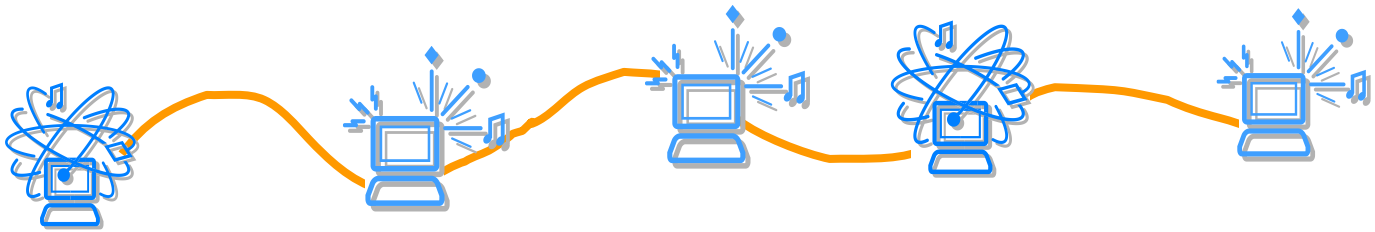
EAP (*Extensible Authentication Protocol*)
RFC 3748



Redes de Comunicação

Departamento de Engenharia da Electrónica e Telecomunicações e de Computadores

Instituto Superior de Engenharia de Lisboa

EAP (*Extensible Authentication Protocol*)

- O EAP foi originalmente criado como parte do PPP (***Point-to-Point Protocol***) [RFC 2284]
  - O ***Extensible Authentication Protocol*** **(EAP)** é um protocolo que foi criado para autenticação no PPP e que suporta múltiplos mecanismos de autenticação. Foi desenvolvido em resposta ao aumento da procura de autenticação para utilizadores de acessos remotos que utilizam outros mecanismos de segurança.

- **Usando EAP, pode ser adicionado o suporte para diversos mecanismos de autenticação definindo EAP-Types**. O suporte pode incluir cartões de *token*, *one-time passwords*, autenticação com chave pública usando cartão inteligente, certificados digitais e outros.

- **O EAP esconde os detalhes do mecanismo de autenticação dos elementos da rede** que não necessitam de o conhecer.
  - Por exemplo, em PPP, só o cliente (suplicante) e o servidor de autenticação (AAA) necessitam conhecer o tipo EAP, o *Network Access Server* (autenticador) não necessita.

EAP

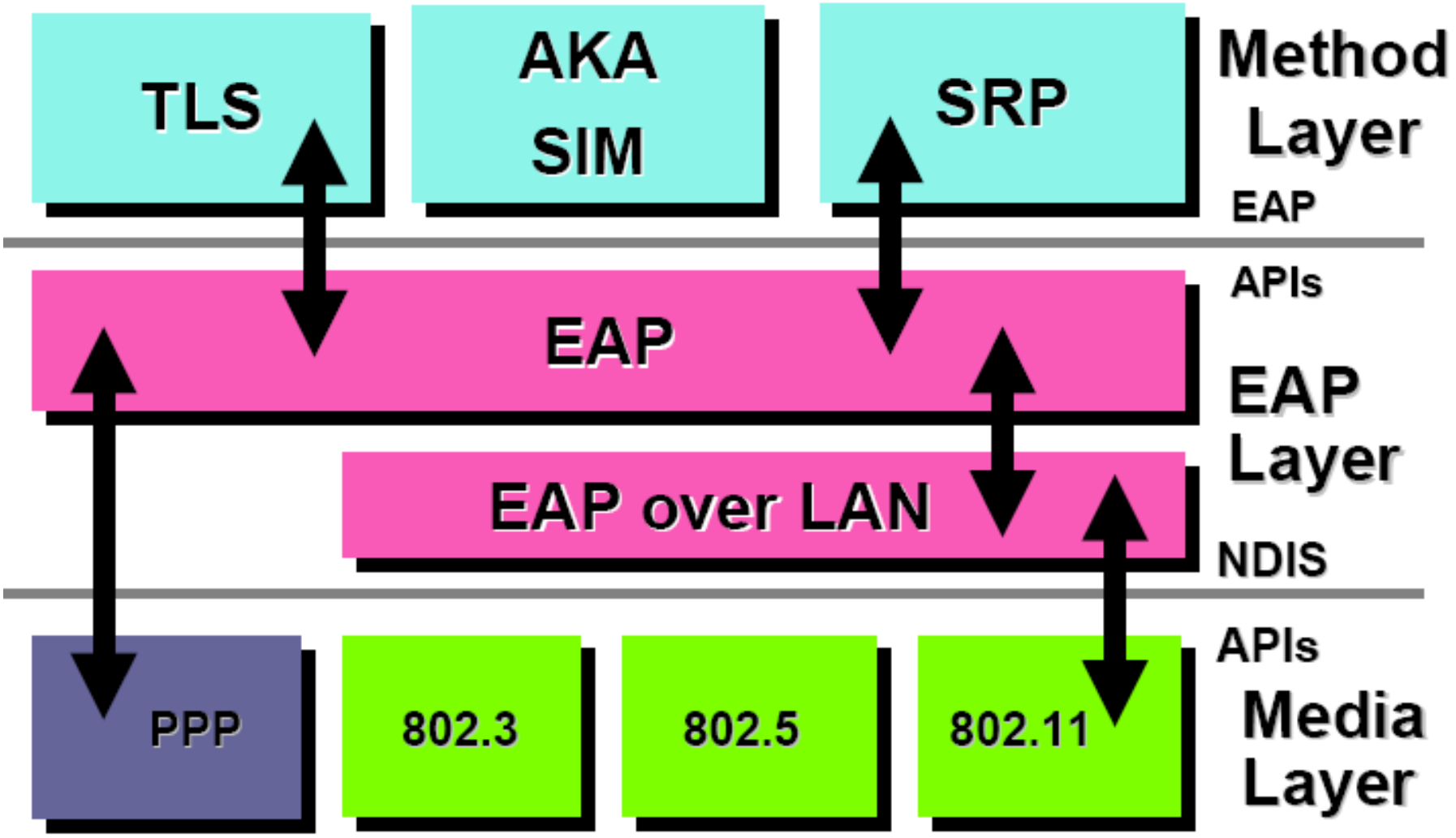
- **O EAP não seleciona um mecanismo de autenticação especifico na fase de *Link Control*, adia isso até à fase de *Authentication***:

  - Isto permite ao autenticador requerer mais informação antes de determinar o mecanismo de autenticação especifico.

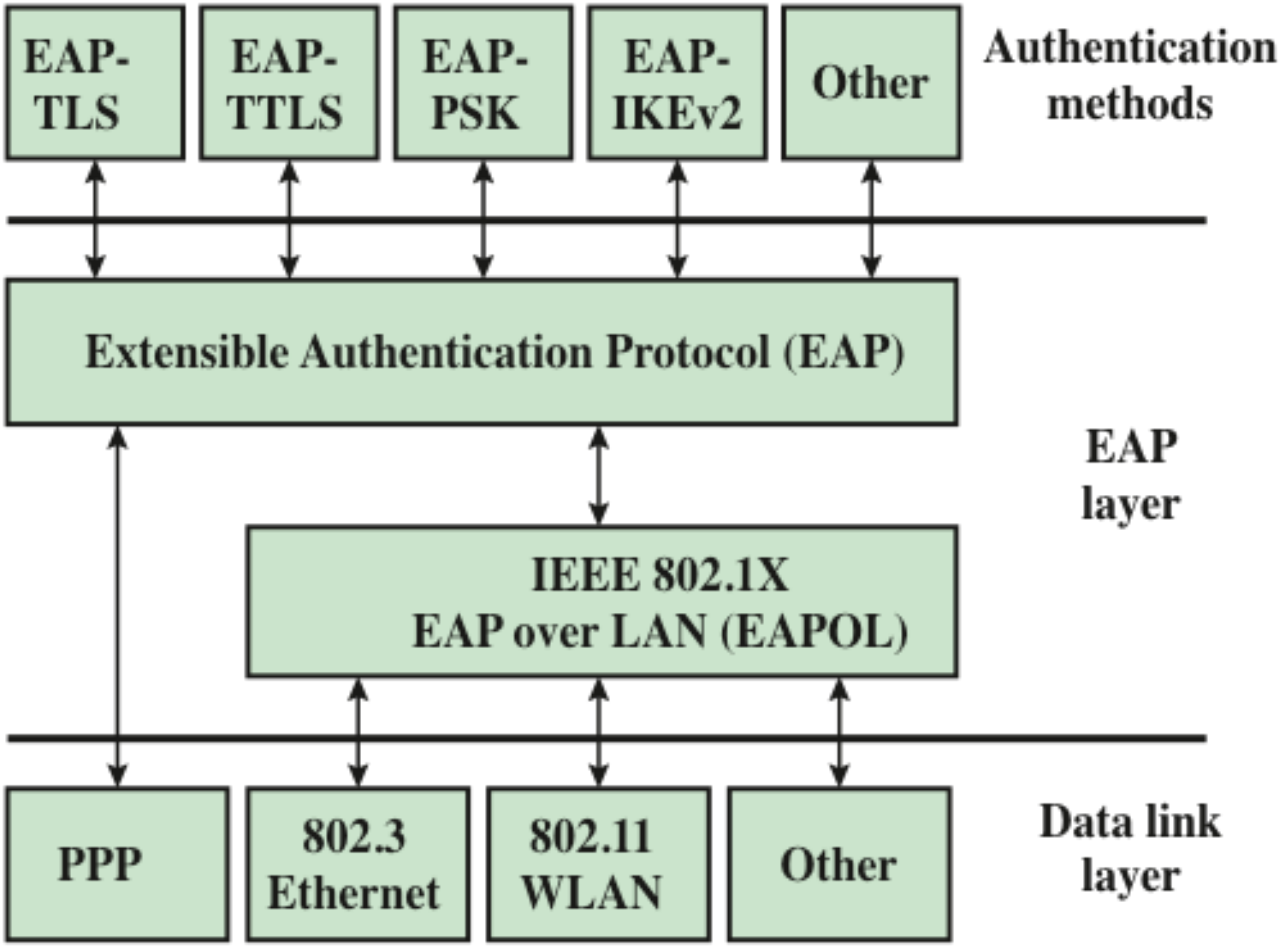
  - Isto permite também a utilização de um servidor de "*back-end*", o qual actualmente implementa vários mecanismos enquanto o autenticador PPP se limita a enviar a informação de autenticação.

  - Possibilita a utilização do EAP sobre outros protocolos para além do PPP.

EAP: Arquitectura



EAP: Arquitectura



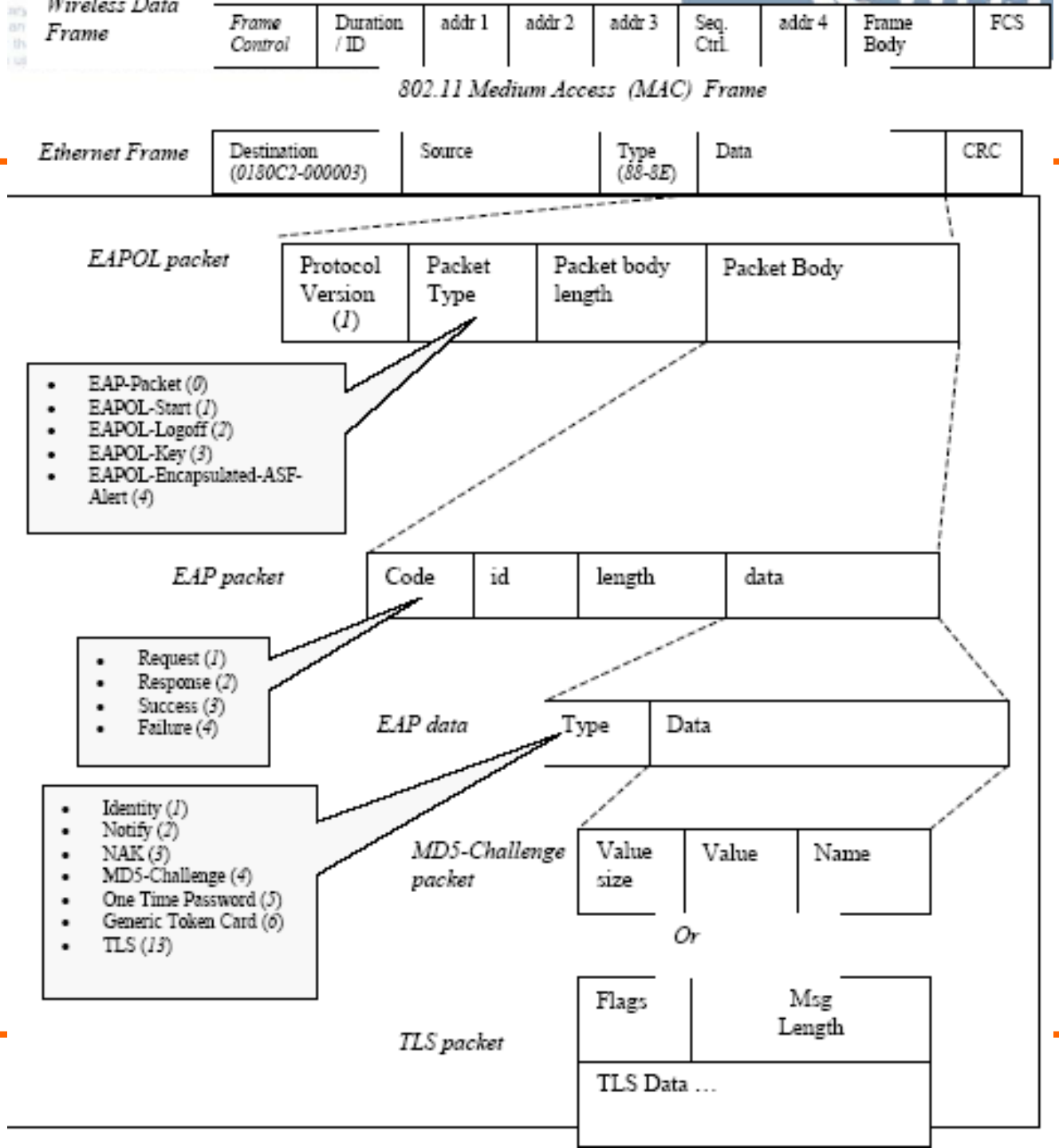
"Cryptography and Network Security", 7th edition, William Stallings

Common EAPOL Frame Types

Frame Type	Definition
EAPOL-EAP/Packet	Contains an encapsulated EAP packet.
EAPOL-Start	A supplicant can issue this packet instead of waiting for a challenge from the authenticator.
EAPOL-Logoff	Used to return the state of the port to unauthorized when the supplicant if finished using the network.
EAPOL-Key	Used to exchange cryptographic keying information.

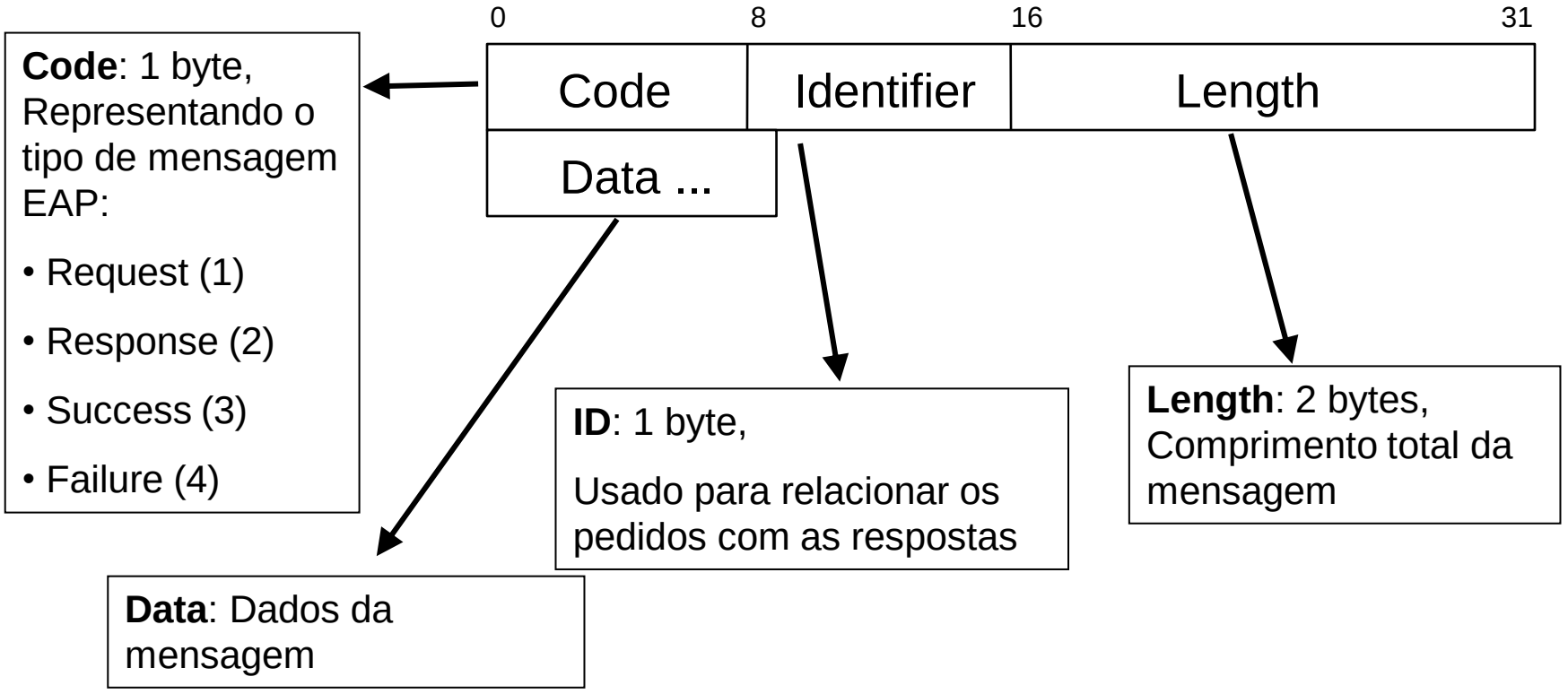
"Cryptography and Network Security", 7th edition, William Stallings

EAP: Alternativas ao PPP



EAP: Mensagens

Todas as mensagens EAP têm um formato comum.



EAP: Mensagens

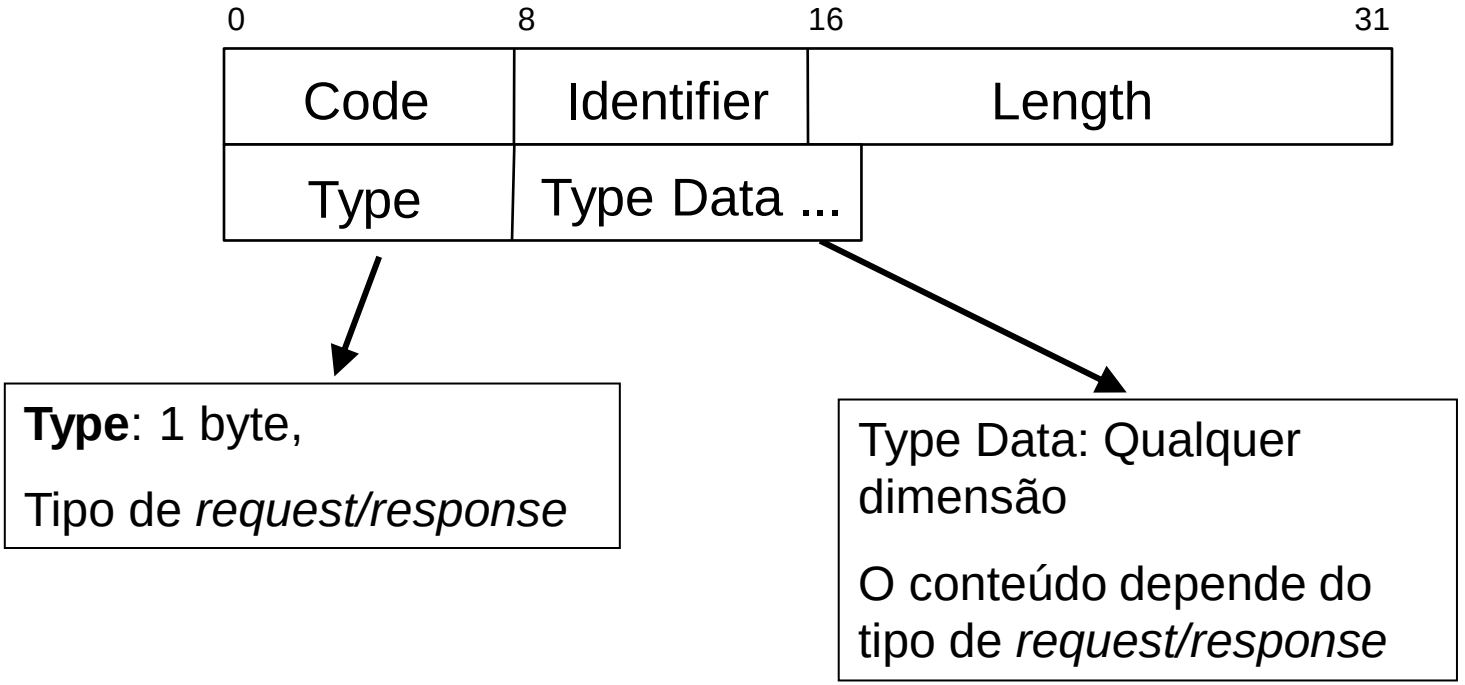
- O EAP utiliza em quatro tipos de mensagens diferentes:
  - ***Request*** (do *Autenticator* para o cliente [Suplicante])
  - ***Response*** (do Cliente para o *Autenticador*)
  - ***Success***
  - ***Failure***

EAP: Mensagens

- Os pedidos e as respostas EAP têm o mesmo formato, com:

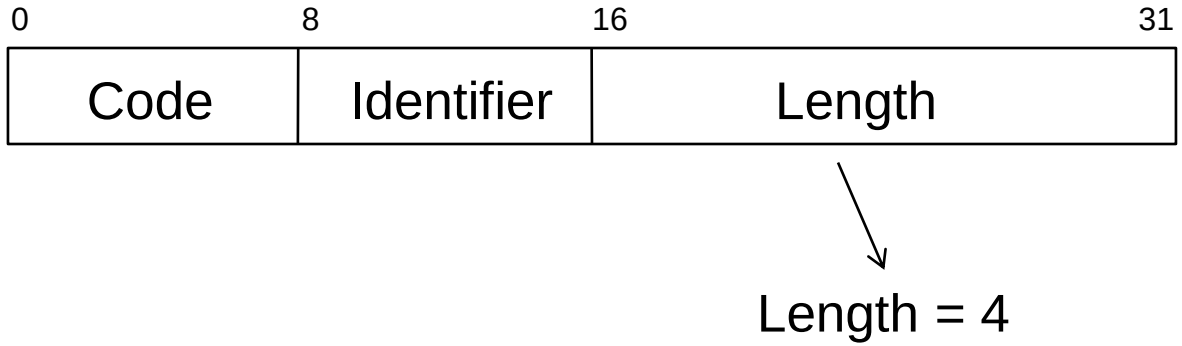
  code*=1** para os ***request

  code*=2** para as ***response



EAP: Mensagens

- As mensagens EAP de *Success* e *Failure* não transportam dados:
  - ***Success*** – *code* = 3 - indica que a autenticação foi concluida com sucesso.
  - ***Failure*** – *code* = 4 **-** indica que a autenticação falhou.



EAP: Tipos de EAP Request/Response

- Inicialmente foram definidos os seguintes tipos de mensagens EAP *request/response*:
  - 1 Identity
  - 2 Notification
  - 3 Nak (apenas Response)
  - 4 MD5-Challenge
  - 5 One-Time Password (OTP) (RFC 1938)
  - 6 Generic Token Card

- Posteriormente foram definidos outros tipos de mensagens.

EAP: Fluxo

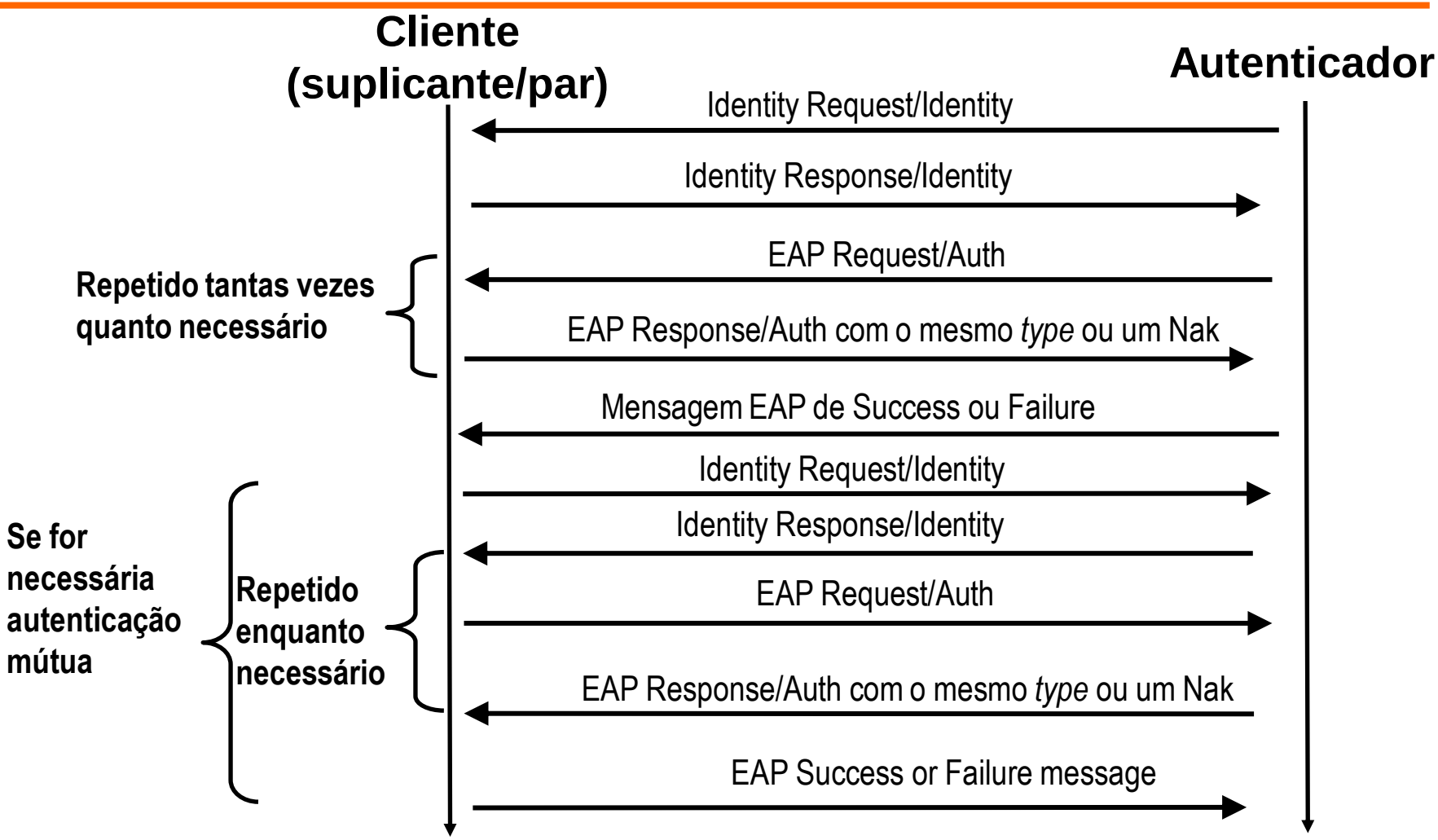
- Depois da fase de estabelecimento da ligação ("*Link Establishment*") estar completa, o Autenticador envia um ou mais *Requests* para autenticar o suplicante.
- O *Request* tem um campo "*type*" para indicar o que está a ser pedido. Exemplos de tipos de *Requests* incluem *Identity*, *MD5-challenge, One-Time Passwords, Generic Token Card*, etc.
  - O tipo *MD5-challenge* corresponde aproximadamente ao protocolo de autenticação CHAP.
- Tipicamente, o Autenticador envia um *Identity Request* inicial seguido por um ou mais *Requests* para informação de autenticação. No entanto, um *Identity Request* inicial não é necessário, e PODE ser dispensado nos casos em que a identidade pode ser presumida (linhas dedicadas, etc.)

EAP: Fluxo

- O suplicante envia um pacote *Response* em resposta a cada *Request*. Tal como com o pacote *Request*, o pacote de *Response* contém um campo *type* que corresponde ao campo *type* do *Request*.

- O autenticador finaliza a fase de autenticação com um pacote de *Success* ou *Failure*.

EAP: Fluxo genérico de autenticação



EAP: Comparação

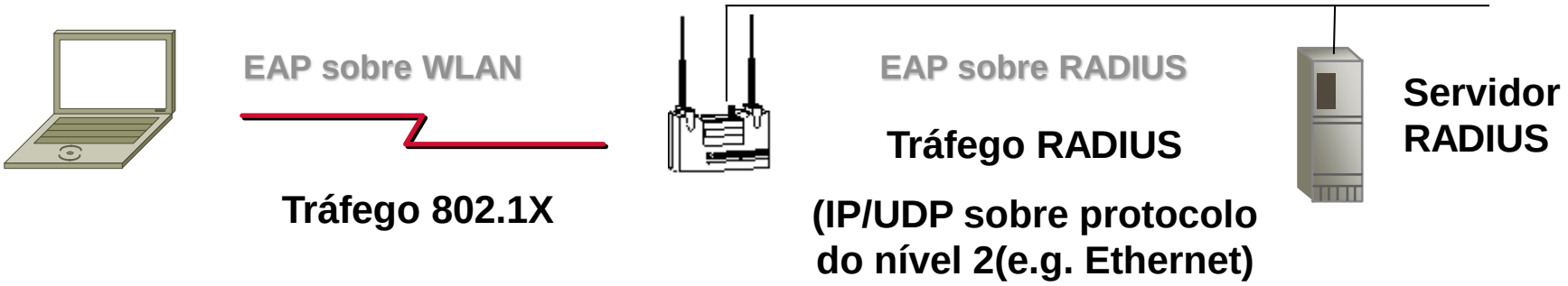
EAP Type	Open/ Proprietary	Mutual Auth	Authentication Credentials		Key Material	User Name	RFC
			Supplicant	Authenticator			
MD5	Open	No	Username/Pwd	None	No	Yes	1321
TLS	Open	Yes	Certificate	Certificate	Yes	Yes	2716
TTLS	Open	Yes	Username/Pwd	Certificate	Yes	No	IETF Draft
PEAP	Open	Yes	Username/Pwd	Certificate	Yes	No	IETF Draft
SIM	Open/GSM	Yes	SIM		Yes		IETF Draft
AKA	Open/UMTS	Yes	USIM		Yes		IETF Draft
SKE	Open/CDMA	Yes			Yes		IETF Draft
LEAP	Proprietary	Yes	Username/Pwd		Yes	Yes	NA

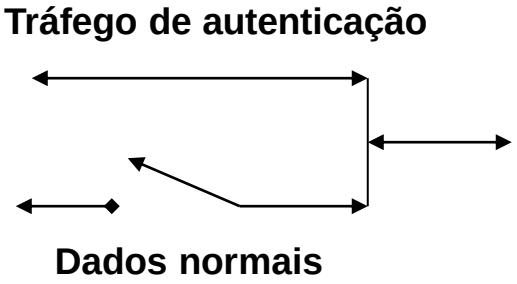
EAP TYPE	DYNAMIC RE-KEYING	MUTUAL AUTHENTI-CATION	USER ID & PASSWORD	ATTACK METHODS	COMMENTS
EAP-MD5	No	No	Yes	♦ Dictionary attack ♦ Man in the middle ♦ Session hijack	♦ Easy to implement ♦ Supported on many servers, but ♦ Insecure ♦ Requires cleartext databases
EAP-TLS	Yes	Yes	No	♦ Offers strong authentication security	♦ Requires client certificates ♦ Increases maintenance & token costs ♦ Two-factor authentication with smartcards
EAP-SRP	Yes	Yes	Yes	♦ Dictionary attack	♦ No certificates (server verifies secrets) ♦ Dictionary attack on credential store ♦ Intellectual property issues
EAP-LEAP	Yes	Yes	Yes	♦ Dictionary attack	♦ Proprietary solution ♦ AP must have LEAP support

EAP-SIM	Yes	Yes	No	♦ May be vulnerable to spoofing	♦ Leverages GSM roaming infrastructure ♦ Two-factor authentication
EAP-AKA	Yes	Yes	No	♦ Offers strong authentication security for cellular environment	♦ Leverages GSM roaming infrastructure ♦ Two-factor authentication
EAP-SecurID	No	No	No	♦ Man in the middle ♦ Session hijack	♦ Users PIN/One-time password ♦ Requires tunneled authentication ♦ Two-factor authentication
EAP-TTLS	Yes	Yes	No	♦ Offers strong authentication security	♦ Creation of secure TLS (SSL) tunnel ♦ Supports legacy authentication methods: PAP, CHAP, MS-CHAP, MS-CHAP V2 ♦ User identity is protected (encrypted)
EAP-PEAP	Yes	Yes	No	♦ Offers strong authentication security	♦ Similar to EAP-TTLS ♦ Creation of a secure TLS (SSL) tunnel ♦ User identity is protected (encrypted)

EAP: Antes de iniciar

- Associação 802.11 entre cliente e autenticador
- A ligação IP é bloqueada pelo AP

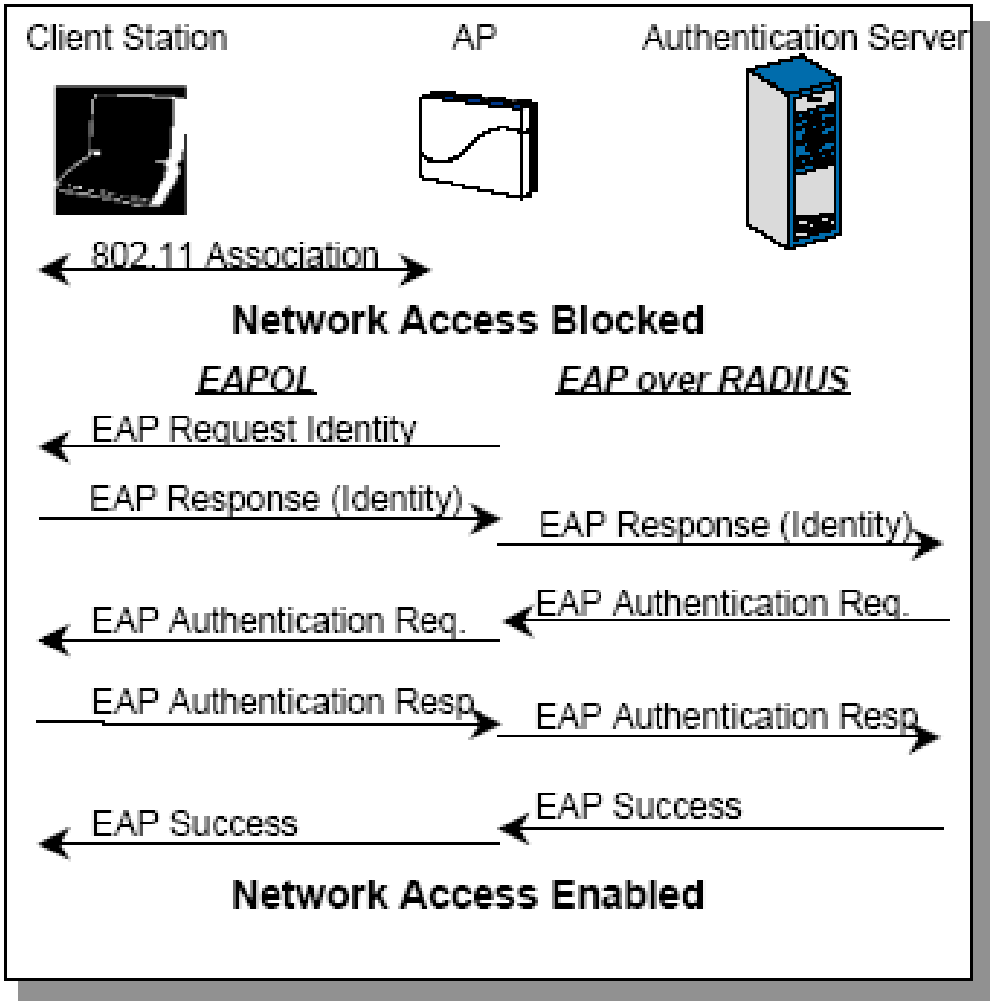




O AP transfer os dados das mensagens EAP sobre 802.1x para mensagens EAP sobre RADIUS e vice versa.

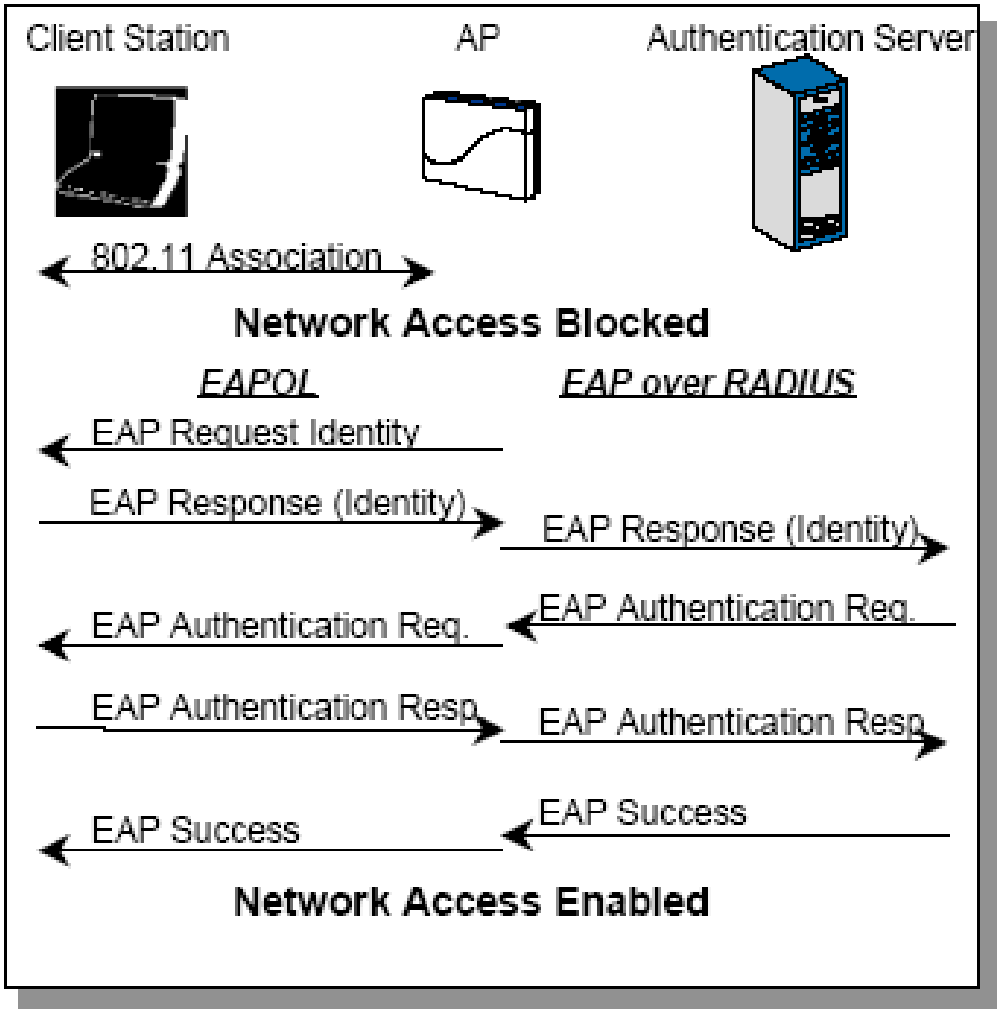
O AP bloqueia a ligação até a mensagem *access-accept* do RADIUS ser recebida.

EAP: Autenticação



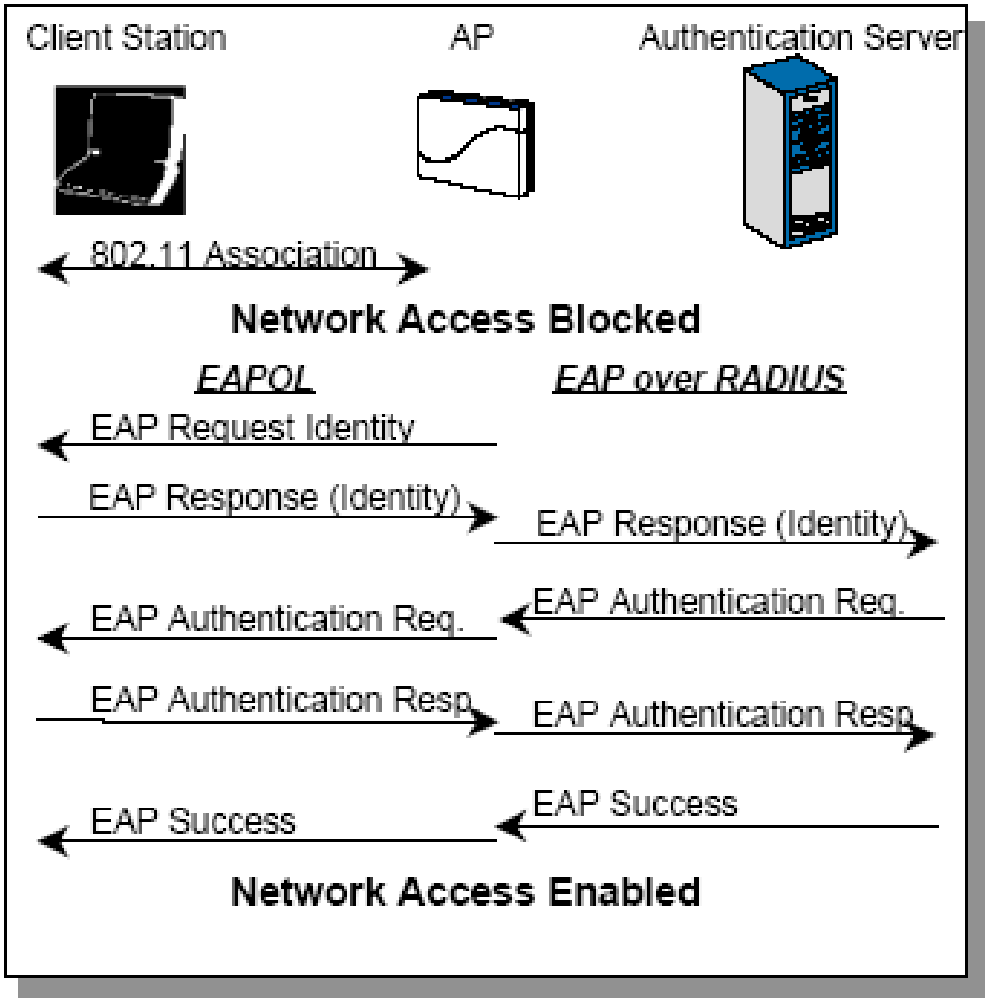
- A ligação física entre a estação cliente e a rede é estabelecida em primeiro lugar, o que para uma rede *wireless* significa que tem de ser terminada uma associação 802.11 (isto é equivalente a ligar-se uma estação Ethernet à tomada de um *switch*).

EAP: Autenticação



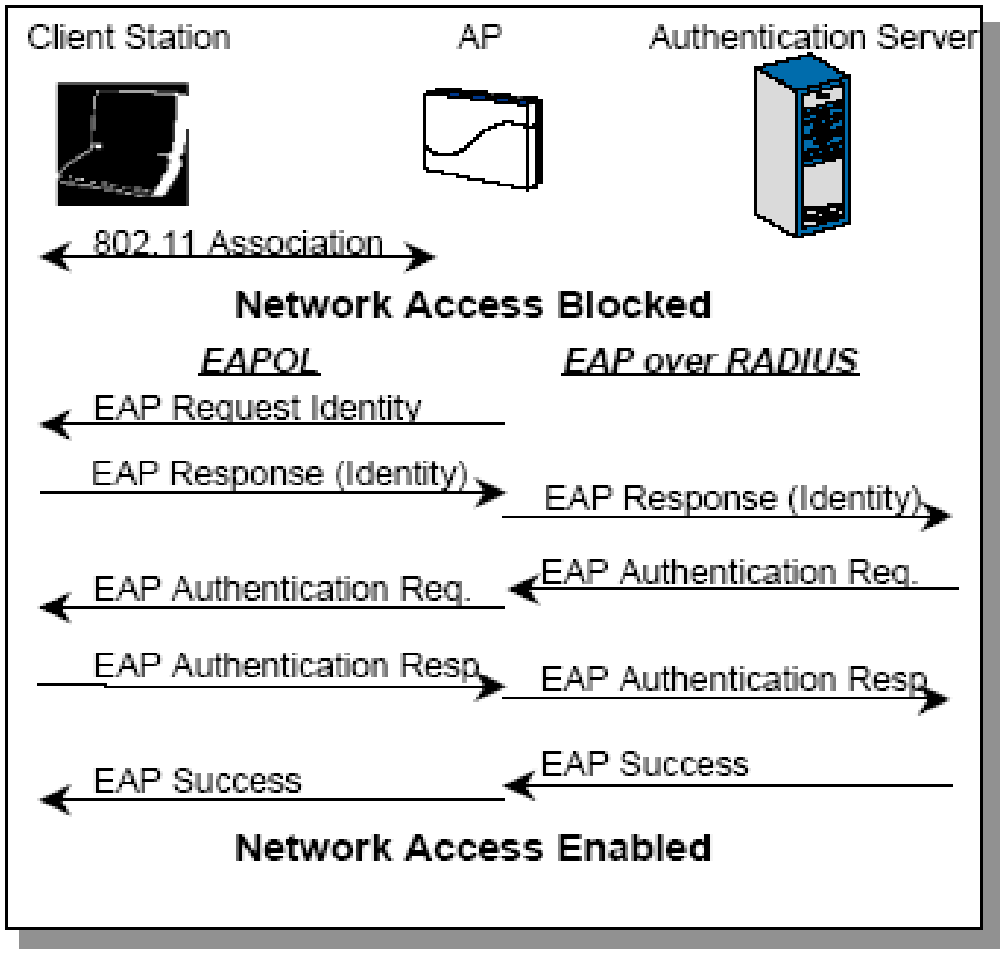
- Depois da associação 802.11 inicia-se a autenticação. Iniciada pelo Autenticador (i.e. o AP ou o *switch* (NAS)), o qual envia um Request EAP ao Suplicante (i.e. a estação cliente) perquntando pelas suas credenciais. Estas credenciais podem ser o nome da máquina ou do utilizador, dependendo do método de autenticação usado.

EAP: Autenticação



- O Suplicante transmite a informação sobre a sua identidade como parte da resposta EAP ao Autenticador, o qual retira o pacote da trama LAN e encapsula-a numa mensagem do protocolo RADIUS para ser transmitida para o Servidor de Autenticação.

EAP: Autenticação



Neste ponto dá-se uma sequência de trocas de mensagens entre o Servidor de Autenticação e o Suplicante (através do Autenticador), das quais os detalhes exactos dependem do método de autenticação usado. O resultado final da sequência completa será ou um resultado positivo, onde o Suplicante será autenticado positivamente, ou negativo onde a autenticação falhou. No primeiro caso a "porta" para a rede é aberta e todos os recursos da rede ficam disponíveis ao dispositivo cliente, enquanto que no segundo caso o acesso à rede continurá bloqueado.

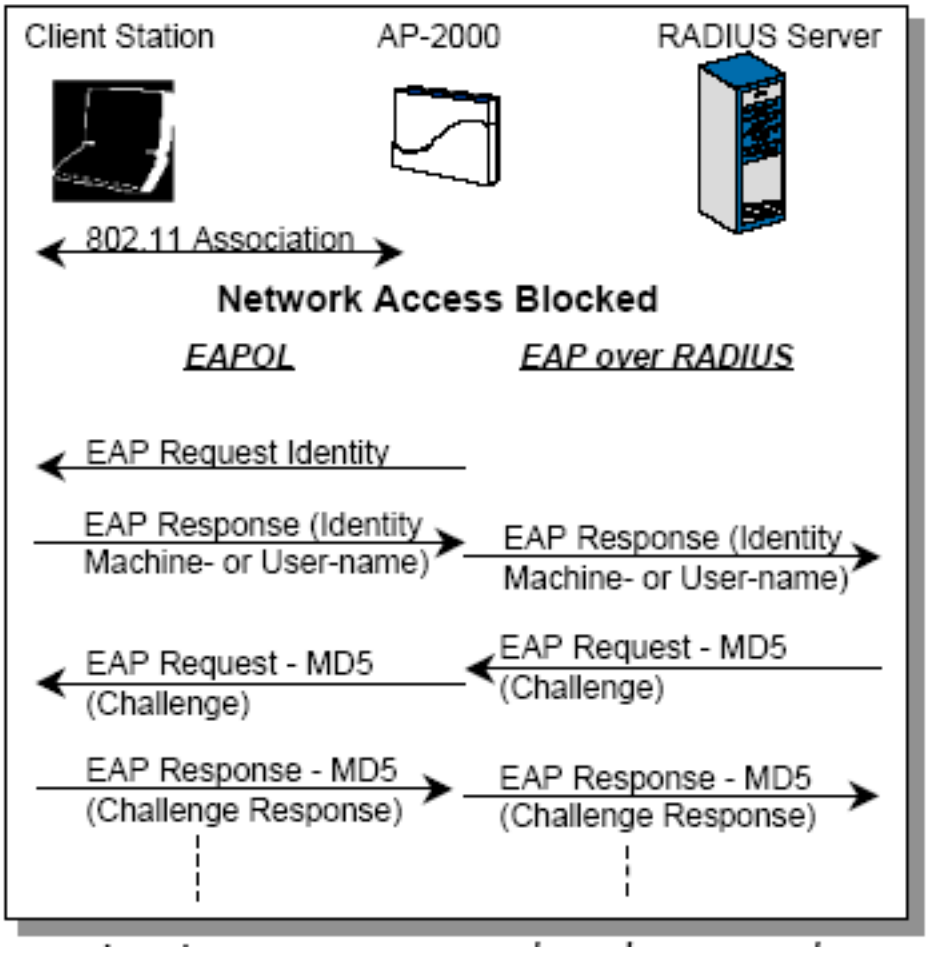
EAP: Métodos de autenticação – MD5

- O EAP – MD5 (*Message Digest* 5) usa o mesmo protocolo "*challenge handshake*" que o CHAP utilizado no PPP, mas os desafios e as respostas são enviados como mensagens EAP.
  - O MD5 pode ser considerado como o "menor denominador comum" dos tipos de autenticação EAP (o mais fraco dos algoritmos comuns a várias implementações).
  - O EAP - MD5 não suporta chaves WEP por sessão nem autenticação mútua do AP e do Cliente.
  - Também não suporta ligações cifradas dos dados do utilizador, desta forma não pode ser utilizada em ambientes 802.11i.

Métodos de autenticação EAP – MD5

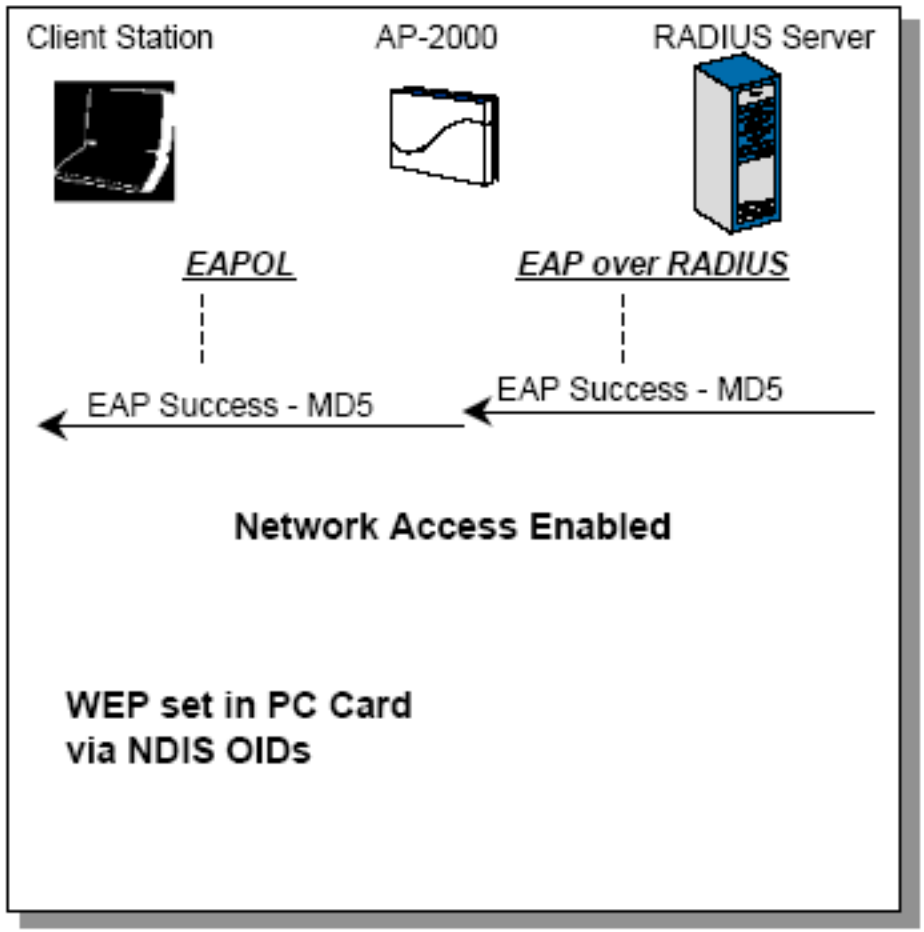
- Este algoritmo pode ser utilizado em aplicações *wireless* com requisitos de segurança menos exigentes.
  - A vantagem de usar EAP-MD5 é que é simples de administrar por um operador, reusando uma base de dados de utilizadores e *passwords* que exista.
  - A desvantagem de usar o EAP-MD5 em aplicações WLAN é não serem geradas chaves de cifra. Embora o protocolo também possa ser utilizado pelo cliente para autenticar a rede é tipicamente utilizado apenas pela rede para autenticar o cliente.

Métodos de autenticação EAP – MD5



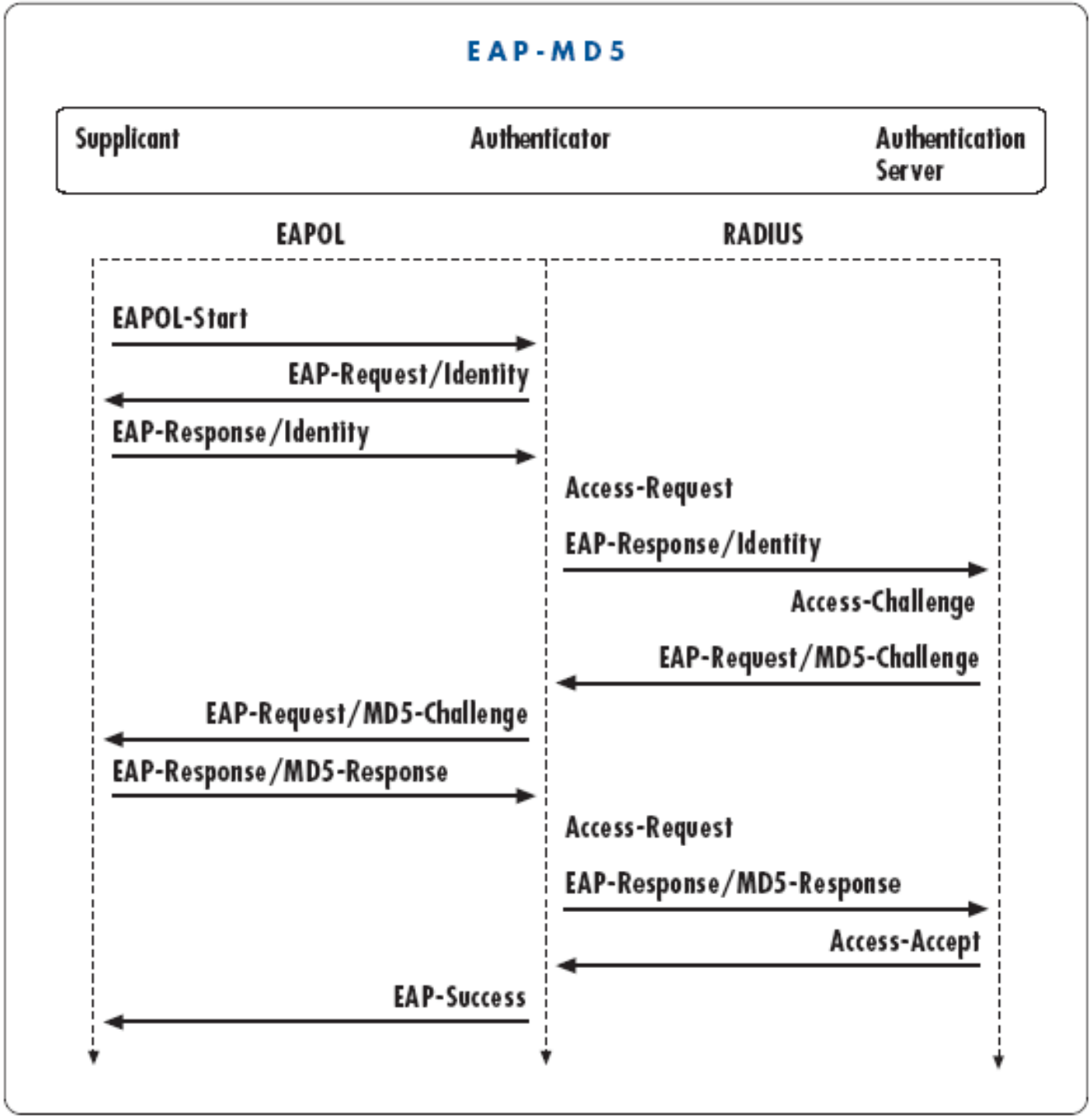
- Uma estação *wireless* associa-se ao seu AP.
- O AP envia uma trama *EAP Request Identity* para a estação cliente
- A estação cliente responde com a sua identidade (nome da máquina ou do utilizador).
- O AP retransmite a mensagem EAP (i.e. a identidade da estação cliente) para o servidor RADIUS, para este dar inicio aos serviços de autenticação.
- O protocolo MD5 responde com um texto de desafio enviado pelo servidor ao cliente.
- O cliente calcula o *hash* do texto de desafio utilizando a *password* do cliente e devolve o resultado.

Métodos de autenticação EAP – MD5



- O servidor compara o resultado utilizando a *password* que está gravada para aquele utilizador.
- Se o resultado for igual ao original o cliente é validado como genuíno.
- Não são geradas chaves de cifra.

EAP – MD5


EAP-MD5
Supplicant
Authenticator
Authentication Server
EAPOL
RADIUS
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
Access-Request
EAP-Response/Identity
Access-Challenge
EAP-Request/MD5-Challenge
EAP-Request/MD5-Challenge
EAP-Response/MD5-Response
Access-Request
EAP-Response/MD5-Response
Access-Accept
EAP-Success

EAP– TLS: Métodos de autenticação

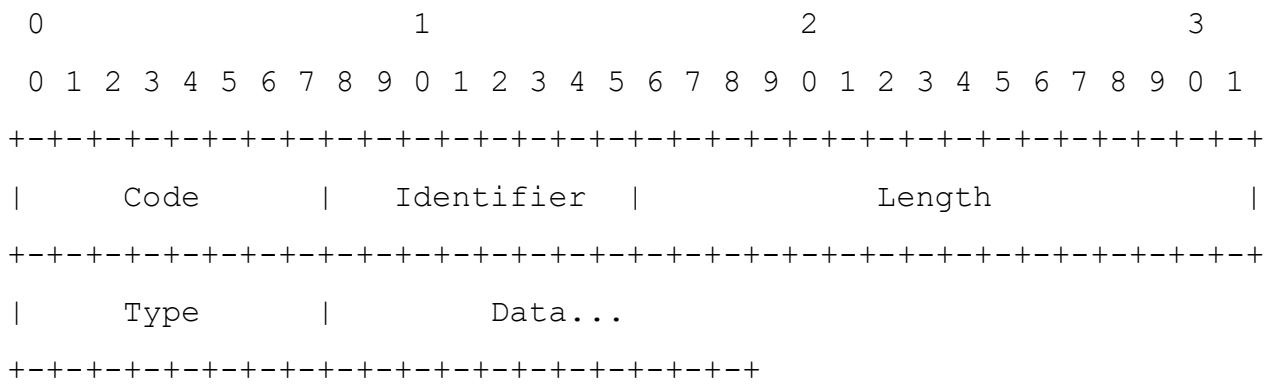
- O "*Transport Layer Security*" (TLS) é um protocolo de autenticação baseado em certificados. O RFC 2716 providencia autenticação mútua do cliente e da rede e suporta chaves WEP por sessão.

- É utilizado uma infraestrutura de chave pública (*Public Key Infrastructure* (PKI)) para dar suporte à autenticação para provar a identidade mútua.

EAP– TLS: Métodos de autenticação

- Um certificado digital inclui os seguintes campos:
  - Versão
  - Número de série do certificado
  - Identificador do algoritmo da assinatura
  - Nome do emissor
  - Período de validade
  - Nome
  - Chave pública
  - Identificadores únicos opcionais
  - Valor da assinatura.

EAP – TLS: Formato do pacote



Code

1 - Request

2 - Response

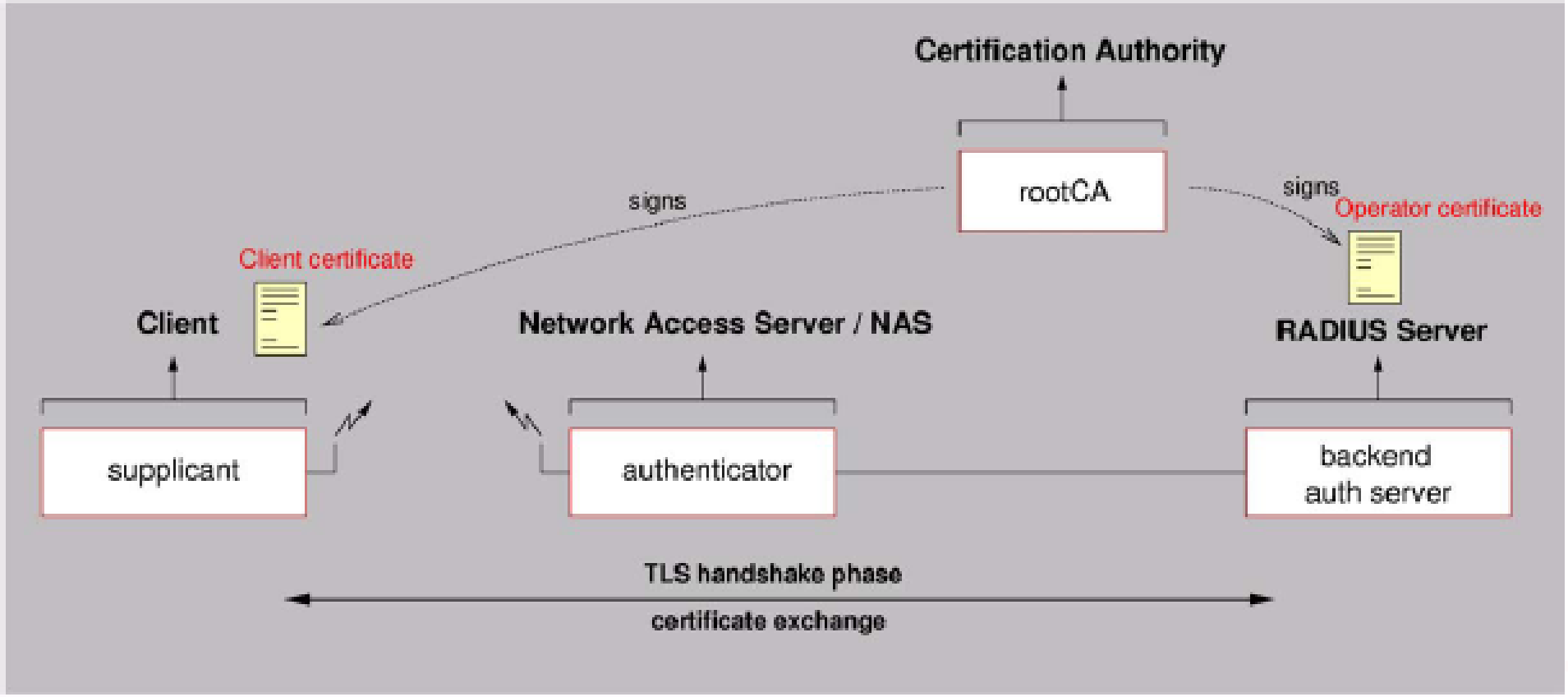
Identifier – Este campo ajuda a relacionar as respostas com os pedidos.

Length - Comprimento do pacote todo

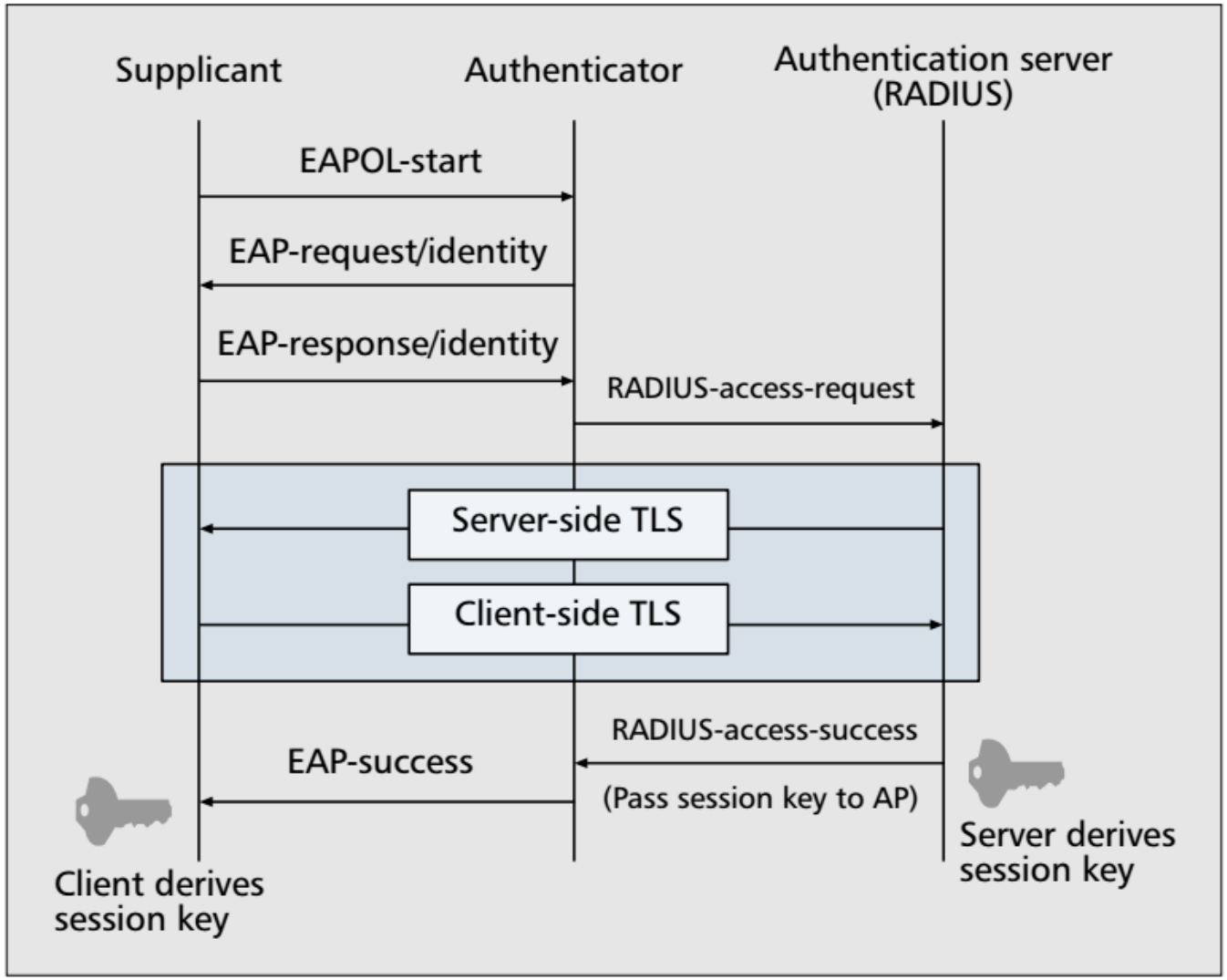
Type

13 – EAP-TLS

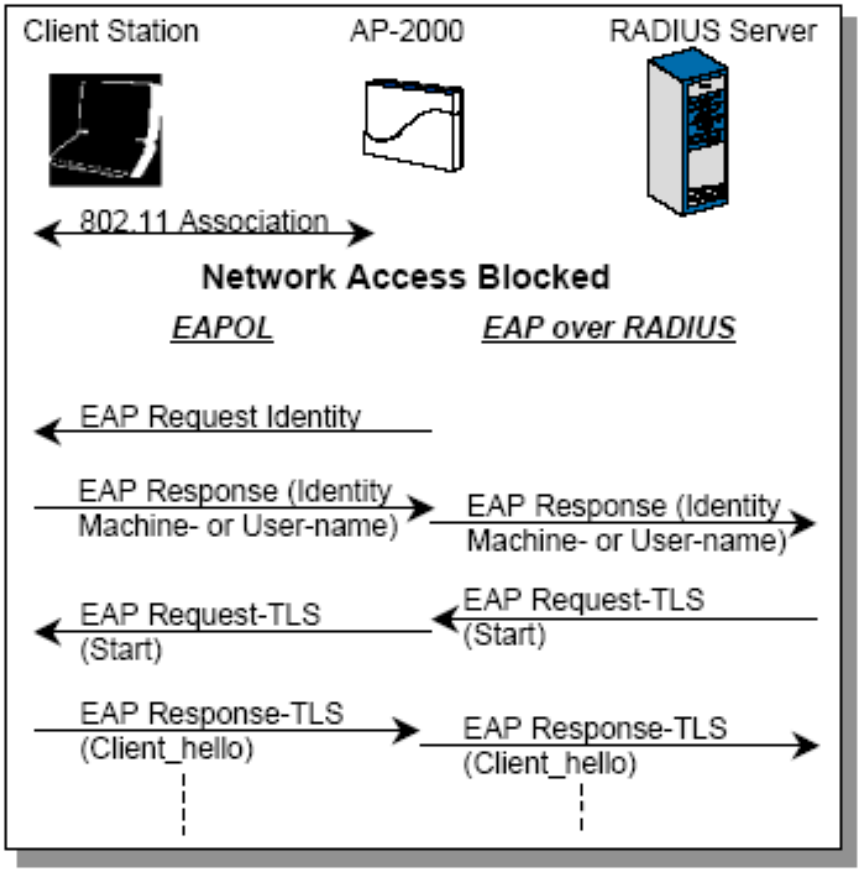
Autoridade de certificação



Fluxo de mensagens de EAP-TLS

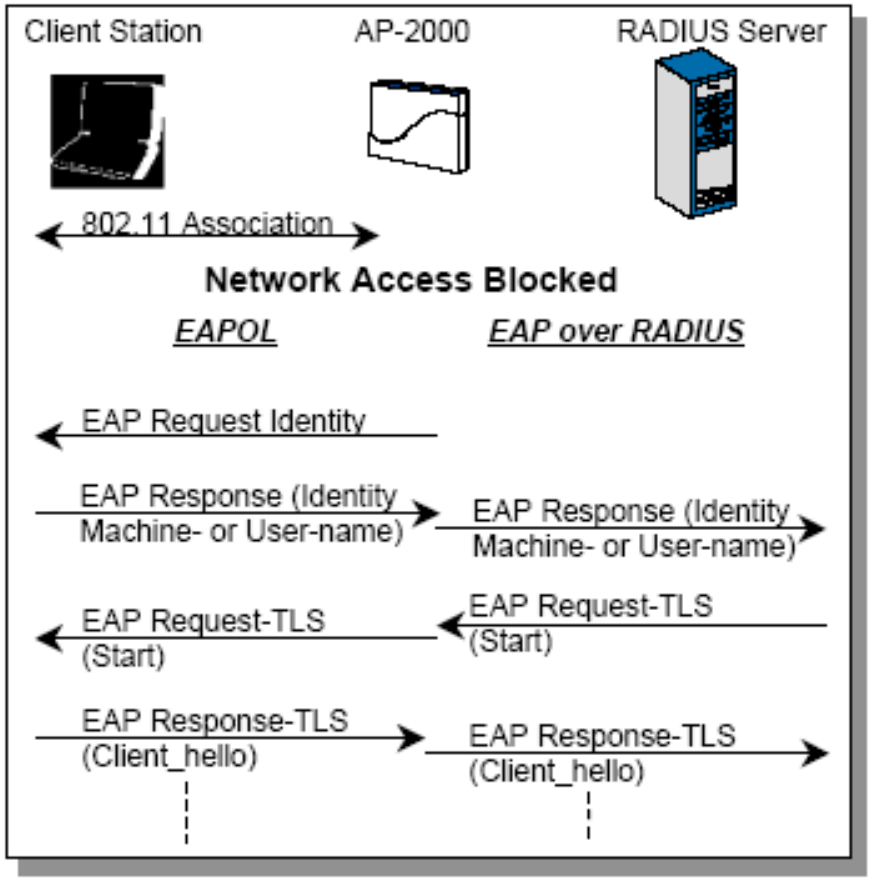


EAP – TLS: Métodos de autenticação



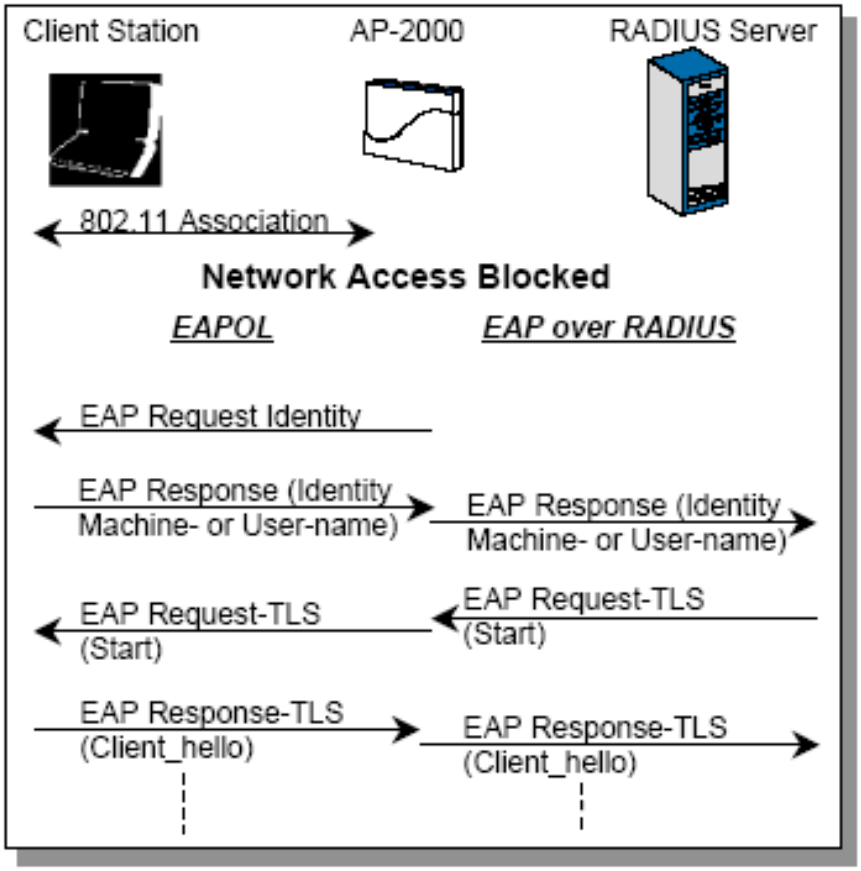
- Uma estação sem fios associa-se ao seu AP.
- O AP envia uma mensagem *EAP Request* a pedir a identidade à estação cliente.

EAP – TLS: Métodos de autenticação



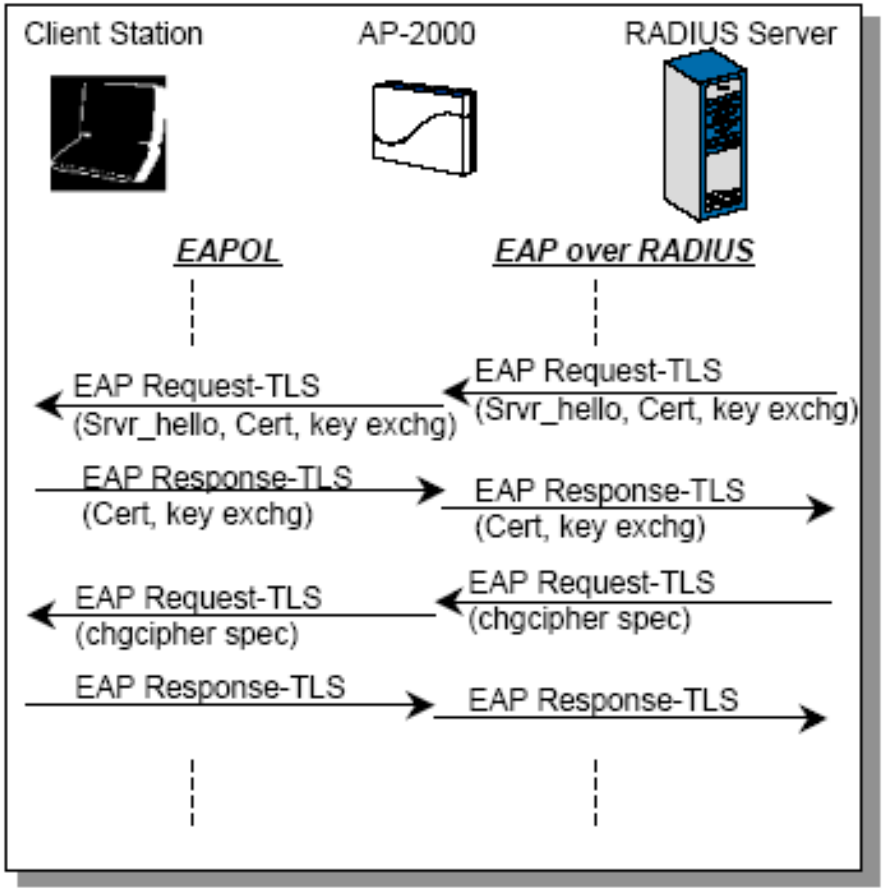
- A estação cliente responde com a sua identidade (nome da máquina ou do utilizador)
- O AP reenvia a mensagem EAP (i.e. identidade da estação cliente) para o servidor RADIUS, para dar inicio aos serviços de autenticação.

EAP – TLS: Métodos de autenticação



- O servidor RADIUS pede as credenciais à estação cliente para confirmar a identidade, enviando um pedido EAP via AP.
- O cliente responde enviando as suas credenciais através do AP.

EAP – TLS: Métodos de autenticação

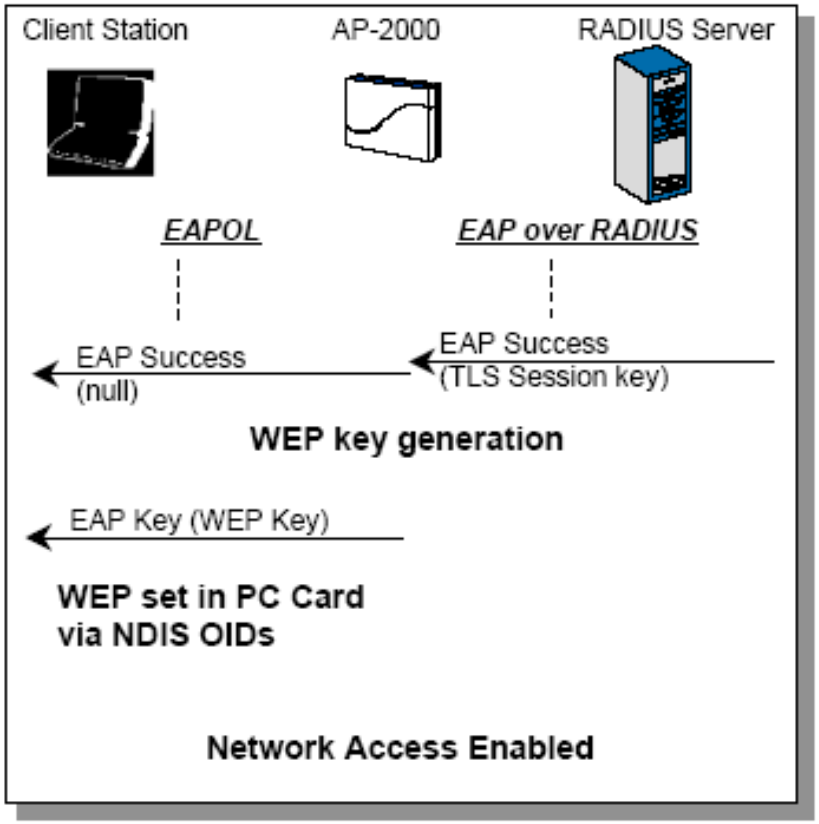


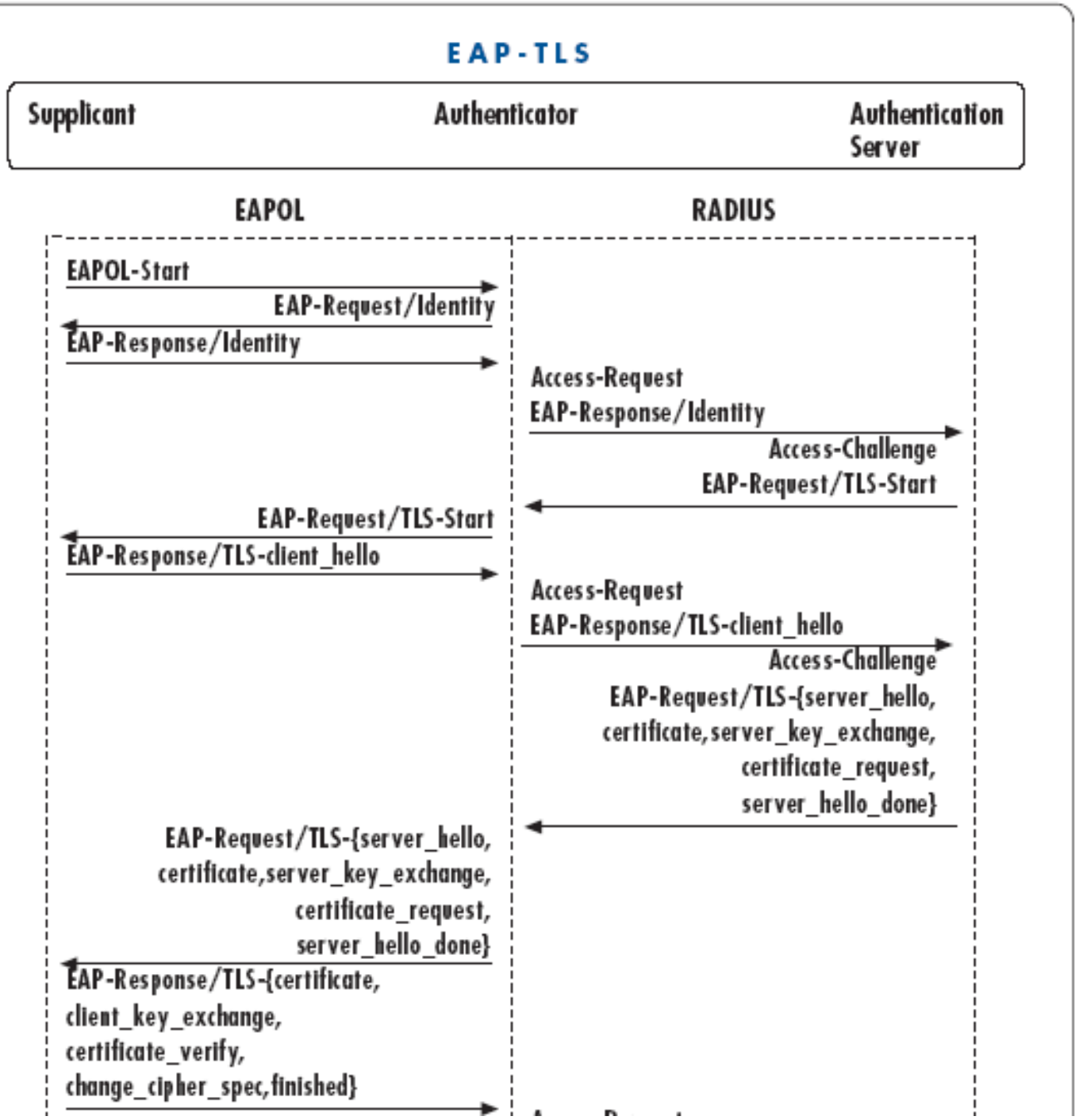
- A mensagem "TLS_Hello" é o inicio do "*handshake*" do protocolo TLS:
  - O servidor começa por enviar o seu Server_hello (incluindo o Certificado, indicando que tipo de algoritmo de cifra pode utilizar).
  - O cliente responde com um Client_Hello, indicando, entre outros, o seu certificado e qual o algoritmo de cifra que foi seleccionado.
  - O cliente e o servidor dão inicio à sequência de troca de chaves ("*Key-Exchange*") (Diffie-Hellman).

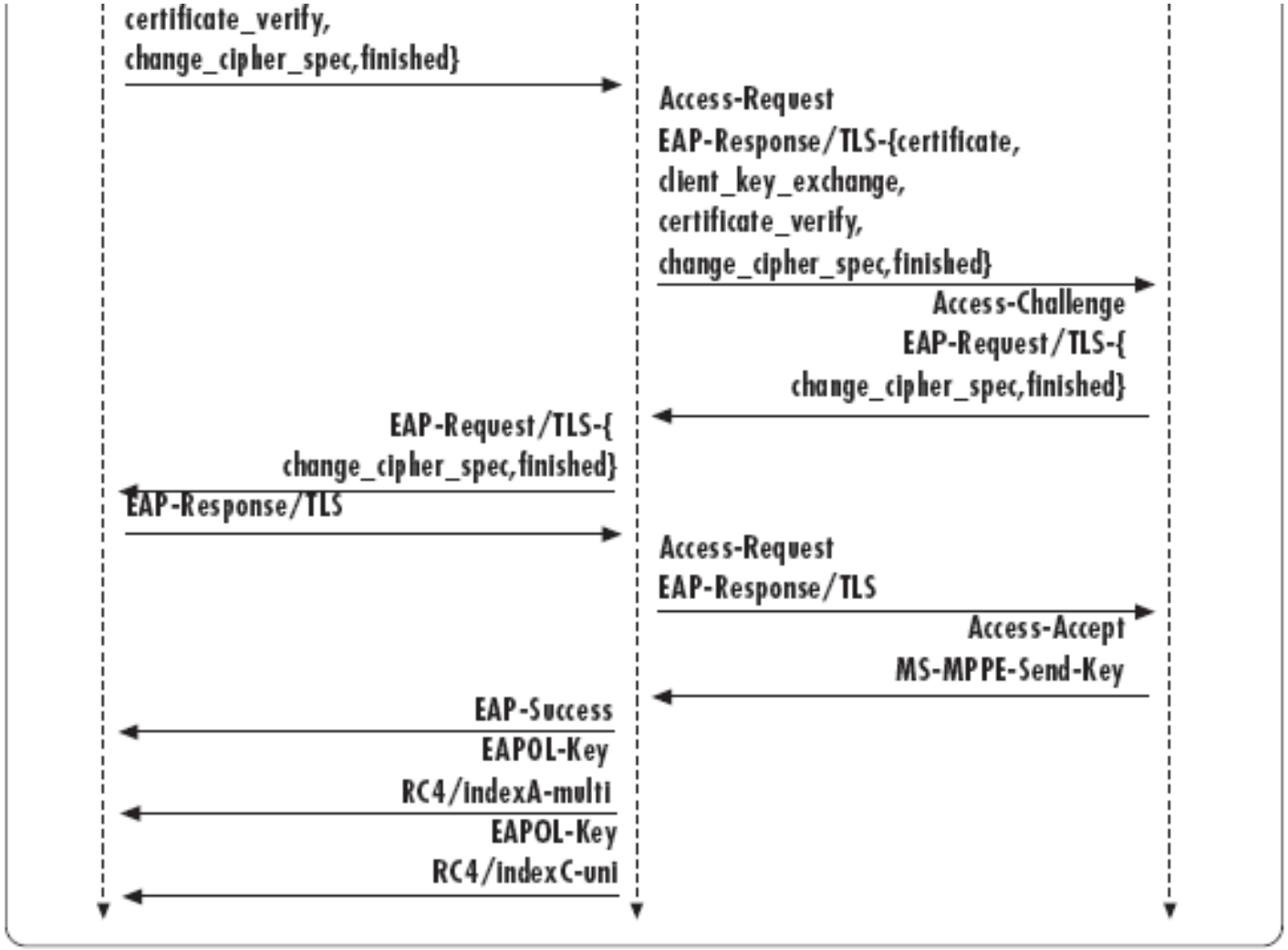
EAP – TLS: Métodos de autenticação

- No fim da troca de chaves DH entre o cliente e servidor, o servidor transmite as suas chaves ao AP.
- Para cifrar as trocas de tramas seguintes entre o AP e o cliente é utilizado um par de chaves, que é gerado pelo AP, e é o mesmo para todos os clientes associados a este AP em particular.
- O AP transmite este par ao cliente e utiliza a chave recebida do servidor para cifrar esta mensagem.
- Quando o cliente recebe as chaves WEP passa-as para a interface de rede via interfaces NDIS e o *driver*.
- A estação e o AP usam estas chaves WEP até a estação se desligar ou até o *timer* de reautenticação expirar.
- Quando uma estação se associa a outro AP é requerido uma reautenticação e são estabelecidas novas chaves WEP.

EAP – TLS: Métodos de autenticação




EAP-TLS
Supplicant
Authenticator
Authentication Server
EAPOL
RADIUS
EAPOL-Start
EAP-Request/Identity
EAP-Response/Identity
Access-Request
EAP-Response/Identity
Access-Challenge
EAP-Request/TLS-Start
EAP-Request/TLS-Start
EAP-Response/TLS-client_hello
Access-Request
EAP-Response/TLS-client_hello
Access-Challenge
EAP-Request/TLS-{server_hello, certificate,server_key_exchange, certificate_request, server_hello_done}
EAP-Request/TLS-{server_hello, certificate,server_key_exchange, certificate_request, server_hello_done}
EAP-Response/TLS-{certificate, client_key_exchange, certificate_verify, change_cipher_spec,finished}


certificate_verify,
change_cipher_spec,finished}
Access-Request
EAP-Response/TLS-{certificate,
client_key_exchange,
certificate_verify,
change_cipher_spec,finished}
Access-Challenge
EAP-Request/TLS-{
change_cipher_spec,finished}
EAP-Request/TLS-{
change_cipher_spec,finished}
EAP-Response/TLS
Access-Request
EAP-Response/TLS
Access-Accept
MS-MPPE-Send-Key
EAP-Success
EAPOL-Key
RC4/indexA-multi
EAPOL-Key
RC4/indexC-uni

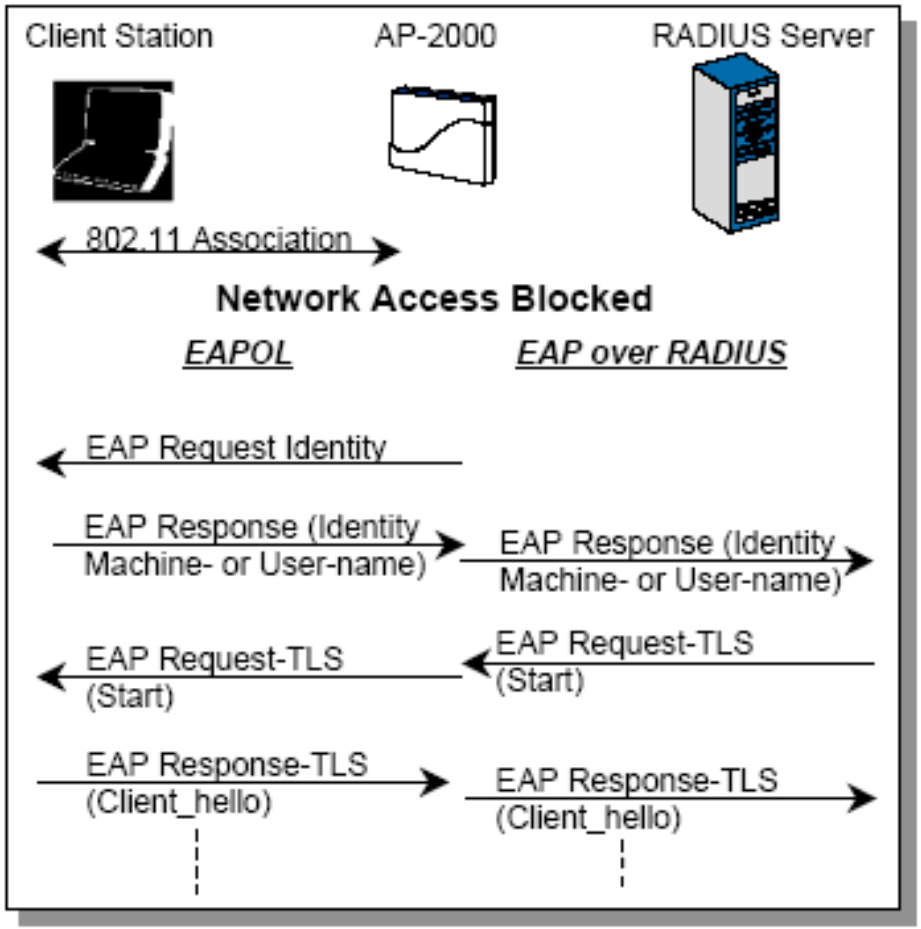
EAP– TTLS: Métodos de autenticação

- *O* ***Tunneled Transport Layer Security*** **(TTLS)** e o ***Protected Extensible Authentication Protocol*** **(PEAP)** são semelhantes no modo de funcionar e ambos seguram o nome do utilizador/*password* e a autenticação mútua.
- O EAP-TTLS é uma combinação de ambos, EAP-TLS e métodos tradicionais baseados em *passwords* tal como o "*Challenge Handshake Authentication Protocol*" (CHAP) e o "*One Time Password*" (OTP). Do lado do cliente são necessárias apenas *passwords* em vez de certificados digitais, o que alivia o administrador de sistemas da gestão e distribuição dos certificados. Do lado do servidor é necessário um certificado.
- Não têm de ser instalados certificados em cada dispositivo cliente. Isto porque são utilizadas técnicas PKI para permitir que o cliente autentique o servidor (através dum certificado instalado no servidor) e formar uma ligação segura entre o cliente e o servidor. Então o servidor autentica o cliente através da ligação segura com o utilizador a fornecer o par: Nome e *password*.
- Este principio é muito parecido com o utilizado nos *browsers* no comércio electrónico. As ligações seguras são estabelecidas antes da informação de autenticação dos utilizadores ser trocada.

EAP– TTLS: Métodos de autenticação

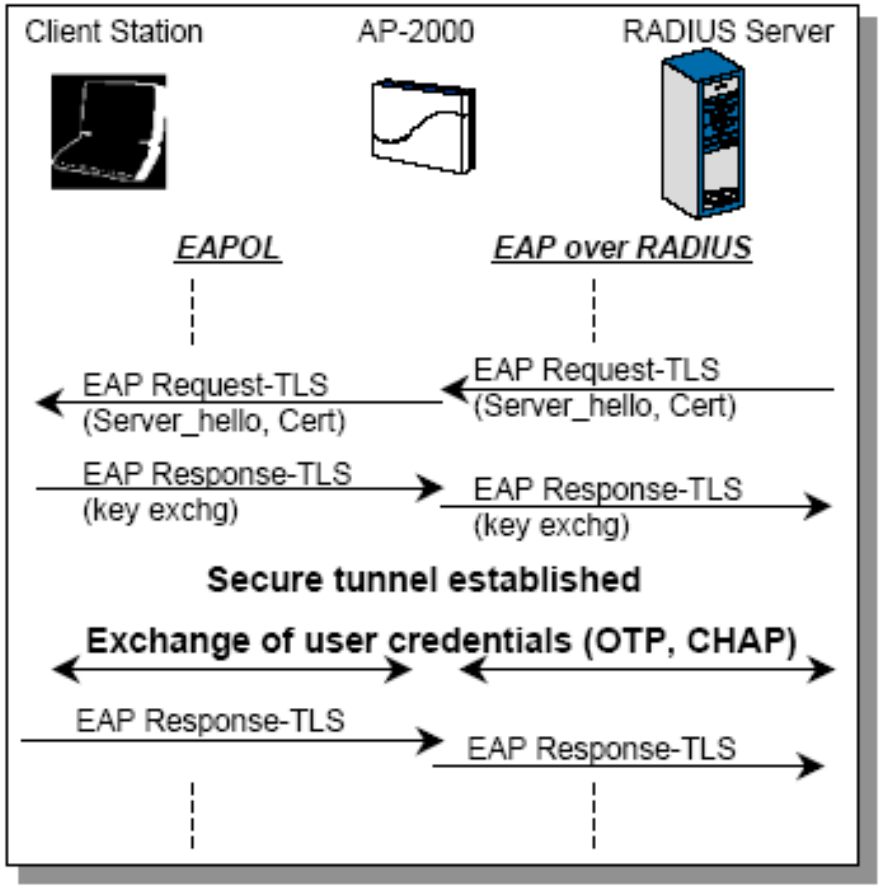
- No EAP-TTLS é estabelecido primeiro um túnel TLS entre o Suplicante e o servidor de autenticação.
- O cliente autentica a rede à qual se está a ligar utilizando o certificado digital fornecido pelo servidor de autenticação. Isto é exactamente o mesmo que as técnicas utilizadas para segurar as ligações dos servidores Web. Uma vez estabelecido um túnel autenticado ocorre a autenticação do utilizador.
- O EAP-TTLS tem o beneficio adicional de proteger a identidade do utilizador final de olhares indiscretos no meio *wireless*.
- O EAP-TTLS também permite que um sistema de autenticação dum utilizador final seja reutilizado.
- O EAP-TTLS é o único tipo de EAP que fornece anonimato ao utilizador final (o túnel já está estabelecido quando a autenticação do cliente é efectuada).

EAP– TTLS: Métodos de autenticação



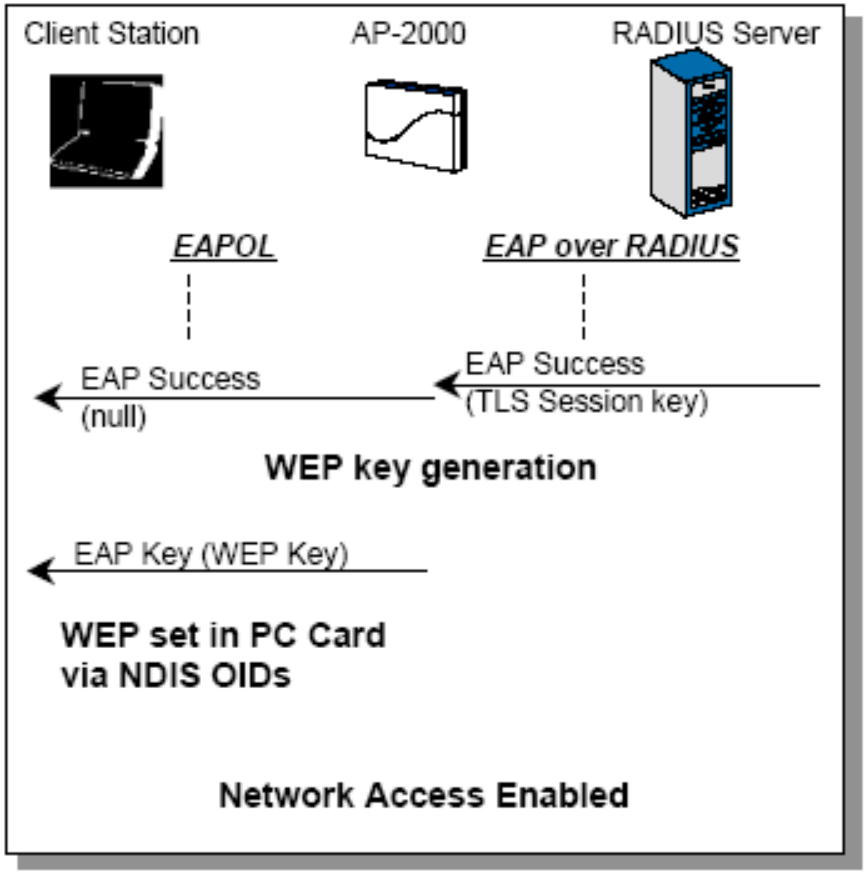
- Uma estação WLAN associa-se ao um AP
- O AP emite uma trama EAP Request Identity para a estação cliente.
- A estação cliente responde com a sua identidade.
- O AP reenvia a mensagem EAP (identidade do cliente) para o servidor RADIUS. Para dar inicio aos serviços de autenticação.
- O protocolo de autenticação entre o servidor RADIUS e a estação cliente é TLS e permite ao cliente autenticar o servidor.

EAP– TTLS: Métodos de autenticação



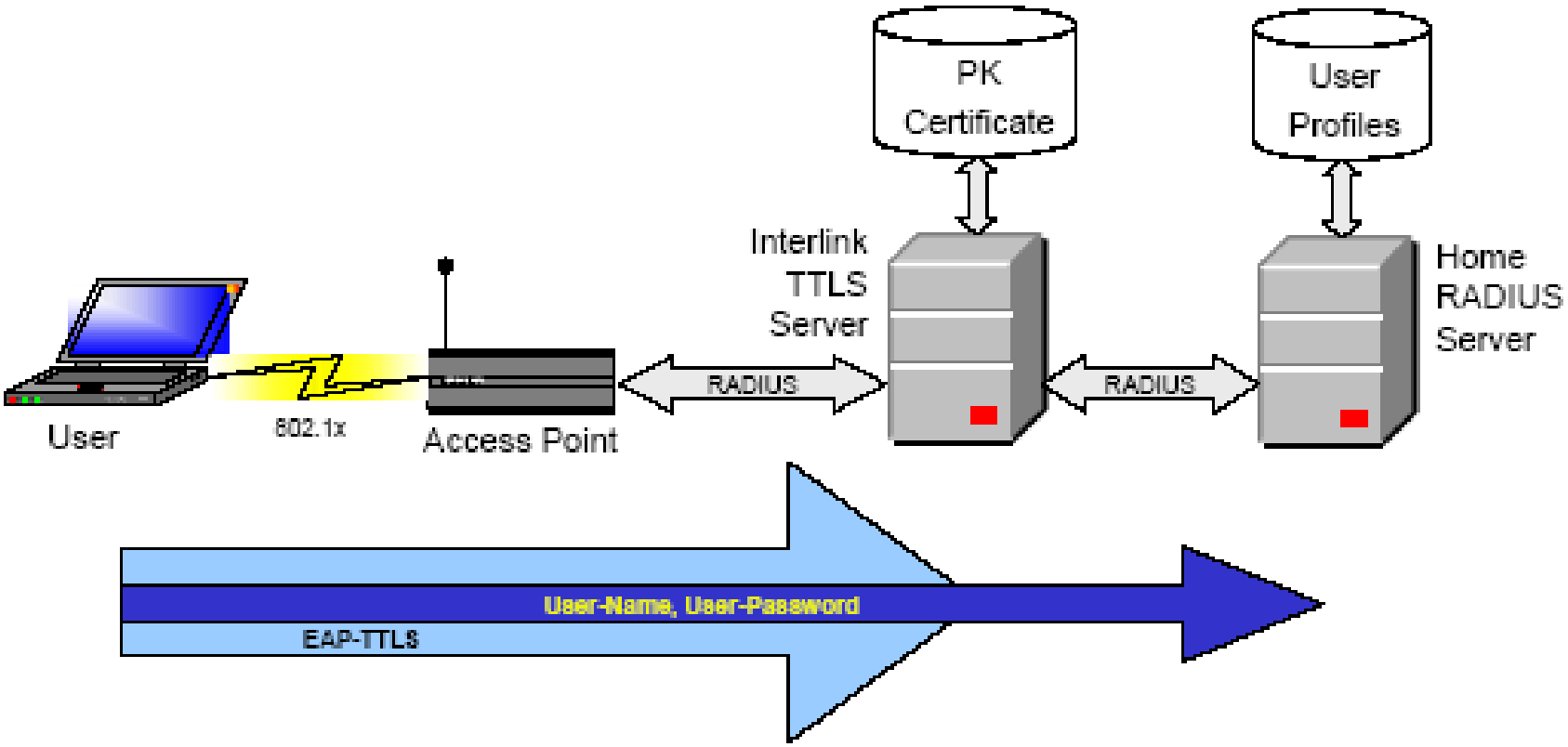
- A mensagem “TLS_Hello” é o inicio do protocolo de hand-shake do TLS:
  - O servidor começa por enviar o seu Server_hello (incluindo o certificado e indicando qual o algoritmo de cifra que pretende utilizar)
  - O cliente responde enviando o seu ack para o protocolo de cifra (não envia certificados)
  - O cliente e o servidor iniciam a sequência de troca de chave (Diffie-Hellman).
  - Agora o túnel está estabelecido e seguro, as restantes credenciais do utilizador são trocadas (usando OTP ou CHAP).

EAP– TTLS: Métodos de autenticação



- Para terminar a troca entre o servidor e o cliente o servidor transmite as suas chaves para o AP.
- Para cifrar as tramas IEEE 802.11 entre o AP e o cliente é utilizado um par de chaves que são geradas pelo AP e que são as mesmas para todos os clientes que usam este AP.
- O AP transmite este par de chaves para o cliente e usa a chave recebida do servidor para cifrar esta mensagem.
- Uma vez recebidas as chaves WEP pelo cliente, serão passadas à interface de rede via NDIS e o *driver*. A estação e o AP usarão estas chaves WEP até a estação se desligar ou o *timer* de autenticação expirar.

EAP– TTLS: Métodos de autenticação



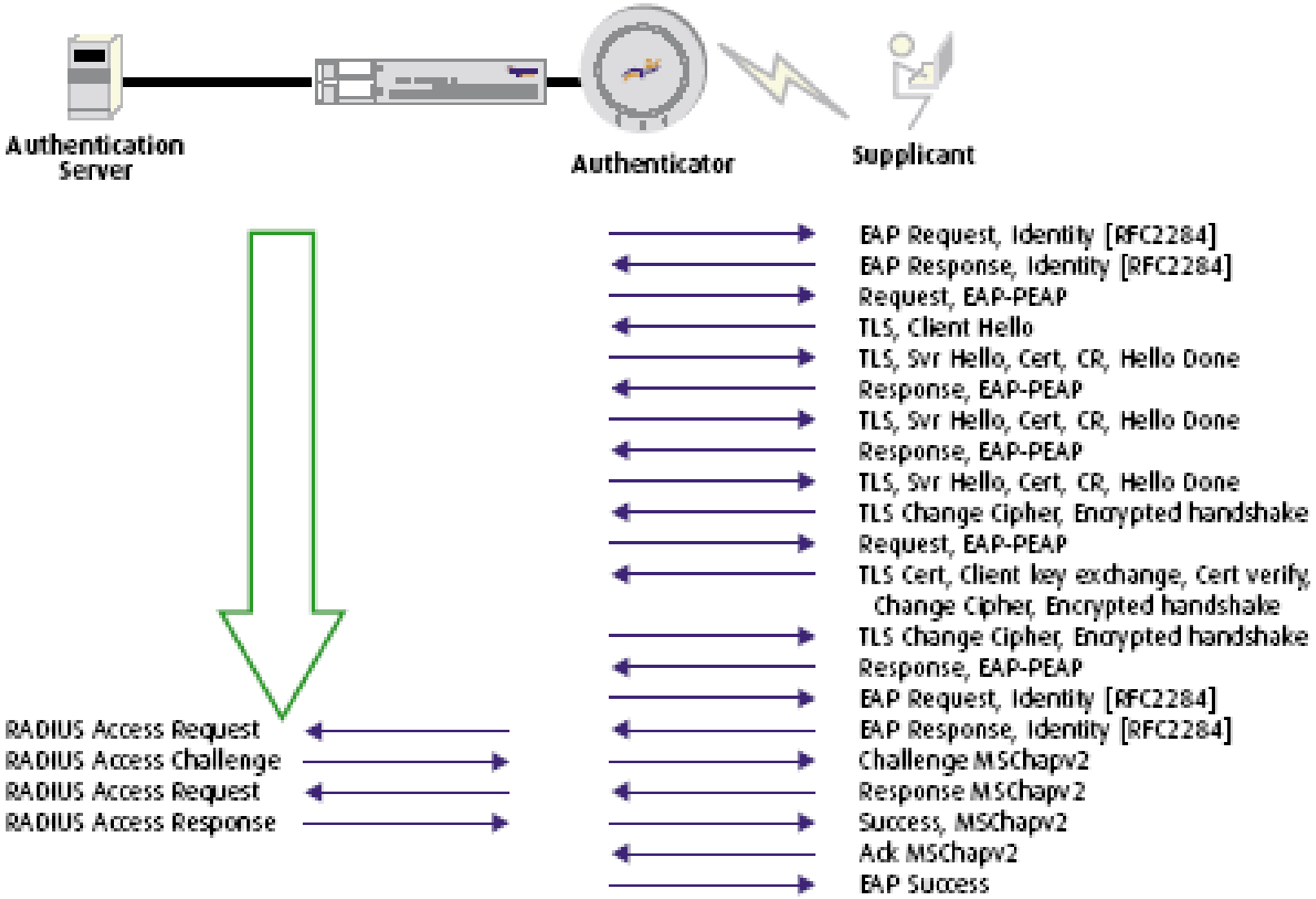
EAP – PEAP: Métodos de autenticação

- **Protected EAP (PEAP):** Versão do EAP desenvolvida pela Microsoft, Cisco e RSA Security que oferece duas opções de implementação:
  - A primeira utiliza o **Microsoft Challenge-Handshake Authentication Protocol Version 2 (MS-CHAPv2)** para autenticação mútua e não requer certificados digitais nos clientes.
  - A segunda implementação usa TLS para autenticação mútua e requer certificados digitais em todos os clientes (muito semelhante ao EAP-TLS).

PEAP com MS-CHAPv2

- O processo de autenticação do PEAP ocorre em duas partes.
- A primeira parte é o uso do EAP do tipo EAP-PEAP para criar um canal TLS cifrado.
- A segunda parte consiste no uso do EAP e de um tipo EAP diferente para autenticar o acesso à rede.
- O que se segue examina a operação do PEAP com MS-CHAPv2 usando como exemplo um cliente *wireless* que tenta autenticar-se num *Access Point* (AP) *wireless* que usa um servidor RADIUS para autenticação e autorização.

EAP– PEAP: Métodos de autenticação



Métodos de autenticação EAP– PEAP

Cliente

EAP-Request / Identity

EAP- Response / Identity [My Domain]

EAP-Request (Type = PEAP, start)

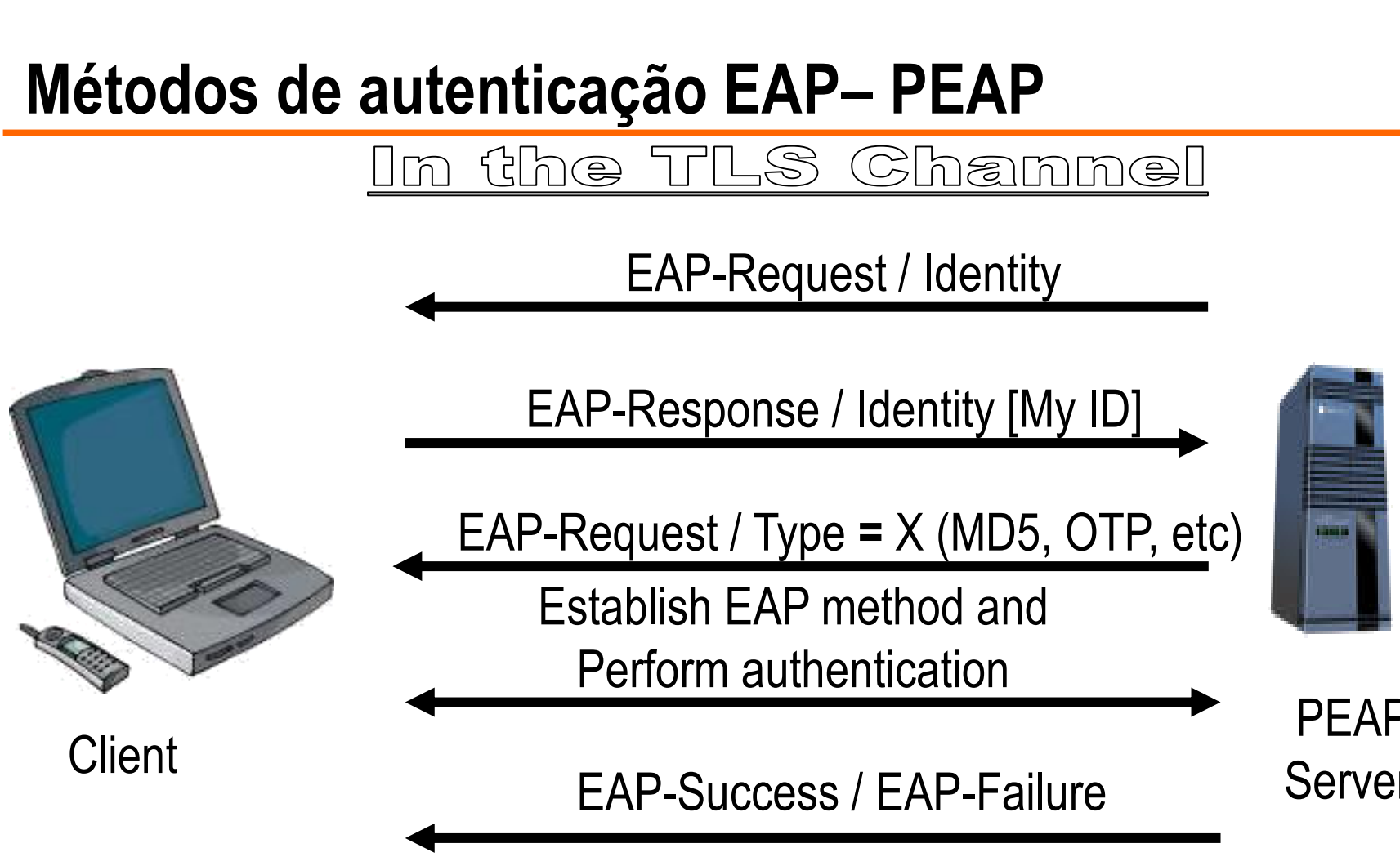
TLS Handshake

TLS Channel Established

EAP- Response (empty)

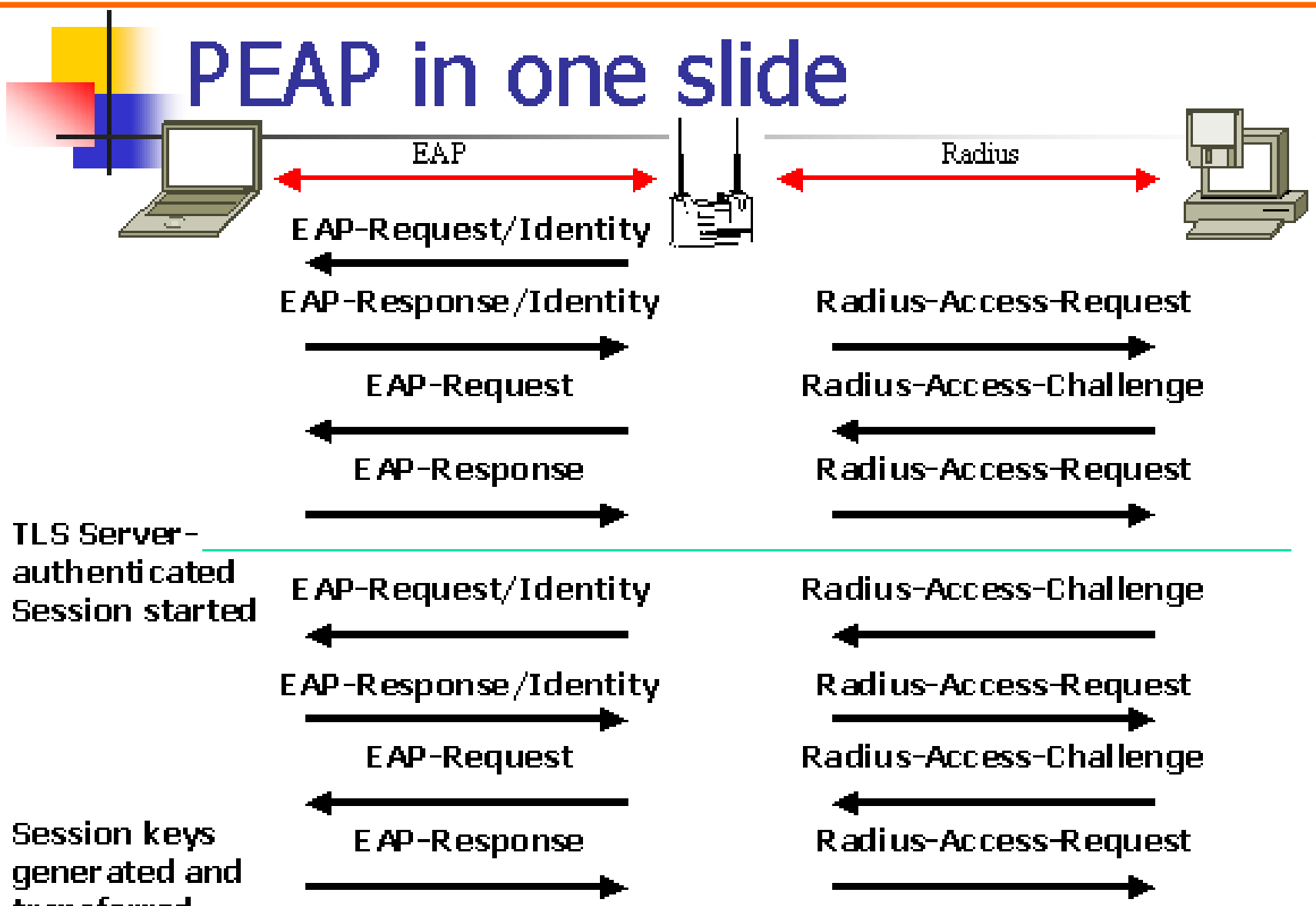
Servidor PEAP

Métodos de autenticação EAP– PEAP

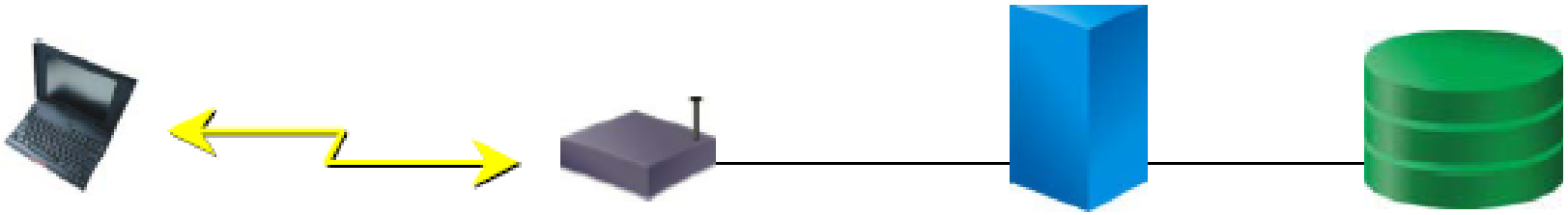


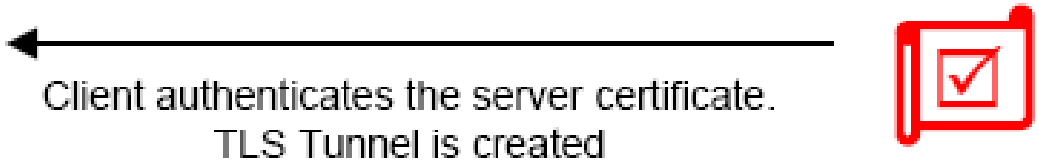
Transferência da chave gerada do servidor PEAP para o NAS se forem máquinas diferentes

Métodos de autenticação EAP– PEAP



Métodos de autenticação EAP– PEAP





PHASE 1

Client authenticates the server certificate.
TLS Tunnel is created

PHASE 2

User Authentication credentials are sent through TLS Tunnel Again using EAP.

RADIUS Server authenticates to user repository.

Client gets network access

AP Gets Encryption Keys