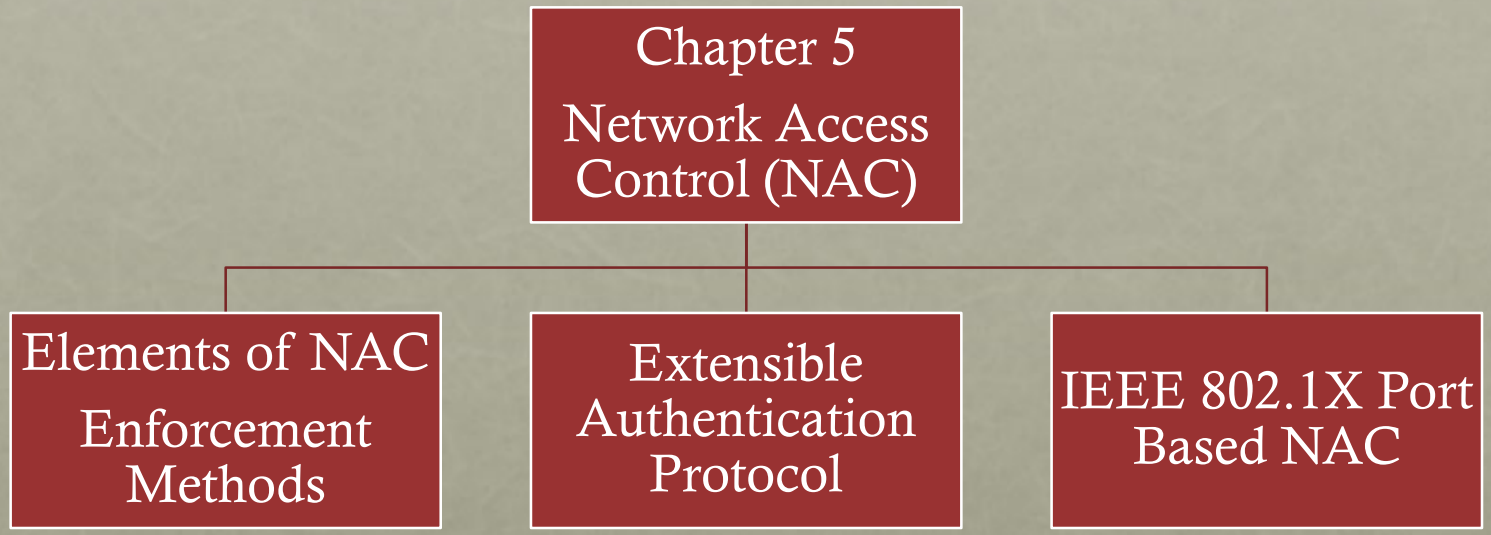
CHAPTER 5

Network Access Control Security

OUTLINE


Chapter 5
Network Access Control (NAC)
Elements of NAC
Enforcement Methods
Extensible Authentication Protocol
IEEE 802.1X Port Based NAC

NETWORK ACCESS CONTROL (NAC)

- **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 attempts 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)***
- 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

NAC GENERIC DIAGRAM

- Steps for ARs to seek access to a network by applying some type of NAS:
  1) **Authentication step:**
     - To verify supplicant's claimed identity and based on the identity.
     - Typically involves some sort of secure protocol and the use of cryptographic keys.
     - Authentication step often results in the establishment of session keys.
  2) **Policy Server (PS) Checks:**
     - PS will perform checks on the AR including:
       - Health, suitability, screening or assessment checks, e.g., antimalware software status, AR's operating system must be fully patched,…, etc.
       - These checks must be performed before access is granted
     - The PS can identify what access privileges, if any.
  3) **Access to resources:**
     - After AR has been authenticated and cleared for a certain level of access, the NAS can enable the AR to interact with the network resources

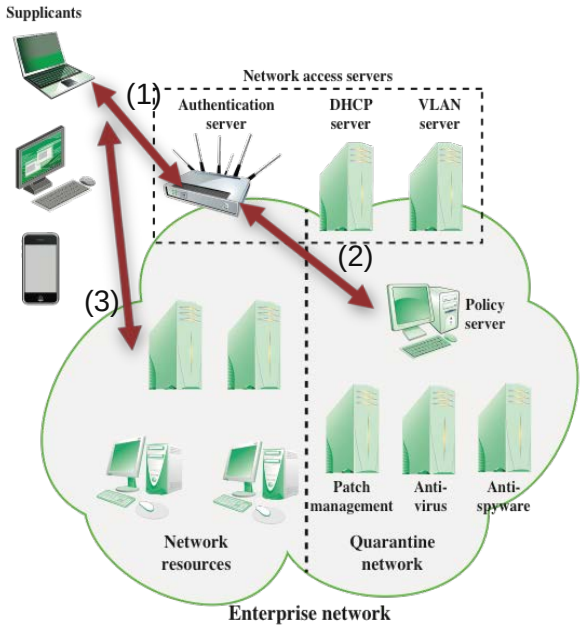


Figure 5.1 Network Access Control Context

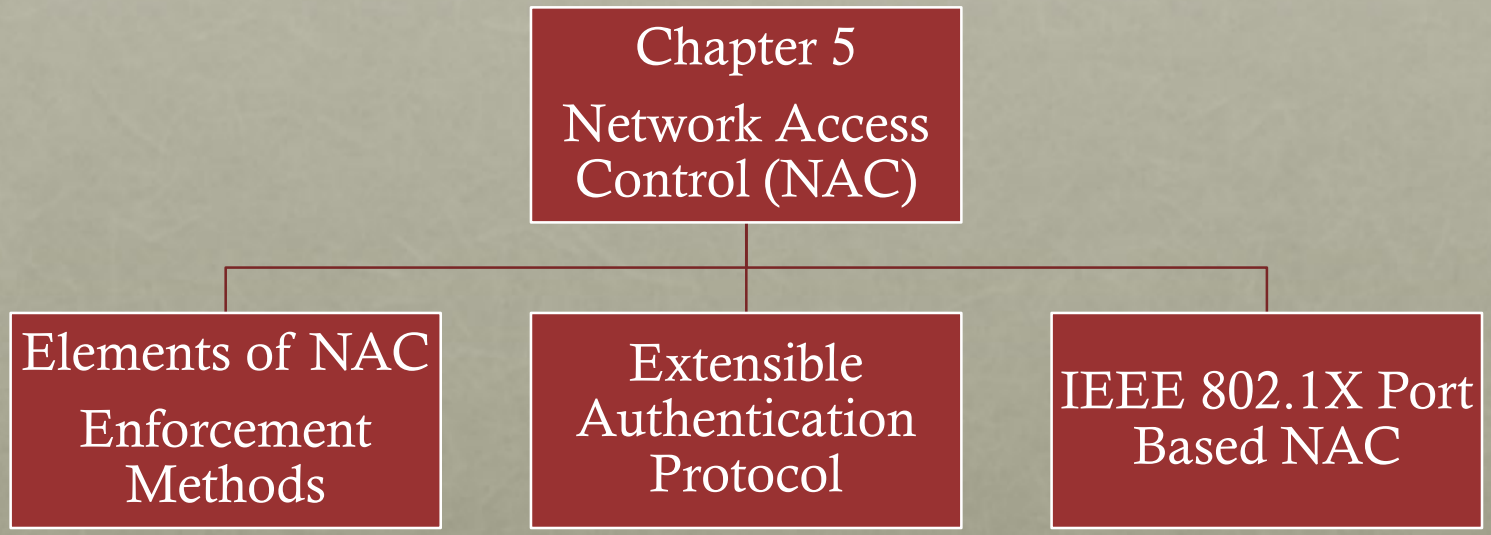
NETWORK ACCESS ENFORCEMENT METHODS

- Enforcement methods: the actions that are applied to ARs to regulate access to the enterprise network

Common NAC enforcement methods:

- **IEEE 802.1X**: enforces authorization before a port is assigned an IP address
- **Virtual local area networks** (VLANs): Network segmentation into logical LANs
  - The NAC system decides to which of the network's VLANs it will direct an AR, based on whether the device needs security remediation, Internet access only, or some level of network access to enterprise resources.
  - For example, if the PS realizes that the antimalware is not updated, the NAC may direct the AR to a quarantine VLAN where only data related to the installation of this antimalware is allowed.
- **Firewall**:
  - A firewall provides a form of NAC by allowing or denying network traffic between an enterprise host and an external user
- **DHCP management**: assign IP dynamically to form subnets
  - NAC enforcement occurs at the IP layer based on subnet and IP assignment.

OUTLINE


Chapter 5
Network Access Control (NAC)
Elements of NAC
Enforcement Methods
Extensible Authentication Protocol
IEEE 802.1X Port Based NAC

EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

- EAP
  - Framework for network access authentication protocols
  - ***EAP provides a generic transport service for the exchange of authentication information between a client system and an authentication server***
  - Provides a set of protocol messages that can encapsulate various authentication methods to be used between a client and an authentication server.
  - Can operate over a variety of network and link level facilities including, point to point links, and LANs.

EAP COMPONENTS

- **EAP peer**: Client computer that is attempting to access a network.
- **EAP authenticator**: An access point or NAS that requires EAP authentication prior to granting access to a network.
- **Authentication server**: A server computer that
  1) negotiates the use of a specific EAP method with an EAP peer
  2) validates the EAP peer's credentials
  3) and authorizes access to the network.
  4) Functions as a backend server that can authenticate peers as a service to a number of EAP authenticators.

Typically, the authentication server is a Remote Authentication Dial-In User Service (RADIUS) server.

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 (TLS)
- EAP Tunneled TLS
- EAP Generalized Pre-Shared Key
- EAP-IKEv2

EAP LAYER

- EAP Layer exists on the top of the Data Link Layer
- EAP works on top of 802.1x (EAPOL)
- EAP facilitates the authentication of ARs running any data link layer technology (WLAN, Ethernet) using any of the authentication methods from higher layers
- For point to point protocol (PPP), EAPOL is not triggered.

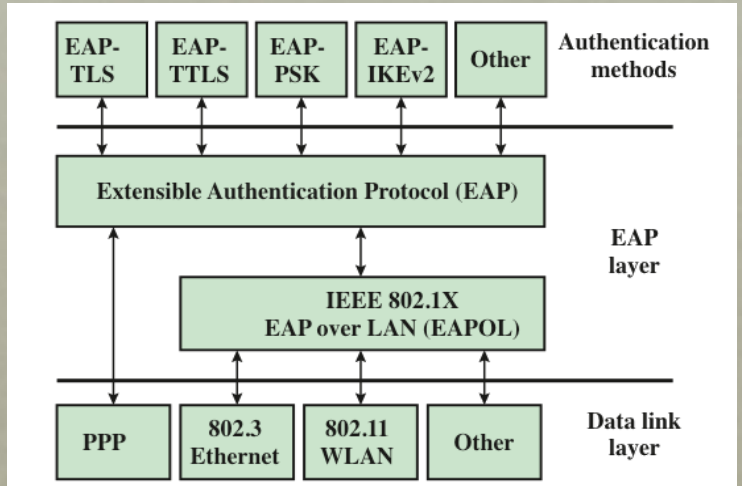


Figure 5.2 EAP Layered Context

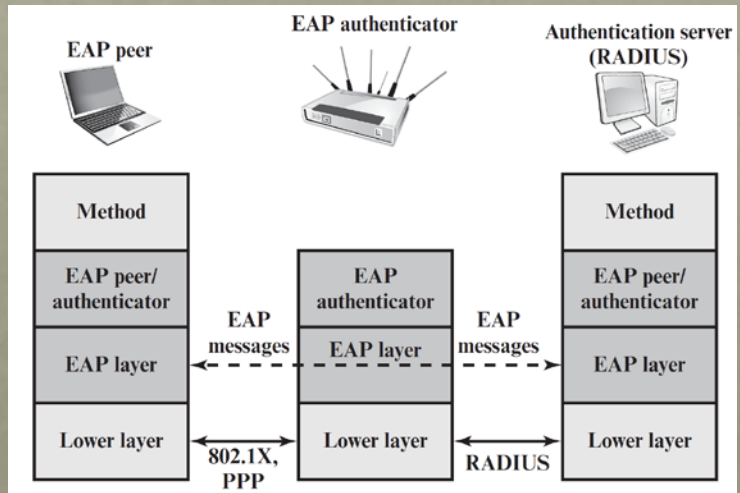


Figure 5.3 EAP Protocol Exchanges

EAP MESSAGE FLOW

The EAP authentication exchange proceeds as follows:

- The authenticator sends a Request to the peer to request an identity,
- and the peer sends a Response with the identity information.
- The server selects an EAP methods and sends the first EAP message with a **TYPE** field related to an authentication method.
- If the peer supports this methods, it replies with a response message of the same type.
- Otherwise the, the peer sends a NACK and the EAP server selects another method or sends a failure message

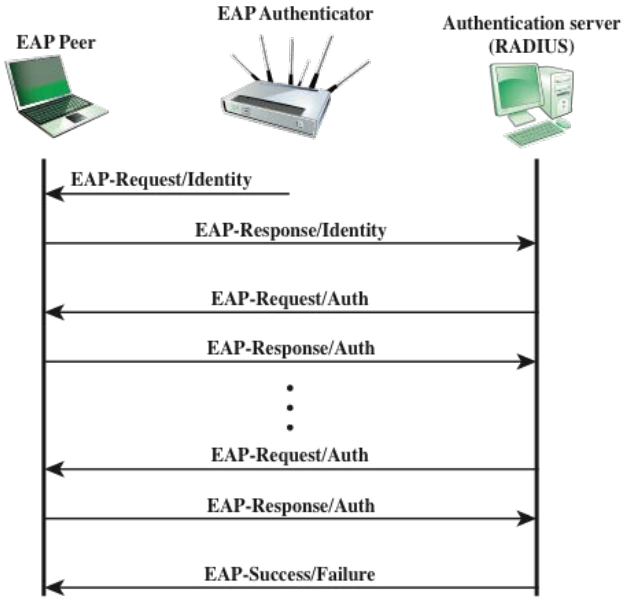


Figure 5.4 EAP Message Flow in Pass-Through Mode

EAP MESSAGE FLOW CONTINUED…

The EAP authentication exchange proceeds as follows:

- When the Authenticator and the peer agree on a method, this is followed by a sequence of Requests by the authenticator
- and Responses by the peer for the exchange of authentication information.
- The information exchanged and the number of Request–Response exchanges needed depend on the authentication method.

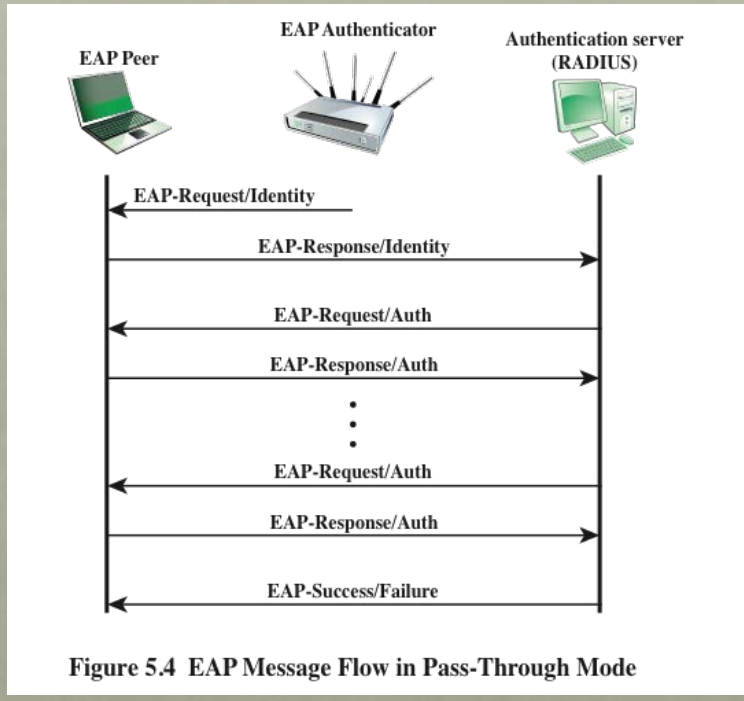


Figure 5.4 EAP Message Flow in Pass-Through Mode

- **The conversation continues until either**

(1) The authenticator determines that it cannot authenticate the peer and transmits an EAP Failure or

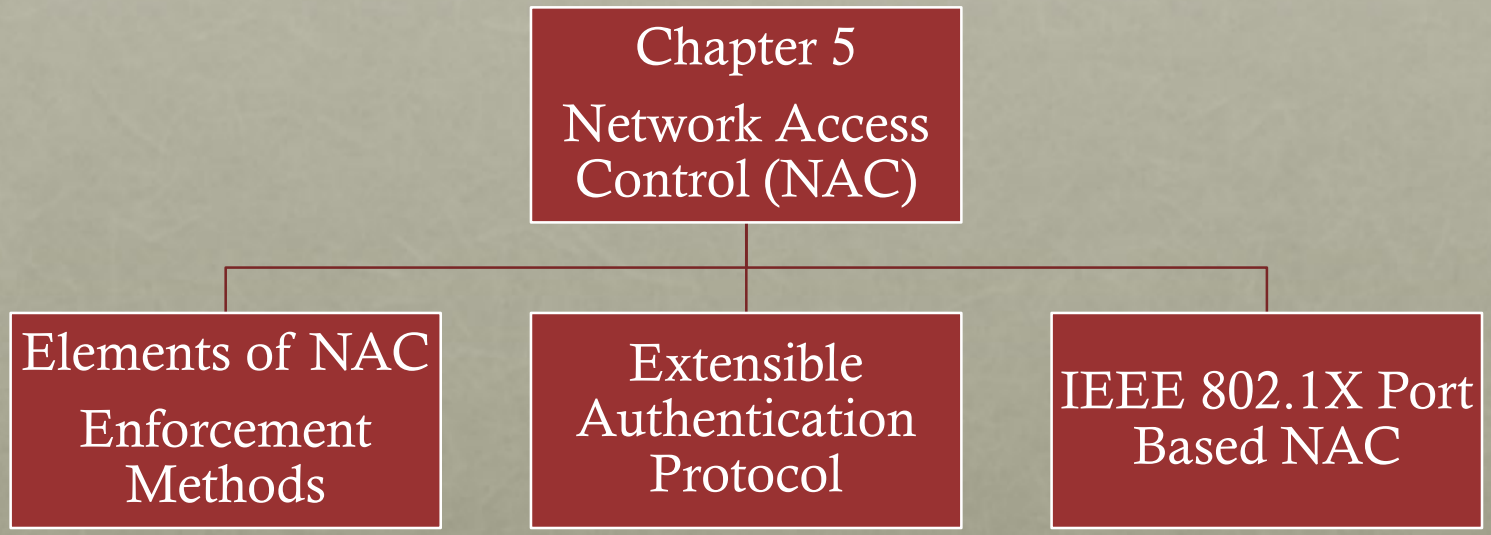
(2)the authenticator determines that successful authentication has occurred and transmits an EAP Success.

EAP MESSAGE FIELDS

- **Code**: Identifies the Type of EAP message. The codes are Request (1), Response (2), Success (3), and Failure (4).
- **Identifier**: Used to match Responses with Requests.
- **Length**: Indicates the length, in octets, of the EAP message, including the Code, Identifier, Length, and Data fields.
- **Data**: Contains information related to authentication. Typically, the Data field consists of a Type subfield, indicating the type of data carried, and a Type-Data field.

The Success and Failure messages do not include a Data field.

OUTLINE


Chapter 5
Network Access Control (NAC)
Elements of NAC
Enforcement Methods
Extensible Authentication Protocol
IEEE 802.1X Port Based NAC

802.1X PORT-BASED NAC

- 8021.1X Highlights
  - Until the AS authenticates a supplicant (AR), the authenticator only passes control and authentication messages.
  - After a successful completion of the authentication step, and keys are provided, the authenticator can forward data.
  - Essential element of 802.1X is a protocol known as EAP Over LAN (EAPOL)
  - EAPOL supports the exchange of EAP packets for authentication

802.1X ACCESS CONTROL

- 802.1X uses the concepts of controlled and uncontrolled ports.
- **An uncontrolled port:**
  - Allows the exchange of protocol data (authentication message, no user data is allowed to be exchanged yet!) units (PDUs) between the supplicant and the AS, regardless of the authentication state of the supplicant.
- **A controlled port**
  - Allows the exchange of PDUs between a supplicant and other systems on the network only if the current state of the supplicant authorizes such an exchange.
- **EAPOL** operates at the network layers and makes use of an IEEE 802 LAN, such as Ethernet or Wi-Fi, at the link level.
- **EAPOL** enables a supplicant to communicate with an authenticator and supports the exchange of EAP packets for authentication.

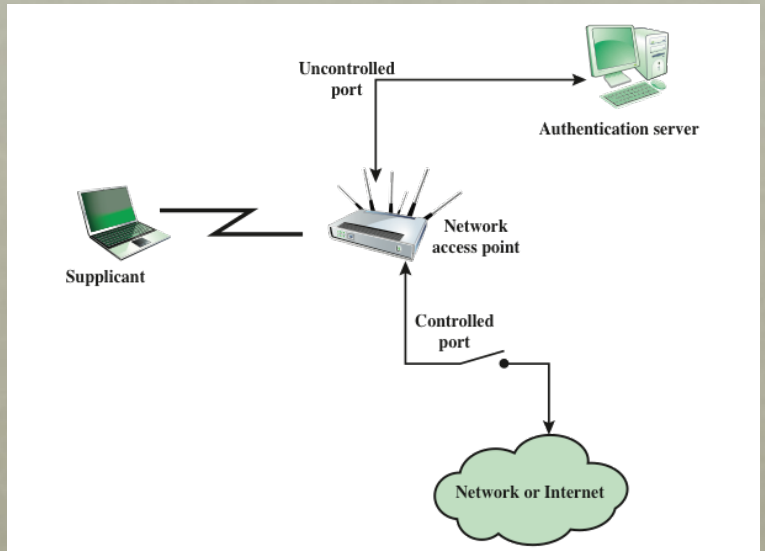


Figure 5.5 802.1X Access Control

Complete Ethernet Frame Structure with EAPOL-EAP

Field	Length (Bytes)	Description
Preamble	7	Used for synchronization
Start of Frame Delimiter (SFD)	1	Marks the end of the preamble and the start of the frame
Destination MAC	6	Destination Media Access Control address
Source MAC	6	Source Media Access Control address
EtherType	2	Type of payload (0x888E for EAPOL)
Protocol Version	1	EAPOL Protocol Version
Frame Type	1	EAPOL Packet Type (e.g., EAP Packet)
Packet Body Length	2	Length of the EAPOL packet body
Code	1	EAP Code (Request/Response/Success/Failure)
Identifier	1	EAP Identifier to match requests/responses
Length	2	Length of the EAP packet, including header
Type	1 (optional)	EAP Type (only for Request & Response)
Data	Variable	EAP Data (depends on EAP Type)
Frame Check Sequence (FCS)	4	Error-checking data calculated from the frame contents

EAPOL Payload

EAP Payload within EAPOL

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.

- By sending **EAPOL-Start** packet to a special group reserved for 802.1X authenticator, a supplicant can determine whether an authenticator is present or not.
- In many cases the authenticator gets notified when a new device gets connected.
-
- The authenticator uses the **EAPOL-Key** packet to send cryptographic keys to the supplicant once it has decided to admit it to the network.

- The “EAP-Request Identity” message is sent inside **EAPOL-EAP** packet

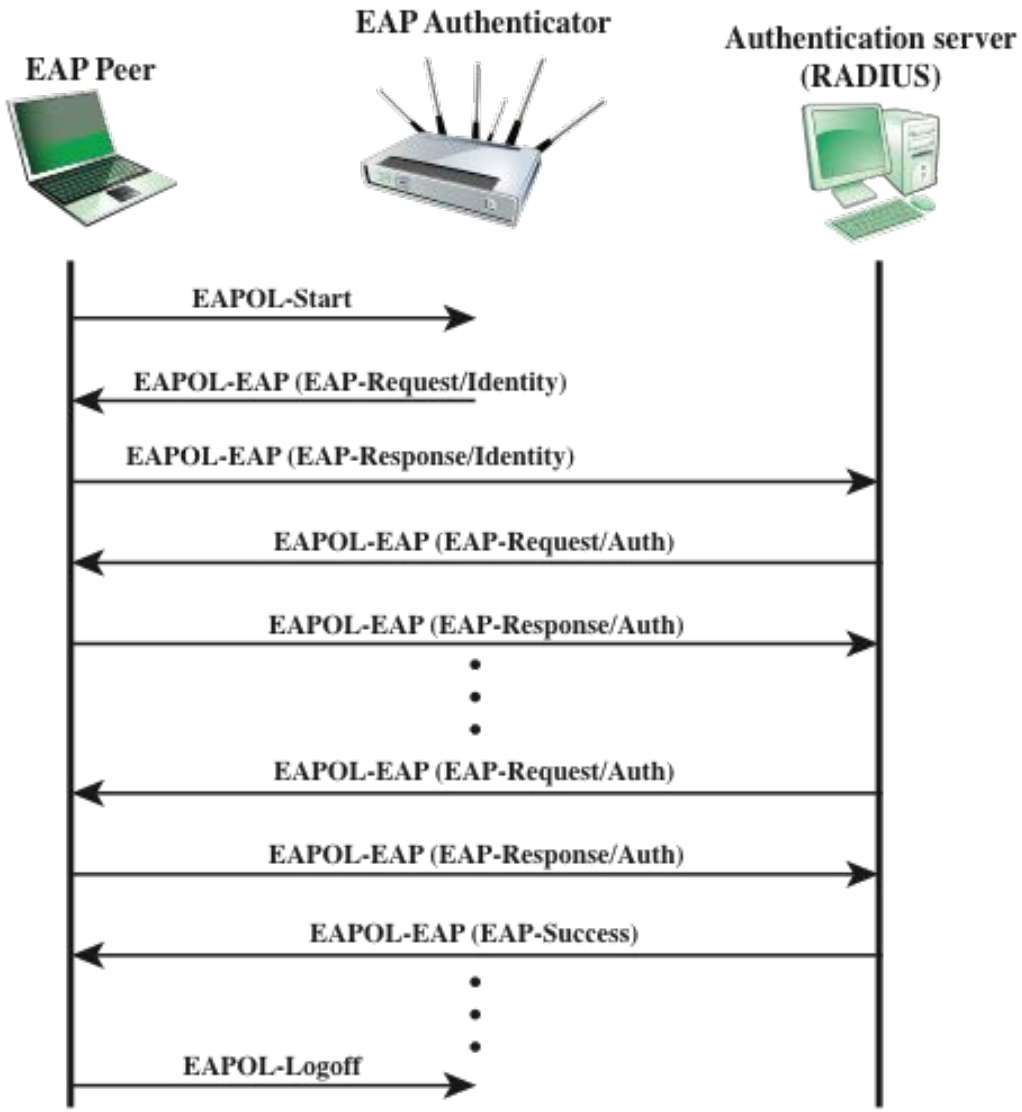


Figure 5.6 Example Timing Diagram for IEEE 802.1X

SUMMARY

- Network access control
  - Elements of a network access control system
  - Network access enforcement methods
- Extensible authentication protocol
  - Authentication methods
  - EAP exchanges
- IEEE 802.1X port-based network access control