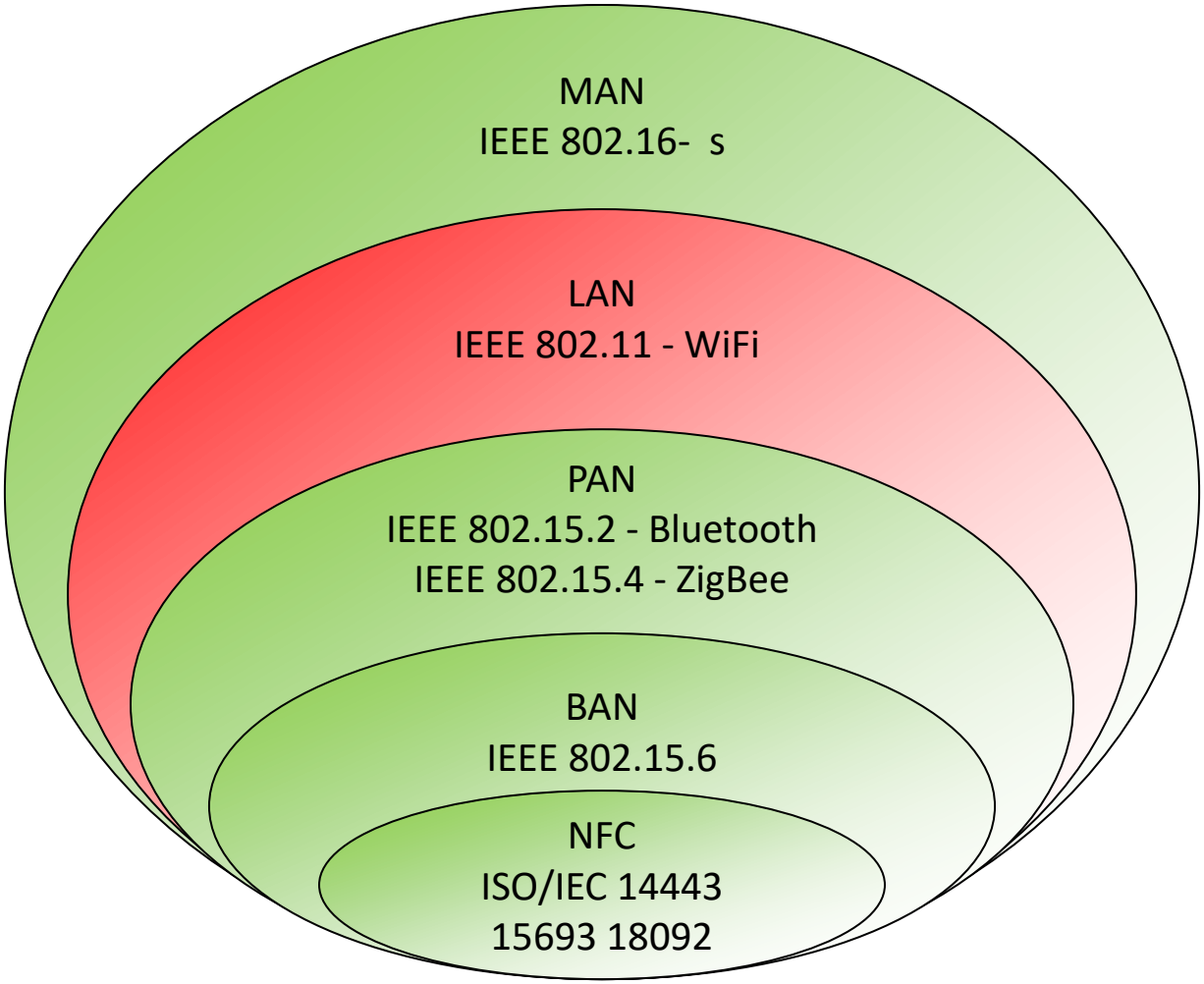
Segurança em redes IEEE 802.11

Panorama simples das comunicações sem fios



Comunicações sem fios: aspetos de segurança

- **Comunicação efetuada em Broadcast**
  - Difícil de controlar a propagação física
  - Limitações físicas são pouco eficientes contra:
    - Interferência com as comunicações legítimas
    - Interceção das comunicações

- **Mitigação**
  - Mecanismos de redução e interceção e interferência
    - No nível físico (PHY)
    - No nível dos dados (MAC)

Phy: Redução de interferência e interceção

- **Prevenir que os atacantes descodifiquem o canal**
  - Codificação do canal necessita de usar uma chave secreta
- **Exemplo: Bluetooth FHSS (Frequency Hopping Spread Spectrum)**
  - Frequência alterada segundo um padrão conhecido para emissor e recetor
    - Dados são divididos em pacotes e transmitidos sobre 79 frequências, segundo um padrão pseudo-aleatório.
    - Apenas emissores e recetores que conhecem o padrão de alteração de frequência conseguem aceder aos dados transmitidos.
  - FHSS aparece como um impulso de ruído de curta duração
    - Transmissor altera frequência 1600 vezes por segundo!

Phy: Redução de interferência e interceção

- **Evita que o canal seja monopolizado por transmissores**
  - Políticas de acesso ao meio físico

- **Exemplos**
  - Bluetooth FHSS: transmissores não sincronizados raramente colidem
  - Wi-Fi: Cada rede utiliza uma frequência específica
  - GSM: Cada terminal transmite numa frequência/instante distinto

Interferência ainda é possível devido a emissores externos ou sobreposição de canais

MAC: Redução de interferência e interceção

- **Evita que atacantes identifiquem os participantes numa comunicação**
  - Cabeçalhos das tramas são cifrados
  - Utilização de endereços temporários
- **Evita que atacantes compreendam os dados**
  - Conteúdo das tramas é cifrado
    - Não implica cifra dos cabeçalhos
- **Evita que atacantes forjem tramas válidas**
  - Tramas necessitam de ser autenticadas
    - Autenticação do emissor e garantia de frescura

IEEE 8902.11: Arquitetura em Redes Estruturadas

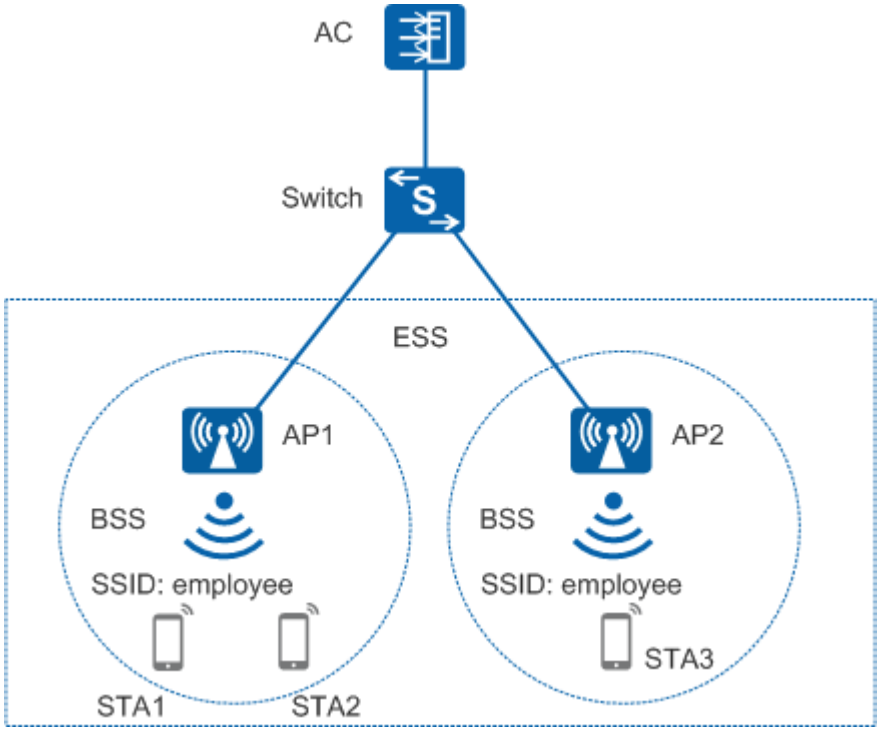
- **Estação (STA)**
  - Dispositivo que se liga a uma rede sem fios
  - Possui um identificador único
    - Endereço MAC (Media Access Control)

- **Ponto de Acesso (AP)**
  - Dispositivo que permite e ligação de dispositivos sem fios
  - Pode permitir a interligação a outras redes com fios

- **Rede sem fios**
  - Conjunto formato por um conjunto de STAs e APs associados entre si e comunicando

IEEE 8902.11: Terminologia

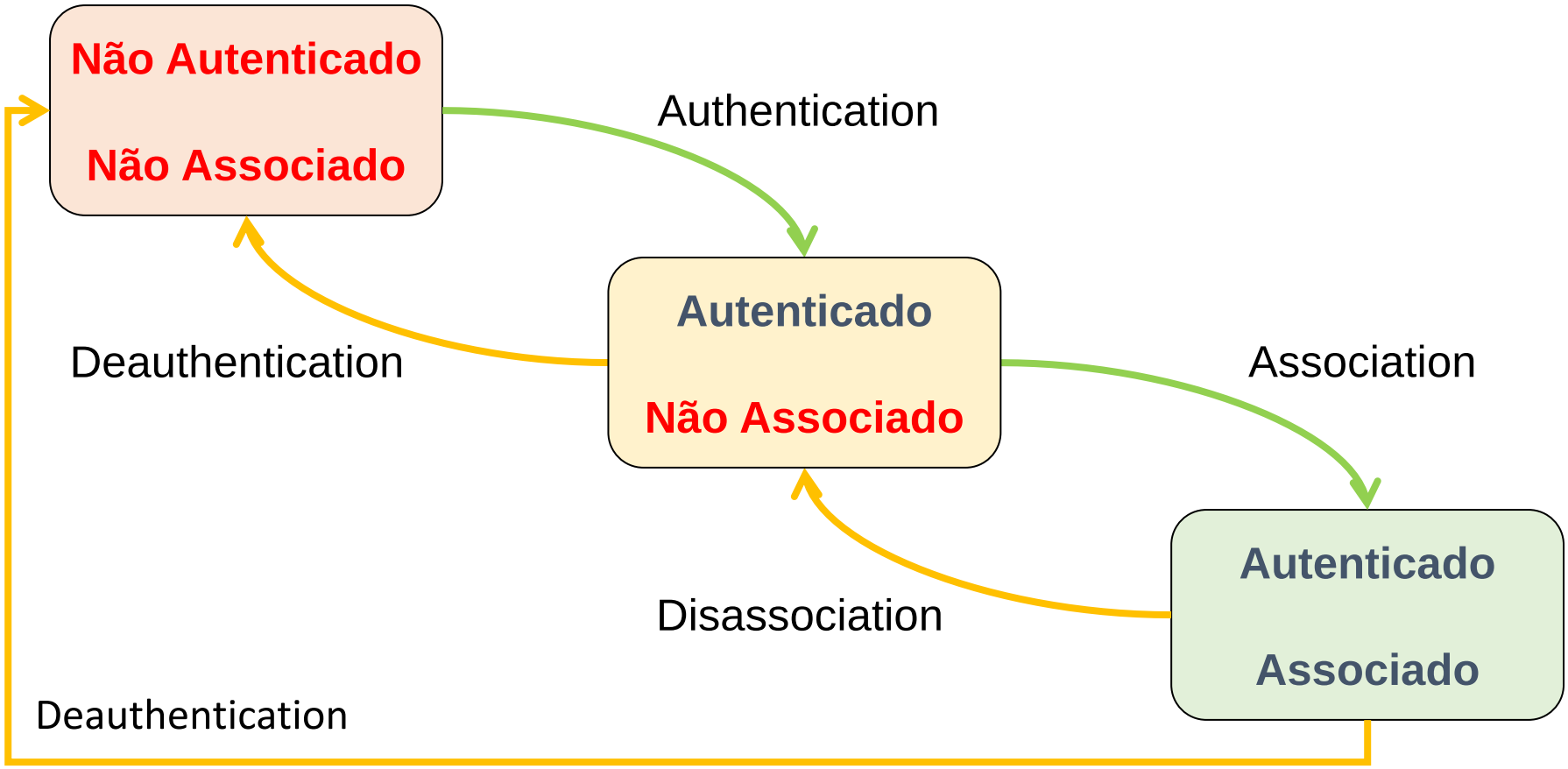
- **Basic Service Set (BSS)**
  - Rede formada por estações associadas a um AP
- **Extended Service Set (ESS)**
  - Rede formada por várias BSS interligadas por um Distribution System (DS)
- **Service Set ID (SSID)**
  - Identificador de uma rede sem fios servida por uma BSS por ESS)
  - Um AP pode fornecer vários SSIDs



Terminologia

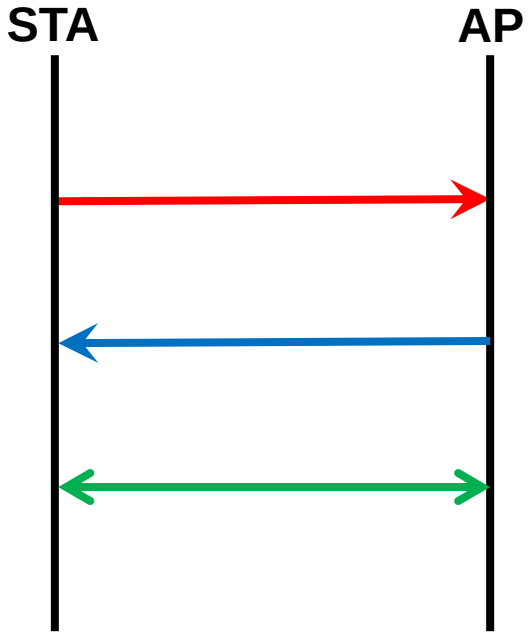
```
$ airport -s
            SSID BSSID             RSSI CHANNEL
         MEO-WiFi 9e:97:26:f1:65:3e -87  11
FON_ZON_FREE_INTERNET 00:05:ca:d3:32:f9 -86  11
         ZON-22D0 00:05:ca:d3:32:f8 -90  11
     Cabovisao-BB20 c0:ac:54:f8:fe:dc -84  6
FON_ZON_FREE_INTERNET 84:94:8c:ae:74:a9 -81  6
         ZON-6E50 84:94:8c:ae:74:a8 -81  6
FON_ZON_FREE_INTERNET 84:94:8c:ad:23:99 -86  2
         ZON-ED50 84:94:8c:ad:23:98 -87  2
FON_ZON_FREE_INTERNET bc:14:01:9b:d0:c9 -88  1
         ZON-D030 bc:14:01:9b:d0:c8 -88  1
```

Autenticação e Associação



Tipos de Mensagens

- **Mensagens de Gestão**
  - Beacon
  - Probe Request & Response
  - Authentication Request & Response
  - Deauthentication
  - Association Request & Response
  - Reassociation Request & Response
  - Disassociation
- **Mensagens de Controlo**
  - Request to Send (RTS)
  - Clear to Send (CTS)
  - Acknowledgment (ACK)
- **Mensagens de Dados**



Segurança do Meio Físico

Tipo de Rede / Funcionalidade		pre-RSN	RSN (Robust Security Network)		
		WEP	WPA	802.11i (ou WPA2)	WPA3
Autenticação		Unilateral (STA)	Bilateral com 802.1X (STA, AP enetwork)		Bilateral com 802.1x
Distribuição de Chaves			EAP ou PSK, 4-Way Handshake		WP2 + OWE e SAE
Política de Gestão de IVs			TKIP	AES-CCMP	AES-GCM
Cifra dos Dados		RC4		AES-CTR	AES-GCM e EC
Controlo de Integridade	**Cabeçalhos**		Michael	AES CBC-MAC	SHA-384 HMAC
	Corpo	CRC-32	CRC-32, Michael		

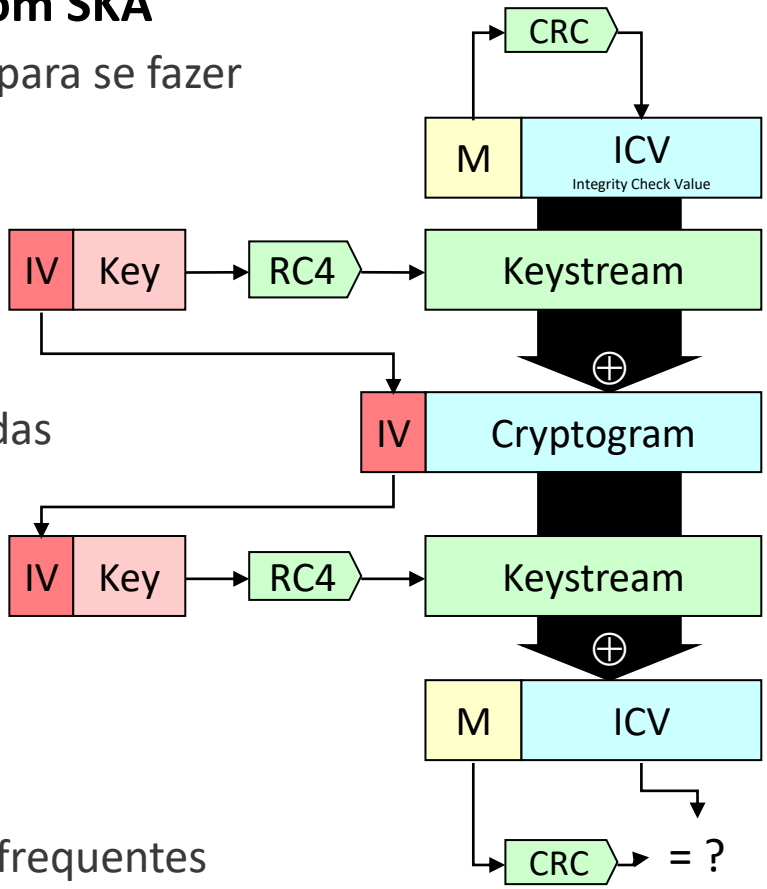
- **Outros**
  - Ocultação do SSID
  - Filtro dos endereços MAC autorizados
  - Aleatoriedade dos endereços MAC (na descoberta)
  - Contra-medidas

WEP (Wired Equivalent Privacy)

- **Autenticação Unilateral e Facultativa**
  - AP pode suportar vários modos em simultâneo
- **OSA: Open System Authentication**
  - Sem qualquer autenticação
- **SKA: Shared Key Authentication**
  - Desafio resposta entre STA e AP
  - Chave distinta por cliente (Endereço MAC) ou rede
  - Autenticação unilateral da STA
    - AP não é autenticado
- **Dados (corpo da mensagem):**
  - cifrados com RC4, chaves de 40 ou 104 bits
  - autenticados usando um CRC-32

WEP (Wired Equivalent Privacy)

- **WEP é completamente inseguro, mesmo com SKA**
  - Atacante pode obter a informação necessária para se fazer passar por uma vítima
  - APs de atacantes não podem ser detetados
- **A mesma chave para autenticação e confidencialidade**
  - Sem distribuição de chaves, chaves sobre-usadas
- **Controlo de integridade fraco**
  - CRC-32 é fraco, e linear
  - Modificação determinística de tramas é trivial
- **Fraca gestão de IVs**
  - IV é demasiado pequeno (24 bits), repetições frequentes
    - Mesmo IV = Mesma Chave => mesma Keystream
  - IVs não geridos, podendo existir duplicação



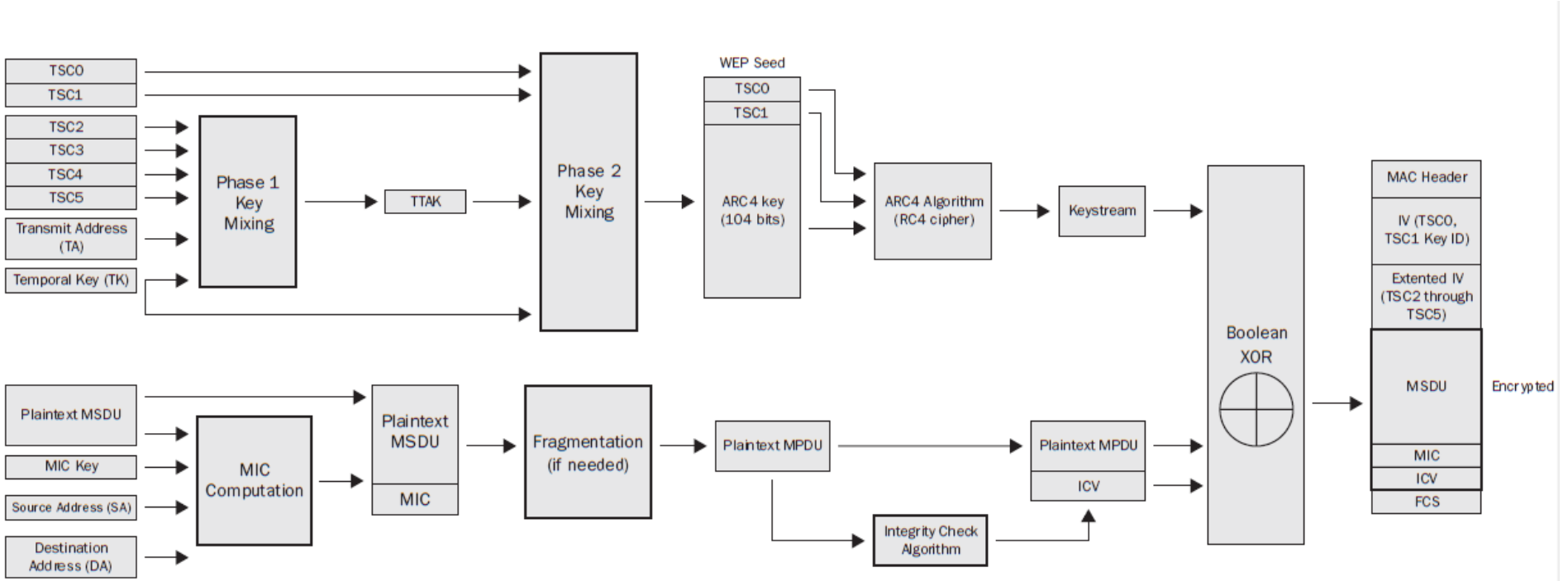
Mitigação dos problemas do WEP: WPA

- **WPA faz uso do WEP de uma forma mais segura**
  - Usa uma chave RC4 diferente por mensagem
  - Chaves RC4 fracas são evitadas
  - Controlo de integridade mais robusto (Michael)
  - Controlo dos IVs (uso sequencial)
- **Implementado inicialmente a nível do driver**
  - depois no firmware
  - Importante: teria de ser suportado por dispositivos “legados” (WEP)
- **Alinhado com a especificação IEEE 802.11i**
  - IEEE 802.11i define a atual arquitetura de segurança do 802.11
  - WPA pode também ser usado com 802.1x para autenticação forte e mútua

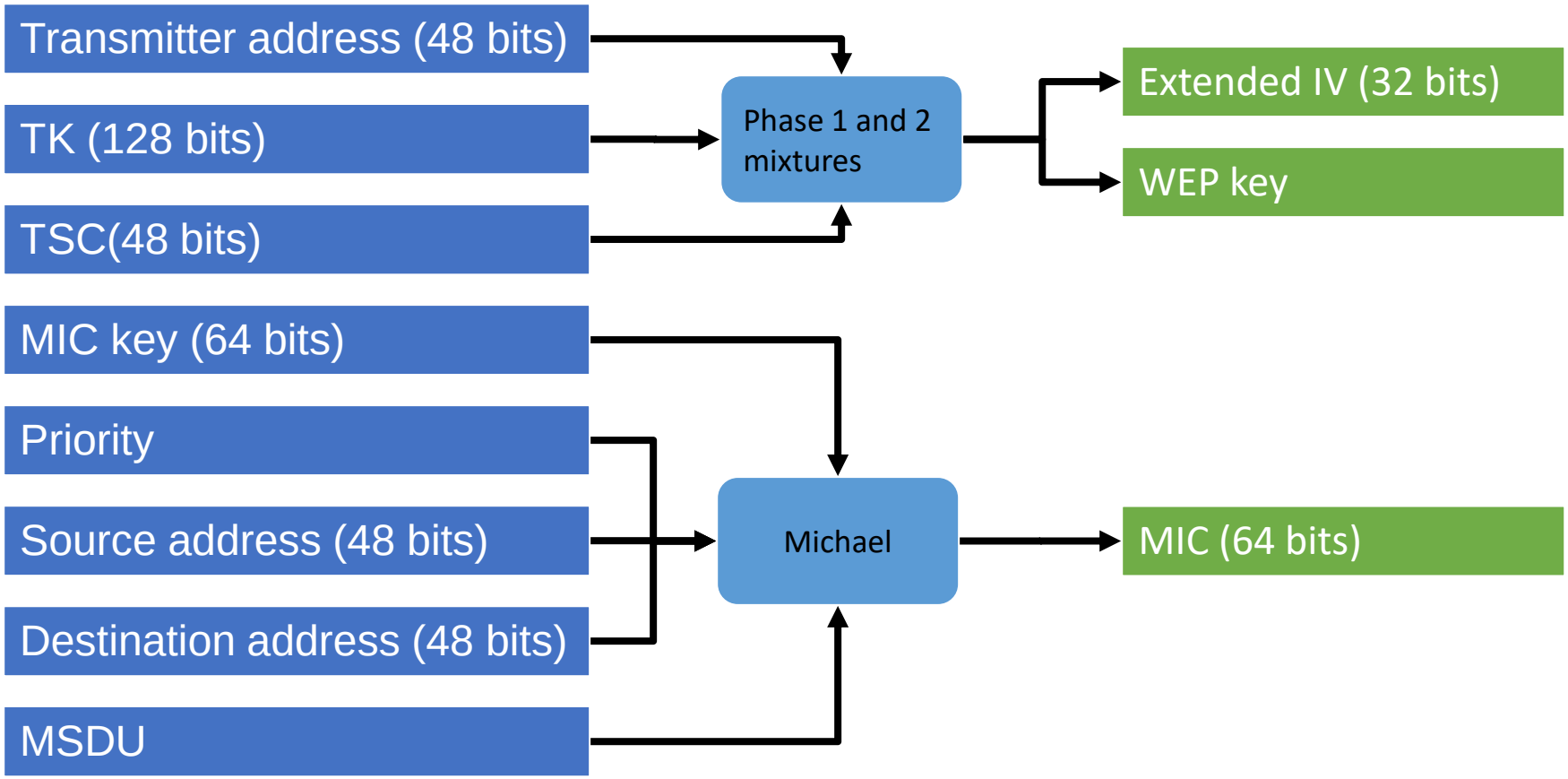
WPA (Wi-Fi Protected Access): TKIP

- **Chaves temporais:**
  - evitar ataques por engenharia social
- **Sequenciação de mensagens**
  - evitar repetição/injeção
- **Mistura de chaves**
  - evitar colisões de IVs
  - evitar chaves fracas
- **Controlo de integridade melhorado (MIC)**
  - Evitar manipulação de pacotes
- **Contra-medidas**
  - Resistir a fraquezas do TKIP MIC

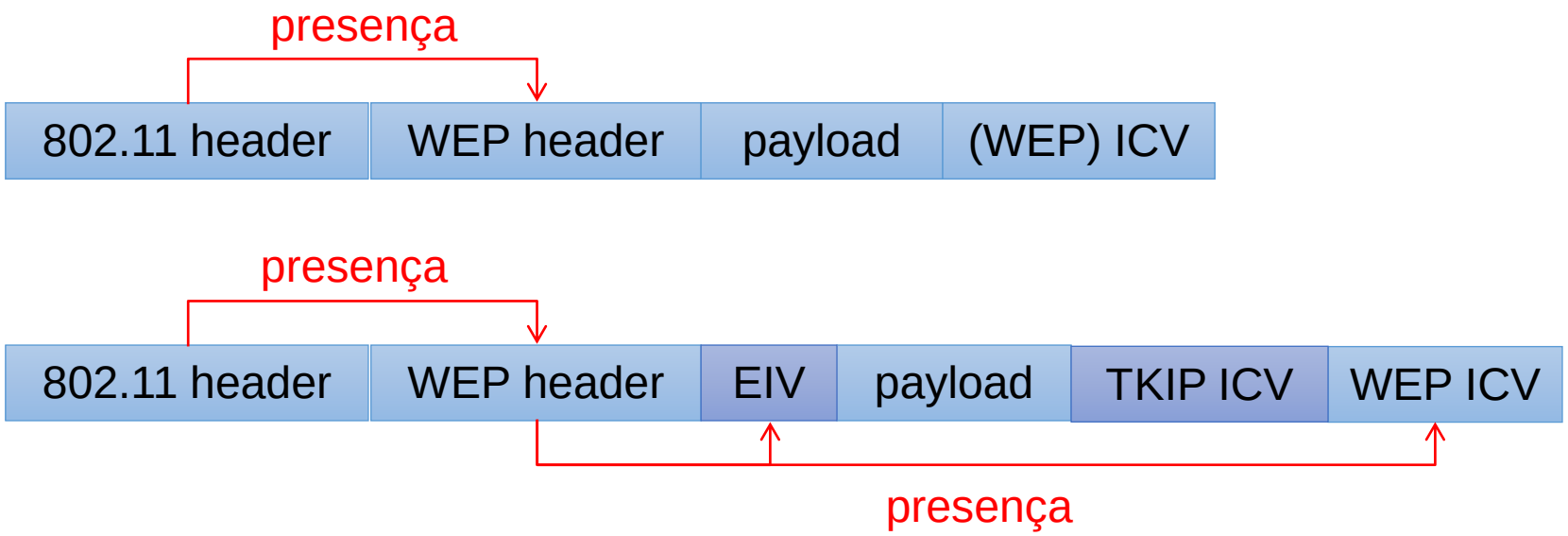
WPA TKIP (Temporal Key Integrity Protocol)



WPA TKIP (Temporal Key Integrity Protocol)



WPA TKIP: Formato das mensagens



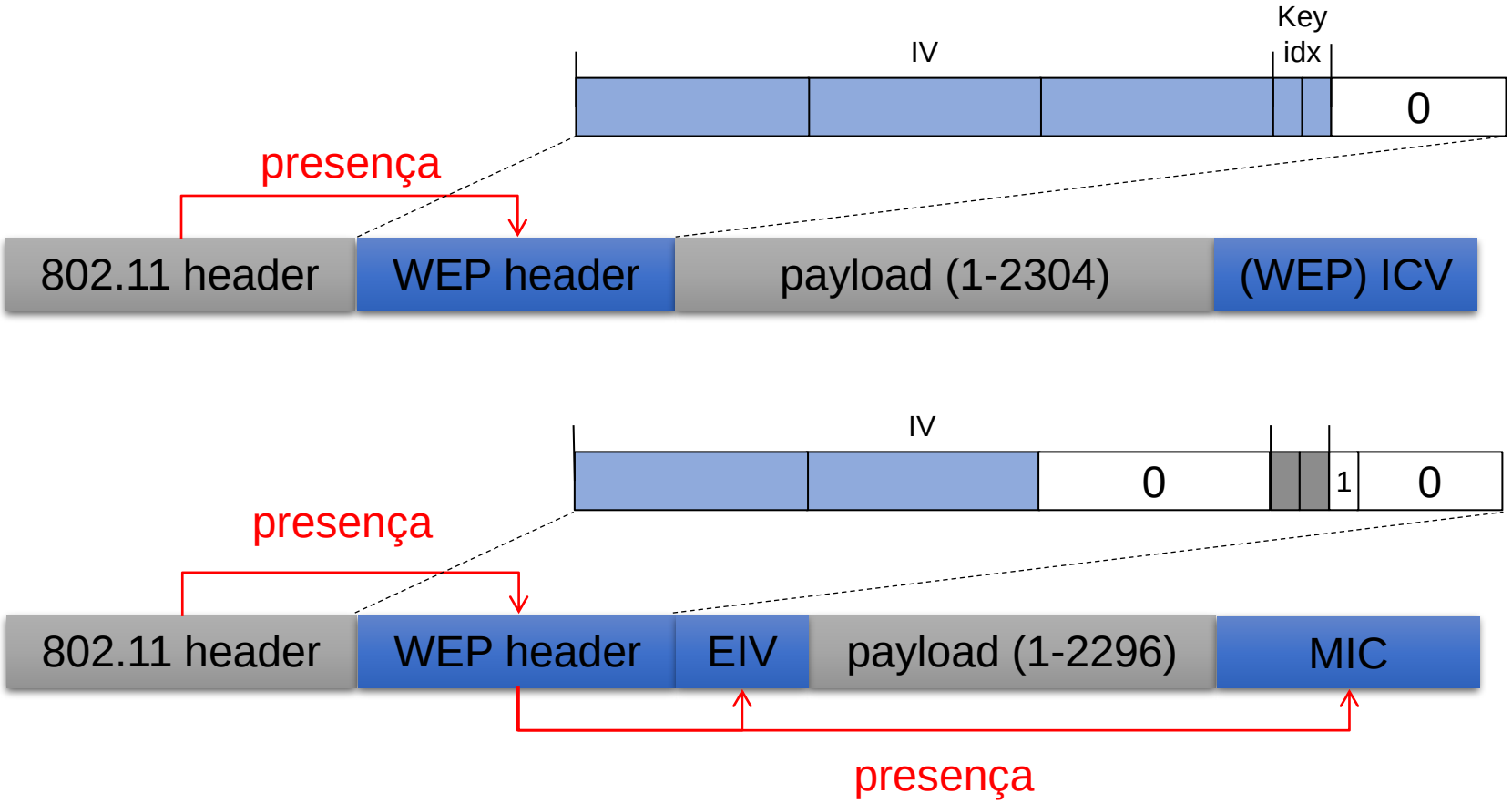
Ataque Beck-Tews

- **Condições**
  - O endereço de rede é parcialmente conhecido (ex 192.168.x.x)
  - A rede suporta QoS (IEEE 802.11e) com 8 canais (TID)
  - O período de renovação TKIP é longo (3600 segundos)
  - Ataque chop-chop: decifrar m bytes de um pacote, enviando m * 128 pacotes, usando força bruta no ICV
- **Ataque**
  - Capturar um pacote ARP (texto conhecido)
    - quase todos os campos são conhecidos exceto endereços IP, MIC e ICV
  - Enviar pacotes "adivinhando" o texto: limite de 1 pacote/TID/min
  - Força bruta sobre o endereço IP (2 bytes)
  - Reverter o MIC e encontrar a chave
    - MICHAEL não é estritamente unidirecional
  - Impacto: Obter a keystream válida para um qualquer TSC

IEEE 802.11i: WPA2

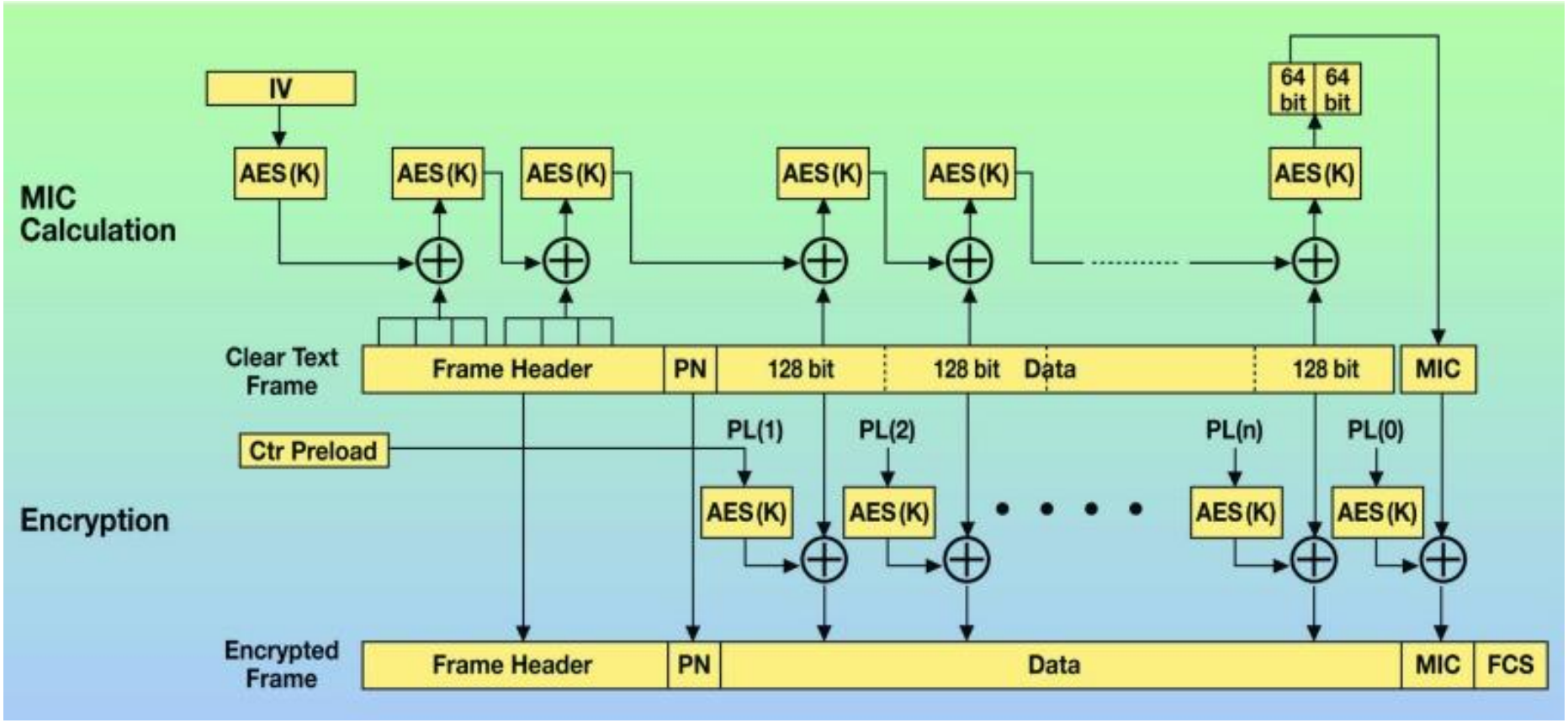
- **Define uma Robust Security Network (RSN)**
  - Redes que suportam WPA e 802.11i
- **Usa mecanismos avançados para proteção de mensagens**
  - AES para cifra dos dados e controlo de integridade
- **Usa 802.1x para autenticação de clientes**
  - Modo simplificado WPA-PSK para SOHO
  - Modo WPA-Enterprise para ambientes de maior dimensão

WEP vs AES-CCMP: Mensagens



IEEE 802.11i: WPA2

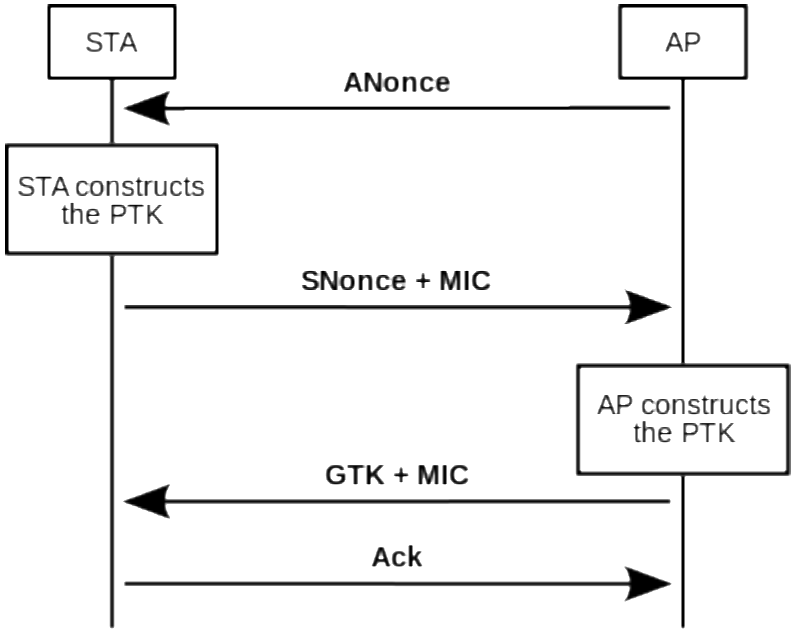
- **AES-CCMP - AES com CBC-MAC**
  - modo de cifra autenticado usando chaves de 128bits



http://2014.kes.info/archiv/online/04-5-036.htm

IEEE 802.1i: WPA

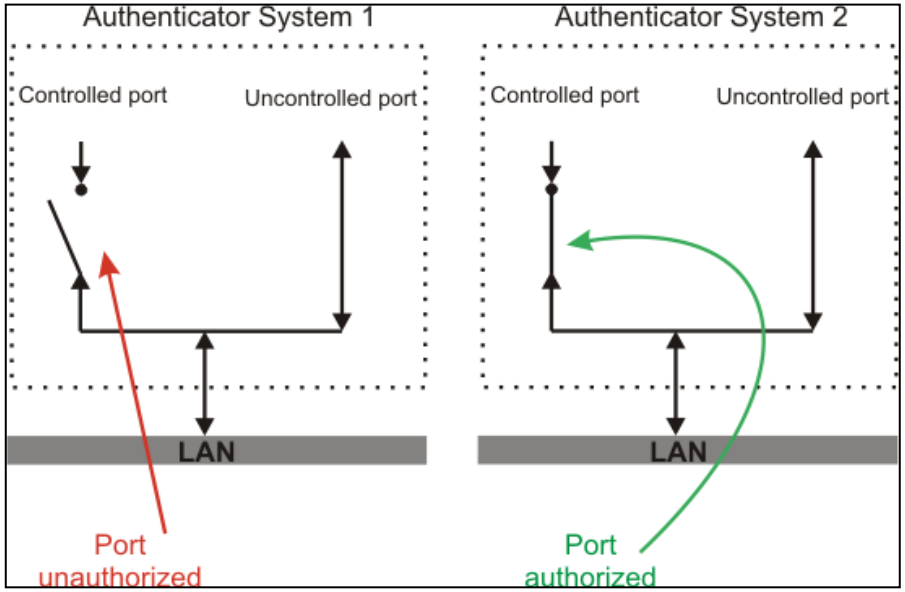
- **PTK: Pairwise Transient Key**
  - PRF(PMK | ANonce | SNonce | AP MAC address |STA MAC address)
  - PRF: Pseudo Random Function
  - PMK = PSK = PBKDF2(HMAC−SHA1, password, ssid, 4096, 256)
- **GTK: Group Temporal Key**
  - Utilizado para tráfego broadcast

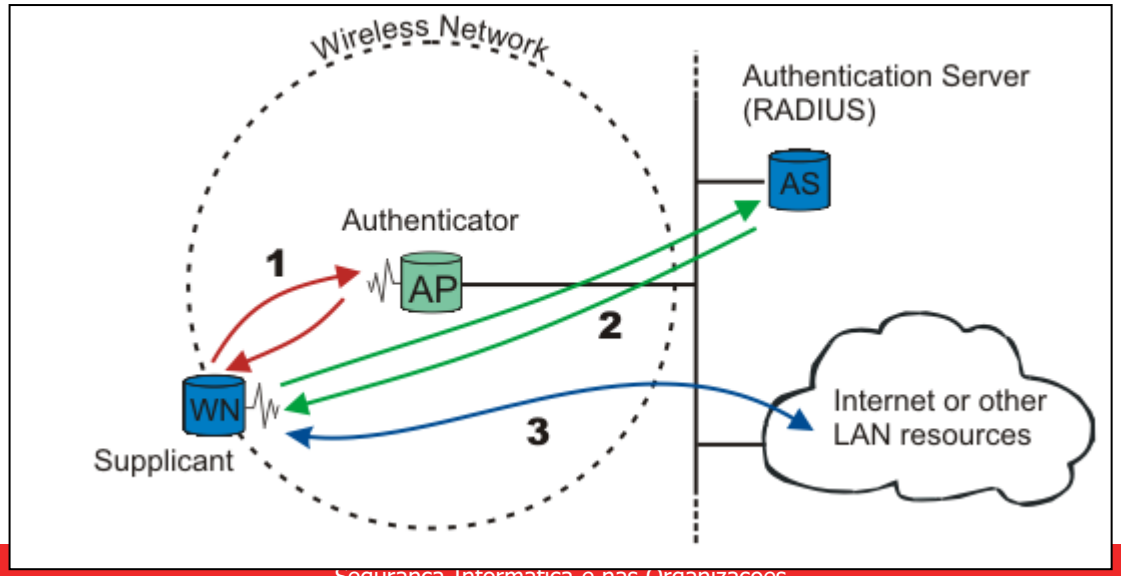


IEEE 802.1X: Autenticação por Portas

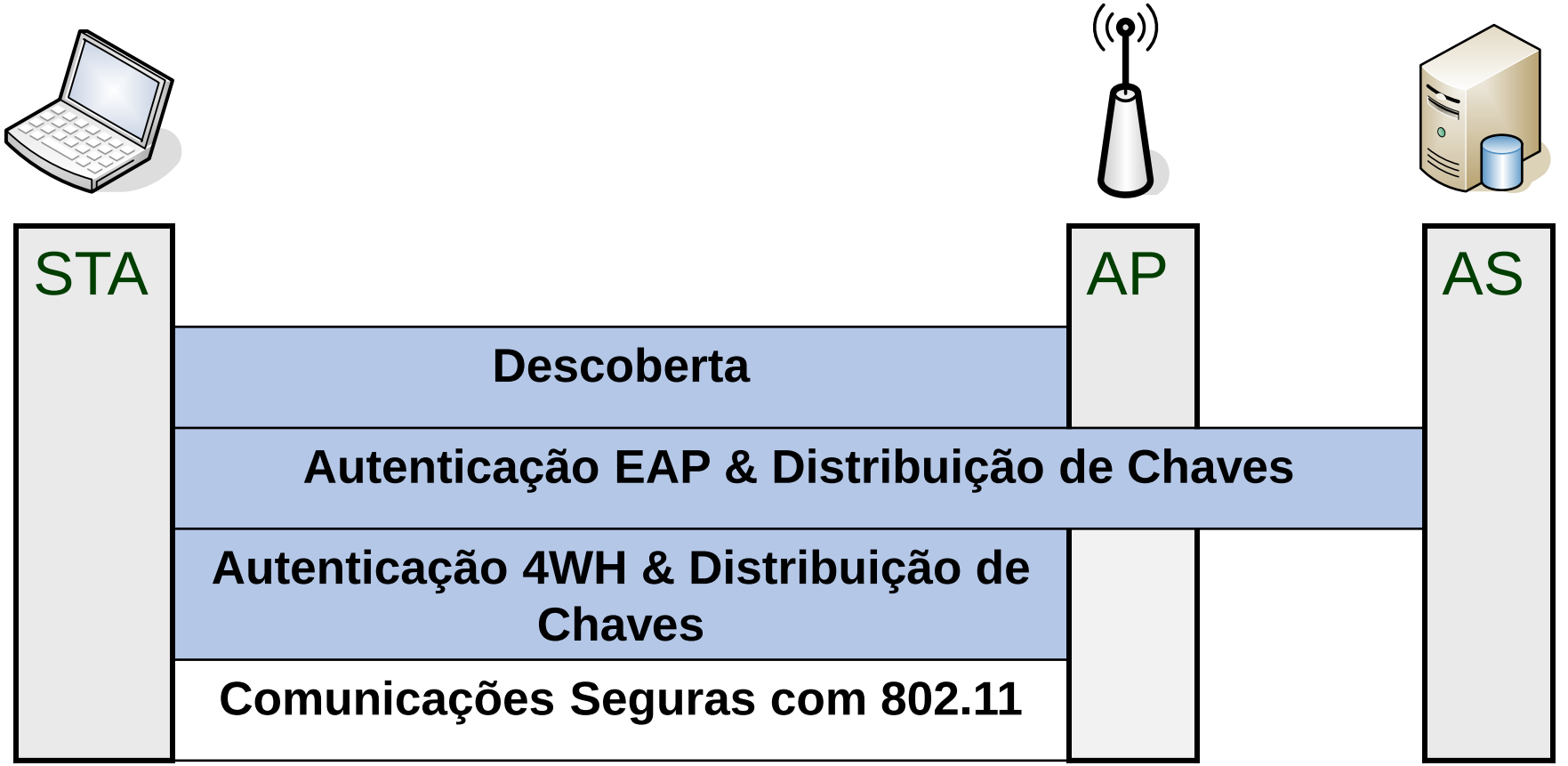
- **Modelo de autenticação para todas as redes IEEE 802**
  - Autenticação mútua a nível MAC (L2)
- **Originalmente desenhado para grandes redes**
  - Campus Universitários, Empresas, ...
  - Modelo foi expandido para redes sem fios
- **Foco: Distribuição de Chaves**
  - Apenas!
  - Outros protocolos focam-se nos restantes processos de segurança

IEEE 802.1x: Arquitetura

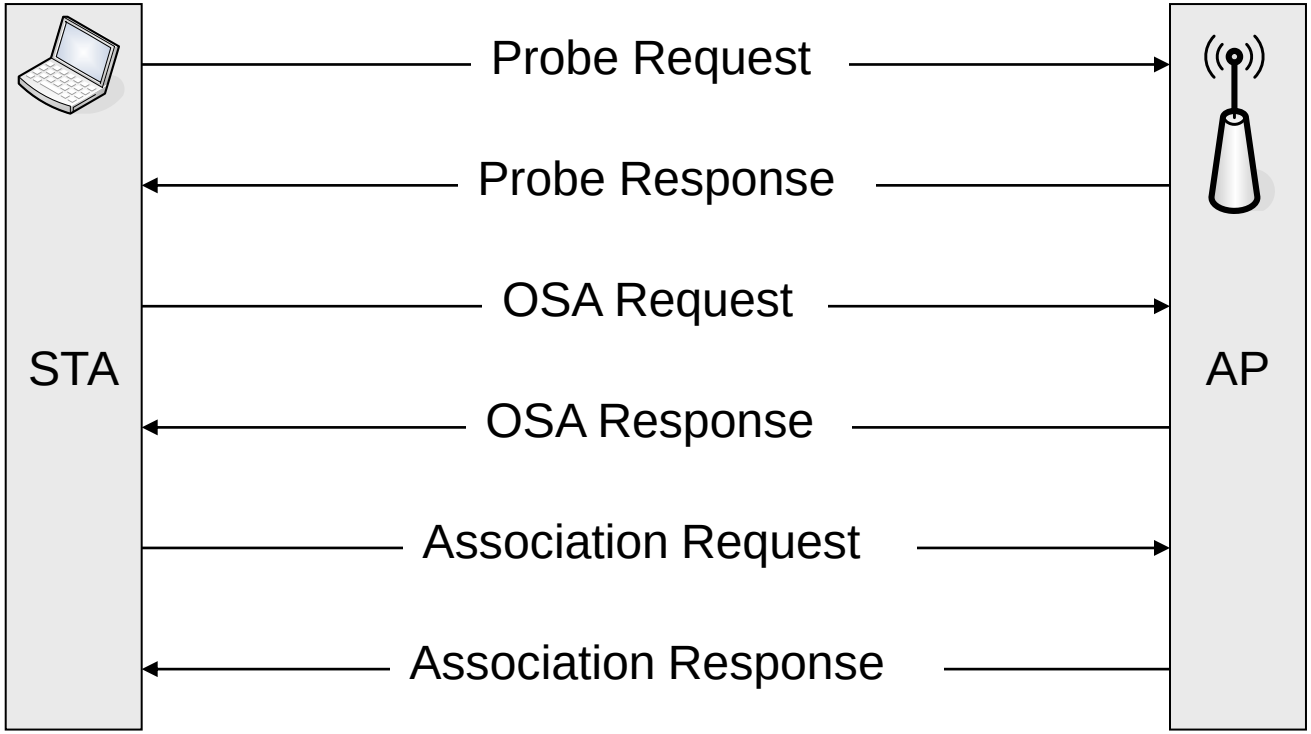




IEEE 802.1x: Fases

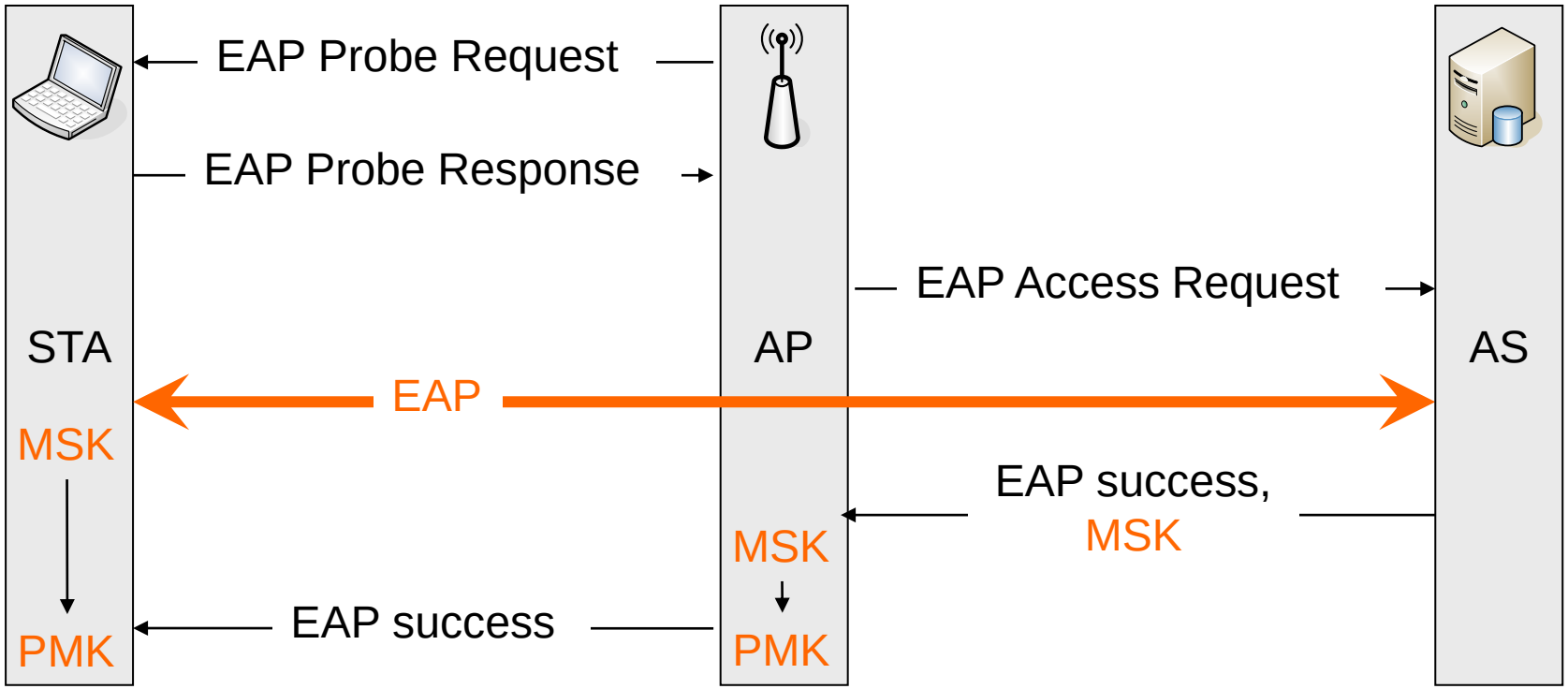


IEEE 802.1x: Fase 1 - Descoberta



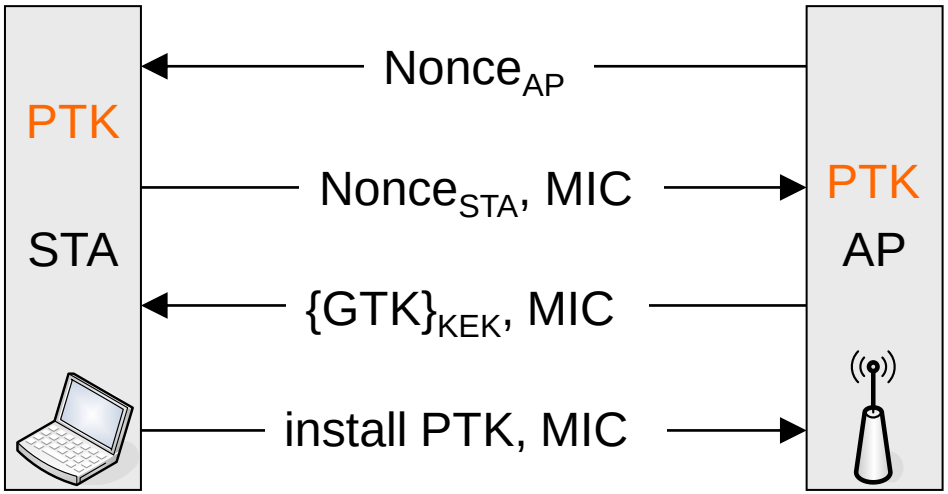
- **Depois deste ponto a STA APENAS conseguiu acesso ao AP**
  - Portas controladas por 802.1x continuam fechadas (não há dados do utilizador)

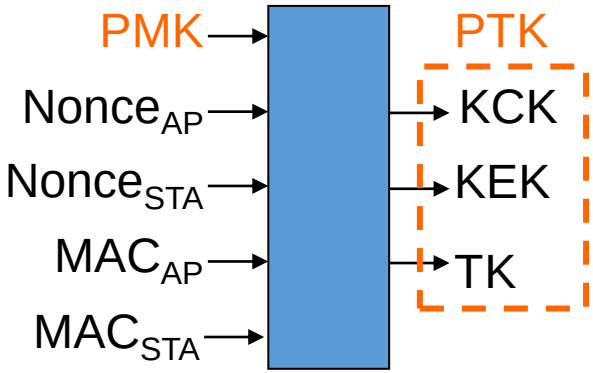
IEEE 802.1x: Fase 2 - Autenticação



- **No final desta fase o AP e a STA partilham informação criptográfica**
  - PMK (*Pairwise Master Key*)
- **Portos controlados (de dados) continuam fechados**

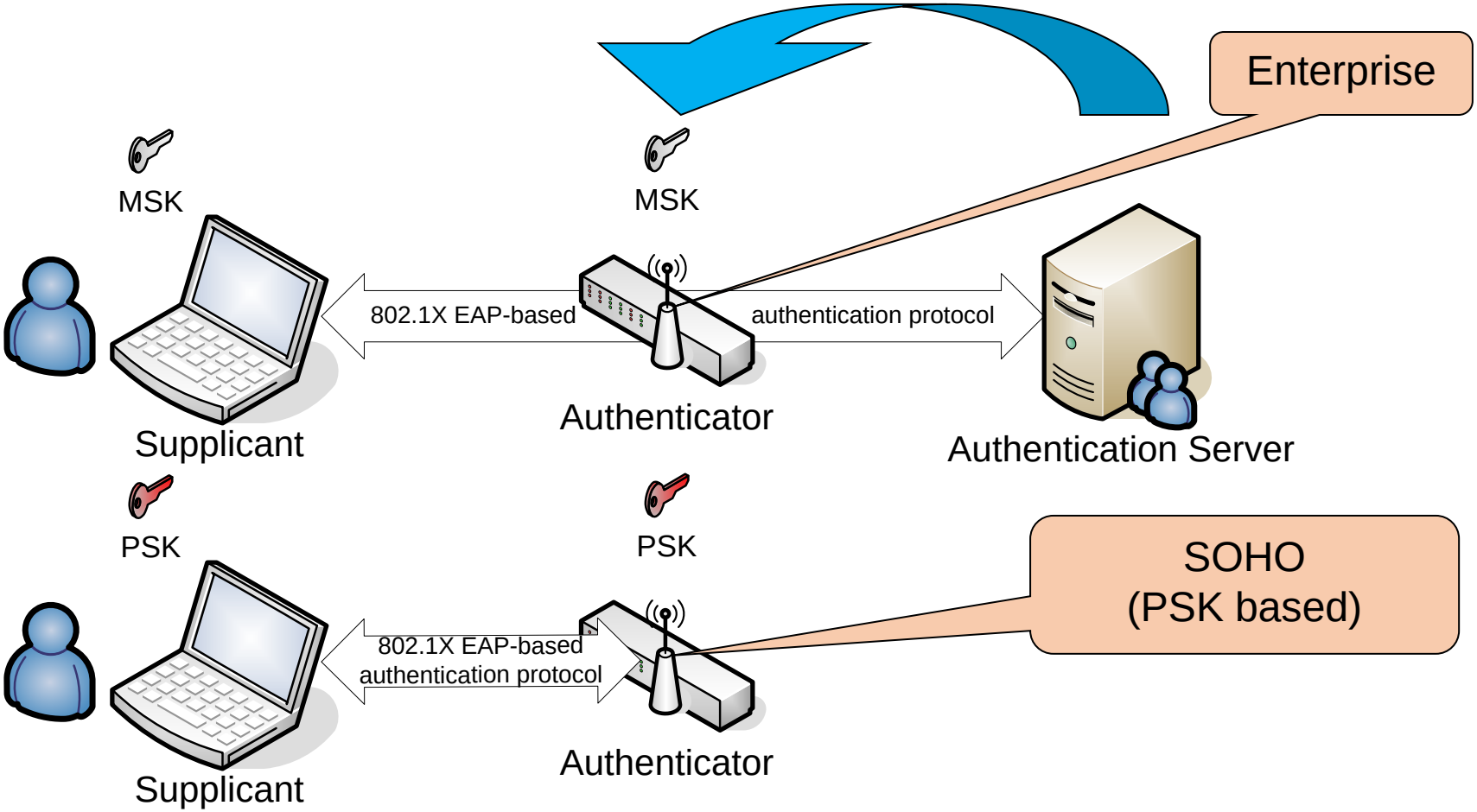
IEEE8 802.1x: Fase 3 - 4 Way Handshake



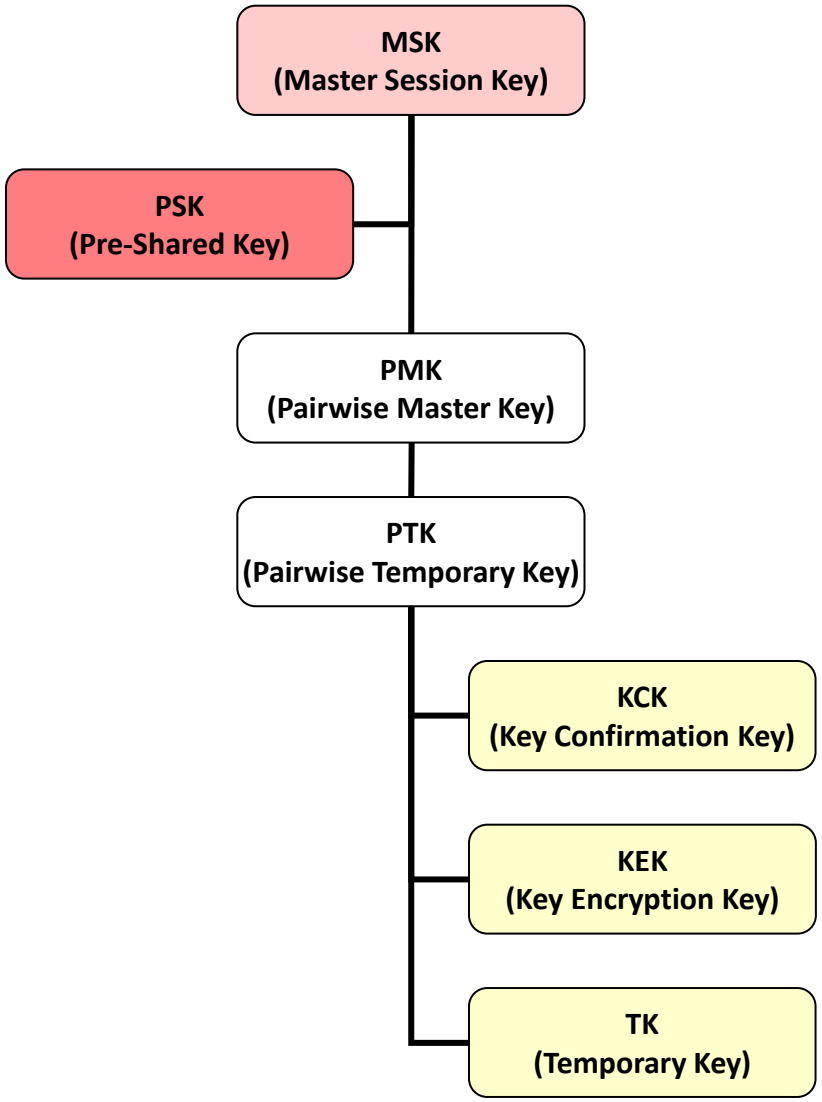


- **No final, o AP e a STA partilham informação criptográfica recente**
  - PTK (Pairwise Transient Key)
  - GTK (Group Transient Key)
- **Ambos acreditam que o outro conhece a PMK e PTK**
  - Através do uso de MICs
- **Portas controladas permitem tráfego Unicast**

IEEE 802.1x: Opções Arquiteturais



IEEE 802.1x: Hierarquia de Chaves



- **MSK**
  - Resultado direto de um processo com EAP
  - Arquitetura Enterprise
- **PSK**
  - Longo termo partilhada entre AP-STA
  - Arquitetura SOHO
- **PMK**
  - Chave recente usada para autenticação mútua da AP-STA
  - Usada no 4WH
- **PTK**
  - Chave para proteger interações entre AP-STA
  - CKC / KEK: protocolo 4WH
    - TK: mesagens de dados do 802.11

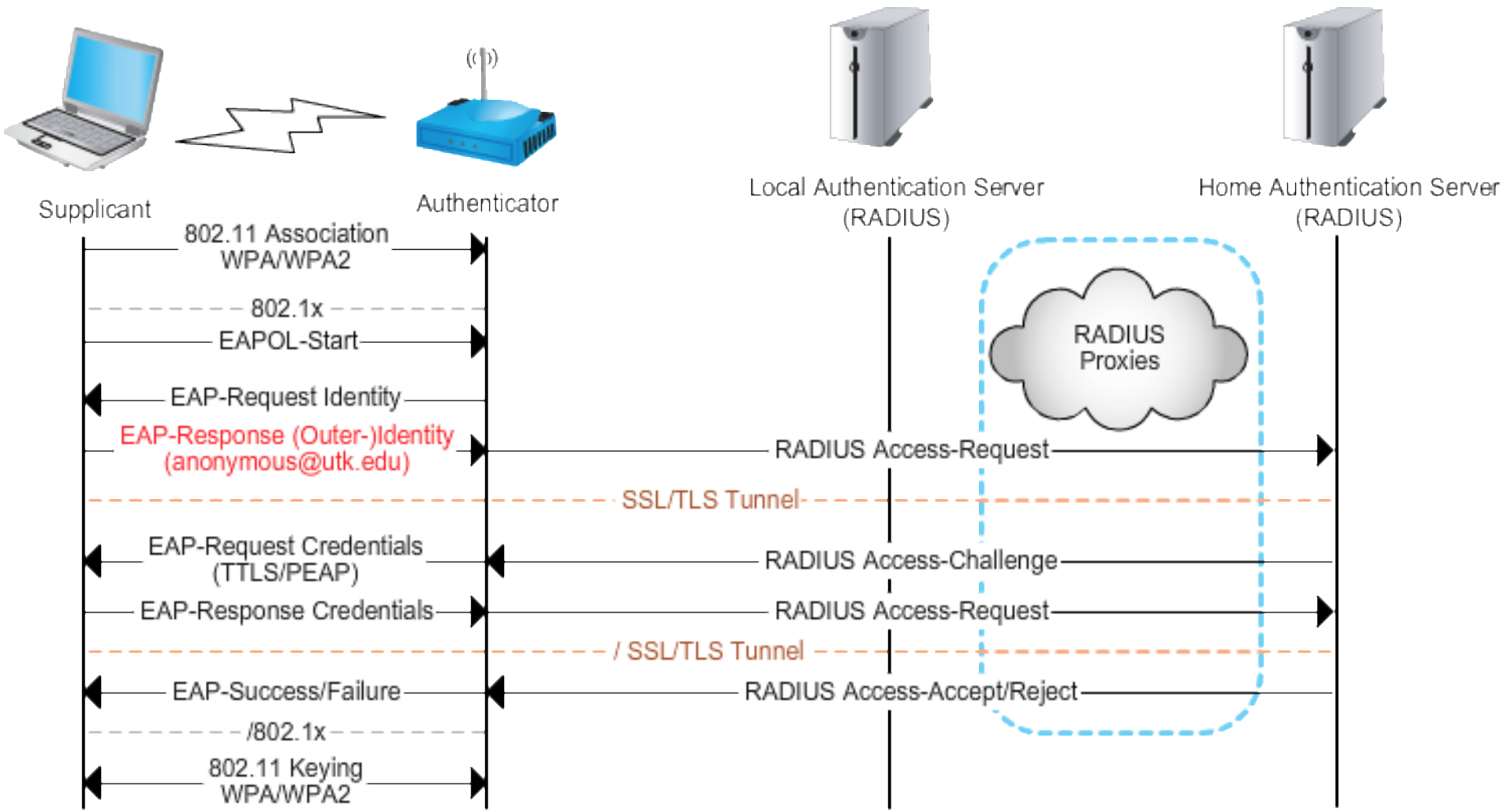
EAP (Extensible Authentication Protocol)

- **Inicialmente desenhado para o PPP**
  - Adaptado para o IEEE 802.1x
- **AP não é envolvido**
  - Reencaminha tráfego EAP
  - Alteração dos protocolos EAP não implicam alteração do AP
- **Não concebido para redes sem fios**
  - Tráfego não é protegido
  - Autenticação mútua não é obrigatória
    - Uma STA pode ser levada a ligar-se a um AP de um atacante

EAP: Alguns protocolos 802.1x

	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
AS	N/A	H(desafio, senha)	Chave Pública (certificado)		
Autenticação	H(desafio, senha)	H(desafio, senha)	Chave Pública (certificado)	EAP, Chave Pública (certificado)	PAP, CHAP, MS-CHAP, EAP
Gestão de Chaves	Não	Sim			
Riscos	- Exposição de identidade - Ataques por Dicionário - Host-in-the-Middle - Roubo de ligações	- Exposição de identidade - Ataques por Dicionário - Host-in-the-Middle	- Exposição de identidade		- Exposição de identidade (fase 1)

eduroam: 802.1x, PEAP, MS-CHAPv2



IEEE 802.11: Segurança resolvida?

- **Ataques por dicionário ainda são possíveis**
  - E irão continuar a existir por algum tempo (... senhas)
- **Apenas os dados são protegidos**
  - Mensagens de gestão não são protegidos
  - Atacantes podem desautenticar/desassociar STAs vitimas
- **Problemas a nível do meio de acesso (CSMA)**
  - Escolha da janela de contenção permite que um atacante tenha mais tempo de acesso

WPA2: Vulnerabilidades

- **Falta de Segurança Futura**
- **Descoberta de senhas (WPA-PSK)**
- **Descoberta do PIN WPS**
- **Reinstalação de Chaves**
- **... outros**

WPA2: Ataques: Segurança Futura

- **Segurança Futura remete para a reutilização de chaves**
  - Um sistema possui segurança futura se a descoberta de uma chave não permitir aceder a sessões no passado

- **WPA-PSK não possui:**
  - Descoberta da PMK/PSK permite decifrar sessões anteriores

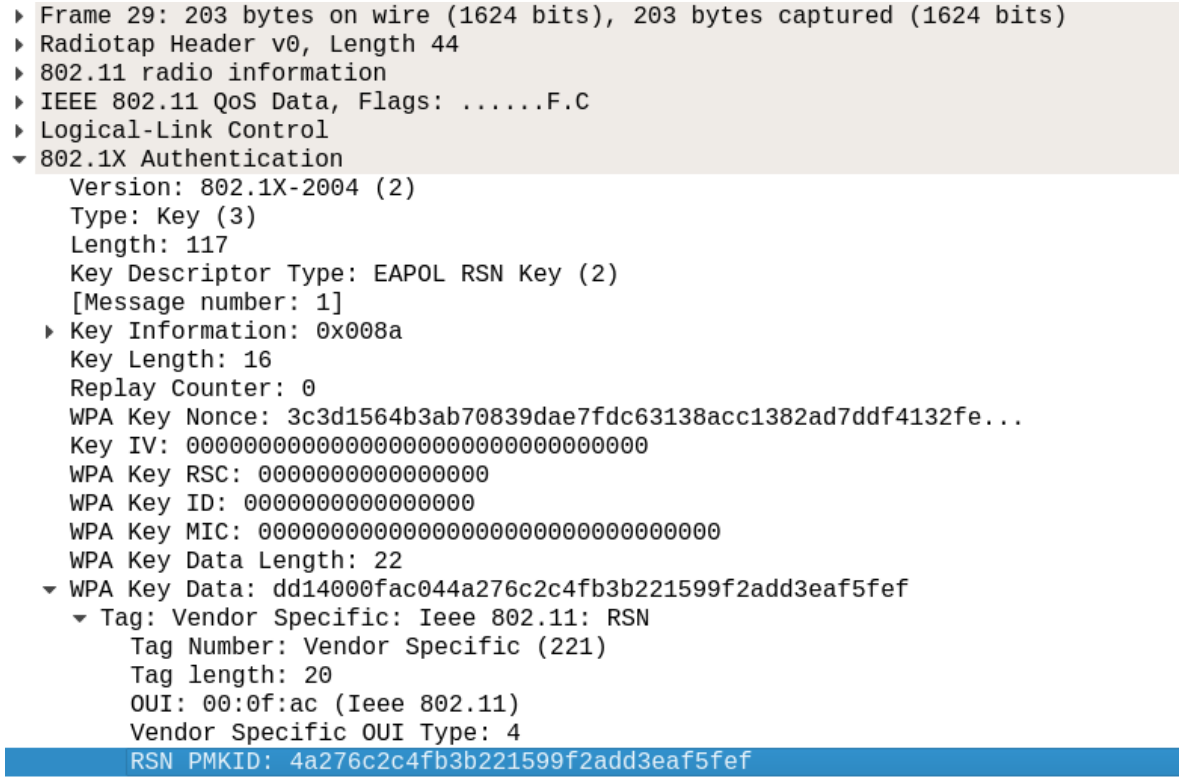
- **WPA-Enterprise pode possuir**
  - Se a PMK for diferente a cada autenticação

WPA2: Descoberta de senhas

- **Durante o 4WH o atacante consegue obter:**
  - ssid, ANonce, SNonce, AP MAC Address, STA MAC address
- **Chaves:**
  - PMK = PBKDF2(HMAC−SHA1, senha, ssid, 4096, 256)
  - PTK = PRF(PMK | ANonce | SNonce | AP MAC |STA MAC)
- **Ataque:**
  - Atacante espera por uma associação
  - ou... injeta uma mensagem de desassociação a uma vítima
    - Não consegue realizar ataque sem clientes
  - Atacante captura SSID, Nonces, endereços MAC
  - Offline: força bruta ou dicionário para calcular PTK
    - Usar MIC capturado na autenticação para validar senhas usadas
    - >400KH/s para um GPU

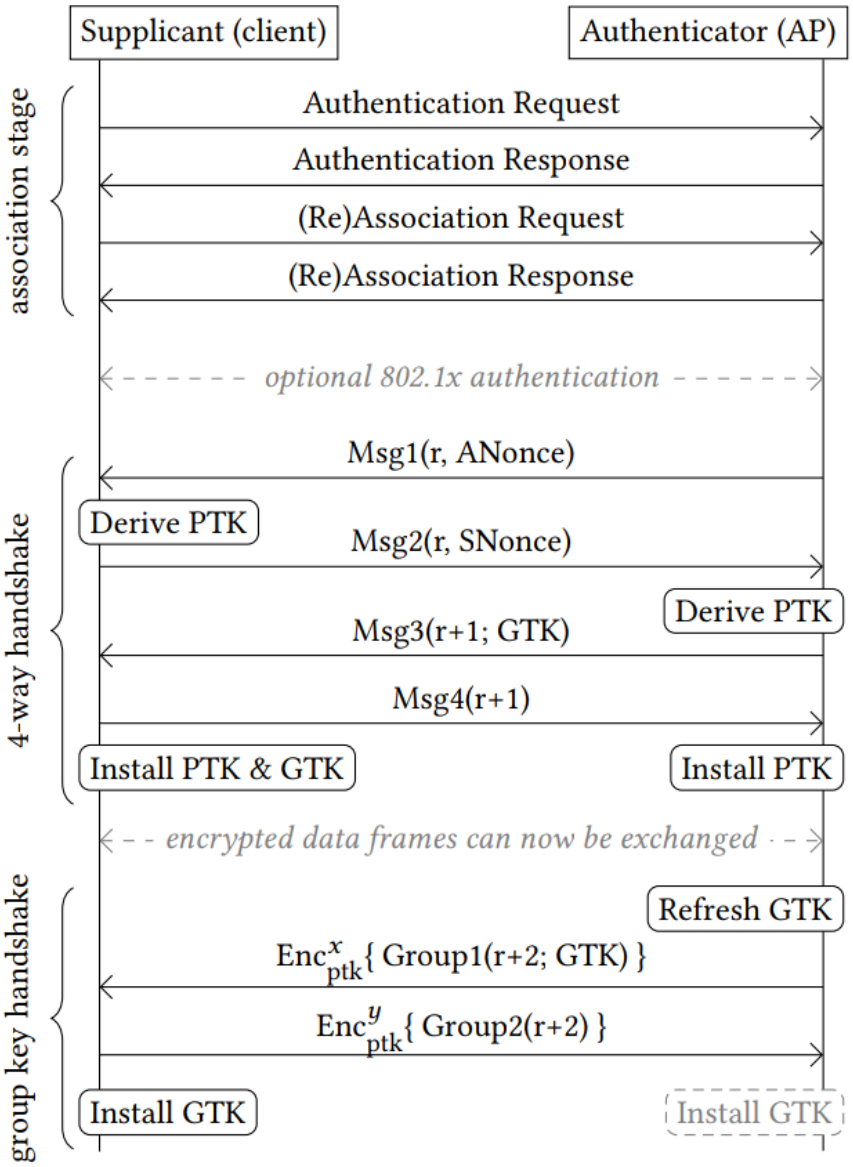
WPA2: Descoberta de senhas

- **APs enviam um valor para acelerar processo de autenticação**
  - PMKID=HMAC-SHA1-128(PMK, "PMK Name" | MAC_AP | MAC_STA)
  - Enviado em algumas mensagens de controlo
  - Ataque: Força bruta/dicionário, mas mais eficiente que 4HW



WPA2: Reinstalação de chaves

- **Objetivo: Forçar a vítima a reutilizar chaves**
- **Vulnerabilidade: Suplicant processa sempre a Msg3**
  - Mesmo que a PTK já esteja instalada
  - Na primeira mensagem, NONCE=1
- **Ataque:**
  - Bloquear Msg4
  - AP irá retransmitir Msg3
  - Chave é reinstalada
  - Pacote de dados volta a usar NONE=1



WPA2: Reinstalação de chaves

- **Objetivo: Forçar a vítima a reutilizar chaves**
- **Vulnerabilidade: Suplicant processa sempre a Msg3**
  - Mesmo que a PTK já esteja instalada
  - Na primeira mensagem, NONCE=1
- **Ataque:**
  - Bloquear Msg4
  - AP irá retransmitir Msg3
  - Chave é reinstalada
  - Pacote de dados volta a usar NONE=1