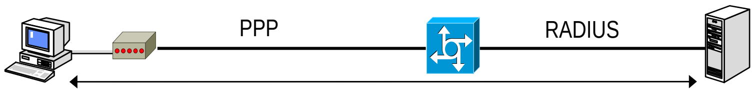
Lecture 4.2:

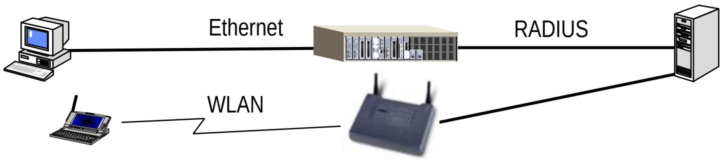
Authentication in LANs/WLANs
-
802.1X Port Based Network Access Control

Recommended reading: IEEE 802.1X-2004, Clause 6,7,8

Difference with PPP/NAS

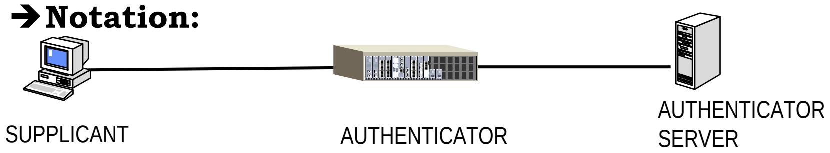


- ➔**PPP: provides link establishment handshake**
  - ⇨And “launches” authentication handshake
- ➔**LAN/WLAN scenario**
  - ⇨No more link establishment
    - ➔LAN: Plug the wire to a switch
    - ➔WLAN: Associate to an AP
  - ⇨How to “launch” and manage local+remote authentication?
  - ⇨And how to prevent unauthorized users to access the network?



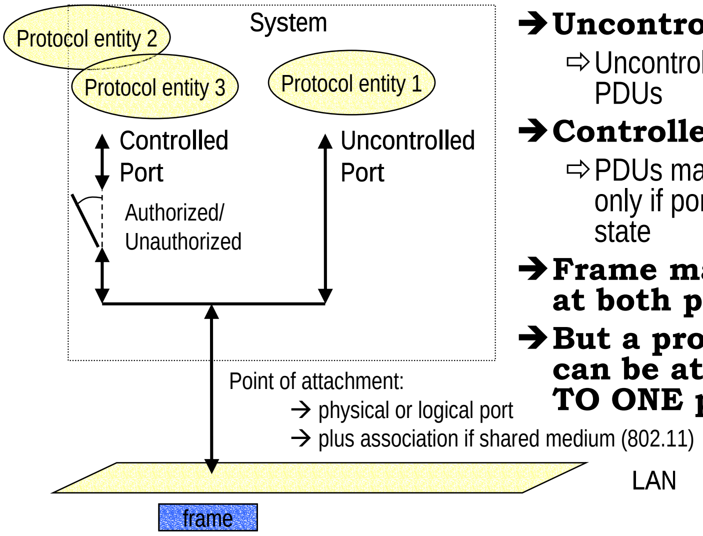
Context and notation

- ➔ **Point-to-point connections, only**
  - ⇨ Physical PC to switch link
  - ⇨ Physical switch/router to switch/router link
  - ⇨ Virtual PC to AP association
    - → Shared medium, but p2p logical relation!
- ➔ **Notation:**



- ➔ **But when mutual authentication, PC=authenticator**
- ➔ **Port: point of attachment to a LAN**
  - ⇨ PC: typically one port
  - ⇨ Bridge/switch: 2+ ports

802.1X port model



- ➔ **Uncontrolled port:**
  - ⇨ Uncontrolled exchange of PDUs
- ➔ **Controlled port:**
  - ⇨ PDUs may be exchanged only if port is in authorized state
- ➔ **Frame made available at both ports…**
- ➔ **But a protocol entity can be attached ONLY TO ONE port!**

Why not 802.1X on shared media?

➔One PC authenticates…

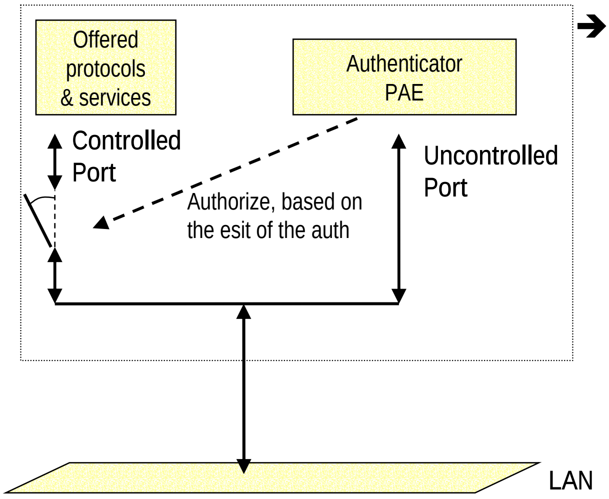
➔… and authorizes the controlled port

➔All the other packets in the LAN may then access the network!

➔Notable exception: 802.11

- ⇨One logical port per each association (= p2p relation)

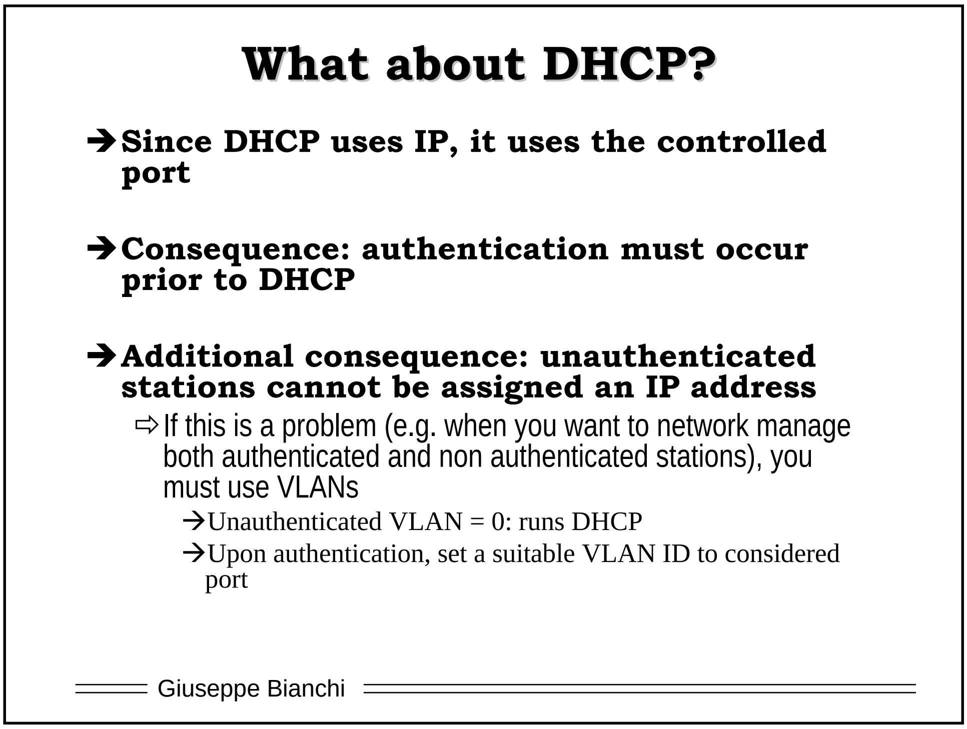
Port Access Entity (PAE)


Offered protocols & services
Authenticator PAE
Controlled Port
Uncontrolled Port
Authorize, based on the esit of the auth
LAN

➔**Authenticator PAE**

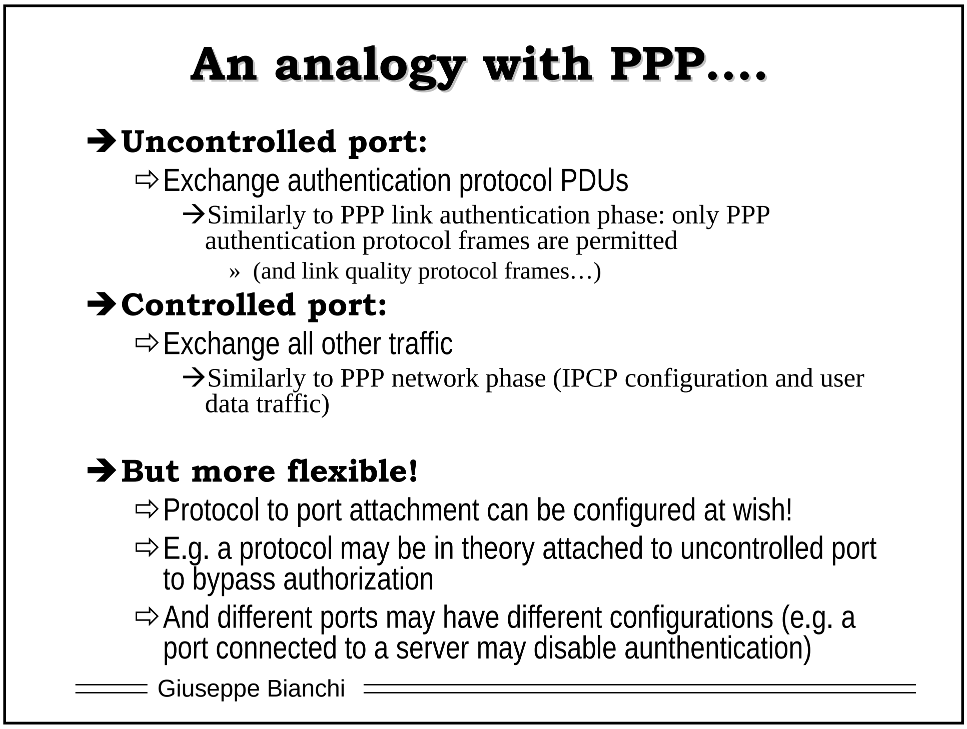
- ⇨Exchange auth data with supplicant PAE
  - →In turns auth PAE responsible of forwarding to a remote server
- ⇨Through uncontrolled port
- ⇨Consequence: auth protocol MUST BE at link layer!!
  - →Since IP attached to controlled port

Mutual authentication: PAE acts as authenticator and supplicant independently in the two directions



What about DHCP?

- ➔ **Since DHCP uses IP, it uses the controlled port**
- ➔ **Consequence: authentication must occur prior to DHCP**
- ➔ **Additional consequence: unauthenticated stations cannot be assigned an IP address**
  - ⇨ If this is a problem (e.g. when you want to network manage both authenticated and non authenticated stations), you must use VLANs
    - →Unauthenticated VLAN = 0: runs DHCP
    - →Upon authentication, set a suitable VLAN ID to considered port



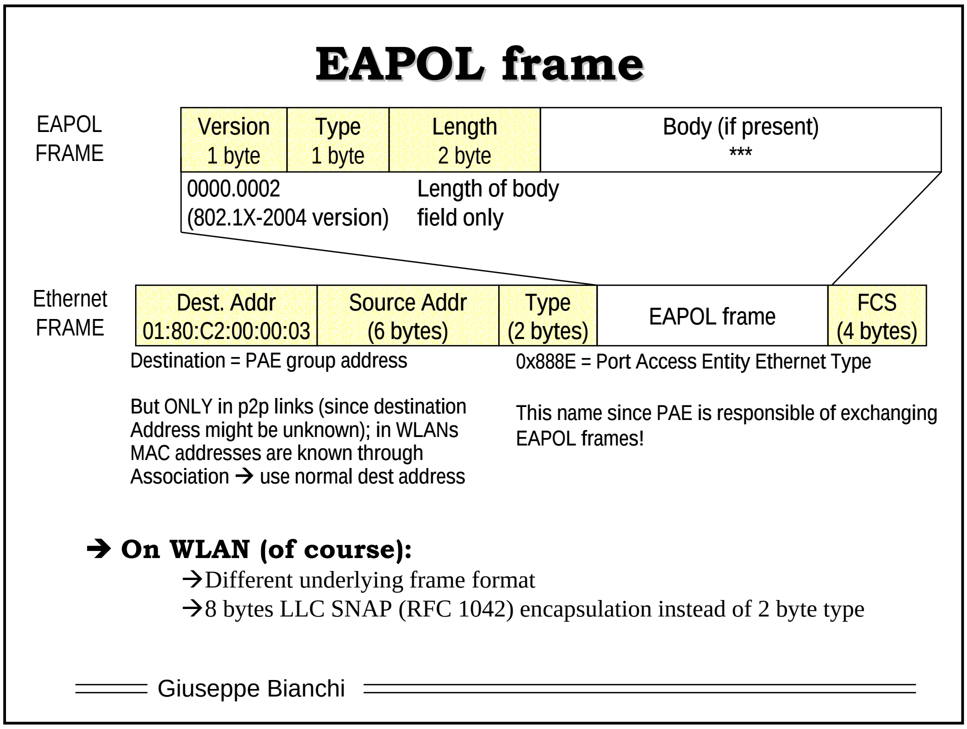
An analogy with PPP....

- ➔ **Uncontrolled port:**
  - ⇨ Exchange authentication protocol PDUs
    - →Similarly to PPP link authentication phase: only PPP authentication protocol frames are permitted
      - » (and link quality protocol frames…)
- ➔ **Controlled port:**
  - ⇨ Exchange all other traffic
    - →Similarly to PPP network phase (IPCP configuration and user data traffic)
- ➔ **But more flexible!**
  - ⇨ Protocol to port attachment can be configured at wish!
  - ⇨ E.g. a protocol may be in theory attached to uncontrolled port to bypass authorization
  - ⇨ And different ports may have different configurations (e.g. a port connected to a server may disable aunthentication)

EAP Encapsulation over LAN (EAPOL)

PAE authentication method

- ➔ **Only one method: EAP!!**
  - ⇨ i.e. many methods, but only one protocol
- ➔ **Typically provided by a remote authentication server**
  - ⇨ E.g. Radius
  - ⇨ PAE acts as pass-through for EAP packets
- ➔ **EAPOL: the protocol which encapsulates EAP packets over a (W)LAN**
  - ⇨ Frequently EAPOL called EAPOW when on an WLAN
    - →(EAPOW = EAPOL which supports EAPOL-Key packets)…
  - ⇨ but it is just jargon (standard never mentions EAPOW)



EAPOL frame

EAPOL FRAME

Version 1 byte	Type 1 byte	Length 2 byte	Body (if present) ***

0000.0002
(802.1X-2004 version)

Length of body
field only

Ethernet FRAME

Dest. Addr 01:80:C2:00:00:03	Source Addr (6 bytes)	Type (2 bytes)	EAPOL frame	FCS (4 bytes)

Destination = PAE group address

But ONLY in p2p links (since destination Address might be unknown); in WLANs MAC addresses are known through Association → use normal dest address

0x888E = Port Access Entity Ethernet Type

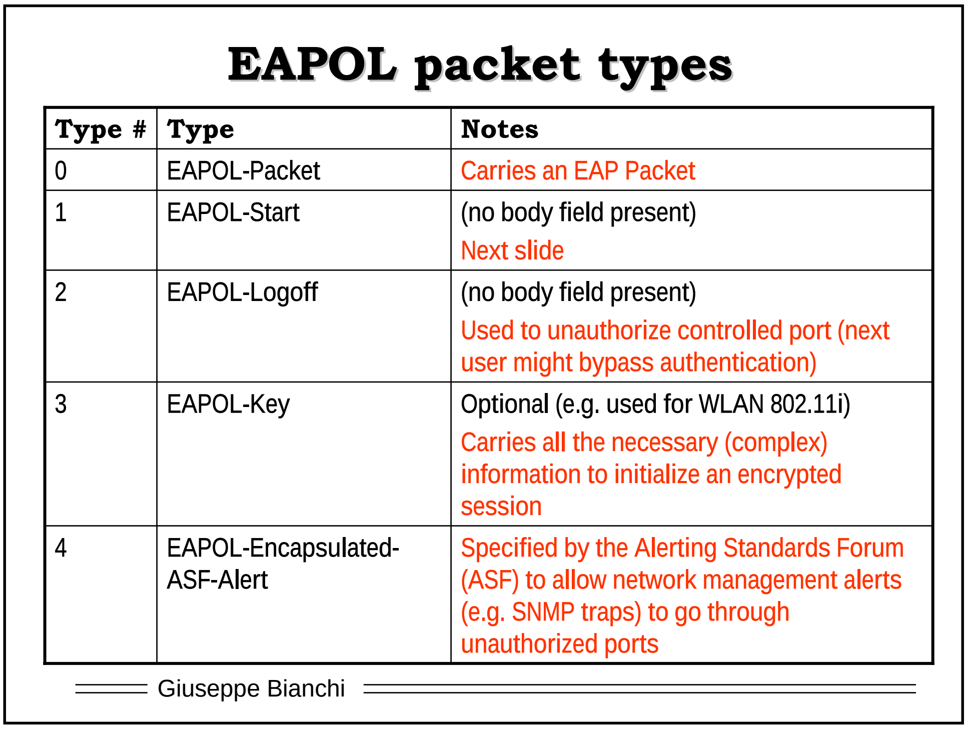
This name since PAE is responsible of exchanging EAPOL frames!

→ **On WLAN (of course):**

→Different underlying frame format

→8 bytes LLC SNAP (RFC 1042) encapsulation instead of 2 byte type

Giuseppe Bianchi



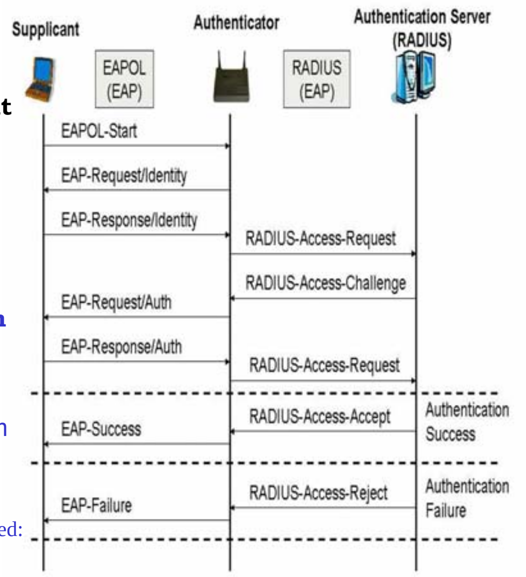
EAPOL packet types

Type #	Type	Notes
0	EAPOL-Packet	Carries an EAP Packet
1	EAPOL-Start	(no body field present) Next slide
2	EAPOL-Logoff	(no body field present) Used to unauthorize controlled port (next user might bypass authentication)
3	EAPOL-Key	Optional (e.g. used for WLAN 802.11i) Carries all the necessary (complex) information to initialize an encrypted session
4	EAPOL-Encapsulated-ASF-Alert	Specified by the Alerting Standards Forum (ASF) to allow network management alerts (e.g. SNMP traps) to go through unauthorized ports

Giuseppe Bianchi

Why EAPOL-Start?

- ➔ **EAP typically started by authenticator**
  - ⇨ with an EAP-Request/Identity
- ➔ **EAPOL-start allows supplicant to initiate authentication**
  - ⇨ EAPOL-Start tells authenticator:
    - → I'm initialized and ready
      - » (the port has become operable)
    - → Normal EAP exchange follows
- ➔ **No rule on who starts first**
  - ⇨ Timer details in 802.1X-2004
- ➔ **EAPOL-Start also useful when**
  - ⇨ EAP-Request lost
    - → Port not yet initialized state
    - → Frame loss on wireless channel
  - ⇨ 802.1X client, but no authentication supported on the switch/AP side
    - → Send 1,2,3 EAPOL-Start
    - → No response
    - → Assume no authentication required: send normal packets!



Supplicant
Authenticator
Authentication Server (RADIUS)
EAPOL (EAP)
RADIUS (EAP)
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
RADIUS-Access-Request
RADIUS-Access-Challenge
EAP-Request/Auth
EAP-Response/Auth
RADIUS-Access-Request
RADIUS-Access-Accept
EAP-Success
Authentication Success
RADIUS-Access-Reject
EAP-Failure
Authentication Failure