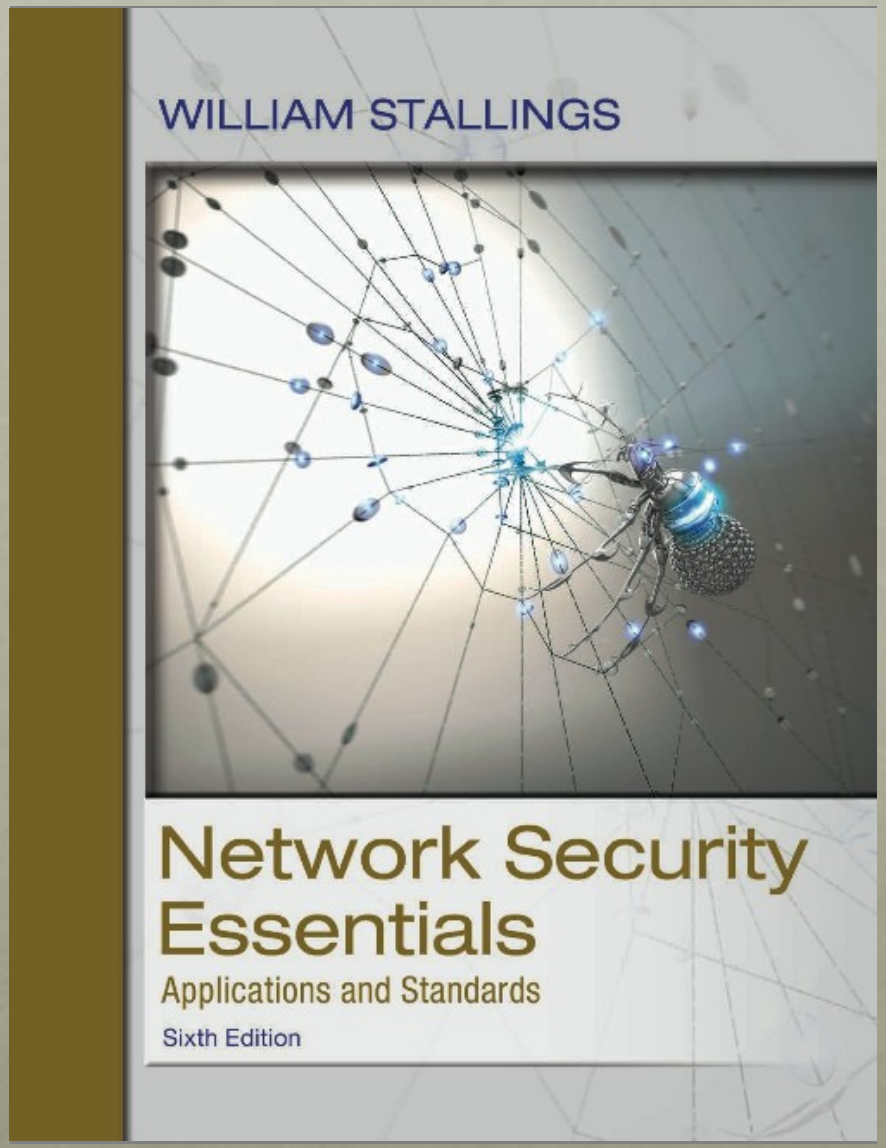
Network Security Essentials

Sixth Edition

by William Stallings



© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Chapter 5

Network Access Control and Cloud Security

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Network Access Control (NAC)

- An umbrella term for managing access to a network
- Authenticates users logging into the network and determines what data they can access and actions they can perform
- Also examines the health of the user's computer or mobile device

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

NAC systems deal with three categories of components:

• Access requestor (AR): The AR is the node that is attempting to access the network and may be any device that is managed by the NAC system, including workstations, servers, printers, cameras, and other IP-enabled devices. ARs are also referred to as supplicants , or simply, clients.

• Policy server: Based on the AR's posture and an enterprise's defined policy, the policy server determines what access should be granted. The policy server often relies on backend systems, including antivirus, patch management, or a user directory, to help determine the host's condition.

• Network access server (NAS): The NAS functions as an access control point for users in remote locations connecting to an enterprise's internal network. Also called a media gateway, a remote access server (RAS), or a policy server, an NAS may include its own authentication services or rely on a separate authentication service from the policy server.

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

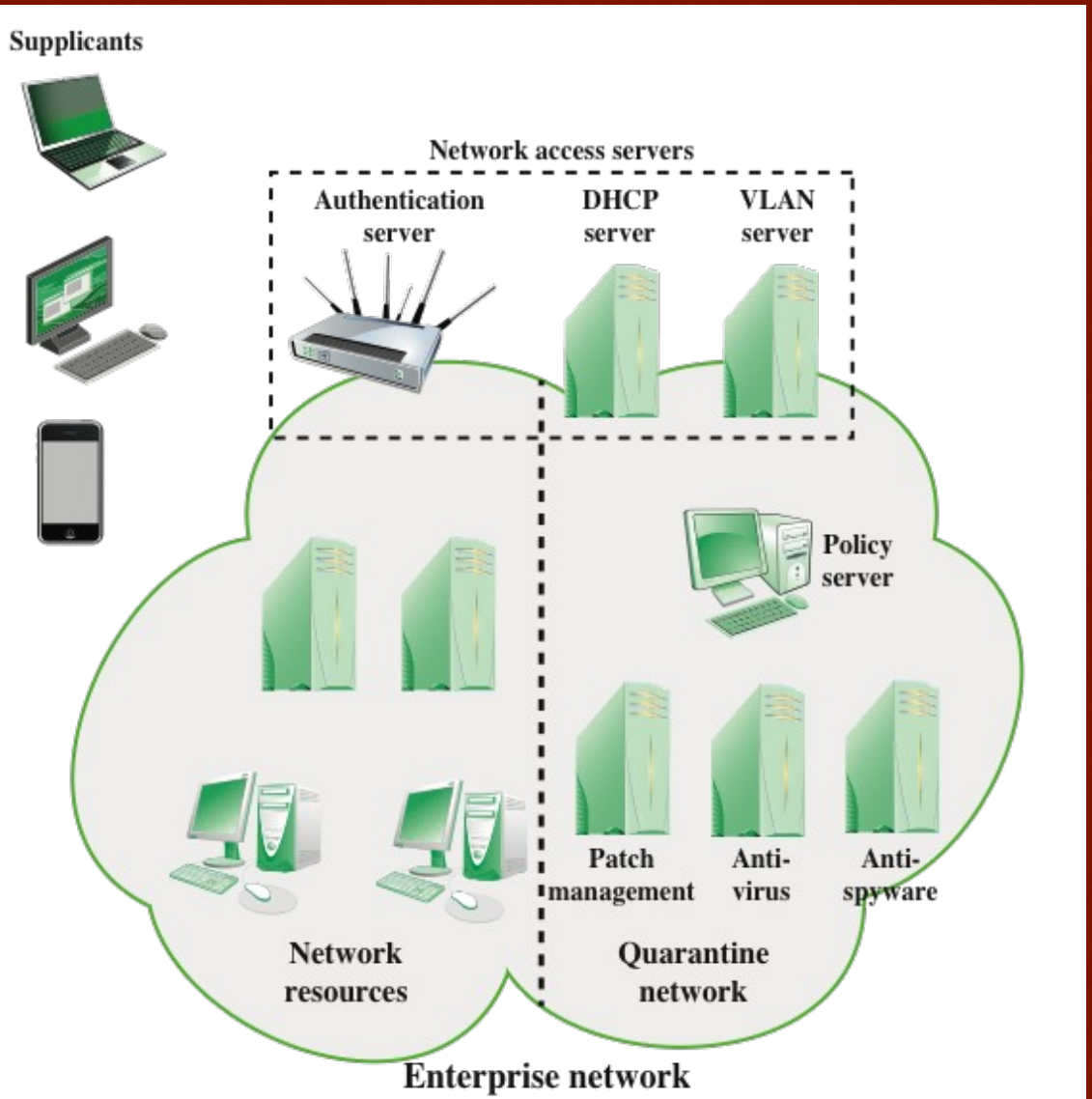


Figure 5.1 Network Access Control Context

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Network Access Enforcement Methods

- The actions that are applied to ARs to regulate access to the enterprise network
  - Many vendors support multiple enforcement methods simultaneously, allowing the customer to tailor the configuration by using one or a combination of methods

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

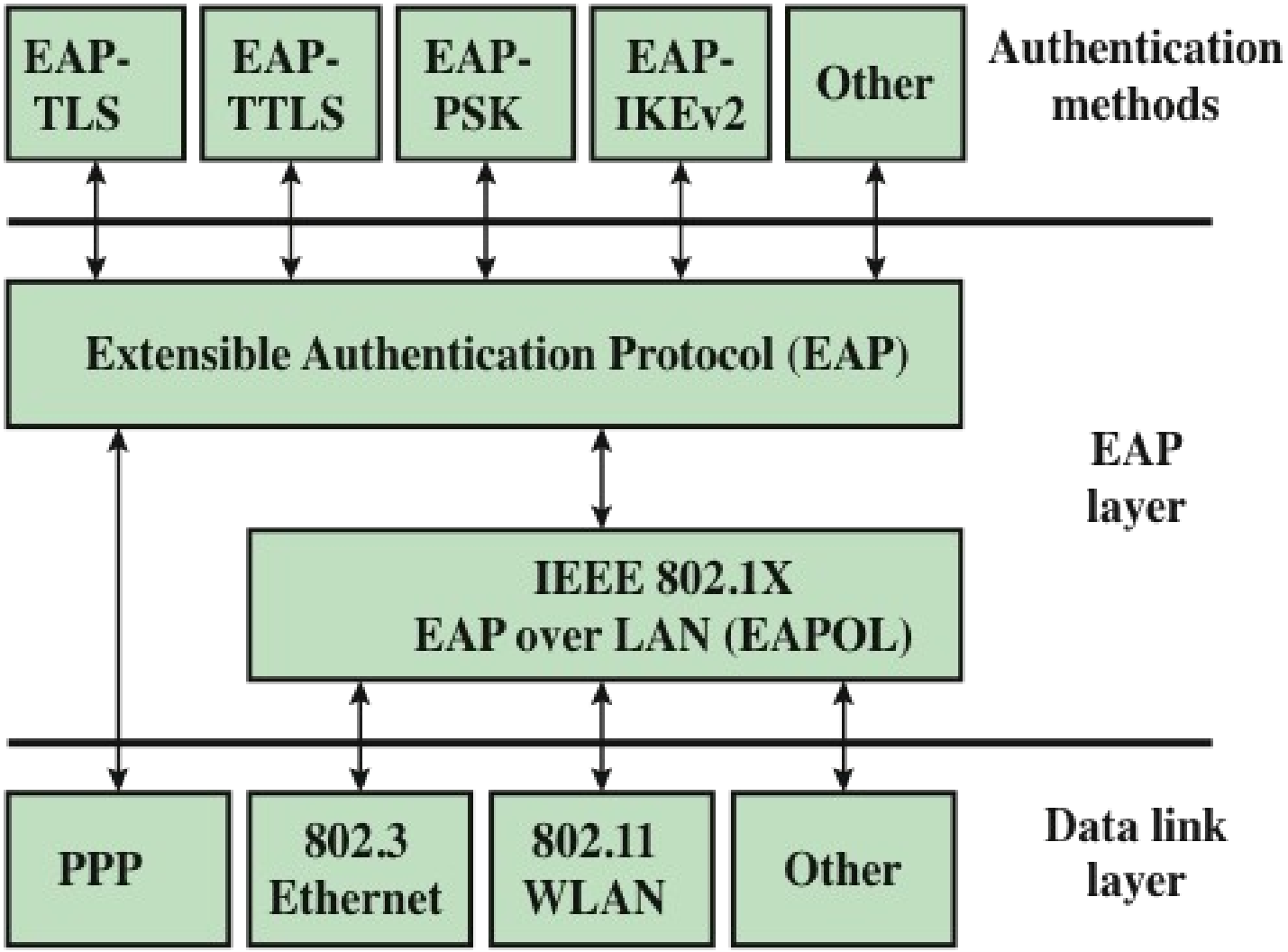


Figure 5.2 EAP Layered Context

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Authentication Methods

- EAP provides a generic transport service for the exchange of authentication information between a client system and an authentication server
- The basic EAP transport service is extended by using a specific authentication protocol that is installed in both the EAP client and the authentication server

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

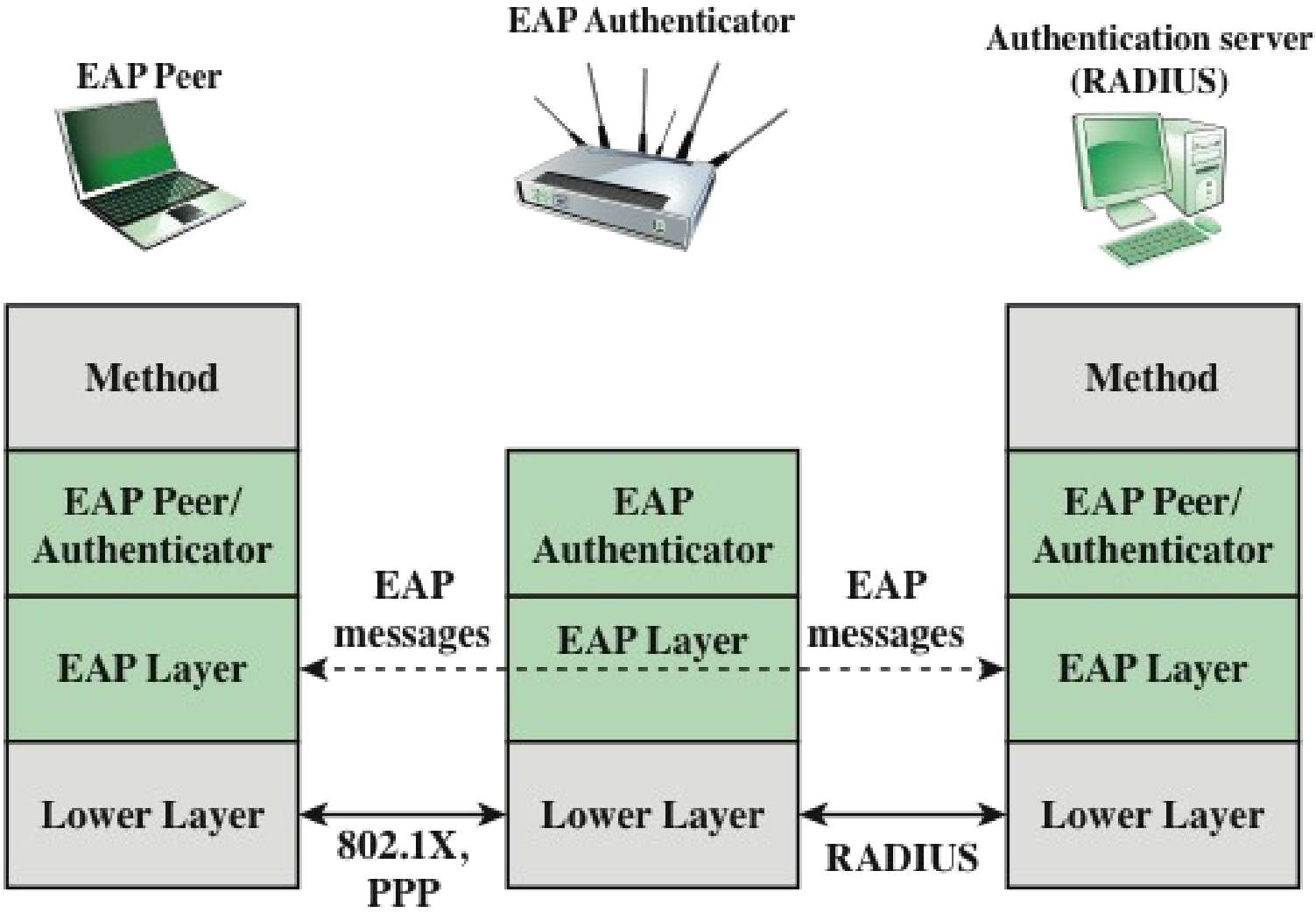


Figure 5.3 EAP Protocol Exchanges

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

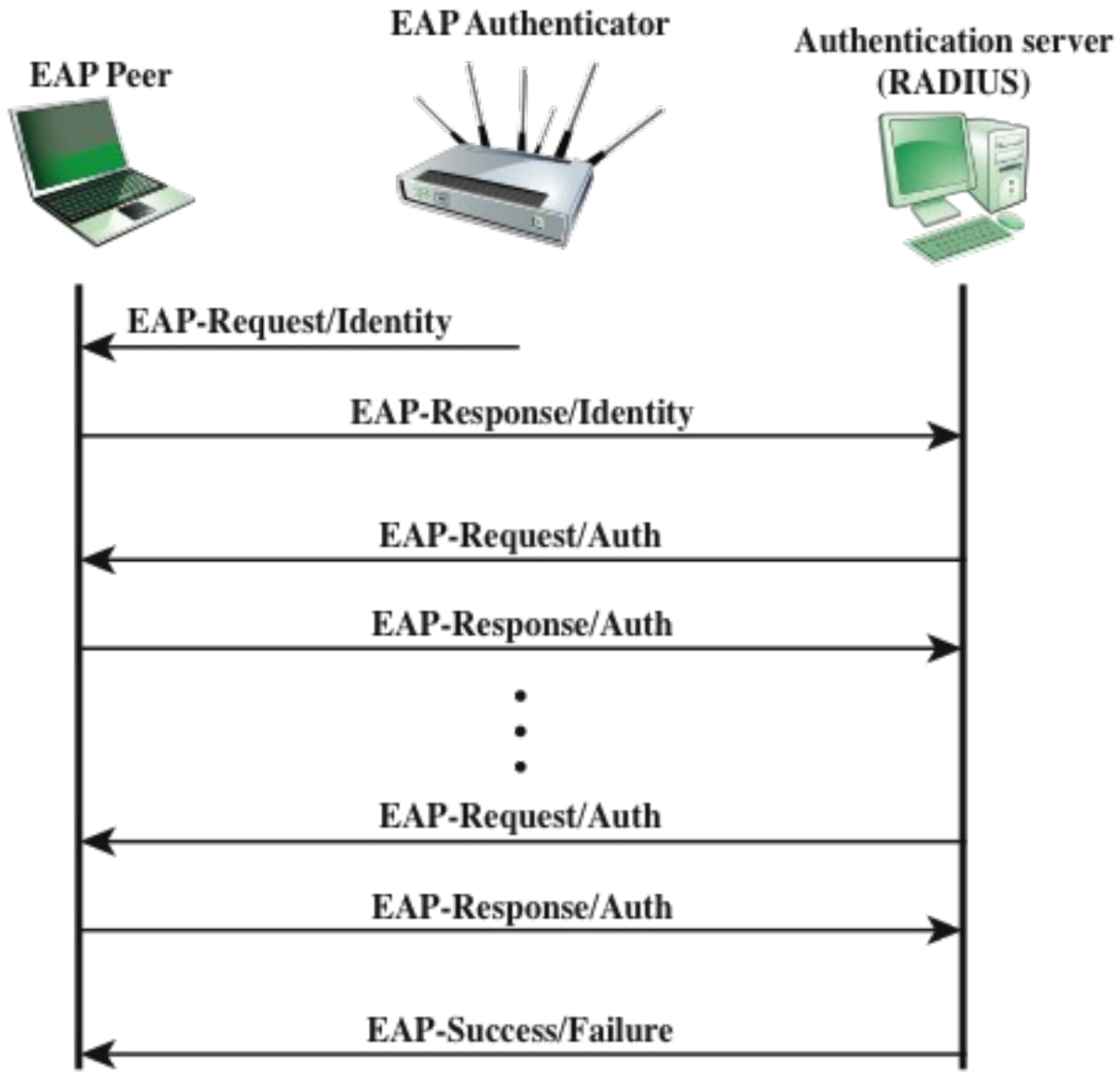


Figure 5.4 EAP Message Flow in Pass-Through Mode

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

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.

Table 5.1

Terminology Related to IEEE 802.1X

(Table can be found on page 152 in textbook)

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

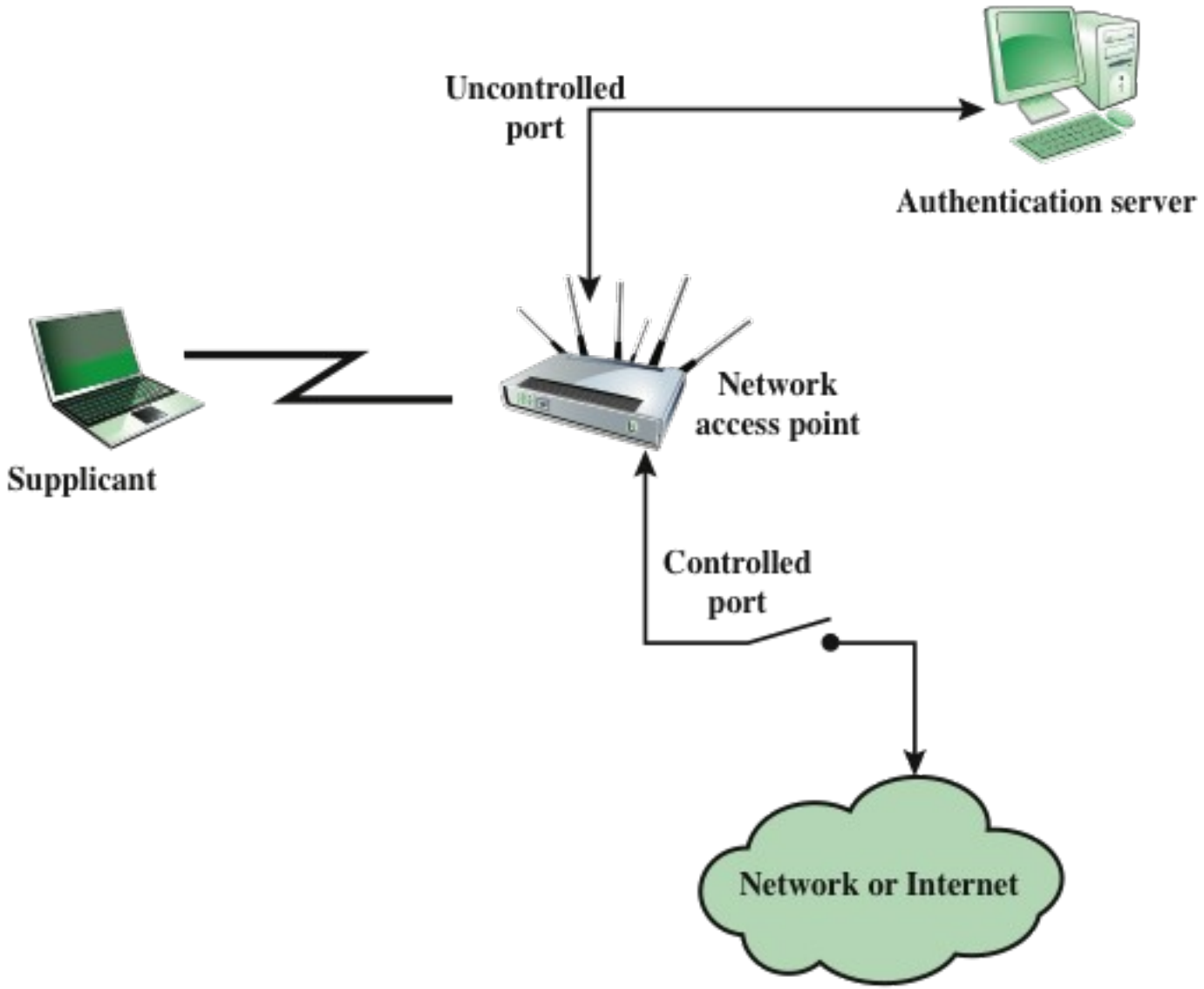


Figure 5.5 802.1X Access Control

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Table 5.2
Common EAPOL Frame Types

EAPOL-Start
EAP Request
EAPOL-EAP

EAPOLEAP is the EAPOL frame type used for transporting EAP packets.

The authenticator uses the EAP-Key packet to send cryptographic keys to the supplicant once it has decided to admit it to the network.

The EAP-Logoff packet type indicates that the supplicant wishes to be disconnected from the network.

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

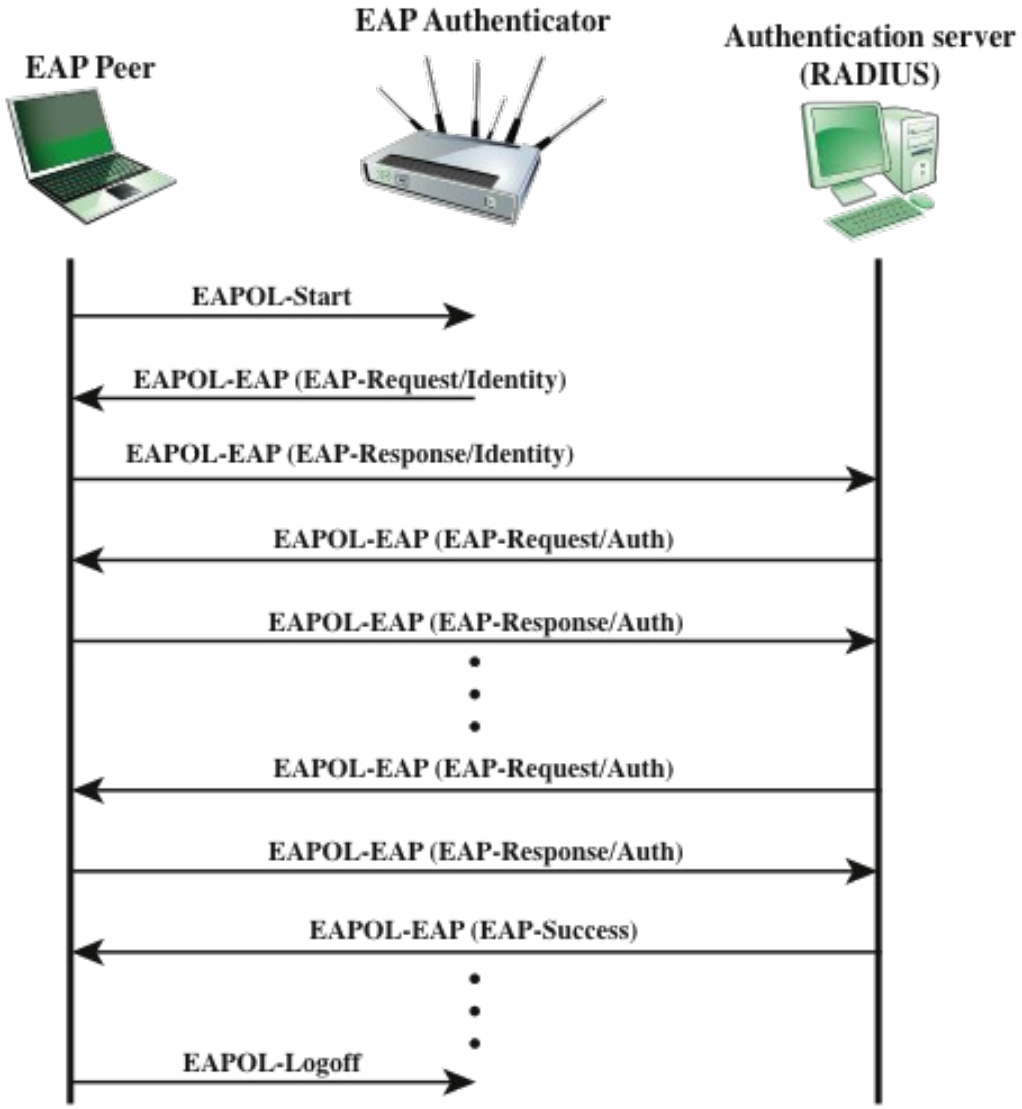


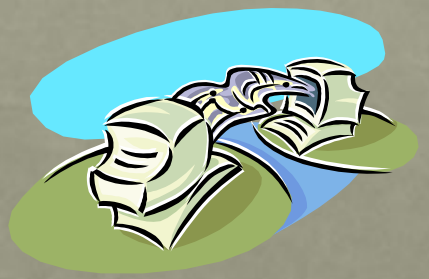
Figure 5.6 Example Timing Diagram for IEEE 802.1X

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Cloud Computing

- NIST defines cloud computing, in NIST SP-800-145 (The NIST Definition of Cloud Computing), as follows:

  "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."



© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

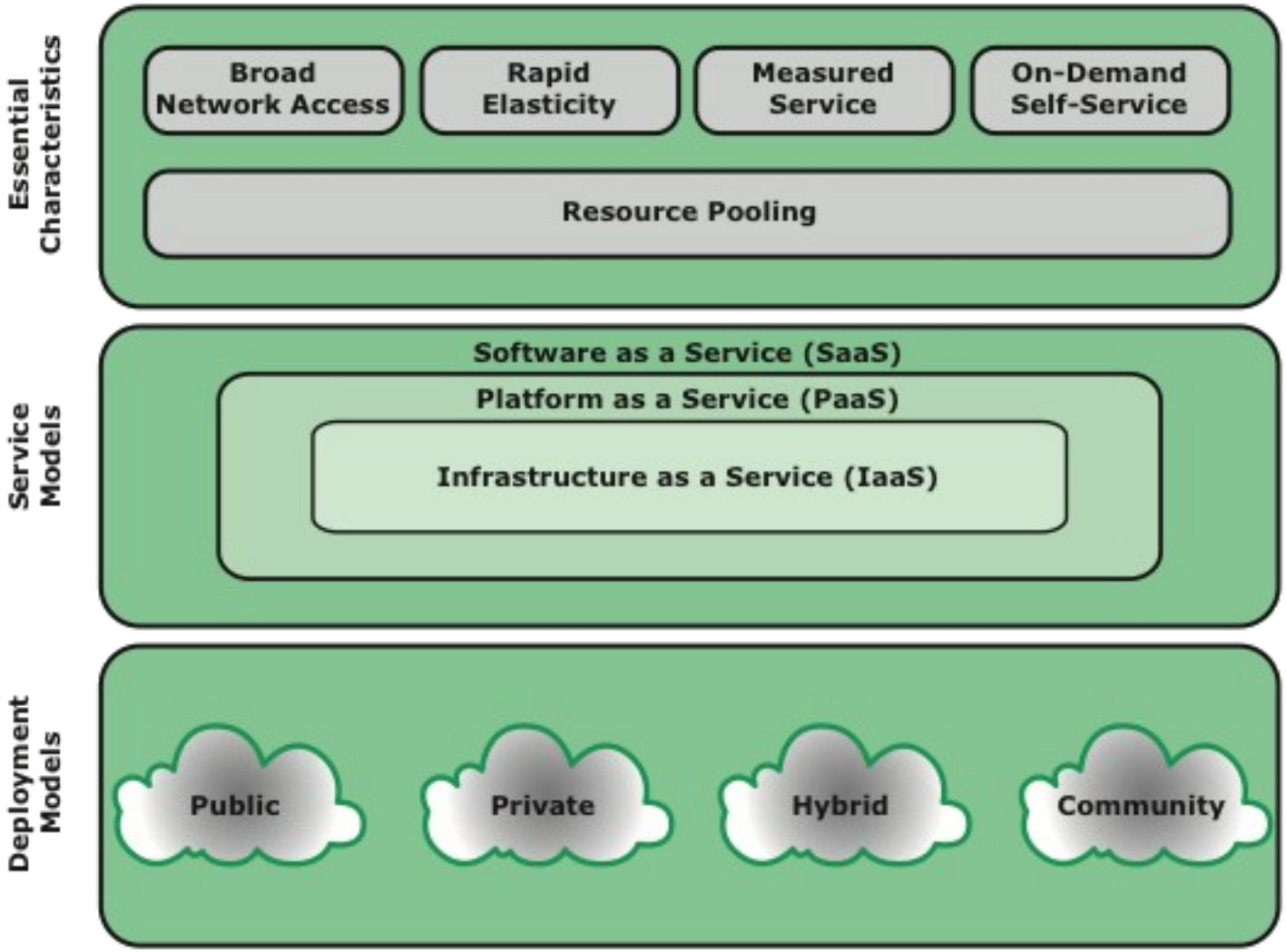


Figure 5.7 Cloud Computing Elements

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

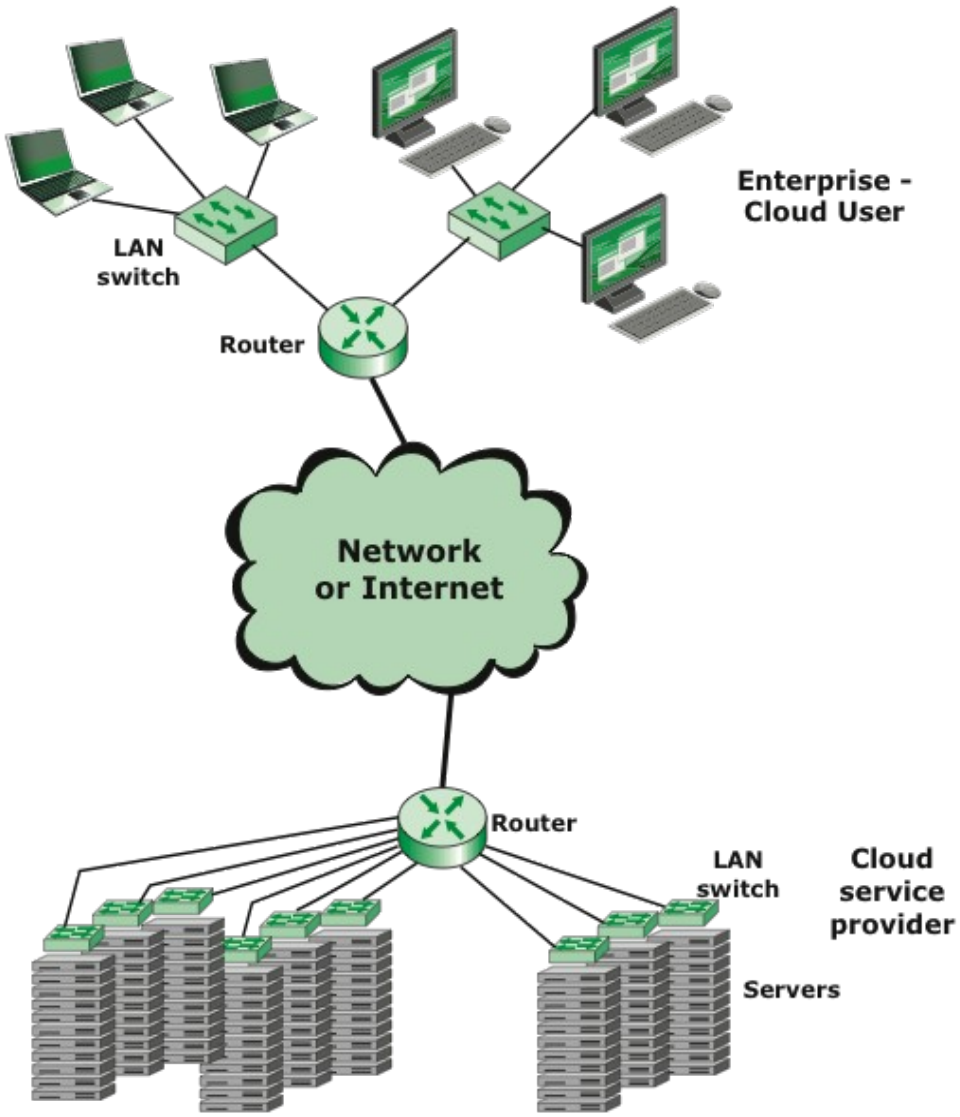


Figure 5.8 Cloud Computing Context

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Cloud Computing Reference Architecture

- NIST SP 500-292 (NIST Cloud Computing Reference Architecture) establishes a reference architecture, described as follows:

  "The NIST cloud computing reference architecture focuses on the requirements of "what" cloud services provide, not a "how to" design solution and implementation. The reference architecture is intended to facilitate the understanding of the operational intricacies in cloud computing. It does not represent the system architecture of a specific cloud computing system; instead it is a tool for describing, discussing, and developing a system-specific architecture using a common framework of reference."

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

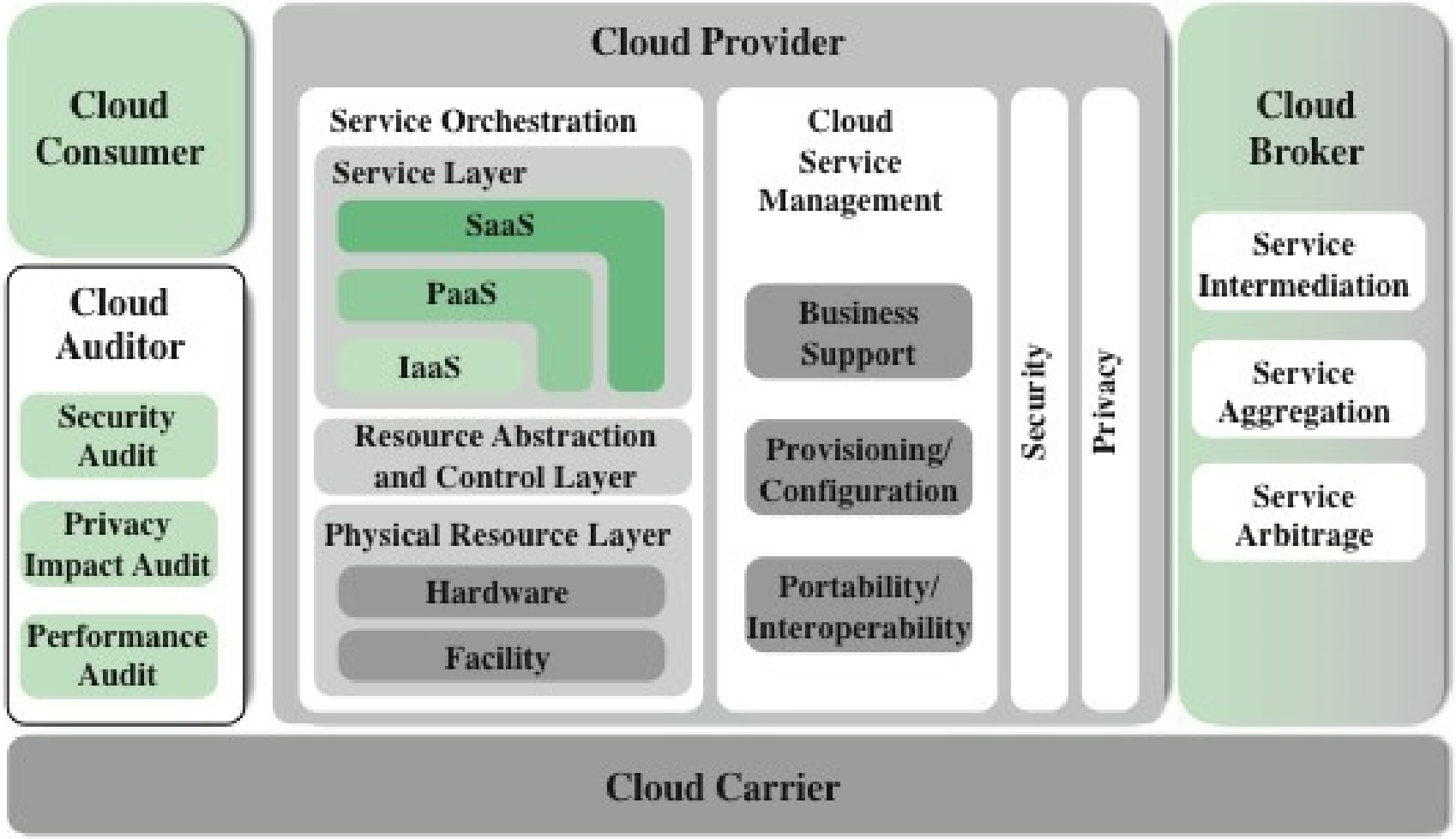


Figure 5.9 NIST Cloud Computing Reference Architecture

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Roles and Responsibilities

The cloud carrier is a networking facility that provides connectivity and transport of cloud services between cloud consumers and CPs. Typically, a CP will set up service level agreements (SLAs) with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and may require the cloud carrier to provide dedicated and secure connections between cloud consumers and CPs.

A cloud broker is useful when cloud services are too complex for a cloud consumer to easily manage. Three areas of support can be offered by a cloud broker:

• Service intermediation: These are value-added services, such as identity management, performance reporting, and enhanced security.

• Service aggregation: The broker combines multiple cloud services to meet consumer needs not specifically addressed by a single CP, or to optimize performance or minimize cost.

• Service arbitrage: This is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a broker has the flexibility to choose services from multiple agencies. The cloud broker, for example, can use a credit-scoring service to measure and select an agency with the best score.

A cloud auditor can evaluate the services provided by a CP in terms of security controls, privacy impact, performance, and so on. The auditor is an independent entity that can assure that the CP conforms to a set of standards.

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Cloud Security Risks and Countermeasures

The Cloud Security Alliance [CSA10] lists the following as the top cloud specific security threats, together with suggested countermeasures:

• Abuse and nefarious use of cloud computing: For many CPs, it is relatively easy to register and begin using cloud services, some even offering free limited trial periods. This enables attackers to get inside the cloud to conduct various attacks, such as spamming, malicious code attacks, and denial of service.

Countermeasures include (1) stricter initial registration and validation processes; (2) enhanced credit card fraud monitoring and coordination; (3) comprehensive introspection of customer network traffic; and (4) monitoring public blacklists for one's own network blocks.

• Malicious insiders: Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the CP. One grave concern is the risk of malicious insider activity. Cloud architectures necessitate certain roles that are extremely high risk. Examples include CP system administrators and managed security service providers.

Countermeasures include the following: (1) enforce strict supply chain management and conduct a comprehensive supplier assessment; (2) specify human resource requirements as part of legal contract; (3) require transparency into overall information security and management practices, as well as compliance reporting; and (4) determine security breach notification processes.

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Risks and Countermeasures (continued)

- Insecure interfaces and APIs: CPs expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. The security and availability of general cloud services are dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

Countermeasures include (1) analyzing the security model of CP interfaces; (2) ensuring that strong authentication and access controls are implemented in concert with encrypted transmission; and (3) understanding the dependency chain associated with the API.

- Shared technology issues: IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture. CPs typically approach this risk by the use of isolated virtual machines for individual clients. This approach is still vulnerable to attack, by both insiders and outsiders, and so can only be a part of an overall security strategy.

Countermeasures include the following: (1) implement security best practices for installation/configuration; (2) monitor environment for unauthorized changes/activity; (3) promote strong authentication and access control for administrative access and operations; (4) enforce SLAs for patching and vulnerability remediation; and (5) conduct vulnerability scanning and configuration audits.

- Data loss or leakage: For many clients, the most devastating impact from a security breach is the loss or leakage of data. We address this issue in the next subsection.

Countermeasures include the following: (1) implement strong API access control; (2) encrypt and protect integrity of data in transit; (3) analyze data protection at both design and run time; and (4) implement strong key generation, storage and management, and destruction practices.

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Risks and Countermeasures (continued)

- Account or service hijacking
  - Countermeasures: prohibit the sharing of account credentials between users and services; leverage strong two-factor authentication techniques where possible; employ proactive monitoring to detect unauthorized activity; understand CP security policies and SLAs
- Unknown risk profile
  - Countermeasures: disclosure of applicable logs and data; partial/full disclosure of infrastructure details; monitoring and alerting on necessary information

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

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 to 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 provider 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 techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Table 5.3

NIST Guidelines on Security and Privacy Issues and Recommendations

(Table can be found on Pages 163-164 in textbook)

Data Protection in the Cloud

The threat of data compromise increases in the cloud!

The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges that are either unique to the cloud or more dangerous because of the architectural or operational characteristics of the cloud environment.

There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data.

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Data Protection in the Cloud

- Data must be secured while at rest, in transit, and in use, and access to the data must be controlled
- The client can employ encryption to protect data in transit, though this involves key management responsibilities for the CP
- For data at rest the ideal security measure is for the client to encrypt the database and only store encrypted data in the cloud, with the CP having no access to the encryption key
- A straightforward solution to the security problem in this context is to encrypt the entire database and not provide the encryption/decryption keys to the service provider
  - The user has little ability to access individual data items based on searches or indexing on key parameters
  - The user would have to download entire tables from the database, decrypt the tables, and work with the results
  - To provide more flexibility it must be possible to work with the database in its encrypted form

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

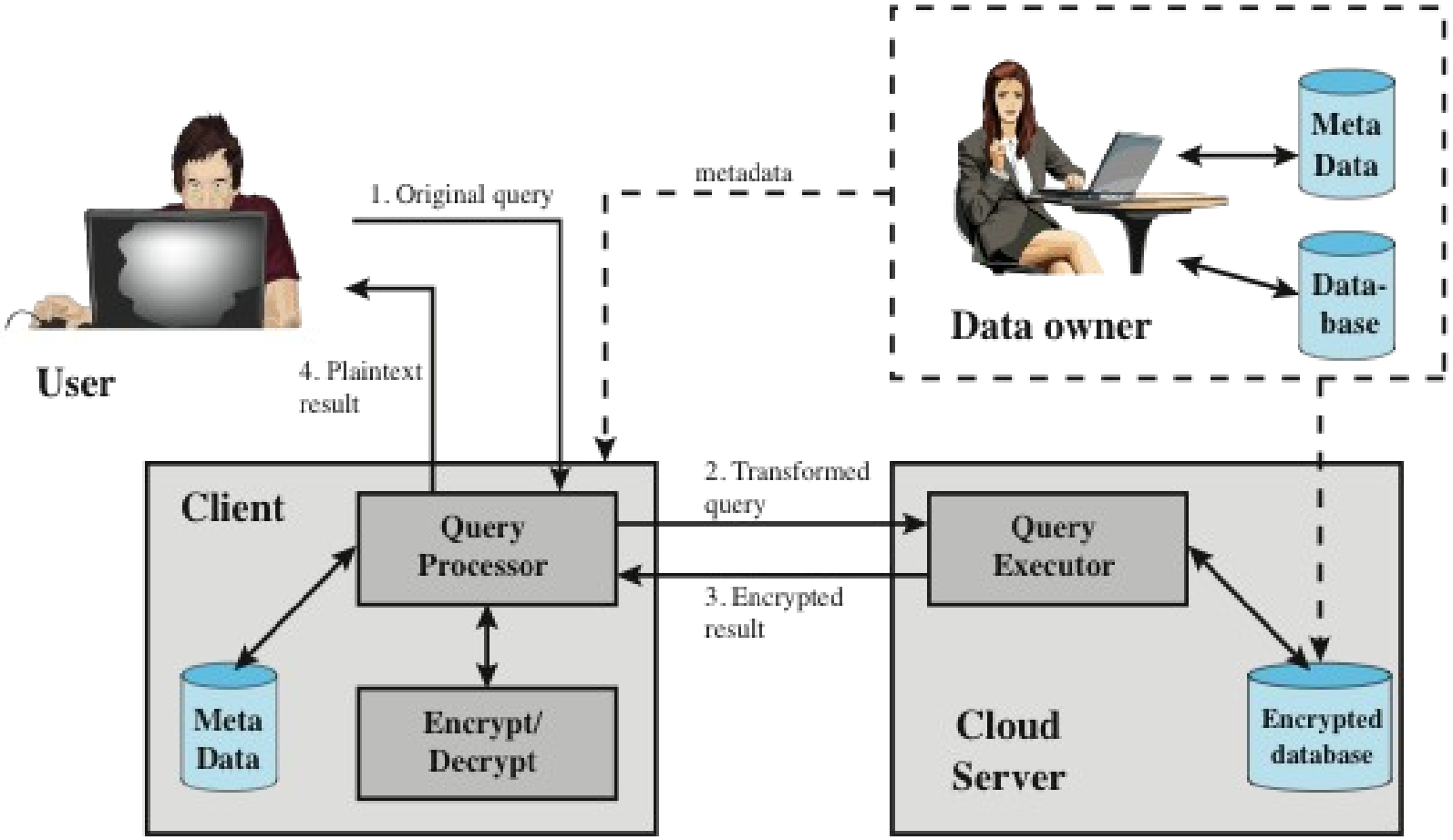
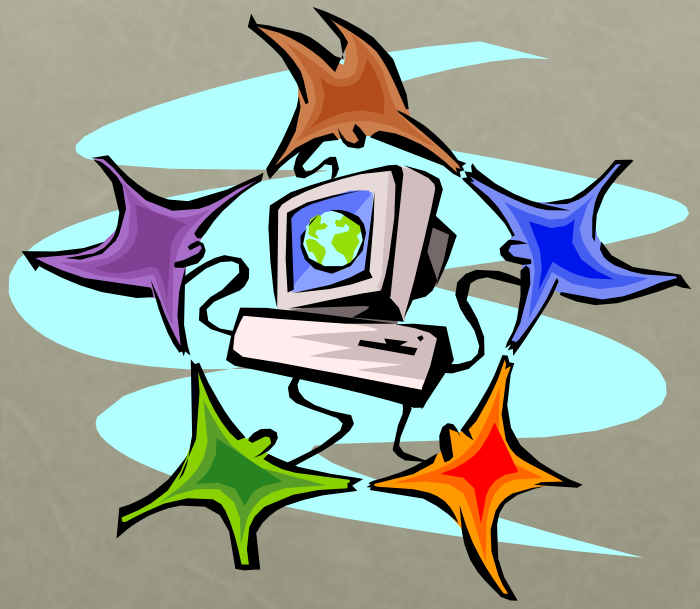


Figure 5.10 An Encryption Scheme for a Cloud-Based Database

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Cloud Security as a Service (SecaaS)

- The Cloud Security Alliance defines SecaaS as the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers' on-premise systems
- The Cloud Security Alliance has identified the following SecaaS categories of service:
  - Identity and access management
  - Data loss prevention
  - Web security
  - E-mail security
  - Security assessments
  - Intrusion management
  - Security information and event management
  - Encryption
  - Business continuity and disaster recovery
  - Network security



© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

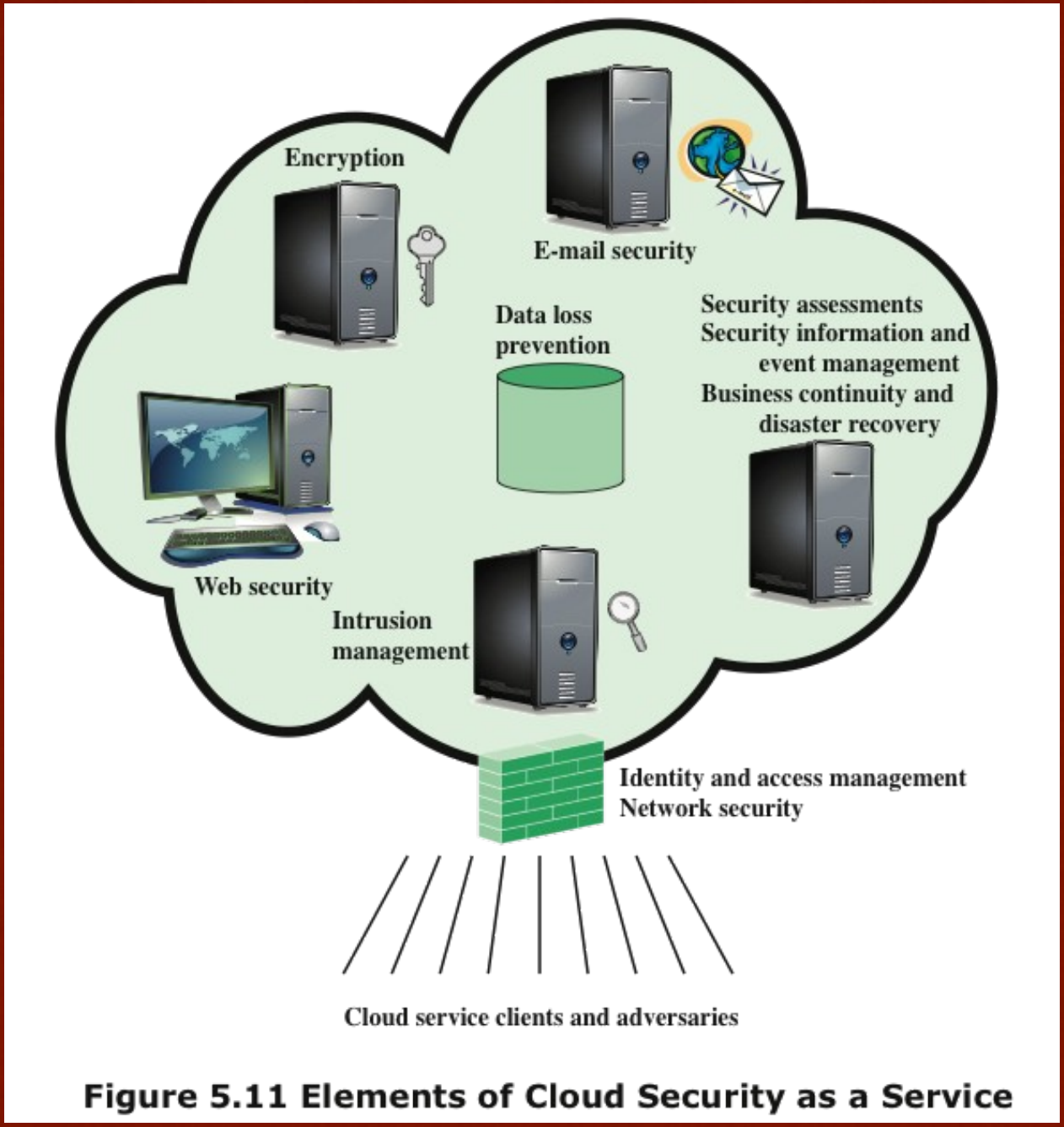


Figure 5.11 Elements of Cloud Security as a Service

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Summary

- Network access control
  - Elements of a network access control system
  - Network access enforcement methods
- Extensible authentication protocol
  - Authentication methods
  - EAP exchanges
- Cloud security as a service
- IEEE 802.1X port-based network access control
- Cloud computing
  - Elements
  - Reference architecture
- Cloud security risks and countermeasures
- Data protection in the cloud
- Addressing cloud computing security concerns

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Table 5.4
Control Functions and Classes

Technical	Operational	Management ...
Access Control Audit and Accountability Identification and Authentication System and Communication Protection	Awareness and Training Configuration and Management Contingency Planning Incident Response Maintenance Media Protection Physical and Environmental Protection Personnel SecuritySystem and Information Integrity	Certification, Accreditation and Security Assessment PlanningRisk Assessment System and Services Acquisition

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Cloud Provider

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Table 5.3

NIST Guidelines on Security and Privacy Issues and Recommendations

(page 2 of 2)

(Table can be found on Pages 163-164 in textbook)

© 2017 Pearson Education, Inc., Hoboken, NJ. All rights reserved.