

# Autenticazione tramite IEEE 802.1x

Pietro Nicoletti

Studio Reti s.a.s

www.studioreti.it

## Nota di Copyright

- Questo insieme di trasparenze (detto nel seguito slides) è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo ed i copyright relativi alle slides (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica e testo) sono di proprietà degli autori indicati a pag. 1.
- Le slides possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione e al Ministero dell'Università e Ricerca Scientifica e Tecnologica, per scopi istituzionali, non a fine di lucro. In tal caso non è richiesta alcuna autorizzazione.
- Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente, le riproduzioni su supporti magnetici, su reti di calcolatori e stampate) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori.
- L'informazione contenuta in queste slides è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, ecc. In ogni caso essa è soggetta a cambiamenti senza preavviso. Gli autori non assumono alcuna responsabilità per il contenuto di queste slides (ivi incluse, ma non limitatamente, la correttezza, completezza, applicabilità, aggiornamento dell'informazione).
- In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste slides.
- In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.

## Server AAA e Radius

- Server AAA (Authentication, Authorization & Accounting)
- R.A.D.I.U.S.: **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice.
  - Il Radius Server è di tipo AAA ed è usato per certificare gli utenti che chiedono accesso ad una rete, e ne autorizza l'accesso (solitamente tramite verifica di username e password). Utilizzabile anche per l'accounting.
  - Basato su protocollo UDP.
  - Porte assegnate:
    - Authentication 1812/udp (1645/udp obsoleta),
    - Accounting 1813/udp (1646/udp obsoleta).
  - Prevede utilizzo di una chiave o password "secret" per autenticare server e autenticatore.

## IEEE 802.1x: generalità

- Port Base Network Access Control
- Obiettivo:
  - Riprodurre sulle Switched LAN e LAN le condizioni di controllo tipiche dell'accesso Dial-Up dove è possibile abbattere la connessione dell'utente non autorizzato.
  - Gli utenti devono essere connessi in modalità punto-punto all'apparato che supporta 802.1x
    - a quelli autenticati e autorizzati viene permesso l'accesso alla rete
    - quelli non autorizzati vengono sconnessi elettronicamente dalla porta
- Presente sugli switch e gli Access Point Wireless di ultima generazione

## IEEE 802.1x: definizioni

- Autenticatore:
  - E' un'entità posta all'estremità di una connessione punto-punto di un segmento LAN che si occupa di autenticare l'entità posta l'estremità opposta.
- Server di autenticazione:
  - E' un'entità che fornisce i servizi di autenticazione ad un autenticatore.
  - Il server determina, in base alle credenziali fornite dal supplicante, se questo è autorizzato ad accedere ai servizi forniti dall'autenticatore.
  - La funzione di Server di autenticazione può essere collocata con quella di autenticatore oppure si può accedere ad essa attraverso la rete dove l'autenticatore ha l'accesso

## IEEE 802.1x: definizioni

- Network Access Point:
  - E' una porta di connessione di un apparato denominato System alla LAN.
  - La porta può essere:
    - fisica come nel caso di uno switch;
    - logica come nel caso di associazione tra una stazione e un Access Point in una rete WLAN.
- Port Access Entity (PAE):
  - E' un entità protocollare associata all'Autenticatore, al Supplicante o entrambi

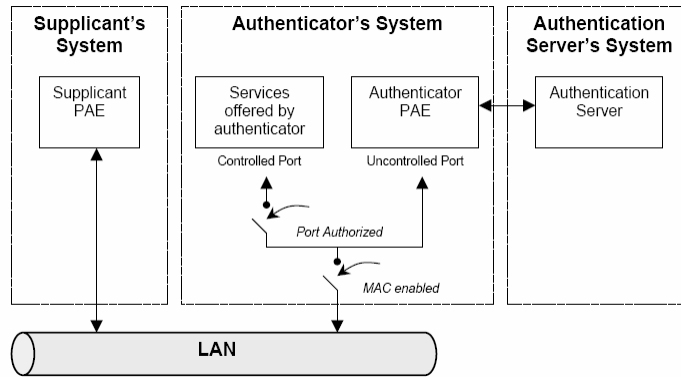
## IEEE 802.1x: definizioni

- **Supplicante:**
  - E' un'entità posta all'estremità di una connessione punto-punto di un segmento LAN che deve essere autenticata tramite l'Autenticatore posto all'estremità opposta.
- **System:**
  - E' un apparato che è connesso alla LAN tramite una o più porte (caso di aggregazione).
  - Esempi di System sono: stazioni, Server ecc.

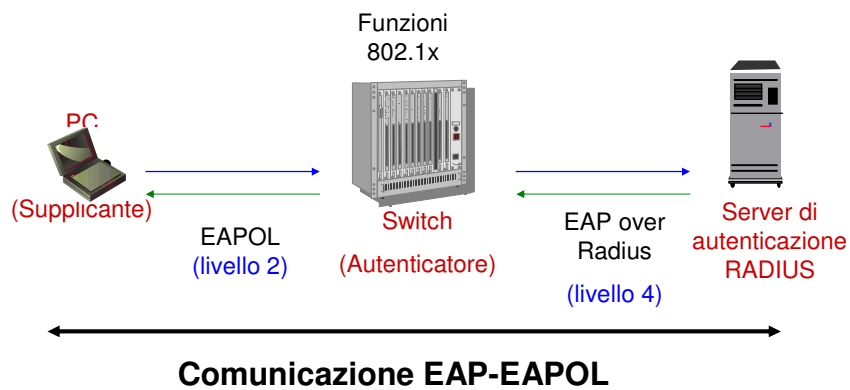
## Autorizzazione e autenticazione: gli elementi coinvolti - 1

- Il server di autenticazione (RADIUS)
- I protocolli di autenticazione EAP e EAPOL per le comunicazioni tra Server di Autenticazione, Autenticatore e Supplicante
- Le funzioni previste dallo standard 802.1x negli apparati di rete per controllare l'accesso alla rete da parte di stazioni

## Autorizzazione e autenticazione: gli elementi coinvolti - 2

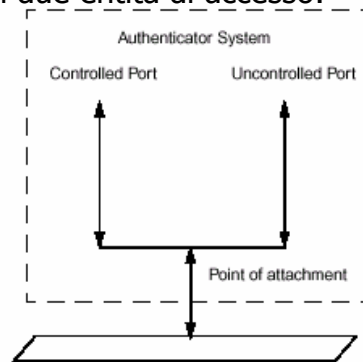


## Comunicazione EAP - EAPOL e 802.1x



## Autenticatore e Port Access Entity (PAE)

- Nell'autenticatore l'entità di accesso alla porta (PAE):
  - è responsabile della comunicazione tra il supplicante e il Server di autenticazione per stabilire le credenziali del supplicante, necessarie a permetterne l'accesso alla rete.
- Ogni punto di accesso, sia esso costituito da una porta fisica o logica, consiste in due entità di accesso:
  - controlled port
  - uncontrolled port

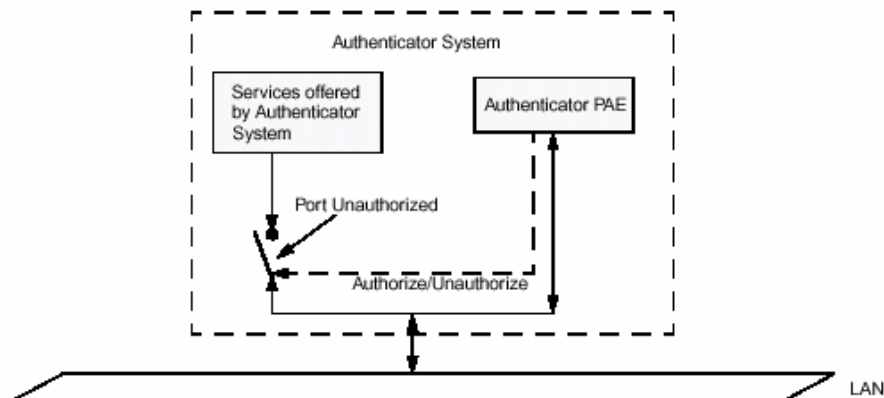


802-1-X-2004 -Switch 11

LAN ita a pag. 2

## Uso di Controlled e Uncontrolled Port

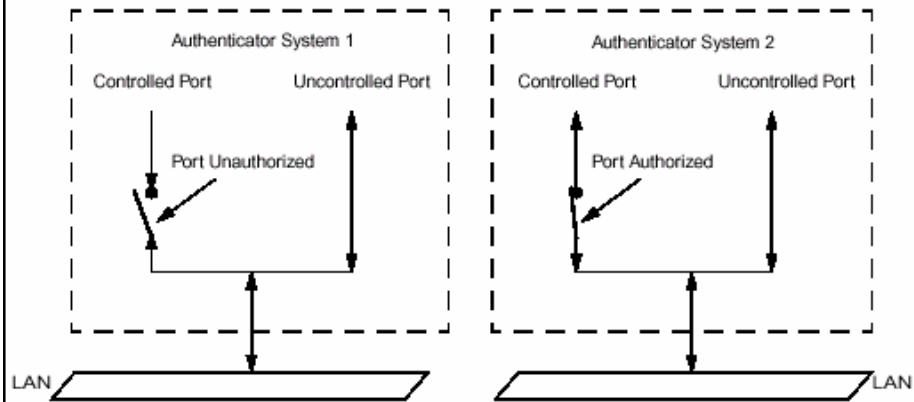
- Uncontrolled Port è l'entità utilizzata per lo scambio di pacchetti di servizio necessari per stabilire l'autorizzazione o il divieto di accesso



802-1-X-2004 -Switch 12

© P. Nicoletti: si veda nota a pag. 2

## Porte autorizzate e non autorizzate

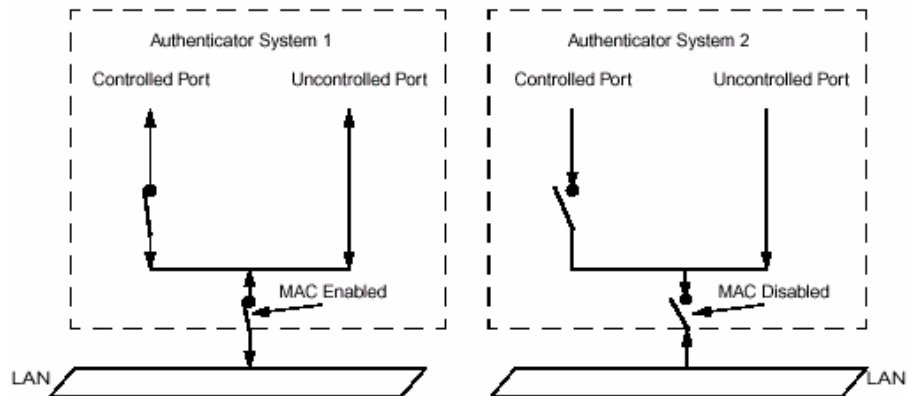


802-1-X-2004 -Switch 13

© P. Nicoletti: si veda nota a pag. 2

## Acesso basato su autenticazione e indirizzo MAC

- La disabilitazione della porta basata sull'indirizzo MAC provoca lo stato Unauthorized sulla Controlled port



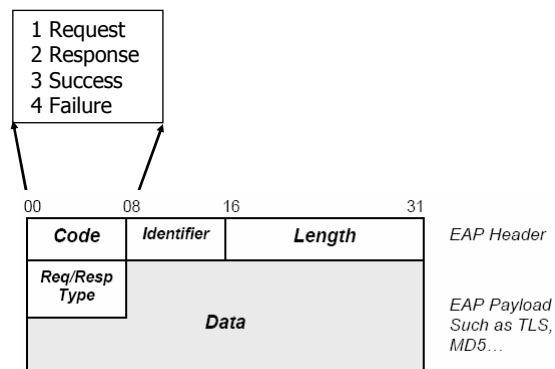
802-1-X-2004 -Switch 14

© P. Nicoletti: si veda nota a pag. 2

## Protocollo EAP

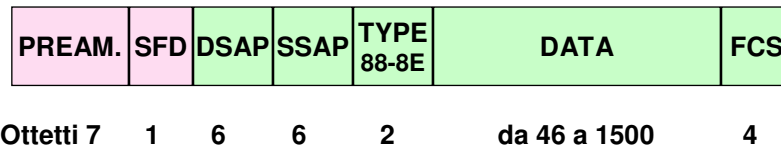
- PPP Extensible Authentication Protocol (EAP) definito nella RFC 2284
  - Codice protocollo EAP = c227
  - Supporta meccanismi multipli di autenticazione senza aver bisogno di pre-negoziare un particolare meccanismo durante la fase LCP
  - Originariamente PPP supportava solo autenticazioni basate su
    - PAP (Password Authentication Protocol), codice protocollo c023
    - CHAP (Challenge Handshake Authentication Protocol), codice protocollo c223

## Trama EAP



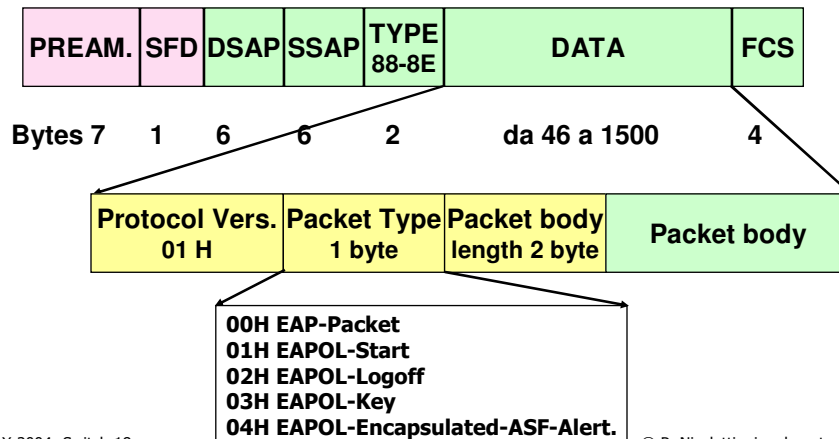
## Protocollo EAPOL

- E' l'implementazione del protocollo EAP su LAN (EAP Over LAN)
- L'header EAP viene incapsulato nella trama LAN 802.x
- La Port Access Entity utilizza le trame EAPOL nella comunicazione tra Autenticatore e Supplicante
- Le trame EAPOL vengono trasmesse all'indirizzo di gruppo 01-80-C2-00-00-03
- Le trame EAPOL su Ethernet:
  - il codice protocollo inserito nel campo Type è 88-8E



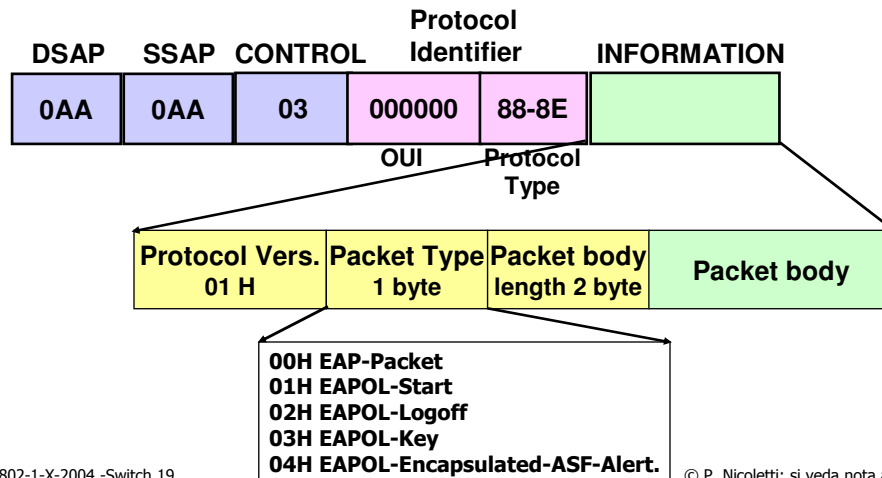
## Codifica EAPOL su trame Ethernet V 2.0

- Nelle trame EAPOL su Ethernet il codice protocollo inserito nel campo Type è 88-8E



## Codifica EAPOL su trame 802.x

- Gli standard 802.x (a parte Ethernet V 2.0) codificano i protocolli nell'LLC Header della LLC-PDU



## EAP & EAPOL

