第5章 终端安全管理措施

一个复杂的信息系统可以由若干个分系统或子系统组成。无论从全系统、分系统还是子系统的角度，信息系统一般都由支持软件运行的硬件系统、对系统资源进行管理和为用户使用提供基本支持的系统软件以及实现信息系统应用功能的应用系统软件等组成。这些硬件和软件协作运行，实现信息系统的整体功能。从安全角度而言，组成信息系统各个部分的硬件和软件都应有相应的安全功能，确保在其所管辖范围内的信息安全和提供确定的服务。这些安全功能可分为4个层面：确保硬件系统安全的物理安全，确保数据网上传输、交换安全的网络安全，确保操作系统安全的系统安全，确保应用软件安全运行的应用安全。这4个层面再加上为保障其安全功能达到应用的安全性必须采取的管理措施，构成了信息系统安全的5个层面。为实现信息系统的安全，对信息系统中的重要组成部分——终端也要有相应的安全管理措施。

为实现终端安全，需要建立立体的安全防护体系，以应对终端面临的各类威胁。终端安全管理平台是终端安全管理实施中重要的技术支撑平台，通过协调统一的安全管理技术对终端信息进行全面管理。为了获取终端的实际工作状态，通常终端安全管理均采用客户/服务器方式，在终端中安装由信息系统安全管理中心制定、下发的安全防护策略，终端中的客户端按照安全防护策略中的相关规则，对终端中的进程、服务、接口、外部设备进行管控，并获取终端的硬件、软件资产信息，提供病毒防御、补丁管理、终端准入、安全审计、溯源追踪等功能，依托云端大数据的海量数据分析，对已知和未知的安全威胁进行防御。

5.1 环境管理

我国在2007年制定、2008年实施的《信息安全技术 信息系统物理安全技术要求》(GB/T 21052—2007)中对信息系统的物理安全作了相关规定。环境管理主要从终端的物理安全方面考量，涉及整个系统的配套部件、设备和设施的安全性能，所处的环境安全，以及整个系统可靠运行等方面，是信息系统安全运行的基本保障。

终端的物理安全管理措施是为了保证信息系统安全、可靠运行，确保信息系统在对信息进行采集、处理、传输、存储过程中不至于受到人为或自然因素的危害，而使信息丢失、泄露或破坏，对计算机设备、设施(包括机房建筑、供电、空调等)、环境、人员、系统等采取适当的安全措施。终端的物理安全主要从设备安全和运行安全着手。

5.1.1 设备安全

设备安全是为保证信息系统的安全、可靠运行，降低或阻止人为或自然因素给硬件设备安全、可靠运行带来的安全风险，对硬件设备及部件所采取的适当安全措施，主要包括抗静电、抗电磁辐射、抗电磁传导、抗浪涌冲击等方面的相关技术要求。相关标准可参考第 4 章的内容。

5.1.2 运行安全

运行安全是为保证信息系统的安全、可靠运行而提供的安全运行环境，使信息系统得到物理上的保护，从而降低或避免各种安全风险。运行安全措施主要是指终端设备正常运行所需的安全保护措施，包括场地安全、防火、电磁辐射防护、电磁屏蔽、电源安全、静电防护、防雷、温湿度控制、防盗、出入控制、记录介质安全等方面的相关技术要求。相关标准可参考第 4 章的内容。

5.2 资产管理

企事业单位每年都投入大量资金购置各种信息资产，但随着信息资产的使用、转移，很难及时、清楚地知道信息系统内部及下属机构拥有多少信息资产，分布在哪些部门，存放在何处，谁在使用，安全状况如何，等等。在员工离职或工作变动时，可能出现资产交接不完整的情况，无法快速、完整地了解员工保管的资产，从而造成组织机构资产的流失。由于资产管理制度、管理人员、使用人员等方面原因，在终端资产发生变化时，无法高效、精确地进行硬件资产管理，确定每台计算机的硬件配置变化情况，无法跟踪硬件资产的历史使用记录，也不能及时掌握资产变动情况。而传统资产统计、管理都需要消耗大量的人力、物力、时间，对提高企事业单位资产管理和工作效率影响非常大。对于大型的信息系统，由于信息资产数量多，分布分散，导致核查和盘点工作量大，出错率较高，给组织机构的资产管理部门带来很多问题。

随着企事业单位信息化程度的提高，信息系统中计算机终端数量日益增多，分支机构地理分布距离远，日常终端运维管理的工作压力十分巨大，主要表现在以下几方面：

(1) 终端数量多，部署分散，导致对终端运维支持困难。

(2) 统一补丁修复和软件分发问题。如果计算机终端中存在的操作系统安全漏洞不能及时修复，将带来极大的安全风险。计算机终端需要利用管理手段快速、统一分发操作系统补丁，但架设 WSUS(Windows Server Update Services，Windows Server 升级服务)服务器配置麻烦，维护工作量大，而且也不具备普通软件分发功能。

(3) 传统防病毒软件误杀带来的问题。传统防病毒软件为了提高病毒查杀率，奉行从严的查杀策略，导致单位内部应用程序或重要文档被误杀，因而产生了大量不必要的维护工作。

(4) 现场维护工作量大。计算机终端用户报告使用故障时，需要 IT 维护人员亲自赶

赴现场处理，但通常大部分上报的故障都是比较简单的，完全可以通过远程协助由用户自己解决。

5.2.1　硬件资产管理

终端是信息系统重要的资源和基础结构，对终端固定资产的管理是企业的一项重要基础工作。固定资产的数量、质量、技术结构标志着企业的生产能力，也标志着企业生产力的发展水平，是企业赖以生存的主要资产。

对于计算机终端类的固定资产，传统的资产管理采用手工管理方式和一般的固定资产管理软件，通过手工记账、资产档案信息化方式进行管理。而在大型信息系统中，终端数量庞大，组织机构复杂，部署分散，传统方式的管理工作量非常大，提供的管理能力非常有限。随着终端管理技术的发展，企业逐渐转向通过相关的技术手段和管理措施对终端硬件资产进行管理。

(1) 通过在终端中安装的客户端程序，利用终端系统中的 API 读取硬件信息，利用驱动程序的接口返回相关信息，并将配置信息统一上报终端安全管理平台，这些配置信息包括计算机硬件型号、硬件配置信息、计算机整机型号等。

(2) 通过自动收集终端的相关信息，包括硬件信息、操作系统信息、终端登记信息等内容，对终端硬件变动产生告警信息。对收集的信息进行统一处理，可以通过输出报表、报告等方式以方便管理人员对资产变动信息的收集与统计。

(3) 设置终端自助资产登记。对于终端数量较大的信息系统，应支持自助资产登记功能，设置资产必填信息项以及输入的数据类型，为终端管理提供便捷、高效的使用环境。

在终端硬件资产的全生命周期(涵盖规划、调研、采购、验收、使用、维修、报废等)中，在硬件资产进入组织信息网络之前，应安装硬件资产管理软件或组件，利用计算机技术完成对信息系统中硬件资产的信息化，实现对终端安全的实时管理和控制。

5.2.2　软件资产管理

随着社会经济的不断发展，企业业务逐步走向多样化、精细化、定制化，企业日常生产环境基本上离不开各类应用软件的使用。为了提高企业管理效率和使用体验，越来越多的企业开始在内部使用购买、研发、定制各种各样的软件系统。随着企业内部软件数量的增加，软件在发放、下载、安装、更新、卸载、统计等方面就成为企业资产管理面临的一大问题。同时，软件在企业内网中传播渠道的不统一以及软件获取来源的不确定性对企业的信息安全也造成了极大的隐患。

企业对软件缺乏统一的管理，导致管理人员无法全面、及时地掌握企业内网软件安装情况。因此，如何规范软件管理，防止恶意软件流入，发挥软件给企业带来的价值，成为信息系统管理者重点关注的问题。企业在软件管理方面遇到的问题主要如下：

(1) 缺乏统一、高效的软件分发平台。

(2) 缺乏对软件生命周期(下载、安装、升级、卸载)和软件统计运维信息的管理。

(3) 无序的软件传播渠道使得软件安全性无法保证。

(4) 有限的企业软件资源无法满足终端用户个性化使用需求。

(5) 终端用户同时下载软件时,容易大量占用企业对外网络接口带宽,影响企业正常业务。

(6) 全网已安装的软件没有统计记录,对软件无法统一管理。

(7) 企业购买收费软件并将软件授权序列号分发给终端用户之后,往往较难统计软件的实际使用情况,管理员对于企业内软件资产的使用、分配、利用率等情况无法掌控。

为解决软件资产管理问题,可以采用以下措施。

1. 统一软件获取渠道

为统一企业内部软件获取渠道,可以通过在企业内网中设置软件分发中心,满足企业内部用户普遍性的软件需求,全面覆盖企业网内软件下载、使用需求,以保障企业下载软件的安全。通过统一软件获取渠道,使得内网终端用户不必通过互联网等不可信渠道获取无法确认安全性的软件,规范软件获取渠道,从而保障终端和信息系统的软件安全。

这种管理措施面临的问题是:由于企业业务的多样性,软件的种类、版本、授权管理等也多种多样。在管理中可以进行业务优化,指定业务使用软件的集合,通过对有限范围内的软件进行管理,实现软件获取渠道的统一。

2. 软件统一部署

企业日常生产环境已基本固化,不同的生产环境使用不同的生产模板,通过对终端中软件的统一部署,避免终端使用者安装与生产环境不一致的软件产品,从而降低和避免由于软件不统一导致的风险。同时,通过软件安装统计功能,监控全网软件安装,并可以对软件进行分发安装、升级、卸载等操作,便于管理员统一管理内网软件。一些软件管理平台可以在线查看终端已安装软件的授权序列号以及使用情况,为企业优化软件资产分配和软件采购提供数据支撑。

在第 4 章中介绍的国外有关终端的典型处理流程中就包含软件统一部署的管理措施。在终端到达使用者手中时,已完成了基础软件的统一部署安装,实现了软件统一部署的管理措施。国内很多企事业单位也已实现了类似的管理措施。

3. 应用控制

应用控制功能应支持以下 4 个基本功能:

(1) 进程启动控制。用于控制终端上能运行的进程,只有经过管理人员明确允许的进程才可以运行。

(2) 文件保护。用于保护关键目录,使其不被其他软件非法更改。

(3) 注册表保护。用于保护关键注册表,使其不被其他软件非法更改。

(4) 进程保护。用于保护关键进程,以避免被其他软件恶意结束。

应用控制功能应包含以下 3 部分:

(1) 策略系统。用于编辑应用控制功能的策略,并将策略下发到终端系统。策略包括:是否开启其他功能,允许或禁止的进程特征,受保护的文件、注册表和进程,以及访问例外等。

(2) 客户端。主要由策略解析引擎、驱动程序和决策引擎等部分组成。策略解析引擎负责接收和解析终端安全管理平台下发的策略;驱动程序负责拦截系统的进程启动、文件访问、注册表访问、进程访问等 API 操作;决策引擎接收驱动程序回调的系统行为信息,并根据下发的策略进行决策,并将决策结果反馈给驱动程序。

(3) 日志系统。用于记录终端的相关过程。管理员通过分析日志可以判断是否有错误拦截或遗漏拦截,从而能够及时调整规则。

5.2.3　过时终端安全管理

过时终端主要是指到期终端、临时入网终端等需要在终端资产管理中注销以及特别关注的相关终端。

对于组织统一管理的到期终端,需要做好报废前的准备工作,包括相关信息登记、处理流程等。在这一过程中需要注意的是识别和处理与到期终端相关联的其他资产信息,不能因到期终端的报废引起其他关联的、未到期资产的损失或损坏。应注意对到期终端中存储的信息进行处理,避免信息泄露。到期终端报废后,应在资产管理中注销并做好相关记录,避免非法终端冒充报废终端接入组织内部网络中。

对于临时入网终端,应建立相应的管理制度。例如,临时入网终端需提交终端接入申请,包括接入设备名称、接入设备类型、接入用途、接入区域、访问资源范围、计划终止时间等,随后由系统完成接入审批、接入安全检查等工作流程。在临时终端脱离组织内网后,需要提交相应的取消终端接入申请,完成临时入网终端的闭环管理。

5.3　存储介质管理

5.3.1　常规存储介质管理

对于固定硬盘、磁带、光盘等常规存储介质,应对存放环境、使用、维护和销毁等方面进行规定,确保存储介质存放在安全的环境中,并对存储介质进行控制和保护。如果含有重要数据的存储介质需要带出,应提前做好加密和备份工作。对于需要送出维修或销毁的存储介质应采用多次读写覆盖的方法消除敏感或秘密数据,对于无法执行删除操作的受损存储介质必须销毁,并做好相关的记录。如果有数据异地备份的需求,应做好相关的数据备份计划,相关技术参见 5.8 节。

5.3.2　移动存储介质管理

移动存储介质包括移动硬盘、手机、数码相机、摄像机、iPod、MP3/MP4、PDA 以及各种存储卡等。移动存储设备由于其体积小、携带方便、存储量大、使用灵活等特点,迅速得以广泛应用。根据对典型移动存储设备的产品销售量进行估算,当前全球使用中的各类移动存储设备超过 30 亿个,而且还在迅速增长。

对移动存储介质管理,通常是根据组织信息安全需求进行的。需要注意的是,由于移

动存储介质大部分使用 USB 接口，如果在设备管理中将 USB 接口设置为禁用，虽然移动存储介质被禁止使用了，但是某些使用 USB 接口的外设（例如鼠标、键盘）同样也会被禁用，影响终端用户对此类外部设备的使用。

5.3.3 安全 U 盘

U 盘在带给用户使用便捷性的同时，也成为计算机病毒传播及信息泄露的首要途径。

U 盘由芯片控制器和闪存两部分组成，芯片控制器负责与 PC 的通信，闪存用来存储数据。闪存中有一部分区域是用来存放 U 盘控制程序的固件，它的作用类似于操作系统，控制软硬件交互，通常无法通过直接访问等普通技术手段读取。由于普通 U 盘基本没有安全防护功能，对于其中保存的数据无法实现安全防护，针对此类情况，安全 U 盘应运而生。

安全 U 盘采取的数据保护技术一般分为两种：一种是硬件加密，另一种是软件加密。简单地说，硬件加密技术一般指采用专用的安全芯片对产品进行加密，将加密芯片、密钥、数据整合在一起进行加密运算，这种技术有防止暴力破解、防止密码猜测、数据恢复等功能；而软件加密则是通过产品内置的加密软件实现对数据的加密功能。

硬件加密的方式主要有键盘式加密、刷卡式加密、指纹式加密、声纹式加密等，而软件加密的方式主要有密码加密、证书加密等。硬件加密比软件加密在数据安全方面具有更高的可靠性，即插即用，无须安装加密软件，使用方便；而软件加密在实现技术以及成本上要低于硬件加密，容易实现，性价比高。从安全性的角度来看，软件加密更容易被破解，通过暴力破解方式破解软件加密有很高的成功率；而硬件加密由于加密模块是固化在硬件控制芯片中的，整个加密和解密过程是在 U 盘内部完成的，没有在计算机中留下任何痕迹，而且密码在传输过程中也是以密文形式传递的，所以很难被截获，即使通过技术手段截获得到的信息也是乱码，所以破解的可能性非常低。表 5-1 对采用这两种加密技术的安全 U 盘进行了对比。

表 5-1 硬件加密安全 U 盘和软件加密安全 U 盘的区别

比 较 项 目	硬件加密安全 U 盘	软件加密安全 U 盘
容量	2～32GB	支持任意容量的普通 U 盘
数据机密性	• 硬件参与密钥的保护和维护，防止数据未授权访问 • 使用硬件保护密文 • 加密算法不可被调试 • 使用私有文件系统	• 密钥加密存储，但没有访问控制措施 • 对密文无保护 • 加密算法可被调试 • 使用标准文件系统
数据完整性	• 使用硬件保护数据完整性 • 病毒、木马无法破坏数据	• 数据可以被篡改，无完整性校验 • 病毒、木马可以破坏数据
身份认证	硬件参与身份认证过程	身份认证信息可以被篡改

续表

比 较 项 目	硬件加密安全 U 盘	软件加密安全 U 盘
日志审计	对用户行为的审计准确度高，可以审计外部网络的用户行为，使用硬件保护审计日志完整性	用户行为审计准确度低，在外部网络环境下没有行为审计日志
产品稳定性及维护	稳定性高，有统一的质量管控和售后维护	硬件厂商的 U 盘质量不同，无法防止在制作过程中或使用过程中对 U 盘造成不可逆的损坏；无法提供售后维护或只能提供有限的售后服务
读写权限管理	通过硬件管理读写权限，安全性高	通过软件管理读写权限，容易被攻破

除了 U 盘容量以外，在数据机密性、数据完整性、身份认证、日志审计、产品稳定性及维护、读写权限管理等方面，硬件加密安全 U 盘均优于软件加密安全 U 盘。安全 U 盘使用已有或定制开发的安全芯片，对 U 盘的固件进行多种安全保护设计，防止攻击者利用对 U 盘的固件进行逆向重新编程、改写 U 盘的操作系统等方式对 U 盘进行攻击，有效提高了 U 盘的硬件安全性能。所以，企业若想有效降低因 U 盘使用给内网带来的安全隐患，应优先选择硬件加密安全 U 盘。

5.4 设备管理

Windows 操作系统通过 GUID 来管理硬件的动态变化（参考第 2 章相关内容）。GUID 是一个 128 位值，可以利用 WDK 和 Windows SDK 中包含的 Uuidgen 工具生成，考虑到 128 位所能表达的值的范围，从统计意义上几乎可以保证生成的 GUID 是全局唯一的。通过设备对应的 GUID 值，可以读取终端设备中对应的接口和设备。

1. 接口 GUID 值

表 5-2 列出了终端中常见接口的 GUID 值。

表 5-2　终端中常见接口的 GUID 值

接口标识	GUID 值	接 口 说 明
CDROM	4D36E965-E325-11CE-BFC1-08002BE10318	CD-ROM 驱动器接口
1394	6BDD1FC1-810F-11D0-BEC7-08002BE2092F	IEEE 1394 主控制器接口
Image	6BDD1FC6-810F-11D0-BEC7-08002BE2092F	摄像头、扫描仪接口
Media	4D36E96C-E325-11CE-BFC1-08002BE10318	视频、音频设备接口
PCMCIA	4D36E977-E325-11CE-BFC1-08002BE10318	PCMCIA 控制器接口
Ports	4D36E978-E325-11CE-BFC1-08002BE10318	端口（串口）
Ports	97F76EF0-F883-11D0-AF1F-0000F800845C	端口（并口）
USB	36FC9E60-C465-11CF-8056-444553540000	USB 主控器、集线器接口

2. 设备 GUID 值

终端中常见设备的 GUID 值如表 5-3 所示。

表 5-3　终端中常见设备的 GUID 值

设备标识	GUID 值	设备说明
CDROM	4D36E965-E325-11CE-BFC1-08002BE10318	CD-ROM 驱动器
DiskDrive	4D36E967-E325-11CE-BFC1-08002BE10318	磁盘驱动器
Display	4D36E968-E325-11CE-BFC1-08002BE10318	显示适配器
FDC	4D36E969-E325-11CE-BFC1-08002BE10318	软盘控制器
FloppyDisk	4D36E980-E325-11CE-BFC1-08002BE10318	软盘驱动器
HDC	4D36E96A-E325-11CE-BFC1-08002BE10318	磁盘控制器
HID Class	745A17A0-74D3-11D0-B6FE-00A0C90F57DA	人机交互设备
Image	6BDD1FC6-810F-11D0-BEC7-08002BE2092F	摄像头、扫描仪
Infrared	6BDD1FC5-810F-11D0-BEC7-08002BE2092F	红外设备
Keyboard	4D36E96B-E325-11CE-BFC1-08002BE10318	键盘
Modem	4D36E96D-E325-11CE-BFC1-08002BE10318	调制解调器
Mouse	4D36E96F-E325-11CE-BFC1-08002BE10318	鼠标
Media	4D36E96C-E325-11CE-BFC1-08002BE10318	视频、音频设备
Bluetooth	E0CBF06C-CD8B-4647-BB8A-263B43F0F974	蓝牙设备
Net	4D36E972-E325-11CE-BFC1-08002BE10318	网卡
SCSI Adapter	4D36E97B-E325-11CE-BFC1-08002BE10318	SCSI、RAID 控制器
System	4D36E97D-E325-11CE-BFC1-08002BE10318	系统总线、桥等
Printer	4658EE7E-F050-11D1-B6BD-00C04FA372A7	打印设备
MTP Device	EEC5AD98-8080-425F-922A-DABF3DE3F69A	SD 存储卡
USB	36FC9E60-C465-11CF-8056-444553540000	USB 主控器、集线器
USB	F72FE0D4-CBCB-407d-8814-9ED673D0DD6B	ADB 设备

5.5 网络安全管理

企业、组织机构的信息系统需要确保接入内部网络的终端设备符合安全标准。在这些设备被授予网络访问权之前，必须首先确定这一点。网络安全管理可帮助安全管理人员更好地控制信息系统的接入点，有效阻止安全威胁和非法访问企图。

5.5.1　终端认证

网络安全管理从设备接入发现、用户注册、认证授权、安全检查、隔离修复、访问控制等方面对用户终端入网进行管控。为提高安全性，可以采用多种认证技术、多因素认证凭证、多条件绑定机制、混合认证模式和多层防护体系，以适应各种复杂网络环境。通常可以采用防火墙、网络访问控制设备等安全设备，通过各种认证方式对终端访问网络进行管控。以下介绍终端认证常用的几种方式。

1. IEEE 802.1x 接入认证

IEEE 802.1x 是基于端口的网络访问控制(Port-based Network Access Control，PNAC)的 IEEE 标准，它是 IEEE 802.1 的一部分，为连接到 LAN 或 WLAN 的设备提供认证服务。IEEE 802.1x 定义了可扩展认证协议(Extensible Authentication Protocol，EAP)在 IEEE 802 上的封装，被称为 EAP over LAN 或 EAPOL。EAPOL 最初设计用于 IEEE 802.1x—2001 中的 IEEE 802.3 以太网，经过修改和调整，也适用于其他 IEEE 802 LAN 技术(例如 IEEE 802.1x—2004 中的 IEEE 802.11 无线和光纤分布式数据接口，即 ISO 9314-2)。EAPOL 协议也可用于 IEEE 802.1x—2010 中的 IEEE 802.1ae(介质访问控制安全协议，MACSec)和 IEEE 802.1ar(安全设备标识，DevID)以支持本地 LAN 段上的服务识别和可选的点对点加密。

图 5-1 是 IEEE 802.1x 的认证数据流示意图。

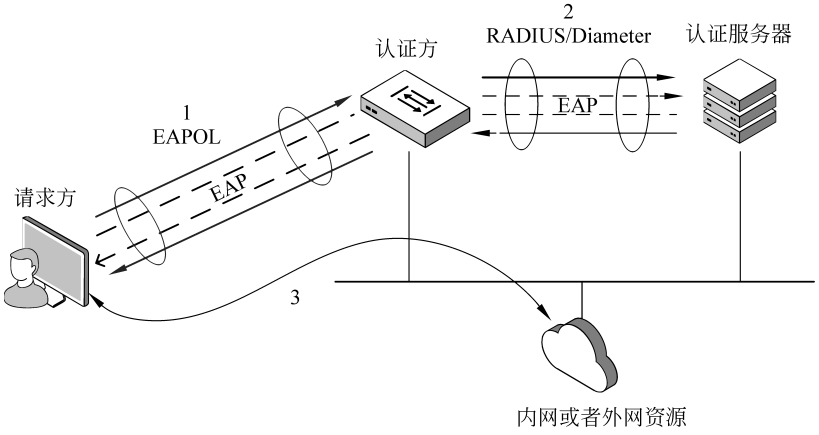

图 5-1　IEEE 802.1x 的认证数据流示意图

IEEE 802.1x 认证涉及三方：请求方、认证方和认证服务器。请求方是申请连接到 LAN/WLAN 设备的终端(例如台式计算机终端或笔记本电脑终端)，也可以是在终端上运行的向认证方提供凭证的软件；认证方通常是指网络设备，它提供客户端和网络之间的数据链路，并且可以在两者之间允许或阻止网络流量，主要是以太网交换机或无线接入点；认证服务器通常是运行支持 LDAP、RADIUS 和 EAP 协议的主机，是可信任的服务器，可以接收和响应网络访问请求，并且可以告知请求方是否允许连接，以及应该应用于该客户端的连接或设置的各种设置。EAP 数据首先封装在请求方和认证方之间的

EAPOL 帧中，然后使用 RADIUS 或 Diameter 在认证方和认证服务器之间重新封装。

认证方就像一个受保护网络的安全警卫。请求方（即客户端设备）不允许未通过认证就访问网络的受保护资源，直到请求者得到认证和授权。使用基于 IEEE 802.1x 端口的身份认证，请求方向身份认证程序提交凭据（例如用户名/密码或数字证书），身份认证程序将凭据转发到认证服务器进行认证。如果认证服务器确定凭据有效，则允许请求者（客户端设备）访问位于网络受保护端的资源。

图 5-2 给出了 IEEE 802.1x 的认证流程。

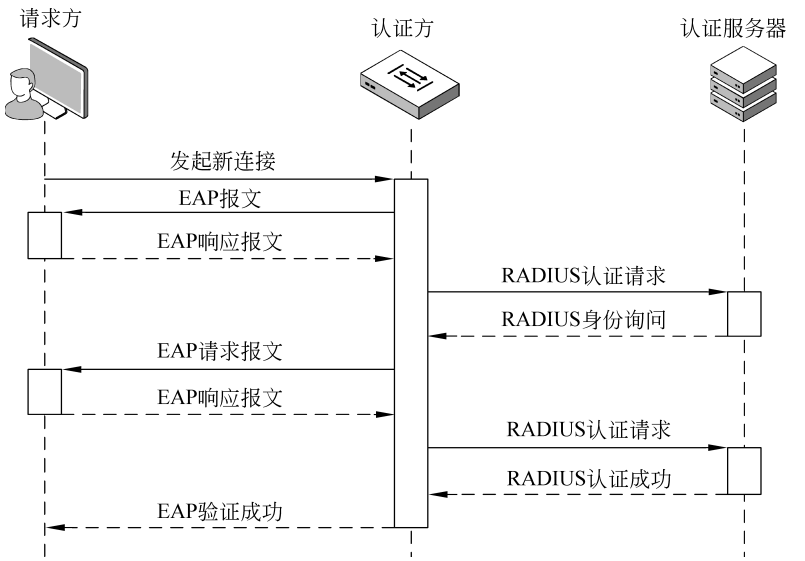

图 5-2　IEEE 802.1x 的认证流程

IEEE 802.1x 典型的认证流程包括：

（1）初始化。在检测到新的请求方时，交换机（认证方）上的端口被启用并设置为“未授权”状态。在这种状态下，只允许 IEEE 802.1x 协议的数据流通过，其他协议（例如 TCP、UDP 等）的数据流将被丢弃。

（2）启动。为启动认证，认证器将周期性地将 EAP-Request Identity 帧发送到本地网段上特殊的第二层地址（01:80:C2:00:00:03）。请求方在这个地址上侦听，并且在收到 EAP-Request Identity 帧时，用包含请求方标识符（例如用户 ID）的 EAP-Response Identity 帧进行响应。然后认证方将此身份响应封装在 RADIUS Access-Request 数据包中，并将其转发给认证服务器。请求方也可以通过向认证方发送 EAPOL-Start 帧来启动或重新启动认证，然后认证方将使用 EAP-Request Identity 帧进行回复。

（3）协商。认证服务器向认证方发送一个回复（封装在 RADIUS Access-Challenge 包中），其中包含一个指定 EAP 方法（它希望请求方执行的基于 EAP 的认证类型）的 EAP 请求。认证方将 EAP 请求封装在 EAPOL 帧中，并将其发送给请求者。此时，请求方可以开始使用其请求的 EAP 方法，或者执行 NAK（“否定确认”）并用它可以执行的 EAP 方法进行响应。