# Capítulo 7 – Segurança em Redes IEEE 802.11

As redes sem fios, em particular as redes 802.11, também conhecidas como redes WLAN (*Wireless Local Area Network*) ou redes Wi-fi são inegavelmente cómodas para suportar a comunicação de dados em diversos cenários operacionais.
Os problemas de segurança colocados pelas redes sem fios são:

- A autenticação entre um equipamento Móvel (STA – *Station*) e as redes sem fios a que acede.
- O controlo de acesso de um STA a uma rede sem fios.
- A confidencialidade das mensagens trocadas via rádio.
- A autenticidade, ou controlo de integridade, das mensagens recebidas.

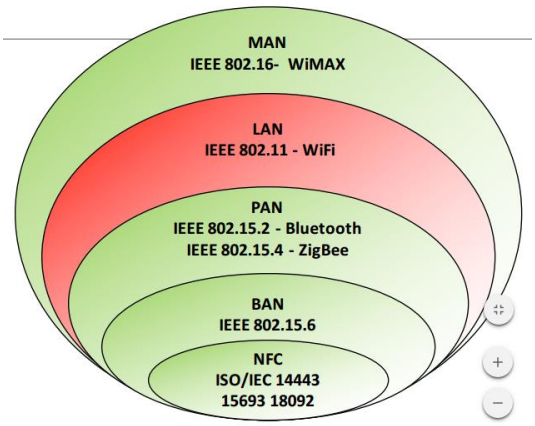



*Figura 1 - Comunicações sem Fios*

## 7.1. Cabladas vs Sem Fios: Aspetos de Segurança

- Comunicação por *Broadcast*

Difícil aplicar limites físicos de propagação

Características físicas vulneráveis onde existe interferência nas comunicações e observação das comunicações.

- Mitigação

| Mecanismos para reduzir interferências e observação | |
|---|---|
| Nível Físico | Nível de Dados |
| - Impossibilitar atacantes de descodificar o canal onde a codificação necessita de usar um segredo partilhado e as condições de transmissão dependem deste segredo.<br><br>- Exemplo Bluetooth FHSS (Frequency Hoping Spread Spectrum):<br>♦ Emissor e recetor acordam num padrão de mudança de canal<br>♦ Dados são divididos em pacotes e transmitidos sobre 79 frequências | - Prevenir que atacantes identifiquem participantes da comunicação onde cifra sobre os cabeçalhos e criação de identificadores temporários.<br><br>- Prevenir que atacantes compreendam os dados transmitidos com cifra das tramas onde normalmente apenas é aplicada ao conteúdo e não aos cabeçalhos. |

| | |
|---|---|
| onde a frequência é alterada 1600 vezes por segundo e apenas dispositivos sincronizados com a mesma frequência terão acesso aos dados.<br>♦ FHSS é detetado pelos atacantes como pequenos impulsos de ruido<br>♦ Interferências numa frequência específica possuem impacto limitado. | - Prevenir que atacantes criem tramas de dados válidas, onde tramas têm de ser autenticadas com a autenticação da origem ou autenticação de grupo e a atualidade das tramas. |
| - Prevenir transmissores de monopolizarem o canal onde existem políticas de acesso ao meio físico.<br><br>- Exemplos:<br>♦ Bluetooth FHSS: transmissores que não estejam sincronizados raramente colidem.<br>♦ Wi-fi: Cada rede é instanciada sobre uma frequência especifica<br>♦ GSM: cada terminal móvel transmite sobre uma frequência determinada pela estação móvel.<br><br>A interferência ainda é possível ao emitir em múltiplos/todos os canais. | |

## 7.2. IEEE 802.11: Arquitetura (em redes estruturadas)

- Estação (STA – *Station*)
  Dispositivo que se liga a uma rede sem fios
  Possui um identificador (único) como o endereço Mac (Media Access Control Address)
- Access Point (AP)
  Dispositivo que serve de ponto de coordenação para os dispositivos de uma rede
  Pode fornecer ligação a uma rede cablada
- Rede Sem Fios (Wireless)
  Rede formada por um conjunto de STAs e APs que comunicam com sinais rádio

O padrão 802.11 permite duas arquiteturas de rede alternativas:

- ***Ad hoc***: Nesta arquitetura cada STA pode comunicar com outros segundo um modelo P2P. O conjunto de equipamentos que constitui cada rede *ad hoc* forma um BSS.

- ***Estruturada***: Nesta arquitetura os STA comunicam com as AP, que funcionam *switches*, apenas possuindo portas para comunicar com redes cabladas e antenas para comunicar com os STA.

## 7.3. IEEE 802.11: Terminologia de uma rede estruturada

. Basic Service Set (BSS)

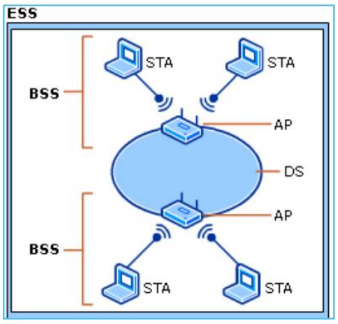
Rede formada por STAs associadas a um AP

- Extended Service Set (ESS)

Rede formada por várias BSS ligadas por um Sistema de distribuição (DS)

- Service Set ID (SSID)

Identificador de uma rede servida num BSS ou ESS. A mesma infraestrutura pode usar vários SSID.




## 7.4. IEEE 802.11: Máquina de Estados de Autenticação e Associação

Quando um STA se pretende ligar a uma rede sem fios, admitindo que já conhece o seu SSID, concretiza esse propósito em duas etapas: autenticação e associação. Na figura demonstra as mudanças de estados inerentes às etapas de autenticação e associação. Estes estados servem para condicionar os tipos de Tramas que o AP e o STA podem emitir e receber em cada instante e fornecem igualmente um contexto correto para a sua interpretação.

No estado 1 não se trocam ou interpretam tramas de associação, desassociação ou reassociação e apenas no estado 3 (autenticado e associado) se podem trocar tramas de dados.

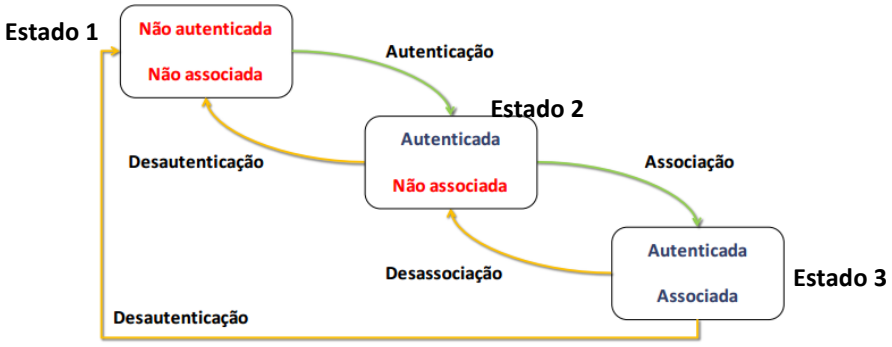



*Figura 2 - Máquina de Estados que relaciona as etapas de autenticação e associação*

| Autenticação | Associação |
|---|---|
| A autenticação é feita recorrendo a múltiplas trocas de tramas *Authentication Request/ Authentication Response*.<br>No processo de autenticação o AP pode pedir ao STA que prove pertencer a um determinado utente. Nesse processo o AP força o uso do protocolo de autenticação configurado para usar o mesmo. | A etapa de associação associa o STA a um AP, o que na prática significa que o AP reserva recursos para identificar o STA e para gerir a comunicação com o mesmo. A associação normalmente é realizada com a troca de tramas *Association Request / Association Response*. Na mesma é referido o SSID da rede sem fios a que se refere a associação, bem como inúmeros parâmetros operacionais.<br>Durante uma associação, bem como antes com tramas *Beacon, Probe Request e Probe Response*, o STA e o AP trocam um valor de 16 bits, designado por *Capability Information*, que informa o recetor acerca de certo tipo de capacidades operacionais do emissor. |

| Desautenticação | Desassociação |
|---|---|
| A desautenticação entre um STA e um AP pode ser comunicada por qualquer dos interlocutores através de uma trama *Deauthentication*. A desautenticação permite que ambos libertem recursos afetos ao estado de autenticado (estado 2), eventualmente constituído por chaves criptográficas partilhadas. A desautenticação ocorre no estado 3, provoca uma transição direta para o estado 1, o que implica uma desassociação automática. | A desassociação entre STA e um AP pode ser comunicada por qualquer dos interlocutores através de uma trama *Disassiciation*. A desassociação permite que o AP liberte recursos afetos à associação (estado 3) e que o STA esteja livre para se associar a qualquer outro AP. |
| **Reassociação** | |
| Um pedido de reassociação é feito com a troca de trama *Reassociation Request / Reassociation Response*, que diferem das anteriores por conterem na primeira, *Reassociation Request*, um identificador do AP a que antes o STA estava associado. | |

## 7.5. IEEE 802.11: Tipos de Tramas

Numa rede sem fios estruturada 802.11, a comunicação entre um STA e um AP é feita recorrendo a tramas de diversos tipos.

- Tramas de dados

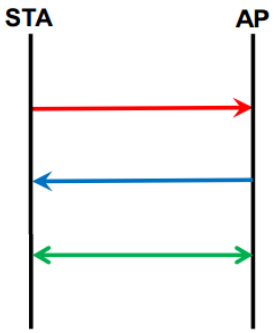
As tramas de dados servem para efetuar uma troca de dados útil, nomeadamente datagramas IP, entre o STA e o AP. Cada trama de dados transporta, como dados úteis, o que se designa como MPDU (MAC *Protocol Data Unit*), que pode ser um fragmento de algo maior, um MSDU (MAC *Service Data Unit*). A informação relativa à fragmentação de um MSDU em múltiplos MPDU, que é relevante para conduzir a desfragmentação, está presente no cabeçalho da trama.

- Tramas de Gestão

As tramas de gestão permitem que um STA e um AP negoceiem e mantenham uma ligação entre si. Este tipo de tramas inclui tramas de sinalização de uma rede (*beaconing*), verificação de existência de uma rede (*probing*), autenticação do STA e associação, reassociação ou desassociação do STA ao AP.

Estas tramas servem para fazer numa rede sem fios ações equivalentes a ligar e desligar um cabo entre um equipamento e um *switch* numa rede cablada. Um STA liga-se a uma rede sem fios através de uma associação a um AP dessa rede sem fios. De forma semelhante, desliga-se uma rede sem fios desassociando-se do AP ao qual está associado.

**Beacon**
**Probe Request & Response**
**Authentication Request & Response**
**Deauthentication**
**Association Request & Response**
**Reassociation Request & Response**
**Disassociation**



-Tramas de Controlo

As tramas de controlo servem para gerir a comunicação entre os STA e os AP. Estas tramas são usadas para gerir o acesso ao meio de comunicação e para evitar a ocorrência de colisões provocadas por comunicações simultâneas. Servem também para confirmar a correta receção de tramas, devido ao meio de comunicação ser tipicamente muito ruidoso.

- Request to Send (RTS)
- Clear to Send (CTR)
- Acknowledgment (ACK)

## 7.5. IEEE 802.11 Segurança do Nível de dados

Os problemas de segurança das redes WLAN, derivam do facto de ser complexo ou mesmo impossível limitar fisicamente o acesso de pessoas não autorizadas ao sinal de rádio usado nas redes WLAN ou aos AP que as suportam. Por outro lado, é igualmente complexo limitar fisicamente que numa dada área apenas existam os AP autorizados e não terceiros que tentem enganar os utentes dos STA.

Em suma, o confinamento físico de redes WLAN é complexo ou impossível de fazer de forma confiável.

Todas as tramas de dados e de gestão incluem um cabeçalho onde existe um bit – WEP bit no campo *Frame Control*, que indica se se está ou não cifrada para proteção da sua confidencialidade e para garantir a sai integridade, Logo, apenas é possível usar WEP nas tramas de dados e em algumas tramas *Authentication Request*.

| Tipo de Rede / Funcionalidade | | pré-RSN | RSN (Robust Security Network) | |
|---|---|---|---|---|
| | | WEP | WPA | 802.11i (ou WPA2) |
| Autenticação | | Unilateral (STA) | Bilateral com 802.1X (STA, AP e rede) | |
| Distribuição de Chaves | | | EAP ou PSK, 4-Way Handshake | |
| Política de Gestão de IV | | | TKIP | AES-CCMP |
| Cifra dos dados | | RC4 | | AES-CTR |
| Controlo de Integridade | Cabeçalhos | | Michael | AES CBC-MAC |
| | Dados | CRC-32 | CRC-32, Michael | |

Inicialmente, a segurança das redes estruturadas 802.11 era baseada no protocolo WEP. Este protocolo permite a autenticação unidirecional dos STA e a confidencialidade e o controlo de integridade do dados trocados entre os STA e os AP.

O WAP (*Wi-fi Protected Access*) tem a vantagem de permitir reutilizar os equipamentos de rede dos STA que suportam apenas WEP mas exige que os AP saibam operar com WAP.

O WAP permite configurações de segurança mais simples, particularmente interessantes para ambientes SOHO (*Small Office, Home Office*). O WPA mantém a utilização integral do WEP, mas fá-lo de maneira a evitar os problemas de segurança que o mesmo, por si só, levanta.

## 7.6. IEEE 802.11: WEP (*Wired Equivalent Privacy*)

O WEP inclui duas funcionalidades distintas: autenticação de STA e confidencialidade e controlo de integridade dos dados trocados. Estas funcionalidades são parcialmente independestes e aplicadas em instantes distintos da interação entre um STA e um AP.

### 7.6.1. Autenticação

- OSA (*Open System Authentication*): Neste caso não existe qualquer autenticação dos STA, logo a sua associação ao AP é sempre autorizada. Este modelo de autenticação é útil em alguns cenários operacionais específicos. Caso se pretenda fornecer um acesso totalmente público e

livre a uma determinada rede. É ainda útil caso se prescinda da autenticação WEP para se usar outros protocolos de autenticação alternativos.4

Em suma, sem autenticação. Apenas o processo de associação e autenticação.

- SKA (*Shared Key Authentication*): Neste caso deverá existir uma chave secreta partilhada entre o STA e o AP para autenticação do primeiro (PSK – *Pre-Shared Key*). A autenticação é feita usando um processo simples de desafio-resposta: o AP envia um desafio ao STA, e este deverá devolvê-lo cifrado com a chave partilhada de autenticação. A cifra é feita usando o mecanismo-base do WEP para a cifra de tramas de dados.

Desafio/Resposta entre STA e AP
Chave (palavra passe) por pessoa (endereço MAC) ou rede
Autenticação Unilateral das STA (sem autenticação do AP e Rede)

A autenticação com SKA pressupõe uma pré-distribuição de chaves PSK ao STA e ao AP. Esta pré-distribuição não é contemplada pelo WEP e depende dos fabricantes dos AP. Cada AP permite associar um conjunto de quatro chaves a cada SSID endereço MAC de cada STA autorizado. O primeiro modo fornece uma autenticação não personalizada, ao contrário do segundo.
O STA inicia esta fase com uma mensagem *Authentication Request*, indicando o modelo de autenticação pretendido, devendo o AP responder com um erro caso não seja permitido. Se a permissão existir, que não é mais do que um conjunto de 128 octetos, enviados pelo AP. O STA deverá enviar uma nova trama *Authentication Request*, com uma copia do desafio mas com a proteção WEP. O desafio é cifrado com uma chave PSK, que deverá ser comum so STA e ao AP. Após a decifra da trama, o AP compara o desafio recebido com o que anteriormente enviou. Se foram iguais, envia uma trama *Authentication Response* com uma autorização de acesso. Caso contrário, envia a mesma trama, mas indicando uma falha na fase de autenticação.

### 7.6.2. Confidencialidade e controlo de integridade

Nesta área o WEP tem uma funcionalidade elementar, limitando-se a suportar a exploração de canais de comunicação seguros, dotados de confidencialidade e controlo de integridade. A confidencialidade e controlo de integridade são ainda limitados a tramas *unicast* (ponto a ponto), não existindo qualquer suporte para a proteção de tramas *multicast* ou *broadcast*.

O WEP usa um mecanismo de cifra contínua baseado no algoritmo RC4 e um mecanismo de controlo de integridade não criptográfico baseado no algoritmo CRC-32.
Para cada trama é escolhido um vetor de iniciação (VI) que juntamente com a chave WEP, são usados como chave do algoritmo RC4 para gerar uma chave continua. Esta chave contínua é somada aos dados a enviar via rádio e à sua soma de controlo calculada com CRC-32, transformando-os num criptograma.
A decifra de um criptograma segue um processo inverso: o recetor retira o VI da mensagem que recebeu, usa-o juntamente com a chave WEP para gerar a chave continua e soma-a ao criptograma recebido, de onde resultam os dados em claro inicialmente apresentados para cifra.

### 7.6.3. WEP: Imensos problemas de segurança…

- SKA é completamente inseguro pois um atacante possui toda a informação para se fazer passar por uma vitima e não é necessário saber a chave. As APs falsas não podem ser detetadas.
- A mesma chave é usada para autenticação e confidencialidade, sem distribuição de chaves, chaves sobre-utilizadas.
- Controlo de integridade fraco com CRC-32 linear e modificação determinística das tramas é trivial.
- Gestão de IV é medíocre pois IV é muito pequeno (24 nis), repetido a cada 23 GB de dados (no máximo). O IV não é gerido, pois não tem controlo/prevenção de reutilização.

### 7.6.4. WEP: Problema Critico de segurança

- Descoberta uma vulnerabilidade no RC4 pois é um algoritmo não público (mas bem conhecido) e descobertas chaves fracas pois alguns bits da keystream refletem bits da chave.
- Impacto no WEP pois os atacantes escutam tramas com um IV apropriado para uma chave fraca onde inevitavelmente acontece de forma repetida e os atacantes podem acelerar o processo enviando tramas adicionais. As tramas são recolhidas, permitindo-se encontrar a chave secreta onde o tempo de ataque cresce de forma linear com o tamanho da chave.

## 7.7. Limitação dos problemas do WEP: WPA (Wifi Protected Access)

- WPA utiliza WEP de uma forma mais segura:
  - Uma chave RC4 diferente por cada trama
  - Chaves fracas RC4 são evitadas
  - Controlo de integridade adicional
  - IV usado de forma incremental (limitar repetições)
- Implementado inicialmente nos controladores (drivers):
  - Mais tarde no firmware
- Alinhado com a norma IEEE 802.11i:
  - A norma que define a segurança da IEEE 802.11
  - WPA pode ser utilizada com 802.1X para autenticação mútua segura

## 7.8. WPA (Wifi Protected Access)

O WAP manteve toda a funcionalidade do WEP, tipicamente fornecida pelas interfaces de rede, e acrescentou-lhe funcionalidade ao nível da gestão de chaves de cifra e ao nível do controlo de integridade das tramas.

- Com o WAP cada trama é cifrada com uma chave WEP diferente de forma a que não seja possível construir dicionários de chaves continuas até mesmo quando se usa a mesma PSK repetidas vezes.
- O controlo de integridade do WEP é complementado com um controlo de integridade criptográfico mais abrangente.
- O controlo de integridade deixa de ser apenas por trama, mas contempla a ordem das tramas.
- A autenticação de interlocutores é muito melhorada, passando a permitir a autenticação mútua entre os STA, a rede e os AP, e distribuição de chaves de sessão.

Nos STA o WPA pode ser implementado em *software* pelos sistemas operativos ou no hardware das interfaces de rede.

## IEEE 802.11i ou WPA2

O 802.11i, também por vezes designado por WPA2, é um padrão complexo que define um modelo de segurança para redes 802.11.

O 802.11i usa o conceito de redes de segurança robusta, RSN (*Robust Security Network*). Uma rede diz-se pré-RSN se apenas suportar WEP para proteção de tramas e a autenticação inicial do 802.11. Uma rede RSN tem de suportar uma autenticação mais eficaz dos interlocutores, baseada em 802.1X.

Usa mecanismos mais avançados para proteção das tramas, ou seja, métodos que não implicam suporte do hardware existente, como AES-CCMP, AES-CTR, CBC-.MAC.

Utiliza IEEE 802.1X para autenticação, com o modo simplificado: WPA-PSK e modo baseado em EAP para ambientes mais robustos.

## AES-CCMP

O AES-CCMP é a combinação-base de mecanismos de segurança do 802.11i para proteger tramas 802.11. Esta combinação tem por base o algoritmo criptográfico AES com chaves e blocos de dados de 128 bits.

O AES-CCMP usa o modo de operação CCM (*Counter with* CBC-MAC). Este é um modo de operação concebido para fornecer simultaneamente autenticação e controlo de integridade usando cifra por blocos de 128 bits.

A cifra do CCM é uma cifra continua com base numa cifra por blocos operando em modo CTR. O controlo de integridade do CCM é realizado com CBD-MAC.

O modelo de operação AES-CCMP é muito semelhante ao do TKIP, mas usando apenas uma chave de sessão para cifra e controlo de integridade: TK.

## O WPA assenta em dois pilares

### TKIP (*Temporel Key Integrity Protocol*)

Lida com a autenticação e confidencialidade das tramas.

O TKIP encapsula o WEP, usa-o mas de forma a não expor as suas vulnerabilidades. As funcionalidades do TKIP podem-se resumir do seguinte modo:

- Usa um VI de 48 bits, TSC (TKIP *Sequence Counter*); com o dobro dos bits do VI do WEP, que varia de forma bem definida e que permite controlo de ordem na receção.
- Produz chaves WEP diferentes para cada trama e em cada sentido da comunicação.
- Exclui as chaves fracas do RC4 do conjunto de chaves produzido por combinação dos VI com as chaves WEP.

O TKIP usa três chaves partilhadas com o interlocutor: uma chave para confidencialidade, TK (*Temporal Key*) de 128 bits, e duas outras para controlo de integridade, chaves MIC, de 64 bits cada, uma para cada sentido da comunicação.

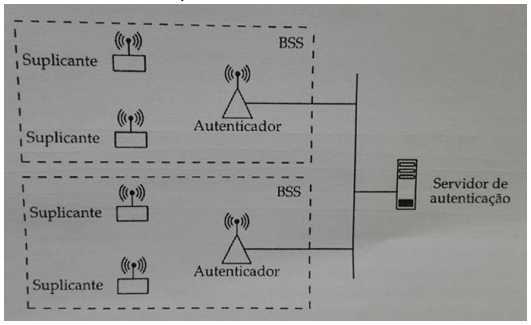
O TKIP pode ser usado com chaves PSK, ambas as chaves serão calculadas a partir dessa PSK e o processo é globalmente designado por WPA-PSK.

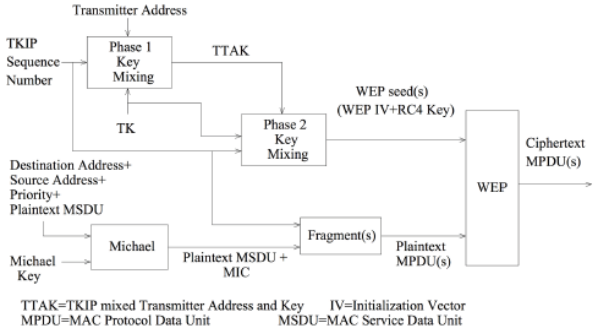
### 802.1X

Lida com a autenticação entre interlocutores e distribuição de chaves de sessão após uma operação de associação.

Este protocolo serve para efetuar a autenticação mutua entre interlocutores, STA e rede, aquando da ligação de um STA a uma rede sem fios. Este protocolo permite criar e distribuir chaves de sessão frescas aos equipamentos que efetuam a troca efetiva de mensagens via rádio, STA e AP.

No 802.1X distinguem-se três tipos de interlocutores: suplicante, autenticador e servidor de autenticação. O **suplicante** é um equipamento (móvel) que pretende ligar-se a rede. O **autenticador** é o elemento que controla o estado do porto de acesso do suplicante à rede. O **servidor** de autenticação é um servidor central, gerido no âmbito do domínio de segurança da rede, que efetivamente conduz o processo de autenticação mutua entre os suplicantes e a rede.






- **Confidencialidade**

O processo que o TKIP usa para gerar uma chave RC4 /chave WEP e VI) para WEP a partir da chave TK e do TSC tem múltiplos objetivos.

Comparando o TKIP com o WEP, apenas em termos de gestão da confidencialidade, verificamos que o TKIP consegue usar o WEP mas de forma a anular todas as vulnerabilidades conhecidas.

- **Controlo de Integridade**

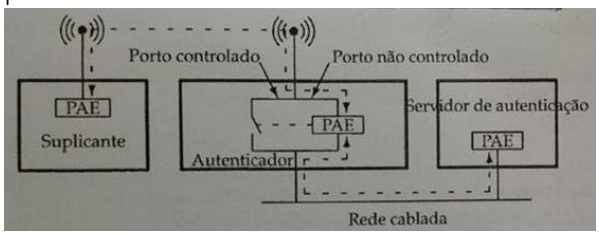
Com o TKIP o controlo de integridade dos dados recebidos é feito em múltiplas etapas e de forma a minimizar a ocorrência de falsos positivos:

- Verificar o FCS (*Frame Check Sequence*) da trama; se estiver incorreto, descartar a trama.
- Verificar o valor de TSC recebido na trama; se tiver um valor inferior ao ultimo recebido para o mesmo transmissor, descartar a trama.
- Verificar o CRC-32 do WEP; se estiver incorreto, descartar trama;
- Depois de receber todos os fragmentos de um MSDU, enviados em múltiplos MPDU validados através dos passos anteriores, verificar o MIC recebido; se estiver errado descartar o MSDU.

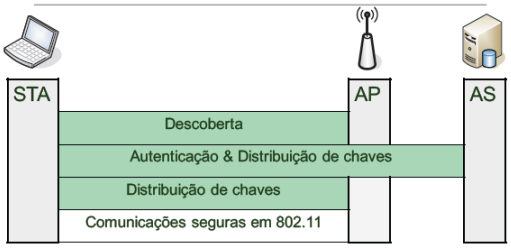
-**Autenticação baseada em Portas**

É um modelo comum para todas as redes IEEE 802 com autenticação mútua ao nível dos dados. Concebido inicialmente para redes de grandes dimensões como: campus universitário ou tecnológico. O modelo foi estendido às redes sem fios. Foca-se muito na distribuição de chaves em que outros protocolos implementam aspetos chave do processo.

Um porto pode ser controlado ou não controlado. Um porto **não controlado** não impõe qualquer restrição à troca de dados através de si. Um porto **controlado** possui estados distintos e permite efetuar controlo de trocas de dados em cada estado: no estado "não autorizado" não permite a troca de dados, enquanto no estado "autorizado" permite.




- **Fases Operacionais**

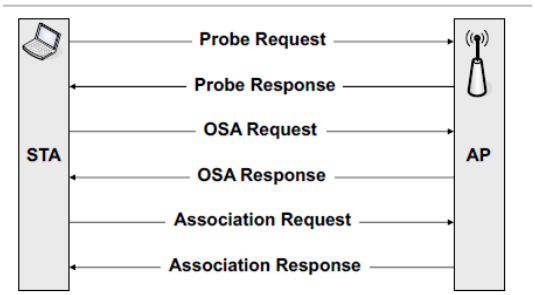



## Etapas da 802.1X

As operações realizadas no âmbito do 802.1X em redes sem fios dividem-se em três etapas. Após a terceira etapa pode ter lugar a troca de dados segura entre o STA e a rede a que AP está ligado. Os dados serão protegidos usando o material criptográfico e os algoritmos negociados entre o AP, o servidor de autenticação e o STA.

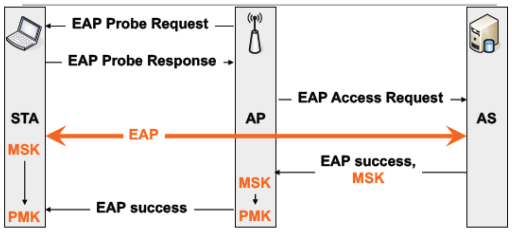
- **Primeira etapa: descoberta e associação 802.11**

O suplicante (STA) liga-se à rede sem fios. É efetuado o processo normal das redes 802.11 da descoberta da rede, autenticação do STA e de associação entre o STA e o AP. Como esta autenticação é dispensável, face à que se está globalmente a fazer via 802.1X, usa-se o modelo OSA, o qual não se impoe quaisquer restrições. No final desta etapa o suplicante deverá estar autenticado e associado junto de um AP que irá supervisionar ou controlar as etapas seguintes. No final desta etapa o porto controlado está no estado "não autorizado".



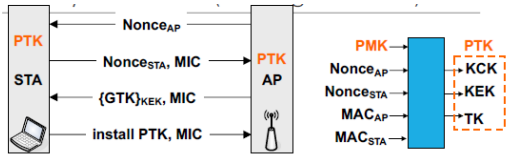
- Segunda Etapa: autenticação EAP

É realizada a autenticação mútua e uma distribuição de chaves de sessão entre o suplicante (utente/STA) e o servidor de autenticação. O autenticador supervisiona um diálogo entre o suplicante e o servidor de autenticação, o qual é o único permitindo através do porto não controlado. A troca de mensagens relativa á autenticação segue o metaprotocolo EAP. No final desta etapa o porto controlado continua no estado não autorizado.



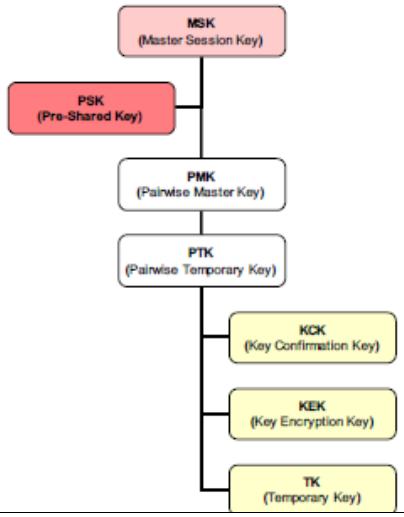

-Terceira Etapa: acordo em quatro passos

É realizada uma autenticação mútua e uma distribuição de chaves de sessão entre o suplicante e o autenticador. A autenticação é fundamental para o suplicante garantir que está a interagir com um autenticador (AP) que pertence ao mesmo domínio de segurança do servidor de autenticação, e não um impostor. A distribuição de chaves visa criar uma chave de sessão fresca entre o suplicante e o autenticador, que irá servir de base à proteção de dados trocados entre ambos. Porque esta etapa envolve a troca de quatro mensagens, é referida como *4-Way Handshake*. No final desta etapa o porto controlado já está no estado "autorizado".




## IEEE 802.1X: Hierarquia de chaves

- MSK
  - Resultado de uma execução do protocolo EAP
  - Arquitetura empresarial
- PSK
  - Chave partilhada entre AP-STA (De longa duração)
  - Arquitetura SOHO
- PMK
  - Chave fresca utilizada para autenticação mútua e para distribuição no 4WH.
- PTK
  - Chave utilizada para proteger trocas de dados
    - CKC/KEK: Protocolo 4WH
    - TK: 802.11 Tramas de dados



## 7.8. EAP (*Extensible Authentication Protocol*)

O EAP é um metaprotocolo concebido para encapsular outros protocolos de autenticação. Ele não foi concebido especificamente para 802.1X, já existia para permitir flexibilizar a autenticação noutros protocolos.

No caso do 802.1X, o EAP é fundamental para libertar o AP (autenticador) da tarefa de gerir aspetos particulares do modelo de autenticação adotado. A autenticação centralizada no servidor de autenticação e consegue-se alterar os paradigmas de autenticação da rede sem alterar o *software* dos AP.

| | EAP-MD5 | LEAP | EAP-TLS | EAP-TTLS | PEAP |
|---|---|---|---|---|---|
| **AS** | N/A | síntese(desafio, password) | Chave pública (certificado) | | |
| **Autenticação** | síntese(desafio, password) | Síntese(desafio, password) | Chave pública (certificado) | EAP, Chave pública (certificado) | PAP, CHAP, MS-CHAP, EAP |
| **Distribuição de chaves** | Não | Sim | | | |
| **Riscos** | Exposição da identidade<br>Ataques por dicionário<br>Host ITM<br>Roubo de ligações | Exposição da identidade<br>Ataques por dicionário<br>Host ITM | Exposição da identidade | | Exposição da identidade |

*Figura 3- Alguns protocolos EAP para 802.1X*

## 7.9. Segurança em IEEE 802.11: Todos os problemas resolvidos: Não…

PSK e alguns métodos EAP vulneráveis a ataques por dicionário e continuarão a ser enquanto as passwords forem escolhidas pelos utilizadores.

Proteção apenas abrange tramas de dados:

- Tramas de gestão
- Atacantes podem desautenticar/desassociar STAs
- Atacantes podem adivinhar tipo de tráfego pelos tempos/tamanhos
- Muitos protocolos expõem identidade do utilizador

Problemas ao nível do acesso ao meio (CSMA)

- Valores da janela de congestão baixos permitem acesso prioritário ao meio