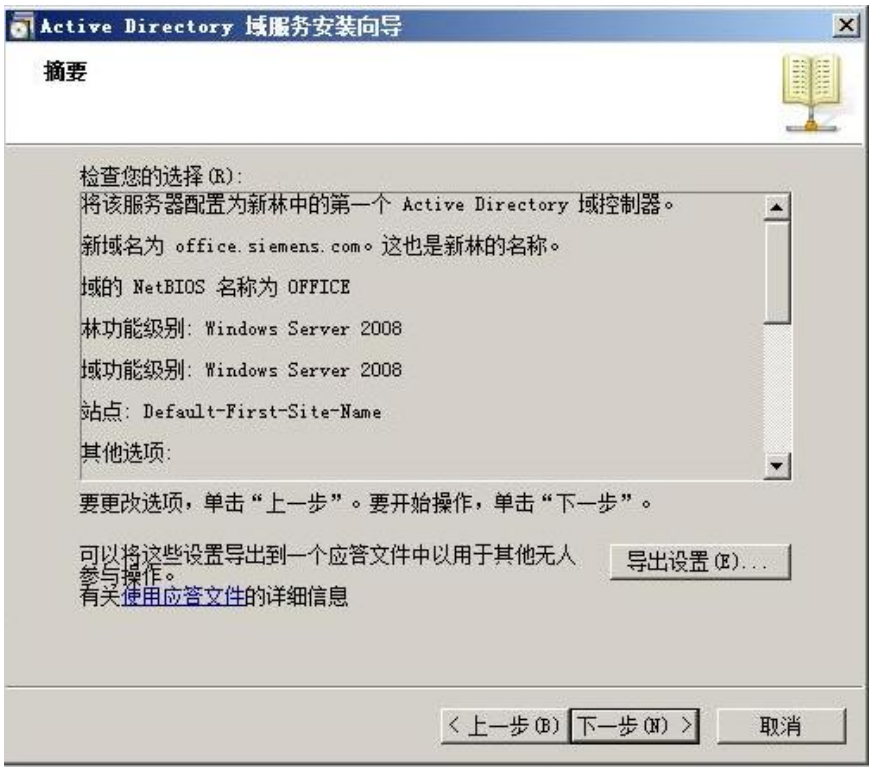

图 2-19 域服务配置向导

图 2-20 域服务配置向导

图 2-21 域服务配置向导

2.2 配置组策略

MD5 Challenge 认证方式需要更改 Windows Server 2008 的默认密码存储策略。Windows Server 2008 对存储的密码是有加密保护的，如果应用程序使用了要求知道用户密码才能进行身份验证的协议，需要使用可还原的加密存储密码。该策略和存储明文版本密码在本质上是相同的。因此，除非应用程序有比保护密码信息更重要的要求，否则不必启用该策略。

在图 2-22 中步骤中，启用使用可还原的加密存储密码。打开“开始——管理工具——组策略管理”，打开如图 2-22。在左侧目录选择“域——office.siemens.com——组策略对象——Default Domain Policy”，在右侧选择“策略——Windows 设置——安全设置——帐号策略，密码策略”。点击“显示”可以查看当前的策略。选中“帐号策略，密码策略”，点击右键，菜单中选择“配置”，打开如图 2-23 的界面。

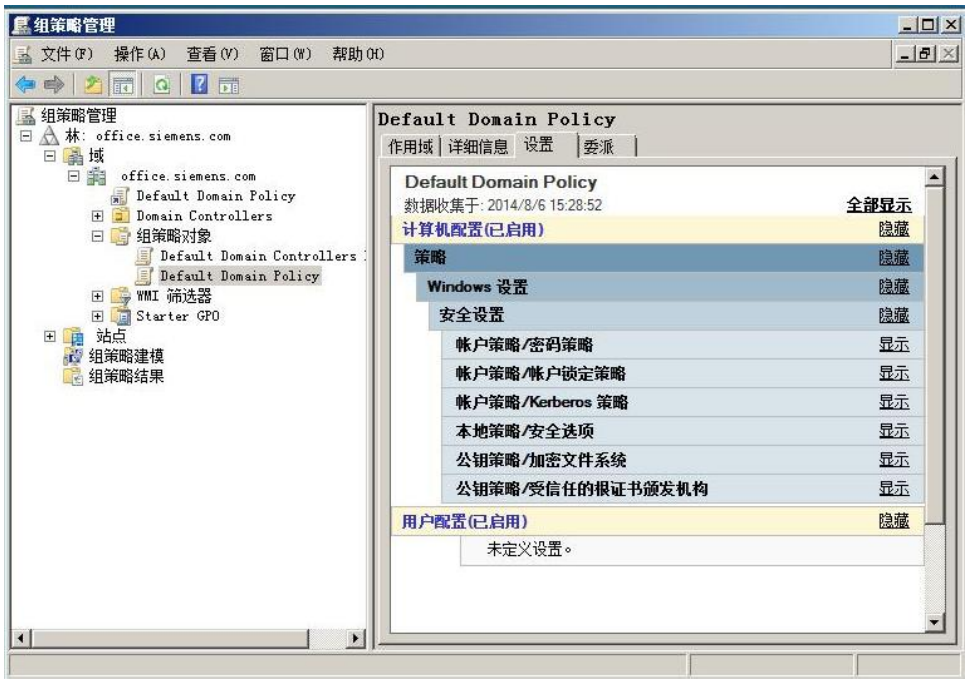

图 2-22 密码策略设置

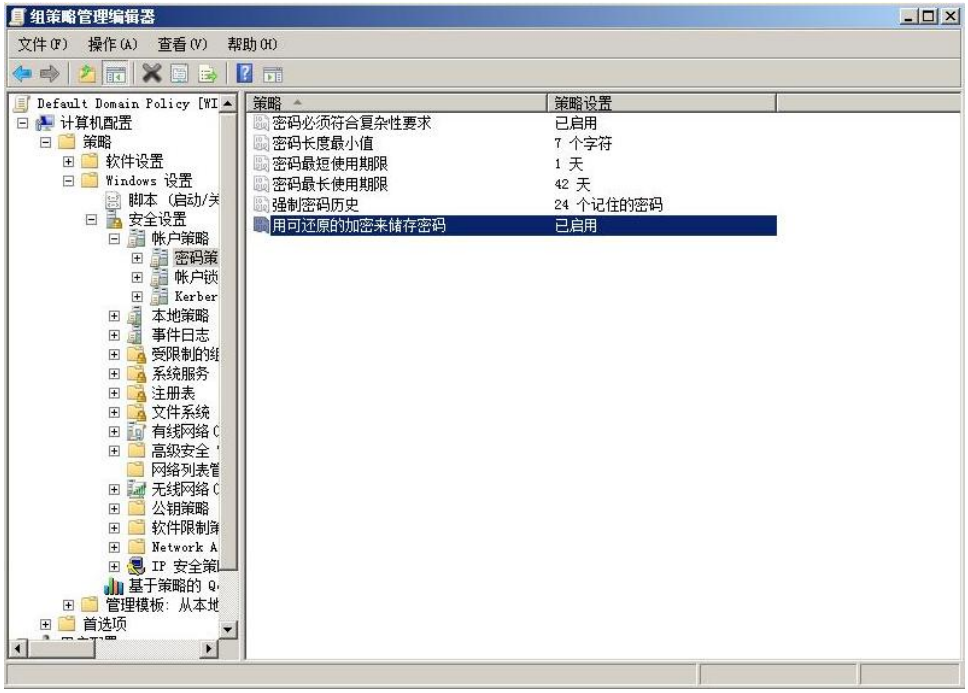

图 2-23 密码策略设置

在图 2-23 中，左侧菜单选择“计算机配置——策略——Windows 设置——安全设置——密码策略”，在右侧启用“用可还原的加密来存储密码”。

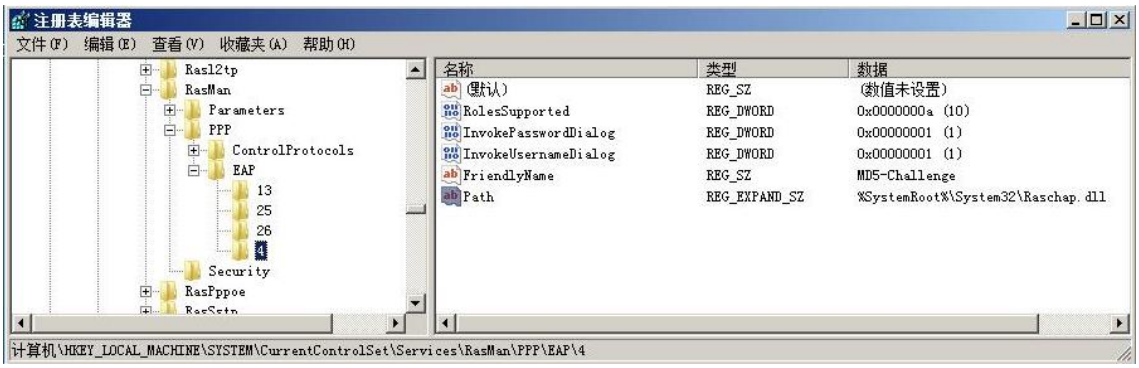

图 2-24 在注册表中使能 MD5-Challenge 认证

为了安全起见，Windows Server 2008 默认关闭了安全性不高的 MD5-Challenge 认证方式，需要通过更改注册表重新使能。

在运行里输入 regedit 打开注册表，找到以下位置：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\

创建新项“4”如下：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\4

然后添加以下键值：

键名：RolesSupported

类型：REG_DWORD

键值：0000000a

键名：FriendlyName

类型：REG_SZ

键值：MD5-Challenge

键名：Path

类型：REG_EXPAND_SZ

键值：%SystemRoot%\System32\Raschap.dll

键名：InvokeUsernameDialog

类型：REG_DWORD

键值：00000001

键名：InvokePasswordDialog

类型：REG_DWORD

键值：00000001

2.3 配置用户组

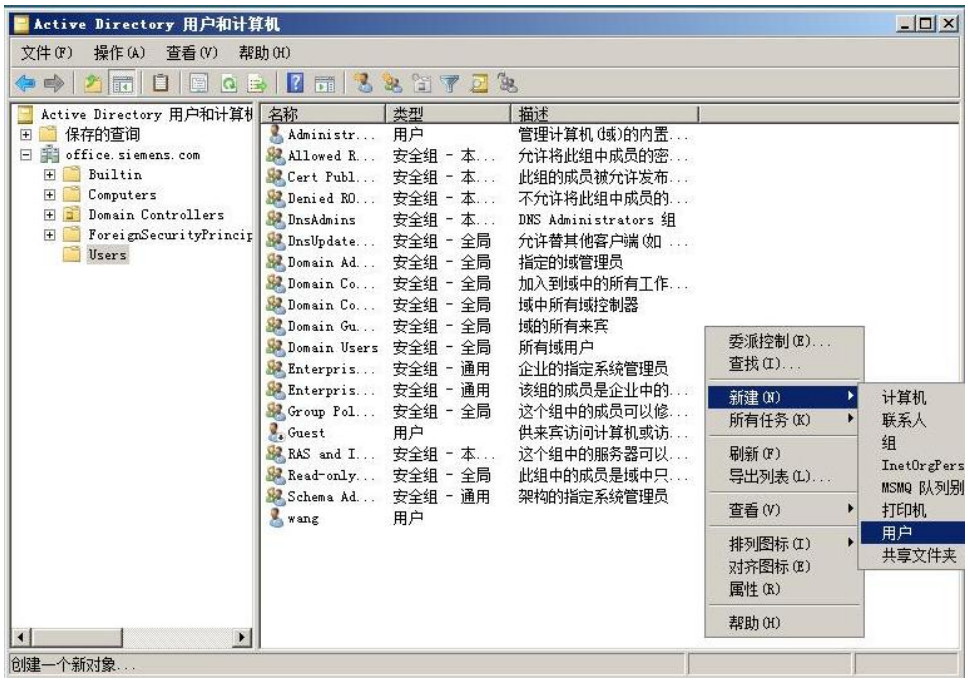

图 2-25 配置用户组

打开“开始——管理工具——Active Directory 用户和计算机”。打开如图 2-25 的界面。在空白处点击右键，菜单中选择“新建——用户”。新建一个用户“ cs1cs1”，如图 2-26 所示。

图 2-26 新建用户

图 2-27 新建用户

在图 2-27 中，设置新用户的用户名和密码。

图 2-28 新建用户

图 2-29 新建用户组

新建用户完成后，然后新建一个用户组“ CS”。同新建用户方式相同，在图 2-25 界面中空白处点击右键，菜单中选择“新建——用户组”。

图 2-30 将用户加入用户组

图 2-31 将用户加入用户组

现在需要将新建的用户“cs1cs1”加入用户组“cs”。如图 2-30，选择“添加”，在对话框中选择高级，打开如图 2-31 的界面，点击“立即查找”，在搜索结果中选择“cs1cs1”，将其添加到用户组“cs”。

图 2-32 将用户加入用户组

添加成功后，在用户组“cs”的“成员”选型页中可以看到组成员“cs1cs1”。

2.4 安装并配置网络策略和访问服务

图 2-33 安装网络策略和访问服务

打开“开始——服务管理器”，添加新角色。勾选网络策略和访问服务。

图 2-34 安装网络策略和访问服务

图 2-35 安装网络策略和访问服务

图 2-36 安装网络策略和访问服务

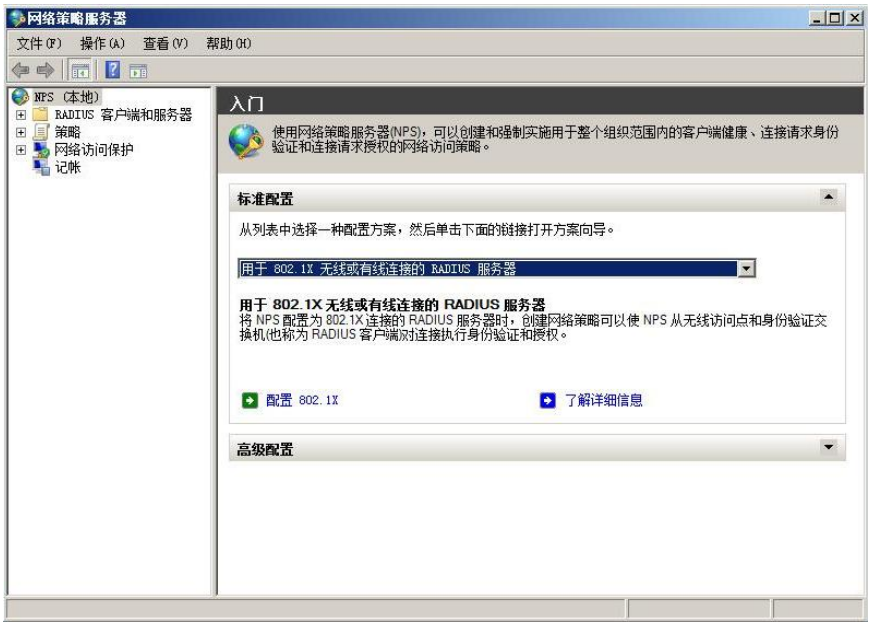

图 2-37 配置网络策略和访问服务

打开“开始——管理工具——网络策略服务器”，打开如何 2-37 所示的界面。在下拉列表中选择“用于 802.1x 无线或有线的 Radius 服务器”。

图 2-38 配置网络策略和访问服务

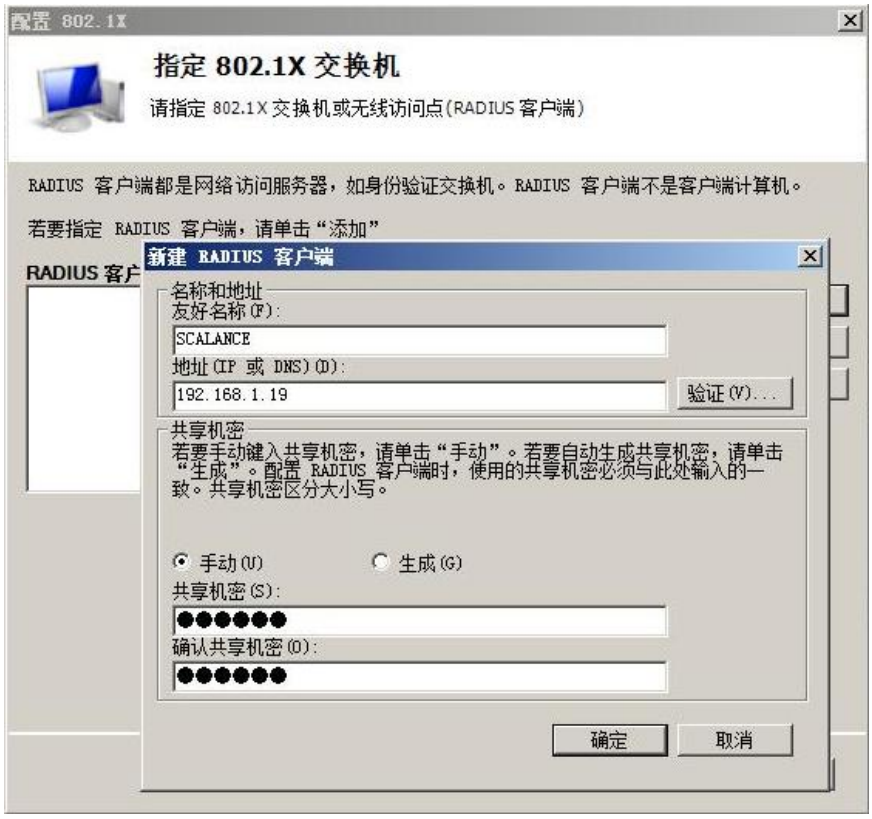

图 2-39 配置网络策略和访问服务

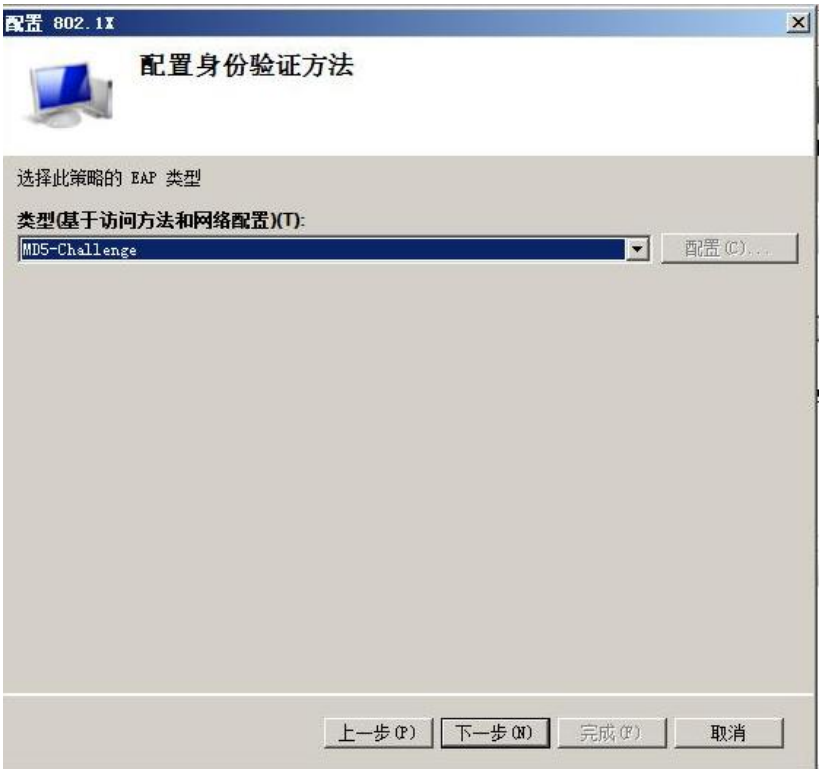

图 2-40 配置网络策略和访问服务

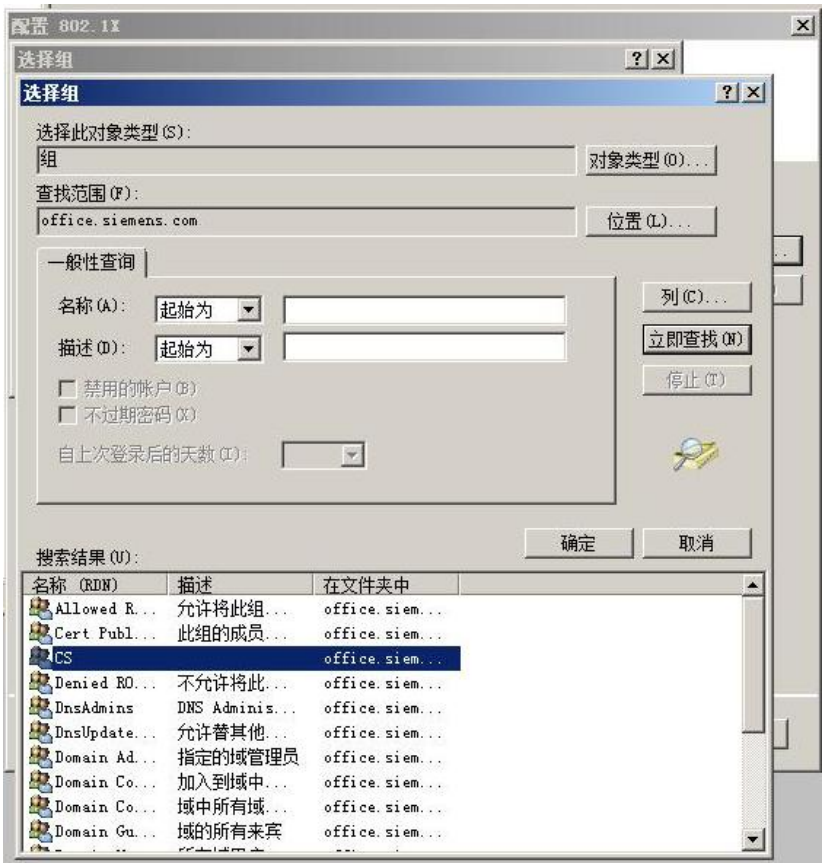

图 2-41 配置网络策略和访问服务

在图 2-39 中，配置 Radius 客户端，该处 Radius 客户端是 Scalance X 交换机。设置交换机的 IP 地址和共享密码。需要与交换机实际参数设置一致。

在图 2-40 中设置认证方式为 MD5-Challenge。

在图 2-41 中将用户组“ CS”加入允许访问的用户组。这样，用户组“ CS”中的所有用户都可以访问。

图 2-42 配置网络策略和访问服务

图 2-43 配置网络策略和访问服务

图 2-44 配置网络策略和访问服务

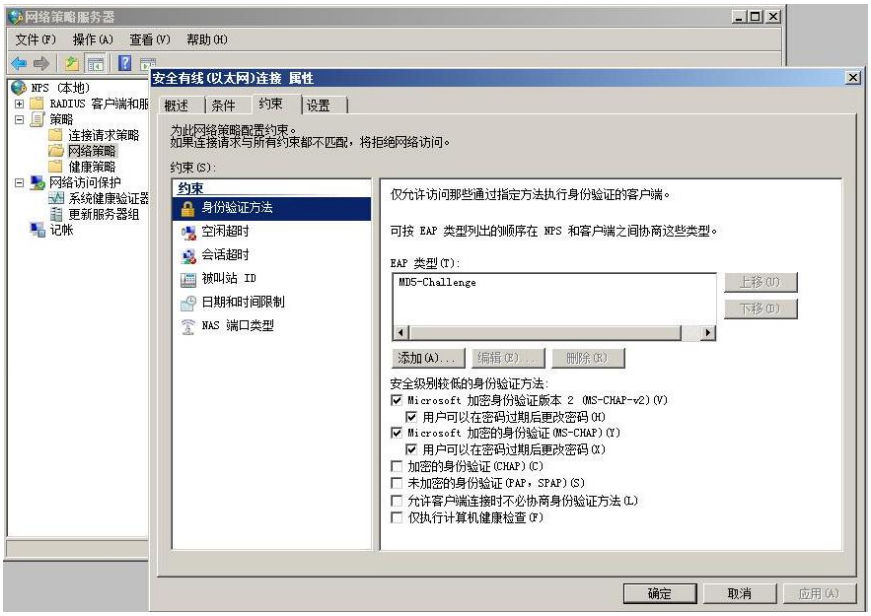

图 2-45 配置网络策略和访问服务

2.5 配置交换机

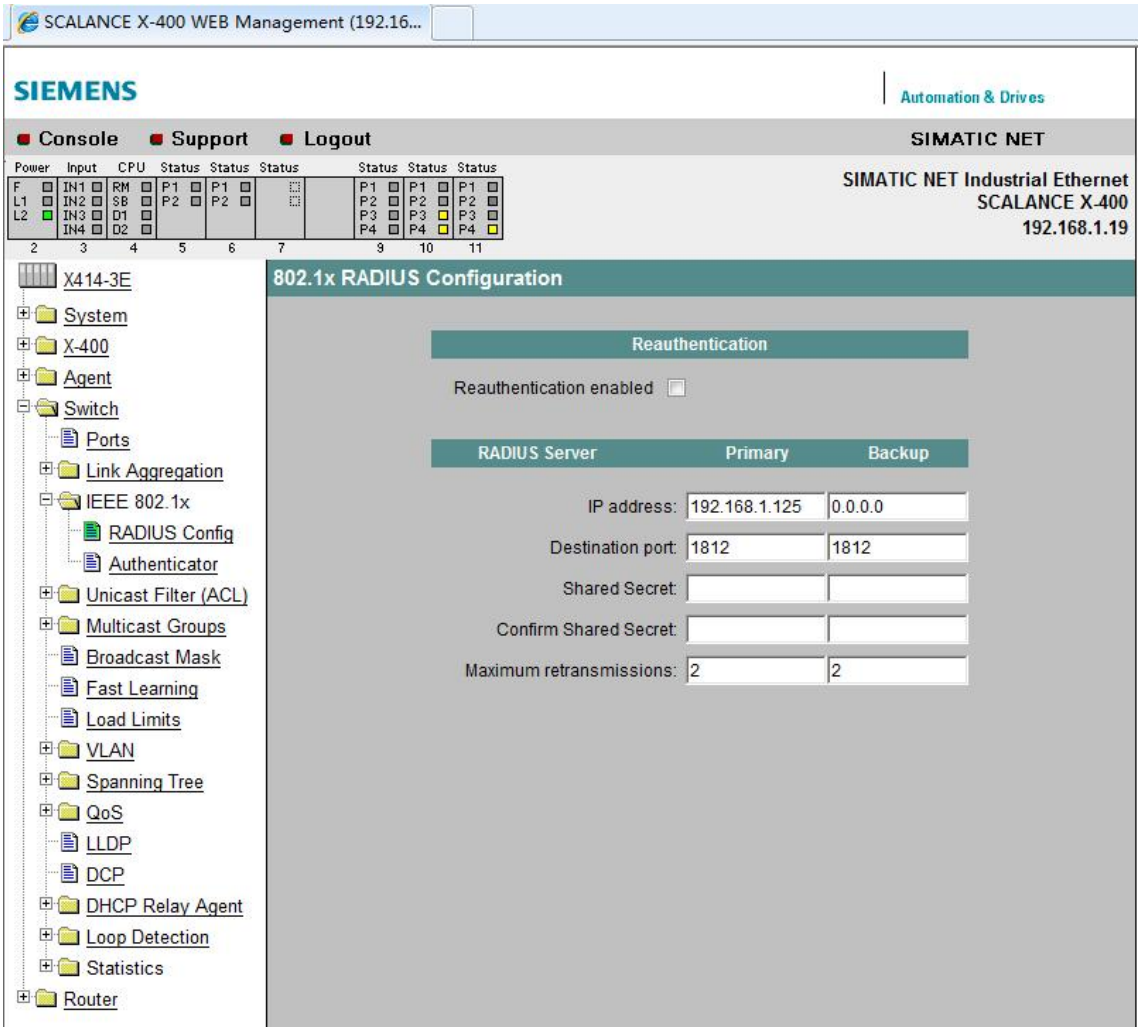

图 2-46 交换机配置

上图是 SCALANCE X414-3E 交换机的配置界面。在“ Switch——IEEE802.1x——Radius Config”界面中填写 Radius Server 的 IP 地址，可以最多填写两个，一个作为备用。“ Shared Secret”填写共享密码，与图 2-39 中设置的密码要相同。“ Confirm Shared Secret”再次填写共享密码。设置完成后点击“ Set Value”。

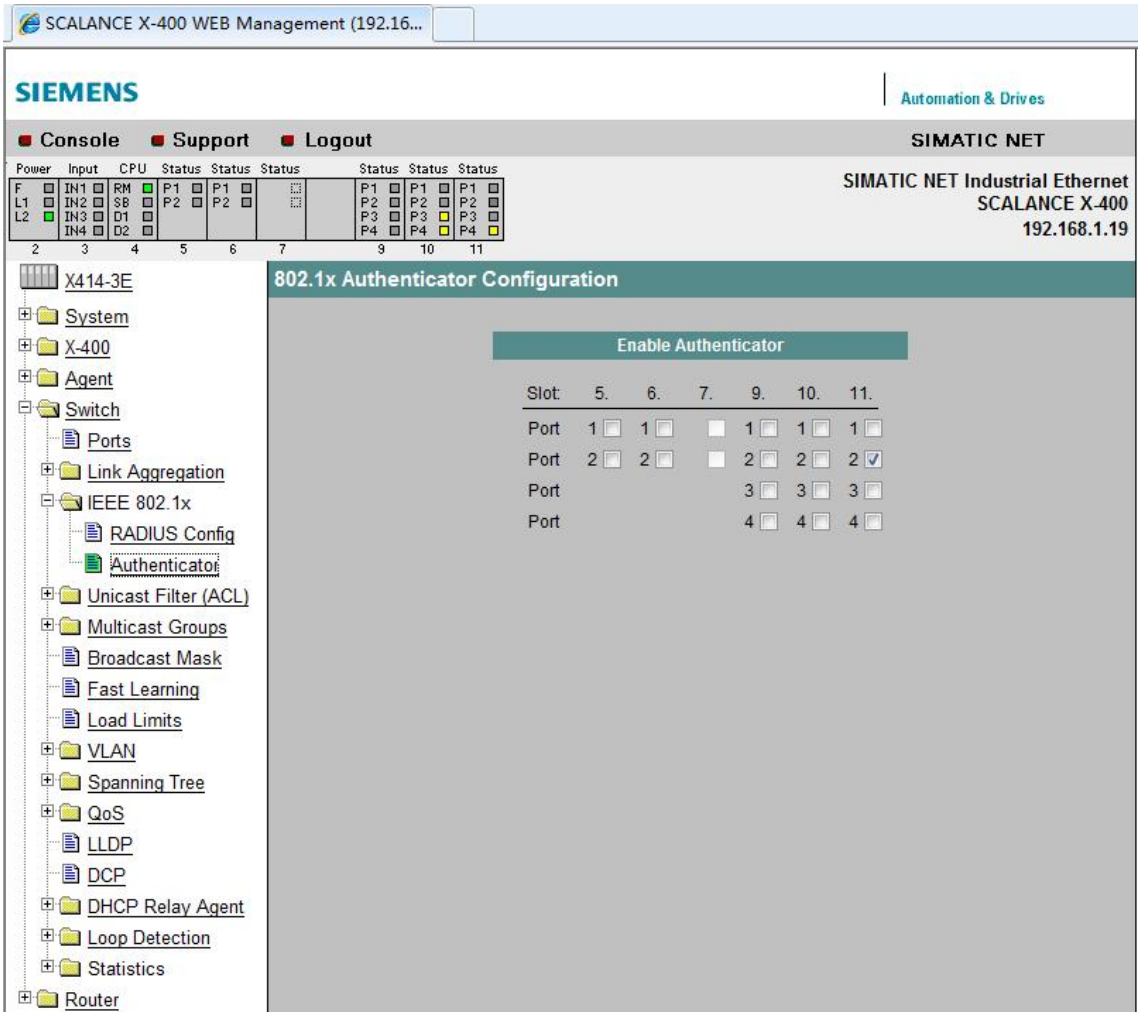

图 2-47 交换机配置

在“ Switch——IEEE802.1x——Radius Config——Authenticator”中设置端口。申请者，也就是客户端电脑连接在交换机的 PORT11.2，这里就勾选 PORT11.2，交换机会对该端口的连接请求进行认证。只有认证通过后，该端口才会完全打开，否则只允许认证报文通行，其他报文被阻断。

2.6 客户端电脑设置

在客户端电脑中，选择 “计算机”右键菜单中选择“管理”，然后“服务和应用程序”，打开“服务”。启动服务“ Wired AutoConfig”，将启动方式更改为“自动”。如果使用的电脑是 Win7，需要更改注册表，使能 MD5 质询方式认证。更改方式见图 2-24。

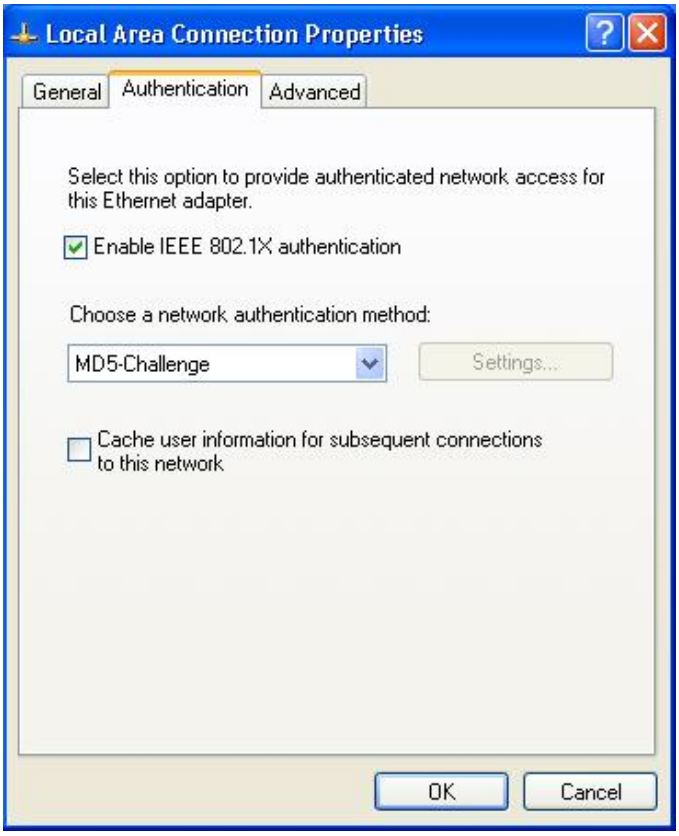

图 2-48 客户端电脑设置

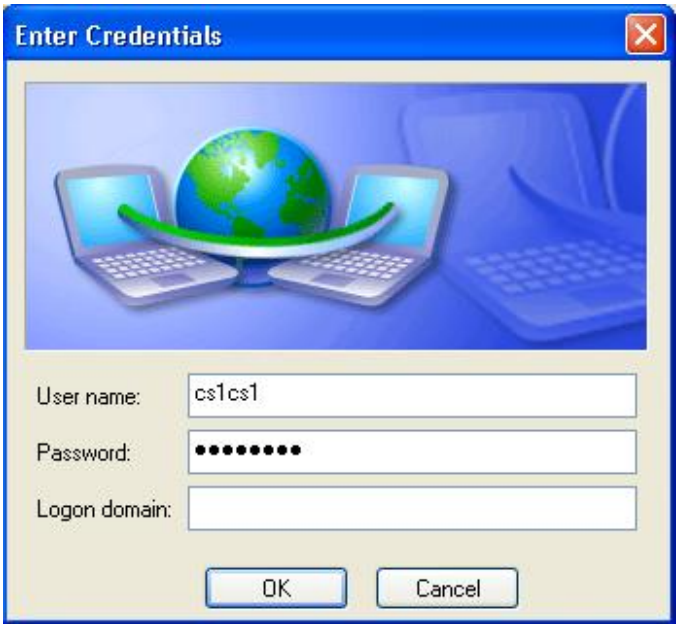

图 2-49 客户端电脑设置

在客户端电脑上，打开本地连接，在认证页面中勾选 802.1X 认证，认证方式选为 MD5-Challenge。点击确认后，电脑本地连接图标处会提示需要输入更多信息，点击提示，出现

如图 2-49 所示的对话框。输入用户名“ cs1cs1”和密码，点击确认后，客户端电脑显示验证通过。

在未认证时，本地连接显示问号，客户端无法通过交换机的 11.2 端口连接到网络。认证通过后显示连接建立，客户端可以通过 11.2 端口 Ping 通网络上的任意设备。

3 PEAP 认证方式配置

3.1 安装 CA 服务器

PEAP 需要 CA 服务器颁发数字证书。这里将 Windows Server 2008 配置成为 CA 服务器，并给 Radius Server 服务器颁发数字证书。

图 3-1 安装证书服务

点击“开始——服务器管理器”添加角色。勾选“ Active Directory 证书服务”和“ Web 服务器”，点击下一步开始安装。

图 3-2 安装证书服务

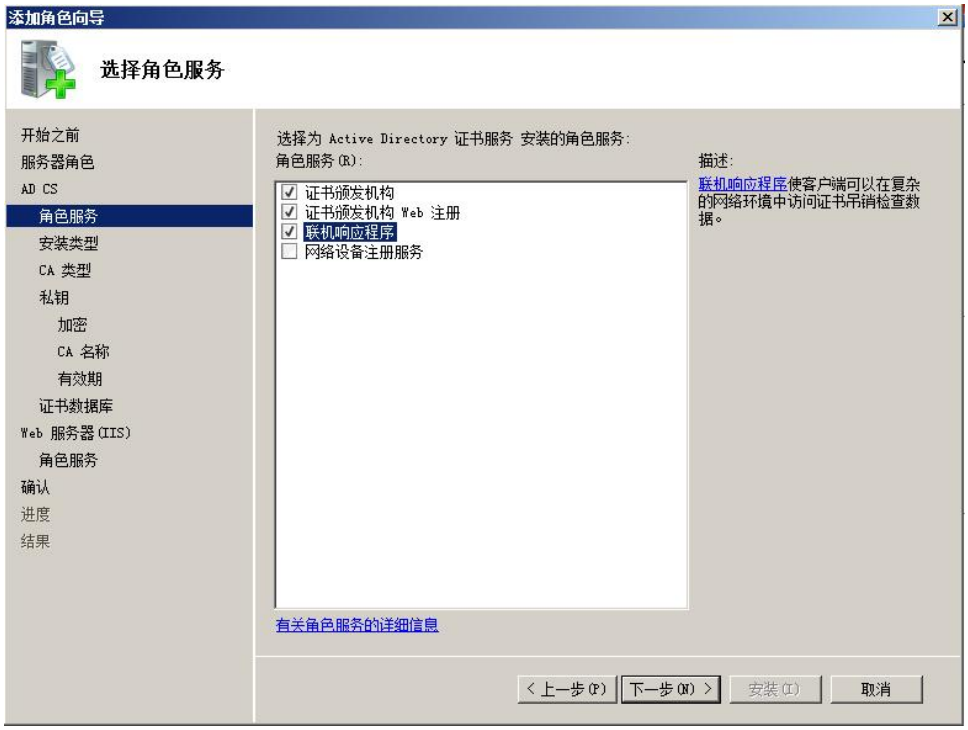

图 3-3 安装证书服务

如上图，勾选“证书颁发机构”，“证书颁发机构 Web 注册”，“联机响应程序”。

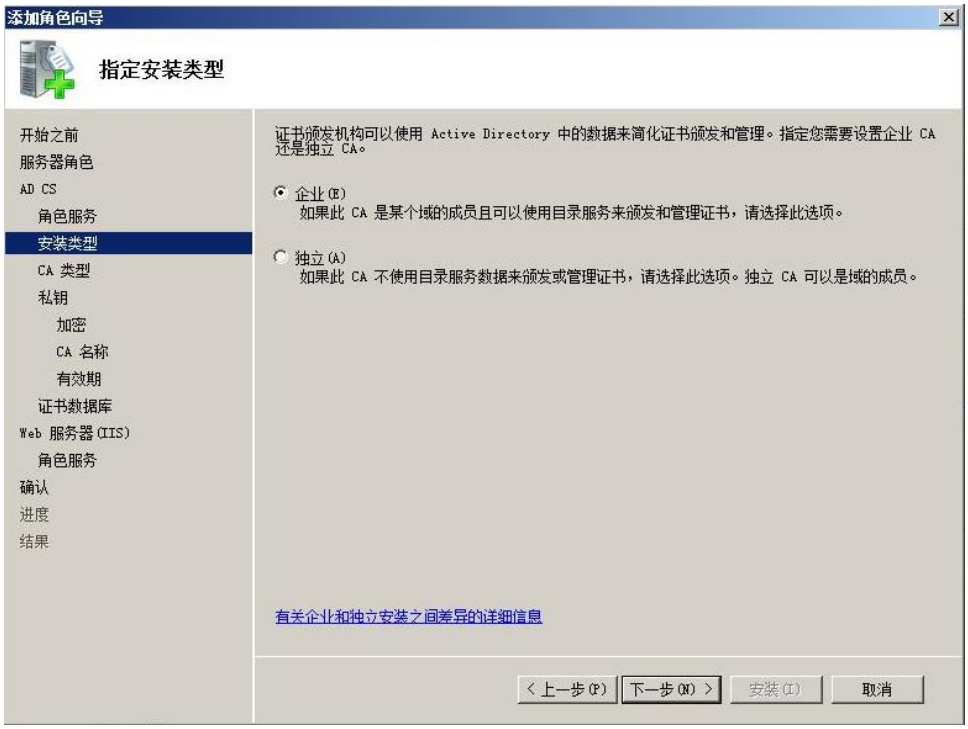

图 3-4 安装证书服务

由于之前已经配置了域，这里将 CA 服务器配置为企业 CA。配置为独立 CA 也是可以的。以下的配置都以企业 CA 为例子。

图 3-5 安装证书服务

在图 3-5 中，由于这里没有隶属于任何 CA，所以将其配置为根 CA。

图 3-6 安装证书服务

由于是第一次配置 CA 服务器，所以这里选择“新建私钥”。

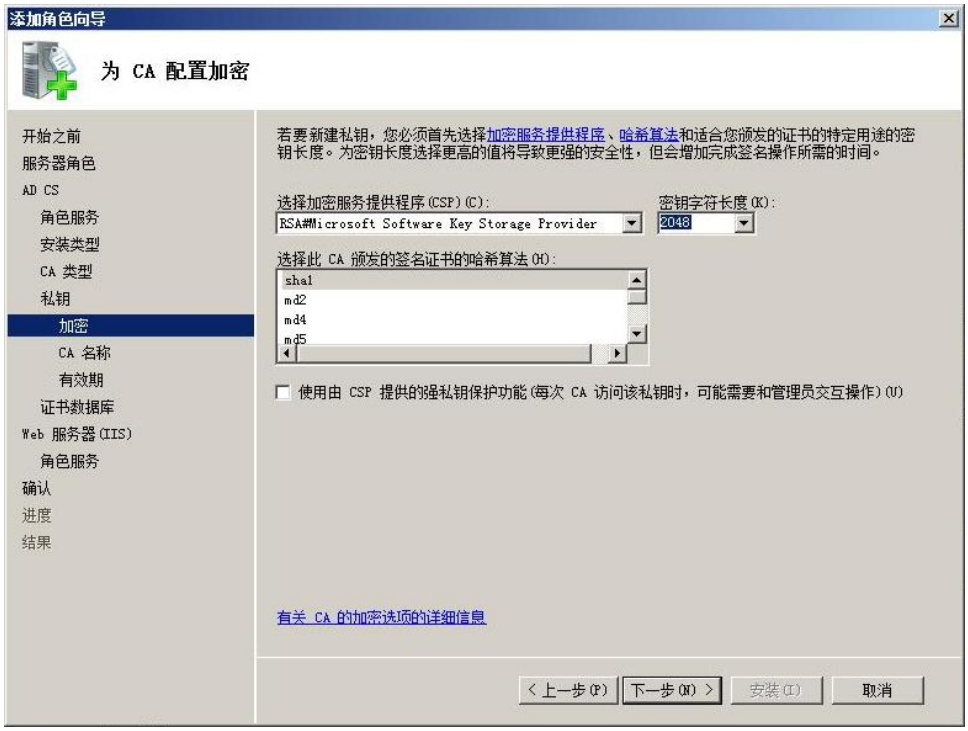

图 3-7 安装证书服务

密钥越长，越不容易被破解，选择 2048。签名证书的哈希算法选择更安全的“ sha1"。

图 3-8 安装证书服务

在图 3-8 的界面中，设置 CA 的公用名称为“ office-win-testca”。

图 3-9 安装证书服务

图 3-10 安装证书服务

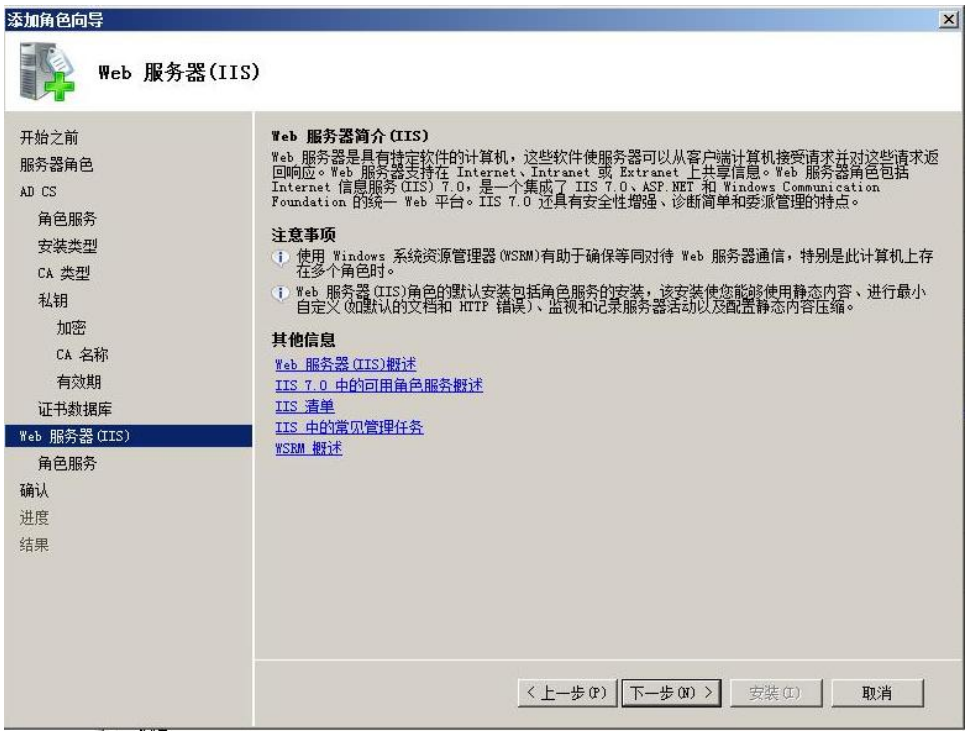

图 3-11 安装 IIS 服务

申请数字证书需要使用到 Web Server，因此这里需要安装 IIS 服务。

图 3-12 安装 IIS 服务

图 3-13 安装 IIS 服务

图 3-14 确认安装

图 3-15 成功安装证书服务和 IIS 服务

3.2 配置 CA 服务器

角色服务安装完成后，在开始菜单中打开“管理工具”。选中其中的“ Certification Authority”打开。如下图的界面。其中证书颁发机构“ office-win-testca”就是刚才建立的根 CA。下面的各个目录中分别是：吊销的证书，颁发的证书，挂起的申请，失败的申请。

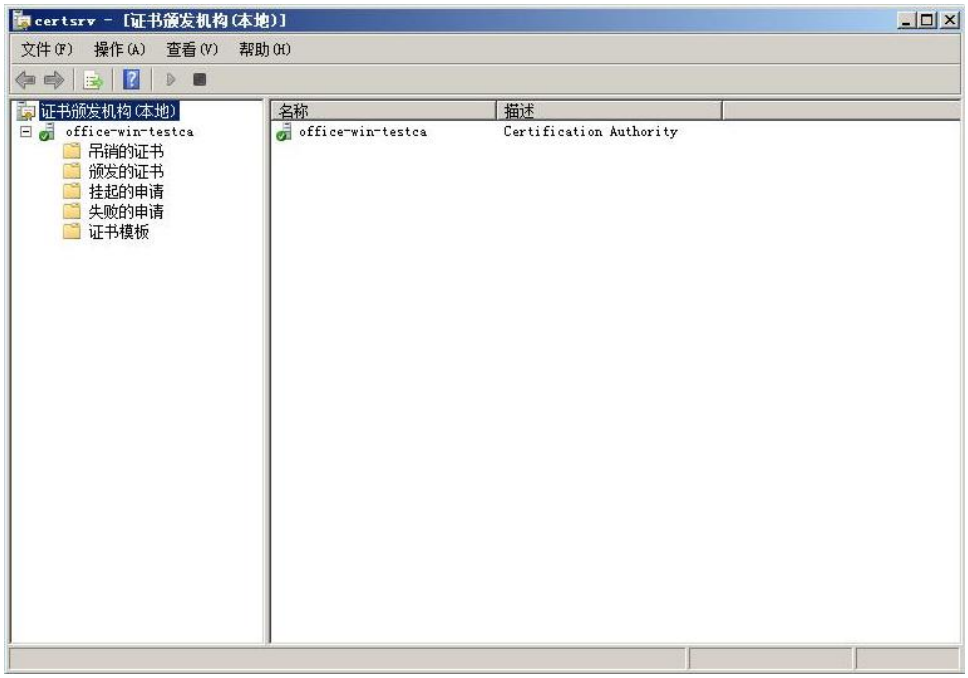

图 3-16 证书颁发机构

由于向 CA 申请数字证书需要使用 HTTPS 的方式，所以首先要给 CA 服务器的 WEB Server 申请一个数字证书。该数字证书是基于根证书颁发机构“ office-win-testca”申请的。也就是说，其它计算机只要信任该根证书颁发机构，就能信任 CA Web Server 的数字证书。

首先给 Web 服务器申请一个数字证书。申请方式如以下步骤。

在开始菜单中打开“管理工具”，打开 IIS 管理器。如图 3-17 所示，左侧选中最顶层目录，双击“服务器证书”的图标打开。点击右侧的创建证书申请，为 IIS WEB 服务器申请一个数字证书。

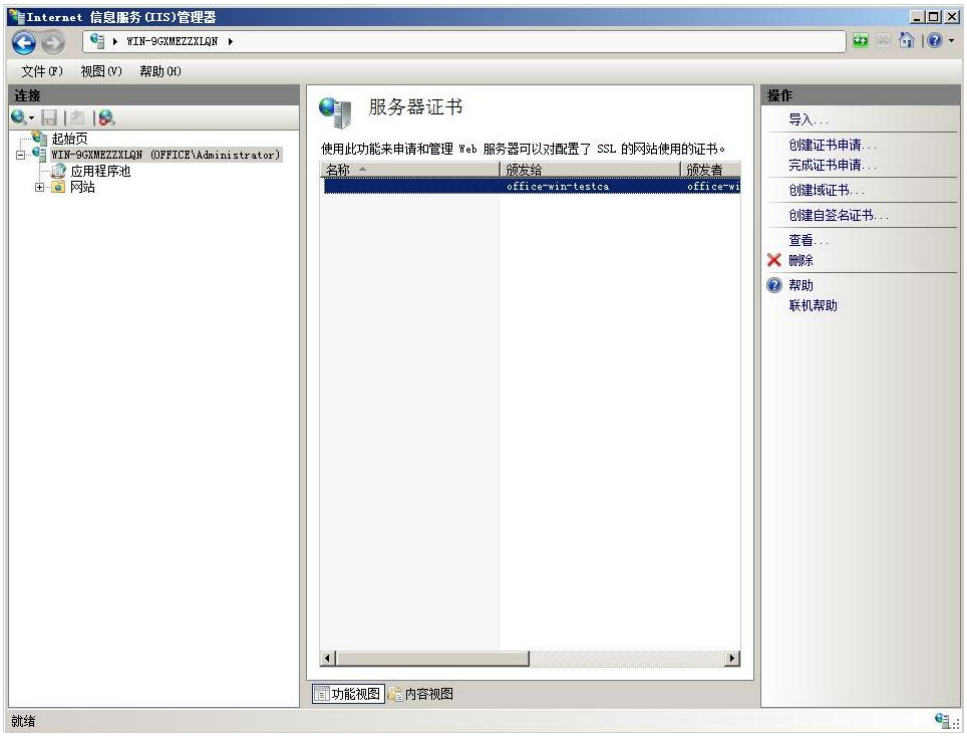

图 3-17 IIS 管理器

图 3-18 申请证书

申请数字证书需要提供一系列机构信息。通用名称指申请数字证书的 WEB 服务器的域名。由于这里没有使用 DNS 解析域名，在此处填写 WEB 服务器的 IP 地址。以下部分是组织结构的详细信息。CA 需要核实这些信息无误后才给申请证书的机构颁发。

图 3-19 选择加密服务程序

图 3-20 选择证书申请文件导出的文件名

这里将证书导出到“C”盘的根目录下，文件名为“CAWEB”。

图 3-21 生成的证书申请文件

图 3-22 申请 WEB 服务器数字证书

由于客户端向 CA 服务器申请数字证书需要通过 WEB 的形式，为了安全性，数字证书的申请采用加密的方式，即 HTTPS 方式，所以首先需要给 WEB 服务器申请一个合法的数字证书。

这里使用刚才配置好的 CA 服务器来提供数字证书。在 IE 浏览器中输入 WEB 服务器的 IP 地址，即服务器的本机 IP “ http://192.168.1.125/certsrv”。

图 3-23 申请 WEB 服务器数字证书

图 3-24 申请 WEB 服务器数字证书

在图 3-23 中可以选择申请的证书类型，这里选择高级证书申请。在图 3-24 中选择使用 base64 编码提交证书申请。

图 3-25 申请 WEB 服务器数字证书

图 3-26 申请 WEB 服务器数字证书

在图 3-25 中，将图 3-21 的内容粘贴到空白栏中。证书模板选择“ Web 服务器”。在图 3-26 中选择“下载证书”。

图 3-27 申请 WEB 服务器数字证书

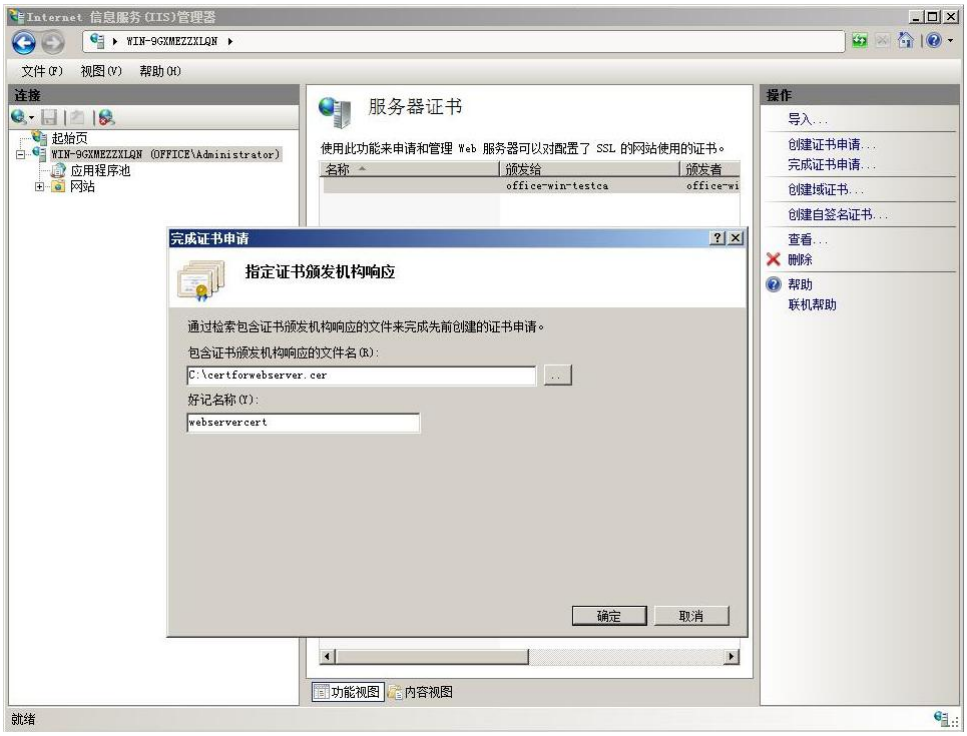

图 3-28 导入证书

如图 3-27，将证书保存为文件“ c:\certforwebserver”，保存类型为安全证书。保存完毕后可以在 C 盘找到该文件。

如图 3-28，打开 IIS 管理器，在左侧选择根目录，然后双击“服务器证书”打开。在右侧选择“完成证书申请”。选择刚才生成的证书，并起一个好记的名字。点击确认将证书导入。

证书导入成功后可以看到该服务器证书已经在列表中，如图 3-29。

图 3-29 导入证书

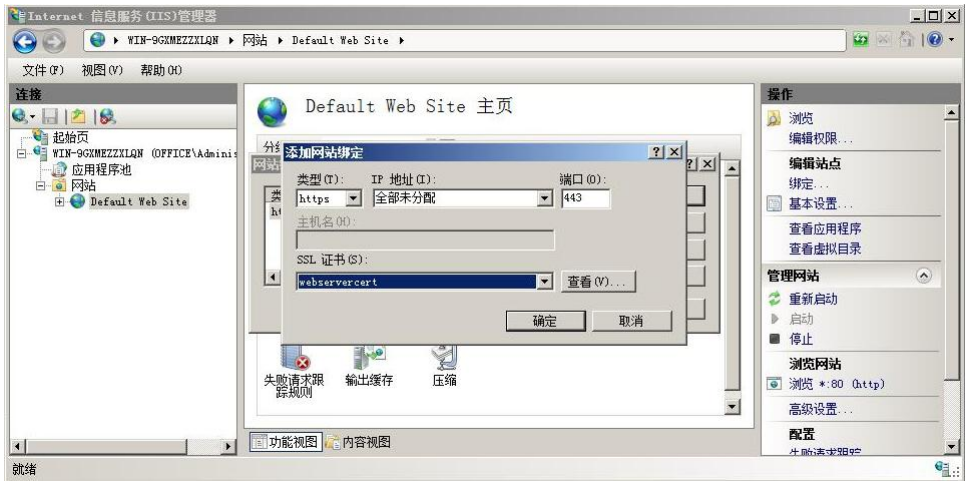

图 3-30 编辑网站绑定

在左侧目录中选择“ Default Web Site"，然后在右侧点击“绑定”。在“网站绑定”对话框点击“添加”按钮，添加一个类型“ https”的绑定。IP 地址选择“全部未分配”，SSL 证书选择刚才生成的证书。

3.3 为 Radius Server 申请管理员证书

PEAP 认证方式需要 Radius Server 申请数字证书，下面用刚才配置好的 CA 服务器 Web 方式申请。在安装 Radius Server 电脑上打开 IE 浏览器，输入域用户的用户名和密码就可以申请，如果在不是 Radius Server 的电脑上申请，需要将申请到的证书导出后再导入到 Radius Server。

下面开始为 Radius Server 申请数字证书。在 IE 浏览器中输入“https://192.168.1.125/certsrv”。自动弹出对话框要求输入用户名和密码。由于本应用中 CA 服务器和 Radius Server 在同一台计算机上，使用共同的用户“administrator”，因此在弹出的对话框中输入管理员的用户名和密码。如果 Radius Server 安装在其它电脑，需要输入为 Radius Server 分配的用户名和密码来申请数字证书。

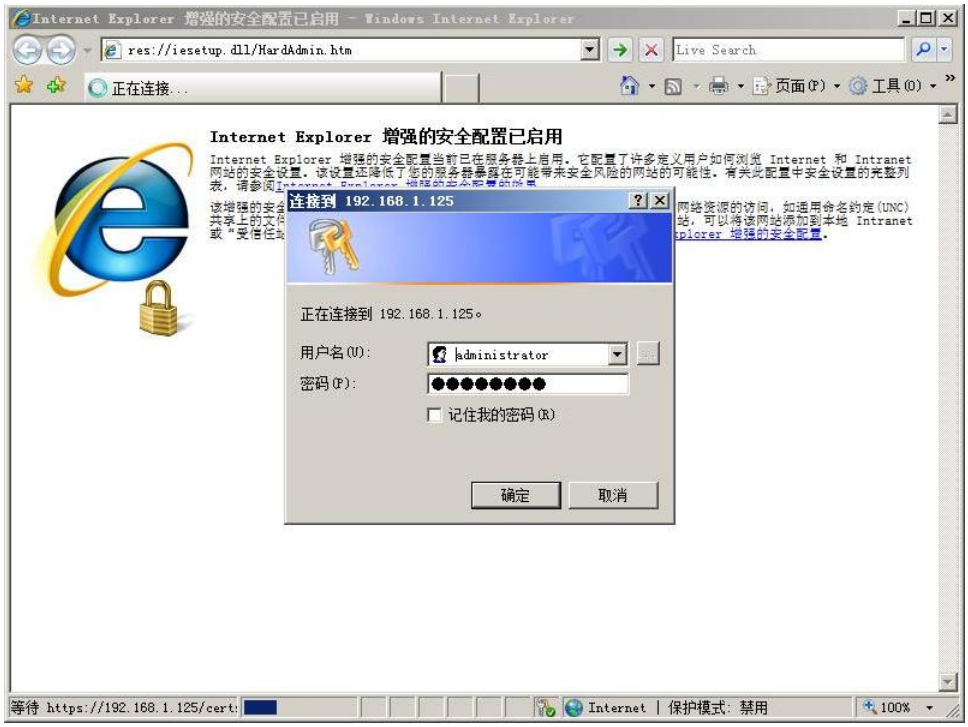

图 3-31 为 Radius Server 申请数字证书

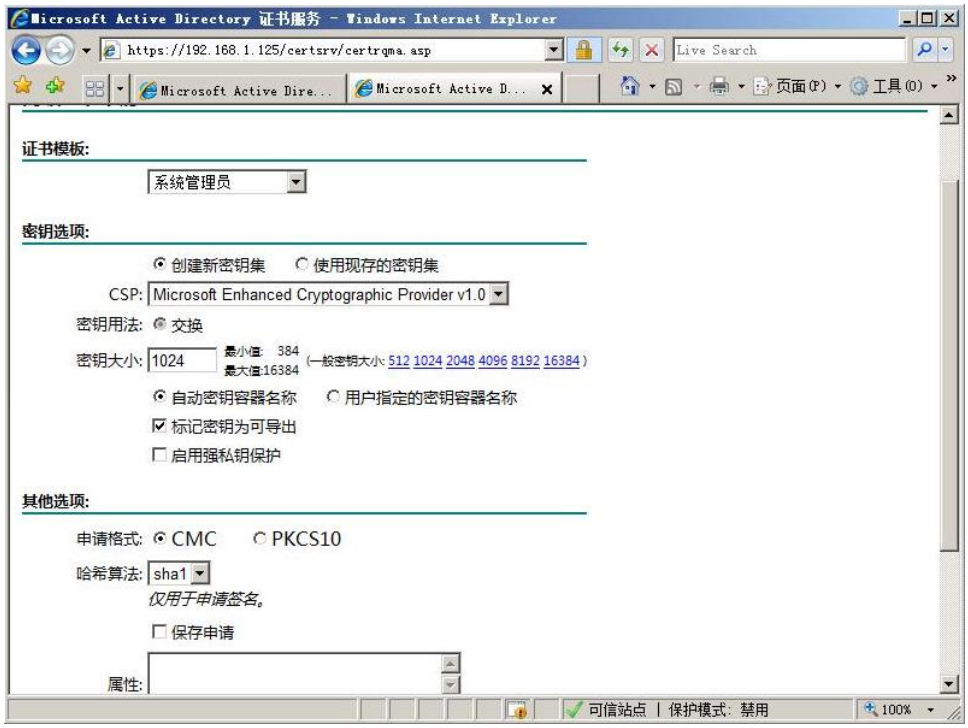

图 3-32 为 Radius Server 申请数字证书

图 3-33 为 Radius Server 申请数字证书

在图 3-32 中，证书模板选择系统管理员，勾选“标记密钥为可导出”，然后确认申请。在图 3-33 中，点击“安装此证书”，将数字证书安装到本机中。

3.4 网络策略配置

网络策略设置与 2.3 章中的设置基本相同。唯一区别如下图。将图 2-45 的 MD5-Challenge 更改为 PEAP 方式。

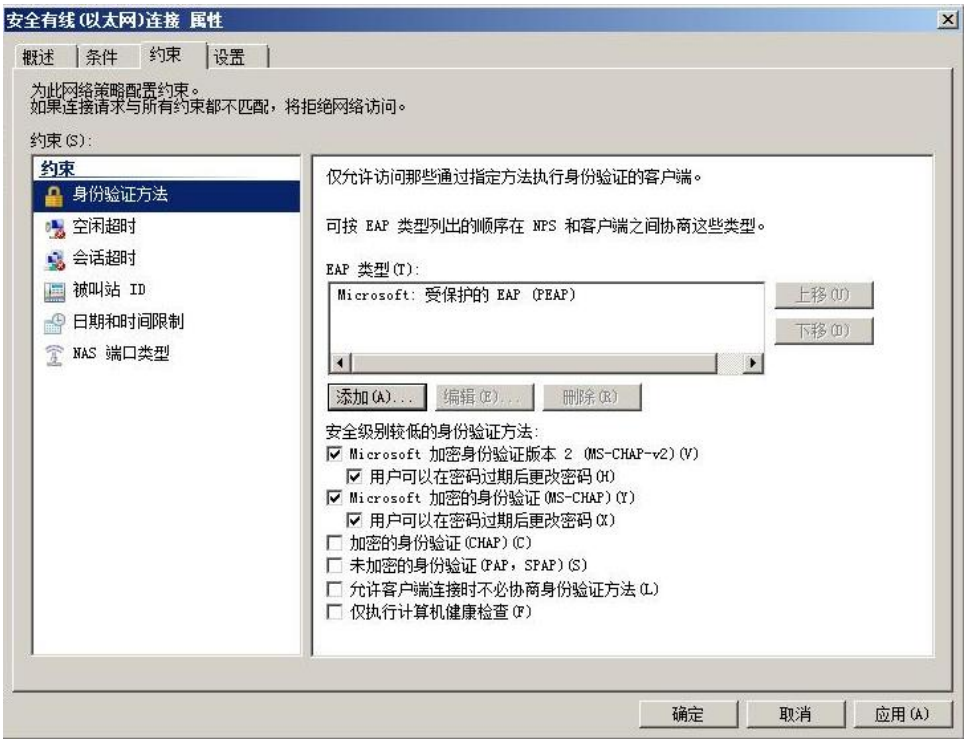

图 3-34 网络策略设置

3.5 客户端配置

本节介绍客户端电脑的配置方式，交换机配置方式与第二章相同，不再赘述。首先将 CA 包含公钥的根证书下载下来。在图 3-35 中，点击“下载 CA 证书，证书链或 CRL”。

然后将下载的证书导入客户端电脑，双击 CA 证书导入，如图 3-36。

图 3-35 下载 CA 根证书

图 3-36 安装 CA 证书到客户端电脑

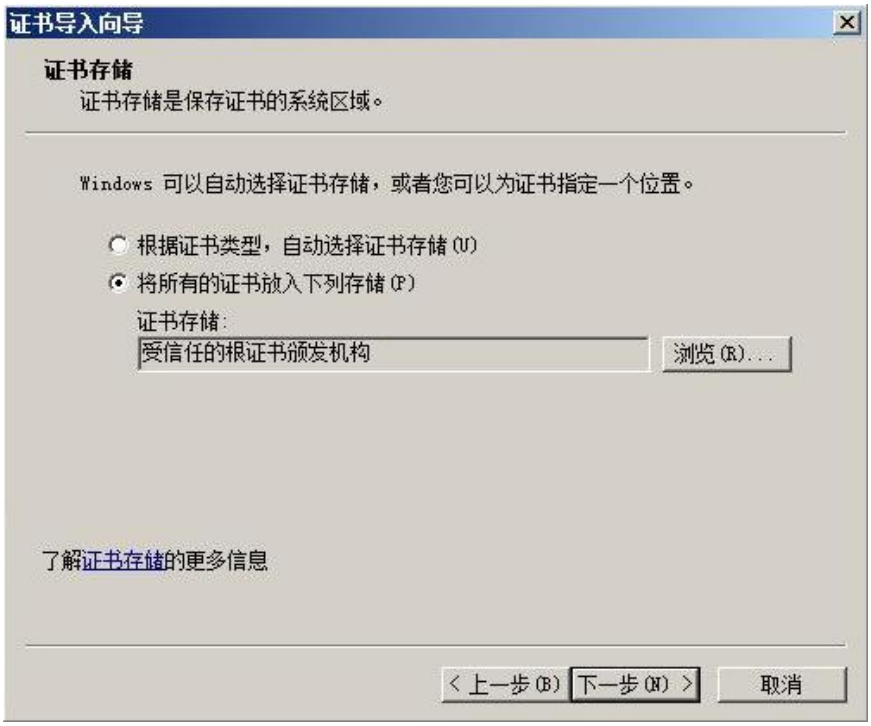

图 3-37 安装 CA 证书到客户端电脑

在图 3-37 中，要选择 CA 证书的安装位置，这里选择“受信任的根证书颁发机构”。

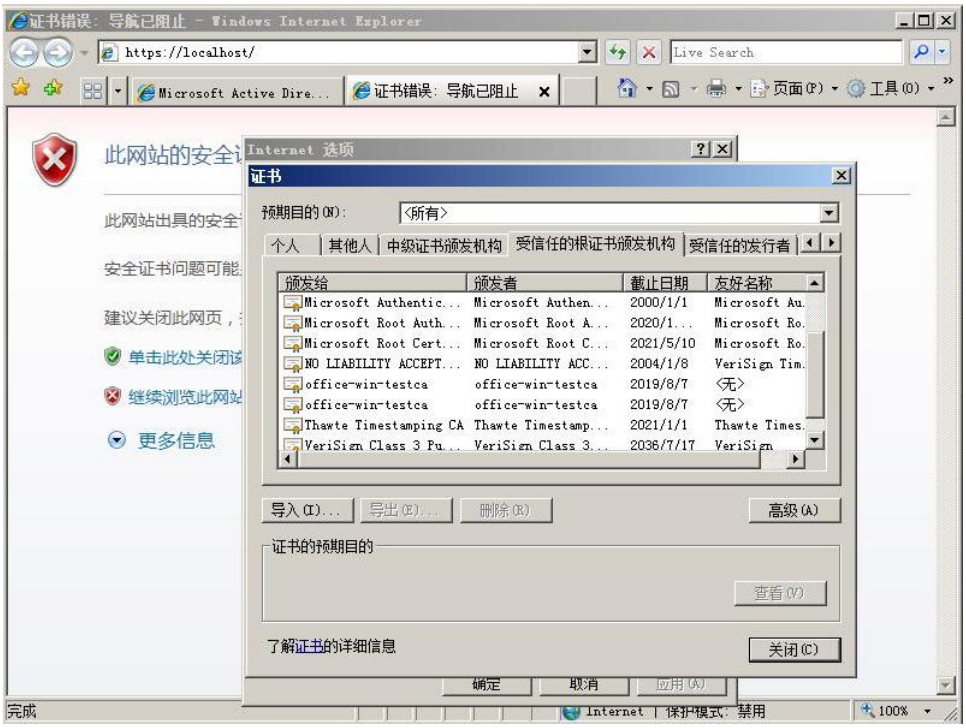

图 3-38 根证书颁发机构

在 IE 浏览器中选择工具菜单——内容页面，点击“证书”按钮打开如图 3-38 的界面。确认刚才创建的根证书颁发机构“ office-win-testca”在受信任的根证书颁发机构中。

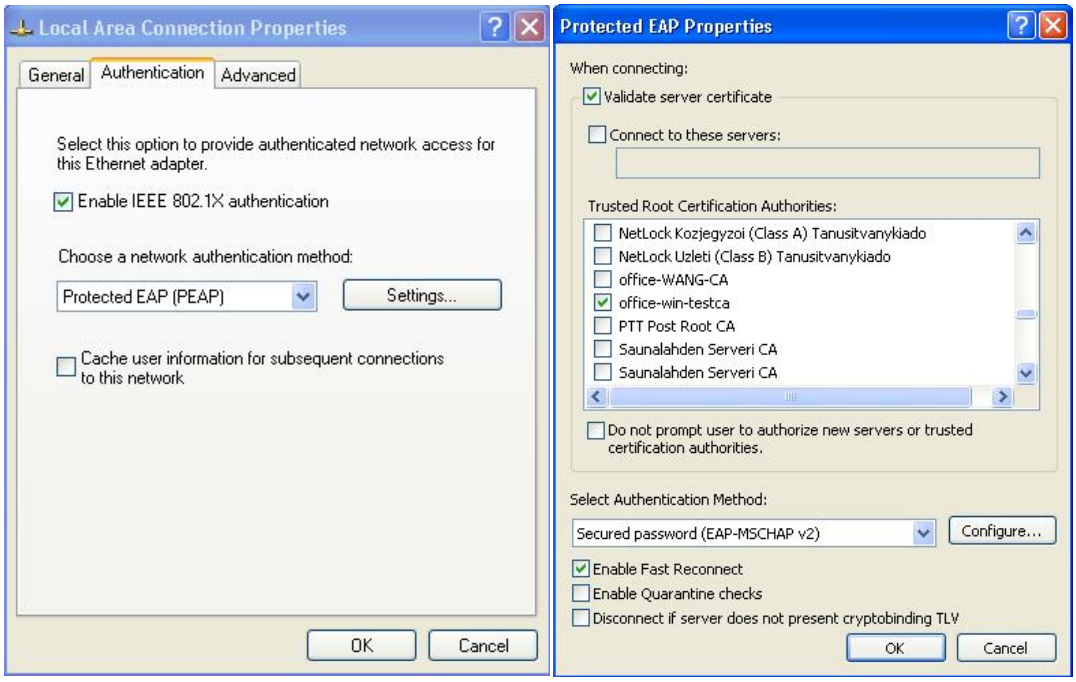

图 3-39 客户端本地连接设置

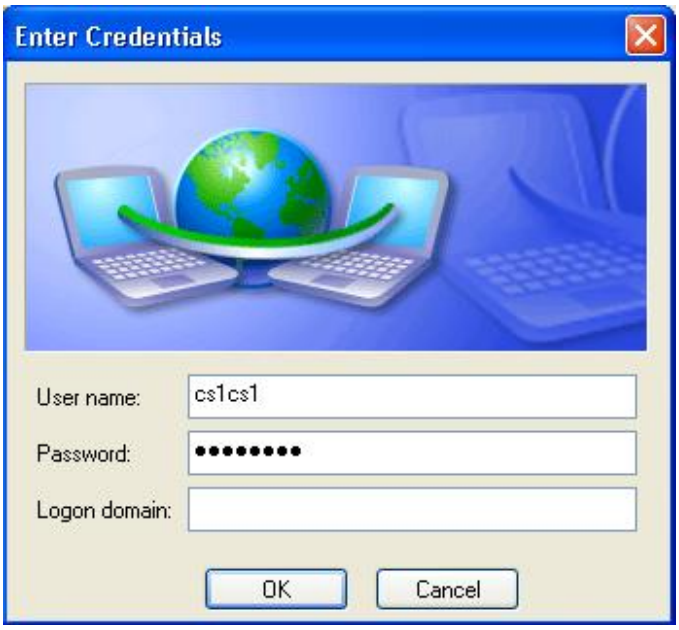

图 3-40 客户端本地连接设置

打开客户端电脑的本地连接，在 Authentication 页面中勾选“ Enable IEEE 802.1X authentication”。网络认证方式选择“ Protected EAP (PEAP)。点击设置按钮，在信任的根

证书颁发机构选择“ office-win-testca”。点击确认后电脑右下角的本地连接会提示需要输入更多信息，点击后输入用户名和密码，如图 3-40。

在未认证时，本地连接显示问号，客户端无法通过交换机的 11.2 端口连接到网络。认证通过后显示连接建立，客户端可以通过 11.2 端口 Ping 通网络上的任意设备。

4 EAP_TLS 认证方式配置

4.1 申请用户证书

使用 EAP_TLS 认证方式前半部分配置与 PEAP 方式相同，在此不再赘述。不同的是使用 EAP_TLS 方式需要给客户端也申请一个数字证书。前面已经配置好了 CA 服务器，并且申请了 Radius Server 的数字证书，下面介绍如何申请客户端的数字证书。如下图 3-41 所示，在 IE 浏览器中输入 Radius Server 的 IP 地址“ https://192.168.1.125/certsrv”，然后在弹出的对话框中输入用户名密码。注意这次需要使用用户名“ cs1cs1”申请数字证书。使用其它的用户名申请的数字证书在后面是无法通过认证的。

图 3-41 申请客户端证书

图 3-42 申请客户端证书

在图 3-42 的界面中点击“用户证书”申请。申请完毕后会提示证书安装。如果申请证书的电脑就是客户端电脑，直接点击安装证书即可。否则，需要将证书导出后，然后导入到客户端电脑。导出及导入方式如下。

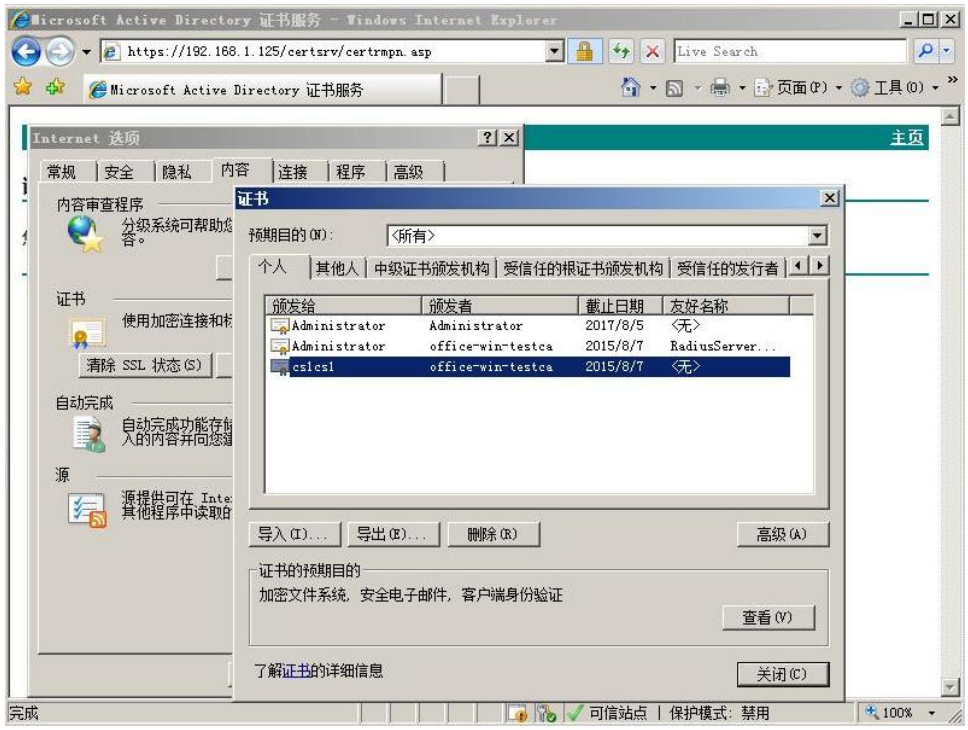

图 3-43 导出“ cs1cs1”用户证书

在 IE 浏览器中选择工具菜单——内容页面，点击“证书”按钮打开如图 3-43 的界面。在“个人”里面找到“ cs1cs1”证书，点击导出按钮将证书导出。如下图 3-44，导出证书时必须勾选“是，导出私钥”。

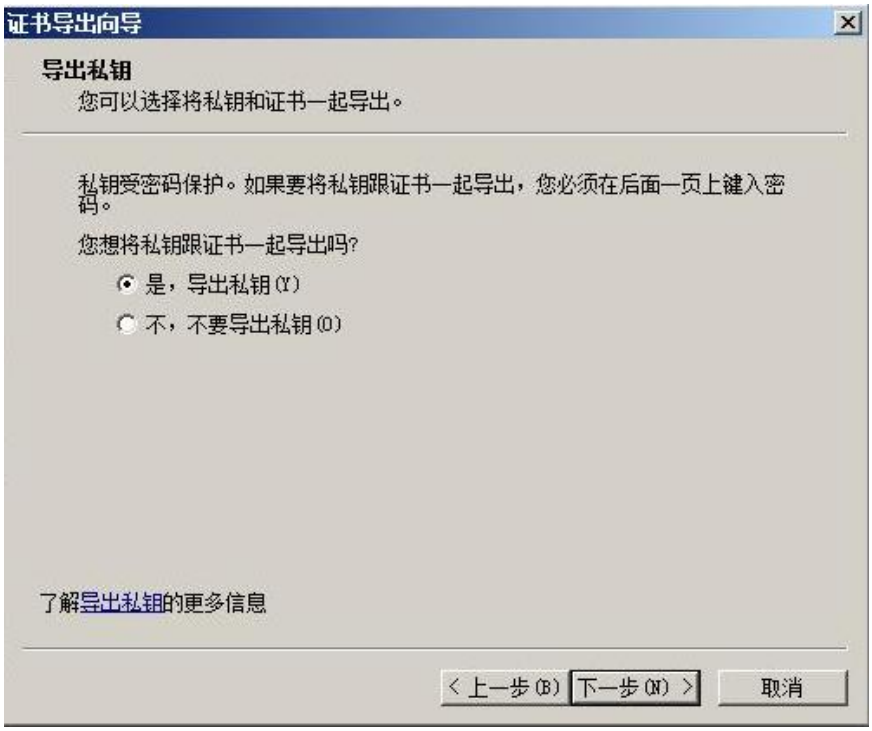

图 3-44 导出“ cs1cs1”用户证书

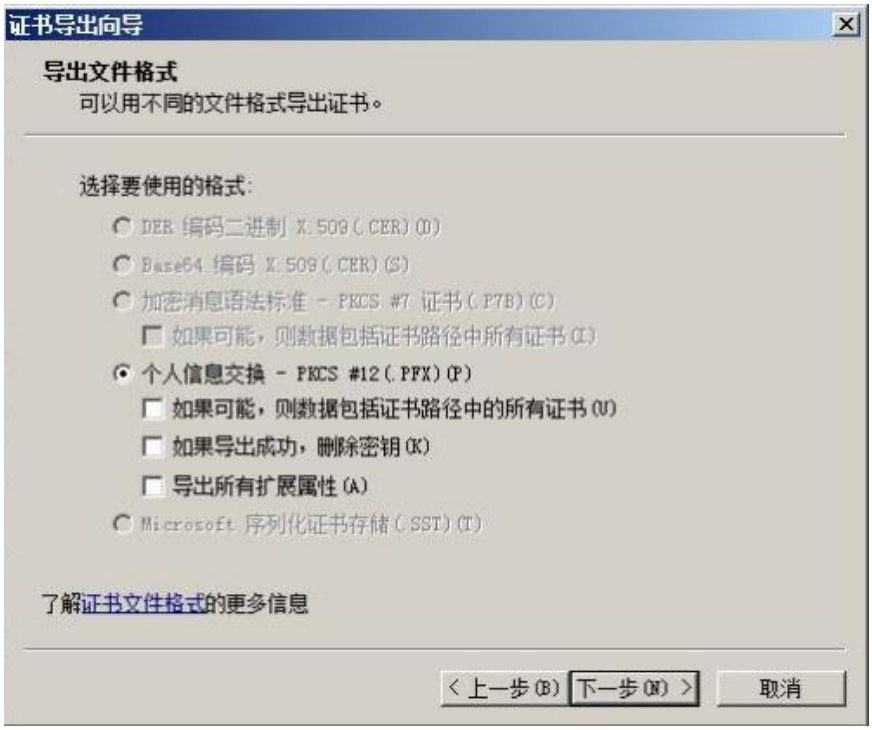

图 3-45 导出“ cs1cs1”用户证书

图 3-46 导出“ cs1cs1”用户证书

图 3-47 导出“ cs1cs1”用户证书

如图 3-46，导出时提示输入密码保护私钥，该处设置的密码在证书导入时需要使用。在图 3-47 中，提示证书导出保存的位置。

证书导出成功后，将证书拷贝到客户端电脑，双击证书，按照提示将证书导入客户端电脑。

4.2 Radius Server 设置

使用 EAP_TLS Radius Server 设置基本与 PEAP 方式相同。唯一不同的是如下步骤。在 PEAP 设置的 3-34 网络策略设置步骤中，EAP 类型更改为“ Microsoft 智能卡或其它证书”。

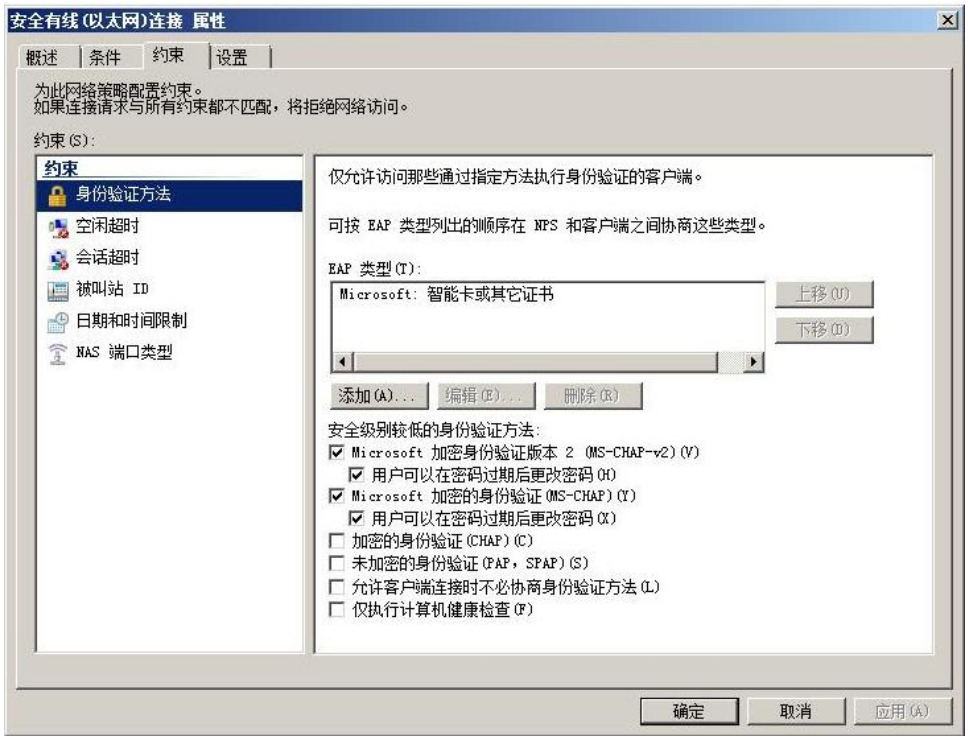

图 3-48 EAP_TLS 网络策略设置

4.3 客户端设置

首先需要将 CA 的证书导出，然后导入到客户端中。具体步骤参考图 3-35 到图 3-38。然后导入用户“ cs1cs1”的证书，如 4.1 章步骤。

在本地连接中，认证页面中勾选“使能 802.1x 认证”。认证方式选择“智能卡或其它证书”。点击设置按钮，在信任的根证书颁发机构选择“ office-win-testca”。点击确认后电脑右下角的本地连接会提示需要输入更多信息，然后弹出如图 3-50 所示的对话框。选择刚才导入的用户证书“ cs1cs1@office.siemens.com”，提示连接建立成功。

在未认证时，本地连接显示问号，客户端无法通过交换机的 11.2 端口连接到网络。认证通过后显示连接建立，客户端可以通过 11.2 端口 Ping 通网络上的任意设备。

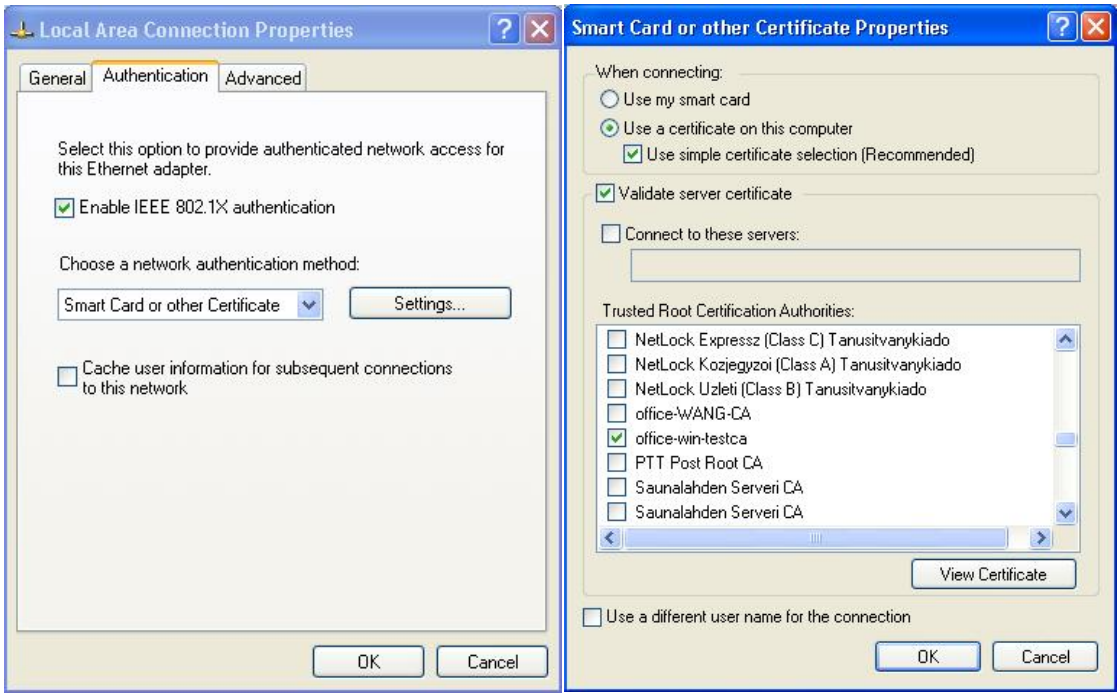

图 3-49 本地连接设置

图 3-50 选择用户证书