# Chap. 5 Network Access Control and Cloud Security

□ Network Access Control (NAC)

□ Extensible Authentication Protocol (EAP)

□ IEEE 802.1x Port-based NAC

# Network Access Control (NAC)

## □ Network Access Control

- A function for controlling access to an enterprise network
- authenticates users accessing into the network and performs authentication, authorization, and accounting
  - authentication: 네트워크에 접속하는 사용자나 장치에 대해 검증 (id-passwd, 인증서 등)
  - authorization: 인증된 장치가 어떤 네트워크 자원에 대해서 접근할 수 있는지에 대해 결정
  - accounting: 과금이나 보안상의 목적으로 네트워크를 접근한 기록을 저장
- examines the health of the user's computer or mobile device; 장치의 상태, 보안설정 등 검사

# Network Access Control (NAC)

## □ NAC system components

### Access requester (AR)

- Node that attempts to access the network; also referred to as *supplicants*, or clients
- (e.g) workstations, printers, cameras, and other IP-enabled devices

### Network access server (NAS)

- Network access control point for users connecting to an enterprise's internal network
- Also called a *remote access server (RAS),*
- May include its own authentication services or rely on a separate authentication service from the policy server

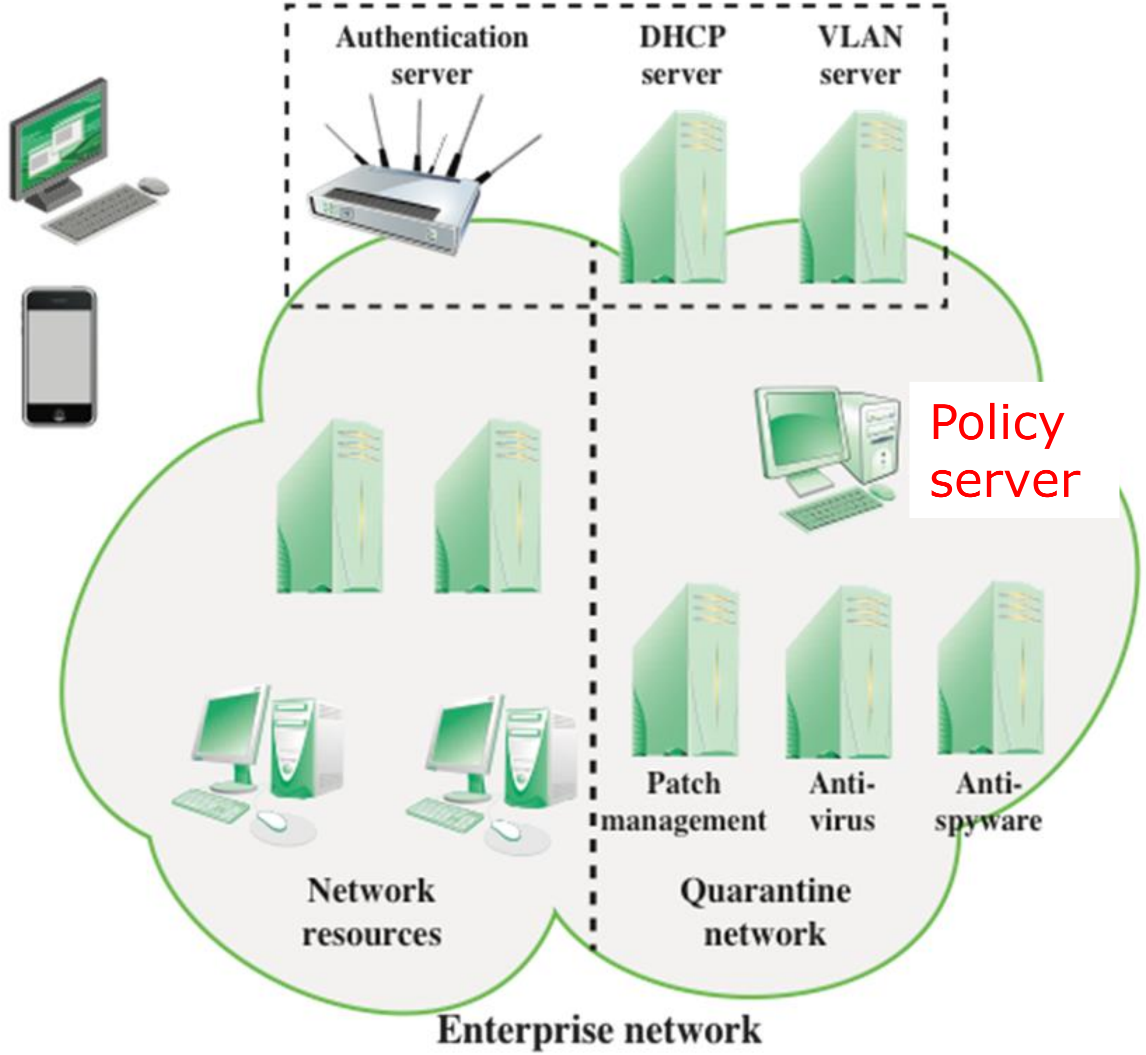
### Policy server

- Node that determines what access should be granted
- Often relies on backend systems

# Network Access Control (NAC)

- □ NAC system components

Network access servers

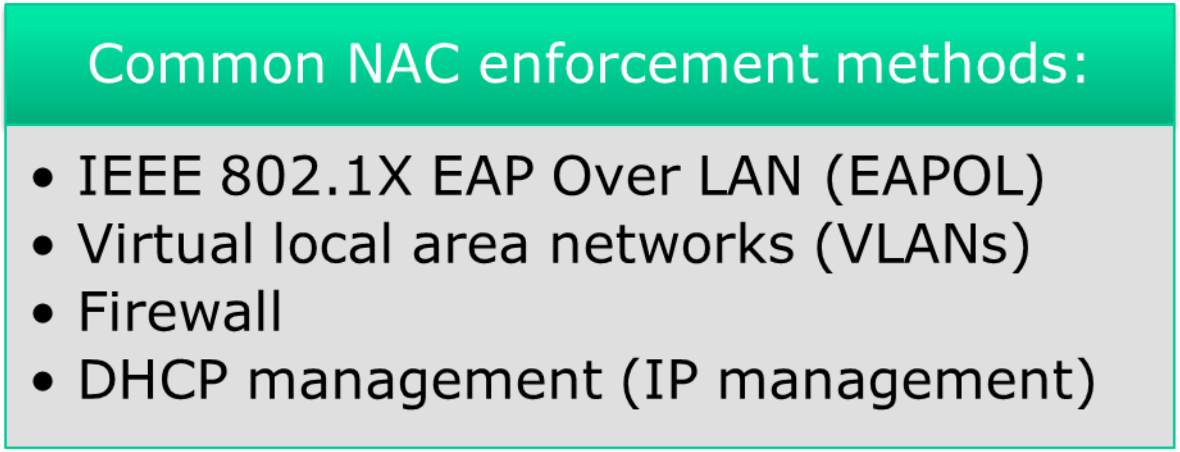


supplicants

Policy server

# Network Access Enforcement Methods

- Network Access Enforcement Methods
  - actions that are applied to ARs to regulate access to the enterprise network
  - Common enforcement methods used to tailor the configuration by combining the methods



Common NAC enforcement methods:

- IEEE 802.1X EAP Over LAN (EAPOL)
- Virtual local area networks (VLANs)
- Firewall
- DHCP management (IP management)

# Network Access Enforcement Methods

- IEEE 802.1x : EAP over LAN (EAPOL)
  - Link layer protocol to control access internal networks
  - provides a port-based NAC mechanism; after authentication, controlled-port is open and IP address is assigned to a port
  - Uses EAP (Extensible Authentication Protocol) as an authentication method

# Network Access Enforcement Methods

- VLAN (Virtual LAN)
  - separates an interconnected enterprise LAN into multiple logical segments (VLANs)
  - NAC system decides to which of the network's VLANs it will direct to an AR based on
    - whether the device needs security remediation,
    - whether the device needs Internet access only, or
    - some level of network access to enterprise resources

# Network Access Enforcement Methods

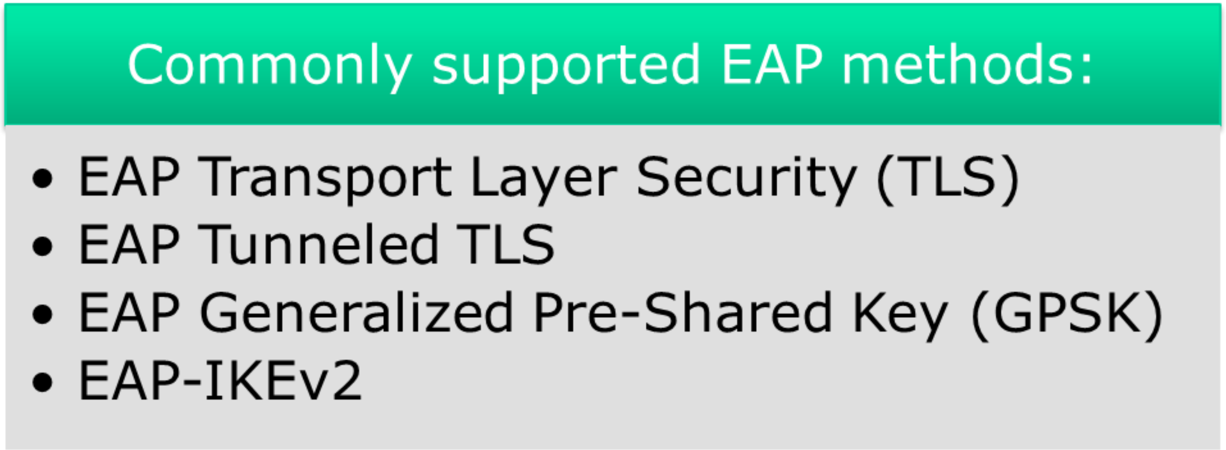
- Firewalls
  - a type of NAC which allows or denies network traffic between host and an internal user
- DHCP
  - a protocol that enables dynamic allocation of IP addresses to hosts
  - DHCP server assigns an IP address in response to a DCHCP request of a client
  - NAC enforcement occurs at the IP layer based on subnet and IP address assignment

# Authentication Methods

- EAP (Extensible Authentication Protocol)
  - provides a generic transport service for the exchange of authentication information between a client system and an authentication server; protocol to encapsulate many authentication methods
  - is extended by using a specific authentication protocol that is installed in both the EAP client and the authentication server

# Authentication Methods

□ Commonly used EAP Protocols



Commonly supported EAP methods:

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

# Authentication Methods

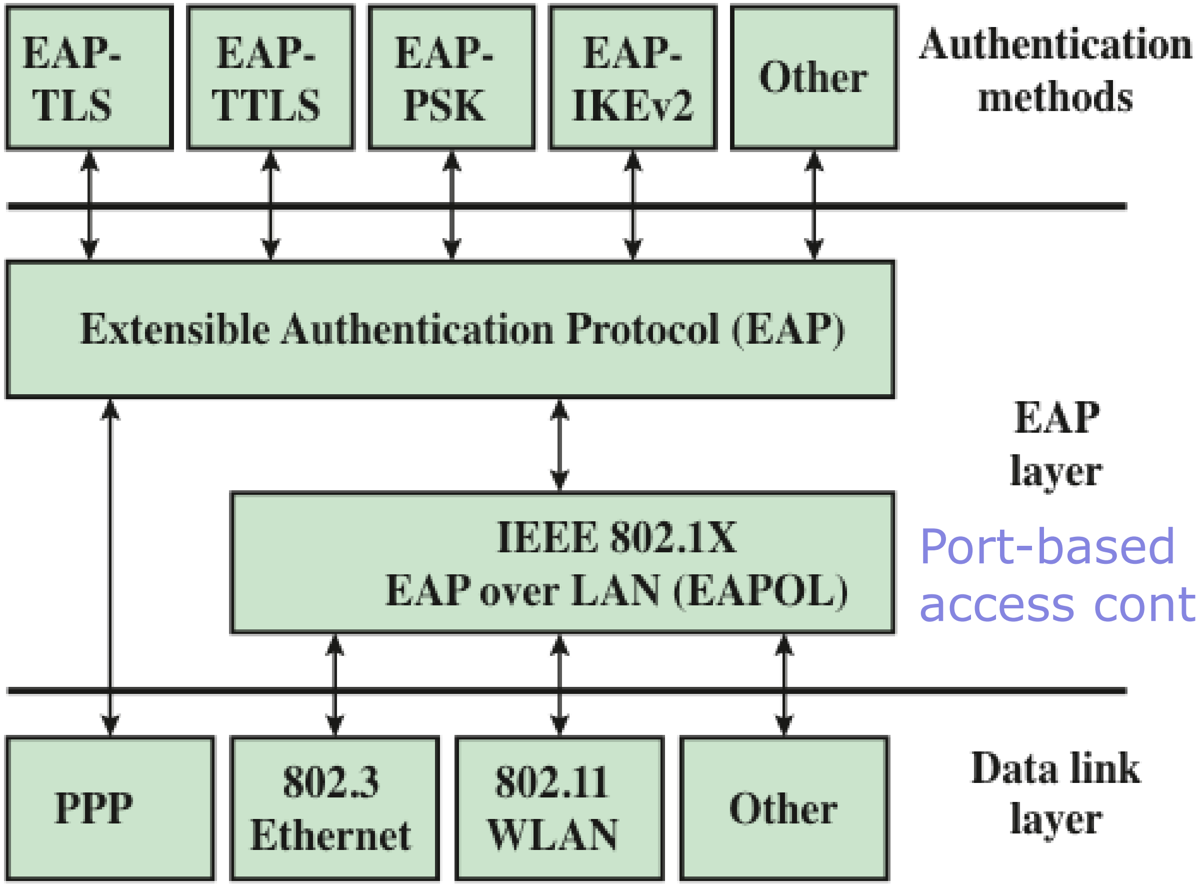
- EAP-TLS Protocol: RFC 5216
  - defines an encapsulation of TLS protocol into EAP messages
  - EAP-TLS uses the handshake protocol in TLS
- EAP-TTLS (Tunneled TLS) Protocol: RFC 5281
  - is like EAP-TLS except only the server has a certificate to authenticate itself to the client
  - Client authentication can be processed after establishing a secure channel (tunnel)

# Authentication Methods

- EAP-GPSK (Generalized Pre-Shared Key) Protocol: RFC 5433
  - An EAP method for mutual authentication and session key distribution using a pre-shared key (PSK)
  - uses a secret key-based cryptographic algorithm based on pre-shared keys
  - efficient (fast) but needs pre-shared keys between each peer and EAP server
- EAP-IKE v2
  - EAP protocol based on IKE v2 protocol

# Network Access Enforcement Methods

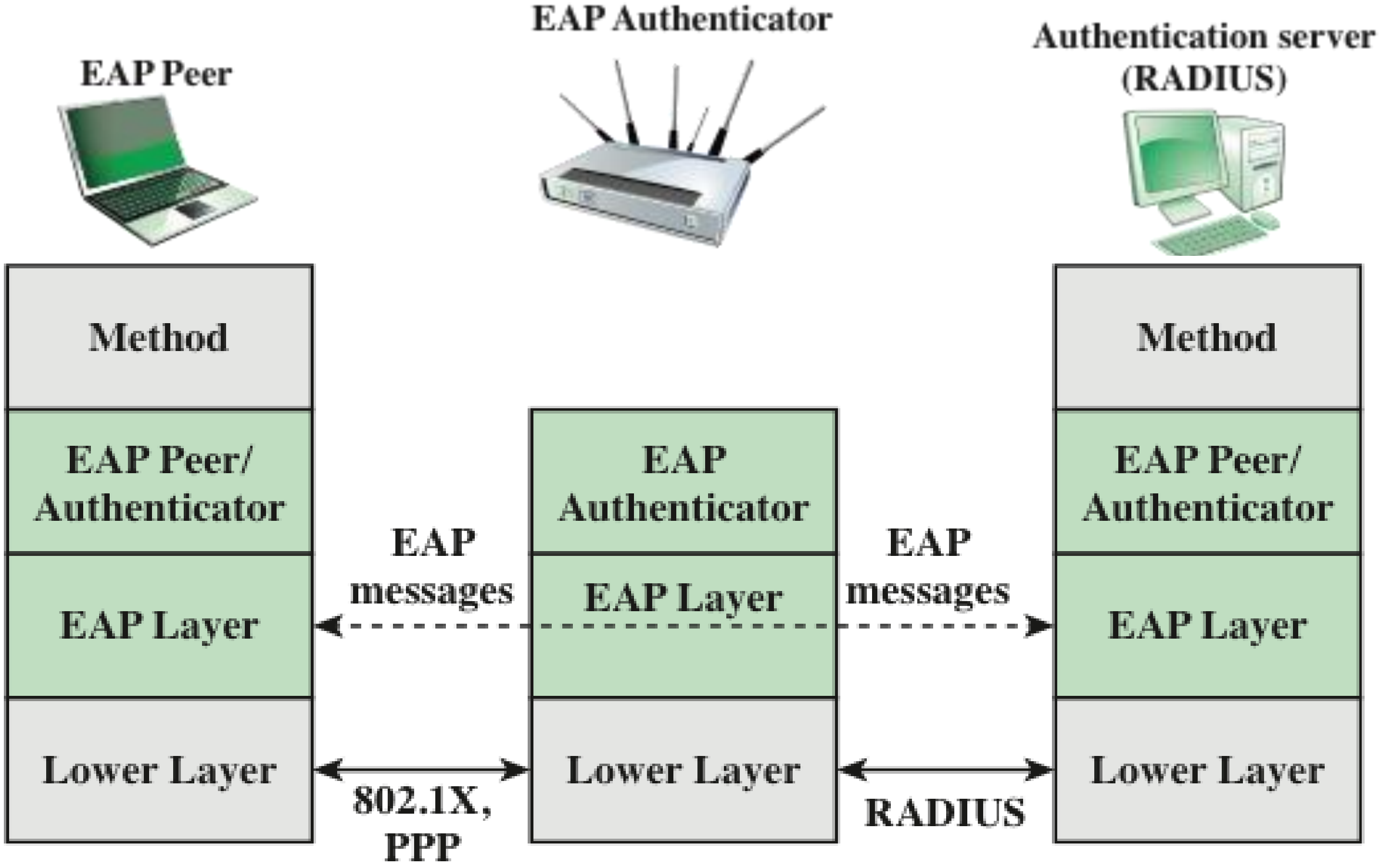
- EAP-based network access enforcement method



Port-based access control

# Authentication Methods

- EAP Protocol exchange

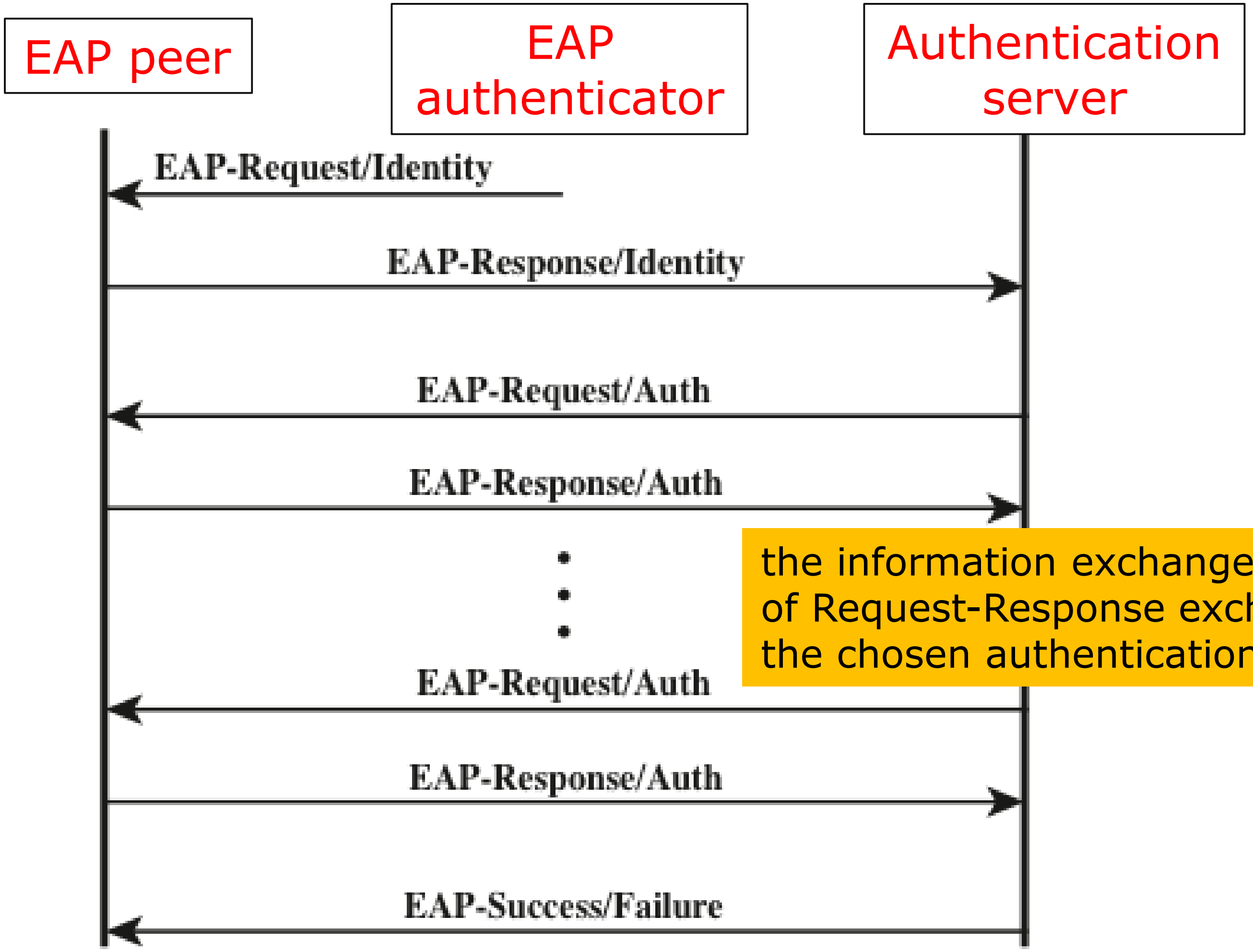


# Authentication Methods

- EAP peer
  - Client computer that attempts to access a network
- EAP authenticator
  - A network access point or RAS that needs EAP authentication prior to granting access to a network
- Authentication server
  - Server that uses an EAP method to validate the EAP peer’s credentials and authorize access to the network
  - typically, RADIUS server

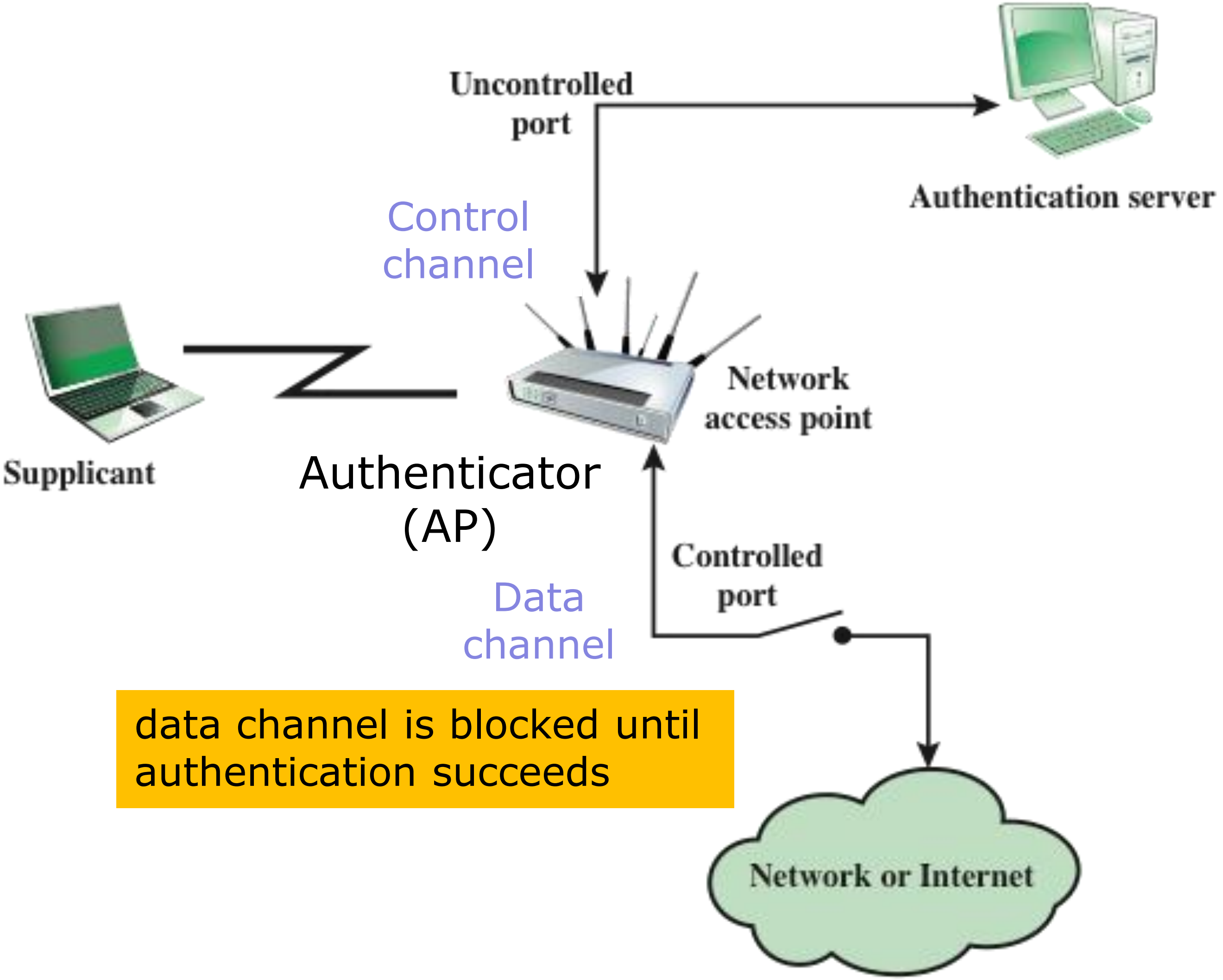
# Authentication Methods

- EAP message flow in Pass-through mode



the information exchanged and the number of Request-Response exchanges depend on the chosen authentication method

# IEEE 802.1X Port-based Access Control



Control channel

Authenticator (AP)

Data channel

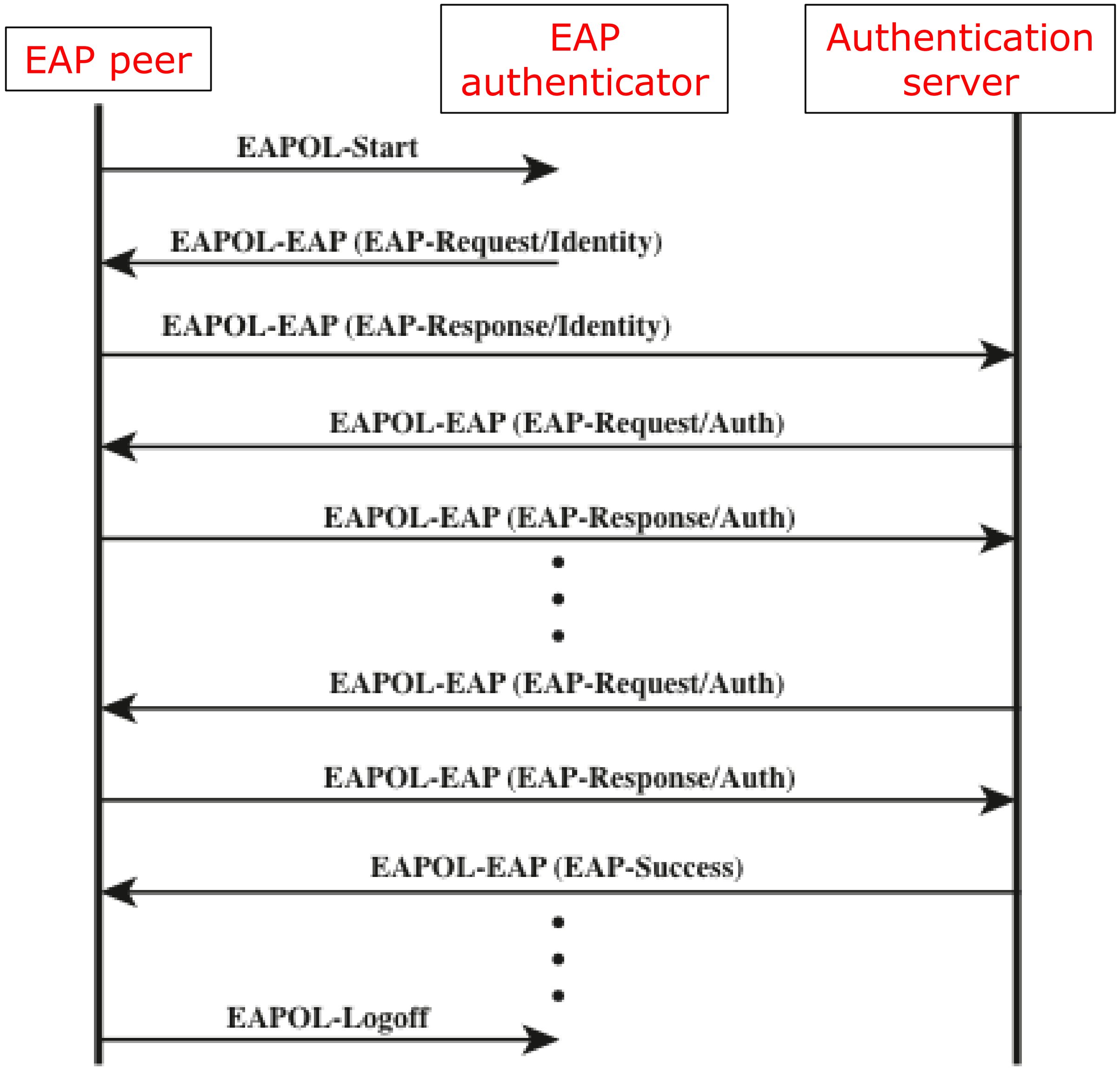
data channel is blocked until authentication succeeds

# IEEE 802.1X Port-based Access Control

- EAPOL (EAP over LAN)
  - EAP message exchange protocol over IEEE 802 LAN
  - EAPOL packets:
    - EAPOL-Start: supplicant sends to start the authentication
    - EAPOL-EAP: contains an encapsulated EAP packet
    - EAPOL-Key: used to exchange cryptographic key information
    - EAPOL-Logoff: supplicant sends this packet to disconnect from the network

# IEEE 802.1X Port-based Access Control

- IEEE 802.1x message exchange


EAP peer
EAP authenticator
Authentication server
EAPOL-Start
EAPOL-EAP (EAP-Request/Identity)
EAPOL-EAP (EAP-Response/Identity)
EAPOL-EAP (EAP-Request/Auth)
EAPOL-EAP (EAP-Response/Auth)
EAPOL-EAP (EAP-Request/Auth)
EAPOL-EAP (EAP-Response/Auth)
EAPOL-EAP (EAP-Success)
EAPOL-Logoff