UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Comunicação Sem Fio (Wireless)

Aula 9 – Segurança em Redes Sem-fio (continuação)

Prof. Fred Sauer

email: fsauer@gmail.com

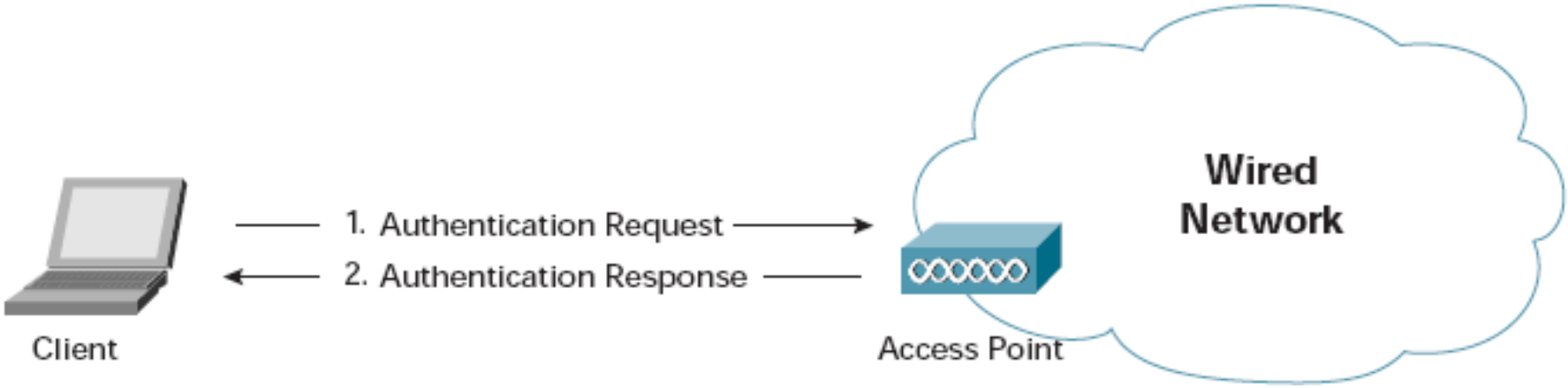
http://www.fredsauer.com.br

WEP

- Autenticidade:
  - Oferece dois mecanismos
    - ✓ Open authentication e Shared key authentication
    - ✓ Ambos não garantem autenticidade
  - Open authentication
    - ✓ Uma estação solicita acesso ao AP e o AP garante o acesso.
    - ✓ Funciona como autenticação nula

WEP

- Autenticidade:
  - Open authentication: Composto de duas mensagens

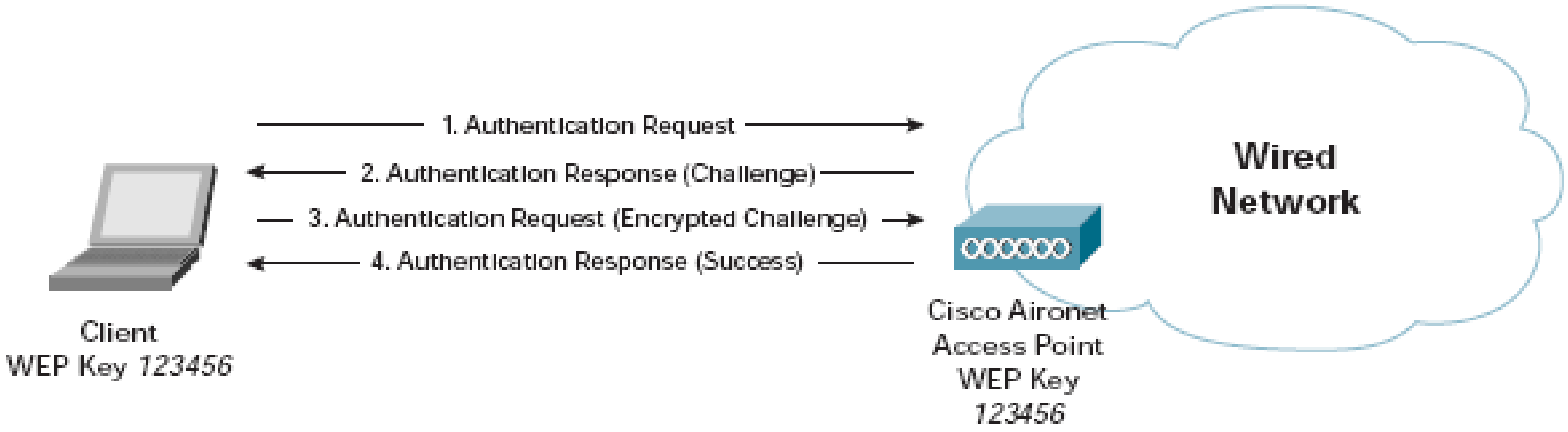


WEP

- Autenticidade:
  - Shared key authentication
    - ✓ Utiliza o esquema de challenge-response
    - ✓ Apenas garante que as chaves são as mesmas
    - ✓Não deve ser utilizado por expor a chave de criptografia
  - Alguns fabricantes oferecem autenticação utilizando o MAC, porém este esquema pode ser forjado (spoofing)

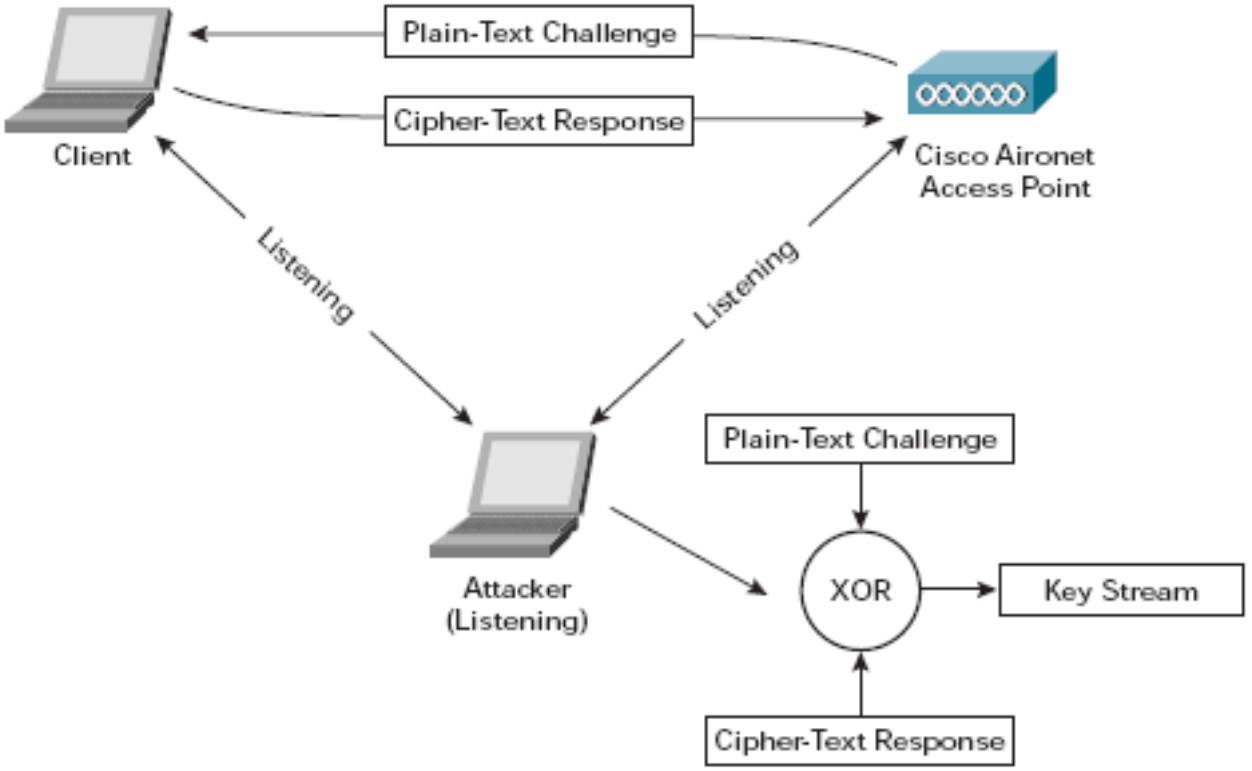
WEP

- Autenticidade:
  - Shared key authentication:



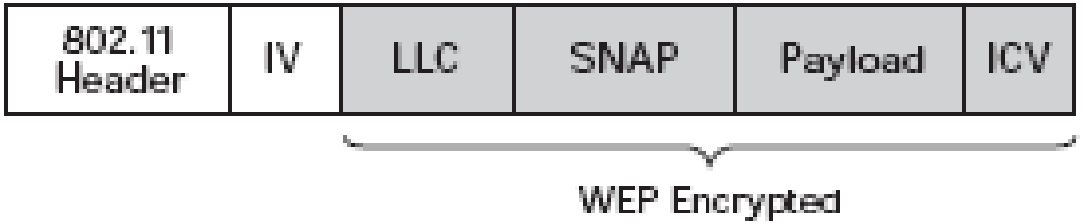
WEP

- Autenticidade:
  - Problema:



WEP

- Integridade:
  - – Permite que o destinatário verifique se o frame foi alterado
  - – Adiciona um campo (Integrity Check Value – ICV) ao frame antes de ser criptografado
  - – O ICV é calculado a partir do frame a ser transmitido
  - –Semelhante ao CRC, porém o CRC não é enviado criptografado e pode ser recalculado e reposto pela ameaça



IEEE 802.1X

- Controle de acesso baseado no conceito de porta
  - Foi definido originalmente para Switches Ethernet
- Formado por três entidades
  - O suplicante, que solicita a conexão
  - Autenticador, que controla o acesso
  - Servidor de autenticação, que processa os pedidos de conexão

IEEE 802.1X

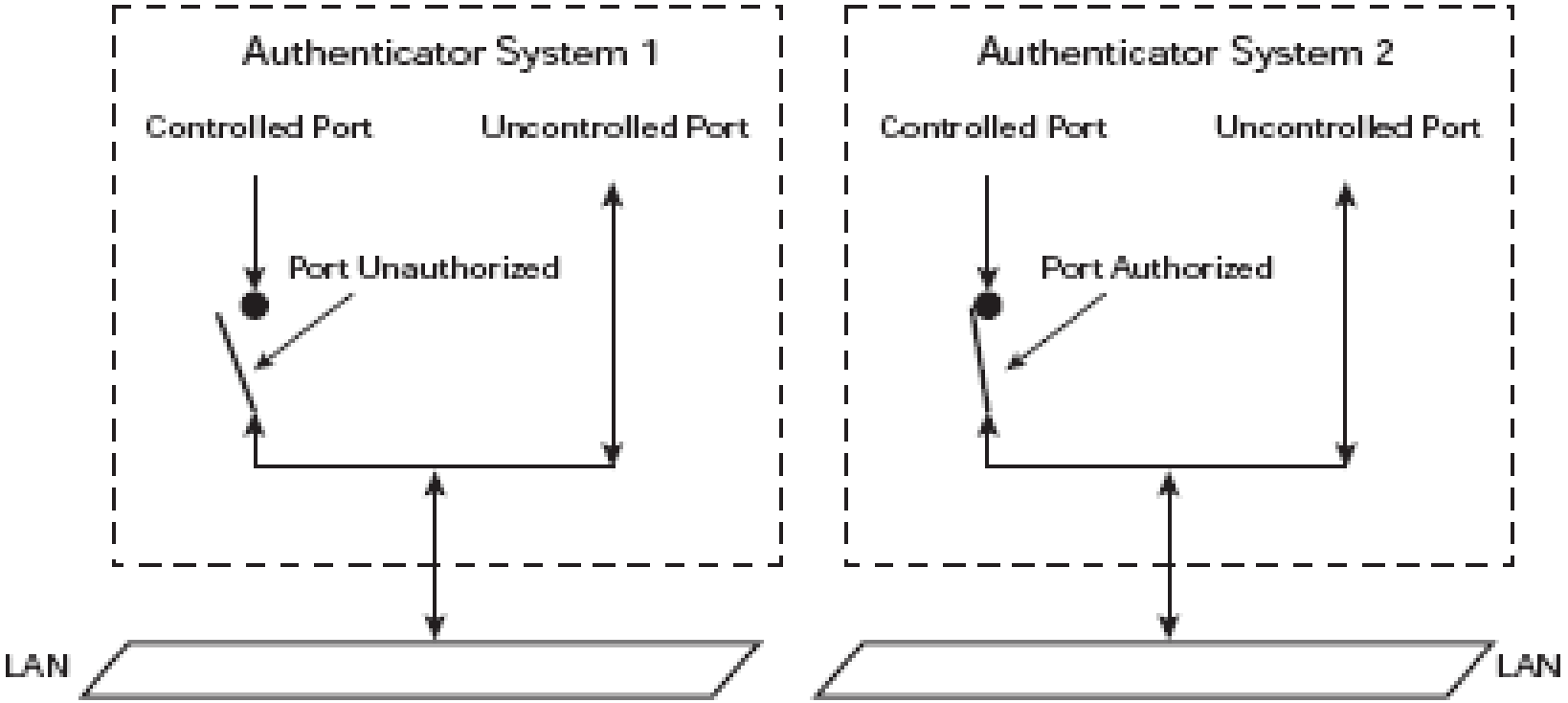
- Utiliza o EAP (Extensible Authentication Protocol), RFC 2284, para interligar os protocolos de autenticação da camada de aplicação com os da camada de enlace.
  - O EAPOL (EAP Over LAN) extensão para ser utilizada em redes 802.*

- Geralmente utiliza o RADIUS como protocolo e servidor de autenticação

- É possível que o AP faça o papel de autenticador e servidor de autenticação

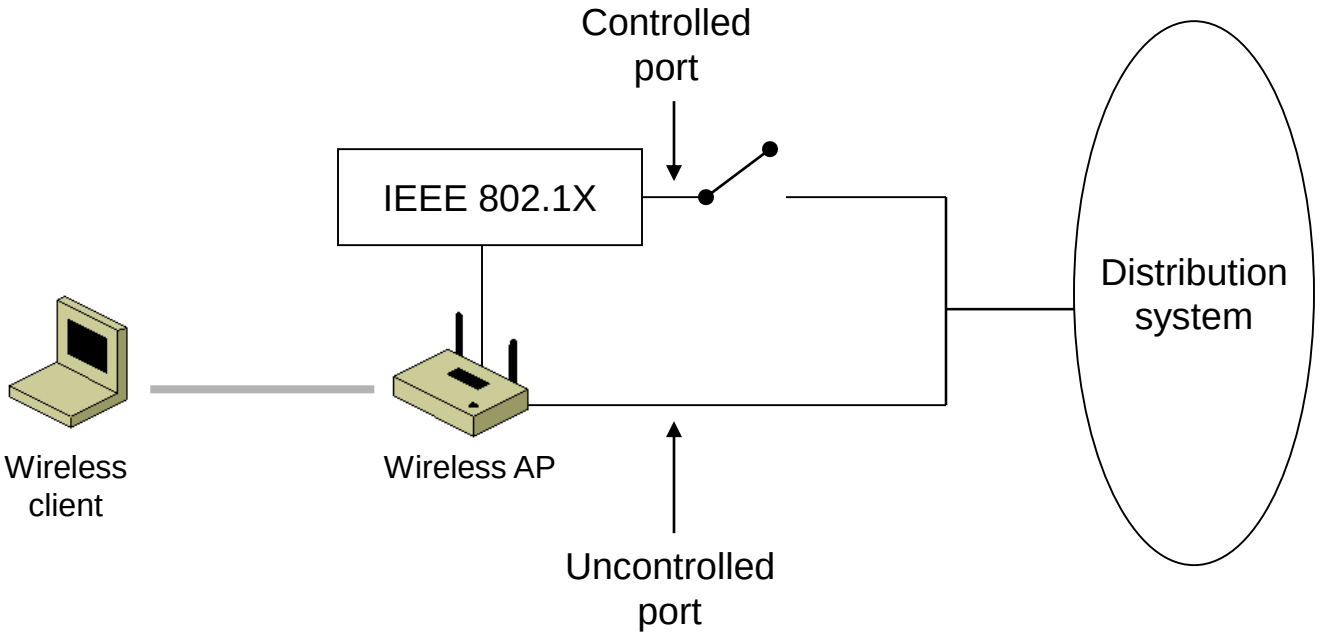
IEEE 802.1X

- Conceito de porta



IEEE 802.1X

- Porta controlada:
  - Usada para encaminhar frames entre o cliente wireless e o sistema de distribuição
- Porta sem controle:
  - Usado para tráfego entre o AP e o sistema de distribuição



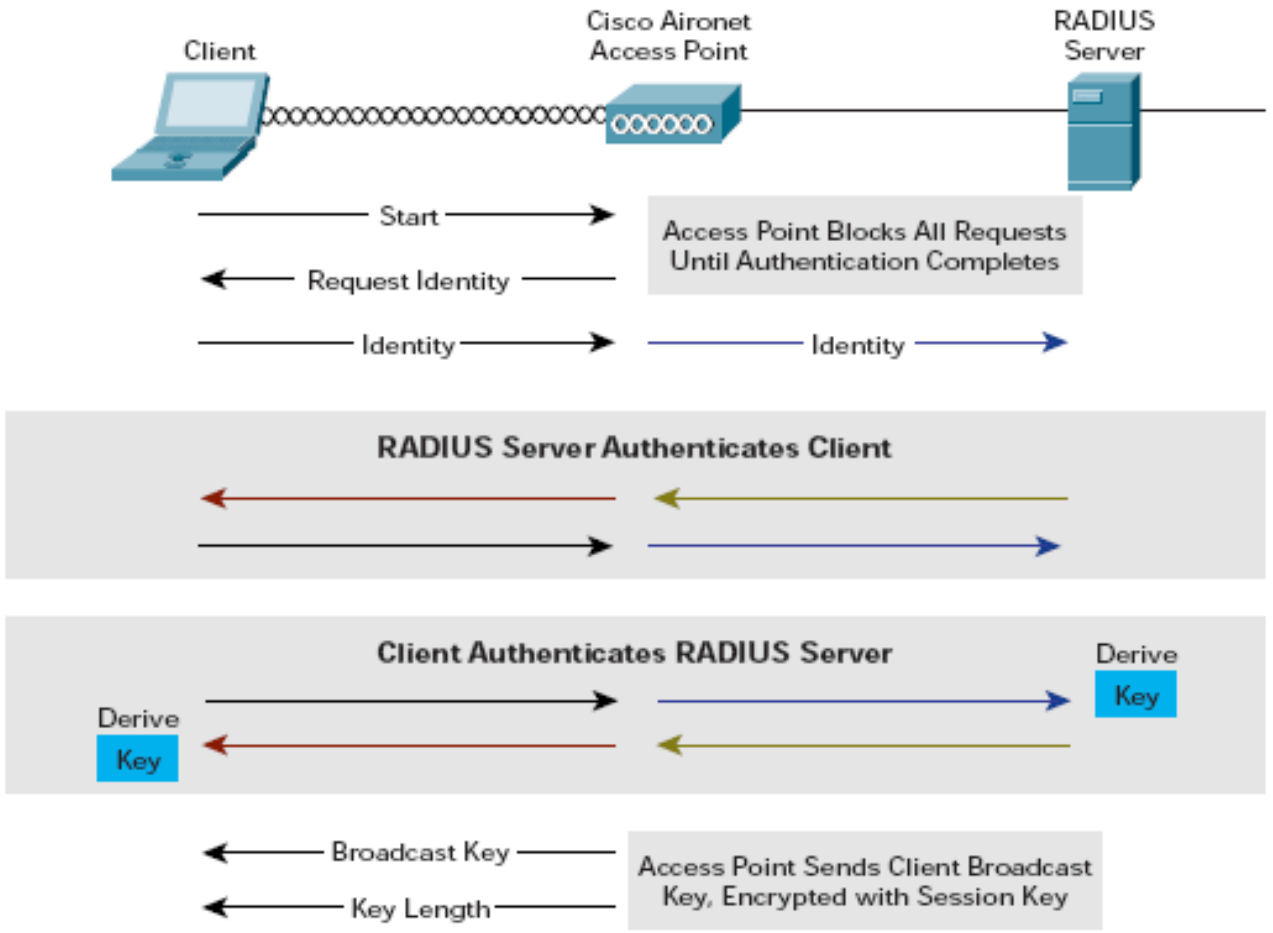
IEEE 802.1X

- Processo de autenticação (resumo):

1) A estação envia uma mensagem do tipo EAP-start, que inicia o processo de autenticação;
2) O AP responde com mensagem EAP-request, solicitando ao cliente sua identificação;
3) A estação envia uma mensagem EAP-response com sua identificação para o AP;
4) O AP envia a mensagem para o servidor de autenticação;
5) O servidor de autenticação verifica as credenciais do cliente e envia uma mensagem para o AP indicando se o cliente está ou não autorizado;
6) O AP envia uma mensagem EAP-success ou EAP-reject para o cliente;
7) Caso o cliente seja autorizado, o AP altera o estado da porta para autorizada.

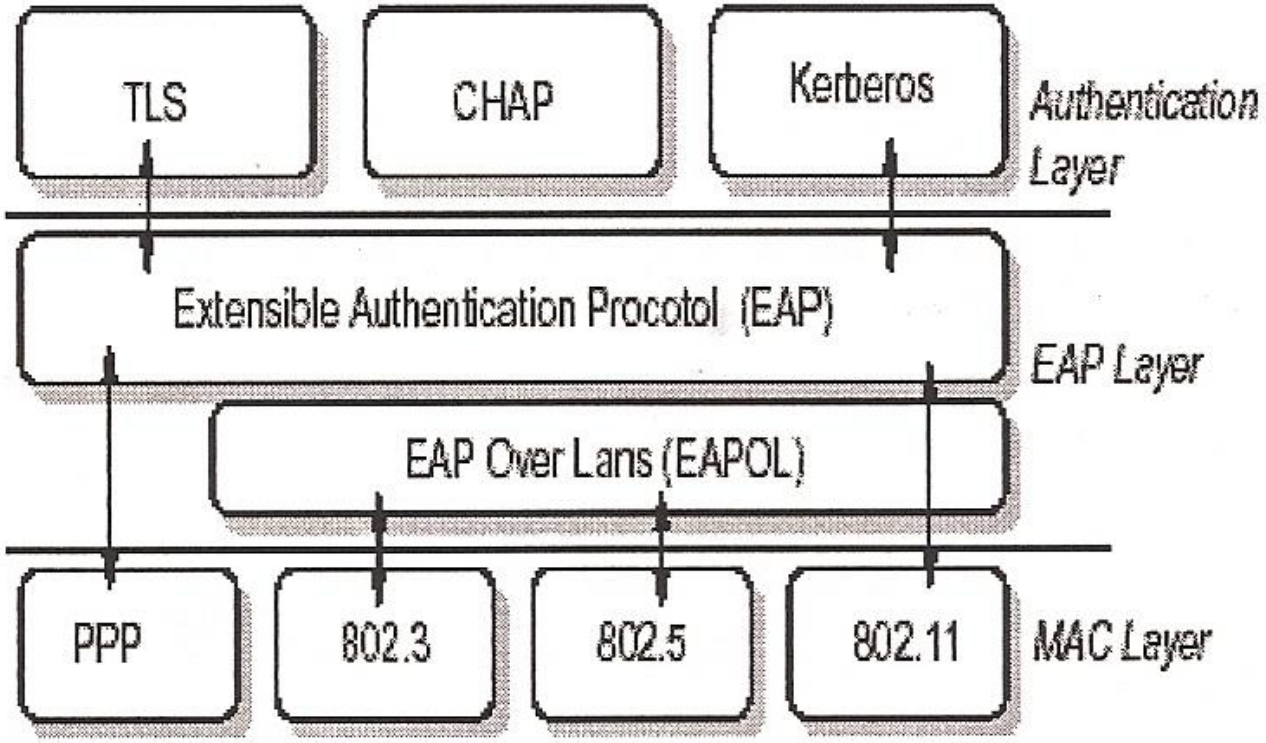
IEEE 802.1X

- Processo de autenticação



IEEE 802.1X

- Camadas:



IEEE 802.1X

- Protocolos de autenticação

1) EAP-TLS (Transport Layer Security);

- ✓ PEAP(protected);
- ✓ TTLS (Tunneled TLS)
- ✓ CISCO LEAP (Light EAP)
- ✓ EAP-SIM (Subscriber Identity Module)
- ✓ Kerberos V5