志存高远 责任为先

网络访问控制与云安全

地址：赣州市红旗大道86号 信息工程学院
网址：www.jxust.edu.cn
邮编：341000

目录/Contents

01
Part

网络访问控制

5.1 网络访问控制(NAC)

- **用于管理网络访问的总称。**
- **对登录网络的用户进行身份验证，并确定他们可以访问哪些数据以及他们可以执行的哪些操作。**
- **检查用户计算机或移动设备（终端）的安全程序。**

网络访问控制系统的组成元素

访问请求者(AR)

- 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，摄像头和其他支持IP的设备。
- 也称为请求者或客户。

策略服务器

- 决定应授予请求者的访问权限。
- 通常依赖诸如杀毒、补丁管理，或者用户目录等后端系统的帮忙来决定主机的状况。

网络访问服务器(NAS)

- 用作连接到企业内部网络的远程用户的访问控制点。
- 也称为媒体网关，远程访问服务器（RAS）或策略服务器。
- 可以包括自己的身份认证服务，也可以依赖策略服务器的分离的认证服务

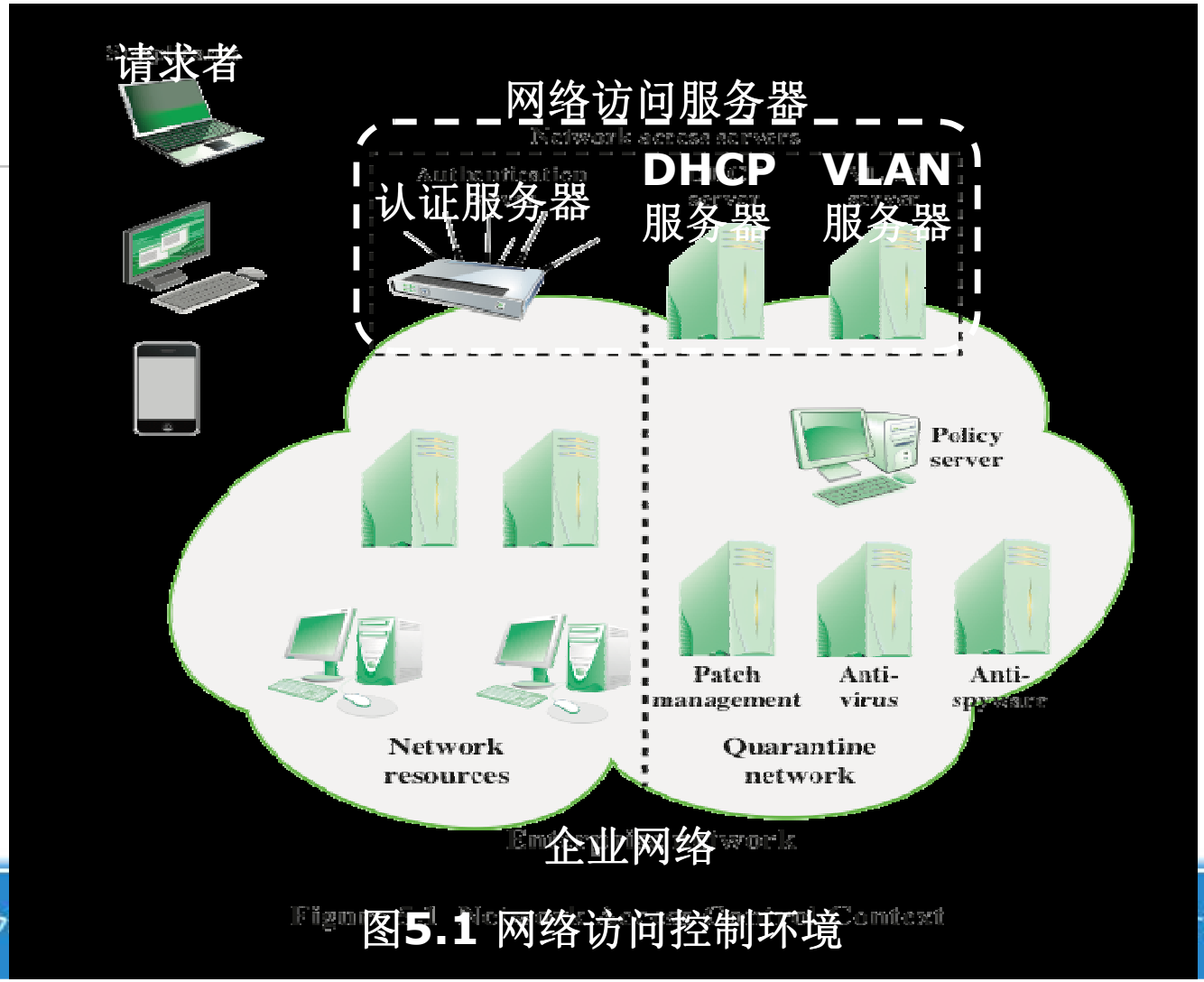


图5.1 网络访问控制环境

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操作。
- 许多供应商同时支持多种执行方法，允许客户使用一种方法或一种方法组合来定制配置。

常用的NAC强制措施：

- IEEE 802.1X
- 虚拟局域网(VLANs)
- 防火墙
- 动态主机配置协议DHCP

02
Part

可扩展认证协议

5.2 可扩展认证协议（EAP）

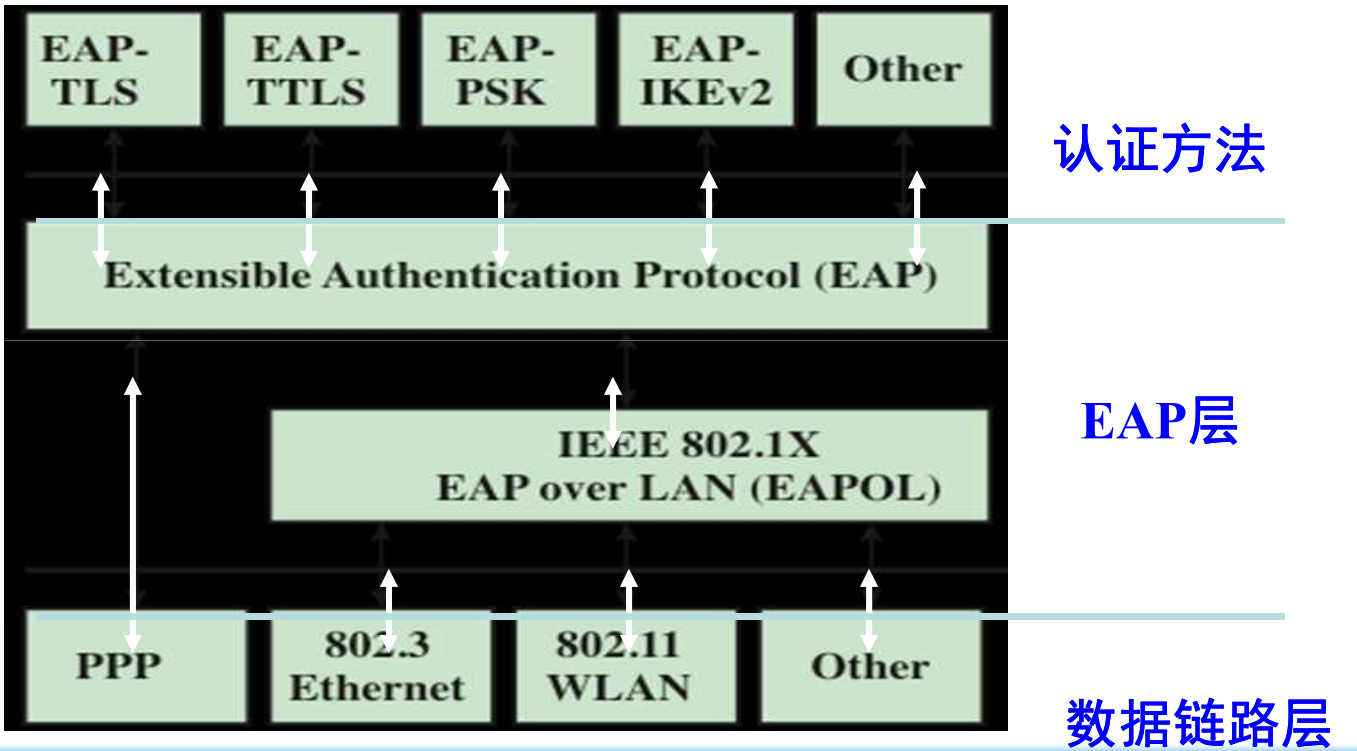


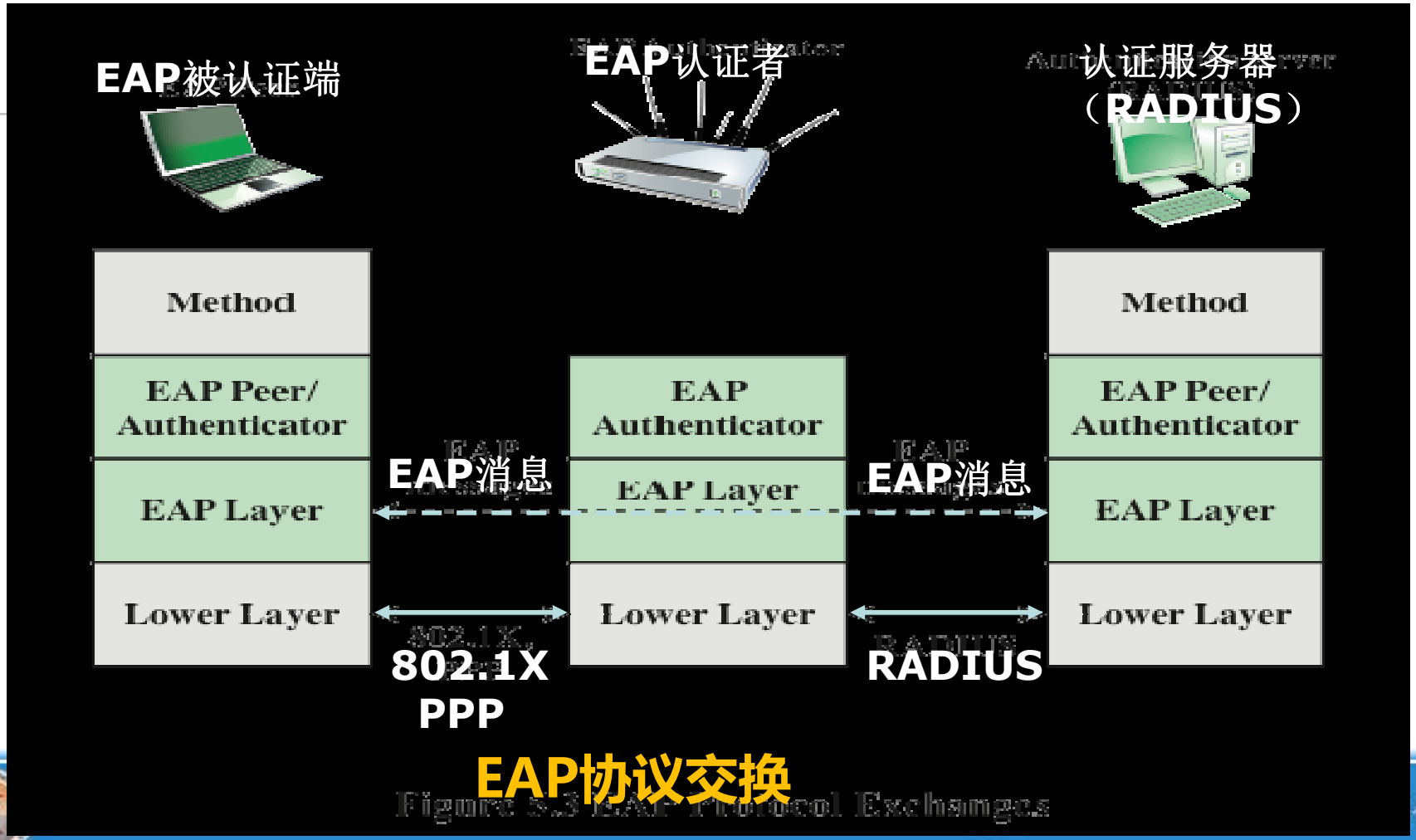
图5.2 EAP层级结构

5.2.1 认证方法

- EAP为客户端系统和身份认证服务器之间交换认证信息提供了一种通用传输服务。
- 通过使用安装在EAP客户端和身份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。
- EAP方法
  - EAP-TLS（EAP传输层安全性）
  - EAP-TTLS（EAP隧道TLS）
  - EAP-GPSK（EAP通用预共享密钥）
  - EAP-IKEv2

5.2.2 EAP交换协议

- 图5.3显示了使用EAP的典型的布局。涉及下列组件：
  - EAP被认证端：尝试访问网络的客户端计算机。
  - EAP认证者：需要EAP身份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被认证方的证书，并授权访问网络。 典型的认证服务器是远程用户拨号认证（RADIUS）服务器。


EAP被认证端
EAP认证者
认证服务器
（RADIUS）
Method
EAP Peer/
Authenticator
EAP Layer
Lower Layer
EAP
Authenticator
EAP Layer
Lower Layer
Method
EAP Peer/
Authenticator
EAP Layer
Lower Layer
EAP消息
EAP消息
802.1X
PPP
RADIUS
EAP协议交换

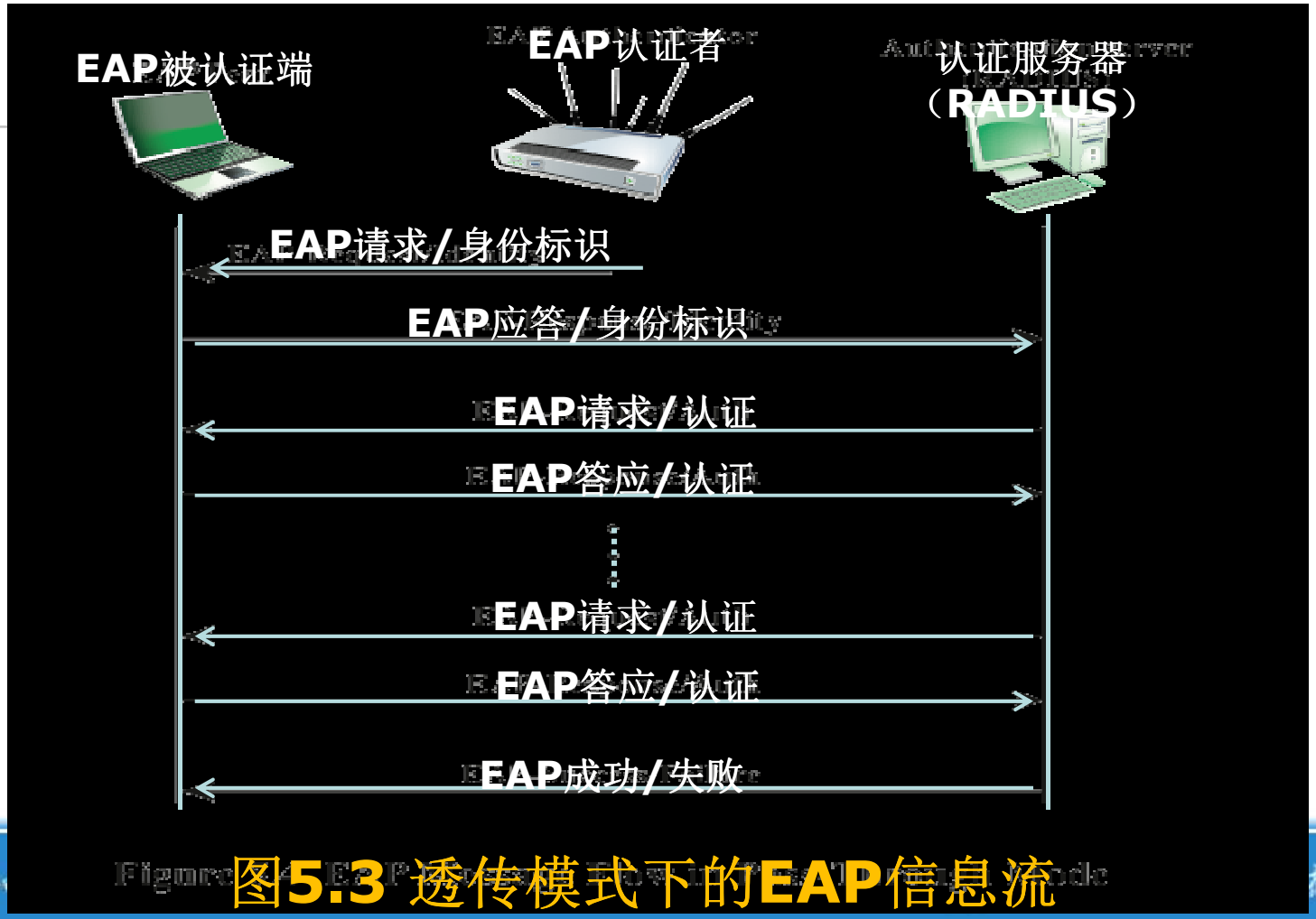


图5.3 透传模式下的EAP信息流

03
Part

IEEE 802.1X
基于端口的网络访问控制

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说明了在IEEE 802.1标准中定义的关键术语
- IEEE 802.1标准中术语　　EAP中术语
- 请求者 → 被认证端
- 网络访问点 → 认证者
- 认证服务器 → 认证服务器

Authenticator
An entity at one end of a point-to-point LAN segment that facilities authentication of the entity to the other end of the link.

Authentication exchange
The two-party conversation between systems performing an authentication process.

Authentication process
The cryptographic operations and supporting data frames that perform the actual authentication.

Authentication server (AS)
An entity that provides an authentication service to an authenticator. This service determines, from the credentials provided by supplicant, whether the supplicant is authorized to access the services provided by the system in which the authenticator resides.

Authentication transport
The datagram session that actively transfers the authentication exchange between two systems.

Bridge port
A port of an IEEE 802.1D or 802.1Q bridge.

Edge port
A bridge port attached to a LAN that has no other bridges attached to it.

Network access port
A point of attachment of a system to a LAN. It can be a physical port, such as a single LAN MAC attached to a physical LAN segment, or a logical port, for example, an IEEE 802.11 association between a station and an access point.

Port access entity (PAE)
The protocol entity associated with a port. It can support the protocol functionality associated with the authenticator, the supplicant, or both.

Supplicant
An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an authenticator attached to the other end of that link.

表 5.1
与IEEE 802.1X 相关的术语
（教材：p118)

802.1X访问控制

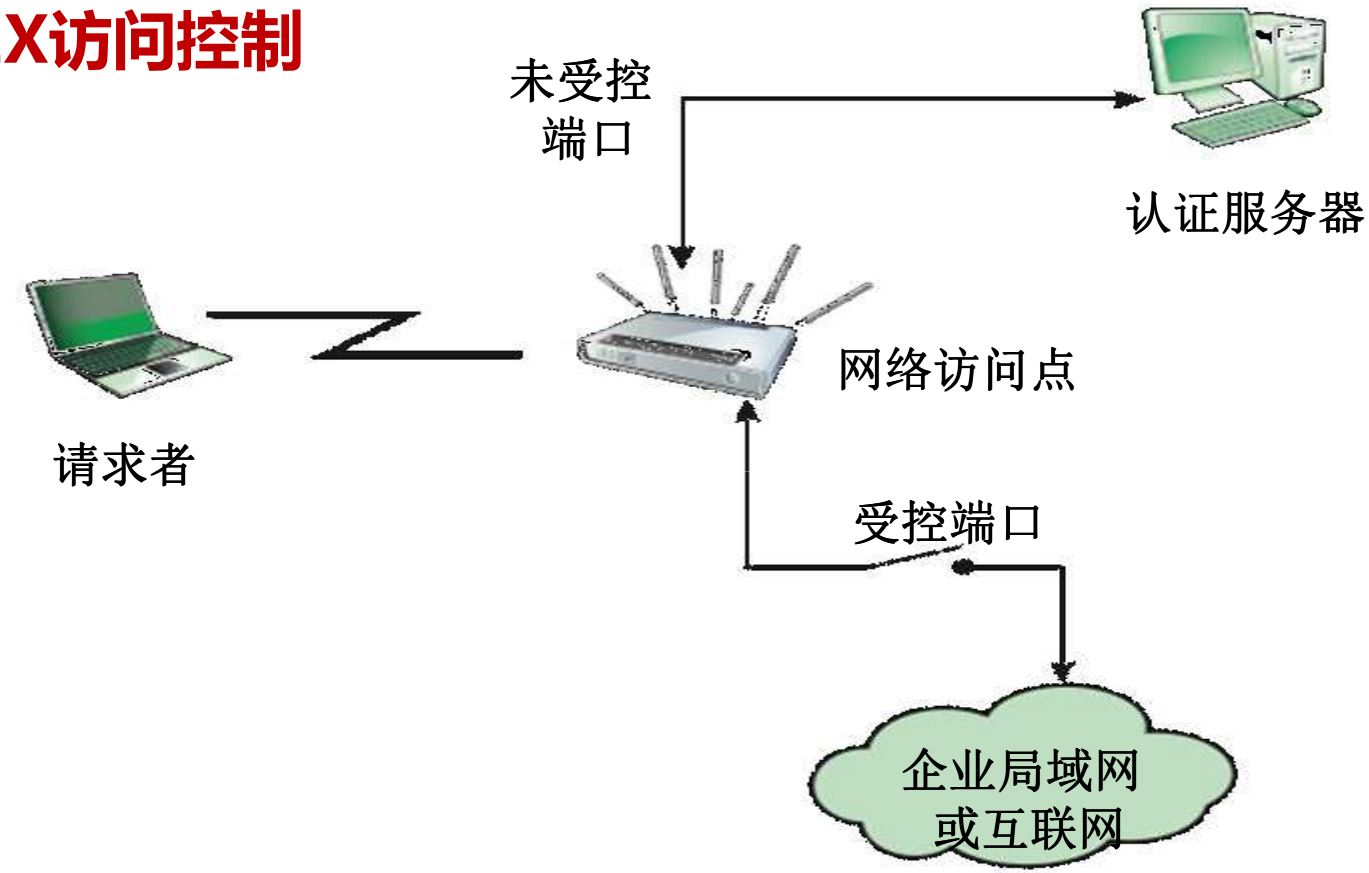
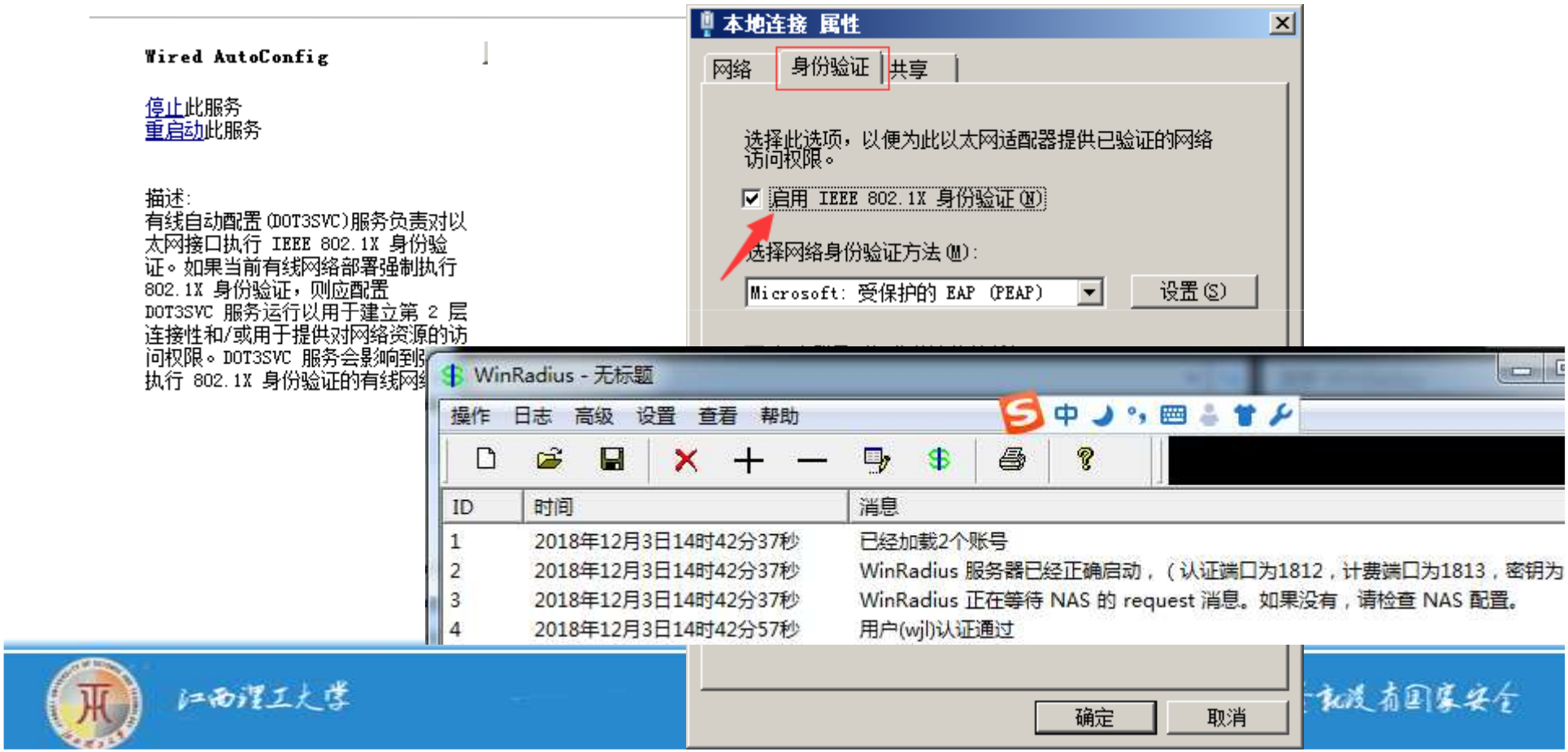


表5.2 常用EAPOL帧类型（p119）

Frame Type	Definition
EAPOL-EAP	Contains an encapsulated EAP packet.
EAPOL-Start	A supplicant can issue this packet instead of waiting for a challenge from the authenticator.
EAPOL-Logoff	Used to return the state of the port to unauthorized when the supplicant if finished using the network.
EAPOL-Key	Used to exchange cryptographic keying information.

图5.6 IEEE 802.1X时序示意图

实例


Wired AutoConfig
停止此服务
重启动此服务
描述:
有线自动配置(DOT3SVC)服务负责对以太网接口执行 IEEE 802.1X 身份验证。如果当前有线网络部署强制执行 802.1X 身份验证，则应配置 DOT3SVC 服务运行以用于建立第 2 层连接性和/或用于提供对网络资源的访问权限。DOT3SVC 服务会影响到
执行 802.1X 身份验证的有线网
本地连接 属性
网络
身份验证
共享
选择此选项，以便为此以太网适配器提供已验证的网络访问权限。
启用 IEEE 802.1X 身份验证(N)
选择网络身份验证方法(M):
Microsoft: 受保护的 EAP (PEAP)
设置(S)
确定
取消
WinRadius - 无标题
操作 日志 高级 设置 查看 帮助
ID 时间 消息
1 2018年12月3日14时42分37秒 已经加载2个账号
2 2018年12月3日14时42分37秒 WinRadius 服务器已经正确启动，（认证端口为1812，计费端口为1813，密钥为
3 2018年12月3日14时42分37秒 WinRadius 正在等待 NAS 的 request 消息。如果没有，请检查 NAS 配置。
4 2018年12月3日14时42分57秒 用户(wjl)认证通过
江西理工大学

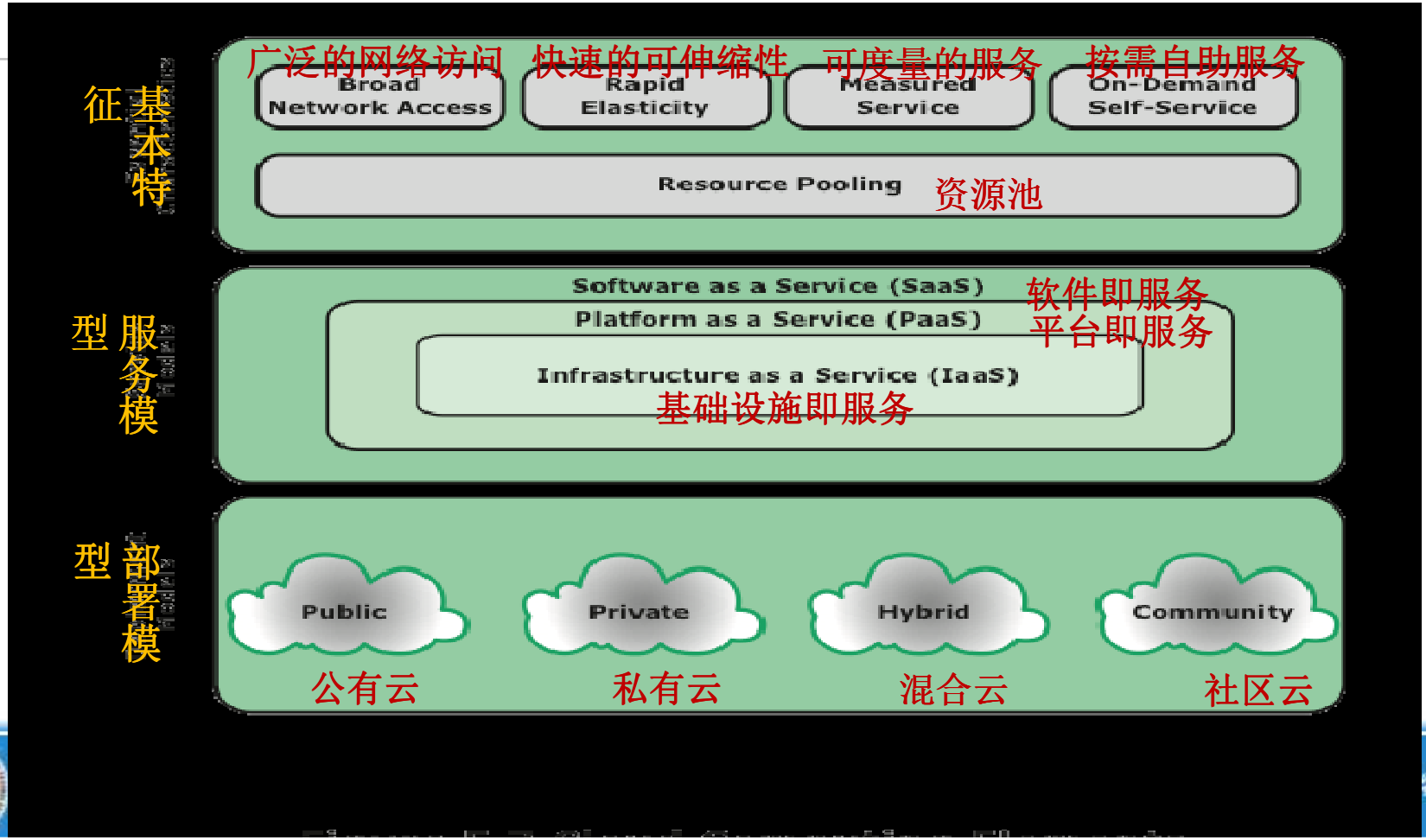
04
Part

云计算

5.4 云计算

- NIST在NIST SP-800-145（云计算的NIST定义）中定义了云计算，如下所示：
  - 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，这些资源来自一个可共享的、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。 云模型由五个基本特征、三个服务模型和四个部署模型组成。

5.4.1 云计算组成元素


征 基本特
广泛的网络访问
快速的可伸缩性
可度量的服务
按需自助服务
Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Resource Pooling
资源池
型 服务模
Software as a Service (SaaS)
软件即服务
Platform as a Service (PaaS)
平台即服务
Infrastructure as a Service (IaaS)
基础设施即服务
型 部署模
Public
Private
Hybrid
Community
公有云
私有云
混合云
社区云

5.4.2 云计算参考架构

- NIST云计算参考架构集中关注云服务商提供的服务，而不是怎样设计与实现解决方案。
- 图5.8说明了典型的云服务。 一个企业维护连接的企业LAN或互联网中的工作站，由路由器通过网络或Internet到云服务提供商。该云服务提供商维护着它管理的大量服务器，具有各种网络管理，冗余和安全工具。 在图中，云基础架构显示为刀片服务器的集合，这是一个共同的架构。

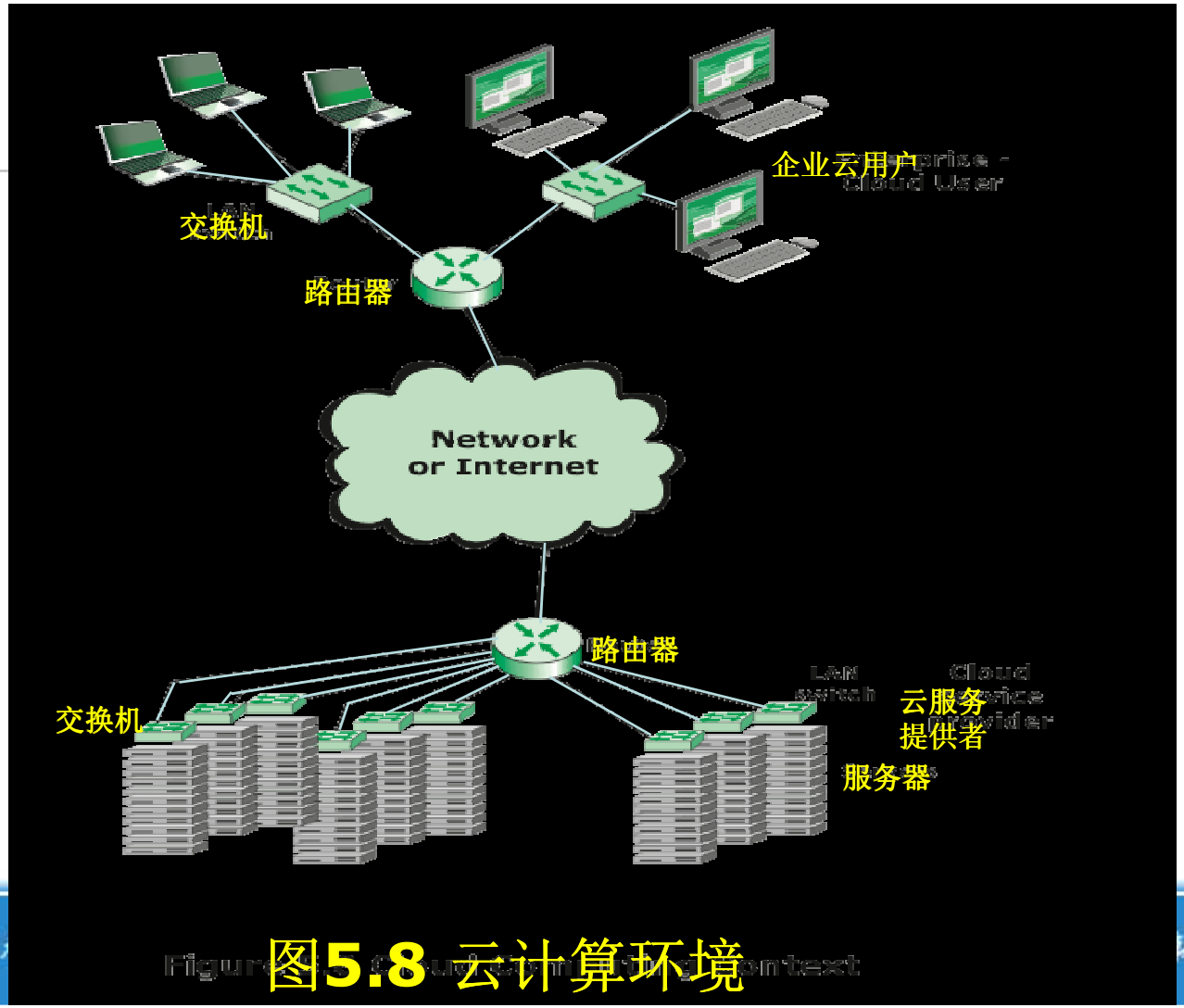


图5.8 云计算环境

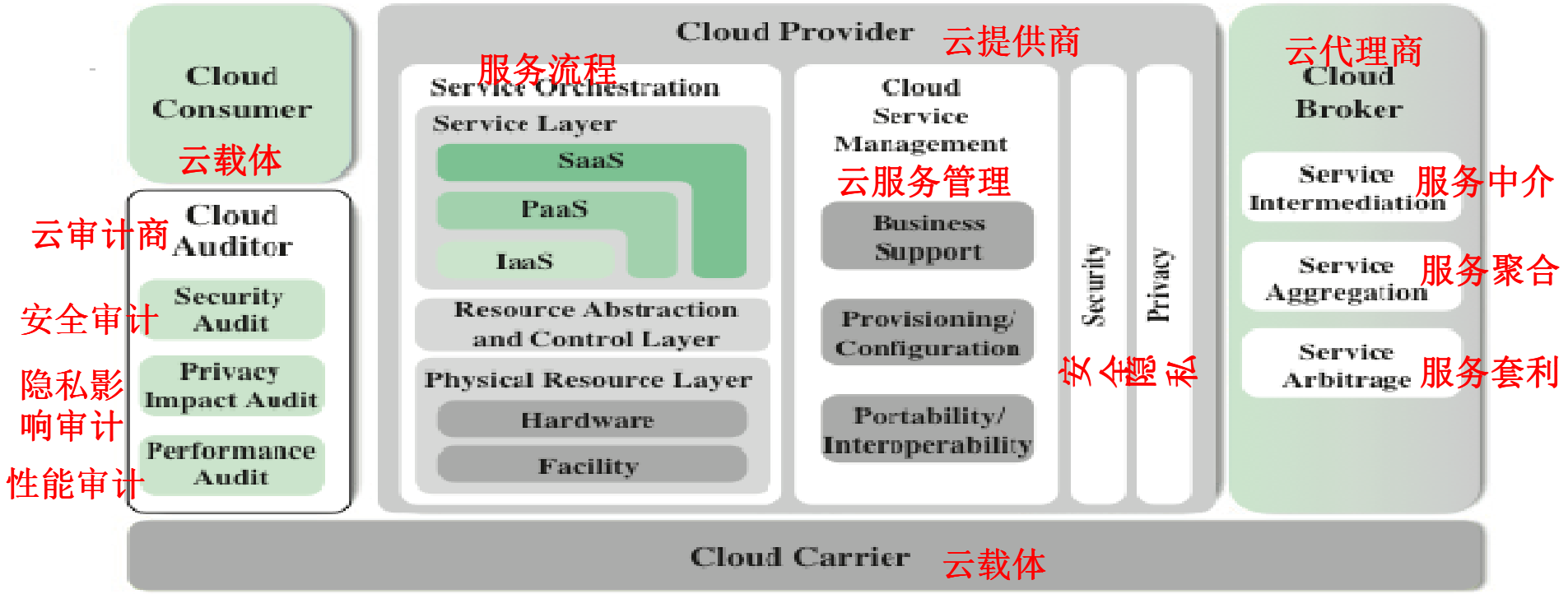


图5.9 NIST云计算参考架构

Figure 5.9 NIST Cloud Computing Reference Architecture

05
Part

云安全风险和对策

5.5 云安全风险和对策

- NIST参考架构旨在帮助理解云计算中的操作复杂性。 它不代表特定云计算系统的系统架构; 相反，它是一个使用共同参考框架描述，讨论和开发特定于系统的体系结构的工具。

5.5 云安全风险和对策

- **下面列出了云安全联盟提出的云安全方面的主要威胁以及建议的对策：**

滥用和恶意使用云计算

- 对策：（1）更严格的首次注册和验证过程；（2）加强信用卡欺诈监控和协调；（3）监督客户网络活动；（4）监控公共黑名单。

恶意内幕消息

- 对策：（1）实施严格的供应链管理，进行全面的供应商评估；（2）指定人力资源要求作为法律合同的一部分；（3）要求透明地了解整体信息安全和管理实践以及合规报告；（4）确定安全漏洞通知流程。

风险与对策（续）

- **帐户或服务劫持**

  对策：（1）禁止在用户和服务之间共享帐户证书;（2）尽可能利用强大的双因素身份验证技术;（3）采用主动监控来检测未经授权的活动;（4）理解提供商安全策略和SLA。

- **未知的风险**

对策：（1）公开适用的日志和数据;（2）部分/全部公开基础设施细节（补丁级别和防火墙）;（4）监控和警惕必要的信息。

风险与对策（续）

不安全的接口和API

对策：（1）分析CP接口的安全模型；（2）确保在加密传输过程中，进行认证以及访问控制；（3）理解与API关联的依赖链。

共享技术问题

对策：（1）安装/配置的最佳安全实践；（2）监控未经授权的变更/活动；（3）促进管理访问和操作的强认证和访问控制；（4）强制执行SLA以进行修补和漏洞修复；（5）进行漏洞扫描和配置审计。

数据丢失泄漏

对策：（1）实施强大的API访问控制；（2）对传输中的数据进行加密以及完整性认证；（3）在设计和运行时进行数据保护；（4）实施强大的密钥生成，存储和管理以及销毁实践

06
Part

云端数据保护

5.6 云端数据保护

云安全涉及许多方面的内容，也有提供云安全的防护措施。 再进一步示例见于NIST在SP-800-14中定义的云计算的指南中看到，在表5.3中列出了该指南。

Governance

Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services.

Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.

Compliance

Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements.

Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.

Trust

Ensure that service arrangements have sufficient means tc allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time.

Establish clear, exclusive ownership rights over data.

Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system.

Continuously monitor the security state of the information system to support ongoing risk management decisions.

Architecture

Understand the underlying technologies that the cloud prcvider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.

Identity and access management

Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.

Software isolation

Understand virtualization and other logical isolation techriques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.

表 5.3

NIST安全和隐私问题指南和建议

（第1页，共2页）

Data protection

Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.

Take into consideration the risk of collating organizational data with those of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value.

Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.

Availability

Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements.

Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.

Incident response

Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization.

Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.

Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

表 5.3

NIST安全和隐私问题指南和建议

（第2页，共2页）

云中的数据保护

- 数据泄露的威胁在云中增加
- 云计算中使用的数据库环境可能有很大差异

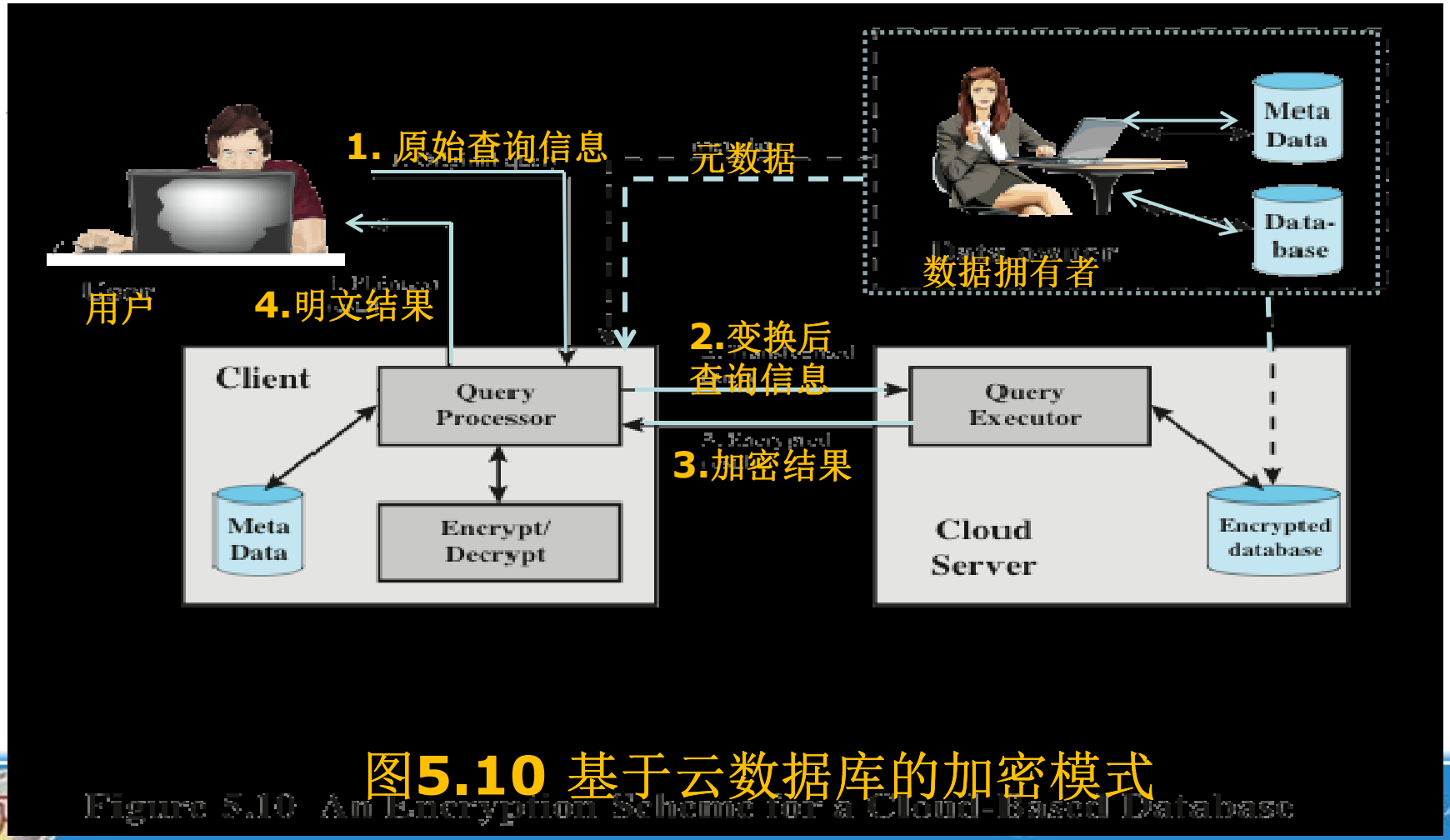


图5.10 基于云数据库的加密模式

Figure 5.10 An Encryption Scheme for a Cloud-Based Database

07
Part

云安全即服务

5.7 云安全即服务（SecaaS）

- **云安全即服务（SecaaS）由云安全提供商来提供一系列安全服务。提供的典型服务有认证、杀毒/间谍软件、入侵检测及安全事件管理。**

云安全联盟已确定以下SecaaS服务类别：

- 身份识别和访问管理
- 数据丢失防护
- Web安全
- 电子邮件安全
- 安全评估
- 入侵管理
- 安全信息和事件管理

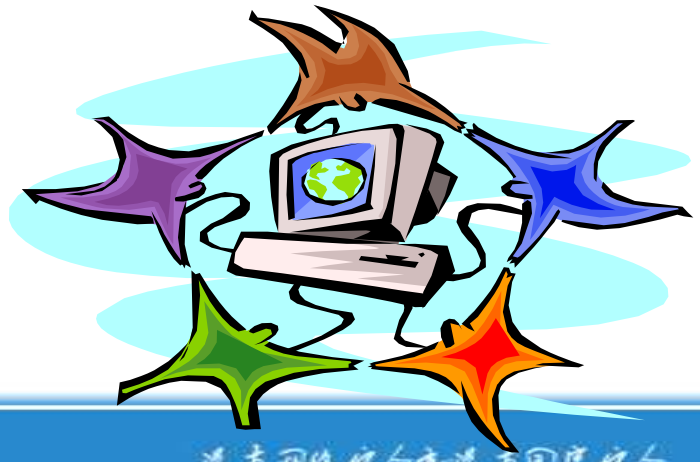


图5.11 云安全即服务的组成要素

小结

- 网络访问控制
- 可扩展认证协议
- IEEE 802.1X基于端口的网络访问控制
- 云计算

志存高远 责任为先

感谢聆听

网址：www.jxust. edu.cn
邮编：341000