

# **Segurança da Informação**

## **Padrão 802.1x - Port-Based Network Access Control**

José Maurício S. Pinheiro

UniFOA - 2008

# 802.1x

- Define o controle de acesso com base em porta, sendo usado para fornecer acesso autenticado nas redes padrão IEEE 802.11 e Ethernet.
- Com o controle de acesso baseado em porta, um dispositivo de rede envia quadros somente após ter o acesso concedido pelo switch (Ethernet) ou pelo Access Point (802.11).
- A permissão se dá através de processo de autenticação onde são verificadas as credenciais do dispositivo que está se conectando, reduzindo as vulnerabilidades de segurança associadas com redes padrão IEEE 802.11.

# 802.1x

- Os padrões IEEE 802.11 especificam dois métodos de autenticação:
  - Baseado na identificação do adaptador (autenticação de sistema aberto)
  - Baseado no conhecimento de chave secreta (autenticação de chave compartilhada).
- O IEEE 802.1x impõe a verificação de credenciais do usuário antes de conceder acesso à rede sem fio e, dependendo do método de autenticação usado, determina dinamicamente as chaves de criptografia para a comunicação.

# EAP

- Protocolo para autenticação ponto a ponto (*Point to Point Protocol* - PPP) com suporte a vários mecanismos de autenticação:
  - TLS e TTLS;
  - MD5-challenge;
  - One-Time Passwords;
  - Generic Token Card;
  - Outros...
- Durante o processo de autenticação, o EAP (*Extension Authentication Protocol*) é usado para controle de tráfego e troca de mensagens.

# 802.1x

- A Segurança em Nível de Transporte EAP (EAP-TLS) é usada em ambientes seguros com base em certificado. Ela proporciona um método seguro de autenticação e determinação de chave.
- A EAP-TLS oferece autenticação mútua, negociação do método de criptografia e determinação da chave criptográfica entre o cliente e o servidor de autenticação - normalmente RADIUS (Remote Authentication Dial-In User Service).

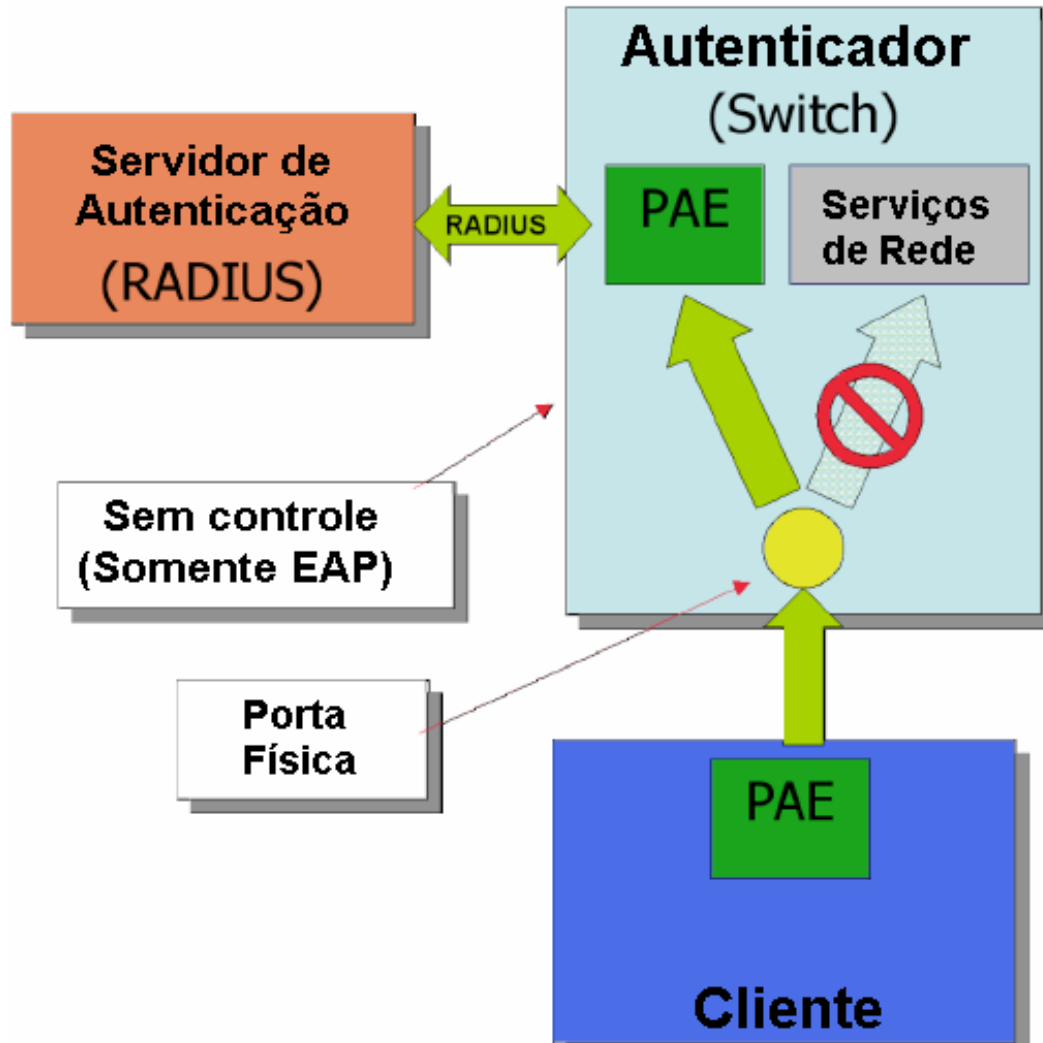
# 802.1x

## Entidades do sistema

- **Autenticador** - ponto de acesso da rede onde o padrão 802.1x está ativo (Switch);
- **Servidor de Autenticação** - executa a autenticação, permitindo ou negando acesso à rede baseado em nome de usuário e senha (Servidor RADIUS);
- **Porta de Acesso de Entrada (PAE)** - componente lógico 802.1x do cliente e do autenticador que troca mensagens EAP;
- **EAP** - protocolo usado entre o cliente e o autenticador;
- **Suplicante (Cliente)** - dispositivo de rede que requer acesso aos serviços da LAN.

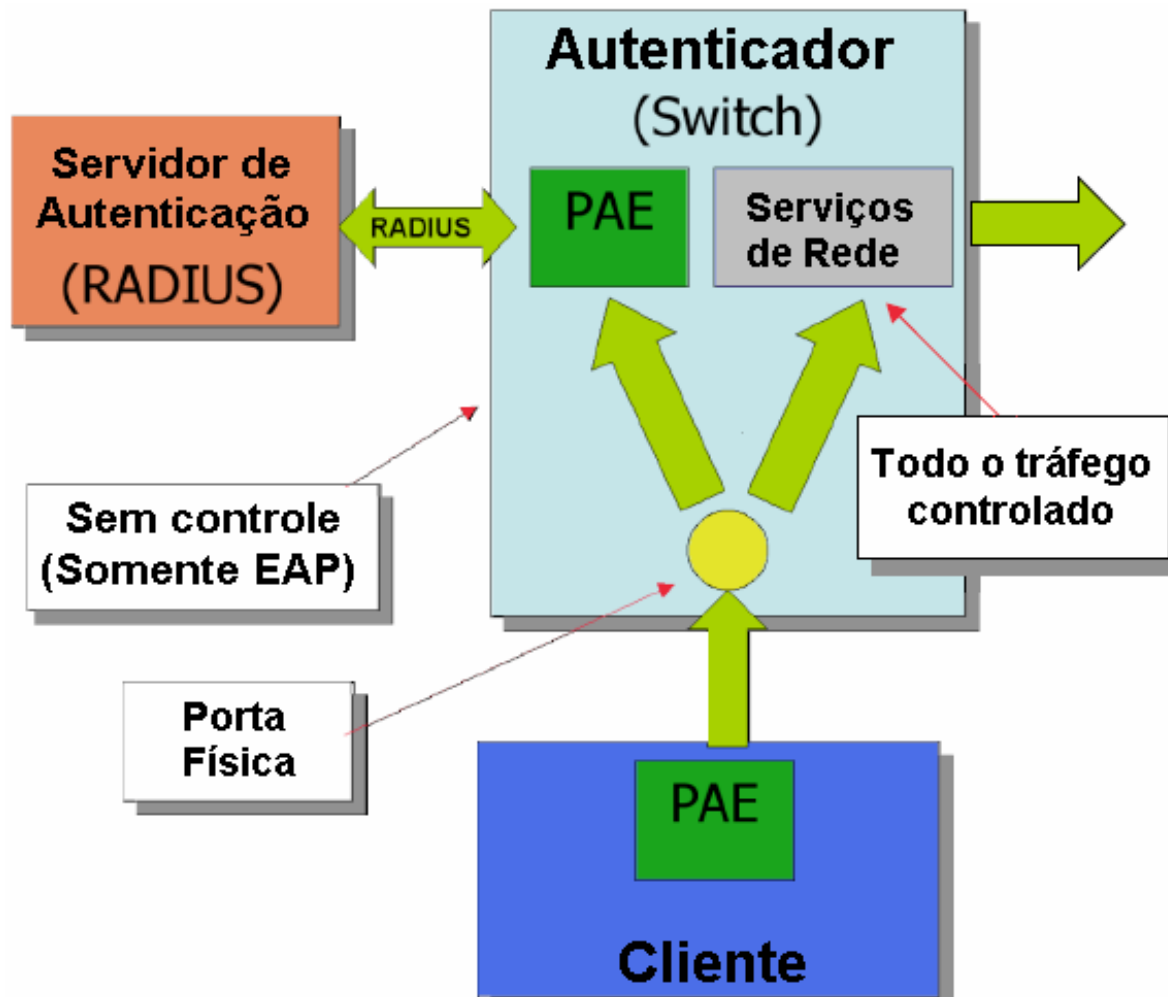
# 802.1x

- Antes da autenticação:



# 802.1x

- Ligação segura entre cliente e servidor de autenticação:





# 802.1x

- Troca de mensagens entre Cliente, EAP e RADIUS:

