

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

Copyright © Siemens AG Copyright year All rights reserved 目录

1	3
1.1 802.1X 介绍	3
1.2 EAP 认证方式	4
1.2.1 EAP_MD5 认证方式	5
1.2.2 PEAP 认证方式	6
1.2.3 EAP_TLS 认证方式	9
1.3 硬件配置	10
2 EAP_ MD5 认证方式配置	11
2.1 配置域服务	11
2.2 配置组策略	23
2.3 配置用户组	26
2.4 安装并配置网络策略和访问服务	30
2.5 配置交换机	38
2.6 客户端电脑设置	39
3 PEAP 认证方式配置	41
3.1 安装 CA 服务器	41
3.2 配置 CA 服务器	49
3.3 为 Radius Server 申请管理员证书	57
3.4 网络策略配置	59
3.5 客户端配置	59
4 EAP_TLS 认证方式配置	63
4.1 申请用户证书	63
4.2 Radius Server 设置	67
4.3 客户端设置	67

Copyright © Siemens AG Copyright year All rights reserved

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 Radi us 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:

Copyright © Siemens AG Copyright year All rights reserved

- 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。
- 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 Radi us 访问请求报文,转发给验证服务器。
- 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-I ogoff 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

Copyright © Siemens AG Copyright year All rights reserved







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 Radi us Server。

5

- 3. Radi us 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。
- 申请者将用户名和密码和 Radi us 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 Radi us Server。
- 5. Radi us 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:

- 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。
- 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。



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。
- 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。
- 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

Copyright © Siemens AG Copyright year All rights reserved



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。
- 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。
- 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。

昆 服务器管理器		
文件(F) 操作(A) 查看(V) 帮助	h 00	
🗢 🔿 🙍 🗊 🚺		
■ 服务器管理器 (MIN-9GXMEZZXLQ ● 角色 功能 回 前 功能 ■ 適断 配置 ● 10 10 10 10 10 10 10 10 10 10 10 10 10	角色	
土 🔚 1子頃	○角色摘要	👔 角色摘要帮助
	⑥角色:已安装 0 (共 16)	■ 添加角色 ■ 删除角色
•	① 上次剔新时间: 2014/8/6 15:13:39 配置刷新	

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"。

一方方	LOF VALUE 44						-
₩7%							
如果网络	络支持此功 斜网络系统	能,则可以 管理员处系	V获取自动 获得适当的	指派的 IP 设	IP 设 置。	置。否则	Ŋ,
〇自	动获得 IP	地址(0)					
_● 使	用下面的 I	P 地址(S)):				
IP Ħ): 近(1):		19	92 .16	8.1	. 125	
子网	掩码(V):		25	55. <u></u> ⊉5	5.255	. 0	
默认	网关(0):						
0.0	24035E Date	00 \$ 98.44	alit ma				
_● 使	明天雨的 10	MS 服务器	። የተኛው በ (E) :	-			
首选	DNS 服务器	\$(P):		1.	-		
备用	DNS 服务器	€(A):	i i	4	1		
						高级 (V)
				1	772-2-	-	and so to

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。

-	/1000 MT Network C	onnection
比连接使用下列项目	0):	配置 (C)
☑ 県Microsoft	网络客户端	
☑ 晨QoS 剱塘巴 ☑ 具Microsoft	计测程序 网络的文件和打印机:	<u>井</u> 豆
🗹 🚣 Internet 抣	ې议版本 6 (TCP/IP√	3)
🗹 🔺 Internet 抣	♪议版本 4 (TCP/IPw	4)
☑ → 链路层拓扑	发现映射器 I/O 驱动	1)程序
🗹 🚣 Link-Layer	Topology Discover	y Kesponder
安準(約) [卸載(0)	属性(R)
244 4.1.1		
		1.41.3637

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。

添加角色向导		X
选择服务器角色		
开始之前 服务器角色 Active Directory 域服务 确认 进度 结果	 选择要安装在此服务器上的一个或多个角色。 角色(R): Active Directory Rights Management Services Active Directory 联合身份验证服务 Active Directory 短期务 Active Directory 短期务 Active Directory 近形服务 DNCP 服务器 DDDI 服务 Web 服务器(IIS) Windows 部署服务 位真服务器 打印服务 文件服务 网络策略和访问服务 文件服务器 这件服务器 经端服务 	描述: Active Directory 技服务(AD DS) 存储有关网络上对象的信息并使此 信息可用于用户和网络管理员。AD DS 使用填控者脑窗间给用户授予通 过一个登录过程访问网络上任何所 允许资源的权限。
	有关服务器角色的详细信息	
	<u>〈上一歩 @) 下一</u>	步 (X) > 安装 (I) 取消

图 2-5 安装域服务

添加角色向导	×
Active I	Directory 域服务
开始之前 服务器角色 Active Directory 域服务 确认 进度 结果	 Active Directory 域服务(AD DS)存储有关网络上的用户、计算机和其他设备的信息。AD DS 有助于管理员安全地管理该信息,并有助于用户间的资源进事和协作。自用目录的应用程序 你如如 Microsoft Dxchange Server)和其他 Windows 服务器技术(例如组集略)也需要 AD DS. ① 都要有助于确保在某台服务器中断的情况下用户仍然可以登录到网络,请至少力域安装两个域控制器。 ① 和 DS 要求将 DMS 服务器安装在网络上。如果未安装 DMS,系统会提示您在该服务器上安装 DMS 服务器角色。 ① 支援 AD DS 之后,使用 Active Directory 域服务安装向导 (deprome.exe)使服务器成为全功能域控制器。 ① 安装 AD DS 之后,使用 Active Directory 域服务安装向导 (deprome.exe)使服务器成为全功能域控制器。 ① 支援 AD DS 之后,使用 Active Directory 域服务安装向导 (deprome.exe)使服务器成为全功能域控制器。 ① DS 整扰 安基 AD DS 简优
	<上一步 (P) 下一步 (R) > 安装 (I) 取消

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。

添加角色向导	<u>×</u>
确认安装选择	
开始之前 服务器角色 Active Directory 域服务	若要安装以下角色、角色服务或功能,请单击"安装"。 ① 2 条信息性消息显示如下
捕队	
结果	● Active Directory 域服务安装向导(dcpromo.exe)使服务器成为全 ① 支装 AD US 之后,使用 Active Directory 域服务安装向导(dcpromo.exe)使服务器成为全
	<u>打印、保存或通过电子邮件发送此信息</u>

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。

■ Active Directory 域服务安装向导	×
命名林根域 林中的第一个域是林根域。其名称也是该林的名称。	
键入新目录林根级域的完全限定的域名 (FQDN)。	
office.siemens.com	
β9134∐. corp. contoso. com	
<u>〈上一步 (8)</u> 下一步 (8)	>

图 2-12 域服务配置向导



图 2-13 域服务配置向导

Active Directory 域服务安装向导	<u>×</u>
其他域控制器选项	
为此域控制器选择其他选项。	
▼ DNS 服务器 (D)	
□ 只读域控制器 (RODC) (R)	
其他信息 (A):	
林中的第一个域控制器必须是全局编录服务	器且不能是 RODC。
建议您将 DNS 服务器服务安装在第一个域	空制器上。
	<u> </u>
有关其他城控制器洗项的详细信息	
<u></u>	

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"。



具他或控制器达坝	
为此域控制器选择其他选项	Q .
☑ DNS 服务器 (D)	
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	R)
无法创建该 DNS 域或者它未运行 结构集成,应该 以确保来自域。 否则,不需要执 是否要继续?	服务器的委派,因为无法找到有权威的父区 Windows DNS 服务器。如果您要与现有 DNS 在父区域中手动创建该 DNS 服务器的委派, ffice.siemens.com 以外的可靠名称解析。 行任何操作。
	是(1) 否(1)

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。

为获得更好的性能和可恢复性,请将数据库和日志	志文件存储在不同的卷上。
数据库文件夹 (0):	
C:\Windows\NTDS	浏览(R)
日志文件文件夹 (L):	
C:\Windows\NTDS	浏览(0)
SYSVOL 文件夹(S):	
C:\Windows\SYSVOL	浏览(W)
有关 <u>放罟 Active Directory 域服务文件</u> 的详细信	記

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。

Copyright © Siemens AG Copyright year All rights reserved

Active Directory 域服务	务安装向导	2
日來服労 だ 原模式的 Admi	inistrator 器的	
目录服务还原模式 Admi	nistrator 帐户不同于域 Administrator 帐户。	
为 Administrator 帐户 制器时使用该帐户。我们	分配一个密码,将在以目录服务还原模式启动此域控]建议您选择一个强密码。	
密码(P):	•••••	
确认密码(C):		
关于且录服务还原模式密	四日的详细信息	
	〈上―歩 03) 下―歩 03) > 取	则消

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。

要	
检查您的选择 (R):	
将该服务器配置为新林中的第一个 Active Directory 域控制器。	-
新域名为 office.siemens.com。这也是新林的名称。	
域的 NetBIOS 名称为 OFFICE	
林功能级别: Windows Server 2008	
域功能级别: Windows Server 2008	
站点: Default-First-Site-Name	
其他选项:	-
」 要更改选项,单击"上一步"。要开始操作,单击"下一步"。	
可以格这些设置导出到一个应答文件中以用于其他无人 参与操作。 有关使用应答文件的详细信息	e)
	Tin Sile

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

Copyright © Siemens AG Copyright year All rights reserved 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

	助 (H)		
Þ 🔿 🔰 🖬 🗶 🗐 😼 📗	? 🖬		
上 二 上 二 上 二 <th二< th=""> 二 <th二< th=""> <th二< th=""></th二<></th二<></th二<>	了 面 家码必须符合复杂性要求 密码长度最小值 密码最近使用期限 密码最长使用期限 强密码最长使用期限 强 强制密码历史 用可还原的加密未储存密码	第略设置 已启用 7 个字符 1 天 42 天 24 个记住的密码 已启用	
	1		

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"。

🗄 🍶 Rasl2tp	-	名称	类型	数据
RasMan Prove Provention Protocols Provention Protocols Protocol	-	 (計込) RolesSupported InvokePasswordDialog InvokeUsernameDialog FriendLyName Path 	REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_EXPAND_SZ	(数值未设置) 0x00000000 (10) 0x00000001 (1) 0x00000001 (1) MD5-Challenge %SystemRoot%\System32\Raschap.dl

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:

- Copyright © Siemens AG Copyright year All rights reserved
- 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

🗧 🏟 🖄 📅 🚺 🖬 🙆 📾	» 🛛 🖬 🔧	2 🔁 🍞 🔁 🕯	g		
Active Directory 用户和计算机 Active Directory 用户和计算机 ● 【保存的查询 ● Diffice siemens.com ● Diffice Siemens.com ● Domain Controllers ● Domain Controllers ● ForeignSecurityPrincip ● Users	23% Administr Allowed R Cert Publ Denied RD Domain Co Domain Ad Domain Co Domain Gu Domain Co Domain Gu Domain Co Bomain Co Benterpris Group Poll RAS and I Schema Ad Swang	类型 用安安安安安安安安安安安安安安安安安安安安安安安安安安安安安安安安安安安安	□ 描述 □ 這理计算机(d或)的内置 允许将此组中成员的密 此组的成员被介许发布 不允许将此组中成员的 DIS Administrators 组 允许替其他客户端(如 指定的域管理员 加入到域中的所有工作 域中所有来宾 所有域用户 企业的指定系统管理员 该组的的成员全企业中的 这个组中的成员是企业中的 这个组中的服务器可以 此组中的服务器可以 此组中的服务器理员 梁构的指定系统管理员	委派控制(0) 查找(1) 新建(0) 所有任务(0) 导出列表(1) 查看(V) 排列图标(1) 对济图标(1) 对济图标(2)	计算机 联系人 组 InetOrgPer: MSM0 队列易 打印机 用户 共享文件夹
				属性 (R) 帮助 (H)	

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。

0		
姓(L):	cs1	
名(17):	cs1	英文缩写(I):
姓名(A):	cslcsl	
用户登录名(V)	:	
cs1cs1		@office.siemens.com 💌
用户登录名(Wi	ndows 2000 以	前版本)(W):
OFFICE\		cs1cs1

图 2-26 新建用户

密码(P):	•••••
确认密码(C):	•••••
□ 用户下次登录时	须更改密码(M)
□ 用户不能更改密	码(5)
□ 密码永不过期(₩)
「 帐户已禁用 (0)	

图 2-27 新建用户

在图 2-27 中,设置新用户的用户名和密码。

建对象 - 用户	
💧 创建于: office.siemens.com/Vsers	
您单击"完成"后,下列对象将被创建:	
全名: cslcsl	<u>_</u>
用户登录名: cslcsl@office.siemens.com	
	Ŧ
	T

图 2-28 新建用户

	e. Siemens. comy users
组名(A):	
CS	
组名(Windows 2000 以前)	版本)(W):
<u>IS</u>	
组作用域	───────────────
C 本地域(0)	○ 安全组(S)
● 全局(G)	○ 通讯组 @)
0 3 m an	

Copyright © Siemens AG Copyright year All rights reserved

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"。

名称	Active Directory 域服务文件夹	-
	选择用户、联系人、计算机或组	
	防律此対象突型(S): 開户、组 或 其他対象	_ 对象类型(0).
	查找位置 (P):	
	office.siemens.com	查找范围(L).
	输入对象名称来选择(<u>示例</u>)(E):	检查名称(C
	高级 (A) 确定	

图 2-30 将用户加入用户组

28

AG Copyright year	All rights reserved
Å	P
	AG Copyright year

· 排用尸、联系	人、计具机或组	and the second		?
选择此对象类型	(S):			
用户、组或其	其他对象			对象类型(0)
查找范围(F):				
office.siemen	s.com		Į.	位置(L)
一般性查询				
名称(A):	起始为 💌			列(C)
描述の):	起始为 🕑 「		2	立即查找 ()()
┏ 禁用的帐	户(6)			停止(T)
□ 不过期密	码()()			
■ 不过期密 自上次登录局	码α) 論天数α): 📘	<u>×</u>		97
□ 不过期密 自上次登录局	码 α) 諭)天数 α):	<u>×</u>	ā;	デジ 定
□ 不过期密 自上次登录局 搜索结果 (U): 3称 (RDN)	ு(ᡘ) 前天数 (ᡘ):		确	
□ 不过期密 自上次登录后 設案结果(U): 称 (RDN) Administr	ு(ᡘ) 諭)天数(ᡘ):	✓ ✓<	确: 在文件夹中 office.siem	デジ 定取消
□ 不过期密 自上次登录后 搜索结果(U): 称 (RDN) Administr CS	ுα) 泊天数 α):		确: 在文件夹中 office.siem office.siem	
□ 不过期密 自上次登录后 豊素结果(U): 森(RDN) Administr CS cs1cs1	码 α) 渝的天数 α): Γ 电子邮件地址		确: 在文件夹中 office.siem office.siem	
□ 不过期密 自上次登录后 製素结果(U): 称(RDN) Administr CS csicsi DnsUpdate	ுα) 渝庆数 α):	▲ 描述 管理计算机(允许替其他	确 在文件夹中 office.siem office.siem office.siem	
□ 不过期密 自上次登录后 搜索结果(U): 称(RDN) Administr CS csicsi DnsUpdate Domain Ad	码 α) 渝庆数 α): [电子邮件地址	✓ ✓ ✓ ✓ 描述 管理计算机(允许替其他 指定的域管理员	确 在文件夹中 office.siem office.siem office.siem office.siem	<u>定</u> 取消 定取消
□ 不过期密 自上次登录后 豊素结果(U): 森(RDN) Administr CS cslcsl DnsUpdate Domain Ad Domain Co	ு α) 部)天数 α):	」 描述 管理计算机(允许替其他 指定的域管理员 加入到域中	确 在文件夹中 office.siem office.siem office.siem office.siem office.siem	
□ 不过期密 自上次登录后 搜索结果(U): 3杯 (RDN) Administr CS cslcsl DonsUpdate Domain Ad Domain Co	码 α) 渝)天数 α): Γ □ 电子邮件地址	道 描述 管理计算机(行许替其他 指定的域管理员 加入到域中 域中所有域	确 在文件夹中 office.siem office.siem office.siem office.siem office.siem office.siem	定 取消 定 取消
□ 不过期密 自上次登录后 也上次登录后 在 2 3 7 3 7 3 7 3 7 3 7 3 7 3 7 3 7 3	码 α) 渝 天 数 α): [] 电子邮件地址	 描述 管理计算机(允许替其他 指定的域管理员 加入到域中 域中所有域 域的所有来宾 	确 在文件夹中 office.siem office.siem office.siem office.siem office.siem office.siem office.siem	定 取消 定 取消
T 不过期密 自上次登录后 也上次登录后 化TDN Administr CS CS CSICSI DonsUpdate Domain Ad Domain Co Domain Co Domain Co Domain Co	码 α) 渝 天 数 α): [] 电子邮件地址	描述 管理计算机(管理计算机(指定的域管理员 加入到域中 域中所有域 域的所有来宾 所有域用户	确: 在文件夹中 office.siem office.siem office.siem office.siem office.siem office.siem office.siem office.siem	

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"。

1212	Active Directory 域服务文件夹
💑 cslesl	office.siemens.com/Users

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

开始之前 服务器角色	选择要安装在此服务器上的一个或多个角色。 角色 (B.):	描述:
网络第略和访问服务 角色服务 角认 生度 書果	Active Directory Rights Management Services Active Directory 経合局份給证服务 Active Directory 经型目录服务 Active Directory 证书服务 DMCP 服务器 ① DMS 服务器 ① DMS 服务器 ① MSA ● TID MSA ● TID MSA ● TID MSA ● DI MER ● DI MER ● DI MERA ● Sime Mark ● Sime Mark ● Sime Mark ● MSA ● MARA	四紹金館總估110周照54種4的貨幣時 服务器 (005) 設備和加定程访问、健 康注册颁发机构 (06A)和主机凭据授 权协议(16AF),这些将有助于应给 的健康和安全。
	有关服务器角色的详细信息。	

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

添加角色向导		×
选择角色服务		
开始之前 服务器角色 网络脊髓和访问服务 角色服务 确认 进度 结果	选择为 网络策略和访问服务 安装的角色服务: 角色服务 (8): ● 留容管照图整整 ● 路由和远程访问服务 ● 近程访问服务 ● 路由 ● 健康注册机构 ● 主机凭据授权协议	描述: 四條鎖酸脂肪含器(UFS)分许的糖和增强组织适图的网络访问範疇,以用 于客户端健康、这境清水验证和主 接请求授权。使用 NFS,近可以部 署网络访问保护(NR2),即一个客户 端健康策略创建、加强和修正的技 木。
	<上一步(P) 下·	一步 (M) 〉 安装 (I) 取消

图 2-35 安装网络策略和访问服务

安装结果	
开始之前 服务器角色 网络策略和访问服务 角色服务 确认 进度 结果	 已成功安装以下角色、角色服务或功能: ▲ 1 警告, 1 条信息性消息显示如下 ● 未留用 ¥indows 自动更新。若要安装最新更新, 请使用"控制面板"中的 ¥indows Update ● 网络策略句访问服务 ④ 网络策略句访问服务 ④ 安装成下角色服务: 网络策略局务器 ④ 您 安装成为 日安装迟下角色服务: ● 加速 计算机中的的写题: ● 加速 计算机分离管理器或单击"开始"、"管理工具"、"网络策略服务器"。

Copyright © Siemens AG Copyright year All rights reserved

图 2-36 安装网络策略和访问服务

参网络策略服务器			
文件(F) 操作(A) 查看(V) 非	調助 (H)		
 ▶ NFS (本地) ▶ ■ RADIUS 客户端和服务器 ● ● 第略 ● ● 网络访问保护 ● 记帐 	入门 使用网络策略服务器(NPS), 验证和连接请求授权的网络	可以创建和强制实施用于整个组织范围内的客户端健康 访问策略。	₹、连接请求身份
	标准配置		-
	从列表中选择一种配置方案,然所	后单击下面的链接打开方案向导。	
	用于 802.1X 无线或有线连接的	RADIUS 服务器	-
	用于 802.1X 无线或有线连接 将 NPS 配置为 802.1X 连接的 RAI 换机(也称为 RADIUS 客户端版拉	的 RADIUS 服务器 DIUS 服务器时,创建网络策略可以使 NPS 从无线访问。 接执行身份验证和授权。	氣和身份验证交
	▶ 配置 802.1X		
	高级配置		

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"。

32

冒责 802.1X	Interfactor and the second			
	选择 802.1X 连接类	型		
802.1X 连接 〇 安全无线) 当您在网 出的连接)	內类型: [接 (5) [上部署 802.1% 无线访问点时, 求。	NPS 可以验证和授权	2通过该访问点连接的无线客	户端
 安全有线 如果您在 Ethernet 	以太网)连接(W) 骆中部署 802.1X 身份验证交拔 客户端发出的连接请求。	與机,NPS 就可以验证	和授权通过这些交换机连接	的
名称:	田作使田该向导创建的每个笑略	夕称的——部分。你可!	以使田野讨文木,也可以修	歩つり
此款认义争彻 。	用作使用该问等创建的母个束畸	名利的一部方。	以使用默认义争,也可以修	汉已
安全有线(以	(1941)连接			
	E-	-步(2) 下一步(0)) 完成 (7) 1 取消	Ĭ

Copyright ⊚ Siemens AG Copyright year All rights reserved

图 2-38 配置网络策略和访问服务

配置 802.1X		×
	指定 802.1X 交换机	
	请指定 802.1X 交换机或无线访问点(RADIUS 客户端)	
RADIUS 客户	端都是网络访问服务器,如身份验证交换机。RADIUS 客户端不是客户端计算机	•
若要指定 RAI	DIUS 客户端,请单击"汯加" 薪建 RADIUS 客户端	×
RADIUS 客户		
	SCALANCE	I Fi
	地址(IP 或 DNS)(D):	
	192.168.1.19 验证(V)	
	「共享机密 若要手动键入共享机密,请单击"手动"。若要自动生成共享机密,请单击 "生成"。配告 RADIUS 客户端时,使用的共享机密必须与此处输入的一 致。共享机密区分大小写。	
	 ● 手动 (0) ● 生成 (6) 共享机密 (5): 	
	•••••	
	确认共享机密 (0):	
	福定即消	

图 2-39 配置网络策略和访问服务

配 置 802.1X					×
	配置身份验证方	方法			
选择此策略的 BA	u 类型				
类型(基于访问方	5法和网络配置)(T):				
MD5-Challenge					配置(C)
		上一步(2)	下一步 (8)	完成(3)	

图 2-40 配置网络策略和访问服务

					×
选择组			Ľ	2 ×	
选择组				? ×	
选择此对象类型0	s):				
组				翅(0)	
, 查找范围(F):					
office. siemens.	com		位置	ta)	
-船性查询]					
AVITE OF 1			1	Tel (c)	
名称(A): 世	站为 🗾			911 (c)	_
描述(0): 世	动为 🔽			立即查找(N)	
┏ 禁用的帐户	L(B)			停止(T)	
□	(0x)				
	4T44 (m)			07	
日上八堂水市	的大致以升			FI	
-			 确定	取消	
搜索结果(V):					
搜索结果(U): 名称 (RDN)	描述	在文件夹中			
搜索结果(V): 名称 (RDN) Allowed R	描述 允许将此组	在文件夹中 office.siem			
搜索结果(U): 名称 (RDN) Allowed R Cert Publ	描述 允许将此组 此组的成员	在文件夹中 office.siem office.siem			
搜索结果(U): 名称 (RDN) Allowed R Cert Publ CS	描述 允许将此组 此组的成员	在文件夹中 office.siem office.siem office.siem			
搜索结果(U): 名称 (RDM) Allowed R Cert Publ CS Denied RO	描述 允许将此组 此组的成员 不允许将此	在文件夹中 office.siem office.siem office.siem office.siem			
搜索结果(U): 名称 (RDN) Allowed R Cert Publ Denied RO DnsAdmins	描述 允许将此组 此组的成员 不允许将此 DNS Adminis	在文件夹中 office.siem office.siem office.siem office.siem			1
搜索结果(U): 名称 (RDN) Allowed R Cert Fubl Denied RO DnsAdmins DnsUpdate	描述 允许将此组 此组的成员 不允许将此 DNS Adminis 允许替其他	在文件夹中 office.siem office.siem office.siem office.siem office.siem]
搜索结果(U): 名称 (RDN) Allowed R Cert Publ Denied RO DnsAdmins DnsUpdate Donain Ad	描述 允许将此组 此组的成员 不允许将此 DNS Adminis 允许替其他 指定的域管理员	在文件夹中 office.siem office.siem office.siem office.siem office.siem office.siem]
搜索结果(U): 名称 (RDN) Allowed R Cert Publ Denied RO DnsAdmins DnsUpdate Domain Ad Domain Co	描述 允许将此组 此组的成员 NS Adminis 允许替其他 指定的域管理员 加入到域中	在文件夹中 office.siem office.siem office.siem office.siem office.siem office.siem office.siem	 确定		
搜索结果(U): 名称(RDN) Allowed R Cert Publ Danied RO DnsAdmins DnsUpdate Domain Ad Domain Co	描述 允许将此组 此组的成员 不允许将此 DNS Adminis 允许替其他 指定的域管理员 加入到域中 域中所有域。2010	在文件夹中 office.siem office.siem office.siem office.siem office.siem office.siem office.siem office.siem	 确定		_]

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。

₩ 五 802.1X			×
	指定用户组 根据网络策略"访问权限"的设置,将行进行访问。	忙许或拒绝属于——个或多~	个选定组成员的用户
若要选择用户 <u>组</u> OFFICE\CS	组,请单击"添加"(0)。如果没有选择 	:任何组,则此策略将应用	∃于所有用户。

图 2-42 配置网络策略和访问服务

【1】 802.1Ⅰ					x
	配置虚拟 LA		ታ ርጎ አ/ AN a		
20	何 002.1 入音 广 %而 /	1月(2月) (15) (6)	10) VLANO		
如果您的 RAD 客户端提供 V 洛。	IUS 客户端(身份验证 LAN 信息。这样 RAD	E交换机和无线访问 IVS 客户端就可以相]点)支持 VLAN,「 限据它从 NPS 处行	则可以配置 NP 导到的指示将测	S 以向 RADIUS 流量路由到相应网
如果您不使用	VLAN 或希望稍后再	配置它们,请单击	"下一步"。		
-VLAN 配置 - 芜更向 NPS	提供组织网络的 1/7,	AN 信白、洁畄牛"	而罢" 。		
石安回 113	TERSESPORTS VI	M 信息,旧丰山	自己。	Г	配置(C)
				-	
		上一步(19)		完成()	

图 2-43 配置网络策略和访问服务

配 置 802.1X	×
正在完成新建 IEEE 802.1X 安全有线和无线连接以及 RADIUS 客户端	
您已成功创建了以下策略,并配置了以下 RADIUS 客户端。	
·若要在默认浏览器中查看配置详细信息,请单击"配置详细信息"。 ·若要更改配置,请单击"上一步"。 ·若要保存配置并关闭此向导,请单击"完成"。	
RADIUS 客户端: SCALANCE (192-168-1-19)	
连接请求策略 : 安全有线(1)大网)连接	
网络策略: 安全有线(以太网)连接	
· <mark>配置详细信息 (C)</mark> 	
上一步 (r) 下一步 (r) 完成 (r) 取消	

图 2-44 配置网络策略和访问服务



Copyright © Siemens AG Copyright year All rights reserved

图 2-45 配置网络策略和访问服务

2.5 配置交换机

SCALANCE X-400 WEB Ma	nagement (192.16			
SIEMENS			Automatic	on & Drives
Console Support	Logout		SIMA	FIC NET
Power Input CPU Status Status	Status Status Status P1 P1 P1 P2 P2 P2 P3 P3 P3 P4 P4 P4		SIMATIC NET I	ndustrial Ethernet SCALANCE X-400 192.168.1.19
2 3 4 5 6	802.1x RADIUS Configuration			
T System		_		
±	Reauth	entication		
E Agent				5
Switch	Reautientication enabled			
Ports	PADILIS Sonior	Drimany	Dackup	Ē.
🗉 🧰 Link Aggregation	RADIUS SEIVEI	Prindry	Баскир	
🖻 🔄 IEEE 802.1x	IP address:	192.168.1.125	0.0.0.0	
RADIUS Config	Destination port	1812	1812	8
Authenticator	Observed Opserved		-	
The Unicast Filter (ACL)	Shared Secret.		I	
Hand Multicast Groups	Confirm Shared Secret:			
Broadcast Mask	Maximum retransmissions:	2	2	
El Lood Limito				ni.
E Spanning Tree				
⊞ 🛄 QoS				
🗉 🧰 DHCP Relay Agent				
Loop Detection				
🗉 🧰 Statistics				
🗄 🧰 Router				

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"。

SCALANCE X-400 WEB Management (192.	16								
SIEMENS								Automation &	Drives
Console Support Logout								SIMATIC	NET
Power Input CPU Status Status Status Status F IN1 RM P1 P	us Status Status P1 P1 P1 P P2 P2 P P3 P3 P3 P P4 P4 P4 P4 10 11						SIMA	TIC NET Ind S(ustrial Ethernet CALANCE X-400 192.168.1.19
X414-3E 802.1x Auth	enticator Config	guration							
⊞ 🛅 <u>System</u>									
🖻 🧰 <u>X-400</u>		En	able Au	Ithentic	ator				
🖲 🧰 Agent	SI	lot 5	6	7	0	10	11		
E Switch		lot 1	1		J.	10.	1		
Ports	F		2				2		
	P	ont 2	2				2		
□ 🖨 IEEE 802.1x	P	lort		19 1					
RADIUS Config		on			•		-		
Authenticator									
<u>Unicast Filter (ACL)</u>									
<u>Multicast Groups</u>									
Broadcast Mask									
Fast Learning									
B Spanning Tree									

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

Copyright © Siemens AG Copyright year All rights reserved

> 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。

39



图 2-48 客户端电脑设置

Enter Credent	ials 🔀
User name:	cs1cs1
Password:	•••••
Logon domain:	
	OK Cancel

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。

开始之前 服务器角色	选择要安装在此服务器上的一个或多个角色。 角色 (R):	描述:
AD CS 角色服务 安装类型 CA 类型 私钥 加密 CA 名称 有效期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度	Active Directory Rights Management Services Active Directory 联合身份验证服务 Active Directory 经型目录服务 Active Directory 证明服务 DKDF 服务器 DKDF 服务器 OBDIF 服务器 Web 服务器 (CDSK) Windows 部署服务 合原服务器 DFMR务 OBS領職和访问服务 OH2F服务器 这件服务 应用程序服务器 终端服务	Active Directory 证书服务(AD CS)用于创建证书颁发机体和相关的 角色服务。可以使多颁发和管理在 各种应用程序中所使用的证书。

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。

添加角色向导	<u>×</u>
Active Directo	ry 证书服务简介
 开始之前 服务器角色 JD CS 角色服务 安装类型 CA 类型 私钥 加密 CA 名称 有效期 证书数据库 Web 服务器(TIS) 角色服务 确认 进度 结果 	Active Directory 证书服务(AD CS) Active Directory 证书服务(AD CS)提供证书基础结构以自用方案,如安全无线网络、虚拟专用网络、Internet 协议安全(IPSec)、网络访问保护(ADA)、加密文件系统(IPS)和智能卡曼汞。 注意事项 ① 安装证书颁发机构(CA)之后,无法更改该计算机的名称和1或设置。如果您想更改计算机名称,加入 一个证据看得该服务器升级力域控制器,请完成这些更改,然后再安装 CA。有关详细信息,请参 阅证书颁发机构命名。 打伤信息 Active Directory 证书服务概述 管理证书颁发机构命名。
	< 上一步 (P) 下一步 (N) >

图 3-2 安装证书服务

添加角色向导		×	(
选择角色服务			
开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 AU 加密 CA 类型 AU 加密 CA 名称 有效期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度 结果	选择为 Active Directory 证书服务 安裝的角色服务: 角色服务 (B): ✓ 证书颁发机构 ✓ 证书颁发机构 Web 注册 ✓ <mark>联机响应程序</mark> → 网络设备注册服务	描述: 一 <u>蘇机响向程序</u> 使客户端可以在夏杂 的网络环境中访问证书吊销检查数 据。	
	有关角色服务的详细信息		
	_<上一步 (2) 下一步	QN) >	

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。

添加角色向导	
🎼 指定 CA 类型	
 开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 私钥 加密 CA 名称 有效期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度 结果 	可以配置根 CA 和从属 CA 的组合来创建分层公钥基础结构(PECI)。根 CA 是发布其自己的自签名证书 的 CA。从属 CA接收来自其他 CA 的证书。指定您需要设置根 CA 还是从属 CA。 (* 根 CA (8) 如果您是第一次安装或您是公钥基础结构中唯一的证书颁发机构,请选择此选项。 (* 子级 CA (0) 如果您的 CA 将从公钥基础结构中更高的另一个 CA 获取其 CA 证书,请选择此选项。
	有关公钥基础结构(PIII)的详细信息
	< 上一步 (P) 【下一步 (N) > 」 安装 (□) 】 取消 】

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。

Copyright © Siemens AG Copyright year All rights reserved

^{添加角色向导} 设置私钥	
开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 私団 加密 CA 名称 有效期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度 结果	 若要生成证书并颁发给客户端,CA必须有一个私钥。指定您要新建私钥还是使用现有私钥。 (*) 新建礼钥(8) 如果您没有私钥的透明长度。若要颁发新证书,还必须选择一个哈希算法。 (*) 使用现名项问确保重新安装 CA时与先前颁发的证书的连续性。 (*) 使用现名项问确保重新安装 CA时与先前颁发的证书的连续性。 (*) 还将一个证书并使用其关联私钥(6) 加累您在化计算机上有一个现有证书,或者加累您希望导入一个证书并使用其关联私钥,请选 编试送现。 (*) 还择此计算机上的现有私钥(2) 加累您已保留末自以前安装的私钥或需要使用其他未源的私钥,请选择此选项。
	有关公钥和私钥的详细信息
	< 上一步 (P) 下一步 (P) > 安装 (I) 取消

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"。

添加角色向导		×
第 为 CA 配置加密		
开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 礼钥 加密 CA 名称 有效期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度 结果	若要新建私锅,您必须首先选择加密服务提供理念的监督的安全性,但会增加完成签名操作所需的时间。 送择加密服务提供程序(CSP)(C): 密钥字符长度(0): 医结子节长度(0): 亚目之子的这个文字。 达择此 CA 颁发的签名证书的哈希算法(0): 亚位、文字》 mad ····································	
	<u>〈上一步 (t)</u> 万一步 (t) 入 _ 安装 (t) _ 取消	

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"。

工始之前	键 \ 从田安我以识别世 CA,世安教会被添加到由该 CA 猫发的所有证书由。可分辨安教的后缀值:
77知之前 服冬哭角岛	动生成的,但可以修改。
AD CS	w ca 的从田夕我 (c)·
角色服务	office-win-testca
安装类型	可分辨名称后缀①)
CA 类型	DC=office, DC=siemens, DC=com
私钥	
加密	
CA 名称	円方辨名称的初気 (7): CN=office-win-testca,DC=office,DC=siemens,DC=com
有效期	
证书数据库	1
Web 服务器(IIS)	
角色服务	
· 编认	
) 世長	
站来	

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"。

Copyright © Siemens AG Copyright year All rights reserved

添加角色向导	
设置有效期	
 开始之前 服务器角色 AD CS 角色服务 安装类型 CA 类型 私钥 加密 CA 名称 有效期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度 结果 	会格一个证书颁发给此 CA 以保护与其他 CA 和请求证书的客户端之间的通信。CA 证书的有效期可以 基于许多因素,包括 CA 的预期目的以及为保护 CA 您已采取的安全措施。 5 年
	有关设置证书有效期的详细信息
	< 上一步 (P) 下一步 (Q) > 安装 (I) 取消

图 3-9 安装证书服务



图 3-10 安装证书服务

添加角色向导	×
Web 服务器(IIS) Teb 昭冬哭箭介(IIS)
7.42 m 服务器角色 AD CS 角色服务 安装类型 CA 类型 私钥 加密 CA 名称 有效期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度 结果	 Web 服务器是具有特定软件的计算机,这些软件使服务器可以从客户端计算机接受请求并对这些请求返回响应。%eb 服务器员有任己结 Internet、Internet 或 Bixtranet 上共享信息。%eb 服务器角色包括 Internet 信息服务 [13] 7.0.2—/ 集成了115 7.0.2 PRITA 和 Windows Communication Promotation 的统一 Web 平台。IIS 7.0 还具有安全性增强、诊断简单和委派管理的特点。 注意事项 使用 %indows 系统资源管理器 (%SRM)有助于确保等同对待 Web 服务器通信,特别是此计算机上存 在多个角色的。 Web 服务器 (IIS)角色的默认安装包括角色服务的安装,该安装使您能够使用静态内容、进行最小自定义 (00試认的文档和 MTTP 错误)、监视和记录服务器活动以反配置静态内容压缩。 其他信息 Yeb 服务器 (IIS)類述 IIS 3.0 地质、器位IIS)類述 IIS 3.0 达到 角色服务概述 IIS 4.0 的意识管理任务 YESM 题述
	<上一步 (2) 下一步 (30) >

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

确认安装选择		
开始之前 服务器角色 AD CS	若要安裝以下角色、角色服务或功能,请单击"安裝"。 <u>1</u> 1 警告,2条信息性消息显示如下	-
角色服务 安装类型 CA 类型 私钥 加密 CA 名称 有效期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度	 (1) 安装完成之后,可能需要重新启动该服务器。 ▲ Active Directory 证书服务 证书颁发机构 ④ 安装了证书颁发机构之后,将无法更改此计算机的名称和域设置。 CA 类型: 企业根 CSP: EAAM CONSTRUCT Software Key Storage Provider 哈希算法: shal 密钥长度: 2048 允许 CSP 交互操作: 已禁用 证书有效期: 2019/8/7 14:47 可分辨名称: CH=>employee CH C: Windows\system32\CertLog 证书教提库包括公置: C: Windows\system32\CertLog 证书教提本的图表表(UIS) 	
结果	 ① 查找有关 Windows 系统资源管理器 (WSRM)以及它如何帮助优化 CPU 使用情况的详细信 Web 服务器 打印、保存或通过电子邮件发送此信息 < 上一步 (P) 下一步 (0) >	

图 3-13 安装 IIS 服务



图 3-14 确认安装

添加角色向导		×
安装结果		
开始之前 服务器角色 AJ CS 角色服务 安装类型	已成功安装以下角色、角色服务或功能: ① 1 条警告消息显示如下 ③ 未自用 Windows 自动更新。若要安 来检查更新。 ④ Active Directory 证书服务	装最新更新,请使用"控制面板"中的 Windows Upde▲
CA 类型 私钥 加密 CA 名称	已安装以下角色服务: 证书颁发机构 证书颁发机构 Web 注册 联机响应程序 ② Web 服务器(IIS)	☑ 安装成功
 有双期 证书数据库 Web 服务器(IIS) 角色服务 确认 进度 结果 	已安装以下角色服务: Web 服务器 常见 HTTP 功能 静态内容 默认文档 目录浏览 HTTP 错误 HTTP 错误 HTTP 重定向 应用程序开发 ASP ISAPI 扩展	
	打印、保存或通过电子邮件发送安装报告	
	<u><</u> E-	-歩 (c) 下一歩 (c) > 关闭 (c) 取消

图 3-15 成功安装证书服务和 IIS 服务

3.2 配置 CA 服务器

Copyright © Siemens AG Copyright year All rights reserved

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。

🍃 certsrv - [证书颁发机构(本	地)]		
文件(F) 操作(A) 查看(V) 帮	助 06)		
	10 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 -		
 □ 正书颁发机构(本地) □ officerwin-testca ○ 示前近正书 ○ 颁发的证书 ○ 颁发的证书 ○ 强起的申请 ○ 正书模板 		描述 Certification Authority	

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。

😋 🖒 🥞 + WIN-9GXMEZZXLQN +		🖾 🖄 🚺
文件 (P) 视图 (V) 帮助 (H)		
连接	▲ 服冬哭证书	操作
&- [] ≥ &		导入
	使用此功能来申请和管理 Web 服务器可以对配置了 SSL 的网站使用的证书。 名称 ^ / 颁发给 / 颁发者	创建证书申请 完成证书申请
E III 网站	office-win-testca office-wi	创建域证书
		创建自签名证书
		查看 ※ 開除
		● 帮助 联机帮助

图 3-17 IIS 管理器

₩ <u> 第</u> 27 <u> 15</u> <u> 15</u>	省/市/自治区和城市/地点必须指定为正式的	名称,并且不得包含缩写
1/式。 通用名称(M):	192. 168. 1. 125	
组织(0):	SIEMENS	
组织单位(V):	SIEMENS	
成市/地点(L)	PEK	
省/市/自治区(S):	PEK	
国家/地区(R):	СИ	*

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。

选择加密服务提供到	程序 积 位长。如28	密密钥的位长决定	了证书的加密强	度。位长越大,	安全性越
短。但较大的应长。 加密服务提供程序。	可能尝摩1%性能。 (S):	,			
Microsoft RSA SC	hannel Cryptogr	raphic Provider	•		
位长(8):					
1024	1				

图 3-19 选择加密服务程序

请证书	文件名				?
为证书申词 为证书申词	青指定文件名。 青指定一个文件	此信息可以发送 非名(B):	给证书颁发机构签	名。	
C:\CAWEB					

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"。

ティンチ (ア)	(白北二)	P) 4	2-F (0)	本手のの	TERE OF	
XH (I)	新祖(E) 1	陷土((0)	宣有(V)	帮助机	
Bi	EGIN	NEW	CERTI	FICATE	REQUE	ST
IIDZD	CCAs0	CAQ	AwZTEL	.MAkGA1	UEBHMC	Q04xDDAKBgNVBAgMA1BFSzEMMAoGA1UE
BownDUE	VLMRA	wDg	YDVQQF	IDAdTSU	VNRU5T	MRAwDgYDVQQLDAdTSUVNRU5TMRYwFAYD
VQQDDA	0x0TI	uMT	Y4LjEi	MTI1MI	GfMAOG	CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC7
f1Jhr	Jd7VL	K2t1	Eo59I5	WE02uJ	cWKGvY	orwJfBe7CRms7ktZ81TGZ6Et025/qmpl
GOZaF	14Zrd	HqDI	HY9Pzo	BCVx+S	YaXGz0	xsKZNOYagxvnSS51GuJuUkF08HF5rZPq
ofjR/	5eq+D	uFH	Ge27sd	+P2G4z	kq.jQ/z	2aUnmOfsHQIDAQABoIIBvTAaBgorBgEE
YISDQ	IDMQw	WC i	YuMC42	2MDAxLi	IWWQYT	KwYBBAGCNxUUMUwwSgIBBQwiVOlOLT1H
E1FW1	DYTFF	OLm'	9mZml ·	iZS5zaŴ	VtZW5z	LmNvbQwUT0ZGSUNFXEFkbWluaXN0cmF0
SIMCO	luZXR	NZ3	IuZXhÌ	MHIGCi	SGAQQB	gicNAgIxZDBiAgEBHloATQBpAGMAcgBv
HMAbw	BmAHQ	ATA	BSAFM/	QQAgAF	MAQwBo	AGEAbgBuAGUAbAAgAEMAcgB5AHAAdABy
GeAce	BhAHA	AaAl	BDAGM/	TABOAH	TAbwB2	AGkAZABIAHIDAQAwgc8GCSaGSIb3DQEI
iGBaT	CBviA	OBgl	NVHQ8F	AFSEBA	MCBPAw	EwYDVR01BAwwCgYTKwYBBQITHAwEweAYT
oZIhv	CNAOk	PBG	SMATA	Begahk	G9mnDD	AgICALAwDgYIKoZIbycNAwQCAgCAMAsG
WCGSA	F1 Aran	BK i	AI Rola	hkoB70	MEASOM	CWY TY T 7 T AWITD BAFC MAGC CWCG SAF1 AWOB
TAURA	IImDa M	CB-	AKRaa	hbiCom	nDR-44	BaWHOAFFaOIMWIIIWaTp67mDNu9148m1
CBb		TKo	7Thurn	IVUEEBU	AD-VEA	MaBSDCFLAL and a AOUS UP 2 mole and a AOUS
Amburk	ewDei +-/V-	UND.		nger Dg	-fkbD	A++TBC: K-Ww1W0-1; -U-DOB :To -+- VKA
ONALIONA	voom_v		10000000000000000000000000000000000000	10111121	CLVDOF	AFT: 7HO:COMUM-TAU-OUD-Cli4-
VI T	IWWIII	ent	SKOUDY	гезнча	SGIDAL	4FIJCHVN9JSSAMXWWVIAHE9HFFSIIW4V
SVUGXE	лкdaw	-				
4						Þ

图 3-21 生成的证书申请文件

│■icrosoft Active Directory 征书服务 - Wind	lows Internet Ex	olorer		
🕞 📀 👻 http://192.168.1.125/certsrv/Defaul	lt. asp	💌 ++ 🗙	Live Search	P -
🚖 🍄 🏾 🏉 Microsoft Active Directory 证书服务		🔂 •	🔊 - 🖶 - 📑 页面	(8) • 🥥 工具 (0) • "
Tingan At Anting Discontants (正书职务	affi an min tant			÷5
Ricrosoft Active Directory WETHINS	oprice-win-test	a		主因
欢迎使用				
使用此网站为您的 Web 浏览器、电子邮件 Web 进行通信的用户确认您的身份、签名	‡客户端或其他积 并加密邮件,并	≧序申请证书。通 根据您申请的证─	过使用证书,您可 书类型执行其他安全	以向通过 全任务。
您也可以使用此网站下载证书颁发机构(CA 态。	4)证书、证书链	, 或证书吊销列表	(CRL),或者查看挂	圭起申请的状
有关 Active Directory 证书服务的详细信题	息 , 请参阅 <u>Acti</u>	ve Directory 证书	部服务文档.	
选择一个任务: <u>申请证书</u> 查看挂起的证书申请的状态 下载 CA 证书、证书链或 CRL				
減		🐠 🐚 🗸 可信站点	保护模式:禁用	100% 🕈 🖉

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"。

Ølicrosoft Active Dir	ectory 证书服务 - Tindows Internet]	Explorer	<u>_ ×</u>
	. 168. 1. 125/certsrv/certrqus. asp	🗾 🍻 🗙 Live Search	P -
😭 🏟 🏾 🏉 Microsoft Act	ive Directory 证书服务	🟠 • 🗟 · 🖶 • 🗗 页面 0	P) • 🎯 工具 (0) • "
Microsoft Active Dir	cectory 证书服务 office-win-tes	otca	主页
甲項一个唯书			
选择一个证书类型: <u>用户证书</u>			
或者,提交一个 高级	证书申请。		
			v
完成		📑 🚯 🗸 可信站点 保护模式:禁用	🗮 100% 🔹 //

图 3-23 申请 WEB 服务器数字证书

GBicrosoft Active Directory 证书服务 - Windows Internet Explorer	<u>- 0 ×</u>
🚱 🕞 👻 🛃 http://192.168.1.125/certsrv/certrqad.asp 💽 🐓 🗙 Live Search	P -
😪 🏟 🏉 Microsoft Active Directory 证书服务 🎒 • 🗟 • 🖶 页面(P) • 🎯	[具(0) → "
Nicrosoft Active Directory 证书服务 office-win-testca	主页
高级证书申请	
CA的策略决定您可以申请的证书类别。单击下列选项之一来:	
创建并向此 CA 提交一个申请。	
使用 base64 编码的 CMC 或 PKCS #10 文件提交 一个证书申请, 或使用 base64 编码的 PKCS # 件续订证书申请。	<u>7文</u>
	Ŧ
」	100% - //

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。

Ølicrosoft Acti	ive Directory 证书服务 - Windows Interne	t Explorer		
🔆 💽 🗸 🙋 htt	tp://192.168.1.125/certsrv/certrqxt.asp	- +, >	Live Search	P -
🙀 🏟 🏾 🏉 Micro	soft Active Directory 证书服务	1 🙆	• 🔝 • 🖶 • 🛃 页面 (P) •	③ 工具(0) ▾ »
Hicrosoft Act	ive Directory 证书服务 office-win-	testca		主页
提交一个证书印	申请或续订申请			
要提交一个保存 编码的 CMC 雪 保存的申请:	字的申请到 CA , 在"保存的申请"框中 或 PKCS #10 证书申请或 PKCS #7 续订	P粘贴一个由外部源(如 丁申请。] Web 服务器)生成的 k	oase-64
Base-64 编码的 证书申请 (CMC 或 PKCS #10 或 PKCS #7):	lvSByhQwDQYJKoZIhvcNAQEFBQADgYEAM o4mbwAte/KqCNRaetQ9g0n7jzTzfyAhPA pOMV5FYWWhYehtsk5U3WFe3H4aSgYB9F4 sKhgxEykq9M= END NEW CERTIFICATE REQUEST-	sBSDCEk ▲ +tIBGiK FIj2Hvn		
证书模板:				
附加属性:	Web 服务器 ▼			
属性:	× ×			
完成		🔽 🚺 🚺 可信站点	保护模式: 禁用	• 100% • //

图 3-25 申请 WEB 服务器数字证书

Ø∎icrosoft Active Directory 证书服务 - Windows Internet Explorer	
🚱 🗢 🖌 http://192.168.1.125/certsrv/certfnsh.asp 💽 🌆 🏹 🗙	Live Search
😪 🍲 🏉 Microsoft Active Directory 证书服务 🔄 🔹	🔊 🔸 🖶 🖬 页面 (P) 🔹 🎯 工具 (D) 🔸 🎽
🕐 Internet Explorer 已经阻止此站点以不安全的方式使用 ActiveX 控件。因此,此页可能显示不正	确。 ×
Microsoft Active Directory 证书服务 office-win-testca	主页
证书已颁发	
您申请的证书已颁发给您。	
◎ DER 编码 或 ○ Base 64 编码	
	味护保式: 奈田 100% ・

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"。

🌈 🖬 i crosoft Active Directory 证书用	务 - Vindows Internet Explorer	- 🗆 ×
🚱 💿 🗸 🙋 http://192.168.1.125/cer	tsrv/certfnsh. asp 💽 🍫 🗶 Live Search	P -
🙀 🎄 🄏 Microsoft Active Directory	证书服务 🍐 👘 🔂 - 🖶 - 🔂 页面 (2) - 🎯)工具(0) • »
🕡 Internet Explorer 已经阻止此站点以不到	安全的方式使用 ActiveX 控件。因此,此页可能显示不正确。	×
Microsoft Active Directory 证书	已完成 0%, 共 certaew.cer (來自 192.168.1 💶 🗙	主页
证书已颁发	S	
您申请的证书已颁发给您。	certnew.cer (朱白 192.168.1.125)	
● DER 编码 或 ○ B <u>■ 下载证书</u>	日 17 新知(18 19 19 17 17 17 17 17 17 17 17 17 17 17 17 17	
·····································		
另存为	×	4
Adm	inistrator + 下载 🛛 👻 搜索 😥	
文件名 00): [::\certforwebserver 💌	ī I
保存类型(T):	安全证书	
◎ 浏览文件夹(B)	保存(S) 取消	1.
• 完成	🛛 👘 🐨 🗸 可信站点 保护模式: 禁用	<u>→</u> 100% → //

图 3-27 申请 WEB 服务器数字证书

文件 (F) 视图 (V) 帮助 (H)		
注稿 ● ● 記給页 ● ● WIN-GOMMEZZILON (OFFICE\Administrator) ● ● G 四泊 日 ● G 阿泊	服务器证书 使用此功能来申请和管理 Web 服务器可以对配置了 SSL 的网站使用的证书。 <u>各称 ^ </u>	操作 导入 砂罐证书申请 空成证书申请 空成证书申请 包運域证书 包運域证书 包運域证书 包運域证书 包運域证书 包運動名征书 包運動名征书 包運動名征书 日 1 1 1 <th1< th=""> <th1< th=""> <th1< th=""> <th< th=""></th<></th1<></th1<></th1<>
完成证书申请	<u>?</u> ×	查看
通过检索包含证书颁 包含证书颁发机构响 C: \cert forwabserve 好记名称 (Y): webservercert	ガスを い (FFI)2 炭机构响应的文件名(g.): r. cer	 2 界的 联邦(表示的)

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。

文件 (F) 视图 (V) 帮助 (H)				
<mark>接</mark> → 🔜 🖆 象	服务器证书	÷		操作 导入
WIN-9GXMEZZXLQN (OFFICE\Adminis	使用此功能来申请和管理	Web 服务器可以对配置了 SSL 的网	站使用的证书。	切理址や中国・・・
——20 应用程序地 B—20 网站	<u>名称</u> ~ webservercert	前友治 office-win-testca 192.168.1.125)放发着 office-win-testca office-win-testca	元限型でP+Fg 创建自至名证书 宣看 号出 续订 × 聯発
	▲		×	 評助 联机帮助

图 3-29 导入证书

Linternet 信息服务(IIS)管理器	_ 🗆 ×
😮 💿 🜘 🕨 WIN-9GXMEZZXLQN 🕨 网站 🕨 Default Web Site 🕨	😰 🖂 🛅 I 🕑 -
文件(P) 视图(V) 帮助(H)	
连接 Default Web Site 主页 ● ● ■ Main Site	2× 2× ▲ 第2× 2× ▲ 第2× 2× ▲ 第第定 雪看应用程序 雪看应用程序 雪看虚拟目录 管理阿法 ▲ ● ● ●
· 可能视图 於 内容视图	配造 + 船速求照空
就绪	6ª

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。

@Internet Explorer 增强的安全跟出	已启用 - Windo	ows Internet Explor	er	-O×
🕞 🕤 - 🙋 res://iesetup. dll/Hardi	Admin. htm		💽 🌛 🗙 Live Search	P -
🟠 🍄 🔘 正在连接			🟠 • 🗟 • 🖶 • 🔂	页面 (?) • 🎯 工具 (0) • "
Internet Internet ス 連邦 文 記 の 文 の 記 の 文 の 記 の 文 会 い 交 、 読 の 文 の 文 の 文 の 文 の 文 の 文 の 文 の 文 の 文 の	Explorer 増売的安全 - 读说言述降低了 - 读说言述降低了 - 读说言述降低了 - 读说言述降低了 - 正在注接到 192.168 - 用户名(0): 密码(0):	奥的安全配器已启用 配量当前已在現券建設在可能等が 這方開募考測者の設立 (1) 125 188.1.125。	. 它配置了许多定义用户如何浏览1 安全风险的两站的可能性。有关发展 了》》 网络资源的方向。 站,可以将资源到 口lover 增强的方向。	nternet 和 Intranet 量中安全设置的完整列 如理再合名的定(UNC) 診測和地 Intranet 空遊量.
等待 https://192.168.1.125/cert:			😔 Internet 保护模式: 禁用	🔩 100% 🔻 //

图 3-31 为 Radius Server 申请数字证书

-	🛿 https://192.168.1.125/certsrv/certrqma.asp 💎 🔒 🌳 🗙 Live	Search
4 88	* 🖉 Microsoft Active Dire 🎯 Microsoft Active D 🗙 📔 🏠 * 🕤 *	🖶 ▼ 🔄 页面 (?) ▼ 🌍 工具 (0)
E书模板:		
	系统管理员	
翻选项:		
	 ● 创建新密钥集 ○ 使用现存的密钥集 	
	CSP: Microsoft Enhanced Cryptographic Provider v1.0 💌	
密钥	用法: @ 交换	
密钥	大小: 1024	
	· 自动密钥容器名称 C 用户指定的密钥容器名称	
	▶ 标记密钥为可导出	
	□ 启用强私钥保护	
其他选项:		
申请	格式: ◎ CMC ○ PKCS10	
哈希	算法: sha1 ▼	
	仅用于申请签名。	
	□ 保存申请	
	属性·	

图 3-32 为 Radius Server 申请数字证书

■icrosoft Active Directory 征书服务 -	Tindows Internet Expl	orer			_02
🕘 🕤 👻 https://192. 168. 1. 125/certsrv/	certfnsh. asp		+ X Live Sea	ch	P -
👔 🍻 🔠 🛪 🏉 Microsoft Active Dire	🏉 Microsoft Active D	×	🙆 • 🗟 • 🖶	◆ <mark>長</mark> > 页面 (P) ◆ (◎工具(0)・'
Microsoft Active Directory 证书服务 ·	office-win-testca				主页
证书已颁发					
您申请的证书已颁发给您。					
安装此证书					
广保存响应					
成			信站点 保护模式:	禁用	100% -

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。

Microsoft Active I	irectory 证书服务 offic	ce-win-testca		主页
欢迎使用				
使用此网站为您的 Web 进行通信的用 您也可以使用此网站	Web 浏览器、电子邮件客户 户确认您的身份、签名并加 站下载证书颁发机构(CA)证书	P端或其他程序用 密邮件,并根据 时、证书链,或1	a请证书。通过使用证书 您申请的证书类型执行 E书吊销列表(CRL),或	8,您可以向通过 其他安全任务。 渚查看挂起申请的状
态。				
有关 Active Direct	ory 证书服务的详细信息,证	青参阅 <u>Active D</u>	irectory 证书服务文档	
选择一个任务: <u>申请证书</u> <u>查看挂起的证书</u> 」 下载 CA 证书、	<mark>电请的状态</mark> 正书链或 CRL			

图 3-35 下载 CA 根证书

这个	 • 正书的目的如下: • 所有颁发策略 • 所有应用程序策略 	
	颁发给: office-win-testca	
	颁发者: office-win-testca	
	有效起始日期 2014/8/7 到 2019/8/7	
	安壮江北 介) 【 杨光孝》	XAB (q

图 3-36 安装 CA 证书到客户端电脑

Wind	wws 可以自动选择i	正书存储,或	者您可以为证·	书指定一个信	立置。
C	根据证书类型,自	自动选择证书	字储 (V)		
œ	将所有的证书放入	、下列存储 (P)	i		
	证书存储:				
	受信任的根证书》	顶发机构			浏览(R)
。翻证书	存储的更多信息				

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"。

➢证书错误:导航已阻止 - ♥indo	ws Internet Explorer				_0×
- R https://localhost/		• *	🕈 🗙 Live	Search	P -
👙 🏟 🔡 🕈 🍘 Microsoft Act	ive Dire 🏉 证书错误:导	就已阻止 ×	* • •	🖶 🔸 🔂 页面 (?) 🔹	③ 工具 (0) → [≫]
此网站的安全证	nternet 选项 正书		<u>?</u>		
此网站出具的安全	预期目的 00): 〈所有〉 个人 其他人 中级证书颁》	发机构 受信任的根证书	颁发机构 受	▶ (信任的发行者) • • • •	
安全证书问题可能	颁发给		截止日期	友好名称▲	
建议关闭此网页,:	Microsoft Authentic Microsoft Root Auth Microsoft Root Cert	Microsoft Authen Microsoft Root A Microsoft Root C NO LIABILITY ACC	2000/1/1 2020/1 2021/5/10 2004/1/8	Microsoft Au. Microsoft Ro. Microsoft Ro. VeriSign Tim.	
	office-win-testca office-win-testca Thawte Timestamping CA	office-win-testca office-win-testca Thawte Timestamp	2019/8/7 2019/8/7 2021/1/1	〈无〉 〈无〉 Thawte Times.	
♥ 更多信息	VeriSien Class 3 Pu	VeriSign Class 3	2036/7/17	VeriSim Y	
	与入 (I)」与出 (I)」			高级 (A)	
				查看(V)	
	了解证书的详细信息			关闭(C)	
		确定 取消	应用 (A.		× 100%
元讷		Inter Inter	net 1米升格	試 : 禁用	₹ 100% × //

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。

Local Area Connection Properties	? ×	Protected EAP Properties	? 🗙
General Authentication Advanced Select this option to provide authenticated network access this Ethernet adapter. Image: Comparison of the second	for	When connecting: Validate server certificate Connect to these servers: Trusted Root Certification Authorities:	
Choose a network authentication method: Protected EAP (PEAP) Settings Cache user information for subsequent connections to this network		NetLock Kozjegyzoi (Class A) Tanusitvanykiado NetLock Uzleti (Class B) Tanusitvanykiado office-WANG-CA office-win-testca PTT Post Root CA Saunalahden Serveri CA Saunalahden Serveri CA Do pot prompt user to authorize pew servers or trusted	
ОК Са	ncel	Certification authorities. Select Authentication Method: Secured password (EAP-MSCHAP √2) ✓ Configur ✓ Enable Fast Reconnect Enable Quarantine checks Disconnect if server does not present cryptobinding TLV OK Cancer	re

图 3-39 客户端本地连接设置

Enter Credent	ials 🔀
User name:	cs1cs1
Password:	•••••
Logon domain:	
	OK Cancel

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

Copyright © Siemens AG Copyright year All rights reserved

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。

Alaternet Explorer 增强的安全配置已启用	- Vindows Internet Explore	r	
🕞 🕞 - 🙋 https://192.168.1.125/certsrv,	1	🔹 😽 🗙 Live Se	arch 👂 🔻
😪 🕸 🔘 正在连接		🔓 • 📾 • 🖶	• 📴 页面 (P) • 🥥 工具 (D) • 🎽
Internet Explorer は 市での で は 市での ま の で 、 で 、 市 参 の に で 、 で 、 、 市 参 の に で 、 、 で 、 、 で 、 、 、 、 、 、 、 、 、 、 、 、 、	注接到 192.168.1.125 正在连接到 192.168.1.125。 用户名①: 日戸名①: 日ではま的3 正はま的3	2 ×) ●●● 一 一 一 一 一 一 一 一 一 一 一 一 一	■ 到覚 Internet 和 Intranet 合大応配量中安全设置的完整列 合访问。如道用命名约定(UNC) 将该两边将加到单地 Intranet 道理的支金配置。
等待 https://192.168.1.125/cert:		😌 Internet 保护模式	:禁用 🛛 💐 100% 👻 🎢

图 3-41 申请客户端证书

🖉 🛛 i er o	soft Active Directory 证书服务 - Windows Internet Explorer	_	
90	🕶 🔊 https://192.168.1.125/certsrv/certrqus.asp	🖌 🖘 🗙 Live Search	ρ
2 🎝	🏉 Microsoft Active Directory 证书服务	🏠 • 🖸 • 🖶 • 🔂 页面 (P) • 🎯 工具 (0)	
Tiora	araft Matina Divastory 江山肥冬 office_wiv_tostas	主义	
BILID	ADII ACTIVE DIRECTOLY ME DAMA OTILE WILL CESTER	<u></u>	1
申请一	-个证书		-
14+12	众江北光刑		
用户	- 1720 中央空. 户证书		
或者,	提交一个 <u>高级证书申请</u> 。		
	The distance of the second secon		-
		可信誌占 保护構式・ 林田 💮 100%	
	j j j j j j i j j i j j i 00 1♥		

Copyright © Siemens AG Copyright year All rights reserved

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。

Slicrosoft Active Directory	证书服务 - Vindows I	nternet Explorer				_ 🗆 ×
G + Attps://192.168.1.	125/certsrv/certrmpn.as	.p.	🔒 😽 🗙	Live Search		P -
👙 🍻 🏉 Microsoft Active Dir	ectory 证书服务		🙆 • (┓ · 🖶 • 🖻 页	面(P) 🕶 🌀)工具(0) • »
Internet 这项 常规 安全 隐私 内容 内容审查程序 W系统可帮助成 子	│ 连接 │ 程序 │ 高級 技	? × ;> B版发机构 受信任的相关	员证书颁发机构 】	受信任的发行者】	×	<u>主页</u>
 使用加密连接和株 	颁友结 Administrator Administrator csles1	颁发者 Administrator office-win-testca office-win-testca	截止日期 2017/8/5 2015/8/7 2015/8/7	友好名称 《元》 RadiusServer 《元》		
	'	. 删除 (R)		高级 查看 (V)		
			✔ 可信站点 ·	保护模式:禁用		<u>▼</u> 100% ▼ //

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"。

书一起导出,您必须在后面一页上往	建入密
〈上一步 여) 入	取消
	书—起导出,您必须在后面—页上i 〈 上—步 (B) 下—步 (X) 〉

图 3-44 导出" cs1cs1"用户证书

出 文件格式 可以用不同的文件格式导出	证书。	
洗择要使用的格式:		
C DER 编码二进制 X.	09 (, CER) (D)	
C Base64 编码 X.509	. CER) (S)	
C 加密消息语法标准	PKCS #7 证书(.P7B)(C)	
□ 如果可能,则数	屠包括证书路径中所有证书 (I)	
● 个人信息交換 - PK	S #12 (. PFX) (P)	
「 如果可能, 则数	据包括证书路径中的所有证书(V)	
「 如果导出成功,	腳涂密钥 (K)	
「 导出所有扩展属	± (A)	
C Microsoft 序列化证	书存储(.SST)(T)	
解 <u>证书文件格式</u> 的更多信息		
证书文件格式的更多信息		

图 3-45 导出" cs1cs1" 用户证书

计导工问导	
密码	
要保证安全,您必须用密码保护私钥。	
54 % 22751 (****)	
獕八升朔认密约 。	
密码(P):	
•••••	
输入并确认密码(Mmm)(C):	

Copyright © Siemens AG Copyright year All rights reserved

图 3-46 导出" cs1cs1" 用户证书

<上一步(B) 下一步(N) >

取消

文件名():	
c:\CS1CS1Cert	浏览 (R)

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"。

東(S): Data	
▲ 身份验证方法	仅允许访问那些通过指定方法执行身份验证的客户端。
2 空闲超时	可按 BAP 类型列出的顺序在 NPS 和客户端之间协商这些类型。
🖁 会话超时	EAP 类型(T):
🔜 被叫站 ID	Microsoft:智能卡或其它证书 上移 (0)
日期和时间限制	下移(0)
E NAS 端口类型	4
	添加 (A) 编辑 (E) 删除 (B)
	安全级别较低的身份验证方法:
	✓ Microsoft 加密身份验证版本 2 (MS-CHAP-v2)(V) ▼ 用户可以在密码过期后更改密码 (H)
	▼ Microsoft 加密的身份验证 (MS-CHAP) (Y)
	☑ 用戶可以在密码过期后更改密码(X) □ 加密的身份验证(CHAP)(C)
	□ 未加密的身份验证 (PAP, SPAP) (S)
	🔰 🗖 允许客户端连接时不必协商身份验证方法 (L)

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。

pyright © Siemens	G Copyright year I rights reserved	
Cop	Al AG	

👃 Local Area Connection Properties 🛛 🔹 🔀	Smart Card or other Certificate Properties
General Authentication Advanced Select this option to provide authenticated network access for this Ethernet adapter. Enable IEEE 802.1X authentication Choose a network authentication method: Smart Card or other Certificate Cache user information for subsequent connections to this network	When connecting: Use my smart card Use a certificate on this computer Use simple certificate selection (Recommended) Validate server certificate Connect to these servers: Trusted Root Certification Authorities: NetLock Expressz (Class C) Tanusitvanykiado NetLock Kozjegyzoi (Class A) Tanusitvanykiado NetLock Kozjegyzoi (Class B) Tanusitvanykiado NetLock Kozjegyzoi (Class B) Tanusitvanykiado Office-WANG-CA Office-win-testca PTT Post Root CA Saunalahden Serveri CA Saunalahden Serveri CA View Certificate
OK Cancel	Use a different user name for the connection

图 3-49 本地连接设置

Select Certificate	a la	? 🔀
User name on certific	ate:	
cs1cs1@office.siem	ens.com	~
Friendly name:		
Issuer:	office-win-testca	
Expiration date:	8/7/2015 15:21:38	
	OK Cancel	View Certificate

图 3-50 选择用户证书