CNS Module -5

.

Network Access Control

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

NAC systems deal with three categories of components:

Access requester (AR)

- 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
- Also referred to as *supplicants,* or clients

Policy server

- Determines what access should be granted
- Often relies on backend systems

Network access server (NAS)

- Functions as an access control point for users in remote locations connecting to an enterprise's internal network
- Also called a *media gateway, remote access server (RAS), or policy server*
- May include its own authentication services or rely on a separate authentication service from the policy server
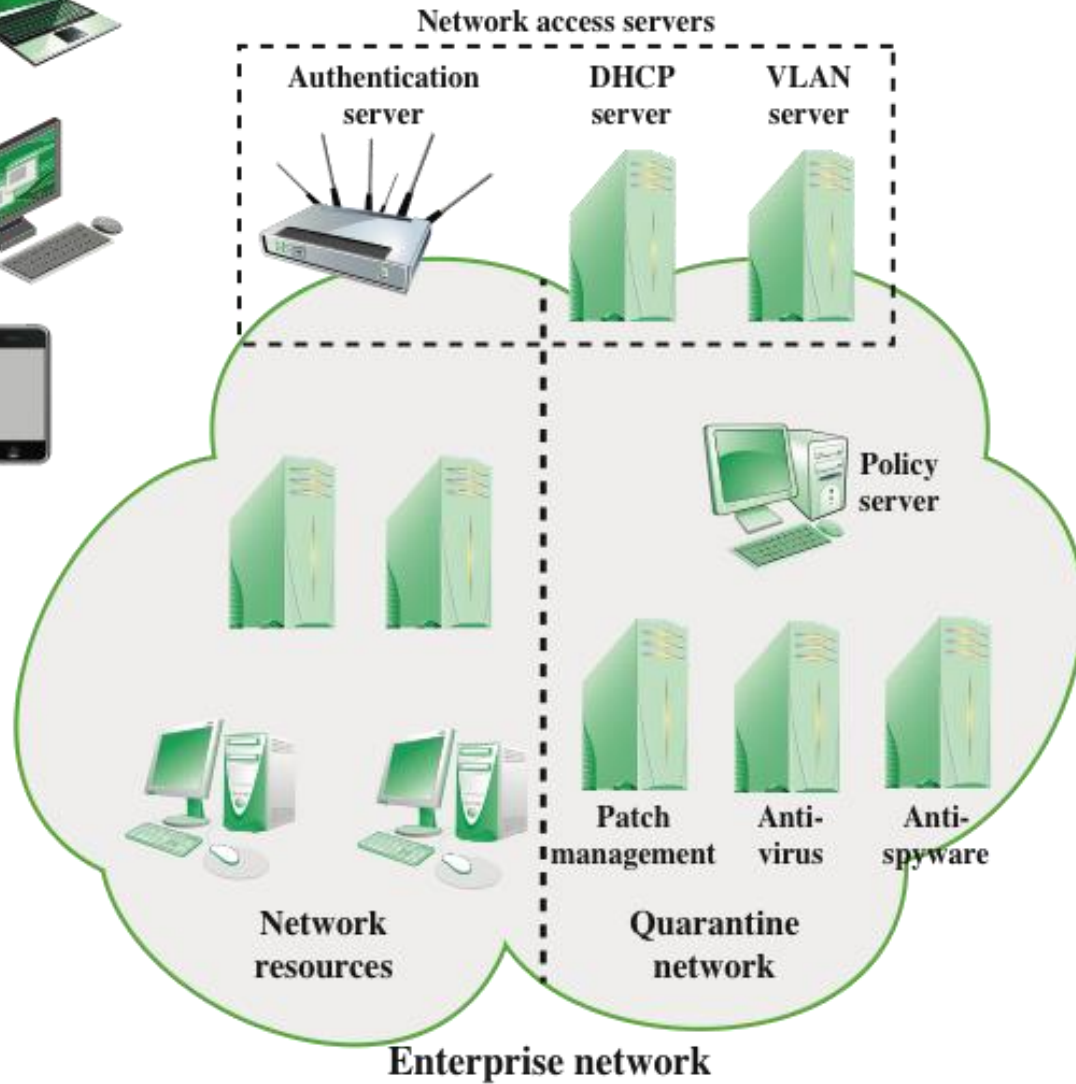
Figure 5.1 Network Access Control Context

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

Common NAC enforcement methods:

- IEEE 802.1X
- Virtual local area networks (VLANs)
- Firewall
- DHCP management
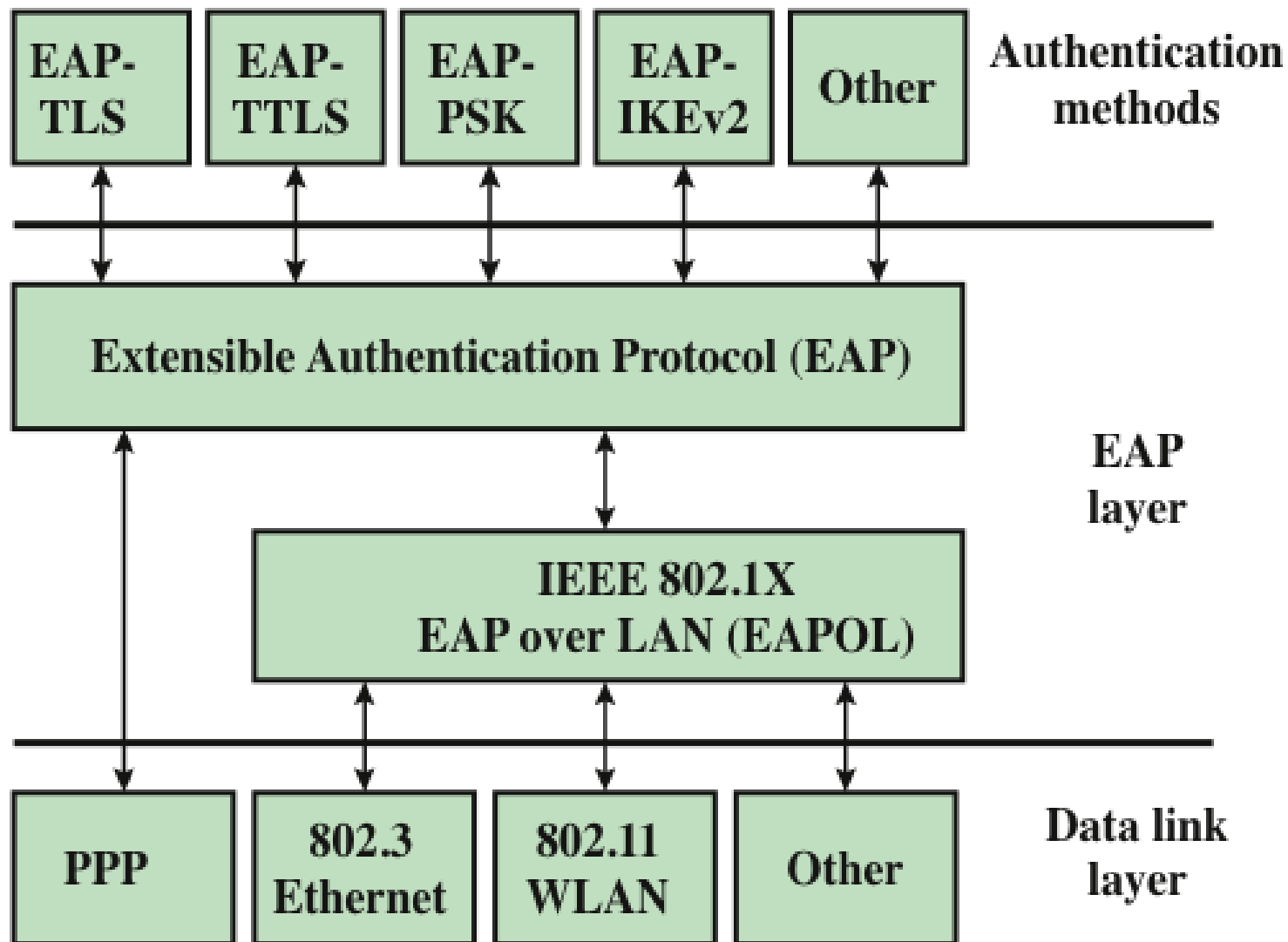
Figure 5.2 EAP Layered Context

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
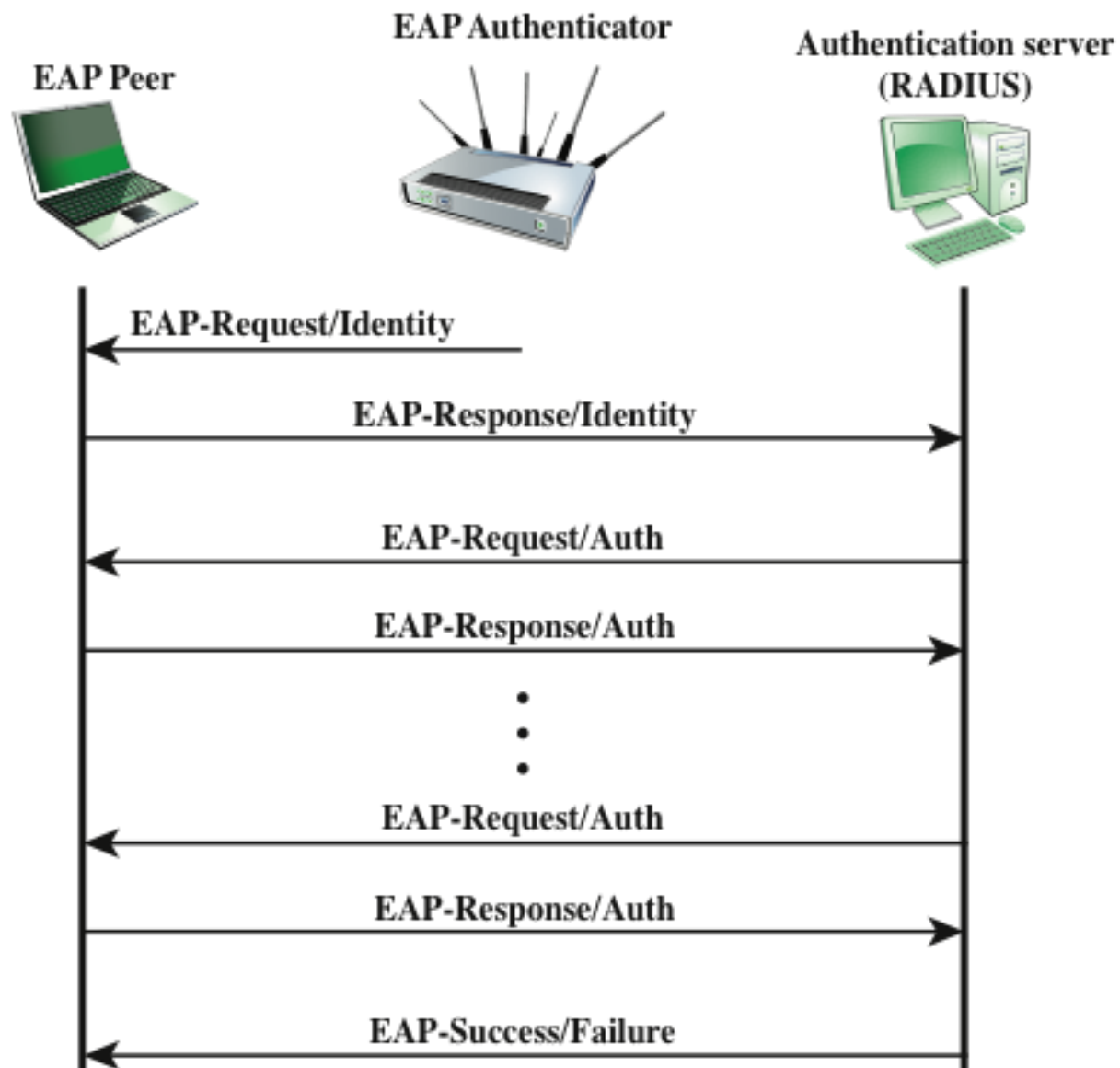
Commonly supported EAP methods:

- EAP Transport Layer Security
- EAP Tunneled TLS
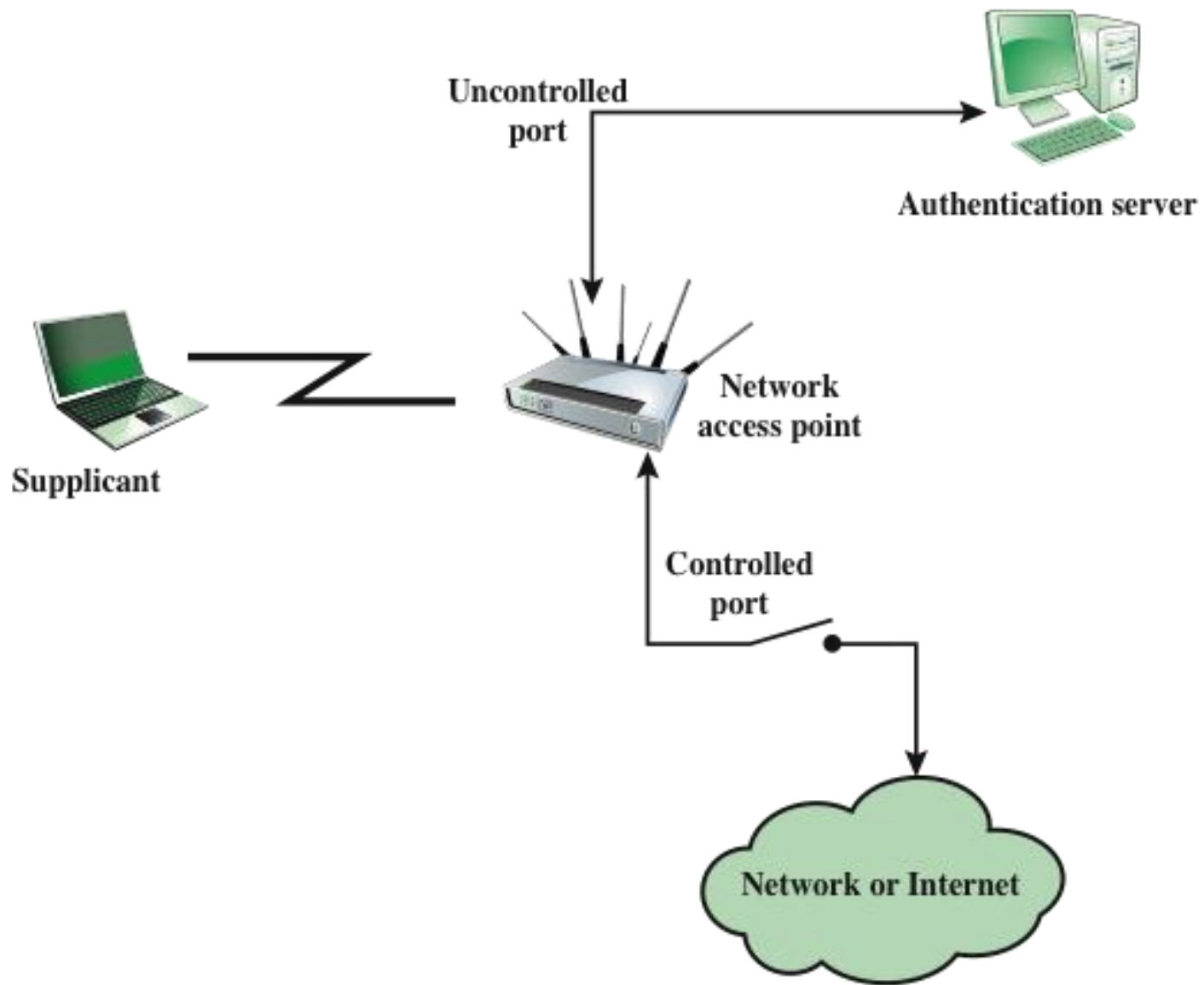- EAP Generalized Pre-Shared Key
- EAP-IKEv2
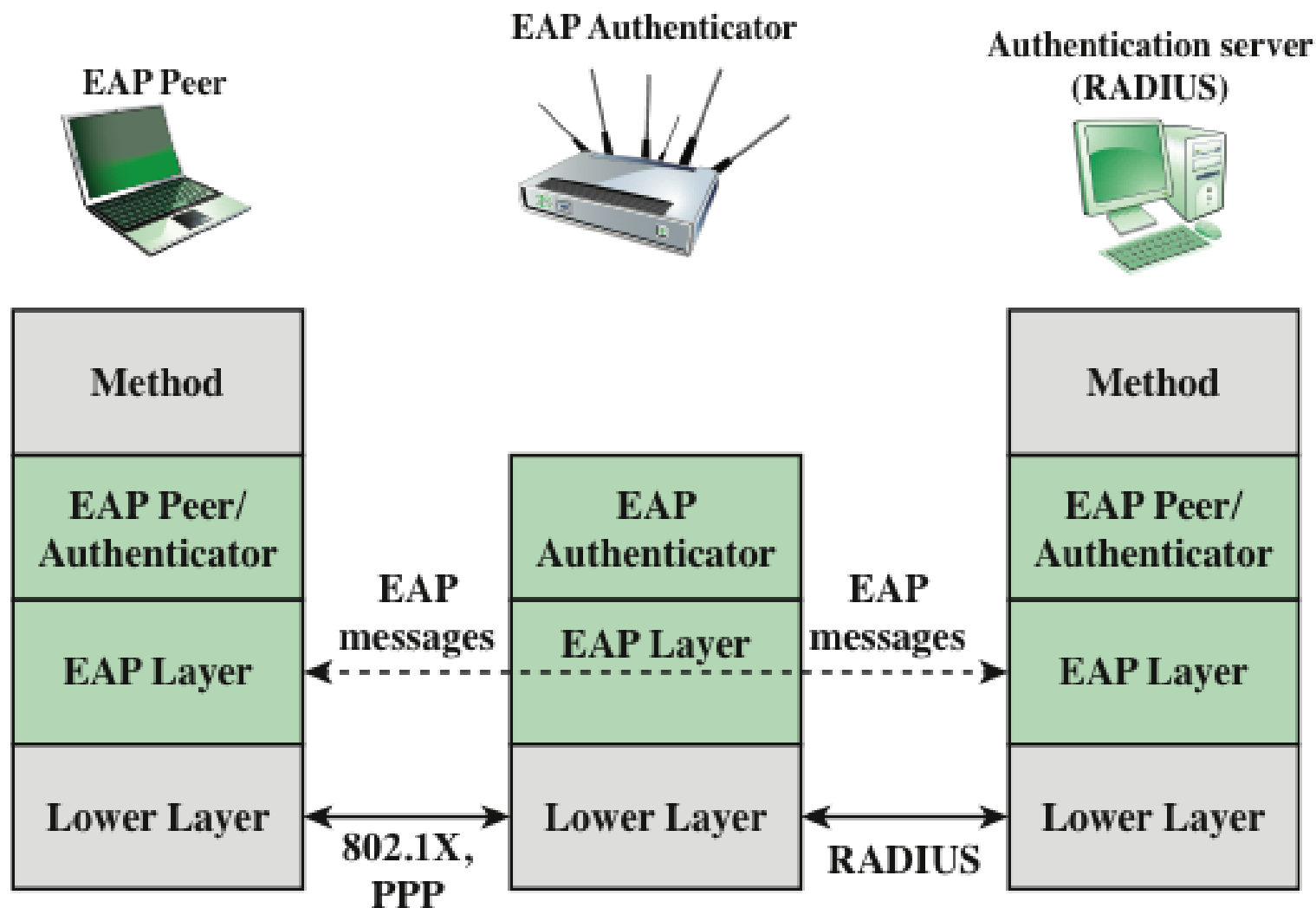
Figure 5.3 EAP Protocol Exchanges

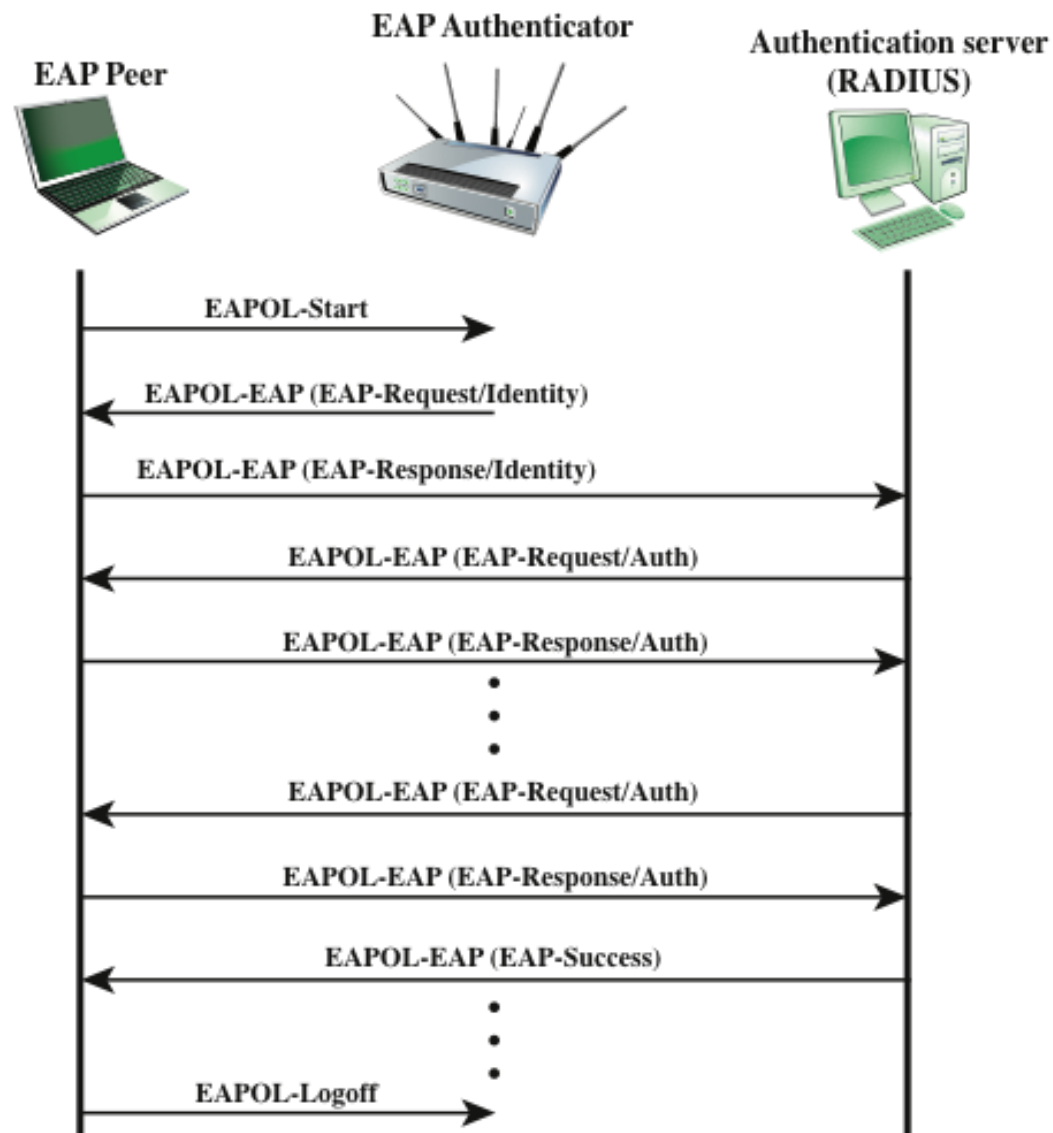Figure 5.4 EAP Message Flow in Pass-Through Mode

Figure 5.5 802.1X Access Control

Figure 5.6 Example Timing Diagram for IEEE 802.1X