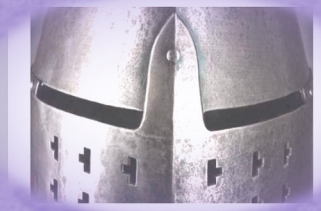


Chapter 18

Network Access
(Wireless Network Security)

Wireless Security

- Some of the key factors contributing to the higher security risk of wireless networks compared to wired networks include:

Channel

Wireless networking typically involves broadcast communications, which is far more susceptible to eavesdropping and jamming than wired networks

Wireless networks are also more vulnerable to active attacks that exploit vulnerabilities in communications protocols

Mobility

Wireless devices are far more portable and mobile than wired devices

This mobility results in a number of risks

Resources

Some wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware

Accessibility

Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations

This greatly increases their vulnerability to physical attacks

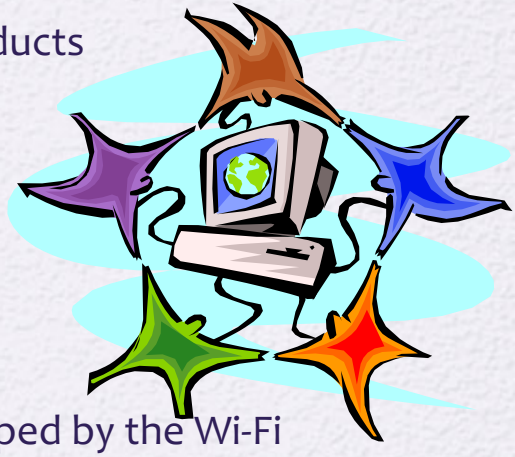
Figure 18.1 Wireless Networking Components

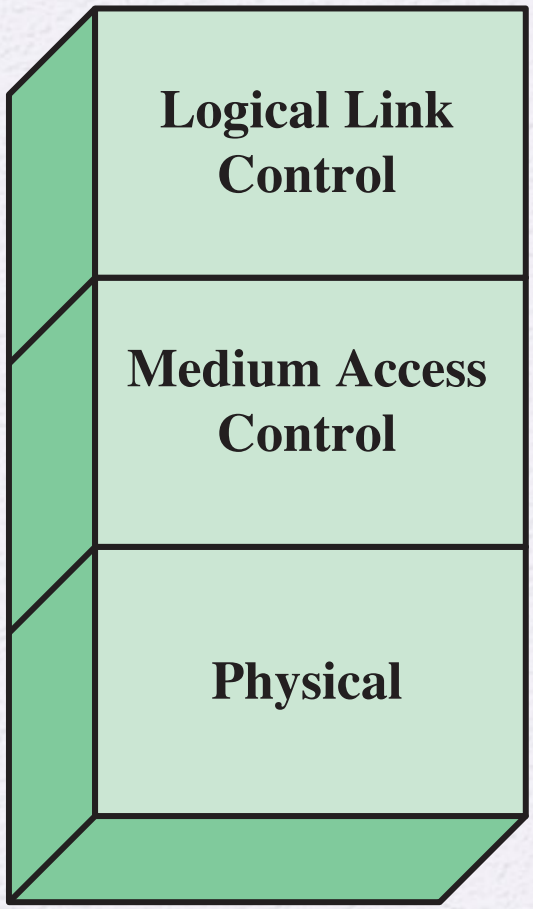
IEEE 802.11 Wireless LAN Overview

- IEEE 802 is a committee that has developed standards for a wide range of local area networks (LANs)
- In 1990 the IEEE 802 Committee formed a new working group, IEEE 802.11, with a charter to develop a protocol and transmission specifications for wireless LANs (WLANs)
- Since that time, the demand for WLANs at different frequencies and data rates has exploded

Wi-Fi Alliance

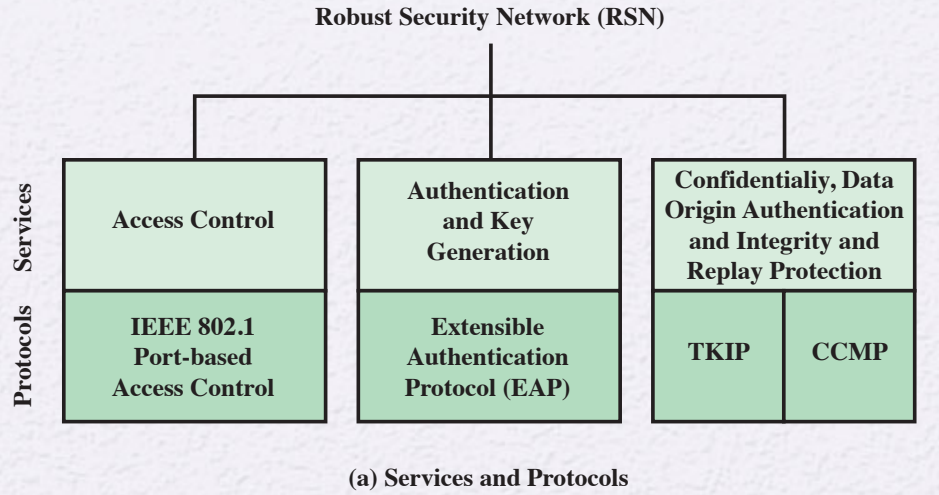
- The first 802.11 standard to gain broad industry acceptance was 802.11b
- Wireless Ethernet Compatibility Alliance (WECA)
  - An industry consortium formed in 1999
  - Subsequently renamed the Wi-Fi (Wireless Fidelity) Alliance
  - Created a test suite to certify interoperability for 802.11 products
- Wi-Fi
  - The term used for certified 802.11b products
  - Has been extended to 802.11g products
- Wi-Fi5
  - A certification process for 802.11a products that was developed by the Wi-Fi Alliance
- Recently the Wi-Fi Alliance has developed certification procedures for IEEE 802.11 security standards
  - Referred to as Wi-Fi Protected Access (WPA)



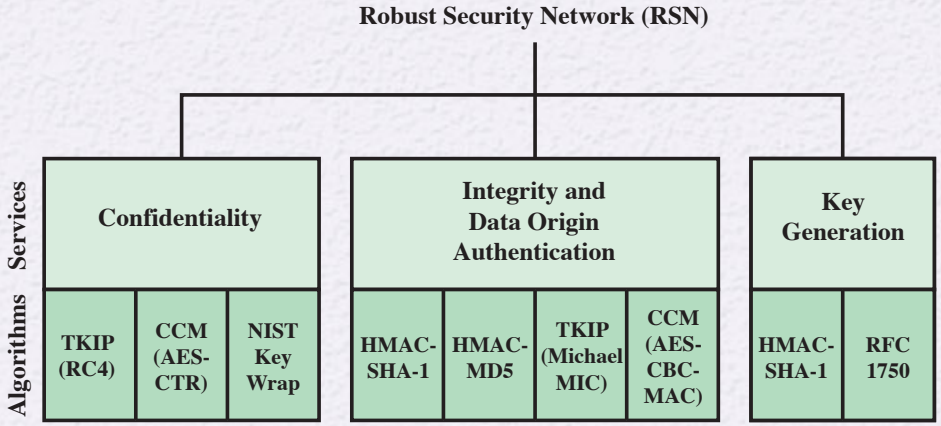


	General IEEE 802 functions	Specific IEEE 802.11 functions
Logical Link Control	Flow control Error control	
Medium Access Control	Assemble data into frame Addressing Error detection Medium access	Reliable data delivery Wireless access control protocols
Physical	Encoding/decoding of signals Bit transmission/ reception Transmission medium	Frequency band definition Wireless signal encoding

Figure 18.3 IEEE 802.11 Protocol Stack



(a) Services and Protocols



(b) Cryptographic Algorithms

CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

Figure 18.6 Elements of IEEE 802.11i

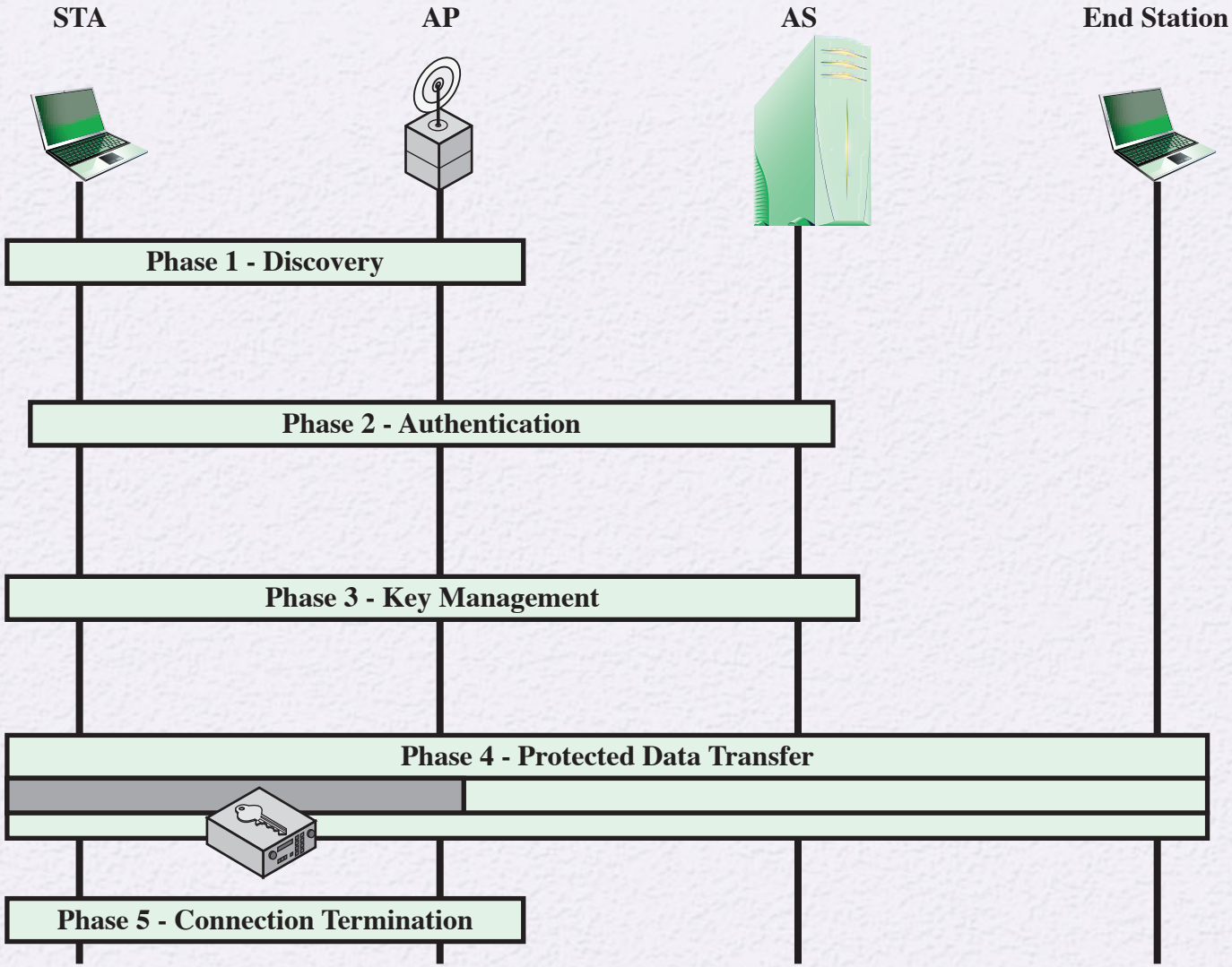


Figure 18.7 IEEE 802.11i Phases of Operation

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**

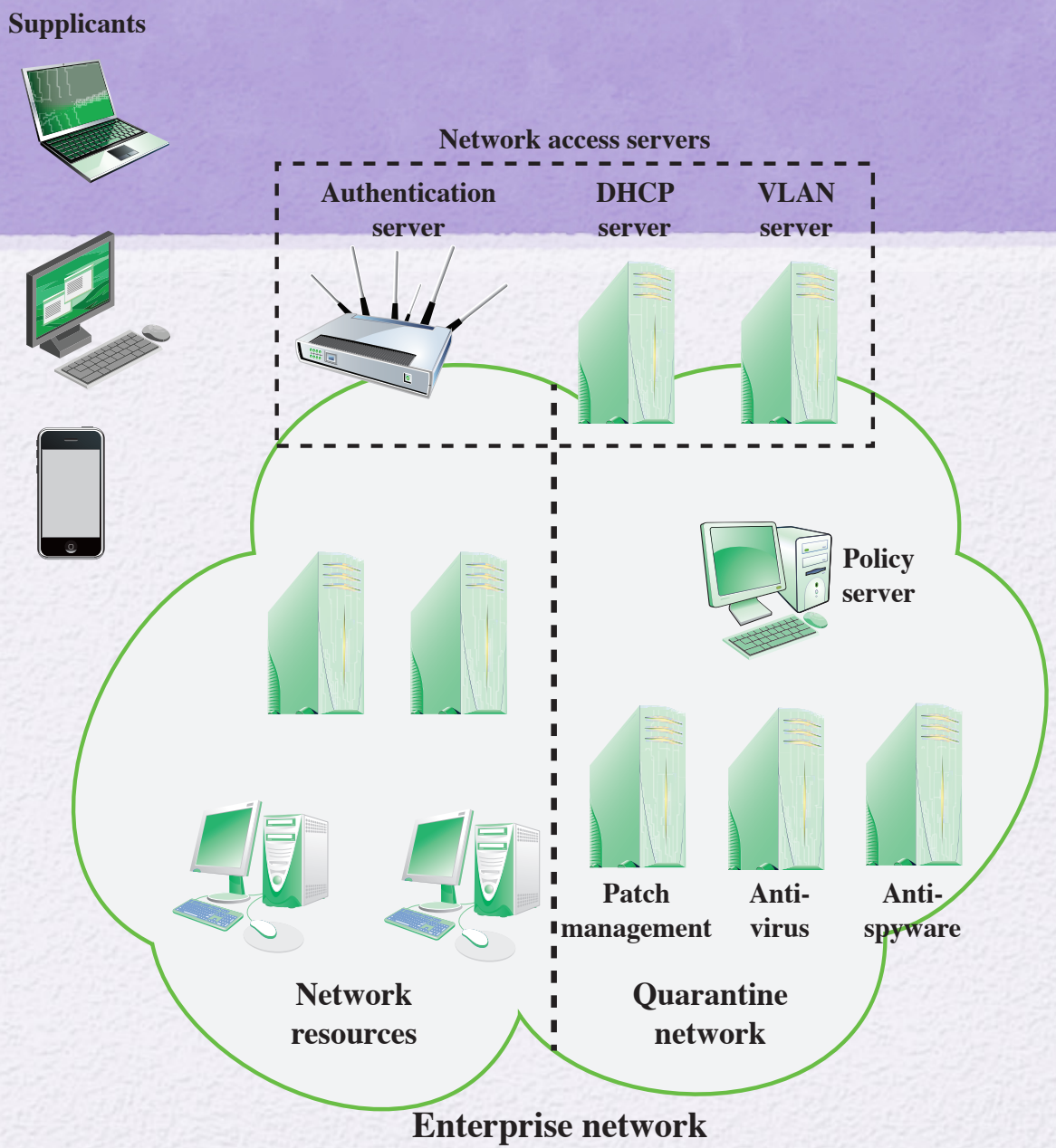
Network access server (NAS)

- 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

Policy server

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

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

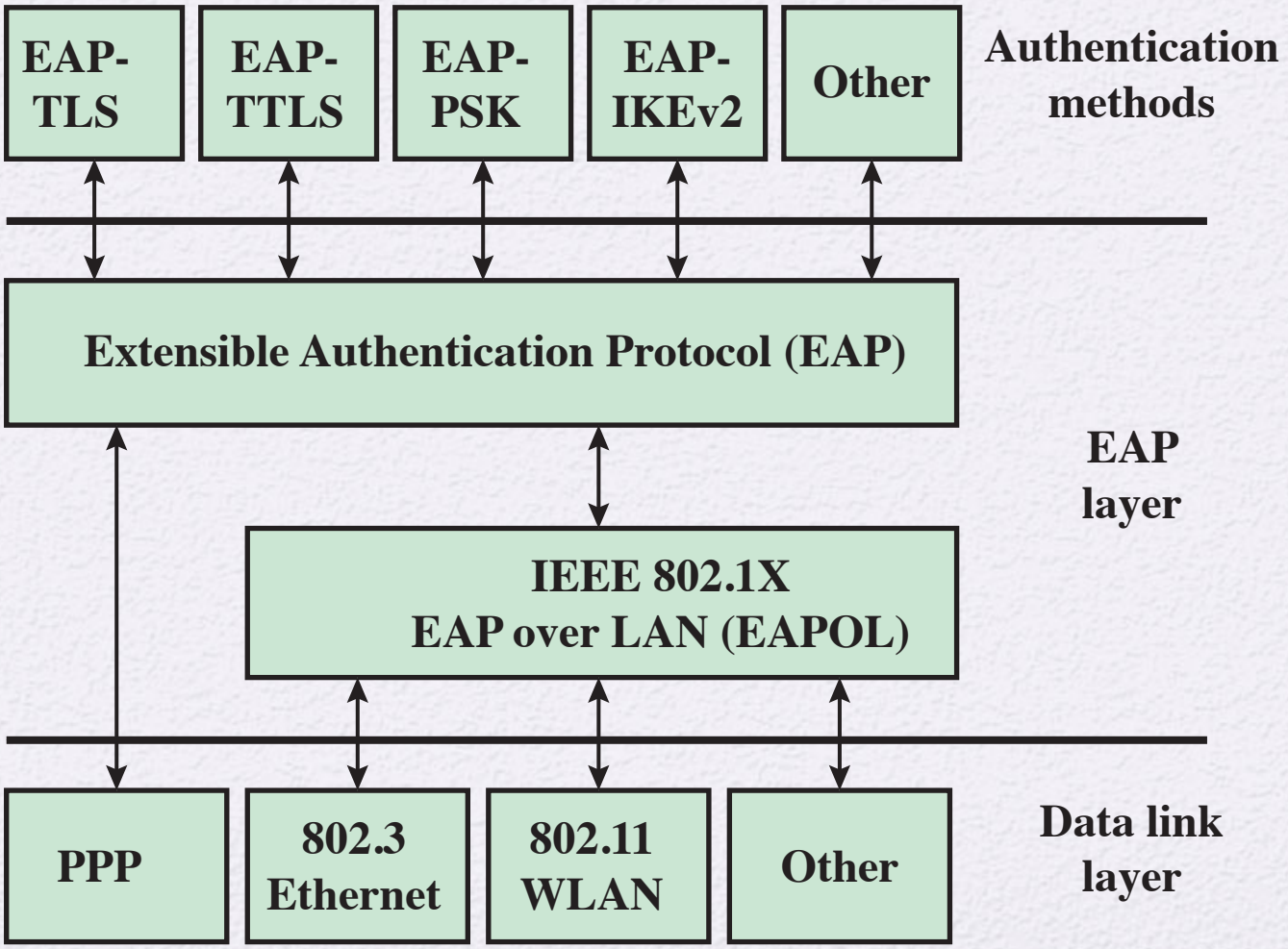
Common NAC enforcement methods:

- IEEE 802.1X (with EAP)
- Virtual local area networks (VLANs)
- Firewall
- DHCP management

IEEE 802.1X Access Control Approach

- Port-Based Network Access Control
- The authentication protocol that is used, the Extensible Authentication Protocol (EAP), is defined in the IEEE 802.1X standard
- 802.1X uses:
  - Controlled ports
    - Allows the exchange of PDUs between a supplicant and other systems on the LAN only if the current state of the supplicant authorizes such an exchange
  - Uncontrolled ports
    - Allows the exchange of PDUs between the supplicant and the other AS, regardless of the authentication state of the supplicant

EAP Layered Context



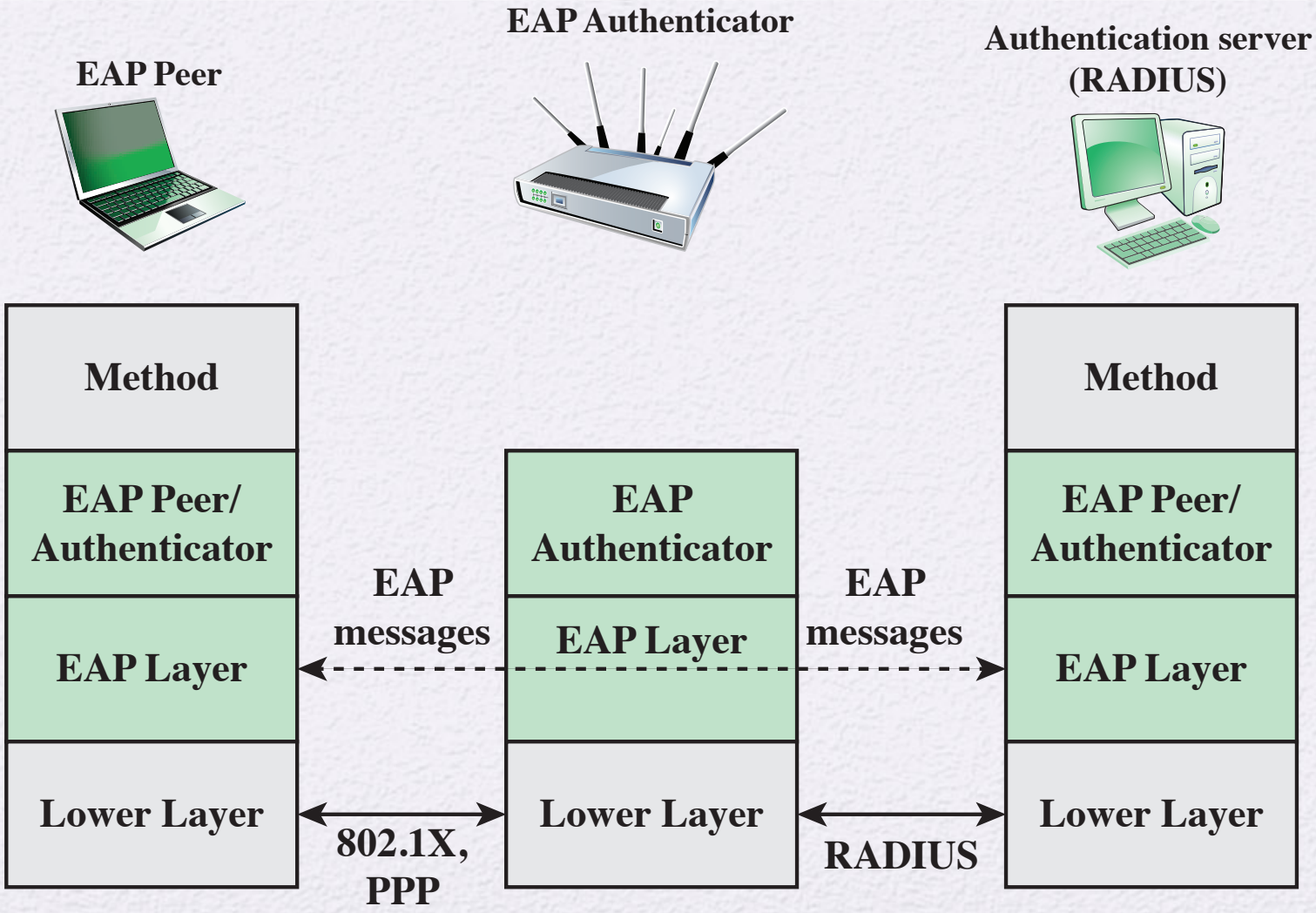
Authentication Methods

- 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

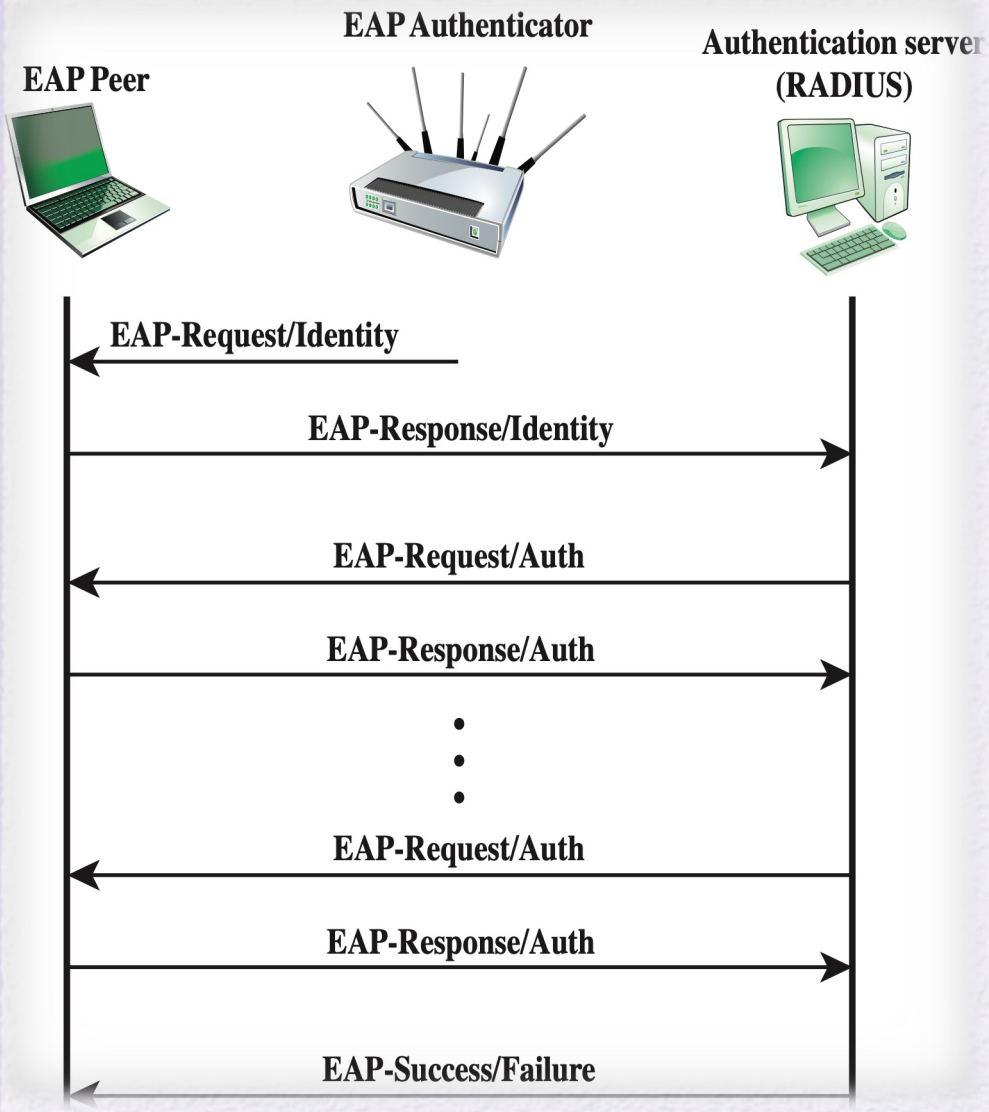
Commonly supported EAP methods:

- EAP Transport Layer Security
- EAP Tunneled TLS
- EAP Generalized Pre-Shared Key
- EAP-IKEv2

EAP Protocol Exchanges



EAP Message Flow in Pass-Through Mode



Terminology Related to IEEE 802.1X

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.

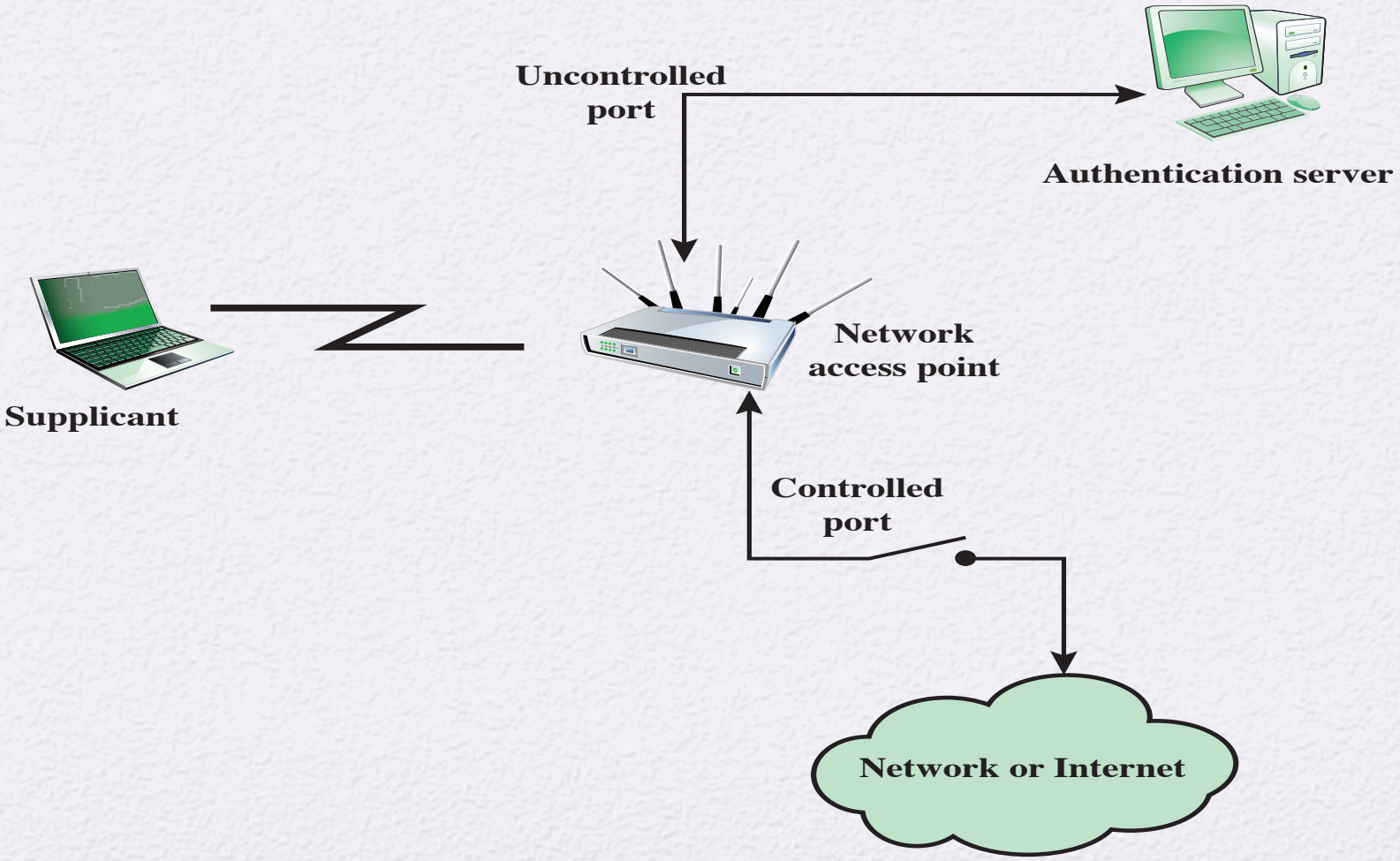
Edge port
A bridge port attached to a LAN that has no other bridges attached to it.

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.

802.1X Access Control



Common EAPOL Frame Types

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.

Example Timing Diagram for IEEE 802.1X