



# Authentication and Security: IEEE 802.1x and protocols EAP based

Pietro Nicoletti  
piero[at]studioreti.it



# Copyright note

- These slides are protected by copyright and international treaties. The title and the copyrights concerning the slides (inclusive, but not only, every image, photograph, animation, video, audio, music and text) are the author's (see Page 1) property.
- The slides can be copied and used by research institutes, schools and universities affiliated to the Ministry of Public Instruction and the Ministry of University and Scientific Research and Technology, for institutional purpose, not for profit. In this case there is not requested any authorization.
- Any other complete or partial use or reproduction (inclusive, but not only, reproduction on discs, networks and printers) is forbidden without written authorization of the author in advance.
- The information contained in these slides are believed correct at the moment of publication. They are supplied only for didactic purpose and not to be used for installation-projects, products, networks etc. However, there might be changes without notice. The authors are not responsible for the content of the slides.
- In any case there can not be declared conformity with the information contained in these slides.
- In any case this note of copyright may never be removed and must be written also in case of partial use.



# Radius

- **R.A.D.I.U.S.:** **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice protocol is used to exchange authentication message from Authenticator and Server
  - The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned
  - RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user
  - RADIUS protocol has been used in the past by Internet Service Providers to authenticate users connected via Dial-Up line to the Access Server



## IEEE 802.1x

- Define a Port Base Network Access Control functions
  - Use physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics (Dial-Up), and of preventing access to that port in cases where the authentication and authorization process fails
- Can be implemented on Switch and Wireless Access Point



## 802.1x main elements

### ■ Authenticator:

- is an entity at one end of a point-to-point LAN segment that requires to authenticate the entity attached to the other end of that link

### ■ Authentication Server:

- is an entity that provides an Authentication Service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the Authenticator



## 802.1x main elements

- Supplicant:
  - is an entity at one end of a point-to-point LAN segment that is being authenticated by an Authenticator attached to the other end of that link (example a Switch)
  - can also an entity that want to be associated and authenticated in a Wireless LAN environment through Access Point
- Port Access Entity (PAE):
  - Is a entity protocol associated to the authenticator, the supplicant or both

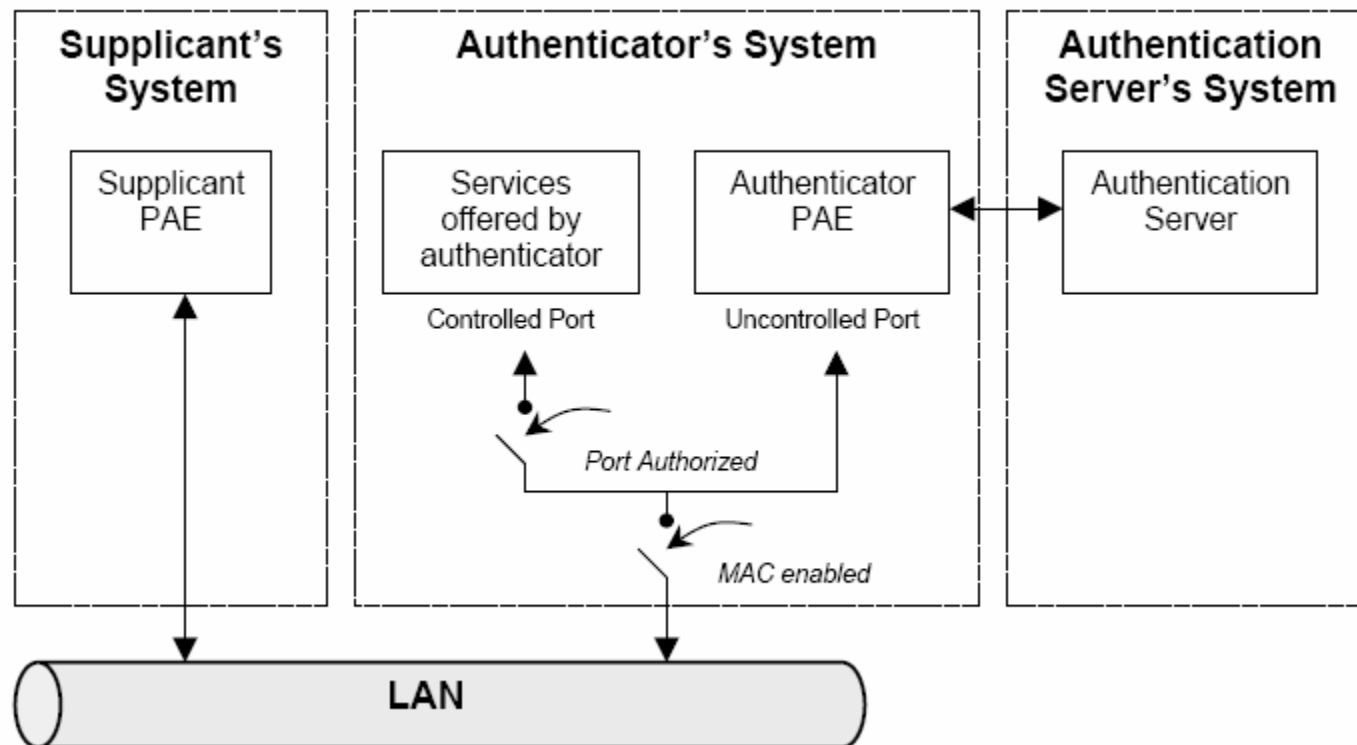


# 802.1x function and protocols used to authenticate supplicant

- Protocol used for communication between Authenticator and Authenticator Server:
  - EAP (Extensible Authentication Protocol) over RADIUS protocol
    - RADIUS is a Layer 7 protocol (application layer)
- Protocol used for communication between Supplicant and Authenticator
  - EAPOL that means EAP Over LAN
    - Is a Layer 2 Protocol because the supplicant may not have an IP address until is authenticated and has been received the IP address by DHCP Server

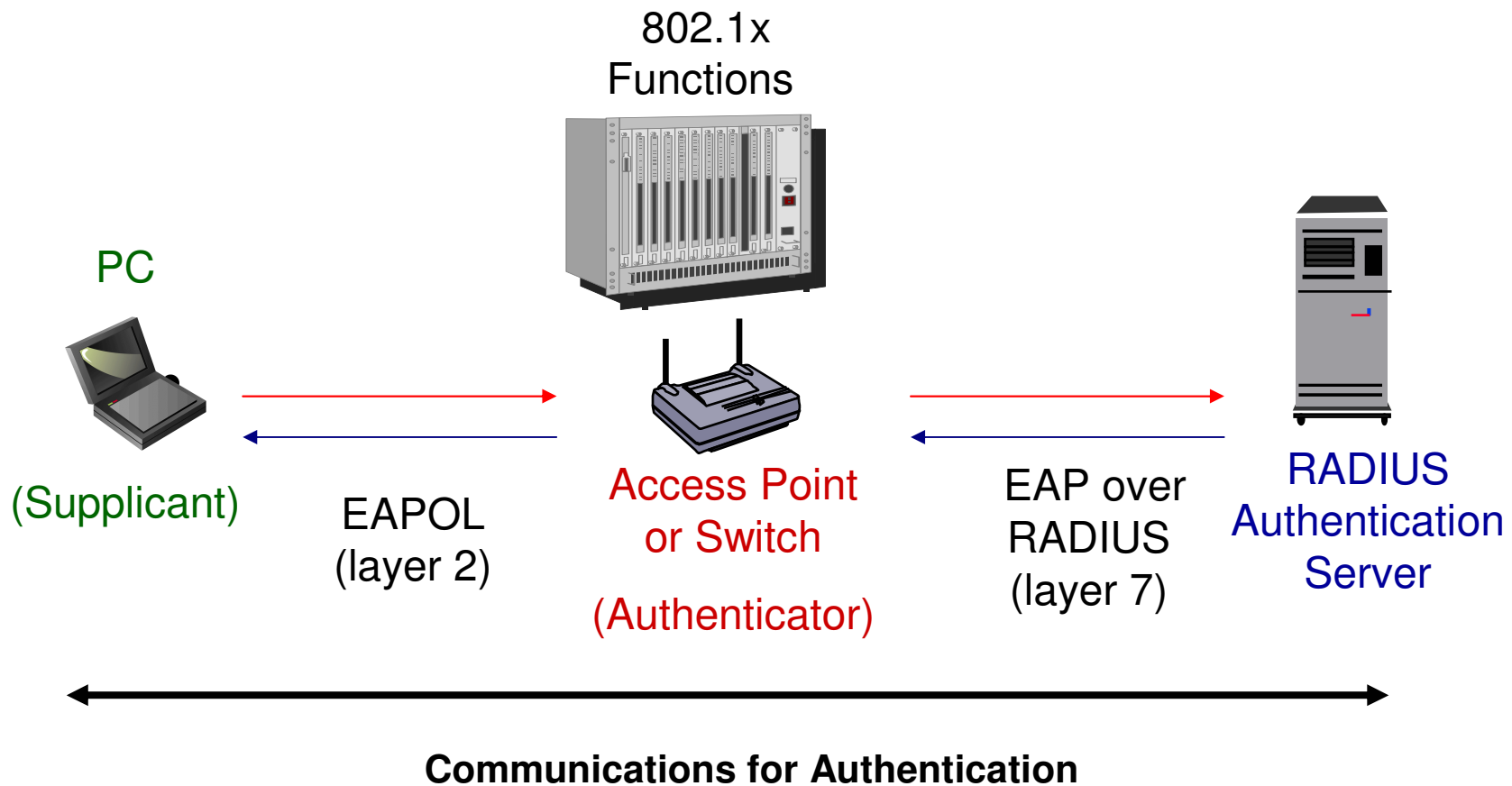


# Authentication elements





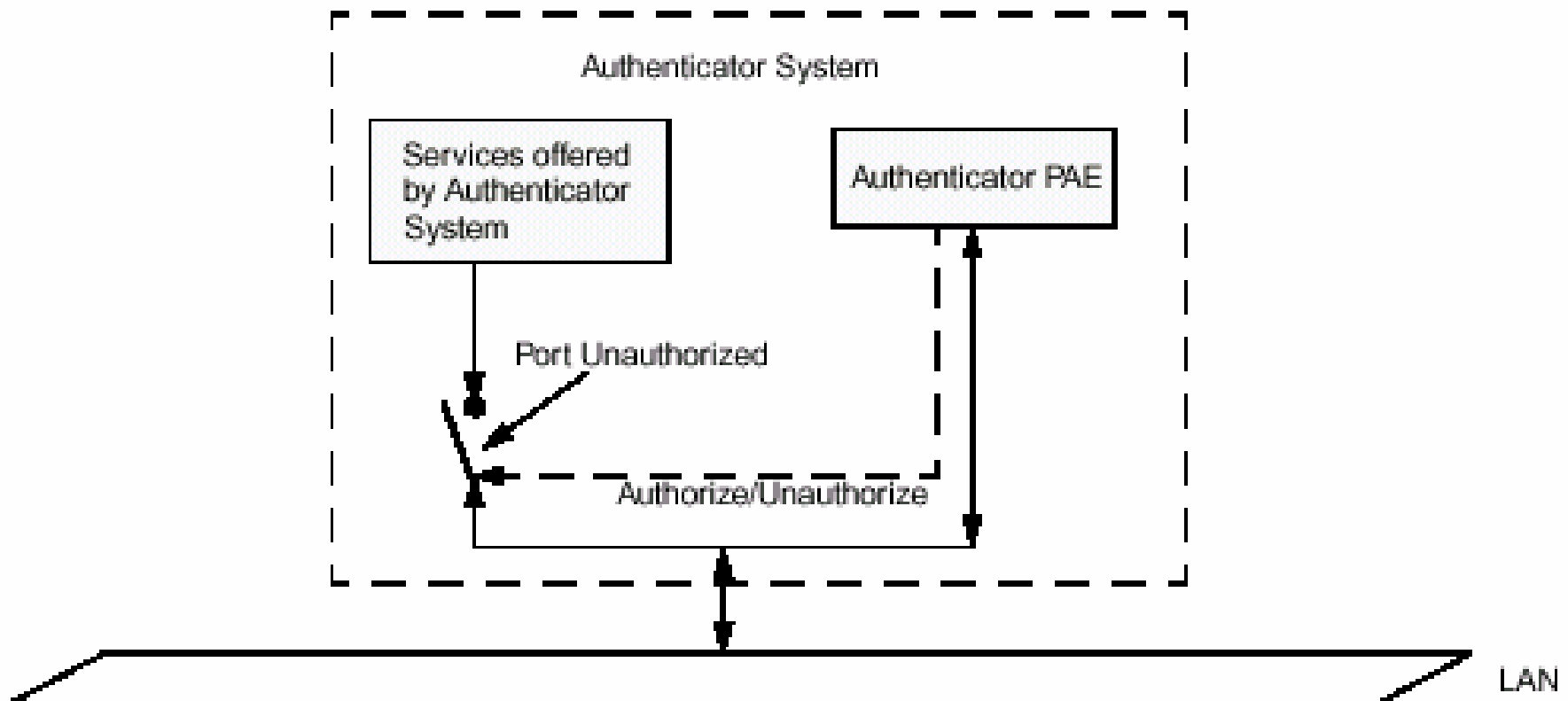
# 802.1x Authentication Model





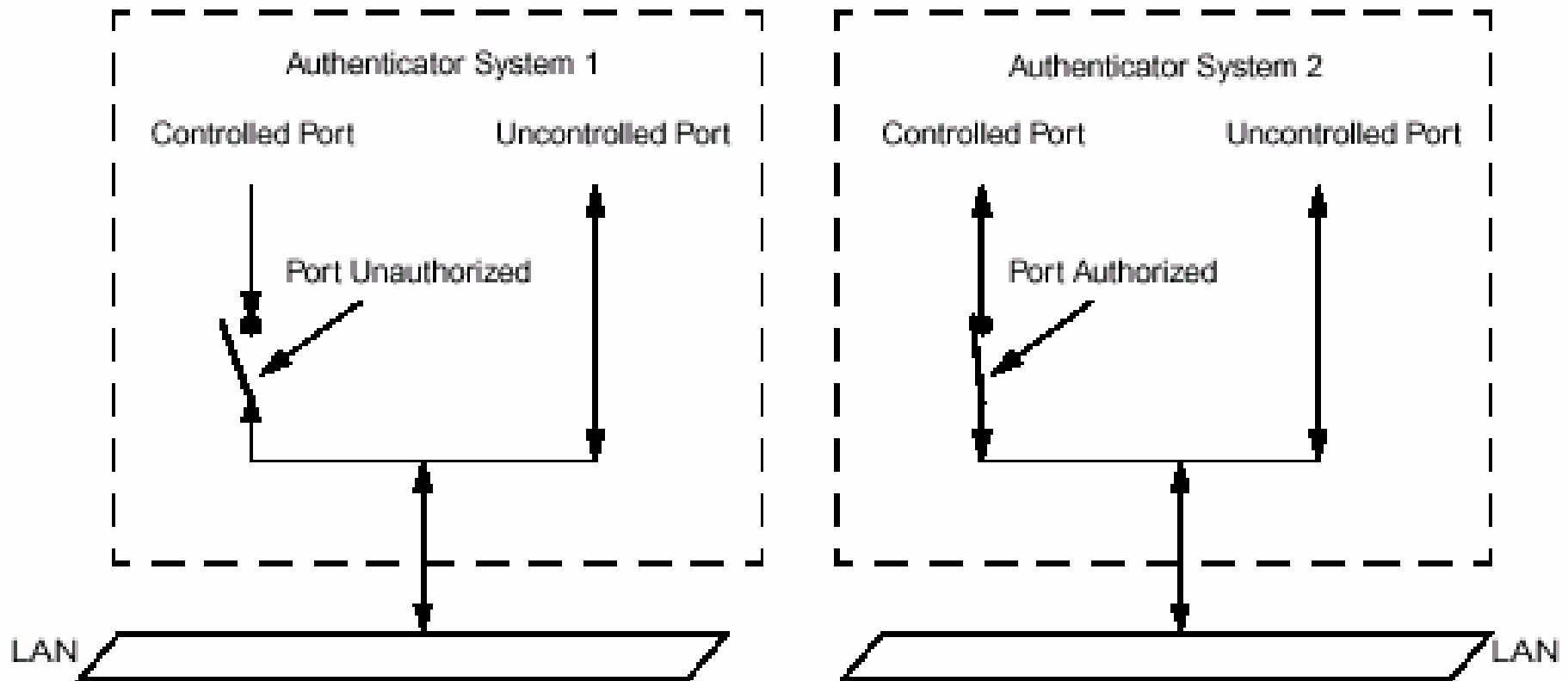
## Use of Controlled & Uncontrolled Port

- Uncontrolled Port is the entity used for service packets exchange her necessary to establishing the authorization or the access prohibition



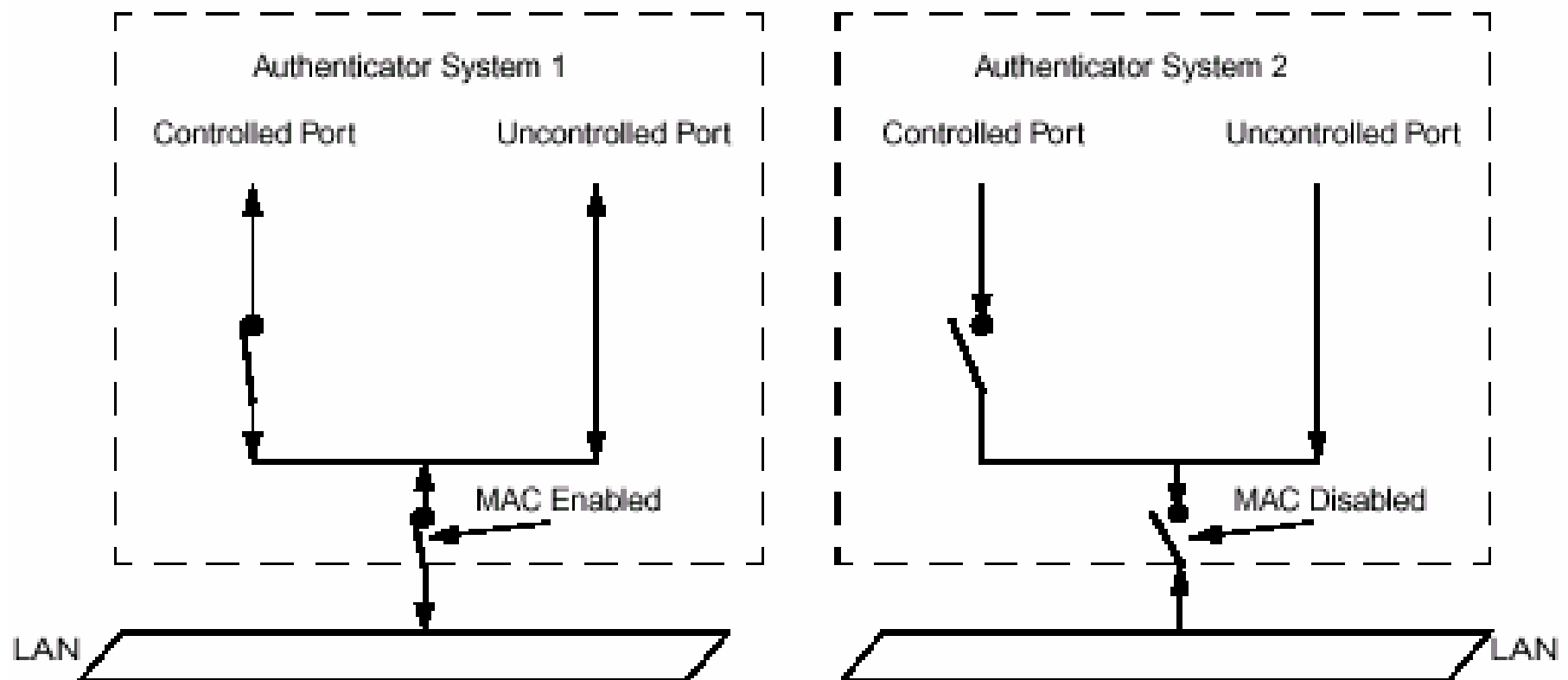


# Authorized & Unauthorized port





# Access based on Authentication & Address MAC



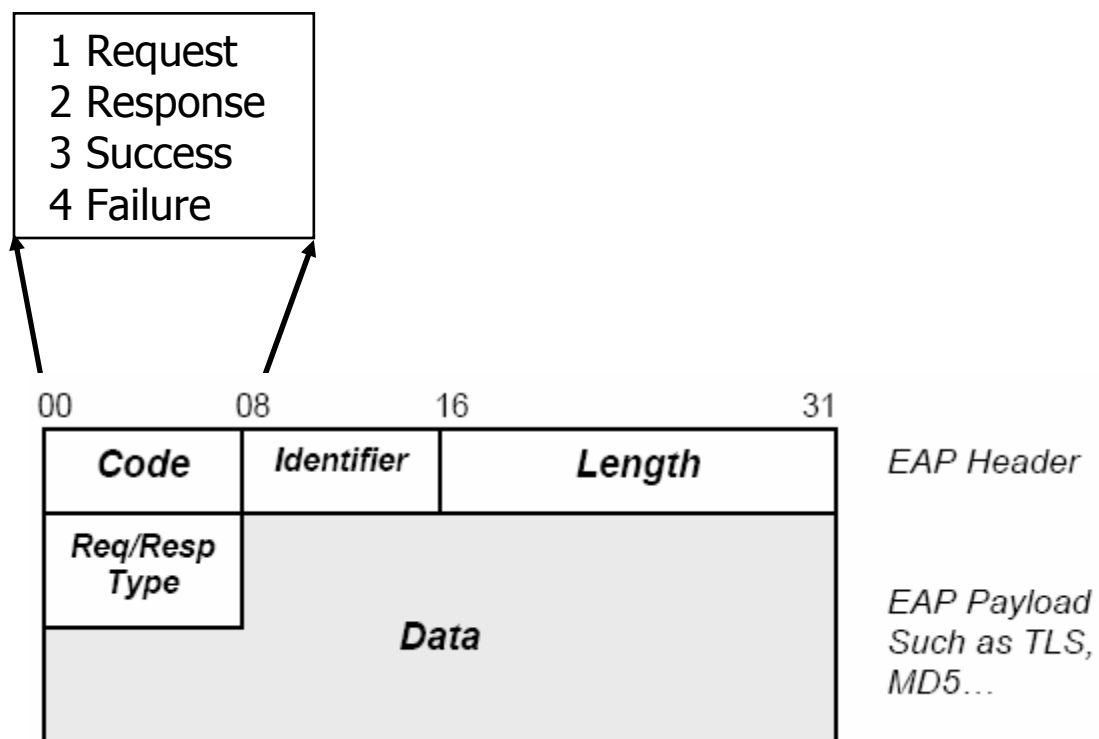


# EAP protocol

- PPP Extensible Authentication Protocol (EAP) defined in RFC 2284
  - Protocol code EAP = c227
  - Support multiple authentication mechanisms without needing to pre-negotiate a specific mechanism during the LCP phase
  - PPP was originally only supporting authentications based up
    - PAP (Authentication Protocol password), protocol code c023
    - CHAP (Authentication Protocol handshake Challenge), c223 protocol code



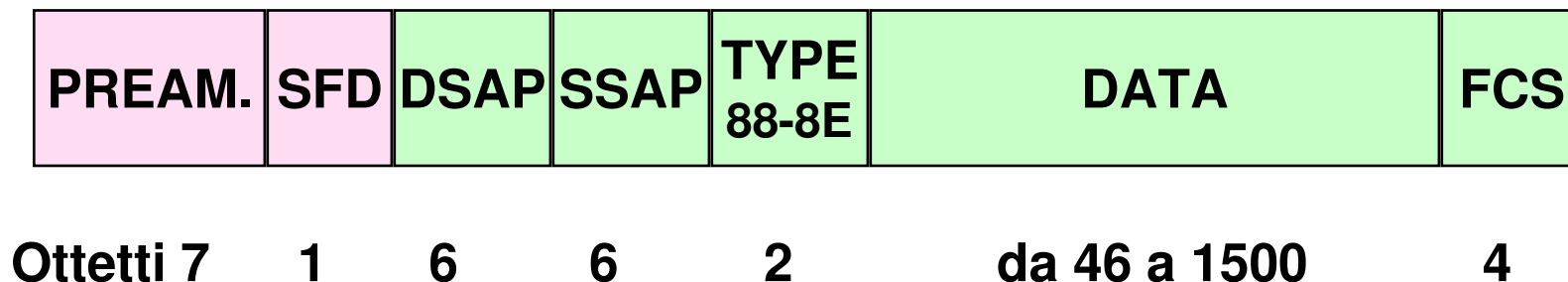
# EAP frame





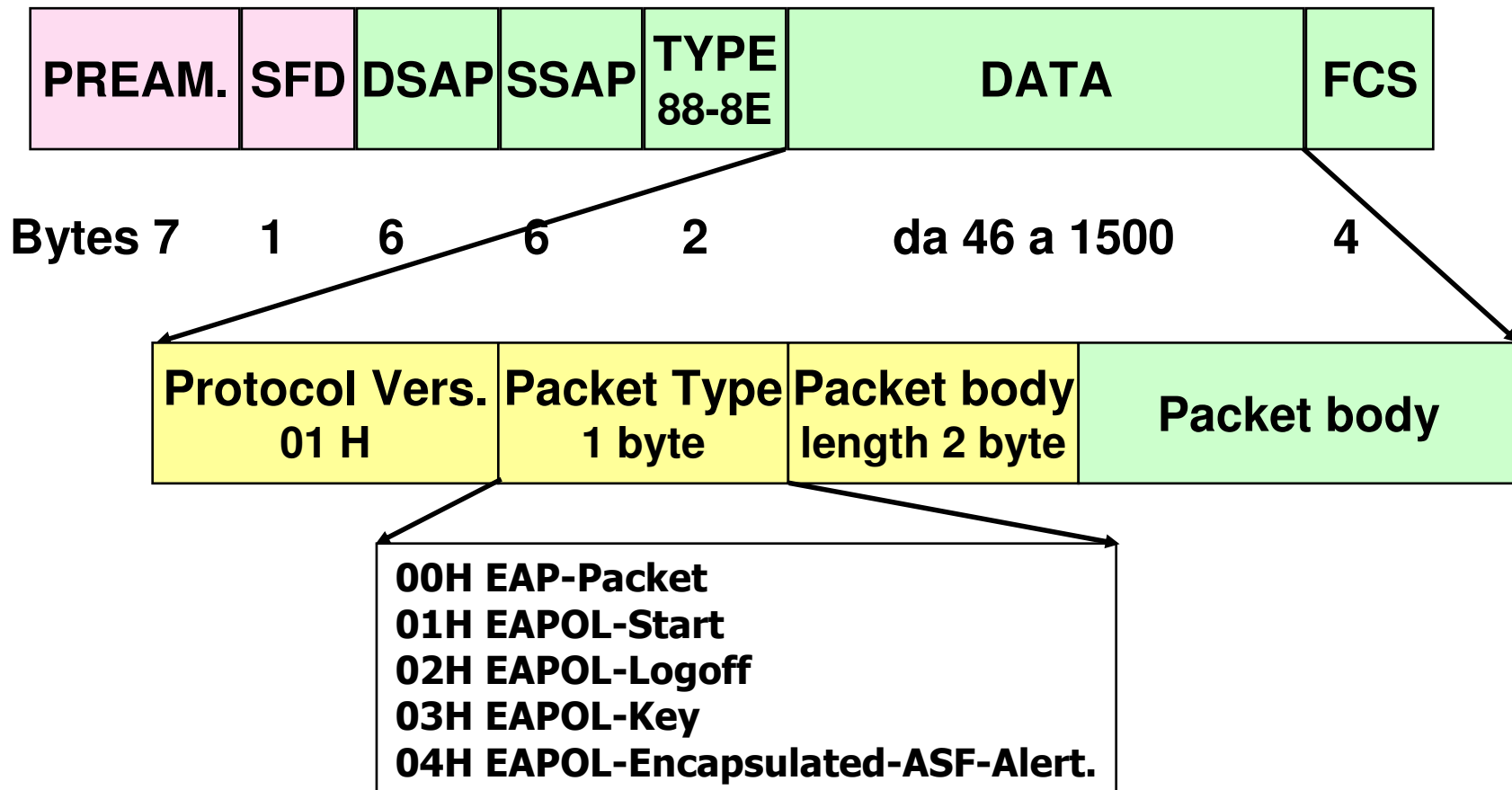
## EAPOL frame

- EAPOL frames are transmitted to the multicast address 01-80-C2-00-00-03
- The EAPOL frame on Ethernet v 2.0:
  - the code protocol inserted in the Type field is 88-8E



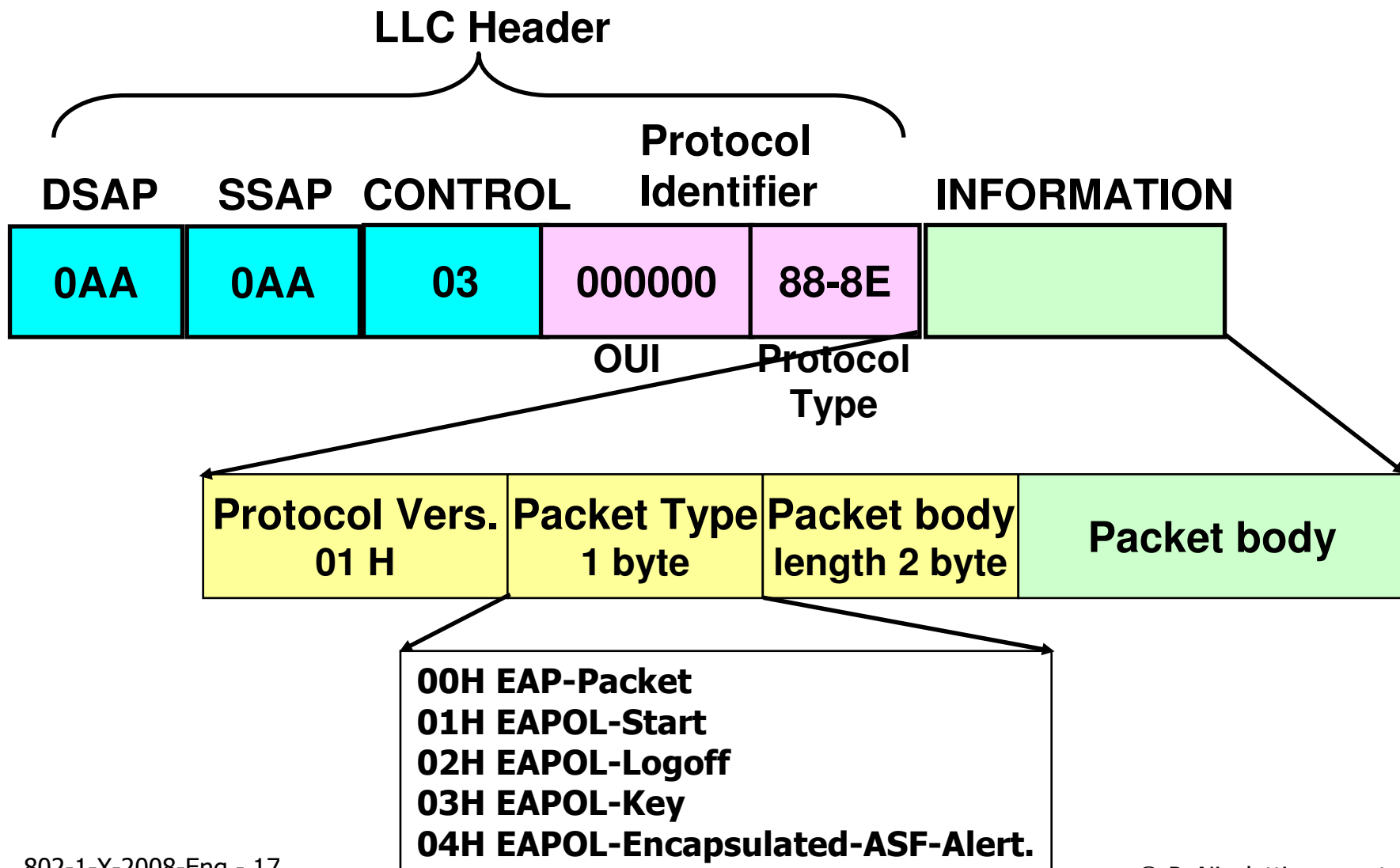


# EAPOL over Ethernet V 2.0 frame



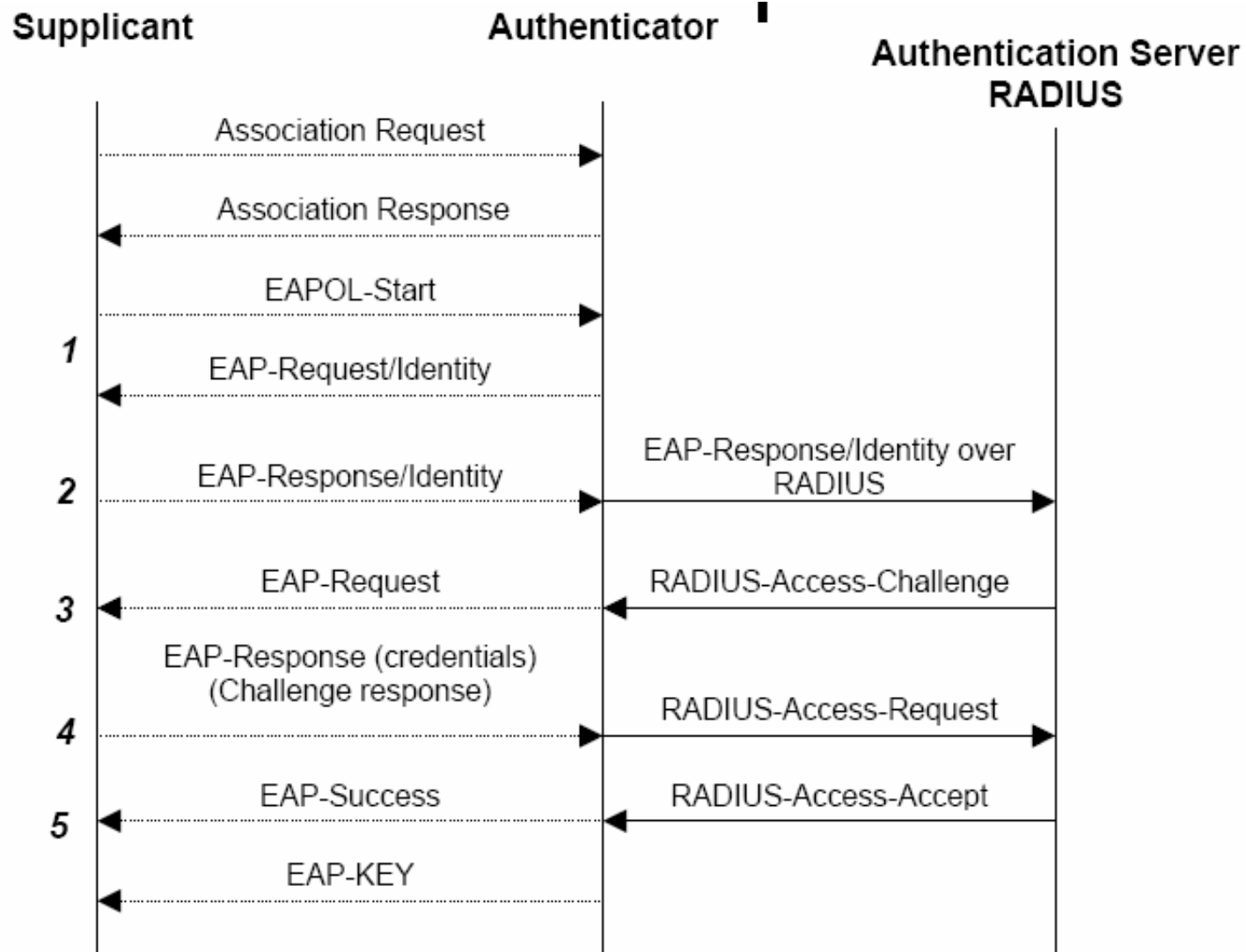


# EAPOL over 802.x frames



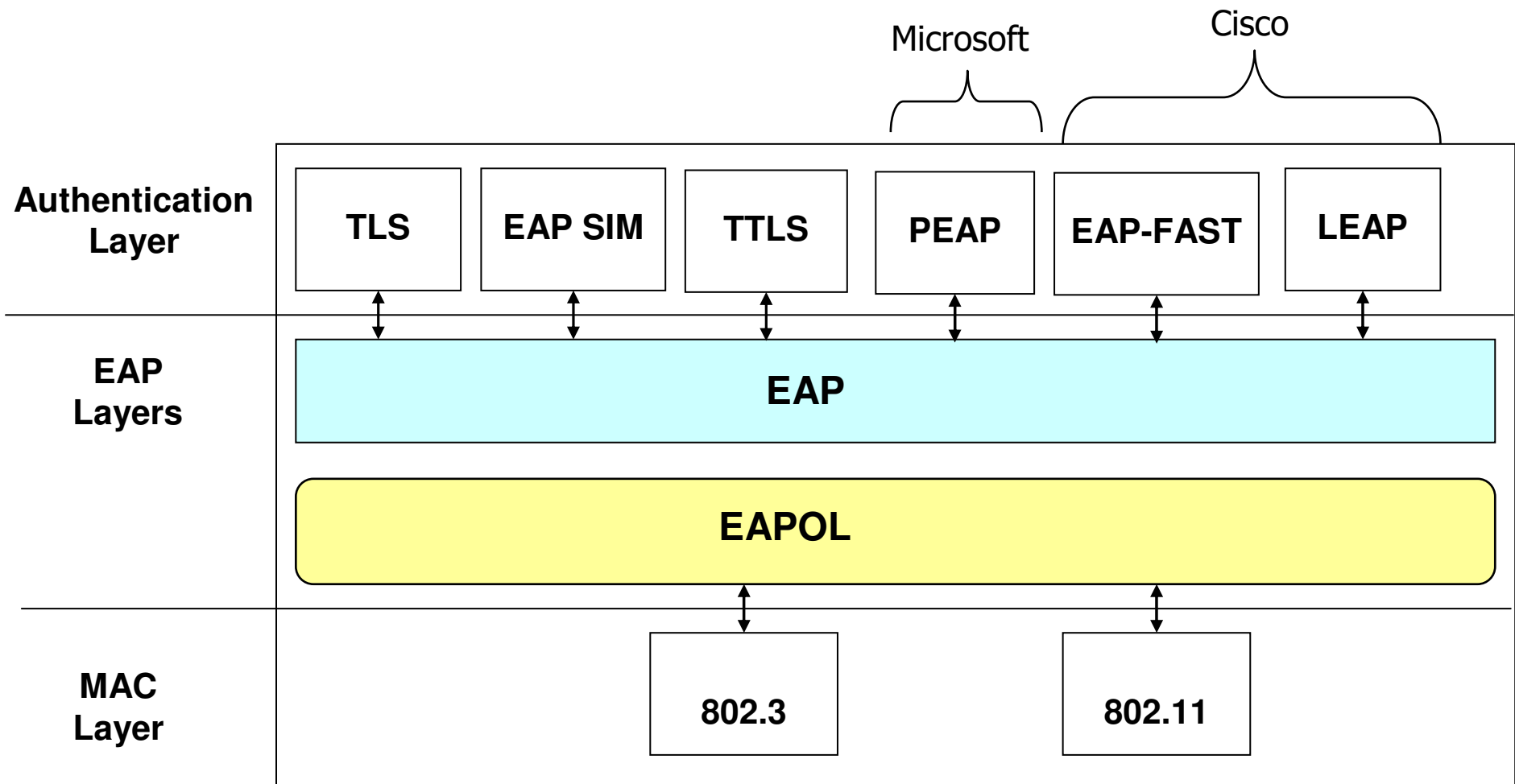


# EAP & EAPOL over wireless networks





# EAP Authentication method





# LEAP (Lightweight Extensible Authentication Protocol)

- EAP-Cisco Wireless Authentication protocol based on “username e password” sent via MS-CHAP without the digital certificates
- Easy and fast to configure because don't need the certificates management
- Limits:
  - Need interface drivers that support LEAP
  - Supported only in wireless NIC



# EAP-TLS

- Mutual Authentication (client and server)
- Based on Digital Certificates for Server and Client
  - The server have the CA (Certification Authority) and the Server Certificate
  - The Client have the CA (Certification Authority) and the Client Certificate
  - Is necessary to generate the CA Certificate, The Server Certificate and the Clients Certificates (one ore more)
- The data sent during authentication process are exchanged in a secure encrypted tunnel



# EAP-TTLS

- Similar EAP-TLS
- Only CA and Server Certificate are necessary
- The client authentication is based on:
  - CA Certificate and specific client Authentication based on:
    - Username/Password CHAP, MSCHAPv2, MD5



# Protected Extensible Authentication Protocol (PEAP)

- Based on EAP-TTLS Authentication Method:
  - Phase 1: establish a secure tunnel through EAP-TTLS authentication
  - Phase 2: realize the supplicant authentication based on EAP protocol plus other specific information of PEAP
- Only CA and Server Certificate are necessary
- The client is authenticated via:
  - CA Certificate and Username/Password MSCHAPv2



## WPA (WiFi Protected Access)

- WPA is a standard-based security solution from the WiFi Alliance that addresses the vulnerabilities in native WLANs
- WPA provides enhanced data protection and access control for WLAN systems. WPA addresses all known Wired Equivalent Privacy (WEP) vulnerabilities in the original IEEE 802.11 security implementation and brings an immediate security solution to WLAN networks in both enterprise and small office, home office (SOHO) environments.
- Use Pre Shared Key (WPA-PSK) for Authentication e Data Encryption
  - WPA-PSK may be in Hexadecimal format or ASCII format (also known as Pass Phrase)



## WPA2 / 802.11i

- WPA 2 is the next generation of Wi-Fi security. WPA 2 is the Wi-Fi Alliance interoperable implementation of the ratified IEEE 802.11i standard
- WPA 2 implements the National Institute of Standards and Technology (NIST)-recommended Advanced Encryption Standard (AES) encryption algorithm with the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
  - AES Counter Mode is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key.



## WPA2 / 802.11i: Server Radius or PSK

- Normally WPA2 use RADIUS Server for Authentication and Encryption Key Generation
- Can even work with Pre Shared Key (PSK) witch can long up to 256 bits (64 Hexadecimal digit)
  - Same PSK used on AP and Clients
  - **pass-phrase** can be use instead of hexadecimal number sequence the standard suggest to use a pass-phrase with minimum 20 characters for security



# Authentication Systems Compare

<i>Method</i>	<i>Description</i>	<i>Authentication Attributes</i>	<i>WEP key generation?</i>	<i>Wireless Security</i>	<i>Deployment Difficulty</i>
<b>MD5</b>	Challenge-based password	One-way Authentication	NO	Weak	Easy
<b>LEAP</b>	Cisco LEAP algorithm (Challenge-based password)	Mutual Authentication	YES	Stronger than MD5 weaker than other EAP solutions	Moderate
<b>TLS</b>	Certificate-based two-way authentication	Mutual Authentication	YES	Strongest	Hard
<b>TTLS</b>	Server authentication via certificate, client via other method	Mutual Authentication	YES	Strong	Moderate
<b>PEAP</b>	Server authentication via certificate, client via other EAP-method	Mutual Authentication	YES	Strong	Moderate



# Dynamic VLAN Assignment & 802.1 x Extensions



# Dynamic VLAN Assignment

- An extension of the 802.1x standard specifications:
  - The new version of 802.1x 2004 define a new type VLAN assignment "authentication based"
  - RFC 2868 of 2000 and above all RFC 3580 of 2003 define some new RADIUS protocol attributes (AV = Attribute Value)
- Through this new function the assignation of VLAN can be done:
  - Per Port
  - Per Protocol
  - Authentication based



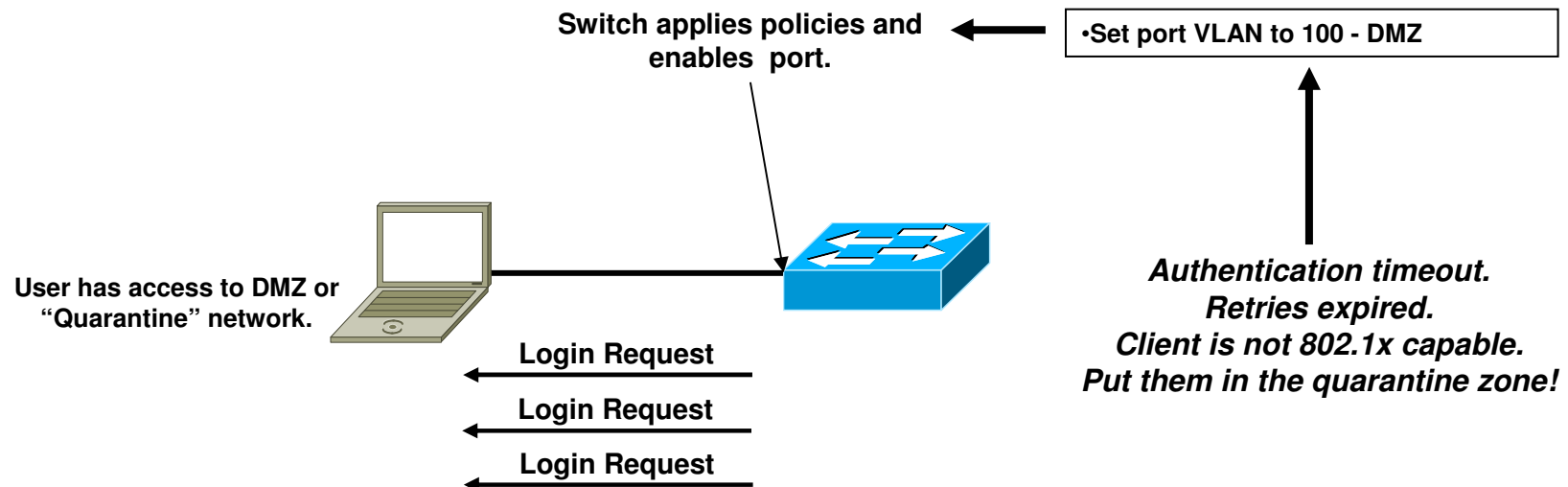
# Advantages of Dynamic VLAN Assignment based on authentication

- Simplifies the network operators' work
  - They do not need change the configuration of VLAN on the ports following the users witch are moving
    - The user's VLAN depends on his credentials
    - The users' ports are set up for the dynamic assignment based on the authentication
    - The user wherever moves in the network keep the credentials for his VLAN
  - Easy to manages VLAN Guest for the guests in switched and wireless networks



# Advantages of Dynamic VLAN Assignment based on authentication

- Increases the security on the business Switches LAN
  - Not authenticated user is put on quarantine VLAN
  - Every user connected to the network is identified (certificates, username, password) by his credentials





# RADIUS protocol and new attributes

- New RADIUS attributes:
  - Tunnel-Type=VLAN (13)
  - Tunnel-Medium-Type=802 (6)
  - Tunnel-Private-Group-ID=VLANID (xxxx)



## RADIUS Protocol:Tunnel type

- 1 Point-to-Point Tunneling Protocol (PPTP) [1]
- 2 Layer Two Forwarding (L2F) [2]
- 3 Layer Two Tunneling Protocol (L2TP) [3]
- 4 Ascend Tunnel Management Protocol (ATMP) [4]
- 5 Virtual Tunneling Protocol (VTP)
- 6 IP Authentication Header in the Tunnel-mode (AH) [5]
- 7 IP-in-IP Encapsulation (IP-IP) [6]
- 8 Minimal IP-in-IP Encapsulation (MIN-IP-IP) [7]
- 9 IP Encapsulating Security Payload in the Tunnel-mode (ESP) [8]
- 10 Generic Route Encapsulation (GRE) [9]
- 11 Bay Dial Virtual Services (DVS)
- 12 IP-in-IP Tunneling [10]
- 13 Virtual LANs (VLAN)



## RADIUS Protocol:Tunnel-Medium type

- 1 IPv4 (IP version 4)
- 2 IPv6 (IP version 6)
- 3 NSAP
- 4 HDLC (8-bit multidrop)
- 5 BBN 1822
- 6 802 (includes all 802 media plus Ethernet "canonical format")
- 7 E.163 (POTS)
- 8 E.164 (SMDS, Frame Relay, ATM)
- 9 F.69 (Telex)
- 10 X.121 (X.25, Frame Relay)
- 11 IPX
- 12 Appletalk
- 13 Decnet IV
- 14 Banyan Vines
- 15 E.164 with NSAP format subaddress



# Dynamic VLAN assignment configuration

- On the Switch:
  - Specify VLAN Assignment authentication based
  - Specify a parking VLAN for non-authorized users
- On RADIUS Server config file add the following parameters
  - Tunnel-Type=13
  - Tunnel-Medium-Type=6
  - Tunnel-Private-Group-ID=xxxx



## Configuration example on HP switch

- aaa authentication port-access eap-radius
- radius-server host 10.200.150.5 key test12345
- aaa port-access authenticator 4 (port 4 of the switch)
- aaa port-access authenticator 4 unauth-vid 100
  - Parking VLAN is: VLAN 100



# FreeRadiusconfiguration example

- File /etc/raddb/user
  - Users: off, connect, stealth
  - Part of User Local Data Base
    - off Auth-Type := Local, User-Password == "invisibile"  
Tunnel-Type = 13,  
Tunnel-Medium-Type = 6,  
Tunnel-Private-Group-Id = 2
    - connect Auth-Type := EAP  
Tunnel-Type = 13,  
Tunnel-Medium-Type = 6,  
Tunnel-Private-Group-Id = 1
    - stealth Auth-Type := EAP  
Tunnel-Type = 13,  
Tunnel-Medium-Type = 6,  
Tunnel-Private-Group-Id = 2



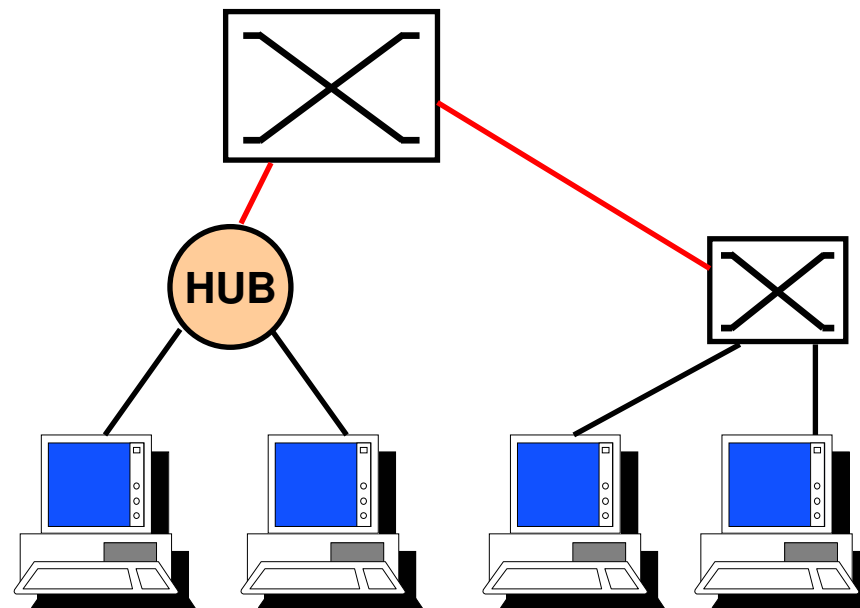
## VLAN and Users

- VLAN and Users in the previous example:
  - **off** = VLAN 2
    - (authentication based on MD5 or PEAP Username/Password)
  - **connect** = VLAN 1
    - authentication based on EAP-TLS
  - **Stealth** = VLAN 2
    - authentication based on EAP-TLS
  - Users not authenticated are in Parking VLAN 100



## Dynamic VLAN assignment limits

- If a hub or a VLAN-Unaware switch is connected to a switch port with dynamic VLAN enabled and if user authenticates himself, the switch port is opened and also other users can connect in network through that authenticated port





## Port Security to prevent intrusion

- On new switch, as for instance the recent ones of Cisco and HP, it is possible to configure the switch to accept a single MAC address for port.
  - Is possible to define the MAC address enabled to the access.
  - The can accept only the first MAC address seen on the port (typically that of PC which authenticates himself)
    - Example on HP Switch
      - Configure port A1 to automatically accept the first device (MAC address) it detects as the only authorized device for that port. (The default device limit is 1.) This command also configures the port to send an alarm to a network management station and disable itself if an intruder is detected on the port.

```
ProCurve(config)# port-security a1 learn-mode static action send-disable
```



## How to increase the security

- To increase the security on port the switch can periodically repeat the user's authentication
  - Example on HP switch
  - `aaa port-access authenticator 4 reauth-period 30`
    - Switch repeat the authentication on port 4 every 30 seconds