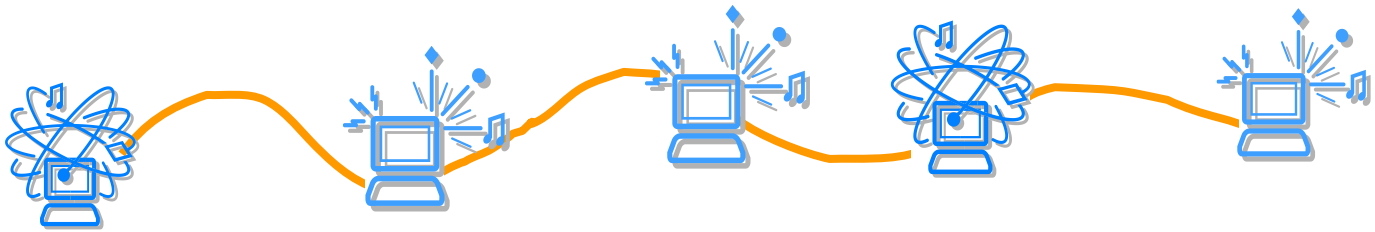
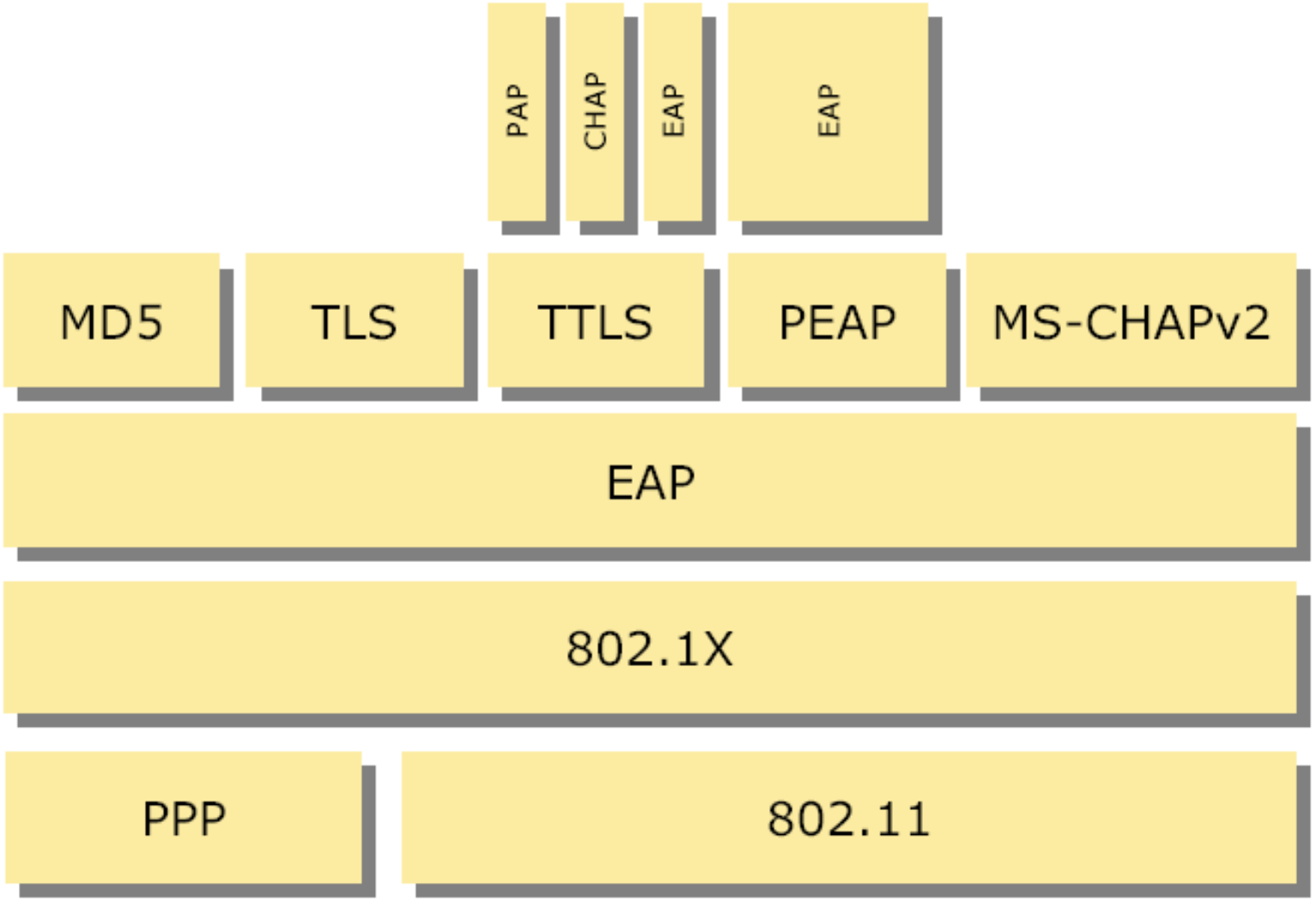
Segurança em Redes de Computadores
IEEE 802.1x



Redes de Comunicação
Departamento de Engenharia da Electrónica e Telecomunicações e de Computadores
Instituto Superior de Engenharia de Lisboa

Protocolos


PAP
CHAP
EAP
EAP
MD5
TLS
TTLS
PEAP
MS-CHAPv2
EAP
802.1X
PPP
802.11

802.1x não é o mesmo que 802.11x

- 802.11x é por vezes utilizado para referir de forma abreviada todas as normas de WLAN (i.e. 802.11a, 802.11b, ...) mas não é uma norma!

- 802.1x é uma norma que define controlo de acessos desenvolvida por 3Com, HP e Microsoft, incluindo um mecanismo de transporte.

- Atualmente a autenticação é efetuada através de mecanismos que utilizam EAP em cima de 802.1x.

IEEE 802.1x

- **IEEE 802.1x** é a forma comum de nos referirmos a uma norma designada por "***Port Based Network Access Control***", a qual indica que a enfase desta é fornecer um mecanismo de controlo para as ligações a uma rede local.

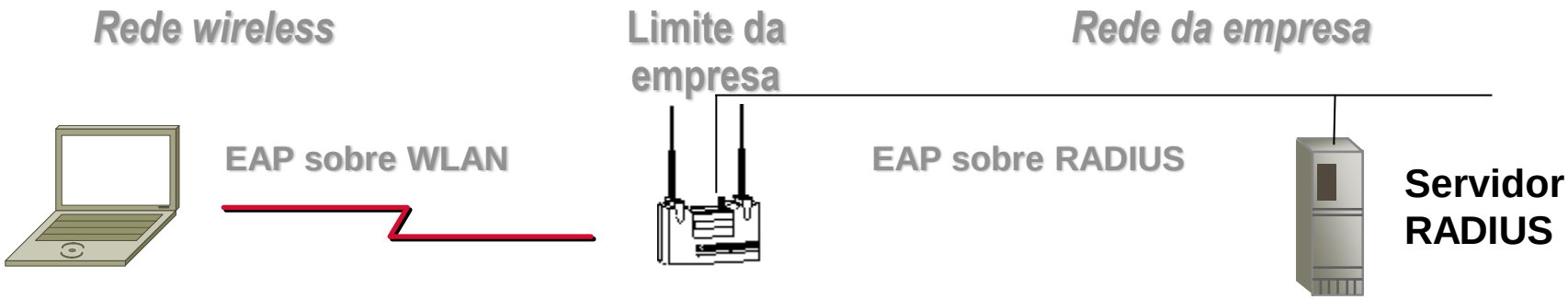
- **A norma não define os métodos de autenticação**, mas fornece os meios que permitem a aplicação desta norma em combinação com qualquer método de autenticação à escolha.

- Adiciona flexibilidade de maneira a que métodos de autenticação actuais ou futuros possam ser usados sem ser necessário alterar a norma.

IEEE 802.1x

- Verdadeira solução (nível 2) para acesso entre cliente e AP
- Vários mecanismos de autenticação disponíveis (EAP-MD5, EAP-TLS, EAP-TTLS, PEAP)
- Normalizado
- Cifra os dados utilizando chaves dinâmicas
- Suporte de RADIUS:
  - Escalável
  - Reusa relações de confiança
- Necessita de software no cliente (no S.O. ou *third-party*)

Descrição geral da terminologia do IEEE 802.1x



Suplicante

Opera no cliente

Autenticador

Opera em dispositivos como APs e *switches*

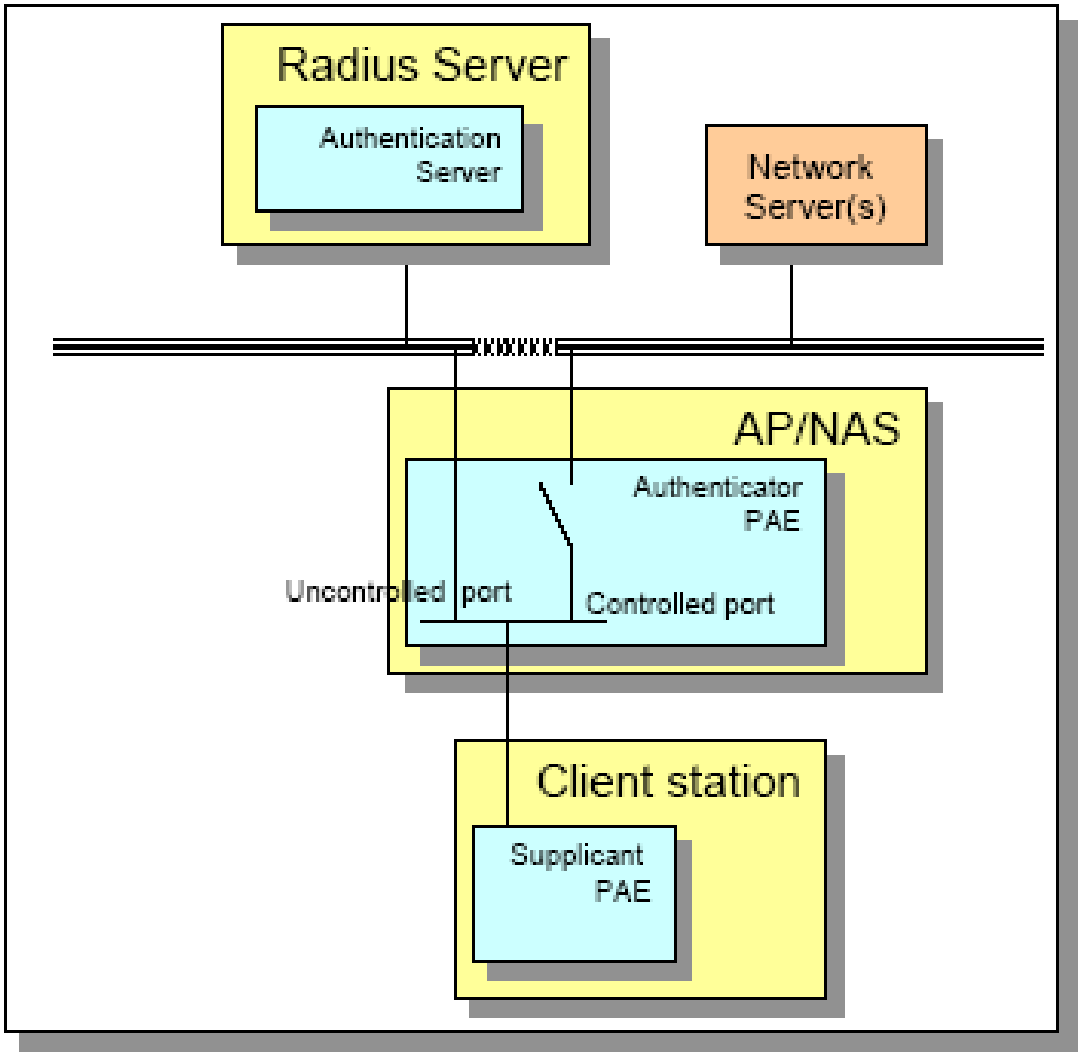
Servidor de Autenticação

Processa pedidos EAP

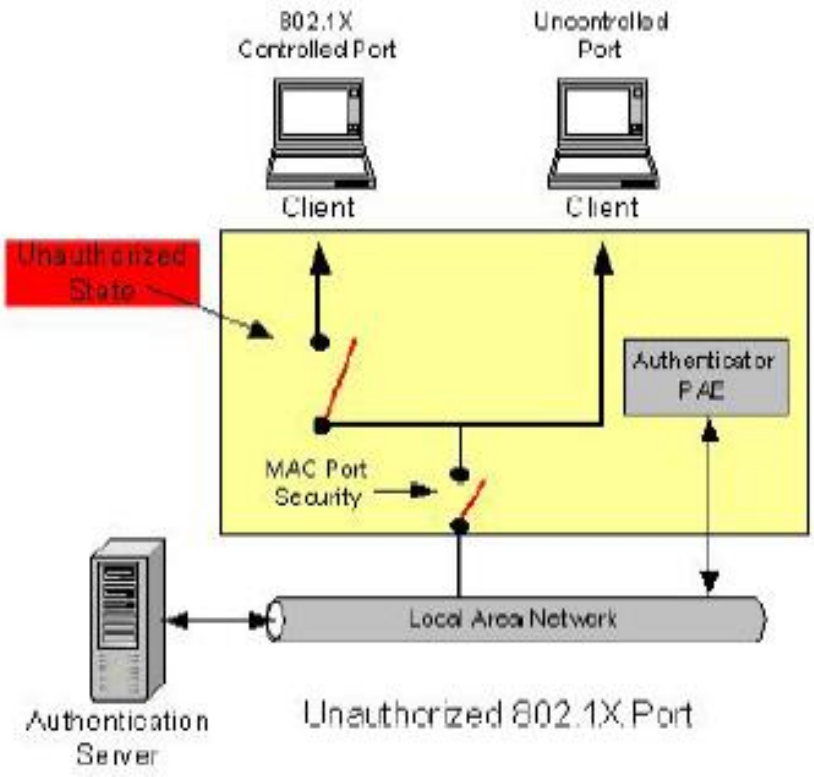
Componentes 802.1x

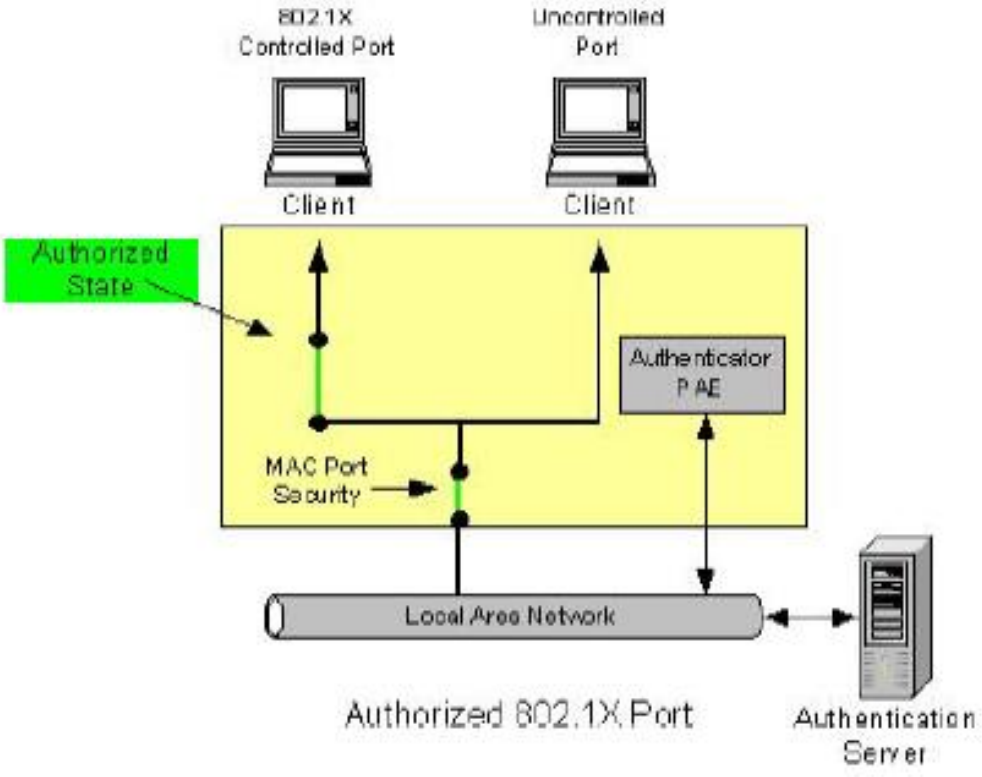
- A norma 802.1x inclui os seguintes conceitos:
  - ***Port Access Entity (PAE)***
    - Refere-se ao mecanismo (algoritmo e protocolo) associado a uma porta LAN (pertencente a uma *bridge* ou a uma estação)
  - ***Supplicant PAE* (Suplicante)**
    - Refere-se a uma entidade que requer autenticação antes de ter acesso à LAN (tipicamente uma estação)
  - ***Authenticator PAE* (Autenticador)**
    - Refere-se a uma entidade que facilita a autenticação de um suplicante (tipicamente uma estação ou AP)
  - ***Authentication Server* (Servidor de Autenticação)**
    - Refere-se à entidade que fornece o serviço de autenticação aos autenticadores na LAN (pode ser um servidor RADIUS)

Componentes 802.1x

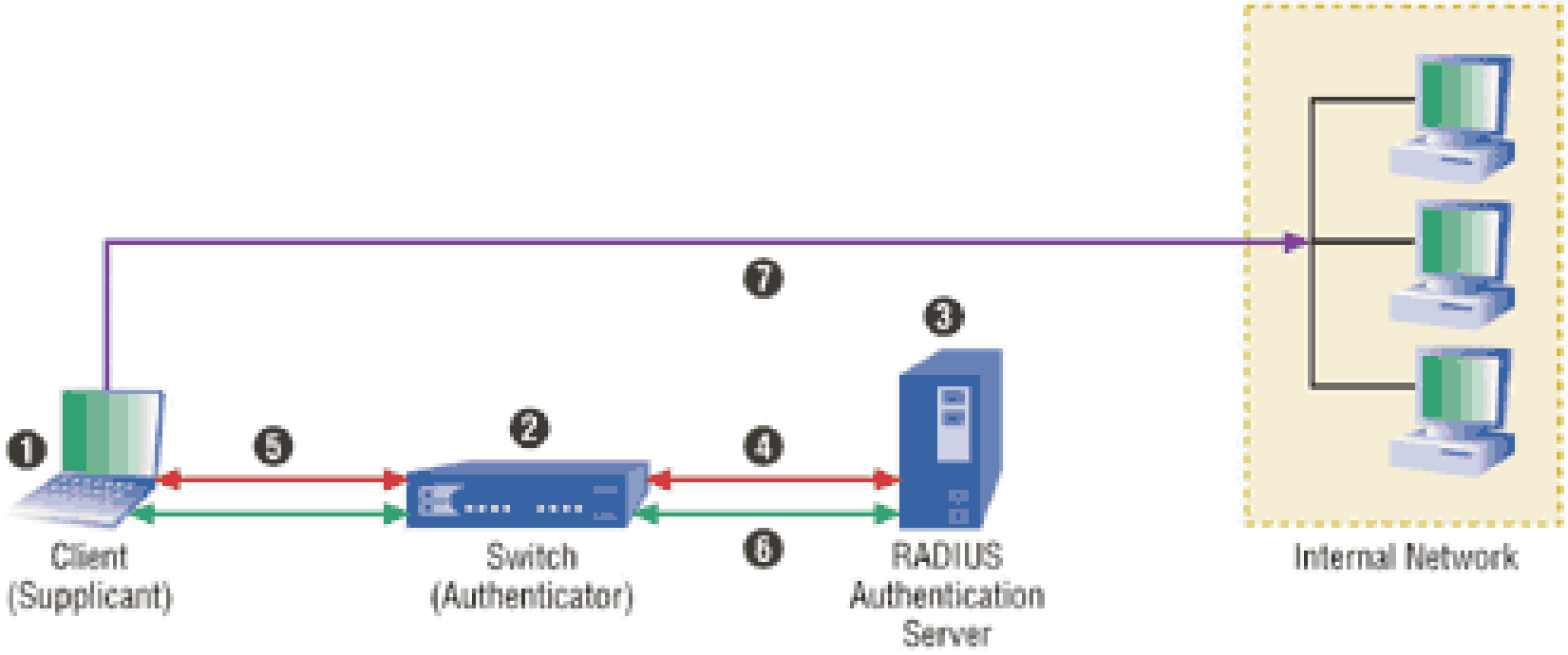


Como funciona o 802.1x?



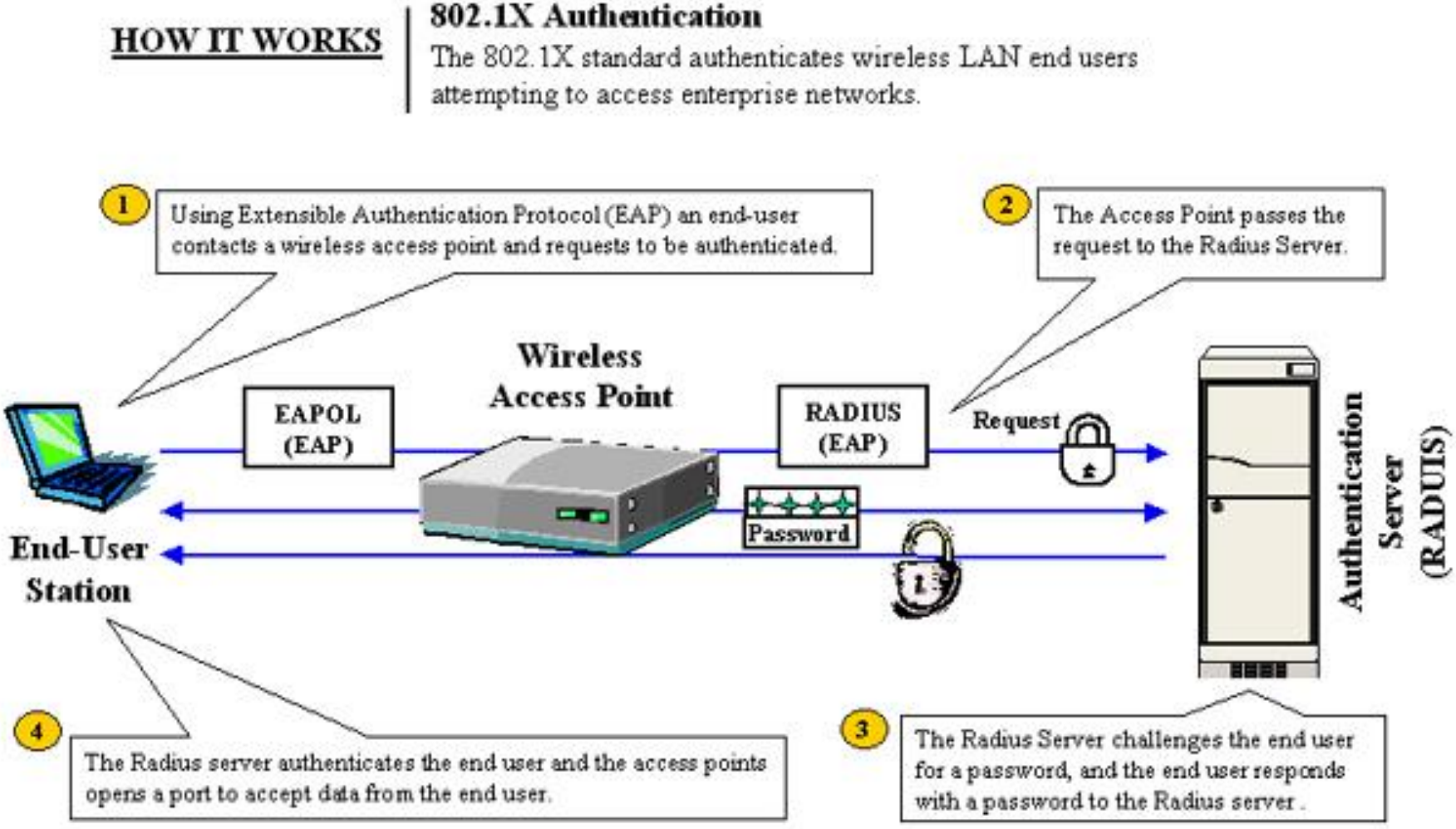


Como funciona o 802.1x?

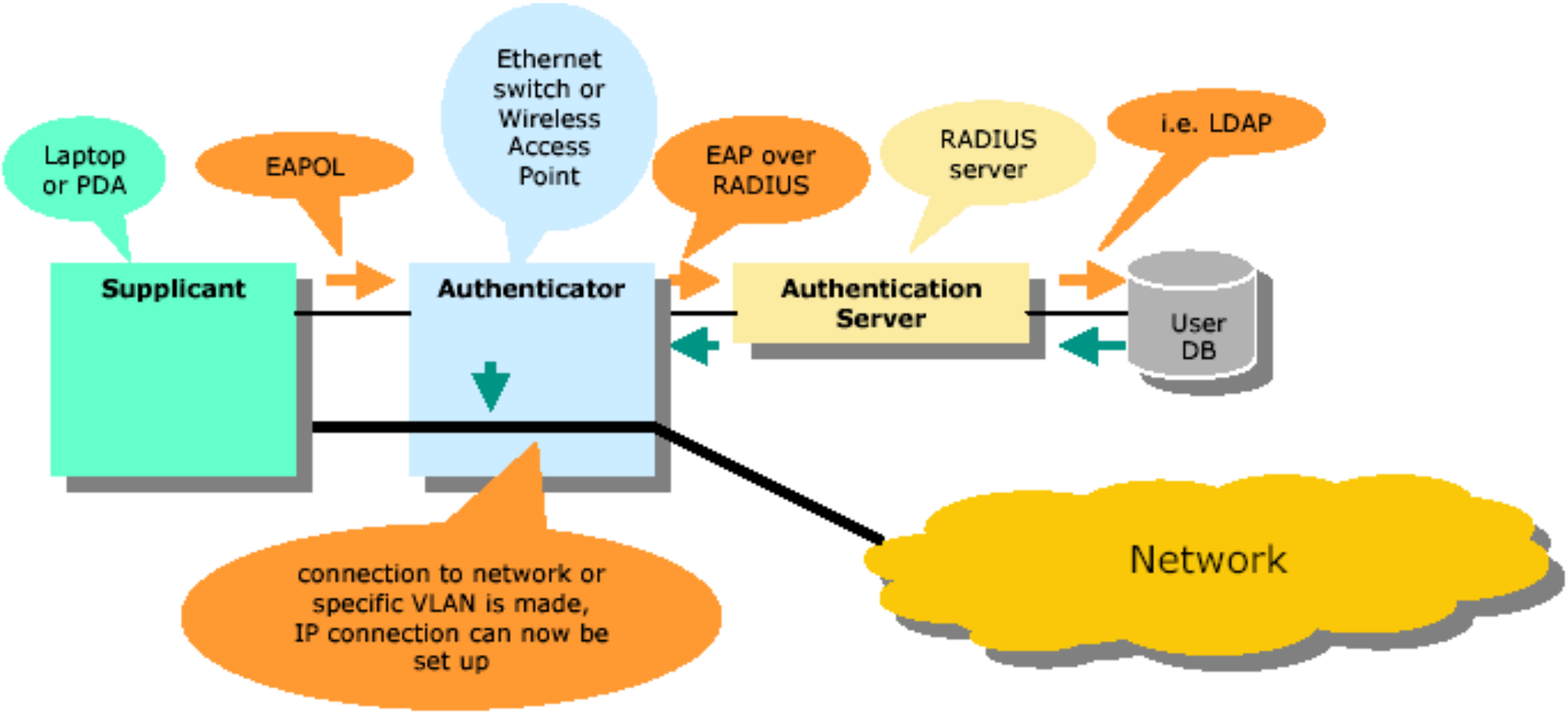


The 802.1X client ❶, also known as the supplicant, attempts to access the network and is stopped by the authenticator ❷, an 802.1X compliant switch or AP, which issues an EAP identity request. The authenticator proxies the response to a RADIUS authentication server ❸, which issues an authentication challenge in RADIUS format ❹. The authenticator encapsulates the challenge in either EAPoL format for a wired connection or EAPoW for wireless, and ❺ passes it to the client. The authenticator then passes ❻ the client's response to the authentication server. If the request is approved, the client gains network access ❼.

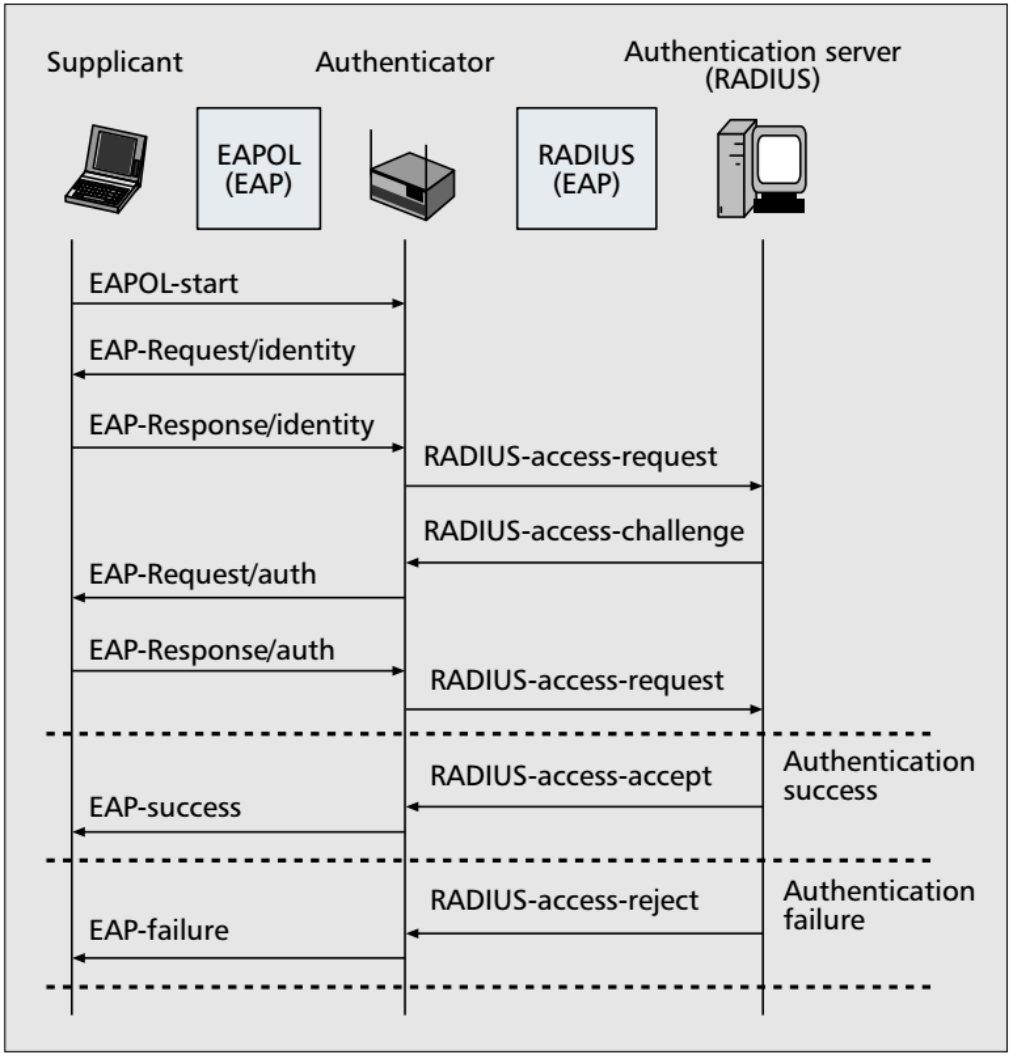
Como funciona o 802.1x?



Como funciona o 802.1x?



Fluxo típico de mensagens no IEEE802.1x



IEEE 802.1x

- Transporta informação de autenticação na forma de carga EAP (*Extensible Authentication Protocol*)
- O autenticador (*switch* ou AP) fica no meio recebendo as mensagens EAP em pacotes 802.1x passando-as ao servidor de autenticação utilizando pacotes RADIUS.
- Existem vários tipos de protocolos que podem ser utilizados com o EAP, as três formas mais comuns de EAP são:
  - EAP-MD5 – *MD5 Hashed Username/Password*
  - EAP-OTP – *One-Time Passwords*
  - EAP-TLS – *Strong PKI Authenticated* ***Transport Layer Security*** (SSL)

EAP sobre 802.1x

- O ***Extensible Authentication Protocol*** (RFC 2284) fornece uma arquitectura na qual vários mecanismos de autenticação podem ser utilizados, como, por exemplo:
  - EAP-MD5: *Username/Password* (pouco seguro)
  - EAP-TLS: PKI (certificados), autenticação forte
  - EAP-TTLS. *Username/Password* (seguro)
  - MS-CHAPv2: *Microsoft Username/Password* (pouco seguro)
  - PEAP: Forma de transporte seguro desenvolvido pela Microsoft/Cisco para o MS-CHAPv2

Mensagens EAPOL (Ethernet)

EAPOL-Start: When the Supplicant first connects to the LAN, it does not know the MAC address of the Authenticator (if any). By sending the EAPOL-Start message to a multicast group, the Supplicant can find out if there is any Authenticator present.

EAPOL-Key: Using this message type, the Authenticator sends encryption (and other) keys to the Supplicant once it has decided to admit it to the network.

EAPOL-Packet: This EAPOL frame is used to send actual EAP messages. It is simply a container to send EAP message across LAN.

EAPOL-Logoff: This message indicates that the Supplicant wishes to be disconnected from the network.

EAPOL-Encapsulated-ASF-Alert: This is provided for use by Alert Standard Forum (ASF) to allow alerts to be forwarded through a port that is in Unauthorized state.

All EAPOL frames have Ether Type of **0x888E**.

Formato das mensagens EAPOL (Ethernet)

PAE Ethernet type: 88-8E

Protocol version: 01

Packet type:

- EAP-Packet [0]
- EAPOL-Start [1]
- EAPOL-Logoff [2]
- EAPOL-Key [3]
- EAPOL-Encapsulated-ASF-Alert [4]

	Octet Number
PAE Ethernet Type (7.5.1)	1-2
Protocol Version (7.5.3)	3
Packet Type (7.5.4)	4
Packet Body Length (7.5.5)	5-6
Packet Body (7.5.6)	7-N

Packet body length: Depende da trama Ethernet

Packet body:

Transporta uma mensagem EAP [0], ou
uma chave [3], ou
um alerta [4].

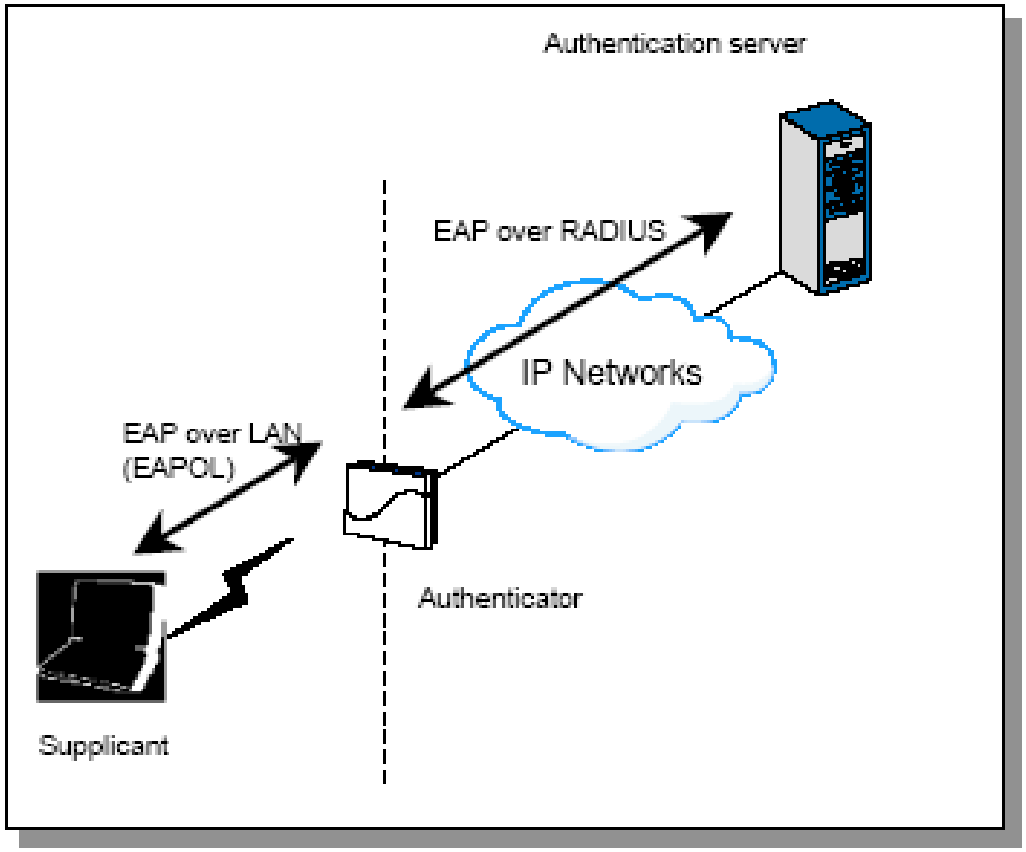
Conteudo da mensagem EAPOL-Key [3]

- No caso do EAPOL-Key [3], o corpo da mensagem contém uma estrutura que descreve a chave a trocar.
- O único algoritmo previsto na norma é o RC4.

	Octet Number
Descriptor Type (7.6.1)	1
Key Length (7.6.2)	2-3
Replay Counter (7.6.3)	4-11
Key IV (7.6.4)	12-27
Key Index (7.6.5)	28
Key Signature (7.6.6)	29-44
Key (7.6.7)	45-Packet Body Length

Tráfego 802.1x

- Como a figura indica, a informação EAP, quando transmitida do Suplicante para o Servidor de Autenticação, é primeiro encapsulada dentro de uma trama LAN (EAPoL). Uma vez recebida pelo Autenticador é extraída da trama LAN e colocada no pacote de acordo com o protocolo RADIUS.
- Este pacote RADIUS é então transmitido utilizando o protocolo RADIUS (sobre UDP).
- O tráfego vindo do Servidor de Autenticação para o Suplicante segue o processo inverso.



Mais informação

- 802.1x http://standards.ieee.org/reading/ieee/std/lanman/802.1X-2001.pdf
- RFC's: see http://www.ietf-editor.org
- EAP RFC 2284
- EAP-MD5 RFC 1994, RFC 2284
- EAP-TLS RFC 2716
- EAP-TTLS http://www.funk.com/NIdx/draft-ietf-pppext-eap-ttls-01.txt
- PEAP http://www.globecom.net/ietf/draft/draft-josefsson-pppext-eap-tls-eap-02.html
- RADIUS RFC 2865, 2866, 2867, 2868, 2869 (I/w EAP)