第 5 章　网络访问控制和云安全

学习目标

学习完这一章后，你应该能够：

- 阐述网络访问控制系统的主要组成元素。
- 阐述主要的网络访问控制强制措施。
- 给出可扩展认证协议的概述。
- 理解 IEEE 802.1X 基于端口的网络访问控制机制的操作流程和地位。
- 给出云计算的基本概念。
- 理解云计算中涉及的独特安全问题。

这一章开头讨论了网络安全，集中讨论了两个主要问题：网络访问控制和云安全。首先给出了网络访问控制系统的概述，总结了在这样一个系统中涉及的主要元素与技术。接着，讨论了两个广泛使用的标准：可扩展认证协议和 IEEE 802.1X，这两个标准是许多网络访问控制系统的基础。

该章节的剩余部分讨论了云安全。首先给出了云计算的概况，接着讨论了云安全中涉及的一些问题。

5.1　网络访问控制

网络访问控制（NAC）是对网络进行管理访问的一个概括性术语。NAC 对登录到网络的用户进行认证，同时决定该用户可以访问哪些数据，执行哪些操作。NAC 同时可以检查用户的计算机或者移动设备（终端）的安全程度。

5.1.1 网络访问控制系统的组成元素

NAC 系统由三种类型的成分组成。

访问请求者（AR）：AR 是一个尝试访问网络的节点，可以是由 NAC 系统控制的任何设备，包括工作站、服务器、打印机、照相机，以及其他支持 IP 的设备。AR 同时也被称为请求者，或者简称为客户。

策略服务器：基于 AR 的态度和企业预先定义好的策略，策略服务器决定授予请求者什么访问权限。策略服务器经常依赖诸如杀毒、补丁管理，或者用户目录等后端系统的帮助来决定主机的状况。

网络访问服务器（NAS）：在远程的用户系统想连接公司内网的时候，NAS 起到一个访问控制点的作用。NAS 同时也被称为介质网关、远程访问服务器（RAS），或者是策略服务器，NAS 有可能包含自己的认证服务，也有可能依赖由策略服务器提供的分离的认证服务。

图 5.1 是一个通用的网络访问图。许多不同的 AR 试图通过申请某种类型的 NAS 而获得企业网络的访问权限。第一步通常是认证 AR。典型的认证包括使用某种安全协议以及使用加密密钥。认证可能由 NAS 直接进行，也可能由 NAS 间接进行。在后面那种情形中，认证发生在请求者与认证服务器之间，认证服务器可以是策略服务器的一部分，也可以由策略服务器直接进行访问。

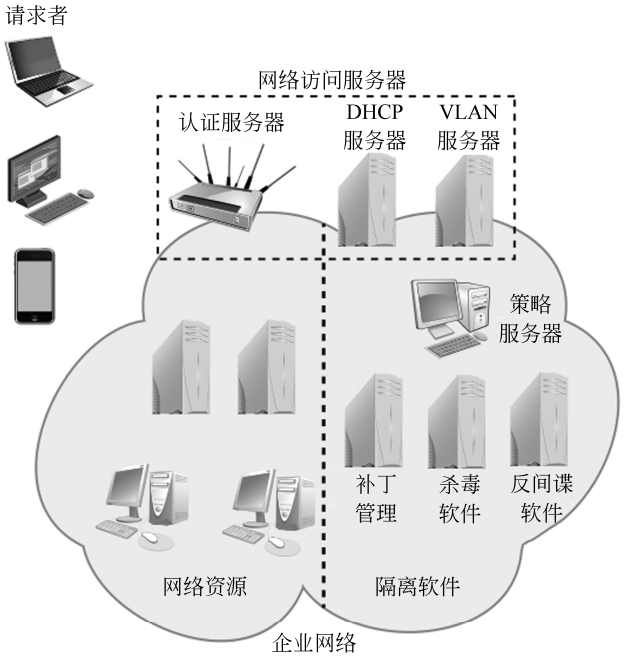

图 5.1 网络访问控制环境

认证过程服务于多种用途。它可以对请求者声称的身份进行验证，根据验证结果，策略服务器决定请求者是否具有访问权限以及具有什么级别的访问权限。认证交换可能导致会话密钥的建立，从而保证将来请求者与企业网络的资源之间可以进行安全通信。

通常，策略服务器或者支持服务器会对 AR 进行检查，以决定是否允许该请求者建立交互式远程访问连接。这些检查，有时也称为健壮性、适合性、筛选或者评估检查，需要用户系统中的软件去遵守来自企业组织的安全配置基准的一些要求。比如，用户的反恶意软件必须是最新的，操作系统必须完全打补丁，远程的计算机必须被组织拥有并受组织控制。这些检查必须在授予 AR 访问企业网络的权限之前被执行。基于这些检查结果，组织能够决定远程计算机是否能够使用交互远程访问的功能。如果用户具有可被接受的认证证书，但是远程计算机没有通过健康检查，用户以及远程计算机会被拒绝访问企业网络，或者只能被限制访问隔离网络，这样，只有被授权的人员可以访问网络，可以解决企业网络中存在的安全缺陷。从图 5.1 中可以看到，企业网络的隔离网络部分由策略服务器以及相关的 AR 适应性服务器组成。在隔离网络中，也有可能包含不需要满足安全阈值要求的应用程序服务器。

一旦 AR 被认证通过，具有访问企业网络的权限，NAS 就会允许 AR 与企业网络中的资源进行交互。NAS 有可能会干涉每一次交换以强制执行安全策略，也有可能使用其他方法限制 AR 的特权。

5.1.2　网络访问强制措施

强制措施被施加到 AR 上来管理用户对企业网络的访问。许多供应商同时支持多种强制措施，允许用户使用一种或者几种措施的组合来定制配置。下面是一些常用的 NAC 强制措施。

IEEE 802.1X：这是一个链接层协议，在一个端口被分配 IP 之前必须强制进行认证。IEEE 802.1X 在认证过程中使用了可扩展认证协议，5.2 节和 5.3 节分别介绍了可扩展认证协议和 IEEE 802.1X。

虚拟局域网（VLAN）：在这种方法中，由互连的局域网组成的企业网络被逻辑划分为了许多 VLAN[1]，NAC 系统根据设备是否需要安全修复，是否只是访问互联网，对企业资源何种级别的网络访问，决定将网络中的哪一个虚拟局域网分配给 AR。VALN 可以被动态创建，VLAN 的两个成员：企业服务器和访问请求者可能会有重叠。也就是说，一个企业服务器或者访问请求者可能属于不止一个虚拟局域网。

防火墙：防火墙通过允许或者拒绝企业主机与外部用户的网络流量来提供一种形式的网络访问控制。我们将在第 12 章介绍防火墙。

动态主机配置协议（DHCP）管理：动态主机配置协议（DHCP）是一个能为主机动态分配 IP 地址的互联网协议。DHCP 服务器拦截 DHCP 请求，分配 IP 地址。因此，基于子网以及 IP 分配，NAC 强制措施会在 IP 层出现。DHCP 服务器很容易安装配置，但是由于经常遭受各种形式的 IP 欺骗，只能提供有限的安全性。

还有许多其他的供应商提供的强制措施可以使用，在前面列表中出现的那些可能是最常见的措施了，而其中 IEEE 802.1X 是最通常的实现方案。

1　VLAN 是 LAN 内的一个逻辑子组，它使用软件创建，而不是通过在布线室手动移动电缆来创建。它将用户基站和网络设备集合成一个单元，忽视了它们所连接到的物理 LAN 段，从而使得数据流通更有效率。VLAN 一般在端口转换集线器和 LAN 开关中实现。

5.2 可扩展认证协议

可扩展认证协议（EAP），在 RFC 3748 中定义，它在网络访问以及认证协议中充当了框架的作用。EAP 提供了一组协议信息，这些协议信息封装了许多在客户端和认证服务器之间使用的认证方法。EAP 可以应用到许多网络层以及链接层的设施上，包括点对点链路，局域网以及其他网络，而且它可以满足许多链接层以及网络层的认证需求。图 5.2 展示了 EAP 结构的协议层次。

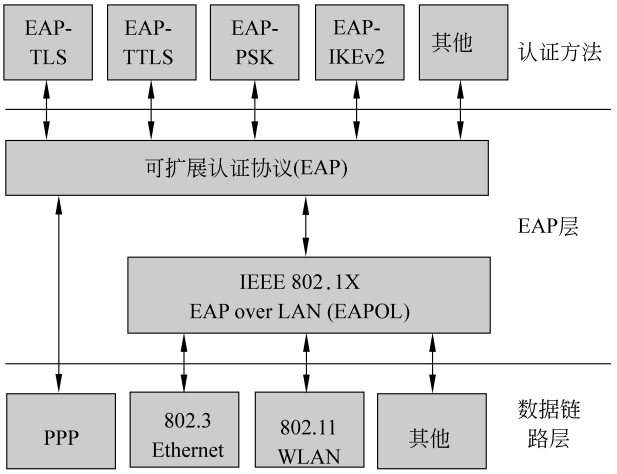

图 5.2 EAP 层级结构

5.2.1 认证方法

EAP 支持多种认证方法。这就是 EAP 被称为可扩展的原因。EAP 为客户端系统与认证服务器之间交换认证信息提供了一种通用传输服务。通过使用在 EAP 客户端与认证服务器上都安装的特殊的认证协议和方法，基本的 EAP 传输服务功能得以扩展。

已经提出了许多方法使用 EAP 进行工作，下面是一些常用的支持 EAP 的方法：

EAP-TLS（EAP 传输层安全）：EAP-TLS（RFC 5216）定义了 TLS 协议（在第 6 章描述）如何被封装在 EAP 信息中。EAP-TLS 在 TLS 中而不是在加密方法中使用了握手协议。客户端和服务器使用数字证书互相认证。客户端使用服务器的公钥加密一个随机数从而产生自己的预备主密钥（pre-master），并将该密钥发送给服务器。客户端与服务器都使用该预备主密钥来产生相同的安全密钥。

EAP-TTLS（EAP 隧道传输层安全）：EAP-TTLS 跟 EAP-TLS 类似，唯一的不同是在 EAP-TTLS 中，服务器首先使用证书向客户端认证自己的身份。在 EAP-TTLS 中，使用安全密钥建立安全连接（又称隧道），建立的连接被继续用于客户端身份的认证过程，也有可能再次认证服务器，这些认证过程使用了 EAP 方法或者是传统的方法，如 PAP（密码认证协议）、CHAP（挑战-握手认证协议）。EAP-TTLS 在 RFC 5281 中定义。

EAP-GPSK（EAP 通用预共享密钥）：EAP-GPSK 在 RFC 5433 中定义，它是一种使用预共享密钥（PSK）进行互相认证以及会话密钥推导的 EAP 方法。EAP-GPSK 基于预共享密钥指定了特定的 EAP 方法，而且采用了基于密钥安全的加密算法。就信息流以及计算成本而言，这种方法是高效的，但是，它需要在每个成员以及服务器之间使用预共享密钥。成对安全密钥的建立也是成员注册过程的一部分，因此必须满足系统的先决条件。当双方认证成功时，EAP-GPSK 为双方的通信提供一个受保护的通信通道，在诸如 IEEE 802.11 等不安全网络上，EAP-GPSK 被用来进行认证。EAP-GPSK 不需要任何公钥密码技术。使用 EAP 方法进行协议交换最少只需要使用四条信息就可以完成。

EAP-IKEv2：它基于互联网密钥交换协议版本 2（IKEv2），将在第 9 章中介绍该协议。它支持互相认证，可以使用许多方法建立会话密钥。EAP-IKEv2 在 RFC 5106 中定义。

5.2.2　EAP 交换协议

不论使用何种方法进行认证，认证信息以及认证协议信息都会包含在 EAP 信息中。

RFC 3748 定义 EAP 信息交换的目标是成功进行认证。在 RFC 3748 文档中规定，成功认证的标志就是 EAP 信息进行交换，最终的结果是认证者允许被认证端的访问，被认证端同意使用此次访问。认证者的决定一般包括认证与授权两个方面；被认证端有可能成功认证认证者，但是由于政策原因，认证者有可能会拒绝此次访问。

图 5.3 展示了 EAP 被使用时的典型的布局，主要包含以下几个组成成分：

EAP 被认证端：尝试访问企业网络的客户端计算机。

EAP 认证者：要求认证优先于授权访问网络的访问点或 NAS。

认证服务器：服务器主机与被认证端协商选择使用哪种 EAP 方法，同时，验证 EAP 被认证端的证书，授权对网络的访问。典型的认证服务器是远程用户拨号认证服务器。

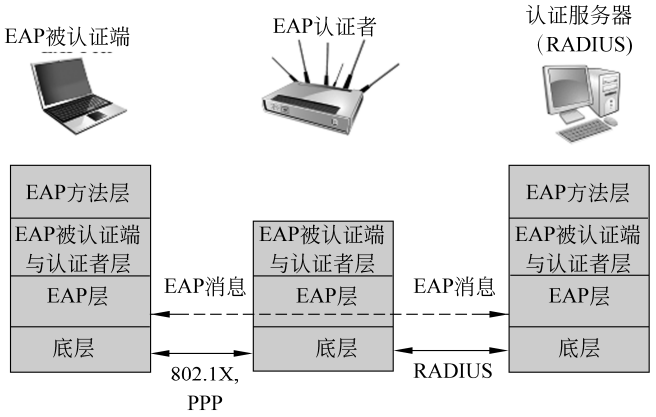

图 5.3　EAP 协议交换

认证服务器作为后端服务器，可以为许多 EAP 认证者提供认证被认证端的服务。EAP 认证者然后决定是否授权访问。这个过程被称为 **EAP 透传模式**。比较少见的还有，认证者同时起到了 EAP 服务器的作用。这样，在 EAP 执行过程中只有两方参与。

首先，使用低层协议，如 PPP（点到点协议）或者 IEEE 802.1X 协议同 EAP 认证者建

立联系。在 EAP 被认证端中，工作在这一级别的软件实体被称为**请求者**。在 EAP 信息中包含了选择使用哪种 EAP 方法的信息，该 EAP 信息在 EAP 被认证端以及认证服务器之间进行交换。

EAP 信息由以下几部分组成。

编码域：标识了 EAP 信息的类型，具体编码方式为：1 表示请求，2 表示应答，3 表示成功，4 表示失败。

标识符域：用来匹配请求与应答。

长度域：表示 EAP 信息的长度，八位字节，包括编码域、标示符域、长度域以及数据域。

数据域：包含认证相关的信息。典型的数据域由类型子域以及数据类型域组成，类型子域表示了该 EAP 信息包含的数据的类型。

EAP 成功与失败信息中不包含数据域。

EAP 认证交换的具体过程如下。首先，低层交换协议建立 EAP 交换的需求，然后，认证者向被认证端发出进行身份验证的请求，接着被认证端发出包含身份信息的应答。这些过程伴随着一连串的验证实体的请求以及被认证端的应答，从而实现认证信息的交换。交换的信息以及请求-应答对的数量依赖于认证的方法。会话过程一直继续，直到满足下面两条之一：（1）认证者无法认证该被认证端，传送 EAP 失败信息；（2）认证者成功认证该被认证端，传送 EAP 成功信息。

图 5.4 给出了一个 EAP 交换的例子。其中，EAP 被认证端使用 EAP 之外的其他协议向认证者发送请求信息或信号，请求进行 EAP 交换，从而获得网络的访问权的过程没有在图中展示。可以使用 IEEE 802.1X 协议完成上述过程，我们将在下一部分介绍该协议。第一对 EAP 请求应答信息是身份类型验证信息，认证者请求被认证端的身份标识，被认证端在应

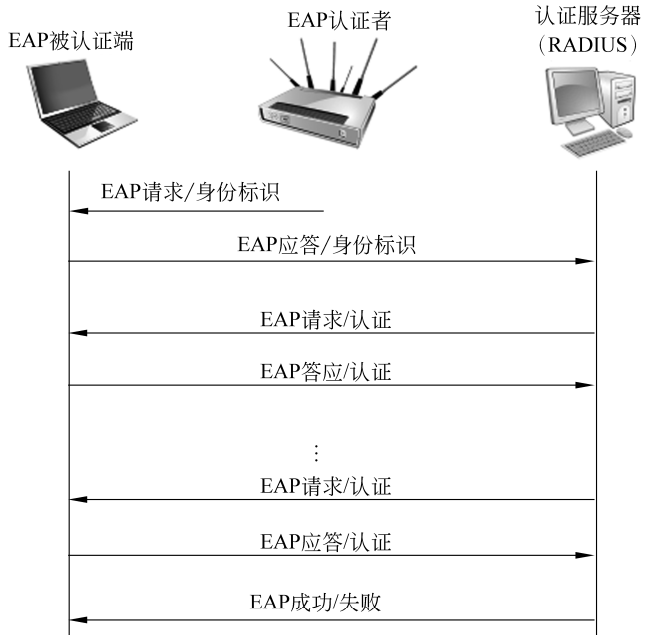

图 5.4　透传模式下的 EAP 信息流

答信息中返回声称的身份标识。应答信息通过认证者转发给认证服务器。随后的 EAP 信息在被认证端以及认证服务器之间进行交换。

当从被认证端收到身份应答信息后，服务器选择一个 EAP 方法，发送第一个 EAP 信息，在该信息中包含与认证方法相关的类型域。如果认证者支持并且同意该 EAP 方法，它用相同类型的应答信息回复。否则，被认证端发送 NAK 应答，EAP 服务器或者选择另一个 EAP 方法，或者终止此次 EAP 执行过程，同时返回失败信息。选择的 EAP 方法决定了请求/应答对的数量。在交换过程中包括密钥信息的认证信息被交换。当服务器决定认证成功或者认证失败且客户端不再尝试时，交换过程结束。

5.3　IEEE 802.1X 基于端口的网络访问控制

IEEE 802.1X 基于端口的网络访问控制是用来为局域网提供访问控制功能的。表 5.1 简要地说明了在 IEEE 802.11 标准中定义的关键术语。在此处的请求者、网络访问点、认证服务器跟 EAP 中的被认证端、认证者、认证服务器一一对应。

表 5.1　与 IEEE 802.1X 相关的术语

认证者
在点到点局域网段一端的实体，对该连接另一端的实体进行认证
认证交换
执行认证过程的系统之间的双方的对话
认证过程
真正用于进行认证的密码操作以及支持的数据帧
认证服务器（AS）
向认证者提供认证服务的实体。根据请求者提供的证书，认证服务决定了请求者是否被授权访问由认证者从属的系统提供的服务
认证传输
在两个系统之间传输认证交换数据包的会话
桥端口
IEEE 802.1D 桥或者 IEEE 802.1Q 桥的端口
边缘端口
只有一个桥端口连接到局域网上的端口
网络访问端口
一个系统连接到局域网上的附着点。可以是物理端口，如一个局域网 MAC 连接到一个物理的局域网段，也可以是一个逻辑端口，比如一个工作站和一个访问点之间的 IEEE 802.11 联系
端口访问实体（PAE）
协议实体跟一个端口相关联。它支持与认证者或/和请求者相关联的协议功能
请求者
在点对点局域网段一端的实体，该实体请求在该连接另一端的认证者的认证

直到认证服务器认证通过了请求者之前（使用认证协议），认证者只能在请求者与认证服务器之间传递控制与认证信息；IEEE 802.1X 控制通道是无阻塞的，但是 IEEE 802.11 数据通道是阻塞的。一旦请求者被认证通过，而且获得了密钥，认证者就可以将来自请求者

的且满足预先定义的访问控制约束的数据转发给企业网络。在这些情况下，数据通道是无阻塞的。

如图 5.5 所示，IEEE 802.1X 使用了受控端口与未受控端口的概念。端口是在认证者之间定义的逻辑实体，可以参照物理网络连接的概念。每一个逻辑端口被映射到两种类型的物理端口中的某一种。未受控端口会忽略请求者的认证状态，允许在请求者以及认证服务器之间交换协议数据单元。受控端口只有在当前请求者被授权允许进行交换时，才可以在请求者与网络上的其他系统间交换协议数据单元。

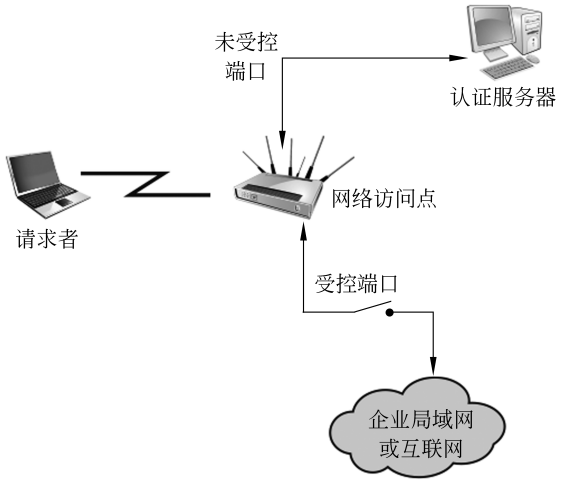

图 5.5　IEEE 802.1X 访问控制

在 IEEE 802.1X 中主要定义了 EAPOL 协议（局域网上的可扩展认证协议）。EAPOL 协议作用在网络层上，使用了 IEEE 802 标准的局域网，如数据链路层上的以太网、Wi-Fi 等。为了进行认证，EAPOL 允许请求者与认证者之间互相通信，以及两者之间进行 EAP 包的交换。

表 5.2 中列出了最常见的 EAPOL 包。当请求者第一次连接到局域网时，他不知道认证者的 MAC 地址。事实上，请求者根本不知道局域网中是否有认证者。请求者通过向 IEEE 802.1X 认证者使用的特殊的多播群组地址发送 **EAPOL-Start** 包，判断该网络中是否存在认证者，如果存在，则通知该认证者请求已经准备好。在很多情况下，硬件会通知认证者有新的设备连接到该网络中。比如，在插到集线器的设备发送任何数据之前，集线器就已经通过电缆的插入感知到设备的存在。在这种情况下，认证者可能会用自己发出的信息取代 EAPOL-Start 信息。不论在哪种情况下，认证者都会发送 EAP 请求身份标识信息，该信息

表 5.2　常用 EAPOL 帧类型

帧类型	定　义
EAPOL-EAP	包含封装的 EAP 包
EAPOL-Start	请求者可以发出这个包，代替等待从认证者发来的挑战
EAPOL-Logoff	当请求者完成对该网络的使用时，用来返回未被授权的端口的状态
EAPOL-Key	用来交换密码系统的密钥信息

被封装在 EAPOL-EAP 包中。**EAPOL-EAP** 是在传输 EAP 包时使用的 EAPOL 帧类型。

一旦决定允许请求者接入网络，认证者就使用 EAP-key 包向请求者发送密钥。EAP-Logoff 包类型表示请求者希望同该网络断开连接。

EAPOL 的数据包格式由下面一些域组成：

协议版本：EAPOL 的版本类型。

包类型：EAPOL 包的类型，如开始、EAP、密钥、注销等。

包主体的长度：如果 EAPOL 包包含一个主体，这个域表示了包体的长度。

包主体：EAPOL 包的有效载荷，如 EAP 包。

图 5.6 展示了一个使用 EAPOL 进行交换的例子。在第 7 章将介绍在 IEEE 802.11 无线局域网安全中如何使用 EAP 和 EAPOL。

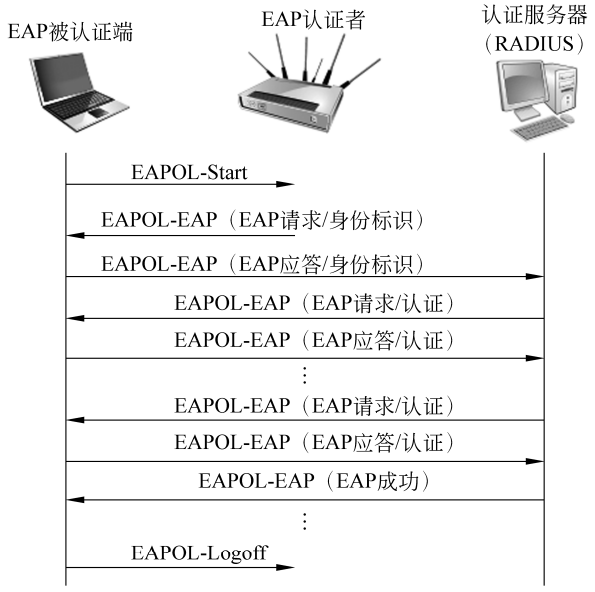

图 5.6　IEEE 802.1X 时序示意图

5.4　云　计　算

当前，有越来越多的企业组织将它们大部分的甚至全部的信息技术操作移动到连接网络的基础设施上，这个过程称为企业云计算。本节将给出云计算的概况。更详细的介绍，见[STAL16b]。

5.4.1　云计算组成元素

NIST 在 NIST SP-800-145（NIST 云计算定义）中对云计算做了如下定义。

云计算：云计算是一种能够通过网络以便利的、按需付费的方式获取计算资源（包括网络、服务器、存储、应用和服务等）并提高其可用性的模式，这些资源来自一个共享的、

可配置的资源池，并能够以最省力和无人干预的方式获取和释放。云模型由 5 个基本特征、3 个服务模型和 4 个部署模型组成。

这个定义提到了许多模型与特征，它们之间的关系如图 5.7 所示。云计算的主要特征如下。

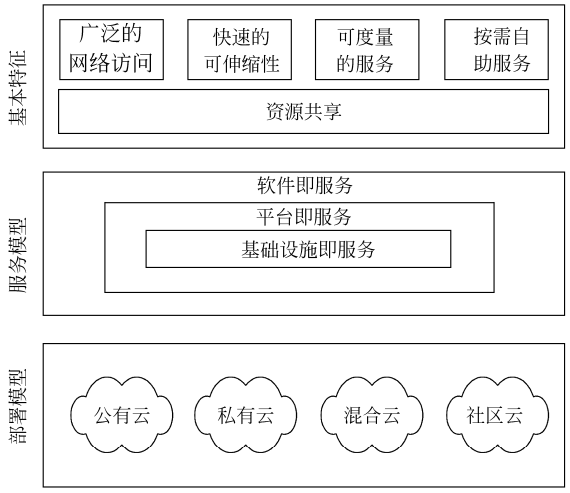

图 5.7　云计算组成元素

广泛的网络访问。具有通过规范机制网络访问的能力，这种机制可以使用各种各样的瘦客户端和胖客户端平台（例如，手机、笔记本电脑以及 PDA）以及其他传统的或者基于云计算的软件服务。

快速的可伸缩性。云计算可以根据用户独特的服务请求，可伸缩性地提供服务。比如，为了完成某项任务，有可能需要大量的服务资源。当完成这项任务后，可以释放这些资源。

可度量的服务。云系统通过一种可计量的能力杠杆，在某些抽象层上自动地控制并优化资源以达到某种服务类型（例如，存储、处理、带宽以及活动用户账号）。资源的使用可以被监视和控制，通过向供应商和用户提供这些被使用的服务报告以达到透明化。

按需自助服务。消费者可以单方面地按需自动获取计算能力，如服务器时间和网络存储，从而免去了与每个服务提供者进行交互的过程。因为服务是按需的，资源并不是都永久保存在 IT 基础设施上。

资源共享。提供商提供的计算资源被集中起来，通过一个多客户共享模型来为多个客户提供服务，并根据客户的需求，动态地分配或再分配不同的物理和虚拟资源。有一个区域独立的观念，就是客户通常不需要控制或者需要知道被提供的资源的确切位置，但是可能会在更高一层的抽象（例如，国家、州或者数据中心）上指定资源的位置。资源的例子包括存储设备、数据加工、内存、网络带宽和虚拟机等。即便是私有云也倾向于在同一组织的不同部分之间共享资源。

NIST 定义了 3 种**服务模型**，可以看作是嵌套的服务替代：

软件即服务（**SaaS**）。客户所使用的服务商提供的这些应用程序运行在云基础设施上。这些应用程序可以通过瘦客户端界面由各种各样的客户端设备所访问，如 Web 浏览器。企业不需要获得软件产品的桌面和服务器许可证就可以从云端获得相同的服务。使用这种类