# Authentication, Authorization and Accounting (AAA)

**Prof. Chien-Chao Tseng**

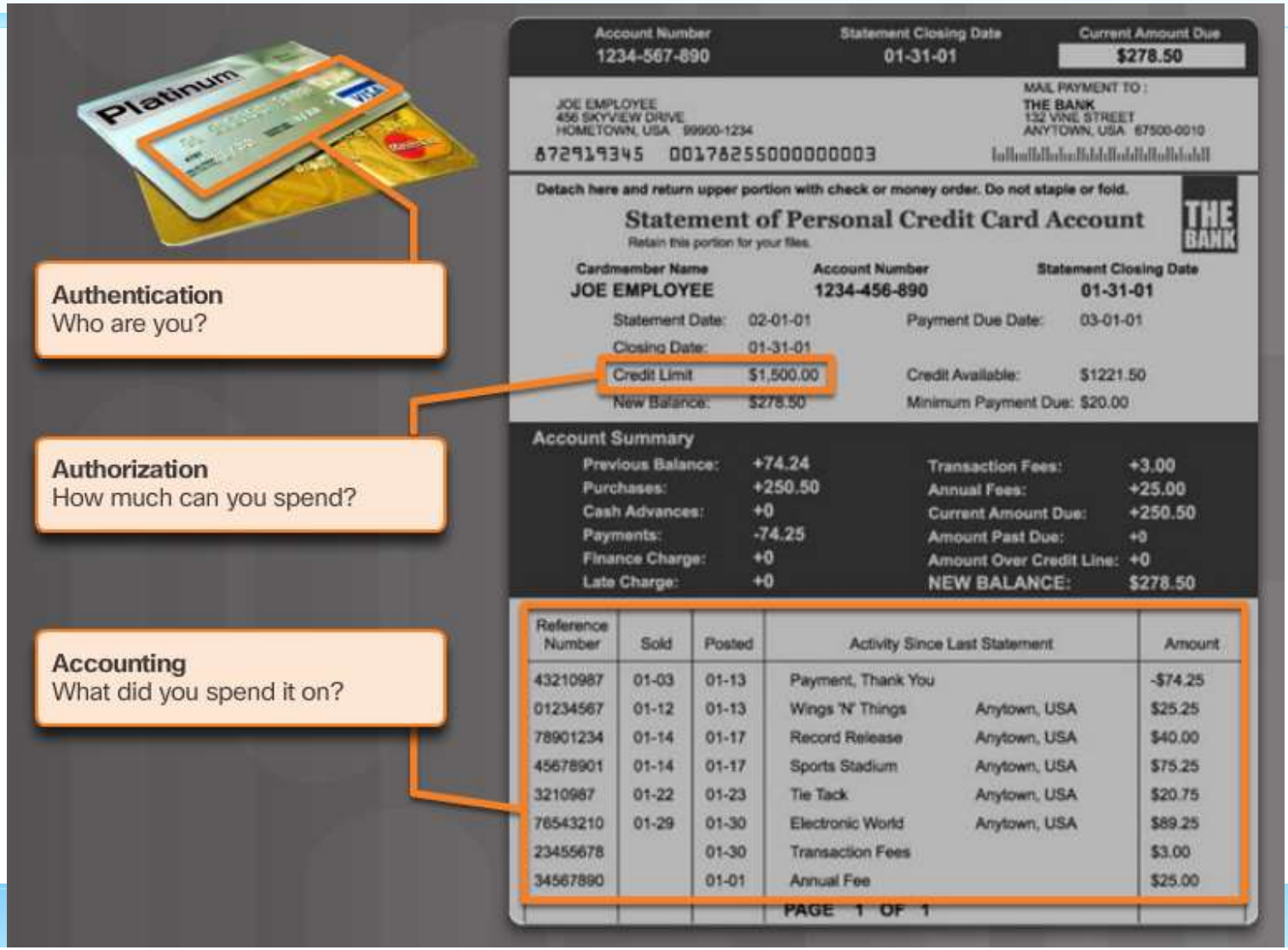
曾 建 超 教授

Department of Computer Science
National Yang Ming Chiao Tung University

cctseng@cs.nctu.edu.tw

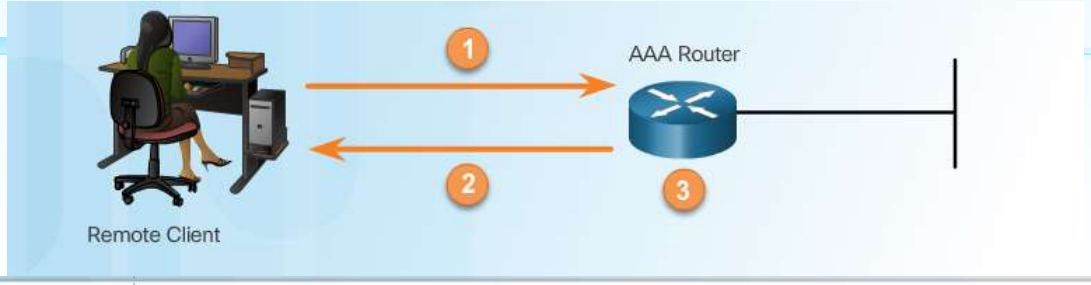
References:
Chapter 3 Authentication, Authorization, and Accounting, CCNA V2.0, Cisco Networking Academy
Remote Authentication Dial-In User Service (RADIUS)- 2058, 2138, 2865
(updated by RFC 2868, RFC 3575, RFC 5080 )

# Authentication, Authorization and Accounting (AAA)



# Authentication Modes

Local AAA Authentication

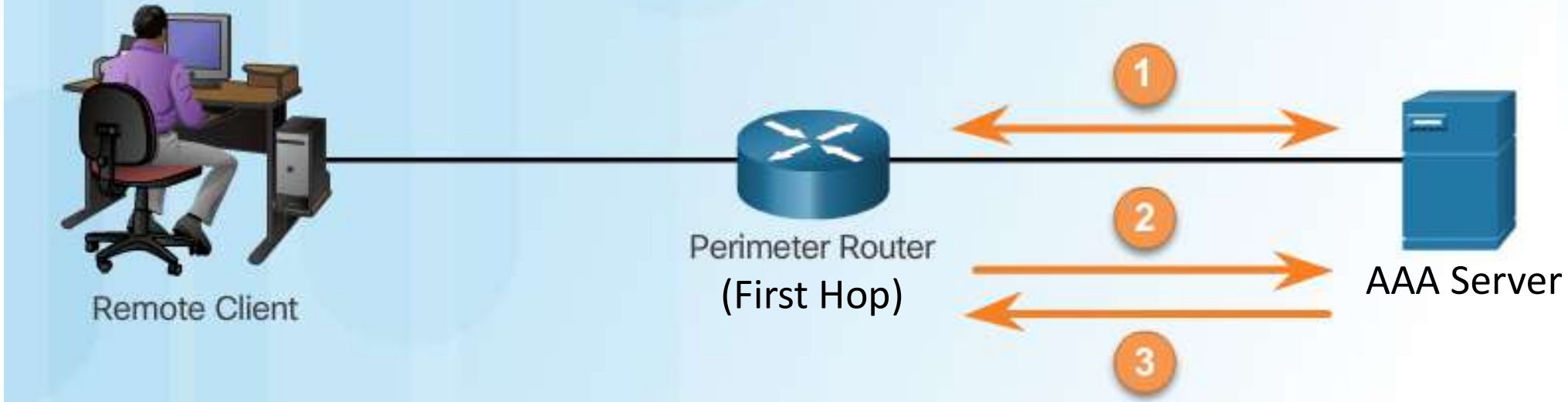



1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is authorized to access the network based on information in the local database.

Server-Based AAA Authentication


1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server.
4. The user is authorized to access the network based on information on the remote AAA Server.

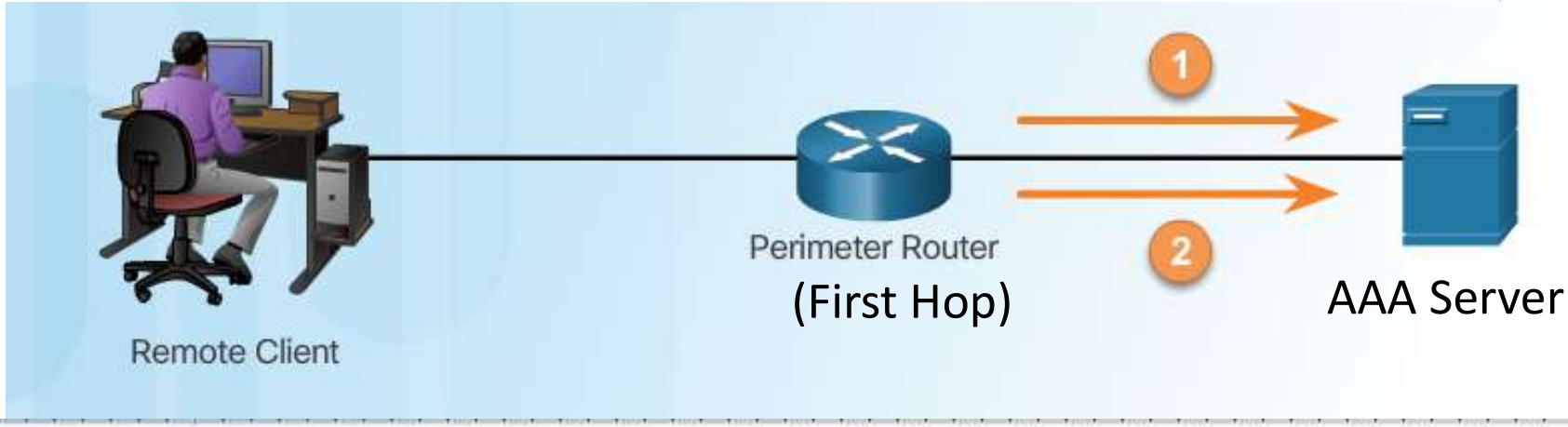
# AAA Authorization




1. When a user has been authenticated, a session is established with the AAA server.
2. The router requests authorization for the requested service from the AAA server.
3. The AAA server returns a PASS/FAIL for authorization.

# AAA Accounting

- Types of accounting information:
  - Network
  - Connection
  - EXEC
  - System
  - Command
  - Resource




1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded and the accounting process ends.

# AAA and RADIUS

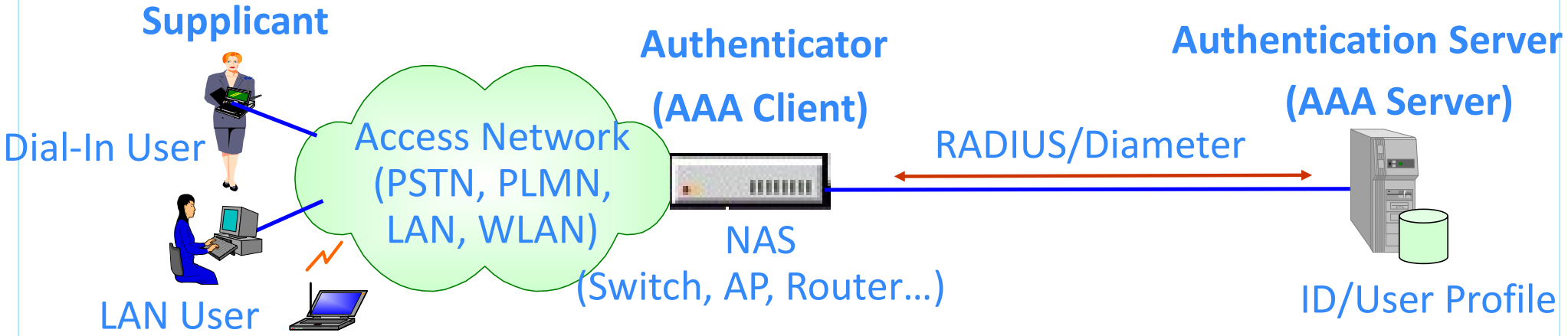
- **AAA = Authentication, Authorization, & Accounting**
  - Authentication: Who are you?
  - Authorization: What can you do?
  - Accounting: What did you do?


(RADIUS Server)

- **RADIUS = Remote Authentication Dial In User Service**
  - An efficient protocol to manage a single database of users for
    - Authentication (verifying user name and credentials)
    - Service provisioning
      - Delivering configuration information of services,
        - e.g., PPP, Telnet, and rlogin
  - Originally developed to manage **dial-in** access to the Internet.
  - Leveraged for other applications and using other access methods.

# AAA Server and RADIUS/Diameter

- **Network Access Server** (NAS) operates as a **Security Client (AAA Client)**
- **Security Server** (AAA Server) and AAA **client** may use **RADIUS or Diameter** as a communication protocol.
- IEEE 802.1X Terms: (**Port-Based** Network Access Control)
  - **Supplicant**: entity wants to join the network
  - **Authenticator**: entity controls the access
  - **Authentication Server (AS)**: entity makes authorization decisions

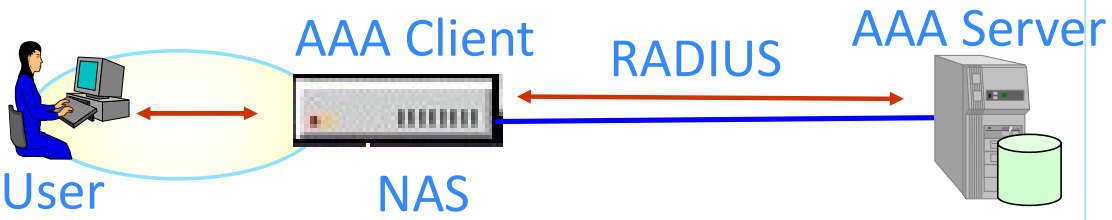


# Introduction to RADIUS

- ✓ Was developed as an **access server authentication and accounting protocol**
  - By Livingston Enterprises, Inc.
  - Uses UDP Port 1812 (1645 in early deployment )

**1) User** presents **authentication information** to **RADIUS client** (NAS)

- User name, password, …, via
  - Customized login prompt, or
  - Link frame protocol,
    - such as Point-to-Point Protocol (PPP)



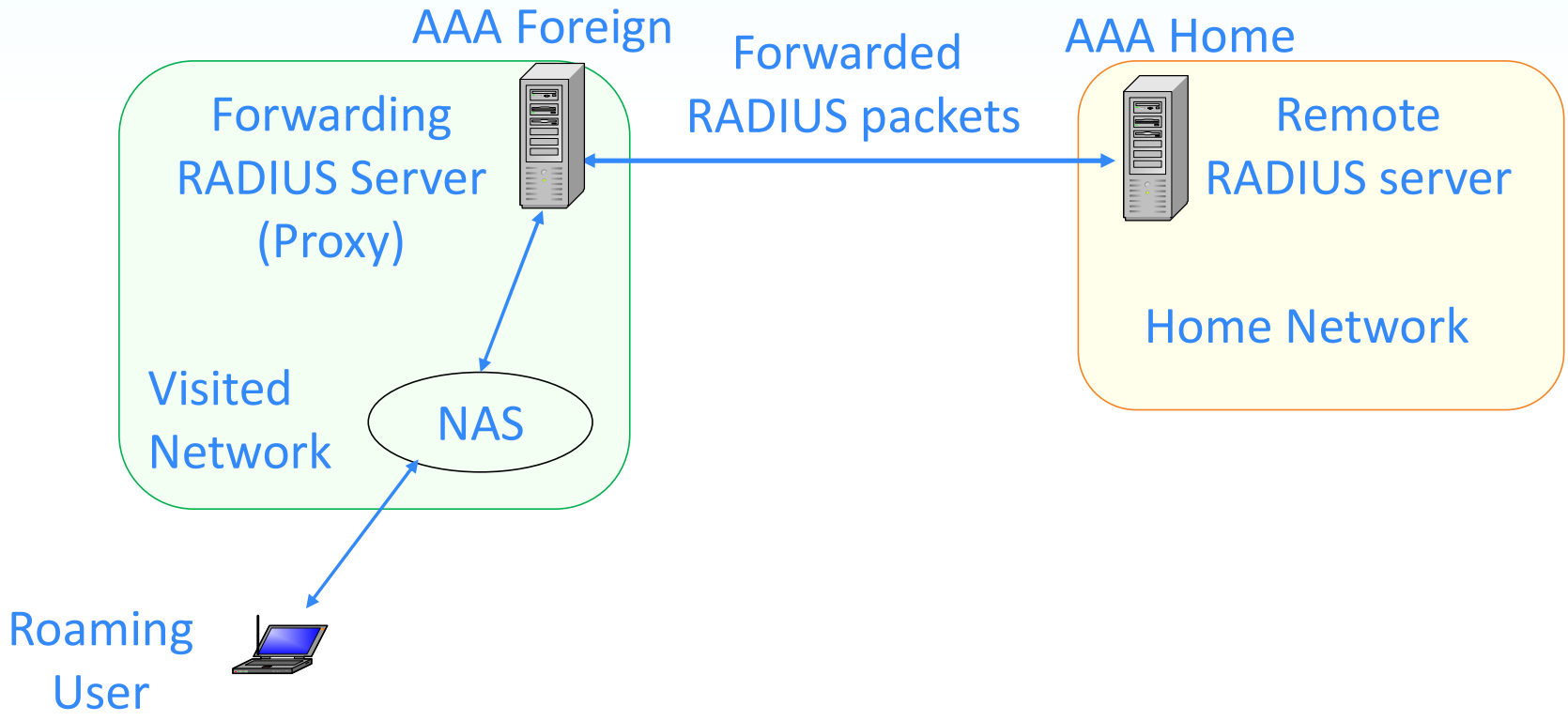

**2) NAS** sends an "Access-Request" message to RADIUS Server

- "Access-Request" message contains **authentication information,**
- May use Message Digest Algorithm MD5 one-way hash function to hide user password
  - NAS and RADIUS servers share a common "secret"

**3) RADIUS server** consults a user database to validate users

# RADIUS for Roaming Users

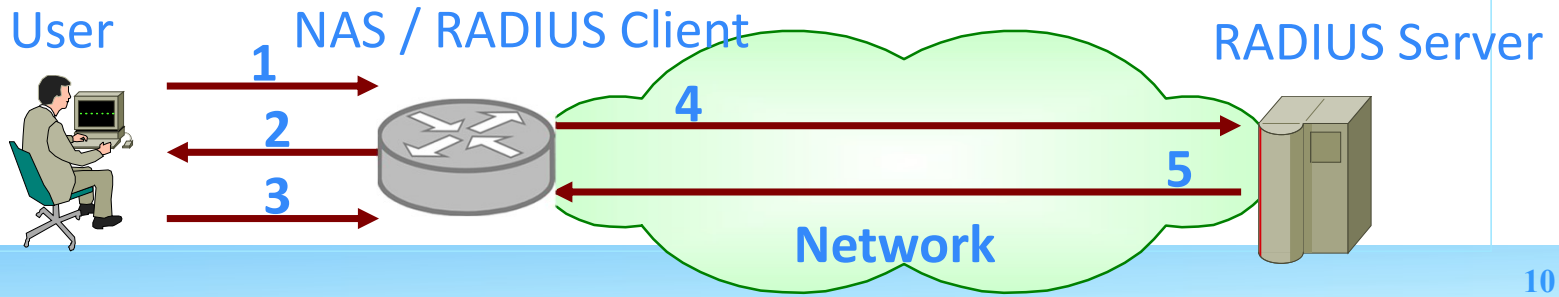
- With Proxy RADIUS, RADIUS can support authentication for **roaming users**



# RADIUS Operations

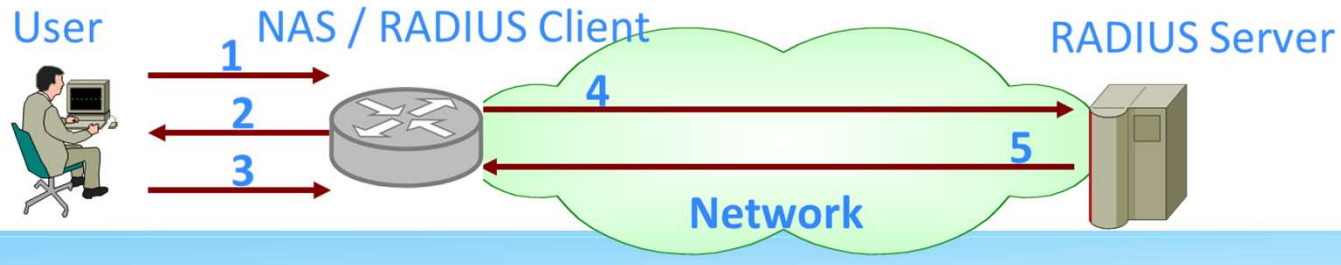
1. User initiates a PPP authentication to the NAS
2. NAS asks for authentication information, possibly
   - Username/Password (for Password Authentication Protocol; PAP) or
   - Challenge (for Challenge-handshake Authentication Protocol; CHAP)
3. User replies with Username and Password (or Challenge)
4. NAS sends user authentication information to RADIUS server
   - Username and encrypted Password (PAP) or
   - Challenge, response, and identity (CHAP)
5. RADIUS server responds with Accept/Reject (or Challenge)

✍ **NAS** acts upon **service parameters** bundled with Accept/Reject

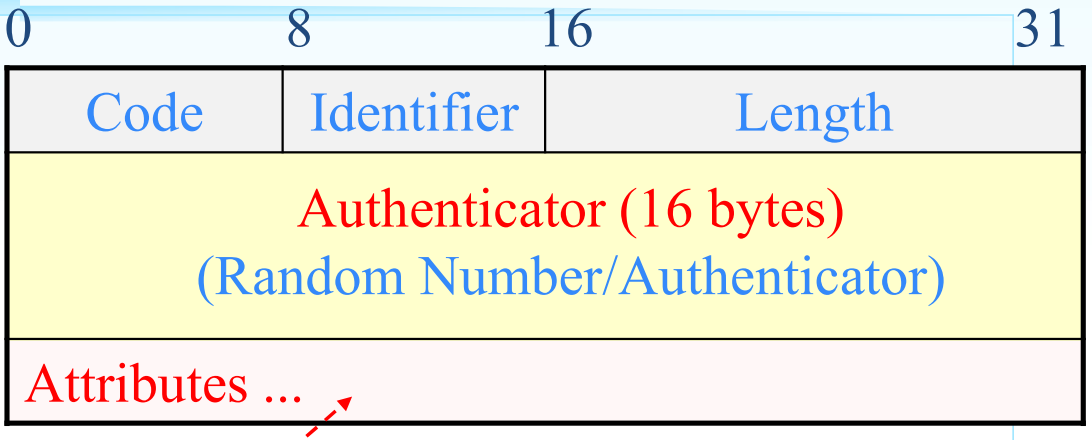


# RADIUS Client and Server Mutual Authentication

- NAS operates as a RADIUS Client.
- RADIUS server
  - is responsible for user authentication and
  - returns user configuration information to RADIUS Client (NAS)
- Mutual Authentication between RADIUS Client and Server:
  RADIUS Server and each RADIUS client share a "**secret**"
  - RADIUS Server: uses source IP of the request to retrieve the shared secret
    - Request from a client without a shared secret MUST be silently discarded
  - RADIUS client: uses **Response Message** (**Response Authenticator**) to validate packets responded from a legal RADIUS server



# RADIUS Packet Format




- Code (1 octet)
  - Type of RADIUS Packet (next slide)
- Identifier (1 octet)
  - Matching requests and replies and detecting duplicate packets
- Length (2 octets)
  - Length of the packet in octets (20 ~ 4096)
- **Attributes (TLV)**
  - Specific **authentication** and **authorization information** and **configuration** details for a **request** or a **reply**, e.g., **User-Name**, **User-Password**, … (Page 15)
- **Authenticator** (16 octets)
  - Request **Authenticator**: **a random Number** used in Password Hiding Algorithm
    - Value of **User-Password** attribute **=** XOR(**password**, MD5(**secret**, **authenticator**))
  - Reply **Authenticator**: used to verify the reply from RADIUS server

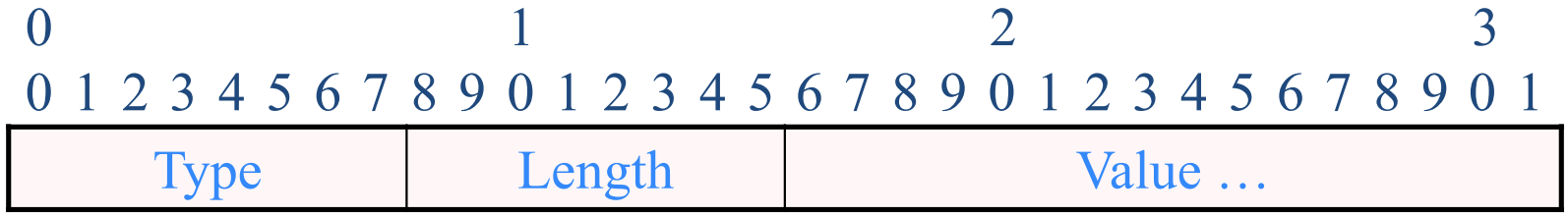
# Code List

Codes

| | |
|---|---|
| 1 | Access-Request |
| 2 | Access-Accept |
| 3 | Access-Reject |
| 4 | Accounting-Request |
| 5 | Accounting-Response |
| 11 | Access-Challenge |
| 12 | Status-Server (experimental) |
| 13 | Status-Client (experimental) |
| 255 | Reserved |

# Attribute Format

- Type (1 octet)
  - Type of RADIUS Attributes
- Length (1 octet)
  - Length of Attribute, including Type, Length and Value fields
  - Max length of Value is 253 bytes
- Value (variable in length)
  - Zero or more octets,
  - Information specific to the Attribute




✍ Examples: User name, Password, Configuration information, …

# RADIUS Attributes List

## Original Support (RFC 2865)

| | | | |
|---|---|---|---|
| 1 | User-Name | 23 | Framed-IPX-Network |
| 2 | User-Password | 24 | State |
| 3 | CHAP-Password | 25 | Class |
| 4 | NAS-IP-Address | 26 | Vendor-Specific |
| 5 | NAS-Port | 27 | Session-Timeout |
| 6 | Service-Type | 28 | Idle-Timeout |
| 7 | Framed-Protocol | 29 | Termination-Action |
| 8 | Framed-IP-Address | 30 | Called-Station-Id |
| 9 | Framed-IP-Netmask | 31 | Calling-Station-Id |
| 10 | Framed-Routing | 32 | NAS-Identifier |
| 11 | Filter-Id | 33 | Proxy-State |
| 12 | Framed-MTU | 34 | Login-LAT-Service |
| 13 | Framed-Compression | 35 | Login-LAT-Node |
| 14 | Login-IP-Host | 36 | Login-LAT-Group |
| 15 | Login-Service | 37 | Framed-AppleTalk-Link |
| 16 | Login-TCP-Port | 38 | Framed-AppleTalk-Network |
| 17 | (unassigned) | 39 | Framed-AppleTalk-Zone |
| 18 | Reply-Message | 40-59 | (reserved for accounting) |
| 19 | Callback-Number | 61 | NAS-Port-Type |
| 20 | Callback-Id | 62 | Port-Limit |
| 21 | (unassigned) | 63 | Login-LAT-Port |
| 22 | Framed-Route | 63 | Login-LAT-Port |

## Tunnel Protocol Support (RFC 3162)

| | |
|---|---|
| 64 | Tunnel-Type |
| 65 | Tunnel-Medium-Type |
| 66 | Tunnel-Client-Endpoint |
| 67 | Tunnel-Server-Endpoint |
| 69 | Tunnel-Password |
| 81 | Tunnel-Private-Group-ID |
| 82 | Tunnel-Assignment-ID |
| 83 | Tunnel-Preference |
| 90 | Tunnel-Client-Auth-ID |
| 91 | Tunnel-Server-Auth-ID |

EAP: Extensible Authentication Protocol

## EAP (RFC 2869)

| | |
|---|---|
| 79 | EAP-Message |
| 80 | Message-Authenticator |

## IPv6 (RFC 2868)

| | |
|---|---|
| 95 | NAS-IPv6-Address |
| 96 | Framed-Interface-Id |
| 97 | Framed-IPv6-Prefix |
| 98 | Login-IPv6-Host |
| 99 | Framed-IPv6-Route |
| 100 | Framed-IPv6-Pool |

# EAP Extension of RADIUS (RFC 3579 )

EAP: Extensible Authentication Protocol (RFC 2869)

- RFC 3579 defines two new RADIUS attributes:
  - Type 79: EAP-Message
  - Type 80: Message-Authenticator
- EAP-Message: Type 79
  - Value field contains **EAP message**
  - If multiple **EAP-Message** attributes are present, their values should be concatenated.
    - ➢ Allows EAP packets longer than 253 octets.
- Message-Authenticator (MA): Type 80, 16 bits
  - For integrity check of RADIUS packets
  - Shared secret is used as the key for HMAC-MD5.
    - MA = HMAC-MD5(Type, Id, Length, Request Authenticator, Attributes)

| Code | Identifier | Length |
|---|---|---|
| Authenticator (16 bytes)<br>(Random Number/Authenticator) | | |
| Attributes ... | | |

| Type | Length | Value |
|---|---|---|
| 79 | ≤ 253 | EAP Message |
| 80 | 2 | MA |

- Multiple EAP-Message attributes

| | | |
|---|---|---|
| 79 | 253 | Value … |
| 79 | ≤ 253 | Value … |

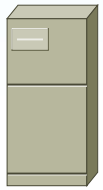
HMAC: Hash-based message authentication code, MD: Message-Digest

# IEEE 802.11i architecture

MN/Supplicant

AP/Authenticator

Authentication Server (AS)



**802.11 three phases**
[Probe]
[Authentication]
[Association]

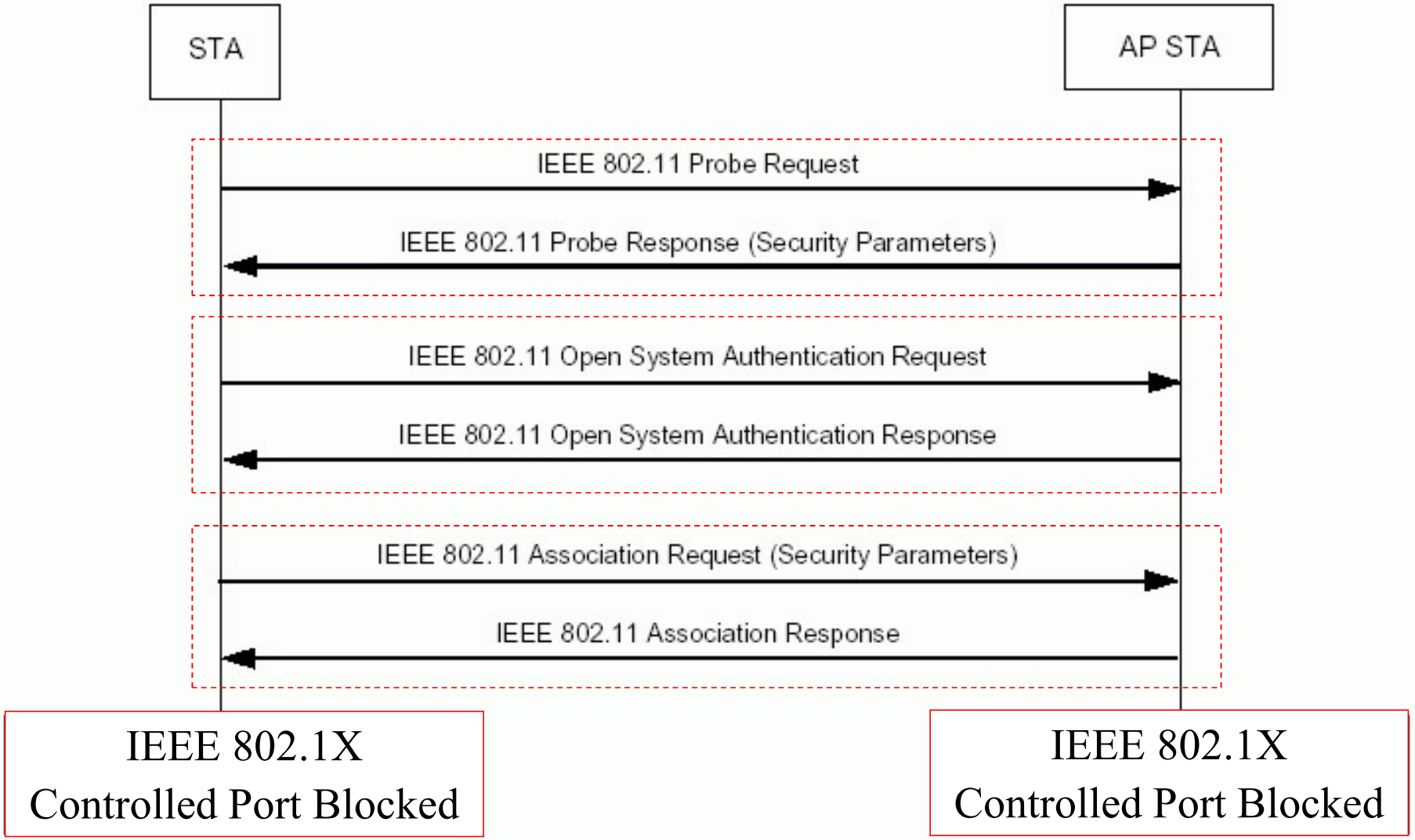
**802.1X/EAPOL Authentication**

**4-Way Handshake**

IEEE 802.11i

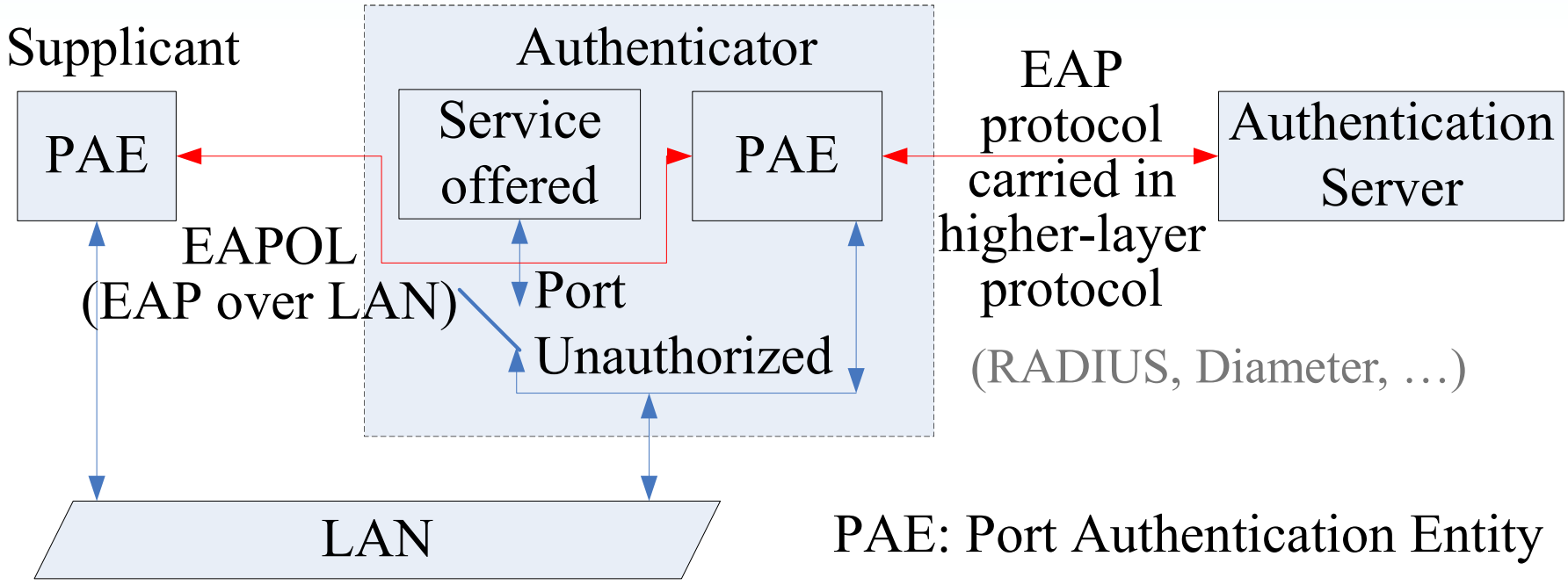
EAPOL: Extensible Authentication Protocol over LAN

# IEEE 802.11 Probe/Authentication/Association

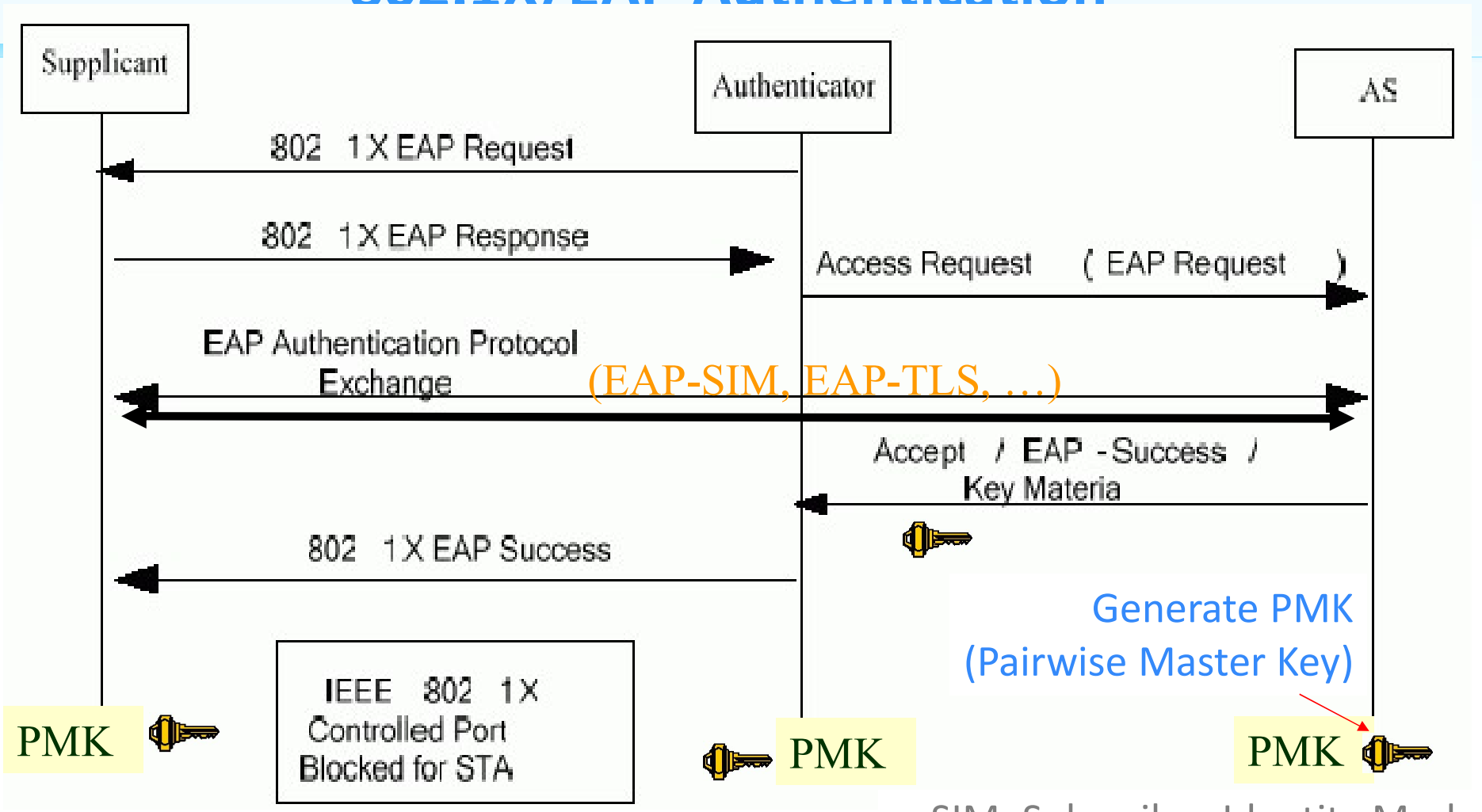


# Role of 802.1X Authenticator

- 802.1X Authenticator



# 802.1X/EAP Authentication

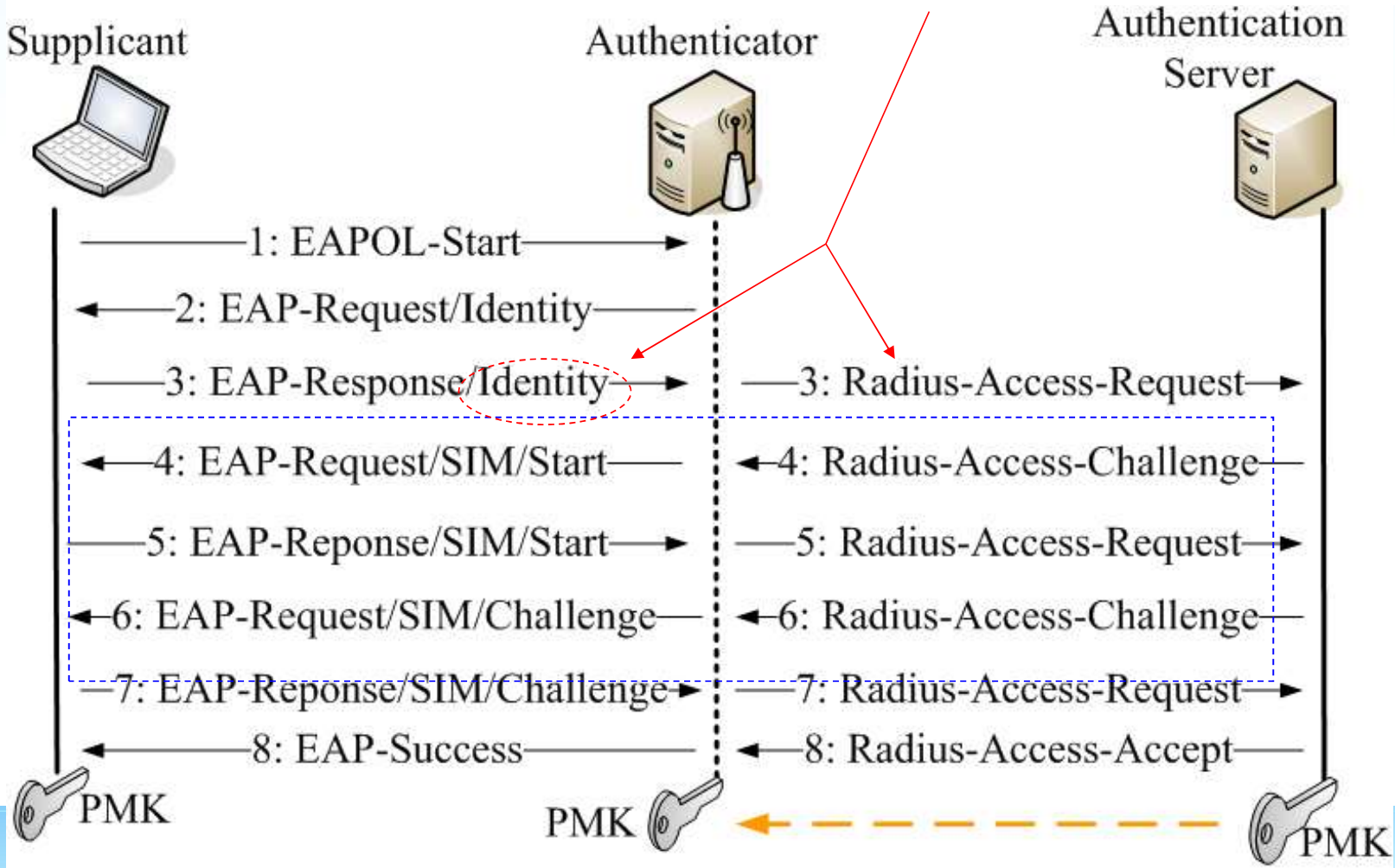



- Supplicant and AS can authenticate each other

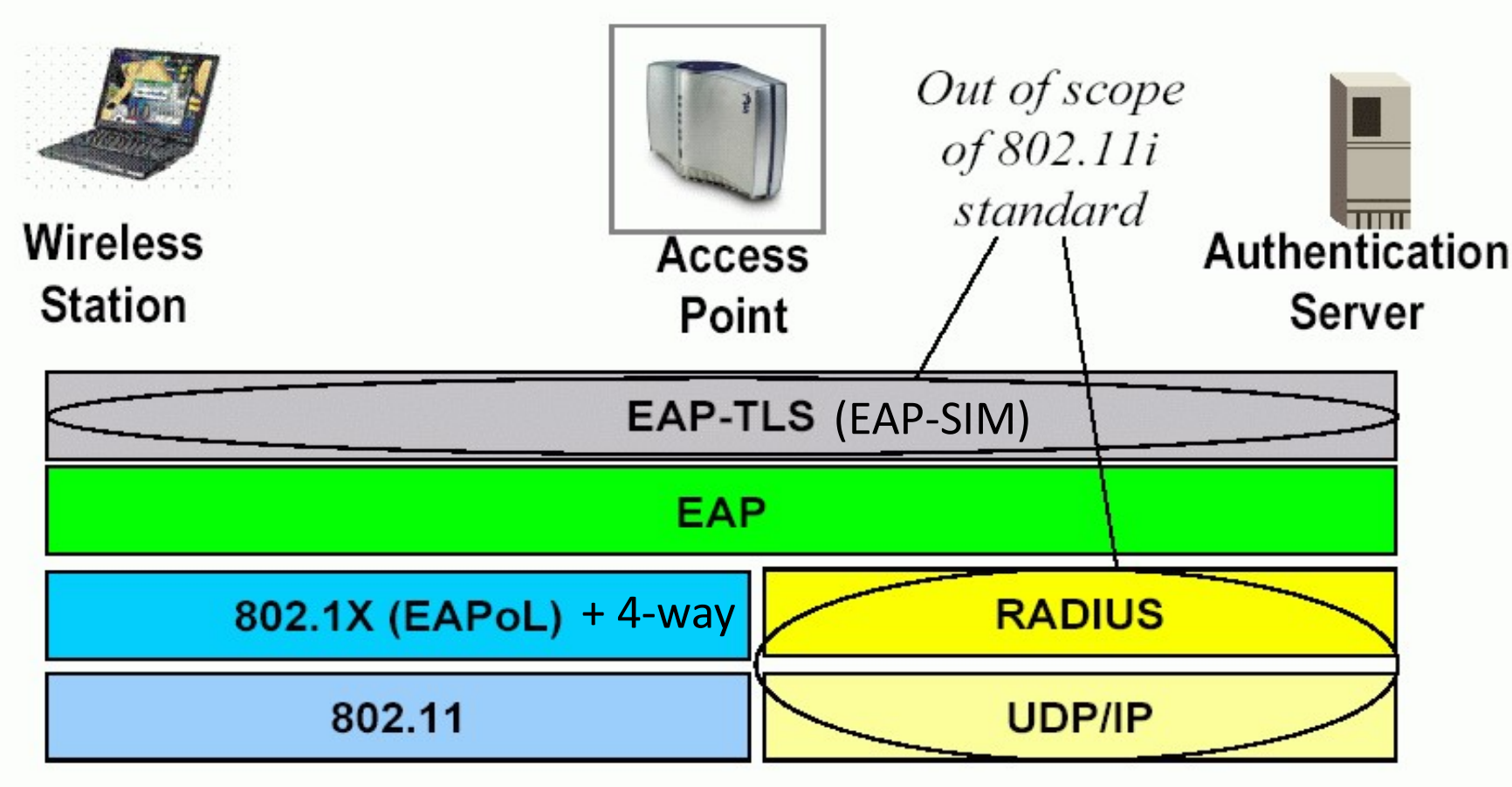
- SIM: Subscriber Identity Module
- TLS: Transport Layer Security

# EAP-SIM Authentication

- Identity used to retrieve the associated authentication policy.



# 802.11i Protocol Stack

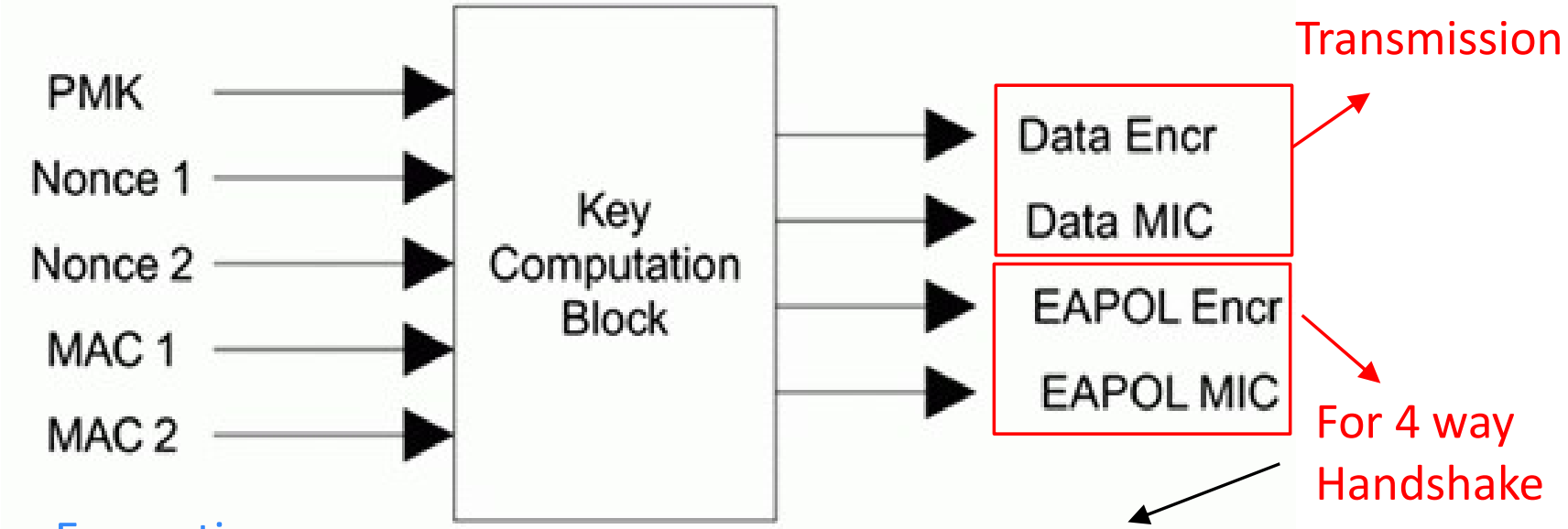



**EAPoL: EAP over LAN** **TLS: Transport Layer Security**

**RADIUS: Remote Authentication Dial-In User Service** RSN: Robust Security Network

# 4 Way Handshake - Keys

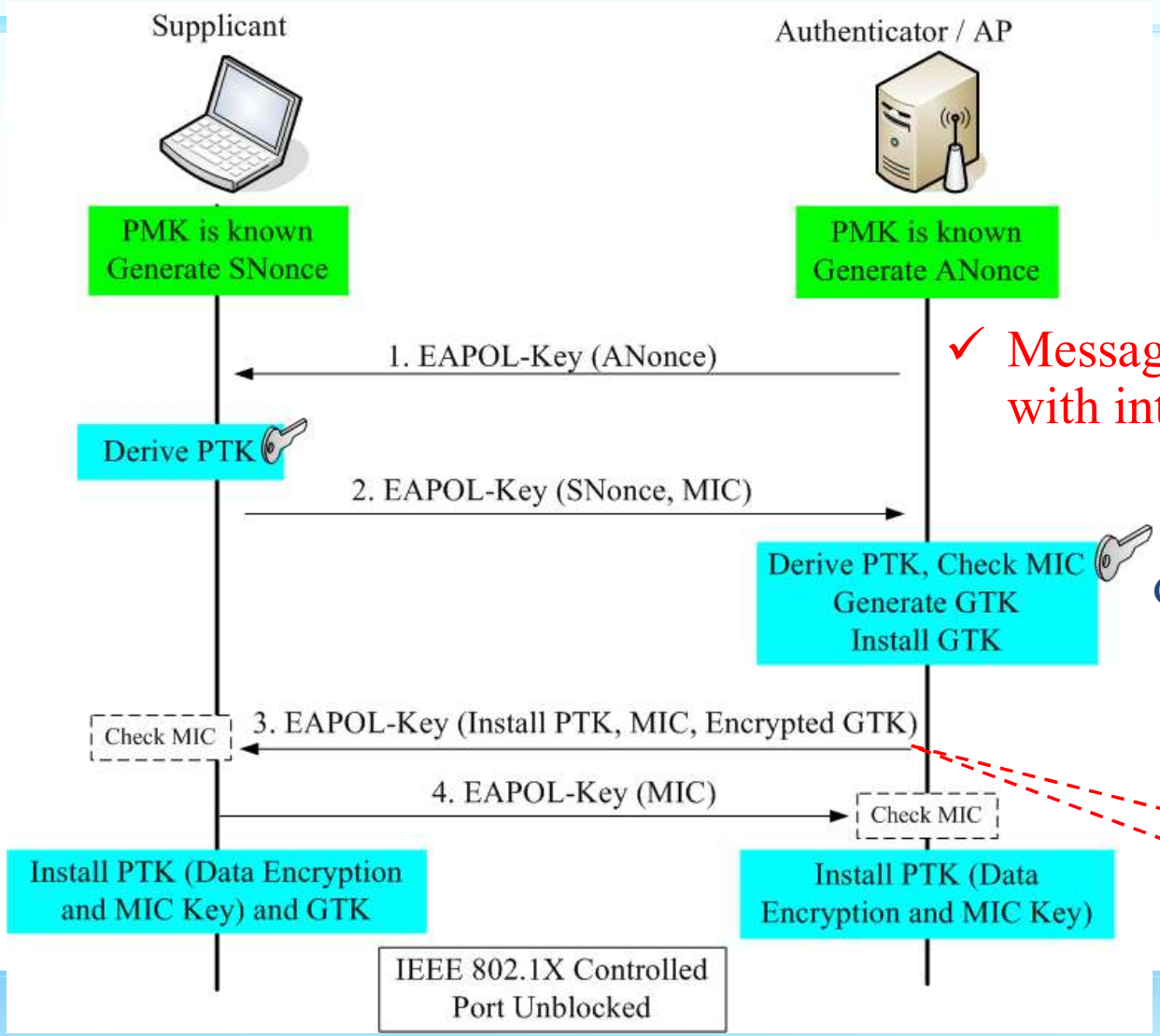
1) Synchronize Pairwise Master Key (PMK) between Supplicant and Authenticator
2) Generate Pairwise Temporal Key (PTK)
   - Data Encr, Data MIC (for data transmission)
   - EAPOL Encr, EAPOL MIC (for 4 Way Handshake)




- Encr: Encryption
- MIC: Message Integrity Code

➢ Allow supplicant and authenticator to exchange secret key information securely

# 4-Way Handshake - Messages




✓ Message 2, 3 and 4 are with integrity check

GTK: Group Temporal Key

**Encrypt GTK with EAPOL Encryption Key**